



**Deluxe
Edition**

Network+

FT MEADE
MRC

MRC

TK 5105
.5
.N46673
2005
Copy 1

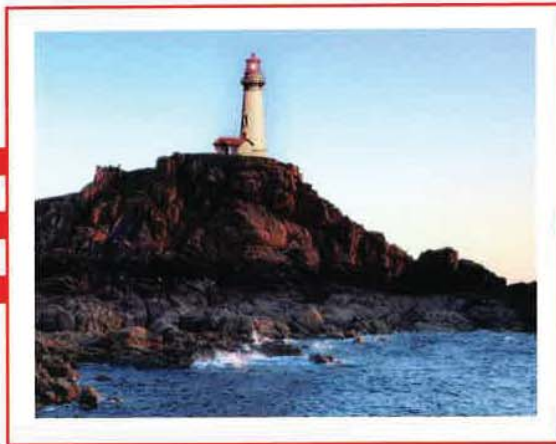
**NEW DELUXE EDITION FOR 2005 EXAM
INCLUDES VIRTUAL LAB SOFTWARE**

Network+™



**STUDY GUIDE
Deluxe Edition**

**Second Edition
Exam N10-003**



**David Groth
Toby Skandier
Todd Lammle
William Tedder**



**Includes Two CDs—
Network+ Virtual Lab
and Advanced Test Prep Tools**

- Network and Operating System Simulation Software—A US \$100 Retail Value! Includes 24 Hands-on and 31 Review Labs
- Test Engine with Assessment Test, Chapter Review Questions, and Four Bonus Exams!
- Electronic Flashcards for PCs, Pocket PCs, Palm Handhelds, and the Entire Book in PDF



**Second CD Includes Advanced Network+
Virtual Lab Simulation Software**



**Roku Exhibit 1038
Roku Inc. v. Universal Elecs. Inc.
IPR2022-01289
Page 00001**

Network+

Study Guide, Deluxe Edition

If you're serious about getting your Network+ certification and advancing your career in the field of networking, then here's the book you need. Revised for the new version of the Network+ exam, N10-003, this Deluxe Edition of the best-selling *Network+ Study Guide* was developed to meet the exacting requirements of today's IT certification candidates. In addition to the engaging and accessible instructional style that has made author David Groth a reader favorite for years, this updated edition provides:

- In-depth coverage of every Network+ exam objective
- Practical instruction and insights drawn from real-world experience
- Leading-edge exam preparation software, including the *Network+ Virtual Lab*, as well as Sybex's custom test engine, electronic flashcards, and the entire book in PDF

Authoritative coverage of all exam objectives, including:

- Media and Topologies
- Network Implementation
- Protocols and Standards
- Network Support

About the Authors **David Groth**, Network+, MCSE, CNI, is a full-time author and consultant. He is the author of Sybex's best-selling *A+ Complete Study Guide*. **Toby Skandier**, Network+, i-Net+, Server+, is in technical education development and delivery for Sprint Corporation. **Todd Lammle**, CCNA, CCNP, has over 20 years of experience working with various LANs and WANs, and has been working on Cisco router networks since 1986. He is CEO and chief scientist of RouterSim, LLC., and president of GlobalNet Training, Inc. **William Tedder**, president of RouterSim, LLC., is the person responsible for the intuitive, easy-to-use, and effective interface of the *Network+ Virtual Lab*.



This book has been reviewed and approved as CompTIA Authorized Quality Curriculum (CAQC). Students derive a number of important study advantages with CAQC materials, including coverage of all exam objectives, implementation of important instructional design principles, and instructional reviews that help students assess their learning comprehension and readiness for the exam.



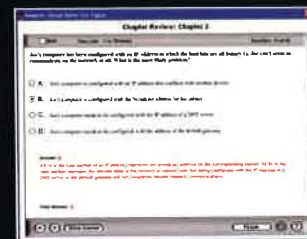
Visit www.sybex.com for your CompTIA certification needs.



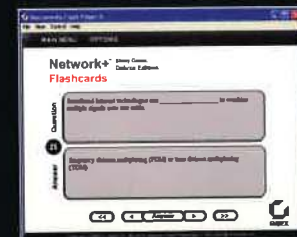
Featured on the CDs



NETWORK+ VIRTUAL LAB: Get hands-on practice in a simulated network and operating system environment, including Windows XP and 2000, Mac OS X, and Mandrake Linux. Also allows you to configure networks using Cisco 1900 series switches and 2501 series routers.



SYBEX TEST ENGINE: Test your knowledge with advanced testing software. Includes assessment test, chapter review questions, and four bonus exams.



ELECTRONIC FLASHCARDS: Reinforce your understanding with flashcards that can run off your PC, Pocket PC, or Palm handheld.

Also on the CD, you'll find the entire book in searchable and printable PDF.

COMPUTER BOOK SHELF CATEGORY
Certification/Networking

US\$89.99 CAN\$125.95 UK£59.99

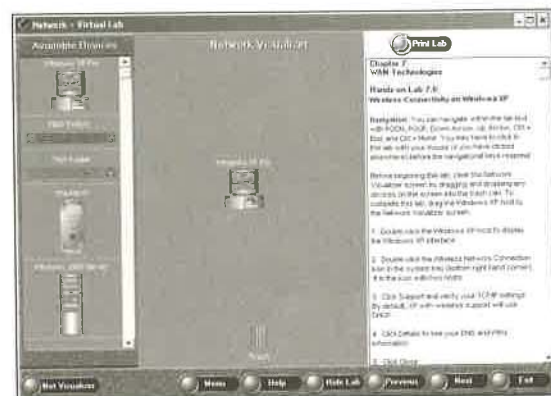
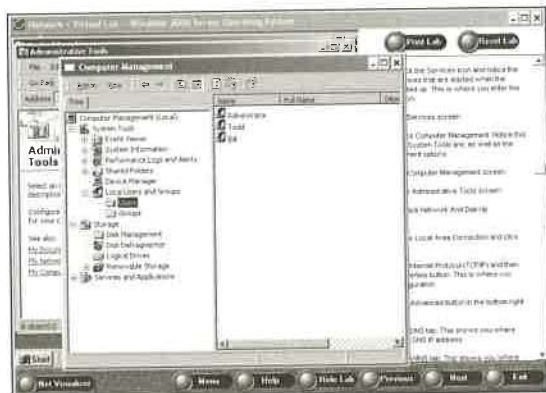
ISBN 0-7821-4416-0



Get the Hands-on Experience you need to

Create Virtual Network with Drag-and-Drop Hardware Devices!

- The Network Visualizer allows you to create your very own virtual network by dragging network devices and connecting them together.
- You'll work with routers, switches, and server and client hardware configured with the server and desktop operating systems you need to prepare for the exam.

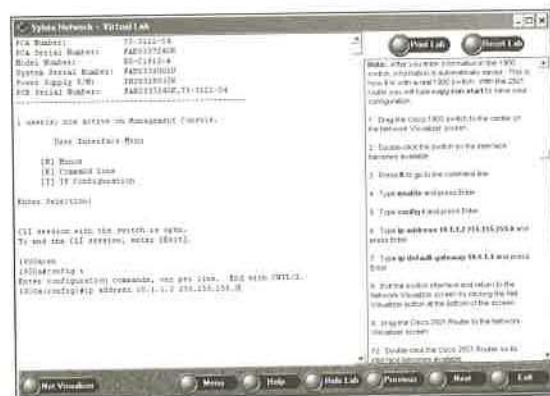


Access Simulated Operating System Interfaces and Features!

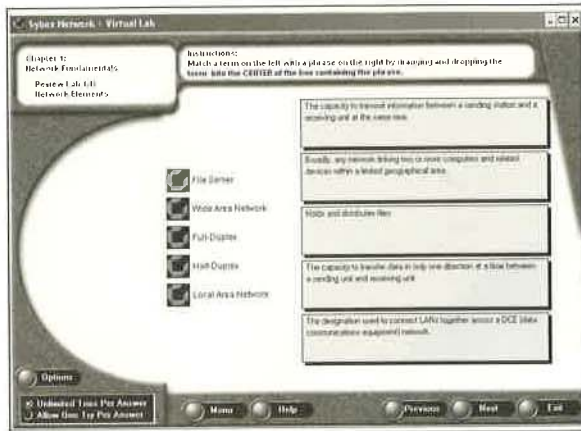
- After you create a virtual network, you can access a simulated server and desktop operating system interfaces and practice configuration and management tasks.

Hone your Skills with Dozens of Hands-on Labs!

- Hands-on labs provide clear instructions to guide you through critical networking installation, configuration, and management tasks you'll encounter both on the exam and in the real world.
- Review labs offer you an additional study tool to help reinforce your knowledge of key exam topics.



pass the Network+ Exam with this Virtual Lab!

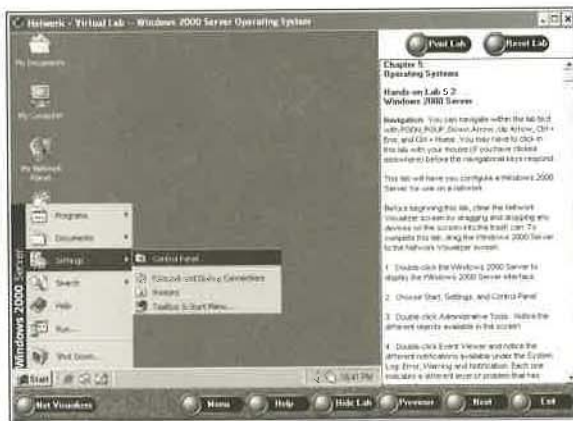


When you're done practicing with the hundreds of sample questions in this book, reinforce your knowledge with Practice Labs and more Review Questions!

- Use any of the dozens of drag-and-drop and multiple choice questions.
- You can be sure that this Virtual Lab will expose you to the level of difficulty found on the actual Network+ exam.

Master the subjects you need to approach the Network+ Exam with confidence!

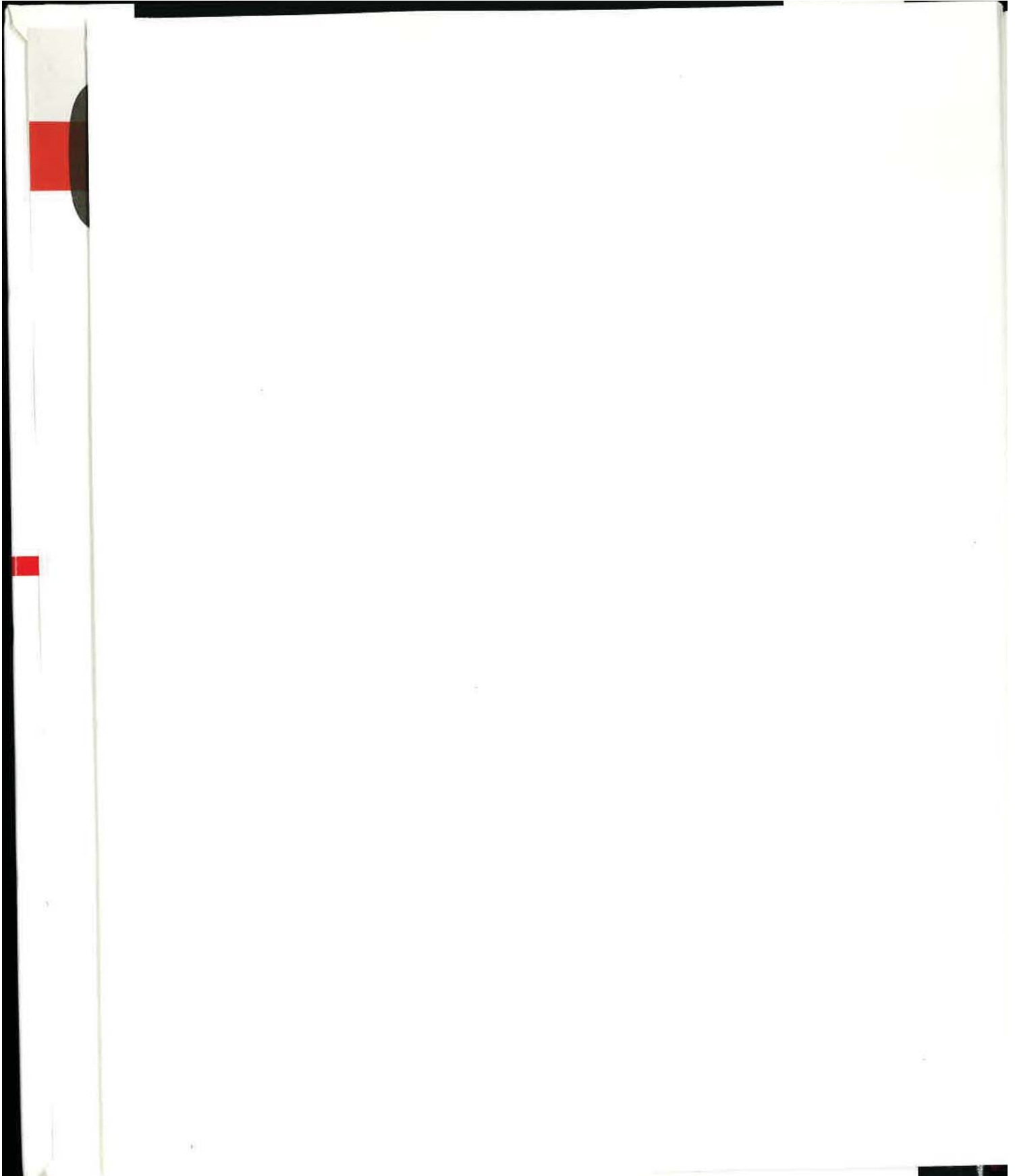
- This powerful certification tool will give you the practical experience you need.



Created by Todd Lammle and William Tedder—Leaders in the industry!

- Todd Lammle, author of the best-selling book *CCNA: Cisco Certified Network Associate Study Guide*, is one of the most foremost experts on LAN/WAN installation, configuration, and administration.
- William Tedder, president of Interactive Designs Group Inc., is the person responsible for the intuitive, easy-to-use, and effective interface of the CCNP Virtual Lab.









Network+ Study Guide

Exam N10-003

OBJECTIVE	CHAPTER
DOMAIN 1.0 - MEDIA AND TOPOLOGIES	
1.1 Recognize the following logical or physical network topologies given a diagram, schematic or description: Star, Bus, Mesh, Ring	1
1.2 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 (Carrier Sense Multiple Access/Collision Avoidance) and CSMA / CD (Carrier Sense Multiple Access / Collision Detection)), Topology, Media	1, 2
1.3 Specify the characteristics (For example: 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; 10GBASE-SR, 10GBASE-LR and 10GBASE-ER	1
1.4 Recognize the following media connectors and describe their uses: RJ-11 (Registered Jack), RJ-45 (Registered Jack), F-Type, ST (Straight Tip), SC (Subscriber Connector or Standard Connector), IEEE 1394 (FireWire), Fiber LC (Local Connector), MT-RJ (Mechanical Transfer Registered Jack), USB (Universal Serial Bus)	1
1.5 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) optic cable; MMF (Multimode Fiber) optic cable	1
1.6 Identify the purposes, features and functions of the following network components: Hubs, Switches, Bridges, Routers, 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	1
1.7 Specify the general characteristics (For example: carrier speed, frequency, transmission type and topology) of the following wireless technologies: 802.11 (Frequency hopping spread spectrum), 802.11x (Direct sequence spread spectrum), Infrared, Bluetooth	6
1.8 Identify factors which affect the range and speed of wireless service (For example: interference, antenna type and environmental factors).	6
DOMAIN 2.0 - PROTOCOLS AND STANDARDS	
2.1 Identify a MAC (Media Access Control) address and its parts.	2
2.2 Identify the seven layers of the OSI (Open Systems Interconnect) model and their functions.	2
2.3 Identify the OSI (Open Systems Interconnect) layers at which the following network components operate: Hubs, Switches, Bridges, Routers, NICs (Network Interface Card), WAPs (Wireless Access Point)	2



OBJECTIVE	CHAPTER
2.4 Differentiate between the following network protocols in terms of routing, addressing schemes, interoperability and naming conventions: IPX / SPX (Internetwork Packet Exchange / Sequence Packet Exchange), NetBEUI (Network Basic Input / Output System Extended User Interface), AppleTalk / AppleTalk over IP (Internet Protocol), TCP / IP (Transmission Control Protocol / Internet Protocol)	2, 3
2.5 Identify the components and structure of IP (Internet Protocol) addresses (IPv4, IPv6) and the required setting for connections across the Internet.	3
2.6 Identify classful IP (Internet Protocol) ranges and their subnet masks (For example: Class A, B and C).	3
2.7 Identify the purpose of subnetting.	3
2.8 Identify the differences between private and public network addressing schemes.	3
2.9 Identify and differentiate between the following IP (Internet Protocol) addressing methods: Static, Dynamic, Self-assigned (APIPA (Automatic Private Internet Protocol Addressing))	3
2.10 Define the purpose, function and use of the following protocols used in the TCP / IP (Transmission Control Protocol / Internet Protocol) 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)	3
2.11 Define the function of TCP / UDP (Transmission Control Protocol / User Datagram Protocol) ports.	3
2.12 Identify the well-known ports associated with the following commonly used services and protocols: 20 FTP (File Transfer Protocol), 21 FTP (File Transfer Protocol), 22 SSH (Secure Shell), 23 Telnet, 25 SMTP (Simple Mail Transfer Protocol), 53 DNS (Domain Name Service), 69 TFTP (Trivial File Transfer Protocol), 80 HTTP (Hypertext Transfer Protocol), 110 POP3 (Post Office Protocol version 3), 119 NNTP (Network News Transport Protocol), 123 NTP (Network Time Protocol), 143 IMAP4 (Internet Message Access Protocol version 4), 443 HTTPS (Hypertext Transfer Protocol Secure)	3
2.13 Identify the purpose of network services and protocols (For example: DNS (Domain Name Service), NAT (Network Address Translation), ICS (Internet Connection Sharing), WINS (Windows Internet Name Service), SNMP (Simple Network Management Protocol), NFS (Network File System), Zeroconf (Zero configuration), SMB (Server Message Block), AFP (Apple File Protocol), LPD (Line Printer Daemon) and Samba).	3



Exam objectives are subject to change at any time without prior notice and at CompTIA's sole discretion. Please visit CompTIA's Web site (www.comptia.org) for the most current listing of exam objectives.



OBJECTIVE	CHAPTER
2.14 Identify the basic characteristics (For example: speed, capacity and media) of the following WAN (Wide Area Networks) technologies: Packet switching, Circuit switching, ISDN (Integrated Services Digital Network), FDDI (Fiber Distributed Data Interface), T1 (T Carrier level 1) / E1 / J1, T3 (T Carrier level 3) / E3 / J3, OCx (Optical Carrier), X.25	7
2.15 Identify the basic characteristics of the following internet access technologies: xDSL (Digital Subscriber Line), Broadband Cable (Cable modem), POTS / PSTN (Plain Old Telephone Service / Public Switched Telephone Network), Satellite, Wireless	7
2.16 Define the function of the following remote access protocols and services: RAS (Remote Access Service), PPP (Point-to-Point Protocol), SLIP (Serial Line Internet Protocol), PPPoE (Point-to-Point Protocol over Ethernet), PPTP (Point-to-Point Tunneling Protocol), VPN (Virtual Private Network), RDP (Remote Desktop Protocol)	7
2.17 Identify the following security protocols and describe their purpose and function: IPSec (Internet Protocol Security), L2TP (Layer 2 Tunneling Protocol), SSL (Secure Sockets Layer), WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access), 802.1x	8
2.18 Identify authentication protocols (For example: CHAP (Challenge Handshake Authentication Protocol), MS-CHAP (Microsoft Challenge Handshake Authentication Protocol), PAP (Password Authentication Protocol), RADIUS (Remote Authentication Dial-In User Service), Kerberos and EAP (Extensible Authentication Protocol)).	8
DOMAIN 3.0 - NETWORK IMPLEMENTATION	
3.1 Identify the basic capabilities (For example: 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 (Internet Protocol)	5
3.2 Identify the basic capabilities needed for client workstations to connect to and use network resources (For example: media, network protocols and peer and server services).	1, 8
3.3 Identify the appropriate tool for a given wiring task (For example: wire crimper, media tester / certifier, punch down tool or tone generator).	6
3.4 Given a remote connectivity scenario comprised of a protocol, an authentication scheme, and physical connectivity, configure the connection. Includes connection to the following servers: UNIX / Linux / MAC OS X Server, Netware, Windows, Appleshare IP (Internet Protocol)	7
3.5 Identify the purpose, benefits and characteristics of using a firewall.	8
3.6 Identify the purpose, benefits and characteristics of using a proxy service.	8
3.7 Given a connectivity scenario, determine the impact on network functionality of a particular security implementation (For example: port blocking / filtering, authentication and encryption).	8
3.8 Identify the main characteristics of VLANs (Virtual Local Area Networks).	3



OBJECTIVE	CHAPTER
3.9 Identify the main characteristics and purpose of extranets and intranets.	3
3.10 Identify the purpose, benefits and characteristics of using antivirus software.	9
3.11 Identify the purpose and characteristics of fault tolerance: Power, Link redundancy, Storage, Services	9
3.12 Identify the purpose and characteristics of disaster recovery: Backup / restore, Offsite storage, Hot and cold spares, Hot, warm and cold sites	9
DOMAIN 4.0 - NETWORK SUPPORT	
4.1 Given a troubleshooting scenario, select the appropriate network utility from the following: Tracert / traceroute, ping, arp, netstat, nbtstat, ipconfig / ifconfig, winipcfg, nslookup / dig	4
4.2 Given output from a network diagnostic utility (For example: those utilities listed in objective 4.1), identify the utility and interpret the output.	4
4.3 Given a network scenario, interpret visual indicators (For example: link LEDs (Light Emitting Diode) and collision LEDs (Light Emitting Diode)) to determine the nature of a stated problem.	10
4.4 Given a troubleshooting scenario involving a client accessing remote network services, identify the cause of the problem (For example: file services, print services, authentication failure, protocol configuration, physical connectivity and SOHO (Small Office / Home Office) router).	10
4.5 Given a troubleshooting scenario between a client and the following server environments, identify the cause of a stated problem: UNIX / Linux / Mac OS X Server, Netware, Windows, Appleshare IP (Internet Protocol)	10
4.6 Given a scenario, determine the impact of modifying, adding or removing network services (For example: DHCP (Dynamic Host Configuration Protocol), DNS (Domain Name Service) and WINS (Windows Internet Name Service)) for network resources and users.	10
4.7 Given a troubleshooting scenario involving a network with a particular physical topology (For example: bus, star, mesh or ring) and including a network diagram, identify the network area affected and the cause of the stated failure.	10
4.8 Given a network troubleshooting scenario involving an infrastructure (For example: wired or wireless) problem, identify the cause of a stated problem (For example: bad media, interference, network hardware or environment).	10
4.9 Given a network problem scenario, select an appropriate course of action based on a logical troubleshooting strategy. This strategy can include the following steps: 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 effects; 6. Test the result; 7. Identify the results and effects of the solution; 8. Document the solution and process	10



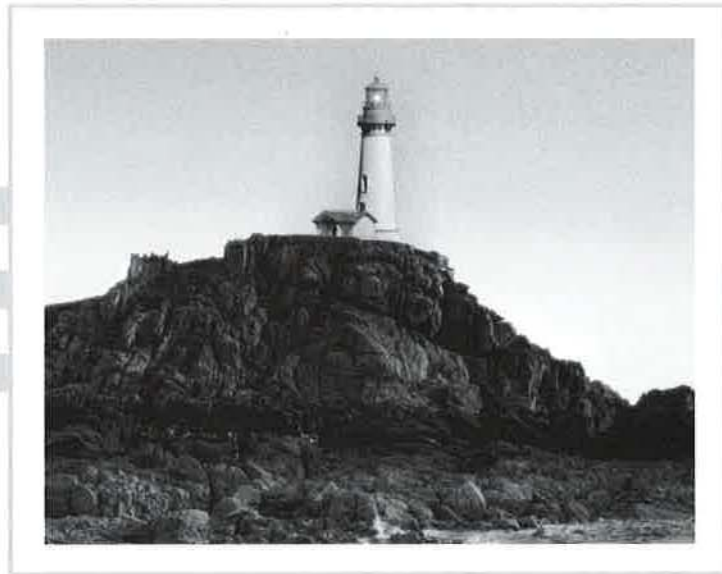
Exam objectives are subject to change at any time without prior notice and at CompTIA's sole discretion. Please visit CompTIA's Web site (www.comptia.org) for the most current listing of exam objectives.

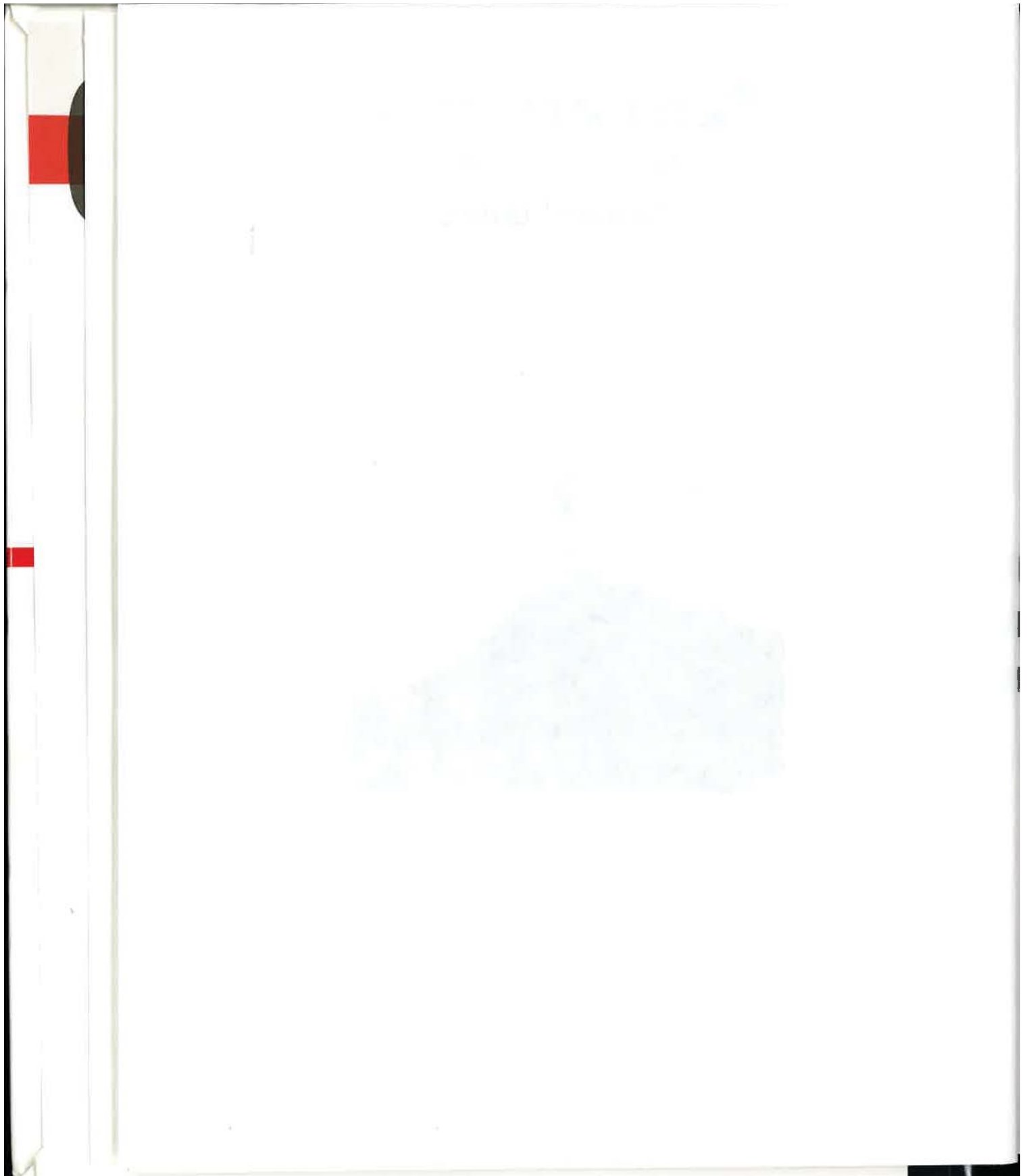


Network+

Study Guide

Deluxe Edition





Network+TM

Study Guide

Deluxe Edition



David Groth
Toby Skandier
Todd Lammle
William Tedder

San Francisco • London



Publisher: Neil Edde
Acquisitions Editor: Jeff Kellum
Developmental Editor: Jeff Kellum
Production Editor: Lori Newman
Technical Editor: James Kelly
Copy Editor: Judy Flynn
Compositor: Jeffrey Wilson, Happenstance Type-O-Rama
Graphic Illustrator: Happenstance Type-O-Rama
CD Coordinator: Dan Mummert
CD Technician: Kevin Ly
Proofreaders: Jim Brook, Candace English, Nancy Riddiough
Indexer: Ted Laux
Book Designer: Bill Gibson, Judy Fung
Cover Designer: Archer Design
Cover Photographer: Photodisc and Victor Arre



Copyright © 2005 SYBEX Inc., 1151 Marina Village Parkway, Alameda, CA 94501. World rights reserved. No part of this publication may be stored in a retrieval system, transmitted, or reproduced in any way, including but not limited to photocopy, photograph, magnetic, or other record, without the prior agreement and written permission of the publisher.

First edition copyright © 1999 SYBEX Inc.

Second edition copyright © 2001 SYBEX Inc.

Third edition copyright © 2002 SYBEX Inc.

Library of Congress Card Number: 2005920773

ISBN: 0-7821-4416-0

SYBEX and the SYBEX logo are either registered trademarks or trademarks of SYBEX Inc. in the United States and/or other countries.

Screen reproductions produced with FullShot 99. FullShot 99 © 1991–1999 Inbit Incorporated. All rights reserved.

FullShot is a trademark of Inbit Incorporated.

Screen reproductions of Mac OS X courtesy of Apple Computer, Inc.

The CD interface was created using Macromedia Director, COPYRIGHT 1994, 1997–1999 Macromedia Inc. For more information on Macromedia and Macromedia Director, visit <http://www.macromedia.com>.

Internet screen shot(s) using Microsoft Internet Explorer 6 reprinted by permission from Microsoft Corporation.

Sybex is an independent entity from CompTIA and is not affiliated with CompTIA in any manner. Neither CompTIA nor Sybex warrants that use of this publication will ensure passing the relevant exam. Network+ is either a registered trademark or trademark of CompTIA in the United States and/or other countries.

TRADEMARKS: SYBEX has attempted throughout this book to distinguish proprietary trademarks from descriptive terms by following the capitalization style used by the manufacturer.

The author and publisher have made their best efforts to prepare this book, and the content is based upon final release software whenever possible. Portions of the manuscript may be based upon pre-release versions supplied by software manufacturer(s). The author and the publisher make no representation or warranties of any kind with regard to the completeness or accuracy of the contents herein and accept no liability of any kind including but not limited to performance, merchantability, fitness for any particular purpose, or any losses or damages of any kind caused or alleged to be caused directly or indirectly from this book.

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1



To Our Valued Readers:

Thank you for looking to Sybex for your Network+ exam prep needs. We at Sybex are proud of our reputation for providing certification candidates with the practical knowledge and skills needed to succeed in the highly competitive IT marketplace. Certification candidates have come to rely on Sybex for accurate and accessible instruction on today's crucial technologies.

Sybex serves as a participant member of CompTIA's Network+ Advisory Committee, and just as CompTIA is committed to establishing measurable standards for certifying individuals who will support today's complex network systems, Sybex is committed to providing those individuals with the skills needed to meet those standards.

The author and editors have worked hard to ensure that the Deluxe edition of the Network+ Study Guide you hold in your hands is comprehensive, in-depth, and pedagogically sound. With the addition of the Network+ Virtual Lab software on the second CD, we're confident that this book will exceed the demanding standards of the certification marketplace and help you, the Network+ certification candidate, succeed in your endeavors.

As always, your feedback is important to us. If you believe you've identified an error in the book, please send a detailed e-mail to support@sybex.com. And if you have general comments or suggestions, feel free to drop me a line directly at nedde@sybex.com. At Sybex we're continually striving to meet the needs of individuals preparing for certification exams.

Good luck in pursuit of your Network+ certification!

Neil Edde
Publisher—Certification
Sybex, Inc.

Software License Agreement: Terms and Conditions

The media and/or any online materials accompanying this book that are available now or in the future contain programs and/or text files (the "Software") to be used in connection with the book. SYBEX hereby grants to you a license to use the Software, subject to the terms that follow. Your purchase, acceptance, or use of the Software will constitute your acceptance of such terms. The Software compilation is the property of SYBEX unless otherwise indicated and is protected by copyright to SYBEX or other copyright owner(s) as indicated in the media files (the "Owner(s)"). You are hereby granted a single-user license to use the Software for your personal, noncommercial use only. You may not reproduce, sell, distribute, publish, circulate, or commercially exploit the Software, or any portion thereof, without the written consent of SYBEX and the specific copyright owner(s) of any component software included on this media.

In the event that the Software or components include specific license requirements or end-user agreements, statements of condition, disclaimers, limitations or warranties ("End-User License"), those End-User Licenses supersede the terms and conditions herein as to that particular Software component. Your purchase, acceptance, or use of the Software will constitute your acceptance of such End-User Licenses.

By purchase, use or acceptance of the Software you further agree to comply with all export laws and regulations of the United States as such laws and regulations may exist from time to time.

Software Support

Components of the supplemental Software and any offers associated with them may be supported by the specific Owner(s) of that material, but they are not supported by SYBEX. Information regarding any available support may be obtained from the Owner(s) using the information provided in the appropriate read.me files or listed elsewhere on the media.

Should the manufacturer(s) or other Owner(s) cease to offer support or decline to honor any offer, SYBEX bears no responsibility. This notice concerning support for the Software is provided for your information only. SYBEX is not the agent or principal of the Owner(s), and SYBEX is in no way responsible for providing any support for the Software, nor is it liable or responsible for any support provided, or not provided, by the Owner(s).

Warranty

SYBEX warrants the enclosed media to be free of physical defects for a period of ninety (90) days after purchase. The Software is not available from SYBEX in any other form or media than that enclosed herein or posted to www.sybex.com. If you discover a defect in the media during this warranty period, you may obtain a

replacement of identical format at no charge by sending the defective media, postage prepaid, with proof of purchase to:

SYBEX Inc.
Product Support Department
1151 Marina Village Parkway
Alameda, CA 94501
Web: <http://www.sybex.com>

After the 90-day period, you can obtain replacement media of identical format by sending us the defective disk, proof of purchase, and a check or money order for \$10, payable to SYBEX.

Disclaimer

SYBEX makes no warranty or representation, either expressed or implied, with respect to the Software or its contents, quality, performance, merchantability, or fitness for a particular purpose. In no event will SYBEX, its distributors, or dealers be liable to you or any other party for direct, indirect, special, incidental, consequential, or other damages arising out of the use of or inability to use the Software or its contents even if advised of the possibility of such damage. In the event that the Software includes an online update feature, SYBEX further disclaims any obligation to provide this feature for any specific duration other than the initial posting.

The exclusion of implied warranties is not permitted by some states. Therefore, the above exclusion may not apply to you. This warranty provides you with specific legal rights; there may be other rights that you may have that vary from state to state. The pricing of the book with the Software by SYBEX reflects the allocation of risk and limitations on liability contained in this agreement of Terms and Conditions.

Shareware Distribution

This Software may contain various programs that are distributed as shareware. Copyright laws apply to both shareware and ordinary commercial software, and the copyright Owner(s) retains all rights. If you try a shareware program and continue using it, you are expected to register it. Individual programs differ on details of trial periods, registration, and payment. Please observe the requirements stated in appropriate files.

Copy Protection

The Software in whole or in part may or may not be copy-protected or encrypted. However, in all cases, reselling or redistributing these files without authorization is expressly forbidden except as specifically provided for by the Owner(s) therein.

To my wonderful book team members. Thanks for your help in making our book a success.

—David Groth

To my incredibly understanding and supportive wife, Karen, and my wonderful kids, Toby, Tiffani, Trey, and Taylor. Thank you for making such an impossibly odd schedule seem commonplace and acceptable.

—Toby Skandier

Acknowledgments

It takes many people to put a book together. This will be the fourth edition of this book, so I can safely say that these people know what they're doing and that I can count on working with talented people.

I would first like to thank my co-author Toby Skandier. He has a vast amount of technical knowledge and his contributions to this book helped to make it the best possible. Also, this book would not exist if it weren't for my acquisitions and developmental editor, Jeff Kellum. Thank you for all of your encouragement and support. I appreciate all of the hard work you contribute to each one of my book projects. Additionally, many thanks go to Lori Newman, our book team's tireless production editor. Kudos to you for juggling all sorts of deadlines spanning many projects and for basically keeping your eye on the ball for me all of the time. Kudos should also go to Judy Flynn, editor extraordinaire. Thank you for your careful attention to each of the chapters. Many thanks should also go to Jeffrey Wilson, the compositor at Happenstance Type-O-Rama, for laying out the very pages you see before you. Finally, one last cheer of the proofreaders who checked every last detail before sending the pages to the printer: Jim Brook, Candace English, and Nancy Riddiough.

I would also like to recognize my wife, family, and friends. My wife, Linda, tirelessly wrote and edited the appendices and kept me on the right track. She was a real trooper because she managed to do that while watching our kids. Thank you to my family and friends who understood when I couldn't go out or help them with projects because I had to work on the book. I really appreciate that.

Finally, thank you, the reader, for purchasing this book. I know that it has all the information in it to help you pass the test. If you have questions about Network+ or this book, feel free to e-mail me at dgroth@cableone.net. All of us involved in the book project have worked very hard to make it the best Network+ Study Guide available. I hope you feel the same.

—David Groth

I would like to thank David Groth for laying the foundation in earlier editions that could so easily grow into the modernized work you now hold, based on CompTIA's 2005 objectives for the prized and respected Network+ certification. Thanks also to David for his valuable work on this edition.

My gratitude and respect go out to the wise and professional Sybex team that brought this project together. Any author could shine with the care and polish provided by this wonderful group. A special thanks to Jeff Kellum for spearheading the production of our Study Guide. I really appreciate the support and unerring direction he provided.

I hope you will feel the way we do about this book. I know it will prove to be your most valuable resource in your quest for Network+ certification. Please let me know if there is anything additional you feel we could offer in future editions that will make the candidate's experience more successful and enjoyable. Don't hesitate to send your questions or comments to tskandier@hotmail.com. I am honored by your support for our efforts and hope you realize this book exists solely for you.

—Toby Skandier

Contents at a Glance

<i>Introduction</i>	<i>xix</i>
<i>Assessment Test</i>	<i>xxxi</i>
Chapter 1 Network Fundamentals	1
Chapter 2 The OSI Model	45
Chapter 3 TCP/IP Fundamentals	99
Chapter 4 TCP/IP Utilities	163
Chapter 5 Network Operating Systems	203
Chapter 6 Wired and Wireless Networks	231
Chapter 7 WAN and Remote Access Technologies	281
Chapter 8 Network Access and Security	317
Chapter 9 Fault Tolerance and Disaster Recovery	367
Chapter 10 Network Troubleshooting	407
Glossary	451
<i>Index</i>	491

Contents

<i>Introduction</i>	<i>xix</i>
<i>Assessment Test</i>	<i>xxxi</i>
Chapter 1	Network Fundamentals 1
Network Elements	3
Local Area Network	3
Wide Area Network	4
Host, Workstation, and Server	5
Peer-to-Peer vs. Client/Server Architecture	7
Physical Topologies	10
Bus Topology	10
Star Topology	11
Ring Topology	13
Mesh Topology	14
Backbones and Segments	15
Selecting the Right Topology	16
Physical Media	16
Coaxial Cable	17
Twisted-Pair Cable	20
Fiber-Optic Cable	25
Cable Type Summary	30
Common Network Connectivity Devices	31
NIC	32
Hub	32
Switch	32
Bridge	33
Router	33
Gateways	33
Other Devices	34
Summary	37
Exam Essentials	37
Review Questions	38
Answers to Review Questions	42
Chapter 2	The OSI Model 45
Introducing the OSI Model	46
The OSI Model's Lower Layers	51
The Physical Layer	51
The Data Link Layer	59

The OSI Model's Middle Layers	70
The Network Layer	70
The Transport Layer	77
The OSI Model's Upper Layers	80
The Session Layer	80
The Presentation Layer	81
The Application Layer	81
Upper-Layer Devices	81
Networking Protocols	81
TCP/IP	82
IPX/SPX	84
NetBEUI	86
AppleTalk and AppleTalk over IP	87
Summary	91
Exam Essentials	91
Review Questions	93
Answers to Review Questions	97
 Chapter 3 TCP/IP Fundamentals	 99
Introducing TCP/IP	102
A Brief History of TCP/IP	102
TCP/IP Design Goals	103
TCP/IP and the OSI Model	105
The Transmission Control Protocol	107
The Internet Layer Protocols	109
The Internet Protocol	109
Internet Control Message Protocol (ICMP)	112
Address Resolution Protocol (ARP) and Reverse ARP (RARP)	112
Routers and Routing	113
The Application Protocols	114
Simple Network Management Protocol (SNMP)	115
File Transfer Protocol (FTP)	115
Trivial File Transfer Protocol (TFTP)	115
Secure File Transfer Protocol (SFTP)	115
Simple Mail Transfer Protocol (SMTP)	116
Post Office Protocol (POP)	116
Internet Message Access Protocol, Version 4 (IMAP4)	116
Line Printer Daemon (LPD)	116
Network File System (NFS)	117
Telnet	117
Secure Shell (SSH)	117
Hypertext Transfer Protocol (HTTP)	117
Hypertext Transfer Protocol Secure (HTTPS)	117

Network Time Protocol (NTP)	117
Network News Transfer Protocol (NNTP)	118
Secure Copy Protocol (SCP)	118
Lightweight Directory Access Protocol (LDAP)	118
Internet Group Management Protocol (IGMP)	118
Line Printer Remote (LPR)	119
Other Upper-Layer Protocols	119
User Datagram Protocol (UDP)	119
Server Message Block (SMB)	120
AppleTalk Filing Protocol (AFP)	120
Internet Connection Sharing (ICS)	121
Overview of Ports and Sockets	121
Understanding IP Addressing	125
Overview of Ethernet Addresses	125
Overview of IP Addresses	125
Understanding Subnets	130
Subnetting a Class C Network	131
Classless Inter-Domain Routing (CIDR)	133
IP Proxy Servers	134
Name Resolution Methods	136
Internet Domain Organization	137
Using HOSTS	138
Using DNS	138
Using WINS	142
Configuring TCP/IP on Windows Workstations	145
The IP Settings Tab	147
The DNS Tab	148
The WINS Tab	148
The Options Tab	150
The Windows Registry	151
Zero Configuration (ZeroConf)	151
Virtual LANs (VLANs)	153
Summary	154
Exam Essentials	155
Review Questions	157
Answers to Review Questions	161
Chapter 4 TCP/IP Utilities	163
Using the Address Resolution Protocol (ARP)	164
The Windows ARP Table	165
Using The <i>arp</i> Utility	165
Using the <i>netstat</i> Utility	167
The <i>-a</i> Switch	168
The <i>-e</i> Switch	169

The <i>-r</i> Switch	170
The <i>-s</i> Switch	171
The <i>-n</i> Switch	173
The <i>-p</i> Switch	174
Using the <i>nbtstat</i> Utility	174
The <i>-a</i> Switch	175
The <i>-A</i> Switch	177
The <i>-c</i> Switch	177
The <i>-n</i> Switch	178
The <i>-r</i> Switch	178
The <i>-R</i> Switch	179
The <i>-S</i> Switch	179
The <i>-s</i> Switch	180
Using The File Transfer Protocol (FTP)	180
Starting FTP and Logging In to an FTP Server	181
Downloading Files	182
Uploading Files	184
Using the <i>ping</i> Utility	185
Using <i>winipcfg</i> , <i>ipconfig</i> , and <i>ifconfig</i>	186
Using the <i>winipcfg</i> Utility	186
Using the <i>ipconfig</i> Utility	188
Using the <i>ifconfig</i> Utility	190
Using the <i>tracert</i> Utility	191
Using the <i>Telnet</i> Utility	191
Using the <i>nslookup</i> Utility	194
Summary	195
Exam Essentials	195
Review Questions	197
Answers to Review Questions	201
 Chapter 5 Network Operating Systems	 203
Microsoft Windows	204
Features	205
Client Support	206
Interoperability	206
Authentication	207
File and Print Services	208
Application Support	208
Security	208
Novell NetWare	209
Features	209
Client Support	210
Interoperability	210
Authentication	211

Directory Structure	213
File and Print Services	215
Application Support	215
Security	215
UNIX/Linux	216
Features	216
Client Support and Interoperability	217
Authentication	217
File and Print Services	217
Application Support	218
Security	218
Macintosh	219
Features	219
Client Support	221
Interoperability	221
Authentication	222
File and Print Services	222
Application Support	222
Security	223
Summary	223
Exam Essentials	223
Review Questions	225
Answers to Review Questions	229
Chapter 6 Wired and Wireless Networks	231
Before Installing New Hardware or Software	232
Standard Operating Procedures	232
Environmental Issues	237
Error Messages and Log Files	242
Current Configuration and Baselines	243
Other Documentation	244
Wireless Networking	244
Wireless Network Components	244
Wireless Network Installation	248
Installation Type	252
Workstation Configuration	260
Configuring a Windows 9x Network	260
Configuring a Windows 2000 Network Client	264
Configuring Windows Clients for NetWare Network Access	265
Network Installation Tools	267
Wire Crimper	267
Media Testing Tools	268
Punchdown Tool	271
Summary	273

	Exam Essentials	273
	Review Questions	275
	Answers to Review Questions	279
Chapter 7	WAN and Remote Access Technologies	281
	Remote Access Connection Configuration Requirements	283
	Hardware Requirements	284
	Software Requirements	285
	Remote Access Connection Methods	286
	The Public Switched Telephone Network (PSTN)	286
	Integrated Services Digital Network (ISDN)	288
	Other Digital Options	289
	Remote Access Protocols	296
	Serial Line Internet Protocol (SLIP)	296
	Point-to-Point Protocol (PPP) and PPPoE (Point-to-Point Protocol over Ethernet)	297
	Point-to-Point Tunneling Protocol (PPTP)	302
	Windows Remote Access Services (RAS)	308
	Remote Desktop Protocol (RDP)	308
	Summary	309
	Exam Essentials	309
	Review Questions	310
	Answers to Review Questions	314
Chapter 8	Network Access and Security	317
	Accessing Network Resources	320
	Client Selection	320
	Installing the Windows 95/98 and NT/2000 Client	320
	Installing the NetWare Client	321
	Installing the UNIX Client	323
	Selecting a Primary Client	324
	Managing User Account and Password Security	324
	Network Resource-Sharing Security Models	325
	Managing Accounts	325
	Managing Passwords	328
	Using Firewalls	332
	Firewall Technologies	332
	Comparing Firewall Operating System Platforms	341
	Understanding and Defending against Hacker Attacks	343
	Hacker Tools: Common Network Attacks	344
	Intruder Detection: Defense Techniques	345
	DoD Security Standards	347
	Trusted Computer System	347

Trusted Network Interpretation	348
Certified Operating Systems and Networks	348
Understanding Encryption	350
Uses for Encryption	350
How Encryption Works	351
Encryption Keys	351
Security Policies	353
Security Audit	354
Clean Desk Policy	354
Recording Equipment	354
Other Common Security Policies	355
Breaking Policy	357
The Exit Interview	357
Summary	358
Exam Essentials	358
Review Questions	360
Answers to Review Questions	364
 Chapter 9	 Fault Tolerance and Disaster Recovery
	367
Assessing Fault Tolerance and Disaster Recovery Needs	368
Hot Site	369
Warm Site	371
Cold Site	372
Power Management	372
Surge Protectors	373
Battery Backup Systems	374
Line Conditioners	376
Disk System Fault Tolerance	377
Disk Mirroring	378
Disk Duplexing	378
Disk Striping	380
Redundant Array of Inexpensive (or Independent) Disks (RAID)	380
Backup Considerations	382
Backup Media Options	383
Backup Utilities	385
Backup Types	386
Tape Rotation Schedule	390
Virus Protection	392
Types of Viruses	393
Updating Antivirus Components	394
Scanning for Viruses	395
Software Revisions	397
Is It Necessary?	397

Where to Get Patches	397
How to Apply Patches	398
Summary	399
Exam Essentials	400
Review Questions	401
Answers to Review Questions	405
Chapter 10 Network Troubleshooting	407
Narrowing Down the Problem	409
Did You Check the Simple Stuff?	409
Is Hardware or Software Causing the Problem?	412
Is It a Workstation or a Server Problem?	413
Which Segments of the Network Are Affected?	414
Are There Any Cabling Issues?	414
Troubleshooting Steps	415
Step 1: Establish Symptoms	415
Step 2: Identify the Affected Area	415
Step 3: Establish What Has Changed	416
Step 4: Select the Most Probable Cause	417
Step 5: Implement a Solution	418
Step 6: Test the Result	420
Step 7: Recognize the Potential Effects of the Solution	420
Step 8: Document the Solution	420
The Troubleshooter's Resources	421
Log Files	421
Manufacturers' Troubleshooting Resources	434
Hardware Network Troubleshooting Tools	436
Software Troubleshooting Tools	439
Troubleshooting Tips	440
Don't Overlook the Small Stuff	440
Prioritize Your Problems	440
Check the Software Configuration	441
Don't Overlook Physical Conditions	441
Don't Overlook Cable Problems	442
Check for Viruses	442
Summary	443
Exam Essentials	443
Review Questions	445
Answers to Review Questions	449
Glossary	451
<i>Index</i>	491

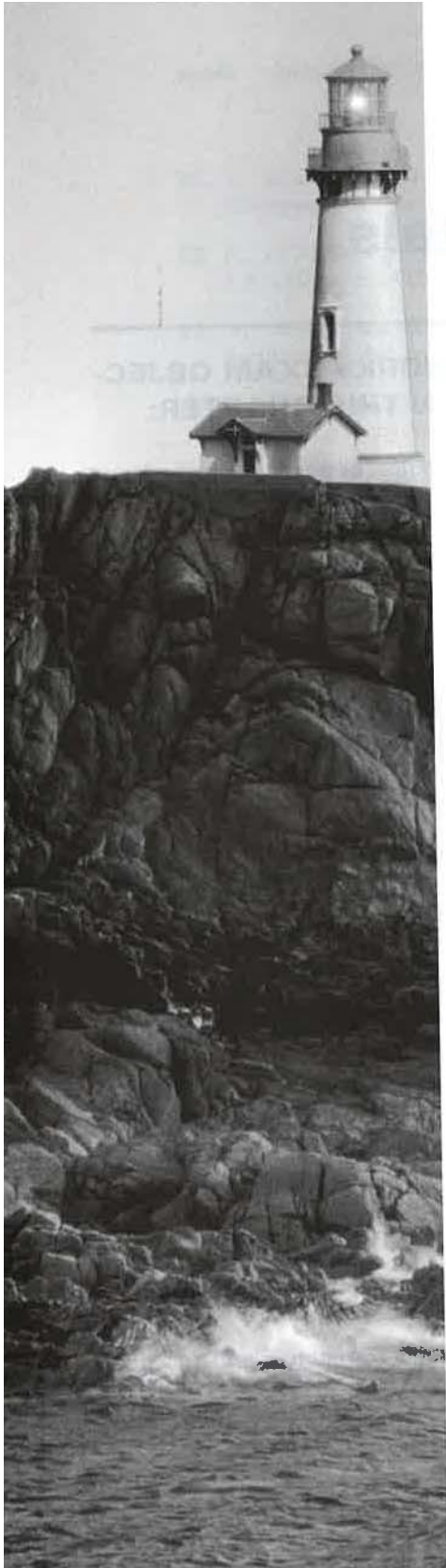
26. A. Although all of these answers are saying similar things, the only setting that exists in Windows 9x is Obtain IP Address Automatically. Please see Chapter 6 for more information.
27. A. OC-3 has a potential bandwidth of 155Mbps; T1 has a throughput of 1.544Mbps; ISDN is 1.544Mbps; and POTS has 53Kbps. Please see Chapter 7 for more information.
28. A. Of the protocols listed, only the Point-to-Point Protocol (PPP) provides TCP/IP Internet connections over dial-up (modem) connections. Please see Chapter 7 for more information.
29. D. Windows 2000 Server supports many different types of clients, including Windows, Macintosh, and Linux-based clients. Please see Chapter 5 for more information.
30. B. An HTTP proxy cache will cache (or store temporarily) copies of commonly used web page elements on a server on your LAN, thus the common elements will be received directly from the proxy at LAN speeds instead of Internet speeds. Please see Chapter 8 for more information.

Chapter 1

Network Fundamentals

THE FOLLOWING NETWORK+ EXAM OBJECTIVES ARE COVERED IN THIS CHAPTER:

- ✓ 1.1 Recognize the following logical or physical network topologies given a diagram, schematic, or description:
 - Star
 - Bus
 - Mesh
 - Ring
- ✓ 1.2 Specify the main features of 802.2 (Logical Link Control), 802.3 (Ethernet), 802.5 (Token Ring), 802.11 (wireless), and Fiber Distributed Data Interface (FDDI) networking technologies, including:
 - Speed
 - Access method (CSMA/CA [Carrier Sense Multiple Access/Collision Avoidance] and CSMA/CD [Carrier Sense Multiple Access / Collision Detection])
 - Topology
 - Media
- ✓ 1.3 Specify the characteristics (for example, speed, length, topology, and cable type) of the following cable standards:
 - 10Base-T and 10Base-FL
 - 100Base-TX and 100Base-FX
 - 1000Base-TX, 1000Base-CX, 1000Base-SX, and 1000BASE-LX
 - 10GBase-SR, 10GBase-LR, and 10GBase-ER
- ✓ 1.4 Recognize the following media connectors and describe their uses:
 - RJ-11 (Registered Jack)
 - RJ-45 (Registered Jack)
 - F-Type



- ST (straight tip)
- SC (subscriber connector)
- IEEE1394 (FireWire)
- LC (local connector)
- MTRJ (Mechanical Transfer Registered Jack)
- USB (Universal Serial Bus)

✓ **1.5 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) optic cable
- MMF (multimode fiber) optic cable

✓ **1.6 Identify the purposes, features, and functions of the following network components:**

- Hubs
- Switches
- Bridges
- Routers
- Gateways
- CSU/DSU (Channel Service Unit/Data Service Unit)
- NICs (network interface cards)
- ISDN (Integrated Services Digital Network) adapters
- WAPs (wireless access points)
- Modems
- Transceivers (media converters)
- Firewalls

✓ **3.2 Identify the basic capabilities needed for client workstations to connect to and use network resources (for example, media, network protocols, and peer and server services).**



By themselves, computers are powerful tools. When they are connected in a network, they become even more powerful because the functions and tools that each computer provides can be shared with other computers. Networks exist for one major reason: to share information and resources.

Networks can be very simple, such as a small group of computers that share information, or they can be very complex, spanning large geographical areas. Regardless of the type of network, a certain amount of maintenance is always required. Because each network is different and probably utilizes many diverse technologies, it is important to understand the fundamentals of networking and how networking components interact.

This chapter will introduce the components of a network and help you establish a base of knowledge that you can use throughout your networking studies, as well as help you prepare for the Network+ certification exam.

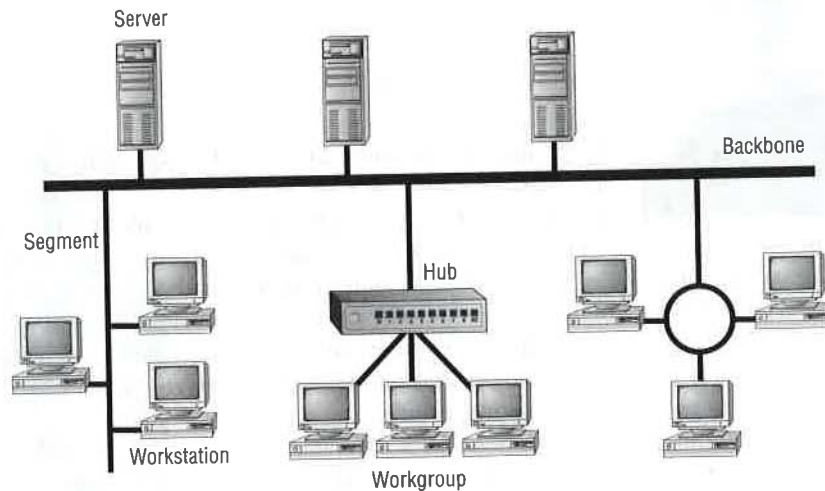
Network Elements

In the computer world, the term *network* describes two or more connected computers that can share resources such as data, a printer, an Internet connection, applications, or a combination of these. In the following sections, we'll discuss each type of network and describe the situation that is most appropriate for its use.

Local Area Network

By definition, a *local area network (LAN)* is limited to a specific area, usually an office, and cannot extend beyond the boundaries of a single building. The first LANs were limited to a range (from a central point to the most distant computer) of 185 meters (about 600 feet) and no more than 30 computers. Today's technology allows a larger LAN, but practical administration limitations require dividing it into small, logical areas called workgroups.

A *workgroup* is a collection of individuals (a sales department, for example) who share the same files and databases over the LAN. Figure 1.1 shows an example of a small LAN and its workgroups.

FIGURE 1.1 A small LAN

Wide Area Network

Chances are you are an experienced *wide area network* (WAN) user and don't even know it. If you have ever connected to the Internet, you have used the largest WAN on the planet. A WAN is any network that crosses metropolitan, regional, or national boundaries. Most networking professionals define a WAN as any network that uses routers and public network links. The Internet fits both definitions.

WANs differ from LANs in the following ways:

- WANs cover greater distances.
- WAN speeds are slower.
- WANs can be connected on demand or permanently connected; LANs have permanent connections between stations.
- WANs can use public or private network transports; LANs primarily use private network transports.
- WANs can use either full- or half-duplex communications. LANs have typically used half-duplex communications, although many local area networks today use full-duplex communications (see the sidebar "Full-Duplex vs. Half-Duplex Communications").

The Internet is actually a specific type of WAN. The Internet is a collection of networks that are interconnected and, therefore, is technically an *internetwork* (*Internet* is short for the word *internetwork*).

A WAN can be centralized or distributed. A centralized WAN consists of a central computer (at a central site) to which other computers and dumb terminals connect. The Internet, on the other hand, consists of many interconnected computers in many locations. Thus, it is a distributed WAN.

Full-Duplex vs. Half-Duplex Communications

All network communications (including LAN and WAN communications) can be categorized as half-duplex or full-duplex. With half-duplex, communications happen in both directions, but in only one direction at a time. When two computers communicate using half-duplex, one computer sends a signal and the other receives; then, at some point, they switch sending and receiving roles. Chances are that you are familiar with half-duplex communications. If you have ever used a push-to-talk technology, such as a CB radio or walkie-talkie, you were communicating via half-duplex: One person talks, and then the other person talks.

Full-duplex, on the other hand, allows communication in both directions simultaneously. Both stations can send and receive signals at the same time. Full-duplex communications are similar to a telephone call, in which both people can talk simultaneously.

Host, Workstation, and Server

Networks are made up of lots of different components, but the three most common network entities are the host, workstation, and server. For the Network+ exam, you need a good understanding of these three primary components of a network. Each one of these items can be found on most networks.

Understanding Workstations

In the classic sense, a *workstation* is a powerful computer used for drafting or other math-intensive applications. The term is also applied to a computer that has multiple central processing units (CPUs) available to users. In the network environment, the term *workstation* normally refers to any computer that is connected to the network and used by an individual to do work.

It is important to distinguish between workstations and clients. A *client* is any network entity that can request resources from the network; a workstation is a computer that can request resources. Workstations can be clients, but not all clients are workstations. For example, a printer can request resources from the network, but it is a client, not a workstation.

Understanding Servers

In the truest sense, a *server* does exactly what the name implies: It provides resources to the clients on the network ("serves" them, in other words). Servers are typically powerful computers that run the software that controls and maintains the network. This software is known as the *network operating system*.



We'll discuss this topic in detail in Chapter 3, "TCP/IP Fundamentals."

Servers are often specialized for a single purpose. This is not to say that a single server can't do many jobs, but, more often than not, you'll get better performance if you dedicate a server to a single task. Here are some examples of servers that are dedicated to a single task:

File Server Holds and distributes files.

Print Server Controls and manages one or more printers for the network.

Proxy Server Performs a function on behalf of other computers. (*Proxy* means "on behalf of.")

Application Server Hosts a network application.

Web Server Holds and delivers web pages and other web content using the Hypertext Transfer Protocol (HTTP).

Mail Server Hosts and delivers e-mail. It's the electronic equivalent of a post office.

Fax Server Sends and receives faxes (via a special fax board) for the entire network without the need for paper.

Remote Access Server Listens for **inbound requests** to connect to the network from the outside. Remote access servers provide **remote users** (working at home or on the road) with a connection to the network, either via modems or an IP connection.

Telephony Server Functions as a "smart" answering machine for the network. It can also perform call center and call-routing functions.

Notice that each server type's name consists of the type of service the server provides (remote access, for example) followed by the word *server*, which, as you remember, means **to serve**.

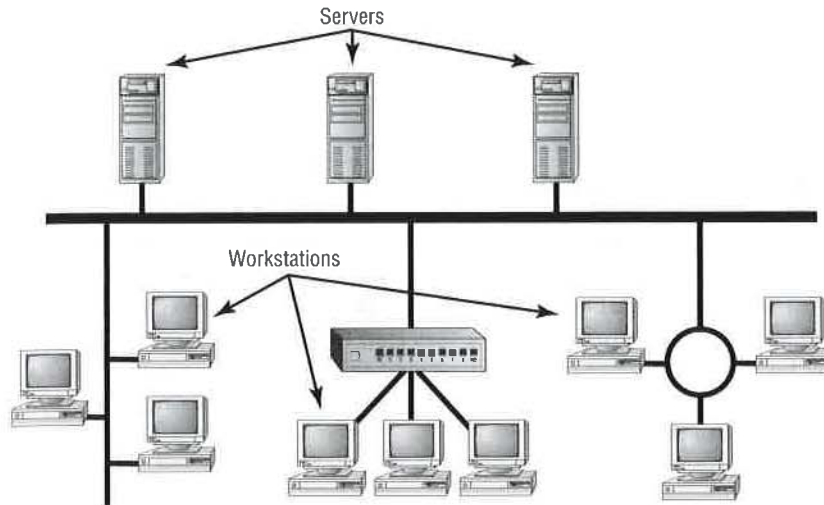
Regardless of the specific role (or roles) these servers play, they should all have the **following** in common:

- Hardware and/or software for data integrity (such as backup hardware and software)
- The capability to support a large number of clients

Figure 1.1, earlier in this chapter, shows a **sample network**. Physical resources, such as hard-drive space and memory, must be greater in a **server** than in a workstation because the server needs to provide services to many clients. Also, a server should be located in a physically secure area. Figure 1.2 shows a **sample network** that includes both workstations and servers. Note that there are more workstations than servers because a few servers can serve network resources to hundreds of users simultaneously.



If the physical access to a server is not controlled, you don't have security. Use this guideline: If anybody can touch it, it isn't secure. The value of the company data far exceeds the investment in computer hardware and software. We'll look at network security in detail in Chapter 8, "Network Access and Security."

FIGURE 1.2 A sample network including servers and workstations

Understanding Hosts

The term *host* covers pretty much every other networking device, but it can also refer to a workstation and server and is most commonly used when discussing TCP/IP-related services and functions. In fact, a host, in TCP/IP terms, is any network device that has an IP address. Workstations, servers, and any other network device (as long as it has one or more IP addresses) can all be considered hosts. In conversation, you may also hear the word *host* used to describe any minicomputer or server. For the Network+ exam, however, you should stick to the classic definition used here (i.e., workstations, servers, and other network devices).

The term *host* comes from the era when the only intelligent devices on the network were mainframes, which were commonly referred to as hosts regardless of TCP/IP functionality. Nearly all other devices were known as dumb terminals, but no other device had intelligence, only the mainframe. As TCP/IP came into the picture, only the mainframes, or hosts, received IP addresses. This is the same era that produced the term *gateway* to refer to any layer 3 intermediate device, such as a router. Just as the term *gateway* remains in common use today, such as in the very common term *default gateway*, the term *host* is still used, but its use is much broader now that nearly every end and intermediate device is intelligent and has at least one IP address, making them hosts.

Peer-to-Peer vs. Client/Server Architecture

As you learned earlier in this chapter, the purpose of networking is to share resources. How this is accomplished depends on the architecture of the network operating system software. The two most common network types are peer-to-peer and client/server.

If you were to look at an illustration of a group of computers in a LAN, it would be impossible to determine if the network was a peer-to-peer or a client/server environment. Even a videotape of this same LAN during a typical workday would reveal few clues as to whether it is peer-to-peer or client/server. Yet, the differences are huge. Since you can't see the differences, you might guess correctly that they are not physical but logical.

Physical vs. Logical Concepts

Throughout this book, you'll see us refer to physical and logical networking topics. Generally speaking, when we're referring to the physical aspects of a network, we're referring to some aspect of the network that you can touch or that has physical substance (like electrons, electrical pulses, or the way cables are run). That is, they exist in the physical world. Logical concepts, on the other hand, are more imaginary and esoteric and deal with things like how data flows in a network. So, when we're describing something as either physical or logical in nature, you'll understand how those terms apply.

Peer-to-Peer Network

In *peer-to-peer networks*, the connected computers have no centralized authority. From an authority viewpoint, all of these computers are equal. In other words, they are peers. If a user of one computer wants access to a resource on another computer, the security check for access rights is the responsibility of the computer holding the resource.

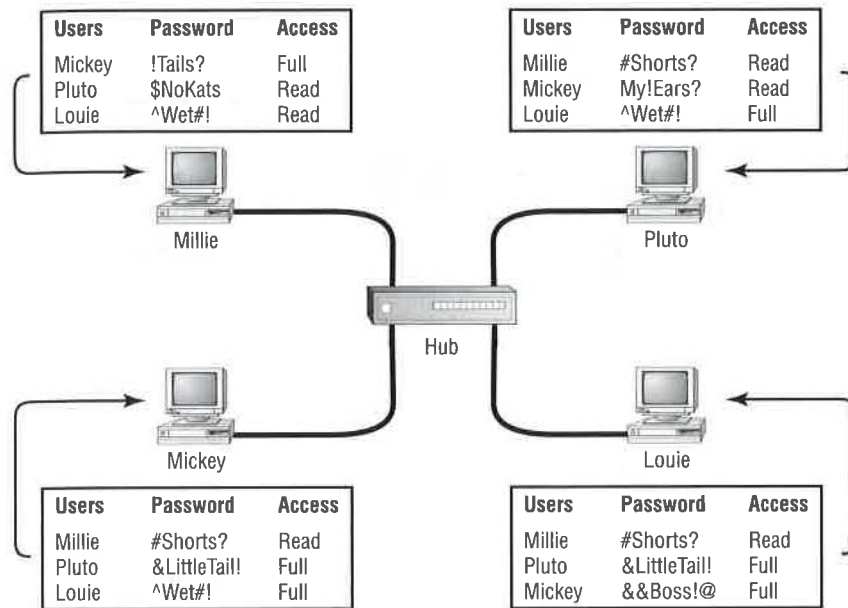
Each computer in a peer-to-peer network can be both a client that requests resources and a server that provides resources. This is a great arrangement, provided the following conditions are met:

- Each user is responsible for local backup.
- Security considerations are minimal.
- A limited number of computers are involved.

Networks that run Windows 95/98 as their network operating system and networks using Windows NT, 2000, or XP in a workgroup are considered peer-to-peer networks. Figure 1.3 shows an example of a peer-to-peer network. Peer-to-peer networks present some challenges. For example, backing up company data becomes an iffy proposition. Also, it can be difficult to remember where you stored a file. Finally, because security is not centralized, users and passwords must be maintained separately on each machine, as you can see in Figure 1.3. Passwords may be different for the same users on different machines (or for different resources on Windows 9x machines).

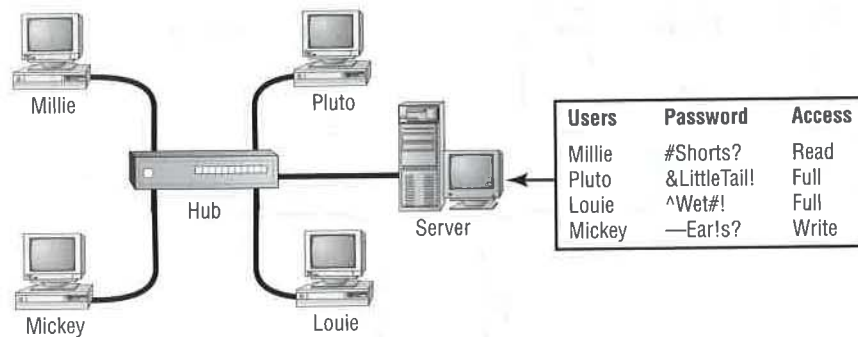
Client/Server Network

In contrast to a peer-to-peer network, a *client/server network* uses a network operating system designed to manage the entire network from a centralized point, which is the server. Clients make requests of the server, and the server responds with the information or access to a resource.

FIGURE 1.3 A peer-to-peer network

Client/server networks have some definite advantages over peer-to-peer networks. For one thing, the network is much more organized. It is easier to find files and resources because they are stored on the server. Also, client/server networks generally have much tighter security. All usernames and passwords are stored in the same database (on the server), and individual users can't use the server as a workstation. Finally, client/server networks have better performance and can scale almost infinitely. It is not uncommon to see client/server networks with tens of thousands of workstations. Figure 1.4 shows a sample client/server network. Note that the server now holds the database of user accounts, passwords, and access rights.

Note that today's networks are very often hybrids of the peer-to-peer model and the client/server model. Clients of early Novell NetWare networks, for example, had no ability to share their resources, not that they had many worth sharing, for the most part. Conversely, today's Microsoft and Apple networks, for example, have well-defined servers. They also allow the simultaneous sharing of resources from lesser devices that run what are considered workstation operating systems, which are capable of fewer inbound connections but are running the server service nonetheless. Purists shun the less organized mixture of this resource sharing among servers and clients alike, but the reality is that most networks would be worse off for losing this capability.

FIGURE 1.4 A client/server network

Physical Topologies

A topology is basically a map of a network. The physical topology of a network describes the layout of the cables and workstations and the location of all network components. Often, physical topologies are compared to logical topologies, which define how the information or data flows within the network. The topologies are usually similar. It is important to note, however, that a network can have one type of physical topology and a completely different logical topology. This was discussed earlier in the sidebar “Physical vs. Logical Concepts.”

The cables or connections in a physical topology are often referred to as network media (or *physical media*). Choosing how computers will be connected in a company’s network is critical. A wrong decision in the physical topology makes the media difficult to correct because it is costly and disruptive to change an entire installation once it is in place. The typical organization changes the physical layout and physical media of a network only once about every 10 years, so it is important to choose a configuration that you can live with and that allows for growth.

In the next section, we’ll look at physical media. In the following sections, we’ll look at the five most common topologies:

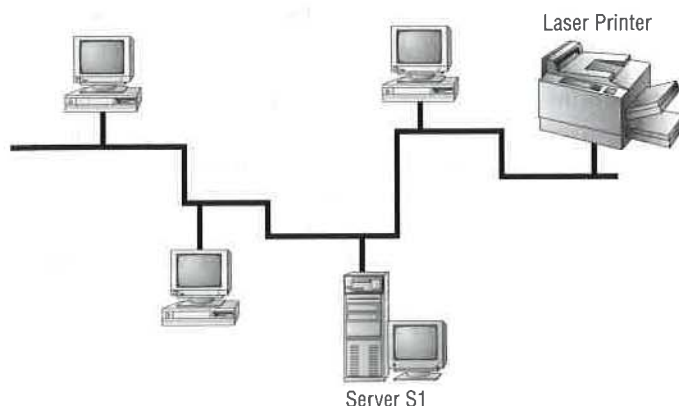
- Bus
- Star
- Ring
- Mesh

Bus Topology

In a *bus topology*, all computers are attached to a single continuous cable that is terminated at both ends, which is the simplest way to create a physical network. Originally, computers were attached to the cable with wire taps. This did not prove practical, so drop cables were used to

attach computers to the main cable. In 10Base-2 Ethernet, no drop cables are used, but instead, a “T” is inserted in the main cable wherever a station needs to connect. Figure 1.5 shows an example of a bus network. Notice how the cable runs from computer to computer with several bends and twists.

FIGURE 1.5 An example of a physical bus topology



When communicating on a network that uses a bus topology, all computers see the data on the wire. This does not create chaos, though, because the only computer that actually accepts the data is the one to which it is addressed. You can think of a bus network as a small party. David is already there, along with 10 other people. David would like to tell Joe something. David yells out, “Joe! Will you grab me a cup of coffee, please?” Everyone in the party can hear David, but only Joe will respond. A star network with a hub, which you’ll read about later, also operates in this manner.

As with most things, there are pros and cons to a bus topology. On the pro side, a bus topology has the following characteristics:

- Is simple to install
- Is relatively inexpensive
- Uses less cable than other topologies

The following characteristics describe the con side of a bus topology:

- Is difficult to move and change
- Has little fault tolerance (a single fault can bring down the entire network)
- Is difficult to troubleshoot

Star Topology

Unlike those in a bus topology, each computer in a *star topology* is connected to a central point by a separate cable or wireless connection. The central point is a device known by such names as *hub*, *MAU*, *concentrator*, *switch*, and *access point*, depending on the underlying technology.



Real World Scenario

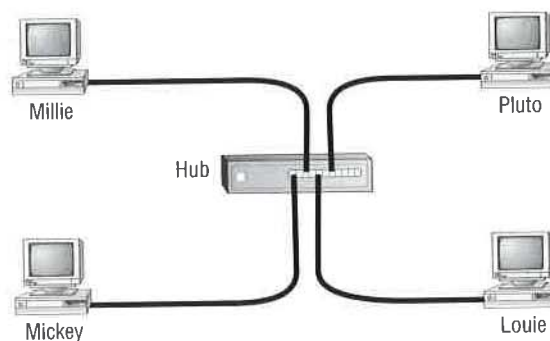
A bus sounds good, but . . .

Despite the simplicity of the bus topology, there are some inherent disadvantages to this design. For example, what happens if the wire breaks or is disconnected? Neither side can communicate with the other, and signal bounce occurs on both sides. The result is that the entire network is down. For this reason, bus topologies are considered to have very little fault tolerance.

Sometimes, because a cable is inside a wall, you cannot physically see a break. To determine if a break has occurred, you can use a tool known as a *Time Domain Reflectometer*, or *TDR* (also called a *cable tester*). This device sends out a signal and measures how much time it takes to return. Any break in the cable will cause some portion of the signal to return prematurely, thus indicating the presence of, and the distance to, a break in the cable. Programmed with the specifications of the cable being tested, it determines where the fault lies with a high degree of accuracy. We'll discuss cable testers in Chapter 6, "Wired and Wireless Networks."

Although this setup uses more cable than a bus, a star topology is much more fault tolerant than a bus topology. This means that if a failure occurs along one of the cables connecting to the hub, only that portion of the network is affected, not the entire network. Depending on the type of device at the other end of that cable, this may affect only a single device. It also means that you can add new stations just by running a single new cable. Figure 1.6 shows a typical star topology.

FIGURE 1.6 A typical star topology with a hub



The design of a star topology resembles an old wagon wheel with the wooden spokes extending from the center point. The center point of the wagon wheel would be considered the hub. Like the wagon wheel, the network's most vulnerable point is the hub. If it fails, the whole system collapses. Fortunately, hub failures are extremely rare.

As with the bus topology, the star topology has advantages and disadvantages. The increasing popularity of the star topology is mainly due to the large number of advantages, which include the following:

- New stations can be added easily and quickly.
- A single cable failure won't bring down the entire network.
- It is relatively easy to troubleshoot.

The disadvantages of a star topology include the following:

- Total installation cost can be higher because of the larger number of cables, but prices are constantly becoming more and more competitive.
- It has a single point of failure (the hub, or other central device).

There are two subtle special cases for the star topology, the point-to-point link and the wireless access point. If you think of a point-to-point connection as one spoke of a star-wired network, with either end device able to play the role of the hub or spoke device, then you can begin to see the nature of any star-wired topology. What about when there is no wire, though? It takes a firm understanding of what the devices making up the wireless network are capable of to be able to categorize the wireless topology. Wireless access points, discussed in detail in Chapter 6, are nothing more than wireless hubs or switches, depending on capability, that are able to act as wireless bridges by establishing a wireless point-to-point connection to another wireless access point. Either use is reminiscent of the wired star/point-to-point topologies they emulate.



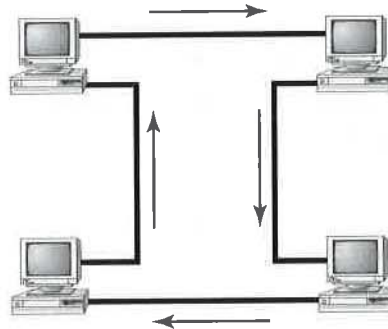
More information about wireless networking can be found in Chapter 6.

Ring Topology

In the *ring topology*, each computer is connected directly to two other computers in the network. Data moves down a one-way path from one computer to another, as shown in Figure 1.7. The good news about laying out cable in a ring is that the cable design is simple. The bad news is that, as with bus topology, any break, such as adding or removing a computer, disrupts the entire network. Also, because you have to “break” the ring in order to add another station, it is very difficult to reconfigure without bringing down the whole network. For this reason, the physical ring topology is seldom used.



Although its name suggests a relationship, Token Ring does not use a physical ring topology. It instead uses a physical star, logical ring topology (and runs at speeds of either 4Mbps or 16Mbps). You will learn more about logical topologies later in this chapter.

FIGURE 1.7 A typical ring topology

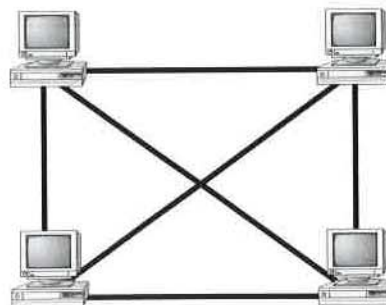
A few pros and many cons are associated with a ring topology. On the pro side, the ring topology is relatively easy to troubleshoot. A station will know when a cable fault has occurred because it will stop receiving data from its upstream neighbor.

On the con side, a ring topology has the following characteristics:

- Expensive, because multiple cables are needed for each workstation.
- Difficult to reconfigure.
- Not fault tolerant. A single cable fault can bring down the entire network.

Mesh Topology

In a *mesh topology* (as shown in Figure 1.8), a path exists from each station to every other station in the network, resulting in the most physical connections per node of any topology. While not usually seen in LANs, a variation on this type of topology—the hybrid mesh—is used on the Internet and other WANs in a limited fashion. Hybrid mesh topology networks can have multiple connections between some locations, but this is done only for redundancy. In addition, it's called a hybrid because other types of topologies might be mixed in as well. Also, it is not a full mesh because there is not a connection between each and every node, just a few for backup purposes. Notice in Figure 1.8 how complex the network becomes with four connections.

FIGURE 1.8 A typical mesh topology

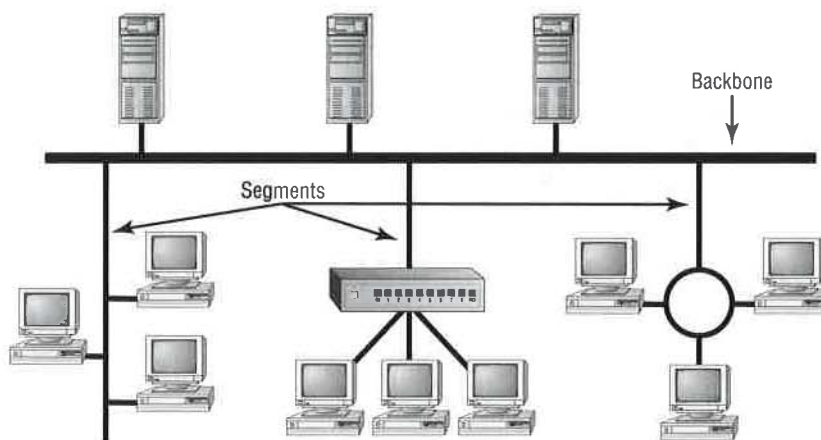
As you can see in Figure 1.8, a mesh topology can become quite complex as wiring and connections increase exponentially. For every n stations, you will have $n(n-1)/2$ connections. For example, in a network of 4 computers, you will have $4(4-1)/2$ connections, or 6 connections. If your network grows to only 10 computers, you will have 45 connections to manage! Given this impossible overhead, only small systems can be connected this way. The payoff for all this work is a more fail-safe, or fault-tolerant, network, at least as far as cabling is concerned.

Today, the mesh topology is rarely used, and then only in a WAN environment and only because the mesh topology is fault tolerant. Computers or network devices can switch between these multiple, redundant connections if the need arises. On the con side, the mesh topology is expensive and, as you have seen, quickly becomes too complex. Using what is known as a partial mesh is a workable compromise between the need for fault tolerance and the cost of a full mesh topology. With a partial mesh, the same technology can be used between all devices, but not all devices are interconnected. Strategy becomes the name of the game when deciding which devices to interconnect.

Backbones and Segments

With complex networks, we must have a way of intelligently identifying which part of the network we are discussing. For this reason, we commonly break networks into backbones and segments. Figure 1.9 shows a sample network and identifies the backbones and segments. You should refer to this figure when necessary as you read about backbones and segments.

FIGURE 1.9 Backbone and segments on a sample network



Understanding the Backbone

A *backbone* is the part of the network to which all segments and servers connect. A backbone provides the structure for a network and is considered the main part of any network. It usually uses a high-speed communications technology of some kind, such as Fiber Distributed Data

Interface (FDDI) or 1 or 10 Gigabit Ethernet. All servers and all network segments typically connect directly to the backbone so that any segment is only one segment away from any server on that backbone. Because all segments are close to the servers, the network is more efficient. Notice in Figure 1.9 that the three servers and three segments connect to the backbone.

Understanding Segments

Segment is a general term for any short section of the network that is not part of the backbone. Just as servers connect to the backbone, workstations connect to segments. Segments are connected to the backbone to allow the workstations on them access to the rest of the network. Figure 1.9 shows three segments.

Selecting the Right Topology

Each topology has its advantages and drawbacks. The process of selecting a topology can be much like buying a pair of shoes. It's a matter of finding something that fits, feels right, and is within your budget. Instead of asking what your shoe size is, ask questions such as, How much fault tolerance is necessary? and How often will I need to reconfigure the network? Creating a simple network for a handful of computers in a single room is usually done most efficiently by using a wireless access point and wireless network cards because they are simple and easy to install and don't require the running of cables. Larger environments are usually wired in a star because moves, adds, and changes to the network are performed more efficiently with a physical star than with any of the other topologies.

If you need uptime to the definition of fault resistant (that is, 99.9-percent uptime or less than 8 hours total downtime per year), you should seriously consider a partial mesh layout. While you are thinking about how fault tolerant a full mesh network is, let the word *maintenance* enter your thoughts. Remember that you will have $n(n-1)/2$ connections to maintain in a full mesh configuration and a subset of that for a partial mesh, which will quickly become a nightmare and could exceed your maintenance budget.

Generally speaking, you should balance the following considerations when choosing a physical topology for your network:

- Cost
- Ease of installation
- Ease of maintenance
- Cable fault tolerance

Physical Media

Although it is possible to use several forms of wireless networking, such as radio frequency and infrared, the majority of installed LANs today communicate via some sort of cable. In the following sections, we'll look at three types of cables:

- Coaxial
- Twisted pair
- Fiber optic

Coaxial Cable

Coaxial cable (or *coax*) contains a center conductor, made of copper, surrounded by a plastic jacket, with a braided shield over the jacket. A plastic such as polyvinyl chloride (PVC) or fluoroethylenepropylene (FEP, such as DuPont's Teflon) covers this metal shield. The Teflon-type covering is frequently referred to as a *plenum-rated coating*. That simply means that the coating doesn't begin burning until a much higher temperature, doesn't release as many toxic fumes as PVC when it does burn, and is rated for use in air plenums that carry breathable air, usually as nonenclosed fresh-air return pathways that share space with cabling. This type of cable is more expensive but may be mandated by local or municipal fire code whenever cable is hidden in walls or ceilings. Plenum rating applies to all types of cabling and is an approved replacement for all other compositions of cable sheathing and insulation, such as PVC-based assemblies.



NOTE

As a certified Network+ technician, you no longer need to concern yourself with the Thicknet and RG-58A/U (Radio Grade) types of coaxial cable, unless you would like to do your own research for historical or nostalgic purposes. Today, your focus should migrate from the 50ohm coax of early Ethernet to the 75ohm coax of early (and modern, of course) cable television. The reason for this is that while coax in the Ethernet world is all but a thing of the past, RG-6 or CATV coax is alive and well in the world of broadband cable (cable modem) technology. Chapter 7 will detail the location of 75ohm coaxial cable when used in a cable-modem system. The connectors used with coax in this environment are the same F-Type connectors used for standard cable television connectivity. In fact, the data rides on the same medium, just over different frequencies.

Using Thin Ethernet

Thin Ethernet, also referred to as *Thinnet* or 10Base-2, is a thin coaxial cable. It is basically the same as thick coaxial cable except that the diameter of the cable is smaller (about $\frac{1}{4}$ " in diameter). Thin Ethernet coaxial cable is RG-58. Figure 1.10 shows an example of Thin Ethernet.

With Thinnet cable, you use *BNC* connectors (see Figure 1.11) to attach stations to the network. It is beyond my province to settle the long-standing argument over the meaning of the abbreviation BNC. BNC could mean Bayonet Connector, Bayonet Nut Connector, or British Navel Connector. But it is most commonly referred to as the Bayonet Neill-Concelman connector. What is relevant is that the BNC connector locks securely with a quarter-twist motion.

FIGURE 1.10 A stripped-back Thinnet**FIGURE 1.11** A male and female BNC connector

The BNC connector can be attached to a cable in two ways. The first is with a crimper, which looks like funny pliers and has a die to crimp the connector. Pressing the levers crimps the connector to the cable. Choice number two is a screw-on connector, which is very unreliable. If at all possible, avoid the screw-on connector!

In order to attach the backbone cable run to each station, a passive device, known as a T-connector, is used. Picture the uncut backbone cable extending to the back of each device. In order to complete the connection, the cable needs to be cut at the point where the loop is closest to the interface. The two cut ends then need to be terminated with male BNC connectors and plugged into the two female BNC interfaces of the T-connector, with the third, male connector attaching to the female BNC interface on the device's NIC card. It is in violation of the standard to have any sort of drop cable extending from the back of the device, unlike 10Base-5, where

such an attachment was customary. This requirement introduces a minimum of two caveats. The first is that any user that gains access to the back of their computer, and that wouldn't be very hard, could disconnect the connectorized ends of the cut backbone, thus producing two unterminated LAN segments, neither one working properly. The second is that so many interconnections introduce failure points and opportunities for noise introduction.

Table 1.1 shows some of the specifications for the different types of coaxial cable.

TABLE 1.1 Coaxial Cable Specifications

RG Rating	Popular Name	Ethernet Implementation	Type of Cable
RG-58 U	N/A	None	Solid copper
RG-58 A/U	Thinnet	10Base2	Stranded copper
RG-8	Thicknet	10Base5	Solid copper
RG-62	ARCnet	N/A	Solid/stranded



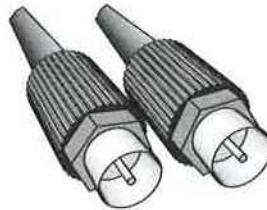
Although some great advantages are associated with using coax cable, such as the braided shielding that provides fair resistance to electronic pollution like *electromagnetic interference (EMI)* and *radio frequency interference (RFI)*, all types of stray electronic signals can make their way onto a network cable and cause communications problems. Understanding EMI and RFI is critical to your networking success. For this reason, we'll go into greater detail in Chapter 6.

Using F-Type Connectors

The F-Type connector is a threaded, screw-on connector that differs from the BNC connector of early Ethernet mainly in its method of device attachment. Additionally, as alluded to earlier, you typically find F-Type connectors with 75ohm coaxial media and BNC connectors with 50ohm applications. As with most other coax applications, the F-Type connector uses the center conductor of the coaxial cable as its center connecting point. The other conductor is the metal body of the connector itself, which connects to the shield of the cable. Again, due to the popularity of cable modems, the F-Type coaxial connector has finally made its way into mainstream data networking. Figure 1.12 shows an example of an F-Type coaxial connector.



There is also a twist-on F-Type connector used in fiber-optic cabling, known as the FC connector.

FIGURE 1.12 An example of an F-Type coaxial cable connector

Twisted-Pair Cable

Twisted-pair cable consists of multiple, individually insulated wires that are twisted together in pairs. Sometimes a metallic shield is placed around the twisted pairs. Hence, the name *shielded twisted-pair (STP)*. (You might see this type of cabling in Token Ring installations.) More commonly, you see cable without outer shielding; it's called *unshielded twisted-pair (UTP)*. UTP is commonly used in twisted-pair Ethernet (10Base-T, 100Base-TX, etc.), star-wired networks.

Let's take a look at why the wires in this cable type are twisted. When electromagnetic signals are conducted on copper wires that are in close proximity (such as inside a cable), some electromagnetic interference occurs. In this scenario, this interference is called *crosstalk*. Twisting two wires together as a pair minimizes such interference and also provides some protection against interference from outside sources. This cable type is the most common today. It is popular for several reasons:

- It's cheaper than other types of cabling.
- It's easy to work with.
- It permits transmission rates considered impossible 10 years ago.

UTP cable is rated in the following categories:

Category 1 Two twisted wire pairs (four wires). Voice grade (not rated for data communications). The oldest UTP. Frequently referred to as POTS, or plain old telephone service. Before 1983, this was the standard cable used throughout the North American telephone system. POTS cable still exists in parts of the Public Switched Telephone Network (PSTN). Supports signals limited to a frequency of 1MHz.

Category 2 Four twisted wire pairs (eight wires). Suitable for up to 4Mbps, with a frequency limitation of 10MHz.

Category 3 Four twisted wire pairs (eight wires) with three twists per foot. Acceptable for transmissions up to 16MHz. A popular cable choice since the mid-1980s, but now limited mainly to telecommunication equipment.

Category 4 Four twisted wire pairs (eight wires) and rated for 20MHz.

Category 5 Four twisted wire pairs (eight wires) and rated for 100MHz.

Category 5e Four twisted wire pairs (eight wires) and rated for 100MHz, but capable of handling the disturbance on each pair caused by transmitting on all four pairs at the same time, which is needed for Gigabit Ethernet.

Category 6 Four twisted wire pairs (eight wires) and rated for 250MHz. Became a standard in June 2002.



Frequently, you will hear *Category* shortened to *Cat*. Today, any cable that you install should be a minimum of Cat 5e. This is a minimum because some cable is now certified to carry a bandwidth signal of 350MHz or beyond. This allows unshielded twisted-pair cables to exceed speeds of 1Gbps, which is fast enough to carry broadcast-quality video over a network. A common saying is that there are three ways to do things: the Right way, the Wrong way, and the IBM way. IBM uses types instead of categories when referring to TP (twisted-pair) cabling specifications. Even though a cabling type may seem to correspond to a cabling category (such as Type 1 and Category 1), the two are not the same; IBM defines its own specifications.

Now that you've learned the different types of UTP cables, you will learn how best to connect them to the various pieces of networking equipment using UTP.



Real World Scenario

Category 5e Cabling Tips

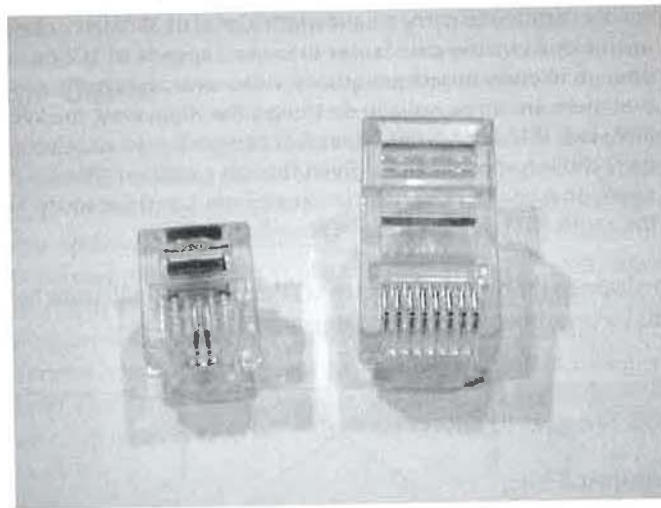
If you expect data rates faster than 10Mbps over UTP, you should ensure that all components are rated to the category you want to achieve and be very careful when handling all components. For example, pulling too hard on Cat 5e cable will stretch the number of twists inside the jacket, rendering the Cat 5e label on the outside of the cable invalid. Also, be certain to connect and test all four pairs of wire. Although today's wiring usually uses only two pairs, or four wires, the standard for Gigabit Ethernet over UTP requires that all four pairs, or eight wires, be in good condition.

You should also be aware that a true Cat 5e cabling system uses rated components from end to end, patch cables from workstation to wall panel, cable from wall panel to patch panel, and patch cables from patch panel to hub. If any components are missing or if the lengths do not match the Category 5e specification, you don't have a Category 5e cabling installation. Also, installers should certify that the entire installation is Category 5e compliant. However, this requires very expensive test equipment that can make the appropriate measurements.

Connecting UTP

Clearly, a BNC connector won't fit easily on UTP cable, so you need to use an *RJ* (*Registered Jack*) connector. You are probably familiar with RJ connectors. Most telephones connect with an RJ-11 connector. The connector used with UTP cable is called RJ-45. The RJ-11 has four wires, or two pairs, and the network connector RJ-45 (also known as an 8P8C connector when referring to the plug instead of the jack) has four pairs, or eight wires, as shown in Figure 1.13.

FIGURE 1.13 RJ-11 and RJ-45 connectors



In almost every case, UTP uses RJ connectors. Even the now-extinct ARCnet used RJ connectors. You use a crimper to attach an RJ connector to a cable, just as you use a crimper with the BNC connector. The only difference is that the die that holds the connector is a different shape. Higher-quality crimping tools have interchangeable dies for both types of cables.

Signaling Methods

The amount of a cable's available bandwidth (overall capacity, such as 10Mbps) that is used by each signal depends on whether the signaling method is **baseband** or **broadband**. With **baseband**, the entire bandwidth of the cable is used for each signal (using one channel). It is typically used with digital signaling. With **broadband**, on the other hand, the available bandwidth is divided into discrete bands. Multiple signals can then be transmitted within these different bands. Some form of tuning device, or demodulator, is required to choose the specific frequency of interest, as opposed to baseband receiving circuitry, which can be hardwired to a specific frequency. Don't confuse this *broadband* with the term that is the opposite of *narrowband*, which is any bit rate of T1 speeds (1.544Mbps) or slower. That *broadband* refers to speeds in excess of T1/E1 rates, such as Broadband-ISDN (B-ISDN), which has been developed under the ATM specifications.

Ethernet Cable Descriptions

Ethernet cable types are described using a code that follows this format: *N<Signaling>-X*. Generally speaking, *N* is the signaling rate in megabits per second, and *<Signaling>* is the signaling type, which is either base or broad (baseband or broadband). *X* is a unique identifier for a specific Ethernet cabling scheme.

Let's use a generic example: 10BaseX. The two-digit number 10 indicates that the transmission speed is 10Mb, or 10 megabits. The value *X* can have different meanings. For example, the 5 in 10Base5 indicates the maximum distance that the signal can travel—500 meters. The 2 in 10Base2 is used the same way, but fudges the truth. The real limitation is 185 meters. Only the IEEE committee knows for sure what this was about. We can only guess that it's because 10Base2 seems easier to say than 10Base1.85.

Another 10Base standard is 10Base-T. The *T* is short for *twisted-pair*. This is the standard for running 10-Megabit Ethernet over two pairs (four wires) of Category 4, 5e, or 6 UTP. The fourth, and currently final, 10Base is 10Base-FL. The *F* is short for *fiber*, while the *L* stands for *link*. 10Base-FL is the standard for running 10-Megabit Ethernet over fiber-optic cable to the desktop. Table 1.2, shown a bit later, summarizes this data.

Similarly, there are also standards for 100Base, 1000Base, and 10GBase cabling. Let's take a closer look at these standards:

100Base-TX As network applications increased in complexity, so did their bandwidth requirements. Ten-megabit technologies were too slow. Businesses were clamoring for a higher speed standard so that their data could be transmitted at an acceptable rate of speed. A 100-megabit standard was needed. Thus the 100Base-TX standard was developed.

The 100Base-TX standard is a standard for Ethernet transmission at a data rate of 100Mbps. This Ethernet standard is also known as *Fast Ethernet*. It uses two UTP pairs (four wires) in a minimum of Category 5 UTP cable.

1000Base-TX 1000Base-TX, most commonly known as Gigabit Ethernet, allows 1000Mbps throughput on standard twisted-pair, copper cable (rated at Category 5e or higher).

1000Base-SX The implementation of Gigabit Ethernet running over multimode fiber-optic cable (instead of copper, twisted-pair cable) and using short wavelength laser.

1000Base-LX The implementation of Gigabit Ethernet over single-mode and multimode fiber using long wavelength laser.

1000Base-CX An implementation of Gigabit Ethernet over balanced, 150ohm copper cabling and uses a special 9-pin connector known as the *High Speed Serial Data Connector (HSSDC)*.

10GBase-SR An implementation of 10 Gigabit Ethernet that uses short wavelength lasers at 850 nanometers(nm) over multimode fiber. It has a maximum transmission distance of between 2 and 300 meters, depending on the size and quality of the fiber.

10GBase-LR An implementation of 10 Gigabit Ethernet that uses long wavelength lasers at 1310 nm over single-mode fiber. It also has a maximum transmission distance between 2 meters and 10 kilometers, depending on the size and quality of the fiber.

10GBase-ER An implementation of 10 Gigabit Ethernet running over single-mode fiber. It uses extra long wavelength lasers at 1550 nm. It has the longest transmission distances possible of the 10-Gigabit technologies: anywhere from 2 meters up to 40 kilometers, depending on the size and quality of the fiber used.



See the upcoming section, “Fiber-Optic Cable,” in this chapter, for more information on single-mode and multimode fiber and on fiber in general.

IEEE Standard 1394 (FireWire)

One unique cabling type that is used in a limited sense is IEEE standard 1394, more commonly known as *FireWire* (or as Sony calls it, *i.Link*). Developed by Apple Computer, FireWire runs at 100, 200, 400Mbps (800Mbps in the 1394b standard), but in its standard mode it has a cable length limitation of 15 feet (4.5 meters), which limits it to specialized applications like data transfer between two computers located in close proximity or data transfer between a computer and another device (like an MP3 player).

FireWire uses two types of connectors: the 6 pin and the 4 pin. The 6-pin connector (as shown in Figure 1.14) is for devices that need to be powered from the computer. FireWire cables with the 6-pin connector contain two pairs (four conductors) of copper wire for carrying data and one pair for powering devices, all within a common, braided metal shield. Cables using the 4-pin connector (Figure 1.15) are for data transfer only, and they contain only the four conductors for data, none for power.

FIGURE 1.14 Six-pin FireWire connector (male)

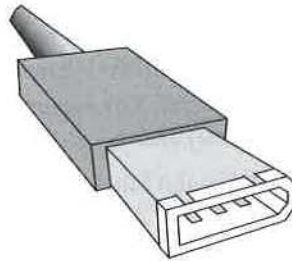
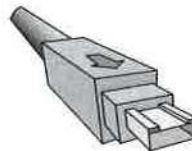


FIGURE 1.15 Four-pin FireWire connector (male)





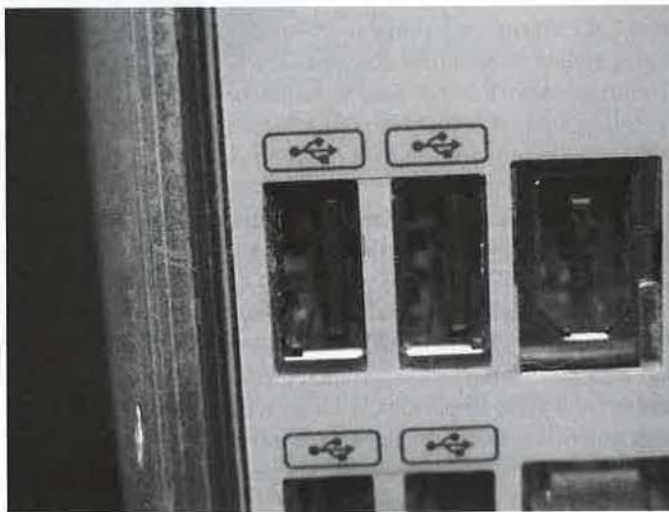
More information about FireWire and its associated standards can be found at the 1394 Trade Association website at www.1394ta.org.

Universal Serial Bus (USB)

Over the past few years, computer peripherals have been moving away from parallel or serial connection and to a new type of bus. That bus is the *Universal Serial Bus (USB)*. The built-in serial bus of most motherboards generally offers a maximum of 2 external interfaces for connectivity to a PC, although add-on adapters can take that count up to as many as 16 serial interfaces. USB, on the other hand, can connect a maximum of 127 external devices. Also, USB is a much more flexible peripheral bus than either serial or parallel. USB supports connections to printers, scanners, and many other input devices (such as keyboards, joysticks, and mice).

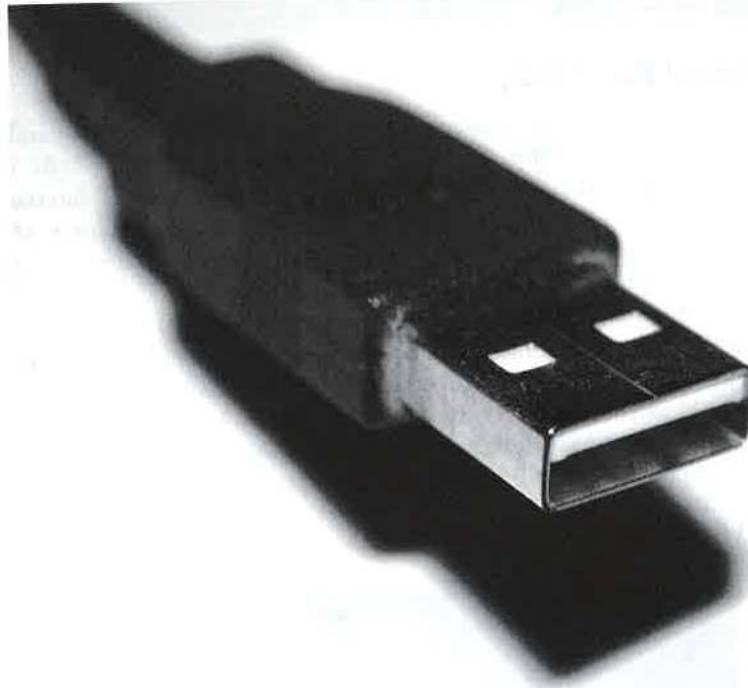
When connecting USB peripherals, you must connect them either directly to one of the USB ports (as shown in Figure 1.16) on the PC or to a USB hub that is connected to one of those USB ports. Hubs can be chained together to provide multiple USB connections. Although you can connect up to 127 devices (each device has a USB plug, as shown in Figure 1.17), it is impractical in reality. Most computers with USB interfaces will support around 12 USB devices.

FIGURE 1.16 A USB port



Fiber-Optic Cable

Because fiber-optic cable transmits digital signals using light impulses rather than electricity, it is immune to Electromagnetic Interference (EMI) and Radio Frequency Interference (RFI).

FIGURE 1.17 A USB plug

You will find a complete discussion of these terms in Chapter 6, but you should know at this point that both could affect network performance.

Anyone who has seen UTP cable for a network run down an elevator shaft would, without doubt, appreciate this feature of fiber. Light is carried on either a glass or a plastic core. Glass can carry the signal a greater distance, but plastic costs less. Regardless of which core is used, the core is surrounded by a glass or plastic cladding, which is more glass or plastic with a different index of refraction that refracts the light back into the core. Around this is a layer of flexible plastic buffer. This can be then wrapped in an armor coating (where necessary), typically Kevlar, and then sheathed in PVC or plenum.



For more information about fiber-optic cabling, see *Cabling: The Complete Guide to Network Wiring, Third Edition*, by David Barnett, David Groth, and Jim McBee (Sybex, 2004).

The cable itself comes in two different styles: single-mode fiber (SMF) and multimode fiber (MMF). The difference between single-mode fibers and multimode fibers is in the number of

light rays (and thus the number of signals) they can carry. Generally speaking, multimode fiber is used for shorter-distance applications and single-mode fiber for longer distances.

If you happen to come across a strand of fiber in the field and want to know if it's single mode or multimode, here are some general guidelines. First of all, if it's got a yellow jacket, it's probably single mode. If it's got an orange jacket, it's most likely multimode. Also, check the writing on the cable itself. You'll find a number like 62.5/125. These are the outside diameters of the core and the cladding (respectively). If the first number is a 8, 9, or 10, it is most likely a single mode. On the other hand, if the numbers read as before (62.5/125), it's most likely a multimode strand of fiber. Use these two tips to help you identify that errant strand of fiber.

Although fiber-optic cable may sound like the solution to many problems, it has pros and cons just as the other cable types. Here are the pros:

- Is completely immune to EMI or RFI
- Can transmit up to 40 kilometers (about 25 miles)

Here are the cons of fiber-optic cable:

- Is difficult to install
- Requires a bigger investment in installation and materials

Fiber-Optic Connectors

Fiber-optic cables can use a myriad different connectors, but the two most popular and recognizable are the *straight tip (ST)* and *subscriber (or square) connector (SC)* connectors. The ST fiber-optic connector, developed by AT&T, was one of the most widely used fiber-optic connectors. It uses a BNC attachment mechanism similar to the Thinnet connection mechanism, which makes connections and disconnections relatively easy. Its ease of use is one of the attributes that makes this connector so popular. Figure 1.18 shows an example of an ST connector. Notice the BNC attachment mechanism.

The SC connector (sometimes known also as a square connector) is another type of fiber-optic connector. As you can see in Figure 1.19, SC connectors are latched connectors. This latching mechanism holds the connector in securely while in use and prevents it from just falling out.



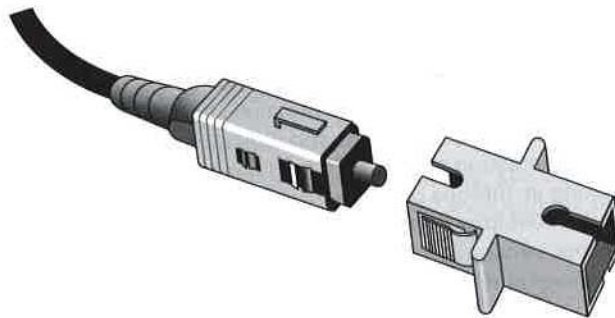
If data runs are measured in kilometers, fiber optic is your cable of choice because copper cannot reach more than 500 meters (about 1500 feet) without electronics regenerating the signal, and that's for the all-but-obsolete 10Base5 coaxial standard. The standards limit UTP to a mere 100 meters. You may also want to opt for fiber-optic cable if an installation requires high security, because it does not create a readable magnetic field. Although fiber-optic technology was initially very expensive and difficult to work with, it is now being used in some interesting places, such as Gigabit or 10GB Internet backbones. Ethernet running at 10Mbps over fiber-optic cable to the desktop is designated 10Base-FL; the 100Mbps version of this implementation is 100Base-FX. The *L* in the 10Mbps version stands for *link*, as opposed to such other designations as *B* for *backbone* and *P* for *passive*.

SC connectors work with either single-mode or multimode optical fibers, and they will last for around 1000 matings. They are seeing increased use but aren't as popular as ST connectors for LAN connections.

FIGURE 1.18 An example of an ST connector



FIGURE 1.19 A sample SC connector



Small Form Factor Fiber-Optic Connectors

One of the more popular styles of fiber-optic connectors is the *small form factor (SFF)* style of connector. SFF connectors allow more fiber-optic terminations in the same amount of space over their standard-sized counterparts. The two most popular are the *mechanical transfer registered jack (MT-RJ or MTRJ)*, designed by AMP, and the *Local Connector (LC)*, designed by Lucent.

MT-RJ

The MT-RJ fiber-optic connector was the first small form factor fiber-optic connector to see widespread use. It is one-third the size of the SC and ST connectors it most often replaces. It had the following benefits:

- Small size
- TX and RX strands in one connector
- Keyed for single polarity
- Pre-terminated ends that require no polishing or epoxy
- Easy to use

Figure 1.20 shows an example of an MT-RJ fiber-optic connector

FIGURE 1.20 A sample MT-RJ fiber-optic connector



LC

Local Connector is a newer style of SFF fiber-optic connector that is overtaking MT-RJ as a fiber-optic connector. It is especially popular for use with Fibre Channel adapters and Gigabit Ethernet adapters. It has similar advantages to MT-RJ and other SFF-type connectors but is easier to terminate. It uses a ceramic insert as standard-sized fiber-optic connectors do. Figure 1.21 shows an example of the LC connector.

FIGURE 1.21 A sample LC fiber-optic connector



Cable Type Summary

Table 1.2 summarizes the cable types.

TABLE 1.2 Common Ethernet and FDDI Cable Types

Ethernet Name	Cable Type	Maximum Speed	Maximum Transmission Distance	Notes
10Base5	Coax	10Mbps	500 meters per segment	Also called Thicknet, this cable type uses vampire taps to connect devices to cable.
10Base2	Coax	10Mbps	185 meters per segment	Also called Thinnet, a very popular implementation of Ethernet over coax.
10Base-T	UTP	10Mbps	100 meters per segment	One of the most popular network cabling schemes.
100Base-TX	UTP, STP	100Mbps	100 meters per segment	Two pairs of Category 5 UTP.
10Base-FL	Fiber	10Mbps	Varies (ranges from 500 meters to 2000 meters)	Ethernet over fiber optics to the desktop.
100Base-FX	Multimode fiber	100Mbps	2000 meters	100Mbps Ethernet over fiber optics.
1000Base-T	UTP	1000Mbps	100 meters	Four pairs of Category 5e or higher.
1000Base-SX	Multimode fiber	1000Mbps	550 meters	Uses SC fiber connectors. Max length depends on fiber size.
1000Base-CX	Balanced, shielded copper	1000Mbps	25 meters	Uses special connector, the HSSDC.
1000Base-LX	Multimode and single-mode fiber	1000Mbps	550 meters multimode/2000 meters single mode	Uses longer wavelength laser than 1000Base-SX. Uses SC and LC connectors.

TABLE 1.2 Common Ethernet and FDDI Cable Types *(continued)*

Ethernet Name	Cable Type	Maximum Speed	Maximum Transmission Distance	Notes
10GBase-SR	Multimode fiber	10Gbps	300 meters	850 nm laser. Max length depends on fiber size and quality.
10GBase-LR	Single-mode fiber	10Gbps	10 kilometers	1310 nm laser. Max length depends on fiber size and quality.
10GBase-ER	Single-mode fiber	10Gbps	40 kilometers	1550 nm laser. Max length depends on fiber size and quality.
FDDI	Multimode fiber	100Mbps	10 kilometers	Uses MIC connector.

Common Network Connectivity Devices

Now that you are familiar with the various types of network media and connections, you should learn about some devices commonly found on today's networks. Because these devices connect network entities, they are known as connectivity devices:

- The network interface card (NIC)
- The hub
- The switch
- The bridge
- The router
- The gateway
- Other devices



These will be discussed in more detail in Chapter 2, "The OSI Model."

NIC

The *network interface card (NIC)*, as its name suggests, is the expansion card you install in your computer to connect, or interface, your computer to the network. This device provides the physical, electrical, and electronic connections to the network media. A NIC is either an expansion card (the most popular implementation) or built in to the motherboard of the computer. In most cases, a NIC connects to the computer through *expansion slots*, which are special slots located on a computer's motherboard that allow peripherals to be plugged directly into it. In some notebook computers, NIC adapters can be connected to the printer port or through a PC card slot.

NIC cards generally all have one or two light emitting diodes (LEDs) that help in diagnosing problems with their functionality. If there are two separate LEDs, one of them may be the Link LED, which illuminates when proper connectivity to an active network is detected. This often means that the NIC is receiving a proper signal from the hub/MAU or switch, but it could indicate connectivity to and detection of a carrier on a coax segment or connectivity with a router or other end device using a crossover cable. The other most popular LED is the Activity LED. The Activity LED will tend to flicker, indicating the intermittent transmission or receipt of frames to or from the network.



The first LED you should verify is the Link LED because if it's not illuminated, there will be no chance for the Activity LED to illuminate.

Hub

As you learned earlier, in a star topology Ethernet network, a hub is the device that connects all the segments of the network together. Every device in the network connects directly to the hub through a single cable. Any transmission received on one port will be sent out all the other ports in the hub, including the receiving pair for the transmitting device, so that CSMA/CD on the transmitter can monitor for collisions. So, if one station sends it, all the others receive it; but based on addressing in the frame, only the intended recipient listens to it. This is to simulate the physical bus that the CSMA/CD standard was based on. It's why we call the use of a hub in an Ethernet environment a *physical star/logical bus topology*. It is important to note that hubs are nothing more than glorified repeaters, which are incapable of recognizing frame boundaries and data structures; that's why they act with such a lack of intelligence. A broadcast sent out by any device on the hub will be propagated to all devices connected to the hub. Any two or more devices connected to the hub have the capability of causing a collision with each other, just as in the case of a physical bus.

Switch

Like a hub, a switch connects multiple segments of a network together, with one important difference. Whereas a hub sends out anything it receives on one port to all the others, a switch recognizes frame boundaries and pays attention to the destination MAC address of the incoming frame as well as the port on which it was received. If the destination is known to be on a different port than the port over which the frame was received, the switch will forward the frame

out over only the port on which the destination exists. Otherwise, the frame is silently discarded. If the location of the destination is unknown, then the switch acts much like a hub in that it floods the frame out every port, except for the port over which it was received, unlike a hub. The only way any party not involved in that communication will receive the transmission is if it shares a port with the transmitter or receiver of the frame. This can occur if a hub is attached to the switch port, instead of in a 1:1 relationship of end devices and switch ports. The benefit of a switch over a hub is that the switch increases performance because it is able to support full wire speed on each and every port with a nonblocking backplane, meaning the electronics inside the switch are at least equivalent in speed to the sum of the speeds of all ports.

Bridge

A *bridge*, specifically a transparent bridge, is a network device that connects two similar network segments together. The primary function of a bridge is to keep traffic separated on both sides of the bridge. Traffic is allowed to pass through the bridge only if the transmission is intended for a station on the opposite side. The main reasons for putting a bridge in a network are to connect two segments together and to divide a busy network into two segments. A switch can be thought of as a hardware-based multiport bridge.

Router

A *router* is a network device that connects multiple, often dissimilar, network segments into an inter-network. The router, once connected, can make intelligent decisions about how best to get network data to its destination based on network performance data that it gathers from the network itself.

Routers are very complex devices. Often, routers are computers unto themselves with their own complex operating systems to manage the routing functions (Cisco's IOS, for example) and CPUs dedicated to the functions of routing packets. Because of their complexity, it is actually possible to configure routers to perform the functions of other types of network devices (like gateways, firewalls, etc.) by simply implementing the feature within the router's software.

Gateways

A *gateway* is any hardware and software combination that connects dissimilar network environments. Gateways are the most complex of network devices because they perform translations at multiple layers of the OSI model.

For example, a gateway is the device that connects a LAN environment to a mainframe environment. The two environments are completely different. LAN environments use distributed processing, baseband communications, and the ASCII character set. Mainframe environments use centralized processing, broadband and baseband communications, and the EBCDIC character set. Each of the LAN protocols is translated to its mainframe counterpart by the gateway software.

Another popular example is the e-mail gateway. Most LAN-based e-mail software, such as Novell's GroupWise and Microsoft's Exchange, can't communicate directly with Internet mail servers without the use of a gateway. This gateway translates LAN-based mail messages into the SMTP format that Internet mail uses.

Other Devices

In addition to these network connectivity devices, there are several devices that, while maybe not directly connected to a network, participate in moving network data:

- Modems
- ISDN terminal adapters
- Wireless access points
- CSU/DSUs
- Transceivers (media converters)
- Firewalls

Modems

A *modem* is a device that modulates digital data onto an analog carrier for transmission over an analog medium and then demodulates from the analog carrier to a digital signal again at the receiving end. The term *modem* is actually an acronym that stands for MOdulator/DEModulator.

When we hear the term *modem*, three different types should come to mind:

- Traditional (POTS)
- DSL
- Cable

Traditional (POTS)

Most modems you find in computers today fall into the category of traditional modems. These modems convert the signals from your computer into signals that travel over the plain old telephone **service** (POTS) lines. The majority of modems that exist today are POTS modems, mainly because **PC manufacturers** include one with a computer.

DSL

Digital subscriber line (DSL) is quickly replacing traditional modem access because it offers higher data rates for a reasonable cost. In addition, you can make regular phone calls while online. DSL uses higher frequencies (above 3200Hz) than regular voice phone calls use, which provides greater bandwidth (up to several megabits per second) than regular POTS modems provide while still allowing the standard voice frequency range to travel at its normal frequency to remain compatible with traditional POTS phones and devices, an advantage over ISDN. DSL “modems” are the devices that allow the network signals to pass over **phone lines** at these higher frequencies.

Most often, when you sign up for DSL service, **the company** you sign up with will send you a DSL modem for free or for a very low cost. This modem is usually an external modem (although internal DSL modems are available), and it usually has both a phone line and an Ethernet connection. You must connect the phone line to a wall jack and the Ethernet connection to your computer (you must have an Ethernet NIC in your computer in order to connect to the DSL modem). Alternatively, a router, hub, or switch may be connected to the Ethernet port of the DSL modem, increasing the options available for the Ethernet network.



If you have DSL service on the same phone line you use to make voice calls, you must install DSL filters on all the phone jacks where you have a phone. Or, a DSL filter will be installed after the DSL modem for all the phones in a building. Otherwise, you will hear a very annoying hissing noise (the DSL signals) on your voice calls.

Cable

Another high-speed Internet access technology that is seeing widespread use is cable modem access. Cable modems connect an individual PC or network to the Internet using your cable television cable. The cable TV companies use their existing cable infrastructure to deliver data services on unused frequency bands.

The cable modem itself is a fairly simple device. It has a standard coax connector on the back as well as an Ethernet port. You can connect one PC to a cable modem (the PC will need to have an Ethernet NIC installed), or you can connect the modem to multiple PCs on a network (using a hub or switch). A router may also be used to enhance the Ethernet network's capabilities.

ISDN Terminal Adapters

Integrated Services Digital Network (ISDN) is another form of high-speed Internet access. It delivers digital services (over 64Kbps channels) over conditioned telephone copper pairs. The device you must hook up to your computer to access ISDN services is properly known as an *ISDN Terminal Adapter*. It's not a modem in the truest sense of the word because a modem changes from digital to analog for transmission. An ISDN TA doesn't change from digital to analog. It just changes between digital transmission formats.

The box itself is about the size of a modem and looks similar to one. But, as with DSL modems, there is a phone jack and an Ethernet jack. You connect a phone cord from the phone jack to the wall jack where your ISDN services are being delivered. Then you connect an Ethernet cable from your PC to the ISDN TA's Ethernet jack. Older, less-capable TAs used an EIA/TIA-232 serial port for PC connectivity.

Wireless Access Points (WAPs)

A *wireless access point (WAP)* allows mobile users to connect to a wired network wirelessly via radio frequency technologies. WAPs also allow wired networks to connect to each other via wireless technologies. Essentially, they are the wireless equivalent of a hub or a switch in that they can connect multiple wireless (and often wired) devices together to form a network.

One of the most popular use for wireless access points is to provide Internet access in public areas, like libraries, coffee shops, hotels, and airports. WAPs are easy to set up; most often, you just need to plug them in to a wired network and power them up to get them to work. Plus, without the clutter or added expense of cables to hook them up, they make ideal foundations for small business networks.



You'll learn the intricate details of wireless access points that a Network+ technician should know in Chapter 6.

CSU/DSUs

The Channel Service Unit/Data Service Unit (CSU/DSU) is a common device found in equipment rooms when the network is connected via a T-series data connection or other digital serial technology (e.g., a T1 or Digital Data Server [DDS]). It is essentially two devices in one that are used to connect a digital carrier (the T-series or DDS line) to your network equipment (usually to a router). The *Channel Service Unit (CSU)* terminates the line at the customer's premises. It also provides diagnostics and remote testing, if necessary. The *Data Service Unit (DSU)* does the actual transmission of the signal through the CSU. It can also provide buffering and data flow control.

Both components are required if you are going to connect to a digital transmission medium, such as a T1 line. Sometimes, however, one or both of these components may be built into a router. If both components are built into a router, you only have to plug the T1 line directly into the router. Otherwise, some Physical Layer specification, like V.35 or HSSI, will have to be used to cable the interface on the router to the external CSU/DSU.

Transceivers (Media Converters)

Another small device that is commonly seen on a network is the external transceiver (also known as a media converter). These are relatively simple devices that allow a NIC or other networking device to connect to a different type of media than it was designed for. Many NICs have special connectors that will allow this, as do hubs and switches.

For example, if you have a 100Base-TX switch and would like to connect it to another switch using fiber-optic cabling, you would connect a fiber transceiver to each switch's transceiver port and then connect the two transceivers together with the appropriate fiber-optic cabling.

With early Ethernet-style DB-15 female Digital-Intel-Xerox (DIX, or more commonly Attachment Unit Interface [AUI]) NIC interfaces, which are still available as medium-independent connectors on more advanced NICs and other networking devices, an external transceiver has to be used to convert the electrical signal from the device to one that is compatible with the cabling medium. Every other popular type of Ethernet technology, such as the xBase-T standards, has a built-in transceiver on the NIC card or device interface. An external transceiver is necessary with these technologies only to act as a media converter.

Firewalls

A *firewall* is probably the most important device on a network if that network is connected to the Internet. Its job is to protect LAN resources from attackers on the Internet. Similarly, it can prevent computers on the network from accessing various services on the Internet. It can be used to filter packets based on rules that the network administrator sets. These rules state what kinds of information can flow into and out of a network's connection to the Internet.

Firewalls can be either stand-alone "black boxes," or can be set up in software on a server or router. Either way, the firewall will have at least two network connections: one to the Internet (known as the "public" side), and one to the network (known as the "private" side). Sometimes, there is a third network port on a firewall. This port is used to connect servers and equipment that can be considered both public and private (like web and e-mail servers). This intermediary network is known as a *demilitarized zone*, or *DMZ*.

Firewalls are the first line of defense for an Internet-connected network. If a network was directly connected to the Internet without a firewall, an attacker could theoretically gain direct access to the computers and servers on that network with little effort.

Summary

In this chapter, you learned about the items that can be found on a typical network. You first learned what a network is and the various elements that make up a network, such as servers, workstations, and hosts. Then you learned about the different ways of laying out a network. You learned about bus, star, ring, mesh, and hybrid topologies.

You also learned about the different types of physical media in use on networks today, including coaxial, twisted-pair, and fiber-optic media.

Finally, you learned about some common network devices—including NICs, hubs, switches, bridges, routers, and gateways—seen on a typical network.

Exam Essentials

Know how to identify different network topologies. A single cable with computers attached to it is a bus. A central hub with cables radiating out to computers is a star. A crisscross, redundant connection to all computers is a mesh. An outer loop connecting all computers is a ring.

Know the operational characteristics of various cable standards. You should know the signaling rate (in Mbps), signaling method (baseband or broadband), media type (copper or fiber), and the other specifics for the various cable standards such as 10Base-T, 10Base-FL, 100Base-TX, 1000Base-T, and 10GBase-SR.

Be able to recognize different media connectors and describe their uses. You should know that RJ-11 is used to connect a phone jack to a telephone; RJ-45 is used for 10Base-T, 100Base-TX, and 1000Base-T twisted-pair Ethernet connections; BNC is used for 10Base2 Ethernet connections; AUI, a DB-15 connector/PC game connector, is used for 10Base5 connections from vampire tap to NIC; ST, the most popular fiber-optic connector, is a barrel connector with a locking ring; and SC, another common fiber connector, is a square-ended connector with a latching mechanism. You should also understand the different types of IEEE 1394 (FireWire) connectors and their different uses.

Understand the different media types and their uses. You should know the different types of commonly used network media (copper cabling and fiber-optic media) and the different applications of each. You must know the differences between Category 3, 5, 5e, and 6 UTP and what the category ratings mean. You should also know the operational characteristics of the different types of fiber-optic cable (single mode and multimode).

Be able to explain the basic purpose and function of many different network devices. You should understand how each network device—including hubs, switches, routers, bridges, firewalls, and wireless access points—functions.

Review Questions

1. Which of the following are characteristic of a peer-to-peer network? (Choose all that apply.)
 - A. It has centralized security and administration.
 - B. A computer can be both a client and a server.
 - C. A limited number of computers are involved.
 - D. It does not require a hub.
2. Which cabling standard can send data at up to 10,000Mbps?
 - A. 10Base-T
 - B. 100Base-TX
 - C. 1000Base-TX
 - D. 10GBase-SR
3. Which of the following are not small form factor fiber connectors? (Choose all that apply.)
 - A. MT-RJ
 - B. LC
 - C. FC
 - D. SC
4. Which LED on your NIC might save you the most frustration if you start your troubleshooting efforts by monitoring its illumination?
 - A. Link
 - B. Activity
 - C. Collision
 - D. 10/100
5. Which of the following is a characteristic of a mesh network?
 - A. It controls cable costs.
 - B. It offers improved reliability.
 - C. It is required by fire code.
 - D. It needs a token to operate.
6. Which of the following are advantages of a star-wired topology? (Choose all that apply.)
 - A. The star topology uses the least amount of cable.
 - B. A cable cut between a lone device and its concentrating device affects only the lone device.
 - C. There is a single point of failure in the central concentrating device.
 - D. Troubleshooting is simplified compared to the other topologies.

7. Besides the newer high-speed Token Ring, what are the other two standard ring speeds for the Token Ring technology? (Choose all that apply.)
 - A. 4Mbps
 - B. 16Mbps
 - C. 100Mbps
 - D. 4Gbps
8. Which of the following is a characteristic of a physical mesh topology?
 - A. It has the most physical connections per device.
 - B. It is the most common physical LAN topology.
 - C. Each device has only an inbound port and an outbound port.
 - D. When one device transmits, all other devices hear the transmission.
9. Which of the following FireWire connectors are for devices that need to be powered from the computer?
 - A. 4 pin
 - B. 6 pin
 - C. 8 pin
 - D. 10 pin
10. Plenum-rated cable has which of the following characteristics?
 - A. It has a lower cost than PVC.
 - B. It meets fire codes for installation in suspended ceilings.
 - C. It transmits data faster.
 - D. All the above.
11. Which of the two following cable, connector, length triples meet the specifications for 1000Base-SX and 1000Base-LX?
 - A. UTP, RJ-45, 100m
 - B. MMF, LC, 550m
 - C. SMF, FC, 2000m
 - D. MMF, SC, 550m
12. Which of the following devices would help your laptop communicate with a mainframe on the same LAN segment?
 - A. Transceiver
 - B. Gateway
 - C. Switch
 - D. Router

13. Which Ethernet standard is designed to use only two pairs of wires in a UTP cable?
- A. 1000Base-CX
 - B. 100Base-FX
 - C. 1000Base-T
 - D. 100Base-TX
14. A transmission technology that divides that transmission medium into discrete channels so that multiple signals can share the same cable is known as _____.
- A. duplex communications
 - B. baseband communications
 - C. sideband communications
 - D. broadband communications
15. If you need to change the type of media a NIC is able to connect to, which device would you use?
- A. Bridge
 - B. Hub
 - C. Transceiver
 - D. All the above
16. An RJ-45 connector should be wired with _____ pairs when used on a Category 5e UTP cable.
- A. 1
 - B. 2
 - C. 4
 - D. 8
17. 10GBase-SR can be extended to _____ meters per segment.
- A. 100
 - B. 200
 - C. 300
 - D. 1000
18. Which network component is used in conjunction with a router to provide access to a T1 circuit?
- A. Gateway
 - B. T1 modem
 - C. CSU/DSU
 - D. Switch

19. If you need to protect internal LAN resources from an external threat, which device can help most?
- A. Router
 - B. Firewall
 - C. Proxy server
 - D. HTTPS-compatible NIC card
20. Which of the following is a difference between the 100Base-TX and 1000Base-T Ethernet specifications?
- A. 1000Base-T is 10 times faster because it uses fiber optics.
 - B. 100Base-TX requires a minimum of Category 5 UTP, while 1000Base-T must be run over no less than Category 5e UTP.
 - C. Because it's slower and more stable, 100Base-TX can be run over longer distances.
 - D. Although both technologies require the same number of pairs for transmitting and receiving, 1000Base-T uses them differently.

Answers to Review Questions

1. B, C. Computers participating in a peer-to-peer network can be either client or server or both. Additionally, the peer-to-peer model has some practical limitations, including the number of computers involved. Answer A is incorrect because the administration is *not* centralized. Answer D is incorrect because the use of hubs is not related to the implementation of peer-to-peer or client/server networks.
2. D. The 10G in the 10GBase-SR designation can be thought of as standing for 10Gbps or 10,000Mbps, whichever helps you remember.
3. C, D. MT-RJ and LC are both forms of SFF fiber connectors. FC and SC are larger and do not permit the port density afforded by the other two.
4. A. Looking at the Link LED first could save you the frustration of waiting for the Activity LED to light up, which may never happen as long as there are issues with network connectivity (indicated by a dark Link LED).
5. B. The major advantage to mesh networks is their increased reliability. There are multiple redundant connections between all nodes in the network. Answer A is incorrect because the cable costs are much, much more than other networks. Answer C is simply a distracter; mesh is *not* required by fire codes. Answer D is incorrect because most token-based networks could not operate in a mesh environment.
6. B, D. The star topology has the advantage of simplifying the troubleshooting process because, when a device fails, you should check that device and its NIC, the network cable connected to that NIC, and the port on the concentrating device (hub, MAU, switch, etc.) to which the other end of the network cable is connected. Somewhat related to this point, it also has the advantage of localizing problems to the single device or cable segment. While it is true that the central concentrating device is a single point of failure, this is one of the disadvantages of star topologies.
7. A, B. The two early ring speeds of Token Ring were 4Mbps and 16Mbps.
8. A. Of the physical topologies, the mesh has the most physical connections per device. This complete interconnection is what creates the mesh. The mesh is not used in the majority of LAN implementations, mostly with WAN links. The most common physical LAN topology is the star topology. Answer C describes a physical ring topology, and D describes a logical bus topology.
9. B. There are only two main types of FireWire connectors, the 4 pin and the 6 pin. The 6-pin connector has two extra pins that provide power from the computer to the device.
10. B. Answer B is the only correct answer because plenum-rated cable meets fire codes for installation in suspended ceilings, raised floors, and any other open area through which ventilation-system air is returned. Plenum cable actually has a higher cost than PVC. Additionally, because the conductors are also made of copper, it doesn't conduct data any faster than PVC-coated cable.
11. B, D. Both the SX and LX standards of gigabit Ethernet are based on fiber-optic cable, not copper. However, while 1000Base-LX permits the use of single-mode fiber over distances of 2000m, it does not use the FC connector. Both it and the SX standard allow the use of SC or LC connectors on multimode fiber over a distance of 550m.

12. B. If your PC does not have native connectivity, say via TCP/IP, with a mainframe, none of the devices will assist you in communicating with the mainframe. The only help a router would be is if the mainframe were not on the same LAN segment, but it would have to speak the same protocol as your laptop or a gateway would still be necessary. Of all the answers, gateway is decidedly the best.
13. D. 100Base-FX can be ruled out immediately because the *F* indicates a fiber-optic media dependency, while more subtly, 1000Base-CX can be quickly eliminated due to its media dependency on STP, not UTP. 1000Base-T is incorrect because, although it calls for the use of Category 5e UTP, it requires all four pairs for both transmit and receive use.
14. D. In broadband communications (television communications, for example), the communications medium is divided into discrete channels. Each channel can carry its own signal. In baseband communications, the transmission takes up the whole communications channel. Full duplex communications give a sender and receiver the ability to each send and receive signals simultaneously. Sideband is a distracter.
15. C. Although all the devices listed can be purchased with the variety of interfaces necessary to satisfy the objective, an external transceiver's sole purpose is to change the type of media a NIC or device interface connects to (provided there is a transceiver port available on the NIC or that you purchase a transceiver with the appropriate interconnections).
16. C. Although you can wire any combination of pairs in an RJ-45 connector, you should wire all four pairs in a Category 5 UTP into an RJ-45 connector to support those network technologies that may need all four pairs (such as 1000Base-T), even if you aren't currently using them. Additionally, this habit supports all currently available technologies. So, in case you decide to change from Token Ring to Ethernet, if you create a straight-through wired channel, there is no reason to rewire any cables because the popular wire pairing standards will cover both of these technologies and many more.
17. C. The maximum segment length for 10GBase-SR is 300 meters.
18. C. The Channel Service Unit/Data Service Unit (CSU/DSU) translates LAN signals into signals that are used on T1 lines. Some people incorrectly call it a "T1 modem." It's not a modem because it doesn't translate data into analog and back. Every signal stays in the digital format.
19. B. Although a router possesses certain access control capabilities, a firewall's hardened configuration set makes it a superior choice for establishing a secure entryway into a LAN, blocking malicious traffic with pinpoint accuracy while allowing trusted traffic access to the internal resources. A proxy server may include some firewall capabilities, but not to the level of a stand-alone firewall. Besides, in the end, the proxy component that provides this functionality is a firewall, making it the best answer here. HTTPS is not a function of NIC cards, nor would hardening a NIC card help guard an entire LAN against outside threats.
20. B. 100Base-TX works fine with two pairs of at least Category 5 UTP, but due to the fact that 1000Base-T uses all four pairs simultaneously (a reason D is incorrect), a minimum of Category 5e UTP is required for proper functioning. Both of these standards are specified over twisted-pair copper (the *T* in their name signifies this), not fiber optics. Both standards are limited to the same 100m segment length.



Chapter 2

The OSI Model

THE FOLLOWING NETWORK+ EXAM OBJECTIVES ARE COVERED IN THIS CHAPTER:

- ✓ 1.2 Specify the main features of 802.2 (Logical Link Control), 802.3 (Ethernet), 802.5 (Token Ring), 802.11 (wireless), and Fiber Distributed Data Interface (FDDI) networking technologies, including:
 - Speed
 - Access method (CSMA/CA [Carrier Sense Multiple Access/Collision Avoidance] and CSMA/CD [Carrier Sense Multiple Access/Collision Detection])
 - Topology
 - Media
- ✓ 2.1 Identify a MAC (Media Access Control) address and its parts.
- ✓ 2.2 Identify the seven layers of the OSI (Open Systems Interconnect) model and their functions.
- ✓ 2.3 Identify the OSI (Open Systems Interconnect) layers at which the following network components operate:
 - Hubs
 - Switches
 - Bridges
 - Routers
 - NICs (network interface cards)
 - WAPs (wireless access points)
- ✓ 2.4 Differentiate between the following network protocols in terms of routing, addressing schemes, interoperability, and naming conventions:
 - IPX/SPX (Internetwork Packet Exchange/Sequenced Packet Exchange)
 - NetBEUI (Network Basic Input/Output System Extended User Interface)
 - AppleTalk/AppleTalk over IP (Internet Protocol)
 - TCP/IP (Transmission Control Protocol/Internet Protocol)