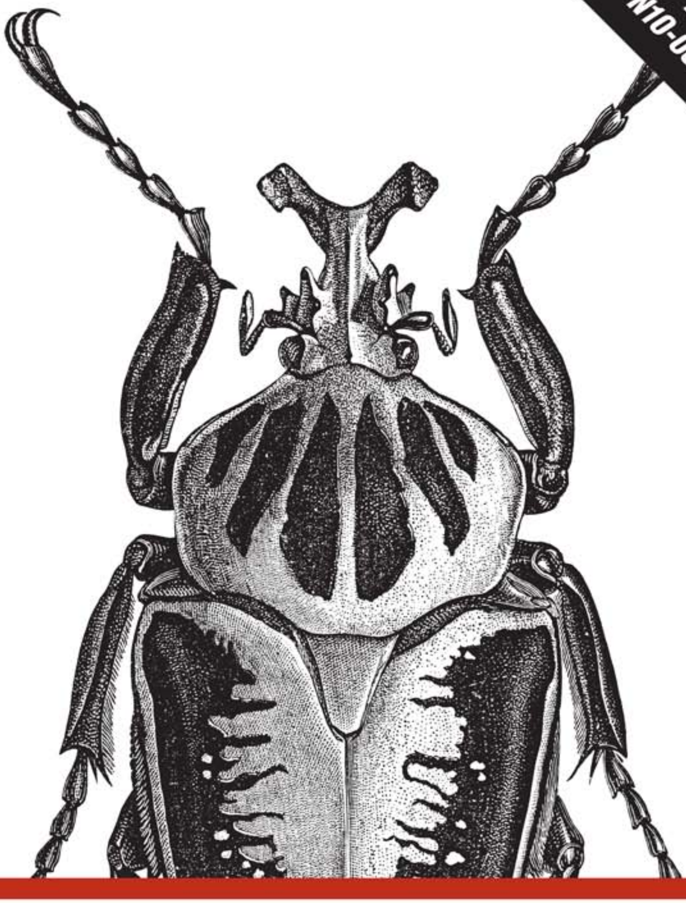
Covers the Essentials, 220-602, 220-603, 220-604, N10-003, SY0-101 Exams



A+, NETWORK+, SECURITY+ EXAMS IN A NUTSHELL

A Desktop Quick Reference

O'REILLY®

Pawan K. Bhardwaj

www.allitebooks.com

A+, NETWORK+, SECURITY+ EXAMS

IN A NUTSHELL

www.allitebooks.com

Other resources from O'Reilly

Related titles

- MCSE Core Required Exams in a Nutshell
- MCSE Core Elective Exams in a Nutshell
- MCSA on Windows Server 2003 Core Exams in a Nutshell
- Security Warrior
- Network Security Assessment
- Internet Core Protocols: The Definitive Guide
- TCP/IP Network Administration
- 802.11 Wireless Networks: The Definitive Guide
- PC Hardware in a Nutshell
- Linux in a Nutshell
- Windows Vista in a Nutshell
- Unix in a Nutshell

oreilly.com

oreilly.com is more than a complete catalog of O'Reilly books. You'll also find links to news, events, articles, weblogs, sample chapters, and code examples.

O'REILLY NETWORK

oreillynet.com is the essential portal for developers interested in open and emerging technologies, including new platforms, programming languages, and operating systems.

Conferences

O'Reilly brings diverse innovators together to nurture the ideas that spark revolutionary industries. We specialize in documenting the latest tools and systems, translating the innovator's knowledge into useful skills for those in the trenches. Visit *conferences.oreilly.com* for our upcoming events.

O'REILLY NETWORK Safari Bookshelf

Safari Bookshelf (*safari.oreilly.com*) is the premier online reference library for programmers and IT professionals. Conduct searches across more than 1,000 books. Subscribers can zero in on answers to time-critical questions in a matter of seconds. Read the books on your Bookshelf from cover to cover or simply flip to the page you need. Try it today for free.

www.allitebooks.com

A+, NETWORK+, SECURITY+ EXAMS

IN A NUTSHELL

Pawan K. Bhardwaj

O'REILLY®

Beijing • Cambridge • Farnham • Köln • Paris • Sebastopol • Taipei • Tokyo

www.allitebooks.com

A+, Network+, Security+ Exams in a Nutshell
by Pawan K. Bhardwaj

Copyright © 2007 Pawan K. Bhardwaj. All rights reserved.
Printed in the United States of America.

Published by O’Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, CA 95472.

O’Reilly books may be purchased for educational, business, or sales promotional use. Online editions are also available for most titles (*safari.oreilly.com*). For more information, contact our corporate/institutional sales department: (800) 998-9938 or *corporate@oreilly.com*.

Editors: Jeff Pepper and Colleen Gorman
Production Editor: Mary Brady
Copyeditor: Mary Brady
Proofreader: Tolman Creek Design

Indexer: Tolman Creek Design
Cover Designer: Karen Montgomery
Interior Designer: David Futato
Illustrators: Robert Romano and Jessamyn Read

Printing History:

March 2007: First Edition.

Nutshell Handbook, the Nutshell Handbook logo, and the O’Reilly logo are registered trademarks of O’Reilly Media, Inc. The *In a Nutshell* series designations, *A+, Network+, Security+ Exams in a Nutshell*, the image of a Goliath beetle, and related trade dress are trademarks of O’Reilly Media, Inc.

Many of the designations used by manufacturers and sellers to distinguish their products are claimed as trademarks. Where those designations appear in this book, and O’Reilly Media, Inc. was aware of a trademark claim, the designations have been printed in caps or initial caps.

While every precaution has been taken in the preparation of this book, the publisher and author assume no responsibility for errors or omissions, or for damages resulting from the use of the information contained herein.

This book uses RepKover™, a durable and flexible lay-flat binding.

ISBN-10: 0-596-52824-8
ISBN-13: 978-0-596-52824-9
[M]

www.allitebooks.com

Table of Contents

www.allitebooks.com

Part II. A+ Exams 220-602, 220-603, and 220-604

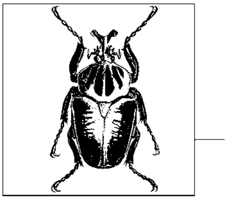
Part III. Network+

www.allitebooks.com

Part IV. Security+

www.allitebooks.com

www.allitebooks.com



Preface

Welcome to *CompTIA: A+, Network+ and Security+ Exams in a Nutshell*. I designed this book for the IT professional who wants to complete his Computer Technology Industry Association (CompTIA) certifications. CompTIA offers multiple entry-level certification exams for various fields of the IT industry. These certifications are platform-independent and are endorsed by several leaders in the IT industry such as Microsoft, IBM, Hewlett Packard, etc. If you are looking to enter the exciting field of IT support, the certifications you will be most interested in are as follows:

A+

The A+ certification is entry-level and is meant for those individuals who want to get into the exciting field of computer hardware and software support. You will need to pass two exams to complete the A+ certification track. The first is A+ Essentials, and it is required. The second exam can be chosen from one of the three exams leading to three different certifications. Exam 220-602 is intended for those individuals who work in a mobile or corporate environment, which calls for a high level of face-to-face client interaction. Candidates who pass the A+ Essentials and the 220-602 exams receive the *IT Technician* certification. The second exam, 220-603, is for those individuals who work remotely to interact with clients. The combination of A+ Essentials and the 220-603 exam leads to the *Remote Support Technician* certification. The third exam, 220-604, is for those individuals who work in repair houses that call for high level of hardware-related troubleshooting, and who seldom interact directly with the client. The combination of A+ Essentials and the 220-604 exam leads to the *Depot Technician* certification.

Network+

The Network+ certification is entry-level and is for those individuals who wish to pursue a career in computer network support. Although it is not a requirement, CompTIA does recommend that a candidate has at least nine months of hands-on experience before she attempts to take this exam.

www.allitebooks.com

CompTIA also recommends that the candidate get the A+ certification before getting the Network+ certification. This certification can be achieved by passing only one exam: N10-003.

Security+

The Security+ certification is entry-level and is for those individuals who wish to pursue a career in computer security. Although it is not a requirement, CompTIA does recommend that the candidate has at least two years of hands-on experience in computer networking with emphasis on security. It also recommends that the candidate get the Network+ certification before getting the Security+ certification. Like the Network+ certification, the Security+ certification can also be attained by passing only one exam: SYO-101.

Each of these CompTIA certifications is covered in this book, and if taken appropriately, each track can get you an entry-level job in the IT field of your choice. These exams just give a head start to your IT career. You can further enhance your career in any of the IT fields by pursuing more advanced certifications from other vendors. Several IT industry leaders, such as Microsoft, IBM, or Hewlett Packard, recognize the CompTIA certifications. For example, Microsoft recognizes the combination of A+ and Network+ certifications as one of the elective exams in its MCSA and MCSE tracks.

The focus of this book is on providing the core knowledge to prepare you for the two A+ exams—the Network+ exam and the Security+ exam. This book is meant to be used as part of your final preparation, and not as your only preparation. Think of this as the notes you'd have written down if you were to highlight and then record every essential nugget of information related to the skills being measured in the A+, the Network+, and the Security+ exams.

Basically, what I did was to boil the required knowledge down to its finest core. Thus, rather than having 500 to 700 pages covering each exam, there's just approximately 150 pages for each. With this in mind, the best way to use this book is as part of your final review. So after you've built sufficient hands-on expertise and studied all the relevant texts, grab this book and study it cover to cover as part of your final exam cram.

> Most of the individuals start their IT support career with the A+ certification, and then move on to the Network+ certification to prove their skills in computer network support. The Security+ certification is basically meant for those individuals who either work in a secure computing environment or wish to attain more advanced security-related certifications. It is highly recommended that if you are just starting your IT career, you should start with the A+ certification, choosing an appropriate A+ track.

One of the good things about the CompTIA exams is that once you pass the exam for any of the available tracks, the certification never expires so you don't have to worry about the retirement of exams. But this certainly does not mean that you should quit studying. Studies are as essential as hands-on experience in any technical field. So, upgrading yourself with newer exam objectives in order to keep you updated with changes in technology is not a bad idea.

Conventions Used in This Book

Each part within this book corresponds to a single Microsoft exam and consists of the following sections:

Exam Overview
    Provides a brief introduction to the exam's topic, a list of objectives, and a cross reference to where the objectives are covered.

Study Guide
    Provides a comprehensive study guide for the skills being measured on the exam. You should read through and and study this section extensively. If you encounter topics you haven't practiced with and studied extensively prior to reading this text, you should do more hands-on work with the related area of study and refer to an expanded discussion in a relevant text. Once you've built the real-world know-how and developed the essential background needed to succeed, you can resume your studies and move forward.

Prep and Practice
    Provides exercises that we suggest to supplement your studies, highlights from all the topics covered for the exam, and practice questions to help test your knowledge. Sample questions are followed by answers with explanations where necessary.

The following font conventions are used in this book:

`Constant width`
    Used for code terms, command-line text, command-line options, and values that should be typed literally.

Italics
    Used for URLs, variables, and to introduce new terms.

Additionally, we will also use the following elements:

Notes are used to provide additional information or highlight a specific point.

Warnings are used to provide details on potential problems.

Other Study Resources

There is no single magic bullet for passing the CompTIA Certification exams. Your current knowledge will largely determine your success with this Study Guide and on the exams. If you encounter topics you haven't practiced with and studied extensively prior to reading this text, you need further preparation. Get the practical hands-on know-how and the practical knowledge before continuing.

Throughout your preparations for certification, we recommend that you regularly visit the CompTIA web site at *http://certification.comptia.org*. The related pages will help you keep up to date with the certification process and any changes that may occur from time to time.

A wide variety of CompTIA certification study guides, training classes, and learning resources are available. Also, a large number of practice tests and exam simulations are available for purchase and for free on the Web. These tests, like this book, are useful as part of your exam preparation.

How to Contact Us

I have worked with the good folks at O'Reilly to test and verify the information in this book to the best of my ability, but you may find that features have changed (or even that I have made mistakes!). To make this book better, please let me know about any errors you find, as well as your suggestions for future editions, by writing to:

O'Reilly Media, Inc.
1005 Gravenstein Highway North
Sebastopol, CA 95472
800-998-9938 (in the United States or Canada)
707-829-0515 (international/local)
707-829-0104 (fax)

You can also send us messages electronically. To be put on the mailing list or request a catalog, send email to:

info@oreilly.com

O'Reilly has a web page for this book, which lists errata, examples, and any additional information. You can access this page at:

http:///www.oreilly.com/catalog/9780596528249

To ask technical questions, to comment on the book, or more information about the authors, please send email to:

bookquestions@oreilly.com

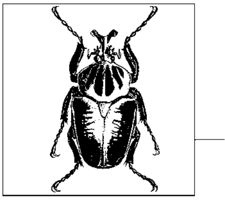
For more information about O'Reilly, please visit:

http://www.oreilly.com

Acknowledgments

Special thanks go to Jeff Pepper for pioneering the entire project from start to finish. I would like to thank John Vacca for his fine work in editing this entire text. Chris Crayton and Erik Eckel did a superb job of finding technical issues and making sure that all topics were covered appropriately. I also wish to thank Mary Brady at O'Reilly for ensuring a smooth production process.

A+ Essentials



1

Overview of A+ Essentials Exam

The A+ Essentials exam is the first of CompTIA's two exams required for completing the A+ certification. The A+ certification is an entry-level certification for those individuals who wish to pursue their careers in computer hardware and software support. The candidate must pass two exams in order to get his A+ certification. You can choose one of the other three elective exams—*IT Technician Exam 220-602, Remote Support Technician Exam 220-603* or *Depot Technician Exam 220-604*—to get an appropriate A+ certification. The second part of this book (Chapters 4, 5, and 6) covers the elective exams.

The main focus of the A+ Essentials exam is to test your knowledge on the basics of computer hardware. The exam focuses on your skills to install, build, upgrade, repair, configure, troubleshoot, optimize, diagnose problems, and to perform preventive maintenance of personal computers and the installed operating systems.

Aside from testing your knowledge of computer components and operating systems, this exam also covers networking concepts and printing and scanning devices. It has recently been revised to include newer areas of study, such as computer security, safety and environmental issues, and communications and professionalism. Another new area is the knowledge of laptops and portable devices. In each of the study areas, you are expected to be skilled in identifying individual computer components as well as in installing, upgrading, and configuring them. You must also have hands-on experience in optimizing performance, using appropriate tools to diagnose problems, and performing preventive maintenance.

The approximate percentage of each section in Exams 220-602, 220-603, and 220-604 is given in Table 1-1.

Table 1-1. A+ Essentials exam domains and percentage of coverage

Domain	Percentage of coverage
Personal computer components	21 percent
Laptops and mobile devices	11 percent
Operating systems	21 percent
Printers and scanners	9 percent
Networks	12 percent
Security	11 percent
Safety and environmental issues	10 percent
Communication and professionalism	5 percent

CompTIA recommends that in order to be prepared for the A+ Essentials exam, you should have approximately 500 hours of actual active experience with computer hardware, either in the field or in a lab. It is a good idea to have studied an A+ certification exam self-paced study guide or attended a training course before you attempt to write any of the A+ exams. If you have, you should be ready to use this section of the book as your final exam preparation.

A+ Essentials is the first of the two required exams to complete your A+ certification. For the second exam, you can choose from Exams 220-602, 220-603, and 220-604. The combination of A+ Essentials and 220-602 gets you the *IT Technician* certification. *A+* Essentials and Exam 220-603 gets you the *Remote Support Technician* certification. Similarly, the combination of A+ Essentials and 220-604 gets you the *Depot Technician* certification.

Areas of Study for the A+ Essentials Exam

Personal Computer Components

- Identify the fundamental principles of using personal computers.
- Identify the names, purposes and characteristics of the following storage devices:
  - — FDD
  - — HDD
  - — CD/DVD/RW (e.g., drive speeds and media types)
  - — Removable storage (e.g., tape drive and solid states such as thumb drive, flash and SD cards, USB, external CD-RW, and hard drives)
- Identify the names, purposes, and characteristics of the following motherboards:
  - — Form Factors (e.g., ATX/BTX and micro ATX/NLX)
  - — Components:
    - Integrated I/Os (e.g., sound, video, USB, serial, IEEE 1394/firewire, parallel, NIC, and modem)
    - Memory slots (e.g., RIMM and DIMM)
    - Processor sockets
    - External cache memory
    - Bus architecture
    - Bus slots (e.g., PCI, AGP, PCIE, AMR, and CNR)
    - EIDE/PATA
    - SATA
    - SCSI Technology
  - — Chipsets
  - — BIOS/CMOS/Firmware
  - — Riser card/daughter board
- Identify the names, purposes, and characteristics of power supplies—for example, AC adapter, ATX, proprietary, and voltage.
- Identify the names, purposes and characteristics of processor/CPUs, such as the following:
  - — CPU chips (AMD and Intel)
  - — CPU technologies:
    - Hyperthreading
    - Dual core
    - Throttling
    - Micro code (MMX)
    - Overlocking

        - Cache
        - VRM
        - Speed (real versus actual)
        - 32-bit versus 64-bit

- Identify the names, purposes, and characteristics of memory, such as the following:
    - Types of memory (e.g., DRAM, SRAM, SDRAM, DDR/DDR2, and RAMBUS)
    - Operational characteristics:
        - Memory chips (8,16,32)
        - Parity versus non-parity
        - ECC versus non-ECC
        - Single-sided versus double-sided
- Identify the names, purposes, and characteristics of display devices—for example, projectors, CRT, and LCD:
    - Connector types (e.g., VGA, DVI/HDMi, S-Video, and Component/RGB)
    - Settings (e.g., V-hold, refresh rate, and resolution)
- Identify the names, purposes, and characteristics of input devices—for example: mouse, keyboard, bar code reader, multimedia (e.g., web and digital cameras, MIDI, and microphones), biometric devices, and touch screens.
- Identify the names, purposes, and characteristics of adapter cards:
    - Video including PCI/PCI-E and AGP
    - Multimedia
    - I/O (SCSI, serial, USB, and Parallel)
    - Communications, including network and modem
- Identify the names, purposes, and characteristics of ports and cables—for example, USB 1.1 and 2.0, parallel, serial, IEEE 1394/Firewire, RJ45 and RJ11, PS2/MINI-DIN, centronics (e.g., mini, and 36), multimedia (e.g., 1/8 connector, MIDSI COAX, and SPDIF).
- Identify the names, purposes, and characteristics of cooling systems—for example: heat sinks, CPU and case fans, liquid cooling systems, and thermal compounds.
- Install, configure, optimize, and upgrade personal computer components.
- Add, remove and configure internal and external storage devices:
    - Drive preparation of internal and external storage devices, including format/filesystems and imaging technology
- Install display devices.
- Add, remove, and configure basic input and multimedia devices.
- Identify tools, diagnostic procedures, and troubleshooting techniques for personal computer components.

- Recognize the basic aspects of troubleshooting theory—for example:
  - Perform backups before making changes
  - Assess a problem systematically and divide large problems into smaller components to be analyzed individually
  - Verify even the obvious. Determine whether the problem is something simple or complicated, and make no assumptions
  - Research ideas and establish priorities
  - Document findings, actions, and outcomes
- Identify and apply basic diagnostic procedures and troubleshooting techniques—for example:
  - Identify the problem using techniques such as questioning the user and identifying any user changes to the computer
  - Analyze the problem, including considering potential causes and making an initial determination of software and/or hardware problems
  - Test related components using avenues such as inspection, connections, hardware/software configurations, device managers, and consulting vendor documentation
  - Evaluate results and take additional steps if needed, such as consultation, use of alternate resources, and manuals
  - Document activities and outcomes
- Recognize and isolate issues with display, power, basic input devices, storage, memory, thermal, and POST errors (e.g., BIOS and hardware).
- Apply basic troubleshooting techniques to check for problems (e.g., thermal issues, error codes, power, connections—including cables and/or pins—compatibility, functionality, and software/drivers) with components—for example:
  - Motherboards
  - Power supply
  - Processor/CPUs
  - Memory
  - Display devices
  - Input devices
  - Adapter cards
- Recognize the names, purposes, characteristics, and appropriate application of tools.
- Perform preventive maintenance on personal computer components.
- Identify and apply basic aspects of preventive maintenance theory—for example:
  - Visual/audio inspection
  - Driver/firmware updates
  - Scheduling preventive maintenance

www.allitebooks.com

  - Use of appropriate tools and cleaning materials
  - Ensuring proper environment
- Identify and apply common preventive maintenance techniques for devices such as input devices and batteries.

Laptops and Portable Devices

- Identify the fundamental principles of using laptops and portable devices.
- Identify names, purposes, and characteristics of laptop-specific items, such as:
  - Form Factors such as memory and hard drives
  - Peripherals (e.g., docking stations, port replicators, and media/accessory bays)
  - Expansion slots (e.g., PCMCIA I, II, and III, and card and express bus)
  - Ports (e.g., mini PCI slot)
  - Communication connections (e.g., Bluetooth, infrared, cellular WAN, and Ethernet)
  - Power and electrical input devices (e.g., auto-switching and fixed-input power supplies and batteries)
  - LCD technologies (e.g., active and passive matrix, resolution, such as XGA, SXGA+, UXGA, WUXGA, contrast radio, and native resolution)
  - Input devices (e.g., stylus/digitizer, function (Fn) keys, and pointing devices such as touch pad and point stick/track point)
- Identify and distinguish between mobile and desktop motherboards and processors, including throttling, power management, and Wi-Fi.
- Install, configure, optimize, and upgrade laptops and portable devices.
- Configure power management:
  - Identify the features of BIOS-ACPI
  - Identify the difference between suspend, hibernate, and standby
- Demonstrate safe removal of laptop-specific hardware such as peripherals, hot-swappable devices, and non-hot-swappable devices.
- Identify tools, basic diagnostic procedures, and troubleshooting techniques for laptops and portable devices.
- Use procedures and techniques to diagnose power conditions, video, keyboard, pointer, and wireless card issues—for example:
  - Verify AC power (e.g., LEDs and swap AC adapter)
  - Verify DC power
  - Remove unneeded peripherals
  - Plug in external monitor
  - Toggle Fn keys
  - Check LCD cutoff switch

- — Verify backlight functionality and pixilation
- — Stylus issues (e.g., digitizer problems)
- — Unique laptop keypad issues
- — Antenna wires

- Perform preventive maintenance on laptops and portable devices.
- Identify and apply common preventive maintenance techniques for laptops and portable devices—for example, cooling devices, hardware and video cleaning materials and operating environments, including temperature and air quality, storage, and transportation and shipping.

Operating Systems

Identify the fundamentals of using operating systems

- Identify differences between operating systems (e.g., Mac, Windows, and Linux), and describe operating system revision levels, including GIU, system requirements and application and hardware compatibility.
- Identify names, purposes, and characteristics of the primary operating system components, including registry, virtual memory, and filesystem.
- Describe features of operating system interfaces—for example:
  - — Windows Explorer
  - — My Computer
  - — Control Panel
  - — Command Prompt
  - — My Network Places
  - — Taskbar/Systray
  - — Start Menu
- Identify the names, locations, purposes, and characteristics of operating system files—for example:
  - — *BOOT.INI*
  - — *NTLDR*
  - — *NTDETECT.COM*
  - — *NTBOOTDD.SYS*
  - — Registry data files
- Identify concepts and procedures for creating, viewing, and managing disks, directories, and files in operating systems—for example:
  - — Disks (e.g., active, primary, extended, and logical partitions)
  - — Filesystems (e.g., FAT 32 and NTFS)
  - — Directory structures (e.g., create folders, navigate directory structures)
  - — Files (e.g., creation, extensions, attributes, permissions)
- Install, configure, optimize, and upgrade operating systems (references to upgrading from Windows 95 and NT may be made).

- Identify procedures for installing operating systems, including:
  - Verification of hardware compatibility and minimum requirements
  - Installation methods (e.g., boot media—such as CD, floppy, or USB—network installation, and drive imaging)
  - Operating system installation options (e.g., attended/unattended, file-system type, and network configuration)
  - Disk preparation order (e.g., start installation, partition, and format drive)
  - Device driver configuration (e.g., install and upload device drivers)
  - Verification of installation
- Identify procedures for upgrading operating systems, including:
  - Upgrade considerations (e.g., hardware and application and/or network compatibility)
  - Implementation (e.g., back up data and install additional Windows components)
- Install/add a device, including loading and adding device drivers and required software, and perform the following actions, such as:
  - Determine whether permissions are adequate for performing the task
  - Device driver installation (e.g., automated and/or manual search and installation of device drivers)
  - Using unsigned drivers (e.g., driver signing)
  - Verify installation of the driver (e.g., device manager and functionality)
- Identify procedures and utilities used to optimize operating systems—for example, virtual memory, hard drives, temporary files, services, startup, and applications.
- Identify tools, diagnostic procedures, and troubleshooting techniques for operating systems.
- Identify basic boot sequences, methods, and utilities for recovering operating systems:
  - Boot methods (e.g., safe mode, recovery console, and boot to restore point)
  - Automated System Recovery, aka ASR (e.g., Emergency Repair Disk [ERD])
- Identify and apply diagnostic procedures and troubleshooting techniques—for example:
  - Identify the problem by questioning the user and identifying user changes to the computer
  - Analyze the problem, including identifying potential causes and making an initial determination of a software and/or hardware problem
  - Test related components, including connections, hardware/software configurations, and device managers by consulting vendor documentation

  - Evaluate results and take additional steps if needed, such as consultation and using alternate resources and manuals
  - Document activities and outcomes
- Recognize and resolve common operational issues such as blue screen, system lock-up, input/output devices, application installs, start or load, and Windows-specific printing problems (e.g., a device/service failed to start or a device/program in registry is not found).
- Explain common error messages and codes—for example:
  - Boot (e.g., invalid boot disk, inaccessible boot drive, and missing NTLDR)
  - Startup (e.g., a device/service failed to start, a device/program in registry is not found)
  - Event Viewer
  - Registry
  - Windows reporting
- Identify the names, locations, purposes, and characteristics of operating system utilities—for example:
  - Disk management tools (e.g., DEFRAG, NTBACKUP, CHKDSK, and Format)
  - System management tools (e.g., device and task manager, and *MSCONFIG.EXE*)
  - File management tools (e.g., Windows Explorer and *ATTRIB.EXE*)
- Perform preventive maintenance on operating systems.
- Describe common utilities for performing preventive maintenance on operating systems—for example, software and Windows updates (e.g., service packs), scheduled backups/restores, and restore points.

Printers and Scanners

- Identify the fundamental principles of using printers and scanners.
- Identify the differences between types of printer and scanner technologies (e.g., laser, inkjet, thermal, solid ink, and impact).
- Identify names, purposes, and characteristics of printer and scanner components (e.g., memory, driver, and firmware) and consumables (e.g., toner, ink cartridge, and paper).
- Identify the names, purposes, and characteristics of interfaces used by printers and scanners, including port and cable types—for example:
  - Parallel
  - Network (e.g., NIC and print servers)
  - USB
  - Serial

    - IEEE 1394/firewire
    - Wireless (e.g., Bluetooth, 802.11, and Infrared)
    - SCSI
- Identify basic concepts of installing, configuring, optimizing, and upgrading printers and scanners.
- Install and configure printers and scanners:
    - Power and connect the device using a local or network port
    - Install and update the device driver and calibrate the device
    - Configure options and default settings
    - Print a test page
- Optimize printer performance—for example, printer settings, such as tray switching, print spool settings, device calibration, media types, and paper orientation.
- Identify tools, basic diagnostic procedures, and troubleshooting techniques for printers and scanners.
- Gather information about printer/scanner problems:
    - Identify the symptom
    - Review device error codes, computer error messages, and history (e.g., event log and user reports)
    - Print or scan test page
    - Use appropriate generic or vendor-specific diagnostic tools, including web-based utilities
- Review and analyze collected data:
    - Establish probable causes
    - Review the service documentation
    - Review the knowledge base and define and isolate the problem (e.g., software versus hardware, the driver, connectivity, or the printer)
- Identify solutions to identified printer/scanner problems:
    - Define the specific cause and apply a fix
    - Replace consumables as needed
    - Verify functionality and get user acceptance of the problem fix

Networks

- Identify the fundamental principles of networks.
- Describe basic networking concepts:
    - Addressing
    - Bandwidth
    - Status indicators
    - Protocols (e.g., TCP/IP [including IP], classful subnet, and IPX/SPX [including NWLINK and NETBWUI/NETBIOS])

- — Full-duplex or half-duplex
- — Cabling (e.g., twisted pair, coaxial cable, fiber optic, and RS-232)
- — Networking models, including peer-to-peer and client/server

- Identify names, purposes, and characteristics of the common network cables:
  - — Plenum/PVC
  - — UTP (e.g., CAT3, CAT5/5e, and CAT6)
  - — STP
  - — Fiber (e.g., single-mode and multimode)
- Identify names, purposes, and characteristics of network connectors (e.g., RJ45 and RJ11, ST/SC/LC, USB, and IEEE 1394/firewire).
- Identify names, purposes, and characteristics of technologies for establishing connectivity—for example:
  - — LAN/WAN
  - — ISDN
  - — Broadband (e.g., DSL, cable, and satellite)
  - — Dial-up
  - — Wireless (all 802.11)
  - — Infrared
  - — Bluetooth
  - — Cellular
  - — VoIP
- Install, configure, optimize, and upgrade networks.
- Install and configure network cards.
- Install, identify, and obtain wired and wireless connection.
- Identify tools, diagnostic procedures, and troubleshooting techniques for networks.
- Explain status indicators—for example, speed, connection and activity lights, and wireless signal strength.

Security

- Identify the fundamental principles of security.
- Identify names, purposes, and characteristics of hardware and software security—for example:
  - — Hardware deconstruction/recycling
  - — Smart cards/biometrics (e.g., key fobs, cards, chips, and scans)
  - — Authentication technologies (e.g., username, password, biometrics, and smart cards)
  - — Malicious software protection (e.g., viruses, Trojans, worms, spam, spyware, adware, and grayware)

  - Software firewalls
  - File system security (e.g., FAT32 and NTFS)
- Identify names, purposes, and characteristics of wireless security—for example:
  - Wireless encryption (e.g., WEP.x and WPA.x) and client configuration
  - Access points (e.g., disable DHCP/use static IP, change SSID from the default, disable SSID broadcast, use MAC filtering, change the default username and password, update firmware, and firewall)
- Identify names, purposes, and characteristics of data and physical security—for example:
  - Data access (basic local security policy)
  - Encryption technologies
  - Backups
  - Data migration
  - Data/remnant removal
  - Password management
  - Locking workstation (e.g., hardware and operating system)
- Describe importance and process of incidence reporting.
- Recognize and respond appropriately to social engineering situations.
- Install, configure, upgrade, and optimize security.
- Install, configure, upgrade, and optimize hardware, software, and data security—for example:
  - BIOS
  - Smart cards
  - Authentication technologies
  - Malicious software protection
  - Data access (basic local security policy)
  - Backup procedures and access to backups
  - Data migration
  - Data/remnant removal
- Identify tools, diagnostic procedures, and troubleshooting techniques for security.
- Diagnose and troubleshoot hardware, software, and data security issues—for example:
  - BIOS
  - Smart cards and biometrics
  - Authentication technologies
  - Malicious software
  - File system (e.g., FAT32 and NTFS)
  - Data access (e.g., basic local security policy)
  - Backup
  - Data migration

- Perform preventive maintenance for computer security.
- Implement software security preventive maintenance techniques such as installing service packs and patches and training users about malicious software prevention technologies.

Safety and Environmental Issues

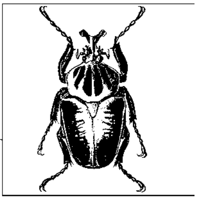
- Describe the aspects and importance of safety and environmental issues.
- Identify potential safety hazards and take preventive action.
- Use Material Safety Data Sheets (MSDS) or equivalent documentation as well as appropriate equipment documentation.
- Use appropriate repair tools.
- Describe methods to handle environmental and human accidents, including incident reporting.
- Identify potential hazards and implement proper safety procedures, including ESD precautions and procedures, a safe work environment, and equipment handling.
- Identify proper disposal procedures for batteries, display devices, and chemical solvents and cans.

Communication and Professionalism

- Use good communication skills—including listening and tact/discretion—when communicating with customers and colleagues.
- Use job-related professional behavior, including notation of privacy, confidentiality, and respect for the customer and customers' property.
- Behavior:
  - Use clear, concise, and direct statements.
  - Allow the customer to complete statements—avoid interrupting.
  - Clarify customer statements—ask pertinent questions.
  - Avoid using jargon, abbreviations, and acronyms.
  - Listen to customers.
- Property:
  - Telephone, laptop, desktop computer, printer, monitor, etc.

2

A+ Essentials Study Guide



This chapter provides a study guide for the CompTIA A+ Essentials exam. Various sections in this chapter are organized to cover the related objectives of the exam. Each section identifies the exam objective, provides an overview of the objective, and then discusses the key details that you should master before taking the exam.

An overview of the sections in this chapter is as follows:

Personal Computer Components
: This section describes the components of personal computers such as the processor, memory, storage devices (such as hard disks and removable drives), display devices, input/output devices (such as the keyboard and mouse), and various ports and types of cables used to connect these components. Installing, configuring, upgrading, and troubleshooting these components are also covered in this section.

Laptops and Portable Devices
: This section describes the identification of different components of portable computers. Installing, configuring, upgrading, and troubleshooting these portable computers is also covered in this section.

Operating Systems
: This section describes requirements and installation procedures for various operating systems used on personal computers such as Mac OS X, Linux, Windows 98, Windows 2000, and Windows XP. Upgrading a previously installed operating system and troubleshooting common problems is also covered in this section.

Printers and Scanners
: This section describes the basics of installing, configuring, optimizing, upgrading, and troubleshooting printers and scanners.

Networks

This section describes the fundamentals of wired and wireless computer networking, including concepts, network topologies, networking components (such as cables, hubs, switches and routers), and procedures to diagnose and rectify common networking problems.

Security

This section describes basic concepts behind computer security, including the identification of security threats, hardware, software and data security. Maintaining operating system and data security by installing software updates, hot fixes, and service packs is also covered in this section.

Safety and Environmental Issues

This section describes the aspects and importance of various safety issues related to personal computers, including safety hazards and environmental and human-generated accidents. It also covers the implementation of proper precautions and procedures to prevent such accidents. Incident reporting is covered in this section as well.

Communication and Professionalism

This section describes methods of professionalism on the job and communication techniques when interacting with customers. Active listening techniques, customer privacy, and other standard customer service standards are covered in this section.

> There is a great deal of overlap between the objectives of the A+ Essentials exam and the A+ exams 220-602, 220-603, and 220-604. Chapter 5 includes a detailed discussion of these topics. I recommend that you read Chapter 5 before taking the A+ Essentials exam because it may include questions from either of these chapters.

In order to complete the study for the A+ Essentials exam, I suggest that you gain access to a computer that can be opened and, if required, have its parts inspected, uninstalled, reinstalled, or upgraded. The personal computer should preferably have the following hardware configuration:

- An Intel 233 MHz or faster processor (350 MHz recommended) with a CD-ROM or DVD drive
- A minimum of 256 MB RAM (512 MB recommended)
- At least 2 GB of free hard disk space
- A Super VGA or higher-resolution monitor
- A keyboard and a mouse

You must also have access to a printer with appropriate driver software and, if possible, a scanner. Aside from this, you need appropriate tools in order to install, uninstall, or upgrade the components of your personal computer.

www.allitebooks.com

The exercises included in this book should be part of your preparation for the exams. Do not perform any exercises in a production environment and do not use any PC that you use for your regular work, but instead create a test environment with the recommended hardware.

Personal Computer Components

This part of the A+ Essentials exam deals mainly with the identification, installation, upgrading, and basic troubleshooting of different parts of personal computers. This part of the study guide covers about one-fifth of the exam objectives. As a hardware technician, you are expected to have extensive knowledge of different components of personal computers. These components include storage devices, motherboards, processors, memory, power supplies, and adapter cards. It is also necessary to have a good understanding of ports and cable types that are used inside the computer and for connecting external peripherals. This section provides an overview of these components.

Components of Motherboards

The motherboard or the system board is made up of several components such as the central processing unit (CPU), memory slots, video section, and so on. Each component on the motherboard has a specific job. In this section, we will look at some of the most common motherboard components and their functions. Motherboards are mainly divided into the following two categories:

Integrated motherboards

Integrated motherboards have most of the essential components on them, which are otherwise installed as separate adapter cards on expansion slots. The major advantage of this type of motherboard is that all major functions are handled by a single circuit board. On the other hand, the drawback is that if one of the components fails, you might need to replace the entire motherboard. Most of the new motherboards fall into this category.

Non-integrated motherboards

Non-integrated motherboards do not have all components on them but are installed as adapter cards on expansion slots. These components include video cards, disk controllers, network adapters, and audio circuitry. The main advantage is that if an individual component fails, it can be replaced easily. The disadvantage is that the inside of the computer is full of adapters and wires. Most of the motherboards on older computers fall into this category.

Form Factors

Form Factor refers to the design of the motherboard. It describes how the components are laid out and what type of case they fit into, and what type of power supply the motherboard uses. Popular Form Factors include ATX, Micro ATX, BTX, and NLX. These are summarized in the following paragraphs:

ATX

ATX stands for *Advanced Technology Extended*. This technology was designed by Intel to allow easier expansion. Currently, ATX motherboards are the most popular motherboards. With most of the components integrated onto the motherboard, there is still sufficient scope to add additional components. The expansion slots are located at right angles to the processor and memory, which makes it easier to install full-length adapter cards. Moreover, the processor and memory are located at the back of the card, in line with the power supply, which makes better air flow for cooling them. It supports *soft power off* support, meaning that the system can be turned off using the operating system instead of using the power switch. It also supports a 3.3 volt power supply from an ATX power supply. The power supply connector is a single 20-pin connector.

Micro ATX

The Micro ATX Form Factor uses a smaller footprint than its big brother ATX. The maximum motherboard size is 9.6"×9.6". It uses a compact design, which is meant for a lower number of integrated components, lesser expansion slots, and lesser memory slots. This simply means that the power supply can be of lower wattage than the standard ATX motherboard to reduce power consumption. The Micro ATX motherboard can still fit well into a standard ATX case. To compromise with a lesser number of components, it provides additional USB ports to connect external devices. Another variation of Micro ATX is the *Flex ATX*, with the size of the motherboard reduced to 9.6"×7.5" (the smallest in the ATX family). Both Micro ATX and Flex ATX offer limited expandability.

BTX

The BTX Form Factor is the latest in motherboard designs. The major concern behind this design is the layout of heat-producing components such as chipsets, processors, and graphics controllers. This design specifies that all heat-producing components can use the primary airflow of the computer thereby reducing the need for additional cooling fans that produce more noise. The BTX Form Factor specifies better placement of components for back panel I/O controllers. Although it is smaller than the Micro ATX in size, the BTX design is scalable and can be taken to the tower-size cases.

NLX

NLX stands for *New Low Profile Extended* Form Factor. In this design, most of the expansion slots are placed sideways on special *riser cards*. The adapter cards are installed on riser card expansion slots, which ultimately become parallel to the motherboard. Motherboards with this design can use the ATX power supplies. The NLX design did not become very popular and was eventually replaced by newer advanced technologies such as the Micro ATX.

Components of motherboards

In older computers, motherboards had very few integrated components and required a large number of adapter cards for video and hard disk and floppy disk interfaces. In contrast, as the technology advanced, several interfaces were integrated on the motherboard and fewer adapters were required. This section covers a summary of different components that are generally found on the computer motherboard. Different components of a typical motherboard are shown in Figure 2-1.

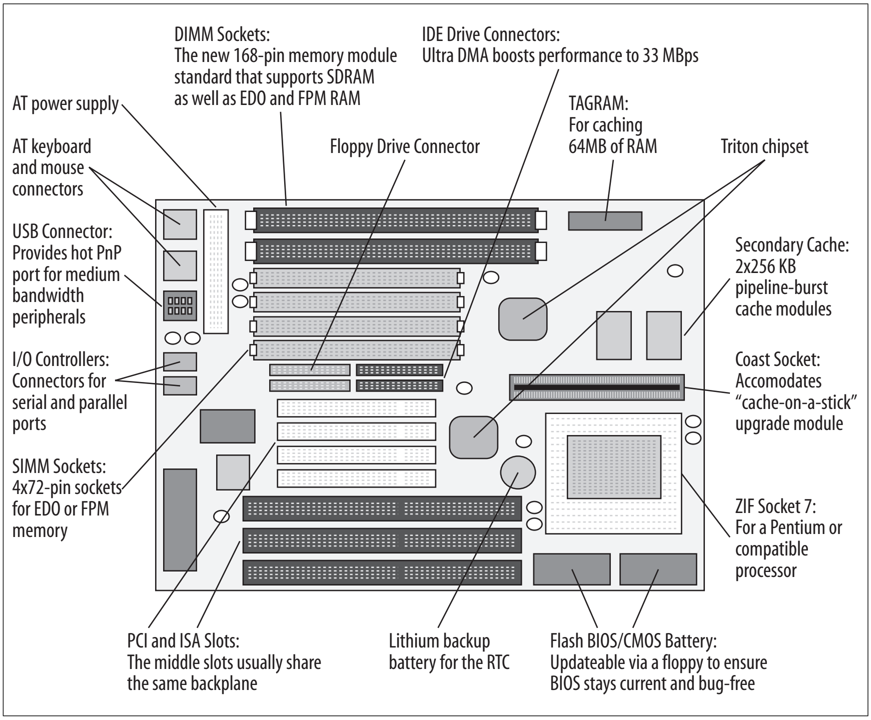

DIMM Sockets:
The new 168-pin memory module standard that supports SDRAM as well as EDO and FPM RAM
IDE Drive Connectors:
Ultra DMA boosts performance to 33 MBps
AT power supply
TAGRAM:
For caching 64MB of RAM
AT keyboard and mouse connectors
Floppy Drive Connector
Triton chipset
USB Connector:
Provides hot PnP port for medium bandwidth peripherals
Secondary Cache:
2x256 KB pipeline-burst cache modules
I/O Controllers:
Connectors for serial and parallel ports
Coast Socket:
Accomodates "cache-on-a-stick" upgrade module
SIMM Sockets:
4x72-pin sockets for EDO or FPM memory
ZIF Socket 7:
For a Pentium or compatible processor
PCI and ISA Slots:
The middle slots usually share the same backplane
Lithium backup battery for the RTC
Flash BIOS/CMOS Battery:
Updateable via a floppy to ensure BIOS stays current and bug-free

Figure 2-1. Components of a motherboard

Chipsets. The *chipset* of a motherboard refers to the collection of semiconductor chips that provide interfaces for expansion cards, memory, peripherals, and interfaces. The make and model of a chipset depends on a particular *Original Equipment Manufacturer (OEM)*. Each chipset is designed to offer certain features such as onboard audio and video functionality. Chipsets are divided into two main categories—Northbridge and Southbridge:

Northbridge

The *Northbridge* is a chipset that does not refer to any brand name but is the technique used to allow communication among high-speed peripherals such as memory, the Peripheral Component Interconnect (PCI) bus, the Accelerated Graphics Port (AGP) bus and the Level 2 processor cache (L2 Cache). The Northbridge communicates with the processor using a *front side bus (FSB)*. The actual performance of the motherboard depends on the performance of the Northbridge chipset. It also manages communication with the Southbridge chipset.

Southbridge

The *Southbridge* chipset controls all of the computer's onboard Input/Output (I/O) functions such as USB, Firewire, PS/2, parallel, serial, wired, and wireless LAN ports, and IDE, audio, and so on. Southbridge usually consists of a single semiconductor chip.

BIOS/Firmware. The *Basic Input/Output System (BIOS)* or *firmware* of the computer is low-level software stored on a semiconductor chip, which is called the *BIOS chip*. BIOS controls how the processor and chipsets interact with the installed operating system, and it also helps detect the hardware and to allocate system resources to it. BIOS is activated as soon as the computer is powered on. The BIOS chip is a dual-line chip with 28 or 32 pins and is usually marked as such. Major manufacturers of BIOS chips include AMI, Phoenix/Award, and Winbond.

The *cmplementary metal-oxide semiconductor (CMOS)* chip, on the other hand, is a memory chip that stores certain computer settings (such as the date and time) even when the computer is powered off. The CMOS chip gets its power from a small cylindrical battery, called the *CMOS battery*, installed on the motherboard.

Memory slots. The primary memory of the computer is the *random access memory (RAM),* which is used to temporarily store data during normal operation of the computer. The slots for memory on the motherboard are different for each type of memory and for each type of motherboard design. Most motherboards have slots for *dual inline memory modules (DIMMs)*. DIMMs come in different pin configurations, such as 168-pin, 184-pin, and 240-pin. Some old motherboards use *single inline memory modules (SIMMs)* that come in 30-pin or 72-pin configurations. It is easy to identify the memory slots on the motherboard, as they are long and located very close to each other. A latch on each side of the slot is used to firmly attach the memory module in place. The pair of memory sockets is also called *memory bank.*

External cache memory. Computers use the processor cache memory for improved performance. Each processor comes with a built-in cache memory, which is known as *Level 1 Cache*. Another name for it is *internal cache*, which runs at the speed of the CPU. To further enhance the performance of the system, motherboards have external cache memory, which is called *Level 2 Cache* or *External Cache*. The External Cache runs at the speed of the system bus.

Processor sockets. The *central processing unit (CPU)*, or simply the *processor*, lies at the heart of a computer motherboard. The type, shape, size, and pin configuration of a processor socket depends on the processor itself. Processor *sockets* or *slots* are identified by standards written for installing different types of processors on motherboards. Processor sockets are normally flat in shape and have several rows and columns of pins. It is not difficult to identify a processor socket on the motherboard. Most Pentium class processors are installed along with a heat sink and a cooling fan because they generate a lot of heat during normal operation. A processor slot is another way to connect a processor to the motherboard. Slots were used on earlier Pentium II and Pentium III processors. The processor is mounted on a special expansion card and is inserted vertically in the slot.

Most of the processor sockets are square in shape, and the processor is usually marked with a dot to correctly align it with the socket. This is done to ensure that the processor pins are not damaged during insertion. Some processors use a special socket called the *zero insertion force (ZIF)* socket that makes it easy to insert and remove the processor.

Integrated I/O ports. Many of the standard I/O controllers for peripherals are integrated in the motherboard. Their connectors are accessible from the rear of the computer case and are used to connect I/O devices. The most common connectors include the following:

The 15-pin SVGA connector
Used to connect a CRT or LCD monitor.

The 6-pin PS/2 connector (mini DIN)
Used to connect the keyboard and mouse. Old motherboards have a 5-pin DIN connector, which is little bigger than the PS/2 connector.

The 9-pin serial connector
Used to connect serial devices such as modems or scanners.

The 25-pin parallel connector
Primarily used to connect printers.

The 8-pin RJ-45 connector
Used to connect network cable.

The 4-pin RJ-11 connector
Used to connect the telephone cable.

USB connector
Used for USB devices.

IEEE 1394 connector
Used to connect devices that support the Firewire interface.

Expansion bus slots. Expansion bus slots on the motherboard can be easily identified, as they are located close to each other and near the rear end of the case. Figure 2-2 shows some common expansion bus slots on the motherboard.

Each type of expansion bus slot serves a particular function, as summarized in the following paragraphs:

Peripheral Component Interconnect (PCI)
PCI slots are available in most computers these days. These slots are used to connect PCI compatible cards. They are usually white and are about three inches long.

Accelerated Graphics Port (AGP)
AGP slots are used to connect video cards. The AGP port allows the video adapter to communicate directly with the processor. The AGP slot is usually brown.

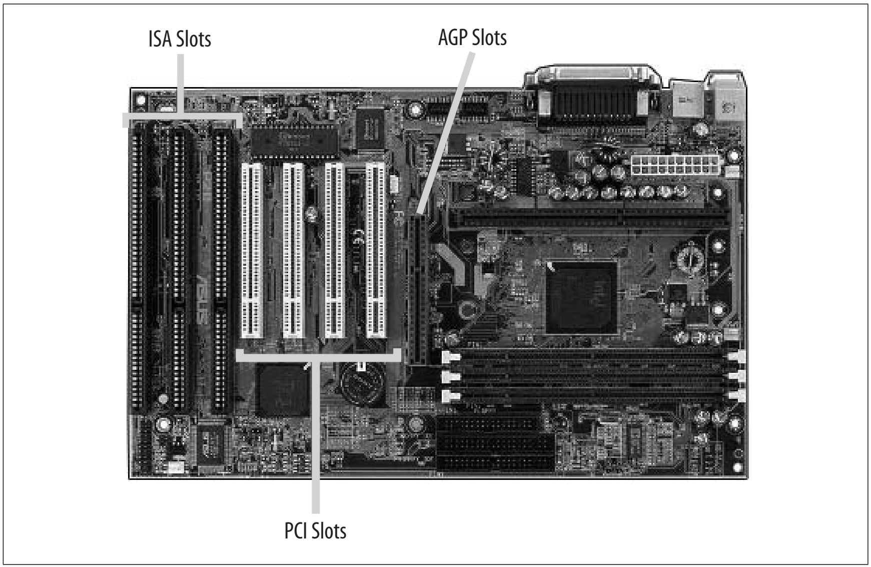


Figure 2-2. Expansion bus slots

PCI Express (PCIe)
: PCIe is available on many new motherboards. This slot was designed to replace the PCI and AGP slots. But most motherboards have PCI as well as PCIe slots.

Audio/Modem Riser (AMR)
: AMR has 46 pins and is found on some old motherboards. This slot is mainly used to separate analog devices, such as the modem, from other digital circuits on the motherboard.

Communications and Networking Riser (CNR)
: CNR has 60 pins and is mainly used to enhance the built-in capabilities of the motherboard by installing additional components.

Industry Standard Architecture (ISA)
: ISA is the oldest type of expansion slot on motherboards. This black-colored slot is long in shape and has two parts: one small and the other long. ISA slots are hardly visible in modern motherboards. You might find that some old motherboards have both ISA and PCI slots.

Floppy disk and hard disk connectors. Most of the motherboards have integrated hard disk and floppy disk controllers. The floppy disk connector is used to connect a floppy disk drive, while the hard disk connector can be used for connecting hard drives or CD/DVD drives. Depending on the motherboard, these connectors can be any of the following types:

EIDE/PATA
: The Enhanced Integrated Drive Electronics (EIDE) interface is the term used to describe the Advanced Technology Attachment (ATA) interface. EIDE connectors are found on most motherboards. These connectors have 40 pins

and use a flat ribbon cable. The first pin on the cable is marked with a red lining. Since the data is transferred in parallel fashion from motherboard to the drive, the interface is also called Parallel ATA (PATA). EIDE drives use a 4-pin power connector.

SATA

The Serial Advanced Technology Attachment (SATA) transfers data between the motherboard and the drive in serial fashion. The connectors for SATA interfaces have seven pins. SATA drives use a 15-pin power connector.

SCSI

The Small Computer System Interface (SCSI) is rarely built on the motherboard for desktop computers. This interface is integrated more commonly on server motherboards. If you have a SCSI device, you can obtain a SCSI card to connect the device.

Power supply connectors. There is only one main power supply connector on the motherboard. There is also a small 4-pin connector for the CPU/fan assembly. It is rectangular in shape and white in color. ATX motherboards use a 20-pin power supply connector in which the holes are polarized to prevent incorrect connection.

Power supplies

The purpose of the power supply is to convert 110-volt or 220-volt AC voltage into DC voltage for different parts of the computer. The power supply unit for the computer has its own case. These DC voltages include 3.3 volts, +5 volts, –5 volts, +12 volts, and –12 volts. The rating of the power supply unit is given in watts, which is a measure of power. The higher the rating, the more power it can supply to different parts of the computer.

Most common power supplies come in the range of a 250- to 500-watt rating. The +3.3 volts and +5 volts DC supply was first used in ATX motherboards that supported *soft power off* functions.

Power supply connectors. There are several different types of power supply connectors used on computer motherboards and peripherals. Some of the common connector types are listed in the following paragraphs:

Floppy drive power connector

This is a small, flat connector with four pins. This connector has 4 wires and supplies 5 volts (red wire) and 12 volts (yellow wire) DC to the floppy drive. The connector is polarized and cannot be connected in wrong orientation.

Molex connectors for peripherals

Peripherals such as the hard drive and CD/DVD drives use a 4-pin Molex connector. This connector is bigger than the floppy drive power connector. It has a particular rectangular shape that allows the connection only in correct polarity. It uses the same color codes for wires as the floppy drive power connector does.

AT motherboard power connector

This is a pair of two connectors with six pins each. The connectors have small tabs on them so that they can be securely attached to the motherboard connector. You need to place the connectors side by side with black-colored wires in the center, align the connectors in correct orientation, and then slightly push them together onto the motherboard connector.

ATX power connector

This is used for supplying power to ATX motherboards. It is also known as ATX System Connector. This is a single 20-pin connector that supplies six different types of voltages to the ATX motherboard. The connector is rectangular in shape and has a small plastic lock that secures the connector in place. Another variation of the ATX power connector is the ATX12V standard connector, which requires two additional power connectors for the motherboard. One of these is a 6-pin connector that supplies additional +5 volts and +3.3 volts. The other is a 4-pin connector that supplies two +12 volt supplies.

SATA power connector

Serial ATA (SATA) devices use a 15-pin power supply connector. This connector supplies three sets of DC power, for +3.3 volts, +5 volts, and +12 volts.

Remember the number of pins, wire colors, and voltages for power supply connectors of standard peripherals such as the floppy drive and the hard disk drive? These connectors have four pins and the red wire carries +5 volts while the yellow wire carries +12 volts of DC supply. The black wires are used for ground connection. The color codes for floppy drives and hard drives or CD/DVD drive connectors are identical.

Processors

The processor, or the central processing unit (CPU), is the heart of the computer. It controls and directs all functions inside the computer. The term *microprocessor* refers to the semiconductor chip on the motherboard that contains millions of transistors. The CPU is the most important component of the computer so far as the computing power is concerned. The size and packing of old CPUs used to be very large compared to the size and shape we see these days. Old CPUs also had limited capabilities and features. The two main manufacturers of microprocessor chips are Intel and AMD.

Old processors came in a rectangular shape and with *Dual inline package (DIP)*, with two rows of connection pins on each side. New processors come in *Pin Grid Array (PGA)* packaging, which is a square shape and has connection pins on all four sides. Some processors use a *Single Edge Contact Cartridge (SECC)* Form Factor. This uses a separate printed circuit board for the same PGA-type processor. Processors are mounted on the motherboard using a special socket or a slot. As the processor technology grows in features and advanced capabilities, the space on the motherboard becomes the main limitation. The *Staggered Pin Grid Array (SPGA)* packaging solves this problem. SPGA uses arrays of pins, which form a diagonal square.

Characteristics of processors. The following paragraphs summarize some basic characteristics of processors:

Hyper-threading Technology (HTT)

HTT is the specialized form of *simultaneous multi-threading (SMT)* used in Intel's Pentium 4 microprocessors. This technology improves the performance of microprocessors by providing useful work to idle execution units and allowing multiple threads to run simultaneously. Processors using the hyper-threading technology appear to the operating system as two processors. If the operating system supports *symmetrical multiprocessing (SMP)*, it can take advantage of this technology by scheduling separate processes on the same HTT-capable microprocessor.

Multicore

A multicore processor integrates two or more processors into a single package. The operating system treats the single multicore processor as two separate processors. The operating system must support symmetrical multiprocessing to take full advantage of a multicore processor. Intel's Dual Core processor is an implementation of the multicore technology that contains two independent processors in a single chip.

Throttling

CPU throttling is the process of controlling the time spent by the processor on each application. The idea behind throttling is to fairly divide the CPU time among various applications. CPU throttling is mainly used on servers that need to distribute even time to all applications running on it.

Microcode and MMX

Microcode (or *microprogram*) is the instruction set of a CPU. The CPU uses the microcode to execute various instructions. Microcode consists of a series of microinstructions that control the CPU at its most fundamental level. Microcode is designed for the fastest possible execution of instructions, and it resides in a special high-speed memory of the computer called the *control store*.

MMX refers to *MultiMedia Extensions*, a special microcode developed for Intel's Pentium MMX processors. MMX microcode takes the load off executing multimedia-related instructions from the processor and acts like a co-processor.

Overclocking

Overclocking is used in microprocessors and other computer components to increase their performance. CPU overclocking forces the processor to run at higher clock rates than that for which it was designed. When the CPU is overclocked, arrangements must be made to dissipate the additional heat that it will generate due to increased processing.

Cache

Cache is a high-speed memory that is used to store data and instructions that are most likely to be required by the CPU. The cache located within the CPU is called *Level 1 Cache (L1 Cache)*, and the external cache on the motherboard is called *Level 2 Cache (L2 Cache)*. If the cache does not have the necessary data or instructions, a process named *cache miss* brings the information from RAM and stores it in the cache.

Voltage Regulator Module (VRM)

A VRM is an electronic device that provides the microprocessor with appropriate supply voltage. A VRM allows microprocessors requiring different power supply voltages to be used on the same motherboard. At startup, the microprocessor signals the VRM about the correct voltage supply that it needs. The VRM then supplies a consistent correct voltage to the processor.

Speed

The speed of a microprocessor is represented by its *clock frequency*, which is measured in *Megahertz (MHz)* or *Gigahertz (GHz)*. Clock rates or frequencies can be misleading when the speeds of the microprocessors are compared. This is due to the fact that the amount of work a microprocessor can do in one clock cycle varies from one CPU chip to another.

32-Bit versus 64-Bit Bus

The number of data bits that can be transmitted or processed in parallel is represented by the bus width, which can be 32-bit or 64-bit. The 32-bit bus transmits 32 bits in parallel while the 64-bit bus transmits 64 bits of data in parallel. The width of the data lines that connect the microprocessor to the primary memory of the computer is known as the bus width. The wider the bus, the more data can be processed in a given amount of time. It is important to note that if you are using a 64-bit operating system, you must ensure that the CPU supports 64-bit bus width.

Memory

Random access memory (RAM) is considered the *primary* or *main memory* of the computer, and it allows quick data storage and access. This memory is used as temporary storage by the system and by applications during normal operation of the computer. *Memory modules*, or *memory sticks*, are small, thin circuit boards that are installed on the motherboard as several rows close to each. In this section, we will look at some basic characteristics and types of memory, as well as memory packaging.

Error checking in memory. There are two main mechanisms used for error checking in computer memory. These are explained in the following paragraphs:

Parity RAM

Parity RAM uses a *parity checking* mechanism to check the integrity of digital data stored in memory by detecting errors. Memory modules using parity checking are known as *parity RAM*. These modules are hardly used these days. A *parity bit* is used as error-detecting code. The parity bit is a binary digit (0 or 1) that indicates whether the total number of bits with a value of 1 in a given set is even or odd. Two types of parity bits are used: *even parity bit* and *odd parity bit*. The even parity bit is set to 0 when the total count of 1s in the given set is even. If the total count of 1s is odd, the bit is set to 1. On the other hand, the odd parity bit is set to 0 when the total count of 1s in the given set is odd. If the total count of 1s is odd, the bit is set to 0. Parity checking is only a method of checking errors. It does not indicate the cause of the error and does not correct it.

www.allitebooks.com

Non-parity RAM
If parity RAM is used, the memory modules need to have more chips for calculation of parity. This not only increases the size of the module but also increases costs. For this reason, non-parity RAM is used on most computers.

Error Checking and Correction RAM (ECC RAM)
ECC RAM automatically detects and corrects errors in memory, without the involvement of the motherboard circuitry. The ECC mechanism generates checksums before storing data in memory. When the data is retrieved from the memory, the checksum is calculated again to determine whether any of the data bits have been corrupted. ECC memory can generally detect 1-bit and 2-bit errors, but can only correct errors that are 1 bit per word.

Types of memory. Computer memory or RAM is used to temporarily store data. RAM can be dynamic or static. For most common functions, the *dynamic random access memory (DRAM)* is used as the main memory of the computer, while the *static random access memory (SRAM)* is mostly used for the system cache. The following paragraphs summarize different types of memory:

DRAM
DRAM stands for *dynamic random access memory*. The term *dynamic* refers to the requirement of the memory chip to be periodically refreshed in order to retain its contents—if this fails, the stored contents can be lost. DRAM is much cheaper than other types of memory and is most commonly used to expand the computer memory. Popular variations of DRAM include SDRAM, DDR, DDR2, and RAMBUS.

SDRAM
SDRAM stands for *synchronous dynamic random access memory*. SDRAM has a synchronous interface, which means that it waits for a clock signal before it responds to an input. It is synchronized with the computer's processor. The system bus. SDRAM interfaces with the processor in a parallel 8-byte (64-bit) bus and thus, a 100 MHz clock signal produces 800 MBps throughput. The 100 MHz SDRAM modules are commonly identified as PC100 chips.

DDR SDRAM
DDR SDRAM refers to *double data rate synchronous dynamic random access memory*. These memory modules can double the data transfer rate by using both rising and falling edges of the clock without actually increasing the frequency of the system bus. This means that a 100 MHz DDR has an effective clock rate of 200 MHz For a 100 MHz clock signal, the effective data rate becomes 1600 MBps (2 × 8 × 100). DDR SDRAM modules are also referred to as PC1600 chips.

DDR2 SDRAM
DDR2 SDRAM refers to *double data rate 2 synchronous dynamic random access memory*. This type of memory first doubles the clock rate by using both edges of the clock signal and then further splitting a single clock into two, thus doubling the number of operations for each clock cycle. DDR2 SDRAM uses 1.8 volts (as compared to the 2.5 volts used by DDR SDRAM) to keep the power consumption low. DDR2 modules are referred to as DDR2-400 or PC2-3200 chips.

DRDRAM

DRDRAM stands for *Direct Rambus dynamic random access memory*, a technology developed by Rambus Corporation. These types of memory modules are no longer really in use. DRDRAM supports the PC800 standard and operates at 400 MHz The effective data transfer rate is 1600 MBps on a 2 byte (16-bit) data bus.

SRAM

SRAM stands for *static random access memory*. The term *static* means that the contents of the memory are retained as long as the power is turned on. SRAM is much faster and much more expensive than DRAM. It is mainly used for cache memory.

Mbps stands for *megabits per second* and MBps stands for *megabytes per second*. Note the small and capital B in these notations. One byte contains 8 bits.

Memory modules. Memory modules, or memory sticks, are available in a variety of packaging. The most common of them in use as of date are as follows:

SIMM

SIMM stands for *single inline memory module*. There are two main types of SIMMs: 30-pin, which has an 8-bit data bus, and 72-pin, which has a 32-bit data bus. SIMMs do not have a standard pin configuration. SIMM has largely been replaced by DIMM.

DIMM

DIMM stands for *dual inline memory module*. DIMM is a 64-bit module used for SDRAM, DDR, and DDR2 memory. A standard SDRAM has 84-pins on each side, making it a 168-pin module. DDR DIMM has 184 pins with 1 keying notch, and the DDR2 DIMM has 240 pins with 1 keying notch. The DDR2 DIMM also has an aluminum cover on both sides that is used as a heat sink to prevent overheating.

RIMM

RIMM refers to *Rambus inline memory module*. It is a custom memory module made by Rambus. RIMM modules come in 16-bit single channel width or in 32-bit dual channel bus width. The 16-bit modules have 184 pins, and the 32-bit modules have 232 pins. Sixteen-bit modules need pairs of slots on the motherboard, while the 32-bit modules require only one. RIMM also has an aluminum cover for dissipation of heat.

SO-DIMM

SO-DIMM stands for *small outline dual inline memory module*. It is mainly used in laptop computers. The old 32-bit SO-DIMM had 72 pins, while the new 64-bit modules come in 144-pin and 200-pin configurations.

Micro DIMM

Micro DIMM is the smallest of all DIMM packages (about 50 percent the size of SO-DIMM) and is mainly used in laptop computers. These modules have a 64-bit bus width and come in 144-pin or 172-pin configurations.

Storage devices

As noted earlier in this section, the RAM is called the primary memory of the computer. The hard disk drive remains the main storage device for most personal computers and is called the *secondary storage device*. Besides hard disk drives, other secondary storage devices are also frequently used for storing data, but most of these are categorized as removable storage devices. These include floppy disks, zip drives, tape drives, USB drives, and CD and DVD drives. This section summarizes the types and characteristics of different styles of storage devices.

Floppy disk drives. A *floppy disk*, or diskette, consists of a circular piece of thin plastic magnetic sheet encased in a plastic case. These disks are read and written in floppy disk drives (FDD). Earlier floppy disks were 8 inches in size, later reduced to 5.25 inches, and finally reduced to 3.5 inches. The storage capacity of a normal double-sided floppy disk is usually 1.44 MB. Many new computers do not have a floppy disk drive at all due to high storage capacity and falling prices of CD and DVD disks and drives.

The 5.25-inch floppy disk was known as *minifloppy disk* and had a capacity of 360 KB for a double-sided double-density disk, and a capacity of 1.2 MB for a double-sided high-density disk. The capacity of 3.5-inch disks, called the *microfloppy disk*, is 720 KB for a double-sided disk, 1.44 MB for a high-density disk, and 2.88 MB for an extended density disk.

Hard disk drives. Hard disk drives are the main storage devices for all personal computers and servers. Data is stored on hard disks in the form of files, which is a collection of bytes. A hard disk is usually 3.5 inches wide, and its capacity is measured in *gigabytes (GB)*. It is not uncommon to see hard disks with capacities ranging from 20 GB to even 250 GB. The hard disk drive subsystem of the computer consists of the following three components:

Controller board
: Operates the drive. It is typically located on the hard disk itself and controls different motors, electrical signals, and sensors located inside the disk.

Disk
: Consists of a number of thin disks or platters and read/write heads. The disks are the main medium used to store data. They are placed close to each other inside an enclosure. The disks spin at a speed of 3600 to 7200 (or even 10,000) revolutions per minute (rpm). An arm mechanism holds the read/write heads and moves them very precisely at a fast speed. The data is stored on disks in sectors and tracks.

Hard disk adapter
: Typically built in the motherboard. It converts signals from the disk and the controller so that the motherboard can understand it. In old computers, the hard disk adapter was installed on one of the expansion slots.

CD-ROM drives. A *compact disc read-only memory (CD-ROM)* is used for long-term storage of data and for distribution of software. The term *read-only* means that data can be written only once on the CD. Nearly all computers have a CD-ROM drive. The capacity of a typical CD-ROM is about 700 MB. CD-ROM drives are rated in terms of their speed, which is a multiple of 150 Kbps. It is expressed as 2X, 4X, 8X, etc., which means that a 2X CD-ROM drive can transfer data at the rate of 300 Kbps. Most new CD-ROM drives are rated between 48X to 52X.

CD burners. CD burners refer to drives that can write data on *CD-Recordable (CD-R)* and *CD-ReWritable (CD-RW)* discs. The main difference between the two is that the CD-R can be used to store data only once while the data on a CD-RW can be erased and the space can be reused any number of times. Some advanced software applications allow you to reuse the CD-R disc until it is full. The speed of CD-R and CD-RW differs when reading the disk, writing data, and rewriting. A rating of 32X-16X-4X means that the drive can read data at 32X speed, write data at 16X speed, and rewrite at 4X speed.

DVD-ROM drives. A *digital versatile disc (DVD)* has a larger capacity than a CD-ROM. DVDs can store up to 4.7 GB of data on a single-sided, single-layered disk. Since the DVD-ROM drive is basically the same as the DVD player, you can use it to play DVD movies on your computer. A double-sided, double-layered DVD can store up to 17 GB of data. The DVD drive has the same appearance as the CD drive. The only way to identify it is from the DVD logo on the front panel.

DVD burners. A *DVD burner*, or a *DVD writer*, refers to a DVD drive that can write data on a DVD disc. A single-sided, double-layered DVD disc can store up to 8.5 GB of data. DVD burners and writable DVDs have several formats that include DVD-ROM, DVD-R, DVD+R, DVD+RW, and DVD-RAM, depending on the burning technology used. A drive meant for a particular technology may not support burning on other types of DVD discs.

Tape drives. Tape drives are the traditional type of removable storage media used for taking data backups. Tape drives can be internal or external devices and can be digital or analog. The capacity of tape drives is much more than the hard disks.

Flash memory. Flash memory, which was at one time used as the main memory for computers, is still used for booting devices such as network routers and switches. For example, Cisco stores its *Internetwork Operating System (IOS)* in flash memory. It is accessed at the startup time to boot the device. Other forms of flash memory include *Secure Digital (SD) cards, USB thumb drives*, and *PC cards*. SD cards are used in mobile phones, digital cameras, and camcorders for additional storage space. It has a write-protect tab that prevents accidental erasure of data. USB thumb drives are very popular for their convenience with transporting data from one computer to another. These drives are considered a good replacement for other types of removable media such as floppy disks, Zip, and Jazz drives. All thumb drives are Plug and Play (PnP)-compatible.

External disk drives. External disk drives offer additional storage space and are connected to serial, parallel, or USB ports on the computer. Most of the new external disk drives are USB-compatible, which further offer the PnP features. PnP allows the device to be detected and configured automatically. One interesting thing to note is that the external disk drives use the same disk that is used in the computer with additional circuitry to convert the interface to USB.

Display devices

Computer display devices or monitors fall into two main categories: *cathode ray tube (CRT)* and *liquid crystal display (LCD)*. Each type of the device is supported by a *video display unit (VDU)* adapter or integrated video controller on the motherboard. There are several different types of video technologies, each offering different levels of screen resolution and color depth. *Resolution* refers to the number of horizontal and vertical pixels that a monitor is able to display. For example, a resolution of 800×600 would use 800 horizontal and 600 vertical pixels to draw text or images on the screen. *Color depth* refers to the number of colors the monitor is able to display.

Video technologies. A summary of different video technologies is given in the following paragraphs:

Monochrome

Earlier video technology used *monochrome* or black and white video displays. The monochrome video had a maximum screen resolution of 720×350 pixels. Initially, the monochrome technology was unable to display graphics. The *Hercules Graphics Card (HGC)* was used to display graphics. HGC used two separate modes: text mode for text, and graphics mode for images. Monochrome monitors used a DB-9 D-sub connector that had nine pins arranged in two rows.

Color Graphics Adapter (CGA)

IBM was the first to introduce the CGA video technology. It could use a screen resolution of 640×200 pixels with two colors, one of which was black. With four colors, the resolution dropped to 320×200 pixels.

Enhanced Graphics Adapter (EGA)

To overcome the limitations of the CGA technology, IBM introduced the EGA video technology. EGA was able to display 16 colors and a screen resolution of 640×350 or 320×200.

Video Graphics Array (VGA)

The VGA uses 256 KB of on-board video memory and is able to display 16 colors with 640×480 resolution or 256 colors with 320×200 resolution. The main difference between the earlier technologies and the VGA technology is that VGA used analog signals instead of digital signals for the video output. VGA uses an HDB-15 D-sub connector with 15 pins arranged in 3 rows.

Super Video Graphics Array (SVGA)

The *Video Electronics Standards Association (VESA)* developed the SVGA video technology. SVGA initially supported a screen resolution of 800×600 pixels with 16 colors. Later, the new developments made the SVGA display 1024×768 resolution with 256 colors. SVGA also uses an HDB-15 D-sub connector with 15 pins arranged in 3 rows.

Extended Graphics Adapter (XGA)

XGA is another development by IBM that uses the *Micro Channel Architecture (MCA)* expansion board on the motherboard instead of a standard ISA or EISA adapter. XGA video technology supports a resolution of 1024×768 for 256 colors and 800×600 resolution with 65,536 colors.

Digital Video Interface (DVI)

DVI is a digital video technology that is different from the analog VGA technologies. DVI connectors look like the standard D-sub connectors but actually are different in pin configurations. The three main categories of DVI connectors are *DVI-A* for analog-only signals, *DVI-D* for digital-only signals, and *DVI-I* for a combination of analog and digital signals. The DVI-D and DVI-I connectors come in two types: *single link* and *dual link*.

High Definition Multimedia Interface (HDMI)

HDMI is an all-digital audio/video interface technology that offers very high-resolution graphics and digital audio on the same connector. HDMI provides an interface between any compatible audio/video source—such as a DVD player, a video game system, or an AV receiver—and a digital audio video monitor—such as digital television (DTV). It transfers uncompressed digital audio and video for the highest and crispest image quality.

S-Video

S-video or *Separate-video* is an analog video signal that carries video signals as two separate signals. It is also known as Y/C video, where Y stands for a *luminance* (grayscale) signal and C stands for *chrominance* (color). The basic connector for S-Video is a 4-pin mini-DIN connector that has 1 pin each for Y and C signals, and 2 ground pins. A 7-pin mini-DIN connector is also used in some cases. S-Video is not considered good for high-resolution video due to lack of bandwidth.

Composite Video

Composite Video is a technology in which all components are transmitted on a single cable. This is in contrast with *Component Video*, which is an analog video technology that splits the video signals into red, green, and blue components. Component video uses three separate RCA cables for each color.

Types of monitors. Monitors are mainly classified into two categories: CRT and LCD, which are summarized in the following paragraphs.

CRT monitor

A cathode ray tube (CRT) monitor is the most commonly used display device for desktop computers. It contains an electron gun that fires electrons onto the back of the screen, which is coated with a special chemical called *phosphors*. The screen glows at parts where the electrons strike. The beam of electrons scans the back of the screen from left to right and from top to bottom to create the image. A CRT monitor's image quality is measured by its dot pitch and refresh rate. The *dot pitch* specifies the shortest distance between two dots of the same color on the screen. Lower dot pitch means better image quality. Average monitors have a dot pitch of 0.28 mm. The *refresh rate*, or *vertical scan frequency*, specifies how many times in one second the scanning beam can create an image on the screen. The refresh rate for most monitors varies from 60 to 85 Hz.

LCD monitor

LCD monitors are used in desktop computers as well as laptops. LCD displays are covered later in the section "Laptops and Portable Devices."

Input devices

An input device for a computer is used to transfer information from a user or another device to the computer for processing. While a keyboard and a mouse are the basic types of input devices used for user input, some other types of devices (such as a touch screen, multimedia devices, and biometric devices) are also considered input. The computer basically receives input, processes it, and produces results. The following sections cover a brief discussion of some of the commonly used input devices.

Mouse. A mouse is a pointing device used to interact with the computer. It controls the movement of the cursor on the screen and you can point to an object and click a button on the mouse to select it. The following are the basic types of mouse:

Mechanical mouse
: This uses a rubber ball on its bottom side, which can roll in all directions. Mechanical sensors within the mouse detect the direction of the ball and move the screen pointer accordingly.

Opto-mechanical mouse
: This is similar to the mechanical mouse but uses optical sensors to detect the motion of the ball.

Optical mouse
: This does not have a ball or any other moving parts. It uses light signals to detect the movement of the mouse. This mouse must be used with a special mouse pad that reflects the optical signals. Newer optical mice use laser signals that do not even need an optical pad.

Wireless mouse
: Also called a cordless mouse, this has no physical connection with the computer and uses infrared radio signals to communicate with it.

A mouse can be connected to the computer by a serial port, a USB port, or a PS/2 port, or it can be a wireless mouse using radio signals. You can configure the properties of the mouse in the operating system to change the way a mouse responds to various user actions. For example, the functions of left and right buttons can be interchanged, the speed of a button click can be changed, or the shape of the pointer can be selected from a variety of shapes.

Keyboard. A keyboard is the most popular and useful of all input devices. A layout of keys on a normal keyboard resembles the keyboard of an old styled QWERTY typewriter. A standard AT keyboard has 84 keys, while newer keyboards normally have 101. In addition to standard alphabetic, numeric, and punctuation keys, computer keyboards have special arrow keys and function keys labeled F1, F2, and so on. A separate number pad allows a user to enter numbers with faster speed. As with the mouse, a keyboard can also be connected to a computer using the serial port, a PS/2 port, or a USB port. In addition, it can be a wireless keyboard using infrared radio signals to communicate with the computer.

Barcode reader. A barcode reader (or a barcode scanner) is a device that scans the code printed on a surface. Barcode scanners are widely used in retail stores or warehouses as input devices. It consists of an LED or laser-based light source, a set of lenses, and a photoconductor to translate the optical signals into electrical signals. Barcode scanners are connected to the computer using a serial port or a USB port.

Multimedia devices. Multimedia input devices are mainly classified into two categories: audio and video. A variety of audio and video devices can be connected to the computer to send, receive, or process information. The most common examples of multimedia input devices include web cameras, digital cameras, microphones, and MIDI devices. The connection details of the device depend on the type of device and may vary from one device to another.

Biometric devices. Biometric devices are security devices that are used to control access to a system. A biometric device measures the physical characteristics (fingerprints, eye retina scan, or voice patterns) of a person for the purpose of identification. The information collected by the biometric device is sent to the computer for processing. The computer matches the input from a biometric device and compares it with its database to grant or deny access to the person.

Touch screen. Touch screens are considered a replacement for a standard keyboard and a mouse. A user can simply touch the screen, which translates the user's actions into electrical signals. The computer receives these signals and processes the user's request. Touch screens are not only used for computers but also for a variety of other applications, such as retail stores, PDA devices, bank machines, vehicles, and several appliances.

Adapter cards

Adapter cards, or expansion cards, are used to extend the functionality of a computer. These cards are separate printed circuit boards that are installed on one of the available expansion slots of the computer. Depending on the system bus available in your computer, you must be careful when selecting an adapter card. For example, if you buy a PCI card, the motherboard must have PCI expansion slots. In this section, we will take a look at different types of adapter cards.

Video card. A video card, or a video adapter, allows you to produce the video output of the computer on a display device such as the CRT or LCD monitor. Most of the new video cards use either the *Peripheral Component Interconnect (PCI)* bus or the *Accelerated Graphics Port (AGP)* bus. Some new adapters are PCIe-compatible.

Network card. The network card, or network interface card (NIC) allows the computer to communicate with other computers on the network. It translates the parallel data stream on the system bus into serial data stream that can be transmitted on the network and vice-versa. Network cards can be PCI-, PCIe-, or ISA-compatible. Each network card has at least one RJ-45 socket where the network cable is connected. When you install a network adapter, you must install its device driver and configure network properties of the OS such as the network protocol. Most new motherboards have built-in network functionality.

Sound card. A sound card is used to convert the digital signals into sound and get sound input through a microphone for recording. These cards have audio/video jacks for connection to speakers, headphones, and microphones. Most sound cards support the *Musical Instrument Digital Interface (MIDI)* functions and have a 5-pin mini-Din connector.

Modem card. A modem card is used when you have a dial-up Internet connection. The term *modem* stands for *modulator demodulator*. It converts the digital signals from the computer into analog signals that can travel on ordinary telephone lines and vice versa. Modems have a standard RJ-11 socket where the telephone line is connected. The modem card can be installed on a PCI, ISA, or PCIe expansion slot depending on the type of motherboard and the card. Most new motherboards include an integrated modem.

I/O cards. Any adapter card that extends the input/output capabilities of a computer can be termed an I/O card. For example, an SCSI card can be an I/O card that can be used to connect SCSI devices. Similarly, a parallel adapter can be used to connect a parallel printer, which is an output device. I/O adapters can use any of the ports available in a computer or can add an additional port for connecting I/O devices. USB 2.0 and Firewire (IEEE 1394) adapters are very common these days, due to a variety of devices supporting these standards.

Types of port connectors

Standard ports on computers serve as interfaces where you can connect external devices. Each type of port uses a different set of cables, and the device is attached using a different connector. In this section, we will look at some common types of connection ports and connectors. Figure 2-3 shows common ports found on a typical personal computer.

Universal Serial Bus (USB). To date, the USB is the most common of all computer interfaces. It is used to connect a wide variety of external devices to the computer. USB 2.0 is the latest version of the USB standard. USB devices are Plug and Play (PnP)–compatible, and you can connect up to 127 devices in star topology on the same USB port using USB hubs. Most computers have two or more USB ports. USB hubs can be used to extend the number of USB ports. There are two types of USB connectors: Type A and Type B. A standard USB cable has a Type A connector on one end and a Type B connector on the other end. The cable end with the Type A connector is always connected to the computer. The Type B side is connected to the USB device. Each USB connector has a polarity and cannot be attached incorrectly.

Firewire. The Firewire (IEEE 1394) ports are used primarily for their speed advantages. Firewire operates at a maximum data transfer speed of 400 Mbps. *Firewire 800 (IEEE 1394b)* supports a maximum throughput of 800 Mbps and a cable

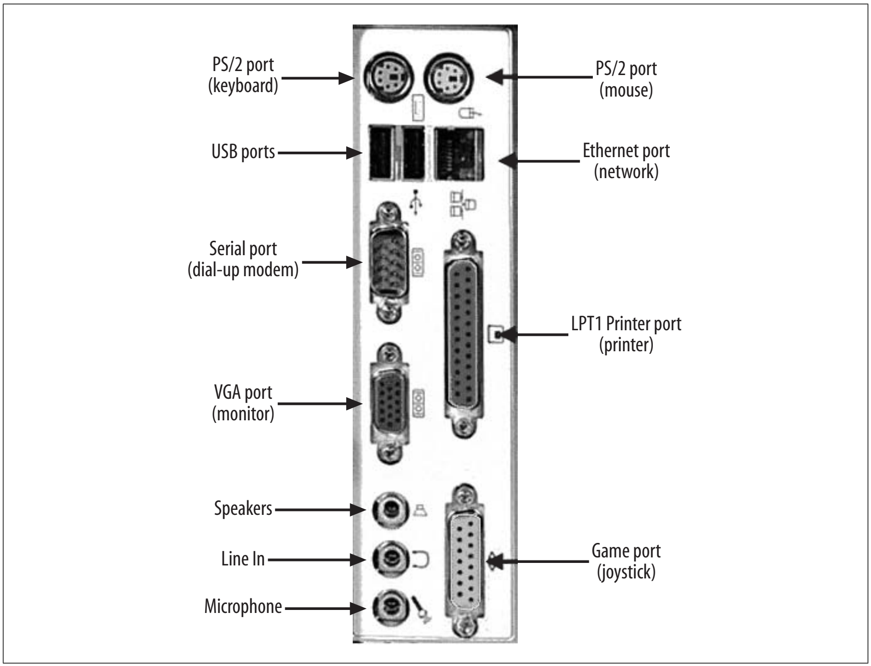


Figure 2-3. Common ports on a personal computer

distance of 100 meters. Firewire devices are hot-swappable, (can be connected and/or disconnected while the system is powered on) and you can connect up to 63 devices. The maximum cable distance between devices can be up to 4.5 meters. The Firewire port on the computer has a 6-pin connector, and the devices have a 4-pin connector.

Parallel. Most parallel ports use a 25-pin D-sub connector. The other end of the parallel cable has either another 25-pin D-sub connector or a 36-pin centronics connector. Most new printers use the USB port these days.

Serial. A standard serial port has a 9-pin socket and the connector is 9-pin D-sub. Some other forms of serial interfaces include USB and Firewire. Serial cables are of two types: *standard* and *null modem*. Table 2-1 lists some common configurations of serial cables.

Table 2-1. Serial cable configurations

Cable type	First connector	Second connector
Standard modem cable	DE-9 Female	DB-25 Female
Null modem cable	DB-25 Female	DB-25 Female
Null modem cable	DE-9 Female	DE-9 Female
Serial extension cable	DE-9 Female	DE-9 Male
Standard serial cable or extension cable	DB-25 Female	DB-25 Male

www.allitebooks.com

RJ-Series. *Registered Jack (RJ)* connectors are used for connecting the computer to a telephone line or to the network. The telephone cables use an RJ-11 connector and sockets. It has two pins for a single line and four pins for two lines. The network port has an RJ-45 socket with eight pins and connects to an Ethernet cable with a matching RJ-45 connector. A small plastic latch on the connector locks the connector in the socket.

PS/2 (mini-DIN). PS/2, or mini-DIN, ports are mainly used to connect the keyboard and the mouse to the computer. The connector is round in shape and has six pins. Old computer keyboards used a 5-pin DIN connector that is little bigger than the mini-DIN connector. The PS/2 port for the keyboard is purple in color and the mouse connector is green. These ports are usually marked on the computer to prevent incorrect connection. There is a small plastic pin in the center of the connector that also helps in attaching the connector in correct polarity.

Centronics. A centronics connector is used to connect the parallel printers and SCSI devices. This connector is not located on the computer. The connector has two clips on each side to firmly lock it in place. On the computer side, a 25-pin D-sub port is used for connecting a parallel device.

A/V jacks. Most audio/video (A/V) jacks on computers are of RCA type. These jacks are used for connecting speakers, headphones, or microphones.

Cooling systems

Computer components produce heat during operation. Some components, such as the CPU, produce so much heat that if some arrangement is not made to dissipate the heat, it can destroy itself. Nearly all computers have cooling systems to keep the internal components cool. These cooling systems also help in maintaining a proper flow of air inside the computer case. Additionally, heat sinks are used with some components to dissipate the heat from their surface. In this section, we will look at different cooling systems inside the computer.

Fans. Fans inside the computer are used to maintain the proper flow of air. The following types of fans are found on most computers:

Power supply fan
: Used to cool the power supply. It is located inside the power supply unit.

Rear exhaust fan
: Used to blow out the hot air inside the computer case.

Front intake fan
: Used to bring fresh cool air from outside the computer case.

CPU fan
: Used to cool the microprocessor. It is located on top of the CPU heat sink.

Chipset fan
: Helps cool the chipset on the motherboard.

Video card cooling fan

Used on some high-performance video cards to keep the video chipset cool. It is located on the video adapter.

CPU cooling. Keeping the CPU cool is very critical for the normal operation of the computer. The CPU is one of the PC's greatest heat-producing components. Some motherboards have an on-board CPU heat sensor and a CPU fan sensor. These monitor the temperature and shut down the computer if the heat reaches a level where it can damage the CPU or other critical chips.

The most common method of dissipating the heat generated by the CPU is to install a heat sink right on top of the CPU. A special chemical, called *thermal compound*, is placed between the CPU and the heat sink to improve the thermal transmission between the CPU's surface and the heat sink. Additionally, a small fan is installed on top of the heat sink that blows the hot air away from the CPU surface. Figure 2-4 shows a CPU cooling fan.

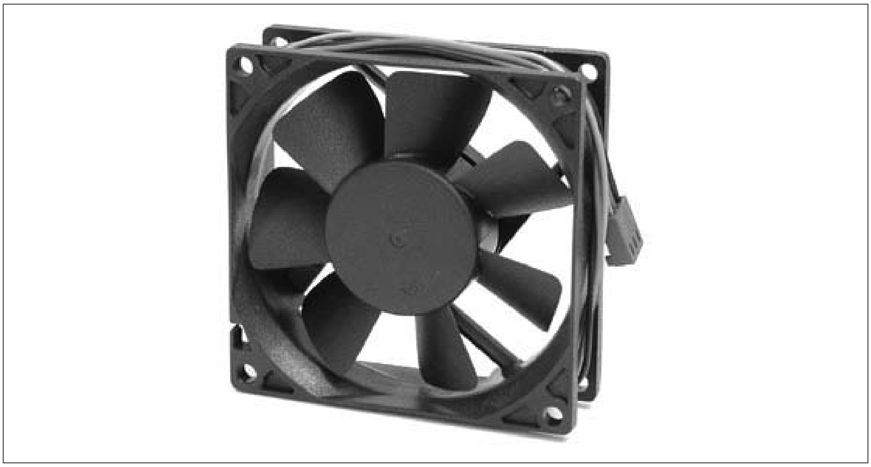


Figure 2-4. CPU cooling fan

On some CPUs, the heat sinks use heat pipes to take the heat away from the CPU surface. Some other manufacturers use CPU coolers that consist of a heat sink of copper plates and high-performance cooling fans.

In some cases, a *liquid cooling system* is used to keep the CPU cool. In this method, a water block is used to take the heat away from the CPU and the chipsets. Water is circulated from the water block to the radiator, where it is cooled. The major advantage of liquid cooling is that the cooling parts do not produce noise as do air-cooling systems.

Phase change cooling is another, more extreme cooling technology that takes advantage of the phase change from liquid to gas. The phase change cooler unit contains a small compressor similar to the compressor in a freezer. This unit is located underneath the computer. The compressor squeezes a cool gas and condenses it to liquid form. The liquid is pumped to the processor through a pipe, which heats it, causing its own heat to dissipate.

Installing, Configuring, and Optimizing Personal Computer Components

So far, you have learned about different types of components in a personal computer. As a PC technician, you are expected to be skilled in installing, removing, and upgrading these components. In this section, we will take a look at some basic techniques required when performing these tasks for specific devices such as storage, display, and input devices.

Installing storage devices

The main storage device for a personal computer is the hard disk. When installing, removing, or upgrading the hard disk, you need to prepare the disk before it is actually installed in the drive bay inside the computer.

Drive preparation. Drive preparation refers to the task of performing some basic jobs before the hard disk is actually installed in the computer. In some systems, you may be required to format the disk before installation or configure its jumper settings to make it a Master or Slave drive. Hard drives fall into two main categories: ATA/IDE and SCSI. The procedure for configuring jumper settings is identical for hard disks as well as for CD/DVD drives when the motherboard has an ATA/IDE interface.

A typical computer motherboard has two IDE connectors, each with two connectors on a single cable. This means that you will be limited to four drives on one computer. When using the SCSI interface, you can connect up to seven drives on a single SCSI cable.

The following steps are completed before installing an IDE drive in the drive bay:

1. Set the Master/Slave jumpers on the drive. The jumpers on the drive can be set to Master, Slave, or Cable Select (marked as M, S, and CS respectively). Look for the jumper settings diagram on top of the drive. Each IDE interface can have only one Master connected to its cable, and the other drive must be set as Slave. If this is the only drive connected to the interface, it must be set as Master.
2. Remove the drive bay from the computer case, if required.
3. Install the drive in the drive bay.
4. Reinstall the drive bay in case you have removed it.
5. Connect the power supply connector with correct orientation.
6. Select an appropriate connector from the ribbon cable. Identify its first pin (Pin 1) on the ribbon cable, which is usually a red-colored wire on one edge. Pin 1 or the red-colored wire is held close to the power supply connector. Insert the connector carefully.
7. Start the computer. Most drives are PnP-compatible, meaning that they will be identified and configured automatically by the system BIOS. If the computer BIOS does not automatically detect and configure the drive, you may need to enter the BIOS setup program and manually configure the drive.

8. Once the drive is installed, you need to partition and format the hard disk drive. This step is not necessary for CD/DVD drives. For hard disks, you can use the Disk Management utility to partition and format the drive if the computer already has an operating system installed on another hard disk. If this is the first or only drive in the computer, the drive can be partitioned and formatted during the installation of the operating system.

For installing *Small Computer System Interface (SCSI)* disks, the procedure is a little different. An SCSI drive can be an internal or external drive, depending on the hardware configuration of the computer. Also, the SCSI bus can be an 8-bit, 16-bit, or 32-bit bus. The main issues with preparing SCSI drives are as follows:

Cables, connectors, and termination

A typical computer may have an SCSI-1, SCSI-2, or SCSI-3 interface, each with a different number of pins. SCSI-1 has a 50-pin connector, SCSI-2 can have a 25, 50, or 68-pin connector, and the SCSI-3 interface can have a 68-pin or 80-pin connector. If the SCSI devices are internal devices, the single SCSI cable will have several connectors and the first connector is attached to the SCSI adapter. If the SCSI devices are external devices, they can be connected to the SCSI cable in a daisy-chain fashion. Each external SCSI device has two connectors. The first connector is attached to the SCSI cable from the adapter, and the second is attached to the next SCSI device using a similar SCSI cable, and so on. The second connector on the last SCSI device is terminated. Some SCSI devices have a built-in terminator.

Addressing

All SCSI devices must also be assigned a SCSI identification number (SCSI ID), which must be unique on the SCSI bus. These ID numbers are from 0 to 7 on an 8-bit bus, from 0 to 15 on a 16-bit bus, and from 0 to 31 on a 32-bit bus. A device with a lower SCSI ID always gets higher priority and performs better than devices with higher SCSI IDs. If the SCSI drive you are installing will be a bootable device, you must assign it SCSI ID 0.

> The procedure for installing and configuring an SCSI device is much more complex than installing an IDE device. Always refer to the documentation that comes with the device in order to configure it correctly. Remember that each SCSI device must be assigned an SCSI ID, and the SCSI bus must be terminated. If any of these settings are missing or incorrectly configured, the device will not work.

Installing/upgrading display devices

Installing or upgrading a display device is a common task for helpdesk and support technicians. The task typically involves replacement of an old or nonworking monitor with a new one. It seems to be a simple task, compared to installing other devices such as the hard disk. The following are some important steps that you must take when installing or upgrading monitors:

- Always ensure that the power supply to both the computer and monitor is turned off. Remove the main power supply cables from the wall socket.

- If replacing a monitor, remove the monitor cable from the rear panel of the computer case by removing the DB-15 connector.
- Obtain the driver for the new monitor. It is usually included in the monitor package, or you can download it from the manufacturer's web site.
- Connect the new monitor to the computer and connect to the AC main supply.
- Turn on the computer and look to see whether the computer BIOS and the OS detect the new hardware device.
- If required, install the driver software using an OS utility such as the Device Manager in Windows XP/2000.
- Refer to the user manual of the monitor to adjust brightness, contrast, and color levels. You may also need to adjust the horizontal and/or vertical positioning.

Installing and removing input/multimedia devices

The procedure for installing or replacing input/multimedia devices depends on the type of device. Installing or replacing a standard keyboard or mouse is fairly simple. These devices are typically connected to either the PS/2 port or the USB port of the computer. Both PS/2 and USB devices are PnP-compatible, meaning that no further manual configuration is required when any of these devices are installed. If you are replacing a PS/2 or USB keyboard or mouse with a wireless keyboard or mouse, you need to refer to the user manual to correctly configure the device settings. Wireless devices need a wireless adapter to be installed on the motherboard.

Troubleshooting Tools and Procedures

Troubleshooting is one of the major tasks that helpdesk and support technicians have to perform. Problems with computers may be a result of a user error, hardware failure, or a software issue. In this section, we will discuss the troubleshooting theory, basic diagnostic procedures, and the identification of problems with different components of the personal computer.

Basic troubleshooting theory

The basic troubleshooting theory can be summarized as follows:

Back up user data

If you need to make changes to the system, always back up the system and user data. Although you should not expect this, it is not uncommon that the system may break down because of the changes you make. Backing up data will ensure that the same can be restored when the system is repaired.

Systematic approach

Always apply a systematic approach when troubleshooting a problem. More complex problems can be easily broken down into smaller components. These components should then be analyzed individually to correctly identify the source of the problem.

Make no assumptions

Always give importance to even the smallest cause of the problem. Never assume that a certain problem is always due to a specific reason only. Similar problems on different systems may have different reasons. Verify the identified cause of the problem before you apply a resolution.

Establish priorities

When faced with several calls, you must establish priorities. You need to decide which problem needs your attention immediately and which problem can wait. For example, if the entire network is down and a single user is complaining that he cannot open a file on his computer, the network problem needs to be resolved first.

Documentation

Whenever you resolve a problem, make sure that you complete the documentation. The documentation may include the date and time the problem is reported, symptoms of the problem, the actions you took to resolve the problem, and whether the problem was resolved.

Basic diagnostic procedures

Troubleshooting a computer problem requires that you follow some basic diagnostic procedure, which starts from identification of the problem symptoms, isolating the affected area, and so on. Following a logical procedure not only makes troubleshooting easy but also reduces the time it takes to resolve the problem. The following paragraphs summarize these steps:

1. Define and identify the problem. The first step in diagnosing a problem is to define and identify it. This ensures that you are applying your diagnostic skills to resolve a correct problem. A problem can be identified only when you have sufficient information. Gather as much information as you can. Check the problem symptoms and question the user. Check whether the user has made any configuration changes to the hardware or the software. Collected information will help in correctly identifying the problem.
2. Analyze the problem. You need to make a thorough analysis of the problem to find out whether the problem is due to a user error, a hardware failure, or a software bug. Most often, simply restarting the computer resolves a problem. The best plan is to always check the simple things first. For hardware-related problems, check whether the power is on, check loose connections, and check whether all components are seated properly.
3. Test and isolate the failed component. You may also need to isolate the cause of the problem and correctly identify the hardware component that has failed. Once detected, you must test the failed component to make sure that it has actually failed. For OS-related problems, you can use built-in utilities such as the Device Manager, the System Configuration Utility (MSCONFIG), or the Advanced Boot Options.
4. Consult documentation and other resources. Replacing a failed hardware component or applying a fix to a software problem may require you to consult vendor documentation. If this is not available, you may need to check other sources of information, such as vendor's web site, online forums, and user groups that use the same or similar products. It is very much possible that someone else has faced a similar problem.

5. Apply the solution. Once you have identified the problem, you will need to find out a solution and apply it. Applying the solution requires that you test your solution thoroughly before handing over the computer to the end user.
6. Document your activities. When the problem is resolved, you must prepare documentation of your activities. These include the date and time the problem was reported, the details about the computer and the user, symptoms of the problem reported, what you did to identify the problem, and what actions were taken to resolve it. Documentation is very helpful if you face a similar problem again or if someone else needs help resolving a similar problem.

Basic troubleshooting tools

Troubleshooting tools can be classified into two main categories: hardware and software. These are explained in the following paragraphs:

Hardware tools. The following tools are categorized as hardware tools:

Screwdrivers
The most common screwdrivers required for installation and repair of computer components are flat blade, Phillips head, and Torx. You may also need a magnetic screwdriver with different types of bits to reach internal parts that you cannot reach with smaller screwdrivers.

Long nose pliers
A long nose pair of pliers is required to hold connectors or to pick up small screws that accidentally fall in the computer case or on the motherboard. Additionally, you should keep a tweezers set.

Flashlight
A flashlight is very helpful in locating parts of the computer where light is not adequate. Keep extra batteries for the flashlight as well.

Soldering iron
A soldering iron is required to make connections using a solder wire. You may hardly need to use a soldering iron on new computers, but it is good to keep it in your toolkit.

Wire strippers
A wire strippers set is used to cut wire and strip off the insulation.

Compressed air can
A small can of compressed air is useful in blowing off dust from internal or external parts of the computer.

Multimeter
A multimeter is used to check resistance (continuity), voltage, and current. You can have an analog multimeter, which shows the readings on a scale, or you can have a digital multimeter, which shows the readings on an LCD panel.

Software tools and utilities. A large number of personal computer problems are caused by software applications, incorrectly configured hardware devices, or user errors. A variety of software diagnostic tools and utilities can be used to resolve these problems. Some of the software tools include the following:

Bootable disks

Bootable floppy disks are very useful for starting a computer with MS-DOS. You can make a bootable disk and include on it such essential utilities as the FORMAT and EDIT commands. If the computer can start using the bootable disk, you can examine other components such as the RAM, the hard disk, and device drivers, and you can replace any failed component, if required.

Power-On Self-Test

Every computer has a Power-On Self-Test (POST) routine, which is typically stored on the BIOS chip. The POST detects and tests major hardware components installed on the computer. A successful completion of the POST confirms that the basic components of the computer are functioning as expected. Depending on the BIOS software used on the motherboard, certain hardware errors can be identified from the beep codes. You will need to refer to the user manual of the motherboard to understand the correct meaning of these beep codes.

Hard Drive Self-Test

Normally, the POST would indicate whether there is a problem with the hard disk. You can also use the Microsoft Diagnostics (MSD) program to test the integrity of the hard disk. Some hard drive manufacturers include a software utility to do the testing. For example, Hitachi has a software utility named Drive Fitness Test to test hard disks.

Software diagnostic tools

Software diagnostic tools help test the hardware components of a personal computer. Commonly used software diagnostic tools include Microsoft Diagnostics (MSD), CheckIt Pro, AMIDiag, and QAPlus. Several software utilities are propitiatory to manufacturers and can be used to test their hardware devices.

Identifying problems

Problems with the components of a personal computer can be resolved only when they are correctly identified. If a problem cannot be identified, it is difficult to solve it. This section covers troubleshooting techniques for common problems with computer components.

Motherboard and CPU problems. Problems with the motherboard or the CPU typically result in a "dead" computer. If the motherboard or the CPU is not functioning, the computer will not start. Most technicians do not repair a faulty motherboard, and they do not have the resources to do so in an office or at a client location. This means that a defective motherboard must be replaced. A CPU, on the other hand, can be damaged due to overheating if the cooling fan fails or gets jammed due to excessive dust. If a CPU has failed immediately after installation, the most probable cause is that it has not been installed correctly. After installation, make sure that the CPU is inserted properly in its socket and that the cooling fan is working. You may need to remove the CPU to verify that its pins are not bent or broken due to incorrect insertion.

Power supply problems. If a power supply is malfunctioning, the computer will not respond when it is started. If the power supply fans are jammed or not working, the power supply will suddenly shut down or reset the computer during normal operation. This symptom appears on those power supply units that are built with thermal protection. The first thing to check with a power supply is whether the cooling fan is working. If required, you may open the computer case and measure voltages on different connectors using a multimeter. A completely failed power supply unit must be replaced with another power supply unit of the same rating.

Memory problems. Most problems with memory modules (RAM) can be identified from the slow response of the computer. If one of the memory modules has failed, the computer performance will go down. Applications will take a long time to open, or the computer will take a long time to process requests. On some computers, the Power-On Self-Test indicates whether there is a problem with memory modules. Before you replace a memory module, try to remove and reinstall the original modules. Sometimes, the problem is due to improper seating and/or loose connections.

Problems with display devices. Display device problems occur due to incorrect configuration, a loose connection of the video adapter, or a failed monitor. There could be either no display at all or a bad video. A monitor can be easily checked by connecting it to another computer. If it works well with another computer, the problem is certainly with the on-board video controller or the video adapter card. If the monitor does not work with another computer, the best way to resolve the problem is to replace it with another working monitor. Make sure that you turn off power to both the computer and the monitor before disconnecting or connecting the monitor. It is not advisable to repair the monitor yourself at a user's desk or at a client location.

Problems with input devices. The most common input devices for a computer are the keyboard and the mouse. Many problems with the keyboard are caused due to dust that accumulates on the keys. You can try to fix the problem by cleaning it with a special keyboard cleaning product. If that does not help, you should replace the keyboard. It is meaningless to repair the keyboard because a new keyboard costs much less than the time that you would spend in repairs. Mouse problems are also due to a dirty environment. When you notice that the pointer is jumping around the screen, you may either try to clean the mouse or replace it. First, try connecting the mouse to another computer to verify whether it is working properly. A mouse with a rubber ball has rollers and sensors. Dust accumulated on the ball, on the sensors, and on the rollers causes the erratic behavior of the pointer. If cleaning the mouse ball and rollers does not help, replace the mouse.

Hard disk problems. A working hard disk generally generates a sound that comes from its spinning. Problems with hard disks can be due to a faulty adapter card, a failed hard disk, or an incorrect/loose connection. If the disk is incorrectly connected or the adapter is loose on the expansion slot, the computer will not go beyond POST. This symptom is fairly easy to identify. Similarly, if the hard disk has completely failed, the POST routine will not be able to identify the bad disk. Sometimes, you can recover a failed disk by simply reformatting it. This does not help in all situations because a reformatted disk is likely to fail again. Due to a failing process of computer components, it is advisable to replace the failed disks instead of trying other solutions such as low-level formatting.

CD/DVD problems. Most problems with CD and DVD drives are related to media, i.e., the disc itself. Try replacing the disc with a new disc. If the new disk works well and old discs do not, you have identified the problem. Problems with newly installed disks are caused by incorrect jumper settings, incorrect connections, or the inability of the system BIOS to recognize the drive. Check your connections, including the power supply connection. Try using a different power supply connector, if one is available.

Adapter card problems. Most of the new motherboards have built-in interfaces for many functions that were earlier derived from adapter cards. Some of the common adapters include the network card, the modem card, the sound card, and the video card. If any of these are not working, you need to do a visual inspection first. Make sure that the card is seated properly in the expansion slot. For example, if there is a network connectivity problem, check that the network cable is securely attached to the RJ-45 socket on the card and that the LED status indicators are showing normal activity. Similarly, if the modem is not responding or not able to dial, first check that the telephone cable is properly connected and you have a dial tone.

Preventive Maintenance (PM)

Preventive maintenance helps reduce the chances of computer breakdowns and improves overall system performance. It is essential to perform preventive maintenance at regular intervals. As a computer technician, you are expected to be aware of different forms of preventive maintenance and how these measures can be implemented. In this section, we will brief some essential preventive maintenance tasks for personal computer components.

Scheduling preventive maintenance

Preventive maintenance should be done for all desktops in an office or at home. It is good to have a written preventive maintenance schedule and to ensure that it is followed. The schedule should outline what PM tasks are to be performed and on which computers. Regular PM tasks include the following:

- A visual inspection of internal and external components.
- Updating the operating system and/or device drivers.

www.allitebooks.com

- Cleaning the components.
- Fragmenting the hard disk and performing a disk cleanup.
- Ensuring that the computer is operating in a healthy environment with acceptable levels of temperature and humidity.

Visual and audio inspection

Perhaps the first and most important step in performing preventive maintenance on a computer is to do a visual and audio inspection. Visual inspection inside the computer will reveal if any of the components are loose in their respective sockets or if some cooling fans are jammed. Visual indicators such as the hard disk activity, LED, or status indicators on NICs are very helpful in determining whether a component is working. Similarly, beep codes of the system BIOS will usually indicate whether some hardware component is not functioning as expected. Audio inspection also refers to listening to the spinning noise of the hard disk or CD/DVD discs.

Driver and firmware updates

Due to continuous enhancements in technology, manufacturers of hardware components, software applications, and operating systems keep on making changes to their products. These changes are released to customers as updates. It is important to check with vendors about the latest driver software for their devices. Software/driver updates also ensure that the devices will work when the operating system is upgraded. Similarly, the BIOS or the firmware must also be kept updated so that it can support new devices built on new technologies.

Heat and temperature

No matter how many ventilation slots and cooling fans exist within a computer, it is essential that the external cooling factors should also be taken care of. If the computer is located in an area where the temperature is not controlled and no proper ventilation exists, it will eventually heat up after prolonged hours of operation. You must make sure that the computer is operated in a room where adequate air-conditioning and ventilation is available.

Humidity

Humidity also needs to be mentioned in this section. Computers need to be located in areas with moderate humidity. Dry areas or areas with too much moisture do affect the life and performance of computers. If the air around computers is too dry, it will cause static electricity to build up that may damage expensive computer parts.

PM for display devices

Display devices, or monitors, produce heat when working and are also exposed to dust around the area where the computer is installed. If not cleaned regularly, dust accumulates on the screen and the case, and also makes its way inside the monitor through the ventilation slots provided for keeping the monitor cool. Accumulated dust can also block some ventilation slots. Monitors should be regularly cleaned using a lint-free cloth.

PM for power supply

A majority of computer problems are a result of failure of the power supply. Care must be taken to ensure that the computer gets a clean and consistent power supply. Some of the preventive maintenance methods for power supply are as follows:

Uninterruptible Power Supply (UPS)
Should be used to provide a clean and consistent voltage to the computer. UPS systems protect the computer from power spikes, surges, and sags that can cause significant damage to computer parts.

Power strips
Useful for providing extra power slots and are also helpful in protecting the computer from sudden changes in voltage levels such as power spikes and sags.

Surge protector
Used to supply a constant voltage to computers and prevent damage due to power surges. A power surge refers to a sudden change of voltage in the power line.

Regular cleaning of the computer's power supply unit
Helps prevent the power supply unit from heating up during normal preparation (especially cleaning the cooling fan and ventilation).

PM for input devices

When possible, all input devices, including the keyboard, mouse, scanners, etc., should be kept covered when not in use. Keyboards collect dust from the surrounding areas. As a result, the keys start having intermittent jamming problems. Dust accumulated on the sides of the keys can be blown out using compressed air. You can also use a soft brush to get rid of the dust accumulated around and between key tops.

PM for storage devices

There are a number of preventive maintenance methods for storage devices, each suitable for a particular type of device. Even if the computer is located in clean surroundings, cleaning internal parts of computers regularly does help in extending the life of its components. Some of the preventive maintenance procedures for storage devices are as follows:

- Hard disks should be regularly defragmented and cleaned up of unnecessary temporary files. You can use built-in operating system utilities such as Disk Defragmenter (*defrag.exe*) and Disk Cleanup. You can also check hard disks regularly using standard procedures such as defragmentation and regular clean up. Additionally, you can check for and fix bad sectors in disks using the Check Disk (*chkdsk.exe*) utility.
- CD and DVD drives rely on laser beams and an optical lens to read and write data. Dust accumulates on the lens surface that causes intermittent disk read/write problems. You should regularly clean CD and DVD drives using appropriate lens cleaners.

- Tape drives should be cleaned using tape drive head cleaners.
- Floppy disk drives should be cleaned using a floppy disk drive head cleaner.

PM for motherboards, memory, and adapters

Motherboards, memory modules, and add-on cards (adapters) are all thermally sensitive devices. Ensuring that the computer is used in an area where temperature, humidity, and dust are controlled helps enhance their performance, extend their life, and reduce breakdowns. Make sure that all the cooling fans are working properly, that dust has not accumulated around them, and that the ventilation slots of the computer case are not blocked. To ensure that problems are minimized, regularly blow out dust from tops of motherboards, CPU fans, memory modules, and adapter cards. Cooling fans usually get jammed due to accumulation of dust around blades and walls.

Laptops and Portable Devices

Laptops are built for mobile computing. They are much smaller in size and weight than desktop computers, and they are portable, which means that they can easily be carried from one place to another. Due to their smaller size, the components that make up a laptop have to be compact. Although laptops cannot beat desktops in features, performance, and computing capabilities, their functionality is comparable for everyday computing needs. Laptops use special components that are different from normal desktops, and they need special handling and maintenance. In this section, we will discuss unique features of laptop components, their power management options, troubleshooting techniques, and preventive maintenance procedures.

Overview of Laptop Components

One of the major differences between a laptop and a desktop is that the laptop is portable while the desktop is not. Some of the other factors that distinguish between a desktop and a laptop are as follows:

Size

A laptop is much smaller than a desktop because all of its components are in a single case. This helps when you do not have sufficient space to keep individual desktop components such as the CPU, the monitor, and the keyboard.

Cost

The cost of a laptop is much more than that of a desktop. It is still about 50 percent more than a standard desktop of comparable configuration, but the gap is reducing fast.

Ease of operation

Desktops offer ease of operation due to a larger keyboard, a bigger mouse, and larger displays. If you are used to working on a desktop, you may find that it takes time to get used to working on a laptop.

Performance

Due to limitations in size, the laptop components are not equal in performance to desktops.

Expandability/Upgradability

Laptops offer limited expandability or upgradability in terms of motherboard, memory, and storage devices. On the other hand, desktops can be easily expanded when required.

Reparability

Desktops are easy to repair. All you have to do is open the case and repair or replace a faulty component. Laptops require special skills and proprietary replacement parts.

The next sections include a brief discussion of major laptop components.

Motherboards

Most laptop motherboards are *proprietary*, meaning that each manufacturer follows its own standards. The only thing they have in common is that they have a very small Form Factor as compared to desktop motherboards. The design of the motherboard largely depends on the laptop case. In order to save space, most of the interfaces—such as serial, parallel, USB, video, network, modem, sound, and so on—are integrated on the motherboard itself or on a small add-on board known as the *daughter board*. The main advantage of integrated components on a single board is that it does save space, but it comes at the cost of performance and durability. If one of the components goes bad, the entire motherboard has to be replaced. This simply means that repairs of laptop motherboard are an expensive affair.

Processors

Laptop processors are not as fast as desktop processors. As of this writing, desktop processors are available in speeds of nearly 4 GHz, whereas laptop processors are still in the 2.4 GHz range. The laptop processor has a smaller Form Factor compared to the desktop processor. Some of the differences between laptop and desktop processors are as follows:

- Most laptops have their processors directly soldered to the motherboard. This means that the processor cannot be removed. If it goes bad, you will need to replace the motherboard. Some laptops use a Micro-Flip Chip Ball Grid Array (Micro-FCBGA) socket for mounting the processor.
- Laptop processors can be slowed down when they are not required to run in full capacity. A process known as processor *throttling* allows the OS to put the processor in active sleep mode or slow-down mode.
- Laptop processors run at lower clock rates than desktop processors, which helps reduce the heat produced when the processor is running at its full capacity.
- Laptop processors require less power to run than desktop processors. This results in slower performance than desktop processors but helps conserve battery power.

Intel's Centrino and AMD's Mobile Athlon are among the popular processors used in laptops. *Intel Centrino Duo* and *AMD Turion 64 X2 Mobile* are the current laptop processor models as of the writing of this book.

Power supplies

Laptops rely on battery power when not connected to the mains AC power. An AC adapter is used to supply DC power to the laptop when connected to the AC mains. This adapter also keeps on charging the battery, as long as the laptop is connected to the AC mains. Batteries come in a variety of shapes and sizes, depending on the make and model of the laptop. Most laptops use Nickel Cadmium (NiCd), Nickel MetalHydride (NiMH) or Lithium-Ion (LiIon). The LiIon batteries have become popular because of their light-weight and longer life. NiCd batteries have limited life because they can only be charged for a specific number of times. Moreover, these batteries suffer from *memory effect*, which reduces overall battery life.

The life of a charged battery depends on how the laptop is used and how the power options are configured to conserve power. The power management software on operating systems allows you to configure power options that, in the long run, also extend the life of the battery. The milliAmp-Hour (mAH) rating noted on top of the battery pack indicates the capacity of the battery. The higher the mAH rating of a battery, the longer its runtime.

Another variation of a laptop power supply is a DC adapter that can be plugged into a DC power outlet in a car or an airplane. You can plug this adapter in the cigarette lighter socket and power on your laptop. This adapter is good for people who frequently travel.

Memory

Both desktops and laptops use dual inline memory modules (DIMMs) but they are different in shape, size, and capacity. Laptops use smaller memory modules that fall into two main categories: *SO-DIMM* and *MicroDIMM*. These are explained in the following sections.

Small Outline-Dual In-line Memory Module (SO-DIMM). SO-DIMM is the most popular memory module used in laptops. A SO-DIMM has 72, 100, 144, or 200 pins. The 72- and 100-pin SO-DIMMs support 32-bit data transfers while the 144- and 200-pin SO-DIMMs support a 64-bit data bus. SO-DIMMs have a storage capacity of up to 2 GB.

Micro Dual In-line Memory Module (MicroDIMM). MicroDIMM is the smallest and latest in laptop memory modules. The most commonly used MicroDIMM has 144 or 172 pins and supports a 64-bit data bus. A MicroDIMM is about half the size of a SO-DIMM, with a capacity of up to 1 GB, and it is more expensive than SO-DIMM.

Display devices

Laptops use LCD screens, which are driven by a video control circuitry and a dedicated power supply unit called the inverter. The video card sends the output in digital format unlike the analog format for the normal monitors in desktops. In this section, we will cover a brief discussion of LCD technologies and other terms associated with LCD displays.

LCD technologies. LCD screens for laptops are classified into two categories: Active Matrix and Passive Matrix, as summarized in the following paragraphs:

Active Matrix
An Active Matrix LCD screen utilizes the Thin Film Transistor (TFT) technology and is made up of a matrix of several pixels. Each pixel has a thin transistor, which is used to align the pixel and switch its color. Active matrix LCDs offer very good response times and good screen resolution, and produce crisp picture quality. The only disadvantage is that they consume more battery power than passive matrix LCD screens.

Passive Matrix
Passive Matrix LCD screens use a simple grid to supply charge to a particular pixel in the display. Passive matrix LCD screens offer lower screen resolutions, slower response times, and poorer image quality than do active matrix LCD screens.

LCD resolution and aspect ratio. Screen *resolution* in CRT and LCD screens is measured by the number of rows and columns of pixels. The higher the resolution, the higher the image quality of the LCD screen. *Aspect ratio* refers to the ratio of width and height of the screen. There are a number of resolution standards supported by LCD technologies, such as XVGA, SXGA+, UXGA, WUXGA, and QXGA. The main standards are summarized in Table 2-2.

Table 2-2. LCD resolutions

Standard	Resolution	Aspect ratio
Extended Graphics Array (XGA)	800 × 600 1024 × 768	4:3
Super Extended Graphics Array Plus (SXGA+)	1400 × 1050	4:3
Ultra Extended Graphics Array (UXGA)	1600 × 1200	4:3
Widescreen Ultra Extended Graphics Array (WUXGA)	1920 × 1200	16:10
Quad Extended Graphics Array (QXGA)	2048 × 1536	4:3

With constant enhancements in the LCD technologies, it is difficult to keep track of different video standards, supported resolutions, and aspect ratios. For the A+ exams, just remember the main terms used in LCD video technologies such as XGA, SXGA+, UXGA, WUXGA, and QXGA.

Native resolution. Most manufacturers make their LCD screens with a single fixed resolution called the native resolution. This is unlike the CRT desktop monitors in which you can change the screen resolution depending on the frequency of the video signal. This means that the LCD screen used with a laptop must match the video interface inside the laptop. A mismatch of the video interface and the LCD screen may cause a distortion in the display.

Contrast ratio. The contrast ratio measures the ratio of the lightest color and the brightest color that a video display can produce. Older LCD screens used to have low contrast ratios of about 500:1, whereas the new LCD screens offer a better contrast ratio of about 1200:1. Better contrast ratio means that you are able to view good color depth for images.

Storage devices

Laptops use hard drives, floppy drives, and CD/DVD drives for data storage. While the hard disk is an essential component of every laptop, not every laptop has a floppy drive or a CD/DVD drive. You will find that most new laptops have a special DVD drive that can be used to read and write DVDs as well as CDs. The following paragraphs provide a summary of these storage devices.

Hard drive. A hard drive is an essential part of a laptop and is used as the primary means of data storage. Due to limitations of space, the size of the hard drive is much smaller than the normal 3.5" desktop hard drive. A laptop hard drive is about 2.5" wide and ½" thick, and it has smaller connectors. The storage capacity is also lesser than the desktop hard drives. Laptop hard drives use ATA and UDMA technologies as do the desktop drives.

CD/DVD drives. As with the hard drives, the CD and DVD drives for laptops are also much smaller in size (about ½" thick) than the desktop drives. These drives come in many formats, such as CD-ROM, CD-R, CD-RW, DVD, DVD-RAM, etc. Most new laptops have a CD burner or a DVD burner drive that combines the functions of reader and a writer. Irrespective of their shapes and sizes, the functionality and features of these drives remain comparable to the ones used on desktops.

Floppy drive. The floppy drive for a laptop is becoming optional because of the popularity of CD and DVD drives. You can still connect a floppy drive to a laptop using a drive bay, if it is available on the laptop. Most of the external floppy devices and connecting cables are proprietary, and a device made for one make cannot be connected to another make.

Input devices

This section covers some basic information on input devices used for laptops. While both desktop and laptops use keyboards for typing in the input, the function of a mouse is handled by pointing devices such as a trackball or a touchpad in a laptop.

Keyboards. The keyboard for the laptop is built into the lower portion of the case, unlike the desktop, in which the keyboard is a separate external device. Laptop keyboards usually have a much lower number of keys than normal computer keyboards. One major difference is that the number keypad is missing. But you can still use perform number pad tasks using special function keys labeled as *Fn*, which appear in blue color letters. Function keys offer several other actions such as toggling internal and external devices.

Pointing devices. On a normal desktop, a mouse is used to control the pointer on the computer screen. On a laptop, this function is handled by the devices described in the following list:

Trackball
: A trackball was used in earlier laptops as a pointing device. The function of a trackball is similar to a normal mouse turned upside down. When you move the ball with your thumb or finger, the on-screen pointer moves, and you can use the click button to select an item on the screen.

Touchpoint
: A touchpoint or a finger mouse was introduced with IBM's ThinkPad series of laptops. It uses a small stick with a rubber tip. When you move the stick in a particular direction, the on-screen pointer moves in the same direction. The harder you push the stick, the faster the movement of the pointer.

Touchpad
: The touchpad was developed to overcome limitations of a trackball. It consists of a rubber pad that is sensitive to the touch of a finger. As you touch the pad with your finger and move it, the on-screen pointer moves in the same direction. A touchpad has two more buttons on its left and right side for left-click and right-click functions.

Touch Screen
: A touch screen pointing device is what you see in many retail stores and on ATMs. Just touch an appropriate button in order to select an item from the menu. Touching the screen button produces the same result as selecting an item on the screen by double-clicking the mouse button.

Expansion buses and ports

Laptops are smaller in size, lightweight, and compact in design. The portability of laptops makes them ideal computing devices for traveling people. The functionality of laptops cannot be expanded like desktop computers but still there are options to add external devices using standard expansion bus and ports. Some of the ports on laptops are similar to those found on desktops while others are totally different. In this section, we will summarize various types of expansion buses and communication ports available on laptops.

Mini PCI. The Mini PCI bus is a laptop/notebook variation of Peripheral Component Interconnect (PCI) bus used on desktop computers. It is essentially a 32-bit bus operating at 33 MHz, and it uses a 3.3 volt power connection. Three different Form Factors of Mini PCI bus are Type I, Type II, and Type III. Type I and Type

II bus have 100-pin connectors while the Type III bus has a 124-pin connector. Commonly used Mini PCI bus components include modems, network cards, sound cards, ATA, and SCSI controllers. You can also use an adapter to convert Mini PCI bus to a PCI or vice versa.

Personal Computer Memory Card International Association (PCMCIA). The PCMCIA standard was mainly developed to expand the functionality of laptops by adding devices. It is also known as the PC Card standard. PC Card bus adapters are now available for desktop computers. The size of a PCMCIA card approximately equals that of a credit card. The most commonly used standard is the 16-bit PCMCIA 2. PCMCIA 3 increased the bus width to 32 bit with a bus speed of 33 MHz. The two main components of the PC Card are: Socket Services software and Card Services software, as summarized in the following paragraphs:

Socket Services software

This is a BIOS-level interface for the PCMCIA expansion slot. It is mainly used to hide the details of the PC Card from the computer and can detect the type of the card when it is connected.

Card Services software

It is the interface between the applications running on the computer and the Socket Services. Applications need to know the I/O ports and the IRQs that the PC Card is using. The Card Services software gives this information to applications.

> All PCMCIA implementations support Plug and Play functionality, and the devices are hot-swappable.

PC Cards come in different types, as summarized in Table 2-3.

Table 2-3. Types of PC Cards

Type	Thickness	Common use
Type I	3.3 mm	Memory modules
Type II	5 mm	Network adapters, modems, sound, and SCSI controllers
Type III	10.5 mm	Hard drives

The Type II card is the most commonly used type of PC Card, and most systems have at least two Type II slots or one Type III slot.

ExpressBus. The ExpressBus was designed to expand the functionality of standard USB ports. These ports were used in earlier laptops when the USB port did not have expansion capabilities. As an alternative, manufacturers provided an ExpressBus hub. One side of the hub was connected to a USB port on the laptop while the other side provided seven extra USB ports for connecting USB devices. More hubs could be connected to form a daisy chain, and up to 127 USB devices were supported on the bus.

USB ports. As with desktop computers, laptops also come with built-in USB ports. Usually, every laptop has two or three of these. Most external components made for laptops, such as the external mouse, keyboard, and removable drives, can be connected to USB ports. USB ports are covered in detail in the first section of this chapter.

Mouse and keyboard port. The desktop keyboard and mouse usually have PS/2 connectors. These can be connected to a laptop externally on PS/2 ports available on the laptop. If the laptop does not have built-in PS/2 ports, you can get a USB to PS/2 converter. On the other hand, if the laptop has PS/2 ports instead of USB ports, and the keyboard or the mouse is a USB device, you can use a PS/2 to USB converter.

Monitor port. Most laptops have a 15-pin connector for attaching an external monitor. The external monitor can be a CRT or an LCD. Besides providing ease of operation, external devices for laptops such as the monitor also help troubleshoot problems with built-in devices.

Communication ports. Communication ports for laptops are used for connecting a laptop with a wired or a wireless network. Different communication ports are summarized in the following paragraphs:

Bluetooth

Bluetooth wireless communication standards are described in IEEE 802.15.1 specifications. Bluetooth technology is popularly used for wireless personal area networks (PANs). It supports transmission speeds from 1 Mbps (Bluetooth 1.0) to 3 Mbps (Bluetooth 2.0). A wireless device using Bluetooth technology can communicate only in small distances of up to 30 feet and needs a line of sight for its operation. Bluetooth is more of a mobile phone technology than a wireless network technology. You can use external wireless devices such as a keyboard or a mouse with a laptop if they support the Bluetooth standards.

Infrared

An infrared port allows you to connect to external wireless devices such as a keyboard or a mouse. Infrared devices need a clear line of sight to operate. Most common applications of infrared devices are found on home entertainment appliances such as the TV or the music system. They can also be used for connecting laptops devices. The transmission speed of infrared devices is about 4 Mbps, and the maximum range of the signal is about 10 feet.

Ethernet

Most new laptops come equipped with both wired and wireless networking solutions. A built-in 10/100 Mbps network adapter can be used to connect the laptop to a wired local area network (LAN). The wired network interface has a standard RJ-45 connection socket while the wireless connectivity is obtained through a built-in antenna. In old laptops, you might have to use a Type II PC Card for connecting to the LAN.

www.allitebooks.com

Wireless standards are defined in IEEE 802.11 specifications and are collectively known as *WiFi (Wireless Fidelity)* standards. The most commonly used wireless networking standard in laptops is the 802.11b, which operates at 11 Mbps speed. The 802.11g standard is also gaining popularity due to its higher transmission speed of 54 Mbps. Both 802.11b and 802.11g operate in the unlicensed frequency band of 2.4 GHz.

> Some laptops support the IEEE 802.11a wireless standard, which operates at a 5 GHz frequency band. The 802.11a devices are not compatible with 802.11b or 802.11g devices.

Cellular

Though many of the new mobile phones provide Internet access and other advanced features, the laptops are not behind the race. More and more laptop manufacturers are adding cellular communications support in their products. Besides the regular phone services, the ISP in this case provides its subscribers with complete Internet connectivity solutions.

Docking station

A docking station is a platform where a laptop can be installed for everyday use. Once inserted into a docking station, a laptop works just like a desktop computer. The docking port contains expansion ports, drive bays for storage devices, and connectors for peripherals. You can use a desktop monitor, a full-sized keyboard, and a mouse, besides other peripherals, just as you would use them with a normal desktop. Most laptops have a proprietary *docking port*, which is used to connect the laptop to the docking station.

A *port replicator* does what its name suggests. It enables you to keep the external components such as the monitor, keyboard, and mouse, connected to the docking station while the laptop can be simply disconnected.

Power Management and Device Removal

Most new laptops conform to either Advanced Power Management (APM) or Advanced Configuration and Power Interface (ACPI) standards for managing how the system components use and conserve power. This is especially important for laptops when they are running on battery power. In this section, we will take a look at ACPI standards and then explain what power management features are available in Windows operating systems. This section also covers a summary of how you can safely remove laptop-specific components.

Overview of ACPI standards

The ACPI standard describes how the power management features are to be implemented in desktops and laptops. For a computer to be ACPI-compliant, both the hardware and the operating system must support the ACPI standards. Let us first have a look at how the ACPI standards define various states of computer components:

Global states

The G0 state specifies the normal working state of the computer. This state describes that all devices and applications are running normally. The G1 state describes the power-saving or sleep mode. G1 is further divided into four states named S1, S2, S3, and S4, described here:

S1

The most power-hungry sleep mode. Applications are stopped but only unrequired devices are turned off.

S2

This is a deeper sleep state than S1. The CPU is powered off and the computer uses less power than in S1 mode.

S3

This state is known as *standby* mode in Windows. The power is maintained only to the RAM. This state is also called *Suspend to RAM* because all information for applications is written to RAM before sending the computer to sleep mode.

S4

This state is known as *hibernate* mode in Windows and as *Safe Sleep* in Mac OS. The information in the RAM is written to the hard disk, and the RAM is powered off. The user can bring the computer back to G0 state, but it takes a little time.

G2

This describes the *soft off* mode, in which the computer can be turned off by using the Shut Down or Turn Off button in Windows.

G3

This is called the *mechanical off*, where the power is switched off using the power switch.

Processor states

Processor states are defined in terms from C0 to C3. *C0* is the normal operational mode, *C1* is the halt mode when the processor can instantaneously come back to action, *C2* is the stop-clock mode that uses less power than the C1 mode, and *C3* is the sleep mode when the processor clears its cache.

Device states

The device states are defined from in terms from D0 to D3 and are device-dependent. *D0* is the Fully On state when the device is in operating state. *D3* is the Off state, and the *D1* and *D2* states depend on specific devices.

Performance states

The performance state depends on whether the device is operating (in C0 or D0 state) or is in sleep mode. These states are dependent on how they are implemented and are designated from P0 to Pn, where *n* can be any number between 1 and 16. The bigger the number *n*, the more power is saved.

Power options in Windows

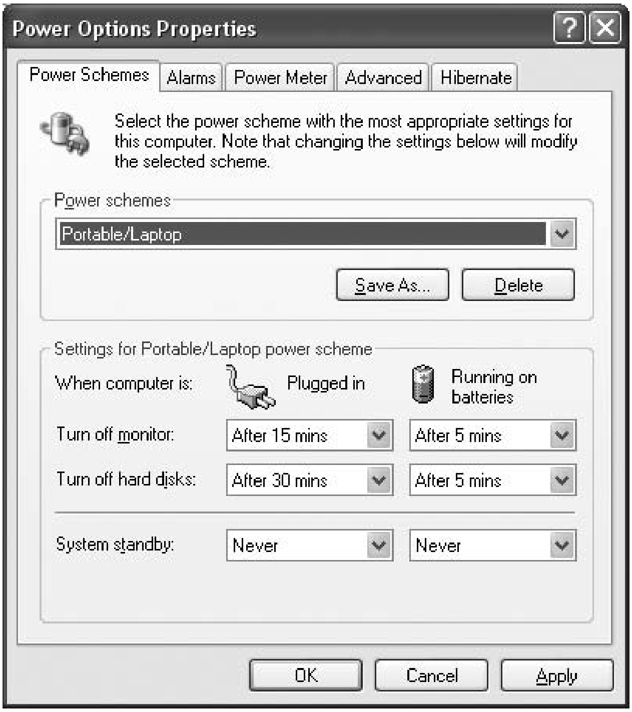
Power management features in Windows XP and Windows 2000 operating systems help you manage the amount of power consumed by different parts of the system. This utility is very useful for laptop computers, which are frequently operated on battery power. Windows OS also supports APM and ACPI standards. But before you can utilize any of the power options, you must make sure that your computer hardware—including the system BIOS—supports these features.

The Power Options utility in the Control Panel allows you to configure different power schemes to turn the monitor and the hard disk on or off after a specified idle time has lapsed. You can also put the system in standby mode, configure hibernate options, and configure the UPS settings.

There are two ways to access the Power Options in Windows:

- Open Control Panel from the Start menu and click Power Options.
- Right-click an empty area on the desktop and click Properties. Click the Screen Saver tab and then click the Power button (the Power Meter and Alarms tabs are not available with this option, but a UPS tab is added).

The Power Options window is shown in Figure 2-5.



Select the power scheme with the most appropriate settings for this computer. Note that changing the settings below will modify the selected scheme.

Power schemes: Portable/Laptop

Settings for Portable/Laptop power scheme

When computer is:	Plugged in	Running on batteries
Turn off monitor:	After 15 mins	After 5 mins
Turn off hard disks:	After 30 mins	After 5 mins
System standby:	Never	Never

Figure 2-5. Configuring Power Options in Windows

Various tabs in this window allow you to configure power settings as follows:

Power schemes
The Power Options page allows you to select from one of the preconfigured power-saving schemes. You can choose the Portable/Laptop option and configure the monitor and hard disk to turn off timings for both AC power and battery power. Additionally, you can configure the time to lapse before the laptop goes into standby or hibernate mode.

Alarms
The Alarms page allows you to configure how the system will respond when the battery power becomes very low.

Power Meter
The Power Meter page shows the current status of the battery and remaining battery life. Alternatively, you can click the battery icon on the Taskbar to check the battery's status when the laptop is running on it.

Advanced
The Advanced page allows you to configure a password when the laptop returns from standby mode, and then choose whether the computer will go into hibernate mode or standby mode when the lid is closed. You can also configure the function of power and sleep buttons on the laptop.

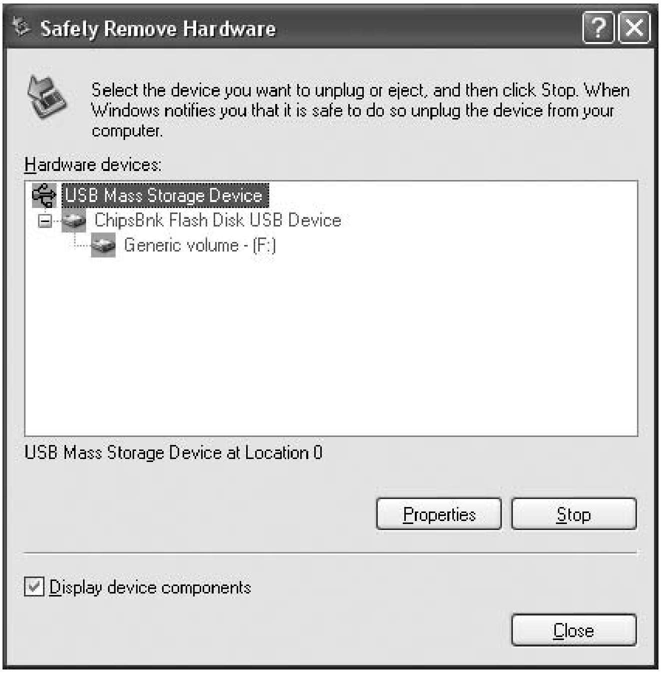
Hibernate
The Hibernate page is used to enable or disable the hibernation on the laptop. You must have free hard disk space, which should be at least equal to the amount of RAM in your laptop.

Removing laptop-specific hardware

Laptop hardware is mainly classified into external and internal. External devices are easier to connect or disconnect than internal devices. Most of the external devices connected to a laptop are USB-compatible. You will need to make sure that the device is not in use when you are preparing to remove it. Windows provides an icon in the Taskbar to help you safely remove USB devices. This icon can be used to stop the device and then unplug it safely while the laptop is powered on.

To remove an external USB device such as thumb drive or a mouse, click the Safely Remove Hardware icon on the Taskbar. As shown in Figure 2-6, a window pops up that shows different devices connected to the laptop. Select the device that you want to remove and click the Stop button. Windows will stop the device and show a message that it is safe to remove the device. At this point, you can unplug or disconnect the device.

In case of a PCMCIA device, the process is as simple as removing the device by using the eject button provided next to the slot. Removing or replacing internal devices such as a CD or DVD drive requires first stopping the device, as mentioned earlier. Then turn over the laptop to access the latches or locks that hold it. You might also have to disconnect the cables before removing the device.



Safely Remove Hardware

Select the device you want to unplug or eject, and then click Stop. When Windows notifies you that it is safe to do so unplug the device from your computer.

Hardware devices:

- USB Mass Storage Device
  - ChipsBnk Flash Disk USB Device
    - Generic volume - (F:)

USB Mass Storage Device at Location 0

☑ Display device components

Figure 2-6. Safely removing hardware

Troubleshooting Laptops

There may be several reasons for a laptop computer problem. The battery or an internal component or an external peripheral, such as the data entry keypad, may have caused the problem. A loose network connection or a distant access point will generally cause connectivity problems, whereas problems with power supply components will cause the laptop or a mobile device to shut down unexpectedly. In this section, we will look at some common problems and appropriate solutions to fix them.

Power problems

Most laptops suffer from power problems that may be due to the main AC power adapter or to the built-in battery. When trying to fix power-related problems, make sure that the mains AC supply is properly connected. The following simple steps will help you verify the AC input power.

1. Verify that the mains power cord is properly attached to the adapter. If it has become loose or does not attach properly to the adapter, try replacing it.
2. Check the small LED on top of the adapter. If it is not glowing, the AC power may not be connected or may be turned off.

3. Touch the AC adapter surface. A reasonably warm surface is usually an indication of a working adapter. If the power adapter seems to be overheated, it may have to be replaced.
4. Verify that the DC power cord is not damaged and that the connector is properly inserted into the laptop.
5. Remove the DC power cord and verify the DC power output of the adapter.
6. If there is no output or a very low DC output, the AC is properly connected, and the LED is lit, try replacing the adapter with a new one.

Input problems

If you are having troubles with the laptop keyboard, try connecting an external keyboard to a USB port using a PS/2-to-USB converter. You will notice that function keys in laptops are different on a laptop keyboard than on a desktop. If one of the function keys is stuck, only those functions will work that the key is used for. Try toggling the function key to solve the problem. In some situations, the pointer does not move as expected due to problems with the touchpad. You can try connecting an external mouse and turn off the touch pad in the Control Panel to identify the cause of the problem.

Most stylus problems are caused due to rough handling. Some problems directly relate to the alignment of the stylus pen. A soft or hard reset sometimes helps resolve this problem or a built-in utility can be used for the purpose. You may also use some freely available software on the Internet to get around the alignment problem.

Display problems

The laptop display unit is made up of an LCD screen, the video controller card, and the inverter unit that supplies backlight for the LCD screen. A cut-off switch ensures that the backlight is switched off when the lid is closed. If you have problems with the LCD display, connecting an external monitor can quickly determine whether the problem lies with the LCD display or the video controller card. You will need to toggle the display using a function key. You can also try to increase or decrease the brightness level to determine the problem. Check that the cut-off switch is not damaged.

Networking problems

Most new laptops have built-in wired adapters as well as wireless adapters. There can be more than one reason for a connectivity problem, and the correct solution can be applied only after you have isolated the problem and determined the exact reason behind the problem. If you are having troubles connecting to a wired network, check that the network cable is properly attached and is not loose. Also check the status LEDs on the network adapter.

If you are having troubles connecting to a wireless network, make sure that the wireless connection is enabled in Windows, that you are using a correct SSID setting, and that the laptop is within the coverage area of an access point. You will not see a wireless antenna in most new laptops, but it might be required on some older laptops that use a PCMCIA wireless adapter. Antenna wires are very helpful in troubleshooting connectivity problems when a laptop is placed far away from the wireless access point.

You can also try to use the Repair utility in Windows to reconfigure the TCP/IP protocol settings. Right-click the Local Area Connection icon in the Taskbar and select Status. Click the Support tab in the Local Area Connection Status window. Click the Repair button to refresh the TCP/IP connection settings.

Problems with external devices

Many problems with laptops can be resolved simply by removing unneeded external peripherals. For example, if you do not need an external USB modem or a hard drive permanently connected to the laptop, you should remove it. Depending on the type of the connected device, you might have to uninstall the driver of the device, power off the laptop, remove the device physically, and then power on the laptop again.

Preventive Maintenance (PM)

PM helps prevent many problems with laptops and enhances their performance and life span. Since laptops are portable devices, they need to be cared for more than desktops. In this section, we will look at some preventive maintenance measures for laptops.

Operating environment

Keeping the operating environment healthy for the laptop is the first and most important preventive maintenance method to keep problems away. The main environmental factors that affect the performance of a laptop are as follows:

- Temperature
- Humidity
- Cleanliness

Ensuring a healthy environment helps prevent several operational problems in laptops. Laptops are compact devices that use very small components, which produce heat during normal operation. You must ensure that the laptop is not operated in areas with high temperatures and that sufficient cooling is available.

An air-conditioned room is perfect because both temperature and humidity are controlled. Do not operate a laptop for long periods if proper air-conditioning is not available or if the conditions are very hot. If you regularly operate the laptop in areas of high temperature, you can install an external *cooling pad*. A cooling pad lifts the laptop above the table about one inch and has extra fans for cooling the bottom of the laptop.

Make sure that the area where a laptop is operated is clean and dust-free. Regularly check that the cooling/exhaust fans are working and that dust has not accumulated around ventilation slots. Clean the LCD screen regularly with a damp soft cloth. Do not use glass-cleaning sprays on LCD screens.

Handling

Since laptops are portable devices, they need to be handled with care when carrying them from one place to another. Always carry them in their protective bags, which should have sufficient cushioning to prevent damage during travel. Keep the laptop lid closed when the laptop is not in use. Use a piece of foam between the LCD screen and the keyboard for protection.

Operating Systems

Computer hardware, such as the motherboard, CPU, adapter cards, display devices, and I/O devices, are only a part of the entire computer system. To make this hardware work, we need software that acts as an interface between human beings and the hardware. Software can be classified into three major categories as follows:

Operating systems
: The operating system interacts directly with the computer hardware and provides a platform for applications and device drivers. It manages computer memory, input, output, disks, and filesystems.

Device drivers
: Device drivers act as an interface between the operating system and the specific devices for which the driver software is written.

Applications
: An application is the software program that takes commands from the user for a specific task, executes them, and produces the results.

The operating system is the primary software that makes the computer hardware usable. In this section, we will discuss some of the fundamentals of using operating systems, their installation and upgrade methods, troubleshooting techniques, and preventive maintenance procedures.

Overview of Operating Systems

Once we start discussing various operating systems, we certainly need to know about their revision levels. In this section, we will cover some basics of Microsoft Windows, Apple MAC, and Linux.

Windows

Microsoft Windows is no doubt the largest used operating system to date. This operating system evolved from *Microsoft Disk Operating System (MS-DOS)*, which had a command-line interface. In contrast to the MS-DOS operating systems, Windows uses a *Graphical User Interface (GUI)*. Windows has gone through various revisions since its introduction. A summary of Windows versions is given in the following sections.

Windows 1. Windows 1 was the graphical version of Microsoft's DOS operating system with added support for mouse, menus, and tiling windows. It supported running multiple applications simultaneously, a feature known as *co-operative multitasking*. This version of Windows did not have the icons that we see and use in modern versions of Windows.

Windows 2. This version of Windows included support for *Program Information Files (PIFs)* and had icons to launch applications.

Windows 3.x. The main attraction of Windows 3.0 was the operating system's ability to effectively manage memory. When used in enhanced mode, the OS could use a part of hard disk space for supplementing memory. This feature is still used in modern Windows versions and is known as *virtual memory* or *paging file*. This version had support for networking Windows and included additional features such as the Program Manager and the File Manager.

Windows 3.1. Windows 3.1 supported multimedia devices, had an improved GUI, and included error protection for system and applications through *Object Linking and Embedding (OLE)*.

Windows 3.11. Windows could support only 16-bit applications until version 3.11. Windows 3.11, also known as Windows for Workgroups, added support for both 16-bit and 32-bit applications.

Windows 95. As is evident from the name, this version of Windows was released in 1995. It supported both 16- and 32-bit applications, and had the ability to network computers. The major advancement in this version was the support for Plug and Play (PnP) devices. For the PnP feature to work properly, the system motherboard (and the BIOS), the OS, and the device, all had to be PnP-compatible. Once all three conditions were met, the PnP devices could be automatically detected and configured by the OS. At the time of this writing, most devices, operating systems and applications still support the PnP functionality.

Windows 98, Windows ME, and Windows NT. Windows 98 was released in 1998, followed by Windows ME (Millennium Edition), and Windows NT (New Technology). Windows NT was a major upgrade for the Windows platform and was much more powerful than Windows 98 and Windows ME. Windows NT Workstation and Windows NT Server had versions named Windows NT 3.5x and Windows NT 4.0.

Windows 2000. Windows 2000 Professional and Windows Server 2000 operating systems were released in the year 2000. These operating systems were meant as desktop (client) and server operating systems respectively. With Windows NT, Microsoft introduced the concept of *domains*, which are meant to effectively manage users, computers, resources, and security in the network.

Windows XP. Windows XP followed after the release of Windows 2000. This operating system is mainly used as a standalone OS for home computers or as an alternative to Windows 2000 Professional as a client operating system in a networked environment. Most of the discussion in this section is related to Windows 2000 Professional and Windows XP operating systems.

Windows XP has different versions, each addressing the needs of specific applications, as follows:

Windows XP Professional
This is designed as a client operating system in networked environments.

Windows XP Home
This is designed for standalone home computers.

Windows XP Media Center
This is designed to be used in situations where multimedia capabilities are more important than other features.

> Two other editions of the Windows XP family are: Windows Tablet PC and Professional X64.

Windows Server 2003. The most current server operating system in use today is Windows Server 2003. This includes several enhancements to earlier server operating systems such as Windows NT Server 4.0 and Windows 2000 Server. This OS is basically designed to overcome many drawbacks of previous server versions of Windows and to compete with its peer operating systems such as Unix, MAC OS, NetWare, and Linux. Different editions of Windows Server are as follows:

- Web Edition
- Standard Edition
- Enterprise Edition
- Datacenter Edition

Windows Small Business Server 2003 is also a popular network operating system targeted for small businesses. Windows Server 2003 has a new version named *Windows Server 2003 R2*.There is a long list of features supported in Windows Server 2003, some of which are as follows:

- It supports both 32- and 64-bit microprocessors.
- It supports large amounts of physical memory (RAM) and efficiently manages it.
- It supports centralized management for applications, users, data storage, and security through a centralized database called *Active Directory*.
- It has strong support for client/server-based applications and services such as SQL Server, Internet Information Server (IIS), Terminal Server, Domain Name System (DNS) server, and Dynamic Host Configuration Protocol (DHCP) server.
- It supports server clusters for providing fault tolerance and network load-balancing for improved performance.

Windows Vista. Windows Vista is the latest desktop operating system. This OS is meant to replace Windows XP. The list that follows describes different editions of Windows Vista.

- Home Basic
- Home Premium
- Business Edition
- Ultimate
- Enterprise Edition

One of the most attractive features of Windows Vista is Windows Aero, which is a 3-D graphical interface. Windows Vista also includes Internet Explorer 7 (the new version of Microsoft's web browser application), and it supports speech and handwriting recognition. This OS will be more secure than Windows XP and Widows 2000 Professional.

MAC OS X

The MAC OS X is used primarily on Apple Macintosh computers. Apple has recently released the Intel version of MAC OS X that can be installed in place of Windows on Intel-based personal computers. The MAC OS has a GUI that looks similar to Windows and is called *Aqua*. The most current version of this OS is the MAC OS X. Mac OS X is considered a much more secure OS than Windows.

The applications that run on Apple computers running the MAC OS need to be written specifically for the MAC OS platform. This is due to the fact that the technology behind microprocessors used in Apple computers is entirely different from the technology used in Intel microprocessors. Apple computers use PowerPC microprocessors.

Linux

Linux has become an extremely popular operating system in the recent years. This OS has Unix-like functionality, which is mainly used on high-end servers and mainframe computers. It is extremely stable and reliable and provides several advantages over Microsoft's Windows operating systems. Different variations of Linux are available as of this writing. Some of the main variations of Linux OS are as follows:

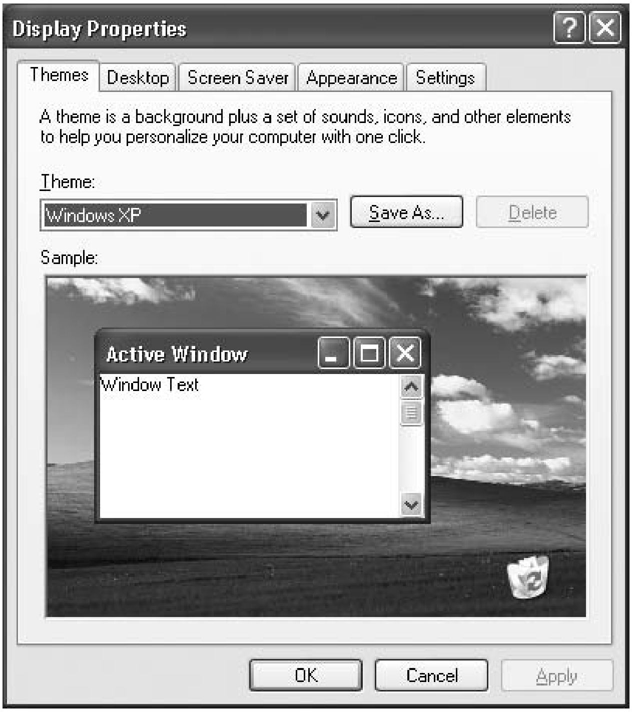
- Red Hat
- Mandrake
- SuSe
- Debian

Linux OS does not require hardware as powerful as most new versions of Windows. The hardware requirements for each variation of Linux OS are different, depending on the particular distribution you are using or intend to use. There is no standard graphical user interface for Linux. Also, if an organization plans to use Linux OS as the primary operating system in the organization, it must either develop software applications in-house or obtain applications that are specifically written for Linux.

Working with Windows interfaces

Microsoft Windows includes several GUIs that are used to manage the operating systems and run applications. For most of the versions of Windows, such as Windows Me, Windows NT, and Windows 2000, these GUIs look similar, but the functionality of each is a little different when you start using them. This section provides a brief discussion of some of the main interfaces.

Windows desktop. The Windows desktop is the screen that appears as soon as you start Windows and successfully log on. This is the place where you find most of the icons (shortcuts) for most of the system utilities and application programs. It includes the Start menu, the Taskbar, and other icons placed as shortcuts to application programs. You can change the way your desktop looks by right-clicking an empty area on the desktop and selecting one of the choices from the context menu. You can rearrange the icons or change the display settings by selecting Properties. As shown in Figure 2-7, the Display Properties pages allow you to configure its settings.



A theme is a background plus a set of sounds, icons, and other elements to help you personalize your computer with one click.

Theme: Windows XP

Figure 2-7. Configuring Display Properties

Table 2-4 lists the main Desktop configuration pages available in the Display Properties pages.

Table 2-4. Display properties

Display Properties page	Function
Themes (Windows XP only)	From this page, you can select a theme to quickly customize the look and feel of Windows, including display picture, sounds, icons, etc.
Desktop	This page allows you to choose a background color and picture for the desktop. You can also cleanup the unused icons from the desktop.
Screen Saver	Change the screensaver settings and choose a screensaver program. By default, the screensaver starts when the computer is not in use for 10 minutes. Screen savers are used to enhance monitor life.
Appearance	This page several settings to configure different windows, color schemes, button styles, and font sizes. The Effects button configures settings such as transition effects, large icons, shadows under menus, displaying window items while dragging, etc.
Settings	The settings tab includes configuration options such as screen resolution and color quality. This tab also includes a troubleshooting button as well as a button for advanced setting options for each display adapter.
Effects (Windows 2000)	This page contains several options to change the visual look of the desktop.
Web (Windows 2000)	You can configure the Active Desktop settings from this page. Same as the Customize My Desktop option in Windows XP.

Taskbar. The bottommost part on the Windows desktop is known as the Taskbar. It contains the Start menu and the System Tray (systray). The System Tray includes the Quick Launch area on the lefthand side and the Notification Area on the righthand side. The Start menu is used to run programs as well as to configure system settings. In the middle of the Taskbar, Windows displays buttons for programs that are currently running. When you right-click an empty area on the Taskbar, a menu appears from where you can configure the following settings:

- Change the Properties of the Start Menu and the Taskbar
- Launch the Task Manager utility
- Automatically hide the Taskbar when not in use
- Cascade Windows or tile them horizontally or vertically
- Lock the Taskbar at its position

Start menu. When you click the Start button located on the lefthand bottom corner of the Windows screen, the Start menu appears, which displays the name of the user who is currently logged on to the computer. The Start menu includes shortcuts to installed programs, the Control Panel, a Settings button, and folders such as My Documents, My Recent Documents, My Pictures, My Music, My Computer, My Network Places, and so on. The appearance of the Start menu can be changed to classic style from the Start menu tab of the Taskbar Properties. Some of the common menu items are listed in the following paragraphs:

Shut Down

Depending on whether you are using Windows 2000 or Windows XP, the Shut Down button gives several options, such as log off the current user, switch user, shut down the computer, activate the Standby mode, or restart the computer.

Programs/All Programs

Installed application programs can be launched from the Programs/All Program icon on the Start menu. When you see an arrow pointing towards the righthand side, this means that the selected menu contains submenus.

Help (Windows 2000)/Help and Support (Windows XP)

The Help window is displayed in Windows 2000 when you select the Help option in the Start menu. In Windows XP, the Help and Support shortcut in the Start menu launches the Help and Support Center which is very helpful for getting help with using, configuring, and troubleshooting the operating system. The Help and Support center in Windows XP also includes online help options from Microsoft support. You can also use the Remote Assistant to get help from an expert when connected to the network.

Search

The Search option opens a search window where you can find files or folders stored on the hard disk.

Run

The Run option opens the Run dialog box where you can enter a command or the name of an executable file to launch the program. You must use the correct path of the executable file when using the Run option.

Desktop icons. Some standard icons are available on both Windows 2000 and Windows XP. Some of the icons have been removed from the desktop in Windows XP and placed inside the Start menu. The following is a summary of these icons:

My Computer

The My Computer icon is used to explore the computer (including the disk drives) and view their contents. These drives include floppy drives, hard disk drives and their partitions, and CD and DVD drives. You can double-click any drive to view its contents. You can configure your computer by right-clicking this icon and selecting Manage from the context menu. The Manage option opens the Computer Management console.

My Network Places (Windows XP)/Network Neighborhood (Windows 2000)

This icon is used to browse the Windows network. You can view or connect to any computer on the network where you have appropriate permissions. In Windows XP, the My Network Places icon is available in the Start menu. The Properties pages allow you to configure your network, wireless, or dial-up connections.

Recycle Bin

The purpose of the Recycle Bin is to collect all files or folders that you delete from the computer. It is actually a separate folder on the hard disk that stores the deleted objects. The main advantage of the Recycle Bin is that you can restore a file or folder that you might have accidentally deleted. When you no longer need a deleted file or are running out of disk space, you can right-click the Recycle Bin icon and select the Empty Recycle Bin option to permanently delete the objects.

The Windows operating system is made up of several components, including the Windows Registry, Control Panel, Virtual memory, and File Systems. The following sections explain the purpose and characteristics of these components.

Control Panel

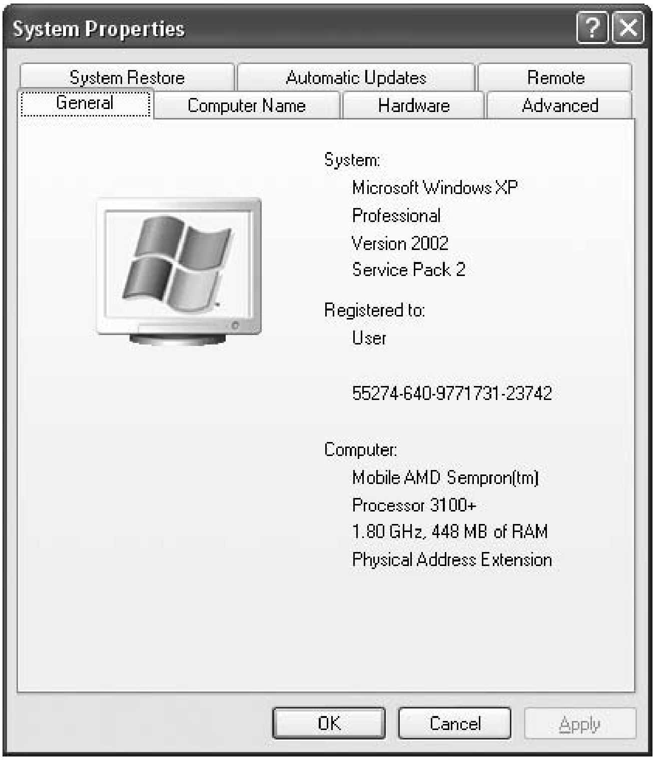
The Control Panel in Windows is the utility that you can use for most of the configuration tasks related to the operating system itself as well as to the devices and drives. To access it, click Start and select Control Panel. In Windows XP, you will first see a list of categories, while in Windows 2000, you will go directly to the Control Panel folder. The Control Panel further contains icons for various utilities. Table 2-5 lists some of the common utilities available in the Control Panel.

Table 2-5. Control Panel utilities

Utility	Function
Add Hardware or Add/Remove Hardware	Used to add and configure hardware.
Add or Remove Programs or Add/Remove Programs	Used to install or uninstall application software.
Administrative Tools	Used to perform administrative tasks on the computer.
Date/Time or Date And Time	Used to change system date and time and sets the time zone.
Display	Used to change display settings.
Folder Options	Used to configure folder settings. You can change how folders are displayed and whether or not to display hidden and/or system files.
Fonts	Used to add or remove fonts.
Internet Options	Used to configure Internet connections and security settings.
Keyboard	Used to configure keyboard settings.
Mouse	Used to configure mouse settings.
Sound and Audio Devices or Multimedia or Scanners and Cameras	Used to configure audio, video, and sound settings.
Network And Dial-up Connections or Network Connections	Used to configure networking options such as protocols, clients, and services.
Phone and Modem Options or Modems	Used to configure phone and modem settings.
Power Options	Used to configure power options such as power schemes and UPS settings.
Printers and Faxes	Used to add, remove, and configure printers and fax machines.
System	Used to configure system settings.
Windows Firewall (Windows XP with SP2)	Used to configure Windows Firewall in Windows XP, which is added when Service Pack 2 is installed.

The System Control Panel

The *System* utility in the Control Panel is used to configure most of the system settings such as computer name/identification, virtual memory, startup and recovery options, remote desktop/remote assistance, hardware devices, user profiles, and network options. Different tabs included in the System Properties page are General, Computer Name/Network Identification, Hardware, Advanced, System Restore (XP), Remote (XP), Automatic Updates, etc. Figure 2-8 shows the System Properties window in the Control Panel utility.



System:
Microsoft Windows XP
Professional
Version 2002
Service Pack 2

Registered to:
User

55274-640-9771731-23742

Computer:
Mobile AMD Sempron(tm)
Processor 3100+
1.80 GHz, 448 MB of RAM
Physical Address Extension

Figure 2-8. System Properties in Control Panel

The General tab displays information about the computer, installed operating system, system memory, and registration information. The configuration options in other tabs are summarized in the following discussion.

Computer Name (Windows XP)/Network Identification (Windows 2000)
This tab allows you to change the name of the computer and whether the computer is a part of a workgroup or an Active Directory domain.

Hardware
This page includes several tools to manage hardware devices and drivers installed on the system. The Device Manager button opens the Device Manager snap-in where you can view and manage all hardware devices. The Driver Signing option allows you to configure system behavior when unsigned device drivers are installed. The Hardware Profiles button allows you to enable/disable devices for specific hardware profiles. You can add, delete, copy, or change user profiles. In Windows XP, the User Profiles button is available in the Advanced tab.

Advanced

This tab includes buttons to fine-tune system performance, system startup, and recovery options and environment variables. The Settings button in the Performance section provides options to configure virtual memory settings. The Settings button in the User Profiles section (Windows XP) provides options to add, delete, copy, or change user profiles. The Settings button in the Startup and Recovery section provides options to configure system startup and recovery options. You can change the default operating system to load for a multiboot system. You can also edit the *BOOT.INI* file.

System Restore (Windows XP)

This utility is new to Windows XP and can be used to configure system restore points that are used to restore the operating system to a working condition in case it becomes unstable.

Remote (Windows XP)

This tab includes buttons to enable or disable Remote Desktop and Remote Assistance. You can select users that will be allowed to make remote connections with the computer. These features are not available in Windows 2000 Professional.

Automatic Updates (Windows XP)

This tab is used to enable or disable Automatic Updates for the operating system. You can choose how the updates are downloaded and whether they are installed automatically or require user action.

Windows Registry

Windows Registry is a collection of system configuration settings stored in a hierarchical data file. This data includes the operating system settings, user specific settings, application data, hardware components, and installed device drivers. The hierarchy is organized into keys and subkeys, each of which can have one or more values. The value can be a text identifier, string, binary, word, a multiple string, or an expandable string. There are five main subtrees in the Registry hierarchy and are as follows:

HKEY_CLASSES_ROOT

This subtree mainly stores Object Linking and Embedding (OLE) data and file associations. File associations link files to the programs used to run them.

HKEY_CURRENT_USER

This subtree contains data about the currently logged-on user that is taken from her user profile.

HKEY_LOCAL_MACHINE

This subtree contains all the hardware-specific configuration data for the machine that essentially includes OS and hardware configuration.

HKEY_USERS

This subtree contains a default set of settings as well as data for each user profile.

HKEY_CURRENT_CONFIG

This subtree contains data about the currently loaded hardware profile.

Registry Editor. Under extreme circumstances, if you require changes to the Registry, you should first make a backup copy of the existing Registry files. The Registry Editor (*REGEDIT.EXE or REGEDT32.EXE)* program is located in the *%SystemRoot%\System* folder. It can either be run from the command prompt or from the Run option in the Start menu.

> With most of the systems settings and configurations made easy using the Windows Wizards, you will hardly need to edit the Registry directly. Unless you do not have another way to configure your system, you should not edit the Registry to change any configuration values. Improperly editing the Registry may render your system unable to boot or generate unexpected errors.

You must have advanced level knowledge of the Windows OS and Registry keys in order to configure the registry correctly. If you are unsure of your actions, do not attempt to edit the Registry. Otherwise, you may damage the operating system and may have to reinstall it.

Virtual memory

Virtual memory is a part of the hard disk that the operating system uses as temporary storage. This memory is also known as *swap file* or *paging file*. Windows treats this hard disk space as RAM and uses it as and when the system runs out of RAM. The operating system automatically configures the size of the paging file during installation.

Windows system files

Several files are critical for the Windows 2000 or Windows XP operating system to start successfully. By default, all of these files are marked as system files and are hidden. You will need to change folder options to view these files. These files are protected so that a user won't delete them accidentally. While some of these files are stored in the root of the system partition, others are located in the System32 subfolder in the drive where you installed the operating system. The most important of all system startup files are listed in Table 2-6.

Table 2-6. Windows system startup files

Filename	Function
NTLDR	This file starts loading the operating system.
BOOT.INI	This file contains information as to which operating system is to be loaded and from which disk partition.
BOOTSECT.DOS	This file is used in dual-boot systems and contains a copy of MS-DOS or Windows 9x OS.
NTDETECT.SYS	This file is used to detect the hardware installed on the system and also loads the hardware profile.
NTBOOTDD.SYS	This file is used to detect and load the SCSI interface.
NTOSKRNL.EXE	This file loads the Windows operating system kernel.
HAL.DLL	The hardware abstraction layer file.

Managing disks

Hard disks are the primary data storage devices used in computers. Hard disks are treated as fixed storage devices and are connected to IDE or SCSI interfaces. USB disks, CD-ROMS, and DVDs are called removable storage media. Windows OS supports two types of hard disks for data storage: Basic disks and Dynamic disks.

Basic disks. Basic disks are the traditional type of disks used in computer systems. Windows OS treats all disks as Basic unless they are converted to Dynamic using the Disk Management utility. The disks are divided into one or more *partitions*, each of which can be a logical storage unit accessible by a drive letter. Windows XP Professional stores partition information in a partition table that is not a part of the operating system and can be accessed from any operating system besides Windows. Partitions in Basic disks can be Primary or Extended.

Primary Partition
: Each Basic disk can have up to four primary partitions, or three primary and one extended partition. One of the primary partitions is marked as the *Active Partition* and is used to boot the system. There can be only one active partition on a computer. The primary partition is formatted using one of the file systems: FAT, FAT32, or NTFS.

Extended Partition
: An Extended Partition is created on unallocated space on the hard disk. You then create logical drives on this partition and assign them drive letters. Extended Partitions cannot be formatted with any filesystem, and they cannot be assigned drive letters.

Logical Partition
: Logical Partitions are created inside the Extended Partitions. Logical drives cannot be marked as active and cannot be used to boot the system. These partitions are used to organize files and folders on the hard disk.

Dynamic disks. Dynamic disks are the disks that are specifically converted from Basic disks using the Disk Management utility. Dynamic disks treat the entire disk as a single partition and you can create volumes on the disk to organize your files and folders. Dynamic volumes can be extended on single or multiple Dynamic disks and offer fault tolerance features. You can create the following types of volumes on Dynamic disks:

Simple volume
: A Simple volume contains space from all or part of a single Dynamic disk. They are similar to a partition on a Basic disk.

Spanned volume
: A Spanned volume contains space from a single or multiple Dynamic disks. You can add unallocated space from 2 to 32 Dynamic disks to create a large Spanned volume. Each disk can be of any size.

Striped volume

A Striped volume combines space from 2 to 32 Dynamic disks to make a single Dynamic volume. Data is stored on Spanned volumes in stripes (chunks of 64 KB) on each disk in turns so that each disk has an equal amount of disk space. Striped volumes cannot be extended and are not fault-tolerant. If one of the disks in a Striped volume fails, all data is lost.

Disk drives are managed using the Disk Management utility found within the Computer Management console. Right-click the My Computer icon and select Manage to open the Computer Management console. The Disk Management tool is located under the Storage folder.

Creating partitions. To create a partition, right-click a disk and click Create Partition. The New Partition Wizard guides you through the process of creating a primary, an extended, or a logical drive. Once you have created a partition, you can format it with FAT, FAT32, or NTFS filesystem. Right-click the partition and select Format. Existing volumes can also be formatted from Windows Explorer. This action destroys all data on the partition. The Format option also allows you to assign a volume label and drive letter to the partition.

Converting from Basic disk to Dynamic disk. To convert a Basic disk to Dynamic, you must have at least 1 MB of free space at the end of the disk, and the sector size must not be larger than 512 bytes. Right-click the disk and select Convert To Dynamic Disk. This action does not cause any loss of data.

> If the Convert To Dynamic option is not available for a particular disk, the disk is either already a Dynamic disk or you are trying to convert the disk on a portable computer. Remember that Dynamic disks are not supported on portable computers. This option is also not available on removable disks such as CD-ROMS, floppy drives, and Zip drives.

Converting from Dynamic disk to Basic disk. Converting a disk from Basic to Dynamic is a one-way process. Conversion from Dynamic disk back to a Basic disk destroys all data on the disk. You must first back up all the data on the disk before attempting to perform this conversion. To convert a disk back to Basic, right-click the disk in Disk Management and select Convert To Basic Disk.

Filesystems. Filesystems refer to the method operating systems use to manage disk partitions and data storage. Filesystems help the OS keep track of files and folders on the disk. You will need to decide on a filesystem when partitioning and formatting a disk. The following are the main filesystems used in Windows operating systems:

FAT

The File Allocation Table (FAT) was implemented in DOS operating systems. Its main characteristics include:

- Supports only 8-character filenames with a 3-character extension, known as 8.3 file format.

- No spaces are allowed in filenames.
- The maximum partition size is 2 GB in Windows 95, Windows 98, and Windows ME. In Windows NT 4.0, Windows 2000, and Windows XP, the maximum supported FAT partition size is 4 GB.

FAT32

FAT32 is an improved version of FAT and is supported in Windows 95 (OSR2) and later operating systems. Windows XP, Windows ME, and Windows 95 OSR2 also support the FAT32 filesystem. Main characteristics of FAT32 include:

- More reliable storage than FAT.
- Not compatible with FAT.
- Uses smaller disk cluster sizes to prevent wasting disk space.
- Support for long filenames of up to 255 characters.
- Extended disk partition size of up to 2 TB (Terabytes) or 2048 GB.

NTFS

NTFS is the preferred filesystem for Windows XP Professional, Windows Server 2003, Windows 2000, and Windows NT operating systems. Some of the benefits of using NTFS are as follows:

- It supports long file names of up to 255 characters.
- It supports disk sizes of up to 16 EB (Exabytes).
- It supports file- and folder-level security.
- NTFS Encrypting File System (EFS) secures files and folders from unauthorized access.
- It supports Disk Quotas to limit the use of disk space on a per-user basis.
- It supports files larger than 4 GB in size.
- It provides file compression to save disk space.
- It supports Dynamic disks to efficiently use and manage disks and partitions.

CDFS

CDFS stands for Compact Disk File System, which is used on compact disks (CDs).

UDF

UDF stands for Universal Disk Format, which is used on digital versatile disks (DVDs).

Managing files and folders

Files and folders are managed using Windows Explorer in both Windows XP and Windows 2000. The Windows Explorer utility is located in the Accessories folder in Programs/All Programs in the Start menu. The following tasks can be completed using this utility:

- Viewing and navigating files and folders.
- Copying and moving files and folders from one location to another.

- Creating new folders and subfolders.
- Deleting files or folders.
- Viewing or changing file or folder attributes.
- Executing (running) program files.
- Searching for a particular file or folder.
- Sharing folders and setting permissions.
- Formatting a disk.

A simple way to perform any of the given file or folder task is to right-click it and select the desired action such as copy, cut (and paste at another location), delete, rename, etc. You can select the Properties from the context menu to open the Properties window to view or change permissions, sharing, and file/folder attributes.

File extensions. Each file is associated with an extension. Windows operating systems use file associations to open files with specific extensions. Common file extensions are as follows:

.EXE
Executable files

.DLL
Dynamic link library files

.SYS
System files

.LOG
Log files

TXT
Text files

DOC
Document files

.HTM and .HTML
Web page files

.AVI, .MPG, .MP3
Audio video files

.BMP, .TIF, and .JPG
Picture files

File attributes. File and folder attributes determine the type of actions a user can perform on them. For example, if a file attribute is set as read-only, a user cannot delete the file or make changes to it. You can use the Properties page of a file or folder in Windows Explorer to view or change attributes. The types of attributes supported in Windows XP and Windows 2000 are described next.

Read-only

A file or folder with the Read-only attribute cannot be deleted or its contents cannot be changed.

Hidden

A file or folder with the Hidden attribute is not visible when navigating in the Windows Explorer. It cannot be deleted or copied.

System

A file or folder with the System attribute is used by the operating system. It is marked as both Hidden and Read-only.

When you click the Advanced button, the following attributes can be viewed or changed:

Archiving

The file or folder has been changed after the last backup. The Windows Backup utility uses this archive to select files and folders for backing up data.

Indexing

A file or folder marked with the Index attribute is used by Windows Indexing Service for a faster search. This attribute is available on NTFS volumes only.

Compression

The Compression attribute is used for compressed files and folders to save disk space. This attribute is available on NTFS volumes only.

Encryption

The Encryption attribute is used to store files and folders in encrypted format for security purposes. This attribute is available on NTFS volumes only.

> In both Windows XP and Windows 2000, encryption and compression are mutually exclusive. This means that an encrypted file cannot be compressed and a compressed file cannot be encrypted.

The following exercise explains the procedure to view or change attributes:

1. Open Windows Explorer and navigate to the file or folder.
2. Right-click and select Properties.
3. Examine the file/folder attributes in the Attributes area.
4. Click the checkbox for the Read-only, Hidden, or System attribute, as required. Click OK.
5. Click the Advanced button if you want to change the Archiving, Indexing, Compression, or Encryption attributes.
6. Click the appropriate checkbox and click OK.
7. Click OK or the Apply button.
8. If you are changing the attributes of a folder, a dialog box prompts you to select whether you want to change the attributes of the selected folder only or all subfolders and files under the folder.
9. Make your selection and click OK.
10. Close Windows Explorer.

File permissions. File permissions are used to control access to files. Permissions determine which users are allowed to access files. Windows XP and Windows 2000 support two types of permissions: NTFS file permissions and share permissions. The share permissions can be configured on NTFS as well as FAT volumes, while the NTFS permissions are supported only on disk partitions formatted with NTFS filesystem. File and folder permissions can be assigned to individual users as well as user groups. The following is a list of standard NTFS permissions:

Full Control
: The Full Control permission grants the user all rights on the resource.

Modify
: The Modify permission allows a user to change the contents of the file.

Read and Execute
: The Read and Execute permission allows a user to read the file and execute (run) it.

List Folder Contents
: The List Folder Contents permission allows the user to list the files and subfolders inside a folder.

Read
: The Read permission allows a user to read a file.

Write
: The Write permission allows a user to write files to a folder.

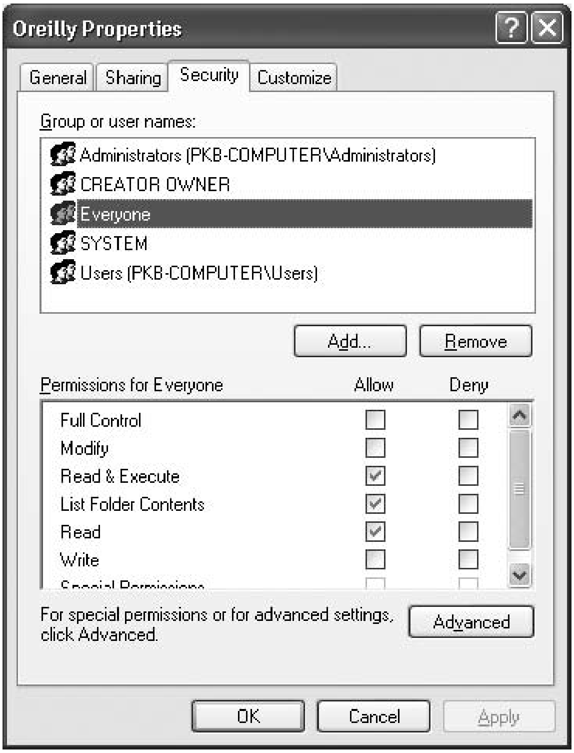
> When both NTFS and share permissions are assigned for a user or for a group, the more restrictive of the two becomes effective.

To assign share permissions on a folder, open Windows Explorer and navigate to the folder. Right-click the folder and select the Sharing and Security option. This opens the Sharing tab of the folder properties. You can share the folder and click the Permissions button to assign share permissions.

To assign NTFS permissions, open Windows Explorer and navigate to the file or folder. Right-click it and select the Sharing and Security option. Click the Security tab, which opens the NTFS permissions page as shown in Figure 2-9. Click the Add button to select a user or a group. Select the user or group in the upper Group or user names box. Click the appropriate checkbox in the Permissions box to assign the desired permission.

Installing and Configuring Operating Systems

Computers are useless without the operating system or software applications. As a PC technician, you must have good hands-on knowledge of installing operating systems. Since Windows XP and Windows 2000 are the most widely used operating systems, the A+ exams mainly cover these two operating systems. In this section, we will take a look at a variety of tasks involved in installing and configuring the Windows operating system.



Group or user names:

- Administrators (PKB-COMPUTER\Administrators)
- CREATOR OWNER
- Everyone
- SYSTEM
- Users (PKB-COMPUTER\Users)

Permissions for Everyone	Allow	Deny
Full Control	□	□
Modify	□	□
Read & Execute	☑	□
List Folder Contents	☑	□
Read	☑	□
Write	□	□
Special Permissions	□	□

For special permissions or for advanced settings, click Advanced.

Figure 2-9. Assigning NTFS permissions

Installing the operating system

Before you start installing the operating system or upgrading an existing one, you will be required to make some preparations that include checking the minimum hardware requirements, verifying compatibility of components, deciding on disk partitions, selecting the filesystem, and determining whether the computer will join a workgroup or a domain. Next, you will decide on an installation method, which can be CD-based or from the network, and whether the installation will be attended or unattended. In this section, we will take a look at various installation and upgrade scenarios.

Minimum hardware requirements. Before starting the actual installation process, you will need to ensure that your computer meets the minimum hardware requirements. Although many new computers will surpass these requirements, older computers will need to be checked against these minimum requirements. The minimum hardware requirements for Intel-based computers are shown in Table 2-7.

Table 2-7. Minimum and recommended hardware requirements for Windows XP and Windows 2000 Professional

Hardware Component	Windows XP Professional	Recommended for Windows XP Professional	Windows 2000 Professional	Recommended for Windows 2000 Professional
Processor	Pentium 233 MHz	Pentium II 350 MHz or faster	Pentium 133	Pentium II or higher
Memory	64 MB	128 MB (4GB maximum supported)	64 MB	128 MB
Free Disk Space	1.5 GB Free	2 GB	2 GB with 650 MB free space	2 GB or 4 GB
Display	VGA Adapter and Monitor	Super VGA (SVGA) Monitor and PnP Monitor	VGA	SVGA
Network Adapter	Not Necessary (required if installing over the network)	Any Network Adapter (required if installing over the network)	Not Necessary (required if installing over the network)	Any Network Adapter (required if installing over the network)
CD or DVD	Required	Required	Required	Required
Keyboard and Mouse	Required	Required	Required	Required

Hardware compatibility. The components of the computer should be compatible with the operating system you have selected to install. You can check the compatibility with Windows 2000 Professional from the *Hardware Compatibility List (HCL)*, which contains a list of hardware tested with the OS. With the release of Windows XP, Microsoft changed the name of this list to *Windows Catalog*, which includes software applications as well.

Installation methods. You can choose from a variety of installation methods for installing or upgrading the operating system. Unlike Windows 98 and older versions, which were available on floppy disks, Windows XP and Windows 2000 are distributed on bootable CD-ROMs. If you want to start the installation process from the CD-ROM, you must first change the BIOS settings to make the CD drive as the first boot drive. The following is a summary of installation methods:

Attended installation

When you install Windows XP/2000 from a CD-ROM and are physically present to answer the questions prompted by the setup program, the installation is known as attended. This installation can be started from the setup CD-ROM or from a shared network folder where all setup files are already copied.

Unattended installation

In the unattended installation method, an *answer file* provides answers to most of the questions that are prompted during the installation. The answer file contains answers to most common parameters required by the setup program. You must first create an answer file using Notepad or the Setup Manager utility. The answer file is usually named *unattend.txt*.

SysPrep installation

The System Preparation (*SysPrep*) utility is actually a disk duplication method. It is used to prepare a master image of an existing Windows XP/2000 Professional installation. This image can then be copied to other computers with identical hardware. The Sysprep utility removes the computer-specific information from the image. This method can only be used for clean installations. The computer used for this purpose is known as the master or reference computer and can have any number of applications installed besides the OS. After running SysPrep, you must use a third-party utility to create the actual image of the disk.

Remote Installation Service (RIS)

You can use the RIS for unattended large-scale deployments of Windows XP and Windows 2000 Professional. RIS requires that the computer must be connected to a Windows domain; a domain controller running Active Directory service, and a DNS server, and that a DHCP server is available during installation.

Installation options. The Windows setup program gives you several options for the installation. These include the installation method, a choice of the filesystem for the disk partition, network configuration, and provision for multibooting the computer (installing two or more operating systems on the same computer).

Installation type

You can choose from typical, full, minimal, or custom. The typical installation installs most common components while the full installation installs all mandatory as well as optional components. If you are experienced in installations, you can customize the installation using the custom installation option.

Network configuration

Installing the network components is optional at the time of initial setup. You can install these components later. Even when you have selected to include the networking components, you can initially let the setup join the computer to a workgroup and later change it to a domain membership.

Multiple-boot system

You can install Windows XP or Windows XP Professional with any other Windows OS and keep the system as a multiboot system. At the time of installation, you are given the option of whether you want to delete the existing OS, upgrade it, or keep the system as dual or multiboot.

Disk partition. One of the most important decisions when installing the operating system is about disk partitions. A *partition* is a logical section of the hard disk where the system can store data. When you start installing the operating system, the setup program lets you install the operating system on an existing hard disk partition, or you can create a new partition. If you decide on using the existing partition to creatre a new one, all previously stored data on that partition will be lost

Microsoft recommends that you should create only one partition during installation that is to be used for installing the operating system and that you make other partitions after the installation is complete. When you partition the disk, you must also format it using the FAT or NTFS filesystem. In case you are dual-booting the system with Windows XP/2000 Professional and another operating system, you should install each operating system in a separate disk partition. It is recommended that you use the NTFS filesystem for all disk partitions due to its efficiency and advanced security features. In case you are dual-booting Windows XP/2000 with an old operating system such as Windows 95 or Windows Me, which do not recognize NTFS partitions, you must keep the boot partition as FAT.

Installing Windows XP Professional

Windows XP Professional comes on a single CD-ROM with a product key that will be used during the installation. If your computer BIOS supports booting from the CD-ROM, simply insert the Windows XP Professional CD in the CD-ROM drive and start the computer. The setup process starts with *text mode*, during which the hard disk is prepared and necessary installation files are copied to the hard disk. Setup then enters the *GUI phase*, when the user is prompted for information about the computer, username, and password, etc. This phase includes the network phase where the setup program detects the network adapter and collects information about networking components. The installation completes when the setup program copies final files to the hard disk, creates Start menu items, registers components, removes temporary setup files, and restarts the computer.

Text mode. The text mode phase copies the initial setup files to the computer, creates hard disk partitions, and then copies setup files to the hard disk. The following steps are completed:

1. If the computer BIOS supports booting from the CD-ROM, you can start the text mode by inserting the Windows XP Professional CD-ROM into the CD-ROM drive. Restart the computer, and the text mode of installation begins.
2. If you are already running an operating system, simply insert the CD-ROM and choose whether you want to upgrade the previous operating system or perform a clean installation from the Welcome screen.
3. If you wish to install any third-party device drivers, such as a SATA disk controller, press F6.
4. Installation continues with copying initial setup files into memory. A Welcome screen appears. Press Enter to continue.
5. Press the F8 key to accept the Licensing Agreement.
6. In the Disk Partitioning section, select the disk partition you wish to use for Windows XP Professional. Press C to create a new partition or press D to delete an existing partition.
7. The setup program checks the selected partition for errors and formats the partition with the selected filesystem. Setup then copies necessary files to the hard disk partition.
8. The computer restarts and enters the GUI phase, as explained in the next section.

GUI mode. After the computer restarts, the setup wizard starts. This is known as the *GUI phase* or *GUI mode*. The following steps explain the procedure:

1. Press Enter to continue installation. During this time, setup detects and installs various devices and drivers. This takes several minutes before the next screen is displayed.
2. The Regional and Language Options screen appears. Make your selections appropriately and click Next.
3. In the Personalize Your Software page, fill in the correct information and click Next. Enter the correct 25-digit Product Key and click Next.
4. In the Computer Name and Administrator Password screen, enter a name for the computer and enter the password that you wish to assign to the computer's local administrator. Click Next.
5. In the Date and Time screen, check and, if required, correct the date, time, and time zone settings and click Next.
6. The setup now enters the *Network Phase*. Networking components are detected and installed. Choose Typical if you wish to proceed with automatic configuration; otherwise, choose Custom. Typical networking components include Client for Microsoft Networks, File and Print Sharing for Microsoft Networks, and TCP/IP protocol with automatic IP addressing. Click Next.
7. The Workgroup or Computer Domain name screen appears next. If you select a domain name, you will be asked about the domain administrator's username and password. Enter the correct information and click Next. Setup copies several files to the hard disk.
8. Setup completes the installation by installing the Start menu items, registers various components you selected, saves your configuration to the registry, removes temporary installation files, and restarts the computer.

When the computer restarts, the Welcome screen appears if you selected to join a workgroup. If you selected to join a domain during installation, the Logon to Windows screen appears instead.

Installing over the network. When installing Windows XP Professional over the network, the installation files are stored on a network file server known as the *distribution server*. The setup process is started using either the *winnt.exe* or *winnt32.exe* command, depending on the operating system currently in use.

- If you are using MS-DOS or Windows 3.x versions, run *winnt.exe* to start the installation process.
- If you are currently using Windows 95, Windows 98, Windows Me, Windows NT 4.0, or Windows 2000 Professional operating systems, run the *winnt32.exe* to start the installation.

The following are some essential steps that you must take before starting the installation:

1. Locate the distribution server and the correct path to connect to the shared folder.

2. Create a FAT partition on the computer where you want to install Windows XP Professional.
3. Install necessary network client software in order to enable the computer to connect to the distribution software. If the computer does not have any operating system, you can use a boot floppy disk that contains network client software to communicate on the network.
4. Start the computer either using the currently installed operating system or from the network client boot disk.
5. Connect to the shared folder (*/i386*) on the distribution server.
6. Start the installation by running the *winnt.exe* or *winnt32.exe* from the command prompt.

Both the *winnt.exe* and *winnt32.exe* utilities include a number of parameters. Tables 2-8 and 2-9 list some of the commonly used parameters for these commands respectively.

Table 2-8. Parameters for the winnt.exe command

Parameter	Function
`/r[`*`folder`*`]`	Copies and saves an optional folder.
`/rx[:`*`folder`*`]`	Copies an optional folder. The folder is deleted after installation.
`/s[:`*`sourcepath`*`]`	Specifies the location of source files in the format \\server\share\\ *[path]*.
`/t[:`*`tempdrive`*`]`	Specifies the temp drive to contain installation files.
`/u[:`*`answer file`*`]`	Specifies an answer file for unattended installation. This parameter must be used with the `/s` parameter.
`/udf:id[,`*`UDF_file`*`]`	Specifies the identifiers that setup uses to see how a uniqueness database file (UDF) modifies the answer file.

Table 2-9. Parameters for the winnt32.exe command

Parameter	Function
`/checkupgradeonly`	Only checks whether the computer can be upgraded to Windows XP Professional.
`/cmd:command_line`	Specifies a command that should be run immediately after installation.
`/cmdcons`	Installs Recovery Console as a startup option.
`/copydir:foldername`	Creates an additional folder with the *%systemroot%* folder.
`/debug[level] [:`*`filename`*`]`	Creates a debug file for troubleshooting.
`/dudisable`	Disables dynamic updates during installation.
`/makelocalsource`	Copies all installation files to the local hard drive.
`/noreboot`	Executes another command before restarting the computer when the text phase is complete.
`/s:sourcepath`	Specifies the location of source files for Windows XP Professional installation.
`/tempdrive:driveletter`	Copies installation files on this temporary drive and installs the operating system on that drive.

Table 2-9. Parameters for the winnt32.exe command (continued)

Parameter	Function
`/udf:id[,UDF_file]`	Specifies the identifiers that setup uses to see how a uniqueness database file (UDF) modifies the answer file. If you do not specify a UDF file, you are prompted to insert a disk containing the $UNIQUE$. UDB file.
`/unattend`	Used to upgrade previous versions of Windows 98, Windows ME, Windows NT 4.0, and Windows 2000 without any user input. Copies all user settings from previous version of Windows.
`/unattend[num]:[answerfile]`	Used to perform a fresh installation of Windows XP Professional in unattended mode using the specified answer file. The `num` option specifies the time that must lapse after copying of files and the restart of the computer. Dynamic updates are downloaded and included in installation files.

Installing Windows 2000 Professional

Start from the Windows 2000 Professional installation CD-ROM. Make sure that the CD-ROM is set to start before the hard disk does. Insert the CD-ROM, and then when you are prompted, press any key to start the Windows 2000 Professional installation. The following steps explain the installation process:

1. Setup inspects computer's hardware configuration, and installation begins. When the Microsoft Windows 2000 Professional screen appears, press Enter.
2. Press the F8 key to accept the terms of the license agreement.
3. When the Windows 2000 Professional Setup screen appears, either press Enter to install on the selected partition, or press C to create a new partition.
4. You may choose to leave the current partition as is, format it using FAT, convert it to NTFS, or format it using NTFS. Press Enter after you make your selection. Setup examines the existing hard disks and then copies the required files for installation. The computer is then restarted.
5. Installation enters the GUI mode. Click Next to start the GUI wizard. Setup detects and installs necessary devices such as the keyboard and the mouse.
6. The Regional Options page appears. Customize your installation for locale, number format, currency, time, date, and language, if necessary. Click Next.
7. The Personalize Your Software dialog box appears. Type your name and the name of your organization, and then click Next.
8. In the Product ID dialog box, type the 25-character product key, and then click Next.
9. The Computer Name and Password dialog box is displayed. Either accept the default name or type a different name for the computer. You are prompted for an administrative password—type a password for the Administrator account. Click Next.
10. The Date and Time Settings dialog box appears. Set the correct date and time for your computer and select a time zone. Click Next.
11. The installation now enters the networking phase. Setup detects network settings and installs the networking software. Choose Typical to set default network settings such as File and Print Sharing for Microsoft Networks,

Client for Microsoft Networks, and TCP/IP protocol. Choose Custom to specify the network components that you require for network environment, and then click Next.

12. In the next dialog box, specify whether to join the computer to a workgroup or domain. If you indicate that you are part of a domain, you will need to specify your domain username and password. Click Next.
13. The setup enters the final phase. It installs Start menu items, registers components, saves settings, and removes temporary files. Remove the Windows 2000 CD-ROM, and then click Finish to restart the computer.
14. After the computer restarts, click Next in the Welcome to the Network Identification Wizard dialog box. Specify whether users must enter a username and password or whether Windows 2000 should automatically log on a specific user when the computer starts. Click Finish.

Completing post-installation tasks. After the installation is complete, you must perform a number of tasks such as product activation (Windows XP), updating device drivers, copying user data files, and verifying the installation. These tasks are explained in the following paragraphs:

Product activation (Windows XP)

The retail and evaluation copies of Windows XP Professional must be activated within 30 days of installation. Activation is not required if the copy of Windows XP Professional is a part of volume licensing plan. After 30 days, the Windows XP Professional ceases to work and does not allow you to log on to the system.

Update OS and device drivers

Once the basic installation is complete, you might need to update the drivers for certain devices such as the network adapter or a printer. Some vendors might have updated their drivers after the release of the operating system. You must also check whether Microsoft itself has updated the OS. For Windows 2000 Professional, you need to install Service Pack 4. In the case of Windows XP Professional, you need Service Pack 2 if it is not included on the setup CD-ROM.

Copy user data files

After the installation is complete, you will need to install application software and restore data files for the user who works on the computer. You will also need to restore his desktop settings as well. You can use the File and Settings Transfer Wizard in Windows XP to copy user settings and files from another computer. This wizard is located in the System Tools subfolder in the Accessories folder in the Start Menu. This wizard can copy application settings and user data files as well as several other settings such as Internet Explorer settings, Outlook settings, desktop settings, folder options, etc.

Verifying installation

After the installation is complete, you must verify that the OS and the applications work as expected. Reboot the computer and examine the functionality of different devices. Make sure that it is able to connect to the network and printers. Run a couple of applications and verify that they do not produce unexpected errors.

Upgrading an operating system

In some situations, you might be required to upgrade a previously installed version of Windows to Windows XP or Windows 2000 Professional. You will need to make certain checks to perform a successful upgrade installation. These checks include verifying that an upgrade path exists, the new OS supports the computer hardware and the applications are compatible. When you decide to perform the upgrade, you will also be required to back up the existing data files. In the discussion that follows, we will take a look at these aspects.

Available upgrade paths. Not all previous versions of Windows can be directly upgraded to Windows XP or Windows 2000 Professional. Table 2-10 lists the options available for performing an upgrade installation for both of these operating systems.

Table 2-10. Upgrade paths for Windows XP and Windows 2000

Previous operating system	Upgrade to Windows XP Professional	Upgrade to Windows 2000 Professional
Windows 95	No; upgrade to Windows 98 first	Yes
Windows 98	Yes	Yes
Windows ME	Yes	No
Windows NT Workstation 4.0 with SP4	Yes	Yes
Windows 2000 Professional	Yes	N/A

> Memorize the details given in Table 2-10 because questions on upgrading OS generally make their way into the A+ exams. Also make it a point to figure out a tricky question where you would be asked to upgrade a previous server operating system (Windows NT 4.0 Server to Windows 2000 Professional or a Windows 2000 Server to Windows XP Professional). Remember that only client operating systems can be upgraded to new client operating systems.

Checking hardware compatibility. Both Windows XP and Windows 2000 Professional setup programs include an option to test whether the current computer hardware and software can be upgraded or not. Run the following command from the */i386* folder on the CD-ROM drive:

```
winnt32 /checkupgradeonly
```

When the test is complete, it displays the compatibility report. This report is saved as the file *UPGRADE.TXT*.

Checking application compatibility. You will need to ensure that the currently installed applications are compatible with the new OS. If they are not compatible, choose whether you will need to obtain newer versions of applications or apply updates to make them so.

Installing additional Windows components. When upgrading a previous version of Windows to a newer version, you might need to apply OS updates before starting the installation. The updates can be in the form of a service pack (SP), hotfixes, or patches. For example, if you want to upgrade a Windows 2000 Professional computer to Windows XP Professional, you will first need to install Windows 2000 Service Pack 4 (SP4).

Network compatibility. If the computer is connected or will be connected to a network, ensure that the new OS supports the network adapter and its driver. You might also need to obtain information on protocol configuration such as TCP/IP addresses.

Upgrade utility. You must decide on a built-in utility to perform the upgrade. Depending on the currently installed OS on the computer, you can use one of the following utilities:

- Use *winnt.exe* to upgrade from a 16-bit OS such as Windows 95 and MS-DOS.
- Use *winnt32.exe* to upgrade from a 32-bit OS such as Windows 98 and later.

Backing up user data. Considering that the upgrade installation is successful, the user data, desktop, and application settings will be migrated to the new OS. But you should not take chances and always plan to back up at least user data files before starting the installation.

Performing the upgrade. Performing an upgrade install is fairly simple compared to a fresh installation. Start the computer with its currently installed OS and insert the bootable setup CD for Windows XP or Windows 2000, as required. You will see an option to upgrade the currently installed OS. Click Yes and click the setup program.

The upgrade wizard for Windows 2000 Professional guides you through the process as follows:

License agreement and product key

You will be prompted to accept the End User License Agreement (EULA) and enter a valid 25-digit product key.

Providing upgrade packs

This option provides an opportunity to apply upgrade packs for applications. You can still apply the upgrade packs after the upgrade is complete.

Upgrading to NTFS File System

You may choose to upgrade the disk filesystem to NTFS or leave the current filesystem as is. Microsoft recommends that you upgrade the filesystem to NTFS if not already using it. If you are dual-booting the new OS with another OS that is not compatible with NTFS, select No for this option.

Upgrade the PnP driver files

You are given an option to update driver files for PnP devices. If you do not have these files handy, you can install them after the upgrade is complete.

Upgrade report

The setup program prepares an upgrade report that includes compatibility issues with currently installed hardware and software. You have the option to continue with the upgrade process or exit it in order to obtain necessary updated software for applications of device drivers.

Once these steps are complete, the setup program proceeds with the installation (which is more or less automated), and you are not required to answer any further questions.

When upgrading to Windows XP, you will need to accept the EULA and enter a 25-digit product key after you choose the Upgrade option. If the computer is connected to the Internet, the setup program checks for update files on Microsoft's web site and automatically downloads them to install them during the upgrade. The upgrade to Windows XP is also a simple process, and you are not asked many questions. After the installation is complete, you will need to activate the product with Microsoft within 30 days of installation.

Installing devices and drivers

Once the basic installation of the OS is complete, you might be required to install or upgrade devices and their drivers to enhance the capabilities of the computer. These may include input/output (I/O) devices such as printers, scanners, mouse devices, monitors, modems, or network adapters. Some of the essential tasks associated with installing devices are covered in the following sections.

Identifying the PnP and non-PnP devices. Computer devices can be classified into two main categories: Plug and Play (PnP) and non-Plug and Play. While PnP devices are automatically detected and configured by the computer BIOS and the OS, the non-PnP devices need to be manually configured. For a PnP device to function properly, the computer BIOS and the OS should support the PnP functionality. Almost every device on the market these days is PnP-compatible.

Permissions and rights. You must have adequate permissions in order to install devices and drivers on Windows XP and Windows 2000 computers. If you are logged on as an administrator or a member of the administrators group, you can perform the installation without any problems. Otherwise, you will need to have the load and unload device drivers right on the computer. If the device driver has a digital signature, any user can install the device, provided that no user interaction is required during installation.

Driver signing. The driver signing feature in Windows ensures that only those drivers are installed that are verified by Windows Hardware Quality Labs (WHQL). These drivers carry a digital signature that verifies that the driver has been tested and approved by Microsoft or the vendor to work with the operating system. Windows XP Professional includes another utility known as *Signature Verification (signverif.exe)* to verify that the installed device drivers have digital signatures. Only administrators or members of administrators can install unsigned device drivers.

Obtaining device drivers. Most device driver files are distributed on CD-ROMs that come with the device. You will need to obtain the driver and check its compatibility with the OS before installing it on the computer. In case you have lost the original driver CD or are updating a currently installed driver, you may also download the driver from the vendor's web site, if it is available.

Connecting the device. The device must be connected to the computer before you install its driver. In case the device is PnP, it will be automatically detected when you start the computer. In case of USB devices, you will install the drivers first and then can connect them while the computer is powered on. In any case, you must follow the manufacturer's instructions for the correct installation process.

Installing and configuring the driver. You can use the CD-ROM that contains the device driver, download it from the manufacturer's web site or have the Add Hardware wizard install the driver. After the installation is complete, you must restart the computer so that the new device can be used. This action is not necessary for devices that are hot-swappable, such as the USB devices.

PnP devices are automatically configured to use appropriate system resources such as IRQ, I/O port, and DMA address during installation. For some other devices, you must go through a series of steps to fully configure it. For example, printers, scanners, and cameras must be configured for optimum performance and requirements.

Adding devices in Windows 2000. The following steps explain the device installation process in Windows 2000 Professional:

1. Turn off the computer and physically install the device in an appropriate expansion slot or to an external port.
2. If the device is detected, Windows will try to locate an appropriate driver for it. If it cannot find one, it will prompt for the location of driver files.
3. If the device is not detected, you can use the Add/Remove Hardware utility in the Control Panel to manually install the driver.
4. The wizard prompts you whether you want to Add/Troubleshoot a device or Uninstall/Unplug a device. Choose the Add/Troubleshoot option.
5. The OS searches for PnP devices that do not have a driver installed yet. You are prompted to choose a device from a list of devices. Click the Add a New Device option on top of the list.
6. You are prompted to have Windows search for a suitable driver, or you can click the Have Disk button to install the driver from the CD or from another location on the hard disk.

Adding devices in Windows XP. The following steps explain the device installation process in Windows XP:

1. Turn off the computer and physically install the device in an appropriate expansion slot or in an external port.

2. Restart the computer and wait for Windows XP to detect the hardware device. You can either choose to let Windows search for and install a suitable driver or choose to install the driver manually. With the first option, Windows tries to search for an appropriate driver. If you insert the driver CD, Windows will locate the driver files automatically.
3. Once the driver files are located, Windows XP checks whether the driver is digitally signed or not. You are given an option to stop the installation in case the driver is found to be unsigned.
4. Once you click the Continue Anyway button, the driver is installed and the device is ready to use.

Verifying device driver installation. Once the device is installed and the driver is loaded, you can verify it from the Device Manager. A device with an incorrect driver is flagged with a big yellow question mark (?). A black exclamation point (!) on a yellow field indicates the device is in a problem state. Note that a device that is in a problem state can be functioning. You can double-click the device and view its properties.

Optimizing performance

Optimizing Windows is the process of fine-tuning its performance. Both Windows XP and Windows 2000 include some utilities that help optimize the OS performance. In this section, we will discuss how the OS can be fine-tuned for optimum performance.

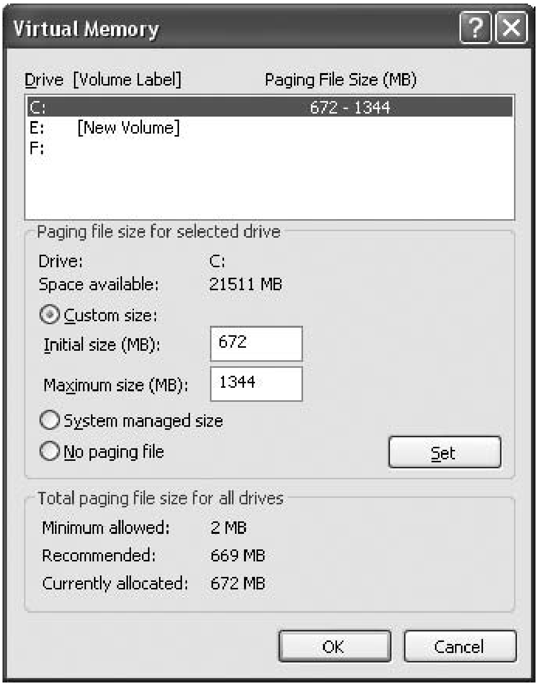
Virtual memory. Windows operating systems use virtual memory to temporarily store data when it is running out of the physical memory (RAM) in the computer. This data is stored in a file on the hard disk (which is known as swap file or paging file). For most Windows installations, the OS automatically manages the size of the paging file. You can manually increase or decrease the size of this file or split the file across multiple hard disks depending on your requirements.

If you feel that the system performance is poor, you can increase the size of this file or divide the file into multiple disks. The following steps explain how you can change the virtual memory settings in Windows XP:

1. Click Start → Control Panel → System.
2. Click the Advanced tab.
3. Click the Settings button in the Performance area.
4. Click Advanced.
5. Click Change in the Virtual Memory area.
6. Enter the “Initial size” and “Maximum size” and click Set. Refer to Figure 2-10.
7. Close all windows.

In Windows 2000, the virtual memory can be fine-tuned with the following steps:

1. Click Start → Control Panel → System.
2. Click the Advanced button.
3. Click the Performance Options button.



Drive [Volume Label]	Paging File Size (MB)
C:	672 - 1344
E: [New Volume]	
F:	

Paging file size for selected drive

Drive: C:
Space available: 21511 MB

● Custom size:
Initial size (MB): 672
Maximum size (MB): 1344
○ System managed size
○ No paging file

Total paging file size for all drives

Minimum allowed: 2 MB
Recommended: 669 MB
Currently allocated: 672 MB

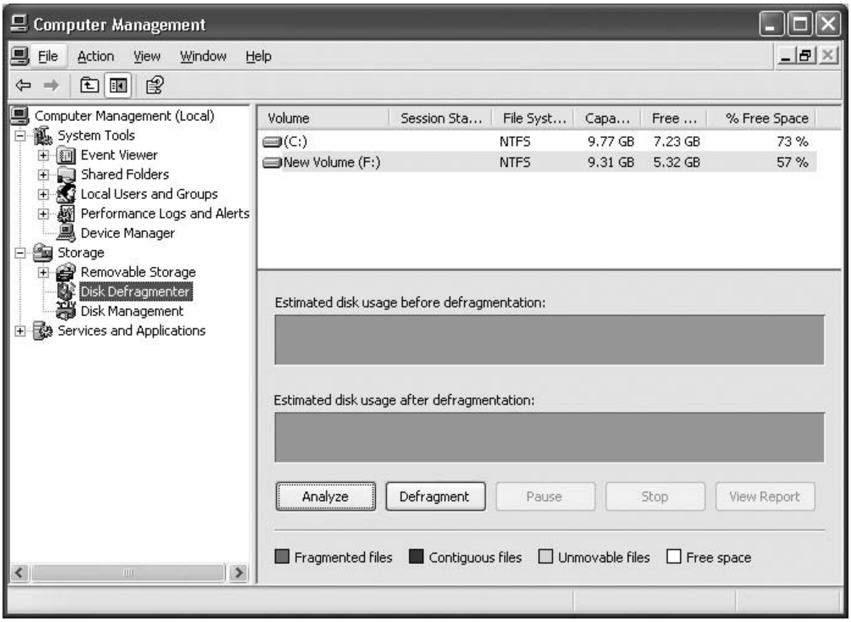
Figure 2-10. Virtual Memory settings

4. Select the Applications or Background Processes button, as required.
5. Click the Change button to change the size of paging file.
6. In the Virtual Memory page, enter the initial and maximum size of the paging file.
7. Click Set and click OK.

Defragmenting hard disks. Defragmenting hard disks helps improve their read/write performance. Hard disks become fragmented when some applications are installed or after a large number of files are moved or deleted. *Fragmentation* refers to the state of a hard disk when it no longer has contiguous space available to store new files or folders. The Disk Defragmenter utility can analyze hard disks and defragment them to free up contiguous space. Disk Defragmenter works on FAT, FAT32, and NTFS volumes.

There are several ways to access the Disk Defragmenter:

- Click Start → All Programs → Accessories → System Tools → Disk Defragmenter.
- Open Windows Explorer; open the properties of disk or volume. Select the Tools tab. Click Defragment Now to open the Disk Defragmenter snap-in.
- Right-click My Computer, and click Manage to open Computer Management. The Disk Defragmenter is located under the Storage folder as shown in Figure 2-11.



Volume	Session Sta...	File Syst...	Capa...	Free ...	% Free Space
(C:)		NTFS	9.77 GB	7.23 GB	73 %
New Volume (F:)		NTFS	9.31 GB	5.32 GB	57 %

Figure 2-11. Disk Defragmenter snap-in

At the top of the window you can select the disk or volume that you wish to analyze or defragment. The two buttons on the bottom of the screen give you the following two options:

The Analyze button
Used to analyze the entire disk and display the results in the graphical form.

The Defragment button
Used to start the defragmentation process. The disk is automatically analyzed before it is defragmented.

Temporary files. The Disk Cleanup utility in Windows XP is used to free up disk space by deleting temporary files and folders from the disk or volume. This utility can be accessed from Windows Explorer or from the System Tools folder under Accessories in the All Programs menu. Disk Cleanup essentially gives you options to delete several types of files. These files include:

- Program files downloaded from the Internet, including ActiveX controls and Java Applets.
- Temporary Internet files to clear the computer cache. These files are stored in the Temporary Internet Files Folder.
- Temporary Files located in the Temp folder.
- Files stored in the Recycle Bin.

Configuring services. System performance is greatly affected on the startup type of services. Windows installs several services during the installation process. Many of these services are never used but automatically start when the computer boots and keep running in the background. Identifying unused services and disabling them can improve the system performance. The Services utility in the Control Panel is used to configure the startup behavior of services. You can stop a running service, start a stopped service, or configure its startup type as automatic, manual, or disabled. When the startup type for a service is configured as manual, it starts only when some application requires it.

Troubleshooting Techniques

In order to troubleshoot problems related to the operating system, you must understand the Windows boot sequence, the advanced boot options available, and basic diagnostic procedures. Additionally, you must have good knowledge of using built-in troubleshooting utilities. Familiarity with different types of error messages and common operational problems will help you resolve problems easily and quickly.

Understanding boot sequence

The following discussion explains the boot sequence in both Windows XP and Windows 2000:

Pre-boot sequence. When the computer is started, it performs a *pre-boot sequence* in the following manner:

1. A POST is performed to check the hardware components, which include physical memory (RAM), video, and the keyboard. In case the computer BIOS supports Plug and Play (PnP), the configuration of PnP-compatible hardware devices is performed.
2. The Master Boot Record (MBR) is loaded from the selected boot device. The MBR in turn loads the NTLDR file from the boot device. In case the computer has a Small Computer System Interface (SCSI) device as the boot device without its own BIOS, the *NTBOOTDD.SYS* file is loaded.

Boot sequence. NTLDR takes charge of the process from here on and performs the following steps:

1. NTLDR switches the processor to 32-bit flat memory mode and loads the filesystems driver to access the FAT, FAT32, or NTFS partitions.
2. NTLDR reads the *BOOT.INI* file and selects an operating system. If multiple operating systems are installed on the computer, the *BOOT.INI* file prompts the user to select an operating system. If the MS-DOS operating system is selected, NTLDR loads the boot sector from the *BOOTSECT.DOS* file.
3. NTLDR calls on the *NTDETECT.COM* file to perform hardware detection, which displays error messages if any hardware problems exist. If the computer has more than one hardware profile, the user is given a choice to select an appropriate profile.

Kernel Load and initialization. The Kernel Load phase begins and performs the following steps:

1. NTLDR calls on NTOSKRNL.EXE file (the Windows Kernel), which changes the screen color from black to blue. The Kernel loads another module known as the hardware abstraction layer (*HAL.DLL*).
2. The kernel initializes by creating a registry key known as HKEY_LOCAL_MACHINE\HARDWARE. This key contains information about the hardware devices on the computer based on the results of *NTDETECT.COM*.
3. The kernel creates a Clone Control Set by copying the control set in the HKEY_LOCAL_MACHINE\SYSTEM\Select subkey of the registry.
4. The kernel loads low-level device drivers and filesystems. The device drivers initialize as they are loaded. The user mode subsystem is loaded and the computer display changes to the GUI mode.
5. Once the kernel has loaded and is initialized, the system services are started.

Logon process. The logon process starts as soon as the *Winlogon* service is started. The Local Security Authority displays the logon screen. The Service Control Manager scans the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services subkey of the Registry to look for services that should start automatically. After you log on successfully to the system, the operating system copies the Clone Control Set to the Last Known Good control set.

Understanding the Advanced Boot Options

Some of the Windows startup problems can be resolved using the Advanced Boot Options during the startup phase. The most commonly used advanced options include Safe Mode, Last Known Good Configuration and Recovery Console. When Windows fails to complete the boot process, you can access any of these options by pressing the F8 key immediately after the POST is complete.

Safe Mode

In the Safe Mode, Windows XP loads with minimum basic system services and device drivers sufficient to boot the operating system. These components include the keyboard, mouse, hard disks, the VGA monitor, and other most essential system services. Safe Mode provides access to all system and device configuration options so that you can enable or disable components one by one and try to pinpoint the problem.

Safe Mode with Networking

Safe Mode with Networking is similar to Safe Mode except that networking devices, drivers, and services are also initialized.

Safe Mode with Command Prompt

Safe Mode with Command Prompt loads the command interpreter, just like in MS-DOS, instead of the GUI.

Last Known Good Configuration

The Last Known Good Configuration option loads the last used system configuration that allows you to return the system to the previous working configuration. Windows saves two types of configurations in the Registry: Default and Last Known Good. The Default configuration is saved to the registry when you shut down the system. The Last Known Good Configuration is saved when you log on to the system.

The Last Known Good Configuration will not be useful if you have already logged on to the system with incorrect configuration. This option must be used before a successful logon happens.

Enable Boot Logging

This mode enables the boot logging option that stores the boot process information in a file named *NTBTLOG.TXT*. This file is stored in the */WINNT* directory and is helpful is diagnosing startup problems.

Enable VGA Mode

This mode loads Windows with basic VGA device drivers and other normal configuration. This mode is helpful in diagnosing problems with the display driver.

Recovery Console

The Recovery Console is useful in resolving system startup problems when the Safe Modes and Last Known Good Configurations do not work. The Recovery Console allows you to repair critical system files that might have been corrupted by copying original files from the Windows XP/2000 Professional setup CD-ROM. You can also enable or disable services that you think might be causing the problem. The Recovery Console can either be started from the Windows setup CD-ROM or can be installed as one of the Advanced Boot Options as explained in the following paragraphs.

Once the Recovery Console is installed, you can type `help` and press the Enter key at any time to get a list of available commands. Type `exit` and press the Enter key again to close the Recovery Console and restart the system.

Starting Recovery Console from the Windows XP/2000 setup CD-ROM

1. Insert the Windows XP/2000 setup CD-ROM into the CD-ROM drive. Make sure that the computer BIOS is set to start from the CD-ROM. Restart the computer.
2. Press Enter when the Setup Notification message appears.
3. At the Welcome screen, press R to repair a Windows XP Installation Using Recovery Console.
4. In case there is more than one Windows XP installation on the computer, type the installation number corresponding to the installation that you wish to repair, and press Enter.
5. Press C at the Windows XP Recovery Console screen to start the Recovery Console.

6. Type the Administrator password when prompted and press Enter. This password must be the password of the Local Administrator.
7. The Recovery Console displays a command prompt.

Installing Recovery Console as Advanced Boot Options

1. Insert the Windows XP setup CD-ROM in the CD-ROM drive while running Windows XP Professional.
2. Select NO when you are prompted to upgrade to Windows XP Professional.
3. Click Start → Run to open the Run dialog box. Type `cmd` and press Enter to open the command prompt.
4. At the command prompt, type the following command, replacing the word *drive* with the drive letter of your CD-ROM drive:

   ```
   drive:\i386\winnnt32.exe /cmdcons
   ```

5. Restart the computer.

Once installed, the Recovery Console appears as one of the options in the Advanced Boot Options menu when you press F8 during the startup process.

System Restore (Windows XP)

The System Restore in Windows XP helps restore the system to a working state after you make changes to the system settings or install applications that make it unstable. It uses system restore points to store a snapshot of system settings at regular intervals. When you run the System Restore, a calendar is displayed in which you can pick a particular System Restore point. The System Restore can be accessed in one of the following methods:

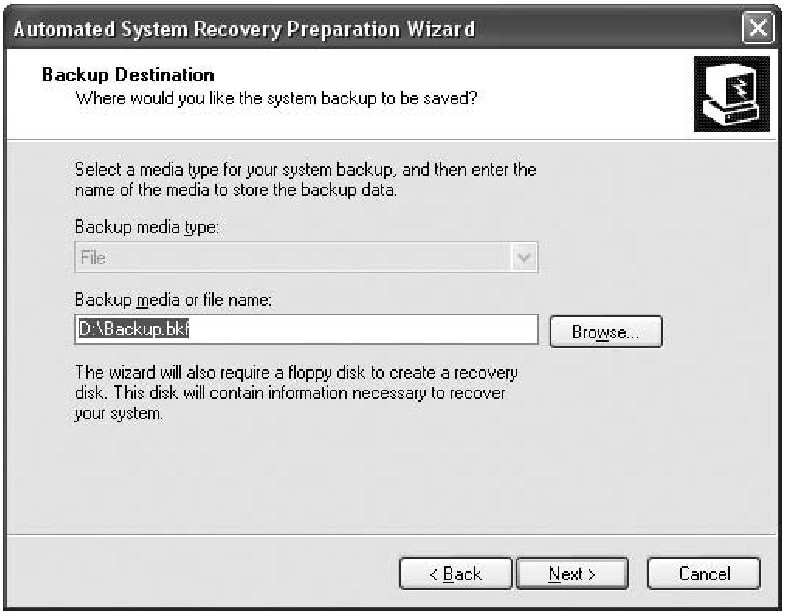
- Open the Help And Support Center, located in the Start menu. Under Pick a Task, click Undo Changes to Your Computer Using System Restore.
- Click Start → All Programs → Accessories → System Tools → System Restore.

You can also create System Restore points manually when you expect to make changes to your system. The following steps explain how you can create a System Restore point:

1. Click Start → All Programs → Accessories → System Tools → System Restore.
2. Click Create A Restore Point. Click Next.
3. Type a name to identify the restore point in the Restore Point Description box.
4. Click Create.

Automated System Recovery (Windows XP)

The Automated System Recovery (ASR) Wizard in Windows XP is located in the Backup utility. This utility is used to restore the system after a major failure. Click the Automated System Recovery Wizard on the Backup Utility window to prepare an ASR backup for the computer. You will need a blank floppy disk and a full backup of the system partition of the computer. The ASR Wizard is shown in Figure 2-12.


Automated System Recovery Preparation Wizard

Backup Destination
Where would you like the system backup to be saved?

Select a media type for your system backup, and then enter the name of the media to store the backup data.

Backup media type:
File

Backup media or file name:
D:\Backup.bkf

The wizard will also require a floppy disk to create a recovery disk. This disk will contain information necessary to recover your system.

Figure 2-12. ASR Wizard in Windows

The following procedure explains how the Automated System Recovery Wizard can be used to back up critical system components:

1. Click Start → Programs → Accessories → System Tools → Backup.
2. Click the Automated System Recovery Wizard from the Backup Utility window. This opens the Automated System Recovery Wizard dialog box. Click Next.
3. Select the Backup Media Type and the Backup Media or Filename. Click Next.
4. Check the information on the Completing the Automated System Recovery Preparation Wizard page. If correct, click Finish.
5. It takes the system about an hour or so to back up the system files. You are prompted to insert a blank floppy disk.
6. The backup completes writing to the floppy disk and presents an option to view the report.
7. Click Close to close the backup process and close the Backup Utility window.

When you need to restore the system using the ASR, you can use the floppy disk to restore the system partition of the computer. You must also restore critical system files that you backed up on the tape drive or a network file share. Other applications and data can be restored using your regular backup sets.

Emergency Repair Disk (Windows 2000)

In Windows 2000 you can prepare Emergency Repair Disks (ERDs) or boot disks (a set of four floppy disks) to help start the system when it cannot boot normally from the hard drive. You will need the setup CD-ROM to create the boot disk set. As with the ASR utility in Windows XP, the ERD utility in Windows 2000 is also located in the Backup utility. You can also create the ERD disks by running the file *MAKEBOOT.EXE* from the BOOTDISK folder on the setup CD-ROM.

In order to use the ERD, you will need to choose the Repair option after starting the installation using the setup CD-ROM. The installation process will then prompt you to provide the ERD disk set.

Troubleshooting procedures

The troubleshooting process starts when someone reports a problem and asks for your help to resolve it. The first step to troubleshoot a problem is to talk to the user and gather as much information as you can. This is followed by identifying potential causes and isolating the problem. The discussion that follows explains the troubleshooting process that you are expected to know for the A+ exams as well as at your workplace.

Talking to the user. As noted earlier, the first step in troubleshooting a problem is to gather information about the problem and its symptoms. You will need to talk to the computer user to gather necessary information that can help you get started in the process of resolving the problem. You might need to ask a few questions and should be patient when listening to the user. Do not jump to a conclusion at this point.

Gathering information. Gathering sufficient information from the user or from the system event logs will ensure that you know what happened between the time the computer was working and when it stopped. The problem might be due to a user error, a malfunctioning device, or a configuration change. Find out if a new application was installed, if a new hardware device was added, if a device driver was updated, or if the user tried to install a new version of a game or just tried to open an application. Unless you have enough information, you will not be able to correctly identify the cause of the problem.

Identifying potential causes. One you have enough information about the problem, the next step is to look into several possible causes that could result in the specific problem. Try not to make assumptions on initial information and do not overlook even the least important cause.

Isolating the problem. Once you have identified a number of potential causes for the problem, you will need to eliminate the causes that do not directly relate to the problem. In case of a hardware problem, you might need to disable one or more hardware devices and try starting the computer with minimum configuration. Isolating the problem ensures that you have correctly identified the cause of it.

Testing related components. Sometimes problems do not come alone. One problem leads to another and the process continues. When you have identified the cause of the problem, check whether the problem itself created other problems. This will ensure that you take care of other problems as well when applying a corrective solution.

Apply a solution and test results. Next, decide on what you need to do to rectify the problem. The solution may be as simple as reconnecting a network cable or as complex as reinstalling the operating system. Whatever is the solution to the problem, you must first make sure that it will work as expected and will return the computer to its working state. You might need to consult your seniors, refer to the instructional manuals, or search the Internet to find a resolution. Apply the solution and test the results before you finally hand over the computer to the end user.

Document the solution. Once the problem is rectified, you should make a note of the problem in the logbook, which is usually available with the help desk department. Include the day and date, the computer name, the installed OS, the name of the user, the type of problem reported, the cause of the problem and what you did to rectify the problem. Documentation is helpful in backtracking future problems with the same computer or user. It is also helpful in getting quick help when the problem is repeated on some other computer.

Operational problems

Some of the problems with operating systems appear as users do their regular jobs on computers. These problems are termed as operational problems, as summarized in the following paragraphs.

Blue Screen. A Blue Screen error in Windows is also commonly known as the *STOP Error* or *Blue Screen of Death*. This error is seen in many Windows operating systems and is considered one of the most critical errors. In most cases, the STOP errors are related to hardware issues and are identified by an 8-digit hexadecimal number such as STOP 0X0000000A, STOP 0X0000007F, etc. Windows writes the error in event logs. You can use the Event Viewer to diagnose these errors. If this is not helpful, you can also search Microsoft's TechNet or search Knowledge Base articles on how to resolve these errors.

System lock up. System lock up or system freezing is usually caused when the system is out of resources. It causes long delays in launching applications, delayed responses to user's keystrokes, or even results in permanent lockup of the system. The most common reason for a system lock up is shortage of RAM. The most effective resolution for system lock up problems is to increase physical RAM in the system and configure the size of paging files (virtual memory). In case you have recently added a hardware component or a software application, you should remove it to see whether the problem is resolved.

I/O device not accessible or does not function. Each I/O device has an associated software device driver, which must be installed if it is not automatically installed and configured by the OS. When you configure the device driver, you must be careful about allocation of system resources. You can use the Device Manager utility to find more information about a device that does not respond. If required, reinstall the device driver to see whether it resolves the problem.

Application failed to start. This error is a result of a misconfigured application or a missing component of the application. An incorrectly installed application is also likely to cause this error. Reinstalling the application usually resolves this problem.

Printing problems. Printing problems are also common operation issues. The “Printers and Scanners” section later in this chapter covers printing problems in detail.

Dr. Watson errors. The Dr. Watson utility (*drwtsn32.exe*) is included in most Windows operating systems to interpret errors and inform the user of potential causes. The information provided by this utility can be helpful in diagnosing problems. Dr. Watson creates a text file named *DRWTSN32.LOG*, which contains critical information about the error.

Illegal operation. The illegal operation error is reported when an application attempts to perform an action that is not permitted by the operating system. The text of the error message reads as:

> The application has performed an illegal operation and will be shut down. If the problem persists, contact the program vendor.

Windows displays a text box containing this error message and three buttons: OK, Cancel, and Details. The Details button displays more information about the error. You can click either the OK button or the Cancel button to close the application.

General protection fault (GPF). A GPF occurs when an application attempts to access the areas of memory that are used by other applications. To resolve GPF errors, reboot the computer, and the computer memory will be cleared. If the error continues to appear, you may need to identify the application that causes this error. Once the rogue application is detected, you can contact the vendor to see whether they have a fix for the problem.

Common error messages

The following sections cover some more common error messages that you are likely to encounter:

Missing NTLDR

The “NTLDR is Missing” error is accompanied by a “Press Any Key to Restart” message. This error is caused if any of the system startup files are missing or have become corrupt. The files that can cause this error include *NTLDR*, *NTDETECT.COM*, and *BOOT.INI*. You can restore these files by using the Recovery Console, an Emergency Repair Disk (ERD in Windows 2000), or by using the setup CD-ROM and selecting the Repair option when the installation starts. You can also restore these files using a system restore utility in Windows XP.

Invalid Boot Disk

This error is displayed when the system BIOS cannot access the disk partition that is supposed to contain system startup files. You might have to reinstall the OS to address this problem.

Operating System Not Found

This error means that the BIOS cannot find an operating system on the configured boot partition or boot device. This error is common in new computers that do have a boot partition configured in the BIOS and on which no OS has been installed so far.

Inaccessible Boot Device

This error is displayed when the computer finds a critical error with a boot device. This can be due to a malfunctioning device driver or to some resource conflicts.

Device or Service Failure

If the operating system has started, you may still receive an error saying that a particular device or a service has failed to start. You can open the Event Viewer console and locate the appropriate error message to get help in finding the cause of the problem.

Missing Registry Entry

Windows Registry is a database of complete system configuration. Every system service, driver, and application is registered in Registry before it can work with the installed operating system. If a component fails to create an entry in the appropriate Registry key, it will not be able to start. One of the easiest methods to resolve these errors is to reinstall the driver or application that has generated the error.

Troubleshooting utilities

Windows XP and Windows 2000 include some built-in management utilities that are helpful in troubleshooting problems as well as optimizing system performance. These are mainly classified as disk management, system management, and file management. This section covers a summary of these utilities.

Disk Management utilities. In this section, we will look at some common disk management tools that can be run from the Windows command prompt.

DEFRAG

The *defrag.exe* command is used to defragment hard disks. It can be used to analyze and perform disk defragmentation. Disk defragmentation rearranges files on contiguous sectors on the hard disk, which improves the disk read-write performance. You can also run the Disk Defragmenter utility from the Computer Management console. Another way to start the defragmentation utility is to open the Properties window of a disk partition and select Defrag Now from the Tools tab.

NTBACKUP

The *ntbackup.exe* command starts the Windows backup utility. You can also run the backup utility from the System Tools folder under Accessories in the All Programs menu.

CHKDSK

The *chkdsk.exe* utility is used to check disks for filesystem errors and then fix them. It can also be started from the Properties window of a disk partition and by selecting Check Now from the Tools tab.

FORMAT

The *format.exe* command is used to format a disk partition using FAT or NTFS filesystems. You can also format a disk in Windows Explorer. Right-click a disk partition and select Format from the context menu. Formatting a disk deletes all the contents on a disk partition.

DISKPART (Windows XP)

The *diskpart.exe* is a new disk management utility in Windows XP that can be used to manage all aspects of disks, volumes, and partitions except for formatting the disk. This is an advanced utility and must be used with caution.

System management utilities. In this section, we will look at some common system management tools that can be helpful in diagnosing problems related to system services, devices, and applications.

Computer Management Console

The Computer Management Console is a centralized place to manage the entire system, services, and applications. You can also manage disks, shared folders, and manager users and groups. It includes the Event Viewer utility, which is a great troubleshooting tool. To start the Computer Management console, right-click the My Computer Icon on the desktop and select Manage. You can also access this console from the Administrative Tools folder in the Start menu.

Device Manager

The Device Manager utility helps manage and troubleshoot hardware devices and drivers. This utility is a part of the Computer Management console. You can also access this utility from the Hardware tab inside System Properties in the Control Panel. Device Manager can be used to check whether a device is working or not and what resources it is using, to uninstall or update drivers, and to rollback to a previously working driver in case a newly installed driver does not work.

Task Manager

The Task Manager provides a real-time view of system performance including CPU, memory, processes, networking, and applications. You can end an application or a process if it is stalled or not responding. The Processes tab provides a view of how much memory and CPU time each process is using. The Performance tab provides a graphical view of the CPU and paging file usage. The Networking tab (Windows XP) provides statistics about network connection and percentage of network utilization. The Users tab (Windows XP) provides information about users currently connected to the computer.

MSCONFIG (Windows XP)

The *msconfig.exe* command opens the System Configuration Utility window. This utility is helpful in verifying the system startup environment. The options for managing system startup include boot options, services, and applications configured for auto-start. You can use this utility to configure the system to start in a diagnostic mode by selecting items from a given menu.

REGEDIT and REGEDT32

The *regedit.exe* and *regedt32.exe* commands are used to edit the settings stored in the Windows Registry. The Windows Registry is a collection of system configuration settings in a hierarchical data file. The configuration data includes the operating system settings, user specific settings, application data, hardware components, and all installed device drivers. Under extreme circumstances, if you need to make changes to the Registry, you should first make a backup copy of the existing Registry files. It can either be run from the command prompt or from the Run option in the Start menu.

Event Viewer

The Event Viewer console displays error messages, warnings, and other information about system activities. It is also used to view the contents of log files and includes tools to search particular events from the logs. You can open the Event Viewer console from the Administrative Tools utility in the Control Panel or from the Computer Management console. The Application Log contains errors, warnings, or other information generated by application programs. The Security Log contains errors, warnings, and information about security events and security problems such as incorrect logons that are included here by default. The System Log contains errors, warnings, and information about system events such as system startup and shutdown, services, and devices and drivers. You can use the Log Filtering feature in the event viewer to search for specific events.

File management utilities. In this section, we will look at some common file management tools that can be helpful in troubleshooting problems related to files and folders.

Windows Explorer

Windows Explorer is perhaps the most commonly used utility to manage files and folders. You can manage all aspects of files and folders, configure sharing, set sharing and NTFS permissions, copy and move files and folders, and even format disk partitions.

The ATTRIB command

The *attrib.exe* command is run from the Windows command prompt to view or change the attributes of a file or folder. File attributes include System (S), Read-only (R), Hidden (H), and Archive (A). The System attribute protects critical system files from being displayed or deleted by making them read-only and hidden. The Read-only attribute prevents a file from being deleted accidentally or deliberately. The Hidden attribute prevents a file or folder to be displayed in Windows Explorer. The Archive attribute sets the archive bit on files so that they are included in the next backup. Use the plus sign (+) with an attribute to set it and use the minus sign (–) to remove the attribute. For example, the command `attrib textfile.doc +h` will make the file hidden.

The EDIT command

The *edit.com* command is used to edit text files in the Windows command shell. The files are saved in ASCII file format.

COPY and XCOPY commands

Although most of the file copy operations can be performed using Windows Explorer, the *copy* and *xcopy* commands are still used frequently from the command line to copy files from one location to another. These commands include a number of optional parameters. You can type `copy /?` or `xcopy /?` at the command prompt to view the syntax of the commands and a list of available switches.

Windows Reporting. Windows includes a utility called Error Reporting that sends error messages and symptoms of the error to Microsoft when an application fails. This utility works well for those computers that are connected to the Internet. Microsoft collects this information to check the cause of application failure and make improvements in its applications such as MS Word, MS Excel, etc. This utility is enabled by default. If disabled, you can enable the utility by completing the following steps:

1. Click Start → Control Panel → System, or right-click My Computer and select Properties.
2. Click the Advanced Tab and click Error Reporting to open the Error Reporting window.
3. Click the Enable Error Reporting radio button.
4. Click Choose Programs and select the appropriate options by clicking the Add button.
5. Click OK and close all Windows.

Preventive Maintenance (PM)

PM for the operating system helps maintain system performance and reduces the chances of system failures. In this section, we will take a look at some common preventive maintenance procedures.

Software updates

Software updates keep the operating system and application software up-to-date. Software vendors regularly release updates to fix known bugs in their applications. For example, Microsoft regularly releases updates for its operating systems and applications such as MS Office to address operating problems. These updates are described in the following list.

Although most vendors provide software updates free of cost, it is good to test them before installing them on multiple computers. Do not install updates only because it is offered without charge. Verify with the vendor or from documentation about the specific issues that an update addresses.

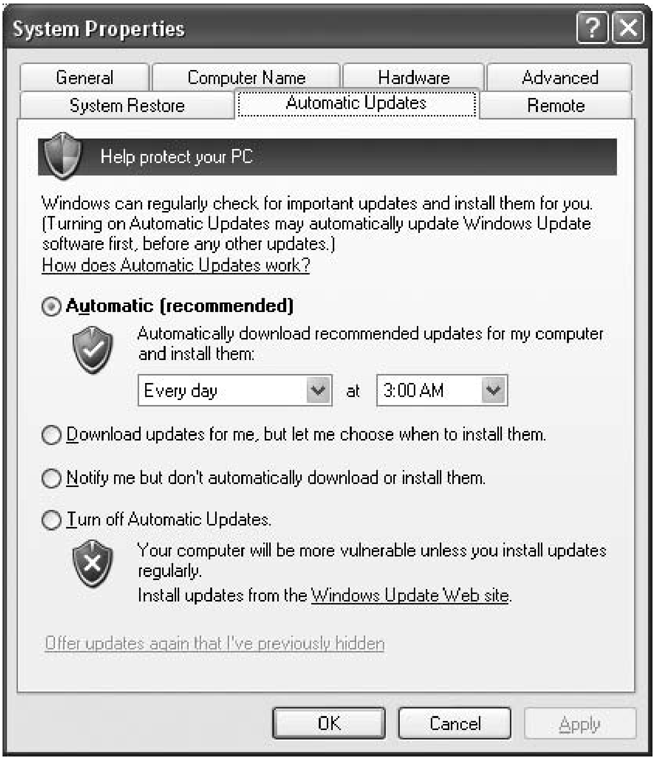
Hotfixes
Small pieces of software that are used to address a specific problem with the operating system or an application.

Patches
Usually meant to immediately address some security-related issue with the operating system.

Service Packs
A collection of a number of hotfixes and updates released by the software manufacturer. Manufacturers usually test service packs on a variety of hardware platforms and check their compatibility with various applications.

Windows Update

Windows Update (or Automatic Updates) is a built-in feature for Windows-based operating systems. This feature can be configured to automatically check for, download, and install updates to the installed operating system. This utility can be accessed from the Start menu or from the System properties window located in the Control Panel. Refer to Figure 2-13, which shows the Automatic Updates page in Windows XP.



Windows can regularly check for important updates and install them for you. (Turning on Automatic Updates may automatically update Windows Update software first, before any other updates.)

How does Automatic Updates work?

● Automatic (recommended)

Automatically download recommended updates for my computer and install them:

Every day at 3:00 AM

○ Download updates for me, but let me choose when to install them.

○ Notify me but don't automatically download or install them.

○ Turn off Automatic Updates.

Your computer will be more vulnerable unless you install updates regularly.

Install updates from the Windows Update Web site.

Offer updates again that I've previously hidden

Figure 2-13. Automatic Updates

A user can configure Windows Update options in one of the following ways:

- Automatic (with user selected days and timings).
- Download updates for me, but let me choose when to install them.
- Notify me but don't automatically download or install them.
- Turn off Automatic Updates.

When Automatic Updates are configured for particular days and times, the computer should be left connected to the Internet so that Microsoft's web site can check for new updates and install them as required.

Data backup and restoration

Data backup is one of the most important aspects of preventive maintenance. It ensures that data will be available even when a system crashes or in the event of a disaster. As a technician, you must be aware of the software or built-in utilities available for data backups. Data can be backed up using one or more types of backup methods. Magnetic tapes are very popular as backup media due to their large storage capacity, but you can also back up on CD-RW disks or on a network drive. Backup tapes must be safely stored at an off-site and secure location.

On Windows operating systems, backup of a single computer can be taken using the Windows Backup utility. Remember that this utility can also back up data stored on other network drives. This utility can back up the entire contents of a disk including the operating system data, which is called the *System State Data*. You can also create ASR disks that are helpful in restoring the system in the event of a system crash.

> Remember that Windows XP and Windows 2000 cannot back up data directly onto CD-RW and DVD disks. However, you can copy data to a hard drive or to a shared network folder and then burn a CD-RW or a DVD disk.

Backed-up data is useless if it cannot be restored. You must perform test restores periodically to ensure that the restoration methods used are working properly and that the data is being correctly backed up as desired.

Antivirus software

Antivirus software keeps track of viruses and other malicious software. It helps protect the system from viruses, Trojan horses, worms, and other malware such as spyware and adware. Antivirus software uses virus signatures to detect the presence of malicious software. You must run antivirus software often to detect the presence of malicious code in the computer. Virus signatures must be updated regularly so that the antivirus application can effectively detect and clean the system of any new viruses.

Creating System Restore Points

The System Restore utility in Windows XP uses System Restore Points to restore an unstable system to a working state. A System Restore Point stores a snapshot of system settings at regular intervals. You can create System Restore Points manually when you expect to make changes to your system. The following steps explain how you can create a System Restore Point:

1. Click Start → All Programs → Accessories → System Tools → System Restore.
2. Click Create A Restore Point, and then click Next.
3. Type a name to identify the restore point in the Restore Point Description box.
4. Click Create.

Printers and Scanners

Printers are output devices that convert the electronic information into hard copy and reproduce the output on a piece of paper. *Scanners*, on the other hand, are input devices that read information from a piece of paper and convert it into electrical signals. Both of these devices are electromechanical, meaning that they use electrical/electronic and mechanical parts to do their jobs. Here we will discuss some fundamentals of using printers and scanners and installing them, and take a look at the available tools to diagnose common problems.

Printer and Scanner Technologies

Printers and scanners are available in different types and forms, with varying capabilities and pricing, depending on the technology they are built upon. In this section, we will take a look at the printing and scanning technologies, their components, and how they are connected to computers.

Laser printers

Laser printers use a sharp beam of light, the *laser beam*, to produce the text or image on paper. This is called the ElectroPhotographic (EP) process, originally developed by Xerox, and it is based on use of static electricity to transfer the ink, which is in the form of toner, to the paper according to electrical signals received from the computer. They are used for high-quality text and image printing, have faster speed than other printers, and have low cost of printing per page. Laser printers are known as *page printers* and their printing speed is represented as *pages per minute (ppm)*.

Components of a laser printer. An internal view of the laser printer is shown in Figure 2-14. Different parts of a laser printer are as follows:

Main power supply
The main power supply converts the AC voltage into DC voltage used in various circuit boards and other parts of the printer. These DC voltages include +24 volts, +5 volts, and –5 volts.

High-voltage power supply
The high-voltage power supply produces very high voltages used in the printing process. These high voltages are used to charge the EP drum, the toner, paper, and the corona wires.

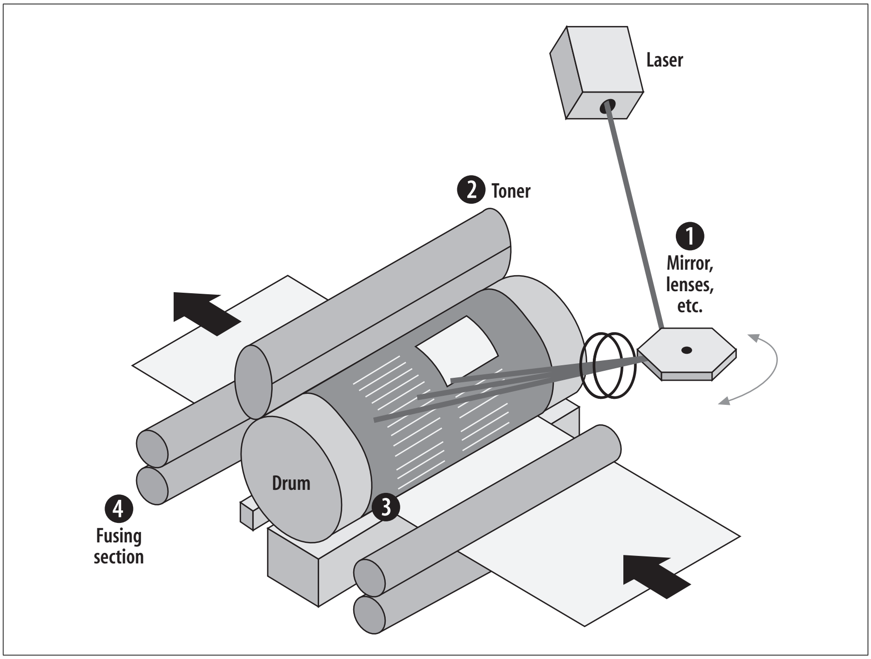


Figure 2-14. Components of a laser printer

EP drum
: The EP drum is a revolving cylinder coated with a highly photoconductive material (also called a *photoreceptor*). This drum is charged with high negative voltage (–600 volts) by the primary corona wire. As the drum rotates, a highly focused laser beam strips the charge from certain points on the drum.

Main motor assembly
: This assembly is used for movement of different rollers in the laser printer.

Scanning motor assembly
: Parts in this assembly contain motors and mirrors to move the laser beam across the EP drum.

Primary corona wire
: The primary corona wire is used to charge the EP drum with a high negative voltage (–600 volts).

Transfer corona wire
: The transfer corona wire is used to charge the paper surface with a high positive voltage so that it can attract the negatively charged toner.

Writing mechanism
: The writing mechanism guides the laser beam across the EP drum according to the image stored in the printer memory.

Toner cartridge
: The toner cartridge is made up of several subassemblies that include toner, developer, and a cleaner blade.

Fuser assembly

The fuser assembly contains heat and pressure rollers to properly bond the toner particles to the paper.

Erasing mechanism

The erasing mechanism is used to remove the image from the EP drum after the image has been transferred to the paper.

Cleaning assembly

This assembly is used to remove the residual toner particles from the surface of the EP drum.

Paper movement assembly

This assembly is used to move the paper through different parts of the printer.

Electronic control package

This unit (also known as the logic assembly) contains the main circuit board of the printer that communicates with computers to receive print jobs. This assembly contains the raster image processor (RIP) that converts the incoming signals into signals used by other sections of the printer.

Control panel

This is the main user interface located on the top of the printer and contains different controls/buttons for the user. High-end laser printers might include a touch screen as well as buttons to get user input.

Connection interface

This connects the printer to the computer or to the network. It can be a parallel, serial, USB, IEEE 1394, or a network port (for network printers), depending on the type of printer.

> Some laser printers use *corona rollers* instead of *corona wires* in order to transfer the high voltage. Corona rollers are considered environment-friendly because they help reduce the emission of ozone gas during the high-voltage transfer process.

The Laser printing process. The following is the printing process used in most laser printers:

Cleaning

The EP drum must be clean of toner particles leftover from the previous image before it can take a new image on its surface. A *rubber blade* in the cleaning assembly removes the particles of toner residing on the drum surface. The removed toner is collected in the debris cavity or waste reservoir located on one side of the cleaning unit. A *discharge lamp* having a specific wavelength then removes the remaining charge from the drum. After the charge is removed, the drum becomes electrically neutral.

Conditioning

The electrically neutral drum is insensitive to light and cannot take any image. A very thin wire, called the *primary corona wire*, is used to distribute a high negative charge (–600 to –1000 volts) evenly on the surface of the drum. This negative charge again makes the drum photosensitive or photoconductive.

Writing

At this stage of the process, the printer's laser beam writing unit and a series of mirrors are used to draw tiny dots on the EP drum, which represent the final image to be produced. The area of the drum that the laser beam comes in contact with loses some of its negative charge (by approximately −100V) and becomes relatively more positive (the charge is still considered negative, just not as negative as the areas not hit by the laser beam). When the laser beam has finished creating the image on the relatively positive EP drum, the printer's controller starts the paper sheet-feed process by pulling a sheet of paper into the printer. The paper stands ready at the printer's registration rollers until the controller directs it further into the printer.

Developing

The drum is rolled in a toner reservoir containing fine dry plastic particles mixed with carbon black or coloring agents. These toner particles are charged with –200 to –500 volts. The charged toner particles are electrostatically attracted to the drum's surface where the laser light left the image. The surface of the drum now holds the image pattern in the form of toner particles.

Transferring

The drum is pressed over rolled paper, which is positively charged. A different type of corona wire known as the *transfer corona wire* is used to charge the paper with very high positive charge. The positively charged paper attracts the toner particles from the drum leaving the image on the paper.

Fusing

The paper is passed through the *fuser* assembly containing *pressure rollers* and *heating rollers*. The rollers in the fuser assembly apply heat and pressure to the paper to firmly bond the toner particles to the paper surface. The heating rollers provide up to 200 degrees Celsius of temperature.

Once the printing process is complete, the printer paper is rolled out in an output tray. At the same time, the EP drum is cleaned of the residual toner particles and stripped of the negative charge to make it electrostatically neutral.

For the A+ exams, you must remember the steps in the laser printing process. Memorize all the voltages given in these steps. Note that the primary corona wire is used to transfer a high negative charge to the EP drum while the *transfer corona wire* is used to transfer a high positive charge to paper.

Inkjet printers

An inkjet printer creates text or image on the surface of paper by spraying small droplets of ink. The droplets are very small in size and are positioned very precisely. Inkjet printers are very popular because they are inexpensive, easy to use, and can produce high quality text and graphics. The speed of these printers is expressed as pages per minute (ppm) and resolution as dots per inch (dpi). Inkjet printers fall into the following categories:

Thermal Inkjet

These printers use water-, pigment-, or dye-based inks. The print cartridge contains small, electrically heated chambers. The printer runs a pulse of current through these chambers to produce steam that forms an ink bubble. This ink bubble is dropped on to the paper to form an image.

Piezoelectric Inkjet

These printers use a piezoelectric crystal in each nozzle instead of heating elements. The piezoelectric process uses crystals that react to electric charge. When charged, a crystal draws or pulls ink from an ink storage unit held above the crystal. In simple terms, the piezoelectric process can cut or refine the exact amount of ink needed to refine the dot placed on paper. This reduces the smudging effect of traditional inkjet technology and provides better printer resolution. In fact, this process allows resolutions greater than 1440 dpi.

Continuous Inkjet

These printers are mainly used for marking and coding of products. A high-pressure pump directs liquid ink from the ink reservoir into a small nozzle, thereby creating a continuous stream of tiny ink drops. A piezoelectric crystal creates ink droplets from the stream of ink. These tiny ink drops are electrically charged, which are further directed to printing paper.

Components of an inkjet printer. Inkjet printers consist of the following components:

Printhead assembly

The printhead assembly consists of a printhead, ink cartridge, printhead stepper motor, and belt. The *printhead* consists of a series of nozzles that spray the ink on to the paper. The *ink cartridge* contains the ink, which can be just black ink or a combination of different colors. The *stepper motor* is used to move the printhead assembly back and forth across the paper surface. The *belt* is used to attach the printhead assembly to the stepper motor. A *stabilizer bar* ensures that the movement of the printhead is precise.

Paper movement assembly

The paper movement assembly consists of a paper feed tray or feeder, a paper feed motor, paper sensors, and rollers. The *paper feed tray* or *feeder* is where the paper is loaded. The *paper feed motor* moves the paper through the printer with the help of rubber *rollers*. The stepper motor precisely moves the paper from the paper feed tray through the printer and drops it in the output tray after printing. Input *paper sensors* check the availability of paper in the paper feed tray.

Power supply

The power supply unit of the inkjet printer converts the mains AC voltage into the DC voltages used by various motors and circuit boards.

Controller assembly

The controller assembly consists of electronic circuitry that converts the incoming signals and controls the movement of different mechanical parts.

Connection interface

The connection interface connects the printer to the computer or to the network. Depending on the type of printer, the interface can be a parallel port, a serial port, a USB, or an IEEE 1394 port.

Inkjet printing process. The inkjet printing process involves the following steps:

1. The printing process starts with the cleaning of the printhead.
2. The controller assembly initiates the paper feed assembly. The stepper motor engages a number of rollers to pick a piece of paper from the paper tray and guides it into the printer. A sensor checks whether the tray is empty and gives an “Out of Paper” error.
3. The printhead stepper motor uses a belt to move the printhead assembly across the paper. This assembly stops at each point for a fraction of a second to spray multiple dots of ink on the paper surface and then moves again to the next position.
4. The paper feed motor moves the paper to the next line. This process continues until the printing process is complete.
5. Once the printing process is complete, the paper feed assembly pushes the paper onto the paper tray. The printhead is then *parked* in its home position.

Impact printers

Impact printers use a head or a needle that is hit against an ink ribbon to place a mark on paper. The paper is held firmly on a solid roller called a *platen*. These printers produce significant noise when they are operating but are considered very efficient for printing multipart forms such as invoices. Some of the commonly used impact printers include the following:

- Dot matrix printers
- Daisy wheel printers
- Line printers

The dot matrix printer is the most commonly used printer for personal and small business applications. The line printer is used where speed and volume of printing is a main requirement.

> The speed of line printers is expressed as *lines per minute (lpm)*, and the speed of dot matrix printers is expressed as *characters per second (cps)*. Similarly, the printing speed of laser printers and inkjet printers is expressed as pages per minute (ppm) because these printers are also called *page printers*. The printing speed varies by the quality of printing. The higher the resolution, the lower the printing speed.

Daisy wheel printers. As the name indicates, these printers use a wheel on the printhead that contains raised characters on its petals. During printing, the printhead moves the wheel to select the appropriate character on the petal in front of the electromechanical hammer (called *solenoid*). When the hammer strikes, it pushes the daisy wheel petal against an ink ribbon, which leaves a mark on the paper.

The movement of the paper, printhead, and daisy wheel is precisely bound by the control circuitry on the logic board (motherboard).

Dot matrix printers. *Dot matrix* refers to the way a printer creates text characters or images on paper. Dot matrix printers use a printhead containing a number of pins held vertically in one or two columns. Low-resolution printers have a printhead with 1 column of 9 pins while high-resolution printers have a printhead with 2 columns containing 24 pins. The pins strike on an ink ribbon that makes impressions on paper as small dots when the printhead moves back and forth. As the printhead moves in a horizontal direction, the printhead controller sends electrical signals and forces pins to strike against the ink ribbon. The timing of the electrical signals is programmed in the printer for every character it is able to print. The impressions appear as small dots and form appropriate characters on paper. It is possible to change the character style by electronically controlling how and when the pins strike the paper.

Thermal printers

Thermal printers use heated printhead pins that are pushed against heat-sensitive paper called *thermochromic paper* or *thermal paper*. Some fax machines (except plain paper faxes) and calculators with printing capability use the thermal printing process. These printers are inexpensive, but the cost of thermal paper is one of the considerations when calculating recurring cost of consumables. Thermal printers also use a combination of dots to create the text or image impression on paper. The following are two main types of thermal printers:

Direct thermal printers
: These create images by burning a matrix of dots on heat-sensitive paper when the paper is passed over a thermal printhead. The area of paper where it is stroked by the heated printhead turns black, while other areas remain white.

Thermal wax transfer
: These use wax-based ink, which is melted from the ribbon and transferred to the paper surface to create text or graphic images. The main disadvantage of this type of printer is that the same amount of ink is used, whether the output is full of text/images or only a part of the paper is printed.

Solid ink printers

Solid ink printers use sticks of solid ink instead of inkjet or toner cartridges. Once the stick is installed in a printer, the ink is melted and used to produce images on paper. These printers are mainly used in offices for printing high-quality graphics images. The printing process in solid ink printers is similar to that used in offset printing. The solid ink sticks are installed in printers. The ink is melted and fed into printheads that contain piezoelectric crystals. The printhead sprays the ink onto a rotating drum that is coated with oil. The paper is then passed over the drum that transfers the image onto the paper.

Solid ink printers can produce images on a variety of paper and even transparencies. The image quality is superb and better than many other printing technologies. Solid ink is helpful in protecting the environment due to reduced waste output. The disadvantages of solid ink printers include high power consumption and long warm up times.

Printer interfaces

Printers are connected to computers using standard interfaces such as parallel, serial, SCSI, USB, or IEEE 1394. Network capable printers have a built-in network interface and are connected directly to a network port. The following is a summary of different interfaces that can be used to connect printers:

Parallel

A parallel interface (IEEE 1284) works by sending an 8-bit parallel data stream to the printer. It uses a parallel printer cable, which has a DB-25 connector for connection to the computer and a 36-pin Centronics connector for connection to the printer. The maximum length of the parallel cable is usually limited to 10 feet.

Serial

A serial interface sends data to the printer one bit at a time. These interfaces need to be configured to serial communication parameters such as baud rate, parity bit, or start and stop bits. Serial printers are rarely used these days.

Universal Serial Bus (USB)

The USB is the most common type of printer interface used on small and medium-range printers (and many other peripherals). USB is faster than other types of interfaces. USB printers come with PnP-compatibility and can be automatically detected and configured by the operating system.

IEEE 1394

The IEEE 1394 (also called *Firewire*) interface is not built-in on many printers or computers and is mainly used where highly demanding printing applications are used.

Network

Most high-end printers come with a built-in network adapter or can be upgraded by installing one. These printers can be directly attached to one of the free network ports and can be assigned a network identification such as an IP address. The printer uses a standard network cable with an RJ-45 connector. In busy offices, a dedicated computer that is used to route all print jobs to the printer is called a *print server*.

Wireless

Computers and printers can also be connected using wireless connections that support 802.11, Bluetooth, or Infrared standards. The main advantage of wireless connections is that both the computer and the printer can be moved freely so long as they remain within the coverage area of the wireless network. Wireless networks mainly rely on radio signals and are prone to electromagnetic and radio frequency interferences.

Small Computer System Interface (SCSI)

Very few printers have a SCSI. These printers are becoming obsolete due to other, faster technologies such as the USB and the IEEE 1394. SCSI printers use the SCSI interface on the computer, and an SCSI ID is used to identify the device on the SCSI bus that can have more than one device attached to the SCSI chain.

Printer software

Printers come with their own software, which includes the following components:

Basic Input/Output System (BIOS)
: The printer BIOS or *firmware* is just like the computer BIOS that detects various components of the printer during startup. The BIOS is usually located on a semiconductor chip on the motherboard or logic board of the printer.

Printer driver
: A printer driver acts as an interface between the operating system and the printer. It converts print jobs into a format that the printer can understand. When you install a printer on a Windows XP or a Windows 2000 desktop, you will also be required to install the printer driver if the OS does not automatically configure it for you. Installing an incorrect printer driver results in garbled printing or no printing at all.

Page description language (PDL)
: The PDL is used to convert an incoming print job into electrical signals so that the text or the image can be reproduced on paper. Common PDLs include PostScript and *Printer Control Language (PCL)*.

Printer memory

Printers use RAM to temporarily store print jobs during printing. High-end printers have large amounts of RAM to accept large print jobs. Some printers also have a built-in hard disk that further helps improve printing performance. Some printers allow you to upgrade the printer memory to enhance its performance.

Printer supplies

Printer supplies include consumables such as inkjet or toner cartridges and paper. Printer supplies also include spare parts for repairs and upgrades. This section includes a brief summary of these supplies:

Paper and transparencies
: Printer paper and transparencies are collectively known as *print media*. Manufacturers always insist on using quality paper with their printers. This is due to the fact that using inferior or cheap paper might degrade the life of the printer components such as printheads and rubber rollers. Cheap paper also causes lots of printer problems including paper jams. Paper comes in different grades and sizes. The *letter* (8.5" × 11") size is the most commonly used, while *legal* (8.5" × 14") and *tabloid* (11" × 17") sizes are used for larger pages. The quality of paper is measured in terms of its weight, and the most common type of paper is 20-pound bond paper. Paper quality also differs by its brightness or whiteness. *Transparencies* are thin sheets of plastic used for presentations on LCD projectors. Transparencies are made for particular printers and should not be used on others. Consult the printer documentation or call the vendor to get specifications of the type of transparencies that can be used with a particular printer.

Ink cartridges

Ink cartridges are used in inkjet and bubblejet printers. These cartridges are specifically made for each make and model of printer. Manufacturers usually provide instructions in printer documentation as well as on printers (near the printhead assembly) on the type of cartridge used in the printer.

Ribbons

Ribbons are used in daisy wheel and dot-matrix printers. As with ink cartridges, the ribbons are also different for different types of printers.

Toner cartridges

Toner cartridges are used in laser printers. Different types of laser printers use different types of toner cartridges. Check the printer documentation to find out the correct type of toner used with your printer. Toner cartridges should be recycled when they become empty.

Spare parts

Manufacturers offer spare parts in order to repair printers. If a printer breaks down and you are responsible for carrying out the repairs, you will need to find out the part number of the part that you need to replace. Check the printer documentation, which usually includes identification numbers or part numbers for different components.

Optional upgrade components

Optional upgrade components usually include extra paper feed trays, finishing assemblies, and printer memory. You must make sure that the printer you need to upgrade has the options to upgrade, what optional components are available for upgrade, and how the upgrades are to be carried out. Consult the printer documentation or check with the manufacturer for printer-specific instructions.

Refilled ribbons, ink cartridges, and toner cartridges are usually available for common brands of printers. These products are cheaper but may not be able to provide good quality printing.

Types of scanners

Scanners are input devices that are used to take a snapshot of a paper containing text or images and then convert them into an electronic format or a document. This document can be saved as a file, altered and used to reproduce the image as another printed document, or used as part of any other electronic document. Scanners are widely used in the printing and publishing industry and even at home due to increased popularity of multifunction printers. Scanners are classified into the following main categories:

Flatbed

Flatbed scanners are the most widely used type of scanners. These use a glass platform where a paper is placed face down. A motorized belt moves a lamp to scan the image.

Handheld

Handheld scanners scan the image using the same method as a flatbed scanner, with the only difference being that the scanner is moved against the stationery image.

Sheet-fed

Sheet-fed scanners are commonly found in home printers. In these, the paper is moved over a scanning lamp that remains stationary.

Drum

Drum scanners are high-end scanners used in the printing and publishing industry to produce high-quality graphic images. The image to be scanned is placed on a glass drum or cylinder. The scanning process uses a PhotoMultiplier Tube (PMT) to convert the optical signals reflected from the image into an electrical signal.

Components of a scanner

The following is a summary of different components of a typical scanner and their functions:

Glass plate and scanner cover

The glass plate functions as a platform where the user places the document. In some scanners, the plate is made of acrylic. The scanner cover has a white surface and is used to keep the document in place during scanning.

Scanning head assembly

The scanning head contains a light source, a set of mirrors, and a lens that focuses the light onto a charged coupled device. The light source is made up of a *Cold Cathode Fluorescent Lamp (CCFL)*, which is used to illuminate the document surface. An array of *charged-coupled devices (CCDs)* or a *Contact Image Sensor (CIS)* converts the optical signals into electrical signals.

Stepper motor assembly

The stepper motor assembly is used to precisely move the scanning head across the surface of the document. The scanning head is attached to the stepper motor using a belt.

Driver software

The device driver acts as an interface between the scanner and the operating system.

> The components of a scanner depend on the type of scanner. For example, handheld scanners do not have a stepper motor assembly or any glass plate and cover. Similarly, sheet-fed scanners have a paper movement assembly instead of a scanning head movement assembly.

Scanning process. The scanning process involves the following steps:

1. The user places the document upside down on the glass plate and closes the scanner cover.

2. The document is illuminated by a CCFL.
3. The scanning head is moved across the document using a belt attached to the main stepper motor.
4. The image of the document is passed through a set of reflective mirrors and focused onto a lens.
5. The lens passes the image to an array of CCDs through an image filter.
6. The scanner driver passes the image of the document to the application software used to acquire the image from the scanner.
7. The applications (Photoshop, Corel Draw, etc.) use a standard language, such as *TWAIN*, that acts as an interpreter between the scanner and the application.

Scanner interfaces

As with printers, scanners can also be connected to computers using a variety of interfaces, which include the following:

- Parallel port
- Serial port
- USB port
- IEEE 1394/Firewire port
- SCSI port

Most of the newer scanners come with built-in USB or IEEE 1394 Firewire ports. Some older scanners used parallel, serial, and SCSI ports. You will need to refer to the particular scanner documentation for specific instructions on connecting and configuring the scanner.

Installing, Configuring, and Upgrading Printers and Scanners

The A+ exams expect you to know the basic tasks involved in performing printer and scanner installations, configurations, and upgrades. These tasks include checking compatibility of the device with the operating system, obtaining device drivers, installing devices, and verifying the installation. You should also be familiar with the tasks that involve upgrading these devices. In this section, we will take a look at some of the common tasks that you might have to perform when working as a computer technician.

Installing printers and scanners

Installing a printer or scanner involves the following common tasks:

- Checking the compatibility of the device with the operating system installed on the computer.
- Obtaining necessary hardware, connection cables, and device drivers.
- Connecting the device to an appropriate port such as a parallel, serial, USB, IEEE 1394, SCSI, wired, or wireless network port.

- Installing the device driver if it is not automatically installed by the operating system.
- Configuring or calibrating the device.
- Verifying the installation and testing its functionality by printing a test page or by scanning text and graphics pages.

Verifying compatibility. It is important to verify the compatibility of a printer or scanner with the installed desktop or network operating system and applications before they are purchased. Compatibility with the operating system ensures that the documents will be correctly formatted before going to the printer or that the computer will correctly read the scanned images. Compatibility with the application software ensures that the application can successfully use the device. This is particularly applicable for scanners, which are mainly used by graphics applications such as Corel Draw and Photoshop. Most manufacturers test their devices and drivers with a variety of operating systems and applications to ensure flawless operability.

Connecting the device. A printer or scanner must be connected to an available computer port before its device driver can be installed or configured. In the case of a printer, you can connect it to a local port such as the parallel (LPT1 or LPT2), serial, (COM1 or COM2) or network port. You will need an appropriate cable to connect the device, such as the parallel printer cable or a network cable. Once the device is connected, hook up its power cable and turn it on. The device will perform a self-test and display a ready mode.

Install the device driver. Most new printers and scanners are PnP-compatible, which means that they are automatically configured when they are detected by the operating system. If this is not the case, you might have to install the device driver using the Add Hardware wizard utility in the Control Panel. The wizard will guide you through the installation process, during which you can select the device driver from the driver CD-ROM that comes with the product.

Installation of a printer driver completes with the printing of a test page that verifies that a correct driver has been installed and that the OS can successfully print a test page. Similarly, when you install a scanner driver, the scanner completes some self-test routines. You can scan an image or a text page and view it using a graphics application.

Configure the device. Configuring a printer or scanner includes tasks such as setting the default options and preferences. These tasks are performed using the Properties pages of the device that you can access from the Printers and Scanners utility available in the Start menu. Nearly all printers and scanners include a calibration option in the device Properties pages. Calibrating a scanner guarantees that it will correctly read the image using the configured resolution. Configuring a printer ensures that the default settings such as the paper type and orientation works well for most applications and the printer performance is optimized. Advanced configuration of devices depends on the type of the device—you might need to refer to the manufacturer's instructions.

Verifying installation. Installation can be tested using a built-in utility included with most printers and scanners. Windows XP and Windows 2000 include an option to print a test page to verify that the printer has been installed correctly. Similarly, acquiring a scanned image using a graphics application such as Photoshop or Corel Draw can test the scanner installation.

Upgrading printers

Printers can be upgraded in several different ways that include adding memory, updating printer driver and firmware, and installing optional components such as additional paper trays. This section summarizes the common upgrade options available for printers.

Memory. High-end laser printers require a large amount of built-in RAM to temporarily store the documents submitted for printing. The larger the amount of RAM, the larger the number of documents a printer can accept for printing. Most of these printers have the option to extend the memory by installing additional memory modules or memory sticks. In most cases, the manufacturer's support technicians perform the memory upgrades. If you are asked to upgrade a printer's memory, you will need to make sure that expansion slots are available in the printer to upgrade the memory, and that the memory modules are compatible with the make and model of the printer. It is recommended that you obtain the memory module directly from the printer manufacturer and ask for necessary installation instructions. If none are available, you should refer to printer documentation for help.

Drivers. Like most software and hardware vendors, printer manufacturers also regularly update the printer drivers and make these updated drivers available free of cost on their web sites. This usually happens when the operating system is upgraded on the print server. Printer manufactures also update printer drivers for their old printers to make them compatible with the new version of the OS. Updated or new printer drivers must be tested before they are finally installed on print servers.

On a Windows XP desktop, a printer driver can be updated from the Advanced tab of the printer Properties window. Click on the New Driver tab to launch the Add Printer Driver Wizard. The Wizard guides you through the installation process, which is more or less similar to the process for installing a new printer driver.

> Note that the Rollback Driver feature in Device Manager is not available for printers. If a new updated printer driver does not work for some reason, you will have to manually reinstall the previous version from the printer Properties window.

Firmware. Firmware refers to the BIOS of the printers or scanners. In some cases, it is necessary to upgrade the firmware to take advantage of new or advanced features of the device. Firmware upgrades are usually done by either replacing the firmware chip in the device or through the software application provided by the device manufacturer. You should consult the device documentation and follow the manufacturer's instructions on how to obtain and install firmware updates.

Network interface. Most high-end printers are network-capable these days. They can be directly connected to an available network port and given some other identification. For example, most network printers can be assigned an IP address. Some manufacturers do not include the network interface with the standard printer but offer it as an upgrade. In other situations, you might have to upgrade the network interface of an older network printer to increase its communication speed. Follow the manufacturer's instructions or refer to the instruction manual to complete the upgrade.

Paper feed trays and finishers. Several printer manufacturers do not include all types of paper feed trays or finishing assemblies (folder, hole puncher, and stapler) with the standard product. These parts are offered as optional upgrades. This is due to the fact that the manufacturers want to keep the price of the standard product to a minimum. If required, a consumer can just order these. In most circumstances, a service representative of the manufacturer installs these upgrades. You will need to follow the manufacturer's instructions on how to install paper feed trays or finishing assemblies.

Troubleshooting Printers and Scanners

Printers are used at almost every place where computers are used. Most printers are now easy to use but are also difficult to troubleshoot. All-in-one, low-cost inkjet printers now include the functionality of a fax machine and scanner. In this section, we will take a look at troubleshooting some common problems related to printers and scanners. But first, we will summarize the basic troubleshooting procedure that applies to both printers as well as scanners.

Basic troubleshooting procedures

The following is a summary of basic troubleshooting procedures. Remember that this is a generalized troubleshooting procedure that can be applied to any situation:

1. Gather information. The first step in every troubleshooting scenario is to gather as much information about the problem as you can. Ask questions from the user, take a look at the errors generated by the device, try printing a test page, or check the event logs on the computer. You may need to use any one or all of these methods to get sufficient information about the problem. Check with the user if he has tried to make any changes to software or changed anything with the device hardware. It might also be helpful to use the troubleshooting utility included with the specific device.
2. Analyze collected data. Next, you will need to review and analyze the information you collected to identify one or more possible causes of the problem. Check the device documentation to find out what could have caused the problem. In some cases, checking with the vendor's documentation on the web site also helps a lot.

3. Identify the most probable cause. You will need to isolate the problem and identify the most probable cause that has generated the problem. This can be done by eliminating the causes that are not directly related to the problem.
4. Apply the solution. Once you have identified the correct cause of the problem, you are ready to find a suitable corrective action. This may be in the form of simply recycling power to the device or a change in user permissions, or it might be as complex as replacing a component. Once the solution is applied, you must test that the solution works well and does not give rise to further problems.

Troubleshooting inkjet printers

The following sections summarize the symptoms of common problems with inkjet printers, as well as their possible causes and solutions:

Paper jams

Paper jams are a result of obstruction in the path that the paper travels within the printer. Paper jams are mainly caused by one of the following reasons:

- Worn out rollers in the paper movement assembly
- Incorrect type of paper
- Poor quality of paper

Remember that loose paper sheets pick up moisture from the atmosphere that can also cause paper jams.

Poor printing quality

There can be several reasons behind poor printing quality. Some of them are as follows:

- Dry ink in the ink cartridge
- Damaged ink cartridge
- Alignment of printhead

Poor printing quality is a major problem where refilled ink cartridges are heavily used. Even when you buy a new printer or replace an ink cartridge and do not use it for long, the ink becomes dry. Misalignment of the printhead can also cause poor printing quality. (A simple symptom of a misaligned printhead is that horizontal or vertical straight lines do not look straight. Most printers have a built-in utility to align printer heads.) Another reason for poor printing quality is that the printhead needs to be cleaned.

Blank pages

If the printer or the application does not produce any errors but blank pages are coming out of the printer, the ink cartridge is out of ink and should be replaced.

Patches on ink

If the inkjet printer is leaving patches of ink scattered across different parts of paper, or if the printed characters look smeared, the inkjet cartridge needs to be replaced.

Troubleshooting laser printers

The following list summarizes some common problems with laser printers, as well as their possible causes and solutions:

Paper jams

Paper jams are mainly caused by poor paper quality or worn out pick-up rollers. A broken gear may also cause this problem. The only solution is to replace the gear or the roller, whichever might be causing the problem. Always use a vendor-recommended paper supply and keep paper inside plastic jackets. Loose paper picks up moisture, which can also cause paper jams. Perform preventive maintenance at regular intervals so that the paper path remains clear of dust and paper particles.

Blank pages

A laser printer produces blank pages due to one of the following reasons:

- The toner cartridge is out of toner and needs replacement.
- The transfer corona wire assembly is faulty. If the wire is broken or damaged, the image cannot be transferred from the EP drum to the paper. It is easy to replace a broken transfer corona wire.
- The high-voltage power supply is not functioning. High voltage charges the primary and transfer corona wires. If the high-voltage power supply is not working, both corona wires will not be able to do their respective jobs.

Black pages

A faulty primary corona wire causes black pages. If this wire is not working, it cannot strip the EP drum of high negative voltage. The toner sticks to the entire surface of the EP drum, which is then transferred to the paper.

Toner marks scattered across paper

Repetitive toner marks scattered across the paper is a result of some problem with the toner cartridge. This problem is very common with refilled toner cartridges.

Vertical black or white lines

This problem is due to a defect on the surface of the EP drum. There might be a little scratch on the drum where it cannot get the high-voltage charge and attract the toner particles.

Image ghosting

Ghosted images appear when the previous image is not completely erased from the surface of the EP drum. A broken cleaning rubber blade or some other defect in the erasure lamp assembly causes ghosted images on paper. Depending on the situation, you might need to replace the defective erasure lamp or the cleaning rubber blade.

Garbled printing

An incorrect printer driver mainly causes garbled printing output. Reinstall the driver to correct this problem.

Troubleshooting dot matrix printers

The following list summarizes some common problems with dot-matrix printers, as well as their possible causes and solutions:

Paper jams

Paper jam problems are very common in dot matrix printers. This is due to the fact that they are mainly used to print multipart forms with perforations. The paper used for these forms is usually not of very good quality. Moreover, they use continuous sheets of paper, which if not monitored during printing, can easily skip a hole, get misaligned, and cause paper jams. It is very common to find small pieces of paper sticking to the paper feed assembly inside the printer. Dot matrix printers need regular preventive maintenance so that the paper path can be kept clear.

Poor printing quality

As noted earlier, poor printing quality can be caused by several factors. The following is a list of some common causes of poor printing quality:

- If you see a blank line across the width of the paper, one of the pins on the printhead is broken.
- If the printer is printing nonreadable characters (garbled prints), the problem lies with the printer driver software.
- If the printer is producing consistently faded characters, the printing ribbon needs to be replaced.
- If the printer is producing normal printing noise but nothing appears on paper, the printing ribbon might be improperly installed or out of ink.
- If you notice that the printing quality reduces across the width of the paper, the ribbon is possibly not rotating. Check the ribbon movement assembly that advances the ribbon when the printhead moves.

Stepper movement problems

Dot matrix printers rely on stepper motors for paper movement as well as for movement of the printhead. A problem with the stepper motor is easy to identify because it causes irregular movement of the printhead or the paper. The stepper motor is an expensive part, and the only way to enhance its life is to perform regular preventive maintenance of the printer.

Common problems with scanners

The following are some of the common operational problems with scanners:

Scanner does not scan

If the scanner is powered on but does not scan when commands are issued from the application, try to scan the document manually using the Scan button located on the scanner's control panel. If both actions fail to start the scanning process, reboot the computer and the scanner to see if the problem persists. With some scanners, it is required that the scanner should be powered on before the computer. Check that the lock of the scanning head is not blocking its movement. If this does not resolve the problem, reinstall the scanner driver.

Poor image quality of scanned document

Poor quality of the scanned document can either be caused by incorrect scanning resolution or by dust on the glass plate, scanning lamps, or mirrors.

Scanner produces strange noise

Scanners usually produce strange noises when they are powered on. This is due to the fact that the scanner must perform its self-test and calibrate its different settings on start-up. If the noise is heard every time you turn on the scanner, do not be alarmed. It is a normal process. If the noise continues and the scanner does not complete scanning a document, you may need to look at the movement of the scanning head.

Scanner does not power on

If the scanner does not turn on when you press the power button or the switch, check that the mains AC cord is plugged in properly to the scanner as well as to the wall socket. If the mains cord is properly plugged in, try replacing the cord with another good cord.

Networks

Networks allow computer users to connect computers together and share resources such as files and printers. Networking also allows better management of data, security, and resources in large companies where hundreds of employees work on computers. In this section, we will cover some basic fundamentals of computer networks, installation of networks, and common troubleshooting methods.

Networking Fundamentals

A computer network refers to two or more computers linked together to share files, printers, and other resources. The network may be as small as just two or more computers linked together at home or in an office, or as big as a corporate network at multiple locations spanned across the globe.

Chapter 8 covers a detailed study of computer networks.

Types of networks

The following are main categories of computer networks:

Local area network (LAN)

A LAN is a network of computers joined together in a local area such as a small office, home, or building. The area covered by a LAN is usually restricted to a single location. The function of a LAN is to provide high-speed connectivity to all computers and network devices.

Wide area network (WAN)

A WAN is a network that connects two or more local area networks. A WAN typically connects separate LANs at different geographic locations. A third-party such as an Internet service provider or a local telephone company is responsible for providing the required dedicated hardware and/or connectivity lines to implement a WAN. These hardware devices include modems or routers that are required to connect the local LANs to the service providers network.

Personal area network (PAN)
A PAN refers to a network of devices located in close proximity of each other. The devices may include computers, PDAs, mobile phones, and similar items, connected using a wireless or a wired network.

Metropolitan area network (MAN)
A MAN is a large internetwork connecting local area networks in a campus or inside the boundaries of one city.

Networking models

Networking models can be divided into the following two categories:

- Centralized computing
- Decentralized computing

In a centralized computing network model, all processing is done on a central computer. This computer provides data storage as well as controls to all peripherals including the clients, which are called *dumb terminals*. A *client/server* network is based on the centralized computing model. A centralized server holds control of all system and network resources located across the network. These include network services, storage, data backup, security management, and access control. The network consists of dedicated servers and desktops (clients). Servers run network operating systems such as Windows Server 2000/2003, Unix/Linux, etc., and the desktops run client operating systems such as Windows XP or Windows 2000. The following are some features of client/server computing:

- This model is scalable to very large-scale internetworks.
- Skilled administrators are required to manage the network.
- Dedicated server and network hardware may be required, which increases the cost of ownership.
- Security of the resources can be effectively maintained from a central point.

In a decentralized computing network model, all processing and resources are distributed among several computers, thereby increasing performance. All systems can run independent of each other. A *peer-to-peer (P2P)* network or a *workgroup* is based on a decentralized computing model. Every computer is responsible for processing applications, storage of data, and controlling access to its resources. The following are some features of a peer-to-peer networking model:

- These networks are suitable for about 10 computers only.
- They are cost effective as compared to the client/server model.
- A *network operating system* (NOS) or skilled administrators are not required.
- These networks are not as secure as the client/server model because each user individually maintains security of resources on her computer.

Network topologies

A *topology* refers to the physical layout of a network. It describes how networking devices such as servers, desktops, printers, and network devices are connected together.

Star topology

In a star topology, computers (or nodes) connect to each other through a central device, called a *hub* or a *switch*. Since each device is connected independently to the central device using a separate cable, the star network can be expanded at any time without affecting the operation of the network. Failure of one or more nodes also does not affect the network operation. The central device becomes the single point of failure because all nodes are connected to it.

Bus topology

In a bus topology, all computers are connected to a single cable called a *backbone* using *T-connectors*. Both ends of the backbone use *terminators* in order to prevent reflection of signals. If the terminator is missing or is deliberately removed, the data transmissions are disrupted.

Mesh topology

In a mesh topology, each computer makes a point-to-point connection to every other computer. This makes the network highly fault-tolerant and reliable because a break in the cable or a faulty computer does not effect network operation. Data can travel from one computer to another using a number of paths.

Ring topology

In a ring topology, each computer is connected to its neighboring computer to form a logical ring. If one of the computers in the ring fails or if the cable is broken, the entire network becomes inaccessible. Addition or removal of computers also disrupts network transmissions. A *Multi-Station Access Unit (MSAU)* or *Media Access Unit (MAU)* acts as the central device.

Wireless topology

In a wireless topology, computers connect to each other using radio frequencies. Wireless networks can be either *Ad-hoc* or *Infrastructure* topology-based. In an ad-hoc wireless network, two or more computers directly communicate to each other without using a central device. There is no central device (hub), and these networks can be created anywhere almost spontaneously. In an *Infrastructure* network, a central wireless device known as the *Access Point (AP)* is used to authenticate and configure wireless clients that fall within its range. A special identifier known as the *Service Set Identifier (SSID)* must be configured on the AP and each wireless client. The AP can further be connected to the wired LAN so that wireless clients can access the wired LAN also.

Full-duplex and half-duplex. In computer networking, a *duplex* communication system is the one where data can be transmitted and received simultaneously in both directions. In a *half-duplex* communication, setup data can flow in both directions, but only in one direction at a time. If one end is transmitting data, it cannot receive at the same time. In a *full-duplex* communication setup, both ends can transmit and receive data simultaneously.

Network cabling

The cables used for computer networks fall into three main categories: coaxial (thin and thick), twisted pair (unshielded and shielded), and fiber optic (single-mode and multi-mode). Each of the cable types has its own merits and demerits in terms of their cost, installation, maintenance, and susceptibility to interferences. Coaxial cables are not covered in the A+ Essentials exam as these are rarely used these days.

Twisted pair cables. Twisted pair cables use pairs of insulated cables bundled inside a plastic sheath. The twists in cables are used to prevent electromagnetic interference, which results in crosstalk among cables. Twisted pair cables are easy to install and lower in cost than coaxial and fiber optic cables. These cables are identified by their category numbers, denoted as CAT-1, CAT-2, CAT-3, CAT-5, etc. Figure 2-15 shows a piece of a twisted pair cable.

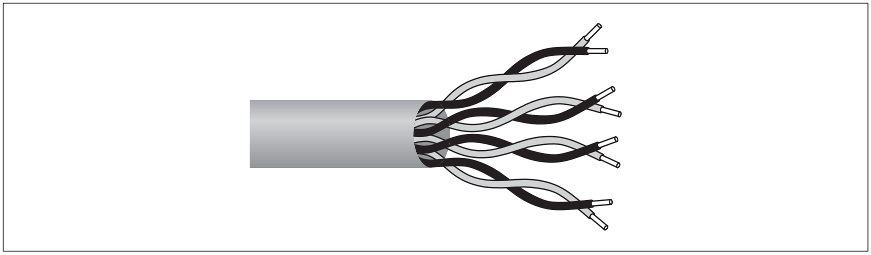


Figure 2-15. Twisted pair cable

Unshielded twisted pair

Unshielded twisted pair (UTP) cables are the most commonly used of the two types of twisted pair cable categories. UTP cables are inexpensive and easy to install and maintain. These cables are vulnerable to electromagnetic interferences (EMI) and radio frequencies interferences (RFI) and hence cannot carry data signals to longer distances.

Shielded twisted pair

Shielded twisted pair (STP) cables come with a layer of shielding material between the cables and the sheath. STP cables do provide some degree of protection from EMI and RF disturbances and can carry signals to greater distances. But this advantage comes with extra cost of installation.

Table 2-11 lists some of the popular UTP and STP categories.

Table 2-11. Categories of UTP and STP cables

Category	Description
CAT-3	Used for both voice and data transmissions in Ethernet, Fast Ethernet, and Token Ring networks.
CAT-4	Used for both voice and data transmissions in Ethernet, Fast Ethernet, and Token Ring networks.
CAT-5	Used for both voice and data transmissions in Ethernet, Fast Ethernet, Token Ring, and ATM networks.

Table 2-11. Categories of UTP and STP cables (continued)

Category	Description
CAT-5e	Used in Gigabit Ethernet networks.
CAT-6	Used for both voice and data transmissions in Ethernet, Fast Ethernet, Token Ring, and ATM networks.
CAT-6 (STP)	Used for data transmissions in Ethernet, Fast Ethernet, Gigabit Ethernet, Token Ring, and ATM networks.

Plenum/PVC. The term *plenum* refers to the space between the main ceiling and the dropped ceiling of a building. This space is used for air circulation in heating and air-conditioning systems. The network cable used in this space is known as *plenum cable*. A fire-retardant plastic jacket surrounds the plenum cable. The jacket consists of a low smoke *polyvinyl chloride (PVC)* or *fluorinated ethylene polymer (FEP)*. These cables are highly resistant to fire and should be used in plenum space. UTP and STP cables should not be used in this space because they pose a serious fire hazard in case of a fire.

Fiber optic. Fiber optic cable is made up of very thin glass or plastic stretched out and put inside a sheath. The transmission in fiber optic cables is carried by light signals and is immune to EMI and RF disturbances. They can also carry data signals to longer distances than UTP or STP cables and is considered the most secure of all cable types. Fiber optic cables are very expensive in terms of the cost involved in installation and maintenance. They need expensive hardware, skilled technicians, and special tools for installation. This is the reason that fiber optic cable is used only in data centers for providing high-end connections to critical servers and other network devices where high-speed data transfers are required. Figure 2-16 shows a fiber optic cable.

Figure 2-16. Fiber optic cable

Fiber optic cables fall into the following two categories:

Single-mode fiber optic cable
: The single-mode fiber optic cable is made up of 8 to 10 micron core glass or plastic fiber surrounded by 125 micron cladding. It uses a single beam of light and can thus travel to greater distances than multimode fiber optic cable.

Multimode fiber optic cable
: The multimode fiber optic cable is made up of 50 or 62.5 micron core and 125 micron cladding. In this cable, multiple beams of light travel through the core and are reflected by the cladding. Some of the beams even get refracted into the cladding causing loss of signal.

Connectors

Connectors are used for terminating cables and provide an interface to connect the cables to devices. It is not possible to connect a cable to a device without first terminating it with a suitable connector. Each connector has two variations: a male and a female. The following is a brief description of connectors used for computer networking:

Registered Jack-11 (RJ-11)
The RJ-11 connector is mainly used for terminating telephone wires. It has a capacity of three telephone lines (six pins) but only four pins are commonly used. A single telephone line uses only two pins. but four pins are used for a Digital Subscriber Line (DSL).

Registered Jack-45 (RJ-45)
The RJ-45 is an 8-pin connector that is used for terminating twisted pair cables. It is the most common type of connector used in computer networks. Cables can be wired in either a straight or *crossover* fashion.

Subscriber/Standard Connector (SC)
An SC connector is used to terminate fiber optic cables. It uses the push-pull mechanism to make the connection.

Straight Tip (ST)
An ST connector is an older type of fiber optic connector. It uses the "twist-on/twist-off" bayonet mechanism to make the connection.

Lucent (LC)
An LC connector is also used for fiber optic cables with a push-pull mechanism. It has a small flange on top that secures the connection in place.

Mechanical Transfer-Registered Jack (MT-RJ)
An MT-RJ connector resembles RJ type connectors. They always hold two fiber cables to allow full-duplex communications.

Universal Serial Bus (USB)
USB connectors are available in a variety of sizes and shapes, but the two most popular types are *USB Type A* and *USB Type B*. The Type A connector is mainly used on computers, and the Type B connectors are usually used for peripherals.

IEEE 1394
An IEEE 1394 connector is also known as *Firewire* connector. These connectors are mainly used for digital video and portable storage devices. The IEEE 1394 connectors come in 6-pin and 4-pin configurations.

Refer to Chapter 8, which shows figures of different types of network connectors.

Network devices

This section covers a brief description of commonly used networking devices, which include hubs, switches, MAUs, bridges, and routers.

Hubs. An *Ethernet hub* (or a *concentrator*) is the central device that connects all nodes in the segment. It receives signals on one of its ports and retransmits it to all other ports except the receiving port. In a typical implementation, UTP cables are used to connect nodes (computers or printers) to hubs. An *active hub* receives signals at its ports and regenerates it before passing it on to all other ports. A *passive hub* acts as a simple gateway for the incoming signals and does not regenerate the signal before passing it on to other ports. Ethernet hubs are available in a variety of sizes and costs, depending on the number of ports. Smaller hubs with 4, 8, or 12 ports are known as *workgroup hubs*, while hubs with 24 or 32 ports are known as *high-density hubs*. Hubs can be cascaded (joined together) to extend the network segment.

Switches

Like a hub, a *switch* is also the central device that connects multiple nodes in a network segment using UTP or STP cables. But unlike the hub that sends the received signal to every port, a switch sends the signal only to the destination node. A switch is an intelligent device that *learns* the hardware address or *Media Access Control (MAC)* address of the destination from the data packet and sends the packet only to the intended node. This results data direct communication between two nodes, improved network performance, and a reduced number of collisions.

Switches can work in a full-duplex mode, a mode that enables nodes to transmit and receive data simultaneously. Thus a 100 Mbps switch working in a full-duplex mode can provide 200 Mbps data transfer speed. Switches are preferred in large networks where hubs can become a bottleneck for network performance.

Media Access Unit (MAU). An MAU, also called Multi-Station Access Unit (MSAU), is used in Token Ring networks as a central device that connects all nodes in the network segment. This is equivalent to using a hub or a switch in Ethernet networks and results in giving the network a physical star look, though its logical topology remains a ring. Multiple MAUs can be connected using the *Ring In (RI)* and *Ring Out (RO)* ports in order to extend the network. The RO port of one MAU is connected to the RI port of the second MAU, and so on. The RO port of the last MAU is connected back to the RI port of the first MAU in the network to complete the ring.

Bridges. A network bridge is used for two purposes: connecting to LAN segments to form a larger segment and dividing a large network segment into smaller segments. Like network switches, bridges also learn the MAC address of the devices and forward data packets based on the destination MAC address. Most of the newer bridges can dynamically build lists of MAC addresses by analyzing data frames. These bridges are called learning bridges due to this advanced functionality. Most of the functionality of bridges is now included in switches.

Routers

Routers are used to connect two or more network segments. Routers use IP addresses to determine the source and destination of the data packet. Typically, routers receive the data packet, determine the destination IP address, and forward the packet to the next *hop* (which may either be the final destination of the packet or another router on the path). Routers can be implemented as a software service or as a dedicated hardware device. A wired or wireless router in a home network is an example of a small network router that connects the home network to the ISP's network.

Routers communicate to each other using *routing protocols*. Routers maintain a list of IP addresses in *routing tables*. Routing tables can be built statically or dynamically as discussed in the following sections:

Static routing
: When static routing is used, administrators manually configure routing tables by entering appropriate routing information. This method works only for very small networks.

Dynamic routing
: In a dynamic routing environment, routers use *Routing Information Protocol (RIP)* or *Open Shortest Path First (OSPF)* to build, maintain, and advertise their routing tables. Most networks are based on dynamic routing.

Networking protocols

Networking protocols allow computers to communicate to each other through the networking media. Some of these protocols are common to all operating systems while others are platform-dependent. This section covers a brief description of the commonly used protocols TCP/IP, IPX/SPX, and NetBEUI.

Transmission Control Protocol/Internet Protocol (TCP/IP). TCP/IP is a set of several protocols. It is the most widely used protocol suite in private networks as well as on the Internet. TCP/IP is not proprietary to any organization but is a public protocol suite. It is a fully routable protocol and is supported by all major network and desktop operating systems. Some of the well-known TCP/IP protocols and their functions are listed in Table 2-12.

Table 2-12. TCP/IP protocols and their functions

Protocol	Function
Internet Protocol (IP)	IP is a connection-less protocol that provides IP addressing and routing functions.
Transmission Control Protocol (TCP)	TCP is a connection-oriented protocol that guarantees delivery, flow control, error detection, error correction, and packet sequencing.
User Datagram Protocol (UDP)	UDP is a connection-less transport protocol. It does not provide guaranteed delivery of data.

Table 2-12. TCP/IP protocols and their functions (continued)

Protocol	Function
File Transfer Protocol (FTP)	FTP is a client/server application used for file transfers between remote computers.
Trivial File Transfer Protocol (TFTP)	TFTP is also used to transfer files between two remote computers. It is faster but less reliable than FTP.
Simple Mail Transfer Protocol (SMTP)	SMTP is used to transport messages between remote email servers.
HyperText Transfer Protocol (HTTP)	HTTP allows text, images, and multimedia to be downloaded from web sites.
HTTP Secure (HTTPS)	HTTPS is the secure version of the HTTP protocol that authenticates web servers and clients before the communication session starts.
Post Office Protocol 3 (POP3)	POP3 is used to download or retrieve email messages from mail servers running the SMTP protocol.
Internet Message Access Protocol 4 (IMAP4)	IMAP4 is also used to securely retrieve email from mail servers.
Telnet	Telnet allows connections to remote hosts such as network devices for administrative and maintenance purposes.
Internet Control Message Protocol (ICMP)	ICMP provides error checking and reporting functions.
Address Resolution Protocol (ARP)	ARP is used to resolve IP addresses to MAC addresses.
Network News Transfer Protocol (NNTP)	NNTP provides newsgroup services such as posting and retrieving messages on discussion forums.
Line Printer Remote (LPR)	LPR provides client connectivity to printers in network operating systems such as Unix, Linux, and Windows.

Internet Packet Exchange/Sequenced Packet Exchange (IPX/SPX). IPX/SPX is a full protocol suite used in Novell NetWare networks. The IPX/SPX protocol suite is fully routable, but due to the increasing popularity and extended features of the TCP/IP protocol suite, the usage of IPX/SPX has reduced significantly. Both Microsoft and Novell have made TCP/IP their default protocol in recent versions of operating systems. Different protocols in this suite are listed in Table 2-13.

Table 2-13. IPX/SPX protocols and their functions

Protocol	Function
Netware Core Protocol (NCP)	Allows client/server interactions such as file and print sharing.
Service Advertising Protocol (SAP)	Allows systems to advertise their services such as file and print services.
Internet Packet Exchange (IPX)	Provides network addressing and routing services.
Sequenced Packet Exchange (SPX)	Provides connection-oriented services on top of the IPX protocol.
Routing Information Protocol (RIP)	This is the default routing protocol for IPX/SPX networks. It uses Distant Vector Routing Algorithm for building routing tables.
NetWare Link State Protocol (NLSP)	Provides routing services based on Link State Algorithm for routes and building routing tables.
Open Datalink Interface (ODI)	Allows NetWare systems to work with any network interface card.

When discussing the IPX/SPX protocol suite, it is important to include the *frame types* used in NetWare networks. If there is some connectivity problem between two systems using different versions, it is a good idea to check the frame types used on the network. NetWare uses the following types of frames for encapsulating data at the Data Link layer:

- NetWare 2.x and NetWare 3.x use IEEE 802.3 as the default frame type.
- NetWare 4.x uses IEEE 8.2.2 as the default frame type.

NetBEUI. NetBEUI stands for *NetBIOS Extended User Interface*. It is an old Microsoft networking protocol used in small Windows-based networks. This protocol uses a broadcast method of finding computer names, and it creates significant network traffic. It is not a routable protocol and as such, cannot be used on large routed networks. It is easy to install and the fastest of all protocols covered in the A+ Essentials exam. Due to its severe limitations, it is not even used in Microsoft networks these days.

Host naming and addressing

Network hosts or computers are identified either by their names or their addresses. The term *network addressing* refers to the method of identifying networks and hosts located in a particular network. Different networking protocols employ different methods for addressing networks and hosts, as described in the following sections.

TCP/IP addressing. Hosts in a TCP/IP network follow IP addressing schemes. The IP address consists of 32 bits composed of 4 sets of 8 bytes (octet) each. It is expressed as decimal numbers separated by a period known as *dotted decimal* notation. 192.168.2.10 is an example of an IP address. IP addresses can further be divided into *public* (registered) or *private* (unregistered) addresses. Organizations using public addresses can be connected to the Internet while the private IP addresses can only be used internally.

IP addresses are classified into classes A, B, C, D, and E. Only addresses from the classes A, B and C are assigned to organizations and are known as *Classful IP Addresses*. The first byte of an IP address identifies the class of IP addresses used in the network. For example, a host with an IP address 92.137.0.10 is using a class A IP address and a host with an IP address 192.170.200.10 is using a class C IP address.

A second 32-bit number, known as *subnet mask*, is used to identify the network address from the host address. When converted to a binary number, the network part is assigned a binary value of 1 and the host part is assigned a value of 0 in the subnet mask. For example, if the subnet mask is 255.255.0.0, the first 16 bits of the IP address would represent the network address and the last 16 bits would represent the host address.

Table 2-14 summarizes the main classes of IP addresses, the number of networks and hosts in each class, and the default subnet masks.

Table 2-14. Classful IP address ranges

Class	Range of first byte	Number of networks	Hosts per network	Default subnet mask
A	1-126	126	16,777,214	255.0.0.0
B	128-191	16,384	65,534	255.255.0.0
C	192-223	2,097,150	254	255.255.255.0
D	224-239	N/A	N/A	N/A
E	240-255	N/A	N/A	N/A

> Notice from Table 2-14 that the network ID 127 is not included in any of the classes. This is because the IP address 127.0.0.1 is reserved as a *loopback* address for troubleshooting TCP/IP configuration of the computer.

Classful subnetting. *Subnetting* is the process of creating two or more network segments by using the host portion of the IP address. Subnetting creates multiple broadcast domains to reduce broadcast traffic and allows administrators to more effectively manage the IP address range. It also increases security of the network and helps contain network traffic to local network segments.

Consider a network with a class C IP address of 192.168.2.0. With the default subnet mask of 255.255.255.0, you can have only one large network segment with 254 hosts. If you use some bits from the host portion, you can create two, three, or four segments. But as the number of segments increases, the number of hosts in each segment reduces.

IPX addressing. In a NetWare network environment, only the servers are assigned hostnames. These names consist of a maximum of 47 characters. The clients do not have hostnames and use their IPX addresses instead. NetWare networks are assigned a 32-bit hexadecimal address. The servers and workstations use a 48-bit hexadecimal address, which is the MAC address of the network interface card. This address is appended to the network address to create a unique node address. The following is an example of an IPX address:

```
0AC74E02:02254F89AE48
```

Note that the first part of the IPX address is the address of the logical network, and the second part is the unique MAC address of the network interface card. If there are any leading zeros, they are not written. Sometimes the IPX address is also written as groups of four hexadecimal numbers separated by colons. The above address can thus be written as:

```
AC7:4E02:0225:4F89:AE48
```

NetBEUI addressing. The NetBEUI protocol uses NetBIOS naming conventions for the purpose of addressing computers in a network. NetBIOS computer names consist of a maximum of 15 characters such a Server1, Workstation1, etc. NetBEUI uses the three methods that are shown next to resolve NetBIOS computer names to IP addresses.

Broadcasting

If a host does not have the IP address of a NetBIOS host in its cache, it broadcasts the NetBIOS name in the entire network.

LMHOSTS file

This is a text file that maps IP addresses to NetBIOS computer names.

NBNS

This is the NetBIOS Name Server (known as the *WINS* server) that maps NetBIOS names to IP addresses.

Since NetBIOS name resolution mainly depends on broadcasts, the NetBEUI protocol creates significant network traffic if there are a large number of computers on the network.

Automatic Private IP Addressing (APIPA). The default configuration on most TCP/IP based operating systems is to dynamically obtain an IP address configuration from a *Dynamic Host Configuration Protocol (DHCP)* server. When the DHCP server is not available for some reason, the computer can assign itself an IP address automatically. The automatically assigned address is from the range 169.254.0.0 to 169.254.255.255 and a subnet mask of 255.255.0.0. With an APIPA address, the computer can connect only to the other computers with an APIPA address on the local network segment but cannot access any other computers on a remote network. If a computer is configured to obtain an IP address from a DHCP server but does not support APIPA, its IP address defaults to 0.0.0.0.

Bandwidth

In computer networks, the term *bandwidth* refers to the speed of data transmissions. It is a measure of the data that can be transmitted from one point to another in a given amount of time. This bandwidth is expressed as bits of data transmitted in one second or bits per second (bps). Since bps is a very small figure for most modern networks, the bandwidth is expressed as megabits per second (Mbps). Sometimes, the bandwidth is also expressed as bytes per second (Bps) or megabytes per second (MBps), where 1 byte is equal to 8 bits.

> It makes sense to mention *bandwidth bottlenecks* in this section. In a complex network, the complete path from one computer to another is composed of several links. Each link may have its own bandwidth. The bandwidth of the complete path is determined by the slowest link in the path. If the bandwidth is very low, the link becomes a bandwidth bottleneck.

LAN technologies

Ethernet networking and cabling technologies are defined in IEEE 802.3 standards. There are several variations in this standard, depending on speed, length, topology, and cabling used in implementing networks. The following sections provide a brief summary of the standards tested on the A+ exam.

10 Mbps Ethernet. The 10 Mbps standards include 10Base2, 10BaseT, and 10BaseFL. All of these standards define a maximum data transfer speed of 10 Mbps. This speed is now considered obsolete for most networks. It is unlikely that you will encounter any 10 Mbps networks in your career. The following are different variations of 10 Mbps networks.

10Base2
: This standard defines use of RG-58 coaxial cabling with a maximum segment length of 185 meters. The network can achieve a maximum speed of 10 Mbps. The segments are typically wired in physical bus topology.

10BaseT
: The *10BaseT* Ethernet standard defines use of CAT 3, 4, or 5 UTP cables with a maximum of 100 meters for each cable length. All computers (nodes) are connected to a central device known as the *hub* or the *switch*. It is typically wired in a physical star topology.

10BaseFL
: The 10BaseFL Ethernet standard uses fiber optic cables in order to increase the cable segment lengths to 2000 meters.

Table 2-15 gives a summary of 10 Mbps networking standards.

Table 2-15. Summary of 10 Mbps networking standards

Standard	Cable	Length of segment	Network topology	Connector
10Base2	Thin Coaxial	185 Meters	Bus	BNC
10BaseT	UTP CAT 3, 4, or 5	100 Meters	Star	RJ-45
10BaseFL	Fiber Optic	2000 Meters	Star	SC or ST

100 Mbps Ethernet. Most of the modern networks support 100 Mbps speeds, which provides better bandwidth for demanding applications. The following is a brief description of 100 Mbps standards:

100BaseTX
: 100BaseTX networks use two pairs or UTP CAT 5 cable. The length of cable segments can be up to 100 meters.

100BaseT4
: 100BaseT4 networks use four pairs of CAT 3, 4, or 5 type cables. The length of cable segments can be up to 100 meters.

100BaseFX
: 100BaseFX networks use multimode or single-mode fiber optic cables and provide up to 100 Mbps of data transfer rates. The length of cable segment can be up to 412 meters for multimode and up to 10,000 meters for single-mode cable.

Table 2-16 gives a summary of 100 Mbps networking standards.

Table 2-16. Summary of 100 Mbps networking standards

Standard	Cable	Length of segment	Network topology	Connector
100BaseTX	CAT 5	100 Meters	Star	RJ-45
100BaseT4	4 Pairs of CAT 3, 4 or 5	100 Meters	Star	RJ-45
100BaseFX	MM Fiber or SM Fiber	MM Fiber-412 Meters SM Fiber-10,000 Meters	Star	SC or ST

1000 Mbps Ethernet. The 1000 Mbps (equal to 1 Gigabit) Ethernet networks are also known as *Gigabit Ethernet*. These networks use either copper-based or fiber optic cabling. These networks are implemented mainly as a backbone for large networks. The following is a brief description of Gigabit Ethernet standards.

1000BaseX

Gigabit standards include *1000BaseLX, 1000BaseSX*, and *1000BaseCX*. The 1000BaseLX and 1000BaseSX use multimode or single-mode fiber optic cables. The 1000BaseCX standard specifies use of shielded twisted pair (STP) cables.

1000BaseT

This standard uses four pairs of CAT 5 UTP cable. Each pair of the CAT 5 cable can achieve maximum data transfer speeds of up to 25 Mbps, making it an overall 1000 Mbps.

Table 2-17 gives a summary of Gigabit Ethernet networking standards.

Table 2-17. Summary of Gigabit Ethernet networking standards

Standard	Cable	Length of segment
1000BaseLX	MM fiber optic or SM fiber optic	MM Fiber –550 meters SM Fiber –5,000 meters
1000BaseSX	MM Fiber –50 Micron	550 meters
1000BaseCX	STP	25 meters
1000BaseT	UTP	75 meters

WAN technologies

A wide area network (WAN) consists of two or more interconnected connect local area networks (LANs). Usually a third party—a telephone company or an ISP—is involved in providing a connectivity solution to the organization that needs to set up a WAN. A WAN can be set up using a dial-up telephone line for low bandwidth requirements, or it may be set up using a high-bandwidth dedicated line. It is also possible to tunnel the WAN connection through the Internet. The following sections describe various technologies used for WAN connectivity.

Internet Service Provider (ISP). The term *Internet Service Provider* refers to an organization that provides Internet access or wide area networking facilities. ISPs provide low-cost Internet connectivity to home users via *dial-up*, *cable modem*, *ISDN (BRI)*, or *Digital Subscriber Lines*. For large organizations that require high speed and bandwidth, the connectivity is provided through *Gigabit Ethernet, ATM, ISDN (PRI)*, *T-carriers*, or *Sonet*.

On the Internet, there is actually a hierarchy of lower-level and higher-level ISPs. Just as customers connect to an ISP, the ISPs themselves are connected to their upstream ISPs. Several ISPs are usually engaged in *peering*, where all ISPs interconnect with each other at a point known as *Internet Exchange (IX)*. This is done to allow routing of data to other networks. ISPs who do not have upstream ISPs are called *Tier 1 ISPs*. These ISPs sit at the top of the Internet hierarchy.

Integrated Services Digital Network (ISDN). ISDN is a *packet-switched* network that allows transmission of data and voice over telephone lines. This results in better quality and higher data transfer speeds than regular dial-up connections. ISDN requires dedicated telephone lines or *leased lines* and hence is expensive. When the two ends need to communicate, one dials the specified ISDN number and the connection is set up. When the communication between the two nodes is over, the user hangs up and the ISDN line becomes free. Computers using the ISDN line need a special network interface known as an *ISDN adapter* or *terminal adapter*.

ISDN communications use two types of channels: a bearer channel (*B channel*) used for data (or voice), and a delta channel (*D channel)* used for control signals. The two main implementations of ISDN as follows:

Basic Rate Interface (BRI)
: *BRI ISDN* uses 2 B channels of 64 Kbps each for data/voice, and a D channel of 16 Kbps. The total data transfer speed of BRI ISDN using two B channels is 128 Kbps. The two B channels can also be used separately with 64 Kbps speed.

Primary Rate Interface (PRI)
: *PRI ISDN* uses 23 B channels of 64 Kbps each for data/voice, and a D channel of 64 Kbps. The total data transfer speed of PRI ISDN is up to 1.544 Mbps. The PRI ISDN is usually carried over dedicated (leased) T1 lines.

Table 2-18 summarizes the two ISDN implementations.

Table 2-18. BRI and PRI ISDN connections

Characteristic	BRI	PRI
Carrier line	ISDN	T1
Channels	2B+1D	23B+1D
Total speed	128 Kbps	1.544 Mbps

Digital Subscriber Line (DSL). DSL is a family of technologies that uses ordinary analog telephone lines to provide digital data transmissions. It uses different frequencies for voice and data signals, and the same telephone line can simultaneously be used for phone and data transfer. It is commonly used for high-speed Internet access from homes and offices. Different DSL technologies are collectively noted as *xDSL* and support data transfer speeds from 128 Kbps to 24 Mbps, as given in the following list:

Asymmetrical DSL (ADSL)
ADSL is the most common of all types of DSL variations. The download speed of data is faster than upload speeds. It uses one channel for analog voice (telephone) transmissions; a second channel for data uploads, and a third channel for data downloads.

Symmetrical DSL (SDSL)
SDSL supports equal speeds for both data uploads and downloads. It cannot be used for voice transmissions and hence is suitable only for Internet access at offices.

ISDN DSL (IDSL)
IDSL is a variation of symmetric DSL. It does not support analog voice transmissions and is used only in those environments where ADSL and SDSL are not available.

Rate Adaptive DSL (RADSL)
RADSL is a variation of asymmetric DSL that can vary the transfer speeds depending on line conditions. It supports both data and voice transmissions.

Table 2-19 provides a summary of different DSL variations and their data transfer speeds.

Table 2-19. DSL variations

DSL variation	Download speed	Upload speed	Phone usage
ADSL	8 Mbps	1 Mbps	Yes
SDSL	1.5 Mbps	1.5 Mbps	No
IDSL	144 Kbps	144 Kbps	No
RADSL	7 Mbps	1 Mbps	Yes

Broadband. *Broadband Internet Access*, or simply *Broadband*, is provided by the cable companies that provide digital cable services. It is a reliable and efficient means of Internet access. The coaxial cable connects to a cable modem that further connects to the computer or other network device (hub, switch, or router) using a UTP cable. The cable connection can be shared among several computers in a home or in small offices using low-cost wired or wireless routers.

With a cable modem, the user does not have to dial the ISP and the connection is always there. This might pose a security risk for computers that are used for critical purposes. Most cable modems support bandwidths from 1.5 Mbps to 3 Mbps for the Internet access. The cable modem usually supports up to 10 Mbps data speeds for the LAN. The actual Internet access speed depends on the utilization of the shared cable signals in the area. The available bandwidth is always shared with other users in the area and may vary from time to time. In the periods of peak usage, the speed may be low compared to the periods when usage is low.

Satellite. In such areas where DSL or cable is not available, satellite is the only option for high-speed WAN connectivity and Internet access. For this reason, it is commonly used in rural areas. The signals travel from the ISP to a satellite and then from the satellite to the user. The data transmission speeds vary from 512 Kbps (upload) to 2 Mbps (download). Major drawbacks of satellite Internet access are that it is expensive and offers low-transfer speeds compared to DSL and cable.

Satellite Internet access suffers from *propagation delays* or *latency* problems. Latency refers to the time taken for the signal to travel from ISP to the satellite, located in the geostationary orbit at 35,000 Km. above earth, and then back to the user. Latency also depends on atmospheric conditions.

Dial-up. Dial-up networking using the Plain Old Telephone System (POTS) and the Public Switched Telephone Network (PSTN) is the traditional method of connecting to the Internet or to remote access servers. The user typically dials the telephone number of the ISP to authenticate and get Internet connectivity or to connect to another remote network. The telephone line is connected to a modem, which is further connected to a serial or USB port of the user's computer. Most computers these days have built-in modems that can be directly connected to the telephone line. POTS/PSTN provides a maximum data transfer speed of 56 Kbps.

Wireless. Wireless networks rely on radio frequencies to communicate instead of network cabling used for normal computer networks. Radio frequencies create *electromagnetic (EM)* fields, which become the medium to transfer signals from one computer to another. As you go away from the hub, or the main equipment generating the radio frequency of the wireless network, the strength of the EM field reduces and the signal becomes weak.

Wireless networks defined in IEEE 802.11 standards use radio frequencies with *spread spectrum* technology. The two spread spectrum technologies are as follows:

Frequency-hopping spread spectrum (FHSS)
: This is the method of transmitting RF signals by rapidly switching frequencies according to a pseudorandom pattern, which is known to both the sender and the receiver. FHSS uses a large range of frequency (83.5 MHz.) and is highly resistant to noise and interference.

Direct-sequence spread spectrum (DSSS)
: This is a modulation technique used by wireless networks, which uses a wide band of frequency. It divides the signal into smaller parts and then transmits them simultaneously on as many frequencies as possible. DSSS is faster than FHSS and ensures data protection. It utilizes a frequency range from 2.4 GHz to 2.4835 GHz and is used in 802.11b networks.

The most popular of the IEEE 802.11 wireless network standards are 802.11b, 802.11a, and 802.11g. Table 2-20 gives a brief comparison of the characteristics of different 802.11 standards.

Table 2-20. Comparison of 802.11 standards

802.11 standard	Operating frequency	Maximum speed
802.11	2.4 GHz	1 Mbps or 2 Mbps
802.11b	2.4 GHz	11 Mbps
802.11a	5 GHz	54 Mbps
802.11g	2.4 GHz	54 Mbps

Infrared

Infrared technology uses electromagnetic radiations using wavelengths that are longer than the visible light but shorter than radio frequency. Common examples of Infrared devices are the remote controls used in TVs and audio systems. The following are some of the key characteristics of IrDA wireless communication technology:

- It provides point-to-point wireless communications using a direct line of sight.
- Infrared waves cannot penetrate through walls.
- It supports data transfer speeds ranging from 10 to 16 Mbps.
- Infrared devices consume very low power.
- Infrared frequencies do not interfere with radio frequencies.
- It provides a secure wireless medium due to the short distance (usually 3 to 12 feet).

Bluetooth. Bluetooth wireless networking technology provides short-range communications between two or more devices. It is a low-cost networking solution widely used in telephones, entertainment systems, and computers. It is designed to overcome the limitations of IrDA technology. The following are some of the key characteristics of Bluetooth-based wireless communications:

- It supports transmission speeds from 1 Mbps (Bluetooth 1.0) to 3 Mbps (Bluetooth 2.0) over the unlicensed frequency range of 2.4 GHz.
- The devices must be within a short range of less than 10 meters.
- It offers high resistance to electromagnetic interferences.
- Unlike the Infrared signals, it does not require direct line of sight.
- It consumes very low power.
- Two or more Bluetooth computers form an ad-hoc wireless network.

Cellular. A cellular wide area network is made up of a large number of radio cells. A separate transmitter located at a fixed site powers each radio cell. This site is known as a base station. The coverage area of a particular cellular network depends on the number of base stations. The most common example of a cellular network is the mobile phone network.

VoIP. VoIP stands for Voice over Internet Protocol. Other popular names for this technology are Internet Telephony, IP Telephony, and Broadband Phone. VoIP is a mechanism to transmit voice signals over Internet Protocol (IP). The special protocols used to carry voice signals over an IP network are called *VoIP protocols*. One of the major advantages of VoIP is the ability of a user to make telephone calls from anywhere in the world. Since the VoIP service is heavily dependent on availability and reliability of the Internet connection, this technology is still in the development process.

Installing and Maintaining Networks

As a computer technician, you must be able to install and configure a network adapter. Most new computer motherboards have an integrated network interface. In case you are required to install an additional network adapter or install it on a nonintegrated motherboard, you must know how to complete the required tasks such as obtaining the network connection and configuring the properties of networking protocol. This section covers a brief study of network related exam objectives.

Installing and configuring network cards

Most new desktops come equipped with built-in network adapters. In newer computers, the network interface is integrated with the motherboard. But you might have to install, replace, or upgrade network adapters in some old desktops. For example, you might be asked to replace a 10 Mbps network adapter with a 10/100 Mbps fast network adapter.

Installing a network adapter. When installing a network adapter, you will need to make sure that:

- The adapter is compatible with the existing computer hardware.
- The adapter driver is meant for the operating system installed on the computer.
- The operating system supports the adapter driver.
- Whether the adapter is PnP or not.
- The adapter driver is available for installation if it is not automatically installed by the operating system.

The following exercise explains the steps involved in installing a network adapter:

1. Turn off the power to the computer.
2. Remove the computer case cover. Locate an expansion slot and remove the plastic or metal strip that covers the case opening.
3. Insert the network adapter into the expansion slot and tighten the screw, if required.
4. Put the computer case cover back and tighten the screws.
5. Obtain a network patch cable and connect it to the RJ-45 socket provided on the network adapter and the wall outlet.
6. Turn on the computer.

Configuring the network card. Most new network adapter are PnP-compatible. PnP adapters are automatically detected and configured by most operating systems. This configuration includes setting aside system resources such as IRQ, I/O, and DMA for the adapter as well as installation of an appropriate driver.

In case the network adapter is not PnP, you will be required to install the network driver manually. You will need to obtain the driver, which may be available either on the CD-ROM accompanying the network adapter or from the vendor's web site. On Windows XP and Windows 2000 Professional computers, you can use the Add/Remove Hardware applet in the Control Panel to add the network adapter. The Device Manager snap-in can be used to install the network adapter device driver.

Troubleshooting Techniques

The following sections cover some of the common network problems and basic troubleshooting techniques.

Status indicators

One of the easiest methods to troubleshooting network connectivity is to check the visual status indicators on network devices. Almost every network device has some form or other visual indicator that can help find out if the device is working or not. Some network devices have LEDs that change color according to the condition of the device or an interface of the device.

The following list provides guidelines for diagnosing a connectivity problem depending on the status of the LED lights:

No light or yellow
: The device or the port is not operational. It is either not connected or is faulty.

Solid green
: The device or port is connected but there is no activity on the port.

Flashing green
: The device or the port is functioning properly. It is transmitting and receiving data as expected.

Flashing amber
: The network is congested and collisions are occurring on the network media.

Certain devices provide separate LEDs for power, activity, and network collisions. Each of these LEDs can be a good indicator of the connectivity problem.

Troubleshooting network media

The cables and connectors used to interconnect network devices are often the cause of a network connectivity problem. Some of the key points to remember while troubleshooting network media are as follows:

- Verify that a correct cable type and connectors are used and that they are properly attached.

- The total length of a cable used to connect devices must not exceed the specifications.
- UTP cables are also prone to interferences generated by crosstalk and electromagnetic interferences. UTP cables should not be run in areas of high EMI (such as near transformers or beside high-voltage electric cables). For ceilings and ducts, a special type of cable known as *plenum*-rated cable should be used.

Troubleshooting network devices

The following are some of the common problems with network devices:

- If a hub fails, all computers connected to the hub will experience connectivity problems.
- A failed switch will also result in connectivity problems to all computers in the network segment.
- Routers are used to connect network segments. If a router fails, computers on one of the network segments will not be able to connect to any other network segment.

Troubleshooting wireless connectivity

The following list provides a quick review of the factors that may affect the wireless networks:

- Wireless signals degrade as they travel away from a wireless signal-generating device such as the access point. This degradation or attenuation of signals is caused by several environmental factors such as EMI, RFI, walls, etc.
- Make sure that the wireless devices such as wireless router, access points, and wireless adapters all support the standard used on the network.
- The *Service Set Identifier (SSID)* enables wireless clients to connect to a wireless access point and access network resources. If a wireless client is reporting connectivity problems, wireless configuration should be checked to make sure that the client is using the correct SSID.
- If a user cannot log on to a wireless network, make sure that he has sufficient permissions to log on. Additionally, confirm that the encryption and authentication settings are configured correctly on his computer.

Security

Security was not a big concern when computers were not networked and when the Internet was not as widely used as it is used today. Connecting to the Internet opens your computer or the entire network to the outside world. If security methods are not implemented, the computers or the Internet may be at risk of being exploited. Security threats come in various forms and can cause loss of connectivity or loss of valuable data. As a PC technician, you are expected to have a good knowledge of basic security concepts. In this section, we will discuss some fundamental security concepts.

Principles of Security

In this section, we will study some basic elements of computer security. These topics include authentication technologies and protocols, malicious software, and elements of wireless security.

Authentication technologies and protocols

Authentication is the process of verifying the identity of a person. It is considered the first point of controlling access to a system. In the context of computer security, authentication is the method of verifying that the identity of a person or an application seeking access to a system, object, or a resource is true. For example, if a user wants to access a computer, the identity of the user is usually verified by having the user enter a valid username and password. If the username and password of the user matches the ones stored in the security database of the computer, the user is allowed access. This process is known as the authentication process. Depending on the requirements of an organization, one or more authentication mechanisms can be implemented to ensure security of an individual computer or for the entire network.

The following sections discuss a number of authentication technologies and protocols used in computer networks.

Username and password. Almost all operating systems implement some kind of authentication mechanism wherein users can simply use a locally created username and password to get access to the system. When the user enters his credentials (the combination of username and password), the local security database is checked to verify that the credentials match the ones stored in the local security database of the computer. If a match is found, the user is granted access; otherwise, the user is not allowed to log on to the system. This is the simplest form of authentication and can be implemented easily, but it also comes with its own limitations. Many organizations document and implement password policies that control how users can create and manage their passwords in order to secure network resources.

Biometrics. Biometrics refers to the authentication technology used to verify the identity of a user by measuring and analyzing human physical and behavior characteristics. This is done with the help of advanced biometric authentication devices that can read or measure and analyze fingerprints, scan the eye retina, and facial patterns, and/or measure body temperature. Handwriting and voice patterns are also commonly used as biometrics. Biometric authentication provides the highest level of authenticity about a person, which is much more reliable than a simple username and password combination. It is nearly impossible to impersonate a person when biometric authentication is used for authentication.

Smart cards. Smart cards store a small amount of data that is generally used to authenticate the holder or owner of the card. These cards typically come in the size of a standard credit/debit card. When used for authentication and identification purposes, they prevent modification of the data stored on them. Smart cards are designed well to protect them against theft of data and are immune to EMI and RFI and have built-in protection against physical damage.

Security tokens. A security token (also known as an *authentication token* or a *hardware token*) is considered to be the most trusted method for verifying the identity of a user or a system. Tokens provide a very high level of security for authenticating users because of the multiple factors employed to verify the identity. It is almost impossible to duplicate the information contained in a security token in order to gain unauthorized access to a secure network. In its simplest form, an authentication token or a security token consists of two parts: a hardware device that is coded to generate token values at predetermined intervals, and a software-based component that tracks and verifies that these codes are valid.

Security tokens are also known as *key fobs* because they are small enough to be carried on a key chain or in a wallet. Some security tokens may contain cryptographic keys while others may contain biometrics data such as fingerprints of the user. Some tokens have a built-in keypad, and the user is required to key in a *personal identification number (PIN)*.

Digital certificates. *Certificates* or *digital certificates* are widely used for Internet-based authentications, as well as for authentication of users and computers in network environments, to access network resources and services where directory services such as Microsoft's Active Directory service are implemented. Certificates are a part of *public key infrastructure (PKI)*. In a PKI, certificate servers are used to create, store, distribute, validate, and expire digitally created signatures and other identity information about users and systems. Certificates are created by a trusted third-party known as a *Certification Authority* or *Certificate Authority (CA)*. Examples of commercially available CAs are Verisign and Thwate. It is also a common practice to create a CA within an organization to manage certificates for users and systems inside the organization or with trusted business partners. In Windows 2000 and later server operating systems, certificates are used for authenticating users and granting access to Active Directory objects. CA used within an organization is known as an *enterprise CA* or a *Standalone CA*.

Another common use of certificates is for *software signing*. Software is digitally signed to ensure the user that it has been developed by a trusted software vendor. It also ensures that the software has not been tampered with since it was developed and made available for download. Certificates are also implemented in Internet services to authenticate users and verify their identity.

Multifactor. In computer authentication-using secure methods, a *factor* is a piece of information that is present to prove the identity of a user. In a multifactor authentication mechanism, any of the following types of factors may be utilized:

- A *something you know* factor, such as your password or PIN.
- A *something you have* factor, such as your hardware token or a smart card.
- A *something you are* factor, such as your fingerprints, your eye retina, or other biometrics that can be used for identity.
- A *something you do* factor, such as your handwriting or your voice patterns.

Multifactor authentication is considered to be acceptably secure because it employs multiple factors to verify the identity of the user.

Challenge-Handshake Authentication Protocol (CHAP). This protocol is widely used for local and remote access authentication. CHAP is a modified form of *Password Authentication Protocol (PAP)*, which transmits user credentials in clear text. CHAP periodically verifies the authenticity of the remote user using a three-way handshake even after the communication channel has been established. CHAP authentication involves an authentication server and the client. The process is carried out as follows:

1. When the communication link has been established, the authentication server sends a "challenge" message to the peer.
2. The peer responds with a value calculated using a *one-way hash* function such as Message Digest 5 (MD5).
3. The authentication server checks the response to ensure that the value is equal to its own calculation of the hash value. If the two values match, the authentication server acknowledges the authentication; otherwise, the connection is terminated.
4. The authentication server sends the challenge message to the peer at random intervals and repeats steps 1 to 3.

One drawback of CHAP is that it cannot work with encrypted password databases and is considered to be a weak authentication protocol. Microsoft has implemented its own version of CHAP known as MS-CHAP, which is currently in version 2.

Kerberos. Kerberos is a cross-platform authentication protocol used for mutual authentication of users and services in a secure manner. Kerberos V5 is the current version of this protocol and is used on Windows servers as the default authentication protocol. The protocol ensures the integrity of authentication data (user credentials) as it is transmitted over the network. It is widely used in all other major operating systems, such as Unix and Cisco IOS.

Kerberos works in a *Key Distribution Center (KDC)*, which is typically a network server used to issue secure encrypted keys and tokens *(tickets)* to authenticate a user or a service. The tickets carry a timestamp and expire as soon as the user or the service logs off. The following steps are carried out to complete the authentication process:

1. The client presents its credentials to the KDC for authentication by means of username/password, smart card, or biometrics.
2. The KDC issues a *Ticket Granting Ticket (TGT)* to the client. The TGT is associated with an *access token* that remains active until the time the client is logged on. This TGT is cached locally and is used later if the session remains active.
3. When the client needs to access the resource server, it presents the cached TGT to the KDC. The KDC grants a session ticket to the client.
4. The client presents the session ticket to the resource server, and the client is granted access to the resources on the resource server.

The TGT remains active for the entire session. Kerberos is heavily dependent on synchronization of clocks on the clients and servers. Session tickets granted by the

KDC to the client must be presented to the server within the established time limits or else they may be discarded.

Protection from malicious software

Malicious software or *malware* are software applications specifically written to launch attacks against individual computers or networks. The basic purpose of malicious software is to gain unauthorized access and cause damage to the system or steal confidential information. Examples of code attacks include viruses, Trojan horses, worms, logic bombs, spyware, and adware. These are discussed in the following paragraphs.

Virus. A *virus* is a self-replicating application that inserts itself into executable files on the computer and spreads itself using the executable. A computer virus is typically created for the sole purpose of destroying a user's data. In order for the virus to work or infect a computer, it must first load itself into system memory. When the hosting executable file is run, the virus code is also executed and destroys user data or critical system files.

> A virus must first infect an executable file to run successfully. The infected file is known as the virus host. The infected program must be executed before the virus can spread to infect other parts of the system or data.

The following are different types of viruses:

Boot sector or bootstrap virus
: Infects the first sector on the hard disk, which is used for booting or starting up the computer. The boot sector virus becomes active as soon as the computer is started.

Parasitic virus
: Infects an executable file or an application on a computer. The infected file actually remains intact, but when the file is run, the virus runs first.

If the infected computer is connected to the network, the virus can travel from one computer to another and can infect every computer on its way. A virus can infect data stored on floppy disks, hard disks, and even on network storage devices.

Trojans. A *Trojan horse* (or simply a *Trojan*) is a malicious code that is embedded inside a legitimate application. The application appears to be very useful or interesting and harmless to the user until it is executed. Trojans are different from other computer viruses in that they must be executed by the victim who falls for the "interesting software."

Most of the modern Trojans contain code that is basically used to gather information about the user. These Trojans fall into the category of *spyware* and appear as pop-up windows on a user's computer screen. The sole purpose of these Trojans is to somehow trick the user into executing the application so that the code can execute. Some Trojans are written very precisely to allow the user's computer to be controlled remotely by the attacker.

The main difference between a virus and a Trojan is that viruses are self-replicating programs while Trojans need some action taken on the part of the user. If the user does not fall into the trap of the Trojan, it does not execute.

Worms. A worm is a computer virus that does not infect any particular executable or application but resides in the active memory of computers. This virus usually keeps scanning the network for vulnerabilities and then replicates itself onto other computers using those security holes. The effects of worms are not easily noticeable until entire systems or network resources appear to have been consumed by the virus. The most common type of worm is the email virus that uses email addresses from the address book of a user to spread itself.

Spam. Spam, or email spam, refers to unsolicited junk mail that fills up your mail box everyday. These messages come from unknown persons and are rarely of any interest or use to the recipient. Spammers collect email addresses from user forums, news groups, and so on. They also use specially created applications known as *Spamware* to collect email addresses and send messages to them. In most cases, the sending email address of spammers is not traceable by a normal computer user.

Spyware. Spyware software is used to collect personal information stored in the computer and send it to a third party without the permission or knowledge of the user. This process is carried out in the background, and the user does not even know that his personal information has been stolen. The personal information is usually stored in cookies. The information may include your name and password that you use on other web sites. The third parties who receive this information use it to send you unsolicited advertisements for selling their products.

Adware. The term *adware* is used for software that displays advertisements on your computer. Adware appears as unsolicited pop-up windows on the computer screen. These advertisements appear when the computer is connected to the Internet. Most of these advertisements offer free software, screen savers, or tickets.

Grayware. The term *grayware* is used for those software programs that work in an undesirable or annoying manner. These programs may also negatively affect the performance of the computer. Grayware includes software programs such as spyware, adware, and so on. Pop-up windows are also classified as grayware.

Software firewalls

A *firewall* is a hardware device or a software application that sits between the internal network of the organization and the external network to protect the internal network from communicating with outside networks. A properly configured firewall blocks all unauthorized access to the internal network. It also prevents internal users from accessing potentially harmful external networks.

Firewalls can be implemented in the form of dedicated hardware devices or through the use of special software applications. When a computer or a network is protected using software applications, the firewall implementation is known as *software firewall*. *Windows Firewall* in Windows XP SP2 is a simple example of software firewall, which can be implemented on personal computers.

The three common firewall technologies are:

Packet-filtering firewalls

Packet-filtering firewalls inspect the contents of each IP packet entering the firewall device and, based on predefined and configured rules, allows or blocks packets inside the network. These firewalls permit or block access to specific ports or IP addresses and work on two basic policies: *Allow by Default* and *Deny by Default*. Following the *Allow by Default* policy, all traffic is allowed to enter the network except the specifically denied traffic. In the *Deny by Default* policy, all traffic entering the firewall is blocked except the one specifically allowed. *Deny by Default* is considered the best firewall policy, as only authorized traffic is allowed to enter the network using specified port numbers or IP addresses.

Application layer firewalls

Application layer firewalls are also known as *Application firewalls* or *Application Layer gateways*. This technology is more advanced than packet filtering, as it examines the entire packet to allow or deny traffic. Proxy servers use this technology to provide application layer filtering to clients. Inspection of data packets at the application layer (of the OSI model) allows firewalls to examine the entire IP packet and, based on configured rules, allow only intended traffic through them. One of the major drawbacks of application layer firewalls is that they are much slower than packet filtering firewalls because every IP packet is broken at the firewall, inspected against a complex set of rules, and reassembled before allowing it to pass.

Stateful inspection firewalls

Stateful inspection firewalls work by actively monitoring and inspecting the state of the network traffic, and they keep track of all the traffic that passes through the network media. This technology overcomes the drawbacks of both packet filtering and application layer firewalls. It is programmed to distinguish between legitimate packets for different types of connections. Only those packets are allowed that match a known connection state. This technology does not break or reconstruct IP packets and hence is faster than application layer technology.

Filesystem security. Windows operating systems provide file- and folder-level security using the *NT File System (NTFS)*. Files can even be stored and transmitted over the network in secure encrypted form. To keep tight control of access permissions of shared resources, the Windows operating system allows you to configure two types of permissions: *Share permissions* and *NTFS permissions*. Share permissions provide an outer layer of control, while NTFS permissions provide more granular control on file and folder access. A list of standard NTFS permissions is shown next.

Full Control
Grants the user all rights on the resource.

Modify
The Modify permission allows a user to change the contents of the file.

Read and Execute
Allows a user to read the file and execute (run) it.

List Folder Contents
Allows the user to list the files and subfolders inside a folder.

Read
Allows a user to read a file.

Write
Allows a user to write files to a folder.

> NTFS permissions are available only on those disk partitions that are formatted using NTFS. These permissions cannot be configured on disks formatted with the FAT filesystem. Moreover, Share permissions do not apply to a user who is logged on locally to the computer.

Wireless security

Wireless networks rely on radio frequencies to communicate instead of the network cabling used for normal computer networks. Radio frequencies create electromagnetic (EM) fields, which become the medium to transfer signals from one computer to another. Wireless networks are also prone to malicious attacks if they are not properly secured. This section covers a brief discussion of different mechanisms that can be used to protect computers using wireless networking.

Wireless networking protocols. Wireless networks defined in IEEE 802.11 standards use radio frequencies with *spread spectrum* technology. The two spread spectrum technologies are as follows:

Frequency-hopping spread spectrum (FHSS)
This is the method of transmitting RF signals by rapidly switching frequencies according to a pseudorandom pattern, which is known to both the sender and the receiver. FHSS uses a large range of frequency (83.5 MHz) and is highly resistant to noise and interference.

Direct-sequence spread spectrum (DSSS)
This is a modulation technique used by wireless networks that uses a wide band of frequency. It divides the signal into smaller parts and transmits them simultaneously on as many frequencies as possible. DSSS is faster than FHSS and ensures data protection. It utilizes a frequency range of 2.4 GHz to 2.4835 GHz and is used in 802.11b networks.

The most popular of the IEEE 802.11 wireless network standards are 802.11b, 802.11a and 802.11g. The most popular of the IEEE 802.11 wireless network standards are 802.11b, 802.11a and 802.11g. Security standards for these protocols are defined in the 802.11i standard.

Wireless authentication. Wireless authentication is implemented in one of the following methods:

Open system
: This is actually not authentication. Every computer trying to connect to a wireless network is granted a connection.

Shared key
: This method requires that every wireless client knows the shared secret key. The access point and all wireless clients must use the same shared secret key.

IEEE 802.1x
: This method requires use of advanced encryption and authentication techniques to provide strong authentication.

WPA or WPA2 with preshared key
: This method can be used for smaller home or office networks that cannot implement the IEEE 802.1x authentication mechanisms. The preshared key consists of a 20-character-long paraphrase containing upper- and lowercase letters and numbers.

Wired Equivalent Privacy (WEP). WEP is the primary security standard for 802.11 wireless networks and is designed to provide privacy in transmissions occurring between the AP and wireless client. It uses *shared key authentication* that allows encryption and decryption of wireless transmissions. Up to four different keys can be defined on the AP and the client, and these keys can be rotated to enhance security. WEP encryption can use either 40- or 128-bit keys. When WEP is enabled on the AP and the wireless clients, the encryption keys and the SSID must match on both ends. WEP is easy to implement because the administrator or the user can define the keys.

WEP uses CRC-32 checksum for data integrity, and privacy is ensured with RC4 encryption algorithm. RC4 is a stream cipher, and both the AP and the client encrypt and decrypt messages using a known preshared key. The sender runs the plain-text message through an integrity check algorithm (CRC-32) to produce the *integrity check value (ICV)*. The ICV is added to the plain text message. A random 24-bit *initialization vector (IV)* is generated and added to the beginning of the secret key to ensure security of the key. The IV is changed every time to prevent reuse of the key.

Wireless Transport Layer Security (WTLS). WTLS is designed to provide end-to-end security for WAP devices. WTLS is based on the *Transport Layer Security (TLS)* protocol that is a further derivative of *Secure Socket Layer (SSL)*. WTLS is designed to provide privacy and availability for both the WAP server and the WAP client. WTLS works for applications that run on devices with low-processing capabilities, low bandwidth, and limited memory. WTLS uses a compressed certificate format following the X.509v3 standard but defines a smaller data structure.

Protecting wireless networks from attacks

It is important that steps are taken to protect wireless networks from potential outside threats and attacks. Some of the protective measures are listed here:

- Administrators should keep their software and hardware updated by regularly checking for updates on vendors' web sites.
- When installing a wireless network, the default settings of the AP, such as the SSID, should be changed. Hackers usually know the default settings of devices.
- WEP should always be used. Even if 40-bit encryption is used, it is better than not using encryption at all. WEP can be easily cracked, but the network can still be protected from a number of amateur hackers.
- Wherever possible, wireless adapters and AP devices should support 128-bit WEP, MAC filtering, and disabling of SSID broadcasts.
- If SSID broadcasts are not disabled on APs, use of a DHCP server to automatically assign IP addresses to wireless clients should be avoided. Wardriving software can easily detect your internal IP addressing scheme if SSID broadcasts are enabled and DHCP is in use.
- Static WEP keys should be frequently rotated so that they are not compromised.
- Place the wireless networks in a separate network segment. If possible, create a separate perimeter network (also known as a *Wireless Demilitarized Zone*) for the wireless network that is separate from the main network of the organization.
- Conduct regular site surveys to detect the presence of rogue APs near your wireless network.
- Placement of the AP is critical for wireless security. Place APs in the center of the building and avoid placing them near windows and doors.

Data security. *Data security* refers to securing critical user and system data using authentication mechanisms, encryption, and access control. A number of methods can be implemented to ensure security of critical data stored on computers. Some of these methods are listed in the following sections.

Data access. Access to data must be granted only to authorized employees of the organization. The following are some of the important considerations when setting access control:

- Files and folders should be secured using appropriate NTFS permissions.
- Local security policies such as the right to Log On Locally and Access This Computer From Network should be defined on computers to restrict access.
- Users who need not access or work on critical or confidential files should not be allowed to access them.
- Access to critical data files should be audited.
- Use of floppy disks or CD/DVD discs to copy data should be prohibited.

Backups. Data backup is one of the fundamental elements of ensuring data security in the event of a disaster. Backed-up data is copied to another media such as magnetic tapes or compact disks (CDs or DVDs), which are safely and securely stored at an offsite location. Commonly used backup methods include the following:

Full backup
: This method backs up all the data in a single backup job. The backed-up data includes systems files, applications, and all user data on a computer. Full backup changes the *archive bit* on files to indicate that it has been backed up. It takes longer to complete the backup process, but the data can be restored faster, as only a single backup set is required.

Incremental backup
: This method backs up all the data that has changed after the last full or incremental backup was taken. It uses the archive bits and changes them after the backup process is complete. It takes the least amount of time to complete the backup process but it is the slowest method when data needs to be restored. The last full backup tape and all incremental tapes after the full backup are required to completely restore data.

Differential backup
: This method backs up all the data that has changed after the last full backup. It does not change the archive bits and thus does not disturb any scheduled incremental backups. Since it does not use the archive bits, if differential backup is taken more than once after a full backup, the differential backup tapes will contain duplicate data. When restoring data, only the last full backup tape and the differential backup tape are required. It is faster to restore than the incremental backup

Most organizations implement a mix of one or more backup types to create weekly, monthly, and yearly backup plans. Depending on the requirements of an organization and the amount of data to be backed up, different organizations may adopt different backup schemes. One of the commonly used backup methods is to use a combination of full backup on weekends and incremental backups on weekdays.

> Backup tapes must be stored at a secure offsite location so that they are readily available in the event of a disaster. As a routine practice, test restores should be performed to ensure that data could be restored from backup media.

Encryption. Encryption is the process of encoding a message using cryptographic algorithms so that it is not readable unless it is decrypted. Encryption converts readable plain text into cryptographic text, or *cyphertext*. Encryption is used as a protective cover for the locally stored data as well for data transmitted over network media from one computer to another. Encryption keeps the data secure from unauthorized access by users and by professional hackers. *Encryption algorithms* lay the foundation for such security mechanisms as confidentiality, authentication, digital signatures, and public key cryptography. Encryption algorithms are used to calculate a *secret key*, which is used to encrypt and decrypt messages. Only the persons who possess the key can encrypt or decrypt messages. Encryption algorithms fall into the following main categories:

Symmetric algorithms

Symmetric algorithms, or symmetric key algorithms, use one key for both encryption and decryption of messages. The sender of data and the receiver each keep a copy of the secret key. The process is also known as *secret key* encryption or *shared secret* encryption. CompTIA refers to this mechanism as Private Key Encryption. Some of the popular symmetric algorithms are Data Encryption Standard (DES), 3DES, Advanced Encryption Standard (AES), and International Data Encryption Algorithm (IDEA).

Asymmetric algorithm

Asymmetric algorithms are commonly used for Public Key Cryptography. Asymmetric algorithms use two keys, one for encryption (*public key*) and the other for decryption (*private key*). The encryption key can be freely distributed, but the private key must be held in strict confidence. Deffie-Hellman, RSA, and El-Gamal are examples of asymmetric algorithms.

Hashing algorithm

A hashing algorithm (also called *Hash Function*) creates a small and unique digital "fingerprint" from any kind of data. This fingerprint is known as the *hash value*. The hash value is represented as a short string of random letters and numbers. If the original data changes even by one character, the hash function will produce a different hash value. Thus, the receiver will know that original data has changed. The hashing function is considered a one-way process because it is not possible to create the original text using any reverse hashing function. This is why hashing functions are also known as one-way hashing functions. *Message Digest 5 (MD5)* and *Secure Hashing Algorithm (SHA-1)* are examples of hashing algorithms.

> The terms *encryption* and *cryptography* are used interchangeably. Similarly, the encrypted data is also known as *cyphertext*.

Data migration. Data migration is the process of transferring data from one operating system platform to another or from one database application to another. This process converts the data from one format to another. Data migration also refers to the transfer of data from one computer to another or from one partition of the hard disk to another partition. The process is typically performed after a full backup of data so that if the data becomes unavailable or is accidentally destroyed during migration, a working copy can be restored from the backup set. When the data has been successfully migrated, administrators may need to reconfigure access control permissions. Data migration is a common scene when organizations upgrade their operating systems or migrate from one OS platform to another.

Data remnant removal. Data remnant removal refers to the process of secure destruction of data stored on unused disks and other storage media such as magnetic tapes, floppy disks, CD/DVD discs, etc. This process is required when old systems are replaced or old storage media is upgraded with new media. Data destruction ensures that the data stored on old storage media does not fall into the wrong hands and cannot be misused by a third party. One of the common methods used for removing data from magnetic media is to degauss them. Hard disks can be formatted before they are sent out as garbage.

Password management. A *password management policy* describes how users should create, use, and change their passwords. A password is the user's key to gaining access to the organization's resources stored on computers. Without having a sound password policy, employees may make their passwords weak or disclose their passwords to unauthorized people. Professional hackers may exploit an organization's confidential resources by guessing insecure passwords. Password policies include the following essential elements:

- Use of blank passwords should not be allowed for any employee.
- Passwords should have at least eight characters.
- A password should be made up of a combination of upper- and lowercase letters, special characters, and numbers.
- Employees should be forced to change their passwords regularly.
- Employees should not be allowed to reuse their old passwords for a certain amount of time.
- Administrators should use normal user accounts when not performing any administrative tasks. Only designated IT employees should have administrative privileges.

Passwords should be longer and stronger to prevent *brute force* or *dictionary attacks*. Password policies can be enforced through operating systems.

Physical security

Physical security refers to physically securing servers and desktops in a network. Some of the common methods used to ensure physical security are listed here:

Locking workstations

Users should be educated to keep their workstations locked when not in use. For example, when a user has to go out for lunch, she should lock her workstation so that any unauthorized person may not get access to data stored on the computer. Additionally, users can configure screensaver passwords to protect their desktops.

Physical barriers

Most organizations keep the critical servers and network equipment in a locked room, and unauthorized access is denied. Server rooms should be locked and equipped with alarm systems. Logbooks should be maintained for entries to the secure room. All equipment should be locked down with strong passwords. If some outsiders need to work inside secure rooms, an employee of the organization must remain with them all the time.

Incident reporting

Incidents related to security can be disastrous for an organization. It can cause disruptions in network services, failure of one or more systems, or failure of the entire network. An organization can loose confidential and valuable data due to a security breach. If there is a security breach in the network or the network is under attack from an outsider, there should be a plan to handle the incident promptly. *Incident reporting* refers to the method of informing the management or any other responsible employee of the organization as soon as the incident is detected. If the incident is about to occur or is in progress, the management can take immediate action to prevent damage. If there is an Incident Response Policy in the organization, it should be followed. If there is evidence, it should be secured and preserved. Some organizations contract third-party organizations to investigate security related incidents.

Social engineering

Social engineering is the process of getting personal or confidential information or information about an organization by taking an individual into confidence. The so-called "social engineer" generally tricks the victim over the telephone or on the Internet to reveal sensitive information about the organization. Unfortunately, no technical configuration of systems or networks can protect an organization from social engineering. There is no firewall that can stop attacks that result from social engineering. The best protection against social engineering is to train users about the security policies of the organization.

Security Problems and Preventive Maintenance

Security should be implemented in such a way that it secures system and network resources. It should not become a problem for users who need to perform their everyday jobs on computers. Users should be able to access system and network resources with convenience but should be restricted from accessing confidential data of the organization. The following sections outline some of the common security-related problems and methods of performing regular preventive maintenance tasks for ensuring a secure working environment.

Security-related problems

The following sections provide a summary of some common security-related problems:

BIOS

BIOS in computers can be protected with a password. If a user does not know the password for accessing the BIOS setup, she will not be able to access the BIOS setup program and make any changes.

Smart cards

Smart cards are used to authenticate users. Problems with smart cards appear when the card is either worn out or an unauthorized person uses it.

Biometrics

Biometric devices use human characteristics to verify the identity of a person. A biometric device will immediately detect if an unauthorized person is trying to gain access to a secure system.

Malicious software

The purpose of malicious software is to destroy data on a user's computer or to obtain personal information. If an antivirus application is installed, it should be able to detect the presence of malicious software, provided that virus signatures are up-to-date.

Filesystem and data access

Filesystem problems result due to incorrect settings of NTFS permissions. In some cases, unauthorized users may gain access to data that they are not supposed to. On the other hand, authorized users may complain that they are unable to access data that they should be usually allowed to access.

Backup

Backup problems result from a system's inability to access backup media, bad media, or an incomplete backup process. The best way to ensure that backup problems are prevented is to perform test restores.

Data migration

Problems arising after data migration are related to differing sets of permissions on the source and target computers.

Preventive maintenance procedures

Some of the important preventive maintenance procedures for computer security include installation of antivirus software, keeping the applications and operating system updated, securing network devices, configuring auditing and logging, and educating users. The following is a summary of these procedures.

Antivirus software. Every computer in a network should have antivirus software installed on it. This software regularly monitors for the presence of viruses and malicious software in computers. It helps with early detection and removal of malicious code. Antivirus applications use virus signatures to detect the presence of a malicious code in a computer. As new virus programs are written, the vendors of antivirus applications also update virus signatures for their applications. Administrators should ensure that the virus signatures are updated regularly.

Operating system updates. Manufacturers of operating systems such as Microsoft, Novell, and others keep updating their operating systems and applications. These updates are known as software updates and are available free of cost for downloading from the manufacturers' web sites. Every computer user is not required to download and install all updates. Some updates are meant to add a new feature to an application, and some others are meant for repairing a security bug. Operating system updates fall into the following categories:

Hotfixes

This is a small piece of software that is used to address a specific problem with the operating system. Hotfixes are generally released as soon as the manufacturer discovers a serious issue with the operating system. Test the hotfixes on nonproduction desktops before installing them on production systems. In some rare situations, hotfixes have opened up security holes in critical servers.

Patches

Software patches are released to immediately address a small problem in an application or an OS. Most of the patches are related to security but they often address other problems, such as compatibility issues or malfunctioning of a particular component of the OS.

Service packs

This is a collection of a number of hotfixes and updates released by the manufacturer of the OS or NOS. Manufacturers usually test service packs on a variety of hardware platforms and check their compatibility with various applications. As with updates and hotfixes, service packs must be fully tested on nonproduction servers before they are installed on production servers.

Application updates. Software applications should be kept updated with the latest patches or hotfixes. These updates are usually available free of cost from the vendors' web sites.

Auditing and logging. Auditing is the process of tracking or monitoring activities of users and services. Auditing allows administrators to keep an eye on malicious activities of internal users as well as of outside attackers. For example, the Object Access audit policy can reveal which users have tried to get unauthorized access to confidential data files. Audit entries are written to log files. Log files should be regularly checked to detect potential problem areas with system, network, or data access.

Network devices. As with operating systems and applications, network devices also need to be updated with the latest device drivers, firmware updates, and proper configurations. An improperly configured network router can expose the entire network and critical servers to outside attackers. Default configurations of several network devices are known to professional attackers. Administrators should disable default usernames and passwords so that attackers do not use these credentials to launch attacks against the corporate network.

Security policies. Security policies in an organization ensure that everyone follows the same set of rules related to computer and data security. Security policies in large networks are usually implemented using Group Policies. Procedures ensure that the policies are followed as required. If required, administrators can perform auditing to monitor that the security policies are followed as expected.

User education. Perhaps the most important aspect of effectively implementing security polices in a network is to train and educate users about the importance of computer security in the organization. For example, there is no use implementing a strong password policy if users write their username or password on a piece of paper and stick it to their monitors. Users should know how important the security of the organization's data is for conducting its business. They should be trained to secure their individual workstations, applications, and data.

Safety and Environmental Issues

This section is not covered in Exam 220-603.

As a computer technician, you must be aware of safety and environmental issues related to installation and maintenance of computers and their peripherals. This section covers some important aspects of safety and environmental protection.

Safety and Environment Issues

This discusses identification of safety hazards at the workplace and explains standard procedures to create a safe working environment.

Identifying potential safety hazards

A *hazard* is something that can potentially cause physical harm or injury and that can directly affect the employees (such as exposure to dangerous chemicals), or can affect the environment in general such as waste materials used in the organization. Organizations need to ensure that all hazards, physical or environmental, are identified and appropriate measures are taken to reduce the risks associated with hazardous materials used in the workplace.

In busy workplaces such as an organization using hundreds of computers, a loose and trailing cable, exposed electrical wiring or a slippery surface can all be potential safety hazards. It is important to identify any potential safety hazards. A risk assessment must be done to evaluate the hazards. Identification of hazards requires that you are able to distinguish between the following:

- Hazards in the workplace, such as its layout.
- Hazards associated with activities of the employees.
- Hazards that cause harm to the environment.

Most hazards can be easily spotted or their risk can be reduced. There are still some hazards that are generally ignored and can be dangerous. The following general guidelines can help identify potential health, safety, and environmental hazards:

- Loose or trailing network and electrical cables must be contained.
- Network and electrical cables should be running through proper routes and should not be exposed in areas where employees walk.
- Faulty electrical equipment should be either repaired or stored safely.
- Workstations located near hazardous materials should be relocated elsewhere.
- Persons working on computers, printers, and other network devices should take precautions to prevent *electrostatic discharge (ESD)*, such as wearing wrist straps.
- Ladders must be used properly.
- Material Safety Data Sheets should be on hand and consulted for proper handling, usage, transportation, and storage of hazardous materials.

- Flammable material should be handled appropriately.
- Chemicals, batteries, and cleaning products must be stored at appropriate designated places.
- Waste materials should be disposed of using appropriate guidelines.
- Proper protective wear should be used.
- Employees should be trained on safe use of hazardous materials.
- Only trained personnel should be allowed to work in locations where hazards exist. For example, a qualified electrician should be called to work on an electrical problem.

Aside from the above precautions, the workplace should be well lit and there should be adequate ventilation. A poorly laid out workplace increases the chances of accidents.

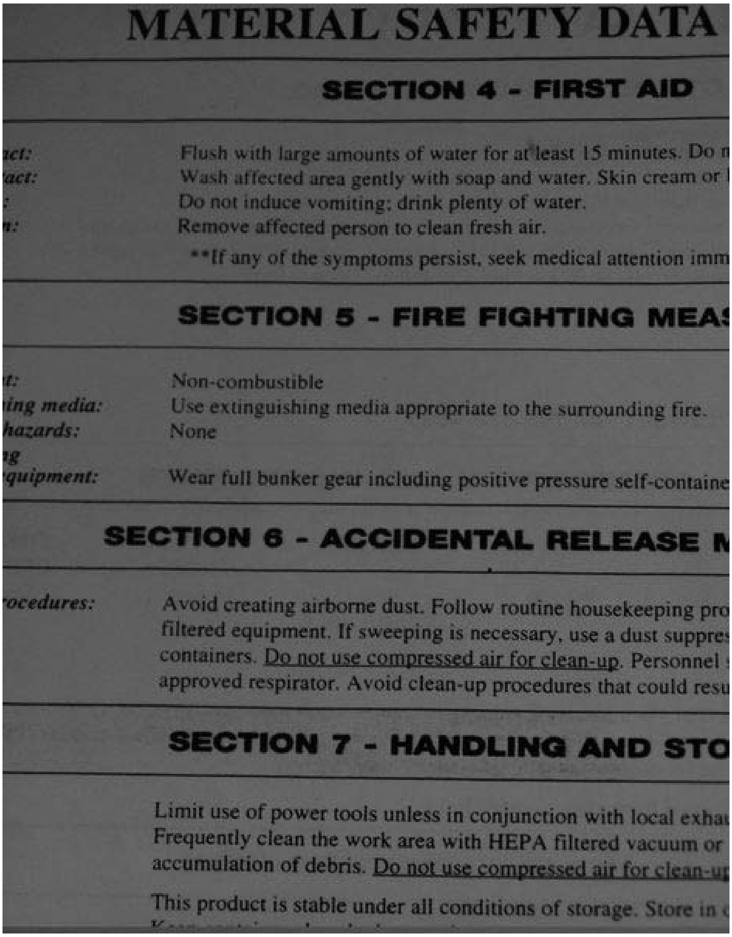
Material Safety Data Sheet (MSDS)

The MSDS is an important document required at workplaces that deal with hazardous materials such as chemicals. It is a printed document that accompanies every chemical product or other hazardous materials. MSDS provides guidance on the material's safe usage, its potential hazards, and methods for its safe disposal. In the United States, the Occupational Safety and Health Administration (OSHA) requires that every hazardous material be accompanied by an MSDS. In Canada, the Workplace Hazardous Materials Information System (WHIMS) program enforces this requirement.

The MSDS is required to identify the health and safety risks of a material and its impact on the environment. The MSDS may come as a label on the product or as a separate sheet accompanying the product packaging. Figure 2-17 shows a sample MSDS sheet.

The MSDS for a particular hazardous product essentially contains the following information:

- The name of the product, its chemical name, and the name of the manufacturer, address and telephone number.
- The ingredients of the product that are considered hazardous. For example, a product can be listed as hazardous due to reasons such as toxic, corrosive, or flammable nature.
- The physical properties of the product such as its state (solid, liquid, or gas) and its color, odor, boiling point, etc.
- Health hazards associated with the product, including guidelines for its safe usage.
- The explosive nature of the product. For example, a product might burn or explode when subjected to certain conditions.
- Procedures for safe storage, handling, moving, and transportation of the product. Information on labels or signs should be posted inside and outside the designated storage place.



MATERIAL SAFETY DATA

SECTION 4 - FIRST AID

ıct: Flush with large amounts of water for at least 15 minutes. Do n
'act: Wash affected area gently with soap and water. Skin cream or l
: Do not induce vomiting; drink plenty of water.
n: Remove affected person to clean fresh air.
**If any of the symptoms persist, seek medical attention imm

SECTION 5 - FIRE FIGHTING MEA

t: Non-combustible
ing media: Use extinguishing media appropriate to the surrounding fire.
hazards: None
ng
quipment: Wear full bunker gear including positive pressure self-containe

SECTION 6 - ACCIDENTAL RELEASE M

ocedures: Avoid creating airborne dust. Follow routine housekeeping pro
filtered equipment. If sweeping is necessary, use a dust suppre
containers. Do not use compressed air for clean-up. Personnel
approved respirator. Avoid clean-up procedures that could resu

SECTION 7 - HANDLING AND STO

Limit use of power tools unless in conjunction with local exha
Frequently clean the work area with HEPA filtered vacuum or
accumulation of debris. Do not use compressed air for clean-u

This product is stable under all conditions of storage. Store in

Figure 2-17. Material Safety Data Sheet

- Information on how to contain spillage or leakage of the product.
- Special precautions such as any protective clothing, equipment, or tools that are required to handle the product.

Workplace safety requires that the MSDS be easily accessible to all employees working near the hazardous products. It is also important that employees be provided proper training in handling of the hazardous products.

Using appropriate repair tools

When you are working as a computer support technician, you will need a bunch of tools to accomplish a given service task. It is important that you use appropriate tools in order to successfully complete the job. Using incorrect tools for a given job will not only cause unnecessary delays but can also cause personal injury. As a simple example, removing the cover from a computer cabinet requires that you have a "+" or "-" screwdriver. You cannot do this job with a set of pliers.

Similarly, you must use a correct method or technique to rectify a problem. This implies that you must also use all safety precautions when using a particular tool. As a service technician, you should carry your commonly used repair tools in your tool kit to avoid using an incorrect tool.

Handling safety incidents

Incidents related to the health and safety of the employees must immediately be reported to the management or appropriate department. Incident reporting procedures should be in place in all organizations where safety hazards exist. For example, a company involved in electrical wiring should train all its employees on safety procedures and how to handle and report incidents.

All unexpected hazards, unusual incidents, accidents, and injuries must be immediately addressed. The reporting may be in the form of verbal communication when the injury needs immediate attention. Later, an appropriate document should be prepared to elaborate on the sequence of events. Incidents can be minor, such as a simple injury that does not require immediate treatment or medication. In some situations, the incident may be serious and the affected person might require immediate medical treatment. Depending on the type and severity of the incident, any of the following approaches may be adopted for reporting the incident:

Observation of a hazard

A person working near a hazard observes a potential problem such as leakage of a gas or spillage of a chemical. The person observing the hazard can submit a written report to the concerned supervisor. The concerned department should address the incident immediately to stop deterioration of the situation.

Incident without injury

An incident occurs that does not involve the injury of anyone or there is no harm to the environment. The person observing or involved in such an incident should report it to the concerned department or staff. The department should take steps to address the problem so that the incident is not repeated in the future.

Incident involving serious injury or illness

All incidents involving serious injury or illness of one or more persons need instant attention and action from the concerned staff. The incident should be immediately reported verbally or over the telephone. A detailed report can be completed later. These types of incidents must be investigated by an internal or external agency.

Incident involving damage to the property

Incidents that might cause damage to the property or where the safety of the workplace is at stake must also be reported to the concerned staff. The concerned department might want to close the area until the problem is resolved.

Incident resulting in disturbances

There are certain incidents that do not directly relate to the workplace but that cause a significant disturbance to the employees. Examples of such incidents include a gas leak in a nearly building or smoke coming from external fire. If it is unsafe to continue working, the building may be evacuated until it is declared safe.

All incidents need to be reported. Serious incidents must be addressed immediately. An investigation should be done to find out the cause of the incident and prevent similar incidents in future. Detailed documentation should be prepared in order to train and educate employees regarding potential safety hazards. Employees must also be educated on existing safety policies and incident reporting methods.

Safety Procedures

Working with computer and network equipment requires that you conform to common safety procedures. Following safety procedures ensures that the equipment is not damaged and that you do not get involved in any unforeseen incident causing personal injury. Common safety procedures include ESD precautions and equipment handling methods.

ESD precautions

Electrostatic discharge (ESD), or *static electricity*, is the sudden discharge of a high voltage from electric or electronic equipment. It usually happens when two bodies with different electric charges come in contact with each other. Most electrostatic discharges are visible in the form of a spark while they are not visible to human eyes but still can cause significant damage to electronic components. Most people experience electrostatic discharge after walking on a carpet or when getting out of a car.

As a computer technician, you must be aware of the loss it can cause to computers, printers, network equipment, and their components. ESD can cause immediate and noticeable failure of a component that contains semiconductor devices such as processors and memory chips. It can also cause gradual degradation in performance that eventually results in complete failure. Computer parts such as motherboards, network adapters, video cards, and hard drives are very sensitive to ESD. Technicians must take necessary precautions to prevent ESD-related incidents when handling this type of equipment. Figure 2-18 shows an ESD wrist strap, which is an essential part of ESD precautions.

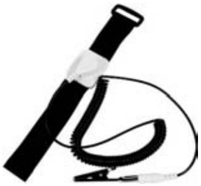


Figure 2-18. Antistatic wrist strap

Some basic ESD precautions include wearing ESD wrist straps, using ESD floor mats, and storing computer parts in ESD bags. People working on electronic components must also discharge themselves by touching a metal object before touching the component. Controlling humidity levels can also reduce the effects of ESD. Electrostatic charge is maximum when the humidity level is between 10 and 25 percent. It can be reduced by maintaining the relative humidity between 60 and 80 percent. For example, just walking on a carpet can generate approximately 35,000 volts when the humidity level is 10 to 25 percent.

Some of the essential ESD precautions include the following:

- Wearing ESD wrist straps when working on computer components.
- Placing components on antistatic ESD table mats. Do not remove the components from the packaging until they are ready to be installed.
- Discharging static electricity in your body by touching a grounded metal surface before handling computer components.
- Holding printed circuit boards such as network adapters and memory cards from edges. Avoid touching the semiconductor chips and connection pins on these cards.
- Using conductive flooring in places where repairs are done.
- Using ESD-safe protective packaging for storing and transporting components.
- Controlling humidity levels. Increasing humidity levels to 70 percent or above helps reduce static charge build-up. Cool and dry temperatures build up static electricity.
- Keeping insulating materials (such as plastic bags) prone to electrostatic charging away from static sensitive devices.

Equipment handling. Most accidents in the workplace can be prevented by safe equipment handling practices. As a computer technician, you must be trained in safety procedures involving movement, handling, and storage of expensive equipment. Safety precautions must also be taken when handling hazardous materials. Whether you are working as an in-house helpdesk technician or as an onsite technician, you must take necessary precautions to prevent accidental injury and equipment safety. The following are some of the essential safety procedures involving equipment and personal safety:

- Using ESD precautions to prevent damage to electronic components.
- Electrical and electronic equipment should be connected using grounded 3-pin power cables.
- Checking the power cords regularly for possible damage.
- Powering off and unplugging the equipment before opening the cover for service or repair.
- Moving computer parts such as CPUs and printers in carts.
- Not lifting or carrying any heavy equipment by hand.
- Storing computer equipment in designated places where humidity and temperature are controlled.
- Storing hazardous materials in designated places where proper caution signs are posted.

Disposal Procedures

As a computer service technician, you may be tasked with the disposal of damaged, unused, or irreparable material, such as computer monitors and UPS batteries. You are expected to know the procedures for safe disposal of components and chemicals. This will not only help prevent accidents due to exposure to hazardous materials but also help save the environment. In this section, we will explain procedures for safe disposal of batteries, display devices, and chemicals.

Batteries

Batteries are used almost everywhere these days. A *battery* is an electrochemical device that converts chemical energy to electrical energy and provides power to electronic devices. They contain metals and chemicals such as cadmium, copper, mercury, zinc, manganese, lithium, or nickel. These substances may be hazardous if not disposed of properly. Smaller-sized batteries such as AA, AAA, C, and D are commonly thrown in the garbage when they are exhausted. These ultimately go to landfills along with other household waste. Potential environmental and health hazards associated with batteries include the following:

- They contribute to pollution of lakes as the metals vaporize into the air.
- They expose the water and environment to lead and acid.
- They can cause burns and are dangerous to eyes and the skin.

Most batteries collected from a household are disposed of in hazardous waste landfills. One way to reduce hazards due to battery waste is to buy rechargeable batteries. Rechargeable batteries have longer life but they still contain heavy metals. Batteries can also be given to recycling programs where they exist.

Some municipal and provincial governments have waste battery collection and recycling programs. Battery dealers and retailers also collect used batteries. Batteries should not be stored in areas of high temperature to prevent explosion. They should also not be burned because the metals inside them may explode. When burned, the heavy metal such as mercury evaporates and pollutes the air quality.

Large-sized batteries such as those used in Uninterruptible Power Supplies (UPSs) and automobiles contain larger quantities of chemicals and heavy metals. These batteries should be stored in safe areas when they are not needed any longer or are completely exhausted. You should check with your municipal office for procedures and guidelines on safe disposal or a recycling program for these batteries.

Display devices

Computer display devices or monitors contain cathode ray tubes or CRT, which can contain a significant quantity of lead. Lead is considered a hazardous material, and it must be recycled or disposed off properly. The Environmental Protection Agency (EPA) has banned the dumping of CRTs in landfills. Local and statewide regulatory agencies now monitor the recycling and disposal programs for computer equipment, including CRTs.

CRTs contain toxic substances such as lead, mercury, cadmium, phosphorus, and barium. When CRTs are sent as waste to landfills, they are crushed by heavy machinery. This causes the hazardous materials inside the CRTs to be released into surrounding areas. These toxic materials ultimately contaminate our regular water supply. Similarly, when glass is crushed, it causes airborne hazards.

Recycling old, used, and irreparable CRT monitors is the best way to dispose of them. As with the disposal of batteries, most local municipalities collect hazardous materials. You should check with your local municipal office on procedures and guidelines for safe disposal of CRT monitors.

Chemicals

Some chemicals and solvents pose serious risks of personal injury, burns, itching, or other health hazards. Chemicals should be used, stored, and disposed of using the guidelines that accompany the product. In most countries, there are regulations that prohibit the draining of chemicals. Drained chemicals ultimately pollute the environment, including water and air. You must consult the label on the packaging to make sure that they are stored and disposed of using correct procedures. Chemical wastes are considered hazardous if they are:

- Corrosive
- Highly toxic
- Reactive
- Flammable

The following are some guidelines on disposing chemicals:

- Check the label on the container or read the MSDS instructions on how to safely dispose of the chemical.
- Keep unused chemicals in their original containers.
- Check with your local municipal office for procedures for disposing of chemicals.
- Do not drain the unused part of chemicals in household drainage.

Improperly drained chemicals pose serious environmental hazards. They can cause fires, or can explode and pollute the air. They may also corrode drain pipes and may mix with other chemicals to form poisonous gases.

Communications and Professionalism

This section is not covered in Exam 620-604.

Communication and professionalism are major components of customer support. A customer support or helpdesk technician should not only be skilled technically but also be a good communicator and well behaved. This is particularly true when the customer support technicians are visiting onsite customer locations for service calls. In this section, we will explain different aspects of communication and professionalism as related to computer customer support.

Communication Skills

Effective communication skills are required for every computer support technician. It does not matter whether you are working as an in-house helpdesk technician for an organization, or whether you have to travel to a customer's place for service and support calls. These include maintaining customer privacy and confidentiality, effective talking and listening skills, and asking the right questions to understand and resolve the problem. At the same time, you will try not to use technical jargon to unnecessarily impress the customer and will refrain from being judgmental. This section explains the essentials of communication skills.

Privacy and confidentiality

Due to increasing competition in almost every field today, organizations needs to ensure that its confidential data is not stolen or misused, client confidentiality is maintained, and the support technician completes his work to maintain the mutual trust.

Customer privacy, as related to computer support, refers to the fact that support technicians do not copy, take away, or misuse confidential data belonging to the organization. Most organizations take certain measures to prevent undesired disclosure of data to third parties including computer support technicians. As a support technician, you will need to abide by these rules when you visit a client organization to resolve a computer-related problem. Chances are that you will come across such confidential data stored on a user's computer or her home directory. You are not supposed to copy this data or take it outside the client office in any case. If you do this, you may be subject to legal actions as per the rules of the organization or regulatory consumer privacy laws.

Client confidentiality refers to the principle that any individual or an organization should not reveal or disclose confidential information about their clients to any third party without the consent of the client. The only exception is that this disclosure is required for legal reasons. In most of the countries, this principle is enforced by law. As a computer support technician, it is your primary responsibility to respect and maintain the trust of your client.

Apart from physical theft of data, you should also keep yourself from talking to the customer in such a way that he thinks that you are being too personal and trying to obtain private information. This is social engineering. It is the process of gathering personal information about a client in order to use it later for commercial gains. This is particularly important when you are trying to gather information about a problem over the telephone or when you are talking face-to-face with a customer. You must ensure that the customer does not suspect your questioning skills.

For example, a user may reveal his username and password to you to help you resolve a connectivity problem. In case this user has remote access permissions to the network, these credentials can later be misused to get unauthorized access to the network. This is unethical and you should not indulge in any such activities.

Talking to the customer

Control your facial expressions. Do not look upset, confused, or frustrated when the user is talking. When talking to the client, make sure that your tone of voice matches your body language and facial expressions. You should not give an impression that you do not have time to talk to the client. Hurriedly asking about a problem with just a few questions and suddenly jumping to a conclusion without letting the client properly explain the problem usually results in an incorrect resolution.

When the client is talking, listen to him. Active listening is one of the most important constituents of good communication skills that a customer support technician must have. The following are some important aspects of talking to clients:

- Listen carefully and attentively.
- Let the client complete his statement.
- Do not interrupt the client.
- Do not be judgmental.
- Do not jump to conclusions.
- Use effective voice tone.
- Control your body language.
- Do not use obscene jokes or talk about sex or race.

Another important aspect of talking to clients is *paraphrasing*. Paraphrasing refers to the repetition of what the client has said in order to give him a feeling that you understand correctly what he is saying. Secondly, it gives the client a good impression that you are interested in what he has to say. Finally, it gives the client an opportunity to correct any misunderstanding.

Your verbal and nonverbal language should not contradict each other. For example, you are trying to assure the client that you are very much interested in resolving his problem, but your body language or facial expressions give the impression that you are feeling tired or frustrated. Make sure that your facial expressions, body movement, and gestures match with what you are saying.

Active listening

When talking to a user, you will need to employ the technique of active listening. Active listening ensures that whatever the user has to say is fully understood by you. In other words, active listening techniques improve mutual understanding. It is often noticed that support technicians do not listen properly, which results in misunderstanding the actual user problem and an incorrect resolution. Active listening techniques consist of the following components:

- Listen attentively and respond with a nod when needed.
- Do not look distracted.
- Do not look angry, frustrated, or confused.
- Do not keep thinking about something else.
- Keep the problem in focus.
- If necessary, take notes.

The user should not at any point in time think that you are not paying attention to what she is saying. It is quite obvious that if you do not listen to the user properly, you will either miss half of the information she is providing or completely misunderstand the problem. This often results in an incorrect approach in resolving the problem. Your first goal should be to gather as much information as you can, which should be helpful in diagnosing the problem.

Active listening does not necessarily mean that you have to agree with the user. Simply repeating what she has said confirms to the user that you are attentively listening to her and trying to understand her problem. Based on the information provided by the user, you may have to ask questions to further clarify a point or to obtain more information about the problem. When the user feels that you are paying attention and understanding her, she is encouraged to talk more and provide more information.

Asking questions

Active listening is closely related to asking reasonable questions in order to clarify the problem. The first thing you must do is listen carefully to what the client has to say. During the process, you may feel that you need more information. This information can only be gathered by asking meaningful questions. You will need to have good questioning skills to get to the root of the problem. Usually you will ask questions in order to do the following:

- Seek clarification on client statements.
- Learn whether the client has some other needs.
- Encourage the client to elaborate more on certain points.
- Gather more facts and details.

When asking questions, you must keep the following things in mind:

- The questions must be directly related to the problem.
- The customer should not feel embarrassed or let down.
- The questions should be open-ended so that the client is encouraged to come up with a variety of answers.
- It is good to show interest when the client is responding. It’s useless to ask a question if you do not bother listening to the answer.
- Do not ask too many questions in a row. Let the client respond to one question before you ask the next.

When you ask questions, listen to the answers. Do not interrupt the client but let him complete his sentence or statement. Do not just say, “Oh, I know what you mean. I faced these problems before.” This is incorrect. When asking questions, make sure that your questions do not offend the client in any way.

Use nontechnical vocabulary

Your client may or may not be a technical person. He may just be an accountant who does not know anything about computer components or software applications and may just be working on a computer to get his job done. When talking to a client, you should not use technical vocabulary (jargon) just to impress him. This will have a negative impression on the client and he may feel confused. He may also not feel like talking to you anymore, thinking that you will figure out the problem yourself. This is a dangerous step so far as problem-solving is concerned. If a client stops talking, you may not gather sufficient information to resolve the issue.

Always talk to the client in a friendly way. Use terms that the client can understand. This is known as the *frame of context*. Give examples that are relevant to the problem or to the client's job. Your target should be to get as much information as possible to correctly resolve his problem in minimum possible time.

Don't be judgmental

As a sincere customer support technician, you should not be judgmental while listening to a client's problem. This ensures that you will understand the problem correctly, diagnose it properly, and apply a resolution effectively. Nonjudgmental listening involves the following factors:

- Do not finish the sentence for your client. Let him complete what he has to say.
- Do not respond too soon or jump to a conclusion. Interpret the client's statement, think of a suitable response, and then start talking.
- Do not react emotionally to a client's statement.
- Do not try to minimize a problem.
- Never ask something like "Why?" or say something like "You should not do this."
- Never criticize a client if the problem is a result of some of his actions.
- Do not try to teach the client.

Professional Behavior

In order to work to the satisfaction of your client as well as your employer, you must follow certain basic ethical standards of customer support. These include respect for the client, professional behavior, and proper use of his property. Whether you need to use his laptop, his Internet connection, or his telephone, you must ask the client for his permission. This section explains some of the common aspects of professional behavior.

Professional behavior

A customer support technician should not only be skilled in his technical problem-solving skills but should also have a clear understanding of professional behavior. This is not only applicable to in-house helpdesk support technicians but also to those technicians who provide onsite customer support. Some of the common elements of professional behavior are as follows.

Positive attitude. Keeping a positive attitude simply means that you should avoid negative thinking. It helps find a faster and meaningful solution to problems. A positive attitude not only makes the life of a customer support technician easier but also helps maintain interest in the job. This certainly creates a good customer base for the organization he works for. You must always feel energetic about your job and motivate yourself in order to achieve success in your profession. A positive attitude will not only earn you respect, but people will also love to work with you.

A positive attitude can be maintained by positive thinking. If you are called to attend to a customer support call, the first thing you should think is that it is your duty. Do not feel that you are being forced to solve another problem. If the clients do not make mistakes or do not get into trouble, there would be no need for customer support technicians.

Keeping a positive attitude always helps you look at the brighter side. For example, when you talk to a client about a problem, keep in mind that you are the one who can solve it. Maintain a good tone in your voice and listen to the client actively. Get involved in the conversation and give the client the impression that you fully understand the problem.

Avoid arguments. It is very easy for a customer support technician to get involved in arguments with her clients. This is often the result of one or two statements and counter-statements. Arguments with clients sometimes lead to developing bitter relationships between organizations. They can even result in cancellation of valuable service.

Even when you are extremely annoyed by the statements of a client, you should try to keep your calm. If you are facing an in-house user, he may be trying to spit out the frustration caused by his workload. If you are attending to an onsite customer support call, you may find that the client is upset by the loss of business due to computer downtime. He may start arguing with you as soon as you arrive at the site. Your job is to attend to the problem and not to get involved in the arguments. You must try to listen to the client and understand whether the reason for the argument is the computer problem or some other reason, such as a leftover unresolved problem by one of your colleagues.

Understand the problem. A solution to a computer problem can only be reached when you fully understand it. Understanding the problem correctly is like getting half the job done. Talking to the client, listening to him attentively, and asking pertinent questions leads to correctly identifying the problem.

Information gathering is the first step in understanding and resolving a computer problem. In order to understand it, you must first round up information by talking to the client or by analyzing the system status. This may be in the form of a symptom noticed by the client. If the client does not have any idea how the problem occurred, you may have to collect information from the system log files. Once you have enough information, you may think of a corrective action to resolve it.

Be respectful. You will be involved in actively interacting with the client right from the moment you arrive at the client's site or the client's desktop. This interaction is usually in the form of talking to the client. You must maintain a positive attitude and be respectful to him. Never use offensive language or dirty jokes, or get involved in political, racist, or sex talks. Do not let the client feel that you are there to just attend another support call. Be respectful to the client as well as to his workplace.

As noted earlier in this section, actively listening to the client is one of the best ways to be respectful. It also shows that you are a true professional and not just another support technician. While you talk to the client, pay attention to the details hidden in his words. Sometimes, a mention of a very unrelated thing reveals the cause of the problem.

If there are language differences or the client is not able to use the language correctly to describe the problem, ask questions. Do not try to correct language or grammar mistakes and do not paraphrase his sentences only to correct what he is trying to say. These actions embarrass the client. Just make him feel that you understand what he is trying to say, instead of laughing at his language or correcting it time and again. Having said this, when it is your turn to talk to a client who has language difficulty, you should speak slowly and pause between sentences so that he can easily understand you.

Being respectful to a client also means that you should trust him when he is telling you about the problem. Also, make him feel that you understand and trust what he is saying. Do not think that the client is lying to cover his actions that may have caused the problem. If you trust the client, he will also trust in return that you are the right person to do the job. The way you look at the client while he is talking makes a big difference when it comes to respect. You should never frown at the client when you two are talking.

Interruptions. When the client is talking, you should not interrupt him. Let him complete what he has to say. Never break the conversation by just saying, "Oh, I know that. I have faced this problem many times." Interrupting the client makes him feel that you are not interested, or that you are too experienced for problems like this. He might think that you have enough knowledge to resolve the problem without his help. Listen to the client and repeat back to him what you believe he is saying. (Use the paraphrasing technique.)

One important aspect of customer support is to keep the client involved in the problem-solving process. Do not forget that if you do not listen to the client properly or do not let him say what he is trying to say, he may feel offended and may not be willing to help you. He may also leave you there alone to resolve the problem. In some situations, it is very important to take help from the client to completely resolve the problem. Consider a situation where you need to test the connectivity of a computer after rebooting it and logging on to the domain. If the client has left you at the desktop alone, you may not be able to complete the test.

Use of property

Customer support technicians working at onsite locations are regularly faced with using client property such as telephones, fax machines, and Internet access. The client organization's property must be used with care and not damaged accidentally or otherwise. There are certain rules that the support technician must follow in order to maintain good rapport among clients. This section explains some of the essential parts of professional behavior as related to use of client property.

Telephone and fax. When you need access to a telephone or a fax machine, you must get permission from the appropriate authorities. In case you just want to use the telephone on your client's desk, it is a good idea to seek his permission instead of simply picking up the phone and starting to dial a number. Once you have used the fax machine, make sure that you leave it in the same power condition as it was before you used it. This means that if the machine was powered on, leave it on, and if it was powered off and you turned it on for sending or receiving a fax, turn it off when you are done.

Desktops. As a computer support or helpdesk technician, you are supposed to resolve desktop problems. It is obvious that you will work on the desktop to identify and resolve the problem. In some situations, you might need to use another desktop to test a component or install software on another desktop. In such a situation, you must ask the user of that desktop or seek permission from her manager so that you do not violate the security policy of the organization. In case you need to move a desktop, you must be very careful while handling it.

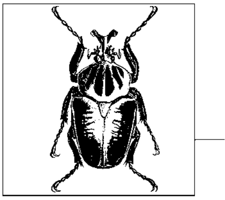
Laptops. Laptops are portable devices that can be kept and operated anywhere. You may find that most laptops are connected to a wireless part of the client organization's network. In some situations, they may also be connected to the wired network. If you are carrying your own laptop to the organization, ask for permissions from the appropriate manager or network administrator before connecting it to the wired or wireless network.

Internet. It is not unusual to use the Internet connection from remote locations these days. For example, you may need to connect to the Internet in order to download a software update, a service pack, or a new device driver from a vendor's web site. In such a situation, you should check the client organization's policy regarding guidelines or permissions for Internet usage for external users.

Printers. The same principles apply to the usage of printers as to fax machines and desktops. If you need to print some documents, you should get permission or at least inform the network administrator that you will be printing a few pages. When you are on a printer support call, you will need to print test pages to test printer configuration. Most importantly, if there is a printer problem and some documents are stuck in the printer spooler, you might need the administrator's help to clear the print queue. You should not delete any documents that are held in the print queue without first getting permission from the network administrator.

Monitors. A monitor is a delicate part of the computer and must be handled carefully. If you need to move a monitor in order to test it on a different computer or replace it with another one, ask the administrator for her help. You might get a cart to move the monitor. In case you need to test the computer using another user's monitor, ask for permission. Do not disconnect a monitor from another desktop for testing purposes without getting permission from its user or the network administrator.

Although cafeteria and restrooms are not mentioned in the A+ exam objectives, it is important to add these places in this section. These places are part of the client organization's property. It is a good idea to ask someone for permission before using these facilities. For example, instead of simply walking to the cafeteria and pouring a cup of coffee, you should accompany the onsite network administrator there. You should also be careful to leave the place clean before leaving.



3 Prep and Practice for the A+ Essentials Exam

The material in this chapter is designed to help you prepare and practice for the A+ Essentials exam. The chapter is organized into four sections:

Preparing for the A+ Essentials Exam
: This section provides an overview of the types of questions on the exam. Reviewing this will help you understand how the actual exam works.

Suggested Exercises for the A+ Essentials Exam
: This section provides a numbered list of exercises that you can follow to gain experience in the exam's subject areas. Performing the exercises will help ensure that you have hands-on experience with all areas of the exam.

Highlighters Index
: This section compiles the facts within the exam's subject areas that you are most likely to need another look at—in other words, the areas of study that you might have highlighted while reading the Study Guide. Studying the highlights is useful as a final review before the exam.

Practice Questions for the Exam
: This section includes a comprehensive set of practice questions to assess your knowledge of the concepts. The questions are similar in format to the exam. After you've reviewed the Study Guide, performed the Suggested Exercises, and studied the Highlighters Index, read the questions and see whether you can answer them correctly.

Before you take any of the A+ exams, review the exam overview, perform the suggested exercises, and go through the practice questions provided. Many online sites provide practice tests for the exam. Duplicating the depth and scope of these practice exams in a printed book isn't possible. Visit CompTIA's certification web site for pointers to online practice tests (*http://certification.comptia.org/a*).

Preparing for the A+ Essentials Exam

The A+ exams are computer-generated. The exams are timed, and an onscreen timer clock displays the amount of time remaining on the exam. Most questions on the exam are multiple choice. The multiple-choice questions are either one of the following:

Multiple-choice, single answer
A radio button allows you to select a single answer only.

Multiple-choice, multiple answer
A checkbox allows you to select multiple answers. Usually the number of correct answers is indicated in the question itself.

CompTIA reserves the right to change the testing techniques at any time. It is recommended that you visit the CompTIA A+ certification web site regularly to get updates on any changes in exam format. Individuals with adequate hands-on experience who have reviewed the Study Guide, performed the practice exercises, memorized the essentials, and taken practice tests should do well on this type of exam. Individuals who lack adequate hands-on experience and have not prepared appropriately will find the exam hard to pass.

CompTIA suggests the following tips for taking the exam:

- Read the question slowly and carefully.
- Do not expect to find clues in every question, though they may be present in some.
- Be aware of the distractions/confusions in statements. The first choice is often the best choice.
- Do not attempt to create situations based on a question. Your answer should be based on whatever information is provided.
- If you are retaking the exam, utilize your previous score report to concentrate on areas that need more study or practice.
- If you get stuck, mark and skip the question. You can do it later.

Typically, the test environment will have Previous/Next and Mark For Review options. You can navigate through the test using the Previous/Next buttons. You can click the Mark For Review checkbox to flag a question for later review.

Suggested Exercises for the A+ Essentials Exam

The A+ Essentials exam expects you to have a good understanding of concepts related to computer hardware and software. Hands-on experience is recommended and is good to have. You should be very conversant with hardware terminology, operating systems, and basic security concepts, and you should have the basic skills to troubleshoot problems. You will need to review the Study Guide and pay close attention to the areas that are new for you and with which you feel uncomfortable.

This section includes some exercises that you can perform either on a standalone computer or in a network to gain some hands-on experience. Since the A+ Essentials exam mainly covers basic knowledge and skills in installing, configuring, and troubleshooting computer hardware and software, you will need plenty of experience in completing these tasks. You must know what specifications to look for when selecting a component and how to correctly install the hardware and configure device drivers.

> It is recommended that you do not perform any of the suggested exercises in your organization or on any computer running in a production network. Create a test environment for completing these exercises. Even if you just want to view configuration settings for different components of a personal computer in a production environment, make sure a senior administrator accompanies you or you get permissions from your supervisor. In any case, you should follow the policies of the organization. For most exercises where you need to work on internal parts of a computer, make sure that you are wearing a properly grounded antistatic wrist strap.

Examine the Motherboard

1. Open the PC's case.
2. Examine the motherboard.
3. Determine the motherboard's Form Factor.
4. Determine whether it is an integrated or non-integrated motherboard.
5. Determine which components are on the motherboard and which are on adapter cards.

BIOS/Firmware

1. Examine the chipset on the motherboard.
2. Locate the BIOS chip.
3. Note the BIOS manufacturer and its version number.
4. Locate the CMOS battery.

Identify Processor and Memory

1. Locate the microprocessor.
2. Examine the motherboard to see whether it uses a socket for the processor or a slot.
3. Locate the RAM modules.
4. Determine whether extra slots are available for expanding memory.

I/O Ports and Expansion Bus Slots

1. Identify the I/O ports on the motherboard.
2. Determine which ports are integrated.
3. Make a list of I/O ports/connectors and the numbers of pins for each.
4. Examine the expansion bus and determine its type.
5. Determine whether the motherboard has an on-board AGP slot.
6. Locate the connectors for the hard disk and the floppy drive.
7. Determine the type of hard disk ports.

Power Supply and Its Connectors

1. Locate all power supply connectors.
2. Examine the color codes of wires for each connector.
3. Examine the difference between the hard disk/CD/DVD drive connector and the floppy drive connector.
4. Disconnect the connector from the motherboard and count the number of pins and determine polarity.

Memory Modules

1. Locate the latches that hold the memory modules.
2. Remove one of the installed memory modules.
3. Determine the type of the module and its capacity.
4. Reinstall the memory module after inspection.

Hard Disk Drive

1. Determine how to remove the hard disk.
2. Disconnect the hard disk's data and power connections.
3. Remove the hard disk from the drive bay.
4. Examine the Master/Slave jumper settings.
5. Reinstall the drive and reconnect data and power cables.

Input Devices

1. Remove the keyboard and mouse cables.
2. Examine the female connectors on the computer.
3. Examine the male connectors on the keyboard and the mouse.
4. Determine the type of mouse.
5. Remove and replace the rubber mouse ball.

Common Ports on a PC

1. Make a list of all expansion ports available on the computer.
2. Identify the type and number of pins for each connector.
3. Count the number of USB ports.
4. Discover the difference between an RJ-11 and RJ-45 connector.
5. Check the colors of the keyboard and mouse connectors.
6. Note the markings on audio connectors.

Cooling Fans

1. Examine the CPU fan and determine how it is installed.
2. Check the type of heat sink and its installation.
3. Carefully remove the CPU heat sink and the fan.
4. Examine the thermal compound.
5. Reinstall the heat sink and fan.
6. Locate any additional cooling fans inside the computer.

Software Diagnostic Utilities

1. Turn on the computer and read the information during startup.
2. Enter the BIOS setup and exit without saving changes.
3. Prepare an ERD disk for a Windows 2000 computer.
4. Examine the Automated System Recovery (ASR) Wizard for a Windows XP computer.

Troubleshooting

1. Remove the power supply connector from the hard disk.
2. Turn on the computer and notice symptoms or error messages.
3. Remove the data cable from the hard disk and repeat step 2.
4. Reconnect the data and power supply cables.

Preventive Maintenance

1. Perform a visual inspection of internal and external components.
2. Check whether any connectors are loose or whether any cables are damaged.
3. Turn on the computer.
4. Run the Disk Defragmenter utility and analyze the disk for fragmentation.
5. Clean the floppy drive using a cleaning diskette.
6. Clean the CD/DVD drive using an optical cleaning disk.

Laptop Motherboard, Processor, and Memory

1. Obtain the manuals for the laptop.
2. Determine how to open the laptop case.
3. Carefully open the case and examine the motherboard.
4. Locate the CPU and memory modules.
5. Determine the type of memory modules.
6. Close the laptop case carefully.

Laptop Display

1. Determine the type and size of the LCD screen.
2. Check the laptop documentation to learn the features of the LCD screen.
3. Determine the aspect ratio, contrast ratio, and maximum and native resolution.
4. Read the procedure for cleaning the LCD screen.

Safely Removing Hardware

1. Connect a USB thumb drive to a working laptop.
2. Locate the Safely Remove Hardware icon on the Taskbar.
3. Open Windows Explorer and examine the contents of the removable drive.
4. Close Windows Explorer.
5. Use the Safely Remove Hardware icon to stop and remove the drive.

Configuring Power Options

1. Open the Control Panel.
2. Open the Power Options utility.
3. Select the Portable/Laptop power scheme.
4. Configure the monitor and hard disk settings when running on battery.
5. Turn on the Hibernate mode.

Configuring Windows Desktop

1. Click on an empty area of the Windows desktop and select Properties.
2. Change the appearance and screensaver using appropriate pages.
3. Change the screen resolution from the Settings tab.

Configuring Taskbar

1. Right-click an empty area of the Taskbar and select Properties.
2. Click the Auto-Hide the Taskbar checkbox and click OK.
3. Examine how the Taskbar hides when not in use.
4. Change the settings back to always show the Taskbar.

Control Panel

1. Open the Control Panel from the Start menu.
2. Examine the icons for different utilities.
3. Double-click the System icon, examine its various tabs and settings, and then close it.

Changing the Computer Name

1. Open the System Control Panel from the Start menu.
2. Click the Computer Name tab.
3. Change the name of the computer using the Change button.
4. Restart the computer.

Exploring Windows Registry

1. Open the Run dialog box from the Start menu.
2. Type `REGEDIT.EXE` and press the Enter key to open the Windows Registry.
3. Examine the Registry subtrees but do not make any changes.
4. Close the Windows Registry.

Creating a Disk Partition

1. Open the Disk Management snap-in from the Computer Management Console.
2. Locate an unallocated space on a disk.
3. Right-click the unallocated space, select New, and then select Partition.
4. Create an Extended Partition.
5. Format the partition using the NTFS filesystem.
6. Examine the status of the partition.

Using Windows Explorer

1. Open Windows Explorer from the Accessories folder in the Start menu.
2. Expand all drives and locate your working folder.
3. Copy some files from one folder to another.
4. Move some files from one folder to another.
5. Click the Tools menu and click Folder Options.
6. Click the View tab, and then click the radio button for Show Hidden Files and Folders.

Changing File Attributes

1. Open Windows Explorer and locate a folder.
2. Right-click the folder and select Properties.

3. Change the attributes of the folder to make it a hidden file.
4. Locate another folder and change its compression attributes from the Advanced Attributes page.

Configuring File Permissions

1. Right-click a folder in Windows Explorer and select Sharing and Security.
2. From the Security tab, share the folder and enter a share name.
3. Click the Security tab and examine the available NTFS permissions.
4. Click the Advanced button and examine special NTFS permissions.

Configuring Paging File

1. Open the System Control Panel utility.
2. Click the Advanced tab and click the Settings button in the Performance area.
3. Click Advanced and click Change in the Virtual Memory area.
4. Enter the Initial Size and Maximum Size and then click Set.

Examining Advanced Boot Options

1. Restart the computer and press the F8 key immediately after POST is complete.
2. Examine the Advance Boot menu.
3. Select Safe Mode and press the Enter key.
4. Examine the Windows Desktop in Safe Mode.
5. Check whether you can connect to a network drive.
6. Repeat the process and select Safe Mode with Networking.

Preparing an ASR

1. Obtain a blank floppy disk.
2. Start the Windows Backup utility from System Tools in Accessories folder in the Start menu.
3. Click the ASR Wizard button.
4. Follow the onscreen instructions to create an ASR disk.

Creating System Restore Point (Windows XP)

1. Log on to a Windows XP Professional computer.
2. Select System Restore in the System Tools menu in the Accessories folder.
3. Create a System Restore Point and provide a name for identification.

Configuring Automatic Updates

1. Open the System Control Panel utility.
2. Click the Automatic Updates tab.
3. Enable Automatic Updates.
4. Configure Automatic Updates to download and install updates automatically.

Laser Printing Process

1. Print a document on a laser printer.
2. Hold the printed page. Notice that it is warm.
3. Print another document, selecting a different paper tray.
4. Obtain the user manual for the printer and read maintenance procedures.
5. Verify the type of memory in the printer and whether it can be upgraded.
6. Check the recommended supplies for the printer.

Inkjet Printers

1. Obtain the user manual of an inkjet printer.
2. Check the instructions for changing the ink cartridge.
3. Read the instructions to clean and align the printhead.
4. Follow the instructions to change the print cartridge.
5. Open the Device Manager and note the details of the printer driver.

Scanners

1. Examine the interface and the type of cable used to connect the scanner.
2. Turn on the scanner and examine the startup and calibration process.
3. Use a graphics application (Photoshop or Corel Draw) to scan a document.
4. Scan another document using the Scan button on the scanner.
5. Open the Device Manager and note the details of the scanner driver.

Printing Problems

1. Replace the toner cartridge of a laser printer with an empty cartridge.
2. Print a document from a computer connected to the printer.
3. Examine the quality of the printed document.
4. Replace the original toner cartridge.

Network Topologies

1. Obtain the layout diagram of your office network.
2. Determine the network topology.

3. Examine a few network cables and connectors.
4. Check how the network devices (hub or switch) are connecting the computers.
5. Examine how the cables are run from network devices to computers.

Network Cables and Connectors

1. Determine the type of cables used in the network.
2. Remove the network cable from one of the computers and examine the type of connector.
3. If fiber optic cables are in use, check where and why they are used.

Network Protocols, Services, and Addressing

1. Contact your network administrator.
2. Determine which networking protocol is used in the network and why.
3. Determine which network services are running.
4. Verify the method of network addressing.
5. Verify whether addresses are assigned to desktops automatically or manually.

WAN/Internet Connectivity

1. Determine how the computers are getting Internet Connectivity.
2. Determine the name of the ISP and the type of WAN technology.
3. Determine the bandwidth of the Internet connection.
4. Determine whether a Proxy Service is being used.

Network Troubleshooting

1. Examine the status indicators on the network adapter on a desktop.
2. Examine the color of lights when the computer is connected.
3. Remove the network cable and examine the color of indicators again.
4. Reconnect the network cable.

Authentication Methods

1. Contact your system or network administrator.
2. Determine which authentication method is used and why.
3. Determine the authentication protocol used for local users.
4. Determine the authentication protocol used for remote users.

Protection from Malicious Software

1. Log on to a Windows XP/2000 computer.
2. Check whether antivirus software is installed.

3. Determine whether the software is configured to automatically detect and clean viruses.
4. Download the latest virus signatures from the vendor's web site and update the software.

Password Management

1. Contact the system or network administrator.
2. Determine whether any password policies are in effect.
3. Determine what the policies are and how they are implemented.
4. Determine how often users should change their passwords.
5. Determine how many invalid logon attempts are allowed.

Preventive Maintenance for Security

1. Contact the system or network administrator.
2. Determine how preventive maintenance is carried out for security.
3. Determine the tasks performed.
4. Determine how the schedule is followed.
5. Determine whether users are allowed to update the OS and applications themselves.

Highlighters Index

In this section, we've attempted to compile the facts within the exam's subject areas that you are most likely to need another look at—in other words, the areas of study that you might have highlighted while reading the Study Guide. The title of each highlighted element corresponds to the heading title in the A+ Essentials Study Guide. In this way, if you have a question about a highlight, you can refer back to the corresponding section in the Study Guide. For the most part, the entries under a heading are organized as term lists with main points that you need to memorize for the exam.

Personal Computer Components

This subsection covers a summary of highlights from the "Personal Computer Components" section in the A+ Essentials Study Guide.

Types of motherboards

- There are two types of motherboards: integrated and nonintegrated.
- Integrated motherboards natively possess most essential components (a video adapter and network interface card are two examples) on it.
- A nonintegrated motherboard needs such components to be installed as add-on cards.
- Most new personal computers have integrated motherboards.
- The Form Factor specifies the design of the motherboard as well as details such as size and layout of components.

ATX

- ATX is an integrated motherboard Form Factor, which allows for easier expansion.
- The expansion slots are located at right angles to the processor and memory.
- The ATX Form Factor allows for better airflow for cooling the core components.
- The ATX supports *soft power off*, meaning that the OS can be used to turn off the computer.
- The power supply uses a single 20-pin connector.

Micro ATX

- Uses a smaller Form Factor than ATX and offers limited expandability.
- Contains fewer expansion slots for add-on cards and memory.
- Can fit into an ATX case.
- Provides a number of USB ports for connecting external components.

BTX

- BTX uses a smaller Form Factor than ATX and Micro ATX.
- The design provides better airflow inside the computer and reduces the need for additional cooling fans.
- It offers better placement of components for back panel I/O ports.

NLX

- Most of the components are placed sideways on riser cards.
- The add-on cards are parallel to the motherboard.
- This design uses an ATX power supply.

Chipsets

- Refers to the collection of semiconductor chips on the motherboard.
- Provides interfaces for expansion cards, memory, peripherals, and interface cards and ports.
- Each is designed to offer certain features.
- The Northbridge and the Southbridge are two types of chipsets.
- Northbridge chipset communicates with the processor using front side bus (FSB).
- Southbridge chipset controls all of the computer's onboard Input/Output (I/O) functions.

BIOS/Firmware

- This software is stored on a semiconductor chip called the BIOS chip.
- It is activated as soon as the computer is powered on.
- It detects the hardware and allocates system resources to it.
- It controls how the processor and chipsets interact with the OS.
- The CMOS chip stores certain computer settings such as the date and time.
- It gets its power from a small battery, called the CMOS battery.

Memory slots and cache

- Random Access Memory (RAM) is the primary memory of the computer.
- Motherboards have slots for expanding the memory.
- Computers use the processor cache for improved performance.
- The built-in memory inside the processor is called *L1 Cache*.
- The external cache memory is called *L2 Cache*.

Processor sockets

- The type, shape, size, and pin configuration of a processor socket depend on the processor.
- Processor sockets or slots are identified by standards.
- Sockets are flat in shape and have several rows and columns of pins.
- Most Pentium class processors use heat sinks and cooling fans because they generate considerable heat.
- The Zero Insertion Force (ZIF) socket makes it easy to insert and remove processors.
- Pentium II and III processors use slots.
- The processor is mounted on an expansion card, which is inserted vertically in the slot.

Integrated I/O ports

- Connectors for integrated I/O ports are accessible from the computer's rear side.
- The 15-pin SVGA connector is used to connect a CRT or LCD monitor.
- The 6-pin PS/2 (mini DIN) connectors are used to connect keyboards and mice.
- The 9-pin serial connector is for serial devices such as modems or scanners.
- The 25-pin parallel connector is mainly used to connect printers.
- The 8-pin RJ-45 connector is used to connect network cables.
- The 4-pin RJ-11 connector is used to connect telephone cables.
- USB connectors are used for USB devices such as printers and digital cameras.
- The IEEE 1394 connector is used to connect devices with Firewire interface.

Expansion bus slots

- Peripheral Connect Interface (PCI) slots are usually white and are about three inches long.
- The Accelerated Graphics Port (AGP) slot is brown and is for video.
- The PCI Express (PCIe) slot is designed to replace the PCI and AGP slots and possesses different sizes depending upon version (x1, x4, and x16 are the most common).
- The Audio Modem Riser (AMR) slot has 46 pins and is used on some old motherboards.
- The Communications and Networking Riser (CNR) slot has 60 pins.

- The Industry Standard Architecture (ISA) slots are black and are long in shape.
- ISA slot has two parts: one small and the other long.

Floppy disk and hard disk connectors

- The term *Enhanced Integrated Drive Electronics (EIDE)* interface is used for the Advanced Technology Attachment (ATA) interface.
- EIDE/ATA connectors have 40 pins and use a flat ribbon cable.
- The first pin on the cable is marked with a red line. Since the data is transferred in parallel fashion from the motherboard to the drive, the interface is also called Parallel ATA (PATA).
- EIDE/ATA drives use a four-pin power connector.
- The connectors for SATA interfaces have seven pins.
- SATA drives use a 15-pin power connector.

Power supplies

- A power supply converts 110-volt or 220-volt AC voltage into DC voltage.
- The rating of the power supply unit is given in watts.
- DC voltages include +3.3 volts, +5 volts, –5 volts, +12 volts, and –12 volts.
- The +3.3 volts and +5 volts DC supply is used in ATX motherboards.

Characteristics of processors

- Hyper-Threading Technology (HTT) is a form of simultaneous multithreading (SMT) used in Intel's Pentium 4 processors.
- A multicore processor integrates two or more processors into a single package.
- CPU throttling is the process of controlling the time spent by the processor on each application.
- Microcode (or microprogram) is the instruction set of a CPU.
- CPU overclocking forces the processor to run at higher clock rates for improved performance.
- Cache is a high-speed processor memory used to store data and instructions.
- A Voltage Regulator Module (VRM) provides appropriate voltage to the microprocessor.
- The speed of a microprocessor is measured in megahertz (MHz) or gigahertz (GHz).

Random Access Memory (RAM)

- This is the primary or main memory of the computer.
- It is used as temporary storage by the system and applications.
- Parity RAM uses Parity Checking for checking the integrity of data stored in RAM.
- ECC RAM automatically detects and corrects errors in memory.

Types of memory

- Dynamic Random Access Memory (DRAM)
  - Mainly used as RAM.
  - DRAM requires that the memory be periodically refreshed in order to retain its contents.
  - Variations of DRAM include SDRAM, DDR, DDR2, and RAMBUS.
  - SDRAM has a synchronous interface, and it waits for clock signal before it responds to an input.
  - SDRAM interfaces with the processor in a parallel 8-byte (64-bit) bus.
  - DDR SDRAM can double the data transfer rate by using both rising and falling edges of the clock.
  - DDR2 SDRAM doubles the clock rate by using both edges of the clock signal and then further splits a single clock into two, thus doubling the number of operations for each clock cycle.
- Static Random Access Memory (SRAM)
  - SRAM is much faster than DRAM and is mainly used for system cache.

Memory modules (Packaging)

- SIMMs have 30 pins with 8-bit data bus and 72 pins with 32-bit data bus.
- DIMM is a 64-bit module used for SDRAM, DDR, and DDR2 memory.
- Standard SDRAM has 84 pins on each side, making it a 168-pin module.
- DDR DIMM has 184 pins with one keying notch.
- DDR2 DIMM has 240 pins and an aluminum cover as a heat sink to prevent overheating.
- RIMM modules come in 16-bit (184 pins) single channel or 32-bit 232 dual channel.
- SO-DIMM, used in laptops, has 32-bit (72 pins) or 64-bit (200 pins).
- Micro DIMM has a 64-bit bus width and comes in 144-pin or 172-pin configurations.

Hard disk drives

- Hard disk drives are the main storage devices for all computers.
- A hard disk is usually 3.5 inches wide, and its capacity is measured in gigabytes (GB).
- The hard disk controller that operates the drive is located on the hard disk.
- The disk itself consists of a number of thin disks or platters and read/write heads.
- The disks spin at a speed of 3,600 to 7,200 (and even 10,000) revolutions per minute (rpm).
- The hard disk adapter, typically built-in on the motherboard, is used for signal conversion.

CD drives

- A CD-ROM is used for long-term storage and distribution of data.
- The capacity of a typical CD-ROM is about 700 MB.
- Most new CD-ROM drives are rated between 48X to 52X.
- CD burners are drives that can write data on CD-R and CD-RW discs.

DVD drives

- DVDs can store up to 4.7 GB of data on a single-sided, single-layered disk.
- A double-sided, double-layered DVD can store up to 17 GB of data.
- A DVD burner or a DVD writer can write data on a DVD disc.
- DVD formats include DVD-R, DVD+R, DVD-RW, and DVD-RAM.

Flash memory

- Flash memory is mainly used for booting devices such as network routers and switches.
- Various forms of flash memory include Secure Digital (SD) cards, USB thumb drives, and PC cards.
- SD cards are used in mobile phones, digital cameras, and camcorders.
- USB thumb drives are used for transporting data from one computer to another.

Video technologies

- Monochrome video had a maximum screen resolution of 720×350 pixels.
- CGA supports resolution of 640×200 pixels with two colors, and 320×200 pixels with four colors.
- EGA supports 16 colors with a resolution of 640×350 or 320×200 pixels.
- VGA can display 16 colors with 640×480 resolution or 256 colors with 320×200 resolution.
- VGA uses an HDB-15 D-sub connector with 15 pins arranged in 3 rows.
- SVGA supports a resolution of 800×600 pixels and 16 colors.
- New SVGA technologies support up to 1024×768 resolution and 256 colors.
- XGA supports a resolution of 1024×768 with 256 colors or 800×600 resolution with 65,536 colors.
- HDMI is a digital audio/video interface offering very high-resolution graphics and digital audio on the same connector.
- S-video is an analog video signal that carries video signals as two separate signals.
- Component video is an analog video technology that splits the video signals into red, green, and blue components.

Types of monitors

- A Cathode Ray Tube (CRT) monitor is the most commonly used display device.
- It uses an electron gun that fires electrons onto the back of the screen coated with phosphors.

- The screen glows at parts where the electrons strike.
- The dot pitch specifies the shortest distance between two dots of the same color.
- Average monitors have a dot pitch of 0.28 mm.
- The refresh rate specifies how many times the scanning beam can create an image in one second.
- The refresh rate for most monitors varies from 60 to 85 Hz.
- Liquid Crystal Display (LCD) monitors have a flat screen.
- LCD monitors are used with both laptops and desktops.

Types of port connectors

- Standard port connectors on computers are used to connect external devices.
- The USB is a common computer interface.
- A standard USB cable has a Type A connector for the computer and a Type B for the device.
- The Firewire port on the computer has a 6-pin connector, and the devices have a 4-pin connector.
- Most parallel ports use a 25-pin D-sub connector.
- A standard serial port has a 9-pin socket, and the connector is 9-pin D-sub.
- Serial cables are of two types: standard serial cable and null modem serial cable.
- RJ connectors are used for telephone (RJ-11) and network (RJ-45) connections.
- PS/2 (mini DIN) ports have six pins and are mainly used to connect the keyboard (identified with a a purple color) and the mouse (identified with a green color).
- A centronics connector is used to connect the parallel printers and SCSI devices.

Cooling fans

- The power supply fan is located inside the power supply unit.
- The rear exhaust fan is used to blow out the hot air from inside the computer case.
- The front intake fan is used to bring fresh cool air from outside the computer case.
- The CPU fan is located right on top of the CPU above a heat sink.
- The chipset fan helps cool the chipset on the motherboard.
- A video card cooling fan is used on some high-performance video cards.

CPU cooling

- The CPU is one of the greatest heat-producing components.
- The most common method of cooling the CPU is to install a heat sink right on top of it.
- A thermal compound is placed between the CPU and the heat sink.

- In liquid cooled systems, a water block is used to remove the heat from the CPU and the chipsets.
- Phase change cooling is an extreme cooling technology that takes advantage of the phase change from liquid to gas.

Drive preparation

- A typical computer motherboard has two IDE connectors for connecting up to four drives.
- The Master/Slave jumpers on IDE drives can be set to Master, Slave, or Cable Select.
- Each IDE interface can have only one Master connected to its cable. The other drive must be set to Slave.
- If connecting only one drive, set it as Master.
- You can connect up to seven drives on a single SCSI cable.
- An SCSI bus can be 8-, 16-, or 32-bit wide.
- SCSI-1 has a 50-pin connector, SCSI-2 can have a 25-, 50-, or 68-pin connector, and the SCSI-3 interface can have a 68- or 80-pin connector.
- The first connector on an internal SCSI cable is attached to the SCSI adapter, and devices are connected in a daisy-chain fashion.
- All SCSI devices are assigned a unique SCSI ID.
- A device with lower SCSI ID always gets higher priority.
- The SCSI bus must be terminated.

Installing/upgrading display devices

- Ensure that the power supply to both the computer and monitor is turned off.
- If replacing a monitor, remove the monitor cable.
- Obtain the driver for the new monitor.
- Connect the new monitor, connect the AC mains, turn on the computer, and let the computer detect the new hardware.
- If required, install the driver software using an OS utility such as the Device Manager in Windows XP/2000.
- Adjust brightness, contrast, color levels, and the horizontal and/or vertical positioning.

Basic troubleshooting theory

- Always back up the system and user data before making changes.
- Break complex problems into smaller components.
- Do not ignore even the smallest cause of the problem.
- Establish priorities when faced with several calls simultaneously.
- Complete the documentation after the problem is resolved.

Basic diagnostic procedures

- Define and identify the problem.
- Analyze the problem thoroughly to find out whether it is due to a user error, a hardware failure, or a software bug.
- Test a failed component before concluding that it has actually failed.
- Consult documentation and other resources, such as the vendor's web site, online help, or user forums.
- Apply the solution and test to confirm that it has fixed the problem.
- Prepare documentation of your activities.

Hardware tools

- The most common screwdrivers required for installation and repair of computer components are the flat blade, Phillips head, and Torx.
- Long nose pliers are required to hold connectors or pick up small screws.
- A flashlight is very helpful for locating parts of the computer where light is not adequate.
- A soldering iron is required to make connections using a solder wire.
- A wire stripper set is used to cut wire and strip off the insulation.
- A small can of compressed air is useful for removing dust from internal and external parts of the computer, fans, and other components.
- An analog or digital multimeter is used to check resistance (continuity), voltage, and current.

Software tools and utilities

- Bootable floppy disks are very useful for starting a computer using MS-DOS.
- The POST routine detects and tests major hardware components installed on the computer.
- A successful completion of POST confirms that the basic components of the computer are functioning as expected.
- Software diagnostic tools, such as MSD, help test hardware components.

Identifying problems

- Problems with the motherboard or the CPU typically result in a "dead" computer.
- If a power supply is malfunctioning, the computer will not respond when it is started.
- Problems with memory modules (RAM) can be identified from slow response of the computer.
- Display problems occur due to incorrect configuration, loose connections, or a failed monitor.
- Problems with the keyboard are caused due to a dirty environment.
- When the pointer is jumping around the screen, you may clean the mouse or replace it.

- Problems with hard disks can be due to a faulty adapter, a failed hard disk, or an incorrect/loose connection.
- Problems with CD and DVD drives are mainly related to media—i.e., the disc itself.

Preventive maintenance (PM)

- Regular PM helps reduce the chances of breakdowns and improves system performance.
- The scheduled PM should outline what PM tasks are to be performed and on what intervals.
- Visual inspection reveals whether any components are loose in sockets or whether some cooling fans are jammed.
- Device drivers, applications, and BIOS should be updated as and when new updates become available.
- Temperature and humidity should be controlled in areas where computers are installed.
- Regular cleaning of the monitor, keyboard, and mouse should be done with appropriate cleaning products.
- UPS and surge protectors should be used for a clean power supply.
- Hard disks should be regularly defragmented and unnecessary temporary files should be cleaned out.
- CD and DVD drives should be cleaned using lens cleaners.
- Tape drives should be cleaned using tape drive head cleaners.
- Floppy disk drives should be cleaned using floppy disk drive head cleaners.

Laptop and Portable Devices

This subsection covers a summary of highlights from the "Laptop and Portable Devices" section in the A+ Essentials Study Guide.

Laptop components

- The size of a laptop is much smaller than a desktop because all of its components are in a single case.
- The cost of a laptop is more than a standard desktop of comparable configuration.
- Laptop components are not equally good in performance compared to desktops, and offer limited expandability.
- Laptops require special repair skills and proprietary replacement parts.

Laptop motherboards and processors

- Most laptop motherboards are proprietary and have a small form factor compared to desktop motherboards.
- Most interfaces—such as serial, parallel, USB, video, network, modem, and sound—are integrated due to shortage of space.
- Laptop processors are usually soldered directly to the motherboard.

- Processor throttling allows the OS to put the processor in active sleep mode or slow-down mode when not in use.
- Laptop processors require less power to run than desktop processors.

Laptop power supply

- Laptops use battery power when not connected to the AC mains.
- The AC adapter charges the battery as long as the laptop is connected to the AC mains.
- A DC adapter can be plugged into a DC power outlet in a car or an airplane.
- Nickel Cadmium (NiCd), Nickel Metal Hydride (NiMH), or Lithium-Ion (LiIon) are leading types of batteries used for laptops.
- The milliAmp-Hour (mAH) rating indicates the capacity of the battery.
- Most laptops use LiIon batteries because they are lightweight and have a longer life.

Laptop memory

- Laptops use smaller memory modules called MicroDIMM or SO-DIMM.
- MicroDIMM has 144 or 172 pins and supports a 64-bit data bus.
- MicroDIMM is about half the size of a SO-DIMM and has a capacity of up to 1 GB.
- SO-DIMM has 72, 100, 144, or 200 pins.
- The 72- and 100-pin SO-DIMMs support a 32-bit data transfer while the 144- and 200-pin SO-DIMMs support a 64-bit data bus.
- SO-DIMMs have a storage capacity of up to 2 GB.

LCD technologies

- An Active Matrix LCD screen utilizes the Thin Film Transistor (TFT) technology.
- An Active Matrix LCD screen is made up of a matrix of several pixels.
- Active Matrix LCDs offer good response time, high screen resolution, and crisp picture quality.
- Passive Matrix LCD screens use a simple grid to supply a charge to a particular pixel in the display.
- Passive Matrix LCD screens offer lower screen resolution, slower response time, and poorer image quality than does an Active Matrix LCD.

Resolution, native resolution, aspect ratio, and contrast ratio

- The number of rows and columns of pixels measure screen resolution.
- Aspect ratio refers to the ratio of width and height of the screen.
- The single fixed resolution of the LCD screen is called the native resolution.
- Contrast ratio is the ratio of lightest color and the brightest color that a video display can produce.

Storage devices

- Laptops use hard drives, floppy drives, and CD/DVD drives for data storage.
- A laptop hard drive is about 2.5" wide and ½" thick, and has smaller connectors.
- The CD and DVD drives for laptops are about ½" thick.
- A floppy drive is optional in most laptops.

Pointing devices

- A trackball functions just like a normal mouse turned upside down.
- A touchpoint or a finger mouse uses a small stick with a rubber tip that moves the on-screen pointer.
- The touchpad consists of a rubber pad, which is sensitive to a finger's touch.
- On a touch screen, you just have to touch an appropriate button in order to select an item from the menu.

Laptop expansion buses and ports

- The Mini PCI bus is a 32-bit bus operating at 33 MHz that uses a 3.3 volt power connection.
- Three different form factors of Mini PCI bus are Type I, Type II, and Type III.
- Type I and Type II buses have a 100-pin connector while the Type III bus has a 124-pin connector.
- A Type I PC Card is used for memory modules, Type II is used for network and modem adapters, and Type III is used for hard drives.
- The PCMCIA bus standard is also known as the PC Card standard.
- PCMCIA 2 has a 16-bit bus, and the PCMCIA 3 has a 32-bit bus.
- Socket Services Software and Card Services Software are two main components of a PC Card.
- External devices such as thumb drives, keyboards, or a mouse can be connected using USB ports.
- Most laptops have a 15-pin VGA connector for attaching an external monitor.
- Laptops support a variety of wireless connections for networking.
- An Ethernet connection can be made using the RJ-45 port.
- A telephone line is connected for a dial-up modem using the RJ-11 port.

Docking station

- A docking station is a platform where a laptop can be installed for everyday use.
- A proprietary docking port is used to connect the laptop to the docking station.
- The docking port contains expansion ports, drive bays for storage devices, and connectors for peripherals.
- A port replicator enables you to keep the external components connected to the docking station.

Power management

- Laptops conform to ACPI or APM standards for managing how the system components use and conserve power. These standards describe how the power management features are to be implemented. For a computer to be ACPI/APM-compliant, both the hardware and the operating system must support the standards.
- The ACPI standard describes the global states, processor states, device states, and performance states.
- The S3 state defines the standby mode, and the S4 state defines the hibernate mode in Windows.
- The G2 state defines the soft off mode and the G3 state defines the mechanical off mode.

Power Options in Windows

- The Power Options utility is located within the Control Panel.
- The Power Options page allows you to select from preconfigured power-saving schemes.
- The Alarms page allows you to configure system response on low battery power.
- The Power Meter page shows the current status of the battery.
- The Advanced page allows you to configure a password when the laptop returns from standby mode.
- The Hibernate page is used to enable or disable the hibernation.

Safely removing devices

- Most of the external devices connected to a laptop are USB-compatible.
- The device should not be in use when you are preparing to remove it:
    1. Click the Safely Remove Hardware icon on the Taskbar.
    2. Select the device that you want to remove in the Safely Remove Hardware window and click the Stop button.
    3. Unplug the device when the window prompts that it is safe to remove the device.

Power problems

- Power problems may be due to the AC adapter or due to the battery pack.
- Verify that the mains power connection is good and check the small LED on top of the adapter.
- A reasonably warm adapter surface is usually an indication of a working adapter.
- Verify that the DC power cord is not damaged and that the connector is properly inserted into the laptop.
- Remove the DC power cord and verify the DC power output of the adapter with a multimeter.
- If there is no output, or a very low DC output, the AC is properly connected, and the LED is lit, try replacing the adapter with a new one.

Keyboard and pointing device problems

- If the built-in keyboard does not work, try connecting an external keyboard.
- If the pointer does not move as expected due to problems with the touchpad, try connecting an external mouse.
- Stylus problems are usually caused due to rough handling.
- A soft or hard reset helps resolve this problem, or a built-in utility can be used for this purpose.

Display problems

- The laptop display has an LCD screen, a video controller, and the inverter.
- A cut-off switch switches off the backlight when the lid is closed.
- By connecting an external monitor, you can quickly figure out whether the problem is with the LCD screen or the video controller.
- Verify that the cut-off switch is not damaged.

Networking problems

- There can be several reasons for a connectivity problem, such as loose connections, incorrect configuration, or insufficient permissions.
- For a wired network, verify that the network cable is properly attached.
- For a wireless network problem, verify that the wireless connection is enabled in Windows, that a correct SSID setting is used, and that the laptop is within the coverage area of an access point.
- You can try to use the Repair utility in Windows to reconfigure the TCP/IP protocol settings.

Preventive maintenance (PM)

- The main environmental factors that affect the performance of a laptop are temperature, humidity, and cleanliness.
- Laptops use very small components that produce heat during normal operation.
- You must ensure that the laptop is not operated in areas with high temperatures, and you must ensure that sufficient cooling is available.
- Make sure that the area where a laptop is operated is clean and dust-free.
- Always carry laptops in protective bags.

Operating Systems

This subsection covers a summary of highlights from the "Operating Systems" section in the A+ Essentials Study Guide.

Windows 3.x

- Windows 3.x was the first 16-bit OS to effectively manage computer memory.
- Windows 3.1 supported multimedia devices and had an improved GUI.
- It included error protection for system and applications through Object Linking and Embedding (OLE).
- Windows 3.11 (Windows for Workgroups) supported both 16- and 32-bit applications.

Windows 95/98/Me/NT/2000

- Windows 95 supported both 16- and 32-bit applications.
- It had the ability to network computers, and supported Plug and Play (PnP) devices.
- Windows 98 was released in 1998, followed by Windows Me.
- Windows NT Workstation and Windows NT Server had versions named Windows NT 3.5x and Windows NT 4.0.
- Windows NT supported multitasking.
- Windows NT introduced domains for effectively managing users, computers, resources, and security in the network.
- Windows 2000 OS has Windows 2000 Professional and Windows 2000 Server editions.

Windows XP

- Windows XP Professional Edition is used as a client operating system in networked environments.
- Windows XP Home Edition is used for standalone home computers.
- Windows XP Media Center Edition is used where multimedia capabilities are more important than other features.

Windows Server 2003

- Windows Server 2003 R2 is the current server OS.
- Editions of this OS include Windows Small Business Server, Web, Standard, Enterprise, and Datacenter.
- It supports both 32- and 64-bit microprocessors.
- It supports centralized management for applications, users, data storage, and security through a centralized database called Active Directory.
- It has strong support for client/server-based applications and services.
- It supports server clusters for providing fault tolerance and network load balancing for improved performance.

Windows Vista

- Windows Vista is the latest desktop operating system from Microsoft.
- Different editions of this OS include Home Basic, Home Premium, Business, Ultimate, and Enterprise.
- Windows Aero (which is a 3-D graphical interface) and centralized management are some of the attractions of Windows Vista.
- Windows Vista includes Internet Explorer 7.

MAC OS

- The MAC OS is used primarily on Apple Macintosh computers.
- Its GUI is similar to Windows and is called Aqua.
- The most current version of this OS is the MAC OS X.
- Older Apple computers used PowerPC microprocessors but now use both Power PC and Intel processors.

Linux

- Linux has Unix-like functionality and is an extremely stable and reliable OS.
- Some distributions of Linux are Red Hat, Mandrake, SuSe, and Debian.
- The hardware requirements for each variation of Linux OS are different.
- There is no standard graphical user interface for Linux.

Windows desktop

- The Windows desktop is the screen that appears after logon.
- It includes the Start menu, the Taskbar, and other icons for application shortcuts.
- You can rearrange the icons or change the desktop settings.
- The Themes page allows you to select a theme to quickly customize the look and feel of the Windows desktop.
- The Desktop page allows you to choose a background color and picture for the desktop.
- The Screen Saver page allows you to change the screensaver settings.
- The Appearance page has several settings to configure different windows, color schemes, button styles, menus, icons, and font sizes.
- The Settings tab includes options for troubleshooting and setting screen resolution and color quality, and displaying adapter configuration.
- The Effects page in Windows 2000 contains options to change the visual look of the desktop.
- The Web page in Windows 2000 contains Active Desktop settings.

Taskbar

- The Taskbar is the bottom-most part on the Windows desktop.
- It contains the Start menu, the Quick Launch area, and the Notification Area.
- The Start menu is used to run programs as well as configure system settings.
- In the middle of the Taskbar, Windows displays buttons for programs that are currently running.
- You can change the properties of the Start menu and the Taskbar by right-clicking the Taskbar and selecting an option.

Start menu

- The Start menu appears when you click the Start button.
- The Start menu includes shortcuts to installed programs, the Control Panel, a Settings button, and folders such as My Documents, My Recent Documents, My Pictures, My Music, My Computer, and My Network Places.
- The Start menu's appearance can be changed to Classic style.

Desktop icons

- The My Computer icon is used to explore the computer—including the disk drives—and to view their contents.
- The My Network Places/Network Neighborhood icon is used to browse the Windows network.
- The Recycle Bin is a folder that collects all deleted files or folders.

Control Panel

- You can use the Control Panel utilities for most of the configuration tasks related to the operating system itself as well as to the devices and drives.
- To access the Control Panel, click Start and select Control Panel.
- Windows XP first displays a list of categories of configuration items.
- Windows 2000 opens the Control Panel directly.

The System Control Panel

- The System utility in the Control Panel is used to configure system settings.
- The Computer Name (Windows XP)/Network Identification (Windows 2000) tab allows you to change the computer name and workgroup or domain membership.
- The Hardware page includes tools to manage hardware devices and drivers.
- The Advanced tab has buttons to fine-tune performance, system startup, recovery options, and environment variables.
- The System Restore utility (Windows XP) is used to restore the OS to a working condition in case it becomes unstable.
- The Remote tab (Windows XP) has options to enable/disable Remote Desktop and Remote Assistance.
- The Automatic Updates tab (Windows XP) is used to enable/disable Automatic Updates for the OS.

Windows Registry

- Windows Registry is a collection of system configuration settings.
- The Registry hierarchy is organized into keys and subkeys.
- The HKEY_CLASSES_ROOT subtree stores Object Linking and Embedding (OLE) data and file associations.
- The HKEY_CURRENT_USER subtree contains data about the currently logged-on user.
- The HKEY_LOCAL_MACHINE subtree contains all the OS and hardware-specific configuration data.
- The HKEY_USERS subtree contains a default set of settings and data for each user.
- The HKEY_CURRENT_CONFIG subtree contains data about the currently loaded hardware profile.
- The Registry can be edited using the *REGEDIT.EXE or REGEDT32.EXE* utilities.

Virtual memory

- Virtual memory is the hard disk space used for temporary data storage.
- It is also known as the swap file or paging file.
- Windows uses virtual memory when the system runs out of RAM.

Windows system files

- These files are critical to startup and normal operation of the OS.
- These files are marked as System and Hidden and are protected as Read-only.
- The *NTLDR* file is used to start loading the operating system.
- *The BOOT.INI* file is used to select an OS and the disk partition where the OS is installed.
- The *BOOTSECT.DOS* file is used in dual-boot systems and contains a copy of MS-DOS or Windows 9x OS.
- The *NTDETECT.SYS* file is used to detect installed hardware and to load a hardware profile.
- The *NTBOOTDD.SYS* file is used to detect and load the SCSI interface.
- The *NTOSKRNL.EXE* file loads the Windows operating system kernel.
- The *HAL.DLL* is the hardware abstraction layer file.

Basic disks

- Basic disks are the traditional type of disks.
- Windows OS treats all disks as Basic unless they are converted to Dynamic.
- Basic disks are divided into one or more partitions.
- Windows stores partition information in a partition table.
- Each Basic disk can have four primary partitions or three primary and one extended partition.
- One of the primary partitions is marked as the Active Partition and is used to boot the system.
- An Extended Partition is used to create logical drives.
- Logical drives cannot be marked as Active.
- Extended Partitions cannot be formatted.

Dynamic disks

- Dynamic disks are converted from Basic disks using the Disk Management utility.
- Dynamic disks treat the entire disk as a single partition.
- Dynamic volumes can be extended on single or multiple Dynamic disks.
- A Simple volume contains space from all or part of a single Dynamic disk.
- A Spanned volume contains space from single or multiple (2 to 32) Dynamic disks.
- A Striped volume combines space from 2 to 32 Dynamic disks to make a single Dynamic volume.
- Dynamic disks on Windows XP and Windows 2000 Professional do not support fault tolerance.

Filesystems

- FAT supports 8.3 file format naming and a maximum partition size of 2 GB in Windows 95/98/Me and of 4 GB in Windows NT 4.0/2000/XP.
- FAT32 is supported in Windows 95 (OSR2) and later operating systems.

- FAT32 supports long filenames up to 255 characters, and disk partitions up to 2 TB (2048 GB).
- NTFS supports Dynamic disks, long filenames up to 255 characters, disk sizes up to 16 EB (Exabytes), file-level security, Encrypting File System (EFS), compression, Disk Quotas, and files larger than 4 GB.

Windows Explorer

- Windows Explorer is used to manage files and folders.
- You can view, navigate, copy, and move files and folders.
- You can create new folders and subfolders and/or delete them.
- You can view or change file or folder attributes.
- You can search for a particular file or folder and execute program files.
- Sharing folders and setting permissions is also done in Windows Explorer.
- Windows Explorer can be used for formatting a disk.

File attributes

- Attributes determine the actions a user can perform on a file or folder.
- A file or folder with the Read-only attribute cannot be deleted or its contents cannot be changed.
- A file or folder with the Hidden attribute is not visible in Windows Explorer.
- A file or folder with the System attribute is marked as both Hidden and Read-only.
- Advanced attributes include Archiving, Indexing, Compression, and Encryption.

File permissions

- File permissions are used to control access to files.
- The Full Control permission grants a user all rights on the resource.
- The Modify permission allows a user to change the contents of the file.
- The Read and Execute permission allows a user to read the file and execute (run) it.
- The List Folder Contents (folders only) permission allows a user to list the files and subfolders inside a folder.
- The Read permission allows a user to read a file.
- The Write permission allows a user to write files to a folder.

OS installation methods

- Attended installation can be started from the setup CD-ROM or from a shared network folder.
- In an unattended installation method, an answer file provides answers to the questions that are prompted during the installation.
- The System Preparation (SysPrep) utility is a disk duplication method that is used to prepare a master image of an existing Windows XP/2000 Professional installation.
- The Remote Installation Service (RIS) is used for large-scale unattended deployments of Windows XP and Windows 2000 Professional.

Installing Windows

- Start the installation from the Windows 2000 Professional installation CD-ROM.
- Make sure that the CD-ROM is set to start before the hard disk starts.
- The setup process starts with text mode, during which the hard disk is prepared and necessary installation files are copied to the hard disk.
- In the GUI phase, the user is prompted for information about the computer, username, and password.
- The GUI phase includes the network phase, in which the setup program detects the network adapter and collects information about networking components.
- The installation completes when the setup program copies final files to the hard disk, creates Start menu items, registers components, removes temporary setup files, and restarts the computer.

Installing over the network

- The installation files are stored on a network file server known as the distribution server.
- The setup process is started using either the *winnt.exe* or *winnt32.exe* command.
- From MS-DOS or Windows 3.x, run *winnt.exe* to start the installation process.
- From Windows 95/98/Me/NT 4.0 or Windows 2000 Professional, run *winnt32.exe* to start the installation.

Post-installation tasks

- Activate the retail and evaluation versions of Windows XP Professional within 30 days of installation.
- Update the hardware device drivers.
- Install software updates for the operating system, including service packs.
- Install application software and restore user data files.

Installing devices and drivers

- You must have administrative rights in order to install devices and drivers.
- If the device driver has a digital signature, any user can install the device provided that no user interaction is required during installation.
- PnP devices are automatically detected and configured by the computer BIOS and the OS.
- Non-PnP devices need to be manually configured.

Optimizing performance

- Change the settings of the virtual file from the System Control Panel or divide it into multiple disks.
- Defragment hard disks using the Disk Management utility to improve their read/write performance.

- Use the Disk Cleanup utility to free up disk space by deleting temporary files.
- Use the Services utility in the Control Panel to identify and disable unused services.

Understanding boot sequence

- Power-On Self-Test (POST) checks the hardware components and MBR is loaded.
- The MBR loads the *NTLDR* file from the boot device.
- The *NTBOOTDD.SYS* file is loaded if the boot device is SCSI and does not have its own BIOS.
- NTLDR loads the filesystems driver to access the FAT, FAT32, or NTFS partitions.
- NTLDR reads the *BOOT.INI* file and selects an operating system.
- NTLDR calls on the *NTDETECT.COM* file to perform hardware detection.
- NTLDR calls on the *NTOSKRNL.EXE* file and the Windows kernel, which changes the screen color from black to blue.
- The kernel loads another module known as hardware abstraction layer (*HAL.DLL*).
- The kernel is initialized, and it loads low-level device drivers and filesystems.
- The device drivers initialize as they are loaded. The user mode subsystem is loaded, and the computer display changes to the graphical user interface (GUI) mode.
- Once the kernel has loaded and is initialized, the system services are started.
- The Winlogon service is started, and a logon screen is displayed.

Advanced boot options

- Safe Mode loads only minimum basic system services and device drivers sufficient to boot the OS.
- Safe Mode with Networking is similar to Safe Mode but networking devices, drivers, and services are also initialized.
- Safe Mode with Command Prompt loads the command interpreter.
- The Last Known Good Configuration option loads the last used system configuration that worked well.
- The Enable Boot Logging mode is used for diagnosing startup problems.
- The Enable VGA Mode starts Windows with basic VGA device drivers.

Recovery Console

- This is useful in resolving system startup problems.
- It allows you to repair critical system files.
- You can also enable or disable services that may be causing startup problems.
- Recovery Console can be started from the Windows setup CD-ROM, or it can be installed as one of the Advanced Boot Options.

System Restore (Windows XP)

- This helps restore the system to a working state if it has become unstable.
- It uses System Restore points to store a snapshot of system settings at regular intervals.
- It can be accessed from the System Tools in Accessories or from the Help And Support Center.

Automated System Recovery (ASR) (Windows XP)

- This is located in the Windows Backup utility.
- It is used to restore the system after a major failure.
- An ASR disk and a full backup of the system partition of the computer is required.

Troubleshooting procedures

- Talk to the user and gather information about the problem.
- Identify the potential causes.
- Isolate the problem.
- Test-related components.
- Apply and test the solution.
- Document your activities.

Operational problems

- The Blue Screen or the STOP errors are related to hardware and/or incorrectly configured drivers. They are identified by an 8-digit hexadecimal number.
- System lockup is usually caused when the system is out of resources.
- Problems with I/O devices are due to incorrect configuration of device drivers or failed devices.
- An incorrectly installed or configured application will result in the Application Failed to Start error.
- The Illegal Operation error is reported when an application attempts to perform an action that is not permitted by the operating system.
- A General Protection Fault (GPF) occurs when an application attempts to access the areas of memory that are used by other applications.
- The NTLDR is Missing error appears if any of the system startup files are missing or have become corrupt.
- The Invalid Boot Disk error is displayed when the system BIOS cannot access the boot partition of the disk.
- The Inaccessible Boot Device error appears when the computer finds a critical error with a boot device.

Disk management utilities

- The *defrag.exe* utility is used to defragment hard disks.
- The *ntbackup.exe* command starts the Windows backup utility.
- The *chkdsk.exe* utility is used to check disks for filesystem errors, and then fix them.

- The *format.exe* command is used to format a disk partition.
- The *diskpart.exe* utility in Windows XP is used to manage disks, volumes, and partitions.

System management utilities

- The Computer Management Console is a centralized place to manage the entire system, services, and applications.
- The Device Manager utility helps manage and troubleshoot hardware devices and drivers.
- The Task Manager provides a real-time view of system performance including CPU, memory, processes, networking, and applications.
- The *msconfig.exe* command opens the System Configuration Utility, which is helpful in verifying the system startup environment.
- The *regedit.exe* and *regedt32.exe* commands are used to edit the settings stored in the Windows Registry.
- The Event Viewer console displays error messages, warnings, and other information about system activities.

Printers and Scanners

This subsection covers a summary of highlights from the "Printers and Scanners" section in the A+ Essentials Study Guide.

The laser printing process

- Laser printing involves cleaning, conditioning, writing, developing, transferring, and fusing processes.
- In the cleaning process, a rubber blade in the cleaning assembly removes the particles of toner residing on the drum's surface, and a discharge lamp removes the remaining charge from the drum and makes it neutral.
- In the conditioning process, the *primary corona wire* charges the drum surface with a high negative voltage (–600 to –1000 volts).
- In the writing process, a highly focused beam of laser light scans the drum surface and removes some of the charge.
- In the developing process, the toner particles charged with –200 to –500 volts are electrostatically attracted to the drum's surface where the laser light left the image.
- In the transferring process, the positively charged paper attracts the toner particles from the drum, leaving the image on the positively charged paper when the drum is pressed over the paper.
- In the fusing process, the paper is passed through the *fuser* assembly containing *pressure rollers* and *heating rollers* to apply heat and pressure to the paper that firmly bonds the toner particles to the paper surface.

Inkjet printing process

- The printing process starts with cleaning the printhead.
- The stepper motor engages rollers to pick a piece of paper from the paper tray and guide it into the printer.

- The printhead stepper motor moves the printhead assembly across the paper and stops at each point for a fraction of a second to spray multiple dots of ink on the paper surface.
- The paper feed motor then moves the paper to the next line. This process continues until the printing process is complete.
- Once the printing process is complete, the paper feed assembly pushes the paper onto the paper tray, and the printhead is then parked in its home position.

Impact printers

- These printers use a head or a needle that is hit against an ink ribbon to place a mark on the paper.
- These produce significant noise but are very efficient for printing multipart forms.
- Dot matrix, daisy wheel, and line printers are all impact printers.

Dot matrix printers

- These printers use a printhead containing a number of pins.
- Low-resolution printers have one column of nine pins in the printhead.
- High-resolution printers have 2 columns containing 24 pins in the printhead.
- The pins strike an ink ribbon that makes impressions on paper.
- The impressions appear as small dots and form appropriate characters on paper.

Thermal printers

- These printers use heated printhead pins.
- These use heat-sensitive paper called *thermochromic* or *thermal* paper.
- Direct Thermal printers create images by burning a matrix of dots on paper.
- Thermal Wax Transfer printers use wax-based ink, which is melted from the ribbon and transferred to the paper surface.

Solid ink printers

- These printers use sticks of solid ink.
- These are used for printing high-quality graphics images.
- The ink is melted and fed into printheads that contain piezoelectric crystals.
- These printers have high-power consumption and long warm-up times.

Printer interfaces

- A parallel interface (IEEE 1284) sends an 8-bit parallel data stream to the printer.
- Parallel printers use a parallel printer cable, which has a DB-25 connector (computer) and a 36-pin Centronics connector (printer).
- A serial interface sends data to the printer one bit at a time.
- The Universal Serial Bus (USB) is the most common type of printer interface.
- The IEEE 1394 (Firewire) is the fastest of all types of computer interfaces.
- Very few printers have a Small Computer System Interface (SCSI).

Printer software

- The printer BIOS/Firmware detects various components of the printer during startup.
- The printer driver acts as an interface between the OS and the printer.
- The Page Description Language (PDL) is used to convert an incoming print job into electrical signals.

Printer supplies

- Printer paper and transparencies are collectively known as print media.
- Ink cartridges are used in inkjet and bubblejet printers.
- Ribbons are used in daisy wheel and dot-matrix printers.
- Toner cartridges are used in laser printers.
- Spare parts are considered supplies because they are used to repair printers.
- Optional upgrade components include extra paper feed trays, finishing assemblies, and printer memory.

Types of scanners

- Flatbed scanners use a glass platform where a paper is put face down. A motorized belt moves a lamp to scan the image.
- Handheld scanners move the scanner across the image.
- In sheetfed scanners the paper is manually moved over a scanning lamp.
- Drum scanners are used for high-end applications. The image is placed over a drum, and photomultiplier tubes (PMT) are used to convert optical signals into electrical signals.

Components of a scanner

- The acrylic glass plate functions as a platform for placing documents.
- The scanning head assembly contains a light source, a set of mirrors, and a lens that focuses the light onto a charged coupled device.
- The light source is made up of a cold cathode fluorescent lamp (CCFL).
- An array of charged coupled devices (CCDs) or a contact image sensor (CIS) converts the optical signals into electrical signals.
- The stepper motor assembly is used to precisely move the scanning head across the surface of the document.
- The device driver acts as an interface between the scanner and the operating system.

The scanning process

- The user places the document upside down on the glass plate.
- The document is illuminated by a CCFL.
- The scanning head is moved across the surface of the document using a belt attached to the main stepper motor.
- When the entire document is scanned, the scanner completes one pass.
- The image is passed through a set of reflective mirrors and focused onto a lens.

- The lens passes the image to an array of CCDs through an image filter.
- The scanner driver passes the image to the application software used to acquire the image from the scanner.
- The application (Photoshop, Corel Draw, etc.) uses a standard language, such as TWAIN, that acts as an interpreter between the scanner and the application.

Scanner interfaces

- Most of the newer scanners come with built-in USB or IEEE 1394 Firewire ports.
- Some older scanners use parallel, serial, and SCSI ports.

Installing printers and scanners

- Check the compatibility of the device with the OS.
- Obtain necessary hardware, connection cables, and device drivers.
- Connect the device to an appropriate port such as parallel, serial, USB, IEEE 1394, SCSI, wired, or wireless network port.
- Install the device driver.
- Configure and calibrate the device.
- Verify the installation and test the device's functionality by printing a test page or by scanning a text and graphics pages.

Troubleshooting inkjet printers

- Paper jams are a result of obstruction in the path that the paper travels.
- Paper jams can be a result of worn out rollers, the incorrect type of paper, or poor paper quality.
- Poor image quality is a result of dry ink, a damaged ink cartridge, or misalignment of the printhead.
- Blank pages are a result of an empty ink cartridge.

Troubleshooting laser printers

- Paper jams are mainly caused by poor paper quality or worn out pick up rollers.
- Blank pages appear when the toner cartridge is out of toner or when the transfer corona wire is broken.
- A faulty primary corona wire causes black pages.
- A bad toner cartridge can cause repetitive toner marks scattered across the paper.
- A damaged drum can produce vertical lines across the page.
- Ghosted images appear when the previous image is not completely erased from the surface of the EP drum.
- An incorrect printer driver causes garbled printing output.

Troubleshooting dot-matrix printers

- Dot-matrix printers need regular preventive maintenance to keep the paper path clear.
- If one of the pins on the printhead is broken, a blank line appears across the width of the paper.
- If the printer is printing nonreadable characters (garbled prints), the problem lies with the printer driver software.
- If the printer is producing consistently faded characters, the printing ribbon needs to be replaced.
- If you notice that the printing quality reduces across the width of the paper, the ribbon is possibly not rotating.

Problems with scanners

- If a powered-on scanner does not scan from the application, try to scan manually.
- Try to resolve the problem by rebooting the computer.
- Incorrect scanning resolution and dust on the glass plate, scanning lamps, or mirrors can cause poor quality of the scanned documents.
- The scanning noise is caused at startup because the scanner calibrates itself.
- If the scanner does not turn on, check the power cord and the AC mains supply.

Networks

This subsection covers a summary of highlights from the "Networks" section in the A+ Essentials Study Guide.

Types of networks

- A local area network (LAN) is a network of joined computers in a small office, a home, or a building.
- A wide area network (WAN) connects two or more LANs.
- A personal area network (PAN) is a network of devices located in close proximity of each other.
- A metropolitan area network (MAN) connects LANs in a campus or inside the boundaries of one city.

Networking models

- In the centralized computing model, all processing is done on a central computer, and the clients are called dumb terminals.
- A client/server network is based on the centralized computing model.
- A client/server network is scalable to very large-scale internetworks.
- In a decentralized computing model, all processing and resources are distributed among several computers.
- A peer-to-peer (P2P) network or a workgroup is based on a decentralized computing model.

Network topologies

- In a star topology, computers (or nodes) connect to each other through a central device, called a hub or a switch.
- In a bus topology, all computers are connected to a single cable called a backbone using T-connectors.
- In a mesh topology, each computer makes a point-to-point connection to every other computer.
- In a ring topology, each computer is connected to its neighboring computer to form a logical ring using a Multi-Station Access Unit (MSAU).
- In a wireless topology, computers connect to each other using radio frequencies.

Twisted pair cables

- These cables use pairs of insulated cables bundled inside a plastic sheath.
- The twists are used to prevent electromagnetic interference, which causes crosstalk.
- These cables are identified by category numbers denoted as CAT-1, CAT-2, CAT-3, CAT-5, etc.
- Unshielded twisted pair (UTP) cables are inexpensive. CAT5 UTP is the most commonly used type.
- Shielded twisted pair (STP) cables come with a layer of shielding material between the cables and the sheath for preventing interferences.

Plenum/PVC

- Plenum refers to the space between the main ceiling and the dropped ceiling.
- The network cable used in this space is known as plenum cable and is surrounded by a fire-retardant jacket.
- The jacket consists of a low-smoke polyvinyl chloride (PVC) or fluorinated ethylene polymer (FEP).

Fiber optic cable

- This cable is made up of very thin glass or plastic stretched out and put inside a sheath.
- The data transmission is through light signals and is immune to EMI and RF disturbances.
- Fiber optic cables are very expensive and need skilled professionals for installation and maintenance.
- The single-mode fiber optic cable uses a single beam of light and is made up of 8 to 10 micron core glass/plastic fiber surrounded by 125 micron cladding.
- The multimode fiber optic cable uses multiple beams of light and is made up of 50 or 62.5 micron core and 125 micron cladding.

Network connectors

- The Registered Jack-11 (RJ-11) is a 4-pin connector and is mainly used for terminating telephone wires.
- The Registered Jack-45 (RJ-45) is an 8-pin connector used for terminating twisted pair cables.

- An SC connector (subscriber/standard connector) is a push-pull connector used to terminate fiber optic cables.
- An ST (Straight Tip) connector uses the “twist-on/twist-off” bayonet mechanism and is an older type of fiber optic connector.
- An LC (Lucent Connector) is also used for fiber optic cables with a push-pull mechanism.

Network devices

- An Ethernet hub (concentrator) is the central device that connects all nodes in the segment.
- A switch connects multiple nodes in a network segment and sends the signal only to the destination node based on the MAC address.
- A MAU, also called a Multi-Station Access Unit (MSAU), is used in Token Ring networks as a central device.
- A network bridge connects LAN segments to form a larger segment and divide a large network segment into smaller segments.
- Routers are used to connect two or more network segments.

Transmission Control Protocol/Internet Protocol (TCP/IP)

- This is the most widely used protocol suite in private networks as well as on the Internet.
- It is a fully routable protocol.
- It is supported in all major network and desktop operating systems.

Internet Packet Exchange/Sequenced Packet Exchange (IPX/SPX)

- This is a full protocol suite used in Novell NetWare networks.
- It is fully routable.

TCP/IP addressing

- TCP/IP networks use IP addresses to identify networks and hosts.
- IP addresses are divided into public (registered) or private (unregistered) addresses.
- The IP address consists of 32 bits composed of 4 sets of 8 bytes (octet) each.
- It is expressed in dotted decimal notation.
- Classful IP addresses are divided into classes A, B, and C.
- A subnet mask is used to identify the network address from the host address.

Subnetting

- This is the process of creating two or more network segments by using the host portion of the IP address.
- It creates multiple broadcast domains to reduce broadcast traffic.
- It also increases security and helps contain network traffic to local network segments.

IPX addressing

- In NetWare, network-only servers are assigned a maximum of 47-character hostnames.
- IPX/SPX clients do not have hostnames and use their IPX addresses.
- NetWare networks are assigned a 32-bit hexadecimal address.
- The servers and workstations use a 48-bit hexadecimal address.

LAN technologies

- The 10 Mbps standards include 10Base2, 10BaseT, and 10BaseFL.
- Most of the modern networks support 100 Mbps network speed based on 100BaseTX and 100BaseFX standards.
- Gigabit Ethernet networks work at 1000 Mbps and use either copper or fiber optic cabling.
- Gigabit standards include 1000BaseLX, 1000BaseSX, and 1000BaseCX.
- The 1000BaseT standard uses four pairs of CAT 5 UTP cable.

Internet Service Provider (ISP)

- ISP refers to an organization that provides Internet access or WAN connectivity.
- ISPs provide low-cost Internet connectivity to home users via dial-up, cable modem, ISDN (BRI), or Digital Subscriber Lines (DSL).
- High-speed connectivity to large organizations is provided through gigabit Ethernet, ATM, ISDN (PRI), T-carriers, or Sonet.
- A hierarchy of lower- and higher-level ISPs exists to provide connectivity.
- ISPs interconnect with each other at a point known as Internet Exchange (IX).

Integrated Services Digital Network (ISDN)

- This allows transmission of data and voice over telephone lines.
- It requires dedicated or leased telephone lines.
- Computers using the ISDN line need an ISDN adapter or terminal adapter.
- BRI ISDN uses 2 B channels of 64 Kbps each for data/voice, and a D channel of 16 Kbps.
- PRI ISDN uses 23 B channels of 64 Kbps each for data/voice, and a D channel of 64 Kbps.

Digital Subscriber Line (DSL)

- DSL technologies use ordinary analog telephone lines to provide digital data transmissions.
- A DSL supports data transfer speeds from 128 Kbps to 24 Mbps.
- Asymmetrical DSL (ADSL) is the most common and offers higher download speed than upload speed.
- Symmetrical DSL (SDSL) supports equal speeds for both data uploads and downloads.

Wireless

- Wireless networks rely on radio frequencies to communicate.
- Wireless networks defined in IEEE 802.11 standards use radio frequencies with spread spectrum technology.
- Frequency-hopping spread spectrum (FHSS) is the method of transmitting RF signals by rapidly switching frequencies.
- Direct-sequence spread spectrum (DSSS) uses a wide band of frequency and is a modulation technique used by wireless networks.
- The most popular of the IEEE 802.11 wireless network standards are 802.11b, 802.11a, and 802.11g.

Infrared

- This provides point-to-point wireless communications using direct line of sight.
- Infrared radio waves cannot penetrate through walls.
- Infrared supports data transfer speeds ranging from 10 Mbps to 16 Mbps.
- It provides a secure wireless medium due to the short distance.

Bluetooth

- This provides short-range communications and is widely used in telephones.
- Bluetooth 2.0 supports transmission speeds up to 3 Mbps.
- It works over the unlicensed frequency range of 2.4 GHz.
- It offers high resistance to electromagnetic interferences.
- It does not require direct line of sight.

Installing a network adapter

- Ensure that the adapter is compatible with the existing computer hardware.
- Ensure that the adapter driver is meant for the OS installed on the computer.
- Check whether the adapter is PnP or non-PnP.
- Most PnP adapters are automatically detected and configured.
- Use the Add/Remove Hardware utility in the Control Panel to add a non-PnP network adapter.

Status indicators

- Status indicators on network adapters help troubleshoot connectivity problems.
- If the LED light status is “no light or yellow,” then the device or the port is not operating, not connected, or faulty.
- If the LED light status is “solid green,” then the device or port is connected but there is no activity on the port.
- If the LED light status is “flashing green,” then the device or the port is functioning and is transmitting and receiving data.
- If the LED light status is “flashing amber,” then the network is congested and collisions are occurring on the network media.

Troubleshooting network media

- Verify that connectors are properly attached.
- Verify that the cables or connectors are not damaged.
- Verify that the total length of cables does not exceed the specifications.
- Ensure that UTP cables are not run in areas of high EMI such as near transformers or beside high-voltage electric cables.

Troubleshooting network devices

- If a hub fails, all computers will get disconnected.
- A failed switch will also result in connectivity problems to all computers.
- If a router fails, an entire network segment will not connect to other segments.

Troubleshooting wireless connectivity

- Wireless signals degrade due to environmental factors such as EMI, RFI, or walls.
- Make sure that all devices support the same wireless standard on the network.
- Verify that the clients and the access point are using the correct SSID.
- Verify the encryption and authentication settings for the wireless protocol are in use.

Security

This subsection covers a summary of highlights from the "Security" section in the A+ Essentials Study Guide.

Authentication technologies and protocols

- Authentication is the process of verifying the identity of a person.
- It is the first point of controlling access to a system.
- In computer security, authentication protocols are used to verify the identity of a person or an application seeking access to a system, object, or resource.

Username and password

- The username and password combination is used in all operating systems for authentication.
- When the user enters her username and password, the local security database is checked to find a match.
- Access is granted only if a match is found.

Biometrics

- Biometric devices verify the identity of a user by using human physical and behavior characteristics.
- Biometric devices can read or measure and analyze fingerprints, as well as scan the eye retina and facial patterns and/or measure body temperature.
- Biometric authentication provides the highest level of security.

Smart cards

- These cards store a small amount of data that is used to authenticate a person.
- These prevent modification of the data stored on them.
- They are immune to EMI and RFI and have built-in protection against physical damage.

Security Tokens

- A security token is the most trusted method for verifying the identity of a user or a system.
- Security tokens are also known as Key Fobs.
- They employ multiple factors to verify the identity.
- A security token consists of two parts: a hardware device that generates token values at predetermined intervals, and a software component that tracks and verifies the validity of codes.

Digital certificates

- These are mainly used for Internet-based authentications.
- Certificates are a part of the public key infrastructure (PKI).
- They are created by a trusted third party known as the Certification Authority or the Certificate Authority (CA).
- Certificate servers are used to create, store, distribute, validate, and expire digital certificates.
- A CA used within an organization is known as an Enterprise CA or a Standalone CA.
- Revoked certificates are published in a Certification Revocation Lists (CRL).
- Certificates are also used for software signing.

Multifactor

- In computer authentication, a factor is a piece of information that is present to prove the identity of a user.
- Utilize a *something you know* factor such as the password or PIN.
- Utilize a *something you have* factor such as a hardware token or a smart card.
- Utilize a *something you are* factor such as fingerprints, eye retina, or other biometrics that can be used for identity.
- Utilize a *something you do* factor such as handwriting or voice patterns.

Challenge Handshake Authentication Protocol (CHAP)

- This is widely used for local and remote access authentication.
- It is a modified form of Password Authentication Protocol (PAP).
- It periodically verifies the authenticity of the remote user using a three-way handshake even after the communication channel has been established.
- CHAP authentication involves an authentication server and the client.
- CHAP cannot work with encrypted password databases.

Kerberos

- This is a cross-platform authentication protocol used for mutual authentication.
- Kerberos v5 is used on Windows servers as the default authentication protocol.
- It ensures the integrity of authentication data as it is transmitted over the network.
- It works in a Key Distribution Center (KDC), which is a network server.
- The KDC issues secure, encrypted keys and tokens (tickets) for authentication.
- The tickets carry a timestamp and expire as soon as the user or the service logs off.

Virus

- This is a self-replicating application that inserts itself into executable files.
- It is created for the sole purpose of destroying a user's data.
- The boot sector virus infects the first sector of a hard disk and becomes active as soon as the computer is started.
- A parasitic virus infects an executable file or an application on a computer.

Trojan

- This is a malicious code that is embedded inside a legitimate application.
- The application appears to be very useful, interesting, and harmless to the user until it is executed.
- Most modern Trojans are used to gather information about the user.
- Some Trojans allow the user's computer to be controlled remotely by the attacker.

Worm

- This does not infect any particular executable file.
- It resides in the active memory of computers.
- It keeps scanning the network for vulnerabilities and replicates itself onto other computers.

Spam

- Spam, or email spam, refers to unsolicited junk mail.
- Spam comes from unknown persons and is rarely of any use.
- Spammers collect email addresses using Spamware.

Spyware, adware, and grayware

- Spyware is used to collect personal information stored in the computer.
- Adware is the software that displays pop-up advertisements on your computer.
- Grayware programs work in an undesirable and annoying manner and may negatively affect the computer's performance.

Software firewalls

- A firewall is used to protect a private network from external networks or users.
- Windows Firewall in Windows XP SP2 is an example of personal software firewall.
- Packet Filtering Firewalls inspects the contents of each Internet Protocol (IP) packet and allows or blocks packets inside the network based on predefined and configured rules.
- Application Layer Firewalls (application layer gateways) are more advanced than packet filtering, because they examine the entire packet to allow or deny traffic.
- Stateful Inspection Firewalls work by actively monitoring and inspecting the state of the network traffic.

Filesystem security

- Windows provides file- and folder-level security using the NT File System (NTFS).
- Files can also be stored and transmitted in encrypted form.
- Share permissions provide an outer layer of access control.
- NTFS permissions provide more granular control on file and folder access.

Wireless authentication

- Open system authentication is no authentication, and any computer trying to connect is granted a connection.
- Shared key authentication requires that the access point and every wireless client know the shared secret key.
- The IEEE 802.1x authentication method requires use of advanced encryption and authentication techniques to provide strong authentication.
- WPA or WPA2 with Preshared Key authentication methods can be used for smaller home or office networks that cannot implement the IEEE 802.1x authentication mechanisms.

Wired Equivalent Privacy (WEP)

- This provides privacy in transmissions between the AP and wireless client.
- It uses a CRC-32 checksum for data integrity and privacy.
- It uses shared key authentication that allows encryption and decryption of wireless transmissions.
- It can use either 40- or 128-bit keys. Up to four different keys can be used.
- When it is enabled, the encryption keys and the SSID must match on the AP and the clients.

Data access security

- Files and folders should be secured using appropriate NTFS permissions.
- Local security policies should be defined on computers to restrict access.
- Access to data should be based on job roles of users.

- Access to critical data files should be audited.
- Use of floppy disks or CD/DVD discs to copy data should be prohibited.

Backups

- Data backup ensures data security in the event of a disaster or system failure.
- The full backup method backs up all the data in a single backup job.
- The incremental backup method backs up all the data that has changed after the last full or incremental backup was taken and changes the archive bit.
- The differential backup method backs up all the data that has changed after the last full backup but does not change the archive bit.
- Backup tapes must be stored in a secure offsite location.

Encryption

- This is the process of encoding a message using encryption algorithms.
- It converts readable plain text into unreadable cryptographic text or cyphertext.
- Encryption algorithms provide such security mechanisms as confidentiality, authentication, digital signatures, and public key cryptography.
- They are used to calculate a secret key, which is used to encrypt and decrypt messages.
- Symmetric algorithms use one key for both encryption and decryption of messages.
- Asymmetric algorithms use two keys—one for encryption (public key) and the other for decryption (private key).
- A hashing algorithm is used to provide integrity of data.

Data migration

- This is the process of transferring data from one OS platform to another or from one database application to another.
- This process converts the data from one format to another.
- It is typically performed after a full backup.

Data remnant removal

- This is the process of secure destruction of data.
- It is required when old systems are replaced or when old storage media is upgraded.
- It ensures that the data does not fall into the wrong hands and cannot be misused by a third party.

Password management

- A Password Management Policy describes how a user should create, use, and change his passwords.
- Blank passwords should not be allowed for any employee.
- Passwords should have at least eight characters.
- A password should be made up of a combination of upper- and lowercase letters, special characters, and numbers.

- Employees should be forced to change their passwords regularly.
- Employees should not be allowed to reuse their old passwords for a certain amount of time.
- Administrators should use normal user accounts when not performing any administrative tasks.

Physical security

- Users should be educated to lock their workstations when not in use.
- Users can also configure screensaver passwords to protect their desktops.
- Critical servers and network equipment should be located in a locked room.
- Server rooms should be equipped with alarm systems.
- Servers and network devices should be configured with strong administrative passwords.

Incident reporting

- This is the method of informing the management or other responsible staff as soon as an incident is detected.
- If there is an Incident Response Policy in the organization, it should be followed.
- The purpose of incident reporting is to prevent the incident or minimize its effects.

Social engineering

- This is the process of getting personal or confidential information or information about an organization by taking an individual into confidence.
- User education is the best defense against social engineering attacks.

Preventive maintenance procedures for security

- Every computer in a network should have antivirus software installed on it, and the virus signatures should be kept updated.
- NTFS and share permissions should be correctly configured.
- Administrative access to systems and network devices should be granted only to authorized employees.
- Operating systems should be updated with the latest service packs, hotfixes, or security patches.
- Applications should be configured properly, and the latest updates should be installed.
- Firmware/BIOS should be updated as and when updates are available.
- Auditing should be enabled on critical systems and data, and audit logs should be regularly monitored.
- Network devices should be configured for optimum security.
- The default configuration of network devices and wireless devices should be disabled.
- Users should be educated and trained for creating a secure and safe working environment.

Safety and Environmental Issues

This subsection covers a summary of highlights from the “Safety and Environmental Issues” section in the A+ Essentials Study Guide.

Safety hazards

- A safety hazard can potentially cause physical harm or injury.
- A poorly laid-out workplace increases the chances of accidents.
- Hazards in the workplace must be identified.
- Most hazards can be easily spotted or their risk can be reduced.

Identifying safety hazards

- Identify loose or trailing network and electrical cables or cables that are not running through proper routes.
- Faulty electrical equipment should either be repaired or stored safely.
- Workstations located near hazardous materials should be relocated elsewhere.
- Persons working on electronic devices should use precautions to prevent electrostatic discharge (ESD).
- Consult MSDS for proper handling, usage, transportation, and storage of hazardous materials.
- Flammable material should be handled appropriately.
- Chemicals, batteries, and cleaning products should be stored at designated places.
- Waste materials should be disposed of using appropriate guidelines.
- Proper protective wear should be used when working with hazardous materials.
- Employees should be trained on safe use of hazardous materials.
- Only trained personnel should be allowed to work on locations where hazards exist.

Material Safety Data Sheet (MSDS)

- This is a document accompanying chemicals or other hazardous materials.
- It provides instructions on safe usage, potential hazards, and methods for safe disposal of a hazardous material.
- The MSDS contains the product name, its chemical name, the name of the manufacturer, and the address and telephone number.
- A product can be listed as hazardous due to reasons such as toxic, corrosive, or flammable nature.
- A product might burn or explode when subjected to certain conditions.
- The MSDS contains procedures for safe storage, handling, moving, and transportation of the product.
- It explains what labels or signs should be posted inside and outside the designated storage place.
- It explains how to contain spillage or leakage of the product.

Handling safety incidents

- The person observing a hazard should immediately report it to the concerned supervisor.
- Incidents that do not involve personal injury should also be reported.
- Incidents involving serious personal injury need immediate attention.
- Safety incidents can also cause damage to the property.

ESD precautions

- Wear ESD wrist straps when working on computer components.
- Place components on antistatic ESD table mats.
- Discharge static electricity in your body by touching a grounded metal surface.
- Hold printed circuit boards from the edges.
- Avoid touching the semiconductor chips and connection pins on cards.
- Use conductive flooring in places where repairs are done.
- Use ESD safe protective packaging for storing and transporting components.
- Humidity levels should be controlled. Increasing humidity levels to 70 pecent or above helps reduce static charge build-up.

Equipment handling

- Electrical and electronic equipment should be connected using grounded 3-pin power cables.
- Check the power cords regularly for possible damage.
- Power off and unplug the equipment before opening the cover for service or repair.
- Move computer parts such as CPUs and printers in carts.
- Do not lift or carry any heavy equipment by hand.
- Store computer equipment in designated places where humidity and temperature are controlled.

Disposal procedures

- Batteries contain metals and chemicals such as cadmium, copper, mercury, zinc, manganese, lithium, and nickel.
- Batteries collected from households are disposed of in hazardous waste landfills.
- CRT monitors contain toxic substances such as lead, mercury, cadmium, phosphorus, and barium.
- Batteries and monitors should be sent to recycling centers.
- Read the MSDS instructions on how to safely dispose of chemicals.
- Keep unused chemicals in their original containers.
- Do not drain the unused part of chemicals into household drainage.

Communication and Professionalism

This subsection covers a summary of highlights from the "Communications and Professionalism" section in the A+ Essentials Study Guide.

Privacy

- *Customer privacy* means that support technicians should not copy, take away, or misuse a customer's confidential data.
- *Client confidentiality* means that any individual or an organization should not disclose confidential information about their clients to any third party without the consent of the client.
- Respect and maintain the trust of your client.

Talking to the customer

- Listen carefully and attentively.
- Let the client complete his statement and do not interrupt.
- Do not be judgmental or jump to conclusions.
- Use effective voice tone and control your body language.
- Do not use obscene jokes or talk about sex or race.

Active listening

- Listen attentively and respond with a nod when needed.
- Do not look distracted, angry, frustrated, or confused.
- Do not keep thinking about something else.
- Keep the problem in focus and, if necessary, take notes.

Asking questions

- The questions should be directly related to the problem.
- The customer should not feel embarrassed or let down.
- Ask open-ended questions that encourage the client to come up with a variety of answers.
- Show interest when the client is responding.
- It's useless to ask a question if you do not bother listening to the answer.
- Let the client respond to one question before you ask another question.

Do not be judgmental

- Do not finish the sentence for your client. Let her complete what she has to say.
- Do not respond too soon or jump to a conclusion. Interpret the client statement, think of a suitable response, and then start talking.
- Do not react emotionally to a client's statement.
- Do not try to minimize a problem.
- Never ask something like "Why?" or say something like "You should not do this." Never criticize a client if the problem is a result of some of her actions.
- Do not try to teach the client.

Professional behavior

- Keep a positive attitude.
- Avoid arguments with the client.
- Try to understand the problem.
- Be respectful to the client.
- Do not interrupt the client when he is talking.

Use of property

- Ask for permission before using a client's telephone, fax machine, or other equipment.
- Ensure that the client's property is used with care.
- Ask for permission when using the Internet connection.

Practice Questions for the A+ Essentials Exam

1. You have just been hired as field technician with a computer support company. Which of the following types of motherboards are you most likely to see more than others while on the job?

   ❍ A. AT

   ❍ B. Baby AT

   ❍ C. ATX

   ❍ D. NLX

   Answer C is correct. Although you can find any of the listed motherboards in the field, the most popular of the given designs is the ATX and its variations. The AT and Baby AT designs are almost obsolete. The NLX design also did not become very popular.

2. Which of the following motherboards uses a riser card for providing expansion slots?

   ❍ A. AT

   ❍ B. Baby AT

   ❍ C. ATX

   ❍ D. NLX

   Answer D is correct. The NLX design specifies the use of a special riser card to provide expansion slots. The expansion or add-on cards become parallel to the motherboard when installed on the riser card. In all other designs, the expansion slots are available directly on the motherboard, and the add-on cards are installed in a vertical position.

3. Which of the following is another (and official) name for IDE and EIDE drives?

   ❍ A. ATA

   ❍ B. SATA

   ❍ C. SCSI

   ❍ D. EISA

Answer A is correct. The IDE/EIDE drives are the most popular ones used on personal computers. The official name for this interface is Advanced Technology Attachment (ATA). SATA refers to the Serial Advanced Technology Attachment interface, SCSI refers to Small Computer System Interface, and EISA refers to Extended Integrated Device Electronics expansion bus.

4. Which of the following ports is commonly used to connect a keyboard and a mouse?

   ○ A. RJ-45

   ○ B. PS/2

   ○ C. DB-25

   ○ D. Serial

   Answer B is correct. A 6-pin mini DIN connector is used to connect a keyboard and a mouse. The difference between two connectors is that the keyboard connector is purple while the mouse connector is green. The RJ-45 connector is for network connections, the DB-25 connector is for parallel devices, and the 9-pin serial connector is for serial devices. You may find a mouse connected to the serial port in some old computers.

5. One of the following storage devices has a large storage capacity, is used for data storage for frequent access, and does not loose its contents even when the power is turned off. Identify this device from the given list.

   ○ A. Cache

   ○ B. RAM

   ○ C. ROM

   ○ D. Hard disk

   Answer D is correct. The hard disk has the largest storage capacity among all the given devices. It does not lose its contents even when the computer is turned off. System cache and RAM are also storage devices but they retain their contents while the power is on only. Data in a ROM (Read Only Memory) can be written only once. The type of ROM used for BIOS/Firmware is called *Electrically Erasable Programmable ROM (EEPROM)* and can be programmed or *flashed*.

6. Which of the following expansion ports is always used for a high-speed, high-resolution, 3-D graphics video adapter?

   ○ A. AGP

   ○ B. PCI

   ○ C. PCIe

   ○ D. ISA

   Answer A is correct. The Accelerated Graphics Port (AGP) is specially designed for high-speed, high-resolution, graphics video adapters and is always used for these cards. Other video adapters can be connected to ISA, PCI, or PCIe expansion slots.

7. You have been asked to install an internal SCSI hard disk on a computer. Which two things must you take care of during the installation?

   ❏ A. Select the disk as Master.

   ❏ B. Leave the default Master/Slave configuration.

   ❏ C. Configure the SCSI ID.

   ❏ D. Terminate the SCSI bus.

   ❏ E. Format the disk.

   Answers C and D are correct. When installing an SCSI hard disk or any other SCSI device, you must assign it a unique SCSI ID and make sure that the SCSI bus is terminated. An SCSI device cannot function if any of these settings is missing or incorrectly configured. You can format the disk after installation.

8. Which of the following devices are most commonly used for keeping computer components cool during normal operation? Select three answers.

   ❏ A. Fan

   ❏ B. Cooling liquid

   ❏ C. Compressed air

   ❏ D. Heat sinks

   ❏ E. Thermal compound

   Answers A, D, and E are correct. Most computers have cooling fans and heat sinks. Compressed air is rarely used as a cooling agent. The thermal compound is applied between the CPU surface and the heat sink for conduction of heat from the CPU to the heat sink.

9. Which of the following ports is considered the fastest and supports a number of external devices for a laptop as well as for desktops?

   ○ A. PS/2

   ○ B. Parallel

   ○ C. USB

   ○ D. RJ-11

   Answer C is correct. The Universal Serial Bus (USB) port is available on both desktops and laptops and is the fastest port. Most new devices—such as the keyboard, mouse, printers, and scanners—have USB interfaces these days. The PS/2 port is usually meant for the keyboard and mouse on desktops while the parallel port is mainly used to connect parallel printers. The RJ-11 port is used for connecting a telephone wire for built-in modems.

10. Which of the following types of PC Cards are commonly used for devices such as network adapters, sounds cards, and modems in laptops?

    ○ A. Type I

    ○ B. Type II

    ○ C. Type III

    ○ D. Type IV

Answer B is correct. The Type II PC Cards are most commonly used for expansion devices such as network adapters, sound cards, and modems. Type I bus is used for memory modules while the Type III bus is used for hard drives.

11. One of the following pointing devices has a flat surface and can convert touch signals into electrical signals to select an item on the menu displayed on the screen. Identify this device.

    ❍ A. Trackball

    ❍ B. Digitizer

    ❍ C. Touch button

    ❍ D. Touch screen

    Answer D is correct. A touch screen (also called touch pad) converts touch signals into electrical pulses when a button on the screen is touched with a finger. A trackball is just like an ordinary mouse turned upside down.

12. Which of the following ACPI-defined power states specifies the standby mode in Windows?

    ❍ A. S1

    ❍ B. S2

    ❍ C. S3

    ❍ D. S4

    Answer C is correct. The S3 power state is defined in ACPI standards as the standby mode in Windows. In this state, the computer maintains power only to the RAM. The S1 state is considered to consume the most power of all power-saving modes. The S2 state powers down the processor. The S4 state is called hibernation in Windows, and all the contents of the RAM are copied to the hard disk.

13. Which of the following operating systems is distributed as open source and does not have a standard GUI?

    ❍ A. Windows 3.11

    ❍ B. Windows NT 4

    ❍ C. Linux

    ❍ D. Mac OS X

    Answer C is correct. The Linux OS is distributed as open source by several vendors. It does not have a standard GUI. Windows-based operating systems and MAC OS X are proprietary and have a standard GUI in each version.

14. Which of the following attributes are not available on files and folders stored on a FAT32 partition? Select two answers.

    ❑ A. System

    ❑ B. Compression

    ❑ C. Encryption

    ❑ D. Hidden

    ❑ E. Read Only

Answers B and C are correct. The compression and encryption attributes are available only on files and folders that are stored on partitions formatted with the NTFS filesystem. Other attributes are available on both FAT32 and NTFS partitions.

15. Identify the tasks associated with files, folders, and disks that can be completed using Windows Explorer. Select all correct answers.

    ❑ A. Copy and move files.

    ❑ B. Rename and delete files.

    ❑ C. Perform disk defragmentation and cleanup.

    ❑ D. Create disk partitions.

    ❑ E. Format a disk.

    Answers A, B, C, and E are all correct. You can use Windows Explorer to copy and move files, rename and delete files, perform disk defragmentation and disk cleanup, and format a disk. You cannot, however, create disk partitions using Windows Explorer. For formatting a disk, you must use the FORMAT command (by right-clicking a drive within Windows Explorer) or the Disk Management snap-in.

16. How can you restore a deleted file in Windows without using the backup tapes?

    ❍ A. Using the Recycle Bin.

    ❍ B. Using the ASR wizard.

    ❍ C. Using the ERD.

    ❍ D. From the Control Panel.

    Answer A is correct. Deleted files are stored in the Recycle Bin, which is a separate folder on the hard disk. But when you delete a file using the Shift and Delete keys together, the file is not stored in the Recycle Bin and is permanently deleted. The Automated System Recovery (ASR) Wizard and the Emergency Repair Disk (ERD) are used to restore corrupt system files. You cannot use the Control Panel for restoring deleted files.

17. Which of the following file permissions is not a standard NTFS permission but a special permission?

    ❍ A. Read

    ❍ B. Execute

    ❍ C. Read Attributes

    ❍ D. Full Control

    Answer C is correct. The Read Attributes is a part of the set of special NTFS permissions. Special permissions are configured using the Advanced button in the NTFS permissions dialog box. Read, Execute, and Full Control are all standard NTFS permissions.

18. Which of the following Windows startup files is used only if there is an SCSI interface in the computer?

    ❍ A. *NTBOOTDD.SYS*

    ❍ B. *BOOTSECT.DOS*

❍ C. *NTOSKRNL.EXE*

❍ D. *BOOT.INI*

Answer A is correct. The *NTBOOTDD.SYS* file is used to detect the SCSI interface installed in a computer. This file contains the SCSI device driver and is stored on the partition from where the computer starts up. The *NTBOOTSECT.DOS* is used in dual boot systems and contains a copy of MS-DOS or Windows 9x OS. The *NTOSKRNL.EXE* file loads the Windows operating system kernel. The *BOOT.INI* file contains information about operating systems and the partition where they are installed.

19. How can you create an ERD for a Windows XP Professional computer?

❍ A. From the Windows Backup utility.

❍ B. From the System Tools.

❍ C. From the Disk Management utility.

❍ D. You cannot do it.

Answer D is correct. The ERD is used on Windows NT and Windows 2000 computers and is not supported in any version of the Windows XP operating system. In Windows XP, you can use an AS disk for restoring the operating system. The ASR Wizard is located in the Windows Backup utility.

20. You want to keep your Windows XP Professional computer up to date with the latest service packs and security patches. Which of the following utilities will you use for this purpose?

❍ A. Task Manager

❍ B. Download Manager

❍ C. Automatic Updates

❍ D. Update Manager

Answer C is correct. The Automatic Updates utility is used to configure a Windows XP computer to automatically download and install updates including the service packs and security patches. This utility is located in the System Control panel. You cannot use the Task Manager or the Disk Management tools for this purpose. There is no such term as "Update Manager" in the Windows XP operating system.

21. How much voltage is discharged from the EP drum in a laser printer by the laser beam that scans the drum with the information about the image?

❍ A. +600 volt

❍ B. -600 volt

❍ C. +100 volt

❍ D. –100 volt

Answer D is correct. The EP drum is charged to a voltage of –600 volts by the primary corona wire. When the laser beam scans the drum, it discharges parts of the drum by about –100 volts. These parts of the drum now have a negative charge of about –500 volts that is relatively higher than the remaining parts of the drum.

22. Which of the following measures is used to represent the printing speed of a dot-matrix printer?

    ❍ A. Characters per second

    ❍ B. Lines per minute

    ❍ C. Dots per second

    ❍ D. Pages per minute

    Answer A is correct. The printing speed of dot matrix printers is measured in terms of characters per second (cps), the speed of line printers is measured in terms of lines per minute (lpm), and the speed of laser printers is measured in pages per minute (ppm). Dots per second is not used for measuring the speed of any kind of printer.

23. Which of the following processes help deposit the toner from the EP drum onto paper?

    ❍ A. Writing

    ❍ B. Developing

    ❍ C. Transferring

    ❍ D. Fusing

    Answer C is correct. The transferring process deposits the toner from the EP drum to the paper. The transfer corona wire charges the paper with a high positive charge that attracts the toner from the EP drum. There are two corona wires (or corona rollers in some laser printers) in a laser printer. The primary corona wire transfers a high negative charge (–600 volt) to the EP drum.

24. Which of the following devices is used as a central device in a network using the star topology. Select two answers.

    ❏ A. Hub

    ❏ B. Bridge

    ❏ C. Switch

    ❏ D. Router

    ❏ E. Gateway

    Answers A and C are correct. The central device in a star network can be a hub or a switch. A hub just acts as a multiport repeater (which receives a signal and sends it to all connected devices) while the switch is an intelligent device that forwards signals received on its ports only to the computer to which it is addressed. Switches use the computer hardware addresses to locate and forward network traffic.

25. Which of the following types of cables is most expensive in terms of cost, installation, and maintenance?

    ❍ A. Plenum

    ❍ B. Fiber optic

    ❍ C. UTP

    ❍ D. STP

Answer B is correct. The fiber optic cable is the most expensive of all given types of cables in terms of cost, installation, and maintenance. The advantage of a fiber optic cable is that it has low attenuation, supports longer cable segments, and is immune to electromagnetic and radio frequency interferences. Plenum-rated network cables are used in plenum areas of the building. STP cables are more expensive than UTP cables and offer better protection against electromagnetic interferences.

26. Which of the following IP addresses is used as a loopback address?

○ A. 172.16.0.1

○ B. 127.0.0.1

○ C. 169.254.0.1

○ D. 192.168.0.1

Answer B is correct. The IP address 127.0.0.1 is reserved as a loopback address and is used for troubleshooting a network adapter and its configuration. IP addresses 172.16.0.1 and 192.168.0.1 are from IP address ranges reserved for private networks. The IP address 169.254.0.1 is from the IP addresses range reserved for Automatic Private IP Addressing (APIPA).

27. Which of the following protocols is responsible for addressing hosts in a TCP/IP-based network?

○ A. TCP

○ B. UDP

○ C. DHCP

○ D. IP

Answer D is correct. The Internet Protocol (IP) is responsible for addressing hosts in a TCP/IP network. The Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP) are used for sending and receiving messages between TCP/IP hosts. The Dynamic Host Configuration Protocol (DHCP) is used for automatic assignment of IP addresses to DHCP-enabled clients.

28. Which of the following troubleshooting utilities is common to all operating systems and is used for testing connectivity of two hosts on a network?

○ A. Tracert

○ B. Ipconfig

○ C. Ping

○ D. Nslookup

Answer C is correct. The Ping utility is supported in almost all operating systems to test the connectivity between two network hosts. This utility is a part of the TCP/IP protocol suite and uses Internet Control Message Protocol (ICMP) echo packets. The Tracert utility is used to trace the route a network packet takes from the source to destination. The Ipconfig utility is used in Windows to examine the TCP/IP configuration of one or more network adapters. The Nslookup utility is used to test the name resolution functionality.

29. Which of the following authentication technologies utilizes a challenge text?

❍ A. CHAP

❍ B. PAP

❍ C. EAP

❍ D. Kerberos

Answer A is correct. The Challenge Handshake Authentication Protocol (CHAP) uses a challenge text for authenticating a user. The Microsoft version of CHAP is called MS-CHAP. Password Authentication Protocol (PAP) is a simple authentication method that transmits usernames and passwords (user credentials) in clear text. Kerberos is the default authentication protocol for Windows servers and uses access tokens. Kerberos is supported in other network operating systems also. Extensible Authentication Protocol (EAP) is a general authentication protocol that supports several other authentication methods such as tokens, Kerberos, certificates, and smart cards.

30. Which of the following is not a factor in multifactor authentication?

❍ A. Something you know.

❍ B. Something you have.

❍ C. Something you are.

❍ D. Something you want to have.

Answer D is correct. The factors used in multifactor authentication techniques are: *something you are*, *something you have*, and *something you know*. *Something you want to have* is not a factor because this is what you want to have after you are authenticated.

31. Which of the following methods provides an outer layer of security for shared folders stored on an NTFS volume?

❍ A. Special permissions

❍ B. File permissions

❍ C. Share permissions

❍ D. Password policies

Answer C is correct. Share permissions provide an outer level of access control for shared folders on NTFS drives. Share level permissions are not applicable when a user logs on locally to the system. On the other hand, NTFS permissions provide a higher level of security for both local and network users. Note that share permissions can be configured on both FAT32 and NTFS volumes while file permissions are available on NTFS volumes. Password policies define how users should create and maintain their passwords.

32. What is the main purpose of a software firewall? Select two answers.

❑ A. Prevent external attacks.

❑ B. Detect malicious software.

❑ C. Improve network performance.

❑ D. Enforce security policies.

Answers A and B are correct. Software firewalls prevent external attacks on a network as well as detect malicious code that potentially affects network services. Firewalls do not help improve network performance. They also do not help enforce security policies. The best way to enforce security policies in a Windows Server-based network is to use Group Policies.

33. Which of the following is the best method for preventing social engineering attacks?

   ○ A. User education

   ○ B. Security tokens

   ○ C. Biometric devices

   ○ D. Encryption

   Answer A is correct. The best protection against social engineering attacks is to educate users on the importance of security. Users must know why security is important for individual and organization data. Security tokens and biometric devices are used for authenticating users while encryption is used to secure data while it travels on network media.

34. Which of the following safety measures help reduce the effects of static discharge? Select all correct answers.

   ❑ A. Antistatic bag

   ❑ B. Antistatic wrist strap

   ❑ C. Antistatic table mat

   ❑ D. Antistatic body wraps

   ❑ E. Antistatic head covers

   Answers A, B, and C are correct. Antistatic bags, antistatic wrist straps, and antistatic table and floor mats all help reduce the effects of static electricity.

35. What should you do with batteries that are no longer useful?

   ○ A. Recycle them.

   ○ B. Put them in the trash.

   ○ C. Flush them in the nearest sewer.

   ○ D. Burn them in a safe place.

   Answer A is correct. Batteries must be taken to a recycling center. They should not be thrown in the trash or flushed in the sewer, which will eventually send them to a landfill.

36. Which of the following contains essential information about the handling, storage, and safe disposal of hazardous chemicals?

   ○ A. OSHA

   ○ B. MSDS

   ○ C. Product label

   ○ D. All of above

   Answer B is correct. The Material Safety Data Sheet contains information about the handling, storage, transportation, and disposal of hazardous chemicals.

37. You have removed a faulty CRT monitor from your manager's computer and replaced it with a new LCD monitor. What should you do with the old CRT monitor?

   ❍ A. Put it in the trash.

   ❍ B. Discharge the high voltage and put it in the trash.

   ❍ C. Send it to the recycling center.

   ❍ D. Take it home.

   Answer C is correct. Monitors have a definite lifetime and should be sent to the recycling center after the end of their life cycle.

38. You have been called to attend to a failed server at a customer's site. Upon arrival, you find that the manager is worried about losing critical data stored on the server. How should you react?

   ❍ A. Tell him it happens everywhere and with everybody.

   ❍ B. Cheer him up with jokes.

   ❍ C. Remain serious all the time.

   ❍ D. Tell him confidently that you will do your best to rectify the problem.

   Answer D is correct. You should show confidence in resolving such problems and ensure the customer that you will try to save the data stored on the failed server.

39. You have been asked to solve a problem on a Windows XP computer. What should you do when the user is telling you about the problem?

   ❍ A. Keep smiling.

   ❍ B. Nod repeatedly to let the user know that you are listening.

   ❍ C. Take small notes.

   ❍ D. Just tell the user that you know all about this problem.

   Answer C is correct. Taking notes when the user is telling you about the problem shows that you are listening attentively. Active listening is one of the most important aspects of communication.

40. You need to shut down the DNS server, which will leave the network with only one DNS server. What should you do before you shut down the server?

   ❍ A. Inform the IT manager.

   ❍ B. Send a message to all users.

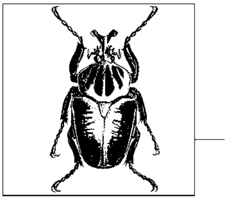
   ❍ C. Ask the users to stop using the DNS server.

   ❍ D. Postpone the shutdown until after office hours.

   Answer B is correct. The DNS server usually affects all users. Although it is important to inform the IT manager about the shutdown event, you must also send a message to all users that the DNS server is being shut down.

II

A+ Exams 220-602, 220-603, and 220-604



4

Overview of the A+ Exams 220-602, 220-603, and 220-604

After you have passed the A+ Essentials exam, you must pass one of the three available elective exams to complete your A+ certification. These exams are numbered 220-602, 220-603, and 220-604 and are for getting your IT Technician, Remote Support Technician and Depot Technician credentials, respectively. As noted earlier in this book, the A+ certification is an entry-level certification for those individuals who wish to pursue their careers in computer hardware support. The elective A+ exams let you choose the right role in the computer support industry where you intend to work or want to demonstrate your skills. Unlike the A+ Essentials exam, the elective exams are designed to test your skills beyond basic identification, installation, upgrade, and troubleshooting of personal computer hardware. The areas of study for these exams depend on the track you choose to complete your certification. The following tracks are available:

IT Technician
: The *IT Technician Exam 220-602* is meant for those individuals who work or intend to work in a corporate or mobile environment, which has a high level of face-to-face client interaction. Job titles for these skills may include Enterprise Technician, IT Administrator, Field Service Technician, or PC Technician. According to CompTIA, this certification may also be useful for some nontechnical positions such as students, sales personnel, and small business office managers.

Remote Support Technician
: The *Remote Technician Exam 220-603* is meant for those individuals who work or intend to work in a remote-based hardware support environment where client interaction, client training, operating systems, and connectivity issues are important. Job titles for these skills may include Remote Support Technician, Helpdesk Technician, or Call Center Technician.

Depot Technician

The *Depot Technician Exam 220-604* is meant for those individuals who work or intend to work in environments where client interaction is limited, but the main emphasis is on computer hardware repairs. Job titles for these skills may include Depot Technician or Bench Technician.

The A+ exams have recently been revised to include newer areas of study such as computer security, safety and environmental issues, and communications and professionalism. Another new area is knowledge of laptops and portable devices. In each of the study areas, you are expected to be skilled in identifying individual computer components as well as in installing, upgrading, and configuring them. You must also have hands-on knowledge of using appropriate tools to diagnose problems, perform preventive maintenance, and optimize performance.

The approximate percentage of each section in Exams 220-602, 220-603, and 220-604 is shown in Table 4-1.

Table 4-1. A+ exam domains and percentage of coverage

Domain	220-602	220-603	220-604
Personal computer components	18 percent	15 percent	45 percent
Laptops and mobile devices	9 percent	Not covered	20 percent
Operating systems	20 percent	29 percent	Not covered
Printers and scanners	14 percent	10 percent	20 percent
Networks	11 percent	11 percent	Not covered
Security	8 percent	15 percent	5 percent
Safety and environmental issues	5 percent	Not covered	10 percent
Communication and professionalism	15 percent	20 percent	Not covered

CompTIA recommends that in order to be prepared for the A+ exams, you should have approximately 500 hours of actual hands-on experience with computer hardware either in the field or in a lab. It is a good idea to have studied an A+ certification self-paced study guide or attended a training course before you attempt to write any of the A+ exams. You will then be ready to use this section of the book as your final exam preparation.

> This section of the book covers all three A+ elective exams: 220-602, 220-603, and 220-604. It is highly recommended that you pass the A+ Essentials exam before attempting the elective exam of your choice. Although it is not a requirement, some experts suggest writing both of the A+ exams on the same day because some of the study areas overlap. Interestingly, Exam 220-602 covers most of the skills required for other exams. The last two sections "Safety and Environmental Issues" and "Communication and Professionalism" are covered in Chapter 2 in the A+ Essentials Study Guide. Refer to Chapter 2 for revision of these topics.

Areas of Study for A+ Exams 220-602, 220-603, and 220-604

Personal Computer Components

- Install, configure, optimize and upgrade personal computer components.
  - Add, remove, and configure personal computer components, including selection and installation of appropriate components.
- Identify tools, diagnostic procedures, and troubleshooting techniques for personal computer components.
  - Identify and apply basic diagnostic procedures and troubleshooting techniques.
  - Recognize and isolate issues with peripherals, multimedia, input devices, internal and external storage, and CPUs.
  - Identify the steps used to troubleshoot components (e.g., check proper seating, installation, appropriate components, settings and current drivers).
  - Recognize names, purposes, characteristics, and appropriate application of tools.
- Perform preventive maintenance of personal computer components.
  - Identify and apply common preventive maintenance techniques for personal computer components.

Laptops and Portable Devices

This section is not covered in Exam 220-603.

- Identify the fundamental principles of using laptops and portable devices:
  - Identify appropriate applications for laptop-specific communication connections such as Bluetooth, infrared, cellular WAN, and Ethernet.
  - Identify appropriate laptop-specific power and electrical input devices and determine how amperage and voltage can affect performance.
  - Identify the major components of the LCD, including inverter, screen, and video card.
- Install, configure, optimize, and upgrade laptops and portable devices:
  - Removal of laptop-specific hardware such as peripherals, hot-swappable devices, and non-hot-swappable devices.
  - Describe how video sharing affects memory upgrades.
- Use tools, diagnostic procedures, and troubleshooting techniques for laptops and portable devices.
  - Use procedures and techniques to diagnose power conditions, video, keyboard, pointer, and wireless card issues.

Operating Systems

This section is not covered in Exam 220-604.

- Identify the fundamental principles of operating systems.
  - — Use command-line functions and utilities to manage operating systems, including proper syntax and switches.
  - — Identify concepts and procedures for creating, viewing, and managing disks, directories, and files on operating systems.
  - — Locate and use operating system utilities and available switches:
    - Device Manager and Task Manager
    - *MSCONFIG.EXE*
    - *REGEDIT.EXE*
    - *REGEDT32.EXE*
    - *CMD*
    - Event Viewer
    - System Restore
    - Remote Desktop
- Install, configure, optimize, and upgrade operating systems.
  - — Identify procedures and utilities used to optimize operating systems.
- Identify tools, diagnostic procedures, and troubleshooting techniques for operating systems.
  - — Demonstrate the ability to recover operating systems (e.g., boot methods, recovery console, ASR, or ERD).
  - — Recognize and resolve common operational problems.
  - — Recognize and resolve common error messages and codes.
  - — Use diagnostic utilities and tools to resolve operational problems.
- Perform preventive maintenance for operating systems.
  - — Demonstrate the ability to perform preventive maintenance on operating systems, including software and Windows updates (e.g., service packs), scheduled backups/restores, and restore points.

Printers and Scanners

- Identify the fundamental principles of using printers and scanners.
  - — Describe processes used by printers and scanners, including laser, ink dispersion, thermal, solid ink, and impact printers and scanners.
- Install, configure, optimize, and upgrade printers and scanners.
  - — Install and configure printers and scanners.
  - — Install and configure printer upgrades including memory and firmware.
  - — Optimize scanner performance including resolution, file format, and default settings.

- Identify tools and diagnostic procedures for troubleshooting printers and scanners.
  - — Gather information about printer and scanner problems.
  - — Review and analyze collected data.
  - — Isolate and resolve identified printer and scanner problems, including defining the cause, applying the fix, and verifying functionality.
  - — Identify appropriate tools used for troubleshooting and repairing printer and scanner problems.
- Perform preventive maintenance of printers and scanners.
  - — Perform scheduled maintenance according to vendor guidelines (e.g., install maintenance kits or reset page counts).
  - — Ensure a suitable environment.
  - — Use recommended supplies.

Networks

This section is not covered in Exam 220-604.

- Identify the fundamental principles of networks.
  - — Identify names, purposes, and characteristics of basic network protocols and terminologies.
  - — Identify names, purposes, and characteristics of technologies for establishing connectivity.
- Install, configure, optimize, and upgrade networks.
  - — Install and configure browsers.
  - — Establish network connectivity.
  - — Demonstrate the ability to share network resources.
- Use tools and diagnostic procedures to troubleshoot network problems.
  - — Identify names, purposes, and characteristics of tools.
  - — Diagnose and troubleshoot basic network issues.
  - — TCP/IP (e.g., gateway, subnet mask, DNS, WINS, and static and automatic address assignment).
  - — IPX/SPX (NWLink).
- Perform preventive maintenance of networks including securing and protecting network cabling.

Security

- Identify the fundamentals and principles of security.
  - — Identify the purposes and characteristics of access control.
  - — Identify the purposes and characteristics of auditing and event logging.
- Install, configure, upgrade, and optimize security.
  - — Install and configure software, wireless, and data security.

- Identify tool and diagnostic procedures and troubleshooting techniques for security.
  - — Diagnose and troubleshoot software and data security issues.
- Perform preventive maintenance for security.
  - — Recognize social engineering and address social engineering situations.

Safety and Environmental Issues

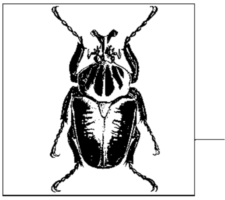
This section is not covered in Exam 220-603.

- Identify potential hazards and proper safety procedures, including power supply, display devices, and environment (e.g., trip, liquid, situational, atmospheric hazards, and high-voltage and moving equipment).

Communication and Professionalism

This section is not covered in Exam 220-604.

- Use good communication skills, including listening, tact, and discretion, when communicating with customers and colleagues.
  - — Use clear, concise, and direct statements.
  - — Allow the customer to complete statements—avoid interrupting.
  - — Clarify customer statements—ask pertinent questions.
  - — Avoid using jargon, abbreviations, and acronyms.
  - — Listen to customers.
- Use job-related professional behavior including notation of privacy, confidentiality, and respect for the customer and customers' property.
  - — Behavior
  - — Property



5

Study Guide for A+ Exams 220-602, 220-603, and 220-604

This chapter provides a study guide for CompTIA A+ Exams 220-602, 220-603, and 220-604. Various sections in this chapter are organized to cover the related objectives of the exam. Each section identifies the exam objective, provides an overview of the objective, and then discusses the key details that you should grasp before taking the exam.

Note that the Exam 220-602 includes all sections given in this chapter. Some sections are omitted in Exams 220-603 and 220-604 and have been noted at appropriate places in the chapter. An overview of the sections in this chapter is provided in the following paragraphs:

Personal Computer Components
: This section covers the basic steps involved in installing, configuring, upgrading, and troubleshooting personal computer components, such as processor, memory, and storage devices, including hard disks, removable drives, display devices, and input/output devices. Preventive maintenance of these components is also covered in this section.

Laptops and Portable Devices
: This section covers a discussion of communication technologies used for laptops and mobile devices; installation and optimization of laptop specific hardware; and basic diagnostic procedures to troubleshoot and resolve problems. *This section is not covered in Exam 220-603.*

Operating Systems
: This section discusses configuring various components of the operating system, performance optimization, troubleshooting tools and techniques, and preventive maintenance procedures. *This section is not covered in Exam 220-604.*

Printers and Scanners
: This section covers the basics of printing and scanning processes, optimizing performance, troubleshooting techniques, and preventive maintenance of printers and scanners.

Networks

This section covers the fundamentals of computer networking, installation, troubleshooting techniques, and preventive maintenance procedures. *This section is not covered in Exam 220-604.*

Security

This section discusses the basic concepts of computer security, including access control methods, configuration of software, data security, and troubleshooting. Also covered in this section are preventive maintenance measures for maintaining a secure working environment.

> The objectives for A+ Exams 220-602, 220-603, and 220-604 also include “Safety and Environmental Issues” and “Communications and Professionalism” topics. Refer back to Chapter 2 for a review of these topics. Also note that “Safety and Environmental Issues” is not covered in Exam 220-603, and “Communications and Professionalism” is not covered in Exam 220-604.

In order to complete study for these A+ exams, we recommend that you get access to a computer that can be opened and, if required, its parts can be inspected, uninstalled, reinstalled, or upgraded whenever necessary. The personal computer should preferably have the following hardware configurations:

- An Intel 233 MHz or faster processor (350 MHz recommended) with a CD-ROM or DVD drive
- A minimum of 256 MB RAM (512 MB recommended)
- A least 2 GB of free hard disk space
- A Super VGA or higher-resolution monitor
- A keyboard and a mouse

You must also have access to a printer with appropriate driver software and, if possible, a scanner. Besides this, you will need appropriate tools in order to install, uninstall, or upgrade the components of the personal computer.

> The exercises included in this Study Guide should be part of your preparation for the exam. Do not perform any exercises in a production environment and do not use any PC that you use for your regular work. Instead, create a test environment with the recommended hardware.

Personal Computer Components

This part of the A+ exam deals mainly with installing, upgrading, and basic troubleshooting of different parts of personal computers. As a hardware technician, you are expected to have good knowledge of installation and upgrading procedures for different components of personal computers, including storage devices, motherboards, processors, memory, power supplies, adapter cards, ports, and cable types used both inside the computer and for connecting external peripherals. This section provides an overview of installation, optimization, troubleshooting, and preventive maintenance procedures for these components.

Chapter 2 includes a detailed discussion of various components of personal computers, their identification, characteristics, and basic installation and troubleshooting procedures. I encourage you to review the fundamentals one more time before you take Exams 220-602, 220-603, or 220-604.

Adding, Removing, and Upgrading Computer Components

Every component inside and outside a computer needs to be installed or upgraded using certain standard procedures. Most of these procedures come in the form of instructions from the vendor. In some situations, when no predefined procedure or instructions are available, you might have to use your common sense, knowledge, skills, and experience to complete the given task. The installation and upgrade process starts right from selecting an appropriate component, installing it, and testing it to verify that it works as expected. This section provides a discussion of some basic procedures to install, remove, and upgrade computer components.

Storage devices

Hard disks, floppy disks, CD-ReWritable (CD-RW), and DVDs are all categorized as storage devices in computers. Among these, the hard disks remain the primary means of data storage. The normal size of a hard disk drive is 3.5 inches (as opposed to 5.25 inches for CD and DVD drives). When installing additional drives, you might require appropriate screws to fix the drive into the cage. It is a good idea to test the screws for their size before installing a drive in the drive cage. In this section, we will look at adding, removing, and upgrading procedures for these devices.

Selecting an appropriate storage device. Storage devices are available in various makes, models, types, and capacities. You need to have a good understanding of your requirements. When installing or upgrading a storage device, you must make sure the following is true:

- The device fulfills your storage requirements.
- The device is compatible with the existing computer hardware.
- The computer Basic Input Output System (BIOS) supports the type of device you are going to install.
- The operating system can recognize the device and use its full storage capacity.
- There are provisions in the existing system for adding another device.
- When you have selected a drive and its specification, check the return or refund policy of the vendor.
- Shop around a little to get the best price and after-sales support.

As a simple example, if you are running out of hard disk storage and want to add another drive, you must make sure that there is enough room inside the computer case for installing another drive. Some computers are already full of CDs, DVDs, and multiple hard drives and do not have room for additional devices. For CD and DVD ROM drives, you need to verify the speed of the drive. CD-Recordable (CD-R) and CD-RW drives have different speeds for reading and writing the disk. Check your requirements before you select a drive. In the case of DVD writers, make sure that the drive supports the format you are already using or intend to use. Most new drives support multiple formats such as DVD-R or DVD+R.

Installing a hard disk. Installing hard disk drives requires special attention. Make sure that the drive is kept in its protective cover until you are ready to install it. When you take out the drive from the cover, avoid touching the bare areas of the drives where its circuit board or small semiconductor parts are located. The following steps should be followed when installing a hard disk:

1. Set the jumpers on the hard disk to configure it for Cable Select, Master, or Slave (in case of multiple drives). If you put the jumper on Cable Select, the motherboard will view the drive as primary or secondary. Be careful about the orientation of the jumpers. Jumper configuration is usually printed on top of the drive. Setting the jumpers incorrectly is a common mistake when installing hard disks.
2. Select the primary or secondary hard drive cable (IDE cable) and appropriate connector. Most IDE cables have two connectors, while some of them have only a single connector. In the case of Cable Select, you can connect the hard drive to any of the connectors. The extra connector is used to install another hard drive or a CD/DVD drive.
3. In case you are replacing the drive, carefully remove the installed drive by first removing the connectors and then its screws. Make sure that you do not force the screw. In some computer cases, you might have to remove the drive cage itself that holds all drives.
4. Insert the new drive carefully in the drive cage and connect the IDE cable connector. Tighten the screws and connect the power connector. The power connector has polarity that ensures that you will not connect it in the wrong direction.
5. Reinstall the drive cage if you removed it to install the hard disk.

New hard disks must be formatted before you can use them. You can run the Disk Management snap-in on a Windows XP or Windows 2000 computer to partition and format the disk and assign drive letter(s) and volume label(s). You can also run the *format.exe* command from the command prompt to format the disk. The DISKPART utility in Windows XP can be used for all disk related tasks except formatting the disk.

> You can test whether a newly installed hard drive is working even before you format it. Connect the data cable and the power supply connector with proper orientation and turn on the computer power. The spinning sound of the hard disk confirms that the hard disk is working.

Installing a CD/DVD drive. Some computer cases do not require screws for CD and DVD drives. The drive is simply pushed, and it snaps-in and secures in its place inside the drive cage. In some other cases, the drive must be inserted and then the screws need to be tightened. The following steps should be followed when installing a CD or DVD drive in case it needs to be tightened using screws:

1. Remove the plastic slot cover from the computer case.
2. Set the appropriate jumpers on the drive to configure it as a slave drive. In most cases, the CD or DVD drive is configured as a slave drive.
3. Select the appropriate IDE cable to connect it to the primary or secondary port.
4. Insert the drive and tighten the screws. Make sure that you do not use force while using the screwdriver.
5. Connect the IDE cable carefully with the correct orientation and polarity.
6. Connect the audio cable, if available.
7. Connect the power cable.
8. Reinstall the drive cage, in case you removed it before installing the drive.

Installing a floppy disk drive. The screws used for floppy drives are different from the ones used for hard drives and CD and DVD drives. Floppy drives use small screws with fine threads. Make sure that you have the correct size of screws available. Test one or two screws before installing the drive into the cage. Follow the steps below when installing a floppy disk drive:

1. Insert the floppy drive into the drive cage at an appropriate location.
2. Tighten the screws gently. Do not use force.
3. Locate and connect the cable with the correct orientation. If this is an additional floppy drive (Drive B:), use the correct connector from the cable.
4. Connect the power cable.
5. Reinstall the drive cage, in case you removed it before installing the drive.

Motherboards

Motherboards may need to be taken out and reinstalled in computers for the purpose of troubleshooting or when they need to be replaced with new ones. When you are required to replace a motherboard, you must be careful when selecting an appropriate motherboard. The following are some guidelines for selecting motherboards:

- Define your requirements clearly and make sure your selection meets or surpasses these requirements.
- Do your homework regarding selection of a make, model, and vendor.
- Check the technical details of the board, such as the chipset used, the speed of the system bus, and the type of memory modules (RAM). The system bus speed determines how fast the data is transferred to different parts of the computer.
- Check the amount of onboard memory and the maximum supported memory, and whether there is a provision to add memory when required.

- Check what components are built onboard and what features will require add-on cards. For example, many motherboards have built-in dial-up modem and network adapters.
- Check how many expansion slots are available for add-on cards (adapters).
- Check what different kinds of I/O ports are available on board. Also check the number of ports. For example, most new motherboards have built-in firewire and several USB ports.
- If the computer is to be used for graphics applications, check the amount of video RAM available on the motherboard.

There may be other special requirements depending on how the computer is to be used. Make sure that you ask for and understand the vendor's support and return and refund policies.

Installing a motherboard. Complete the following steps to remove and/or install a motherboard in the computer case. But first, make sure that you are wearing an antistatic wrist strap, and that you keep the new motherboard in its protective cover (called the *antistatic bag*) until you are ready to install it.

1. Open the case covers carefully. The correct procedure depends on the type of case you have on the computer.
2. Remove the IDE and power cable connectors from the hard disk and CD/DVD drives as well as all the connectors from the floppy disk drives.
3. Check whether you will need to remove the drive cage in order to remove the existing motherboard and install a new one. Put all the screws in a safe place.
4. Carefully remove the front cover and then the drive cage (by removing any required screws).
5. Examine the back panel of the computer case to determine which screws need to be removed.
6. Remove the main screws that hold the motherboard to the case. You might have to remove the I/O shield as well.
7. Remove the old motherboard carefully and put it aside.
8. Hold aside all the power cables and the cables from parts such as speakers so that the area is clear of any hindrances.
9. Take out the new motherboard from its protective cover. Place the motherboard inside the case and see whether it fits well in its place. Hold the motherboard only from its sides and do not touch any components to avoid damage by static discharge from your body. Make sure that the screws can be fixed at appropriate locations (called *standoffs*). You might have to move some standoffs to appropriate places, as required by the new motherboard.
10. Secure the motherboard to the case using proper screws. This completes the physical installation.
11. Connect the power cable, the speaker cable, the reset switch cable, the hard disk LED, and other LED cables, depending on the type of motherboard and the computer case. Consult the motherboard manual for specific instructions.
12. Reconnect all cables at appropriate places.

13. Reinstall the drive cage in case you removed it earlier.
14. Test the motherboard by connecting the monitor, the keyboard, the mouse and other devices as appropriate.
15. When the testing is done and everything works perfectly, reinstall the case covers as required.

> After you have installed the motherboard, test it by installing the minimum number of components required to boot the system. Once you are sure that the motherboard is working fine, install all other components, one by one, and repeat the testing. This way you can easily detect whether any of the add-on components are not compatible with the new motherboard.

Power supplies

If you are assembling a new computer, you will find that the power supply unit comes preinstalled with the case. Most vendors of computer cases deliver power supplies with the case. If you are replacing a defective power supply, the procedure is very simple. Before you purchase a power supply unit, consider the following:

- Make sure that you select a power supply with correct voltage and current ratings.
- Different motherboard chipsets require different types of power supplies. Make sure that you obtain the correct type of power supply unit.
- Ensure that the power supply will fit into the computer case.
- Check with the vendor about the return or refund policy.

The following is a general procedure to replace and install a power supply unit:

1. Turn off the computer and remove the power cord from the wall socket as well as from the rear panel of the computer.
2. Open the computer case and put it aside. If the computer was on for long hours, let it cool down for about 15 minutes.
3. Remove the power supply connectors from the motherboard and disk drives.
4. Remove the front panel and disconnect the two mains cables from the power switch.
5. Remove the screws that hold the power supply from the rear panel of the computer.
6. Determine whether you will need to remove additional components to safely remove the power supply unit from the case.
7. Remove the power supply unit gently so that it does not hit any internal parts of the computer.
8. Place the new power supply in the computer case and tighten the screws on the rear panel.
9. Connect all connectors back one by one. Do not use force.
10. Replace the front panel of the computer after connecting the power switch.

11. Reconnect the power cable. Turn on the computer to test that the new power supply unit is functioning as expected.
12. When the testing is done, replace the computer case.

Processors/CPUs

Installing a CPU requires that you always wear the antistatic wrist strap. Do not remove the new CPU from its protective cover until you are ready to insert it in the CPU socket on the motherboard. The following steps explain the general procedure for installing or replacing a CPU:

1. Open the computer case and examine the existing CPU and type of socket. Check the type of CPU socket and whether you will need any special tools to remove the CPU from the socket.
2. Some CPUs come preinstalled with a heat sink and a cooling fan. On some other CPUs, you must use the old heat sink and fan. Examine how these can be removed safely and reinstalled on the new CPU.
3. Most CPU sockets have a lever on one side that frees the CPU from the socket.
4. Pull the CPU socket lever (also called the *Zero Insertion Force* lever) gently to loosen the CPU from the socket. Remove the CPU carefully and put it aside in a protective cover.
5. Examine the small pinholes on the socket. You will notice that the CPU cannot be inserted with the wrong orientation.
6. Take out the new CPU from its cover. Examine it and hold it only from its edges in the correct direction. Place the CPU in the socket with the correct orientation.
7. Push the socket lever down gently to secure the CPU in the socket.
8. If you need to install the heat sink and the cooling fan, you will need a thermal conductive compound or tape that sits between the CPU and the heat sink. This compound or tape ensures the flow of heat from the CPU surface to the heat sink. Place a drop or two of the compound on the CPU surface or place the thermal tape on the bottom of the heat sink, as required. Follow the instructions that come with the CPU package.
9. Place the heat sink and the fan assembly on top of the CPU and secure it in its place by locking the steel clips or other mechanism as required.
10. Connect the cooling fan wires to the appropriate connector on the motherboard.

You can test the installation by simply turning on the computer. The initial BIOS test displays the speed of the processor. This test will indicate whether there is any problem with the installation. When you are done, reinstall the cover of the computer case.

You can test a new power supply even before you install it in the computer case. If you know different voltages on connector pins, turn on the power supply, take a multimeter, and measure all DC voltages on all connector pins one by one. You can also use a power supply tester for this purpose. You will need to short circuit the main cables that are connected to the power switch by using a simple wire. Be careful and do this before you plug in the main cable to the wall socket.

Memory (RAM)

There are a few important things that you must make sure of before purchasing a new memory module. These are as follows:

- There is a provision for expanding memory on the motherboard. This means that free slots (also called *memory banks*) are available. If not, you might have to replace the old memory modules with new ones (as opposed to simply adding more RAM).
- If you are adding memory modules in free slots, make sure that the new modules are compatible with the existing ones. Incompatible modules will either not work at all or will create intermittent system problems.
- If you need to buy new memory modules, check the motherboard manual to see what type of memory it supports and the maximum amount of installable memory.

Consult the motherboard manual to verify that the system bus will support the memory module you are buying or installing.

Make sure that you are wearing a properly grounded antistatic wrist strap all the time. Static charge from your body can immediately damage the memory module. Hold the module only from its edges.

The following is a general procedure for adding or removing memory modules:

1. Keep the memory sticks in their protective antistatic covers until you are ready to install them.
2. Always wear grounded antistatic wrist straps.
3. Remove the old memory sticks carefully by releasing the side levers.
4. Hold the new memory stick in the correct orientation, align it to the socket, and push it down firmly using your two thumbs.
5. Push the levers back into place.

You can test the new memory module or expanded memory capacity by turning on the computer. The BIOS test on system startup will indicate the amount of memory you have on the system. If the total amount of memory does not match the expected capacity, there may be some problem with the memory module or with your installation.

Display devices

Adding or removing a display device or a monitor is a simple process. You must select an appropriate monitor to suit your requirements. Verify that the new monitor supports the number of colors and the resolution you need. For graphics applications, you might require a monitor with 1280 × 1024 pixels or better resolution with high 32-bit color depth. Moreover, you might have to look for an LCD monitor if space is limited.

To replace an old monitor, power off the monitor and remove the power cord from the wall socket. Remove the cord that connects the monitor to the computer. Place the new monitor and make the necessary connections. If no driver needs to be installed, the monitor is ready to use when you turn on power.

Monitors are usually automatically detected, and the operating system will install the necessary drivers for them. For most applications, you can configure the monitor colors and screen resolution from the Display properties window. Right-click an empty area on the desktop and click Properties. Click the Settings tab to configure the color depth and screen resolution. For some graphics applications such as Photoshop, you may need to configure the monitor properties appropriately to set the display. This is known as adjusting the monitor gamma.

Input devices

The procedure for adding or removing an input device depends on the type of device you are installing. Simple input devices such as the keyboard and mouse are easy to remove and install. On some older computers, the mouse is installed on the serial port and a driver is installed for the operating system to recognize it. Most newer computers use the PS/2 ports or the USB ports for both devices, and the Plug and Play (PnP) feature automatically detects them and the operating system automatically installs appropriate drivers.

Adapter cards

The installation of an adapter card depends on the card's type and purpose. Most of the cards are installed on one of the available expansion slots on the motherboard. When you are replacing an old adapter or buying a new one for the computer, verify the following things:

- Check the type of expansion slots available in the computer. In new computers, all expansion slots are the PCI type, while some old computers have ISA or EISA slots. Some computers have a mix of ISA and PCI slots. If you are working on an old computer, make sure that the system bus will support the type of adapter you are going to buy or install in the computer.
- Check that the adapter driver is supported by the operating system. Go for an adapter that has been tested by Windows Hardware Quality Labs (WHQL). WHQL tests and verifies the functionality of the adapters and other devices. Insist on signed device drivers.
- Check with the vendor whether an upgraded device driver is available. The driver might have been upgraded after the adapter was manufactured and shipped to the retailer.

- Check whether the new adapter is PnP-compatible. PnP adapters are automatically detected by computer BIOS and the operating system.

Always check with the vendor or manufacturer of adapter cards if any updated drivers are available. If a supplier does not know, you can check the web site of the manufacturer for the latest versions of the device driver.

The following is a general procedure for replacing or installing an adapter card:

1. Remove the computer case by removing the screws.
2. Find an empty expansion slot. Use a slot that is easily accessible so that you can insert the card without disturbing other installed adapters.
3. Remove the slot cover from the computer case using long nose pliers.
4. Insert the adapter in the selected expansion slot and push it gently so that it sits well in the slot. Tighten the screw, if required.
5. Turn on the computer to see whether the BIOS and operating system recognize the adapter. If the adapter is not PnP-compatible or the system BIOS does not support PnP, you might have to test the adapter by installing its device driver.

When the testing is done and the adapter works as expected, you may close the computer cover.

Troubleshooting Tools and Techniques

Troubleshooting personal computers requires special skills that you learn by experience. The more experience you have, the more quickly you will be able to identify the cause of the problem and apply a correct solution. This section deals with some very general and basic troubleshooting tools and techniques that will help you build a basic understanding of the computer troubleshooting process.

Basic diagnostic procedures

Basic troubleshooting procedures include gathering information about the problem from the user, looking at problem symptoms, and determining the most probable cause. Then you can isolate the problem and determine an appropriate solution to rectify the problem.

Visual inspection. Visual inspection of problem symptoms is very helpful in starting the troubleshooting process. For example, if some user has reported a network connectivity problem, you can verify that the network cable is securely connected to the computer, that the connector is attached properly, and that the LED indicators are showing normal operation.

Similarly, if the problem is with an internal component of a computer, you can open the computer case and make a visual inspection to make sure that the adapters and memory modules are seated well in their respective slots. In case a drive is not functioning, check whether the power cable or the data cable is disconnected or loosely connected.

Audible inspection. Audible inspection refers to beep codes generated by the computer BIOS when the computer is powered on. The *Power-On Self-Test (POST)* is run on system startup to determine that the system is functioning properly. It detects various components installed in the system. Since this test is run during system startup and the BIOS does not yet have access to the video card or the monitor, it produces audible signals or beeps to report any error messages. The pattern of beeps usually indicates the type of problem.

To exactly understand the meaning of a beep pattern, you might need to refer to the motherboard manual or the documentation of the BIOS manufacturer. American Megatrends Incorporated (AMI), Award, and Phoenix are the three main vendors of computer BIOS programs.

You will need to know the correct BIOS make and its version number to determine the meaning of beep patterns. A missing beep usually indicates a problem with the motherboard. Beep codes can be a long beep, a short beep or a combination of long and short beeps to make a specific pattern, indicating a problem with a certain part of the motherboard. If the beep pattern indicates normal system startup and there is no display, make sure that the monitor is properly connected. You can also replace the monitor to verify that the problem is not with the monitor.

Minimum configuration. Removing add-on components from the computer and starting it with a minimal configuration can help trace several problems. For example, you can remove the network adapter, the modem card, or an extended graphics card one by one and restart the computer to see whether the computer starts working again.

On the software side, Windows XP and Windows 2000 Professional include advanced boot options to help determine problems with system components. You can use Safe Mode to start the system with minimum configuration. If this works well, you can use Safe Mode with Networking to add the networking components. Safe Mode allows you to disable additional hardware components and their associated drivers one by one to help find out the exact cause of the problem.

Troubleshooting steps

Troubleshooting system components involves a basic procedure that can be applied to any computer. This includes verification of the physical installation of the components, that the correct device drivers are installed, and that they are correctly configured to use system resources. These steps are discussed briefly in this section.

Verifying proper installation. When you replace a component, you must verify that it is properly installed. You must follow the installation procedure and instructions provided by the manufacturer. Make sure that components such as adapter cards and memory modules are seated properly in their respective slots. Verifying the compatibility of adapters and input and output devices, and their proper configuration is very important to make sure that they will perform as expected with minimum troubles. Whenever you install or replace a computer component, test it thoroughly before handing it over to the end user.

Verifying device drivers. Device drivers function as an interface between the device and the operating system. Make sure that you have installed a driver that is compatible with the operating system you are using. Incompatible device drivers can be easily uninstalled or updated using the Device Manager snap-in. Make sure that you are using the most current version of the device driver.

Verifying resource usage. Every component in a computer requires certain system resources to interact with the CPU. These include the IRQ, DMA, and I/O addresses. In old computers, the resource settings were configured using jumpers on adapters. New computers have PnP-compatible system BIOS and operating systems, and most devices support PnP functionality. The PnP feature allows systems to detect system components and assign resources to them automatically.

If you suspect that a problem is caused by the incorrect allocation of system resources, you can use the Device Manager snap-in on Windows XP and Windows 2000 computers to see whether there are resource conflicts. You can view Resources by Connection or Resources by Type from the View menu to detect resource allocation conflicts. If you suspect that a particular device is causing trouble, you can open its Properties window and click the Resources tab to find out whether there are any conflicts. Windows Device Manager is discussed later in this chapter.

Verifying configuration settings. You should verify that the replaced or newly installed components or input/output devices are configured according to the instructions provided by the manufacturer. Improper configuration not only causes problems with the installed component but can also pose problems for other devices. For example, if you have manually configured incorrect resource settings for an add-on card, and some other device uses these settings, both of the components might stop responding. Incorrect configuration sometimes results in a system crash.

Troubleshooting tools

As a computer technician, you are expected to have a good quality toolkit for installing, removing, upgrading, or troubleshooting computers and associated peripherals. You can either go for a ready-made PC toolkit or buy different tools separately to make your own. Even when you buy a ready-made toolkit, you may still have to add a few tools that are specifically used for computers. The following is a brief description of some essential tools that will be very helpful in troubleshooting:

Multimeter. A multimeter is one of the most essential instruments used by computer technicians and electricians. It can measure voltage and current as well as test connectivity between various points inside the computer. Two types of multimeters are available on the market: analog and digital. Analog multimeters are cheap but are sometimes difficult to read. Digital Multimeters are a little more expensive but provide an accurate reading on an LCD screen. Multimeters are useful for checking short-circuits and measuring input and output voltage of power supplies.

Screwdrivers. A good set of screwdrivers with different types of bits is an essential part of your troubleshooting and repair kit. Most technicians prefer to have screwdrivers with long shafts that help reach the interior parts of the computer. At minimum, you must have two different screwdrivers: one with a flat bit and another with a Philips bit. Screwdrivers with magnetic bits are commonly used because they prevent screws from falling down into the computer case. It is not a bad idea to keep additional screwdrivers or at least a screwdriver with interchangeable bits.

Antistatic straps and pads. Computers and other peripherals contain semiconductor chips that are very sensitive to static electricity. Static electricity can permanently damage semiconductors chips and adapter cards if not handled with caution. Antistatic wrist straps and antistatic pads (also known as *antistatic table mats*) should be used whenever you are working on computer parts. These products are very helpful in preventing damage to expensive computer parts due to a sudden discharge of static electricity from your body.

Loopback plugs. Loopback plugs are also known as *loopback adapters*. These small plugs are used with appropriate software to test the functionality of different ports on the computer, such as parallel, serial, and network ports. The accompanying software sends and receives electrical signals through the loopback plug to verify that the port is working properly. Loopback plugs and the associated test software differ from one manufacturer to another. They are very useful when you cannot test a particular port in an actual working environment. For example, if you do not have a printer, you can still test the functionality of the LPT1 port using a loopback plug.

Cleaning products. Cleaning products fall into different categories that include cleaning solutions or chemicals, vacuum cleaners, and cleaning cloths. In some cases, you will need to take out an adapter card and clean its connection pins. Here is a brief introduction to cleaning accessories:

- Soft, lint-free cloth or cleaning pads can be used for cleaning the monitor and other external parts of the computer.
- A can of compressed air can be useful for cleaning without having to use any cleaning chemicals.
- A handheld vacuum cleaner can replace the compressed air can when you cannot or are not allowed to blow out dust.

Additional specialty tools. There are some special tools that are helpful in certain odd situations or with some special requirements. These include the following:

Small flashlight
Helpful to inspect the dark areas inside a computer or a printer.

Wire stripper
Useful for cutting wires and stripping their ends.

Soldering iron
Required to attach two wires or to attach a wire to a printed circuit board.

Chip extractors
Used to safely remove semiconductor chips from their sockets.

Small tweezer
Useful for holding small parts or screws that fall inside the computer case.

Long nose pliers
Helpful in holding small parts where your hands cannot reach.

Roll of electrical insulation tape
Used to cover unused wire ends.

Extra screws of different shapes and sizes
Just in case you lose some screws during the repair/upgrade process.

Extra antistatic bags in different sizes
Useful for storing and carrying spare parts such as adapters and memory modules.

> It is always good to carry essential tools and even some extra tools when going out on a service call. Remember that the customer may not be able to provide you with any tools or accessories when you are badly in need. Asking the customer for a screwdriver or some other small tweezers leaves a bad impression about you and your company.

Preventive Maintenance (PM)

Preventive maintenance helps reduce the chances of computer breakdowns, and it improves overall system performance. It is essential to perform preventive maintenance at regular intervals. As a computer technician, you are expected to be aware of different forms of PM and how these measures can be implemented. In this section, we will briefly study some essential preventive maintenance tasks for specific computer components.

Display devices

Display devices refer to computer monitors, which are an external part of the computer. Monitors produce heat when working and are also exposed to dust around the area where the computer is installed. If not cleaned regularly, dust accumulates on the screen and the case, and it also makes its way inside the monitor through the ventilation slots provided for keeping the monitor cool. Accumulated dust can also block some ventilation slots.

Monitors should be regularly cleaned using a lint-free cloth. You can also use a cleaning solution on the monitor cover but you must be careful not to let it spill over. Make sure that all ventilation slots are clear so that air can pass through them. When monitors are not to be used for longer periods, they should be kept covered.

Power supply

A majority of computer problems are a result of the failure of the power supply. Care must be taken to ensure that the computer gets a clean and consistent power supply. Some of the preventive maintenance methods for power supply are as follows:

UPS System
: Use Uninterruptible Power Supply (UPS) to supply a clean and consistent voltage to the computer. UPS systems protect the computer from power spikes, surges, and sags that can cause significant damage to computer parts. In case of a power failure, the UPS can be very useful as it gives the user time to save his open documents or programs.

Power strips
: Power strips are useful for not only providing extra power slots but are also helpful in protecting the computer from sudden changes in voltage levels such as power spikes and sags. Some power strips come with a built-in fuse that blows off if there is a sudden voltage change.

Surge protector
: A power surge refers to a sudden change of voltage in the power line. A surge protector is used to supply a constant voltage to computers and prevent damage due to power surges.

Ventilation slots and cleaning
: Regular cleaning of the power supply unit of the computer, especially the cooling fan and ventilation slots, helps lower heat during normal operation. You can use a handheld vacuum cleaner to clean the dust accumulated around the ventilation slots. Make sure that the computer is switched off and that the main cord is disconnected from the power source or wall socket.

Additional preventive maintenance measures for power supply include the following:

- Always use 3-pin power cables with computers and peripherals to provide the ground connection.
- Provide a separate dedicated circuit when there are a large number of computers and peripherals.
- Turn off computers and then cut off the main switch during storms and thunderstorms.
- Turn off the main switch when there is a blackout. When the power returns, there might be a sudden voltage spike causing damage to computers.

Input devices

All input devices, including keyboard, mouse, and scanners, should be kept covered when not in use. Keyboards collect dust from the surrounding areas, and as a result, the keys start having intermittent jamming problems. Dust accumulated on the sides of the keys can be blown out using compressed air. Care should be taken if you use a vacuum cleaner. A powerful vacuum cleaner can knock off key tops from the surface of the keyboard. You can also use a soft brush to get rid of the dust accumulated around and between key tops.

Storage devices

There are a number of preventive maintenance methods for storage devices, each suitable for a particular type. The life and performance of storage devices can be enhanced by using some standard procedures. Even if the computer is located in clean surroundings, cleaning internal parts of the computer regularly does help extend the life of its components. Some of the preventive maintenance procedures for storage devices are as follows:

- Hard disks should be defragmented regularly and should be cleaned of unnecessary temporary files. You can use built-in operating system utilities such as Disk Defragmenter (*defrag.exe*) and Disk Cleanup. Additionally, you can check for and fix bad sectors in disks using the Check Disk (*chkdsk.exe*) utility.
- CD and DVD drives rely on laser beams and an optical lens to read and write data. Dust accumulates on the lens surface that causes intermittent disk read/write problems. You should regularly clean CD and DVD drives using appropriate lens cleaners.
- Tape drives should be cleaned using tape drive head cleaners.
- Floppy disk drives should be cleaned using a floppy disk drive head cleaner.

Motherboards, adapters, and memory

Motherboards, add-on cards (adapters), and memory modules are all thermally sensitive devices. Ensuring that the computer is operated in an area where temperature, humidity, and dust are controlled helps enhance their performance, extend their life, and reduce breakdowns. The CPU and other semiconductor chips on these cards produce heat during normal operation. While a CPU has a dedicated heat sink and an exhaust fan to keep it cool, its heat ultimately has to be blown out of the computer case. If this is not done, the temperature builds up inside the computer and can cause damage to these components.

Make sure that all the cooling fans are working properly, that dust is not accumulated around them, and that the ventilation slots of the computer case are not blocked. Regularly blowing out dust from the top of motherboards, from CPU fans, from memory modules, and from adapter cards will ensure that problems are minimized. Cooling fans usually get jammed due to the accumulation of dust around the blades and walls.

External ventilation factors

No matter how many ventilation slots and cooling fans exist within a computer, it is essential that the external cooling factors should also be taken care of. If the computer is located in an area where temperature is not controlled and no proper ventilation exists, it will eventually heat up after prolonged hours of operation. You must make sure that the computer is operated in a room where adequate air-conditioning and ventilation is available. Care must also be taken that the computer is placed at some distance from walls so that the power supply fan can blow out the internal heat. Placing the computer very close to the wall blocks airflow from the power supply.

Humidity also needs to be mentioned in this section. Computers should be located in areas with moderate humidity. Very dry areas or areas with too much moisture affect the life and performance of computers. If the air around computers is too dry, it will cause static electricity to build up, which may damage expensive computer parts.

Laptops and Portable Devices

This section is not covered in Exam 220-603.

Laptops are portable computers that use less power and make less noise than ordinary desktops. They are a little more expensive than desktops but have become very popular due to sharply falling prices. They have limited processing and graphics capabilities compared to desktops. They can work on AC power as well as DC power supplied through a built-in battery pack that runs for a few hours depending on what applications are running, what devices are connected, and how the laptop is configured to conserve power. Laptop components produce very small amounts of heat. This section discusses some fundamentals of laptops as well as installation and troubleshooting methods for components such as power devices, external monitors, and keypads.

Fundamental Principles

In this section, we will focus our attention on communication technologies for wireless communications, power devices for laptops, and components of the LCD.

Communication technologies for laptops

Laptops can be connected to a corporate network or to the Internet using wired or a wireless solution. In this section, we will take a brief look at how laptops can use different network communication methods.

Bluetooth. Bluetooth wireless networking technology provides short-range communications between two or more laptop and desktop computers. It is designed to overcome the limitations of IrDA technology. It supports transmission speeds from 1 Mbps (Bluetooth 1.0) to 3 Mbps (Bluetooth 2.0) and works over the unlicensed frequency range of 2.4 GHz. The devices must be within a short range of less than 10 meters, and 2 or more Bluetooth computers form an ad-hoc wireless network that offers high resistance to electromagnetic interferences. Bluetooth devices consume very little power.

Infrared. Infrared technology uses electromagnetic radiations that employ wavelengths that are longer than visible light but shorter than radio frequency. Common examples of Infrared devices are the remote controls used in TVs and audio systems. It supports point-to-point wireless communications between two devices using a direct line of sight. It also supports data transfer speeds ranging from 10 to 16 Mbps. Infrared devices consume very little power.

Cellular wide area network (WAN). A cellular WAN is made up of a large number of radio cells. A separate transmitter located at a fixed site powers each radio cell.

This site is known as the base station. The coverage area of a particular cellular network depends on the number of base stations. The most common example is the mobile phone network. To increase the capacity of a cellular network, the same radio frequency is used in different areas for completely different transmissions. When the same frequency is used in different cells, there must be a gap of at least one cell among them to prevent interferences. Cellular networks offer increased coverage, reduced usage of power, and increased capacity.

When the laptop is out of the range of a wireless network (or a Wi-Fi network), it is still possible to connect remotely to a network or to the Internet using the cellular networking technology. This is particularly useful when you need Internet connectivity and are not able to find a hotspot. In older laptops, add-on PC card modems (also called PCMCIA cellular capable modems) can be installed to take advantage of cellular networking, while many newer laptops now come equipped with integrated cellular modules. With add-on cards, the modem has to be connected to the mobile phone, which dials the number of the Internet Service Provider (ISP) to get Internet connectivity.

Ethernet. Most laptops come with built-in Ethernet adapters. This adapter is usually integrated onto the main board of the laptop. Earlier laptops did not have these and external cards had to be installed to connect a laptop to the network. Most modern laptops now come with a standard 10/100 Mbps network adapter.

Power supplies

A laptop derives its power from a battery pack, unlike the desktop that essentially runs on AC power. Both laptops and desktops use a small battery to run and maintain the real-time clock. The life of a charged battery depends on how the laptop is used and how the power options are configured to conserve power. The power management software on operating systems allows you to configure power options that, in the long run, also extend the life of the battery. Laptop-specific battery packs fall into the following categories:

Lithium Ion (LiIon)

These batteries are used on most modern laptop computers and other portable devices due to their light weight and longer life. Their thin size makes them suitable for laptop computers. They can be charged whenever needed, and frequent charging or overcharging does not overheat the battery. A typical LiIon laptop battery lasts for about three to four hours when fully charged. Some manufacturers claim that their LiIon batteries can last for even five hours. These batteries do not suffer from the memory effect present in NiCad batteries (described later in this list). The overall life of a LiIon battery depends on aging instead of its charge/discharge cycles.

Nickel-Metal Hydride (NiMH)

These batteries fall somewhere in between LiIon and NiCad batteries. They use Nickel (Ni) and a hydride-absorbing alloy instead of Cadmium. They last longer and have less memory effect than NiCd batteries. Overall, these batteries have a shorter life than other battery types. A typical NiMH laptop battery lasts for about two hours when fully charged.

Nickel Cadmium (NiCd)

These batteries are the oldest type of batteries used in laptop computers. Nickel (Ni) and Cadmium (Cd) are the active chemicals. These suffer from *memory effect*, which reduces the overall battery life. To get around the memory effect, the battery must be fully discharged before charging it again. Another disadvantage of a NiCd battery is that it can produce *dendrites* when left unused for a long time. Dendrites are very thin conductive crystals that cause short circuits. A major disadvantage of Cadmium is that it poses a serious environmental hazard.

Improving battery performance. The actual runtime of laptop batteries largely depends on the power requirements of various internal and external laptop components. Using power-demanding software applications such as graphics programs and video games, drains the battery sooner than expected. The use of hard drives, monitors, and USB devices also depends on battery power. In order to ensure maximum power, you can configure the power management features of the laptop. The *milliAmp-Hour (mAH)* rating noted on top of the battery pack indicates the capacity of the battery. The higher the mAH rating, the longer its runtime.

The following are some useful tips on optimizing battery performance:

- A charged battery will eventually lose its power if left unused. Recharge batteries on unused laptops after removing them from storage. If a laptop will not be used for over a month or so, it is recommended that the battery pack be removed and stored separately in a cool and dry place.
- It is necessary to fully discharge and then charge a battery every two to three weeks. This process is known as *battery conditioning*. This helps prevent memory effect in batteries (except in the LiIon battery, which, as already noted, does not have this problem).
- Lower the brightness of the LCD and turn it off when not in use.
- Adding more physical memory (RAM) helps reduce the use of the hard disk for temporary storage. The more you use the hard disk, the more battery power is drained.
- Avoid playing games or watching videos on laptops. Close running software applications when the laptop is not in use.
- Remove unneeded external peripherals that draw power from the laptop.
- Use the Power Options utility in Windows operating systems to configure standby and hibernate modes to optimize battery runtime.
- Use the power management features in laptop BIOS.

Components of LCD

LCD refers to *liquid crystal display*. LCD displays are used for laptop computers. There are three main types of LCD screens used in laptops: Transmissive, Transflective, and Reflective. A majority of laptops use the transmissive, color active matrix LCD displays. These displays offer the best quality and can render the best color depth. An Active Matrix LCD display, also known as a *Thin Film Transistor*

(TFT) display, has a grid of ultra-small wires containing small switching transistors that collectively form a matrix. Thousands of these transistors are placed close to each other. When a current is passed through them, they light up in different colors depending on the amount of current. These displays are illuminated by fluorescent backlight.

The four main components of a laptop LCD assembly are: screen, backlight, inverter, and the video controller card. A brief discussion on each of these components is provided here:

Screen
: An LCD screen is made up of two polarized materials with liquid crystal solution between them. The solution is so sensitive to electricity that when a small amount of current is passed through it, the crystals group together and do not allow light to pass through them. Each liquid crystal acts like a gate, either allowing light to pass through it or stopping it. This creates pixels or dots on the screen. The video controller card guides the electrical signals through the liquid crystal.

Backlight
: The LCD backlight is a *Cold Cathode Fluorescent Tube (CCFT)* or *Cold Cathode Fluorescent Light (CCFL)*. These tubes are placed behind the LCD. A white diffusion panel scatters the light evenly to ensure uniform display. An inverter powers the backlight tubes.

Inverter
: The sole purpose of the inverter in a laptop LCD assembly is to provide power to the backlight. It converts power to high-frequency voltage and supplies it to the CCFL. The inverter unit is held at the back of the LCD. If the screen works but seems to be very dim, there is probably something wrong with the inverter. Backlight failures are very common in laptops, often due to the failure of the inverter.

Video card
: The video card, or video controller card, is the component that controls the display of the bright dots and their color in LCD screens.

Installing, Optimizing, and Upgrading

As a computer technician, you must have a good understanding of laptop components and are expected to know how to install, optimize, and upgrade them, including both hot-swappable and non-hot-swappable parts. You should also understand how memory upgrades affect the video sharing.

Installing and removing devices

Laptop devices can be internal or external. *Internal devices* include battery, memory modules, modems, hard disks, and CD/DVD drives. *External devices* include an external battery pack, a battery adapter (charger), and several other components that can be connected to USB ports such as an external CD/DVD drive, hard disks, and PCMCIA cards.

The installation or upgrade procedure for a specific device depends on the specific make and model of the laptop. Some laptop models are very user-friendly when it comes to adding or removing devices, while others must be handled by skilled technicians. There are essentially two categories of devices, as follows:

Hot-swappable devices

Most hot-swappable devices are PnP-compatible and can be plugged into available ports while the laptop is powered on. You can also remove these devices safely without turning off the power. The laptop BIOS and the operating system must support PnP functionality. A small USB thumb drive is an example of a hot-swappable device that can be connected to a laptop as well as a desktop. The laptop recognizes and configures hot-swappable devices as soon as they are connected.

Non-hot-swappable devices

Non-hot-swappable devices usually do not support PnP functionality. To install or remove such a device, you must first turn off the power, install, and remove the device, and then turn on the power again. After the installation, you must install the necessary device driver and configure it for optimum performance. When removing these devices, you might need to uninstall the device driver and then physically remove the device.

Upgrading memory

The first thing to make sure of before upgrading a laptop's memory is to find out whether the laptop supports memory upgrades. Some laptops already have the maximum amount of memory they can support and cannot be further upgraded. Others do have provisions to upgrade the memory. Before you purchase a memory module (aka the memory stick) for a laptop, you must refer to the documentation or call the vendor's support line to get instructions on the upgrade process. You must also make sure that the memory module you are buying is compatible with a particular make and model. Detailed information about upgrades and specific issues can be found on most vendors' web sites. Some laptop vendors include the documentation as PDF files on the laptop itself. These manuals usually describe the amount of memory currently installed and the maximum amount of memory supported.

It is always good to wear an antistatic wrist strap when opening any of the lids of the laptop to protect it from potential static discharge. Also, keep the memory module in its protective cover until you are ready to insert it in its appropriate slot in the laptop. When upgrading memory or any part of the laptop, you must first remove the AC adapter and remove the battery pack. When the battery pack is removed, you should follow the manufacturer's instructions to remove the old memory module and add the new one. When this is done, you may reinstall the battery pack. Power on the laptop and verify that the new memory is recognized by the BIOS and the operating system. On Windows OS, you can verify the upgraded memory by opening the System Properties window from the Control Panel.

Memory upgrades greatly affect how shared videos are downloaded and played on the laptop. The same principle is true for desktops also. Most videos that run in real-time depend on physical memory (RAM) to temporarily store the downloaded data in the memory buffer. Since videos consist of large files, having a large amount of RAM in a laptop ensures that the video is downloaded and starts playing immediately. There will also not be interruptions due to a shortage of memory.

Troubleshooting Tools and Procedures

Problems with laptops and other devices can be resolved with normal troubleshooting techniques. The following troubleshooting procedure applies to laptop computers as well as desktop computers:

- Gather information from the user or from the problem symptoms.
- Identify the cause of the problem by analyzing the collected information.
- Isolate the problem.
- Find an appropriate solution to fix the problem.
- Test the results of the solution.
- Apply the solution and complete documentation.

There may be several reasons for a laptop problem. The battery, an internal component, or an external peripheral such as the data entry keypad, may have caused the problem. A loose network connection or a distant access point will generally cause connectivity problems, whereas problems with power supply components will cause the laptop or a mobile device to shut down unexpectedly. In this section, we will look at some common problems and appropriate solutions to fix them.

Power problems

Most laptops suffer from power problems that may be due to the main AC power adapter or due to the built-in battery. When trying to fix power-related problems, make sure that the main AC supply is properly connected. The following simple steps will help you verify the AC input power.

- Verify that the main power cord is properly attached to the adapter. If it has become loose or does not attach properly, try replacing it.
- Check the small LED on top of the adapter. If it is not glowing, the AC power may not be connected or may be turned off.
- Touch the AC adapter surface. A reasonably warm surface is usually an indication of a working adapter. If the power adapter seems to be overheated, it may have to be replaced.
- Verify that the DC power cord is not damaged and the connector is properly inserted into the laptop.
- Remove the DC power cord and verify the DC power output of the adapter.
- If there is no output or a very low DC output and the AC is properly connected and the LED is lit, try replacing the adapter with a new one.

Removing unneeded devices

Many problems with laptops can be resolved simply by removing unneeded external peripherals. For example, if you do not need an external USB modem or a hard drive permanently connected to the laptop, you should remove it. Depending on the type of the connected device, you might have to uninstall the driver of the device, power off the laptop, remove the device physically, and then power on the laptop again. It is easier to remove external devices than to remove the internal devices. You should refer to the product documentation for the correct procedure to remove any device that you think is not needed. If in doubt, you should not hesitate to call the manufacturer's customer support.

> In some situations, you might think that a device connected to a laptop is not needed, but that might not be the case. It is a good idea to ask the user what that device is used for or to seek expert advice from the manufacturer before removing any component or device.

External monitor

The LCD screen of a laptop is one of the major components that drain battery power. Most laptops have a connector that facilitates the connection of an external monitor. External monitors help conserve battery power since the LCD monitor is turned off. This is a good option to extend battery life, especially for those laptops whose battery life is coming to an end.

If you have problems with the LCD display, connecting an external monitor can quickly determine whether the problem lies with the LCD display or the video controller card.

Function keys

Functions keys in laptops are different from the ones present in normal desktop computers. These keys have specific functions, which vary from one model to another. Usually the functions of these keys are noted on the top of the key itself. For example, you can use the function keys to increase or decrease screen brightness, contrast, and volume. You can also toggle the display between the LCD screen and the external monitor using the appropriate function key. These keys are useful when diagnosing a problem with the LCD screen. Due to the compact design of the laptop keyboard, the function keys are usually dual purpose. You must first press the Fn key before you can use the function key.

External keypad

The external keypad for laptops helps accountants and data entry operators speed up their data entry jobs. This external 17-key keypad connects to one of the USB ports on the laptop and makes data entry easy for such users. Users often complain about the different functionality of the keys on the external keypad.

The functions of number keys on external keypads might differ from the regular number keys located on the top row of the built-in keyboard, and you might have to refer to the product documentation. If users complain about uneasiness using a combination of laptop keyboard and the external keypad, you can provide them with an external keyboard.

The LCD cut-off switch and backlight

The cut-off switch for the LCD screen is used to turn the backlight of the screen off or on when the LCD lid is closed. This helps conserve battery power and extends the life of the battery as well as the LCD screen itself. Due to frequent opening and closing of the LCD lid, this switch sometimes gets stuck when you open the lid. This may even happen when the laptop is operated in areas with lots of dust. The dust makes its way into the switch opening and keeps accumulating around the switch until it becomes inoperable or causes intermittent problems.

An indication of a problem with the cut-off switch is that the screen shows a faint image even when the LCD lid is fully open. In some situations, you would see a normal image on the screen, which becomes faint after a while. The inverter that supplies power to the backlight might cause this problem.

In case the LCD screen produces a garbled display, you can connect an external monitor to find out whether the problem is with the LCD display or the video controller card. If the external monitor works fine, the LCD screen might not be connected properly to the video controller.

Digitizer problems

Digitizers are devices that convert analog signals into digital signals and store them on the connected device. They are commonly used on Tablet PCs and *Personal Digital Assistants (PDAs)* to facilitate functions such as data input. A *graphic tablet*, on the other hand, is an electronic device that consists of a flat surface on which a user can draw or write something using a *stylus*, which looks like a pen. The device is connected to a computer, and the image appears on the computer screen. Graphic tablets should not be confused with Tablet PCs.

Most stylus problems are caused by rough handling. Some problems directly relate to the alignment of the stylus pen. A soft or hard reset sometimes helps resolve this problem, or a built-in utility can be used for the purpose. You may also use some freely available software on the Internet to get around the alignment problem.

Exhaust fans

Laptops are very compact computers and consume less power than desktops. Since all components are packed in a thin case, they produce significant heat. Exhaust fans are located on the sides of the laptop to fan out heat produced by internal components. Older laptops produce large amounts of heat that cause major component failures. These laptops can be used with external fans or *laptop coolers*, which are fans mounted on the base of the laptop—there are usually two fans. These fans are connected to one of the USB ports and draw power from the laptop itself.

Antenna wires

An antenna is used with a laptop to boost its wireless signal power. You will not see a wireless antenna in most of the new laptops, but it might be required on some older laptops that use a PCMCIA wireless adapter. Antenna wires are very helpful in troubleshooting connectivity problems when a laptop is placed far away from the wireless access point. You can also try using a signal booster with the access point if all of your laptop users are complaining of connectivity problems. Another resolution to this problem is to move the access point itself to a location near the laptop users.

Operating Systems

The A+ Essentials exam tests your knowledge of introductory concepts of operating systems. Exams 220-602, 603, and 604 test your ability to identify and use tools and utilities to manage operating systems and diagnose common problems related to the components of operating systems. In this section, we will discuss commonly used tools and utilities to manage the operating system, utilities to troubleshoot startup and recovery problems, and the maintenance of disks and filesystems. The two major desktop operating systems covered on the A+ exams are Windows 2000 Professional and Windows XP Professional. A majority of the tools and utilities covered in the following sections are available on both of these operating systems.

> There are some overlapping objectives covered in A+ Essentials and Exams 220-602, 220-603, and 220-604. I encourage you to review the fundamental concepts of operating systems covered in Chapter 2.

Fundamental Principles

This section focuses on identifying, locating, and using command-line utilities, as well as disk and system management tools. These utilities are very helpful in diagnosing and resolving common system problems.

Command-line functions and utilities

Most of the system management tasks can be accomplished using command-line utilities, which are available in both Windows 2000 Professional and Windows XP operating systems. Although most system administrators and technicians prefer to use the graphical user interfaces (GUIs) or wizards to perform everyday administrative tasks, the command-line utilities are considered more powerful than the GUIs. Windows commands can be used in batch files and scripts to automate most of the everyday administrative tasks. This section covers the most basic command-line utilities and their usage.

> The commands used in Windows operating systems are not case-sensitive. You can either use upper- or lowercase characters to run a command. We have used a mix of upper- and lowercase in this chapter for the purpose of clarity only.

cmd. Windows commands are used inside the Windows command shell. This is invoked using one of the following methods:

- Click Start → Run, type `cmd` in the Run dialog box, and press the Enter key.
- Click Start → All Programs → Accessories → Command Prompt.

A black-and-white window, by default, opens and a command prompt (C:\>) with a blinking cursor is displayed. To change the properties of this window, click the command icon on the top lefthand corner of the command prompt window and click Properties. The following four tabs are available to modify the command prompt window settings:

Options
Use to change the size of the cursor, the command history buffer, edit mode, and window size.

Fonts
Use to choose a font and its size.

Layout
Use to change the screen buffer, size, and position of the window.

Colors
Use to choose display colors inside the command prompt window.

help. The number of commands available in Windows is so large that it is not possible to remember the syntax or switches for every command. This is where the *help* command comes in handy. This command is useful if you need help with any other command. There are two ways to use the *help* command:

- In the command prompt window, type `help` and press the Enter key. A list of all available commands is displayed.
- To get help on a particular command, type `help <command>` and press the Enter key. This displays the purpose, syntax, available switches, and usage examples for the specified command. For example, if you need help for the *copy* command (discussed later), you can use the following command:

  ```
  C:\>help copy
  ```

  You can also get help on a particular command by typing `/?` after the command. For example, to get help for the *attrib* command, type the following at the command prompt and press Enter:

  ```
  C:\>attrib /?
  ```

dir. The *dir* command is used to display a list of files, directories (folders), and subdirectories (subfolders) stored on a selected disk drive. The command also displays the total number of files and folders on the drive. When used without specifying any switches, the command displays the contents of the current working directory. You can specify a particular drive and directory by using the [*drive*:][*path*] switch as follows:

```
dir D:\Myfolder
```

The syntax of this command is as follows:

```
dir [drive:][path][filename] [/A[[:]attributes]] [/B] [/C] [/D] [/L] [/N]
  [/O[[:]sortorder]] [/P] [/Q] [/S] [/T[[:]timefield]] [/W] [/X] [/4]
```

Table 5-1 lists the other switches available with this command and their functions.

Table 5-1. Switches available with the dir command

Switch	Function
`/A:Attributes`	Displays files or folders that have the specified attributes. Attributes include directory (D), read-only (R), system (S), ready for archiving (A), and hidden (H).
`/B`	Does not display headings in display format.
`/C`	Displays the thousand separators for file sizes.
`/D`	Same as the `/W` switch, but lists are sorted by columns.
`/L`	Displays the list in lowercase characters.
`/N`	Displays names using the long filename format.
`/O:Sortorder`	Displays files in specified sort order.
`/P`	Pauses the command when the command prompt screen is full.
`/Q`	Displays the owner or the file.
`/S`	Lists files in specified directory and all subdirectories.
`/T:Timefield`	Specifies timefield to use. Options are C (Creation), A (Last Access), and W (Last Written).
`/W`	Displays files using a wide list format.
`/X`	Displays file and folder names in 8.3 format.
`/4`	Displays four-digit years.

The following example shows how you can use the *dir* command to display the contents of a particular folder and all subfolders that are hidden:

```
dir D:\myfolder /A:H
```

> Windows commands can be used with wildcards to expand the search results. For example, you can use the command dir D:\My*.* to display all files and folders that start with characters “My”. Similarly, you can display a list of all files with the extension “.doc” by using the command dir D:\*.doc.

attrib. The *attrib* command is used to display or change the attributes of a file or folder. Attributes of files and folders include the following:

A The archive attribute, which is used for backing up a file or folder.

H The hidden file attribute. Hidden files are not displayed in Windows Explorer.

R The read-only file attribute.

S The system file attribute.

The syntax of the *attrib* command is as follows:

```
attrib [+R | -R] [+A | -A] [+H |-H] [+S |-S] [drive:][path][filename]
```

The plus (+) sign sets an attribute, and the minus (–) sign removes it. For example, you can set a read-only attribute of a file in the *E:\Myfiles* folder as shown in the following example:

```
attrib +R E:\Myfiles\report1.doc
```

The following example shows how you can remove the hidden file attribute:

```
attrib -H D:\Myfolder\report.doc
```

edit. The *edit* command is an older 16-bit MS-DOS command used to edit text files. This command is hardly used these days due to the availability of advanced utilities such as Notepad. The syntax of this command is as follows:

```
edit [/B] [/H] [/R] [/S] [/<nnn>] [file(s)]
```

The switches available with this command and their functions are listed in Table 5-2.

Table 5-2. Switches available with the edit command

Switch	Function
`/B`	Uses monochrome mode.
`/H`	Displays the maximum number of lines.
`/R`	Loads the file in read-only mode.
`/S`	Forces the use of short filenames in 8.3 format.
`/nnn`	Loads binary files and limits the line width to <*nnn*> characters.
`File(s)`	Specifies the file to load.

copy. The *copy* command is used to copy one or more files and folders from one location to another. The syntax of this command is as follows:

```
copy [/D][/V][/Y|/-Y][/A|/B][Z] Source Destination
```

The switches available with the *copy* command and their functions are listed in Table 5-3.

Table 5-3. Switches available with the copy command

Switch	Function
`/D`	Used when the source file is encrypted. The command copies the file to destination in decrypted format.
`/V`	Verifies the copy operation.
`/Y` or `/-Y`	`/Y` is used to suppress the warning messages. An overwrite warning message appears when another file with the same name exists on the destination. `/-Y` is used to confirm overwriting of an existing file.
`/A` or `/B`	`/A` indicates an ASCII file. `/B` indicates a binary file.
`/Z`	Copies files from a network location in resumable mode.
`Source`	Specifies the location of source files.
`Destination`	Specifies the location of destination files.

To copy a single file from one location to another, you can use the following example command:

```
copy picture1.bmp D:\Pictures
```

Using wildcards, you can copy all picture files with *.bmp* extension from one folder to another, as shown in the following example:

```
copy C:\Oldpics\*.bmp D:\Newpics
```

You can also change the name of a file using the *copy* command, as shown in the following example:

```
copy Oldfile.doc D:\Myfiles\Newfile.doc
```

> Remember that you cannot copy a file onto itself. For example, the following command will not work and will display an error:
>
> ```
> copy D:\Myfiles\Report1
> The file cannot be copied onto itself
> 0 file(s) copied.
> ```

The *copy* command can also be used to copy files to devices connected to LPT or COM ports. The following example command sends the file *File1* to the printer connected to the LPT1:

```
copy D:\File1.doc >lpt1
```

xcopy. The *xcopy* command is used to copy multiple files simultaneously from one location to another. The difference in the functionality of the *copy* and *xcopy* commands is that *xcopy* can be used to copy files as well as directories. This command is more versatile and provides more operational flexibility than *copy*. It also has built-in exit codes that can be used in batch files for error-handling during the copy process. The syntax of this command is as follows:

```
xcopy source [destination] [/A | /M] [/D[:date]] [/P] [/S [/E]] [/V] [/W]
                           [/C] [/I] [/Q] [/F] [/L] [/G] [/H] [/R] [/T] [/U]
                           [/K] [/N] [/O] [/X] [/Y] [/-Y] [/Z]
                           [/EXCLUDE:file1[+file2][+file3]...]
```

Most commonly used switches with the *xcopy* command and their functions are listed in Table 5-4.

Table 5-4. Switches available with the xcopy command

Switch	Function
/A or /M	The /A switch copies files with their archive bits set. The /M switch copies these files and changes (turns off) the archive bit.
/D:*date*	Specifies the date in MM-DD-YYYY format to copy only those files that have changed on or after the given date.
/P	Used to Prompts a confirmation message before creating files.
/S	Copies the directory and all subdirectories. Only the empty directories are not copied.

Table 5-4. Switches available with the xcopy command (continued)

Switch	Function
`/V`	Verifies the copy operation.
`/C`	Continues the copy process even when the command encounters errors.
`/Q`	Suppresses filenames while copying.
`/F`	Displays the names of files and directories during the copy process.
`/L`	Displays only the list of files to be copied without actually copying the files.
`/G`	Specifies that the files are to be stored in decrypted format on the destination.
`/H`	Copies hidden and system files.
`/R`	Forces overwriting of read-only files.
`/O`	Copies the ownership and Access Control List (ACL) of the files.
`/Exclude:`*`file1`* `[+`*`file2`*`]...`	Excludes the specified files from the copy process.

Since the command uses a large number of switches, here are some examples to show the usage of this command:

```
xcopy A: B: /s /h
```

This command will copy all files including subdirectories from drive A: to drive B:, which are usually floppy disk drives. The /S and /H switches will force copying of system and hidden files respectively.

```
xcopy C:\Mydir D:\Newfiles /S /D:10-26-2006
```

This command will copy all files and subdirectories that have changed on the 26th of October, 2006 or after, to a folder named *D:\Newfiles*.

```
xcopy C:\Mydir D:\Newfiles /Exclude:*.doc
```

This command will copy all files and subdirectories to the *D:\Newfiles* folder but will exclude the files with a *.doc* extension.

format. The *format* command is used to format a disk partition or a floppy disk using a specified filesystem. Floppy disks support only the File Allocation Table (FAT) filesystem while disk partitions (called volumes) support both FAT/FAT32 and/or NTFS. The syntax of this command is as follows:

```
format volume [/FS:file-system] [/V:label] [/Q] [/A:size] [/C] [/X]
format volume [/V:label] [/Q] [/F:size]
format volume [/V:label] [/Q] [/T:tracks /N:sectors]
format volume [/V:label] [/Q]
format volume [/Q]
```

Some of the commonly used switches available with the *format* command and their functions are listed in Table 5-5.

Table 5-5. Switches available with the format command

Switch	Function
`Volume`	Specifies the disk partition or volume drive letter.
`/FS:`*`filesystem`*	Specifies the filesystem as FAT, FAT32, or NTFS.
`/V:`*`label`*	Specifies a label for the formatted volume.
`/Q`	Used to perform a quick format.
`/A:`*`size`*	Specifies the allocation unit size.
`/C`	Specifies that all files stored on the formatted volume will be compressed. Works only with NTFS.
`/X`	Used on NTFS to dismount the mounted volumes.
`/F:`*`size`*	Used on a floppy disk to specify its size.
`/T:`*`tracks`* `/N:`*`sectors`*	Specifies the number of tracks and sectors per track.

The following example shows how you can format a disk partition using the NTFS filesystem:

```
format D: /FS:NTFS
```

You can also format a partition and assign it a volume label using the /V switch as shown in the following example:

```
format D:/FS: NTFS /V:Mydrive
```

Note that formatting a disk or a volume deletes all existing data. You must be careful while using the *format* command. Never experiment with this command on a user's desktop or a production server.

md. The *md* (or *mkdir*) command is used to create a new directory. This command has the following simple syntax:

```
md [Drive:][Path]
mkdir [Drive:][Path]
```

To create a directory named *Mydir* on drive D:, you can use the following command:

```
md D:\Mydir
```

You can also create a directory inside existing directories as shown in the following example:

```
md D:\Mydocs\Reports\Report05
```

rd. The *rd* (or *rmdir*) command is used to delete a directory. The syntax of this command is as follows:

```
rd [/S] [/Q] [drive:]path
rmdir [/S] [/Q] [drive:]path
```

This command uses only two switches: /S and /Q. The /S switch is used to delete the specified directory along with files and subdirectories. The /Q switch is used to suppress the warning message when the files or subdirectories are deleted.

cd. The *cd* (or *chdir*) command is used to change the working directory when using the command prompt. This command can be used in any of the following ways:

```
chdir [/D] [drive:][path]
chdir [..]
CD [/D] [drive:][path]
CD [..]
```

The use of double dots (..) or a backslash (\) specifies that you want to change the parent directory. The /D switch specifies that you want to change the current drive as well as the current directory.

ipconfig and ping. The *ipconfig* command is used to display and change the TCP/IP configuration on a computer, and the *ping* command is used to test connectivity between two TCP/IP hosts. For more details and information about switches available with these commands, refer to the "Troubleshooting Network Problems" section later in this chapter.

Managing disks

The tasks related to managing disks on Windows desktop operating systems include creating disk partitions, formatting disks using FAT/FAT32 or NTFS filesystems, creating and managing directory structures, managing file attributes, and assigning file permissions. First, let's look at different types of disks and partitions used on Windows 2000 and Windows XP computers.

Basic disks

These are the traditional type of disks used in computer systems. Windows XP Professional initializes all disks as Basic, unless they are converted to Dynamic using the Disk Management utility. The disks are divided into one or more *partitions*, each of which can be a logical storage unit accessible by a drive letter.

Dynamic disks

These are specifically converted from Basic disks using the Disk Management utility. Dynamic volumes can be extended on single or multiple Dynamic disks, and offer fault-tolerance features. You can create Simple, Spanned, and Striped volumes on Dynamic disks.

Primary partition

Each basic disk can have up to four primary partitions or three primary and one extended partition. One of the primary partitions is marked as the *Active Partition* and is used to boot the system. There can be only one Active partition on a computer.

Extended partition

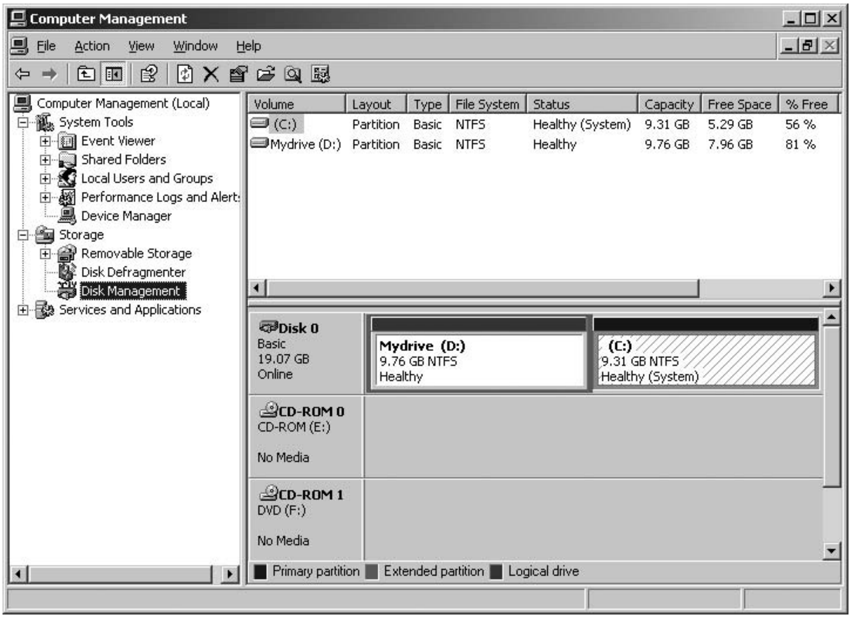
An Extended partition is used to create logical drives and assign them drive letters. Extended partitions cannot be formatted with any filesystem, and they cannot be assigned drive letters.

Logical partition

Logical partitions are created inside the Extended partitions. Logical drives cannot be marked as active and cannot be used to boot the system.

Most of the disk management tasks can be performed using the Disk Management snap-in located in the Computer Management console. You can also manage disks using the *DISKPART* command-line utility, which is more flexible and versatile than the Disk Management snap-in.

Right-click the My Computer icon on the desktop and select Manage. This opens the Computer Management console. Navigate to the Disk Management snap-in located in the Storage folder. Click Disk Management to view the details of installed disks and currently configured disk partitions (volumes) in the right-hand side details pane, as shown in Figure 5-1.



Volume	Layout	Type	File System	Status	Capacity	Free Space	% Free
(C:)	Partition	Basic	NTFS	Healthy (System)	9.31 GB	5.29 GB	56 %
Mydrive (D:)	Partition	Basic	NTFS	Healthy	9.76 GB	7.96 GB	81 %

Figure 5-1. Disk Management snap-in

Creating partitions. The Disk Management snap-in can be used to create partitions and format them using FAT/FAT32 or NTFS. To create a new partition, you must either have a new unformatted disk or unallocated space on one of the installed disks. The following steps explain how you can create a Primary or Extended partition:

1. Right-click the unallocated space where you want to create a partition.
2. Select New Partition to launch the New Partition Wizard.
3. Select Primary Partition and click Next.
4. Specify the amount of disk space in MB to use for the Primary partition on the Specify Partition Size page. Click Next. (Click Finish if you are creating an Extended partition.)
5. Choose a drive letter or path from the available drive letters. Click Next.
6. The Format Partition page appears. Click Format This Partition, select a filesystem, and assign a volume label. Click Next.
7. Click Finish on the Completion page. It takes a few minutes before the partition is created and formatted.

You may have noted from the given exercise that Extended partitions are not formatted or assigned drive letters. In fact, logical drives are created inside Extended partitions. These drives are formatted and assigned drive letters. The procedure for creating a logical drive is similar to the procedure used for creating primary or extended drives. You will need to select Logical Drive on the Select Partition Type page and follow further instructions.

Formatting a volume. Volumes on Windows XP and Windows 2000 desktops can be formatted using one of the following methods:

- In Disk Management, when the partition or volume is created.
- In Disk Management, by right-clicking an existing partition and selecting Format.
- In Windows Explorer, by right-clicking a drive letter and selecting Format.
- By using the *format.exe* command.

You can also perform a Quick Format, which saves formatting time by skipping the disk checks. While formatting partitions, you can assign a drive letter when the partition is not an Extended partition, select the filesystem (FAT/FAT32 or NTFS), and enable file and folder compression.

Using DiskPart to manage disks. *DiskPart* is a command-line utility that is used to manage disks and volumes. When you run the *diskpart.exe* command from the command prompt, the *DiskPart* interpreter starts and the prompt changes to `DISKPART>`. You can type help at the `DISKPART>` prompt to get a list of available commands to manage disks. The only facility not available with the *DiskPart* utility is the ability to format volumes. You must use the *format* command to format disks and partitions.

Creating directory structures. The easiest method to create directories and subdirectories on a Windows desktop is to use Windows Explorer. Open Windows Explorer and navigate to the desired disk drive or volume. Right-click an empty area on the righthand side, select New, and click Folder. A new folder appears named *New Folder*. You can rename this folder as required. To create subfolders inside the new folder, click the folder name on the lefthand side pane and repeat the process on the righthand side pane.

Another method to create folders and subfolders is to use the *md* or *mkdir* command from the command prompt, as explained earlier in this section. You can navigate through the folders using Windows Explorer, or using *cd* or *chdir* commands, as required.

Changing file attributes and permissions. File and folder attributes and permissions can be changed from Windows Explorer. The following steps explain the procedure:

1. Click Start → All Programs → Accessories → Windows Explorer.
2. Navigate to the file or folder that you wish to view, change the attributes of, or manage the permissions of.
3. Double-click to open the Properties window for the file or folder.
4. Click the Appropriate checkbox to set (or clear) the Read Only, System, or Hidden attributes. Click OK.
5. Click the Security tab to configure NTFS permissions, or click the Sharing tab to configure the Share permissions for a folder.
6. Click Add to select the appropriate user or a group to set permissions on the folder.
7. Repeat step 6 for each user or group to configure additional permissions.
8. When done, close the Properties dialog box.

> Note that NTFS permissions apply to both the local user as well as any user accessing the folder from the network. Share permissions do not apply to the user who is logged on locally to a computer.

Disk maintenance

Windows XP Professional includes three basic utilities to maintain disks. These are *Disk Defragmenter*, *Check Disk*, and *Windows Backup*. Each of these utilities is explained in the following sections.

Disk Defragmenter. *Fragmentation* refers to the state of a hard disk when it no longer has contiguous space available to store new files or folders. The Disk Defragmenter utility can analyze hard disks and defragment them to free up contiguous space. There are several ways to access the Disk Defragmenter, as follows:

- Click Start → All Programs → Accessories → System Tools → Disk Defragmenter.
- Open Windows Explorer, and then open the properties of a disk or volume. Select the Tools tab. Click Defragment Now to open the Disk Defragmenter.
- Right-click My Computer, and click Manage to open Computer Management. The Disk Defragmenter is located under the Storage folder.
- Click Start → Run, type `compmgmt.msc`, and select Disk Defragmenter.

There are two options available:

Analyze

When you click the Analyze button, the utility analyzes the entire disk and displays the results in the graphical form in the Analysis band.

Defragment
When you click the Defragment button, the utility starts to defragment the disk. The disk is automatically analyzed before it is defragmented.

Check Disk. The Check Disk utility checks hard disks for filesystem errors and scans and attempts to recover bad sectors on the disk. As with Disk Defragmenter, Check Disk can also be accessed in a number of ways. An equivalent command-line utility known as *chkdsk.exe* is also available for this purpose. There are two options available with the Check Disk utility:

Automatically Fix File System Errors
Allows you to scan the disk for filesystem errors and fix them automatically.

Scan For and Attempt Recovery of Bad Sectors
Allows you to scan and fix bad sectors on the hard disk. If you check this option, you do not need to check the Automatically Fix File System Errors option because all those actions are included in this utility.

The Check Disk utility can also be started from the command prompt with the *chkdsk.exe* command. A number of switches are available with this command. You can type chkdsk /? to get help on syntax and switches.

> Disk Defragmenter, Check Disk, and Disk Cleanup are the three main utilities for maintaining disks. Each is used for different purposes, and you must know which utility is the best to use for a given situation.

Windows Backup. The Windows Backup Wizard is located under the Start menu. Click Start → All Programs → Accessories → System Tools → Backup. You can also launch the Backup Wizard by running the *ntbackup.exe* command from the Run dialog box. The three main options in the Backup utility include the Backup Wizard, the Restore Wizard, and the Automated System Recovery Wizard. The Windows Backup is shown in Figure 5-2.

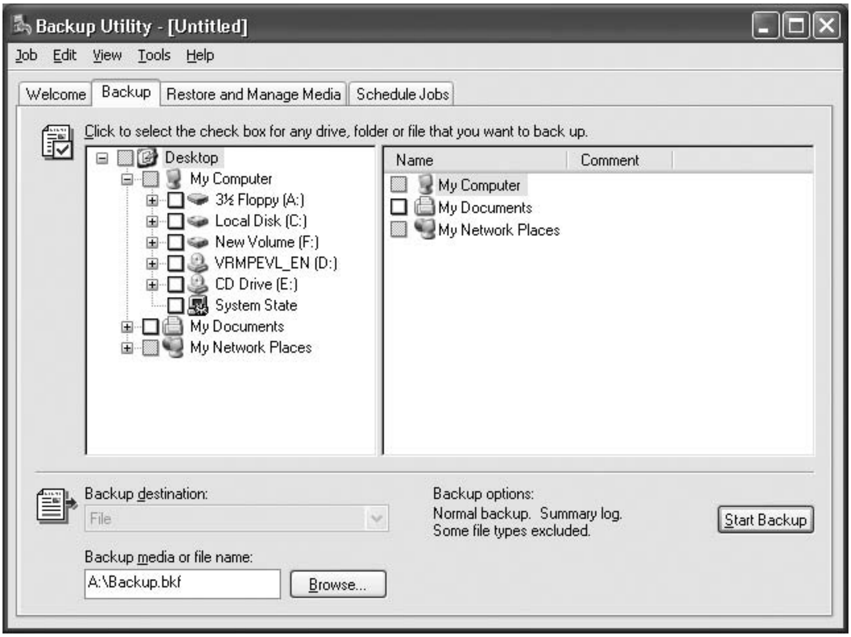
You must be a member of the Administrators group or the Backup Operators group in order to back up and restore data. The Backup Files and Directories user right also allows users to perform backups, while Restore Files and Directories allows them to perform restores.

The following types of backups are supported in Windows 2000 Professional and Windows XP Professional operating systems:

Normal or Full Backup
This option backs up all selected files and folders irrespective of when the files were last modified. This operation clears the backup Archive Bits.

Copy
This is similar to the Normal backup, but it does not clear the Archive Bits.

Incremental
This backs up all files and folders that have changed since the last Normal Backup indicated by the Archive Bits and clears the archive marker.



Backup destination: File

Backup media or file name: A:\Backup.bkf

Backup options:
Normal backup. Summary log.
Some file types excluded.

Figure 5-2. Windows Backup

Differential
This backs up all selected files and folders that have changed since the last Normal backup. This type of backup does not clear the Archive Bits.

Daily
This backs up all file folders changed during the current date. This type of backup neither uses the Archive Bits nor does it clear them.

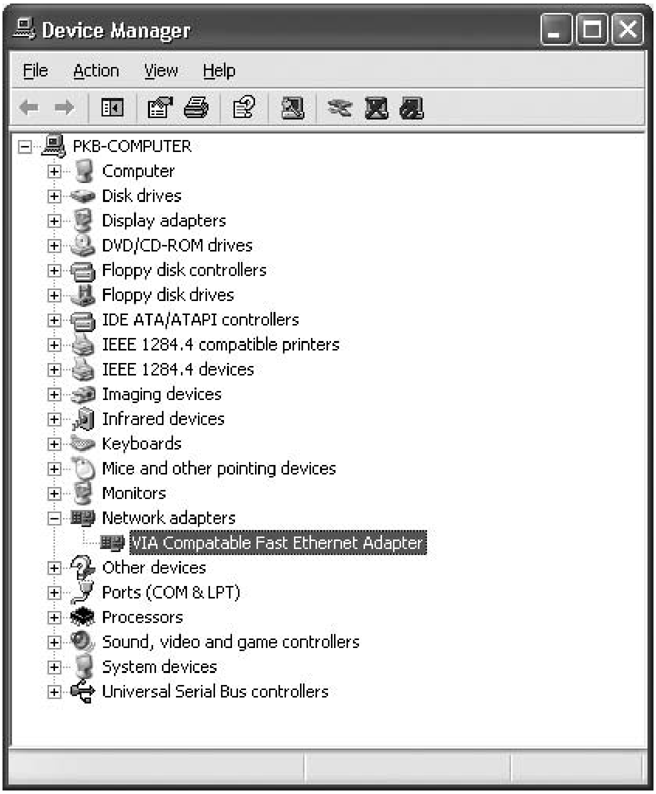
You can schedule backup jobs in order to run them in unattended modes. The Task Scheduler service must be running on the computer where you wish to perform the unattended scheduled backup jobs.

Backed-up data can be restored from the Restore tab of the Backup utility. You can specify the location of backed-up files and the destination where the files should be restored as follows:

- Original location
- Alternate location
- Single folder

Device Manager. The Device Manager utility is used to manage hardware devices and drivers in Windows XP Professional. This utility is shown in Figure 5-3 and can be accessed in one of the following ways:

- From the Computer Management console, the Device Manager is located under the System Tools Folder.
- From the Start menu, click Start → Control Panel → System. The Device Manager is located within the Hardware tab.



- PKB-COMPUTER
  - Computer
  - Disk drives
  - Display adapters
  - DVD/CD-ROM drives
  - Floppy disk controllers
  - Floppy disk drives
  - IDE ATA/ATAPI controllers
  - IEEE 1284.4 compatible printers
  - IEEE 1284.4 devices
  - Imaging devices
  - Infrared devices
  - Keyboards
  - Mice and other pointing devices
  - Monitors
  - Network adapters
    - VIA Compatable Fast Ethernet Adapter
  - Other devices
  - Ports (COM & LPT)
  - Processors
  - Sound, video and game controllers
  - System devices
  - Universal Serial Bus controllers

Figure 5-3. Device Manager

The Device Manager provides a snapshot of all installed devices in the system. Any unrecognized or malfunctioning device is flagged with a big yellow colored question mark (?). A black exclamation point (!) on a yellow field indicates that the device is in a problem state. A red X indicates a disabled device. You can list devices from the View menu in one of the following ways:

- Devices by type
- Devices by connection
- Resources by type
- Resources by connection

You can use the Device Manager to manage device drivers from the Drivers tab of the Device Properties dialog box. This tab includes the following options:

- Click the Driver Details button to view the information about driver files and the manufacturer.
- Click the Update Driver button to update a device driver with a more recent version. You can also reinstall a driver if the previous installation did not work for some reason.
- Click the Roll Back Driver button to revert to the previously working device driver if you find that the newly installed updated driver does not work.
- Click the Uninstall Driver button to uninstall a device driver when you wish to remove a device from the computer.

Task Manager. The Task Manager utility provides real-time information to monitor applications, processes, system performance, and networking from a single window. You can start programs, stop any running processes, and get an overview of system network utilization. You can access the Task Manager in one of the following ways:

- Press the Ctrl+Alt+Delete keys together.
- Right-click the Taskbar and select Task Manager.
- Press the Ctrl+Shift+Esc keys together.

The Task Manager window is shown in Figure 5-4.

The Task Manager window is divided into five different tabs: Applications, Processes, Performance, Networking, and Users. These are described next.

Applications

This window displays applications currently running on the system. You can click any of the applications. Click the End Task button to terminate the application.

Processes

This tab displays all the processes running on the system including the system processes. By default, the Processes tab displays all running processes for the current user. You must select the Show Processes From All Users box to display all active processes. Windows displays the name of the process, the name of the user running the process, CPU usage, memory usage, and the assigned session ID. You can change the Base Priority or set processor Affinity from this tab. *Base Priority* refers to the way the operating system allocates CPU time to various processes. Available base priorities include: Real-time, High, Above Normal, Normal, Below Normal, and Low. Both Windows XP Professional and Windows 2000 Professional Edition support up to two microprocessors. When two microprocessors are installed in the computer, you can assign a particular process to a particular microprocessor. This is called *Processor Affinity* and can be set to 0 or 1 for a specific process.

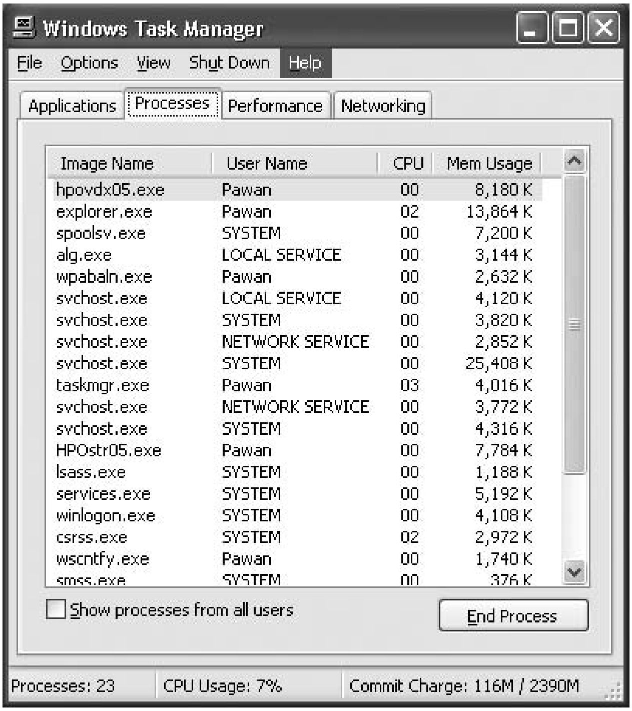


Image Name	User Name	CPU	Mem Usage
hpovdx05.exe	Pawan	00	8,180 K
explorer.exe	Pawan	02	13,864 K
spoolsv.exe	SYSTEM	00	7,200 K
alg.exe	LOCAL SERVICE	00	3,144 K
wpabaln.exe	Pawan	00	2,632 K
svchost.exe	LOCAL SERVICE	00	4,120 K
svchost.exe	SYSTEM	00	3,820 K
svchost.exe	NETWORK SERVICE	00	2,852 K
svchost.exe	SYSTEM	00	25,408 K
taskmgr.exe	Pawan	03	4,016 K
svchost.exe	NETWORK SERVICE	00	3,772 K
svchost.exe	SYSTEM	00	4,316 K
HPOstr05.exe	Pawan	00	7,784 K
lsass.exe	SYSTEM	00	1,188 K
services.exe	SYSTEM	00	5,192 K
winlogon.exe	SYSTEM	00	4,108 K
csrss.exe	SYSTEM	02	2,972 K
wscntfy.exe	Pawan	00	1,740 K
smss.exe	SYSTEM	00	376 K

□ Show processes from all users

Processes: 23 | CPU Usage: 7% | Commit Charge: 116M / 2390M

Figure 5-4. Windows Task Manager

Performance
This tab displays a real-time graphical view of the system performance. You can view CPU usage, page file usage, process threads, and physical memory usage in this tab.

Networking
This tab gives you an overview of real-time network performance and utilization. A list of installed network adapters, their link speed, network utilization, and current status is displayed by default in the lower panel.

> When monitoring network utilization from the Task Manager, keep in mind that the percentage of network utilization for a standard Ethernet connection is from 60 to 80 percent, and the percentage of network utilization for wireless networks is from 30 to 40 percent.

msconfig. The *msconfig.exe* is a command-line tool that eventually opens a GUI called the *System Configuration utility*. This utility displays the current system configuration and allows you to safely change system settings. The settings that you can change include the following:

- System startup options for diagnosing startup problems.
- Advanced boot options to start the system in a selected diagnostic mode.

- Changes to the *BOOT.INI* file for selecting an operating system in multiboot systems. You can also make changes to the *WIN.INI* file.
- System services that start automatically during the system start.
- Startup programs that start automatically during the system start.

The *msconfig* utility can be used to safely change system startup parameters to alter the behavior of the system during startup for diagnosing problems.

regedit and regedt32. The *regedit.exe* and *regedt32.exe* commands are used to edit the settings stored in the Windows Registry. The Windows Registry is a collection of system configuration settings in a hierarchical data file. The configuration data includes the operating system settings, user specific settings, application data, hardware components, and all installed device drivers. The hierarchy is organized into keys and subkeys, each of which can have one or more values. The value can be a text identifier, string, binary, word, multiple string, or expandable string. There are five main subtrees in the Registry hierarchy, as follows:

- HKEY_CLASSES_ROOT
- HKEY_CURRENT_USER
- HKEY_LOCAL_MACHINE
- HKEY_USERS
- HKEY_CURRENT_CONFIG

Under extreme circumstances, if you need to make changes to the Registry, you should first make a backup copy of the existing Registry files. The Registry Editor (*regedit.exe* or *regedt32.exe*) program is located in the *%SystemRoot%\System* folder. It can either be run from the command prompt or from the Run option in the Start menu.

> With most of the system settings and configurations made easy using the Windows Wizards such as the System Configuration Utility (*msconfig.exe*), you will hardly need to edit the Registry directly. Unless you do not have another way to configure your system, you should not edit the Registry to change any configuration values. Improperly editing the Registry may render your system unable to boot or generate unexpected errors.

Event Viewer. The Event Viewer console displays error messages, warnings, and other information about system activities. It is also used to view the contents of log files and includes tools to search particular events from the logs. You can open the Event Viewer console from the Start menu, the Control Panel, or the Administrative Tools utility. By default, the console displays the following three types of logs:

Application Event Log
: This log contains errors, warnings, or other information generated by application programs. If an application crashes, you can check the Application Event Log to find details on what actually caused the event.

Security Log

This log contains errors, warnings, and information about security events and security problems such as incorrect logons that are included here by default.

System Logs

This log contains errors, warnings, and information about system events such as system startup and shutdown, services, devices, and drivers.

Log Filtering is included in the Event Viewer to search for specific events. To view specific events, from the View menu, select Filter or Find. You can filter events by event types, event source, category, event ID, user, or computer.

The properties of event logs can be configured to change the way they are saved. The default size of the log files is 512 KB, but you can set the size anywhere from 64 KB to 4 GB.Three options are available:

- Overwrite Events As Needed
- Overwrite Events Older Than X Days
- Do Not Overwrite Events (Clear Logs Manually)

System Restore. The System Restore in Windows XP desktops helps restore the system to a working state after you make changes to the system settings or install applications that make it unstable. It uses *system restore points* to store a snapshot of system settings at regular intervals. When you run the system restore, a calendar is displayed where you can pick a particular system restore point. The System Restore utility can be accessed in one of the following methods:

- Open Help And Support Center located in the Start Menu. Under Pick a Task, click Undo Changes to Your Computer Using System Restore. Follow the instructions.
- Click Start → All Programs → Accessories → System Tools → System Restore. Follow the instructions.

You can create a system restore point manually to aid recovery whenever you are about to make system changes that could render the system inoperable.

1. Click Start → All Programs → Accessories → System Tools → System Restore.
2. Click Create A Restore Point. Click Next.
3. Type a name to identify the restore point in the Restore Point Description box.
4. Click Create.

> System Restore is different from uninstalling applications. To remove applications, you must use the Add or Remove Programs utility located in the Control Panel.

Remote Desktop. Remote Desktop allows you to get access to a remote computer and control it from your own computer. This feature is available only in Windows XP Professional and Windows Server 2003 computers. It is very helpful in troubleshooting operating system and application problems when it is not possible to personally visit the remote computer. You can get full control over the desktop of the remote computer and run programs or configure it as if you were sitting locally on that computer. The following requirements must be met before establishing a Remote Desktop connection:

- The remote computer must be connected to the network and running Windows XP Professional.
- Terminal Services must be running on the Windows XP computers.
- The user who wants to connect to the remote computer using Remote Desktop must be a member of the Remote Desktop Users group or Administrators group on the remote computer.
- If Windows Firewall is configured on the computer, it must be configured to allow a Remote Desktop connection.

In order to configure a computer to accept the incoming Remote Desktop connection, the following steps must be completed:

1. Right-click My Computer and select Properties to open the System Properties dialog box.
2. Click the Remote tab.
3. Click the Allow Users To Connect Remotely To This Computer checkbox.
4. Click the Select Remote Users button to add the users who will be allowed to connect remotely to this computer.
5. Click OK to close the System Properties dialog box.

To connect to a remote computer using Remote Desktop, complete the following steps.

1. Click Start → All Programs → Accessories → Communications → Remote Desktop Connection. This opens the Remote Desktop Connection dialog box (see Figure 5-5).
2. In the General tab, enter the name or IP address of the remote computer, as well as the username, password, and domain name. You can choose to save the password, if you want to.
3. Click Connect.

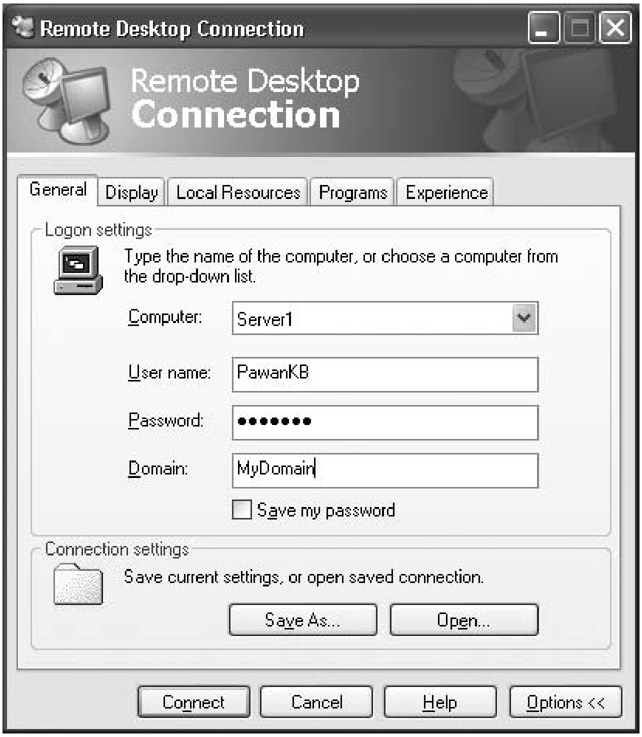
To end a remote Desktop Connection, you can simply log off or use the Disconnect option in the Start menu.

Optimize Operating Systems

Optimization refers to fine-tuning system components in order to enhance their performance. Windows operating systems include several methods to optimize system and application performance. Some of these methods are explained in the following sections.

Virtual memory

When the amount of random access memory is running low, Windows temporarily stores data in a portion of the hard disk called *virtual memory* or the *paging file*. Fine-tuning the paging file setting helps improve system performance by distributing the hard disk space between multiple physical disk drives. The system



Type the name of the computer, or choose a computer from the drop-down list.

Computer: Server1

User name: PawanKB

Password: •••••••

Domain: MyDomain

□ Save my password

Save current settings, or open saved connection.

Figure 5-5. Remote Desktop

automatically sets the paging file and optimizes it for best performance. You can also set the paging file manually, as shown in the following steps:

1. Click Start → Control Panel → System.
2. Click the Advanced tab.
3. Click Settings under Performance.
4. Click the Advanced tab and then click Change in the Virtual Memory section.
5. Change the Initial Size and Maximum Size settings by selecting each disk drive and configuring the settings you wish to use.

If you have increased the virtual memory size, the settings take effect immediately. But when you decrease the virtual memory size, you must restart the system to make the changes effective.

Defragmenting hard disks

Hard disks become fragmented after continuous usage, and when a large number of files are deleted or when some applications are installed. Fragmentation reduces disk performance. Degfragmenting hard disks helps improve system performance by placing files in contiguous locations. Disk fragmentation is covered earlier in the "Disk maintenance" section.

Removing temporary files

Temporary files created by applications and Internet sites consume hard disk space. These files can be removed by a system utility called Disk Cleanup. It is used to free up disk space by deleting temporary files and folders and other data from the disk or volume. This utility is also available from either Windows Explorer or from System Tools under Accessories in the All Programs menu. Disk Cleanup essentially gives you options to delete several types of files. These files include:

- Program files downloaded from the Internet, including ActiveX controls and Java Applets.
- Temporary Internet files to clear the computer cache. These files are stored in the Temporary Internet Files folder.
- Temporary Files located in the Temp folder.
- Files stored in the Recycle Bin.

Managing services

Windows services keep running whether or not a user is logged onto the system. Some services depend on other services and thus create service dependencies. The Services Console in the Administrative Tools utility in the Control Panel allows you to manage services. You can start, stop, pause, or resume any service, control the startup type, or configure how the system should behave if any service fails. The Services Console provides an excellent means of system maintenance. You can access the Services Console in any of the following ways:

- From the Services icon under Administrative Tools in the Control Panel.
- From the Computer Management console. The Services node is located under Services And Applications.
- By running the command *services.msc* from the Run dialog box in the Start menu.

Most of the services are configured to automatically start when the system starts. Disabling unwanted services helps improve system startup and performance. To start, stop, pause, resume, or disable a service, you can right-click it and select the appropriate action. You can also double-click a service to open its Properties window.

System startup

Windows XP and 2000 desktops can be optimized for fast startup performance using several techniques as described in the following list:

- Disable unused system services or set their startup type as manual.
- Use the System Configuration utility (*msconfig.exe*) to remove applications configured to autostart with system.
- Remove any unused applications using Add or Remove Programs in the Control Panel.
- Disconnect all unused mapped network drives.

- Defragment disks periodically using Disk Defragmenter.
- Remove temporary system, application, and Internet files regularly using the Disk Cleanup utility.

Application tuning

Applications can be fine-tuned for optimum performance in Windows XP and Windows 2000 desktop operating systems. When an application starts, it asks the operating system to look for sufficient memory resources and reads data from the disk. Applications can be fine-tuned for performance by carefully organizing system resources such as processor time, memory, and disk space. Optimizing Windows virtual memory also helps improve performance.

On multiprocessor systems, you can use the Task Manager to improve application performance by setting the *processor affinity*, which allows you to dedicate a processor to an application. Using the Task Manager, you can also set *Base Priority*, which allows setting a dedicated processor time for applications.

Diagnostic Tools and Troubleshooting Techniques

As an A+ technician, you will be frequently called on to help users troubleshoot common system problems. You must demonstrate your ability to recover system files, resolve everyday operational problems, interpret error messages, and be able to recognize and apply suitable diagnostic utilities to resolve problems. This section covers a discussion of some of the common troubleshooting tasks and utilities.

Operating system recovery

Operating system recovery is one of the critical tasks that helpdesk professionals have to deal with. Windows XP and Windows 2000 make this job easy by including some built-in utilities that save time and effort in recovering a system that is unable to boot. These utilities include Advanced Boot Options, Recovery Console, Automated System Recovery, and Emergency Repair Disk.

Advanced Boot Options. Some Windows startup problems can be resolved using Advanced Boot Options during the startup phase. When Windows fails to complete the boot process, you can access several recovery options by pressing the F8 key immediately after the POST is complete. The advanced boot options include the following:

Safe Mode

In the Safe Mode, Windows loads with minimum basic system services and device drivers, which is just sufficient to boot the operating system. These components include the keyboard, mouse, hard disks, VGA monitor, and other most essential system services. Safe Mode allows you to enable or disable components one by one in order to pinpoint the troublesome system component.

Safe Mode with Networking

Safe Mode with Networking is similar to Safe Mode except that networking devices, drivers, and services are also initialized.

Safe Mode with Command Prompt

Safe Mode with Command Prompt loads the command interpreter, just like in MS-DOS, instead of the GUI.

Last Known Good Configuration

The Last Known Good Configuration allows you to return to the previous working configuration. This option is normally helpful in cases where you have made changes to the system configuration.

> Note that the Last Known Good Configuration will not be useful if you have already logged on to the system with an incorrect configuration. This option must be used before a successful logon happens.

Recovery Console. The Recovery Console is useful in resolving system startup problems when Safe Mode and the Last Known Good Configuration do not work. Recovery Console allows you to repair critical system files that might have been corrupted by copying original files from the Windows XP Professional setup CD-ROM. You can also enable or disable services that you think might be causing the problem.

The Recovery Console can either be started from the Windows XP/2000 Professional setup CD-ROM or can be installed as one of the Advanced Boot Options. Once in the Recovery Console prompt, you can type help and press the Enter key at any time to get a list of available commands. Type `exit` and press Enter to close the Recovery Console and restart the system.

Automated System Recovery (ASR). The ASR Wizard is located in the Backup Utility. This utility is used to restore the system when there is a major failure. Click the Automated System Recovery Wizard on the Backup Utility window to prepare an ASR backup for the computer. You will need a blank floppy disk and a full backup of the system partition of the computer. This backup can be taken on a tape drive or on a network file server. When you need to restore the system using the Automated System Recovery, you can use the floppy disk to restore the system partition of the computer. You must also restore critical system files that you backed up on the tape drive or a network file share. Other applications and data can be restored using your regular backup sets.

Emergency Repair Disk (ERD). The ERD is used on Windows NT and Windows 2000 desktops to repair a system that fails to start. The most common use of an ERD is to restore critical Windows startup files like *NTLDR*, *NTDETECT.COM*, *NTBOOTDD.SYS*, and *BOOT.INI*. In brief, the ERD can be used for the following purposes:

- To inspect and repair the system startup environment.
- To inspect and repair the boot sector of a disk.
- To verify startup files and replace any missing or corrupt files.

You can create an ERD on a Windows 2000 desktop by using the Backup utility located under the System Tools folder. In Windows NT, the disk can be created using the command-line utility *rdisk.exe*. Note that this method is not available on Windows XP computers.

Resolving common operational problems

Helpdesk technicians should be able to resolve common problems occurring on end-user computers. It is important to understand the basic troubleshooting techniques for resolving a problem. The following sections cover some of the common problems and contain pointers on how they can be resolved.

Printing problems. Printing problems can be caused due to a number of reasons, including the following:

- Insufficient user rights
- Incorrectly selecting a printer, paper type, or paper orientation
- Incorrect printer driver at user's computer
- Loss of network connection
- Stalled printer spooler at the print server
- Paper jams due to poor paper quality
- Failure of a printer component

Depending on the type and exact cause of the problem, you might have to gather information and then correctly identify the correct cause of the problem. An appropriate solution can be applied once you have isolated the problem. For example, if one of the documents has stalled in the print spooler, you can access the printer properties window and delete the document. If a user is complaining about garbled print outputs, you can check the printer driver and version on his desktop. Similarly, if a user is complaining about blank pages, check whether the toner cartridge or the inkjet cartridge is empty and needs to be replaced.

Auto-Restart errors. In Windows XP, a feature known as auto-reboot causes the system to reboot when a critical error is encountered in an application or a system service. If you find that the computer is frequently restarting, you might want to turn off this feature. The following steps explain how you can do so:

1. Click Start → Control Panel → System, or right-click My Computer and select Properties.
2. Click the Advanced Tab.
3. Click the Settings button in the Startup and Recovery section.
4. Clear the Automatically Restart checkbox.
5. Click OK to save settings.

Turning off Auto Restart sometimes results in displaying blue screens with error messages.

Blue Screen errors. A Blue Screen error in Windows is also commonly known as a STOP error or the Blue Screen of Death. This error is seen in many Windows operating systems and is considered one of the most critical. The text that appears on the blue-colored screen usually notifies the user of the cause of the error. These errors are hard to interpret for a normal user. Even some technicians and administrators need external help to resolve them. In most cases, the STOP errors are related to hardware.

Blue Screen errors or STOP errors are identified by an 8-digit hexadecimal number such as STOP 0X0000000A, or STOP 0X0000007F. Windows writes the error in event logs. You can use the Event Viewer to diagnose these errors. If this is not helpful, you can also search Microsoft's TechNet or search Knowledge Base articles on how to resolve the issue. In case the error is caused by a recently added hardware component or a software application, you should remove it to see whether the error is corrected.

System lockup. System lock-up or system freezing is usually caused when the system is out of resources. It either causes long delays in launching an application program, delayed responses to a user's keystrokes, or even permanent lockup of the entire system. The most common reason for a system lockup is shortage of RAM. The most effective resolution for system lockup problems is to increase physical RAM in the system and configure the size of paging files (virtual memory).

Device driver failure. Device driver failures on Windows systems can cause the devices to stop responding or even cause the entire system to fail. They can be caused by incompatible device drivers, corrupt driver files, or incompatible upgrades to installed drivers. Windows uses driver signing to make sure that only signed and tested device drivers are installed on the computers. But, it is possible for a user to install an incompatible driver when the driver-signing options are not properly configured.

The *driver-signing options* allow administrators to stop installation, warn the user, or let the user install unsigned drivers without displaying an error message. You can also use the File Signature Verification (*sigverif.exe*) utility to verify that the installed device drivers are tested and verified by Windows Hardware Quality Labs (WHQL).

When problems occur due to incorrect upgrades of device drivers, you can use the driver Rollback Driver option in Device Manager to rollback to the working device driver. This utility helps resolve many driver-related problems. If this does not work, you can use the Uninstall Driver and Update Driver features to install a correct driver. Most hardware devices come with built-in troubleshooting utilities that help diagnose problems with hardware and drivers.

Application failures. Application failures can start right from the point of installation. If installed successfully, applications can also cause problems when starting or when you are using them. Critical application errors can even freeze the system or restart it automatically. These errors may be due to incorrect configuration or runtime problems when the application accesses system memory. Most of the application-related errors are written to the Application Event logs. You can open the Event Viewer console to get more information about an error.

Application errors are displayed in a small pop-up window, which is usually sufficient to explain the cause of the problem. The following steps are helpful in avoiding application errors:

- Test the applications thoroughly before installation.
- Install only the applications that are compatible with the version of Windows you are using.
- Use the Microsoft Application Verifier (available for free download from Microsoft's web site) software to test compatibility of applications with a particular version of Windows.
- Fine-tune application performance by setting its priority if the application needs more resources than are automatically assigned by the system.
- Keep the application updated using the latest updates from the vendor.
- Educate and train users for correct usage of the application.

Interpreting common error messages

Helpdesk and remote support technicians are required to interpret error messages for operating systems and hardware devices on a regular basis. This section explains some of the common error messages and their probable causes.

Missing Boot Disk or Invalid Boot Drive. The Missing Boot Disk or Invalid Boot Drive error is reported on older computer systems that are configured in BIOS to use either a floppy disk or a CD-ROM drive as the first boot device. The system displays this error when a nonsystem (also known as nonbootable) disk or a CD-ROM that is not able to boot the system is inserted into the drive and the system is restarted. To resolve this error, remove the nonbootable disk from the drive. New computers will automatically skip the first boot disk configured in system BIOS and find a drive that contains the boot files.

Missing NTLDR. The "NTLDR is Missing" error is accompanied by the message "Press Any Key to Restart." This error occurs if any of the following files are missing or have become corrupt:

- *NTLDR*
- *NTDETECT.COM*
- *BOOT.INI*

These files can be restored using one of the following methods:

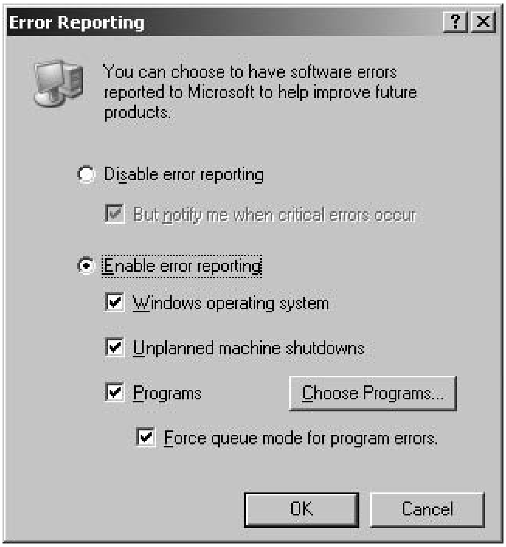
- Using a boot disk (or emergency repair disk) to restart the system (Windows 2000).
- Using Recovery Console.
- Using the setup CD-ROM and selecting the repair option. Press R when prompted.
- Using a System Restore.

Device or service failure. The failure of a driver or a service is usually written to the event logs. You can open the Event Viewer console and locate the appropriate error message to get help in finding the cause of the problem.

Missing Registry entry. Windows Registry is a database of the complete system configuration. Every system service, the drivers, and the applications are registered in the Registry before they can work with the installed operating system. If a component fails to create an entry in the appropriate Registry key, it will not be able to start. One of the easiest methods to resolve these errors is to reinstall the driver or application that generates errors related to Registry entries.

Windows reporting. Windows includes a utility called Error Reporting that sends error messages and symptoms of the error to Microsoft when an application fails. This utility works well for those computers that are connected to the Internet. Microsoft collects this information to check the cause of application failure and make improvements in its applications such as Microsoft Word or Microsoft Excel. This utility is enabled by default. If disabled, you can enable the utility as shown in the following steps:

1. Click Start → Control Panel → System, or right-click My Computer and select Properties.
2. Click the Advanced Tab and click Error Reporting to open the Error Reporting window, as shown in Figure 5-6.
3. Click the Enable error reporting radio button.
4. Click Choose Programs and select the appropriate options by clicking the Add button.
5. Click OK and close all Windows.



You can choose to have software errors reported to Microsoft to help improve future products.

○ Disable error reporting

☑ But notify me when critical errors occur

● Enable error reporting

☑ Windows operating system

☑ Unplanned machine shutdowns

☑ Programs

☑ Force queue mode for program errors.

Figure 5-6. Error Reporting

Utilities for diagnosing operational problems

Most operational problems can be diagnosed and resolved using some common troubleshooting techniques. Common categories of available troubleshooting resources include built-in operating system utilities, documentation, and the Internet. In this section, we will take a brief look at each of these resources.

Bootable media. Bootable media refers to installation setup media or the CD-ROM that contains the operating system setup files. In case the system files become corrupt, you can repair or replace these files using a setup CD-ROM. When the operating system is started using a setup CD-ROM, you are given an option to repair the existing installation.

Startup modes. As noted earlier in this section, Windows operating systems can be started in diagnostic mode by using Advanced Boot Options. These options include Safe Mode, Safe Mode with Networking, Safe Mode with Command Prompt, and Last Known Good Configuration. These options can be very helpful in troubleshooting startup problems.

Documentation. Nothing plays as important a role as documentation. Documentation of operating systems, devices, and application software not only serves as a training resource but is also very helpful in troubleshooting problems that arise from time to time. Helpdesk technicians must read the documentation before installing a piece of hardware to check for its compatibility, its requirements, the installation procedure, and general troubleshooting guidelines.

Most documentation for add-on devices, software applications, and utilities comes in the form of printed manuals. In some cases, the documentation is included on the distribution CD-ROM. For example, Microsoft now includes documentation on the setup CD-ROMs. Other sources of documentation include manufacturers' web sites.

When resolving Windows-based operating system problems, you must check the following for additional help:

- Microsoft TechNet
- Knowledge Base articles
- Microsoft User Community
- Third-party user forums that provide help with Microsoft products

A number of training materials are also available from Microsoft's web site. Some are offered free of charge while others have a nominal fee. Some sites will require you to register and log in before you can access the web site.

Task Manager. Task Manager provides real-time performance data about system, network, and application processes. You can end a nonresponsive application or fine-tune an application performance by adjusting the base priority. It provides a quick snapshot of system activities, including usage statistics for the CPU, paging file, memory, network interfaces, and protocols.

Device Manager. As the name suggests, Device Manager is used to manage devices and troubleshoot problems with devices and drivers. You can install, uninstall, or update device drivers as well as roll back to a working driver in case the newly installed driver does not work.

Event Viewer. As discussed earlier in this section, the Event Viewer console is used to view event logs. You can launch this console from the Administrative Tools folder in the Start Menu.

System Configuration utility. The System Configuration utility can be launched using the *msconfig.exe* command from the Run dialog box in the Start menu. This utility is helpful in verifying the system startup environment. The options for managing the system startup include boot options, services, and applications configured for auto-start. You can use this utility to configure the system to start in a diagnostic mode by selecting items from a given menu. You can also modify the *BOOT.INI* file and select the modified file or the original file to start the system.

Recovery CD. Most vendors supply their desktop computers with a pre-installed operating system. These bundled operating systems do not come with a separate setup CD for the operating system. Instead, the vendor supplies a special CD called the *Recovery CD*. This contains essential operating system files to reinstall the operating system in case the original installation fails to start the computer, or in case startup files become corrupt.

Remote Assistance. Like Remote Desktop, Remote Assistance also helps troubleshoot when it is not possible to personally visit the user's computer. This utility is included in Windows XP and Windows Server 2003 computers. It helps users to get help from helpdesk technicians or administrators when they are facing a problem with the operating system or their applications. The user first sends an invitation to the technician/administrator or *helper* over the network connection. The helper must accept the invitation before the session can start. When the connection is established, the helper can take shared control of the user's computer with the user's permission. This allows the helper to send and receive files to the remote user. The Remote Assistance connection is started from the Help And Support Center located in the Start menu.

System File Checker. The *System File Checker (sfc.exe)* is a command-line utility that helps verify the protected system files after the computer is restarted. If the utility finds a missing, overwritten, or corrupted protected system file, it retrieves the correct version of the file and replaces the incorrect file with the correct one. The following switches can be used with this command:

`/scannow`
: Scans all protected system files immediately.

`/scanonce`
: Scans all protected system files at once at the next boot.

`/scanboot`
: Scans all protected system files every time the system is started.

`/revert`
: Returns the scan to its default operation.

`/purgecache`
: Purges the Windows File Protection cache and scans all protected system files immediately.

`/cachesize=x`
: Used to set the size of cache file.

Preventive Maintenance (PM)

Operating systems and application software must be maintained in order to get good performance and reduce downtimes. Preventive maintenance is one of several methods that can be very effective in preventing system breakdowns. PM methods include tasks such as applying service packs, software updates, hotfixes, and regularly backing up data. In this section, we will briefly discuss these preventive maintenance methods.

Software updates

Software updates keep the operating system and application software up to date. These updates are released regularly by software vendors to fix known bugs in their applications. For example, to address operating problems, Microsoft frequently releases updates for its operating systems and applications such as MS Office. These updates are offered free of cost and are usually available for download from the manufacturer's web site. It is always recommended that you test the updates thoroughly on a test computer before installing them on your users' computers.

Hotfixes. A hotfix is a small piece of software that is used to address a specific problem with the operating system. Hotfixes are generally released as soon as the manufacturer discovers a serious issue with the operating system

Patches. Patches are meant to address small problems immediately. Most patches are related to security, but they often address other problems, such as compatibility issues or the malfunctioning of a particular component of the OS. Manufacturers usually do not announce the release of patches to their software.

Service packs. A service pack is a collection of a number of hotfixes and updates released by the software manufacturer. Manufacturers usually test service packs on a variety of hardware platforms and check their compatibility with various applications.

Windows Update

Windows Update (or Automatic Updates) is a built-in feature for Windows-based operating systems. This feature can be configured to automatically check for, download, and install updates to the installed operating system. This utility can be accessed from the Start menu or from the System Properties window located in the Control Panel. A user can configure Windows Update options in one of the following ways:

- Automatic with user-selected days and timings
- Download automatically but let me choose when to install them
- Notify me but don't automatically download or install them
- Turn Off Automatic Updates

When Automatic Updates are configured for particular days and times, the computer should be left connected to the Internet so that Microsoft's web site can check for new updates and install them as required.

Data backup and restoration

Data backup is one of the most important aspects of preventive maintenance. It ensures that data will be available even when a system crashes or in the event of a disaster. As a technician, you must be aware of the software or built-in utilities available for data backups. Data can be backed up using one or more types of backup methods. Magnetic tapes are very popular as backup media due to their large storage capacity, but you can also back up on CD-RW disks or a network drive. Backup tapes must be safely stored at an off-site and secure location.

On Windows operating systems, backup of a single computer can be taken using the Windows Backup utility. Remember that this utility can also back up data stored on other network drives, and it can back up the entire contents of a disk including the operating system data, which is called the *System State Data*. You can also create ASR disks that are helpful in restoring the system in the event of a system crash.

Remember that Windows XP and Windows 2000 cannot back up data directly onto CD-RW and DVD disks. However, you can copy data to a hard drive or to a shared network folder and then burn a CD-RW or a DVD disk.

Backed-up data has to be available for restoration when required. This implies that you must perform test restores periodically to ensure that the restoration methods used are working properly and that the data is being correctly backed up as desired. Performing test restores is as important as backing up data. Backed-up data is useless if it cannot be restored.

Antivirus software

Antivirus software keeps track of viruses and other malicious software. It helps protect the system to keep it safe and secure from *viruses*, *Trojan horses*, *worms*, and other *malware* such as *spyware* and *adware*. Antivirus software uses virus signatures to detect the presence of malicious software. Virus signatures must be updated regularly so that the antivirus application can effectively detect and clean the system of any new viruses.

Printers and Scanners

This section of the study guide covers essential information required for support jobs related to printers and scanners. Printers are used in every computing environment, and support technicians are expected to attend to service calls for printer installation and troubleshooting on a regular basis.

Fundamentals of Printers and Scanners

As a support technician, you are expected to have a good understanding of the processes involved in printing and scanning. You must also be aware of basic troubleshooting and preventive maintenance procedures. This section covers a brief study of these topics.

The printing process

The following is an overview of the process that takes place on Windows desktops when a user sends a document for printing:

1. When the document is submitted for printing using an application program, the application calls the Graphics Device Interface (GDI). The GDI further calls the driver installed for the selected printer.
2. The print job has specific data type. Print jobs submitted by Windows XP and Windows 2000 have the enhanced metafile (EMF) data type. Many other applications use the RAW data type, which is usually in ready-to-print format.
3. The GDI and the printer driver work together to convert the document format into a language that the printer understands. This data is passed on to the *print spooler*, a special folder on the hard disk that holds print jobs in a queue until the printer is ready to accept the print job. The *local print provider*, which is a component of the print spooler, helps write the print job to the spooler.
4. The local print provider polls the *print processor*, which identifies the print job's data type and receives the print job. The print processor then converts the print job according to its data type.
5. The control of the print job is assigned to the *separator page processor*, which adds a separator page, if the printer is configured to use a separator page to differentiate between print jobs.
6. The print job is taken out of the print spooler and submitted to the print monitor. If the printer is a bidirectional printer, a *language monitor* handles the two-way communication between the computer and the printer.
7. The print job is then passed on to a *port monitor*. The port monitor sends the print job to a printer port where the printer is connected.
8. The printer converts the print job into a bitmap format and prints it.

Remember the names of all components involved in the printing process on Windows computers.

Laser printers

A laser printer is commonly used for producing high-quality text and graphic pages using static electricity. It uses a laser beam to create an image on a photosensitive roller called the *EP drum*. The laser beam hits parts of the EP drum surface and creates an electric charge. This drum is then rolled into a *toner* reservoir, and the toner sticks to the portions of the drum that have the electric charge. This toner is then transferred to paper using heat and pressure in the *fuser* assembly. The speed of these printers is expressed as *pages per minute (ppm)*, and the resolution as *dots per inch (dpi)*.

Laser printers have some valuable advantages over dot matrix, thermal, and inkjet printers. These advantages include:

- High resolution for text and graphics
- Lower cost of printing per page
- Faster speed
- No smearing of ink

Components of a laser printer. In Chapter 2, you learned about various components of a laser printer. Table 5-6 provides a review and summary of the functions of the main components of a laser printer.

Table 5-6. Components of a laser printer

Name	Function
Main Power Supply	Converts the AC power to DC for different circuit boards inside the printer.
High-Voltage Power Supply	Used to produce high voltage to charge the EP drum.
EP Drum	A cylinder coated with photoconductive material.
Primary Corona Wire	Used to supply high negative charge to the EP drum.
Transfer Corona Wire	Used to supply high positive charge to the paper.
Main Motor Assembly	Used by different rollers in the printer.
Scanner Motor Assembly	Consists of motors and mirrors to move the beam of laser light across the EP drum.
Writing Mechanism	Used to guide the laser beam across EP drum, depending on the image stored in printer memory.
Toner Cartridge Assembly	Contains subassemblies for cleaning, developing, and moving toner particles.
Fuser Assembly	Used to provide heat and pressure to paper in order to properly bond the toner powder on it.
Erasing Lamp	Used to remove the image from the EP drum after the image has been transferred onto paper.
Cleaning Assembly	Used to remove the residual toner particles from the EP drum.
Paper Movement Assembly	Used to move the paper through different parts of the printer.
Electronic Control Package (ECP)	Also known as the Logic Assembly. This unit contains the main circuit board of the printer that communicates with computers to receive print jobs.
Control Panel Assembly	This is the main user interface containing different controls for the user.

Laser printing process. This section will explain the printing process used in most laser printers. The laser printing process is composed of the following components:

Cleaning

The EP drum must be clean of toner particles leftover from the previous image before it can take a new image on its surface. A *rubber blade* removes the particles of toner residing on the drum surface. The removed toner is collected in the debris cavity or waste reservoir located on one side of the cleaning unit. A discharge lamp with a specific wavelength then removes the remaining charge from the drum. After the charge is removed, the drum becomes electrically neutral.

Conditioning

The electrically neutral drum is insensitive to light and cannot take any image. A very thin wire called the *primary corona wire* is used to distribute a high negative charge (–600 to –1000 volts) evenly on the surface of the drum. This negative charge again causes the drum to be photosensitive or photoconductive.

Writing

At this stage of the process, the printer's laser beam writing unit and a series of mirrors are used to draw tiny dots on the EP drum, which represent the final image to be produced. The area of the drum that the laser beam comes in contact with loses some of its negative charge (by approximately –100V) and becomes relatively more positive (the charge is still considered negative, just not as negative as the areas not hit by the laser beam). When the laser beam has finished creating the image on the relatively positive EP drum, the printer's controller starts the paper sheet feed process by pulling a sheet of paper into the printer. The paper stands ready at the printer's registration rollers until the controller directs it farther into the printer.

Developing

The drum is rolled in a toner reservoir containing fine dry plastic particles mixed with carbon black or coloring agents. These toner particles are charged with –200 to –500 volts. The charged toner particles are electrostatically attracted to the drum's surface where the laser light left the image. The surface of the drum now holds the image pattern in the form of toner particles.

Transferring

The drum is pressed over rolled paper, which is positively charged. A different type of corona wire known as the *transfer corona wire* is used to charge the paper with a very high positive charge. The positively charged paper attracts the toner particles from the drum leaving the image on the paper.

Fusing

The paper is passed through the fuser assembly containing *pressure rollers* and *heating rollers*. The rollers in the fuser assembly apply heat and pressure to the paper to firmly bond the toner particles to the paper surface. The heating rollers provide up to 200 degrees Celsius of temperature.

Once the printing process is complete, the printer paper is rolled out in an output tray. At the same time, the EP drum is cleaned of the residual toner particles and is stripped of the negative charge to make it electrostatically neutral.

> For the A+ exams, you must remember the steps in the laser printing process. Memorize all the voltages given in these steps. Note especially what the primary corona wire and the transfer corona wire are used for.

Inkjet printers

Inkjet printers work by depositing tiny drops of ink onto the paper surface. They are most commonly used in homes and small offices. This is due to the fact that they are inexpensive and easy to use, and can produce high-quality text and graphics. A print cartridge holds the ink necessary to print. The speed of these printers is expressed as ppm and resolution as dpi.

Inkjet printers fall into the following categories:

Thermal Inkjet
: These printers are mainly used in the consumer market. These printers use water, pigment, or dye-based inks. The print cartridge contains small electrically heated chambers. The printer runs a pulse of current through these chambers to produce steam that forms an ink bubble. This ink bubble is dropped onto the paper to form an image.

Piezoelectric Inkjet
: Most commercial and industrial facilities use these types of printers. These use a piezoelectric crystal in each nozzle instead of heating elements. The piezoelectric process uses crystals that react to electric charge. When charged, a crystal draws or pulls ink from an ink storage unit held above the crystal. In simple terms, the piezoelectric process can cut or refine the exact amount of ink needed to refine the dot placed on the paper. This reduces the smudging effect of traditional inkjet technology and provides better printer resolution. In fact, this process allows resolutions greater than 1440 dpi.

Continuous Inkjet
: These printers are mainly used for the marking and coding of products. A high-pressure pump directs liquid ink from the ink reservoir into a microscopic nozzle, thereby creating a continuous stream of tiny ink drops. A piezoelectric crystal creates ink droplets from the stream of ink. These tiny ink drops are electrically charged, which are further directed to printing paper.

The inkjet printing process. The inkjet printing process consists of the following steps:

Printhead cleaning
: The printhead is cleaned to ensure that there is no residual ink on the printhead from the last printing job.

Paper feed

The control circuitry initiates the paper feed assembly that contains a stepper motor. This motor engages a number of rollers to pick up a piece of paper from the paper tray and guide it into the printer. A sensor checks to determine if the tray is empty and gives an "Out of Paper" error.

Printhead movement

The printhead stepper motor uses a belt to move the printhead assembly across the paper. This assembly stops at each point for a fraction of a second to spray the ink on the paper surface and then moves again to the next position. It is almost impossible to judge the stopping and moving of the printhead due to its speed.

Printing next line

The printhead drops multiple dots of ink at each stop. The paper feed motor then moves the paper to the next line. This continues until the printing process is complete.

Printhead parking

Once the printing process is complete, the paper feed assembly pushes the paper onto the paper tray. The printhead is then parked in its home position.

Solid ink

The solid ink printing technology was originally developed by Tektronics, whose printing division was later taken over by Xerox. Solid ink printers use sticks of solid ink instead of inkjet or toner cartridges. Once the stick is installed in a printer, the ink is melted and used to produce images on paper. These printers are mainly used in offices for printing high-quality graphics images.

The printing process in solid ink printers is similar to the one used in offset printing. The solid ink sticks are installed in printers. The ink is melted and fed into printheads that contain piezoelectric crystals. The printhead sprays the ink onto a rotating drum that is coated with oil. The paper is then passed over the drum that transfers the image onto the paper.

According to Xerox (the main producer of the Phaser brand of solid ink printers), these printers offer the following advantages over other types of printers:

- Solid ink printers can produce images on a variety of paper and even transparencies.
- The image quality is superb and better than many other printing technologies.
- Solid ink printers are easy to use and maintain.
- Solid ink is helpful in protecting the environment due to reduced waste output.

The disadvantages of solid ink printers include their high power consumption and long warm-up times.

Thermal printers

Thermal printers work by pushing heated printhead pins against heat-sensitive paper called *thermochromic paper* or *thermal paper*. Some fax machines (except plain-paper faxes) and calculators with printing capability use the thermal printing process. These printers are inexpensive, but the cost of thermal paper is one of the considerations when calculating recurring cost of consumables. Thermal printers also use a combination of dots to create the text or image impression on paper. There are two main methods of transferring text or images on paper in thermal printers:

Direct Thermal
: These printers create images by burning a matrix of dots on heat-sensitive paper when the paper is passed over a thermal printhead. The area of paper where it is stroked by the heated printhead is turned black, and other areas remain white.

Thermal Wax Transfer
: A second type of thermal printer uses wax-based ink, which is melted from the ribbon and transferred to the paper surface to create text or graphics images. The main disadvantage of this type of printer is that the same amount of ink is used whether the paper is full of text/images or only a part of the paper is printed on.

Impact printers (dot matrix)

Impact printers work by hitting a head or a needle against an ink ribbon to place a mark on paper. The paper is held firmly on a solid roller called *platen*. These printers produce significant noise when they are operating but are considered very efficient for printing multipart forms such as invoices. Some of the commonly used impact printers include the following:

- Dot matrix printers
- Daisy wheel printers
- Line printers

The dot matrix printer is the most commonly used printer for personal and small business applications. The line printer is used when speed and volume of printing is a main requirement.

> The speed of line printers is expressed as *lines per minute (lpm)*, and the speed of dot matrix printers is expressed as *characters per second (cps)*. Similarly, the printing speed of laser printers and inkjet printers is expressed as pages per minute (ppm) because these printers are also called *page printers*. The printing speed varies by the quality of printing. The higher the resolution, the lower the printing speed.

The dot matrix printing process. *Dot matrix* refers to the way a printer creates text characters or images on paper. Dot matrix printers use a printhead containing a number of pins held vertically in one or two columns. Low-resolution printers have a printhead with 1 column of 9 pins while high-resolution printers have a printhead with 2 columns containing 24 pins. The pins strike an ink ribbon that makes an impression of small dots on paper when the printheads moves back and forth. As the printhead moves in a horizontal direction, the printhead controller sends electrical signals and forces pins to strike against the ink ribbon. The timing of the electrical signals is programmed in the printer for every character it is able to print. The impressions appear as small dots and form appropriate characters on paper. It is possible to change the character style by simply changing how and when the pins strike the paper. Figure 5-7 shows how a matrix of dots forms a character on paper.

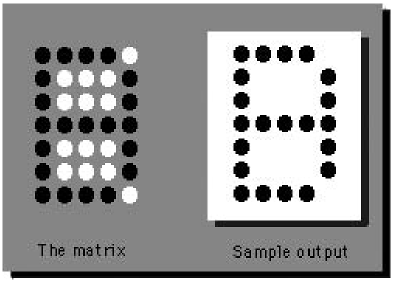


Figure 5-7. Dot matrix printing

Scanners and the scanning process

In very simple language, scanners are used to take a snapshot of a paper containing text or images and create an electronic document. This document can be saved as a file, can be altered and used to reproduce the image as another printed document, or can be used as part of any other electronic document. Scanners are widely used in the printing and publishing industry and even at home, due to the increased popularity of multifunction printers.

Types of scanners. Before we discuss the scanning process, let's look at different types of scanners. Scanners are classified into the following main categories:

Flatbed
These are the most widely used type of scanners. They use a glass platform where a paper is put face down. A motorized belt moves a lamp to scan the image.

Handheld
These scan the image using the same method as flatbed scanners, with the only difference being that the scanner is moved against the stationary image.

Sheetfed
These are commonly found in home printers. In these scanners, the paper is moved over a scanning lamp that remains stationary.

Drum

These are high-end scanners used in the printing and publishing industry to produce high-quality graphics images. The image to be scanned is placed on a glass drum or cylinder. The scanning process uses a *photomultiplier tube (PMT)* to convert the optical signals reflected from the image into an electrical signal.

The scanning process. The scanning process involves placing a document on a glass platform and moving a scanning head across the surface of the document. The optical signals generated by light reflect off the document, are collected by charged coupled devices (CCD), and converted into electrical signals. The following steps explain the scanning process in detail:

1. The user places the document face down on the glass plate and closes the scanner cover. The cover is usually white and provides a reference point for the scanner.
2. The document is illuminated by a CCFL.
3. The scanning head is moved slowly across the surface of the document using a belt attached to the main stepper motor. When the scanning head has finished the entire document, it has completed one pass. Some high-resolution scanners use multiple passes to complete the scanning.
4. The image of the document is passed through a set of reflective mirrors and focused onto a lens.
5. The lens passes the image to an array of CCDs through an image filter. In the case of multiple pass scanners, there are different filters for different colors.
6. The scanner driver passes the image of the document to the application software used to acquire the image from the scanner.
7. The applications (Photoshop, Corel Draw, etc.) use a standard language, such as TWAIN, that acts as an interpreter between the scanner and the application.

Installing and Configuring Printers and Scanners

Installation and configuration of printers and scanners is one of the most important jobs for a computer technician. You must be able to verify compatibility, as well as install a printer or a scanner, install a suitable driver, and then configure it for optimum performance. The procedure for installing or configuring will vary from one model to another, but the basic steps remain the same. This section of the Study Guide provides some essential installation and configuration topics for printers and scanners that you are expected to know for the A+ exams as well as in the field.

Installing and configuring printers

New printers are added from the Printers and Faxes utility in the Control Panel. Right-click the Printers, and the Add Printer Wizard walks you though various pages that collect information about the printer and then installs the printer driver. You can configure the new printer as a local printer or as a network printer depending on where the printer is actually connected and by specifying the printer port. You can select one of the preconfigured ports on the computer such as LPT1, or you can create a new port. When you select the Create a New Port button, you can specify the type of port that you want to use. This is where you can configure a printer connected directly to the network.

Finally, you are prompted to specify whether you want to share the printer. When you share a printer, you need to configure clients so that users can locate and send print jobs to the new printer. All client computers need a printer driver in order to print to the shared printer. Windows XP Professional will automatically download printer drivers for Windows 2000, Windows NT 4.0, Windows Me, Windows 98, and Windows 95 clients.

Verifying compatibility. It is important to verify the compatibility of a printer or scanner with the installed desktop or network operating system (and with applications) before they are purchased. It is useless to purchase a printer or scanner if it does not work with either the operating system or the application. Compatibility with the operating system ensures that the documents will be correctly formatted before being sent to the printer. Compatibility with the application software ensures that the application can successfully use the device. This is particularly applicable for scanners, which are mainly used by graphics applications such as Corel Draw and Photoshop. These applications acquire the scanned images through device drivers.

Device compatibility can be checked by any of the following methods:

- Marketing brochures and device documentation
- Web site of the device manufacturer
- Web site of the operating system and application software manufacturer

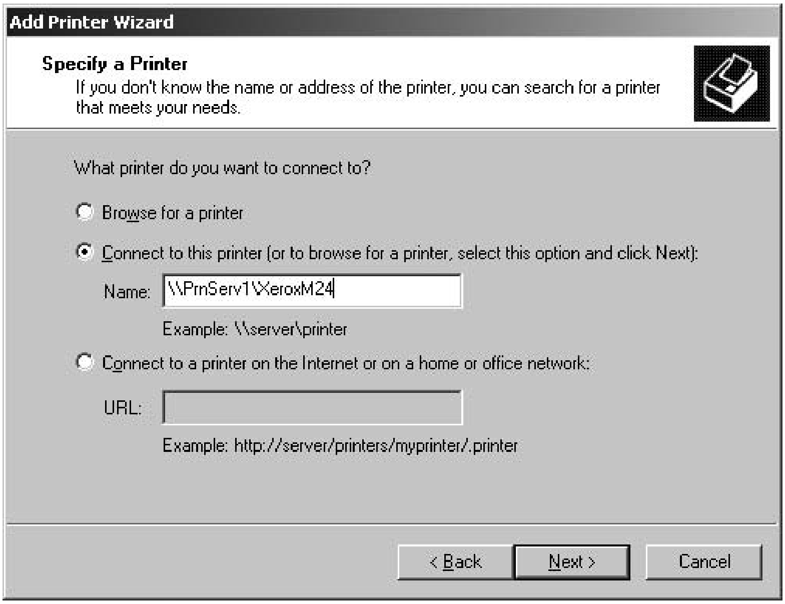
Most manufacturers test their devices and drivers with a variety of operating systems and applications to ensure flawless interoperability. In case you have an older printer or scanner, you will need to get updated driver software to make sure that the device works well with a new version of the OS or the application. You can also verify compatibility by installing the device on a test computer before making it available to end users.

Connecting to a local port. The Add Printer Wizard in Windows desktop allows you to select either a local port or a network port when installing a printer. A printer can be attached to a local port such as LPT1 or a USB port. The following steps explain the installation process:

1. Click Start → Printers and Faxes. This opens the Printers and Faxes window.
2. Click Add A Printer. This starts the Add Printer Wizard dialog box.
3. In the Local or Network Printer page, click Local Printer Attached to this Computer.
4. Click Automatically Detect and Install my Plug And Play Printer. Click Next.
5. In the Select A Printer Port page, click LPT1 in the Use the Following Port box.
6. Follow the next instructions to complete the installation process.

Connecting to a network port. This process depends on whether the network printer is attached to another computer such as a print server or is directly connected to a network port. The following steps explain the installation process:

1. Click Start → Printers and Faxes. This opens the Printers and Faxes window.
2. Click Add A Printer. This starts the Add Printer Wizard dialog box.
3. In the Local or Network Printer window, click Network Printer or a Printer Attached to Another Computer.
4. If you are connecting to a printer attached to a print server, type the name of the server and the printer share name in the \\*Print_Server**Printer_Share* format as shown in Figure 5-8.
5. If you are connecting to a printer directly attached to a network port, click A Local Printer Attached to this Computer.
6. Click Create a New Port and select Standard TCP/IP Port. This starts the Add Port Wizard.
7. Type the IP address or the name of the printer. The name of the port will be displayed. Follow the instructions to complete the process.


Add Printer Wizard

Specify a Printer

If you don't know the name or address of the printer, you can search for a printer that meets your needs.

What printer do you want to connect to?

○ Browse for a printer

● Connect to this printer (or to browse for a printer, select this option and click Next):

Name: \\PrnServ1\XeroxM24

Example: \\server\printer

○ Connect to a printer on the Internet or on a home or office network:

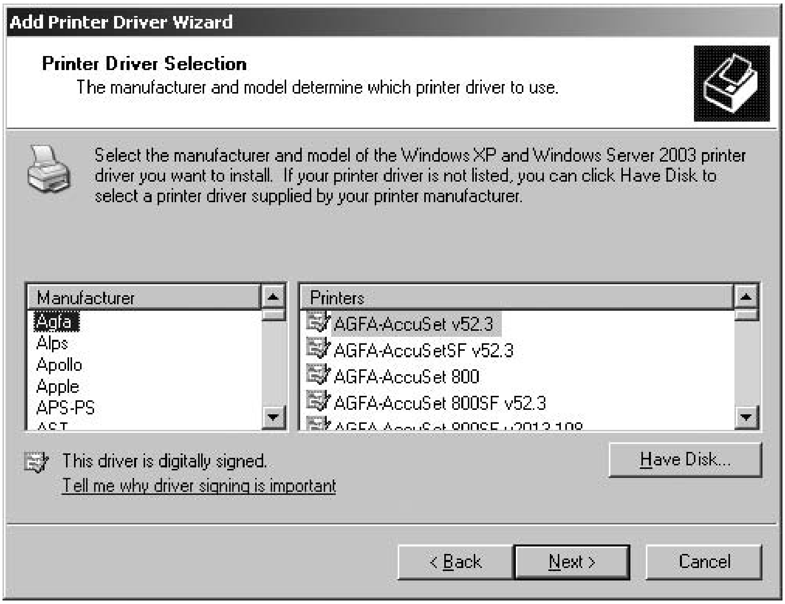
URL:

Example: http://server/printers/myprinter/.printer

Figure 5-8. Installing a network printer

Installing printer drivers. Most printers for personal computers are the PnP type that are automatically detected and installed by the operating system. The only condition is that the computer BIOS, the operating system, and the printer should all support PnP. Desktop operating systems (such as Windows XP Professional and Windows 2000 Professional) have a built-in library of common printer drivers that install an appropriate driver for the printer. When a PnP printer is detected, the New Hardware Found Wizard starts, which guides you through the driver installation.

If the printer is not PnP or is not supported by the operating system, you can install the printer driver manually. Connect the printer to a local or network port and turn on the power. Use the Add Hardware utility in the Control Panel to install the printer driver that came with the printer. During the driver installation phase, the Add Printer Driver Wizard allows you to select a printer and model from a built-in list as shown in Figure 5-9. If the printer you are installing does not appear in this list, click the Have Disk button to install the driver from the disk or CD-ROM that shipped with the printer. Make sure that the printer is connected and powered on when you install the printer driver.



Add Printer Driver Wizard

Printer Driver Selection

The manufacturer and model determine which printer driver to use.

Select the manufacturer and model of the Windows XP and Windows Server 2003 printer driver you want to install. If your printer driver is not listed, you can click Have Disk to select a printer driver supplied by your printer manufacturer.

Manufacturer: Agfa, Alps, Apollo, Apple, APS-PS, AST

Printers: AGFA-AccuSet v52.3, AGFA-AccuSetSF v52.3, AGFA-AccuSet 800, AGFA-AccuSet 800SF v52.3, AGFA-AccuSet 800SF v2013.108

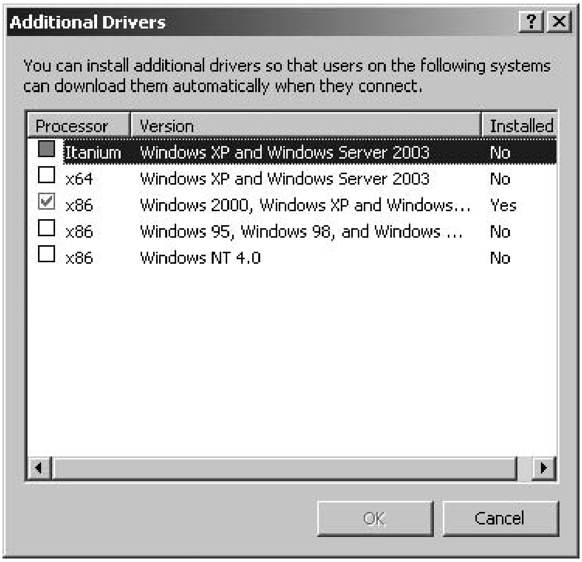
This driver is digitally signed.

Tell me why driver signing is important

Figure 5-9. Installing a printer driver

As noted earlier in this section, when you share a printer on a Windows XP/2000 computer, you are given an option to install additional drivers for other Windows-based computers that will send print documents to the printer. Figure 5-10 shows the dialog box that appears when you click the Additional Drivers button in the Sharing tab of the Printer Properties dialog box.

Calibrating printers. All newly installed printers need to be calibrated for accurate printing. This is due to the fact that alignment of printer parts, such as the printhead, gets a bit misaligned during transportation. *Calibration* readjusts the alignment to ensure that the printed images do not appear smeared on paper. Most printers come with a calibration utility, which is installed automatically along with the printer driver.



Additional Drivers

You can install additional drivers so that users on the following systems can download them automatically when they connect.

Processor	Version	Installed
■ Itanium	Windows XP and Windows Server 2003	No
☐ x64	Windows XP and Windows Server 2003	No
☑ x86	Windows 2000, Windows XP and Windows...	Yes
☐ x86	Windows 95, Windows 98, and Windows ...	No
☐ x86	Windows NT 4.0	No

Figure 5-10. Installing additional printer drivers for Windows clients

In some inkjet printers, the calibration utility is triggered automatically when you change the print cartridge. The printer display and the user control panel located on top of the printer help you through the steps of the calibration process.

Configure printer options. Printer properties vary from one printer to another. To access the configuration page, open the Printers and Faxes folder from the Start menu. Right-click the printer and select Properties from the context menu. Figure 5-11 shows the properties page for a typical printer where you can configure its settings.

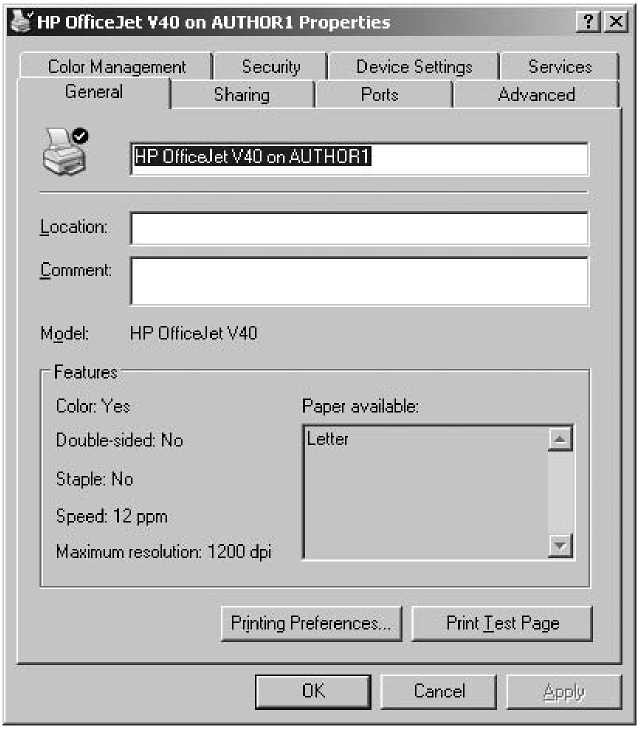
The following configuration options are available on most printers:

General
This page has options for specifying the printer location, setting printing preferences, and printing a test page.

Sharing
This page allows you to share the printer (or stop sharing, if already shared), specify the share name, and install additional printer drivers for clients.

Ports
This page allows you to configure the port that is connected to the printer. You can add or delete a port and can also enable Printer Pooling. *Printer Pooling* is used for load sharing when you have multiple identical printers connected to the same port.

Security
This page allows you to set access permissions for both local and network users who send print jobs to the printer. Printer permissions are explained later in this section.



HP OfficeJet V40 on AUTHOR1

Location:

Comment:

Model: HP OfficeJet V40

Features

Color: Yes

Double-sided: No

Staple: No

Speed: 12 ppm

Maximum resolution: 1200 dpi

Paper available:

Letter

Figure 5-11. Configuring printer options

Advanced
This page lets you configure availability of the printer, printer priority, and spooling options. *Printer priority* is defined when you have configured multiple logical printers for the same printer. It enables you to prioritize print jobs sent to the printer. In this page, you can update the printer driver, if required. You can also set printing defaults, set a separator page, and specify which print processor is to be used by the printer.

Device Settings
This page enables you to configure device specific settings. These settings differ from one device to another.

Color Management
This page is used to configure color options so that there is consistency between the colors displayed on the monitor and those printed on paper.

Services
The settings in this tab depend on the make and model of the installed printer. Usually, these include maintenance functions such as printhead alighment, cleaning, and so on.

Educating users

Most printer and scanner problems occur due to lack of user training. Users do not know how to select a printer when multiple printers are installed in the network. Sometimes they do not know how to choose the appropriate paper size or paper tray. The first and most important step in educating users is to educate yourself. You can do this either by attending a training session organized by the vendor or by reading the documentation.

The following are some important points regarding user education and training regarding printers and scanners:

- Hold training sessions for all users or groups of users in case there are a large number of users.
- Educate the users about the main features of the printers or scanners.
- Show them how to select an appropriate printer from within an application.
- Show them how to select paper from the available paper trays/sizes and how to select paper orientation (portrait or landscape).
- Show the users how to make changes to printing preferences for a particular document.
- In organizations where the printers are leased and charged on per printed page basis, it is helpful to tell the users to carefully select black and white or color prints.
- Train the users on how they can manage their own documents from their desktops.
- Advise users about keeping the area around the printers clean.
- Encourage the users not to attempt fixing problems themselves. They should not try to open the printer or scanner covers to change toner or clear paper jams, but should call the helpdesk instead.

Upgrading printers and scanners

As with other devices, printers also need to be upgraded due to changes in requirements. Changes in computer system hardware to which a printer or scanner is attached might require upgrades to these devices or might require operating system upgrades. Upgrades can be in the form of new and updated device drivers, new firmware releases, or the expansion of device capabilities in the form of a memory expansion.

Memory. High-end laser printers are typically used in office environments where the volume of printing is significantly large. These printers are usually installed on a print server but may be physically connected to one of the network ports. These printers require large built-in RAM to temporarily store the documents submitted for printing. The larger the amount of RAM, the larger the number of documents a printer can accept for printing. Most of these printers have the option to extend the memory by installing additional memory modules or memory sticks. In most cases, the manufacturer's support technicians perform the memory upgrades.

In some situations, you may be required to upgrade a printer memory. You need to make sure that the memory module is compatible with the make and model of the printer. It is recommended that you obtain the memory module directly from the printer manufacturer, and that you ask for necessary installation instructions. Otherwise, you should refer to the printer documentation for help. Make sure that the memory module is compatible with the expansion slots available in the printer.

Drivers. Like most software and hardware vendors, printer manufacturers also regularly update the printer drivers and make these updated drivers available free of cost on their web sites. This usually happens when the operating system version is changed and printer manufactures have to update the drivers for their old printers for the new version. Updated or new printer drivers must be tested before they are finally installed on print servers.

On a Windows XP desktop, a printer driver can be updated from the Advanced tab of the printer Properties window. Click on the New Driver tab to launch the Add Printer Driver Wizard. The Wizard guides you through the installation process, which is more or less similar to the process for installing a new printer driver.

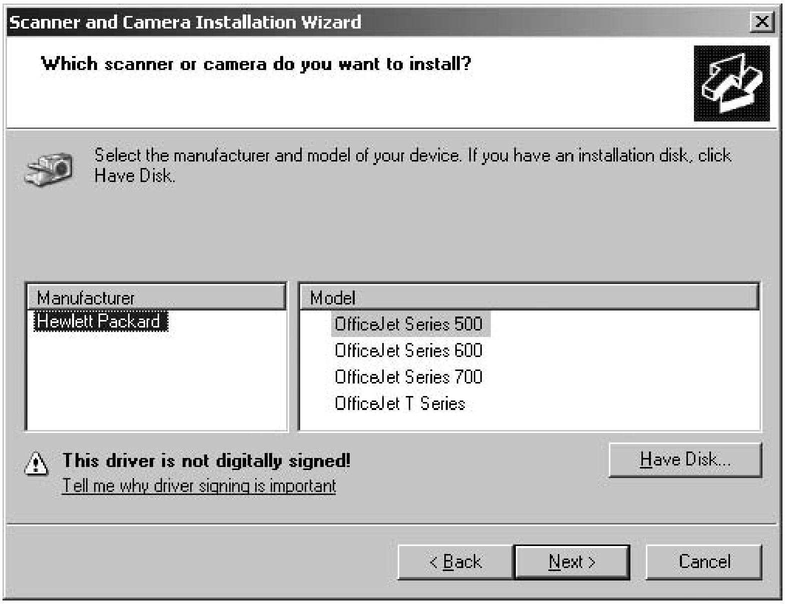
Firmware. Firmware refers to the BIOS of the printers or scanners. In some cases, it is necessary to upgrade the firmware to take advantage of new or advanced features of the device. Firmware upgrades are usually done by either replacing the firmware chip in the device or through a software application provided by the device manufacturer. You should consult the device documentation and follow the manufacturer's instructions on how to obtain and install firmware updates.

Installing and configuring scanners

The process for installing a scanner is very straightforward in Windows XP and Windows 2000 computers. Make sure that the scanner is connected to an appropriate port, such as a serial, USB, or SCSI port, and then turn on the power. Most of the new scanners are PnP devices that are automatically detected by the operating system, and an appropriate device driver is installed. If the scanner is not PnP-compatible, or in case the OS does not recognize the device, it can be manually installed using the disk or CD-ROM provided by the manufacturer.

The Scanners and Cameras utility in the Control Panel is where you can install scanners. Complete the following steps to install a scanner:

1. Open the Control Panel from the Start menu.
2. Double-click the Scanners and Cameras icon.
3. Double-click the Add Device icon to start the Scanners and Cameras Installation Wizard as shown in Figure 5-12.
4. Select the scanner from the list of devices and click Next.
5. Follow the instructions for the installation of an appropriate driver.
6. If the device is not listed in the Scanner and Camera Installation window, you can click the Have Disk button to manually install the driver from the manufacturer's disk or CD-ROM.



Scanner and Camera Installation Wizard

Which scanner or camera do you want to install?

Select the manufacturer and model of your device. If you have an installation disk, click Have Disk.

Manufacturer	Model
Hewlett Packard	OfficeJet Series 500 OfficeJet Series 600 OfficeJet Series 700 OfficeJet T Series

This driver is not digitally signed!

Tell me why driver signing is important

Figure 5-12. Installing a scanner

Scanner configuration is done using the device driver application that is shipped with the scanner. These utilities guide you through different settings to correctly set the parameters so that the scanner functions in the desired way. Some graphics applications such as Corel Draw or Photoshop can also be used to fine-tune the scanner settings.

Optimizing printer and scanner performance

In its default configuration, a printer is set to provide acceptable performance levels. *Performance* refers to the efficient use of ink or toner, as well as establishing an acceptable printing speed. The quality of text and images is configured in such a way that the least amount of ink or toner is used and the printing speed is optimized. The quality of images can be improved by increasing the resolution, but this comes at the cost of printing speed. The greater the resolution, the slower the printing speed. The same is also true with scanners. If you increase the scanning resolution, the scanning speed is reduced.

Resolution. Resolution of a printer or scanner refers to the dpi of the printed or scanned image. This is a measurement of the image quality for both printers and scanners. In the case of scanners, the resolution refers to the number of dots scanned per inch on the document, while for printers it is the number of dots printed per inch on the paper. The higher the dpi value, the better the resolution. Most printers and scanners allow you to adjust the resolution for an individual document, or you can set the altered resolution as default. These adjustments are usually done using the built-in driver utilities. For normal printing, you can choose from draft, economy, normal, or best-quality print outputs.

Color profiles. Color profiles allow you to adjust the colors of the printed image based on the type of media being used and the current configuration of the printer. Color profiles are also used in scanners to adjust the quality of scanned documents.

File formats. File formats and images largely affect the quality of a document. While you do not have much choice in selecting the format for text documents, image documents vary in file sizes and quality depending on the file format used. Image file formats vary depending on their resolution and the number of colors used. Popular image formats include TIFF, BMP, JPEG, GIF, and PNG.

Troubleshooting Printers and Scanners

Any electronic device that has moving parts in it is prone to developing problems. In printers, both the paper guide assembly and the printhead move, while in scanners, only the scanning assembly moves. These problems may be related to the inability of end users to connect to or use the device, or they might be related to device performance. The troubleshooting process for printers and scanners depends on the type, make, and model of the device. The following troubleshooting procedure is generalized and can be used for both printers and scanners.

Gathering information

The first step in troubleshooting is to gather sufficient information about the symptoms of the problem. Information gathering is vital to the problem-solving process. In some cases, you might have to collect information by telephone, which is rather a difficult process compared to onsite troubleshooting.

This information may come from the user, from error messages on the device, from the system where the device is connected, or from system event logs. In some cases, the noise in a printer or a scanner coming from a broken gear might tell you what is causing the problem. It is important to make note of what happened and in what sequence it happened.

Information about the problem may be as simple as a user reporting that he cannot print to a specific printer or as complex as the printer is not responding. There may be more than one reason behind a nonresponsive printer. The printer might be out of paper, there may be a paper jam, or the user's computer may not be connected to the print server.

For unattended printers attached to a network port, the problem might be reported as just a nonfunctioning printer. You might have to send a document for printing to know the exact symptoms of the problem. This is known as recreating the problem. Recreating the problem is necessary when there is no one to give you any information on symptoms of the problem.

Analyzing the collected data

The next step is to analyze the collected data. This analysis gives you a number of possible causes of the problem. Note down all the possibilities on a piece of paper and try to figure out what could be the most probable reason for the problem. When you arrive at a conclusion, you may be able to find an appropriate solution.

For example, if a user has reported that he cannot print to a network printer, there could be several reasons behind it as follows:

- The user does not have sufficient permissions to use the printer.
- The user is not connected to the network.
- The user is sending the print job to a wrong printer.
- The user is selecting a wrong paper source (tray).

There could be more than one reason behind a problem, and you must be careful not to ignore even the smallest potential cause. A careful study of collected data will enable you to look at the problem from all possible angles.

Isolating the problem

Once you have concluded the most probable cause of the problem, you will need to isolate the problem in order to find an appropriate solution. Doing this ensures that you have correctly identified the problem. Correct identification further ensures that a correct solution will be applied.

Here are some main pointers to isolating printer problems:

- Verify whether the problem is due to device malfunction or due to user error.
- Verify that the device is Online and in Ready mode.
- Check for visual indicators on the device panel. Visual indicators refer to status LEDs on the front panel that indicate the current status.
- For printer-specific problems, verify that there is not a paper jam and that the paper path is clear.
- If all users are complaining of a nonresponsive printer, verify that the print server is online, that the print queue is not stuck, and that it has sufficient hard disk space to hold spooled documents.
- If required, delete the stuck document on the print server or clear the print queue. This is known as clearing the print spooler.
- As a last resort, you might have to recycle power on the printer. This action clears all documents currently in printer memory.

Applying the solution

Once the problem is identified, you will need to find an appropriate fix or solution. This solution depends on whether the problem is concerned with the device configuration or with some mechanical failure. If it is a mechanical failure, you might have to replace a part or might need to call the supplier's support technician to fix it. In case the problem is related to an incorrect configuration, you might be able to solve the problem by yourself by following the supplier's guidelines or common troubleshooting techniques. In case you need to order some parts from the supplier, you will need to note down the make and model of the printer or scanner, as well as the correct part number of the printer assembly that needs replacement.

Most problems in printers are caused by an incorrect configuration, either on the printer itself or on the print server. When you need to make some configuration changes to resolve the issue, make sure that you test your solution properly so that the solution does not create further problems. For example, setting user permissions incorrectly for a printer might leave the user unable to print to the printer. As another example, incorrectly configuring the printer might escalate the problem and cause significant delays in fixing the problem. Follow the guidelines of the supplier/manufacturer or get help from your superiors if you are not sure about a particular resolution.

When the problem is fixed, you need to test your solution by verifying the functionality of the printer. Print a test page locally on the printer and take a test pattern sheet with which to compare the printer image. Test patterns are explained later in this chapter. You should also ask a few users to send print jobs to the printer.

Repair tools

If a printer or scanner needs a new or replacement part, you will need appropriate tools to open the device in order to install a new part or assembly. Correct selection and use of tools ensures that the internal mechanism of the device is not damaged during the repair or when replacing an assembly.

Multimeter. A multimeter is a small, handheld instrument that is used for testing connectivity and to measure voltage or current passing through a wire. It is particularly helpful in measuring the input and output voltage on power supplies and the amount of power supplied to various assemblies inside a device. Multimeters are mainly available in two categories: analog and digital. *Analog* multimeters display the output using a scale and needle. *Digital* multimeters display the output on a small LCD screen. Analog multimeters are sometimes called Voltmeter, Ohmmeter, and Ammeter (VOM). Digital multimeters are simply called DMMs.

A rotary switch on the front allows you to select an appropriate range of the voltage, current, or resistance to be measured. There are two test cables, each with a smaller end and a longer end. The smaller end is inserted into the multimeter sockets while the longer end is used to test voltage or current by touching the end to appropriate pins.

Screwdrivers and extension magnet. A screwdriver is the most basic tool that every technician should have. When working with printers and scanners, you will need to have different types of screwdrivers, each with a different type of bit. You can also keep a single screwdriver in which the bit can be changed according to the shape of the screw. Different types of bits are shown in Figure 5-13. These bits are named as slotted (a), Philips (b), Posidrive (c), Torx (d), and Hex (e).

When replacing parts in printers and scanners, you might need to open screws that are located far inside the device where your hand cannot reach easily. In such cases, an extension magnet helps in reaching these places. The extension magnet ensures the safety of the technician as well as prevents screws from falling down when they becomes loose. It is also used to pick up screws that fall down accidentally.

Cleaning solutions. Cleaning solutions are used to clean parts of scanners and printers. These include the glass surface, the light tube, the reflecting lenses, and those parts of laser printers where excessive toner usually spills during normal

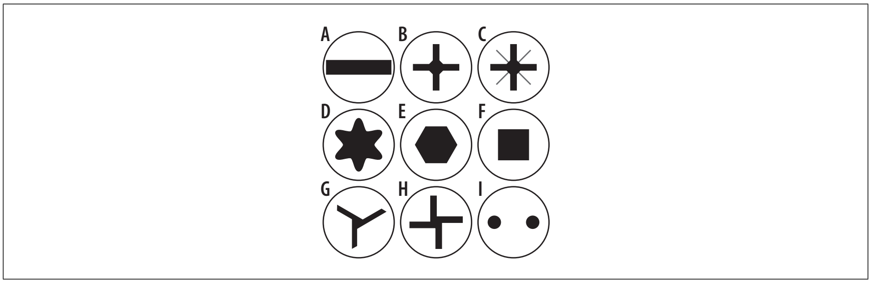


Figure 5-13. Types of screwdriver bits

operation. The cleaning solutions contain chemicals and should be stored and carried safely. They should be used with caution using protective gloves.

Test patterns. Most printers come with software testing utilities to test the functionality of the printer. The test pattern is a reference page that is compared to the printer output to identify the variation of actual print from the test pattern. The test pattern is used as a reference point for comparing resolution, color quality, and alignment. If there are differences in the printed page and the test pattern, the printer needs to be calibrated or its heads need to be realigned. High-end laser color printers have test patterns for both black and white and color printing. Figure 5-14 shows a sample test pattern.

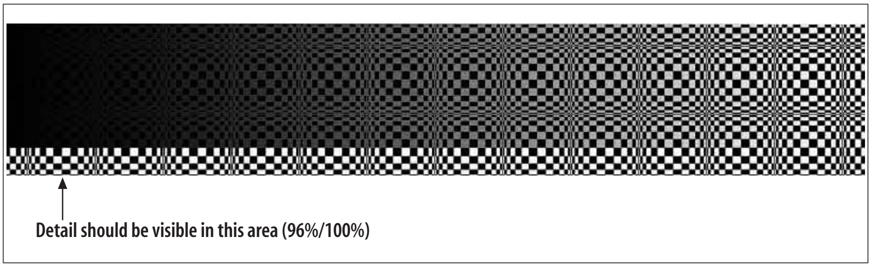


Figure 5-14. Sample test pattern

On smaller PC printers, the printer driver allows you to print a test page to verify that the printer has been installed correctly. The test page shows different horizontal and vertical lines to test printhead alignment. Black and white and color images are printed to verify the resolution of the printer. On a Windows XP/2000 desktop, you can print a test page for the installed printer from the Printer Properties window.

Preventive Maintenance (PM)

Preventive maintenance is important to achieve maximum uptime and quality of service from printers and scanners. Lack of regular scheduled maintenance can cause failure of electronic and mechanical parts. The failure of even a small part can cause disruptions in business activities. A+ technicians are expected to understand the purpose, importance, and components of preventive maintenance. In this section, we will summarize the importance of scheduled preventive maintenance, environment, and supplies.

Scheduled maintenance

Scheduled maintenance refers to performing maintenance of printers and scanners at predetermined intervals. Scheduled maintenance usually includes the following actions:

- Printers use ribbon, ink, or toner. These materials can smear or spill over different parts of the printer after regular usage. Besides this, pieces of paper fall into the open corners and make their way inside the printers. Cleaning of printer parts helps in preventing breakdowns.
- Both printers and scanners use small mirrors that accumulate dust with the passage of time. Scanners and multifunction printers that include a scanner or fax have glass surfaces where users put documents. This surface becomes dirty and must be cleaned regularly.

Environment

Environmental factors such as humidity, cleanliness, and temperature play an important role in the functionality of all electronic and electromechanical devices. These factors need to be controlled to minimize the breakdown of equipment.

Humidity. Humidity should be maintained between 60 and 80 percent for normal operation of printers and scanners. Extremely humid or extremely dry conditions should be avoided.

Temperature. Printers and scanners should be located in areas where temperature is controlled. Extremely high temperatures cause failure of electronic components. Printers and scanners generate heat during their normal operation. Laser printers have a fuser assembly that adds to the heat generated by other parts of the printer. An air-conditioned room is best suited for this equipment as it controls both temperature and humidity.

Cleanliness. Besides preventive maintenance that includes cleaning of internal parts of printers and scanners, the area around printers and scanners must be kept clean. Dust from paper particles around heavily used printers is a common scene in offices. Dust around the equipment eventually gathers around or gets inside the equipment and causes electronic or mechanical failures.

Supplies

Supplies of paper and other consumables must conform to guidelines given by the printer manufacturer. Consumable supplies mainly fall into the categories discussed next.

Paper. The quality of paper needs special attention in all types of printers. Low-quality paper ruins printer parts and causes paper jams. Paper jams further cause mechanical and electronic failures in printers.

Ink cartridges, ribbons, and toner cartridges. The ink cartridges, toner, and ribbons should be purchased directly from the printer vendor or from another supplier approved by the vendor. Refilled cartridges and ribbons do not last long. Poor quality ribbons sometimes cause printhead jams in dot matrix printers. Always stick to the specifications of the printer supplier. Refer to the documentation in case of confusion.

Spares. The spare parts used for printers and scanners should always be purchased directly from the vendor or from an approved supplier. You will need to provide information about the make and model number and the serial number of the printer or scanner when ordering spares.

Networks

This section is not covered in Exam 220-604.

This section covers a detailed study of fundamental aspects of networks. We will also review the basic concepts already covered in the A+ Essentials Study Guide.

Network Fundamentals

Before you install or configure network adapters and drivers and connect to a network, you must be familiar with different networking topologies, standards, protocols, services, and connectivity technologies. This section provides some basic information about networking fundamentals.

OSI model

The *Open System Interconnect (OSI)* defines the seven layers of a networking model. These layers define the standards for implementing networking functions and protocols. The functions of each layer are described in the following sections. Table 5-7 provides a summary of the functions of different layers of the OSI model.

Table 5-7. Summary of different layers of the OSI model

OSI layer	Functions
Physical (Layer 1)	Provides specifications for the physical topology of the network.
Data Link (Layer 2)	Handles functions such as media access method, hardware addressing, and error detection and correction. Consists of MAC and LLC sublayers.
Network (Layer 3)	Provides routing functions and discovery of the best network path to the destination network.
Transport (Layer 4)	Provides guaranteed delivery, segmentation of data, flow control, and error detection and correction.
Session (Layer 5)	Manages dialog (sessions) between applications running on remote computers. It sets up, regulates, and terminates the sessions.
Presentation (Layer 6)	Provides data format translation of data formats such as encryption/decryption, encoding/decoding, and compression/decompression.
Application (Layer 7)	Provides an interface for applications to access the network services.

Networking protocols

Networking protocols provide ways for computers to communicate with each other through the networking media. In this section, we will discuss the features of different networking protocols, as well as their advantages and limitations.

TCP/IP. The *Transmission Control Protocol/Internet Protocol (TCP/IP)* is a set of several protocols. It is the most widely used protocol suite in private networks as well as on the Internet. Unlike the AppleTalk and IPX/SPX protocols, TCP/IP is not proprietary to any organization but is a public protocol suite. Needless to say, it is a fully routable protocol. The routing functionality is provided by a number of routing protocols such as RIP and OSPF. The TCP/IP protocol suite is supported by all major network and desktop operating systems. Some of the well-known protocols and their functions are discussed later in this section.

The following are some of the main configuration settings on a typical computer:

IP address

An *IP address* is a unique address used to identify a computer or a host on the network. This address is made up of 32-bit numbers written in dotted decimal notation in the *w.x.y.z* format. Each eight bits are known as an *octet* or a *byte*. A part of the IP address is known as the *network address* or *network ID* and the rest of it is known as the *host address* or *host ID*. These parts are based on the class of IP addresses used on the network. All computers on a particular network must have the same number as the network address, while the host address must be unique on the entire network.

Subnet mask

Every IP address is accompanied by a subnet mask. It is used to help identify the part of the network where the host is located. Like the IP address, the subnet mask is a 32-bit binary number that distinguishes the network ID from the host ID.

Default gateway

A default gateway allows computers on a network segment to communicate with computers on another segment. The default gateway for all computers on a particular segment is the IP address of the router interface that is connected to the local segment. If a computer is not configured with the IP address of a default gateway, it cannot communicate with computers on a different network segment.

DNS address

The IP address of a DNS server is configured on TCP/IP hosts so that all name resolution queries are sent to the designated DNS server. Most network and desktop operating systems allow you to configure multiple DNS servers.

WINS address

The IP address of a WINS server is configured to resolve NetBIOS name resolution queries. As with the DNS address, you can configure more than one WINS server address on a TCP/IP host.

Static IP addressing

When static IP addressing is used, network administrators manually configure all TCP/IP settings on a computer. This method is useful only on very small networks.

Automatic IP Addressing

TCP/IP hosts can be configured to obtain IP address configuration automatically from a Dynamic Host Configuration Protocol (DHCP) server. This is the default configuration on most desktop and server operating systems.

Internet Packet Exchange/Sequenced Packet Exchange (IPX/SPX). IPX/SPX is a full protocol suite used in Novell NetWare networks. It is a fully routable protocol. Different protocols in this suite are listed in Table 5-8.

Table 5-8. IPX/SPX protocols

Protocol	Function
Service Advertising Protocol (SAP)	Allows systems to advertise services such as file and print services.
NetWare Core Protocol (NCP)	Allows client/server interactions such as file and print sharing.
Internet Packet Exchange (IPX)	Provides network addressing and routing services.
Sequenced Packet Exchange (SPX)	Provides connection-oriented services on top of the IPX protocol.
Routing Information Protocol (RIP)	The default routing protocol for IPX/SPX networks; based on distance vector routing algorithm.
NetWare Link Services Protocol (NLSP)	Provides routing services based on link state algorithm.

The servers and workstations use a 48-bit hexadecimal address that defaults to the MAC address of the network interface card. The node address is appended to the network address to create a unique node address in the internetwork. The following is an example of an IPX address:

```
0AC74E02:02254F89AE48
```

In a NetWare network environment, only the servers are assigned hostnames consisting of a maximum of 47 characters. NetWare clients do not have hostnames and use their IPX addresses instead. Logical NetWare networks are assigned 32-bit hexadecimal addresses.

NetBEUI/NetBIOS. NetBEUI stands for *NetBIOS Extended User Interface*. It is an old Microsoft networking protocol used in small networks. This protocol provides services at the transport and network layer of the OSI model. It is not a routable protocol and as such, cannot be used on large routed networks. It is easy to install and the fastest of all protocols covered in the A+ exam. The computers using the NetBEUI protocol use *Network Basic Input Output System (NetBIOS)* naming conventions. NetBIOS computer names consist of a maximum of 15 characters such as Server1 or Workstation1.

> Since the NetBIOS name resolution mainly depends on broadcasts, the NetBEUI protocol creates significant network traffic if there are a large number of computers on the network. This protocol is used only on nonrouted Microsoft networks.

Simple Mail Transfer Protocol (SMTP). SMTP is a connection-oriented application layer protocol that is used to transport messages between remote email servers. It uses TCP at the transport layer and hence guarantees delivery of data.

Internet Message Access Protocol 4 (IMAP4). Like POP3, IMAP4 is also used to retrieve email from mail servers. The advantage of using IMAP4 over POP3 is that it provides a secure authentication mechanism.

Internet Control Message Protocol (ICMP). ICMP works at the network layer to provide error checking and reporting functions. It is a connection-less protocol and uses IP for providing best-effort delivery. It is used in network management and maintenance systems. For example, PING is a troubleshooting utility that uses the ICMP protocol.

Address Resolution Protocol (ARP). ARP works at the network layer. It is used to resolve IP addresses to MAC addresses. Upper-layer protocols use ARP to correctly deliver data packets to the destination host. ARP maintains a mapping of IP addresses and MAC addresses in the system memory called the *ARP cache*. If the ARP cache does not have an entry for a requested IP address, it broadcasts the IP address on the local network to find out which host has the specified IP address.

HyperText Transfer Protocol (HTTP). HTTP is an application layer protocol that allows text, images, and multimedia to be downloaded from web sites. It is also a connection-oriented protocol that uses TCP at the transport layer. HTTP works with a *uniform resource locator (URL)* to connect to the desired web site. An example of a URL is *http://www.oreilly.com*.

HTTP Secure (HTTPS). HTTPS is the secure version of the HTTP protocol that allows servers and clients to be authenticated before the communication session starts. This protocol is also an application layer protocol and uses TCP at the transport layer. It is commonly used for online banking and other e-commerce functions. It uses a *secure socket layer (SSL)* to encrypt the network traffic between the web server and the web client. A web site using SSL has a URL starting with *https://*.

Secure Socket Layer (SSL). SSL is an encryption protocol popularly used for Internet-based transactions such as online banking. This protocol is based on public key encryption mechanisms. Transport Layer Security (TLS) is the successor of SSL but can be scaled down to SSL 3.0 mode for backward-compatibility. SSL provides end-to-end security for Internet communications by using encryption. In typical implementations, only the server component is required to use public keys for authentication. For end-to-end security, a Public Key Infrastructure (PKI) is required. Both the server and the client must be SSL-enabled to communicate over a secure channel.

Telnet. Telnet is an application layer protocol that allows connections to remote hosts. Administrators use this protocol to connect remotely to network devices and run commands in order to configure or maintain them. Telnet is also a connection-oriented protocol and uses TCP at the transport layer.

File Transfer Protocol (FTP). FTP works at the application layer to provide file transfers between remote computers. FTP uses TCP as its transport protocol. FTP is a client/server application that authenticates users before allowing access to servers that host the FTP service. Most FTP servers allow anonymous logons that enable multiple users to connect to the server and download files. FTP is commonly used on the Internet for file downloads. One of the major limitations of the FTP protocol is security. The authentication method uses clear text usernames and passwords, which is a serious security concern. FTP uses several commands for file transfers as listed in Table 5-9.

Table 5-9. FTP commands

FTP command	Description
ascii	Allows file transfers in ASCII mode.
binary	Allows file transfers in binary mode.
cd	Used to change the working directory on the remote computer.
get	Used to download a single file from the remote computer.
ls	Used to list files on the remote computer.
mget	Used to download multiple files from the remote computer.
mput	Used to upload multiple files on the remote computer.
put	Used to upload a single file on the remote computer.

DNS. DNS stands for Domain Name System. The DNS service is used to translate fully qualified domain names (FQDN) to their respective IP addresses. Large corporate networks and all hosts on the Internet use FQDN notation to identify computers on the network. A fully qualified domain name can consist of a maximum of 63 characters including the dots. An example of a fully qualified domain name is *www.us.books.oreilly.com*.

DNS servers on a network run the DNS service and are responsible for resolving DNS queries for their clients. They can do it either by themselves or by having the queries resolved though referring to another DNS server. DNS clients are configured to use one or more DNS servers when configuring their TCP/IP properties.

Windows Internet Naming System (WINS). A WINS server is used to translate NetBIOS computer names to IP addresses. NetBIOS names consist of a maximum of 15 characters. These servers are used only on Windows networks. The WINS server maintains a mapping of NetBIOS names to IP addresses. When a Windows client needs to resolve a computer name to its IP address, it sends a name resolution query to the WINS server. This helps limit the amount of broadcast traffic generated by a broadcast method of name resolution. Windows clients can be configured to use one or more WINS servers.

Connectivity technologies

Network connectivity is achieved using a number of technologies. These technologies are different for local area connections, wide area connections, and wireless connections. This section discusses some of the commonly used connectivity technologies.

LAN technologies

Ethernet networking and cabling technologies are defined in IEEE 802.3 standards. There are several variations in this standard—depending on speed, length, topology, and cabling—used in implementing networks. The following sections provide a brief summary of the standards tested on the A+ exam.

10 Mbps Ethernet. The 10 Mbps standards include 10Base2, 10BaseT, and 10BaseFL. All of these standards define a maximum data transfer speed of 10 Mbps. It is unlikely that you will encounter any 10 Mbps networks in your career. Table 5-10 gives a summary of 10 Mbps networking standards.

Table 5-10. Summary of 10 Mbps networking standards

Standard	Cable	Length of segment	Network topology	Connector
10Base2	Thin Coaxial	185 Meters	Bus	BNC
10BaseT	UTP CAT 3, 4, or 5	100 Meters	Star	RJ-45
10BaseFL	Fiber Optic	2000 Meters	Star	SC or ST

100 Mbps Ethernet. Most of the modern networks support 100 Mbps speed, which provides better bandwidth for demanding applications. Table 5-11 gives a summary of 100 Mbps networking standards.

Table 5-11. Summary of 100 Mbps networking standards

Standard	Cable	Length of segment	Network topology	Connector
100BaseTX	CAT 5	100 Meters	Star	RJ-45
100BaseT4	4 Pairs of CAT 3, 4, or 5	100 Meters	Star	RJ-45
100BaseFX	MM Fiber or SM Fiber	MM Fiber-412 Meters SM Fiber-10,000 Meters	Star	SC or ST

1000 Mbps Ethernet. 1000 Mbps (1 Gigabit) Ethernet network is also known as a *Gigabit Ethernet*. This uses either copper or fiber optic cabling. These networks are implemented mainly as a backbone for large networks. Table 5-12 offers a summary of Gigabit Ethernet networking standards.

Table 5-12. *Summary of Gigabit Ethernet networking standards*

Standard	Cable	Length of segment
1000BaseLX	MM Fiber Optic or SM Fiber Optic	MM Fiber-550 Meters SM Fiber-5,000 Meters
1000BaseSX	MM Fiber –50 Micron	550 Meters
1000BaseCX	STP	25 meters
1000BaseT	UTP	75 Meters

WAN technologies

A WAN consists of two or more interconnected connect LANs. Usually a third party, a telephone company, or an ISP is involved in providing a connectivity solution to the organization that needs to set up a WAN. A WAN can be set up using a dial-up telephone line for low-bandwidth requirements or may be set up using a high-bandwidth dedicated line. It is also possible to tunnel the WAN connection through the Internet. The following sections describe various technologies used for WAN connectivity.

Internet Service Provider (ISP). The ISP refers to an organization that provides Internet access or WAN facilities. ISPs provide low-cost Internet connectivity to home users via dial-up, cable modem, ISDN (BRI), or Digital Subscriber Lines (DSLs). For large organizations that require high speed and bandwidth, the connectivity is provided through Gigabit Ethernet, ATM, ISDN (PRI), T-carriers, or Sonet. These technologies are covered in greater detail in Chapter 8.

On the Internet, there is actually a hierarchy of lower- and higher-level ISPs. Just as customers connect to an ISP, the ISPs themselves are connected to their upstream ISPs. Several ISPs are usually engaged in *peering*, in which all ISPs interconnect with each other at a point known as the *Internet Exchange (IX)*. This is done to allow routing of data to other networks. ISPs who do not have upstream ISPs are called *Tier 1 ISPs*. These sit at the top of the Internet hierarchy.

Dial-up. Dial-up using the Plain Old Telephone Service (POTS) and Public Switched Telephone Network (PSTN) is the traditional method of connecting to remote access servers or the Internet. These are dial-up methods, and the user has to dial the telephone number of the ISP to authenticate and get Internet connectivity. The telephone line is connected to a modem that is further connected to a serial or USB port on the user's computer. Most computers have built-in modems that can be directly connected to the telephone line.

POTS/PSTN provide a maximum data transfer speed of 56 Kbps. There are several ISPs that offer dial-up Internet access. Most ISPs provide added features such as free email accounts and access to newsgroups, and some even offer hosting of a small web site for the user.

Digital Subscriber Line (DSL). DSL is a family of technologies that uses ordinary analog telephone lines to provide digital data transmissions. It uses different frequencies for voice and data signals; the same telephone line can simultaneously be used for phone and data transfer. It is commonly used for high-speed Internet access from homes and offices. Different DSL technologies are collectively noted as *xDSL* and support data transfer speeds from 128 Kbps to 24 Mbps, as discussed in the following list:

Asymmetrical DSL (ADSL)
: ADSL is the most common of all types of DSL variations. The download speed of data is faster than upload speeds. It uses one channel for analog voice (telephone) transmissions, a second channel for data uploads, and a third channel for data downloads.

Symmetrical DSL (SDSL)
: SDSL supports equal speeds for both data uploads and downloads. It cannot be used for voice transmissions and hence is suitable only for Internet access at offices.

ISDN DSL (IDSL)
: IDSL is a variation of symmetric DSL. It does not support analog voice transmissions and is used only in those environments where ADSL and SDSL are not available.

Rate Adaptive DSL (RADSL)
: RADSL is a variation of asymmetric DSL that can vary the transfer speeds depending on line conditions. It supports both data and voice transmissions.

Table 5-13 provides a summary of different DSL variations and their data transfer speeds.

Table 5-13. DSL variations

DSL variation	Download speed	Upload speed	Phone usage
ADSL	8 Mbps	1 Mbps	Yes
SDSL	1.5 Mbps	1.5 Mbps	No
IDSL	144 Kbps	144 Kbps	No
RADSL	7 Mbps	1 Mbps	Yes

Broadband. *Broadband Internet Access*, or simply *Broadband*, is provided by the cable companies that provide digital cable services. It is a reliable and efficient means of Internet access. The coaxial cable connects to a cable modem that further connects to the computer or other network device (hub, switch, or router) using a UTP cable. The cable connection can be shared among several computers in a home or in small offices using low-cost wired or wireless routers.

With a cable modem, the user does not have to dial the ISP, and the connection is always there. This might pose a security risk for computers that are used for critical purposes. Most cable modems support bandwidths from 1.5 to 3 Mbps for the Internet access. The cable modem usually supports up to 10 Mbps data speeds for the LAN connection. The actual Internet access speed depends on the utilization of the shared cable signals in the area.

Satellite. In areas where DSL or cable is not available (such as rural areas), satellite is the only option for high-speed WAN connectivity. The signals travel from the ISP to a satellite and then from the satellite to the user. The data transmission speeds vary from 512 Kbps (upload) to 2 Mbps (download). Major drawbacks of satellite Internet access are that it is expensive, and it offers low transfer speeds as compared to DSL and cable.

Satellite Internet access suffers from *propagation delays* or *latency* problems. Latency refers to the time taken for the signal to travel from the ISP to the satellite, located in the geostationary orbit at 35,000 Km above earth, and then back to the user. Latency also depends on atmospheric conditions.

ISDN. ISDN is a *packet switched* network that allows transmission of data and voice over telephone lines. This results in better quality and higher data transfer speeds than regular dial-up connections. ISDN requires dedicated telephone lines or *leased lines* and hence is expensive. When the two ends need to communicate, one of them dials the specified ISDN number and the connection is set up. When the communication between the two nodes is over, the user hangs up and the ISDN line becomes free. Computers using the ISDN line need a special network interface known as the *ISDN adapter*, or *terminal adapter*.

ISDN communications use two types of channels: a *bearer* channel (*B channel*) used for data (or voice), and a *delta* channel (*D channel*) used for control signals. The two main implementations of ISDN are as follows:

Basic Rate Interface (BRI)
BRI ISDN uses 2 B channels of 64 Kbps each for data/voice, and a D channel of 16 Kbps. The total data transfer speed of BRI ISDN using two B channels is 128 Kbps. The two B channels can also be used separately with 64 Kbps speed.

Primary Rate Interface (PRI)
PRI ISDN uses 23 B channels of 64 Kbps each for data/voice, and a D channel of 64 Kbps. The total data transfer speed of PRI ISDN is up to 1.544 Mbps. The PRI ISDN is usually carried over dedicated (leased) T1 lines.

Table 5-14 summarizes the two ISDN implementations.

Table 5-14. BRI and PRI ISDN connections

Characteristic	BRI	PRI
Carrier Line	ISDN	T1
Channels	2B+1D	23B+1D
Total Speed	128 Kbps	1.544 Mbps

Wireless. Wireless networks rely on radio frequencies to communicate instead of the network cabling used for normal computer networks. Radio frequencies create electromagnetic (EM) fields, which become the medium to transfer signals from one computer to another. As you go away from the hub, or from the main equipment generating the radio frequency of the wireless network, the strength of the EM field reduces and the signal becomes weak.

Wireless networks defined in IEEE 802.11 standards use radio frequencies with *spread spectrum* technology. The two spread spectrum technologies are as follows:

Frequency-hopping spread spectrum (FHSS)
: FHSS is the method of transmitting RF signals by rapidly switching frequencies according to a pseudorandom pattern, which is known to both the sender and the receiver. FHSS uses a large range of frequency (83.5 MHz) and is highly resistant to noise and interference.

Direct-sequence spread spectrum (DSSS)
: DSSS is a modulation technique used by wireless networks that uses a wide band of frequency. It divides the signal into smaller parts and transmits them simultaneously on as many frequencies as possible. DSSS is faster than FHSS and ensures data protection. It utilizes a frequency range from 2.4 to 2.4835 GHz and is used in 802.11b networks.

The most popular of the IEEE 802.11 wireless network standards are 802.11b, 802.11a, and 802.11g. Table 5-15 gives a brief comparison of the characteristics of different 802.11 standards.

Table 5-15. Comparison of 802.11 standards

802.11 standard	Operating frequency	Maximum speed
802.11	2.4 GHz	1 or 2 Mbps
802.11b	2.4 GHz	11 Mbps
802.11a	5 GHz	54 Mbps
802.11g	2.4 GHz	54 Mbps

Infrared (IrDA)

Infrared technology employs electromagnetic radiations using wavelengths that are longer than the visible light but shorter than radio frequency. Common examples of Infrared devices are the remote controls used in TVs and audio systems. The following are some of the key characteristics of IrDA wireless communication technology:

- It provides point-to-point wireless communications using direct line of sight.
- Infrared waves cannot penetrate through walls.
- It supports data transfer speeds ranging from 10 to 16 Mbps.
- Infrared devices consume very low power.
- Infrared frequencies do not interfere with radio frequencies.
- It provides a secure wireless medium due to the short distance (usually 3 to 12 feet).

Bluetooth. Bluetooth wireless networking technology provides short-range communications between two or more devices. It is a low-cost networking solution widely used in telephones, entertainment systems, and computers. It is designed to overcome the limitations of IrDA technology. Some of the key characteristics of Bluetooth-based wireless communications are listed next.

- It supports transmission speeds from 1 (Bluetooth 1.0) to 3 Mbps (Bluetooth 2.0) over the unlicensed frequency range of 2.4 GHz.
- The devices must be within a short range of less than 10 meters.
- It offers high resistance to electromagnetic interferences.
- Unlike the Infrared signals, it does not require direct line of sight.
- Bluetooth devices consume very low power.
- Two or more Bluetooth computers form an ad-hoc wireless network.

Cellular. A *cellular network* is actually a radio network made up of cells that operate at radio frequencies. Each of the cells is served by a base station or a cell site and covers a predefined area. Cellular networks use *Frequency Division Multiple Access (FDMA)* and *Code Division Multiple Access (CDMA)* methods to distinguish between signals transmitted by different cells. With the FDMA technology, each neighboring cell uses a different frequency. This helps reuse a particular frequency in distant cells and thereby increases the coverage of the cellular network.

The most common example of a cellular network is the mobile (wireless) network. Large geographical areas are divided into small cells, with each cell being served by a cell site or base station. Mobile phones within a cell transmit and receive voice and text messages through the base station.

It is possible to connect a computer through a mobile phone. The computer dials the telephone number of the ISP through a mobile phone to establish Internet connectivity.

VoIP. VoIP stands for *Voice over Internet Protocol*. Other popular names for this technology are Internet telephony, IP Telephony, and Broadband Phone. VoIP is a mechanism to transmit voice signals over Internet Protocol (IP). The special protocols used to carry voice signals over an IP network are called VoIP protocols. One of the major advantages of VoIP is the ability of a user to make telephone calls from anywhere in the world. VoIP allows VoIP phones to integrate with other Internet services (such as video conversations and file exchanges) simultaneously with verbal conversations. Since the VoIP service is heavily dependent on availability and reliability of the Internet connection, this technology is still in the development process.

Installing, Configuring, and Optimizing Networks

This section covers fundamental concepts of installing and configuring network adapters and drivers as well as configuring their properties on a Windows desktop. It also discusses some troubleshooting utilities and diagnostic procedures to resolve common network connectivity problems.

Establishing network connectivity

The first step in establishing network connectivity for a computer is to obtain a network connection from the network administrator. The network administrator provides an available port on the network hub or switch where the new desktop can be connected. From the desktop technician, the connection is available in the form of a UTP or STP network cable attached to a male RJ-45 connector. This cable is attached to the female RJ-45 socket on the network adapter installed on the desktop.

Installing and configuring network adapters. Most new desktops come equipped with built-in network adapters. In newer computers, the network interface is integrated with the motherboard. But you might have to install, replace, or upgrade network adapters in some old desktops. For example, you might be asked to replace a 10 Mbps network adapter with a 10/100 Mbps fast network adapter. When installing a network adapter, you will need to make sure of the following:

- The adapter is compatible with the existing computer hardware.
- The adapter driver is meant for the operating system installed on the computer.
- The operating system supports the adapter driver.
- Whether the adapter is PnP or not.
- The adapter driver is available for installation if it is not automatically installed by the operating system.

Most new network adapters are PnP. PnP adapters are automatically detected and configured by most operating systems. This configuration includes setting aside system resources such as IRQ, I/O, and DMA for the adapter as well as installation of an appropriate driver.

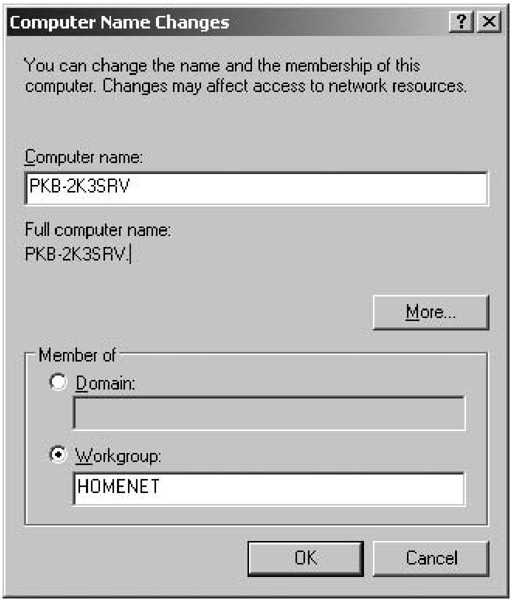
In case the network adapter is not PnP, you will be required to install the network driver manually (you will need to obtain the driver, which may be available either on the CD-ROM accompanying the network adapter or from the vendor's web site). On Windows XP and Windows 2000 Professional computers, you can use the Add/Remove Hardware applet in the Control Panel to add the network adapter. The Device Manager snap-in can be used to install the network adapter device driver.

Configuring client and network options. Installing or configuring a desktop operating system on a home computer is straightforward. Most technicians leave the default configuration options, which are good for most users. The scene is different when working in a network environment. You will need to configure networking options on the desktop, which will enable the user to use shared resources on the network. These configuration tasks include joining a workgroup or a domain in a Windows environment or an NDS tree in a NetWare environment, and then configuring file and folder permissions for other users.

Joining a Windows workgroup or domain

On Windows XP and Windows 2000 Professional computers, you can join a workgroup or a domain during or after the installation of the operating system. In case the computer will join an existing workgroup, you will need the name of the workgroup or you can create a new one. The steps that are shown next explain how you can change the network settings on Windows XP or Windows 2000 Professional computers.

1. Open the Control Panel from the Start menu.
2. Double-click the System icon to open System Properties.
3. Click the Computer Name Tab. The current settings for computer name and workgroup/domain membership are displayed.
4. Click the Change button.
5. Click the radio button for Domain or Workgroup in the Member Of section, as required.
6. Enter the name of an existing Domain or the Workgroup in the Computer Name Changes dialog box, as shown in Figure 5-15.
7. Click OK twice to close all dialog boxes. Close the Control Panel.



Computer Name Changes

You can change the name and the membership of this computer. Changes may affect access to network resources.

Computer name: PKB-2K3SRV

Full computer name: PKB-2K3SRV.

Member of

○ Domain:

● Workgroup: HOMENET

Figure 5-15. Joining a workgroup or domain

In case the computer will join an existing domain, you will need the following information from the domain administrator:

- The DNS name of the domain. This is usually in the format *mydomain.com*.
- A computer account in the domain. An administrator should create this account before you start the installation process. If you have been given the Add Workstations to Domain right, you can create the computer account yourself during installation.
- An available domain controller and a DNS server to validate your credentials during installation.

On NetWare platforms, you will need Supervisor rights in the NDS tree that you are trying to join. The following information is required when configuring a desktop to join an NDS Tree:

- Username and password
- Internal network number
- Network number
- The directory context
- The name of the directory tree

The directory context and tree names can sometimes be too complex for a user to remember. To get around this problem, it is a common practice to configure the user's desktop with context and tree names.

Sharing network resources

The main purpose of creating networks is to share resources. File and folder sharing is one of the fundamental tasks of a network technician. In a workgroup environment, each user is responsible for sharing files and folders on her desktop and to configure appropriate permissions for other network users. In large networks such as Windows domain or NetWare NDS tree environments, these actions are performed by administrators and supervisors respectively. In the following sections, we will look at some basic steps required to configure file and folder permissions.

Configuring permissions. File- and folder-level permissions are managed in Windows XP and Windows 2000 Professional computers using the filesystem. Disk partitions formatted with NTFS filesystem support both folder- and file-level permissions. FAT and FAT32 filesystems support only folder-level permissions. Tables 5-16 and 5-17 list standard NTFS file and folder permissions respectively.

Table 5-16. NTFS file permissions

Permission	Description
Read	Read the file and its attributes, permissions, and ownership.
Read and Execute	Run the file, plus access granted by the Read permission.
Write	Overwrite the file, change file attributes, and view permissions and ownership.
Modify	Modify and delete the file, plus the access granted by the Write and the Read and Execute permissions.
Full Control	All actions that are permitted by other NTFS permissions, plus the Change and the Take Ownership permissions.

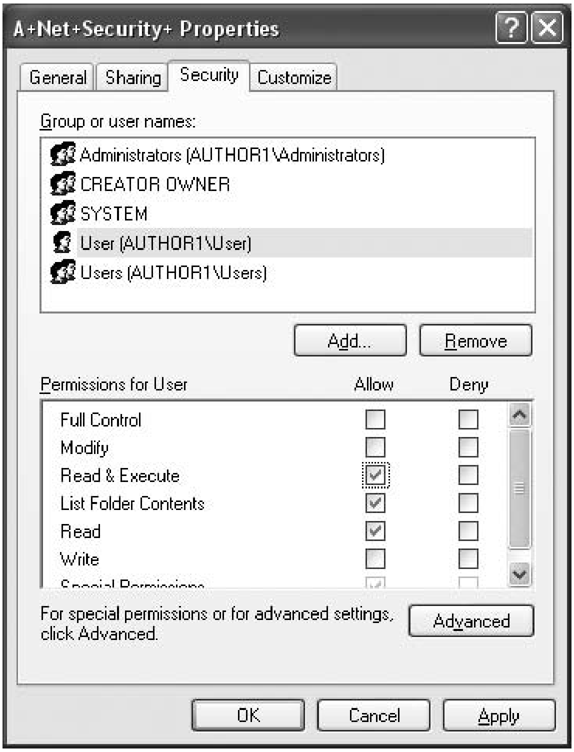
Table 5-17. NTFS folder permissions

Permission	Description
Read	View files and subfolders in the folder and its attributes and permissions.
List Folder Contents	View the names of files and subfolders.
Read and Execute	Move through folders and subfolders and other permissions are granted by Read and List Folder Contents.

Table 5-17. NTFS folder permissions (continued)

Permission	Description
Write	Create new files and subfolders within the folder and change folder attributes.
Modify	Delete the folder, plus other permissions granted by the Read and Execute and the Write permissions.
Full Control	Change Permissions, delete files and subfolders, and take ownership. Includes all other NTFS folder permissions.

The preceding permissions can be set to Allow or Deny any user or group. By default, administrators and owners of the file or folder get Full Control permissions. Permissions can be assigned to users and groups from the Security tab of the file or folder properties window, as shown in Figure 5-16.



A+Net+Security+ Properties

Group or user names:

- Administrators (AUTHOR1\Administrators)
- CREATOR OWNER
- SYSTEM
- User (AUTHOR1\User)
- Users (AUTHOR1\Users)

Permissions for User	Allow	Deny
Full Control	□	□
Modify	□	□
Read & Execute	☑	□
List Folder Contents	☑	□
Read	☑	□
Write	□	□
Special Permissions	☑	□

For special permissions or for advanced settings, click Advanced.

Figure 5-16. NTFS permissions

The following steps explain how NTFS permissions can be configured for a user or a group:

1. Right-click a folder and select Properties from the menu.
2. Click the Security tab in the Properties dialog box.
3. Click the Add button to add a user or group.

4. Select a user or group from the Select Users and Groups dialog box. Click OK.
5. Click the Allow or Deny checkbox for appropriate permissions. Click OK.

NetWare file permissions. NetWare filesystems work by providing users access to hard disk partitions, known as *volumes*. Clients can map their disk drives to server disk volumes on which they have appropriate rights. File permissions on NetWare servers are assigned through the use of a complex set of rights, as given in the following list:

Supervisor
Includes all rights to the file. This is equivalent to the Full Control permission in Windows.

Read
Allows users to read the file.

Write
Allows users to write to the file.

Create
Allows users to create a new file.

Erase:
Allows users to erase (delete) the file.

Modify
Allows users to modify the file contents.

Filescan
Allows users to view a file.

Access Control
Allows the user to change permissions on the file.

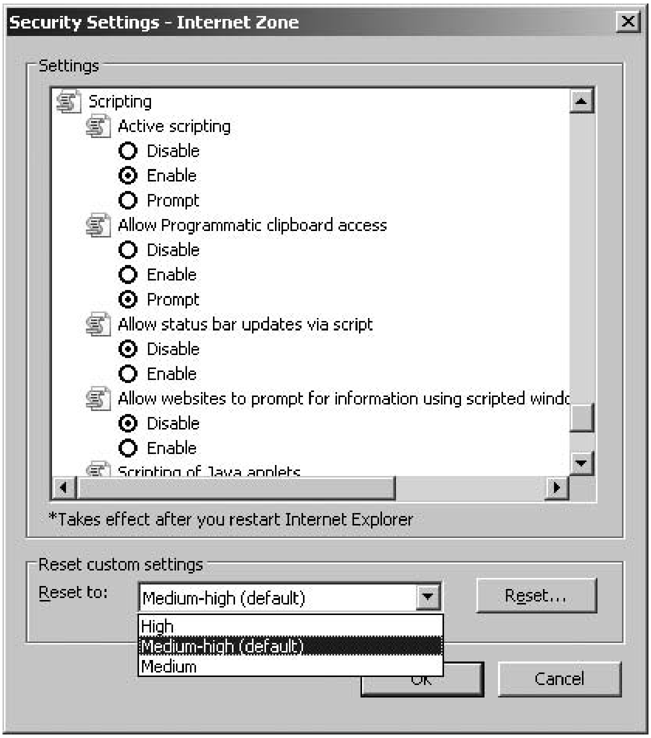
Installing and configuring network browsers

As a computer support technician, you will frequently be tasked with configuring Internet settings on desktop computers. This section covers configuration of network browsers, including enabling and disabling of scripts, configuring browsers to use a proxy server, and configuring security settings. Fundamental knowledge of these settings will help you perform these tasks correctly and conveniently.

Configuring script settings. JavaScript, ActiveX controls, and cookies are client-side components of Internet services and are often overlooked. In order to secure web browsers from potential security vulnerabilities, these components must be properly configured. They are usually downloaded from the web server and run on the client computer. In case of a problem, the client computer is affected instead of the web server. Script support can be configured on Microsoft Internet Explorer on a Windows computer as shown in the following steps:

1. Open Internet Explorer.
2. Click Tools → Internet Options.

3. Click the Security tab.
4. Click the Custom Level tab.
5. Scroll down to the Scripting section as shown in Figure 5-17.
6. Configure the scripting options as required.
7. Click OK to close the dialog box.



Security Settings - Internet Zone

Settings

Scripting

Active scripting
- ○ Disable
- ● Enable
- ○ Prompt

Allow Programmatic clipboard access
- ○ Disable
- ○ Enable
- ● Prompt

Allow status bar updates via script
- ● Disable
- ○ Enable

Allow websites to prompt for information using scripted windc
- ● Disable
- ○ Enable

Scripting of Java applets

*Takes effect after you restart Internet Explorer

Reset custom settings

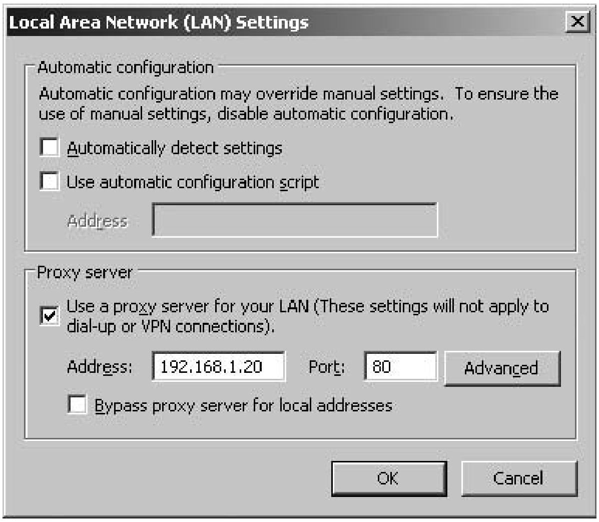
Reset to: Medium-high (default)
- High
- Medium-high (default)
- Medium

Figure 5-17. Configuring script settings in Internet Explorer

Configuring proxy settings. Internet browsers can be configured to connect to the Internet either directly or through a proxy server. A *proxy server* enables administrators to share a single Internet connection among multiple network users. It provides better performance by means of caching frequently visited web pages. Administrators can configure advanced security as well as track user activities. Microsoft's Internet Explorer can be configured to use a proxy server as given in the following steps:

1. Open Internet Explorer.
2. Click Tools → Internet Options.
3. Click the Connections tab.
4. Click the LAN settings tab to open the dialog box shown in Figure 5-18.
5. Click the checkbox under Proxy Settings.

6. Enter the IP address of the proxy server in the Address box and enter `80` in the Port box.
7. Click OK to close the dialog box.



Local Area Network (LAN) Settings

Automatic configuration

Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

☐ Automatically detect settings

☐ Use automatic configuration script

Address

Proxy server

☑ Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).

Address: 192.168.1.20 Port: 80

☐ Bypass proxy server for local addresses

Figure 5-18. Proxy server settings for Internet Explorer

Configuring security settings. Security settings for Internet Explorer can be configured as shown in the following steps:

1. Open Internet Explorer.
2. Click Tools → Internet Options.
3. Click the Security tab.
4. Choose a Security Zone from the options: Internet, Local Intranet, Trusted Sites, and Restricted Sites.
5. For each zone, add or remove web sites using the Sites button, as required.
6. Use the slider bar in the bottom half of the window to set the security level for the selected zone.
7. You can use the Custom Level button to configure advanced security settings or click the Default Level to apply preconfigured settings.
8. Click OK to close the Internet Options dialog box.

Troubleshooting Network Problems

In addition to installation, configuration, and upgrading computer-related hardware and software, troubleshooting network problems is an on-going task for most support technicians. This includes attending to regular support calls, problems caused by equipment failure, improper configuration of devices, user mistakes, and lack of preventive maintenance. This section covers identification and resolution of network problems using common diagnostic tools and utilities.

Troubleshooting tools

Most network equipment, operating systems, and software applications come with built-in diagnostic tools to help technicians and administrators diagnose and resolve problems. As far as networks are concerned, there are some diagnostic tools that are available on most operating systems as well as on network equipment. This section covers troubleshooting network problems using some of these common tools and utilities.

ipconfig. *ipconfig* is a command-line utility used on Microsoft Windows operating systems to diagnose TCP/IP configuration problems. It can be used to display, release, and renew the IP address configuration of Windows computers. In Windows 2000, Windows XP, and Windows Server 2003 operating systems, this utility can also release and renew a computer's IP configuration with the domain name system (DNS) servers.

The *ipconfig* utility is commonly used with the */all* parameter to display complete TCP/IP configuration of all network adapters installed on a computer. You can also select a particular adapter to view its configuration. It can reveal one or more configuration problems, and an administrator can take necessary corrective action to resolve the problem.

Table 5-18 lists the parameters and their functions available with the *ipconfig* command.

Table 5-18. ipconfig command parameters

Parameter	Function
/all	Displays the TCP/IP configuration of all network adapters on the local host.
/release	Used to release the IP address of specified adapter.
/renew	Used to renew the IP address of specified adapter.

On Windows XP, Windows 2000, and Windows Server 2003 operating systems, the *ipconfig* utility also includes the following parameters:

/flushdns
Used to clear the DNS cache on the local host.

/displaydns
Used to display the entries in the local DNS cache.

/registerdns
Used to register the name of the local host with the DNS server.

When troubleshooting a TCP/IP problem on a particular computer, you may verify the configuration parameters using the *ipconfig /all* command. For example, if the output shows the IP address and the subnet mask as 0.0.0.0, you can be sure that the TCP/IP configuration of the computer is invalid. In this case, you can use the following two commands to renew the TCP/IP configuration with a DHCP server:

```
C:\>ipconfig /release
C:\>ipconfig /renew
```

If a computer is not able to connect to any remote hosts, the default gateway address should be checked in the output of the *ipconfig* command. The default gateway enables a computer to connect to other hosts located in other network segments. This address is usually the IP address of a router interface connected to the local network segment. Similarly, on a Windows XP/2000/2003 system, if the host is unable to resolve DNS names, the *ipconfig /flushdns* command can be used to clear the DNS cache.

> On Unix/Linux and MAC OS operating systems, you can use the *ifconfig* command to display the TCP/IP configuration of a host. This command is an equivalent of the *ipconfig* command on Windows operating systems. Unlike the limited features of the *ipconfig*, this command has much more advanced diagnostic features. Typing `ifconfig help` at a Unix host command prompt gets you all the parameters and other information about how this command could be used. Similarly, you can use the *winipcfg* command on older Windows desktop operating systems, such as Windows 98 and Windows Me.

ping. *ping* is a cross-platform command-line utility used to troubleshoot end-to-end connectivity problems on network hosts. It sends ICMP echo requests to the destination host and waits for a response. This utility is a part of the TCP/IP protocol suite and is installed by default on all TCP/IP devices. *ping* can quickly determine whether the host is connected or not, and how long it takes for the request to make the round trip. You can use the *ping* utility with the IP address of the remote host or with its IP address.

Besides testing connectivity, the *ping* command can also be used to test whether the name resolution is working or not. For example, if you are able to ping a remote host successfully using its IP address but not using its hostname, there could be a problem with the name resolution.

When you use the *ping* utility for diagnosing network problems, you must be able to interpret the output correctly in order to find out the exact cause of the problem. The following are some of the common output messages:

Request Timed Out

This indicates that the echo request message did not get any response from the destination host.

Destination Host Unreachable

This appears in the ping output when the host you are trying to ping is not found.

Unknown Host

This means that the specified hostname could not be resolved.

TTL Expired

This means that the echo message sent to the destination could not get a response, and the TTL value has reduced to 0.

tracert. The *tracert* or *traceroute* utility is used to trace the route from one host to another in a TCP/IP network. All major operating systems and network devices support this utility in one form or another. The output format of this utility differs from one operating system to the next. It uses the *Internet Control Message Protocol (ICMP)* echo packets to trace the route to a specific destination host and reports back the results at every hop on the path.

The syntax of the *traceroute* command in different operating systems is as follows:

Windows

```
tracert <Hostname> or tracert <IPAddress>
```

Unix/Linux and MAC OS

```
traceroute <Hostname> or traceroute <IPAddress>
```

NetWare

```
iptrace
```

The *traceroute* utility provides very useful information when diagnosing connectivity problems. It provides the IP address of every router (hop) that it passes through and reports the time it takes from one hop to another. This is helpful in diagnosing the exact location of the network bottleneck or congestion.

It is easy to interpret the results of the *tracert* utility. The first column shows the *hop number*, which is the network device that responds to the ICMP echo request. The next three columns show the roundtrip time in milliseconds that the packet takes. The next column shows the hostname and the IP address of the responding device.

In some situations, the network is congested. This is shown as "Request Timed Out" in the output. This may be due to a misconfigured router at the seventh hop. But the trace continues to the next hop until it reaches the destination. Once the problem device is identified, you may use some other utility such as *ping* to pinpoint the source of the problem.

nslookup. The *nslookup* utility is used to diagnose problems related to the domain name system (DNS) services. In other words, it is used to resolve name resolution problems. This utility can be used to perform name resolution queries against specified DNS servers or display information about currently configured DNS servers on a local host.

The *nslookup* utility can be executed in either noninteractive mode or interactive mode.

Noninteractive mode

This is useful when you need to run the command with one or two pieces of information. For example, you can use the following command to resolve a specific hostname:

```
nslookup hostname
```

Interactive mode

In this mode, you just type `nslookup` and press the Enter key. The command will display the information about the current hostname and the IP address of the configured DNS server, and it also displays a prompt. You can then type other *nslookup* subcommands on this prompt. To exit the interactive mode, type Exit and press the Enter key. On Windows systems, you can type ? at the interactive prompt to get more information on the syntax and usage of available subcommands.

In order to resolve a hostname using a specific DNS server, you can use the following command instead:

```
C:\ >nslookup www.oreilly.com 192.168.1.5
```

You can also use *nslookup* to resolve IP addresses to hostnames as shown in the following example.

```
C:\ >nslookup 208.201.239.36
```

The commands and parameters used in the *nslookup* utility are case-sensitive and must be typed in lowercase characters.

Cable-testing devices

Cable-testing devices, or cable testers, are used to test whether the cable is working properly. Several different types of methods exist for testing cables. A small multimeter is perhaps the simplest tool for testing continuity in cables. Cable continuity verifies that wires are not broken. Copper-based media testers rely on electrical signals to test the cables. If the electrical current passes through the cable without a break, the cable is considered to be good. Electrical signals are very helpful in testing the continuity of a coaxial cable. For a UTP cable, you will need to test continuity for each individual wire.

Optical Time Domain Reflectometer. A special tester called the *Optical Time Domain Reflectometer (OTDR)* is used to pinpoint the correct location of the break-in fiber optical cables. OTDR is an expensive instrument and is mostly used by professional fiber optic network installers. Fiber optic cables are tested using optical cable testers. These testers use light signals to test the cable instead of using electrical signals. Optical cables are prone to breakages that can prevent light signals from reaching the other end. A break in an optical cable is easy to determine but very hard to find.

Tone generators and tone locators. *Tone generators* and *tone locators* are devices that help find cable faults by means of audio signals. This device generates an audio tone (beep) and sends it over the cable. A tone locator is attached to the other end of the cable to check whether the tone reaches there. Using a tone generator is a time-consuming process, and it takes two persons to use the device. Testing cables with a tone generator is also known as the *fox and hound* method. The tone generator must be attached to each individual wire separately.

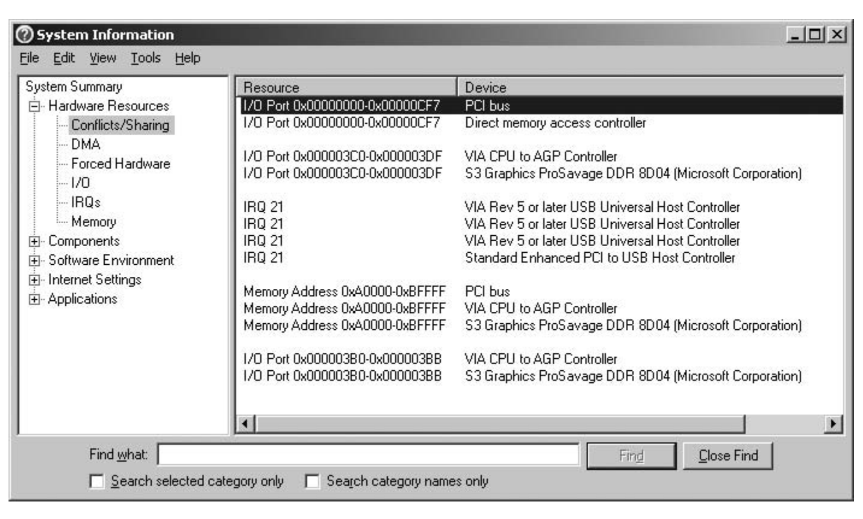
Loopback connectors. Loopback connectors or adapters are hardware devices that work with special test software to verify the functionality of a network port such as RJ-45, and serial and parallel ports. These are small connectors that are wired so that the outgoing transmission pins are connected back to the incoming receiving pins. The test software accompanying the loopback connectors sends and receives data signals to verify that the port being tested is correctly transmitting and receiving data.

Configuration problems

Network problems often result due to improper configuration of network adapters, drivers, and protocols. When all of these are correctly configured, the problem may further be attributed to permissions assigned to shared network resources. Improperly configured port and protocol settings on security devices such as firewalls or proxy servers may also cause problems related to access of external networks such as the Internet. This section discusses some common issues that may cause network problems.

Network interface and driver. Every network adapter comes with a software component that provides an interface for the operating system and applications to interact with the network. While most network adapters are PnP devices, older network adapters must be correctly configured in order to enable them to interact with the system and the network. Like other devices on the computer, network adapters also use system resources such as Interrupt Request (IRQ), Input/Output Address (I/O Address), and Direct Memory Access (DMA). Older network adapters had to be manually configured to use these resources. It was not uncommon to see a large number of problems occurring due to resource conflicts. When two or more devices try to use the same resource, it results in system problems with one or both devices not able to function as expected.

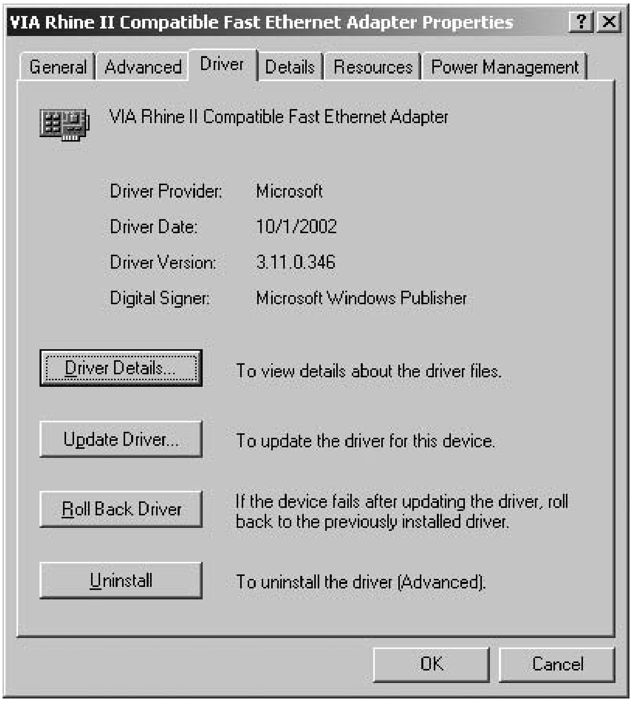
If you are tasked with resolving a network problem in a system that has an old network adapter installed on it, make sure that it is correctly configured to use only free system resources. In most new computers, the PnP functionality takes care of dynamic allocation and sharing of system resources. When in doubt, you may verify resource conflicts in a system by using some built-in utility. For example, on Windows XP computers, you can use the System Information utility to detect problems caused by resource conflicts. This utility is located in the System Tools folder under Accessories. Figure 5-19 shows a sample output of the System Information utility.



Resource	Device
I/O Port 0x00000000-0x00000CF7	PCI bus
I/O Port 0x00000000-0x00000CF7	Direct memory access controller
I/O Port 0x000003C0-0x000003DF	VIA CPU to AGP Controller
I/O Port 0x000003C0-0x000003DF	S3 Graphics ProSavage DDR 8D04 (Microsoft Corporation)
IRQ 21	VIA Rev 5 or later USB Universal Host Controller
IRQ 21	VIA Rev 5 or later USB Universal Host Controller
IRQ 21	VIA Rev 5 or later USB Universal Host Controller
IRQ 21	Standard Enhanced PCI to USB Host Controller
Memory Address 0xA0000-0xBFFFF	PCI bus
Memory Address 0xA0000-0xBFFFF	VIA CPU to AGP Controller
Memory Address 0xA0000-0xBFFFF	S3 Graphics ProSavage DDR 8D04 (Microsoft Corporation)
I/O Port 0x000003B0-0x000003BB	VIA CPU to AGP Controller
I/O Port 0x000003B0-0x000003BB	S3 Graphics ProSavage DDR 8D04 (Microsoft Corporation)

Figure 5-19. System Information utility in Windows XP

If you suspect a network adapter or driver problem, you can check the Device Manager utility in Windows XP. This utility is provided as a snap-in under the Computer Management console. It makes it easy to view whether the device is functioning or not and allows you to view driver details, and update or uninstall a network driver. In case a network driver has been replaced with an incompatible driver, you can use the Roll Back Driver option to replace the driver with the one that was previously working properly. Figure 5-20 shows the Driver tab of the Network Adapter properties.



VIA Rhine II Compatible Fast Ethernet Adapter

Driver Provider: Microsoft

Driver Date: 10/1/2002

Driver Version: 3.11.0.346

Digital Signer: Microsoft Windows Publisher

To view details about the driver files.

To update the driver for this device.

If the device fails after updating the driver, roll back to the previously installed driver.

To uninstall the driver (Advanced).

Figure 5-20. Properties of the Network Adapter Driver

An incorrect network driver can also cause connectivity problems in a computer. Make sure that only network drivers that are fully supported by the vendor are installed. You must also verify that the operating system you are using supports the network adapter and the driver. In case the vendor updates the network adapter driver, you must first test the new version of the driver before installing it on any production server or desktop computer.

TCP/IP configuration. TCP/IP is the most widely used networking protocol to date. TCP/IP is in fact a suite of protocols that work together to provide connectivity solutions in most medium- to large-scale networks. If TCP/IP is the protocol used on your network, you must understand how the network adapters should be correctly configured to connect to the network and successfully access network resources.

Computers or hosts in a TCP/IP network connect to each other using IP addresses. Each network host is assigned an IP address, which should be unique in the entire network. The allocation of IP addresses can be done either statically (manually) or dynamically. Static IP address assignment is suitable only for a small network of about 10 computers. When manually assigning IP addresses, the following addresses must be configured correctly:

IP address
: The unique address of a host in a network.

Subnet mask
: Another IP address that helps identify the network and host part of the IP address.

Default gateway
: The IP address of the local network interface of the router. The default gateway helps the host connect to hosts on remote network segments.

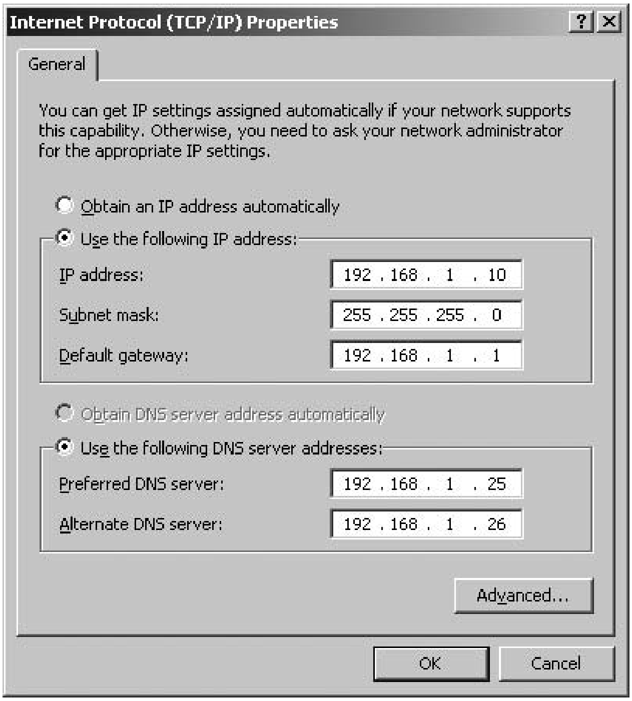
If any of the preceding addresses are incorrect, the computer will not be able to communicate to other computers. An incorrect or missing IP address will completely isolate the computer in the network. A missing subnet mask will not allow the computer to communicate to other computers, even in the same network segment. If the default gateway is missing or incorrect, the computer will not be able to communicate to other computers located on remote network segments.

In addition to the TCP/IP configuration settings just described, the computers must also be configured correctly for IP addresses of DNS servers and WINS servers. If the DNS server is not configured correctly or is missing, the computer will not be able to resolve hostnames to IP addresses. Figure 5-21 shows the manual TCP/IP configuration on a Windows XP computer.

The TCP/IP configuration can also be assigned automatically or dynamically using a *Dynamic Host Configuration Protocol (DHCP)* server. The DHCP server is configured with a pool of IP addresses called the *DHCP scope*. The DHCP server assigns IP addresses and other TCP/IP parameters to DHCP-enabled hosts for a limited period of time, called a *lease*. The DHCP clients must renew the lease before it expires. On Windows-based computers, the DHCP clients must try to renew the TCP/IP configuration with a DHCP server when 50 percent of the lease period expires. The default configuration of most Windows operating systems is to obtain TCP/IP configuration automatically from any available DHCP server.

Since the DHCP servers can be configured to service multiple network segments, it is possible that one or more DHCP scopes contain duplicate or overlapping IP address ranges. This causes the DHCP server to allocate duplicate IP addresses to network clients, which results in connectivity issues. DHCP scopes must be properly configured with the correct address scopes and correct addresses of DNS and WINS servers.

If you are tasked with resolving a TCP/IP configuration problem, you may use any of the built-in TCP/IP diagnostic utilities such as *ipconfig* (Windows NT/2000/XP/2003), *winipcfg* (Windows 95/98/Me), and *ifconfig* (Unix/Linux/MAC OS). These utilities are very helpful in locating the cause of the problem. A simple ping



Internet Protocol (TCP/IP) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 1 . 10

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 1 . 1

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 1 . 25

Alternate DNS server: 192 . 168 . 1 . 26

Figure 5-21. Manually configured TCP/IP properties

to the loopback address 127.0.0.1 also verifies that the TCP/IP protocol is correctly installed on the local computer.

IPX/SPX configuration. As with the TCP/IP protocol, incorrectly configured network adapters are the main causes of network problems in a NetWare IPX/SPX network. It is essential to verify that all adapters are installed with correct settings and without hardware or software conflicts. The IPX/SPX configuration includes the following parameters:

Internal network number
This number uniquely identifies the IPX/SPX host on a NetWare network. It must not be duplicated on any host.

Network number
This number is a hexadecimal number that identifies a single network segment. Every host on the same LAN segment must have an identical network number.

Frame type
A correct Ethernet frame type must be configured for the adapter to function properly. Newer versions of NetWare operating systems support automatic detection of frame type when the network adapter driver is installed. While most versions of NetWare support 802.2 frames with 802.2 headers, versions 2.x and 3.x supported the 802.3 frame type.

If your network has a mix of NetWare and Windows servers, you might want to verify that Windows clients who wish to connect to NetWare servers have the *NWLink IPX/SPX NetBIOS Compatible Transport Protocol* installed. This protocol allows Windows clients to connect to NetWare servers. In Windows NT and older operating systems, the *Gateway Service for NetWare (GSNW)* is required to be installed on Windows servers to allow client access to Network servers. Besides this, Windows clients can directly communicate to NetWare servers using the *Client Service for NetWare (CSNW)*.

Resource permissions. When network connectivity is not an issue, resource access permissions can cause a number of service calls. Users who wish to access particular files, folders, or printers but do not have sufficient permissions will ultimately call helpdesk technicians to resolve the access problems. Assignment of resource access problems is mainly the responsibility of system administrators. In certain smaller networks, the network technicians may also be tasked with assigning and managing permissions to network resources such as a user's home directory.

Any user who needs to save files on a folder must have at least Write permissions on the folder. If this permission is missing or only a Read or Execute permission is assigned, the user might not be able to save her work to the designated folder.

On Windows server operating systems, administrators put users in groups and assign permissions to groups. A user can be a member of more than one group, with each group having a different level of access permissions. In such cases, user permissions are clubbed together and the highest level of permissions is granted. Similarly, share permissions and NTFS permissions can be assigned to resources. When there is a conflict between share and NTFS permissions, the most restrictive permissions are applied to a user.

> Troubleshooting permission problems could be a time-consuming task. You will need to act with patience and not try to grant the user the highest level of permissions in order to save time or to get rid of the problem. Doing this might put you in trouble because certain documents may be confidential, and you might need to get permission from your supervisors before granting access permissions to any user. It is always better to check with your seniors when modifying permissions on shared resources. The same rule applies when a user asks you to share a particular folder for him but he is not authorized to have access for it.

Firewall configuration. Firewall protects a network from unauthorized internal and external access. It can either be a dedicated hardware device or can be running as a software application on one of the network servers. If your organization has an Internet presence, it is quite possible that the internal network of the organization is protected by firewalls.

Firewall settings mainly affect the users trying to access the network from outside. For example, a remote access user must be properly authenticated before he/she can log onto and access network resources. Firewalls function using rules and these rules can be configured to allow or deny access based on source and destination TCP/IP protocols, ports, or IP addresses.

If a user is having difficulty accessing the network from outside, firewalls settings have to be checked to verify that the user is connecting using a correct protocol, port, and IP address. The protocol, port, or IP address must be allowed through the firewall to let the user successfully connect to the network.

Electrical interference. Electrical interferences degrade signal quality as the signal travels down the length of network cables. This interference can be caused by either crosstalk among cables or by power equipment located close to network cables. Similarly, wireless signals can be affected by both electrical interference as well as radio frequency signals. UTP cables should not be run in areas of high EMI such as near transformers and besides high-voltage electric cables.

Wireless networks are susceptible to electromagnetic and radio frequency interferences (EMI and RFI). Wireless access points should not be located near areas of high interference. Wireless signals degrade as they travel away from a wireless signal-generating device such as the access point. This degradation or attenuation of signals is caused by several environmental factors such as EMI, RFI, walls, etc. Weakening of wireless signals can be prevented to some extent by careful location of a wireless antenna, use of signal boosters, and the correct placement of wireless access points. It is good to know the maximum range of the wireless access points used in the network.

Preventive maintenance for networks

Preventive maintenance of networks is performed to ensure that every component of the network works per expectations. Network administrators take all possible steps to prevent a breakdown of the network. This includes securing network connections, providing redundancy for network servers and services, restricting unauthorized access to network equipment, implementing a data backup plan, and keeping software updated with the latest service packs. The main purpose of preventive maintenance is to provide maximum uptime. This section explains the key factors behind preventive maintenance of networks.

Securing network cables. Loose connections cause a majority of network connectivity problems. They are also the most frustrating when it comes to locating and troubleshooting problems. Network administrators and technicians must ensure that all cables, connectors, patch panels, and patch cables are of correct specifications. These must also be firmly attached to servers, workstations, printers, network hubs, switches, and routers. Cables must not be loosely attached to connectors, and the correct type of cables should be in use.

Cables are run from network hubs, switches, or routers to end stations. It is important to label each end of the cable, which makes it easy to locate a faulty cable and replace it if necessary. It is not possible to trace a faulty cable from a workstation to a hub or switch in a large network if there is no labeling system in place. If the cables are labeled, you can easily find out which cable needs to be replaced. Cables must be periodically checked for loose connectivity or wear-and-tear, and worn out cables should be replaced with new ones.

Another important aspect of securing network cables is the routing of cables. Improper routing of cables results in damaged or broken cables. Network cables should always be run in designated areas. Cables should not be running in areas where people usually walk. People can get trapped in loose cables on the floor and may fall down and get injured besides causing connectivity problems. Make sure that all cables are securely and firmly attached to computers, printers, and network devices.

Documentation always helps. A layout diagram of the network cabling is very helpful in troubleshooting network connectivity problems. It is also helpful if you need to expand the network due to the growing business requirements of the organization. It is easy to help new network technicians understand the network layout if you have appropriate network documentation.

Restricting physical access. Physical access to core network equipment such as critical servers, network hubs, switches, and routers should be restricted to authorized personnel only. It must be ensured that only designated administrators are allowed to install, configure, and maintain this equipment. Improper configuration changes in network equipment can cause network problems and can also render the equipment vulnerable to hackers.

Server and desktop hardening. The network operating systems on servers and desktop operating systems on workstations should be regularly updated with the latest service packs, hotfixes, and security patches. Similarly, application software should also be updated as and when the vendors release updates. Updates are meant to remove bugs in operating systems and application software. It is important to test updates in a test environment before installing them on production equipment.

All servers and workstations should have virus-scanning software to help detect and remove malicious software. Antivirus applications should be regularly run on servers and workstations. Virus-scanning software depends on a database called virus signatures, which should be regularly updated to detect and remove newer virus applications.

Every computer should be locked when not in use. It is not uncommon to notice people leaving their workstations unlocked. A password policy ensures that employees use strong passwords and change them regularly. This helps prevent external attacks on the network using hacked usernames and passwords.

Data backups and recovery. A backup and recovery plan helps restore critical data in case of a disaster. Disasters can come in any form: fire, storm, flood, and earthquake are all different forms of disaster and cause significant damage to businesses. A properly planned, implemented, and documented disaster recovery plan is crucial to the functioning of any network—small or large. Data backups also help restore files and folders that are accidentally deleted or modified by users. Regular backups must be supported by test restores to ensure that the data can be restored successfully in the event of a disaster.

Power redundancy. Fault-tolerant or redundant power supplies help reduce the chances of a system going down due to unexpected power failure. Most network servers come equipped with redundant power supplies. UPS systems not only ensure clean power to servers and network equipment, but also ensure that sufficient time is available to save your work in case the power goes out. They help prevent system damage caused by power spikes, surges, sags, brownouts, and blackouts.

Link redundancy. Link redundancy refers to providing secondary connections to critical network equipment. It ensures that if the primary connection fails due to some reason, a secondary connection is available to prevent downtime and keep the essential network services running. Some servers come with multiple network adapters that provide fault tolerance as well as efficient utilization of network bandwidth.

Server clusters. Server clustering is the process of providing fault tolerance and load balancing for critical servers in the network. Critical servers such as domain controllers, DNS servers, web servers, and mail servers, can be configured in clusters so that these services are not affected when one of the servers experiences a breakdown.

Hot, warm, and cold sites. Hot, warm, and cold sites are part of the disaster recovery plan for those businesses that are heavily dependent on computers for conducting their everyday business. These sites are usually separate locations equipped with necessary hardware and network connections. Depending on the type of site, network and business operations can be resumed with minimal efforts in case the primary site is destroyed by a disaster. The following is a brief description of hot, warm, and cold sites:

Hot site

Allows organizations to resume business activities almost immediately. It is equipped with fully configured hardware, software, network devices, and telephone lines. The data is replicated to servers at hot sites.

Warm site

Normally is equipped with necessary hardware, software, network devices, and telephone lines. Hardware and software must be configured, and data must be restored from backup tape sets.

Cold site

Requires the maximum amount of time to be set up and made functional. It contains only partial hardware, software, and network devices that are not configured.

Hot and cold spares. Hot spares and cold spares are used for critical servers and network equipment to ensure maximum uptime. They are helpful in minimizing the time it takes to restore failed network equipment. Hot and cold spares are closely related to hot swapping and cold swapping. The following is a brief description of each of these terms:

Hot spares

Spare components that are installed inside critical servers and readily take over a failed component.

Cold spares

Spare components that are installed inside a critical server but must be configured manually by an administrator.

Hot swapping

The ability of a server to allow replacement of a failed component (usually a hard disk in the disk array) while the server is powered on.

Cold swapping

The process of fully powering down a server before a failed component can be replaced.

Security

The security section of the A+ exams tests your knowledge of basic principles of implanting security on desktop computers. You must have a good understanding of security fundamentals and be able to troubleshoot general problems related to security settings on a personal computer.

Principles of Security

This section covers the basic aspects of computer security, including access control methods, auditing, and logging. Besides this, I briefly explain the procedures for implementing basic security mechanisms on personal computers and methods to troubleshoot problems related to security settings.

Access control

The term *access control* refers to the method of granting or denying access to network resources by means of security policies, hardware devices, or software applications. In its simplest form, access control is applied on files and folders, or on other shared network resources by means of assigning permissions. Smart cards and biometric devices are examples of hardware devices used for access control. Access control can also be implemented by means of network devices such as routers and wireless access points (WAPs). Access control mainly falls into the following categories:

Mandatory Access Control (MAC)

A mechanism, usually hardcoded into an operating system, to protect computer processes, data, and system devices from unauthorized use. It may also be built into an application to grant or deny permissions, and is universally applied to all objects. MAC is also known as *label-based access control*.

Discretionary Access Control (DAC)

This is usually implemented in the operating system in the form of user rights and permissions. NTFS permissions used in Windows-based computers are a good example of DAC.

Role-based Access Control (RBAC)

This is used to implement security on objects based on roles (job functions) of individual users or user groups. RBAC is highly flexible and configurable and provides centralized administration.

User accounts

A user account is the most basic form of security on a network. A user account allows a user to log onto the system and the network and access resources. While a local user account allows access only to the resources located on the local computer, a domain/network account allows access to all resources located across different parts of the network. Local user accounts are stored on the local computer only. Network accounts are stored in a centralized database on a network server.

Local user accounts

A local user account allows users to log on locally to a computer and access resources located on the local computer only. These accounts are stored in the local security database, which authenticates users when they log on. Local user accounts cannot be used on any other computer on the network.

Domain user accounts

A domain user account allows users to log on to the network from any computer in the network domain. User accounts in Windows 2000 and Windows Server 2003 domains are stored in a centralized database known as the Active Directory database, which is located on the Domain Controller. If there are multiple domain controllers in the network, the user accounts are replicated to all domain controllers along with other Active Directory data.

On Windows XP and Windows 2000 Professional operating systems, the following types of local user accounts can be created:

Administrator

The administrator account has full control over the operating system and resources located on it. This account is used for creating and maintaining user accounts, assigning permissions, managing shared resources, installing and configuring devices, and configuring local security policies.

Guest

The guest account allows occasional users to log on and access local resources. This account is usually disabled by default.

User

Normal users fall into this category. These accounts are created to allow users to log on to the system and access resources for which they have been assigned permissions.

All desktop and network operating systems provide methods to create and manage user accounts. For example, on a Windows XP computer, local user accounts can be created using the User Accounts utility in the Control Panel. Similarly, in Windows 2000 and Windows Server 2003 domains, user accounts are created using the Active Directory Users and Computers utility. Active Directory allows administrators to create, delete, and disable user accounts.

Access control using groups

A *group* is a collection of user accounts. Groups simplify the administration of resources on a local computer or on a network server. They allow administrators to assign permissions to resources to multiple users simultaneously instead of assigning permissions to individual users. Administrators usually choose users based on their job roles and put them into groups. These groups are then assigned permissions on local or network resources. Windows XP and Windows 2000 Professional computers have the following common built-in groups:

Administrators
: Members of this group can perform all administrative tasks on the system. The Administrator account is a member of this group by default.

Power Users
: Members of this group can create and manage user accounts and shared resources on the computer.

Guests
: Members of this group can occasionally log onto the system and perform only those tasks for which they have been assigned permissions. The Guest user account is a member of this group by default.

Backup Operators
: Members of this group can back up and restore files and folders on the local computer.

Users
: Members of this group contain all user accounts created on the system. Users can perform only those tasks and access only those resources for which they have permissions.

Permissions and level of access

Permissions allow users to access resources and perform specific tasks based on the type and level of access granted. Administrators use groups to assign permissions on shared resources. Shared resources on a computer usually include files, folders, and printers. Resource permissions mainly fall into the following categories:

File permissions
: File permissions or NTFS permissions can be configured on individual files on computers using NTFS. NTFS permissions are applied to local users as well as to network users. The FAT filesystem does not support file-level permissions.

Folder permissions
: Folder permissions can be configured to the entire folder, subfolders, and files within the folder. These permissions are also applied to local and network users.

Share permissions
: Share permissions can be configured on both NTFS and FAT filesystems. These permissions do not affect the user who logs on locally to the system, and are applicable only to the users who connect from the network.

Printer permissions
: Printer permissions allow users to connect and send print documents to a shared printer. In Windows XP and Windows 2000 Professional, users must have at least Print permissions to send print jobs to a shared printer.

Level of access. The level of access granted to a user or group on a shared resource is controlled by permissions. Each file, folder, and printer on a Windows computer has an associated ACL that defines the level of access granted to users or groups. The levels of access on files and folders fall into the following categories:

Read permission
Allows users to read the contents of a file or folder.

Write permission
Allows users to create new files and subfolders in folders and write data to files.

Read and Execute permission
Allows users to read the contents of a file and execute it.

Modify permission
Allows users to modify the contents of a file or a folder.

Full Control permission
Allows users to change permissions on a file or folder and perform all actions permitted by other permissions.

List Folder Contents (Folder Only) permission
Allows users to navigate through the folder and subfolders.

The level of access on printers can be configured as follows:

Print permission
Allows users to print to the printer and manage (pause, resume, restart, and cancel) their own documents.

Manage Documents permission
Allows users to print to the printer and manage (pause, resume, restart, and cancel) all documents sent to the printer.

Manage Printers permission
Allows users to print and manage documents (pause, resume, restart, and cancel), share the printer, create and delete a printer, and change print permissions.

Restricted spaces

Restricted spaces in computer networks refer to those areas where physical access is restricted to authorized personnel only. These areas usually include network operating centers (NOCs), telecommunication rooms, and other computer rooms. Restricted physical access ensures safety and security of expensive and critical network equipment, servers, and cabling systems. Critical servers and network equipment such as switches, routers and firewalls are located inside network operating centers. Strict security policies are enforced to restrict access. Organizations usually employ one or more of the following methods to restrict access to these areas:

- Entry is permitted only to authorized administrators and technical support personnel.
- Doors are equipped with authentication methods such as biometric devices or keypad locks.

- Log books are maintained to keep record of persons entering the restricted rooms.
- Restricted rooms are equipped with alarm systems to prevent theft.
- Unused and faulty equipment is not allowed to be stored inside restricted areas.
- No trash or garbage is placed inside these areas.

Auditing and event logging

The term *auditing* refers to the process of tracking and logging activities of users and processes on computer systems and networks. Auditing can be useful in multiple scenarios, such as troubleshooting a failed process, finding a security breach on the part of an internal or external user, and tracking unauthorized access to secure data. Auditing enables administrators to track security breaches such as unauthorized access to confidential data by identifying the user who made the attempt. It also helps diagnose problems related to process failures.

Auditing is essentially a two-step process. The first part deals with enabling auditing on system and network resources. The second part is to view and analyze the data collected by audits. Collecting audit information in logs is known as *event logging*. The following sections explain the purpose and characteristics of the auditing and logging process.

Auditing. Auditing is the process of tracking system usage and authorized or unauthorized access to system services and data. This may also be helpful in diagnosing problems related to application failures during the development or implementation phase. Since auditing puts a significant processing load on servers, you must first make sure that the benefits of auditing are clearly understood and visible. While administrators should implement certain audits manually, network operating systems include processes that automatically audit the system process and log audit data that can be analyzed later in order to troubleshoot system failures. In its basic form, a secure computing environment can be established by splitting the duties of employees within an organization. This ensures that whatever actions are taken by an employee are consistently supervised or controlled by someone superior in the organizational hierarchy.

On Windows desktops, the following types of events can be audited for success or failure:

Account Management
: Includes events related to creation, modification, and deletion of user accounts by administrators.

Log Off and Log On
: Includes events related to users logging on or logging off the local computer.

Process Tracking
: Includes events related to actions performed by software applications.

Object Access
: Includes events related to access of files and folders by users.

Privilege Use

Includes events related to users exercising their rights, such as changing the system time.

System Events

Includes events related to system processes such as shutting down or restarting the computer. These events also relate to system security.

Logging. Almost all network operating systems include methods to audit system processes and user activities. These audits can be logged in special log files. The log files can be viewed and analyzed to track problems related to security breaches and to troubleshoot process problems. Operating systems such as Microsoft Windows XP, Windows 2000, and Windows Server 2003 include a management console snap-in named *Event Viewer* where you can view the logs related to system processes, security, and applications.

Install, Configure, and Upgrade Security

The task of installing, configuring, and maintaining security involves knowledge of authentication technologies for both wired and wireless networks. This section provides a brief description of authentication methods, configuring auditing, and configuring permissions to ensure data access security.

Authentication technologies

Authentication technologies ensure secure access to system and network resources. The most commonly used and basic form of authentication is the username and password combination, which allows users to log on to a system or a network. Other forms of secure authentication include tokens, biometrics, and multifactor, as discussed in the following sections.

Username and password. Almost all network operating systems implement some kind of authentication mechanism wherein users can simply use a locally created username and password to get access to the network and shared resources within the network. This is the simplest form of authentication and can be implemented easily, but it also comes with its own limitations. Many organizations document and implement password policies that control how users can create and manage their passwords in order to secure network resources. The following are common elements of a password policy:

- Passwords must be at least seven characters long.
- Passwords must contain a combination of upper- and lowercase characters, numbers, and special characters.
- Passwords must not contain the full or part of the first or last name of the user.
- Users must change their passwords periodically.
- Users must not reuse old passwords.

Tokens. An *Authentication token* (also known as *security token* or *hardware token*) is considered the most trusted method for verifying the identity of a user or a system. Tokens provide a very high level of security for authenticating users because of multiple factors employed to verify the identity. In its simplest form, an authentication token consists of the following two parts:

Hardware device
This is a small device that can be carried on a key chain or in a wallet. Some tokens are coded to generate token values at predetermined intervals. Some security tokens may contain cryptographic keys while others may contain biometrics data such as the fingerprints of the user.

Software component
This tracks and verifies that the codes or keys used by the hardware device are valid.

Biometrics. Biometrics refers to the authentication technology used to verify the identity of a user by measuring and analyzing human physical and behavioral characteristics. This is done with the help of advanced biometric authentication devices, which can read or measure and analyze fingerprints, as well as scan the eye retina and facial patterns, and measure body temperature. Handwriting and voice patterns are also commonly used as biometrics.

Multifactor. In computer authentication, a *factor* is a piece of information that is present to prove the identity of a user. In a multifactor authentication mechanism, any of the following factors may be utilized:

- A *something you know* factor, such as your password or PIN.
- A *something you have* factor, such as your hardware token or a smart card.
- A *something you are* factor, such as your fingerprints or eye retina, or other biometrics that can be used for identity.
- A *something you do* factor, such as your handwriting or your voice patterns.

Wireless authentication. Wireless authentication is implemented in one of the following methods:

Open System
This authentication is actually no authentication. Every computer trying to connect to a wireless network is granted a connection.

Shared Key
This authentication requires that every wireless client knows the shared secret key. The access point and all wireless clients must use the same shared secret key.

IEEE 802.1x
This authentication requires use of advanced encryption and authentication techniques to provide strong authentication.

WPA or WPA2 with Preshared Key
This authentication method can be used for smaller home or office networks that cannot implement the IEEE 802.1x authentication mechanisms. The preshared key consists of a 20-character long paraphrase containing upper- and lowercase letters and numbers.

Software firewalls

A *firewall* is a dedicated hardware device or a software application that prevents a system or a network from unauthorized access. A software firewall is usually a software application or is installed as one of the operating system features. For example, Windows XP SP2 includes a firewall that can be configured to permit or deny certain network traffic.

Software firewalls installed on individual PCs are also known as *personal firewalls*. They do nothing more than protect the individual computer on which they are installed. The firewall functionality is often provided by the operating system or a software application. They differ from conventional network firewalls in that network firewalls are often dedicated hardware devices or the firewall functionality is built into routers.

In a workgroup environment, each user can turn on the firewall and configure its settings on her desktop on Windows XP computers. The following steps explain how firewall settings can be configured on a Windows XP SP2 computer:

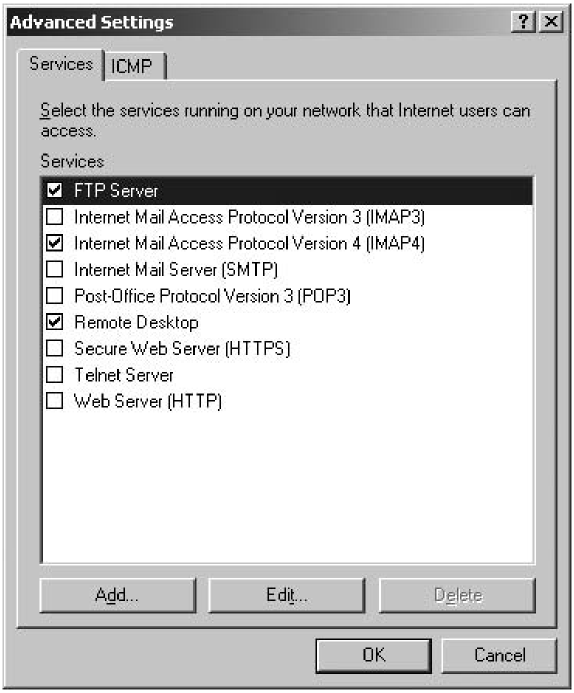
1. Click Start → Control Panel → Windows Firewall.
2. Click the ON radio button to turn on the firewall.
3. Click the Advanced tab to open the advanced firewall settings for the network adapter.
4. Select the checkbox for the shown network adapter and click Settings. Note that all services are disabled by default.
5. Select the services that you want to allow, as shown in Figure 5-22.
6. Click OK.
7. Click the Settings button for ICMP. Note that all options are disabled by default.
8. Click the checkboxes for ICMP messages that you want to allow.
9. Click OK.

Enabling and disabling auditing

Enabling auditing on Windows desktops is a two-step process. First, you will need to enable auditing in the Local Security Policy, and second, you will need to enable auditing on files or folders. Remember that file and folder auditing can only be enabled on NTFS partitions. FAT and FAT32 do not support auditing. The following two exercises explain the steps involved in configuring auditing.

Enabling auditing in Local Security Policy

1. Click Start → Control Panel
2. Double-click Administrative Tools.
3. Double-click Local Security Policy.
4. Expand the Local Policies folder in the Local Security Policy window.
5. Click Audit Policy to display available policies in the Details pane.
6. Double-click the event that you need to audit. For this exercise, double-click Object Access.



Select the services running on your network that Internet users can access.

Services

☑ FTP Server
□ Internet Mail Access Protocol Version 3 (IMAP3)
☑ Internet Mail Access Protocol Version 4 (IMAP4)
□ Internet Mail Server (SMTP)
□ Post-Office Protocol Version 3 (POP3)
☑ Remote Desktop
□ Secure Web Server (HTTPS)
□ Telnet Server
□ Web Server (HTTP)

Figure 5-22. Firewall settings in Windows XP

7. The Audit Object Access Properties dialog box opens. Click the Success and Failure checkboxes.
8. Click OK. Close the Local Security Policy window and restart the computer.

Configuring auditing on a folder

1. Open Windows Explorer.
2. Navigate to the folder on which you want to configure auditing.
3. Right-click the folder and click Properties.
4. Click the Security tab and click Advanced to open the Advanced Security Settings window.
5. Click the Auditing tab and click Add to add audit entries for users.
6. Click the list of events that you wish to audit.
7. Click OK to return to Advanced Security Settings window.
8. Click OK twice to close all windows.

Wireless client configuration

For most home networks, wireless routers come with Zero Configuration features to automatically configure the Windows XP computers to use the wireless network as well as share the Internet connection. This configuration dynamically assigns IP addresses to computers. For infrastructure networks in medium- to large-scale networks, the wireless networks need to be configured to connect to an appropriate wireless Access Point (WAP). Security in wireless networks is configured using the Wired Equivalent Privacy (WEP), Wireless Protected Access (WPA), or WPA2. In Infrastructure networks, both the access point and the Windows XP computers need to be configured.

Configuring the access point. The wireless access point must be configured as follows:

- Configure the name of the wireless network, which is known as the *Service Set Identifier (SSID)*.
- Enable WPA with Temporal Key Integrity Protocol (TKIP) or WEP, as required.
- Enable WPA preshared key authentication or WEP authentication.
- Enter the WPA preshared key or select the WEP key format.

Configuring the wireless clients. The wireless client on a Windows XP with an SP2 computer can be configured to use WEP authentication using the following steps:

1. Click Start → Control Panel → Network Connections.
2. Double-click the Wireless Connections applet.
3. Click View Available Wireless Networks to open the wireless connections dialog box.
4. Double-click the name of the wireless network.
5. Type the WEP key and re-enter it in the confirmation box.
6. Click Connect.
7. In the Network Authentication box, click Open.
8. In the Data Encryption box, click WEP.
9. Type the WEP encryption key in the Network Key and the Confirm Network Key boxes.
10. Click OK to save the settings to the wireless connection.

Data access

The most basic form of implementing data security is through assigning permissions to users and groups. Access permissions are granted to users or groups based on their job functions. On Windows 2000 Professional and Windows XP Professional desktops, file and folder access is configured using filesystem permissions and share permissions. While file-level security is available only on disk partitions formatted with NTFS, share-level security can be configured on all FAT and FAT32 and NTFS filesystem partitions.

To configure NTFS permissions on a file or folder located on a Windows desktop, the following steps need to be completed:

1. Open Windows Explorer and navigate to the file or folder.
2. Double-click the file or folder to open its Properties window.

3. Click the Security tab to view currently configured permissions.
4. Click the Add button to add users or groups that you need to allow access to.
5. Select the user or group from the list of users.
6. Click the checkboxes for appropriate permissions.
7. Click OK to close the Properties window of the file or folder.

Share permissions can be assigned to shared folders as described in the following steps:

1. Open Windows Explorer and navigate to the file or folder.
2. Double-click the file or folder to open its Properties window.
3. Click the Sharing tab.
4. Click the Permissions button to add users or groups and configure their permissions.
5. Click OK to close the Properties window of the folder.

> Note that the Security tab in the Properties window of a file or folder is available only when the disk partition where the file or folder is located is formatted with NTFS. This is because FAT and Fat32 filesystems do not support NTFS permissions.

Converting from FAT or FAT32 to NTFS. Windows XP Professional and Windows 2000 Professional operating systems include a command-line utility called *convert.exe* to convert FAT or FAT32 partitions to NTFS. This process does not cause any loss of existing data on the partition. The following steps explain the usage of this command to convert a partition D from FAT16 or Fat32 to NTFS:

1. Click Start → Run.
2. Type `cmd` in the dialog box and press the Enter key. This opens the Windows command prompt.
3. Type the following command and press the Enter key:

   ```
   convert D: /FS:NTFS
   ```

If the partition you are converting is a system volume, the conversion is done after the system restarts.

> Remember that you can convert from FAT or FAT32 to NTFS at any time during or after the installation without losing any data. This conversion is a one-way process. You cannot convert from NTFS back to FAT or FAT32 without losing data.

Diagnostic and Troubleshooting Techniques

Troubleshooting security-related problems is a daunting task if network devices and individual systems are not configured properly. This section covers some of the sources of security-related problems and explains how these problems can be prevented.

Software firewall issues

Software firewalls can pose problems if not configured properly. Incorrectly configured firewalls can deny access to legitimate users and can also allow access to hackers. Software firewalls work according to *firewall rules* that are usually configured to allow or deny access to a network based on the following parameters:

- Source and destination IP address
- Source and destination port numbers
- The protocol used to gain access
- The application that attempts to gain access

It is recommended that software firewall configuration be tested thoroughly to ensure that it works as expected. A firewall should not allow any undesired network traffic, but legitimate users should not suffer due to incorrectly configured firewall rules.

Wireless client configuration issues with SSID

SSID enables wireless clients to connect to a wireless access point and to access network resources. If a wireless client is reporting connectivity problems, wireless configuration should be checked to make sure that the client is using the correct SSID. Remember that both the access point and the wireless client should be configured with the same SSID.

In large corporate networks, security is a prime concern, and most administrators configure certain authentication mechanisms to prevent unauthorized access to confidential company data. If a user cannot log on to a wireless network, make sure that he has sufficient permissions. Additionally, confirm that the encryption and authentication settings are configured correctly on his computer. Wireless networks use *Wired Equivalent Privacy (WEP)* protocol, which supports both 64- and 128-bit encryption. Make sure that the client is configured to use the correct WEP encryption standard.

Data access issues

Problems involving access of resources are very commonly seen in networks. Users often complain of an “Access is Denied” message popping up on their desktops when they want to connect to a computer or access a shared file, folder, or printer. The following are some of the common reasons for data access problems:

Insufficient permissions

A user may not be able to access a shared resource due to insufficient permissions. For example, if a user is allowed only the Read or the Read and Execute permission, she may not be able to make any changes to a file. Similarly, if a user is granted the List Folder Contents permission, she may not be able to even open or run a file within the folder.

Permission conflicts

Administrators usually assign permissions to groups instead of configuring permissions for each individual user. In some cases, a particular user may be a member of more than one group with different levels of permissions assigned to each group. This conflict of permissions may also result in access problems. On Windows desktops with NTFS permissions, if a Deny permission is assigned to any user, it overrides all his permissions for a particular file or folder. For example, if a user is allowed access in one group to a folder, but another group has a Deny permission on that folder and the user is a member of both groups, his effective permission would be calculated as deny access. Moreover, when both share permissions and NTFS permissions are configured on a folder, the most restrictive permissions are applied to a user or a group.

Local security policies

Local security policies such as Log On Locally or Access This Computer From Network affect how the user can log on or access local resources on a computer. If a user or group is allowed share permissions on a folder, but a member user is not allowed to access the computer from the network, he will not be able to access the shared folder.

Encryption problems

Encryption problems result in denying access to a user, to a system, or to the entire network. The user may not be able to log on to a desktop or to a domain due to incorrect configuration settings. Encryption problems usually fall into the following categories:

Unsupported encryption protocols

The user's operating system or software application may not support the encryption method required by the system. This is a common problem for users trying to connect remotely to a network.

Protocol mismatch

If two computers are using different encryption protocols, they may not be able to communicate, resulting in denial of access for a user on one system to another system.

Preventive Maintenance for Security

Implementing strong security measures for networks is one of the most critical tasks for most network administrators. When properly implemented, security mechanisms protect network resources from unauthorized access and damage to critical data. Apart from implementing security, administrators need to implement certain procedures and policies to make sure that security implementation works as desired and is not breached due to loopholes or lack of user training.

Security policies

It is important to emphasize the importance of implementing security policies in an organization. Security policies consist of the following essential components:

Account policies

Account policies define how the user accounts are handled by the system when someone tries to log on using an incorrect password. A user's account may be locked after a certain number of unsuccessful logon attempts.

Password policies

Password policies define how users maintain their passwords. These policies include minimum password length, maximum password age, and password complexity requirements.

Audit policies

Audit policies define whether or not object access and use of privileges and rights are to be audited.

Software restriction policies

Software restriction policies define which applications are not allowed to run on a system. These policies prevent damage of critical operating system files.

Registry

The registry component of security policies defines security for registry keys and subkeys to prevent unauthorized modification.

Social engineering

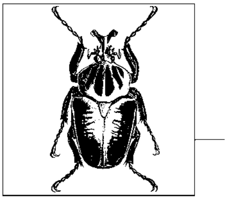
Social engineering refers to the process of obtaining personal or confidential information about someone by taking that person into confidence. The so-called "social engineer" generally tricks the victim over the telephone or on the Internet to reveal sensitive information. Instead of exploiting any security vulnerabilities in computer systems, the person becomes a victim of his own tendency of trusting someone who is trying to exploit the sensitive information collected from the victim.

Social engineering also involves face-to-face interactions between a computer user and an attacker to get access to the computer by taking the victim into confidence. It may also come in the form of an email attachment that asks the user to give away confidential information to the sender of the message. *Phishing* attacks are very common outcomes of social engineering. In a phishing attack, a user of computer systems frequently has interesting chats over the Internet or over the phone to unknown attackers in which she reveals sensitive information such her password or credit card numbers. Responding to fraudulent email messages can also make you a victim of a phishing attack.

Addressing social engineering issues. Unfortunately, no technical configuration of systems or networks can protect an organization from social engineering. There is no firewall that can stop these attacks. The best protection against social engineering is to train the users about security policies of the organization.

In case it is found that some user has disclosed his username or password to an outsider, the user account should be immediately locked or the user should be asked to change his password immediately. This can prevent the possibility of loss of information or confidential company data due to misuse of user credentials.

> The last two sections for Exam 220-602 (“Safety and Environmental Issues” and “Communications and Professionalism”) are covered in Chapter 2. Refer to this chapter for revision of these topics. Also note that Exam 220-603 does not have a “Safety and Environmental Issues” section, and that Exam 220-604 does not cover “Communication and Professionalism.”



6

Prep and Practice for the A+ Exams 220-602, 220-603, and 220-604

The material in this chapter is designed to help you prepare and practice for A+ Exams: 220-602, 220-603, and 220-604. The chapter is organized into four sections:

Preparing for the A+ Exams
: This section provides an overview of the types of questions on the exam. Reviewing this section will help you understand how the actual exam works.

Suggested Exercises for the Exams
: This section provides a numbered list of exercises that you can follow to gain experience in the exam's subject areas. Performing the exercises will help ensure that you have hands-on experience with all areas of the exam.

Highlighters Index
: This section compiles the facts within the exam's subject areas that you are most likely to need another look at—in other words, the areas of study that you might have highlighted while reading the Study Guide. Studying the highlights is useful as a final review before the exam.

Practice Questions for the Exams
: This section includes a comprehensive set of practice questions to assess your knowledge of the concepts. The questions are similar in format to the exam. After you've reviewed the Study Guide, performed the Suggested Exercises, and studied the Highlighters Index, read the questions and see whether you can answer them correctly.

Before you take any of the A+ exams, you should review the exam overview, perform the suggested exercises, and go through the practice questions provided. Many online sites provide practice tests for the exam. Duplicating the depth and scope of these practice exams in a printed book isn't possible. Visit CompTIA's certification web site for pointers to online practice tests (*http://certification.comptia.org/a*).

The objectives for A+ Exams 220-602, 220-603, and 220-604 also include the topics “Safety and Environmental Issues” and “Communications and Professionalism” Refer to Chapter 3 for the Highlighters Index and practice questions on these two topics.

Preparing for the A+ Exams

The A+ exams are computer-generated. They are timed; an onscreen timer clock displays the amount of time remaining on the exam. Most questions on the exam are multiple-choice. The multiple-choice questions are either one of the following:

Multiple-choice, single answer
A radio button allows you to select a single answer only.

Multiple-choice, multiple answer
A checkbox allows you to select multiple answers. Usually the number of correct answers is indicated in the question itself.

CompTIA reserves the right to change the testing techniques at any time. It is recommended that you visit the CompTIA A+ certification web site regularly to get updates on any changes in the exam format. CompTIA has divided the A+ objectives into multiple domains, with each domain covering a defined percentage of objectives. Individuals with adequate hands-on experience who have reviewed the Study Guide, performed the practice exercises, memorized the essentials, and taken practice tests should do well on this type of exam. Individuals who lack adequate hands-on experience and have not prepared appropriately will find the exam hard to pass.

CompTIA suggests the following tips for taking the exam:

- Read the questions slowly and carefully.
- Do not expect to find clues in every question, though they may be present in some.
- Be aware of the distractions/confusions in statements. The first choice is often the best choice.
- Do not attempt to create situations based on a question. Your answer should be based on whatever information is provided.
- If you are retaking the exam, utilize your previous score report and concentrate on areas that need more study or practice.
- If you get stuck, mark and skip the question. You can do it later.

Typically, the test environment will have Previous/Next and Mark For Review options. You can navigate through the test using the Previous/Next buttons. You can click the Mark For Review checkbox to flag a question for later review.

Suggested Exercises for the Exams

The A+ exams expect you to have a good understanding of concepts related to computer hardware and software. Hands-on experience is recommended and is good to have. You should be well-acquainted with hardware terminology, operating systems, and basic security concepts, and you should have the basic skills to troubleshoot problems. You will need to review the Study Guide and pay close attention to the areas that are new for you or that you feel uncomfortable with.

This section includes some exercises that you can perform either on a standalone computer or in a network to gain some hands-on experience. Since the A+ exams mainly cover all core basic knowledge skills related to installing, configuring, and troubleshooting computer hardware and software, you will need plenty of experience in these tasks. You must know what specifications to look for when selecting a component and how to correctly install the hardware and device drivers.

> It is recommended that you do not perform any of the suggested exercises in your organization or in any running computer network. Create a test environment consisting of two computers for completing these exercises. Even if you just want to view network settings in a production environment, make sure a senior administrator accompanies you. In any case, you should follow the policies of the organization. For most exercises where you need to work on internal parts of a computer, make sure that you are wearing a properly grounded antistatic wrist strap.

Installing a Hard Drive

1. Obtain a hard drive with sufficient storage capacity.
2. Disconnect the old drive and carefully remove it from the computer case.
3. Set the Master, Slave, or Cable Select jumpers on the new drive.
4. Select the data cable to which the disk will be connected.
5. Insert the new drive and reconnect the data cable and the power supply cable.
6. Turn on the computer and test the new drive.

Upgrading Memory

1. Open the computer case and inspect the installed memory modules.
2. Make sure that you have extra slots for expanding memory.
3. Obtain new memory modules that are compatible with the system bus.
4. Do not remove the memory modules from protective covering until you are ready to install them.
5. Remove the old memory module if you are adding more memory to the system.
6. Carefully insert the new memory modules in the slots with correct orientation.
7. Turn on the computer and verify the total system memory from the BIOS self-test.

Installing an Adapter Card

1. Obtain a new adapter card and ensure that it is compatible with the system bus.
2. Ensure that the adapter driver is compatible with the installed operating system.
3. Find an empty expansion slot on the motherboard.
4. Insert the new card carefully and tighten the screw.
5. Turn on the system to see whether the operating system automatically detects the new adapter.
6. If the card is not a PnP device, or if the OS does not recognize the adapter, install the device driver manually using Add Hardware wizard.
7. Use the Device Manager to verify that the card is working as expected.

Visual Inspection of Internal Components

1. Inspect all external connectors to ensure that they are attached properly.
2. Inspect the LEDs on front panel of the system.
3. Inspect the LEDs on the adapter cards on the rear panel of the system.
4. Turn off the computer and open the computer case.
5. Perform a thorough visual inspection of all components.
6. Ensure that all adapters and memory modules are seated properly in their appropriate slots.
7. Ensure that all connectors are properly attached.
8. Verify that the CPU fan is working and that there is no dust accumulated.
9. Verify that all ventilation slots are clean.

Audible Codes

1. Check the make and model of the motherboard and obtain its user manual.
2. Note down the BIOS manufacturer's name and the version number of the BIOS software.
3. Turn on the computer and listen carefully to the beeps during the Power-On Self-Test (POST).
4. Note down the number of beeps and whether they are long or short.
5. Check the meaning of the beep codes from the user manual.

Testing the Power Supply DC Output Voltages

1. Open the computer case.
2. Locate an unused power supply cable.
3. Turn on the computer and measure all DC voltages using a multimeter.

Starting the Computer with Minimum Configuration

1. Open the computer case and write down all add-on components.
2. Find out which components or adapters are rarely used or not necessary and can be removed.
3. If you need to reinstall the adapters, obtain drivers for each of them.
4. Remove all these components one by one.
5. Restart the system without any of these components and note down the startup behavior.
6. Turn off the system.
7. Install the components one at a time along with its driver (if required) and restart the computer.

Adding/Removing Laptop-Specific Components

1. Obtain a USB thumb drive or other USB-compatible device for the laptop.
2. Turn on the laptop and connect the drive to a free USB port.
3. Verify that the operating system automatically recognizes and configures the device.
4. Locate the small icon that appears in the notification area of the Taskbar.
5. Right-click the icon and click Safely Remove Hardware.
6. Check the list of devices and click Stop to stop the USB device.
7. Remove the device carefully.

Connecting External Devices

1. Obtain a USB mouse and a USB keyboard.
2. Connect the mouse and the keyboard to the laptop using free USB ports.
3. Check that the devices are working.
4. Obtain a color monitor and connect it to the monitor port on the rear panel of the laptop.
5. Verify that the monitor is recognized and works as expected.

Connecting a Laptop to a Wireless Network

1. Obtain a laptop with a built-in or add-on wireless network adapter.
2. Ensure that the network adapter supports the type of available wireless network.
3. Bring the laptop within the coverage area of the wireless network.
4. Verify that the laptop detects the wireless network.
5. Open the Control Panel and configure the wireless settings from the properties of the wireless adapter.

Using the Windows Command Prompt

1. Open the Run dialog box from the Start menu.
2. Type `cmd` and press the Enter key.
3. Type `help` in the command prompt window to view a list of available commands.
4. Type `attrib /?` and press the Enter key to get help with the syntax of this command.
5. Display a directory listing using the `dir` command.
6. Copy a file from one folder to another using the `copy` command.
7. Make a directory using the `md` command and copy a few files to this directory using the `copy` command.
8. Remove the new directory using the `rd` command.
9. Click the icon on the top, lefthand corner of the window and click Properties.
10. Change the properties of the command prompt window.
11. Type `exit` and press the Enter key to close the command prompt window.

Creating New Folders

1. Open Windows Explorer and navigate to a folder.
2. Right-click an empty space, click New, and select Folder.
3. Type the name of the new folder.
4. Create a few subfolders within the new folder by repeating steps 2 and 3.

Changing File/Folder Attributes

1. Open Windows Explorer and navigate to a folder.
2. Right-click the folder and select Properties.
3. View the attributes of the folder.
4. Click the Read-Only or Hidden checkboxes to change the folder attributes.
5. Verify that the hidden folder is not visible in Windows Explorer.

Disk Partitioning and Formatting

1. Right-click My Computer and select Manage to open the Computer Management Console.
2. Navigate to the Disk Management snap-in.
3. View the existing disk partitioning information.
4. Create a new partition in the unused disk space.
5. Format the new partition using the NTFS filesystem.
6. Verify that the status of the new partition is shown as “Healthy.”

Converting a Disk from FAT to NTFS

1. Open the Disk Management snap-in.
2. Select a disk partition formatted with the FAT filesystem and write down its drive letter.
3. Open the Windows command prompt from the Run dialog box in the Start menu.
4. Use the *convert* command to convert the partition from FAT to NTFS.
5. Open the Disk Management snap-in to verify that the partition has been converted to NTFS.

Using Disk Maintenance Tools

1. Open the Disk Management snap-in.
2. Select a partition and open its Properties window.
3. Click the Tools tab to view the available disk maintenance tools.
4. Click Defragment Now to defragment the disk.
5. Examine how the disk analysis and defragmentation takes place.

Examining System Startup Environment

1. Open the Run dialog box from the Start menu.
2. Type `msconfig.exe` and press the Enter key.
3. The System Configuration Utility window is displayed.
4. Navigate through different tabs to examine the system startup settings.

Configuring Virtual Memory

1. Open the System Properties window from the Control Panel.
2. Click the Advanced tab and click Settings under Performance.
3. Click Advanced and then click Change in the Virtual Memory section.
4. Change the Initial Size and Maximum Size settings by selecting each disk drive.

Changing the System Startup Settings

1. Open the System Properties window from the Control Panel.
2. Click Advanced and then click Startup And Recovery.
3. Change the Default Operating System to another installed operating system.
4. Change the Time To Display List Of Operating Systems.

Using Event Viewer

1. Right-click My Computer and select Manage to open the Computer Management Console.
2. Navigate to the Event Viewer snap-in.
3. Examine the Application, Security, and System folders.
4. Double-click a number of log entries to view the details.

Using Task Manager

1. Right-click the Taskbar and open the Task Manager.
2. Notice the CPU usage and number of running processes.
3. Click the Processes tab and examine the usage for the CPU, paging file, and memory.
4. Open some applications and examine the CPU, paging file, and memory usage again.
5. Select running applications one by one and click End Task.
6. Click the Networking tab and examine the percentage of network utilization.

Using Device Manager

1. Right-click My Computer and select Manage to open the Computer Management Console.
2. Click the Device Manager snap-in.
3. Examine the installed devices and their properties.
4. Examine any device flagged as Unknown or unrecognized device.
5. Click View and select Resources by Type.
6. Click View again and select Resources by Connection.

Accessing Advanced Boot Options

1. Restart the computer and press F8 to access the Advanced Boot menu.
2. Navigate through the menu options.
3. Select Safe Mode from the available options and press the Enter key.
4. Examine how Windows starts in Safe Mode.
5. Disable the network adapter and restart Windows.
6. Select the Safe Mode with networking this time and verify whether you can connect to the network.
7. Enable the network adapter and restart the computer.

Enabling Automatic Updates

1. Open the System properties window from the Control Panel.
2. Click the Automatic Updates tab.
3. Enable Automatic Updates.
4. Configure Automatic Updates to download automatically but to prompt you before installation.

Connecting the Printer to a Local Port

1. Obtain a parallel printer and its driver.
2. Connect the printer to the computer using a centronics cable.
3. Turn on the printer and see whether the operating system detects it.
4. Open the Printers and Faxes window from the Control Panel in the Start menu.
5. Use the Add Printer Wizard to install the printer.
6. Select the Have Disk option to install the printer driver manually.
7. Print a test page to verify that the printer is correctly installed.

Configuring and Verifying TCP/IP Properties

1. Open Network Connections from the Control Panel.
2. Use the New Connection Wizard to add a network connection.
3. Open the Properties window of the new connection.
4. Select the Internet Protocol (TCP/IP) and click Properties.
5. Verify that the Obtain an IP Address Automatically and the Obtain DNS Server Address Automatically options are selected.
6. Click Use the Following IP Address and enter a valid IP address, subnet mask, and default gateway address.
7. Close the TCP/IP Properties window.
8. Ping the loopback address 127.0.0.1 to verify that the TCP/IP configuration is working.
9. Change the TCP/IP settings back to automatic.

Testing Network Connectivity

1. Examine the status indicators on the network adapter.
2. Open the command prompt window.
3. Ping the loopback address 127.0.0.1 and examine the output.
4. Ping the IP address of a computer on the local network segment and examine the output.
5. Ping the IP address of the default gateway and examine the output.
6. Ping the IP address of a remote host and examine the output.

Configuring Share Permissions

1. Open Windows Explorer and navigate to a shared folder.
2. Right-click the folder and select Sharing and Security.
3. Click Permissions and examine the configured share permissions.
4. Examine what share permissions are available for configuration.
5. Add a few users and groups and configure different share permissions for each.

Enabling and Configuring Windows Firewall

1. Log on to a Windows XP computer and open the Windows Firewall from the Control Panel.
2. Click the ON radio button to turn on the firewall.
3. Click the Advanced tab to open advanced firewall settings for the network adapter.
4. Select the checkbox for the shown network adapter and click Settings. Note that all services are disabled by default.
5. Select the services that you want to allow.
6. Click the checkboxes for ICMP messages that you want to allow from the ICMP tab.

Viewing Access Permissions

1. Open Windows Explorer and select a shared folder.
2. Examine Share Permissions from the Sharing tab.
3. Examine what share permissions can be configured for users and groups.
4. Examine NTFS permissions from the Security tab.
5. Examine what NTFS permissions can be configured for users and groups.
6. Examine what special NTFS permissions are available.

Configuring Auditing and Logging

1. Open the Local Security Policy from Administrative Tools in the Control Panel.
2. Enable the audit policy for Object Access.
3. Select both Success and Failure events.
4. Open Windows Explorer and select a folder to enable auditing.
5. Open the Properties window for the folder and click the Advanced tab.
6. Click the Auditing tab and add audit entries.

Viewing the Local Security Policy

1. Open the Local Security Policy folder in the Administrative Tools located in the Control Panel.
2. Examine the settings for Account Lockout Policy and the Password Policy.
3. Examine the Audit Policy settings.
4. Examine the settings for Security Policy and User Rights Assignment.

Highlighters Index

In this section, we've attempted to compile the facts within the exam's subject areas that you are most likely to need another look at—in other words, the areas of study that you might have highlighted while reading the Study Guide. The title of each highlighted element corresponds to the heading title in the Study Guide A+ Exams. In this way, if you have a question about a highlight, you can refer back to the corresponding section in the Study Guide. For the most part, the entries under a heading are organized as term lists with main points that you need to memorize for the exam.

Personal Computer Components

This subsection covers a summary of highlights from the "Personal Computer Components" section in the A+ Exams Study Guide.

Adding, removing, or upgrading computer components

- Follow standard procedures when performing repairs or upgrades.
- Use compatible components and follow the vendor's instructions.
- Use appropriate tools.
- Take ESD precautions.

Selecting a storage device

- The storage device should be compatible with the existing computer hardware.
- The Computer BIOS must support the type of device you are going to install.
- The operating system should be able to use its full storage capacity.
- Make sure that you have provisions in the existing system for adding another device.
- Check the return/refund policy and after-sales support.

Installing a hard disk

- Set the jumpers on the hard disk to configure it for Cable Select, Master, or Slave.
- Select the primary or secondary hard drive cable (IDE cable) and appropriate connector.
- Carefully remove the previously installed drive by removing the connectors and then its screws.

- Connect the new drive with the correct data and power cables.
- New drives must be partitioned and formatted before they can be used.

Selecting a motherboard

- Your selection must meet or surpasses the requirements.
- Check the technical details of the board, such as the chipset used, the speed of the system bus and the type of memory modules (RAM).
- The system bus speed determines how fast the data is transferred on different parts of the computer.
- Check the amount of onboard memory and the maximum supported memory, and whether there is a provision to add memory when required.
- Check what components live onboard and what features will require add-on cards.
- Check how many expansion slots are available for add-on cards (adapters).
- Check the type and number of available I/O ports.
- If the computer is to be used for graphics applications, check the amount of video RAM available on the motherboard.

Installing the motherboard

- Keep the new motherboard in its protective cover until you are ready to install it.
- Consult the motherboard manual for specific installation instructions.
- Wear an antistatic wrist strap and use an antistatic table mat.
- Remove the old motherboard carefully and put it aside.
- Clear the area of all power and data cables.
- Hold the new motherboard from its sides only and do not touch any components to avoid damage by static discharge from your body.
- Make sure that the screws can be fixed at appropriate locations (called *standoffs*).
- Secure the motherboard to the case by using proper screws to complete the physical installation.
- Connect the power cable, speaker cable, reset switch cable, hard disk LED, and other LED cables.

Installing a power supply

- Select a power supply with correct voltage and current ratings.
- Ensure that the power supply will fit into the computer case.
- Turn off the computer and remove the power cord from the wall socket.
- Let the computer cool down for about 15 minutes.
- Remove the power supply connectors from the motherboard and disk drives.
- Determine whether you will need to remove additional adapters to safely remove the power supply unit from the case.
- Remove the power supply unit gently so that it does not hit any internal parts of the computer.

- Place the new power supply in the computer case and tighten the screws on the rear panel.
- Connect all connectors back one by one. Do not use force.
- Replace the front panel of the computer after connecting the power switch.
- Reconnect the power cable and turn on the computer to test that the new power supply unit is functioning as expected.

Installing a CPU

- Always wear an antistatic wrist strap.
- Read the installation instructions that came with the new CPU.
- Examine the existing CPU and the type of socket.
- Some CPUs come pre-installed with a heat sink and a cooling fan.
- Examine whether the heat sink and fan can be removed safely and reinstalled on the new CPU.
- Most CPU sockets have a lever on one side that frees the CPU from the socket.
- Pull the CPU socket lever gently to loosen the CPU from the socket. Remove the CPU carefully and put it aside in a protective cover.
- Examine the small pinholes on the socket to find out the orientation of the CPU.
- Hold the new CPU from its edges only, in the correct direction.
- Place the CPU in the socket with the correct orientation.
- Push the socket lever down gently to secure the CPU in the socket.
- Use the thermal conductive compound for installing the heat sink.
- Place the heat sink and the fan assembly on top of the CPU and lock it in place.
- Connect the cooling fan wires to the appropriate connector on the motherboard.

Upgrading RAM

- Check the motherboard user manual to see the type and maximum amount of RAM supported.
- Ensure that there is provision for expanding memory on the motherboard.
- Ensure that the new modules are compatible with the existing ones.
- Keep the memory sticks in their protective covers until you are ready to install them.
- Always wear grounded antistatic wrist straps.
- Remove the old memory sticks carefully by releasing the side levers.
- Hold the new memory stick in the correct orientation, align it to the socket, and push it down firmly using your two thumbs.
- Push the levers back into their place.

Installing adapter cards

- Check the type of expansion slots available in the computer.
- Check that the adapter driver is supported by system BIOS and the operating system.
- Check whether the new adapter is PnP-compatible.
- Check with the vendor whether an upgraded device driver is available.
- Find an empty expansion slot that is easily accessible.
- Remove the slot cover from the computer case using long nose pliers.
- Insert the adapter in the selected expansion slot and push it gently so that it sits well in the slot.
- Turn on the computer to see whether the BIOS and operating system recognize the adapter.
- If the adapter is not PnP-compatible or the system BIOS does not support PnP, test the adapter by installing its device driver.

Basic diagnostic procedures

- Visual inspection involves verifying that all cables and connectors are properly attached and that adapters and memory modules are seated properly.
- Inspect the LED indicators on the front panel and on the adapter cards.
- Audible inspection refers to beep codes generated by the computer BIOS when the computer is powered on.
- Start the computer with the minimum configuration and add components one by one to diagnose problems.
- Verify proper installation of components.
- Verify that correct device drivers are installed.
- Verify that there are no resource conflicts.
- Verify that the devices are configured properly.

Laptop and Portable Devices

This subsection covers a summary of highlights from the “Laptop and Portable Devices” section in the A+ Exams Study Guide.

Communication technologies for laptops

- Bluetooth provides ad-hoc short-range (up to 10 meters) communications between laptops.
- Bluetooth transmission speeds range from 1 to 3 Mbps and work in the frequency range of 2.4 GHz.
- Infrared technology provides point-to-point wireless communications between two devices using a direct line of sight.
- Infrared supports data transfer speeds from 10 to 16 Mbps.
- A cellular wireless network is made up of a large number of radio cells.
- Laptops can also be connected to wired networks using Ethernet technologies with built-in or add-on network adapters.

Power supplies

- Laptops can be operated with the AC main supply or with a battery.
- The milliAmp-Hour (mAH) rating noted on top of the battery pack indicates the capacity of the battery.
- Nickel Cadmium (NiCd) batteries suffer from memory effect, which reduces overall battery life.
- Lithium Ion (LiIon) batteries are lightweight and have longer life.
- LiIon batteries last for about three to four hours when fully charged.
- LiIon batteries do not suffer from the memory effect.
- Nickel Metal Hydride (NiMH) batteries last longer and have less memory effect than NiCd batteries.

Improving battery performance

- Recharge batteries on unused laptops after removing them from storage.
- Fully discharge and then charge a battery every two to three weeks.
- Battery conditioning helps prevent memory effect in batteries (except the LiIon battery).
- Lower the brightness of the LCD and turn it off when not in use.
- Add more RAM to reduce the use of the hard disk for temporary storage, which draws more battery power.
- Avoid playing games or watching videos on laptops.
- Remove unneeded external peripherals that draw power from the laptop.
- Use Power Options in Windows OS to configure standby and hibernate modes.
- Use the power management features in the laptop's BIOS.

Components of LCD

- An Active Matrix LCD display is also known as a Thin Film Transistor (TFT) display.
- The LCD screen is made up of two polarized materials with liquid crystal solution between them.
- The LCD backlight is a cold cathode fluorescent tube (CCFT) or cold cathode fluorescent light (CCFL).
- The inverter provides the power supply to the backlight.
- The video controller controls the display on the LCD screen.

Installing and removing devices

- Internal devices include battery, memory modules, modems, hard disks, and CD/DVD drives.
- External components include the battery pack, battery adapter (charger), and other components connected to USB ports, such as the external CD/DVD drive, hard disks, and PCMCIA cards.
- PnP devices are automatically detected and configured.
- Use the Safely Remove Hardware feature to remove PnP devices.

- Hot-swappable devices are PnP-compatible and can be plugged into a port while the laptop is powered on.
- To install or remove a non-PnP or non-hot-swappable device, you must first turn off power, install/remove the device, and then turn on power again.

Upgrading memory

- The laptop must have additional memory slots to support upgrades.
- Refer to the documentation or call the vendor support for instructions on how to upgrade memory.
- The memory module should be compatible with the make and model of the laptop.
- Always wear an antistatic wrist strap when working inside the laptop.
- On Windows OS, you can verify the upgraded memory from the System Properties page in the Control Panel.

Power problems

- Verify that the main power cord is properly attached.
- Check the LEDs on top of the adapter.
- A warm adapter surface is an indication of a working adapter.
- Verify that the DC power cord is not damaged and that the connector is properly inserted into the laptop.
- Remove the DC power cord from the laptop and measure the DC power output of the adapter.
- If there is no output or a low DC output, the AC is properly connected, and the LED is lit, try replacing the adapter with a new one.

Troubleshooting

- Use external devices with toggle function keys to diagnose problems with a touch pad, keyboard, or screen brightness.
- Check the cut-off switch to diagnose problems with backlight.
- Keep the exhaust fans free of dust to prevent problems generated by the internal heating of laptop components.
- Check SSID settings and/or move the laptop within the coverage area of a wireless network to diagnose network connectivity problems.

Operating Systems

This subsection covers a summary of highlights from the “Operating Systems” section in the A+ Exams Study Guide.

Command-line utilities

- The *attrib* command is used to display or change the attributes of a file or folder.
- The *edit* command is a 16-bit MS-DOS command used to edit text files.
- The *copy* command is used to copy one or more files and folders from one location to another.

- The *xcopy* command is used to copy multiple files, directories, and subdirectories simultaneously from one location to another.
- The *format* command is used to format a disk partition or a floppy disk.
- The *md* (or *mkdir*) command is used to create a new directory.
- The *rd* (or *rmdir*) command is used to delete a directory.
- The *cd* (or *chdir*) command is used to change the working directory when using the command prompt.
- The *ipconfig* command is used to display and change the TCP/IP configuration on a computer.
- The *ping* command is used to test connectivity between two TCP/IP hosts.

Hard disks

- Basic disks are the traditional type of disks used in computer systems.
- Dynamic disks are specifically converted from Basic disks using the Disk Management utility.
- Each Basic disk can have up to four primary partitions, or three primary and one extended partition.
- Only one Primary partition can be marked as an Active Partition; this is used to boot the system.
- An Extended partition is used to create logical drives and assign them drive letters.
- Extended partitions cannot be formatted and cannot be assigned drive letters.
- Logical partitions are created inside the extended partitions.

Creating partitions

- Partitions and volumes are managed using the Disk Management snap-in.
- You can also use the *diskpart* command-line utility to create and delete partitions.
- Open the Disk Management snap-in and right-click the unallocated space where you want to create a partition.
- You can create Primary, Extended, or Logical partitions using the New Partition Wizard.
- Specify the size of the partition when prompted.
- Select the drive letter or path when prompted.

Formatting a partition or volume

- Partitions can be formatted using FAT, FAT32, or NTFS filesystems.
- You can format the partition when or after you create it.
- You can also use Windows Explorer or the *format* command to format a partition.

Changing file or folder attributes

- Use Windows Explorer or the *attrib* command to change file or folder attributes.
- File and folder attributes include system (S), hidden (H), read-only (R), and archive (A).

- Open the Properties page of the file or format to change attributes.
- Click the checkbox to set the attributes or clear it as required.
- Click the Advanced button to set advanced attributes such as encryption and compression.

Disk Defragmenter

- Disks become fragmented after continuous usage.
- Fragmentation causes files to be stored at noncontiguous locations inside the disk.
- Disks should be defragmented to improve performance.
- The Disk Defragmenter tool can be accessed from the Disk Management snap-in or from the System Tools folder in the Start menu.
- The defragmentation process automatically analyzes disks.

Check Disk

- The Check Disk utility checks hard disks for filesystem errors.
- It also scans and attempts to recover bad sectors on the disk.
- You can access the Check Disk utility from Windows Explorer or from the System Tools menu under Accessories.
- You can also run the *chkdsk* command to start the utility.
- The Automatically Fix File System Errors option allows you to scan the disk for filesystem errors and fix them automatically.
- The Scan For and Attempt Recovery of Bad Sectors option allows you to scan and fix bad sectors on the hard disk.

Windows Backup

- You can access the Windows Backup utility from the System Tools folder under Accessories in the Start menu.
- You can also start this utility by running the *ntbackup* command.
- You must be a member of the Administrators group to backup or restore files or directories.
- The Backup Files and Directories user right also allows users to perform backups.
- The Restore Files and Directories user right allows users to perform restores.
- You can perform a Normal, Full, Copy, Differential, or Incremental backup.
- Backups can be scheduled to run at off-peak hours.
- Files or folders can be restored at the original location, an alternate location, or a single folder.

Device Manager

- The Device Manager utility is used to manage hardware devices and drivers.
- It gives a snapshot of all installed devices in the system.
- Unrecognized or malfunctioning devices are flagged with a yellow question mark.

- A black exclamation point (!) on a yellow field indicates the device is in a problem state (it may still be functioning).
- The View menu allows you to list devices by type and by connection, and to list resources by type or by connection.
- The Driver Details button displays information about driver files.
- The Update Driver button allows you to update a device driver.
- The Roll Back Driver button allows you to revert to the previously working device driver.
- The Uninstall Driver button is used to remove a device driver.

Task Manager

- The Task Manager utility displays real-time information on applications, processes, performance, and networking.
- You can start programs and stop nonresponsive processes and applications.
- The Applications tab displays applications currently running on the system.
- The Processes tab displays all application and system processes currently running.
- The Performance tab displays a real-time graphical view of system performance.
- The Networking tab shows real-time network performance and utilization.

msconfig

- The *msconfig* command-line tool opens the System Configuration utility.
- This tool displays the system configuration and allows you to safely change systems settings.
- You can change system startup and the *BOOT.INI* file, and manage services and applications that automatically start.

REGEDIT and REGEDT32

- The *regedit.exe* and *regedt32.exe* commands are used to edit Windows Registry settings.
- The Registry stores OS settings, user specific settings, application data, hardware components, and configuration of installed device drivers.
- HKEY_CLASSES_ROOT, HKEY_CURRENT_USER, HKEY_LOCAL_MACHINE, HKEY_USERS, and HKEY_CURRENT_CONFIG are subkeys of the Registry.
- You should first make a backup copy of the existing Registry files before you edit them.

Event Log

- The Event Viewer displays error messages, warnings, and other information about system activities.
- Log Filtering allows you to search for specific events.
- The Application Log contains errors, warnings, or other information generated by application programs.

- The Security Log displays information about security-related events.
- The System Log contains errors, warnings, and information about system events.

System Restore

- The System Restore in Windows XP desktops helps restore the system to a working state.
- You can use the System Restore utility for troubleshooting an unstable system.
- It uses system restore points to store a snapshot of system settings at regular intervals.
- It is located in the Help and Support Center, or it can be accessed from System Tools under Accessories in the Start menu.

Remote Desktop

- Remote Desktop allows you to get access to a remote computer and control it from your computer.
- It requires terminal services to be running on both computers.
- It is available only in Windows XP and Windows Server 2003 computers.
- Use it when it is not possible to personally visit a computer to resolve a problem.
- Incoming connections are configured from System Properties in the Control Panel.
- To connect to a remote system, use the Remote Desktop Connection from the Accessories folder in the Start menu.

Virtual Memory

- Windows temporarily stores data in the hard disk when the amount of RAM is running low.
- The hard disk space used for this purpose is called Virtual Memory or the paging file.
- The OS automatically sets the paging file and optimizes it for best performance.
- You can manually increase or decrease the size of the paging file from the System utility in the Control Panel.

System Startup Optimization

- Disable unused system services or set their startup type as manual.
- Use the *msconfig* utility to remove applications configured as autostart with the system.
- Remove any unused applications using Add or Remove Programs in the Control Panel.
- Disconnect all unused mapped network drives.
- Defragment disks periodically using the Disk Defragmenter.
- Remove temporary system, application, and Internet files regularly using the Cleanup utility.

Advanced Boot Options

- In Safe Mode, Windows loads with minimum basic system services and device drivers just sufficient enough to boot the operating system.
- Safe Mode with Networking includes networking to the Safe Mode.
- Safe Mode with Command Prompt loads the command interpreter.
- The Last Known Good Configuration allows you to return to the previous working configuration.

Recovery Console

- The Recovery Console is used to repair corrupt or missing system files.
- You can copy original files from the setup CD-ROM.
- You can also enable or disable services that might be causing startup problems.
- The Recovery Console can either be started from the Windows setup CD-ROM, or it can be installed as one of the Advanced Boot Options.

Automated System Recovery (ASR)

- ASR is used to restore the system when there is a major failure.
- The ASR Wizard is located in the Backup utility.
- You need a blank floppy disk and a full backup of the system partition.

Application failures

- Critical application errors can freeze the system or restart it automatically.
- Application errors can be caused by an incorrect configuration or runtime problems.
- Test the applications thoroughly after installation.
- Install only OS-compatible applications.
- Fine-tune application performance by setting its priority.
- Keep the application updated using the latest updates from the vendor.
- Educate and train users for correct usage of the application.

Missing Boot Disk and Missing NTLDR errors

- The Missing Boot Disk or Invalid Boot Disk error appears on computers that are configured to use a floppy disk or a CD-ROM drive as the first boot device.
- The Missing NTLDR error appears if the *NTLDR*, *NTDETECT.COM*, or *BOOT.INI* file is missing or has become corrupt.
- These files can be restored using a boot disk from the Recovery Console or using the System Restore utility.

Preventive maintenance

- Use software updates to keep the OS and applications up to date.
- Use Windows Update to automatically download and install critical updates.
- Back up data and system files regularly.
- Install antivirus software and keep it updated with the latest virus signatures.

Printers and Scanners

This subsection covers a summary of highlights from the "Printers and Scanners" section in the A+ Exams Study Guide.

Printing and scanning terms

- Resolution refers to the quality of the image printed or scanned.
- It is measured in dots per inch (dpi).
- The higher the resolution of a printer or a scanner, the lower its speed.
- *Speed* refers to the number of pages or lines printed per minute.
- The printing speed of laser and inkjet printers is represented as pages per minute (ppm).
- The speed of dot matrix, line, and daisy wheel printers is represented as characters per second (cps).

The printing process

- Print jobs submitted by Windows XP/2000 have the enhanced metafile (EMF) data type.
- The RAW data type is ready to print format.
- The printing application calls the Graphics Device Interface (GDI), which further calls the printer driver.
- The GDI and the printer driver convert the document format into printer language.
- This data is passed on to the print spooler with the help of a local print provider.
- The print spooler is a special folder on the hard disk that holds print jobs in a queue.
- The print processor identifies the data type and receives and converts the print job according to its data type.
- The control is assigned to the separator page processor, which adds a separator page.
- The print job goes from the print spooler to the print monitor.
- The print job is passed on to a port monitor that sends it to the printer.
- The printer converts the print job into a bitmap format and prints it.

Laser printing process

- In the cleaning step, the EP drum is cleaned of toner particles by a rubber blade.
- In the conditioning step, the drum is charged with a high negative voltage (–600 to –1000 volts) by the primary corona wire.
- In the writing step, parts of the drum surface are stripped of some negative charge according to the image.
- In the developing step, toner is applied to parts of the drum surface, which has the lesser negative charge.

- In the transferring step, the drum is rolled over paper, which is positively charged by the transfer corona wire. Negatively charged toner particles are transferred to paper, leaving an image on it.
- In the fusing step, the paper is passed through pressure and heating rollers in the fuser assembly to firmly bond the toner particles to paper.

The inkjet printing process

- The printhead is cleaned to ensure that there is no residual ink.
- A stepper motor in the paper feed assembly pushes a sheet of paper into the printer.
- The belt attached to the stepper motor moves the printhead back and forth.
- The printhead leaves drops of ink at different spots on the paper according to the image.
- The printhead moves to the next line.
- After the printing is over, the printhead moves to its home position.

Solid ink printers

- Solid ink printers use sticks of solid ink.
- The ink is melted and fed into printheads.
- Solid ink printers can print on a variety of paper and transparencies.
- The image quality is superior to other printing technologies.
- These printers are easy to use and maintain.
- Solid ink protects the environment due to reduced waste output.

Thermal printers

- Thermal printers work by pushing heated printhead pins against heat-sensitive paper, called *thermal paper*.
- Thermal printers use a combination of dots to create the image on the paper.
- Thermal wax transfer printers use wax-based ink, which is melted from the ribbon and transferred to the paper to create images.

Impact printers

- Dot matrix, line printers, and daisy wheel printers are all impact printers.
- Impact printers use a head or a needle, which is stroked against an ink ribbon to place a mark on the paper.
- These printers produce significant noise.
- These printers are very efficient for printing multipart forms.

Dot matrix printers

- Dot matrix printers use a printhead containing 9 or 24 pins.
- These pins strike on an ink ribbon that makes an impression on paper.
- The printhead controller sends electrical signals and forces pins to strike against the ink ribbon.
- The impression appears as a matrix of dots to form characters on paper.

Types of scanners

- Flatbed scanners use a glass platform where a paper is placed face down. A motorized belt moves a lamp to scan the image.
- In handheld scanners, the scanner is moved across the image.
- In sheetfed scanners, the paper is moved over a scanning lamp.
- Drum scanners are used for high-end applications. The image is placed over a drum, and photomultiplier tubes (PMT) are used to convert optical signals into electrical signals.

The scanning process

- The user places the document with its face down on the glass plate.
- The document is illuminated by a cold cathode fluorescent lamp (CCFL).
- The scanning head is moved across the surface of the document using a belt attached to the main stepper motor.
- When the entire document is scanned, the scanner is said to have completed one pass.
- The image is passed through a set of reflective mirrors and focused onto a lens.
- The lens passes the image to an array of charged coupled devices (CCD) through an image filter.
- The scanner driver passes the image to the application software used to acquire the image from the scanner.
- The application (Photoshop, Corel Draw, etc.) uses a standard language, such as *TWAIN*, that acts as an interpreter between the scanner and the application.

Verifying printer compatibility

- The printer's compatibility with the OS ensures that documents will be correctly formatted before being sent to the printer.
- The printer's compatibility with the application software ensures that the application can successfully use the device.
- You can check compatibility from the printer documentation or from the vendor's web site.
- Manufacturers test their printers and drivers with a variety of operating systems and applications.

Installing a local printer

- Printers connected to the local computer or directly to a network port are installed as local printers.
- Local printers can be attached to a parallel port (LPT1) or a USB port.
- Use the Add Printer Wizard in the Printers and Faxes folder to install the printer.
- Click the Local Printer Attached to This Computer button in the Local or Network Printer page.
- Select a port in the Select a Local Port page.

- Click Automatically Detect and Install My Printer if the printer is PnP-compatible.
- For non-PnP-compatible printers, select the Have Disk option to install the printer driver.

Installing a network printer

- A printer attached to a print server is installed as a network printer.
- Click the Network Printer button in the Local or Network Printer page.
- Type the name of the server and the printer share name in the `\\Print_Server\Printer_Share` format.

Educating users

- Most printer and scanner problems occur due to lack of user training.
- Educate and train the users about the main features of the printers or scanners.
- Show them how to select an appropriate printer from within an application.
- Show them how to select paper from the available paper trays/sizes.
- If printers are leased and charged on a per-page basis, it is useful to tell the users to carefully select black and white and color prints.
- Train the users on how they can manage their own documents from their desktops.
- Teach users about keeping the area around the printers clean.
- Encourage the users not to attempt fixing problems themselves.

Upgrading printer memory

- High-end printers require large amounts of RAM.
- Printer memory can be upgraded by installing additional memory modules.
- Obtain memory modules directly from the printer manufacturer to avoid problems.
- If upgrading printer memory yourself, follow the manufacturer's instructions on how to do so.

Updating printer and scanner drivers

- New versions of drivers should be thoroughly tested.
- Drivers can be updated using the Device Manager.
- Click the Drivers tab to install an updated driver for a scanner.
- You can upgrade a printer driver from the Advanced tab of the Printer Properties page.
- This option starts the Add Printer Driver Wizard.

Printer and scanner performance

- The default configuration of most printers and scanners provides optimum performance.
- The Properties page of a printer or scanner can be used to fine-tune its performance.
- Use of correct image formats enhances performance levels.
- When you increase the printing or scanning resolution, the speed decreases.

Resolving printing problems

- You must gather information about a problem before reaching a conclusion.
- Printing problems can be due to hardware, software, or user errors.
- A user may not have sufficient permissions, his computer may not be connected to the network, or he may be sending the print job to a wrong printer.
- You must verify that the printer is online and not out of paper.
- Try printing from a different computer or using a different application.
- Use test patterns to test the quality of the printed image.

Preventive maintenance of printers and scanners

- Scheduled maintenance helps prevent several problems and improves the life and performance of printers and scanners.
- Printers and scanners should be located in environments where temperature and humidity are controlled.
- The area around these devices should be kept clean.
- Manufacturer-recommended paper supplies only should be used.
- Refilled inkjet and toner cartridges do not produce good quality images.
- When required, use only recommended replacement spares.

Networks

This subsection covers a summary of highlights from the "Networks" section in the A+ Exams Study Guide.

Installing and configuring a network adapter

- Ensure that the adapter is compatible with computer hardware and the OS.
- Check whether the adapter is PnP-compatible.
- Obtain the adapter driver if the OS does not automatically install it.
- Manual configuration includes setting parameters such as IRQ, I/O, and DMA.
- You can use the Add Hardware Wizard to install the network adapter.
- The Device Manager can be used to install or upgrade a driver for the installed adapter.

Joining a Windows workgroup or domain

- You can join a workgroup or a domain during installation of the OS.
- After installation, the computer can be joined to a workgroup or a domain from the System tab inside the Control Panel.
- You will need administrative privileges to join a domain.
- The DNS name of the domain is required.
- A DNS server and a domain controller must be available to validate your credentials.

Joining a NetWare network

- You need supervisor rights to join a computer to a NetWare network.
- You must know the internal network number, directory context, and the name of the directory tree.
- Configure the user's desktop with context and tree names, as a user may find these difficult to remember.

NTFS permissions

- File and folder permissions are assigned from the Properties window.
- NTFS permissions are available only on NTFS partitions.
- FAT partitions support only share permissions.
- Permissions can be set to Allow or Deny an object.
- Administrators and owners of an object have full control permissions on an object.

Configuring script settings

- JavaScript, ActiveX controls, and cookies are client-side components of Internet services.
- These components are downloaded from the web server and run on the client computer.
- Support for scripts is configured on a Windows computer from the Security tab available in Internet Options.
- Custom level security settings allow you to configure settings as required.

Configuring proxy settings

- Internet browsers can be configured to connect to the Internet directly or through a proxy server.
- A proxy server is used to share a single Internet connection among multiple network users.
- It provides better performance by caching frequently visited web pages.
- Open the Connections tab in Internet Options to configure the computer to use a proxy server.
- Click the LAN settings button and enter the IP address of the proxy server.

Network troubleshooting utilities

- *ipconfig* is used to test the TCP/IP configuration of a computer.
- *ping* is used to test connectivity between two hosts.
- *tracert* is used to trace the route taken by a data packet from the source to the destination.
- *nslookup* is used to resolve name resolution problems.

Troubleshooting tools

- Cable testers are used to test whether the cable is working properly.
- Tone generators and tone locators are used to test cables by means of audio signals.

- Loopback connectors are used to test functionality of network ports.
- An optical time domain reflectometer (OTDR) is used to test fiber optic cables.

Adapter configuration problems

- Improperly configured protocol or port settings cause networking problems.
- Network adapters use system resources such as IRQ, I/O address and DMA.
- These resources must not be in conflict with other devices.
- Use the System Information utility to find out resource conflicts.
- Driver problems can be resolved using the Device Manager.
- The Device Manager allows you to update, uninstall, or rollback drivers.

TCP/IP configuration problems

- The network adapter must have a valid IP address, subnet mask, and gateway address.
- The chance of assigning an incorrect IP address increases when clients are configured with static addresses.
- A DHCP server can prevent the duplication of IP addresses by automatically allocating IP addresses.
- DNS and WINS addresses must also be correct to prevent name resolution problems.
- You can ping the loopback address of the adapter to verify TCP/IP protocol.

IPX/SPX configuration problems

- The internal network number must be unique for every host.
- The network number must be the same for all hosts in a network.
- A correct frame type must be configured on every host that needs manual configuration.

Problems with resource access permissions

- A user who wants to access a resource must be granted sufficient permissions.
- Reading and executing a file needs the Read and Execute permission.
- Saving files or folders requires at least the Write permission.
- Changing file ownership or modifying permissions needs Full Control permissions.
- Conflicting group permissions can also prevent access to resources.
- Conflicts in share and NTFS permissions can also deny access to a user who otherwise should have it.

Electrical interference

- Electrical interference degrades signal quality as it travels on network cables.
- Degradation of signals is called *attenuation*.
- UTP cables should not be run in areas of high electromagnetic interference (EMI).

- Wireless signals are affected by both electromagnetic and radio frequency interference (RFI).
- Signal boosters can be used for extending the area of wireless coverage.

Preventive maintenance for networks

- Network cables should be run through secure routes.
- Cable connectors must be securely attached to devices.
- Physical access to network equipment should be restricted to authorized personnel.
- Apply security for servers and desktops by using permissions.
- Install the latest software updates on servers and desktops.
- Data backup and recovery procedures should be implemented.
- Clean power supply should be provided for equipment, and it must be redundant.

Security

This subsection covers a summary of highlights from the "Security" section in the A+ Exams Study Guide.

Access control

- Access control is the method of granting or denying access to system or network resources.
- It is applied on files, folders, or other shared resources by assigning permissions.
- Mandatory access control is hardcoded into devices and is universally applied.
- Discretionary access control is applied through the operating system by means of permissions.
- Role-based access control is implemented on objects for roles of users and groups.

User accounts

- A user account allows a user to log on to the system and access resources.
- A local user account allows users to log on locally to a computer and access local resources.
- A domain user account allows users to log on to the network from any computer in the network and access network-wide resources.
- The administrator account has full control over the system.
- The guest account is meant for occasional users.
- Normal user accounts are created for users to access resources for which they have permissions.

Using groups to control access

- A group is a collection of user accounts.
- Users are grouped based on their job roles; permissions are assigned to groups.
- Groups simplify the administration of resources.

Permissions

- File permissions are configured on individual files.
- File permissions are applied to both local and network access.
- Folder permissions are configured on folders.
- Shared folder permissions are applied only for network access.
- Printer permissions are applied only for accessing and managing printers.

Levels of access

- The level of access is defined in the Access Control List (ACL) for each object.
- The Read permission allows users to read the contents of a file or folder.
- The Write permission allows users to create new files and subfolders in folders and to write data to files.
- The Read and Execute permission allows users to read the contents of a file and execute the file.
- The Modify permission allows users to modify the contents of a file or a folder.
- The Full Control permission allows users to change permissions on a file or folder and perform all actions permitted by other permissions.
- The List Folder Contents (Folder Only) permission allows users to navigate through the folder and subfolders.

Restricted spaces

- Restricted physical access ensures the safety and security of expensive and critical network equipment, servers, and cabling systems.
- Physical access to restricted spaces is granted to authorized personnel only.
- Restricted spaces are equipped with alarm systems to prevent theft.
- Logbooks are maintained to keep record of the persons entering the restricted rooms.

Auditing and event logging

- Auditing is the process of tracking system usage resource access.
- It also helps diagnose application failures.
- Account management includes events related to the creation, modification, and deletion of user accounts by administrators.
- Log Off and Log On includes events related to users logging on or off the local computer.
- Process Tracking includes events related to actions performed by software applications.

- Object Access includes events related to the access of files and folders by users.
- Privilege Use includes events related to a user exercising her rights, such as changing the system time.
- System Events includes events related to system processes such as shutting down or restarting the computer. These events also relate to system security.
- The audit entries are written to log files.
- Log files can be analyzed to track security breaches and troubleshoot problems related to application processes.

Enabling and disabling auditing

- Auditing on Windows XP and Windows 2000 is available only on NTFS drives.
- The Auditing policy has to be enabled from the Local Security Policies snap-in.
- Auditing for individual files is enabled from its properties.

Authentication technologies

- The username and password is the most basic form of authentication.
- Hardware tokens or security tokens are the most trusted means of authentication.
- Biometric devices authenticate a user by his physical characteristics.
- Wireless authentication methods include open system, shared key, 802.1x, and WPA.

Software firewalls

- A software firewall is an application or a part of the operating system.
- A personal firewall is installed on an individual PC.
- Windows XP includes a firewall feature that can be turned on from the Control Panel.

Data access security

- Data access security is configured using NTFS and share permissions.
- Permissions are assigned to users and groups.
- The most restrictive of share and NTFS permissions takes effect.
- NTFS permissions for a user in multiple groups are combined to grant the highest level of access.

Troubleshooting software firewall issues

- Firewall rules or settings should be checked for proper configuration.
- Access can be allowed or denied based on the source and destination IP address, port, and protocols.
- Improperly configured firewall settings can deny access to legitimate users.
- It can also allow access to external attacks.

Troubleshooting security issues

- The Service Set Identifier (SSID) configuration on wireless clients is a common problem.
- Improperly configured or insufficient permissions can also deny access to users.
- Conflicts in share and NTFS permissions create access problems.
- Mismatching or unsupported encryption protocols will not allow a user to log on.

Preventive maintenance for security

- Account policies define how user accounts are handled when someone tries to log on using an incorrect password.
- Password policies define how users maintain their passwords.
- Audit policies can track logon attempts and reject access by unauthorized users.
- Software restriction policies define which applications are not allowed to run on a system.
- Security policies for the Windows Registry help prevent unauthorized modification.

Social engineering

- Social engineering is the process of acquiring personal or confidential information about someone.
- Social engineering attacks are usually launched over the phone or through email and chatting.
- Social engineering can also be launched during face-to-face interactions between a user and an attacker.
- Phishing attacks are a form of social engineering.
- The best protection against social engineering is to educate users about the security policies of the organization.

Practice Questions for the A+ Exams

1. You have been asked to install an IDE disk to a personal computer. This will be the only disk in the computer connected to the primary channel. How would you set the jumper?

   ○ A. Master

   ○ B. Slave

   ○ C. Cable Select

   ○ D. Auto

   Answer A is correct. A single disk is connected to the primary channel and acts as a master disk.

2. Which of the following is the most important factor when selecting a memory module to upgrade memory in a personal computer?

   ○ A. The module has the highest memory available in the market.

   ○ B. The module is built with state-of-the art technology.

   ○ C. The module is compatible with the system bus.

   ○ D. The module can double the system memory.

   Answer C is correct. The most important factor when selecting a memory module is to verify that the module is compatible with the system bus on the motherboard.

3. Which of the following is the name for the diagnostic process built into motherboards?

   ○ A. POST

   ○ B. CMOS

   ○ C. BIOS

   ○ D. DHCP

   Answer A is correct. The POST is the diagnostics program built into all motherboards. POST checks the functionality of all the hardware components of the motherboard.

4. You have just disconnected a hard disk from a computer and detected a red stripe on the data cable. What is the purpose of this red stripe?

   ○ A. It indicates the last pin of the cable.

   ○ B. It indicates the first pin of the cable.

   ○ C. It indicates that the cable was tested by the manufacturer.

   ○ D. It indicates the top end of the cable.

   Answer B is correct. The red marking on the data cable indicates pin number 1.

5. Which of the following is the most important precaution you should take while working on internal parts of the computer? Select two answers.

   ❑ A. Turn off the power supply.

   ❑ B. Disconnect the power cables from all drives.

   ❑ C. Disconnect the power cable from the motherboard.

   ❑ D. Wear a properly grounded antistatic wrist strap.

   Answers A and D are correct. You must turn off power to prevent shocks and wear a properly grounded antistatic wrist strap when working on internal parts of a computer. Semiconductor devices on the motherboard and adapter cards are very sensitive to static electricity.

6. You have just replaced a malfunctioning motherboard in a computer with a brand new one. You want to make sure that the new motherboard is functioning well before you connect other components such as the network

adapter and graphics card. Which of the following methods can be used to test the basic functionality of the motherboard?

❍ A. POST

❍ B. Beep codes

❍ C. Successful boot

❍ D. BIOS

Answer B is correct. Beep codes will usually indicate whether there is any problem with the basic functionality of the motherboard. Different manufacturers of BIOS software have different beep codes, and you must refer to the motherboard user manual for the exact meaning of a particular beep code.

7. Which of these methods can be used to test a 10/100 Mbps network port built on the motherboard without connecting it to the network?

❍ A. Multimeter

❍ B. Loopback adapter

❍ C. Visual indicators

❍ D. Beep codes

Answer B is correct. A loopback adapter can be used to test the network port built onto a motherboard or onto a separate network adapter. The loopback tester usually works with accompanying software to send and receive data signals to test whether the port is working.

8. Which of the following components ensure that thermally sensitive devices do not overheat during the normal operation of a personal computer? Select all correct answers.

❑ A. UPS

❑ B. Heat sink

❑ C. Fans

❑ D. Ribbon cables

❑ E. Ventilation slots

Answers B, C, and E are correct. Heat sinks are used to dissipate heat from the surface of semiconductor devices such as the CPU. The exhaust fans blow the hot air away from internal components. Ventilation slots ensure proper flow of air inside the computer case.

9. During the POST you can hear only a single beep. What does this beep usually indicate?

❍ A. A problem with on-board memory.

❍ B. A problem with expanded memory.

❍ C. An audio problem.

❍ D. A successful POST.

Answer D is correct. In most motherboards, the BIOS is programmed to sound a single beep during a POST to indicate that the POST has successfully completed.

10. Which of the following is considered to be the fastest port and is commonly used on laptops?

❍ A. PS/2

❍ B. USB

❍ C. Serial

❍ D. Parallel

Answer B is correct. USB ports are commonly used on laptop computers and are relatively faster than all other ports.

11. Which of the following wireless IEEE standards uses a radio frequency of 2.4 GHz with a data transfer speed of 11 Mbps?

❍ A. 802.11b

❍ B. 802.11c

❍ C. 802.11e

❍ D. 802.11g

Answer A is correct. The 802.11b standard specifies a radio frequency band of 2.4 GHz with a data transmission speed of 11 Mbps. The frequency specified for 802.11g is also 2.4 GHz but with a data transmission speed of 54 Mbps.

12. The laptop used by your manager is having video problems. What should you do to find out whether there is a problem with the LCD screen? Select two answers.

❑ A. Connect an external monitor.

❑ B. Change the LCD screen.

❑ C. Remove the LCD screen cable and reconnect it.

❑ D. Recycle power on the laptop.

❑ E. Toggle the video function key.

Answers A and E are correct. You can try connecting to an external monitor to find out whether the problem is with the LCD screen or the video card. You will also need to use the video toggle key to use the external monitor.

13. Which of the following is not a recommended method to enhance the life and performance of a laptop battery?

❍ A. Fully discharge and recharge the battery every day.

❍ B. Fully discharge and recharge the battery every two to three weeks.

❍ C. Use only NiCd batteries.

❍ D. Use the power management features available in the operating system.

Answer B is correct. The laptop battery should be fully discharged and recharged every two or three weeks. It is not a good idea to fully discharge the battery and recharge it every day.

14. You need to edit a file using Notepad but the Windows XP system does not allow you to save the file. How can you resolve this problem using the command line?

    ❍ A. Type `help` with the filename at the command prompt.

    ❍ B. Use the *attrib* command to change the read-only attribute of the file.

    ❍ C. Use the *copy* command to copy the file to a different location and then edit it.

    ❍ D. Use the *edit* command instead of using the Notepad to edit the file.

    Answer B is correct. The file has the read-only attribute set, which should be changed using the *attrib* command before you can edit the file and save it with the same filename.

15. You have noticed that the performance of your Windows 2000 Professional computer is degrading day by day. You suspect that the hard disk does not respond as quickly as it should when you open files. What should you first do to improve the hard disk performance?

    ❍ A. Analyze the hard disk.

    ❍ B. Defragment the hard disk.

    ❍ C. Run the *chkdsk* utility.

    ❍ D. Replace the disk immediately.

    ❍ E. Upgrade to Windows XP Professional.

    Answer B is correct. The disk should be defragmented in order to improve its performance. Just analyzing the disk will only give you information about its fragmentation. When you perform defragmentation, the disk is automatically analyzed for fragmentation. The *chkdsk* utility is used to check for and fix file system errors and problems with bad sectors on a disk.

16. Which of the following methods can be used to format a disk partition? Select all correct answers.

    ❑ A. The *format* command

    ❑ B. The *diskpart* utility

    ❑ C. Windows Explorer

    ❑ D. The Disk Management snap-in

    ❑ E. The Device Manager snap-in

    Answers A, C, and D are correct. You can format a disk partition using the *format* command, Windows Explorer, or the Disk Management snap-in. The *diskpart* utility does not include any command for formatting a disk partition.

17. You upgraded the driver of your printer after downloading it from the manufacturer's web site. The printer stopped working after the upgrade. How can you resolve the problem? Select two answers.

    ❑ A. Reinstall the old printer driver.

    ❑ B. Use the Rollback Driver button in the Device Manager.

    ❑ C. Completely remove the new printer driver and reinstall it.

    ❑ D. Turn off the printer when installing the driver.

Answers A and B are correct. You will need to reinstall the old printer driver that was working. You can also use the Rollback Driver button in the Device Manager to install the printer driver. Reinstalling the new driver after completely removing it will not help. The printer should be connected and turned on when the driver is installed.

18. You have decided to use the System Restore utility to fix a computer running Windows XP, which is showing intermittent problems. Which of the following is required in order to use the system restore utility?

   ○ A. A full backup of the system.

   ○ B. A system restore point.

   ○ C. A backup of the System State data.

   ○ D. An Automatic System Restore disk.

   Answer B is correct. You must first create a system restore point in order to use the System Restore utility.

19. Which of the following is an alternative to adding more random access memory (RAM) to a computer?

   ○ A. Add internal CPU cache memory.

   ○ B. Add a new hard disk.

   ○ C. Increase the size of the paging file.

   ○ D. Decrease the size of the paging file.

   Answer C is correct. An alternative to adding RAM to a computer is to increase the size of the paging file. The computer uses the paging file to swap data when there is insufficient RAM in the computer.

20. You installed a new game on a Windows XP computer, and the computer fails to restart. Which of the following methods can you use to fix this startup problem?

   ○ A. Use the Last Known Good Configuration from the Advanced Boot menu.

   ○ B. Use the Recovery Console to uninstall the new game.

   ○ C. Use the last full backup tape to restore the system.

   ○ D. Use an Emergency Repair Disk (ERD) to repair the startup files.

   Answer A is correct. You can use the Last Known Good Configuration from the Advanced Boot options to restore the system to the previous working configuration. You cannot use the Recovery Console to uninstall the game, nor can you do it using the last full backup tape. ERD will also not help. Moreover, ERD can only be used on Windows NT and Windows 2000 computers.

21. Which of the following is important regarding downloading and installing software updates?

   ○ A. All systems should be configured for automatic download and installation.

   ○ B. All updates should be installed as soon as they are available.

   ○ C. Updates should be thoroughly tested before installation.

   ○ D. There is no need to install any updates unless they address some security issue.

Answer C is correct. All updates from software vendors should be thoroughly tested before installation. It does not matter whether the updates address a specific application issue or a security issue—updates must be tested before they are installed on several computers.

22. One of the printers in your office is not responding. You have checked all physical connections and found that the printer is online. When you check the Printer Properties on the computer where the printer is shared, it shows a long list of documents. Which of the following could be a potential problem?

    ○ A. The printer driver.

    ○ B. The port where the printer is connected.

    ○ C. A document that is stuck in the print spooler.

    ○ D. Permissions associated with the user who sent the print job.

    Answer C is correct. The print job that is on the top of the list of documents in the print spooler is causing the printer problem. There is no problem with either the printer driver or the printer port. It is also unlikely that the problem is associated with print permissions.

23. Which of the following parts in a laser printer is used to transfer a high positive voltage to charge the paper?

    ○ A. Drum

    ○ B. Transfer corona wire

    ○ C. Primary corona wire

    ○ D. Fuser

    Answer B is correct. The transfer corona wire supplies a high positive charge to the paper. The function of the primary corona wire is to charge the drum with a high negative voltage.

24. You have been asked to connect a Windows XP Professional computer to a TCP/IP printer that is directly connected to a network port. Which of the following is the correct procedure to accomplish this task?

    ○ A. Select the Local Printer option and create a new port.

    ○ B. Select the Local Printer option and browse for the network port.

    ○ C. Select the Network Printer option and browse for the network port.

    ○ D. Select the Network Printer option and enter the name of the printer.

    Answer A is correct. To attach to a TCP/IP printer connected directly to a network port, you must select Local Printer Attached To This Computer and create a new TCP/IP port. You select the Network Printer option when the printer is attached to another computer designated as a print server.

25. Which of the following printers is suitable for printing multipart invoices?

    ○ A. Dot matrix printer

    ○ B. Laser printer

    ○ C. Inkjet printer

    ○ D. Bubble-jet printer

Answer A is correct. A dot matrix printer is suitable for use with multipart forms such as invoices. This is because a dot matrix printer is an impact printer that makes a good impression on multiple sheets of paper.

26. Which of the following ports cannot be used to connect a scanner?

    ❍ A. USB

    ❍ B. Serial

    ❍ C. SCSI

    ❍ D. PS/2

    Answer D is correct. Of the given choices, a scanner can be connected to a serial, SCSI, or USB port, but not to a PS/2 port. The PS/2 port is generally used to connect a mouse or a keyboard.

27. Which of the following types of cables is not prone to electromagnetic interferences?

    ❍ A. UTP cable

    ❍ B. STP cable

    ❍ C. Coaxial cable

    ❍ D. Fiber optic cable

    Answer D is correct. The fiber optic cable transfers data using optical (light) signals. This type of cable is not prone to electromagnetic interferences.

28. Which of the following components of an IP address is used to distinguish the network address from a host address?

    ❍ A. Default gateway

    ❍ B. Subnet mask

    ❍ C. DNS server

    ❍ D. WINS server

    Answer B is correct. The subnet mask is used to distinguish a network address from a host address on a TCP/IP network.

29. A computer cannot communicate with any of the computers on a different network segment. It has no problem connecting to other computers that are located on its own network segment. Which of the following IP address parameters are possibly incorrectly configured on the computer?

    ❍ A. IP address

    ❍ B. Subnet mask

    ❍ C. Default gateway

    ❍ D. DNS server

    Answer C is correct. If the IP address of the default gateway is incorrectly configured, the computer will not be able to communicate with any other computers located on different network segments. If the default gateway is configured correctly, you will need to check the IP address and the subnet mask.

30. Which of the following devices connects different network segments and uses tables to create a map of the network topology?

   ❍ A. Router

   ❍ B. Switch

   ❍ C. Bridge

   ❍ D. Hub

   Answer A is correct. A router is used to connect different network segments. It uses routing tables to create a map of the network topology and route packets based on the network addresses in IP packets.

31. Which of the following name resolution methods is best suited when you have only Windows computers, and there is only a single network segment not connected to the Internet?

   ❍ A. *LMHOSTS* file

   ❍ B. *HOSTS* file

   ❍ C. DNS

   ❍ D. WINS

   Answer D is correct. When you have only Windows computers and there is only one network segment, WINS can serve the purpose of name resolution. If the network is large and is connected to the Internet, you will need the DNS server for name resolution.

32. Which of the following is a primary requirement for an Infrared wireless connection?

   ❍ A. A shared frequency band.

   ❍ B. A direct line of sight.

   ❍ C. An access point.

   ❍ D. A wireless router.

   Answer B is correct. The primary requirement for an infrared wireless connection is the direct line of sight. This is why the infrared wireless connection is also called a point-to-point connection. Infrared signals cannot pass through wooden or concrete walls.

33. Which of the following network topologies does not allow you to add or remove computers without affecting the network?

   ❍ A. Ring

   ❍ B. Bus

   ❍ C. Mesh

   ❍ D. Star

   Answer B is correct. The entire network is affected when you add or remove computers in a bus network.

34. Which of the following methods uses the physical characteristics of a user to verify identity?

❍ A. Biometrics

❍ B. Username and password

❍ C. Kerberos

❍ D. CHAP

Answer A is correct. Biometric security devices are used to verify the identity of a person by matching physical characteristics such as fingerprints or eye retina.

35. In which of the following authentication methods is an encrypted challenge text sent to the user to verify her credentials?

❍ A. Kerberos

❍ B. PAP

❍ C. CHAP

❍ D. EAP

Answer C is correct. CHAP stands for Challenge Handshake Authentication Protocol. In this authentication method, a challenge text is sent to the user in encrypted form. The user sends the challenge text back to the authentication server, which compares the two messages. The user is authenticated only if a match is found.

36. One of the senior network administrators who has recently joined the company has asked a few users to give him their usernames and passwords to complete an urgent task. What kind of security attack does this indicate?

❍ A. Man in the Middle

❍ B. Replay attack

❍ C. Spoofing

❍ D. Social engineering

Answer D is correct. When someone is trying to get you to believe that he is acting in your interests and asks for confidential information, he is actually initiating a social engineering attack.

37. Your company has installed a biometric device to take fingerprints of every person who wants to enter the restricted room where servers and network equipment are installed. Which of the following is the purpose of this device?

❍ A. Auditing

❍ B. Data integrity

❍ C. Confidentiality

❍ D. Authentication

❍ E. Access control

Answer D is correct. The purpose of installing biometric devices is to provide authentication. Auditing is configured on network resources while security protocols are used for data confidentiality and integrity.

38. You have been asked to work out a backup plan for the two most critical servers in the office. Your manager wants you to ensure that data could be restored using only a single tape. Which of the following backup methods would you suggest?

    ❍ A. A full backup everyday.

    ❍ B. A full backup on Friday nights and incremental backs from Monday to Thursday.

    ❍ C. An incremental backup on Friday, and differential backups from Monday to Thursday.

    ❍ D. A full backup every Friday.

    Answer A is correct. When you want to restore data from a single backup tape, full backup needs to be performed on a daily basis. A full backup stores complete data on a single tape.

39. Which of the following safety measures help reduce the effects of static discharge? Select all correct answers.

    ❑ A. Antistatic bag

    ❑ B. Antistatic wrist strap

    ❑ C. Antistatic table mat

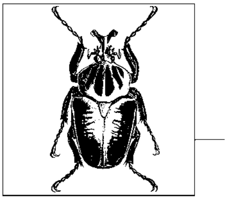
    ❑ D. Antistatic body wrap

    ❑ E. Antistatic head cover

    Answers A, B, and C are correct. Antistatic bags, antistatic wrist straps, and antistatic table and floor mats all help reduce the effects of static electricity.

III

Network+



7
Overview of the Network+ Exam

CompTIA's Network+ certification is for those individuals who intend to prove their expertise in computer networking. You will need to pass only one exam (Exam N10-003) to get this certification. This exam tests your foundation-level knowledge of network media and topologies; protocols and standards; and network implementation and support. A Network+ certified individual is considered to have proven skills in general networking concepts, installation, configuration, and troubleshooting of basic networking hardware. CompTIA's Network+ certification is vendor-neutral and is recognized worldwide.

One good thing about CompTIA's certifications is that they do not expire. In other words, CompTIA's certifications are good for life. You do not have to recertify if the exam objectives change. I still recommend that you check CompTIA's Network+ exam web site from time to time at *http://certification.comptia.org/network* for news and updates on exam objectives.

The approximate percentage of coverage for each domain in the Network+ exam is given in Table 7-1.

Table 7-1. Network+ exam domains and percentage of coverage

Domain	Percentage of coverage
Media and Topologies	20 percent
Protocols and Standards	20 percent
Network Implementation	25 percent
Network Support	35 percent

CompTIA recommends that in order to pass the Network+ exam, a candidate should have at least nine months of hands-on experience working in a networked computer environment. It is also recommended that the candidate pass the A+ exam before attempting to write the Network+ exam. It is a good idea to have studied a Network+ certification exam self-paced study guide or attended a training course before you attempt to take this exam. You will then be ready to use this section of the book for your final exam preparation.

> CompTIA's Network+ Exam N10-003 is fairly easy. If you are well-prepared, you will easily get through this exam. It is recommended that you take this exam after passing the A+ exams. The combination of A+ and Network+ certifications qualify you to get an exemption for one elective exam in *Microsoft's MCSA/MCSE* track.

Areas of Study for the Network+ Exam

Media and Topologies

- Recognize the following logical or physical network topologies given a diagram, a schematic, or a description:
  - — Star
  - — Bus
  - — Mesh
  - — Ring
- Specify the main features of 802.2 (Logical Link Control), 802.3 (Ethernet), 802.5 (token ring), 802.11 (wireless), and FDDI (Fiber Distributed Data Interface) networking technologies, including speed, access method (CSMA/CA and CSMA/CD), topology, or media.
- Specify the characteristics (speed, length, topology, and cable type) of the following cable standards:
  - — 10BASE-T and 10BASE-FL
  - — 100BASE-TX and 100BASE-FX
  - — 1000BASE-T, 1000BASE-CX, 1000BASE-SX, and 1000BASE-LX
  - — 10 GBASE-SR, 10 GBASE-LR, and 10 GBASE-ER
- Recognize the following media connectors and describe their uses:
  - — RJ-11 and RJ-45 (Registered Jacks)
  - — F-Type
  - — ST (Straight Tip) and SC (Subscriber or Standard Connector)
  - — IEEE 1394 (FireWire)
  - — Fiber LC (Local Connector)
  - — MT-RJ (Mechanical Transfer Registered Jack)
  - — USB (Universal Serial Bus)
- Recognize the following media types and describe their uses:
  - — Category 3, 5, 5e, and 6
  - — UTP (unshielded twisted pair)
  - — STP (shielded twisted pair)
  - — Coaxial cable
  - — SMF (Single-Mode Fiber) and MMF (Multimode Fiber) optic cables
- Identify the purposes, features, and functions of the following network components:
  - — Hubs, switches, bridges, routers, and gateways
  - — CSU/DSU (Channel Service Unit/Data Service Unit)
  - — NICs (Network Interface Card)
  - — ISDN (Integrated Services Digital Network) adapters

    - WAPs (Wireless Access Point)
    - Modems
    - Transceivers (media converters)
    - Firewalls
- Specify the general characteristics (carrier speed, frequency, transmission type, and topology) of wireless technologies such as 802.11 (a frequency hopping spread spectrum) or 802.11x (a direct frequency spread spectrum), Infrared, and Bluetooth.
- Identify factors that affect the range and speed of wireless service (interference, antenna type, and environmental factors).

Protocols and Standards

- Identify a MAC (Media Access Control) address and its parts.
- Identify the seven layers of the OSI (Open Systems Interconnect) model and their functions.
- Identify the OSI (Open Systems Interconnect) layers at which the following network components operate:
    - Hubs, switches, bridges and routers
    - NICs (Network Interface Card)
    - WAPs (Wireless Access Point)
- Differentiate between the network protocols in terms of the routing, addressing schemes, interoperability, and naming conventions of IPX (Internetwork Packet Exchange)/SPX (Sequential Packet Exchange), NetBEUI (Network Basic Input/Output System Extended User Interface), AppleTalk/AppleTalk over IP, and TCP/IP (Transmission Control Protocol/Internet Protocol).
- Identify the components and structure of IP (Internet Protocol) addresses (IPv4 and IPv6) and the required setting for connections across the Internet.
- Identify classful IP address ranges and their subnet masks (Class A, B, and C).
- Identify the purpose of subnetting.
- Identify the differences between private and public network addressing schemes.
- Identify and differentiate between static, dynamic, and self-assigned (APIPA) addresses.
- Define the purpose, function and use of the protocols used in the TCP/IP suite:
    - TCP (Transmission Control Protocol)
    - UDP (User Datagram Protocol)
    - FTP (File Transfer Protocol)
    - SFTP (Secure File Transfer Protocol)
    - TFTP (Trivial File Transfer Protocol)
    - SMTP (Simple Mail Transfer Protocol)

  - HTTP (Hypertext Transfer Protocol)
  - HTTPS (Hypertext Transfer Protocol Secure)
  - POP3/IMAP4 (Post Office Protocol version 3)/(Internet Message Access Protocol version 4)
  - Telnet
  - SSH (Secure Shell)
  - ICMP (Internet Control Message Protocol)
  - ARP/RARP (Address Resolution Protocol)/(Reverse Address Resolution Protocol)
  - NTP (Network Time Protocol)
  - NNTP (Network News Transport Protocol)
  - SCP (Secure Copy Protocol)
  - LDAP (Lightweight Directory Access Protocol)
  - IGMP (Internet Group Multicast Protocol)
  - LPR (Line Printer Remote)
- Define the function of TCP/UDP ports.
- Identify the well-known ports associated with the commonly used services and protocols.
- Identify the purpose of network services and protocols, such as DNS, NAT, ICS, WINS, SNMP, NFS, Zeroconf, SMB, AFP LPD, and Samba.
- Identify the basic characteristics (speed, capacity and media) of the following WAN (Wide Area Network) technologies: packet switching, circuit switching, ISDN, FDDI, T1/E1/J1, T3/E3/J3, Ocx, and X.25.
- Identify the basic characteristics of Internet access technologies such as xDSL, broadband cable, POTS/PSTN, satellite, and wireless.
- Define the function of remote access protocols and services such as RAS, PPP, SLIP, PPPoE, PPTP, VPN, and RDP.
- Identify the purpose and function of security protocols such as IPSec, L2TP, SSL, WEP, WPA, and 802.1x.
- Identify authentication protocols such as CHAP, MS-CHAP, PAP, RADIUS, Kerberos, and EAP.

Network Implementation

- Identify the basic capabilities (client support, interoperability, authentication, file and print services, application support, and security) of the following server operating systems to access network resources:
  - Unix/Linux/Mac OS X Server
  - NetWare
  - Windows
  - Appleshare IP

- Identify the basic capabilities needed for client workstations to connect to and use network resources (media, network protocols, and peer and server services).
- Identify the appropriate tool for a given wiring task (wire crimper, media tester/certifier, punch down tool, or tone generator).
- Given a remote connectivity scenario comprised of a protocol, an authentication scheme, and physical connectivity, configure the connection. This includes connection to network servers powered by Unix/Linux/Mac OS X Server, NetWare, Windows, and Appleshare IP.
- Identify the purpose, benefits, and characteristics of using a firewall.
- Identify the purpose, benefits, and characteristics of using a proxy service.
- Given a connectivity scenario, determine the impact on network functionality of a particular security implementation (port blocking/filtering, authentication, and encryption).
- Identify the main characteristics of VLANs (Virtual Local Area Networks).
- Identify the main characteristics and purpose of extranets and intranets.
- Identify the purpose, benefits, and characteristics of using antivirus software.
- Identify the purpose and characteristics of fault tolerance, such as power, link redundancy, storage, and services.
- Identify the purpose and characteristics of disaster recovery:
    - Backup/restore
    - Offsite storage
    - Hot and cold spares
    - Hot, warm, and cold sites

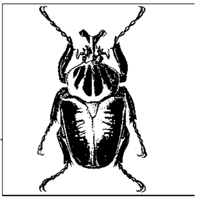
Network Support

- Given a troubleshooting scenario, select the appropriate network utility from the following:
    - *Tracert/ Traceroute*
    - *Ping*
    - *Arp*
    - *Netstat*
    - *Nbtstat*
    - *Ipconfig/Ifconfig*
    - *Winipcfg*
    - *Nslookup/Dig*
- Given output from a network diagnostic utility, identify the utility and interpret the output.
- Given a network scenario, interpret visual indicators to determine the nature of a stated problem.

- Given a troubleshooting scenario involving client-accessing remote network services, identify the cause of the problem.
- Given a troubleshooting scenario between a client and the server environment, identify the cause of a stated problem for the following:
  - Unix/Linux/Mac OS X Server
  - NetWare
  - Windows
  - Appleshare IP
- Given a scenario, determine the impact of modifying, adding, or removing network services (for example: DHCP, DNS, and WINS) for network resources and users.
- Given a troubleshooting scenario involving a network with a particular physical topology and including a network diagram, identify the network area affected and the cause of the stated failure.
- Given a network troubleshooting scenario involving an infrastructure (wired or wireless) problem, identify the cause of a stated problem.
- Given a network problem scenario, select an appropriate course of action based on a logical troubleshooting strategy. This strategy can include the following steps:
  - Identify the symptoms and potential causes.
  - Identify the affected area.
  - Establish what has changed.
  - Select the most probable cause.
  - Implement an action plan and solution including potential effects.
  - Test the result.
  - Identify the results and effects of the solution.
  - Document the solution and process.

8

Network+ Exam Study Guide



This chapter provides a study guide for the Network+ Exam N10-003. Various sections in this chapter are organized to cover the related objectives of the exam. Each section identifies the exam objective, provides an overview of the objective, and then discusses the key details that you should grasp before taking the exam.

An overview of this chapter's sections is as follows:

Media and Topologies
: This section covers the basics of network media, networking standards, and topologies, as well as offers a brief description of networking devices. It also covers both wired and wireless networks.

Protocols and Standards
: This section covers the Open System Interconnect (OSI) networking model, networking protocols, and services. Also included in this section is a description of wireless technologies and Internet access methods.

Network Implementation
: This section includes a study of network operating systems, their interoperability, and methods of implementing security in wired and wireless networks. Remote access, intranets, extranets, fault tolerance, and disaster recovery are also covered in this section.

Network Support
: This section includes a study of concepts related to troubleshooting methods and utilities for different operating systems and topologies. Also discussed in this section are the effects of adding/removing network services and client connectivity problems.

The sections in this chapter are designed to follow the exam objectives as closely as possible. This Study Guide should be used to reinforce your knowledge of key concepts tested in the exam. If you study a topic and do not understand it completely, I recommend that you go over it again and memorize key facts until you feel comfortable with the concepts.

Studying for the Network+ certification requires that you have access to a computer network. Although it is not essential, it is good to have a Windows- or Unix/Linux-based computer network in order to get familiar with the concepts covered in this Study Guide. Identification of network media, cables, and connectors is required as part of your preparation for the exam. A small network with a Windows XP desktop and a Windows or Unix/Linux server would serve the purpose. Needless to say, you will also need an active Internet connection, just in case you need to search for more information on any topic.

> This chapter contains a number of terms, notes, bulleted points, and tables that you will need to review multiple times. Pay special attention to new terms and acronyms—those you are not familiar with—as these may be tested in the exam.

Media and Topologies

Networking standards are the basis of any network implementation. Every network, small or large, is based on a networking topology and might use one or more types of cables. Each networking standard defines a certain physical layout of the components of the network. These include servers, desktops, printers, network devices, cables, and connectors. Network administrators have to decide on a networking topology and cabling before chalking out a network plan. For network technicians, a thorough understanding of networks, network standards, topologies and media is essential for keeping the network functional. This section covers a brief description of essential components of any network, media, and topologies.

Overview of Networks

A *computer network* refers to two or more computers linked together to share files, printers, and other resources. The computers may be linked through cables, telephone lines, satellite, radio frequencies, or Infrared beams. The network may be as small as just two or more computers linked together at home or in an office, or as big as a corporate network at multiple locations spanning across the globe. The following sections describe different types of networks and the concept of centralized and decentralized computing.

Local area network (LAN)

A local area network is a network of computers joined together in a local area such as a small office, a home, or a building. The area covered by a LAN is usually restricted to a single location. The function of a LAN is to provide high-speed connectivity to all computers and network devices. The data transfer speed achieved in a LAN is significantly higher than its counter part, the *wide area network (WAN)*. Figure 8-1 shows a local area network.

Network+ Study Guide

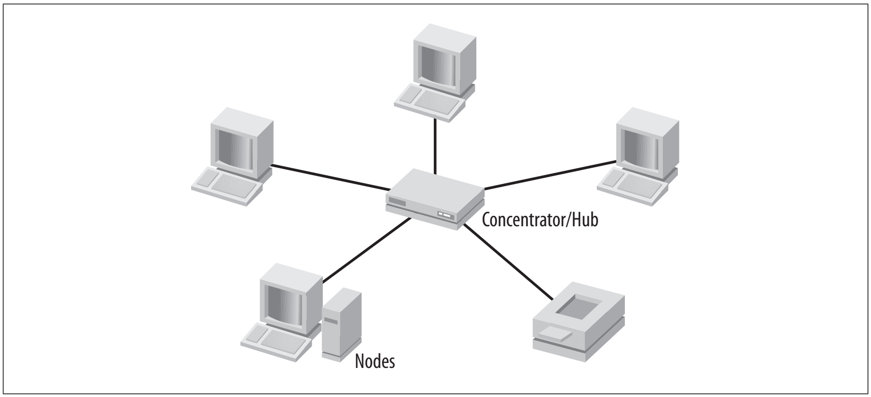


Figure 8-1. Local area network

Wide area network (WAN)

A wide area network is a network that connects two or more local area networks. A WAN typically connects separate LANs at different geographic locations. A third party such as an Internet service provider (ISP) or a local telephone company is responsible for providing the required dedicated hardware and/or connectivity lines to implement a WAN. These hardware devices include modems or routers that are required to connect the local LANs to the service provider's network. Figure 8-2 shows a wide area network.

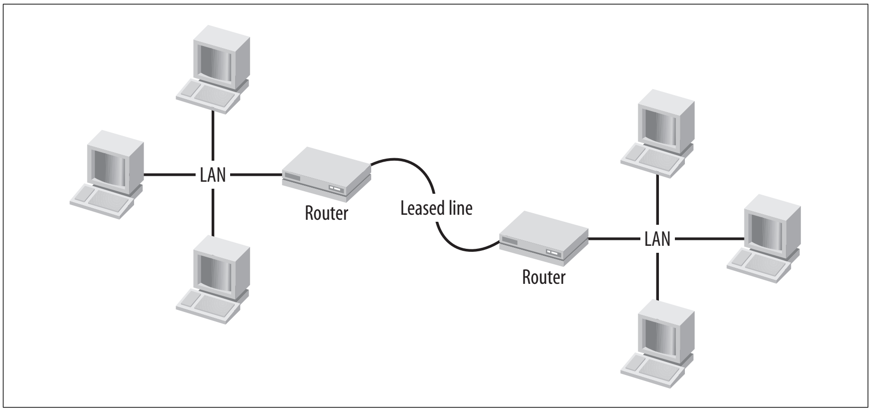


Figure 8-2. Wide area network

Personal area network (PAN)

Unlike the name suggests, a personal area network may or may not belong to a single person. The term *PAN* refers to a network of devices located in close proximity of each other. The devices may include such items as computers, PDAs, or mobile phones, that are connected using a wireless or a wired network. A mobile phone connected to a computer, or a few laptops connected to each other in an ad-hoc fashion are examples of personal area networks. Similarly, two or more computers sharing an Internet connection in a home network is another example of a PAN.

Metropolitan area network (MAN)

A metropolitan area network is a large internetwork connecting local area networks in a campus or inside the boundaries of one city. The MANs are usually connected using high-speed fiber optic cables. Metropolitan Area Networks can further be connected to form wide area networks.

Centralized and decentralized computing

In a *centralized computing model*, all processing is done on a central computer. This computer provides data storage as well as controls all peripherals including the clients. Clients are called *dumb terminals* and are attached to the central computer. This model provides greater security since all functions are controlled from one location. The disadvantage is that it can significantly slow processing, and if the central computer breaks down, the entire system breaks down. The *client/server* networking model is an example of centralized computing.

In a *decentralized computing model*, all processing and resources are distributed among several computers, thereby increasing performance and minimizing breakdown of the system. All systems can run independent of each other. A *peer-to-peer* network is an example of a decentralized computing model.

Peer-to-peer (P2P) network

In a peer-to-peer network, every computer is responsible for processing applications, storing data, and controlling access to its resources. A P2P network is also known as a *workgroup*. These networks are suitable for a small number of computers only. As the network grows, the administration of resources becomes difficult. For this reason, peer-to-peer networks are not suitable for large networks. The following are some characteristics of P2P networks:

- These networks are suitable for only about 10 computers.
- They are cost-effective compared to the client/server model.
- A network operating system (NOS) does not need to be installed on any computer.
- An administrator is not required, and each user is responsible to manage resources on her computer.
- These networks are not considered secure because each user individually maintains security of resources on her computer.

Client/server network

In a client/server network model, a centralized server usually holds control of all system and network resources located across the network. These include network services, storage, data backup, security management, and access control. The network consists of dedicated servers and desktops (clients). Servers run network operating systems, such as Windows Server 2000/2003 or Unix/Linux, and the desktops run client operating systems, such as Windows XP. Most modern network environments use the client/server computing model. Some characteristics of client/server networks are shown next.

- This model is scalable to very large-scale internetworks.
- Skilled administrators are required to manage the network.
- Dedicated server and network hardware may be required, which increases the cost of ownership.
- Security of the resources can be effectively maintained from a centralized point.

Physical Network Topologies

A *network topology* describes the physical and logical layout of the network components. A *physical network topology* refers to the actual layout of computers, cables, and other networking devices. The network topology is determined by the connections between different components. A logical topology refers to the communication methods used by different components. The Network+ Exam covers the commonly used physical topologies: star, bus, mesh, ring, and wireless, described in the following sections.

Star topology

In a star topology, computers (also called *nodes*) connect to each other through a central device, called a *hub* or a *switch*. Since each device is connected independently to the central device using a separate cable, the star network can be expanded at any time without affecting the operation of the network. Failure of one or more nodes also does not affect the network operation. The central device becomes the single point of failure because all nodes are connected to it. This topology is easy to implement, and its cost depends on the type of central device as well as the type of cable used to connect nodes. Figure 8-3 shows a star network, and the advantages and disadvantages are described next.

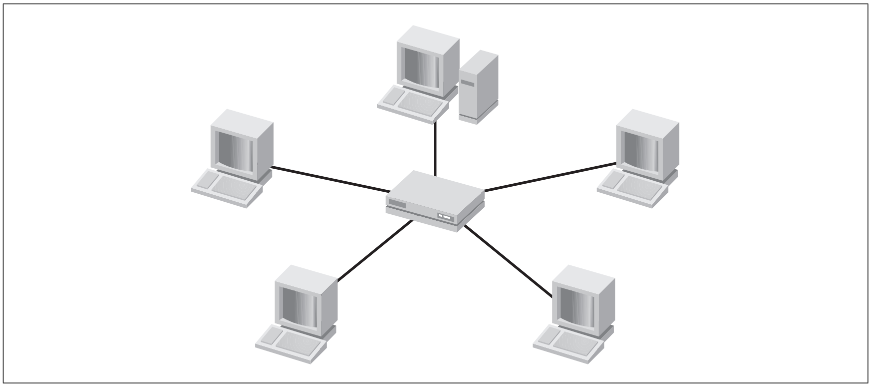


Figure 8-3. A star network

Advantages

- A star network is easy to implement.
- It can be easily expanded without affecting the network operation.

- Failure of a single node or the connecting cable does not affect the entire network's operation.
- It is easy to isolate nodes in order to troubleshoot problems.

Disadvantages

- Failure of the central device (hub or switch) can bring down the entire network.
- The length of cable required is much more than ring and bus networks because each node is connected separately.
- Cable length from the central device can be a limiting factor, depending on the type of cable used.

Bus topology

In a bus topology, all computers are connected to a shared communication line, called a *trunk* or a *backbone*. The computers are connected to the backbone using *T-connectors*. Both ends of the backbone use *terminators* in order to prevent reflection of signals. If the terminator is missing or is deliberately removed, the data transmissions are disrupted. There is no central device or any special configuration. Figure 8-4 shows a bus network, and the advantages and disadvantages are described next.

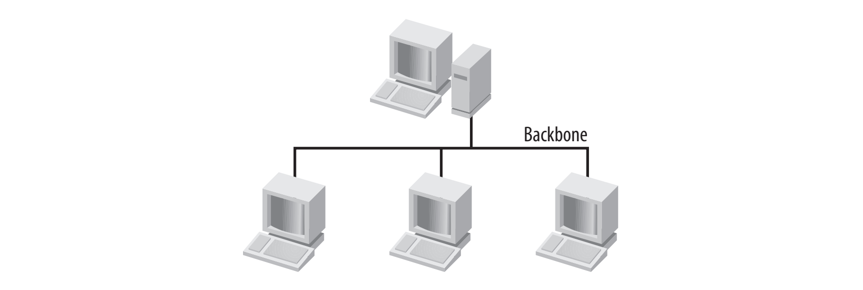


Figure 8-4. A bus network

Advantages

- A bus network is the cheapest of all topologies.
- No special configuration is required.
- It is easy to install, and no special equipment is needed for installation.
- It needs less cable length than do other topologies.

Disadvantages

- A break in cable or a missing terminator can bring down the entire network.
- It is not possible to add or remove computers without disrupting the network.
- It is difficult to troubleshoot and administer.
- Addition of more computers degrades performance.

Mesh topology

In a mesh topology, all computers in the network are connected to every other computer, forming a mesh of connections. Each computer makes a point-to-point connection to every other computer. This makes the network highly fault tolerant and reliable, as a break in the cable or a faulty computer does not effect network operation. Ad-hoc wireless networks fall into this category, as each connection is independent of the other. Data can travel from one computer to another using a number of paths. With the exception of wireless networks, mesh networks are very expensive in terms of the length of cable required to create multiple redundant connections. Figure 8-5 shows a mesh network, and the advantages and disadvantages are described next.

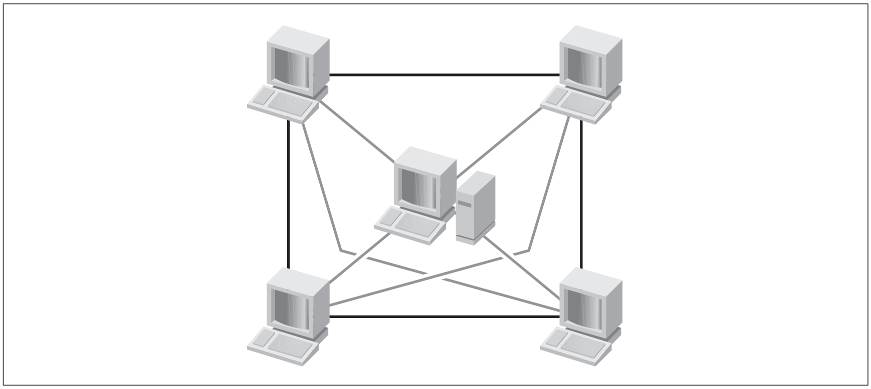


Figure 8-5. A mesh network

Advantages

- A mesh network is highly reliable because of redundant multiple paths between computers.
- The failure of a single computer or a cable fault does not affect network operations.
- Computers can be added or removed without affecting the network.

Disadvantages

- It is difficult to install and troubleshoot.
- It is very expensive because of the length of cable required to make multiple redundant connections.
- Only a limited number of computers can be connected in a mesh topology.

Ring topology

In a ring topology, each computer is connected to its neighboring computer to form a logical ring. Data travels in the ring in a circular fashion from one computer to another, forming a logical ring. If one of the computers in the ring fails or if the cable is broken, the entire network becomes inaccessible. The addition or removal of computers also disrupts network transmissions. Ring networks are less efficient than star networks because of the fact that data must pass through each computer on the way to the destination. The physical layout of a ring network actually forms a star network. In a Token Ring network, a *Multi-Station Access Unit (MSAU)*, or *Media Access Unit (MAU)* acts as the central device or hub to process circulation of a special data packet called a Token. The MSAU has *Ring In (RI)* and *Ring Out (RO)* ports that facilitate connection of one MSAU to another MSAU for expanding the network. The last MSAU is connected to the first MSAU to complete the ring. Figure 8-6 shows a ring network, and the advantages and disadvantages are described next.

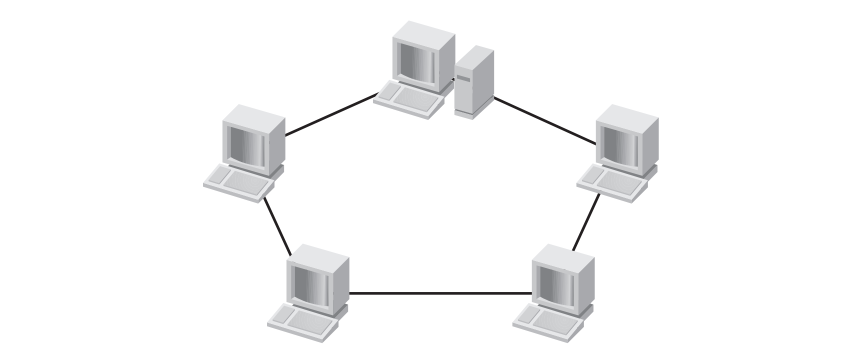


Figure 8-6. A ring network

Advantages

- A ring network is relatively easy to install.
- There are fewer collisions because only one computer transmits at a time.

Disadvantages

- A break-in cable or a faulty computer can bring down the entire network.
- It is not as efficient as a star network.
- It is difficult to troubleshoot a ring network.
- The addition or removal of computers can disrupt network operation.

Wireless topologies

A *wireless network* connects two or more computers without using cables. To communicate with each other, these networks use *spread spectrum technology*, which is based on radio frequencies. Each device in the network is equipped with a wireless network adapter and is called a *station*. The area of communication is limited and is known as the *basic service set*. Wireless stations or clients can freely move within the basic service set. A wireless network can further be connected to a wired network with the help of wireless *access Points (AP)*. The IEEE 802.11 standards define two main configurations of wireless communications: *Ad-hoc* and *Infrastructure*.

Ad-hoc wireless network. An Ad-hoc wireless network is also known as a peer-to-peer or an unmanaged wireless network. Two or more computers directly communicate to each other without using an access point. There is no central device (or hub), and these networks can be created spontaneously anywhere when two or more network devices fall within the range of each other. It provides the fastest way to temporarily connect computers and share resources. For example, two or more laptop computers can be connected in a conference room or in a cafeteria. Figure 8-7 shows an ad-hoc network.

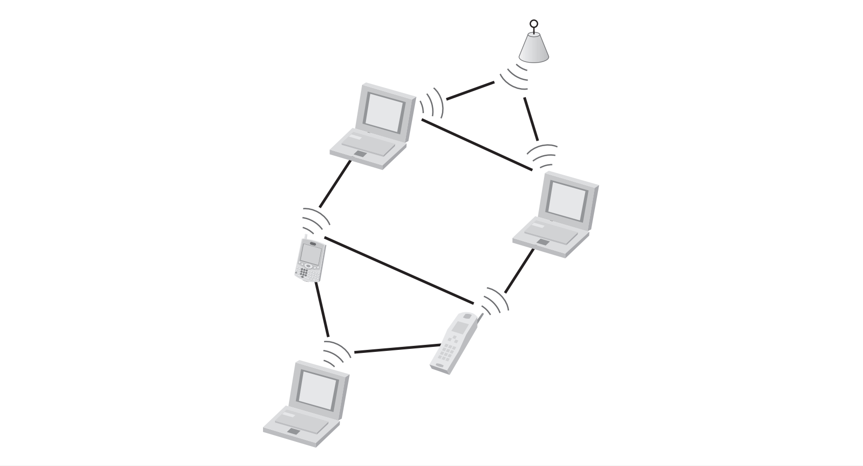


Figure 8-7. An ad-hoc wireless network

Infrastructure wireless networks. In an *Infrastructure* configuration, a central wireless device known as the access point (AP) is used to authenticate and configure wireless clients that fall within its range. Wireless clients communicate to each other through the AP. A special identifier known as a *Service Set Identifier (SSID)* must be configured on the AP and on each wireless client. All clients in one Infrastructure network use the same SSID. Different Infrastructure networks are identified by their unique SSIDs. The AP can further be connected to the wired local area network so that wireless clients can access the wired LAN also. Figure 8-8 shows an infrastructure wireless network.

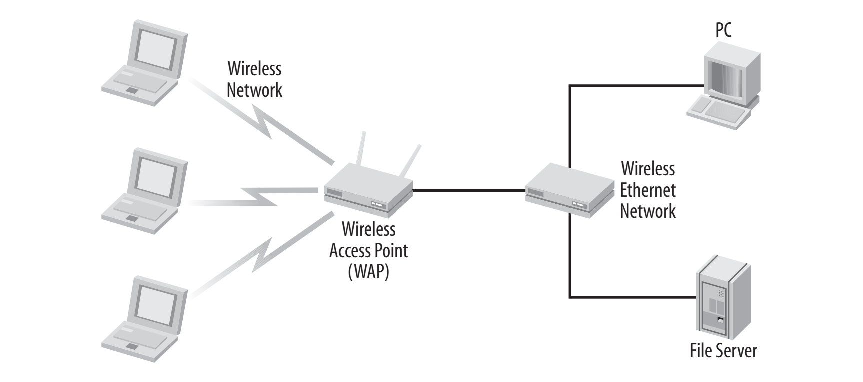


Figure 8-8. An infrastructure wireless network

Networking Standards

The Institution of Electrical and Electronics Engineers (IEEE) has defined standards for local area networks, metropolitan area networks, and wireless LANs as the *IEEE 802 standards*. The IEEE 802 standards describe the operation of networking protocols, services, devices, and media at the two lowermost layers of the seven-layer OSI reference model: the *Data Link* and *Physical* layers. (The OSI model is discussed later in this section.) The Data Link layer is further divided into two layers: the Logical Link Control (LLC) layer and the MAC layer. Table 8-1 lists various standards in the IEEE 802 family.

Table 8-1. The IEEE 802 family of networking standards

Standard	Description
802.1	Defines higher-level standards for internetworking.
802.2	Defines Logical Link Control (LLC).
802.3	Defines Ethernet networks using Carrier Sense Multiple Access/Collision Detection (CSMA/CD).
802.4	Defines Token Bus networks.
802.5	Defines Token Ring networks.
802.6	Defines Metropolitan Area Networks (MANs).
802.7	Technical advisory group for broadband LAN using coaxial cabling. This group is now disbanded.
802.8	Technical advisory group for fiber optic. This group is now disbanded.
802.9	Technical advisory group for integrated services. This group is now disbanded.
802.10	Defines interoperable security for LAN/MAN.
802.11	Defines wireless networks.
802.12	Defines Demand Priority networks using 100 Mbps or more speeds. including the 100BASEVG-AnyLAN (Hewlett-Packard).

Each of the standards listed in Table 8-1 defines different characteristics of the network, such as network access method, topology, speed, and type of cabling.

The Network+ exam covers only IEEE 802.2, 802.3, 802.5, and 802.11 standards.

IEEE 802.2

The 802.2 standard describes how the upper-layer protocols access the *Logical Link Control (LLC)*, which is the upper layer of the two Data Link layers in the OSI model. This standard defines how different protocols manage the *error control* and data *flow control*. Error control refers to detection and retransmission of dropped packets, if requested. Flow control refers to management of data flow between network devices so that they can efficiently handle flow of information.

IEEE 802.3

The IEEE 802.3 standard describes characteristics for Ethernet networks at the Physical layer and at the MAC sublayer of the Data Link layer. This is a whole family of standards that define Ethernet networks with a variety of speeds and cabling. The IEEE 802.3 family of standards is collectively known as 802.3x standards.

Speed
: The original IEEE 802.3 standard defined a speed of 10 Mbps over thin coaxial cable in Ethernet networks. With the Fast Ethernet standard 802.3u, the speed can go up to 100 Mbps. The 802.3z standard defines Gigabit Ethernet with a speed of up to 1000 Mbps.

Access method
: The access method defines the process for network devices to access network media. Ethernet networks use the *Carrier Sense Multiple Access/Collision Detection (CSMA/CD)* method. Devices on the network continuously monitor the network media. If two devices start the transmission simultaneously, data collision occurs. If a collision occurs, the sending device is required to wait for a specified time before it can retransmit.

Topology
: Original Ethernet networks could be wired using either the star or the bus topology using coaxial or twisted pair cables. IEEE 802.3u and 802.3z use only star topology with twisted pair cables.

Media
: Media refers to the physical cabling of the network. A variety of cables types can be used with IEEE 802.3x standards including coaxial, twisted pair, and fiber optic. The choice of cables mainly depends on the specific standard used in the network.

IEEE 802.5

The IEEE 802.5 standard defines characteristics for Token Ring networks, originally developed by IBM. *Token Ring* is a LAN protocol that works at the Data Link layer of the OSI model. The Token Ring technology is rarely used these days because of the popularity of Ethernet networks. Even IBM no longer supports networks based on Token Ring technology. The characteristics of the IEEE 802.5 standard are as follows:

Speed
: The transfer speed of IEEE 802.5 Token Ring networks is 4 Mbps and 16 Mbps.

Access method
: Token Ring networks use the *Token Passing* access method. This uses a special three-byte frame known as a *token* that travels around the ring. The token keeps looking for a device on the ring that needs to transmit data. The device must acquire the token before it can transmit data on the network. Only one device can possess the token and transmit data at a time. The token travels with the data to the destination device where it is detached from the data and becomes free.

Topology

The physical setup of a Token Ring network is a star, while the logical setup is in a ring topology. A central device known as Multi-Station Access Unit (MSAU or MAU) is used to create a physical star topology.

Media

The IEEE 802.5 standard defines the use of unshielded twisted pair (UTP) and shielded twisted pair (STP) cables.

IEEE 802.11

The IEEE 802.11 family of standards defines several protocols used for wireless communications. This standard defines all aspects of wireless communications from the frequency range specifications to physical layouts to authentication mechanisms. The original IEEE 802.11 standard is known as *legacy 802.11*. The characteristics of the IEEE 802.11 standard are as follows:

Speed

The data transfer speed defined in the legacy 802.11 standard was limited to 1 or 2 Mbps within the frequency range of 2.4 GHz. Speeds for other 802.11 standards are discussed later in this section.

Access method

Wireless networks use Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA), which is a variation of the CSMA/CD access method. The devices on the wireless network “listen” to the network for “silence” before they start transmission. This helps avoid collisions on the network media.

Topology

Wireless networks defined in IEEE 802.11 standards can be implemented in either *Ad-hoc* or *Infrastructure* topology as discussed earlier in this section.

Wireless networks defined in IEEE 802.11 standards use radio frequencies with spread spectrum technology: *frequency-hopping spread spectrum (FHSS)* or *direct-sequence spread spectrum (DSSS)*. Spread spectrum technologies are discussed later in this section. The most popular of the IEEE 802.11 wireless network standards are 802.11b, 802.11a, and 802.11g. Security standards for these protocols are defined in the 802.11i standard.

IEEE 801.11b. The *IEEE 802.11b* standard defines DSSS-based network devices that use a 2.4 GHz frequency range and can communicate at speeds of 1,2, 5.5, or 11 Mbps. This standard is compatible with the legacy 802.11 standard. 802.11b is designed for a *point-to-multipoint* wireless communication setup. Usually a wireless access point (AP) is used with an omni-directional transmission antenna and can communicate with wireless clients located in the coverage area around the AP. The indoor range of a 802.11b wireless AP is about 100 feet (30 meters) at 11 Mbps speed When used with 1 Mbps speed, the range can be as high as 300 feet (90 meters).

IEEE 802.11a. The IEEE 802.11a standard uses a 5GHz frequency range with up to 54 Mbps data transmission speed. This standard defines the use of 52-subcarrier *Orthogonal Frequency-Division Multiplexing (OFMD)*, which is a modulation technique. (Modulation techniques are covered later in this section.) If required, the data speed can be reduced to 48, 36, 24, 18, 16, 12, 9, and 6 Mbps. The IEEE 802. 11a standard is not backward-compatible with the 802.11b standard. The range for 802.11a-based devices is also about 100 feet (30 meters) when used indoors.

IEEE 802.11g. The IEEE 802.11g standard defines a frequency range of 2.4 GHz (same as 802.11b) but with much higher data transfer speeds of up to 54 Mbps. The data speed can fall back to lower values. IEEE 802.11g is backward-compatible with 802.11b standard devices. The devices normally use the OFDM modulation technique but can switch back to *Quadrature Phase-Shift Keying (QPSK)* modulation when the data speed falls back to 5.5 or 11 Mbps. Since it operates in the already crowded frequency range of 2.4 GHz, the 802.11g device is also susceptible to interferences such as the 802.11b devices.

Table 8-2 gives a brief comparison of the characteristics of different 802.11 standards.

Table 8-2. Comparison of 802.11 standards

802.11 standard	Operating frequency	Maximum speed	Modulation technique
802.11	2.4 GHz	1 Mbps or 2 Mbps	FHSS or DSSS
802.11b	2.4 GHz	11 Mbps	DSSS
802.11a	5 GHz	54 Mbps	OFDM
802.11g	2.4 GHz	54 Mbps	OFDM and QPSK

Fiber Distributed Data Interface (FDDI)

The FDDI networking standard is based on Token Ring topology and describes the use of dual rings in order to provide fault tolerance to the network. It uses fiber optic cables, and the length of a single cable segment can be more than 200 Km. A variation of FDDI exists that uses copper wires and is called the *Copper Distributed Data Interface (CDDI)*. CDDI uses the same protocols as FDDI. The characteristics of the FDDI standard are as follows:

Speed

FDDI networks can achieve a maximum data transfer speed of up to 100 Mbps.

Access method

Since this topology is based on Token Ring, the devices use the token passing method to access network media

Topology

FDDI is based on dual ring topology that provides fault tolerance.

Media

As the name suggests, FDDI uses fiber optic cables.

Types of Cables

The cables used for computer networks fall into three main categories: Coaxial, Twisted Pair, and Fiber Optic. Each of the cable types has its own merits and demerits in terms of their cost, installation, maintenance, and susceptibility to interferences. Coaxial cables are rarely used these days because of the vast popularity gained by twisted pair cables. The following sections discuss each of the cable types covered in the Network+ exam.

Coaxial cable

Coaxial cables are mainly used for carrying television signals (for example, CATV), but some older computer networks based on the 10Base2 standard also utilized these cables for connecting workstations and other network devices. Usually the coaxial cables used for different purposes have different characteristics; cables for one purpose cannot be used for another. For example, the cable used for CATV cannot be used for computer networks. Figure 8-9 shows a piece of coaxial cable.

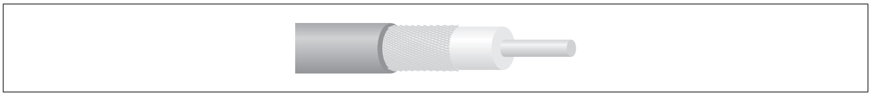


Figure 8-9. Coaxial cable

Coaxial cable networks are easy to install and low in cost. The downside is that they are prone to degradation of signals as they travel long distances. This degradation is called *attenuation*. They can also break easily and cause network downtime. Coaxial cables fall mainly into the following two categories:

Thin coaxial cable
: Also known as *Thinnet*. The type of thin coaxial cable used for computer networks is *RG-58*, which has 50-Ohm resistance. Network segments using this cable are used with 50-Ohm *terminators* and devices are connected using 50-Ohm *BNC-T* connectors. The *RG-6* type coaxial has 75-Ohm resistance and is used for CATV and cable modem.

Thick coaxial cable
: Also known as *Thicknet*. The type of thick coaxial cable used for computer networks is *RG-8*. As the name suggests, this cable is about twice as thick in diameter as thin coaxial cable. These cables use vampire taps, which cut through the cable to provide connectivity to network devices. *Vampire Taps* use transceivers with a 15-pin AUI connector. Thick coaxial cables also use 50-Ohm terminators on both ends of the network segment.

Twisted pair cables

Twisted pair cables have replaced coaxial cables in most computer networks. These cables use twisted pairs of insulated cables bundled inside a plastic sheath. The twists in cables are used to prevent electromagnetic interference, which results in crosstalk, among cables. Twisted pair cables are easy to install, lower in cost than coaxial and fiber optic cables, and can achieve greater data transmission speeds than coaxial cables. These cables are usually identified by their category numbers. The *category number* indicates the number of cable pairs and the purpose for which they can be used. These category numbers are denoted as CAT-1, CAT-2, CAT-3, CAT-5, etc. Figure 8-10 shows a piece of twisted pair cable.

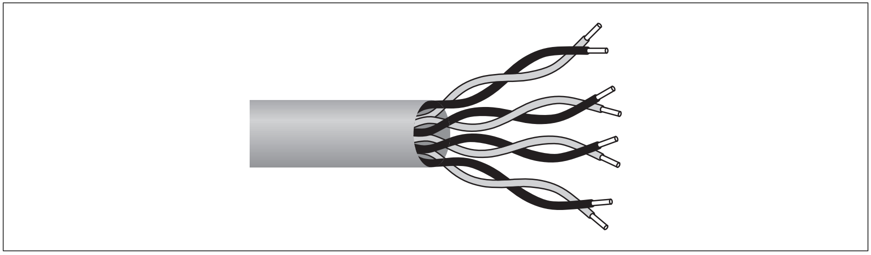


Figure 8-10. Twisted pair cable

Unshielded Twisted Pair (UTP) cables. UTP cables are the most commonly used of the two types of twisted pair cable categories. UTP cables are inexpensive and easy to install and maintain. These cables are vulnerable to electromagnetic interferences (EMI) and radio frequencies interferences (RFI) and hence cannot carry data signals to longer distances. Electric or electronic equipment and high-voltage electric cables in the vicinity of these cables can cause significant disturbances.

Shielded Twisted Pair (STP) cables. STP cable comes with a layer of shielding material between the cables and the sheath. STP cables provide some degree of protection from EMI and RF disturbances and can carry signals to greater distances. But this advantage comes with the extra cost of installation.

Table 8-3 lists some of the popular UTP and STP categories.

Table 8-3. Categories of UTP and STP cables

Category	Description
CAT-1	Used for voice transmissions; not suitable for data transmissions.
CAT-2	Used for voice and low speed data transmissions up to 4 Mbps.
CAT-3	Used for both voice and data transmissions. Used in Ethernet, Fast Ethernet, and Token Ring networks. It is rated at 16 MHz and 10 Mbps speed.
CAT-4	Used for both voice and data transmissions. Rated at 20 MHz and 16 Mbps speed. Used in Ethernet, Fast Ethernet, and Token Ring networks.
CAT-5	Used for both voice and data transmissions. Rated at 100 MHz. Used in 100 Mbps Ethernet, 1000BaseT Fast Ethernet, Token Ring, and 155 Mbps ATM networks.
CAT-5e	Used for 100 Mbps and 1000 Mbps Gigabit Ethernet networks. Rated at 125 MHz.
CAT-6	Used for both voice and data transmissions. Rated at 250 MHz. Used in Ethernet, Fast Ethernet, Token Ring, and 155 Mbps ATM networks.
CAT-6 (STP)	Used for data transmissions. Supports up to 600 MHz and used in Ethernet, Fast Ethernet, Gigabit Ethernet, Token Ring, and 155 Mbps ATM.

Fiber optic cables

Fiber optic (also called *Optical Fiber*) cable is made up of very thin glass or plastic stretched out and put inside a sheath. The transmission in fiber optic cables is based on the transport of light signals. An optical transmitter is located at one side of the cable and a receiver is at the other side. Fiber optic cables are immune to EMI and RF disturbances because they depend on optical signals unlike electrical signals in UTP/STP cables. They can also carry data signals longer distances than do UTP or STP cables due to minimal attenuation. It is also considered the most secure of all cable types.

Fiber optic cables are very expensive in terms of the cost involved in installation and maintenance. It needs expensive hardware, skilled technicians, and special tools for installation. This is the reason that fiber optic cable is used only in data centers for providing high-end connections to critical servers and other network devices where high-speed data transfers are required. Figure 8-11 shows a piece of fiber optic cable.

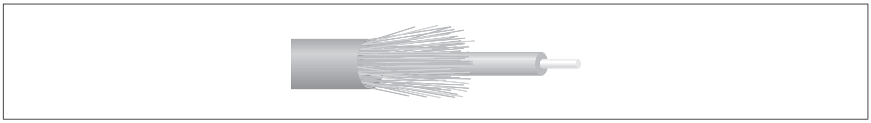


Figure 8-11. Fiber optic cable

The two main types of fiber optic cables are *single mode* and *multimode*.

Single mode fiber optic cable. The single mode fiber optic cable is made up of a core glass or plastic fiber surrounded by a cladding. It uses a single beam of light and can thus travel to greater distances than a multimode fiber optic cable. Single mode fiber optic cable uses an 8 to 10 micron core and 125 micron cladding. Figure 8-12 shows a typical single mode fiber optic cable.

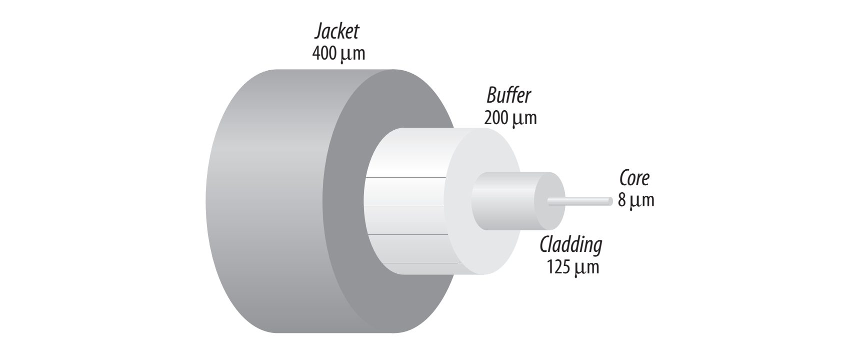


Figure 8-12. Single mode fiber optic cable

The core and cladding for fiber optic cables is measured in terms of *microns*. One micron is equal to one millionth of a meter or one thousandth of a millimeter.

Multimode fiber optic cable. The multimode fiber optic cable is made up of a 50 micron or a 62.5 micron core and 125 micron cladding. In this cable, multiple beams of light travel through the core and are reflected by the cladding. Some of the beams even get refracted into the cladding, causing loss of signal. This reduces the distance that data signals can travel in a multimode fiber optic cable.

Networking and Cable Standards

Ethernet networking and cabling are defined in IEEE 802.3 standards. There are several variations in this standard, depending on speed, length, topology, and cabling used in implementing networks. The following sections provide a brief summary of the standards tested on the Network+ exam.

10 Mbps Ethernet

The 10 Mbps standards include 10Base2, 10BaseT, and 10BaseFL. All these standards define a maximum data transfer speed of 10 Mbps. This speed is now considered obsolete for most networks. It is unlikely that you will encounter any 10 Mbps networks in your career. The following are different variations of 10 Mbps networks:

10Base2

The IEEE 802.3a standard defines 10Base2 Ethernet networks. This standard defines the use of RG-58 coaxial cabling with a maximum segment length of 185 meters. The network can achieve a maximum speed of 10 Mbps. The segments are typically wired in physical bus topology using *BNC connectors*, and each end of the cable must be terminated using *50-Ohm terminators*. The 10Base2 standard allows a maximum of five segments, out of which only three segments can be populated. There should be a minimum distance of 0.5 meter between nodes.

10BaseT

The 10BaseT Ethernet standard defines use of CAT 3, 4, or 5 UTP cables with a maximum of 100 meters for each cable length. All computers (nodes) are connected in a point-to-point fashion to a central device known as the hub or the switch. These devices can further be cascaded to extend the network. It is typically wired in a physical star topology that makes it easy to add or remove nodes without affecting the network. 10BaseT also allows a maximum of five network segments in each network. The five segments can be connected using four repeaters. Unlike the 10Base2 networks, all five segments can be populated.

10BaseFL

The 10BaseFL Ethernet standard uses fiber optic cables in order to increase the cable segment lengths to 2000 meters. It is also wired in a physical star topology using SC or ST connectors. Due to its speed limitations, this technology is hardly used these days.

Table 8-4 gives a summary of 10 Mbps networking standards.

Table 8-4. Summary of 10 Mbps networking standards

Standard	Cable	Length of segment	Network topology	Connector
10Base2	Thin coaxial	185 meters	Bus	BNC
10BaseT	UTP CAT 3, 4, or 5	100 meters	Star	RJ-45
10BaseFL	Fiber optic	2000 meters	Star	SC or ST

100 Mbps Ethernet

Most of the modern networks support 100 Mbps speeds, which provide better bandwidth for demanding applications. In fact, the 100 Mbps standard has become a minimum requirement these days. The following is a brief description of 100 Mbps standards.

100BaseTX

100BaseTX networks use two pairs of UTP CAT 5 cable. The length of cable segments can be up to 100 meters.

100BaseT4

100BaseT4 networks use four pairs of CAT 3, 4, or 5 type cables. The length of cable segments can be up to 100 meters.

100BaseFX

100BaseFX networks use multimode or single mode fiber optic cables and provide up to 100 Mbps of data transfer rates. The length of cable segment can be up to 412 meters for multimode and 10,000 meters for single mode cable.

Table 8-5 gives a summary of 100 Mbps networking standards.

Table 8-5. Summary of 100 Mbps networking standards

Standard	Cable	Length of segment	Network topology	Connector
100BaseTX	CAT 5	100 meters	Star	RJ-45
100BaseT4	Four pairs of CAT 3, 4, or 5	100 meters	Star	RJ-45
100BaseFX	MM fiber or SM fiber	MM fiber-412 meters SM fiber-10,000 meters	Star	SC or ST

The 10Base2 and 100BaseT4 are not covered in the Network+ exam. These are included in this section for your reference only.

1000 Mbps Ethernet

The 1000 Mbps (1 Gigabit) Ethernet networks are also known as *Gigabit Ethernet*. These networks use either copper-based or fiber optic cabling. These networks are implemented mainly as a *backbone* for large networks. The following is a brief description of Gigabit Ethernet standards:

1000BaseX

The IEEE 802.3z specifies the 1000BaseX standards that describe three different Gigabit standards: 1000BaseLX, 1000BaseSX and 1000BaseCX. The 1000BaseLX and 1000BaseSX use multimode or single mode fiber optic cables. The 1000BaseLX uses long wavelength laser beams while the 1000BaseSX uses short wavelength laser beams. The 1000BaseCX standard specifies use of shielded twisted pair (STP) cables.

1000BaseT

The IEEE 802.3ab specifies the 1000BaseT standard. It uses four pairs of CAT 5 UTP cable. Each pair of the CAT 5 cable can achieve maximum data transfer speeds of up to 250 Mbps, making it an overall 1000 Mbps.

Table 8-6 gives a summary of Gigabit Ethernet networking standards.

Table 8-6. Summary of Gigabit Ethernet networking standards

Standard	Cable	Length of segment
1000BaseLX	MM fiber optic or SM fiber optic	MM fiber-550 meters SM fiber-5,000 meters
1000BaseSX	MM fiber –50 Micron	550 meters
1000BaseCX	STP	25 meters
1000BaseT	UTP	75 meters

10 Gigabit Ethernet

The 10 Gigabit Ethernet networks are specified in the IEEE 802.3ae standard. These networks can achieve a maximum data transfer speed of up to 10,000 Mbps (10 Gbps). All these networks are used for *baseband* transmissions, in which digital or analog signals are carried on a single channel. The following is a brief description of 10 Gigabit Ethernet standards:

10GBaseSR

SR stands for *Short Range* optical technology. These networks use 50 micron or 62.5 micron multimode fiber optic cable. The length of the cable segment varies from 33 meters to 330 meters, depending on the type of cable used.

10GBaseLR

LR stands for *Long Range* optical technology. These networks use single mode fiber optic cable. The length of the cable segment can be up to 10,000 meters (10 Km).

10GBaseER

ER stands for *Extended Range* optical technology. These networks use single mode fiber optic cable. The length of a cable segment can be up to 40,000 meters (40 Km).

Table 8-7 provides a summary of 10 Gigabit Ethernet standards.

Table 8-7. Summary of 10 Gigabit Ethernet networking standards

Standard	Cable	Length of segment
10GBaseSR	MM fiber optic	33 meter for 50 or 62.5 micron, and 330 meter for 50 micron
10GBaseLR	SM fiber optic	10,000 meter
10GBaseER	SM fiber optic	40,000 meter

Other 10Gbps standards described in the IEEE 802.3ae specification are 10GBaseSW, 10GbaseEW, and 10GBaseLW. None of these is covered in the Network+ exam.

Media Connectors

Media connectors are used for terminating cables. In other words, they provide an interface to connect the cables to devices. Different types of cables use different types of connectors. It is not possible to connect a cable to a device without first terminating it with a suitable connector. Each connector has two variations: a male connector and a female connector. The following sections provide a summary of connectors used for computer networking.

Registered Jack-11 (RJ-11)

The RJ-11 connector is mainly used for terminating telephone wires. It has a capacity of three telephone lines (six pins) but only four pins are commonly used. The connector looks similar to the RJ-45 connector used in computer networking. It comes in a plastic casing and is smaller than the RJ-45 connector. Only two pins are used for a single telephone line, but four pins are used for a Digital Subscriber Line (DSL). Most installers provide all four wires in order to connect an extra telephone line, if required.

Registered Jack-45 (RJ-45)

The RJ-45 connector is little bigger than the RJ-11 connector and is used for terminating twisted cables. It uses eight pins, instead of four or six, in the RJ-11 connector. RJ-45 is the most common type of connector used in computer networks. Cables can be wired in either a straight or crossover fashion using the RJ-45 connectors. Figure 8-13 shows an RJ-45 connector.

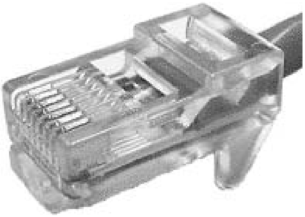


Figure 8-13. RJ-45 connector

F-Type

The F-Type connector (or simply the *F connector*) is used to terminate RG/6 and RG/59 coaxial cables used with cable television. They are also used for connecting cable modems and satellite receivers. The connector has a screw that is tightened to secure the physical connection. Figure 8-14 shows an F-Type connector.

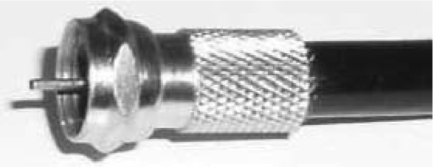


Figure 8-14. F-Type connector

BNC connectors

BNC connectors (BNC stands for *Bayonet Neil-Concelman*) are also used for terminating coaxial cables, but unlike the F-Type connectors, they do not use the screw. The connector is twisted to make the connection. These connectors are commonly used with 10Base2 networks that use thin coaxial cable. Since 10Base2 networks are rarely used these days, the BNC connectors are also not much in use. The BNC family of connectors includes T-connectors, Barrel connectors, and terminators. Figure 8-15 shows some BNC T-connectors.

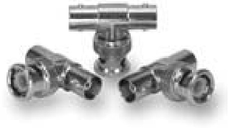


Figure 8-15. BNC connectors

Fiber optic connectors

Connectors used for fiber optic cabling come in a variety of shapes. Due to fast developments in this technology, a large number of connectors are not available in the market. These include push-pull, snap-in, and twist type connectors. All connectors are used in pairs to allow *full-duplex* communications. The Network+ exam expects you to identify only four types of connectors: SC, ST, LC, and MT-RJ. A brief description of these connectors is given in the following paragraphs:

Subscriber/Standard Connector (SC)
An SC connector uses the push-pull mechanism and is shown in Figure 8-16. This connector provides good protection for the ends of a fiber optic cable and is easier to connect and disconnect in tight spaces than the ST connector, which is listed next.

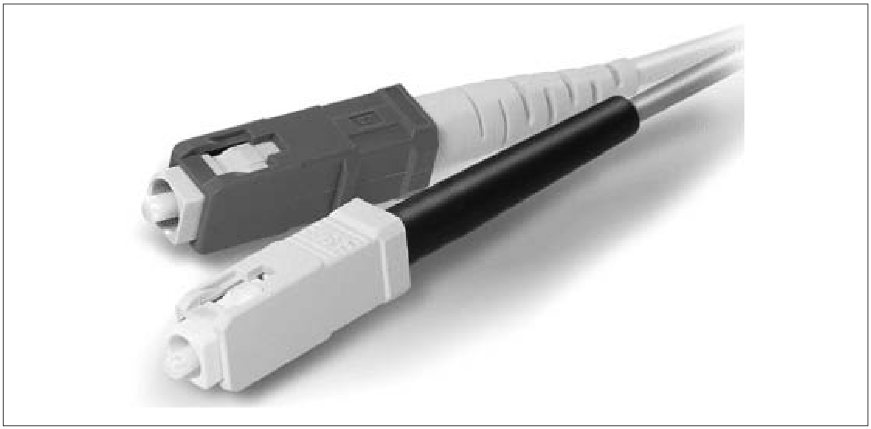


Figure 8-16. SC connectors

Straight Tip (ST)
An ST connector is an older type of fiber optic connector. It uses the "twist-on/twist-off" bayonet mechanism to make the connection. Figure 8-17 shows an ST connector.

Lucent Connector (LC)
An LC connector has a small flange on top that secures the connection in place. This connector also uses the push-pull mechanism. Figure 8-18 shows an LC connector.

Mechanical Transfer-Registered Jack (MT-RJ)
An MT-RJ connector resembles an RJ type connector. These connectors always hold two fiber cables to allow full-duplex communications. Figure 8-19 shows two MT-RJ connectors.

IEEE 1394

The IEEE 1394 interface is also known as *Firewire*. This interface is mainly used in high-bandwidth applications, such as digital video and portable storage. The IEEE 1394 connectors come in six-pin and four-pin configurations as shown in Figure 8-20.

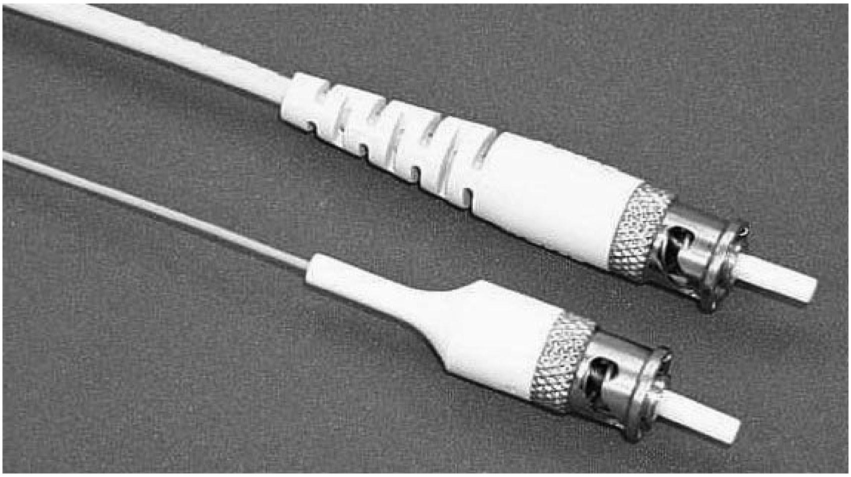


Figure 8-17. ST connectors

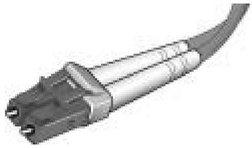


Figure 8-18. LC connector

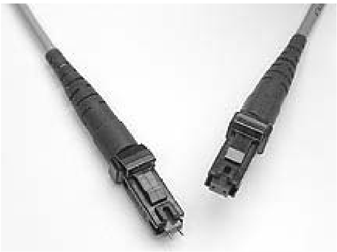


Figure 8-19. MT-RJ connectors

Universal Serial Bus (USB)

USB interfaces have become very popular in computers and other digital consumer devices due to their performance and Plug-n-Play-compatibility. USB devices can be connected or disconnected into any device without having to turn off power. These devices do not need any manual configuration. USB connectors are available in a variety of sizes and shapes, but the two popular types are: *Type A* and *Type B*. The Type A connector is mainly used on computers and the Type B connectors are mainly used for peripherals. Figure 8-21 shows both Type A and Type B connectors.

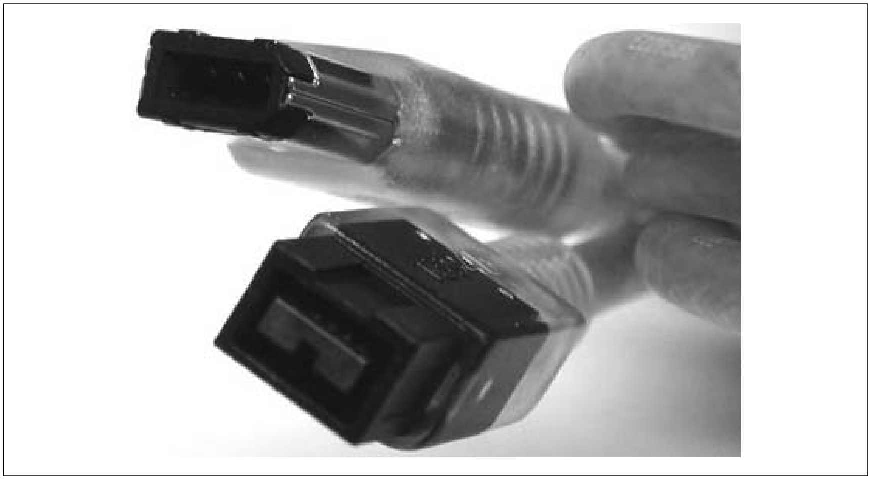


Figure 8-20. IEEE 1394 connectors

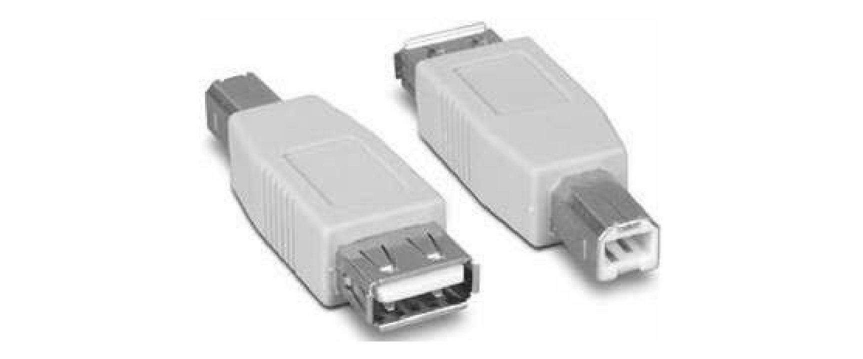


Figure 8-21. USB Type A(Left) and Type B (Right) connectors

Network Devices

As noted earlier in the section "Physical Network Topologies," a small bus network can be built without any active device. This network is difficult to expand due to its limitations. Network devices, as discussed in the following sections, are used to connect multiple systems as well as to connect smaller network segments to form a large *internetwork*. This section covers a brief description of commonly used networking devices, which include network interface cards (NICs), hubs, switches, bridges, and routers.

Hubs

An *Ethernet hub* (or a *concentrator*) is the central device in a network segment that connects all nodes in the segment. It receives signals on one of its ports and retransmits them to all other ports except the receiving port. It is also known as a multiport repeater. Hubs work at the Physical layer (Layer 1) of the OSI model.

Since a hub cannot decide the destination port, it is considered an inefficient device. In a typical implementation, UTP cables are used to connect nodes (computers or printers) to hubs. Hubs can be cascaded (joined together) to extend the network segment. Most ports of the hub use RJ-45 connectors, but AUI and BNC connectors are also provided to extend the segment to legacy 10Base2 and 10Base5 networks. The two types of hubs are described here:

Active hub
: An active hub receives signals at its ports and regenerates them before passing them onto all other ports. However, it does not perform any processing in terms of error checking.

Passive hub
: A passive hub acts as a simple gateway for incoming signals and does not regenerate them before passing them onto other ports.

Ethernet hubs are available in a variety of sizes and costs, depending on the number of ports. Smaller hubs with 4, 8, or 12 ports are known as *workgroup hubs*, while hubs with 24 or 32 ports are known as *high-density hubs*.

Switches

Like a hub, a switch is also the central device that connects multiple nodes in a network segment using UTP or STP cables. But unlike the hub that sends the received signal to every port, a switch sends the signal only to the destination node. A switch is an intelligent device that learns the MAC address of the destination from the data packet and sends the packet to the intended node only. This results in data direct communication between two nodes, improved network performance, and reduced collisions.

Switches work at the Data Link layer (Layer 2) of the OSI networking model. Switches can work in a *full-a mode*, which is a mode that enables nodes to transmit and receive data simultaneously. Thus a 100 Mbps switch working in a full-duplex mode can provide 200 Mbps data transfer speed. Switches are preferred in large networks where hubs can become a bottleneck for network performance.

Switches forward data packets using one of the following forwarding techniques:

Cut Through
: The switch reads only the hardware address from the data frame and starts sending it to the destination. It does not perform any error checking. This improves speed. A switch using a cut-through technique may fall back to the store-and-forward technique if it finds that the destination port is busy at the time of transmission.

Store-and-Forward
: The switch stores the entire packet in its memory buffer and performs error checking. This prevents forwarding of errors onto the rest of the network. This method is slower than the cut-though method due to the error-checking process, and affects network performance.

Fragment Free

The switch takes advantage of both cut-through and store-and-forward techniques. It reads the first 64 bytes of the frame and leaves error checking to the next device working at the upper layers of OSI model.

> The fourth switching method used by switches is *adaptive switching*, which is not covered on the Network+ exam. Adaptive switching allows a switch to automatically switch between the other switching methods as needed.

Media Access Unit (MAU)

An MAU—also called Multi-Station Access Unit (MSAU)—is used in Token Ring networks as a central device that connects all nodes in the network segment. This is equivalent to using a hub or a switch in Ethernet networks and results in giving the network a physical star look, though its logical topology remains a ring. Multiple MAUs can be connected using the Ring In (RI) and Ring Out (RO) ports in order to extend the network. The RO port of one MAU is connected to the RI port of the second MAU, and so on. The RO port of the last MAU is connected back to the RI port of the first MAU in the network to complete the ring.

Bridges

A network *bridge* is used for two purposes: connecting two LAN segments to form a larger segment and dividing a large network segment into smaller segments. It works at the Data Link layer (Layer 2) of the OSI model. Like network switches, bridges also learn the MAC address of devices and forward data packets based on the destination MAC address. In older bridges, the MAC addresses had to be defined manually, and it took a significant amount of time to configure a bridge. Most of the newer bridges can dynamically build lists of MAC addresses by analyzing data frames. These bridges are called *learning bridges*, due to this advanced functionality.

Most of the functionality of bridges is now available in switches. Hence, they are rarely used in networks these days. Bridges fall into the following categories:

Transparent Bridge

This bridge forwards data packets to the destination network segment by reading the destination MAC address. The network devices are unaware of the presence of the bridge. This bridge builds the MAC address table as it receives data packets. If the bridge does not find a destination MAC address in its list, it floods all ports with the data packet except the source port.

Source Route Bridge

This bridge is used in Token Ring networks. The bridge uses two frame types to find the route for the data: a *Source Route (SR)* frame and an *All-Route (AR)* frame.

Translation Bridge

This bridge is used to connect two network segments that use different protocols at the Data Link layer. For example, a translation bridge can join a Token Ring network to an Ethernet network or an FDDI to a Token Ring.

Spanning tree protocol. The problem with bridges is that they cannot be used for large networks. When multiple bridges are used in a large network, they start confusing each other. This results in *bridging loops*, a term used when one bridge makes the other bridge believe that a device is located in a network segment—while it actually is not. To overcome the bridging loops problem, bridges use the *spanning tree protocol*. This is defined in the IEEE 802.1d standard. Using this protocol, the bridge interfaces are assigned a value that helps control the way bridges learn MAC addresses and disable inactive or nonexisting links.

Routers

Routers are used to connect two or more network segments. These devices work on the *Network layer (Layer 3)* of the OSI model. Routers use Internet Protocol (IP) addresses to determine the source and destination of the data packet. Typically, routers receive the data packet, determine the destination IP address, and forward the packet to the next *hop*, which may either be the final destination of the packet or another router on the path. Routers can be implemented as a software service or as a dedicated hardware device. A wired or wireless router in a home network is an example of a small network router that connects the home network to the ISP's network. Microsoft's Routing and Remote Access Service (RRAS) is an example of a software router. A Windows Server 2000/2003 computer with at least two network interface cards can be configured as a router to connect network segments.

Routers communicate to each other using routing protocols. They maintain a list of IP addresses in *routing tables*. Routing tables can be built statically or dynamically as discussed in the following list:

Static routing

When *static routing* is used, administrators manually configure routing tables by entering appropriate routing information. This method works only for very small networks. In large networks, it is very difficult to manually configure routing tables. As the routing tables grow or there is a change in the network, the routing tables must be updated manually. The process is time-consuming and error-prone.

Dynamic routing

Routers use dynamic routing protocols when working in a dynamic routing environment. Dynamic routing protocols enable routers to get routing information from other routers and advertise their own routing information in order to build and maintain routing tables. Dynamic routing protocols fall into two categories, discussed next.

Distance vector routing protocol. A distance vector routing protocol assumes that the network is made up of several routers. Routers using this protocol depend on other routers to advertise their routing information periodically. These advertisements (or updates) are typically sent every 30 seconds. Routers can also be configured to send triggered updates when they detect any change in network topology.

RIPv1 (Routing Information Protocol version 1) and RIPv2 (Routing Information Protocol version 2) are distance vector protocols that work on the principle of *hop count*. RIPv1 works only on TCP/IP networks, while RIPv2 works on both TCP/IP and IPX/SPX networks. The RIP version that supports IPX is sometimes called *IPX RIP* also. A *hop* is a value assigned to each router on the way to the final destination. RIP supports a maximum of 15 hops in the network. A destination beyond 15 hops is considered unreachable. The following are the main disadvantages of distance vector routing protocols:

- Periodic update is a slow process that affects network performance.
- Periodic updates generate considerable network traffic, making the protocol inefficient on large networks.
- *Routing loops* are created when routers advertise incorrect routing information.

There are two methods to get around the routing loops problem in distance vector protocols. The first method is *split horizon*, which prevents a router from advertising a route to the same router from which it received the route information. The second method is *poison reverse*, which advertises back the route it learns from a router with a hop count of 16 (unreachable).

Link state routing protocol. Link state routing protocols use *Link State Advertisements (LSA)* to update routing tables. The LSA is a data packet that contains routing information about the sending router only. This packet is sent to all routers in the network so that other routers can build routing tables. This is in contrast with the distance routing protocols where all routers advertise their entire routing tables to all other routers, thus generating significant amount of network traffic.

Open Shortest Path First (OSPF) and NetWare Link State Protocol (NLSP) are examples of link state routing protocols. The link state routing protocols are best suited for large networks, as there is no limit such as the hop count. They keep update traffic to the minimum and can correct the routing table information quickly if there is a change in the network topology. This characteristic is known as *convergence*.

Gateways

In computer networks, a gateway is a device that translates one format of data packets to another format. They are also called *protocol translators*. A router connecting two different types of network segments or a bridge connecting two network segments using different Layer 2 protocols are examples of gateways. Gateways are necessary to provide interoperability between two distinct network formats. It is notable that gateways only convert (translate) data formats, but the that data itself remains unchanged.

Channel Service Unit (CSU)/Data Service Unit (DSU)

A CSU/DSU is a digital interface device that connects a local area network to a wide area network. Typically, the CSU/DSU is installed between a LAN and the access point provided by the provider of the WAN service. Most of the newer routers now include the functionality of CSU/DSU. For example, a router connecting a LAN to the Internet is also functioning as a CSU/DSU unit.

Network Interface Card (NIC)

An NIC, or a *network adapter*, is a hardware device that connects a computer to the network. It allows computers to communicate over the network using standard networking protocols. It works at the Data Link layer (Layer 2) of the OSI model. Every card has an RJ-45, a BNC, or an AUI socket where the network cable is connected. A light-emitting diode (LED) usually indicates the status of the card whether it is active or not. Older cards supported only 10 Mbps data transfer speeds, but the newer cards support 10/100 Mpbs or even 1000 Mpbs speeds.

Like other devices in the computer, network cards must also be configured to use certain system resources such as I/O Address (Input/Output Address), IRQ (Interrupt Request), and DMA (Direct Memory Access). Most of the newer cards are Plug-n-Play and are automatically configured by the system. However, before a card is purchased or installed, ensure that it supports the type of cabling used in the network. For example, a NIC-supporting fiber optic cable may not work in a network where UTP/STP cables are used.

Every network card comes with a device driver that needs to be installed to configure it properly on a system. In older cards, network technicians had to configure them manually by setting jumpers for the I/O address and IRQ. The driver software also had to be installed manually. As noted earlier, most new cards are automatically configured by software. However, in certain situations, you may need to download a driver from the vendor's web site and install it in order to let the system configure the card appropriately.

ISDN adapters

An ISDN adapter, or a *terminal adapter*, refers to a hardware device that connects a computer (terminal) to the *Integrated Services Digital Network (ISDN)* network. It is also called an ISDN modem. ISDN technology is mainly used for wide area networking using either Basic Rate Interface (BRI) or Primary Rate Interface (PRI). This technology provides higher data transfer speeds as compared to other technologies such as dial-up over ordinary telephone lines.

ISDN adapters can be added to a system on an expansion slot, or they can be standalone external devices connecting to the serial port of the computer. For example, some routers provide ISDN interfaces as a built-in feature. The ISDN technology is not so popular and has now been replaced by faster and more flexible WAN technologies.

Wireless Access Point (WAP)

A WAP, or simply an Access Point (AP), is a hardware device that is used to connect wireless devices to form a network. In its typical implementation, a WAP is also connected to the wired network and allows wireless clients to communicate to the clients located on the wired local area network (LAN). In a wireless network, all nodes, including the AP, have wireless transmitters and receivers, and communication takes place using radio frequencies. The transmission range of an AP is limited, and a large wireless network may need more than one AP to provide connectivity to all clients located at different places of the building. The range of the AP signals depends on the type of wireless standard used as well as on electromagnetic and radio frequency interferences.

WAPs are available in several different forms and capabilities. For example, a low-cost, small wireless router used to share an Internet connection at home also acts as an AP. This device not only provides connectivity to all computers but also acts as a gateway for Internet connectivity and automatically assigns IP addresses to them.

WAP also refers to *Wireless Application Protocol*, an open standard that enables mobile devices such as mobile phones or personal digital assistants (PDAs) to access the Internet.

Modems

The term *modem* is derived from *Modulator/Demodulator*. A modem is a hardware device that is used to convert digital signals from a computer to analog signals (modulation) in order to transmit them over analog lines. At the receiving end, it converts the analog signals back to digital signals (demodulation) so that a computer can understand them. In their typical usage, modems are connected to a computer in order to provide remote access (or Internet connectivity) using analog telephone lines. It can be built onto the motherboard of the computer, can be installed as an extension card, or can be an external device. External modems can either be connected to one of the serial ports or to the USB port of the computer.

When used as an internal device, modems must be configured to use system resources such as an I/O address or IRQ. Modems use the serial communication (COM) ports in a computer, and resources used by these ports must be available in order to correctly configure the modem. Table 8-8 provides a summary of the COM ports and resources used by them.

Table 8-8. COM ports and system resources

Serial port	IRQ	I/O address
COM1	4	03F8H
COM2	3	02F8H
COM3	4	03E8H
COM4	3	02E8H

Modems are available in different sizes, speed capabilities, and costs. The data transmission speed of a modem depends mainly on the type of Universal Asynchronous Receiver/Transmitter (UART) chip used and varies from 9.6 Kbps to over 900 Kbps. Modems with up to 115 Kbps speeds are commonly used for dial-up networking.

Transceivers and media converters

As the name indicates, a transceiver is a device that combines the functions of a transmitter and a receiver. It does not refer to any standalone or separate hardware device but is normally built into devices such as network cards, modems, hubs, switches, or routers. Depending on the type of network cabling in use, you may find fiber optic transceivers used in fiber optic networks; RF transceivers used in wireless networks, and Ethernet transceivers.

Media converters are used to enable interconnection of one type of media (usually cabling) to another type. For example, you may want to connect a network segment wired with a fiber optic cable to another segment wired with UTP/STP cables. In another example, you may wish to connect a coaxial cable segment to a UTP/STP network segment.

Firewalls

In a computer network, a firewall is a hardware device or software that is used to prevent undesired traffic. It protects the network from unauthorized external access and thereby protects system and network resources critical for running the business operations. Firewalls work on the basis of *rules* that dictate which traffic should be allowed and which traffic should be blocked. A firewall usually sits between an internal network and an external public network such as the Internet. They may also be used to separate different departments within an organization.

Software-based firewalls are usually a built-in feature of many network operating systems. Administrators usually configure these firewalls depending on the requirements of an organization. *Hardware-based* firewalls are either dedicated devices, or the functionality is built into other devices, such as routers.

Wireless Technologies

Wireless networks rely on radio transmissions to communicate instead of the network cabling used for normal computer networks. Radio frequencies create Electromagnetic (EM) fields, which become the medium to transfer signals from one computer to another. As you go away from the hub, or from the main equipment generating the wireless network's radio transmissions, the strength of the EM field reduces and the signal becomes weak. EM fields are also prone to interference, which can be introduced by walls, reflected radio waves, and the presence of other EM fields. The presence of wireless telephones, microwave ovens, television sets, and a number of other devices can potentially interfere and reduce the signal strength of wireless devices.

Spread spectrum wireless technology

In order to reduce the effects of interfering frequencies, wireless devices use the spread spectrum technology. This technology helps share available frequency bandwidth common to wireless devices. It also helps prevent jamming of radio signals due to strong interference from another source of radio frequency. Instead of using a fixed frequency, such as that used with radio and television broadcasts, wireless networks use a spectrum of frequencies. The sender uses a number of narrow-band frequencies to communicate with the receiver. Each narrow band of frequencies contains only a part of the signal. The receiver correlates the signals received at different frequencies to retrieve the original information. Spread spectrum technology synchronizes wireless signals using one of the following methods:

Frequency Hopping Spread Spectrum (FHSS)
: FHSS is the method of transmitting RF signals by rapidly switching frequencies according to a pseudorandom pattern, which is known to both the sender and the receiver. FHSS uses a large range of frequency (83.5 MHz) and is highly resistant to noise and interference. The amount of time the signal spends on any frequency is known as *dwell time*, and the amount of time it takes from switching one frequency to another is known as *hop time*. FHSS signals are difficult to intercept because the signals usually appear as noise. FHSS works in the unlicensed frequency range of 2.4 GHz and is used in HomeRF and Bluetooth. It has a limited speed of transmission that ranges from 1.6 to 10 Mbps.

Direct Sequence Spread Spectrum (DSSS)
: DSSS is a modulation technique used by wireless networks. It uses a wide band of frequency and it divides the signal into smaller parts and is transmitted simultaneously on as many frequencies as possible within a particular frequency band. DSSS adds redundant bits of data known as *chips*. The ratio of chips to data is known as *spreading ratio*. The higher the spreading ratio, the higher the immunity to interference. DSSS is faster than FHSS and ensures data protection, because chips are redundant and simultaneously transmitted. It utilizes a frequency range from 2.4 GHz to 2.4835 GHz and is used in 802.11b networks.

Infrared

Infrared technology employs electromagnetic radiations that use wavelengths that are longer than the visible light but shorter than radio frequency. This technology is used in night-vision equipment, thermography, digital cameras, and digital communication systems. Common examples of Infrared devices are the remote controls used by TVs and audio systems. The Infrared technology is standardized by the Infrared Data Association (IrDA). The following are some of the key characteristics of IrDA wireless communication technology:

- It supports point-to-point wireless communications between two devices.
- Infrared transmission uses a direct line of sight suitable for personal area networks.
- Infrared waves cannot penetrate walls.
- IrDA wireless communication technology supports data transfer speeds ranging from 10 to 16 Mbps.
- Infrared devices consume very low power.
- Infrared frequencies do not interfere with radio frequencies.
- IrDA wireless communication technology provides a secure wireless medium due to the short distance (usually 3 to 12 feet) between devices.

Bluetooth

Bluetooth wireless networking technology provides short-range communications between two or more devices. It is a low-cost networking solution widely used in telephones, entertainment systems, and computers. It is designed to overcome the limitations of IrDA technology. The following are some of the key characteristics of Bluetooth-based wireless communication:

- It supports transmission speeds from 1 Mbps (Bluetooth 1.0) to 3 Mbps (Bluetooth 2.0).
- It works over the unlicensed frequency range of 2.4 GHz.
- The devices must be within a short range of less than 10 meters.
- It uses FHSS technology.
- It offers high resistance to electromagnetic interferences.
- Unlike the Infrared signals, it does not require a direct line of sight.
- Bluetooth devices consume very low power.
- Two or more Bluetooth computers form an ad-hoc wireless network.

Factors that affect wireless services

Wireless services use radio frequencies that travel through the atmosphere. There are several factors that may affect the speed, signal quality, and range of wireless signals. These include interference from other electrical devices, the type of antenna used, and other environmental factors. This section covers a brief discussion of these factors.

Interferences. Atmospheric interferences to wireless signals cannot be prevented, but they can certainly be reduced to achieve optimum performance. Some of the major causes of interference include the following:

- Physical objects such as buildings, trees, concrete and steel walls. These objects can either significantly reduce signals or even completely block them.
- Electromagnetic interference (EMI) generated by high-power electric lines, power transformers, heavy electrical machinery, fans, light fixtures, etc.
- Radio frequency interference (RFI) generated by other wireless equipment working in the same frequency ranges used by computer wireless devices. Examples of these types of equipment are wireless phones, wireless game controllers, or microwave ovens.

Type of antenna. The range of wireless signals depends on the type of antenna used for transmitting radio frequency signals. Selection of an antenna is a critical part of implementing a wireless network. Different shapes and sizes of antennas offer different signal levels. The strength of a wireless antenna (called its *gain*) is measured in *decibels isotropic* (denoted as *dBi*). An isotropic antenna sends signals of equal strength in all directions. A simple rule for calculating effective strength of an antenna is that every 3 dBi of gain almost doubles its output.

Omni-directional antennas send wireless signals in all directions. This type of antenna is useful when the coverage is required equally around the point of transmission. On the other hand, *directional* antennas transmit signals in one direction only. This helps send the entire output of the transmitting device in one direction, in which case, signals are more effectively transmitted.

Environmental factors. Environmental conditions, including weather, significantly affect the speed, range, and coverage of wireless signals. These factors can have a bad impact on wireless signals.

Protocols and Standards

This section covers a study of different networking protocols and standards. First, I will explain the OSI networking model and then discuss commonly used networking protocols. I will explain how networking protocols are associated with network operating systems. This will be followed by a detailed study of the TCP/IP protocol suite, which are the most widely used networking protocols on private networks. The TCP/IP protocol suite is the only one used on the Internet.

Media Access Control (MAC) Address

The MAC address is a unique 48-bit (6 bytes) hardware address that is hardcoded into almost every networking device. This address is used by network protocols to deliver data to the correct host in the network. In devices that have multiple network interfaces, each interface has a unique MAC address. The Data Link layer of the OSI model is responsible for managing MAC addresses of network devices in the network.

The 48-bit MAC address is written as hexadecimal numbers in six groups of two bytes each, separated by colon (:) signs or hyphens (-). These numbers include 0 to 9 and A to F. The first group of 3 bytes (24 bits) uniquely identifies the manufacturer of the device and is assigned by the IEEE. The last group of three bytes is assigned to the interface by the manufacturer to uniquely identify the interface. This ensures that no two devices have an identical MAC address. The following is an example of a MAC address:

```
02-25-4F-89-AE-48
```

Network protocols, such as the *Address Resolution Protocol (ARP)* of the TCP/IP protocol stack, maintain a table that maps MAC addresses to their corresponding IP addresses. The method of identifying the MAC address of a network interface that is installed in a system varies from one operating system to another. The following list provides a look at the operating system utilities used to obtain the MAC address of an interface:

- Windows XP/NT/2000/2003: `ipconfig /all`
- Windows 95/98/ME: `winipcfg`
- Novell NetWare: `config`
- Unix/Linux: `ifconfig -a`

The OSI Networking Model

The Open System Interconnect (OSI) model defines the seven layers of networking. These layers define the standards for implementing networking functions and protocols. The functions of each layer are described in the following sections.

Physical layer (Layer 1)

The Physical layer of the OSI model defines the network medium, hardware, and topology used in the network; the maximum speed, bandwidth, and cable lengths are also defined in this layer. It also details the electrical characteristics of the media, such as voltage or current. In wireless networks, it defines the frequencies over which the signals travel. The following are two main components of this layer:

Topology
: The physical network topology used may be bus, ring, star, or mesh.

Hardware
: The network hardware includes the network media such as cables and connectors, and their connection details.

Network hubs and repeaters work at the physical layer of the OSI model.

Data Link layer (Layer 2)

The Data Link layer defines the interface between the physical media and the software running on the computer. It is responsible for sending and receiving the data frames to and from the Physical layer. This layer performs functions such as packet addressing, error detection, error correction, and hardware addressing. This layer is further divided into the following two sublayers:

Media Access Control (MAC)
: The MAC sublayer is defined in the IEEE 802.1 standard. It is responsible for controlling access to network media and for moving the data packets from one network interface to another. The IEEE 802.1 standard defines the MAC address (also called the *hardware address*) of the network interfaces. A MAC address is hardcoded onto every network interface.

Logical Link Control (LLC)
: The LLC sublayer is defined in the IEEE 802.2 standard. It is responsible for error detection, error correction, synchronization of data frames, and flow control.

Network interface cards, switches, bridges, and wireless access points work at the Data Link layer of OSI model.

Network layer (Layer 3)

The Network layer is responsible for end-to-end communications between two computers on different networks. One of the primary functions of this layer is *routing*, which enables computers to forward traffic to a remote network. This functionality is provided by network protocols. Network protocols perform *route selection*, which is a process that determines the best path to a destination network.

Unlike the Data Link layer that uses a MAC address to forward packets to a host in a single network, the Network layer uses software-configured, Layer 3 addresses (such as an IP address or an IPX address) to send the packet to its destination network. Other functions of the network layer include *packet sequencing*, *end-to-end error detection*, *congestion control*, and *addressing*.

The IP and the IPX work at the Network layer of the OSI model. Besides this, routing protocols such as RIP, OSPF, and NLSP also work at this layer.

Transport layer (Layer 4)

The Transport layer works with the Network layer to provide guaranteed delivery of data packets in order to acknowledge that data is received at the destination. It performs segmentation of data by breaking it down into manageable packets. End-to-end error detection ensures that the data is received without damage. Flow control ensures that transmission speed is regulated in order to avoid dropped packets.

Both connectionless and connection-oriented protocols work at the Transport layer. UDP is a connectionless protocol, while TCP is a connection-oriented protocol.

Session layer (Layer 5)

The Session layer provides several functions to regulate the communications session between two computers on the network. It is responsible for setting up and terminating a session as well as for controlling the dialog between applications on two computers.

Presentation layer (Layer 6)

The Presentation layer is responsible for translating syntax or format of data so that the receiving computer can understand it. The translating syntax also provides functions such as compression/decompression, encoding/decoding, and encryption/decryption. Some of the common data formats working at this layer include the following:

- Graphic file formats such as JPEG, TIFF, or GIF
- Text and data file formats such as American Standard Code for Information Interchange (ASCII) and Extended Binary Coded Decimal Interchange Code (EBCDIC)
- Sound and Video formats such as MPEG, AVI, QuickTime Video, or MIDI files

Application layer (Layer 7)

The Application layer is responsible for accepting requests from users and applications and passing them on to the lower layers of the OSI model. In other words, it provides an interface between the applications running on the computer and network protocols. Applications (such as file transfers, email, FTP, or Telnet) use the services provided by Application layer protocols, which in turn use the lower-layer protocols to communicate over the network.

Table 8-9 provides a summary of the functions of the different layers of the OSI model.

Table 8-9. Summary of the different layers of OSI networking model

OSI layer	Function
Physical (Layer 1)	Provides specifications for the physical topology of the network
Data Link (Layer 2)	Handles functions such as the media access method, hardware addressing, and error detection and correction. Consists of MAC and LLC sublayers
Network (Layer 3)	Provides routing functions and discovery of the best network path to the destination network
Transport (Layer 4)	Provides guaranteed delivery, segmentation of data, flow control, and error detection and correction
Session (Layer 5)	Manages dialog (sessions) between applications running on remote computers; it sets up, regulates, and terminates the sessions
Presentation (Layer 6)	Provides data format translation of data formats such as encryption/decryption, encoding/decoding, and compression/decompression
Application (Layer 7)	Provides interface to applications to access the network services

Table 8-10 provides a list of commonly used network devices and the OSI model layers they work at.

Table 8-10. Mapping OSI model layers to network devices

OSI model layer	Network device
Physical (Layer 1)	Hubs, repeaters, cables, and connectors
Data Link (Layer 2)	NICs, switches, bridges, and WAPs
Network (Layer 3)	Routers

Network Protocols

Networking protocols provide the ability for computers to communicate to each other through the networking media. In this section, we will discuss the features of different networking protocols, their advantages, and their limitations.

NetBEUI

NetBEUI stands for *NetBIOS Extended User Interface*. It is an old Microsoft networking protocol used in small networks. This protocol provides services at the Transport and Network layer of the OSI model. It is not a routable protocol and cannot be used on large routed networks. It is easy to install and is the fastest of all protocols covered in the Network+ exam.

Computers using the NetBEUI protocol use NetBIOS naming conventions. NetBIOS computer names consist of a maximum of 15 characters, such a Server1 or Workstation1. NetBEUI uses the following three methods to resolve NetBIOS computer names to IP addresses:

IP Broadcasting
: If a host does not have the IP address of a NetBIOS host in its cache, it broadcasts the NetBIOS name to the entire network.

LMHOSTS File
: This is a text file that maps IP addresses to NetBIOS computer names.

NBNS
: This is a NetBIOS Name Server that maps NetBIOS names to IP addresses.

Since NetBIOS name resolution mainly depends on broadcasts, the NetBEUI protocol creates significant network traffic if there are a large number of computers on the network. This protocol is used only on nonrouted Microsoft networks. Due to its severe limitations, it is rarely used even in Microsoft networks these days.

Internet Packet Exchange/Sequenced Packet Exchange (IPX/SPX)

IPX/SPX is a full protocol suite used in Novell NetWare networks. It is a fully routable protocol. Different protocols in this suite are as follows:

Service Advertising Protocol (SAP)
: This protocol works at the application, presentation, and session layers, and it allows systems to advertise their services (such as file and print services).

NetWare Core Protocol (NCP)
: This protocol works at the application, presentation, and session layers, and it allows client/server interactions (such as file and print sharing). NCP is a connection-oriented protocol.

Internet Packet Exchange (IPX)
: This protocol works at the transport and network layers, and it provides network addressing and routing services. It is a connection-less protocol and provides fast and reliable communication between computers.

Sequenced Packet Exchange (SPX)
: This protocol works at the Transport layer to provide connection-oriented services on top of the IPX protocol.

Routing Information Protocol (RIP)
: This protocol works at the Network layer and is the default routing protocol for IPX/SPX networks. It uses the distance vector routing algorithm for calculating routes and building routing tables.

NetWare Link State Protocol (NLSP)
: This protocol works at the Network layer to provide routing services based on a link state algorithm for calculating routes and building routing tables.

Open Datalink Interface (ODI)
: This protocol works at the Data Link layer to allow NetWare systems to work with any network interface card.

NetWare hostnames. In a NetWare network environment, only the servers are required to be assigned hostnames. These names consist of a maximum of 47 characters. The NetWare clients do not have hostnames. They use their IPX addresses instead.

IPX addresses. Logical NetWare networks are assigned 32-bit hexadecimal addresses. The servers and workstations use a 48-bit hexadecimal address that defaults to the MAC address of the network interface card. The node address is appended to the network address to create a unique node address in the internetwork. The following is an example of an IPX address:

```
0AC74E02:02254F89AE48
```

Note that the first part of the IPX address is the address of the logical network, and the second part is the unique MAC address of the network interface card. The colons from the MAC address are removed. Also, if there are any leading zeros, they are not written. Sometimes the IPX address is written as groups of four hexadecimal numbers separated by colons. The above address can thus be written as:

```
AC7:4E02:0225:4F89:AE48
```

NetWare frame types. When discussing the IPX/SPX protocol suite, it is important to include the frame types used in NetWare networks. If there is some connectivity problem between two systems using different versions, it is a good idea to check the frame types used on the network. NetWare uses the following types of frames for encapsulating data at the Data Link layer:

- NetWare 2.x and NetWare 3.x use IEEE 802.3 as the default frame type.
- NetWare 4.x uses IEEE 8.2.2 as the default frame type.

IPX/SPX interoperability and routing. The IPX/SPX protocol suite is fully routable and interoperates with many other protocols. Most notably, Microsoft operating systems include the NWLink IPX/SPX Compatible Protocol and the Microsoft Client for NetWare Networks for interoperability with Novell networks. Due to the increasing popularity and extended features of the TCP/IP protocol suite, the usage of IPX/SPX has declined significantly. Both Microsoft and Novell have made TCP/IP their default protocol.

AppleTalk

The AppleTalk protocol suite is used to interconnect Apple computers. Like IPX/SPX and TCP/IP, this protocol is also fully routable. The AppleTalk protocol suite consists of the following different protocols:

AppleShare
: This protocol works at the Application layer and provides file- and printer-sharing services.

AppleTalk Filing Protocol (AFP)
: This protocol works at the Presentation layer and is used to manage file sharing between AppleTalk hosts. It is also called Apple Filing Protocol.

AppleTalk Data Stream Protocol (ADSP)
This protocol works at the Application and Presentation layers, and provides services for establishing communication between AppleTalk hosts.

Zone Information Protocol (ZIP)
This protocol works at the Session layer to divide an AppleTalk network into zones.

AppleTalk Session Protocol (ASP)
This protocol works at the Session layer to establish and terminate connections between hosts.

Printer Access Protocol (PAP)
This protocol works at the Session layer to provide printing services on an AppleTalk network.

AppleTalk Address Resolution Protocol (ARP)
This protocol works at the Network layer to resolve AppleTalk addresses to Ethernet or Token Ring addresses.

Datagram Delivery Protocol (DDP)
This protocol works at the Network layer to handle routing functions and delivery of datagrams.

AppleTalk Transaction Protocol (ATP)
This protocol works at the Transport layer to provide a connectionless session between hosts.

Name Binding Protocol (NBP)
This protocol also works at the Transport layer to map AppleTalk hostnames to network layer addresses.

Routing Table Maintenance Protocol (RTMP)
This protocol works at the Transport layer to maintain routing tables.

EtherTalk Link Access Protocol (ELAP)
This protocol works at the Data Link layer and provides compatibility with Ethernet protocol.

TokenTalk Link Access protocol (TLAP)
This protocol works at the Data Link layer and provides compatibility with Token Ring protocol.

AppleTalk addressing and naming. An AppleTalk host address consists of a 24-bit long number with 16 bits assigned to the network and 8 bits assigned to the host. This address is expressed in a decimal format. An administrator assigns the network address while the host address is automatically generated by the system when it is first started. It is a randomly generated number and is broadcast to the entire AppleTalk network as soon as it is generated. An example of an AppleTalk address is 5.48, where 5 is the network address and 48 is the host address. AppleTalk hostnames are resolved using the Name Binding Protocol (NBP), which is similar to the Domain Name System (DNS) used on TCP/IP networks.

AppleTalk interoperability and routing. AppleTalk is a fully routable protocol but cannot be used on the Internet. The Routing Table Maintenance protocol provides a functionality that is similar to the RIP used on TCP/IP networks. Unix/Linux and Microsoft operating systems have limited support for AppleTalk networks. As with the IPX/SPX protocol suite, the AppleTalk protocol is also losing ground due to the increasing popularity of the TCP/IP protocol.

Transmission Control Protocol/Internet Protocol (TCP/IP)

The TCP/IP is a set of several protocols. It is the most widely used protocol suite in private networks as well as on the Internet. Unlike the AppleTalk and IPX/SPX protocols, TCP/IP is not proprietary to any organization, but is a public protocol suite. Some of the well-known protocols and their functions are discussed later in this section.

TCP/IP addressing. Hosts in a TCP/IP network follow IP addressing schemes. IPv4 is the current and most commonly used version of IP address. The IP address consists of 32 bits and is expressed as decimal numbers separated by a period. This is called the *dotted decimal notation*. An IP address is composed of four sets of eight bytes (*octet*) each. 192.168.2.10 is an example of an IP address.

Since a TCP/IP network can be composed of several segments, it becomes necessary to identify the network segment in which a particular host is located. For this purpose, a second 32-bit number is associated with an IP address. This number is used to identify the network address from the host address, and is called the *subnet mask*. When converted to a binary number, the network part is assigned a binary value of 1 and the host part is assigned a value of 0 in the subnet mask. For example, if the subnet mask is 255.255.0.0, the first 16 bits of the IP address would represent the network address, and the last 16 bits would represent the host address.

IP addresses are divided into classes A, B, C, D, and E. Out of these, classes A, B, and C are available for assignment to private organizations. IP addresses can further be divided into public (registered) or private (unregistered) addresses. Organizations using public addresses can be connected to the Internet, while the private IP addresses can only be used internally. TCP/IP addressing is covered in greater detail later in this chapter in the section "IP Addressing."

TCP/IP naming. TCP/IP hosts can be identified either by their IP addresses or by their hostnames. A DNS server performs the translation of IP addresses to computer names. In smaller networks, a text file named *hosts* can also be created on every computer to provide name resolution.

TCP/IP routing. Needless to say, TCP/IP is a fully routable protocol. The routing functionality is provided by a number of routing protocols, such as RIP and OSPF.

TCP/IP interoperability. The TCP/IP protocol suite is supported by all major network and desktop operating systems. Apart from Unix/Linux operating systems, Microsoft, Apple, and NetWare have also made TCP/IP their default protocols. As of now, TCP/IP is the most versatile and feature-rich protocol suite available in all operating system environments.

IP Addressing

An IP address is a unique address used to identify a computer or a host on the network. This address is made up of 32-bit numbers written in dotted decimal notation in the *w.x.y.z* format. Each eight bits are known as an *octet* or a *byte*. A part of the IP address is known as the *network address*, or *network ID*, and the rest of it is known as the *host address*, or *host ID*. These parts are based on the class of IP addresses used on the network. All computers on a particular network must have the same number as the network address, while the host address must be unique on the entire network. A second address, the subnet mask, is used to help identify the part of the network where the host is located.

IP addresses are assigned and controlled by an organization called Internet Assigned Numbers Authority (IANA). There are two current versions of IP addressing: IPv4 and IPv6.

IPv4 addresses

IPv4 addresses are classified into classes A, B, C, D, and E. Only addresses from the classes A, B, and C are assigned to organizations and are known as *classful IP addresses*. The first byte of an IP address identifies the class of IP addresses used in the network. For example, a host with an IP address of 92.137.0.10 is using a class A IP address. A host with an IP address of 192.170.200.10 is using a class C IP address. The IP addresses in the A, B, and C classes are available for public companies and can be assigned by an ISP. The class D and E addresses are reserved for special usage.

Subnet mask. Every IP address is accompanied by a subnet mask, which is used to help identify the part of the network where the host is located. Like the IP address, the subnet mask is a 32-bit binary number that distinguishes the network ID from the host ID. Its digits are set to 1 and 0, where 1 represents the network portion of the address and 0 represents the host portion. Table 8-11 summarizes the main classes of IP addresses, the number of networks and hosts in each class and the default subnet masks.

Table 8-11. IP address classes

Class	Range of first byte	Number of networks	Hosts per network	Default subnet mask
A	1–126	126	16,777,214	255.0.0.0
B	128–191	16,384	65,534	255.255.0.0
C	192–223	2,097,150	254	255.255.255.0
D	224–239	N/A	N/A	N/A
E	240–255	N/A	N/A	N/A

Notice in Table 8-11 that the network ID 127 is not included in any of the classes. Actually, the IP address 127.0.0.1 is reserved as a *loopback* address for troubleshooting TCP/IP configuration of the computer.

Apart from the IP addresses, the hosts on a network also have a general alphanumeric hostname or a Fully Qualified Domain Name (FQDN) in the format *server1.mycompany.com*. Each hostname corresponds to an IP address, and the DNS is used to translate the IP address of a host to its domain name.

When configuring the IP address of a computer or some other network device, you will need to specify the IP address, the subnet mask, and the default gateway address. The IP address must be unique in the network, while the subnet mask must be same on all computers in a particular network segment.

Default gateway. A default gateway allows computers on a network segment to communicate with computers on another segment. The default gateway for all computers on a particular segment is the IP address of the router interface that is connected to the local segment. If a computer is not configured with the IP address of a default gateway, it cannot communicate with computers on a different network segment.

Public and private IP addresses

Public IP addresses (or *registered IP addresses*) are those addresses of those networks that are accessible from outside the organization. For example, if any host is connected to a network, it is using a public IP address. If an organization needs to connect its network to the Internet, it will need to obtain a public IP address from its Internet Service Provider. Typically, web servers, email servers, DNS servers, FTP servers, and VPN servers are connected directly to the Internet and use public IP addresses.

Private IP addresses (or *unregistered IP addresses*), on the other hand, are used when an organization's computer network is private. In other words, it is not connected to the Internet or if it is, it is located behind a proxy server or a firewall. Access to private networks is usually restricted to users inside the organization. The Internet Assigned Numbers Authority (IANA) has set aside a range of IP addresses in each of A, B, and C address classes that can be used by private organizations for their internal IP addressing. These addresses are listed in Table 8-12.

Table 8-12. Private IP address ranges

Class	Start address	End address	Subnet mask
A	10.0.0.0	10.255.255.255	255.0.0.0
B	172.16.0.0	172.31.255.255	255.240.0.0
C	192.168.0.0	192.255.255	255.255.0.0

Subnetting

Subnetting is the process of creating two or more network segments by using the host portion of the IP address. Subnetting creates multiple broadcast domains that help reduce undesired broadcast traffic. Subnetting allows administrators to more effectively manage the IP address range. It also increases security of the network and helps contain network traffic to local network segments.

With a default subnet mask, you can have only one network segment. With subnetting, the number of segments increases, while the number of hosts in each segment reduces. For example, consider a network with an IP address of 192.168. 2.0. With the default subnet mask of 255.255.255.0, you can have only one large network segment with 254 hosts. If you use some bits from the host portion, you can create two, three, or four segments. But as the number of segments increases, the number of hosts in each segment reduces.

IPv6 addresses

The most significant advantage of IPv6 over IPv4 is the increase in the number of network addresses available for network devices. This is an important consideration because most of the IPv4 addresses have already been allocated, and the availability is continuously decreasing. IPv6 uses a 128-bit address as opposed to the 32-bit address used in IPv4.

An IPv6 address is composed of two logical parts: a 64-bit network prefix and a 64-bit host address. The host address can either be dynamically generated from the MAC address of the host interface or can be sequentially assigned.

The IPv6 address is written as eight groups of four hexadecimal digits separated by colons. The following is an example of an IPv6 address:

```
2001:0db8:85a3:08d3:1319:8a2e:0370:7334
```

If any of the four-digit group is composed of all zeros, it can be omitted. Consider another example:

```
2001:0db8:0000:08d3:1319:8a2e:0000:7334
```

This address can be written as follows:

```
2001:0db8::08d3:1319:8a2e::7334
```

Address assignment

In every network based on the TCP/IP protocol, whether it is small or large, there has to be some means of assigning IP addresses to the computers. At the minimum, the TCP/IP address configuration requires assignment of an IP address and a subnet mask. If it is a routed network (a network with multiple segments), the address of the default gateway must also be configured. IP address assignment can be done manually (static addressing) or automatically (dynamic addressing), as discussed in the following paragraphs:

Static

In the static IP address assignment method, an administrator manually configures the IP addresses on every computer. This method is prone to typing errors and cannot be used in large networks. In case the organization changes the IP addressing scheme, each computer must again be manually configured, which makes it a tedious task for the administrator. Moreover, an administrator may assign duplicate addresses, leaving a system unable to communicate on the network.

Dynamic

Dynamic IP addressing refers to automatic assignment of TCP/IP configuration by using a centralized server known as a *Dynamic Host Configuration Protocol (DHCP)* server. The DHCP server is configured with IP address scopes for each network segment. This not only saves the administrator from manually entering IP addresses, but it also prevents typing errors and duplicate addresses. If there is a change in the IP addressing scheme, the administrator has only to make changes on the DHCP server.

The DHCP server maintains a list of available IP addresses in a scope. When a client is assigned an IP address from a scope, the DHCP server can also provide the subnet mask and default gateway address. Optionally, the addresses of DNS and WINS servers can also be assigned to the client (WINS is discussed later in this section). IP addresses are assigned for a specific period of time known as a *lease*. Clients must renew their IP addresses with the DHCP server when 50 percent of the lease period expires.

If a DHCP server is configured to assign IP addresses to clients located across routers, the routers must either be RFC 1542-compliant or configured to forward BOOTP broadcasts.

Automatic Private IP Addressing (APIPA)

The default configuration on most operating systems is to dynamically obtain an IP address configuration from a DHCP server. When the DHCP server is not available for some reason, the computer can assign itself an IP address automatically. This feature is enabled by default on all Windows XP computers. The automatically assigned address is from the range 169.254.0.1 to 169.254.255.254 with a subnet mask of 255.255.0.0.

With an APIPA address, the computer can connect only to the other computers with APIPA addresses on the local network segment, but cannot access any other computers or a remote network. A computer assigned with APIPA keeps on trying to locate a DHCP server every five minutes in order to obtain a genuine IP address. If a computer is configured to obtain an IP address from a DHCP server but does not support APIPA, its IP address defaults to 0.0.0.0.

TCP/IP protocols

As noted earlier, the TCP/IP protocol suite is a set of a number of protocols and services, each with a specific function working at one or more layers of the networking model. Some of the commonly used protocols and their functions are listed here:

Internet Protocol (IP)

IP is a connection-less protocol that works at the network layer to provide IP addressing and routing functions.

Transmission Control Protocol (TCP)

TCP is a connection-oriented protocol that works at the transport layer to provide guaranteed delivery, flow control, error detection, error correction, and packet sequencing.

User Datagram Protocol (UDP)

UDP is a connection-less protocol that works at the transport layer but does not provide guaranteed delivery of data. It does not perform any error checking or correction and hence is faster and consumes less network bandwidth than TCP.

File Transfer Protocol (FTP)

FTP works at the Application layer to provide file transfers between remote computers. FTP uses TCP as its transport protocol and is a client/server application that authenticates users before allowing access to servers that host the FTP service. Most FTP servers allow anonymous logon that enables multiple users to connect to the server and download files. FTP is commonly used on the Internet for file downloads. One of the major limitations of the this protocol is security. The authentication method uses clear-text usernames and passwords, which is a serious security concern. FTP uses several commands for file transfers, as described in Table 8-13.

Table 8-13. Commonly used FTP commands

FTP command	Description
ascii	Allows file transfers in ASCII mode
binary	Allows file transfers in binary mode
cd	Used to change the working directory on the remote computer
get	Used to download a single file from the remote computer
ls	Used to list files in on the remote computer
mget	Used to download multiple files from the remote computer
mput	Used to upload multiple files on the remote computer
put	Used to upload a single file on the remote computer

Secure File Transfer Protocol (SFTP)

SFTP is the secure version of FTP protocol. It is used to transfer data in an encrypted format between the client and the server. Secure Shell (SSH) is used to provide secure authentication between the two computers.

Trivial File Transfer Protocol (TFTP)

TFTP is an Application-layer protocol used to transfer files between two remote computers. It is limited in functionality compared to FTP. It uses UDP as its transport protocol and is hence less reliable, but faster than, FTP.

Simple Mail Transfer Protocol (SMTP)

SMTP is a connection-oriented Application-layer protocol that is used to transport messages between remote email servers. It uses TCP at the transport layer and hence guarantees delivery of data.

HyperText Transfer Protocol (HTTP)

HTTP is an Application-layer protocol that allows text, images, and multimedia to be downloaded from web sites. It is also a connection-oriented protocol that uses TCP at the transport layer. HTTP works with a Uniform Resource Locator (URL) to connect to the desired web site. An example of a URL is *http://www.oreilly.com*.

HTTP Secure (HTTPS)

HTTPS is the secure version of the HTTP protocol that allows servers and clients to be authenticated before the communication session starts. This protocol is also an Application layer protocol and uses TCP at the Transport layer. It is commonly used for online banking and other e-commerce functions. It uses the secure socket layer (SSL) to encrypt the network traffic between the web server and the web client. A web site using SSL has a URL starting with *https://*.

Post Office Protocol 3 (POP3)

POP3 is used to download or retrieve email messages from mail servers running the SMTP protocol. One of the limitations of the POP3 protocol is that it uses clear-text usernames and passwords, which is a serious security concern.

Internet Message Access Protocol 4 (IMAP4)

Like POP3, IMAP4 is also used to retrieve email from mail servers. The advantage of using IMAP4 over POP3 is that it provides a secure authentication mechanism.

Telnet

Telnet is an Application-layer protocol that allows connections to remote hosts. Administrators use this protocol to connect remotely to network devices and run commands in order to configure or maintain them. This is also a connection-oriented protocol and uses TCP at the Transport layer.

Secure Shell (SSH)

SSH is the secure alternative to connecting to remote systems or devices instead of using Telnet. It provides strong authentication mechanisms and encryption of information between two remote hosts.

Internet Control Message Protocol (ICMP)

ICMP works at the Network layer to provide error checking and reporting functions. It is a connection-less protocol and uses IP for providing best-effort delivery. It is used in network management and maintenance systems. For example, *ping* is a troubleshooting utility that uses the ICMP protocol.

Address Resolution Protocol (ARP)

ARP works at the Network layer and is used to resolve IP addresses to MAC addresses. Upper-layer protocols use ARP to correctly deliver data packets to the destination host. ARP maintains a mapping (called the *ARP cache*) of IP addresses and MAC addresses in the system memory. If the ARP cache does not have an entry for a requested IP address, it broadcasts the IP address on the local network to find out which host has the specified IP address.

Reverse Address Resolution Protocol (RARP)

The function of RARP is opposite to that of the ARP. It is used to obtain the IP address of a host whose MAC address is known.

Network Time Protocol (NTP)

NTP is used to exchange time information between TCP/IP hosts. One of the systems is usually configured as a time provider, which uses NTP to transmit time information to other hosts.

Network News Transfer Protocol (NNTP)

NNTP works at the application layer to provide newsgroup services such as posting and retrieving messages on discussion forums. It uses TCP at the Transport layer.

Secure Copy Protocol (SCP)

SCP works at the Application layer to enable secure copying of files from Unix/Linux systems. It uses SSH technology for a secure information exchange between two systems. It is a safe alternative to the Remote Copy Protocol (RCP).

Lightweight Directory Access Protocol (LDAP)

LDAP is an Application-layer protocol that enables users to access and query directory services such as Microsoft's Active Directory, Novell's eDirectory, and Novell Directory Services (NDS). LDAP functions can be performed from the command line or from graphic user interfaces (GUIs).

Internet Group Management Protocol (IGMP)

IGMP works at the network layer of the OSI model and is used to register and discover network devices in a multicasting group. IGMP enables devices to exchange messages within the members (network devices) of a multicasting group.

Line Printer Remote (LPR)

LPR works at the application layer to provide client connectivity to printers in all major network operating systems, such as Unix/Linux and Windows. *Line Printer Daemon (LPD)* is a server component that accepts client print requests sent using the LPR application.

Table 8-14 provides a list of the different protocols in the TCP/IP suite discussed in this section, and the OSI model layers associated with them.

Table 8-14. OSI model layers and TCP/IP protocols

OSI model layer	Protocols
Application (7)	HTTP, HTTPS, SNMP, SMTP, FTP, TFTP, SFTP, SCP, Telnet, SSH, NTP, NNTP, POP3, IMAP4, LDAP, and LPR
Presentation (6)	SSL and TLS (not covered in this section)
Transport (4)	TCP and UDP
Network (3)	IP, ARP, RARP, ICMP and IGMP

Port assignments in TCP/IP

Every application, service, or protocol in the TCP/IP suite has a specific port number assigned to it. A *port* is like a socket that the application uses to send or receive data packets. When a computer receives a data packet, it checks the associated port number to determine which application will receive the data. For example, the FTP service uses port numbers 20 and 21. TCP/IP port numbers fall in following three categories:

- Well-known port numbers range from 0 to 1,023.

- User ports (registered ports) range from 1,024 to 46,151.
- Dynamic/private ports range from 46,152 to 65,535.

For the Network+ exam, you will need to know the port numbers used by various network protocols and services. Table 8-15 lists some of the well-known ports.

Table 8-15. Well-known TCP/IP port numbers

Port number	Application/Service/Protocol
20	File Transfer Protocol (FTP) –(data port)
21	File Transfer Protocol (FTP) (control port)
22	Secure Shell (SSH)
23	Telnet
25	Simple Mail Transfer Protocol (SMTP)
53	Domain Name System (DNS)
58	Dynamic Host Configuration Protocol (DHCP)
67 and 68	Bootstrap Protocol (BOOTP); also used by Dynamic Host Configuration Protocol (DHCP)
69	TFTP
80	HyperText Transfer Protocol (HTTP)
110	Post Office Protocol version 3 (POP3)
119	Net News Transfer Protocol (NNTP)
137, 138, and 139	NetBIOS Name Service (Windows operating systems)
143	Internet Message Access Protocol version 4 (IMAP4)
161, and 162	Simple Network Management Protocol (SNMP)
389	Lightweight Directory Access Protocol (LDAP)
443	Secure Socket Layer (SSL) or HTTPS

The port numbers listed in Table 8-15 are frequently tested on the Network+ exam. Make sure that you review these port numbers before you write the exam.

Network services

Network services enable administrators to effectively manage and administer the network environment. These services are essential components of any small or large network and help centralize and control common functions of everyday network administration. Some of the services covered in the Network+ exam are discussed in the following sections.

Domain Name Service (DNS). The DNS service is used in a TCP/IP network to resolve hostnames to their corresponding IP addresses. This enables a common user to use easy-to-remember hostnames such as *computer1.oreilly.com*, instead of using hard-to-remember IP addresses such as 192.168.8.245. The DNS service is platform-independent and is used on all major operating systems. A DNS server maintains a database of hostnames and their IP addresses. When a network client needs to communicate to another client in the network using its hostname, a DNS query is sent to the DNS server that resolves the hostname to its IP address.

Hostnames on the Internet or large-scale networks are also known as Fully Qualified Domain Names (FQDN). For example, if a server is named *mail1* and resides in the *oreilly.com* domain, it is referred to as *mail1.oreilly.com*.

In very small networks where it is not possible to implement a DNS server, name resolution can be performed by using the *HOSTS* file. The *HOSTS* file is a text file that the administrator must create on every computer in the network. It contains mappings of hostnames to IP addresses. If there is a change in IP addressing, the administrator has to make changes to the *HOSTS* file on every computer. This method is error-prone and is rarely used these days.

Windows Internet Name Service (WINS). The WINS service is used exclusively in Microsoft networks where the DNS service has not been implemented or is not required. This service is used to resolve NetBIOS names to their IP addresses The main purpose of using the WINS service is to prevent broadcast traffic due to name resolution requests. A WINS server maintains a database of NetBIOS names and IP addresses. Network clients send queries to the WINS server for name resolution. As with the DNS service, the WINS service allows users to use easy-to-remember computer names in the network.

Another method to resolve NetBIOS names in a Windows network is to use the *LMHOSTS* file. This is a text file that contains NetBIOS names to IP address mappings. The *LMHOSTS* file can either be stored locally on a computer or on a central file server. This file also must be created and maintained manually by a network administrator.

Network Address Translation (NAT). NAT is the process of hiding all internal IP addresses from the outside network by using a single public IP address. The most common use of NAT is to enable computers on an internal network to share a single Internet connection. Another utilization of the NAT service is to effectively use the IPv4 address space, which is depleting day by day. An organization can obtain just one public IP address for its main router connected to the Internet. All internal computers can then be assigned IP addresses from the private IP address range. The computer with the public (registered) IP address acts as a gateway for the internal computers.

Some of the main advantages of NAT are as follows:

- It is a cost-effective way to share a single Internet connection among several clients on a private network.
- It provides security for the private network by hiding the internal IP addressing scheme from external networks.
- It is more scalable than Internet Connection Sharing (ICS), as more than one public IP address can be used in a NAT implementation.
- It allows use of DNS and DHCP servers inside the network.
- It makes it possible to host web and email services from a private network.

Internet Connection Sharing (ICS). ICS is a scaled-down version of NAT. As the name suggests, ICS is used in small networks for sharing a single network connection. The main difference between NAT and ICS is that ICS can only be used in very small networks that do not have any segments. Another limitation of ICS is that the internal clients are always configured with class C IP addresses in the 192.168.0.1 range. ICS does not provide any security for the internal network. Due to all these limitations, ICS is used only in very small networks.

Simple Network Management Protocol (SNMP). SNMP is used in TCP/IP-based networks to monitor and manage network devices. Network devices send information to a centralized server known as the *SNMP Manager* that maintains a database known as *Management Information Base (MIB)*. SNMP-enabled devices run a management application called the *SNMP agent*. The SNMP agent sends messages known as *SNMP traps* to the SNMP server. SNMP actively monitors the entire network and can take appropriate administrative actions when certain events occur.

Network File System (NFS). NFS is mainly associated with Unix/Linux network environments for accessing and retrieving files from a remote computer. This service is also supported in MAC and Windows operating systems. NFS is the default filesystem used in Unix/Linux networks.

Zero Configuration (ZeroConf). ZeroConf is a mechanism that enables computers or other network devices to communicate to each other without requiring any special configuration. Without ZeroConf, devices must be configured either manually or by some network server in order to start communicating on a network. A ZeroConf device must meet the following conditions:

- It must support Automatic Private IP Addressing (APIPA).
- It must be capable of resolving hostnames.
- It must be able to advertise its services on the network.
- It must be able to discover services in the network.

With a number of wireless and small devices appearing in the market everyday, ZeroConf has gained popularity, because it does not require any user intervention to configure it.

Server Message Block (SMB). SMB is an Application-layer protocol used for file and printer sharing in a network. Another name for this is *Common Internet File System (CIFS)*. It is the default file and printer access method used in Microsoft Windows networks. It also provides authentication for application processes. Microsoft has made many improvements in SMB in its Windows 2000 and later operating systems.

Apple File Protocol (AFP). AFP is mainly used on Macintosh computers for accessing file shares. It is also known as *AppleTalk Filing Protocol*. This protocol is an equivalent of NFS in Unix/Linux and of SMB/CISF in Windows networks. It is the default method of file access on Apple Macintosh networks.

Line Printer Daemon (LPD). The LPD service provides network printing and spooling functions for Unix/Linux systems. Printer spooling is a mechanism that holds print jobs on the server hard disk until they are sent to the physical printer. LPD also enables administrators to use a set of commands to control print jobs in the print queue. A printer that supports LPD/LPR protocol is also known as a TCP/IP printer.

Samba. Samba is the Unix/Linux equivalent of the SMB service used in Microsoft networks. It enables Windows users to access shared files and printers on Unix/Linux servers as if they were located on a Windows server.

WAN Technologies

A WAN connects LANs at different locations. A number of different technologies can be used to implement a WAN. The choice of a particular technology depends mainly on the speed and bandwidth requirements as well as on budget limitations. WANs can be built using packet-switched or circuit-switched networks. The connection can be as simple as a dial-up, or as expensive and complicated as a dedicated T1 line. This section explains some of the WAN technologies covered in the Network+ exam.

Packet switching

In packet switching, the data is split into small segments known as *packets*. Each packet has a label that contains information such as its source address and destination address. The packets are routed individually on different intermediate nodes. The Internet is the best example of a packet-switched network. Data from the source computer to the destination computer is routed in individual packets that take different routes. Each packet is sent using the best and shortest route.

Packet-switched networks use a routing algorithm to send the individual packets to their destination. Often a route with the shortest path (lowest cost) is selected for a packet. It is very possible that the next packet travels by a different route. The individual packets arrive at the destination in a random order. The destination node waits for all the packets to arrive, checks their sequence numbers, and then reconstructs the information.

Circuit switching

In circuit-switched networks, a dedicated physical circuit is established before the two nodes can communicate. Each circuit or communication channel is reserved and cannot be used by other nodes until the nodes already using the channel release it. The Plain Old Telephone System (POTS) is an example of a circuit-switched network. An ISDN is another example where a separate channel is used for control and administrative purposes.

The advantages of circuit switching include reliable connection and guaranteed speed of data transmission. The disadvantage is that resources are wasted due to dedicated physical connections. Circuit switching is different from packet switching in which data is split into packets and sent over a shared network. Packet switching allows several nodes to communicate simultaneously over the same network.

Integrated Services Digital Network (ISDN)

ISDN is a packet-switched network that is designed to allow transmission of data and voice over the same copper wires used in telephone systems. This results in better quality and higher data transfer speeds than regular dial-up connections. ISDN is actually a set of protocols that define rules for establishing and terminating connections. It also provides several advanced features. At the same time, ISDN requires dedicated telephone lines and therefore is expensive.

As with a regular dial-up connection, an ISDN connection also uses a dial-up telephone number—but these telephone lines are considered *leased lines*. When the two ends need to communicate, one of them dials the specified ISDN number, and the connection is set up. When the communication between the two nodes is over, the user hangs up and the ISDN line becomes free. Computers using the ISDN line need the special network interface known as the ISDN adapter (or the terminal adapter).

ISDN communications use two types of channels: a *bearer channel (B channel)* that is used for data (or voice), and a *delta channel (D channel)* that is used for control signals. There are two main implementations of ISDN as follows:

Basic Rate Interface (BRI)
BRI ISDN uses 2 B channels of 64 Kbps each for data/voice, and a D channel of 16 Kbps. The total data transfer speed of BRI ISDN using two B channels is 128 Kbps. The two B channels can also be used separately with 64 Kbps speed.

Primary Rate Interface (PRI)
PRI ISDN uses 23 B channels of 64 Kbps each for data/voice, and a D channel of 64 Kbps. The total data transfer speed of PRI ISDN is up to 1.544 Mbps. The PRI ISDN is usually carried over dedicated (leased) T1 lines.

Table 8-16 summarizes the two ISDN implementations.

Table 8-16. BRI and PRI ISDN connections

Characteristic	BRI	PRI
Carrier line	ISDN	T1
Channels	2B+1D	23B+1D
Total speed	128 Kbps	1.544 Mbps

Fiber Distributed Data Interface (FDDI)

FDDI provides data transmissions in local area networks that can extend up to 200 kilometers (124 miles). It is primarily based on the Token Ring protocol and uses the token-passing media access method. Unlike Token Ring topology, FDDI uses two rings for providing fault tolerance. The nodes in an FDDI network are attached to two rings, and the two tokens rotate on the rings, each in the opposite direction. The first ring is used for carrying data while the second ring is used for fault tolerance.

FDDI can support thousands of network nodes spread over wide geographical locations. Due to the increasing popularity of Gigabit Ethernet, FDDI is rarely used in modern networks. The following are some of the main characteristics of FDDI:

- It is resistant to electromagnetic and radio frequency interferences (EMI and RFI).
- It provides fault tolerance because of two rings.
- Fiber optic cables can have a maximum distance of 200 kilometers.
- It has a built-in error-detection mechanism known as *beaconing*.
- It is very expensive in terms of the cost associated with devices and media.
- It is difficult to implement and maintain.

> It is also possible to use UTP/STP copper cables in the same configurations as the FDDI. In this case, the topology becomes the *Copper Distributed Data Interface (CDDI)*.

T-Carrier

The T-carrier lines are high-speed, dedicated digital lines that can carry both data and voice signals. These lines can be leased from the local telephone company. The basic unit of T-carrier lines is the DS0, which has a transmission speed of 64 Kbps and is used for one voice circuit. Although dedicated T lines are expensive, they provide a consistent point-to-pint connection between two end systems.

The European equivalent of T-carrier is the *E-carrier*, while in Japan the *J-carrier* is used. The most common of all T-carriers are T1 and T3 lines, with data transmission speeds of 1.544 Mbps and 44.736 Mbps respectively. Table 8-17 lists various T, E, and J carriers.

Table 8-17. T, E, and J carriers and their transmission speeds

Carrier	Transmission speed
T1	1.544 Mbps
T2	6.312 Mbps
T3	44.736 Mbps
E0	64 Kbps
E1	2.048 Mbps
E2	8.448 Mbps
E3	34.368 Mbps
J0	64 Kbps
J1	1.544 Mbps
J2	6.312 Mbps
J3	32.064 Mbps

Optical Carrier (OC)

OC levels describe the range of digital signals (data, voice, and video) that can be carried over SONET. SONET is a fiber optic network developed by Bell Communications. The minimum speed of an optical carrier is 51.84 Mbps, and it can go up to 2.488 Gbps. Different OC levels are listed in Table 8-18.

Table 8-18. OC levels and transmission speeds

OC level	Transmission speed
OC-1	51.84 Mbps
OC-3	155.52 Mbps
OC-12	622.08 Mbps
OC-24	1.244 Gbps
OC-48	2.448 Gbps
OC-192	9.953 Gbps

Note that the OC levels are expressed as *OC-n*, where *n* is a number. The speed of any given OC level is calculated by multiplying the level number *n* by 51.8 Mbps. For example, the speed of OC-3 is calculated as 3X51.84 Mbps, which is equal to 155.52 Mbps.

X.25

X.25 is a packet-switching WAN technology that uses telephone or ISDN hardware. It works at a maximum data transfer speed of 56 Kbps. It is a globally accepted standard, but is slowly becoming obsolete due to newer and more efficient technologies. Since it is a packet-switching technique, the X.25 network works well when there is congestion on any part. It can route different packets on different routes. The packets are assembled at the destination using special devices known as *Packet Assemblers/Disassemblers (PADs)*. Each end of the X.25 connection is attached to a PAD.

Internet Access Technologies

Internet access has become a necessity these days. There is hardly any business that does not have it. In its early days, the Internet was available only through dial-up connections or leased lines. With the advancement of technologies, several new techniques have evolved to access the Internet, including DSL, wireless, satellite, and broadband. This section discusses some of the commonly used Internet access methods.

Digital Subscriber Line (DSL)

DSL is a family of technologies that use ordinary analog telephone lines to provide digital data transmissions. It uses different frequencies for voice and data signals, and the same telephone line can simultaneously be used for phone and data transfer. It is commonly used for high-speed Internet access from homes and offices. Different DSL technologies are collectively noted as *xDSL* and support data transfer speeds from 128 Kbps to 24 Mbps, as discussed in the following list:

Asymmetrical DSL (ADSL)

ADSL is the most common of all types of DSL variations. The download speed of data is faster than upload speeds. It uses one channel for analog voice (telephone) transmissions, a second for data uploads, and a third for data downloads.

Symmetrical DSL (SDSL)

SDSL supports equal speeds for both data uploads and downloads. It cannot be used for voice transmissions and hence is suitable only for Internet access at offices.

ISDN DSL (IDSL)

IDSL is a variation of symmetric DSL. It does not support analog voice transmissions and is used only in those environments where ADSL and SDSL are not available.

Rate Adaptive DSL (RADSL)

RADSL is a variation of asymmetric DSL that can vary the transfer speeds depending on line conditions. It supports both data and voice transmissions.

High Data Rate DSL (HDSL)

HDSL is a variation of asymmetric DSL that uses twisted copper wires. It supports both data and voice transmissions.

Very High Data Rate DSL (VHDSL)

VHDSL is a symmetric variation of DSL that supports high-speed transmissions. It does not support sharing the line with voice signals.

Table 8-19 provides a summary of different DSL variations and their data transfer speeds.

Table 8-19. DSL variations

DSL variation	Download speed	Upload speed	Phone usage
ADSL	8 Mbps	1 Mbps	Yes
SDSL	1.5 Mbps	1.5 Mbps	No
IDSL	144 Kbps	144 Kbps	No
RADSL	7 Mbps	1 Mbps	Yes
HDSL	768 Kbps	768 Mbps	No
VHDSL	13 Mbps	1.6 Mbps	Yes

Broadband cable

Broadband Internet Access, or simply Broadband, is provided by the cable companies that provide digital cable services. It is a reliable and efficient means of Internet access. Access is provided through a cable modem that further connects to the computer or to other network devices. Low-cost wired or wireless routers are commonly used to share a single broadband connection among several computers in a home or in small offices.

With a cable modem, the user does not have to dial the ISP, and the connection is always live. This might pose a security risk for computers that are used for critical purposes. Most cable modems support bandwidths from 1.5 to 3 Mbps for Internet access. The cable modem usually supports up to 10 Mbps data speeds for the LAN. The actual Internet access speed depends on the utilization of the shared cable signals in the area. The available bandwidth is always shared with other users in the area and may vary from time to time. In the periods of peak usage, the speed may be low compared to the periods when usage is low.

> Both broadband and baseband are signaling technologies. In simple terms, the broadband technology supports transmission of multiple signals, while the baseband technology supports transmission of only one signal at a time. Most computer networks employ the baseband technology. The broadband technology is used for cable TV.

Plain Old Telephone System/Public Switched Telephone Network (POTS/PSTN)

POTS and *PSTN* are the traditional methods of Internet access. These are dial-up methods; the user has to dial the telephone number of the ISP to authenticate and get Internet connectivity. The telephone line is connected to a modem that is further connected to a serial or USB port of the user's computer. Most computers have built-in modems that can be directly connected to the telephone line. In case the model is connected to an external port such as the serial or the USB port, its software driver must also be installed.

POTS and PSTN provide a maximum data transfer speed of 56 Kbps. There are several ISPs that offer dial-up Internet access. Depending on the area in which the user lives, one must be careful while selecting the ISP. Most ISPs provide added features, such as free email accounts and access to newsgroups, and some even offer small web site for the user.

Satellite

In such areas where DSL or cable is not available, satellite Internet is the only option for high-speed Internet access. For this reason, it is commonly used in rural areas. The signals travel from the ISP to a satellite and then from the satellite to the user. The data transmission speeds vary from 512 Kbps (upload) to 2 Mbps (download). Major drawbacks of satellite Internet access are that it is expensive, and it offers low transfer speeds compared to DSL and cable.

Satellite Internet access suffers from *propagation delays* or *latency* problems. Latency refers to the time taken for the signal to travel from the ISP to the satellite and back to the user. The signals have to travel to a satellite located in the geostationary orbit that is about 35,000 Km away. This means that the signals have to travel approximately 70,000 Km before they reach the user. Latency also depends on atmospheric conditions. This might be a problem for businesses or home users that rely on real-time applications.

Wireless

Wireless Internet access is used by portable devices such as laptop computers, PDAs, mobile phones, and other handheld devices. A *wireless Internet service* *provider (WISP)* usually creates *hotspots* at airports, hotels, coffee shops and other places where people are likely to visit and connect to the Internet. The WISP installs one or more *wireless Access Points (APs)* near the hotspot to share the Internet connection. Most of the newer handheld and portable devices include a built-in wireless adapter. A wireless connection is automatically detected and configured in most cases. Anyone who is in the close proximity of the AP can connect to the Internet almost immediately.

Remote Access Protocols and Services

Remote Access refers to connecting to and accessing the shared resources located on the remote network. All major network and desktop operating systems have built-in support for remote access. There are several different techniques to establish remote access connections. There are also a variety of standards and protocols used for encryption and authentication to provide security for Remote Access Services. In this section, we will take a look at different remote access protocols and services.

Remote Access Service (RAS)

RAS is Microsoft's implementation of remote access protocols and standards. It is available on all Windows Server operating systems. Microsoft renamed it as *Routing and Remote Access Service (RRAS)* in Windows 2000 Server and later operating systems. A Remote Access Server is configured to provide connectivity to remote clients that support remote access protocols. This server acts as a gateway for the organization's internal network. The Remote Access Server authenticates the remote clients before they are allowed access to resources located on other internal servers.

Serial Line Internet Protocol (SLIP)

SLIP is an older remote access protocol that provides point-to-point connections over TCP/IP using serial connections. It was mainly used on Unix platforms. Security is a main concern with SLIP because all usernames and passwords are transmitted in clear text. It does not support any methods for encryption or secure authentication. Besides this, it does not ensure guaranteed delivery of data because of the absence of any error detection, correction, or packet-sequencing mechanisms. In most major network operating systems, Point-to-Point Protocol (PPP) has replaced SLIP.

Point-to-Point Protocol (PPP)

PPP is the standard protocol for remote access due to its clear advantages over SLIP and added security features. It is a protocol suite that includes several protocols. It is a cross-platform protocol and works with all major operating system environments, including Windows, Unix/Linux, NetWare, and Mac OS.

PPP allows encryption of remote user credentials during the authentication process. It also allows administrators to select an appropriate LAN protocol for use over the remote connection. Administrators can choose from NetBEUI, NetBIOS, IPX/SPX, AppleTalk, or TCP/IP. PPP supports several protocols for authentication, such as PAP, SPAP, CHAP, MS-CHAP, and EAP. The administrator can configure multiple protocols, depending on the requirements of remote clients.

PPP Over Ethernet (PPPoE). PPPoE is a combination of PPP and Ethernet protocols. It encapsulates the PPP information inside an Ethernet frame. This enables multiple users on a local Ethernet network to share the remote connection through a common device. For example, multiple users can share the same Internet connection through the cable modem simultaneously.

Although all users on the Ethernet network share a single physical connection to the remote network, PPPoE allows administrators to configure individual authentication for each user. PPPoE also enables administrators to track connection statistics (such as the connection time) of individual users.

Virtual Private Networking

As the name suggests, a *Virtual Private Network (VPN)* provides a secure means of communication between remote users of an organization, between different locations of an organization, or between distinct organizations. The communication takes place using a public network such as the Internet. VPN provides a cost-effective way to provide connectivity to remote users of the organization. This technology saves costs for those organizations that have a large number of telecommuting employees. These employees can connect to internal resources of the organization from anywhere because of the global availability of the Internet. All employees need to do to connect to the organization's network is to simply connect to the local ISP. VPN technologies employ secure authentication and data transmission protocols that work by creating a tunnel in the publicly accessible network (Internet). The tunneling protocols encapsulate authentication and other data within other packets before transmitting over the Internet.

VPN is composed of the following components:

VPN Client

The remote user who wants to establish a connection to the organization's network.

VPN Server

A server running Remote Access Service; authenticates connection requests from the remote client.

Carrier Protocols

Used to transfer data from one point to another over the Internet.

Encapsulating Protocols (tunneling protocols)

Used to wrap the original data before it is transmitted over the Internet. PPTP, L2TP, IPSec, and Secure Shell (SSH) are examples of encapsulating protocols.

VPN can be implemented in one of the following ways:

Remote Access VPN

This is also known as *Private Virtual Dial-up Network (PVDN)*. This type of VPN provides remote access to remote users over the Internet. The remote user is responsible for creating the tunnel and starting the communication. Remote Access VPN is a great solution for an organization that has a large number of users spread across different locations. By using VPN technologies, organizations can save on costs involved in having users directly dial in to the organization's internal network.

Site-to-Site VPN

This is also called an *Intranet* and is established between different offices of the same organization spread across multiple physical locations. This can be a very cost-effective solution because the organization does not have to maintain dedicated WAN connections between physically separated locations. Software-based VPNs require proper planning and secure implementations, as these are prone to the vulnerabilities of the operating system. Hardware implementations are expensive but are generally more secure than their software counterparts.

As noted earlier, VPN essentially depends on a tunneling protocol to successfully and securely transmit data from one location to another using the Internet. The choice of tunneling protocol depends on the solution chosen to implement a VPN. The tunneling process is usually transparent to the end user, who only has to provide appropriate credentials to gain access to internal resources of the organization. The only requirement is that each end of the tunnel must be able to support the selected tunneling protocol. Tunneling protocols are discussed later in this chapter.

Remote Desktop Protocol (RDP)

RDP is used in Microsoft's Windows networks to provide a connection to a server running Microsoft Terminal Services. With Terminal Services, clients connect and run applications on the terminal server as if they are located on the local computer. Terminal Services either run in Remote Administration Mode or in Application Server Mode. With Windows Server 2003 and later operating systems, the Remote Administration Mode has been replaced with the Remote Desktop feature.

Clients for Terminal Services include most versions of Windows and other operating systems such as Unix/Linux and MAC OS. Windows XP Professional and Windows Server 2003 have built-in remote desktop clients. RDP uses TCP port number 3389 by default.

Security Protocols

Network security depends on effective use of security protocols. A variety of protocols are available for implementing security in networks, and administrators must select appropriate protocols in order to provide a secure working environment. Some of the security protocols covered on the Network+ exam are covered in this section.

IP Security (IPSec)

Internet Protocol Security (IPSec) is a standardized framework used to secure IP communications by encrypting and authenticating each IP packet in a data stream. This protocol ensures confidentiality and authentication of IP packets so that they can securely pass over a public network, such as the Internet. IPSec is considered to be an "open standard" because it is not bound to a particular application, authentication method, or encryption algorithm.

IPSec is implemented at the Network layer (Layer 3) of the OSI model. It is made up of the following two components:

Authentication Header (AH)
: The AH secures data or payload by signing each IP packet to maintain its authenticity and integrity.

Encapsulating Security Payload (ESP)
: The ESP protocol also ensures authenticity and integrity of data but adds confidentiality to the data using encryption techniques.

AH and ESP can either be used together or separately. When AH and ESP are used together, the sender and receiver of data can be assured of complete security. IPSec can be implemented in any of the following modes:

Transport mode
: When implemented in transport mode, only the *payload* (the actual message or data) inside the IP packet is encrypted during transmission. The transport mode is generally implemented in host-to-host communications over VPNs or inside a LAN.

Tunnel mode
: When implemented in tunnel mode, the entire IP packet is encrypted. The added security comes at the cost of transmission speed. Tunnel mode IPSec is implemented in gateway-to-gateway VPNs.

IPSec authentication. As noted earlier, IPSec ensures authenticity, integrity, and confidentially of data. IPSec uses the Internet Key Exchange (IKE) mechanism to authenticate the two ends of the tunnel by providing a secure exchange of shared secret keys before the transmission starts. Both ends of the transmission use a password known as a *preshared* key. Both ends exchange a hashed version of the preshared key during IKE transmissions. Upon receipt of the hashed data, it is recreated and compared. A successful comparison is required to start the transmission.

IPSec can also be used for digital signatures. A *digital signature* is a certificate issued by a third-party Certificate Authority (CA) to provide authenticity and non-repudiation. *Non-repudiation* means that the sender cannot deny that he sent the data and can be held responsible for the sent data or message.

Point-to-Point Tunneling Protocol (PPTP)

PPTP is a popular tunneling protocol used to implement VPNs. PPTP uses TCP port 1723, and It works by sending a regular PPP session using Generic Routing

Encapsulation (GRE) protocol. PPTP is easy to configure and supports all major network and desktop operating systems such as Windows, Unix/Linux, and MAC. Due to its low administrative costs, PPTP is the choice of many administrators for VPNs that require medium security. It is commonly used in Microsoft networks, as is Microsoft Point-to-Point Encryption (MPPE), which is used for encrypting data.

Following are some of the limitations of PPTP:

- It cannot be used if the RAS servers are located behind a firewall.
- It works only in IP networks.
- When used alone, PPTP does not provide encryption for authentication data. Only the transmissions after the initial negotiations are encrypted.

Layer 2 Tunneling Protocol (L2TP)

L2TP is another tunneling protocol that is widely supported by most vendors in the IT industry. It uses the Data Link layer (Layer 2) of the OSI model to carry data from one point of the tunnel to another over the Internet. This protocol uses UDP port 1701 for transport. L2TP offers combined benefits of the PPTP and the L2F (Layer 2 Forwarding) protocol from Cisco. It was considered a major improvement over PPTP but still lacks encryption capabilities when used alone. A combination of L2TP and IPSec is generally used to provide secure transmissions for VPN connections. L2TP/IPSec can be used behind firewalls, provided UDP port 1701 is opened for incoming and outgoing packets. Besides this, both ends of the communications must support the L2TP/IPSec protocols.

Some of the advantages of using a L2TP/IPSec combination over PPTP for implementing VPNs include the following:

- L2TP/IPSec requires two levels of authentication: computer or network hardware authentication, and user-level authentication.
- IPSec provides confidentiality, authentication, and integrity for each packet. This helps prevent replay attacks. PPTP provides only data confidentiality.
- IPSec establishes security associations during the transmission of the user-level authentication process. This ensures that the authentication data is not sent unencrypted.
- L2TP/IPSec supports use of RADIUS and TACACS+ for centralized authentication, while PPTP does not.
- L2TP/IPSec can be used on top of several protocols such as IP, IPX, and SNA, while PPTP can only be used with IP.

Secure Socket Layer (SSL)

SSL is an encryption protocol popularly used for Internet-based transactions such as online banking and e-commerce. This protocol is based on public key encryption mechanisms. SSL provides end-to-end security for Internet communications by using encryption. In typical implementations, only the server component is required to use public keys for authentication. For example, when you access a secure server on the Internet that uses SSL, the address of the web site begins with *https://*, while the addresses of unsecure web sites begin with *http://*.

When both the client and the server need to authenticate each other, the SSL communications start with the following steps:

- Both the client and the server negotiate the encryption algorithm.
- The client and the server exchange session keys using public key-based encryption.
- The client and the server authenticate each other using certificates.
- Communications start, and all traffic is encrypted using a symmetric cipher.

The client and the server negotiate a common encryption algorithm and a hashing algorithm. For end-to-end security using SSL, a Public Key Infrastructure (PKI) is required. Both the server and the client must be SSL-enabled to communicate over a secure channel.

Transport Layer Security (TSL) is the successor of Secure Socket Layer (SSL) but can be scaled down to the SSL mode for backward-compatibility.

Wired Equivalent Privacy (WEP)

WEP is a security protocol used mainly for IEEE 802.11 wireless networks. Because wireless networks communicate using radio signals, they are susceptible to eavesdropping. *Eavesdropping* refers to the monitoring and capturing of signals as they travel over network media. WEP is designed to provide a comparable privacy (confidentiality) to a wired network. When sending data over radio frequencies, a WEP-enabled client adds a 40-bit secret key to the data while it is passed through an encryption process. The resulting data is called *cipher text*. On the receiving end, the data is decrypted using the secret key to recover the plain text.

Initial implementations of WEP used a 40-bit encryption key and were not considered very secure. It was still better than not using WEP at all. Soon, a number of tools appeared that could crack the WEP keys. A later version of WEP uses 128-bit encryption keys, which is more secure than the earlier version.

Wi-Fi Protected Access (WPA)

WPA is used for secure access to wireless networks, and it overcomes many weaknesses found in WEP. It is backward-compatible with wireless devices that support WEP, but use of large encryption keys makes it a better choice than WEP. The following are some of the features of WPA:

- It provides enhanced data encryption security by using a *Temporal Key Integrity Protocol (TKIP)*. TKIP scrambles encryption keys using a hashing algorithm. At the receiving end, the hash value of the key is passed through an integrity check to ensure that the key has not been tampered with during transmission.
- WPA uses several variations of Extensible Authentication Protocol (EAP) and public key cryptography.

WPA can also be used in personal mode or a preshared key mode. Each user must know and use a *paraphrase* to access the wireless network. A paraphrase is a short text message that is configured on all wireless devices. In other words, it is the secret key shared by all wireless devices on a network. The preshared key mode is less secure than the standard mode but allows small offices or home networks to secure wireless transmissions. This is particularly useful for small organizations that cannot afford the cost of implementing PKI.

802.1x

802.1x is a secure authentication protocol standard used in wired and wireless networks to provide port-based access control. This standard was mainly developed to provide enhanced security to WLANs. 802.1x provides secure point-to-point connection between a WAP and a host computer. This protocol is based on Extensible Authentication Protocol (EAP) and is usually implemented in closed wireless networks to provide authentication. The authentication process uses the following two components:

Supplicant

Supplicant refers to the software component installed on the user's computer that needs access to a wireless access point.

Authenticator

Authenticator refers to a centralized wireless access point. The authenticator forwards the authentication request to the authentication server, such as a RADIUS server.

When a user (the supplicant) wants access to a wireless network, the 802.1x protocol sends the request to an access point (authenticator). After the communication begins, the supplicant is placed into an *unauthorized* state. There is an exchange of EAP messages between the authenticator and the supplicant, wherein the authenticator requests the credentials of the supplicant. After receiving the credentials, the authentication request is sent to the authentication server, such as the RADIUS server. The authentication server either accepts the credentials of the supplicant and grants access, or rejects it, thereby rejecting the connection request. If the connection is accepted, the user is placed into an *authorized* state.

Authentication Protocols

Authentication is the process of verifying the credentials of a user. In the case of remote access, the user connecting remotely must present one or more sets of credentials to get access to the Remote Access Server. Once the Remote Access Server authenticates the user, further access to network resources is governed and limited by the permissions set on the resources and are applicable to the remote user.

The following are commonly used authentication protocols for remote access:

Challenge Handshake Authentication Protocol (CHAP)

The CHAP authentication protocol is very commonly used for remote access. When the remote link is established, the user is sent a challenge text. The remote user responds with a shared secret in encrypted form using an MD5 hashing algorithm. The user is authenticated only if the secret matches the one stored on the Remote Access Server. CHAP periodically verifies the identity of the user by sending challenge text at random times during the connection.

Microsoft Challenge Handshake Authentication Protocol (MS-CHAP)
MS-CHAP is Microsoft's implementation of the CHAP authentication protocol used on Windows systems. It is a password-based authentication mechanism that is more secure than CHAP. MS-CHAP is an earlier version of MS-CHAPv2 that supports only one-way authentication. MS-CHAPv2 supports two-way authentication in which both client and server authenticate each other using encrypted passwords.

Password Authentication Protocol (PAP)
PAP is the oldest and most basic form of authentication in which the username and password are transmitted in clear text over the dial-up network. The transmissions are unencrypted and insecure.

Extensible Authentication Protocol (EAP)
EAP is the most secure of all authentication mechanisms. It enables the use of a variety of encryption methods for remote access, VPN, and wired and wireless LANs. It supports the use of smart cards for secure authentication.

Shiva Password Authentication Protocol (SPAP)
SPAP is used for authentication to Shiva Remote Access Servers. This protocol is more secure than PAP but not as secure as CHAP, MS-CHAP, or EAP.

Remote Authentication Dial-in User Service (RADIUS)

RADIUS is used to provide centralized authentication for remote users connecting to the internal network of an organization through simple dial-up, VPN, or wireless connection. When a remote user needs access to the internal resources of an organization, he must provide his credentials to the Network Access Server (NAS). The NAS, in turn, sends the user's credentials to the RADIUS server for authentication. If the RADIUS server authenticates the user, the connection request is accepted; otherwise, it is refused.

A RADIUS server can either work as a standalone server to authenticate all connection requests coming from outside users, or it can be a part of a distributed RADIUS setup. Larger organizations deploy multiple RADIUS servers to distribute the authentication load among multiple RADIUS servers. RADIUS servers support several popular protocols such as PAP, PPP, CHAP, and EAP.

When a remote or wireless user sends a connection request, the RADIUS authentication process takes place as follows:

1. When the user attempts to connect to the RAS server, he is asked to supply his credentials, which in most cases are the username and password.
2. The RAS server encrypts the credentials of the user and forwards the request to the RADIUS server.
3. The RADIUS server makes an attempt to verify the user's credentials against a database.

4. If the user's credentials match those stored in the centralized database, the server responds with an *access-accept* message. If the user's credentials do not match the stored credentials, the server sends an *access-reject* message.
5. The RAS server acts upon receipt of access-accept or access-reject messages and grants or denies a connection to the remote user appropriately.
6. If the connection is granted, the RADIUS server may also be configured to automatically assign an IP address to the remote client.

Kerberos

Kerberos is a cross-platform authentication protocol used for mutual authentication of users and services in a secure manner. Kerberos v5 is the current version of this protocol. The protocol ensures the integrity of data as it is transmitted over the network. It is widely used in all other major operating systems, such as Unix and Cisco IOS. The authentication process is the same in all operating system environments.

Kerberos protocol is build upon Symmetric Key Cryptography and requires a trusted third party. Kerberos works in a Key Distribution Center (KDC)—which is usually a network server—used to issue secure encrypted keys and tokens (*tickets*) to authenticate a user or a service. The tickets carry a timestamp and expire as soon as the user or the service logs off. The following steps are carried out to complete the authentication process:

1. The client presents its credentials to the KDC for authentication by means of username and password, smart card, or biometrics.
2. The KDC issues a *Ticket Granting Ticket (TGT)* to the client. The TGT is associated with an *access token* that remains active until the time client is logged on. The TGT is cached locally and is used later if the session remains active.
3. When the client needs to access the resource server, it presents the cached TGT to the KDC. The KDC grants a session ticket to the client.
4. The client presents the session ticket to the resource server, and the client is granted access to the resources on the resource server.

The TGT remains active for the entire active session. Kerberos is heavily dependent on synchronization of clocks on the clients and servers. Session tickets granted by the KDC to the client must be presented to the server within the established time limits; otherwise, they may be discarded.

Network Implementation

This section of the Study Guide focuses on the implementation of the network. Implementing a network is certainly not the job of a single network technician or administrator. It involves several steps that start from planning. Making a good network implementation plan requires that the responsible team of administrators considers all aspects of implementation, such as the organization's requirements, choice of network operating system, application support, security issues, and disaster recovery plans.

A single administrator cannot be expected to have the required knowledge and skills in all areas of network implementation. But, at the same time, each member of the team is expected to have a basic knowledge of essential components of the network. You will need to have a basic understanding of different network operating systems and their interoperability issues. You will also need to know the tools required for network installation and troubleshooting. You must be aware of the security issues and how the firewalls and proxy servers can be used to secure network resources. Finally, a disaster recovery plan must be in place to recover from unforeseen situations, such as fire or floods.

Network Operating Systems (NOS)

NOS provides the basic framework for all computing requirements in a large network. The NOS used these days includes features such as file and print services, authentication, remote access, web services, security, and client configuration. Most vendors provide methods to integrate their NOS with other operating systems. In this section, we will discuss some basic features of network operating systems and their interoperability.

Linux/Unix

Linux is an open source operating system and is freely distributed. With several vendors distributing Linux code, there are many different variations of this operating system—each offering different features. Some of the common distributions are Red Hat, Mandrake, SuSe, and Debian. Linux is based on Unix code, and most of the features available in Unix operating systems are also available in Linux.

Authentication. Linux/Unix users must supply a username and password to log onto an authentication server. A list of users is kept in text files on the authentication server, and the credentials supplied by users are verified from this file, which is called */etc/passwd* (and */etc/shadow*). Linux also supports other authentication mechanisms such as Kerberos, RADIUS, and LDAP. On most Linux distributions, a *Pluggable Authentication Module (PAM)* provides an interface for authentication. PAM is a set of libraries that provides a consistent interface to most authentication protocols.

File and print services. Linux servers have several features to support file and print sharing. Linux uses Network File System (NFS) and Virtual File System (VFS) to manage files and folders. Both NFS and VFS provide file shares to clients. Once the share has been established, the shared files appear to be located on the local system. Samba is used on Linux operating systems, in order to provide file access to Windows clients. Samba provides Server Message Block functionality in order to share folders and printers with Windows clients.

The Linux filesystem allows administrators to control access to files and directories by assigning rights. The following are some of the basic user rights:

Read

Allows users to list, open, and read files.

Write

Allows users to create files, write to files, and modify files.

Execute

Allows users to execute (run) files.

Printing services in Linux/Unix operating systems are provided by the Line Printer Daemon (LPD). A Linux/Unix server should have LPD services running in order to share printers. Newer versions of Linux/Unix use Common Unix Printing System (CUPS), which has extended print services functionality.

Application support. Nearly all server applications written for the Linux operating system platform are third-party applications. In fact, Linux itself is an open source operating system. Most vendors of Linux bundle some basic applications with the operating system. The number of freely available Linux applications is much higher than that available for Windows and NetWare. This is because there are plenty of Linux code developers who consistently provide these applications and make them freely available.

Security. When configured appropriately, Linux is quite a secure operating system. Linux servers are commonly used for email, web services, and as firewalls in medium and large networks. Access to shared resources and network services on Linux servers is controlled through user permissions. Each object has an associated *Access Control List (ACL)* that governs the users' actions. Linux ACLs are stored in text files such as *hosts.allow* and *hosts.deny*.

Users are required to authenticate to a Linux/Unix server before they can access local resources. This authentication is often performed by a username/password combination. When file permissions are configured on Linux servers, administrators have a variety of options to control access, depending on the requirements of the organization.

MAC OS X

The Macintosh Operating System (MAC OS) works mainly on Apple computers. MAC OS 9 was the major operating system used on these computers until MAC OS X was released. The main difference between older versions of MAC operating systems and MAC OS X is that it is based on Linux/Unix technologies.

Authentication. User authentication in MAC OS X is provided through the following types of user accounts:

Limited

This is the most basic type of user account and has very limited permissions.

Standard

This account is meant for most network users. A user can run applications and store files in his home directories, but he cannot make any changes to the system configuration.

Administrator

This account has full control over all other user accounts, file permissions, and system configurations. There must be at least one administrator account on every MAC OS X server.

File and print services. MAC OS X supports *Hierarchical File System Plus (HFS+)*. HFS was originally started with MAC OS 4 and continued until MAC OS 8.1. It supports several advanced features (much like its competitor NTFS in Windows), such as file-level permissions, hiding file extensions, and disk quotas. Journaling is one of the commonly talked about features of HFS+, which keeps a log of hard disk activities. In case there is a system crash, the journal can help the system recover lost files.

In order to provide interoperability with other operating systems, MAC OS X supports other filesystems such as FAT and FAT32, NTFS (Windows NT and later), UDF (Universal Disk Format, used on DVDs), and ISO9660 (used on CD-ROMs). It is important to note that MAC OS X has only read-only support for NTFS.

MAC OS X also supports the following file sharing protocols:

- Network Filing System (NFS) for Linux/Unix platforms.
- Server Message Blocks (SMB) and Common Internet Filing System (CIFS) for Windows operating systems. This functionality is achieved through Samba, which is installed on MAC OS X server by default.
- Apple Filing Protocol (AFP), the native protocol under the MAC TCP/IP protocol suite.

Security. Following the initial installation, a MAC OS X server is fairly secure. The first account created on the server is the administrator account. Each file or folder in MAC OS X has associated sets of permissions. These permissions control the level of access for users and groups. The creator of a file or folder is known as the owner of the object. Users are collected to form groups. A special group named *Everyone* contains all users.

NetWare

NetWare was the operating system of choice for many organizations until Windows and Linux started to gain massive popularity. NetWare Directory Services (NDS) posed tough competition for Windows server operating systems. Microsoft came up with Active Directory services in Windows 2000 Server. NDS is a centralized database of network objects. NetWare is a full-featured network operating system, and several network services such as DHCP, DNS, web, and FTP are bundled with the package. It also supports strong authentication and security mechanisms besides a large number of third-party applications.

Authentication. Like other operating systems, NetWare requires users to provide credentials—usually username and password—to get access to the resources located across the network. A user must supply the following pieces of information to log on to the network:

- Username
- Password
- Directory Context
- Name of the directory tree

The Directory Context and tree names can sometimes be too complex for a user to remember. To get around this problem, it is a common practice to configure the user's desktop with context and tree names.

File and print services. NetWare filesystems work by providing users access to hard disk partitions, known as *volumes*. Clients can map their disk drives to server disk volumes on which they have appropriate rights. File permissions on NetWare servers are assigned through the use of a complex set of rights, as described in the following list:

Supervisor
Includes all rights to the file. This is equivalent to the Full Control permission in Windows.

Read
Allows users to read the file.

Write
Allows users to write to the file.

Create
Allows users to create a new file.

Erase
Allows users to erase (delete) the file.

Modify
Allows users to modify the file contents.

Filescan
Allows users to view a file.

Access Control
Allows users to change permissions on the file.

NetWare supports Novell Distributed Print Services (NDPS) for printing support from NetWare version 6. This version also introduced *iPrint*, which allows users to locate shared printers across the network by clicking a graphical network map.

Application support. The NetWare operating system includes many built-in applications for common network services, such as the DNS, DHCP, and web server. For the most part, NetWare depends on third-party applications. The support for NetWare applications is not as much as for Windows applications. This is due to the fact that NetWare has been losing market share in the recent past to its competitors, Windows and Linux. There are still a plenty of applications available for the NetWare platform.

Security. Access to resources in NetWare is controlled through NetWare Directory Services. Appropriate permissions must be configured for users and groups who need to access shared resources, such as files, folders, and printers, located on NetWare servers. User permissions in the NetWare environment are known as *rights*. The eDirectory remains the centralized place for storing all objects in the network. Objects are stored in containers, and configuring appropriate user rights controls access to container objects. NetWare also allows administrators to lock the console of servers when it is not in use. A command-line utility named *scrsaver* is used for this purpose.

Windows 2000 Server and Windows Server 2003

Windows 2000 Server introduced the concept of Active Directory, which is a centralized database that stores information about all objects, such as computers, users, groups, file shares, or printers. This enables administrators to control the entire network from a single point. Another benefit is that information about network services and resources is not duplicated. Active Directory-based Windows networks operate in domains. A *domain* refers to the logical part of the Active Directory database. Administrators implement group policies that can be applied to the entire domain, or they implement smaller administrative units called *organizational units (OUs)*.

The servers that run the Active Directory services and store the Active Directory database are called *domain controllers*. In large networks, multiple domain controllers are installed to provide fault tolerance, load balancing, and performance. Servers that run other network services except Active Directory service are called *member servers*. File servers, web servers, and DHCP and RRAS servers are some examples of member servers in Active Directory-based Windows networks.

> It is important to note that all domain controllers in an Active Directory network are peers and store read/write copies of the directory database. This is different from Windows NT networks where only Primary Domain Controllers (PDC) stored the Read/Write copy of the directory database and Backup Domain Controllers (BDC) existed for fault tolerance.

Authentication. Windows networks operate in an Active Directory domain. Users are required to log onto the domain only once in order to get access to all network resources located on different network servers. Most of the servers running network services (such as database servers, mail servers, routing and Remote Access Servers, and DNS servers) rely on Active Directory to authenticate users.

Windows 2000 Server and Windows Server 2003 use Kerberos authentication protocol by default. Other authentication protocols, such as NT LAN Manager (NTLM), are also supported for backward-compatibility with legacy Windows clients. For remote access, Windows supports PAP, CHAP, MS-CHAP, and EAP protocols. Use of biometric devices and smart cards requires special hardware. These devices also need advanced administrative skills to implement.

File and print services. In Windows operating systems, files and printers are shared among various users. This task is performed by a service called File and Print Sharing for Microsoft Networks. This service is installed by default on all Windows server and desktop operating systems. Administrators create shared folders on file servers and configure permissions for users and groups. *Groups* are a collection of users with similar job functions. Users are put into groups and groups are assigned permissions to shared files and printers.

To keep tight control on shared resource access, Windows systems enable administrators to configure two types of permissions: Share permissions and NTFS permissions. Share permissions provide an outer layer of control, while NTFS permissions provide more granular control on file and folder access. The following is a list of standard NTFS Permissions:

Full Control
Grants the user all rights on the resource

Modify
Allows a user to change the contents of the file

Read and Execute
Allows a user to read the file and execute (run) it

List Folder Contents
Allows the user to list the files and subfolders inside a folder

Read
Allows a user to read a file

Write
Allows a user to write files to a folder

When a user is a member of multiple groups, the permissions assigned to him in different groups are combined. When both share permissions and NTFS permissions are configured on a folder, the most restrictive of both permissions becomes effective.

> NTFS permissions are available only on those disk partitions that are formatted using NTFS. These permissions cannot be configured on disks formatted with the FAT filesystem.

Printers are usually installed on print servers. When a printer is shared on a Windows server, it allows administrators to add appropriate drivers for Windows clients such as Windows XP, Windows NT, Windows 98, etc. This ensures that Windows clients always use the correct version of the printer driver.

Application support. The Windows operating systems have the largest market share (it is believed to have about 90 percent). This is the reason that this operating system provides support for a majority of software applications. Microsoft itself provides a large number of applications for its operating systems. Besides this, it supports several third-party applications. Essential network services—such as

DNS, DHCP, Internet Information Server (IIS), and Routing and Remote Access (RRAS)—are built into the Windows Server operating system. Windows also comes with limited network monitoring tools to fine-tune the network performance.

Security. As noted earlier, Windows uses the Kerberos authentication protocol by default. Windows servers provide file- and folder-level security using the NTFS. Files can be stored and transmitted over the network in encrypted form. Windows supports use of IP Security (IPSec) for secure transmission of data inside the LAN or over a WAN. For stronger security requirements, Windows has built-in support for digital certificates to provide encryption, authentication, data integrity, and non-repudiation.

Client support. Windows Server operating systems have strong support for Windows-based desktop operating systems such as Windows XP and Windows 2000 Professional. Microsoft always provides support for its legacy operating systems such as Windows NT Workstation, Windows ME, Windows 98, and Windows 95. On some older versions of Windows, additional software might be needed to get full benefits of the new Active Directory features.

Interoperability of operating systems. Windows servers come with built-in support for Unix/Linux, MAC OS X, and NetWare desktop clients. File and Print Services for Macintosh, Client Service for NetWare, etc., are some of the examples of Windows support for other operating systems. The following is a summary of interoperability of common operating systems:

Windows and NetWare

In older Windows desktop operating systems, Client Services for NetWare (CSNW) is installed on Windows clients to enable them to directly connect to NetWare Servers. On Windows servers, the Gateway Service for NetWare (GSNW) is used to provide Windows clients connectivity to NetWare Servers through Windows servers. In Windows Server 2003 platforms, the Windows Services for NetWare is available for free download from Microsoft's web site to provide connectivity to NetWare networks.

Windows and Unix/Linux

Windows and Unix/Linux operating systems are integrated using standard TCP/IP file transfer protocols such as FTP. Clients do not need any additional software or service to interact with Unix/Linux servers. On some versions of Unix and Linux, Windows Services for Unix can be used for limited interoperability.

Linux and NetWare

Most of the interoperability between Linux and NetWare servers is obtained through standard TCP/IP protocols, since both operating systems support TCP/IP. Some older versions of Linux support the IPX/SPX protocol for limited interaction with NetWare servers. NetWare, on the other hand, provides several utilities in its eDirectory to interoperate with Linux servers.

Network Wiring Tools

As a network technician, you might be required to use a number of tools for network installation, testing, and maintenance. Some of these tools are used for preparing cables, while others are used for testing and locating cable faults. On the Network+ exam, you must be able to identify an appropriate tool for a given network task. This section takes a look at some of the common network installation and testing tools.

Wire crimpers

A *wire crimper*, or a *crimping tool*, is used to cut cable to length and attach a suitable connector to it. For example, you must use a crimping tool to cut a UTP cable, strip its sleeve, and then attach an RJ-45 connector to it before you can connect the cable to a networking device. Each type of cable requires a different crimping tool. Some vendors also make crimping tools that can be used for more than one type of cable and connector.

The wire crimper looks just like a special type of pliers. All you need to do is strip the wires off their sleeves, align and insert them properly into the connector housing, and then press the crimping tool. A click sound indicates that the wire has been attached to the connector. You need crimping tools only if you need to make your own cables. You must know the pin configuration for connectors. For example, connections for a UTP straight cable are different from connections for a crossover cable. It is a good idea to have connection details handy. You should also test each piece of cable before using it on the network. Untested cables can cause connectivity problems at a later stage.

Punchdown tools

A punchdown tool is used to attach wires to a patch panel. The *patch panel* is usually a small box where all network or telephone cables are terminated. Each individual wire in the UTP cable is punched down to a single connection point inside the patch panel. The patch panel is usually mounted on a wall.

The connector where the cable wires are attached is known as an *insulation displacement connector (IDC)*. To use a punchdown tool, just push the wires inside appropriate slots, place the tool on top of the wires, and slightly push it down to fix the wires in the slots.

Media testers/certifiers

Media testers, or cable testers, are used to test whether the cable is working properly. Several different types of methods exist for testing cables. A small *multimeter* is perhaps the simplest tool for testing continuity in cables. Cable continuity verifies that wires are not broken. It is very helpful in testing the continuity of a coaxial cable. For a UTP cable, you need to test continuity for each individual wire. Copper-based media testers rely on electrical signals to test the cables. If the electrical current passes through the cable without a break, the cable is considered to be good.

Fiber optic cables are tested using optical cable testers. These testers use light signals to test the cable instead of using electrical signals. Optical cables are prone to breakages that can prevent light signals from reaching the other end. A break in an optical cable is easy to determine, but very hard to find. A special tester called the *Optical Time Domain Reflectometer (OTDR)* is used to pinpoint the correct location of the break in an optical cable. OTDR is an expensive instrument and is mostly used by professional fiber optic network installers.

Tone generators

Tone generators and tone locators are devices that help find cable faults by means of audio signals. The tone generator creates an audio tone (beep) and sends it over the cable. A tone locator is attached to the other end of the cable to check whether the tone reaches there. Using a tone generator is a time-consuming process, and it takes two persons to use the device. Testing cables with a tone generator is also known as the *fox and hound* method. The tone generator must be attached to each individual wire separately.

Loopback connectors

Loopback connectors/adapters are used to test the functionality of a specific port on a network device. These are small connectors that are wired in such a way that the outgoing transmission pins are connected back to the incoming receiving pins. Loopback connectors are often used with RJ-45, serial, and parallel ports. They are used with special software that sends and receives data signals to verify that the port being tested is correctly transmitting and receiving data.

Components of Network Security

In this section, we will cover the main components of network security. Network security is achieved through the use of both software applications and hardware devices. It is possible that you will encounter one or more types of security mechanisms in medium- to large-scale networks. As a network technician, you are expected to have some basic knowledge of essential components of network security. The components tested on the Network+ exam include firewalls, proxy servers, virtual LANs, intranets, and extranets.

Firewalls

A firewall is a hardware device or a software application that sits between the internal network of the organization and the external network in order to protect the internal network from communicating with outside networks. A properly configured firewall blocks all unauthorized access to the internal network. It also prevents internal users from accessing potentially harmful external networks. The three common firewall technologies are:

- Packet filtering firewalls
- Application layer firewalls
- Stateful inspection firewalls

These firewalls are discussed in the following sections.

Packet filtering firewalls. Packet filtering firewalls inspect the contents of each IP packet entering the firewall device, and, based on predefined and configured rules, allows or blocks packets inside the network. These firewalls permit or block access to specific ports or IP addresses, and they work on two basic policies: *Allow by Default* and *Deny by Default*. In the *Allow by Default* policy, all traffic is allowed to enter the network except the specifically denied traffic. In the *Deny by Default* policy, all traffic entering the firewall is blocked except the one specifically allowed. *Deny by Default* is considered to be the best firewall policy, as only authorized traffic is allowed to enter the network using specified port numbers or IP addresses.

Packet filtering firewalls use one of the following criteria for allowing or denying network traffic:

IP addresses

Firewalls can be configured to use the source IP addresses or the destination IP address in order to allow or block certain traffic. For example, you can permit external network traffic coming only from a specific IP address. Alternatively, you can allow only certain internal clients to access the Internet based on their IP addresses.

Port number

The services and protocols in the TCP/IP protocol suite are associated with port numbers. Firewalls and proxy servers can also be configured to allow or block network traffic on the basis of port numbers.

Besides this, packet filtering firewalls can be configured to allow or block traffic based on protocol ID and/or MAC address. Remember that packet filtering firewalls work at the Network layer (Layer 3) of the OSI model. One of the benefits of these firewalls is its easy configuration, because a packet is either allowed or blocked. This technique also does not cause any delays in transmissions. There are certain limitations also. The firewall can inspect the header of the packet but does not read the contents of the packet. Another drawback is that if a certain application opens a port dynamically and does not close it, the open port remains as a security risk to the network.

Application layer firewalls. Application layer firewalls work at the Application layer (Layer 7) of the OSI model. They are also known as *Application firewalls* or *Application layer gateways*. This technology is more advanced than packet filtering, as it examines the entire packet to allow or deny traffic. Proxy servers use this technology to provide Application-layer filtering to clients. Application-layer packet inspection allows firewalls to examine the entire IP packet and, based on configured rules, allow only intended traffic through them.

One of the major drawbacks of application layer firewalls is that they are much slower than packet filtering firewalls. Every IP packet is broken at the firewall, inspected against a complex set of rules, and re-assembled before it is allowed to pass. For example, if the firewall finds signatures of a virus in a packet, it can block it. Although this technique allows for more rigorous inspection of network traffic, it comes at the cost of more administration and speed.

Stateful inspection firewalls. Stateful inspection firewalls work by actively monitoring and inspecting the state of the network traffic, and by keeping track of all the traffic that passes through the network media. This technology overcomes the drawbacks of both packet filtering and application layer firewalls. It is programmed to distinguish between legitimate packets for different types of connections, and only those packets are allowed that match a known connection state. This technology does not break or reconstruct IP packets and hence is faster than Application layer technology.

Using this technology, a firewall can monitor the network traffic and dynamically open or close ports on the device on a need basis, as the communication states of common applications are known to the firewall. For example, if legitimate HTTP traffic enters the firewall, it can dynamically open port 80 and then close it when the traffic has been allowed. This is in contrast to packet filtering where the administrator would have to permanently keep port 80 open on the firewall.

> For the Network+ exam, you will need to know how firewalls work, and what type of firewall is suitable for a given situation. If speed is a concern, and you need to permanently allow or deny access to certain IP addresses or ports, packet filtering is best suited. If inspection of packets is required at the Application level, you will need an application layer firewall. Similarly, if the question asks you about monitoring of network traffic or communication states, select stateful inspection firewall.

Proxy servers

Proxy servers are special network servers that allow network users to connect to the Internet in a secure manner. Unlike Network Address Translation (NAT) and Internet Connection Sharing (ICS), which provide Internet connectivity with limited features, proxy servers offer a wide range of features for better administration of client activities and secure computing. Some of the key features of a proxy server are as follows:

- It allows better utilization of available Internet connection bandwidth.
- It stores web pages locally to improve performance by reducing response times.
- It helps reduce the costs involved in implementing an Internet connectivity solution.
- It helps track user activities while surfing web sites.
- It keeps the internal network secure from the Internet by hiding the internal IP addressing scheme.
- It helps in implementing security for Internet connectivity.

A proxy server offers significant improvement in performance for Internet access due to its caching capabilities. *Caching* refers to the function of a server to locally store web pages as network users access them. The next time a user needs to access the same page, it is quickly displayed on the user's computer instead of having to download it again from the Internet. This feature not only reduces wait times but also helps conserve available Internet connection bandwidth. In smaller networks, proxy server applications can also be configured as firewalls to provide security to the internal network.

Virtual Local Area Network (VLAN)

VLAN is not a physical segment of a network, but a virtual or logical grouping of network devices that share common security requirements. Computers connected to a single VLAN behave as if they are in a single network segment, but physically they may be connected to separate segments. Administrators create VLANs using software applications. The advantage of VLANs is that even if the computers are moved from one physical network segment to another; they remain on the same VLAN. A VLAN is thus a mechanism to create logical segments inside a physical network comprised of multiple physical segments.

In large Ethernet networks, collisions are a main problem. *Collisions* occur when a large number of devices attempt to start transmitting signals on the same network media. Network bandwidth gets congested with a large number of collisions. VLANs help reduce these collisions by creating separate broadcast domains. It is also a method to provide security at the Data Link layer (Layer 2) of the OSI model.

Network switches that support VLAN protocols (known as *VLAN-aware devices*) are mainly used to create VLANs. Cisco switches, for example, use the IEEE 802. 1Q standard and Inter-Switch Link (ISL) protocol for creating VLANs. They also use *VLAN Trunking Protocol (VTP)*, which is proprietary to Cisco, to create VLAN Trunks. A *Trunk* is defined as the point-to-point link between one switch to another. VLAN Trunks allow the creation of *VLAN domains* that help in administration of VLANs. The following are some of the other characteristics of VLANs:

- VLANs are created on the basis of groups and memberships. VLAN memberships can be port-based, protocol-based, or MAC address-based.
- Each VLAN functions like a separate physical network segment so far as network traffic is concerned.
- A VLAN can span multiple physical network segments or multiple switches.
- A Trunk carries network traffic between each switch that is a part of a VLAN.

Intranet. Intranet refers to a private internal network. An intranet typically refers to an internetwork that extends the local boundaries of the network and extends connectivity to company employees at remote locations through a public network such as the Internet. Intranet is usually a private part of the web site of an organization that is accessible only by authorized employees of the organization. Intranets use strong authentication methods to provide secure access. When the intranet traffic passes through the Internet, a “tunnel” is created in the Internet using tunneling protocols such as PPTP or L2TP. The L2TP protocol is used with IPSec to provide an additional layer of security for the transmission of data. Remote Access Service (RAS) and Virtual Private Network (VPN) are examples of Intranets.

The following are some of the important security considerations when implementing intranets:

- Make sure the firewalls are configured properly with rules to allow only intended traffic and block all unwanted or malicious traffic.
- Make sure that only authorized administrators have physical access to configure and maintain firewalls and servers for the intranet.
- Make sure to regularly monitor security logs on firewalls and servers. It is a good habit to conduct frequent security audits of intranet equipment.
- Implement L2TP and IPSec protocols for additional security when the intranet uses VPN using the Internet.
- Make sure to keep all servers updated with the latest service packs, security patches, and antivirus software. Virus scanners should be used regularly.
- Educate users on secure computing habits; this is one of the best defenses against outside attacks. Users must lock their workstations when not in use.

Extranet. Extranets allow external clients to access internal network resources of an organization through the use of VPNs or RAS. Extranets may also be implemented to allow two or more partner organizations to connect their networks. Users who require access to internal resources of an organization are required to use strong authentication mechanisms to ensure security of the network. The same is true when employees of partner organizations attempt to access resources outside their internal network. Extranets should be implemented with the same level of security as that used for implementing intranets. It is always good to use authentication, access control and authorization methods, and encryption for transferring data between employees of different companies. Aside from this, only a handful of employees should be granted access to only the data they require from networks of other organizations.

> Make sure that you understand the difference between *Internet*, *intranet*, and *extranet*. All of these methods can be used to provide secure remote access. Intranets and extranets are typically implemented as VPNs.

Implementing Network Security

Regardless of the network operating system used on the network, there are some essential components of network security that the administrators must understand in order to effectively implement security in a network. Network administrators are expected to have a basic understanding of the different methods available, how they work, and where they can be implemented.

Port blocking/filtering

Port blocking, or *port filtering*, is the process of blocking unwanted traffic to enter a secure network. Port filtering is configured on firewalls and proxy servers to block specific port numbers. For example, if you do not want any FTP traffic to enter the internal network, you may block port number 21 at the firewall.

Blocking a specific port at the firewall thus stops all external traffic destined for the specific port at the firewall itself.

TCP/IP port numbers fall in the following three categories:

- Well-known port numbers range from 0 to 1,023.
- User ports (registered ports) range from 1,024 to 46,151.
- Dynamic private ports range from 46,152 to 65,535.

For the Network+ exam, you will need to know the port numbers used by various network protocols and services. Refer to Table 8-15 to review a list of protocols, services, and their associated port numbers.

Authentication

In the context of computer security, authentication is the method of verifying the identity of a person or an application that wants access to a system, object, or resource. For example, if a user wants to access a network domain, then the authentication or the digital identity of the user is usually verified by the username and password supplied by the user. These are also known as user *credentials*. If the username and password match the ones stored in the security database of the computer, the user is allowed access.

Authentication can be a *one-way* or a *two-way* process. In one-way authentication, only one of the entities verifies the identity of the other, while in a two-way authentication, both entities verify the identity of each other before a secure communication channel is established.

User credentials supplied by the user during the authentication process can be transmitted either in clear text or in encrypted form. Some applications, such as File Transfer Protocol (FTP) and Telnet, transmit usernames and passwords in clear text. User credentials transmitted in clear text are considered security risks, as anyone monitoring the network transmissions can easily capture these credentials and misuse them.

Mutual Authentication. Mutual Authentication, or *Two-way Authentication*, is a process during which both parties authenticate each other before the communication link can be established. In case the communication is to be set up between a client and a server, both the client and server would authenticate one another using a mutually acceptable authentication protocol. This ensures that both the client and the server can verify each other's identity. In a typical setup, the process is carried out in the background without any user intervention.

Username/Password. The combination of username and password is one of the most common methods of authenticating users in a computer network. Almost all network operating systems implement some kind of authentication mechanism wherein users can simply use a locally created username and password to get access to the network and shared resources within the network. These include Microsoft's Windows, Unix, Netware OS, MAC OS X, and Linux.

Many organizations document and implement password policies that control how users can create and manage their passwords in order to secure network resources. If any user does not follow these policies, her user account may be locked until the administrator manually unlocks it. The following is an example of a strong password policy:

- Passwords must be at least seven characters long.
- Passwords must contain a combination of upper- and lowercase characters, numbers, and special characters.
- Passwords must not contain the full or part of the first or last name of the user.
- Passwords must not contain anything with personal identity, such as birthdays, Social Security numbers, names of hometowns, or names of pets.
- Users must change their passwords every six weeks.
- Users must not reuse old passwords.

With a properly enforced password policy, an organization can attain improved security for its network resources.

Biometrics

Biometrics refers to the authentication technology used to verify the identity of a user by measuring and analyzing the physical and behavioral characteristics of a person. This is done with the help of advanced biometric devices, which can read or measure and analyze fingerprints, scan the eye retina and facial patterns, and/or measure body temperature. Handwriting and voice patterns are also commonly used as biometrics. Biometric authentication provides the highest level of authenticity about a person, which is much more reliable than a simple username and password combination. It is nearly impossible to impersonate a person when biometric authentication is used for authentication.

Multifactor. In computer authentication using secure methods, a *factor* is a piece of information that is present to prove the identity of a user. In a multifactor authentication mechanism, any of the following types of factors may be utilized:

- A *something you know* factor, such as your password or PIN.
- A *something you have* factor, such as your hardware token or a smart card.
- A s*omething you are* factor, such as your fingerprints, your eye retina, or other biometrics that can be used for identity.
- A *something you do* factor, such as your handwriting or your voice patterns.

Multifactor authentication is considered to be acceptably secure because it employs multiple factors to verify the identity of the user or service requesting authentication. For example, when withdrawing money from a bank's ATM, you need a debit card, which is a *something you have* factor. You will also need to know the correct PIN to complete the transaction, which is a *something you know* factor.

Encryption

The terms *cryptography* and *encryption* are used interchangeably. Encryption is the process of applying a procedure known as an algorithm to plain text to produce an unreadable text. This unreadable text can only be read if someone has the key to decrypt the message and convert it back to plain text. For all others, the encrypted text remains useless. The following are some of the concepts behind using encryption in network transmissions.

Confidentiality

Confidentiality means that only the intended recipient can decrypt the message and read its contents. The main idea behind encryption is to ensure confidentiality of messages that travel from one computer to another.

Integrity

Integrity of a message ensures that the message has not been intercepted, modified, or altered while it traveled from one point to another. In cryptography, most asymmetric encryption algorithms have built-in mechanisms to ensure message integrity.

Digital signatures

Digital signatures are used to provide data integrity and non-repudiation of data. These ensure that the data sent was not intercepted or modified on its way from the source to the destination.

Authentication

Authentication refers to identity verification. Symmetric encryption algorithms do not provide authentication mechanisms. Asymmetric algorithms have built-in mechanisms to provide authenticity of the messages or data.

Non-repudiation

Non-repudiation ensures that the sender of the message cannot deny that he has sent the digitally signed message. Once again, digital signatures are used to ensure non-repudiation, besides providing the integrity of the message.

Types of malicious codes

Malicious code, or *Malware*, is a software application that is designed to infiltrate a user's computer without his knowledge or permission. Malware includes viruses, Trojan horses, worms, and applications such as adware, spyware, botnets, or loggers. The following are the main categories of malware:

Viruses and worms

These applications are written to infect a system without any obvious commercial gains.

Trojan horses, rootkits, and back doors

These applications are written to infect the target system and conceal the identity of the attacker. These applications often appear interesting and worthwhile to the user, and he is likely to install it.

Spyware, botnets, and adware

These applications are written specifically to gather information about the active user on the system in order to gain some kind of commercial profit. These applications often appear as pop-up windows on the user's computer.

Viruses

A computer virus is a self-replicating application that inserts itself into other executables on the computer and spreads itself using the executable. A computer virus is essentially a malware that is created for the sole purpose of destroying a user's data. The executable file in which the virus inserts itself is called the *virus host*. A virus needs an executable file to spread itself. In order to let the virus work or infect a computer, it must first load into the memory of a system, and the system then must follow the instruction code written in the virus program.

A computer virus can travel from one computer to another infecting every computer on its way, just like a real-life infection. A virus can infect data stored on floppy disks, hard disks, and even on network storage devices. Remember that the infected program must be executed before the virus can spread to other parts of the system or data.

The following are different types of viruses:

Boot sector virus

A boot sector, or *bootstrap* virus, is that which infects the first sector on the hard disk. The first sector of the hard disk is used for booting or starting up the computer. If this sector is infected with a virus, the virus becomes active as soon as the computer is started.

Parasitic virus

A parasitic virus infects an executable file or an application on a computer. The infected file actually remains intact, but when the file is run, the virus runs first.

Worms

A worm is a computer virus that does not infect any particular executable or application but resides in the computer's active memory. This virus usually keeps scanning the network for vulnerabilities and then replicates itself onto other computers using those security holes. The effects of worms are not easily noticeable until entire system or network resources appear to have been consumed by the virus.

The most common type of worm is the email virus, which uses email addresses from the user's address book to spread itself.

Trojan horses

A Trojan horse, or simply a *Trojan*, is a malicious program that is embedded inside a legitimate application. The application appears to be very useful, interesting, and harmless to the user until it is executed. Trojans are different from other computer viruses in that they must be executed by the victim user who falls for the interesting "software."

Most of the modern Trojans contain code that is basically used to gather information about the user. These Trojans fall into the category of spyware and appear as a pop-up window on a user's computer screen. The sole purpose of these Trojans is to somehow trick the user into executing the application so that the code can execute. Some Trojans are written to allow the user's computer to be controlled remotely by the attacker or to collect personal information stored on your computer.

> The main difference between a virus and a Trojan is that viruses are self-replicating programs, while Trojans need some action on the part of the user. If the user does not fall into the trap of the Trojan, it does not execute.

To protect computers from Trojan horses, the following precautions can be taken:

- Keep your operating system updated with the latest service packs, security patches, and hotfixes offered by the manufacturer.
- Install antivirus software on your system and keep it updated.
- Use email settings so that attachments contained in incoming mail do not open automatically. Some Trojans come embedded within email attachments.
- Do not use peer-to-peer sharing networks, such as Kazaa or Limewire. These networks are generally unprotected from Trojans and other viruses.

Some of the well-known Trojans include Back Orifice (and Back Orifice 2000), Beast Trojan, NetBus, SubSeven, and Downloader EV.

Logic bombs

A logic bomb is a specially written malicious code that resides in a particular system and waits for some condition to be met or for an event before it triggers itself. For example, a virus may wait for a specific date or time to trigger itself. A programmer may have a special code written to delete all data and other files from his system as soon as he leaves the company. The action may trigger as soon as the administrator deletes or disables the programmer's account from the network. Another programmer may write a code that waits for a specific date such as April 1st (the April Fools' day) to trigger it.

Fault Tolerance and Disaster Recovery

Fault tolerance refers to the ability of a system to continue functioning in the event of the failure of a component. Every component of the network needs some form of fault tolerance so that the network downtime can be reduced due to failures of server components such as disks and power supplies, network links, and data loss due to user error or disasters. In this section, we will discuss some basic methods used to provide fault tolerance.

Disk fault tolerance

Hard disks are the main storage devices used in servers and desktops. Preventing data loss from disk failures is the primary concern of any organization. Server hardware usually comes equipped with redundant disk arrays to prevent data loss due to disk failures. Disk fault tolerance is achieved by using Redundant Array of Inexpensive Disks (RAID). Different RAID configurations provide varying levels of data protection and performance. A RAID solution can be implemented either through the network operating system or thorough dedicated server hardware. Software-based RAID solutions are inexpensive but are not as efficient as hardware-based RAID solutions. Depending on the requirements of an organization and the allowed budget, the following types of RAID solutions can be implemented.

RAID-1. RAID-1 is one of the most commonly used disk fault tolerance solutions. It is also known as *disk mirroring*. RAID-1 requires exactly two hard disks, equal in size and preferably of the same make and model. RAID-1 provides fault tolerance by writing duplicate data to both disks simultaneously. In case one of the disks fails, data is available from the second disk and the server can continue functioning. To provide a complete fault tolerant RAID-1 solution, both hard disks are connected to separate controllers. This ensures that the server will continue working even if the disk controller fails. This type of RAID-1 solution is known as *disk duplexing*.

The following are some key features of RAID-1:

- It is an inexpensive, entry-level disk fault tolerance solution because it needs only two disks.
- It offers good read performance. There is no advantage for write performance because the data has to be written to two disks simultaneously.
- Disk utilization is 50 percent because only one of the disks is used at a time.
- No special software is required to implement a RAID-1 solution. Most network operating systems have built-in support for implementing RAID-1.
- Disk controllers can also be made fault tolerant by attaching each disk to a separate controller.

Figure 8-22 shows a RAID-1 disk configuration.

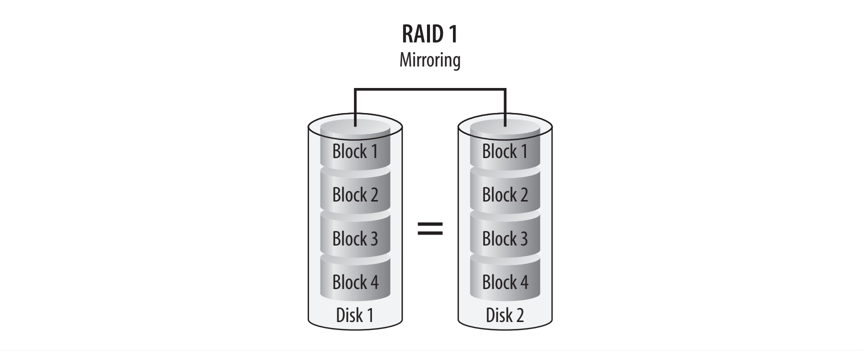


Figure 8-22. RAID-1 disk configuration

RAID-5. RAID-5 is also known as *Disk Striping with Parity*. RAID-5 volumes consist of a minimum of three hard disks. In this configuration, the data is written to the disks, along with parity information, which is distributed among all participating disks. Whenever there is a disk failure, the data stored on the failed disk is rebuilt using the parity information. An equivalent of one disk is used for writing parity information. This means that if you have five 80 GB hard disks (total of 400 GB) in a RAID-5 implementation, you will only be able to use disk space equal to four hard disks (320 GB).

Most server hardware comes equipped with a built-in RAID-5 solution. It is also possible to build a RAID-5 solution using the network operating system. Hardware-based RAID-5 solutions provide better reliability and performance levels than those implemented using the operating system. For example, in a server with hotswap capability, a spare disk will automatically take over a failed disk, and the process will be transparent to the users.

The following are some key features of RAID-5:

- An equivalent of one full disk space is used up for writing parity information.
- RAID-5 offers good disk read performance but poor write performance.
- Hardware-based RAID-5 solutions are expensive. The cost of the server depends on the number of disks installed and whether or not hot-swapping is included in the solution.
- An inexpensive RAID-5 solution can be implemented using the network operating system.

Figure 8-23 shows a RAID-5 disk configuration.

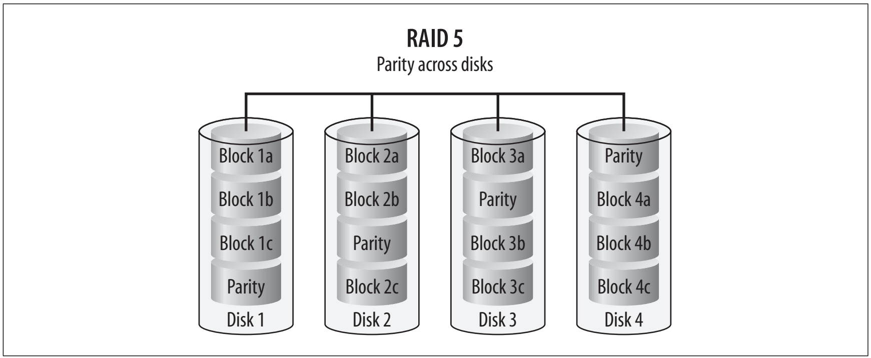


Figure 8-23. RAID-5 disk configuration

Server fault tolerance

Now we know that data stored on hard disks can be protected from loss by using fault-tolerant disk arrays. A hard disk is only one of the components of a network server. The server can also break down due to some other reason, such as failure of the processor, memory, network adapter, or some other critical component. It is important to implement some sort of server fault tolerance also. This ensures that if one of the critical servers fails, another is ready to take over to continue providing access to applications, data, and network services. Both stand-by servers and cluster servers can fulfill this requirement.

Stand-by servers. The stand-by server configuration consists of a minimum of two identical servers: a *primary* server and a *secondary* server. The secondary server is configured identically to the primary server—this is known as *fail-over configuration*. The secondary server monitors the heartbeats of the primary server in order to detect failures. As soon as it detects that the primary server has failed, it takes over the responsibilities of the primary server.

The advantage of configuring stand-by servers is that an additional server is always available to continue essential network services. The disadvantage of this approach is that the secondary server remains unutilized until the primary server has failed. In other words, the server hardware utilization is only 50 percent, which may not be affordable for some organizations.

Server clustering. Server clustering provides fault tolerance as well as high availability for organizations that can afford to install multiple servers for critical network services. Servers are grouped to form a cluster. Applications are installed on the servers and, in case of failure of a single server in the cluster, other servers take over the functions of the failed server. This process remains transparent to network users. The only disadvantage of server clustering is the cost of implementation, which may not be within the budget of some organizations.

Power supply. When planning for a fault-tolerant system, it is important to consider the role of redundant power supplies. Redundant power supplies provide an alternate source of power to servers and other network devices. Some types of server hardware have built-in redundant power supplies. External redundancy can be implemented by using uninterruptible power supply (UPS) systems.

The following are some key benefits of using UPS systems:

- They protect against loss of data due to sudden power failure.
- They provide time to save necessary files and shut down the server properly in case of a power failure.
- They protect expensive hardware from power threats such as spikes, surges, and sags.

Power problems vary in intensity and in consistency. The damage from a bad power source can cause significant losses to an organization due to hardware. A UPS system provides protection from the following types of power problems:

Spike
: A sharp increase in voltage for a very short period of time.

Surge
: A little longer increase in voltage, usually less intense than a spike.

Sag
: A sharp drop in voltage for a short period of time.

Blackout
: A complete failure of power supply.

Brownout
: A drop in voltage that lasts for a significant time.

Link redundancy. Link redundancy refers to providing secondary connectivity solutions to server hardware. This ensures that if the primary network connection is lost for some reason, a secondary connection is always available to take over to prevent interruptions in network services. This is accomplished by *adapter teaming*, which is a process that not only provides fault tolerance but also offers improved performance and effective utilization of available network bandwidth.

The following are some of the key benefits of using adapter teaming to provide link redundancy:

Adapter fault tolerance
: This solution requires two network adapters. One of the adapters is configured as primary and the other as secondary. In case the primary adapter fails, the secondary adapter takes over.

Adapter load balancing
: This solution not only provides fault tolerance but also improved performance. So long as both adapters are working, they share the processing load among themselves. When one of the adapters fails, the second takes over.

Link aggregation
: This refers to effective utilization of available network bandwidth. For example, two 100 Mbps network adapters can provide a total of 200 Mbps bandwidth.

Disaster recovery

Disasters can come at any time and in any form. It may be in a fire, flood, terrorist attack, or some other unknown form. A disaster recovery plan should take into account all possible kinds of internal and external threats. It is important to make necessary plans to protect the critical data from any such events in order to let the organization recover in a minimum amount of time and resume its business as soon as possible. Data-backup methods, secure recovery of data, and a well designed and documented disaster recovery and business continuity plan should be in place. Do not wait for a real disaster to occur.

Data backup

Data backup is one of the fundamental elements of a disaster recovery plan. Backed-up data is copied to another media such as magnetic tapes or compact disks (CDs or DVDs), which are safely and securely stored at an offsite location. The administrators must decide what data to back up and at what frequency, depending on the volume of the backup data and the requirements of an organization. Commonly used backup methods include the following:

Full backup
: This method backs up all the data in a single backup job. The backed-up data includes systems files, applications, and all user data on a computer. Full backup changes the *archive bit* on files to indicate that it has been backed up. It takes longer to complete the backup process, but the data can be restored faster as only a single backup set is required.

Incremental backup

This method backs up all the data that has changed after the last full or incremental backup was taken. It uses the archive bits and changes them after the backup process is complete. It takes the least amount of time to complete the backup process but is the slowest method when data needs to be restored. The last full backup tape and all incremental tapes after the full backup are required to completely restore data.

Differential backup

This method backs up all the data that has changed after the last full backup. It does not change the archive bits, and thus does not disturb any scheduled incremental backups. Since it does not use the archive bits, if differential backup is taken more than once after a full backup, the differential backup tapes will contain duplicate data. When restoring data, only the last full backup tape and the differential backup tape is required. It is faster to restore than the incremental backup.

Copy backup

This method copies all the data on the system but, unlike the full backup, does not change the archive bit.

Most organizations implement a mix of one or more backup types to create weekly, monthly, and yearly backup plans. Depending on the requirements of an organization and the amount of data to be backed up, different organizations may adopt different backup schemes. The combination of full backup on weekends and incremental backups on weekdays is one of the commonly used methods.

> Make sure that you understand different backup types, the function of the archive bit, and the pros and cons of each backup type. The difference between copy backup and full backup is commonly asked in the Network+ exam because both make a full backup of the system. Remember that a copy backup does not use or change the archive bit, while the full backup does both. Similarly, the difference between incremental and differential backup types is another common exam question.

Tape rotation. Magnetic tapes are the most popular media used for backups. In order to reduce the cost involved in purchasing new tapes for every backup, most organizations reuse the tapes after a certain amount of time and according to a pre-set tape rotation plan. A commonly used tape rotation plan is known as *Grandfather-Father-Son (GFS)*. Backup tapes are categorized into daily, weekly, and monthly sets. With this rotation scheme, a full backup is taken every week and differential or incremental backups are taken every day. The daily and weekly tapes are stored offsite at the end of the week, and new tapes are used the next week. Additionally, another full backup is taken at the end of the month.

When the month changes, the tapes used for the first week in the previous month are reused, followed by the tapes used in the second week and so on. In the GFS rotation scheme, the daily tape set is known as *son*, the weekly tape set is known as *father*, and the monthly full backup tape set is known as *grandfather*. It is important to note that the grandfather tape set is not reused as it contains all files changed during a particular month.

Offsite storage. It is important that the tapes be stored at a safe and secure offsite location. Offsite storage helps protect critical data stored on tapes in the event of a disaster. If backup tapes are not stored offsite, they are vulnerable to destruction along with other equipment when a disaster strikes. Organizations may store tapes at another location or can engage a third-party professional organization for the purpose. It is important that administrators make an assessment that the safety and security requirements are fulfilled if offsite storage is managed by a third party.

Secure recovery. The secure recovery of data is a part of the backup process. Data may need to be recovered from backup tapes even when a small incident such as accidental deletion of files happens or when a virus application corrupts files. The damage may occur on a single system or on multiple systems across the network. Also, administrators should not forget that the organization might be subject to outside malicious activity by professional hackers. The worst-case scenario is a disaster that requires administrators to carefully make a disaster recovery plan and define procedures for secure and quick restoration of data.

The safety of backup tapes is of prime concern. This includes protecting the tapes from physical damage and theft of the stored data. Aside from this, procedures and guidelines must be in place to describe how the data can be restored with minimal delays. Large organizations usually have dedicated backup operators who are proficient in backup and restoration functions. Offsite storage is an excellent way to secure tapes. Large organizations can also have alternate sites, which can be used to resume business in case of a disaster.

Hot and cold spares. Most organizations keep spare parts for critical servers in order to prevent delays in restoring a failed system. Hot and cold spares are part of disaster recovery plans of the organization. In case a server component such as the hard disk or a power supply fails, network technicians or administrators can quickly replace the failed part to restore the functioning of the server.

Hot spares

Refer to spare components that are installed inside critical servers and readily take over a failed component. These spares do not need any action from the administrator. The hot spare automatically takes charge of the failed component almost immediately, and the functioning of the server is not affected at all.

Cold spares

Refer to spare components that are installed inside a critical server but must be configured manually by an administrator.

Hot swapping

Refers to the ability of a server to allow replacement of a failed component (usually a hard disk in the disk array) while the server is powered on. The most common use of hot swapping is in hard disk arrays used in fault-tolerant RAID systems. Unlike hot spares, hot swapping requires manual replacement by an administrator.

Cold swapping

Refers to servers that do not support the replacement of failed components while they are powered on. A technician or an administrator must fully power down the server and manually replace the failed component. Cold-swapped components are usually not installed in the system and are stored outside of it.

Most of the server hardware that provides critical network services or is critical to the functioning of the business is equipped with hot spares. In organizations where server downtimes are not acceptable, hot spares are a necessity.

Hot, warm, and cold sites. Alternate sites are critical to all organizations that do not want any delay in restoration of data after a disaster strikes. An *alternate site* is a temporary facility away from the original location of the organization that enables administrators to restore a working network in a minimum amount of time so that the organization can resume its business. Alternate sites can be classified into the following types:

Hot site
: A hot site is equipped with the necessary hardware, software, network devices, and telephone lines. It allows organizations to resume business activities almost immediately. The equipment is fully configured, data is replicated to servers at the site in real time, and, in case of a disaster, the organization can resume business with minimal delays.

Warm site
: A warm site normally is equipped with the necessary hardware, software, network devices, and telephone lines. Unlike a hot site, this site is not fully configured and does not store a working copy of data. Hardware and software must be configured and data must be restored from backup tape sets. It takes administrators a little while before this site can be made functional.

Cold site
: A cold site requires the maximum amount of time to be set up and made functional. It contains only partial hardware, software, and network devices that are not configured. This site needs to be built from scratch to make it fully functional.

Network Support

The term *network support* refers to providing network services to end users. It involves tasks such as installation, maintenance, and troubleshooting. Network and system administrators, helpdesk staff and network technicians work together to provide maximum availability and seamless operations of network services. The objective is to minimize interruptions in regular work due to network downtimes. This section covers a study of troubleshooting utilities and techniques for supporting computer networks.

Troubleshooting Utilities

Network troubleshooting is an essential part of the responsibilities of a network technician. A network technician is expected to have knowledge and skills to use appropriate troubleshooting utilities to diagnose problems and find solutions. This section provides an overview of commonly used troubleshooting utilities available for troubleshooting network connectivity problems.

tracert/traceroute

The *tracert* or *traceroute* utility is used to trace the route to from one host to another in a TCP/IP network. All major operating systems include this utility in one form or another. The name of the utility might differ, but the purpose is the same: to find out the path between two TCP/IP hosts. The output format of this utility differs from one operating system to another. It uses the *Internet Control Message Protocol (ICMP)* echo packets to trace the route to a specific destination host and reports back the results at every hop on the path.

The syntax of the *traceroute* command in different operating systems is as follows:

- Windows operating systems: `tracert <Hostname>` or `tracert <IPAddress>`
- Unix/Linux and MAC OS: `traceroute <Hostname>` or `traceroute <IPAddress>`
- NetWare: `iptrace`

The *traceroute* utility offers very useful information when diagnosing connectivity problems. It provides the IP address of every router (hop) that it passes through and reports the time it takes from one hop to another. This is helpful in diagnosing the exact location of the network bottleneck or congestion.

The following example shows the output of the *tracert* utility when used to trace the route to the web site *www.oreilly.com*:

```
C:\ >tracert www.oreilly.com
Tracing route to www.oreilly.com [208.201.239.37]
over a maximum of 30 hops:
  1     1 ms    <1 ms    <1 ms  192.168.1.1
  2    65 ms    91 ms    88 ms  72.138.64.129
  3    25 ms    59 ms    49 ms  10.1.65.129
  4    52 ms    50 ms    65 ms  gw01.hnsn.phub.net.cable.rogers.com
[66.185.80.25]
  5    47 ms    61 ms    57 ms  gw02.mtnk.phub.net.cable.rogers.com
[66.185.81.94]
  6    68 ms   137 ms    63 ms  igw01.ny8th.phub.net.cable.rogers.com
[66.185.81.13]
  7     *        *        *     Request timed out.
  8    95 ms    76 ms    55 ms  so-2-1-0.cr1.ord1.us.nlayer.net
[69.22.142.106]
  9   116 ms   112 ms   128 ms  so-2-3-0.cr1.sfo1.us.nlayer.net
[69.22.142.78]
 10   152 ms   155 ms   108 ms  ge2-7.hr2.sfo1.us.nlayer.net [69.22.143.26]
 11   158 ms   161 ms   137 ms  sonic.ge2-3.hr2.sfo1.us.nlayer.net
[69.22.130.62
 12   131 ms   121 ms   120 ms  0.at-1-0-0.gw4.200p-sf.sonic.net
[64.142.0.186]
 13   159 ms   141 ms   118 ms  0.ge-0-1-0.gw.sr.sonic.net [64.142.0.197]
 14   146 ms   143 ms   166 ms  gig49.dist1-1.sr.sonic.net [209.204.191.30]
 15   166 ms   148 ms   115 ms  ora-demarc.customer.sonic.net
[64.142.122.36]
 16   153 ms   164 ms   146 ms  www.oreillynet.com [208.201.239.37]
Trace complete.
```

It is easy to interpret the results of the *tracert* utility. The first column shows the hop number, which is the network device that responds to the ICMP echo request. The next three columns show the roundtrip time in milliseconds that the packet takes. The next column shows the hostname and the IP address of the responding device.

In some situations, the network is congested. This is shown as `Request Timed Out` in the output. This may be due to a misconfigured router at the seventh hop. But the trace continues to the next hop until it reaches the destination. Once the problem device is identified, you may use some other utility, such as *ping,* to pinpoint the source of the issue.

The following is an example of an unsuccessful attempt to trace route to the web site *comptia.org*. Notice that after tracing the route up to 13 hops, the ICMP echo request is being timed out. In other words, the *tracert* utility has failed to get a response from the next hop device.

```
C:\ >tracert comptia.org
Tracing route to comptia.org [208.252.144.4]
over a maximum of 30 hops:
  1    <1 ms    <1 ms    <1 ms  192.168.1.1
  2    30 ms    29 ms    29 ms  72.138.64.129
  3    24 ms    29 ms    29 ms  10.1.65.129
  4    28 ms    29 ms    29 ms  gw01.nmkt.phub.net.cable.rogers.com
[66.185.80.109]
  5    27 ms    29 ms    29 ms  gw01.mtpk.phub.net.cable.rogers.com
[66.185.81.213]
  6    28 ms    27 ms    29 ms  66.185.80.46
  7    41 ms    35 ms    40 ms  igw01.chcrmk.phub.net.cable.rogers.com
[66.185.80.201]
  8    51 ms    54 ms    53 ms  so-4-3-0.mpr1.ord7.us.above.net
[64.124.11.21]
  9    56 ms    57 ms    60 ms  above-oc12.ord.ALTER.net [64.125.12.246]
 10    59 ms    59 ms    62 ms  0.so-5-2-0.XL2.CHI2.ALTER.NET [152.63.68.6]
 11    68 ms    60 ms    64 ms  0.so-7-0-0.XL2.CHI1.ALTER.NET
[152.63.64.137]
 12    64 ms    58 ms    60 ms  POS7-0.GW4.CHI1.ALTER.NET [152.63.68.233]
 13   224 ms   226 ms   219 ms  Comptia-chi-gw.customer.ALTER.NET
[157.130.102.146]
 14     *        *        *     Request timed out.
 15     *        *        *     Request timed out.
 16     *        *        *     Request timed out.
 17     *        *        *     Request timed out.
```

ping

The *ping* utility is used to test connectivity between two TCP/IP hosts. Like the *tracert* utility, it also uses ICMP echo requests to the destination host. This utility is a part of the TCP/IP protocol suite and is installed by default on all TCP/IP devices. Ping can quickly determine whether the host is connected or not and how long it takes for the request to take the roundtrip. Aside from testing connectivity, the *ping* command can also be used to test whether the name resolution is working.

On Windows XP/2000/2003 computers, the *ping* command sends out four ICMP echo packets by default. The following is an example of a successful *ping* command:

```
C:\ >ping www.google.com
Pinging www.l.google.com [72.14.207.99] with 32 bytes of data:
Reply from 72.14.207.99: bytes=32 time=20ms TTL=246
Reply from 72.14.207.99: bytes=32 time=24ms TTL=246
Reply from 72.14.207.99: bytes=32 time=19ms TTL=246
Reply from 72.14.207.99: bytes=32 time=22ms TTL=246
Ping statistics for 72.14.207.99:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 19ms, Maximum = 24ms, Average = 21ms
```

ping command parameters. The *ping* command supports a number of parameters for increased functionality. Some of the common parameters and their functions are listed in Table 8-20.

Table 8-20. ping command parameters

Parameter	Function
`ping -a`	Resolves and displays the given IP address to the hostname.
`ping -n Count`	Specifies the number of echo requests to be sent. By default, four messages are sent in Windows OS.
`ping -r Count`	Specifies that the count hops be recorded. The *Count* must be a number between 1 and 9.
`ping -s Count`	Specifies that the timestamp be used to record echo request messages. The *Count* must be a number between 1 and 4.
`ping -i TTL`	Specifies the Time-To-Live (TTL) value for echo request messages. For Windows operating systems, the value of *TTL* must be less than 255.
`ping -t`	This parameter forces the *ping* command to continue sending echo messages until manually stopped.
`ping -w Timeout`	Specifies the timeout value in milliseconds for each echo reply.

Understanding ping output messages. When you use the *ping* utility to diagnose network problems, you must be able to interpret the output correctly in order to find out the exact cause of the problem. The following are some of the common output messages that you must be able to understand:

Request Timed Out

A *Request Timed Out* message indicates that the echo request message did not get any response from the destination host. The destination device might not be connected to the network, be powered down, or configured correctly. It may also mean that the destination host does not exist, and you might be using an incorrect address with the *ping* command. Some intermediate device on the path may also not be functioning. The code that follows is an example of this message.

```
Pinging 192.168.0.2 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 192.168.0.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss)
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Destination Host Unreachable

The *Destination Host Unreachable* error message appears in the *ping* output when the host you are trying to *ping* is not found. Check that the local host is correctly configured with the IP address of the default gateway. The following is an example of this error message. Note that the ping statistics are similar to the *Request Timed Out* message.

```
Pinging 192.168.0.2 with 32 bytes of data:
Destination host unreachable.
Destination host unreachable.
Destination host unreachable.
Destination host unreachable.
Ping statistics for 192.168.0.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Unknown Host

The *Unknown Host* error message means that the specified hostname could not be resolved. This problem is associated with the DNS. Check that the DNS server address is correctly configured on the local host and the DNS server is online and connected to the network. This may also mean that the *HOSTS* file is not correctly configured on the local host. In this situation, you might need to use another utility, such as *nslookup* or *dig*, to find out the exact problem. The following is an example of this message:

```
C:\>ping www.mydomain.com
Unkown host www.mydomain.ca
```

TTL Expired

Each *ping* command is executed with a default Time-To-Live (TTL) value. Each time the *ping* echo message encounters a network device, the TTL value is subtracted by 1. The purpose of the TTL is to prevent the echo message from looping around different network devices. The TTL Expired error message means that the echo message sent to the destination could not get a response, and the TTL value is reduced to 0. This indicates a routing problem on the network. On Windows operating systems, you can use the *ping –i* command to increase the TTL value to a maximum of 255. The following is an example of this message:

```
Reply from 192.168.0.2: TTL Expired in transit.
```

Troubleshooting with ping. *ping* is one of the most frequently used troubleshooting utilities, which is available in all implementations of the TCP/IP networks. When diagnosing a connectivity problem with *ping*, the following steps should be taken:

1. *ping* the local loopback address 127.0.0.1. A successful *ping* to this address verifies that the TCP/IP is correctly installed and working on the local host. If the request times out, you might need to reinstall the TCP/IP on the local host.
2. *ping* the IP address configured on the network interface of the local host. If this is successful, the TCP/IP is correctly installed and configured on the network interface. If the request times out, the interface might not be correctly bound to TCP/IP, or it may not be using a correct driver.
3. *ping* the IP address of another host on the local network segment. If this is successful, the local host can connect to other hosts on the local segment. If the request times out, you might need to check the network connections on the local host, or on the hub or switch.
4. *ping* the IP address of the default gateway configured on the local host. If this is successful, the local host can connect to remote hosts located in other network segments. If this command fails, verify that the default gateway is correctly configured and that it is operational on the network.
5. Finally, when the *ping* to the default gateway is successful, you can try to *ping* the IP address of a remote host.

If these steps do not resolve the problem, you might have to use other TCP/IP diagnostic utilities.

arp

The arp is used to resolve an IP address to the MAC address. The *arp* is a command-line utility that can be used to diagnose address resolution problems. Hosts on TCP/IP networks use IP addresses to communicate to each other. IP addresses are further resolved to their MAC addresses in order to deliver IP packets to the correct host. These MAC addresses are temporarily stored on the local host in the ARP cache. The ARP cache is a table that maps recently resolved IP addresses and their corresponding MAC addresses. It is periodically refreshed with newer entries, and older entries are deleted. Whenever a host needs to send a packet to another host, it first checks its local ARP cache before sending a broadcast message on the local network.

There are two types of entries in the ARP cache: *dynamic* and *static*. The dynamic entries are created automatically as the local host resolves IP addresses. The static entries are added manually using the *arp –s* command. You can check the ARP cache of the local computer anytime by using the *arp –a* command the *arp –g* command. Here is an output of this command on a Windows XP computer:

```
C:\ >arp -a
Interface: 192.168.1.100 --- 0x10003
  Internet Address      Physical Address      Type
  192.168.1.1           00-40-f4-e4-48-50     dynamic
```

The *arp* command supports several parameters, as listed in Table 8-21.

Table 8-21. arp command parameters

Parameter	Function
`-a` or `-g`	Displays the ARP cache entries.
`eth_addr`	Specifies a MAC address.
`inet_addr`	Specifies the Internet address.
`-N <if_addr>`	Specifies a particular network interface.
`-d`	Deletes an entry from the ARP cache.
`-s`	Adds a static entry in the ARP cache.

netstat

The *netstat* utility is used to display the protocol statistics and current active TCP/IP connections on the local host. When used without using any parameters, this utility displays all inbound and outbound TCP/IP connections, as shown in the following output.

```
C:\ >netstat
Active Connections
Proto  Local Address    Foreign Address            State
TCP    pkb:1038         phx.gbl:1863               ESTABLISHED
TCP    pkb:1049         209.123.81.160:http        CLOSE_WAIT
TCP    pkb:1050         209.123.81.160:http        CLOSE_WAIT
TCP    pkb:1054         209.123.81.167:http        CLOSE_WAIT
TCP    pkb:1055         209.123.81.167:http        CLOSE_WAIT
TCP    pkb:4064         qb-in-f99.google.com:http  ESTABLISHED
TCP    pkb:4065         qb-in-f99.google.com:http  ESTABLISHED
TCP    pkb:4078         ns-vip2.hitbox.com:http    ESTABLISHED
TCP    pkb:4080         208.252.144.4:http         ESTABLISHED
TCP    pkb:4081         208.252.144.4:http         ESTABLISHED
TCP    pkb:4083         qb-in-f99.google.com:http  ESTABLISHED
TCP    pkb:4084         206-5.amazon.com:http      ESTABLISHED
TCP    pkb:4085         209.123.81.153:http        ESTABLISHED
TCP    pkb:4086         209.123.81.166:http        ESTABLISHED
```

The output includes columns such as protocol, local address and port number; foreign address (destination) and its port number; and the current state of the connection. The *netstat* utility includes several parameters that can be used to correctly pinpoint a specific problem with the TCP/IP connections. Table 8-22 lists different parameters available with this command.

Table 8-22. netstat command parameters

Parameter	Function
`-a`	Displays all current connections and listening ports.
`-e`	Displays Ethernet statistics. You may combine this with the `-s` parameter.
`-n`	Displays addresses and port numbers in numerical form.
`-p Protocol`	Displays statistics for the specified protocol.
`-r`	Displays the routing table.
`-s`	Displays per-protocol statistics. By default, statistics are shown for IP, ICMP, TCP, and UDP.
`Interval`	Redisplays the selected statistics and pauses between each display by the time specified by `Interval`.

The following examples explain how the *netstat* utility can be used to display the current TCP/IP activities on the local host using various parameters. While interpretation of all output statistics is beyond the scope of the Network+ exam, most of the outputs are self-explanatory.

Displaying detailed TCP/IP connection statistics. You can also use the *netstat –s* command to display detailed statistics of different protocols such as IP, ICMP, TCP, and UDP, as shown in the following output:

```
C:\ >netstat -s

IPv4 Statistics
  Packets Received                   = 172706
  Received Header Errors             = 0
  Received Address Errors            = 8624
  Datagrams Forwarded                = 0
  Unknown Protocols Received         = 0
  Received Packets Discarded         = 0
  Received Packets Delivered         = 166185
  Output Requests                    = 147800
  Routing Discards                   = 0
  Discarded Output Packets           = 0
  Output Packet No Route             = 0
  Reassembly Required                = 0
  Reassembly Successful              = 0
  Reassembly Failures                = 0
  Datagrams Successfully Fragmented  = 0
  Datagrams Failing Fragmentation    = 0
  Fragments Created                  = 0

ICMPv4 Statistics
                           Received    Sent
  Messages                  289         20
  Errors                    32          1
  Destination Unreachable   253         19
  Time Exceeded             3           0
  Parameter Problems        0           0
  Source Quenches           1           0
  Redirects                 0           0
  Echos                     0           0
  Echo Replies              0           0
  Timestamps                0           0
  Timestamp Replies         0           0
  Address Masks             0           0
  Address Mask Replies      0           0

TCP Statistics for IPv4
  Active Opens                        = 3110
  Passive Opens                       = 114
  Failed Connection Attempts          = 80
  Reset Connections                   = 383
  Current Connections                   = 5
  Segments Received                     = 130377
  Segments Sent                         = 111391
  Segments Retransmitted                = 1507

UDP Statistics for IPv4
  Datagrams Received    = 35498
  No Ports              = 6811
  Receive Errors        = 1
  Datagrams Sent        = 34941
```

Activities of network interface. The activities of the network interface card can be displayed using the *netstat –e* command, as shown in the following output:

```
C:\ >netstat -e
Interface Statistics
                           Received            Sent
Bytes                     127209366        46129918
Unicast packets              164016          147614
Non-unicast packets            8591             191
Discards                          0               0
Errors                            0               0
Unknown protocols                 0
```

TCP and UDP statistics. The statistics for TCP and UDP can be displayed using the *netstat –a* command, as shown in the following output:

```
C:\ >netstat -a
Active Connections
Proto  Local Address          Foreign Address      State
TCP    pkb:epmap              pkb:0                LISTENING
TCP    pkb:microsoft-ds       pkb:0                LISTENING
TCP    pkb:1025               pkb:0                LISTENING
TCP    pkb:netbios-ssn        pkb:0                LISTENING
TCP    pkb:1038               phx.gbl:1863         ESTABLISHED
TCP    pkb:1049               209.123.81.160:http  CLOSE_WAIT
TCP    pkb:1050               209.123.81.160:http  CLOSE_WAIT
UDP    pkb:microsoft-ds       *:*
UDP    pkb:isakmp             *:*
UDP    pkb:1028               *:*
UDP    pkb:1031               *:*
UDP    pkb:1045               *:*
UDP    pkb:ntp                *:*
UDP    pkb:netbios-ns         *:*
UDP    pkb:netbios-dgm        *:*
UDP    pkb:10891              *:*
UDP    pkb:45762              *:*
UDP    pkb:57838              *:*
```

Displaying the routing table. The routing table of the local host can be displayed using the *netstat –r* command, as shown in the following output:

```
C:\ >netstat -r
IPv4 Route Table
===========================================================================
Interface List
0x1 ........................... MS TCP Loopback interface
0x10003 ...00 0b 6a 0b 71 d8 ...... VIA Rhine II Fast Ethernet Adapter
===========================================================================
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      192.168.1.1    192.168.1.100     20
        127.0.0.0        255.0.0.0        127.0.0.1        127.0.0.1      1
      192.168.1.0    255.255.255.0    192.168.1.100    192.168.1.100     20
    192.168.1.100  255.255.255.255        127.0.0.1        127.0.0.1     20
    192.168.1.255  255.255.255.255    192.168.1.100    192.168.1.100     20
        224.0.0.0        240.0.0.0    192.168.1.100    192.168.1.100     20
  255.255.255.255  255.255.255.255    192.168.1.100    192.168.1.100      1
Default Gateway:       192.168.1.1
===========================================================================
Persistent Routes:
  None
```

nbtstat

The *nbtstat* utility is exclusive to Windows operating systems. It is used to display the NetBIOS over TCP/IP connection statistics. In case there is a problem with NetBIOS name resolution, the *nbtstat* utility comes in handy to diagnose it. Table 8-23 lists common parameters available for this command and their functions.

Table 8-23. nbstat command parameters

Parameter	Function
-a	Displays the NetBIOS name table of a remote host given its name.
-A	Displays the NetBIOS name table of a remote host given its IP address.
-c (cache)	Displays the name table of the remote host.
-n (names)	Displays local NetBIOS names.
-r (resolved)	Displays the NetBIOS names resolved using WINS.
-R (Reload)	Purges the NetBIOS cache of the specified remote host.
-RR	Sends name release packets to WINS and then begins again.
-s	Displays sessions table with only IP addresses.
-S	Displays sessions table converting destination IP addresses to NetBIOS names.
nbtstat RemoteName	Displays the machine name of a remote host.
nbtstat IPAddress	Displays the IP address in a dotted decimal notation.
nbtstat Interval	Redisplays selected statistics pausing the number of seconds, as specified in the Interval parameter, between each display.

> The parameters available with the *nbtstat* utility are case-sensitive. For example, the function of *nbtstat –a* is different from the *nbstat –A* function. Similarly, the functions *-s* and *–S* parameters and, -r and –R parameters are not the same. This is different from most other Windows commands, which are not case-sensitive.

The following is a sample output of the *nbtstat* command when used with the *–n* parameter. The output lists the entries in the local NetBIOS name cache.

```
C:\ >nbtstat -n
Local Area Connection:
Node IpAddress: [192.168.1.100] Scope Id: []
                NetBIOS Local Name Table
       Name              Type         Status
    ---------------------------------------------
    PKB              <00>  UNIQUE      Registered
    WORKGROUP       <00>  GROUP       Registered
    PKB              <20>  UNIQUE      Registered
    WORKGROUP       <1E>  GROUP       Registered
    WORKGROUP       <1D>  UNIQUE      Registered
```

ipconfig

The *ipconfig* utility is used in Windows operating systems to display the TCP/IP configuration of the local host. It is commonly used with the /all parameter to display the configuration of all network adapters installed on the system. The following is a sample output of the *ipconfig /all* command:

```
C:\ >ipconfig /all
Windows IP Configuration
   Host Name . . . . . . . . . . . . : pkb
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Unknown
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
Ethernet adapter Local Area Connection:
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : VIA Rhine II Fast Ethernet Ada
pter
   Physical Address. . . . . . . . . : 00-0B-6A-0B-71-D8
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IP Address. . . . . . . . . . . . : 192.168.1.100
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DNS Servers . . . . . . . . . . . : 192.168.1.1
   Lease Obtained. . . . . . . . . . : Monday, October 02, 2006 12:40:09 PM
   Lease Expires . . . . . . . . . . : Monday, October 02, 2006 1:40:09 PM
```

Table 8-24 lists the parameters and their functions available with the *ipconfig* command.

Table 8-24. ipconfig command parameters

Parameter	Function
`/all`	Displays the TCP/IP configuration of all network adapters on the local host.
`/release`	Releases the DHCP supplied TCP/IP configuration of the network adapter.
`/renew`	Renews DHCP supplied TCP/IP configuration of the network adapter.

On Windows XP, Windows 2000, and Windows Server 2003 operating systems, the *ipconfig* utility also includes the following parameters:

`/flushdns`
: Used to clear the DNS cache on the local host.

`/displaydns`
: Used to display the entries in the local DNS cache.

`/registerdns`
: Used to register the name of the local host with the DNS server.

ipconfig is very useful in troubleshooting configuration problems on a TCP/IP host. The output of the *ipconfig /all* command can reveal one or more problem areas, and an administrator can take necessary corrective action to resolve the problem. For example, if the output does not show a valid IP address, the *ipconfig /release* and *ipconfig /renew* commands can renew the IP address of the host with the DHCP server. On a Windows XP/2000/2003 system, if the host is unable to resolve DNS names, the *ipconfig /flushdns* can be used to clear the DNS cache. Similarly, if the host is not able to connect to any remote hosts, the default gateway address should be checked in the output of the *ipconfig* command.

ifconfig

The *ifconfig* command is the Unix/Linux and MAC OS X equivalent of the Windows *ipconfig* command. Unlike the limited features of *ipconfig*, this command has much more advanced diagnostic features. Typing `ifconfig help` at a Unix host command prompt gets you all the parameters and other information about how this command could be used.

winipcfg

The *winipcfg* command was used on Windows 95, Windows 98, and Windows Me computers to display the current TCP/IP configuration settings. Unlike other TCP/IP utilities, this is a graphical utility that displays all information in a window. The output of the *winipcfg* command includes the following information:

- The MAC address of the network adapter.
- The IP address and the subnet mask assigned to the computer.
- The IP address of the default gateway.
- The IP address of the configured DHCP server.
- The IP addresses of the primary and secondary WINS servers.
- Information about when the current lease was obtained and when it is due to expire.

The output of the *winipcfg* command can be analyzed to correctly diagnose a connectivity problem on Windows 95/98/Me computers. For example, if the computer is not able to connect to any other computer on a remote network, the IP address of the default gateway might be incorrect, or it may not be online. Similarly, if the computer is not able to connect to any other computer on the local network segment, the local computer might have an incorrect IP address or subnet mask. If the computer is not able to browse the network, the WINS IP addresses may be incorrect.

nslookup

The *nslookup* utility is used to diagnose problems related to the DNS services. In other words, it is used to resolve name resolution problems. This utility can be used to perform name resolution queries against a specified DNS server or to display information about currently configured DNS servers on a local host.

Unlike other commands discussed in this section, the *nslookup* command can be executed in either interactive mode or noninteractive mode as explained in the following paragraphs:

Non-interactive mode

The non-interactive mode is useful when you need to run the command with one or two pieces of information. For example, you can use the following command to resolve a specific hostname:

```
nslookup hostname
```

You can also specify a DNS server to resolve the hostname, as shown in the following example:

```
nslookup hostname -dns_server
```

If you do not specify the DNS server, the DNS server configured on the local host is used by default to resolve the query.

Interactive mode

In interactive mode, just type `nslookup` and press the Enter key. The command will display the information about the current hostname and the IP address of the configured DNS server along with a prompt. You can then enter other *nslookup* subcommands on this prompt. To exit the interactive mode, type `Exit` and press the Enter key.

The interactive mode includes a number of subcommands. On Windows systems, you can type ? at the interactive prompt to get more information on the syntax and usage of these. Table 8-25 lists some of the commonly used parameters and their functions.

Table 8-25. nslookup subcommands

Parameter	Function
`All`	Prints information about options, the current DNS server, and the host.
`[no]debug`	Prints debugging information.
`[no]d2`	Prints exhaustive debugging information.
`[no]defname`	Appends a domain name to each query.

Table 8-25. nslookup subcommands (continued)

Parameter	Function
`[no]recurse`	Asks for a recursive answer to each query.
`[no]search]`	Uses a domain search list.
`[no]vc`	Always uses a virtual circuit.
`domain=name`	Sets the default domain name to `name`.
`searchlist=N1[/N2/N3.../N6]`	Sets the domain to N1 and the search list to N1, N2, etc.
`root=name`	Sets the root server to `name`.
`Retry=x`	Sets the domain to N1.
`timeout=x`	Sets the initial timeout to x seconds.
`type=x`	Sets the query type (for example, A, ANY, CNAME, MX, NS, PTR, SOA, or SRV).
`querytype=x`	Same as `type`.
`server NAME`	Sets the server name to `name` using the current default server.
`Exit`	Exits the interactive mode.

The following example shows how the *nslookup* command can be used to resolve a hostname using the non-interactive mode:

```
C:\ >nslookup www.oreilly.com
Server:  localhost
Address:  192.168.1.1

Non-authoritative answer:
Name:    www.oreilly.com
Addresses:  208.201.239.36, 208.201.239.37
```

In case you need to resolve a hostname using a specific DNS server, you can use the following command instead:

```
C:\ >nslookup www.oreilly.com 192.168.1.5
```

You can also use *nslookup* to resolve IP addresses to hostnames, as shown in the following example.

```
C:\ >nslookup 208.201.239.36
Server:  localhost
Address:  192.168.1.1

Name:    www.oreillynet.com
Address:  208.201.239.36
```

The commands and parameters used in the *nslookup* utility are case-sensitive and must be typed in lowercase characters.

dig

The *dig* command is used on Unix/Linux and MAC OS X systems to perform DNS queries. It is more versatile than the *nslookup* command. This command does not work in interactive mode, and all command-line parameters have to be supplied at the main prompt. When used without any parameters, this command searches the root DNS server. The following is the basic syntax of a standard *dig* command:

```
dig @server name type
```

The following are standard parameters of the *dig* command:

Server
: Specifies the name of the DNS server to query.

Name
: Specifies the hostname to be resolved.

Type
: Specifies the type of query such as A, ANY, MX, etc. The default query type is A.

The *dig* command supports a number of options for extended functionality. These options are beyond the scope of the Network+ exam. The output of a standard *dig* query includes the following three main sections:

Query section
: This section displays the type and class of the DNS query.

Answer section
: This section displays the name of the host and its IP address for which the query is being performed.

Authority section
: This section displays information about authoritative DNS servers for the domain against which the query is performed.

In addition to the above sections, the output also includes information on the total time taken to resolve the query, the time when the query was resolved, and the size of the message.

Visual Indicators

When troubleshooting network connectivity problems, one of the easiest methods is to check the visual indicators on network devices. Almost every network device has some form of visual indicator that can help find out whether the device is working or not. Network interface cards, hubs, switches, and routers all have light emitting diodes (LEDs) that indicate whether the device is functioning properly or not.

Some network devices have LEDs that change color according to the condition of the device or of an interface of the device. For example, hubs and switches have LEDs on every port; the color of the LED on a port indicates the port's condition. Similarly, NICs have small LEDs that can be helpful in detecting the source of a connectivity problem.

The following list provides guidelines for diagnosing a connectivity problem depending on the status of the LED lights. Note that these status lights may vary from one manufacturer to another.

No light or yellow
: The device or the port is not in operation. It is either not connected or is faulty.

Solid green
: The device or port is connected, but there is no activity on the port.

Flashing green
: The device or the port is functioning properly. It is transmitting and receiving data as expected.

Flashing amber
: The network is congested and collisions are occurring on the network media.

Certain devices provide separate LEDs for power, activity, and network collisions. Each of these LEDs can be a good indicator of the connectivity problem. Depending on the type and vendor of the network device used, the documentation of the device may be very helpful in understanding the meaning of LED status lights.

Troubleshooting Remote Connectivity

Remote connectivity problems include problems with connecting to a corporate network using Remote Access Services, VPN, and the Internet. When resolving remote connectivity problems, you will need to make certain basic checks to identify the problem and then find an appropriate resolution. The issue might be due to physical connectivity, permissions, authentication, incorrect protocol settings, or some device such as the wireless router. A logical approach to resolving a given problem will lead you to find a suitable corrective action. In this section, I will discuss some basic problem areas related to remote access.

File and print permissions

The main purpose of remote access is to connect to the company network and get access to network resources. When the remote connection is established, users might need to access file and print services in order to continue with the work for which they have connected to a remote network. If users report problems accessing or using shared resources located on the company network, you should check that they have appropriate permissions on the specific resources. Even when the RAS server has granted access to the network, access to file and printing services may be restricted or may vary from one user to another.

Authentication failures

Every client/server network environment, including the RAS server, requires some form of authentication. In smaller networks, the RAS server itself is configured to grant remote access to clients. In larger networks however, special servers, such as the RADIUS server, are configured to process authentication requests from multiple remote access clients. If a single client is reporting a logon problem, you should make sure that the client is authorized to connect remotely to the network. If multiple remote users are complaining of logon problems, the problem might lie with the remote access server or the authentication server. Even when the remote clients are granted remote access, permissions on network resources such as files and folders may still be restricted and vary from one shared resource to another.

Protocol configuration

Problems related to RAS protocol configurations usually rest with client computers. On a typical TCP/IP network, you should make sure that all remote clients are using the correct IP address, default gateway, and DNS addresses. In large networks, a DHCP server usually assigns these settings to clients. In smaller networks, the RAS server itself may be configured to assign IP addresses to remote clients. Both the client and the server should support at least one common authentication protocol. You must also make sure that both ends are using similar settings for the authentication protocol. For example, if the RAS server is requesting an EAP-based authentication protocol and the client does not support it, communications between the client and the RAS server cannot be established.

Physical connectivity

Remote access connectivity problems start with physical connections involving dial-up modems, routers, cables, and connectors. Telephone lines, DSL modems, and broadband cable may also cause connectivity problems. The following is a list of some quick checks that you can make so you are able to identify the cause of the problem and take an appropriate corrective action:

Dial-up connections

- Make sure that there is a dial tone when you dial a number.
- Make sure that the correct number is being dialed.
- Make sure that the call-waiting feature is turned off. Call waiting causes dial-up connections to drop when a call is received.
- Make sure that the modem connections and settings are correct.
- Make sure that the correct username and password are used.
- If everything seems to be in order, call the ISP to find out whether the problem lies at the other end.

DSL

- Check that the DSL cables are connected properly to the DSL modem and the computer.
- Check to make sure that the network interface is using correct driver software.
- Check that the LED indicators on the DSL modem and the network interface are communicating.
- Make sure that the correct username and password are used.
- If everything seems to be in order, call the ISP to find out whether the problem lies at the other end.

Cable

- Check that the coaxial cable is properly attached to the cable modem, and that the modem is properly attached to the computer.
- Check to make sure that the network interface is using the correct driver software.
- Check that the LED indicators on the DSL modem and the network interface are communicating.
- Make sure that the correct username and password are used.
- If everything seems to be in order, call the ISP to find out whether the problem lies at the other end.

Wireless Internet access

- Check the connection status indicators on the wireless router.
- Check the physical connections of the wireless interface and wireless router.
- If the computer is experiencing intermittent connectivity problems, check that it is located within the range of the wireless router. If possible, move the computer a bit closer to the wireless router.

Troubleshooting Network Connectivity Problems

In this section, we will discuss issues related to network connectivity. Network connectivity is provided through several components of the network infrastructure. These components essentially include network services, devices, and media. We will also discuss how problems related to network topology can be resolved. Finally, we will take a look at the logical steps involved in identifying, isolating, and resolving a given network problem.

Troubleshooting network services

A network requires several services to function properly. These services are run on one or more network servers and include DNS, DHCP, and WINS. Network services are critical to the functioning of the entire network. Addition of, removal of, or changes made to these services have network-wide effects. You must understand how these services affect the network users if any change is made. In this section, we will discuss the effects of problems with network services.

Adding, removing, or modifying the DHCP service. The DHCP service is used to dynamically assign IP addresses and related configurations to TCP/IP hosts in a network. The addresses assigned by the DHCP server are valid for a certain period of time called a *lease*. When 50 percent of the lease period expires, the DHCP clients attempt to renew their lease with the DHCP server. When clients are added or removed from the network, the DHCP server takes care of IP address assignments.

When a DHCP client boots up for the first time, it searches for a DHCP server that can assign it an IP address configuration. Any available DHCP server can service the request. The network traffic generated by the DHCP clients and servers is negligible and is not of much concern. The longer the lease duration, the less

DHCP traffic is generated by clients. In other words, if network congestion is a problem, you might consider increasing the lease duration.

If a new DHCP server is added to the network, the DHCP clients might need to be reconfigured so that they contact the right DHCP server to obtain and renew their IP addresses. On the other hand, removing the DHCP server will affect almost every client in the network. Clients will not able to obtain or renew their IP addresses. This simply means that the clients will not be able to connect to the network. If it is a small network, the clients can be configured with static IP addresses. For a large network, you might have to make an alternate DHCP server available to continue normal network functions.

Adding, removing, or modifying the DNS service. The DNS service is used in a network to resolve hostnames to IP addresses. Users connect to remote hosts using their easy-to-remember names instead of IP addresses that are hard to remember. Without the DNS service, users may not be able to connect to the remote hosts using their names. For example, if a client is able to connect to a remote host using its IP address but not by using the hostname, there might be a problem with the DNS server.

On client computers, the DHCP server dynamically assigns the DNS configuration. It may also be entered manually on each computer. DNS resolutions can also be performed using a local text file named *HOSTS* that keeps a mapping of hostnames to IP addresses.

> Adding, removing, or making changes to the DNS server requires advanced skills. These skills depend on the network operating system being used on the network. As far as the Network+ exam is concerned, you must remember that unavailability of DNS service in the network mainly leads to name resolution problems.

Adding, removing, or modifying the WINS service. The WINS service is used to resolve NetBIOS names to IP addresses. The WINS service helps reduce broadcast traffic on networks that may cause network congestion. It is exclusively used in Windows networks where NetBIOS names are used. Every time a Windows client needs to connect to a remote computer or browse the network, the WINS server is contacted to resolve the computer name to its IP address.

If the WINS server is not available, the computer might attempt to resolve the computer names using the broadcast method. Network broadcasts are not preferred in large networks as they create significant network traffic and might cause network congestion. Besides this, most routers do not forward broadcast messages in order to prevent the local broadcast traffic to cross over to other network segments. It is important to note that the WINS service itself does not generate much network traffic but instead is helpful in reducing network traffic.

As an alternative to a WINS server, Windows client computers may also use a text file named *LMHOSTS* to resolve NetBIOS names. Windows client computers are dynamically configured with a preferred and alternate WINS server through the DHCP server. It is also possible to manually configure client computers with WINS addresses in small networks.

It is obvious that WINS is helpful in reducing network broadcast traffic. Before removing a WINS server from the network, you must either plan to install an alternate WINS server or configure the *LMHOSTS* file manually on each Windows client.

Troubleshooting physical topologies

When troubleshooting a network connectivity problem, the first thing you need to know is which network topology is in use. Depending on the topology, the troubleshooting methods will also vary. The following sections explain common troubleshooting methods for bus, star, ring, and mesh topologies.

Bus network. Networks with physical bus topology are hardly in use these days due to the popularity of twisted pair cabling and star topology. However, there are still chances that you will find quite a few old networks that use coaxial cable and bus topology. The following are some of the common points to remember when troubleshooting connectivity problems in a bus network:

- Breaks in coaxial cables are hardest to locate in a bus network. If the cable breaks, all computers will be disconnected from the network.
- The two ends of the bus network must be terminated with a 50-Ohm terminator. Even if one of the terminators is missing, the network segment will be down.
- One end of the bus network cable must be grounded. If the cable is not grounded, users will report intermittent connectivity problems.
- Addition or removal of computers from the bus network usually causes interruptions in network connectivity. When a computer is added or removed from the network, make sure that BNC T-connectors are properly attached.
- If the network interface on one of the computers in the network fails, it will also cause network failures.

Star network. Star topology is the most widely used network topology these days. In a star network, a central device called a hub or a switch provides a point-to-point connection to all devices in the network segment. The length of the cable used to connect a single device depends on the type of cable. The following are some of the common points to remember when troubleshooting connectivity problems in a star network:

- Hubs and switches have visual indicators (LEDs) to indicate the status of different ports. Depending on the make and model of the hub/switch, the light of the LED might be helpful to determine whether the problem is with one port or with all ports. LEDs can help you determine whether a port is connected or disconnected, or whether there are collisions on the media.
- Remember that in a star network, the hub or switch is the single point of failure. If several users on a network segment are reporting connectivity problems, you should check whether the hub or switch has failed.
- If only a single user is reporting a connectivity problem, you might have to trace the cable from his computer to the hub/switch and check the status indicator on that port. If it shows a disconnected cable, although it is

connected, the port may not be working or the cable may be faulty. First, try to plug the cable into a different port. If that does not help, try replacing the cable.

- Sometimes, a few new computers are added to a star network, but none of them can connect to the network. In such a situation, you should verify that correct cable type and length is used. Make sure that patch panels and patch cables are attached properly.

Ring network. Ring networks are, in fact, installed as physical star networks but function as a logical ring. Like the bus networks, ring networks are also hard to find these days. The central device used in ring networks is the Multi-Station Access Unit (MSAU), or the Media Access Unit (MAU). The cables in use may be fiber optic or twisted pair. The following are some of the common points to remember when troubleshooting connectivity problems in a ring network:

- The central device or the MSAU is a single point of failure in a ring network. If the MSAU is not working or if a single port on the MSAU is not working, all users on the network will report connectivity problems.
- When installing or replacing an MSAU, make sure that the Ring-In (RI) and Ring-Out (RO) are properly connected and configured.
- In order to have a completely working ring network, you must verify that all network interface cards are operating at the same speed.
- Verify that the cable used to connect network devices is not broken. If a single cable breaks, the ring will be broken and the network will be down.
- When adding or removing network cables and connectors, and when adding new workstations or printers, to a ring network make sure that the cables and connectors are of correct specifications.

Mesh network. A mesh network provides the best fault tolerance of all network topologies. Every device (computer or printer) is connected to every other device. Even if one or two cables are broken, an alternate connection is always available. Although a mesh network provides the best performance and fault tolerance, it may be the most difficult network to troubleshoot. This is due to the number of connections and the number of cables involved in setting up the network. Connectivity problems in a mesh network do not appear unless all connections to a device are broken. Mesh networks are rarely implemented in organizations these days due to the cost involved. This type of network is used only in areas of high availability.

Troubleshooting network infrastructure

The network infrastructure includes almost every component of the network. For example, hubs, switches, routers, cables, connectors, terminators, and wireless access points are all part of the network infrastructure. Although servers that provide network services such as DNS, WINS, DHCP, and RAS are also part of the network infrastructure, this section deals with troubleshooting only the physical components of the network. Given a network problem scenario, you must have a troubleshooting strategy in place.

Network media and devices. The cables and connectors used to interconnect network devices are often the cause of a network connectivity problem. Some of the key points to remember while troubleshooting network media are as follows:

Connectors

Troubleshooting bad connectors involves verifying that the correct type of connector is used and that it is properly attached. For example, in a bus network, a loose connector or a loose terminator may result in all users being unable to communicate on the network segment. For fiber optic cabling, you must ensure that devices and connectors are compatible with each other.

Cables

A correct cable type should be used. For example, if a crossover UTP cable is used where a straight cable is required, connectivity problems will arise. In a star network, a single broken cable usually affects only a single workstation.

Media range

Media range refers to the specified range of network cable or the range of a wireless access point. The total length of a cable used to connect devices must not exceed the specifications. Similarly, the wireless devices must be located within the range of the access point in wireless networks.

Wireless interferences

Wireless networks are susceptible to electromagnetic and radio frequency interferences (EMI and RFI). Wireless access points should not be located near areas of high interference.

Cable crosstalk

Unshielded twisted pair (UTP) cables are also prone to interference generated by crosstalk and electromagnetic interference. UTP cables should not be run in areas of high EMI, such as near transformers and beside high-voltage electric cables. For ceilings and ducts, a special type of cable known as *plenum-rated* cable must be used.

The following are some of the common problems with network devices:

Hubs

If a hub fails, all computers connected to the hub will experience connectivity problems. Check that the hub is powered on and try to resolve the problem by recycling the power. If the problem is not solved, you might have to replace the hub.

Switches

A failed switch results in connectivity problems to all the computers in the network segment. Check that the switch is powered on and try to resolve the problem by recycling the power. If the problem is not solved, you might have to replace the switch.

Bridges

Bridges are used to connect network segments. A failed bridge results in computers in one network segment being unable to connect to computers in another segment.

Routers

Routers are used to connect network segments, but the function of the router is much more advanced than the bridge. If a router fails, computers on one of the network segments will not be able to connect to any other network segment. If the router is connected to the Internet, then no one will be able to access the Internet. You can test the router connectivity using TCP/IP troubleshooting utilities such as *ping* or *tracert/traceroute*.

Wireless Access Points (WAPs)

WAPs are used to provide network connectivity to wireless clients. They are also used to connect the wired network to a wireless network. If all the users on the wireless network are experiencing connectivity problems, the WAP may not be working. You may need to recycle power on the WAP or replace it if it is faulty.

Wireless network. The following list provides a quick review of the factors that may affect the wireless networks:

Signal strength

Wireless signals degrade as they travel away from a wireless signal-generating device, such as the access point. This degradation or attenuation of signals is caused by several environmental factors, such as EMI, RFI, or walls. The weakening of wireless signals can be prevented, to some extent, by careful location of wireless antennae, the use of signal boosters, and correct placement of wireless access points. It is good to know the maximum range of the wireless access points used in the network.

Type of wireless standards

Wireless devices come in different makes and models and conform to several standards. You must make sure that the wireless devices—such as wireless routers, access points, and adapters—all support the standards used on the network. Incompatibility of wireless standards causes connectivity issues.

SSID settings

The Service Set Identifier (SSID) enables wireless clients to connect to a wireless access point and access network resources. If a wireless client is reporting connectivity problems, wireless configuration should be checked to make sure that the client is using the correct SSID. Remember that both the access point and the wireless client should be configured with the same SSID.

Authentication

In large corporate networks, security is a prime concern, and most administrators configure certain authentication mechanisms to prevent unauthorized access to confidential company data. If a user cannot log on to a wireless network, make sure that he has sufficient permissions to log on. Additionally, confirm that the encryption and authentication settings are configured correctly on his computer. Wireless networks use WEP protocol, which supports both 64- and 128-bit encryption. Make sure that the client is configured to use the correct WEP encryption standard.

Coverage of access point

Wireless access points are like hubs or switches for the wired network. They have a limited coverage area. All wireless clients must be located within the coverage area to properly transmit and receive signals. When troubleshooting wireless client problems, you should consider factors such as the distance of the wireless client from the access point and signal attenuation due to environmental factors. Wireless repeaters and signal boosters can be used for clients who are located in distant places.

Troubleshooting strategy

Troubleshooting network problems requires that you follow some basic logical steps. The troubleshooting process should start with identifying the problem symptoms, isolating the affected area, and so on. Following a logical procedure not only makes troubleshooting easy, but it also reduces the time it takes to resolve the problem.

The Network+ exam expects you to understand the following basic steps in resolving a network problem:

1. Identify the symptoms and potential causes.
2. Identify the affected area.
3. Establish what has changed.
4. Select the most probable cause.
5. Implement an action plan and solution, including potential affects.
6. Test the results.
7. Identify the results and effects of the solution.
8. Document the solution and process.

These steps are explained in the following sections.

> It is important that you memorize the steps given in this section to correctly answer questions related to network troubleshooting. You must be prepared to face one or two questions on the Network+ exam asking you to pick a correct step based on a given troubleshooting scenario. You may also be asked to select the correct order of actions to resolve a given problem.

Identify the symptoms and potential causes. The first step in troubleshooting is to identify the symptoms of the problem. This is critical and involves gathering related information. If a user has reported the problem, you might need to ask questions to identify the symptoms. In case the problem has occurred on an unattended desktop or server, the system event logs and error messages are very helpful. In any case, you will need to have a good understanding of the operating system in use. You will also need to show good communication skills when talking to the user about the problem. When you have gathered sufficient information, you may well have identified the symptoms of the problem.

Identify the affected area. Once you have identified the symptoms of the problem, it's time to check how many users have been affected. The problem may lie with a single computer affecting just one user, or it may be affecting several computers, a single network segment, or the entire network. Problems reported by a single user often end on a single desktop itself. You will need to verify exactly how many users and which network segments have been affected.

Establish what has changed. The next step is to check whether anything has been changed on the computer that is experiencing the problem. For example, a user may report a problem with connectivity to a mail server. You will need to check whether the user has made any changes to the email settings on his computer. Some problems start when a computer's network configuration is changed. Another potential reason for a problem could be that the user has installed new applications or a new service pack, hotfix, or an update.

Select the most probable cause. Based on the information you have gathered so far, you will certainly have identified one or more causes of the problem. You will now need to find out the most probable cause. This is usually done by the elimination process and short-listing the ones that seem to have caused the problem. The reason that does not seem to be logical is eliminated. This will lead you to identify the correct cause.

Implement an action plan and solution including potential effects. Once you have identified the reason behind the network problem, you need to decide on a corrective action. But before you do anything, you will need to find out what effects the corrective action might have on the network. For example, you might have to disconnect a critical server from the network or you might have to take it offline for necessary repairs. In such a situation, you will need to find out how this will affect network users. You might also have to report this to one of your senior administrators. Be prepared to state how long it will take to get the job done.

This is a critical step in network troubleshooting—applying your planning skills to resolve the problem as quickly and as effectively as possible. You might have to reinstall certain applications, apply a hotfix, or replace a faulty component in a server. In some situations, the problem might not be resolved with a single action. You must be careful to try just one solution at a time. For example, if you need to replace two defective parts in a server, replace one first and then replace the second.

Test the results. Once you have identified the effects of the corrective action you are going to take, you will need to test the results. Sometimes, one solution gives rise to another problem. In some cases, an incorrect solution leads to multiple problems. This is particularly important when the solution has to be applied to multiple computers on the network. For example, a small change in permissions on a mail server may result in several users complaining of "access denied" problems. Hence, it is important that you test the results of the solution thoroughly before you finally apply it.

Identify the results and effects of the solution. Once the solution has been applied, you will need to identify the results and effects of it. Sometimes, the solution will have a negative and cascading effect on other parts of the network. Some solutions cause multiple-layered problems. Actions such as adding or deleting users, changing permissions, and replacing critical network components such as a switch or a hub affect several users and multiple network segments. You must be able to foresee any possible problems that may occur due to the solution you have applied.

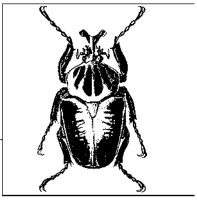
Document the solution and process. When the problem has been resolved and everything seems to be okay, you should create a document stating all the steps that you have taken to get to the final solution. The documentation is important because it may be referred to at a later date if the same or a similar problem occurs again. The documentation is also helpful in tracking down a person who resolved the problem.

The following are some of the important components of troubleshooting documentation:

- The date the problem occurred.
- Why did the problem occur? What were the symptoms?
- What was done to resolve the problem?
- What were the results or effects of the problem?
- Who resolved the problem and prepared the documentation?

9

Network+ Exam Prep and Practice



The material in this chapter is designed to help you prepare and practice for the Network+ Exam: N10-003. The chapter is organized into four sections:

Preparing for the Network+ Exam
: This section provides an overview of the types of questions on the exam. Reviewing this section will help you understand how the actual exam works.

Network+ Exam Suggested Exercises
: This section provides a numbered list of exercises that you can follow to gain experience in the exam's subject areas. Performing the exercises in this section will help ensure that you have hands-on experience with all areas of the exam.

Network+ Exam Highlighters Index
: This section compiles the facts within the exam's subject areas that you are most likely to need another look at—in other words, the areas of study that you might have highlighted while reading the Study Guide. Studying the highlights is useful as a final review before the exam.

Network+ Exam Practice Questions
: This section includes a comprehensive set of practice questions to assess your knowledge of the concepts. The questions are similar in format to the exam. After you've reviewed the Study Guide, performed the Suggested Exercises, and studied the Highlighters Index, read the questions and see whether you can answer them correctly.

Before you take the Network+ exam, you should read the exam overview, perform the suggested exercises, and go through the practice questions provided. Many online sites provide practice tests for the exam. Duplicating the depth and scope of these practice exams in a printed book is not possible. Visit CompTIA's certification web site for pointers to online practice tests (*http://certification.comptia.org/network*).

Preparing for the Network+ Exam

The Network+ exam is computer-generated. It is timed, and an onscreen timer clock displays the amount of time remaining on the exam. Most questions on the exam are multiple-choice. Multiple-choice questions are either:

Multiple-choice, single answer
A radio button allows you to select a single answer only.

Multiple-choice, multiple answer
Checkboxes allow you to select multiple answers. Usually the number of correct answers is indicated in the question itself.

CompTIA reserves the right to change the testing techniques at any time. It is recommended that you visit the CompTIA Network+ certification web site regularly to get updates on any changes in the exam format. Individuals with adequate hands-on experience who have reviewed the Study Guide, performed the practice exercises, memorized the essentials, and taken practice tests should do well on this type of exam. Individuals who lack adequate hands-on experience and have not prepared appropriately will find the exam hard to pass.

CompTIA suggests the following tips for taking the exam:

- Read the questions slowly and carefully.
- Do not expect to find clues in every question, though they may be present in some.
- Be aware of the distractions/confusions in statements. The first choice is often the best choice.
- Do not attempt to create situations based on a question. Your answer should be based on whatever information is provided.
- If you are retaking the exam, utilize your previous score report to concentrate on areas that need more study or practice.
- If you get stuck, mark and skip the question. You can do it later.

Typically, the test environment will have Previous/Next and Mark For Review options. You can navigate through the test using the Previous/Next buttons. You can click the Mark For Review checkbox to flag a question for later review.

Network+ Exam Suggested Exercises

The Network+ exam expects you to have a good understanding of concepts related to computer networks. Hands-on experience is recommended and is good to have. You should be very familiar with network terminology, protocols, and standards, and you should have basic troubleshooting skills. You will need to review the Study Guide and pay close attention to the areas that are new for you or that you feel uncomfortable with.

This section includes some exercises that you can perform either on a standalone computer or in a network to gain some hands-on experience. Since the Network+ exam mainly covers foundation-level knowledge of computer networking, you are not expected to know how to configure a particular type of hardware or an application. However, you must have essential basic knowledge, such as identification of network topology, cables, and connectors.

> It is recommended that you do not perform any of the suggested exercises in your organization or in any running computer network. Create a test environment consisting of two computers for completing these exercises. Even if you just want to view network settings in a production environment, make sure a senior administrator accompanies you. In any case, you should follow the policies of the organization.

Network Topologies

1. Check the local area network in your office.
2. Determine the type of network topology.
3. Draw a diagram of the network layout.

Network Media

1. Disconnect the network cable from your desktop.
2. Determine the type of cable used.
3. Determine the type of connector used.
4. Note the wire colors on both ends of an RJ-45 connector.

Wireless Network

1. Obtain a wireless router or access point.
2. Note the type of connections on the rear panel.
3. Determine whether it is only an access point or a router, or both.
4. Read the manual to find out its specifications.

Cable Types

1. Obtain small pieces of coaxial and UTP cables.
2. Strip the ends of cable and check the core and shield.
3. Count the number of wires in the UTP cable and find out its category number.
4. Obtain a fiber optic cable.
5. Determine how light passes from one end to another.

Media Devices

1. Access a working hub or a switch.
2. Determine the number of ports for connecting workstations.
3. Determine how the device is used to extend the network.

4. Check the types of indicators on the front panel.
5. Connect a new workstation to the hub or switch.

MAC Address

1. Log on to a Windows XP desktop.
2. Start the command prompt.
3. Run the *ipconfig /all* command.
4. Determine the MAC address of the network interface card.

Networking Protocols

1. Log on to a Windows XP desktop.
2. Determine the name of the desktop.
3. Open the properties of the Local Area Connection from the Control Panel.
4. Determine the network protocol in use.
5. Determine the types of services configured.

IP Addressing

1. Log on to a Windows XP desktop.
2. Open the properties of the Local Area Connection.
3. Determine whether the IP address is configured manually or automatically.
4. Determine the IP address and subnet mask.
5. Note the IP address of the default gateway.

TCP/IP Services

1. Log on to a Windows XP desktop.
2. Open the properties of the Local Area Connection.
3. Determine how the DNS and WINS servers are configured.
4. Connect to another computer using its IP address.
5. Connect to another computer using its computer name or hostname.

WAN and Internet Technologies

1. Find the type of WAN connection used on the network.
2. Determine the name of the Internet service provider or ISP.
3. Determine the total bandwidth available.
4. Determine how Internet access is provided to office users.
5. Check the total bandwidth available for Internet access.

Remote Access Protocols and Services

1. Log on to the remote access server in your office.
2. Determine the remote access protocol used.
3. Determine how the remote clients are authenticated.
4. Note the type of security protocol used for remote access.

Network Operating Systems

1. Log on to a Windows Server 2003 domain.
2. Connect to a file server.
3. Open the properties of a shared folder.
4. Determine the permissions assigned to users and groups.

Interoperability of Network Operating Systems

1. Log on to a Windows XP desktop.
2. Open the properties of the Local Area Connection.
3. Add Client Service for NetWare.
4. Add AppleTalk Protocol.

Network Wiring Tools

1. Obtain a piece of UTP cable and two RJ-45 connectors.
2. Obtain a wire-crimping tool.
3. Use the crimping tool to attach the connectors on both sides.
4. Test the cable by connecting it to a desktop and a hub.

Network Security

1. Determine whether a firewall or a proxy server is used on the network.
2. Check with your administrator on how the device is configured.
3. Note the port numbers or IP addresses that are blocked or allowed.
4. Try to connect to an external network using a blocked IP address.

Fault Tolerance

1. Log on to a file server.
2. Open the Disk Management application.
3. Determine what type of disk fault tolerance is in use.
4. Determine whether the RAID solution is software- or hardware-based.
5. Determine the total number of disks in the server and the available disk capacity.

Disaster Recovery

1. Log on to a backup server or have the backup operator help you.
2. Determine the type of backup used for critical data backups.
3. Determine how the backup tapes are labeled and where they are stored.
4. Perform a test restoration for a nonproduction file or folder.
5. Note the tape rotation scheme.

Troubleshooting Utilities

1. Log on to a Windows XP desktop.
2. Open the command prompt window.
3. Run the command *tracert www.comptia.org*
4. Read the output carefully.
5. Check whether there are any Request Timed Out messages.

Troubleshooting Network Connectivity

1. Remove the network cable from your desktop.
2. Open the command prompt window.
3. Run the command *ping 127.0.0.1* and notice the output.
4. Ping another computer on the network and note the results.
5. Ping the default gateway of the network segment.
6. Ping a remote computer.
7. Reconnect the cable and repeat the above ping commands.
8. Read the output carefully to interpret the messages.

Troubleshooting Network Devices

1. Remove the network cable from your desktop.
2. Go to the network hub or switch.
3. Note that the LED for the port is not glowing.
4. Check other ports and note the color of the LEDs.
5. Reconnect the network cable and again check the port status on the hub/switch.

Using the arp Command

1. Open the command prompt window on your desktop.
2. Run the command *arp –a*.
3. Note the entries in the ARP cache.
4. Run the command *arp –d* to clear the ARP cache.
5. Again run the command *arp –a* and note the output.

Using the netstat Command

1. Open the command prompt window on your desktop.
2. Run the command *netstat –s*.
3. Carefully read all parts of the output.
4. Try to interpret the statistics for different TCP/IP protocols.

Network+ Exam Highlighters Index

In this section, I've attempted to compile the facts within the exam's subject areas that you are most likely to need another look at—in other words, the areas of study that you might have highlighted while reading the Study Guide. The title of each highlighted element corresponds to the heading title in the Network+ Exam Study Guide, so, if you have a question about a highlight, you can easily refer back to the corresponding section in the Study Guide. For the most part, the entries under a heading are organized as term lists with main points that you need to memorize for the exam.

Media and Topologies

This subsection covers a summary of highlights from the "Media and Topologies" section in the Network+ Exam Study Guide.

Types of networks

- A local area network (LAN) connects computers in a single location.
- A wide area network (WAN) connects LANs at different geographical locations.
- A metropolitan area network (MAN) connects LANs in a campus or within a city.
- A personal area network (PAN) connects devices located in close proximity.

Centralized and decentralized computing

- In centralized computing, all processing is done on a single computer.
- A client/server model is an example of centralized computing.
- In decentralized computing, processing and resources are distributed on multiple computers.
- A peer-to-peer network is an example of decentralized processing.

Peer-to-peer network

- Every computer is responsible for processing and controlling access to its resources.
- These networks are suitable for only about 10 computers.
- They are cost-effective compared to the client/server model.
- No network operating system (NOS) needs to be installed on any computer.
- No administrator is required, and each user is responsible for managing resources on her computer.
- These networks are not considered secure because each user individually maintains resource security on her computer.

Client/server network

- A centralized server administers network resources.
- This model is scalable to very large-scale networks.
- Skilled administrators are required to manage the network.
- Dedicated server and network hardware may be required, which increases the cost of ownership.
- Resource security can be effectively maintained from a centralized point.

Star topology

- Computers are connected through a central device called a *hub* or a *switch*.
- A star network is easy to implement, troubleshoot, and expand.
- The failure of a single node or the connecting cable does not affect the network operation.
- The failure of the central device (hub or switch) can bring down the entire network.
- The length of cable required is much more than ring and bus networks.

Bus topology

- All computers are connected to a shared cable called a *trunk* or a *backbone*.
- Computers are connected to the backbone using T-connectors.
- Each end of the cable is terminated using 50-Ohm terminators.
- Bus is the cheapest of all topologies and does not require special configuration.
- It is easy to install, and no special equipment is needed for installation.
- It needs less cable length compared to other topologies.
- A break in a cable or a missing terminator can bring down the entire network.
- It is not possible to add or remove computers without disrupting the network.

Mesh topology

- Every computer is connected to every other computer.
- It is highly reliable because of redundant multiple connections.
- Computers can be added or removed without affecting the network.
- It is difficult to install and troubleshoot.
- It is very expensive because of the length of cable required to make multiple redundant connections.

Ring topology

- Each computer is connected to its neighboring computer to form a logical ring.
- A Multi-Station Access Unit (MSAU or MAU) acts as the central device or hub.
- A special data packet called a *Token* circulates around the ring.
- The MSAU has Ring In (RI) and Ring Out (RO) ports to connect the MSAUs.
- A ring network is relatively easy to install but difficult to troubleshoot.

- A break in the cable or a faulty computer can bring down the entire network.
- The addition or removal of computers can disrupt network operation.

Wireless topologies

- Ad-hoc networks provide the fastest way to connect wireless computers.
- In ad-hoc mode, two or more wireless computers communicate without using a central device.
- Infrastructure wireless networks use an access point to communicate.
- Access points also connect wireless segments to wired segments.
- SSID must be configured on the access point and on all wireless computers.

Networking standards

- The IEEE has defined networking standards.
- The IEEE 802 standards describe networking protocols, services, devices, and media.

IEEE 802.3

- The original IEEE 802.3 Ethernet standard defined a speed of 10 Mbps over thin coaxial cable.
- The Fast Ethernet standard 802.3u defines the speed up to 100 Mbps.
- The Gigabit Ethernet standard 802.3z defines the speed up to 1000 Mbps.
- The access method defines how devices access network media.
- Ethernet networks use the Carrier Sense Multiple Access/Collision Detection (CSMA/CD) method.
- If a collision is detected, the sending device waits for a specified time.
- Most Ethernet networks use the star topology.
- IEEE 802.3x standards define a variety of cable media including coaxial, twisted pair, and fiber optic.

IEEE 802.5

- The IEEE 802.5 defines standards for Token Ring networks.
- The transfer speed of IEEE 802.5 Token Ring networks is 4 and 16 Mbps.
- Token Ring networks use the Token Passing access method.
- The physical setup of a Token Ring network is the star topology, while the logical setup is in a ring topology.
- An MSAU, or MAU, is used to create a physical star topology.
- Unshielded twisted pair (UTP) and shielded twisted pair (STP) cables are used as media.

IEEE 802.11

- The IEEE 802.11 standards define protocols for wireless communications.
- The data transfer speed defined in the legacy 802.11 standard was limited to 1 or 2 Mbps within the frequency range of 2.4 GHz.
- 802.11 networks use Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA).

- Wireless networks can use either ad-hoc or infrastructure topology.
- IEEE 802.11 networks use radio frequencies with spread spectrum technology.
- Spread spectrum technology is of two types: Frequency-hopping spread spectrum (FHSS) and Direct-sequence spread spectrum (DSSS).
- The IEEE 802.11b devices use a 2.4 GHz frequency range and an 11 Mbps data transfer speed.
- The IEEE 802.11a devices use a 5 GHz frequency range and a 54 Mbps data transfer speed.
- The IEEE 802.11g devices use a 2.4 GHz frequency range and a 54 Mbps data transfer speed.
- The 802.11b and 802.11g devices are susceptible to interferences.

Fiber Distributed Data Interface (FDDI)

- FDDI is based on Token Ring topology.
- It uses fiber optic cables, and cable segments can be reach up to 200 Km.
- It uses dual rings in order to provide fault tolerance.
- The maximum data transfer speed is 100 Mbps.
- The devices use the token-passing method to access network media.

Coaxial cable

- The thin coaxial cable (thinnet) used for computer networks is RG-58.
- Thinnet has 50-Ohm resistance and uses 50-Ohm terminators.
- Devices are connected using BNC-T connectors.
- The thick coaxial cable (thicknet) is RG-8 cable and is used for backbones.
- Thicknet uses vampire taps and 15-pin AUI connectors.

Twisted pair cables

- These cables use twisted pairs of insulated wires inside a plastic sheath.
- The twists in cables are used to prevent electromagnetic interference, which is called *crosstalk*.
- Twisted pair cables have category numbers.
- Unshielded twisted pair (UTP) cables are the most commonly used of the two types of twisted pair cable categories.
- Shielded twisted pair (STP) cables have shielding material between the cables and the sheath.
- STP cables provide protection from electromagnetic and radio frequency interferences (EMI and RFI).
- STP cables can carry signals to greater distances than UTP cables.
- Refer to Table 8-3 in Chapter 8 for a list of common twisted pair cables.

Fiber optic cables

- A fiber optic cable is made up of thin glass or plastic and put inside a sheath.
- The transmission is based on the transport of light signals.
- Fiber optic cables are immune to EMI and RFI disturbances.

- These cables are expensive in terms of cost, installation, and maintenance.
- A single-mode fiber optic cable uses 8 to 10 micron core and 125 micron cladding.
- A fiber optic cable uses a single beam of light.
- The multimode fiber optic cable is made up of 50 micron or 62.5 micron core and 125 micron cladding.
- Multiple beams of light travel through the core and are reflected by the cladding.
- Single-mode fiber cables can travel to greater distances than multimode fiber cables.

10 Mbps Ethernet

- The 10 Mbps standards include 10Base2, 10BaseT, and 10BaseFL.
- Most modern networks support 100 Mbps speeds, which provide better bandwidth.
- The 1000 Mbps (1 Gigabit) Ethernet networks are also known as Gigabit Ethernet.
- The 10 Gigabit Ethernet networks support a maximum data transfer speed of 10,000 Mbps.

Media connectors

- The RJ-11 connector is used for terminating telephone wires.
- The RJ-45 connector is used for terminating twisted pair cables.
- The F-Type connector is used to terminate RG/6 and RG/59 cable TV coaxial cables.
- BNC connectors are used for terminating computer coaxial cables and include T-Connectors, Barrel Connectors, and Terminators.
- FC, SC, ST, LC and MT-RJ connectors are used for fiber optic cables.
- The IEEE 1394 (FireWire) interface is used for high-bandwidth applications such as digital video and portable storage.
- The USB Type A connector is used for computers, and the Type B connectors are used for peripherals.

Hubs

- A hub or a concentrator is the central device that connects all nodes in the segment.
- It is also known as a *multiport repeater*.
- It works at the physical layer of the OSI model.
- An active hub regenerates signals before passing them on to all other ports.
- A passive hub does not regenerate signals before relaying them.

Switch

- A switch is also the central device that connects multiple nodes in a network.
- A switch sends the signal only to the destination node.
- It works at the Data Link layer of the OSI networking model.

- Switches use the MAC address of devices to forward data.
- Switches use cut-through, store and forward, and fragment-free switching techniques.

Bridge

- A bridge connects LAN segments to form a larger segment.
- It can also divide a large network segment into smaller segments.
- It works at the Data Link layer of the OSI model.
- A transparent bridge forwards data by reading the destination MAC address.
- Source route bridges are used in Token Ring networks.
- A translation bridge connects two network segments that use different Data Link layer protocols.
- Bridges use the spanning tree protocol to overcome the bridging loops problem.

Router

- Routers are used to connect two or more network segments.
- They work at the Network layer of the OSI model.
- Routers use IP addresses to determine the source and destination of the data packet.
- They maintain a list of IP addresses in routing tables.
- When static routing is used, administrators manually configure routing tables.
- Dynamic routing protocols enable routers to dynamically build routing tables.

Distance vector routing protocol

- Routers using this protocol depend on other routers to advertise their routing tables every 30 seconds.
- RIPv1 and RIPv2 are distance vector protocols that work on the basis of hop count.
- A destination beyond 15 hops is considered unreachable.
- Periodic updates generate considerable network traffic.
- Routing loops are created when routers advertise incorrect routing information.
- Split horizon and poison reverse methods are used to prevent routing loops.

Link state routing protocol

- Routers using this protocol use Link State Advertisements (LSA) to update routing tables.
- OSPF and NLSP are examples of link state routing protocols.
- The link state routing protocols are best suited for large networks.

Gateway

- A gateway is a device that translates one format of data packets to another.
- They are also called protocol translators.
- Gateways convert only data formats; the data itself remains unchanged.

CSU/DSU

- A digital interface connects a local area network to a wide area network.
- Most new routers include CSU/DSU functionality.

Network interface card

- An NIC is a hardware device that connects a computer to the network.
- It works at the Data Link layer of the OSI model.
- Every network card comes with a device driver that needs to be installed.

ISDN adapter

- An ISDN adapter is also called a terminal adapter or ISDN modem.
- It connects a computer to the ISDN network.
- ISDN adapters can be installed on an expansion slot or can be connected externally to a computer's serial port.

WAP

- A wireless Access Point (WAP) connects wireless devices to form a network.
- It also connects a wired network to a wireless network.
- A WAP's signal range depends on the wireless standard used.

Modem

- A modem is used to convert a computer's digital signals to analog signals.
- It can be installed as an extension card or can be an external device.
- Modems must be configured to use system resources such as an I/O address or IRQ.
- Serial port modems use COM ports in a computer.

Firewalls

- A firewall protects the network from unauthorized external access.
- Firewalls are configured with rules to allow or block network traffic.
- Software-based firewalls are a built-in feature of many network operating systems.
- Hardware-based firewalls are dedicated devices or built into other devices, such as routers.

Spread spectrum wireless technology

- The spread spectrum technology shares available bandwidth.
- It prevents the jamming of signals due to interference from other sources.
- It uses a spectrum of frequencies instead of a fixed frequency.
- Each narrow band of frequencies contains only a part of the signal.
- FHSS uses 83.5 Mhz frequency range and is resistant to noise and interference.
- FHSS transmission speed ranges from 1.6 to 10 Mbps.
- DSSS divides the signal into smaller parts that are transmitted simultaneously on as many frequencies as possible.
- DSSS adds redundant bits of data known as chips.

- It utilizes a frequency range from 2.4 to 2.4835 GHz.
- DSSS and FHSS technologies are used in 802.11 networks.

Infrared

- Infrared supports point-to-point wireless communications between two devices.
- Infrared transmission uses a direct line of sight.
- Infrared waves cannot penetrate walls.
- Infrared supports data transfer speeds ranging from 10 to 16 Mbps.
- Infrared frequencies do not interfere with radio frequencies.
- Infrared provides a secure wireless communication usually limited to 3 to 12 feet.

Bluetooth

- Bluetooth supports transmission speeds from 1 to 3 Mbps.
- It works over the unlicensed frequency range of 2.4 GHz.
- The devices must be within a short range of less than 10 meters.
- Bluetooth offers high resistance to electromagnetic interference.
- It does not require a direct line of sight.

Factors affecting wireless signals

- Physical objects such as buildings, trees, concrete, and steel walls can reduce or block signals.
- EMI generated by high-power electric lines, power transformers, heavy electrical machinery, fans, light fixtures, and so on can cause disturbances.
- RFI generated by other wireless equipment causes disturbances.
- The type of antenna used can impact the signal strength.
- Environmental factors such as weather can reduce wireless signals.

Protocols and Standards

This subsection covers a summary of highlights from the "Protocols and Standards" section in the Network+ Exam Study Guide.

MAC address

- This is a unique 48-bit (6 bytes) hardware address that is hardcoded into most networking devices.
- The Data Link layer manages MAC addresses.
- The numbers and letters used in a MAC address include 0 to 9 and A to F respectively.
- The address is written as hexadecimal numbers in six groups of 2 bytes each, separated by colons (:) or hyphens (-).
- `02-25-4F-89-AE-48` is an example of a MAC address.
- The Address Resolution Protocol is used to translate IP addresses to MAC addresses.

OSI networking model

- The OSI networking model has seven layers.
- The OSI model layers are Application, Presentation, Session, Transport, Network, Data Link, and Physical.
- The Data Link layer (Layer 2) consists of a Logical Link layer (LLC) and Media Access Control (MAC) sublayers.

NetBEUI

- NetBEUI is used in small Microsoft networks.
- It is not routable and cannot be used on large networks.
- It uses NetBIOS naming conventions.
- NetBIOS computer names consist of a maximum of 15 characters.
- NetBIOS name resolution mainly depends on broadcasts.

Internet Packet Exchange/Sequenced Packet Exchange (IPX/SPX) protocol suite

- IPX/SPX is a fully routable protocol suite used in Novell NetWare networks.
- The Service Advertising Protocol (SAP) allows systems to advertise their services.
- The NetWare Core Protocol (NCP) allows client/server interactions such as file and print sharing.
- IPX provides network addressing and routing services.
- SPX provides connection-oriented services for IPX.
- The Routing Information Protocol (RIP) is the default routing protocol for IPX/SPX networks.
- The NetWare Link Services Protocol (NLSP) provides routing services based on the link state algorithm.
- The Open Datalink Interface (ODI) allows NetWare systems to work with any network interface card.

NetWare hostnames

- Only the servers are assigned hostnames (with a maximum of 47 characters).
- NetWare clients do not have hostnames.
- Clients use their IPX addresses instead.

IPX addresses

- NetWare networks are assigned a 32-bit hexadecimal address.
- The servers and workstations use a 48-bit hexadecimal address.
- These addresses default to the MAC address of the network interface card.
- The node address is appended to the network address to make it unique.
- `0AC74E02:02254F89AE48` is an example of an IPX address.

AppleTalk

- The AppleTalk protocol suite is used to interconnect Apple computers.
- AppleShare provides file- and printer-sharing services.

- The AppleTalk Filing Protocol (AFP) manages file sharing between AppleTalk hosts. It is also called the Apple Filing Protocol.
- The AppleTalk Data Stream Protocol (ADSP) is used for setting up communications.
- The Zone Information Protocol (ZIP) is used to divide an AppleTalk network into zones.
- The AppleTalk Session Protocol (ASP) is used to establish and terminate connections.
- The Printer Access Protocol (PAP) provides printing services.
- The AppleTalk Address Resolution Protocol (AARP) resolves AppleTalk addresses to Ethernet or Token Ring addresses.
- The Datagram Delivery Protocol (DDP) provides routing functions.
- The AppleTalk Transaction Protocol (ATP) provides a connectionless session.
- The Name Binding Protocol (NBP) maps AppleTalk hostnames to network layer addresses.
- The Routing Table Maintenance Protocol (RTMP) is used to maintain routing tables.
- The EtherTalk Link Access Protocol (ELAP) provides compatibility with Ethernet protocol.
- The TokenTalk Link Access Protocol (TLAP) provides compatibility with the Token Ring protocol.

AppleTalk addressing and naming

- An AppleTalk host address consists of 24-bits expressed in decimal format.
- An administrator assigns 16-bit addresses to the network.
- The 8-bit host address is an automatically generated random number.
- An example of an AppleTalk address is 5.48, where 5 is the network address and 48 is the host address.

TCP/IP addressing

- Hosts in a TCP/IP network follow IP addressing schemes.
- The IP address consists of 32 bits: four sets of 8 bytes (octet) each.
- It is expressed as four decimal numbers separated by dots.
- A second 32-bit number, known as a *subnet mask*, is used to identify the network address from the host address.

TCP/IP naming

- Hosts can be identified either by their IP addresses or by their hostnames.
- A Domain Name System (DNS) server translates IP addresses to hostnames.
- A text file named *HOSTS* can also be used for name resolution.

IPv4 addressing

- An IP address is a unique address that identifies a host on the network.
- A part of the IP address is known as the network address and the rest is known as the host address.

- The subnet mask identifies the network portion of the address.
- The default gateway allows computers to communicate with computers on another network segment.
- IPv4 addresses are classified into classes A, B, C, D, and E.
- Address 127.0.0.1 is reserved and used as a loopback address for troubleshooting.

Private and public IP addresses

- Private IP addresses are used when an organization's computer network is private and is not publicly accessible.
- Public IP addresses are addresses of those networks that are accessible from outside the organization.

Subnetting

- Subnetting creates multiple network segments by using the host portion of the IP address.
- It creates multiple broadcast domains and reduces broadcast traffic.
- It increases security and helps contain network traffic to local segments.
- It increases the number of subnets, but the number of hosts per segment decreases.

IPv6 addressing

- IPv6 uses a 128-bit address.
- An IPv6 address has two parts: a 64-bit network prefix and a 64-bit host address.
- It is written as eight groups of four hexadecimal digits separated by colons.
- `2001:0db8:85a3:08d3:1319:8a2e:0370:7334` is an example of IPv6 address.

IP address assignment

- IP addresses can be assigned statically or dynamically.
- Static IP addresses are configured manually.
- Static assignment is not suitable for large networks.
- IP addresses are assigned dynamically by a DHCP server.
- The DHCP server is configured with address scopes for each network segment.
- This prevents typing errors and duplicate addresses.
- IP addresses are assigned for a specific period of time known as a *lease*.
- Client must renew their IP addresses when 50 percent of the lease period expires.

Automatic Private IP Addressing (APIPA)

- The APIPA address range is from 169.254.0.1 to 169.254.255.254 with a subnet mask of 255.255.0.0.
- It is supported on computers configured to obtain IP addresses automatically.
- APIPA is configured when the computer does not find a DHCP server.

TCP/IP protocol suite

- TCP is a connection-oriented protocol and provides guaranteed delivery, flow control, error detection, error correction, and packet sequencing.
- IP is a connection-less protocol and provides IP addressing and routing functions.
- UDP is a connection-less protocol and is faster than TCP but does not provide guaranteed delivery of data.
- FTP provides file transfer functions between remote computers.
- FTP uses several commands for file transfers, as listed in Table 8-13 in Chapter 8.
- SFTP is the secure version of FTP.
- TFTP is also an application-layer protocol used to transfer files between two remote computers.
- SMTP is used to transport messages between remote email servers.
- HTTP allows text, images, and multimedia to be downloaded from web sites.
- HTTPS is the secure version of HTTP that allows servers and clients to be authenticated before the communication session starts.
- POP3 is used to download or retrieve email messages from mail servers running the SMTP protocol.
- IMAP4 is also used to retrieve email from mail servers and also provides a secure authentication mechanism.
- Telnet is an Application layer protocol that allows administrative connections to remote hosts.
- SSH is the secure alternative to connecting to remote systems or devices instead of using Telnet.
- ICMP works at the Network layer to provide error checking and reporting functions.
- ARP works at the Network layer to resolve IP addresses to MAC addresses.
- RARP is used to obtain the IP address of a host whose MAC address is known.
- NTP is used to exchange time information between TCP/IP hosts.
- NNTP provides newsgroup services such as posting and retrieving messages on discussion forums.
- SCP enables secure copying of files from Unix/Linux systems.
- LDAP enables users to access and query directory services.
- IGMP is used to register and discover network devices in a multicasting group.
- LPR provides client connectivity to printers in all major network operating systems such as Unix/Linux and Windows.
- A Line Printer Daemon (LPD) is a server component that accepts client print requests that are sent using the LPR application.

Port assignments in TCP/IP

- Every application, service, or protocol in the TCP/IP suite has a specific port number assigned to it.
- Well-known port numbers range from 0 to 1,023.
- User ports (registered ports) range from 1,024 to 46,151.
- Dynamic/private ports range from 46,152 or 65,535.

Domain Name System (DNS)

- The DNS service is used to resolve hostnames to IP addresses.
- A DNS server maintains a database of hostnames and their IP addresses.
- Hostnames on the Internet or large networks are also known as Fully Qualified Domain Names (FQDN).
- DNS is used on all major network operating systems.
- A local *HOSTS* file can also be used to resolve hostnames to IP addresses.

Windows Internet Name System (WINS)

- The WINS service is used to resolve NetBIOS names to IP addresses.
- It is used exclusively in Windows networks.
- A WINS server maintains a database of NetBIOS names and IP addresses.
- The *LMHOSTS* file can also be used to resolve NetBIOS names.

Network Address Translation (NAT)

- NAT is a cost-effective way to share a single Internet connection.
- It provides security for the private network by hiding the internal IP addressing scheme.
- It is scalable because more than one public IP address can be used.
- NAT allows the use of DNS and DHCP servers inside the network.
- NAT makes it possible to host web and email services from a private network.

Internet Connection Sharing (ICS)

- ICS is used to share an Internet connection in small networks that are not segmented.
- All internal clients are configured with class C IP addresses in the 192.168.0.1 range.
- It does not provide any security for the internal network.

Simple Network Management Protocol (SNMP)

- SNMP is used to monitor and manage the network devices.
- A centralized server known as the SNMP Manager maintains information in the Management Information Base (MIB).
- SNMP-enabled devices run a management application called an *SNMP agent*.
- The SNMP agent sends messages known as SNMP traps to the SNMP server.

Zero Configuration (ZeroConf)

- ZeroConf enables devices to communicate without any special configuration.
- The device must support Automatic Private IP Addressing (APIPA).
- The device must also be capable of resolving hostnames, it must advertise its services on the network, and it must be able to discover other services in the network.

Packet switching

- In packet-switched networks, the data is split into small segments known as *packets*.
- Packets are routed on different routes.
- The route selected for each packet is often the shortest route.
- The packets are reconstructed at the destination.

Circuit switching

- In circuit-switched networks, a dedicated physical circuit is established.
- Circuit switching provides a reliable connection and guaranteed speed of data transmission.
- The Plain Old Telephone Service (POTS) and Integrated Services Digital Network (ISDN) are examples of circuit-switched networks.

Integrated Services Digital Network (ISDN)

- ISDN requires dedicated telephone lines called *leased lines*.
- ISDN allows transmission of data and voice over leased telephone lines.
- Computers using the ISDN line need to be connected through an ISDN adapter.
- BRI ISDN uses 2 B channels of 64 Kbps each for data/voice, and one D channel of 16 Kbps with a total data transfer speed of 128 Kbps.
- PRI ISDN uses 23 B channels of 64 Kbps each for data/voice, and a D channel of 64 Kbps with a total data transfer speed of 1.544 Mbps.

Fiber Distributed Data Interface (FDDI)

- FDDI is based on the Token Ring and uses the token passing media access method.
- It uses two rings for providing fault tolerance.
- It is resistant to EMI and RFI.
- Fiber optic cables can have a maximum distance of 200 kilometers.
- It has a built-in error detection mechanism known as *beaconing*.
- It is very expensive in terms of the cost associated with devices and media.

T-Carrier

- The T-carrier lines are high-speed dedicated lines that can carry both data and voice.
- The E-carriers are used in Europe.
- The J-carries are used in Japan.

Optical Carrier (OC)

- Optical Carrier (OC) levels describe the range of digital signals that can be carried over SONET.
- OC levels are expressed as OC-x.
- The number *x* is multiplied by 51.84 Mbps to obtain the transmission speed.

X.25

- X.25 is a packet-switching WAN technology.
- It uses telephone or ISDN hardware.
- It has a maximum data transfer speed of 56 Kbps.
- Each end of the connection is attached to a packet assembler/disassembler (PAD).

Digital Subscriber Line (DSL)

- DSL uses ordinary analog telephone lines to provide digital data transmissions.
- ADSL download speeds are faster than upload speeds.
- SDSL supports equal speeds for both data uploads and downloads.
- IDSL is symmetric DSL and is used where ADSL and SDSL are not available.
- RADSL is asymmetric DSL that can vary the transfer speeds depending on line conditions.
- HDSL is a variation of asymmetric DSL that uses twisted copper wires.
- VHDSL is a symmetric variation that supports high-speed transmissions.

Broadband cable

- Broadband Internet access is mostly provided by the cable companies.
- A cable modem is used to connect computers to a cable.
- Most cable modems support bandwidths from 1.5 to 3 Mbps.
- Broadband cable provides a consistent connection.

Remote Access Service (RAS)

- RAS is Microsoft's implementation of remote access protocols and standards.
- A RAS server provides connectivity to remote clients.
- The RAS server authenticates the remote clients.

Virtual Private Networking (VPN)

- VPN provides a secure means of communication for remote users of an organization.
- A VPN Client is the remote user who wants to establish a connection to the organization's network.
- A VPN Server is a server running remote access service and authenticates connection requests from the remote client.
- Carrier Protocols are used to transfer data from one point to another over the Internet.
- Encapsulating Protocols (tunneling protocols) are used to wrap the original data before it is transmitted over the Internet.

- PPTP, L2TP, IPSec, and Secure Shell (SSH) are examples of Encapsulating Protocols.
- Remote Access VPN provides remote access to remote users over the Internet.
- Site-to-Site VPN provides a secure connection between different sites of the same organization.

IP Security (IPSec)

- IPSec is used to secure Internet Protocol (IP) communications by encrypting and authenticating each IP packet.
- The Authentication header signs each IP packet to maintain its authenticity and integrity.
- Encapsulating Security Payload adds confidentiality to the data.
- In transport mode, only the data inside the IP packet is encrypted.
- In tunnel mode, the entire IP packet is encrypted.

IPSec authentication

- IPSec uses Internet key exchange (IKE) to authenticate the sender and recipient.
- Shared secret keys are exchanged securely before the transmission starts.
- Both ends use a password known as a *preshared key*.
- IPSec can also be used for digital signatures or certificates.
- Digital certificates provide authenticity and non-repudiation.

Point-to-Point Tunneling Protocol (PPTP)

- PPTP is a tunneling protocol used to implement VPNs.
- PPTP uses TCP port 1723.
- It is used in Windows networks with Microsoft Point-to-Point Encryption (MPPE).
- It cannot be used if the RAS servers are located behind a firewall.
- It works only in IP networks.
- When used alone, PPTP does not provide encryption for authentication data.
- It does not provide centralized authentication.

Layer 2 Tunneling Protocol (L2TP)

- L2TP uses UDP port 1701 and is more secure than PPTP.
- A combination of L2TP and IPSec is used to provide secure transmissions for VPN connections.
- L2TP/IPSec can be used behind firewalls.
- L2TP/IPSec requires two levels of authentication: computer and user.
- L2TP/IPSec supports the use of RADIUS and TACACS+ for centralized authentication.

  L2TP/IPSec can be used with IP, IPX, and SNA.

Secure Socket Layer (SSL)

- SSL encryption is used for Internet-based transactions.
- It is based on public key encryption mechanisms.

- It provides end-to-end security for Internet communications by using encryption.
- A Public Key Infrastructure (PKI) is required for end-to-end security using SSL.

Wired Equivalent Privacy (WEP)

- WEP is a security protocol used for IEEE 802.11 wireless networks.
- It is designed to provide privacy (confidentiality) to a wired network.
- A WEP-enabled client adds a 40-bit secret key to the data.
- The data is decrypted using the secret key on the receiving end to recover the plain text.
- The newer version of WEP uses 128-bit encryption keys.

Wi-Fi Protected Access (WPA)

- WPA overcomes many weaknesses found in WEP.
- It uses large encryption keys.
- It provides enhanced data encryption security by using a Temporal Key Integrity Protocol (TKIP).
- It uses several variations of Extensible Authentication Protocol (EAP) and public key cryptography.
- WPA can be used in a preshared key mode.
- Each user must know and use a paraphrase to access the wireless network.

802.1x

- 802.1x is a secure authentication protocol that provides port-based access control.
- It is based on Extensible Authentication Protocol (EAP).
- *Supplicant* refers to the client software that needs access to a wireless access point.
- *Authenticator* refers to a centralized wireless access point that forwards authentication requests to an authentication server such as a RADIUS server.

Authentication protocols

- Authentication is the process of verifying the credentials of a user.
- Challenge Handshake Authentication Protocol (CHAP) periodically verifies the identity of the user.
- Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) is a password-based authentication mechanism.
- Password Authentication Protocol (PAP) is the most basic form of authentication in which the username and password are transmitted in clear text.
- Extensible Authentication Protocol (EAP) is the most secure of all authentication mechanisms.
- Shiva Password Authentication Protocol (SPAP) is used for authentication to Shiva remote access servers.

Remote Authentication Dial-in User Service (RADIUS)

- The RADIUS server provides centralized authentication for remote users.
- RADIUS servers support several popular protocols such as PAP, CHAP, MS-CHAP, EAP, and SPAP.
- Large organizations use multiple RADIUS servers to distribute the authentication load.

Kerberos

- Kerberos is a cross-platform authentication protocol.
- It is used for mutual authentication of users and services.
- It requires a trusted third party.
- It works in a Key Distribution Center (KDC), which is used to issue secure encrypted keys and tokens.
- The tickets carry a timestamp and expire as soon as the user or the service logs off.
- Kerberos is dependent on synchronization of clocks on the clients and servers.

Network Implementation

This subsection covers a summary of highlights from the "Network Implementation" section in the Network+ Exam Study Guide.

Linux/Unix

- Linux is an open source operating system and is freely distributed.
- Users must supply a username and password to log on.
- Linux uses the Network File System (NFS) and Virtual File System (VFS) to mange files and folders.
- The Line Printer Daemon (LPD) provides printing services.
- Most server applications are third-party applications.
- Each object has an associated Access Control List (ACL).
- Linux ACLs are stored in text files such as *hosts.allow* and *hosts.deny*.

MAC OS X

- MAC OS X is designed for Apple computers.
- User authentication is provided through user accounts.
- *Limited*, *standard*, and *administrator* are three types of accounts.
- MAC OS X supports Hierarchical File System Plus (HFS+).
- Each file or folder in MAC OS X has associated sets of permissions.

NetWare

- NetWare is a full-featured network operating system.
- Several network services such as DHCP, DNS, Web, and FTP are built-in.
- NetWare also requires users to provide credentials such as username, password, Directory Context, and the name of the directory tree.

- The NetWare filesystem provides users access to hard disk partitions, known as *volumes*.
- NetWare supports Novell Distributed Print Services (NDPS) for printing.
- Access to resources in NetWare is controlled through NetWare Directory Services.

Windows 2000 Server and Windows Server 2003

- Windows 2000 Server and Windows Server 2003 are based on Active Directory.
- Active Directory is a centralized database that stores information about all objects.
- Servers running Active Directory services are called *domain controllers*.
- Objects include computers, users, groups, file shares, and printers.
- Windows networks operate in domains.
- Administrators apply group policies to domains or Organizational Units (OUs).
- Users are required to log on to the domain once only, upon which they are permitted access to objects listed within Active Directory.
- Windows servers use Kerberos authentication protocol by default.
- File and Print Sharing for Microsoft Networks provides file and print services.
- Windows servers provide file- and folder-level security using the NT File System (NTFS).
- Files can be stored and transmitted over the network in encrypted form.
- IP Security (IPSec) can be used for secure data transmission of data in the LAN or over a WAN.

Network wiring tools

- A wire crimper is used to cut cable to length and attach a suitable connector.
- A punchdown tool is used to attach wires to a patch panel.
- Media testers or cable testers are used to test whether the cable is working properly.
- An Optical Time Domain Reflectometer (OTDR) is used to locate breaks in fiber optic cables.
- Tone generators and tone locators are used to find cable faults using audio signals.

  Loopback connectors/adapters are used to test the functionality of network ports.

Firewalls

- A firewall protects the internal network from outside networks.
- Packet-filtering firewalls inspect the contents of each IP packet.
- Packet-filtering firewalls work on two basic policies: *Allow by Default* and *Deny by Default*.

- Packet-filtering firewalls can be configured to allow or block traffic based on IP address, port number, protocol ID, and/or MAC address.
- Application layer firewalls work at the Application layer of the OSI model.
- They are also called application firewalls or application layer gateways.
- Application layer firewalls are much slower than packet filtering firewalls.
- Stateful inspection firewalls actively monitor the state of the network traffic.

Proxy servers

- A proxy server allows network users to connect to the Internet in a secure manner.
- It allows better utilization of available Internet connection bandwidth.
- It stores web pages locally to improve performance by reducing response times.
- It helps track user activities while surfing web sites.
- It keeps the internal network secure from the Internet by hiding the internal IP addressing scheme.

Virtual Local Area Network (VLAN)

- A VLAN is a virtual or logical grouping of network devices.
- VLANs help reduce collisions by creating separate broadcast domains.
- Network switches that support VLAN protocols are used to create VLANs.
- VLANs are created on the basis of groups and memberships.
- A VLAN can span multiple physical network segments or multiple switches.
- A Trunk carries network traffic between each switch that is a part of VLAN.

Intranet

- Intranet refers to a private internal network.
- It extends connectivity to remote employees through the Internet.
- A tunnel is created in the Internet using protocols such as PPTP and L2TP.

Extranet

- Extranets allow external clients to access internal resources.
- Extranets also allow partner organizations to connect their networks.
- They are implemented through VPNs or RAS.

Port blocking/filtering

- Port blocking is the process of blocking unwanted traffic from entering a network.
- Port filtering is configured on firewalls and proxy servers.
- Blocking a specific port at the firewall thus stops all external traffic.

Authentication

- Authentication is the method of verifying the identity of a person or a system.
- In a one-way authentication, only one of the entities verifies the identity of the other.

- In a two-way authentication, both entities verify one another's identity.
- User credentials supplied for authentication can be transmitted in clear text or in encrypted form.

Username/password

- The username and password is the most common method of authentication.
- Passwords must be at least seven characters long and contain a combination of upper- and lowercase letters, numbers, and special characters.
- Passwords must not contain the full or partial first or last name of the user.
- Users must change their passwords periodically, and old passwords must not be reused.

Biometrics

- Biometrics devices identify a person based on her physical characteristics.
- Common biometrics include fingerprints and retinal scans.
- Handwriting, voice patterns, and body temperature are also used in biometrics.

Multifactor

- In multifactor authentication, many factors may be utilized.
- *Something you know* is a factor such as your password or PIN.
- *Something you have* is a factor such as your hardware token or a smart card.
- *Something you are* is a factor such as your fingerprints, your eye retina, or other biometrics that can be used for identity.
- *Something you do* is a factor such as your handwriting or your voice patterns.

Encryption

- Encryption applies an algorithm to plain text to produce an unreadable text.
- It ensures the confidentiality of messages.
- The integrity of a message ensures that the message has not been modified.
- Digital signatures provide data integrity and non-repudiation of data.
- Authentication refers to the verification of the identity of a person.
- Non-repudiation ensures that the sender cannot deny he sent the message.

Types of malicious codes

- Malicious code infects a user's computer without his knowledge.
- Viruses and worms infect a system without any obvious commercial gains.
- Trojan horses, rootkits, and backdoors infect the target system and conceal the identity of the attacker.
- Spyware, botnets, and adware gather information about the user in order to gain some kind of commercial profit.
- A boot sector, or bootstrap, virus infects the first sector on the hard disk.
- A parasitic virus infects an executable file.

Disk fault tolerance

- Disk fault tolerance is achieved by using a Redundant Array of Inexpensive Disks (RAID).
- A RAID solution can be implemented either through the NOS or through dedicated hardware.
- A software-based RAID solution is inexpensive, but it is not as efficient as a hardware-based RAID solution.

RAID-1

- RAID-1, or disk mirroring, is inexpensive because it needs only two disks.
- It offers good read performance.
- Disk utilization is 50 percent because only one of the disks is used at a time.
- No special software is required.

RAID-5

- RAID-5 is also called *disk striping with parity*.
- If one of the disks fails, the data is rebuilt using the parity information.
- An equivalent of one full disk space is used for writing parity information.
- It offers good disk read performance but poor write performance.
- Hardware-based RAID-5 solutions are expensive but more efficient.
- Inexpensive RAID-5 solutions can be implemented through the NOS.

Server fault tolerance

- In a stand-by server configuration, two identical servers are used: a primary and a secondary.
- The secondary server monitors the heartbeats of the primary server to detect failures.
- Server clustering provides fault tolerance as well as high availability.

Power supply

- Redundant power supplies provide an alternate source of power.
- An Uninterruptible Power Supply (UPS) provides external redundancy.
- A UPS protects the loss of data due to sudden power failure.
- It provides time to save necessary files and shut down the server properly.
- It protects expensive hardware from power threats such as spikes, surges, and sags.

Power problems

- A spike is a sharp increase in voltage for a very short period of time.
- A surge is a little longer increase in voltage, usually less intense than a spike.
- A sag is a sharp drop in voltage for a short period of time.
- A blackout is a complete failure of power supply.
- A brownout is a drop in voltage that lasts for a significant time.

Link redundancy

- Link redundancy ensures that a stand-by connection is available if the primary connection fails.
- Adapter teaming provides fault tolerance and improved performance.
- Adapter fault tolerance requires two network adapters.
- Adapter load balancing provides fault tolerance but also improved performance.
- Link aggregation effectively utilizes available network bandwidth.

Data backups

- A full backup backs up all the data in a single backup job.
- An incremental backup backs up the data that has changed after the last full or incremental backup was taken.
- A differential backup backs up the data that has changed since the last full backup.
- A copy backup copies all the data on the system.

Hot and cold spares

- Hot spares are installed inside critical servers and readily take over a failed component.
- Cold spares are installed inside a critical server but must be configured manually.
- Hot swapping is the ability of a server to allow replacement of a failed component while the server is powered on.
- Cold swapping does not allow replacement of failed components while the system is powered on.

Hot, warm, and cold sites

- A hot site is equipped with all necessary hardware and allows organizations to resume business activities almost immediately after a disaster.
- A warm site normally is equipped with necessary hardware but it is not fully configured.
- A cold site requires the maximum amount of time to be set up and made functional.

Network Support

This subsection covers a summary of highlights from the "Network Support" section in the Network+ Exam Study Guide.

tracert/traceroute

- This utility is used to trace the route from one host to another.
- It uses ICMP echo packets.
- If the network is congested, the output shows Request Timed Out.
- Windows operating systems use the commands: `tracert <Hostname>` or `tracert <IPAddress>`.

- Unix/Linux and MAC OS use the commands: `traceroute <Hostname>` or `traceroute <IPAddress>.`
- NetWare uses the command: `iptrace`

ping

- This utility is used to test connectivity between two TCP/IP hosts.
- It can also test whether name resolution is working or not.
- A Request Timed Out error means that the echo request did not get a response.
- A Destination Host Unreachable error appears when the host is not found.
- An Unknown Host error means that the hostname could not be resolved.
- A TTL Expired error means that no response was received before the TTL value reduced to zero.

Troubleshooting with ping

- Ping the local loopback address 127.0.0.1.
- Ping the IP address configured on the network interface of the local host.
- Ping the IP address of another host on the local network segment.
- Ping the IP address of the default gateway configured on the local host.
- Ping the IP address of a remote host.

arp

- The *arp* utility is used to resolve an IP address to the MAC address.
- Recently resolved MAC addresses are stored locally in the ARP cache.
- Dynamic entries are created automatically in the ARP cache.
- Static entries are added manually using the *arp –s* command.

netstat

- This utility displays the protocol statistics and current active TCP/IP connections.
- The output columns include protocol, local address and port number, foreign address and its port number, and the state of the connection.

nbtstat

- This utility is used only in Windows operating systems.
- It is used to display the NetBIOS over TCP/IP connection statistics.
- It is useful for diagnosing problems in Windows networks.

ipconfig

- This utility is used in Windows to display the TCP/IP configuration of the local host.
- When used with the `/all` parameter, it displays configuration of all network adapters.
- The *ipconfig* utility can also be used to release and renew IP configuration of a network adapter.

ifconfig

- This command is the Unix/Linux and MAC OS X equivalent of Windows *ipconfig*.
- It is used to display the TCP/IP configuration.

winipcfg

- This utility is used in Windows 95, Windows 98, and Windows ME.
- It displays current TCP/IP configuration settings.

nslookup

- This utility is used to diagnose name resolution problems.
- It can be executed in the interactive mode or in the noninteractive mode.
- In the noninteractive mode, it is run with one or two pieces of information.
- The interactive mode includes a number of subcommands, as listed in Table 8-25 in Chapter 8.

dig

- This command is used on Unix/Linux/MAC OS systems to perform DNS queries.
- Standard command parameters include the DNS server name, the name to be resolved, and the type of query.
- The query section displays the type and class of the DNS query.
- The answer section displays the name of the host and its IP address for which the query is being performed.
- The authority section displays information about authoritative DNS servers.

Troubleshooting with visual indicators

- No light or a yellow light indicates that the device or port is not operational, not connected, or faulty.
- A solid green light indicates that the device or port is connected but there is no activity.
- A flashing green light indicates that the device or port is functioning properly.
- A flashing amber light indicates that the network is congested and collisions are occurring.

Troubleshooting remote connectivity

- Users may not be allowed access due to file permissions.
- If a single client has a logon problem, make sure that the client is authorized to connect remotely.
- If multiple clients are having logon problems, check the RAS server or the authentication server.
- Make sure that all remote clients are using the correct TCP/IP configuration.
- Check the physical connectivity for DSL modems/cable modems/wireless access points.
- Check the LED indicators on modems and wireless access points and routers.
- Verify that a dial tone exists for dial-up modems.
- Verify the SSID settings on the access point and wireless clients.

Adding, removing, or modifying the DHCP service

- The DHCP service is used to dynamically assign IP addresses to clients.
- If a new DHCP server is added, the DHCP clients might need to be reconfigured to obtain and renew their IP addresses.
- If a DHCP server is removed, the clients will not able to obtain or renew their IP addresses.
- If the DHCP server is not available for a long time, the clients will not be able to connect to the network.

Adding, removing, or modifying the DNS service

- The DNS service is used to resolve hostnames to IP addresses.
- If the DNS server is removed, the clients will not be able to connect using hostnames.
- Clients will still be able to connect using IP addresses.
- If a new DNS server is added, the reconfiguration of DHCP clients should be configured through the DHCP server by modifying the DHCP scope.

Adding, removing, or modifying the WINS service

- The WINS service is used to resolve NetBIOS names to IP addresses.
- If the WINS server is not available, Windows clients will use the broadcasts to resolve computer names.
- Network broadcasts create significant network traffic and cause network congestion.
- If a new DNS server is added, the reconfiguration of DHCP clients should be configured through the DHCP server by modifying the DHCP scope.

Troubleshooting bus networks

- If the coaxial cable breaks, all computers will be disconnected.
- If one or both terminators are missing, the network is down.
- If the cable is not grounded, users will report intermittent connectivity problems.
- Addition or removal of computers from the bus network usually causes interruptions in network connectivity.
- If the network interface on a computer fails, it will also cause network failures.

Troubleshooting a star network

- Hubs and switches have LEDs to determine whether a port is connected or disconnected or whether there are collisions on the media.
- The hub or switch is the single point of failure, and all users in the segment will report connectivity problems.
- If only one user has a connectivity problem, trace the cable from his computer to the hub/switch and try to plug in the cable in a different port, or replace the cable.
- If all new computers cannot connect, verify that the correct cable type and length is used.
- Make sure that patch panels and patch cables are connected properly.

Troubleshooting ring networks

- The MSAU is a single point of failure, and all users will report connectivity problems if it fails.
- Make sure that the Ring In and Ring Out ports are properly connected.
- Verify that all network interface cards are operating at the same speed.
- Verify that the cable connecting the devices is not broken.

Troubleshooting network media

- Verify that the correct types of connectors are used and that they are properly attached.
- Verify that the correct cable type is used.
- Verify that the total length of a cable does not exceed the specifications.
- Wireless access points should not be located near areas of high interference.
- UTP cables should not be run in high EMI areas.
- For ceilings and ducts, plenum-rated cable must be used.

Troubleshooting network devices

- If a hub fails, all computers will experience connectivity problems.
- A failed switch will also result in connectivity problems to some or all computers.
- A failed bridge will cause connectivity problems from one segment to another.
- If a router fails, computers on one of the network segments will not be able to connect to any other network segment.
- If the router is connected to the Internet, no one will be able to access the Internet.
- You can test router connectivity using the *ping* and the tracert/*traceroute* commands.

Troubleshooting a wireless network

- Wireless signals degrade as they travel away from the access point.
- Prevent signal degradation by carefully locating the wireless antenna.
- Make sure that all wireless devices support the standard used on the network.
- Make sure that the AP and all clients are using the correct SSID.
- Make sure that the client is configured to use the correct WEP encryption standard.

Troubleshooting strategy

- Identify the symptoms and potential causes.
- Identify the affected area.
- Establish what has changed.
- Select the most probable cause.
- Implement an action plan and solution, including potential effects.
- Test the results.
- Identify the results and effects of the solution.
- Document the solution and process.

Network+ Exam Practice Questions

1. Which of the following media access methods is utilized in 802.11b wireless networks?

   ○ A. CDMA/CD

   ○ B. CDMA/CA

   ○ C. Token passing

   ○ D. Radio waves

   Answer B is correct. 802.11b-based networks use the Collision Detection Multiple Access/Collision Avoidance (CDMA/CA) media access method.

2. Which of the following statements associated with bus topology networks are correct? Select two answers.

   □ A. These networks are prone to EMI and RFI.

   □ B. A break in cable can bring down the network.

   □ C. It is wired in a dual ring physical layout.

   □ D. A central device is connected to all computers.

   □ E. A single cable is used to connect all computers.

   Answers B and E are correct. Bus networks use a single cable to connect all computers. A break in cable can bring down the entire network segment.

3. You have been asked to install a small network consisting of eight computers. Your manager wants the best possible fault tolerance. Which of the following topologies would you choose?

   ○ A. Bus

   ○ B. Star

   ○ C. Ring

   ○ D. Mesh

   Answer D is correct. The mesh topology provides the best fault tolerance. Every computer in a mesh network is connected to every other computer, thus providing multiple redundant paths.

4. Which of the following networks can be easily expanded without interrupting the other network devices and users? Select two answers.

   □ A. Bus

   □ B. Ring

   □ C. Star

   □ D. Mesh

   Answers C and D are correct. Star and mesh networks can be expanded without affecting the current network devices or the users.

5. Which of the following networks is configured in dual rings to provide fault tolerance?

   ○ A. Star

   ○ B. 802.5

   ○ C. FDDI

   ○ D. 802.3

Answer C is correct. The Fiber Distributed Data Interface (FDDI) standard-based networks are configured in dual ring topology to provide fault tolerance. If one of the rings fails, the other ring takes over.

6. Which of the following connectors cannot be attached with a fiber optic cable? Select two answers.

   ❑ A. RJ-45

   ❑ B. MT-RJ

   ❑ C. SC

   ❑ D. ST

   ❑ E. BNC

   Answers A and E are correct. The RJ-45 and BNC connectors are used with twisted pair and coaxial cables respectively. They cannot be used with fiber optic cables.

7. What is the maximum length of a UTP cable segment in a 10BaseT star network?

   ❍ A. 100 meters

   ❍ B. 200 meters

   ❍ C. 500 meters

   ❍ D. 2,000 meters

   Answer A is correct. The maximum length of a UTP cable segment in a 10BaseT star network is 100 meters.

8. Which if the following terms correctly describes the loss of signal while it travels down a particular medium?

   ❍ A. Crosstalk

   ❍ B. EMI

   ❍ C. Attenuation

   ❍ D. RFI

   Answer C is correct. Loss of signal as it travels to larger distances is known as *attenuation*.

9. Which of the following affects the performance of an 802.11b network?

   ❍ A. A broken cable

   ❍ B. EMI

   ❍ C. Addition of two new computers

   ❍ D. Crosstalk

   Answer B is correct. 802.11b is a wireless network standard. Wireless signals travel though radio waves, which can be affected by electromagnetic interference (EMI).

10. Identify the hardware associated with a network wired with coaxial cable. Select two answers.

    ❑ A. BNC connector

    ❑ B. Terminator

    ❑ C. RJ-11

    ❑ D. RJ-45

    ❑ E. SC

    Answers A and B are correct. Coaxial cables use BNC connectors and 50-Ohm terminators. The BNC T-connectors are used to attach computers, while the terminators are used at the ends of the cable.

11. One of the following network devices forwards the data it receives on a port to all other connected ports. Identify the device from the following:

    ❍ A. Router

    ❍ B. Bridge

    ❍ C. Hub

    ❍ D. Switch

    Answer C is correct. A hub forwards the data it receives on one port to all other connected ports.

12. Which of the following devices is used in Token Ring networks as the central device?

    ❍ A. Hub

    ❍ B. Switch

    ❍ C. Router

    ❍ D. MSAU

    Answer D is correct. An MSAU is the central device in Token Ring networks that connects to all devices.

13. Which of the following statements correctly describes the function of a router? Select two answers.

    ❑ A. It forwards data based on the MAC addresses of devices.

    ❑ B. It is used to forward data based on the destination IP address.

    ❑ C. It is used to join two network segments to make a large network.

    ❑ D. It is used to segment a large network.

    ❑ E. It is used to forward signals to all other ports.

    Answers B and D are correct. A router is used to segment a large network into smaller segments. It forwards the data based on the IP address of the destination.

14. Which of the following methods to build and maintain routing tables takes maximum administrative efforts and time in a large network?

    ❍ A. Static

    ❍ B. Dynamic

    ❍ C. Link state

    ❍ D. Distance vector

    Answer A is correct. Static routing tables are created and maintained manually by administrators. In large networks, it is not possible to use this method because it takes significant administrative time and effort and is prone to typing errors.

15. Which of the following addresses is an invalid MAC address?

    ❍ A. 5F-00-AD-2E-E4-34

    ❍ B. 00-12-ED-AG-K7-9E

    ❍ C. 00-0C-B8-22-AC-F3

    ❍ D. 6A-7D-00-E5-A8-58

    Answer B is correct. A MAC address can have numbers from 0 through 9, and letters from A to F.

16. Which of the following protocols uses a MAC address as part of the host address?

    ❍ A. TCP/IP

    ❍ B. IPX/SPX

    ❍ C. NetBEUI

    ❍ D. AppleTalk

    Answer B is correct. The IPX/SPX suite of protocols uses a MAC address as part of the host address.

17. Which of the following protocols does not depend on addresses or numbers to identify computers on a network?

    ❍ A. NetBEUI

    ❍ B. TCP/IP

    ❍ C. IPX/SPX

    ❍ D. AppleTalk

    Answer A is correct. In older Windows networks, the NetBEUI protocol uses computer names to identify computers. The NetBEUI protocol does not use any addressing scheme for networks or network hosts.

18. Which of the following are two constituent layers of the Data Link layer in the OSI networking model? Select two answers.

    ❑ A. Network

    ❑ B. Media Access Control (MAC)

    ❑ C. Application

    ❑ D. Logical Link Control (LLC)

    ❑ E. Transport

Answers B and D are correct. The two constituent layers of the Data Link layer are MAC and LLC.

19. Which of the following protocol suites includes the Routing Table Maintenance Protocol (RTMP)?

    ❍ A. AppleTalk

    ❍ B. IPX/SPX

    ❍ C. TP/IP

    ❍ D. NetBEUI

    Answer A is correct. The RTMP is included in the AppleTalk protocol suite. It is used to build and maintain routing tables.

20. At which of the following layers of the OSI network model does a network adapter work?

    ❍ A. Layer 1

    ❍ B. Layer 2

    ❍ C. Layer 3

    ❍ D. Layer 4

    Answer B is correct. A network adapter (network interface card) works at the layer 2 (the Data Link layer) of the OSI networking model.

21. Which of the following is a class C address?

    ❍ A. 128.10.54.120

    ❍ B. 92.200.138.24

    ❍ C. 168.28.10.165

    ❍ D. 193.10.160.45

    Answer D is correct. 193.10.160.45 is a class C address. The class C IP address range is from 192 to 223.

22. One of the network administrators in your company has asked you to block port 23 on the router. Which of the following services is he asking you to block?

    ❍ A. FTP

    ❍ B. Telnet

    ❍ C. SMTP

    ❍ D. HTTP

    Answer B is correct. TCP/IP port number 23 is used by the Telnet service.

23. Which of the following is a function of a WINS server? Select two answers.

    ❑ A. It resolves hostnames to IP addresses.

    ❑ B. It resolves IP addresses to MAC addresses.

    ❑ C. It resolves NetBIOS names to IP addresses.

    ❑ D. It is used to allocate IP addresses dynamically.

    ❑ E. It is used to reduce broadcast traffic.

Answers C and E are correct. The function of a WINS server is to resolve NetBIOS names to IP addresses. This helps reduce broadcast traffic because network clients send NetBIOS name resolution queries to the WINS server.

24. Which of the following protocols is used to secure HTTP transactions on the Internet?

    ❍ A. SCP

    ❍ B. SFTP

    ❍ C. SSL

    ❍ D. SSH

    Answer C is correct. The Secure Socket Layer (SSL) protocol is used to secure the HyperText Transfer Protocol (HTTP) transactions on the Internet. The addresses of web sites using the SSL protocol start with *https://*.

25. Which of the following statements correctly describes the function of a subnet mask?

    ❍ A. It is used to separate the network address from the host address within an IP address.

    ❍ B. It is used to forward data to remote network segments.

    ❍ C. It is used to block undesired network traffic.

    ❍ D. It is used to enable computers to communicate in different operating system environments.

    Answer A is correct. The subnet mask enables network devices to identify the network address and the host address from an IP address.

26. Which of the following protocols can be used to secure remote access connections when they are established through the Internet?

    ❍ A. PPP

    ❍ B. PPTP

    ❍ C. TCP/IP

    ❍ D. IPX/SPX

    Answer B is correct. The Point-to-Point Tunneling Protocol (PPTP) is used to establish a secure remote connection though the Internet.

27. Which of the following is a correct URL of a web site using the SSL protocol?

    ❍ A. *http://www.oreilly.com*

    ❍ B. *httpssl://www.oreilly.com*

    ❍ C. *http://www.oreilly.com/ssl*

    ❍ D. *https://www.oreilly.com*

    Answer D is correct. The URL of a web site using SSL protocol for security starts with *https://*.

28. What is the total bandwidth of an ISDN BRI connection when both data channels are used?

❍ A. 1.544 Mbps

❍ B. 128 Kbps

❍ C. 64 Kbps

❍ D. 56 Kbps

Answer B is correct. The total bandwidth of an ISDN BRI connection is 128 Kbps. Each channel of an ISDN BRI connection provides a bandwidth of 64 Kbps.

29. You need to allow only secure Internet traffic in and out of your company network. Which of the following ports would you open on the firewall?

❍ A. 22

❍ B. 53

❍ C. 80

❍ D. 443

Answer D is correct. Secure Internet sites use the Secure Socket Layer protocol. Since SSL uses port number 443, you will need to open port 443 on the firewall.

30. Which of the following advantages are associated with using a firewall?

❍ A. It provides an inexpensive means to share the Internet connection.

❍ B. It is used to block undesired external access to internal network resources.

❍ C. It is used to monitor the use of Internet by internal users.

❍ D. It is used to hide the internal addressing scheme of the network.

Answer B is correct. A firewall is used to block undesired external access to internal network resources.

31. Which of the following is not a benefit of implementing a proxy server for Internet access?

❍ A. The costs associated with Internet access.

❍ B. Activities of users can be monitored.

❍ C. It provides a centralization of Internet access.

❍ D. The Internet hostnames can be resolved internally.

❍ E. It allows improved performance for web browsing.

Answer D is correct. A proxy server does not help resolve external host names internally. External DNS servers must resolve hostnames that are external to the network.

32. Which of the following backup methods reset the archive bit? Select two answers.

   ❑ A. Full backup

   ❑ B. Copy backup

   ❑ C. Incremental backup

   ❑ D. Differential backup

   Answers A and C are correct. The full and incremental backups reset the archive bit after taking the backup. The copy backup and differential backup do not change the archive bit.

33. You are using five 80 GB hard disks in your file server to configure RAID-5. What will be the maximum capacity of the RAID be after the configuration is complete?

   ❍ A. 80 GB

   ❍ B. 160 GB

   ❍ C. 320 GB

   ❍ D. 400 GB

   Answer C is correct. In a RAID-5 configuration, space equal to one full disk is utilized for writing parity information. This means that space equal to four hard disks (320 GB) will actually be available for data storage.

34. Which of the following terms is associated with a power outage for a long period of time?

   ❍ A. Sag

   ❍ B. Blackout

   ❍ C. Brownout

   ❍ D. Spike

   Answer B is correct. If the power remains out for a long period of time, it is known as power blackout.

35. You have been asked to make a plan to back up all critical servers in the office. Where should you keep the backup tapes after the backup is complete?

   ❍ A. Inside the server room.

   ❍ B. In a locked closet outside the server room.

   ❍ C. At a secure offsite location.

   ❍ D. In the manager's cabin.

   Answer C is correct. Backup tapes should be stored at a secure offsite location to prevent accidental damage. This helps with data recovery in the event of a disaster.

36. One of the users in your office complains that he is not able to connect to the network or the Internet. Which of the following steps should you take first in order to troubleshoot the connectivity problem?

   ❍ A. Ping the loopback address.

   ❍ B. Ping a remote host.

❍ C. Ping the default gateway.

❍ D. Ping the IP address of the user's computer.

Answer A is correct. The first step in troubleshooting a connectivity problem in a TCP/IP host is to *ping* the loopback address 127.0.0.1.

37. Which of the following utilities would you use when a Windows XP user is not able to connect using computer names?

❍ A. *ping*

❍ B. *nbtstat*

❍ C. *netstat*

❍ D. *tracert*

Answer B is correct. The *nbtstat* utility is used in a Windows network to resolve connectivity problems. *nbtstat* displays the current NetBIOS over TCP/IP statistics and the currently active connections.

38. Which of the following utilities is used on a Linux system to verify TCP/IP configuration?

❍ A. *ipconfig*

❍ B. *dig*

❍ C. *arp*

❍ D. *ifconfig*

Answer D is correct. The *ifconfig* utility is used on Unix and Linux systems to verify the TCP/IP configuration of the local host.

39. A new network administrator has configured some new wireless clients. None of these clients is able to connect to the network. Other clients already on the same access point do not have any connectivity problem. Which of the following is the possible reason for the problem?

❍ A. An incorrect SSID

❍ B. An incorrect IP address

❍ C. A faulty access point

❍ D. A poor signal due to EMI

Answer A is correct. The connectivity problem is most probably caused by incorrect SSID settings on the new wireless clients.

40. One of the users has reported problems with his desktop. He is somewhat unclear about the problem's symptoms and you need to visit his desk to rectify the problem. What should be your first step to resolve the problem?

❍ A. Check event logs on the desktop.

❍ B. Ask the user to restart the desktop.

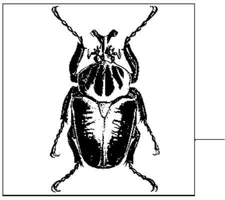
❍ C. Try to recreate the problem.

❍ D. Gather more information from the user.

Answer D is correct. The first step to resolve a network problem is to gather as much information as possible from the user.

IV

Security+



10
Overview of Security+ Exam

CompTIA's Security+ certification is for those individuals who work or intend to work in organizations that have a secure IT infrastructure. You will need to pass only one exam (*Exam SYO-101*) to get this certification. Exam SYO-101 tests your foundation-level knowledge in general security concepts, communications and infrastructure security, basics of cryptography, and operational and organizational security. This exam was developed in response to increasing demand from security professionals in the IT industry. A Security+-certified individual is considered to have proven her skills in implementing basic security in the IT infrastructure. CompTIA's vendor-neutral certifications, including the Security+ certification, are now recognized worldwide.

There are several other security-related certifications available in the IT industry, but the Security+ certification is considered the most basic of all. One good thing about CompTIA's certifications is that they do not expire. In other words, CompTIA's certifications are good for life. You do not have to recertify if the exam objectives change after a period of time. I still recommend that you check the Security+ certification page on the CompTIA web site from time to time at *http://certification.comptia.org/security* for news and updates on exam objectives.

The approximate percentage of each section in Security+ Exam SYO-101 is given in Table 10-1.

Table 10-1. Security+ exam domains and percentage of coverage

Domain	Percentage of coverage
General Security Concepts	30 percent
Communication Security	20 percent
Infrastructure Security	20 percent
Basics of Cryptography	15 percent
Operational/ Organizational Security	15 percent

CompTIA recommends that, in order to pass the Security+ exam, a candidate should have at least two years of hands-on experience working in an organization where IT security is a prime concern. It is also recommended that the candidate have passed the A+ and the Network+ exams before attempting to take this exam. It is a good idea to have studied a Security+ certification exam self-paced study guide or to have attended a training course before you attempt to take this. After all this, you will be ready to use this section of the book as your final exam preparation tool.

> The Security+ certification exam, *SYO-101* is considered to be one of the toughest of all CompTIA exams. The percentage of marks required to pass this exam is very high, and you have to be well prepared. You must study the preparation material thoroughly and try some self-test practice exams before you attempt to take the actual exam. Once you pass this, you also get an exemption for one elective exam in Microsoft's MCSE/MCSA: Security track.

Areas of Study for Security+ Exam

General Security Concepts

- Recognize and be able to differentiate and explain the following access control models:
  - MAC (Mandatory Access Control)
  - DAC (Discretionary Access Control)
  - RBAC (Role Based Access Control)
- Recognize and be able to differentiate and explain the following methods of authentication:
  - Kerberos
  - CHAP (Challenge Handshake Authentication Protocol)
  - Certificates
  - Username/Password
  - Token
  - Multifactor
  - Mutual
  - Biometrics
- Identify non-essential services and protocols, and know what actions to take to reduce the risks of those services and protocols.
- Recognize the following attacks and specify the appropriate actions to take to mitigate vulnerability and risk:
  - DOS/DDOS (Denial of Service / Distributed Denial of Service)
  - Back door
  - Spoofing
  - Man in the Middle
  - Replay
  - TCP/IP hijacking
  - Weak keys
  - Mathematical
  - Social engineering
  - Birthday
  - Password guessing using brute force and the dictionary
  - Software exploitation
- Recognize the following types of malicious code and specify appropriate actions to take to mitigate vulnerability and risk:
  - Viruses
  - Trojan horses
  - Logic bombs
  - Worms

- Understand the concept of and know how to reduce the risks of social engineering.
- Understand the concept and significance of auditing, logging, and system scanning.

Communication Security

- Recognize and understand the administration of the following types of remote access technologies:
    - 802.1x
    - VPN (Virtual Private Network)
    - RADIUS (Remote Authentication Dial-In User Service)
    - TACACS (Terminal Access Controller Access Control System)
    - L2TP/PPTP (Layer 2 Tunneling Protocol/Point-to-Point Tunneling Protocol)
    - SSH (Secure Shell)
    - IPSec (Internet Protocol Security)
    - Vulnerabilities
- Recognize and understand administration of the following email security concepts:
    - S/MIME (Secure Multipurpose Internet Mail Extensions)
    - PGP (Pretty Good Privacy) technologies
    - Vulnerabilities
    - Spam
    - Hoaxes
- Recognize and understand administration of the following Internet security concepts:
    - SSL/TLS (Secure Sockets Layer/Transport Layer Security)
    - HTTP/S (Hypertext Transfer Protocol/Hypertext Transfer Protocol over Secure Sockets Layer)
    - Instant Messaging, including vulnerabilities, packet sniffing, and privacy
    - Vulnerabilities in Java Script, ActiveX, Buffer Overflows, Cookies, Signed Applets, CGI, and SMTP Relay
- Recognize and understand administration of the following directory security concepts:
    - SSL/TLS (Secure Sockets Layer/Transport Layer Security)
    - LDAP (Lightweight Directory Access Protocol)
- Recognize and understand administration of the following file transfer protocols and concepts:
    - S/FTP (File Transfer Protocol)
    - Blind FTP (File Transfer Protocol)/Anonymous
    - File sharing

- Vulnerabilities
- Packet sniffing
- 8.3 naming conventions

- Recognize and understand administration of the following wireless technologies and concepts:
  - WTLS (Wireless Transport Layer Security)
  - 802.11 and 802.11x
  - WEP/WAP (Wired Equivalent Privacy/Wireless Application Protocol)
  - Vulnerabilities, including site surveys

Infrastructure Security

- Understand the security concerns and concepts of the following types of devices:
  - Firewalls
  - Routers
  - Switches
  - Wireless
  - Modems
  - RAS (Remote Access Server)
  - Telecom/PBX (Private Branch Exchange)
  - VPN (Virtual Private Network)
  - IDS (Intrusion Detection System)
  - Network monitoring/Diagnostics
  - Workstations
  - Servers
  - Mobile devices
- Understand the security concerns for the following types of media:
  - Coaxial cable
  - UT/ STP (unshielded twisted pair/shielded twisted pair)
  - Fiber optic cable
  - Removable Media such as tape, CD-R, hard drives, diskettes, flashcards, and smart cards
- Understand the concepts behind the following kinds of security topologies:
  - Security zones such as DMZ (Demilitarized Zone), intranet, and extranet
  - VLAN (Virtual Local Area Network)
  - NAT (Network Address Translation)
  - Tunneling

- Differentiate the following types of intrusion detection; be able to explain the concepts of each type; and understand the implementation and configuration of each kind of intrusion detection system:
  - Network-based: active detection and passive detection
  - Host-based: active detection and passive detection
  - Honey pots
  - Incident response
- Understand the following concepts of Security Baselines; be able to explain what a Security Baseline is; and understand the implementation and configuration of each kind of intrusion detection system:
  - OS/NOS (Operating System/Network Operating System) hardening, including filesystem and updates (hotfixes, service packs, patches)
  - Network hardening, including updates (firmware), enabling/disabling services and protocols, and configuring Access Control Lists
  - Application hardening, including software updates (hotfixes, service packs, and patches), web servers, email servers, FTP servers, DNS servers, NNTP servers, file/print servers, DHCP servers, and data repositories (directory services and databases)

Basics of Cryptography

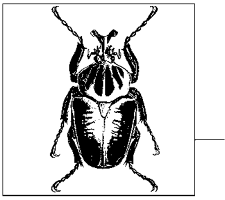
- Be able to identify and explain different kinds of cryptographic algorithms, such as hashing, symmetric and asymmetric.
- Understand how cryptography addresses the following security concepts:
  - Confidentiality
  - Integrity using digital signatures
  - Authentication
  - Non-repudiation and digital signatures
  - Access control
- Understand and be able to explain the following concepts of PKI:
  - Certificates, certificate policies, and certificate practice statements
  - Revocation
  - Trust models
- Identify and be able to differentiate between different cryptographic standards and protocols.
- Understand and be able to explain the following concepts of Key Management and certificate lifecycles:
  - Centralized versus decentralized
  - Storage hardware versus software and private key protection
  - Escrow

  - Expiration
  - Revocation, suspension, and status checking
  - Recovery (including M-of-N Control), renewal, and destruction
  - Key usage

Operational/Organizational Security

- Understand the application of the following concepts of physical security:
  - Access control using physical barriers and biometrics
  - Social engineering
  - Environment (including wireless cells, location, shielding, and fire suppression)
- Understand the security implications of the following topics of disaster recovery:
  - Backups and offsite storage
  - Secure recovery
  - Disaster recovery plan
- Understand the security implications of business continuity.
- Understand the concepts and uses of security and incident response policies and procedures:
  - Security policy, including acceptable use, due care, privacy, separation of duties, need to know, password management, service level agreements, disposal and destruction, and human resources policy (including termination, hiring, and code of ethics)
- Explain the following concepts of privilege management:
  - User/group role management
  - Single sign-on
  - Centralized versus decentralized
  - Auditing (Privilege, Usage, Escalation)
  - MAC/DAC/RBAC (Mandatory Access Control/Discretionary Access Control/Role-based Access Control)
- Understand the concepts of the following topics of forensics:
  - Chain of custody
  - Preservation of evidence
  - Collection of evidence
- Understand and be able to explain the concepts of risk identification and asset identification.
- Understand the security relevance of the education and training of end users, executives, and human resources.

- Understand and explain the following documentation concepts:
  - Standards and guidelines
  - Systems architecture
  - Change documentation
  - Logs and inventories
  - Classification and notification
  - Retention/storage and destruction
  - Data destruction



11

Security+ Exam Study Guide

This chapter provides a study guide for the Security+ Exam SYO-101. Each section of this chapter is designed to cover specific objectives of the exam. Each section heading identifies the exam domain, and discusses the key details that you should grasp before taking the exam.

An overview of the sections in this chapter that cover the objectives of the Security+ exam is as follows:

General Security Concepts
: This section covers the details of general concepts and terms related to IT security. These concepts include methods of access control, authentication, and auditing. This section also includes a study of various types of attacks and malicious code, identifying and disabling nonessential services, and protocols to reduce vulnerability of computers and networks.

Communication Security
: This section covers a study of security concepts related to computer communications such as remote access, email, Internet-based services, directory services, and file transfer protocols. You will also learn about the security risks involved in wireless networks.

Infrastructure Security
: This section includes a study of implementing security in the IT infrastructure by creating security baselines, implementing Intrusion Detection Systems (IDS), and other security topologies. This also includes a study of vulnerable points in the network, such as network devices and media.

Basics of Cryptography
: This section includes a study of concepts related to encryption methods that are used to provide confidentiality, integrity, authentication, and non-repudiation. These encryption methods protect the transfer of data from one location to another in a network. You will learn how encryption algorithms and digital certificates are used to create a Public Key Infrastructure (PKI). The PKI is responsible for the creation, distribution, storage, expiration, and revocation of digital certificates.

Operational and Organizational Security

This section covers concepts related to operational and organizational security. This includes a study of the physical security of the network, as well as creating backup and disaster recovery policies, security policies, and incident response policies. You will also learn about privilege management, computer forensics and risk identification, and guidelines for training end users on how to create documentation related to security practices in an organization.

The sections in this chapter are designed to follow the exam objectives as closely as possible. This Study Guide should be used to reinforce your knowledge of key concepts tested in the exam. If you study a topic and do not understand it completely, I recommend that you go over it again and memorize key facts until you feel comfortable with the concepts. The chapter contains a number of terms, notes, bulleted points, and tables that you will need to review multiple times. Pay special attention to new terms and acronyms (the ones you are not familiar with) because these may be tested in the exam.

Studying for the Security+ certification exam requires that you have access to a computer network. Although it is not essential, it is good to have a Windows-based computer network to perform the exercises included in this chapter. These exercises are a required part of your preparation for the exam. A small network with a Windows XP desktop and a Windows 2000 Server or Windows Server 2003 would serve the purpose as well. Needless to say, you will also need an active Internet connection.

> The exercises included in this Study Guide should be part of your preparation for the exam. Do not perform any exercises in a production environment. Instead, create a test environment where you can work without having to worry about the security risks while performing the given exercises.

General Security Concepts

The first section of this chapter deals mainly with fundamental knowledge of authentication, access control, and auditing, also known as AAA in the computer security arena. Along with this, you will learn about different types of attacks and about malicious code that can cause significant damage to the organization's security setup. The concepts discussed in the following section are as follows:

- Access control methods
- Authentication methods
- Auditing and logging
- System scanning
- Types of attacks
- Types of malicious code
- Risks involved in social engineering
- Identifying and disabling nonessential services and protocols

Each of these concepts is discussed in the following sections.

Access Control Models

In this section, you will learn about different types of access control methods. These methods are used to grant or deny access to a network or computer resource by means of security policies and hardware or software applications. In its simplest form, access control to files, folders, and other shared network resources is achieved by means of assigning permissions. Smart cards and biometric devices are examples of hardware devices used for access control. Access control can also be implemented by means of network devices, such as routers and wireless Access Points (APs). You can also achieve access control by implementing security policies, such as remote access policies and rules for connecting to a virtual private network (VPN). The following are the main models or mechanisms employed for access control:

- Mandatory Access Control
- Discretionary Access Control
- Role-Based Access Control

Mandatory Access Control (MAC)

MAC is a mechanism, usually hardcoded into an operating system, that protects computer processes, data, and system devices from unauthorized use. Once implemented, MAC is applied universally to all objects on the system. It may also be built into an application to grant or deny permissions and is universally applied to all objects. The basic concept behind MAC is that it cannot be changed by any user. Moreover, the control of access can be defined at multiple levels to provide granular control.

All operating systems, such as Microsoft's Windows, Unix/Linux, and Netware, include MAC mechanisms. The operating systems hardcode access control individually on each object, and even the owners of the object or resource cannot change the implemented level of access. In other words, MAC is nondiscretionary, and the users who create an object may not have so-called "full control" over the object they create.

The main purpose of MAC is to define a security architecture that makes evaluations of contexts based on security labels. In a nutshell, MAC is hardcoded and nondiscretionary, is universally applied to all objects by the operating system, and is sometimes also known as *label-based access control*.

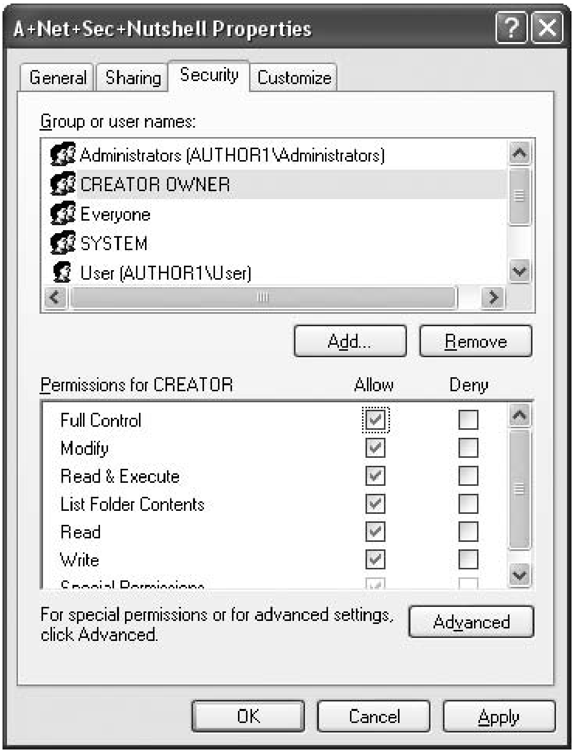
Discretionary Access Control (DAC)

DAC is a mechanism that is usually implemented by the operating system. Administrators or users who are creators/owners of an object or resource are the main users of DAC, which allows them to grant or deny permissions. NTFS permissions (used in Windows-based computers) are a good example of DAC. It is also possible to change ownership of objects or resources when DAC is used.

The owner or administrator of the object mainly controls the control of access to an object or resource. As with MAC, you can also have multiple levels of access control with DAC. But at the same time, DAC does not provide the level of access control that is available with MAC. It is not hardcoded into any operating system.

To have an idea of how DAC is applied, we will perform the following exercise on a Windows XP Professional computer that has a drive formatted with an NTFS file system:

1. Click Start → Programs → Accessories → Windows Explorer.
2. Locate a user data folder.
3. Right-click the folder and select Properties.
4. Click on the Security tab.
5. The NTFS permissions that have been set on the folder are displayed, as shown in Figure 11-1. The shared folder in this case is the network resource and the permissions assigned to the folder are termed the *DAC list*.
6. Click Cancel to close the dialog box.



Group or user names:

- Administrators (AUTHOR1\Administrators)
- CREATOR OWNER
- Everyone
- SYSTEM
- User (AUTHOR1\User)

Permissions for CREATOR	Allow	Deny
Full Control	☑	□
Modify	☑	□
Read & Execute	☑	□
List Folder Contents	☑	□
Read	☑	□
Write	☑	□
Special Permissions	☑	□

For special permissions or for advanced settings, click Advanced.

Figure 11-1. Viewing DAC permissions on an object

Role-Based Access Control (RBAC)

The RBAC is a mechanism used to implement security on objects based on the roles or job functions of individual users or user groups. Employees of an organization are categorized by their need to perform different types of roles (jobs) within the organization, and permissions to computer or network resources are granted to these users based on their roles.

RBAC offers the most flexibility in defining access control to available network resources. For example, users in a network can be classified into various categories or groups based on their job functions, and access permissions to objects can be granted to these groups. The job functions and access permissions can be modified at any point in time based on the requirements of the organization. RBAC thus provides simplified and centralized administration of network resources. It is more flexible than MAC and is highly configurable.

Authentication Methods

Authentication is the process of confirming that someone or something is authentic, which means that the claim made about something is true. In the context of computer security, authentication is the method of verifying that the identity of a person or an application seeking access to a system, object, or a resource is true. For example, if a user wants to access a network domain, the authentication of the user (or the user's digital identity) is usually verified by the username and password supplied by the user. These data items are also known as the credentials of the user. If the username and password of the user matches those stored in the security database of the computer, the user is allowed access. This process is known as the *authentication process*.

Authentication can be a one-way or two-way-process. In one-way authentication, only one of the entities verifies the identity of the other, while in a two-way authentication, both entities verify the identity of each other before a secure communication channel is established. In the previous example, you learned about the simplest form of one-way authentication wherein the identity of the user is verified by the system.

Authentication is termed as the first point of controlling access to a system. Further access can be controlled by using *authorization*, which is a term very closely related to authentication. Authorization is provided as part of the operating system and is the process of allowing access to only those resources to which a particular user is authorized. These resources may include the system services and devices, data, and application programs.

User credentials sent by the user during the authentication process can be transmitted either in clear text or in encrypted form. Some applications, such as File Transfer Protocol (FTP) and Telnet, transmit usernames and passwords in clear text. User credentials transmitted in clear text are considered security risks, as anyone monitoring the network transmissions can easily capture these credentials and misuse them. There are several methods, as you will learn in the following pages, that can be used to encrypt and secure user credentials as they are transmitted over the network.

The following sections discuss a number of authentication mechanisms that are used in computer networks.

Kerberos

Kerberos is a cross-platform authentication protocol used for mutual authentication of users and services in a secure manner. This protocol is created and maintained by the Massachusetts Institute of Technology (MIT) and is defined in RFC 1510. Kerberos v5 is the current version. The protocol ensures the integrity of data as it is transmitted over the network. Microsoft's Windows-based network operating systems (Windows 2000 and later) use Kerberos v5 as the default authentication protocol. It is also widely used in other operating systems, such as Unix and Cisco IOS. The authentication process is the same in all operating system environments.

Kerberos protocol is built upon Symmetric Key Cryptography and requires a trusted third party. In Windows Server 2003 environments, Kerberos can be implemented in its own Active Directory domains. Kerberos works in a *Key Distribution Center (KDC)*, which is usually a network server used to issue secure encrypted keys and *tokens (tickets)* to authenticate a user or a service. The tickets carry a timestamp and expire as soon as the user or the service logs off.

Let's look at how Kerberos authentication works. Consider a Kerberos realm that includes a KDC (also known as the authentication server), a client (a user, service, or a computer), and a resource server. Consider that the client needs to access a resource or shared object on the resource server. The following steps are carried out to complete the authentication process:

1. The client presents its credentials to the KDC for authentication by means of username and password, smart card, or biometrics.
2. The KDC issues a Ticket Granting Ticket (TGT) to the client. The TGT is associated with an access token that remains active until the time the client is logged on. This TGT is cached locally and is used later if the session remains active.
3. When the client needs to access the resource server, it presents the cached TGT to the KDC. The KDC grants a session ticket to the client.
4. The client presents the session ticket to the resource server and the client is then granted access to the resources on the resource server.

The Kerberos authentication process is known as a *realm*, as shown in Figure 11-2.

The TGT remains active for the entire active session. It carries a timestamp to ensure that it is not misused to launch *replay*, or *spoofing*, attacks against the network. Replay attacks happen when someone captures network transmissions, modifies this information, and then retransmits the modified information on the network to gain unauthorized access to resources. You will learn more about security attacks later in this section.

Kerberos is heavily dependent on the synchronization of clocks on the clients and servers. Session tickets granted by the KDC to the client must be presented to the server within the established time limits, or else they may be discarded. TGT is not dependent on time and remains valid until the client is logged on. TGT is cached locally by the client and can be used if the user session remains active.

Challenge Handshake Authentication Protocol (CHAP)

CHAP is widely used for remote access in conjunction with the Point-to-Point Protocol (PPP). CHAP periodically verifies the authenticity of the remote user

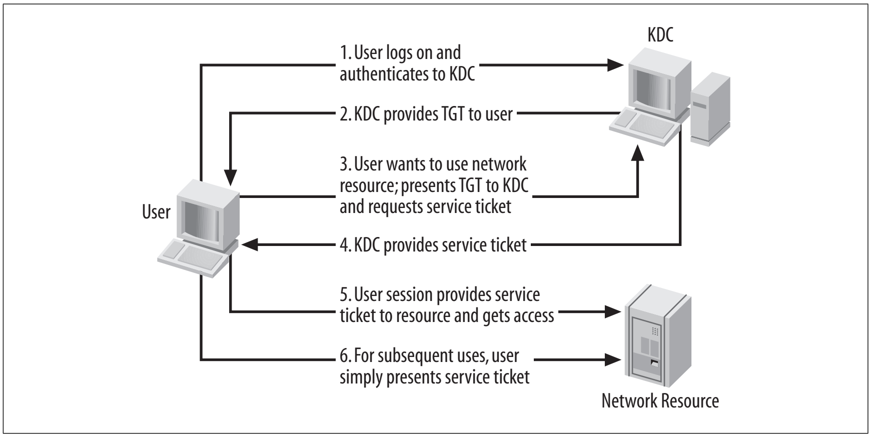

KDC
1. User logs on and authenticates to KDC
2. KDC provides TGT to user
3. User wants to use network resource; presents TGT to KDC and requests service ticket
User
4. KDC provides service ticket
5. User session provides service ticket to resource and gets access
6. For subsequent uses, user simply presents service ticket
Network Resource

Figure 11-2. Kerberos authentication process

using a three-way handshake even after the communication channel has been established. CHAP authentication involves the following steps:

1. When the communication link is established, the authentication server sends a “challenge” message to the peer.
2. The peer responds with a value calculated using a one-way hash function such as Message Digest 5 (MD5).
3. The authentication server checks the response to ensure that the value is equal to its own calculation of the hash value. If the two values match, the authentication server acknowledges the authentication; otherwise, the connection is terminated.
4. The authentication server sends the challenge message to the peer at random intervals and repeats steps 1 to 3.

One drawback of CHAP is that it cannot work with encrypted password databases and is considered a weak authentication protocol. It is still better than *Password Authentication Protocol (PAP)*, in which passwords are transmitted in clear text. Microsoft has implemented its own version of CHAP, known as *MS-CHAP*, which is currently in version 2.0 and is the preferred authentication protocol for remote access services.

Certificates

Certificates, or Public Key Certificates, use *digital signatures* to bind a public key to the identity of a person or a computer. The certificates are used to ensure that the public key belongs to the individual. Certificates are widely used for Internet-based authentications, as well as for authenticating users and computers in network environments, to access network resources and services where directory services are implemented. They are also used when data transmissions are secured using Internet Protocol Security (IPSec) protocol. All of these are parts of the PKI, which is discussed later in this chapter.

In a PKI certificate, servers are used to create, store, distribute, validate, and expire digitally created signatures and other identity information about users and systems. Certificates are created by a trusted third party known as the Certification Authority, or Certificate Authority (CA). Examples of commercially available CAs are Verisign and Thawte. It is also a common practice to create a CA within an organization to manage certificates for users and systems within the organization or with trusted business partners. In Windows 2000 and later operating systems, certificates are used for authenticating users and granting access to Active Directory objects. CA used within an organization is known as an *Enterprise CA* or a *Standalone CA*.

Another common use of certificates is for software signing. Software is digitally signed to ensure the user who downloads it that it is legitimate or has been developed by a trusted software vendor. Digitally signed software ensures that the software has not been tampered with since it was developed and made available for download. Certificates are also implemented in Internet services to authenticate users and verify their identity. Web servers must have a certificate installed in order to use the Secure Socket Layer (SSL).

A certificate essentially includes the following information:

- The public key being signed.
- A name that can be that of a user, a computer, or an organization.
- The name of the CA issuing the certificate.
- The validity period of the certificate.
- The digital signature of the certificate, which is generated using the CA's private key.

Username/Password

The combination of username and password is one of the most common methods of authenticating users in a computer network. Almost all network operating systems implement some kind of authentication mechanism wherein users can simply use a locally created username and password to get access to the network and shared resources within that network. These include Microsoft's Windows, Unix/Linux, Netware OS, and MAC OS X. This is the simplest form of authentication and can be implemented easily, but it also comes with its own limitations. In a secure network environment, simply using the combination of a username and password may not be enough to protect the network against unauthorized access.

Many organizations document and implement password policies that control how users can create and manage their passwords in order to secure network resources. If any user does not follow these policies, her user account may be locked until the administrator manually unlocks it. The following is an example of strong password policy:

- Passwords must be at least seven characters long.
- Passwords must contain a combination of upper- and lowercase letters, numbers, and special characters.

- Passwords must not contain the full or partial first or last name of the user.
- Passwords must not contain anything to do with personal identity such as birthdays, Social Security numbers, name of their hometown, names of pets, etc.
- Users must change their passwords every six weeks.
- Users must not reuse old passwords.

With a properly enforced password policy, an organization can attain some security for its network resources.

Tokens

An *authentication token* (also known as a *security token* or a *hardware token*) is considered the most trusted method to verify the identity of a user or a system. Tokens provide a very high level of security for authenticating users because of the multiple factors employed to verify the identity. It is almost impossible to duplicate the information contained in a security token in order to gain unauthorized access to a secure network. Figure 11-3 shows different types of security tokens.

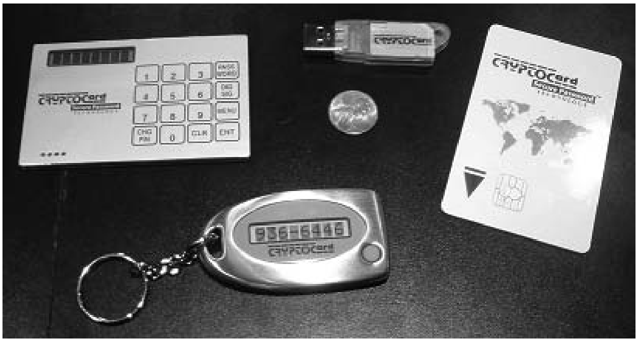


Figure 11-3. Security tokens

In its simplest form, an authentication token consists of the following two parts:

- A hardware device that is coded to generate token values at predetermined intervals.
- A software-based component that tracks and verifies that these codes are valid.

Hardware tokens are small enough to be carried on a key chain or in a wallet. Some security tokens may contain cryptographic keys while others may contain biometrics data such as the user's fingerprints. Some tokens have a built-in keypad, and the user is required to key in a Personal Identification Number (PIN).

Authentication tokens come in a variety of packaging and features. RSA's *SecureID* is one type of security token that employs a two-factor authentication mechanism. Other vendors employ digital signatures methods, while still others use the single sign-on software mechanisms. Some tokens utilize the one-time password technology. With the *single sign-on* software, the user need not remember his passwords as they are stored on tokens and are regularly changed. With the *one-time password* technology, the password changes after each successful login or after a specified interval of time.

Multifactor

When using secure methods in computer authentication, a factor is a piece of information that is present to prove the identity of a user. In a multifactor authentication mechanism, any combination of the following types of factors may be utilized:

- A *something you know* factor, such as your password or PIN.
- A *something you have* factor, such as your hardware token or a smart card.
- A *something you are* factor, such as your fingerprints, your eye retina, or other biometrics that can be used for identity.
- A *something you do* factor, such as your handwriting or your voice patterns.

Multifactor authentication is considered acceptably secure because it employs multiple factors to verify the identity of the user or service requesting authentication. For example, when withdrawing money from a bank's ATM, you need a debit card, which is a *something you have* factor. You will also need to know the correct PIN to complete the transaction, which is a *something you know* factor.

Mutual authentication

Mutual authentication, or two-way authentication, is the process where both parties authenticate each other before the communication link can be established. In case the communication is to be set up between a client and a server, both the client and server would authenticate each other using a mutually acceptable authentication protocol. This ensures that both the client and the server can verify each other's identity. In a typical setup, the process is carried out in the background without any user intervention.

In secure web transactions, such as online banking, mutual authentication may use secure socket SSL or certificates for the authentication purpose. However, due to the complexity, the cost involved, and the effectiveness, most web applications are built in so that the clients are not required to have certificates. This leaves the transaction or the communication open to *Man-in-the-Middle (MITM)* attacks.

Almost all network operating systems provide ways for mutual authentication when offering remote access to clients. *Remote Authentication Dial-in User Service (RADIUS)* is one of the commonly used authentication protocols employed in remote access. RADIUS provides mutual authentication to verify and authenticate both sides of the communication.

Biometrics

Biometrics refers to the authentication technology used to verify the identity of a user by measuring and analyzing human physical and behavior characteristics. This is done with the help of advanced biometric authentication devices that can read or measure and analyze fingerprints, scan the eye retina and facial patterns, and/or measure body temperature. Handwriting and voice patterns are also commonly used in biometrics. Biometric authentication provides the highest level of authenticity about a person, which is much more reliable than a simple username and password combination. It is nearly impossible to impersonate a person when biometric authentication is used for authentication.

Auditing and Logging

Auditing is the process of tracking and logging activities of users and processes on computer systems and networks. It can be useful in multiple scenarios such as: troubleshooting a failed process, detecting a security breach on the part of an internal or external user; and tracking unauthorized access to secure data. Auditing and logging enables administrators to link desired or undesired processes to specific user accounts and system processes. When linked to user accounts, it is possible to track a security breach such as unauthorized access to confidential data by identifying the user who made the attempt. When linked to processes, it is helpful in diagnosing problems related to process failures. Auditing and logging, in certain situations, may also be helpful in collecting evidence that can be used against an unauthorized user during criminal investigations.

System auditing

System auditing is the process of tracking usage and authorized or unauthorized access to system services and data. This may also be helpful in diagnosing problems related to application failures during the development or implementation phase. Since auditing puts a significant processing load on servers, you must first make sure that the benefits of auditing are clearly understood and visible.

While administrators should implement certain audits manually, network operating systems include processes that automatically audit system process and log audit data that can be analyzed later in order to troubleshoot system failures. Administrators usually configure auditing of network and system resources as well as privileges assigned to a user manually. Auditing is essentially a two-step process: first, auditing is enabled on resources; and second, administrators must view and analyze the data collected by the audits.

In its basic form, a secure computing environment can be established by splitting duties of employees within an organization. This ensures that whatever actions are taken by an employee are consistently supervised or controlled by someone superior in the organizational hierarchy. Some of the basic guidelines are as follows:

- The same person should not be authorized to both originate a request and approve it.
- Access to classified and confidential data must be restricted.
- Conversion, copying, and concealment of data must not be allowed.

Logging

Almost all network operating systems include methods to audit system processes and user activities. These audits can be logged in special log files, which is a process called *event logging*. The log files can be viewed and analyzed to track problems related to security breaches and to troubleshoot process problems. Operating systems such as Microsoft Windows Server 2003 include a management console named *Event Viewer*, where you can view the logs related to system processes, security, and applications.

Log files essentially contain confidential data that a typical user must not be able to access. It is a common practice to send log files to a secure location where it is not possible to modify the data, and only authorized personnel can view and analyze information.

System Scanning

System scanning is the process of analyzing the current security settings of a system or a network to identify and repair potential vulnerabilities. These vulnerabilities weaken the system security and open it up for possible attacks or security breaches against a particular system or against the entire network. System scanning is performed by software utilities, usually included with network operating systems. Third-party software tools may also be used for this purpose.

Apart from identifying weak or vulnerable areas of the system, system-scanning utilities can also be useful in ensuring system reliability and performance. These utilities make sure that password and account policies are strong enough to prevent unauthorized access. They test the response of a system or the network in scenarios that could lead to a potential attack by an outsider. An example of such an attack is the *Denial of Service (DoS)* attack.

System scanning tools are generally used to make sure that the system is accessible only through the use of acceptable means of inside and outside access. They are also used to create false attacks against the network to ensure that the network is capable of detecting the attacks and taking appropriate corrective action. Some of the popular scanning tools used for system scanning are the System Administrator's Tool for Analyzing Networks (SATAN) and Nessus. Both of these tools work in Unix and Linux environments. SATAN is mainly used to detect known vulnerabilities in a system and fix them. Nessus is a client/server-based tool that can even launch a false attack against a network. Nessus is very useful for scanning remote systems.

At the time of this writing, Microsoft plans to release *Windows Defender*, a real-time spyware monitoring tool for Windows-based systems. This tool will mainly be used to detect and block pop-up windows and detect performance problems.

Types of Attacks

Attacks on computer systems and networks are launched in several different ways and with several different techniques. Attacks on computer networks may be targeted at an application, a service, or the entire network. It may be an active or a passive attack. By definition, attacks can be classified into the following categories:

Active attack

When the person attacking a system or a network is actively involved in the process, the attack is said to be active. Active attacks can be easily detected. In most active attacks, the attacker quietly captures data transmitted on network wires and attempts to cause a partial or complete shutdown of a network service. DoS and Distributed Denial of Service (DDoS) are examples of active attacks.

Passive attack

When the person trying to attack a system or network is quietly monitoring the network for some condition to be met, or just collecting information to launch an attack, the attack is said to be passive. Examples of passive attacks include *sniffing*, *eavesdropping*, and *vulnerability scanning*.

Password attack

These attacks are launched using one or more methods of guessing the password of a legitimate user of the network. Examples of password attacks include *dictionary-based attacks*, *password guessing*, and *brute force attacks*.

Malicious code attack

When the attacker uses applications written specifically to cause damage to a system or network, the attack is said to be a code attack. Examples of code attacks include *viruses*, *Trojan horses*, *worms*, and *logic bombs*.

A brief description of different types of attacks are given in the following sections.

Denial of Service (DoS)

In computer security, a DoS attack is an attack on computer systems, services, resources, or the entire network that results in the unavailability of a network or its resources to its legitimate users. Potential targets of DoS attacks are the main components of Internet services such as high-profile web servers and DNS servers. The intent is to bring down an organization's web site(s). The attacker may use any of the following methods to launch a DoS attack:

- Try to flood the network in order to prevent legitimate network traffic from passing through.
- Try to disrupt the connection between two systems in order to prevent access to a service.
- Try to prevent a legitimate user from accessing a service or a resource.
- Try to disrupt service from a particular system or a part of the network.

DOS attacks generally do not cause an outage of all network services. They are targeted at specific services, such as the Domain Name System (DNS) service. If the attack on a DNS server is successful, the users may not be able to resolve domain names or even to connect to the Internet.

DoS attacks usually result in the following:

- A significant consumption of system or network resources such as CPU time, disk space, or network bandwidth. This is also termed as a *resource consumption attack*.

- The modification or change in the configuration of network hardware such as network servers, routers, and switches.
- The disruption of the network services and applications such as databases, applications, and web servers.

All of the given outcomes of a DoS attack prevent legitimate users from using a system, network services, or shared resources. The following are some examples of DoS attacks:

SYN flood
: A SYN flood attack is carried out by sending a flood of TCP/SYN packets with forged information about the sender. SYN flood attacks are discussed later in this section.

ICMP flood
: An ICMP flood attack includes *smurf attacks* and *ping floods*. A smurf attack is launched by using misconfigured network devices. Malicious packets are sent to all hosts on a particular network by using the broadcast messages. These packets carry false IP addresses of the sender. A ping flood attack is launched by sending a large number of ping requests to network hosts, which may result in the consumption of a significant amount of network bandwidth.

UDP flood
: A UDP flood attack is carried out by sending a large number of UDP echo packets to a large number of network hosts. The attacker uses a fake source IP address.

Land attack
: A land attack involves sending a spoofed (having false information) TCP SYN packet to a target network host. The packet contains the host's own IP address as its source and destination. The result is that after receiving the packet, the host continues to reply to itself until it crashes.

Nukes
: Nukes are malformed or specially crafted packets. They usually exploit an open TCP port on a network host to launch an attack. For example, WinNuke uses the NetBIOS open port 139 to send out-of-band data to a network host, causing it to crash.

Application-level floods
: Application-level floods usually cause *buffer overflows* in a system. The system becomes so confused that it consumes all of its resources—such as CPU time or disk space—and then eventually crashes. Buffer overflow is discussed later in this section.

An amplified form of DoS is the DDoS, which is explained in the next section.

Distributed Denial of Service (DDoS)

A DDoS attack is an amplified form of a DoS attack that is targeted at the entire network instead of at a single system or service. This is a two-step attack. The attacker first compromises a number of computers spread across the Internet and installs a specially created software application on them. The computers are known as *masters*. The application installed on these compromised computers or masters then helps the attacker further by installing the application on several more computers that are known as *zombies*. Zombies launch attacks on thousands of computers connected to the Internet and then collectively attack a particular Internet host to make it unavailable to legitimate users. In the event of a DDoS attack, it is nearly impossible to detect the originator of the attack because the attack takes place in multiple steps, and several Internet hosts are involved in attacking a particular Internet host.

Usually, the attacker first employs some kind of technique to detect vulnerabilities in Internet hosts. The applications that detect these vulnerabilities are known as *Rootkits*. Figure 11-4 illustrates the basic structure of a DDoS attack setup.

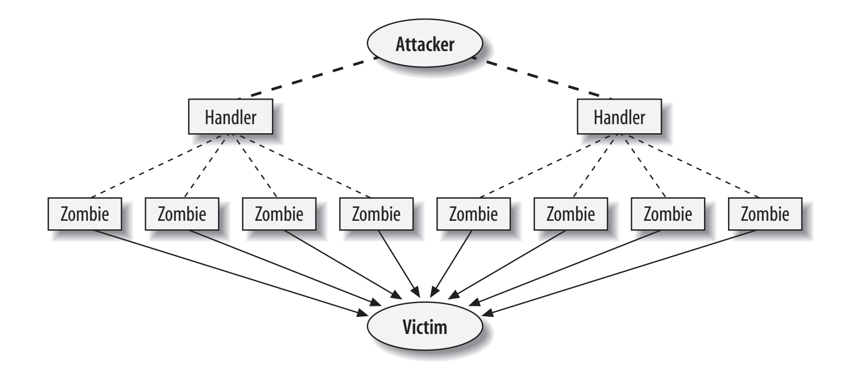


Figure 11-4. DDoS attack setup

In a nutshell, the computers or hosts involved in a DDoS attack include the following:

Master
: An Internet host on which the attacker installs the software application.

Zombie
: The intermediate Internet host that gets the client side of the application.

Target Host
: A particular host on the Internet that is subject to the DDoS attack.

DDoS attacks are essentially targeted at computers directly connected to the Internet. While some of the target computers become masters, others become zombies. Zombies act upon instructions from masters to launch a collective DDoS attack against the target Internet host.

The following describes the components of a DDoS:

Client
: This is the software application that is used by the attacker to initiate the DDoS attack. The client sends instructions to its subordinates to launch the attack.

Daemon

This is the component of the application that is installed and run on zombies to further launch attacks on target Internet hosts. The target Internet host becomes the victim of a simultaneous attack from multiple zombies.

Reflected DDoS attack. A reflected DDoS attack happens when large numbers of computers receive forged requests that otherwise appear to be legitimate. The IP address of the sender is forged using spoofing methods. All computers that receive the request reply to it. The replies go to the target or the victim computer. When the victim computer receives the (many) responses, it becomes flooded and unable to service legitimate clients. ICMP Echo requests are one of the several types of requests that can be used in reflected DDoS attacks. Other types of DDoS attacks that can be launched by zombies include SYN floods, UDP floods, etc.

SYN flood

The SYN flood, or *TCP/SYN*, attack utilizes a common weakness of TCP/IP. A TCP/IP session between two hosts is established using the exchange of *TCP/SYN*, *TCP/SYN-ACK*, and *TCP/ACK* messages. The attacker sends a large number of TCP/SYN messages to the target host with a forged source IP address. The server getting these requests treats these messages as connection requests and sends TCP/SYN-ACK messages to all of the forged IP addresses that do not exist. The result is that the server leaves the ports open to receive TCP/ACK messages from hosts that do not exist, and the response never arrives. These half-open connections are actually consumed resources of the server that otherwise would have been utilized by legitimate users to connect to the server. The server ultimately looks busy and denies connections to the actual clients.

IP spoofing

If you are pretending to be someone who you are not, you are spoofing. In other words, *spoofing* is the process of providing false identity about someone's identity in order to gain unauthorized access to secure resources on a system or the network. In computer security, attackers use IP spoofing in order to gain access to secure system resources or networks. Attackers send IP packets that contain a false IP address.

Computer attacks using IP spoofing can be categorized as follows:

Blind IP spoofing

Blind IP spoofing occurs when the attacker just sends IP packets to the target computer and does not usually wait for a response. The attacker is only making a guess that at some point he may be able to get a response from the target computer. If the attempt is successful, the attacker may further cause damage to the computer or get confidential information from the person communicating with the attacker.

Informed IP spoofing

Informed IP spoofing, or non-blind IP spoofing, occurs when the attacker is sure about getting a response from the target computer to begin a communication session. This may result in significant loss to the target computer or to the person communicating with the attacker. For example, the attacker may pose as a bank or an employee of a credit company and ask for confidential information from the victim.

Most IP spoofing occurs between trusted computers on the Internet or on internal networks of large organizations. Trust relationships between networks or domains usually allow users to log on to other domains without supplying credentials. By spoofing the IP address of a trusted computer, the attacker may be able to connect to the target computer without authentication.

The best protection against IP spoofing is to use packet filtering in networks. *Packet filtering* allows administrators to block packets that originate from outside the network but that carry IP addresses of hosts inside the network. Network routers usually handle this part. TCP/IP has built-in protection against IP spoofing as it uses sequential numbers when computers communicate to each other. Using encryption and mutual authentication can also prevent IP spoofing.

Man-in-the-Middle Attacks (MITM)

A MITM attack occurs when the attacker is actively listening or monitoring the communications between two hosts. The attacker is able to read, insert, or modify the messages being exchanged between the two hosts, without any of them knowing that the information is being compromised.

As noted earlier in the previous section, a TCP/IP communication session is established after a successful three-way handshake. The computer requesting a connection sends a TCP/SYN packet to the server, and the server then responds with a TCP/SYN-ACK message, which the computer requesting the connection accepts by sending a TCP/ACK message. This is illustrated in Figure 11-5.

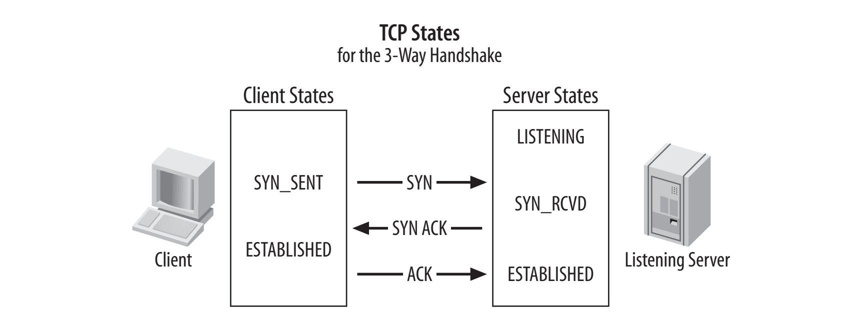


Figure 11-5. TCP/SYN process

When host A wants to communicate with host B, which is a server, it sends a TCP/SYN packet to host B. This packet contains the IP address of the source, which is host A. The attacker can place himself somewhere between hosts A and B and monitor the communication taking place between the two hosts. He can intercept the TCP sequence numbers and successfully use these to falsify information going to host B. From then onwards, the communication takes place between host B and the attacker, and host A keeps waiting for a response from host B.

MITM attacks remain a serious threat to many organizations, even those that use encrypted communications between systems and networks. The best protection against MITM attacks is to use encrypted messaging systems so that the attacker is not able to decrypt or intercept the communication taking place. Other methods of preventing MITM attacks include the following:

- Use strong mutual authentication.
- Use strong passwords.
- Use advanced techniques of authentication, such as biometrics.
- Use public key cryptography to encrypt information exchange.

Replay attacks

A replay attack is usually launched against an entire network in which the valid data transmitted across the network is repeated or delayed. This attack is the result of poor security in the TCP/IP protocol wherein TCP sequence numbers can be regenerated. For example, consider that Jeff wants to do some online banking. An attacker named Adam is monitoring the entire exchange of messages between Jeff's computer and the bank's server. Adam captures a significant amount of data during these transmissions and tries to repeat the transactions on the bank's server using this information.

In case the attacker is not able to capture the correct TCP sequence numbers, he tries to guess all kinds of numbers to get a correct sequence number to gain access to a secure server. This may cause the legitimate user's connection to drop.

To prevent replay attacks, session tokens can be used. In the preceding example, if session tokens are used, the bank's server would generate a session token for Jeff that would expire as soon as Jeff completed the transaction. Any replay by the attacker would not be successful. Other safeguards against replay attacks include use of timestamping, Secure Shell (SSH), IPSec, more randomization of TCP sequence numbers, and so on.

TCP/IP hijacking

TCP/IP hijacking, or *session hijacking*, refers to the capture of session information by an attacker to gain unauthorized access to the information. The attacker generally is able to hijack insecure TCP/IP sessions such as FTP, Telnet, Rlogin, or other unencrypted TCP/IP sessions. Internet cookies that store personal information about a user can also lead to an attacker getting confidential information and hijacking an active TCP/IP session. Cookies, which are stored locally on a user's computer, normally contain a user's login credentials such as the username and password. Several Internet-based applications heavily rely on cookies to initiate and maintain a communication session between the user's computer and the web server. The attacker would simply steal a user's cookie and hijack the TCP/IP communication session, while the legitimate user would get a "session expired" or a "session timeout" message. The user might consider it normal, and the attacker would continue to use the hijacked session for his personal gains.

TCP/IP hijacking can be prevented by using secure session keys, which are normally encrypted and randomized. In the case of Internet-based applications, SSL encryption should be used along with strong random session keys.

Weak keys

The term *weak key* refers to the method of generating a key for an encryption algorithm that would make the resulting encryption exhibit undesirable behavior. It is always preferred that the encryption algorithm used should not have any weak keys. The following encryption algorithms are said to contain weak keys:

DES
: The Data Encryption Standard (DES) is known to have a few weak keys, which cause the DES algorithm to behave identically in encryption and decryption processes.

RC4
: The weak Initialization Vectors (IV) in an RC4 algorithm can expose a wireless system to plaintext attacks. RC4 is very commonly used in popular protocols such as SSL.

IDEA
: It is easy to identify the weak keys used in the International Data Encryption Algorithm (IDEA) in a plain-text attack.

Blowfish
: The Blowfish algorithm is known to use weak keys that result in production of bad substitution boxes (S-Boxes).

No encryption algorithm is actually designed to have weak keys. When all the keys used in an algorithm are equally strong, the key design is known as *flat keyspace*.

Password attacks

Password attacks occur when an attacker attempts to get a user's password by guessing it or finding it stored in a database using a *dictionary attack* or a *brute force attack*. A password attack is known as *password cracking*. These attacks are discussed in the following sections.

Password guessing. Many users do not understand the purpose and usefulness of strong passwords and choose weak passwords that anyone can easily guess. It is also a common practice to use passwords that contain very few characters, contain names of hometowns, pets, or dates of birth. Sometimes, users keep their passwords blank for quick logon. Most of the newer network operating systems do not allow blank or weak passwords. Particularly when password policy is forced in a Windows Server 2003 domain, users are not allowed to keep blank passwords or passwords that contain full or part of their usernames. They are also forced to change their passwords at regular intervals.

It is also very common for users to keep the default password assigned to them. This makes it easy for an attacker to guess the user password to gain unauthorized access to the system. This is particularly true with network hardware when administrators forget to change the default passwords used to configure the hardware.

Dictionary attacks. A dictionary attack also exploits the tendency of users to choose weak passwords. Password-cracking applications come with built-in "dictionaries" or lists of words that can be easily used to guess a weak password by multiple combinations of characters. The cracking program tries to guess a password by encrypting each word in the dictionary, each time checking to see whether there is any match between the encrypted password and the generated password. These applications are so efficient that they can try thousands of combinations per second.

Brute force attack. A brute force attack is the process of defeating an encryption scheme by trying a large number of possibilities. The applications written to launch brute force attacks try to use different combinations of keys to decrypt an encrypted message. In the context of password guessing, the brute force attack is perhaps a last resort that an attacker can use to crack a password. Brute force techniques usually speed up the process of guessing passwords.

Most modern network operating systems store passwords in an encrypted form. The encryption is carried out by using a *one-way hashing* function. *Message Digest 5 (MD5)* is one of the common hashing functions used to create a hash of stored passwords. One-way hashing ensures that once the password is hashed, it cannot be restored. When a user enters a password, it again goes through the same hashing function and the output is compared to the stored value. If the values match, the user is allowed access. An attacker using the brute force technique will not be able to launch a password attack unless he obtains a copy of the username and the hashed passwords. If the attacker is able to guess a password using a brute force attack, the password is considered cracked.

Buffer overflow

A buffer overflow is a system condition that causes a breach in system security or a memory usage exception resulting in a system crash. It can be a result of either a programming error or an active attack on the system. An attacker may launch a buffer overflow attack by writing malicious code specifically aimed at filling all the memory buffers of the target system. Buffer overflow may also be due to an incorrect choice of a programming language that cannot handle memory buffers appropriately. Buffer overflows may cause systems to produce undesired results or even crash.

Software exploitation

Software exploitation refers to taking undue advantage of a software bug, glitch, or vulnerability in an application code to gain unauthorized access to a system or to launch a DoS attack against the system. Software exploitation is closely related to buffer overflows. Software written by in-house programmers may leave security holes that could be used by attackers to launch such attacks as the buffer overflow attack. Software exploitation may also result in escalated privileges being granted to an unauthorized user.

Back door

A back door is the process of bypassing the normal authentication process of a computer to gain access to its resources. There are several applications specifically designed to gain back door access to systems and networks. A slight modification to an installed application on a system can also cause back door entry to a system. Even legitimate applications can cause back doors and remain invisible to a normal computer user. Examples of such applications are PCAnywhere (Symantec) and Back Orifice, both used for remote administration of computer systems.

Trojan horses and *rootkits* are also termed as back doors. While the Trojan horse appears to be a useful application to the unsuspecting user, rootkits are designed to look for vulnerabilities in a system. An attacker can easily mask his presence using a rootkit. These applications grant remote access to the attacker.

Back doors are of two types: *symmetric* and *asymmetric*. A symmetric back door is the traditional type, and anyone who finds one can use it to exploit the system. The asymmetric back door is specially designed to allow system access to only the creator of the program.

It is possible to detect malicious software, including back doors, but when a legitimate application acts as a back door or is configured to act as one, the task becomes difficult.

Types of Malicious Codes

Malicious code or *malware*, is a software application that is designed to infiltrate a user's computer without his knowledge or permission. Malware includes viruses, Trojan horses, worms, and applications such as adware, spyware, botnets, and loggers. The following are main categories of malware:

Viruses and worms
: These applications are written to infect a system without any obvious commercial gains.

Trojan horses, rootkits, and back doors
: These applications are written to infect the target system and conceal the identity of the attacker. They appear to the user as if they are in his interest. If the user installs the application, he becomes a victim.

Spyware, botnets, and adware
: These applications are written specifically to gather information about the active user on the system in order to gain some kind of commercial profits. These applications generally appear as pop-up windows on the user's computer.

Viruses

A computer *virus* is a self-replicating application that inserts itself into other executables on the computer and spreads itself using that executable. A computer virus is essentially malware that is created for the sole purpose of destroying a user's data. The executable file in which the virus inserts itself is called the *virus* *host*. A virus needs an executable file to spread itself. In order to let the virus work or infect a computer it must first load into the memory of a system, and the system must then follow the instruction code contained in the virus program.

A computer virus can travel from one computer to another, and infects every computer on its way—just like a real life infection. A virus can infect data stored on floppy disks, in email, on hard disks, and even on network storage devices. Remember that the infected program must be executed before the virus can spread to infect other parts of the system or data.

The following are different types of viruses:

Boot sector virus
: A boot sector, or *BootStrap* virus infects the first sector on the hard disk. This sector is used to boot or start up the computer. If this sector is infected with a virus, the virus becomes active as soon as the computer starts.

Parasitic virus
: A parasitic virus infects an executable file or an application on a computer. The infected file actually remains intact, but when the file is run, the virus runs first.

Worms

A worm is a computer virus that does not infect any particular executable or application but resides in the active memory of computers. This virus usually keeps scanning the network for vulnerabilities and then replicates itself onto other computers using those security holes. The effects of worms are not easily noticeable until entire system or network resources appear to have been consumed by the virus.

The most common type of worm is the email virus that uses email addresses from the address book of a user to spread itself.

Trojan horses

A Trojan horse, or simply a *Trojan*, is a malicious code that is embedded inside a legitimate application. The application appears to be very useful or interesting and harmless to the user until it is executed. Trojans are different from other computer viruses because they must be executed by the victim user who falls for the interesting "software."

Trojans fall into the following two categories:

- Software applications that are otherwise useful but have been corrupted by a malicious user by inserting code into the application that triggers itself when the application is executed.
- Software applications that are specifically created to cause damage to the user's computer when executed. These types of Trojans are usually hidden inside games, image files, or software that appears to give access to some free stuff to the user. The purpose of the Trojan is to somehow trick the user into executing the application.

Most of the modern Trojans contain code that is basically used to gather information about the user. These Trojans fall into the category of *spyware* and appear as pop-up windows on the user's computer screen. Some Trojans are written very precisely to allow the user's computer to be controlled remotely by the attacker.

The main difference between a virus and a Trojan is that viruses are self-replicating programs while Trojans need some action on the part of the user. If the user does not fall into the trap of the Trojan, it does not execute. So, the next time you notice a pop-up window offering you free emoticons or desktop screen savers, be careful. A Trojan may be waiting to execute in order to steal personal information stored on your computer.

To protect computers from Trojan horses, the following precautions can be taken:

- Keep your operating system updated with the latest service packs, security patches, and hotfixes offered by the manufacturer.
- Install antivirus software on your system and keep it updated.
- Configure your email settings so that attachments contained in incoming mail do not open automatically. Some Trojans come embedded within email attachments.
- Do not use peer-to-peer sharing networks such as Kazaa or Limewire. These leave open ports on your computer when you are sharing your data with others on the Internet. These networks are generally unprotected from Trojans and other viruses.

Some of the well-known Trojans include Back Orifice (and Back Orifice 2000), Beast Trojan, NetBus, SubSeven, and Downloader EV.

Logic bombs and time bombs

Logic bombs and time bombs are types of specially written malicious code that reside in a particular system and wait for some condition to be met or for a specific event to happen before it triggers itself. A logic bomb is a virus, and a time bomb is a Trojan. A programmer may have a special code written to delete all data and other files from his system as soon as he leaves the company (a logic bomb). The action may trigger as soon as the administrator deletes or disables the programmer's account from the network. Another programmer may write code that waits for a specific date such as April 1st (April Fools' day) to trigger it (a time bomb).

> Remember the difference between logic bombs (virus) and time bombs (Trojan) as they are related to computer security.

Wardialing

Wardialing is used in remote access networks to gain access to a remote access server by dialing a large block of known telephone numbers. The attacker uses an application known as *war dialer* to automatically dial a large block of numbers to search for a server that will respond. These types of applications also log whatever information they find on the remote servers. It is very uncommon to find any connected modems without the knowledge of administrators, but the attacker works on the theory of probability. If he is able to access any server that has a connected modem, and it responds to the attackers dialing attempts, the attacker is successful in penetrating into the network of the organization.

Dumpster diving

Dumpster diving is the process of physically "diving" into trash containers and collecting pieces of information from corporate or domestic waste. People often throw away pieces of paper or other items that contain personal information such as their name, address, phone number, date of birth, Social Security number, etc. A dumpster diver may collect this information and use it for his benefit. In large organizations, users even throw away pieces of paper that contain their usernames and passwords. To prevent dumpster diving, it is useful to get a good paper shredder so that papers are destroyed before they are thrown into trash.

Risks Involved in Social Engineering

Social engineering refers to the process of getting personal or confidential information about someone by taking him into confidence. The so-called "social engineer" generally tricks the victim over the telephone or on the Internet into revealing sensitive information. Instead of exploiting any security vulnerabilities in computer systems, the attacker capitalizes on the victim's own tendency of trusting someone.

Social engineering also involves face-to-face interactions between a computer user and an attacker to get access to the computer by taking the victim into confidence. It may also come in the form of an email attachment that asks the user to give away confidential information to the sender of the message. *Phishing* attacks are very common outcomes of social engineering. In a phishing attack, users of computer systems frequently indulge in interesting chats over the Internet or over the phone with unknown attackers, and witlessly reveal sensitive information such as their password or credit card number.

Unfortunately, no technical configuration of systems or networks can protect an organization from social engineering. There is no firewall that can stop social engineering attacks. The best protection against social engineering is to train the users about the security policies of the organization.

Identifying and Disabling Nonessential Services and Protocols

When you install an operating system, several services and protocols are installed by default. Chances are good that most of these services or protocols will never be used, but they may leave the system vulnerable to outside attacks. In order to protect and secure the system from potential attacks, it is necessary that any nonessential services and protocols be identified and disabled or be completely removed from the system. This not only improves system performance but also helps to fill in possible security holes.

Nonessential services

Nonessential services include those system services and applications that are not used on a server or a desktop computer. For example, services such as the Dynamic Host Control Protocol (DHCP), DNS, FTP, Telnet, or the Remote Access Service (RAS) are mostly configured on servers and may never be used on desktops. These services not only consume system resources but also make the system vulnerable to outside attacks. These and other services that are not required on a system should be disabled as part of your actions to maintain a secure network environment. If a system is not a part of the Active Directory domain, you may remove the directory services and the DNS from a Windows system. Similarly, if a system does not require file and print services, these may be disabled or removed.

Nonessential protocols

Nonessential protocols are not used on a desktop or a server. For example, if a system is not connected to a legacy Windows systems, you may remove the NetBIOS protocol. Similarly, you may disable the Internet Control Message Protocol (ICMP) if you do not want the system to respond to system management queries. If there are no NetWare servers in the network, there is no reason to keep the Internet Packet Exchange/Sequenced Package Exchange (IPX/SPX) protocol installed on any system.

There may be situations where you need some protocols and services installed on certain systems but not on others. A thorough study of all services and protocols that are installed by default on each system may be a good idea to help decide whether the services or protocols are not required and can be disabled.

> You must be very careful when disabling or removing nonessential services and protocols on a system. Some services depend on other services to work that otherwise may seem to be nonessential. Removing services that other services depend on may leave your system inaccessible to other services.

Communication Security

Communication security refers to protection of data transmitted over the network cables or wireless networks. The main purpose of communication security is to ensure authenticity, confidentiality, integrity, and availability of data while it is transferred from one location to another. Measures taken to ensure communication security include securing remote access systems, messaging systems, wireless networks, and web services. Secure transmission methods must be implemented whether the data is transmitted between internal users of the organization within a single location, or between an organization and its trusted external users located at multiple remote locations.

In this section, I will cover the following aspects of communications security:

- Remote access
- Email security
- Internet security concepts
- Directory Services security
- File Transfer protocols
- Wireless communications

Remote Access

This section covers remote access protocols and authentication methods, their vulnerabilities, and methods of protection against possible attacks. There are several technologies used to provide remote access to users who require access to the internal resources of an organization. Administrators must ensure that these users are granted secure access to the internal network, but at the same time, unauthorized access must be prevented. There has to be a balance between implementing security and granting access. Remote access security is generally implemented using secure protocols and strong authentication techniques, and grants only as much access to a remote user as he needs to do his job. The principle of least privilege is commonly applied while granting remote access.

The Security+ exam expects you to have an in-depth knowledge of remote access protocols, authentication techniques, and security issues related to the protocols. This essentially means that you must be familiar with remote access protocols and services used for authentication. The following sections cover some of the commonly used protocols and services used for remote access.

802.1x

802.1x is an authentication protocol standard used in wireless local area networks (WLANs). This standard was developed by the Institute of Electrical and Electronics Engineers (IEEE) to replace the 802.11 standard in order to provide enhanced security to WLANs. This standard was developed mainly to overcome the vulnerabilities in the 802.11 standard and is known as *Wired Equivalent Privacy (WEP)*. Wireless networks use radio frequencies and are often subject to eavesdropping attacks. 802.1x provides a secure point-to-point connection between a wireless Access Point (AP) and a host computer. 802.1x is based on the Extensible Authentication Protocol (EAP) and is usually implemented in closed wireless networks to provide authentication.

802.1x authentication works using the following two components:

Supplicant
This refers to the software component installed on the user's computer that needs access to a wireless access point.

Authenticator
This refers to a centralized wireless access point. The authenticator forwards the authentication request to an authentication server (such as a RADIUS server).

When a user (the supplicant) wants access to a wireless network, the 802.1x protocol sends the request to an access point (the authenticator). After the communication begins, the supplicant is placed into an unauthorized state. There is an exchange of EAP messages between the authenticator and the supplicant wherein the authenticator requests the credentials of the supplicant. After receiving the credentials, the request is sent to an authentication server such as RADIUS. The authentication server either accepts the credentials of the supplicant and grants access or rejects the credentials, thereby rejecting the connection request. If the connection is accepted, the user is placed into an authorized state.

> Be careful not to confuse the 802.1x authentication standard with 802.11x wireless standards. You will learn about 802.11 standards later in this chapter.

Extensible Authentication Protocol (EAP). EAP is a widely used authentication standard employed by wireless and point-to-point remote access networks. The EAP standard has been adopted by the Internet Engineering Task Force (IETF). EAP is a universal authentication standard and can also be used in wired local area networks (LANs). It is basically an authentication framework and not an authentication mechanism. The 802.1x standard is also based on the EAP standard. There are several authentication methods or mechanisms that are based on EAP standards. Some of these are as follows:

Extensible Authentication Protocol-Transport Layer Security (EAP-TLS)

EAP-TLS is considered to be one of the most secure authentication protocols and is widely supported by many vendors in the IT industry. It uses PKI to secure communications to the RADIUS server. Since the task of creating and maintaining certificates for clients is major, EAP-TLS is rarely deployed by organizations.

Extensible Authentication Protocol-Tunneled Transport Layer Security (EAP-TTLS)

EAP-TTLS is widely supported across various platforms. It offers good security and uses PKI certificates, but only for the authentication server.

Extensible Authentication Protocol-Message Digest 5/Challenge Handshake Authentication Protocol (EAP-MD5/CHAP)

EAP-MD5/CHAP uses an MD5 one-way hash function but offers minimal security. The MD5 one-way hash is prone to dictionary attacks.

Protected EAP (PEAP)

PEAP was jointly developed by Cisco, Microsoft, and RSA Security to secure the authentication process. Its design is very similar to EAP-TTLS, and it requires PKI certificates on the authentication server only. The TLS tunnel is provided to protect user authentication.

There are two versions of PEAP, as follows:

Protected Extensible Authentication Protocol version 0/Microsoft Challenge Handshake Authentication Protocol (PEAPv0/MS-CHAPv2)

This protocol was developed jointly by Microsoft, Cisco, and RSA Security. It is widely supported by most network operating systems. Microsoft's implementation of server-side PKI certificates use PEAPv0-MS-CHAPv2. This service is known as the *Internet Authentication Service (IAS)*.

Protected Extensible Authentication Protocol version 1/Generic Token Card (PEAPv1/GTC)
This protocol was developed by Cisco.

Lightweight Extensible Authentication Protocol (LEAP)
LEAP is proprietary to Cisco. None of the Windows operating systems support this. It provides minimal security because it is prone to dictionary attacks like the EAP-MD5 is.

EAP-FAST
FAST stands for *Flexible Authentication via Secure Tunneling*. EAP-FAST was developed by Cisco to overcome drawbacks in its EAP-LEAP protocol. Although Cisco claims this protocol is more secure than EAP-LEAP, it still suffers from vulnerabilities of poor implementation.

EAP-SIM
EAP-SIM is used for authentication and session key distribution in Global System for Mobile (GSM) communications that use a Subscriber Identity Module (SIM).

Remote Authentication Dial-In User Service (RADIUS)
RADIUS is one of the most widely supported protocols for authentication, authorization, and accounting for remote access systems. RADIUS is covered later in this section.

For the Security+ exam, you will not need to go into much detail on different EAP protocols, but you must remember the main protocols based on EAP standards.

Vulnerabilities in the 802.1x authentication protocol. WEP uses the RC4 encryption algorithm, also known as *stream cipher*. This algorithm is known for its simplicity, but it is vulnerable because of its weak keys. RC4 falls short of security standards set by cryptographers. It is not recommended for new applications. RC4 works by expanding a short key into a key stream. The key stream generated by RC4 is slightly biased in favor of a certain sequence of bytes. The sender combines the key stream with the original message, which is in plain text, to create cipher text. The receiver of the message uses a similar key to generate an identical key stream. When the key stream is applied to the cipher text, the receiver can view the original message in plain text.

Since the RC4 algorithm utilizes the same key twice, an attacker can easily capture the key to recover the plain text. The vulnerabilities in the RC4 algorithm were discovered by Fluhrer, Martin, and Shamir. They were able to crack the WEP keys by guessing the first byte of the plain text. This is commonly known as *Fluhrer, Martin and Shamir Attack*. They discovered that the first few bytes of the key are strongly nonrandom, which may result in leaking information about the key.

AirSnort (*http://airsnort.sourceforge.net*) and *WEPCrack* (*http://wepcrack.sourceforge.net*) are two popular tools available on the Internet for testing the vulnerabilities of WEP keys. These tools can recover the keys or even crack the keys employed in the 802.1x authentication using the RC4 algorithm. While AirSnort is mainly used for recovering encryption keys used for 802.1x authentication, the WEPCrack tool is simply used for cracking (or breaking) the encryption keys. These tools work by capturing a large number of packets (about 5 to 10 million) transmitted over network media.

Virtual Private Networking

As the name suggests, a VPN provides a secure means of communication between remote users of an organization, between different locations of an organization, or between distinct organizations. The communication takes place using a public network such as the Internet. VPN is a cost-effective way to provide connectivity to remote users of the organization. This technology saves money for those organizations that have a large number of telecommuting employees. These employees can connect to the internal resources of the organization from anywhere because of the global availability of the Internet. All they need to do to connect to the organization's network is to simply connect to the local Internet Service Provider (ISP). VPN technologies employ secure authentication and data transmission protocols that work by creating a tunnel in the publicly accessible network (the Internet). The tunneling protocols encapsulate the authentication and other data within other packets before transmitting over the Internet.

VPN utilizes the following types of protocols for tunneling purposes:

Carrier protocols
: These protocols are used by the Internet to transfer data from one point to another over the Internet.

Encapsulating protocols
: These protocols are used to wrap the original data before it is transmitted over the Internet. PPTP, L2TP, IPSec, and SSH are examples of encapsulating protocols.

Passenger protocol
: This is the original data that is transmitted by the user.

VPN can be implemented in one of the ways discussed in the following sections.

Remote Access VPN. A Remote Access VPN is also known as *Private Virtual Dial-up Network (PVDN)*. This type of VPN provides remote access to remote users over the Internet. The remote user is responsible for creating the tunnel for starting the communication. He dials into the local ISP, which provides Internet connectivity to the user. The user then connects to the secure intranet site of the organization, which is permanently connected to the Internet.

A Remote Access VPN is a great solution for an organization that has a large number of users spread across different locations. By using VPN technologies, organizations can save on costs involved in having users that directly dial in to the organization's internal network.

Site-to-Site VPN. A Site-to-Site VPN is established between different offices of the same organization spread across multiple physical locations. This can be a very cost-effective solution because the organization does not have to maintain dedicated wide area network (WAN) connections between physically separated locations. Organizations may choose from software implementations of VPN, such as Microsoft's Routing and Remote Access Service (RRAS) in Windows Server 2003 or from hardware solutions such as CheckPoint or SonicWALL. Software-based VPNs require proper planning and secure implementations, as these are prone to vulnerabilities of the operating system. Hardware implementations are expensive but are generally more secure than their software counterparts. Figure 11-6 shows a typical Remote Access VPN setup.

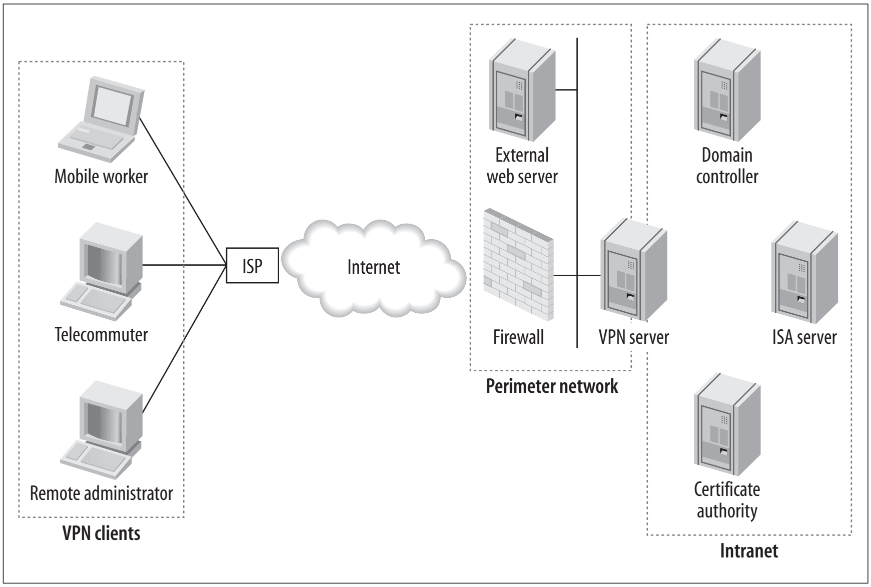


Figure 11-6. Remote Access VPN

As noted earlier, VPN essentially depends on a tunneling protocol to successfully and securely transmit data from one location to another using the Internet. The choice of tunneling protocol depends on the solution chosen to implement a VPN. The tunneling process is usually transparent to the end user, who only has to provide appropriate credentials to gain access to the internal resources of the organization. The only requirement is that each end of the tunnel must be able to support the selected tunneling protocol. Commonly used protocols associated with VPN implementations include the following:

- PPTP: Point-to-Point Tunneling Protocol
- L2TP: Layer 2 Tunneling Protocol
- IPSec: IP Security
- SSH: Secure Shell

These protocols are discussed later in this section. Remember that aside from using secure tunneling protocols, organizations may also require clients to authenticate using centralized authentication servers such as the RADIUS server, discussed next. Many large ISPs are now offering VPN solutions for small and medium-sized organizations that do not want to get involved in setup, maintenance, and administration tasks.

Remote Authentication Dial-in User Service (RADIUS)

RADIUS is used to provide centralized authentication for remote users connecting to the internal network of an organization through a simple dial-up, VPN, or wireless connection. When a remote user needs access to the internal resources of an organization, he must provide his credentials to the Network Access Server (NAS), which in turn sends the user's credentials to the RADIUS server for authentication. If the RADIUS server authenticates the user, the connection request is accepted; otherwise, the connection is refused. RADUIS is essentially an authentication, authorization, and auditing service used in medium and large organizations including ISPs.

RADIUS servers can either work as standalone servers to authenticate all connection requests coming from outside users, or they can be a part of a distributed RADIUS setup. Larger organizations deploy multiple RADIUS servers in order to distribute the authentication load. These servers support several popular protocols such as PAP, PPP, CHAP, and EAP.

When a remote or wireless user sends a connection request, the RADIUS authentication process takes place as follows:

1. The user attempts to connect to the RAS or NAS server of the organization. The user is requested to supply his credentials, which in most cases are his username and password.
2. The RAS/NAS server encrypts the credentials of the user using a shared secret and forwards the encrypted authentication request to the RADIUS server.
3. The RADIUS server makes an attempt to verify the user's credentials against its own database or against a centralized database such as Windows Server 2000/2003 Active Directory.
4. If the user's credentials match those stored in the centralized database, the server responds with an access-accept message. If the user's credentials do not match the stored credentials, the server sends an access-reject message.
5. The RAS/NAS server acts upon receipt of access-accept or access-reject messages and grants or denies connection to the remote user appropriately.
6. If the connection is granted, the RADIUS server may also be configured to automatically assign an IP address to the remote client. In larger organizations, dedicated DHCP servers usually handle automatic assignment of IP addresses.
7. When the user wants to terminate the connection, the RAS/NAS server notifies the RADIUS server of the terminated connection.

Most implementations of RADIUS servers are prone to buffer overflow attacks. An attacker may flood the memory buffer of RADIUS servers in order to make it unavailable to legitimate remote users. Buffer overflow attacks can even bring down a server that is vulnerable to such attacks.

Terminal Access Controller Access Control System (TACACS)

TACACS is another type of remote access authentication protocol that provides centralized authentication in Unix environments. One major disadvantage of

TACACS is that it supports only authentication and authorization—it does not provide accounting. The centralized authentication server is known as the *TACACS Daemon*, or simply *TACACSD*. TACACS uses User Datagram Protocol (UDP) port number 49.

Cisco developed another version of TACACS and named it *Extended TACACS*, or *XTACACS*. This protocol was not widely accepted. Both TACACS and XTACACS were replaced by TACACS+, discussed next.

TACACS+

TACACS+ was developed by Cisco to provide centralized authentication for remote access. TACACS+ supports authentication, authorization, and accounting. It also supports separation of all of these functions on separate databases instead of using a single database server, as is done in TACACS protocol. This protocol is not compatible with TACACS and XTACACS. Unlike the TACACS protocol, TACACS+ uses Transport Control Protocol (TCP) as its transport on port number 49.

> For the Security+ exam, remember that RADIUS uses port numbers 1812 and 1813; TACACS uses UDP port 49 while the TACACS+ protocol uses TCP port 49 as its transport. RADIUS combines the authentication and authorization in one user profile while TACACS+ provides authentication, authorization, and accounting, and is capable of separating these functions.

Both TACACS and TACACS+ protocols have vulnerabilities that make these protocols prone to attacks. Vulnerabilities in TACACS and TACACS+ protocols include the following:

- The sequence numbers of TCP/IP packets in TACACS+ always start with 1. This makes TACACS+ vulnerable to replay attacks.
- TACACS+ is prone to birthday attacks, due to relatively short session IDs.
- TACACS+ is prone to buffer overflow attacks.
- The accounting data in TACACS+ transmissions is not encrypted, which makes it vulnerable to attackers.
- It is very easy to steal passwords in TACACS+ using a packet-sniffing tool.

Point-to-Point Tunneling Protocol (PPTP)

PPTP is a popular tunneling protocol used to implement VPNs. It uses TCP port 1723 and works by sending a regular PPP session using a Generic Routing Encapsulation (GRE) protocol. A second session on TCP port 1723 is used to start and maintain the GRE session.

PPTP is easy to configure and supports Unix, MAC, and Linux as its clients. It is supported on almost all major versions of Microsoft Windows. Due to its low administrative costs, PPTP is the choice of many administrators for VPNs that require medium security. It is commonly used in Microsoft networks, which use Microsoft Point-to-Point Encryption (MPPE) for encrypting data.

Following are some of the limitations of PPTP:

- It cannot be used if the RAS/NAS servers are located behind a firewall.
- It works only in IP networks.
- When used alone, it does not provide encryption for authentication data. Only the transmissions after the initial negotiations are encrypted.

Layer 2 Tunneling Protocol (L2TP)

L2TP is another tunneling protocol that is widely supported by most vendors in the IT industry. It uses the *Data Link layer* (Layer 2 of the OSI model) to carry data from one point of the tunnel to another over the Internet. This protocol uses UDP port 1701 for transport. L2TP offers the combined benefits of the PPTP and the L2F (Layer 2 Forwarding) protocol from Cisco. It is considered a major improvement over PPTP, but it still lacks encryption capabilities when used alone. A combination of L2TP and IP Security (IPSec) is generally used to provide secure transmissions for VPN connections. L2TP/IPSec can be used behind firewalls provided UDP port 1701 is opened for incoming and outgoing packets. Besides this, both ends of the communications must support the L2TP/IPSec protocols.

Some of the advantages of using the L2TP/IPSec combination over PPTP for implementing VPNs include the following:

- L2TP/IPSec requires two levels of authentication: computer or network hardware authentication and user-level authentication. This provides better authentication security.
- IPSec provides confidentiality, authentication, and integrity for each packet. This helps prevent replay attacks. PPTP provides only data confidentiality.
- IPSec establishes *security associations (SA)* during the transmission of the user-level authentication process. This ensures that the authentication data is not sent unencrypted. This is an advantage over PPTP in which the user-level authentication is never encrypted.
- L2TP/IPSec supports the use of RADIUS and TACACS+ for centralized authentication, while PPTP does not.
- L2TP/IPSec can be used on top of several protocols such as IP, IPX, and SNA, while PPTP can be used only with IP.

Internet Protocol Security (IPSec)

IPSec is a standardized framework used to secure *Internet Protocol (IP)* communications by encrypting and authenticating each IP packet in a data stream. This protocol ensures confidentiality and authentication of IP packets so that they can securely pass over a public network such as the Internet. IPSec is considered to be an “open standard” because it is not bound to a particular application, authentication method, or encryption algorithm. IPSec is implemented at the Network layer (Layer 3 of the OSI model). This makes IPSec independent of application compatibility.

IPSec can be implemented in any of the modes that are described in the next sections.

Transport mode. When implemented in transport mode, only the *payload* (the actual message or data) inside the IP packet is encrypted during transmission. The IP header is not encrypted. This results in better transmission speeds. Transport mode is generally implemented in *host-to-host* communications over VPNs or inside a local area network (LAN).

Tunnel mode. When implemented in tunnel mode, the entire IP packet is encrypted. This includes the IP header (AH) as well as the data (ESP) (AH and ESP are discussed next). The advantage is that both the IP header and the data inside the IP packet are secured. This comes at the cost of transmission speed. Tunnel mode IPSec is implemented in gateway-to-gateway VPNs.

IPSec components. IPSec is made up of two distinct security components: Authentication Header (AH) and Encapsulating Security Payload (ESP), described here:

Authentication Header (AH)
The AH protocol secures data or payload by signing each IP packet to maintain its authenticity and integrity.

Encapsulating Security Payload (ESP)
The ESP protocol also ensures authenticity and integrity of data but adds confidentiality to the data that uses encryption techniques.

AH and ESP can either be used together or separately. When they are used together, the sender and receiver of data can be assured of complete security.

> Using AH alone ensures authenticity and integrity (but not confidentiality), while the use of ESP ensures authenticity, integrity, and confidentiality.

IPSec authentication. As noted earlier, IPSec ensures authenticity, integrity, and confidentiality of data. IPSec uses the Internet key exchange (IKE) mechanism to authenticate the two ends of the tunnel by providing a secure exchange of shared secret keys before the transmission starts. Both ends of the transmission use a password known as *preshared* key. Both ends exchange a hashed version of the preshared key during IKE transmissions. Upon receipt of hashed data, it is recreated and compared. A successful comparison is required to start the transmission.

IPSec can also be used for *digital signatures*. A digital signature is a certificate issued by a third-party Certificate Authority (CA) to provide authenticity and *no-repudiation*. Non-repudiation means that the sender cannot deny that he sent the data and can be held responsible for it.

IPSec uses *Security Association (SA)*, which determines how the two ends of the tunnel will handle AH and ESP. SAs can be created either manually or by using the *Internet Security Association Key Management Protocol (ISAKMP)*. ISAKMP is a framework that describes how SAs are negotiated, established, modified, and deleted. It is a preferred method and greatly reduces the time required to set up and start IPSec-based communications.

Secure Shell (SSH)

SSH is mainly used for secure communications between a server and a remote client. It is considered a replacement of file transfer protocols such as FTP, telnet, and rlogin, and uses TCP port number 22. It ensures confidentiality and integrity of data transmissions between a server and a remote client. SSH starts the communication before the two ends exchange usernames and passwords. Data security is ensured using *session keys*. SSH provides protection against different types of attacks such as packet sniffing, IP spoofing, and modification of data.

> Remember the ports used by different protocols. PPTP uses TCP port 1723, L2TP uses UDP port 1701, and SSH uses TCP port 22.

Vulnerabilities in Remote Access Services (RAS)

Remote Access Services are prone to the following types of attacks:

Eavesdropping
This means to silently listen to the network traffic and capture as much data as possible. This is considered a passive attack because the attacker is just listening to and capturing data, but she is not modifying it.

IP spoofing
Since the information about the sender and the receiver is contained in IP headers, it is easy for an attacker to listen to the IP packets. IP spoofing occurs when the attacker constructs packets so that they may appear to the receiver as if they are being sent by the legitimate sender.

Data modification
This occurs when someone changes the data being transmitted on the network media. This is a kind of Man-In-The-Middle attack. The attacker listens to and captures the traffic passing between the host and the client and then inserts fake responses that appear legitimate to the host or the client. The best protection against data modification is to use IPSec with digital signature.

Administrative and user errors
These errors may occur during configuration of network and remote access devices, which may leave security holes in the entire setup.

Email

Email security is of prime concern to every computer user, whether an individual or an organization. Since email messages may contain confidential, personal, or business information, it is important that only the intended recipient of the message receives and reads the message. Sending an email message from one person to another involves several components of the transaction: the sender, the receiver, the email client application, the email servers, and the transfer protocols that are used to carry the message from one network to another. Most email clients allow messages to be formatted in plain text or in HyperText Markup Language (HTML).

When sending an email to a recipient, the sender uses the recipient's email address, which is in the format *someone@somedomain.com*. The message first goes to the sender's email server. Some of the popular email servers include Microsoft Exchange, Lotus Notes, and Sendmail. The email server looks at the top-level domain in the email address and tries to resolve the DNS name of the recipient from one of the DNS servers on the Internet. The DNS server locates the *mail exchange (MX)* record for the *somedomain.com* domain to obtain the IP address of the email server. After this IP address has been located, the message is forwarded to the recipient email server, which in turn drops the message into the actual recipient's mailbox.

Since there are several steps involved in sending and receiving email, it is important that the messages be secured to prevent data theft. The best protection is to use encryption. Encryption ensures that only the recipient is able to view the message. Anyone else who gets the message by chance or by capturing the message is not able to decrypt it. *Pretty Good Privacy (PGP)* and *Secure/Multipurpose Internet Mail Extensions (S/MIME)* are two popular methods used to encrypt email messages. These are discussed in the following sections.

Multipurpose Internet Mail Extensions (MIME)

MIME is an extension of Simple Mail Transfer Protocol (SMTP). Internet mail is so closely associated with SMTP that it sometimes is referred to as *SMTP/MIME*. MIME allows inclusion of audio, video, images, and other types of files inside the email messages. It works by inserting a header in the beginning of the message so that the email client at the recipient end can choose an appropriate application to open the data included with the message. When the message arrives, the recipient email client, (such as Microsoft Outlook) associates these files with appropriate programs to open them. For example, if an email message contains a video file, Microsoft Outlook will automatically launch Windows Media Player to run the video.

Secure/Multipurpose Internet Mail Extensions (S/MIME)

S/MIME was developed by RSA Data Security to overcome the security vulnerabilities of MIME. S/MIME digitally signs the email message using public encryption to ensure authenticity, integrity, and confidentiality of email messages. It also offers non-repudiation of the message, which means that the sender of the message cannot deny that he sent it. S/MIME is a standard that describes how all of these security functions are to be handled at the origin and destination of the message.

S/MIME uses a symmetric cipher to encrypt messages and public key algorithms for secure exchange of keys and digital signatures. It can be used with a variety of encryption algorithms such as DES (Data Encryption Standard), 3DES (Triple DES), and *RC2*. S/MIME is built-in to several popular email client applications such as Outlook Express, Netscape Communicator, Apple Mail, Mozilla Mail, and Lotus Notes.

Pretty Good Privacy (PGP)

PGP is an application that provides security for email messaging by using encryption and authentication. This encryption mechanism is not compatible with S/MIME and is usually installed as a plug-in on email client applications such as Microsoft Outlook. Once installed, the email messages can be encrypted, decrypted, and digitally signed. The sender and receiver use a secret key to encrypt or decrypt the message.

PGP is one of the most trusted methods of securing email. When used properly, it can provide a very high level of security for email messaging. In addition to email security, PGP is also capable of securing data stored on file servers. It uses public key cryptography: a combination of public and private keys for securing email messages. The sender uses a public key to encrypt the message. The receiver uses his private key to decrypt it.

A PGP plug-in is available for email applications such as Microsoft Outlook. When PGP is installed in Outlook, it compares the digital signatures with the public keys that are stored locally in a *key ring*, which is a collection of public keys belonging to other users whom the user trusts. If Outlook cannot find an appropriate public key to decrypt the email message, the user is prompted to acquire a public key from a key authority. PGP uses *paraphrase* texts to protect the key assigned to users. If a user forgets his password when he needs to decrypt an encrypted message, he is prompted for the paraphrase.

Email vulnerabilities

Email has become one of the most popular and widely used means of communication since the inception of the Internet. It is the most convenient method of transferring information to others. This popularity comes with several vulnerabilities that are a result of the abuse of email technologies. This includes email spams, hoaxes, and exploitation of SMTP relay.

Spam. Email *spam* is the equivalent of unsolicited junk mail that fills up your mailbox everyday. These messages come from unknown persons and the recipients are usually responsible for the cost of delivery, storage, and destruction of these messages. These messages are rarely of any interest or use to the recipient. Email addresses of hundreds or thousands of persons are collected for spam from newsgroups and forums without their knowledge or approval. Spammers also use specially created applications known as *spamware* to collect email addresses and send them messages. In most cases, spammers use spoofed mail addresses that are not traceable.

Spam is essentially a form of a Denial of Service attack, as it has the potential of bringing down the mail servers of an organization. The email servers can become filled with junk messages, which are of no use to the organization or any employee. Organizations usually configure their mail servers to reject any mail that is sent to a large number of employees. Such emails usually contain fake addresses of the senders. Mail servers block any email that is received from an unknown address. Spam takes advantage of SMTP messaging servers that do not check the origin of the message but blindly forward them to the recipient.

Marketing organizations usually send bulk emails to several thousand customers simultaneously. Many ISPs do not allow this and treat bulk email as spam. Legitimate organizations maintain lists of their customers and send them information about new products or promotions regularly. This is the flip side of spam—where the customers are given the option to be removed from mailing lists.

The following are some methods to avoid spam:

- Individual users can use email filters or spam filters to filter out unsolicited emails.
- Users can disable cookies in their Internet browsers. Cookies contain personal information about the user, which can be used by spammers.
- Administrators can configure mail servers to stop spam at the server itself before it is delivered to employees.
- Spam can be reported to your ISP so that steps are taken to filter spam at the ISP level.
- Use of antivirus or antispyware programs can largely help to reduce the chances of spam.
- Users can disable the use of HTML email and other rich content.
- A user can search for her email address on the Internet. If she find its on any web site, she can ask the administrator to remove it.

Email hoaxes. A *hoax* is a message that tricks the receiver into believing that it is real while it is not. An email hoax is an email message sent to multiple users around the Internet about something they might be very interested in. For example, you may receive an email that you have been selected by Microsoft to receive a special prize of $250 because you have been an active user of Windows XP, and you may believe it. You may be asked to provide details of your bank account, so that the money could be directly deposited into your account. Beware! This is an email hoax.

Another form of email hoax is known as a *virus hoax*. It is an email message sent to millions of email users on the Internet with a warning about a virus that does not actually exist. If this message contains instructions on how to remove the "virus," do not blindly follow them. You may be deleting some critical files that will ultimately leave your system unable to start. Ask for expert advice or search the Internet for more information.

Email viruses. Viruses are often sent to recipients of email as attachments to messages. As soon as the recipient clicks the attachment, the virus becomes active and installs itself on the recipient's computer. It is always wise not to open any email from an unknown person, especially when it contains an attachment. Email programs should be configured to use plain-text messages. Emails with rich content such as HTML must be avoided. Email applications should be regularly scanned with antivirus software before messages are delivered to the recipients. Organizations usually implement virus scanning at the mail server level. Any email that contains a virus is deleted at the mail server itself. Administrators should regularly update virus signatures so that the software is able to detect newer and known viruses.

SMTP relay. SMTP relay is a feature of SMTP that allows anyone on the Internet to relay (send) a message to all recipients in the destination domain. It is also known as *open mail relay*. A poorly configured SMTP server can be easily exploited to send bulk email messages to millions of recipients around the globe. SMTP servers must be properly configured so that message relay is prevented at the server itself. SMTP relay is mostly used for email spam; an open SMTP relay gives spammers free and reliable delivery of messages.

Newer technologies allow configuration of SMTP servers to prevent open SMTP relay. Many ISPs use *DNS Block Lists (DNSBLs)*, also called *DNS Based List* or *DNS Black List*, to disallow relay of mail from open SMTP relays. Once a mail server is found to be relaying mail from any third party, it is placed on the DNSBL. Any other mail servers using those lists would stop accepting mails from the blocked sites. Most of the newer mail servers do not allow open SMTP relay.

Internet Security Concepts

Internet security, or web security, not only concerns organizations that host web sites but also those who visit these sites. Web sites and web clients are two ends of an active Internet surfing session, and both of these ends should be properly configured to prevent undesired outcomes that result from the exploitation of vulnerabilities existing in programming or configuration. Web sites are commonly hacked or exploited due to poorly written scripts that run from within web pages stored on web servers, while web clients can be exploited by poorly configured web browsers. For example, a hacker can obtain personal and confidential information from cookies stored on a client computer, while another hacker may be interested in launching a buffer overflow attack against a web site. This section covers some of the common concerns of Internet security.

Securing web servers

Some of the actions that can be taken to secure web servers from illegal activities include the following:

- Manage access control on web servers so that only authorized personnel are allowed to work on them. Activities of authorized users should be audited and logged as part of the security policy.
- Place web servers, messaging servers, and database servers used for the organization's web site inside a perimeter network secured by firewalls. All traffic coming in and going out of the network should be monitored.
- Regularly back up web and database servers so that the web site can be restored in the event of a disaster. Applications and data stored on web servers (and associated database servers) are items that the organization may be using to maintain its presence, or even to run its business, on the Internet. Only authorized employees should be given permission to access or modify this data.
- Properly test web server content such as applications and scripts before they are deployed on the site. Poorly written applications and scripts can open doors to attacks on the web site.
- Only authorized administrators should install web servers on specific server hardware. It is not uncommon to find *rogue web servers* within an organization because one or more users may have installed web server software unintentionally on their computers.

- Deploy the Intrusion Detection Systems (IDS) to monitor suspected network traffic and take corrective action if signs of an attack are detected.
- Understand and be concerned about security in an organization. Nothing can replace proper training and implementation of security policies.

Securing web browsers

Some of the actions that can be taken to secure web clients include the following:

- Internet access should be monitored so that users do not visit sites that are not required for their regular jobs.
- Cookies are commonly exploited to obtain personal information about users. Web browsers should be properly configured to handle cookies.
- Web browsers should be properly configured to handle Java applets, JavaScript, and ActiveX controls.
- Users should be allowed to download only those applications or programs from the Internet that are digitally signed.
- As much as possible, Instant Messaging (online chatting) should be prohibited outside the organization.

Secure Socket Layer/Transport Layer Security (SSL/TSL)

SSL is an encryption protocol popularly used for Internet-based transactions such as online banking. This protocol is based on public key encryption mechanisms. TSL is the successor of SSL, but it can be scaled down to the SSL 3.0 mode for backward-compatibility. SSL provides end-to-end security for Internet communications by using encryption. In typical implementations, only the server component is required to use public keys for authentication. For end-to-end security, a Public Key Infrastructure is required. Both the server and the client must be SSL-enabled to communicate over a secure channel.

SSL communications start with the following steps:

1. Both the client and the server negotiate an encryption algorithm.
2. The client and the server exchange session keys using public key-based encryption.
3. The client and the server authenticate each other using certificates.
4. Communications start and all traffic is encrypted using symmetric cipher.

The client and the server may negotiate one of the following encryption algorithms:

- RSA, Diffie-Hellman, or DSA for public key encryption
- RC2, RC4, IDES, DES, 3DES, or AES for symmetric cipher
- MD5 or SHA for hash functions

These algorithms are covered later in the section “Basics of Cryptography.”

SSL is vulnerable to attacks because of short key length, expired certificates (or self-signed certificates), and other errors made during implementation of the PKI. In its early days, SSL supported only a 40-bit key because the U.S. government did not allow export of longer keys. The current version of SSL is SSL 3.0, which uses a 128-bit key.

HTTP/HTTPS

HyperText Transfer Protocol (HTTP) is widely used on the Internet to transfer information between a web server and a browser. HTTP is a client/server, or request/response, application that enables communications between a web client (browser) and a web server. The HTTP client initiates a request by establishing a TCP connection to TCP port 80 on the web server. The server responds, and the client requests information on the web server by using a Universal Resource Locator (URL).

HTTP/S is simply HTTP used with SSL. Web sites using SSL normally require the web client to use "https://" before the URL instead of "http://". HTTP/S uses TCP port 443. Both HTTP/S and SSL use X.509-based digital certificates for authentication purposes.

> Remember that the port used by HTTP is 80, and the port used by HTTP/S is 443. Both HTTP/S and SSL use X.509 digital certificates.

Instant Messaging (IM)

IM is the process of real-time communications between two persons over the network media in the form of typed text. MSN Messenger (now Windows Live Messenger), Yahoo! Messenger, AOL Instant Messenger (AIM), and other online chatting tools are examples of Instant Messaging. IM is a great tool for a business that wants its employees to collaborate on running projects. It is considered an easy and cost-effective way to communicate compared to emails or telephone calls.

In spite of its benefits, Instant Messaging is generally prohibited inside organizations because of the security risks involved in real-time communications. An experienced hacker can easily exploit the vulnerabilities of instant messaging applications and launch a DoS attack against the organization's critical servers or even the entire network. It is also prone to buffer overflow attacks.

The privacy of an individual and that of the organization is one of the main security concerns involved with Instant Messaging. Until now there was no way to log activities of users involved in Instant Messaging. Organizations that use Instant Messaging for business purposes deploy specialized applications. These applications allow administrators to monitor messages and log activities of users.

Another security concern is that it is easy to determine a user's IP address during conversations. An attacker posing as a friend can easily discover this IP address to launch an attack against the user's home computer.

Vulnerabilities in Internet services

Some of the common vulnerabilities in Internet services have to do with the use of JavaScript, ActiveX controls, and cookies. These are client-side components of

Internet services and are often overlooked. In order to secure web browsers from potential outside threats, these components must be properly configured as a safeguard. These components are usually downloaded from the web server and run on the client computer. In case of a problem, the client computer is affected instead of the web server. The discussion that follows provides details of some of the common vulnerabilities found in Internet services. These vulnerabilities are covered in the Security+ exam.

Java Applets and JavaScript. *Java*™ is a programming language developed by Sun Microsystems. It is used to create small applications or applets for web sites. These applets are coded into web pages and are executed when a user accesses a web page from the server. Java applets use Java Virtual Machine (JVM) on a client computer to execute the code. A hacker may use Java applets to execute malicious code on the client computer in order to retrieve confidential information about the user.

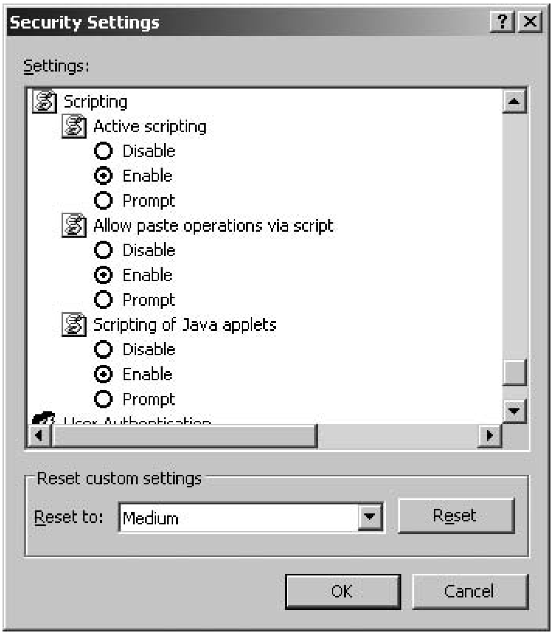
JavaScript is typically a part of the programming language such as HyperText Markup Language (HTML). It comes in two flavors, server side and client side. When a user accesses a document on a web site, JavaScript runs using an interpreter. It is possible that an attacker may write a script to obtain information about a web site or a client computer. This is known as *Cross-Site Scripting*. The user is usually unaware that a malicious script is running on his computer while he is browsing his favorite web site. JavaScript is less likely to crash a user's computer.

ActiveX. ActiveX, or *ActiveX Controls*, is Microsoft's implementation of applets that are embedded in HTML documents. These controls allow the web client to perform a number of functions, such as running multimedia files. When the web page is downloaded to a client computer, the applet checks to see whether the client has ActiveX support enabled. If not, the applet attempts to install these controls on the client's computer. ActiveX controls also run on a client computer instead of on the web server.

Protecting the Internet client. To protect the client computer from Java applets, JavaScript, and ActiveX Controls, the client can configure the web browsers to filter content of web pages. This may prevent applets and ActiveX Controls from automatically executing when a web page is accessed. Similarly, JavaScript can be exploited to gather confidential information about a user by writing malicious JavaScripts. The client can change the security settings of the web browser if it detects active content in a web page as follows:

- Enable or Always Allow
- Disable or Always Deny
- Prompt (for user input)

Figure 11-7 shows how Microsoft Internet Explorer can be configured to enable, disable, or prompt for user action upon detection of Active Content. This is done from the Security tab available under Internet Options.



Security Settings

Settings:

- Scripting
  - Active scripting
    - ○ Disable
    - ● Enable
    - ○ Prompt
  - Allow paste operations via script
    - ○ Disable
    - ● Enable
    - ○ Prompt
  - Scripting of Java applets
    - ○ Disable
    - ● Enable
    - ○ Prompt
- User Authentication

Reset custom settings

Reset to: Medium

Figure 11-7. Configuring Internet Explorer for Active scripting

Besides this, the web clients must keep their software updated with the latest security patches. In large organizations, administrators should test the software patches before deploying them to client computers.

Protecting the web server. On the web server side, most of the problems with Java applets, JavaScript, and ActiveX Controls can be prevented by having in-house programmers write the code themselves. A normal tendency is to pick freely available applets from the Internet and embed them into web pages. Although this saves program development time, it comes with problems when the code is not tested thoroughly. Programmers must ensure that any applets or JavaScript code is taken from a trusted site. The code should be authenticated, meaning that it should be signed by trusted vendors.

Cookies. *Internet cookies, HTTP cookies*, or *web cookies* refer to information that a web server sends to a web client that is stored locally on the client's computer. Cookies are used for authenticating, tracking, and maintaining user specific information. Every time the user visits the same web site, cookies stored locally on the client computer are used to restore his preferences. Cookies are extremely useful in allowing web sites to store user specific information, such as a user's shopping cart during online purchasing. Most web browsers allow storage of cookies on computers.

Since cookies contain identification information about a user, they pose a major security concern. They raise questions about a user's privacy. Some web pages do not contain all the information on the same web site. The information may be retrieved from other sites located across the Internet. These other web sites may also use cookies to store information about the user and are known as *third-party cookies*. Advertising companies use third-party cookies to track information about all the web sites visited by a user. The company can use these statistics to build user profiles that may help them promote their own products.

Most Internet browsers allow the user to limit the usage of cookies on their computers. This helps prevent theft of personal information by hackers. Some of the common settings available for configuring first-party and third-party cookies are as follows:

- Allow all types of cookies and allow web sites to read them.
- Block all types of cookies and restrict web sites from reading cookies without the user's consent.
- Block third-party cookies.
- Block cookies from web sites that do not have a privacy policy.
- Block web sites from accessing personally identifiable cookies without the user's consent.
- Set an expiration time for cookies so that they are deleted from the user's computer after a set period of time.

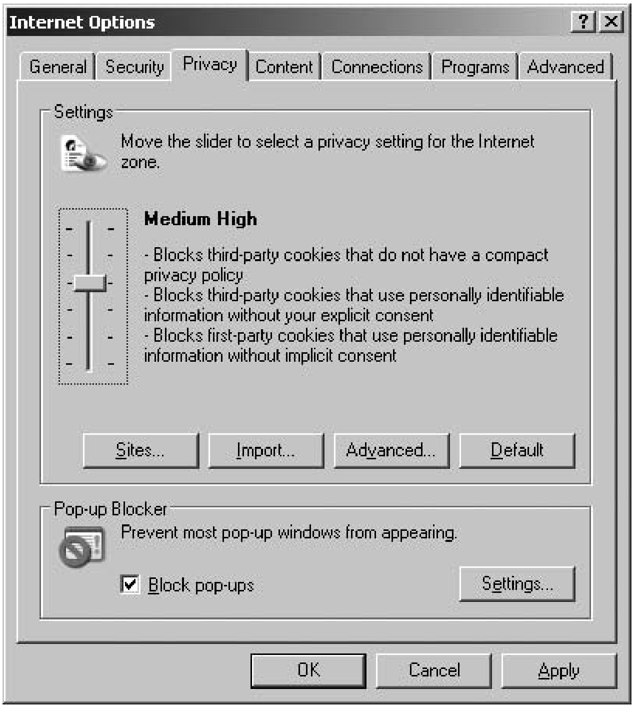
Figure 11-8 shows how the Privacy tab available in Internet Options of Microsoft Internet Explorer can be configured to store and use cookies.

Buffer overflows. A *buffer* is a temporary storage area in the computer memory used by an application. It is used to speed up processing command execution and to move data in and out of the hard disk. When the information sent to the buffer is more than what it can handle, it results in buffer overflow. In a typical buffer overflow situation, an application or a process attempts to write data beyond the limits of a fixed length buffer. As a result, the extra data overwrites the adjacent buffers and causes the application to produce unexpected and incorrect results. In some cases, buffer overflows can even cause termination of the application. Buffer overflows can occur in one of the following ways:

- Stack-based overflows
- Heap-based overflows

Stack and *heap* are two areas of computer memory that are allocated to applications. Stack stores most of the function calls of the application, while heap is used to store dynamically allocated variables. If a hacker writes malicious code in the heap, such as an invalid filename, username or a password, the application may pick up invalid variables. For example the application may pick up a wrong file to execute. If this is an executable file, the program will run this file, which is not intended to run. Many function calls do not check the size of the memory buffer that results in buffer overflows.

Professional hackers can easily exploit weaknesses of applications to launch buffer overflow attacks against web servers. Buffer overflows are based on how well programming languages are used to manage memory buffers. To use buffer



Move the slider to select a privacy setting for the Internet zone.

Medium High

- Blocks third-party cookies that do not have a compact privacy policy
- Blocks third-party cookies that use personally identifiable information without your explicit consent
- Blocks first-party cookies that use personally identifiable information without implicit consent

Prevent most pop-up windows from appearing.

☑ Block pop-ups

Figure 11-8. Configuring cookies in Internet Explorer

overflows in writing malicious code, the hacker must have in-depth knowledge of the programming language as well as the operating system. Buffer overflow attacks can be detected and filtered out by using *application gateway firewalls*. These firewalls perform *deep packet inspection* to detect attack signatures and prevent a possible buffer overflow attack.

Preventing buffer overflows should be one of the main concerns of programmers who write code for web servers. Programmers can use languages that provide dynamic allocation of memory buffers. Languages such as C and C++ do not have built-in capabilities to manage memory buffers. They should check the correctness of the code to ensure that it can manage memory buffers as expected and will not cause buffer overflows. They should use libraries that are considered safe. A technique known as *stack-smashing protection* helps detect most common buffer overflows. Other techniques used to avoid buffer overflows include *Executable Space Protection*, which prevents hackers from inserting malicious code, and *Address Space Layout Randomization*, which helps randomization of memory areas.

Signed applets. Signed applets refer to those program applets that have been authenticated (digitally signed) by their vendors or developers. The process is also known as *code signing*, which ensures that the applet is authenticated by the vendor. Users can trust the authenticity of the code they download from the

Internet, since it carries the digital signatures of the vendor. Authenticated code is also known as *Authenticode*. The digital certificate is issued by a third-party CA such as VeriSign or Thawte, and it carries the following:

- The digital signature of the CA.
- The name of the vendor.
- The encryption algorithm used.
- The dates of validity of the certificate, and a serial number.

All these components of the certificate ensure the user that the signed code is valid and has not been modified.

Digital signatures can be applied to a number of file types. Developers can use VeriSign Authenticode for files with extensions such as .EXE (executable files), .CAB (compressed cabinet files), .CAT (digital thumbprint files), .OCX (ActiveX Control files), .DLL (dynamic link library file), and .STL (certificate trust list file).

Problems with signed applets. The following are some of the problems associated with signed applets:

- One must rely on third-party CAs to get the code authenticated. The CA can provide a digital certificate but cannot validate the authenticity of the developer. Professional hackers may use fake identities to get their malicious code authenticated.
- A developer may acquire digital signatures for a file, but the signatures are attached to a different file.
- If web browsers are not configured properly to check for expired certificates, the user can keep downloading code with expired or revoked certificates.
- When CAs are used internally by an organization, users can start self-signing the code. For example, you can set up a CA within the organization using Microsoft's Certificate server and issue certificates to users. Such a code can be dangerous for the organization if it is used without thorough testing.

Common Gateway Interface (CGI). CGI is a standard protocol for interfacing external applications with a web server. CGI provides a gateway to these applications so that they can be incorporated and executed on the server. CGI scripts are used as middlemen to pass data between the web client and the web server applications. This data may be any user input, which is passed on to the web server and then to the external application. The output is returned to the web client again through the web server. CGI scripts are executed on the web server and do not have any effect on the client. Typical uses of CGI scripts include Internet chat rooms and shopping carts in e-commerce sites such as eBay and Amazon.

Experienced hackers can easily exploit CGI scripts. Vulnerabilities in CGI scripts are easy to locate. CGI scripts are executed on web servers using the privileges of the server software. Hackers can easily obtain information about web sites and access directories and files to perform undesired actions against the site. Poorly written CGI scripts open the door to hackers who use applications such as *nikto* (*http://www.cirt.net/code/nikto.shtml*) and *whisker* (not available now) to locate vulnerabilities in scripts. These vulnerabilities can even enable hackers to reach web servers located behind firewalls or protected perimeter networks.

Webmasters and web server administrators should themselves use these scanning tools to detect vulnerabilities in CGI scripts. Tools such as nikto can be used to detect vulnerabilities in poorly written CGI scripts. Programmers can use CGI *wrappers* to enhance security of their scripts. CGIWrap is one such application that checks each CGI script before it is allowed to execute. If it finds problems with the script, it is prevented from executing. Programmers must be careful when new scripts are added or older scripts are modified to add new features to a web site. All changes to the CGI scripts must be tested before they are used on web sites.

Directory Services Security

Directory services in most of the network operating systems use the *Lightweight Directory Access Protocol (LDAP)*. LDAP is based on the X.500 directory service standard protocol. LDAP makes is easy for clients to query and modify directory objects using the TCP/IP protocol. The current version is LDAPv3. Study of directory security directly involves study of LDAP security. Most of the implementations of LDAP directory services tend to use the DNS for structuring the directory hierarchy, which consists of forests, trees, domains, sites, and organizational units (OUs). Each of these entities may further have objects such as computers, printers, users, and groups.

LDAP services are used to store, query, and modify information about objects in a directory. LDAP clients must first authenticate to the server before they are allowed access. An example of such a server is the domain controller running Active Directory services in the Windows Server 2003 network.

An LDAP session starts when a client sends an authentication request to the server. By default, LDAP uses TCP port number 389. This authentication request is known as a *bind* operation. The connection is secured using Transport Layer Security (TLS). Once the client is authenticated, it can send more search queries to the LDAP server. The client can also add, delete, or modify entries in the directory as well as move entries from one location in the directory tree to another, depending on permissions assigned to her account. When the client terminates the connection, the process is called the *unbind* operation.

LDAP naming conventions

The LDAP naming convention follows the X.500 standards. A directory is a tree of directory entries or objects. Each entry or object has a set of attributes. Each attribute has one or more values. Each object has a unique identifier known as its *Distinguished Name (DN)*. The DN of the object correctly describes its position in the directory hierarchy. It is made up of the *Relative Distinguished Name (RDN)* of the object, followed by the parent object in the directory. The following is an example of DN:

CN=JohnSmith OU=Editors DC=Oreilly DC=com

In this example, "CN=JohnSmith" is the RDN of a user named John Smith. This user object is located in the OU named "Editors," which is the parent object and is located in the oreilly.com domain. Clients connect to the LDAP server using the

DN of an object. Operating systems such as Windows Server 2003 provide graphical user interfaces that make it easy for the administrators to manage objects in Active Directory.

LDAP security

LDAP communications can be secured using the SSL, which extends LDAP usage over the Internet. In order to use LDAP with SSL, the server must have an X.509 server certificate, and SSL must be enabled on the LDAP server. When used for web services, the LDAP server can provide centralized authentication for remote clients by maintaining a user account database on the server. The users have to be authenticated only once in order to access the internal resources of the organization. This means that users will need a single sign-on to access directory services. Defining and applying policies on the LDAP server can also govern authentication of users.

LDAP servers are prone to several types of attacks from unauthorized users or attackers. These include spoofing of directory services and DoS and buffer overflow attacks.

File Transfer Protocols (FTP)

FTP is the most popular protocol for transferring files from one computer to another over the networks that support TCP/IP. It is commonly used on the Internet to transfer files between FTP servers and clients. FTP works at the Application layer (Layer 1 of the OSI model) within the TCP/IP protocol suite and uses TCP ports 20 and 21. Port 20 is used for data transfer while port 21 is used for control messages. There are two computers involved in FTP communications: an FTP server, which runs the FTP server software, and the client, which runs the FTP client software.

Blind FTP

Blind FTP, or *Anonymous FTP*, refers to those FTP connections that do not require a user to log in with a valid username and password. This is done in order to provide access to those users who do not have accounts on the FTP server. Blind FTP is a common method to make files available to users over the Internet. While this is a great facility for general users, the flip side is that hackers can easily misuse this to launch DoS attacks against the FTP server.

The best protection against attacks on FTP servers is to prevent anonymous logons and to disable nonessential services on the servers. Problems with FTP are that passwords and data are transmitted in clear text with no security. If anyone captures data being transmitted between the FTP server and the FTP client, he can easily obtain a valid username and password to launch an attack on the FTP server. A solution is to use the Secure FTP (FTPS), as summarized ahead.

Secure FTP (S/FTP)

Secure FTP (also called *FTP over SSH*) should not be confused with other methods of securing FTP transfers such as *FTP over SSL (FTPS or FTP/SSL)*. S/FTP adds encryption to FTP transfers for protection against eavesdropping and packet sniffing because normal FTP transfers are done using clear text.

Wireless Communications

This section covers a detailed study of wireless networks, technologies involved in wireless topologies, authentication standards and protocols, and vulnerabilities of wireless networks to external threats. The Security+ exam expects you to know several key terms associated with wireless networks, as well as the strengths and weaknesses of wireless topologies and authentication methods. Before we discuss wireless topologies or authentication mechanisms and explore their vulnerabilities, we will take a look at some concepts behind wireless communications.

Wireless local area networks

Wireless networks rely on radio frequencies (RF) to communicate instead of the network cabling used for normal computer networks. Radio frequencies create *electromagnetic (EM) fields*, which become the medium to transfer signals from one computer to another. As you travel away from the hub or from the main equipment generating the radio frequency of the wireless network, the strength of the EM field reduces, and the signal becomes weak. The EM field is also prone to interference such as solid walls, reflected radio waves, and presence of other EM fields. Presence of wireless telephones, microwave ovens, television sets, and a number of other devices can potentially interfere and reduce the signal strength of wireless devices.

Spread spectrum wireless technology. In order to reduce the effects of interfering frequencies, wireless devices use the *spread spectrum* technology. This technology helps share available frequency bandwidth that may be common to other wireless devices. This technology also helps prevent the jamming of radio signals due to strong interference from another source of radio frequency. Instead of using a fixed frequency such as that used with radio and television broadcasts, wireless networks use a spectrum of frequencies. The sender uses a number of narrow band frequencies to communicate with the receiver. Each narrow band of frequencies contains only a part of the signal. The receiver correlates the signals received at different frequencies to retrieve the original information.

Spread spectrum technology synchronizes wireless signals using one of the following methods:

Frequency-hopping spread spectrum (FHSS)

FHSS is the method of transmitting RF signals by rapidly switching frequencies according to a pseudorandom pattern, which is known to both the sender and the receiver. FHSS uses a large range of frequency (83.5 MHz) and is highly resistant to noise and interference. The amount of time the signal spends on any frequency is known as *dwell time*, and the amount of time it takes to switch one frequency to another is known as *hop time*. FHSS signals are difficult to intercept because the signals usually appear as noise. FHSS works in the unlicensed frequency range of 2.4 GHz and is used in HomeRF and Bluetooth. FHSS has a limited speed of transmission that ranges from 1.6 to 10 Mbps.

Direct-sequence spread spectrum (DSSS)

DSSS is a modulation technique used by wireless networks. It uses a wide band of frequency and divides the signal into smaller parts. It is transmitted simultaneously on as many frequencies as possible within a particular frequency band. DSSS adds redundant bits of data known as *chips*. The ratio of chips to data is known as the *spreading ratio*. The higher the spreading ratio, the higher the immunity to interference. DSSS is faster than FHSS and ensures data protection, as chips are redundant and simultaneously transmitted. It utilizes a frequency range from 2.4 to 2.4835 GHz and is used in 802.11b networks.

Wireless Application Protocol (WAP)

WAP is an open standard for applications that use wireless communications. It is typically used with hand-held devices such as mobile phones and personal digital assistants (PDAs) to access information on the Internet. It works with most major operating systems, and it can be used to browse the Internet much like Internet browsers on computers. Microsoft Windows CE, PalmOS, and JavaOS are some examples of operating systems that use WAP. Mobile Internet sites or WAP sites are specially built for mobile devices using Wireless Markup Language (WML) and can be accessed using a WAP browser installed on a mobile hand-held device. WAP 2.0 is the current version.

Wireless Transport Layer Security (WTLS)

The WTLS protocol is designed to provide end-to-end security for WAP devices. WTLS is based on the TLS protocol that is a further derivative of the SSL. It is designed to provide privacy and availability for both the WAP server and the WAP client. WTLS works for applications that run on devices with low-processing capabilities, low bandwidth, and limited memory. It uses a compressed certificate format following the X.509v3 standard but defines a smaller data structure.

IEEE 802.11

IEEE 802.11 is a standard that defines the operation of wireless networks within the 2.4 GHz frequency range using either FHSS or DSSS. This standard defines all aspects of wireless communications from the frequency ranges specifications and physical layouts to authentication mechanisms. The original 802.11 standard is known as *legacy 802.11*. The 802.11 family of standards define several protocols used for wireless communications—802.11b, 802.11a and 802.11g are the most commonly used. Security in these protocols is defined in the 802.11i standard.

IEEE 802.11b. IEEE 802.11b is the most commonly used standard in wireless networks as of this writing. This standard defines DSSS-based network devices that use the 2.4 GHz frequency range and can communicate at speeds of 1.2, 5.5, or 11 Mbps. This standard is compatible with the legacy 802.11 standard. 802.11b is designed for a point-to-multipoint wireless communication setup. Usually a wireless Access Point (AP) is used with an omnidirectional transmission antenna and can communicate with wireless clients located in the coverage area around the AP. The indoor range of the 802.11b AP is about 100 feet (30 meters) at 11 Mbps speed. When used with 1 Mbps speed, the range can be as high as 300 feet (90 meters).

IEEE 802.11a. The IEEE 802.11a standard uses the 5 GHz frequency range with up to 54 Mbps data transmission speed. This standard defines use of 52-subcarrier Orthogonal Frequency-Division Multiplexing (OFMD), which is a modulation technique. If required, the data speed can be reduced to 48, 36, 24, 18, 16, 12, 9, and 6 Mbps. 802.11a is not backward-compatible with the 802.11b standard. The range for 802.11a-based devices is also about 100 feet (30 meters when used indoors).

IEEE 802.11g. The IEEE 802.11g standard defines the frequency range of 2.4 GHz (same as 802.11b) but uses much higher data transfer speeds of up to 54 Mbps. The data speed can fall back to lower values. IEEE 802.11g is backward-compatible with 802.11b standard devices. The devices normally use the OFMD modulation technique but can switch back to Quadrature Phase-Shift Keying (QPSK) modulation when the data speed falls to 5.5 or 11 Mbps. Although its is a popular standard, it operates in the already crowded frequency range of 2.4 GHz. *Bluetooth* devices, cordless telephones, and microwave ovens also operate within this frequency range. For this reason, 802.11g devices are susceptible to interferences similar to the 802.11b devices.

Table 11-1 gives a brief comparison of different 802.11 standards.

Table 11-1. Comparison of 802.11 standards

802.11 standard	Operating frequency	Maximum speed	Modulation technique	Indoor range
802.11b	2.4 GHz	11 Mbps	DSSS	100 Feet
802.11a	5 GHz	54 Mbps	OFDM	100 Feet
802.11g	2.4 GHz	54 Mbps	OFDM and QPSK	100 Feet

Ad-hoc and Infrastructure wireless networks. The IEEE 802.11 standards define two main configurations of wireless communications: *Ad-hoc* and *Infrastructure*. The Ad-hoc wireless configuration consists of several wireless devices that are within range of each other. There is no central device (hub), and these networks can be created spontaneously anywhere when two or more network devices fall within reach of each other. A home network with wireless adapters is an example of Ad-hoc wireless configuration.

In Infrastructure configuration, a central wireless device known as the *Access Point (AP)* is used to authenticate and configure wireless clients that fall within its range. Wireless clients communicate to each other through the AP. A special identifier known as the *Service Set Identifier (SSID)* must be configured on the AP and each wireless client. All clients in one Infrastructure network use the same SSID. Different Infrastructure networks are identified by their unique SSIDs. The AP can further be connected to the wired local area network so that wireless clients can access the wired LAN also.

Figures 11-9 and 11-10 show ad-hoc and infrastructure wireless network configurations respectively.

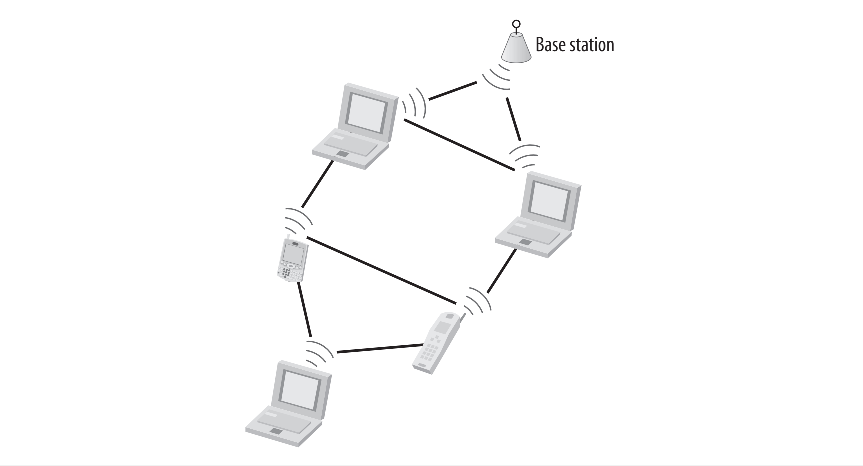


Figure 11-9. Ad-hoc wireless network

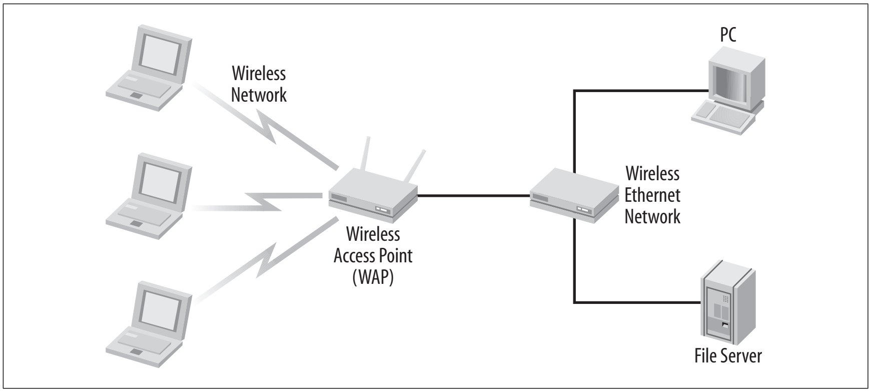


Figure 11-10. Infrastructure wireless network

Wired Equivalent Privacy (WEP)

WEP is the primary security standard for 802.11 wireless networks, and it is designed to provide privacy in transmissions occurring between the AP and wireless client. It uses *shared key authentication*, which allows encryption and decryption of wireless transmissions. Up to four different keys can be defined on the AP and the client, and these keys can be rotated to enhance security. WEP encryption can use either 40- or 128-bit keys. When WEP is enabled on the AP and the wireless clients, the encryption keys and the SSID must match on both ends. WEP is easy to implement because the administrator or the user can define the keys.

WEP uses the CRC-32 checksum for data integrity, and privacy is ensured with the RC4 encryption algorithm. RC4 is a stream cipher, and both the AP and the client encrypt and decrypt messages using a known preshared key. The sender runs the plain text message through an integrity check algorithm, Cyclic Redundancy Check (CRC-32), to produce the Integrity Check Value (ICV). The ICV is added to the plain text message. A random 24-bit Initialization Vector (IV) is generated and added to the beginning of the secret key to ensure the key's security. The IV is changed every time to prevent reuse of the key.

Authentication in wireless networks

The IEEE 802.11 standard defines the following two types of authentication in wireless networks.

Open authentication. Open authentication is device-specific, and allows almost all devices access to the wireless network. It should not be assumed that the open authentication method does not use encryption because all devices are granted access. This method can also require the use of WEP keys. Any client who knows the SSID of the AP can connect to the wireless network.

Shared key authentication. Shared key authentication is used to grant access only to those wireless clients who possess the SSID and the shared key. The authentication process begins when a client (also called the *supplicant*) requests a connection with the AP (also called the *authenticator*). The AP sends a random challenge text to the client. The client receives this, encrypts it with the shared key, and sends it back to the AP. The AP receives the encrypted text, decrypts it, and compares it with the original challenge text. If the two texts match, the client is authenticated and granted access.

Shared key authentication is susceptible to plain text attacks because the initial challenge text is sent to the client as plain text. As a result, the shared key authentication is considered a weak authentication method. But it is still better than having no authentication at all.

802.1x authentication. The 802.1x is an authentication standard designed to provide security for port-based access to wireless devices. It provides more options for the administrators to pick up suitable encryption and key management mechanisms. Most of the newer AP devices are 802.1x-compliant. For more details about the 802.1x authentication process, refer to the "Remote Access" section earlier in this chapter.

Some of the benefits of using 802.1x authentication are as follows:

- It allows dynamic creation of per-user session keys. These keys need not be kept with the AP.
- It provides mutual authentication. Both the client and the AP can authenticate each other before the communications begins. This helps prevent MITM attacks.
- When used with the EAP, it provides per-packet authentication and data integrity protection.
- It defines strong mechanisms for identification and authentication.

Types of attacks on wireless networks

Wireless networks are prone to both active and passive attacks, which include DoS, MITM, spoofing, packet sniffing, war driving, jamming, network hijacking, and many more. Passive attacks on wireless networks are very common and are very difficult to detect because the attacker usually indulges in collecting information only. Active attacks are launched when a hacker has gathered sufficient information about the network after several successful passive attacks. The following is a list of some of the common attacks against wireless networks:

War driving

Hackers can use freely available war-driving software (such as NetStumbler) to launch passive attacks on wireless networks. They use this software to detect insecure wireless networks where they can easily get in.

Man-in-the-Middle (MITM)

These attacks are common on wireless networks. The attacker tries to plant a rogue AP in the range of an existing wireless network. The wireless users are not aware of whether they are connecting to a legitimate AP or to a rogue AP planted by a hacker. Since the range of AP devices may extend outside the building, a hacker may even use an AP device inside a car parked outside the building.

Plain-text attacks

The WEP standard is prone to these attacks because it uses the RC4 encryption algorithm. In WEP authentication, the initial challenge text is sent in plain text. The RC4 encryption algorithm uses stream cipher and is known for its weaknesses. It uses a 24-bit IV for both 40- and 128-bit encryption, which is easy to predict. WEP encryption keys can be easily cracked using tools such as WEPCrack and AirSnort.

Packet sniffing and eavesdropping

These are two of the common techniques used to launch attacks on wireless networks. *Sniffing* refers to the monitoring of network traffic using legitimate network analysis tools. Hackers can choose any of the monitoring tools, such as AiroPeek, Ethereal, or TCPDump, to monitor wireless networks. These tools enable hackers to find unprotected networks that can be exploited. Wireless networks can be protected against these attacks by using strong encryption and authentication methods.

Jamming

This refers to the flooding of radio frequencies with undesired signals. It usually results in the unavailability of required signals to the wireless devices.

Network hijacking

This refers to hijacking the wireless network of a user's active session. The hacker can insert himself between a network server and the wireless client—and from that point on, the communication takes place between the hijacker and the client or the server. The hacker may also use rogue APs to divert a client session.

Denial of Service (DoS)

Most of the active attacks on wireless networks eventually result in these attacks. A DoS attack occurs when the legitimate client is prevented from accessing network resources due to unavailability of the services.

Flooding

Hackers can flood a wireless network using any of the attack methods, such as ICMP flooding (Ping flooding) and SYN flooding, etc.

Protecting wireless networks from attacks

It is important that administrators take steps to protect wireless networks from potential outside threats and attacks. Some of the protective measures that can be taken are listed here:

- Administrators should keep their software and hardware updated by regularly checking for updates on vendors' web sites.
- When installing a wireless network, the default settings of the AP, such as the SSID, should be changed. Hackers usually know the default settings of devices.
- WEP should always be used. Even if 40-bit encryption is used, it is better than not using encryption at all. WEP can be easily cracked, but the network can still be protected from a number of amateur hackers.
- Wherever possible, wireless adapters and AP devices should support 128-bit WEP, MAC filtering, and disabling of SSID broadcasts.
- IF SSID broadcasts are not disabled on APs, use of a DHCP server to automatically assign IP addresses to wireless clients should be avoided. Wardriving software can easily detect your internal IP addressing scheme if SSID broadcasts are enabled and DHCP is in use.
- Static WEP keys should be frequently rotated to so that they are not compromised.
- The wireless networks should be placed in a separate network segment. If possible, create a separate perimeter network (also known as a *Wireless Demilitarized Zone*) for the wireless network that is separate from the main network of the organization.
- Regular site surveys should be supported to detect the presence of rogue APs near a wireless network.
- Placement of the AP is critical for wireless security. APs should be placed in the center of the building; avoid placing them near windows and doors.

Site surveys. Site surveys enable network administrators to detect the boundaries of their wireless network beyond the required limits. The tools used to conduct site surveys are typically the same tools that the hackers use to detect unprotected wireless networks. Popular tools that can be used for site surveys include NetStumbler, Kismet, AirSnort, and WEPCrack. It is also important to conduct a physical inspection of the surroundings of the building. Hackers sometimes use antennas to receive and amplify weak wireless signals from the APs in order to indulge in malicious activities. Site surveys also include keeping an eye on suspicious activities of people around the building.

Infrastructure Security

Designing, implementing, and maintaining a network infrastructure includes ensuring security for the network. It is not an easy task because there are several components of the network, such as network devices, media, server and workstation hardware, network operating systems, and applications. It is important that administrators take steps to ensure security for each of these components so that the entire network is safe from possible attacks by outsiders. This section covers the concepts and security aspects of network components that need proper configuration to provide a safe and secure working organization.

Device-based Security

Network devices should be selected wisely and installed with correct configurations to prevent security loopholes. It is important to know the potential security problems in network devices and how devices can be configured to prevent outsiders from unauthorized access of the network or any of its servers containing confidential data. There are several devices that make up a complete secure network and each are discussed in the following sections.

Firewalls

A firewall is a hardware device or a software application that sits between the internal network of the organization and external networks in order to protect the internal network from communicating with the outside networks. A properly configured firewall blocks all unauthorized access to the internal network and also prevents internal users from accessing potentially harmful external networks. The three common firewall technologies are packet-filtering firewalls, Application-layer firewalls, and Stateful Inspection Firewalls.

Packet-filtering firewalls. *Packet-filtering firewalls* inspect the contents of each IP packet entering the firewall device and, based on predefined and configured rules, allow or block packets inside the network. These firewalls permit or block access to specific ports or IP addresses. These firewalls work on two basic policies: *Allow by Default* and *Deny by Default*. In the *Allow by Default* policy, all traffic is allowed to enter the network except specifically denied traffic. In the *Deny by Default* policy, all traffic entering the firewall is blocked except that which is specifically allowed. *Deny by Default* is considered the best firewall policy, as only authorized traffic is allowed to enter the network using specified port numbers or IP addresses.

Packet-filtering firewalls use IP addresses and TCP/IP port numbers to decide whether certain traffic is to be allowed or blocked. The firewall can be configured to allow or deny traffic based on the source IP address, the destination IP address, the source port, or the destination port. TCP/IP port numbers fall into the following three categories:

- Well-known port numbers that range from 0 to 1023.
- User ports (registered ports) that range from 1,024 to 46,151.
- Dynamic/private ports that range from 46,152 or 65,535.

For the Security+ exam, you will need to know the port numbers used by various network protocols and services. Table 11-2 lists some of the well-known ports.

Table 11-2. Well-known port numbers

Port number	Protocol/Service
20	File Transfer Protocol (FTP) (Data Port)
21	File Transfer Protocol (FTP) (Control Port)
22	Secure Shell (SSH)
23	Telnet
25	Simple Mail Transfer Protocol (SMTP)
53	Domain Name System (DNS)
67 and 68	BootStrap Protocol (BOOTP); also used by the Dynamic Host Configuration Protocol (DHCP)
80	HyperText Transfer Protocol (HTTP)
110	Post Office Protocol version 3 (POP3)
119	Net News Transfer Protocol (NNTP)
137, 138, and 139	NetBIOS Name Service (Windows operating systems)
143	Internet Message Access Protocol version 4 (IMAP4)
161 and 162	Simple Network Management Protocol (SNMP)
389	Lightweight Directory Access Protocol (LDAP)
443	Secure Socket Layer (SSL) or HTTPS

Packet-filtering firewalls work at the Network layer (Layer 3) of the OSI model. One of the benefits of these is the ease of configuration because a packet is either allowed or blocked. This technique also does not cause any delays in transmissions. There are certain limitations also. The firewall can just inspect the header of the packet but does not read the contents of the packet. Another drawback is that if a certain application opens a port dynamically and does not close it, the open port remains a security risk to the network.

Application-layer firewalls. Application-layer firewalls work at the Application layer (Layer 7) of the OSI model. They are also known as *Application firewalls* or *Application layer gateways*. This technology is more advanced than packet filtering because it examines the entire packet to allow or deny traffic. Proxy servers use this technology to provide application-layer filtering to clients. Application-layer packet inspection allows firewalls to examine the entire IP packet and, based on configured rules, allow only intended traffic through them.

One of the major drawbacks of application-layer firewalls is that they are much slower than packet-filtering firewalls. Every IP packet is broken at the firewall, inspected against a complex set of rules, and re-assembled before allowing it to pass. For example, if the firewall finds virus signatures in a packet, it can block them. Although this technique allows for more rigorous inspection of network traffic, it comes at the cost of administration and speed.

Stateful Inspection Firewalls. Stateful Inspection Firewalls work by actively monitoring and inspecting the state of the network traffic and keeping track of all the traffic that passes through the network media. This technology overcomes the drawbacks of both packet-filtering and application-layer firewalls. It is programmed to distinguish between legitimate packets for different types of connections, and only those packets are allowed that match a known connection state. This technology does not break or reconstruct IP packets and hence is faster than application-layer technology.

Using this technology, a firewall can monitor the network traffic and dynamically open or close ports on the device on an as-needed basis, as the communication states of common applications are known to the firewall. For example, if legitimate HTTP traffic enters the firewall, it can dynamically open port 80 and then close it when traffic has been allowed. This is in contrast to packet filtering, where the administrator would have to permanently keep port 80 open on the firewall.

> For the Security+ exam, you will need to know how firewalls work and what type of firewall is suitable for a given situation. If speed is a concern and you need to permanently allow or deny access to certain IP addresses or ports, packet filtering is best suited. If inspection of packets is required at the application level, you will need an application-layer firewall. Similarly, if the question asks you about monitoring network traffic or communication states, select the Stateful Inspection Firewall.

Routers

Routers are hardware devices or software implementations that connect two segments of an internetwork. Routers have usually two or more interfaces that connect to different network segments. They can help provide secure communications between two network segments inside an organization, or even between an organization's network and an external network such as the Internet. Routers pass IP packets between segments based on IP addresses configured in routing tables. Routing tables can be dynamic or static (created manually by administrators). In addition to routing tables, routers also support Access Control Lists (ACLs) to determine which IP packets should be allowed and which should be blocked. RRAS in Windows Server 2000 and 2003 is an example of a software router.

Most of the routers come with built-in security features. They can be configured based on the requirements of an organization. It is always wise to change the default configurations of routers, as hackers know these configurations. Routers use routing protocols such as *distant vector* and *link state* to dynamically build routing tables. These tables are prone to spoofing and eavesdropping. Using routing protocols, attackers sometimes are able to insert false IP address entries in routing tables and can take control of the network. Defining static routes is one way to prevent spoofed entries in routing tables, but for a large internetwork it is simply not possible to build static routing tables.

Switches

Switches are network devices similar to network hubs that connect network components within a LAN. Switches are different from routers because routers operate at the Network layer (Layer 3) of the OSI model while switches operate at the Data Link layer (Layer 2). Routers use IP addresses to forward traffic, while switches use MAC addresses for this purpose. A MAC address is permanently configured on network adapters by their manufacturers and cannot be changed. Some Layer 3 switches operate at the Network layer of the OSI model.

Switches offer better security to networks because they use MAC addresses and can filter out traffic coming in from an unknown MAC address. Switches are better than hubs because they forward only incoming packets to the desired destination instead of broadcasting them to all devices. One of the major security concerns related to switches is that if a hacker is able to take administrative control of the switch, he can easily hijack the entire network. Software applications such a *Switch Port Analyzer (SPAN)* can be used to send a duplicate copy of all packets passing through the switch to a specific port, which may be in the control of the hacker. SPAN is generally used by administrators for troubleshooting purposes, but it can also be exploited.

Switches can also be subject to Address Resolution Protocol (ARP) spoofing and DoS and MITM attacks. Since switches can be configured using Telnet sessions, an attacker can perform packet sniffing to capture Telnet session traffic in order to obtain an administrative username and password. Administrators should use secure Telnet sessions using SSH. *MAC flooding* is another way to flood switches with a large number of MAC addresses.

Wireless

Wireless network cards, wireless routers, and wireless access points are the main devices associated with wireless networking. Wireless security was covered in the "Wireless Communications" section earlier in this chapter.

Modems

Modems are devices usually connected to remote access servers (RAS) to provide access to remote users or telecommuters. Remote users dial in to a RAS modem or a *modem bank* using ordinary telephone lines and a preconfigured telephone number. Although this technology is becoming obsolete with the increased use of broadband, older systems still use modems to grant remote access. Modems are prone to war-dialing attacks by hackers. Hackers can use wardialing software in an attempt to locate a modem connected to a RAS server that will respond to the hacker. When properly configured with security features such as *callback*, modems can be secured from unauthorized access. Remote access policies can further be implemented on RAS servers to enhance security.

Remote Access Servers (RAS)

RAS typically use modem banks to provide remote access to remote users. These modems are configured with telephone numbers; when a remote user dials a predetermined number, any of the free modems in the modem bank can respond. Once the communication starts, the remote user is authenticated using his dial-in permissions and remote access policies. RAS servers use a number of authentication and authorization protocols to grant access only to authorized users. These protocols include CHAP, MS-CHAP, and EAP. Insecure protocols such as PAP and the Shiva Password Authentication Protocol (SPAP) can also be used, but should be avoided as much as possible.

Some RAS server security policies include mandatory caller ID, callback, and limitation of calling days and hours. These policies ensure that only an authorized user connects to the RAS server from a predetermined telephone number and during permitted days and hours. Caller ID ensures that the call is coming from an authorized telephone number. Restriction on calling days and hours ensures that if a hacker does not know about these restrictions, his calling attempt is detected. A strong password security policy should also be in place. Additionally, administrators may restrict the use of unnecessary protocols on RAS servers.

Virtual Private Networks (VPNs)

A VPN is a low-cost alternative to providing remote access to corporate networks. It is also used for creating intranets and extranets using a secure tunnel through a public network. It is less expensive for large companies to connect its branch office networks to the corporate network because dedicated circuits are not required. Typically, all offices are connected to the local ISPs, which further provide connectivity to the Internet. Similarly, remote users or telecommuters can simply dial in to the local ISP to connect to their office networks. This saves them the cost of long-distance calls.

Depending on their implementation, VPNs can be of the following types:

Remote Access VPN
: This is used to provide remote connectivity to individual employees who work from remote sites. These employees include telecommuters or those who work from home.

Site-to-Site VPN (intranet)
: This is used between local area networks of an organization located at different geographical locations. *Intranet* refers to the network created for different offices of the same organization. A site-to-site VPN typically uses demand-dial routing in order to reduce the costs involved in permanent connections to the Internet.

Site-to-Site VPN (extranet)
: This is used to connect networks of two or more different organizations. *Extranet* refers to the network created for these different organizations. Usually, organizations with common interests or partner companies implement extranets for secure data transfers.

Figures 11-11 and 11-12 show Remote Access VPN and Site-to-Site VPN respectively.

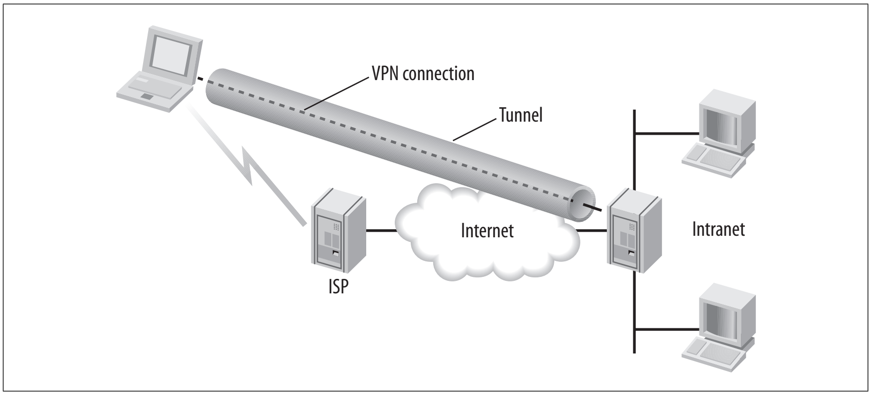


Figure 11-11. Remote Access VPN

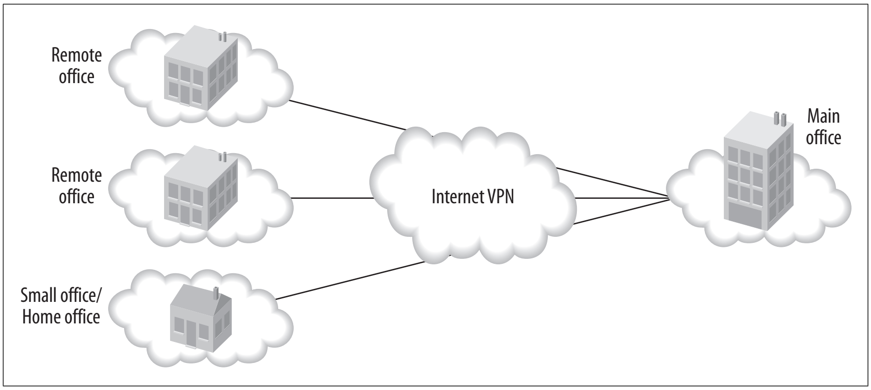


Figure 11-12. Site-to-Site VPN

A VPN works by creating a tunnel through the Internet. It can be implemented using high degrees of security. Commonly used tunneling protocols include PPTP and L2TP/IPSec. The combination of L2TP and IPSec is considered more secure than PPTP. Data traveling through the Internet is encrypted and secure from eavesdroppers. SSH can also be used as a security mechanism. Additionally, organizations can implement firewalls to secure their VPN servers. VPN servers can also be placed inside secure perimeter networks, which is usually separate from the main local area network of the organization.

Network monitoring

Network monitoring allows administrators to keep an eye on network traffic in order to detect abnormal behaviors or network congestions and take corrective action to resolve network problems. Most large networks employ some kind of monitoring or sniffing software applications to monitor network traffic. While these applications are good when used appropriately, they also pose security risks because a malicious user or an outsider can take advantage by gathering data from the network media. Equipment used to diagnose network problems may also be prone to malicious activities if left attached to the network. The vulnerabilities associated with network monitoring applications or diagnostic equipment are generally limited to collection of data by unauthorized persons. With the collected data, an intruder or an unauthorized person can obtain critical information about the network in order to launch an active attack.

Workstations

Workstations refer to desktop computers used by common users in an organization. They typically require access to servers and are considered some of the most vulnerable systems inside a network. This is because there are far more workstations than there are servers in a network. Securing workstations is more difficult because of their large number and location in different segments around the network. Exploiting a workstation is easy due to the fact that they use a variety of network protocols to connect to servers such as TCP/IP and NetBIOS. Older Windows operating systems use the NetBIOS protocol, which is vulnerable to active attacks such as DoS. Such attacks can render a workstation unable to communicate on the network or even cause it to crash. In situations where workstations communicate to servers without any encryption mechanism, the chances of exploitation increase. Workstations are also prone to MITM attacks or hijacked sessions. They always have local access to servers, and they need to be secured by using the latest security patches for operating systems and other applications. The following are some of the important points about securing workstations:

- Security policies should be implemented to ensure that users do not keep weak passwords. Passwords should be changed at regular intervals.
- Virus scanners with the latest virus signatures should be used on all workstations.
- If users are allowed Internet access from their workstations, the web browsers should be properly configured to avoid downloading or running active content from different web sites.
- Users should be instructed to lock their workstations when they move away from their seats.

Servers

Servers are used in medium- and large-scale organizations to service requests from multiple clients (workstations) simultaneously. Servers are the core of any network service and the central repository for most of the confidential data of the organization. Consequently, attackers are more interested in servers than in any other network equipment. If servers are compromised, it can cause significant damage to the organization. Administrators should take steps to ensure the security of servers to minimize potential threats from inside and outside the organization. The following are some important points for ensuring the security of servers:

- Servers should be kept in locked rooms, with limited physical access available to authorized administrators only.
- Servers should be configured for the auditing and logging of user activities, including administrative access.

- Users should be granted only need-based (or role-based) access to servers. Files and folders should be protected using ACLs.
- The network operating system (NOS) installed on servers should be kept up to date with the latest security patches, hotfixes, and service packs.
- From the network point of view, servers accessible from outside the organization, such as web servers, mail servers, remote access servers, and VPN servers, should be placed in Demilitarized Zones (DMZ) protected by firewalls. A DMZ is also known as a perimeter network.
- As much as possible, all communications between servers and workstations should be encrypted to protect against eavesdropping and packet sniffing.

Mobile devices

Mobile devices such as cellular phones and PDAs are becoming popular because of the significant enhancement in their features and consistently falling prices. Newer PDAs as well as many new models of cellular phones are capable of connecting to the Internet, sending/receiving emails, and connecting to remote network applications. These devices usually store personal and confidential information about the owner. It is very common to leave mobile devices, such as PDAs and cell phones, at a friend's house, a hotel, at the airport, or on a restaurant table. These devices pose a major security risk because of their capability to connect to the Internet and other features. It is always good to encrypt the data stored on mobile devices so that if a device is stolen, the data remains out of bounds to the thief. Another way to protect data stored on mobile devices is to use strong passwords.

Media Security

Network media refers to all types of cabling (used for connecting network devices), removable media (such as floppy disks), USB storage devices, magnetic tapes, CD-ROMs, DVD-ROMs, and writable CDs and DVDs. This media needs to be secured in order to prevent malicious activities by insiders as well as outsiders. The Security+ exam puts emphasis on securing the data transmitted through the physical media types discussed in the following sections.

Coaxial cable

Coaxial cables are mainly used for carrying television signals (for example, CATV), but some older computer networks also utilized these cables for connecting workstations and other network devices. Usually the coaxial cables used for different purposes have different characteristics, so that cables for one purpose cannot be used for another. For example, the cable used for CATV cannot be used for computer networks. Coaxial cables fall mainly into the following two categories:

Thin coaxial cable

Also known as *Thinnet*. The type of thin coaxial cable used for computer networks is RG-58, which has 50-Ohm resistance. Network segments using this type of cable are to be used with 50-Ohm terminators, and devices are connected using BNC-T connectors. The type of thin coaxial cable used for CATV has 75-Ohm resistance.

Thick coaxial cable

Also known as *Thicknet*. The type of thick coaxial cable used for computer networks is RG-8. As the name suggests, this cable is about twice as thick in diameter as thin coaxial cable. These cables use a *vampire tap*, which cuts through the cable, to provide connectivity to network devices. Vampire taps use transceivers with a 15-pin AUI connector. Thick coaxial cables also use 50-Ohm terminators on both ends of the network segment.

Both thin and thick cables suffer from the same types of vulnerabilities. It is easy to perform a DoS attack on networks that use coaxial cabling. Coaxial cables are used in networks with bus topology. In a bus network, each device is a critical part of the network, and if a single workstation is down, the entire network segment comes down. If someone removes the terminator deliberately, it can bring down the entire network segment.

Unshielded fwisted pair/shielded twisted pair (UTP/STP) cables

UTP and STP cables have replaced coaxial cabling in most networks. The twists in cables are used to prevent electromagnetic interference, which results in crosstalk among cables. UTP and STP cables are twisted pairs of insulated cables bundled inside a plastic sheath. An STP cable comes with a layer of shielding material between the cables and the sheath. UTP/STP cable types are usually identified by their category numbers, which indicate the number of pairs inside the cable and for what purpose they can be used. These category numbers are denoted as CAT-1, CAT-2, CAT-5, etc. Table 11-3 lists some of the commonly used UTP/STP cables.

Table 11-3. Categories of UTP and STP cables

Category	Description
CAT-1	Used only in voice transmissions; not suitable for data transmissions.
CAT-2	Used for voice and low-speed data transmissions up to 4 Mbps.
CAT-3	Used for both voice and data transmissions. Used in Ethernet, Fast Ethernet, and Token Ring networks. Rated at 10 MHz.
CAT-4	Used for both voice and data transmissions. Used in Ethernet, Fast Ethernet, and Token Ring networks. Rated at 20 MHz.
CAT-5	Used for both voice and data transmissions. Used in Ethernet, Fast Ethernet, Token Ring, and 155 Mbps ATM networks. Rated at 100 MHz.
CAT-6	Used for both voice and data transmissions. Used in Ethernet, Fast Ethernet, Token Ring, and 155 Mbps ATM networks. Rated at 250 MHz.
CAT-6 (STP)	Used for data transmissions. Supports up to 600 MHz and used in Ethernet, Fast Ethernet, Gigabit Ethernet, Token Ring, and 155 Mbps ATM.
CAT-7	Also supports up to 600 MHz and used in Ethernet, Fast Ethernet, Gigabit Ethernet, Token Ring, and 155 Mbps ATM.

UTP/STP cables use Registered Jack-11 (RJ-11) and Registered Jack-45 (RJ-45) connectors to connect workstations and network devices, such as hubs, switches, and routers. They can be used in bus, star or Token Ring network topologies. The main advantage of using UTP/STP cables with the star topology is that even if one of the workstations is disconnected, the network is not affected.

UTP cables are vulnerable to Electromagnetic Interference (EMI) and Radio Frequencies Interference (RFI). Electric or electronic equipment in the vicinity of these cables can cause EMI and RFI disturbances. In order to prevent these, high-potential electric cables should not be run beside UTP cables. STP cables do provide some degree of protection from EMI and RFI disturbances, but it is more expensive than UTP cables. UTP cables are also vulnerable to eavesdropping.

Fiber optic cable

Fiber optic cable is made up of very thin glass or plastic stretched out and put inside a sheath. The transmission in fiber optic cables is based on transporting light signals. An optical transmitter is located at one side of the cable and a receiver at the other. Fiber optic cabling is very expensive in terms of the cost involved in installation and maintenance. It is used only in data centers to provide high-end connections to critical servers and other network devices where high-speed data transfers are required. They can also carry data signals for longer distances than UTP or STP cables.

Fiber optic cables are immune to EMI and RFI disturbances because they depend on optical signals, unlike the electrical signals in UTP/STP cables. They provide protection against eavesdropping and sniffing attacks.

> You will probably be asked a few questions about the selection of appropriate cable type for a given situation. Remember that when EMI and RFI disturbances exist, you can either use the STP cable or the fiber optic cable. When cost is a concern, UTP cable is your best choice for Ethernet and Fast Ethernet connections. Most building codes require the use of a specially built, fire-retardant cable known as *plenum-rated* cable. Plenum-rated network cables are generally required in overhead ceiling areas, called the *plenum area*.

Removable media

Removable media is used to transport data physically from one place to another or from one computer to another. They are also used for the long-term or short-term storage of data. For example magnetic tapes are used for data backups while compact disks are mainly used for distribution of software. This section covers security aspects related to removable media.

Magnetic tapes. Magnetic tapes are commonly used for backing up data because of their large capacity and their ability to be reused. These tapes come in the form of small cassettes with a variety of speeds and capacity. Tapes are vulnerable to physical thefts, as anyone with access to them can easily smuggle them out of the organization and get access to critical data. Some of the methods to secure data stored in magnetic tapes are described here:

- Data backed up on tapes should be encrypted so that if an unauthorized person gets access to the tapes, it is still difficult to get to actual data.

- Backup tapes should be stored at an offsite location. This not only ensures that the data will remain safe in case of a disaster but it also prevents data theft.
- Some organizations have installed security doors in data centers that help prevent bringing in or taking out any magnetic media.

When magnetic tapes are used for the storage of critical data (such as database servers), only authorized personnel should be allowed to perform backup operations, and a log of activities should be kept to trace any malicious activities.

Compact Disk-Recordable (CD-R). CD-R is one of the common media types used for software distribution and data storage. These disks use laser technology to read and write data. They are thus not susceptible to any magnetic, electromagnetic, or radio frequency interference. Due to their large capacity, they are commonly used to back up individual systems. A CD-R is vulnerable to physical scratches on its surface, which may even make it unusable. Theft of CD-Rs is also a vulnerability, and taking out CD-Rs from the organization should be prohibited in order to protect confidential data. The same security rules apply to Compact Disk-ReWritables (CD-RWs) also.

Hard drives. Hard drive refers to hard disks that are permanently installed inside computers and to removable hard drives that are externally attached to computers. Hard drives are also one type of magnetic media. They are not generally considered removable media, but for the purpose of the Security+ exam, the term *hard drive* refers to removable media. This is because many state-of-the-art servers support hot-swap mechanisms that allow removal of hard drives even when the server is powered on. Removable hard drives come in the form of Universal Serial Bus (USB) drives that can be easily attached or detached in systems that support Plug-n-Play (PnP) features.

For securing data stored in hard drives, there are a number of techniques that can be implemented. Some are as follows:

- Data stored on hard drives should be encrypted.
- Hard drives should be kept away from locations where strong magnetic fields exist.
- Only authorized administrators should be allowed to perform physical maintenance on hard drives, such as the addition or removal of defective drives and changes in configurations.
- Physical security of servers should be considered since hard drives are part of the server hardware.

Floppy disks. Floppy disks are another type of magnetic media used to transfer small amounts of data. Before CD-Rs and CD-RWs came into mass usage, floppy disks were the most common method of transferring data. To prevent data theft, floppy disks should not be allowed to be taken out of the organization. Similarly, employees should not be allowed to bring in floppy disks, as they might contain viruses or other malicious code. Many organizations these days do not even have floppy disk drives in their servers and workstations.

Flash cards. Flash cards are used for transferring small amounts of data from one place to another. These come in different varieties, depending on their type and capacity. Types of flash cards include the following:

- Memory stick cards, found in digital cameras and mobile phones.
- CompactFlash and SmartMedia cards, found in digital cameras.
- PCMCIA Type I and Type II cards, used in notebook (laptop) computers.
- Memory cards, used in video games.

Flash cards are prone to damage when they are dropped or brought within areas with high-static electricity. They are small in size and can easily be stolen. Some of the newer flash cards offer security features such as data encryption and authentication. It is good to use these security features to protect data from theft. Older cards that have limited storage capacity and no security features should be replaced with newer cards.

Smart cards. Smart cards usually store a small amount of data that is generally used to authenticate the holder or owner of the card. They typically come in the size of a standard credit/debit card. When used for authentication and identification purposes, these cards prevent modification of the data stored on them. Smart cards are designed to protect them against theft of data. They are immune to EMIs and RFIs and have built-in protection against physical damage.

Security Topologies

Not all networks are implemented in the same way. They differ by the network media and topologies, and placement of network devices, critical servers, and workstations around the building. Security topologies refer to the mechanisms used by organizations to secure the network from outside threats such as hackers. These mechanisms also help isolate the network from external networks such as the Internet. The topics covered in this section include concepts behind security zones.

Security zones

A security zone refers to the part of the network that has special security requirements. It is specifically built to protect critical servers against unauthorized access from inside and outside the network, and only need-based access is granted. DMZs, intranets, extranets, and virtual local area networks (VLANs) are all considered security zones. The following sections describe some of the common techniques used to create security zones for an organization.

The type of NOS used on servers inside a security zone is not important. For example, a security zone may have servers with a variety of NOS such as Unix, Windows Server, NetWare, or MAC OS. Security zones are protected by software- or hardware-based firewalls. These firewalls have the ability to perform the following actions:

- They allow only limited traffic based on certain rules, and block all unwanted, unsolicited, and malicious traffic.
- They maintain audit logs for incoming and outgoing traffic.

- They perform additional authentication for enhanced security.
- They mask the presence of network hosts inside the security zone to hide the internal map of the network segment.

Several hardware firewalls include a number of features such as VPN and IDS. The more features a single firewall supports, the higher its chances of being compromised at some point in time. Administrators need to be extra careful when using firewalls so that they are appropriately configured and regularly monitored to reduce the risk of an outside attack.

Demilitarized zone (DMZ). A DMZ, also known as a *Perimeter Network*, is a segment of the network that sits between the internal network of the organization and an external network, usually the Internet. In its typical implementations, the DMZ sits on the outer boundaries of the network, where network devices such as firewalls, routers, and switches allow only intended traffic and block all unwanted traffic. These devices perform a two-way action. The internal users are not allowed to reach harmful external Internet sites, and the external access is limited to resources located inside the DMZ. Figure 11-13 shows a DMZ.

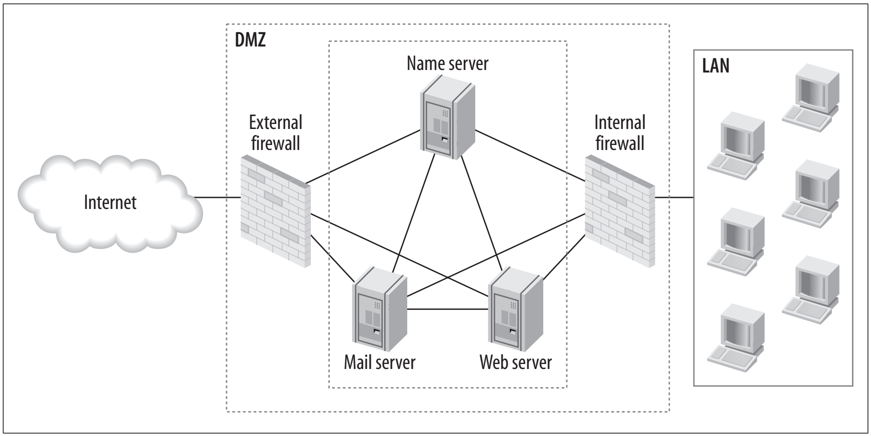


Figure 11-13. Demilitarized zone (or Perimeter Network)

Remember that mail servers, web servers, FTP servers, and DNS servers are usually placed inside the DMZ. The DMZ firewalls are configured in such a way that these servers are accessible to both internal and external clients. In some implementations, Intrusion Detection System (IDS) is also a component of DMZ.

There are two main types of DMZ implementations, as follows:

Multiple interface firewall

In this type of implementation, a single firewall with multiple interfaces sits between the Internet, the DMZ, and the internal network. This firewall has at least three interfaces. This implementation is used to reduce the cost involved in installing, administering, and maintaining the firewall.

Layered DMZ

In this type of implementation, the secure servers are placed between two distinct firewalls: external and internal. Each are configured with a different set of traffic filtering rules. Clients from the Internet are allowed limited access to the servers inside the DMZ by the external firewall, but the internal firewall blocks all access to the internal network. Each of the firewalls has two network interfaces. The interfaces of the external firewall connect to the Internet and the DMZ while the interfaces of the internal firewall connect to the DMZ and the internal network.

Depending on the size of the organization, there may be multiple DMZs in the internal network. Examples of these DMZs include: one for data storage; one for processing business information; one for financial data processing; and one for the research and development department. As the number of DMZs increase, the administration and maintenance of security also increases. Administrators have to deal with a large number of ACLs, firewall rules, and IDS signatures. This not only increases the administrative load but also slows down network traffic across different network segments. A smaller number of DMZs is easy to secure and maintain.

Intranet. Intranet refers to a private internal network. An intranet typically refers to an internetwork that extends the local boundaries of the network and extends connectivity to company employees at remote locations through a public network such as the Internet. The intranet is usually a private part of the web site of an organization that is accessible only by authorized employees. Intranets use strong authentication methods to provide secure access. When the intranet traffic passes through the Internet, a "tunnel" is created in the Internet using tunneling protocols such as PPTP or L2TP. The L2TP protocol is used with IPSec to provide an additional layer of security for transmission of data. RAS and VPN are examples of intranets.

Make sure that you understand the difference between the Internet, intranets, and extranets. Do not confuse these terms with Perimeter Network or Demilitarized Zones. A DMZ can be implemented for any or all of these services.

The following are some of the important security considerations when implementing intranets:

- Firewalls should be configured properly with access rules to allow only intended traffic and to block all unwanted or malicious traffic.
- Only authorized administrators should have physical access to configure and maintain firewalls and servers for the intranet.
- Security logs should be regularly monitored on firewalls and servers. It is a good habit to conduct frequent security audits of intranet equipment.
- L2TP and IPSec protocols should be implemented for additional security when the intranet uses VPN on the Internet.

- All servers should be kept updated with the latest service packs, security patches, and antivirus software. Virus scanners should be used regularly.
- Users must lock their workstations when not in use. Educating users on secure computing habits is one of the best defenses against outside attacks.

Extranet. Extranets allow external clients to access the internal network resources of an organization through the use of VPNs or RAS. Extranets may also be implemented to allow two or more partner organizations to connect their networks. Users who need access to internal resources of an organization are required to use strong authentication mechanisms to ensure network security. The same is true when employees of partner organizations attempt to access resources outside their internal network. Extranets should be implemented with the same level of security as used for implementing intranets. It is always good to use authentication, access control, and authorization methods, and to use encryption for transfer of data between employees of different companies. Aside from this, only a handful of employees should be granted access, and even then to only the data they require from networks of other organizations.

Virtual local area network (VLAN)

A VLAN is a virtual or logical grouping of network devices that share common security requirements. It is not a separate physical segment of a network. Computers connected to a single VLAN behave as if they are in a single network segment although they may be physically connected to separate segments. Administrators create VLANs using software applications. The advantage of VLANs is that even if the computers are moved from one physical network segment to another, they remain on the same VLAN. A VLAN is thus a mechanism to create logical segments inside a physical network comprised of multiple physical segments.

In large Ethernet networks, *collisions* are a main problem. Collisions occur when a large number of devices attempt to start transmitting signals on the same network media. Network bandwidth gets congested with large numbers of collisions. VLANs help reduce these collisions by creating separate broadcast domains. This also provides security at the Data Link layer (Layer 2) of the OSI model.

Network switches that support VLAN protocols (known as *VLAN-aware devices*) are mainly used to create VLANs. Cisco switches, for example, use the IEEE 802.1Q standard and the Inter-Switch Link (ISL) protocol to make VLANs. Cisco switches also use VLAN Trunking Protocol (VTP), which is proprietary to Cisco, to create VLAN *Trunks*. A Trunk is defined as the point-to-point link between one switch and another. VLAN Trunks allow the creation of *VLAN domains*, which help administrate VLANs. The following are some of the other characteristics of VLANs:

- They are created on the basis of groups and memberships. VLAN memberships can be port-based, protocol-based, or MAC address-based.
- They function like a separate physical network segment as far as network traffic is concerned.
- They can span multiple physical network segments or multiple switches.
- A Trunk carries network traffic between each switch that is a part of a VLAN.

Network address translation (NAT)

NAT is a feature of firewalls, proxy servers, and routing services, such as RRAS in Windows Server 2003. It is used to provide secure Internet access to clients on the internal network. One of its main features is it hides the internal IP addressing scheme and network design from the outside world. If an attacker does not know the internal design of the network, it is difficult for him to exploit it by gaining access to internal resources. NAT also enables organizations to host web and mail services securely.

In a typical NAT implementation, only one server running the NAT protocol is connected to the Internet. This server shares the connection with internal clients and allocates IP addresses to these clients from the private IP address range. Private IP address ranges include the following addresses:

- Class A: 10.0.0.0 to 10.255.255.255
- Class B: 172.16.0.0 to 31.255.255
- Class C: 192.168.0.0 to 192.168.255.255

Private IP addresses are *nonroutable*, meaning that they cannot be used to directly access the Internet. The external interface of the NAT device or server uses one (or more) public (registered) IP address. A NAT device translates private IP addresses into one (or more) public IP address to provide Internet access to internal clients. This enables the NAT device to hide internal address assignments from an outside hacker. This function is also known as a *NAT firewall*.

On Windows XP computers, a scaled-down version of NAT called *Internet Connection Sharing (ICS)* is available. The only difference is that ICS can use only one public IP address, while internal clients can use only the class C private IP addresses. This makes ICS suitable for only a very small network that does not have any subnets.

Tunneling

Tunneling is used to create a virtual tunnel (a point-to-point communication link) between one computer and another or on a network using a public network such as the Internet. Details of VPNs and tunneling protocols and their security aspects were covered in the “Virtual Private Networks (VPNs)” section earlier in this chapter.

Intrusion Detection System (IDS)

IDS is used to detect intrusions and malicious activities in corporate networks that usually cannot be detected by conventional firewalls. IDS typically works by continuous monitoring of the network activities and comparing them to known attack signatures. They can be hosted on a single system to monitor activities on the host or on dedicated devices across the network to monitor the entire network traffic. IDS is classified into the following two categories:

Active IDS

An active IDS (or reactive IDS) monitors the network traffic and, upon detection of an attack or a security breach, can reprogram the firewalls or routers or even block certain network traffic from entering or leaving the network.

Passive IDS

A passive IDS monitors the network traffic and, on detection of an attack or a breach of security, logs the necessary information and sends an alert to the administrator. It is up to the administrator to take a corrective action to foil the attack or malicious activity.

To be effective, any IDS should be able to detect attack signatures and generate necessary administrative alerts, update log files, and take corrective action. Improperly configured IDS is prone to *false positives* and *false negatives*. A false positive occurs when an IDS triggers an alert even when there is no attack. A false negative occurs when the IDS is not able to trigger an alert even when there is a real outside attack. IDS can be implemented in any of the methods discussed in the following sections.

Network Intrusion Detection System (NIDS). An NIDS (or a network-based IDS) detects intrusions by monitoring all network traffic and multiple hosts (usually critical servers) in the network. An NIDS gains access to network traffic by connecting to hubs, switches, and routers that are configured for port monitoring. *Snort* is an example of a typical NIDS. Most NIDSs can also perform a corrective action if they detect an intrusion in the network. These actions range from sending an alert message to the administrator to blocking traffic from specific IP addresses or port numbers in the network. One of the major drawbacks of an NIDS is that it can slow down the network because it monitors and analyzes all IP packets in each network segment.

Network-based IDS are passive devices that can monitor the entire network traffic without affecting the performance of the network. They are easy to install and usually difficult for hackers to foil. The drawback is that these systems may overlook attacks launched during peak traffic hours in large networks. Another limitation is that they cannot monitor encrypted traffic, unless they are used with specialized hardware.

Host-based IDS. A host-based IDS is a software application that monitors network traffic coming in or going out of a specific network host. These applications monitor system logs, filesystem modifications, or system calls by malicious applications. A host-based IDS works only on the host where it is installed. It can monitor activities on the host with a high level of detail and can detect whether any user is involved in malicious activities. It can detect even activities that the network-based IDS cannot. A host-based IDS is also capable of examining encrypted network traffic, storage devices, and application activities.

A limitation of host-based IDS is that it logs malicious activities only on the computer on which it is installed. Professional hackers can disable the IDS application by a DoS attack. Host-based IDS also requires significant processing time, storage, and memory on the host, which affects the host's performance.

Signature based IDS. Signature-based IDS is the most widely used IDS. It continuously monitors the network traffic to detect signs of an attack. *Attack signatures* are defined as a set of events that constitute an attack pattern. If a match is detected, an alert is generated so that administrators can take corrective action. It is important for administrators to keep the attack signature database up to date, which is the most difficult part of implementing IDS. Most attack signatures are constructed by running different types of attacks against the network and looking for a unique pattern of the attack.

A limitation of signature-based IDS is that it can detect only those attacks for which signatures or patterns are known. Attackers can evade the signatures by modifying IP packets and thus hiding the real signature of the attack. Also, if the attack signature database is not kept up to date, it is easy for an attacker to evade the entire detection system.

Application protocol-based IDS. Application protocol-based IDS usually monitors the activities of specific applications and the protocols used by these applications. It is able to detect attacks by analyzing application logs, and it can identify a variety of attacks. It can also monitor malicious activities of individual users and is able to work with encrypted data. The drawback is that these IDS consume a significant amount of processing time on the host where they are installed.

Protocol-based IDS. Protocol-based IDS monitors the communication protocol used by incoming traffic in a system.

Hybrid IDS. Hybrid IDS combines one or more approaches to monitor network traffic. *Prelude* is an example of hybrid IDS.

Honeypots

A honeypot is a trap used to attract attacks on a network. It is a computer system or a part of the network that is deliberately left exposed to attackers so that they can launch different types of attacks on the network. The setup consists of a number of vulnerable servers, firewalls, and routers, most left with their default configurations. To the attacker, a honeypot appears to be a critical server or part of a network that contains information valuable to the attacker, but is actually an isolated and protected network segment. In most cases, the attacker does not know that he is attacking a fake network site. The part of the network that is exposed to attackers is known as a *honeynet*.

The purpose of using honeypots and honeynets is to test the intrusion detection systems used by an organization. Administrators use these as surveillance and early warning tools. Administrators use honeypots to lure attackers and have them indulge in malicious activities. It provides them with the opportunity to know the attack mechanisms used by attackers, and to use them later to update the attack signature database. Honeypots must be administered with care because they may accidentally expose the organization's real network. It may require a full-time administrator to properly configure the honeypot and regularly monitor the activities of the attackers.

> Make sure that you can distinguish between a honeypot and a honeynet. A *honeypot* is a computer system that is deliberately exposed to an external network. A *honeynet* is a network specifically configured to lure outside attackers. On the other hand, attackers are also clever enough to use *honeypot detection systems*.

Incident response

When an attack is detected, administrators must take some sort of corrective action to prevent the attack. In some situations, it takes time for administrators to collect enough information and evidence about the attack and to decide on a corrective action. They may need to know the origin of the attack, the method used by the attacker, and the target system or network segment. Administrators must log all the information so that if the attacker is identified, there is enough information that can be used as evidence. The activity log files must be saved for possible prosecution of attackers. Incident response is covered in more detail in the "Operational and Organizational Security" section of this chapter.

Operating System Hardening

Operating system hardening refers to locking down the operating system to protect the system from vulnerabilities of default configurations. These include both the desktop operating system (OS) and the network operating system (NOS). Basic operating system hardening starts with granting need-based or role-based access to operating system files, data files, and other applications that run on a system. The process of system hardening may include implementing access control on the filesystem and keeping the operating system updated with the latest service packs, hotfixes, and security patches.

Filesystems

Filesystems such as NTFS used in Windows NT and later network operating systems allow administrators to grant need-based access to files and folders. Administrators generally apply the *principle of least privilege* while assigning permissions to users on shared resources. Users are categorized according to their job functions and put into groups. These groups are then assigned as much permission for shared resources as is necessary to perform their jobs. The main idea behind the principle of least privilege is to grant restricted access to resources in order to prevent undesired and unauthorized access to resources. This helps protect valuable system resources from potential damage from inside users as well as from the outside. It is also important to note that administrators regularly audit the use of privileges and monitor activities to detect any malicious attempt to gain unauthorized attempt to restricted documents.

Updates

Manufacturers of operating systems and network operating systems release updates from time to time to address specific problems with their software. For example, Microsoft regularly releases security updates for all of its current operating systems. It is necessary that administrators keep the OS and NOS updated as per the manufacturer's guidelines. These updates come in three different types, as explained in the following sections. All updates, including security updates, should be tested before they are installed on production servers or desktops. All updates are offered free of cost to registered users of OS and NOS on the manufacturer's web site.

Hotfixes. A hotfix is a small piece of software that is used to address a specific problem with the operating system. Hotfixes are generally released as soon as the manufacturer discovers a serious issue. Administrators should be careful to test the hotfixes on nonproduction servers and desktops before installing them on production servers. In some rare situations, hotfixes are known to have opened up security holes in critical servers.

Service Packs (SPs). An SP is a collection of a number of hotfixes and updates released by the operating system manufacturer. OS/NOS manufacturers usually test service packs on a variety of hardware platforms and check their compatibility with various applications. As with updates and hotfixes, service packs must be fully tested on nonproduction servers before they are installed on production servers. Administrators should spend some time reading instructions that accompany service packs. It is wise to check the problems addressed by these service packs. Manufacturers usually announce service pack releases, and they are available for download free of cost on each manufacturer's web site, or they can be ordered on a compact disk (CD).

Patches. Patches are released by operating system manufacturers to immediately address a small problem. Most of the patches are related to security but they often address other problems, such as compatibility issues or malfunctioning of a particular OS component. Manufacturers usually do not announce the release of patches to their software. It is up to the administrators to regularly check the web sites of manufacturers to keep up to date about these.

Network Hardening

Network hardening is the process of locking down network devices and media to protect it from external and internal threats. Network hardware such as routers, switches, and firewalls also have operating systems. Cisco IOS (Internetwork Operating System) is an example of an operating system used on Cisco routers. Network hardening tasks include updating the firmware on network devices, correctly configuring devices, and configuring access control for administrative access.

Updating firmware. Firmware is software that is embedded in a hardware device. It is usually stored in flash ROMs inside the device or provided as a binary image file that can be uploaded into the device. It is also stored on *Electrically Erasable Programmable Read Only Memory (EEPROM)* installed inside hardware devices. Like OS and NOS, manufacturers of network devices also release updates for firmware to address specific operating problems. If a manufacturer releases a firmware update, administrators should check for the issues that it addresses and, after proper testing, update the network devices.

Configuration. Network devices, such as routers, switches, and firewalls, usually come with default configurations. For most common applications, these configurations are set by the manufacturers. It is not necessary that these configurations fulfill the requirements of a particular network setup. Administrators are required to configure these devices as per the needs of the organization or the network setup. An improperly configured network device may leave security holes in the network, making it vulnerable to outside threats. Attackers are always looking for loosely configured network devices or for devices with the default configuration in order to find methods of exploiting a network.

Access Control Lists (ACLs). Like operating systems and network operating systems, network devices also use ACLs, which can be configured to allow administrative access to these devices to authorized personnel only. Firewalls use ACLs to define traffic rules. Similarly, a router can be configured with these ACLs to permit or deny traffic based on protocol, port number, IP address, or interface. Besides administrative access, these devices also allow administrators to configure the following types of ACLs for each connection to the device:

- The protocols allowed passing through the device.
- The port number(s) that can be used by protocols or applications.
- The source and destination IP address for the network connection.
- The source and destination MAC address (in case of a switch) for the network connection.
- The interface used by the connection.

As much as possible, administrative access to network devices should not be allowed to unauthorized personnel. Using Telnet sessions for remotely managing these devices is also considered a security risk because Telnet sessions use unencrypted transmissions.

Application Hardening

Applications installed on desktops and servers should be kept up-to-date with the latest service packs, hotfixes, and security patches. Vendors of applications often offer these updates for free download on their web sites. Updates are sometimes meant only for cosmetic changes to the application, while hotfixes and patches are meant to address known functional problems that have been detected by the vendor or were reported by users. Administrators must be careful to read the accompanying information about application updates to find out whether a specific update is really needed for their installations. If a security patch, hotfix, or service pack is required, it first must be thoroughly tested on nonproduction servers before it is installed.

Web servers

Web servers are used to host web pages on the Internet. Examples of web servers include Microsoft's Internet Information Server (IIS) for Windows, and Apache web server for Unix/Linux. Web servers are accessible by users who are outside the organization, and it is important that these servers are properly secured before outside access is allowed. Here are some important points for web server security:

- The NOS over which the web services are running must be secured properly, and it should be kept up to date with security patches, hotfixes, and service packs.
- Antivirus software should be run regularly with updated virus signatures.

- Web services should not be left in their default configurations.
- If a web service uses a named account to authenticate anonymous users, its access should be restricted to so that it does not grant any anonymous user administrative or local access to the web server.
- If the organization is involved in e-commerce, user authentications should be done using strong protocols, and all transactions should be encrypted.
- Web servers should be placed inside a DMZ.

Email servers

Email servers run messaging applications such as Microsoft Exchange and are usually connected to the Internet. Similar to web servers, they are also subject to unauthorized outside access. It is important to lock down email servers to prevent possible security breaches or attacks. Here are some important points for email server security:

- The NOS over which the email services are running must be secured properly, and it should be kept up to date with security patches, hotfixes, and service packs.
- Antivirus software should be run regularly with updated virus signatures.
- Email relay (SMTP relay) should be disabled because it can cause DoS attacks.
- Viruses usually spread through email attachments. Users must be careful not to open suspicious messages.
- Use of HTML email should be avoided.
- Internet Messaging (IM) outside the organization should be monitored, if it cannot be prevented.
- Email servers should be placed inside a DMZ.

FTP servers

FTP servers are also permanently connected to the Internet and also attract malicious users from outside the organization. Most FTP servers allow anonymous or unrestricted access to resources on the FTP server. This is a potential security issue that must be addressed by administrators. The following are some important points regarding FTP server hardening:

- The NOS over which the email services are running must be secured properly, and it should be kept up to date with security patches, hotfixes, and service packs.
- Antivirus software should be run regularly with updated virus signatures.
- Filesystem security should be appropriately configured.
- Access control, authentication, and authorization systems should be in place.
- An audit policy should be implemented, and security logs should be reviewed regularly.
- FTP servers should be placed inside a DMZ.

DNS servers

DNS servers are used to resolve domain names to IP addresses. Apart from normal NOS hardening, DNS servers should be configured properly to allow only authorized network traffic. DNS servers are of special interest to attackers because they store the names and IP addresses of the entire network in resource records. Most new DNS servers have the ability to get their records dynamically updated by DHCP servers. An attacker can easily plant false resource records and direct all network traffic to a DNS server that is in his control. DNS servers are usually victims of DoS and MITM attacks. The following are some important points regarding DNS server hardening:

- DNS servers update other DNS servers using a process known as *zone transfers*. Administrators should configure zone transfers to authorized DNS servers only.
- DNS servers should listen to name resolution requests from intended interfaces only.
- If using dynamic updates, secure dynamic updates should only be used.
- Administrators should make sure that there are no rogue DNS servers in the network.
- DNS servers that are used for web services should be placed inside a DMZ.

NNTP servers

Network News Transfer Protocol (NNTP) servers that are used to carry newsgroup feeds from the Internet are also vulnerable to outside attacks such as a DoS attack. NNTP server vulnerabilities are similar to email servers. It is important that NNTP servers are properly configured for storage, that they purge newsgroup records, and that they place a limit on attachments. Malicious code coming with attachments can be dangerous if it is accepted and stored on NNTP servers. NOS hardening, filesystem permissions, and antivirus software are some of the factors that must be kept in mind when securing NNTP servers.

File and print servers

File and print servers are the most frequently used servers within an organization, and thus are heavily loaded. They constitute a majority of shared network resources. These servers run a file- and printer-sharing service so that users on the network can connect to and work on shared resources located on these servers. These servers are also used to host critical data for an organization, and should be properly secured with ACLs, authentication, and effective auditing and logging. Some filesystems such as Microsoft's NTFS were known to have built-in vulnerability in Windows NT and Windows 2000 operating systems. When a file or folder was shared, the *Everyone* group, which included all inside and outside users, was automatically assigned full control permissions. Aside from this, the file- and printer-sharing service in Windows uses NetBIOS with Server Message Block (SMB) broadcasts to advertise shared resources on a computer. NetBIOS and SMB are considered vulnerable to malicious attacks on file and print servers.

File and printer sharing should be secured to prevent any malicious activities by an insider or an outsider. If a user does not need to share a file or folder, he should not share it. Administrators should configure proper access permissions on a user's home directories and other shared resources. Default share permissions should be disabled, and anonymous access should not be allowed at all. Insecure network protocols such as NetBEUI and NetBIOS should be disabled, if not required.

DHCP servers. DHCP servers are used to automatically assign IP addresses to DHCP clients when they start up. DHCP servers maintain blocks of IP addresses in DHCP scopes. If an outsider gains access to a DHCP server, he can easily get information about the internal IP addressing scheme used by the organization. Administrators should take steps to properly configure DHCP servers in order to prevent accidental exposure to outsiders. Operating systems such as Microsoft's Windows Server 2003 have the ability to detect the presence of a rogue DHCP server inside the network. A rogue DHCP server can cause IP address conflicts if allowed to assign IP addresses. However, Windows Server 2003 DHCP servers interact with the Active Directory service and the DNS service. DHCP servers must be authorized in Active Directory before they can serve clients. But older Windows NT and Windows 2000 DHCP servers may still exist in a Windows network with invalid IP address scopes and may act as rogue DHCP servers.

The following are some important points regarding DHCP server hardening:

- The NOS over which the email services are running must be secured properly, and it should be kept up to date with security patches, hotfixes, and service packs.
- Antivirus software should be run regularly with updated virus signatures.
- If rogue DHCP servers are detected, they should be disabled or taken offline immediately.
- IF DHCP servers interact with DNS servers to update DNS records dynamically, secure updates should only be configured.
- Only authorized administrators should be permitted to manage DHCP servers.

> One of the major security concerns in older operating systems was the use of username as *administrator* and a blank password for the administrator account. Even now some applications allow administrators to keep their passwords blank. This is a serious security concern; administrators should not exercise this option at any cost.

Data repositories

Data repositories in a network include data storage systems, which can be servers running directory services, database servers, *Network Attached Storage (NAS)* systems, or *Storage Area Networks (SAN)*. Since these systems store critical data required to run the organization's business, steps should be taken to properly configure them in order to prevent data theft or other malicious activities. As much as possible, the data should be stored in an encrypted format, and all traffic to and from these systems should also be secured.

Directory services. Novell's E-Directory and Microsoft's Active Directory offer several mechanisms, including authentication, encryption, and filesystem permissions, in order to address unauthorized access to data repositories and storage networks. Systems hosting directory services should be hardened with the latest service packs, security patches and hotfixes. These systems must be managed by authorized, trained, and trusted administrators only. Administrators should use strong passwords and change them frequently. When working from remote systems, an administrator must be careful to log off before she leaves her seat and to lock her workstation. Another important security (and safety) precaution is to use a regular user account when not performing any administrative task.

Databases. Examples of database servers include Microsoft's SQL Server and Oracle. These database servers pose a challenging task for administrators in terms of hardening these servers and maintaining their security. Database applications are usually the client/server type where the database server is called the *backend* and the client workstation is called the *frontend*. Administration of database applications and servers usually requires separate database administrators who manage access control, authentication, and auditing of these services. These administrators must ensure the security of data stored in the databases, which may be very critical to the functioning of the organization. Organizations involved in e-commerce also use database servers to store product information and client information. Database servers used for e-commerce should be placed in a DMZ. As with other servers, database servers must also be kept up to date with the latest security patches, hotfixes, and service packs for both the NOS and the database application.

Basics of Cryptography

The term *cryptography* is derived from a Greek word that means "hidden." In computing, cryptography refers to the methods used to "hide," or secure, communications from unauthorized access. Cryptography is also known as *encryption*. Encryption is done using established encryption algorithms or procedures. These algorithms may include symmetric, asymmetric, or hashing algorithms. Encryption algorithms further lay the foundation for a PKI, which is one of the widely used methods to secure network communications. This section includes a discussion of important encryption terms, algorithms, and Public Key Infrastructure.

> The terms *cryptography* and *encryption* are used interchangeably in the following text.

Encryption Algorithms

An *algorithm* is defined as a procedure or a well-defined set of instructions to accomplish a task when the initial state of the problem is given. In encryption methods, the term *encryption algorithm* is used to define the process of creating a scrambled or unreadable text (known as *cyphertext*), from a given readable text (known as *plaintext*), using the defined procedure. Encryption is used as a protective cover for the data transmitted over network media from one computer to another. Encryption keeps the data secure from unauthorized access by users and by professional hackers. Encryption algorithms lay the foundation for such security mechanisms as confidentiality, authentication, digital signatures, and public key cryptography. They are used to calculate a *secret key*, which is used to encrypt and decrypt messages. Only the persons who possess the key can encrypt or decrypt messages. Encryption algorithms fall into the following main categories:

- Symmetric algorithms
- Asymmetric algorithms
- Hashing algorithms

Symmetric algorithms

Symmetric algorithms, or *symmetric key algorithms*, use one key for both encryption and decryption of messages. One copy of the key is known to each end of the communication. It is also commonly known as *secret key encryption*, or *shared secret encryption*. In some implementations, and for the Security+ exam, symmetric key encryption is referred to as *private key encryption*. Symmetric key encryption is widely used for encryption because of its simplicity, ease of implementation, and speed. The strength of the key is determined by its size. The larger the key, the stronger the encryption.

Symmetric algorithms are prone to *brute force attacks*. In a brute force attack, the attacker attempts to break the key by guessing it. He may use a number of mechanisms to guess the key until the key is able to decrypt the message. Symmetric algorithms are also vulnerable to plain-text attacks. The keys need to be chosen, stored, and distributed using secure methods. Symmetric keys must be changed frequently to protect them from being compromised.

Symmetric algorithms are divided into *stream ciphers* and *block ciphers*. Stream ciphers encrypt bits of the message, one at a time. Block ciphers take blocks of bits, usually 64 bits at a time, and encrypt them as one unit. Some of the popular symmetric algorithms are DES, 3DES, AES, and IDEA, as discussed in the following sections.

Data Encryption Standard (DES). DES is one of the oldest symmetric encryption algorithms. It works on block ciphers of fixed length. DES uses a single 64-bit block of plain text for encryption. It also uses a 64-bit key, and out of these, 56 bits are used for data and 8 bits are used for checking parity. The actual length of the key is thus only 56-bits. The DES key is broken into 16 48-bit subkeys, one for each round, known as *feistel function*. DES is known for its weak encryption security due to the small size of the key (56 bits). It is prone to brute force attacks, and in some cases, it has taken less than 24 hours for attackers to break the key.

DES has been replaced by *Triple DES* (written as *3DES* or *TDES*). 3DES uses the same 56-bit key three times to make the key size larger. Two or three 56-bit keys are connected to form 112- or 168-bit keys respectively. The resulting ciphertext is far more secure than the DES encryption and can prevent more brute force and MITM attacks.

Advanced Encryption Standard (AES). AES is also known as *Rijndael* (pronounced "rain dall") and is the most widely used block cipher symmetric encryption standard. This is mainly due to its support for large ranges of text blocks and key sizes. It supports key sizes of 128, 192, and 256 bits. It is stronger and faster than 3DES and consumes less processing power and memory. The number of bits used for a data block is 128 broken into four groups of 32 bits. Instead of using feistel cycles, it uses *iterative rounds* for keys. The number of rounds depends on the size of the key. The 128-bit key has 10 rounds, the 192-bit key has 12 rounds, and the 256-bit key has 14 rounds.

The only known successful attack against AES is a *side-channel attack*, an attack based on information gained from physical implementation of an encryption mechanism instead of the weakness of the algorithm. Another type of known attack is called *cache-timing attack* (or simply *timing attack*), which takes advantage of the time taken to perform encryption. Since AES uses 10, 12, or 14 rounds, the last known attack has been on 7 rounds. As a result, AES is considered to be a strong encryption algorithm.

International Data Encryption Algorithm (IDEA). IDEA is a faster and more secure algorithm than DES. This is due to the fact that each round consists of more simple operations than feistel cycles in DES. IDEA operates on 64-bit blocks with a 128-bit subkey. The encryption and decryption process uses eight rounds with 16-bit subkeys per round. IDEA is used as one of the components of PGP for secure messaging.

Asymmetric algorithms

Asymmetric algorithms are commonly used for public key cryptography. Asymmetric algorithms use two keys—one for encryption (*public key*) and the other for decryption (*private key*). The encryption key can be freely distributed, but the private key must be held in strict confidence. The two keys are generated together, but the private key cannot be derived from a public key. Figure 11-14 shows how message encryption and decryption are accomplished using public key cryptography.

Asymmetric algorithms are much slower than symmetric algorithms. The process puts a significant load on the computer's processor and memory. Aside from this, the keys used for asymmetric encryption are much larger than those used for symmetric encryption. Asymmetric keys are used only for encrypting small amounts of data. The most common application of asymmetric keys is for ensuring confidentiality of data. Public key digital signatures are used for authentication and non-repudiation of the sender. These terms are explained later in the section "Concepts of Cryptography."

The sections that follow cover asymmetric encryption algorithms.

Diffie-Hellman. The Diffie-Hellman algorithm, or the *Diffie-Hellman key exchange*, is used for a secure key exchange. It allows two parties to establish a shared secret key over an insecure communication channel. This key can then be used to establish a secure encrypted communication using a symmetric key encryption. The messages encrypted by one party can be decrypted only by the other party that

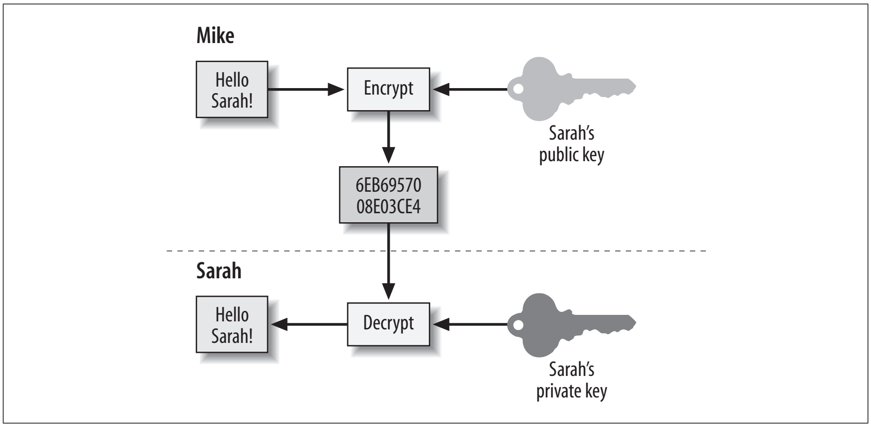


Figure 11-14. Using public and private keys in an asymmetric algorithm

possesses the secret key. This algorithm is used only for the transportation of secret keys and not for encrypting data. The following steps are involved in a key exchange:

- The two parties agree on two numbers: a large prime number and a small integer number.
- The two parties separately generate another number, equivalent to a private key, which is kept secret. Both parties make calculations involving the private key and the previously agreed numbers. The result of the calculation (the public key) is sent to the other party.
- The two parties then exchange their public keys. Each party then makes another calculation using its private key and the other party's public key to produce another number known as the *session key*. The session key that is calculated by each party should be the same.
- The session key can then be used as a secret key for further encryption. No third party can decrypt the message without knowing the secret key.

If the initial numbers are chosen carefully, the Diffie-Hellman key exchange can be a strong algorithm for protecting the shared secret key because both the private key and the public key are actually very large integers. IPSec uses the Diffie-Hellman key exchange along with RSA authentication for exchanging session keys. This algorithm is considered secure against eavesdropping and MITM attacks.

RSA. The RSA algorithm was developed by Rivest, Shamir, and Adleman (hence the name RSA) as another public key encryption system. It shares many similarities with Diffie-Hellman but is much faster. However, it is much slower than DES. RSA was the first asymmetric algorithm found to be suitable for digital signatures as well as for encryption. RSA also involves two keys: a private key and a public key. With RSA encryption, the key distribution must be handled by a PKI to protect it from MITM attacks.

ElGamal. The ElGamal asymmetric key encryption algorithm is an extended and improved version of the Diffie-Hellman key exchange algorithm. Practically, this algorithm is considered as secure as RSA. ElGamal produces large sizes of ciphertext and can be used on fast WAN links only. It is used in some recent versions of PGP. *Digital Signature Algorithm (DSA)* is a variant of the ElGamal signature scheme and is based on the ElGamal algorithm.

Hashing algorithms

A hashing algorithm (also called a *hash function*) is the process of creating a small and unique digital "fingerprint" from any kind of data. The fingerprint is known as the *hash value*. The hash value is represented as a short string of random letters and numbers. If the original data changes even by one character, the hash function will produce a different hash value. Thus, the receiver will know that original data has changed. The hash function is also known as a one-way process, because it is not possible to create the original text using any reverse hashing function. Figure 11-15 shows an example of the hashing function.

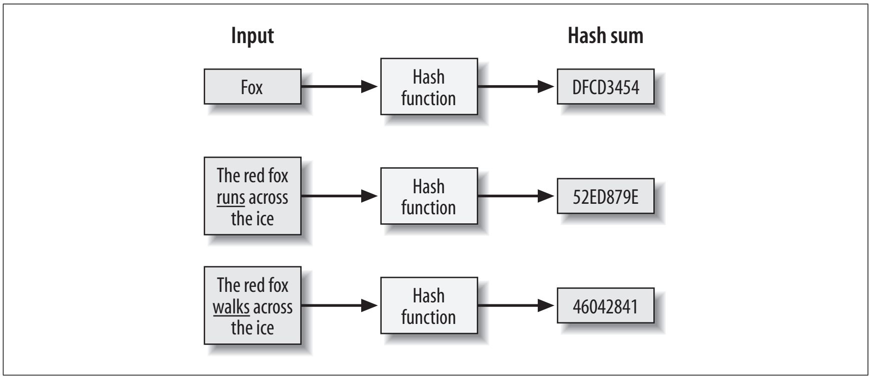


Figure 11-15. Example of a hash function

Hashing algorithms are used to provide integrity and authentication of data sent over network media from one computer to another. A good hashing algorithm is the one that will not produce the same hash values for any two inputs, which is a property known as *collisions*.

It is common to store encrypted passwords as hashes in secure networks. When a user sets her password, it is passed through a hashing function, and only the encrypted hash is stored. When the user logs on to the network, her password is hashed again and the two hash values are compared. If a match is found, the user is granted access; otherwise, she is denied. The following are two commonly used hashing algorithms:

Message Digest5 (MD5)
: MD5 is a widely used hashing algorithm with a 128-bit hash value. This algorithm is mainly used for digital signatures to check the integrity of data. The older version, MD4, also used a 128-bit hash value but this had flaws in it.

Secure Hash Algorithm-1 (SHA-1)

SHA-1 was developed by the National Security Agency (NSA). It uses a 160-bit key hash value and is considered more secure than MD5. It is commonly used with IPSec installations.

> At the time of this writing, SHA-2 is the current version of SHA. SHA-2 is a collection of four variations that include SHA-224, SHA-256, SHA-384, and SHA-512. The Security+ exam covers only the SHA-1 algorithm. Also remember that creating a hash value using a hashing algorithm is a one-way process.

Concepts of Cryptography

The terms cryptography and encryption are used interchangeably. Encryption is the process of applying a procedure, known as an algorithm, to plain text in order to produce an unreadable text. This unreadable text can be read only if someone has the key to decrypt the message and convert it back to plain text. For all others, the encrypted text remains useless. The following are some of the concepts behind using encryption in network transmissions.

Confidentiality

The main idea behind encryption is to ensure the confidentiality of messages that travel from one computer to another. *Confidentiality* means that only the intended recipient can decrypt the message and read its contents. Confidentiality of network transmissions can be assured only when users keep their secret keys (used in symmetric algorithms) and private keys (used in asymmetric algorithms) *really* secret. They are not supposed to, and should not, give their keys to anyone else. If the secret key or the private key is lost or compromised, confidentiality of messages from the sender cannot be assured.

Integrity

The integrity of a message ensures that the message has not been intercepted, modified, or altered while it traveled from one point to another. In cryptography, most asymmetric encryption algorithms have built-in mechanisms to ensure the integrity of messages (simply called *Data Integrity*). Digital signature is one of the methods to ensure data integrity and non-repudiation. Digital signatures are helpful in protecting messages against MITM attacks.

Digital signatures. Digital signatures are used to provide data integrity and non-repudiation of data. These ensure that the data sent was not intercepted or modified on its way from the source to the destination. When the message is sent, it is subject to a hash using one of the hashing algorithms to produce a hash value. The hash is further encrypted using the sender's private key, and appended to the message. The receiver uses the sender's public key to decrypt the hash created by the sender. The receiver also creates a hash of the message, and the two hash values are compared. If the receiver's hash value matches the sender's, the receiver is ensured that the message has not been modified on its way.

Authentication

Authentication refers to verification of the sender of the message. Symmetric encryption algorithms do not provide authentication mechanisms. Asymmetric algorithms have built-in mechanisms to provide authenticity of the messages or data. In asymmetric encryption, the message is encrypted using the sender's private key, and, because each person is responsible for maintaining his private key, the receiver is assured that by decrypting the message using the sender's public key that only the intended sender has sent the message. This proves the authenticity of the message.

Non-repudiation

Asymmetric encryption algorithms ensure that the sender of the message cannot deny that he has sent the digitally signed message. The process is known as non-repudiation. This relies on the fact that the sender keeps his private key truly private—this private key should not be given to anyone else. The receiver can be assured that only the sender has a specific private key and that he has sent the message. Once again, digital signatures are used to ensure non-repudiation in addition to providing the integrity of the message.

Public Key Infrastructure (PKI)

A PKI enables an organization to securely exchange messages through the insecure public network (such as the Internet). It enables users to securely exchange confidential data using public and private keys obtained through a trusted authority. This section covers a summary of different terms and concepts used in the public key cryptography infrastructure.

Certificates

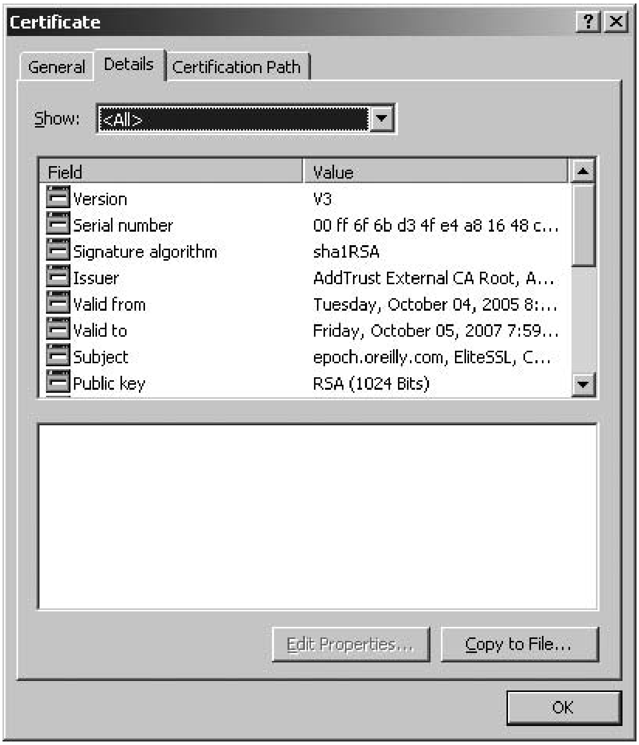
A certificate, or a *digital certificate*, is based on the X.509 standard and is used to identify an individual or an organization. It is issued by a CA to bind a public key to an individual or an organization. The name of the individual or the organization appears as a distinguished name, an email address, or a DNS name. An organization may use certificates for a variety of purposes such as encryption of email messages, doing business on the Internet, or digitally signing software applications.

When downloading software from the Internet or when making online purchases, you may check the validity of the digital certificate of the organization (or its web site) by clicking the little lock sign that appears on the righthand bottom corner of the web browser. Follow the steps given here to view the details of a digital certificate:

1. Open a web site where you can do some online shopping. For example, go to *www.oreilly.com*.
2. Choose a book and click the Add to Cart button. You are taken to the secure web site, *https://epoch.oreilly.com*.
3. The next page shows a little yellow lock sign in the righthand bottom corner of the web browser.

4. Double-click the lock sign. This opens the Certificate window and displays the general properties of the certificate.
5. Click the Details tab to view the details of the certificate.
6. Click OK to close the window.

Figure 11-16 shows a sample certificate issued to O'Reilly's web site, *www.oreilly.com*.



Show: <All>

Field	Value
Version	V3
Serial number	00 ff 6f 6b d3 4f e4 a8 16 48 c...
Signature algorithm	sha1RSA
Issuer	AddTrust External CA Root, A...
Valid from	Tuesday, October 04, 2005 8:...
Valid to	Friday, October 05, 2007 7:59...
Subject	epoch.oreilly.com, EliteSSL, C...
Public key	RSA (1024 Bits)

Figure 11-16. Digital certificate

A certificate provides critical information about the certificate, its owner, and the issuing authority. The essential components of information provided on the certificate is as follows:

Version
: The version number of the certificate.

Serial number
: A unique number that identifies the certificate.

Signature algorithm
: The algorithm used to create the signature.

Valid from
: The date and time of the certificate's issue.

Valid to
The date and time of the certificate's expiration.

Public key
The public key that corresponds to the private key.

Enhanced key usage
The purpose for which the key is issued.

CRL distribution point
The URL of the web site that can provide information about the Certificate Revocation List (CRL). CRL is discussed later in this section.

Thumbprint algorithm
The algorithm used to create the unique value of the certificate.

Thumbprint
The unique value that identifies the certificate. This can be checked with the issuer of the certificate.

> Make sure that you know what information is provided on a digital certificate, as shown in Figure 11-16. This is a common Security+ exam question. You must also be able to single out any piece of information that the certificate *does not* provide.

Certificate Policies (CPs). CP is a set of rules that defines how the CA will issue the certificates. Certificate Policies are defined in the X.509v3 standard as a "named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements."

Certificate Practice Statements (CPSs). A CPS is a document written in plain text that describes how the CA plans to manage the certificates that it issues. Organizations that want to subscribe to a third-party CA usually ask for the CPS document from the organization running the CA. These applications may include the following:

- Providing digital signatures for email (or use of S/MIME).
- Verification of the identity of a web site.
- Encryption of data.
- Further issuance of certificates (delegation of control to subordinate CAs).

Certificate policies may be marked as critical or noncritical, in order to limit the liability of the CA. Each CP is a plain-text document and sustained a unique object identifier.

Trust models

PKI can be implemented in one of the following trust models:

- Single CA model
- Hierarchical model
- Web of trust model

Single CA model. In a Single CA model, there is only one CA in the entire PKI. Anyone who needs to use the CA is given the CA's public key. Another CA, known as the *Registration Authority (RA)*, is used for identification and verification of the digital certificates' subscriber. The RA is responsible for setting up the necessary trust between the CA and the end user.

Hierarchical model. The Hierarchical model is comprised of a *root* CA, *subordinate* CAs, *leaf* CAs, and end users. The root CA, also known as the *enterprise* CA, issues a self-signed certificate to itself and makes it available to all users including the subordinate CAs and leaf CAs. The root CA is followed in the hierarchy by subordinate CAs, which are also known as *intermediate* CAs. Intermediate CAs issue certificates to leaf CAs that are next to them in the hierarchy. Finally, the leaf CAs issue certificates to end users. Figure 11-17 shows a hierarchical CA trust model.

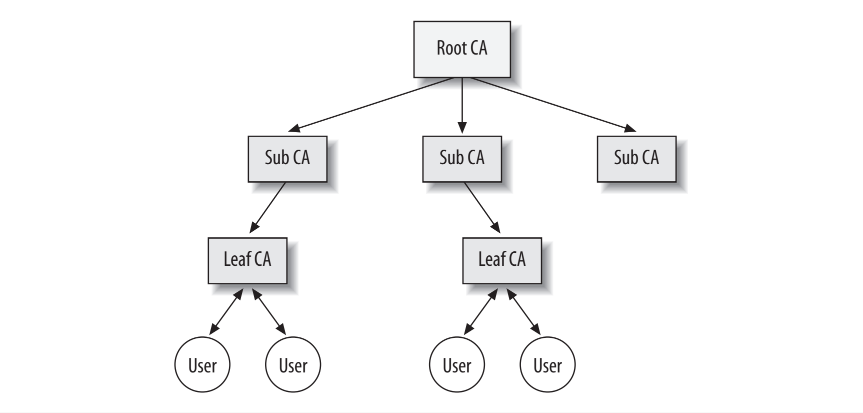


Figure 11-17. Hierarchical CA trust model

Hierarchical CA trust models are suitable for very large-scale organizations where thousands of end users require digital certificates. Key management in such a model is easy due to the fact that it can be decentralized with a number of administrators delegated the duty of CAs at various levels.

Web of trust model. In the web of trust CA model, all CAs sign the certificates of each other. The validation of certificates and keys is based on the trust the participating parties have on each other. PGP, which is used for email encryption, is a nice example of a web of trust model.

PKI standards and protocols

PKI standards are defined by RSA Security in documents known as *Public Key Cryptography Standards (PKCS)*. These standards are used as the basis for designing and implementing PKI. As of this writing, there are about 15 standards named from PKCS#1 to PKCS#15. Most notable of these are PKCS#1, #3, and #5. PKCS#1 defines the usage of RSA Cryptography standards. PKCS#3 is based on the Diffie-Hellman key exchange standard, and PKCS#5 is a password-based cryptography standard.

Key management and certificate lifecycles

There are a number of tasks associated with the creation and management of certificates and keys. The tasks related to the entire lifecycle of keys include storage, distribution, revocation, suspension, expiration, and renewal of certificates, are jointly known as *key management*. The administrators managing the CAs are responsible for key management processes.

Management of keys can be accomplished in a *centralized* or in a *decentralized* manner. In a centralized method, all certificates and keys are stored in a centralized location and managed from a single point of administration. In large organizations, where the number of users requiring certificates and keys is very large, the management of keys is a daunting task. In such situations, the key management tasks can be decentralized. For example, if an organization has over 10,000 employees, it will not be possible to manage keys from a single location. The organization can decentralize the key management functions based on the locations of the organization or on different units of the organization.

Storage. Storage of certificate keys is considered one of the most critical aspects of maintaining a PKI. Depending on how the PKI is implemented and administered, keys can be stored in hardware devices such as smart cards, or they can be stored on network servers. There are two main methods for storing keys, as follows:

Hardware key storage

Private keys can be stored on hardware devices such as smart cards, PCMCIA cards, and other hardware devices. These devices are commonly known as *hardware storage modules (HSM)*. Limitations of hardware storage include the chances of key theft and ageing after a certain time has passed. Smart cards are considered to be the best method of hardware key storage due to their reliability, but they are expensive.

Software key storage

Software storage of private keys is not considered a secure storage method compared to hardware storage. Some network operating systems, such as Microsoft's Windows Server 2003, can be used to store private keys in the Active Directory database. This allows administrators to set filesystem permissions to restrict access to keys. But, at the same time, administrators have to regularly monitor a variety of network activities to prevent misuse or compromise of the keys.

Escrow. Escrow is used for the storage of keys in order to make them more secure. In this arrangement, the private keys are stored with two different companies, each one holding only a part of the keys. This arrangement falls in line with separation of duties because no single company can misuse the keys to decrypt messages or compromise the private keys in any way. Key escrow also enables government agencies to obtain and decrypt encrypted messages when they suspect any criminal activity that is against national security.

Expiration. When a CA issues a certificate, it assigns its validity dates. These dates appear as "Valid from" and "Valid to" on the certificate. The certificate and the key pairs are valid only between these dates. The CA has the authority to verify the certificate during this period of time. When the certificate nears the expiry date, it should either be renewed or destroyed.

Revocation. Sometimes it becomes necessary to revoke the certificate of an individual or an organization. Circumstances that may lead to this include the following:

- The private key of an individual has been compromised.
- The individual leaves the organization.
- The organization has moved to a new location.
- The organization has changed the ISP.

When a certificate is revoked, the information is sent to the CA and the CA authenticates the request and advertises the revoked certificate in the Certificate Revocation List (CRL). The administrator of CA can also manually revoke the certificate of a user without receiving or authenticating any request from the user.

The status of certificates can be checked with CAs in one of the two following methods:

Certificate Revocation List (CRL)

A CRL is maintained by the CA to keep a record of all revoked and suspended certificates. When a certificate is revoked, information in the CRL is updated. There are two main forms of CRLs: *Simple* and *Delta*. A Simple CRL contains the list of all revoked certificates, the date and time when the CRL was last published, and the next date and time when the next CRL will be published. Delta CRLs are used in large organizations where the revocation of certificates occurs in large numbers, and the size of the Simple CRL file becomes a limitation. When Delta CRLs are used, a base CRL is sent to all parties to initiate their copies of CRLs. Once this is done, further updates are periodically sent to these parties as Delta CRLs, which contain only the new and updated information.

Online Certificate Status Protocol (OSCP)

OSCP is a modified method of checking the status of revoked certificates. OSCP eliminates the need to transfer large CRL files when a party needs to check the status of revoked certificates. When the CRL receives a status request for a particular certificate over HTTP protocol, the CA responds only with the status of that particular certificate. The status information contains the status of the certificate (good, revoked, or unknown), the last update on the status, the next update of the status, and the time when the status response was sent to the requesting party. The main limitation of OSCP is that it can return the status of only a single certificate about which information is requested.

Suspension. A certificate and its associated keys are *suspended* when the owner will not be using it for a certain period of time. Suspension of keys is helpful in protecting the keys from being misused. The status of a suspended certificate or key is shown as *Certification Hold* in the CRL. A suspended key should not be confused with a revoked key.

Recovery. As noted earlier in this section, private keys are stored in safe places. If a user forgets his private key, it becomes necessary to recover his key from storage. In large organizations that are heavily dependent on secure communications using a PKI, there is usually a special server, called the *key recovery server*, that is used for the sole purpose of backing up and recovering private keys. An administrator is designated as the *key recovery agent*. In some key recovery configurations, two key recovery agents are required for the process, for added security. Key recovery servers and CAs require some basic information, known as *Key Recovery Information (KRI)*, before a private key is recovered. This information includes the name of the key owner, the time when the key was created, and the name of the issuing server. Once the recovery server verifies this information, the key recovery process begins.

When the key recovery process is broken up into multiple key recovery agents, the process is known as *M-of-N Control*. The idea behind having multiple recovery agents is to ensure that the key is not compromised during the recovery process. In M-of-N control, *N* is an integer greater than 1 and *M* is less than or equal to *N*. For example, if we have three designated key recovery agents (N), at least two of them must be present (M) to recover the key.

Note the basic concept behind M-of-N Control, its purpose, and how it works for recovery of keys.

Renewal. When a key expires or is near its expiration date, it has to be renewed with the CA. One method is to request a key renewal with the same CA using the old key pair. The CA issues a new key based on the trust and good standing of the key owner. Another method is known as *key update*. In this method, the CA generates a new key pair by modifying the old keys.

When the keys of the CA expire, it also needs to renew its own keys. The key renewal process holds true for the CA also. In most situations, the CA renews its keys using its old keys. Since the CA signs its own keys, there has to be a method to update the subordinate CAs and clients about this information. The process involves the following steps:

1. The CA creates a self-signed certificate and signs the new public key using the old private key that is due to expire.
2. The CA then signs the old public keys with the new private key.
3. Finally, the new public key is signed with the new private key. This key is used when the old private key expires.

This changeover from old keys to new keys at the CA level is transparent to the clients. It is important to remember that the CA signs its own certificates and renews its own keys.

Destruction. When a key pair is no longer needed, the administrators should destroy all records of the key pair so that the key pair is not misused to generate fake certificates. A common method of key destruction is to *deregister* the key pair with the CA. When a key pair is deregistered, the association between the CA, the key pair, and the owner of the key is broken.

Key usage. In most of the PKI-based secure networking environments, a *single key pair* is used for different functions. A PKI is used for managing communication between servers and clients in VPNs, digital signatures, access control, secure Internet access, and secure email. There may be situations where administrators may need to use *dual key pairs*. This situation arises when there is a need to back up private keys, but at the same time, the fear of forged digital signatures exists. For example, a backup operator may decide to misuse the private key of the chief of the company for illegal purposes. Many PKI implementations support the use of dual key pairs to protect keys against misuse. In these situations, one key pair is used for encryption and authentication, while the second key pair is used for digital signatures. Each key pair is stored in a different location.

Operational and Organizational Security

Operational and organizational security covers a variety of topics such as setting security policies for the entire organization, user training and awareness, risk assessment, physical security of the equipment, privilege management, and implementing a backup and recovery plan. The sole purpose of implementing organizational and operational security is to ensure a safe and secure working environment where users know what is expected from them, and management has the guidelines to respond to unexpected situations in order to maintain business continuity. The sections that follow cover the concepts of some of the main areas of organizational and operational security.

Physical Security

Physical security involves keeping the network equipment, computer hardware, and software secure from unauthorized access. This includes having appropriate access control systems in place, training the users to protect them from social engineering, and maintaining a perfect operating environment for the equipment. Each component of the business network is vulnerable to different types of external and internal threats. It is important that physical security be given priority while designing and implementing security policies.

The following sections explain how physical security can be ensured by taking care of access control, implementing physical barriers, and controlling environmental factors.

Access control

Access control is used to grant only authorized personnel of the organization access to necessary physical network equipment. For example, a server room may be locked for ordinary users and may be accessible only to those administrators who need to manage servers. Creating physical barriers for unauthorized personnel is one way to control access to critical network equipment, which includes server hardware and network hardware such as firewalls, routers, and switches.

Access control is implemented using physical barriers and biometrics, as summarized in the following paragraphs:

Physical barriers

Most organizations keep the critical servers and network equipment in a locked room, and unauthorized access is denied. Server rooms should be locked and equipped with alarm systems. Logbooks should be maintained for entries to the secure room. All equipment should be locked down with strong passwords. If some outsiders need to work inside secure rooms, an employee of the organization must remain with them all the time.

Biometrics

Authenticating users with biometric methods is considered more secure than other techniques, such as using passwords. Biometric devices use the physical characteristics of a person—for example, fingerprints, facial attributes, or voice patterns. Biometric equipment used for authentication is an expensive alternative but allows for tighter authentication and access control.

Social engineering

Social engineering is acquiring personal information or confidential information, or information about an organization by taking an individual into confidence. The so-called social engineer generally tricks the victim over the telephone or on the Internet to reveal sensitive information about the organization. Unfortunately, no technical configuration of systems or networks can protect an organization from social engineering. There is no firewall that can stop attacks resulting from social engineering. The best protection against this is to train users about the security policies of the organization.

Environment

Preventing unauthorized access to critical network equipment is meaningless if the environmental factors are ignored. The environment surrounding the network equipment includes temperature, humidity, electrical interference, and airflow, among other factors. Equipment should be operated within acceptable limits of temperature and humidity. Server rooms especially should be equipped with temperature and humidity control systems. An increase in temperature inside a computer leads to a defect known as *chip creep* or *socket creep*. It makes computer chips loose in sockets. The following are some of the measures to protect against environmental factors:

- Temperatures should be kept within limits. Alarms should be installed to monitor temperatures and should sound alerts, if required.
- Humidifiers or dehumidifiers, as required, should be installed to control humidity levels.
- Hardware technicians should wear ESD wristbands to prevent electrostatic discharge.
- Arrangements should be made to maintain good air quality inside server rooms.
- Servers and other network equipment should be located properly in racks, well above the ground level. Most modern server rooms are built on raised floors.

- If required, an STP cable should be used to protect the equipment from electromagnetic interference (EMI) and radio frequency interference (RFI).
- Fire suppression equipment should be used to prevent damage from accidental fire breakouts. Remember that water sprinklers are not recommended for server rooms. Fire extinguishers used for server rooms are known as *clean agents* that put out the fire but do not damage equipment.

Disaster Recovery

Disasters can come at any time and in any form. It may be a fire, a flood, or a terrorist attack, or it may even take some other unknown form. A disaster recovery plan should take into account all possible kinds of internal and external threats. It is important to make necessary plans to protect the critical data from any such events in order to let the organization recover in a minimum amount of time and resume its business as soon as possible.

Data backup methods, secure recovery of data, and a well-designed and documented disaster recovery and business continuity plan should be in place. The disaster recovery plan should not wait for a real disaster to occur.

Backups

Data backup is one of the fundamental elements of a disaster recovery plan. Backed-up data is copied to another media such as magnetic tapes or compact disks (CDs or DVDs), which are safely and securely stored at an offsite location. The administrators must decide what data is to be backed up and what should be the frequency, depending on the volume of the backup data and the requirements of an organization. Commonly used backup methods include the following:

Full backup

This method backs up all the data in a single backup job. The backed up data includes systems files, applications, and all user data on a computer. Full backup changes the *archive bit* on files to indicate that it has been backed up. It takes longer to complete the backup process, but the data can be restored faster, as only a single backup set is required.

Incremental backup

This method backs up all the data that has changed after the last full or incremental backup was taken. It uses the archive bits and changes them after the backup process is complete. It takes the least amount of time to complete the backup process but is the slowest method when data needs to be restored. The last full backup tape and all incremental tapes after the full backup are required to completely restore data.

Differential backup

This method backs up all the data that has changed after the last full backup. It does not change the archive bits and thus, does not disturb any scheduled incremental backups. Since it does not use the archive bits, if a differential backup is taken more than once after a full backup, the differential backup tapes will contain duplicate data. When restoring data, only the last full backup tape and the differential backup tape are required. It is faster to restore than the incremental backup.

Copy backup

This method copies all the data on the system but unlike the full backup, does not change the archive bit.

Most organizations implement a mix of one or more backup types to create weekly, monthly and yearly backup plans. Depending on the requirements of an organization and the amount of data to be backed up, different organizations may adopt different backup schemes. The combination of full backup on weekends and incremental backups on weekdays is one of the commonly used methods.

> Make sure that you understand different backup types, the function of the archive bit, and the pros and cons of each backup type. The difference between copy backup and full backup is commonly asked in the Security+ exam because both make a full backup of the system. Remember that a copy backup does not use or change the archive bit while the full backup uses and changes the archive bit. Similarly, the difference between incremental and differential backup types is another common exam question.

Tape rotation. Magnetic tapes are the most popular media used for backups. In order to reduce the cost involved in the purchase of new tapes for every back up, most organizations reuse the tapes after a certain amount of time and according to a preset tape rotation plan. A commonly used tape rotation plan is known as *Grandfather-Father-Son (GFS)*. Backup tapes are categorized into daily, weekly, and monthly sets. With this rotation scheme, a full backup is taken every week, and differential or incremental backups are taken every day. The daily and weekly tapes are stored offsite at the end of the week and new tapes are used for the next week. Additionally, another full backup is taken at the end of the month. When the month changes, the tapes used for the first week in the previous month are reused, followed by the tapes used in the second week, and so on. In the GFS rotation scheme, the daily tape set is known as *son*, the weekly tape set is known as *father*, and the monthly full backup tape set is known as *grandfather*. It is important to note that the grandfather tape set is not reused as it contains all files changed during a particular month.

Offsite storage. It is important that the tapes be stored at a safe and secure offsite location. Offsite storage helps protect critical data stored on tapes in the event of a disaster. If backup tapes are not stored offsite, they are vulnerable to destruction along with other equipment when a disaster strikes. Organizations may store tapes at another location or can engage a third-party professional organization for the purpose. It is important that administrators make an assessment that the safety and security requirements are fulfilled if offsite storage is managed by a third party

Secure recovery

The secure recovery of data is a part of the backup process. Data may need to be recovered from backup tapes, even when a small incident such as accidental deletion of files happens, or when some virus application corrupts files. The damage may occur on a single system or on multiple systems across the network. Administrators should also not forget that the organization might be subject to outside malicious activity by professional hackers. The worst-case scenario is a disaster that requires administrators to carefully make a disaster recovery plan and define procedures for secure and quick restoration of data.

The safety of backup tapes is of prime concern. This includes protecting the tapes from physical damage and theft. Aside from this, procedures and guidelines must be in place to describe how the data can be restored with minimal delays. Large organizations usually have dedicated backup operators who are proficient in backup and restoration functions. Offsite storage is an excellent way to secure tapes. Large organizations can also have alternate sites, which can be used to resume business in case of a disaster.

Alternate sites. Alternate sites are critical to all such organizations that do not want any delay in restoration of data after a disaster strikes. An alternate site is a temporary facility away from the original location of the organization that enables administrators to restore a working network in a minimum amount of time so that the organization can resume its business. Alternate sites can be classified into the following types:

Hot site

A hot site is equipped with all necessary hardware, software, network devices, and telephone lines. It allows organizations to resume business activities almost immediately. The equipment is fully configured, data is replicated to servers at the site in real-time, and in case of a disaster, the organization can resume business with minimal delays.

Warm site

A warm site normally is equipped with all necessary hardware, software, network devices, and telephone lines. Unlike a hot site, this site is not fully configured and does not store a working copy of data. Hardware and software must be configured, and data must be restored from backup tape sets. It takes administrators a little while before this site can be made functional.

Cold site

A cold site requires the maximum amount of time to be set up and made functional. It contains only partial hardware, software, and network devices that are not configured. This site needs to be built from scratch to make it fully functional.

Disaster recovery plan

A disaster recovery plan is a written document that defines how the organization will recover from a disaster and how the business can be restored with minimum delays. This document describes how the risks of a disaster are to be evaluated, and offers data backup and restoration methods, alternative sites, and individual skills of administrators and users that can be helpful in case of a disaster. It also notes what estimated cost is involved in resuming business after the disaster.

Business continuity plan

A business continuity plan is a written document that defines the major threats that a company may face, including disasters, and sets up policies and procedures to ensure that the business resumes with minimum delays after an interruption due to any unforeseen circumstances. This plan is developed after a careful assessment of risks and the impact of each type of disaster and event. Essential elements of a business continuity plan are as follows:

Disaster recovery plan
: This plan defines the recovery procedures for after a disaster strikes.

Business recovery plan
: This plan describes the procedures to resume business functions at an alternate site after a disaster.

Business resumption plan
: This plan describes the procedures to resume functions of critical systems in order to go back to business as normal.

Contingency plan
: This plan describes the procedures to resume business after a disaster strikes or when additional unforeseen events take place during the recovery process.

Utilities. Utilities essential for network services include electricity, Uninterruptible Power Supplies (UPS), and power generators. Although system and network administrators might have taken every step to provide reliable and efficient system services, they are still dependent on these utilities to keep the systems working. UPS systems are useful when there is a power outage, but they are good only for a small amount of time. If the power outage remains for longer periods, power generators may be required to supply essential electricity to the network. It is essential that the organizations select reliable third-party vendors to install and maintain such utilities as UPS systems and power generators.

High availability and fault tolerance. High availability refers to maximum uptime as well as efficiency of the systems and the network. It can be achieved only if there are adequate arrangements in place to maintain network services in case of a system failure. *Network load balancing* is a common method used to share the load of requests for a particular service such as a web server or a DNS server. *Server clustering* is another method to ensure high availability. As far as a single server is concerned, most of the system crashes are caused by failure of hard disks. Server hardware addresses the problem of hard disk failures by implementing a *Redundant Array of Inexpensive Disks (RAID)*, also known as *fault-tolerant* disks. Servers equipped with RAID systems normally allow hot swapping of hard disks so that the server does not need to be taken offline when a failed disk is to be replaced. The following types of fault-tolerant RAID systems are commonly used:

RAID 1 (Disk Mirroring)
: This RAID system uses exactly two disks, preferably of the same size and make. The data written to one of the disks is copied to the second disk. In this system, the disk utilization is only 50 percent.

RAID 5 (Disk Striping with Parity)

This RAID system uses 3 to 32 disks, preferably of the same size and make. The data is evenly written to all hard disks simultaneously. The failure of a single disk does not bring down the server.

RAID systems can be either hardware- or software-based. Hardware-based systems are more expensive but more efficient than software RAID systems. Software RAID systems are implemented using the network operating system. They have limited functionality and are used only where the cost of implementing a RAID system is to be kept to a minimum.

Security Policies and Procedures

Security policies and procedures are sets of written documents that describe how a safe and secure computing environment is to be created and maintained inside an organization. The following sections explain some of the security policies and procedures covered in the Security+ exam.

Acceptable use policy. An acceptable use policy describes the guidelines for users so that they use the computers and the technology appropriately. It explains what activities are permitted and what are prohibited. The following are some of the guidelines included in an acceptable use policy:

- Users should not indulge in activities that might damage the image of the company.
- Users should not participate in activities that might consume network resources beyond limits.
- Users must follow the rules that restrict visits to web sites and email programs.
- Users should not print any confidential documents and/or take them out of the organization.
- Users should not transmit classified or confidential information over the Internet.

Some organizations enforce the acceptable use policies by having the employees sign an agreement when they are hired.

Due care policy. A due care policy describes how the employees should handle computer hardware and software in order to protect it from damage. Since computer equipment and software are expensive, employees should be given guidelines on how to properly work on them. Efforts should also be made to protect the integrity of data by performing regular virus scans and detection of malicious software. A simple example of due care in protecting operating systems is to use the Shut Down feature instead of directly turning off power. Users should follow manufacturers' guidelines when using any type of equipment. Administrators are expected to keep OS/NOS and other applications updated with the latest service packs, hotfixes, and security patches.

Privacy policy. *Privacy* is one of the major issues concerning almost every employee of the organization. Aside from the privacy of an individual, the privacy of a particular department and of the organization is also important. Employees should be trained on how to maintain privacy while using modern technologies. They should be instructed to refrain from such activities as disclosing personal or organizational information over the Internet, through emails, or in chatting. A privacy policy also usually states that the organization has the right to inspect personal data stored on company computers. This data can be inspected anytime by the appropriate authorities and can be done by performing regular audits on users' personal folders, emails, and other software that they might be using. Data critical to the operation of an organization is also considered private and confidential. Administrators must make sure that all efforts are made to protect this confidentiality of data.

Separation of duties policy. The separation of duties policy ensures that critical tasks are not assigned to a single person. These tasks should usually be divided among two or more persons so that no single person has control over the task or procedure from beginning to end. Employees should not be allowed to monopolize any task that is critical to a department's function, or to an organization's function. This also ensures that no single employee has complete information about a particular project, which results in more security. If a single person has all the information related to a project, the chances of leakage of confidential information increase. Senior employees, such as supervisors and managers, should break up duties among their subordinates and should be responsible for coordination among them. Another positive side of separation of duties is that individual employees can concentrate on their specific jobs and become experts in whatever task they are performing.

Need-to-know policy. The need-to-know policy dictates that employees should be given only as much information as they need to perform their job functions. Giving excessive information to employees might result in inappropriate handling of information, or even its leakage to third parties. If any employee needs more information than what he is authorized to obtain, he should submit a written request to his supervisor, who in turn should forward it to the departmental manager. This ensures that permission to use classified information is in the control of supervisors and managers. Organizations usually protect confidential information by having employees sign a non-disclosure agreement at the time of hiring.

Password management policy. A password management policy describes how employees should manage their passwords. A password is the employee's key to gaining access to the organization's resources stored on computers. Without having a sound password policy, employees may make their passwords weak or disclose their passwords to unauthorized people. Professional hackers may exploit an organization's confidential resources by guessing insecure passwords. Password policies include the following essential elements:

- The use of blank passwords should not be allowed for any employee.
- Passwords should have at least eight characters.

- A password should be made up of a combination of upper- and lowercase letters, special characters, and numbers.
- Employees should be forced to change their passwords regularly.
- Employees should not be allowed to reuse their old passwords for a certain amount of time.
- Administrators should use normal user accounts when not performing any administrative tasks. Only designated IT employees should have administrative privileges.

Passwords should be longer and stronger to prevent brute force or *dictionary attacks*. Password policies can be enforced through the NOS. For example, in Windows Server 2003, administrators can enforce a *group policy* (Group Policies are mainly used to enforce enterprise wide policies) to enforce a password policy throughout the network.

Service Level Agreements (SLA). An SLA is an agreement between an organization and a third party or a vendor providing critical services to the organization. SLAs usually describe the expected level of performance and confidentiality of the organization. For example, an organization might not be able to afford a full-time IT staff to maintain its computer network. It may hire another company to install, upgrade, administer, and maintain the IT setup. The SLA can also be used inside an organization, describing what the company can expect from its IT employees and what procedures they should follow to perform their duties.

SLAs often include information on the maximum allowed downtime of the computer systems and the network. In other terms, SLAs can describe the expected uptime. This information is usually given as *nines*. This ensures that the IT staff or a third-party IT maintenance company will be responsible to provide expected system and network uptime. Table 11-4 shows how expected uptime and downtime are calculated.

Table 11-4. Calculating expected uptime and downtime

Availability percentage	Maximum downtime per year
99.999 percent	5.3 minutes
99.99 percent	53 minutes
99.9 percent	8.7 hours
99 percent	87 hours

Disposal and destruction policy. A safe disposal and destruction policy for data should be in place to protect the organization from undesired leakage of confidential information by means of old computers that are either thrown away or sold to third parties. As time passes, the computer and network equipment become obsolete and are replaced by newer models with added features and functions. It is common for organizations to dispose of old and unused equipment, either by destroying it or by selling it to others. But before older servers and desktops are disposed of, it is important to make them free of any confidential data that may be stored on their hard disks. Data stored on magnetic tapes and floppy disks should be destroyed by using a *degausser* (also called *bulk demagnetizer*). Hard disks should be formatted to clear them of any data.

Similarly, documents printed on paper should not be put into recycle boxes without first shredding them. Printed documents might contain confidential information that could be used by an individual or a third party. As noted earlier, someone may go dumpster diving in order to obtain confidential information about the organization.

Human resources policies. The human resources (HR) department works closely with all other departments of an organization, particularly with the IT department, when most of the employees are working on computers. An HR policy should be in place to enforce rules on what should be done about employees' desktops and user accounts when people are hired, terminated, or promoted, or when they voluntarily resign. In some situations, people go on a long leave of absence, or sometimes an employee is involved in criminal activities and is being investigated. The HR policy plays an important role in ensuring the safety and security of the employees as well as the security of the organization's computer network. The HR staff is supposed to contact the IT staff as soon as any of the noted incidents take place. If an employee is hired, the IT staff is contacted to create a user account for him. When an employee resigns or is terminated, the IT staff is again requested to disable or delete his account. Similarly, when an employee is promoted or changes duties within the organization, his need to access computer resources also changes and he may need higher privileges. The HR department is supposed to enforce policies that should serve as guidelines on how the interaction between the HR department and the IT department will take place.

Code of ethics. Another term closely related to computer security is the code of ethics. The code of ethics describes how the employee is expected to work in the organization, and what principles are in place regarding racism, sexism, and other fair business practices. A code of ethics dictates that the employee is expected to abide by the law and by other rules and regulations of the organization. Employees may be required to sign a document that enforces the code of ethics in the organization—if an employee refuses to do so, she could face termination or dismissal.

Incident response policy

The incident response policy describes how employees will respond to unexpected incidents involving personal safety, security, and other incidents involving the safety and security of the resources of the organization. The incident response policy describes what actions will be taken and who will take those actions in case of an untoward incident. This ensures that the right persons are selected to perform particular tasks, such as finding out the reasons behind the incident or preparing a report. The incident response policy has the following common elements:

- How are incidents to be handled in an appropriate manner without causing a panic?
- Who will be in charge of investigating and analyzing the reasons behind the incident?

- Who will be in charge of finding an immediate and acceptable solution to the problem caused by the incident?
- What other documents can be referred to in order to help resolve the problem?

Large organizations usually have a special *incident response team*, which handles all aspects of the incident from initial collection of evidence to preparation of the final report.

Privilege Management

Privilege Management involves administrative tasks that control access to the shared network resources. Access control allows administrators to assign access permissions for internal and external users. In most cases, the access to resources is based on job functions of users or groups of users. In this section, we will summarize some basic concepts behind privilege management to ensure security of the organizational data and other network resources.

User/Group/Role management

Every user in a computer network is assigned a user account. The user account can further be a member of a group of users. Administrators are responsible for creating and managing user accounts and groups, and assigning them permissions on the basis of their roles (job functions) in the organization. The administrator himself is assigned a user account with higher privileges. Access to shared resources is restricted by means of permissions. When a user leaves an organization or is terminated, his user account is disabled. Users are given permissions to resources based on the rule of least privilege.

Single sign-on

Single sign-on enables users to log on and be authenticated to the corporate network once, and to access resources in all parts of the network where he is assigned appropriate permissions. Network operating systems (such as Windows Server 2003) store and maintain user accounts in multiple Active Directory database servers known as *domain controllers*. When a change is made to a user account or to the permissions assigned to it, they are replicated to all domain controllers in the network.

Centralized verses decentralized

Network servers can be located either at a centralized location or they can be distributed at multiple locations, depending on the requirements of the organization. For a small or medium-sized organization, all servers can be located at a centralized location in secure server rooms. Access to these rooms can be restricted to only authorized administrators. In large organizations with multiple geographical locations, servers can be spread across locations to simplify administration and maintenance tasks. The IT staff at each location is responsible for configuring the security of these servers. Decentralization has an added benefit of fault tolerance. A particular server at one location can have its mirror at another location so that if one fails, the other is available to service user requests. The advantage of centralizing servers is the ease of administration and tighter physical security. But, at the same time, a centralized location is not considered optimal from disaster recovery and business continuity viewpoints.

Auditing

Auditing, as discussed in the beginning of this chapter, is the process of tracking actions of users and services on a particular server, or on the entire network. Auditing helps administrators troubleshoot, as well as keep an eye on user actions. It helps with regular monitoring of network activities in order to take corrective action if something goes wrong. Auditing requires significant planning and configurations on servers and network equipment. The events that are tracked are written to log files that can be analyzed at any time. Auditing also helps investigate the criminal activities of a malicious user. Audit logs are used as evidence against the person involved in criminal activities. For example, if a user is trying to log on to the network when he is not supposed to, or is trying to access resources he is not permitted to, the audit logs can reveal this information. If someone else is trying to log on to the network using another account, the audit logs can be helpful to track the source of this illegal attempt.

Mandatory Access Control/ Discretionary Access Control/Role-based Access Control (MAC/DAC/RBAC)

MAC, DAC, and RBAC are different types of mechanisms used to control and restrict access to system and network resources. For more details on access control methods, refer to the section "General Security Concepts" covered earlier in this chapter.

Computer Forensics

Computer forensics is the application of computer expertise and skills to establish factual information about an incident for a judicial review. It involves activities such as collecting and preserving evidence, examining evidence, and transferring it using electronic media. Presentation of evidence is also considered an aspect of this. Computer forensics is done using a method that adheres to standards of evidence that are acceptable in a court of law. It is important that these standards are followed to collect and preserve evidence so that it is not damaged in a way that lawyers may argue its validity and the judges may consider it inadmissible.

It is important that users are made aware of the consequences of incidents that may lead to criminal investigations. If there is some incident that is considered a criminal activity, it should be reported to the incident response team. This team follows the incident response policy of the organization in order to deal with the incident. Each person on the incident response team has a specific role. Criminal investigations consist of people performing the following activities:

The first responder
: Identifies and protects the crime scene. He also preserves any evidence that may be volatile (information that may change over a period of time).

The investigator

Establishes a chain of command/chain of custody and conducts a search of the crime scene. He is responsible for maintaining the integrity of the evidence.

The crime scene technician

Is responsible for preserving volatile evidence and duplicating computer disks. He shuts down the system for transportation, logs activities, tags the system, packages the system, and makes arrangements for transportation. He is also responsible for processing the collected evidence, such as performing analysis of log files or screen captures.

> Remember the four essential components of computer forensics: collection of evidence, examination, preservation, and presentation. Every component has associated documentation created when performing these activities.

Chain of custody

A chain of custody describes how the evidence is transferred from the crime scene to the court of law. Evidence has to be handled using standard procedures, and proper documentation is created at each step. The chain of custody specifies the personnel who will be responsible for maintaining and preserving the evidence right from the scene crime. Each piece of evidence is kept inside a sealed bag, no matter how small or big it is. Sealed bags are tagged and signed. The chain of custody is detailed in the evidence log and specifies the persons who had possessed the evidence or worked on it. Each time the evidence is transferred from one person or another, or from one place to another, a log entry is written to the documentation.

Preservation of evidence

Preservation of evidence refers to the evidence integrity. In computer forensics, preservation of pieces of data and equipment from damage is important so that the original evidence is not damaged. The following are important aspects regarding preservation of evidence:

- Steps should be taken to preserve the volatile data first.
- Photographs of screens should be taken to capture the data displayed on monitors at the time of the incident.
- Images of hard disks should be done using accepted imaging tools.
- The system should be shut down using normal shutdown procedures.
- Photographs of the existing system setup should be taken before moving any piece of hardware.
- Each piece of hardware should be unplugged and tagged.
- Appropriate safety procedures should be followed when handling hardware. These include using antistatic wrist straps with proper grounding.

- Circuit boards, hard disks, and other smaller pieces of hardware should be placed inside antistatic plastic bags.
- All equipment should be kept away from strong electromagnetic fields, radio frequencies, and heat sources.

Aside from the steps given here, all steps taken to preserve evidence should be documented in appropriate logs.

Collection of evidence

Collection of evidence is the process of identifying, locating, processing, and making appropriate documentation. This starts by securing the scene of the crime (for example, a server room) and preventing unauthorized personnel from entering the area and accessing the evidence. Once the evidence is identified and secured, the investigation team can start the process of examining the evidence and take steps for collection. Collection of evidence from servers can be done in a variety of ways, such as a review of audit log files and screen displays, and a recovery of data files using acceptable software utilities such as SafeBack, EnCase, and ProDiscover. These software utilities are recognized by investigating agencies and are capable of performing several checks on recovered data to ensure its integrity. The collected data must then be preserved in order to prevent it from damage. Once again, the volatile data must be collected and preserved before collecting and preserving any other types of evidence. Steps taken in collection of evidence should be recorded in appropriate logs.

Education and Training

Educating and training users is one of the important aspects of creating a safe and secure working environment. Organizations may go for in-house training or can hire a professional training company to provide training to users. This is an ongoing process, especially when new equipment is installed or a new application is implemented. This training applies to employees of all departments of the organization.

Communication

Users must know the different methods available to communicate to their peers, their supervisors, management, and employees in other departments. Telephone and email are considered the most common and effective means of communication. For employees at remote locations, corporate intranets enable employees to send internal memos and emails through the intranet. Some organizations allow Instant Messaging (IM) inside the corporate network to enable employees to talk to each other or to allow employees in a specific department to collaborate on an ongoing project. Organizations can use different security mechanisms to protect internal communications from eavesdroppers. For example, email can be encrypted or digitally signed so that only the intended recipient can read the message.

User awareness

In any organization, small or large, employees are expected to follow the rules and regulations. Computer users, in particular, should be aware of the issues related to good work ethics and rules governing their work inside and outside the organization. It is necessary that users are made aware of rules, regulations, and security issues in order to create and maintain a secure working environment. Administrators must take steps to make the users aware of their responsibilities and of what is expected of them. This can be done by keeping users informed about existing rules, policies, and any periodic changes.

Education

User education is the primary means of enhancing skills and expertise in users' respective fields. Where security is concerned, educating users about security issues and methods to tackle them is important. Users should be made aware and educated on how to handle minor as well as major issues concerning security of equipment and data resources.

Online resources

There are a number of online resources available to educate and train users. These resources are also helpful in keeping users informed about any new developments in their field. For example, most of the software vendors post security patches, updates, hotfixes, and service packs on their web sites, which are free for download. Similarly, hardware venders post updates on their web sites. Making the users aware of these issues can be very helpful in keeping them informed and educated. In some cases, free education and training resources are made available online by vendors. Aside from this, there are several articles on the Internet that might be helpful in resolving technical and security-related issues. Microsoft's Knowledge Base is just one example of such an online resource.

Risk Identification

Risk Identification is the process of identifying assets, risks, threats, and vulnerabilities in a system. A *risk* is the possibility of incurring some loss due to unexpected situations. It is the possibility of certain loss and does not necessarily mean that loss will occur. For example, a disaster such as a fire or a flood can potentially cause a heavy loss to an organization in terms of lost business and lost clientele. Risks can be caused by internal or external sources. It is necessary that all forms of risks are evaluated and that threats from these risks be identified.

Asset identification

Assets are the physical property and resources that belong to an organization such as servers, desktops, network equipment, printers, scanners, and critical data stored on servers. Even furniture and office supplies are considered to be assets of an organization. The organization needs to take steps to identify all types of assets and make an evaluation. This helps identify the costs involved in replacing a particular asset. Important assets that are critical to the functioning of an organization's business should be identified and tagged. Inventory should be taken and lists should be prepared. This helps decide what assets will be replaced on a priority basis in the event of a disaster. Even employees are the assets of the organization.

Risk assessment

Different types of assets will have different type of risks associated with them. After collecting information about assets, the organization needs to identify and assess the type and severity of risks associated with each type of asset. In order to make an assessment of risk, organizations may get help from insurance companies, police departments, news agencies, or other investigating organizations. The likelihood of the occurrence of a risk within one year is known as *Annual Rate of Occurrence (ARO)*. This is helpful in calculating the dollar amount of loss due to the risk for an asset. The dollar value of this loss is known as *Single Loss Expectancy (SLE)*. Multiplying ARO and SLE gives a value of *Annual Loss Expectancy (ALE)*. Thus, the formula for calculating the loss resulting from a risk is as follows:

$$\text{ALE}=\text{ARO}\times\text{SLE}$$

For example, consider a critical data server that has failed. The organization was running e-commerce services using this server. The ARO for the server is 30 percent and its SLE is $20,000. The ALE for the server would be calculated as follows:

$$\text{ALE}=0.3\times 20{,}000$$

The result is $60,000. Thus, the ALE resulting from the risk associated with the data server will be $60,000.

Threat identification

Identification of threats is usually done after the identification of risks. Identification of risks may lead to identification of possible threats to a system. Organizations must make sure that risk assessment is properly calculated in order to reduce the possibility of threats. Appropriate steps should be taken to avoid potential threats. It is important to identify the threats and decide how a particular threat can be dealt with. For example, if an organization concludes that the risks and cost of assets is to high, it may move the assets to another secure location where the threats can be reduced. Threats commonly include incidents involving vandalism, theft of equipment or data, physical and software intrusions, and other situations varying from one organization to another.

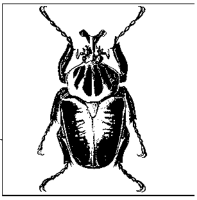
Vulnerabilities

Vulnerability is defined as the weakness of a system. It can lead to exposure of critical and confidential information. Vulnerabilities can lead to internal malicious activities or even outside security attacks. Every software application is vulnerable, if not configured and secured properly. Failing to secure server and desktop hardware, operating systems, and software applications can be fatal for an organization that depends on computers to run its business.

> Removing a known vulnerability is the only way to secure a system and protect it from unexpected damages. It is important to note that the threat of a malicious activity, internally or externally, will exist until the vulnerability is removed. Keeping OS/NOS and application software virus-free and up to date with the latest security patches, hotfixes, and service packs is helpful in reducing vulnerabilities.

Organizations must make sure that proper security policies are implemented and all software applications are scanned for viruses, as well as kept up to date with the latest security updates and service packs.

12



Security+ Exam Prep and Practice

The material in this chapter is designed to help you prepare and practice for the Security+ Exam: SYO-101. The chapter is organized into four sections:

Preparing for the Security+ Exam
: This section provides an overview of the types of questions on the exam. Reviewing this section will help you understand how the actual exam works.

Security+ Exam Suggested Exercises
: This section provides a numbered list of exercises that you can follow to gain experience in the exam's subject areas. Performing the exercises in this section will help ensure you have hands-on experience with all areas of the exam.

Security+ Exam Highlighters Index
: This section compiles the facts within the exam's subject areas that you are most likely to need another look at—in other words, the areas of study that you might have highlighted while reading the Study Guide. Studying the highlights is useful as a final review before the exam.

Security+ Exam Practice Questions
: This section includes a comprehensive set of practice questions to assess your knowledge of the concepts. The questions are similar in format to the exam. After you've reviewed the Study Guide, performed the Suggested Exercises, and studied the Highlighters Index, read the questions and see whether you can answer them correctly.

Before you take the Security+ exam, review the exam overview, perform the suggested exercises, and go through the practice questions provided. Many online sites provide practice tests for the exam. Duplicating the depth and scope of these practice exams in a printed book isn't possible. Visit CompTIA's certification web site for pointers to online practice tests (*http://certification.comptia.org/security*).

Preparing for the Security+ Exam

The Security+ exam is computer-generated. The exam is timed, and an onscreen timer clock displays the amount of time remaining on the exam. Most questions on the exam are multiple-choice. Multiple-choice questions are either:

Multiple-choice, single answer
A radio button allows you to select a single answer only.

Multiple-choice, multiple answer
A checkbox allows you to select multiple answers. Usually the number of correct answers is indicated in the question itself.

CompTIA reserves the right to change the testing techniques at any time. It is recommended that you visit the CompTIA Security+ certification web site regularly to get updates on any changes in the exam format. Individuals with adequate hands-on experience who have reviewed the Study Guide, performed the practice exercises, memorized the essentials, and taken practice tests should do well on this type of exam. Individuals who lack adequate hands-on experience and have not prepared appropriately will find the exam hard to pass.

CompTIA suggests the following tips for taking the exam:

- Read the question slowly and carefully.
- Do not expect to find clues in every question, though they may be present in some.
- Be aware of the distractions/confusions in statements. The first choice is often the best choice.
- Do not attempt to create situations based on a question. Your answer should be based on whatever information is provided.
- If you are retaking the exam, utilize your previous score report to help you focus on areas that need more study or practice.
- If you get stuck, mark and skip the question. You can do it later.

Typically, the test environment will have Previous/Next and Mark For Review options. You can navigate through the test using the Previous/Next buttons. You can click the Mark For Review checkbox to flag a question for later review

Security+ Exam Suggested Exercises

The Security+ exam expects you to have a good understanding of concepts related to computer security. Hands-on experience is recommended and is good to have. You should be well conversant with terminology and should understand the requirements of a secure computing environment. You will need to review the Study Guide and pay close attention to the areas that are new for you until you feel comfortable with them.

This section includes some exercises that you can perform, either on a standalone computer or in a network, to gain some hands-on experience. Since the Security+ exam mainly covers foundation-level knowledge on securing a network from internal and external threats, you are not expected to know how to configure a particular type of hardware or application. But you must know the terms and concepts associated with computer security.

It is recommended that you do not perform any of the suggested exercises at a workstation or server in your organization or on any running computer network. Create a test environment consisting of two computers for completing these exercises. Even if you just want to view security settings in a production environment, make sure a senior administrator accompanies you. In any case, you should follow the security policies of the organization.

Access Control

1. Log on to a Windows XP computer.
2. Open Windows Explorer and locate a shared folder.
3. Open the Properties dialog box of the folder.
4. Check the permissions assigned to the folder.

Authentication

1. Accompany your administrator to the server room.
2. Gather information about different authentication methods used to access servers.
3. Check whether only a username/password combination is used or whether some access tokens are used.
4. Check the authentication protocol used for the network.
5. Check whether desktops and servers require mutual authentication.

Auditing and Logging

1. Log on to a Windows 2000 or Windows 2003 file server.
2. Note the resources on which auditing is enabled.
3. Note the services on which auditing is enabled.
4. Open the Event Viewer to view different types of logs.
5. Read the details on some log entries.

System Scanning

1. Open Internet Explorer on a desktop.
2. Go to *www.nessus.org*.
3. Locate the product information and read the features.
4. Note the operating system that it can scan.
5. Note the vulnerabilities it can detect.

Disabling Non-Essential Services and Protocols

1. Log on to a Windows 2000 or Windows 2003 server.
2. Open the Services console from the Administrative Tools folder.
3. View the status of and the startup type of different services.
4. Check the function of the server.
5. Open the Properties of a service and check its dependencies.
6. Disable service if it is not required on the server.

Social Engineering Attack

1. Inform your administrator or manager that you are going to try a social engineering attack.
2. Call several persons inside the organization.
3. Try to gather some personal information.
4. Check whether these persons trust you to give out confidential company information.
5. Gather as much information as you can.
6. Report the results to your administrator or manager.

Remote Access and VPN

1. Log on to a Windows XP computer.
2. Open the Network and Dialup Connections window from the Control Panel.
3. Select Connect to a Private Network Through the Internet.
4. Configure the dial-up properties to connect to a remote access or VPN server.

Email Security

1. Check what security method is used for messaging servers.
2. Check the security configuration for email clients.
3. Check whether HTML email is allowed.
4. Check how the messaging servers detect email spam.
5. Check how SMTP Relay is configured on the messaging server.
6. Set up secure email with one of your colleagues.
7. Send an encrypted message and see whether the receiver is able to read it.

Wireless Security

1. Gather information from your administrator on wireless protocols used.
2. Check where the Wireless Access Points are placed.
3. Check how SSID is configured on the access point and the clients.
4. Note down the location of wireless clients.

5. Check whether more than one wireless network is present.
6. Check how the wireless network is connected to the wired network.
7. Visit *www.netstumbler.com* and read the features of this wardriving software.
8. Check what wireless cards are supported by this application.

Web Server Security

1. Log on to any Windows 2000 or Windows 2003 server in the presence of your administrator.
2. Open Internet Explorer, type `http://localhost`, and press Enter.
3. If the default web page opens, web services are installed on this server.
4. If this server is not designated as a web server, it is a rogue web server.
5. Remove the Internet Information Services from this server.
6. Repeat the exercise on several other servers.

Web Browser Security

1. Open Internet Explorer on a Windows XP desktop.
2. Open the Internet Options dialog box from the Tools menu.
3. Open the Security properties and click on the Security tab.
4. Check the configured security zone.
5. Check the security settings by clicking the Custom Level button.
6. Click the Privacy tab to view settings for cookies.
7. Move the slider to view settings in high- and low-level settings of privacy.

Demilitarized Zones

1. Ask your administrator about DMZ in the organization.
2. Check whether the DMZ is a separate network segment.
3. Check how firewalls are configured to allow or block traffic inside the DMZ.
4. Gather information about servers placed inside the DMZ.
5. Draw a rough network diagram showing the DMZ.

System Hardening

1. Note the operating system version on some servers.
2. Check which applications are installed on these servers.
3. Visit the web sites of vendors of the operating systems and applications.
4. Gather information about the latest service packs, hotfixes, or updates.
5. Check whether the latest updates are installed for applications and operating systems.

Data Backup

1. Check what type of backup is performed on servers.
2. Check with the administrator about what files are backed up and why.
3. Check how the tapes are rotated.
4. Check whether the tapes are stored in-house or at an offsite location.

Disaster Recover Plan

1. Check whether the organization has a disaster recovery plan.
2. Check how the plan is implemented.
3. Gather information about different components of the plan.

Security+ Exam Highlighters Index

In this section, we've attempted to compile the facts within the exam's subject areas that you are most likely to need another look at—in other words, the areas of study that you might have highlighted while reading the Study Guide. The title of each highlighted element corresponds to the heading title in the Security+ Exam Study Guide. In this way, if you have a question about a highlight, you can refer back to the corresponding section in the Study Guide. For the most part, the entries under a heading are organized as term lists with main points that you need to memorize for the exam.

General Security Concepts

This subsection covers a summary of highlights from the "General Security Concepts" section in the Security+ Exam Study Guide.

Mandatory Access Control (MAC)

- MAC is usually hardcoded into a device and is nondiscretionary.
- MAC is universally applied to all objects.
- Administrators or owners of the object cannot change MAC settings.
- MAC is also known as label-based access control.

Discretionary Access Control (DAC)

- DAC is usually provided by the operating system.
- Administrators or owners of objects implement DAC.
- DAC makes it possible to change the ownership of objects.

Role-based Access Control (RBAC)

- RBAC is used to implement security on objects based on the job functions/roles of users.
- It is highly configurable and offers the most flexibility in implementing access control.

- It provides simplified and centralized administration of shared resources.
- Administrators put users into groups and configure permissions based on job roles.

Authentication methods

- Authentication verifies the identity of a person who wants to access a resource.
- Authentication can be a one-way or a two-way process.
- User credentials can be supplied by username/password combination, biometrics, smart cards, or multifactor methods.

Kerberos

- Kerberos is an authentication protocol used for mutual (two-way) authentication.
- It uses symmetric key cryptography with the help of a third party.
- Kerberos realms leverage a Key Distribution Center (KDC) to issue secure encryption keys and tokens.
- When a user presents his credentials, a Ticket Granting Ticket (TGT) is cached locally on the user's computer.
- The user presents the TGT to the server to obtain a session key, which is timestamped and expires as soon as the user logs off.
- Kerberos helps prevent replay and spoofing attacks.

Challenge Handshake Authentication Protocol (CHAP)

- CHAP is used to verify the authenticity of the client periodically.
- It uses a three-way handshake even after the session has been set up.
- CHAP cannot work with encrypted password databases.
- MS-CHAP, used in Microsoft Windows networks, is considered secure.

Digital certificates

- Digital certificates use digital signatures to bind the identity of a person to a certificate.
- A Public Key Infrastructure (PKI) is used to issue and manage certificates.
- A Certification Authority (CA) issues digital certificates.
- Certificates can be used for authentication of a user, a server, or an organization.
- Information on certificates includes the name of the certificate holder, the issuing authority, the validity dates, and the encryption method used.
- Web servers must use certificates in order to use the Secure Socket Layer (SSL) for secure transactions.

Username/Password

- The combination of username and password is used for supplying the credentials of the user.
- This method is most commonly used by all major operating systems.

- Password policies should enforce the use of secure passwords.
- Password policies require users to use long passwords with a mix of characters, to change passwords regularly, and to not reuse old passwords.

Security tokens

- A security tokens is a hardware device that contains the credentials of a person for authentication.
- It is considered to be the most trusted method of verifying the identity of a user.
- The hardware device is coded to generate token values at predetermined intervals.
- The software component of the token tracks and verifies that these codes are valid.
- Tokens use a variety of authentication methods such as one-time password, single sign-on, or two-factor.

Multifactor authentication

- Multifactor authentication uses two or more factors to identify a person:
  - — A *something you know* factor, such as your password or PIN.
  - — A *something you have* factor, such as your hardware token or a smart card.
  - — A *something you are* factor, such as your fingerprints, your eye retina, or other biometrics that can be used for identity.
  - — A *something you do* factor, such as your handwriting or your voice patterns.

Mutual authentication

- Mutual authentication is used to verify the identity of both ends of communication.
- This method prevents Man-In-The-Middle Attacks (MITM).
- Most network operating systems provide mechanisms for mutual authentication.

Biometrics

- Biometrics is used to authenticate a person using physical and behavioral characteristics.
- Advanced biometric devices help identify a person using fingerprints, handwriting, voice patterns, or eye retina scans.
- This is the most trusted method of authentication.

Auditing and logging

- Auditing helps track the activities of users and system processes and helps save audit entries in log files.
- Auditing is a two-step process: enabling auditing on resources and viewing audit log files.
- It can help troubleshoot and diagnose system and network problems.
- It can help track internal and external security breaches.

- System auditing helps track authorized and unauthorized access of system resources and processes.
- Unauthorized activities include attempts to access classified information, concealment, conversion, and copying of confidential data.
- Log files must not be accessible to unauthorized users.

System scanning

- System scanning is used to examine the security settings of a system or network.
- It helps detect vulnerabilities.
- It is also useful to test the performance of a system.
- Administrators can take corrective steps to protect the network based on the results of system scanning.

Types of attacks

- In an active attack, the attacker is actively involved in the process.
- In a passive attack, the attacker just monitors the network and collects information.
- In password attacks, the attacker uses different methods such as password guessing, dictionary attacks, or brute force attacks.
- In a malicious code attack, the attacker tries to run malicious code, such as viruses, worms, Trojans, or logic bombs.

Denial of Service (DoS) attack

- A DoS is an active attack that results in the unavailability of a network service to legitimate users.
- The attacker attempts to consume all resources on a server or on the entire network.
- Examples include SYN flood, ICMP flood, UDP flood, buffer overflows, land attacks, and nukes.

Distributed Denial of Service (DDoS) attack

- DDoS is an amplified form of a DoS attack launched in the client/server mode.
- The attacker installs a server side of the malicious application on Internet hosts called the Master.
- The Master installs a client-side component on other Internet hosts called Zombies.
- Zombies are instructed to simultaneously launch a DoS attack on the target host or network.

SYN flood attack

- A SYN flood attack utilizes the three-way TCP/IP handshake process.
- The attacker sends a large number of TCP/SYN messages to the target host with forged source IP addresses.
- The server sends responses to forged IP addresses, thus leaving TCP ports open.
- These half-open ports result in denial of services to legitimate IP addresses.

IP spoofing

- Spoofing is the process of presenting a fake identity in order to gain access to secure resources.
- IP spoofing is the process of using a false IP address to gain access to a server or network.
- Blind IP spoofing occurs when the attacker just sends IP requests to the target and does not wait for a response.
- Informed IP spoofing occurs when the attacker is sure of getting responses from the target.

Man-in-the-Middle (MITM) attack

- An MITM attack occurs when the attacker is actively listening to communications between two hosts.
- It uses the TCP/IP three-way handshake process.
- The attacker places himself between the server and the legitimate client.
- The server is made to send responses to a client's requests to a computer that is in the attacker's control.
- The use of mutual authentication, strong passwords, and encryption can prevent MITM attacks.

Replay attack

- A replay attack occurs when a valid data transmission is delayed or sent repeatedly to a server.
- This attack occurs due to poor security mechanisms used for TCP/IP communications.
- The attacker uses TCP/IP sequence numbers to generate valid messages.
- The use of session tokens with timestamping, more random TCP/IP numbers, SSH, and IPSec can be used to prevent replay attacks.

TCP/IP hijacking

- An attacker captures TCP/IP sessions between two hosts.
- Insecure FTP, Telnet, or Rlogin sessions are usually targets of TCP/IP hijacking.
- Use of secure session keys can prevent hijacking of TCP/IP sessions.

Weak keys

- Weak keys result from encryption algorithms that use short keys.
- Keys used in DES, RC4, IDEA, and Blowfish are known to have some weakness.
- The selected encryption algorithm should set all keys as equally strong.

Password attacks

- The attacker tries to obtain a user's password using a variety of methods.
- Weak passwords are vulnerable to password guessing attacks.
- Dictionary attacks use all possible combinations of words listed in a dictionary.

- A brute force attack uses software applications to decrypt an encrypted message by trying different combinations of encryption keys.
- The attacker must have the username and hashed password in order to launch a brute force attack.

Buffer overflow

- In a buffer overflow attack, the attacker tries to exploit security breaches or memory usage by applications and then tries to crash the target host.
- The attacker executes malicious code to fill all memory spaces in the target.
- Applications with privileged access levels may terminate exposing vulnerabilities to attackers.
- Buffer overflows can also result from incorrect selection or use of a programming language.

Software exploitation

- Software exploitation is used by attackers to take advantage of software glitches, bugs, or inappropriately written code.
- It may also result in giving escalated privileges to an unauthorized user.

Back door

- A back door attack is the process of bypassing normal authentication processes to gain access to a system.
- Trojan horses and rootkits are known to use the back door process to exploit a system.
- A symmetric back door application allows anyone to use it.
- An asymmetric back door application is used only by its creator.

Types of malicious code

- Malicious code, or malware, is an application used to gain access to a system without the user's knowledge or permission.
- Malware includes viruses, Trojan horses, worms, and applications such as adware, spyware, botnets, or loggers.

Virus

- A virus is a self-replicating application.
- It inserts into an executable and spreads when the file is run.
- A bootstrap virus infects the boot sector of the hard disk.
- A parasitic virus resides in an executable file.

Worm

- A worm resides in the active memory of the computer and is usually not noticeable.
- It keeps scanning the network for vulnerabilities.
- It spreads itself on to other computers in the network.

Trojan horse

- A Trojan horse is malicious code embedded inside a legitimate application.
- It appears as a very useful application to the user.

- It is used to collect personal information about the user.
- Most spyware, adware, and pop-up windows fall into this category.

Logic bombs and Time bombs

- A logic bomb is malicious code that waits for some condition to be met before it executes.
- It can also execute when some event happens.
- A time bomb is another type of malicious code that waits for a particular time to execute.

Wardialing

- Wardialing is used to gain unauthorized access to a remote network server.
- Attackers use wardialing software to dial several telephone numbers to search for a server that responds.
- If any remote access server responds, the attacker can penetrate into the corporate network.

Dumpster diving

- Dumpster diving refers to searching the trash to get information from personal or corporate waste.
- Printed papers containing information should be shredded to prevent leaking information to dumpster divers.

Social engineering

- Social engineering is the process of getting personal information by taking someone into confidence.
- Information can be collected face-to-face, over the phone, or over the Internet.
- The person becomes a victim by trusting someone and reveals personal or corporate information.
- It results in phishing attacks.

Disabling nonessential services and protocols

- Several services and protocols are installed by default when an OS is installed.
- Nonessential services or protocols are vulnerable to external attacks if not correctly configured.
- These services and protocols should be disabled or removed.
- Service dependencies should be checked before services are disabled.

Communication Security

This subsection covers the summary of highlights from the "Communication Security" section in the Security+ Exam Study Guide.

Remote access security

- Remote access servers need to be secured against unauthorized external access.

- Authentication protocols are used to identify remote users.
- Users are granted access based on the principle of least privilege.

802.1x authentication

- 802.1x is the authentication standard for wireless networks.
- It uses EAP as authentication protocol to both wired and wireless LANs.
- *Supplicant* refers to the software component installed on client computer.
- *Authenticator* refers to the wireless access point that forwards a client authentication request to a server such as a RADIUS server.
- This protocol helps prevent eavesdropping attacks.

Extensible Authentication Protocol (EAP)

- EAP is used in wireless networks and point-to-point connections.
- EAP-TLS is considered most secure and is implemented in a Public Key Infrastructure (PKI).
- EAP-MD5/CHAP uses a one-way hash function to provide security but is prone to dictionary attacks.
- PEAP is used in wireless networks.
- RADIUS is the most widely used protocol for authenticating remote users.

Virtual Private Networking (VPN)

- VPN is implemented by creating a communication tunnel in a public network (Internet).
- Carrier protocols are used on the Internet to carry data.
- Encapsulating protocols (PPTP, L2TP/IPSec, SSH, etc.) are used to wrap data before transmission.
- A site-to-site VPN is used to provide connectivity between two remote offices of an organization.
- Remote access VPN is used to provide connectivity to individual remote users.

Remote Authentication Dial-In User Service (RADIUS)

- RADIUS is the most widely used protocol for centralized authentication of remote clients.
- It can be used for dial-up clients, VPN, and wireless connections.
- It provides authentication and authorization.
- It supports use of PPP, CHAP, EAP, MS-CHAPv2, and PAP protocols.
- It uses UDP ports 1812 and 1813.
- RADIUS is prone to buffer overflow attacks.

Terminal Access Controller Access Control System (TACACS)

- TACACS is used for centralized authentication in Unix environments.
- It provides authentication and authorization.
- TACACS uses UDP port 49.

- TACACS+ uses TCP port 49 and provides authentication, authorization, and accounting.
- Both TACACS and TACACS+ are prone to replay, birthday, packet-sniffing, and buffer overflow attacks.

Point-to-Point Tunneling Protocol (PPTP)

- PPTP is used to create secure VPN tunnels using TCP port 1723.
- It is easy to implement and administer.
- It works only in IP networks and does not provide encryption of authentication data.
- Only the data transmitted after initial authentication is encrypted.
- MMPE protocol is used for data encryption in Microsoft networks.

Layer 2 Tunneling Protocol (L2TP)

- This combination is used for secure VPN communications and uses TCP port 1701.
- L2TP provides computer authentication as well as user authentication.
- When used with IPSec, it provides confidentiality, authentication, and integrity.
- It can be used in IP, IPX, and SNA networks.

IP Security (IPSec)

- IPSec provides secure IP communications by encrypting each IP packet.
- The Authentication Header (AH) is used to sign each IP packet to ensure authenticity and integrity.
- The Encapsulating Security Payload (ESP) is used for authenticity, integrity, and confidentiality to each IP packet.
- The transport mode is used for host-to-host communications and encrypts only the payload (the actual data or the ESP).
- The tunnel mode is used for gateway-to-gateway communications and uses AH only.

Multipurpose Internet Mail Extensions (MIME)

- MIME is an extension of the Simple Mail Transfer Protocol (SMTP) used for messaging.
- Secure Mime (S/MIME) is used for secure messaging using symmetric cipher and public keys.
- S/MIME uses digital signatures for integrity, and a variety of encryption algorithms for confidentiality of messages.

Pretty Good Privacy (PGP)

- PGP is used for secure messaging by providing encryption and authentication.
- PGP uses secret keys known to sender and receiver, which are stored in a local computer.
- *Paraphrase* is used to protect keys.

Email spam

- Spam is unsolicited email sent to a large number of recipients.
- These messages fill mailboxes.
- Spam filters can be used for protection.
- Cookies should be disabled to protect personal information from leakage.

SMTP relay, email viruses, and hoaxes

- Email viruses can be embedded in messages.
- Hoaxes are messages that make the receiver believe something that is not true.
- SMTP relay is used to send unsolicited messages from a third-party server to multiple users.
- DNS blocking lists can be used to prevent SMTP relay.

Securing web servers

- Only authorized personnel should be allowed to work on servers.
- Web servers should be placed inside a perimeter network secured by firewalls.
- All traffic coming in and going out of the network should be monitored.
- Web servers and database servers should be regularly backed up.
- Web server content such as applications and scripts should be properly tested.
- Rogue web servers should be detected and disabled.
- The Intrusion Detection Systems (IDS) should be deployed.

Securing web browsers

- Internet access should be monitored.
- Web browsers should be properly configured to handle cookies.
- Java applets, JavaScript, and ActiveX controls must be configured carefully.
- Users should be allowed to download only digitally signed software.
- Instant Messaging (online chatting) should be prohibited outside the organization.

Secure Socket Layer/Transport Layer Security (SSL/TSL)

- The client and the server negotiate an encryption algorithm and exchange session keys.
- Both ends authenticate each other using certificates.
- Communications start, and all traffic is encrypted using symmetric cipher.
- RSA, Diffie-Hellman, or DSA are used for public key encryption.
- RC2, RC4, IDES, DES, 3DES, or AES are used for symmetric cipher.
- MD5 or SHA1 are used for hash functions.

Vulnerabilities in Internet services

- Java Applets, JavaScript, ActiveX controls, and cookies are vulnerable components.
- JavaScript and ActiveX are parts of HTML and run in the browser.
- Cookies store personal information about the user.
- These components should be configured carefully to protect web clients.

Buffer overflow

- Buffer overflow attacks on web servers exploit weaknesses in program codes.
- Buffer overflow occurs when more data is written to the memory than it can handle.
- Stack-based and heap-based overflows are two types of buffer overflows.
- Programmers should use correct language and test web applications to prevent buffer overflow attacks.

Signed applets

- Web programmers should download only digitally signed applets.
- The code-signing process ensures that code or an applet is authenticated by its vendor and has not been modified.
- Unsigned applets or code may create vulnerabilities in web applications.

Common Gateway Interface (CGI)

- CGI is a web-side application that runs on the web server to provide interfaces to applications.
- Hackers can exploit poorly written CGI scripts to launch attacks.
- CGI scripts should be scanned for vulnerabilities before being used on web servers.

Directory Services and FTP security

- Lightweight Directory Access Protocol (LDAP) follows X.500 naming conventions.
- LDAP transmissions can be secured using server certificates and SSL.
- In normal FTP, the passwords and data are transmitted in clear text.
- FTP file transfers should be secured using secure FTP (S/FTP) protocol.

Wireless communications

- Wireless communications rely on radio frequencies.
- They are susceptible to electromagnetic and radio frequency interference (EMI and RFI).
- Spread spectrum wireless technologies are used to reduce the effects of EMI and RFI.

Frequency-hopping spread spectrum (FHSS)

- RF signals are transmitted by rapidly switching frequencies.
- FHSS works in the unlicensed frequency range of 2.4 GHz.
- It has limited transmission speed of 1.6 to 10 Mbps.
- It is used in Home RF and Bluetooth.

Direct-sequence spread spectrum (DSSS)

- DSSS is a modulation technique that uses a wide band of frequency.
- It adds redundant bits of data known as *chips*.
- The ratio of chips to data is called the *spreading ratio*.
- DSSS is faster than FHSS and ensures data protection.
- It utilizes a frequency range of 2.4 GHz to 2.4835 GHz and is used in 802.11b networks.

Wireless Application Protocol (WAP)

- WAP is an open protocol for handheld wireless devices.
- Microsoft Windows CE, PalmOS, and JavaOS are some examples of operating systems that use WAP.
- A WAP browser is used to access Internet sites that use Wireless Markup Language.
- The current version is WAP 2.0.

Wireless Transport Layer Security (WTLS)

- WTLS protocol is designed to provide end-to-end security for WAP devices.
- WTLS provides privacy and availability for both the WAP server and the WAP client.
- WTLS uses a compressed certificate format following the X.509v3 standard.

802.11

- The IEEE 802.11 standard defines the operation of wireless networks within the 2.4 GHz frequency range using either FHSS or DSSS.
- The 802.11b standard defines DSSS network devices using the 2.4 GHz frequency range that can communicate at speeds of 1, 2, 5.5, or 11 Mbps
- The 802.11a standard uses the 5 GHz frequency range with a data transmission speed of up to 54 Mbps.
- The 802.11g standard uses the 2.4 GHz frequency range and transfer speeds of up to 54 Mbps.

Ad-hoc and Infrastructure wireless networks

- In Ad-hoc wireless configuration, there are several wireless devices within range of each other.
- In Ad-hoc networks, there is no Access Point (AP), and two or more wireless devices create a network by connecting to one another.
- In Infrastructure configuration, wireless clients communicate with one another and other resources through the AP.
- The AP authenticates and configures wireless clients.
- A special identifier known as the Service Set Identifier (SSID) must be configured on the AP and on each wireless client.
- Different Infrastructure networks are identified by their unique SSIDs.
- The AP can further be connected to the wired Local Area Network (LAN).

Wired Equivalent Privacy (WEP)

- WEP is the security standard for 802.11 wireless networks.
- It provides privacy in transmissions occurring between the AP and the wireless client.
- It uses shared key authentication that allows encryption and decryption.
- Up to four different 40- or 128-bit keys can be defined on the AP and the client.
- The keys can be rotated for enhanced security.
- WEP uses the CRC-32 checksum for data integrity.
- Confidentiality is ensured with the RC4 encryption algorithm.

Open and Shared Key Authentication

- Open Authentication is device-specific, and all devices are granted access.
- Shared Key Authentication is used to grant access to only those wireless clients who possess the SSID and the shared key.
- The client is called the supplicant, and the AP is called the authenticator.
- Shared key authentication is susceptible to plain-text attacks.

Protecting wireless networks from attacks

- Software and hardware should be kept updated.
- When installing, the default settings of the AP (such as the SSID) should be changed.
- Even 40-bit encryption is better than not using WEP encryption at all.
- If SSID broadcasts are not disabled on APs, a DHCP server should not be used.
- Static WEP keys should be frequently rotated for enhanced security.
- Place the wireless networks in a separate network segment.
- Conduct regular site surveys to detect the presence of rogue APs.
- Place APs in the center of the building and not near windows.

Site surveys

- Site surveys are used to detect the boundaries of a wireless network.
- The tools used to conduct site surveys are typically the same tools that the hackers use to detect unprotected wireless networks.
- Tools such as NetStumbler, Kismet, AirSnort, and WEPCrack are used for site surveys.
- A physical inspection of the building's surroundings should be conducted.

Infrastructure Security

This subsection covers a summary of highlights from the "Infrastructure Security" section in the Security+ Exam Study Guide.

Packet-filtering firewalls

- These firewalls permit or block access to specific ports or IP addresses.
- In the *Allow by Default* policy, all traffic is allowed except that which is specifically denied.

- In the *Deny by Default* policy, all traffic is blocked except that which is specifically allowed.
- Well-known port numbers range from 0 to 1023.
- User ports (registered ports) range from 1024 to 46,151.
- Dynamic/private ports range from 46,152 or 65,535.

Application layer firewalls

- These firewalls examine the entire packet to allow or deny traffic.
- They are much slower than packet-filtering firewalls.
- Proxy servers use these firewalls to provide application layer filtering.

Stateful Inspection Firewalls

- These firewalls actively monitor and inspect the state of network traffic.
- They are faster than application layer firewalls.
- They can dynamically open and close ports as needed by applications.

Routers

- Routers connect two segments of an internetwork and work at Layer 3 of the OSI model.
- They use a table of IP addresses to forward network traffic.
- Administrators build static routing tables in small networks.
- Distant vector and link states are dynamic routing protocols.
- Routers support Access Control Lists (ACLs) to determine which IP packets should be allowed or blocked.
- Dynamically built routing tables are prone to spoofing and eavesdropping.

Switches

- Switches connect network segments and work at Layer 2 of the OSI model.
- Switches use MAC addresses to forward network traffic.
- Switches offer better security than routers.
- Switches are prone to ARP spoofing, DoS, and MITM attacks.
- Hackers can use MAC flooding to exploit a poorly configured switch.

Securing workstations

- Users should not create weak passwords.
- Passwords should be changed at regular intervals.
- Virus scanners with the latest virus signatures should be used on all workstations.
- Web browsers should be properly configured to avoid downloading or running active content from different web sites.
- Users should be instructed to lock their workstations when they are away.

Securing servers

- Servers should be kept in locked rooms with limited physical access.
- Auditing and logging of user and administrator activities should be done.

- Users should be granted only need-based (or role-based) access to servers.
- Files and folders should be protected using ACLs.
- Network Operating Systems (NOSs) installed on servers should be kept up to date.
- Servers accessible from outside, such as web servers, mail servers, remote access servers, and VPN servers, should be placed in demilitarized zones.
- All communications between servers and workstations should be encrypted.

UTP/STP cables

- The twists in cables prevent electromagnetic interference, which results in crosstalk.
- These cables are twisted pairs of insulated cables bundled inside a plastic sheath.
- Their category number usually identifies them.
- UTP/STP cables use RJ-11 (for telephone) and RJ-45 (for computers) connectors.
- UTP cable is vulnerable to EMI, RFI, and eavesdropping.
- STP cable provides protection from EMI and RFI.

Fiber optic cable

- Fiber optic cable is made up of very thin glass or plastic inside a sheath.
- The data transmission is based on the transport of light signals.
- Fiber optic cables can also carry data signals to longer distances than UTP or STP cables.
- They are immune to EMI and RFI and provide protection against eavesdropping and sniffing attacks.

Magnetic tapes

- Magnetic tapes are used for backing up data because of their large capacity and their ability to be reused.
- Data backed up on tapes should be encrypted.
- Tapes should be stored offsite to protect them from theft and provide safety in case of disasters.
- Employees should not be allowed to bring in or take out any magnetic media.

Hard drives

- Data stored on hard drives should be encrypted.
- Hard drives should be kept away from locations where strong magnetic fields exist.
- Only administrators should add, remove, or configure drives.
- Servers should be physically secured since hard drives (and the data they contain) are part of the server hardware.

Floppy disks and flash cards

- To prevent data theft, floppy disks should not be allowed to be removed from the building.
- Flash cards are small in size and can easily be stolen.
- They can be damaged when dropped or placed near high-static electricity.

Security zones

- A security zone is a part of a network that possesses special security requirements.
- DMZ, intranet, extranet, and VLAN are all considered security zones

Security zones are protected by firewalls

- Firewalls allow only limited traffic based on certain rules, and they block unwanted, unsolicited, and malicious traffic.
- They maintain audit logs for incoming and outgoing traffic.
- They perform additional authentication for enhanced security.
- They mask the internal map of network hosts inside the security zone.

Demilitarized Zone (DMZ)

- DMZ is a network segment that sits between the internal network and an external network, usually the Internet.
- Firewalls, routers, and switches protect the DMZ and block all unwanted traffic.
- They do not allow internal users to reach harmful external Internet sites.
- In a Multiple Interface Firewall DMZ, a single firewall with multiple interfaces is used.
- In a Layered DMZ, the secure servers are placed between two firewalls: external and internal.

Intranets and extranets

- Firewalls should be configured to allow only intended traffic and to block all unwanted traffic.
- Only authorized administrators should have physical access to firewalls and servers for the intranet and extranet.
- Security logs should be regularly monitored on firewalls and servers.
- L2TP and IPSec protocols should be implemented for additional security.
- All servers should be kept updated with the latest service packs, security patches, and antivirus software.

Virtual Local Area Network (VLAN)

- A VLAN is a logical grouping of network devices that share common security requirements.
- It helps reduce network collisions by creating separate broadcast domains.
- It also provides security at the Data Link layer (Layer 2) of the OSI model.
- Network switches are mainly used to create VLANs.
- VLANs are created on the basis of groups and memberships.

- The memberships can be port-based, protocol-based, or MAC address-based.
- Each VLAN functions like a separate physical network segment.
- It can span multiple physical network segments or multiple switches.
- A Trunk is the point-to-point link between one switch and another.
- The Trunk carries network traffic between each switch that is a part of a VLAN.

Network Address Translation (NAT)

- NAT is a feature of firewalls, proxy servers, and routing services.
- It is used to provide secure Internet access to clients on the internal network.
- It also enables organizations to host web and mail services securely.
- It hides the internal IP addressing scheme and network design.
- One server or a network device shares the Internet connection with internal clients.
- It allocates IP addresses to these clients from one of the following private IP address ranges:
  - — Class A: 10.0.0.1 to 10.255.255.254
  - — Class B: 172.16.0.1 to 31.255.254
  - — Class C: 192.168.0.1 to 192.168.255.254
- Internet Connection Sharing (ICS) in Windows XP is a scaled-down version of NAT.
- ICS can use only one public IP address, and internal clients can use class C private IP addresses.
- ICS is suitable only for very small networks that do not have any subnets.

Intrusion Detection System (IDS)

- An IDS is used to detect intrusions and malicious activities in networks.
- It monitors the network continuously for activities and compares them to known attack signatures.
- An active IDS can reprogram the firewalls and routers upon detection of an attack.
- A passive IDS logs the information and sends an alert upon detecting an attack.
- A false positive occurs when the IDS triggers an alert even when there is no attack.
- A false negative occurs when the IDS does not trigger an alert when there is a real attack.
- A Network-based IDS (NIDS) detects intrusions by monitoring the entire network traffic and multiple hosts in the network.
- A Host-based IDS is a software application that monitors network traffic coming in or going out of a specific network host.
- A Signature-based IDS monitors network traffic to detect attack signatures.
- An Application-based IDS monitors the activities of applications.

Honeypots

- A honeypot is a trap used to attract attacks on a network.
- It appears to be a critical server or part of a network containing valuable information to the attacker.
- The attacker does not know that he is attacking a fake network site.
- It is used to test the intrusion detection systems and create attack signatures.

Filesystems

- Filesystems allow administrators to grant need-based access to files and folders.
- Users are put into groups, and permissions are configured for groups.
- The principle of least privilege is applied when assigning permissions.
- The principle of least privilege restricts access to resources and prevents unauthorized access.

Updates, hotfixes, and service packs

- Manufacturers release updates (service packs, hotfixes, and security patches) to address problems with their software.
- A hotfix is a small piece of software that is used to address a specific problem with the operating system.
- A service pack is a collection of a number of hotfixes and updates.
- Updates should be tested before they are installed.
- Administrators should check manufacturers' web sites regularly for the release of updates.

Network hardening

- Network hardening locks down network devices to protect them from external and internal threats.
- Firmware of devices should be updated as and when necessary.
- Network devices should not be used with default configurations.
- Access Control Lists (ACLs) of devices should be configured to prevent unauthorized traffic.
- The ACLs can be configured on the basis of interface, port numbers, protocols, IP address, or MAC address.

Application hardening

- Software applications on desktops and servers should be kept up to date with the latest service packs, hotfixes, and security patches.
- Security patches, hotfixes, or service packs must be thoroughly tested before installation.
- Updates that provide only cosmetic changes need not be installed.
- Appropriate access should be configured on applications.
- Antivirus software should be run regularly with updated virus signatures.

Web servers

- The NOS must be secured properly, and it should be kept up to date.
- Antivirus software should be used with updated virus signatures.

- A web service should not be left in its default configurations.
- Named accounts should not allow anonymous access to web servers.
- User authentication should be processed using strong protocols, and all transactions should be encrypted for e-commerce web servers.
- Web servers should be placed inside a Demilitarized Zone (DMZ).

Email servers

- The NOS over which the email services are running must be secured properly.
- Antivirus software should be run regularly with updated virus signatures.
- SMTP relay should be disabled as it can cause DoS attacks.
- Users must be careful not to open suspicious attachments that may contain email viruses.
- Usage of HTML email should be avoided.
- Internet Messaging (IM) outside the organization should be monitored.
- Email servers should be placed inside a DMZ.

FTP servers

- FTP servers are permanently connected to the Internet and attract malicious users.
- Filesystem security should be appropriately configured.
- Access control, authentication, and authorization systems should be in place.
- Audit policy should be implemented and security logs should be reviewed regularly.
- FTP servers should be placed inside a DMZ.

DNS servers

- DNS servers update other DNS servers using zone transfers.
- Zone transfers should be configured for authorized DNS servers only.
- DNS servers should listen to name resolution requests from intended interfaces only.
- Secure dynamic updates should be used only.
- Administrators should detect and remove rogue DNS servers on the network.
- DNS servers for web services should be placed inside a DMZ.

File and print servers

- File and print servers are the most frequently used and heavily loaded servers.
- They should be secured with Access Control Lists, authentication processes, and effective auditing and logging.
- If a user does not need to share a file or folder, he should not.
- Default share permissions should be disabled, and anonymous access should not be allowed.

DHCP servers

- DHCP servers are used to automatically assign IP addresses to DHCP clients.
- DHCP servers maintain blocks of IP addresses in DHCP scopes.

- Access to a DHCP server can provide information about an internal IP addressing scheme.
- DHCP servers must be secured properly and kept up to date with security patches, hotfixes, and service packs.
- Rogue DHCP servers should be detected and taken offline immediately.
- DHCP servers should be configured to send secure dynamic updates to DNS servers.
- Only authorized administrators should be permitted to manage DHCP servers.

Basics of Cryptography

This subsection covers a summary of highlights from the "Basics of Cryptography" section in the Security+ Exam Study Guide.

Symmetric encryption algorithms

- A symmetric algorithm uses one key for both encryption and decryption.
- It is also known as a secret key, a private key, or a shared secret encryption.
- It is widely used because of simplicity, easy implementation, and speed.
- Symmetric algorithms are divided into stream ciphers and block ciphers.
- Stream ciphers encrypt bits of the message, one at a time.
- Block ciphers take 64-bit blocks and encrypt them as one unit.
- Symmetric algorithms are prone to brute force attacks.

Data Encryption Standard (DES)

- DES uses a single 64-bit block of plain text for encryption.
- It also uses a 64-bit key—56 bits for data and 8 bits for parity.
- DES is known for weak security due to the small size of the key.
- 3DES (Triple DES) uses the 56-bit key three times to make the key size larger.

Advanced Encryption Standard (AES)

- AES supports a large range of text blocks and key sizes.
- Key sizes of 128, 192, and 256 bits are used.
- The 128-bit data block is broken into four groups, each with 32 bits.
- It is stronger and faster than 3DES and consumes less processing power and memory.

International Data Encryption Standard (IDEA)

- IDEA operates on 64-bit data blocks with a 128-bit subkey.
- The encryption and decryption process uses eight rounds with 16-bit subkeys per round.
- It is a faster and more secure algorithm than DES.

Asymmetric encryption algorithms

- Asymmetric encryption algorithms are used in public key cryptography.
- Two separate keys are used: one for encryption (the public key) and the other for decryption (the private key).

- The public key can be freely distributed, but the private key must be held in strict confidence.
- Asymmetric algorithms are much slower than symmetric algorithms.
- Asymmetric algorithms are used for confidentiality, integrity, authenticity, and non-repudiation.
- Diffie-Hellman, ElGamal, and RSA are asymmetric algorithms.

Hashing algorithms

- Hashing algorithms are used for integrity and authentication of data.
- A hashing algorithm, or a hash function, creates a unique digital fingerprint from data known as the hash value.
- If the original data changes, the hash function will produce a different hash value.
- The hashing function is considered a one-way process.
- Encrypted passwords are stored as hashes in secure networks.
- Message Digest 5 (MD5) is a hashing algorithm that uses a 128-bit hash value.
- Secure Hashing Algorithm 1 (SHA1) uses a 160-bit hash value.

Concepts of cryptography

- Confidentiality means that only the intended recipient can decrypt and read a message.
- Integrity means that the data/message has not been changed during transmission.
- Authentication refers to the verification of identity.
- Non-repudiation means that the sender cannot deny that he sent the message.
- Digital signatures are used to ensure data integrity and non-repudiation.

Digital certificates

- Certificates are used to identify a user or an organization.
- Certificates are based on the X.509 standard.
- The Certification Authority (CA) is a PKI that binds a private key to an individual or organization.
- Certificates are used for encryption of email and e-commerce, and for digitally signing software.
- Certificate policies define how the CA will issue certificates.
- Certificate Practice Statements (CPS) describe how the CA plans to manage the certificates that it issues.

Trust models

- In a single CA model, there is only one CA that issues and manages certificates.
- A hierarchical model is comprised of a root CA (enterprise CA), subordinate CAs, leaf CAs, and end users.
- The root CA uses a self-signed certificate.
- In the web of trust model, all CAs sign the certificates of each other.

Storage of private keys

- Private certificate keys can be stored on hardware devices or software.
- Hardware devices such as smart cards or PCMCIA cards can be used to store private keys.
- Network operating systems also allow storage of private keys.
- In Escrow storage arrangement, the private keys are stored with two different companies, each holding only a part of the keys.

Certificate revocation

- Certificates are revoked if they are compromised—for example, when a user leaves a company or if an organization changes the ISP.
- When a certificate is revoked, the information is sent to the CA.
- The CA publishes the revoked certificate in the certificate revocation list (CRL).
- Online certificate status protocol (OCSP) allows users to check the status of a particular certificate.
- In large organizations, multiple CAs maintain a base CRL.
- The base CRL is updated using Delta CRLs.

Certificate expiry, renewal, suspension, and destruction

- Every certificate has a defined expiry date.
- A certificate must be renewed with the CA before the expiry date.
- CAs renew certificates either by issuing a new key or by updating the old key.
- The CA can renew its own certificate.
- If the user will not be using the certificate, it can be suspended to help secure the private key.
- When the certificate is no longer needed, it is destroyed.

Recovery of private keys

- If a user forgets his private key, it needs to be recovered from storage.
- An administrator is designated as a key recovery agent.
- In large organizations, two key recovery agents are required for added security.
- When the key recovery process is broken up into multiple key recovery agents, the process is known as *M-of-N Control*.
- M-of-N Control states that out of a total of *N* recovery agents, at least *M* must be present for key recovery.

Operational and Organizational Security

This subsection covers a summary of highlights from the "Operational and Organizational Security" section in the Security+ Exam Study Guide.

Physical security

- Access Control is used to grant physical access to network equipment to authorized personnel.

- Critical servers and network equipment should be kept in a locked room.
- These rooms should be equipped with alarm systems.
- Log books should be maintained for recording entries to the secure room.
- Strong authentication methods such as biometrics should be used.
- If outsiders work inside secure rooms, an employee should accompany them.

Environment

- The temperature should be kept within limits.
- Alarms should be installed to monitor temperature and to sound alerts, if required.
- Humidifiers or dehumidifiers, as required, should be installed.
- Hardware technicians should wear ESD wristbands.
- Good air quality should be maintained inside server rooms.
- Equipment should be located in racks on raised floors.
- If required, STP cable should be used to protect the equipment from EMI and RFI.
- Fire suppression equipment should be used to prevent damage from accidental fire breakouts.
- Water sprinklers should not be used in server rooms.

Backups

- Data backup is a critical element of a disaster recovery plan.
- Backup media should be stored at an offsite location.
- The full backup backs up all the data in a single backup job and changes the archive bit.
- It takes longer to back up, but restoration is fast.
- An incremental backup method backs up all the data that has changed after the last full or incremental backup and changes the archive bit.
- The last full backup tape and all incremental tapes after the full backup are required to completely restore data.
- The differential backup method backs up all the data that has changed after the last full backup and does not change the archive bit.
- Only the last full backup and the differential backup tapes are required for restoring data.
- The copy backup method copies all the data on the system, but unlike the full backup, does not change the archive bit.

Tape rotation and offsite storage

- Backup tapes are reused in order to reduce costs.
- Grandfather-father-son (GFS) is the most commonly used tape rotation plan.
- The daily tape set is known as *son*, the weekly tape set is known as *father*, and the monthly full backup tape set is known as *grandfather*.
- A full backup is taken every week; differential or incremental backups are taken every day; and another full backup is taken every month.

- When the month changes, the tapes used for the first week in the previous month are reused.
- The grandfather tape set is not reused.
- Offsite storage of backup tapes protects critical data in the event of a disaster.

Alternate sites

- An alternate site is a temporary facility away from the original location.
- It enables administrators to restore a working network on short notice.
- A hot site is equipped with necessary hardware, software, network devices, and telephone lines, which allows organizations to resume business immediately.
- A warm site is equipped with necessary hardware, but the hardware and software must be configured and data must be restored to make the site operational.
- A cold site contains only partial hardware, software, and network devices and needs to be built from scratch.
- The cold site requires the maximum amount of time to be set up.

Business continuity plan

- A business continuity plan is developed after assessment of risks, threats, and disasters.
- The disaster recovery plan defines the procedures to recover after a disaster strikes.
- The business recovery plan describes the procedures to resume business functions at an alternate site after a disaster.
- The business resumption plan describes the procedures to resume functions of critical systems in order to begin business again.
- The contingency plan describes the procedures to resume business after a disaster strikes or when additional unforeseen events take place during the recovery process.

High availability and fault tolerance

- High availability refers to providing maximum uptime and availability of network services.
- Network load balancing is used to distribute load across several servers.
- Server clustering is used to provide system fault tolerance.

Disk fault tolerance

- RAID systems are used to provide fault tolerance for hard disks in a server.
- RAID 1 uses two disks with 50 percent disk utilization.
- RAID 5 uses 3 to 32 disks and also supports the hot swapping of disks.

Acceptable use policy

- Acceptable use policy describes the guidelines for users for appropriate use of computers.
- Users should not indulge in activities that might damage the image of the company.

- Users should not be involved in activities that might consume network resources beyond limits.
- Users should follow the rules that restrict visits to web sites and email programs.
- Users should not print any confidential documents.
- Users should not transmit confidential information over the Internet.

Due care policy

- A due care policy describes how the employees should handle hardware and software.
- Employees should be given guidelines on how to properly use equipment.

Privacy policy

- Employees should be educated on maintaining individual and organizational privacy.
- Organizations reserve the right to inspect personal data stored on company computers.
- Organizations can also monitor an end user's Internet usage and email.
- Critical data is also considered private and confidential.

Separation of duties

- This policy ensures that critical tasks are not assigned to a single person.
- No single person should have control over a task from beginning to end.
- Monopolization of duties should be prevented.
- Separation of duties makes users experts in their respective fields.

Need-to-know policy

- This policy defines restricted access to information.
- Users should be given permissions based on the principle of least privilege.
- Excessive information to employees might result in inappropriate handling.

Password management policy

- This policy describes how employees should manage their passwords.
- A password is the employee's key to gaining access to the organization's resources.
- Use of blank passwords should not be allowed.
- Passwords should have at least eight characters.
- A password should be made up of a combination of upper- and lowercase letters, special characters, and numbers.
- Employees should be forced to change their passwords regularly.
- Employees should not be allowed to reuse old passwords.
- Administrators should use normal user accounts when not performing any administrative tasks.
- Only designated IT employees should have administrative privileges.

Service Level Agreement (SLA)

- An SLA is usually signed between the organization and a third party that is providing critical services.
- It can also be used inside an organization describing what the company expects from its IT staff.
- It describes the expected level of performance and confidentiality.
- SLAs may also often include information on the maximum allowed downtime for computer systems.

Incident response policy

- This policy describes how employees will respond to unexpected incidents involving personal and organizational safety and security.
- It describes how incidents are to be handled without causing a panic.
- It asks the following common questions:
  - Who will investigate and analyze the reasons behind the incident?
  - Who will find an immediate and acceptable solution to the problem caused by the incident?
  - What other documents can be referred to in order to help resolve the problem?

Computer forensics

- Computer forensics is the application of computer expertise to establish factual information for judicial review.
- It involves activities such as collection, preservation, examination, and transfer of information using electronic media.
- All electronic crimes are reported to the incident response team.
- The first responder identifies and protects the crime scene.
- The investigator establishes a chain of command/chain of custody, conducts a search, and maintains the integrity of the evidence.
- The crime scene technician preserves volatile evidence, duplicates computer disks, shuts down the system for transportation, and logs activities.

Chain of custody

- A chain of custody describes how the evidence is transferred from the crime scene to the court of law.
- It specifies the personnel responsible for maintaining and preserving the evidence.
- It is entered in an evidence log and specifies the persons who possessed the evidence or who worked on it.

Preservation of evidence

- Crime scene data is protected from being damaged.
- Steps are taken to preserve the volatile data first.
- Photographs of screens are taken.
- Images of hard disks are made using accepted imaging tools.

- The system is shut down normally.
- Photographs of the existing system setup are taken before moving.
- Each piece of hardware is unplugged and tagged.
- Appropriate safety procedures are followed when handling hardware.
- Smaller pieces of hardware are placed inside antistatic plastic bags.
- Equipment is kept away from strong EMI and RFI.

Collection of evidence

- Collection of evidence is the process of identifying, locating, and processing evidence.
- Appropriate documentation is made.
- The crime scene is secured and unauthorized entry is prohibited.
- The evidence is identified and secured.
- The investigation team examines the evidence and takes steps for collection.
- Evidence is collected from audit logs, screen displays, and recovered data files.

Education and training

- Educating and training users helps to create a safe and secure working environment.
- Users must know available methods to communicate to their peers, their supervisors, management, and employees in other departments.
- Users should be made aware of rules, regulations, and security issues when working on computers.
- Online resources help educate, train, and keep users informed.

Risk identification

- A risk is the possibility of incurring some loss due to unexpected situations.
- Risk identification is the process of identifying assets, risks, threats, and vulnerabilities in a system.
- Organizations need to take steps to identify all types of assets and make an evaluation.
- After identifying assets, the type and severity of risks associated with each type of asset should be identified and assessed.
- The likelihood of occurrence of a risk within one year is called the Annual Rate of Occurrence (ARO).
- The dollar value of the loss is known as Single Loss Expectancy (SLE).
- Multiplying ARO and SLE gives a value of Annual Loss Expectancy (ALE).
- The formula for calculating the loss resulting from a risk is ALE=ARO x SLE.

Threat identification

- Identification of risks leads to identification of possible threats to a system.
- Threats include incidents involving vandalism, theft of equipment or data, and physical or software intrusions.
- Appropriate steps should be taken to avoid potential threats.

Vulnerabilities

- Vulnerability is defined as the weakness of a system.
- It can lead to exposure of critical and confidential information.
- Vulnerabilities can lead to internal malicious activities or even outside security attacks.
- Every software application and all hardware devices are vulnerable if not configured and secured properly.

Security+ Exam Practice Questions

1. Removal of nonessential services and protocols helps in all of the following except:

   ❍ A. Securing the system

   ❍ B. Network performance

   ❍ C. System performance

   ❍ D. Reduction of administrative overheads

   Answer D is correct. When you remove nonessential services and protocols from a system, it does not reduce administrative overheads. In fact, more administrative efforts are required to detect and disable or remove nonessential services and protocols from different servers across the network.

2. Which of the following authentication methods is used with timestamped session tickets?

   ❍ A. CHAP

   ❍ B. MS-CHAP

   ❍ C. Kerberos

   ❍ D. PAP

   Answer C is correct The Kerberos authentication protocol uses timestamped session tickets. The ticket expires when the user logs off.

3. You have been told to develop a system to control how and when a user will be allowed to connect to a remote access server. You should specify which media should be used to connect and to which groups the user should belong. Which of the following aspects of computer security are you supposed to work with?

   ❍ A. Access control

   ❍ B. Authorization

   ❍ C. Auditing

   ❍ D. Authentication

   Answer A is correct. Defining the stated conditions essentially applies to an access control system. You are deciding on how the users should connect if they need access to the remote access server.

4. You have just taken charge of some file servers in your organization. You suspect that someone is repeatedly trying to get unauthorized access to a confidential folder on one of the file servers. You decide to configure auditing on this server. Which of the following events should you audit?

   ❍ A. Object Access Failure

   ❍ B. Object Access Success

   ❍ C. Logon/logoff Failure

   ❍ D. Logon/logoff Success

   Answer A is correct. The person is trying to access the folder but is not successful. This means that the failure events for object access should be recorded in audit logs. It is also a good idea to audit successful object access events, just in case someone has obtained legitimate user credentials to access confidential information.

5. Which of the following is known as a label-based access control method and is hardcoded into a device?

   ❍ A. RBAC

   ❍ B. DAC

   ❍ C. MAC

   ❍ D. None of above

   Answer C is correct. The mandatory access control (MAC) method is hard-coded into devices and is known as label-based access control.

6. Which of the following is a probable cause of a hacker creating a back door in a system?

   ❍ A. The hacker is trying to guess the credentials of the user.

   ❍ B. The hacker is trying to get access without having to authenticate.

   ❍ C. The hacker is trying to get personal information from the user over the phone.

   ❍ D. The hacker is trying to connect to the user's wireless home network.

   Answer B is correct. A back door attack occurs when a hacker tries to get access to a system without having to authenticate. Attackers usually perform a back door attack by exploiting some system configuration or software vulnerability.

7. A programmer has written malicious code that will delete all systems files on a critical file server. This code will execute as soon as the programmer is terminated from the company and his user account is disabled or deleted. What kind of malicious code is this?

   ❍ A. Trojan horse

   ❍ B. Worm

   ❍ C. Virus

   ❍ D. Logic bomb

   Answer D is correct. A logic bomb is malicious code that waits for an event to occur. In this case, the code will wait for the user's account to be disabled or deleted.

8. Which of the following actions best describes the term *IP spoofing*?

   ❍ A. Trying to guess a password.

   ❍ B. Pretending to be someone you are not.

   ❍ C. Capturing TCP/IP traffic.

   ❍ D. Trying to crack an encryption key.

   Answer B is correct. In an IP spoofing attack, the attacker tries to use a false IP address in order to make the security system believe that the attacker's machine is a legitimate host on the network when it is not.

9. Which of the following has the necessary privileges to assign permissions to a shared resource when the discretionary access control method is used?

   ❍ A. All users

   ❍ B. The administrator

   ❍ C. The owner of the resource

   ❍ D. A power user

   Answer C is correct. When the discretionary access control method is used to control access to system and network resources, the owner of the resource has the necessary privileges to assign permissions.

10. An e-commerce web site is using digital certificates. Which part of authentication, access control, and auditing (AAA) is provided by these certificates?

    ❍ A. Authentication

    ❍ B. Access control

    ❍ C. Authorization

    ❍ D. Auditing

    Answer A is correct. Digital certificates are used to provide authenticity of a user or an organization. In this case, the e-commerce company is proving its identity to the users of a secure web site.

11. Which of the following transport protocols is used by TACACS+?

    ❍ A. IP

    ❍ B. IPX

    ❍ C. TCP

    ❍ D. UDP

    Answer C is correct. The TACACS+ standard uses TCP as its transport protocol.

12. You have decided to use WEP for securing the wireless network segment in the organization. Which of the following terms describes the user who wants to connect to this secure network?

    ❍ A. Applicant

    ❍ B. Supplicant

    ❍ C. Authenticator

    ❍ D. RADIUS

Answer B is correct. Wired Equivalent Privacy (WEP) is an 802.1x authentication standard. The wireless client in this setup is known as the supplicant, and the access point is known as the authenticator. The authenticator forwards the supplicant's authentication request to a centralized authentication server such as the RADIUS server.

13. You have just received an email, which says that most of the stocks listed on the NY stock exchange would be sold for $1 on the Fourth of July (Independence Day). You check with some of your friends, and they also received the same message. Which of the following terms best describes this kind of message?

 ○ A. SMTP relay

 ○ B. Trojan horse

 ○ C. Email hoax

 ○ D. Email spam

 Answer C is correct. An email hoax is a message that tries to make you believe in something that does not exist or some upcoming event that will never occur.

14. You have decided to implement IPSec protocol to provide secure end-to-end communication to remote access clients. In which of the following modes should you implement this protocol?

 ○ A. Tunnel mode

 ○ B. Encryption mode

 ○ C. Transport mode

 ○ D. A and B

 Answer C is correct. When IPSec is implemented in transport mode, it provides end-to-end communication security.

15. Which of the following is not an advantage of using L2TP/IPSec over using PPTP in remote access?

 ○ A. It provides two levels of authentication.

 ○ B. It works only in IP networks.

 ○ C. It can use RADIUS authentication.

 ○ D. It provides protection against replay attacks.

 Answer B is correct. Unlike PPTP, the L2TP/IPSec combination works in IP, IPX, and SAN networks. PPTP works only in IP networks.

16. Which of the following is the best method to protect a user from email spam? Select two answers.

 □ A. Use encryption.

 □ B. Educate users.

 □ C. Use authentication.

 □ D. Use spam filters.

 □ E. Restrict SMTP relay.

Answers B and D are correct. The best protection against email spam is to educate users. Some messaging applications allow you to configure spam filters to stop messages that look like spam at the server itself and protect individual mailboxes.

17. Identify the 802.1x method that can be used for mutual authentication of the supplicant and the authenticator.

   ❍ A. EAP-TLS

   ❍ B. EAP-MD5

   ❍ C. EAP-SHA1

   ❍ D. EAP-RC4

   Answer A is correct. EAP-TLS (Extensible Authentication Protocol-Transport Layer Security) provides mutual authentication. MD5 and SHA1 are hashing algorithms, while RC4 is a stream cipher symmetric algorithm.

18. Which of the following authentication methods are defined by the 802.11 wireless standard?

   ❍ A. Open and shared key

   ❍ B. Shared key and private key

   ❍ C. Private key and secret key

   ❍ D. Open key and closed key

   Answer A is correct. The 802.11 wireless standard defines two authentication methods: open authentication and shared key authentication. The shared key authentication is also known as private key or secret key authentication.

19. Which of the following is the intent of conducting site surveys?

   ❍ A. To determine all wireless networks in the neighborhood

   ❍ B. To measure the frequency range used by the network

   ❍ C. To determine the speed of the wireless network

   ❍ D. To determine the extent to which the wireless network goes beyond the building

   Answer D is correct. Site surveys help determine the extent to which the wireless network extends beyond the physical boundary of the building.

20. Which of the following is considered the best place for placing wireless access points?

   ❍ A. Away from server rooms

   ❍ B. Inside server rooms

   ❍ C. Away from walls and windows

   ❍ D. B and C

   Answer C is correct. Wireless access points should be kept away from walls and windows of the building. This helps prevent the wireless signals from extending beyond the physical boundaries of the building.

21. You are configuring a firewall to allow only secure HTTP traffic to enter the network. Which of the following ports do you need to open on the firewall?

○ A. 22

○ B. 25

○ C. 80

○ D. 443

Answer D is correct. Secure Hypertext Transfer Protocol (HTTPS) uses TCP/IP port 443, and HTTP uses port 80. If you wish to allow only HTTP traffic, you will need to open port 80 on the firewall and close port 443.

22. You were conducting a scan of all active servers in the network and found that several servers are listening on port 80. What should you do with these servers?

○ A. Identify rogue HTTP servers and disable them.

○ B. Identify rogue DNS servers and disable them.

○ C. Identify rogue DHCP servers and disable them.

○ D. Identify rogue LDAP servers and disable them.

Answer A is correct. Port 80 is used by HTTP service. If a number of servers are listening on port 80, this means that HTTP is configured on these servers. You need to identify the servers that are not supposed to host HTTP service and disable them.

23. You receive an email from a software vendor letting you know that a new security update is available on its web site for its messaging application. Which of the following actions should you take immediately? Select two answers.

□ A. Download and install the update immediately on all email servers.

□ B. Immediately inform your manager that you need to install the update.

□ C. Download the update and read the accompanying instructions.

□ D. Install the update on a nonproduction email server and test it for bugs.

Answers C and D are correct. Updates, hotfixes, and service packs should be tested on nonproduction servers before they are installed on production servers. Sometimes the updates contain bugs that might leave the production servers inaccessible or open to external threats.

24. A large number of employees burn CDs on their desktops and take them home. You suspect that some employees might be burning CDs with confidential corporate data as well. What should you do?

○ A. Remove CD burners from all desktops.

○ B. Ask management to design a policy restricting burning of CDs on company computers.

○ C. Email all employees that this is not a good practice.

○ D. Ask the security department to conduct physical checks of all employees when they leave.

Answer B is correct. The best way to protect confidential data, and to prevent data theft and other illegal activities (such as burning of music CDs on company computers) is to design a security policy that restricts all such activities. The management should make sure that the policy is enforced for all employees.

25. Most of the employees in the marketing department have laptop computers. They take their laptops with them when traveling. These laptops have confidential marketing information that needs to be protected. You are afraid that if any of the laptops are stolen, the confidential data can be leaked and used against the organization. Which of the following is the best method to protect data stored on laptops?

    ○ A. Encrypt the data.

    ○ B. Compress the data.

    ○ C. Make data read-only.

    ○ D. Archive the data.

    Answer A is correct. The data stored on laptop computers should be encrypted so that if the laptop is stolen, the data is secure from being read and used by a third person.

26. The organization you work for has strict security requirements for all computer users. User authentication is performed using digital keys. The organization wants users to authenticate using 128-bit keys. Which of the following devices would you recommend to provide the best security for the private keys?

    ○ A. Floppy disks

    ○ B. Smart cards

    ○ C. Compact disks

    ○ D. Memory cards

    Answer B is correct. Smart cards are considered to be the best devices to store 128-bit private keys.

27. Your company has merged with another and you are required to design a web site that would allow employees of both companies to access resources on each other's network resources. What kind of network would you design?

    □ A. DMZ

    □ B. VLAN

    □ C. Extranet

    □ D. Intranet

    Answers C and D are both correct. You will need to design an extranet or an intranet. These are two types of virtual private networks that allow two or more partner companies to share and exchange network resources.

28. In which area of the network should you place private web servers, domain controllers, and database servers?

    ○ A. Intranet

    ○ B. Extranet

    ○ C. VLAN

    ○ D. DMZ

Answer A is correct. All critical servers that are to be used internally should be placed in the intranet. Servers that should be accessible from outside the organization should be placed inside the DMZ.

29. Your network has several critical servers that are accessible from the Internet. The servers have been the targets of attackers in the past. You want to keep the attackers away from your actual network but still want to monitor their activities. How can you accomplish this?

    ○ A. Create a honeypot for the attacker.

    ○ B. Block all internal and external access to the servers.

    ○ C. Block all internal access to the servers.

    ○ D. Block all external access to the servers.

    Answer A is correct. In order to monitor the activities of the attackers and still keep the servers secure from them, you need to create a honeypot. A honeypot is a server that appears to be a critical server, but it actually is not. This server contains dummy information that seems interesting to the attacker.

30. Which of the following describes the function of a VLAN?

    ○ A. A VLAN is used to create a DMZ to secure critical servers.

    ○ B. A VLAN can be used to create a tunnel through the Internet.

    ○ C. A VLAN is used to create network segments for enhanced security.

    ○ D. A VLAN is used to hide internal addressing schemes from the Internet.

    Answer C is correct. A Virtual Local Area Network (VLAN) creates separate broadcast domains in an internetwork. It is a logical grouping of network devices, which is based on functions rather than physical location. It adds another layer of security for the network.

31. You have installed an intrusion detection system on one of the production servers to monitor malicious activities of applications and users only on that server. What kind of IDS is this?

    ○ A. Active IDS

    ○ B. Passive IDS

    ○ C. Network-based IDS

    ○ D. Host-based IDS

    Answer D is correct. An IDS installed on a single computer is known as host-based IDS. This IDS monitors activities on the computer on which it is installed only.

32. You have detected an attack on one of your organization's web servers running Microsoft's Internet Information Server 6.0 (IIS 6.0). What should you do immediately? Select two answers.

    □ A. Call Microsoft Help and Support.

    □ B. Call the police.

    □ C. Preserve all evidence.

    □ D. Disable IIS 6.0.

    □ E. Shut down the server.

Answers B and C are correct. An attack on the web server of an organization is considered a criminal activity. Depending on the severity of the incident, if the situation calls for it, you must call the police and preserve all evidence that might be helpful in investigations.

33. You have just been informed that one of your web servers has stopped responding due to an attack. When you check the event logs on the server, you don't find any clues related to the attack. Which of the following parts of server hardening likely has not been implemented?

    ○ A. Auditing

    ○ B. Authorization

    ○ C. Access control

    ○ D. All of above

    Answer A is correct. Auditing has not been configured on the server. This is the reason that no activity related to the attack has been recorded in the event logs.

34. You have been asked to design mechanisms for creating a secure computing environment. Each user and computer must be authenticated and all network traffic must be encrypted. The first thing you need to look at is the strength of an encryption algorithm. Which of the following components directly affect the strength of an encryption algorithm? Select two answers.

    □ A. The number of data bits

    □ B. The experience of the hacker

    □ C. The size of the encryption key

    □ D. The security of the private key

    □ E. The software available to the hacker

    Answers C and D are correct. The size of the encryption key and its security are two main factors that directly affect the strength of the encryption algorithm. The longer the size of the key, the more time it takes for the hacker to crack it. Similarly, keys must be stored securely to prevent their compromise.

35. Which of the following is the main weakness of symmetric encryption algorithms?

    ○ A. The size of the keys

    ○ B. The distribution of keys

    ○ C. The vulnerability to attacks

    ○ D. Processing capabilities

    Answer B is correct. The main weakness of symmetric encryption algorithms is distribution of the private key. Since the same key is used for both encryption and decryption, sending the key to the other party securely is the main problem.

36. Which of the following are properties of a one-way hashing algorithm? Select two answers.

- ❑ A. It is not possible to factorize it.
- ❑ B. It can produce the same output from any two inputs.
- ❑ C. It is not possible to reverse the function.
- ❑ D. It is difficult to get the input if output is given.
- ❑ E. It can be used with symmetric algorithms.

Answers C and D are correct. One-way hashing algorithms are not reversible. It is not possible to determine the input even if the output is given and the algorithm is known.

37. A digital certificate issued to an organization for conducting on-line business is about to expire. What should the organization do in order to continue using digital certificates?

- ❍ A. Renew the certificate.
- ❍ B. Get a new certificate.
- ❍ C. Revoke the certificate.
- ❍ D. Destroy the certificate.

Answer A is correct. The organization must renew the certificate in order to use it before it expires. The issuing CA should be contacted for the purpose. The organization cannot use an expired certificate to conduct online business.

38. Which of the following is used to allow users to access resources on different servers in the domain when they log on to their computers?

- ❍ A. Centralized authentication
- ❍ B. Centralized authorization
- ❍ C. Single sign-on
- ❍ D. Digital certificates

Answer C is correct. The term *single sign-on* refers to the ability of a user to access resources distributed on several servers in a domain when she logs onto the domain from her desktop. She doesn't need to log on to every server, which prevents mistakes made during typing of usernames and passwords.

39. While discussing the disaster recovery plan for the company's network servers, your manager has asked you to suggest a backup method that would take the minimum time for the restoration of data. Which of the following backup types would you suggest?

- ❍ A. Full backup everyday
- ❍ B. Full backup and incremental backup
- ❍ C. Full backup and differential backup
- ❍ D. Incremental and differential backup

Answer A is correct. The full backup takes longer to complete but is the fastest when data needs to be restored in case of a disaster. When you are taking full backup everyday, if a disaster strikes, you will need only the previous day's full backup tape to fully restore the data.

40. Your manager has asked you to suggest whether access to secure server rooms should be controlled using biometric devices. He has asked you to specify the information that would be needed to access the room when these devices are installed. Which of the following pieces of information could the biometric devices require?

 ❍ A. Username and password

 ❍ B. Username and PIN number

 ❍ C. Facial characteristics and password

 ❍ D. Fingerprints, voice patterns, and retina scans

 Answer D is correct. Biometric devices rely on unique human characteristics to identify a person. Fingerprints, voice patterns, and retina scans vary from person to person and are used to enforce strong security.

Index

We’d like to hear your suggestions for improving our indexes. Send email to *index@oreilly.com*.

About the Author

Pawan K. Bhardwaj is an independent technical trainer and author. Pawan is MCSE, MCT, Security+, Network+, I-Net+, and A+ certified. He was one of the first 100 people in India to attain MCSE certification in 1997. He teaches Windows Administration and Networking classes, and provides consultancy to training institutions. He has authored or contributed to over 12 certification books, including *MCSE Core Elective Exams in a Nutshell* (O'Reilly). Pawan was also the technical reviewer for the bestselling titles *MCSE 2003 Core Required Exams in a Nutshell* and *MCSE Windows 2000 Exams in a Nutshell* (both published by O'Reilly).

Colophon

The animal on the cover of *A+, Network+, Security+ Exams in a Nutshell* is a Goliath beetle. This is the largest type of beetle that exists, and it actually is one of the largest insects in the world. They are native to the tropics of Africa and feed off the moist, rotting wood in the rainforests located there.

Like all beetles, the Goliath beetle begins life as an egg, hatching into a larva. The larva mainly lives off dead trees and plants, and so it is considered very good for the environment, helping to clean up waste. After many months of eating and growing, the larva builds itself a cocoon, from which it emerges completely transformed into the Goliath beetle. Once a beetle, it doesn't have too long to live. Its primary focus in this stage is reproduction.

These beetles have colorful markings on their shells, although they are mostly black and white. They also share some other features with all beetles, such as the *elytra*, which are the hard, shell-like wings that form a protective cover over a second set of wings—the actual wings the beetle uses to fly. A male Goliath beetle has a Y-shaped horn on the top of its head (used for grappling with other beetles), while the female has no horn. These insects also have a set of claws on each leg, which are incredibly powerful. These claws, known as *tarsi*, allow the beetle to cling firmly to tree bark.

The cover image is from Cassell's *Natural History*. The cover font is Adobe ITC Garamond. The text font is Linotype Birka; the heading font is Adobe Myriad Condensed; and the code font is LucasFont's TheSans Mono Condensed.

A+/Certification

A+, NETWORK+, SECURITY+ EXAMS IN A NUTSHELL

If you're preparing for the new CompTIA 2006 certification in A+ or the current Network+ and Security+ certifications, you'll find this book invaluable. It provides all the information you need to get ready for these exams, including the four new A+ exams: the required Essentials exam and three elective exams that pertain to your particular area of specialization.

As with other O'Reilly Nutshell books for certification exams, *A+, Network+, Security + in a Nutshell* follows a proven style and approach. It reviews all of the topics needed to master each exam in a remarkably concise format, with required knowledge condensed to the core. Instead of requiring you to plow through 500 to 700 pages to prepare for each exam, this book covers each one in approximately 150 pages. And, because the objectives for the three elective A+ exams are redundant, the book covers them in one section.

The exams covered include:

- A+ Essentials: Required for A+ 2006 certification
- EXAM 220-602: For the A+ IT Technician specialization
- EXAM 220-603: For the A+ Remote Support Technician specialization
- EXAM 220-604: For the A+ IT Depot specialization
- EXAM N10-003: For Network+ Certification
- EXAM SYO-101: For Security+ Certification

Each exam is covered in three parts: Exam Overview, Study Guide, and Prep and Practice. Plenty of detailed tables and screen shots are included, along with study notes and practice questions. Once you have completed the exams successfully, you will find this all-in-one book to be an important reference to core administration and security skills.

Pawan K. Bhardwaj is an independent technical trainer and author who holds MCSE, MCSA, Security+, Network+, I-Net+, and A+ certifications. He teaches Windows Administration and Networking classes, and provides consulting to training institutions. An author and contributor to 14 books, Pawan is the author of O'Reilly's *MCSE Core Elective Exams in a Nutshell*, and coauthor of *MCSA on Windows Server 2003 Core Exams in a Nutshell*.

O'REILLY® www.oreilly.com

US $54.99 CAN $71.99
ISBN-10: 0-596-52824-8
ISBN-13: 978-0-596-52824-9

55499

9 780596 528249

Safari® BOOKS ONLINE ENABLED

Includes FREE 45-Day Online Edition