EMMETT DULANEY

- Targeted Review Tool for Both CompTIA A+ Exams
- The Perfect Companion to Any A+ Exam Study Tool
- Includes a CD with Four Practice Exams, Flashcards, and a Glossary of Key Terms

CompTIA A+® Complete REVIEW GUIDE

EXAM 220-701
EXAM 220-702

SYBEX | SERIOUS SKILLS.

CompTIA
A+® Complete
Review Guide

CompTIA A+® Complete Review Guide

Emmett Dulaney

WILEY
Wiley Publishing, Inc.

Acquisitions Editor: Jeff Kellum
Development Editor: Thomas Cirtin
Technical Editors: Quentin Docter and Neil Hester
Production Editors: Tim Tate and Amy Weintraub
Copy Editor: Elizabeth Welch
Editorial Manager: Pete Gaughan
Production Manager: Tim Tate
Vice President and Executive Group Publisher: Richard Swadley
Vice President and Publisher: Neil Edde
Media Project Manager 1: Laura Moss-Hollister
Media Associate Producer: Josh Frank
Media Quality Assurance: Marilyn Hummel
Book Designers: Judy Fung and Bill Gibson
Compositor: Craig Woods, Happenstance Type-O-Rama
Proofreader: Candace English
Indexer: Ted Laux
Project Coordinator, Cover: Lynsey Stanford
Cover Designer: Ryan Sneed

Published simultaneously in Canada

ISBN: 978-0-470-48650-4

Library of Congress Cataloging-in-Publication Data
Dulaney, Emmett A.
CompTIA A+ complete review guide (exams 220-701/220-702) / Emmett Dulaney. — 1st ed.
p. cm.
Summary: "Organized by exam objectives, this is a focused, concise review guide that works hand-in-hand with any learning tool, including the CompTIA A+ Complete Study Guide. The CompTIA A+ certification is the industry standard in terms of measuring a technician's hardware and software knowledge. As the most popular entry-level certification, it is particularly popular among individuals switching from another career to computers. This focused guide will help you focus on preparing to take the CompTIA A+ certification exam! A well-organized, ideal companion study tool to the Sybex CompTIA A+ guides. Each chapter discusses the main topics that are featured in the two parts of the exam. Discusses hardware, troubleshooting and maintenance, operating systems and software, networking, security, and operating procedures. Author is a well-known certification columnist and bestselling author."—Provided by publisher.
ISBN 978-0-470-48650-4
1. Electronic data processing personnel—Certification. 2. Computer technicians—Certification—Study guides. 3. Microcomputers—Maintenance and repair—Examinations—Study guides. 4. Computing Technology Industry Association—Examinations—Study guides. I. Title.
QA76.3.D82273 2009
004.165—dc22
2009025050

10 9 8 7 6 5 4 3 2 1

Dear Reader,

Thank you for choosing *CompTIA A+ Complete Review Guide*. This book is part of a family of premium-quality Sybex books, all of which are written by outstanding authors who combine practical experience with a gift for teaching.

Sybex was founded in 1976. More than 30 years later, we're still committed to producing consistently exceptional books. With each of our titles, we're working hard to set a new standard for the industry. From the paper we print on, to the authors we work with, our goal is to bring you the best books available.

I hope you see all that reflected in these pages. I'd be very interested to hear your comments and get your feedback on how we're doing. Feel free to let me know what you think about this or any other Sybex book by sending me an email at `nedde@wiley.com`. If you think you've found a technical error in this book, please visit `http://sybex.custhelp.com`. Customer feedback is critical to our efforts at Sybex.

Best regards,

Neil Edde
Vice President and Publisher
Sybex, an Imprint of Wiley

For Jim and Linda: thank you for always being there.

Acknowledgments

There are a great many people without whom this book would not be possible. Among them is Jeff Kellum, who does his job as an acquisitions editor extremely well and pulls you along with him, as well as Tom Cirtin and Amy Weintraub, who helped make sure this book is all it could be. Thanks must also go to Faithe Wempen and David Groth for their work on a previous edition.

About the Author

Emmett Dulaney holds or has held 18 vendor certifications and is the author of over 30 books. An assistant professor at Anderson University, he is the former director of training for Mercury Technical Solutions. He specializes in certification and cross-platform integration, and is a columnist for CertCities. Emmett can be reached at `eadulaney@comcast.net`.

Contents at a Glance

Contents

Introduction

The A+ certification program was developed by the Computing Technology Industry Association (CompTIA) to provide an industry-wide means of certifying the competency of computer service technicians. The A+ certification, which is granted to those who have attained the level of knowledge and troubleshooting skills that are needed to provide capable support in the field of personal computers, is similar to other certifications in the computer industry. The theory behind these certifications is that if you needed to have service performed on any of their products, you would sooner call a technician who has been certified in one of the appropriate programs than you would just call the first so-called "expert" in the phone book.

CompTIA's A+ exam objectives are periodically updated to keep the certification applicable to the most recent hardware and software. This is necessary because a technician must be able to work on the latest equipment. The most recent revisions to the objectives—and to the whole program—were introduced in 2009 and are reflected in this book.

This book and the Sybex *CompTIA A+ Complete Study Guide* (both the Standard and Deluxe Editions) are tools to help you prepare for this certification—and for the new areas of focus of a modern computer technician's job.

What Is A+ Certification?

The A+ certification program was created to offer a wide-ranging certification, in the sense that it's intended to certify competence with personal computers from many different makers/vendors. Everyone must take and pass the A+ Essentials exam (220-701) and the A+ Practical Application exam (220-702). This differs from the previous version of the certification, in which you took Essentials and then had a choice of three electives, from which you had to choose one.

CompTIA has left the door open for possible additional exams and designations. For more information on the exams, visit CompTIA's website at `www.comptia.org`.

You don't have to take the Essentials exam and the Practical Application exam at the same time; you have 90 days from the time you pass one exam to pass the second test. The A+ certification isn't awarded until you've passed both tests. For the latest pricing on the exams and updates to the registration procedures, call Prometric at 866-Prometric (776-6387) or 800-77-MICRO (776-4276) or Pearson VUE at (877) 551-7587. You can also go to either `www.2test.com` or `www.prometric.com` for Prometric or `www.vue.com` for Pearson VUE for additional information or to register online. If you have further questions about the scope of the exams or related CompTIA programs, refer to the CompTIA website at `www.comptia.org`.

Who Should Buy This Book?

If you want to acquire a solid foundation in personal-computer basics, and your goal is to prepare for the exams by filling in any gaps in your knowledge, this book is for you. You'll find clear explanations of the concepts you need to grasp and plenty of help to achieve the high level of professional competency you need in order to succeed in your chosen field.

If you want to become certified as an A+ holder, this book is definitely what you need. However, if you just want to attempt to pass the exam without really understanding the basics of personal computers, this guide isn't for you. It's written for people who want to acquire skills and knowledge of personal-computer basics.

How to Use This Book and the CD

We've included several testing features in the book and on the CD. These tools will help you retain vital exam content as well as prepare to sit for the actual exams:

Chapter Review Questions To test your knowledge as you progress through the book, there are review questions at the end of each chapter. As you finish each chapter, answer the review questions and then check your answers—the correct answers appear on the page following the review questions. You can go back to reread the section that deals with each question you got wrong to ensure that you answer correctly the next time you're tested on the material.

Electronic Flashcards You'll find flashcard questions on the CD for on-the-go review. These are short question and answers, just like the flashcards you probably used to study in school. You can answer them on your PC or download them onto a Palm device for quick and convenient reviewing.

Test Engine The CD also contains the Sybex Test Engine. Using this custom test engine, you can identify weak areas up front and then develop a solid studying strategy using each of these robust testing features. Our thorough readme file will walk you through the quick, easy installation process.

In addition to taking the assessment test and answering the chapter review questions in the test engine, you'll find sample exams on the CD. Take these practice exams just as if you were taking the actual exam (without any reference material). When you've finished the first exam, move on to the next one to solidify your test-taking skills. If you get more than 90 percent of the answers correct, you're ready to take the certification exams.

Glossary of Terms in PDF The CD contains a very useful glossary of terms in PDF (Adobe Acrobat) format so you can easily read it on any computer. If you have to travel and brush up on any key terms, and you have a laptop with a CD-ROM drive, you can do so with this useful resource.

Minimum System Requirements

You should have a minimum of 45MB of disk space, as well as Windows 2000 or higher to use the Sybex Test Engine. You will also need Adobe Acrobat Reader (included on the CD) for the glossary.

Tips for Taking the A+ Exams

Here are some general tips for taking your exams successfully:

- Bring two forms of ID with you. One must be a photo ID, such as a driver's license. The other can be a major credit card or a passport. Both forms must include a signature.
- Arrive early at the exam center so you can relax and review your study materials, particularly tables and lists of exam-related information.
- Read the questions carefully. Don't be tempted to jump to an early conclusion. Make sure you know exactly what the question is asking.
- Don't leave any unanswered questions. Unanswered questions are scored against you.
- There will be questions with multiple correct responses. When there is more than one correct answer, a message at the bottom of the screen will prompt you to either "Choose two" or "Choose all that apply." Be sure to read the messages displayed to know how many correct answers you must choose.
- When answering multiple-choice questions you're not sure about, use a process of elimination to get rid of the obviously incorrect answers first. Doing so will improve your odds if you need to make an educated guess.
- On form-based tests (nonadaptive), because the hard questions will eat up the most time, save them for last. You can move forward and backward through the exam.
- For the latest pricing on the exams and updates to the registration procedures, visit CompTIA's website at `www.comptia.org`.

Exam Objectives

CompTIA goes to great lengths to ensure that its certification programs accurately reflect the IT industry's best practices. The company does this by establishing Cornerstone Committees for each of its exam programs. Each committee comprises a small group of IT professionals, training providers, and publishers who are responsible for establishing the exam's baseline competency level and who determine the appropriate target audience level.

Once these factors are determined, CompTIA shares this information with a group of hand-selected Subject Matter Experts (SMEs). These folks are the true brainpower behind the certification program. They review the committee's findings, refine them, and shape them into the objectives you see before you. CompTIA calls this process a Job Task Analysis (JTA).

Finally, CompTIA conducts a survey to ensure that the objectives and weightings truly reflect the job requirements. Only then can the SMEs go to work writing the hundreds of questions needed for the exam. And, in many cases, they have to go back to the drawing board for further refinements before the exam is ready to go live in its final state. So, rest assured, the content you're about to learn will serve you long after you take the exam.

Exam objectives are subject to change at any time without prior notice and at CompTIA's sole discretion. Please visit the certification page of CompTIA's website at `www.comptia.org` for the most current listing of exam objectives.

CompTIA also publishes relative weightings for each of the exam's objectives. The following tables list the objective domains and the extent to which they're represented on each exam. For example, on the Essentials exam expect to spend more time answering questions that pertain to operating systems than to professionalism.

Essentials Exam Domains	**% of Exam**
1.0 Hardware	27%
2.0 Troubleshooting, Repair & Maintenance	20%
3.0 Operating System and Software	20%
4.0 Networking	15%
5.0 Security	8%
6.0 Operational Procedure	10%
Total	**100%**

Practical Application Exam Domains	**% of Exam**
1.0 Hardware	38%
2.0 Operating Systems	34%
3.0 Networking	15%
4.0 Security	13%
Total	**100%**

The following sections look at the objectives beneath each of these in more detail.

CompTIA A+ Essentials Exam (220-701) Objectives

1.0 Hardware

1.1 Categorize storage devices and backup media

- FDD
- HDD
  - Solid state vs. magnetic
- Optical drives
  - CD / DVD/ RW / Blu-Ray
- Removable storage
  - Tape drive
  - Solid state (e.g. thumb drive, flash, SD cards, USB)
  - External CD-RW and hard drive
  - Hot swappable devices and non-hot swappable devices

1.2 Explain motherboard components, types and features

- Form Factor
  - ATX / BTX
  - Micro ATX
  - NLX
- I/O interfaces
  - Sound
  - Video
  - USB 1.1 and 2.0
  - Serial
  - IEEE 1394 / Firewire
  - Parallel
  - NIC
  - Modem
  - PS/2
- Memory slots
  - RIMM
  - DIMM
  - SODIMM
  - SIMM

- Processor sockets
- Bus architecture
- Bus slots
  - PCI
  - AGP
  - PCIe
  - AMR
  - CNR
  - PCMCIA
- PATA
  - IDE
  - EIDE
- SATA, eSATA
- Contrast RAID (levels 0, 1, 5)
- Chipsets
- BIOS/ CMOS / Firmware
  - POST
  - CMOS battery
- Riser card / daughter board

1.3 Classify power supplies types and characteristics

- AC adapter
- ATX proprietary
- Voltage, wattage and capacity
- Voltage selector switch
- Pins (20, 24)

1.4 Explain the purpose and characteristics of CPUs and their features

- Identify CPU types
  - AMD
  - Intel
- Hyper threading
- Multi core
  - Dual core
  - Triple core
  - Quad core

- Onchip cache
  - L1
  - L2
- Speed (real vs. actual)
- 32bit vs. 64bit

1.5 Explain cooling methods and devices

- Heat sinks
- CPU and case fans
- Liquid cooling systems
- Thermal compound

1.6 Compare and contrast memory types, characteristics and their purpose

- Types
  - DRAM
  - SRAM
  - SDRAM
  - DDR / DDR2 / DDR3
  - RAMBUS
- Parity versus Non-parity
- ECC vs. non-ECC
- Single sided vs. double sided
- Single channel vs. dual channel
- Speed
  - PC100
  - PC133
  - PC2700
  - PC3200
  - DDR3-1600
  - DDR2-667

1.7 Distinguish between the different display devices and their characteristics

- Projectors, CRT and LCD
- LCD technologies
  - Resolution (e.g. XGA, SXGA+, UXGA, WUXGA)
  - Contrast ratio
  - Native resolution

- Connector types
  - VGA
  - HDMi
  - S-Video
  - Component / RGB
  - DVI pin compatibility
- Settings
  - Refresh rate
  - Resolution
  - Multi-monitor
  - Degauss

1.8 Install and configure peripherals and input devices

- Mouse
- Keyboard
- Bar code reader
- Multimedia (e.g. web and digital cameras, MIDI, microphones)
- Biometric devices
- Touch screen
- KVM switch

1.9 Summarize the function and types of adapter cards

- Video
  - PCI
  - PCIe
  - AGP
- Multimedia
  - Sound card
  - TV tuner cards
  - Capture cards
- I/O
  - SCSI
  - Serial
  - USB
  - Parallel

- Communications
  - NIC
  - Modem

1.10 Install, configure, and optimize laptop components and features

- Expansion devices
  - PCMCIA cards
  - PCI Express cards
  - Docking station
- Communications connections
  - Bluetooth
  - Infrared
  - Cellular WAN
  - Ethernet
  - Modem
- Power and electrical input devices
  - Auto-switching
  - Fixed input power supplies
  - Batteries
- Input devices
  - Stylus / digitizer
  - Function keys
  - Point devices (e.g. touch pad, point stick / track point)

1.11 Install and configure printers

- Differentiate between printer types
  - Laser
  - Inkjet
  - Thermal
  - Impact
- Local vs. network printers
- Printer drivers (compatibility)
- Consumables

2.0 Troubleshooting, Repair and Maintenance

2.1 Given a scenario, explain the troubleshooting theory

- Identify the problem
  - Question user and identify user changes to computer and perform backups before making changes
- Establish a theory of probable cause (question the obvious)
- Test the theory to determine cause
  - Once theory is confirmed determine next steps to resolve problem
  - If theory is not confirmed re-establish new theory or escalate
- Establish a plan of action to resolve the problem and implement the solution
- Verify full system functionality and if applicable implement preventative measures
- Document findings, actions and outcomes

2.2 Given a scenario, explain and interpret common hardware and operating system symptoms and their causes

- OS related symptoms
  - Bluescreen
  - System lock-up
  - Input/output device
  - Application install
  - Start or load
  - Windows specific printing problems
    - Print spool stalled
    - Incorrect / incompatible driver
- Hardware related symptoms
  - Excessive heat
  - Noise
  - Odors
  - Status light indicators
  - Alerts
  - Visible damage (e.g. cable, plastic)
- Use documentation and resources
  - User / installation manuals
  - Internet / web based
  - Training materials

2.3 Given a scenario, determine the troubleshooting methods and tools for printers
- Manage print jobs
- Print spooler
- Printer properties and settings
- Print a test page

2.4 Given a scenario, explain and interpret common laptop issues and determine the appropriate basic troubleshooting method
- Issues
  - Power conditions
  - Video
  - Keyboard
  - Pointer
  - Stylus
  - Wireless card issues
- Methods
  - Verify power (e.g. LEDs, swap, AC adapter)
  - Remove unneeded peripherals
  - Plug in external monitor
  - Toggle Fn keys or hardware switches
  - Check LCD cutoff switch
  - Verify backlight functionality and pixilation
  - Check switch for built-in WIFI antennas or external antennas

2.5 Given a scenario, integrate common preventative maintenance techniques
- Physical inspection
- Updates
  - Driver
  - Firmware
  - OS
  - Security
- Scheduling preventative maintenance
  - Defrag
  - Scandisk
  - Check disk
  - Startup programs

- Use of appropriate repair tools and cleaning materials
  - Compressed air
  - Lint free cloth
  - Computer vacuum and compressors
- Power devices
  - Appropriate source such as power strip, surge protector or UPS
- Ensuring proper environment
- Backup procedures

3.0 Operating Systems and Software

Unless otherwise noted, operating systems referred to within include Microsoft Windows 2000, Windows XP Professional, XP Home, XP Media-Center, Windows Vista Home, Home Premium, Business and Ultimate.

3.1 Compare and contrast the different Windows Operating Systems and their features

- Windows 2000, Windows XP 32bit vs. 64bit, Windows Vista 32bit vs. 64bit
  - Sidebar Aero, UAC, minimum system requirements, system limits
  - Windows 2000 and newer – upgrade paths and requirements
  - Terminology (32bit vs. 64bit – x86 vs. x64)
  - Application compatibility, installed program locations (32bit vs. 64bit), Windows compatibility mode
  - User interface, start bar layout

3.2 Given a scenario, demonstrate proper use of user interfaces

- Windows Explorer
- My Computer
- Control Panel
- Command prompt utilities
  - telnet
  - ping
  - ipconfig
- Run line utilities
  - msconfig
  - msinfo32
  - Dxdiag

- Cmd
- REGEDIT
- My Network Places
- Task bar / systray
- Administrative tools
  - Performance Monitor, Event Viewer, Services, Computer Management
- MMC
- Task Manager
- Start Menu

3.3 Explain the process and steps to install and configure the Windows OS

- File systems
  - FAT32 vs. NTFS
- Directory structures
  - Create folders
  - Navigate directory structures
- Files
  - Creation
  - Extensions
  - Attributes
  - Permissions
- Verification of hardware compatibility and minimum requirements
- Installation methods
  - Boot media such as CD, floppy or USB
  - Network installation
  - Install from image
  - Recover CD
  - Factory recovery partition
- Operating system installation options
  - File system type
  - Network configuration
  - Repair install
- Disk preparation order
  - Format drive
  - Partition
  - Start installation

- Device Manager
  - Verify
  - Install and update devices drivers
  - Driver signing
- User data migration – User State Migration Tool (USMT)
- Virtual memory
- Configure power management
  - Suspend
  - Wake on LAN
  - Sleep timers
  - Hibernate
  - Standby
- Demonstrate safe removal of peripherals

3.4 Explain the basics of boot sequences, methods and startup utilities

- Disk boot order / device priority
  - Types of boot devices (disk, network, USB, other)
- Boot options
  - Safe mode
  - Boot to restore point
  - Recovery options
    - Automated System Recovery (ASR)
    - Emergency Repair Disk (ERD)
    - Recovery console

4.0 Networking

4.1 Summarize the basics of networking fundamentals, including technologies, devices and protocols

- Basics of configuring IP addressing and TCP/IP properties (DHCP, DNS)
- Bandwidth and latency
- Status indicators
- Protocols (TCP/IP, NETBIOS)
- Full-duplex, half-duplex
- Basics of workgroups and domains
- Common ports: HTTP, FTP, POP, SMTP, TELNET, HTTPS
- LAN / WAN

- Hub, switch and router
- Identify Virtual Private Networks (VPN)
- Basics class identification

4.2 Categorize network cables and connectors and their implementations

- Cables
  - Plenum / PVC
  - UTP (e.g. CAT3, CAT5 / 5e, CAT6)
  - STP
  - Fiber
  - Coaxial cable
- Connectors
  - RJ45
  - RJ11

4.3 Compare and contrast the different network types

- Broadband
  - DSL
  - Cable
  - Satellite
  - Fiber
- Dial-up
- Wireless
  - All 802.11 types
  - WEP
  - WPA
  - SSID
  - MAC filtering
  - DHCP settings
- Bluetooth
- Cellular

5.0 Security

5.1 Explain the basic principles of security concepts and technologies

- Encryption technologies
- Data wiping / hard drive destruction / hard drive recycling

- Software firewall
  - Port security
  - Exceptions
- Authentication technologies
  - User name
  - Password
  - Biometrics
  - Smart cards
- Basics of data sensitivity and data security
  - Compliance
  - Classifications
  - Social engineering

5.2 Summarize the following security features

- Wireless encryption
  - WEPx and WPAx
  - Client configuration (SSID)
- Malicious software protection
  - Viruses
  - Trojans
  - Worms
  - Spam
  - Spyware
  - Adware
  - Grayware
- BIOS Security
  - Drive lock
  - Passwords
  - Intrusion detection
  - TPM
- Password management / password complexity
- Locking workstation
  - Hardware
  - Operating system
- Biometrics
  - Fingerprint scanner

6.0 Operational Procedure

6.1 Outline the purpose of appropriate safety and environmental procedures and given a scenario apply them

- ESD
- EMI
  - Network interference
  - Magnets
- RFI
  - Cordless phone interference
  - Microwaves
- Electrical safety
  - CRT
  - Power supply
  - Inverter
  - Laser printers
  - Matching power requirements of equipment with power distribution and UPSs
- Material Safety Data Sheets (MSDS)
- Cable management
  - Avoiding trip hazards
- Physical safety
  - Heavy devices
  - Hot components
- Environmental – consider project disposal procedures

6.2 Given a scenario, demonstrate the appropriate use of communication skills and professionalism in the workplace

- Use proper language – avoid jargon, acronyms, slang
- Maintain a positive attitude
- Listen and do not interrupt a customer
- Be culturally sensitive
- Be on time
  - If late contact the customer
- Avoid distractions
  - Personal calls
  - Talking to co-workers while interacting with customers
  - Personal interruptions

- Dealing with a difficult customer or situation
  - Avoid arguing with customers and/or being defensive
  - Do not minimize customers' problems
  - Avoid being judgmental
  - Clarify customer statements
    - Ask open-ended questions to narrow the scope of the problem
    - Restate the issue or question to verify understanding
- Set and meet expectations / timeline and communicate status with the customer
  - Offer different repair / replacement options if applicable
  - Provide proper documentation on the services provided
  - Follow up with customer / user at a later date to verify satisfaction
- Deal appropriately with customers confidential materials
  - Located on computer, desktop, printer, etc.

CompTIA A+ Practical Application Exam (220-702) Objectives

1.0 Hardware

1.1 Given a scenario, install, configure and maintain personal computer components

- Storage devices
  - HDD
    - SATA
    - PATA
    - Solid state
  - FDD
  - Optical drives
    - CD / DVD / RW / Blu-Ray
  - Removable
  - External
- Motherboards
  - Jumper settings
  - CMOS battery
  - Advanced BIOS settings
  - Bus speeds
  - Chipsets

- Firmware updates
- Socket types
- Expansion slots
- Memory slots
- Front panel connectors
- I/O ports
  - Sound, video, USB 1.1, USB 2.0, serial, IEEE 1394 / FireWire, parallel, NIC, modem, PS/2

- Power supplies
  - Wattages and capacity
  - Connector types and quantity
  - Output voltage
- Processors
  - Socket types
  - Speed
  - Number of cores
  - Power consumption
  - Cache
  - Front side bus
  - 32bit vs. 64bit
- Memory
- Adapter cards
  - Graphics cards
  - Sound cards
  - Storage controllers
    - RAID cards (RAID array – levels 0,1,5)
    - eSATA cards
  - I/O cards
    - FireWire
    - USB
    - Parallel
    - Serial
  - Wired and wireless network cards
  - Capture cards (TV, video)
  - Media reader

- Cooling systems
  - Heat sinks
  - Thermal compound
  - CPU fans
  - Case fans

1.2 Given a scenario, detect problems, troubleshoot and repair/replace personal computer components

- Storage devices
  - HDD
    - SATA
    - PATA
    - Solid state
  - FDD
  - Optical drives
    - CD / DVD / RW / Blu-Ray
  - Removable
  - External
- Motherboards
  - Jumper settings
  - CMOS battery
  - Advanced BIOS settings
  - Bus speeds
  - Chipsets
  - Firmware updates
  - Socket types
  - Expansion slots
  - Memory slots
  - Front panel connectors
  - I/O ports
    - Sound, video, USB 1.1, USB 2.0, serial, IEEE 1394 / FireWire, parallel, NIC, modem, PS/2
- Power supplies
  - Wattages and capacity
  - Connector types and quantity
  - Output voltage

- Processors
  - Socket types
  - Speed
  - Number of cores
  - Power consumption
  - Cache
  - Front side bus
  - 32bit vs. 64bit
- Memory
- Adapter cards
  - Graphics cards - memory
  - Sound cards
  - Storage controllers
    - RAID cards
    - eSATA cards
  - I/O cards
    - FireWire
    - USB
    - Parallel
    - Serial
  - Wired and wireless network cards
  - Capture cards (TV, video)
  - Media reader
- Cooling systems
  - Heat sinks
  - Thermal compound
  - CPU fans
  - Case fans

1.3 Given a scenario, install, configure, detect problems, troubleshoot and repair/replace laptop components

- Components of the LCD including inverter, screen and video card
- Hard drive and memory
- Disassemble processes for proper re-assembly
  - Document and label cable and screw locations
  - Organize parts

        - Refer to manufacturer documentation
        - Use appropriate hand tools
    - Recognize internal laptop expansion slot types
    - Upgrade wireless cards and video card
    - Replace keyboard, processor, plastics, pointer devices, heat sinks, fans, system board, CMOS battery, speakers

1.4 Given a scenario, select and use the following tools

- Multimeter
- Power supply tester
- Specialty hardware / tools
- Cable testers
- Loop back plugs
- Anti-static pad and wrist strap
- Extension magnet

1.5 Given a scenario, detect and resolve common printer issues

- Symptoms
    - Paper jams
    - Blank paper
    - Error codes
    - Out of memory error
    - Lines and smearing
    - Garbage printout
    - Ghosted image
    - No connectivity
- Issue resolution
    - Replace fuser
    - Replace drum
    - Clear paper jam
    - Power cycle
    - Install maintenance kit (reset page count)
    - Set IP on printer
    - Clean printer

2.0 Operating Systems

Unless otherwise noted, operating systems referred to within include Microsoft Windows 2000, Windows XP Professional, XP Home, XP Media-Center, Windows Vista Home, Home Premium, Business and Ultimate.

2.1 Select the appropriate commands and options to troubleshoot and resolve problems

- MSCONFIG
- DIR
- CHKDSK (/f /r)
- EDIT
- COPY (/a /v /y)
- XCOPY
- FORMAT
- IPCONFIG (/all /release /renew)
- PING (-t –l)
- MD / CD / RD
- NET
- TRACERT
- NSLOOKUP
- [command name] /?
- SFC

2.2 Differentiate between Windows Operating System directory structures (Windows 2000, XP, and Vista)

- User file locations
- System file locations
- Fonts
- Temporary files
- Program files
- Offline files and folders

2.3 Given a scenario, select and use system utilities / tools and evaluate the results

- Disk management tools
  - DEFRAG
  - NTBACKUP
  - Check Disk

- Disk Manager
  - Active, primary, extended and logical partitions
  - Mount points
  - Mounting a drive
  - FAT32 and NTFS
  - Drive status
    - Foreign drive
    - Healthy
    - Formatting
    - Active unallocated
    - Failed
    - Dynamic
    - Offline
    - Online
- System monitor
- Administrative tools
  - Event Viewer
  - Computer Management
  - Services
  - Performance Monitor
- Devices Manager
  - Enable
  - Disable
  - Warnings
  - Indicators
- Task Manager
  - Process list
  - Resource usage
  - Process priority
  - Termination
- System Information
- System restore
- Remote Desktop Protocol (Remote Desktop / Remote Assistance)
- Task Scheduler
- Regional settings and language settings

2.4 Evaluate and resolve common issues

- Operational Problems
  - Windows specific printing problems
    - Print spool stalled
    - Incorrect / incompatible driver / form printing
  - Auto-restart errors
  - Bluescreen error
  - System lock-up
  - Devices drivers failure (input / output devices)
  - Application install, start or load failure
  - Service fails to start
- Error Messages and Conditions
  - Boot
    - Invalid boot disk
    - Inaccessible boot drive
    - Missing NTLDR
  - Startup
    - Device / service failed to start
    - Device / program in registry not found
  - Event viewer (errors in the event log)
  - System Performance and Optimization
    - Aero settings
    - Indexing settings
    - UAC
    - Side bar settings
    - Startup file maintenance
    - Background processes

3.0 Networking

3.1 Troubleshoot client-side connectivity issues using appropriate tools

- TCP/IP settings
  - Gateway
  - Subnet mask
  - DNS

- DHCP (dynamic vs. static)
- NAT (private and public)

- Characteristics of TCP/IP
  - Loopback addresses
  - Automatic IP addressing
- Mail protocol settings
  - SMTP
  - IMAP
  - POP
- FTP settings
  - Ports
  - IP addresses
  - Exceptions
  - Programs
- Proxy settings
  - Ports
  - IP addresses
  - Exceptions
  - Programs
- Tools (use and interpret results)
  - Ping
  - Tracert
  - Nslookup
  - Netstat
  - Net use
  - Net /?
  - Ipconfig
  - telnet
  - SSH
- Secure connection protocols
  - SSH
  - HTTPS
- Firewall settings
  - Open and closed ports
  - Program filters

3.2 Install and configure a small office home office (SOHO) network

- Connection types
  - Dial-up
  - Broadband
    - DSL
    - Cable
    - Satellite
    - ISDN
  - Wireless
    - All 802.11
    - WEP
    - WPA
    - SSID
    - MAC filtering
    - DHCP settings
  - Routers / Access Points
    - Disable DHCP
    - Use static IP
    - Change SSID from default
    - Disable SSID broadcast
    - MAC filtering
    - Change default username and password
    - Update firmware
    - Firewall
  - LAN (10/100/1000BaseT, Speeds)
  - Bluetooth (1.0 vs. 2.0)
  - Cellular
  - Basic VoIP (consumer applications)
- Basics of hardware and software firewall configuring
  - Port assignment / setting up rules (exceptions)
  - Port forwarding / port triggering
- Physical installation
  - Wireless router placement
  - Cable length

4.0 Security

4.1 Given a scenario, prevent, troubleshoot and remove viruses and malware

- Use antivirus software
- Identify malware symptoms
- Quarantine infected systems
- Research malware types, symptom and solutions (virus encyclopedia)
- Remediate infected systems
- Update antivirus software
  - Signature and ending updates
  - Automatic vs. manual
- Schedule scans
- Repair boot blocks
- Scan and removal techniques
  - Safe mode
  - Boot environment
- Educate end user

4.2 Implement security and troubleshoot common issues

- Operating systems
  - Local users and groups: Administrator, Power Users, Guest, Users
  - Vista User Access Control (UAC)
  - NTFS vs. Share permissions
    - Allow vs. deny
    - Difference between moving and copying folders and files
    - File attributes
  - Shared files and folders
    - Administrative shares vs. local shares
    - Permission propagation
    - Inheritance
  - System files and folders
  - Encryption (Bitlocker, EFS)
  - User authentication
- System
  - BIOS security
    - Drive lock
    - Passwords
    - Intrusion detection
    - TPM

CompTIA A+ Essentials

PART I

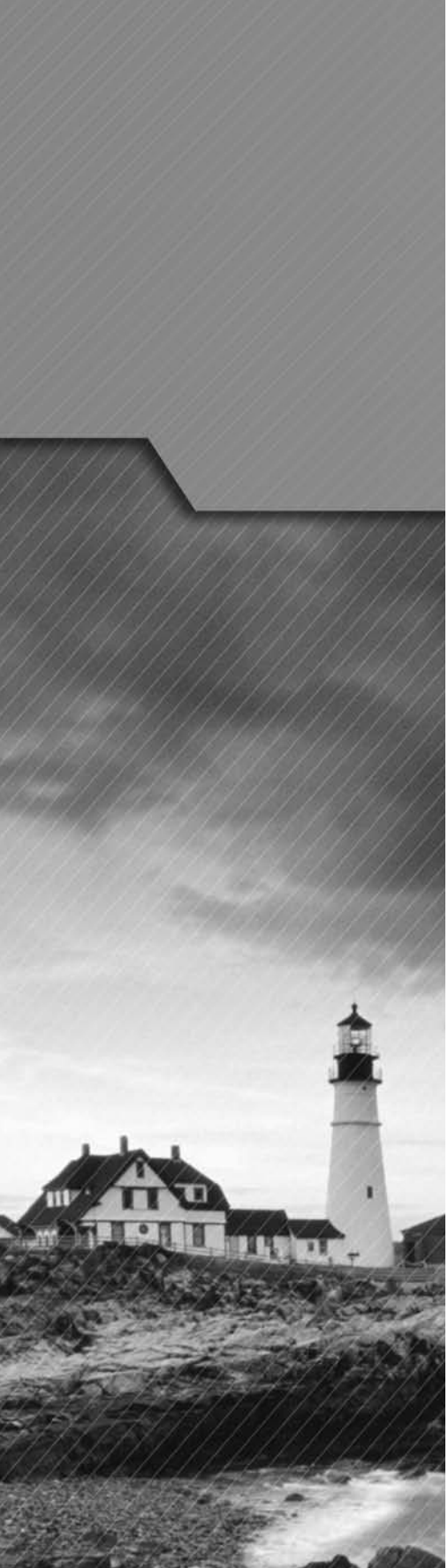
Chapter

1

Hardware

COMPTIA A+ ESSENTIALS EXAM OBJECTIVES COVERED IN THIS CHAPTER:

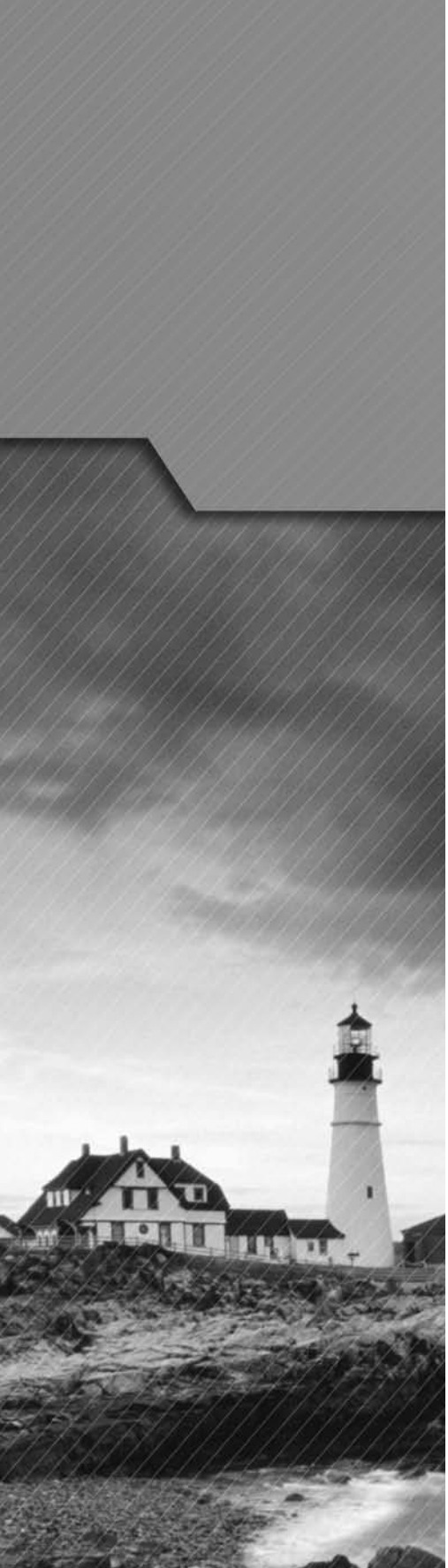
- ✓ **1.1 Categorize storage devices and backup media**
  - FDD
  - HDD
    - Solid state vs. magnetic
  - Optical drives
    - CD / DVD/ RW / Blu-Ray
  - Removable storage
    - Tape drive
    - Solid state (e.g. thumb drive, flash, SD cards, USB)
    - External CD-RW and hard drive
    - Hot swappable devices and non-hot swappable devices
- ✓ **1.2 Explain motherboard components, types and features**
  - Form Factor
    - ATX / BTX
    - micro ATX
    - NLX
  - I/O interfaces
    - Sound
    - Video
    - USB 1.1 and 2.0
    - Serial
    - IEEE 1394 / Firewire
    - Parallel
    - NIC



- Modem
- PS/2
- Memory slots
  - RIMM
  - DIMM
  - SODIMM
  - SIMM
- Processor sockets
- Bus architecture
- Bus slots
  - PCI
  - AGP
  - PCIe
  - AMR
  - CNR
  - PCMCIA
- PATA
  - IDE
  - EIDE
- SATA, eSATA
- Contrast RAID (levels 0,1,5)
- Chipsets
- BIOS/ CMOS / Firmware
  - POST
  - CMOS battery
- Riser card / daughterboard

✓ 1.3 Classify power supplies types and characteristics

- AC adapter
- ATX proprietary
- Voltage, wattage, and capacity



- Voltage selector switch
- Pins (20,24)

✓ **1.4 Explain the purpose and characteristics of CPUs and their features**

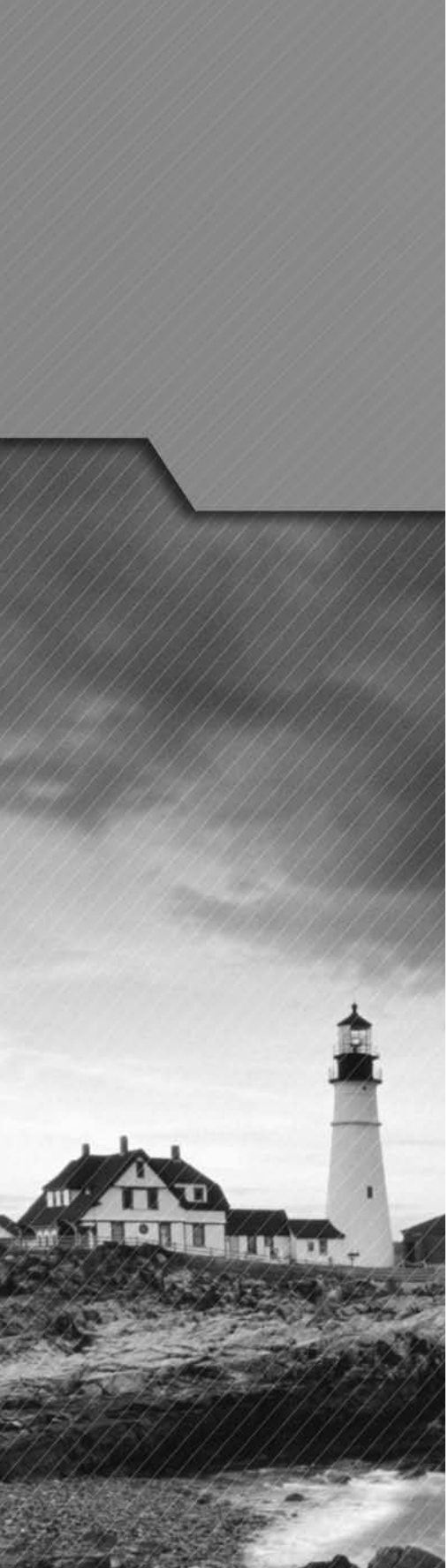
- Identify CPU types
  - AMD
  - Intel
- Hyperthreading
- Multi core
  - Dual core
  - Triple core
  - Quad core
- Onchip cache
  - L1
  - L2
- Speed (real vs. actual)
- 32 bit vs. 64bit

✓ **1.5 Explain cooling methods and devices**

- Heat sinks
- CPU and case fans
- Liquid cooling systems
- Thermal compound

✓ **1.6 Compare and contrast memory types, characteristics and their purpose**

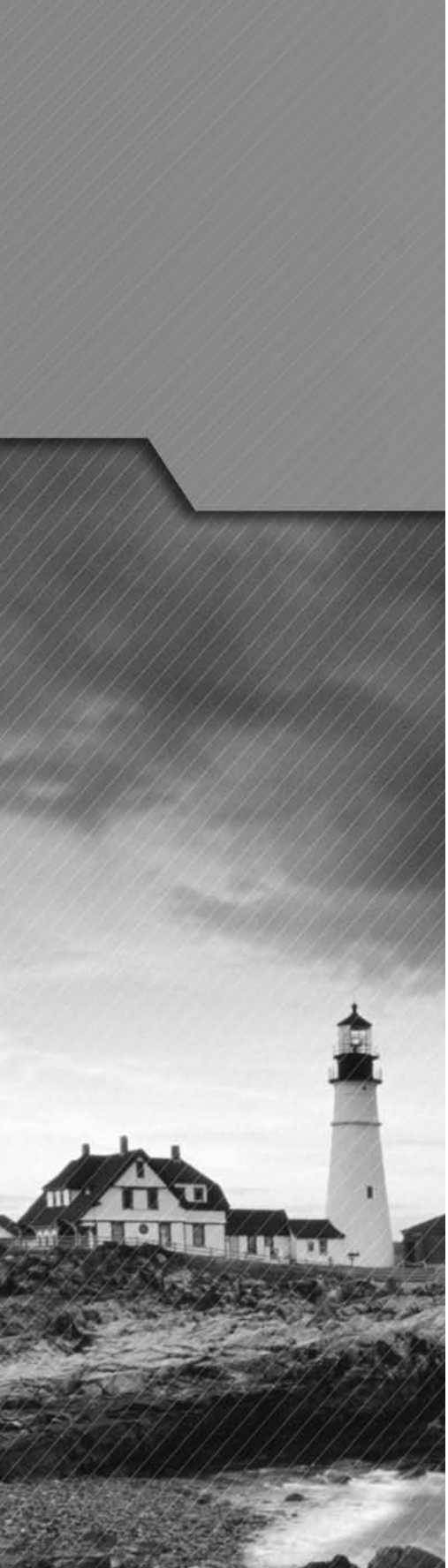
- Types
  - DRAM
  - SRAM
  - SDRAM
  - DDR / DDR2 / DDR3
  - RAMBUS



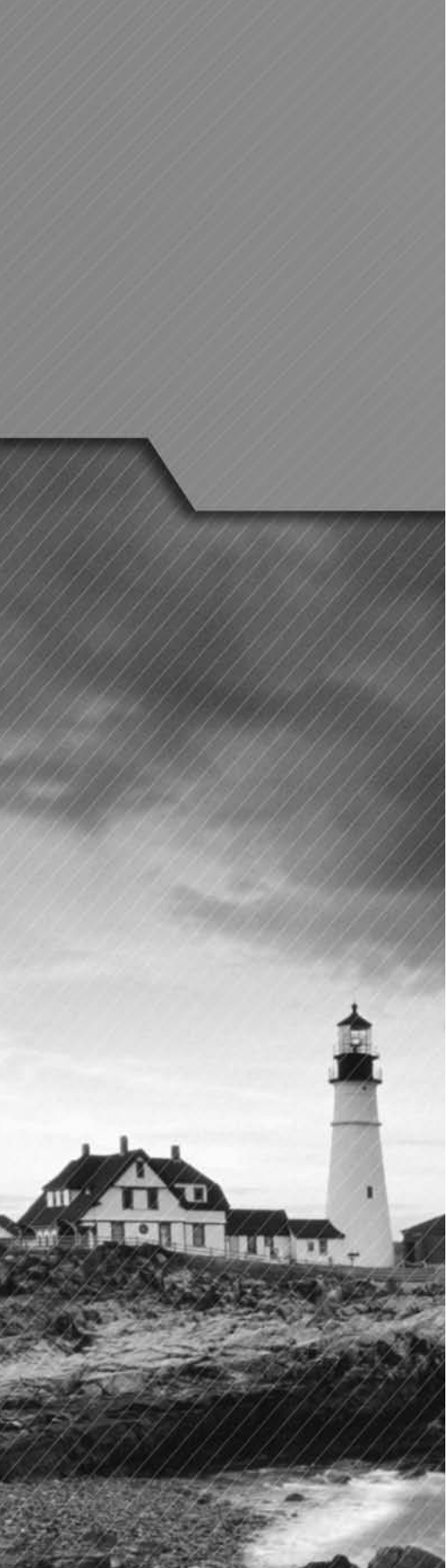
- Parity vs. non-parity
- ECC vs. non-ECC
- Single sided vs. double sided
- Single channel vs. dual channel
- Speed
  - PC100
  - PC133
  - PC2700
  - PC3200
  - DDR3-1600
  - DDR2-667

✓ **1.7 Distinguish between the different display devices and their characteristics**

- Projectors, CRT and LCD
- LCD technologies
  - Resolution (e.g. XGA, SXGA+, UXGA, WUXGA)
  - Contrast ratio
  - Native resolution
- Connector types
  - VGA
  - HDMi
  - S-Video
  - Component / RGB
  - DVI pin compatibility
- Settings
  - Refresh rate
  - Resolution
  - Multi-monitor
  - Degauss



- ✓ **1.8 Install and configure peripherals and input devices**
  - Mouse
  - Keyboard
  - Bar code reader
  - Multimedia (e.g. web and digital cameras, MIDI, microphones)
  - Biometric devices
  - Touch screen
  - KVM switch
- ✓ **1.9 Summarize the function and types of adapter cards**
  - Video
    - PCI
    - PCIe
    - AGP
  - Multimedia
    - Sound card
    - TV tuner cards
    - Capture cards
  - I/O
    - SCSI
    - Serial
    - USB
    - Parallel
  - Communications
    - NIC
    - Modem
- ✓ **1.10 Install, configure and optimize laptop components and features**
  - Expansion devices
    - PCMCIA cards
    - Express bus
    - Docking station



- Communications connections
  - Bluetooth
  - Infrared
  - Cellular WAN
  - Ethernet
  - Modem
- Power and electrical input devices
  - Auto-switching
  - Fixed input power supplies
  - Batteries
- Input devices
  - Stylus / digitizer
  - Function keys
  - Point devices (e.g. touch pad, point stick / track point)

✓ 1.11 Install and configure printers

- Differentiate between printer types
  - Laser
  - Inkjet
  - Thermal
  - Impact
- Local vs. network printers
- Printer drivers (compatibility)
- Consumables

This chapter covers a lot of material—in fact, it could easily be a book in and of itself. One of the things that CompTIA is notorious for is having overlap between domains and exams, and the A+ is no exception. This domain is weighted at 27 percent (the highest of any) of the Essentials exam, and a great deal of the material covered here also appears in other domains (not to mention in the Practical Application exam).

Because of this, you'll want to make sure you're comfortable with the information presented in this chapter before moving on to other chapters. As a doctor must be intimately acquainted with human anatomy, so a computer technician must understand the physical and functional structure of a personal computer.

Identify Principles of Personal Computer Storage

Any PC is a complex machine. It could be described as a melting pot of various technologies and products, manufactured by a host of companies in many different countries. This diversity is a great advantage because it gives the PC its versatility. However, these components don't always "melt" together into a unified whole without the help of a technician. The different products—whether they're hard disks, network cards, sound cards, or memory boards—must share one processor and one motherboard and therefore must be designed to work in harmony. For this reason, configuration of the computer components is especially emphasized on the A+ Essentials exam, and nearly one-third of the exam's question pool pertains to the objectives reviewed in this chapter.

Before sitting for the exam, you'll need to have a working knowledge of the components that make up a computer, and their function within the system as a whole. The exam will test your knowledge of the types of components and their functions. The objective of this chapter is to review and identify the main components and their functions.

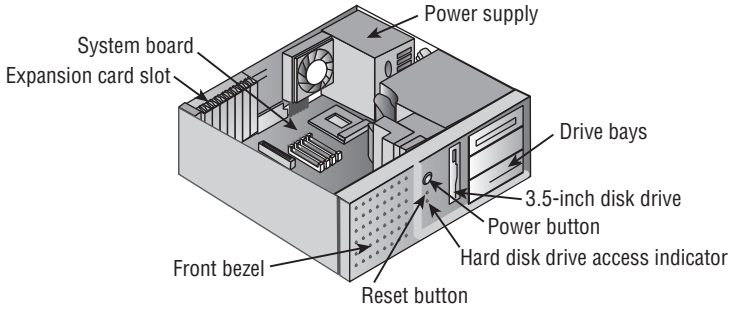
To pass the exam, you must be able to recognize these components and understand their relationship to one another.

Critical Information

This first objective is on storage devices, but to put it in perspective, you must blend together many diverse topic areas as they relate to PCs. Figure 1.1 shows a typical PC, its components, and their locations.

Throughout this chapter, you will need to know about key component categories: storage devices, motherboards, power supplies, processor/CPUs, memory, display devices, input devices, adapter cards, ports and cables, and cooling systems. The first of these is discussed in the section that follows.

FIGURE 1.1 Typical PC components



Storage Devices

Storage media hold the data being accessed, as well as the files the system needs to operate and data that needs to be saved. The various types of storage differ in terms of capacity, access time, and the physical type of media being used.

Floppy Drives

Though not something you are likely to find on a newer PC, a floppy disk drive (referred to by CompTIA as FDD) is a magnetic storage medium that uses a floppy disk made of thin plastic enclosed in a protective casing. The floppy disk itself (or *floppy*, as it's often called) enables the information to be transported from one computer to another easily. The downside of a floppy disk drive is its limited storage capacity. Floppy disks are limited to a maximum capacity of 2.88MB, but the most common type of floppy that you may find in use today holds only 1.44MB. Table 1.1 lists the various floppy disks and their capacity. For the most part, all of these are obsolete, but you must still know them for the exam.

TABLE 1.1 Floppy Disk Capacities

Floppy Drive Size	Common Designation	Number of Tracks	Capacity
3.5″	Double-sided, double-density	80	720KB
3.5″	Double-sided, high-density	80	1.44MB
3.5″	Double-sided, ultra-high-density	80	2.88MB

Prior to 3½″ disks, the most popular were 5¼″, but these went the way of the dodo bird.

Hard Disk Systems

Hard disks reside inside the computer (usually) and can hold more information than other forms of storage. The hard disk system contains three critical components:

- The controller
- The hard disk
- The host adapter

The controller controls the drive, the hard disk provides a physical medium to store the data, and the host adapter is the translator.

CompTIA favors the acronym HDD for *hard disk drive*.

Optical Drives

Optical drives work by using a laser rather than magnetism to change the characteristics of the storage medium. This is true for CD-ROM drives, DVD drives, and Blu-ray, all of which are discussed in the following sections.

CD-ROM DRIVES

CD-ROM stands for Compact Disc Read-Only Memory. The CD-ROM is used for long-term storage of data. CD-ROMs are read-only, meaning that once information is written to a CD, it can't be erased or changed. Access time for CD-ROMs is considerably slower than for a hard drive. CDs normally hold 650–700MB of data and use the ISO 9660 standard, which allows them to be used in multiple platforms.

DVD-ROM DRIVES

Because DVD-ROMs use slightly different technology than CD-ROMs, they can store up to 1.6GB of data. This makes them a better choice for distributing large software bundles. Many software packages today are so huge that they require multiple CDs to hold all the installation and reference files. A single DVD, in a double-sided, double-layered configuration, can hold as much as 17GB (as much as 26 regular CDs).

BLU-RAY DRIVES

Blu-ray recorders have been available since 2003, and have the ability to record more information than a standard DVD using similar optical technology. In recent years, Blu-ray has been more synonymous with recording television and movie files than data, but the Blu-ray specification (1.0) includes two data formats: BD-R for recoding PC data, and BD-RW for

rewritable media. Bonus View, the minimum required standard since 2007, is also known as Profile 1.1. BD-Live, which is basically 1.1 with an Internet connection, is called Profile 2.0.

In the official specification, as noted on the Blu-ray Disc Association website (`http://us.blu-raydisc.com/`), the "r" is lowercase. CompTIA favors the uppercase "R."

The current capacity a Blu-ray disc can hold is 50GB with 400GB on the horizon, and an aim for 1TB by 2013. As a final note, there was a long-running (but finally complete) battle between Blu-ray and HD DVD to be the format of the future, and Blu-ray won out.

Removable Storage

Removable storage is any that you can eject or quickly take with you. Within this broad category, the types that CompTIA wants you to know are tape drive, solid state (e.g., thumb drive, flash, SD cards, USB), external CD-RW and hard drive, and hot-swappable and non-hot-swappable devices.

TAPE DRIVES

Another form of storage device is the tape backup. Tape backup devices can be installed internally or externally and use a magnetic tape medium instead of disks for storage. They hold much more data than any other medium but are also much slower. They're primarily used for archival storage.

SOLID STATE DRIVES

Flash drives have been growing in popularity for years and replacing floppy disks due to their capacity and small size. Flash is ideally suited for use not only with computers, but also with many other things—digital cameras, MP3 players, and so on.

Although the CompTIA objective lists flash and SecureDigital (SD) cards separately, in reality SD cards are just one type of flash; there are many others. The maximum capacity of a standard SD card is 4GB, while there are two other standards that go beyond this: SDHC can go to 32GB, and SDXC to 2TB. Figure 1.2 shows a CompactFlash card (the larger of the two) and an SD card (the smaller of the two) along with an 8-in-1 card reader/writer. The reader shown connects to the USB port and then interacts with CompactFlash, CompactFlash II, Memory Stick, Memory Stick PRO, SmartMedia, xD-Picture Cards, SD, and MultiMediaCards.

You can find flash cards in any of these formats available in a variety of sizes (16MB, 128MB, 256MB, and so on). The size of the flash card does place some limitation on the maximum capacity of the media, but most cards on the market are well below that maximum.

Thumb drives are USB flash drives that have become extremely popular for transporting files. Figure 1.3 shows three thumb drives (also known as *keychain drives*) next to a pack of gum for size comparison.

As with other flash drives, you can find these in a number of different size capacities. Many models include a write-protect switch to keep you from accidentally overwriting files stored on the drive. All include an LED to show when they're connected to the USB port. Other names for thumb drives include travel drives, flash drives, jump drives, and a host of others.

FIGURE 1.2 CompactFlash and SD cards together with a reader

FIGURE 1.3 Three thumb drives shown with a pack of gum

EXTERNAL DRIVES

A number of vendors are now making external hard drives. These often connect to the computer through the USB port, but can also connect through the network (and be shared by other users) or other connections. While some are intended for expansion, many are marketed for the purpose of "mirroring" data on the internal drive(s) and often incorporate a push-button switch that starts a backup.

While not as common as they once were, Iomega's Zip and Jaz drives are detachable, external hard disks that are used to store a large volume (around 100MB for the Zip, 1GB and 2GB for the Jaz) of data on a single, thick floppy-sized disk. The drives connect to either a parallel port or a special interface card. The major use of Zip and Jaz drives is to transport large amounts of data from place to place. This used to be accomplished with several floppies.

HOT SWAPPABLES

The term "hot swappable" is used to refer to any media that can be changed without the system being brought down. In RAID arrays (discussed later in this chapter), if a failed hard drive can be replaced with a new hard drive without needing to bring the system down, then it is said to be hot swappable.

Floppy and Other Removable Disk Drive Problems

Most floppy drive problems result from bad media. Your first troubleshooting technique with floppy drive issues should be to try a new disk.

One of the most common problems that develops with floppy drives is misaligned read/write heads. The symptoms are fairly easy to recognize—you can read and write to a floppy on one machine but not on any others. This is normally caused by the mechanical arm in the floppy drive becoming misaligned. When the disk was formatted, it wasn't properly positioned on the drive, thus preventing other floppy drives from reading it.

Numerous commercial tools are available to realign floppy drive read/write heads. They use a floppy drive that has been preformatted to reposition the mechanical arm. In most cases, though, this fix is temporary—the arm will move out of place again fairly soon. Given the inexpensive nature of the problem, the best solution is to spend a few dollars and replace the drive or upgrade and get rid of it altogether.

Another problem you may encounter is a phantom directory listing. For example, suppose you display the contents of a floppy disk, and then you swap to another floppy disk but the listing stays the same. This is almost always a result of a faulty ribbon cable; a particular wire in the ribbon cable signals when a disk swap has taken place, and when that wire breaks, this error occurs.

CD-ROM/DVD/Blu-ray Issues

CD-ROM, DVD, and Blu-ray problems are normally media-related. Although compact disc technology is much more reliable than floppy disks, it's not perfect. Another factor to consider is the cleanliness of the disc. On many occasions, if a disc is unreadable cleaning it with an approved cleaner and a lint-free cleaning towel will fix the problem.

If the operating system doesn't see the drive, start troubleshooting by determining whether the drive is receiving power. If the tray will eject, you can assume there is power to it. Next, check BIOS Setup (for IDE drives) to make sure the drive has been detected. If not, check the master/slave jumper on the drive, and make sure the IDE adapter is set to Auto, CD-ROM, or ATAPI in BIOS Setup.

In order to play movies, a DVD drive must have MPEG-decoding capability. This is usually accomplished via an expansion board, but it may be built into the video card or sound card, or it may be a software decoder. If DVD data discs will play but movies won't, suspect a problem with the MPEG decoding.

If a CD-RW, DVD, or Blu-ray drive works normally as a regular CD-ROM drive but doesn't perform its special capability (doesn't read DVD discs, or doesn't write to blank CDs), perhaps software needs to be installed to work with it. For example, with CD-RW drives, unless you're using an operating system such as Windows XP that supports CD writing, you must install CD-writing software in order to write to CDs.

There are also a few quick fixes you can try: cleaning the disc and examining it for scratches are the easiest. If there are scratches, you can occasionally repair them using scratch repair that is available at most office supply sites. You should also clean the drive regularly using a commercial cleaning disc, available as well at most office supply stores.

Exam Essential

Know the various types of storage devices. Even though it is difficult to locate a PC today with a floppy drive, you must still be familiar with their capabilities and limitations as you prepare for this exam. You must also know the basics of hard drives, optical drives, and removable storage.

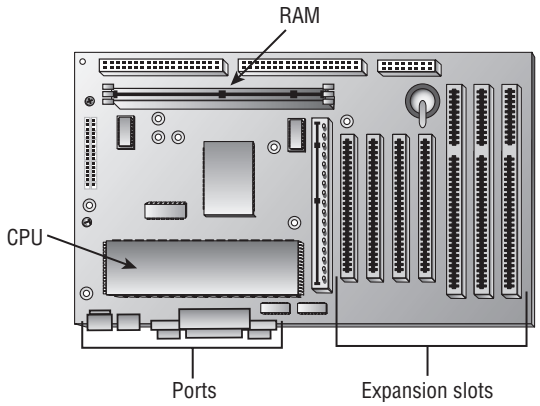
Identifying Motherboards

This objective is a complex one, for it requires you to not only know the various types of motherboards, but also be able to recognize their features. Therefore, this objective requires a great deal of memorization for you to pass the exam.

Critical Information

This second objective is focused on motherboards, and requires you to know that the motherboard is the backbone of a computer. The components of the motherboard provide basic services needed for the machine to operate and provide a platform for devices such as the processor, memory, disk drives, and expansion devices. For this objective, you should study the types of motherboards, their ports and memory, the types of CPU sockets, and the types of expansion slots. The spine of the computer is the *system board*, or *motherboard*. This component is made of green or brown fiberglass and is placed in the bottom or side of the case. It's the most important component in the computer because it connects all the other components of a PC together. Figure 1.4 shows a typical PC system board, as seen from above. On the system board you'll find the CPU, underlying circuitry, expansion slots, video components, RAM slots, and a variety of other chips.

FIGURE 1.4 A typical system board



Integrated Components

Some motherboards have some of the peripheral devices built in, such as video, sound, and/or networking. These are referred to as *integrated system boards*. Such boards are cost-effective because they don't require a separate video card, sound card, and so on. The built-in components can be disabled through BIOS Setup if they should ever malfunction or need to be replaced by newer models.

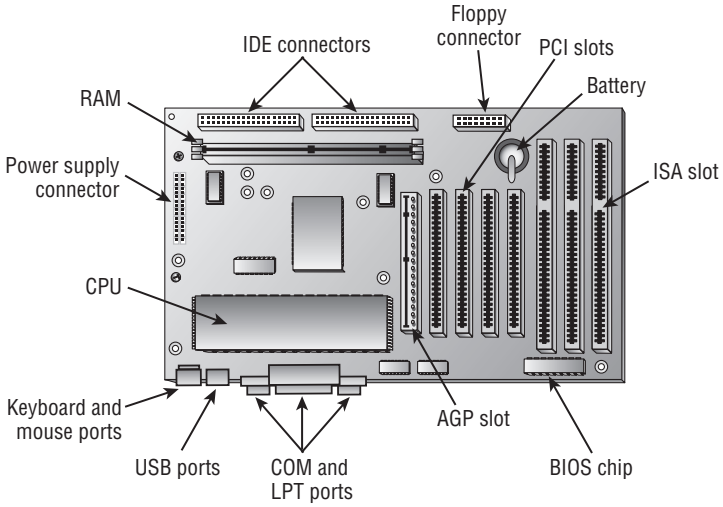
System Board Components

Motherboards include components that provide basic functionality to the computer. The following components are found on a typical motherboard:

- Expansion slots (AGP, PCI, etc.)
- Memory (RAM) slots
- CPU slot or socket
- Power connector
- Floppy and IDE drive connectors
- Keyboard and mouse connectors
- Peripheral port connectors (COM, LPT, USB)
- BIOS chip
- Battery

Figure 1.5 illustrates many of the components found on a typical motherboard. Many of these components are discussed elsewhere in this chapter as they relate to other objectives. Next let's look at those that are important to focus on.

FIGURE 1.5 Components on a motherboard



Memory Slots

Memory, or RAM, slots contain the memory chips. There are many and varied types of memory for PCs today. We'll further discuss memory later in this chapter. PCs use memory chips arranged on a small circuit board. These circuit boards are called *single inline memory modules* (*SIMMs*) or *dual inline memory modules* (*DIMMs*). DIMMs utilize memory chips on both sides of the circuit board, whereas SIMMs utilize memory chips on a single side. There is also a high-speed type of RAM called *Rambus dynamic RAM (RDRAM),* which comes on circuit boards called *RIMMs* (Rambus inline memory module).

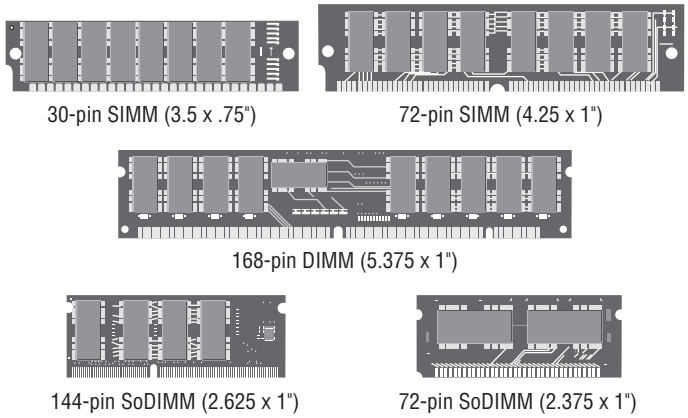
Along with chip placement, memory modules also differ in the number of conductors, or pins, that the particular module uses. The number of pins used directly affects the overall size of the memory slot. Slot sizes include 30-pin, 72-pin, 168-pin, and 184-pin. Laptop memory comes in smaller form factors known as *small outline DIMMs* (*SoDIMMs*). Figure 1.6 shows the form factors for the most popular memory chips. Notice that they basically look the same, but the memory module sizes are different.

Memory slots are easy to identify on a motherboard. They're usually white and placed very close together. The number of memory slots varies from motherboard to motherboard, but the appearance of the different slots is similar. Metal pins in the bottom make contact with the soldered tabs on each memory module. Small metal or plastic tabs on each side of the slot keep the memory module securely in its slot.

Central Processing Unit (CPU) and Processor Slots

The CPU slot permits the attachment of the CPU to the motherboard, allowing the CPU to use the other components of the system. There are many different types of processors, which means many types of CPU connectors.

FIGURE 1.6 Various memory module form factors



The CPU slot can take on several different forms. In the past, the CPU slot was a rectangular box called a PGA socket, with many small holes to accommodate the pins on the bottom of the chip. With the release of new and more-powerful chips, additional holes were added, changing the configuration of the slot and its designator or number. Figure 1.7 shows a typical PGA-type CPU socket.

With the release of the Pentium II, the architecture of the slot went from a rectangle to more of an expansion-slot style of interface called an SECC. This style of CPU slot includes Slot 1 and Slot 2 for Intel CPUs, and Slot A for Athlon (AMD) CPUs. This type of slot looks much like an expansion slot, but it's located in a different place on the motherboard than the other expansion slots.

To see which socket type is used for which processors, examine Table 1.2.

FIGURE 1.7 A PGA CPU socket

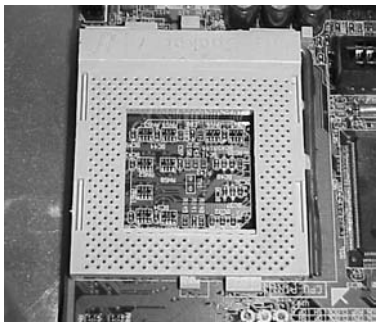


TABLE 1.2 Socket Types and the Processors They Support

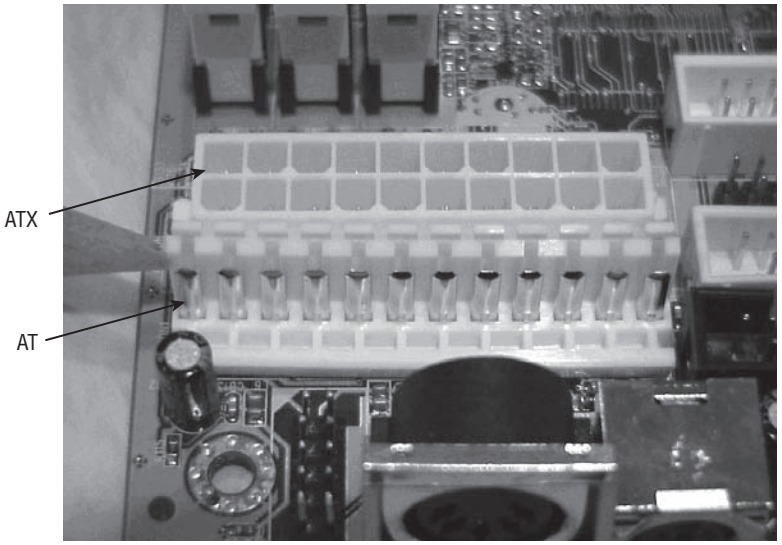
Connector Type	Processor
Socket 1	486 SX/SX2, 486 DX/DX2, 486 DX4 Overdrive
Socket 2	486 SX/SX2, 486 DX/DX2, 486 DX4 Overdrive, 486 Pentium Overdrive
Socket 3	486 SX/SX2, 486 DX/DX2, 486 DX4 486 Pentium Overdrive
Socket 4	Pentium 60/66, Pentium 60/66 Overdrive
Socket 5	Pentium 75-133, Pentium 75+ Overdrive
Socket 6	DX4, 486 Pentium Overdrive
Socket 7	Pentium 75-200, Pentium 75+ Overdrive
Socket 8	Pentium Pro
Socket 370	Pentium III
Socket 423	Pentium 4
Socket 478	Pentium 4 and Celeron 4
SECC (Type I), Slot 1	Pentium II
SECC2 (Type II), Slot 2	Pentium III
Slot A	Athlon
Socket 603	Xeon
Socket 754	AMD Athlon 64
Socket 939	Some versions of Athlon 64
Socket 940	Some versions of Athlon 64 and Opteron
Socket LGA775	Core 2 Duo/Quad
Socket AM2	Athlon 64 family (replacing earlier socket usage)
Socket F	Opteron

Power Connectors

A power connector allows the motherboard to be connected to the power supply. On an ATX, there is a single power connector consisting of a block of 20 holes (in two rows). On an AT, there is a block consisting of 12 pins sticking up; these pins are covered by two connectors with six holes each.

Figure 1.8 shows a very versatile motherboard that happens to have both kinds, so you can compare. The upper connector is for ATX, and the lower one is for AT.

FIGURE 1.8 Power connectors on a motherboard



On-Board Floppy and IDE Connectors

With the exception of diskless workstations, every PC made today uses some type of disk drive to store data and programs until they're needed. Disk drives need a connection to the motherboard in order for the computer to utilize the disk drive. These connections are known as *drive interfaces*. There are two primary types: *floppy drive interfaces* and *IDE interfaces*. Floppy drive interfaces allow floppy disk drives to be connected to the motherboard, and, similarly, IDE interfaces do the same for hard disks, CD drives, and other IDE-based drives. When you see them on the motherboard, these interfaces are said to be *on board*, as opposed to being on an expansion card, known as *off board*. The interfaces consist of circuitry and a port. A few motherboards also have SCSI interfaces that can be used for connecting drives.

Battery

Your PC has to keep certain settings when it's turned off and its power cord is unplugged. These settings include the date, time, hard drive configuration, and some basic settings in memory.

Your PC stores the settings in a special memory chip called the CMOS chip. To retain these settings, the CMOS chip requires power constantly. To prevent the CMOS chip from losing its charge, a small battery is located on the motherboard. The CMOS chip holds the BIOS.

System Board Form Factors

Form factor refers to the size and shape of a component. Most system boards today use the ATX form factor. Some of its key features are its orientation of the expansion slots parallel to the narrow edge of the board, a one-piece power connector from the power supply, the built-in I/O ports on the side, and the orientation of the CPU in such a position that the power-supply fan helps to cool it.

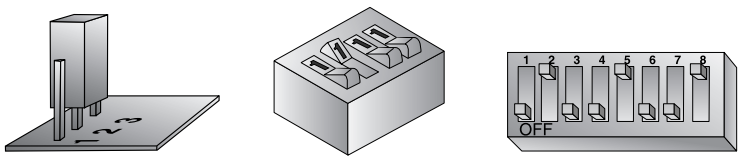
An older, alternative form factor for a system board is the baby AT style. This type uses a two-piece power supply connector, uses ribbon cables to connect ports to the board, and orients the expansion slots parallel to the wide edge of the board.

A case is generally designed to hold one or the other of these motherboard form factors, and a power supply is designed to work with one or the other; therefore, those three components must be chosen as a group.

Jumpers and DIP Switches

Jumpers and DIP switches are used to configure various hardware options on the motherboard. Processors use different voltages and multipliers to achieve their target voltage and frequency. You must set these parameters on the motherboard by changing the jumper or DIP switch settings. Figure 1.9 shows a jumper and two types of DIP switches. Individual jumpers are often labeled with the moniker *JP*x (where *x* is the number of the jumper). These are far less common than they used to be; many settings are now configured through the BIOS.

FIGURE 1.9 A jumper set and DIP switches



Jumper "Rocker-type" DIP switch "Slide-type" DIP switch

Cases

The *case* is the metal or plastic box in which the motherboard, power supply, disk drives, and other internal components are installed. A case is typically—but not always—purchased with a power supply already installed.

Choosing the right case for the motherboard is important. Recall from the preceding sections that motherboards come in two form factors: ATX and AT. Each requires a different style of case and a different type of power supply.

One case may also be distinguished from another in terms of its orientation. A desktop case lies with its widest side flat on the desk; a tower case stands up on end.

Finally, one case differs from another in terms of the number of drive bays it has. For example, within the broad category of *tower* cases are mini-towers (typically with two large and two small drive bays), mid-towers, and full towers (typically with four large and three small drive bays). However, there is little standardization of the number of drive bays that constitute a particular size; one manufacturer's full tower may have more or fewer bays than another's.

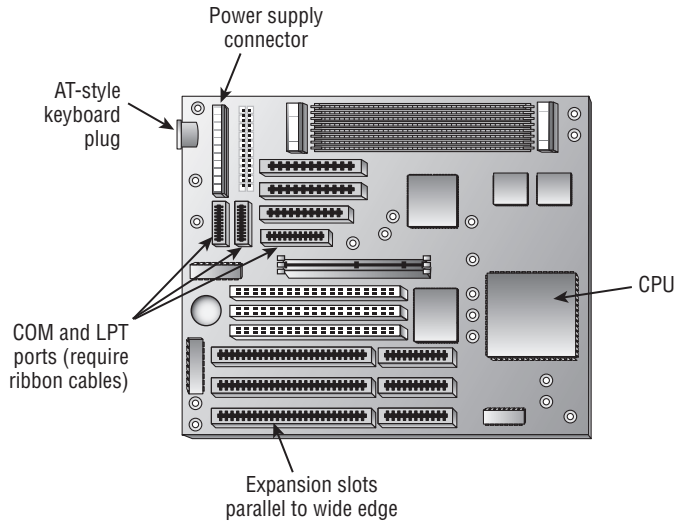
Although it isn't common, you may occasionally encounter a slim-line case, which is a desktop-orientation case that is shorter and thinner than a normal one—so short that normal expansion boards won't fit perpendicular to the motherboard. In such cases a *riser card* is installed, which sits perpendicular to the motherboard and contains expansion slots. The expansion cards can then be oriented parallel to the motherboard when installed.

Shapes

Form factor refers to the size and shape of a component. There are five popular motherboard form factors for desktop PCs:

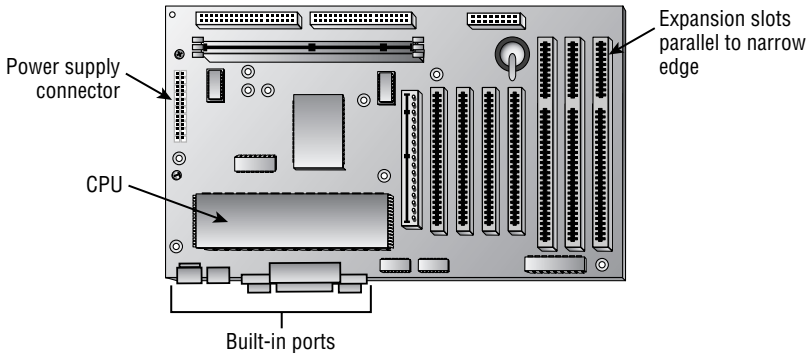
AT AT (Advanced Technology) is an older style of motherboard. A slightly more modern variant of it is the baby AT, which is similar but smaller. Its key features are a two-piece power-supply connector, ribbon cables that connect the I/O ports to the board, and an AT-style keyboard connector. The expansion slots are parallel to the wide edge of the board. See Figure 1.10.

FIGURE 1.10 An AT-style motherboard



ATX Most system boards today use the ATX (Advanced Technology Extended) form factor. It provides many design improvements over the AT, including I/O ports built directly into the side of the motherboard, the CPU positioned so that the power-supply fan helps cool it, and the ability for the PC to be turned on and off via software. It uses a PS/2-style connector for the keyboard. The expansion slots are parallel to the narrow edge of the board. See Figure 1.11.

FIGURE 1.11 An ATX-style motherboard



BTX The Balanced Technology Extended (BTX) motherboard was designed by Intel to deal with issues surrounding ATX (heat, power consumption, and so on). The BTX motherboard is larger than ATX, so there is more room for integrated components; there is also an optimized airflow path and a low-profile option.

Micro ATX The micro ATX (most commonly written as microATX) was released in 1997 for smaller—and typically cheaper—systems. It has become popular in recent years in low-cost PCs. The maximum size of a micro ATX motherboard is 244mm square, compared to 305mm×244mm for a standard ATX motherboard. The micro ATX is backward compatible with the ATX.

NLX An acronym for New, Low profile eXtended, this form factor is used in low-profile case types. It incorporates expansion slots that are placed on a *riser board* to accommodate the reduction in case size. However, this design adds another component to troubleshoot.

I/O Interfaces

While there are many types of I/O (input/output) interfaces available, the key ones to know for this portion of the exam are USB and IEEE 1394/FireWire, as the others are discussed in other places in this chapter and inclusion here would be repetitive.

USB USB is a newer expansion bus type that is used almost exclusively for external devices. All motherboards today have at least two USB ports. Some of the advantages of USB include hot-plugging and the capability for up to 127 USB devices to share a single set

of system resources. USB 1.1 runs at 12Mbps, and USB 2.0 runs at 480Mbps. Because USB is a serial interface, its width is 1 bit.

IEEE 1394/FireWire Some newer motherboards have a built-in IEEE 1394/FireWire port, although this port is more typically found on a PCI expansion board. It transfers data at 400Mbps and supports up to 63 chained devices on a single set of resources. It's hot-pluggable, like USB. Figure 1.12 shows the connections on a FireWire card.

FIGURE 1.12 FireWire connections

Troubleshooting I/O Ports and Cables

I/O ports include USB, FireWire, and legacy parallel and serial ports, all of which are used to connect external peripherals to the motherboard. When a port doesn't appear to be functioning, check the following:

- Cables are snugly connected.
- The port has not been disabled in BIOS Setup.
- The port has not been disabled in Device Manager in Windows.
- No pins are broken or bent on the male end of the port or of the cable being plugged into it.

If you suspect that the cable, rather than the port, may be the problem, swap out the cable with a known good one. If you don't have an extra cable, you can test the existing cable with a multimeter by setting it to ohms and checking the resistance between one end of the cable and the other.

Use a pin-out diagram, if available, to determine which pin matches up to which at the other end. There is often—but not always—an inverse relationship between the ends. In other words, at one end pin 1 is at the left, and at the other end it's at the right on the same row of pins.

Memory

To pass the A+ exam and be a productive computer technician, you must be familiar with memory. Not only will you be tested on this subject, but one of the most common upgrades performed on a PC is adding memory. Adding memory is a simple task, but before you can add memory you must have the correct type. When I say *memory*, we are most often referring to random access memory (RAM). However, there are other types of memory. We'll discuss them all in this section. Be familiar with the various types and their usage.

Physical Memory

Physically, memory or RAM is a collection of integrated circuits that store data and program information as patterns of 1s and 0s (on and off states) in the chip. Most memory chips require constant power (also called a constant *refresh*) to maintain those patterns of 1s and 0s. If power is lost, all those tiny switches revert back to the off position, effectively erasing the data from memory. Some memory types, however, don't require a refresh.

There are many types of RAM. Let's examine each type in detail.

SRAM

Static RAM (SRAM) stores whatever is placed in it until it's changed and it is used as cache memory (discussed later). Unlike dynamic RAM (DRAM), it doesn't require constant electrical refreshing. Another name for it is nonvolatile RAM (NVRAM). It's expensive, so it isn't typically used for the main memory in a system.

DRAM

Dynamic RAM (DRAM) is an improvement over SRAM. DRAM uses a different approach to storing the 1s and 0s. Instead of using transistors, DRAM stores information as charges in very small capacitors. If a charge exists in a capacitor, it's interpreted as a 1. The absence of a charge is interpreted as a 0.

Because DRAM uses capacitors instead of switches, it needs to use a constant refresh signal to keep the information in memory. DRAM requires more power than SRAM for refresh signals and, therefore, is mostly found in desktop computers.

DRAM technology allows several memory units, called *cells*, to be packed to a high density. Therefore, these chips can hold very large amounts of information. Most PCs today use DRAM of one type or another.

Let's take a brief look at some of the different types of DRAM:

Fast Page Mode (FPM) An older type of RAM (almost always 72-pin SIMM packaging) that isn't synchronized in speed with the motherboard. It's rated in nanoseconds of delay, with lower numbers being better (for example, 60ns). FPM is now obsolete.

Extended Data Out (EDO) Like FPM, an older type of RAM, usually in 72-pin SIMM form. It performs a bit better than normal FPM RAM because it needs to be refreshed less frequently. Like FPM, it's now obsolete.

Synchronous DRAM (SDRAM) Synchronized to the speed of the motherboard's system bus. Synchronizing the speed of the systems prevents the address bus from having to wait for the memory because of different clock speeds. A 100MHz clock signal produces 800Mbps, and such memory modules are referred to as *PC100*. *PC133*, which replaced PC100, used a 133MHz clock to produce 1067Mbps of throughput.

The relationship between clock speed and throughput is always roughly 1:8 and thus *PC2700* modules are designed specifically for a motherboard with a speed of 333MHz, and *PC3200* modules are designed for a motherboard with a speed of 400MHz.

SDRAM typically comes in the form of 168-pin DIMMs or 184-pin RIMMs.

Double Data Rate (DDR) SDRAM/DDR2 Essentially, clock-doubled SDRAM. The memory chip can perform reads and writes on both sides of any clock cycle (the up, or start, and the down, or ending), thus doubling the effective memory executions per second. So, if you're using DDR SDRAM with a 100MHz memory bus, the memory will execute reads and writes at 200MHz and transfer the data to the processor at 100MHz. The advantage of DDR over regular SDRAM is increased throughput and thus increased overall system speed.

The next generation of DDR SDRAM is DDR2 (Double Data Rate 2). This allows for two accesses per clock cycle and effectively doubles the speed of the memory. *DDR2-667* chips work with speeds of 667MHz and PC2-5300 modules, while DDR3-1600 chips support a 12800Mbps throughput.

RAMBUS A relatively new and extremely fast (up to 800MHz) technology that uses, for the most part, a new methodology in memory system design. RAMBUS (also known as direct Rambus) is a memory bus that transfers data at 800MHz, and is named after the company that designed it. RAMBUS memory models (often called Rambus inline memory modules [RIMMs]), like DDR SDRAM, can transfer data on both the rising and falling edges of a clock cycle. That feature, combined with the 16-bit bus for efficient transfer of data, results in the ultra-high memory transfer rate (800MHz) and the high bandwidth of up to 1.6GBps.

Memory Chip Package Types

Memory chips come in many different types of packages. Let's look at the ones most frequently encountered.

Dual Inline Package (DIP)

Dual inline package (DIP) memory is so named because the individual RAM chips use the DIP-style package for the memory module. Older computers, such as the IBM AT, arranged these small chips like rows of caskets in a small memory "graveyard." This type of memory has long been obsolete.

SIMMs

Single inline memory modules (SIMMs) were developed because DIPs took up too much real estate on the logic board. Someone got the idea to put several DIP chips on a small circuit board and then make that board easily removable.

Each of these RAM circuit boards is a *stick* of RAM. There are two sizes of SIMMs: 30-pin and 72-pin. The 30-pin are older, 8-bit sticks. The 72-pin are 32-bit sticks. Figure 1.13 shows one of each. SIMMs are called *single* because they're single-sided. When you count the number of pins (the metal tabs) along the bottom, there are 30 or 72 of them. In contrast, DIMMs (dual inline memory modules) are double-sided; for example, a 168-pin DIMM has 84 pins on each side.

DIMMs and RIMMs

DIMMs (dual inline memory modules) are double-sided memory chips used in modern systems (Pentium and higher). They typically have 168 pins and are 64 bits in width. Figure 1.14 shows a DIMM.

FIGURE 1.13 Single inline memory modules (SIMMs)

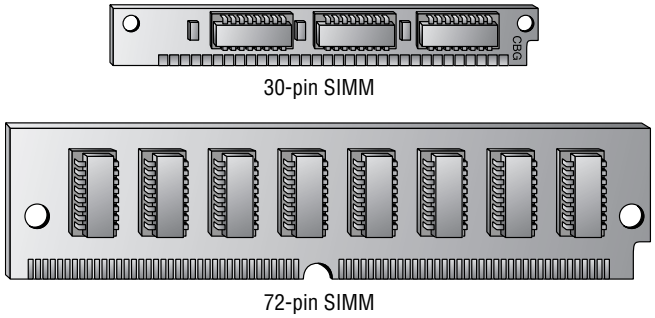
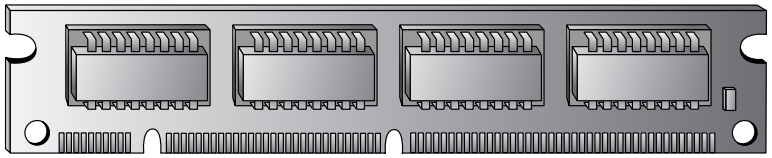


FIGURE 1.14 Dual inline memory module (DIMM)



A RIMM (Rambus inline memory module) is just like a DIMM, except it's a Rambus DRAM stick, has 184 pins, and is slightly longer in size.

SoDIMMs and MicroDIMMs

Portable computers (notebooks and subnotebooks) require smaller sticks of RAM because of their smaller size. Two types are small outline DIMM (SoDIMM), which can have 72, 144, or 200 pins, and MicroDIMM, which has either 172 or 214 pins.

Parity and Nonparity RAM

Some sticks of RAM have a parity bit on them for error detection. The parity bit works by adding up the number of 1s in a particular row of data in RAM (for example, 32-bit RAM has 32 individual binary digits). It then adds either 1 or 0 to that total to make it come out even. When retrieving the data from RAM, it re-adds the 1s again, and if the parity bit doesn't come out the same, it knows an error has occurred.

You can identify a parity SIMM by counting the number of chips on the stick. If there are nine, it's parity RAM. If there are eight, it's nonparity.

When do you choose parity RAM? Usually the motherboard requires either parity or nonparity; a few motherboards will accept either. Nowadays parity RAM is rarely needed because advances in RAM technology have created reliable RAM that seldom makes errors.

One type of parity RAM is error correction code (ECC). This is a now-obsolete type of parity RAM. Most RAM today is non-ECC.

RAM Banks and Bit Width

As explained earlier, 30-pin SIMMs are 8-bit, 72-pin SIMMs are 32-bit, and DIMMs are 64-bit. The motherboard has an address bus that carries data from the RAM to the CPU and chipset. It has a certain width. On Pentium and higher systems, it's 64-bit; on earlier systems, it's 32-bit (386 and 486) or less (286 and below). A bank of RAM is a single stick or a group of sticks where the collective bit width adds up to the width of the address bus.

For example, on a Pentium motherboard, a single bank consists of a single 64-bit DIMM or a pair of two 32-bit SIMMs. For a 486 motherboard, a single bank is a single 32-bit SIMM or four 8-bit SIMMs.

Video RAM

Video memory (also called *video RAM [VRAM]*) is used to store image data for processing by the video adapter. The more video memory an adapter has, the better the quality of image that it can display. Also, more VRAM allows the adapter to display a higher resolution of image.

Processor Sockets

The processor socket is the interface for the CPU. Table 1.2 listed the various CPU slots and sockets you may find in a motherboard and explained which CPUs will fit into them. The *central processing unit (CPU)* is a processor chip consisting of an array of millions of integrated circuits. Its purpose is to accept, perform calculations on, and eject numeric data. It's considered the "brain" of the computer because it's the part that performs the mathematical operations required for all other activity.

There are two form factors for CPU chips: pin grid array (PGA) and single edge contact cartridge (SECC). The PGA style is a flat square or rectangular ceramic chip with an array of pins in the bottom. The actual CPU is a tiny silicon wafer embedded inside that ceramic chip. The SECC style is a circuit board with the silicon wafer mounted on it. The circuit board is then surrounded by a plastic cartridge for protection; the circuit board sticks out of the cartridge along one edge. This edge fits into a slot in the motherboard.

All CPUs today require cooling because they generate heat as they operate. The cooling can be either active or passive. A *passive heat sink* is a block of heat-conductive material that sits close to the CPU and wicks away the heat into the air. An *active heat sink* contains a fan that pulls the hot air away from the CPU.

One way to determine which CPU your computer is using is to open the case and view the numbers stamped on the CPU. However, some passive heat sinks are glued to the CPU, so the numbers may not be visible without removing it. Another way to determine a computer's CPU is to save your work, exit any open programs, and restart the computer. Watch closely as the computer returns to its normal state. You should see a notation that tells you what chip you're using. The General tab of the System Properties in Windows may also report the CPU speed. Later versions of Windows will also report the CPU speed in the System Information tool.

External Speed (Clock Speed)

The *clock speed*, or *external speed*, is the speed at which the motherboard communicates with the CPU. It's determined by the motherboard, and its cadence is set by a quartz crystal (the system crystal) that generates regular electrical pulses.

Internal Speed

The *internal speed* is the maximum speed at which the CPU can perform its internal operations. This may be the same as the motherboard's speed (the external speed), but it's more likely to be a multiple of it. For example, a CPU may have an internal speed of 1.3GHz but an external speed of 133MHz. That means for every tick of the system crystal's clock, the CPU has 10 internal ticks of its own clock.

Cache Memory

A *cache* is an area of extremely fast memory used to store data that is waiting to enter or exit the CPU. The *Level 1 cache*, also known as the *L1* or *front-side cache*, holds data that is waiting to enter the CPU. On modern systems, the L1 cache is built into the CPU. The *Level 2 cache*, also known as the *L2* or *back-side cache*, holds data that is exiting the CPU and is waiting to return to RAM. On modern systems, the L2 cache is in the same packaging as the CPU but on a separate chip. On older systems, the L2 cache was on a separate circuit board installed in the motherboard, and was sometimes called *cache on a stick* (COAST).

On some CPUs, the L2 cache operates at the same speed as the CPU; on others, the cache speed is only half the CPU speed. Chips with full-speed L2 caches have better performance.

Some newer systems also have an *L3 cache*, which is external to the CPU. It sits between the CPU and RAM to optimize data transfer between them.

The Bus

The processor's ability to communicate with the rest of the system's components relies on the supporting circuitry. The system board's underlying circuitry is called the *bus*. The computer's bus moves information into and out of the processor and other devices. A bus allows all devices to communicate with one another. The motherboard has several buses. The *external data bus* carries information to and from the CPU and is the fastest bus on the system. The *address bus* typically runs at the same speed as the external data bus and carries data to and from RAM. The PCI, AGP, and ISA interfaces also have their own buses with their own widths and speeds. With newer architectures, the System or Front Side Bus (FSB) connects the CPU to northbridge (or memory) hub. The back side bus connects CPU with Level 2 (L2) cache, aka secondary or external cache and the memory bus connects northbridge (or memory) hub to RAM.

The CPU must be compatible with the motherboard in the following ways:

Physical Connectivity The CPU must be in the right kind of package to fit into the motherboard.

Speed The motherboard's chipset dictates its external data bus speed; the CPU must be capable of operating at that external speed.

Instruction Set The motherboard's chipset contains an instruction set for communicating with the CPU; the CPU must understand the commands in that set. For example, a motherboard designed for an AMD Athlon CPU can't accept an Intel Pentium CPU, because the instruction set is different.

Voltage The CPU requires that a certain voltage of power be supplied to it via the motherboard's interface. This can be anywhere from +5V for a very old CPU down to around +2.1V for a modern one. The wrong voltage can ruin the CPU. One reason a given motherboard can't support many different CPUs is that it must provide the correct voltage. To get around this issue, some motherboards have *voltage regulator modules (VRMs)* that are able to change the voltage based on the CPU.

There are several ways of differentiating one CPU from another. The following sections explain specifications according to type, speed, voltage, and cache memory.

CPU Speed

The CPU's speed is the frequency at which it executes instructions. This frequency is measured in millions of cycles per second, or megahertz (MHz); or billions of cycles per second, or gigahertz (GHz).

The CPU has an internal and an external speed. The external speed corresponds with the motherboard's speed, based on its system crystal. The system crystal pulses, generating a cadence at which operations occur on the motherboard. Each pulse is called a clock tick. The CPU's internal speed is usually a multiple of that, so that multiple operations occur internally per clock tick. A CPU's speed as described in its specifications is its internal speed.

CPU Manufacturers

The market leader in the manufacture of chips is Intel Corporation, with Advanced Micro Devices (AMD) gaining market share in the home PC market. Other competitors include Motorola and IBM.

INTEL PROCESSORS

The first commercially successful Intel CPU was the 8086, developed in the late 1970s. It was used in the IBM XT, one of the early home and business personal computers. Other early Intel CPUs included the 80286, 80386, and 80486. You may find it useful to learn about the specifications of these CPUs for your own knowledge, but they aren't covered on the current A+ exam.

PENTIUM

Intel introduced the Pentium processor in 1993. This processor has 3.1 million transistors using a 64-bit data path, a 32-bit address bus, and a 16KB on-chip cache, and it comes in speeds from 60MHz to 200MHz. With the release of the Pentium chips, *dual pipelining* was introduced (also called *superscalar architecture*), allowing the chip to process two operations at once.

The term *Pentium* refers to three separate CPUs: first-generation, second-generation, and MMX. First-generation Pentiums were 273-pin PGA CPUs (Socket 4) drawing +5V. They ran at 60MHz or 66MHz. The second-generation Pentiums were 296-pin models (Socket 5 or Socket 7) drawing +3.3V. They ran at between 75Mhz and 200MHz.

Third-generation (MMX) Pentiums, released in 1997, added multimedia extensions (MMX) to help the CPU work with graphic-intensive games. They used Socket 7 sockets, drew +2.8V, and ran at 166MHz to 233MHz. Due to the voltage difference between the Pentium MMX CPU and other Socket 7 CPUs, the MMX CPU required a motherboard that either was specifically for that CPU or had a VRM that could take the voltage down to that level.

PENTIUM PRO

The Pentium Pro, released in 1995, came between the second- and third-generation Pentiums. Physically, the Pentium Pro was a PGA-style, rectangular chip with 387 pins, using a Socket 8 socket drawing +3V. It was designed primarily for server usage, and was optimized for 32-bit operating systems. On a 16-bit OS like Windows 3.1, the Pentium Pro ran more slowly than a Pentium, so it failed to gain widespread consumer support.

The Pentium Pro included *quad pipelining*, which processed four operations at once. It was also the first CPU to include an on-chip L2 cache. Another advantage of the Pentium Pro was *dynamic processing*, which allowed it to run instructions out of order whenever it was waiting for something else to happen.

Throttling is a term CompTIA expects you to know for the exam. With throttling, you artificially reduce the amount of resources available. Although commonly used with bandwidth to prevent one user from absorbing all the resources on a network, it can also be applied to processors and applications. In many senses, throttling in this manner is the opposite of *overclocking*—where you attempt to get the processor to run at a speed higher than it's marked by using a faster bus speed or some other trick.

PENTIUM II

Intel next released the Pentium II. This chip's speeds ranged from 233MHz to over 400MHz. It was introduced in 1997 and was designed to be a multimedia chip with special on-chip multimedia instructions and high-speed cache memory. It has 32KB of L1 cache, dynamic execution, and MMX technology. The Pentium II uses an SECC to attach to the motherboard instead of the standard PGA package used with the earlier processor types.

When released, the Pentium II was designed for single-processor-only applications. Intel also released a separate processor, known as the Pentium II Xeon, to fill the need for multiprocessor applications such as servers. The Xeon's primary advantage is a huge L2 cache (up to 2MB) that runs at the same speed as the CPU. The Xeon uses a special size of SECC-style slot called Slot 2.

Different voltages have been used for the Pentium II over its lifespan, ranging from +2.8V to +2.0V. When you're using a Pentium II, it's important that the motherboard provide the correct voltage to it. This can be achieved with a VRM on the motherboard that detects the CPU's needs and adjusts the voltage provided.

CELERON

To offer a less-costly alternative and to keep its large market share, Intel released the Celeron. In some cases, the Celeron was priced as low as half the retail price of the Pentium II. Because it was developed after the Pentium II, it benefited from some advancements and in

certain aspects outperformed its more expensive counterpart. Intel has also named its low-budget Pentium III CPUs Celeron.

The Celeron CPU has come in several package types, including a 370-pin PGA socket (Socket 370) and an SECC variant called single-edge processor (SEP) that is similar to the circuit board inside an SECC cartridge but without the plastic outer shell.

PENTIUM III

The Pentium III was released in 1999 and uses the same SECC connector as its predecessor, the Pentium II. It included 70 new instructions and a processor serial number (PSN), a unique number electronically encoded into the processor. This number can be used to uniquely identify a system during Internet transactions.

The Pentium III has two styles: an SECC-style cartridge called SECC2, and a PGA-style chip with 370 pins. The Pentium III PGA chip has the CPU chip mounted on the top rather than the bottom of the ceramic square; it's called a flip chip (FC), or FC-PGA.

Like the Pentium II, the Pentium III has a multiprocessor Xeon version as well.

PENTIUM 4

The Pentium 4 was released in 2002. It runs on a motherboard with a fast system bus (between 400MHz and 800MHz) and provides some incremental improvements over the Pentium III. It's a PGA-style CPU.

One of the improvements the Pentium 4 offers is *hyperthreading* technology. This feature enables the computer to multitask more efficiently between CPU-demanding applications.

Dual-core processors, available from Intel as well as AMD, essentially combine two processors into one chip. Instead of adding two processors to a machine (making it a multiprocessor system), you have one chip splitting operations and essentially performing as if it's two processors in order to get better performance. The Centrino processor, for example, was released in 2003 and combines Wi-Fi capability with a multicore processor. A *multicore* architecture simply has multiple completely separate processor dies in the same package, whether its dual core, triple core, or quad core. The operating system and applications see multiple processors in the same way that they see multiple processors in separate sockets. Both dual-core and quad-core processors are common specific cases for the multicore technology. Most multicore processors from Intel come in even numbers, while AMD's Phenom series can contain odd numbers (such as the triple-core processor).

SUMMARY OF INTEL PROCESSORS

Table 1.3 provides a summary of the history of the Intel processors. Table 1.4 shows the physical characteristics of Pentium-class (and higher-class) processors.

Processors were also created for the server market, but you are not required to know of them for this exam. The Itanium chip is one of the most notable: it came out in 2001 and was geared toward high-end servers.

TABLE 1.3 The Intel Family of Processors

Chip	Year Added	Data Bus Width (in Bits)	Address Bus Width (in Bits)	Speed (in MHz)
8080	1974	8	8	2
8086	1978	16	20	5–10
8088	1979	8	20	4.77
80286	1982	16	24	8–12
386DX	1985	32	32	16–33
386SX	1988	32	24	16–20
486DX	1989	32	32	25–50
486SX	1991	32	32	16–33
487SX	1991	32	32	16–33
486DX2	1991	32	32	33–66
486DX4	1992	32	32	75–100
Pentium	1993	32	32	60–166
Pentium Pro	1995	64	32	150–200
Pentium II	1997	64	64	233–300
Pentium II Xeon	1998	64	64	400–600
Celeron	1999	64	64	400–600
Pentium III	1999	64	64	350–1000
Pentium III Xeon	1999	64	64	350–1000
Pentium 4	2002	64	64	1000–3000

A Pentium 4 Extreme Edition was released in 2003. Featuring a dual-core processor as its biggest modification over the Pentium 4, it was targeted for the gaming user.

TABLE 1.4 Physical Characteristics of Pentium-Class Processors

Processor	Speeds (MHz)	Socket	Pins	Voltage
Pentium-P5 (first generation)	60–66	4	273	+5V
Pentium-P54C (second generation)	75–200	5 or 7	296	+3.3V
Pentium-P55C (third generation)	166–233	7	321	+2.8V
Pentium Pro	150–200	8	387	+3V
Pentium II	233–450	SECC	N/A	+2.0V–+2.8V
Pentium III	450–1130	SECC2 or Socket 370	370	+2.0V
Pentium 4	1300–3000 (at this writing)	Socket 423 or Socket 478	423 or 478	+1.53V–+1.75V

INTEL CLONES AND OTHERS

Intel *clones* are processors that are based on the x86 architecture and are produced by other vendors; the most notable is AMD. AMD's competitor to the Pentium II is the K6. The original K6 ran at between 166MHz and 300MHz. The K6-2, at 266MHz to 475MHz, added 3DNow! Technology for improved multimedia. The K6-3, at 400MHz to 450MHz, adds a full-speed L2 cache. Because all the K6 chips are PGA, whereas Pentiums are SECC, you need a special motherboard for the K6 chips designed specifically for them.

AMD's competitor to the Pentium III is the Athlon. It uses an SECC-style slot called Slot A that is physically the same but not pin-compatible with Intel-style Slot 1 SECC. AMD also has a low-budget version called the Duron that has less L2 cache.

On-Motherboard Cache

On older motherboards, the L2 cache is on its own RAM-like stick made of very fast static random access memory (SRAM). It's known as *cache on a stick (COAST)*. On newer systems, the L2 cache is built into the CPU packaging.

Some newer systems also have an L3 cache, which is an external cache on the motherboard that sits between the CPU and RAM.

IDE and SCSI On-Motherboard Interfaces

Most motherboards include two *integrated drive electronics* (IDE) channels but don't include built-in *Small Computer System Interface* (SCSI). A consideration when choosing a motherboard for IDE is that it needs to support the desired level of UltraDMA to match the capabilities of the hard drive you want to use.

Chipsets

The *chipset* is the set of controller chips that monitors and directs the traffic on the motherboard between the buses. It usually consists of two or more chips. Motherboards use two basic chipset designs: the *north/south bridge chipset* and the *hub chipset*.

North/south bridge is the older of the two. The north bridge connects the system bus to the other relatively fast buses (AGP and PCI). The south bridge connects ISA, IDE, and USB. A third chip, SuperIO, connects the legacy parallel and serial ports.

The hub chipset includes a memory controller hub (equivalent to the north bridge), an I/O controller hub (equivalent to the south bridge), and a SuperIO chip.

Troubleshooting Dislodged Chips and Cards

The inside of a computer is a harsh environment. The temperature inside the case of some Pentium computers is well over 100° F! When you turn on your computer, it heats up. Turn it off, and it cools down. After several hundred such cycles, some components can't handle the stress and begin to move out of their sockets. This phenomenon is known as *chip creep,* and it can be really frustrating.

Chip creep can affect any socketed device, including ICs, RAM chips, and expansion cards. The solution to chip creep is simple: open the case, and reseat the devices. It's surprising how often this is the solution to phantom problems of all sorts.

Another important item worth mentioning is an unresponsive but freshly unboxed PC. With the introduction of the Type II and Type II-style processors, the number of dead boxes increased dramatically. In fact, at that time I was leading a 2,000-unit migration for a large financial institution. As with any large migration, time and labor were in short supply. The average dead PC ratio was about 1 out of every 20. When about 10 DOAs had stacked up, I stayed after work one night to assess the problem. After checking the power supply, RAM, and cables on these integrated systems, an examination of the chip provided me with the fix. These large, top-heavy processors can become dislodged during shipment. Shortly thereafter, manufacturers began using a heavier attachment point for the slot style of processor, which has helped tremendously.

CMOS

You can adjust a computer's base-level settings through a Basic Input/Output System (BIOS) Setup program, which you access by pressing a certain key at startup, such as F1 or Delete

(depending on the system). Another name for this setup program is CMOS Setup. The most common settings to adjust in CMOS include port settings (parallel, serial, USB), drive types, boot sequence, date and time, and virus/security protections.

Accessing CMOS Setup

Your PC keeps these settings in a special memory chip called the Complementary Metallic Oxide Semiconductor (CMOS) chip. The CMOS chip must have a constant source of power to keep its settings. To prevent the loss of data, motherboard manufacturers include a small battery to power the CMOS memory. On modern systems, this is a coin-style battery, about the same diameter of a dime and about ¼ inch thick.

You can press a certain key or group of keys to access the setup program during the power-on self-test (POST). This utility allows you to change the configuration through a group of menus. There are many different CMOS Setup programs, depending on the BIOS make and manufacturer, so it's impossible to provide specifics here; instead, we'll look at capabilities.

Load Setup Defaults

The purpose of this setting is to configure the PC back to the default settings set by the factory. If you make changes to your settings and the machine becomes disabled, in most cases selecting this menu item returns the machine to a usable state. You may then try different settings until you achieve your desired configuration. This is an important setting to know about before making any other changes.

Date and Time

One of the most basic things you can change in CMOS Setup is the system date and time. You can also change this from within the operating system.

CPU Settings

In most modern systems, the BIOS detects the CPU's type and speed automatically, so any CPU setting in CMOS Setup is likely to be read-only.

Memory Speed/Parity

Most systems today detect the RAM amount and speed automatically. Some motherboards can use different types of RAM, such as parity and nonparity, or different speeds, and the CMOS Setup program may provide the opportunity to change those settings. Increasingly, however, RAM is becoming a read-only part of CMOS Setup programs.

Power Management

The Power Management settings determine the way the PC will act after it has been idle for certain time periods. For example, you may have choices like Minimum, Maximum, and User Defined. The Minimum and Maximum settings control the HDD Off After, Doze Mode, Standby Mode, and Suspend Mode settings with predefined parameters. If you select User Defined, you must manually configure these settings to your personal preferences.

Ports and Peripherals

In CMOS Setup, you can enable or disable integrated components, such as built-in video cards, sound cards, or network cards. You may disable them in order to replace them with different models on expansion boards, for example.

You can also disable the on-board I/O ports for the motherboard, including parallel, serial, and USB. Depending on the utility, there may also be settings that enable or disable USB keyboard usage, Wake on LAN, or other special features.

In addition to enabling or disabling legacy parallel ports, you can assign an operational mode to the port. Table 1.5 lists the common modes for a parallel port. When you're troubleshooting parallel port problems, sometimes trying a different mode will help.

TABLE 1.5 Parallel Port Settings

Setting	Description	Use
EPP (enhanced parallel port)	Supports bidirectional communication and high transfer rates	Newer ink-jet and laser printers that can utilize bidirectional communication and scanners
ECP (enhanced capabilities port)	Supports bidirectional communication and high transfer rates	Newer ink-jet and laser printers that can utilize bidirectional communication, connectivity devices, and scanners
SPP (standard parallel port)	Supports bidirectional communication	Older ink-jet and laser printers and slower scanners

Passwords

In most CMOS Setup programs, you can set a supervisor password. Doing so requires a password to be entered in order to use the CMOS Setup program, effectively locking out users from making changes to it. You may also be able to set a user password, which restricts the PC from booting unless the password is entered.

To reset a forgotten password, you can remove the CMOS battery to reset everything. There also may be a Reset jumper on the motherboard.

Virus Protection

Some CMOS Setup programs have a rudimentary virus-protection mechanism that prevents applications from writing to the boot sector of a disk without your permission. If this setting is turned on and you install a new operating system, a confirmation box may appear at some point, warning you that the operating system's Setup program is trying to write to the boot sector. Let it.

HDD Auto Detection

Some CMOS Setup programs have a feature that polls the IDE channels and provides information about the IDE devices attached to them. You can use this feature to gather the settings for a hard disk. However, most hard disks these days are fully Plug and Play, so they automatically report themselves to the CMOS Setup.

Drive Configuration

You can specify how many floppy drives are installed and what types they are. Floppy drives aren't automatically detected. The settings needed for a floppy drive are size (3½-inch or 5¼-inch) and density (double-density or high-density). You can also set each floppy drive to be enabled or disabled from being bootable. Almost all floppy drives today are high-density 3½-inch.

Hard drives, on the other hand, can be autodetected by most systems if the IDE setting is set to Auto. The settings detected may include the drive's capacity; its geometry (cylinders, heads, and sectors); and its preferred PIO (Programmed Input/Output), direct memory access (DMA), or UltraDMA operating mode. You can also configure a hard drive by entering its CHS values manually, but doing so is almost never necessary anymore.

CHS stands for *cylinders, heads, and sectors*. This is also called the *drive geometry,* because together these three numbers determine how much data the disk can hold. Most CMOS Setup programs are able to automatically detect the CHS values.

Boot Sequence

Each system has a default boot order, which is the order in which it checks the drives for a valid operating system to boot. Usually, this order is set for floppy first, then hard disk, and finally CD-ROM, but these components can be placed in any boot order. For example, you might set CD-ROM first to boot from a Windows XP Setup disk on a system that already contained an operating system.

Exiting CMOS Setup

The CMOS Setup program includes an Exit command, with options that include Save Changes and Discard Changes. In most programs, Esc is a shortcut for exiting and discarding changes, and F10 is a common shortcut for exiting and saving changes.

BIOS Issues

Computer BIOSs don't go bad; they just become out-of-date. This isn't necessarily a critical issue—they will continue to support the hardware that came with the box. It *does*, however, become an issue when the BIOS doesn't support some component that you would like to install—a larger hard drive, for instance.

Most of today's BIOSs are written to an EEPROM and can be updated through the use of software. Each manufacturer has its own method for accomplishing this. Check out the documentation for complete details.

If you make a mistake in the upgrade process, the computer can become unbootable. If this happens, your only option may be to ship the box to a manufacturer-approved service center. Be careful!

Post Routines

Every computer has a diagnostic program built into its BIOS called the *power-on self-test* (*POST*). When you turn on the computer, it executes this set of diagnostics. Many steps are involved the POST, but they happen very quickly, they're invisible to the user, and they vary among BIOS versions. The steps include checking the CPU, checking the RAM, checking for the presence of a video card, and so on. The main reason to be aware of the POST's existence is that if it encounters a problem, the boot process stops. Being able to determine at what point the problem occurred can help you troubleshoot.

One way to determine the source of a problem is to listen for a *beep code*. This is a series of beeps from the computer's speaker. The number, duration, and pattern of the beeps can sometimes tell you what component is causing the problem. However, the beeps differ depending on the BIOS manufacturer and version, so you must look up the beep code in a chart for your particular BIOS. Different BIOS manufacturers use the beeping differently. AMI BIOS, for example, relies on a raw number of beeps, and uses patterns of short and long beeps.

Another way to determine a problem during the POST routine is to use a *POST card*. This is a circuit board that fits into an ISA or PCI expansion slot in the motherboard and reports numeric codes as the boot process progresses. Each of those codes corresponds to a particular component being checked. If the POST card stops at a certain number, you can look up that number in the manual that came with the card to determine the problem.

BIOS Central is a website containing charts detailing the beep codes and POST error codes for many different BIOS manufacturers: `www.iterasi.net/openviewer.aspx?sqrlitid=px8b_zkg9eiiv-n5ilfowq`.

Bus Architecture and Slots

A *bus* is a set of signal pathways that allows information and signals to travel between components inside or outside a computer. A motherboard has several buses, each with its own speed and width.

The *external data bus*, also called the *system bus*, connects the CPU to the chipset. On modern systems, it's 64-bit. The *address bus* connects the RAM to the CPU. On modern systems, it's 64-bit.

The *expansion bus* connects the I/O ports and expansion slots to the chipset. There are usually several different expansion buses on a motherboard. Expansion buses can be broken into two broad categories: internal and external. Internal expansion buses include Industry Standard Architecture (ISA), Peripheral Component Interconnect (PCI), and

Accelerated Graphics Port (AGP); they're for circuit boards. External expansion buses include serial, parallel, Universal Serial Bus (USB), FireWire, and infrared. The following sections explain some of the most common buses.

There are many obsolete bus types, including Video Electronics Standards Association Local Bus (VESA local bus, or VL-Bus), Microchannel Architecture (MCA), and enhanced ISA (EISA). These were not on the last iteration of the A+ test and should not appear on this one either.

ISA (Industry Standard Architecture)

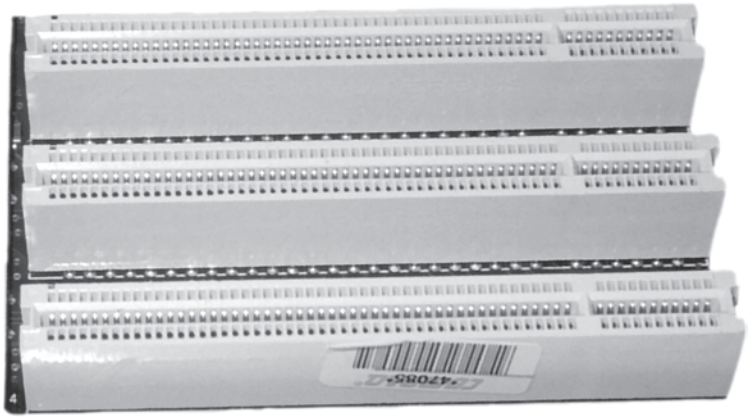
This is a 16-bit bus (originally 8-bit on the oldest computers) that operates at 8MHz. Its slots are usually black. New motherboards will not have this type of slot, because the ISA bus is old technology and has been phased out.

Besides the slow speed and narrow width, another drawback of the ISA bus is that each ISA device requires separate system resources, including separate interrupt requests (IRQs). In a heavily loaded system, this can cause an IRQ shortage. (PCI slots, in contrast, can share some resources.)

PCI (Peripheral Component Interconnect)

The PCI bus is a fast (33MHz), wide (32-bit or 64-bit) expansion bus that is the modern standard in motherboards today for general-purpose expansion devices. Its slots are typically white. PCI devices can share IRQs and other system resources with one another in some cases. All modern motherboards have at least three PCI slots. Figure 1.15 shows some PCI slots.

FIGURE 1.15 PCI bus connectors

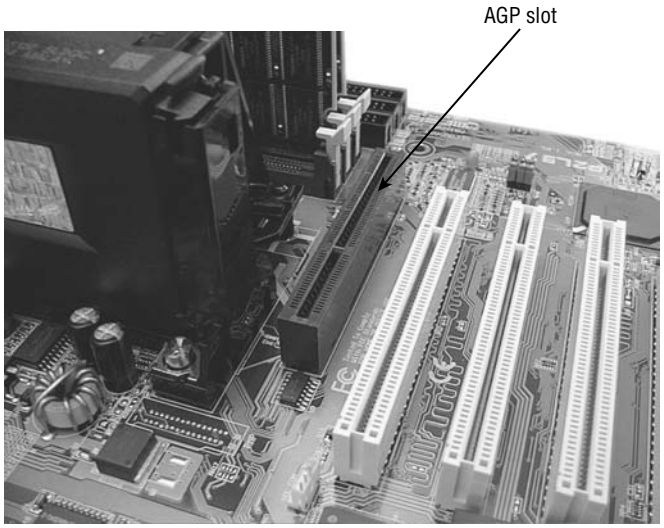


AGP (Accelerated Graphics Port)

As systems got faster, PC game players wanted games that had better graphics, more realism, and more speed. However, as the computers got faster, the video technology couldn't seem to keep up, even with the PCI bus. The AGP bus was developed to meet this need.

The AGP slot is usually brown, and there is only one. It's a 32-bit or 64-bit bus, and it runs very fast (66MHz or faster). It's used exclusively for the video card. If you use a PCI video card, the AGP slot remains empty. See Figure 1.16.

FIGURE 1.16 An AGP slot on a motherboard



PCIE (PCI Express)

PCI Express (PCIE , PCI-E, or PCIe) uses a network of serial interconnects that operate at high speed. It's based on the PCI system; most existing systems can be easily converted to PCIE. Intended as a replacement for AGP and PCI, PCIE has the capability of being faster than AGP, while maintaining the flexibility of PCI. There are currently six different speed levels and they correspond to AGP speeds: 1X, 2X, 4X, 8X, 16X, and 32X.

AMR and CNR

Audio Modem Riser (AMR) was originally created to speed manufacturing (and certification) by separating the analog circuitry (modem and analog audio) onto its own card. Over time, this has been replaced by *Communications Network Riser (CNR)*, which includes the capabilities of AMR and allows the motherboard chipset to be designed with additional integrated features.

PCMCIA (Personal Computer Memory Card International Association)

The PCMCIA standard defines the PC Card (formerly known as the PCMCIA Card), an interface designed for laptop computers. This standard is discussed in more detail later in this chapter.

Legacy Parallel and Serial

These buses are called *legacy* because they're old technology and are being phased out. The legacy serial port, also called an RS-232 port, is a 9-pin or 25-pin male connector. It sends data one bit at a time and is usually limited to about 115Kbps in speed.

The legacy parallel port transfers data 8 bits at a time. It's a 25-pin female connector. A system typically has only one parallel port, but because many printers are now coming with USB interfaces, this is no longer the inconvenience that it used to be.

PATA/IDE/EIDE Devices

IDE drives are the most common type of hard drive found in computers. But IDE is much more than a hard drive interface; it's also a popular interface for many other drive types, including CD-ROM, DVD, and Zip. IDE drives are the most prevalent in the industry today. IDE drives are easy to install and configure, and they provide acceptable performance for most applications. Their ease of use relates to their most identifiable feature—the controller is located on the drive itself.

IDE Technologies

The design of the IDE is simple: put the controller right on the drive, and use a relatively short ribbon cable to connect the drive/controller to the IDE interface. This offers the benefits of decreasing signal loss (thus increasing reliability) and making the drive easier to install. The IDE interface can be an expansion board, or it can be built into the motherboard, as is the case on almost all systems today.

IDE generically refers to any drive that has a built-in controller. The IDE we know today is more properly called AT IDE; two previous types of IDE (MCA IDE and XT IDE) are obsolete and incompatible with it.

There have been many revisions of the IDE standard over the years, and each one is designated with a certain AT attachment (ATA) number—ATA-1 through ATA-8. Drives that support ATA-2 and higher are generically referred to as enhanced IDE (EIDE).

With ATA-3, a technology called ATA Packet Interface (ATAPI) was introduced to help deal with IDE devices other than hard disks. ATAPI enables the BIOS to recognize an IDE CD-ROM drive, for example, or a tape backup or Zip drive.

Starting with ATA-4, a new technology was introduced called UltraDMA, supporting transfer modes of up to 33Mbps.

ATA-5 supports UltraDMA/66, with transfer modes of up to 66Mbps. To achieve this high rate, the drive must have a special 80-wire ribbon cable, and the motherboard or IDE controller card must support ATA-5.

ATA-6 supports UltraDMA/100, with transfer modes of up to 100Mbps.

If an ATA-5 or ATA-6 drive is used with a normal 40-wire cable or is used on a system that doesn't support the higher modes, it reverts to the ATA-4 performance level.

ATA-7 supports UltraDMA/133, with transfer modes of up to 150Mbps and serial ATA (discussed later).

ATA-8 made only minor revisions to ATA-7 and also supports UltraDMA/133, with transfer modes of up to 150Mbps and serial ATA.

IDE Pros and Cons

The primary benefit of IDE is that it's nearly universally supported. Almost every motherboard has IDE connectors. In addition, IDE devices are typically the cheapest and most readily available type.

A typical motherboard has two IDE connectors, and each connector can support up to two drives on the same cable. That means you're limited to four IDE devices per system unless you add an expansion board containing another IDE interface. In contrast, with SCSI you can have up to seven drives per interface (or even more on some types of SCSI).

Performance also may suffer when IDE devices share an interface. When you're burning CDs, for example, if the reading and writing CD drives are both on the same cable, errors may occur. SCSI drives are much more efficient with this type of transfer.

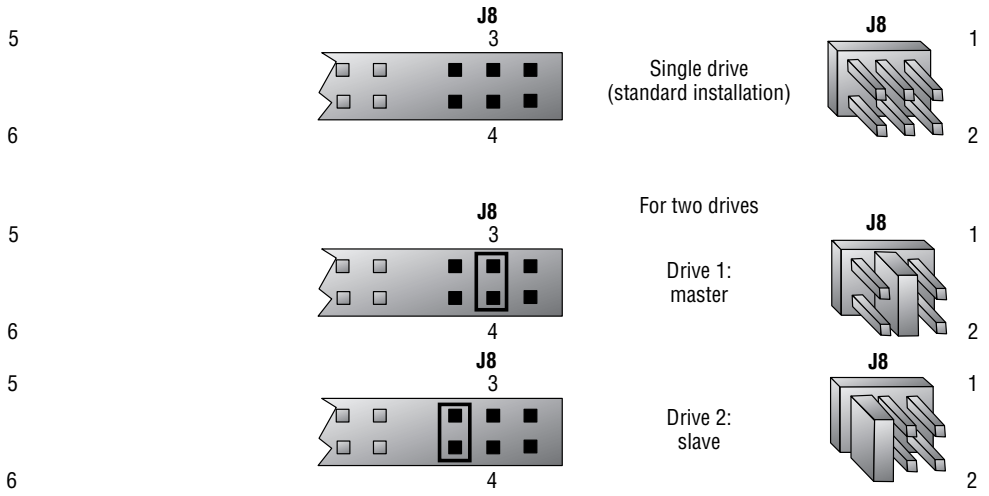
Installation and Configuration

To install an IDE drive, do the following:

1. Set the master/slave jumper on the drive.
2. Install the drive in the drive bay.
3. Connect the power-supply cable.
4. Connect the ribbon cable to the drive and to the motherboard or IDE expansion board.
5. Configure the drive in BIOS Setup if it isn't automatically detected.
6. Partition and format the drive using the operating system.

Each IDE interface can have only one *master* drive on it. If there are two drives on a single cable, one of them must be the *slave* drive. This setting is accomplished via a jumper on the drive. Some drives have a separate setting for Single (that is, master with no slave) and Master (that is, master with a slave); others use the Master setting generically to refer to either case. Figure 1.17 shows a typical master/slave jumper scenario, but different drives may have different jumper positions to represent each state. Today, the need for jumper settings has decreased as many drives can autodetect the master/slave relationship.

FIGURE 1.17 Master/slave jumpers



Most BIOS Setup programs today support Plug and Play, so they detect the new drive automatically at startup. If this doesn't work, the drive may not be installed correctly, the jumper settings may be wrong, or the BIOS Setup may have the IDE interface set to None rather than Auto. Enter BIOS Setup, and find out. Setting the IDE interface to Auto and then allowing the BIOS to detect the drive is usually all that is required.

In BIOS Setup for the drive, you might have the option of selecting a DMA or programmed input/output (PIO) setting for the drive. Both are methods for improving drive performance by allowing the drive to write directly to RAM, bypassing the CPU when possible. For modern drives that support UltraDMA, neither of these settings is necessary or desirable.

Now that your drive is installed, you can proceed to partition and format it for the operating system you've chosen. Then, finally, you can install your operating system of choice.

For a Windows Vista, XP, or 2000 system, allow the Windows Setup program to partition and format the drive, or use the Disk Management utility in Windows to perform those tasks. To access Disk Management, from the Control Panel, choose Administrative Tools and then choose Computer Management.

Hard Disk System Problems

Hard disk system problems usually stem from one of three causes:

- The adapter (that is, the IDE interface) is bad.
- The disk is bad.
- The adapter and disk are connected incorrectly.

The first and last causes are easy to identify, because in either case the symptom will be obvious: the drive won't work. You won't be able to get the computer to communicate with the disk drive.

However, if the problem is a bad disk drive, the symptoms aren't as obvious. As long as the BIOS POST routines can communicate with the disk drive, they're usually satisfied. But the POST routines may not uncover problems related to storing information. Even with healthy POST results, you may find that you're permitted to save information to a bad disk, but when you try to read it back, you get errors. Or the computer may not boot as quickly as it used to, because the disk drive can't read the boot information successfully every time.

In some cases, reformatting the drive can solve the problems described in the preceding paragraph. In other cases, reformatting brings the drive back to life only for a short while. The bottom line is that read and write problems usually indicate that the drive is malfunctioning and should be replaced soon.

Never low-level-format IDE drives! They're low-level-formatted from the factory, and you may cause problems by using low-level utilities on these types of drives.

SATA and eSATA

Serial ATA (SATA) came out as a standard recently and was first adopted in desktops and then laptops. Whereas ATA had always been an interface that sends 16 bits at a time, SATA sends only one bit at a time. The benefit is that the cable used can be much smaller, and faster cycling can actually increase performance.

External SATA (eSATA) is a variant of SATA that was standardized in 2004 for external devices. As such, it competes with FireWire and USB, but differs from them in that it requires its own power connector. The advantage it has over the other technologies is speed—it is approximately three times faster at data transfer than either FireWire or USB 2.0.

RAID

RAID stands for *Redundant Array of Independent Disks*. It's a way of combining the storage power of more than one hard disk for a special purpose such as increased performance or fault tolerance. RAID is more commonly done with SCSI drives, but it can be done with IDE drives.

There are several types of RAID, of which you need to know the following three for the exam:

RAID 0 Also known as *disk striping*. This is technically not RAID, because it doesn't provide fault tolerance. Data is written across multiple drives, so one drive can be reading or writing while the next drive's read-write head is moving. This makes for faster data access. However, if any one of the drives fails, all content is lost.

RAID 1 Also known as *disk mirroring*. This is a method of producing fault tolerance by writing all data simultaneously to two separate drives. If one drive fails, the other contains all the data and can be switched to. However, disk mirroring doesn't help access speed, and the cost is double that of a single drive.

RAID 5 Combines the benefits of both RAID 0 and RAID 1, and is known as Striping with Parity. It uses a parity block distributed across all the drives in the array, in addition to striping the data across them. That way, if one drive fails, the parity information can be used to recover what was on the failed drive. A minimum of three drives is required.

Firmware

Any software that is built into a hardware device is called *firmware*. Firmware is typically in flash ROM and can be updated as newer versions become available. An example of firmware is the software in a laser printer that controls it and allows you to interact with it at the console (usually through a limited menu of options).

Daughterboards

Any boards added to the motherboard to expand its capabilities are known as *daughterboards* ("daughters" of the "mother"). A common use is to insert one daughterboard (also called *daughter boards*) into the motherboard and allow expansion cards to then be inserted into it sideways, thus saving space.

Motherboard and CPU Problems

Most motherboard and CPU problems manifest themselves by the system appearing completely dead. However, "completely dead" can be a symptom of a wide variety of problems, not only with the CPU or motherboard but also with the RAM or the power supply. So, a POST card (described in the preceding section) may be helpful in narrowing down the exact component that is faulty.

When a motherboard fails, it's usually because it has been damaged. Most technicians can't repair motherboard damage; the motherboard must be replaced. Motherboards can become damaged due to physical trauma, exposure to electrostatic discharge (ESD), or short-circuiting. To minimize the risk of these damages, observe the following rules:

- Handle a motherboard as little as possible, and keep it in an antistatic bag whenever it's removed from the PC case.
- Keep all liquids well away from the motherboard, because water can cause a short circuit.
- Wear an antistatic wrist strap when handling or touching a motherboard.
- When installing a motherboard in a case, make sure you use brass stand-offs with paper washers to prevent any stray solder around the screw holes from causing a short circuit with the metal of the screw.

A CPU may fail because of physical trauma or short-circuiting, but the most common cause for a CPU not to work is failure to install it properly. With a PGA-style CPU, ensure that the CPU is oriented correctly in the socket. With an SECC-style CPU, make sure the CPU is completely inserted into its slot.

Exam Essentials

Know what the BIOS does. This is a ROM chip on the motherboard. It contains the BIOS software that tells the processor how to interact with the hardware in the computer. The BIOS chip tells the motherboard how to start up, check itself and its components, and pass off control to the operating system.

Know the different types of memory. DRAM is dynamic random access memory. SRAM is static random access memory. ROM stands for read-only memory, and it's normally used to store the computer's BIOS. CMOS is a special kind of memory that holds the BIOS configuration settings.

Understand the differences between PCI, PCIe, and AGP. Know the bus widths and speeds, and be able to select the best bus type for a given device.

Know what factors go into making memory compatible with a PC. These factors can include physical size, capacity, technology, speed, and compatibility with existing RAM in the system.

Understand the processor's job. The processor is the brain of the PC. Most actions performed by the PC require use of the processor to accomplish their task.

Understand the differences between the classes of Pentium chips. The Intel Pentium has gone through several changes since its release. You'll need to understand the differences between the various classes in terms of their physical packaging, speeds, voltages, and caches.

Know the differences between RAM types. Make sure you can differentiate between all the acronyms, such as SRAM, DRAM, SDRAM, DDR/DDR2/DDR3 and RAMBUS.

Understand the different RAM packaging. Be able to differentiate between SIMMs and DIMMs, including the number of pins each has and their bit widths.

Know the purpose of parity in RAM. Understand how a parity bit is used for error correction.

Know the motherboard form factors. Understand the differences between BTX, ATX, micro ATX, and NLX.

Know what the CMOS Setup utility does. The CMOS Setup utility allows you to configure the characteristics of certain portions of the PC.

Understand RAID levels. Know that RAID 0 is performance enhancement with no fault tolerance, RAID 1 is fault tolerance with no performance enhancement, and RAID 5 offers fault tolerance and enhances performance.

Working with Power Supplies

Power-supply problems are usually among the ones that are easy to troubleshoot: If the system doesn't respond in any way when the power is turned on or you are experiencing randomly frying parts, or an incredibly annoying sound, open the case, remove the power supply, and replace it with a new one.

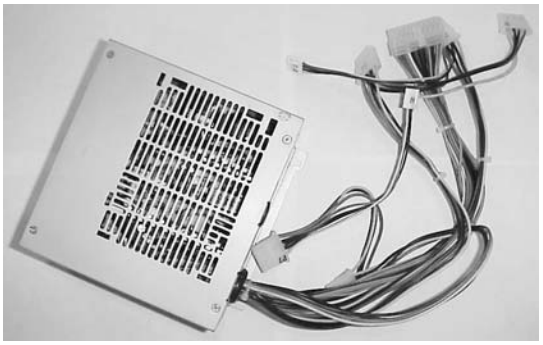
Critical Information

The device in the computer that provides the power is the *power supply*. A power supply converts 110-volt AC current into the voltages a computer needs to operate. On an AT motherboard, these are +5 volts DC, –5 volts DC, +12 volts DC, and –12 volts DC. Components in modern PCs don't use the negative voltages; they're provided for backward compatibility only. On an ATX motherboard, an additional voltage is provided: +3.3 volts DC.

Be aware that different cases have different types of on/off switches. The process of replacing a power supply is a lot easier if you purchase a replacement with the same mechanism. Even so, remember to document exactly how the power supply was connected to the on/off switch before you remove it.

Power supplies contain transformers and capacitors that carry *lethal* amounts of current. They aren't meant to be serviced. *Do not* attempt to open them or do any work on them. Figure 1.18 shows a generic power supply.

FIGURE 1.18 A power supply



A power supply has a rated output capacity in watts, and when you fill a system with power-hungry devices, you must make sure that maximum capacity isn't exceeded. Otherwise, problems with power can occur, creating lockups or spontaneous reboots.

To determine the wattage a device draws, multiply voltage by current. For example, if a device uses 5 amps of +3.3V and 0.7 amps of +12V, a total of 25 watts is consumed. Do this calculation for every device installed. Most devices have labels that state their power requirements. Some devices don't have power labels; for such devices, use the numbers in Table 1.6 for estimations.

As a general rule, you should have a large enough power supply for all the slots in the computer with the most likely devices that will be installed. In other words, you should calculate the power-supply capacity from what is possible and not just what is currently on the motherboard.

TABLE 1.6 Estimating Power Consumption

Component	Watts Consumed, for Estimating Purposes
Motherboard	20–30 watts
CPU	30–70 watts (faster CPU, more watts)
AGP video card	20–50 watts
PCI circuit boards	5 watts each
ISA circuit boards	10 watts each
Floppy drive	5 watts
CD drive	10–25 watts
RAM	8 watts per 128MB
IDE hard drive	5–15 watts
SCSI hard drive	10–40 watts

Power-Supply Problems

Power-supply problems can include randomly frying parts if there is a short. The fan failing will cause annoying sounds and the system will overheat. One key reason the fan can fail is if it is clogged with dust and debris.

Be aware that different cases have different types of on/off switches. The process of replacing a power supply is a lot easier if you purchase a replacement with the same mechanism. Even so, remember to document exactly how the power supply was connected to the on/off switch before you remove it. Be careful, as well, to set the voltage selector switch on the power supply to correspond to your voltage. Most power supplies have the ability to accept input of either 110 or 220 volts. Some expensive power supplies can autosense and need not be set manually, but most do and you want to set the switch to the correct voltage setting or you could cause damage.

A 20-pin main connector from the power supply to the motherboard is standard for all ATX power supplies. In addition to this connector, many will include an auxiliary power connector of either 4 or 6 pins to provide additional power.

In 2004, the ATX12V 2.0 standard was passed, changing the main connector from 20 pins to 24. The additional pins provide +3.3V, +5V, and +12V (the fourth pin is a ground) for use by PCIE cards. When a 24-pin connector is used, there is no need for the optional 4- or 6-pin auxiliary power connectors.

Exam Essentials

Learn to troubleshoot power supplies. Be able to think through common power supply problems and know that when you replace one you should check the voltage selector switch and set it properly.

Recognize power-supply problems. Become familiar with the symptoms of a dead, failing, or overloaded power supply.

Cooling Methods

The cooling system consists of the fan in the power supply, the fan or heat sink on the CPU, and any additional heat sinks or fans in the case. If a system is inadequately cooled, lockups and spontaneous reboots may occur.

Critical Information

Air cooling is the most common cooling method used in PCs. CPUs typically have *active heat sinks*, which are heat sinks that include an electric fan that constantly channels heat away. A CPU that is running too hot may benefit from a better cooling fan. The heat sink portion is a block of spikes that channel heat away from the CPU.

Most *passive heat sinks* (that is, heat sinks that don't include a fan) are attached to the CPU using a glue-like thermal compound. This makes the connection between the heat sink and the CPU more seamless and direct. Thermal compound can be used on active heat sinks too, but generally it isn't because of the possibility that the fan may stop working and need to be replaced. Thermal compound improves thermal transfer by eliminating tiny air pockets between the heat sink and CPU (or other device like a northbridge or video chipset). Thermal glue provides both improved thermal transfer and adds bonding for heat sinks when there are no mounting holes to clamp the heat sink to the device to be cooled. Clamps or screws are commonly used to attach heat sinks to CPUs; therefore thermal compound is used more often than thermal glue for CPU active or passive heatsinks.

In addition to the main fan in the power supply, you can install additional cooling fans in a case to help circulate air through the case.

Liquid-cooled cases are available that use circulating water rather than fans to keep components cool. These cases are typically more expensive than standard ones and may

be more difficult for an untrained technician to work on, but they result in an almost completely silent system.

Cooling Issues

A PC that works for a few minutes and then locks up is probably experiencing overheating due to a heat sink or fan not functioning properly. To troubleshoot overheating, first check all fans inside the PC to ensure they're operating, and make sure any heat sinks are firmly attached to their chips.

In a properly designed, properly assembled PC case, air flows in a specific path from the power-supply fan through the vent holes. Cases are designed to cool by making the air flow in a certain way. Therefore, operating a PC with the cover removed can make a PC more susceptible to overheating, even though it's "getting more air."

Similarly, operating a PC with empty expansion-slot backplates removed can inhibit a PC's ability to cool itself properly because the extra holes change the airflow pattern from what was intended by its design.

Although CPUs are the most common component to overheat, occasionally chips on other devices, particularly video cards, may also overheat. Extra heat sinks or fans may be installed to cool these chips.

Issues with liquid cooled machines can include problems with hoses or fittings, the pump, or the coolant. A failure of the pump can keep the liquid from flowing and cause the system to overheat. A liquid cooled system should also be checked every so often for leaks or corrosion on the hoses and fittings, and the reservoir should be examined to make sure it is full and does not contain contaminants.

Environmental Problems

Computers are like human beings. They have similar tolerances to heat and cold. In general, anything comfortable to us is comfortable to computers. They need lots of clean, moving air to keep them functioning.

Dirt, grime, paint, smoke, and other airborne particles can become caked on the inside of the components. This is most common in automotive and manufacturing environments. The contaminants create a film that coats the components, causing them to overheat and/or conduct electricity on their surface. Blowing out these exposed systems with a can of condensed air from time to time can prevent damage to the components. While you're cleaning the components, be sure to clean any cooling fans in the power supply or on the heat sink.

To clean the power-supply fan, blow the air from the inside of the case. When you do this, the fan will blow the contaminants out the cooling vents. If you spray from the vents toward the inside of the box, you'll be blowing the dust and grime inside the case or back into the fan motor.

One way to ensure that the environment has the least possible effect on your computer is to always leave the *blanks* in the empty slots on the back of your box. These pieces of metal are designed to keep dirt, dust, and other foreign matter from the inside of the computer. They also maintain proper airflow within the case to ensure that the computer doesn't overheat.

Exam Essentials

Learn to troubleshoot overheating issues. When overheating occurs, you need to be able to isolate the source quickly and respond before the problem affects internal system components.

Identify problems that can result from overheating. Overheating can cause spontaneous rebooting or shutdown. Overheating is often caused by nonfunctioning cooling fans or improper airflow through the PC.

Display Devices

Several types of computer displays are used today, including the TV. All of them use either the same *cathode ray tube* (*CRT*) technology found in television sets or the *liquid crystal display* (*LCD*) technology found on all laptop, notebook, and palmtop computers.

Critical Information

There are two ways of measuring a monitor's image quality: dot pitch and refresh (scan) rate. A monitor's *dot pitch* is the distance between two dots of the same color on the monitor. Usually given in fractions of a millimeter (mm), it tells how sharp the picture is. The lower the number, the closer together the pixels are, and thus the sharper the image. An average dot pitch is 0.28mm.

A monitor's *refresh rate* specifies how many times in one second the scanning beam of electrons redraws the screen. The phosphors stay bright for only a fraction of a second, so they must constantly be hit with electrons to stay lit. Given in draws per second, or hertz (Hz), the refresh rate specifies how much energy is being put into keeping the screen lit. Most people notice a flicker in the display at refresh rates of 75Hz or lower because the phosphors begin to decay to black before they're revived; increasing the refresh rate can help reduce eyestrain by reducing the flickering.

The *resolution* of a monitor is the number of horizontal and vertical pixels that are displayed. Most monitors allow for two or more resolutions, and you can pick the one to use in the desktop settings of the operating system. The vertical hold (V-hold) settings can be tweaked to make the image appear properly in the monitor. Connectors commonly used to connect the display device include the following:

VGA This is the traditional connector, which is shaped like a D and has three rows of five pins each, for a total of 15 pins. This is also often called the DB-15 connector.

A 9-pin VGA connector does exist, but it's very uncommon.

Digital Video Interface (DVI) There are several types of DVI pin configurations, but all connectors are D-shaped. The wiring differs based on whether the connector is single-linked or dual-linked (extra pins are used for the dual link). DVI differs from everything else in that it includes both digital and analog signals at the same time, which makes it popular for LCD and plasma TVs. Figure 1.19 shows a DVI connector.

FIGURE 1.19 One of several possible DVI connectors

High Definition Multimedia Interface (HDMi) These connectors are used to connect compatible digital items (DVD players, for example). The Type A connector has 19 pins and is backward compatible with DVI. Type B connectors have 29 pins and aren't backward compatible with DVI, but they support greater resolutions.

S-Video The S-Video connector looks much like a PS/2 connector, except that it has four conductors. These are also known as Y/C connectors; they break the signal into two components (luminance and chrominance) instead of carrying them in a single signal.

Component/RGB Component connectors are similar to what you use to connect video recorders and other items to televisions. They have RCA jacks and use red, green, and blue signals.

Liquid Crystal Displays

Two major types of LCDs are used in laptops today: *active matrix* screens and *passive matrix* screens. Their main differences lie in the quality of the image. Both types use some kind of lighting behind the LCD panel to make the screen easier to view.

Passive Matrix A passive matrix screen uses a row of transistors across the top of the screen and a column of them down the side. It sends pulses to each pixel at the intersections of each row and column combination, telling it what to display.

Passive matrix displays are becoming obsolete because they're less bright and have poorer refresh rates and image quality than active matrix displays. However, they use less power than active matrix displays do.

Active Matrix An active matrix screen uses a separate transistor for each individual pixel in the display, resulting in higher refresh rates and brighter display quality. These screens use more power, however, because of the increased number of transistors that must be powered. Almost all notebook PCs today use active matrix. A variant called thin-film transistor (TFT) uses multiple transistors per pixel, resulting in even better display quality.

Display resolutions include the following, which you must know for the A+ Essentials exam:

XGA Extended graphics array has been around since 1990. It's a 1024×768 resolution that offers fixed-function hardware acceleration for 2D tasks.

SXGA+ Super extended graphics array is a 1400×1050 resolution commonly used on 14- or 15-inch laptops. It's typically considered the maximum resolution that video projectors will work with.

UXGA Ultra extended graphics array is a 1600×1200 resolution and is the next step in the monitor-resolution evolution.

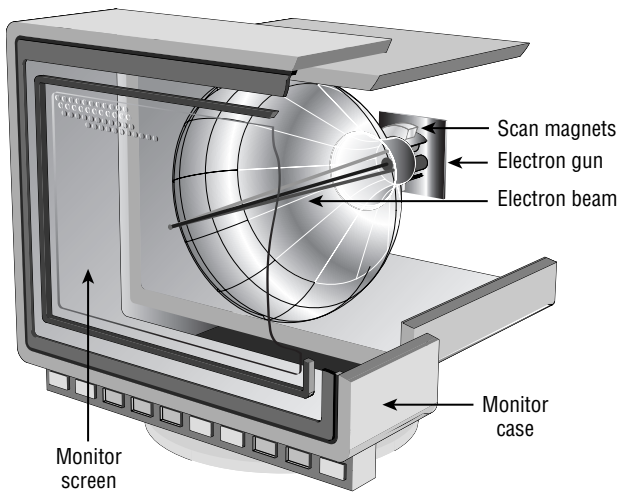
WUXGA Widescreen ultra extended graphics array is a resolution of 1920×1200 with a 16:10 screen aspect ratio. It's also a standard for use with television sets, at a slightly different ratio.

Contrast ratio is a measurement of the brightness of the LCD panels. A general rule of thumb is the greater the contrast ratio, the brighter the display can be, and thus a rating of 3000:1 is preferred over 800:1. The *native resolution* of an LCD monitor is its ideal resolution setting without needing to stretch the image (which causes the image quality to degrade).

CRT Displays

In a CRT (cathode ray tube), a device called an *electron gun* shoots electrons toward the back of the monitor screen (see Figure 1.20). The back of the screen is coated with special chemicals (called *phosphors*) that glow when electrons strike them. This beam of electrons scans the monitor from left to right and top to bottom to create the image.

FIGURE 1.20 How a CRT monitor works



The creation of the image is known as a raster. Rasterizing an image, thus, is creating the image in such a way that it can be displayed in a rectangular ray.

Display System Problems

There are two types of video problems: no video and bad video. *No video* means no image appears on the screen when the computer is powered up. *Bad video* means the quality is substandard for the type of display system being used.

No Video

Any number of things can cause a blank screen. These three are the most common: the power is off, the monitor's cable is unplugged, or the contrast or brightness is turned down.

If you've checked the power as well as the brightness and contrast settings, then the problem could be a bad video card or a bad monitor. Most monitors these days display a *Working* message briefly when you turn them on, so you can ascertain that the monitor is working and that an amber light appears on the front. When the PC starts up, the light on the front of the monitor changes from amber to green, indicating that the monitor is receiving a signal.

If the monitor is working but not receiving a signal from the PC, the video card may be bad. However, no video can also mean a problem with the motherboard, RAM, or CPU, so it isn't a given that the video card is at fault when no video appears.

Malfunctioning monitors are usually not worth fixing, because the cost of the labor involved exceeds the cost of a brand-new monitor. In addition, it may be difficult to find a technician to work on a monitor, because it isn't part of most standard PC technician training programs (due to the risk of electric shock from the high-voltage capacitor inside the monitor).

Bad Video

A monitor that doesn't display one of the three basic colors (red, green, or blue) probably has a bad cable, a bent or broken pin, or a loose connection at either the PC or the monitor. This is the case because different pins on the connectors—and wires in the cable—control different colors.

Color problems may also result from the monitor being out of adjustment. With most new monitors, this is an easy problem to fix. Old monitors had to be partially disassembled to change these settings; new monitors have push-button control panels for changing these settings.

Exposure to a magnetic field can cause swirls and fuzziness even in high-quality monitors. The earth generates magnetic fields, as do unshielded speakers and power surges. Most monitors have metal shields that can protect against magnetic fields. But eventually these shields can become polluted by taking on the same magnetic field as the earth, so they become useless. To solve this problem, these monitors have a built-in feature known as *Degauss*; it removes the effects of the magnetic field by creating a stronger magnetic field with opposite polarity that gradually fades to a field of zero. A special Degauss button or feature in the monitor's onscreen software activates it. You need only press it when the picture starts to deteriorate. The image will shake momentarily during the Degauss cycle and then return to normal.

Upgrading Display Devices

Before connecting or disconnecting a monitor, ensure that the power to both the PC and the monitor is off. Then, connect a VGA (DB-15) cable from the monitor to the PC's video card, and connect the monitor's power cord to an AC outlet.

Other than the power supply, one of the most dangerous components to try to repair is the monitor, or CRT monitor. I recommend that you *not* try to repair monitors. To avoid the extremely hazardous environment contained inside the monitor—it can retain a high-voltage charge for hours after it's been turned off—take it to a certified monitor technician or television repair shop. The repair shop or certified technician will know and understand the proper procedures to discharge the monitor, which involves attaching a resistor to the flyback transformer's charging capacitor to release the high-voltage electrical charge that builds up during use. They will also be able to determine whether the monitor can be repaired or needs to be replaced. Remember, the monitor works in its own extremely protective environment (the monitor case) and may not respond well to your desire to try to open it. The CRT is vacuum-sealed. Be extremely careful when handling it—if you break the glass, the CRT will implode, which can send glass in any direction.

Even though I recommend not repairing monitors, the A+ exam does test your knowledge of the safety practices to use when you need to do so. If you have to open a monitor, you must first discharge the high-voltage charge on it using a high-voltage probe. This probe has a very large needle, a gauge that indicates volts, and a wire with an alligator clip. Attach the alligator clip to a ground (usually the round pin on the power cord). Slip the probe needle under the high-voltage cup on the monitor. You'll see the gauge spike to around 15,000 volts and slowly reduce to zero. When it reaches zero, you may remove the high-voltage probe and service the high-voltage components of the monitor.

If you have a monitor that shows bad distortion, and changing the settings or Degaussing has no effect, then look for magnetic interference caused by nearby florescent lights or large power sources.

Using Multimonitor

Multimonitor, also known as multidisplay, is simply using more than one display device for a single PC. Most PCs allow you to use multiple monitors as long as there is a display card installed for each. While this can be useful for running a window for each monitor, one of the most common uses is the Presenter View in Microsoft PowerPoint. When chosen, this allows a different view of the slideshow to be shown on the main monitor (typically a projector) than what is shown on the secondary monitor (such as presenter notes, the next slide that is set to appear, etc.).

Exam Essentials

Know how to deal with display problems. Know that before you begin to work on a display system, you must take safety precautions because of the power that is stored within.

Be able to determine the cause of display system problems. The most common display problems relate to power, brightness, or contrast. Adjusting the monitor controls should be your first step when troubleshooting.

Input and Peripheral Devices

A virtually unlimited number of types of input devices can be connected to a PC. In addition to the standard keyboard and mouse, there are bar-code readers, digital cameras, microphones, biometric devices, touch screens, and a plethora of others. Many today connect through the USB or FireWire port, using instructions from the vendor. However, you must know about other types of connections for the A+ exam.

Critical Information

Keyboard connectors allow for the direct connection of the keyboard to the motherboard. There are essentially three types of keyboard connectors: AT, PS/2, and USB.

AT connectors are round, about 1½″ in diameter, and have five sockets in the DIN-5 configuration. They're found on AT motherboards. The second style, PS/2 connectors, are smaller and look just like a PS/2 mouse connector; these are found on ATX motherboards. USB keyboards are rapidly growing in popularity and allow you to connect to any available USB port (front, back, side, etc.).

A mouse connector is a PS/2-style connector; on an ATX it's built into the side of the motherboard, and on an AT a small ribbon cable connects a back-mountable port to the motherboard.

Troubleshooting Keyboard and Mouse Problems

Usually, keyboard problems are environmental. Keyboards get dirty, and the keys start to stick.

If a keyboard is malfunctioning (for example, sending the wrong characters to the display), it's most cost-effective to replace it rather than spend hours attempting to fix it, because keyboards are fairly inexpensive.

One way to clean a keyboard is with the keyboard cleaner sold by electronics supply stores. This cleaner foams up quickly and doesn't leave a residue behind. Spray it liberally on the keyboard and keys. Work the cleaner in between the keys with a stiff toothbrush. Blow away the excess with a strong blast of compressed air. Repeat until the keyboard functions properly. If you have to clean a keyboard that's had a soft drink spilled on it, remove the key caps before you perform the cleaning procedure; doing so makes it easier to reach the sticky plungers.

Remember that most of the dollars spent on systems are for labor. If you spend an hour cleaning a $12.00 keyboard, then you have probably just cost your company $20.00. Knowing how to fix certain things doesn't necessarily mean that you *should* fix them. Always evaluate your workload, the cost of replacement, and the estimated cost of the repair before deciding on a course of action.

Similarly, most mouse problems, such as the pointer failing to move in one direction or the other, or the pointer jumping around onscreen, are due to dirt building up inside the mouse. To clean a standard mouse, remove the plate on the bottom of the mouse that holds the ball in place; then remove the ball, and clean the inside chamber with an alcohol-dipped cotton swab. Clean the ball itself with mild soap and water. Don't use alcohol on the ball, because it tends to dry out the rubber.

Rather than being ball-driven, many mice today are optical. This simplifies cleaning, in that the only thing you need to do is wipe dust away from the optical sensor.

Peripheral Ports and Connectors

In order for a PC to be useful, there of course must be a way to get the data into and out of the computer. To accomplish this, several ports are available. The four most common types of ports are the serial, parallel, USB, and game ports. Figure 1.21 shows some typical ports built into an ATX motherboard.

FIGURE 1.21 Built-in ports on a motherboard

These ports are connected to the motherboard using small ribbon cables on an AT system, or they're built directly into the side of the motherboard on an ATX system.

Adapter Cards

Adapter cards are also known by many other names, including *circuit boards/cards* and *expansion boards/cards*. In all cases, adapter cards are circuit boards that fit into expansion slots in the motherboard. They can include modems, network interface cards, sound cards, and many other types of devices.

Adapter cards are purchased to match an available expansion slot in the motherboard. PCI is the most common type of expansion slot for an adapter card in today's PCs. ISA slots are nearly obsolete, and AGP slots are used only for video cards.

Expansion slots are used to install various devices in the computer to expand its capabilities. Some expansion devices that may be installed in these slots include video, network, sound, and disk interface cards.

Expansion slots come in three main types: ISA, PCI, and AGP. Each type is different in appearance and function, as you'll learn in future chapters. You should be able to visually identify the different expansion slots on the motherboard:

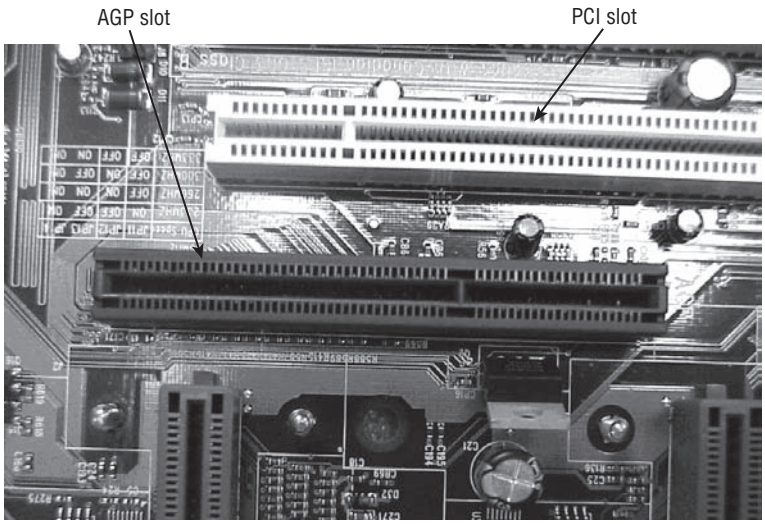
ISA Expansion Slots If you're repairing a computer made before 1997, chances are the motherboard in your computer has a few ISA slots. These slots are usually brown and are separated into two unequal lengths. Computers made after 1997 generally include a few ISA slots for backward compatibility with old expansion cards.

PCI Expansion Slots Most computers made today contain primarily PCI slots. They're easily recognizable, because they're short (around 3 inches long) and are usually white. PCI slots can usually be found in any computer that has a Pentium-class processor or higher.

AGP Expansion Slots AGP slots are very popular today. In the past, if you wanted to use a high-speed, accelerated 3D graphics video card, you had to install the card into an existing PCI or ISA slot. AGP slots were designed to be a direct connection between the video circuitry and the PC's memory. They're also easily recognizable because they're usually brown and located right next to the PCI slots on the motherboard. Figure 1.22 shows an example of an AGP slot, along with a PCI slot for comparison.

PCIE Expansion Slots PCIE combines the functionality of PCI with AGP and was discussed earlier in this chapter.

FIGURE 1.22 An AGP slot compared to a PCI slot



Sound-Card Problems

Sound cards are traditionally one of the most problem-ridden components in a PC. They demand a lot of PC resources and are notorious for being inflexible in their configuration. The most common problems related to sound cards involve resource conflicts (IRQ, DMA, or I/O address). The problem is much less pronounced on PCI than on ISA cards.

Luckily, most sound-card vendors are aware of the problems and ship very good diagnostic utilities to help resolve them. Use your PC troubleshooting skills to determine the conflict, and then reconfigure until you find an acceptable set of resources that aren't in use.

Some legacy sound cards aren't completely Plug and Play–compatible. Windows may detect that new hardware has been installed but be unable to identify the new hardware as a working sound card. To fix this problem, run the Setup software that came with the sound card.

Network Interface Card Problems

In general, network interface cards (NICs) are added to a PC via an expansion slot, but may also be added through a USB or PCMCIA slot. The most common issue that prevents network connectivity is a bad or unplugged patch cable.

Cleaning crews and the rollers on the bottoms of chairs are the most common threats to a patch cable. In most cases, wall jacks are placed 4 to 10 feet away from the desktop. The patch cables are normally lying exposed under the user's desk, and from time to time damage is done to the cable, or it's inadvertently snagged and unplugged. When you troubleshoot a network adapter, start with the most rudimentary explanations first. Make sure the patch cable is tightly plugged in, and then look at the card and see if any lights are on. If there are lights on, use the NIC's documentation to help troubleshoot. More often than not, shutting down the machine, unplugging the patch and power cables for a moment, and then reattaching them and rebooting the PC will fix an unresponsive NIC.

Although this isn't on the test, it's useful information: Wake on LAN cards have more problems than standard network cards. In my opinion, this is because they're always on. In some cases, you'll be unable to get the card working again unless you unplug the PC's power supply and reset the card.

Ports and Cables

A computer's peripheral ports are the physical connectors found outside the computer. Cables of various types are designed to plug into these ports and create a connection between the PC and the external devices that may be attached to it. A successful IT technician should have an in-depth knowledge of ports and cables.

Because the peripheral components need to be upgraded frequently, either to keep pace with technological change or to replace broken devices, the test requires a well-rounded familiarity with the ports and their associated cabling.

Unless a peripheral device connects directly to the motherboard, it must use a port. Ports can be distinguished from one another by three factors:

Bits of Data Simultaneously Conveyed A *serial cable* carries only one bit at a time. A *parallel cable* carries multiple bits at a time (usually eight).

Data Transmission Speed This is expressed in kilobits or megabits per second and refers to the overall data throughput.

Type of Connector A wide variety of connectors are used in PCs today, including the DB style (as with legacy parallel and serial ports and VGA monitors), Centronics style (as with printers and some SCSI devices), and USB.

Parallel vs. Serial

A cable (and its port) can be either parallel or serial, and it isn't always immediately obvious from looking which is which. For example, both parallel and serial cables can use the DB-25 style of connector.

Both parallel and serial cables have multiple wires inside them, but they use them for different purposes. A parallel cable uses eight wires to carry bits of data in each direction, plus extra wires for signaling and traffic control. A serial cable uses only one wire to carry data in each direction; all the rest of its wires are for signaling and traffic control.

Transmission Speed

Neither parallel nor serial is intrinsically faster than the other. There are both fast and slow parallel and serial connections. For example, a legacy serial port such as for an external modem carries data fairly slowly (about 115Kbps), but a USB cable (also serial) carries data very quickly (up to 12Mbps for USB 1.1, and even faster for USB 2.0—480Mbps).

Connector Types

The following are common connector types:

DB A D-shaped connector with a metal ring around a set of pins. Named for the number of pins/holes used: DB-25, DB-9, DB-15, and so on. Can be either parallel or serial. Common uses: VGA video, legacy serial devices such as external modems, and parallel printer cables (the connector on the PC only; the printer end uses Centronics).

RJ Registered jack; a plastic plug with small metal tabs, like a telephone cord plug. Numbering is used in the naming: RJ-11 has two metal tabs, and RJ-14 has four. Both are used for telephone systems. RJ-45 has eight tabs and is used for Ethernet 10BaseT/100BaseT networking. Always serial.

BNC Stands for Bayonet-Neill Connector or British Naval Connector. A metal wire surrounded by shielding, like a cable television connector. Used for 10Base2 Ethernet networking. Always serial.

Centronics A plastic block with metal tabs flat against it, surrounded by a D-shaped metal ring. Used to connect a parallel printer cable to the printer, and also for some SCSI devices. Always parallel.

Ribbon Connector A rectangular block consisting of a set of square holes that connect to pins on a circuit board. Used to connect floppy drives, IDE drives, and some SCSI devices to their controllers. Always parallel.

PS/2 (Mini-DIN) A round connector with six small pins inside, commonly used to connect keyboards on ATX motherboards or PS/2 style mice.

DIN A larger round connector with five rather large pins inside, used for connecting the keyboard on an AT motherboard.

USB A flat rectangular connector, used with USB interfaces.

Cabling

Cables are used to connect two or more entities together. They're usually constructed of several wires encased in a rubberized outer coating. The wires are soldered to modular connectors at both ends. These connectors allow the cables to be quickly attached to the devices they connect.

Cables may be either shielded or unshielded. This refers to shielding against electromagnetic interference (EMI); it has nothing to do with whether the cable is shielded against dirt or water.

A list of common cable types used in PCs, their descriptions, their maximum effective lengths, and their most common uses is given in Table 1.7. The F or M in a connector's designation is for female (holes) or male (pins).

TABLE 1.7 Common PC Cable Descriptions

Application	1st Connector	2nd Connector	Max. Length
Null modem	DB-9F	DB-9F	25 feet
Null modem	DB-25F	DB-25F	25 feet
RS-232 (modem cable)	DB-9F	DB-25M	25 feet
RS-232 (modem cable)	DB-25F	DB-25M	25 feet
Parallel printer	DB-25M	Centronics 36M	10 feet
External SCSI cable	Centronics 50M	Centronics 50M	10 feet (total SCSI bus length)
VGA extension cable	DB-15M	DB-15M	3 feet
UTP Ethernet cable	RJ-45M	RJ-45M	100 meters
Thinnet Ethernet cable	BNC-M	BNC-M	100 meters
Telephone wall cable	RJ-11M or RJ-14M	RJ-11M or RJ-14M	N/A

One cable that deserves special mention is the null modem cable. It allows two computers to communicate with each other without using a modem. This cable has its transmit and receive wires crossed at both ends, so when one entity transmits on its TD line, the other entity receives it on its RD line.

Unshielded twisted pair (UTP) is the most common type of cable used for network cabling. There are various categories of network cabling; the category required for 10BaseT/100BaseT networking is Category 5, often shortened to Cat 5. There is also a Cat 5e cable type, which is used for higher-speed Ethernet such as Gigabit Ethernet.

Miscellaneous Peripherals

There is almost no limit to the number, or type, of peripherals and input devices that can be connected to a computer. CompTIA wants you to know that the day when only the keyboard and mouse were connected have gone by the wayside.

Among the many devices that can be connected today are the following:

- Bar code reader, used for scanning barcodes.
- Biometric devices, used for authentication purposes; among the most common are thumb readers included with a number of laptops.
- Capture cards, used for capturing video, typically using RCA connectors.
- KVM switches, which allow you to use one keyboard, video, and mouse set with a number of PCs.
- Multimedia (such as web and digital cameras, MIDI, microphones); used to input video and audio, and commonly use USB or FireWire connections.
- Touch screen, available for desktops and laptops; this adapter allows you to interact with the software by touching the screen.
- TV tuner cards, used to receive television signals on the computer; most include a capture card built in.

Exam Essentials

Know what RJ-45 connectors are used for. You're likely to be asked what type of connector would be used to attach a network connector to a wall jack.

Know what PS2/mini-DIN connectors are used for. You're likely to be asked what type of connector would be used to connect a keyboard or mouse to the back of a PC.

Know what RJ-11 connectors are used for. You're likely to be asked what type of connector would be used to connect a modem to a telephone jack.

Principles of Laptops and Portable Devices

Whether you choose to call them laptops, portable devices, or something different is mostly a matter of semantics. This objective tests your knowledge of some of the basic operations of laptops. In many cases, the components are the same as in a desktop computer, and they were discussed already. We'll focus now on those that are different.

Critical Information

A portable computer must provide all the functionality of a desktop counterpart yet be able to withstand travel, run in the absence of AC power, and be much smaller and more compact. When you get right down to it, there is not a great deal of difference between laptop and desktop computers, with the exception that laptops are more difficult to disassemble and form factors on items such as motherboards, memory, and hard drives become important. While they perform the same functions, size is critical.

Laptop-specific elements are discussed in this section.

Docking Stations

Some notebook PCs have optional accessories called *docking stations* or *port replicators*. These let you quickly connect/disconnect with external peripherals and may also provide extra ports that the notebook PC doesn't normally have.

A docking station essentially allows a laptop computer to be converted to a desktop computer. When plugged into a docking station, the laptop has access to things it doesn't have as a stand-alone—the network, a workgroup printer, and so on. The cheapest form of docking station (if it can be called that) is a *port replicator*. Typically, you slide a laptop into the port replicator, and the laptop can then use a full-sized monitor, keyboard (versus the standard 84 keys on a laptop), mouse, and so on. Extended, or enhanced, replicators add other ports not found on the laptop, such as PC slots, sound, and more. The most common division between port replicators and docking stations is whether the peripheral provides network access and expands the laptop's capabilities.

Laptops can support Plug and Play at three different levels, depending on how dynamically they're able to adapt to changes:

Cold Docking The laptop must be turned off and back on for the change to be recognized.

Warm Docking The laptop must be put in and out of suspended mode for the change to be recognized.

Hot Docking The change can be made and is recognized while running normal operations.

Each docking station works a little differently, but there is usually a button you can press to undock the notebook from the unit. There may also be a manual release lever in case you need to undock when the button is unresponsive.

Because different hardware is available in docked versus undocked configurations, you may want to set up hardware profiles in Windows to account for the differences.

Autoswitching and Fixed Input

Autoswitching power supplies allow you to use the same supply for more than one voltage. Most autoswitching power supplies can operate on voltages from 100 to 240, allowing them to be used in countries almost anywhere in the world. Fixed-input power supplies, on the other hand, regulate the voltage coming in to make certain it stays consistent.

Notebook Batteries

When you're shopping for notebook batteries, be aware not only of the physical size and shape (which vary depending on the notebook manufacturer's specifications) but also of the battery technology:

Nickel-Cadmium (NiCad) The least preferable. Must be recharged every 3 to 4 hours. A full recharge can take as long as 12 hours. These batteries tend to lose their ability to hold a charge unless they're fully discharged each time before being recharged. Leaving the notebook PC plugged in all the time and using the battery only occasionally for short periods can eventually ruin the battery.

NiCad batteries are not likely to be on any new device these days.

Nickel-Metal Hydride (NiMH) Better than NiCad because they don't use heavy metals with great toxicity. They can also store up to 50 percent more power and don't suffer loss of functionality from partial draining and recharging.

Lithium Ion (Li-ion) Lightweight and have a long life, plus they aren't subject to problems with partial draining and recharging. They tend to be more expensive than NiCad or NiMH, however.

Fuel Cell Casio has announced plans to produce a hydrogen fuel cell battery for notebook computers that promises to last 20 hours or more on a single charge. By the time you read this, it may be available, offering greatly increased performance but at a much higher price than normal notebook batteries.

When dealing with batteries, you must be careful not to dispose of them in the normal way, for they may harm the environment; whenever possible, recycling them is recommended. Here are some rules from the back of a typical battery:

- Don't put in fire or mutilate; may burst or release toxic materials
- Don't crush, puncture, incinerate, or short external circuits
- Don't short-circuit; may cause burns

Depending on the notebook model, the battery may be anywhere, but it's usually under the keyboard. On some models, you can slide the battery out the side by removing a panel or cover; on other models, you must lift the keyboard.

Pull out the battery, and insert a fresh battery in the same slot, pressing it firmly into place. Then, replace the cover over the battery's bay.

While manufacturers recommend a shutdown, in reality batteries are *hot-pluggable/swappable*, so you don't have to shut down in order to remove one. However, unless you have a second battery or are connected to AC power, you'll lose power and the PC will shut off when you remove the battery.

For purposes of exam study, hot-swappable and hot-pluggable are interchangeable terms.

PCMCIA Cards

PCMCIA cards (named after the Personal Computer Memory Card International Association) are the expansion cards for notebook PCs. Most notebook PCs have a PCMCIA bay that can accept one Type III device or two Type I or Type II devices:

Type I Up to 3.3mm thick. Used mostly for memory. These are very rarely used in today's systems, since the new laptops have other means of increasing memory, such as SoDIMMs.

Type II The most common type. Up to 5.5mm thick. Used for devices that would typically be expansion boards in a desktop PC, such as network interface cards.

Type III Up to 10.5mm thick. Used for drives. Not common.

In addition to these types based on thickness, there are other types based on technology. The PCMCIA (PC Card) standard has been updated to a new standard called CardBus; look for CardBus in the specification when you're buying PC Card devices. CardBus devices are backward compatible with older PCMCIA slots. Even newer is the Peripheral Component Interconnect (PCI) Express (PCIe) bus—a serial bus addition that uses low-voltage differential signaling (LVDS), allowing you to attach several devices at the same time (using serial communication instead of the parallel communication standard with most PC buses).

Ports and Communication Connections

Many laptops now include a Mini PCI slot for use with wireless adapters. Mini PCI slots are also common on docking stations. Mini PCI is a 32-bit bus that operates at 32MHz. It operates at only 3.3 volts and has three card configurations: Type I, Type II, and Type III. Whereas Types I and III provide support for an RJ-45 connector, Type II cards have an RJ-45 connector mounted on them.

Other connections/connectors common on laptops include Bluetooth, infrared, cellular WAN, WiFi, and Ethernet. All of these are discussed elsewhere in this book as they apply to networking.

Pointing and Input Devices

Pointing devices with laptops include such options as touchpads, point sticks, and track points. Some laptops come with only one of these, whereas others include a combination; and users can always opt for something else (such as a wireless mouse). Which you use is more a matter of preference and comfort than anything else.

Input devices can include a stylus, or *digitizer*. With this tool, a "pen" allows you to write directly on the screen, and the text written is digitized into data. When data is entered in this way, the laptop is often referred to as a *tablet PC*, maintaining the analogy of a tablet and pen.

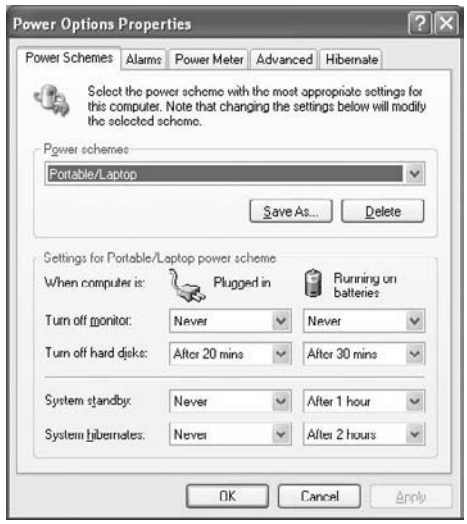
You should also know that the Function (Fn) key on a laptop is typically combined with the function keys and a few other special keys to enable the laptop to perform tasks not present on a desktop. For example, pressing Fn and F8 on a Dell laptop toggles the display in three modes: in the first, the display goes only to the monitor; in the second, it goes to the monitor and an output device such as a projector; and in the third, it goes only to the output device. It's typical to have Fn keys assigned for Standby and Hibernate modes as well as checking the battery status and toggling volume controls.

Power Management

Power management is essential with laptops. You don't want the system going dead when the battery gets low without properly warning you and doing everything possible to save the data. Although laptops include batteries and peripherals, the true strength in power management lies in the operating system.

With Windows XP, for example, you access the power options by choosing Start ➢ Control Panel ➢ Power Options to open a dialog box similar to that shown in Figure 1.23.

FIGURE 1.23 Power options in Windows XP



At least 10 power schemes are possible, including Home/Office Desk (which doesn't use power management), Portable/Laptop (the default on a laptop PC), Always On, Max Battery, and so on. From the Advanced tab, you can choose what happens when you close the lid, when you press the power button, and when you press the sleep button.

If you select "Always show icon on the taskbar," you can change power schemes by clicking that icon without having to access the power properties of the system.

By default, the alarms are set to notify you when only 10 percent of the battery life is left and to put the system in hibernation when only 3 percent of the battery life is left. You can change all these options to fit individual circumstances.

Power Configuration

The Advanced Configuration Power Interface (ACPI) must be supported by the system BIOS in order to work properly. With ACPI, it is the BIOS that provides the operating system with the necessary methods for controlling the hardware. This is in contrast to APM (Advanced Power Management), which only gave a limited amount of power to the operating system and let the BIOS do all the real work. Because of this, it is not uncommon to find legacy systems that can support APM but not ACPI.

There are three main states of power management common in most operating systems:

Hibernate This state saves all the contents of memory to the hard drive and preserves all data and application information exactly where they are. When the system comes out of hibernation, it returns the system to its previous state.

Standby This state leaves memory active but saves everything else to disk.

Suspend In most operating systems, this term is used interchangeably with Hibernate. In Windows XP, Hibernate is used instead of Suspend.

Adding and Removing PC Card Devices

PC Card devices are designed to be easily removed and installed. They're approximately the size and shape of a thick credit card, and they fit into PC Card (PCMCIA) slots in the side of the notebook PC. PC Card devices can include modems, network interface cards (NICs), SCSI adapters, USB adapters, FireWire adapters, and wireless Ethernet cards.

To eject a PC Card device, press the eject button next to its slot. To insert a PC Card device, press the device into the slot. You can do this while the computer is running. (That's called *hot-plugging* or *hot-swapping*.) However, in Windows, it's a good idea to stop the PC Card device before ejecting it, to ensure that all operations involving it complete normally. To do so, double-click the Safely Remove Hardware icon in the system tray, click the device, and then click Stop.

Disassembling a Notebook PC

There are many designs of notebook PC cases, and each one disassembles a little differently. The best way to determine the proper disassembly method is to consult the documentation from the manufacturer.

Some models of notebook PCs require a special T-8 Torx screwdriver. Most PC toolkits come with a T-8 bit for a screwdriver with interchangeable bits, but you may find that the T-8 screws are countersunk in deep holes so that you can't fit the screwdriver into them. In such cases, you need to buy a separate T-8 screwdriver, available at most hardware stores or auto-parts stores.

Prepare a clean, well-lit, flat work surface, assemble your tools and manuals, and ensure that you have the correct parts. Shut down the PC, unplug it, and detach any external devices such as an external keyboard, mouse, or monitor.

Many laptop manufacturers will consider a warranty void if an unauthorized person opens a laptop case and attempts to repair a laptop.

Removing and Replacing Disk Drives

Accessing the hard disk drive usually involves lifting the keyboard or removing it entirely. The hard disk typically has a ribbon cable made of thin plastic; be very careful when detaching it so you don't bend or break it. The hard disk also usually has a power connector that is smaller than that of a typical hard disk in a desktop PC. After you disconnect the hard disk, remove the screws holding it in place and lift it out.

The procedure for removing the floppy disk and/or CD drive varies widely depending on the model. Some notebook PCs are fully modular, so that the floppy disk and CD drives pop out easily without any tools. On other models, you may need to completely disassemble the PC to access them. Consult the documentation from the manufacturer.

After you remove the old drive, insert the new one in the same spot and secure it with screws. Then attach the power cable and ribbon cable, and reassemble the PC.

Adding Memory

Most notebook PCs have a certain amount of memory hard-wired into them that you can't remove. They also typically have a memory expansion slot into which you can insert a single circuit board containing additional RAM.

If such an additional memory module has been installed, you can remove it if desired (perhaps to replace it with one that has larger capacity). Most notebook PCs have a panel on the bottom held in place by screws. Remove this panel to expose the memory expansion slot. Then gently pull out the existing RAM module, if necessary, and insert the new RAM module.

Exam Essentials

Know the different types of PCMCIA cards. PCMCIA cards are the expansion cards for notebook PCs. Most notebook PCs have a PCMCIA bay that can accept one Type III device or two Type I or Type II devices.

Know the different monitor resolutions. The exam expects you to know four different types: XGA, SXGA+, UXGA, and WUXGA. Know the resolution for each of them.

Know the purpose of the Fn key. You should know that the Function (Fn) key on a laptop is typically combined with the function keys and a few other special keys to enable the laptop to perform tasks not present on a desktop.

Know the peripherals discussed. You should be familiar with docking stations and understand the principle reasons for their use.

Know about autoswitching and fixed-input power supplies. You should understand that autoswitching allows the power supply to be used in other countries without making manual adjustments.

Know what hot-swappable means. PC Card devices are hot-swappable, meaning you can remove and insert them while the computer is running. So are USB and FireWire devices. However, if you need to remove a drive, add or remove RAM, or connect or disconnect a monitor or a parallel or serial device, you must shut down the laptop.

Know where to look for the battery and for RAM expansion slots. Batteries are usually accessed either from the sides of a laptop or from under the keyboard. RAM is usually accessed on the bottom of the laptop. There will also be some RAM built into the motherboard that can't be removed.

Installation and Configuration of Printers

This objective tests your knowledge of how printers work and how they connect to computers. Although the A+ exam has traditionally focused heavily on laser printers, you may also see questions about other printer types. Scanners have also been added to this iteration of the exam, and you should know their basic characteristics as well.

Critical Information

The three major areas of study for this objective are printer technologies, printer interfaces, and scanners. The printer technologies include laser, ink-jet (sometimes called ink dispersion), dot matrix, solid ink, thermal, and dye sublimation. The printer interfaces include parallel, network, and Universal Serial Bus (USB), among others.

With regard to scanners, you're expected to know the different types of connections, which are—for the most part—identical to those for printers. Therefore, most of the focus here will be on printers.

This section provides details about various technologies of printers. These printers may be differentiated from one another in several ways, including the following:

Impact vs. Nonimpact Impact printers physically strike an inked ribbon and therefore can print multipart forms; nonimpact printers deliver ink onto the page without striking it. Dot matrix is impact; everything else is nonimpact.

Continuous Feed vs. Sheet Fed Continuous-feed paper feeds through the printer using a system of sprockets and tractors. Sheet-fed printers accept plain paper in a paper tray. Dot matrix is continuous feed; everything else is sheet fed.

Line vs. Page Line printers print one line at a time; page printers compose the entire page in memory and then place it all on the paper at once. Dot matrix and ink-jet are line printers; laser is a page printer.

Printer Components

In addition to the physical body of the printer, components and consumables are associated with it. Components include the following:

Memory As a general rule, the more memory the printer has, the better. The memory is used to hold the print jobs in the printer queue; the more users, and the larger the print jobs, the more memory you'll want.

Drivers These are the software components of the printer (or scanner)—allowing the device to communicate with the operating system. It's important to always have the correct and most current drivers, for the greatest efficiency.

Firmware Although drivers can be updated, firmware rarely is. Firmware is installed on the printer/scanner and can be thought of as the operating system for that device.

Consumables for printers are those items you must change as you use the printer—the variable items that get consumed and must be replenished. These include toner (or ink, depending on the type of printer you're using) and paper.

Be sure to always order and use the consumables that are recommended for your machine.

Dot-Matrix Printers

A dot-matrix printer is an impact printer; it prints by physically striking an inked ribbon, much like a typewriter. It's an impact, continuous-feed line printer.

The printhead on a dot-matrix printer consists of a block of metal pins that extend and retract. These pins are triggered to extend in patterns that form letters and numbers as the printhead moves across the paper. Early models, known as near letter quality (NLQ), printed using only nine pins. Later models used 21 pins and produced much better letter-quality (LQ) output.

The main advantage of dot matrix is its impact (physical striking of the paper). Because it strikes the paper, you can use it to print on multipart forms. Nonimpact printers can't do that. Dot-matrix printers aren't commonly found in most offices these days because of their disadvantages, including noise, slow speed, and poor print quality.

Dot-matrix printers are still found in many warehouses, and other businesses, where multipart forms are used.

Ink-Jet Printers

Ink-jet printers are one of the most popular types in use today. This type of printer sprays ink on the page to print text or graphics. It's a nonimpact, sheet-fed line printer.

Figure 1.24 shows an ink cartridge. Some cartridges, like this one, contain the printhead for that color of ink; you get a new printhead each time you replace the cartridge. On other printer models, the ink cartridge is just an ink reservoir, and the heads don't need replacing.

FIGURE 1.24 A typical ink cartridge (size: approximately 3×1½ inches)

There are two kinds of ink-jet printers: *thermal* and *piezoelectric*. These terms refer to the way the ink is sprayed onto the paper. A thermal ink-jet printer heats the ink to about 400° F, creating vapor bubbles that force the ink out of the cartridge. Thermal ink-jets are also sometimes called *bubble-jets*. A piezoelectric printer does the same thing but with electricity instead of heat.

Ink-jet printers are popular because they can print in color and are inexpensive. However, their print quality isn't quite as good as that of a laser printer, and the per-page cost of ink is much higher than for a laser printer. Therefore, most businesses prefer laser printers for their main printing needs, perhaps keeping one or two ink-jet printers around for situations requiring color printing.

Laser Printers

Laser printers are referred to as *page printers* because they receive their print job instructions one page at a time. They're sheet-fed, nonimpact printers. Another name for a laser printer is an *electrophotographic (EP)* printer.

LED printers are much like laser printers except they use light-emitting diodes (LEDs) instead of lasers. Their process is similar to that of laser printers. They're covered in more detail later in this chapter.

Parts of a Laser Printer

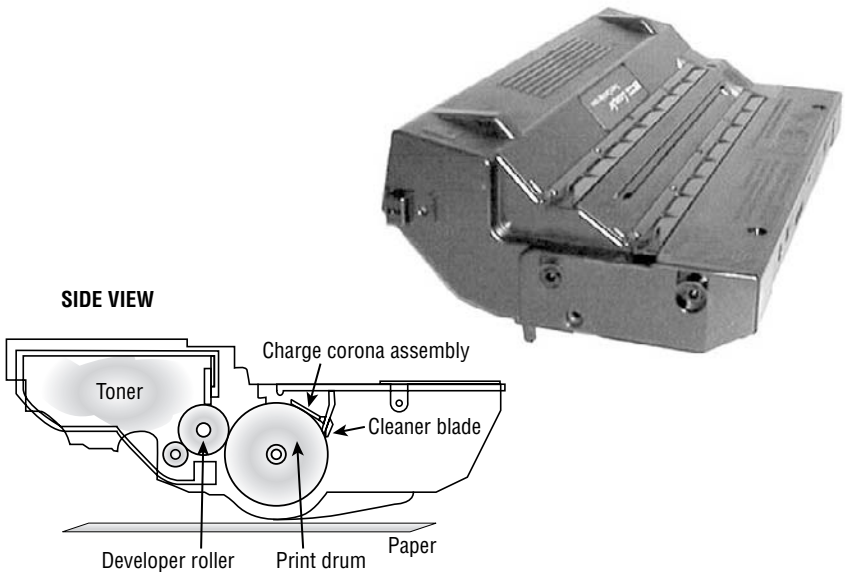
An electrophotographic laser printer consists of the following major components:

Printer Controller A large circuit board that acts as the motherboard for the printer. It contains the processor and RAM to convert data coming in from the computer into a picture of a page to be printed.

Toner Cartridge and Drum A powdery mixture of plastic resin and iron oxide. The plastic allows it to be melted and fused to the paper, and the iron oxide allows it to be moved around via positive or negative charge. Toner comes in a cartridge, like the one shown in Figure 1.25.

The drum is light sensitive; it can be written to with the laser scanning assembly. The toner cartridge in Figure 1.25 contains the print drum, so every time you change the toner cartridge, you get a new drum. In some laser printers, the drum is a separate part that lasts longer, so you don't have to change it every time you change the toner.

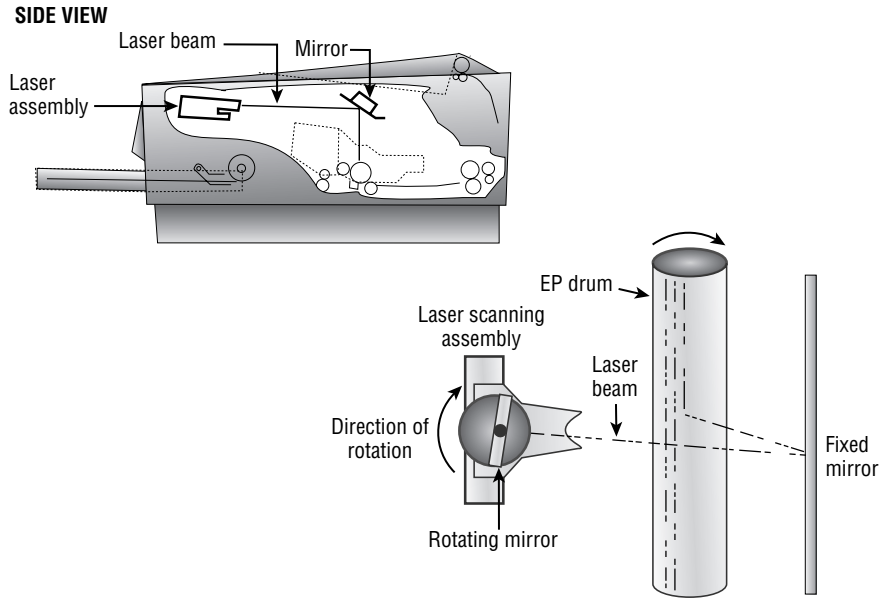
FIGURE 1.25 An EP toner cartridge



Primary Corona (Charge Corona) Applies a uniform negative charge (around –600V) to the drum at the beginning of the printing cycle.

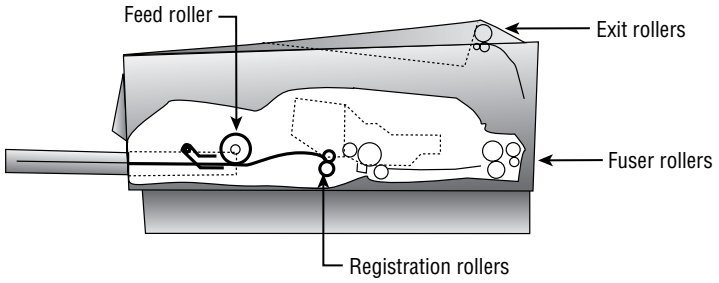
Laser Scanning Assembly Uses a laser beam to neutralize the strong negative charge on the drum in certain areas, so toner will stick to the drum in those areas. The laser scanning assembly uses a set of rotating and fixed mirrors to direct the beam, as shown in Figure 1.26.

FIGURE 1.26 The EP laser scanning assembly (side view and simplified top view)



Paper Transport Assembly Moves the paper through the printer. The paper transport assembly consists of a motor and several rubberized rollers. These rollers are operated by an electronic stepper motor. See Figure 1.27 for an example.

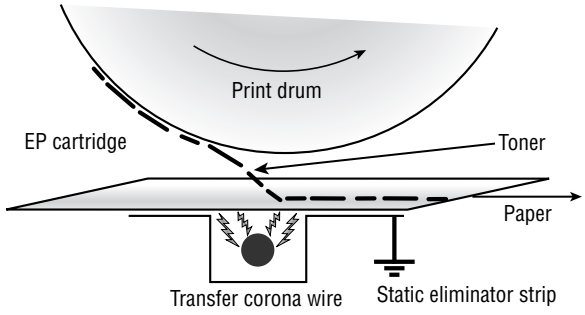
FIGURE 1.27 Paper transport rollers



Transfer Corona Applies a uniform positive charge (about +600V) to the paper. When the paper rotates past the drum, the toner jumps off the drum and onto the paper. Then the paper passes through a static eliminator that removes the positive charge from it. (See Figure 1.28.) Some printers use a transfer corona wire; others use a transfer corona roller.

High-Voltage Power Supply (HVPS) Delivers the high voltages needed to make the printing process happen. It converts ordinary 120V household AC current into high-DC voltages used to energize the primary and transfer corona wires (discussed later).

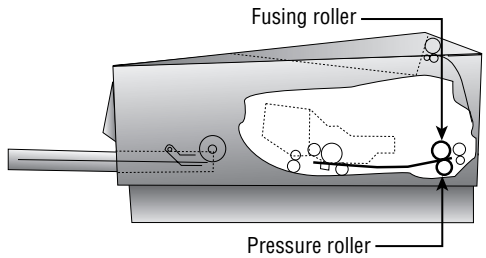
FIGURE 1.28 The transfer corona assembly



DC Power Supply Delivers lower voltages to components in the printer that need much lower voltages than the corona wires do (such as circuit boards, memory, and motors).

Fusing Assembly Melts the plastic resin in the toner so that it adheres to the paper. The fusing assembly contains a halogen heating lamp, a fusing roller made of Teflon-coated aluminum, and a rubberized pressure roller. The lamp heats the fusing roller, and as the paper passes between the two rollers, the pressure roller pushes the paper against the hot fusing roller, melting the toner into the paper. (See Figure 1.29.)

FIGURE 1.29 The fusing assembly



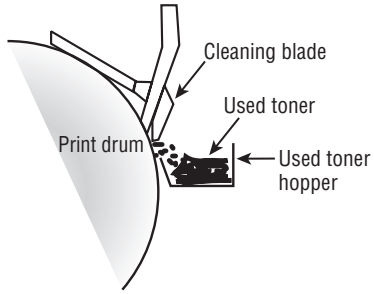
The Laser Printing Process

The laser (EP) print process consists of six steps. Here are the steps in the order you'll see them on the exam:

Step 1: Cleaning In the first part of the laser print process, a rubber blade inside the EP cartridge scrapes any toner left on the drum into a used-toner receptacle inside the EP cartridge, and a fluorescent lamp discharges any remaining charge on the photosensitive drum (remember that the drum, being photosensitive, loses its charge when exposed to light). See Figure 1.30.

The EP cartridge is constantly cleaning the drum. It may take more than one rotation of the photosensitive drum to make an image on the paper. The cleaning step keeps the drum fresh for each use. If you didn't clean the drum, you would see ghosts of previous pages printed along with your image.

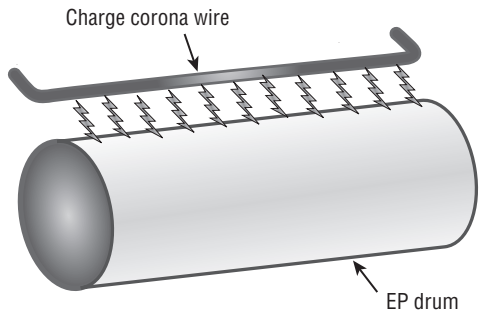
FIGURE 1.30 The cleaning step of the EP process



The actual amount of toner removed in the cleaning process is quite small. The cartridge will run out of toner before the used toner receptacle fills up.

Step 2: Conditioning In the *conditioning step* (Figure 1.31), a special wire (called a *primary corona* or *charge corona*) within the EP toner cartridge (above the photosensitive drum) gets a high voltage from the HVPS. It uses this high voltage to apply a strong, uniform negative charge (around –600VDC) to the surface of the photosensitive drum.

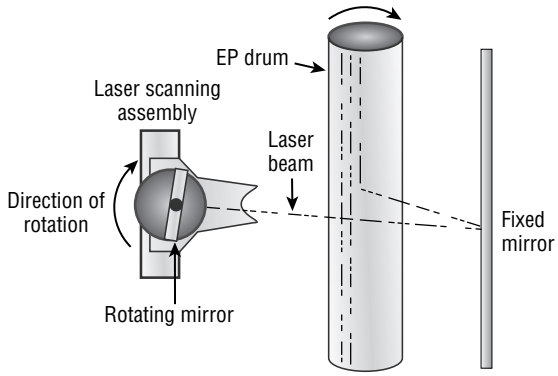
FIGURE 1.31 The conditioning step of the EP process



Step 3: Writing In the *writing step* of the EP process, the laser is turned on and scans the drum from side to side, flashing on and off according to the bits of information the printer controller sends it as it communicates the individual bits of the image. In each area where the laser touches the photosensitive drum, the drum's charge is severely reduced from –600VDC to a slight negative charge (around –100VDC). As the drum rotates, a pattern of exposed areas is formed, representing the images to be printed. Figure 1.32 shows this process.

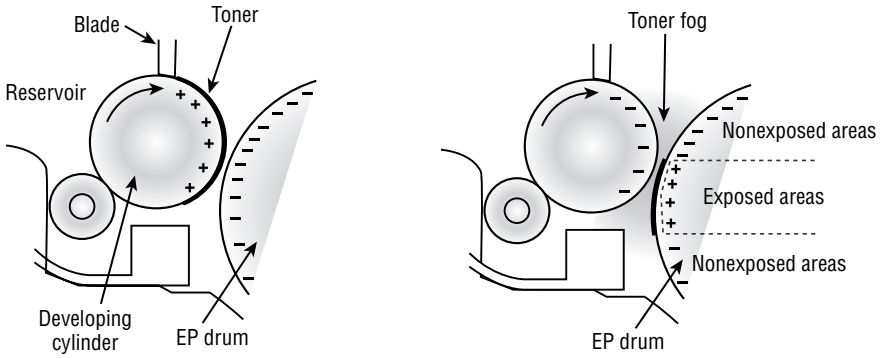
At this point, the controller sends a signal to the pickup roller to feed a piece of paper into the printer, where it stops at the registration rollers.

FIGURE 1.32 The writing step of the EP process



Step 4: Developing Now that the surface of the drum holds an electrical representation of the image being printed, its discrete electrical charges need to be converted into something that can be transferred to a piece of paper. The EP process's *developing step* accomplishes this (Figure 1.33). In this step, toner is transferred to the areas that were exposed in the writing step.

FIGURE 1.33 The developing step of the EP process



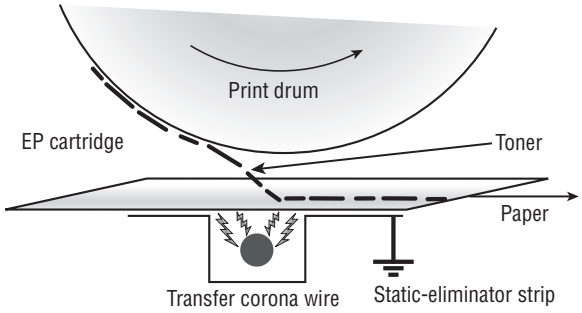
A metallic *developing roller* or *cylinder* inside an EP cartridge acquires a –600VDC charge (called a *bias voltage*) from the HVPS. The toner sticks to this roller because there is a magnet located inside the roller and because of the electrostatic charges between the toner and the developing roller. While the developing roller rotates toward the photosensitive drum, the toner acquires the charge of the roller (–600VDC). When the toner comes between the developing roller and the photosensitive drum, the toner is attracted to the areas that have been exposed by the laser (because these areas have a lesser charge, of –100VDC). The toner also is repelled from the unexposed areas (because they're at the same –600VDC charge, and like charges repel). This toner transfer creates a fog of toner between the EP drum and the developing roller.

The photosensitive drum now has toner stuck to it where the laser has written. The photosensitive drum continues to rotate until the developed image is ready to be transferred to paper in the next step.

Step 5: Transferring At this point in the EP process, the developed image is rotating into position. The controller notifies the registration rollers that the paper should be fed through. The registration rollers move the paper underneath the photosensitive drum, and the process of transferring the image can begin, with the *transferring step*.

The controller sends a signal to the corona wire or corona roller (depending on which one the printer has) and tells it to turn on. The corona wire/roller then acquires a strong *positive* charge (+600VDC) and applies that charge to the paper. The paper, thus charged, pulls the toner from the photosensitive drum at the line of contact between the roller and the paper, because the paper and toner have opposite charges. Once the registration rollers move the paper past the corona wire, the static-eliminator strip removes all charge from that line of the paper. Figure 1.34 details this step. If the strip didn't bleed this charge away, the paper would attract itself to the toner cartridge and cause a paper jam.

FIGURE 1.34 The transferring step of the EP process



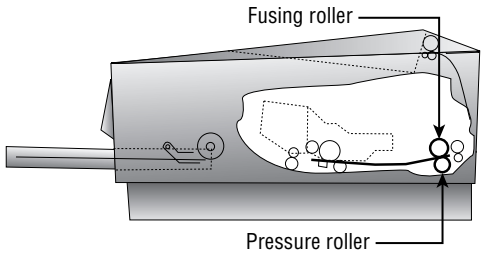
The toner is now held in place by weak electrostatic charges and gravity. It won't stay there, however, unless it's made permanent, which is the reason for the fusing step.

Step 6: Fusing In the final step, the *fusing step*, the toner image is made permanent. The registration rollers push the paper toward the fuser rollers. Once the fuser grabs the paper, the registration rollers push for only a short time more. The fuser is now in control of moving the paper.

As the paper passes through the fuser, the fuser roller melts the polyester resin of the toner, and the rubberized pressure roller presses it permanently into the paper (Figure 1.35). The paper continues on through the fuser and eventually exits the printer.

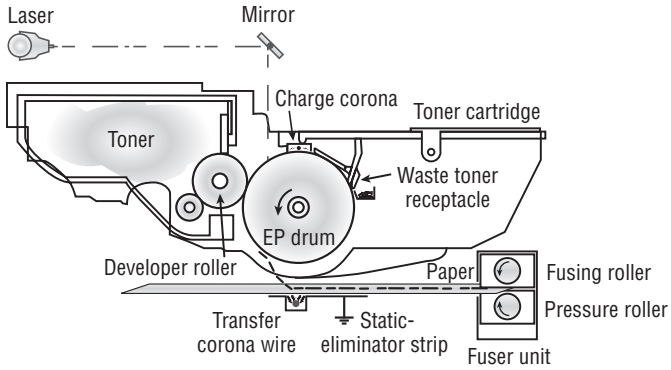
Once the paper completely exits the fuser, it trips a sensor that tells the printer to finish the EP process with the cleaning step. At this point, the printer can print another page, and the EP process can begin again.

FIGURE 1.35 The fusing step of the EP process



Putting It All Together Figure 1.36 summarizes all the EP process printing steps. First, the printer uses a rubber scraper to clean the photosensitive drum. Then the printer places a uniform, negative, –600VDC charge on the photosensitive drum by means of a charge corona. The laser paints an image onto the photosensitive drum, discharging the image areas to a much lower voltage (–100VDC). The developing roller in the toner cartridge has charged (–600VDC) toner stuck to it. As it rolls the toner toward the photosensitive drum, the toner is attracted to (and sticks to) the areas of the photosensitive drum that the laser has discharged. The image is then transferred from the drum to the paper at its line of contact by means of the corona wire (or corona roller) with a +600VDC charge. The static-eliminator strip removes the high, positive charge from the paper, and the paper, now holding the image, moves on. The paper then enters the fuser, where the fuser roller and the pressure roller make the image permanent. The paper exits the printer, and the printer starts printing the next page or returns to its ready state.

FIGURE 1.36 The EP print process



LED Printers

An LED printer uses a light-emitting diode instead of a laser. The LED isn't built into the toner cartridge; it's separate, so that when you replace the toner cartridge, all you get is new toner.

The LED printing process uses a row of small LEDs very close to the drum to expose it. Each LED is about the same size as the diameter of the laser beam used in a laser printer. Except for the writing stage, the operation is the same as the laser printing process.

LED printers are cheaper and smaller than lasers. However, they're considered lower-end printers, and they have a lower maximum dots per inch (dpi)—under 800dpi versus 1200 or more for a laser printer.

Other Printer Technologies

Besides the aforementioned technologies, you may see a question or two about several less popular ones on the A+ exam. They're all high-end color graphics printers designed for specialty professional usage:

Color Laser Works much like a regular laser printer except that it makes multiple passes over the page, one for each ink color. Consequently, the printing speed is rather low.

Thermal Wax Transfer A color nonimpact line printer that uses a solid, wax-like ink. A heater melts the wax and then sprays it onto the page, somewhat like an ink-jet. The quality is very high, but so is the price ($2,500 or so). However, the wax is cheaper per page than ink-jet ink. The quality is as good as a color laser, but the speed is much faster because it needs only one pass.

Dye Sublimation Another color nonimpact line printer. This one converts a solid ink into a gas that is then applied to the paper. Color is applied in a continuous tone, rather than individual dots, and the colors are applied one at a time. The ink comes on film rolls. The paper is very expensive, as is the ink. Print speeds are very low. The quality is extremely high.

Printer Interfaces

Besides understanding the printer's operation, for the exam you need to understand how these devices talk to a computer. An *interface* is the collection of hardware and software that allows the device to communicate with a computer. Each printer, for example, has at least one interface, but some printers have several, in order to make them more flexible in a multiplatform environment. If a printer has several interfaces, it can usually switch between them on the fly so that several computers can print at the same time.

Communication Types

When I say *communication types*, I'm talking about the hardware technologies involved in getting the information to and from the computer. There are seven major types:

Legacy Serial This is the traditional RS-232 serial port found on most PCs. The original printer interface on the earliest computers, it has fallen out of favor and is seldom used anymore for printing because it's so slow.

Legacy Parallel Until recently, the parallel port on a PC was the overwhelming favorite interface for connecting printers, to the point where the parallel port has become synonymous

with *printer port*. It sends data 8 bits at a time (in parallel) and uses a cable with a male DB-25 connector at the computer and a 36-bin Centronics male connector at the printer. Its main drawback is its cable length, which must be less than 10 feet.

Universal Serial Bus (USB) The most popular type of printer interface as this book is being written is the USB. It's the most popular interface for just about every peripheral. The benefit for printers is that it has a higher transfer rate than either serial or parallel and it automatically recognizes new devices. USB is also fully Plug and Play, and it allows several printers to be connected at once without adding ports or using up additional system resources.

Network Most large-environment printers (primarily laser and LED printers) have a special interface that allows them to be hooked directly to a network. These printers have a network interface card (NIC) and ROM-based software that let them communicate with networks, servers, and workstations.

The type of network interface used on the printer depends on the type of network the printer is being attached to. For example, if you're using a Token Ring network, the printer should have a Token Ring interface.

IEEE 1394/FireWire This is a high-speed serial alternative to USB. It's less commonly used for printers than USB is, but FireWire printer interfaces do exist.

Radio Wave Bluetooth is an infrared technology that can connect a printer to a computer at a range of about 35 feet, provided there is an unblocked line of sight.

Wireless A network-enabled printer that has a wireless adapter can participate in a wireless Ethernet (IEEE 802.11b, a, or g) network, just as it would as a wired network client.

Firmware Updates

Printers resemble computers in many ways. Like a computers, they can have their own motherboard, memory, and CPU. They also have firmware—that is, software permanently stored on a chip. If you're using an old computer with a new operating system, an update may be available for the printer's or scanner's firmware. You can find out that information at the printer or scanner manufacturer's website and download the update from there along with a utility program for performing the update.

Printer Configuration

To add a printer, whether it's local or networked, you start the Add Printer Wizard found in Windows by accessing Start ➢ Printers and Faxes (or Start ➢ Printers) and then choosing Add a Printer. Once the printer is installed, you can right-click its icon at any time beneath this dialog box and choose Properties from the context menu. From here, you can print a test page and configure such items as sharing, ports, device settings (including tray selection), and so on. Figure 1.37 shows the spooling options and the settings that allow you to configure the printer to be available only at certain times, and Figure 1.38 shows the tray settings.

FIGURE 1.37 Configure the advanced options.

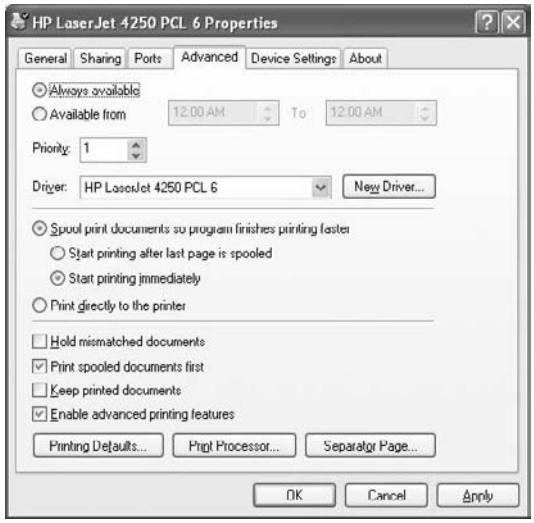
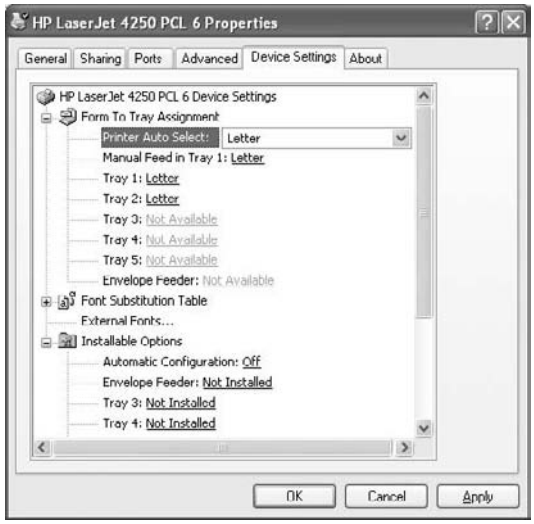


FIGURE 1.38 Configure the tray and other settings.



Exam Essentials

Know the common types of printers. Know and understand the types of printers, such as impact printers, ink-jet printers, and laser printers (page printers), as well as their interfaces and print media.

Know the fundamentals of scanners. Whereas printers are output devices, scanners can be thought of as input devices.

Understand the process of printing for each type of printer. Each type of printer puts images or text on paper. Understand the process that each type of printer uses to accomplish this task.

Know the specific components of each type of printer. Each type of printer uses similar components to print. Know the different components that make up each type of printer, and their jobs.

Understand the print process of a laser printer. You'll most likely be asked questions about certain processes of a laser printer. Know and understand the different steps that make up the print process of a laser printer.

Be familiar with the possible interfaces that can be used for printing. The seven types are legacy parallel, legacy serial, USB, network, IEEE 1394/FireWire, radio wave, and wireless.

Know how to install printers and scanners. The manufacturer is the best source of information about installing printers and scanners. You should, however, know about the wizards available in Windows as well.

Know to keep firmware up-to-date. Firmware updates can be found at the manufacturer's website and installed according to the instructions accompanying them.

Review Questions

1. What two types of expansion slots are found on all modern motherboards? What is a third, older type that might or might not also be present?
2. Name three features that distinguish an ATX motherboard from an AT motherboard.
3. What are PGA and SECC? Which of those types is the Socket 423 used with the Pentium 4?
4. What voltages does a typical power supply provide to the motherboard?
5. On modern systems, what is the relationship between a CPU's internal and external speeds?
6. Which cache is also known as the back-side cache?
7. What is the purpose of a VRM on a motherboard?
8. What is the purpose of a parity bit on a SIMM?
9. Would the POST test identify a problem with RAM?
10. If a legacy serial port is physically fine but does not show up in Windows' Device Manager, how might you enable it?

Answers to Review Questions

1. PCI and AGP. The third type is ISA.
2. Possible answers include: (1) position of CPU, (2) expansion slot orientation, (3) built-in ports on the side, (4) one-piece power supply connector, (5) physical size and shape of the motherboard, and (6) type of keyboard connector.
3. They are the two types of slots/sockets for CPUs in motherboards. PGA is the type with a grid of holes into which pins fit on a flat chip. SECC is the type that accepts a circuit board surrounded by a cartridge. Whenever you see *socket* in the name, it's always a PGA type. SECC types have *slot* in the name.
4. +5V, –5V, +12V, and –12V for all power supplies, plus +3.3V for an ATX power supply.
5. The internal speed is a multiple of the external speed.
6. The L2 cache.
7. To provide different voltages for different CPUs.
8. Error detection.
9. Yes. One of the components the POST checks is the RAM.
10. It may be disabled in BIOS Setup; try enabling it there.

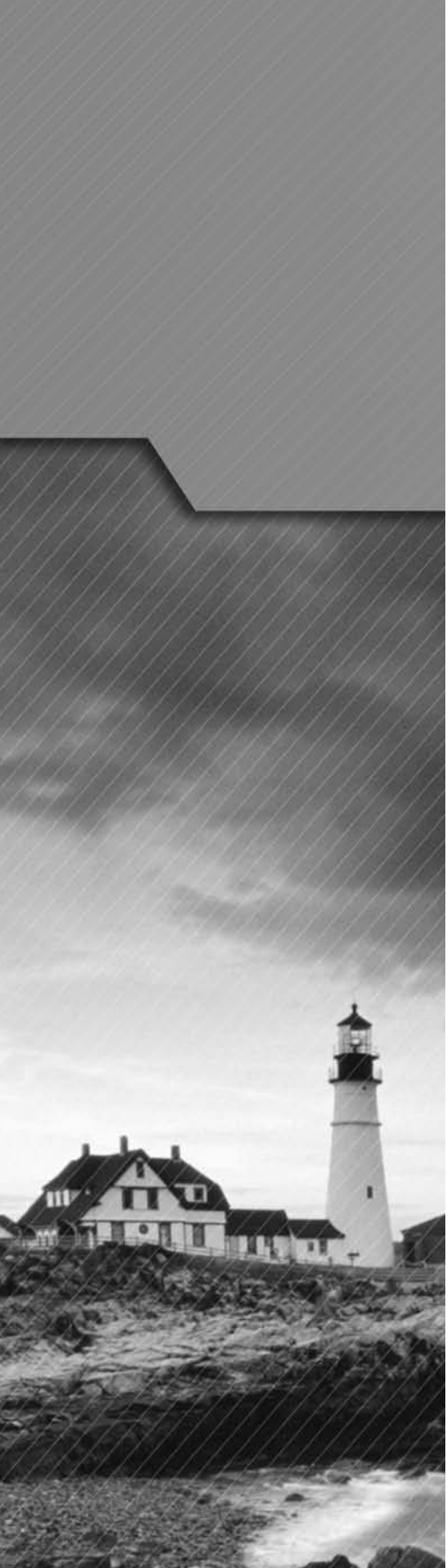
Chapter

2

Troubleshooting, Repair, and Maintenance

COMPTIA A+ ESSENTIALS EXAM OBJECTIVES COVERED IN THIS CHAPTER:

- ✓ **2.1 Given a scenario, explain the troubleshooting theory**
  - Identify the problem
    - Question user and identify user changes to computer and perform backups before making changes
  - Establish a theory of probable cause (question the obvious)
  - Test the theory to determine cause
    - Once theory is confirmed determine next steps to resolve problem
    - If theory is not confirmed re-establish new theory or escalate
  - Establish a plan of action to resolve the problem and implement the solution
  - Verify full system functionality and if applicable implement preventative measures
  - Document findings, actions, and outcomes
- ✓ **2.2 Given a scenario, explain and interpret common hardware and operating system symptoms and their causes**
  - OS related symptoms
    - Bluescreen
    - System lock-up
    - Input/output devices
    - Application install



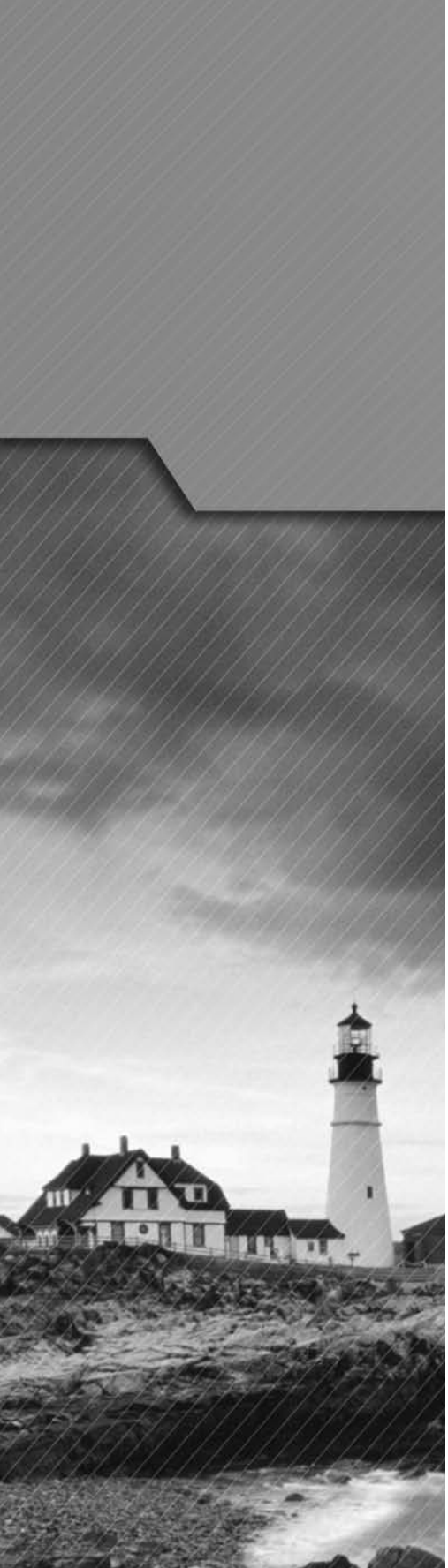
- Start or load
- Windows specific printing problems
  - Print spool stalled
  - Incorrect / incompatible driver
- Hardware related symptoms
  - Excessive heat
  - Noise
  - Odors
  - Status light indicators
  - Alerts
  - Visible damage (e.g. cable, plastic)
- User documentation and resources
  - User / installation manuals
  - Internet / web based
  - Training materials

✓ **2.3 Given a scenario, determine the troubleshooting methods and tools for printers**

- Manage print jobs
- Print spooler
- Printer properties and settings
- Print a test page

✓ **2.4 Given a scenario, explain and interpret common laptop issues and determine the appropriate basic troubleshooting method**

- Issues
  - Power conditions
  - Video
  - Keyboard
  - Pointer
  - Stylus
  - Wireless card issues



- Methods
  - Verify power (e.g. LEDs, swap AC adapter)
  - Remove unneeded peripherals
  - Plug in external monitor
  - Toggle FN keys or hardware switches
  - Check LCD cutoff switch
  - Verify backlight functionality and pixilation
  - Check switch for built-in WIFI antennas or external antennas

✓ **2.5 Given a scenario, integrate common preventative maintenance techniques**

- Physical inspection
- Updates
  - Driver
  - Firmware
  - OS
  - Security
- Scheduling preventative maintenance
  - Defrag
  - Scandisk
  - Check disk
  - Startup programs
- Use of appropriate repair tools and cleaning materials
  - Compressed air
  - Lint free cloth
  - Computer vacuum and compressors
- Power devices
  - Appropriate source such as power strip, surge protector or UPS
- Ensuring proper environment
- Backup procedures

Most of those employed in the IT field who will be seeking CompTIA's A+ certification are regularly in positions where they need to know how to troubleshoot, repair, and maintain computer systems. Given that, you may be tempted to breeze through this chapter. I would, however, encourage you not to do so simply because CompTIA wants you to know how they suggest approaching a problem as opposed to how you might currently do so. The five subobjectives in this category run the gamut from basic approach to specific knowledge, and many of these topics are touched on in other chapters as well.

The Basics of Troubleshooting

There is only one objective here, and it tests your ability to understand the prescribed diagnostic procedures. Be sure you know the steps delineated in the section "Diagnostic Procedures," as they are covered in the exam.

Critical Information

Both for the test and for real life, you should know how to recognize common problems with systems and make certain they're booting correctly. The sections that follow look at the diagnostic procedures that you should walk through when attempting to tackle a problem.

When it comes to diagnostic procedures with operating systems, you need to memorize the steps that CompTIA wants you to take as you approach the problem. Much of this approach carries over to other domains (and objectives) as well. Your approach to the problem should be as follows:

1. Identify the problem by questioning the user and identifying user changes to the computer. Before you do anything else, ask the user what the problem is, when the last time was that the problem didn't exist, and what has changed since then. Be sure that you do a backup before you make any changes so that all of your actions can be undone, if necessary.
2. Analyze the problem, including potential causes, and make an initial determination of whether it's a software and/or hardware problem. As you narrow down the problem, you need to determine whether it's hardware- or software-related so you can act accordingly.

3. Test related components, including connections and hardware/software configurations; use Device Manager; and consult vendor documentation. Whatever the problem may be, the odds are good that someone else has experienced it before. Use the tools at your disposal—including manuals and websites—to try to focus in on the problem as expeditiously as possible. If your theory is confirmed, then determine the next steps you need to take to resolve the problem. If your theory is not confirmed, then come up with a new theory, or bring in someone with more expertise (escalate the problem).
4. Evaluate the results, and take the additional steps (if needed) to fully resolve the problem. Keep in mind that it's possible that more than one thing is causing the problem. If that is the case, you may need to solve one problem and then turn your attention to the next.
5. When the problem is believed to be resolved, verify that the system is fully functional. If there are preventive measures that can be put in place to keep this situation from occurring, take those measures on this machine and all others where that vulnerability exists.
6. Document your activities and outcomes. Experience is a wonderful teacher, but only if you can remember what you've done. Documenting your actions and outcomes will help you (or a fellow admin) troubleshoot a similar problem when it crops up in the future.

Exam Essential

Be able to identify the diagnostic procedures. CompTIA wants you to take a systematic approach to the problem that helps you isolate the problem and quickly identify it. You should be able to list the given steps in order.

Common Symptoms and Causes

This is a catchall category that tests your ability to understand the boot sequence, use diagnostic procedures, recognize some common operational issues, explain a few error messages, and identify the names, locations, purposes, and characteristics of some common utilities that help technicians and experienced end users manage their systems.

Critical Information

Both for the test and for real life, you should know how to recognize common problems with systems and make certain they're booting correctly. The sections that follow look at a number of topics related to keeping your systems booting and running properly.

Common Operational Issues

There are a number of operational issues that you should be familiar with. Although CompTIA calls them "common," they're nowhere near as common as they were in the

past. Each successive release of the Windows OS and service packs has reduced the frequency of these operational conditions from occurring, to the point where many of them are on the verge of extinction.

Blue Screens

Once a regular occurrence when working with Windows, blue screens (also known as the Blue Screen of Death) have become much less frequent. Occasionally, systems will lock up, and you can usually examine the log files to discover what was happening when this occurred and then take the steps necessary to correct it. For example, if you see that a driver or application was loading before the crash, you can begin to isolate it as a possible problem.

In more recent versions of Windows (XP and Vista), information from such crashes is written to XML files by the operating system. When the system becomes stable, a prompt usually appears asking approval to send this information to Microsoft. The goal that Microsoft has in collecting this data is to be able to identify drivers that cause such problems and work with vendors to correct these issues.

System Lockup

The difference between a blue screen and a system lockup is whether the dump message that accompanies a blue screen is present. With a regular lockup, things just stop working. As with blue screens, these have been greatly reduced with more recent versions of Microsoft operating systems (a notable exception may occur with laptops, which go to hibernate and then occasionally do not want to exit this mode). If they occur, you can examine the log files to discover what was happening (such as a driver loading) and take steps to correct it.

Input/Output Device

Errors can occur with devices such as keyboards, printers, and mice. Often, those problems are caused by the hardware—or connections—and can be readily identified. Issues with the software are generally related to the drivers.

Application Failures

If applications fail to install, start, or load, you should examine the log files associated with them to try to isolate the problem. Many applications write logs that can be viewed with Event Viewer (choose Application Logs); others (mostly legacy) write to text files that you can find in their own directories.

Common troubleshooting steps include closing all other applications and then starting the malfunctioning application to see if there is a conflict with other applications, reinstalling the malfunctioning application, and installing and running the problem application on another machine to see if it works properly on another system.

Start/Load Problems

Boot problems can occur with corruption of the boot files or missing components (such as the NTLDR file being “accidentally” deleted by an overzealous user). Luckily, during the

installation of the OS, log files are created in the `%SystemRoot%` or `%SystemRoot%\Debug` folder (`C:\WINNT` and `C:\WINNT\DEBUG`, by default). If you have a puzzling problem, look at these logs to see if you can find error entries there. These are primarily helpful during installation. For routine troubleshooting, we activate boot logging by selecting Enable Boot Logging from the Windows Advanced Options menu to create an ntbtlog.txt in the %systemroot% folder.

During startup, problems with devices that fail to be recognized properly, services that fail to start, and so on, are written to the system log and can be viewed with Event Viewer. This utility provides information about what's been going on system-wise, to help you troubleshoot problems. Event Viewer shows warnings, error messages, and records of things happening successfully. It's found only in NT versions of Windows. You can access it through Computer Management, or you can access it directly from the Administrative Tools in Control Panel.

Printing Problems

Most printing problems today are due to either improper configuration or actual physical problems with the printer. The Windows architecture is such that when a client wants to print to a network printer, a check is first done to see if the client has the latest printer driver. If it doesn't—as judged by the print server—the new driver is sent from the server to the client, and then the print job is accepted. This is an enormous help to the administrator; when a new driver comes out, all the administrator must do is install it on the server, and the distribution to the clients becomes automatic.

Errors occur when a client is configured with a printer different from the one in use. For example, suppose the network has an ABC 6200 printer, but you don't see that among the list of choices when you install the printer on the client. Rather than taking the time to get the correct driver, you choose the ABC 6000, because you've been told that it's compatible. All will work well in this scenario until a new driver is released and loaded on the server. This client won't update (while all others configured with 6200 will), and thus there is the potential for printing problems to occur.

Another problem area is the print spooler: the queue print jobs go into and come out of as they are sent to the printer. There are times when a job will get stuck and appear in the spool even though nothing is printing. This becomes a real problem when the stuck job keeps other submitted jobs from making it to the printer. When this happens, follow these steps:

1. Stop the spooler. There are a number of ways to do this, but the easiest is to type `net stop spooler` at a command prompt. You can also stop the spooler using the Services applet in Computer Management.
2. Delete files beneath `C:\Windows\System32\Spool and C:\Windows\System32\Spool\Printers`. Delete only files, not folders.
3. Restart the spooler. Again, there are a number of ways to do this, but the easiest is to type **`net start spooler`** at a command prompt.

You can solve most other problems using the Printing Troubleshooter (choose Start ➢ Help And Support, and type in **Printing Troubleshooter**). It will walk you through solving individual printing problems.

Hardware Problem Symptoms

While problems can occur with the operating system with little or no physical warning, that is rarely the case when it comes to hardware problems. Your senses will often alert you that something is wrong based on what you hear, smell, or see. The following symptoms are those that CompTIA asks you to be familiar with:

Excessive Heat Under normal conditions, the PC cools itself by pulling air in. That air is used to dissipate the heat created by the processor (and absorbed by the heat sink). When airflow is restricted by clogged ports, a bad fan, and so forth, heat can build up inside the unit and cause problems, with chip creep—the unseating of components—one of the more common.

Since the air is being pulled in to the machine, excessive heat can originate from outside the PC as well, due to a hot working environment. The heat can be pulled in and cause the same problems. Take care to keep the ambient air within normal ranges (approximately 60–90 degrees Fahrenheit) and at a constant temperature.

Noise When it comes right down to it, there are not a lot of moving parts within a PC. When you hear noise, you can begin to readily narrow down the possible culprits. The most common are the fan and the hard drive. No matter what is responsible, you will want to take immediate steps to shut down the machine and start the replacement process.

Odors Odor can be caused by heat or a device going bad; the most common source is the fan. When it is the fan, the smell that is released in the air often resembles cheap hair spray. When you smell an odor, immediately take steps to shut down the machine and try to identify the source of the problem.

Status-Light Indicators Status lights are often found on the (Network Interface Card) as well as on the front of a desktop model and in the display area of a laptop. On the NIC, a display other than a green light can indicate that there are problems with the network; more important, though, the lack of any light can indicate that the card itself has gone bad.

Alerts The operating system communicates with the hardware through the Hardware Abstraction Layer (HAL). In the Windows operating systems, the best interface to this from an alert standpoint is Event Viewer, which will log alerts and errors and often provide some insight into possible causes. Once you know where the problems are, Device Manager becomes a great tool for interacting with the hardware.

Visible Damage Never discount the ability to look at a PC or networking component and recognize that something may be wrong. Just noting that something does not look right can be a great way to identify a problem, or potential problem, that needs to be addressed. The visible damage can range from the blackened back of a fan, telling you that it has burned up, to bare areas on a networking cable, and everything in between.

Documentation and Resources

When dealing with a problem—whether hardware- or software-related—one of the first places you should turn is to a resource where similar problems have occurred and solutions documented. That documentation can be in the form of your own notes or from the

vendor's manuals or websites. You can also find many solutions in study guides, training manuals, and related material.

Regardless of where you find the information that helps you solve the problem, one thing you must always do is document that solution and the steps you walked through in case you, or another administrator, are faced with the same issue in the future.

Exam Essential

Be able to troubleshoot common problems. CompTIA wants you to understand the importance of the log files in the troubleshooting process. These files can hold keys that help you identify what was going on when a problem occurred, whether that problem is a blue screen, an application crash, or anything similar.

Common Printer Problems

Not only does troubleshooting appear on the test, but you may have to accomplish these tasks on a daily basis, depending on your environment. Your ability to get a down printer working will make you more valuable to your employer.

Critical Information

In the real world, you'll find that a large portion of all service calls relate to printing problems. This section will give you some general guidelines and common printing solutions to resolve printing problems.

Managing Print Jobs

Most people know how to send a job to the printer. Clicking on File, then Print, or pressing Ctrl+P on your keyboard generally does the trick. But once the job gets sent to the printer, what do you do if it doesn't print?

When you send a job to the printer, that print job ends up getting in a line with all other documents sent to that printer. The line of all print jobs is called the *print queue*. In most cases, the printer will print jobs on a first-come, first-serve basis. (There are exceptions, but we'll cover those in the next section, "Configuring Printer Properties and Settings.") Once you send the job to the printer, a small printer icon will appear in the system tray in the lower-right corner of your desktop, near the clock. By double-clicking on the icon (or by right-clicking on it and selecting the printer name), you will end up looking at the jobs in the print queue.

From the menu, you can pause, resume, restart, and cancel print jobs, as well as see properties of the selected print job. If you wanted to pause or cancel all jobs going to a printer, you would do that from the Printer menu.

The *print spooler* is a service that formats print jobs in the language that the printer needs. Think of it as a holding area where the print jobs are prepared for the printer. In Windows the spooler is a service that's started automatically when Windows loads.

Configuring Printer Properties and Settings

Where you configure specific printer properties depends a lot on the printer itself, but the most common interface is the Printers And Faxes window. On the left-hand side under Printer Tasks in this interface is an option to select printing preferences and another option to set printer properties (in addition, both options can be executed by right-clicking on the printer and choosing Printing Preferences or Properties, respectively). Various configuration features can be set from each menu option.

Under Printing Preferences (for a printer), you can select the quality of the print job, layout (portrait or landscape), paper size, two-sided printing, and use of color. On the printer's Properties screen, the options are different. The printer's Properties screen is less about how the printer does its job and more about how people can access the printer. Using the printer properties, you can share the printer, set up the port that it's on, and configure when the printer will be available throughout the day (and to which specific users).

On the Advanced tab, you can configure the printer to be available only during certain hours of the day. This might be useful if you're trying to curtail after-hours printing of non-work-related documents, for example. Configuring a printer priority lets you insert higher-priority jobs in front of lower-priority ones, based on the printer they're sent to. You can also configure the spool settings. I recommend that you always spool the jobs instead of printing directly to the printer. However, if the printer is printing garbage, you can try printing directly to it to see if the spooler is causing the problem.

The Printing Defaults button takes you to the Printing Preferences, and Print Processor lets you select alternate methods of processing print jobs (which usually are not needed). Separator Page lets you specify a file to use as a separator page (a document that prints out at the beginning of each separate print job, usually with the user's name on it), which can be useful if you have several (or several dozen) users sharing one printer.

Printing a Test Page

If your printer isn't spitting out print jobs, it may be a good idea to print a test page and see if that works. The test page information is stored in the printer's memory, so there's no formatting or translating of jobs required. It's simply a test to make sure your printer hears your computer. In addition to the Windows Print Test Page button, try the built-in test function on the printer if your printer has such. While going through Windows tests the driver and connectivity, printing directly at the printer tests the print device itself.

When you install a printer, one of the last questions it asks you is if you want to print a test page. If there's any question, go ahead and do it. If the printer is already installed, you can print a test page from the printer Properties window. Just click the Print Test Page button and it should work. If nothing happens, double-check your connections and stop and restart the print spooler. If garbage prints, there is likely a problem with the printer's memory or the print driver.

Printer Driver Issues

Many problems with a printer that won't work with the operating system or that prints the wrong characters can be traced to problems with its software. Computers and printers can't talk to each other by themselves. They need interface software to translate software commands into commands the printer can understand.

For a printer to work with a particular operating system, a driver must be installed for it. This driver specifies the *page description language (PDL)* the printer understands, as well as information about the printer's characteristics (paper trays, maximum resolution, and so on). For laser printers, there are two popular PDLs: Adobe PostScript (PS) and Hewlett-Packard Printer Control Language (PCL). Almost all laser printers use one or both of these.

If the wrong printer driver is selected, the computer will send commands in the wrong language. If that occurs, the printer will print several pages of garbage (even if only one page of information was sent). This "garbage" isn't garbage at all, but the printer PDL commands printed literally as text instead of being interpreted as control commands.

Although HP doesn't recommend using any printer driver other than the one designed for the specific printer, in some cases you can increase the printing performance (speed) of HP LaserJet and DeskJet printers by using older drivers that don't support the newer high-definition printing. I have also had cases where software packages would not function with newer HP drivers. To increase speed or correct printing problems with HP LaserJet printers, follow this rule of thumb: if you're using a 5-series printer (5Si), try a 4-series driver; if that doesn't work, reduce the driver by one series. If a LaserJet III doesn't work, try the LaserJet driver, which should be last on your list of the default drivers built into Windows. In 90 percent of cases, this driver will fix printing problems with some applications.

Memory Errors

A printer can have several types of memory errors. The most common is insufficient memory to print the page. Sometimes you can circumvent this problem by doing any of the following:

- Turn off the printer to flush out its RAM, and then turn it back on and try again.
- Print at a lower resolution. (Adjust this setting in the printer's properties in Windows.)
- Change the page being printed so it's less complex.
- Try a different printer driver if your printer supports more than one PDL. (For example, try switching from PostScript to PCL, or vice versa.) Doing so involves installing another printer driver.
- Upgrade the memory, if the printer allows.

Printer Hardware Troubleshooting

This section covers the most common types of hardware printer problems you'll run into. We'll break the information into three areas, for the three main types of printers in use today.

Dot-Matrix Printer Problems

Dot-matrix printers are relatively simple devices. Therefore, only a few problems usually arise. We'll cover the most common problems and their solutions here.

Low Print Quality Problems with print quality are easy to identify. When the printed page comes out of the printer, the characters may be too light or have dots missing from them. Table 2.1 details some of the most common print-quality problems, their causes, and their solutions.

TABLE 2.1 Common Dot-Matrix Print-Quality Problems

Characteristics	Cause	Solution
Consistently faded or light characters	Worn-out print ribbon	Replace ribbon with a new, vendor-recommended ribbon.
Print lines that go from dark to light as the printhead moves across the page	Print ribbon advance gear slipping	Replace ribbon advance gear or mechanism.
A small, blank line running through a line of print (consistently)	Printhead pin stuck inside the printhead	Replace the printhead.
A small, blank line running through a line of print (intermittently)	A broken, loose, or shorting printhead cable, or a sticking printhead	Secure or replace the printhead cable. Replace or clean the printhead.
A small, dark line running through a line of print	Printhead pin stuck in the out position	Replace the printhead. (Pushing in the pin may damage the printhead.)
Printer makes a printing noise, but no print appears on the page	Worn, missing, or improperly installed ribbon cartridge, or the printhead gap set too large	Replace the ribbon cartridge correctly, or adjust the printhead gap.
Printer prints garbage	Cable partially unhooked, wrong driver selected, or a bad printer control board (PCB)	Hook up the cable correctly, select the correct driver, or replace the PCB (respectively).

Printout Jams Inside the Printer A paper jam happens when something prevents the paper from advancing through the printer evenly. Print jobs jam for two major reasons: an obstructed paper path or stripped drive gears.

An obstructed paper path is often difficult to find. Usually it means disassembling the printer to find the bit of paper or other foreign substance that's blocking the paper path. A common obstruction is a piece of the *perf*—the perforated sides of tractor-feed paper—that has torn off and gotten crumpled up and then lodged into the paper path. It may be necessary to remove the platen roller and feed mechanism to get at the obstruction.

Stepper Motor Problems A *stepper motor* is a motor that can move in very small increments. Printers use stepper motors to move the printhead back and forth as well as to advance the paper (these are called the *carriage motor* and *main motor*, respectively). These motors get damaged when they're forced in any direction while the power is on. This includes moving the printhead over to install a printer ribbon, as well as moving the paper-feed roller to align paper. These motors are very sensitive to stray voltages. And, if you're rotating one of these motors by hand, you're essentially turning it into a small generator, thereby damaging it!

A damaged stepper motor is easy to detect. Damage to the stepper motor will cause it to lose precision and move farther with each step. Lines of print will be unevenly spaced if the main motor is damaged (which is more likely). Characters will be scrunched together if the printhead motor goes bad. If the motor is bad enough, it won't move at all in any direction; it may even make high-pitched squealing noises. If any of these symptoms show themselves, it's time to replace one of these motors. Stepper motors are usually expensive to replace—about half the cost of a new printer. However, because dot-matrix printers are old technology and difficult to find, you may have no choice but to replace the motor if the printer is essential and is no longer available new.

Ink-Jet Printers

Ink-jet printers are the most commonly sold printers for home use. For this reason, you need to understand the most common problems with ink-jet printers so your company can service them effectively.

Bubble-Jet Printers

Bubble-jet printers are very similar to ink-jet with the exception that there is a small heater used to heat the ink. Once heated, the ink drops are ejected through the printer nozzle. A printhead has between 64 and 128 nozzles, each of which is capable of firing heated droplets simultaneously.

Print Quality

The majority of ink-jet printer problems are quality problems. Ninety-nine percent of these can be traced to a faulty ink cartridge. With most ink-jet printers, the ink cartridge contains the printhead and the ink. The major problem with this assembly can be described by, "If you don't use it, you lose it." The ink will dry out in the small nozzles and block them if they aren't used at least once a week.

An example of a quality problem is when thin blank lines or colored stripes appear on the page. This is caused by a plugged hole in at least one of the small, pinhole ink nozzles in the print cartridge. Replacing the ink cartridge solves this problem easily. You may also be able to clear the clogged ink jet by running the printer's cleaning routine, either by pressing buttons on the printer or by issuing a command through the printer's driver in Windows.

If an ink cartridge becomes damaged or develops a hole, it can put too much ink on the page, and the letters will smear. Again, the solution is to replace the ink cartridge. (However, a very small amount of smearing is normal if the pages are laid on top of each other immediately after printing.) Because damage is possible in the process you need to be careful when refilling cartridges, and many manufacturers do not suggest using refilled cartridges at all.

One final print-quality problem that doesn't directly involve the ink cartridge is characterized by the print quickly going from dark to light and then to nothing. As we already mentioned, ink cartridges dry out if not used. That's why the manufacturers include a small suction pump inside the printer that primes the ink cartridge before each print cycle. If this priming pump is broken or malfunctioning, this problem will manifest itself, and the pump will need to be replaced.

If the problem of the ink quickly going from dark to light and then disappearing ever happens to you, and you really need to print a couple of pages, try this trick. Take the ink cartridge out of the printer. Squirt some window cleaner on a paper towel, and gently tap the printhead against the wet paper towel. The force of the tap plus the solvents in the window cleaner should dislodge any dried ink, and the ink will flow freely again.

Paper Jams

Ink-jet printers usually have simple paper paths. Therefore, paper jams due to obstructions are less likely. They're still possible, however, so an obstruction shouldn't be overlooked as a possible cause of jamming.

Paper jams in ink-jet printers are usually due to one of two things:

- A worn pickup roller
- The wrong type of paper

The pickup roller usually has one or two D-shaped rollers mounted on a rotating shaft. When the shaft rotates, one edge of the D rubs against the paper, pushing it into the printer. When the roller gets worn, it becomes smooth and doesn't exert enough friction against the paper to push it into the printer.

If the paper used in the printer is too smooth, it causes the same problem. Pickup rollers use friction, and smooth paper doesn't offer much friction. If the paper is too rough, on the other hand, it acts like sandpaper on the rollers, wearing them smooth. Here's a rule of thumb for paper smoothness: paper slightly smoother than a new dollar bill will work fine.

Laser and Page Printers

Most of the problems with laser printers can be diagnosed with knowledge of the inner workings of the printer and a little common sense.

Paper Jams

Laser printers today run at copier speeds. As a result, their most common problem is paper jams. Paper can get jammed in a printer for several reasons. First, feed jams happen when the paper feed rollers get worn (similar to feed jams in ink-jet printers). The solution to this problem is easy: replace the worn rollers.

If your paper-feed jams are caused by worn pickup rollers, there is something you can do to get your printer working while you're waiting for the replacement pickup rollers. Scuff the feed roller(s) with a pot scrubber pad (or something similar) to roughen up the feed rollers. This trick works only once. After that, the rollers aren't thick enough to touch the paper.

Another cause of feed jams is related to the drive of the pickup roller. The drive gear (or clutch) may be broken or have teeth missing. Again, the solution is to replace it. To determine if the problem is a broken gear or worn rollers, print a test page, but leave the paper tray out. Look into the paper feed opening with a flashlight, and see if the paper pickup roller(s) are turning evenly and don't skip. If they turn evenly, the problem is more than likely worn rollers.

Worn exit rollers can also cause paper jams. These rollers guide the paper out of the printer into the paper-receiving tray. If they're worn or damaged, the paper may catch on its way out of the printer. These types of jams are characterized by a paper jam that occurs just as the paper is getting to the exit rollers. If the paper jams, open the rear door and see where the paper is. If the paper is very close to the exit roller, the exit rollers are probably the problem.

The solution is to replace all the exit rollers. You must replace all of them at the same time, because even one worn exit roller can cause the paper to jam. Besides, they're inexpensive. Don't be cheap and skimp on these parts if you need to have them replaced.

Paper jams can be the fault of the paper. If your printer consistently tries to feed multiple pages into the printer, the paper isn't dry enough. If you live in an area with high humidity, this could be a problem. I've heard some solutions that are pretty far out but that work (like keeping the paper in a Tupperware-type airtight container or microwaving it to remove moisture). The best all-around solution, however, is humidity control and to keep the paper wrapped until it's needed. Keep the humidity around 50 percent or lower (but above 25 percent if you can, in order to avoid problems with electrostatic discharge).

Finally, a metal, grounded strip called the *static eliminator strip* inside the printer drains the corona charge away from the paper after it has been used to transfer toner from the EP cartridge. If that strip is missing, broken, or damaged, the charge will remain on the paper and may cause it to stick to the EP cartridge, causing a jam. If the paper jams after reaching the corona assembly, this may be the cause.

Blank Pages

Blank pages are a somewhat common occurrence in laser and page printers. Somehow, the toner isn't being put on the paper. The toner cartridge is the source for most quality problems, because it contains most of the image-formation pieces for laser and page printers. Let's start with the obvious. A blank page will come out of the printer if there is no toner in the toner cartridge. It's easy to check: just open the printer, remove the toner cartridge, and gently shake it. You'll be able to hear if there's toner inside the cartridge. If it's empty, replace it with a known, good, manufacturer-recommended toner cartridge.

Another issue that crops up rather often is the problem of using refilled or reconditioned toner cartridges. During their recycling process, these cartridges may be filled with the wrong kind of toner (for example, one with an incorrect charge). This may cause toner to be repelled from the EP drum instead of attracted to it. Thus, there's no toner on the page because there was no toner on the EP drum to begin with. The solution is to replace the toner cartridge with the type recommended by the manufacturer.

A third problem related to toner cartridges happens when someone installs a new toner cartridge and forgets to remove the sealing tape that is present to keep the toner in the cartridge during shipping. The solution to this problem is as easy as it is obvious: remove the toner cartridge from the printer, remove the sealing tape, and reinstall the cartridge.

Another cause of blank pages is a damaged or missing corona wire. If a wire is lost or damaged, the developed image won't transfer from the EP drum to the paper. Thus, no image appears on the printout. To determine if this is causing your problem, do the first half of the self-test. If there is an image on the drum but not on the paper, you'll know that the corona assembly isn't doing its job.

To check whether the corona assembly is causing the problem, open the cover and examine the wire (or roller, if your printer uses one). The corona wire is hard to see, so you may need a flashlight. You'll know if it's broken or missing just by looking (it will either be in pieces or just not there). If it's not broken or missing, the problem may be related to the high-voltage power supply (HVPS). The corona wire (or roller) is a relatively inexpensive part and can be easily replaced with some patience and the removal of two screws.

The HVPS supplies high-voltage, low-current power to both the charging and transfer corona assemblies in laser and page printers. If it's broken, neither will work properly. If the self-test shows an image on the drum but none on the paper, and the corona assembly is present and not damaged, then the HVPS is at fault.

All-Black Pages

This happens when the charging unit (the charge corona wire or charge corona roller) in the toner cartridge malfunctions and fails to place a charge on the EP drum. Because the drum is grounded, it has no charge. Anything with a charge (like toner) will stick to it. As the drum rotates, all the toner will be transferred to the page, and a black page will form.

This problem wastes quite a bit of toner, but it can be fixed easily. The solution (again) is to replace the toner cartridge with a known, good, manufacturer-recommended one. If that doesn't solve the problem, then the HVPS is at fault (it's not providing the high voltage the charge corona needs to function).

Repetitive Small Marks or Defects

Repetitive marks occur frequently in heavily used (as well as older) laser printers. The problem may be caused by toner spilled inside the printer. It can also be caused by a crack or chip in the EP drum (this mainly happens with recycled cartridges). These cracks can accumulate toner. In both cases, some of the toner will get stuck onto one of the rollers. Once this happens, every time the roller rotates and touches a piece of paper, it will leave toner smudges spaced a roller circumference apart.

The solution is simple: clean or replace the offending roller. To help you figure out which roller is causing the problem, the service manuals contain a chart. To use the chart, place the printed page next to the chart. Align the first occurrence of the smudge with the top arrow. The next smudge will line up with one of the other arrows. The arrow it lines up with tells you which roller is causing the problem.

Vertical Black Lines on the Page

A groove or scratch in the EP drum can cause the problem of vertical black lines running down all or part of the page. Because a scratch is lower than the surface, it doesn't receive as much (if any) of a charge as the other areas. The result is that toner sticks to it as though it were discharged. Because the groove may go around the circumference of the drum, the line may go all the way down the page.

Another possible cause of vertical black lines is a dirty charge corona wire. A dirty charge corona wire prevents a sufficient charge from being placed on the EP drum. Because the EP drum has almost zero charge, toner sticks to the areas that correspond to the dirty areas on the charge corona wire.

The solution to the first problem is, as always, to replace the toner cartridge (or EP drum, if your printer uses a separate EP drum and toner). You can also solve the second problem with a new toner cartridge, but in this case that would be an extreme solution. It's easier to clean the charge corona with the brush supplied with the cartridge.

Vertical White Lines on the Page

Vertical white lines running down all or part of the page are relatively common problems on older printers, especially ones that see little maintenance. They're caused by foreign matter (more than likely toner) caught on the transfer corona wire. The dirty spots keep the toner from being transmitted to the paper (at those locations, that is), with the result that streaks form as the paper progresses past the transfer corona wire.

The solution is to clean the corona wires. Some printers come with a small corona-wire brush to help in this procedure. To use it, remove the toner cartridge and run the brush in the charge corona groove on top of the toner cartridge. Replace the cartridge and use the brush to brush away any foreign deposits on the transfer corona. Be sure to put it back in its holder when you're finished.

Image Smudging

If you can pick up a sheet from a laser printer, run your thumb across it, and have the image come off on your thumb, then you have a fuser problem. The fuser isn't heating the toner

and fusing it into the paper. This could be caused by a number of things—but all of them can be taken care of with a fuser replacement. For example, if the halogen light inside the heating roller has burned out, that will cause the problem. The solution is to replace the fuser. The fuser can be replaced with a rebuilt unit, if you prefer. Rebuilt fusers are almost as good as new fusers, and some even come with guarantees. Plus, they cost less.

The whole fuser may not need to be replaced. You can order fuser components from parts suppliers and then rebuild them. For example, if the fuser has a bad lamp, you can order a lamp and replace it in the fuser.

Another, similar problem happens when small areas of smudging repeat themselves down the page. Dents or cold spots in the fuser heat roller cause this problem. The only solution is to replace either the fuser assembly or the heat roller.

Ghosting

Ghosting means you can see light images of previously printed pages on the current page. This is caused by one of two things: bad erasure lamps or a broken cleaning blade. If the erasure lamps are bad, the previous electrostatic discharges aren't completely wiped away. When the EP drum rotates toward the developing roller, some toner sticks to the slightly discharged areas. A broken cleaning blade, on the other hand, causes old toner to build up on the EP drum and consequently present itself in the next printed image.

Replacing the toner cartridge solves the second problem. Solving the first problem involves replacing the erasure lamps in the printer. Because the toner cartridge is the least expensive cure, you should try that first. Usually, replacing the toner cartridge will solve the problem. If it doesn't, you'll then have to replace the erasure lamps.

Printer Prints Pages of Garbage

This has happened to everyone at least once. You print a 1-page letter, and 10 pages of what looks like garbage come out of the printer. This problem comes from either the print-driver software or the formatter board:

Printer Driver The correct printer driver needs to be installed for the printer you have. For example, if you have an HP LaserJet III, then that is the driver you need to install. Once the driver has been installed, it must be configured for the correct page-description language: PCL or PostScript. Most HP LaserJet printers use PCL (but can be configured for PostScript). Determine what page description your printer has been configured for, and set the print driver to the same setting. If this isn't done, you'll get garbage out of the printer.

Most printers with LCD displays indicate that they're in PostScript mode with *PS* or *PostScript* somewhere in the display.

If the problem is the wrong driver setting, the garbage the printer prints looks like English. That is, the words are readable, but they don't make any sense.

Formatter Board The other cause of several pages of garbage being printed is a bad formatter board. This circuit board takes the information the printer receives from the computer and turns it into commands for the various components in the printer. Problems with the formatter board generally produce wavy lines of print or random patterns of dots on the page.

It's relatively easy to replace the formatter board in a laser printer. Usually this board is installed underneath the printer and can be removed by loosening two screws and pulling the board out. Typically, replacing the formatter board also replaces the printer interface, which is another possible source of garbage printouts.

Problems with Consumables

Just as it's important to use the correct printer interface and printer software, you must use the correct printer supplies. These supplies include the print media (what you print on) and the consumables (what you print with). The quality of the final print job has a great deal to do with the print supplies.

Paper

Most people don't give much thought to the kind of paper they use in their printers. It's a factor that can have a tremendous effect on the quality of the hard-copy printout, however, and the topic is more complex than people think. For example, if the wrong paper is used (for example, it's too thick for your printer), it can cause the paper to jam frequently and possibly even damage components.

The way that you install the paper on a laser printer can determine whether you end up with a curl in it. Sometimes the arrow on the package really does matter.

Transparencies

Transparencies are still used for presentations made with overhead projectors, even with the explosion of programs like Microsoft PowerPoint and peripherals like LCD computer displays, both of which let you show a whole roomful of people exactly what's on your computer screen. PowerPoint has an option to print slides, and you can use any program to print anything you want on a transparent sheet of plastic or vinyl for use with an overhead projector. The problem is, these "papers" are *exceedingly* difficult for printers to work with. That's why special transparencies were developed for use with laser and ink-jet printers.

Each type of transparency was designed for a particular brand and model of printer. Again, check the printer's documentation to find out which type of transparency works in that printer. Don't use any other type of transparency.

Never run transparencies through a laser printer without first checking to see if they're the type recommended by the printer manufacturer. The heat from the fuser will melt most other transparencies, and they will wrap themselves around it. It's impossible to clean a fuser after this has happened. The fuser will have to be replaced. *Use only the transparencies that are recommended by the printer manufacturer.*

Ink, Toner, or Ribbon

Besides print media, other things in the printer run out and need to be replenished. These items are the print consumables. Most consumables are used to form the images on the print media. Printers today use two main types of consumables: ink and toner.

To avoid problems relating to the ink, toner, or ribbon, use only brand-new supplies from reputable manufacturers. Don't use remanufactured or refilled cartridges.

Cleaning Pads

Some toner cartridges come with a cleaning pad. It's a long, thin strip of felt mounted on a piece of plastic. If a toner cartridge includes one, then somewhere inside the printer is a dirty felt pad that needs to be swapped out with the new one. Failing to do this when you change toner cartridges can cause problems.

Environmental Issues for Printers

Just like computers, printers can suffer from operating in an inhospitable environment such as one that is extreme in temperature or very dusty or smoky. Printers work best in a cool, clean environment where the humidity is between 50 and 80 percent.

Exam Essentials

Know the common printing problems listed. Understand the most common problems that occur in an environment.

Know the possible fixes for the common problem types. Each type of printer has its own common issues. Be familiar with the most likely repair options for each common problem.

Know how to select good-quality, appropriate consumables. Using appropriate paper and new (not remanufactured) toner, ink, or ribbon can prevent many problems.

Common Laptop Issues

Most of the tools used in diagnostics and troubleshooting are the same in the laptop world as in the desktop world, with few exceptions. This section looks at tools (many are just approaches to what is already there) you can use to work with laptops.

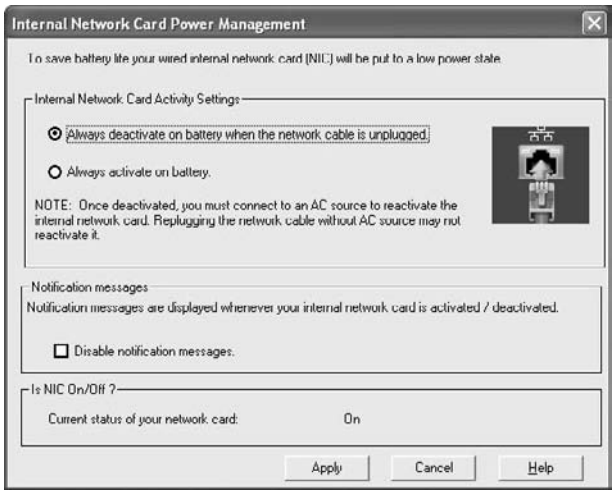
Critical Information

To solve a problem with a laptop or portable device (these terms are mostly used interchangeably by CompTIA), you should fully understand the hardware you're working with. The following list describes the items that CompTIA wants you to be comfortable with for this objective. Some may seem like common sense, in which case you should have no difficulty choosing the correct answer for questions about them on the exam:

AC Power In the absence of AC power, the laptop will attempt to run off the battery. This solution is good for a time, but AC power must be available to keep the battery charged and the laptop running. Most laptops have an indicator light showing whether AC power is being received, and the AC cord typically has an indicator light on it as well to show that it's receiving power. If no lights are lit on the cord or the laptop indicating that AC power is being received, try a different outlet or a different cord.

The presence of AC can affect the action of the NIC. To conserve power, the NIC is often configured not to be active when running on DC power (see Figure 2.1). You can access this dialog box through Start ➢ Control Panel ➢ Internal NIC Configuration.

FIGURE 2.1 The NIC can be disabled when running on DC to conserve battery life.



Stylus Issues A stylus may no longer work on a tablet computer due to damage or excessive wear. When this occurs, you can purchase inexpensive replacement styluses for most units.

Antenna Wires Most laptops today include an internal wireless card. This is convenient, but it can be susceptible to interference (resulting in a low signal strength) between the laptop and the access point. Do what you can to reduce the number of items blocking the signal between the two devices, and you'll increase the strength of the signal.

WiFi Switch Rather than having antennas draping from laptops, most laptops now include WiFi capabilities. One potential issue that can occur is a user accidentally toggling the switch that disables WiFi and then being unable to access a network. Depending on the laptop's manufacturer and model, this switch may be toggled by using one of the Fn key combinations, or by touching one of the lighted switches. As soon as a laptop user reports that they cannot access any network, this should be one of the first items you check.

Backlight Functionality The *backlight* is the light in the PC that powers the LCD screen. It can go bad over time and need to be replaced, and it can also be held captive by the inverter. The *inverter* takes the DC power the laptop is providing and boosts it up to AC to run the backlight. If the inverter goes bad, you can replace it on most models (it's cheaper than the backlight).

DC Power The biggest issue with DC power is the battery's inability to power the laptop as long as it should. This can be caused if the battery builds up a *memory* and thus doesn't offer a full charge. If a feature is available to fully drain the battery, you should use it to eliminate the memory (letting the laptop run on battery on a regular basis greatly helps). If you can't drain the battery and eliminate the memory, you should replace the battery.

External Monitors External monitors may be connected to the laptop directly or through a docking station. If you have an external monitor connected before you boot the laptop, many laptops automatically detect it and send the display there. If you connect after the laptop is booted, you should use the appropriate Fn key to send the display to the monitor.

Keyboards Problems with keyboards can range from their collecting dust (in which case you need to blow them out) to their springs wearing out. If it's the latter, you can replace the keyboard (they cost about 10 times more than desktop keyboards) or choose to use an external one (provided the user isn't traveling and having to lug another hardware element with them).

Pointers The pointer device used on the laptop, like the keyboard, can be affected by dirt/debris as well as by continual use. If the device fails to function properly after a good cleaning, you can replace it (expensive) or opt for an external pointer (such as a wireless mouse).

Unneeded Peripherals To keep the system running at peak efficiency, you should disconnect or disable unneeded peripherals. Every peripheral has the ability to drain power and resources from the PC, and you don't want that if it can be avoided.

Video One of the biggest problems with video is incorrect settings. You can change the video settings easily on the laptop through the operating system. Make sure you have the correct—and most current—drivers.

A few other miscellaneous topics—such as Fn toggling and wireless card issues—are listed by CompTIA beneath this objective, but they have been addressed elsewhere in this book.

LCD Cutoff Switch A thermal cutoff switch is often included in laptops to turn off the system if the temperature rises too high. Although this switch may go bad and cause the laptop

to unduly turn off, usually a shutdown is a symptom of another problem; you should try to isolate what is causing the heat (dirt, debris, and so on) and address that issue.

Exam Essentials

Know how to work with laptop components. Understand the issues that can arise, and know what to look for to begin trying to fix them.

Know the power configuration settings. Using power configuration, it's possible to disable the NIC and other devices to conserve power. You can also receive notification when the battery life reaches low levels.

Performing Preventive Maintenance

Taking care of your company's desktop and laptop computers can extend their life and save considerable money. Most of the actions necessary to maintain laptops fall under the category of what is reasonable, and you would undoubtedly think of them on your own.

Critical Information

Cleaning a computer system is the most important part of maintaining it. Computer components get dirty. Dirt reduces their operating efficiency and, ultimately, their life. Cleaning them is definitely important. But cleaning them with the right cleaning compounds is equally important. Using the wrong compounds can leave residue behind that is more harmful than the dirt you're trying to remove!

Cleaning the Computer

Most computer cases and monitor cases can be cleaned using mild soap and water on a clean, lint-free cloth. Make sure the power is off before you put anything wet near a computer. Dampen (don't soak) a cloth with a mild soap solution, and wipe the dirt and dust from the case. Then, wipe the moisture from the case with a dry, lint-free cloth. Anything with a plastic or metal case can be cleaned in this manner.

Don't drip liquid into any vent holes on equipment. CRTs in particular have vent holes in the top.

To clean a monitor screen, use glass cleaner designed specifically for monitors, and a soft cloth. Don't use commercial window cleaner, because the chemicals in it can ruin the anti-glare coating on some monitors.

To clean a keyboard, use canned air to blow debris out from under keys, and use towelettes designed for use with computers to keep the key tops clean. If you spill anything on a keyboard, you can clean it by soaking it in distilled, *demineralized water*. The minerals and impurities have been removed from this type of water, so it won't leave any traces of residue that might interfere with the proper operation of the keyboard after cleaning. Make sure you let the keyboard dry for at least 48 hours before using it.

The electronic connectors of computer equipment, on the other hand, should never touch water. Instead, use a swab moistened in distilled, *denatured isopropyl alcohol* (also known as electronics cleaner and found in electronics stores) to clean contacts. Doing so will take the oxidation off the copper contacts.

A good way to remove dust and dirt from the inside of the computer is to use compressed air. Blow the dust from inside the computer using a stream of compressed air. However, be sure you do this outdoors, so you don't blow dust all over your work area or yourself. You can also use a vacuum, but it must be designed specifically for electronics—such models don't generate ESD, and have a finer filter than normal.

To prevent a computer from becoming dirty in the first place, control its environment. Make sure there is adequate ventilation in the work area and that the dust level isn't excessive. To avoid ESD, you should maintain 50 to 80 percent humidity in the room where the computer is operating.

Cleaning the Printer

One unique challenge when cleaning printers is spilled toner. It sticks to everything and should not be breathed. Use a vacuum designed specifically for electronics. A normal vacuum's filter isn't fine enough to catch all the particles, so the toner may be circulated into the air.

If you get toner on your clothes, use a magnet to get it out (toner is half iron).

Cleaning the Input

An uninterruptible power supply (UPS) should be checked periodically as part of the preventive maintenance routine to make sure that its battery is operational. Most UPSs have a Test button you can press to simulate a power outage.

Electrical tripping occurs when the breaker on a device such as a power supply, surge protector, or UPS turns off the device because it received a spike. If the device is a UPS, when the tripping happens, the components plugged in to the UPS should go to battery instead of pulling power through the line. Under most circumstances, the breaker is reset and operations continue as normal. Figure 2.2 shows a surge-protector power strip, with the trip button to reset at the top.

FIGURE 2.2 The reset button on the top of a surge-protector power strip

Nuisance tripping is the phrase used if tripping occurs often and isn't a result of a serious condition. If this continues, you should isolate the cause and correct it, even if it means replacing the device that continues to trip.

Surge protectors, either stand-alone or built into the UPS, can help reduce the number of nuisance trips. If your UPS doesn't have a surge protector, you should add one to the outlet before the UPS in order to keep the UPS from being damaged if it receives a strong surge. Figure 2.3 shows an example of a simple surge protector for a home computer.

FIGURE 2.3 A simple surge protector

All units are rated by Underwriters Laboratories (UL) for performance. One thing you should never do is plug a UPS or computer equipment into a Ground Fault Circuit Interrupter (GFCI) receptacle. These receptacles are intended for use in wet areas, and they trip very easily.

Don't confuse a GFCI receptacle with an isolated ground receptacle. Isolated ground receptacles are identifiable by orange outlets and should be used for computer equipment to avoid their picking up a surge passed to the ground by any other device.

Cleaning from a Software Perspective

Remember, preventive maintenance is more than just manipulating hardware; it also encompasses running software utilities on a regular basis to keep the file system fit. These utilities can include Disk Defragmenter, ScanDisk, Check Disk, and Disk Cleanup.

Disk Defragmenter (Defrag)

Disk Defragmenter reorganizes the file storage on a disk to reduce the number of files that are stored noncontiguously. This makes file retrieval faster, because the read/write heads on the disk have to move less.

There are two versions of Disk Defragmenter: a Windows version that runs from within Windows and a DOS version (`DEFRAG.EXE`). The Windows version is located on the System Tools submenu on the Start menu (Start ➢ All Programs ➢ Accessories ➢ System Tools ➢ Disk Defragmenter).

The available switches for the command-line version (`DEFRAG.EXE`) are as follows:

`-a`	Analyze only
`-f`	Force defragmentation even if disk space is low
`-v`	Verbose output

ScanDisk

The ScanDisk utility has moved from being a command-line utility into a graphical tool in each of the operating systems this exam tests on. To access it, right-click on the icon of a hard drive (available through My Computer or just Computer, based on your operating system) and choose Properties. On the Tools tab, click Check Now to start ScanDisk.

Chkdsk (Check Disk)

The fact that Chkdsk is specified as it is in the CompTIA list is an oddity, because it's an old MS-DOS utility that is used to correct logical errors in the FAT. The most common switch for the `CHKDSK` command is `/F`, which fixes the errors that it finds. Without `/F`, Chkdsk is an "information only" utility.

Check Disk, on the other hand (not to be confused with Chkdsk), is a Windows 2000/XP graphical utility for finding and fixing logical errors in the FAT, and optionally also for checking each sector of the disk physically and relocating any readable data from damaged spots.

Check Disk isn't a menu command on the Start menu. To run it, display the Properties box for a hard disk, and then select Check Disk For Errors from the Tools tab.

Disk Cleanup

Disk Cleanup is a Windows-based utility that helps the user recover disk space by deleting unneeded files. It can be run from the System Tools submenu. In some versions of Windows, it automatically runs (or offers to run) when free disk space gets low.

Keeping the System Updated

Aside from the software utilities discussed, you will also want to keep the system updated in terms of drivers, firmware, the operating system, and security. *Device drivers* are the software stubs that allow devices to communicate with the operating system. Called *drivers* for short, they're used for interacting with printers, monitors, network cards, sound cards, and just about every type of hardware attached to the PC. One of the most common problems associated with drivers isn't having the current version—as problems are fixed, the drivers are updated, and you can often save a great deal of time by downloading the latest drivers from the vendor's site early in the troubleshooting process. The easiest way to see/change drivers in Windows is to click the Driver tab in the Properties dialog box for the device.

Any software that is built into a hardware device is called *firmware*. Firmware is typically in flash ROM and can be updated as newer versions become available. An example of firmware is the software in a laser printer that controls it and allows you to interact with it at the console (usually through a limited menu of options).

The operating system can be kept current by Windows Update automatically running (recommended) or you choosing to do so manually (not recommended). You can access and configure the setting from Control Panel.

Security is addressed in Chapter 5, "Security."

Running Regular Backups

Backups are duplicate copies of key information, ideally stored in a location other than the one where the information is currently stored. Backups include both paper and computer records. Computer records are usually backed up using a backup program, backup systems, and backup procedures.

The primary starting point for disaster recovery involves keeping current backup copies of key data files, databases, applications, and paper records available for use. Your organization must develop a solid set of procedures to manage this process and ensure that all key information is protected. A security professional can do several things in conjunction with systems administrators and business managers to protect this information. It's important to think of this problem as an issue that is larger than a single department.

The information you back up must be immediately available for use when needed. If a user loses a critical file, they won't want to wait several days while data files are sent from a remote storage facility. Several different types of storage mechanisms are available for data storage:

Working Copies *Working copy* backups—sometimes referred to as *shadow copies*—are partial or full backups that are kept on the premises for immediate recovery purposes. Working copies are frequently the most recent backups that have been made.

Typically, working copies are intended for immediate use. These copies are typically updated on a frequent basis.

Many file systems used on servers include *journaling*. Journaled file systems (JFS) include a log file of all changes and transactions that have occurred within a set period of time (last few hours, and so on). If a crash occurs, the operating system can look at the log files to see which transactions have been committed and which ones haven't. This technology works well and allows unsaved data to be written after the recovery and the system, usually, to be successfully restored to its pre-crash condition.

Onsite Storage *Onsite storage* usually refers to a location on the site of the computer center that is used to store information locally. Onsite storage containers are available that allow computer cartridges, tapes, and other backup media to be stored in a reasonably protected environment in the building.

Onsite storage containers are designed and rated for fire, moisture, and pressure resistance. These containers aren't *fireproof* in most situations, but they're *fire-rated*: a fireproof container should be guaranteed to withstand damage regardless of the type of fire or temperatures, whereas fire ratings specify that a container can protect the contents for a specific amount of time in a given situation.

If you choose to depend entirely on onsite storage, make sure the containers you acquire can withstand the worst-case environmental catastrophes that could happen at your location. Make sure, as well, that those containers are in locations where you can easily find them after the disaster and access them (near exterior walls, and so on).

Offsite Storage *Offsite storage* refers to a location away from the computer center where paper copies and backup media are kept. Offsite storage can involve something as simple as keeping a copy of backup media at a remote office, or it can be as complicated as a nuclear-hardened high-security storage facility. The storage facility should be bonded, insured, and inspected on a regular basis to ensure that all storage procedures are being followed.

Determining which storage mechanism to use should be based on the needs of the organization, the availability of storage facilities, and the budget available. Most offsite storage facilities charge based on the amount of space you require and the frequency of access you need to the stored information.

Three methods exist to back up information on most systems:

Full Backup A *full backup* is a complete, comprehensive backup of all files on a disk or server. The full backup is current only at the time it's performed. Once a full backup is

made, you have a complete archive of the system at that point in time. A system shouldn't be in use while it undergoes a full backup because some files may not get backed up. Once the system goes back into operation, the backup is no longer current. A full backup can be a time-consuming process on a large system.

Incremental Backup An *incremental backup* is a partial backup that stores only the information that has been changed since the last full or incremental backup. If a full backup were performed on a Sunday night, an incremental backup done on Monday night would contain only the information that changed since Sunday night. Such a backup is typically considerably smaller than a full backup. This backup system requires that each incremental backup be retained until a full backup can be performed. Incremental backups are usually the fastest backups to perform on most systems, and each incremental tape is relatively small.

Differential Backup A differential backup is similar in function to an incremental backup, but it backs up any files that have been altered since the last full backup; it makes duplicate copies of files that haven't changed since the last differential backup. If a full backup were performed on Sunday night, a differential backup performed on Monday night would capture the information that was changed on Monday. A differential backup completed on Tuesday night would record the changes in any files from Monday and any changes in files on Tuesday. As you can see, during the week each differential backup would become larger; by Friday or Saturday night, it might be nearly as large as a full backup. This means the backups in the earliest part of the weekly cycle will be very fast, and each successive one will be slower.

When these backup methods are used in conjunction with each other, the risk of loss can be greatly reduced. You should never combine an incremental backup with a differential backup. One of the major factors in determining which combination of these three methods to use is time—ideally, a full backup would be performed every day. Several commercial backup programs support these three backup methods. You must evaluate your organizational needs when choosing which tools to use to accomplish backups.

Almost every stable operating system contains a utility for creating a copy of configuration settings necessary to reach the present state after a disaster. As an administrator, you must know how to do backups and be familiar with all the options available to you.

Cleaning Miscellany

Removable media devices such as floppy and CD drives don't usually need to be cleaned during preventive maintenance. Clean one only if you're experiencing problems with it. Cleaning kits sold in computer stores provide the needed supplies. Usually, cleaning a floppy drive involves a dummy floppy disk made of semi-abrasive material. When you insert the disk in the drive, the drive spins it, and the abrasive action on the read-write head removes any debris.

Exam Essentials

Know the importance of running scheduled maintenance. Scheduled maintenance can prolong the life of your equipment and help ensure that your output continues to live up to the quality you expect.

Understand the importance of a suitable environment. If you want your equipment to last as long as possible and deliver quality, you should pay attention to the environment in which you place it.

Review Questions

1. What do you need to do if there are stripes on an ink-jet printout?
2. True or false: A laser printer that prints a completely black page may be suffering from a nonfunctioning fuser.
3. Why should you not use transparency film designed for an ink-jet printer in a laser printer?
4. What is the most common cause of small marks or defects in the same spot on every page of a laser printer's printout?
5. True or false: Most computer cases and monitor cases can be cleaned using mild soap and water on a clean, lint-free cloth.
6. When you cannot solve a problem, you should move it to the next highest person that can; this is known as _____ the problem.
7. Hardware errors are often written to an error log, which can be viewed within Windows through which utility?
8. On a printer, a _____ motor is a motor that can move in very small increments.
9. Printers work best in a cool, clean environment where the humidity is between what two percentages?
10. On a laptop, what is the light that powers the LCD screen called?

Answers to Review Questions

1. Clean the ink jets; one or more is clogged.
2. False. A completely black page results from the primary (charging) corona malfunctioning.
3. Because the laser printer's fuser will melt it.
4. A scratch on the drum.
5. True. Most computer cases and monitor cases can be cleaned using mild soap and water on a clean, lint-free cloth.
6. This is known as escalating the problem.
7. The log files in Windows can be read through the use of the Event Viewer utility.
8. A *stepper motor* is a motor that can move in very small increments.
9. Printers work best in a cool, clean environment where the humidity is between 50 and 80 percent.
10. The *backlight* is the light in the laptop that powers the LCD screen.

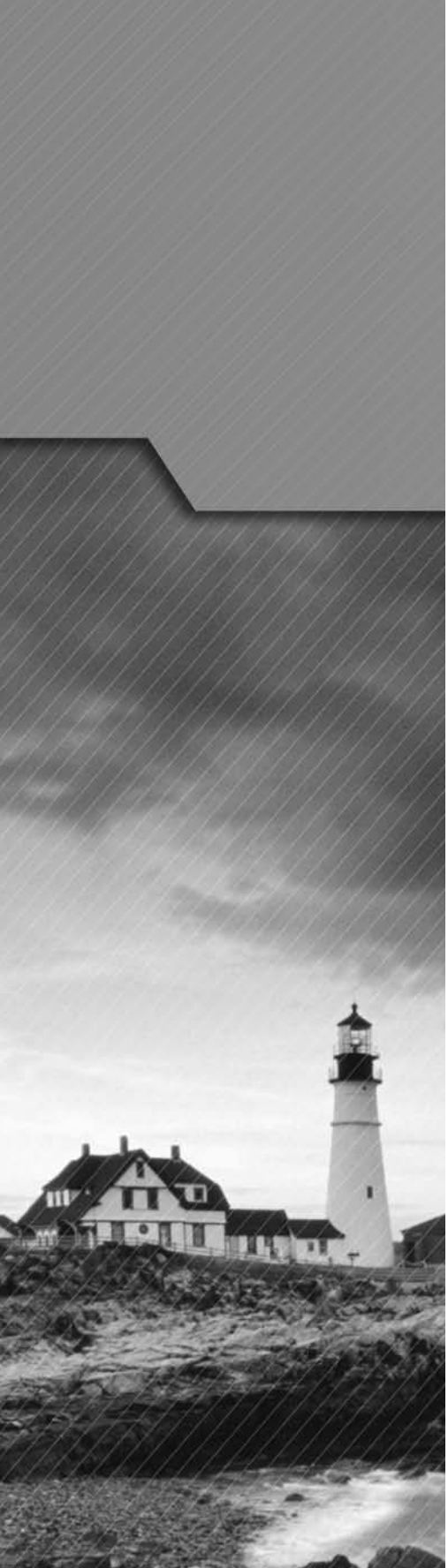
Chapter

3

Operating Systems and Software

COMPTIA A+ ESSENTIALS EXAM OBJECTIVES COVERED IN THIS CHAPTER:

- ✓ **3.1 Compare and contrast the different Windows Operating Systems and their features**
  - Windows 2000, Windows XP 32bit vs. 64bit, Windows Vista 32bit vs. 64bit
    - Side bar, Aero, UAC, minimum system requirements, system limits
    - Windows 2000 and newer – upgrade paths and requirements
    - Terminology (32bit vs. 64bit – x86 vs. x64)
    - Application compatibility, installed program locations (32bit vs. 64bit), Windows compatibility mode
    - User interface, start bar layout
- ✓ **3.2 Given a scenario, demonstrate proper use of user interfaces**
  - Windows Explorer
  - My Computer
  - Control Panel
  - Command prompt utilities
    - telnet
    - ping
    - ipconfig
  - Run line utilities
    - msconfig
    - msinfo32

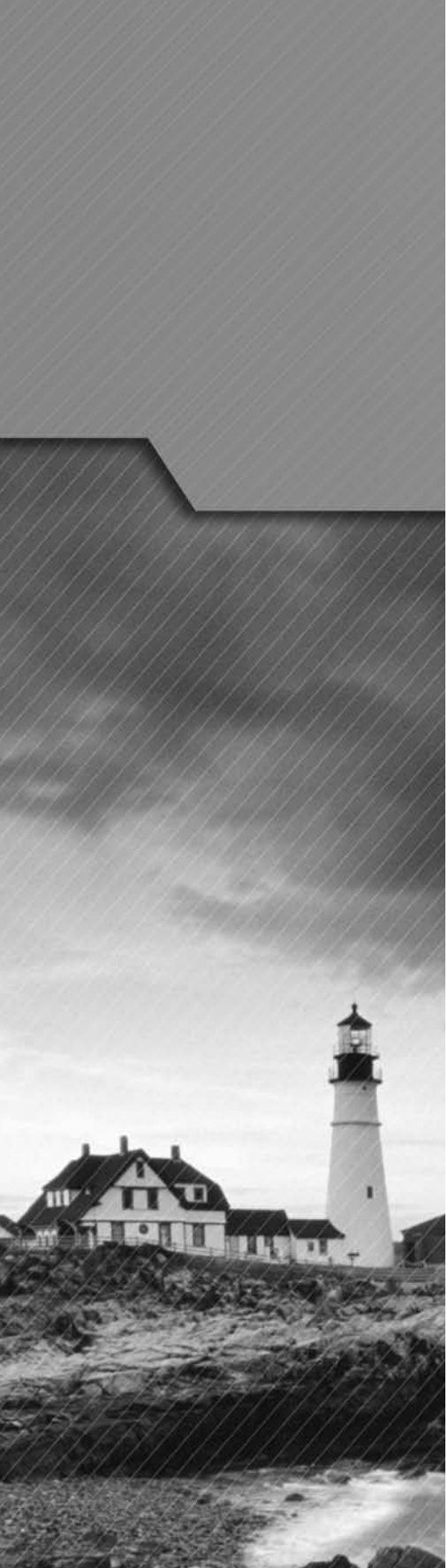


- Dxdiag
- Cmd
- REGEDIT

- My Network Places
- Task bar / systray
- Administrative tools
  - Performance monitor, Event Viewer, Services, Computer Management
- MMC
- Task Manager
- Start Menu

✓ **3.3 Explain the process and steps to install and configure the Windows OS**

- File systems
  - FAT32 vs. NTFS
- Directory structures
  - Create folders
  - Navigate directory structures
- Files
  - Creation
  - Extensions
  - Attributes
  - Permissions
- Verification of hardware compatibility and minimum requirements
- Installation methods
  - Boot methods such as CD, floppy or USB
  - Network installation
  - Install from image
  - Recover CD
  - Factory recovery partition



- Operating system installation options
  - File system type
  - Network configuration
  - Repair install
- Disk preparation order
  - Format drive
  - Partition
  - Start installation
- Device Manager
  - Verify
  - Install and update device drivers
  - Driver signing
- User data migration – User State Migration Tool (USMT)
- Virtual memory
- Configure power management
  - Suspend
  - Wake on LAN
  - Sleep timers
  - Hibernate
  - Standby
- Demonstrate safe removal of peripherals

✓ 3.4 Explain the basics of boot sequences, methods and startup utilities

- Disk boot order / device priority
  - Type of boot devices (disk, network, USB, other)
- Boot options
  - Safe mode
  - Boot to restore point
  - Recovery options
    - Automated System Recovery (ASR)
    - Emergency Repair Disk (ERD)
    - Recovery Console

In one of the recent iterations of the A+ certification, operating systems appeared only on the second exam and not in the core one. Not only does the domain now appear on both the Essentials and the Practical Application exams, but its weighting should signal its importance: 20 percent and 34 percent, respectively. This is a topic that you want to make certain you know well before attempting to become A+ certified.

Operating System Features

This objective deals with one basic question: *what are the differences among the various Windows versions?*

It's essential to know the answer to this question, both for the A+ exam and for real-world work in the PC field. You need to be able to navigate confidently in any operating system (OS) version and tailor your processes to the specific OS version.

Critical Information

Some of this information about Windows functionality may be a review for you, but read through it anyway, to make sure nothing slips between the cracks in your education. Pay special attention to the material on differentiating the OS versions from one another, because you're sure to see some test questions on that topic.

Operating System Generalities

Microsoft Windows isn't the only OS available, but it is the one that this exam tests on. CompTIA expects you to know that others exist but won't ask questions about them. Instead, they will ask about the differences between Windows 2000 (which is tough, since you don't find too many installations of it still around), Windows XP, and Windows Vista.

If you're unsure which version of Windows you have, there are multiple ways to find out. The easiest are to choose System in Control Panel or to type **ver** at a command prompt.

Computers are pretty much useless without software. A piece of hardware makes a good paperweight or doorstop, unless you have an easy way to interface with it. Software is that

interface. While there are many types of software, or programs, the most important application you'll ever deal with is the operating system. Operating systems have many different, complex functions, but two of them jump out as being critical: one, interfacing with the hardware, and two, providing a platform on which other applications can run.

Here are three major distinctions of software to be aware of:

Operating System (OS) The OS provides a consistent environment for other software to execute commands. It gives users an interface with the computer so they can send commands (input) and receive feedback or results (output). To do this, the OS must communicate with the computer hardware to perform the following tasks:

- Disk and file management
- Device access
- Memory management
- Output format

Once the OS has organized these basic resources, users can give the computer instructions through input devices (such as a keyboard or a mouse). Some of these commands are built into the OS, whereas others are issued through the use of applications. The OS becomes the center through which the system hardware, other software, and the user communicate; the rest of the components of the system work together through the OS, which coordinates their communication.

Application Used to accomplish a particular task, an application is software that is written to supplement the commands available to a particular OS. Each application is specifically compiled (configured) for the OS on which it will run. For this reason, the application relies on the OS to do many of its basic tasks. Examples of applications include complex programs, such as Microsoft Word and Internet Explorer, as well as simple programs, such as a command-line FTP program. Either way, when accessing devices and memory, the programs can simply request that the OS do it for them. This arrangement saves substantially on programming overhead, because much of the executable code is *shared*—it is written into the operating system and can therefore be used by multiple applications running on that OS.

All of the Windows versions you need to know for this exam include the ability to convince many applications that they are running in an older version of the operating system than they are if this is needed. In Windows Vista, for example, the Program Compatibility Wizard can be used to configure an application to start in compatibility mode. The operating system choices offered in Vista are Windows 95, Windows NT 4.0 (Services Pack 5), Windows 98, Windows Me, Windows 2000, Windows XP (Service Pack 2), and Windows Server 2003 (Service Pack 1).

Driver A driver is extremely specific software written for the purpose of instructing a particular OS how to access a piece of hardware. For example, each modem or printer has unique features and configuration settings, and the driver allows the OS to properly understand how the hardware works and what it is able to do.

Before we get too far into our discussion of PC operating systems, it will be useful to define a few key terms. The following are some terms you will come across as you study this chapter and visit with people in the computer industry:

Version A version is a particular revision of a piece of software, normally described by a number, which tells you how new the product is in relation to other versions of the product.

Open Source vs. Closed Source This is the actual code that defines how a piece of software works. Computer operating systems can be *open source*, meaning the OS can be examined and modified by users, or they can be *closed source*, meaning users cannot modify or examine the code. For example, Linux is considered an open source operating system, while Microsoft Windows is considered to be closed source.

A word often used interchangeably with *closed source* is *proprietary*.

Shell A shell is a program that runs on top of the OS and allows the user to issue commands through a set of menus or some other graphical interface. Shells make an OS easier to use by changing the user interface.

Graphical User Interface (GUI) The GUI is the method by which a person communicates with a computer. GUIs use a mouse, touchpad, or another mechanism (in addition to the keyboard) to interact with the computer to issue commands.

Network Any group of computers that have a communication link between them is called a network. Networks allow computers to share information and resources quickly and securely.

Cooperative Multitasking The cooperative multitasking method depends on the application itself to be responsible for using and then freeing access to the processor. This is the way very early versions of Windows managed multiple applications. If any application locked up while using the processor, the application was unable to properly free the processor to do other tasks, and the entire system locked, usually forcing a reboot.

Preemptive Multitasking A multitasking method in which the OS allots each application a certain amount of processor time and then forcibly takes back control and gives another application or task access to the processor. This means that if an application crashes, the OS takes control of the processor away from the locked application and passes it on to the next application, which should be unaffected. Although unstable programs still lock, only the locked application will stall—not the entire system.

Multithreading A thread is the smallest operation a task can be divided into. Multithreading is the ability of a single application to submit multiple requests to the processor at one time. This results in faster application performance, because it allows a program to do many things at once.

32-Bit An operating system that is 32-bit is can run on 32-bit processors and also fully utilize the capabilities of the processor. While this may sound simple, the truth of the matter is that it

took many years after the 32-bit processor became available before operating systems (which were 16-bit at the time) were able to utilize their features.

64-Bit A 64-bit operating system is one that is written to utilize the instructions possible with 64-bit processors. A 64-bit processor is one that can move 64 bits of data in or out of the processor with each cycle. Originally, these processors were more common with servers than desktops, but with prices dropping, 64-bit processors have become more common on the desktop, as have operating systems that will run on them.

x86 The phrase *x86* is commonly used to refer to operating systems intended to run on an Intel processor since Intel initially numbered their processors with numbers ending in 86 prior to switching to the Pentium line.

x64 The phrase *x64* is commonly used to denote operating systems that can run on 64-bit processors.

Recent Windows Versions

You can trace Windows back for decades, but the exam does not require you to do that. Prior to Windows 2000 (the starting point for this exam), there were a number of operating systems. One of the earliest was Windows NT. NT (which unofficially stands for New Technology) is an OS that was designed to be far more powerful than any previous Windows version. It used an architecture based entirely on 32-bit code and was capable of accessing up to 4GB (4,000MB) of RAM.

After NT, Windows 2000 was released. It used the same interface as some of the earlier Windows versions (with a few important enhancements). It came in many versions, but the most popular were Windows 2000 Professional (a workstation OS) and Windows 2000 Server (a server OS).

Then came the introduction of Windows XP. XP comes in five versions: Home, Professional, Tablet PC Edition, Professional x64, and Media Center. They are all nearly the same. However, XP Professional contains more corporate and networking features, and Media Center is designed to exploit multimedia connectivity by allowing you to set up your TV through your computer.

Microsoft then released Windows Vista in 2007. Like Windows XP, Vista comes in several flavors: Home, Home Premium, Business, and Ultimate. All Windows Vista versions have the same core technology, but the different versions are designed to work around the role your PC (or handheld PC) plays, not the hardware that it uses.

Among the prominent features included with Vista are a user interface named Windows Aero, Internet Explorer 7, speech and handwriting recognition, and easy-access pop-up sidebars and gadgets. UAC (User Account Control) was added to increase security as well—something it accomplishes by routinely asking you (through pop-ups) if you are sure you want to perform an action that could have negative consequences or if you want to keep an action that just occurred. You can turn off UAC by choosing Start ➢ Control Panel ➢ Security ➢ Security Center ➢ Other Security Settings.

Although Vista was released to replace Windows XP, many users—and businesses—have been slow to adopt it and Windows XP installations remain common.

We will mostly talk about Windows 2000, Windows XP, and Windows Vista in depth throughout the rest of this book because they are the OSs you need to know for the A+ exam.

As of this writing, Microsoft has not announced an official release date for Windows 7, but it is expected to be released in fall 2009. When released, it will be the newest major edition of the Microsoft platform. Key goals of Windows 7 include overcoming the sluggishness in Vista as well as the incompatibilities with applications written for previous versions.

Minimum System Requirements

A later section of this chapter, "Upgrading Operating Systems," discusses the installation and upgrading of operating systems, but one of the things that can prevent you from even considering these options is the hardware requirements of the operating system you are contemplating. Before you can begin to install an OS, there are several items you must consider in order to have a flawless installation. You must perform these tasks before you even put the OS installation disc into your computer's CD-ROM drive. These items essentially set the stage for the procedure you are about to perform:

- Determining hardware compatibility and minimum requirements
- Determining installation options
- Determining the installation method
- Preparing the computer for installation

Let's begin our discussion by talking about hardware compatibility issues and requirements for installing the various versions of Windows.

Determining Hardware Compatibility and Minimum Requirements

Before you can begin to install any version of Windows, it is important that you determine whether the hardware you will be using is supported by the Windows version you will be running. That is, will the version of Windows have problems running any drivers for the hardware you have?

To answer this question, Microsoft has come up with several versions of its *Hardware Compatibility List (HCL)*. This is a list of all the hardware that works with Windows and which versions of Windows it works with. You can find this list at `http://www.microsoft.com/whdc/hcl/search.mspx`. With the release of Windows XP, Microsoft expanded the idea of the HCL to include software as well—and a list that includes both hardware and software can hardly be called a Hardware Compatibility List. The new term is the *Windows Catalog*, and eventually the Windows Catalog will completely replace HCLs.

Another name for the Windows Catalog is the Windows Marketplace, available at `http://www.windowsmarketplace.com`.

The point is, before you install Windows, you should check all your computer's components against this list and make sure each item is compatible with the version of Windows you plan to install.

In addition to general compatibility, it is important that your computer have enough "oomph" to run the version of Windows you plan to install. For that matter, it is important that your computer have sufficient resources to run any software you plan to use. Toward that end, Microsoft (as well as other software publishers) provides a list of both minimum and recommended hardware specifications that you should follow when installing Windows.

Minimum specifications are the absolute minimum requirements for hardware you should have in your system in order to install and run the OS you have chosen. *Recommended* hardware specifications are what you should have in your system to realize usable performance. Always try to have the recommended hardware (or better) in your system. If you don't, you may have to upgrade your hardware before you upgrade your OS. Table 3.1 lists the minimum and recommended hardware specifications for Windows 2000 and XP. Note that in addition to these minimums, the hardware must be compatible with Windows. Also, additional hardware may be required if certain features are installed (for example, a NIC is required for networking support).

TABLE 3.1 Windows 2000 and XP Minimum and Recommended Hardware

Hardware	2000 Professional Requirement	2000 Professional Recommendation	XP Professional Requirement	XP Professional Recommendation
Processor	Pentium 133	Pentium II or higher	233MHz Pentium/ Celeron or AMD K6/Athlon/Duron	300MHz or higher Intel-compatible processor
Memory	64MB	128MB or more	64MB	128MB
Free hard disk space	650MB	2GB, plus what is needed for applications and storage	1.5GB	1.5GB
Floppy disk	Required only if installing from boot disks	Yes	Not required	Not required
CD-ROM or DVD	Required	Yes	Required	Required
Video	VGA	SuperVGA	SuperVGA or better	SuperVGA or better

TABLE 3.1 Windows 2000 and XP Minimum and Recommended Hardware *(continued)*

Hardware	2000 Professional Requirement	2000 Professional Recommendation	XP Professional Requirement	XP Professional Recommendation
Mouse	Required (but not listed as a requirement)	Required (but not listed as a requirement)	Required	Required
Keyboard	Required	Required	Required	Required

Table 3.2 lists the minimum system requirements for the various versions of Windows Vista.

TABLE 3.2 Windows Vista Minimum Hardware

Hardware	Minimum Supported for All Versions	Home Basic Recommendation	Home Premium/Business/ Ultimate Recommendation
Processor	800MHz	1GHz 32-bit (x86) or 64-bit (x64) processor	1GHz 32-bit (x86) or 64-bit (x64) processor
Memory	512MB	512MB	1GB
Free hard disk space	15GB free on a 20GB drive	15GB free on a 20GB drive	15GB free on a 40GB drive
CD-ROM or DVD	CD-ROM	DVD-ROM	DVD-ROM
Video	SVGA	Support for DirectX 9 graphics and 32MG graphics memory	Support for DirectX 9 with: WDDM Driver 128MB of graphics memory Pixel Shader 2.0 in hardware 32 bits per pixel
Mouse	Required (but not listed as a requirement)	Required (but not listed as a requirement)	Required (but not listed as a requirement)
Keyboard	Required (but not listed as a requirement)	Required (but not listed as a requirement)	Required (but not listed as a requirement)
Internet Access	Not listed as a requirement	Required	Required

If there is one thing to be learned from Tables 3.1 and 3.2, it is that Microsoft is nothing if not optimistic. For your own sanity, though, we strongly suggest that you always take the minimum requirements with a grain of salt. They are *minimums*. Even the recommended requirements should be considered minimums. Bottom line: Make sure you have a good margin between your system's performance and the minimum requirements listed. Always run Windows on more hardware rather than less!

Pay particular attention to system memory—get as much memory as you can because some operating systems (such as Windows Vista) are notorious for working better when memory is plentiful.

Other hardware—sound cards, network cards, modems, video cards, and so on—may or may not work with Windows. If the device is fairly recent, you can be relatively certain that it was built to work with the newest version of Windows. But if it is older, you may need to find out who made the hardware and check their website to see if they have drivers for the version of Windows you are installing.

The easiest way to see if your current hardware can run Windows Vista is to download and run the Windows Vista Upgrade Advisor available at `http://www.microsoft.com/windows/windows-vista/get/upgrade-advisor.aspx`.

There's one more thing to consider when evaluating installation methods. Some methods work only if you're performing a clean installation, and not an upgrade. More information about installing and upgrading appears later in this chapter, in the "Configuring Windows" section.

One of the objectives beneath this section is "User interface, start bar layout." That topic is not discussed here since it fits much better in the next section, which focuses exclusively on the user interface. Similarly, the discussion of file locations is spread throughout this chapter. Note as well that CompTIA seems to have invented start bar; Microsoft calls it Windows taskbar, as we correctly call it later in the chapter.

Exam Essentials

Know the major functions of Windows. You should understand what an OS does, what systems it manages, and how it communicates with the human user.

Understand version differences. Know how to group the Windows versions according to similarity and explain how one group differs from the other.

User Interfaces

This objective deals with one basic question: *What desktop components and interfaces form the Windows GUI?*

Just as with other objectives, it is important to know the answer to this question, both for the A+ exam and for real-world work in the PC field.

Critical Information

The *operating system* provides a consistent environment for other software to execute commands. The OS gives users an interface with the computer so they can send commands to it (input) and receive feedback or results back (output). To do this, the OS must communicate with the computer hardware to perform the following tasks:

- Disk and file management
- Device access
- Memory management
- Input/output

Disk and File Management

The OS must be able to store and retrieve files on disks; this is one of its most primary functions. The system components involved in disk and file management include the following:

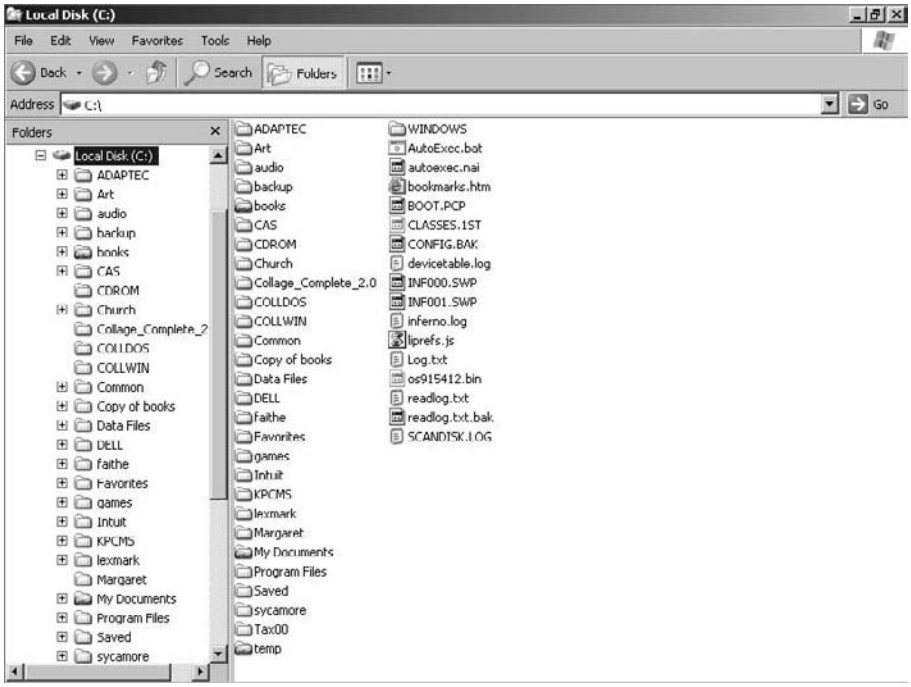
Windows Explorer This is the primary file management interface in Windows. It displays the list of files in the current location at the right and a folder tree of other locations at the left (see Figure 3.1). It starts with the My Documents folder as its default location when opened. Windows Explorer is available in all Windows versions and works approximately the same way in each.

My Computer/Computer My Computer is basically the same interface as Windows Explorer, except it doesn't show the folder tree by default, and it starts with a list of local drives. Originally, the two were separate; but in modern versions of Windows, you can click the Folders button on the toolbar to turn that folder tree on/off, making the two interfaces practically identical.

Control Panel This is a folder that contains applets you can use to configure your system. Common applets in Control Panel include Add Hardware, Add Or Remove Programs, Display, System, and a surplus of others. Some of the entries here—such as Fonts—aren't applets themselves, but rather folders that hold additional entities.

Network Neighborhood/My Network Places Again, this is basically the same interface as the others, but designed for browsing network computers and drives rather than local ones. In early versions of Windows, this was called Network Neighborhood; starting with Windows 2000, the name was changed to My Network Places.

FIGURE 3.1 The Windows Explorer interface



Device Access

Another responsibility of the OS is to manage the way that software on the system interacts with the computer's hardware. More advanced OSs have the ability to avoid conflicts between devices and to prevent applications from interfering with one another.

Windows handles device management by itself in most cases. In instances where users need to get involved, they can use the Device Manager interface. In Windows 2000 and XP, you must display the System Properties box, click the Hardware tab, and then click Device Manager (another way is to right-click My Computer, choose Manage, and then click Device Manager).

Major Operating System Components

All Windows versions have a similar look and feel in their user interface. Figure 3.2 shows Windows 2000, for example.

The main differences between Windows XP and all other Windows versions are the redesigned Start menu and the rounded look of the dialog boxes. Figure 3.3 shows a typical Windows XP screen. With Windows Vista, this changed a bit thanks to the Aero interface, as Figure 3.4 shows, but not as dramatically as many in the media have made it out to be.

FIGURE 3.2 The Windows 2000 interface

FIGURE 3.3 The Windows XP interface

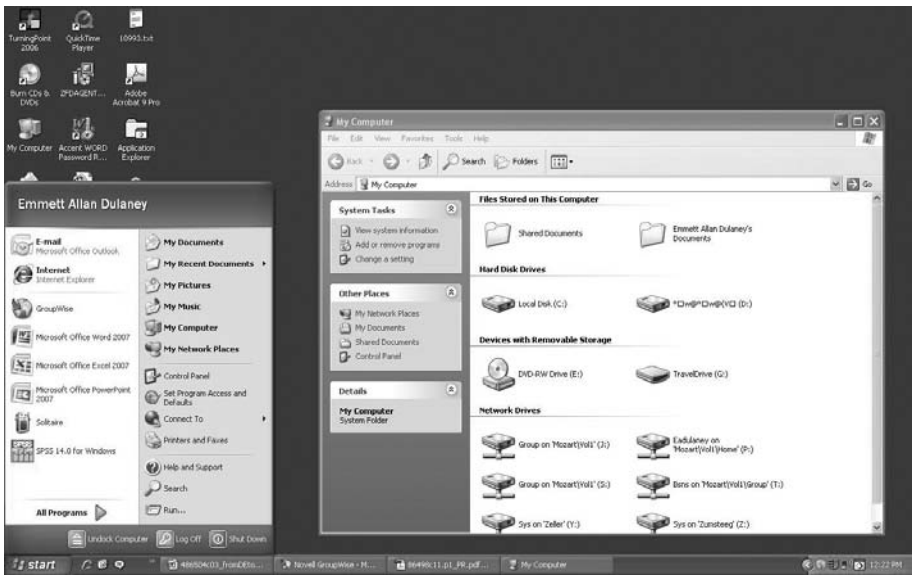


FIGURE 3.4 The Windows Vista interface

Much of this information will be review for those of you who have experience using Windows OSs, but you may want to refresh your mind as to the specific names and attributes of these components. In the following sections, we will first look at what the operating systems have in common, and then discuss any changes specific to Vista.

The Desktop

The Desktop is the virtual desk on which all of your other programs and utilities run. By default it contains the *Start menu*, the *Taskbar*, and a number of *icons*. The Desktop can also contain additional elements, such as web page content, through the use of the Active Desktop feature. Because it is the base on which everything else sits, the way the Desktop is configured can have a major effect on how the GUI looks and how convenient it is for users.

You can change the Desktop's background patterns, screensaver, color scheme, and size by right-clicking any area of the Desktop that doesn't contain an icon. The context menu that appears allows you to do several things, such as create new Desktop items, change how your icons are arranged, or select a special command called Properties, similar to the one shown in Figure 3.5.

FIGURE 3.5 The Desktop context menu

When you right-click the Desktop and choose Properties, you will see the Display Properties window shown in Figure 3.6.

FIGURE 3.6 The Display Properties window

On this window, you can click the tabs at the top to move to the various screens of information related to the way Windows looks. Tabs are similar to index cards; they are staggered across the top so you can see and access large amounts of data within a single small window. Each Properties window has a different set of tabs. The tabs will differ based on the operating system, but among the tabs in the Display Properties window of most OSs are the following:

Themes On this tab, you select a theme that enables you to quickly customize the look and feel of your machine. Selecting a theme sets several items at once, such as a picture to display on the Desktop, the look of icons, sounds to use, and so on. You can also select all of these options individually through the other Desktop Properties tabs. For example, if you're more comfortable with the look and feel of previous versions of Windows, you can select the Windows Classic theme.

Background or Desktop The Background tab in Windows 2000 is used to select an HTML document or a picture to display on the Desktop. In addition to letting you perform this same function, the Desktop tab in Windows XP lets you configure other items through the Customize Desktop button. Examples include changing which default icons to display on the Desktop and configuring web content for the Desktop.

Screen Saver Use this tab to set up an automatic screensaver to cover your screen if you have not been active for a certain period of time. Originally used to prevent burned-in monitors, screensavers are now generally used for entertainment or to password-protect users' Desktops. The Screen Saver tab gives you access to other power settings as well.

Appearance The Appearance tab lets you to select a color scheme for the Desktop or change the color or size of other Desktop elements.

Effects (Windows 2000 Only) This tab contains numerous assorted visual options. In other operating systems, some of these visual options are available via the Customize Desktop button on the Desktop tab.

Web (Windows 2000 Only) The Web tab lets you configure Active Desktop settings. In other operating systems, you can access this tab via the Customize Desktop button on the Desktop tab.

Settings Use the options on this tab to specify the color depth or screen size. This tab also contains an Advanced button, which leads to graphics driver and monitor configuration settings.

You can also access the Display Properties settings by clicking the Display icon in Control Panel.

The Taskbar

The Taskbar (see Figure 3.7) is another standard component of the Windows interface and CompTIA refers to it as the Start Bar in their objectives. Note that although the colors and feel of the Desktop components, including the Taskbar, have changed throughout the operating systems, the components themselves are the same. The Taskbar contains two major items: the Start menu and the *System Tray* (systray). The Start menu is on the left side of the Taskbar and is easily identifiable: it is a button that has the word *Start* on it or—in the case of Windows Vista—is the large Windows icon. The *System Tray* is located on the right side of the Taskbar and contains only a clock by default, but other Windows utilities (for example, screensavers or virus-protection utilities) may put their icons here to indicate that they are running and to provide the user with a quick way to access their features.

FIGURE 3.7 The Taskbar

Windows also uses the middle area of the Taskbar. When you open a new window or program, it gets a button on the Taskbar with an icon that represents the window or program as well as the name of the window or program. To bring that window or program to the front (or to maximize it if it was minimized), click its button on the Taskbar. As the middle area of the Taskbar fills with buttons, the buttons become smaller so they can all be displayed.

You can increase the size of the Taskbar by moving the mouse pointer to the top of the Taskbar and pausing until the pointer turns into a double-headed arrow. Once this happens, click the mouse and move it up to make the Taskbar bigger. Or move it down to make the Taskbar smaller. You can also move the Taskbar to the top or side of the screen by clicking the Taskbar and dragging it to the new location.

In Windows Vista and XP, once you've configured the Taskbar position and layout to your liking, you can configure it so that it can't be changed accidentally. To do so, right-click the Taskbar and select Lock The Taskbar. To unlock the Taskbar and make changes, right-click the Taskbar and select Lock The Taskbar again.

In addition to the Taskbar, Windows Vista includes the Sidebar, shown in Figure 3.8. This provides a quick interface that allows you to access common utilities such as the calendar.

FIGURE 3.8 The Windows Vista Sidebar

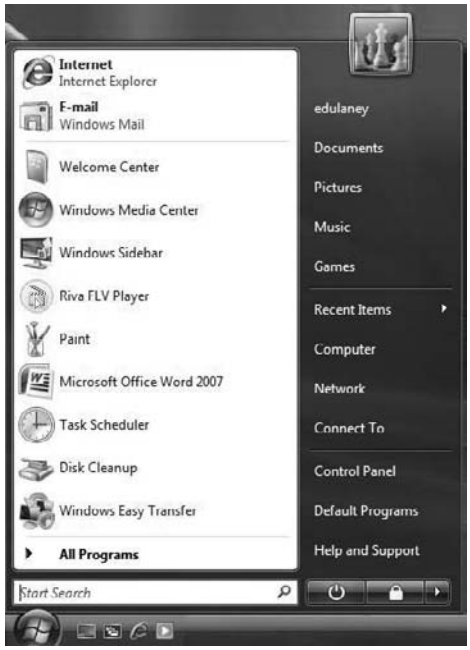
The Start Menu

Back when Microsoft officially introduced Windows 95, it bought the rights to use the Rolling Stones song "Start Me Up" in its advertisements and at the introduction party. Microsoft chose that particular song because the Start menu was the central point of focus in the new Windows interface, as it has been in all subsequent versions.

To display the Start menu, click the Start button in the Taskbar. You'll see a Start menu similar to that shown in Figure 3.9 for Windows XP and Figure 3.10 for Windows Vista. You'll notice that in Windows XP the look of the Start menu is slightly different than that in earlier versions of Windows or Windows Vista, but they all behave the same. Regardless of the operating system, the Start menu always serves the same function: quick access to important features and programs.

FIGURE 3.9 The Windows XP Start menu

FIGURE 3.10 The Windows Vista Start menu



From the Start menu, you can select any of the various options the menu presents. An arrow pointing to the right indicates that a submenu is available. To select a submenu, move the mouse pointer over the submenu title and pause. The submenu will appear; you don't even have to click. (You have to click to choose an option on the submenu, though.) We'll discuss each of the default Start menu's submenu options and how to use them.

One handy feature of the Start menu in pre–Windows XP versions of Windows is that it usually displays the name of the OS type along its side when you activate it if you're using large icons or the large menu. This provides an excellent way to quickly see whether you are on Windows 9*x*, NT, or 2000. In Windows XP and Vista, you don't see the name of the OS; however, the Start menu looks so different that you should be able to identify which operating system you are using.

You can also check which OS you are using by right-clicking the My Computer icon on the Desktop and selecting Properties. The OS type and version are displayed on the first tab. Note that the My Computer icon may not display on the Desktop by default. You can add the icon to the Desktop by using the Display Properties (click Customize Desktop on the Desktop tab, select My Computer on the General tab, and apply your changes), or you can click Start and then right-click the My Computer option and select Properties.

If you are running Windows Vista or XP and are attached to the look and feel of the pre–Windows XP Start menu, you can configure the OS to use the old Start menu layout. To do so, right-click on the Taskbar and select Properties. Click the Start Menu tab, select Classic Start Menu, and click OK.

Programs (Windows 2000)/All Programs (Windows XP and Vista) Submenu

The Programs/All Programs submenu holds the program groups and program icons you can use. When you select this submenu, you will be shown another submenu, with a submenu for each program group. In Windows XP and Vista, the look is again a little different, but the functionality is the same. You can navigate through this menu and its submenus and click the program you wish to start.

The most common way to add programs to this submenu is by using an application's installation program. In Windows 2000 (and Windows XP if you're using the Classic Start Menu), you can also add programs to this submenu by using the Taskbar Properties screen (right-click on the Taskbar and choose Properties).

Documents (2000)/My Recent Documents (Windows XP)/Recent Items (Windows Vista) Submenu

The Documents/My Recent Documents/Recent Items submenu has only one function: to keep track of the last data files you opened. Whenever you open a file, a shortcut to it is automatically made in this menu. To open the document again, click the document in the Documents menu to open it in its associated application.

In Windows XP, this feature is not enabled by default. To enable it, in the Taskbar And Start Menu Properties screen, click the Start Menu tab and then click Customize next to Start Menu. Click the Advanced tab, select the List My Most Recently Opened Documents option, and then click OK. An option called My Recent Documents is added to the Start menu; it lists the 15 most recently opened data files.

To clear the list of documents shown in the Documents/My Recent Documents/Recent Items submenu, go to the Taskbar And Start Menu Properties screen. Then use the Clear button on the Advanced tab. (Remember that you access the Advanced tab in Windows XP via the Customize button on the Start Menu tab.)

Settings Submenu (Windows 2000)

The Settings submenu provides easy access to the configuration of Windows. This menu has numerous submenus, including Control Panel, Printers, and Taskbar & Start Menu. Additional menus are available, depending on which version of Windows you are using. These submenus give you access to Control Panel, printer folder, and Taskbar configuration areas. You can also access the first two areas from the My Computer icon; they are placed together here to provide a common area to access Windows settings.

In Windows XP and Windows Vista, you'll find Control Panel as an option directly off the Start menu (not below a submenu). You can add other options (such as Printers And Faxes) to the Start menu by using the options on the Advanced tab of the Taskbar And Start Menu Properties screen (via the Customize button).

Search (Find) Submenu/Option

The name of this submenu (Windows 2000) or Start menu option (Windows XP and Vista) differs between Search and Find in the various versions of Windows, but its purpose doesn't. In all cases, it's used to locate information on your computer or on a network.

In Windows 2000, to find a file or directory, select the Find or Search submenu and then select Files Or Folders. In the Named field in this dialog box, type in the name of the file or directory you are looking for and click Find Now. Windows will search whatever is specified in the Look In parameter for the file or directory. Matches are listed in a window under the Find window. You can use wildcards (* and ?) to look for multiple files and directories. You can also click the Advanced tab to further refine your search.

In Windows XP or Vista, to find a file or directory, click the Search option in the Start menu. Doing so opens the Search Results dialog box. In the left pane, click All Files And Folders, and then enter the appropriate information in the text fields. Expand the down-pointing double arrows to access advanced search options. To start the search, click Search. The search results display in the right pane.

Help Command (Windows 2000)/Help And Support (Windows XP and Vista)

Windows has always included a very good Help system. In addition, the Help system was updated with a new interface and new tools in Windows XP and Vista. Because of its usefulness and power, it was placed in the Start menu for easy access.

In Windows 2000, when you select the Help command, it brings up the Windows Help window. In the newer operating systems, when you click Help And Support, the Help And Support Center home page opens. This screen may have been slightly customized by a hardware vendor if the operating system was preinstalled on your machine. However, all the options and available tools will still be present.

A quick way to access Help is to press the F1 key.

Run Command (Windows 2000 and Windows XP)

You can use the Run command to start programs if they don't have a shortcut on the Desktop or in the Programs submenu. When you choose Run from the Start menu, a pop-up window appears. To execute a particular program, type its name in the Open field. If you don't know the exact path, you can browse to find the file by clicking the Browse button. Once you have typed in the executable name, click OK to run the program.

While this functionality has not disappeared from Windows Vista, it is a bit different. A blank dialog box appears at the bottom of the Start menu with the default phrase "Start Search" within. Type the name of the command you want to run in here, and press Enter. Vista will look for the executable and run it.

Shut Down Command (Windows 2000)/Turn Off Computer Command (Windows XP and Vista)

Windows operating systems are very complex. At any one time, many files are open in memory. If you accidentally hit the power switch and turn off the computer while these files are open, there is a good chance they will be corrupted. For this reason, Microsoft has added the Shut Down (pre–Windows XP) or Turn Off Computer (Windows XP and Vista) command under the Start menu (in Vista, it appears as an icon of an on/off button and does not have a label). Note that with a configuration called Fast User Switching, Windows XP also displays Shut Down, rather than Turn Off Computer. When you select this option, Windows presents you with several choices. Exactly which options are available depends on the Windows version you are running.

Whether you see options of Shut Down or Turn Off Computer has a lot to do with the way your user interface is configured (Classic View, using the Welcome Screen, etc.). Regardless of the name of the choice, it performs the same function.

The possible choices are as follows:

Shut Down (Windows 2000, XP, and Vista)/Turn Off (Windows XP) This option writes any unsaved data to disk, closes any open applications, makes a copy of the registry, and gets the computer ready to be powered off. Depending on the OS, the computer is then powered down automatically, or you'll see a black screen with the message *It's now safe to*

turn off your computer. In this case, you can power off the computer or press Ctrl+Alt+Del to reboot the computer.

Restart This option works the same as the first option, but instead of shutting down completely, it automatically reboots the computer with a warm reboot.

Stand By (Windows XP and 2000 Only) This option places the computer into a low-power state. The monitor and hard disks are turned off, and the computer uses less power. To resume working, press a key on the keyboard; the computer is returned to its original state. In this state, information in memory is not saved to hard disk, so if a power loss occurs, any data in memory will be lost.

Switch User (XP and Vista only) This option allows you to switch users on a machine without closing programs. This is generally not recommended in a work environment for the security reasons associated with leaving programs running.

Log Off I highly recommend this option over Switch User, as it closes all open programs and then logs off—allowing another user to then log on.

Lock This option leaves programs running, but locks the computer and requires the user's password to be entered again before the session can continue.

Hibernate This option saves the session and turns off the computer. When powered back up, the session resumes.

Sleep This option keeps the session in memory and puts the computer in a low-power state that you can quickly resume from. This is like Hibernate, but without fully powering down the computer.

If you enable Hibernate on a Windows XP machine, you can place the computer into hibernation by holding down the Shift key while clicking Stand By on the Turn Off Computer screen. Using the Hibernate feature, any information in memory is saved to disk before the computer is put into a low-power state. Thus, if power is lost while the machine is in hibernation, your data is not lost. However, going into and coming out of hibernation takes more time than going into and coming out of stand-by mode.

Icons

Icons are not nearly as complex in structure as other operating system elements, but they are very important nonetheless. Icons are shortcuts that allow a user to open a program or a utility without knowing where that program is located or how it needs to be configured. Icons consist of several major elements:

- Icon label
- Icon graphic
- Program location

The label and graphic simply tell the user the name of the program and give a visual hint about what that program does. The icon for the Solitaire program, for instance, is labeled *Solitaire*, and its icon is a deck of cards. By right-clicking an icon once, you make that icon the active icon, and a drop-down menu appears. One of the selections is Properties. Clicking Properties brings up the icon's attributes (see Figure 3.11) and is the only way to see exactly which program an icon is configured to start and where the program's executable is located. You can also specify whether to run the program in a normal window or maximized or minimized.

FIGURE 3.11 The Properties window of an application with its icon above it

In operating systems beginning with Windows 2000, additional functionality has been added to an icon's Properties to allow for backward compatibility with older versions of Windows. To configure this, click the Compatibility tab and specify the version of Windows for which you want to configure compatibility. This feature is helpful if you own programs that used to work in older versions of Windows but no longer run under the current Windows version. In addition, you can specify different display settings that might be required by older programs.

Standard Desktop Icons

In addition to the options in your Start menu, a number of icons are placed directly on the Desktop in Windows 2000, XP, and Vista. Three of the most important icons are My

Computer/Computer, Network Neighborhood/My Network Places/Network, and the Recycle Bin. While these three are important, the My Computer and My Network Places icons no longer display by default on the Desktop; however, you might want to add them. You saw how to add My Computer earlier, in the section "The Start Menu;" you can select My Network Places in the same place you select My Computer to display that icon on the Desktop.

The My Computer Icon If you double-click the My Computer icon, it displays a list of all the disk drives installed in your computer. In pre–Windows XP versions of Windows, it also displays an icon for the Control Panel and Printers folders, which can be used to configure the system.

In Windows XP, My Computer does not by default display an icon for Control Panel (although you can configure it to do so by going to Tools ➢ Folder Options and specifying to show Control Panel in My Computer on the View tab) or for printers; however, in addition to displaying disk drives, it displays a list of other devices attached to the computer, such as scanners, cameras, mobile devices, and so on. In Windows XP, all the disk devices are sorted into categories such as Hard Disk Drives, Devices With Removable Storage, Scanners And Cameras, and so on. If you double-click a disk drive or device, you will see the contents of that disk drive or device.

You can delve deeper into each disk drive or device by double-clicking it. The contents are displayed in the same window. You can use Tools ➢ Folder to configure each folder to open in a new window. Having multiple windows open makes it easy to copy and move files between drives and between directories using these windows.

In addition to allowing you access to your computer's files, the My Computer icon lets you view your machine's configuration and hardware, also called the System Properties.

Right-clicking on Computer in the Start menu allows you to choose Properties and see the same information (choosing Manage instead of Properties brings up the Computer Management interface, in which you can make a plethora of changes).

My Network Places Another icon in Windows relates to accessing other computers to which the local computer is connected, and it's called My Network Places (Network Neighborhood pre–Windows 2000).

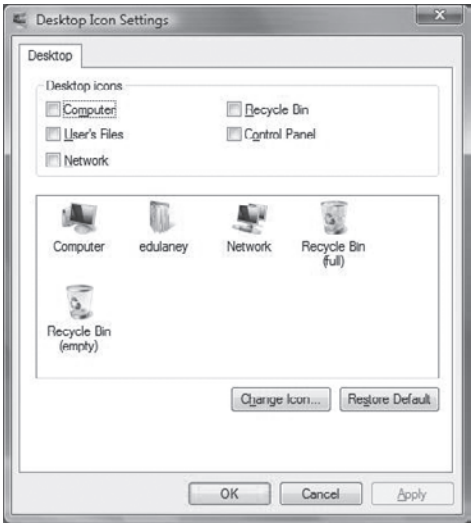
In Windows XP, the My Network Places icon may not display on the Desktop by default. You can add the icon to the Desktop through the Display Properties (in the same manner you can add the My Computer icon to the Desktop if it isn't there), or you can reach My Network Places by clicking Start ➢ My Network Places.

Opening My Network Places enables you to browse for and access other computers and shared resources to which your computer is connected. This might be another computer in a workgroup, domain, or other network environment (such as a Novell NetWare network). You can also use My Network Places to establish new connections to shared resources.

Through the Properties of My Network Places, you can configure your network connections, including LAN and dial-up connections. You will learn about networking in detail in Chapter 9, "Networking."

In Windows Vista, the wording of this option has been changed to simply Network. It can be chosen from the Start menu or you can add it—and other common icons—to the Desktop by choosing Control Panel ➢ Appearance And Personalization ➢ Personalization ➢ Change Desktop Icons (from the choices on the left). This will open the dialog box shown in Figure 3.12.

FIGURE 3.12 Common icons can easily be added to the Vista desktop.



The Recycle Bin All files, directories, and programs in Windows are represented by icons and are generally referred to as *objects*. When you want to remove an object from Windows, you do so by deleting it. Deleting doesn't just remove the object, though; it also removes the ability of the system to access the information or application the object represents. For this reason, Windows includes a special directory where all deleted files are placed: the Recycle Bin. The Recycle Bin holds the files until it is emptied—or you fill the bin—and allows users the opportunity to recover files that they delete accidentally. By right-clicking, you can see how much disk space is allocated. Larger files that cannot fit in the bin will be erased after a warning.

You can retrieve a file you have deleted by opening the Recycle Bin icon and then dragging the file from the Recycle Bin to where you want to restore it. Alternatively, you can right-click a file and select Restore, and the file will be restored to the location it was deleted from.

If you have antivirus software installed, option names in the Recycle Bin might change. For example, if you have Norton Antivirus installed and you right-click on a file, you'll see that the Restore option has been renamed to Recover.

To permanently erase files, you need to empty the Recycle Bin, thereby deleting any items in it and freeing the hard drive space they took up. If you want to delete only specific, but not all, files, you can select those files in the Recycle Bin, right-click, and choose Delete. You can also permanently erase files (bypassing the Recycle Bin) by holding down the Shift key as you delete the file (either by dragging the file and dropping it in the Recycle Bin, pressing the Delete key, or clicking Delete on the file's context menu). By default, if the Recycle Bin has files in it, its icon looks like a full trash can; when there are no files in it, it looks like an empty trash can.

System Management Tools

There are two tools to know well for this section:

Device Manager Device Manager shows a list of all installed hardware and lets you add items, remove items, update drivers, and more. This is a Windows-only utility. In Windows 2000 and XP, when you display the System Properties, click the Hardware tab and then click the Device Manager button to display it.

System Configuration Editor (`MSCONFIG`) This utility, known as the System Configuration Editor, helps troubleshoot startup problems by allowing you to selectively disable individual items that normally are executed at startup. There is no menu command for this utility; you must run it with the Run command (on the Start menu). Choose Start ➢ Run, and type **`MSCONFIG`**. It works in most versions of Windows, although the interface window is slightly different among versions.

The Command Prompt

Although we're talking about the Windows operating system in this book, its ancestor, the Microsoft Disk Operating System (MS-DOS), still plays a role in Windows today. MS-DOS was never meant to be extremely friendly. Its roots are in CP/M, which, in turn, has its roots in Unix. Both of these older OSs are command line–based, and so is MS-DOS. In other words, they all use long strings of commands typed in at the computer keyboard to perform operations. Some people prefer this type of interaction with the computer, including many folks with technical backgrounds (such as yours truly). Although Windows has left the full command-line interface behind, it still contains a bit of DOS, and you get to it through the command prompt.

Although you can't tell from looking at it, the Windows command prompt is actually a 16- or 32-bit Windows program that is intentionally *designed* to have the look and feel of a DOS command line. Because it is, despite its appearance, a Windows program, the command prompt provides all the stability and configurability you expect from Windows. You can access a command prompt by running the 32-bit `CMD.EXE`.

Once at the command prompt, there are three diagnostic utilities that are often run: Telnet, ping, and ipconfig. All three are TCP/IP utilities. (TCP/IP is the protocol that allows networked computers to use the Internet, and as such is something you will probably see a lot of. It's discussed in detail in Chapter 4, "Networking.")

TELNET

Telnet is a protocol that functions at the Application layer of the OSI model, providing terminal-emulation capabilities. Telnet uses the connection-oriented services of the TCP/IP protocol for communications at port 23. With Telnet, the command to initiate the session is `TELNET` itself, or `TELNET` followed by an IP address or hostname to connect to a specific remote host.

The remote host system must be running a Telnet daemon or service. Once a connection is established, you must log on to the server by using a valid username and password (plain text) as if you were sitting at the server. If you connect to a remote host by using the Connect/Remote system option, you may be prompted for the information required for a Telnet session.

If possible, Telnet shouldn't be used. Telnet sends user ID and password information to the Telnet server unencrypted. This creates a potential security problem in an Internet environment.

PING

Another useful connectivity troubleshooting command is `PING`, which stands for packet Internet groper. The `PING` command sends out four 32-byte packets to a destination and waits for a reply. If you cannot make a connection to the remote host, you will get back the following:

```
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

Keep in mind that some Internet sites block pings as a precautionary security measure, so be sure to use a site that you know accepts them if you're using ping as a troubleshooting tool. Generally, you don't use any switches with `PING`. Just type **`PING`** ***`IPaddress`*** or **`PING`** ***`hostname`*** and see if it works. However, switches are available to persistently ping (until we press Ctrl+C to stop ping), change the packet size, change the number of packets sent, and various other things.

Along with `IPCONFIG` and `PING`, another handy connectivity troubleshooting command is `TRACERT`, or trace route. It traces the route between your computer and the destination computer, and can help determine where the breakdown is if you're having connectivity problems.

In every installation of TCP/IP, the address 127.0.0.1 is reserved as the loopback address. If you want to test TCP/IP on the current machine without hitting the network, you can always ping this address.

IPCONFIG

The IPCONFIG command allows you to check on the TCP/IP settings of the machine. In a world where it seems every computer is connected to a network, you'll do a lot of network connection troubleshooting. The IPCONFIG command is one of the first ones you should use when troubleshooting why someone can't get on the network. In fact, it's often the first one I do use. The IPCONFIG command checks your computer's IP configuration. Table 3.3 lists useful switches for IPCONFIG.

TABLE 3.3 IPCONFIG Switches

Switch	Purpose
/ALL	Shows full configuration information
/RELEASE	Releases the IP address, if you are getting addresses from a Dynamic Host Configuration Protocol (DHCP) server
/RENEW	Obtains a new IP address from a DHCP server
/FLUSHDNS	Flushes the domain name server (DNS) name resolver cache

Running IPCONFIG can tell you a lot. For example, if the network cable is disconnected, it will tell you. Also, if your IP address is 0.0.0.0, you're not going to connect to any network resources. An address starting with 169.254 is an address that Microsoft automatically assigns if a DHCP server cannot be found; while this can allow you to continue to network, it will not allow Internet access.

If you get an IP address from a DHCP server but are having connectivity problems, a common troubleshooting method is to release the IP address with IPCONFIG /RELEASE, and get a new one with IPCONFIG /RENEW.

More often than not, when you release and renew an IP address, you'll get the same one you had before. This in itself isn't a problem. The idea is that you basically "reset" your network card to try to get it working again.

Administrative Tools

Microsoft has included a number of tools with each iteration of Windows to simplify administrative tasks. Although some tools have specific purposes and are used only on rare occasions, there are a number of them that you will come to rely on and access on a regular basis. It is this latter set that we will examine in this section, and they include Task Manager, the MMC, the Event Viewer, Computer Management, Services, and Performance Monitor.

Task Manager

This tool lets you shut down nonresponsive applications selectively in all Windows versions. Ever since Windows 2000, it has also been able to do so much more: it allows you to see which processes and applications are using the most system resources, view network usage, see connected users, and so on. To display Task Manager, press Ctrl+Alt+Delete and click the Task Manager button to display it (in earlier Windows versions, you needed only press Ctrl+Alt+Delete). In Windows 2000, you then have to click Task Manager on the Windows Security screen. In Windows XP, whether the Security screen displays depends on whether you're using the Windows XP Welcome screen (you can change this setting on the Screen Saver tab of the computer's Display Properties). By default, in Windows XP and Vista, the Windows Security screen does not display if you press Ctrl+Alt+Del; instead, Task Manager opens right away or you are given a set of tasks, of which Start Task Manager is one.

You can also right-click on an empty spot in the taskbar and choose it from the pop-up menu that appears.

To get to the Task Manager directly in any of the Windows versions that include it, you can press Ctrl+Shift+Esc.

In Windows 2000, the Task Manager has three tabs: Applications, Processes, and Performance. In versions since then, Task Manager can include two additional tabs: Networking and Users. The Networking tab is shown only if your system has a network card installed (it is rare to find one that doesn't). The Users tab is displayed only if the computer you are working on has Fast User Switching enabled, and is a member of a workgroup or is a stand-alone computer. The Users tab is unavailable on computers that are members of a network domain. Let's look at these tabs in more detail:

Applications The Applications tab lets you see which tasks are open on the machine. You also see the status of each task, which can be either Running or Not Responding. If a task/application has stopped responding (that is, it's hung), you can select the task in the list and click End Task. Doing so closes the program, and you can try to open it again. Often, although certainly not always, if an application hangs you have to reboot the computer to prevent the same thing from happening again shortly after you restart the application. You can also use the Applications tab to switch to a different task or create new tasks.

Processes The Processes tab lets you see the names of all the processes running on the machine. You also see the user account that's running the process, as well as the amount of CPU and RAM resources that each process is using. To end a process, select the process in the list and click End Process. Be careful with this choice since ending some processes can cause Windows to shut down. If you don't know what a particular process does, you can look for it in any search engine and find a number of sites that will explain it.

Performance The Performance tab contains a variety of information, including overall CPU usage percentage, a graphical display of CPU usage history, page-file usage in MB, and a graphical display of page-file usage. This tab also provides you with additional memory-related information such as physical and kernel memory usage, as well as the total

number of handles, threads, and processes. Total, limit, and peak commit-charge information also displays. Some of the items are beyond the scope of this book, but it's good to know that you can use the Performance tab to keep track of system performance. Note that the number of processes, CPU usage percentage, and commit charge always display at the bottom of the Task Manager window, regardless of which tab you have selected.

Networking The Networking tab provides you with a graphical display of the performance of your network connection. It also tells you the network adapter name, link speed, and state. If you have more than one network adapter installed in the machine, you can select the appropriate adapter to see graphical usage data for that adapter.

Users The Users tab provides you with information about the users connected to the local machine. You'll see the username, ID, status, client name, and session type. You can right-click on any connected user to perform a variety of functions, including sending the user a message, disconnecting the user, logging off the user, and initiating a remote control session to the user's machine.

Use Task Manager whenever the system seems bogged down by an unresponsive application.

MMC

Microsoft created the Microsoft Management Console (MMC) interface as a front-end that you can run administrative tools in. Many administrators don't even know that applications they use regularly run within an MMC. To start a blank MMC, choose Start ➢ Run, and then type `MMC` and press Enter. If you are running Windows Vista, the User Account Control will ask for verification that you want to start the Microsoft Management Console, and once you click Continue, it will appear.

An easy thing to do at this point is choose Open on the File menu and pick any existing MMC (all have an `.msc` extension). Figure 3.13, for example, shows the Services MMC that is discussed later in this section.

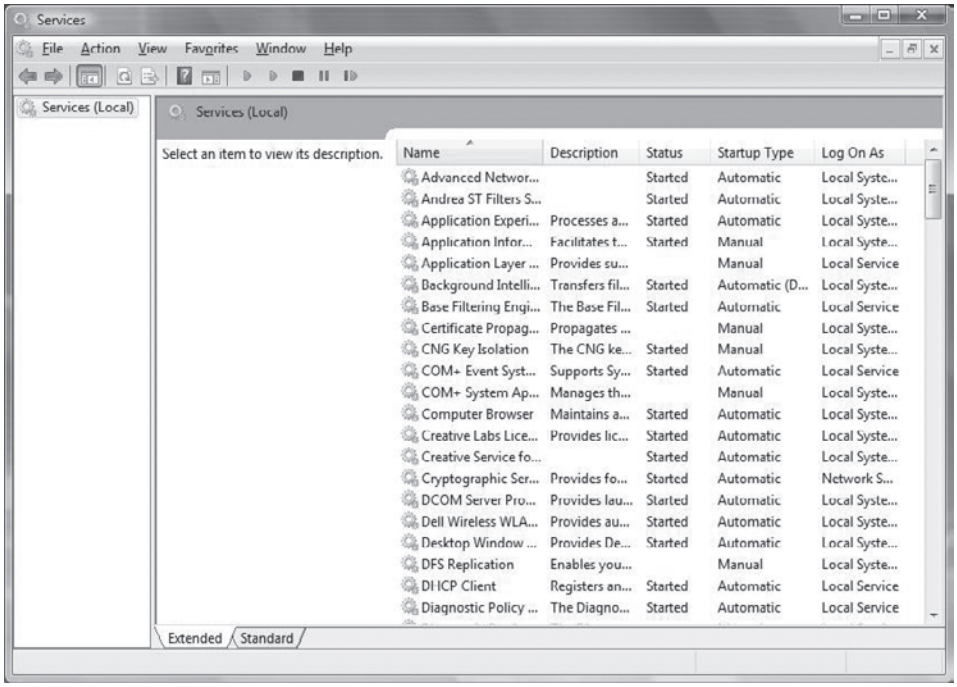
Event Viewer

Windows 2000, XP, and Vista employ comprehensive error and informational logging routines. Every program and process theoretically could have its own logging utility, but Microsoft has come up with a rather slick utility, the Event Viewer, which, through log files, tracks all events on a particular Windows computer. Normally, though, you must be an administrator or a member of the Administrators group to have access to the Event Viewer.

To start the Event Viewer, log in as an administrator (or equivalent) and choose Start ➢ Programs ➢ Administrative Tools ➢ Event Viewer (or right-click My Computer and choose Manage ➢ Event Viewer). In the resulting window, you can view the System, Application, and Security log files:

- The System log file displays alerts that pertain to the general operation of Windows.
- The Application log file logs application errors.
- The Security log file logs security events such as login successes and failures.

FIGURE 3.13 The Services application running within the MMC



These log files can give a general indication of a Windows computer's health.

One situation that does occur with the Event Viewer is that the log files get full. Although this isn't really a problem, it can make viewing log files confusing because there are so many entries. Even though each event is time- and date-stamped, you should clear the Event Viewer every so often. To do this, open the Event Viewer and choose Clear All Events from the Log menu. Doing so erases all events in the current log file, allowing you to see new events more easily when they occur. You can set maximum log size by right-clicking on the log and choosing Properties. By default, when a log fills to its maximum size, old entries are deleted in first in, first out (FIFO) order.

You can save the log files before erasing them. The saved files can be burned to a CD or DVD for future reference. Often, you are required to save the files to CD or DVD if you are working in a company that adheres to strict regulatory standards.

Computer Management

Windows 2000, XP, and Vista include a piece of software to manage computer settings: the Computer Management Console. The Computer Management Console can manage more than just the installed hardware devices; in addition to a Device Manager that functions

almost identically to the one that has existed since Windows 9*x*, the Computer Management Console can also manage all the services running on that computer. It contains an Event Viewer to show any system errors and events, as well as methods to configure the software components of all the computer's hardware.

To access the Computer Management Console in Windows 2000, choose Start ➢ Settings ➢ Control Panel ➢ Administrative Tools ➢ Computer Management. In Windows XP and Vista, you can access Control Panel through the Start button directly. In both operating systems, you can also access Computer Management by right-clicking the My Computer icon and choosing Manage.

After you are in Computer Management, you will see all of the tools available. This is one power-packed interface, which includes the following system tools:

Device Manager This tool lets you manage hardware devices.

Event Viewer This is a link to the previously discussed tool that allows you to view application error logs, security audit records, and system errors.

Shared Folders This allows you to manage all of your computer's shared folders.

Local Users and Groups This allows you to create and manage user and group accounts.

Performance Logs and Alerts This shows you how your system hardware is performing, and alerts you if system performance goes under a threshold you set.

Computer Management also has the Storage area, which lets you manage removable media, defragment your hard drives, or manage partitions through the Disk Management utility. Finally, you can manage system services and applications through Computer Management as well.

Services

This tool is an MMC snap-in that allows you to interact with the services running on the computer. In Windows 2000, for example, select Start ➢ Settings ➢ Control Panel ➢ Administrative Tools, then choose Services, and you will see the services configured on the system. The status of the services will typically either be started or stopped, and you can right-click and choose Start, Stop, Pause, Resume, or Restart from the context menu. Services can be started automatically or manually, or they can be disabled. If you right-click on the service and choose Properties from the context menu, you can choose the startup type as well as see the path to the executable and any dependencies.

Performance Monitor

Performance Monitor differs a bit in versions, but has the same purpose throughout: to display performance counters. While lumped under one heading, there are really two tools available—System Monitor and Performance Logs And Alerts. System Monitor will show the performance counters in graphical format. The Performance Logs And Alerts utility will collect the counter information and then send it to a console (such as the one in front of the admin so they can be aware of the problem) or event log.

The Registry

Windows configuration information is stored in a special configuration database known as the *Registry*. This centralized database contains environmental settings for various Windows programs. It also contains registration information that details which types of file extensions are associated with which applications. So, when you double-click a file in Windows Explorer, the associated application runs and opens the file you double-clicked.

The Registry was introduced with Windows 95. Most OSs up until Windows 95 were configured through text files, which can be edited with almost any text editor. However, the Registry database is contained in a special binary file that can be edited only with the special Registry Editor provided with Windows.

Windows 2000, XP, and Vista have two applications that can be used to edit the Registry: Regedit and Regedt32 (with no *i*). In Windows XP and Vista, Regedt32 opens Regedit. They work similarly, but each has slightly different options for navigation and browsing. In addition, Regedt32 allows you to configure security-related settings for Registry keys, such as assigning permissions.

The Registry is broken down into a series of separate areas called *hives*. These keys are divided into two basic sections—user settings and computer settings. In Windows, a number of files are created corresponding to each of the different hives. Most of these files do not have extensions, and their names are `system`, `software`, `security`, `sam`, and `default`. One additional file that does have an extension is `NTUSER.DAT`.

The basic hives of the Registry are as follows:

`HKEY_CLASSES_ROOT` Includes information about which file extensions map to particular applications.

`HKEY_CURRENT_USER` Holds all configuration information specific to a particular user, such as their Desktop settings and history information.

`HKEY_LOCAL_MACHINE` Includes nearly all configuration information concerning the actual computer hardware and software.

`HKEY_USERS` Includes information about all users who have logged on to the system. The `HKEY_CURRENT_USER` hive is actually a subkey of this hive.

`HKEY_CURRENT_CONFIG` Provides quick access to a number of commonly needed keys that are otherwise buried deep in the `HKEY_LOCAL_MACHINE` structure.

Modifying a Registry Entry

If you need to modify the Registry, you can modify the values in the database or create new entries or keys. You will find the options for adding a new element to the Registry under the Edit menu. To edit an existing value, double-click the entry and modify it as needed. You need administrative-level access to modify the Registry.

Windows uses the Registry extensively to store all kinds of information. Indeed, the Registry holds most, if not all, of the configuration information for Windows. Modifying the Registry in Windows is a potentially dangerous task. Control Panel and other configuration tools are provided so you have graphical tools for modifying system settings. Directly modifying the Registry can have unforeseen—and unpleasant—results. You should only modify the Registry when told to do so by an extremely trustworthy source or if you are absolutely certain you have the knowledge to do so without causing havoc in the Registry. Always bear in mind that Regedit does not have "Save" or "Undo" features; once you make a change, you've made the change for better or worse, and this is not a place to play around in if you're not sure what you're doing.

Restoring the Registry

Windows 2000, XP, and Vista store Registry information in files on the hard drive. You can restore this information using the *Last Known Good Configuration* option, which restores the Registry from a backup of its last functional state. Here's how to use this option:

- Press F8 during startup and then select Last Known Good Configuration from the menu that appears. You can also back up the Registry files to the `systemroot\repair` directory by using the Windows Backup program, or you can save them to tape during a normal *backup*. To repair the Registry from a backup, overwrite the Registry files in `systemroot\system32\config`.
- In Windows 2000, creating an *emergency repair disk* (ERD) also backs up the Registry files (to floppy disk, in this case). To create an ERD, in Windows 2000, use the Backup utility.
- In Windows XP the ERD has been replaced with *Automated System Recovery* (ASR), which is accessible through the Backup utility.

Note that ERD and ASR are considered last-resort options for system recovery.

System Files Configuration Tools

The MSConfig system configuration tool that was available in Windows 9*x* doesn't exist in Windows 2000. It is, however, included with Windows XP and Vista. Some tabs in the Windows XP and Vista versions of MSConfig are the same as those available in the Windows 9*x* version, such as General, `SYSTEM.INI`, `WIN.INI`, and Startup. New tabs in the Windows XP version include `BOOT.INI` and Services. The Boot.ini tab lets you modify the `BOOT.INI` file and also specify other boot options. On the Services tab, you can view the services installed on the system and their current status (running or stopped). You can also enable and disable services as necessary.

If you want to use the MSConfig configuration tool on a Windows computer system lacking it, you can do so by copying `MSCONFIG.EXE` from a Windows XP or Vista computer to the Windows 2000 computer.

The MSinfo32 tool, shown in Figure 3.14, displays a fairly thorough list of settings on the machine. You cannot change any values from here, but you can search, export, save, and run a number of utilities (located beneath the Tools menu option). There are a number of command-line options that can be used when starting MSinfo32, as summarized in Table 3.4.

FIGURE 3.14 The MSinfo32 interface shows configuration values for the system.

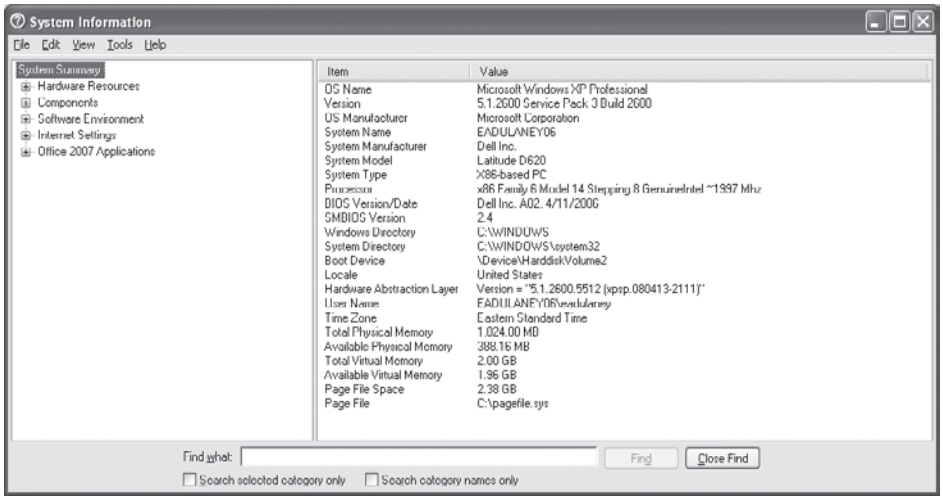


TABLE 3.4 MSinfo32 Command-Line Options for Windows XP and Vista

Option	Function
`/category` (available only in Windows XP)	Specifies a category to be selected when the utility starts
`/computer`	Allows you to specify a remote computer to run the utility on
`/nfo`	Creates a file and saves it in NFO format
`/pch` (available only in Windows XP)	Displays the history view
`/report`	Creates a file and saves it in TXT format

TABLE 3.4 MSinfo32 Command-Line Options for Windows XP and Vista *(continued)*

Option	Function
`/showcategories` (available only in Windows XP)	Shows category IDs instead of friendly names
/? (available only in Windows XP)	Shows the command-line options available for use with the utility

Another utility to know is the DxDiag (DirectX Diagnostic) tool, shown in Figure 3.15. This tool (which can be summoned alone or from the Tools menu of MSinfo32) allows you to test DirectX functionality. When started, you can also verify that your drivers have been signed by Microsoft, as shown in Figure 3.16. DirectX is a collection of application programming interfaces (APIs) related to multimedia.

FIGURE 3.15 The DxDiag tool lets you test functionality with DirectX components.

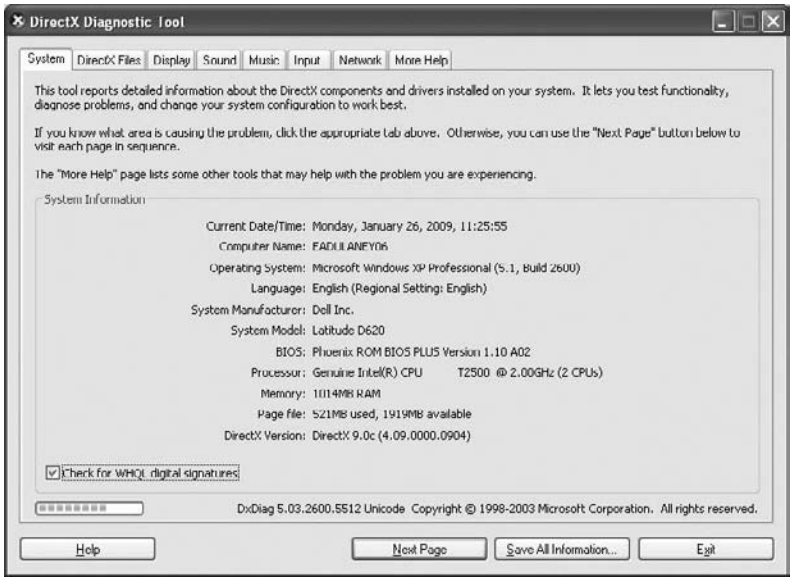


FIGURE 3.16 Verification that drivers have been signed

Exam Essentials

Know the major functions of Windows. You should understand what an OS does, which systems it manages, and how it communicates with the human user.

Know the key utilities. CompTIA has a list of utilities they consider to be key for all administrators to know, and they are listed in the objectives. Make certain you know of each of these utilities and what purpose each serves.

Be able to identify Windows display components. Make sure you can point out the Taskbar, Start button, System Tray, Desktop, and other key features of the OS interface.

Understand version differences. Be able to group the Windows versions according to similarity and explain how one group differs from the other.

Configuring Windows

This objective expects you to know the minimum requirements for the operating systems and different ways to install them. You should know the information at the level it is presented here. You aren't expected to know much about them beyond the basic knowledge level.

Critical Information

The operating systems focused on in this objective are Windows 2000, Windows XP, and Windows Vista. Earlier in this chapter, Tables 3.1 and 3.2 listed the minimum system requirements for these operating systems; this section focuses more on installation methods and options.

Before performing any installation or upgrade, you must back up your existing files to removable media. Doing so provides you with an insurance policy in the event of an unforeseen disaster and is highly recommended.

Given the timing of these updates, and the pending release of Windows 7, you may question the need to know this information. Nevertheless, it's included on the CompTIA test, and you should know the information given here in order to pass this exam.

File Systems

Before discussing installation, you need to know a bit about the files systems and directory structures. The file system is the organizational scheme that governs how files are stored on and retrieved from a disk. There are four major file systems: the original 16-bit FAT

system (a carryover from MS-DOS); the 32-bit version of it called FAT32; the NT File System (NTFS 4.0) supported by Windows NT 4.0; and the improved version of NTFS called NTFS 5.0, supported by Windows 2000, XP, and Vista. Table 3.5 lists some of the file systems and the Microsoft OSs that support them.

TABLE 3.5 Major File Systems

Operating System	FAT16	FAT32	NTFS 4.0	NTFS 5.0
Windows 2000	Yes	Yes	No (must convert)	Yes
Windows XP	Yes	Yes	No (must convert)	Yes
Windows Vista	Yes	Yes	No	Yes

For a hard disk to be able to hold files and programs, it has to be partitioned and formatted. Partitioning is the process of creating logical divisions on a hard drive. A hard drive can have one or more partitions. Formatting is the process of creating and configuring a file allocation table and creating the root directory. Several file system types are supported by the various versions of Windows, such as FAT16, FAT32, and NTFS. Windows 9*x*, Windows Me, and newer use FAT32, but they recognize and support FAT16. Windows NT, 2000, XP, and Vista also support a newer, more robust file system type called NTFS (New Technology File System) and recognize and support FAT16 and FAT32. The file table for the NTFS is called the Master File Table (MFT).

FAT32 Introduced with Windows 95 Release 2, FAT32 is similar to FAT (also known as FAT16) but has a number of advantages. It supports larger drives and smaller allocation units. As a comparison of how the new system saves you space, a 2GB drive with FAT16 has clusters of 32KB; with FAT32, the clusters sizes are 4KB. If you save a 15KB file, FAT needs to allocate an entire 32KB cluster; FAT32 uses four 4KB clusters, for a total of 16KB. FAT32 wastes an unused 1KB, but FAT wastes 15 times as much!

The disadvantage of FAT32 is that it isn't compatible with older DOS, Windows 3.*x*, and Windows 95 OSs. This means that when you boot a Windows 95 Rev B. or Windows 98 FAT32-formatted partition with a DOS boot floppy, you can't read the partition.

Windows 98 includes the FAT32 Drive Converter tool (`CVT1.EXE`), which allows you to upgrade FAT disks to FAT32 without having to reformat them. This preserves all the information on the drive but allows you to take advantage of FAT32's enhancements.

NTFS4 Windows NT's file system, NTFS4, includes enhanced attributes for compressing files or for setting file security. Updating a FAT drive to NTFS is relatively easy and can be done through a command called `CONVERT`. This conversion doesn't destroy any information but updates the file system. NTFS4 is used only with Windows NT 4.0.

NTFS5 The NTFS system updated with Windows 2000, NTFS5 includes enhancements such as file encryption. NTFS5 also includes support for large drive sizes and a new feature called Dynamic Disks that does away with the concept of partitioning to improve drive performance. NTFS5 is used only with Windows 2000, XP, Vista, and the latest Windows Server versions; it was not available in earlier Windows operating systems.

When you're installing any Windows OS, you will be asked first to format the drive using one of these disk technologies. Choose the disk technology based on what the computer will be doing and which OS you are installing.

To create a FAT16 or FAT32 partition, you can use the `FDISK` command. To format a partition, you can use the `FORMAT` command. `FDISK.EXE` is available only with Windows 9*x* and Me (not 2000, XP, or Vista), and you can run it from a command prompt. `FORMAT.EXE` is available with all versions of Windows. You can run `FORMAT` from a command prompt or by right-clicking a drive in Windows Explorer and selecting Format. However, when you install Windows it performs the process of partitioning and formatting for you if a partitioned and formatted drive does not already exist.

Be extremely careful with the `FORMAT` command! When you format a drive, all data on the drive is erased.

In Windows 2000, XP, and Vista, you can manage your hard drives through the Disk Management component. To access Disk Management, access Control Panel and double-click Administrative Tools. Then double-click Computer Management. Finally, double-click Disk Management.

The Disk Management screen lets you view a host of information regarding all the drives installed in your system, including CD-ROM and DVD drives. The list of devices in the top portion of the screen shows you additional information for each partition on each drive, such as the file system used, status, free space, and so on. If you right-click a partition in either area, you can perform a variety of functions, such as formatting the partition and changing the name and drive letter assignment. For additional options and information, you can also access the properties of a partition by right-clicking it and selecting Properties.

Windows 2000, XP Professional, and Vista support both basic and dynamic storage. Basic supports only one partition, while dynamic can be simple, spanned, or striped. Spanning allows for space from multiple disks to be combined into a single volume but does not include any redundancy. Striping is similar in that it combines spaces from two or more drives, but it also incorporates some redundancy.

The partition that the operating system boots from must be designated as *active*. Only one partition on a disk may be marked active. With basic storage, Windows 2000, XP Professional, and Vista drives can be partitioned with *primary* or *extended* partitions. The difference is that extended partitions can be divided into one or more logical drives and primary partitions cannot be further subdivided. Each 2000, XP Professional, and Vista hard disk can be divided into a total of four partitions, either four primary partitions or three primary and one extended partition.

Finally, there is the concept of a *logical partition*. In reality, all partitions are logical in the sense that they don't necessarily correspond to one physical disk. One disk can have several logical divisions (partitions). A logical partition is any partition that has a drive letter.

Sometimes, you will also hear of a logical partition as one that spans multiple physical disks. For example, a network drive that you know as drive H: might actually be located on several physical disks on a server. To the user, all that is seen is one drive, or H:.

The basic unit of storage is the disk. Disks are partitioned (primary, logical, extended) and then formatted for use. With the Windows operating systems this exam focuses on, you can choose to use either FAT32 or NTFS; the advantage of the latter is that it offers security and many other features that FAT32 can't handle.

If you're using FAT32 and want to change to NTFS, the convert utility will allow you to do so. For example, to change the E: drive to NTFS, the command is `convert e: /FS:NTFS`.

Once the disk is formatted, the next building block is the directory structure, in which you divide the partition into logical locations for storing data. Whether these storage units are called directories or folders is a matter of semantics—they tend to be called *folders* when viewed in the graphical user interface (GUI) and *directories* when viewed from the command line.

Files and Folders

For a program to run, it must be able to read information off the disk and write information back to the disk. To be able to organize and access information—especially in larger new systems that may have thousands of files—it is necessary to have a structure and an ordering process.

Windows provides this process by allowing you to create *directories*, also known as *folders*, in which to organize files. Windows also regulates the way that files are named and the properties of files. Each file created in Windows has to follow certain rules, and any program that accesses files through Windows also must comply with these rules. Files created on a Windows system must follow these rules:

- Each file has a filename of up to 255 characters.
- Certain characters, such as a period (.) and slash (\ or /), are reserved for other uses and cannot be used in the filename. This is because periods are used to separate the filename from the extension and the backslash is used to separate the directories in a filename.
- An extension (generally three or four characters) can be added to identify the file's type.

- Filenames are not case sensitive. (You can create files with names that use both upper- and lowercase letters, but to identify the file within the file system, it is not necessary to adhere to the capitalization in the filename.) Thus, you cannot have a file named `working.txt` and another called `WORKING.TXT` in the same directory. To Windows, these filenames are identical, and you can't have two files with the same filename in the same directory. We'll get into more detail on this topic a little later.
- In Windows 3.*x* and DOS, filenames were limited to eight characters and a three-character extension, separated by a period. This is also called the 8.3 file-naming convention. With Windows 95, long filenames were introduced, which allowed the 255-character filename convention.

The Windows file system is arranged like a filing cabinet. In a filing cabinet, paper is placed into folders, which are inside dividers, which are in a drawer of the filing cabinet. In the Windows file system, individual files are placed in subdirectories that are inside directories, which are stored on different disks or different partitions.

Windows also protects against duplicate filenames, so no two files on the system can have exactly the same name and *path*. A path indicates the location of the file on the disk; it is composed of the logical drive letter the file is on and, if the file is located in a directory or subdirectory, the names of those directories. For instance, if a file named `AUTOEXEC.BAT` is located in the root of the C: drive—meaning it is not within a directory—the path to the file is `C:\AUTOEXEC.BAT`. If, as another example, a file called `FDISK.EXE` is located in the `Command` directory under Windows under the root of C:, then the path to this file is `C:\WINDOWS\COMMAND\FDISK.EXE`.

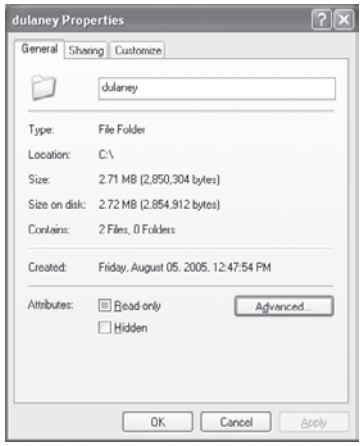
The *root directory* of any drive is the place where the hierarchy of folders for that drive begins. On a C: drive, for instance, `C:\` is the root directory of the drive.

Among the common file extensions you may encounter are `.EXE` for executable files (applications), `.DLL` for dynamic linked library (DLL) files, `.SYS` for system files, `.LOG` for log files, `.DRV` for driver files, and `.TXT` for text files. Note that DLL files contain additional functions and commands applications can use and share. In addition, most applications use specific file extensions for the documents created with each application. For example, documents created in Microsoft Word have a `.DOC` or `.DOCX` extension. You'll also encounter extensions such as `.MPG` for video files, `.MP3` for music files, `.TIF` and `.JPG` for graphics files, `.HTM` or `.HTML` for web pages, and so on. Being familiar with different filename extensions is helpful in working with the Windows file system.

You can create directories from the command line using the `MD` command and from within the GUI by right-clicking in a Windows Explorer window and choosing New ➢ Folder. Once the folder exists, you can view/change its properties, as shown in Figure 3.17, by right-clicking the icon of its folder and choosing Properties.

In the Attributes section, you can choose to make the directory read-only or hidden. By clicking the Advanced button, you can configure indexing, archiving, encryption, and compression settings. The Advanced button is only available if the file resides on an NTFS volume.

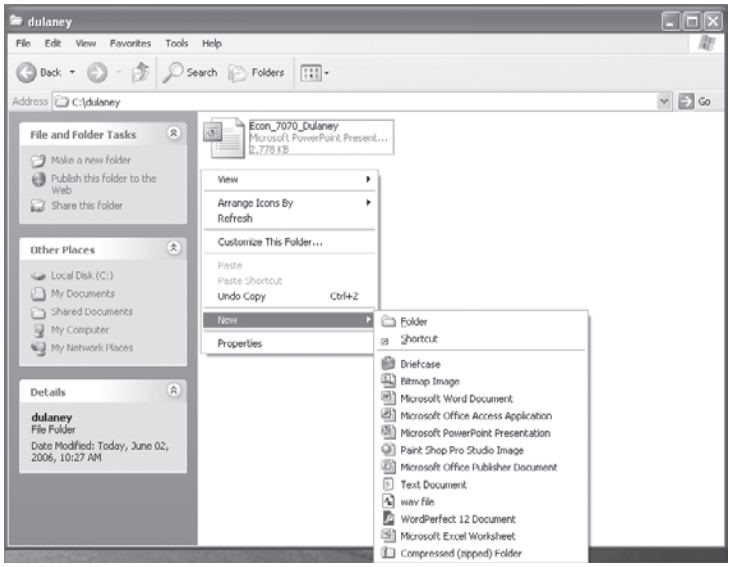
FIGURE 3.17 You can change the attributes associated with a directory.



Even though encryption and compression settings appear in the same frame on the dialog box, the two features are mutually exclusive.

Within directories are files. You can create a file either from within an application or by right-clicking, choosing New, and then selecting the type of item you want to create, as shown in Figure 3.18.

FIGURE 3.18 You can create files of various types with a right-click.



Once the file has been created, you can right-click the file's icon and change properties and permissions associated with the file by choosing Properties from the context menu.

Changing File Attributes

File attributes determine what specific users can do to files or directories. For example, if a file or directory is flagged with the Read Only attribute, then users can read the file or directory but not make changes to it or delete it. Attributes include Read Only, Hidden, System, and Archive, as well as Compression, Indexing, and Encryption. Not all attributes are available with all versions of Windows. We'll look at this subject in more detail in a moment.

Some attributes, such as Read Only, Hidden, System, and Archive, date back to DOS. All others, such as Compression, Indexing, and Encryption, are a part of NTFS.

You can view and change file attributes either with the `ATTRIB` command-prompt command or through the properties of a file or directory. To access the properties of a file or directory in the Windows GUI, right-click the file or directory and select Properties. In Windows XP, you can view and configure the Read Only and Hidden file attributes on the General tab. To view and configure additional attributes, click Advanced.

System files are usually flagged with the Hidden attribute, meaning they don't appear when a user displays a directory listing. You should not change this attribute on a system file unless absolutely necessary. System files are required for the OS to function. If they are visible, users might delete them (perhaps thinking they can clear some disk space by deleting files they don't recognize). Needless to say, that would be a bad thing!

File System Advanced Attributes

Windows 2000, XP, and Vista use the NT File System (NTFS), which gives you a number of options that are not available on earlier file systems, such as FAT or FAT32. A number of these options are implemented through the use of the Advanced Attributes window. To reach these options in Windows 2000, XP, or Vista, right-click the folder or file you wish to modify and select Properties from the context menu. On the main Properties page of the folder or file, click the Advanced button in the lower-right corner.

On the Advanced Attributes screen, you have access to the following settings:

Archiving This option tells the system whether the file has changed since the last time it was backed up. Technically it is known as the Archive Needed attribute; if this box is selected, the file should be backed up. If it is not selected, a current version of the file is already backed up.

Indexing Windows 2000, XP, and Vista implement an Index Service to catalog and improve the search capabilities of your drive. Once files are indexed, you can search them more quickly by name, date, or other attributes. Setting the index option on a folder causes a prompt to appear, asking whether you want the existing files in the folder to be indexed as well. If you choose to do this, Windows 2000, XP, and Vista automatically reset this attribute on subfolders and files. If not, only new files created in the directory are indexed.

Compression Windows 2000, XP, and Vista support advanced *compression* options, which were first introduced in Windows NT. NTFS files and folders can be dynamically compressed and uncompressed, often saving a great deal of space on the drive. As with Indexing, turning on Compression for a folder results in a prompt asking whether you want the existing files in the folder to be compressed. If you choose to do this, Windows automatically compresses the subfolders and files. If not, only new files created in the directory are compressed.

Compression works best on such files as word-processing documents and uncompressed images. Word files and Microsoft Paint bitmaps can be compressed up to 80 percent. Files that are already packed well do not compress as effectively; EXE and zip files generally compress only about 2 percent. Similarly GIF and JPEG images are already compressed (which is why they are used in Internet web pages), so they compress a little or not at all.

Encryption First introduced in Windows 2000 and also available in Windows XP and Vista, *encryption* lets you secure files so that no one else can view them. You simply encode the files with a key that only you have access to. This can be useful if you're worried about extremely sensitive information, but in general, encryption is not necessary on the network. NTFS local file security is usually enough to provide users with access to what they need and to prevent others from getting to what they shouldn't. If you want to encrypt a file, go through the same process you would for indexing or compression.

Encryption and Compression are mutually exclusive—you can set one but not both features on a file or folder. Neither feature is available in XP Home Edition.

If a user forgets their password or is unable to access the network to authenticate their account, they will not be able to open encrypted files. By default, if the user's account is lost or deleted, the only other user who can decrypt the file is the Administrator account.

File Permissions

Windows 2000, XP, and Vista also support the use of *file permissions*, because these OSs can use NTFS, which includes file-level file system security (along with share-level security). Permissions serve the purpose of controlling who has access and what type of access to what files or folders. Several permissions are available, such as Read, Write, Execute, Delete, Change Permissions, Take Ownership, Full Control, and so on. The list is quite extensive. For a complete list, consult the Windows Help files. These permissions are called *special permissions*.

Assigning special permissions individually could be a tedious task. To make it easier for administrators to assign multiple permissions at once, Windows incorporates *standard permissions*. Standard permissions are collections of special permissions, including Full Control, Modify, Read & Execute, Read, and Write. As we said, each of these standard permissions automatically assigns multiple special permissions at once. To see which special permissions are assigned by the different standard permissions, enter **File Permissions (List)** into the Help system's index keyword area.

Note that you can assign permissions to individual users or to groups. You assign standard permissions on the Security tab of a file or folder, which you access through the file or folder's properties.

Be sure you don't make any changes you don't intend to make. Changing permissions without understanding the ramifications can have negative consequences, such as losing access to files or folders.

Installing Operating Systems

Operating systems can be installed in two generic ways: attended or unattended. During an attended installation, you walk through the installation and answer the questions as prompted. Questions typically ask for the product key, the directory in which you want to install the OS, and relevant network settings.

As simple as attended installations may be, they're time-consuming and administrator-intensive in that they require someone to fill in a fair number of fields to move through the process. Unattended installations allow you to configure the OS with little or no human intervention. Windows 2000 Professional offers three main methods for performing unattended installations: Remote Installation Service (RIS), System Preparation Tool, and Setup Manager.

The RIS is a service that runs on a Windows 2000 Server. Client machines to be converted to Windows 2000 Professional access the server service and run the installation across the network.

The System Preparation Tool takes a completely different approach. `Sysprep.exe` is used to prepare an ideal Windows 2000 Professional workstation so that an image can be made of it (this requires a third-party utility). That image, which lacks user/computer-specific information and SIDs (Security IDs), can then be loaded on other computers.

Setup Manager is used to create answer files (known as uniqueness database files [UDFs]) for automatically providing computer or user information during setup. Setup Manager, like Sysprep, isn't installed on the system by default but is stored within the `Deploy` cabinet file on the CD beneath `Support\Tools`.

Windows XP offers similar installation options. For the exam, you should be familiar with the attended installation and know that the other methods exist.

Information on minimum hardware requirements was found earlier in this chapter, in the "Minimum System Requirements" section.

Working with Device Drivers

Device drivers are the software stubs that allow devices to communicate with the operating system. Called *drivers* for short, they're used for interacting with printers, monitors, network cards, sound cards, and just about every type of hardware attached to the PC. One of the most common problems associated with drivers isn't having the current version—as problems are fixed, the drivers are updated, and you can often save a great deal of time by downloading the latest drivers from the vendor's site early in the troubleshooting process.

Adding the `/sos` option to the `operating system` option in the `BOOT.INI` file will show the drivers as they're loaded in Windows 2000, XP, and Vista.

The easiest way to see or change drivers in Windows 2000, XP, and Vista is to click the Driver tab in the Properties dialog box for the device. For example, to see the driver associated with the hard drive in Windows XP, double-click the hard drive in Device Manager (Start ➢ Control Panel ➢ System, and then click the Hardware tab and the Device Manager button), and choose the Driver tab. Among other things, this shows the driver provider, date, version, and signer. You can choose to view details about it, update it, roll it back to a previous driver, or uninstall it.

Upgrading Operating Systems

If you add an OS to a machine that doesn't currently have one (recently formatted, built from scratch, and so on), that is *installing*. If you add an OS so that you can dual-boot (choose which one to run at start), that is *installing*. If you replace one OS with another and attempt to keep the same data/application files, that is *upgrading*.

Whereas installation can typically be done over any existing OS, upgrading can be done only from OSs that are generally compatible with the one you're adding. For example, with Windows 2000 upgrades can be done only from the following programs:

- Windows 95
- Windows 98
- Windows NT Workstation 3.51
- Windows NT Workstation 4.0

`WINNT32.EXE` is the utility to use to initiate the upgrade. The Setup Wizard automatically creates a report of devices that can't be upgraded. Keep in mind that you must uncompress any DoubleSpace or DriveSpace volumes before you start an upgrade.

With Windows XP, you can upgrade to the Home version only from Windows 98 or Windows Me. You can upgrade to the Professional version from Windows 98, Windows Me, Windows NT Workstation 4.0, Windows 2000 Professional, or even Windows XP Home.

Step-by-step upgrade information for Windows XP can be found at http://www.microsoft.com/windowsxp/using/setup/getstarted/default.mspx.

Migrating User Data

Installing an operating system would be simple if it weren't for users and the data that they want to bring with them. To simplify this task, Microsoft has offered a free tool for a number of years: Microsoft Windows User State Migration Tool (USMT). Now up to version 3.0, it allows you to migrate user files settings related to the applications, desktop configuration, and accounts.

Version 3.0 works with Windows XP and Vista, while previous versions, such as 2.6, also worked with Windows 2000. You can download this tool from Microsoft's download page. If all you are doing is a simple migration from one OS to another, you do not need this tool, but it is invaluable during large deployments.

Common Installation Problems

For the most part, the days of having to suffer through installation issues have passed. The wizards available in the Microsoft OSs tend to make installation errors much less common than they were with earlier operating systems. Several categories of errors and fixes that still crop up from time to time are as follows:

Installation Disk Errors Retry the installation once more. If the errors persist, change to a new installation DVD or CD.

Inadequate Disk Space Take corrective action to proceed with the installation, such as deleting temporary files or archiving old data.

Disk Configuration Errors Make sure you're using hardware compatible with the operating system by checking the HCL.

Failure to Connect to a Domain Controller Confirm the NIC is properly configured with a valid TCP/IP address. Verify that you're entering the correct username and password and that the Caps Lock key isn't on.

Domain Name Error Reselect or retype the correct domain name. Confirm the NIC is configured with the proper DNS server address.

Virtual Memory

Windows offers two types of memory: RAM and virtual memory. *RAM* is the physical (hardware) memory installed by means of chips. *Virtual memory* can include RAM and the hard drive (paging file); it allows Windows to run more applications than it has physical RAM for. In an ideal situation, Windows would have enough RAM for all the applications currently running, with a small amount of space to use for file caching. In other words, you can seldom go wrong by adding RAM, because it can improve disk performance by allowing you to hold more files in RAM, which allows for quicker access than from the hard drive. However, this will increase performance only when Windows has memory that isn't being used by applications.

You can use a couple of utilities to identify memory problems. The first is the Performance tool. The object to monitor is Memory, and the counters to watch include the following:

Committed Bytes This counter shows how much memory (virtual and physical) is in use. If this number always exceeds the physical RAM by more than a few megabytes, you probably don't have sufficient RAM. As the counter's value increases, the system will have to page memory in and out more frequently to keep the running programs in memory.

Pages/Sec This counter indicates how many pages per second are being moved to and from memory to satisfy requests. This number should be less than 100; a higher value can indicate that the system is RAM-starved. The counter won't drop to 0 even on a system that has plenty of RAM because some activity must always occur.

You can also gather memory statistics by using Task Manager. The Performance tab shows current utilization and a graph of recent history. A bar-graph icon appears in the System Tray when Task Manager is running. This is an active link to the CPU Usage graph on the Performance tab and can be used to visually gauge CPU activity even when Task Manager is minimized.

You can configure virtual memory parameters from the System applet in Control Panel. To access these settings, follow these steps:

1. Double-click the System applet in Control Panel.
2. Choose the Advanced tab, or in Vista, choose Advanced System Settings under Tasks.
3. In the Performance frame, click the Settings (for Windows XP) or Performance Options (for Windows 2000) button. With Windows XP, you must take the extra step of choosing the Advanced tab.
4. Click the Change button. The Virtual Memory dialog box appears.

The initial paging file size is the amount of contiguous space claimed at each boot. The paging file is dynamic and can always grow. However, if it grows into noncontiguous space, performance can be greatly degraded. It is, therefore, preferable to have the initial size set to a number larger than you expect the file size to grow to.

Keeping the System Current

Upgrades to Windows (all versions) come in the form of *service packs*. Each service pack contains patches and fixes to OS components, as well as additional features. A service pack is a self-running program that modifies your OS. It isn't uncommon within the lifetime of an OS to have two or three service packs.

Successive service packs include all files that have been in previous ones. Therefore, if you perform a new installation, and the latest service pack is Service Pack 4, you don't need to install Service Packs 1, 2, and 3. You need install only Service Pack 4 after the installation to bring the OS up to the current feature set.

As they're released, service packs are shipped monthly for all Microsoft OSs with TechNet. TechNet is a subscription CD service available through Microsoft.

Windows System Files

Among the things you must be familiar with in preparation for the A+ exam are the startup and system files used by Windows 2000, XP, and Vista. We will look at each of them individually, but Windows makes nosing around in the startup environment difficult, and so there is a change you need to make first.

To protect Windows system files from accidental deletion, and to get them out of the way of the average user, they are hidden from the user by default. Because of this, many of the files we are about to talk about will not be visible to you.

To make them visible, you need to change the display Properties of Windows Explorer. Windows 2000, XP, and Vista are all based on Windows NT, and therefore each of their boot processes uses the same key boot files as Windows NT did. In this section, we will discuss these files.

Key Boot Files

Windows 2000, XP, and Vista require only a few files, each of which performs specific tasks. We will discuss these in the order in which they load:

`NTLDR` This file bootstraps the system for Windows XP and 2000. In other words, this file starts the loading of an OS on the computer. In Windows Vista, BOOTMGR performs this operation.

`BOOT.INI` This file in Windows XP and Vista holds information about which OSs are installed on the computer. In Windows Vista, the Boot Configuration Data (BCD) file holds this information.

`BOOTSECT.DOS` In a dual-boot configuration, this file keeps a copy of the DOS or Windows 9*x* boot sector so that the Windows 9*x* environment can be restored and loaded as needed.

`NTDETECT.COM` This file parses the system for hardware information each time Windows 2000 or XP is loaded. This information is then used to create dynamic hardware information in the Registry.

`NTBOOTDD.SYS` On a system with a SCSI boot device, this file used to recognize and load the SCSI interface. On EIDE systems, this file is not needed and is not even installed.

`NTOSKRNL.EXE` This is the Windows OS kernel.

System Files In addition to the previously listed files, all of which except `NTOSKRNL.EXE` are located in the root of the C: partition on the computer, Windows 2000, XP, and Vista need a number of files from the system directories (e.g., `system` and `system32`), such as the hardware abstraction layer (`HAL.DLL`).

Numerous other DLL (dynamic link library) files are also required, but usually the lack or corruption of one of them produces a noncritical error, whereas the absence of `HAL.DLL` causes the system to be nonfunctional.

Power Management

The Advanced Configuration Power Interface (ACPI) must be supported by the system BIOS in order to work properly. With ACPI, it is the BIOS that provides the operating system with

the necessary methods for controlling the hardware. This is in contrast to APM (Advanced Power Management), which gave only a limited amount of power to the operating system and let the BIOS do all the real work. Because of this, it is not uncommon to find legacy systems that can support APM but not ACPI.

There are three main states of power management common in most operating systems:

Hibernate This state saves all the contents of memory to the hard drive and preserves all data and applications exactly where they are. When the system comes out of hibernation, it returns to its previous state.

Standby This state leaves memory active but saves everything else to disk.

Suspend In most operating systems, this term is used interchangeably with Hibernate. In Windows XP, Hibernate is used instead of Suspend.

We discussed the states that you can choose to place your system in (Sleep, Hibernate, etc.) earlier in this chapter. If you are interested in saving power with a system that is not accessed often, one option is to employ Wake On LAN (WoL). Wake On LAN is an Ethernet standard implemented via a card that allows a "sleeping" machine to awaken when it receives a wakeup signal.

Wake On LAN cards have more problems than standard network cards. In my opinion, this is because they're always on. In some cases, you'll be unable to get the card working again unless you unplug the PC's power supply and reset the card.

Safely Removing Peripherals

PC Card devices are designed to be easily removed and installed. They're approximately the size and shape of a thick credit card, and they fit into PC Card (PCMCIA) slots in the side of the notebook PC. PC Card devices can include modems, network interface cards (NICs), SCSI adapters, USB adapters, FireWire adapters, and wireless Ethernet cards.

To eject a PC Card device, press the eject button next to its slot. To insert a PC Card device, press the device into the slot. You can do this while the computer is running. (That's called *hot-plugging* or *hot-swapping*.) However, in Windows it's a good idea to stop the PC Card device before ejecting it, to ensure that all operations involving it complete normally. To do so, double-click the Safely Remove Hardware icon in the System Tray, click the device, and then click Stop.

Determining OS Installation Options

In addition to making sure you have enough and the right kind of hardware, you must determine a few of the Windows installation options. These options control how Windows will be installed, as well as which Windows components will be installed. These options include the following:

- Installation type
- Network configuration

- File system type
- Dual-boot support

Installation Type

When you install applications, OSs, or any software, you almost always have options as to how that software is installed. Especially with OSs, there are usually many packages that make up the software. You can choose how to install the many different components; these options are usually called something like Typical, Full, Minimal, and Custom:

- A *typical installation* installs the most commonly used components of the software, but not all of the components.
- A *full installation* installs every last component, even those that may not be required or used frequently.
- A *minimal installation* (also known as a *compact installation*) installs only those components needed to get the software functional.
- A *custom installation* usually allows you to choose exactly which components are installed.

Some Windows Setup programs include a *portable* installation type as well, which installs components needed for portable system installations on laptops. It includes such features as power management and LCD display software.

All Windows versions use these, or derivations of these installation types, and you should decide ahead of time which method you are going to use (which may be dictated by the amount of disk space you have available).

Network Configuration

With many versions of Windows, you can choose whether to install networking options. If you do install networking, you can also choose (with some versions of Windows) which networking components you want installed. With Windows 2000, XP, and Vista, you also must know which workgroup or domain you are going to install.

File System Type

As Windows has evolved, a number of changes have been made to the basic architecture, as you might expect. One of the architecture items that has changed the most is the disk system structure. When you're installing any Windows OS, you will be asked first to format the drive using one of the available file systems. Choose based on what the computer will be doing and which OS you are installing.

Dual-Boot Support

Occasionally, a mission-critical program (one you can't do your business or function without) doesn't support the OS to which you are upgrading. There may be a newer release in the

future, but at the present time it isn't supported. In that case, you may have to install the new OS in a dual-boot configuration.

It is also possible, in some situations, to have a multiboot configuration where you can choose from a list of OSs. However, this setup makes it more difficult to choose compatible disk formats and often requires multiple disks to accomplish properly.

In a *dual-boot configuration*, you install two OSs on the computer (Windows XP and Windows 2000, for example). At boot time, you have the option of selecting which OS you want to use.

It is possible to multiple-boot to all Microsoft OSs, including DOS and all versions of Windows. Microsoft recommends that each installation be done to a separate disk (or partition) in order to avoid conflicts with built-in programs like Internet Explorer. In addition, you should install the oldest OS first and then proceed in chronological order to the newest.

For more information on dual-boot and multiboot configurations, visit the Microsoft support website at `http://support.microsoft.com`.

Determining the Installation Method

Another decision you must make is which method you are going to use to install Windows. Most versions of Windows come on a CD. It was possible to install older versions of Windows using floppy disks. Granted, there were several disks (the first Windows 95 installation used 19 3.5″ floppy diskettes). However, this isn't the most efficient method. CDs and DVDs, because of their large storage capacity, are the perfect media to distribute software.

Windows 2000 and Windows XP each come on a single CD (not together, of course, but each on its own CD). Windows Vista is available on CD or DVD. It is possible to boot to this disk and begin the installation process. However, your system must have a system BIOS and be capable of supporting bootable media.

If you don't have a bootable CD or DVD, you must first boot the computer using some other bootable media, which then loads the disk driver so that you can access the installation program on the CD or DVD. With Windows 2000, these bootable disks usually come with the packaged operating system or can be made with the makeboot.exe command.

There's one more thing to consider when evaluating installation methods. Some methods work only if you're performing a clean installation and not an upgrade. Table 3.6 shows you four common unattended installation methods and when they can be used.

TABLE 3.6 Windows Unattended Installation Methods

Method	Clean Installation	Upgrade
Unattended Install	Yes	Yes
Sysprep	Yes	No
Bootable Media	Yes	No
Remote Install	Yes	No

Two common categories of installations are attended and unattended. In an *attended installation,* a user must be present to choose all of the options when the installation program gets to that point. As you can imagine, if you have several hundred computers to install, this isn't exactly efficient. The other option is an *unattended installation,* which does not require human intervention once started and is frequently used when installing over the network.

Let's look at each of these in a bit more detail.

Unattended Installation

Answering the myriad of questions posed by Windows Setup doesn't qualify as exciting work for most people. Fortunately, there is a way to answer the questions automatically, and it's through an unattended installation. In this type of installation, an *answer file* is supplied with all of the correct parameters (time zone, regional settings, administrator user name, and so on), so no one needs to be there to tell the computer what to choose or to hit Next 500 times.

Unattended installations are great because they can be used to upgrade operating systems to Windows 2000, XP, or Vista. The first step is to create an answer file. Generally speaking, you'll want to run a test installation using that answer file first before deploying it on a large scale, because you'll probably need to make some tweaks to it. After you create your answer file, place it on a network share that will be accessible from the target computer. (Most people put it in the same place as the Windows 2000, XP, or Vista installation files for convenience.)

Boot the computer that you want to install on using a boot disk, CD, or DVD, and establish the network connection. Once you start the setup process, everything should run automatically.

Sysprep

Another common unattended installation tool is the system preparation tool, or *sysprep*. The sysprep utility works by making an exact image or replica of a computer (called the *master*

computer) to be installed on other computers. Sysprep removes the master computer's Security ID, and will generate new IDs for each computer the image is used to install.

All sysprep does is create the system image. With Windows XP and 2000, you still need a third-party cloning utility to copy the image to other computers. Vista uses a new ImageX tool to provide this capability natively.

Perhaps the biggest caveat to using sysprep is that because you are making an exact image of an installed computer (including drivers and settings), all of the computers that you will be installing the image on need to be identical (or very close) to the configuration of the master computer. Otherwise, you could have to go through and fix driver problems on every installed computer. Sysprep images can be installed across a network or copied to a CD or DVD for local installation. Sysprep cannot be used to upgrade a system; plan on all data on the system (if there is any) being lost after a format.

Several third-party vendors provide similar services, and you'll often hear the service referred to as *disk imaging* or *drive imaging*. The process works the same way as sysprep, except that the third-party utility makes the image as well. Then the image file is transferred to the computer without an OS. You boot the new system with the imaging software and start the image download. The new system's disk drive is made into an exact sector-by-sector copy of the original system.

Imaging has major upsides. The biggest one is speed. In larger networks with multiple new computers, you can configure tens to hundreds of computers by using imaging in just hours, rather than the days it would take to individually install the OS, applications, and drivers.

Bootable Media

For computers not connected to a network, images can be copied to a CD or DVD for local installation. This is a quick way to perform a clean installation of an operating system without consuming all of your network bandwidth.

Remote Install

Windows 2000 Server and newer Windows Server operating systems have a feature called Remote Installation Service (RIS), which allows you to perform several network installations at one time. A *network installation* is handy when you have many installs to do and installing by CD is too much work for many computers.

In a network installation, the installation CD is copied to a shared location on the network. Then individual workstations boot and access the network share. The workstations can boot either through a boot disk or through a built-in network boot device known as a *boot ROM*. Boot ROMs essentially download a small file that contains an OS and network drivers and has enough information to boot the computer in a limited fashion. At the very least, it can boot the computer so it can access the network share and begin the installation.

Preparing the Computer for Installation

Once you have verified that the machine on which you are planning to install Windows is capable of running it properly, you're sure all hardware is supported, and you have chosen your installation options, you need to make certain that the system is ready for the install. The primary question is whether you are planning to perform a fresh install of Windows or whether you are going to upgrade an existing system. For now, we'll focus on new installations.

Preparing the Hard Drive

If you are installing Windows onto a system that does not already have a functioning OS, you have a bit of work to do before you get to the installation itself. New disk drives need two critical functions performed on them before they can be used—partitioning and formatting—both of which were discussed previously. With older operating systems, you dealt with these two procedures by using the `FDISK.EXE` and `FORMAT.COM` commands. Running any sort of command on a machine that has no OS is impossible, though. You need a way to boot the computer—usually with a disk that is bootable.

For Windows 2000, XP, and Vista, the process will always be to boot up (which starts the installation process), partition the drive, and then format the drive.

Partitioning the Hard Drive

Partitioning refers to establishing large allocations of hard drive space. A partition is a continuous section of sectors that are next to each other. In DOS and Windows, a partition is referred to by a drive letter, such as C: or D:. Partitioning a drive into two or more parts gives it the appearance of being two or more physical hard drives. At the beginning of each hard drive is a special file called the *master boot record* (MBR). The MBR contains the partition information about the beginning and end of each partition.

The size of a partition determines certain aspects of a file pointer table called the File Allocation Table (FAT). The larger the drive partition, the more space will be wasted on the drive. NTFS partitions are less wasteful of space than FAT partitions are, because of limitations in FAT cluster sizes.

Formatting the Hard Drive

The next step in management of a hard drive is formatting, initiated by the `FORMAT` command (or automatically by the installation program). When formatting is performed, the surface of the hard drive platter is briefly scanned to find any possible bad spots, and the areas surrounding a bad spot are marked as bad sectors. Then magnetic tracks are laid down in concentric circles. These tracks are where information is eventually encoded. These tracks, in turn, are split into pieces of 512 bytes called *sectors*. Some space is reserved in between the sectors for error-correction information, referred to as cyclic redundancy check (CRC) information. The OS may use CRC information to re-create data that has been partially lost from a sector. An operating system boot record is created along with the root directory. Finally, the File

Allocation Table (FAT) or Master File Table (MFT) is created. This table contains information about the location of files as they are placed onto the hard drive.

The installation processes for operating systems has, arguably, gotten easier over time. Being able to boot to a CD and automatically begin the installation is an example. Although modern operating systems have more options for you to choose from, care has also been taken to minimize the stress involved in the process. We will look next at the Windows 2000 installation process and, in doing so, cover the following topics:

- Installation requirements
- Accessing the Setup files
- Running the Setup program
- Partitioning
- Formatting
- Customizing Setup

Installation Prerequisites

Because it is a power workstation, the hardware requirements for Windows 2000 are higher than those for older versions of Windows, and Windows 2000 also is less forgiving of older, less-efficient software. Make sure you have at least the minimum required hardware before you begin—but really, go for at least the recommended level of hardware.

Accessing the Setup Files

Unlike Windows *9x* Setup, which must run from a functioning OS (an earlier version of DOS or Windows or a boot disk), Windows 2000 is generally a breeze to install on a machine. To start the install process, place the Windows 2000 Professional CD into the CD-ROM drive and restart the computer. After the POST routine for the computer has completed, a message appears that says *Press any key to boot from CD*. Hit a key, any key, and the Windows 2000 Setup program will start.

That is a "perfect world" situation, and sometimes reality intrudes. If the *Press any key* message does not appear, that generally means your PC is not configured to boot from CD-ROM or does not have that capability. In such a case, you need to do one of two things:

- Go into the BIOS to set the machine to boot to its CD drive. Consult your computer's user guide for more information about examining and making changes to the BIOS.
- Create and use Windows 2000 boot disks to start the setup.

Starting a Windows 2000 Installation

The startup options we've listed all eventually lead you to the same point: executing the Setup routine for Windows 2000 Professional. Professional has two different executables used to start Setup, depending on the OS you are using to start the install. These executables are `WINNT.EXE` (used from DOS or Windows *9x*) and `WINNT32.EXE` (used from Windows NT and 2000). These commands have various options associated with them, as shown in Table 3.7.

TABLE 3.7 Common WINNT.EXE Options

Option	Function
/s:*sourcepath*	Allows you to specify the location of the Windows 2000 source files.
/t:*tempdrive*	Allows you to specify the drive that Setup uses to store temporary installation files.
/u:*answer file*	Used in an unattended installation to provide responses to questions the user would normally be prompted for.
/udf:id [,*UDB_file*]	If you are installing numerous machines, each must have a unique computer name. This setting lets you specify a file with unique values for these settings.
/e:*command*	Allows you to add a command (such as a batch script) to execute at the end of Setup.
/a	Tells Setup to enable accessibility options.
/s:*sourcepath*	Allows you to specify the location of the Windows 2000 source files.
/tempdrive:*drive_letter*	Allows you to specify the drive Setup uses to store temporary installation files.
/unattend	Used to run the install without user intervention.
/unattend[*num*]:[*answer_file*]	Allows you to specify custom settings for machines during an unattended installation.
/cmd:*command_line*	Executes a command (such as a batch file at the end of Setup).
/debug[*level*]:[*filename*]	Used to troubleshoot problems during an upgrade.
/udf:*id*[,*UDB_file*]	Allows certain values that need to be unique to be set separately for each machine installed.
/checkupgradeonly	Performs all the steps of an upgrade, but only as a test. The results are saved to an UPGRADE.TXT file that can be examined for potential problems.
/makelocalsource	Specifies that the i386 installation directory from the CD should be copied to the hard drive, allowing for easier updates later.

If you start the install by booting from the CD-ROM or the Windows 2000 boot disks you created, `WINNT.EXE` starts the install by loading a number of files and then presents you with a screen that says *Welcome to Setup*.

Partitioning the Drive in Windows 2000

To start Setup, press Enter at the welcome screen, and you will be shown a list of the partitions currently configured on the machine. If one of them is acceptable, select that partition and press Enter. If you wish to create a new partition, you can do so using the Setup program itself, which replaces `FDISK.EXE` as a way to set up the system's hard drive(s).

To delete an existing partition, highlight the partition and press D. You will be asked to confirm your choice and will be reminded that all information on the partition will be lost. If the disk is new or if the old information is backed up or no longer needed, this is fine.

If you are not sure what is on the drive, find out before you repartition it!

To create a new partition, highlight some free space and press C. You will be asked how big you want the partition to be. Remember that Windows 2000 Professional wants you to have about 2GB as a minimum, but the partition can be as large as the entire drive.

Formatting the Partition in Windows 2000

Once you have created or decided on a partition to use, you are asked to format that partition. In doing so, you need to choose between NTFS and the FAT file system. FAT is the file system of DOS, and its advantages include the following:

- Compatible with DOS and Windows 9*x* dual-boot configurations
- Excellent speed on small drives
- Accessible and modifiable with many standard DOS disk utilities

NTFS, as you might expect, comes from Windows NT and is a more sophisticated file system that has a number of enhancements that set it apart from FAT:

- Supports larger partition sizes than FAT
- Allows for file-level security to protect system resources
- Supports compression, encryption, disk quotas, and file ownership

In most cases, you will find that it is better to go with NTFS.

When you choose one of the format options, the machine formats the installation partition. This generally takes a few minutes, even on a fast PC.

Installing Windows 2000

After the installation partition is formatted, the system checks the new partition for errors and then begins to copy files. While the files are being copied, a progress indicator displays on the screen showing you how far along the process is. Windows installs files into temporary installation folders on the drive and asks you to reboot once the copy is complete. If you do not reboot within 15 seconds of the end of the file copy, the system automatically reboots for you.

If Setup detects any problems during the partition check, it attempts to fix them and immediately asks you to reboot. At that point the install will need to start over. If problems are found, this often indicates problems with the hard drive, and you may want to run a full scan using ScanDisk before returning to the install.

When Windows 2000 Professional reboots, it automatically brings you into a graphical setup that resembles a massive Windows wizard (see Figure 3.19). This is generally referred to as the graphical phase of Windows 2000 Setup, due to the contrast between this phase and the earlier blue-background-and-text text phase where you configured partitions and copied temporary files.

FIGURE 3.19 The Windows 2000 Setup Wizard

During this phase, Windows attempts to identify and configure the hardware in the computer, which may take a few minutes. One of the more unsettling parts of Setup occurs during this time, because the screen flickers—and often goes completely black—while monitor detection occurs.

Windows 2000 comes packaged with an impressive array of drivers and is able to identify and load most modern hardware. Still, not all devices have compatible drivers on the Windows 2000 CD. If your hardware is not detected during startup, you can install additional device drivers after Setup completes, as shown later in the chapter.

After hardware detection is completed, the ever-polite Windows 2000 Setup Wizard welcomes you once again. To move through the wizard, click the Next and Back buttons along the bottom of the window. The screens of the setup process are as follows:

Regional Settings The first screen rarely needs to be modified if you are configuring the machine for use in the United States, but users in other countries will find that this is where they can change keyboard and language settings.

Personalize Your Software Enter the name (required) and organization (optional) of the person to whom the software is registered. Both fields are just text boxes. Enter any values that apply.

Personalize Your Software If you're using a retail version of the OS, you will be prompted for the 25-character product key. You must enter it to proceed.

Computer Name and Administrator Password The *computer name* is the name by which a machine will be known if it participates on a network. This name is generally 15 characters or fewer. The administrator password is used to protect access to the powerful Administrator account. Unlike Windows 9*x*, where usernames and password security are optional, all users must log on with a username and password to use a Windows 2000 Professional Desktop.

Modem Dialing Information If a modem has been detected, you are asked for country, area code, and dialing preference information. If you do not have a modem, this screen is skipped.

Date and Time Settings The Date and Time dialog box also has time zone and daylight savings time information. Any data on this screen can easily be changed later.

Networking Settings/Installing Components After you enter the date and time, you will wait a minute or two as Windows 2000 installs any networking components it has found and prepares to walk you through the network configuration. As you are waiting, the Status area shows you which components are being installed.

Performing Final Tasks The Final Tasks page reports on Setup's progress while it does the following:

Installs Start Menu Items Shortcuts are created to the applications and options installed during Setup.

Registers Components The Registry is updated with Setup information.

Saves Settings Configuration information is saved to disk, and other defaults and user selections are applied (such as area code, time zone, and so on).

Removes Any Temporary Files Used The temporary files saved to the hard drive at the start of Setup and used to install Windows are removed to free drive space.

Eventually, the wizard completes and you are asked to reboot by clicking the Finish button. When the system restarts, Windows 2000 Professional Setup is complete, and the standard Windows 2000 boot process initiates.

Windows XP Installation

As of the writing of this book, Windows XP is the most common end-user operating system in the Microsoft OS family, as Vista has failed to catch on. Installing it is a breeze compared to previous editions of Windows. As a matter of fact, you can install it with a minimum of user interaction. Microsoft has designed Windows XP to be the simplest OS to install yet.

As with other versions of Windows, you will go through various phases of the installation:

- Starting the installation
- Text-based installation phase
- Graphical installation phase

Notice, however, that Windows XP does almost everything for you. It is a very quick OS installation.

Starting the Installation

During this phase, you begin the installation of Windows XP, configure the disk system to accept Windows XP, and start the graphical phase of Windows XP Setup.

In order to start a Windows XP installation, as with the other Windows OSs, you must first check your prerequisites (hardware support, available disk space, and so on). Plus, you must ensure that your computer supports booting to a CD-ROM (most do these days, especially those that are able to support Windows XP).

To start the installation power up the computer and quickly insert the Windows XP CD. If you don't do this quickly enough, you may get an *Operating system not found* message because the CD-ROM wasn't ready as a boot device (it hadn't spun up yet). If this happens, leave the CD in the drive and reboot the computer.

You may have to press a key on some systems. A phrase like *Press any key to boot from CD-ROM* may appear. If it does, press a key to do just that so you can begin the installation.

If the CD is inserted successfully, the screen clears and the words *Setup is inspecting your computer's configuration* appear. After that, the Windows XP Setup main screen appears. Then the Windows XP Setup main screen appears, as shown in Figure 3.20.

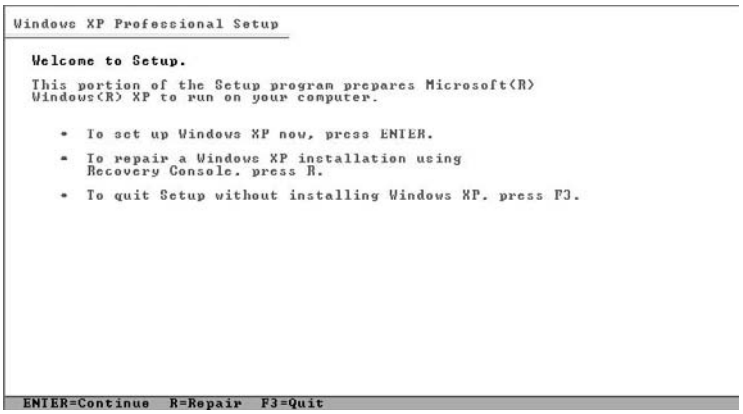
If your computer was produced after the release of Windows XP and you need to install a third-party SCSI, IDE, or RAID driver in order to recognize the disk drives, press F6 as soon as the screen turns from black to blue (Setup will prompt you at the bottom of the screen).

Text-Based Installation Phase

When the Setup screen appears, you can press Enter to begin the installation. The End User License Agreement (EULA) screen appears, and you must accept the EULA (otherwise

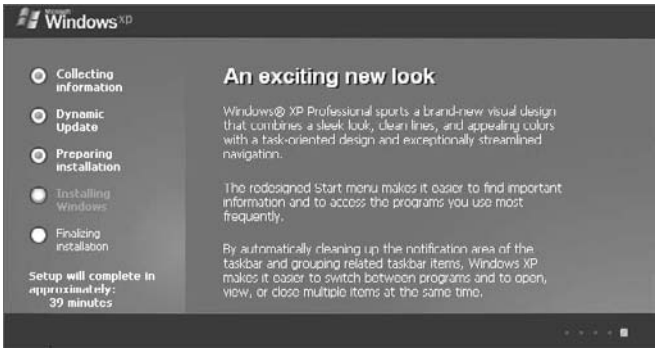
you can't install Windows XP—as with other versions of Windows). Windows Setup then presents you with a series of screens similar to those in previous versions, where you can set up the disk to accept Windows XP with either FAT or NTFS. It is best to choose NTFS for performance, enhanced features, and security reasons.

FIGURE 3.20 Windows XP main Setup screen



Windows Setup now formats the partition as you specified and copies the files needed to start the graphical portion of Setup. When it's finished copying and unpacking the files, Setup reboots the computer and starts the graphical portion of Windows XP Setup. If all is successful, you will see a screen similar to that in Figure 3.21.

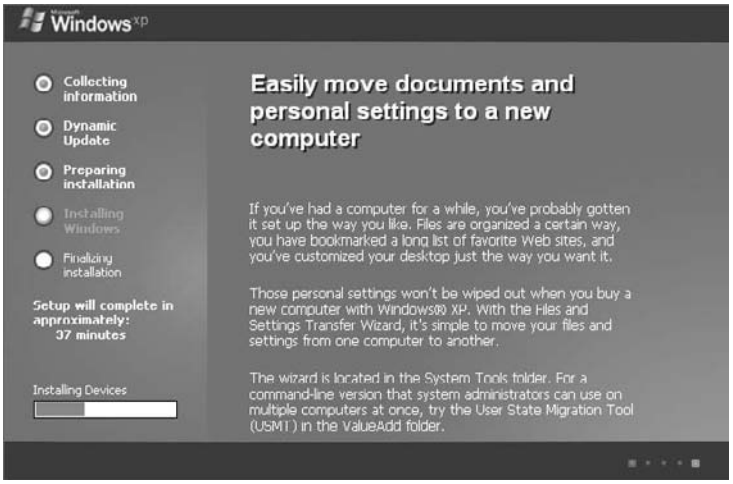
FIGURE 3.21 Windows XP Setup



Graphical Installation Phase

During the graphical installation phase, Windows XP Setup performs almost all of the actions necessary to bring Windows XP to a functional level. The first thing it does is copy files to the hard disk and begin installing devices (as shown in Figure 3.22). This process takes several minutes and should not be interrupted.

FIGURE 3.22 Installing devices in Windows XP Setup



Now, follow these steps:

1. Setup asks you for regional and language settings. The defaults are English (United States) for the language, United States for the location, and US Keyboard Layout for the default text-input method. If you are in a different location or prefer a different input method, you can change either item by clicking the button next to that item (Customize for language and location, Details for text-input method). If you accept the displayed options, click Next to continue the installation.
2. Identify yourself to Windows XP Setup by entering your name and company.
3. Windows asks you for the product key. You must enter the product key that comes with your version of Windows XP. This product key can be used only on this computer. To prevent product key theft, Microsoft requires that you go through product activation after the installation is complete.
4. Enter a computer name to identify this computer. Use something that will be completely unique on the entire network. Windows XP Setup suggests a name automatically, but you can overwrite it and choose your own. You also must enter a password for the Administrator user account (just as with Windows 2000).
5. Set the time, date, and time zone, as well as whether to adjust for daylight savings time. Click Next.
6. Setup prompts you for the network setup information. You can either have Setup install the network for you or choose the settings yourself. My personal preference is to accept the Typical Settings option and to go back and configure them later if they don't work. The typical settings include TCP/IP set to get its IP address automatically via DHCP (most networks are configured this way).

7. Setup asks you if you want to use a workgroup or a domain, similar to the installation of Windows 2000. Select either choice and continue.
8. Windows finishes the installation by copying all the remaining necessary files, puts items on the Start menu, builds the Registry, and cleans up after itself. This last step should take several minutes to complete. When it's finished, Setup reboots the computer.

Windows Activation

New to Windows XP is a process known as *product activation.* To curb software piracy, Microsoft requires that each copy of Windows XP be *activated* (either by phone or Internet) after installation. Without activation, you can run Windows XP, but you can use it for only 30 days. And during that 30 days, Windows XP will constantly remind you to activate your product.

In addition, the activation records what kind(s) of hardware are in your system, and if three or more pieces change, it requires you to activate again. It's somewhat of a hassle on the part of a system owner if he is constantly upgrading systems. However, some types of Windows XP distributions don't require activation (like those under volume license agreements with Microsoft).

The activation process is simple. After installation is complete, a wizard pops up, asking if you want to activate Windows. You can choose either the Internet or Phone option. If you have a connection to the Internet, the Activation Wizard asks you only which country you live in. No other personal information is required. You can then click Activate, and the Activation Wizard will send a unique identifier built from the different types of hardware in your system across the Internet to Microsoft's activation servers. These servers will send back a code to the Activation Wizard that activates your copy of Windows XP. The phone process is similar, but you must enter the code manually after calling Microsoft and receiving it.

For more information about the process, go to `http://www.microsoft.com/windows/windows-vista/quick-start/genuine-validation.aspx`.

Upon reboot, Windows automatically adjusts the screen size for optimum use. You are presented with a screen welcoming you to Windows XP. It walks you through connecting your computer to the Internet and registering and activating your copy of Windows XP, asks you for the names of people who are going to use this computer, and then presents you with the login screen (Figure 3.23). Click on a username you want to log in as, and Windows XP will present you with a Desktop (Figure 3.24).

FIGURE 3.23 A Windows XP login screen

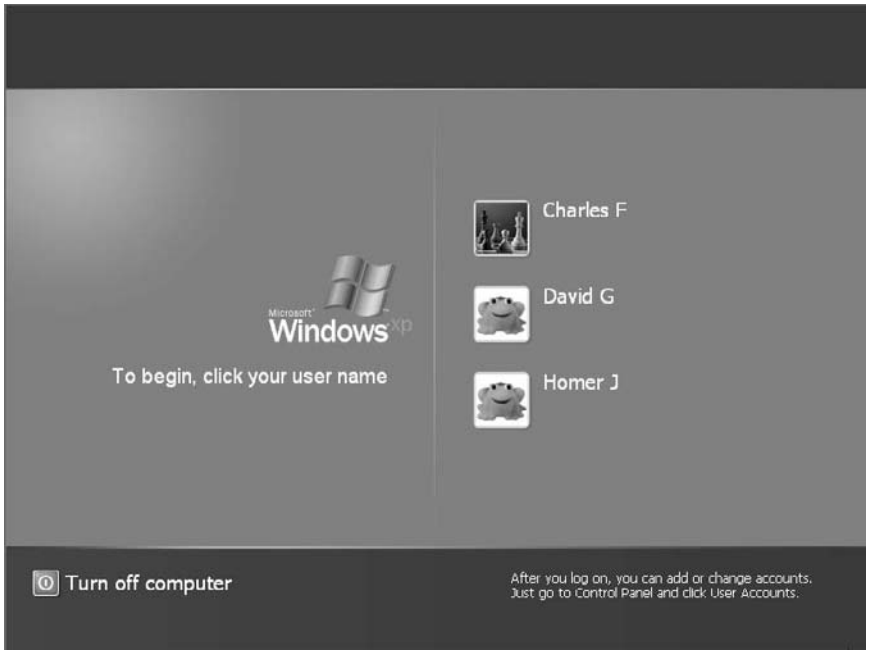


FIGURE 3.24 A Windows XP Desktop

Windows Vista Installation

As of the writing of this book, Windows Vista is the most current Windows version available, but Windows 7 is slated for release. You can install Windows Vista on a machine as a clean install (discussed here), or upgrade the existing operating system to Vista.

There are two methods of running a clean installation (which deletes all data currently on your computer). The first is to start the computer with the bootable Windows Vista DVD (CDs are available if you need them) and run Setup to begin the installation. The second method—the one Microsoft recommends—is that you run Setup from the DVD within your current Windows version. Once the DVD is inserted, the Setup program should automatically begin (if it does not, run `setup.exe` from the root folder) and a menu should appear. On the menu, choose Install Now and then select Custom (Advanced) when the "Which type of installation do you want?" screen appears. Answer the prompts to walk through the installation.

If booting from the DVD, you will get a message upon startup that tells you to press any key to boot from the CD. At this point you simply press a key (don't worry that it is a DVD and not a CD) and walk through the installation.

Postinstallation Routines

Even though you have installed your OS, you are not quite finished. There are a few items you must do in order to be truly finished. These items include the following:

- Updating drivers
- Restoring user data files
- Verifying installation

If you don't perform these tasks, you will find using the newly installed OS less than enjoyable.

Updating Drivers

After you have gotten the OS up and running, you may find that a few items aren't configured or working properly. That is somewhat typical. The drivers for some hardware aren't found on the Windows installation CD. Or, more commonly, the drivers on the installation CD are horribly out of date. It's a good idea, then, to go back after an installation and update the drivers for your hardware.

You should check the version of drivers for the following hardware against their manufacturer's website and ensure you have the most current driver for that item:

- Motherboard and chipset
- Video card
- Network card
- Sound card
- Disk controller

To update a driver, download the appropriate driver file package from the hardware manufacturer's website, extract it, and either run the setup utility that is included or use the Add Hardware Wizard that comes with all versions of Windows.

Restoring User Data Files

After you have installed an OS, you will want to use the computer. This involves installing applications and (if applicable) restoring data from either an older computer or this computer if you are reinstalling the OS.

Most often, restoring data files simply involves copying them from a different medium (such as a floppy disk, removable hard disk, magnetic tape, or other removable media). However, it can also involve copying the older data files from another computer. Windows XP includes a utility known as the *Files and Settings Transfer Wizard* that will transfer most of your files and individual application settings from an old computer to a new one. You connect the two computers (either by LAN or by null modem serial cable) and run the wizard on both computers. The files and settings are transferred to the new computer without much trouble.

You can find out more about using this utility from Microsoft: `http://www.microsoft.com/windowsxp/using/setup/expert/crawford_november12.mspx`.

Verifying Installation

The last thing you should do after installing any operating system is to perform a verification. It sounds easy enough, but many people forget to do it, and not doing it can come back to haunt you later. Simply reboot again (not that the installation didn't reboot a few dozen times already), and log in as a user. Make sure all of the appropriate programs are there and all of the devices (such as the network card and video card) are working properly.

Exam Essentials

Know the system requirements of Windows. You should know the minimum system requirements for Windows 2000, Windows XP, and Windows Vista.

Know the difference between attended and unattended installations. Be able to identify the time savings you can achieve with an unattended installation.

Understand upgrading. You should know that an installation overwrites any existing files whereas an upgrade keeps the same data/application files.

Select the right utility for a scenario. The test is likely to provide you with a troubleshooting or management scenario and ask you to identify which utility you would use. Familiarize yourself with all the utilities discussed.

Know what hot-swappable means. PC Card devices are hot-swappable, meaning you can remove and insert them while the computer is running. So are USB and FireWire devices. However, if you need to remove a drive, add or remove RAM, or connect or disconnect a monitor or a parallel or serial device, you must shut down the laptop.

Identifying Boot Sequences

This is a catchall category, as are many in this domain. Some of the objectives here carry over from previous ones. It tests your ability to understand the boot sequence, use diagnostic procedures, and recognize some common operational issues.

Critical Information

Both for the test and for real life, you should know how to recognize common problems with operating systems and make certain they're booting correctly. The sections that follow look at a number of topics related to keeping your OSs booting and running properly.

Working with the Boot Sequence

The first objective discussed in this chapter introduced the files used to boot the system. Under a normal boot, these files are accessed as needed, and the system is brought to its ready state. If problems are occurring, however, you may need to alter the boot method used. Windows offers a number of choices of altered boot sequences:

Safe Mode To access Safe Mode, you must press F8 when the OS menu is displayed during the boot process. A menu of Safe Mode choices appears, and you can select the mode you want to boot into. This is the mode to boot into if you suspect driver problems and want to load with a minimal set while you diagnose the problem.

Recovery Console (Windows XP and 2000 only) This is a command-line utility used for troubleshooting. From it, you can format drives, stop and start services, and interact with files stored on FAT, FAT32, or NTFS. The Recovery Console isn't installed on a system by default, but you can add it as a menu choice at the bottom of the startup menu.

Restore Points System Restore is arguably the most powerful tool in Windows Vista and XP. It allows you to restore the system to a previous point in time. This feature is accessed from Start ➢ All Programs ➢ Accessories ➢ System Tools ➢ System Restore and can be used to roll back as well as to create a restore point.

Automated System Recovery (ASR) (Windows XP only) It's possible to automate the process of creating a system recovery set by choosing the ASR Wizard on the Tools menu of

the Backup utility (Start ➢ All Programs ➢ Accessories ➢ System Tools ➢ Backup). This wizard walks you through the process of creating a disk that can be used to restore parts of the system in the event of a major system failure.

Emergency Repair Disk (ERD) (Windows 2000 only) The Windows Backup and Recovery Tool/Wizard also allows you to create an ERD. As the name implies, this is a disk you can use to repair a portion of the system in the event of a failure.

Common Error Messages

Unfortunately, there are times when systems do fail. Fortunately, when they do, they now try to explain why. Depending on the OS and settings, it's possible that the user will be asked if they want a report sent to Microsoft, dump logs will be created, log files will be written to, and so on. All of this makes your job as a troubleshooting administrator much easier than it was in the days when the solution to every problem was Ctrl+Alt+Del.

Boot problems can occur with corruption of the boot files or missing components (such as the `NTLDR` file being "accidentally" deleted by an overzealous user). Luckily, during the installation of the OS, log files are created in the `%SystemRoot%` or `%SystemRoot%\Debug` folder (`C:\WINNT` and `C:\WINNT\DEBUG`, by default). If you have a puzzling problem, look at these logs and see if you can find error entries there.

During startup, problems with devices that fail to be recognized properly, services that fail to start, and so on are written to the System log and can be viewed with the Event Viewer. This utility provides information about what's been going on system-wise, to help you troubleshoot problems. The Event Viewer shows warnings, error messages, and records of things happening successfully. It's found in NT versions of Windows only. You can access it through Computer Management, or you can access it directly from the Administrative Tools in Control Panel.

Recovering Operating Systems

Windows includes a number of tools to simplify recovering an operating system after a serious problem has occurred. System Restore is one such tool, as discussed previously. Three others we'll look at here are the Recovery Console, Automated System Recovery (ASR), and emergency repair disks (ERDs).

Recovery Console

The Recovery Console is a Windows XP/2000 command-line utility used for troubleshooting. From it, you can format drives, stop and start services, and interact with files. The latter is extremely important because many boot/command-line utilities bring you into a position where you can interact with files stored on FAT or FAT32, but not NTFS. The Recovery Console can work with files stored on all three file systems.

The Recovery Console isn't installed on a system by default. To install it, use the following steps:

1. Place the Windows CD in the system.
2. From a command prompt, change to the `i386` directory of the CD.
3. Type **`winnt32 /cmdcons`**.
4. A prompt appears, alerting you to the fact that 7MB of hard drive space is required and asking if you want to continue. Click Yes.

Upon successful completion of the installation, the Recovery Console (Microsoft Windows 2000 Recovery Console, for example) is added as a menu choice at the bottom of the startup menu. To access it, you must choose it from the list at startup. If more than one installation of Windows 2000 or Windows NT exists on the system, another boot menu will appear, asking which you want to boot into, and you must make a selection to continue.

To perform this task, you must give the administrator password. You'll then arrive at a command prompt. You can give a number of commands from this prompt, two of which are worth special attention: `EXIT` restarts the computer, and `HELP` lists the commands you can give. Table 3.8 lists the other commands available, most of which will be familiar to administrators who have worked with MS-DOS.

TABLE 3.8 Recovery Console Commands

Command	Purpose
`ATTRIB`	Shows the current attributes of a file or folder, and lets you change them.
`BATCH`	Runs the commands within an ASCII text file.
`CD`	Used without parameters, it shows the current directory. Used with parameters, it changes to the directory specified.
`CHDIR`	Works the same as `CD`.
`CHKDSK`	Checks the disk for errors.
`CLS`	Clears the screen.
`COPY`	Allows you to copy a file (or files, if used with wildcards) from one location to another.
`DEL`	Deletes a file.
`DELTREE`	Recursively deletes files and directories.
`DIR`	Shows the contents of the current directory.

TABLE 3.8 Recovery Console Commands *(continued)*

Command	Purpose
DISABLE	Allows you to stop a service/driver.
DISKPART	Shows the partitions on the drive, and lets you manage them.
ENABLE	Allows you to start a service/driver.
EXPAND	Extracts compressed files.
FIXBOOT	Writes a new boot sector.
FIXMBR	Checks and fixes (if possible) the master boot record.
FORMAT	Allows you to format a floppy or partition.
LISTSVC	Shows the services/drivers on the system.
LOGON	Lets you log on to Windows 2000.
MAP	Shows the maps currently created.
MD	Makes a new folder/directory.
MKDIR	Works the same as MD.
MORE	Shows only one screen of a text file at a time.
RD	Removes a directory or folder.
REN	Renames a file or folder.
RENAME	Works the same as REN.
RMDIR	Works the same as RD.
SYSTEMROOT	Works like CD but takes you to the system root of whichever OS installation you're logged on to.
TYPE	Displays the contents of an ASCII text file.

During the installation of the Recovery Console, a folder named `Cmdcons` is created in the root directory to hold the executable files and drivers it needs. A file named `Cmldr`, with attributes of System, Hidden, and Read-Only, is also placed in the root directory.

If you want to delete the Recovery Console (to prevent users from playing around, for example), you can do so by deleting the `Cmldr` file and the `Cmdcons` folder, and removing the entry from the `Boot.ini` file.

Automated System Recovery (Windows XP only)

It's possible to automate the process of creating a system recovery set by choosing the ASR Wizard on the Tools menu of the Backup utility (Start ➢ All Programs ➢ Accessories ➢ System Tools ➢ Backup). This wizard walks you through the process of creating a disk that can be used to restore parts of the system in the event of a major system failure.

The default name of this file is `BACKUP.BKF`; it requires a floppy disk. The backup set contains all the files necessary for starting the system, whereas the floppy becomes a bootable pointer to that backup set and can access or decompress it.

A weakness of this tool is its reliance on a bootable floppy in a day when many new systems no longer include a 3.5″ drive.

Emergency Repair Disk (Windows 2000 only)

The Windows Backup and Recovery Tool/Wizard allows you to create an emergency repair disk (ERD). As the name implies, this is a disk you can use to repair a portion of the system in the event of a failure.

When you choose this option, the tab changes to the Backup tab, and a prompt tells you to install a blank, formatted floppy disk. A check box inquires whether you want to save the Registry as well. (The default is no.) If you don't choose to save the Registry, the following files are placed on the floppy disk:

- `SETUP.LOG`
- `CONFIG.NT`
- `AUTOEXEC.NT`

This doesn't leave you much to work with. The disk isn't bootable and contains only three minor configuration utilities.

If you check the box to include the Registry in the backup, the floppy disk contains the preceding files plus the following:

- `SECURITY._`
- `SOFTWARE._`
- `SYSTEM._`
- `DEFAULT._`
- `SAM._`
- `NTUSER.DAT`
- `USRCLASS.DAT`

The user profile (NTUSER.DAT) is for the default user; the files with the ._ extension are compressed files from the Registry. The compression utility used is EXPAND.EXE, which offers you the flexibility of restoring any or all files from any Microsoft operating system, including this utility (Windows 95/98, Windows NT, and so on). Because this floppy contains key Registry files, it's important that you label it appropriately and store it in a safe location, away from users who should not have access to it.

During the process of creating the floppy, the Registry files are also backed up (in uncompressed state) to %systemroot%\repair\RegBack.

As before, the floppy isn't bootable, and you must bring the system up to a point (booted) where the floppy can be accessed before it's of any use.

Boot Order and Boot Devices

Within the BIOS of each machine, you can configure which devices are bootable, and in what order they will be tried. Depending upon your machine and BIOS version, the list of devices possible may range from floppy disks all the way up to USB devices and include everything in between. For example, assume you want to be able to boot from a flash drive. To configure this, reboot the workstation and press the corresponding key to take you into the BIOS configuration. (F12 works often, as does Delete. If it is not one of these two, it is usually F1 or F2.)

Within the BIOS configuration options, access the Boot menu and enable Boot USB Devices First or a setting with similar wording. If the option to boot from USB is simply Enable/Disable, choose Enable and then go to the order of boot devices and move USB above the hard drive.

Save the changes and exit the BIOS configuration. This will continue with the reboot and—if your USB drive is plugged in—should boot whatever operating system files are there.

If you get the single-line entry "Boot Error" and nothing else happens, update the BIOS and all should work as intended.

Exam Essentials

Know how to boot into Safe Mode. To access Safe Mode, you must press F8 when the operating system menu is displayed during the boot process.

Be able to identify the diagnostic procedures. CompTIA wants you to take a systematic approach to the problem that helps you isolate the problem and quickly identify it. You should be able to list the steps given in order.

Know the file systems. Make sure you can explain the differences between FAT16, FAT32, NTFS4, and NTFS5 and tell which OSs they're compatible with.

Understand file attributes. You should be able to explain the major file attributes and how to set them.

Use Windows Explorer. This is somewhat of a no-brainer because it's a basic end-user skill, but you should be thoroughly familiar with using Windows Explorer to manage files and folders.

Review Questions

1. True or false: Windows XP does not support FAT32.
2. With what Windows feature is a paging file associated?
3. What is another name for the System Tray?
4. To display a command-line interface in Windows XP, what would you execute from the Run command?
5. What hives does Windows 2000, XP, and Vista use to hold the Registry settings?
6. What needs to be done to a hard disk prior to formatting?
7. Which versions of Windows support NTFS encryption on NTFS5 drives?
8. Which power management state saves all the contents of memory to the hard drive and preserves all data and applications exactly where they are?
9. True or false: FireWire devices are hot-pluggable.
10. What is the command used to install the Recovery Console from the CD?

Answers to Review Questions

1. False. Windows XP supports FAT32 as well as NTFS.
2. Virtual memory creates a paging file, or swap file, and then moves data into and out of RAM to it.
3. Microsoft uses the terms *System Tray* and *Notification Area* roughly synonymously to refer to the area where the clock and the icons for running background programs appear.
4. In Windows 2000 or XP, you use `CMD`. Windows Vista uses Search instead of Run.
5. Windows 2000, XP, and Vista use `SAM`, `SECURITY`, `SOFTWARE`, `SYSTEM`, and `DEFAULT`.
6. Hard disks must be partitioned.
7. NTFS5 is used only with Windows 2000, XP, and Vista.
8. The Hibernate mode saves all the contents of memory to the hard drive and preserves all data and applications exactly where they are.
9. True. FireWire and USB devices are hot-pluggable.
10. `winnt32 /cmdcons`

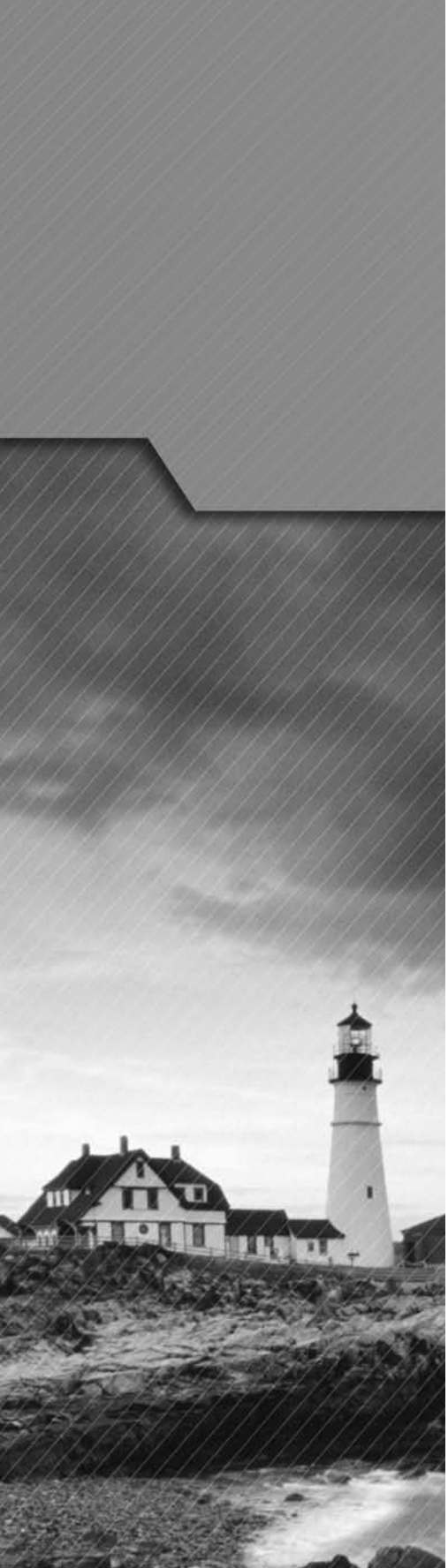
Chapter

4

Networking

COMPTIA A+ ESSENTIALS EXAM OBJECTIVES COVERED IN THIS CHAPTER:

- ✓ **4.1 Summarize the basics of networking fundamentals, including technologies, devices and protocols**
  - Basics of configuring IP addressing and TCP/IP properties (DHCP, DNS)
  - Bandwidth and latency
  - Status indicators
  - Protocols (TCP/IP, NETBIOS)
  - Full duplex, half-duplex
  - Basics of workgroups and domains
  - Common ports: HTTP, FTP, POP, SMTP, TELNET, HTTPS
  - LAN/WAN
  - Hub, switch, and router
  - Identify Virtual Private Networks (VPN)
  - Basic class identification
- ✓ **4.2 Categorize network cables and connectors and their implementations**
  - Cables
    - Plenum / PVC
    - UTP (e.g. CAT3, CAT5 / 5e, CAT6)
    - STP
    - Fiber
    - Coaxial cable
  - Connectors
    - RJ45
    - RJ11



- ✓ **4.3 Compare and contrast the different network types**
  - Broadband
    - DSL
    - Cable
    - Satellite
    - Fiber
  - Dial-up
  - Wireless
    - All 802.11 types
    - WEP
    - WPA
    - SSID
    - MAC filtering
    - DHCP settings
  - Bluetooth
  - Cellular

CompTIA offers a number of other exams and certifications on networking (Network+, i-Net+, and so on), but to become A+ certified, you must have good knowledge of basic networking skills. Not only do you need to know how networks operate, but you also need to know how to troubleshoot and identify common problems with them. Three subobjectives in this category focus more on general knowledge than specific. These topics are tested again—in more specific implementations—in the elective exam (see Chapter 9, "Networking.")

The Basics of Networking

You're expected to know the basic concepts of networking as well as the different types of cabling that can be used. For the latter, you should be able to identify connectors and cables from figures even if those figures are crude line art (think shadows) appearing in pop-up exhibit boxes.

Critical Information

It's important to know how network addressing works and the various protocols that are in use in networks today. Although TCP/IP has the lion's share of the networking market, it isn't the only protocol that may be used, and CompTIA expects you to have a broad range of knowledge in this category.

Basic Concepts

Duplexing is the means by which communication takes place:

- With *full duplexing*, everyone can send and receive at the same time.
- With *half duplexing*, communications travel in both directions, but in only one direction at any given time. Think of a road where construction is being done on one lane—traffic can go in both directions but in only one direction at a time at that location.

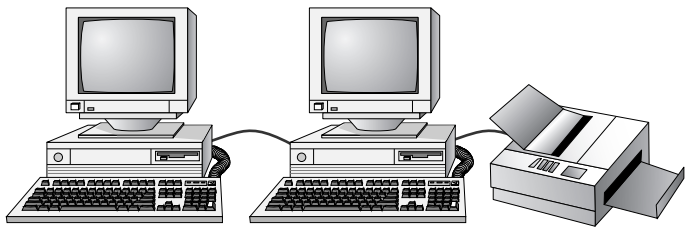
Networks consist of servers and clients. A *server* is a dedicated machine offering services such as file and print sharing. A *client* is any individual workstation accessing the network. A *workstation* is a client machine that accesses services elsewhere (normally from a server). A *host* is any machine or interface that participates in a TCP/IP network—whether as a client or a server. Every interface on a TCP/IP network that must be issued an IP address is considered a host. *Thin clients* are network clients that typically can't boot (and sometimes can't function) without the network. Normally, they lack a hard drive and must boot from the network in order to be operable.

A *local area network* (LAN) is a network that is geographically confined within a small space—a room, a building, and so on. Because it's confined and does not have to span a great distance, it can normally offer higher speeds. A *wide area network* (WAN) is a collection of two or more LANs, typically connected by routers. The geographic limitation is removed, but WAN speeds are traditionally less than LAN speeds. A *domain* is a centrally managed group of computers and physical proximity does not matter; the computers within a domain may all be on the same LAN or spread across a WAN.

Segments are divisions of a LAN made possible if you're using certain topologies—think of them as subnets or logical groupings of computers. The division of the network into segments can be accomplished through the use of switching hubs, multiplexers, bridges, routers, or brouters.

A peer-to-peer network—also known as a *workgroup*—consists of a number of workstations (two or more) that share resources among themselves (see Figure 4.1). The resources shared are traditionally file and print access, and every computer has the capacity to act as a workstation (by accessing resources from another machine) and as a server (by offering resources to other machines). The primary distinction between workgroups and client/server networks is where security is controlled; locally on each workstation or centrally on a server.

FIGURE 4.1 The peer-to-peer model

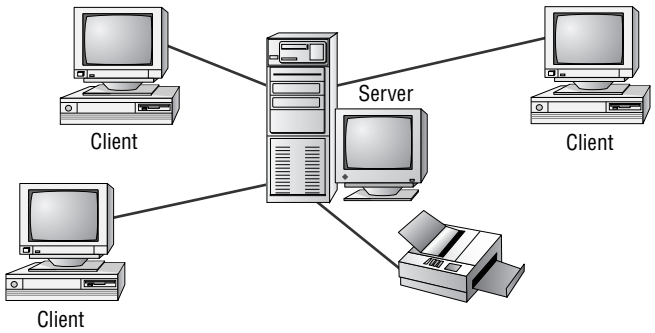


In a server-based network (known as a *client/server network*), users log on to the server by supplying a username and password (see Figure 4.2). They're then authenticated for the duration of their session. Rather than requiring users to give a password for every resource they want to access (share-level), security is based on how they authenticated themselves at the beginning of their session. This is known as *user-level* security, and it's much more powerful than share-level security.

The advantage of a peer-to-peer network is that the cost is lower—you need only add cards and cables to the computers you already have if you're running an operating system that allows such modifications. With a server-based network, you must buy a server—a dedicated machine—and thus the costs are higher. It's never recommended that a peer-to-peer network be used for more than 10 workstations, because the administration and management become so significant that a server-based network makes far greater sense.

The *cable* is the physical pathway for communications, and the *network interface card* (NIC) is the physical entity that goes into the computer and is attached to the cable. A *router* is used to connect LANs together; you can even use a router to connect dissimilar topologies that use the same protocol, because physical specifications don't apply.

FIGURE 4.2 The client/server model



With *baseband*, the entire medium's capacity is used for one signal. The speed possibilities are thus increased because the entire channel is utilized. With *broadband*, the medium is used to carry multiple signals, but all unidirectionally. Some common implementations of broadband include DSL, cable, and satellite.

A *gateway* can have two meanings. In TCP/IP, a gateway is the address of the machine to send data to which is not intended for a host on this network (in other words, a default gateway). A gateway is also a physical device operating between the Transport and Application layers of the OSI model that can send data between dissimilar systems. The best example of the latter is a mail gateway—it doesn't matter which two networks are communicating; the gateway allows them to exchange e-mail.

The International Standards Organization (ISO) created the OSI model to outline networking. They defined the functions that must take place between machines in order to have a network and broke them into seven distinct parts, or layers. At the bottom of the layers, the network deals only with bits and signals; there is no intelligence. At the top layer, the model interacts with users and applications and has a great deal of intelligence built into it. Starting from the bottom, the OSI layers are as follows:

The Physical Layer This layer is made up of components you can see, feel, and touch: cards, cables, terminators, and so on. There is no intelligence, and devices that can operate here include repeaters and multiplexers. A repeater takes in a signal, amplifies it, and sends it on. If the signal coming in is garbage, then amplified garbage comes out—this layer performs no function aside from boosting the signal.

The Data Link Layer This layer takes data from the upper layers and prepares it to be sent across the Physical layer. It's the only layer divided into subcomponents—the Logical Link Control (LLC) and Media Access Control (MAC). In addition to communicating with NICs, it performs error checking and manages link control. Bridges and Layer 2 switches can and do operate at this layer.

The Network Layer This layer directs the flow of data from a source to a destination, regardless of whether there is a dedicated connection. It's responsible for translating names into addresses, monitoring traffic, and finding the best route. Routers operate at this level.

All switching operates at Layer 2 using MAC addresses. Layer 3 switches are so named because they can perform a routing function as well as a switching function. Most switches operate only at the Data Link layer.

The Transport Layer This layer handles packets and network transmissions. Its primary responsibility is to make certain packets transmitted by the Network layer get to where they are going (and oversee error checking/correction). A gateway is the physical device capable of working at this and all upper layers.

The Session Layer This layer determines the synchronization rules the two computers will use and establishes the rules for dialogue (communications). It also contains protocols that are primarily responsible for establishing connections between computers and terminating the connections when the transmission is complete.

The Presentation Layer This layer translates data between the Application layer above it, and all other layers. It can perform compression and encryption, and it's the redirector from the application to the network.

The Application Layer This layer is the interface to network services. All data originates here before going across the network and concludes here on the other side. Some of the possible services are print, file, messaging, and database.

Data originates in the Application layer of the source computer and travels down through subsequent layers. Each layer adds a header to the data and passes it to the next lower layer until it reaches the Physical layer. At the Physical layer, the data travels across the wire to the target computer, where it enters at the Physical layer and begins moving up the layers. On the target computer, each layer strips the header intended for it and passes the data up until it reaches the Application layer once more.

Large numbers of protocols and services operate at various layers of the OSI model. In many cases, a protocol or service can function at multiple layers. A summary of protocols, services, and hardware is shown in Table 4.1.

Integrated Services Digital Network (ISDN) is a WAN technology that performs link management and signaling by virtue of packet switching. The original idea behind it was to let existing phone lines carry digital communications by using multiplexing to support multiple channels. ISDN works with the bottom four layers of the OSI model: Transport, Network, Data Link, and Physical.

TABLE 4.1 OSI Layer Breakout

Layer	Hardware	Protocols and Services	Data Type
Application	Gateway	SMB, NCP, NFS, SNMP, Telnet	Message, user data
Presentation	Gateway	NCP, NFS, SNMP	Packet

TABLE 4.1 OSI Layer Breakout *(continued)*

Layer	Hardware	Protocols and Services	Data Type
Session	Gateway	NFS, SNMP, RPC	Packet
Transport	Gateway	TCP, UDP, SPX, NetBEUI	Segment, datagram, packet
Network	Router, brouter, switch	IP, IPX, ICMP, ARP, RARP, RIP, OSPF, DLC, DecNET	Datagram, packet
Data Link	Bridge, brouter, switch	LLC, MAC	Frame
Physical	Repeater, multiplexer	802.3, 802.5, etc.	Bit, signal

Network Protocols

Hosts on a network communicate using a common language called a protocol. A *protocol* is nothing more than a set of rules that governs the communications between the hosts. Just as humans can speak more than one language, so too can networked hosts—but it's critically important that the hosts speak a common language, or they won't be able to communicate, and no networking will take place.

NetBEUI/NetBIOS

NetBIOS Enhanced User Interface (NetBEUI) is a protocol that Microsoft came up with as an outgrowth of *Network Basic Input Output System (NetBIOS)*. It's very small, has virtually no overhead, and was used in all of Microsoft's early networking products: Windows for Workgroups, LAN Manager, and so on.

Although NetBEUI is ideal for a small network or workgroup, its giant downfall is that it can't be routed. This limits your network to a single location, unless you use a bridge (a device of days gone by).

TCP/IP

Every computer, interface, or device on a *Transmission Control Protocol/Internet Protocol* (TCP/IP) network is issued a unique identifier known as an *IP address* that resembles 209.110.12.123. Because of the Internet, TCP/IP is the most commonly used networking protocol today. You can easily see that it's difficult for most users to memorize these numbers, so hostnames are used in their place. *Hostnames* are alphanumeric values assigned to a host; any host may have more than one hostname.

For example, the host 209.110.12.123 may be known to all users as Gemini, or it may be known to the sales department as Gemini and to the marketing department as Apollo9. All that is needed is a means by which the alphanumeric name can be translated into its IP address. There are four methods of doing so:

On a Small Network On a small network, you can use hosts files. These are ASCII text files located in the `/etc` directory of every machine that performs the translation. When a new host is added to the network, every host must have its hosts file updated to include the new entry. Hosts files work with every platform and every operating system, but they require constant manual updating and editing to keep them current—impractical on large networks.

On a Large Network On a large network, you can add a server to be referenced by all hosts for the name resolution. The server runs Domain Name Services (DNS) and resolves fully qualified domain names (FQDNs) from `www.ds-technical.com` into their IP address. Multiple DNS servers can serve an area and provide fault tolerance for one another. In all cases, the DNS servers divide their area into zones; every zone has a primary server and any number of secondary servers. DNS, like hosts files, works with any operating system and any version.

On a Small Windows-Only Network If the network within which you work is all Microsoft (Windows XP, Windows Vista, and so on), then you're accustomed to using NetBIOS names as computer names. On a small network, you can use LMHOSTS (LAN Manager Hosts) files to translate computer names to IP addresses—much like hosts files do. The big difference is that NetBIOS (computer) names exist only on the Microsoft platform, and LMHOSTS files can't be used with Unix or other operating systems.

On a Large Windows-Only Network If you have a large Microsoft-only network, you can stop editing the LMHOSTS files manually and use a server running Windows Internet Naming Service (WINS). The WINS server dynamically maps NetBIOS names to IP addresses and keeps your network mappings current. Again, this is a replacement for LMHOSTS and works only in the Microsoft world.

You can use a WINS proxy to let Unix and other clients resolve names using the WINS database.

Whether the files or services are case-sensitive or not depends on the operating system. If you're using hosts files in Unix and have a host named GEMINI, you must have the following entry in the file:

```
209.110.12.123 GEMINI
```

In Windows, however, neither the operating system nor the hosts file is case sensitive, and

```
209.110.12.123 Gemini
```

delivers the same result when trying to resolve *GEMINI*, as do references to *gemini*, *gemInI*, and so on.

Hosts files are limited to 256 characters per line, and the pound sign (#) is used as the comment character. Wherever the pound sign is found, the rest of the line is ignored. Consider this example:

```
#This is the first line
209.110.123.4 MARS #This is the second line
```

Line 1 is completely ignored, and line 2 is processed up to the space following the *S*. LMHOSTS files also use the pound sign as the comment character.

The FQDNs mentioned earlier identify the host and information about it. The first part, `www`, identifies the type of service to use. The second part, `ds-technical`, identifies the entity, and `com` identifies the type of entity. Known as a *domain*, the entity type can be any of the values shown in Table 4.2.

TABLE 4.2 Common Domains

Domain	Meaning
`biz`	Business
`com`	Commercial
`edu`	Educational
`info`	Information
`mil`	US Military
`gov`	US Government
`net`	Network—ISP
`org`	Original—organization
xx	Two-character country identifier, such as ca for Canada

Working with DHCP

Dynamic Host Configuration Protocol (DHCP) falls into a different category. Whereas the other services described concentrate on resolving names to IP addresses, DHCP issues IP configuration data.

Rather than an administrator having to configure a unique IP address for every host added on a network (and *default gateway* and *subnet mask*), they can use a DHCP server to issue these values. That server is given a number of addresses in a range that it can supply to clients.

For example, the server may be given the IP range (or *scope*) 209.110.12.1 to 209.11.12.200. When a client boots, it sends out a request for the server to issue it an address (and any other configuration data) from that scope. The server takes one of the numbers it has available and leases it to the client for a length of time. If the client is still using the configuration data when 50 percent of the lease has expired, it requests a renewal of the lease from the server; under normal operating conditions, the request is granted. When the client is no longer using the address, the address goes back in the scope and can be issued to another client.

DHCP is built on the older Bootstrap Protocol (BOOTP) that was used to allow diskless workstations to boot and connect to a server that provided them an operating system and applications. The client uses broadcasts to request the data and thus—normally—can't communicate with DHCP servers beyond their own subnet (broadcasts don't route). A DHCP Relay Agent, however, can be employed to allow DHCP broadcasts to go from one network to another.

The primary purpose of DHCP is to lease IP addresses to hosts. The client contacts the DHCP server and requests an address, and the DHCP server issues one to the client to use for a period of time. This lease can continue to be renewed as long as the client needs it and the server is configured to keep renewing it.

IP addresses are 32-bit binary numbers. Because numbers of such magnitude are difficult to work with, they're divided into four octets (eight bits) and converted to decimal. Thus, 01010101 becomes 85. This is important because the limits on the size of the decimal number are due to the reality that they're representations of binary numbers. The range must be from 0 (00000000) to 255 (11111111) per octet, making the lowest possible IP address 0.0.0.0 and the highest 255.255.255.255. Many IP addresses aren't available because they're reserved for diagnostic purposes, private addressing, or some other function.

Three classes of IP addresses are available; they're identified by the first octet. Table 4.3 shows the class and the range the first octet must fall into to be within that class.

If you're given a Class A address, then you're assigned a number such as 125. With a few exceptions, this means you can use any number between 0 and 255 in the second field, any number between 0 and 255 in the third field, and any number between 0 and 255 in the fourth field. This gives you a total number of hosts that you can have on your network in excess of 16 million.

TABLE 4.3 IP Address Classes

Class	Range
A	1–126
B	128–191
C	192–223

If you're given a Class B address, then you're assigned a number such as 152.119. With a few exceptions, this means you can use any number between 0 and 255 in the third field and any number between 0 and 255 in the fourth field. This gives you a total number of hosts that you can have on your network in excess of 65,000.

If you're given a Class C address, then you're assigned a number such as 205.19.15. You can use any number between 1 and 254 in the fourth field, for a total of 254 possible hosts (0 and 255 are reserved).

The class, therefore, makes a tremendous difference in the number of hosts your network can have. In most cases, the odds of having all hosts at one location are small. Assuming you have a Class B address, will there be 65,000 hosts in one room, or will they be in several locations? Most often, it's the latter.

Working with Subnets

Subnetting your network is the process of taking the total number of hosts available to you and dividing it into smaller networks. When you configure TCP/IP on a host, you typically need only give three values: a unique IP address, a default gateway (router) address, and a subnet mask. The default subnet mask for each class of network is shown in Table 4.4.

Purists may argue that you don't need a default gateway. Technically this is true if your network is small and you don't communicate beyond it. For all practical purposes, though, most networks need a default gateway.

TABLE 4.4 Default Subnet Values

Class	Default Subnet Mask
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

When you use the default subnet mask, you're allowing for all hosts to be at one site and not subdividing your network. Any deviation from the default signifies that you're dividing the network into multiple subnetworks.

TCP and User Datagram Protocol (UDP) both use port numbers to listen for and respond to requests for communications. RFC 1060 defines *common ports* for a number of services routinely found in use, and these all have low numbers—up to 1024. You can, however, reconfigure your service to use another port number (preferably much higher) if you're concerned about security and you don't want your site to be available to anonymous traffic. Common port assignments are listed in Table 4.5.

TABLE 4.5 Common Port Assignments

Service	Port
FTP	20 and 21
Telnet	23
SMTP	25
HTTP	80
POP3	110
NNTP	119
IMAP	143
HTTPS	443

Status Indicators

A status indicator is any tool that offers you a view of the current network condition. As they relate to the exam objective, the most common status indicators are link lights and collision lights. Both of these are discussed in the following paragraphs.

Link lights appear on a hub to show when a connection to a computer is present. If a network cable is plugged into the network device and the light isn't lit, there isn't a valid connection between the network device and the client, or the correct drivers and configuration aren't present. On most network devices, the link lights blink when traffic is traveling through that port. On 10/100 network devices, a different color can be used for the light to indicate whether the connection is made at 10Mbps or 100Mbps. Lit link lights on the NIC card also indicate that a connection is present.

Collision lights are used on hubs, bridges, and so on to indicate when a collision has occurred. Collisions can happen whenever more than one device attempts to send data at the same time. Under normal conditions, the multiple devices wait a short time (milliseconds) and then attempt to resend. Under this condition, the collision lights blink occasionally and go off. If they're on regularly, you don't have enough bandwidth to handle your traffic. Switched hubs can often be used to reduce the number of collisions on a network; you can also increase the bandwidth of the network (from 10Mbps to 100Mbps, for example).

Virtual Private Networks

A *virtual private network (VPN)* is a private network connection that occurs through a public network. A private network provides security over an otherwise unsecure environment. VPNs can be used to connect LANs together across the Internet or other public networks.

With a VPN, the remote end appears to be connected to the network as if it were connected locally. A VPN requires either special hardware to be installed or a VPN software package running on servers and workstations.

VPNs typically use a tunneling protocol such as Layer 2 Tunneling Protocol (L2TP), IPSec, or Point-to-Point Tunneling Protocol (PPTP). VPNs are becoming the connection of choice when establishing an extranet or intranet between two or more remote offices. The major security concern when using a VPN is encryption. PPTP offers some encryption capabilities, although they're weak. IPSec offers higher security, and it's becoming the encryption system used in many secure VPN environments.

Even though a VPN is created through the Internet or other public network, the connection logically appears to be part of the local network. This is why a VPN connection used to establish a connection between two private networks across the Internet is considered a private connection or an extranet. To simplify the difference, know that an extranet specifically extends the company's local network to non-company users while a VPN is often used to remotely connect users who are members of the company.

As mentioned earlier, VPNs are used to make connections between private networks across a public network, such as the Internet. These connections aren't guaranteed to be secure unless a tunneling protocol (such as PPTP) and an encryption system (such as IPSec) are used. A wide range of options, including proprietary technologies, is available for VPN support. Many of the large ISPs and data communications providers offer dedicated hardware with VPN capabilities. Many servers also provide software VPN capabilities for use between two networks.

VPN systems can be dedicated to a certain protocol, or they can pass whatever protocols they see on one end of the network to the other end. A pure VPN connection appears as a dedicated wired connection between the two network ends.

Bandwidth and Latency

Bandwidth is defined in networking as the transmission capacity of a communications channel. This is expressed in terms of megabits or megabytes per second and the higher the number, the faster the data transmission takes place. For example, 100BaseT tells you three things:

- 100—The speed of the network, 100Mbps.
- Base—The technology used (either baseband or broadband).
- T—Twisted-pair cabling. In the case of 100BaseT, it's generally UTP.

Latency is the networking term used for delays. Since there is always some time required to send data, there is always a small amount of latency (low latency) occurring, but problems occur when high latency happens. The delays can cause—or be caused by—bottlenecks that you must find in order to increase the speed of the network. In many cases, the latency is simply a barrier of the bandwidth. and a solution is to increase the speed of the network (a simple example would be to move from an old 10BaseT network to 100BaseT).

Exam Essentials

Understand basic networking concepts. A network is a collection of computers that can interact with one another and share files and resources. The network may be peer-to-peer or client/server-based.

Know the categories of networking connectivity. LANs are confined to local, whereas WANs expand that limit. ISDN, broadband, and cellular are methods of establishing network connections.

Network Cabling and Connectors

This objective tests your knowledge of networking cards and networking connectivity. It expects you to understand the terms and topics and be able to work with them in the real world.

Critical Information

A NIC is a physical card installed within a computer that allows it to communicate on the network. This NIC can allow the system to operate on a wired or wireless network and must be there for communication to be possible.

The Network Interface Card

The NIC provides the physical interface between computer and cabling. It prepares data, sends data, and controls the flow of data. It can also receive and translate data into bytes for the CPU to understand. It communicates at the Physical layer of the OSI model and comes in many shapes and sizes.

Installation

The physical installation of a NIC is the same as with any other internal circuit board. It fits into an ISA or PCI expansion slot in the motherboard or in a USB port as with a USB NIC.

When choosing a NIC, use one that fits the bus type of your PC. If you have more than one type of bus in your PC (for example, a combination ISA/PCI), use a NIC that fits into the fastest type (PCI, in this case). This is especially important in servers, because the NIC can quickly become a bottleneck if you don't follow this guideline.

Configuration

In today's environment, it is rare to need to manually configure a NIC. On legacy cards, however, this was something that had to be done, and I recommend you know the basics as you prepare for the A+ exam.

The NIC's configuration includes such things as a manufacturer's hardware address, IRQ address, base I/O port address, and base memory address. Some NICs may also use direct memory access (DMA) channels to offer better performance.

Each card has a unique MAC address, which is hard-wired into the card during its manufacture. It consists of six two-digit hexadecimal numbers; the first three represent the manufacturer, and the second three are the unique serial number of the card. The MAC address is separate from any logical address that might be assigned to the PC by the networking system, such as an IP address.

Configuring a NIC is similar to configuring any other type of expansion card. Token-ring cards often have two memory addresses that must be allocated in reserved memory for them to work properly.

Drivers

For the computer to use the NIC, it's very important to install the proper device drivers. These drivers communicate directly with the network redirector and adapter. They operate in the MAC sublayer of the Data Link layer of the OSI model.

Media Access Methods

You've put the network together in a topology. You've told the network how to communicate and send the data, and you've told it how to send the data to another computer. You also have the communications medium in place. The next problem you have to solve is how to put the data on the cable. What you need now are the *cable access methods*, which define a set of rules for how computers put data onto and retrieve data from a network cable. The four most common methods of data access are as follows:

Carrier Sense Multiple Access with Collision Detection NICs that use CSMA/CD (think Ethernet) listen to, or "sense," the cable to check for traffic. They compete for a chance to transmit. Usually, if access to the network is slow, it means that too many computers are trying to transmit, causing traffic jams.

Carrier Sense Multiple Access with Collision Avoidance Instead of monitoring traffic and moving in when there is a break, CSMA/CA allows the computers to send a signal that they're ready to transmit data. If the ready signal transmits without a problem, the computer then transmits its data. If the ready signal isn't transmitted successfully, the computer waits and tries again. This method is slower and less popular than CSMA/CD on wired networks. CSMA/CA is the carrier access method used for most wireless networks today.

Token Passing *Token passing* is a way of giving every NIC equal access to the cable. A special packet of data is passed from computer to computer. Any computer that wants to transmit has to wait until it has the token. It can then transmit its data.

This is an old method that was used on IBM token ring networks of the past. It's also sometimes used on fiber rings today.

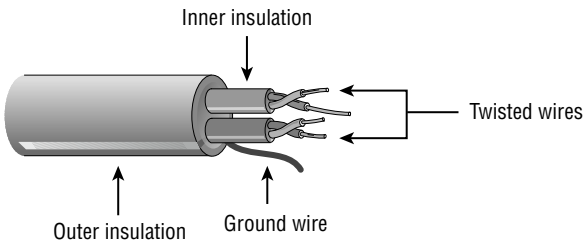
Polling *Polling* is an old method of media access. Not many topologies support polling anymore, mainly because it has special hardware requirements. This method requires a central, intelligent device (meaning that the device contains either hardware or software intelligence to enable it to make decisions) that asks each workstation in turn if it has any data to transmit. If the workstation answers "yes," the controller allows the workstation to transmit its data.

The polling process doesn't scale well—that is, you can't take this method and apply it to any number of workstations. In addition, the high cost of the intelligent controllers and cards has made the polling method all but obsolete.

Cabling

A number of choices are available when you're cabling a network. Twisted-pair wiring is one of the most common; it's made up of pairs of wires twisted around each other, as shown in Figure 4.3, and comes in two varieties:

FIGURE 4.3 Twisted-pair cable



Unshielded Twisted Pair (UTP) This offers no shielding (hence the name) and is the network cabling type most prone to outside interference. The interference can be from a fluorescent light ballast, electrical motor, or other such source (known as *electromagnetic interference [EMI]*) or from wires being too close together and signals jumping across them (known as *crosstalk*).

Shielded Twisted Pair (STP) This adds a foil shield around the twisted wires to protect against EMI.

Twisted-pair cabling is most often used in 10BaseT/100BaseT networks. There are different grades, which are given as categories; and as you may guess, the higher the grade, the more expensive the cabling, and the higher the data rate it can support. The breakout is as follows:

Category 1 For voice-only transmissions. Used in most phone systems today. It contains two twisted pairs.

Category 2 Transmits data at speeds up to 4Mbps. It contains four twisted pairs of wires. It's also not used in networks and is suitable only for voice grade.

Category 3 Transmits data at speeds up to 10Mbps. It contains four twisted pairs of wires with three twists per foot. This is the lowest-level cabling you can safely use in a network.

Category 4 Transmits data at speeds up to 16Mbps. It contains four twisted pairs of wires.

Category 5 Transmits data at speeds up to 100Mbps. It contains four twisted pairs of copper wire to give the most protection.

Category 5e Transmits data at speeds up to 1Gbps. It also contains four twisted pairs of copper wire, but they're physically separated and contain more twists per foot than Category 5 to provide maximum interference protection.

Category 6 Transmits data at speed up to 10Gbps. It contains four twisted pairs of copper wire and is used in 10GBaseT networks.

10BaseT networks require a minimum of CAT-3 cabling, whereas 100BaseT—the minimum in installations today—requires CAT-5 cabling.

Most UTP cable uses RJ-45 connectors that look like telephone connectors (RJ-11) but have eight wires instead of four. STP cable, on the other hand, uses IBM data connector (IDC) or universal data connector (UDC) ends and connects to token ring networks. The common types of STP cable are as follows:

Type 1 The most common STP cable type. Contains two pairs.

Type 2 Like Type 1, but adds two pairs of voice wires.

Type 3 Contains four pairs.

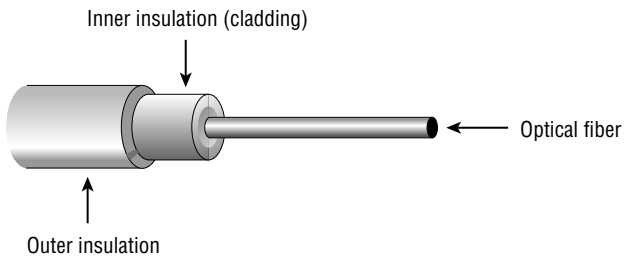
Type 6 Patch cable, used for connecting token ring hubs.

Type 8 A flat type of STP cable used for running under carpets.

Type 9 A two-pair, high-grade type of STP.

Fiber-optic cabling is the most expensive type of those discussed for this exam. Although it's an excellent medium, it's often not used because of the cost of implementing it. It has a glass core within a rubber outer coating and uses beams of light rather than electrical signals to relay data (see Figure 4.4). Because light doesn't diminish over distance the way electrical signals do, this cabling can run for distances measured in kilometers with transmission speeds from 100Mbps up to 1Gbps or higher.

FIGURE 4.4 Fiber-optic cable



Often, fiber is used to connect runs to wiring closets where they break out into UTP or other cabling types, or as other types of backbones. Fiber-optic cable can use either ST or SC connectors: ST is a barrel-shaped connector, and SC is squared and easier to connect in small spaces.

Table 4.6 lists the cabling types discussed and various attributes of each.

FC or LC connectors may also be used but are not as common.

TABLE 4.6 Cable Types

Characteristic	Unshielded Twisted Pair	Shielded Twisted Pair	Fiber-Optic
Cost	Least expensive	Moderate	Expensive
Maximum Length	100m (328ft)	100m (328ft)	>10 miles
Transmission Rates	10Mbps to 2Gbps	10Mbps to 10Gbps for Ethernet, Fast Ethernet, and Gigabit Ethernet; 16Mbps for token ring	100Mbps or more
Flexibility	Most flexible	Fair	Fair
Ease of Installation	Very easy	Very easy	Difficult
Interference	Susceptible	Not as susceptible as UTP	Not susceptible
Preferred Uses	10/100/1000BaseT	10/100/1000BaseT or token ring	Network segments requiring high-speed transmission
Connector	RJ-45	RJ-45 for Ethernet; IDC/UDC for token ring	ST/SC

Plenum/PVC

Plenum/PVC cable is a specific type of cable that is rated for use in plenum spaces. Plenum spaces are those in a building used for heating and air-conditioning systems. Most cable cannot be used in the plenum because of the danger of fire (or the fumes the cables give off as they burn). Plenum cable is fire-rated and meets the necessary standards, which makes it okay to use in these locations.

Exam Essentials

Know the network cable types. UTP is the cheapest type of cable to implement, but it's also the weakest. STP is more expensive, but it isn't subject to EMI. Fiber-optic cabling is the most expensive and most difficult to implement, but it offers the greatest combination of speed and distance.

Understand network cards and their purpose. A network interface card (NIC) is the physical component that allows a host to connect to a network at the Physical layer.

Different Network Types

There is some overlap between this objective and the coverage in the previous two objectives. The information that is unique to this domain focuses on wireless networking.

Critical Information

It's imperative that you understand the different types of networks, including broadband and wireless. The sections that follow will focus on the key issues associated with the different networking types.

Broadband Networks

Broadband networks can be created using several different technologies; CompTIA focuses on four of these:

DSL *Digital Subscriber Line* uses existing phone lines with a DSL modem and a network card. A standard RJ-45 connector is used to connect the network card to the DSL modem, and a phone cord with RJ-11 connectors is used to connect the DSL modem to the phone jack. Multiple types of DSL exist; the most popular are *high bit-rate DSL (HDSL)*, *symmetric DSL (SDSL)*, *very high bit-rate DSL (VDSL)*, *rate-adaptive DSL (RADSL)*, and *asymmetric DSL (ADSL)*. The latter provides slower upload than download speed and is the most common for home use.

Cable A popular alternative to DSL is a cable modem. Instead of the service coming from a telephone company, the service is provided by the cable provider and a *cable modem* is used in place of the DSL modem. While speeds vary based on the number of users the cable company is servicing, as a general rule cable-based broadband service is faster than DSL.

Satellite Whereas the other broadband technologies discussed require the use of physical wiring, with satellite broadband the service provider sends a microwave signal from dish to orbiting satellite and back. One satellite can service many receivers and so this is commonly known as *point-to-multipoint* technology. As a general rule, satellite connections are slower than the other broadband technologies you need to know for the exam.

Fiber Fiber-optic cabling provides excellent speed and bandwidth but is expensive. Not only are the cables that you use costly, but the light-emitting/receiving hardware costs also make this an expensive undertaking. Because of the cost involved, fiber is an option only for businesses when it comes to broadband access, and is not suitable for home use.

Dial-Up Networking

Whereas broadband holds great promise for high-speed connections, there are many people (quite a few in rural areas) who cannot take advantage of this. Thankfully, one of the first methods of remote access, dial-up networking, is still in existence. With dial-up, you simply add a modem to your computer and connect to an Internet service provider (ISP) over the existing phone lines, also known as the *Plain Old Telephone System (POTS)*. With a good connection, you can transmit and receive at 56Kbps.

Wireless Networks

One of the most fascinating cabling technologies today—actually, it doesn't really *use* cable—is wireless. Wireless networks offer the ability to extend a LAN without the use of traditional cabling methods. Wireless transmissions are made through the air by infrared light, laser light, narrow-band radio, microwave, or spread-spectrum radio.

Wireless LANs are growing increasingly popular as businesses become more mobile and less centralized. You can see them most often in environments where standard cabling methods aren't possible or wanted.

Wireless networking requires much the same type of equipment as traditional networking; the main difference is that the special versions of each item rely on radio frequency (RF) signals or infrared instead of cables. For example, each node needs a NIC that has a transceiver in it instead of a cable jack. In addition, there must be a central wireless access point (WAP), the equivalent of a hub, with which the wireless NICs communicate in all but a small ad hoc network.

The first wireless networking standard to become commercially popular was *IEEE 802.11b*, which could send and receive at up to 11Mbps. *IEEE 802.11a* extended that to 54Mbps and can reach over 100Mbps. The *IEEE 802.11g* standard provides for bandwidths of 20Mbps+ in the 2.4GHz frequency spectrum. This offers a maximum rate of 54Mbps and is backward compatible with 802.11b. The *IEEE 802.11n* standard is under development, as of this writing, and will support 100Mbps data rates in either the 2.4GHz or the 5GHz band (depending on which of the two proposals garner the required membership approval).

One of the biggest problems with wireless networks is being able to find and maintain a strong, usable signal. While the distance between the client and the access point is a crucial factor, so is the environment that exists between the two. Such elements as metal filing cabinets, cinder-block walls, and similar items can greatly reduce the strength of the signal, to the point where the user cannot function. Repeaters can help improve the strength of the signal and should be used as needed within the worksite.

To see the signal strength a Windows XP client is receiving, go to Network Connections (Start ➢ My Network Places ➢ View Network Connections), right-click on the wireless network icon, and choose Status. This will show the speed being attained.

Bluetooth Networking

Bluetooth is a short-range wireless standard that uses radio waves, for everything ranging from cell phone headsets to printers, keyboards, and handhelds. There are a number of Bluetooth specifications, all of which transmit in the 2.4–2.485GHz range. Three of these specifications are as follows:

- Version 1.2 supports data transmissions of up to 1Mbps and was adopted in 2003.
- Version 2.0+ is known as Enhanced Data Rate (EDR), and it was adopted in 2004.
- Version 2.1+ EDR can support data rates up to 3Mbps and it was adopted in 2007.

In addition to the three specifications, there are three device classes that differ in range and power usage. These three are as follows:

- Class 1 uses 100 milliwatts and can transmit 100 meters.
- Class 2 uses 2.5 milliwatts and can transmit 10 meters. This is the most common of the three. Devices that fall under Class 2 include headsets and gaming consoles.
- Class 3 uses only 1 milliwatt and has a limited range of only 1 meter. This one is rarely used.

The Bluetooth standard has addressed weaknesses in the technology, and it continues to get more secure. One of the simplest ways to secure Bluetooth devices is to not set their Discoverable attribute to one.

Cellular Networking

BlackBerries have made cellular networking popular, though they are not the only devices capable of using networking; for example, a cellular modem can also be quickly added to a laptop. Cellular networks use a central access point (a cell tower) in a mesh network design. The two competing standards are the *Global System for Mobile Communications (GSM)* and the *Code Division Multiple Access (CDMA)*. The former is the most popular around the world, and the latter exists only in the United States.

WAP/WEP

Wireless systems frequently use the Wireless Application Protocol (WAP) for network communications. Wired Equivalent Privacy (WEP) is intended to provide the equivalent security of a wired network protocol. The following sections briefly discuss these two terms and provide you with an understanding of their relative capabilities.

Wireless Access Protocol

The *Wireless Access Protocol (WAP)* is the technology designed for use with wireless devices. WAP has become a standard adopted by many manufacturers, including Motorola and Nokia. WAP functions are equivalent to TCP/IP functions in that they're trying to serve the same purpose for wireless devices. WAP uses a smaller version of HTML called *Wireless*

Markup Language (WML), which is used for Internet displays. WAP-enabled devices can also respond to scripts using an environment called *WMLScript*. This scripting language is similar to Java, which is a programming language.

The ability to accept web pages and scripts produces the opportunity for malicious code and viruses to be transported to WAP-enabled devices. No doubt this will create a new set of problems, and antivirus software will be needed to deal with them.

WAP systems communicate using a WAP gateway system. The gateway converts information back and forth between HTTP and WAP as well as encodes and decodes between the security protocols. This structure provides a reasonable assurance that WAP-enabled devices can be secured. If the interconnection between the WAP server and the Internet isn't encrypted, packets between the devices may be intercepted, creating a potential vulnerability. This vulnerability is called a *gap in the WAP*.

Wired Equivalent Privacy

Wired Equivalent Privacy (WEP) is a security standard for wireless devices. WEP encrypts data to provide data security. The protocol has always been under scrutiny for not being as secure as initially intended.

WEP is vulnerable due to weaknesses in the way the encryption algorithms are employed. These weaknesses allow the algorithm to potentially be cracked in as few as five minutes using available PC software. This makes WEP one of the most vulnerable protocols available for security.

Wi-Fi Protected Access

The *Wi-Fi Protected Access (WPA)* and *Wi-Fi Protected Access 2 (WPA2)* technologies were designed to address the core problems with WEP. These technologies implement the 802.11i standard. The difference between WPA and WPA2 is that the former implements most—but not all—of 802.11i in order to be able to communicate with older wireless cards (which might still need an update through their firmware in order to be compliant) while WPA2 implements the full standard and is not compatible with older cards.

Wireless Vulnerabilities to Know

Wireless systems are vulnerable to all the different attacks that wired networks are vulnerable to. However, because these protocols use radio frequency signals for *data emanation*, they have an additional weakness: all radio frequency signals can be easily intercepted. To intercept 802.11*x* traffic, all you need is a PC with an appropriate 802.11*x* card installed. Many networks will regularly broadcast their name (known as an *SSID broadcast*) to announce their presence. Simple software on the PC can capture the link traffic in the WAP and then process this data in order to decrypt account and password information.

An additional aspect of wireless systems is the *site survey*. Site surveys involve listening in on an existing wireless network using commercially available technologies. Doing so allows intelligence, and possibly data capture, to be performed on systems in your wireless network.

The term *site survey* initially meant determining whether a proposed location was free from interference. When used by an attacker, a site survey can determine what types of systems are in use, the protocols used, and other critical information about your network. It's the primary method used to gather data about wireless networks. Virtually all wireless networks are vulnerable to site surveys.

If wireless portals are installed in a building, the signals will frequently radiate past the inside of the building, and they can be detected and decoded outside the building using inexpensive equipment. The term *war driving* refers to driving around with a laptop looking for WAPs that can be communicated with. The network card on the laptop is set to promiscuous mode, and it looks for signals coming from anywhere. After intruders gain access, they may steal Internet access or start damaging your data.

Weak encryption was an issue with earlier access points, but most of the newer wireless controllers use special ID numbers (SSID) and must be configured in the network cards to allow communications. However, using ID number configurations doesn't necessarily prevent wireless networks from being monitored, and one particularly mischievous undertaking involves taking advantage of *rogue access points*. Any wireless access point added to your network that has not been authorized is considered a rogue. The rogue may be added by an attacker, or could have been innocently added by a user wanting to enhance their environment—the problem with the user so doing is that there is a good chance they will not implement the security you would and this could open the system up for a man-in-the-middle attack.

Never assume that a wireless connection is secure. The emissions from a wireless portal may be detectable through walls and for several blocks from the portal. Interception is easy to accomplish, given that RF is the medium used for communication. Newer wireless devices offer data security, and you should use it. You can set newer WAPs and wireless routers to non-broadcast in addition to configuring WEP at a higher encryption level. Given the choice, you should choose to use WPA2, WPA, or WEP at its highest encryption level in that order.

One way to increase security is to implement *MAC filtering*. Every network card has a unique 48-bit address assigned to it—half of which identifies the vendor of the card, and the other half of which acts like a serial number. When MAC filtering is implemented, you identify each host by this number and determine specifically which addresses are allowed access the network. While a great security tool, bear in mind that it is identifying the NIC card and not the person sitting at that machine, so it cannot ever be the only form of authentication employed.

The CompTIA objectives also list DHCP settings beneath objective 4.3, but DHCP has been fully covered earlier in this chapter.

Exam Essentials

Understand wired and wireless connectivity. Networks work the same whether there is a physical wire between the hosts or that wire has been replaced by a wireless signal. The same order of operations and steps are carried out regardless of the medium employed.

Know the steps of troubleshooting. Always begin troubleshooting by trying to isolate the problem and understanding how widespread it is. Before you begin drastic operations, make certain the issue isn't confined to just one user.

Know what troubleshooting tools exist. Be familiar with the network troubleshooting tools that exist and what each one can do.

Review Questions

1. What is the difference between full and half duplexing?
2. What is another name for a server-based network?
3. What is the difference between baseband and broadband?
4. Which layer of the OSI model takes data from the upper layers and prepares it for sending across the Physical layer?
5. At which layers of the OSI model does a gateway operate?
6. What is the term for the rules that govern the communications between network clients?
7. What is the term for a network that uses public media, such as the Internet, to connect the nodes?
8. Which type of server translates hostnames to IP addresses?
9. What is the default subnet mask value for a host with a Class B address?
10. What is Bluetooth?

Answers to Review Questions

1. Duplexing is the means by which communication takes place. With full duplexing, everyone can send and receive at the same time. With half duplexing, communications travel in both directions but in only one direction at any given time.
2. A server-based network is also known as a client/server network or a domain.
3. With baseband, the entire medium's capacity is used for one signal. The speed possibilities are thus increased because the entire channel is utilized. With broadband, the medium is used to carry multiple signals.
4. The Data Link layer takes data from the upper layers and prepares it for sending across the Physical layer.
5. A gateway operates at the top four layers: Application, Presentation, Session, and Transport.
6. A protocol is a set of rules that governs the communications between clients.
7. VPNs are used to make connections between private networks across a public network, such as the Internet.
8. A Domain Name Service (DNS) server translates hostnames to IP addresses.
9. The default subnet mask value for a host with a Class B address is 255.255.0.0.
10. Bluetooth is a short-range wireless standard.

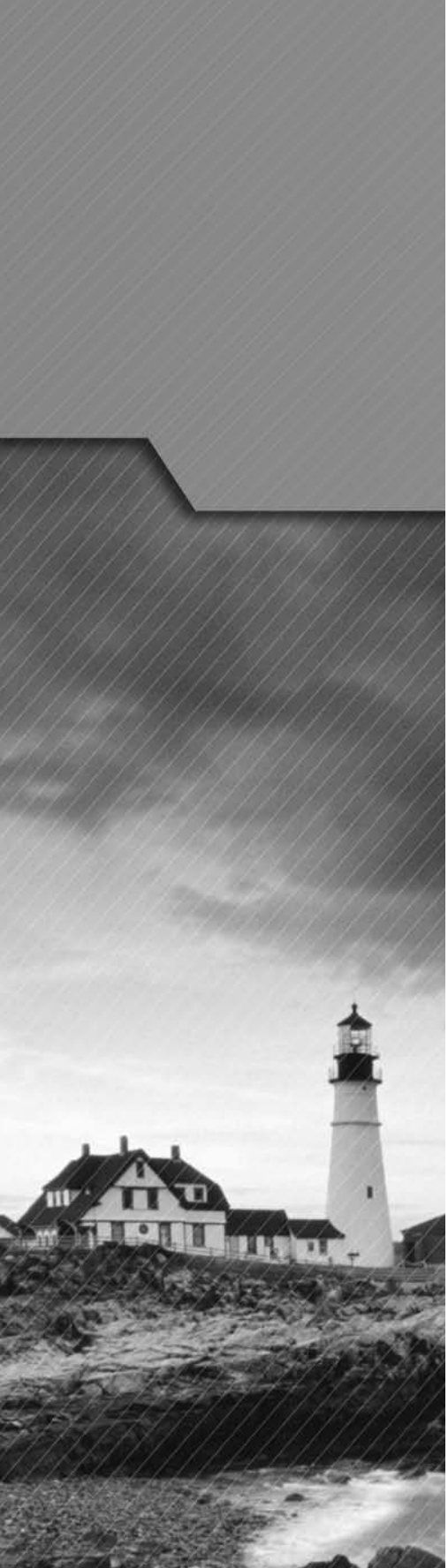
Chapter

5

Security

COMPTIA A+ ESSENTIALS EXAM OBJECTIVES COVERED IN THIS CHAPTER:

- ✓ **5.1 Explain the basic principles of security concepts and technologies**
  - Encryption technologies
  - Data wiping / hard drive destruction / hard drive recycling
  - Software firewall
    - Port security
    - Exceptions
  - Authentication technologies
    - User name
    - Password
    - Biometrics
    - Smart cards
  - Basics of data sensitivity and data security
    - Compliance
    - Classifications
    - Social Engineering
- ✓ **5.2 Summarize the following security features**
  - Wireless encryption
    - WEP*x* and WPA*x*
    - Client configuration (SSID)
  - Malicious software protection
    - Viruses
    - Trojans
    - Worms
    - Spam



- Spyware
- Adware
- Grayware

- BIOS Security
  - Drive lock
  - Passwords
  - Intrusion detection
  - TPM
- Password management / password complexity
- Locking workstation
  - Hardware
  - Operating system
- Biometrics
  - Fingerprint scanner

Given the ever-increasing need for security knowledge in the real world, CompTIA expects those who become A+ certified to have a basic knowledge and understanding of the principles behind it. The two subobjectives in this category do a good job of providing a thorough overview of the topic, and we visit this topic again in the elective exam section (see Chapter 10).

Explain the Basic Principles of Security

Security is unlike any other topic in computing. The word *security* is so encompassing that it's impossible to know exactly what you mean when you say it. When you talk about security, do you mean physically securing servers and workstations from those who might try to steal them, or from damage that may occur if the side of the building collapses? Or do you mean the security of data from viruses and worms and the means by which you keep those threats from entering the network? Or do you mean security of data from hackers and miscreants who have targeted you and have no other purpose in life than to keep you up at night? Or is security the comfort that comes from knowing you can restore files if a user accidentally deletes them?

The first problem with security is that it's next to impossible to have everyone agree on what it means, because it can include all these items. The next problem is that we don't *really* want things to be completely secured. For example, if you wanted your customer list file to be truly secure, you wouldn't put it on the server and make it available. It's on the server because you need to access it, and so do 30 other people. In this sense, security means that only 30 select people can get to the data.

The next problem is that although everyone wants security, no one wants to be inconvenienced by it. To use an analogy, most travelers feel safer by watching airport personnel pat down everyone who heads to the terminal—they just don't want it to happen to them. This is true in computing as well; we all want to make sure data is accessed only by those who truly should be working with it, but we don't want to have to enter 12-digit passwords and submit to retinal scans.

As a computer professional, you have to understand all these concerns. You have to know that a great deal is expected of you, but few people want to be hassled or inconvenienced by the measures you must put in place. You have a primary responsibility to protect and safeguard the information your organization uses. Many times, that means educating your users and making certain they understand the "why" behind what is being implemented.

Physical security, as the name implies, involves protecting your assets and information from physical access by unauthorized personnel. In other words, you're trying to protect those items that can be seen, touched, and stolen. These threats often present themselves as service technicians, janitors, customers, vendors, or even employees. They can steal your equipment, damage it, or take documents from offices, garbage cans, or filing cabinets. Their motivation may be retribution for some perceived misgiving, a desire to steal your trade secrets to sell to a competitor as an act of vengeance, or just greed. They might steal $1,000 worth of hardware that they can sell to a friend for a fraction of that and have no concept of the value of the data stored on the hardware.

Physical security is relatively easy to accomplish. You can secure facilities by controlling access to the office, shredding unneeded documents, installing security systems, and limiting access to sensitive areas of the business. Most office buildings provide perimeter and corridor security during unoccupied hours, and it isn't difficult to implement common-sense measures during occupied hours as well. Sometimes just having a person present—even a guard who spends much of the time sleeping—can be all the deterrent needed to prevent petty thefts.

Many office complexes also offer roving security patrols, multiple-lock access control methods, and electronic or password access. Typically, the facility managers handle these arrangements. They won't generally deal with internal security as it relates to your records, computer systems, and papers; that is your responsibility in most situations.

The first component of physical security involves making a physical location less tempting as a target. If the office or building you're in is open all the time, gaining entry into a business in the building is easy. You must prevent people from seeing your organization as a tempting target. Locking doors and installing surveillance or alarm systems can make a physical location a less desirable target. You can also add controls to elevators, requiring keys or badges in order to reach upper floors. Plenty of wide-open targets are available, involving less risk on the part of the people involved. Try to make your office not worth the trouble.

The second component of physical security involves detecting a *penetration* or theft. You want to know what was broken into, what is missing, and how the loss occurred. Passive videotape systems are one good way to obtain this information. Most retail environments routinely tape key areas of the business to identify how thefts occur and who was involved. These tapes are admissible as evidence in most courts. Law enforcement should be involved as soon as a penetration or theft occurs. More important from a deterrent standpoint, you should make it well known that you'll prosecute to the fullest extent of the law anyone caught in the act of theft. Making the video cameras as conspicuous as possible will deter many would-be criminals.

The third component of physical security involves recovering from a theft or loss of critical information or systems. How will the organization recover from the loss and get on with normal business? If a vandal destroyed your server room with a fire or flood, how long would it take your organization to get back into operation and return to full productivity?

Recovery involves a great deal of planning, thought, and testing. What would happen if the files containing all your bank accounts, purchase orders, and customer information became a pile of ashes in the middle of the smoldering ruins that used to be your office? Ideally, critical copies of records and inventories should be stored off-site in a secure facility.

Critical Information

When discussing computer security in terms of exam preparation, you must be able to identify encryption technologies, the importance of data wiping, software firewall, authentication technologies, and the basics of data sensitivity/security. These five topics are discussed in the sections that follow.

Encryption Technologies

Cryptographic algorithms are used to encode a message from its unencrypted or clear-text state into an encrypted message. The three primary methods are hashing, symmetric, and asymmetric.

Hashing is the process of converting a message, or data, into a numeric value. The numeric value that a hashing process creates is referred to as a *hash total* or *value*. Hashing functions are considered either one-way or two-way. A one-way hash doesn't allow a message to be decoded back to the original value. A two-way hash allows a message to be reconstructed from the hash. Most hashing functions are one-way hashing. Two primary standards exist that use the hashing process for encryption:

Secure Hash Algorithm (SHA) The *Secure Hash Algorithm (SHA)* was designed by the National Security Agency (NSA) to ensure the integrity of a message. The SHA is a one-way hash that provides a hash value that can be used with an encryption protocol. This algorithm produces a 160-bit hash value. SHA has been updated; the first is now referred to as SHA-0, and the new standard is SHA-1.

There is also an SHA-2, but it has failed to catch on in popularity. SHA-3 is in development and expected to be released by 2012.

Message Digest Algorithm (MDA) The *Message Digest Algorithm (MDA)* also creates a hash value and uses a one-way hash. The hash value is used to help maintain integrity. There are several versions of MD; the most common are MD5, MD4, and MD2, all of which use an output size of 128 bits.

Symmetric algorithms require both ends of an encrypted message to have the same key and processing algorithms. Symmetric algorithms generate a secret key that must be protected. A secret key—sometimes referred to as a *private key*—is a key that isn't disclosed to people who aren't authorized to use the encryption system. The disclosure of a private key breaches the security of the encryption system. If a key is lost or stolen, the entire process is breached. These types of systems are common.

Asymmetric algorithms use two keys to encrypt and decrypt data. These keys are referred to as the *public key* and the *private key*. The public key can be used by the sender to encrypt a message, and the private key can be used by the receiver to decrypt the message. Symmetrical systems require the key to be private between the two parties, but with asymmetric systems, each circuit has one key.

The public key may be truly public, or it may be a secret between the two parties. The private key is kept private and is known only by the owner (receiver). If someone wants to

send you an encrypted message, they can use your public key to encrypt the message and then send you the message. You can use your private key to decrypt the message. One of the keys is always kept private. If both keys become available to a third party, the encryption system won't protect the privacy of the message.

Perhaps the best way to think about this system is that it's similar to a safe-deposit box. Two keys are needed: the box owner keeps the public key, and the bank retains the second or private key. To open the box, both keys must be used simultaneously.

Data Wiping

When it comes to hardware, CompTIA expects you to understand that although the user interacts with software, the hardware actually stores the data. The hardware in question can be a hard disk, a backup tape, or some other storage device. This overly simplistic concept is important when it comes to choosing how to dispose of hardware.

If it's possible to verify beyond a reasonable doubt that a piece of hardware that's no longer being used doesn't contain any data of a sensitive or proprietary nature, then that hardware can be recycled (sold to employees, sold to a third party, donated to a school, and so on). That level of assurance can come from wiping a hard drive, reformatting it, or using specialized utilities. When computer systems are retired, the disk drives should be zeroed out, and all magnetic media should be degaussed. Degaussing involves applying a strong magnetic field to initialize the media (this is also referred to as *disk wiping*). Erasing files on a computer system doesn't guarantee that the information isn't still on the disk; a low-level format—which can require a special utility from the manufacturer—can be performed on the system, or a utility can be used to completely wipe the disk clean. This process helps ensure that information doesn't fall into the wrong hands.

If you can't be assured that the hardware in question doesn't contain important data, then the hardware should be destroyed. You cannot, and should not, take a risk that the data your company depends on could fall into the wrong hands.

Software Firewall

Firewalls are one of the first lines of defense in a network. There are different types of firewalls, and they can be either stand-alone systems or included in other devices such as routers or servers. You can find firewall solutions that are marketed as hardware-only and others that are software-only. Many firewalls, however, consist of add-in software that is available for servers or workstations.

Although solutions are sold as hardware-only, the hardware still runs some sort of software. It may be hardened and in ROM to prevent tampering, and it may be customized—but software is present, nonetheless.

The basic purpose of a firewall is to isolate one network from another. Firewalls are becoming available as appliances, meaning they're installed into the network between two networks. *Appliances* are freestanding devices that operate in a largely self-contained manner, requiring less maintenance and support than a server-based product.

Firewalls function as one or more of the following:

- Packet filter
- Proxy firewall
- Stateful inspection

Let's look at each of these.

Packet Filter

A firewall operating as a *packet filter* passes or blocks traffic to specific addresses/ports based on the type of application. The packet filter doesn't analyze the contents of a packet; it decides whether to pass it based on the packet's addressing information. For instance, a packet filter may allow web traffic on port 80 and block Telnet traffic on port 23. This type of filtering is included in many routers. If a received packet request asks for a port that isn't authorized, the filter may reject the request or ignore it. Many packet filters can also specify which IP addresses can request which ports and allow or deny them based on the security settings of the firewall. Items that are allowed to pass through are configured as *exceptions*.

Proxy Firewall

You can think of a *proxy firewall* as an intermediary between your network and any other network. Proxy firewalls are used to process requests from an outside network; the proxy firewall examines the data and makes rules-based decisions about whether the request should be forwarded or refused. The proxy intercepts all the packages and reprocesses them for use internally. This process includes hiding IP addresses.

Stateful Inspection

Stateful inspection is also referred to as *stateful packet filtering*. Most of the devices used in networks don't keep track of how information is routed or used. Once a packet is passed, the packet and path are forgotten. In stateful inspection (or stateful packet filtering), records are kept using a state table that tracks every communications channel. Stateful inspections occur at all levels of the network and provide additional security, especially in connectionless protocols.

Authentication Technologies

Authentication proves that a user or system is actually who they say they are. This is one of the most critical parts of a security system. It's part of a process that is also referred to as *identification and authentication* (*I&A*). The identification process starts when a user ID or logon name is typed into a sign-on screen. Authentication is accomplished by challenging the claim about who is accessing the resource. Without authentication, anybody can claim to be anybody.

Authentication systems or methods are based on one or more of these three factors:

- Something you know, such as a password or PIN
- Something you have, such as a smart card or an identification device
- Something physically unique to you, such as your fingerprints or retinal pattern

Systems authenticate each other using similar methods. Frequently, systems pass private information between one another to establish identity. Once authentication has occurred, the systems can communicate in the manner specified in the design.

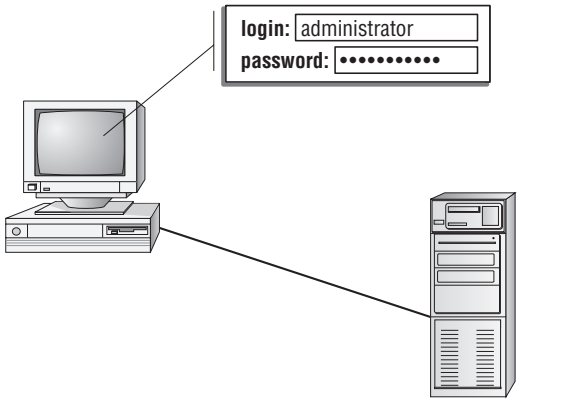
Several common methods are used for authentication. Each has advantages and disadvantages that must be considered when you're evaluating authentication schemes.

Username/Password

A username and password are unique identifiers for a logon process. When users sit down in front of a computer system, the first thing a security system requires is that they establish who they are. Identification is typically confirmed through a logon process. Most operating systems use a user ID and password to accomplish this. These values can be sent across the connection as plain text or can be encrypted.

The logon process identifies to the operating system, and possibly the network, that you are who you say you are. Figure 5.1 illustrates this logon and password process. Notice that the operating system compares this information to the stored information from the security processor and either accepts or denies the logon attempt. The operating system may establish privileges or permissions based on stored data about that particular ID.

FIGURE 5.1 A logon process occurring on a workstation



Password Authentication Protocol (PAP)

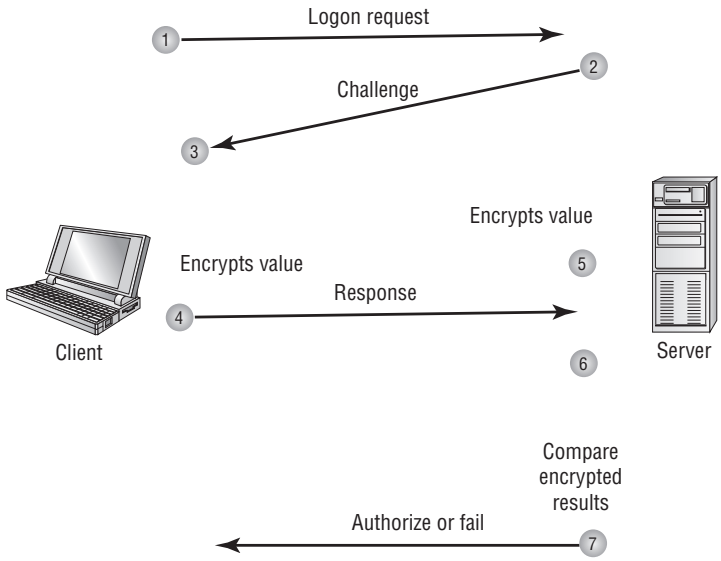
Password Authentication Protocol (PAP) offers no true security, but it's one of the simplest forms of authentication. The username and password values are both sent to the server as clear text and checked for a match. If they match, the user is granted access; if they don't match, the user is denied access. In most modern implementations, PAP is shunned in favor of other, more secure, authentication methods.

Challenge Handshake Authentication Protocol (CHAP)

Challenge Handshake Authentication Protocol (CHAP) challenges a system to verify identity. CHAP doesn't use a user ID/password mechanism. Instead, the initiator sends a logon request

from the client to the server. The server sends a challenge back to the client. The challenge is encrypted and then sent back to the server. The server compares the value from the client and, if the information matches, grants authorization. If the response fails, the session fails and the request phase starts over. Figure 5.2 illustrates the CHAP procedure. This handshake method involves a number of steps and is usually automatic between systems after it's configured.

FIGURE 5.2 CHAP authentication



Certificates

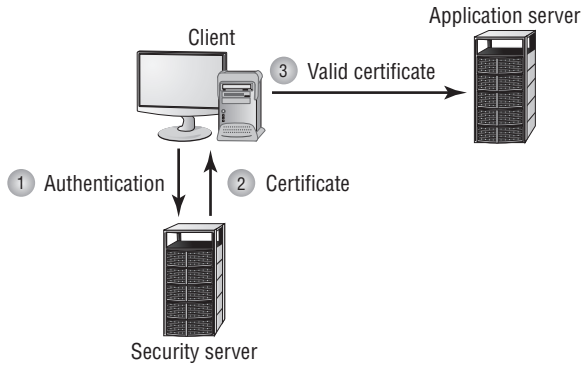
Certificates are another common form of authentication. A server or *certificate authority (CA)* can issue a certificate that will be accepted by the challenging system. Certificates can be either physical access devices, such as smart cards, or electronic certificates that are used as part of the logon process. A *certificate practice statement (CPS)* outlines the rules used for issuing and managing certificates. A *certificate revocation list (CRL)* lists the revocations that must be addressed (often due to expiration) in order to stay current.

A simple way to think of certificates is like hall passes at school. Figure 5.3 illustrates a certificate being handed from the server to the client once authentication has been established. If you have a hall pass, you can wander the halls of your school. If your pass is invalid, the hallway monitor can send you to the principal's office. Similarly, if you have a certificate, you can prove to the system that you are who you say you are and are authenticated to work with the resources.

Security Tokens

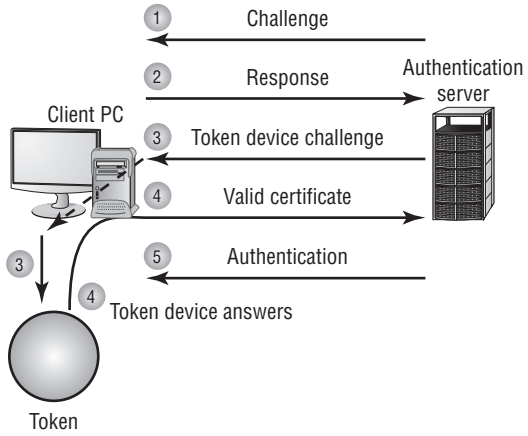
Security tokens, which may be hardware- or software-based, are similar to certificates. They contain the rights and access privileges of the token bearer as part of the token. Think of a token as a small piece of data that holds a sliver of information about the user.

FIGURE 5.3 A certificate being issued once identification has been verified



Many operating systems generate a token that is applied to every action taken on the computer system. If your token doesn't grant you access to certain information, then either that information won't be displayed or your access will be denied. The authentication system creates a token every time a user connects or a session begins. At the completion of a session, the token is destroyed. Figure 5.4 shows the security token process.

FIGURE 5.4 Security token authentication



Kerberos

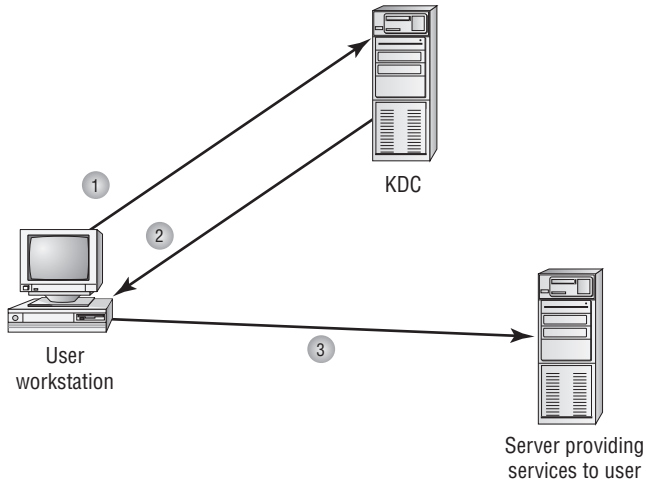
Kerberos is an authentication protocol named after the mythical three-headed dog that stood at the gates of Hades. Originally designed by MIT, Kerberos is becoming very popular as an authentication method. It allows for a single sign-on to a distributed network.

Kerberos authentication uses a *key distribution center* (*KDC*) to orchestrate the process. This KDC consists of both an authentication server (AS) and ticket-granting server (TGS). The KDC authenticates the *principal* (which can be a user, a program, or a system) and provides it

with a ticket. Once this ticket is issued, it can be used to authenticate against other principals. This occurs automatically when a request or service is performed by another principal.

Kerberos is quickly becoming a common standard in network environments. Its only significant weakness is that the KDC can be a single point of failure. If the KDC goes down, the authentication process will stop. If the KDC is compromised by a miscreant, then authentication is jeopardized. Figure 5.5 shows the Kerberos authentication process and the ticket being presented to systems that are authorized by the KDC.

FIGURE 5.5 Kerberos authentication process



1. User requests access to service running on a different server
2. KDC authenticates user and sends a ticket to be used between the user and the service on the server
3. User's workstation sends a ticket to the service

Multifactor Authentication

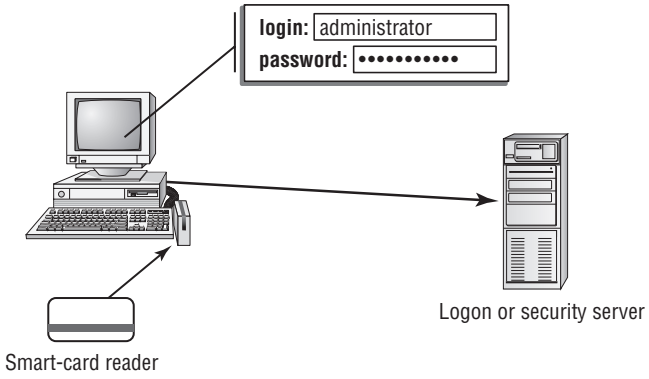
When two or more access methods are included as part of the authentication process, you're implementing a *multifactor* system. A system that uses smart cards and passwords is referred to as a *two-factor authentication* system. Two-factor authentication is shown in Figure 5.6. This example requires both a smart card and a logon password.

Smart Cards

A *smart card* is a type of badge or card that gives you access to resources, including buildings, parking lots, and computers. It contains information about your identity and access privileges. Each area or computer has a card scanner or a reader in which you insert your card.

The reader is connected to the workstation and validates against the security system. This increases the security of the authentication process, because you must be in physical possession of the smart card to use the resources. Of course, if the card is lost or stolen, the person who finds the card can access the resources it allows.

FIGURE 5.6 Two-factor authentication



Most smart cards also require the use of a PIN, just in case the card is lost or stolen.

Smart cards are difficult to counterfeit, but they're easy to steal. Once a thief has a smart card, they have all the access the card allows. To prevent this, many organizations don't put any identifying marks on their smart cards, making it harder for someone to utilize them. Many modern smart cards require a password or PIN to activate the card, and employ encryption to protect the card's contents.

Many European countries are beginning to use smart cards instead of magnetic-strip credit cards because they offer additional security and can contain more information.

Biometrics

Biometric devices use physical characteristics to identify the user. Such devices are becoming more common in the business environment. Biometric systems include hand scanners, retinal scanners, and soon, possibly, DNA scanners. To gain access to resources, you must pass a physical screening process. In the case of a hand scanner, this may include identifying fingerprints, scars, and markings on your hand. Retinal scanners compare your eye's retinal pattern to a stored retinal pattern to verify your identity. DNA scanners will examine a unique portion of your DNA structure in order to verify that you are who you say you are.

Key Fobs

Key fobs are named after the chains that used to hold pocket watches to clothes. They are security devices that you carry with you that display a randomly generated code that you can then use for authentication. This code usually changes very quickly (every 60 seconds is probably the average), and you combine this code with your PIN for authentication.

Authentication Issues to Consider

You can set up many different parameters and standards to force the people in your organization to conform. In establishing these parameters, it's important that you consider the capabilities of the people who will be working with these policies. If you're working in an environment where people aren't computer savvy, you may spend a lot of time helping them remember and recover passwords. Many organizations have had to reevaluate their security guidelines after they've invested great time and expense to implement high-security systems.

Setting authentication security, especially in supporting users, can become a high-maintenance activity for network administrators. On one hand, you want people to be able to authenticate themselves easily; on the other hand, you want to establish security that protects your company's resources.

Be wary of popular names or current trends that make certain passwords predictable. For example, during the first release of *Star Wars*, two of the most popular passwords used on college campuses were C3PO and R2D2. This created a security problem for campus computer centers.

Basics of Data Sensitivity/Security

Information classification is a key aspect of a secure network. Again, the process of developing a classification scheme is both a technical and a human issue. The technologies you use must be able to support your organization's privacy requirements. People and processes must be in place and working effectively to prevent unauthorized disclosure of sensitive information.

If you think about all the information your organization keeps, you'll probably find that it breaks down into three primary categories: public use, internal use, and restricted use. Approximately 80 percent of the information in your organization is primarily for internal or private use. This information would include memos, working papers, financial data, and information records, among other things.

In the following sections, I'll discuss the various information classification systems, roles in the security process, and information access controls.

Public Information

Public information is primarily information that is made available either to the larger public or to specific individuals who need it. Financial statements of a privately held organization might be information that is available publicly, but only to individuals or organizations that have a legitimate need for it.

The important thing to keep in mind is that an organization needs to develop policies about what information is available and for what purposes it will be disseminated. It's also helpful to make sure that members of the organization know who has authorization to make these kinds of disclosures. There are organizations that gather competitive data for a fee; they often use social-engineering approaches to gain information about a business. Good policies help prevent accidents from occurring with sensitive information.

Let's discuss the difference between limited and full distribution:

Limited Distribution *Limited distribution* information isn't intended for release to the public. This category of information isn't secret, but it's private. If a company is seeking to obtain a line of credit, the information provided to a bank is of a private nature. This information, if disclosed to competitors, might give them insight into the organization's plans or financial health. If disclosed to customers, it might scare them and cause them to switch to a competitor.

Some end-user license agreements (EULAs) now limit the information that users can disclose about problems with their software. These new statements have not yet been challenged in court. Try to avoid being the test case for this new and alarming element of some software licenses; read the EULA before you agree to it.

These types of disclosures are usually held in confidence by banks and financial institutions. These institutions will typically have privacy and confidentiality regulations as well as policies that must be followed by all employees of the institution.

Software manufacturers typically release early versions of their products to customers who are willing to help evaluate functionality. Early versions of software may not always work properly, and they often have features that aren't included in the final version. This version of the software is a *beta test*. Before beta testers are allowed to use the software, they're required to sign a nondisclosure agreement (NDA). The NDA tells the tester what privacy requirements exist for the product. The product being developed will change, and any problems with the beta version probably won't be a great secret. However, the NDA reminds the testers of their confidentiality responsibilities.

NDAs are common in the technology arena. Make sure you read any NDA thoroughly before you sign it. You don't have to sign an NDA to be bound by it: if you agree that you'll treat the information as private and then receive the information, you have in essence agreed to an NDA. In most cases, this form of verbal NDA is valid for only one year.

Statements indicating privacy or confidentiality are common on limited-access documents. They should indicate that disclosure of the information without permission is a breach of confidentiality. This may help someone remember that the information isn't for public dissemination.

Full Distribution Marketing materials are examples of information that should be available for *full distribution*. Annual reports to stockholders and other information of a public-relations orientation are also examples of full distribution materials.

The key element of the full distribution classification involves decision-making responsibility. Who makes the decision about full disclosure? Larger organizations have a corporate communications department that is responsible for managing this process. If you aren't sure, it's a

good idea to ask about dissemination of information. Don't assume that you know: this is the purpose of an information classification policy.

Private Information

Private information is intended only for use internally in the organization. This type of information could potentially embarrass the company, disclose trade secrets, or adversely affect personnel. Private information may also be referred to as *working documents* or *work product*. It's important that private information not be disclosed because it can potentially involve litigation if the disclosure was improper.

Let's look at the difference between internal and restricted information:

Internal Information *Internal information* includes personnel records, financial working documents, ledgers, customer lists, and virtually any other information that is needed to run a business. This information is valuable and must be protected.

In the case of personnel and medical records, disclosure to unauthorized personnel creates liability issues. Many organizations are unwilling to do anything more than verify employment because of the fear of unauthorized disclosure.

A school views student information as internal. Schools can't release information about students without specific permission from the student.

Restricted Information *Restricted information* could seriously damage the organization if disclosed. It includes proprietary processes, trade secrets, strategic information, and marketing plans. This information should never be disclosed to an outside party unless senior management gives specific authorization. In many cases, this type of information is also placed on a *need-to-know basis*—unless you need to know, you won't be informed.

Government and Military Classifications

The U.S. government and the military have a slightly different set of concerns relating to information classification. Governmental agencies are concerned about privacy and national security. Because of this, a unique system of classification and access controls has been implemented to protect information.

Here is a list of some of the types of government classifications:

Unclassified This classification is used to indicate that the information poses no risk of potential loss due to disclosure. Anybody can gain access to this category of information. Many training manuals and regulations are unclassified.

Sensitive but Unclassified This classification is used for low-level security. It indicates that disclosure of this information might cause harm but wouldn't harm national defense efforts. The amount of toilet paper a military base uses may be considered sensitive because this information might help an intelligence agency guess at the number of personnel on the base.

Confidential This classification is used to identify low-level secrets; it's generally the lowest level of classification used by the military. It's used extensively to prevent access to sensitive information. Information that is lower than Confidential is generally considered Unclassified. The Confidential classification, however, allows information to be restricted for access under the Freedom of Information Act. The maintenance requirements for a machine gun may be classified as Confidential; this information would include drawings, procedures, and specifications that disclose how the weapon works.

Secret Secret information, if disclosed, could cause serious and irreparable damage to defense efforts. Information that is classified as Secret requires special handling, training, and storage. This information is considered a closely guarded secret of the military or government. Troop movements, deployments, capabilities, and other plans would be minimally classified as Secret. The military views the unauthorized disclosure of Secret information as criminal and potentially treasonous.

Top Secret The Top Secret classification is the highest classification level. It is rumored that there are higher levels of classification, but the names of those classifications are themselves classified Top Secret. Releasing information that is classified as Top Secret poses a grave threat to national security, and therefore it must not be compromised. Information such as intelligence activities, nuclear war plans, and weapons systems development would normally be classified as Top Secret.

The government has also developed a process to formally review and downgrade classification levels on a regular basis. This process generally downgrades information based on age, sensitivity, and usefulness. There are methods of overriding this downgrade process to prevent certain information from being declassified; some secrets are best left secret.

The military also uses an additional method of classifying information and access, which has the effect of compartmentalizing information. For example, if you were a weapons developer, it isn't likely that you would need access to information from spy satellites. You would be given special access to information necessary for the specific project you were working on. When the project was finished, access to this special information would be revoked. This process allows information to be protected and access limited to a need-to-know basis.

The process of obtaining a security clearance either for the military or for a government contractor can be quite involved. The normal process involves investigating you, your family, and potentially anybody else who could put you in a compromised position. The process can take months, and it includes agents doing fieldwork to complete, or augment, the investigation.

Roles in the Security Process

Effective security management requires the establishment of a clear set of roles and responsibilities for everyone involved in the process:

Owner The *owner* of data is primarily responsible for establishing its protection and use. The owner, in most situations, is a senior manager or other decision maker within an organization. The owner is responsible for making sure everyone follows all relevant and appropriate laws and regulations. Ultimately, the owner usually delegates some or all of the roles associated with the data to other individuals in the organization.

Custodian The *custodian* of data is responsible for maintaining and protecting it. In a computer environment, the custodian is usually the IT department. Network administrators, backup operators, and others perform custodial functions on the data. The security policies, standards, and guidelines should lay out these responsibilities and provide mechanisms to perform them.

User The *user* is the person or department that uses data. Users of data may perform input, output, editing, and other functions allowed by the role they have in the process.

Two additional roles warrant discussion, and you may find yourself doing one or both of them:

Security Professional *Security professionals* are concerned with one or more aspects of the process. They may be investigators, implementers, testers, or policy developers. Investigators become involved in the process when a security problem has been identified. Testers, on the other hand, may be called to look for exploits or to test security processes for weaknesses. Policy developers help management develop and implement policies for the organization.

Security professionals frequently encounter information they normally wouldn't need to know. Discretion is a critical skill for a security professional. For example, you may be asked to deny the existence of certain information in an organization. This implicit trust relationship shouldn't be taken lightly.

Auditor *Auditors* are involved in the process of ensuring that practices, policies, mechanisms, and guidelines are followed within an organization. This function may involve reviewing documentation, reviewing activity logs, conducting interviews, and performing any number of other tasks necessary to ensure that organizational security policies are followed. The role of the auditor isn't that of a police officer but rather a consultant. An auditor can help an organization identify and correct deficiencies in security.

Each of these roles presents a special challenge and exposes you to information and processes that most individuals wouldn't encounter in an organization. It's important that you take these responsibilities seriously; you shouldn't divulge the information or processes you uncover to any unauthorized individuals. You must hold yourself to a higher standard than those around you.

Information Access Controls

Access control defines the methods used to ensure that users of your network can access only what they're authorized to access. The process of access control should be spelled out in the organization's security policies and standards. Several models exist to accomplish this. Regardless of the model you use, a few concepts carry over among them:

- *Implicit denies* are those wherein you specifically lock certain users out. In Unix and Linux, for example, you can choose who can use the `at` service by configuring either an `at.allow` or `at.deny` file. If you configure the `at.allow` file, then only those users specifically named can use the service and all others cannot. Conversely, if you configure the `at.deny` file, then only the users named in that file cannot use the service (you are implicitly denying them) and all others can.
- *Least privilege* is the model you should use when assigning permissions. Give users only the permissions they need to do their work and no more.

Rotate jobs on a frequent enough basis that you are not putting yourself—and your data—at the mercy of any one administrator. Just as you want redundancy in hardware, you want redundancy in abilities.

Several models of compliance exist to accomplish this. This section will briefly explain the following models and the classifications they use:

- Bell-La Padula
- Biba
- Clark-Wilson
- Information Flow model
- Noninterference model

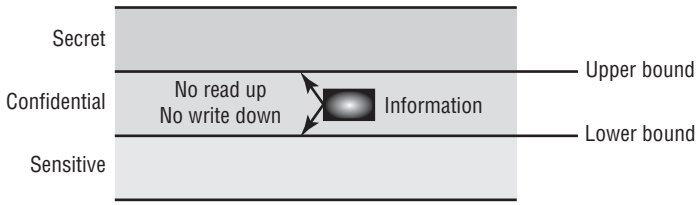
Bell-La Padula Model

The *Bell-La Padula model* was designed for the military to address the storage and protection of classified information. The model is specifically designed to prevent unauthorized access to classified information. It prevents the user from accessing information that has a higher security rating than they're authorized to access. The model also prevents information from being written to a lower level of security.

For example, if you're authorized to access Secret information, you aren't allowed to access Top Secret information, nor are you allowed to write to the system at a level lower than the Secret level. This creates upper and lower bounds for information storage. This process is illustrated in Figure 5.7. Notice in the illustration that you can't *read up* or *write down*. This means that a user can't read information at a higher level than they're authorized to access. A person writing a file can't write down to a lower level than the security level they're authorized to access.

The process of preventing a write-down keeps a user from accidentally breaching security by writing Secret information to the next lower level, Confidential. In our example, you can read Confidential information, but because you're approved at the Secret level, you can't write to the Confidential level. This model doesn't deal with integrity, only confidentiality. A user of Secret information can potentially modify other documents at the same level they possess.

FIGURE 5.7 The Bell-La Padula model



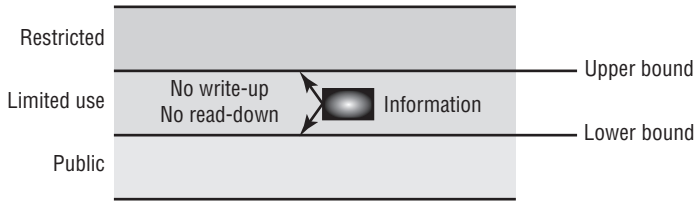
To see how this model works, think about corporate financial information. The chief financial officer (CFO) may have financial information about the company that they need to protect. The Bell-La Padula model keeps them from inadvertently posting information at an access level lower than their access level (writing down), thus preventing unauthorized or accidental disclosure of sensitive information. Lower-level employees can't access this information because they can't read up to the level of the CFO.

The Biba Model

The *Biba model* was designed after the Bell-La Padula model. It's similar in concept to the Bell-La Padula model, but it's more concerned with information integrity, an area that the Bell-La Padula model doesn't address. In this model, there is no write-up or read-down. In short, if you're assigned access to Top Secret information, you can't read Secret information or write to any level higher than the level to which you're authorized. This keeps higher-level information pure by preventing less-reliable information from being intermixed with it. Figure 5.8 illustrates this concept in more detail. The Biba model was developed primarily for industrial uses, where confidentiality is usually less important than integrity.

Think about the data that is generated by a researcher for a scientific project. The researcher is responsible for managing the results of research from a lower-level project and incorporating it into their research data. If bad data were to get into their research, the whole research project would be ruined. With the Biba model, this accident can't happen. The researcher doesn't have access to the information from lower levels: that information must be promoted to the level of the researcher. This system keeps the researcher's data intact and prevents accidental contamination.

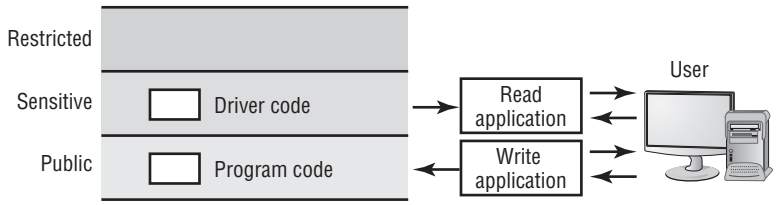
FIGURE 5.8 The Biba model



The Clark-Wilson Model

The *Clark-Wilson model* was developed after the Biba model. The approach is a little different from either the Biba or the Bell-La Padula method. In this model, data can't be accessed directly; it must be accessed through applications that have predefined capabilities. This process prevents unauthorized modification, errors, and fraud from occurring. If a user needs access to information at a certain level of security, a specific program is used. This program may allow only read access to the information. If a user needs to modify data, another application must be used. This allows a separation of duties in that individuals are granted access to only the tools they need. All transactions have associated audit files and mechanisms to report modifications. Figure 5.9 illustrates this process. Access to information is gained by using a program that specializes in access management; this can be either a single program that controls all access or a set of programs that controls access. Many software-management programs work using this method of security.

FIGURE 5.9 The Clark-Wilson model



Let's say you're working on a software product as part of a team. You may need to access certain code to include in your programs. You aren't authorized to modify this code; you're merely authorized to use it. You use a checkout program to get the code from the source library. Any attempt to put modified code back is prevented. The developers of the code in the source library are authorized to make changes. This process ensures that only people authorized to change the code can accomplish the task.

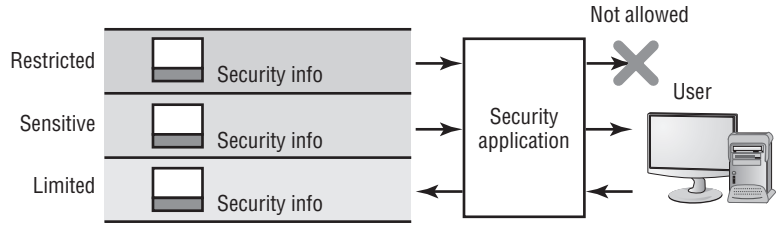
Information Flow Model

The *Information Flow model* is concerned with the properties of information flow, not only the direction of the flow. Both the Bell-La Padula and Biba models are concerned with information flow in predefined manners; they're considered information-flow models. However, this particular Information Flow model is concerned with all information flow, not just up or down. This model requires that each piece of information have unique properties, including operation capabilities. If an attempt is made to write lower-level information to a higher level, the model evaluates the properties of the information and determines whether the operation is legal. If the operation is illegal, the model prevents it from occurring. Figure 5.10 illustrates this concept.

Let's use the previous software project as an example. A developer may be working with a version of the software to improve functionality. When the programmer makes improvements to the code, they want to put that code back into the library. If the attempt to write the code is successful, the code replaces the existing code. If a subsequent bug is

found in the new code, the old code has been changed. The solution is to create a new version of the code that incorporates both the new code and the old code. Each subsequent change to the code requires a new version to be created. This process may consume more disk space, but it prevents things from getting lost, and it provides a mechanism to use or evaluate an older version of the code.

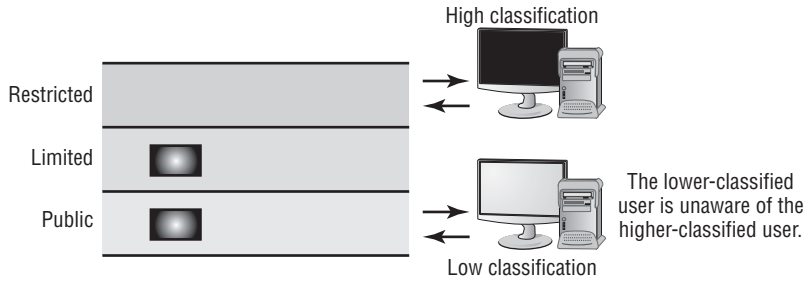
FIGURE 5.10 The Information Flow model



Noninterference Model

The *Noninterference model* is intended to ensure that higher-level security functions don't interfere with lower-level functions. In essence, if a higher-level user changes information, the lower-level user doesn't know about and isn't affected by the changes. This approach prevents the lower-level user from being able to deduce what changes are being made to the system. Figure 5.11 illustrates this concept. Notice that the lower-level user isn't aware that any changes have occurred above them.

FIGURE 5.11 The Noninterference model



Let's take one last look at the software project with which we've been working. If a systems developer is making changes to the library that's being used by a lower-level programmer, changes may be made to the library without the lower-level programmer being aware of them. This lets the higher-level developer work on prototypes without affecting the development effort of the lower-level programmer. When the developer finishes the code, they publish it to lower-level programmers. At this point, all users have access to the changes, and they can use them in their programs.

Incident Reporting

Incident response policies define how an organization will respond to an incident. These policies may involve third parties, and they need to be comprehensive. The term *incident* is somewhat nebulous in scope; for our purposes, an incident is any attempt to violate a security policy, a successful penetration, a compromise of a system, or any unauthorized access to information. This term includes systems failures and disruption of services in the organization.

It's important that an incident response policy establish the following, at minimum:

- Outside agencies that should be contacted or notified in case of an incident
- Resources used to deal with an incident
- Procedures to gather and secure evidence
- List of information that should be collected about the incident
- Outside experts who can be used to address issues if needed
- Policies and guidelines regarding how to handle the incident

According to CERT, a Computer Security Incident Response Team (CSIRT) can be a formalized team, or ad hoc. You can toss a team together to respond to an incident after it arises, but investing time in the development process can make an incident more manageable, because many decisions about dealing with an incident will have been considered earlier. Incidents are high-stress situations; therefore, it's better to simplify the process by considering important aspects in advance. If civil or criminal actions are part of the process, evidence must be gathered and safeguarded properly.

Assume you've discovered a situation where a fraud has been perpetrated internally using a corporate computer. You're part of the investigating team. Your incident response policy lists the specialists you need to contact for an investigation. Ideally, you've already met the investigator or investigating firm, you've developed an understanding of how to protect the scene, and you know how to properly deal with the media (if they become involved).

Social Engineering

Social engineering is a process in which an attacker attempts to acquire information about your network and system by social means, such as talking to people in the organization. A social-engineering attack may occur over the phone, by e-mail, or by a visit. The intent is to acquire access information, such as user IDs and passwords. When the attempt is made through e-mail or instant messaging, this is known as *phishing* and often is made to look as if it is coming from sites where users are likely to have accounts (eBay and PayPal are popular).

These types of attacks are relatively low-tech and are more akin to con jobs. Take the following example. Your help desk gets a call at 4:00 a.m. from someone purporting to be the vice president of your company. She tells the help desk personnel that she is out of town to attend a meeting, her computer just failed, and she is sitting in a Kinko's trying to get a file from her desktop computer back at the office. She can't seem to remember her password and user ID. She tells the help desk representative that she needs access to the information right away or the company could lose millions of dollars. Your help desk rep knows how important this meeting is and gives the vice president her user ID and password over the phone.

Another common approach is initiated by a phone call or e-mail from your software vendor, telling you that they have a critical fix that must be installed on your computer system. If this patch isn't installed right away, your system will crash and you'll lose all your data. For some reason, you've changed your maintenance account password and they can't log on. Your systems operator gives the password to the person. You've been hit again.

Exam Essentials

Know the popular security protocols. Know the difference between SHA, MDA, and Kerberos. Remember that SHA and MDA are popular for hashing, and Kerberos is used for key cryptography.

Know the names, purpose, and characteristics of data and physical security. Know the different types of backups that can be done, as well as the basics of encryption. You should also be aware of social-engineering concerns and the need for a useful incident response policy.

Know the characteristics of security concepts and technologies. Know the basics of encryption. You should also be aware of social-engineering concerns and the need for a useful incident response policy.

Know the roles that exist in data security. In addition to the main three—Owner, Custodian, and User—two more exist: Security Professional and Auditor.

Security Features

There are a number of security "features" that CompTIA expects you to be aware of for this portion of the exam. All constitute some level of protection you can add to make your system more secure. Table 5.1 lists some of the most common problem areas that arise with security.

TABLE 5.1 Identifying Problem Issues

Area	Identifying Symptoms
BIOS	Problems/compromises involving the BIOS typically prevent the system from starting properly. You may be required to enter a password you don't know, or control of the system is never handed to the OS after POST.
Smart cards	Problems with smart cards become apparent when users are unable to access data, or logs show that they accessed data they never truly did.
Biometrics	If there is a problem with biometrics, the user is unable to authenticate and unable to access resources.

TABLE 5.1 Identifying Problem Issues *(continued)*

Area	Identifying Symptoms
Malicious software	Malicious software should be first detected by an antivirus program or other routine operation. If not, it will begin to show itself in the actions taking place on the system (deletion of executables, mass mailing, and so on).
File system	File-system problems can fall into the category of users not being able to access data as they need to, or everyone being granted access to data that they should not see.
Data access	Data-access problems, like file-system issues, are usually those where users legitimately needing access to data can't access it, or too much permission is granted to users who don't need such access. Chapter 7 deals with specific OS approaches to data access.

Critical Information

The six topics that are discussed in the sections that follow are wireless encryption, malicious software protection, BIOS security, password management, locking workstation, and biometrics. Some of these topics were also mentioned earlier in this chapter in the discussion on concepts and technologies.

Wireless Security

Wireless systems are those that don't use wires to send information, but rather transmit data through the air. The growth of wireless systems creates several opportunities for attackers. These systems are relatively new, they use well-established communications mechanisms, and they're easily intercepted. Wireless controllers use special ID numbers called *service-set identifiers* (SSIDs) that must be configured in the network cards to allow communications. However, using SSID number configurations doesn't necessarily prevent wireless networks from being monitored.

This section discusses the various types of wireless systems that you'll encounter, and it mentions some of the security issues associated with this technology. Specifically, this section deals with Wireless Transport Layer Security (WTLS), the IEEE 802 wireless standards, Wired Equivalent Privacy (WEP)/Wireless Applications Protocol (WAP) applications, and the vulnerabilities that each presents.

Wireless Transport Layer Security

Wireless Transport Layer Security (WTLS) is the security layer of WAP, discussed in the section "WAP/WEP." WTLS provides authentication, encryption, and data integrity for wireless devices. It's designed to utilize the relatively narrow bandwidth of these types of

devices, and it's moderately secure. WTLS provides reasonable security for mobile devices, and it's being widely implemented.

WTLS is part of the WAP environment: WAP provides the functional equivalent of TCP/IP for wireless devices. Many devices, including newer cell phones and PDAs, include support for WTLS as part of their networking protocol capabilities.

IEEE 802.11*x* Wireless Protocols

The IEEE 802.11*x* family of protocols provides for wireless communications using radio frequency transmissions. The frequencies in use for 802.11 standards are the 2.4GHz and the 5GHz frequency spectrums. Several standards and bandwidths have been defined for use in wireless environments, and they aren't extremely compatible with each other:

802.11 The *802.11* standard defines wireless LANs transmitting at 1Mbps or 2Mbps bandwidths using the 2.4GHz frequency spectrum and using either frequency-hopping spread spectrum (FHSS) or direct-sequence spread spectrum (DSSS) for data encoding.

802.11a The *802.11a* standard provides wireless LAN bandwidth of up to 54Mbps in the 5GHz frequency spectrum. The 802.11a standard also uses orthogonal frequency division multiplexing (OFDM) for encoding rather than FHSS or DSSS.

802.11b The *802.11b* standard provides for bandwidths of up to 11Mbps (with fallback rates of 5.5, 2, and 1Mbps) in the 2.4GHz frequency spectrum. This standard is also called *WiFi* or *802.11 high rate*. The 802.11b standard uses only DSSS for data encoding.

802.11g The *802.11g* standard provides for bandwidths of 20Mbps+ in the 2.4GHz frequency spectrum. This offers a maximum rate of 54Mbps and is backward compatible with 802.11b.

Three technologies are used to communicate in the 802.11 standard:

Direct-Sequence Spread Spectrum (DSSS) DSSS accomplishes communication by adding the data that is to be transmitted to a higher-speed transmission. The higher-speed transmission contains redundant information to ensure data accuracy. Each packet can then be reconstructed in the event of a disruption.

Frequency-Hopping Spread Spectrum (FHSS) FHSS accomplishes communication by hopping the transmission over a range of predefined frequencies. The changing or hopping is synchronized between both ends and appears to be a single transmission channel to both ends.

Orthogonal Frequency Division Multiplexing (OFDM) OFDM accomplishes communication by breaking the data into subsignals and transmitting them simultaneously. These transmissions occur on different frequencies or subbands.

The mathematics and theories of these transmission technologies are beyond the scope of this book and far beyond the scope of this exam.

WAP/WEP

Wireless systems frequently use WAP for network communications. WEP is intended to provide the equivalent security of a wired network protocol. This section briefly discusses these two terms and provides you with an understanding of their relative capabilities.

WAP The *Wireless Application Protocol (WAP)* is the technology designed for use with mobile devices such as PDAs and cell phones. WAP has become a standard adopted by many manufacturers, including Motorola, Nokia, and others. WAP functions are equivalent to TCP/IP functions in that they're trying to serve the same purpose for wireless devices. WAP uses a smaller version of HTML called *Wireless Markup Language (WML)*, which is used for Internet displays. WAP-enabled devices can also respond to scripts using an environment called *WMLScript*. This scripting language is similar to Java, which is a programming language.

The ability to accept web pages and scripts produces the opportunity for malicious code and viruses to be transported to WAP-enabled devices. No doubt this will create a new set of problems, and antivirus software will be needed to deal with them.

WAP systems communicate using a WAP gateway system. The gateway converts information back and forth between HTTP and WAP, and it also encodes and decodes the security protocols. This structure provides a reasonable assurance that WAP-enabled devices can be secured. If the interconnection between the WAP server and the Internet isn't encrypted, packets between the devices may be intercepted, creating a potential vulnerability. This vulnerability is called a *gap in the WAP*.

WEP *Wired Equivalent Privacy (WEP)* is a relatively new security standard for wireless devices. WEP encrypts data to provide data security. The protocol has always been under scrutiny for not being as secure as initially intended.

WEP is vulnerable due to weaknesses in the encryption algorithms. These weaknesses allow the algorithm to potentially be cracked in less than five hours using available PC software. This makes WEP one of the more vulnerable protocols available for security. WEP is a relatively new technology and will no doubt improve as it moves into the mainstream.

MAC filtering can be used on a wireless network to prevent certain clients from accessing the Internet. You can choose to deny service to a set list of MAC addresses (and allow all others) or only allow service to a set list of MAC addresses (and deny all others).

Wireless Vulnerabilities to Know

Wireless systems are vulnerable to all the different attacks that wired networks are vulnerable to. However, because these protocols use radio frequency signals, they have an additional weakness: all radio frequency signals can be easily intercepted. To intercept 802.11*x* traffic, all you need is a PC with an appropriate 802.11*x* card installed. Simple software on the PC can capture the link traffic in the WAP and then process this data in order to decrypt account and password information.

An additional aspect of wireless systems is the *site survey*. Site surveys involve listening in on an existing wireless network using commercially available technologies. Doing so allows intelligence, and possibly data capture, to be performed on systems in your wireless network.

The term *site survey* initially meant determining whether a proposed location was free from interference. When used by an attacker, a site survey can determine what types of

systems are in use, the protocols used, and other critical information about your network. It's the primary method used to gather data about wireless networks. Virtually all wireless networks are vulnerable to site surveys.

Malicious Software Protection

Computer *viruses*—applications that carry out malicious actions—are one of the most annoying trends happening today. It seems that almost every day, someone invents a new virus. Some of these viruses do nothing more than give you a big "gotcha;" others destroy systems, contaminate networks, and wreak havoc on computer systems. A virus may act on your data or your operating system, but it's intent on doing harm, and doing so without your knowledge. Viruses often include replication as a primary objective and try to infect as many machines as they can, as quickly as possible.

The business of providing software to computer users to protect them from viruses has become a huge industry. Several very good and well-established suppliers of antivirus software exist, and new virus-protection methods come on the scene almost as fast as new viruses. Antivirus software scans the computer's memory, disk files, and incoming and outgoing e-mail. The software typically uses a virus-definition file that is updated regularly by the manufacturer. If these files are kept up-to-date, the computer system will be relatively secure. Unfortunately, most people don't keep their virus definitions up-to-date. Users will exclaim that a new virus has come out, because they just got it. Upon examination, you'll often discover that their virus-definition file is months out-of-date. As you can see, the software part of the system will break down if the definition files aren't updated on a regular basis.

The term *software exploitation* refers to attacks launched against applications and higher-level services. They include gaining access to data using weaknesses in the data-access objects of a database or a flaw in a service. This section briefly outlines some common exploitations that have been successful in the past. The following exploitations can be introduced using viruses, as in the case of the Klez32 virus, or by using access attacks described later in this chapter:

Database Exploitation Many database products allow sophisticated access queries to be made in the client/server environment. If a client session can be hijacked or spoofed, the attacker can formulate queries against the database that disclose unauthorized information. For this attack to be successful, the attacker must first gain access to the environment through one of the attacks outlined later.

Application Exploitation The macro virus is another example of software exploitation. A macro virus is a set of programming instructions in a language such as VBScript that commands an application to perform illicit instructions. Users want more powerful tools, and manufacturers want to sell users what they want. The macro virus takes advantage of the power offered by word processors, spreadsheets, or other applications. This exploitation is inherent in the product, and all users are susceptible to it unless they disable all macros.

E-mail Exploitation Hardly a day goes by without another e-mail virus being reported. This is a result of a weakness in many common e-mail clients. Modern e-mail clients offer many shortcuts, lists, and other capabilities to meet user demands. A popular exploitation

of e-mail clients involves accessing the client address book and propagating viruses. There is virtually nothing a client user can do about these exploitations, although antivirus software that integrates with your e-mail client does offer some protection. To be truly successful, the software manufacturer must fix the weaknesses—an example is Microsoft Outlook's option to protect against access to the address book. This type of weakness isn't a bug, in many cases, but a feature that users wanted.

One of the most important measures you can take to proactively combat software attacks is to know common file extensions and the applications they're associated with. For example, `.scr` files are screensavers, and viruses are often distributed through the use of these files. No legitimate user should be sending screensavers via e-mail to your users, and all `.scr` attachments should be banned from entering the network.

Table 5.2, although not comprehensive, contains the most common file extensions that should or should not, as a general rule, be allowed into the network as e-mail attachments.

TABLE 5.2 Common File Extensions for E-mail Attachments

Should Be Allowed	Should *Not* Be Allowed
`.doc/.docx`	`.bat`
`.pdf`	`.com`
`.txt`	`.exe`
`.xls/.xlsx`	`.hlp`
`.zip`	`.pif`
	`.scr`

Spyware *Spyware* differs from other malware in that it works—often actively—on behalf of a third party. Rather than self-replicating, like viruses and worms, spyware is spread to machines by users who inadvertently ask for it. The users often don't know they have asked for it, but have done so by downloading other programs, visiting infected sites, and so on.

The spyware program monitors the user's activity and responds by offering unsolicited pop-up advertisements (sometimes known as *adware*), gathers information about the user to pass on to marketers, or intercepts personal data such as credit card numbers. One thing separating spyware from most other malware is that it almost always exists to provide commercial gain. The operating systems from Microsoft are the ones most affected by spyware, and Microsoft has released Microsoft AntiSpyware to combat the problem.

Rootkits *Rootkits* have become the software exploitation program du jour. Rootkits are software programs that have the ability to hide certain things from the operating system.

With a rootkit, there may be a number of processes running on a system that don't show up in Task Manager, or connections may be established/available that don't appear in a Netstat display—the rootkit masks the presence of these items. The rootkit does this by manipulating function calls to the operating system and filtering out information that would normally appear.

Unfortunately, many rootkits are written to get around antivirus and antispyware programs that aren't kept up-to-date. The best defense you have is to monitor what your system is doing and catch the rootkit in the process of installation.

Viruses A *virus* is a piece of software designed to infect a computer system. The virus may do nothing more than reside on the computer. A virus may also damage the data on your hard disk, destroy your operating system, and possibly spread to other systems. Viruses get into your computer in one of three ways: on a contaminated floppy or CD, through e-mail, or as part of another program.

Viruses can be classified as several types: polymorphic, stealth, retroviruses, multipartite, armored, companion, phage, and macro viruses. Each type of virus has a different attack strategy and different consequences.

Trojan Horses *Trojan horses* are programs that enter a system or network under the guise of another program. A Trojan horse may be included as an attachment or as part of an installation program. The Trojan horse can create a back door or replace a valid program during installation. It then accomplishes its mission under the guise of another program. Trojan horses can be used to compromise the security of your system, and they can exist on a system for years before they're detected.

The best preventive measure for Trojan horses is to not allow them entry into your system. Immediately before and after you install a new software program or operating system, back it up! If you suspect a Trojan horse, you can reinstall the original programs, which should delete the Trojan horse. A port scan may also reveal a Trojan horse on your system. If an application opens a TCP or IP port that isn't supported in your network, you can track it down and determine which port is being used.

Worms A *worm* is different from a virus in that it can reproduce itself, it's self-contained, and it doesn't need a host application to be transported. Many of the so-called viruses that have made the papers and media were actually worms. However, it's possible for a worm to contain or deliver a virus to a target system.

By their nature and origin, worms are supposed to propagate, and they use whatever services they're capable of to do that. Early worms filled up memory and bred inside the RAM of the target computer. Worms can use TCP/IP, e-mail, Internet services, or any number of possibilities to reach their target.

Spam *Spam* is defined as any unwanted, unsolicited e-mail. Not only can the sheer volume of it be irritating, but it can often open the door to larger problems. Some of the sites advertised in spam may be infected with viruses, worms, and other unwanted programs. If users begin to respond to spam by visiting those sites, then your problems will only multiply.

Just as you can, and must, install good antivirus software programs, you should also consider similar measures for spam. Filtering messages and preventing them from ever entering the network is the most effective method of dealing with the problem.

Adware *Adware* is a term used to describe any application that displays, downloads, or plays an advertisement after it is downloaded or accessed from the web.

Grayware *Grayware* is a term used to describe any application that is annoying or is negatively affecting the performance of your computer. If an application doesn't fall into the virus or Trojan category, it can get lumped under grayware. Spyware and adware are often considered types of grayware, as are programs that log user keystrokes, and certain hacking programs.

BIOS Security

The Basic Input/Output System (BIOS) is used to power up the system and can also allow you to assign a password. Once enabled/activated, that password is stored in CMOS and must be given before the system will fully boot. Most BIOS implementations allow for two different passwords — one for the user and one for the supervisor, the difference between the two being whether or not the ability to access the BIOS setup program is granted.

This provides a simple security solution for a workstation/laptop as the user must give the user password (sometimes also called the system password) in order to be able to access the system; if they cannot give the correct value, the drives are essentially locked. The supervisor password (sometimes also called the setup password) is needed only when the user attempts to access the setup program.

Passwords used for BIOS-level security should follow the same rules as passwords for any account. One other feature to be aware of in the BIOS setup from most vendors is the ability to toggle chassis intrusion detection. If enabled, this will notify you (via a pop-up) if someone has opened the case.

The casual hacker's most common way of working around the password requirement is to remove the battery (thus erasing the CMOS). You should be aware, however, that many BIOS manufacturers include a backdoor password that can be given to bypass the one set by the user. Many of these values can be found on the Internet and are known by more professional hackers.

Another method for getting around the password is to reset CMOS settings to their defaults.

Within the advanced configuration settings on some BIOS configuration menus, you can choose to enable or disable TPM. *Trusted Platform Module (TPM)* can be used to assist with hash key generation. TPM is the name assigned to a chip that can store cryptographic keys, passwords, or certificates. TPM can be used to generate values used with whole disk encryption such as Windows Vista's BitLocker. TPM chip may be installed on the motherboard; when it is, in many cases it is set to off in the BIOS by default.

BitLocker can be used with or without TPM. It is much more secure when coupled with TPM (and is preferable), but does not require it.

TPM can be used to protect cell phones and devices other than PCs as well.

More information on TPM can be found at the Trusted Computing Group's website: `www.trustedcomputinggroup.org/home`.

Password Management

One of the strongest ways to keep a system safe is to employ strong passwords and educate your users. To be strong, passwords should include upper- and lowercase letters, numbers, and other characters as allowed (which characters are allowed may differ based on the operating system).

Users should be educated to understand how valuable data is and why it is important to keep their password strong, secret, and regularly changed.

Locking Workstations

Just as you would not park your car in a public garage and leave its doors wide open with the key in the ignition, you should educate users to not leave a workstation that they are logged in to when they attend meetings, go to lunch, and so forth. They should log out of the workstation or lock it: "Lock when you leave" should be a mantra they become familiar with. Locking the workstation should require a password (usually the same as their user password) in order to resume working at the workstation.

You can also lock a workstation by using an operating system that provides filesystem security. Microsoft's earliest file system was referred to as File Allocation Table (FAT). FAT was designed for relatively small disk drives. It was upgraded first to FAT-16 and finally to FAT-32. FAT-32 (also written as FAT32) allows large disk systems to be used on Windows systems.

FAT allows only two types of protection: share-level and user-level access privileges. If a user has write or change access to a drive or directory, they have access to any file in that directory. This is very unsecure in an Internet environment.

The New Technology File System (NTFS) was introduced with Windows NT to address security problems. Before Windows NT was released, it had become apparent to Microsoft that a new file system was needed to handle growing disk sizes, security concerns, and the need for more stability. NTFS was created to address those issues.

With NTFS, files, directories, and volumes can each have their own security. NTFS's security is flexible and built in. Not only does NTFS track security in access control lists (ACLs), which can hold permissions for local users and groups, but each entry in the ACL can also specify what type of access is given—such as Read-Only, Change, or Full Control. This allows a great deal of flexibility in setting up a network. In addition, special file-encryption programs can be used to encrypt data while it is stored on the hard disk.

Microsoft strongly recommends that all network shares be established using NTFS. While NTFS security is important, though, it doesn't matter at all what file system you are using if you leave your workstation logged in and leave, allowing anyone to sit down at your desk and hack away.

Lastly, don't overlook the obvious need for physical security. Adding a cable to lock a laptop to a desk prevents someone from picking it up and walking away with a copy of your customer database. Every laptop case I am aware of includes a built-in security slot in which a cable lock can be added to prevent it from leaving the premises easily, like the one shown in Figure 5.12.

FIGURE 5.12 A cable in the security slot keeps the laptop from leaving easily.

When it comes to desktop models, adding a lock to the back cover can prevent an intruder with physical access from grabbing the hard drive or damaging the internal components.

Biometrics

With the passing of time, the definition of *biometric* is expanding from simply identifying physical attributes about a person to being able to describe patterns in their behavior. Recent advances have been made in the ability to authenticate someone based on the key pattern they use when entering their password (how long they pause between each key, the amount of time each key is held down, and so forth).

For this objective, however, CompTIA focuses on fingerprint scanners. These simple devices can be built into laptops, connected as external devices (building it into the mouse is common), or be used for authentication at stand-alone stations (Disney will use them to verify the person using a ticket today is the same as the person who used it yesterday). In all cases, a scanner makes a digital image of a person's fingerprint pattern and then compares that each time authentication is needed.

Exam Essentials

Know the names, purpose, and characteristics of wireless security. Wireless networks can be encrypted through WEP and WAP technologies. Wireless controllers use special ID numbers (SSIDs) and must be configured in the network cards to allow communications. However, using ID number configurations doesn't necessarily prevent wireless networks from being monitored, and there are vulnerabilities specific to wireless devices.

Install, configure, upgrade, and optimize hardware, software, and data security. For this objective, you're expected to know the basics of the following items: BIOS security, malicious software protection, password management, and the importance of locking workstations.

Review Questions

1. What is physical security?
2. What does Kerberos use to authenticate a principal?
3. Which authentication method sends a challenge to the client that is encrypted and then sent back to the server?
4. Which type of authentication method uses more than one authentication process for a logon?
5. What type of technology relies on a physical characteristic of the user to verify identity?
6. In which type of attack does someone try to con your organization into revealing account and password information?
7. What type of malicious code attempts to replicate using whatever means are available?
8. Which type of malware enters the system disguised as a legitimate program?
9. What could be one cause of unusual activity on the system disk when no user is accessing the system?
10. What do packet filters prevent?

Answers to Review Questions

1. Physical security is primarily concerned with the loss or theft of physical assets. This would include theft, fire, and other acts that physically deny a service or information to the organization.
2. Kerberos uses a key distribution center (KDC) to authenticate a principal. The KDC provides a credential that can be used by all Kerberos-enabled servers and applications.
3. Challenge Handshake Authentication Protocol (CHAP) sends a challenge to the originating client. This challenge is sent back to the server, and the encryption results are compared. If the challenge is successful, the client is logged on.
4. A multifactor authentication process uses two or more processes for logon. A two-factor method might use smart cards and biometrics for logon.
5. Biometric technologies rely on a physical characteristic of the user to verify identity. Biometric devices typically use either a hand pattern or a retinal scan to accomplish this.
6. Someone trying to con your organization into revealing account and password information is launching a social-engineering attack.
7. A worm is a type of malicious code that attempts to replicate using whatever means are available.
8. A Trojan horse enters with a legitimate program to accomplish its evil deeds.
9. A symptom of many viruses is unusual activity on the system disk. This is caused by the virus spreading to other files on your system.
10. Packet filters prevent unauthorized packets from entering or leaving a network. Packet filters are a type of firewall that block specified port traffic.

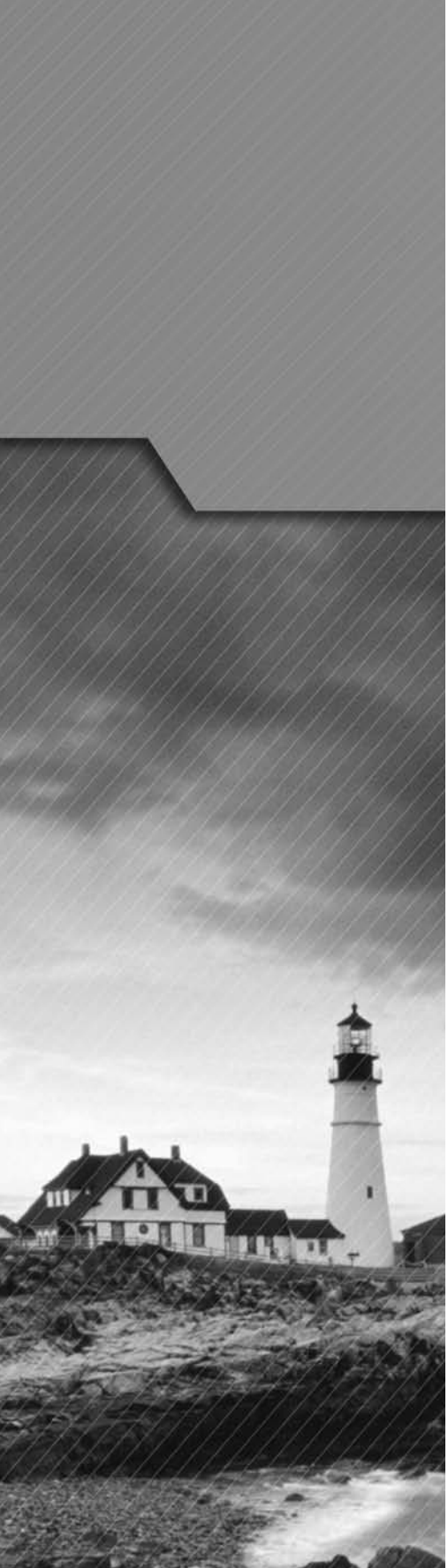
Chapter

6

Operational Procedure

COMPTIA A+ ESSENTIALS EXAM OBJECTIVES COVERED IN THIS CHAPTER:

- ✓ **6.1 Outline the purpose of appropriate safety and environmental procedures and given a scenario apply them**
  - ESD
  - EMI
    - Network interference
    - Magnets
  - RFI
    - Cordless phone interference
    - Microwaves
  - Electrical safety
    - CRT
    - Power supply
    - Inverter
    - Laser printers
    - Matching power requirements of equipment with power distribution and UPSs
  - Material Safety Data Sheets (MSDS)
  - Cable management
    - Avoiding trip hazards
  - Physical safety
    - Heavy devices
    - Hot components
  - Environmental – consider proper disposal procedures



- ✓ **6.2 Given a scenario, demonstrate the appropriate use of communication skills and professionalism in the workplace**
  - Use proper language – avoid jargon, acronyms, slang
  - Maintain a positive attitude
  - Listen and do not interrupt a customer
  - Be culturally sensitive
  - Be on time
    - If late contact the customer
  - Avoid distractions
    - Personal calls
    - Talking to co-workers while interacting with customers
    - Personal interruptions
  - Dealing with a difficult customer or situation
    - Avoid arguing with customers and/or being defensive
    - Do not minimize customers' problems
    - Avoid being judgmental
    - Clarify customer statements
      - Ask open-ended questions to narrow the scope of the problem
      - Restate the issue or question to verify understanding
  - Set and meet expectations / timeline and communicate status with the customer
    - Offer different repair / replacement options if applicable
    - Provide proper documentation on the services provided
    - Follow up with customer / user at a later date to verify satisfaction
  - Deal appropriately with customers confidential materials
    - Located on computer, desktop, printer, etc.

If you looked back over the history of the A+ certification, you would be hard-pressed to find any domain or topics that have changed as much as this one. Much of what is here is common sense, but don't dismiss the chapter based on that. With the topics worth 10 percent of the weighting, doing well on this portion of the exam can increase your chances of acing the Essentials exam.

Safety First

This objective deals with potential hazards, both to you and to the computer system. It focuses on protecting humans from harm due to electricity, heat, and other hazards, and on protecting computer components from harm due to electrostatic discharge (ESD).

Critical Information

ESD is one of the most dangerous risks associated with working with computers. Not only does ESD have the potential to damage components of the computer, but it can also injure you. Not understanding the proper way to avoid it could cause you great harm.

The ESD that we are speaking about here does not have the capability to kill you since it doesn't have the amperage. What does represent a threat, though, is using a wrist strap of your own design that does not have the resistor protection built into it and then accidentally touching something with high voltage while wearing the wrist strap. Without the resistor in place, the high voltage would be grounded through you!

Minimizing Electrostatic Discharge (ESD)

Electrostatic discharge (ESD) is the technical term for what happens whenever two objects of dissimilar charge come in contact—think of rubbing your feet on a carpet and then touching a light switch. The two objects exchange electrons in order to standardize the electrostatic charge between them, with the object of higher charge passing voltage to the object of lower charge. If it happens to be an electronic component that receives the charge, there is a good chance it can be damaged.

The likelihood that a component will be damaged increases with the growing use of complementary metallic oxide semiconductor (CMOS) chips, because these chips contain a thin metal oxide layer that is hypersensitive to ESD. The previous generation's transistor-transistor logic (TTL) chips are more robust than the newer CMOS chips because they don't contain this metal oxide layer. Most of today's integrated circuits (ICs) are CMOS chips, so ESD is more of a concern lately.

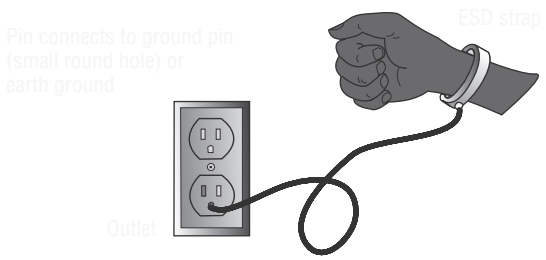
The lowest-static voltage transfer that you can feel is around 3,000 volts (it doesn't electrocute you because there is extremely little current). A static transfer that you can *see* is at least 10,000 volts! Just by sitting in a chair, you can generate around 100 volts of static electricity. Walking around wearing synthetic materials can generate around 1,000 volts. You can easily generate around 20,000 volts simply by dragging your smooth-soled shoes across a carpet in the winter. (Actually, it doesn't have to be winter to run this danger; it can occur in any room with very low humidity. It's just that heated rooms in wintertime generally have very low humidity.)

It would make sense that these thousands of volts would damage computer components. However, a component can be damaged with as little as 80 volts. That means if your body has a small charge built up in it, you could damage a component without even realizing it.

Antistatic Wrist Strap

There are measures you can implement to help contain the effects of ESD. The easiest one to implement is the *antistatic wrist strap*, also referred to as an *ESD strap*. You attach one end of the ESD strap to an earth ground (typically the ground pin on an extension cord) and wrap the other end around your wrist. This strap grounds your body and keeps it at a zero charge. Figure 6.1 shows the proper way to attach an antistatic strap.

FIGURE 6.1 Proper ESD strap connection



If you do not have a grounded outlet available, you can achieve partial benefit simply by attaching the strap to the metal frame of the PC case. Doing so keeps the charge equalized between your body and the case, so that there is no electrostatic discharge when you touch components inside the case.

An ESD strap is a specially designed device to bleed electrical charges away *safely*. It uses a 1 megaohm resistor to bleed the charge away slowly. A simple wire wrapped around your wrist will not work correctly and could electrocute you!

Do not wear the antistatic wrist strap when there is the potential to encounter a high-voltage capacitor, such as when working on the inside of a monitor or power supply. The strap could channel that voltage through your body.

Working with High Voltage

Two computer devices have the potential to carry high voltages: the monitor and the power supply. The power supply converts AC current into DC current, and the capacitor associated with it holds 120 volts for quite a while.

The monitor uses a lot of power as it directs electrons on the screen via a strong magnet. The electrons and magnet require a considerable amount of voltage in order to be able to do their task. Like power supplies, monitors have the ability to hold their charge a long time after the power has been disconnected.

You should never open a power supply or a monitor for the reasons discussed here. The risk of electrocution with these two devices is significant.

If you question the presence of electricity, or the voltage of it, use a voltmeter. Figure 6.2 shows a simple voltmeter capable of working with both AC and DC currents.

FIGURE 6.2 A simple voltmeter

Moving Equipment

When my first child was born, I left the hospital with her strapped securely in the child seat, surrounded by pillows and grandparents, with no possibility of moving an inch. I drove home—all 20 miles—at a speed that never exceeded 30 miles per hour. If she so much as yawned, I immediately looked to see what was going on and whether I needed to stop the car and make some adjustments.

Less than a year after the ride home, I was helping relocate a call center from one part of a busy city to another. Another technician and I were overseeing the work, and the company brought in inmates from a prison to help with heavy lifting. Needless to say, most of them didn't have a great deal of incentive to make sure the equipment was treated well. My partner slapped a mini-tower on a cart and went racing through the parking lot as if he were in a campus bed race. Once he reached the moving truck, he grabbed the tower in a bear hug and tossed it in, but not far enough back—its weight caused it to tip off the ledge and break into little pieces all over the parking lot. That is the way to lose a customer as well as data and any profit that could have been made on the project.

The first example is the one to follow when moving computer equipment—treat every piece you move as if it's your first child. One of the easiest ways to damage equipment is to move it with abandon. Take care to disconnect all cables and move the equipment in such a way as to do no harm.

Every cable should be carefully labeled and each component carefully stowed in a container that will protect it during the move. The move may take longer than you would like, but this approach can save you significant time and expense over having to re-create a system—even one as small as a user's workstation—from scratch.

Antistatic Bags for Parts

Antistatic bags protect sensitive electronic devices from stray static charges. The bags are designed so that static charges collect on the outside of the bags rather than on the electronic components. You can obtain these bags from several sources. The most direct way to acquire antistatic bags is to go to an electronics supply store and purchase them in bulk. Most supply stores have several sizes available. Perhaps the easiest way to obtain them, however, is to hold onto the ones that come your way. That is, when you purchase any new component, it usually comes in an antistatic bag. Once you have installed the component, keep the bag. It may take you a while to gather a sizable collection of bags if you take this approach, but eventually you will have a fairly large assortment.

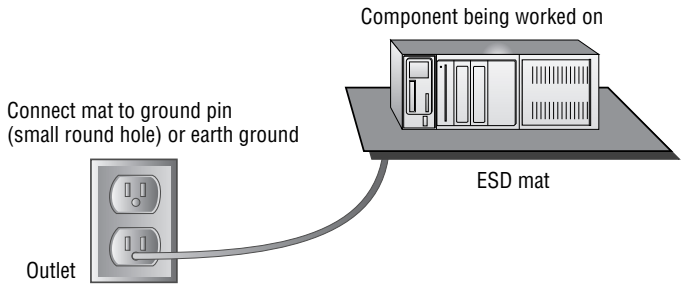
ESD Static Mats

It is possible to damage a device simply by laying it on a bench top. For this reason, you should have an ESD mat (also known as an antistatic mat) in addition to an ESD strap. This mat drains excess charge away from any item coming in contact with it (see Figure 6.3). ESD mats are also sold as mouse/keyboard pads to prevent ESD charges from interfering with the operation of the computer.

Vendors have methods of protecting components in transit from manufacture to installation. They press the pins of ICs into antistatic foam to keep all the pins at the same potential, and circuit boards are shipped in antistatic bags, discussed earlier. However, keep in

mind that unlike antistatic mats, antistatic bags do not drain the charges away—they should never be used in place of antistatic mats.

FIGURE 6.3 Proper use of an ESD mat



Modifying the Relative Humidity

Another preventive measure you can take is to maintain the relative humidity at around 50 percent. Be careful not to increase the humidity too far—to the point where moisture starts to condense on the equipment! Also, use antistatic spray, which is available commercially, to reduce static buildup on clothing and carpets. In a pinch, a solution of diluted fabric softener sprayed on these items will do the same thing.

At the very least, you can be mindful of the dangers of ESD and take steps to reduce its effects. Beyond that, you should educate yourself about those effects so you know when ESD is becoming a major problem.

Electrical Tripping

Tripping occurs when the breaker on a device such as a power supply, surge protector, or *uninterruptible power supply (UPS)* turns off the device because it received a spike. If the device is a UPS, when the tripping happens, the components plugged in to the UPS should go to battery instead of pulling power through the line. Under most circumstances, the breaker is reset and operations continue as normal. Figure 6.4 shows a surge-protector power strip, with the trip button to reset at the top.

Nuisance tripping is the phrase used if tripping occurs often and isn't a result of a serious condition. If this continues, you should isolate the cause and correct it, even if it means replacing the device that continues to trip.

Surge protectors, either stand-alone or built into the UPS, can help reduce the number of nuisance trips. If your UPS doesn't have a surge protector, you should add one to the outlet before the UPS in order to keep the UPS from being damaged if it receives a strong surge. Figure 6.5 shows an example of a simple surge protector for a home computer.

All units are rated by Underwriters Laboratories (UL) for performance. One thing you should never do is plug a UPS or computer equipment into a ground fault circuit interrupter (GFCI) receptacle. These receptacles are intended for use in wet areas, and they trip very easily.

FIGURE 6.4 The reset button on the top of a surge-protector power strip

FIGURE 6.5 A simple surge protector

Don't confuse a GFCI receptacle with an isolated ground receptacle. Isolated ground receptacles are identifiable by orange outlets and should be used for computer equipment to avoid their picking up a surge passed to the ground by any other device.

Electromagnetic Interference (EMI) and Radio Frequency Interference (RFI)

Electromagnetic interference (EMI) and *radio frequency interference (RFI)* are terms that are often used interchangeably. They describe unwanted disturbances that affect your computers or network. The disturbance is a form of electrical radiation, and can emanate from sources such as electrical circuits, wireless devices such as Bluetooth, magnets, cordless phones, or microwave ovens.

Environmental Issues

It is important that you know the potential safety hazards that exist when working with computer elements, and how to address them. It is imperative that you understand such issues as *material safety data sheets* (*MSDSs*) and know how to reference them when needed.

Any type of chemical, equipment, or supply that has the potential to harm the environment or people has to have an MSDS associated with it. These are traditionally created by the manufacturer and you can obtain them from the manufacturer, or from the Environmental Protection Agency at `www.epa.gov`.

Preventing Harm to Humans

Computers, display monitors, and printers can be dangerous if not handled properly. Computers not only use electricity, but they store electrical charge after they're turned off in components called *capacitors*. The monitor and the power supply have large capacitors capable of delivering significant shock, so they should not be disassembled except by a trained electrical repairperson.

In addition, various parts of the printer run at extremely high temperatures, and you can get burned if you try to handle them immediately after they've been in operation. Two examples are the CPU chip and the fusing unit inside a laser printer.

Extinguishing Electrical Fires

Repairing a computer is not often the cause of an electrical fire. However, you should know how to extinguish such a fire properly. Three major classes of fire extinguishers are available, one for each type of flammable substance: A for wood and paper fires, B for flammable liquids, and C for electrical fires. The most popular type of fire extinguisher today is the multipurpose, or ABC-rated, extinguisher. It contains a dry chemical powder that smothers the fire and cools it at the same time. For electrical fires (which may be related to a shorted-out wire in a power supply), make sure the fire extinguisher will work for class-C fires. If you don't have an extinguisher that is specifically rated for electrical fires (type C), you can use an ABC-rated extinguisher.

Power Supply Safety

Although it is possible to work on a power supply, doing so is *not* recommended. Power supplies contain several capacitors that can hold *lethal* charges *long after they have been unplugged*! It is extremely dangerous to open the case of a power supply. Besides, power supplies are inexpensive, so it would probably cost less to replace one than to try to fix it, and it would be much safer.

The number of volts in a power source represents its potential to do work, but volts don't do anything by themselves. Current (amperage, or amps) is the actual force behind the work being done by electricity. Here's an analogy to help explain this concept. Say you have two boulders; one weighs 10 pounds, the other 100 pounds, and each is 100 feet off the ground. If you drop them, which one will do more work? The obvious answer is the 100-pound boulder. They both have the same potential to do work (100 feet of travel), but the 100-pound boulder has more mass, and thus more force. Voltage is analogous to the distance the boulder is from the ground, and amperage is analogous to the mass of the boulder.

This is why we can produce static electricity on the order of 50,000 volts and not electrocute ourselves. Even though this electricity has a great *potential* for work, it does very little work because the amperage is so low. This also explains why we can weld metal with only 110 volts. Welders use only 110 (sometimes 220) volts, but they also use anywhere from 50 to 200 amps!

Printer Safety

Printer repair has hazards and pitfalls. Some of them are discussed here:

- When handling a toner cartridge from a laser printer or page printer, do not vigorously shake the cartridge or turn it upside down. You will find yourself spending more time cleaning the printer and the surrounding area than you would have spent to fix the printer.
- Do not put any objects into the feeding system (in an attempt to clear the path) while the printer is running.
- Laser printers generate a laser that is hazardous to your eyes. Do not look directly into the source of the laser.
- If it's an ink-jet printer, do not try to blow into the ink cartridge to clear a clogged opening—that is, unless you like the taste of ink. Most printers come with software that provides a cleaning method for the cartridge.
- Some parts of a laser printer (such as the EP cartridge) will be damaged if touched. Your skin produces oils and has a small surface layer of dead skin cells. These substances can collect on the delicate surface of the EP cartridge and cause malfunctions. Bottom line: keep your fingers out of where they don't belong!

One of the best tools you have when working with printers is common sense. You will find that this will serve you well when trying to tackle a problem with a printer, as well as when trying to answer an odd question on the topic during the A+ exam.

Monitor Safety

Other than the power supply, one of the most dangerous components to try to repair is the monitor, particularly if it is a cathode ray tube (CRT). We recommend that you *not* try to repair monitors. To avoid the extremely hazardous environment contained inside the monitor—it can retain a high-voltage charge for hours after it's been turned off—take it to a certified monitor technician or television-repair shop. The repair shop or certified technician will know and understand the proper procedures to discharge the monitor, which involves attaching a resistor to the flyback transformer's charging capacitor to release the high-voltage electrical charge that builds up during use. They will also be able to determine whether the monitor can be repaired or needs to be replaced. Remember, the monitor works in its own extremely protective environment (the monitor case) and may not respond well to your desire to try to open it. The CRT is vacuum-sealed. Be extremely careful when handling it—if you break the glass, the CRT will implode, which can send glass in any direction.

Even though I recommend not repairing monitors, the A+ exam does test your knowledge of the safety practices to use when you need to do so. If you have to open a monitor, you must first discharge the high-voltage charge on it using a high-voltage probe. This probe has a very large needle, a gauge that indicates volts, and a wire with an alligator clip. Attach the alligator clip to a ground (usually the round pin on the power cord). Slip the probe needle under the high-voltage cup on the monitor. You will see the gauge spike to around 15,000 volts and slowly reduce to zero. When it reaches zero, you may remove the high-voltage probe and service the high-voltage components of the monitor.

Working with Liquids

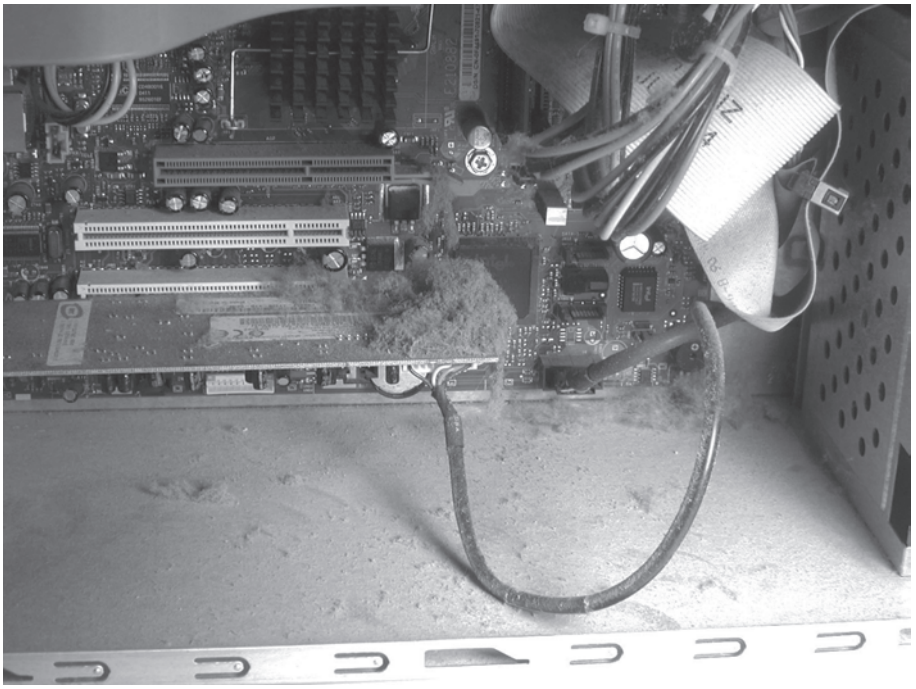
As a rule of thumb, liquids and computers don't mix and should be kept as far apart from each other as two male Siamese fighting fish. Liquid provides a great conductor between electrical components if spilled and can quickly fry a system. This refers not only to the soda an office worker carries in a cup to their cubicle, but also to the venting of the air-conditioning unit in the server room. If it's improperly draining or plumbed, it could cause serious damage to the equipment in its vicinity.

The exception to the liquid rule is cleaning alcohol. Isopropyl alcohol is commonly used for cleaning some components. You can find special-purpose cleaners in computer stores for cleaning specific items; if you use one, consult a material safety data sheet (MSDS) for the product or consult the manufacturer to find out whether any special handling and disposal is required.

Atmospheric Hazards

One of the most harmful atmospheric hazards to a computer is dust. Dust, dirt, hair, and other airborne contaminants can get pulled into computers and build up inside. Because computer fans work by pulling air through the computer (usually sucking it in through the case and then pushing it out the power supply), it's easy for these items to enter and then become stuck. Every item in the computer builds up heat, and these particles are no exception. As they build up, they hinder the fan's ability to perform its function, and the components get hotter than they would otherwise. Figure 6.6 shows the inside of a system in use for only six months in an area with carpeting and other dusty surroundings.

FIGURE 6.6 Dust builds up inside the system.



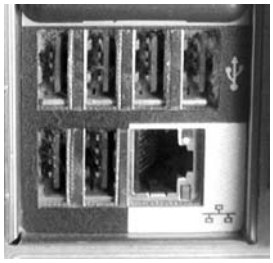
The heat that builds up can lead to *chip creep* and other conditions. Heating the pins too much causes expansion and keeps them seated tighter, but heating them too far and then cooling them repeatedly (at shutdown) causes the chips to gradually "creep" out of the sockets.

You can remove dust and debris from inside computers with compressed air blown in short bursts. The short bursts are useful in preventing the dust from flying too far out and entering another machine, as well as in preventing the can from releasing the air in liquid form. Compressed air cans should be held 2–3 inches from the system and always used upright so the content is released as a gas. If the can becomes cold to the touch, discontinue using it until it heats back to room temperature.

It's possible to use an air compressor instead of compressed-air cans when you need a lot of air. If you take this approach, make sure you keep the pounds per square inch (PSI) at or below 40, and include measures on the air compressor to remove moisture.

Dust can build up not just within the computer but also in crevices on the outside. Figure 6.7 shows USB ports on the back of a system that have become a haven for small dust particles. These ports need to be blown out with compressed air, or cleaned with an electronic vacuum, before being used, or else degradation with the device connected to them could occur.

FIGURE 6.7 Dust collects in unused ports as well.



Relative humidity should be maintained at around 50 percent for optimal operations. Be careful not to increase the humidity too far, to the point where moisture starts to condense on the equipment! Also use antistatic spray, which is available commercially, to reduce static buildup on clothing and carpets. In a pinch, a solution of diluted fabric softener sprayed on these items will do the same thing.

At the very least, be mindful of the dangers of electrostatic discharge (ESD) and take steps to reduce its effects. Beyond that, you should educate yourself about those effects so you know when ESD is becoming a major problem.

Reporting Incidents

As careful as you try to be, there is always the possibility for accidents to occur. Accidents can be environment-related (for example, a flash flood no one could predict suddenly overtakes the server room and shorts out the wiring), or caused by humans (someone mixes the wrong cleaning chemicals together to try and make their own concoction). Regardless of the cause or circumstances, one thing is written in stone: you must fully and truthfully document the problem.

While that documentation must be seen by internal parties (managers, human resources, etc.), it may also need to be seen by external parties. The latter depends on the type of industry that you are in and the type of incident that occurred. For example, if a large amount of battery acid is spilled in the ground, you should contact the Environmental Protection Agency (see reporting procedures at `www.epa.gov`). If employees are injured, you may need to be contact the Occupational Safety and Health Administration (OSHA). On their website (`www.osha.gov`), you can find links to information on issues of compliance, laws and regulation, and enforcement.

It is your responsibility, as an administrator and a professional, to know—or learn—the reporting procedures for incidents that you are faced with and to act accordingly.

Proper Disposal Procedures

It is estimated that more than 25 percent of all the lead in landfills today comes from consumer electronics components. Because consumer electronics contain hazardous substances, many states require that they be disposed of as hazardous waste. Computers are

no exception. Monitors contain several carcinogens and phosphors, as well as mercury and lead. The computer itself may contain several lubricants and chemicals as well as lead. Printers contain plastics and chemicals such as toners and inks that are also hazardous. All of these items should be disposed of properly.

Recycling Computers

We recycle cans, plastic, and newspaper, so why not recycle computer equipment? The problem is that most computers contain small amounts of hazardous substances. Some countries are exploring the option of recycling electrical machines, but most have not enacted appropriate measures to enforce their proper disposal. However, we can do a few things as consumers and environmentalists to promote the proper disposal of computer equipment:

- Check with the manufacturer. Some manufacturers will take back outdated equipment for parts.
- Disassemble the machine and reuse the parts that are good.
- Check out businesses that can melt down the components for the lead or gold plating.
- Contact the Environmental Protection Agency (EPA) for a list of local or regional waste-disposal sites that will accept used computer equipment.
- Check with local nonprofit or education organizations interested in using the equipment.
- Check out the Internet for possible waste-disposal sites. Table 6.1 lists a few websites that deal with disposal of used computer equipment.

TABLE 6.1 Computer Recycling Websites

Site Name	Web Address
Computer Recycle Center	`www.recycles.com/`
PC Disposal	`www.pcdisposal.com`
Re-PC	`www.repc.com/`

The computer itself is not, as a stand-alone entity, the only thing that may need to be disposed of. Sometimes, you will have individual components that have been removed from a computer or peripherals that need to be tossed. The following looks at some of the most common of these elements:

Disposing of Batteries In particular, you should make a special effort to recycle batteries. Batteries contain several chemicals that are harmful to our environment, such as nickel and lead, and won't degrade safely. Batteries should not be thrown away; they should be recycled according to your local laws. Check with your local authorities to find out how batteries should be recycled.

Disposing of CRTs A CRT contains phosphors on the inside of the screen that can harm the environment if placed in a landfill. The large boxy shell of the CRT also takes up a lot of space in a landfill. Dispose of a monitor at your local hazardous-waste recycling center.

Disposing of Circuit Boards Circuit boards contain lead in their soldering, so they should not be put in the regular trash. Take them to the local hazardous-waste disposal site, or contract with a company that handles them.

Disposing of Ink and Toner Cartridges Ink and toner cartridges should be taken to recycling centers for proper disposal. It may also be possible to sell them to companies that refill and reuse them, but some people feel that this is not a good idea. Those remanufactured cartridges sometimes do not work very well, and can damage the printers they are installed in, and by selling such companies your "empties" you are encouraging that industry.

Disposing of Cleaning Chemicals The most common cleaning chemicals used for computers are alcohol and water, neither of which is particularly hazardous to the environment. However, if you use other chemical products, consult an MSDS for the product or consult the manufacturer to find out whether any special disposal is required.

Exam Essentials

Understand ESD. Electrostatic discharge occurs when two objects of unequal electrical potential meet. The object of higher potential transfers some charge to the other one, just as water flows into an area that has a lower water level.

Understand the antistatic wrist strap. The antistatic wrist strap is also referred to as an ESD strap. To use the ESD strap, you attach one end to an earth ground (typically the ground pin on an extension cord) and wrap the other end around your wrist. This strap grounds your body and keeps it at a zero charge, preventing discharges from damaging the components of a PC.

Know what an MSDS is. An MSDS is a material safety data sheet containing instructions for handling an item. It can be acquired from the manufacturer or from the EPA.

Know the fire extinguisher types. Class C is the type of fire extinguisher needed for electrical fires.

Know that a monitor stores high voltage. Monitors and power supplies carry the greatest potential for human harm. This is due to their capacitors, which store high-voltage electrical charges. A monitor in particular can store thousands of volts of charge for weeks after it has been unplugged.

Know that you may need to report incidents. When incidents happen, you must always document them and every attempt should be made to do so both fully and truthfully. Depending upon the type of incident, you may also need to report it to other authorities, such as the EPA or OSHA.

Know what components are not suitable for a landfill. Batteries, CRTs, and circuit boards are all examples of items that should not be thrown away normally because of the elements used in them. Batteries contain metals such as lead and nickel, circuit boards contain lead solder, and CRTs contain phosphors.

Know the safety procedures to follow when working with computers. Be careful when moving computers or working around any electrical components. Know that liquids and computers don't mix, and keep the systems as clean and dust-free as possible to ensure optimal operation.

Good Communication Skills

It's possible that you chose computers as your vocation instead of public speaking because you want to interact with people on a one-to-one basis. As unlikely as that possibility may be, it still exists.

Whether or not you enjoy one-to-one communication, you should know the basics. Fortunately, the multiple-choice questions you'll be asked require more common sense than anything else, and you shouldn't find this domain to be a stumbling block. If the following discussion seems like second nature, you should feel confident that this objective won't be one with which you'll have trouble.

Critical Information

Good communication includes listening to what the user/manager/developer is telling you and making certain that you understand completely what they are trying to say. Just because a user or customer doesn't understand the terminology/syntax/concepts that you do doesn't mean they don't have a real problem that needs addressing. You must, therefore, be skilled not only at listening, but also at translating. Professional conduct encompasses politeness, guidance, punctuality, and accountability. Always treat the customer with the same respect and empathy you would expect if the situation were reversed. Likewise, guide the customer through the problem and the explanation. Tell them what has caused the problem they're currently experiencing and offer the best solution to prevent it from reoccurring.

Customer satisfaction goes a long way toward generating repeat business. If you can *meet* the customer's expectations, you'll almost assuredly hear from them again when another problem arises. If you can *exceed* the customer's expectations, you can almost guarantee that they will call you the next time a problem arises.

Customer satisfaction is important in all communication media—whether you're on-site, providing phone support, or communicating through e-mail or other correspondence. If you're on-site, act in accordance with the following points:

- When you arrive, immediately look for the person (user, manager, administrator, and so on) who is affected by the problem. Announce that you're there, and assure them that you'll do all you can to remedy the problem.

- Listen intently to what your customer is saying. Make it obvious to them that you're listening and respecting what they're telling you. If you have a problem understanding them, go to whatever lengths you need to in order to remedy the situation. Look for verbal and nonverbal cues that can help you isolate the problem.
- Share the customer's sense of urgency. What may seem like a small problem to you can appear to the customer as if the whole world is collapsing around them.
- Be honest and fair with the customer, and try to establish a personal rapport. Tell them what the problem is, what you believe is the cause, and what can be done in the future to prevent it from reoccurring.
- Handle complaints as professionally as possible. Accept responsibility for errors that may have occurred on your part, and never try to pass the blame. Avoid arguing with a customer, because doing so serves no purpose; resolve their anger with as little conflict as possible. Remember, the goal is to keep them as a customer, not to win an argument.
- When you finish a job, notify the user that you're done. Make every attempt to find the user and inform them of the resolution. If it's difficult to find them, leave a note for them to find when they return, explaining the resolution. You should also leave a means by which they can contact you, should they have a question about the resolution or a related problem. In most cases, the number you leave should be that of your business during working hours and your pager, where applicable, after hours.

If you're providing phone support, do the following:

- Always answer the telephone in a professional manner, announcing the name of the company and yourself.
- Make a concentrated effort to ascertain the customer's technical level, and communicate at that level, not above or below it.
- The most important skill you can have is the ability to listen. You have to rely on the customer to tell you the problem and describe it accurately. They can't do that if you're second-guessing them or jumping to conclusions before the whole story is told. Ask questions that are broad at first and then narrow down to help isolate the problem. It's your job to help guide the user's description of the problem. Here are some examples:
  - Is the printer plugged in?
  - Is it online?
  - Are any lights flashing on it?
- Complaints should be handled in the same manner as if you were on-site. Make your best effort to resolve the problem and not argue its points. Again, you want to keep the customer more than you want to accomplish any other goal.
- Close the incident only when the customer is satisfied that the solution you have given them is the correct one and the problem has gone away.
- End the telephone call in a courteous manner. Thanking the customer for the opportunity to serve them is often the best way.

Talking to the user is an important first step in the troubleshooting process. Your first contact with a computer that has a problem is usually through the customer, either directly or by way of a work order that contains the user's complaint. Often, the complaint is something straightforward, such as "There's a disc stuck in the CD drive." At other times, the problem is complex and the customer doesn't mention everything that has been going wrong.

Eliciting Problem Symptoms from Customers

The act of diagnosis starts with the art of customer relations. Go to the customer with an attitude of trust: believe what the customer is saying. At the same time, go to the customer with an attitude of hidden skepticism, meaning *don't* believe that the customer has told you everything. This attitude of hidden skepticism isn't the same as distrust; just remember that what you hear isn't always the whole story, and customers may inadvertently forget to give a crucial detail.

For example, a customer may complain that their CD-ROM drive doesn't work. What they fail to mention is that it has never worked and that they installed it. When you examine the machine, you realize that the customer mounted the drive with screws that are too long and that prevent the tray from ejecting properly.

Having Customers Reproduce Errors as Part of the Diagnostic Process

The most important part of this step is to have the customer show you what the problem is. An excellent method is to say, "Show me what 'not working' looks like." That way, you see the conditions and methods under which the problem occurs. The problem may be a simple matter of an improper method. The user may be doing an operation incorrectly or doing the process in the wrong order. During this step, you have the opportunity to observe how the problem occurs, so pay attention.

Identifying Recent Changes to the Computer Environment

The user can give you vital information. The most important question is, "What changed?" Problems don't usually come out of nowhere. Was a new piece of hardware or software added? Did the user drop some equipment? Was there a power outage or a storm? These are the types of questions you can ask a user in trying to find out what is different.

If nothing changed, at least outwardly, then what was going on at the time of failure? Can the problem be reproduced? Can the problem be worked around? The point here is to ask as many questions as you need to in order to pinpoint the trouble.

Using the Information

Once the problem or problems have been clearly identified, your next step is to isolate possible causes. If the problem can't be clearly identified, then further tests are necessary. A common technique for hardware and software problems alike is to strip the system down to bare-bones basics. In a hardware situation, this may mean removing all interface cards except those absolutely required for the system to operate. In a software situation, this may mean disabling elements within the Device Manager.

Then, you can gradually rebuild the system toward the point where the trouble started. When you reintroduce a component and the problem reappears, you know that component is the one causing the problem.

Putting It in Perspective

Whether you're dealing with customers in person or on the phone, CompTIA expects you to adhere to the rules of common courtesy. These were implied in the discussion previously, but you must understand them and hold fast to their precepts for the exam:

- Use clear, concise, and direct statements—customers want to know what is going on. They want to know that you understand the problem and can deal with it. Being honest and direct is almost always appreciated. While dealing with them, give them your full attention and avoid distractions such as personal calls and other interruptions.
- Allow the customer to complete statements, and avoid interrupting them or arguing with them. Everyone has been in a situation where they haven't been able to fully tell what they wanted to without being interrupted or ignored. It isn't enjoyable in a social setting, and it's intolerable in a business setting. This can lead to frustration and customers feeling as if they need to become defensive.
- Clarify customer statements, and ask pertinent questions. Open-ended questions are helpful at narrowing the scope of the problem, and then you can restate their answers to verify you are understanding what they are saying. The questions you ask should help guide you toward isolating the problem and identifying possible solutions. It is important to not minimize their problem or appear as if you are being judgmental.
- Avoid using jargon, abbreviations, slang, and acronyms. Every field has its own language that can make those from outside the field feel lost. Put yourself in the position of someone not in the field, and explain what is going on using words they can relate to.
- Listen to customers. This is the most important rule of all—people like to feel they're being listened to. As simple an act as it is, it can make all the difference in making customers at ease with your work.
- Maintain a positive attitude. Your approach to the problem, and the customer, can be mirrored back. It is important as well to be culturally sensitive—not everyone enjoys the same humor.
- Treat the customer with respect. Respect not only their equipment, but also their time (if you are going to be late, call ahead), their confidential information (avoid it), and their patronage (document what you have done and follow up with them later to make sure they are satisfied).

Some have marveled at the fact that CompTIA includes questions about customer service on the A+ exam. A better wonder, however, is that there are those in the business who need to know these items and don't. Possessing a great deal of technology skill does not immediately endow one with great people skills. A bit more on appropriate behavior as it relates to the IT field follows.

Appropriate Job-Related Behavior

Critical to appropriate behavior is treating the customer, or user, the way you want to be treated. Much has been made of the Golden Rule—treating others the way you would have them treat you. Six key elements, from a business perspective, are punctuality, accountability, flexibility, confidentiality, respect, and privacy. The following sections discuss each of these.

Punctuality

Punctuality is important and should be a part of your planning process before you ever arrive at the site: If you tell the customer you'll be there at 10:30, you need to make every attempt to be there at that time. If you arrive late, you have given them false hope that the problem would be solved by a set time. That false hope can lead to anger when you arrive late and appear to not be taking their problem as seriously as they are. Punctuality continues to be important throughout the service call and doesn't end with your arrival. If you need to leave to get parts, tell the customer when you'll be back, and then be there at that time. If for some reason you can't return at the expected time, alert the customer and inform them of your new return time.

In conjunction with time and punctuality, if a user asks how much longer the server will be down, and you respond that it will up in five minutes, only to have it remain down for five more hours, you're creating resentment and possibly anger. When estimating down-time, always allow for more time than you think you'll need, just in case other problems occur. If you greatly underestimate the time, always inform the affected parties and give them a new time estimate. Here's an analogy that will put it in perspective: if you take your car to get the oil changed, and the counter clerk tells you it will be "about 15 minutes," the last thing you want is to be sitting there four hours later.

Accountability

Accountability is a trait that's well respected in every technician. When problems occur, you need to be accountable for them and not attempt to pass the buck. You can no doubt think of people who have a sense of accountability, and you can also think of some who don't. It's equally easy for a customer to identify this trait in a technician. For example, suppose you're called to a site to put a larger hard drive into a server. While performing this operation, you inadvertently scrape your feet across the carpeted floor, build up energy, and zap the memory in the server. Some technicians would pretend the electrostatic discharge (ESD) never happened, put in the new hard drive, and then act baffled by the fact that problems unrelated to the hard drive are occurring. An accountable technician will explain exactly what happened to the customer and suggest ways of proceeding from that point—addressing and solving the problem as quickly and efficiently as possible.

Flexibility

Flexibility is another important trait for a service technician. Although it's important that you respond to service calls promptly and close them (solve them) as quickly as you can, you must also be flexible. If a customer can't have you on-site until the afternoon, make

your best attempt to work them into your schedule around the time most convenient for them. Likewise, if you're called to a site to solve a problem, and they're having another problem that they bring to your attention while you're there, make every attempt to address that problem as well. Under no circumstances should you ever give a customer the cold shoulder or not respond to their problems because they weren't on an initial incident report.

You should take all this advice in the context of general information and follow the express guidelines of the company you work for.

Confidentiality

The goal of *confidentiality* is to prevent or minimize unauthorized access to files and folders and disclosure of data and information. In many instances, laws and regulations require specific information confidentiality. For example, Social Security records, payroll and employee records, medical records, and corporate information are high-value assets. This information could create liability issues or embarrassment if it fell into the wrong hands. Over the last few years, there have been several cases in which bank account and credit card numbers were published on the Internet. The costs of these types of breaches of confidentiality far exceed the actual losses from the misuse of this information.

Confidentiality entails ensuring that data expected to remain private is seen only by those who should see it. Confidentiality is implemented through authentication and access controls.

Just as confidentiality issues are addressed early in the design phase of a project, you—as a computer professional—are expected to uphold a high level of confidentiality. Should a user approach you with a sensitive issue—telling you their password, asking for assistance obtaining access to medical forms, and so on—it's your obligation as a part of your job to make certain that information passes no further.

Respect

Much of the discussion in this chapter is focused on respecting the customer as an individual. In addition to respecting them as a person, you must also respect the tangibles that are important to them. Although you may look at a monitor they're using and recognize it as an outdated piece of equipment that should be scrapped, the customer may see it as a gift from their children when they first started their business.

Treat the customer's property as if it has value, and you'll win their respect. Their property includes the system you're working on (laptop/desktop computer, monitor, peripherals, and so on) as well as other items associated with their business. Don't use their telephone to make personal calls or unnecessarily call other customers while you're at this site. Don't use their printers or other equipment unless it's in a role associated with the problem you've been summoned to fix.

Privacy

Although there is some overlap between confidentiality and privacy, *privacy* is an area of computing that is becoming considerably more regulated. As a computing professional, you must stay current with applicable laws, because you're often one of the primary agents expected to ensure compliance.

In addition to the federal laws, most states have laws on computer crime as well. Check `http://nsi.org/Library/Compsec/computerlaw/statelaws.html` for information on your state.

Computer Fraud and Abuse Act

The Computer Fraud and Abuse Act was introduced into law in 1986. The original law was passed to address issues of fraud and abuse that weren't well covered under existing statutes. The law was updated in 1994, in 1996, and again in 2001.

This act gives federal authorities, primarily the FBI, the ability to prosecute hackers, spammers, and others as terrorists. The law is primarily intended to protect government and financial computer systems from intrusion. Technically, if a governmental system, such as an Internet server, were used in the commission of the crime, virtually any computer user of that system could be prosecuted.

The law is comprehensive and allows for stiff penalties, fines, and imprisonment of up to 10 years for convictions under this statute.

For more information on this act, visit `http://cio.energy.gov/ComputerFraud-AbuseAct.pdf`.

Computer Security Act of 1987

The Computer Security Act requires federal agencies to identify and protect computer systems that contain sensitive information. This law requires agencies that keep sensitive information to conduct regular training and audits and to implement procedures to protect privacy. All federal agencies must comply with this act.

For more information on this act, visit `www.epic.org/crypto/csa/`.

Cyberspace Electronic Security Act

The Cyberspace Electronic Security Act (CESA) gives law enforcement the right to gain access to encryption keys and cryptography methods. The initial version of this act allowed federal law enforcement agencies to secretly use monitoring, electronic capturing equipment, and other technologies to access and obtain information. These provisions were later stricken from the act, although federal law-enforcement agencies were given a large amount of latitude to conduct investigations relating to electronic information. This act is generating a lot of discussion about what capabilities should be given to law enforcement in the detection of criminal activity.

For more information on this act, visit `www.cdt.org/crypto/CESA/`.

Cyber Security Enhancement Act of 2002

The Cyber Security Enhancement Act allows federal agencies relatively easy access to ISPs and other data-transmission facilities to monitor communications of individuals suspected of committing computer crimes using the Internet. The act is also known as Section 225 of the Homeland Security Act of 2002.

For more information on this act, visit `www.usdoj.gov/criminal/cybercrime/homeland_CSEA.htm`.

USA PATRIOT Act

The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001 was passed partially because of the World Trade Center attack. This law gives the United States government extreme latitude in pursuing criminals who commit terrorist acts. The definition of a terrorist act is broad.

The law provides for relief to victims of terrorism, as well as the ability to conduct virtually any type of surveillance of a suspected terrorist. This act is currently under revision, and it will probably be expanded.

For more information on this act, visit `www.cbo.gov/showdoc.cfm?index=3180&sequence=0&from=6`.

Exam Essentials

Use good communication skills. Listen to the customer. Let them tell you what they understand the problem to be, and then interpret the problem and see if you can get them to agree to what you're hearing them say. Treat the customer, whether an end user or a colleague, with respect, and take their issues and problems seriously.

Use job-related professional behavior. The Golden Rule should govern your professional behavior. Six key elements to this, from a business perspective, are punctuality, accountability, flexibility, confidentiality, respect, and privacy.

Review Questions

1. From which government agency can you find material safety data sheets?
2. What is the tangible and environmentally unfriendly part of laser printers?
3. True or false: an ESD strap should connect to the ground of an electrical outlet.
4. What is the danger to humans when disassembling and working on a monitor?
5. What type of fire extinguisher is appropriate for electrical fires?
6. While troubleshooting a customer's LAN, you determine the server must be rebooted. This will affect over a dozen current users. What should you do?
7. A customer complains that he cannot print to the workgroup laser printer. What should be the first question you ask?
8. A customer states that they may need to reach you quickly for troubleshooting a mission-critical application, and asks for your cell number. What should you do?
9. Which act gives law enforcement the right to gain access to encryption keys and cryptography methods?
10. Which act gives the U.S. government extreme latitude in pursuing criminals who commit terrorist acts?

Answers to Review Questions

1. The EPA (Environmental Protection Agency) keeps a copy of material safety data sheets.
2. Toner. You must be careful not to spill it and to send used cartridges to recycling centers.
3. True. An ESD strap should connect to the ground of an electrical outlet.
4. A high-voltage capacitor inside the monitor retains a charge even long after the monitor has been unplugged.
5. Class C.
6. A message should be sent to all users notifying them that the system will be going down and giving an estimate of how long the users will be affected. The estimate should include time to address any other issues that you fear may crop up.
7. One of the first questions you should ask the user is if they have ever printed to that printer. This can then be followed up with questions as to how recently they did so and what has changed since then.
8. You should adhere to policies of the company you work for on this matter. Some companies do not mind customers having the cell number for a technician, whereas others want all calls to come to a central location so the calls can be processed more efficiently. Whichever situation applies, you should carefully explain it to your customer and let them know the rules of response time, escalation, and other issues.
9. The Cyberspace Electronic Security Act (CESA) gives law enforcement the right to gain access to encryption keys and cryptography methods.
10. The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001 gives the U.S. government extreme latitude in pursuing criminals who commit terrorist acts. The definition of a terrorist act is broad.

CompTIA A+ Practical Application

PART II

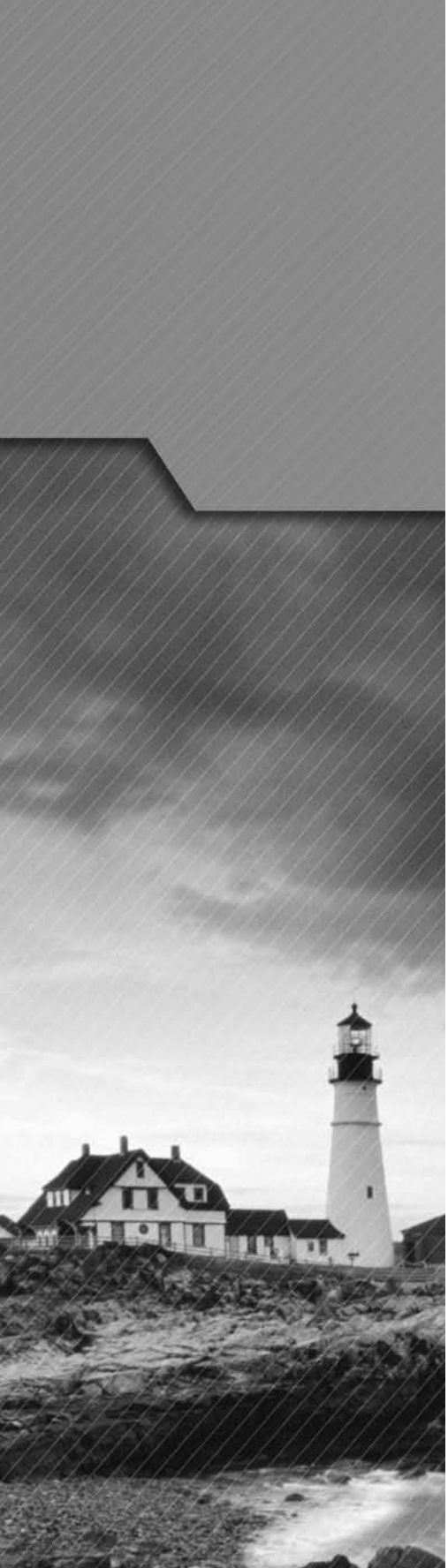
Chapter

7

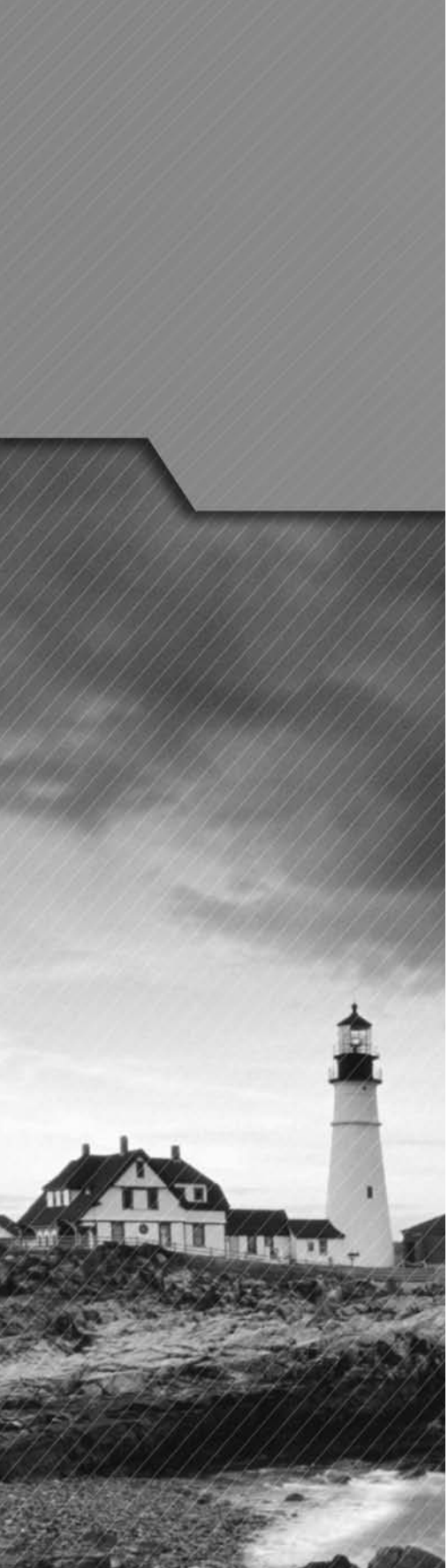
Hardware

COMPTIA A+ PRACTICAL APPLICATION EXAM OBJECTIVES COVERED IN THIS CHAPTER:

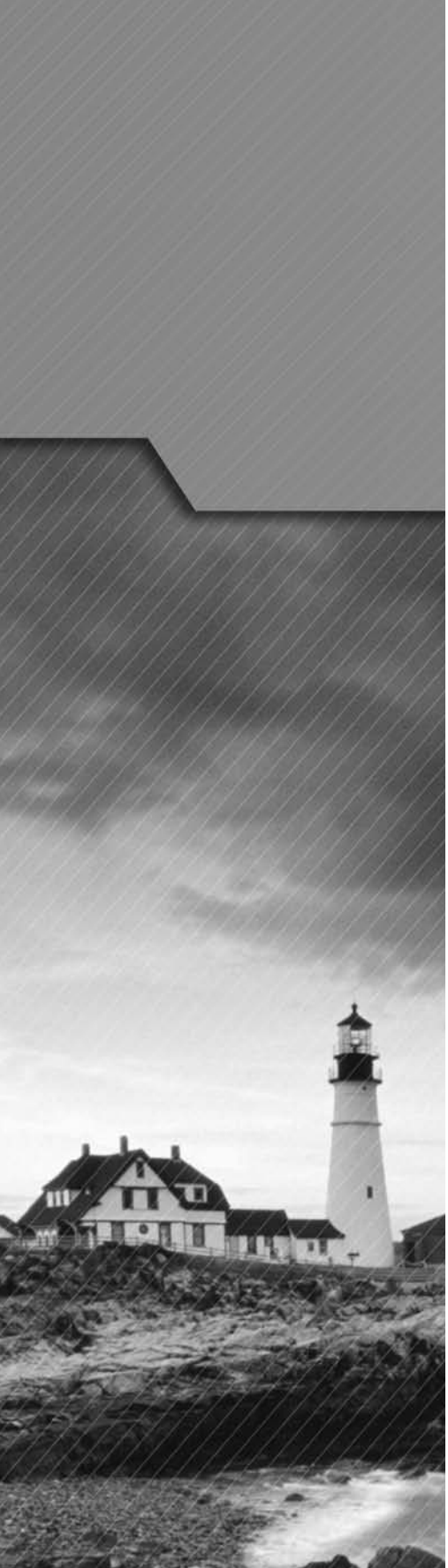
- ✓ **1.1 Given a scenario, install, configure and maintain personal computer components**
  - Storage devices
    - HDD
      - SATA
      - PATA
      - Solid state
    - FDD
    - Optical drives
      - CD / DVD / RW / Blu-Ray
    - Removable
    - External
  - Motherboards
    - Jumper settings
    - CMOS battery
    - Advanced BIOS settings
    - Bus speeds
    - Chipsets
    - Firmware updates
    - Socket types
    - Expansion slots
    - Memory slots
    - Front panel connectors
    - I/O ports
      - Sound, video, USB 1.1, USB 2.0, serial, IEEE 1394 / Firewire, parallel, NIC, modem, PS/2



- Power supplies
  - Wattages and capacity
  - Connector types and quantity
  - Output voltage
- Processors
  - Socket types
  - Speed
  - Number of cores
  - Power consumption
  - Cache
  - Front side bus
  - 32bit vs. 64bit
- Memory
- Adapter cards
  - Graphics cards
  - Sound cards
  - Storage controllers
    - RAID cards (RAID array – levels 0,1,5)
    - eSATA cards
  - I/O cards
    - Firewire
    - USB
    - Parallel
    - Serial
  - Wired and wireless network cards
  - Capture cards (TV, video)
  - Media reader
- Cooling systems
  - Heat sinks
  - Thermal compound
  - CPU fans
  - Case fans



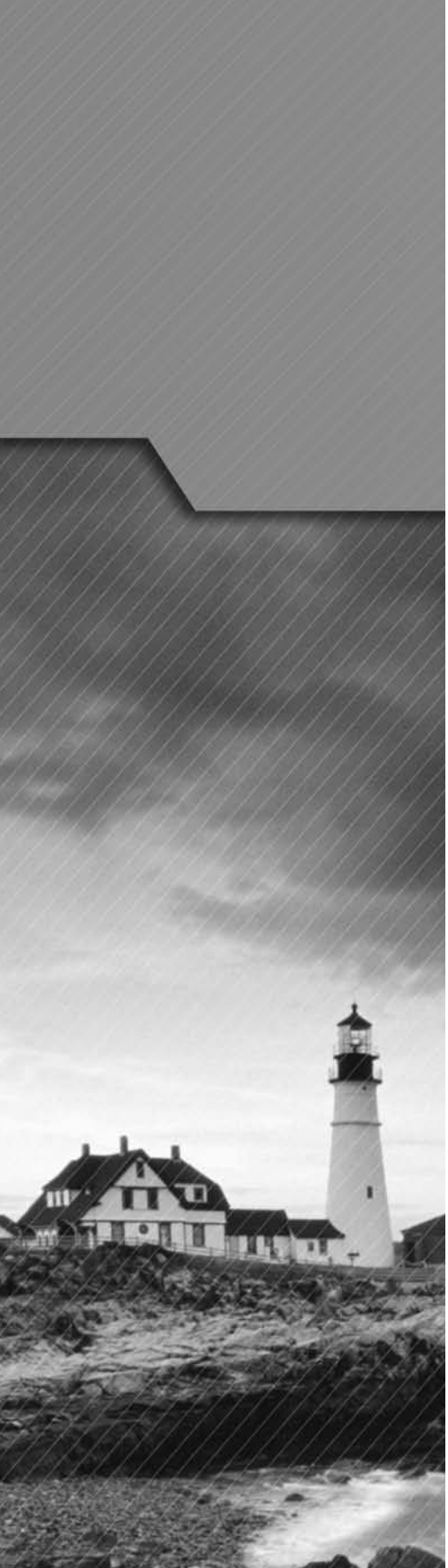
- ✓ **1.2 Given a scenario, detect problems, troubleshoot and repair/replace personal computer components**
  - Storage devices
    - HDD
      - SATA
      - PATA
      - Solid state
    - FDD
    - Optical drives
      - CD / DVD / RW / Blu-Ray
    - Removable
    - External
  - Motherboards
    - Jumper settings
    - CMOS battery
    - Advanced BIOS settings
    - Bus speeds
    - Chipsets
    - Firmware updates
    - Socket types
    - Expansion slots
    - Memory slots
    - Front panel connectors
    - I/O ports
      - Sound, video, USB 1.1, USB 2.0, serial, IEEE 1394 / Firewire, parallel, NIC, modem, PS/2
  - Power supplies
    - Wattages and capacity
    - Connector types and quantity
    - Output voltage



- Processors
  - Socket types
  - Speed
  - Number of cores
  - Power consumption
  - Cache
  - Front side bus
  - 32bit vs. 64bit
- Memory
- Adapter cards
  - Graphics cards
  - Sound cards
  - Storage controllers
    - RAID cards (RAID array – levels 0,1,5)
    - eSATA cards
  - I/O cards
    - Firewire
    - USB
    - Parallel
    - Serial
  - Wired and wireless network cards
  - Capture cards (TV, video)
  - Media reader
- Cooling systems
  - Heat sinks
  - Thermal compound
  - CPU fans
  - Case fans

✓ 1.3 Given a scenario, install, configure, detect problems, troubleshoot and repair/replace laptop components

- Components of the LCD including inverter, screen and video card



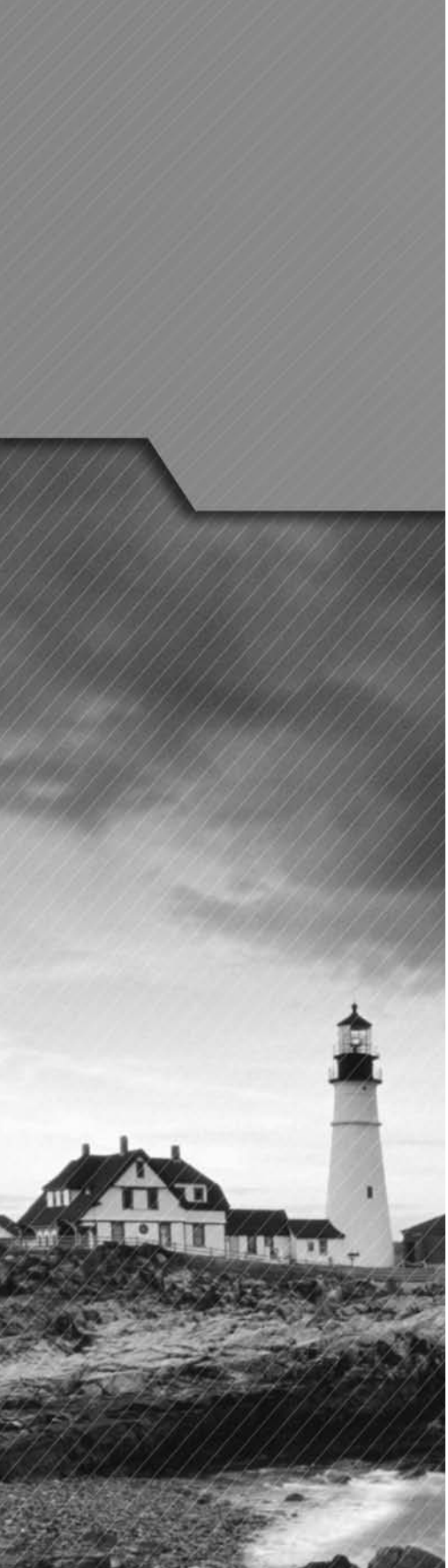
- Hard drive and memory
- Disassemble processes for proper re-assembly
  - Document and label cable and screw locations
  - Organize parts
  - Refer to manufacturer documentation
  - Use appropriate hand tools
- Recognize internal laptop expansion slot types
- Upgrade wireless cards and video card
- Replace keyboard, processor, plastics, pointer devices, heat sinks, fans, system board, CMOS battery, speakers

✓ 1.4 Given a scenario, select and use the following tools

- Multimeter
- Power supply tester
- Specialty hardware / tools
- Cable testers
- Loop back plugs
- Anti-static pad and wrist strap
- Extension magnet

✓ 1.5 Given a scenario, detect and resolve common printer issues

- Symptoms
  - Paper jams
  - Blank paper
  - Error codes
  - Out of memory error
  - Lines and smearing
  - Garbage printout
  - Ghosted image
  - No connectivity



- Issue resolution
  - Replace fuser
  - Replace drum
  - Clear paper jam
  - Power cycle
  - Install maintenance kit (reset page count)
  - Set IP on printer
  - Clean printer

You can't become A+ certified without knowing personal computers inside and out. This domain was heavily weighted on the A+ Essentials exam, and it's heavily weighted on the on the Practical Application exam as well. In fact, in both cases it is the most heavily weighted of any domain.

Installing, Configuring, and Maintaining Personal Computer Components

As you study for this part, you'll want to reread Chapter 1, "Hardware," which you'll need to know for the Essentials exam; make certain you know each component's purpose and some of its basics. For example, understand the difference between memory types and be able to identify a memory card by sight.

Critical Information

This objective demands that you be able to add, remove, and configure a number of different devices. At some point, every computer will need to be upgraded. Upgrading usually means one of two things: replacing old technology with new technology or adding functionality to an existing system. An example of upgrading old technology is replacing a CD-ROM drive with a DVD burner. An example of adding functionality to an existing system is adding more RAM to increase performance. In either case, upgrading usually involves adding a new component. This process consists of several basic steps, each of which must be carefully followed. In this section, we'll cover the following steps:

- Disassembly
- Inspection
- Part replacement and reassembly

As you work inside a PC, be aware of safety hazards both to yourself and to the equipment.

When you choose an area in which to work on a computer, pick a workspace that is sturdy enough to support the weight of a computer and any peripherals you're adding to your system. The area must also be well lit, clean, and large enough to hold all the pieces and necessary tools.

Disassembling the Computer

You don't need to disassemble the computer completely to perform most upgrade and repair jobs; part of being a successful technician is being able to identify what parts must be removed for each job. For example, replacing a motherboard requires almost complete disassembly, but replacing a DVD drive doesn't require any disassembly at all in most cases (except for removing the drive itself).

Preparing Your Work Area

For any work you do on a computer, you must have an adequate workspace. First, the work area must be flat. Second, the area must be sturdy. Make sure the work surface you're using can support the weight of the components. Third, the area must be well lit, clean, and large enough to hold all pieces (assembled and disassembled) and all necessary tools.

Before you begin, make sure all necessary tools are available and in working order. Also make sure the documentation for the system you're working on is available (including owner's manuals, service manuals, and Internet resources).

The final guideline to preparing your work area is to set aside plenty of time to complete the task. Estimate the time required to complete the entire task (disassembly, installation, reassembly, and testing).

Once you've prepared your work area and gathered your tools, you're ready to begin the actual disassembly of the computer. The steps are basically the same for all brands and types of computers.

Disassembly Prerequisites

You need to do several things before you even move the computer to your work area:

1. Shut down any running programs, and turn off the computer.
2. Remove all cables that are attached to the computer.
3. Remove any media, such as CDs, from their drives.
4. Clean around the work surface to make sure you won't be knocking anything into or on the PC as you are working with it.

Disconnect the Display Devices

You should disconnect the monitor and any other display devices (such as a projector) that may be connected to the system. Although some cases can be opened without disconnecting the monitor cable, you run the risk of damaging the display or card if you don't disconnect the cable.

Removing Input Devices

External devices such as the keyboard and mouse should be unplugged before you open the case. Although this step isn't necessary for every upgrade, doing so makes it easier to remove the case cover because the cords and connectors aren't in the way.

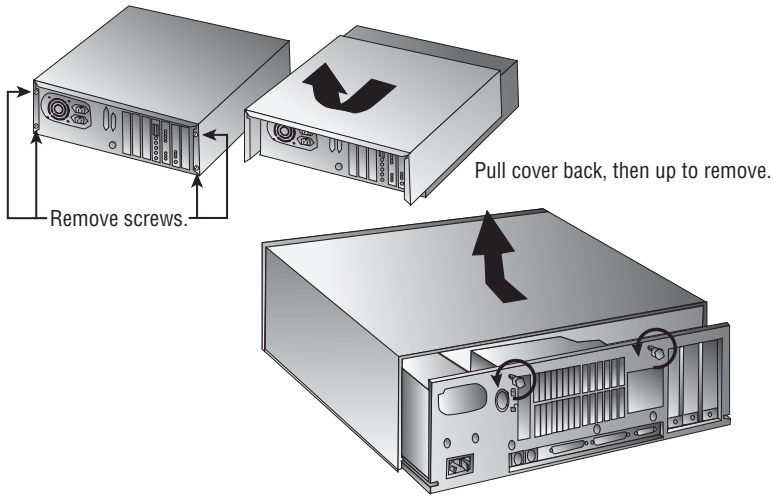
From CompTIA's perspective, input devices can include basic items such as keyboards and mice as well as specialty items such as tablets, joysticks, and microphones. Multimedia devices such as web cameras can fall into this category as well. In all cases, know that you should disconnect them before working on the PC and add them per the vendor's documentation.

Removing the Case Cover

Now you can unfasten the computer's cover by removing any retaining screws at the back of the computer. Some cases don't have screws; instead, they have a sliding bar or latches that release the cover. Many of today's PCs can be completely disassembled without a single tool.

Then, remove the cover by sliding or lifting it. The exact procedure varies greatly depending on the case; Figure 7.1 shows an example for a desktop-style case.

FIGURE 7.1 Removing the case cover on a desktop case



Don't remove all the screws at the back of the computer! Some of these screws hold vital components (such as the power supply) to the case, and removing them will cause those components to drop into the computer.

Removing the Expansion/Adapter Cards

The next step in disassembly is to put on an antistatic wrist strap, plugging one end into the ground plug of an outlet. Then, you can start to remove any expansion cards. There are four major steps in removing the expansion cards, as shown in Figure 7.2:

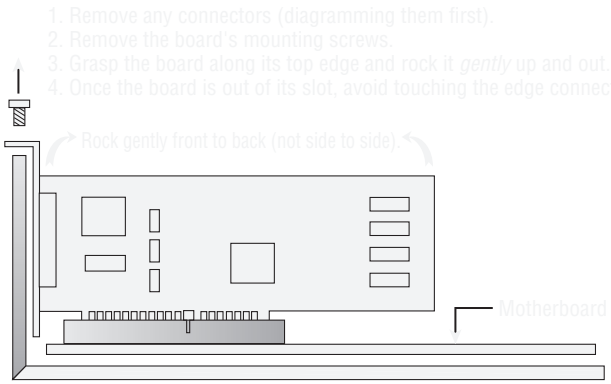
1. Remove any internal or external cables or connectors.
2. Remove any mounting screws that are holding the boards in place, and put the screws somewhere where they won't be lost.

Use an egg carton or something else with compartments to hold and organize screws you're removing so they don't get lost or put back in the wrong spot.

3. Grasp the board by the top edge with both hands and gently rock it front to back (not side to side).
4. Once the board is out, place it in an antistatic bag to help prevent electrostatic discharge (ESD) damage while the board is out of the computer.

Duplicate this procedure for each card.

FIGURE 7.2 Removing an expansion board

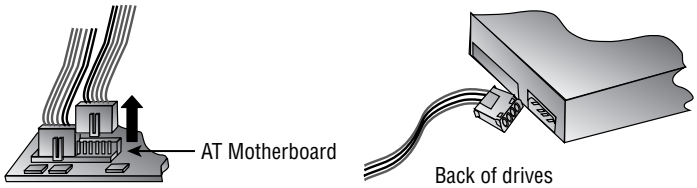


Be sure to note the slot from which you remove each card, because some bus types (including Peripheral Component Interconnect [PCI]) keep track of the slots in which the expansion boards are installed. Reinstalling an expansion card in a different slot later probably won't cause a problem, because the Plug and Play (PnP) BIOS should redetect it— but better safe than sorry.

Removing the Power Supply

Before you remove the power supply from the computer, you must do two things: disconnect the power-supply connectors from the internal devices (as shown in Figure 7.3), and remove the mounting hardware for the power supply. The following steps list the order in which to tackle this:

FIGURE 7.3 Removing power-supply connectors



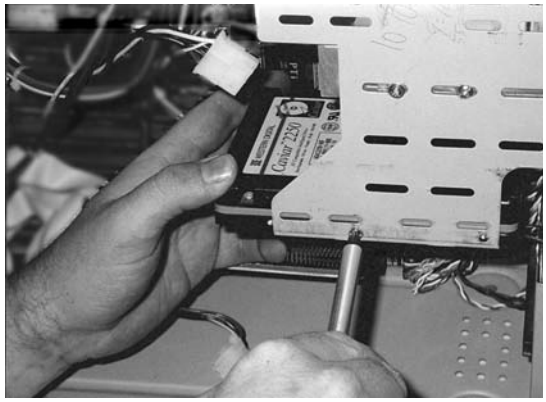
1. Grasp the connector (not the wires), and gently wiggle it out of its receptacle. Then proceed to the next connector. The system board and disk drives both use power connectors. Make sure all of them are removed. AT cases have power leads connected to a switch at the front of the case that also need to be removed.
2. An AT PC power supply (these are getting rarer with each passing day, but you should still know about them for the exam) has two connectors to the motherboard; these plug into receptacles that are side by side. If you get confused about how these connectors attach, the general rule is black-to-black. An ATX power supply has a single 20-wire connector to the motherboard.
3. Once all the power-supply connectors are disconnected from their devices, you can remove the mounting hardware. You can usually detach the power supply from the case by removing four screws. Some power supplies don't need to have screws removed; instead, they're installed on tracks or into slots in the case and need only to be slid out or lifted out.

Removing the Storage Devices

To remove a disk drive, follow these steps:

1. Disconnect it from the power supply (if you haven't done so already).
2. Disconnect the ribbon cable that runs from the drive to the motherboard (or drive controller board).
3. Physically remove the drive from its bay. On some cases, drives are secured in the bays with screws in the sides, as in Figure 7.4; on other cases they slide in and out on rails with clips that release and retain them.

FIGURE 7.4 Removing the hard drive

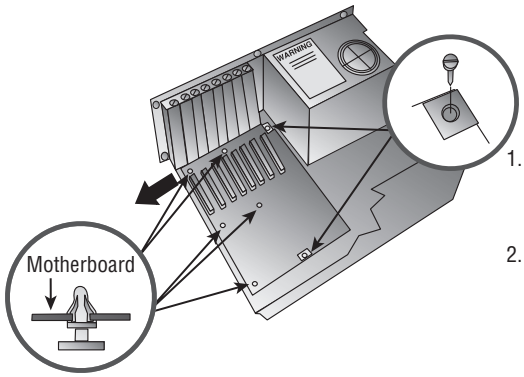


Most servers have hot-pluggable drives, which means they can be added or removed while the computer is running. You remove them by depressing a retaining clip or button. Consult the documentation provided with the machine or drives for the exact details.

Removing the Motherboard

The motherboard is held away from the metal case using brass or plastic spacers called stand-offs and is secured and grounded using mounting screws. To remove the motherboard, you must remove the screws holding the motherboard to the case floor. On an ATX motherboard, you then lift the motherboard out of the case. On an AT motherboard (think legacy), as in Figure 7.5, you must slide the motherboard about 1 inch to one side to release its plastic stand-offs from the mounting holes in the case floor.

FIGURE 7.5 Removing the motherboard



1. Remove the two screws indicated with arrows here.
2. Remove the motherboard by moving it laterally in the direction of the large arrow to disengage the spacers. Do not remove the spacers from the motherboard.

There are five spacers holding the motherboard off the case. A spacer is shown above, viewed from its side.

Removing the Memory

Memory is held in place by retaining clips at both ends of the module. For a single inline memory module (SIMM), the retaining clips are metal. Pull them back, tilt the SIMM back to a 45-degree angle with the motherboard, and then lift it out of the slot. For a dual inline memory module (DIMM), the retaining clips are plastic. Push them down (away from the DIMM), and the DIMM will pop free from its slot automatically; you can just lift it out. Place the removed memory in an antistatic bag to prevent damage.

Inspecting the Computer

Inspecting the computer is an important step in the disassembly and reassembly of the system. You should check the components for any damage and gather any documentation. Damage is sometimes visible on motherboards. Discolored areas on the board are often caused by power surges.

After a component is removed, it's a good idea to create a parts list on a notepad and make sure you have all the supporting documentation and device drivers. If you don't have them, it's good practice to download them from the manufacturer's website or from a multi-vendor information site.

Part Replacement and Reassembly

The reassembly of the machine is almost an exact reversal of its disassembly. Once you have all the necessary documentation and device drivers, the process is simple: you reassemble the computer by replacing the hard-to-reach items first and then attaching the supporting devices.

Installing the System Board

The motherboard attaches to the case by the spacers (stand-offs) that hold it away from the metal case. There are two kinds. Old AT systems use plastic stand-offs that fit into holes in the motherboard and then slide into channels in the case floor. Both AT and ATX systems use brass stand-offs that attach to the floor of the case and have screw holes in their tops for attaching the motherboard screws.

Before you reattach the motherboard, it's best to make sure that the memory and the processor are properly secured and seated in the slots. Doing so will help prevent damage to the chips and protect your hand from cuts, because installing them after the board is secured will leave you with limited space. After you've snapped the board onto its spacers, one or two retaining screws normally need to be attached. When attaching these screws, be sure not to over-tighten them and damage the board.

Installing the Power Supply

The power supply should be installed next. Attach it with the screws you removed during its disassembly. After it's secure, reattach the power leads to their respective connectors on the motherboard. If it's an AT system, make sure the black wires on the motherboard power connectors (usually labeled P8 and P9) are oriented together on the connector.

Installing Drives/Storage Devices

The drives are the next components you attach. First, attach the floppy drive—if you happen to have an old system that still includes one. The ribbon cable and the power connector connect to the back of the drive exactly as they were originally removed.

Next, attach the Integrated Drive Electronics (IDE) drives, such as hard drives and CD drives. They connect to the motherboard's IDE interface via ribbon cable, and they connect to the power supply via a Molex power connector. Be sure to check the ribbon cable's attachment, because it's the most commonly reversed item on the PC. The red stripe on the cable indicates 1, which should be oriented closest to the power connector on the drive.

Installing PCI, ISA, and AGP Devices

After the drives are attached, add any PCI, Industry Standard Architecture (ISA), PCIe, and Accelerated Graphics Port (AGP) devices the system uses, such as a video card, sound card, or modem. If the motherboard has any of these components built in, their ports may be built into the side of the motherboard (typical of an ATX motherboard) or may require you to attach a port to the back of the case and then run a small ribbon cable to connect that port to the motherboard.

Closing the Case

After you install all the components, slide the cover over the metal frame of the case. This may be a challenging part of the repair. Cases are generally designed to be the most inexpensive part of the PC. They're disassembled much more easily than they're reassembled. Tighten the screws on the outside of the case, or make sure the case has snapped into the proper position.

Attaching Input Devices

Input devices such as the keyboard and mouse should be attached in the same ports from which they were removed. Be sure the keyboard and mouse are plugged into the correct ports if they both use a PS/2 connector. A good rule of thumb is that the keyboard attaches to the port closest to the outside of the machine.

Other input devices can be connected through USB or FireWire connections and should be configured per the vendor's documentation.

Attaching Display Devices

Connect the display devices to the system using the connectors discussed in Chapter 1, "Hardware." Display devices can include a simple monitor, a projector, or any of several other choices. In all cases, you should follow the vendor's documentation when adding a new display device to the system.

Optimizing the Personal Computer

The most common need for an upgrade is to increase system performance. Over time, a computer's performance will decrease as newer software is added. In most cases, newer versions of software require additional resources that aren't available. The PC was originally configured

to run at certain performance levels that considered the applications and peripherals available when it was produced. Upgrades increase the system's performance to accommodate newer software and peripheral devices.

Toward the end of the system's life expectancy, it may become necessary to upgrade the system for required programs or for new hardware to function. If the system is too antiquated, it may be more cost efficient to replace the entire computer. However, in many cases the system's performance can be enhanced to acceptable levels by adding resources.

Memory

Since RAM is used to store data temporarily while the PC is operating, if the amount of available RAM is insufficient, the operating system will utilize hard disk space to store some of the data. Because the speed at which the data stored on a hard drive is accessed is considerably lower than the speed at which data can be accessed in RAM, the performance of the system will degrade as more and more information is stored on the hard drive.

Both Windows 2000 Professional and Windows XP require a minimum of 64MB of RAM. This should truly be at least 128MB for daily use on a workstation; and generally, the more you can add to the system, the better the performance you can expect. With Windows Vista, the minimum is 512MB for the Home Basic version and 1GB for all other versions. These numbers, again, represent bare minimums, and the more you can add to the system, the better the performance you can expect.

Disk Subsystem

The disk subsystem consists of the hard drives, the controllers, and the cables used to connect them.

HARD DRIVES

Hard drives are most commonly replaced because the system runs out of space to store data and program files. A small hard drive is replaced with one of larger capacity, or an additional hard disk is added.

Another reason to upgrade a hard drive is to increase the speed at which data can be written to or read from the drive. For example, replacing an old hard disk that conforms to ATA-3 standards with a newer one that conforms to ATA-7 (UltraATA/133) results in a disk that has a much faster access time and data-transfer rate (provided the IDE controller and the cable are of the correct type to support it).

There are two common ways to replace a disk drive in a computer: adding a drive or completely replacing the disk. Each approach has benefits and drawbacks:

Complete Replacement If you need additional hard disk capacity and don't have the physical room for a second drive inside the computer's case, or you don't want to manage two drives, complete replacement is necessary. Complete replacement requires reinstalling or restoring the operating system, program files, and data on the new drive. Because this is a considerable undertaking, drive-image tools have been developed to aid in this process. A drive-image tool takes a snapshot of the drive and allows you to create an image that can be expanded on the larger drive, thus avoiding reinstallation.

These images are normally compressed and require less space than the actual contents of the drive, allowing the images to be placed on a CD or other storage media. Some examples of this type of data transfer programs are Norton Ghost and Seagate PowerQuest Drive Image. Larger corporations use these tools to create a basic image of the operating system and commonly used programs to decrease downtime and lower upgrade and repair costs.

Adding Drives The simplest way to increase hard drive capacity is to add another drive. Most desktop PCs have IDE controllers built into the motherboard. These controllers allow for two devices to be connected to both the primary and secondary controller. With this type of architecture, four IDE devices can be installed in a PC, if space permits.

After adding the drive, you can place data and programs on it. This type of installation doesn't require the reinstallation or restoration of the operating system and program files on the new drive (but will still require partitioning/formatting).

CONTROLLER CARD

If the motherboard is more than a few years old, its IDE interface may not support the latest, fastest UltraATA standards. To get the highest performance out of a new hard drive, you may want to install an IDE or SATA controller card that supports the same standard as the new drive (for example, UltraATA/133, ATA-7, SATA 150, or SATA 2).

CABLE

Many of the UltraATA drives work only with a special 80-wire ribbon cable. When installing such drives on an existing IDE interface, you'll probably also want to replace the 40-wire cable with an 80-wire one. Most new hard disks come with the 80-wire cable.

CPU Upgrade

The frequency at which the processor operates (GHz) determines the speed at which data passes through the processor. Upgrading the processor to a higher frequency will provide a dramatic improvement in the system's overall performance.

It's important to remember that replacing a processor requires some research. Most motherboards support a certain class of processor; they don't have the capacity to upgrade to a different class of chip. For example, it isn't possible to upgrade a Pentium-class chip to a Pentium IV–class chip. This relates not only to the processor slots, but also to the power requirements of the chip. You must consider the additional cooling requirements of the new chip as well. In most cases, processor upgrades are accomplished by replacing the motherboard and processor using a special overdrive chip. Overdrive chips are also discussed in Chapter 1, "Hardware."

Some motherboards support the use of multiple CPUs, and in such motherboards, additional CPUs can improve overall system performance. Although the system doesn't run at a faster speed (in terms of GHz), an additional CPU makes the system able to process more operations per second.

Upgrading the BIOS

When the BIOS no longer supports all the devices that need to be connected to the PC, an upgrade is needed. There are two ways to upgrade the BIOS chip: by manually replacing the chip or by using special flash software.

MANUAL CHIP REPLACEMENT

Manual chip replacement requires you to remove the old chip and replace it with a new chip provided by the motherboard manufacturer. Manual replacement isn't an option in today's PCs.

FLASH BIOS UPGRADE

Flash BIOS is the modern way of upgrading a computer's BIOS. By placing the BIOS update disk on a bootable media (CD, flash drive, etc.) and booting the machine, a technician can reprogram the system's BIOS to handle new hardware devices that the manufacturer has included.

This works because the BIOS in modern systems is written in an electrically erasable programmable ROM (EEPROM) chip. This chip is normally read-only, but when it receives a stronger-than-normal voltage of electricity, it can temporarily become rewritable. The utility for updating the BIOS includes instructions to the motherboard to deliver this extra-strong electricity prior to the new BIOS update being sent to the chip.

Manufacturers periodically post the flash upgrades on their websites for you to download. Be aware that you must take care in this process, because the BIOS could be disabled and require the motherboard to be shipped back to the manufacturer. In most cases, the flash program will give you the opportunity to save the current software and settings to a restore disk that can reverse the changes if necessary.

Upgrading the Cooling System

The cooling system consists of the fan in the power supply, the fan or heat sink on the CPU, and any additional heat sinks or fans in the case. If a system is inadequately cooled, lockups and spontaneous reboots may occur.

Liquid-cooled cases use circulating water rather than fans to keep components cool. These cases are typically more expensive than standard ones and may be more difficult to work on for an untrained technician, but they result in an almost completely silent system.

Air cooling is the most common cooling method used in PCs. CPUs typically have active heat sinks, which are heat sinks that include an electric fan that constantly channels heat away. A CPU that is running too hot may benefit from a better cooling fan. The heat sink portion is a block of spikes that channel heat away from the CPU.

Most passive heat sinks (that is, heat sinks that don't include a fan) are attached to the CPU using a glue-like thermal compound. This makes the connection between the heat sink and the CPU more seamless and direct. Thermal compound can be used on active heat sinks, too, but generally it isn't because of the possibility that the fan may stop working and have to be replaced.

In addition to the main fan in the power supply, you can also install additional cooling fans in a case to help circulate air through the case.

Upgrading to a Faster NIC

The typical speed for an Ethernet network today is 100BaseT, or 100Mbps. This speed requires a 100BaseT network card. 10BaseT network cards can coexist on a 100BaseT

network but will send and receive data at only 10Mbps. Upgrading to a higher-speed network card can improve network performance in such a case.

In addition, new Ethernet technologies such as Gigabit Ethernet are becoming popular; they push the speed beyond 100Mbps. Upgrading to a network interface card (NIC) that supports these even faster speeds may be advantageous if the PC is on a network that supports them.

Specialized Video Cards

A standard 2D video card is adequate for business use, but for the serious graphic artist or gamer, a 3D video card with acceleration features can provide much better performance. These video cards include extra RAM buffers for holding video data, better on-board processing assistance for motion video, and support for the application programming interfaces (APIs) that the popular applications and games are written for, such as DirectX.

Drivers for Legacy Devices

A legacy device is one that is based on old technology. Examples include an ISA expansion card or a device that connects to a COM or LPT port rather than using the newer USB port. The term *legacy* can also refer to a piece of used hardware that is based on older technology internally.

Windows supports a wide variety of legacy devices with its own native drivers, but you may sometimes need to seek out a driver for a legacy device to run under a particular operating system version. The best source is the website of the device manufacturer. Other sources are also available, such as driver repositories on the Web.

Bus Types and Characteristics

When you're selecting upgrade devices, you may have a choice of bus types to which to connect the new device. It's important to understand the benefits of the various buses so you can choose wisely.

For example, you may have a choice of an ISA or PCI internal device, or a COM port or USB device. Or you may need to choose between an AGP and a PCI or PCIe video card.

For external ports, USB is better and faster than both COM (legacy serial) and LPT (legacy parallel). It's further advantageous because of its seamless Plug and Play integration and its hot-plugging ability.

For internal buses, PCIe x 16 is fastest and best for video and AGP is second-best. PCI is the next most desirable. ISA is old technology and nearly obsolete, and you should avoid it whenever possible. One possible exception is an internal modem. Because an internal modem operates at a maximum of only 56Kbps, it will be least affected by being relegated to the ISA bus. In contrast, a video card will suffer greatly on ISA.

Table 7.1 describes the speeds and characteristics of internal expansion buses.

TABLE 7.1 Comparison of ISA, PCI, and AGP Buses

Bus	Width	Speed	Uses
ISA	8-bit or 16-bit	8MHz	Avoid if possible, or use for slow devices like modems
PCI	32-bit	33MHz	All nonvideo internal expansion boards
AGP	64-bit	66MHz to 133MHz	The primary video card in the system

Memory Capacity and Characteristics

When you're selecting RAM for a memory upgrade, it's important to buy the right kind. On a modern system, you must match the RAM to the motherboard's needs in the following areas:

Physical Size 168-pin or 184-DIMMs, or 184-pin RIMMs.

Type SDRAM, double data rate (DDR) SDRAM, or Rambus RAM.

Speed PC100, PC133, and up. Faster RAM than is required will work, but slower RAM will not.

Capacity 128MB and up. Older systems may use SIMMs, which have somewhat more complex shopping issues:

Physical Size 30-pin (8-bit) or 72-pin (32-bit).

Parity Some SIMMs have an extra chip for parity checking. Some motherboards require parity RAM; others make it optional or forbid it.

Refresh Technology Some SIMMs are extended data out (EDO), allowing for better performance through less frequent refreshing. Some motherboards require it; others make it optional or forbid it.

When you're shopping for RAM for a system that uses SIMMs, it's important to consult the motherboard manual to find out any special rules for installation. Some motherboards have complex charts showing the combinations and positions of the SIMMs they will allow.

Motherboards may combine one or more RAM slots into a single logical bank, and all the RAM installed in that set of slots must be identical in every way. Check the motherboard documentation. On systems that use 30-pin SIMMs, four slots typically combine to create a single bank. On 486 systems that use 72-pin SIMMs, each SIMM slot is a separate bank. On Pentium systems that use 72-pin SIMMs, two SIMM slots together form a bank.

System/Firmware Limitations

One of the most common problems in upgrading to a larger hard disk is the BIOS's inability to support the larger disk size. In the original IDE specification, the size limit was 540MB. This limitation was upped to 8GB with the introduction of logical block addressing (LBA) in 1996, which the BIOS must support. A BIOS update may be available for the motherboard to enable LBA if needed.

Since the last update was 11 years ago, this is a situation you should never encounter in the real world, but should be aware of as you study for the CompTIA exam.

The 8GB limitation can be broken if the BIOS supports Enhanced BIOS Services for Disk Drives, a 1998 update. Again, a BIOS update for the motherboard may enable this support if it's lacking.

If no BIOS update is available, the choices are to replace the motherboard, to use the drive at the maximum size the BIOS can recognize, or to install a utility program (usually provided with the hard disk) that extends the BIOS to recognize the new drive. Such utilities are useful but can introduce some quirks in the system that can't be easily undone, so their usage isn't recommended except where no other alternative exists.

Power-Supply Output Capacity

A power supply has a rated output capacity in watts, and when you fill a system with power-hungry devices, you must make sure that maximum capacity isn't exceeded.

Selecting a CPU for a Motherboard

The CPU must be compatible with the motherboard in the following ways:

Physical Connectivity The CPU must be in the right kind of package to fit into the motherboard.

Speed The motherboard's chipset dictates its external data-bus speed; the CPU must be capable of operating at that external speed.

Instruction Set The motherboard's chipset contains an instruction set for communicating with the CPU; the CPU must understand the commands in that set.

Voltage The CPU requires a certain voltage of power to be supplied to it via the motherboard's interface. This can be anywhere from +5V for a very old CPU down to around +2.1V for a modern one. The wrong voltage can ruin the CPU.

Exam Essentials

Know when to attach an antistatic wrist strap. One thing from this chapter that will be on the test is attaching an antistatic wrist strap. You should attach one of these to a ground

mat every time you open a computer. More components are damaged from static discharge than from anything else.

Know the "black wires together" rule. When you're attaching an AT power supply to a motherboard, the connector will be in two pieces, P8 and P9. These must be oriented so the black wires on each connector are near the black wires on the other connector. Otherwise, damage to the motherboard can result.

Know what performance enhancements are achieved by upgrading memory. Upgrading the amount of RAM a computer has will increase the speed of the machine by preventing the use of the hard drive to store data that is being accessed.

Know what performance enhancements are achieved by upgrading the hard drive, the IDE controller, and the IDE ribbon cable. Replacing the hard drive can allow you to add to the overall storage capacity of the machine. In some cases, read/write performance can be improved by upgrading. Understand the UltraATA requirements.

Know what performance enhancements are achieved by updating the BIOS. Replacing the BIOS can increase the number of supported devices.

Understand the benefits of improving system cooling. Make sure you know what symptoms are produced by inadequate cooling and what options are available for upgrading the cooling system.

Diagnostic Procedures for PC Components

The various tools that you can use to discover the available resources on a PC can make installing new hardware a lot easier. Unfortunately, the tools are of little use unless you understand the information they present. In this section, we discuss the various resources that may be used by PC components and how those resources are used.

Interrupt request lines, direct memory access channels, and input/output addresses are configurable aspects of the communication between the devices inside a PC. Interrupt request (IRQ) lines are used to signal that an event has taken place that requires the attention of the CPU. Input/output (I/O) addresses refer to the hardware communication lines that carry data between the CPU and the bus slots of the PC. Direct memory access (DMA) channels allow a storage device or adapter card to send information directly into memory without passing through the CPU, which results in a faster data transfer rate.

With Plug and Play, it is rare to need to manually configure anything anymore. Nevertheless, you should be familiar with how to do so as you prepare for the A+ exam.

Critical Information

At some point, every computer will require the installation of a new component, whether it's a new sound card, a memory upgrade, or the replacement of a failed device. As a technician, you'll be required to perform this task time and time again. You should be well versed in determining the installation configuration and resources.

Whenever a new component is installed into a PC, its resources must be correctly configured, or the device won't function correctly (those resources may be IRQs, I/O addresses, and/or DMA channels). This is the most common problem when installing new circuit boards.

Understanding Computer Resources

In general, there are four main types of PC resources you may need to be aware of when installing a new component: IRQ lines, memory addresses, DMA channels, and I/O addresses.

Interrupt Request Lines

IRQs are appropriately named. Interrupts are used by peripherals to interrupt, or stop, the CPU and demand attention. When the CPU receives an interrupt alert, it stops whatever it's doing and handles the request.

Each device is given its own interrupt to use when alerting the CPU. (There are exceptions; some PCI devices can share with one another, for example, and USB devices all use a single interrupt.) AT-based PCs have 16 interrupts available. Given the limited number of available interrupts, it's critical that you assign them wisely! Table 7.2 lists the standard use and other uses associated with each interrupt.

TABLE 7.2 AT Interrupts

Interrupt	Most Common Use	Other Common Uses
0	System timer	None
1	Keyboard	None
2	None; this interrupt is used to cascade to the upper eight interrupts (see note following this table)	None
3	COM2	COM4
4	COM1	COM3
5	Sound card	LPT2
6	Floppy-disk controller	Tape controllers
7	LPT1	Any device

TABLE 7.2 AT Interrupts *(continued)*

Interrupt	Most Common Use	Other Common Uses
8	Real-time clock	None
9	None	Any device
10	None	Any device
11	None	Any device
12	PS/2-style mouse	Any device
13	Floating-point coprocessor	None
14	Primary IDE channel	SCSI controllers
15	Secondary IDE channel	SCSI controllers and network adapters

Interrupt 2 is a special case. Earlier (XT-based) PCs had only eight interrupts because those computers used an 8-bit bus. With the development of the AT, eight more interrupts were created (to match the 16-bit bus), but no mechanism was available to use them. Rather than redesign the entire interrupt process, AT designers decided to use interrupt 2 as a gateway, or cascade, to interrupts 9–15. In reality, interrupt 2 is the same as interrupt 9. You should never configure your system so that both interrupt 2 and 9 are used.

Most experienced field technicians have the standards (listed in the table) memorized. In studying for the exam, make sure you know all the default assignments, as well as the assignments for COM1–COM4 and LPT1–LPT2.

Memory Addresses

Many components use blocks of memory as part of their normal functioning. NICs often buffer incoming data in a block of memory until it can be processed. Doing so prevents the card from being overloaded if a burst of data is received from the network.

When the device driver loads, it lets the CPU know which block of memory should be set aside for the exclusive use of the component. This prevents other devices from overwriting the information stored there. Certain system components also need a memory address. Memory addresses are usually expressed in a hexadecimal range with eight digits, such as 000F0000–000FFFFF.

Direct Memory Access

Direct Memory Access (DMA) allows a device to bypass the CPU and place data directly into RAM. To accomplish this, the device must have a DMA channel devoted to its use.

All DMA transfers use a special area of memory known as a buffer, which is set aside to receive data from the expansion card (or CPU, if the transfer is going the other direction). The basic architecture of the PC DMA buffers is limited in size and memory location.

No DMA channel can be used by more than one device. If you accidentally choose a DMA channel that another card is using, the usual symptom is that no DMA transfers occur, and the device is unavailable.

Certain DMA channels are assigned to standard AT devices. DMA is no longer as popular as it once was, because of advances in hardware technology, but it's still used by floppy drives and some keyboards and sound cards. The floppy disk controller typically uses DMA channel 2. A modern system isn't likely to run short on DMA channels because so few devices use them anymore.

I/O Addresses

I/O addresses, also known as port addresses, are specific areas of memory that components use to communicate with the system. Although they sound like memory addresses, the major difference is that memory addresses are used to store information that will be used by the device itself. I/O addresses are used to store information that will be used by the system. An I/O address is typically expressed using only the last four digits of the full address, such as 03E8. I/O addresses are usually expressed as a range, such as 03E8–03EF. The exam asks about a few I/O addresses; Table 7.3 provides a list of some hexadecimal addresses you should know.

TABLE 7.3 I/O Addresses

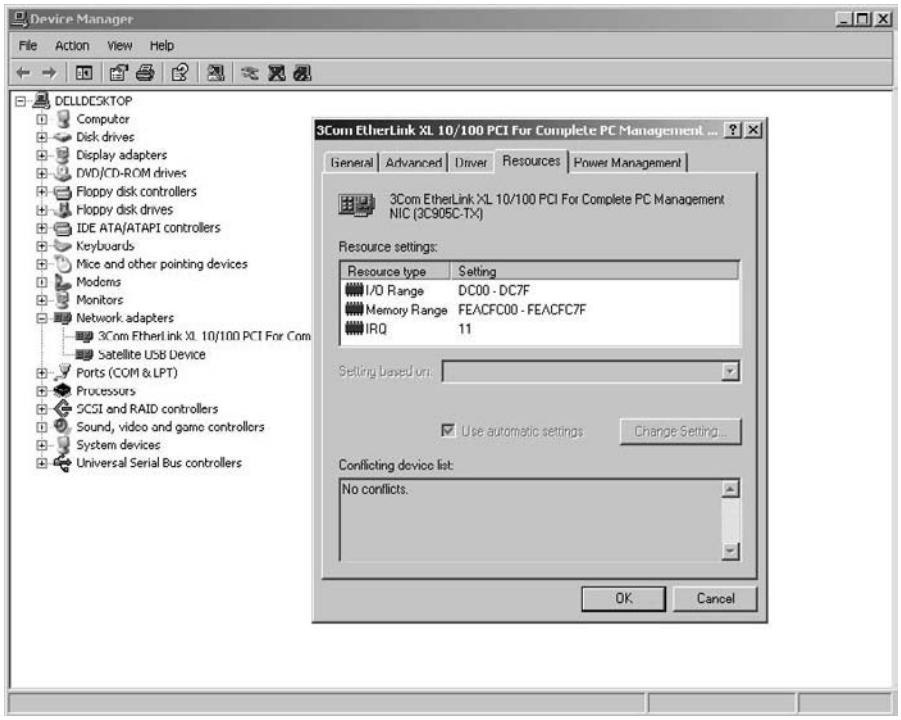
Port	I/O Address
COM1	03F8–03FF
COM2	02F8–02FF
COM3	03E8–03EF
COM4	02E8–02EF
LPT1	0378–037F
LPT2	0278–027F
Primary IDE	01F0–01F7
Secondary IDE	0170–0177

Determining Available Resources

The best way to determine the PC's available resources is by using hardware-configuration-discovery utilities. These software programs talk to the PC's BIOS as well as the pieces of hardware in the computer and display which IRQ, DMA, and memory addresses are being used. Most operating systems include some way of determining this information, including Device Manager in Windows 2000, XP, and Vista. To display it, right-click My Computer and choose Properties, click the Hardware tab, and then click Device Manager.

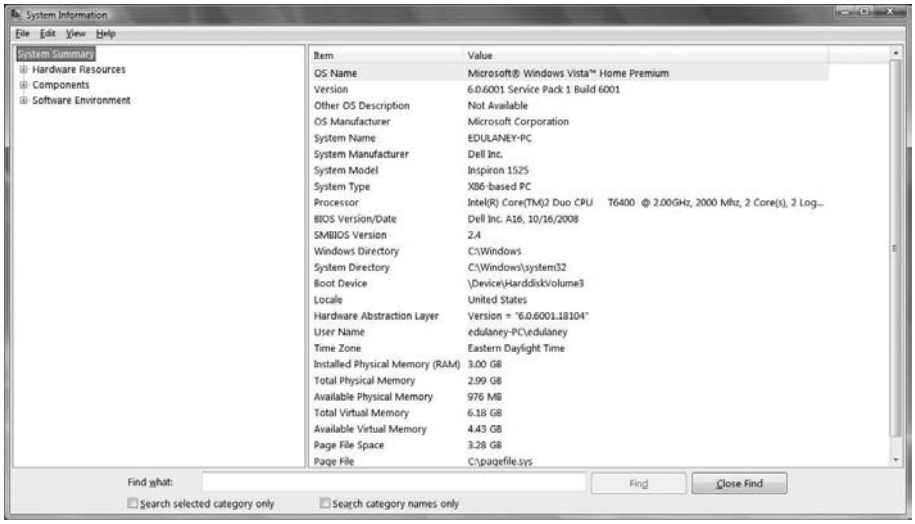
To display a device's resources, open the category by clicking the plus sign next to it and double-clicking the device name. Then look in the Resources tab for that device. (See Figure 7.6.)

FIGURE 7.6 Device Manager under Windows XP



You can also get this same information through the System Information utility. To run it, choose Start ➢ (All) Programs ➢ Accessories ➢ System Tools ➢ System Information. Then click one of the categories in the left pane to see the information in the right pane. (See Figure 7.7.)

FIGURE 7.7 System Information under Windows Vista



Manually Specifying a Resource Assignment

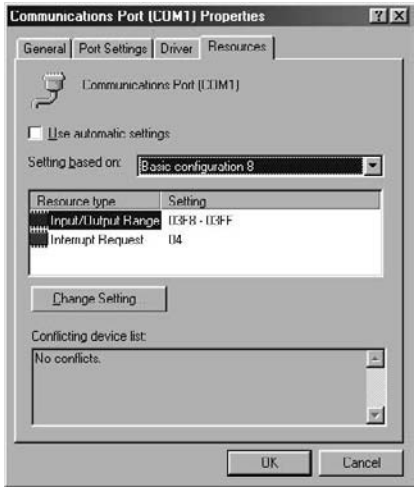
In Windows' Device Manager, you can manually specify the resources for a device to solve a problem with a resource conflict—that is, a situation in which two or more devices lay claim to the same resource. A resource conflict usually appears as a yellow exclamation point next to a device's name in Device Manager. Double-clicking the device opens its Properties box; on the Resources tab, you'll find an explanation of the problem in the Conflicting Device list.

To change a device's resource assignments, clear the Use Automatic Settings check box, and select a different configuration from the Setting Based On drop-down list. (See Figure 7.8.) If none of the alternate configurations resolves the conflict, you can double-click a specific resource on the Resource Type list and enter a manual setting for it.

Most modern computers use a power management and configuration method called Advanced Configuration Power Interface (ACPI), which helps prevent resource conflicts but which also limits the amount of tinkering you can do with manual resource assignments. If you get a message that a particular resource can't be changed, or if the Use Automatic Settings check box is unavailable, it's probably because of ACPI.

If the device isn't Plug and Play–compatible, it may have jumpers for hard-setting the resources assigned to it. If that's the case, Windows won't be able to change these assignments; it will use the assignments the device requires.

FIGURE 7.8 Manually changing a resource assignment



Diagnostic Resources

When you're stumped by a computer problem, where do you turn? The exam objectives specify that you should know about the following resources:

User/Installation Manuals Consult the manuals that came with the hardware and software.

Internet/Web Resources Consult the websites of the companies that make the hardware and software. Updates and patches are often available for download, or the websites may be knowledge bases of troubleshooting information.

Training Materials If you've taken a class pertaining to the hardware or software, consult the materials you received for that class.

Exam Essentials

Know the default IRQs for COM ports and common devices. Know the default IRQs for COM ports and common devices such as modems, sound cards, and disk drives.

Be familiar with Device Manager. Device Manager can display information about the computer's memory, I/O ports, IRQs being used, and many other PC resources.

Understand how manual resource assignments are set. Manual resource assignments for Plug and Play devices are set on the Resources tab of the device's Properties box. For a non-PnP device, resource assignments are controlled by jumpers on the device itself.

Working with Laptops and Portable Devices

Contrary to the name, this objective doesn't expect you to know everything there is to know about laptops—you had to do much of that for the Essentials exam. Instead, this objective focuses on several key areas.

Critical Information

This exam focuses on three key areas, regardless of the elective you've chosen to take. These three are discussed in the following sections. Some of this material is overlap from Chapter 1, "Hardware," and you should be able to breeze through it fairly quickly.

Electrical Issues

Electrical issues can be either AC- or DC-related. AC is the standard current coming from the outlet to the power cord. The power supply converts AC to DC, and the computer runs on DC power (which is why it can run on a battery for so long).

In the absence of AC power, the laptop will attempt to run off the battery. Although this solution is good for a time, AC power must be available to keep the battery charged and the laptop running. Most laptops have an indicator light that shows whether AC power is being received; the AC cord typically has an indicator light as well, to show that it's receiving power. If no lights are lit on the cord or the laptop, indicating that AC power is being received, try a different outlet or a different cord.

One item the AC presence can affect is the action of the network card. To conserve power, the network card is often configured to not be active when running on DC power. You can access the relevant dialog box by choosing Start ➢ Control Panel and selecting Internal NIC Configuration.

The biggest issue with DC power problems is a battery's inability to power the laptop as long as it should. This issue can be caused by an older battery building up a memory and thus not offering a full charge (lithium ion batteries don't suffer this fate). If a feature is available to fully drain the battery, you should use it to eliminate the memory (letting the laptop run on battery on a regular basis greatly helps). If you can't drain the battery and eliminate the memory effect, you should replace the battery.

LCDs

The liquid crystal display (LCD) consists of three key elements: the screen, the inverter, and the video card. The screen is made of liquid crystals to reduce power consumption and the thickness of the monitor (it's a flat panel made from two polarized glass panes with liquid between them). The panels are made of columns and rows called a matrix.

Depending on the capability of the display, most panels fall into the category of active matrix or passive matrix. With a passive matrix, the display is essentially created at one

time, and changes take place to an entire column; with an active matrix, a single liquid crystal (pixel) can be changed.

Video Sharing

Video sharing is extremely popular, whether it's done through streaming media from a popular website (such as YouTube), by sending digital videos from your home camera to grandma and grandpa, or using any of a hundred other possibilities. One effect of the increased use of video is a greater need for memory. The more memory—and the faster the memory—that is installed in a system, the more potential it has to be able to queue or cache the video and deliver it seamlessly.

For the exam, you should know that the increased use of video has the potential to bottleneck other areas as well. Some areas to be aware of are the speed of the network connection (never view an episode of your favorite television show across a dial-up connection) and the computer itself (processor).

Troubleshooting

To solve a problem with a laptop or portable device (the terms are mostly used interchangeably by CompTIA), you should fully understand the hardware you're working with. The following list describes those things CompTIA wants you to be comfortable with for this objective. Some may seem like common sense, in which case you should have no difficulty choosing the correct answers on the exam:

AC Power Issues AC power must be available to keep the battery charged and a laptop running. There is an indicator light on most laptops which shows whether AC power is being received and the AC adapter typically has an indicator light on it as well. If no lights are lit on either the adapter or the laptop indicating that AC power is being received, try a different outlet or different adapter to see if that resolves the problem.

Antenna Wires Most laptops today include an internal wireless card. This is convenient, but it can be susceptible to interference (resulting in a low signal strength) between the laptop and the access point. Do what you can to reduce the number of items blocking the signal between the two devices, and you'll increase the strength of the signal.

Backlight Functionality The backlight is the light in the PC that powers the LCD screen. It can go bad over time and need to be replaced, and it can also be held captive by the inverter. The inverter takes the DC power the laptop is providing and boosts it up to AC to run the backlight. If the inverter goes bad, you can replace it on most models (it's cheaper than the backlight).

DC Power Problems Most NiCad batteries build up a memory and that memory can prevent a battery from offering a full charge. The biggest issue with DC power problems is a battery's inability to power the laptop as long as it should. If a feature is available to fully drain the battery, you should use it to eliminate the memory (letting the laptop run on battery on a regular basis greatly helps). If you can't drain the battery and eliminate the memory effect, you should replace the battery.

External Monitors An external monitor may be connected to the laptop directly or through a docking station. With many laptops, if the external monitor is connected before you boot the laptop, the laptop will automatically detect the monitor and send the display there. If you connect after the laptop is booted, you should use the appropriate Fn key to send the display to the monitor.

Keyboard Problems Problems with keyboards can range from collecting dust (in which case you need to blow them out) to their springs wearing out. In the latter case, you can replace the keyboard (they cost about 10 times more than desktop keyboards) or choose to use an external one (providing the user isn't traveling and having to lug another hardware element with them).

LCD Cutoff Switch A thermal cutoff switch is often included in laptops to turn off the system if the temperature rises too high. Although this switch may go bad and cause the laptop to unduly turn off, usually a shutdown is a symptom of another problem; you should try to isolate what is causing the heat (dirt, debris, and so on) and address that issue.

Pointer Difficulties The pointer device used on the laptop, like the keyboard, can be affected by dirt or debris as well as by continual use. If the device fails to function properly after a good cleaning, you can replace it (expensive) or opt for an external pointer (such as a wireless mouse).

Stylus Issues A stylus may no longer work on a tablet computer due to damage or excessive wear. When this occurs, you can purchase inexpensive replacement styluses for most units.

Unneeded Peripherals To keep the system running at peak efficiency, you should disconnect or disable unneeded peripherals. Every peripheral has the ability to drain power and resources from the PC, and you don't want that if it can be avoided.

Video Issues One of the biggest problems with video is incorrect settings. You can change the video settings easily on the laptop through the operating system. Make sure you have the correct—and most current—drivers.

A few other miscellaneous topics—such as Fn toggling and wireless card issues—have been addressed elsewhere and there is nothing more to say about them, but it is possible that questions regarding them may appear in this section of the exam.

Exam Essentials

Know the various electrical issues discussed. Power supplies convert AC to DC power and problems can occur within either current.

Recognize the need for memory when working with video. Video sharing is popular and requires a lot of resources to function properly. One such resource is memory, and—as a general rule—the more memory, and the faster the memory, the better the performance.

Know how to work with laptop components. Understand the issues that can arise, and know what to look for to begin trying to fix them.

Know the power configuration settings. Using power configuration, it's possible to disable the NIC and other devices to conserve power. It's also possible to receive notification when the battery life reaches low levels.

Building a Toolbox

If you are going to troubleshoot personal computers, you are going to need to have some tools at your disposal. Some of those tools are software-based (and many are built into the operating system) while others are hardware-based and items you will want at your ready. This section takes a look at each of these.

Critical Information

A big part of being a successful technician is knowing what tools are appropriate to correct which problems. The following diagnostic tools and utilities are ones you should be comfortable with.

Software Tools

While there are a number of third-party providers that create tools to allow you to diagnose problems, CompTIA only tests on the ones included with the operating system. Those you should know for this exam are listed here:

Task Manager Lets you shut down nonresponsive applications selectively in all Windows versions. In Windows 2000, XP, and Vista, it does much more, allowing you to see which processes and applications are using the most system resources. To display Task Manager, press Ctrl+Alt+Delete. It appears immediately in some operating systems, while in others you must click the Task Manager button to display it after pressing Ctrl+Alt+Delete. Use Task Manager whenever the system seems bogged down by an unresponsive application.

Dr. Watson This tool enables detailed logging of errors. Use it whenever you think an error is likely to occur (for example, when you're trying to reproduce an error). This tool exists in Windows 2000 and Windows XP, but not in Windows Vista.

Event Viewer This tool enables you to see what's been going on behind the scenes in Windows 2000, XP, and Vista. Use Event Viewer when you want to gather information about a system or hardware problem.

Device Manager As already mentioned, Device Manager shows you what hardware is installed and lets you check its status. Use this when a device isn't functioning and you're trying to figure out why.

WinMSD Another name for System Information, WinMSD is the same utility you can select from the System Tools menu. (Running it at the Run command with `WINMSD` is an alternative.) WinMSD provides comprehensive information about the system's resource usage, hardware, and software environments. Use it when you need to gather information about the system.

Hardware Tools

In addition to the software tools included with the operating system, you should be familiar with a number of hardware tools. The exam objectives specifically mention familiarity with these tools:

Power Supply Tester A power supply tester, as the name implies, is used to test the output of a power supply. These devices can range from simple devices that check the presence of current to complex (and costly) machines that log everything about the current for a period of days and can help you isolate problems.

Cable Testers Cable testers are used to verify that the cable you are using is good. Commonly used with network cabling, you can perform many of the same tests with a multimeter.

Multimeter A multimeter combines a number of tools into one. There can be slight deviations, but a multimeter always includes a voltmeter, an ohmmeter, and an ammeter (and is sometimes called VOM as an acronym).

Antistatic Pad and Wrist Strap A properly grounded strap can save you from suffering a nasty jolt. An antistatic pad works similarly and not only can protect you, but can also protect sensitive equipment from static damage.

Another option is antistatic spray. Usually applied as a mist to carpets, chairs, and so on, this spray reduces the amount of static electricity present and can save computers and components.

Specialty Hardware/Tools Specialty tools can include anything needed for a specific purpose, but there are a few things you should always have: a parts grabber for picking up pieces that have fallen or are hard to hold on to; a chip extractor; and wire cutters, strippers, or crimpers. These tools can be used to solve a number of problems.

Loopback Plugs Also called wrap plugs, loopback plugs take the signal going out and essentially echo it back. This allows you to test parallel and serial ports to make certain they're working correctly.

Extension Magnet An extension magnet is used to reach metal pieces in places where hands can't fit—for example, retrieving a screw that has fallen in a case and wedged between two cards. Be very careful if using any magnet around magnetic media (such as a hard drive), as you can cause data loss by placing the magnet in proximity to the media.

Cleaning Products A good hand vacuum is a necessity. You need to be able to vacuum up dust, debris, and even toner on occasions. So, you want a vacuum that is capable of collecting small particles and won't pass them through the bag and back into the air. Spend the money on a good vacuum, and you'll be glad you did.

An assortment of other cleaning supplies should also be available. These include cleaning pads for monitors, contact cleaner, compressed air, and CD-cleaning supplies.

Exam Essentials

Know the software tools. Be able to differentiate between Task Manager, Dr. Watson, Event Viewer, Device Manager, and WinMSD. Know when to use each one of them and what information each will show.

Know the hardware tools mentioned. Be able to name the hardware tools and their purposes.

Working with Printers

This objective tests your knowledge of some of the basic operations of printers. The emphasis, however, is on detecting and solving problems with them. If you truly want to show your expertise with printers, CompTIA offers another certification, PDI+, which is meant for that purpose.

Critical Information

There are several ways to interact with a printing device, check its status, configure it, and so on. We'll first look at how to check its status and then delve deeper from there.

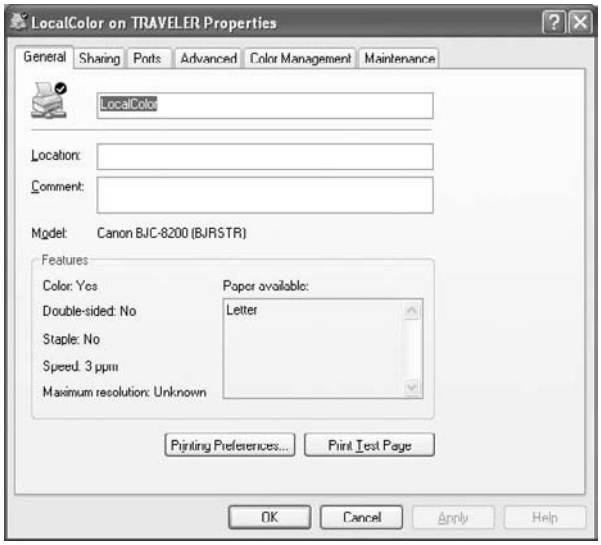
Checking Printer Status

The simplest way to check printer status is to choose Start ➢ Printers and Faxes, (in Windows Vista, Start ➢ Printers) right-click the icon of an installed printer, and choose Properties. Depending on the printer and its capabilities, you'll see a number of tabs, such as those shown in Figure 7.9.

Notice that from here you can choose the Color Management tab (for a color printer) and change the profile used. You can also choose the Maintenance tab and do other operations, such as the following:

- Cleaning
- Deep cleaning
- Roller cleaning
- Nozzle check
- Print-head alignment
- Custom settings (typically involves setting the printer to enhanced capabilities port [ECP] mode)

FIGURE 7.9 Typical property tabs available for a printer in Windows XP



Most printers—particularly those intended for use on networks—include additional software for interacting with them. Figure 7.10 shows the Toolbox program included with several HP LaserJet printers.

In addition to being able to see the status of the toner and maintenance kit via Toolbox, you can click Troubleshooting and access the following:

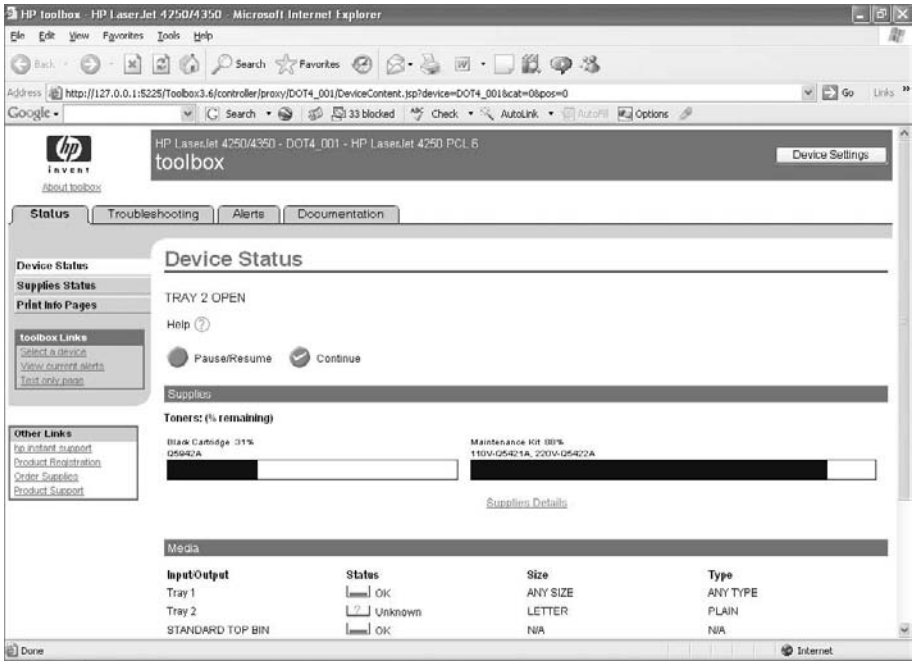
- Print-quality tools (general troubleshooting and print-quality troubleshooting)
- Maintenance
- Error messages (understand the messages as well as the accessory lights)
- Paper jams
- Supported media (always use parts for the specific printer model you have, to prevent a surfeit of problems)
- Printer pages (you can print out the configuration page, the supplies pages, the event log page, and the usage page)

Troubleshooting

To solve a problem of any type, you must always approach it from a systematic position. Solving printer problems is no different from solving network problems, and a recommended approach is as follows.

Gather as much information as you can about the problem. For example, when a user calls to report that they can't print to a network printer, you should immediately ask when they were last able to do so and what has changed since then.

FIGURE 7.10 Vendors generally offer utilities for advanced interaction with printers.



Review and analyze the data you've collected. Now that you've accumulated it, you need to look for the story it's telling you.

Isolate the problem. Is it confined to a single user, a group of users, a room, a floor, or a building, or is everyone affected? Knowing how narrowly you can isolate the issue can help you define the problem and come up with a fix.

Use the appropriate tools. Many times, the tools to use are available within the operating system (think of the troubleshooters available in Windows), and you can solve them easily. Other times, you have to turn to physical tools to help you solve a problem. The following is a list of tools you should be familiar with for printer problems:

Multimeter This device was covered in the previous section.

Screwdrivers A good set of quality screwdrivers fitted to the job you're working on is essential. Never try to force a larger screwdriver into a small slot, or you may do far more damage than was there when you began.

Cleaning Solutions Most liquids don't mix with computer elements, including printers. A few exceptions are those solutions created specifically for the purpose.

Extension Magnet You can use an extension magnet when you're working in tight places, to make certain you don't drop small parts. Be very careful, however, in using any magnet around a device that stores data magnetically (such as a hard drive); use this tool sparingly.

Test Patterns One of the simplest techniques of all is to print a test pattern and compare the results you get to those you desire. Almost every printer allows you to print a test, and this should be one of the first things you do when beginning to tackle a problem.

Other printing problems that can occur on an irregular basis include the following:

The Computer Won't Work While the Printer Is Printing If your operating system supports background printing (such as spooling), make certain those features are turned on.

A Print Job Is Clobbered by Another If you share a network printer, check the printer timeout settings on your workstation. If the number of seconds is too low, a printer can think it has received all of a print job when it hasn't, and accept the next incoming job.

Printing Stops Before It's Done Check the power being delivered to the printer, particularly if it's a laser printer. Because of the high charges and other operations going on, a laser printer pulls a lot of power. If you're sharing a circuit with a number of other things, problems may occur. A typical workgroup laser printer consumes 330 watts when printing, requires a minimum of 8 amps circuit capacity, and has a line voltage requirement of 50–60Hz.

Some specific troubleshooting tips based on printer type follow.

Troubleshooting Dot-Matrix Printers

A dot-matrix printhead reaches high temperatures, and care must be taken to avoid a user or technician touching it and getting burned. Most dot-matrix printers include a temperature sensor to tell if the printhead is getting too hot. The sensor interrupts printing to let the printhead cool down and then allows printing to start again. If this sensor becomes faulty, it can cause the printer to print a few lines, stop for a while, print more, stop, and so on.

The printhead should never be lubricated, but you can clean off debris with a cotton swab and denatured alcohol. Print pins missing from the print head will cause incomplete images or characters or white lines running through the text. This can be remedied by replacing the printhead.

If the printhead isn't at fault, make certain it's close enough to the platen to make the right image. The printhead can be moved closer and farther from the platen depending on the thickness of the paper and other considerations.

Another common culprit is the ribbon. A tight ribbon, or one that isn't advancing properly, will cause smudges or overly light printout.

Preventive maintenance includes keeping the printhead dry and clean, and vacuuming paper shreds from inside the machine.

Troubleshooting Ink-Jet Printers

Ink-jet printers encounter few problems. If the ink becomes goopy on the paper, make certain the nozzles are clean and the heating transistors are working properly. If the ink is drying out quickly, make certain the printhead is reaching the park position after print jobs are completed.

Troubleshooting Laser Printers

Just as laser printers are the most complicated of the types (and offer the most capabilities), they also have the most things that can go awry. A thermal fuse is included to keep the system from overheating, and if it becomes faulty, it can prevent the printer from printing. Many high-capacity laser printers also include an ozone filter to prevent the corona's ozone output from reaching too high a level. On these printers, the filter should be changed as a part of regular maintenance.

Other common problems and solutions are as follows:

Paper Jams While paper jams can be caused by numerous problems, two common ones are the paper not feeding correctly and moisture. To correct improper feeds, make sure you set the alignment guides for the paper you are using and verify the paper is feeding in straight. Keep paper from getting any moisture before feeding into the printer, as moisture often causes pages to stick together and bind.

One employee routinely had problems with a printer each time he went to print on high-quality paper—a problem experienced by no one else. Upon close examination, it turned out that each time he chose to print to the expensive paper, he counted the number of sheets he loaded into the printer—counting that involved licking his finger and then touching each page. A simple directive to stop doing this solved the problem.

Regardless of the cause of a paper jam, you need to always fully clear the printer of any traces of paper (torn or whole) before attempting to print again.

Error Codes Many laser printers include LCD displays for interaction with the printer. When error codes appear, refer to the manufacturer's manuals or website for information on how to interpret the codes and solve the problem causing them.

Out of Memory Error While PCs now may need a minimum of 1GB of RAM to run at a minimal level, it is not uncommon to find printers that still have only 4MB or 8MB of memory. If you are routinely running out of memory on a printer, add more memory if possible, and replace the printer when it is no longer possible to do so.

Lines and Smearing Lines and smearing can be caused by the toner cartridge or the fuser. Try replacing the toner first (and cleaning any that may have spilled). If this does not fix the problem, replace the fuser.

Blank Pages Print Verify that there is toner in the cartridge. If it's an old cartridge, you can often shake it slightly to free up toner once before replacing. If it's a new cartridge, make sure the sealing tape has been removed from the cartridge prior to placing it in the printer.

Be very careful when doing this operation. Someone who has asthma or who is sensitive to microfine particles could be adversely affected by the toner.

Dark Spots Print The most likely culprit is too much toner. Run blank pages through the printer to clean it.

Garbled Pages Print Make sure you're using the right printer driver in your application.

Ghosted Images Print Ghosting—repeating text or images on the page—is usually caused by a bad cartridge. There can be damage to the drum or charging roller and, if so, replacing the cartridge will help with the problem.

No Connectivity If a network printer is not able to receive jobs, it can be an issue with the IP address that it has (or, more correctly, does not have). Often the printer will need to be manually assigned an IP address to make sure that it has the same one each time. Read the manufacturer's documentation for assigning an IP address to the printer and walk through the steps to do so.

Print-Quality Problems See if your printer has the ability to turn Resolution Enhancement Technology (RET) on and off. This is what allows the printer to use partial-sized dots for images that are rounded. If it's turned off, turn it back on.

Preventive Maintenance

To keep your printers working efficiently and extend their life as much as possible, you should start by creating a log of scheduled maintenance as outlined by the vendor's guidelines and then make certain this maintenance log is adhered to. For many printers, the scheduled maintenance includes installing maintenance kits. Maintenance kits typically include a fuser, transfer roller, pick-up rollers (for the trays), separation rollers, and feed rollers.

After installing the maintenance kit, you need to reset the maintenance counter as explained in the vendor's documentation.

Pay a great deal of attention to the ambient surroundings of the printers as well. High temperature, high humidity, and high levels of dust and debris can negatively affect the life of the printer and the quality of print jobs.

Last, always make certain you use recommended supplies. It may be cheaper to buy off-brand supplies that aren't intended for your equipment, but you're taking a gamble with shortening the life of your printer and decreasing the quality of your output.

Preventive maintenance, in addition to the ozone filter, includes the following:

- Never reuse paper that has been through the printer once. Although it may look blank, you're repeating the charging and fusing process on a piece of paper that most likely has something already on it.
- Change the toner when needed. You should recycle; most toner manufacturers participate in a recycling program of some type. The toner cartridge should never be exposed to light for longer than a few minutes; it usually comes sealed in a black plastic light-resistant bag.

- Clean any toner that accidentally spills into the printer with a dry, lint-free cloth. Bear in mind that spilled toner in the paper path should clear after you run a few blank pages through. If toner gets on your clothes, wipe them with a dry cloth and wash them with cold water (hot water works like the fusing process to set them into the material).
- Clean any paper shreds, dust, or dander that gets deposited in the printer. Pressurized air is the most effective method of removal.
- Keep the drum in good working order. If it develops lines, replace it.
- Install the maintenance kit when needed and reset the page count. The maintenance kit (sometimes called a fuser kit), typically includes a fusing assembly, rollers, and separation pads. A printer display similar to "Perform Printer Maintenance" indicates the printer has reached its maintenance interval and a maintenance kit needs to be installed.
- Don't be afraid to cycle the power on an unresponsive printer. Turning it off, leaving it off for one minute to clear, then turning it back on can solve a great many problems.

Exam Essentials

Know how to interact with printers. Know that the Properties page for each, available from Windows, allows you to interact with them, but many printers also include advanced utilities that go beyond basic interaction.

Know the common printing problems listed. Understand the most common problems that occur in an environment.

Be familiar with the tools that can help you fix common problem types. Each tool has its own purpose and can be essential in trying to solve a particular type of problem. Be familiar with the most likely repair options for each common problem.

Know the importance of running scheduled maintenance. Scheduled maintenance can prolong the life of your equipment and help ensure that your output continues to live up to the quality you expect.

Understand the importance of a suitable environment. If you want your equipment to last as long as possible and deliver quality, you should pay attention to the environment in which you place it.

Review Questions

1. When working on a computer, what do you need for an adequate workspace?
2. When removing the case cover, why should you not remove all screws from the back of the PC?
3. What should an antistatic wrist strap be connected to?
4. Before you remove a power supply, what two things must you do?
5. What are hot-pluggable drives?
6. What are stand-offs?
7. Name the default IRQs for COM1 and COM2.
8. In what Windows utility would you manually change a hardware resource assignment?
9. What is one of the most common problems in upgrading to an UltraATA hard disk?
10. What is the default I/O address for LPT1?

Answers to Review Questions

1. First, the work area must be flat. Second, the area must be sturdy. Third, the area must be well lit, clean, and large enough to hold all pieces and necessary tools.
2. Some of these screws hold vital components (such as the power supply) to the case, and removing them will cause those components to drop into the computer.
3. You should plug one end of the antistatic wrist strap into the ground plug of an outlet.
4. Before you remove the power supply from the computer, you must disconnect the power supply connectors from the internal devices, and remove the mounting hardware for the power supply.
5. Hot-pluggable drives are those that can be added or removed while the computer is running.
6. The motherboard is held away from the metal case using brass or plastic spacers called stand-offs.
7. COM1 is usually IRQ4, and COM2 is usually IRQ3.
8. Device Manager.
9. One of the most common problems in upgrading to an UltraATA hard disk is a difference in the connector cable.
10. 0378-037F.

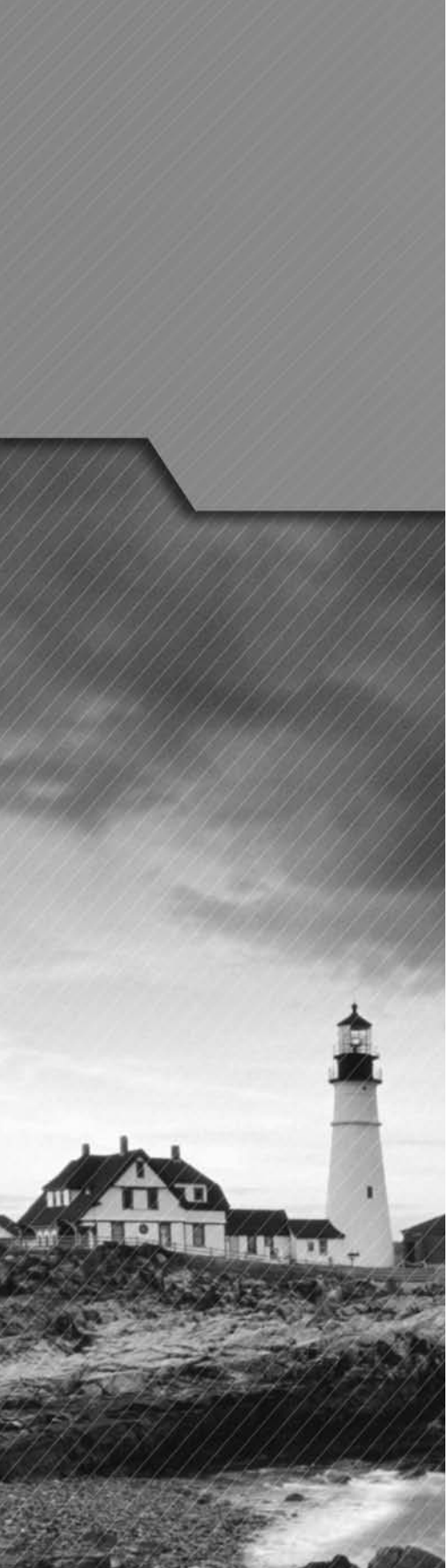
Chapter

8

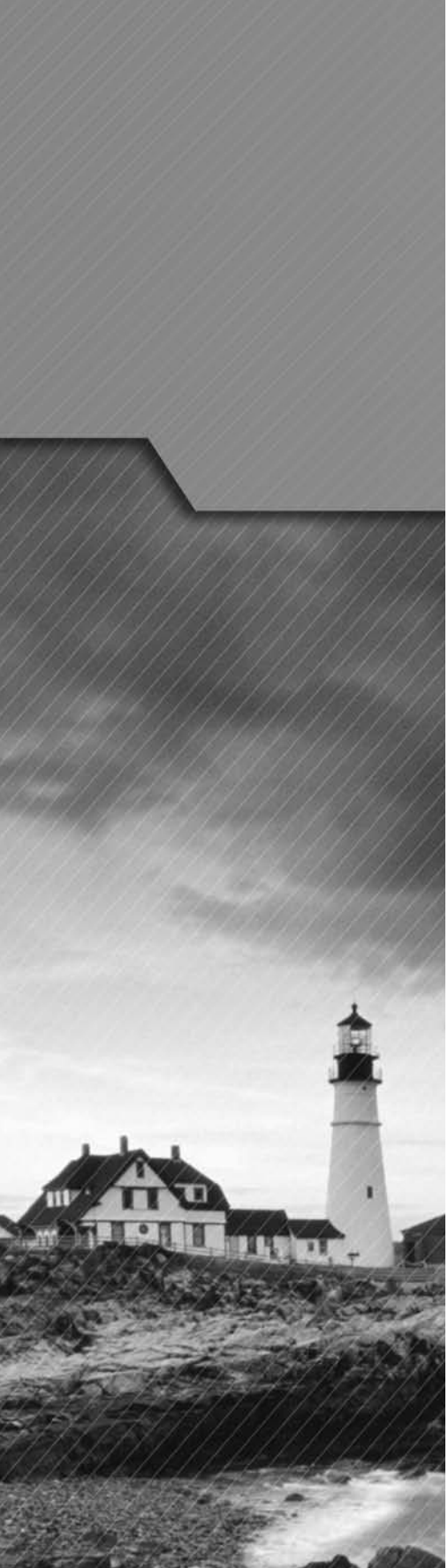
Operating Systems

COMPTIA A+ PRACTICAL APPLICATION EXAM OBJECTIVES COVERED IN THIS CHAPTER:

- ✓ **2.1 Select the appropriate commands and options to troubleshoot and resolve problems**
  - MSCONFIG
  - DIR
  - CHKDSK (/f /r)
  - EDIT
  - COPY (/a /v /y)
  - XCOPY
  - FORMAT
  - IPCONFIG (/all /release /renew)
  - PING (-t –l)
  - MD / CD / RD
  - NET
  - TRACERT
  - NSLOOKUP
  - [command name] /?
  - SFC
- ✓ **2.2 Differentiate between Windows Operating System directory structures (Windows 2000, XP and Vista)**
  - User file locations
  - System file locations
  - Fonts
  - Temporary files
  - Program files
  - Offline files and folders



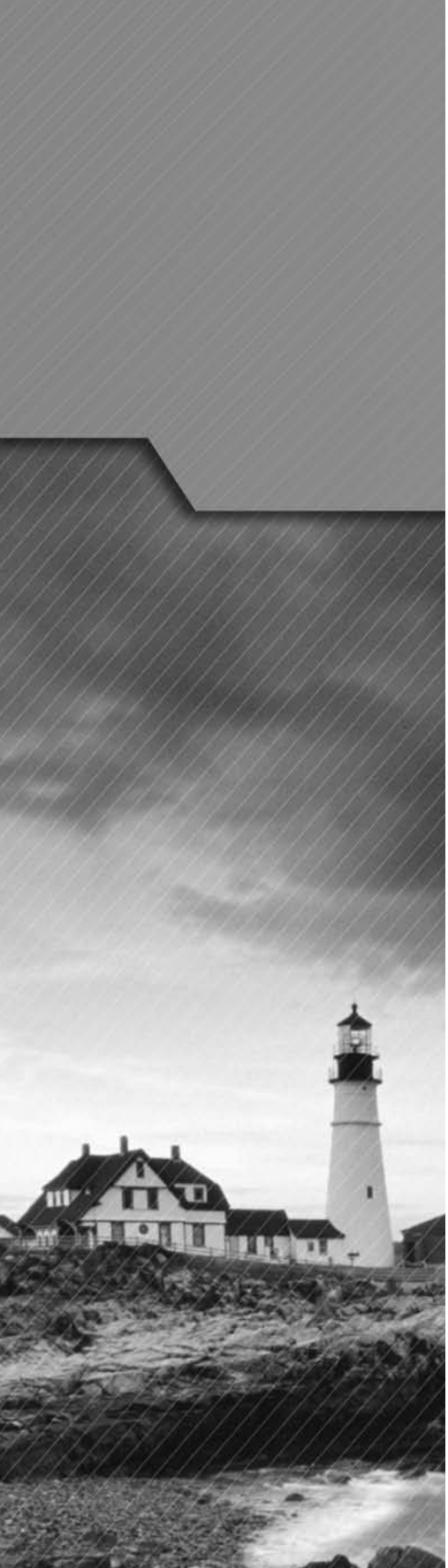
- ✓ **2.3 Given a scenario, select and use system utilities / tools and evaluate the results**
  - Disk management tools
    - DEFRAG
    - NTBACKUP
    - Check Disk
  - Disk Manager
    - Active, primary, extended and logical partitions
    - Mount points
    - Mounting a drive
    - FAT32 and NTFS
    - Drive status
      - Foreign drive
      - Healthy
      - Formatting
      - Active unallocated
      - Failed
      - Dynamic
      - Offline
      - Online
  - System monitor
  - Administrative tools
    - Event Viewer
    - Computer Management
    - Services
    - Performance Monitor
  - Devices Manager
    - Enable
    - Disable
    - Warnings
    - Indicators



- Task Manager
  - Process list
  - Resource usage
  - Process priority
  - Termination
- System Information
- System restore
- Remote Desktop Protocol (Remote Desktop / Remote Assistance)
- Task Scheduler
- Regional settings and language settings

✓ 2.4 Evaluate and resolve common issues

- Operational Problems
  - Windows specific printing problems
    - Print spool stalled
    - Incorrect / incompatible driver / form printing
  - Auto-restart errors
  - Bluescreen error
  - System lock-up
  - Devices drivers failure (input / output devices)
  - Application install, start or load failure
  - Service fails to start
- Error Messages and Conditions
  - Boot
    - Invalid boot disk
    - Inaccessible boot drive
    - Missing NTLDR
  - Startup
    - Device / service failed to start
    - Device / program in registry not found
  - Event viewer (errors in the event log)



- System Performance and Optimization
  - Aero settings
  - Indexing settings
  - UAC
  - Side bar settings
  - Startup file maintenance
  - Background processes

When it comes to the Operating Systems domain, there is something of a good news/bad news situation. The good news is that it is the second-highest weighted domain on the exam—with a weighting of 36 percent, it loses to Hardware by only 1 percent. The bad news is that it is fairly broad in its scope, requiring you to know the tools available in three different versions of Windows: Windows 2000, Windows XP, and Windows Vista.

Commands for Troubleshooting

This objective requires you to know how to work at the command line and run common command-line utilities available with the Windows-based operating systems. Some of the material here overlaps with that discussed in Chapter 3, but you'll want to make certain you know each utility discussed.

Critical Information

Although most of the information presented about Windows utilities and administration should seem like second nature to you (on-the-job experience is expected for A+ certification), you should read these sections thoroughly to make certain you can answer any questions that may appear about them.

The A+ exam's objective topic list expects you to know how to use certain specific commands at a prompt. The CMD utility is used to access a command window. In Windows 2000, XP, and Vista, this utility is used to display a command prompt. You can reach CMD by selecting Start ➢ All Programs ➢ Accessories ➢ Command Prompt.

In Windows 2000, *All Programs* is simply *Programs*.

Another way to reach this utility is to choose Start ➢ Run, type **CMD**, and click OK in Windows 2000 or Windows XP. CMD is a command (cmd.exe) which opens the command prompt window. In Windows Vista, choose Start and then type **CMD** in the Search box, press enter, and the interface will open, allowing you to execute command-line utilities. When you're finished in the command prompt and want to return to Windows, type **EXIT** and press Enter.

Here's a summary of the commands that can be run within this interface that you are expected to know for the exam:

CD This command serves two purposes. When typed at the command line without any parameters, CD (Current Directory) shows you the directory that you're currently in. When given a directory to change to, the CD (Change Directory) utility changes your current directory to the one given.

You can specify the directory you want to change to as either an absolute or a relative path. An absolute path gives the full path regardless of the directory you're currently in (for example, C:\Documents and Settings\All Users). A relative path tells the utility to change you to a location relative to where you currently are. For example, if you're in the C:\Documents and Settings directory, you can move to C:\Documents and Settings\All Users by giving the command

```
CD ALL USERS
```

With relative addressing, you can use two periods (..) to indicate the parent directory or one period (.) to indicate the present directory. For example, if you are in the directory C:\Novell\Messenger\LogFiles, then **CD ..** would move you to C:\Novell\Messenger; **CD .** would not move you to any other directory but would echo C:\Novell\Messenger\LogFiles.

CHKDSK This is a utility that has been around since the days of MS-DOS and is used to correct logical errors in FAT or NTFS volumes. The most common switches for the CHKDSK command are /F and /R, which fix/repair the errors they find. Without /F or /R, CHKDSK is an information-only command.

COPY This command copies files from one location to another. If the location for either the source or the destination isn't included in the command, it's assumed to be the current folder. Here are some examples:

COPY *.* D: This command copies all files from the current folder to the D: drive (an asterisk is a wildcard for any character or combination of characters.)

COPY C:\Windows\Myfile.txt This command copies Myfile.txt from C:\Windows to the current folder.

Three switches to know are /a, /v, and /y. The /a switch tells COPY that you are working with an ASCII text file; /v verifies that the written file matches the original; and /y is used to stop the prompts that normally appear asking you if you want to overwrite an existing file if one by that name already exists in the destination (essentially, it answers "yes" to each prompt for you).

DIR This command displays the contents of the current folder. You can use it by itself or with a file specification to narrow down the listing. Here are some examples:

DIR ????.* This command displays all files that are exactly four letters in name length, with any extension (a question mark is a wildcard for any one character.)

DIR /w This command displays the listing in wide (multicolumn) format, with names only (fewer details).

DIR /p This command displays the listing one screenful at a time. Press Enter to see the next screenful.

EDIT This command opens the Editor utility, a text editor similar to Notepad. You can add a filename to open that file (if it exists) or create a new file (if it doesn't exist). Here's an example:

EDIT CONFIG.SYS This command opens CONFIG.SYS if it's present in the current folder; otherwise it creates it and opens it.

The switches for EDIT are listed in Table 8.1.

TABLE 8.1 The EDIT Switches

Switch	Description
/B	Forces monochrome mode
/H	Displays the maximum number of lines possible for your hardware
/R	Loads the file(s) in read-only mode
/S	Forces the use of short filenames
/<*nnn*>	Loads binary file(s), wrapping lines to <*nnn*> characters wide
[*file*]	Specifies an initial file to load

FORMAT This command prepares media such as a hard disk (or a floppy, if you still can find them) for use by applying a certain filesystem to it. You can use the FORMAT command at a command prompt to format a disk. It's located in the C:\Windows\System32 folder, but it can be accessed from any prompt since this folder is in the default path.

The FORMAT command's switches are listed in Table 8.2.

TABLE 8.2 The FORMAT Switches

Switch	Description
/V[:*label*]	Specifies a volume label
/Q	Performs a quick format
/F:*size*	Specifies the formatted size for a floppy disk; omit for default
/B	Allocates space on the formatted disk for system files to be added later
/S	Copies system files to the formatted disk
/T:*tracks*	Specifies the number of tracks per disk side

TABLE 8.2 The FORMAT Switches *(continued)*

Switch	Description
/N:*sectors*	Specifies the number of sectors per track
/1	Formats a single side of a floppy disk
/4	Formats a 5¼″ 360KB floppy disk
/8	Formats eight sectors per track
/C	Tests clusters that are currently marked as bad

You can also access a Windows-based Format utility by right-clicking a drive icon in Windows and selecting Format.

HELP or /? This command can be used to give you the syntax and a short description of any command-line utility you want information on. You can obtain essentially the same information by following the command with /?. Because of this, the following two commands are identical:

```
HELP CD
```

and

```
CD /?
```

There are some situations where one command does not support both /? and Help and you must use one instead of the other. For example, Help Edit is not successful while Edit /? is.

IPCONFIG You can use IPCONFIG to view the current IP configuration for the client. This command can also be used with a number of switches to change the IP address settings. Here are some examples:

IPCONFIG /all This command shows all the information related to the network card(s), not just the summary information.

IPCONFIG /release This command releases the IP address leased from a DHCP server.

IPCONFIG /renew This command renews an IP address leased from a DHCP server.

IPCONFIG (with the /ALL parameter) also gives you full details on the duration of your current lease. You can verify whether a DHCP client has connectivity to a DHCP server by releasing the client's IP address and then attempting to lease an IP address.

This is one of the first tools to use when you're experiencing problems accessing resources, because it will show you whether an address has been issued to the machine. If the address displayed falls in the 169.254.x.x category, that means the client was unable to reach the DHCP server and has defaulted to Automatic Private IP Addressing (APIPA), which will prevent it from communicating outside its subnet, if not altogether.

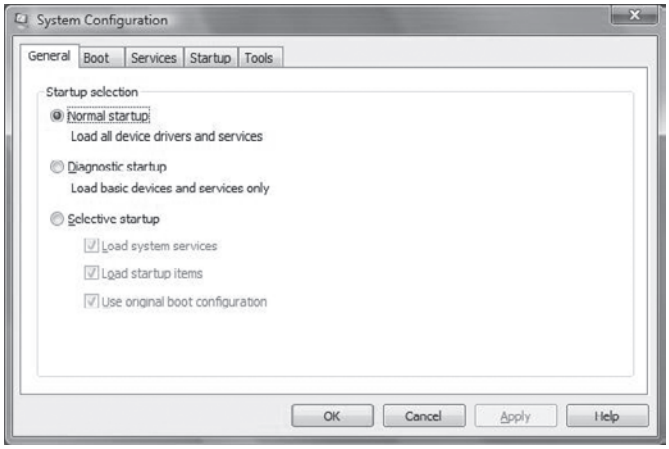
In the Linux world, a command similar to IPCONFIG is IFCONFIG.

MD MD (Make Directory) is used as the name implies. For example, MD BACKUP makes a new directory called BACKUP in the current directory.

In the Windows operating systems world, as opposed to Unix/Linux-based operating systems, commands are not case-sensitive, so MD and md work the same.

MSCONFIG (System Configuration Utility) The msconfig utility helps troubleshoot startup problems by allowing you to selectively disable individual items that normally are executed at startup. There is no menu command for this utility, so in Windows XP, for example, we use Start ➢ Run, type Msconfig, and press Enter. It works in most versions of Windows, although the interface window is slightly different among versions. Figure 8.1 shows an example in Windows Vista.

FIGURE 8.1 Msconfig in Windows Vista



NET Depending on the version of Windows you are using, NET can be one of the most powerful commands at your disposal. While all Windows versions include a NET command, the capabilities of it differ based on whether it is server- or workstation-based and the version of the operating system.

While always command-line-based, this tool allows you to do almost anything you want with the operating system.

Table 8.3 shows the features available and the syntax to use with most Windows versions.

TABLE 8.3 The NET Options

Purpose	Syntax
Set account options (password age, length, etc.)	`NET ACCOUNTS`
Add and delete computer accounts	`NET COMPUTER`
See network-related configuration	`NET CONFIG`
Control services	`NET CONTINUE`, `NET PAUSE`, `NET START`, `NET STATISTICS`, and `NET STOP`
Close open files	`NET FILE`
Create, delete, and change groups	`NET GROUP` and `NET LOCALGROUP`
See general help	`NET HELP`
See specific message help	`NET HELPMSG`
See the name of the current machine and user	`NET NAME`
Interact with print queues and print jobs	`NET PRINT`
Send a message to user(s)	`NET SEND`
See session statistics	`NET SESSION`
Create a share	`NET SHARE`
Set the time to that of another computer	`NET TIME`
Connect to a share	`NET USE`
Add, delete, and see information about a user	`NET USER`
See available resources	`NET VIEW`

These commands are invaluable troubleshooting aides when you cannot get the graphical interface to display properly. You can also use them when interacting with hidden (`$`) and administrative shares that do not appear in the graphical interface.

The `NET` command used with the `SHARE` parameter enables you to create shares from the command prompt, using this syntax:

```
NET SHARE <share_name>=<drive_letter>:<path>
```

To share the C:\EVAN directory as SALES, you would use the following command:

```
NET SHARE SALES=C:\EVAN
```

You can use other parameters with NET SHARE to set other options. Table 8.4 summarizes the most commonly used parameters.

TABLE 8.4 The NET SHARE Options

Parameter	Function
/DELETE	Stops sharing a folder
/REMARK	Adds a comment for browsers
/UNLIMITED	Sets the user limit to Maximum Allowed
/USERS	Sets a specific user limit

NSLOOKUP Nslookup is a command-line utility that enables you to verify entries on a DNS server. You can use NSLOOKUP in two modes: interactive and noninteractive. In interactive mode, you start a session with the DNS server, in which you can make several requests. In noninteractive mode, you specify a command that makes a single query of the DNS server. If you want to make another query, you must type another noninteractive command.

One of the key issues regarding the use of TCP/IP is the ability to resolve a hostname to an IP address—an action usually performed by a DNS server.

PING This command allows you to check a particular IP address or domain name on a network for reachability. For example, PING microsoft.com tells you whether Microsoft's website is up. PING is one of the most useful commands in the TCP/IP protocol. It sends a series of packets to another system, which in turn sends back a response. This utility can be extremely useful for troubleshooting problems with remote hosts.

Some sites will block PING traffic since some forms of attack—most notably denial of service (DoS) and distributed denial of service (DDoS)—use PING to harm the site.

The PING command indicates whether the host can be reached and how long it took for the host to send a return packet. On a LAN, the time is indicated as less than 10 milliseconds. Across WAN links, however, this value can be much greater.

You can use the -t switch to indicate PING should continue to ping the host without stopping until you break out of it (using Ctrl+C). You can also use the -l switch to specify a buffer size.

RD RD (Remove Directory) is used to delete a directory from the system from the command line. For example, RD C:\EDULANEY deletes the EDULANEY directory (assuming it's empty). You cannot delete a directory that has files in it without using the /S parameter.

SFC (System File Checker) The purpose of this utility is to keep the operating system alive and well. SFC automatically verifies system files after a reboot to see if they were changed to unprotected copies. If an unprotected file is found, it's overwritten by a stored copy of the system file from %systemroot%\system32\dllcache. (%systemroot% is the folder into which the operating system was installed.)

Storing system files (some of which can be quite large) in two locations consumes a large amount of disk space. When you install Windows 2000 Professional, make sure you leave ample hard drive space on the %systemroot% drive for growth. By default, the cache for these files is limited to approximately 300-400MB, but it can be changed by using the /CACHESIZE parameter discussed below.

Only users with the Administrator group permissions can run SFC. It also requires the use of a parameter. The valid parameters are shown in Table 8.5.

TABLE 8.5 The SFC Options

Parameter	Function
/CACHESIZE=	Sets the size of the file cache
/CANCEL	Stops all checks
/ENABLE	Returns to normal mode
/PURGECACHE	Clears the cache
/QUIET	Replaces files without prompting
/SCANBOOT	Checks system files on every boot
/SCANNOW	Checks system files now
/SCANONCE	Checks system files at the next boot

TRACERT Tracert is a command-line utility that enables you to verify the route to a remote host. Execute the command TRACERT hostname, where *hostname* is the computer name or IP address of the computer whose route you want to trace. TRACERT returns the different IP addresses the packet was routed through to reach the final destination. The results also include

the number of hops needed to reach the destination. If you execute the TRACERT command without any options, you see a help file that describes all the TRACERT switches.

The Tracert utility determines the intermediary steps involved in communicating with another IP host. It provides a road map of all the routing an IP packet takes to get from host A to host B.

As with the PING command, TRACERT returns the amount of time required for each routing hop.

XCOPY This command is like **COPY**, but it also duplicates any subfolders. For example, XCOPY C:\BOOKS D:\ copies everything from C:\BOOKS to the D: drive and also copies any subfolders and their contents.

There is a large number of commands to know as you prepare for the A+ exam, but the good news is that the names of most of these commands usually telegraph the function of the command. I strongly encourage you to work with each of them on a test system so that you will be familiar with them, and the switches that work with each, when you take the exam.

Exam Essentials

Know the main command-line utilities. Those discussed in this chapter include the ones CompTIA wants you to know for the exam. The commands include, in alphabetic order: /?, CD, CHKDSK, COPY, DIR, EDIT, FORMAT, IPCONFIG, MD, MSCONFIG, NET, NSLOOKUP, PING, RD, SFC, TRACERT, and XCOPY.

Know the switches for specified commands. CompTIA expects you to know the /a, /v, and /y switches for COPY; the /F and /R switches for CHKDSK; and the /all, /release, and /renew switches for IPCONFIG.

Windows Directory Structures

This objective expects you to know the directory structure employed in the three Windows-based operating systems that it tests on: Windows 2000, Windows XP, and Windows Vista. It expects you to know the directories in which key files can be found, and that is the focus of this discussion.

Critical Information

Windows versions have used a similar directory structure since Windows 95, and once you learn the basics of where key files are, you can generally feel comfortable no matter which of the newer operating systems you are using. For this objective, however, the focus is on six key topics:

- User file locations
- System file locations
- Fonts

- Temporary files
- Program files
- Offline files

Each of these will be discussed in the following sections.

User Files

In the Windows environment, beginning with Windows 2000, users are required to authenticate in some way (even if it is just as Guest) before gaining access to a user account. The operating system then uses a user profile to deliver the computer settings (theme, screen saver, and so on) that are configured for them. It is important to realize that the user account (which authenticates the user) and the user profile (which holds their settings) are two separate things—one is needed before the other.

Part of the user profile involves allowing each user to have a set of files that are specific to them. Figure 8.2, for example, shows the folders automatically created for the user edulaney. The same set of folders is automatically created for each user.

FIGURE 8.2 User folders created for the user edulaney

While the address bar simply shows the location as edulaney, in reality the folder being viewed is beneath `%systemdrive%\Users\` (usually `C:\Users\`) in Windows Vista and beneath `%systemdrive%\Documents and Settings\` (usually `C:\Documents and Settings\`) in Windows XP and Windows 2000.

When settings need to apply to everyone who uses the machine, they can be placed in All Users instead of being copied beneath each user's folder set.

System Files

Whereas user files are placed in folders specific to them, system files are those used by the operating system and are used by all users. In all the operating systems you need to know for the exam, these files are beneath `%systemroot%` and many, such as `System32`, appear in the default path. A number of files reside in this directory, with most residing in subdirectories.

Fonts

One of the subdirectories beneath `%systemroot%` is the `Fonts` folder. This folder holds the fonts that are available for viewing and printing. A font is a collection of characters, each of which has a similar appearance (for example, the Arial font). A font family is a group of fonts that have similar characteristics. `Fontmapper` is the routine within Windows that maps an application's request for a font with particular characteristics to the available font that best matches those characteristics.

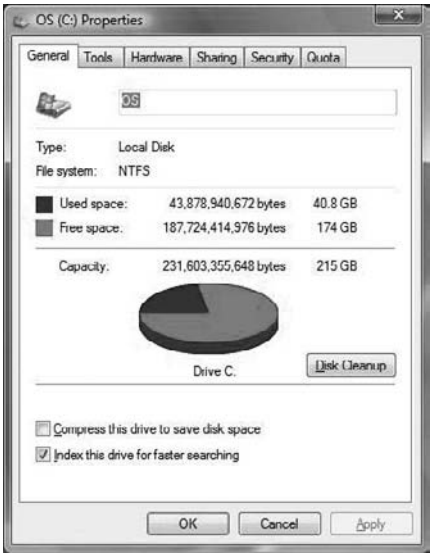
Temporary Files

Temporary files are written to a system on an almost nonstop basis. The purpose behind these files is to hold any information that is needed for only a short time. In addition to temporary files used for print queues, you also have cache from Internet sites and many other programs. You can manually pick files to delete, but one of the simplest solutions is to choose Properties for a drive and then click the General tab. A command button for the Disk Cleanup utility will appear, which you can use to delete most common temporary files, including the following:

- Downloaded program files
- Temporary Internet files
- Offline web pages
- Office setup files
- Recycle Bin contents
- Setup log files
- Temporary files
- Web client/publisher temporary files
- Temporary offline files
- Offline files
- Catalog files for the Content Indexer

Figure 8.3 shows the Disk Cleanup button in the Properties dialog box in Windows Vista.

FIGURE 8.3 The Disk Cleanup button in Windows Vista



Program Files

The `Program Files` directory, beneath `%systemdrive%` (usually `C:\`), holds the files needed for each of the installed applications on a machine. Windows Vista also added a `Program Data` directory, which is hidden by default. It contains the settings needed for applications and works similar to how the `Local Settings` folder did in previous operating systems.

Offline Files

Beginning with Windows 2000, the Windows-based operating systems added the capability to work with resources that are "online" (accessed through the network or other connection) and "offline" (replicated copies of the resource stored locally). The key is to keep the files in synchronization so that multiple versions of the same file stored in different locations match each other, as detailed in the following sections.

Windows 2000

In Windows 2000, the context menu for the resource offers a selection called Make Available Offline. The item you choose to make available offline can be a folder, a file, or even a mapped drive. When you select Make Available Offline, the Offline File Wizard starts, walking you through the steps of replicating this data locally. You can choose to do the synchronization between the copy and the original manually (in Explorer, choose File ➢ Synchronize) or automatically (you log on and log off). The last screen of the wizard offers two important check boxes:

- You can have reminders pop up regularly when you are working offline to tell you that you are not connected to the network. This is the default action.

- A shortcut can be added to the desktop for the offline material. By default, this option is not enabled; you reach the offline data the same way you would access the original data.

If the object you want to make available offline is a folder, a confirmation dialog box will ask whether you want to make available just the contents of the folder, or whether you want to make available all subfolders of the original folder as well. As the files are replicated to a local location, the synchronization dialog box shows results and errors (if there are any).

On a Windows 2000 Server, an administrator can choose to disable offline access of folders if he or she does not want to make them available for security reasons. Choosing to make a file noncacheable prevents it from being available for offline storage. By default, however, shared resources can be made available for offline access.

When you're working offline, an icon of a computer appears in the System Tray at the right end of the taskbar. Clicking the icon will show the status of the network—whether or not you are connected to it. When you become connected to the network again, you can also click that icon in the System Tray to synchronize changes you've made back to the network. Your laptop is not always able to dynamically realize when a connection to the network has been made (hot docking), so you might need to suspend (warm docking) or reboot (cold docking) before the connection is truly established.

If you reboot the system at a time when changes to the offline folders do not correspond with what is online, the icon in the System Tray will have a flashing exclamation mark on it. Click the icon to open the dialog box.

During the synchronization process, a Setup button appears at the bottom right of the box. Clicking this button takes you to Synchronization Manager. Synchronization Manager offers three tabs and is worth examining for its options:

Logon/Logoff Allows you to configure whether synchronization should occur when you log on and/or log off, or whether you should always be prompted before you take any action. This can be configured independently for LAN connections, dial-up connections, VPNs, and so on. It can also be configured for web pages as well as folders.

On Idle Allows you to configure the items to be updated when the system is idle.

Scheduled Allows you to define synchronization jobs. Clicking the Add button brings up the Scheduled Synchronization Wizard, which you can use to schedule jobs to run every day, every week, or at some other interval.

Finally, by clicking the Settings button at the bottom of the Synchronization Manager window, you can access more options. Here, you can configure when the reminders will appear and the amount of local disk space that can be used to store offline folders. The Advanced button allows you to configure the computer so that it can never be used offline (or deviations thereof).

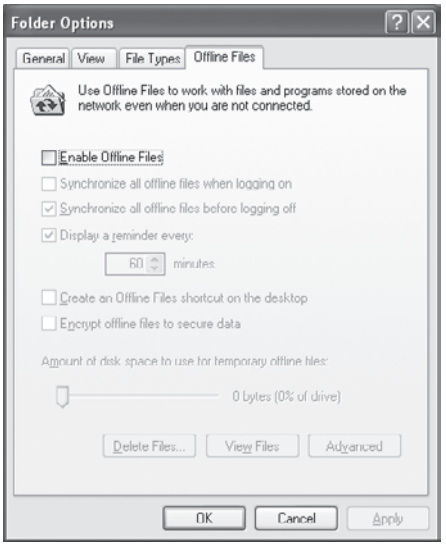
Finally, keep in mind that the offline files and folders consume hard drive space, so you need to allot for this appropriately. All offline content is stored beneath the `%systemroot%` directory in subdirectories of a hidden system folder named `CSC`.

Windows XP

Offline files are accessible in Windows XP in an almost identical fashion to the way they were in Windows 2000. Before you can use this feature, though, you must turn it on. To do so, open My Computer and then choose Folder Options from the Tools menu. When the Properties dialog box appears, click the Offline Files tab and check the Enable Offline Files option, as shown in Figure 8.4.

You cannot enable offline files if Fast User Switching is enabled.

FIGURE 8.4 Offline Files must be enabled before the feature can be used.



Once you check this box, the other options become available. Select the amount of disk space you want to allow to be used for temporary storage of offline files (10% is the default), whether you want to encrypt the files, and so on. Then click OK. Once you have done this, you can click on a network resource, and then choose Make Available Offline from the File menu or from the context menu that appears when you right-click on the file or folder.

You can view the files that are stored offline by opening My Computer and then choosing Folder Options from the Tools menu. When the Properties dialog box appears, click the Offline Folders tab and click the View Files button. Synchronization is accomplished through the use of Synchronization Manager (which you access by choosing Tools ➢ Synchronize in any Explorer window or by typing **mobsync** in the Run box). Figure 8.5 shows the Synchronization Manager interface.

FIGURE 8.5 Click Setup in Synchronization Manager to configure when synchronization should occur.

To disable offline file storage, repeat the process used to set it up, and uncheck the Enable Offline Files option.

Windows Vista

Windows Vista did not change what was already in place with the other operating systems; it just modified some things. The two biggest modifications are the inclusion of the Sync Center and the restriction of offline file support to the Business, Enterprise, and Ultimate versions. If you do not have one of these versions, you will not have the ability to access the Offline Files tab or do any configuration.

All versions of Vista have the Sync Center, shown in Figure 8.6. Access it by choosing Start ➢ Control Panel ➢ Network and Internet.

Sync partnerships can be set up with a large number of devices, ranging from a flash drive (as shown in Figure 8.7) to handheld devices. It is worth noting again that you cannot sync with network folders if you are using Windows Vista Starter, Home Basic, or Home Premium editions.

Exam Essentials

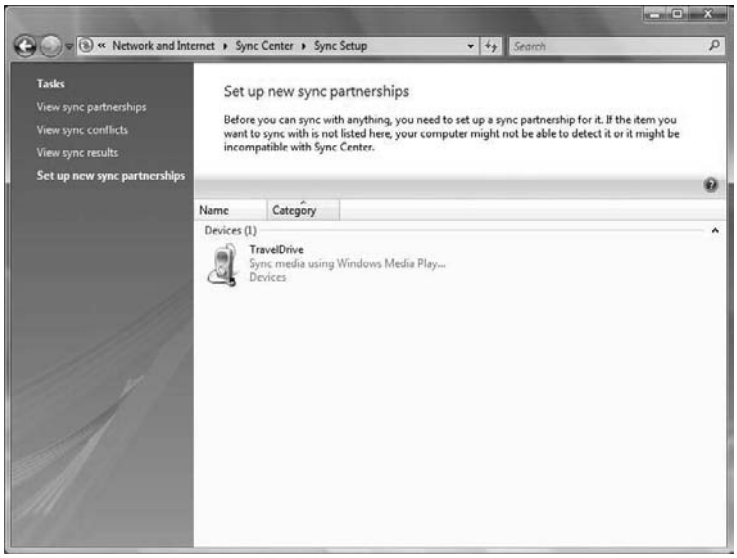
Know the locations of key files. The key files discussed in this chapter include the ones CompTIA wants you to know for the exam. For this objective, the focus is on six key topics: user file locations, system file locations, fonts, temporary files, program files, and offline files and folders.

Know the disk/directory structure. You should be able to create folders from within Windows as well as from the command line. You should also be able to create files and copy them from one location to another.

Know which operating systems can use offline file storage for network drives. This functionality, which existed in previous versions, was reduced in Windows Vista and limited to working with only the Business version and higher.

FIGURE 8.6 The Sync Center in Windows Vista is the primary interface for configuring synchronization.

FIGURE 8.7 Establish a partnership with the device you want to sync with in Sync Center.



System Utilities and Tools

The basic unit of storage is the disk. Disks are partitioned (primary, logical, extended) and then formatted for use. With the Windows operating systems this exam focuses on, you can choose to use either FAT32 or NTFS. The advantage of NTFS is that it offers security and many other features that FAT32 can't handle.

If you're using FAT32 and want to change to NTFS, the convert utility will allow you to do so. For example, to change the E: drive to NTFS, the command is `convert e: /FS:NTFS`.

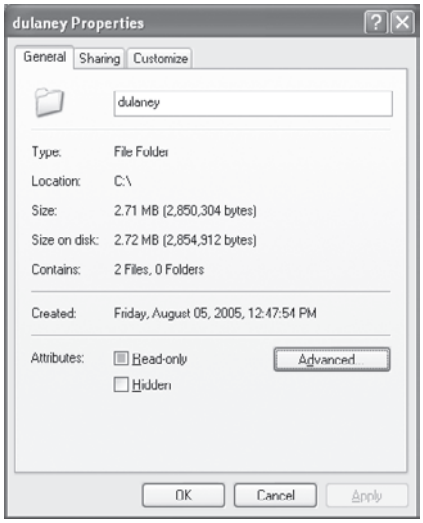
Critical Information

Once a disk is formatted, the unit is the directory structure, in which you divide the partition into logical locations for storing data. Whether these storage units are called directories or folders is a matter of semantics—I tend to call them *folders* when viewing them in the graphical user interface (GUI) and *directories* when viewing them from the command line.

You can create directories from the command line using the `MD` command and from within the GUI by right-clicking in a Windows Explorer window and choosing New ➤ Folder. Once the folder exists, you can view/change its properties, as shown in Figure 8.8, by right-clicking the icon of its folder and choosing Properties.

In the Attributes section, you can choose to make the directory read-only or hidden. By clicking the Advanced button, you can configure indexing, archiving, encryption, and compression settings.

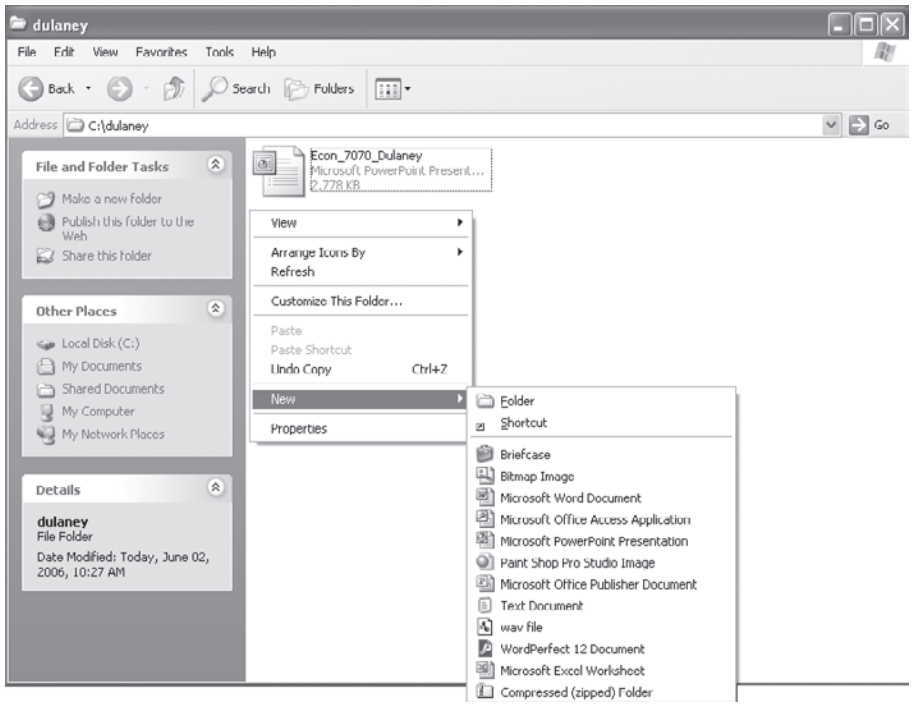
FIGURE 8.8 Change the attributes associated with a directory.



Even though encryption and compression settings appear in the same frame on the dialog box, the two features are mutually exclusive.

The units directories hold are files. You can create a file either from within an application or by right-clicking, choosing New, and then selecting the type of item you want to create, as shown in Figure 8.9.

FIGURE 8.9 You can create files of various types with a right-click.



Once the file has been created, you can right-click the file's icon and change properties and permissions associated with the file by choosing Properties from the context menu.

The following sections will discuss the disk-management tools, Disk Manager and drive basics, System Monitor, administrative tools, Device Manager, Task Manager, System Information, System Restore, Remote Desktop, Task Scheduler, and Regional Settings.

Disk-Management Tools

The disk-management tools that fall in this section are the primary tools used on a regular basis. Most of them relate to data and drives, but that isn't true of all of them. The commands that CompTIA wants you to know are `CHKDSK` (discussed in the first section of this chapter) and two others, discussed in the following sections.

You can start CHKDSK by right-clicking on a drive and choosing Tools from the Properties menu. On the Tools tab, click the Check Now button to check the disk for errors.

DEFRAG

One of the biggest factors affecting hard drive performance over time is fragmentation. The more files are read, added to, and rewritten, the more fragmentation is likely to occur. The Disk Defragmenter utility (DEFRAG) is the best tool for correcting fragmentation.

Disk Defragmenter reorganizes the file storage on a disk to reduce the number of files that are stored noncontiguously. This makes file retrieval faster, because the read/write heads on the disk have to move less.

There are two versions of Disk Defragmenter: a command-line version, and a Windows version that runs from within Windows. The Windows version is located on the System Tools submenu on the Start menu (Start ➢ All Programs ➢ Accessories ➢ System Tools ➢ Disk Defragmenter).

The available switches for the command-line version (`defrag.exe`) include the following:

`-a` Analyze only

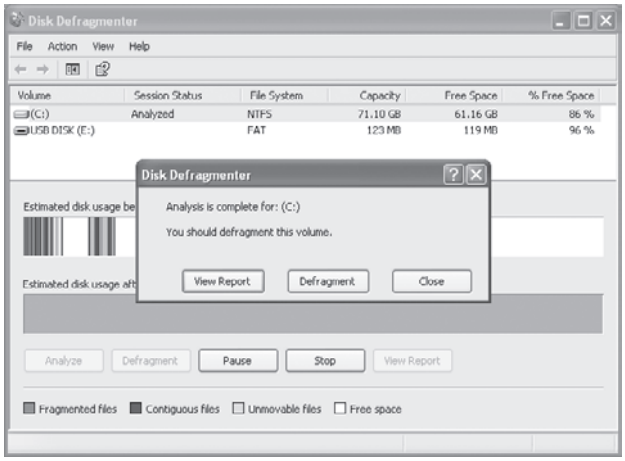
`-f` Force defragmentation even if disk space is low

`-v` Verbose output

You access the tool in Windows XP from Start ➢ All Programs ➢ Accessories ➢ System Tools ➢ Disk Defragmenter. Before doing any operation, you should run Analyze. This will check the volume and recommend an action, as shown in Figure 8.10.

If you choose View Report, you can see the files that are most fragmented in successive order.

FIGURE 8.10 Disk Defragmenter will recommend needed action in Windows XP.



NTBACKUP

With Windows 2000 and XP, you can access the NTBackup utility from the System Tools menu, or from the Tools tab in a hard disk's Properties box. Its purpose is to back up files in a compressed format, so the backups take up less space than the original files would if they were copied. To restore the backup, you must use the same utility again, but in Restore mode. The best insurance policy you have against devastating loss when a failure occurs is a backup of the data that you can turn to when the system is rebuilt. Windows Vista does not include the NTBackup utility with the distribution, but there are plenty of web sites which discuss how to copy it over from previous installations.

When you start the program, by default it begins the Backup Or Restore Wizard (you can disable this default action by deselecting Always Start In Wizard Mode in the first dialog). The wizard will walk you through any backup/restore operation you want to do, or you can click Advanced Mode to get to the interface.

Five backup type choices are available:

Normal A full backup of all files, regardless of the state of the archive bit for each file (the default). After the files are backed up, the archive bit is turned off.

Copy A full backup of all files, regardless of the state of the archive bit. The archive bit is left in its current state.

Incremental Backs up only files for which the archive bit is currently turned on. After the files are backed up, the archive bit is turned off.

Differential Backs up only files for which the archive bit is currently turned on. The archive bit is left in its current state.

Daily Backs up only those files with today's date, regardless of archive bit status. The archive bit is left in its current state.

If you type ntbackup in the command prompt dialog box without using an option, it starts the Backup or Restore Wizard. You can also perform backups from the command line by using the `ntbackup.exe` executable. You can't restore files from the command line with this utility, however. Options include the following:

`/A` Performs an append (adds the new backup to the end of the existing one).

`/F` Identifies the disk path and filename.

`/HC:{on|off}` Toggles hardware compression on or off.

`/J` Signifies the job name.

`/M` Must be followed by a backup type name: `copy`, `daily`, `differential`, `incremental`, or `normal`.

`/N` Signifies a new tape name; can't be used in conjunction with /A.

`/P` Signifies the media pool name.

`/T` Followed by the tape name, this specifies which tape to overwrite or append to.

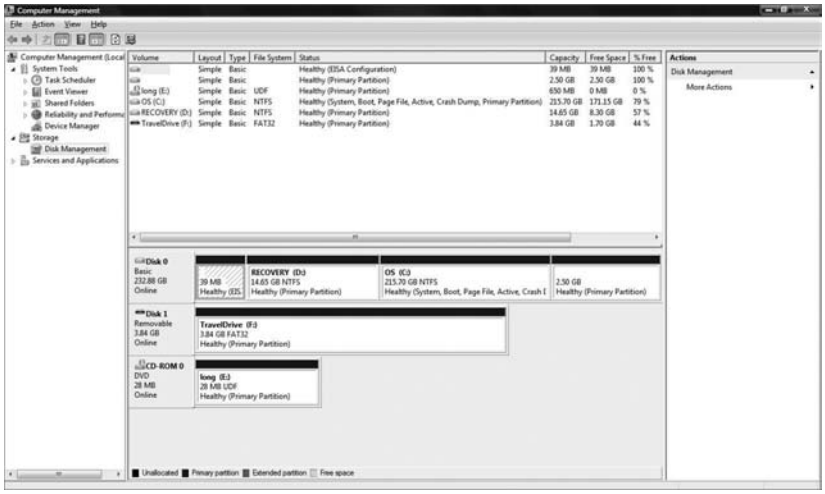
`/V:{yes|no}` Toggles whether to do verification after the completion of the backup.

The Backup utility in each of the different versions of Windows has different capabilities, with newer versions having greater capabilities. In general, you can either run a wizard to create a backup job or manually specify the files to back up, but the objectives specifically ask that you know the NTBACKUP options listed here. In the real world, you can also run backup jobs or schedule them to run at specific time at a specific interval. Refer to the Windows Help system for in-depth information on how to use Backup.

Disk Manager and Drive Basics

The Disk Manager, more commonly known as Disk Management, allows you to perform such actions as resizing a drive or changing the drive letter. To access this tool, click the Start button and then right-click on Computer (or My Computer). From the context menu, choose Manage, then click Disk Management. This snap-in is shown in Figure 8.11.

FIGURE 8.11 You can configure the drives with Disk Management.



While this tool existed in previous versions of Windows, Vista added the ability to extend, shrink, or delete a volume.

As you use this tool, and all tools associated with disks, you must understand the difference in partition types:

- An active partition is the one that is bootable—the one that the operating system is installed on. In Figure 8.11, you can see that this is the C: drive.
- A primary partition is one that is used by the operating system—it may or may not be bootable. In Figure 8.11, C:, D:. E:, and F: all hold primary partitions.
- An extended partition is used to hold files and is secondary to the primary. There can be only one extended partition on a hard drive, but it can be further divided into logical drives. To put it in context, remember that primary partitions cannot be subdivided, but extended ones can. Equally important, only primary partitions may be designated Active.

In addition to the tool discussed here, for the objectives given, you should know about logical partitions, mount points, how to mount a drive, FAT32 and NTFS, and drive status. All these topics are discussed in Chapter 3. The section that follows looks at System Monitor, a useful tool for finding out the status of your system.

System Monitor

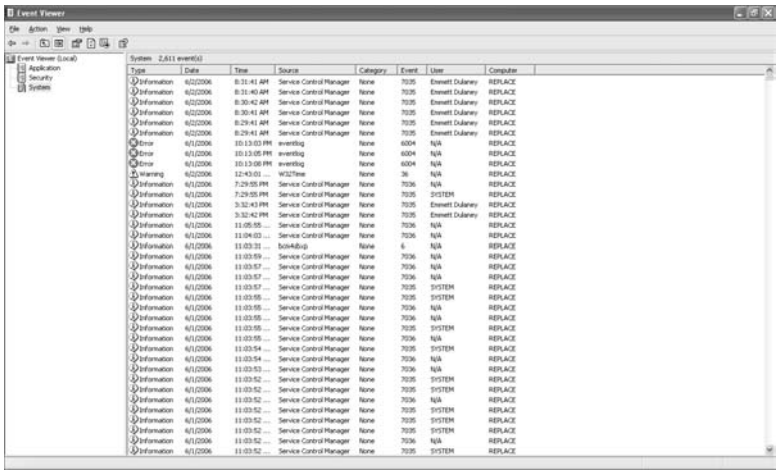
The Performance tool in Windows XP/2000 is divided into two sections: System Monitor and Performance Logs And Alerts. System Monitor allows you to gather real-time statistics about what the system is doing right now in chart format (the default), histogram format (similar to a bar chart), or report format. Performance Logs And Alerts let you record data to create and compare with a baseline (to get a long-term look at how the system is operating) or to send administrative alerts when thresholds are reached. There is no System Monitor or Performance Logs And Alerts in Vista. Instead, Vista has the Reliability and Performance Monitor. This offers two tools beneath it which accomplish similar tasks to what the Performance tool offered in the previous operating systems: Performance Monitor and Reliability Monitor.

Administrative Tools

The four administrative tools CompTIA lumps beneath this section are Event Viewer, Computer Management, Services, and Performance Monitor. We've discussed some of these earlier but they are worth a quick visit.

Event Viewer This utility provides information about what's been going on system-wise, to help you troubleshoot problems. Event Viewer displays warnings, error messages, and records of things happening successfully. It's found in only NT-based versions of Windows (which includes Windows 2000, Windows XP, and Windows Vista). You can access it through Computer Management, or you can access it directly from Administrative Tools in Control Panel. Figure 8.12 shows Event Viewer in Windows XP.

FIGURE 8.12 Event Viewer in Windows XP



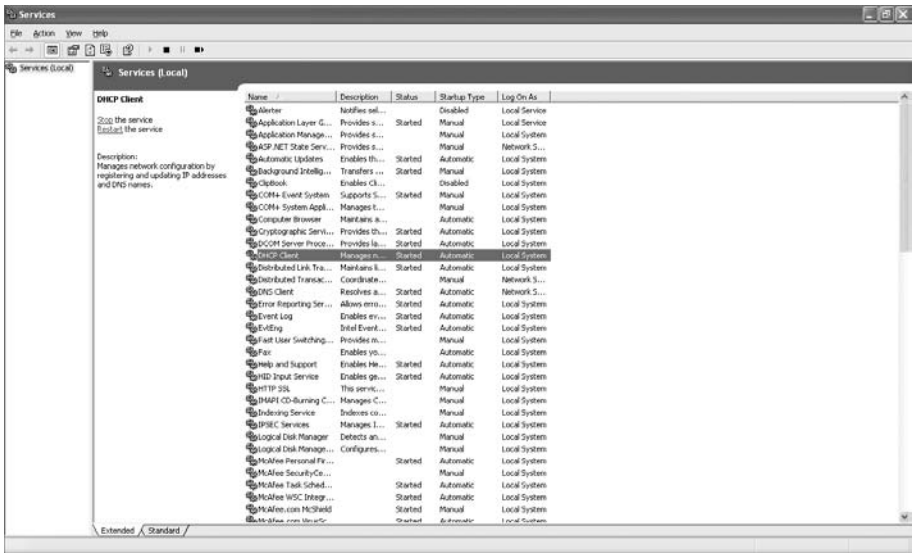
Computer Management Computer Management is the shell that such tools as Disk Management plug in to; it is a predefined Microsoft Management Console (MMC). It provides a common interface that allows you to perform all the actions that can be done separately within one location. To access the Computer Management Console in Windows 2000, choose Start ➢ Settings ➢ Control Panel ➢ Administrative Tools ➢ Computer Management. In Windows XP/Vista, you can access Control Panel through the Start button directly. In both operating systems, you can also access Computer Management by right-clicking the My Computer icon and choosing Manage.

Computer Management also has the Storage area, which lets you manage removable media, defragment your hard drives, or manage partitions through the Disk Management utility. Finally, you can manage system services and applications through Computer Management as well.

Services The more operations your system is trying to perform, the more it must juggle between operations. For this reason—not to mention security—you should limit the services running on a system to only those that you want. Unfortunately, many services are often installed by default, and you have to remove or disable them.

To interact with services, access the Administrative Tools section of Control Panel and choose Services. This starts up the console shown in Figure 8.13. You can right-click any service and choose to start, stop, pause, resume, or restart it. You can also double-click it to access its properties and configure such things as the startup type, dependencies, and other variables.

FIGURE 8.13 Working with services in Windows XP



Performance Monitor The Performance tool in Windows XP/2000 is divided into two sections: System Monitor and Performance Logs And Alerts. As mentioned earlier, System Monitor allows you to gather real-time statistics about what the system is doing right now. Performance Logs And Alerts let you record data to create and compare with a baseline (to get a long-term look at how the system is operating) or send administrative alerts when thresholds are reached. You can use this tool to identify problems with objects. If you want to watch memory, for example, the object to monitor is Memory, and the counters to watch include the following:

Committed Bytes This counter shows how much memory (virtual and physical) is in use. If this number always exceeds the physical RAM by more than a few megabytes, you probably don't have sufficient RAM. As the counter's value increases, the system will have to page memory in and out more frequently to keep the running programs in memory.

Pages/Sec This counter indicates how many pages per second are being moved to and from memory to satisfy requests. This number should be less than 100; a higher value can indicate that the system is RAM starved. The counter won't drop to 0 even on a system that has plenty of RAM because some activity must always occur.

You can also gather memory statistics by using Task Manager. The Performance tab shows current utilization and a graph of recent history. A bar-graph icon appears in the System Tray when Task Manager is running. This is an active link to the CPU Usage graph on the Performance tab and can be used to visually gauge CPU activity even when Task Manager is minimized.

Device Manager

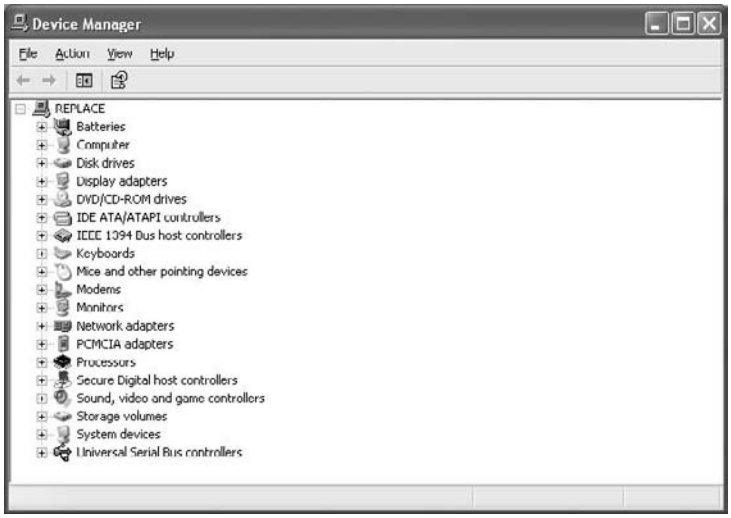
Device Manager shows a list of all installed hardware and lets you add items, remove items, update drivers, and more. This is a Windows-only utility. In Windows 2000/XP, you display the System Properties, click the Hardware tab, and then click the Device Manager button to display it. In Windows Vista, you can reach this tool by choosing Start ➢ Control Panel, then selecting System And Maintenance, System, and Device Manager. Or you can click the Start button, right-click on Computer (or My Computer), choose Manage from the context menu, and then click Device Manager. Figure 8.14 shows Device Manager in Windows XP.

Common choices for devices within Device Manager include Enable and Disable, which allow you to toggle the state of the device. You can also quickly scan the list of devices and see those that are having difficulties (whether only warnings or serious issues) by looking at the icon associated with them. A black exclamation mark in yellow means that the device is in a problem state (but can still be functioning). A red X means the device is disabled. A blue "i" in white means that the device does not automatically.

Task Manager

Task Manager shows running programs and the system resources they're consuming. It can be used for informational purposes, but it's most often used to shut down a nonresponsive application.

FIGURE 8.14 Device Manager in Windows XP



There are three common ways to display the Task Manager. The first is to press Ctrl+Alt+Delete and click the Task Manager button (if required). The second is to right-click in an empty location on the Taskbar and choose Task Manager from the context menu. The third method is to hold down Ctrl+Shift and press Esc.

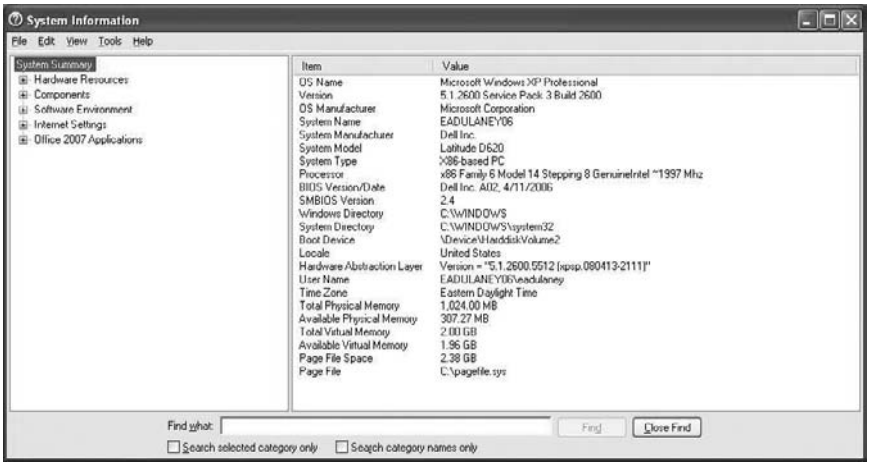
When Task Manager starts, you'll see five tabs. A list of running tasks appears under the Applications tab; you can click one of them and then click End Task to shut it down. Because this shutdown method fails to close files gracefully, you should use it only as a last resort, not as a normal method of shutting down an application. You can also choose the Processes tab to see all processes—not just applications—running, or choose Performance to see CPU, paging, memory, and other parameters. By right-clicking on a running process on the Processes tab, you can choose to change the priority for it. The choices are Realtime (which I strongly suggest you avoid using), High, AboveNormal, Normal, BelowNormal, and Low.

The Networking tab shows usage for all found connections, and the Users tab shows the current users and lets you disconnect them, log them off, or send them a message.

System Information

You can start the System Information tool by running `MSINFO32.EXE` from a command prompt. Not nearly as powerful as Device Manager, System Information is divided into System Summary and by default also includes Hardware Resources, Components, Software Environment, and Internet Settings. It can be further subdivided as needed. Another common division is Office Settings, as shown in Figure 8.15.

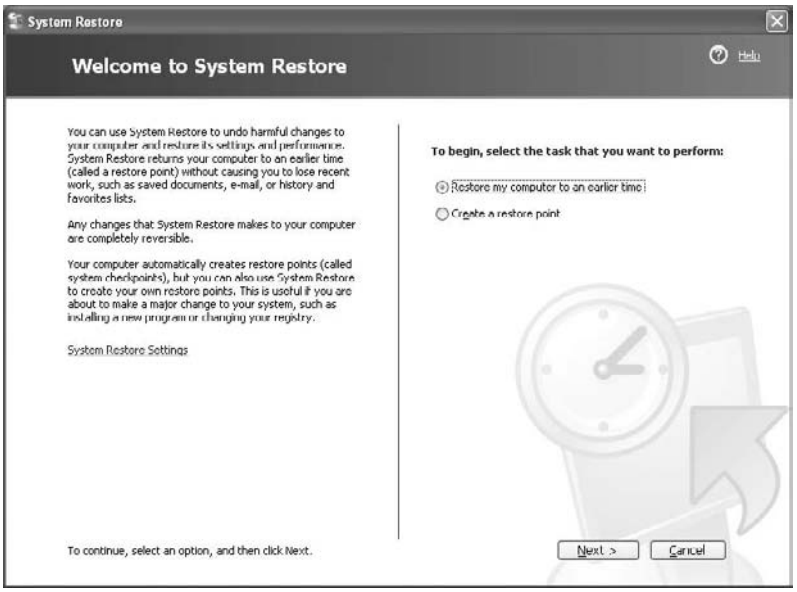
FIGURE 8.15 System Information in Windows XP



System Restore

System Restore is arguably the most powerful tool in Windows XP/Vista. It allows you to restore the system to a previous point in time. You can access it from Start ➤ All Programs ➤ Accessories ➤ System Tools ➤ System Restore and use it to roll back to, as well as create, a restore point, as shown in Figure 8.16.

FIGURE 8.16 Create a restore point or return to one with System Restore.



In addition to letting you manually create a restore point, Windows XP creates a restore point automatically every 24 hours, as well as when you install unsigned device drivers or install (or uninstall) a program with Windows Installer or InstallShield. By default, restore points are kept for 90 days and then deleted in order to conserve space.

You must be a member of Computer Administrators to run System Restore.

Remote Desktop

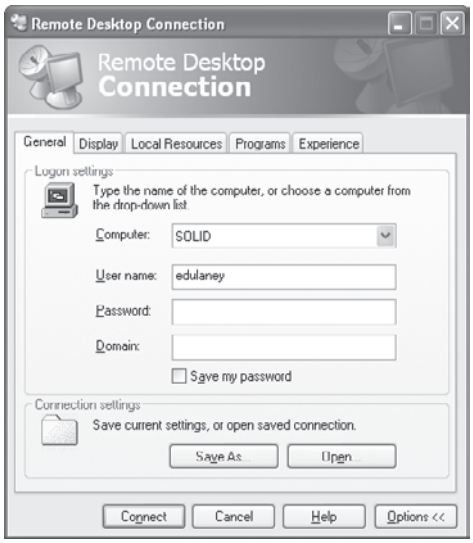
The Remote Desktop feature of Windows XP and Vista allows you to remotely connect to your workstation and use it for a variety of purposes—work from home, teach a user how to do a task, and so on. This utilizes the Remote Desktop Protocol (RDP), and two elements are involved:

- Turning on the ability to access remotely
- Accessing remotely

To accomplish the first, access the System Properties, click the Remote tab, and select the Allow Users To Connect Remotely To This Computer Under Remote Desktop check box. Click Apply, and then click OK to exit.

To access the computer from another XP workstation, select Start ➢ All Programs ➢ Accessories ➢ Communications, and choose Remote Desktop Connection. If you click the Options button, you'll see choices similar to those in Figure 8.17.

FIGURE 8.17 The Remote Desktop Connection dialog box in Windows XP



One of the simplest ways to connect is to enter the IP address of the host. Once you give a valid username and password, you're connected to the host and able to work remotely.

In addition to Remote Desktop, XP and Vista include Remote Assistance. The Remote tab in Windows XP/Vista lets you enable or disable Remote Assistance. Remote Assistance allows the local workstation to be used from a remote computer. This can help an administrator or other support person troubleshoot problems with the machine from a remote location. The local user must invite the remote technician to connect for this to work and the local user can terminate the session at any time (that's how it differs from Remote Desktop).

Remote Assistance is enabled by default. It is handled at two levels. Just having Remote Assistance turned on allows the person connecting to view only the computer's screen. To let that person take over the computer and be able to control the keyboard and mouse, click Advanced and then, in the Remote Control section, click Allow This Computer To Be Controlled Remotely.

Task Scheduler

Task Scheduler allows you to configure jobs to automatically run unattended. To create a new unattended job, follow these steps:

1. Select Start ➢ Programs (or All Programs) ➢ Accessories ➢ System Tools, and choose Scheduled Tasks.
2. Double-click on the Add Scheduled Task icon. The Scheduled Task Wizard appears to walk you through the setup.
3. The first screen informs you of its purpose and offers no options. Click the Next button to continue.
4. A list of applications appears. From the list, choose the application you want to run, or click the Browse button to look elsewhere.
5. Specify how often the program is to run, and provide the name that you want to call the job—this can be the same name as the program, or something completely different. For the run frequency, you can choose any of the following options:
   - Daily
   - Weekly
   - Monthly
   - One time only
   - When the computer starts
   - When you log on
6. After choosing the frequency, you must specify parameters related to it.
7. Because the job will be running in unattended mode, you must provide the name and password of a user who has authorization to run this job. If you cannot provide proper authorization, the job will not run when scheduled.
8. A verification screen shows what you have configured. Click Finish to complete the task. Alternatively, you can click a check box to go to the advanced properties of the task.

You can access a job's advanced properties anytime after the job has been created. To do so, double-click the icon for the job in the Scheduled Tasks screen. In the resulting dialog box, you can configure such things as the properties listed here:

- The username and password associated with the job
- The actual command line used to start the job (in case you need to add parameters to it) and the working directory
- The schedule—and even multiple schedules (for example, in case you don't run the job the last two weeks of the month while the plant is shut down, but you run it extra at tax time)
- Completion, idle time, and power feature parameters

At any time, you can delete a scheduled job by deleting its icon, or you can simply disable a job by removing the check mark from the Enabled box on the Task tab of the task's properties. For jobs that are scheduled to run, a picture of a clock appears in the bottom-left corner of the icon; jobs not scheduled to run do not have that clock.

Regional Settings

The Regional Settings dialog box allows you to customize the user location and keyboard layout.

Exam Essentials

Know the main administrative tools. You should know the primary graphical tools for troubleshooting Windows and working with the operating system. These include the disk-management tools, Disk Manager and drive basics, System Monitor, administrative tools, Device Manager, Task Manager, System Information, System Restore, Remote Desktop, Task Scheduler, and Regional Settings.

Diagnostics and Troubleshooting

There is a great deal of overlap between what is in this objective and what has come before. The primary topics beneath this objective involve recovering operating systems, resolving common operational problems, looking at error messages, and using diagnostic tools. Each of these topics is examined in this section.

Critical Information

As an administrator, you must be able to do all the functions this exam focuses on. But none will make you shine in the eyes of users as much as the ability to get systems back up and running after problems have occurred. The topics beneath this objective focus on that part of the job and your skill set.

Startup

The programs to begin at startup can be configured through the msconfig utility (discussed earlier in this chapter) as well as by right-clicking the Start button, choosing Open, and then selecting Programs And Startup. Those that appear here are few, whereas a much greater number appear in msconfig, because it can access other locations.

Recovering Operating Systems

Windows includes a number of tools to simplify recovering an operating system after a serious problem has occurred. System Restore is one such tool, as discussed previously. Three others we'll look at here are the Recovery Console, Automated System Recovery (ASR), and emergency repair disks (ERDs).

Recovery Console

The Recovery Console, which is not available in Windows Vista, is a command-line utility used for troubleshooting. From it, you can format drives, stop and start services, and interact with files. The latter is extremely important because many boot/command-line utilities bring you into a position where you can interact with files stored on FAT or FAT32, but not NTFS. The Recovery Console can work with files stored on all three file systems.

The Recovery Console isn't installed on a system by default. To install it, use the following steps:

1. Place the Windows CD in the system.
2. From a command prompt, change to the `i386` directory of the CD.
3. Type **winnt32 /cmdcons**.
4. A prompt appears, alerting you to the fact that 7MB of hard drive space is required and asking if you want to continue. Click Yes.

Upon successful completion of the installation, the Recovery Console (Microsoft Windows 2000 Recovery Console, for example) is added as a menu choice at the bottom of the Startup menu. To access it, you must choose it from the list at startup. If more than one installation of Windows 2000 or Windows NT exists on the system, another boot menu will appear, asking which you want to boot into, and you must make a selection to continue.

To perform this task, you must give the administrator password. You'll then arrive at a command prompt. You can give a number of commands from this prompt, two of which are worth special attention: `EXIT` restarts the computer, and `HELP` lists the commands you can give. Table 8.6 lists the other commands available, most of which will be familiar to administrators who have worked with MS-DOS.

TABLE 8.6 Recovery Console Commands

Command	Purpose
`ATTRIB`	Shows the current attributes of a file or folder, and lets you change them.
`BATCH`	Runs the commands within an ASCII text file.

TABLE 8.6 Recovery Console Commands *(continued)*

Command	Purpose
CD	Used without parameters, it shows the current directory. Used with parameters, it changes to the directory specified.
CHDIR	Works the same as CD.
CHKDSK	Checks the disk for errors.
CLS	Clears the screen.
COPY	Allows you to copy a file (or files, if used with wildcards) from one location to another.
DEL	Deletes a file.
DELTREE	Recursively deletes files and directories.
DIR	Shows the contents of the current directory.
DISABLE	Allows you to stop a service/driver.
DISKPART	Shows the partitions on the drive, and lets you manage them.
EXPAND	Extracts compressed files.
ENABLE	Allows you to start a service/driver.
FIXBOOT	Writes a new boot sector.
FIXMBR	Checks and fixes (if possible) the master boot record.
FORMAT	Allows you to format a floppy or partition.
LISTSVC	Shows the services/drivers on the system.
LOGON	Lets you log on to Windows 2000.
MAP	Shows the maps currently created.
MD	Makes a new folder/directory.
MKDIR	Works the same as MD.
MORE	Shows only one screen of a text file at a time.

TABLE 8.6 Recovery Console Commands *(continued)*

Command	Purpose
RD	Removes a directory or folder.
REN	Renames a file or folder.
RENAME	Works the same as REN.
RMDIR	Works the same as RD.
SYSTEMROOT	Works like CD but takes you to the system root of whichever OS installation you're logged on to.
TYPE	Displays the contents of an ASCII text file.

During the installation of the Recovery Console, a folder named `Cmdcons` is created in the root directory to hold the executable files and drivers it needs. A file named `Cmldr`, with attributes of System, Hidden, and Read-Only, is also placed in the root directory.

If you want to delete the Recovery Console (to prevent users from playing around, for example), you can do so by deleting the `Cmldr` file and the `Cmdcons` folder, and removing the entry from the `Boot.ini` file.

Automated System Recovery (Windows XP only)

It's possible to automate the process of creating a system recovery set by choosing the ASR Wizard on the Tools menu of the Backup utility (Start ➢ All Programs ➢ Accessories ➢ System Tools ➢ Backup). This wizard walks you through the process of creating a disk that can be used to restore parts of the system in the event of a major system failure.

The default name of this file is `BACKUP.BKF`; it requires a floppy disk (which can be hard to come by these days). The backup set contains all the files necessary for starting the system, whereas the floppy becomes a bootable pointer to that backup set and can access/decompress it.

A weakness of the Automated System Recovery tool is its reliance on a bootable floppy in a day when many new systems no longer include a 3.5″ drive.

Emergency Repair Disks (Windows 2000 only)

The Windows Backup and Recovery Tool/Wizard allows you to create an emergency repair disk (ERD). As the name implies, this is a disk you can use to repair a portion of the system in the event of a failure.

When you choose this option, the tab changes to the Backup tab, and a prompt tells you to install a blank, formatted floppy disk. A check box inquires whether you want to

save the Registry as well. (The default is no.) If you don't choose to save the Registry, the following files are placed on the floppy disk:

- SETUP.LOG
- CONFIG.NT
- AUTOEXEC.NT

This doesn't leave you much to work with. The disk isn't bootable and contains only three minor configuration utilities.

If you check the box to include the Registry in the backup, the floppy disk contains the preceding files plus the following:

- SECURITY._
- SOFTWARE._
- SYSTEM._
- DEFAULT._
- SAM._
- NTUSER.DAT
- USRCLASS.DAT

The user profile (NTUSER.DAT) is for the default user; the files with the ._ extension are compressed files from the Registry. The compression utility used is EXPAND.EXE, which offers you the flexibility of restoring any or all files from any Microsoft operating system, including this utility (Windows 95/98, Windows NT, and so on). Because this floppy contains key Registry files, it's important that you label it appropriately and store it in a safe location, away from users who should not have access to it.

During the process of creating the floppy, the Registry files are also backed up (in uncompressed state) to %systemroot%\repair\RegBack.

As before, the floppy isn't bootable, and you must bring the system up to a point (booted) where the floppy can be accessed before it's of any use.

ERD does not exist in Vista. The System Restore tab lets you disable/enable and configure the new System Restore feature in Windows XP and Vista. If you have a system crash, it can restore your data back to the restore point. You can turn on System Restore for all drives on your system or for individual drives. Note that turning off System Restore on the system drive (the drive on which the OS is installed) automatically turns it off on all drives.

Common Operational Problems

CompTIA wants you to be aware of six somewhat common operational problems that can occur with Windows. All six are discussed in this section.

Printing Problems

Most printing problems today are due to either improper configuration or actual physical problems with the printer. Physical printer problems are addressed in two other chapters in this book, and so configuration is the focus here.

The Windows architecture is such that when a client wants to print to a network printer, a check is first done to see if the client has the latest printer driver. If it doesn't—as judged by the print server—the new driver is sent from the server to the client, and then the print job is accepted. This is an enormous help to the administrator, for when a new driver comes out, all the administrator must do is install it on the server, and the distribution to the clients becomes automatic.

Errors occur when a client is configured with a printer different from the one in use. For example, suppose the network has an ABC 6200 printer, but you don't see that among the list of choices when you install the printer. Rather than taking the time to get the correct driver, you choose the ABC 6000, because you've been told that it's compatible. All will work well in this scenario until a new driver is released and loaded on the server. This client won't update (while all others configured with 6200 will), and thus there is the potential for printing problems to occur.

You can solve most other problems using the Printing Troubleshooter (select Start ➢ Help And Support, and type in **Printing Troubleshooter**). It will walk you through solving individual printing problems.

Auto-Restart Errors

If the system is automatically restarting, there is the possibility that it has a virus or is unable to continue current operations (in other words, it has become unstable). To solve issues with viruses, Trojans, and the like, install virus-detection software on every client (as well as on the server), keep the definitions current, and run them often.

If the problem is with the system being unstable, examine the log files and try to isolate the problem. Reboot in Safe Mode, and correct any incompatibility issues. You can also deselect the Automatically Restart On Startup And Recovery option of the System applet (Advanced tab) in Control Panel to prevent the system from rebooting.

Occasionally, systems reboot when they have been updated. This is a necessary process, and users are always given warning before the reboot is to occur. If no one is present to choose to reboot later (it's the middle of the night, for example), the reboot will take place.

Blue Screens

Once a regular occurrence when working with Windows, blue screens (also known as the Blue Screen of Death) have become less common. Occasionally, systems will lock up; you can usually examine the log files to discover what was happening when this occurred and take steps to correct it.

System Lockup

The difference between a blue screen and a system lockup is whether the dump message that accompanies a blue screen is present. With a regular lockup, things just stop working. As with blue screens, these are mostly a thing of the past (the exception may be laptops, which go to hibernate mode). If they occur, you can examine the log files to discover what was happening and take steps to correct it.

Driver Failure

Drivers are associated with devices, and you can access them by looking at the properties for the device. The following, for example, are the three most common tabs of an adapter's Properties dialog box (tabs that appear are always dependent on the type of device and it's capabilities):

General This tab displays the device type, manufacturer, and location. It also includes text regarding whether the device is currently working properly and a Troubleshooter button to walk you through diagnostics.

Driver Access this tab to view information on the current driver and digital signer. Three command buttons allow you to see driver details and uninstall or update the driver.

Resources This tab shows the system resources in use (I/O, IRQ, and so on) and whether there are conflicts.

In Device Manager, you can also expand the Monitors tree, right-click on the monitor shown, and choose Properties from the context menu. Doing so shows the General and Driver tabs discussed in the preceding list, but not Resources.

Application Failures

If applications fail to install, start, or load, you should examine the log files associated with them to try to isolate the problem. Many applications write logs that can be viewed with Event Viewer (choose Application Logs), and others (mostly legacy) write to text files that you can find in their own directories.

Common steps to try include closing all other applications and beginning this one, reinstalling fresh, and checking to see whether the application works properly on another machine.

Common Error Messages

When things fail, they try to tell you why—this is a vast improvement in Windows over the old days when cryptic messages were the best you could hope for. Event Viewer is the primary tool for finding problems and uncovering what is going on. Other issues that can occur, however, include problems with booting and system failure.

Booting problems can occur with corruption of the boot files or missing components, and common error messages include an invalid boot disk, inaccessible boot drive, or missing NTLDR file. Luckily, during the installation of the operating system, log files are created in the `%SystemRoot%` and `%SystemRoot%\Debug` folders (`C:\WINNT` for Windows 2000 and `C:\WINDOWS` for Windows XP and Windows Vista). If you have a

puzzling problem, look at these logs and see if you can find error entries there. With Windows 2000, for example, the following six files are created:

`Comsetup.log` This log file holds information about the COM+ installation and any optional components installed. Of key importance are the last lines of the file, which should always show that the setup completed. If the last lines don't show this, they depict where the errors occurred.

`Mmdet.log` This file is used to hold information relevant to the detection of multimedia devices and ports. On most systems used for business, this file is very small and contains only a few lines.

`Netsetup.log` This file differs from all the others in that it's in the `DEBUG` folder and not just `%SystemRoot%`. Entries in it detail the workgroup and domain options given during installation.

`Setupact.log` Known as the Action log, this file is a chronological list of what took place during the setup. There is a tremendous amount of information here; of key importance is whether errors occurred. The last lines of the file can show which operation was transpiring when the installation failed, or whether the installation ended with errors. Like all the log files created during setup, this file is in ASCII text format and can be viewed with any viewer (WordPad, Word, and so on).

`Setupapi.log` This file shows every line run from an INF file and the results. Not only is this file created during installation, but it continues to get appended to afterward. Of key importance is whether the commands are able to complete without error.

`Setuperr.log` The Error log, as this file is commonly called, is written to at the time errors are noted in other log files. For example, an entry in `Setupact.log` may show that an error occurred, and additional information on it will be found in `Setuperr.log`. Not only are the errors here, but also the severity of each is given.

You can configure problems with system failure to write dump files (debugging information) for later analysis when they occur by going to the System applet in Control Panel, choosing the Advanced tab, and clicking Settings under Startup and Recovery. Here, in addition to choosing the default operating system, you can configure whether events should be written to the system log, whether an alert should be sent to the administrator, and the type of memory dump to be written.

Diagnostic Tools

The boot menu and System File Checker are two tools to be familiar with as you prepare for this exam.

Safe Mode

If, when you boot, Windows won't come all the way up (it hangs or is otherwise corrupted), you can often solve the problem by booting into Safe Mode. Safe Mode is a concept borrowed from Windows 95 wherein you can bring up part of the operating system by bypassing the settings, drivers, or parameters that may be causing it trouble during a normal boot. The goal

of Safe Mode is to provide an interface with which you're able to fix the problems that occur during a normal boot and then reboot in normal mode.

To access Safe Mode, you must press F8 when the computer starts/restarts or when the operating system menu is displayed during the boot process if you have multiple operating systems installed. A menu of Safe Mode choices will then appear, as listed in Table 8.7. Select the mode you want to boot into.

TABLE 8.7 Safe Mode Startup Menu

Choice	Loaded
Safe Mode	Provides the VGA monitor, Microsoft mouse drivers, and basic drivers for the keyboard (storage system services, no networking)
Safe Mode With Networking	Same as Safe Mode, but with networking
Safe Mode With Command Prompt	Same as Safe Mode, but without the interface and drivers/services associated with it
Enable Boot Logging	Creates `ntbtlog.txt` in the `%systemroot%` directory during any boot—normal attempted
Enable VGA Mode	Normal boot with only basic video drivers
Last Known Good Configuration	Uses the last backup of the Registry to bypass corruption caused during the previous session
Debugging Mode	Sends information through the serial port for interpretation/troubleshooting at another computer
Boot Normally	Bypasses any of the options here
Return To OS Choices Menu	Gives you an out in case you pressed F8 by accident. This option only appears if you have installed multiple operating systems and/or the Recovery Console

You need to keep a few rules in mind when booting in different modes:

- If problems don't exist when you boot to Safe Mode but do exist when you boot to normal mode, the problem isn't with basic services/drivers.
- If the system hangs when you load drivers, the log file can show you the last driver it attempted to load, which is usually the cause of the problem.
- If you can't solve the problem with Safe Mode, restore the Registry from the ERD to a state known to be good. Bear in mind that doing so will lose all changes that have occurred since the last ERD was made.

System File Checker

The purpose of this utility is to keep the operating system alive and well. SFC.EXE automatically verifies system files after a reboot to see if they were changed to unprotected copies. If an unprotected file is found, it's overwritten by a stored copy of the system file from %systemroot%\system32\dllcache. (%systemroot% is the folder into which the operating system was installed.)

Storing system files (some of which can be quite large) in two locations consumes a large amount of disk space. When you install Windows 2000 Professional, make sure you leave ample hard drive space on the %systemroot% drive for growth. By default, the cache for these files is limited to approximately 300-400MB. It can be changed using the /CACHESIZE parameter (discussed below).

Only users with the Administrator group permissions can run SFC. It also requires the use of a parameter. The valid parameters are listed in Table 8.8.

TABLE 8.8 SFC Options

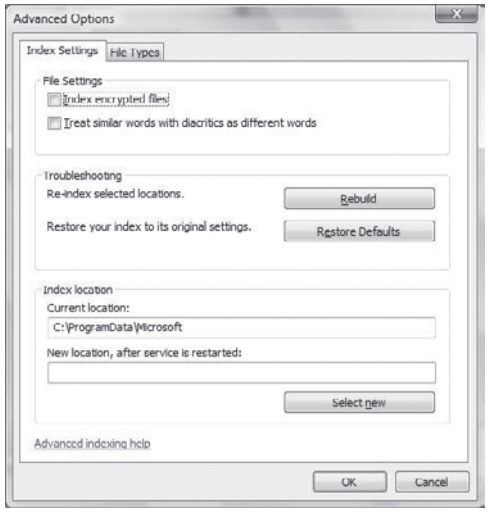
Parameter	Function
/CACHESIZE=	Sets the size of the file cache
/CANCEL	Stops all checks
/ENABLE	Returns to normal mode
/PURGECACHE	Clears the cache
/QUIET	Replaces files without prompting
/SCANBOOT	Checks system files on every boot
/SCANNOW	Checks system files now
/SCANONCE	Checks system files at the next boot

System Performance and Optimization

Windows Vista introduced a number of features that an administrator should be aware of in order to understand how to better optimize a system. The first of these is the Aero interface. Microsoft maintains a list of common issues with Aero—and solutions—at http://windowshelp.microsoft.com/Windows/en-us/help/c33fe91a-9e6f-41f4-ae82-3ed2d5fa2fbf1033.mspx and I strongly encourage you to visit that site.

Indexing Options, available from Control Panel, allow you to configure how the system caches information that can speed up searches within Windows. This service was included with the previous operating system versions, but has become more robust in Windows Vista. The index, when used, holds information about files and their properties (author, date modified, and so on). By default, information within your personal folders is automatically indexed, but program files and system files are not. Figure 8.18 shows the advanced options that are available with indexing. With Windows 2000, you can go to Services, and stop Indexing Services. After that, right-click on it, point to All Tasks, and click Tune Performance to see similar options.

FIGURE 8.18 The Advanced Options dialog box for indexing



The UAC (User Account Control) feature has been discussed in previous chapters and has the sole purpose of keeping the user from running programs that could pose a potential threat by escalating privileges to that of administrator. While turning UAC off is an option, it is not a recommended option. If you have a program you regularly run and do not want to be prompted each time, you can right-click on the icon for that program and then click Properties. Choose the Compatibility tab and then check the box Run This Program As An Administrator. This will prevent the prompt from occurring each time you use the program.

Operating system programs are typically not able to have this feature set and the privileges will stay grayed out on the Compatibility tab.

The Sidebar is a new feature allowing easy access to gadgets. To configure the Sidebar, right-click on an area of it and choose Properties (if the Sidebar is not visible, click Start ➢ All Programs ➢ Accessories ➢ Windows Sidebar). This will bring up the dialog box shown in Figure 8.19.

FIGURE 8.19 Configuring the Sidebar

Startup maintenance can be accomplished in a number of ways. In addition to tools such as msconfig, you can also right-click on Startup in the Start ➢ All Programs menu and choose Properties. This will allow you to change the location, security, and other settings related to startup. Windows Defender will allow you to configure items within the Startup Programs menu as well, as shown in Figure 8.20.

FIGURE 8.20 Configuring Startup Programs in Windows Defender

Background processes, while not unique to Windows Vista, are something to always be aware of. Just because you have only one application you are using, this does not mean that dozens of processes—if not more—aren't busy working on the system. The easiest way to view running processes is with Task Manager, discussed earlier in this chapter.

Exam Essentials

Know the recovery options. Be familiar with the Recovery Console, ASR, and ERD.

Be familiar with the common operational problems. Blue screens and lockups are far less common that they used to be, but they do still occur. Know how to deal with them and the other issues described.

Know the common errors. Be able to identify how to get to error logs, and know the logs created during installation.

List the boot menu options. Know how to access the boot menu and what options appear there.

Review Questions

1. Which command-line utility displays or changes the attributes for one or more files?
2. You have opened a command window with `CMD` and now want to close it. What command should you use to do this?
3. At the command line, what switch can be used with `DIR` to see the listing one screenful at a time?
4. You are in the directory `C:\Documents and Settings\edulaney\photos`. Where will the command `cd ..` take you?
5. What is the command—and syntax—that should be used to change the G: drive from FAT32 to NTFS without losing data?
6. Which command is used to start the System Configuration Editor?
7. Which type of backup copies only the files for which the archive bit is currently turned on, and turns off the archive bit after the files are backed up?
8. When does Windows XP automatically create restore points?
9. What are three ways to start Task Manager?
10. What is the command used to install the Recovery Console from the CD?

Answers to Review Questions

1. `ATTRIB` displays or changes the attributes for one or more files.
2. `EXIT` closes the `CMD` window.
3. `DIR /P` displays the listing one screenful at a time. Press Enter to see the next screenful.
4. This will take you to the directory `C:\Documents and Settings\edulaney`.
5. The command is `convert G: /FS:NTFS`.
6. The command is `MSCONFIG`. You can start it by going to Start ➢ Run, and typing **`MSCONFIG`**.
7. An incremental backup copies only the files for which the archive bit is currently turned on. After the files are backed up, the archive bit is turned off.
8. Windows XP creates restore points automatically every 24 hours, as well as when you install unsigned device drivers or install (or uninstall) a program with Windows Installer or InstallShield.
9. Three ways of starting Task Manager were discussed in this chapter. One way to display the Task Manager is to press Ctrl+Alt+Delete and click the Task Manager button (if needed). The second way is to right-click an empty location on the Taskbar and choose Task Manager from the context menu. The third method is to hold down Ctrl+Shift and press Esc. There are actually more than three. For example typing taskmgr (or `taskmgr.exe`) will do the same in the Run dialog box or at the command prompt.
10. The command is `winnt32 /cmdcons`.

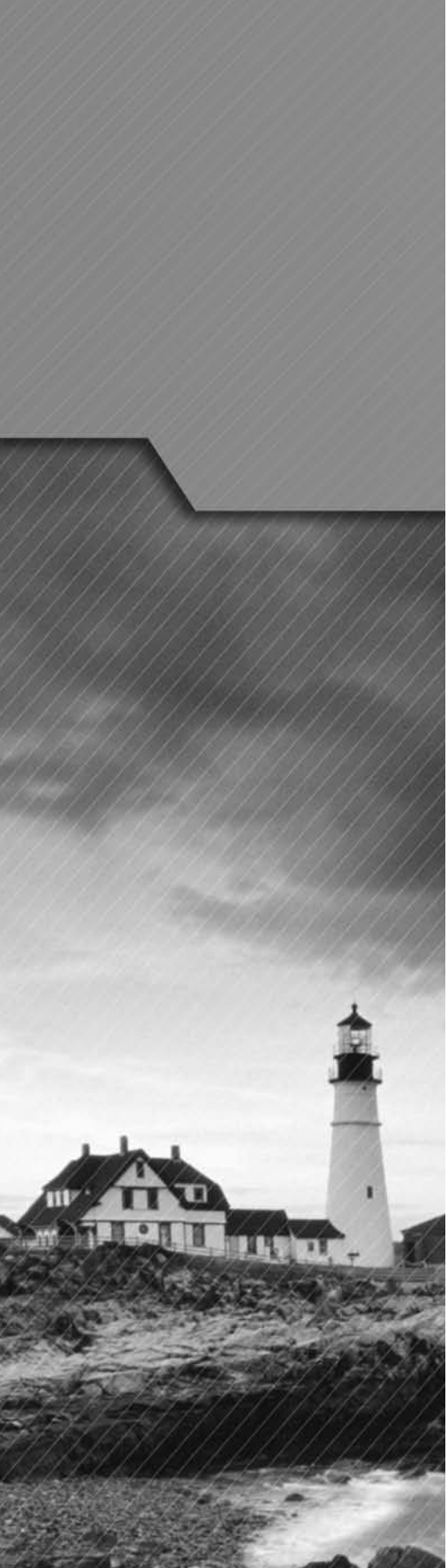
Chapter

9

Networking

COMPTIA A+ PRACTICAL APPLICATION EXAM OBJECTIVES COVERED IN THIS CHAPTER:

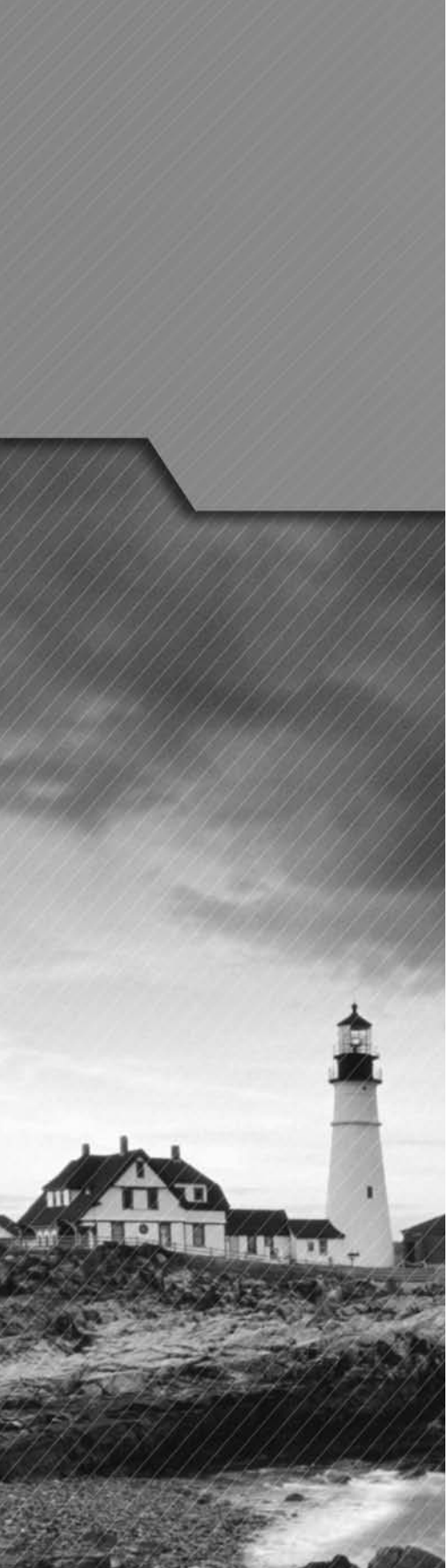
- ✓ **3.1 Troubleshoot client-side connectivity issues using appropriate tools**
  - TCP/IP settings
    - Gateway
    - Subnet mask
    - DNS
    - DHCP (dynamic vs. static)
    - NAT (private and public)
  - Characteristics of TCP/IP
    - Loopback addresses
    - Automatic IP addressing
  - Mail protocol settings
    - SMTP
    - IMAP
    - POP
  - FTP settings
    - Ports
    - IP addresses
    - Exceptions
    - Programs
  - Proxy settings
    - Ports
    - IP addresses
    - Exceptions
    - Programs



- Tools (use and interpret results)
  - Ping
  - Tracert
  - Nslookup
  - Netstat
  - Net use
  - Net /?
  - Ipconfig
  - telnet
  - SSH
- Secure connection protocols
  - SSH
  - HTTPS
- Firewall settings
  - Open and closed ports
  - Program filters

✓ **3.2 Install and configure a small office home office (SOHO) network**

- Connection types
  - Dial-up
  - Broadband
    - DSL
    - Cable
    - Satellite
    - ISDN
  - Wireless
    - All 802.11
    - WEP
    - WPA
    - SSID



- MAC filtering
- DHCP settings
- Routers / Access Points
  - Disable DHCP
  - Use static IP
  - Change SSID from default
  - Disable SSID broadcast
  - MAC filtering
  - Change default username and password
  - Update firmware
  - Firewall
- LAN (10/100/1000BaseT, Speeds)
- Bluetooth (1.0 vs. 2.0)
- Cellular
- Basic VoIP (consumer applications)

- Basics of hardware and software firewall configuration
  - Port assignment / setting up rules (exceptions)
  - Port forwarding / port triggering
- Physical installation
  - Wireless router placement
  - Cable length

Although the networking domain constituted a sizable portion of the Essentials exam, it's just as important on the Practical Application exam, and it's something you will need to be very familiar with in your career in IT.

Some of the material here was also discussed in Chapter 4, "Networking," which covered the Essentials exam. Every attempt has been made to have no more repetition than necessary.

Client-side Connectivity Issues

For this portion of the exam, you're expected to know the definition and characteristics of topics in two key areas:

- TCP/IP protocols
- Troubleshooting utilities

Both of these are covered in this section.

Critical Information

It isn't enough to know how the network you currently have works and to know the technologies you're employing. You must also know about the technologies and protocols you *aren't* using so you can evaluate which ones should be incorporated into your environment. It's important to stay atop of new developments in the field and appraise them for suitability to the needs of your organization.

The following definitions are a refresher on some of those CompTIA expects you to know for this objective.

Protocols, Technologies, and Terms

The following protocols, technologies, and terms are those you should know for this exam:

Automatic Private IP Addressing Automatic Private IP Addressing (APIPA) is a TCP/IP feature Microsoft added to their operating systems. If a DHCP server cannot be found, the clients automatically assign themselves an IP address, somewhat randomly, in the

169.254.x.x range with a subnet mask of 255.255.0.0. This allows them to communicate with other hosts that have similarly configured themselves, but they are unable to connect to the Internet.

DHCP The Dynamic Host Configuration Protocol (DHCP) is a service that runs on a DHCP server and leases to a client IP addresses from a pool of available addresses. The length of the leases is configurable by the administrator, and addresses can be either public or private.

DNS Domain Name Service (DNS) is a network service used in TCP/IP networks that translates hostnames (for example, `www.au-answers.com`) to IP addresses (for example, 209.237.150.20). The first attempts at this were done using static files called hosts files. When the systems grew too large for the files to be feasible, the DNS was created to handle it.

Firewall A firewall is a server that sits between the internal network and the rest of the world and filters what goes between the two. While the filter can be done on programs, most are done on ports since applications and protocols use ports that are recognized. Open ports are those that allow traffic, while closed ports are those that block traffic. The firewall can be software- or hardware-based, and most incorporate both. The firewall may incorporate a proxy, a gateway, and a filter.

FTP The File Transfer Protocol (FTP) is both a TCP/IP protocol and software that permits the transferring of files between computer systems. Because FTP has been implemented on numerous types of computer systems, files can be transferred between disparate systems (for example, a personal computer and a minicomputer). It uses ports 20 and 21 by default. It can be configured to allow or deny access to specific IP addresses and can be configured to work with exceptions. While the protocol can be run within most browsers, a number of FTP applications are available, with FileZilla (`http://filezilla-project.org/`) being one of the more popular.

Gateway A gateway, as it tested on the exam, is the server (router) that allows traffic beyond the internal network. Hosts are configured with the address of a gateway (called the default gateway), and if they need to correspond with a host outside the internal network, the data is sent to the gateway to facilitate this. When you configure TCP/IP on a host, one of the fields that should be provided is a gateway field, which specifies where data not intended for this network is sent in order to be able to communicate with the rest of the world.

HTML Hypertext Markup Language (HTML) is a set of codes used to format text and graphics that will be displayed in a browser. The codes define how data will be displayed.

HTTP Hypertext Transfer Protocol (HTTP) is the protocol used for communication between a web server and a web browser. It uses port 80 by default.

HTTPS Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS) is a protocol used to make a secure connection. It uses port 443 by default.

IMAP Internet Message Access Protocol (IMAP) is a protocol with a store-and-forward capability. It can also allow messages to be stored on an e-mail server instead of downloaded to the client. The current version of the protocol is 4 (IMAP4), and the counterpart to it is Post Office Protocol (POP). IMAP runs on port 143.

Loopback Address The loopback address is used in TCP/IP to check the status of the networking stack on a client without going to the physical wire. In other words, it is used to check that TCP/IP is functioning properly locally without checking the status of the network. This address is 127.0.0.1 and is available on every TCP/IP host regardless of the vendor. The most common test is `ping 127.0.0.1`.

NAT Network Address Translation (NAT) is a protocol used to translate between public and private addresses. By using NAT, it is possible to configure all hosts on the internal network to use private addresses and have the NAT server act as a proxy between them and the public Internet. Most client operating systems from Microsoft include a small version of this, known as Internet Connection Sharing (ICS), for use on small and home networks. Any implementation needing more than what ICS can offer must use a NAT server.

POP The Post Office Protocol (POP) is a protocol for receiving e-mail from an SMTP server. The alternative to POP, which runs on port 110, is IMAP.

Proxy Server A proxy server is any server that acts on the behalf of another in order to obtain network (usually Internet) access. Most proxy servers are also NAT servers, but they need not be. Microsoft Internet Security and Acceleration Server (ISA) is one of the most well-known proxy servers (`http://www.microsoft.com/forefront/edgesecurity/isaserver/en/us/default.aspx`). Proxy servers are configured to allow or deny ports and IP addresses as desired by the administrator.

SMTP Simple Mail Transfer Protocol (SMTP) is a protocol for sending e-mail between SMTP servers. Clients typically use either IMAP or POP to access it. SMTP uses port 25 by default.

SSH The Secure Shell (SSH) application replaces Telnet and provides the same functionality while increasing security. SSH runs on port 22 and encrypts the transmitted data, including the password.

SSL Secure Socket Layer (SSL) is a protocol that secures messages by operating between the Application layer (HTTP) and the Transport layer.

Subnet Mask The value of the subnet mask is used to identify the size of the network this host is on. This value, along with all others needed for TCP/IP configuration, can be manually configured or automatically supplied by the DHCP server.

TCP/IP Transmission Control Protocol/Internet Protocol (TCP/IP) is a suite of networking protocols and applications. To start using it, you typically need three values: a unique IP address for this host (which can be statically assigned or leased through DHCP), a subnet mask, and the address of a default gateway.

Telnet Telnet is a protocol that functions at the Application layer of the OSI model, providing terminal-emulation capabilities. Telnet runs on port 23, but has lost favor to SSH due to the fact that Telnet sends data— including passwords—in plain-text format.

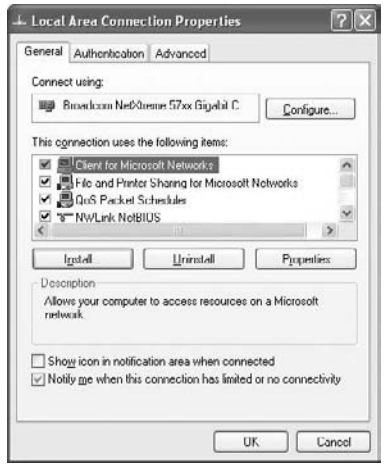
For network connectivity to occur, there must be a network card and a language shared between the hosts. The network card can be a wired card requiring LAN cabling, or it may be a wireless card. The language can be the TCP/IP protocol (the most popular), or any of a number of other possibilities.

To configure a Windows XP client on a new network, choose My Network Places (depending on the Desktop used, it may be on the Desktop or accessible from the Start menu), and then choose Set Up A Home Or Small Office Network (or Set Up A Wireless Network For A Home Or Small Office, if appropriate) beneath Network Tasks. This starts the Network Setup Wizard shown in Figure 9.1 and walks you through the configuration of the client.

FIGURE 9.1 The Network Setup Wizard walks you through the process of adding an XP client to a network.

Once you've configured it on the network, you can always go to Network Tasks and choose Add A Network Place when needed. Doing so starts the Add Network Place Wizard and allows you to configure Internet connections as well as create shortcuts to websites, FTP sites, and other network locations. If you click View Network Connections, right-click a LAN or high-speed Internet connection, and choose Properties, you can install, uninstall, and change the properties for any available client, service, or protocol, as shown in Figure 9.2.

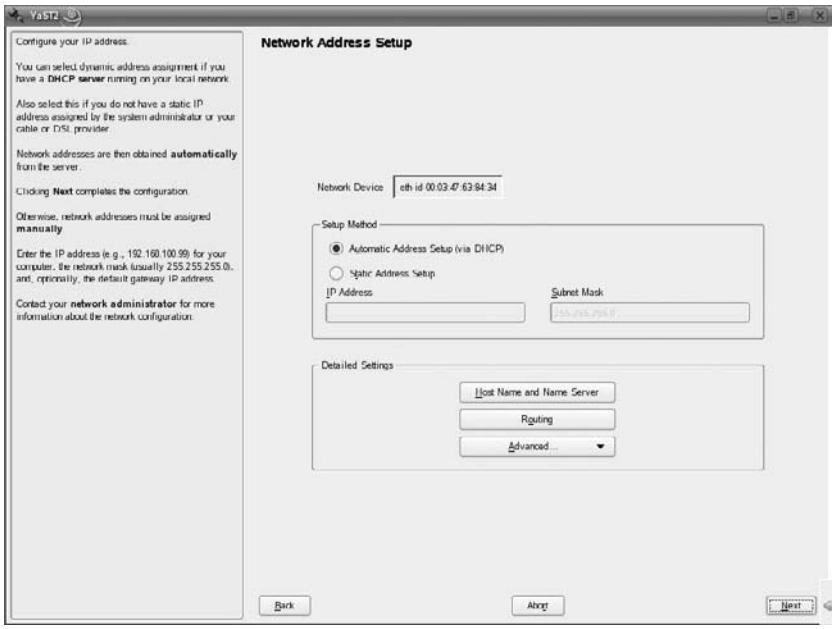
FIGURE 9.2 Configure the client, service, and protocol settings in XP.



The Advanced tab allows you to configure Windows Firewall and Internet Connection Sharing parameters.

Different Linux vendors include the same functionality but use different tools. With SUSE Linux, for example, you can start Yet another Setup Tool (YaST) and then choose the options between Network Devices and Network Services to configure similar parameters. Figure 9.3 shows the settings for the network card in SUSE Linux.

FIGURE 9.3 Configure network card parameters in SUSE Linux.



Sharing Network Resources

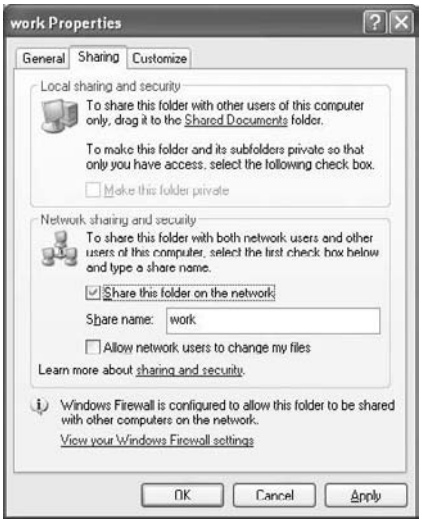
The real reason for a network is to be able to share resources, whether those resources are printers, files, or something different. In each operating system, sharing is almost as simple as configuring network access.

With the Microsoft Windows operating systems, workgroup members who are to share resources must have the File And Printer Sharing For Microsoft Networks client installed (it need not be installed for those who are only going to access it). You can then choose to share printers by right-clicking them and choosing Share This Printer from the dialog box that appears and is shown in Figure 9.4.

Similarly, to share files or folders, right-click them, choose Properties, and then click the Sharing tab (you can also choose Sharing And Security from the context menu). Doing so offers the choices shown in Figure 9.5. Files on FAT drives cannot be shared, only folders can. Similarly, the Security tab is not available for objects stored on FAT disks (or when Simple File Sharing is turned on).

FIGURE 9.4 Configure printer sharing in Windows XP.

FIGURE 9.5 Configure folder sharing in Windows XP.



Once a folder is shared, a hand icon appears beneath it, and others can access it. Share permissions apply only when a user is accessing a file or folder through the network. Local permissions and attributes are used to protect the file when the user is local (always remember: objects of FAT drives have no local security).

If you aren't using a workgroup configuration, then files to be shared are typically placed on the server; rights associated with the server operating system can be used to differentiate between users. Table 9.1, for example, lists NTFS directory permissions.

TABLE 9.1 NTFS Folder Permissions

NTFS Permission	Meaning
Full Control	Gives the user all the other choices and the ability to change permission. The user also can take ownership of the directory or any of its contents.
Modify	Combines the Read & Execute permission with the Write permission, and allows the user to delete everything, including the folder.
Read & Execute	Combines the permissions of Read with those of List Folder Contents, and adds the ability to run executables.
List Folder Contents	Known as List in previous versions. Allows the user to view the contents of a directory and to navigate to its subdirectories. It doesn't grant the user access to the files in these directories unless that is specified in file permissions.
Read	Allows the user to navigate the entire directory structure, view the contents of the directory, view the contents of any files in the directory, and see ownership and attributes.
Write	Allows the user to create new entities in the folder, as well as to change ownership, permissions, and attributes.

Network Tools to Use

The following list of utilities, some of which were also discussed in Chapter 4, "Networking," constitutes those CompTIA wants you to know for this part of the exam.

CompTIA also expects you to have knowledge of cable-testing devices. This is a broad category of any type of device that can isolate a break or problem with a cable or termination.

IPCONFIG.EXE

With Windows-based operating systems, you can determine the network settings that a *Dynamic Host Configuration Protocol* (DHCP) server has leased to your computer by typing the following command at a command prompt:

```
IPCONFIG /all
```

`IPCONFIG` (with the `/ALL` parameter) also gives you full details on the duration of your current lease. You can verify whether a DHCP client has connectivity to a DHCP server

by releasing the client's IP address and then attempting to lease an IP address. You can conduct this test by typing the following sequence of commands from the DHCP client at a command prompt:

```
IPCONFIG /release
IPCONFIG /renew
```

This is one of the first tools to use when experiencing problems accessing resources, because it will show you whether an address has been issued to the machine. If the address displayed falls in the 169.254.x.x category, then the client was unable to reach the DHCP server and has defaulted to Automatic Private IP Addressing (APIPA), which will prevent it from communicating outside of its subnet, if not altogether.

In the Linux world, a utility similar to `IPCONFIG` is `IFCONFIG`.

NET USE

The `NET USE` command is used on Windows-based clients to connect or disconnect from shared resources (which were addressed in the "Sharing Network Resources" earlier in this chapter). You can see what options are available by using `/?` or see what is currently shared by typing **`NET USE`** without any other parameters.

NET /?

The `NET` command is one of the most powerful on the Windows-based network, as illustrated by `NET USE` (which we just discussed). The options that can be used with the command differ slightly based on the Windows operating system you are using; you can view a full list by typing **`NET /?`**.

NETSTAT

The `NETSTAT` (network status) command is used to see what ports are listening on the TCP/IP-based system. The `-a` option is used to show all ports, and `/?` is used to show what other options are available (the options differ based on the operating system you are using).

NSLOOKUP.EXE

Nslookup is a command-line utility that enables you to verify entries on a DNS server. You can use Nslookup in two modes: interactive and noninteractive. In interactive mode, you start a session with the DNS server, in which you can make several requests. In noninteractive mode, you specify a command that makes a single query of the DNS server. If you want to make another query, you must type another noninteractive command.

One of the key issues regarding the use of TCP/IP is the ability to resolve a hostname to an IP address—an action usually performed by a DNS server.

PING.EXE

PING is one of the most useful commands in the TCP/IP protocol. It sends a series of packets to another system, which in turn sends back a response. The ping utility can be extremely useful for troubleshooting problems with remote hosts.

The PING command indicates whether the host can be reached and how long it took for the host to send a return packet. On a LAN, the time is indicated as less than 10 milliseconds. Across WAN links, however, this value can be much greater.

SSH and Telnet

Both SSH and Telnet were mentioned earlier in this chapter. Telnet allows you to remotely connect to a host, and is one of the oldest TCP/IP services/utilities still in use. One of its weaknesses is that it lacks any true security and thus its use is strongly discouraged. The replacement for it is SSH, which performs the same functions but includes security features and measures to make it much less risky.

TRACERT.EXE

Tracert is a command-line utility that enables you to verify the route to a remote host. Execute the command TRACERT *hostname*, where *hostname* is the computer name or IP address of the computer whose route you want to trace. TRACERT returns the different IP addresses the packet was routed through to reach the final destination. The results also include the number of hops needed to reach the destination. If you execute the TRACERT command without any options, you see a help file that describes all the TRACERT switches.

The Tracert utility determines the intermediary steps involved in communicating with another IP host. It provides a road map of all the routing an IP packet takes to get from host A to host B.

As with the PING command, TRACERT returns the amount of time required for each routing hop.

Network Troubleshooting

The following common network problems and their symptoms are those CompTIA wants you to know for this part of the exam:

DNS Problems Issues with DNS not properly working or configured often manifest themselves as a host being unable to communicate using hostnames (fully qualified domain names [FQDNs]) but still able to communicate if IP addresses are used.

Driver Problems Hardware devices use drivers to communicate. With the release of new sets of files, you can change drivers, fix related problems, or add functionality that is presently lacking. Problems with drivers can usually be identified by an inability to perform functions that should be done.

Electrical Interference Problems Electromagnetic interference (EMI) will degrade network performance. This can be identified by the poor operation present. Be sure to run cables around (not over) ballasts and other items that can cause EMI.

Firewall Configuration Problems Issues with firewalls can prevent access to data. By default, once firewalls are enabled, they tend to limit as much as possible; you must configure them to let through the traffic that you want to pass. This is done by configuring ports; for example, to allow SMTP traffic, you open port 25; to block Telnet traffic, you close port 23.

Gateway Problems A default gateway allows traffic out of the network. If the gateway isn't configured properly, the hosts will have no difficulty communicating on the network, but they will be unable to communicate beyond the LAN.

Network Interface Problems If there are problems with the network card, you usually won't be able to communicate at all. Check the card for a status light(s), and verify that it's on. Blinking typically indicates link activity, and a solid light can indicate that all is working well. A light that isn't on indicates that there is no activity and the card should be replaced.

Permission Problems Issues with permissions prevent users from accessing resources. Make sure the users or groups have the appropriate permissions to be able to use the resource as intended.

Static and Automatic Address Assignment Problems If DHCP is used to issue automatic addresses, you must make sure the host can be reached and has enough addresses in its scope to be able to service all clients. If you're using static addresses, one of the most common problems is issuing the same address to two clients, which causes both to be unable to communicate. Every host on the network must have a unique IP address.

Subnet Mask Problems Problems with subnet masks (incorrect values) prevent the client from being able to communicate with other hosts on the network. A common issue is leaving the default value and forgetting to set it to a value your network is using.

Exam Essentials

Know which utilities can be used for troubleshooting. The objectives include four utilities that work in the Windows world, and you should know each of them.

Know common symptoms of network problems. Review the list given in this chapter, and make sure you know common issues and problems and how they manifest themselves.

Know how to establish network connectivity. For a client on a network, you need a network card and a language (protocol) shared between the client and other hosts.

Know how to share resources. Printers and files are the most commonly shared network resources. You can share them easily with the wizards or other tools.

Installing and Configuring a SOHO Network

This objective tests your knowledge of how to configure a small office or home office (SOHO) network. It deals with issues involving the technology (discussed previously in Chapter 4, "Networking") as well as the basics of installation and configuration.

Critical Information

One of the biggest differences between SOHO networks and larger local area networks (LANs) is the way they connect to the outside world. While a LAN would never connect in today's world through a dial-up connection, it is not impossible to still stumble across such a configuration in a SOHO network.

This section will look at the connection types and possibilities that exist for small networks, as well as some of the basics of network configuration.

Connection Types

Let's take a look at the connectivity technologies you should know for this exam.

Again, many of these were discussed in Chapter 4, "Networking," and you should reread that chapter when studying for this exam.

Bluetooth

Bluetooth is a short-range wireless standard that uses radio waves, for everything ranging from cell phone headsets to printers, keyboards, and handhelds. There are a number of Bluetooth specifications, all of which transmit in the 2.4–2.485GHz range. Three of these specifications are as follows:

- Version 1.2 supports data transmissions of up to 1Mbps and was adopted in 2003.
- Version 2.0+ is known as Enhanced Data Rate (EDR), and it was adopted in 2004.
- Version 2.1+EDR can support data rates up to 3Mbps, and it was adopted in 2007.

In addition to the three specifications, there are three device classes that differ in range and power usage:

- Class 1 uses 100 milliwatts and can transmit 100 meters.
- Class 2 uses 2.5 milliwatts and can transmit 10 meters. This is the most common of the three and the most likely to be found in a SOHO network.
- Class 3 uses only 1 milliwatt and has a limited range of only 1 meter. This one is rarely used.

Broadband (DSL, Cable, Satellite, ISDN)

There are essentially three methods of broadband access (using a single medium for several channels) that CompTIA looks at. Digital Subscriber Line (DSL) employs high-speed connections from telephone switching stations. Cable uses a cable modem and the cable line from providers who used to carry only television signals. Satellite replaces the terrestrial cable with signals through the air. The opposite of broadband is *baseband*—which allows only one signal at a time to be transmitted. Integrated Services Digital Network (ISDN) is a WAN technology that performs link management and signaling by virtue of packet switching. The original idea behind it was to let existing phone lines carry digital communications by using multiplexing to support multiple channels.

Cellular

The BlackBerry has made cellular networking popular, though it is not the only device capable of using cellular networking—a cellular modem can also be quickly added to a laptop. Cellular networks use a central access point (a cell tower) in a mesh network design. The two competing standards are the *Global System for Mobile Communications (GSM)* and the *Code Division Multiple Access (CDMA)*. The former is the most popular around the world, and the latter exists only in the United States.

Dial-up Networking

One of the first ways of communicating with ISPs and remote networks was through dial-up connections. Although this is still possible, it isn't used much anymore due to limitations on modem speed.

LAN/WAN

A LAN is a network that is geographically confined in a small space. That small space can be only a single room, a floor, a building, and so on. By being confined, it has tighter security and can normally offer higher speeds. Don't be mislead, however, by the word local—it refers to geography and not the size of the physical space. A wide area network (WAN) is a collection of two or more LANs, typically connected by routers. The geographic limitation is removed, but WAN speeds are traditionally less than LAN speeds.

With Ethernet, you can often use the network type to compute the required length and speed of your cabling. For example, 100BaseT tells you three things:

- 100: The speed of the network, 100Mbps.
- Base: The technology used (either baseband or broadband).
- T: Twisted-pair cabling. In the case of 10BaseT, it's generally UTP.

Routers and Access Points

When you configure a network, one of the first places to turn your attention to is the routers and access points—they are the hardware components on which network access can rely. Because these devices must always be able to be found, it is suggested that DHCP not be used to issue them addresses but that their addresses be statically configured.

To increase security, devices should be behind a firewall and you should always change the administrative username and password that comes preconfigured with these devices to ones that adhere to stringent password policies (mixture of upper- and lowercase alphabet, numbers, characters, etc.), and keep the firmware updated.

With wireless access points, you should change the SSID from its default value (if one is preconfigured) and disable broadcasts. MAC filtering can be used on a wireless network, for example, to prevent certain clients from accessing the Internet. You can choose to deny service to a set list of MAC addresses (and allow all others) or allow service only to a set of MAC addresses (and deny all others).

VoIP

Voice over IP (VoIP) is also known as IP telephony and Internet telephony. It's the routing of voice traffic over the Internet (it could be across any smaller IP-based network, but generally it's the Internet).

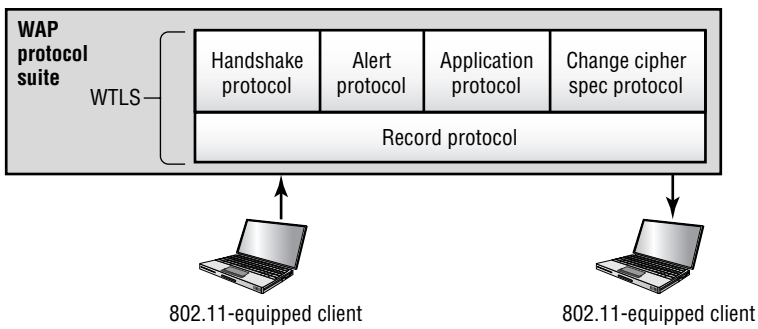
Wireless

The following list examines the various types of wireless systems that you'll encounter. We also explore some of the security issues associated with this technology. Specifically, we deal with Wireless Transport Layer Security (WTLS), the IEEE 802 wireless standards, WAP/WEP applications, and the vulnerabilities that each presents.

Wireless Transport Layer Security *Wireless Transport Layer Security (WTLS)* is the security layer of the Wireless Application Protocol (WAP), discussed in a moment in "WAP/WEP." WTLS provides authentication, encryption, and data integrity for wireless devices. It's designed to utilize the relatively narrow bandwidth of these types of devices, and it's moderately secure. WTLS provides reasonable security for mobile devices, and it's being widely implemented in wireless devices.

Figure 9.6 illustrates WTLS as part of the WAP environment. WAP provides the functional equivalent of TCP/IP for wireless devices. Many devices, including newer cell phones and PDAs, include support for WTLS as part of their networking protocol capabilities.

FIGURE 9.6 WTLS used between two WAP devices



The term *gap in the WAP* is used to describe the security concern that exists when converting between WAP and SSL/TLS.

IEEE 802.11*x* Wireless Protocols

The IEEE 802.11*x* family of protocols provides for wireless communications using radio frequency transmissions. The frequencies in use for 802.11 standards are the 2.4GHz and the 5GHz frequency spectrum. Several standards and bandwidths have been defined for use in wireless environments, and they aren't extremely compatible with one another:

- The *802.11* standard defines wireless LANs transmitting at 1Mbps or 2Mbps bandwidths using the 2.4GHz frequency spectrum and using either frequency-hopping spread spectrum (FHSS) or direct-sequence spread spectrum (DSSS) for data encoding.
- The *802.11a* standard provides wireless LAN bandwidth of up to 54Mbps in the 5GHz frequency spectrum. The 802.11a standard also uses orthogonal frequency division multiplexing (OFDM) for encoding rather than FHSS or DSSS.
- The *802.11b* standard provides for bandwidths of up to 11Mbps (with fallback rates of 5.5, 2, and 1Mbps) in the 2.4GHz frequency spectrum. This standard is also called *Wi-Fi* or *802.11 high rate*. The 802.11b standard uses only DSSS for data encoding.
- The *802.11g* standard provides for bandwidths of up to 54Mbps in the 2.4GHz frequency spectrum. While able to obtain faster speeds, it also suffers from the same interference problems inherent in 802.11b—having to share the spectrum with other devices using that frequency.
- The *802.11n* standard provides for bandwidths of up to 300Mbps in the 5GHz frequency spectrum (it can also communicate at 2.4GHz for compatibility). The advantage of this standard is that it offers higher speed and a frequency that does not have as much interference.

WAP/WEP

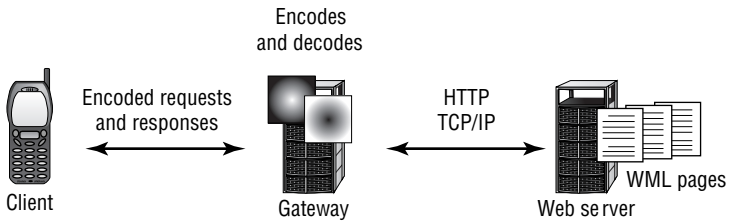
Wireless systems frequently use the Wireless Application Protocol (WAP) for network communications. Wired Equivalent Privacy (WEP) is intended to provide the equivalent security of a wired network protocol.

Wireless Access Protocol (WAP) *Wireless Access Protocol (WAP)* is the technology designed for use with wireless devices. WAP has become a standard adopted by many manufacturers, including Motorola and Nokia. WAP functions are equivalent to TCP/IP functions in that they're trying to serve the same purpose for wireless devices. WAP uses a smaller version of HTML called *Wireless Markup Language (WML)*, which is used for Internet displays. WAP-enabled devices can also respond to scripts using an environment called *WMLScript*. This scripting language is similar to Java, which is a programming language.

The ability to accept web pages and scripts produces the opportunity for malicious code and viruses to be transported to WAP-enabled devices. No doubt this will create a new set of problems, and antivirus software will be needed to deal with them.

WAP systems communicate using a WAP gateway system, as depicted in Figure 9.7. The gateway converts information back and forth between HTTP and WAP as well as encodes and decodes between the security protocols. This structure provides a reasonable assurance that WAP-enabled devices can be secured. If the interconnection between the WAP server and the Internet isn't encrypted, packets between the devices may be intercepted, creating a potential vulnerability. This vulnerability is called a *gap in the WAP*.

FIGURE 9.7 A WAP gateway enabling a connection to WAP devices by the Internet



Wired Equivalent Privacy *Wired Equivalent Privacy (WEP)* is a security standard for wireless devices. WEP encrypts data to provide data security. The protocol has always been under scrutiny for not being as secure as initially intended.

WEP is vulnerable due to weaknesses in the way the encryption algorithms are employed. These weaknesses allow the algorithm to potentially be cracked in as few as five minutes using available PC software. This makes WEP one of the most vulnerable protocols available for security.

Wi-Fi Protected Access (WPA) The *Wi-Fi Protected Access (WPA)* and *Wi-Fi Protected Access 2 (WPA2)* technologies were designed to address the core problems with WEP. These technologies implement the 802.11i standard. The difference between WPA and WPA2 is that the former implements most—but not all—of 802.11i in order to be able to communicate with older wireless cards (which might still need an update through their firmware in order to be compliant), while WPA2 implements the full standard and is not compatible with older cards.

Wireless Vulnerabilities to Know

Wireless systems are vulnerable to all the various attacks that wired networks are vulnerable to. However, because these protocols use radio frequency signals for *data emanation*, they have an additional weakness: all radio frequency signals can be easily intercepted. To intercept 802.11*x* traffic, all you need is a PC with an appropriate 802.11*x* card installed. Many networks will regularly broadcast their name (known as an *SSID broadcast*) to announce their presence. Simple software on the PC can capture the link traffic in the WAP and then process this data in order to decrypt account and password information. To secure your network, it is suggested that you disable SSID broadcasts.

An additional aspect of wireless systems is the *site survey*. Site surveys involve listening in on an existing wireless network using commercially available technologies. Doing so allows intelligence, and possibly data capture, to be performed on systems in your wireless network.

The term *site survey* initially meant determining whether a proposed location was free from interference. When used by an attacker, a site survey can determine what types of systems are in use, the protocols used, and other critical information about your network. It's the primary method used to gather data about wireless networks. Virtually all wireless networks are vulnerable to site surveys.

If wireless portals are installed in a building, the signals will frequently radiate past the inside of the building, and they can be detected and decoded outside the building using inexpensive equipment. The term *war driving* refers to driving around town with a laptop looking for WAPs that can be communicated with. The network card on the laptop is set to promiscuous mode, and it looks for signals coming from anywhere. After intruders gain access, they may steal Internet access or start damaging your data.

Weak encryption was an issue with earlier access points, but most of the newer wireless controllers use special ID numbers (SSIDs) and must be configured in the network cards to allow communications. However, using ID number configurations doesn't necessarily prevent wireless networks from being monitored, and one particularly mischievous undertaking involves taking advantage of *rogue access points*. Any wireless access point added to your network that has not been authorized is considered a rogue. The rogue may be added by an attacker, or could have been innocently added by a user wanting to enhance their environment—the problem with the user doing this is that there is a good chance they will not implement the security you would and this could open the system up for a man-in-the-middle attack.

Never assume that a wireless connection is secure. The emissions from a wireless portal may be detectable through walls and for several blocks from the portal. Interception is easy to accomplish, given that RF is the medium used for communication. Newer wireless devices offer data security, and you should use it. You can set newer WAPs and wireless routers to non-broadcast in addition to configuring WEP at a higher encryption level.

With the popularity of Bluetooth on the rise, two additional vulnerabilities have been added: *blue jacking* and *bluesnarfing*. Blue jacking is the sending of unsolicited messages (think spam) over the Bluetooth connection. While annoying, it is basically considered harmless.

Bluesnarfing is the gaining of unauthorized access through a Bluetooth connection. This access can be gained through a phone, PDA, or any device using Bluetooth. Once access has been gained, the attacker can copy any data in the same way they would with any other unauthorized access.

The Bluetooth standard has addressed weaknesses in the technology, and it continues to get more secure. One of the simplest ways to secure Bluetooth devices is to turn off their Discoverable attribute.

Basics of Hardware and Software Configuration

An *infrastructure* is the basis for all the work occurring in your organization. When discussing infrastructures, keep in mind that this includes servers, networks, network devices, workstations, and the processes in place to facilitate work.

Networks are tied together using the Internet and other network technologies. Let's look at the hardware and software components that make up a network.

Working with Hardware Components

Network hardware components include physical devices such as routers, servers, firewalls, workstations, and switches. The infrastructure is much more than just the sum of all its parts. You must evaluate your network from the standpoint of each and every device within it. It cannot be overstated: the complexity of most networks makes securing them extremely complicated.

Working with Software Components

Hardware exists to run software. The software is intended to make the hardware components easy to configure and easy to support. To a certain extent, however, that software can also make the hardware easy to bypass.

The network infrastructure includes servers, workstations running operating systems, and dedicated devices that have their own communications and control programs. Many larger organizations have built a single area for network monitoring and administrative control of systems. This centralization lets you see a larger overall picture of the network, and it lets you take actions on multiple systems or network resources if an attack is under way. Such a centralized area is called a *Network Operations Center* (NOC). NOCs are expensive and require a great deal of support: factors beyond the economy of scale of all but the largest businesses. After a NOC is developed and implemented, the job doesn't stop there—the NOC must be constantly evaluated and changed as needed.

Working with Firewalls

Aside from the basics of hardware and software configuration discussed earlier, the objectives for this domain include specific knowledge of firewall functionality. Bear in mind that a firewall will be hardware- and/or software-based. At its simplest, firewall configuration is accomplished by configuring ports and rules. A *port* is an interface that is used to connect to a device and identified by number. Throughout this book, many well-known ports have been discussed by their number (SMTP on port 25, for example).

When you use a service, the default port is implied, but you can always change the *port assignment* if you want to increase security. For example, when you attempt to connect to a website, you'll use port 80 by default. (A socket is the combination of the IP address and the port number. If you were accessing a website at 192.168.0.100, the combination of

these two elements would give you a socket; the full address and socket description would then be 192.168.0.100:80).

The assignment can be changed so that a server offers the web service at a port other than the default, such as 8080. If that is done, the service can be accessed by the client by specifying the socket: `http://192.168.0.100:8080`.

Port forwarding (also known as port mapping) is the act of mapping one port to another. This is essentially the same as what NAT does, and allows external users to access the private LAN. This is useful when you want to allow only some external users (partners, for example) to be able to access the network resources remotely. These ports can be left open all the time, or turned on only when needed. If the latter is used, this is known as *port triggering*. With triggering, an inbound attempt at connection triggers the opening of an outbound port and communication is now possible. Obviously, the trigger is activated only after all authentication measures have been successfully met.

Another aspect of firewall configuration is the establishment of rules. The *rules* are criteria given for what is allowed to pass through or connect to the network. These rules are typically accept- or deny-based (but can be configured to include exceptions). For example, you may choose to deny all connections except those specifically allowed—much better than the alternative of allowing all except those specifically denied, which creates a security nightmare.

Rules can typically be created based on the following:

- Direction, which can be inbound or outbound
- Protocol source, which can be either TCP (connection-based) or UDP (connectionless)
- Address source
- Port
- Destination address
- Destination port

If you want to limit all of any one criterion—for example, all destination ports—most firewalls allow you to use the value `any` for this purpose.

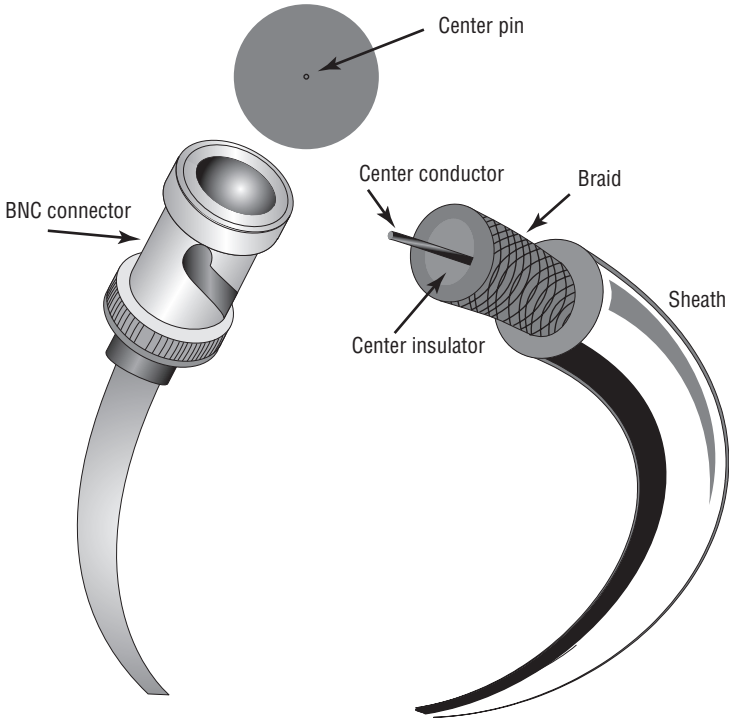
Physical Installation

Nothing happens in a network until data is moved from one place to another. Naturally, this requires some type of cable, wire, or transmission media. Next we'll explore the realm of wiring from a technical and a security perspective. Specifically, you'll learn about coaxial cable, UTP/STP, and fiber-optic media.

Coax

Coaxial cable, or *coax*, is one of the oldest media used in networks. Coax is built around a center conductor or core that is used to carry data from point to point. The center conductor has an insulator wrapped around it, a shield over the insulator, and a nonconductive sheath around the shielding. This construction, depicted in Figure 9.8, allows the conducting core to be relatively free from outside interference. The shielding also prevents the conducting core from emanating signals externally from the cable.

FIGURE 9.8 Coaxial cable construction



Before you read any further, accept the fact that the odds are incredibly slim that you will ever need to know about coax for a new installation in the real world (with the possible exception of RG-6, which is used from the wall to a cable modem). If you do come across it, it will be in an existing installation and one of the first things you'll recommend is that it be changed. That said, you do need to know about coax for this exam.

Connections to a coax occur through a wide variety of connectors, often referred to as *plumbing*. These connectors provide a modular design that allows for easy expansion. The three primary connections used in this case are the T-connector, the inline connector, and the terminating connector (also known as a *terminating resistor* or *terminator*). Figure 9.9 shows some of these common connectors in a coaxial cable–based network.

Coax supports both baseband and broadband signaling. *Baseband* signaling means that a single channel is carried through the coax, and *broadband* refers to multiple channels on the coax. Figure 9.10 illustrates this difference. Baseband signaling is similar in concept to a speaker wire. The speaker wire in your stereo connects one channel from the amplifier to the speaker. Broadband is similar to the cable TV connection in your home. The cable from the cable company carries hundreds of channels. Your TV set uses a tuner to select the channel you choose to watch.

FIGURE 9.9 Common BNC connectors

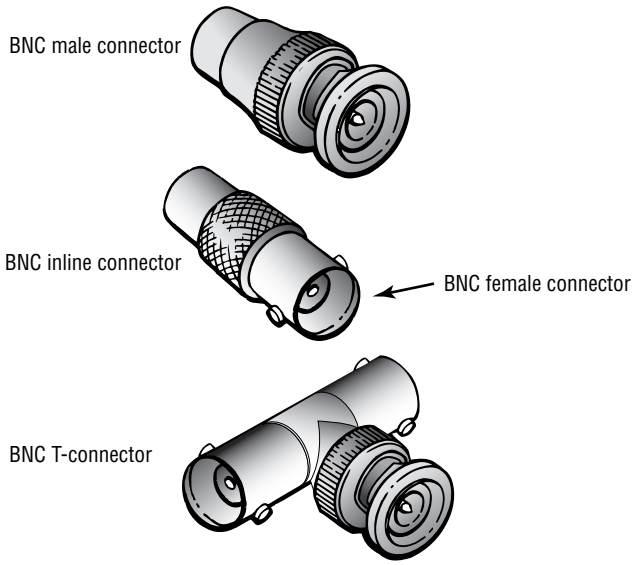
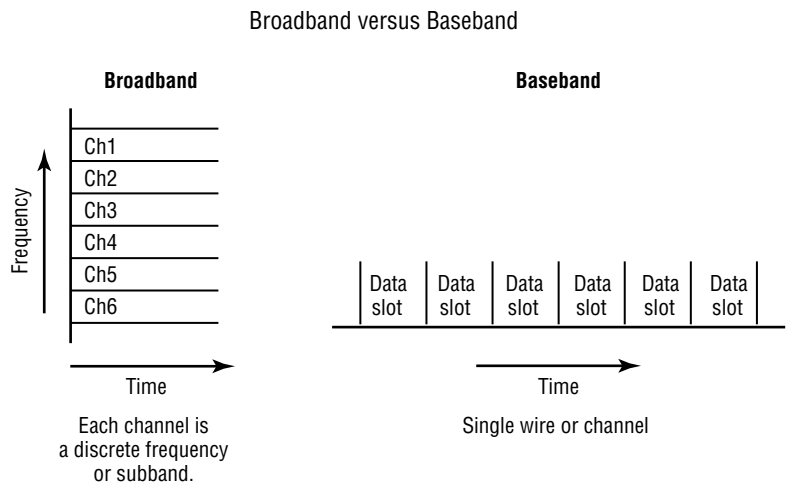


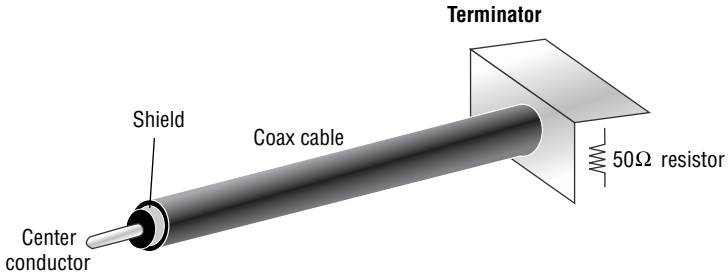
FIGURE 9.10 Baseband versus broadband signaling



In a coax network, some type of device must terminate all the coax ends. Figure 9.11 shows this termination process in more detail. Coax is present in many older networks and tends to provide reliable service once it's installed. However, if a terminator, NIC, T-connector, or inline connector malfunctions or becomes disconnected, the entire segment of wire in that network will malfunction and network services will cease operation. Coax

tends also to become brittle over time, and it can fail when handled. In addition, coax is expensive per foot when compared to UTP cable. These are the primary reasons that coax is falling from favor as a primary network media.

FIGURE 9.11 Network termination in a coax network



Coax has two primary vulnerabilities from a security perspective. The most common is the addition of a T-connector attached to a network *sniffer*. This sniffer would have unrestricted access to the signaling on the cable. The second and less common method involves a connection called a *vampire tap*. A vampire tap is a type of connection that hooks directly into a coax by piercing the outer sheath and attaching a small wire to the center conductor or core. This type of attachment allows a tap to occur almost anywhere in the network. Taps can be hard to find because they can be anywhere in the cable. Figure 9.12 shows the two common methods of tapping a coax cable. The T-connector is a standard connector that can be used any place there is a connector on the cable. An inductive pickup or RF collar can be placed around a coaxial cable to capture any stray RF that isn't blocked by the coax's shield.

Unshielded Twisted Pair and Shielded Twisted Pair

Unshielded twisted pair (UTP) and *shielded twisted pair (STP)* are the most prevalent media installed today. UTP cabling and STP cabling are similar in function, with the exception that STP wraps a shield, like a coax, over the wires. STP is popular, but UTP is by far the more popular cabling in use.

Figure 9.13 illustrates the difference between UTP and STP cable. Notice that the STP cable has a single shield around all the pairs. Some versions of STP also have shields around each pair of wires. This is much less common in computer networks, but it reduces electrical interference susceptibility in the cable.

Our discussion will revolve around UTP, but STP operates the same way. UTP cabling comes in seven grades or categories, which have been discussed previously. The most common cable standard used at this time is Category 5 (Cat-5). Cat-3 is common in older twisted-pair networks. The limit of a cable segment length of twisted-pair for use with Ethernet is 100 meters; beyond this length, the attenuation of the cables may cause reliability problems.

FIGURE 9.12 A vampire tap and a T-connector on a coax

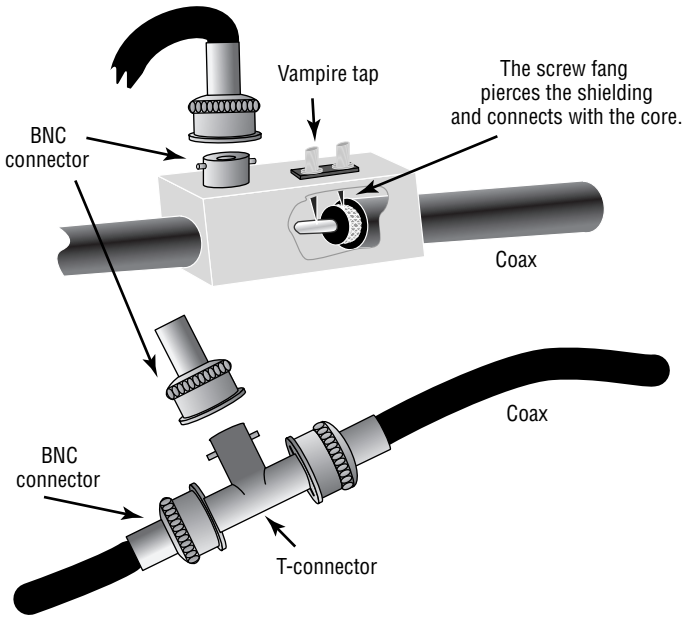
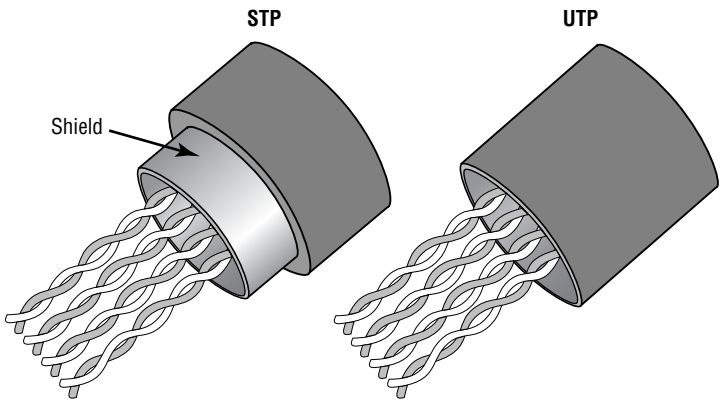


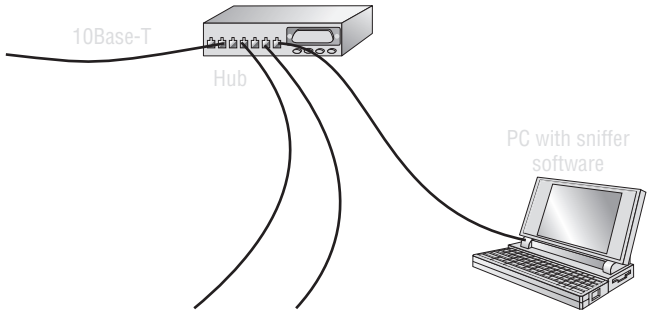
FIGURE 9.13 UTP and STP cable construction



UTP and STP cabling aren't as secure as coax because they can be easily tapped into, and they're used primarily for internal wiring. They're more difficult to splice into a twisted pair cable, but three-way breakout boxes are easy to build or buy. The common networks that use UTP are 10Base-T, 100Base-T, and 1000Base-T. These networks use

hubs for distribution, and hubs allow sniffers to be easily connected. Many modern networks include switches, and network monitoring doesn't work properly through a switch unless the switch is configured to allow it. Remember that each circuit through a switch is dedicated when switched and won't be seen on the other ports. Figure 9.14 illustrates a hub in a 10Base-T network and a sniffer attached to the hub. The sniffer in this situation is a portable PC with a NIC for the network protocol.

FIGURE 9.14 10Base-T network with a sniffer attached at the hub



Fiber Optics

Fiber-optic technology takes network bandwidth to new levels of performance. Telecommunications and data communication providers worldwide have laid fiber cables extensively. At one point, the industry claimed that fiber would surpass wire as the preferred method of making network connections. Fiber optics and their assembly continue to be very expensive when compared to wire, and this technology isn't common on the desktop.

Because fiber-optic cabling uses light in place of an electrical signal, it's less likely than other implementations to be affected by interference problems.

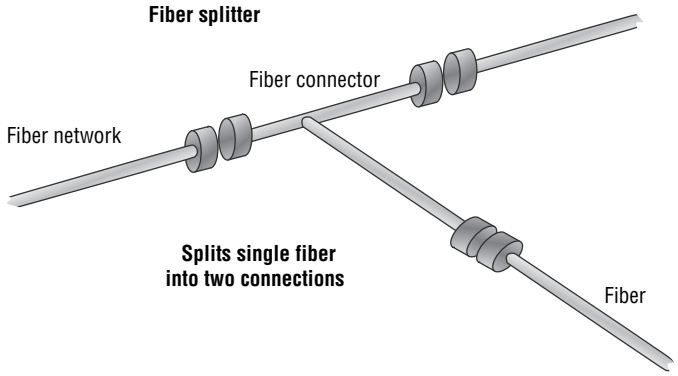
Fiber, as a media, is relatively secure because it can't be tapped. Fiber's greatest security weakness is at the connections to the fiber-optic transceivers. Passive connections can be made at the connections, and signals can be tapped from there. The other common security issue associated with fiber optics is that fiber connections are usually bridged to wire connections. Figure 9.15 shows how a fiber connection to a transceiver can be tapped. This type of splitter requires a signal regenerator for the split to function, and it can be easily detected.

Wireless Router Placement

On a wireless network, one of the most important installation concerns is the placement of the wireless router. Placing the router near a solid wall, for example, will reduce the signal in that direction. This can be useful if you are trying to keep the signal from leaving the building, but harmful if the wall in question is in the middle of your office. Under ideal

circumstances, the router should be placed in the middle of the circle that you want to be the coverage area and at a height where it is unobstructed by solid objects (which can be high, low, or shelf-level, based on your work area).

FIGURE 9.15 An inline fiber splitter



Metal objects can hamper the signal from the router, as can most solid building materials (brick walls, concrete, etc.). You also want to avoid placing the router near such devices as microwave ovens that have the potential to cause interference.

Exam Essentials

Know the protocols and components of a wireless system. The backbone of most wireless systems is WAP. WAP can use the WEP protocol to provide security in a wireless environment. WTLS is the security layer of WAP. WAP and TCP/IP perform similarly.

Know the capabilities and limitations of the 802.11*x* network standards. The current standards for wireless protocols are 802.11, 802.11a, 802.11b, and 802.11g. The 802.11n standard is undergoing review and isn't yet a formal standard.

Know the vulnerabilities of wireless networks. The primary method of gaining information about a wireless network is a site survey. Site surveys can be accomplished with a PC and an 802.11 card. Wireless networks are subject to the same attacks as wired networks.

Know the definitions for various networking protocols. You should be familiar with all the protocols and technologies listed in this chapter and able to differentiate between them.

Know the connectivity options. Be able to discriminate between various options based on definitions given.

Review Questions

1. Which network service is used in TCP/IP networks to translate hostnames to IP addresses?
2. What cabling media is relatively secure because it can't be tapped?
3. Which port does HTTPS use by default?
4. What IP address is known as the loopback address?
5. What do wireless networks broadcast to signify their presence?
6. What protocol in TCP/IP transfers mail between servers?
7. Which two protocols can clients use to access e-mail on servers?
8. What are the two types of signaling that coax supports?
9. What technologies were designed to address the core problems with WEP?
10. What is the routing of voice traffic over the Internet called?

Answers to Review Questions

1. DNS is the network service used in TCP/IP networks to translate hostnames to IP addresses.
2. Fiber-optic cabling.
3. HTTPS uses port 443 by default.
4. The loopback address is 127.0.0.1.
5. SSID.
6. Simple Mail Transfer Protocol (SMTP) is used to send mail between servers.
7. Post Office Protocol (POP) and Internet Message Access Protocol (IMAP) can be used by clients to access e-mail.
8. Coax supports both baseband and broadband signaling.
9. The Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access 2 (WPA2) technologies were designed to address the core problems with WEP.
10. Voice over IP (VoIP) is the routing of voice traffic over the Internet (it could be across any smaller IP-based network, but generally it's the Internet).

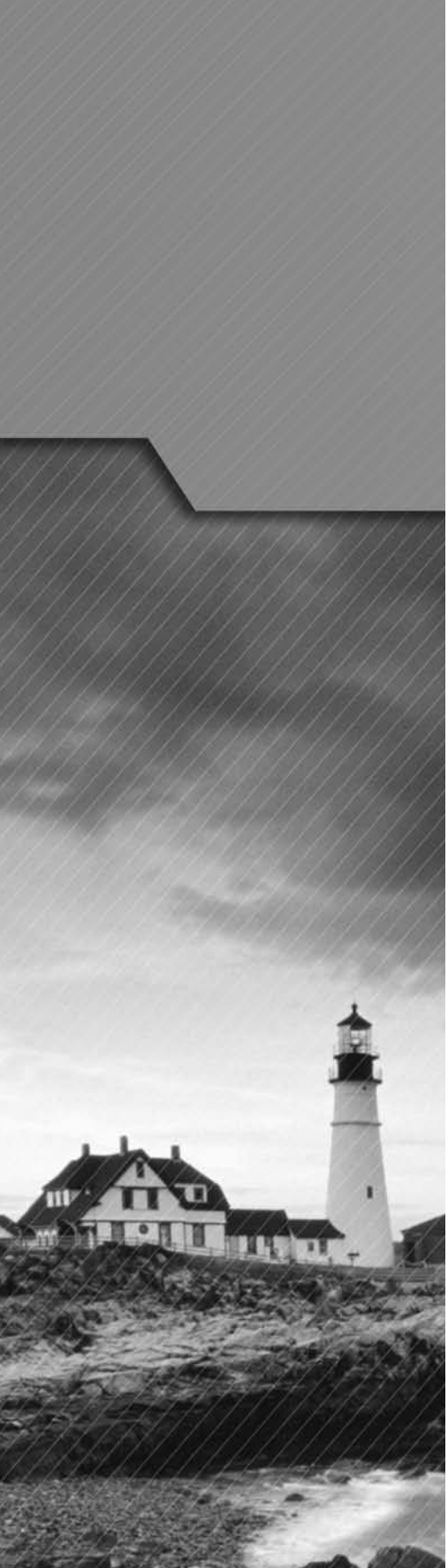
Chapter

10

Security

COMPTIA A+ PRACTICAL APPLICATION EXAM OBJECTIVES COVERED IN THIS CHAPTER:

- ✓ **4.1 Given a scenario, prevent, troubleshoot and remove viruses and malware**
  - Use antivirus software
  - Identify malware symptoms
  - Quarantine infected systems
  - Research malware types, symptom and solutions (virus encyclopedias)
  - Remediate infected systems
  - Update antivirus software
    - Signature and engine updates
    - Automatic vs. manual
  - Schedule scans
  - Repair boot blocks
  - Scan and removal techniques
    - Safe mode
    - Boot environment
  - Educate end user
- ✓ **4.2 Implement security and troubleshoot common issues**
  - Operating systems
    - Local users and groups: Administrator, Power Users, Guest, Users
    - Vista User Access Control (UAC)
    - NTFS vs. Share permissions
      - Allow vs. deny
      - Difference between moving and copying folders and files
      - File attributes



- Shared files and folders
  - Administrative shares vs. local shares
  - Permission propagation
  - Inheritance
- System files and folders
- Encryption (Bitlocker, EFS)
- User Authentication

- System
  - BIOS security
    - Drive lock
    - Passwords
    - Intrusion detection
    - TPM

This domain has been elevated from the 2006 version of the IT Technician exam, where its weight was 8 percent, to the 2009 version, where it is now worth 13 percent. There is a fair amount of overlap between these objectives and the ones you need to know for the Essentials exam. Rather than repeating that information verbatim, the focus here is on the implementation of security in the operating systems.

It's highly recommended that you read Chapter 5, "Security," in addition to this chapter as you study for the Practical Application exam.

Viruses and Malware

We've all been battling malicious, invasive software since we bought our first computers. This software can go by any number of names—virus, malware, and so on—but if you aren't aware of their presence, these uninvited intruders may damage the data on your hard disk, destroy your operating system, and possibly spread to other systems.

Critical Information

You want to make certain that your systems, and the data within them, are kept as secure as possible. The security prevents others from changing the data, destroying it, or inadvertently harming it.

Viruses can be classified as polymorphic, stealth, retroviruses, multipartite, armored, companion, phage, and macro viruses. Each type of virus has a different attack strategy and different consequences.

Estimates for losses due to viruses are in the billions of dollars. These losses include financial loss as well as lost productivity.

The following sections will introduce the symptoms of a virus infection, explain how a virus works, and describe the types of viruses you can expect to encounter and how they generally behave. I'll also discuss how a virus is transmitted through a network and look at a few hoaxes.

Symptoms of a Virus/Malware Infection

Many viruses will announce that you're infected as soon as they gain access to your system. They may take control of your system and flash annoying messages on your screen or destroy your hard disk. When this occurs, you'll know that you're a victim. Other viruses will cause your system to slow down, cause files to disappear from your computer, or take over your disk space.

Because viruses are the most common malware, the term *virus* is used in this section.

You should look for some of the following symptoms when determining if a virus infection has occurred:

- The programs on your system start to load more slowly. This happens because the virus is spreading to other files in your system or is taking over system resources.
- Unusual files appear on your hard drive, or files start to disappear from your system. Many viruses delete key files in your system to render it inoperable.
- Program sizes change from the installed versions. This occurs because the virus is attaching itself to these programs on your disk.
- Your browser, word-processing application, or other software begins to exhibit unusual operating characteristics. Screens or menus may change.
- The system mysteriously shuts itself down or starts itself up and does a great deal of unanticipated disk activity.
- You mysteriously lose access to a disk drive or other system resources. The virus has changed the settings on a device to make it unusable.
- Your system suddenly doesn't reboot or gives unexpected error messages during startup.

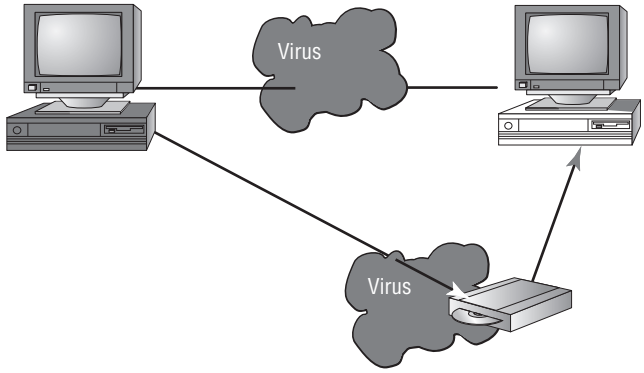
This list is by no means comprehensive. What is an absolute, however, is the fact that you should immediately quarantine the infected system. It is imperative that you do all you can to contain the virus and keep it from spreading to other systems within your network, or beyond.

How Viruses Work

A virus, in most cases, tries to accomplish one of two things: render your system inoperable or spread to other systems. Many viruses will spread to other systems given the chance and then render your system unusable. This is common with many of the newer viruses.

If your system is infected, the virus may try to attach itself to every file in your system and spread each time you send a file or document to other users. Figure 10.1 shows a virus spreading from an infected system either through a network or by removable media. When you give removable media to another user or put it into another system, you then infect that system with the virus.

FIGURE 10.1 Virus spreading from an infected system using the network or removable media



Most viruses today are spread using e-mail. The infected system attaches a file to any e-mail that you send to another user. The recipient opens this file, thinking it's something you legitimately sent them. When they open the file, the virus infects the target system. The virus might then attach itself to all the e-mails the newly infected system sends, which in turn infects the recipients of the e-mails. Figure 10.2 shows how a virus can spread from a single user to literally thousands of users in a very short time using e-mail.

Types of Viruses

Viruses take many different forms. The following sections briefly introduce these forms and explain how they work. These are the most common types, but this isn't a comprehensive list.

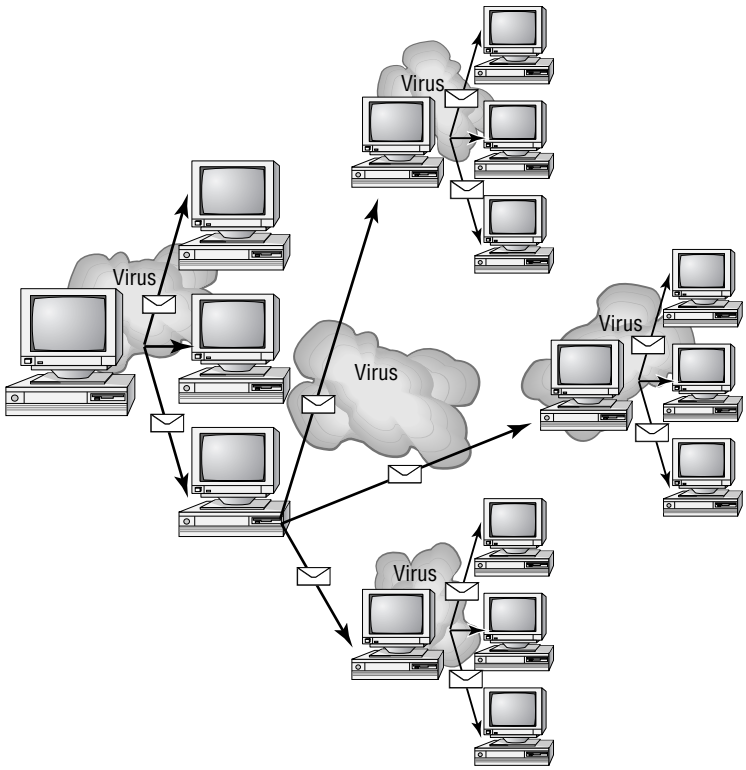
The best defense against a virus attack is up-to-date antivirus software installed and running. The software should be on all workstations as well as the server.

Armored Virus

An *armored virus* is designed to make itself difficult to detect or analyze. Armored viruses cover themselves with protective code that stops debuggers or disassemblers from examining critical elements of the virus. The virus may be written in such a way that some aspects of the programming act as a decoy to distract analysis while the actual code hides in other areas in the program.

From the perspective of the creator, the more time it takes to deconstruct the virus, the longer it can live. The longer it can live, the more time it has to replicate and spread to as many machines as possible. The key to stopping most viruses is to identify them quickly and educate administrators about them—the very things that the armor intensifies the difficulty of accomplishing.

FIGURE 10.2 An e-mail virus spreading geometrically to other users



Companion Virus

A *companion virus* attaches itself to legitimate programs and then creates a program with a different filename extension. This file may reside in your system's temporary directory. When a user types the name of the legitimate program, the companion virus executes instead of the real program. This effectively hides the virus from the user. Many of the viruses that are used to attack Windows systems make changes to program pointers in the Registry so that they point to the infected program. The infected program may perform its dirty deed and then start the real program.

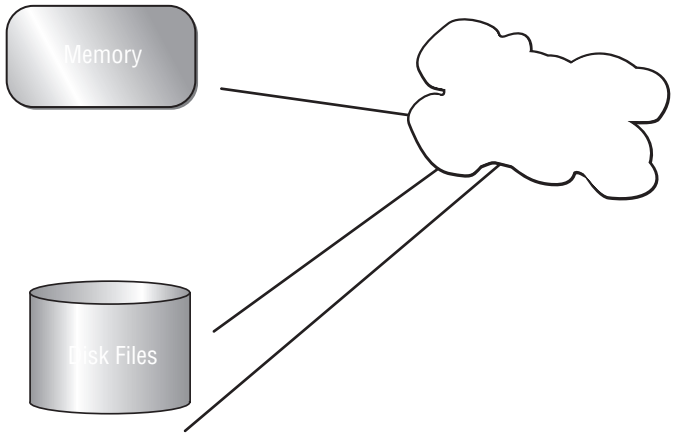
Macro Virus

A *macro virus* exploits the enhancements made to many application programs. Programmers can expand the capability of applications such as Microsoft Word and Excel. Word, for example, supports a mini-BASIC programming language that allows files to be manipulated automatically. These programs in the document are called *macros*. For example, a macro can tell your word processor to spell-check your document automatically when it opens. Macro viruses can infect all the documents on your system and spread to other systems via e-mail or other methods. Macro viruses are the fastest-growing exploitation today.

Multipartite Virus

A *multipartite virus* attacks your system in multiple ways. It may attempt to infect your boot sector, infect all of your executable files, and destroy your application files. The hope here is that you won't be able to correct all the problems and will allow the infestation to continue. The multipartite virus in Figure 10.3 attacks your boot sector, infects application files, and attacks your Word documents.

FIGURE 10.3 A multipartite virus commencing an attack on a system



Phage Virus

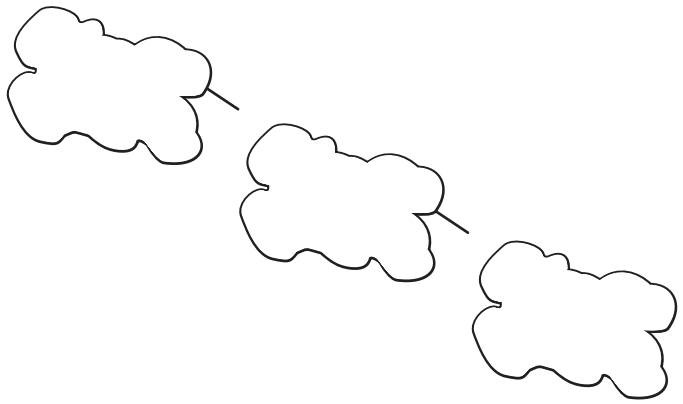
A *phage virus* modifies and alters other programs and databases. The virus infects all of these files. The only way to remove this virus is to reinstall the programs that are infected. If you miss even a single incident of this virus on the victim system, the process will start again and infect the system once more.

Polymorphic Virus

Polymorphic viruses change form in order to avoid detection. These types of viruses attack your system, display a message on your computer, and delete files on your system. The virus will attempt to hide from your antivirus software. Frequently, the virus will encrypt parts of itself to avoid detection. When the virus does this, it's referred to as *mutation*. The mutation process makes it hard for antivirus software to detect common characteristics of the virus. Figure 10.4 shows a polymorphic virus changing its characteristics to avoid detection. In this example, the virus changes a signature to fool antivirus software.

A *signature* is an algorithm or other element of a virus that uniquely identifies it. Because some viruses have the ability to alter their signature, it is crucial that you keep signature files current, whether you choose to manually download them or configure the antivirus engine to do so automatically.

FIGURE 10.4 The polymorphic virus changing its characteristics



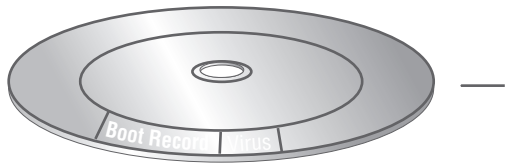
Retrovirus

A *retrovirus* attacks or bypasses the antivirus software installed on a computer. You can consider a retrovirus to be an anti-antivirus. Retroviruses can directly attack your antivirus software and potentially destroy the virus definition database file. Destroying this information without your knowledge would leave you with a false sense of security. The virus may also directly attack an antivirus program to create bypasses for itself.

Stealth Virus

A *stealth virus* attempts to avoid detection by masking itself from applications. It may attach itself to the boot sector of the hard drive. When a system utility or program runs, the stealth virus redirects commands around itself in order to avoid detection. An infected file may report a file size different from what is actually present in order to avoid detection. Figure 10.5 shows a stealth virus attaching itself to the boot sector to avoid detection. Stealth viruses may also move themselves from fileA to fileB during a virus scan for the same reason.

FIGURE 10.5 A stealth virus hiding in a disk boot sector



An updated list of the most active viruses and spyware is on the Panda Software site at `http://www.pandasecurity.com`.

Virus Transmission in a Network

Upon infection, some viruses destroy the target system immediately. The saving grace is that the infection can be detected and corrected. Some viruses won't destroy or otherwise tamper with a system; they use the victim system as a carrier. The victim system then infects servers, file shares, and other resources with the virus. The carrier then infects the target system again. Until the carrier is identified and cleaned, the virus continues to harass systems in this network and spread.

Present Virus Activity

New viruses and threats are released on a regular basis to join the cadre of those already in existence. From an exam perspective, you need only be familiar with the world as it existed at the time the questions were written. From an administrative standpoint, however, you need to know what is happening today.

To find this information, visit the CERT/CC Current Activity web page at `http://www.us-cert.gov/current/current_activity.html`. Here you'll find a detailed description of the most current viruses as well as links to pages on older threats.

Antivirus Software

The primary method of preventing the propagation of malicious code involves the use of *antivirus software*. Antivirus software is an application that is installed on a system to protect it and to scan for viruses as well as worms and Trojan horses. Most viruses have characteristics that are common to families of virus. Antivirus software looks for these characteristics, or fingerprints, to identify and neutralize viruses before they impact you.

More than 200,000 known viruses, worms, bombs, and other malware have been defined. New ones are added all the time. Your antivirus software manufacturer will usually work very hard to keep the definition database files current. The definition database file contains all of the known viruses and countermeasures for a particular antivirus software product. You probably won't receive a virus that hasn't been seen by one of these companies. If you keep the virus definition database files in your software up-to-date, you probably won't be overly vulnerable to attacks.

The best method of protection is to use a layered approach. Antivirus software should be at the gateways, at the servers, and at the desktop. If you want to go one step further, you can use software at each location from different vendors to make sure you're covered from all angles.

The second method of preventing viruses is education. Teach your users not to open suspicious files and to open only those files that they're reasonably sure are virus-free. They

need to scan every disk, e-mail, and document they receive before they open them. You should also have all workstations scheduled to be automatically scanned on a regular basis.

A Virus Out of Control

A large private university has over 30,000 students taking online classes. These students use a variety of systems and network connections. The instructors of this university are being routinely hit with the Klez32 virus. Klez32 (specifically, in this case, the W32/Klez.H@mm virus) is a well-known and documented virus. It uses Outlook or Outlook Express to spread. It grabs a name randomly from the address book and uses that name in the header. The worm then uses a mini-mailer and mails the virus to all the people in the address book. When one of these users opens the file, the worm attempts to disable their antivirus software and spread to other systems. Doing so opens the system to an attack from other viruses, which might follow later.

You've been appointed to the IT department at this school, and you've been directed to solve this problem. Ponder what you can do about it.

The best solution would be to install antivirus software that scans and filters all e-mails that come through the school's servers. You should also inspect outgoing e-mail and notify all internal users of the system when they attempt to send a virus-infected document using the server.

These two steps—installing antivirus scanners on the external and internal connections and notifying unsuspecting senders—would greatly reduce the likelihood that the virus could attack either student or instructor computers.

You can educate yourself and stay current on malware types, symptoms, and solutions by consulting the virus encyclopedia at `http://www.viruslist.com/en/viruslist.html`.

Recovering Operating Systems

Windows includes a number of tools to simplify recovering an operating system after a serious problem has occurred. System Restore is one such tool, as discussed previously. Three others we'll look at here are the Recovery Console, Automated System Recovery (ASR), and emergency repair disks (ERDs).

Recovery Console

The Recovery Console is a command-line utility used for troubleshooting Windows 2000 and Windows XP. From it, you can format drives, stop and start services, and interact with files. The latter is extremely important because many boot/command-line utilities bring you into a position where you can interact with files stored on FAT or FAT32, but not NTFS. The Recovery Console can work with files stored on all three file systems.

The Recovery Console isn't installed on a system by default. To install it, use the following steps:

1. Place the Windows CD in the system.
2. From a command prompt, change to the `i386` directory of the CD.
3. Type **winnt32 /cmdcons**.
4. A prompt appears, alerting you to the fact that 7MB of hard drive space is required and asking if you want to continue. Click Yes.

Upon successful completion of the installation, the Recovery Console (Microsoft Windows 2000 Recovery Console, for example) is added as a menu choice at the bottom of the Startup menu that appears when you press F8 during startup. To access it, you must choose it from the list at startup. If more than one installation of Windows 2000 or any Windows NT–based operating system exists on the system, another boot menu will appear, asking which you want to boot into, and you must make a selection to continue.

To perform this task, you must give the administrator password. You'll then arrive at a command prompt. You can give a number of commands from this prompt, two of which are worth special attention: `EXIT` restarts the computer, and `HELP` lists the commands you can give. Table 10.1 lists the other commands available, most of which will be familiar to administrators who have worked with MS-DOS.

TABLE 10.1 Recovery Console Commands

Command	Purpose
`ATTRIB`	Shows the current attributes of a file or folder, and lets you change them.
`BATCH`	Runs the commands within an ASCII text file.
`CD`	Used without parameters, it shows the current directory. Used with parameters, it changes to the directory specified.
`CHDIR`	Works the same as `CD`.
`CHKDSK`	Checks the disk for errors.
`CLS`	Clears the screen.
`COPY`	Allows you to copy a file (or files, if used with wildcards) from one location to another.
`DEL`	Deletes a file.
`DELTREE`	Recursively deletes files and directories.
`DIR`	Shows the contents of the current directory.

TABLE 10.1 Recovery Console Commands *(continued)*

Command	Purpose
DISABLE	Allows you to stop a service/driver.
DISKPART	Shows the partitions on the drive, and lets you manage them.
EXPAND	Extracts compressed files.
ENABLE	Allows you to start a service/driver.
FIXBOOT	Writes a new boot sector.
FIXMBR	Checks and fixes (if possible) the master boot record.
FORMAT	Allows you to format a floppy or partition.
LISTSVC	Shows the services/drivers on the system.
LOGON	Lets you log on to Windows 2000.
MAP	Shows the maps currently created.
MD	Makes a new folder/directory.
MKDIR	Works the same as MD.
MORE	Shows only one screen of a text file at a time.
RD	Removes a directory or folder.
REN	Renames a file or folder.
RENAME	Works the same as REN.
RMDIR	Works the same as RD.
SYSTEMROOT	Works like CD but takes you to the system root of whichever OS installation you're logged on to.
TYPE	Displays the contents of an ASCII text file.

During the installation of the Recovery Console, a folder named `Cmdcons` is created in the root directory to hold the executable files and drivers it needs. A file named `Cmldr`, with attributes of System, Hidden, and Read-Only, is also placed in the root directory.

If you want to delete the Recovery Console (to prevent users from playing around, for example), you can do so by deleting the `Cmldr` file and the `Cmdcons` folder, and removing the entry from the `Boot.ini` file.

System Recovery Options

The Recovery Console that existed in Windows 2000 and Windows XP has been removed from Vista. In its place is the System Recovery Options menu that appears on the installation disk. While renamed, it serves the same purpose of allowing you to troubleshoot startup problems or restore your system.

To access this feature, restart your system using the installation disk. At the language settings, choose your language and click Next. On the following menu, choose Repair Your Computer. Choose which operating system you are having a problem with (if more than one is installed) and click Next. The System Recovery Options menu will open and you can then choose any tool from the menu and run it. The tools available on the System Recovery Options menu are listed in Table 10.2.

Some manufacturers preinstall the recovery options. If this is the case with your computer, press F8 as the computer restarts, before the Windows logo. On the Advanced Boot Options screen that appears, choose Repair Your Computer.

TABLE 10.2 System Recovery Options Tools

Command	Purpose
`Command Prompt`	Offers access to the tools that were available in the Recovery Console and listed in Table 10.1
`Startup Repair`	Used to fix problem with startup, such as missing operating system files
`System Restore`	Allows you to restore the system to a saved restore point
`Windows Complete PC Restore`	Copies all the files from a backup and overwrites anything currently on the system
`Windows Memory Diagnostic Tool`	Checks the memory for errors

Automated System Recovery and Backups

It's possible to automate the process of creating a system recovery set by choosing the ASR Wizard on the Tools menu of the Backup utility (Start ➢ All Programs ➢ Accessories ➢ System

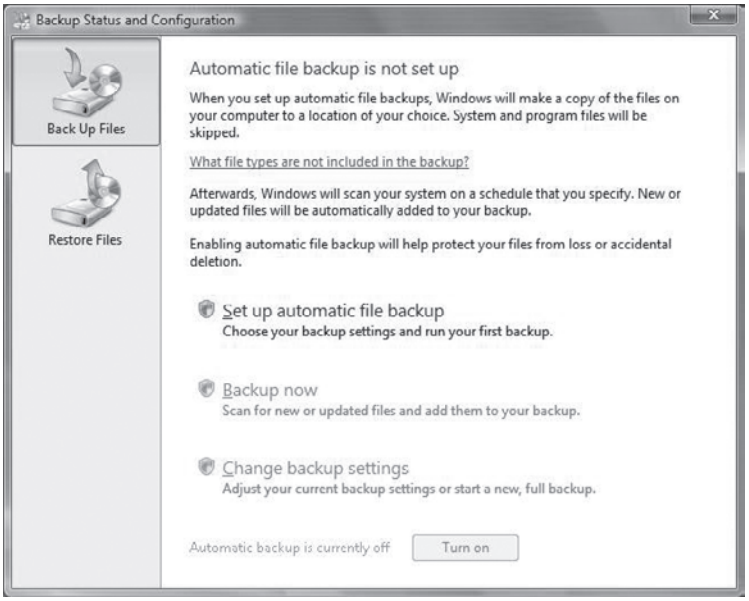
Tools ➢ Backup). Windows XP includes a wizard that walks you through the process of creating a disk that can be used to restore parts of the system in the event of a major system failure.

The default name of this file is `BACKUP.BKF`; it requires a floppy disk. The backup set contains all the files necessary for starting the system.

ASR exists only in Windows XP and replaced the ERD (Emergency Repair Disk) that existed in Windows 2000 (discussed later). The nearest equivalent to this in Windows Vista is the Windows Recovery Environment.

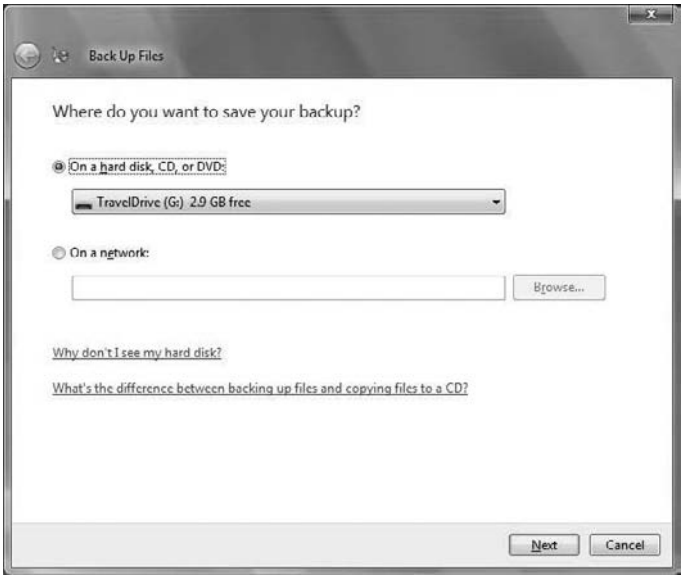
With all versions of Windows, it is important to regularly do backups of some type. In Windows Vista, the Backup utility (NTBACKUP) has been changed to Backup Status And Configuration, as shown in Figure 10.6. You must configure automatic backup before you are allowed to perform any other actions in this tool. As soon as you choose this, you are prompted where you want to save your backup to (as shown in Figure 10.7), with choices falling into the category of local or on the network. For obvious reasons, you cannot back up the data from one drive to another location on that drive.

FIGURE 10.6 You must configure automatic backup in Windows Vista.



The dialog boxes walk you through selecting what you want to back up, and how often you want to do so. Once you've configured this utility, you can access it at any time and change the settings or choose to manually do a backup now.

FIGURE 10.7 The backup can be done locally or to the network.



Emergency Repair Disk (Windows 2000 only)

In Windows 2000, the Windows Backup And Recovery Tool/Wizard allows you to create an emergency repair disk (ERD). As the name implies, this is a disk you can use to repair a portion of the system in the event of a failure.

When you choose this option, the tab changes to the Backup tab, and a prompt tells you to install a blank, formatted floppy disk. A check box inquires whether you want to save the Registry as well. (The default is no.) If you don't choose to save the Registry, the following files are placed on the floppy disk:

- `SETUP.LOG`
- `CONFIG.NT`
- `AUTOEXEC.NT`

This doesn't leave you much to work with. The disk isn't bootable and contains only three minor configuration utilities.

If you check the box to include the Registry in the backup, the floppy disk contains the preceding files plus the following:

- `SECURITY._`
- `SOFTWARE._`
- `SYSTEM._`
- `DEFAULT._`
- `SAM._`

- NTUSER.DAT
- USRCLASS.DAT

The user profile (NTUSER.DAT) is for the default user; the files with the ._ extension are compressed files from the Registry. The compression utility used is EXPAND.EXE, which offers you the flexibility of restoring any or all files from any Microsoft operating system, including this utility (Windows 95/98, Windows NT, and so on). Because this floppy contains key Registry files, it's important that you label it appropriately and store it in a safe location, away from users who should not have access to it.

During the process of creating the backup, the Registry files are also backed up (in uncompressed state) to %systemroot%\repair\RegBack.

As before, the floppy isn't bootable, and you must bring the system up to a point (booted) where the floppy can be accessed before it's of any use.

Diagnostic Tools

Most of the tools discussed in this section have already been covered elsewhere in this chapter. Those that have not already been addressed are the boot menu and System File Checker.

Safe Mode

If, when you boot, Windows won't come all the way up (it hangs or is otherwise corrupted), you can often solve the problem by booting into Safe Mode. Safe Mode is a concept borrowed from Windows 95 wherein you can bring up part of the operating system by bypassing the settings, drivers, or parameters that may be causing it trouble during a normal boot. The goal of Safe Mode is to provide an interface with which you're able to fix the problems that occur during a normal boot and then reboot in normal mode.

To access Safe Mode, you must press F8 when the operating system starts/restarts. If you have multiple operating systems installed, it will be a choice on the menu that is displayed during the boot process. A menu of Safe Mode choices will then appear, as listed in Table 10.3. Select the mode you want to boot into.

TABLE 10.3 Safe Mode Startup Menu

Choice	Purpose
Safe Mode	Provides the VGA monitor, Microsoft mouse drivers, and basic drivers for the keyboard (storage system services, no networking)
Safe Mode With Networking	Same as Safe Mode, but with networking
Safe Mode With Command Prompt	Same as Safe Mode, but without the interface and drivers/services associated with it

TABLE 10.3 Safe Mode Startup Menu *(continued)*

Choice	Purpose
Enable Boot Logging	Creates `ntbtlog.txt` in the %systemroot% directory during any boot—normal attempted
Enable VGA Mode	Normal boot with only basic video drivers
Last Known Good Configuration	Uses the last backup of the Registry to bypass corruption caused during the previous session
Debugging Mode	Sends information through the serial port for interpretation/troubleshooting at another computer
Boot Normally	Bypasses any of the options here
Return to OS Choices Menu	Gives you an out in case you pressed F8 by accident. This option only appears if you have multiple operating systems installed.

You need to keep a few rules in mind when booting in different modes:

- If problems don't exist when you boot to Safe Mode but do exist when you boot to normal mode, the problem isn't with basic services or drivers.
- If the system hangs when you load drivers, the log file can show you the last driver it attempted to load, which is usually the cause of the problem.
- If you can't solve the problem with Safe Mode, restore the Registry from the ERD with Windows 2000 (bear in mind that doing so will lose all changes that have occurred since you created the last ERD) ASR with Windows XP. You can use System Restore points with the Vista Windows Recovery Environment.

System File Checker

The purpose of this utility is to keep the operating system alive and well. `SFC.EXE` automatically verifies system files after a reboot to see if they were changed to unprotected copies. If an unprotected file is found, it's overwritten by a stored copy of the system file from `%systemroot%\system32\dllcache`. (`%systemroot%` is the folder in which the operating system was installed.)

Storing system files (some of which can be quite large) in two locations consumes a large amount of disk space. When you install an operating system, make sure you leave ample hard drive space on the `%systemroot%` drive for growth.

Only users with the Administrator group permissions can run SFC. It also requires the use of a parameter. The valid parameters are listed in Table 10.4:

TABLE 10.4 SFC Options

Parameter	Function
/CACHESIZE=	Sets the size of the file cache
/CANCEL	Stops all checks
/ENABLE	Returns to normal mode
/PURGECACHE	Clears the cache
/QUIET	Replaces files without prompting
/SCANBOOT	Checks system files on every boot
/SCANNOW	Checks system files now
/SCANONCE	Checks system files at the next boot

System Restore

Windows XP and Windows Vista use the concept of restore points. By default, each operating system automatically creates restore points that you can revert to if a problem occurs with one difference being that Windows XP must run a system restore through the operating system (no operating system = no restore). You can access the settings for this feature (and even turn it off if you are foolish enough to choose to do so) from the System applet in Control Panel. In Windows XP, the settings are on the System Restore tab. In Windows Vista, you access the settings by clicking the System Protection menu choice to open the dialog box shown in Figure 10.8 (if you do not see this option, choose the System Protection tab in the System Properties dialog box).

FIGURE 10.8 Automatic restore points are created by default in Windows Vista.

Clicking the System Restore button brings up the wizard, allowing you to choose the most current restore point or opt for an older one (the idea is that you will pick the most recent one that you know to be good). You can click the Create button to manually choose to create a restore point right now—something you do before making significant changes to the operating system settings.

With both Windows XP and Windows Vista, choose Start ➢ All Programs ➢ Accessories ➢ System Tools ➢ System Restore and you can manually initiate the creation of a restore point, or choose to restore one. You must be a member of Computer Administrators to run System Restore.

Exam Essentials

Know the recovery options. Be familiar with the recovery console, ASR, and ERD.

Know the boot menu options. Know how to access the boot menu and what options appear there.

Know the characteristics and types of viruses used to disrupt systems and networks. Several different types of viruses are floating around today. The most common ones are polymorphic viruses, stealth viruses, retroviruses, multipartite viruses, and macro viruses.

Be able to describe how antivirus software operates. Antivirus software looks for a signature in the virus to determine what type of virus it is. The software then takes action to neutralize the virus based on a virus definition database. Virus definition database files are regularly made available on vendor sites.

Security and Troubleshooting

Hardening is the process of reducing or eliminating weaknesses, securing services, and attempting to make your environment immune to attacks. Typically, when you install operating systems, applications, and network products, the defaults from the manufacturer are to make the product as simple to use as possible and allow it to work with your existing environment as effortlessly as possible. That isn't always the best scenario when it comes to security.

Critical Information

You want to make certain that your systems, and the data within them, are kept as secure as possible. The security prevents others from changing the data, destroying it, or inadvertently harming it. This can be done by assigning users the least privileges possible in the

Administrator/Power Users/Users/Guest hierarchy and hardening as much of the environment as possible.

Hardening the OS

Any network is only as strong as its weakest component. Sometimes, the most obvious components are overlooked, and it's your job as a security administrator to make certain that doesn't happen. You must make sure the operating systems running on the workstations and on the network servers are as secure as they can be.

Hardening an operating system (OS) refers to the process of making the environment more secure from attacks and intruders. This section discusses hardening an OS and the methods of keeping it hardened as new threats emerge. This section will also discuss some of the vulnerabilities of the most popular operating systems and what can be done to harden those OSs.

Hardening Microsoft Windows 2000

Windows 2000 entered the market at the millennium. It includes workstation and several server versions. The market has embraced these products, and they offer reasonable security when updated. Windows 2000 provides a Windows Update icon on the Start menu; this icon allows you to connect to the Microsoft website and automatically download and install updates. A large number of security updates are available for Windows 2000—make sure they're applied.

In the Windows environment, the Services manager or applet is one of the primary methods (along with policies) used to disable a service.

The server and workstation products operate in a manner similar to Windows NT 4. These products run into the most security-related problems when they're bundled with products that Microsoft has included with them. Some of the most attack-prone products include Internet Information Server (IIS), FTP, and other common web technologies. Make sure these products are disabled if they aren't needed, and keep them up-to-date with the most recent security and service packs.

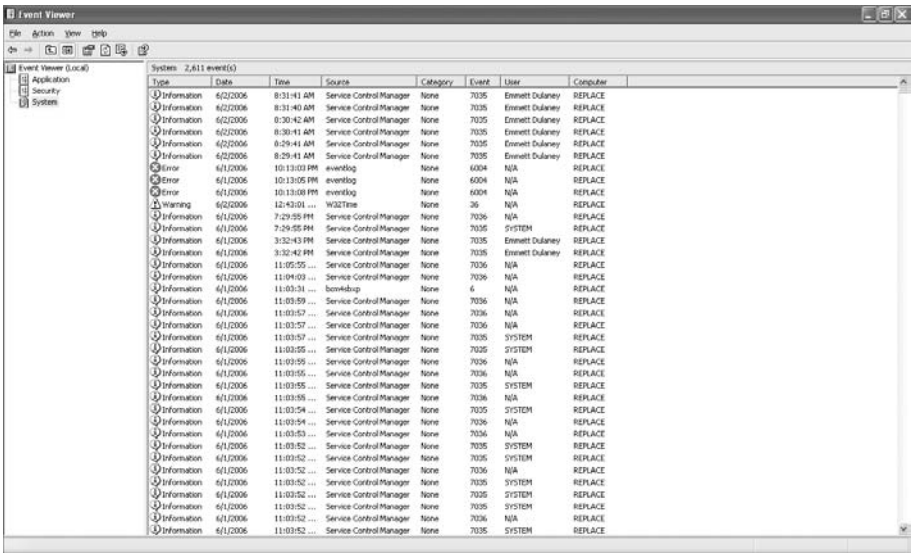
Many security updates have been issued for Windows 2000. The Microsoft TechNet and Security websites provide tools, whitepapers, and materials to help secure Windows 2000 systems.

You can find the Microsoft TechNet website at `http://technet.microsoft.com/default.aspx`. The Microsoft security website is at `http://www.microsoft.com/security/`.

Windows 2000 includes extensive system logging, reporting, and monitoring tools. These tools help make the job of monitoring security fairly easy. In addition, Windows 2000 provides a great deal of flexibility in managing groups of users, security attributes, and access control to the environment.

The Event Viewer is the main tool for reviewing logs in Windows 2000. Figure 10.9 shows a sample Event Viewer log. A number of different types of events can be logged using the Event Viewer, and administrators can configure the level of events that are logged.

FIGURE 10.9 Event Viewer log of a Windows 2000 system



Another important security tool is Performance Monitor. As an administrator of a Windows 2000 network, you must know how to use Performance Monitor. This tool can be a lifesaver when you're troubleshooting problems and looking for resource-related issues.

Windows 2000 servers can run a technology called *Active Directory (AD)*, which lets you control security configuration options of Windows 2000 systems in a network. Unfortunately, you won't be able to take advantage of the full power of AD unless all the systems in your network are running Windows 2000 or higher.

Hardening Microsoft Windows XP

Windows XP functions as a replacement for both the Windows 9*x* family and Windows 2000 Professional. There are multiple versions of Windows XP, including the Home, Media Center, and Professional editions.

The Windows XP Home edition was intended specifically to replace Windows 9*x* clients and could be installed either as an upgrade from Windows 9*x* or as a fresh installation on new systems. Media Center adds entertainment options (such as a remote control for TV), and Windows XP Professional is designed for the corporate environment. Windows XP Professional has the ability to take advantage of the security possible from Windows 200*x* servers running Active Directory.

With Microsoft's increased emphasis on security, it's reasonable to expect that the company will be working hard to make this product secure. At the time of this writing, the

third service pack for XP is available. The service packs fix minor security openings within the operating system, but nothing substantial has been reported as a weakness with XP.

Hardening Windows Vista

The update for Microsoft's Windows XP line of products is Windows Vista, which is also available in a number of editions. This product added or enhanced a number of security features, such as the following:

- Internet Connection Firewall (now called the Windows Firewall)
- Wireless connections
- Software restriction policies
- Encryption and cryptography enhancements

The best method of hardening the operating system, however, is to keep each implementation of it current. As of this writing, two service packs have been released. The latest service pack should be installed in every installation, and as an administrator, you should routinely monitor any security patches or updates released by Microsoft at the Windows Security Blog (`http://windowsteamblog.com/blogs/windowssecurity/default.aspx`).

You can find the Windows Vista Security Guide at `http://technet.microsoft.com/en-us/library/bb629420.aspx`.

The Event Viewer, which has always been an important tool in Windows, has kept the same focus and purpose but has been updated in appearance a bit, as shown in Figure 10.10.

One new feature worth being aware of for the exam is the Vista User Account Control (UAC) (don't be confused—currently, the CompTIA objectives mistakenly call it the User *Access* Control, but it is Account). UAC is an attempt to take security to the application level by allowing software to run only as a regular user (and not administrator) by default. This is an attempt to limit privilege escalation and will bring up a prompt if an application attempts to escalate its privileges. Some applications—such as administrative tools within the operating system—naturally must escalate their privileges to run properly, and they will appear in listings with a Windows security shield beside them, similar to the one shown in Figure 10.11.

Hardening File Systems

Several file systems are involved in the OSs we've discussed, and they have a high level of interoperability between them—from a network perspective, that is. Through the years, the different vendors have implemented their own sets of file standards. Some of the most common file systems include the following:

Microsoft FAT Microsoft's earliest file system was referred to as File Allocation Table (FAT). FAT is designed for relatively small disk drives. It was upgraded first to FAT16 and finally to FAT32. FAT32 allows large disk systems to be used on Windows systems. FAT

allows only two types of protection: share-level and user-level access privileges. If a user has write or change access to a drive or directory, they have access to any file in that directory. This is very unsecure in an Internet environment.

FIGURE 10.10 The opening view of the Event Viewer on a Windows Vista system

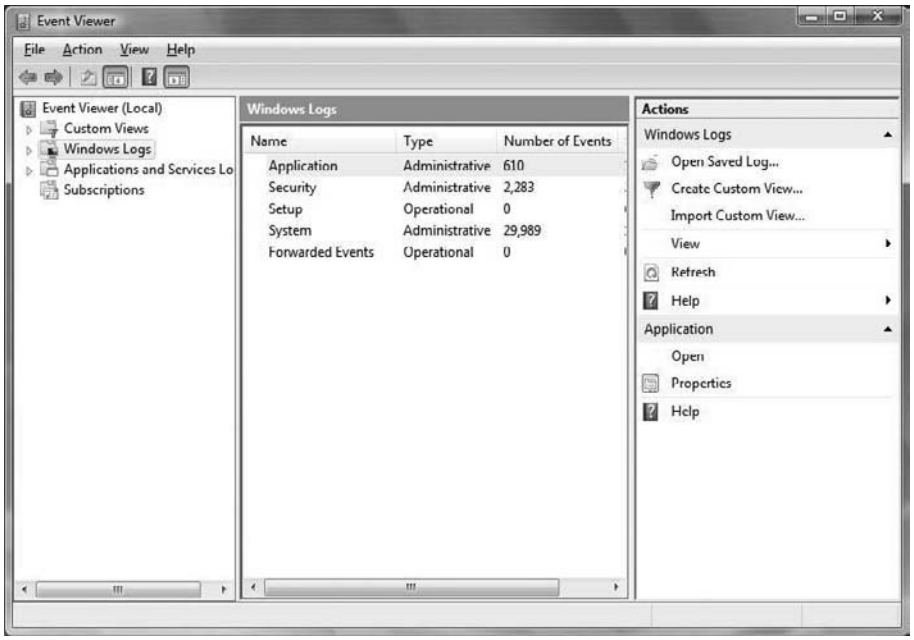


FIGURE 10.11 The Windows security shield indicates the application must run with administrator privileges.

Microsoft NTFS The New Technology File System (NTFS) was introduced with Windows NT to address security problems. Before Windows NT was released, it had become apparent to Microsoft that a new file system was needed to handle growing disk sizes, security concerns, and the need for more stability. NTFS was created to address those issues.

Although FAT was relatively stable if the systems that were controlling it kept running, it didn't do well when the power went out or the system crashed unexpectedly. One of the benefits of NTFS was a transaction tracking system, which made it possible for Windows NT to back out of any disk operations that were in progress when Windows NT crashed or lost power.

With NTFS, files, directories, and volumes can each have their own security. NTFS's security is flexible and built in. Not only does NTFS track security in ACLs, which can hold permissions for local users and groups, but each entry in the ACL can specify what type of access is given—such as Read-Only, Change, or Full Control. This allows a great deal of flexibility in setting up a network. In addition, special file-encryption programs were developed to encrypt data while it was stored on the hard disk.

Microsoft strongly recommends that all network shares be established using NTFS. Several current OSs from Microsoft support both FAT32 and NTFS. It's possible to convert from FAT32 to NTFS without losing data, but you can't do the operation in reverse (you would need to reformat the drive and install the data again from a backup tape).

If you're using FAT32 and want to change to NTFS, the convert utility will allow you to do so. For example, to change the `E:` drive to NTFS, the command is `convert e: /FS:NTFS`.

Share permissions apply only when a user is accessing a file or folder through the network. Local permissions and attributes are used to protect the file when the user is local. With FAT and FAT32, you do not have the ability to assign "extended" or "extensible" permissions, and the user sitting at the console effectively is the owner of all resources on the system. As such, he can add, change, and delete any data or file that he wants.

With NTFS as the file system, however, you are allowed to assign more comprehensive security to your computer system. NTFS permissions are able to protect you at the file level. Share permissions can be applied to the directory level only. NTFS permissions can affect users logged on locally or across the network to the system where the NTFS permissions are applied. Share permissions are in effect only when the user connects to the resource via the network.

Permissions can be allowed or denied individually on a per-folder basis. You can assign any combination of the values shown in Table 10.5.

TABLE 10.5 NTFS Directory Permissions

NTFS Permission	Meaning
Full Control	Gives the user all the other choices and the ability to Change Permission. The user also can take ownership of the directory or any of its contents.
Modify	Combines the Read & Execute permission with the Write permission and further allows the user to delete everything, including the folder.
Read & Execute	Combines the permissions of Read with those of List Folder Contents and adds the ability to run executables.

TABLE 10.5 NTFS Directory Permissions *(continued)*

NTFS Permission	Meaning
List Folder Contents	The List Folder Contents permission (known simply as List in previous versions) allows the user to view the contents of a directory and to navigate to its subdirectories. It does not grant the user access to the files in these directories unless that is specified in file permissions.
Read	Allows the user to navigate the entire directory structure, view the contents of the directory, view the contents of any files in the directory, and see ownership and attributes.
Write	Allows the user to create new entities within the folder, as well as to change ownership, permissions, and attributes.

Clicking the Advanced button allows you to configure auditing and ownership properties. You can also apply NTFS permissions to individual files. This is done from the Security tab for the file; Table 10.6 lists the NTFS file permissions.

TABLE 10.6 NTFS File Permissions

NTFS Permission	Meaning
Full Control	Gives the user all the other permissions as well as permission to take ownership and change permission
Modify	Combines the Read & Execute permission with the Write permission and further allows the user to delete the file
Read	Allows the user to view the contents of the file and to see ownership and attributes
Read & Execute	Combines the Read permission with the ability to execute
Write	Allows the user to overwrite the file, as well as to change attributes and see ownership and permissions

By default, the determination of NTFS permissions is based on the *cumulative* NTFS permissions for a user. Rights can be assigned to users based on group membership and individually; the only time permissions do not accumulate is when the Deny permission is invoked.

Updating Your Operating System

OS manufacturers typically provide product updates. For example, Microsoft provides a series of regular updates for their operating systems (proprietary systems) and other applications. However, in the case of public source systems (such as Linux), the updates may come from a newsgroup, the manufacturer of the version you're using, or a user community.

In both cases, public and private, updates help keep OSs up to the most current revision level. Researching updates is important; when possible, so is getting feedback from other users before you install an update. In a number of cases, a service pack or update has rendered a system unusable. Make sure your system is backed up before you install updates.

Make sure you test updates on test systems before you implement them on production systems.

Three different types of updates are discussed here: hotfixes, service packs, and patches.

Hotfixes

Hotfixes are used to make repairs to a system during normal operation, even though they may require a reboot. A hotfix may entail moving data from a bad spot on the disk and remapping the data to a new sector. Doing so prevents data loss and loss of service. This type of repair may also involve reallocating a block of memory if, for example, a memory problem occurred. This allows the system to continue normal operations until a permanent repair can be made. Microsoft refers to a bug fix as a *hotfix*. This involves the replacement of files with an updated version.

Service Packs

A *service pack* is a comprehensive set of fixes consolidated into a single product. A service pack may be used to address a large number of bugs or to introduce new capabilities in an OS. When installed, a service pack usually contains a number of file replacements.

Make sure you check related websites to verify that the service pack works properly. Sometimes a manufacturer releases a service pack before it has been thoroughly tested. An untested service pack can cause extreme instability in an OS or, even worse, render it inoperable.

Patches

A *patch* is a temporary or quick fix to a program. Patches may be used to temporarily bypass a set of instructions that have malfunctioned. Several OS manufacturers issue patches that can be either manually applied or applied using a disk file to fix a program.

When you're working with customer support on a technical problem with an OS or applications product, customer service may have you go into the code and make alterations to the binary files that run on your system. Double-check each change to prevent catastrophic failures due to improperly entered code.

When more is known about the problem, a service pack or hotfix may be issued to fix the problem on a larger scale. Patching is becoming less common, because most OS manufacturers would rather release a new version of the code than patch it.

General Rules

As with most objectives, there are a number of general rules to adhere to, regardless of which OSs are employed on your servers and clients. Among those rules for this objective are the following:

- Know the authentication possibilities for the OSs you use, and know what each allows. In addition to those that come standard with the OS, you can also employ add-on devices such as biometric scanners to increase the security of the authentication process.
- Understand that firewalls can be software- or hardware-based, and are usually some combination of the two. Software-only firewalls are usually limited to home use and provide the line of defense preventing outside users from gaining access to the home computer.
- Event logging is used to record events and provide a trail that can be followed to determine what was done. Auditing involves looking at the logs and finding problems.
- Wireless clients can be configured to access the network the same as wired clients, but wireless security is a touchy issue. There are protocols that you can use to add security, but it's still difficult to secure a wireless network the same way you can secure a wired one. Unused wireless connections are the same as leaving a security door open.
- Data access can be limited a number of different ways—permissions to the data and basic local security policies are two universal methods that should be used regardless of the OS you're employing.
- The file system you're using can determine what permissions you have available to assign to resources. NTFS offers a great deal of granularity in terms of permissions, whereas FAT32 offers few choices. You can convert from FAT32 to NTFS without data loss by using the convert utility.
- To increase the level of authentication, you can employ biometrics, key fobs, and smart cards. Smart card readers may be contact-based (you have to insert the card) or contactless (the card is read when it's in proximity to the reader). Key fobs are often used to provide a randomly generated number that you can enter for authentication, and biometric devices identify the user by some physical aspect (such as a thumb print).

While key fobs are often thought of as generating random numbers, the term *key fob* is also used for many small devices that allow for keyless entry into buildings or vehicles. While those require only proximity and a clear line of sight, when it comes to true security, you want something that also incorporates a challenge/response to authenticate the user.

Working with Access Control Lists

Access control lists (ACLs) enable devices in your network to ignore requests from specified users or systems, or to grant them certain network capabilities. You may find that a certain IP address is constantly scanning your network, and thus you can block this IP address from your network. If you block it at the router, the IP address will automatically be rejected any time it attempts to utilize your network.

ACLs allow a stronger set of access controls to be established in your network. The basic process of ACL control lets the administrator design and adapt the network to deal with specific security threats.

If at all possible, don't share the root directories of a disk drive. Doing so allows access to system files, passwords, and other sensitive information. Establish shares off hard drives that don't contain system files.

General Rules

You should adhere to a number of general rules, regardless of which OSs are employed on your servers and clients. Among those rules are the following:

- Limit access to the OS to only those who need it. As silly as it may sound, every user should be a user who has to access the system. This means that every user has a unique username and password that are shared with no one else. Don't allow users to use guest accounts or admin accounts (regardless of whether your OS calls them admin, root, supervisor, and so on).
- Not only do you require users to have unique access, but you limit that access to only what they need access to. In other words, you start out assuming they need access to nothing, and then you back off slowly from that position. It's always better to have a user with too little permission, and whose settings you have to tweak a bit, than to have one with too much permission who "accidentally" deletes important files.
- Trying to manage individual users becomes more of a nightmare as the size of the systems increases. For that reason, management should be done (as much as possible) by groups. Users with similar traits, job duties, and so on, are added to groups, and the groups are assigned the permissions the users need. If a user needs access to more than what a specific group offers, you make them a member of multiple groups—don't try to tweak their settings individually.
- All administrative tools, utilities, and so on should be safely guarded behind secure rights and permissions. You should regularly check to see who has used such tools (see the discussion of auditing in the next section), and make sure they aren't being accessed by users who shouldn't be able to do so.
- Control permissions to resources as granularly as possible. The next objective discusses permissions and ACLs as they apply to different OSs. Know the ones that exist in your environment and how to use them effectively.

Guard the Guest Account

The Guest account is used when someone must access a system but lacks a user account on that system. The Guest account leaves a security risk at the workstation and should be disabled. To turn the Guest account off, follow these steps:

1. Choose Start ➢ Control Panel ➢ User Accounts.
2. Click Guest. Click Turn Off The Guest Account.
3. Exit the User Accounts dialog box and close Control Panel.

Working with Profiles and Policies

One of the most wide-sweeping administrative features that Windows 200*x* offers over its predecessors and other OSs is that of *Group Policy*. A part of IntelliMirror, the Group Policy feature enables administrators to control desktop settings, utilize scripts, perform Internet Explorer maintenance, roll out software, redirect folders, and so forth. All of these features can be an administrator's dream in supporting LAN users.

Consider this analogy: when you connect a television set to the subscription cable coming through the living room wall, you get all the channels to which you subscribe. If you pay an extra $50 per month (depending on where you live), you can get close to 100 channels, including a handful of premium channels.

When you turn on the television, you're free to watch any of the channels—regardless of whether the content is questionable or racy. And when you're gone, your children are free to do the same. Enter the V-chip. Before leaving your children alone with the television, you enable the V-chip. The V-chip lets you (the "administrator") restrict access to stations that air questionable or racy programming.

How is this example analogous to an OS? On Windows 2000 Professional, for example, users can do just about anything they want. They can delete programs and never be able to run them again; they can send huge graphics files to a tiny printer that can print only one page every 30 minutes; they can delete the Registry and never be able to use the system again; and so forth. Enter Group Policy.

Group Policy places restrictions on what a user/computer is allowed to do. It takes away liberties that were otherwise there; therefore, they are never implemented for the benefit of the user (restrictions don't equal benefits) but are always there to simplify administration for the administrator.

From an administrator's standpoint, if you take away the ability to add new software, then you don't have to worry about supporting nontested applications. If you remove the ability to delete installed printers (accidentally, of course), then you don't have to waste an hour reinstalling the printer. By reducing what users can do, you reduce what you must support, and you also reduce the overall administrative cost of supporting the network/computer/user.

Before going any further, it's important to differentiate between roaming users and mobile users, because the two are often confused. As the name implies, *roaming users* are users who roam throughout the LAN. One example is a secretary in a secretarial pool. On Monday, the secretary may be working in Accounting, on Tuesday in Human Resources, and for the remainder of the week in Marketing. Within each department, the secretary has a different computer but is still on the same LAN. By placing the secretary's profile on the network and configuring them as a roaming user, you give them the same desktop and access to all resources regardless of where the secretary works on any given day. Not only that, but the same Group Policy applies (and is routinely refreshed), to prevent the secretary from permanently deleting software that has been assigned, changing the desktop, and so on.

An example of a *mobile user,* on the other hand, is a salesperson who is in the field calling on customers. In their possession is a $6,000 laptop capable of doing everything shy of changing the oil of the company car. Whenever the salesperson has a problem with the computer, they call from 3,000 miles away and begin the conversation with, "It did it again." You not only have no idea to whom you're talking, you have no idea what "it" refers to.

In short, roaming users use different computers within the same LAN, whereas mobile users use the same workstation but don't connect to the LAN. Because you can't force mobile users to connect to a server on your LAN each time they boot (and when they do, it's over slow connections), you're less able to enforce administrative restrictions—such as Group Policies. However, it isn't impossible to apply administrative restrictions to mobile users. System Policies (used in Windows *9x*) are the predecessors of Group Policies. They're restricted to governing Registry settings only, whereas Group Policies exceed that functionality.

In the absence of a regular connection to the LAN (and, therefore, to Active Directory), there are a number of Group Policy restrictions that you can't enforce or utilize. Therefore, it's always in the best interest of the administrators to have the systems connect to the network (and require them to do so) whenever possible. The following is a list of restrictions that can't be enforced without such a connection:

Assigning and Publishing Software The Software Installation extension enables you to centrally manage software. You can publish software to users and assign software to computers.

Folder Redirection The Folder Redirection extension lets you reroute special Windows 2000 folders—including My Documents, Application Data, Desktop, and the Start Menu—from the user profile location to elsewhere on the network.

Remote Installation The Remote Installation Services (RIS) extension enables you to control the Remote Operating System Installation component, as displayed to the client computers.

Roaming Profiles By placing the user's profile on the server, they can have the same desktop regardless of which computer they use on a given day.

In addition to these, you can place all the other settings directly on the mobile computer—making them local policies. Local policies can apply to the following:

Administrative Templates The administrative templates consist mostly of the Registry restrictions that existed in System Policies. They let you manage the Registry settings that control the desktop, including applications and OS components.

Scripts Scripts enable you to automate user logon and logoff.

Security Settings The Security Settings extension lets you define security options (local, domain, and network) for users within the scope of a Group Policy object, including Account Policy, encryption, and so forth.

Creating the Local Policy

You can create a local policy on a computer by using the Group Policy Editor. You can start the Group Policy Editor in one of the following two ways:

- Choose Start ➢ Run, and then enter **gpedit.msc**.
- Choose Start ➢ Run, and then enter **MMC**. In the MMC console, choose File ➢ Open, and then select `GPEDIT.MSC` from the `System32` directory of the %systemroot% folder.

When opened, a local policy has two primary divisions: Computer Configuration and User Configuration. The settings you configure beneath Computer Configuration apply to the computer, regardless of who is using it. Conversely, the settings you configure beneath User Configuration apply only if the specified user is logged on. Each of the primary divisions can be useful for certain circumstances. Note that the Computer Configuration settings are applied whenever the computer is on, whereas the User Configuration settings are applied only when the user logs on.

The following options are available under the Computer Configuration setting:

Software Settings These settings typically are blank on a new system.

Administrative Templates These settings are those administrators commonly want to apply.

Windows Settings The Windows Settings options are further divided:

Scripts Scripts are divided into Startup and Shutdown, both of which enable you to configure items (`.EXE`, `.CMD`, `.BAT`, and other files) to run when a computer starts and stops. Although your implementation may differ, for the most part, little here is pertinent to the mobile user.

Security Settings Security Settings options are divided into Account Policies, Local Policies, Public Key Policies, and IP Security Policies on the local machine.

The following sections examine some of the Security Settings choices.

Account Policies

Account Policies further divides into Password Policy and Account Lockout Policy. The following seven choices are available under Password Policy, and the majority of

them were previously in the Account Policy menu of User Manager on Windows NT Workstation:

Enforce Password History This allows you to require unique passwords for a certain number of iterations. The default number is 0, but it can go as high as 24.

Maximum Password Age The default is 42 days, but values range from 0 to 999.

Minimum Password Age The default is 0 days, but values range from 0 to 999.

Minimum Password Length The default is 0 characters (meaning no passwords are required), but you can specify a number up to 14.

Passwords Must Meet Complexity Requirements of the Installed Password Filter The default is disabled.

Store Password Using Reversible Encryption For All Users In The Domain The default is disabled.

User Must Logon To Change The Password The default is disabled, thus allowing a user with an expired password to specify a new password during the logon process.

Because the likelihood of laptops being stolen always exists, it's strongly encouraged that you use good password policies for this audience. Here's an example:

- Enforce Password History: 8 passwords remembered
- Maximum Password Age: 42 days
- Minimum Password Age: 3 days
- Minimum Password Length: 6 to 8 characters

Leave the other three settings disabled.

Account Lockout Policy

The Account Lockout Policy setting divides into the following three values:

Account Lockout Counter This is the number of invalid attempts before lockout occurs. The default is 0 (meaning the feature is turned off). Invalid attempt numbers range from 1 to 999. A number greater than 0 changes the values of the following two options to 30 minutes; otherwise, they are "not defined."

Account Lockout Duration This is a number of minutes ranging from 1 to 99999. A value of 0 is also allowed here and signifies that the account never unlocks itself—administrator interaction is always required.

Reset Account Lockout Counter After This is a number of minutes, ranging from 1 to 99999.

When you're working with a mobile workforce, you must weigh the choice of users calling you in the middle of the night when they've forgotten their password against keeping the system from being entered if the wrong user picks up the laptop. A good recommendation is to use a lockout after five attempts for a period of time between 30 and 60 minutes.

Local Policies

The Local Policies section divides into three subsections: Audit Policy, User Rights Assignment, and Security Options. The Audit Policy section contains nine settings; the default value for each is No Auditing. Valid options are Success and/or Failure. The Audit Account Logon Events entry is the one you should consider turning on for mobile users to see how often they log in and out of their machines.

When auditing is turned on for an event, the entries are logged in the Security log file.

The User Rights Assignment subsection of Local Policies is where the meat of the old System Policies come into play. User Rights Assignment has many options, most of which are self-explanatory. Also shown in the list that follows are the defaults for who can perform these actions; Not Defined indicates that no one is specified for this operation. You can add groups and users, but you can't remove them. (This functionality isn't needed.) If you want to "remove" users or groups from the list, uncheck the box granting them access. If your mobile users need to be able to install, delete, and modify their environment, make them members of the Power Users group.

The Security Options section includes a great many options, which, for the most part, are Registry keys. The default for each is Not Defined; the two definitions that can be assigned are Enabled and Disabled, or a physical number (as with the number of previous logons to cache).

General Rules

As with the first two objectives, you should adhere to a number of general rules, regardless of which OSs are employed on your servers and clients. Among those rules for this objective are the following:

- Software-only firewalls are typically suitable only for home use. They protect the computer they're running on but require resources from that computer (which could potentially slow down the user using the computer and other applications sharing the computer).
- Wireless networks need to be carefully configured to allow access to legitimate clients and only the legitimate network clients.
- Data access and encryption can work together. You should be able to limit access to only those eyes that need to see the data, but encrypting data helps to keep it secure if it does fall into the wrong hands.

Working with Disks and Directories

The basic building block of storage is the disk. Disks are partitioned (primary, logical, extended) and then formatted for use. With the Windows operating systems this exam focuses on, you can choose to use either FAT32 or NTFS; the advantage of the latter is that it offers security and many other features that FAT32 can't handle.

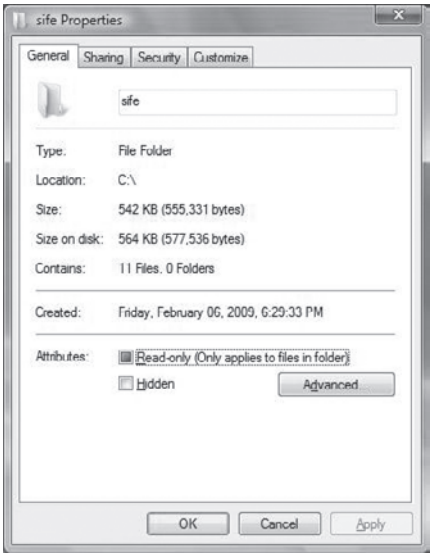
If you're using FAT32 and want to change to NTFS, the convert utility will allow you to do so. For example, to change the E: drive to NTFS, the command is `convert e: /FS:NTFS`.

Once the disk is formatted, the next building block is the directory structure, in which you divide the partition into logical locations for storing data. Whether these storage units are called directories or folders is a matter of semantics—they tend to be called *folders* when viewed in the graphical user interface (GUI) and *directories* when viewed from the command line.

You can create directories from the command line using the `MD` command and from within the GUI by right-clicking in a Windows Explorer window and choosing New ➢ Folder. Once the folder exists, you can view/change its properties, as shown in Figure 10.12, by right-clicking the icon of its folder and choosing Properties.

In the Attributes section, you can choose to make the directory read-only or hidden. By clicking the Advanced button, you can configure indexing, archiving, encryption, and compression settings.

FIGURE 10.12 Change the attributes associated with a directory.



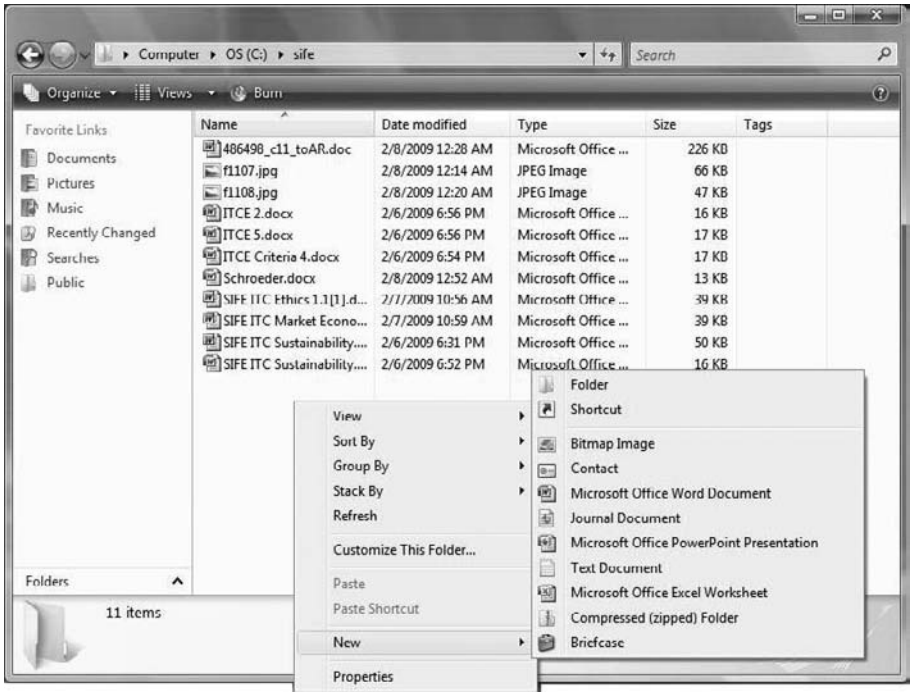
Even though encryption and compression settings appear in the same frame on the dialog box, the two features are mutually exclusive.

The building blocks of directories are files. You can create a file either from within an application or by right-clicking, choosing New, and then selecting the type of item you want to create, as shown in Figure 10.13.

Once the file has been created, you can right-click the file's icon and change properties and permissions associated with the file by choosing Properties from the context menu. Know that when users copy or move a file, they may get results different from what they

expected when it comes to permissions. In most operating systems, a file copied into a folder will, by default, inherit the rights of the folder. This will be the same with encryption—if a user copies an unencrypted file into an encrypted folder, the file will become encrypted. Conversely, if the user copies an encrypted file into an unencrypted folder, the file becomes unencrypted.

FIGURE 10.13 You can create files of various types with a right-click.



If a user moves a file from one folder to another, the file system will keep the permissions that existed as long as the new folder can support them. This is an important caveat, for if an NTFS file is moved to a FAT-based flash drive, the permissions existing only in NTFS will be gone.

Administrative Tools

The administrative tools that fall beneath this section are the primary tools used on a regular basis. Most of them relate to data and drives, but that isn't true of all of them. The tools that CompTIA wants you to know are as follows:

CHKDSK `CHKDSK` is an old MS-DOS command that is used to correct logical errors in the FAT. The most common switch for `CHKDSK` is `/F`, which fixes the errors that it finds. Without `/F`, `CHKDSK` is an information-only command.

DEFRAG This command runs the Disk Defragmenter utility. Disk Defragmenter reorganizes the file storage on a disk to reduce the number of files that are stored noncontiguously. This makes file retrieval faster, because the read/write heads on the disk have to move less.

There are two versions of Disk Defragmenter: a command-line version, and a Windows version that runs from within Windows. The Windows version is located on the System Tools submenu on the Start menu (Start ➢ All Programs ➢ Accessories ➢ System Tools ➢ Disk Defragmenter).

The available switches for the command-line version (`defrag.exe`) include the following:

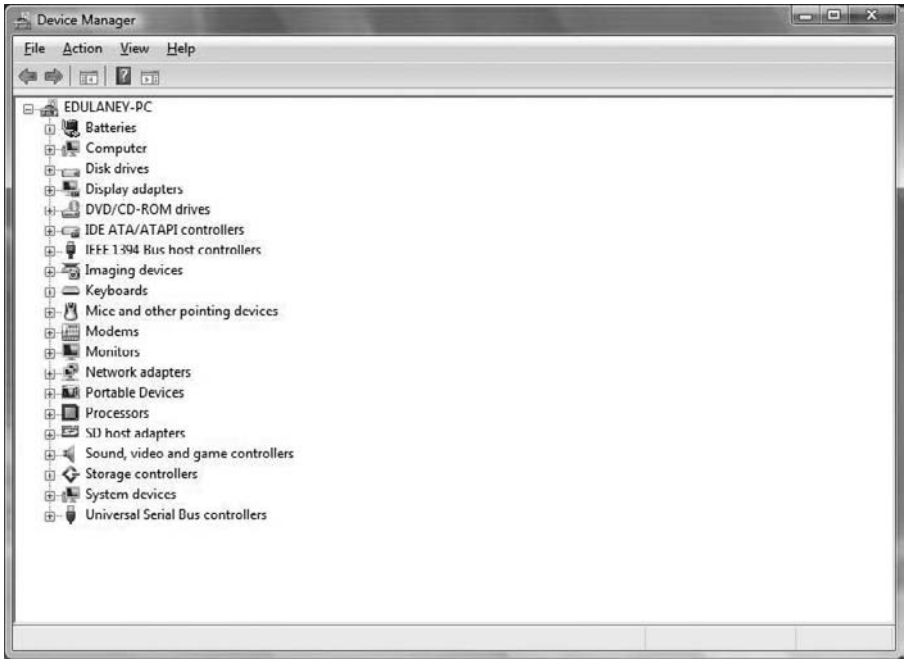
`-a` Analyze only

`-f` Force defragmentation even if disk space is low

`-v` Use verbose output

Device Manager Device Manager shows a list of all installed hardware and lets you add items, remove items, update drivers, and more. This is a Windows-only utility. In Windows 2000/XP, you display the System Properties, click the Hardware tab, and then click the Device Manager button to display it. With Windows Vista, choose System And Maintenance in Control Panel, select System, and click Device Manager in the left menu. Figure 10.14 shows the Device Manager in Windows Vista.

FIGURE 10.14 The Device Manager in Windows Vista



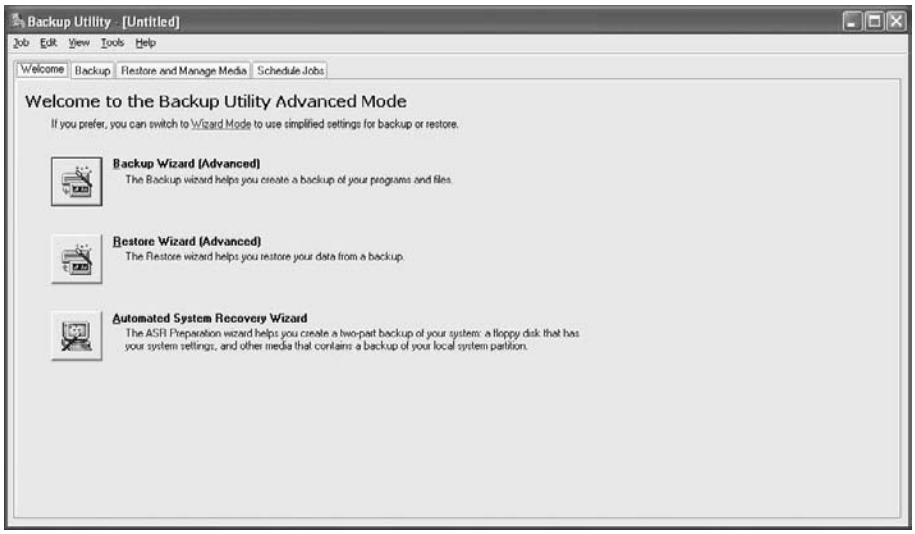
Event Viewer This utility was discussed previously in the discussion on hardening operating systems. It provides information about what's been going on system-wise, to help you troubleshoot problems. Event Viewer shows warnings, error messages, and records of things happening successfully. It's found only in NT-based versions of Windows (which include Windows 2000, Windows XP, and Windows Vista). You can access it through Computer Management, or you can access it directly from the Administrative Tools in Control Panel.

MSCONFIG (System Configuration Utility) This utility helps troubleshoot startup problems by allowing you to selectively disable individual items that normally are executed at startup. There is no menu command for this utility; you must run it with the Run command (on the Start menu). Choose Start ➢ Run, and type **`MSCONFIG`**. It works in most versions of Windows, although the interface window is slightly different among versions.

NTBackup With Windows 2000 and XP, you can access this utility from the System Tools menu, or from the Tools tab in a hard disk's Properties box. Its purpose is to back up files in a compressed format, so the backups take up less space than the original files would if they were copied. To restore the backup, you must use the same utility again but in Restore mode. The best insurance policy you have against devastating loss when a failure occurs is a backup of the data that you can turn to when the system is rebuilt.

When you start the program, by default it begins the Backup Or Restore Wizard (you can disable this default action by deselecting Always Start In Wizard Mode in the first dialog box). The wizard will walk you through any backup/restore operation you want to do, or you can click Advanced Mode to get to the interface shown in Figure 10.15.

FIGURE 10.15 Advanced mode of the Backup utility in Windows XP



Five backup type choices are available:

Normal A full backup of all files, regardless of the state of the archive bit (the default). After the files are backed up, the archive bit is turned off.

Copy A full backup of all files, regardless of the state of the archive bit. The archive bit is left in its current state.

Incremental Backs up only files for which the archive bit is currently turned on. After the files are backed up, the archive bit is turned off.

Differential Backs up only files for which the archive bit is currently turned on. The archive bit is left in its current state.

Daily Backs up only those files with today's date, regardless of archive bit status.

You can also perform backups from the command line by using the `ntbackup.exe` executable. You can't restore files from the command line with this utility, however. Options include the following:

`/A` Performs an append

`/F` Identifies the disk path and filename

`/HC:{on|off}` Toggles hardware compression on or off

`/J` Signifies the job name

`/M` Must be followed by a backup type name: `copy`, `daily`, `differential`, `incremental`, or `normal`

`/N` Signifies a new tape name; can't be used in conjunction with `/A`

`/P` Signifies the media pool name

`/T` Followed by the tape name

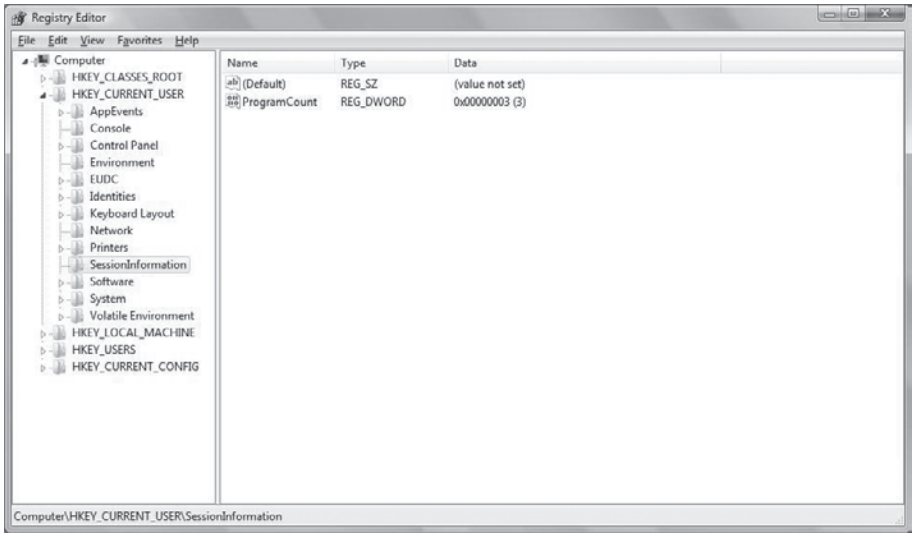
`/V:{yes|no}` Toggles whether to do verification after the completion of the backup

Regedit and Regedt32 (Registry Editor) The Registry Editor is used to change values and variables stored in a configuration database known as the Registry. This centralized database contains environmental settings for various Windows programs along with registration information, which details the types of file extensions associated with applications. So, when you double-click a file in Windows Explorer, the associated application runs and opens the file you double-clicked.

The Registry Editor, shown in Figure 10.16, enables you to make changes to the large hierarchical database that contains all of Windows' settings. These changes can potentially disable the entire system, so they should not be made lightly.

There is no menu command for the Registry Editor. You must execute it with the Run command. Regedit is the name of the program. Windows 2000 includes a second Registry Editor program called Regedt32. This alternative program accesses the same Registry but does so in a slightly different way; it shows each of the major key areas in a separate window. In Windows XP and Windows Vista, the command `REGEDT32` is available, but running it launches Regedit; they have been rolled into a single utility.

FIGURE 10.16 The Registry Editor in Windows Vista



The Registry holds great power but can also cause great harm. Never edit the Registry without being completely sure what you're doing.

Remote Desktop The Remote Desktop feature of Windows XP allows you to remotely connect to your workstation and use it for a variety of purposes—work from home, teach a user how to do a task, and so on. Two elements are involved:

- Turning on the ability to access remotely
- Accessing remotely

To do the first, access the System Properties, click the Remote tab, and select the Allow Users To Connect Remotely To This Computer Under Remote Desktop check box. Click Apply, and then click OK to exit.

To access the computer from another XP workstation, select Start ➢ All Programs ➢ Accessories ➢ Communications, and choose Remote Desktop Connection.

For Windows Vista, simply click Start ➢ All Programs ➢ Accessories, and choose Remote Desktop Connection.

If you click the Options button, you'll see choices similar to those in Figure 10.17.

FIGURE 10.17 The Remote Desktop Connection dialog box in Windows XP

One of the simplest ways to connect is to enter the IP address of the host. Once you give a valid username and password, you're connected to the host and able to work remotely.

Task Manager Task Manager shows running programs and the system resources they're consuming. It can be used for informational purposes, but it's most often used to shut down a nonresponsive application.

There are three common ways to display the Task Manager. The first is to press Ctrl+Alt+Delete and click the Task Manager button (if required). The second is to right-click in an empty location on the Taskbar and choose Task Manager from the context menu. The third method is to hold down Ctrl+Shift and press Esc.

A list of running tasks appears under the Applications tab; you can click one of them and then click End Task to shut it down. Because this shutdown method fails to close files gracefully, you should use it only as a last resort, not as a normal method of shutting down an application. You can also choose the Processes tab to see all processes—not just applications—running, or choose Performance to see CPU, paging, memory, and other parameters. The Networking tab shows usage for all found connections, and the Users tab shows the current users and lets you disconnect them, log them off, or send them a message.

Windows Explorer Windows Explorer is the primary file-management interface in Windows. It displays the list of files in the current location at the right and a folder tree of other locations at the left. It starts with the My Documents folder as its default location when opened. Windows Explorer is available in all Windows versions and works approximately the same way in each.

Auditing and Logging

Most systems generate *security logs* and *audit files* of activity on the system. These files do absolutely no good if they aren't periodically reviewed for unusual events. Many web servers provide message auditing, as do logon, system, and application servers. Security auditing is the process of establishing what events are recorded in the Security Events Log (e.g. file or folder access, successful logon, unsuccessful logon, etc.). By default, nothing is recorded and we use an audit policy to select the success or failure events that we want to be recorded.

The amount of information these files contain can be overwhelming. You should establish a procedure to review them on a regular basis. A rule of thumb is to never start auditing by trying to record everything, because the sheer volume of the entries will make the data unusable. Approach auditing from the opposite perspective, and begin auditing only a few key things; then, expand the audits as you find you need more data.

These files may also be susceptible to access or modification attacks. The files often contain critical systems information, including resource sharing, security status, and so on. An attacker may be able to use this information to gather more detailed data about your network.

In an access attack, these files can be deleted, modified, and scrambled to prevent systems administrators from knowing what happened in the system. A logic bomb could, for example, delete these files when it completes. Administrators might know that something happened, but they would get no clues or assistance from the log and audit files.

You should consider periodically inspecting systems to see what software is installed and whether passwords are posted on sticky notes on monitors or keyboards. A good way to do this without attracting attention is to clean all the monitor faces. While you're cleaning the monitors, you can also verify that physical security is being upheld. If you notice a password on a sticky note, you can "accidentally" forget to put it back. You should also notify that user that this is an unsafe practice and not to continue it.

Under all conditions, you should always work within the guidelines established by your company.

You should also consider obtaining a vulnerability scanner and running it across your network. A *vulnerability scanner* is a software application that checks your network for any known security holes; it's better to run one on your own network before someone outside the organization runs it against you.

BIOS Security

BIOS security, and all the objectives beneath it, were discussed in Chapter 5, "Security." The material that follows repeats information located there but does so in an abbreviated way. The system Basic Input/Output System (BIOS) is used to power up the system and can also allow you to assign a password. If enabled/activated, the password is then stored in CMOS and a user must give it before the system will fully boot or the supervisor can gain access to the BIOS setup program.

The BIOS setup from most vendors includes the ability to toggle chassis intrusion detection. If enabled, this will notify you (via a pop-up) if someone has opened the case.

Within the advanced configuration settings on some BIOS configuration menus, you can choose to enable or disable TPM. A *Trusted Platform Module (TPM)* can be used to assist with hash key generation. TPM is the name assigned to a chip that can store cryptographic keys, passwords, or certificates. TPM can be used to generate values used with whole disk encryption such as Vista's BitLocker. The TPM chip may be installed on the motherboard; when it is, in many cases it is set to off in the BIOS by default.

BitLocker can be used with or without TPM. It is much more secure when coupled with TPM (and is preferable), but does not require it.

TPM can be used to protect cell phones and devices other than PCs as well.

More information on TPM can be found at the Trusted Computing Group's website: `https://www.trustedcomputinggroup.org/home`.

Encrypting File System

BitLocker is far from the only way to encrypt data. Versions of Windows since Windows 2000 have included the Encrypting File System (EFS). EFS allows you to toggle an attribute for a file or folder just as you would any other, and it protects the contents. If the object you select is a folder, all contents of the folder—files, subfolders, and so on—also become encrypted. Unencrypted files moved to an encrypted folder are encrypted whether moved by dragging and dropping or by other means. The reverse is not true. Dragging an encrypted file from an encrypted folder to an unencrypted folder does not automatically decrypt the file (except in the condition noted in the Note below).

To use EFS, the file system must be NTFS, and the files must not be compressed. Some files (system files in particular) cannot be compressed. If you move or copy an encrypted file to one of these partitions, it becomes unencrypted automatically.

From the time a file is encrypted, a digital code associated with the user (encryption certificate) is assigned to it. This allows the encrypting user to open and work with the file exactly as if it were unencrypted, but prevents anyone else from doing so. Because only the encrypting user can open the file, EFS is perfect for personal data but unusable for any data you want to share if you are using Windows 2000 (both Windows XP and Windows Vista allow for sharing of encrypted files).

You can use the Export command in the Certificates snap-in to copy your file encryption certificates to another location. Doing so will allow you to unencrypt your files should a restore operation be necessary after a media failure (at which time you can use the Import command to bring them back from the other media).

EFS is an integrated component of the NT kernel. To encrypt an entity, simply choose its properties and click the Advanced button to access the Advanced Attributes dialog box. Check the box Encrypt Contents To Secure Data and click OK. Each encrypted file is given a unique encryption key. All keys are stored in nonpaged memory for security purposes.

When you choose to encrypt a file, a dialog box appears asking if you want to encrypt only the one file or the file and its parent folder (the default action). A check box gives you the option of choosing to always encrypt only the file, thus preventing the dialog box from reappearing in the future.

Exam Essentials

Know the concepts of data security. You should know that it's imperative to keep the system up-to-date and to install all relevant upgrades as they become available. You should also understand the importance of using a secure file system.

Know the purpose and characteristics of access control. The purpose of access control is to limit who can access what resources on a system. The characteristics depend on the type of implementation utilized. You should always harden your systems to make them as secure as possible.

Diagnose and troubleshoot software and data security issues. It's important to know the reason why policies exist and the types of possibilities they offer to an administrator. What were once called System Policies have now become Group Policies in the Microsoft world. They let you lock down workstations and prevent users from making changes you don't want to allow.

Know the purpose and characteristics of auditing and logging. Log files are created to hold entries about the operations that take place on the system. Auditing is establishing what events are recorded in the Security Events Log (by default, nothing is recorded) and viewing those log files. There is often a fair amount of granularity in choosing what you want to allow into a log—the danger in recording too much information is that it can overwhelm you when you examine it.

Review Questions

1. What is hardening?
2. When does Windows XP automatically create restore points?
3. What is the command used to install the Recovery Console from the CD?
4. Which command-line utility displays or changes the attributes for one or more files?
5. What is the major tool for reviewing logs in Windows 200*x*?
6. Which Windows 2000*x* tool can be a lifesaver when you're troubleshooting problems and looking for resource-related issues?
7. How many service packs are available for Windows Vista?
8. Which type of backup copies only the files for which the archive bit is currently turned on, and turns off the archive bit after the files are backed up?
9. What file system can FAT32 be upgraded to—without loss of data—in many current Microsoft operating systems?
10. What is the default value for the Account Lockout Counter in Group Policy?

Answers to Review Questions

1. Hardening is the process of reducing or eliminating weaknesses, securing services, and attempting to make your environment immune to attacks.
2. Windows XP creates restore points automatically every 24 hours, as well as when you install unsigned device drivers or install (or uninstall) a program with Windows Installer or InstallShield.
3. The command is `winnt32 /cmdcons`.
4. `ATTRIB` displays or changes the attributes for one or more files.
5. The Event Viewer is the major tool for reviewing logs in Windows 200*x*.
6. Performance Monitor can be a lifesaver when you're troubleshooting problems and looking for resource-related issues.
7. At the time of this writing, one service pack is available for Windows Vista.
8. An incremental backup copies only the files for which the archive bit is currently turned on. After the files are backed up, the archive bit is turned off.
9. FAT32 can be upgraded to NTFS without data loss through the use of the convert utility.
10. Account Lockout Counter is the number of invalid attempts it takes before lockout occurs. The default is 0.

Appendix

About the Companion CD

IN THIS APPENDIX:

- ✓ What you'll find on the CD
- ✓ System requirements
- ✓ Using the CD
- ✓ Troubleshooting

What You'll Find on the CD

The following sections are arranged by category and summarize the software and other goodies you'll find on the CD. If you need help with installing the items provided on the CD, refer to the installation instructions in the "Using the CD" section of this appendix.

Sybex Test Engine

For Windows

The CD contains the Sybex test engine, which includes four bonus exams located only on the CD.

PDF of Glossary of Terms

For Windows

We have included an electronic Glossary in `.pdf` format. You can view the electronic Glossary with Adobe Reader.

Adobe Reader

For Windows

We've also included a copy of Adobe Reader so you can view PDF files that accompany the book's content. For more information on Adobe Reader or to check for a newer version, visit Adobe's website at `www.adobe.com/products/reader/`.

Electronic Flashcards

For PC and Pocket PC

These handy electronic flashcards are just what they sound like. One side contains a question or fill-in-the-blank question, and the other side shows the answer.

System Requirements

Make sure your computer meets the minimum system requirements shown in the following list. If your computer doesn't match up to most of these requirements, you may have problems

using the software and files on the companion CD. For the latest and greatest information, please refer to the ReadMe file located at the root of the CD.

- A PC running Microsoft Windows 98, Windows 2000, Windows NT4 (with SP4 or later), Windows Me, Windows XP, or Windows Vista
- An Internet connection
- A CD-ROM drive

Using the CD

To install the items from the CD to your hard drive, follow these steps:

1. Insert the CD into your computer's CD-ROM drive. The license agreement appears.

Windows users: The interface won't launch if you have Autorun disabled. In that case, click Start ➢ Run (for Windows Vista, Start ➢ All Programs ➢ Accessories ➢ Run). In the dialog box that appears, type `D:\Start.exe`. (Replace *D* with the proper letter if your CD drive uses a different letter. If you don't know the letter, see how your CD drive is listed under My Computer.) Click OK.

2. Read the license agreement, and then click the Accept button if you want to use the CD.

The CD interface appears. The interface allows you to access the content with just one or two clicks.

Troubleshooting

Wiley has attempted to provide programs that work on most computers with the minimum system requirements. Alas, your computer may differ, and some programs may not work properly for some reason.

The two likeliest problems are that you don't have enough memory (RAM) for the programs you want to use or you have other programs running that are affecting installation or running of a program. If you get an error message such as "Not enough memory" or "Setup cannot continue," try one or more of the following suggestions and then try using the software again:

Turn off any antivirus software running on your computer. Installation programs sometimes mimic virus activity and may make your computer incorrectly believe that it's being infected by a virus.

Close all running programs. The more programs you have running, the less memory is available to other programs. Installation programs typically update files and programs; so if you keep other programs running, installation may not work properly.

Have your local computer store add more RAM to your computer. This is, admittedly, a drastic and somewhat expensive step. However, adding more memory can really help the speed of your computer and allow more programs to run at the same time.

Customer Care

If you have trouble with the book's companion CD, please call the Wiley Product Technical Support phone number at (800) 762-2974. Outside the United States, call +1(317) 572-3994. You can also contact Wiley Product Technical Support at `http://sybex.custhelp.com`. John Wiley & Sons will provide technical support only for installation and other general quality-control items. For technical support on the applications themselves, consult the program's vendor or author.

To place additional orders or to request information about other Wiley products, please call (877) 762-2974.

Index

Note to the Reader: Throughout this index **boldfaced** page numbers indicate primary discussions of a topic. *Italicized* page numbers indicate illustrations.

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Y

Z

Wiley Publishing, Inc.
End-User License Agreement

READ THIS. You should carefully read these terms and conditions before opening the software packet(s) included with this book "Book". This is a license agreement "Agreement" between you and Wiley Publishing, Inc. "WPI". By opening the accompanying software packet(s), you acknowledge that you have read and accept the following terms and conditions. If you do not agree and do not want to be bound by such terms and conditions, promptly return the Book and the unopened software packet(s) to the place you obtained them for a full refund.

1. License Grant. WPI grants to you (either an individual or entity) a nonexclusive license to use one copy of the enclosed software program(s) (collectively, the "Software," solely for your own personal or business purposes on a single computer (whether a standard computer or a workstation component of a multi-user network). The Software is in use on a computer when it is loaded into temporary memory (RAM) or installed into permanent memory (hard disk, CD-ROM, or other storage device). WPI reserves all rights not expressly granted herein.

2. Ownership. WPI is the owner of all right, title, and interest, including copyright, in and to the compilation of the Software recorded on the physical packet included with this Book "Software Media". Copyright to the individual programs recorded on the Software Media is owned by the author or other authorized copyright owner of each program. Ownership of the Software and all proprietary rights relating thereto remain with WPI and its licensers.

3. Restrictions On Use and Transfer.

(a) You may only (i) make one copy of the Software for backup or archival purposes, or (ii) transfer the Software to a single hard disk, provided that you keep the original for backup or archival purposes. You may not (i) rent or lease the Software, (ii) copy or reproduce the Software through a LAN or other network system or through any computer subscriber system or bulletin-board system, or (iii) modify, adapt, or create derivative works based on the Software.

(b) You may not reverse engineer, decompile, or disassemble the Software. You may transfer the Software and user documentation on a permanent basis, provided that the transferee agrees to accept the terms and conditions of this Agreement and you retain no copies. If the Software is an update or has been updated, any transfer must include the most recent update and all prior versions.

4. Restrictions on Use of Individual Programs. You must follow the individual requirements and restrictions detailed for each individual program in the About the CD-ROM appendix of this Book or on the Software Media. These limitations are also contained in the individual license agreements recorded on the Software Media. These limitations may include a requirement that after using the program for a specified period of time, the user must pay a registration fee or discontinue use. By opening the Software packet(s), you will be agreeing to abide by the licenses and restrictions for these individual programs that are detailed in the About the CD-ROM appendix and/or on the Software Media. None of the material on this Software Media or listed in this Book may ever be redistributed, in original or modified form, for commercial purposes.

5. Limited Warranty.

(a) WPI warrants that the Software and Software Media are free from defects in materials and workmanship under normal use for a period of sixty (60) days from the date of purchase of this Book. If WPI receives notification within the warranty period of defects in materials or workmanship, WPI will replace the defective Software Media.

(b) WPI AND THE AUTHOR(S) OF THE BOOK DISCLAIM ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WITH RESPECT TO THE SOFTWARE, THE PROGRAMS, THE SOURCE CODE CONTAINED THEREIN, AND/OR THE TECHNIQUES DESCRIBED IN THIS BOOK. WPI DOES NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE SOFTWARE WILL MEET YOUR REQUIREMENTS OR THAT THE OPERATION OF THE SOFTWARE WILL BE ERROR FREE.

(c) This limited warranty gives you specific legal rights, and you may have other rights that vary from jurisdiction to jurisdiction.

6. Remedies.

(a) WPI's entire liability and your exclusive remedy for defects in materials and workmanship shall be limited to replacement of the Software Media, which may be returned to WPI with a copy of your receipt at the following address: Software Media Fulfillment Department, Attn.: *CompTIA A+ Complete Review Guide (Exams 220-701/220-702)*, Wiley Publishing, Inc., 10475 Crosspoint Blvd., Indianapolis, IN 46256, or call 1-800-762-2974. Please allow four to six weeks for delivery. This Limited Warranty is void if failure of the Software Media has resulted from accident, abuse, or misapplication. Any replacement Software Media will be warranted for the remainder of the original warranty period or thirty (30) days, whichever is longer.

(b) In no event shall WPI or the author be liable for any damages whatsoever (including without limitation damages for loss of business profits, business interruption, loss of business information, or any other pecuniary loss) arising from the use of or inability to use the Book or the Software, even if WPI has been advised of the possibility of such damages.

(c) Because some jurisdictions do not allow the exclusion or limitation of liability for consequential or incidental damages, the above limitation or exclusion may not apply to you.

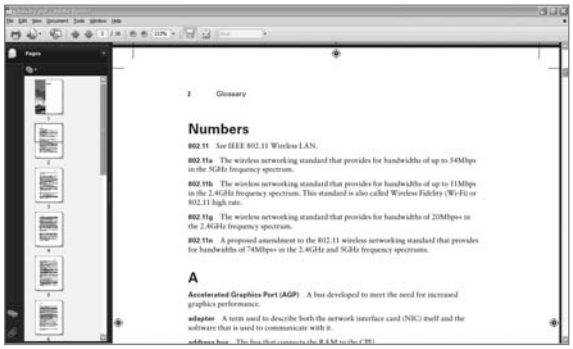
7. U.S. Government Restricted Rights. Use, duplication, or disclosure of the Software for or on behalf of the United States of America, its agencies and/or instrumentalities "U.S. Government" is subject to restrictions as stated in paragraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause of DFARS 252.227-7013, or subparagraphs (c) (1) and (2) of the Commercial Computer Software - Restricted Rights clause at FAR 52.227-19, and in similar clauses in the NASA FAR supplement, as applicable.

8. General. This Agreement constitutes the entire understanding of the parties and revokes and supersedes all prior agreements, oral or written, between them and may not be modified or amended except in a writing signed by both parties hereto that specifically refers to this Agreement. This Agreement shall take precedence over any other documents that may be in conflict herewith. If any one or more provisions contained in this Agreement are held by any court or tribunal to be invalid, illegal, or otherwise unenforceable, each and every other provision shall remain in full force and effect.

The Best CompTIA A+ Quick Reference Book/CD Package on the Market!

Brush up on key A+ topics with hundreds of challenging review questions!

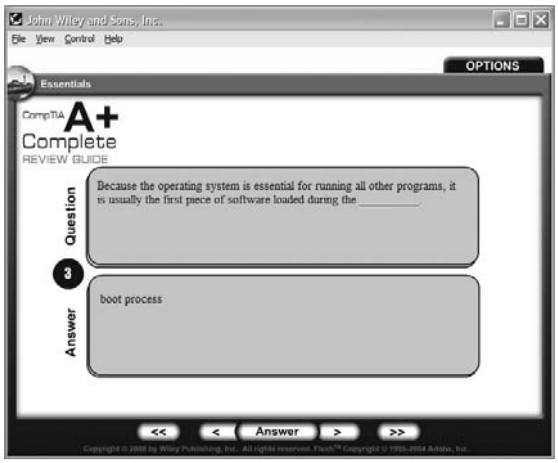
- Four bonus exams—two for the Essentials (220-701) exam and two for the Practical Application (220-702) exam—available only on the CD. Each question includes a detailed explanation.
- Over 200 electronic flashcards.
- Glossary of Key Terms for instant reference.



Use the Glossary for instant reference!

Reinforce your understanding of key concepts with electronic flashcards, for the PC or Pocket PC and many smart phones.

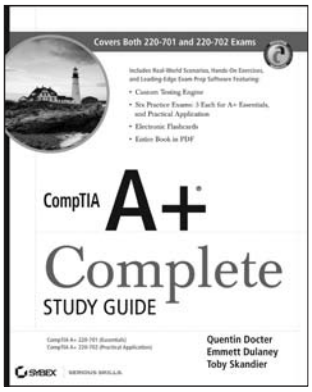
- Contains over 200 flashcard questions.
- Quiz yourself anytime, anywhere.



SYBEX | SERIOUS SKILLS.

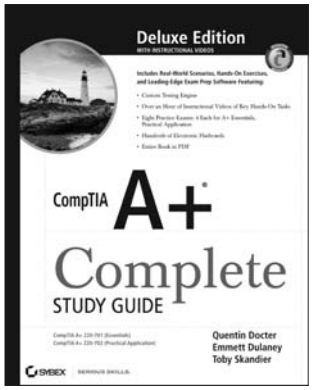
We've got A+ covered.

CompTIA has revised its A+ certification exams for the first time in years, and Sybex is ready with a full line of new CompTIA A+ Study and Review Guides.



- Full coverage of all exam objectives
- Clear and concise information on hardware and operating system maintenance, troubleshooting, and other crucial topics
- CD with Sybex test engine, flashcards, and more

978-0-470-48649-8
$59.99 US • $71.99 CAN

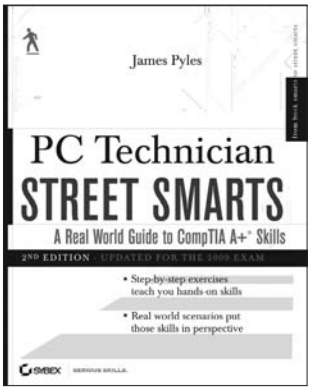


- Everything our regular Study Guide offers, plus bonus exams and flashcards
- Features over an hour's worth of instructional videos on key tasks!

978-0-470-48648-1
$79.99 US • $95.99 CAN

- Brush up on key topics for both exams with over 400 review questions
- CD with bonus questions and exams, flashcards, and a searchable key term database

978-0-470-48650-4
$29.99 US • $35.99 CAN



- Step-by-step instruction on the most common tasks
- Explores scenarios and challenges you'll face in the field

978-0-470-48651-1
$29.99 US • $35.99 CAN

- Perfect for the price-savvy A+ candidate! Three prep guides in one value-priced kit
- Prepare for the exams—and a career

978-0-470-48647-4
$99.97 US • $119.97 CAN

Available from www.sybex.com or wherever books are sold.

SYBEX
An Imprint of WILEY

Glossary

Numbers

802.11 *See* IEEE 802.11 Wireless LAN.

802.11a The wireless networking standard that provides for bandwidths of up to 54Mbps in the 5GHz frequency spectrum.

802.11b The wireless networking standard that provides for bandwidths of up to 11Mbps in the 2.4GHz frequency spectrum. This standard is also called Wireless Fidelity (Wi-Fi) or 802.11 high rate.

802.11g The wireless networking standard that provides for bandwidths of 20Mbps+ in the 2.4GHz frequency spectrum.

802.11n A proposed amendment to the 802.11 wireless networking standard that provides for bandwidths of 74Mbps+ in the 2.4GHz and 5GHz frequency spectrums.

A

Accelerated Graphics Port (AGP) A bus developed to meet the need for increased graphics performance.

adapter A term used to describe both the network interface card (NIC) itself and the software that is used to communicate with it.

address bus The bus that connects the RAM to the CPU.

Aero The graphical user interface included with Windows Vista.

antistatic wrist strap Also called an ESD strap. A specially designed device used to bleed electrical charges away safely. It uses a 1-megaohm resistor to bleed the charge away slowly. Attaching this device to a grounding mat protects the computer system's components from accidental damage.

application Software that is added to an operating system to give it enhanced functionality, such as a word processor or a game.

Application Programming Interface (API) A set of standards to help the programmers writing applications and the hardware designers of video cards and other hardware develop products that work together.

asymmetric algorithms Encryption that uses two keys to encrypt and decrypt data. These keys are referred to as the *public key* and the *private key*.

ATA Packet Interface (ATAPI) An interface that allows other non–hard disk devices (such as tape drives and CD-ROMs) to be attached to an ATA interface and coexist with hard disks.

attribute An option set on a file that identifies it as part of a particular class of files or changes it in some way.

B

backup A usable copy of data made to media. Ideally, the backup is made to removable media and stored for recovery should anything happen to the original data.

baseband A means of transmission in which the entire medium's capacity is used for one signal.

beep code A series of beeps from the PC speaker that indicate the nature of a problem that is preventing the PC from booting normally. Each BIOS manufacturer has a set of beep codes that they use, although some of the meanings are the same across many manufacturers.

biometric devices Authentication tools that use physical characteristics to identify the user. Biometric systems include hand scanners and retinal scanners.

BIOS The basic input/output system for an IBM-based PC. It is the firmware that allows the computer to boot.

BIOS chip A special memory chip that contains the BIOS software that tells the processor how to interact with the hardware in the computer.

boot disk A disk used to troubleshoot or install an operating system.

boot files Files used to start a computer and prepare it for use by the operating system.

broadband A means of transmission in which the medium is used to carry multiple signals simultaneously.

bus A set of signal pathways that allows information and signals to travel between components inside or outside of a computer. A computer contains three types of buses: the external bus, the address bus, and the data bus.

C

cache An area of extremely fast memory, used to store data that is waiting to enter or exit the CPU.

cache memory A storage area for frequently used data and instructions.

capacitor An electronic component that stores an electrical charge.

central processing unit (CPU) A processor chip consisting of an array of millions of integrated circuits. Its purpose is to accept, perform calculations on, and eject numeric data. It's considered the "brain" of the computer because it's the part that performs the mathematical operations required for all other activity.

Challenge Handshake Authentication Protocol (CHAP) A protocol that challenges a system to verify identity. CHAP is an improvement over Password Authentication Protocol (PAP) that adds one-way hashing into a three-way handshake. RFC 1334 applies to both PAP and CHAP.

chip creep A condition that occurs when components slowly move out of their sockets due to being heated to high temperatures and then cooled repeatedly.

chipset The set of controller chips that monitors and directs the traffic on the motherboard between the buses.

client 1) Software that allows a machine to communicate with a particular type of network. 2) The part of a client/server network where end users typically sit. In a typical setting, a client uses the server for remote storage, backups, or security (such as a firewall).

client/server network A server-centric network in which all resources are stored on a file server and processing power is distributed among workstations and the file server.

CMD The utility that opens a command prompt window under NT versions of Windows.

CMOS battery A battery that provides power to the CMOS (or BIOS) chip that stores CMOS settings. A PC must retain certain settings when it's turned off and its power cord is unplugged.

CMOS chip A chip used to retain system settings when the PC is turned off or unplugged.

command interpreter A program that supplies a command prompt with which users can interact.

command prompt A command-line interface, such as in MS-DOS or in a command-prompt window opened through Windows.

D

DC power supply (DCPS) A power supply that converts house current into three voltages used by a printer: +5VDC and –5VDC for the logic circuitry and +24VDC for the paper-transport motors. This component also runs the fan that cools the printer's internal components.

default gateway The router to which all packets are sent when the workstation doesn't know where the destination station is or when it can't find the destination station on the local segment.

defragment To rearrange the storage clusters on a disk so that as many files as possible are stored contiguously, thus improving performance.

degauss To disrupt a magnetic field in a monitor that is making the picture distort. Degaussing is used to improve video quality.

Device Manager The utility used to report detailed information about the computer's devices and their resource usage.

dial-up A form of Internet or other network connection that requires connection via telephone lines.

differential backup A type of backup that includes only new files or files that have changed since the last full backup. Differential backups differ from incremental backups in that they don't clear the archive bit upon their completion.

Digital Subscriber Line (DSL) A technology that uses regular telephone lines to carry high-speed Internet.

direct memory access (DMA) A method used by peripherals to place data in memory without utilizing CPU resources.

direct Rambus A memory bus that transfers data at 800MHz over a 16-bit memory bus. Rambus inline memory modules (often called RIMMs), like DDR SDRAM, can transfer data on both the rising and falling edges of a clock cycle, resulting in an ultra-high memory transfer rate (800MHz) and a high bandwidth of up to 1.6GBps.

docking station A box containing ports (and sometimes drive bays) that add capabilities to a notebook computer whenever it's connected (docked) to the box. These capabilities may include extra keyboard and mouse ports, USB ports, extra serial or parallel ports, a SCSI adapter, an extra IDE adapter, and so on.

Domain Name Service (DNS) The network service used in TCP/IP networks that translates hostnames to IP addresses. *See also* Transmission Control Protocol/Internet Protocol (TCP/IP).

double data rate SDRAM (DDR SDRAM) A type of RAM that runs at twice the speed of the system bus.

Dr. Watson A program in some versions of Windows that intercepts errors and reports on them.

driver Software used to access a particular piece of hardware.

dual inline memory module (DIMM) A double-sided RAM circuit board used in modern systems. DIMMs typically are 168-pin and 64-bit.

Dynamic Host Configuration Protocol (DHCP) A protocol used on a TCP/IP network to send client configuration data, including IP address, default gateway, subnet mask, and DNS configuration, to clients. DHCP uses a four-step process: Discover, Offer, Request, and Acknowledgement. *See also* default gateway, Domain Name Service (DNS), Transmission Control Protocol/Internet Protocol (TCP/IP).

Dynamic RAM (DRAM) A type of RAM that loses its data rapidly if it isn't constantly electrically refreshed.

E

electronically erasable programmable read-only memory (EEPROM) A type of ROM chip that can be flash-updated with software.

electrostatic discharge (ESD) An exchange of electrons that happens when two objects of dissimilar charge come in contact with one another, thereby standardizing the electrostatic charge between them. This charge can, and often does, damage electronic components.

emergency repair disk (ERD) A floppy disk containing data that can help the Windows NT, 2000, or XP Setup utility repair a Windows installation more successfully.

enhanced capabilities port (ECP) A printer or parallel port setting that allows bidirectional communications and can be used with newer ink-jet and laser printers, scanners, and other peripheral devices.

enhanced parallel port (EPP) A printer or parallel port setting that allows bidirectional communications and that can be used with newer ink-jet and laser printers.

expansion bus A bus that connects I/O ports and expansion slots to the motherboard chipset. The expansion bus allows the computer to be expanded using a modular approach. When you need to add something to the computer, you plug specially made circuit boards into the expansion slots on the expansion bus. The devices on these circuit boards are then able to communicate with the CPU and are part of the computer.

extended data out (EDO) An older type of DRAM that requires refreshing less frequently than regular FPM RAM, resulting in improved performance.

extended memory RAM above the 1MB mark in a PC.

extension A set of characters appended to a filename that defines how the file should be handled by the operating system.

external command A command that is an executable file, such as `FORMAT` or `FDISK`.

external data bus The bus that carries data from the CPU to the chipset on the motherboard.

external modem A modem that is contained in a separate box connected to your computer by a cable. It doesn't require resource assignment because it uses the resources assigned to the port to which it connects.

external speed The speed at which the CPU communicates with the motherboard.

F

fast page mode RAM (FPM) An older type of DRAM that measures its speed in nanoseconds of delay. Typical of SIMMs.

fiber-optic cable A type of cable consisting of thin flexible glass fiber surrounded by a rubberized outer coating. Uses an ST or SC connector.

File Transfer Protocol (FTP) A protocol used to transfer data across the Internet, from computer to computer, or on an intranet.

file system The organizational scheme that governs how files are stored and retrieved from a disk. Examples include FAT16, FAT32, NTFS 4.0, and NTFS 5.0.

firewall A form of protection that can be either a stand-alone system or included in other devices, such as routers or servers. You can find firewall solutions that are marketed as hardware-only and others that are software-only. Either way, their role is to limit the traffic in (or out) of the network.

flash update Special software provided by the motherboard manufacturer to replace or change the capabilities of the BIOS.

floppy A magnetic storage medium that uses a floppy disk made of thin plastic enclosed in a protective casing.

form factor The size and shape of a component. For example, AT and ATX are two form factors for motherboards.

format To prepare a disk for use in a specific operating system by creating the allocation units that will be used for storage.

formatter board A circuit board that takes the information a printer receives from the computer and turns it into commands for the various components in the printer.

full backup A backup that copies all data to the archive medium.

G

General Protection Fault (GPF) An error caused when a Windows program accesses memory that another program is using.

ghosting Light images of previously printed pages that you can see on the current page.

grayware Any application that is annoying or that negatively affects the performance of your computer.

H

hardening The process of reducing or eliminating weaknesses, securing services, and attempting to make your environment immune to attacks.

hardware compatibility list (HCL) A list of all hardware that has been verified to work with a particular operating system.

hashing The process of converting a message, or data, into a numeric value for security purposes.

high-voltage differential (HVD) An improved SCSI technology that results in very high maximum distances but that is incompatible with SE and LVD systems.

high-voltage power supply (HVPS) A power supply that provides high-voltage, low-current power to both the charging and transfer corona assemblies in laser and page printers.

hot-plugging/hot-swapping The ability to insert or remove devices without powering down the system.

hyperthreading A feature that enables the computer to multitask more efficiently between CPU-demanding applications.

I

IEEE 802.11 A family of protocols that provides for wireless communications using radio-frequency transmissions.

IEEE 802.11 Wireless LAN Defines the standards for implementing wireless technologies such as infrared and spread-spectrum radio.

image smudging A problem that occurs when toner isn't properly fused to the paper. You can smudge the printed text or graphics by wiping a finger across the page.

incremental backup A type of backup in which only new files or files that have changed since the last full backup or the last incremental backup are included. Incremental backups clear the archive bit on files upon their completion.

Integrated Services Digital Network (ISDN) A digital type of communications that can support two simultaneous 64Kbps data channels on one channel. ISDN is often used to provide a backup line for routers to communicate across a serial connection.

internal command A command that is built into the command interpreter (`COMMAND.COM`) and doesn't exist as an executable file outside of it, such as `DEL` or `DIR`.

internal modem A modem consisting of an expansion card that fits into the PC. It requires a resource assignment, which may come either from Plug and Play or from manual configuration.

internal speed The speed at which a CPU processes data inside its registers.

Internet service provider (ISP) A company that provides access to the Internet.

interrupt request (IRQ) lines Signals used by peripherals to interrupt or stop the CPU and demand attention.

ipconfig A utility used in Windows to display TCP/IP configuration information.

J–L

jumpers and DIP switches Means of configuring various hardware options on the motherboard.

L1 cache The front-side cache holding data waiting to enter the CPU.

L2 cache The back-side cache holding data that has exited from the CPU.

legacy device A device that is based on old technology and isn't Plug and Play–compatible, such as a non-PnP circuit board, an ISA board, or a device that connects to a COM port.

local area network (LAN) A network that is restricted to a single building, a group of buildings, or even a single room. A LAN can have one or more servers.

logical drive An area of space within a partition mapped for use by the operating system and identified by a drive letter, such as `C:` or `D:`.

M

MAC address The address that is either assigned to a network card or burned into the NIC. PCs use MAC addresses to keep track of one another and keep each other separate.

master An IDE drive responsible for managing data transfers for itself and the slave drive.

Media Access Control (MAC) A sublayer of the Data Link layer of the Open Systems Interconnection (OSI) model that controls the way multiple devices use the same media channel. It controls which devices can transmit and when they can transmit.

memory address The named hexadecimal address of a particular location in memory. The operating system uses memory addresses to keep track of what data is stored in what physical location with memory banks.

memory management The methods used by the operating system to manage the transfer of information from storage on the hard disk to a place in RAM.

memory slots Slots on the motherboard that hold the memory chips.

N

network A group of devices connected by some means for the purpose of sharing information or resources.

network interface card (NIC) A computer peripheral card that allows the PC to communicate with a network. The NIC provides the physical interface between the computer and cabling. It prepares data, sends data, and controls the flow of data. It can also receive and translate data into bytes for the CPU to understand.

notification area An alternative term for the System Tray, the area in the bottom-right corner of the Windows screen where the clock resides along with icons for programs running in the background.

NTLDR The bootstrap or startup file for NT-based Windows versions. It starts the loading of the operating system.

O–P

operating system Software that takes charge of the computer in order to manage disk and file behavior, device access, memory management, input/output, and the user interface.

page description language (PDL) A language that describes a whole page being printed by sending commands that describe the text as well as the margins and other settings.

paging file The file used for virtual memory swapping on the hard disk. Also called the *swap file*.

paper transport assembly The part of a printer responsible for moving the paper through the printer. It consists of a motor and several rubberized rollers that each perform a different function.

parallel cable A cable that carries data multiple bits at a time in a given direction.

partition A logical division of a physical hard disk, used to create separate drive letters. Also refers to the act of creating partitions.

passive terminator A terminator that uses resistors to perform the termination.

PC Card device A small card, about the size of a thick credit card, that plugs into the side of a notebook PC and adds capabilities to it. Also called a *PCMCIA device*. The modern standard for such devices is called *CardBus*.

Peripheral Component Interconnect (PCI) An interconnection system that supports both 64-bit and 32-bit data paths, so it can be used in both 486 and Pentium-based systems. In addition, it's processor-independent. The bus communicates with a special bridge circuit that communicates with both the CPU and the bus. The modern standard for general-purpose expansion devices in a PC.

ping A TCP/IP utility used to test whether another host is reachable. An Internet Control Message Protocol (ICMP) request is sent to the host, which responds with a reply if it's reachable. The request times out if the host isn't reachable.

Plug and Play The technology that enables a PC and an operating system to automatically recognize certain types of hardware, including most peripheral devices. It installs the needed drivers for the hardware without user intervention.

port replicator Roughly the same as a docking station, except it tends to be smaller and doesn't contain drive bays.

POST card A circuit board that monitors the PC's boot process and displays a numeric code indicating the part of the boot process being executed.

Post Office Protocol Version 3 (POP3) The protocol used to download e-mail from an SMTP e-mail server to a network client.

power-on self-test (POST) A diagnostic program that runs when you turn on the computer.

power supply The device in a computer that provides the power.

printer controller circuitry A large circuit board that converts signals from the computer into signals for the various assemblies in a laser printer.

printer driver A software component that allows an application to interface with the hardware of a printer.

printer pool A single logical printer that prints to more than one printing device.

processor slot A slot that permits the attachment of the CPU to the motherboard, allowing the CPU to use the other components of the system.

protocol A computer language. Examples of protocols are NetBEUI, IPX/SPX, and TCP/IP.

proxy server A server that acts as an intermediary between a PC and the Internet, caching frequently used information and providing some security.

R

RAID *See* Redundant Array of Independent Disks (RAID).

Real mode Sixteen-bit hardware access. The application has direct access to the resources of the computer without using the operating system.

Redundant Array of Independent Disks (RAID) A method of making several physical disks work together to create a single volume that has properties not possible on a single physical drive.

Registry The hierarchical configuration database in Windows, containing Windows initialization settings. It includes information about both the computer and the users on the system.

resource conflict A problem caused by two or more devices trying to use the same resource.

riser board A circuit board that connects to the motherboard and provides expansion slots (ISA, PCI) so the expansion boards can sit parallel to the motherboard. Common on NLX (low-profile or slimline) systems.

routers Highly intelligent devices that connect multiple network types and determine the best path for sending data. They can route packets across multiple networks and use routing tables to store network addresses to determine the best destination.

S

Safe mode A method of running Windows using a minimal set of system drivers.

search path (*also referred to as* path) A list of locations where the OS looks for a command's needed file when you try to execute the command.

serial cable A cable that carries data one bit at a time in each direction.

server A computer that provides resources to the clients on the network.

service Software that allows a PC to receive and respond to requests from the network.

service information sources Service manuals that can be used for troubleshooting. These manuals can come in several forms, such as booklets, readme files on a CD or DVD, and the manufacturer's website. In most cases, the most up-to-date information is on the website.

service pack A collection of updates to an operating system or application that brings it to a certain update level.

sharing The process of making a resource or folder available for use by other PCs through a network.

shielded twisted pair (STP) A type of cable consisting of two or more pairs of twisted wires that carry data with electrical pulses, surrounded by a metal mesh casing for EMI shielding.

Sidebar A desktop feature of Windows Vista allowing you to add gadgets that do such things as show CPU usage, date, time, and so on.

signed driver A driver that has been certified to work under a specific Windows version and hasn't been changed since its creation.

single-ended (SE) The standard type of SCSI (including SCSI-1 and SCSI-2).

single inline memory module (SIMM) An easily removable circuit board that contains RAM chips. SIMMs are either 8-bit, 30-pin or 32-bit, 72-pin.

slave drive A drive that shares a channel with the master and doesn't manage data transfers. It's totally reliant on the master drive for communication.

smart card A type of badge or card that gives you access to resources.

social troubleshooting The process of troubleshooting a problem by talking with end users.

spyware Malicious software that acts on behalf of a third party. Rather than self-replicating, like viruses and worms, spyware is spread to machines by users who inadvertently ask for it. The users often don't know they have asked for it; they do so by downloading other programs, visiting infected sites, and so on. The spyware program monitors the user's activity and often responds by offering unsolicited pop-up advertisements.

stand-off A spacer between the motherboard and the case floor, made of brass or plastic.

standard parallel port (SPP) A printer or parallel port setting that allows bidirectional communications and that can be used with older ink-jet and laser printers.

static RAM (SRAM) A type of RAM that doesn't require constant electrical refreshing.

switches Like hubs, devices used to link several computers together. Switches differ from hubs in a few important ways. As hubs do, switches repeat signals to the ports, with one exception: rather than send network traffic to all ports, switches have enough intelligence to send the traffic directly to the port the packet was intended for. This reduces the work done by the OSI layers below the Network layer. This, in turn, segments network traffic, resulting in fewer collisions and therefore improved network performance.

symmetric algorithms Encryption that requires both ends of an encrypted message to have the same key and processing algorithms.

synchronous DRAM (SDRAM) DRAM that is synchronized to the speed of the systems in which it's used (PC66 SDRAM runs at 66MHz, PC100 runs at 100MHz, PC133 runs at 133MHz, and so on). Synchronizing the speed of the systems prevents the address bus from having to wait for the memory because of different clock speeds.

system board The spine of the computer, also called the *motherboard*. This component is made of green or brown fiberglass and is placed in the bottom or side of the case.

system files Files used to load the operating system, including its graphic interface and other system components.

T

toner cartridge The printer component that holds the toner. Toner is a black, carbon substance mixed with polyester resins and iron oxide. In most cases, the toner cartridge contains a medium called the *developer*, the print drum, and a cleaning blade.

transfer corona assembly A laser-printer assembly that has a high-voltage electrical charge and that carries toner from the photosensitive drum onto the paper. When the laser writes the images on the photosensitive drum, the toner sticks to the exposed areas. The transfer corona assembly charges the paper, which pulls the toner from the photosensitive drum.

tripping A condition that occurs when the breaker on a device such as a power supply, surge protector, or UPS turns it off because it received a spike.

troubleshooting The process of determining what is wrong with a machine and then taking steps to solve the problem.

U

UAC *See* User Account Control

UltraDMA An operating mode for IDE hard disks that conforms to the ATA-4 standard and higher, allowing high-speed data access (33MBps to 100MBps).

Universal Serial Bus (USB) A high-speed, hot-pluggable serial interface used for connecting external peripherals to a PC. USB is the fastest-growing interface type at this time. The flexibility of the device architecture provides manufacturers with a high-speed chainable port system that is easy to configure. USB devices can be chained with the use of hubs, allowing up to 32 devices to be connected to one port. The transfer rate is also very good, with a maximum throughput of 4Mbps.

unshielded twisted pair (UTP) A type of cable consisting of two or more pairs of twisted wires that carry data with electrical pulses. Doesn't have EMI shielding.

update A newer version of a piece of software. Upgrades generally have new features and must be purchased, but updates are usually free and are provided to fix problems or improve performance.

upgrade An installation of a newer or more feature-rich version of existing software that preserves existing settings.

Upgrade Wizard A utility in the Setup program for Windows 2000/XP that examines the current Windows installation and determines whether there will be any hardware or software compatibility problems in upgrading.

User Account Control (UAC) A feature of Windows Vista that limits applications to standard user privileges and prompts for administrator authorization before allowing any applications to run with escalated privileges.

V

virtual machine A separate computing space created by an operating system to run an application separate from the rest of the system.

virtual memory An area of the hard disk set aside for simulating additional RAM by swapping data into and out of the real RAM.

virus A self-replicating program that "infects" files on a computer. Viruses can be harmless, or they can be extremely destructive.

voltage regulator module (VRM) A device on a motherboard that can adjust the voltage provided to the CPU, to accommodate different CPUs.

W

wide area network (WAN) A network that crosses local, regional, and/or international boundaries.

wildcard A character that stands for other characters. An asterisk (*) stands for any number of characters; a question mark (?) stands for any single character.

Windows component A part of the operating system that can be individually installed or uninstalled.

winipcfg A utility used in Windows to display TCP/IP configuration information.

Wired Equivalent Privacy (WEP) A security standard for wireless devices. WEP encrypts data to provide data security.

Wireless Applications Protocol (WAP) The technology designed for use with wireless devices. WAP functions are equivalent to TCP/IP functions in that they're trying to serve the same purpose for wireless devices. The acronym WAP is also used for Wireless Access Point.

working directory The place where an application stores files it creates during the course of its operation. This is the application's "cubicle."

THE PERFECT COMPANION TO SYBEX'S
COMPTIA A+ COMPLETE STUDY GUIDE

Use the interactive CD included with the book for extra practice. It provides four practice exams, electronic flashcards, and a searchable glossary of key terms.

Approach the A+ Essentials and Practical Application exams with confidence

Before you take the new CompTIA A+ Essentials exam (220-701) or Practical Application exam (220-702), reinforce your test preparation with this concise guide that reviews everything you need to know for both. You'll find full coverage of all exam objectives for both exams and a CD packed with additional study tools.

- Easy-to-use book is organized by exam objectives for quick review
- Flexible review guide goes hand-in-hand with any learning tool on the market, including the Sybex *CompTIA A+ Complete Study Guide*
- "Exam Essentials" sections in each chapter help you zero in on what you need to know
- Book includes over 400 review questions and practice tools

ABOUT THE AUTHOR

Emmett Dulaney, A+, Network+, Security+, is an assistant professor at Anderson University. He has written several certification books on Windows, Security, IT project management, and UNIX. He is the coauthor of two of Sybex's leading certification titles: *CompTIA A+ Complete Study Guide* and *CompTIA Security+ Study Guide*. He is also a well-known certification columnist for *Redmond Magazine* and CertCities.com.

WWW.SYBEX.COM

ISBN: 978-0-470-48650-4

$29.99 US
$35.99 CAN

Sybex®
An Imprint of
WILEY

COMPUTERS/CERTIFICATION GUIDES