i-Net+ Study Guide

by David Groth

with David Wall

and Michael de Beer

Associate Publisher

Neil Edde

Contracts and Licensing Manager

Kristine O’Callaghan

Acquisitions & Developmental Editor

Linda Lee

Editor

Judy Flynn

Project Editor

Rebecca Rider

Technical Editors

Robert Gradante, Donald Fuller

Book Designer

Bill Gibson

Graphic Illustrator

Tony Jonick

Comprehensive exam preparation for the i-NET+ certification.
Electronic Publishing Specialist
Bill Gibson

Project Team Leader
Leslie Higbee

Proofreader
Molly Glover

Indexer
Nancy Guenther

CD Coordinator
Kara Schwarz

CD Technicians
Keith McNeil, Ginger Warner

Cover Designer
Archer Design

Cover Photographer
The Image Bank

SYBEX, Network Press, and the Network Press logo are a registered trademarks of SYBEX Inc.

Screen reproductions produced with Collage Complete.

Collage Complete is a trademark of Inner Media Inc.

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

FullShot is a trademark of Inbit Incorporated.

The CD Interface music is from GIRA Sound AURIA Music Library © GIRA Sound 1996.

Netscape Communications, the Netscape Communications logo, Netscape, and Netscape Navigator are trademarks of Netscape Communications Corporation.

Netscape Communications Corporation has not authorized, sponsored, endorsed, or approved this
publication and is not responsible for its content. Netscape and the Netscape Communications Corporate Logos are trademarks and trade names of Netscape Communications Corporation. All other product names and/or logos are trademarks of their respective owners.

Internet screen shot(s) using Microsoft Internet Explorer 5 reprinted by permission from Microsoft Corporation.

The i-Net+ Certification program is an industry-wide, vendor-neutral program developed and sponsored by the Computing Technology Industry Association (CompTIA). Sybex is an independent entity from CompTIA, and not affiliated with CompTIA in any manner. Neither CompTIA nor Sybex warrants that use of this publication will ensure passing the relevant exam.

Network+, A+ Certification, and i-Net+ are trademarks of CompTIA in the United States and/or other countries. The i-Net+ Certification program logo is a registered trademark of CompTIA. All rights reserved.

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.

Photographs and illustrations used in this book have been downloaded from publicly accessible file archives and are used in this book for news reportage purposes only to demonstrate the variety of graphics resources available via electronic access. Text and images available over the Internet may be subject to copyright and other rights owned by third parties. Online availability of text and images does not imply that they may be reused without the permission of rights holders, although the Copyright Act does permit certain unauthorized reuse as fair use under 17 U.S.C. Section 107.

Copyright © 2000 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.

Library of Congress Card Number: 99-69307


Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1
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.

Customer Service Department

1151 Marina Village Parkway
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.

For my wife and daughter, without whom I could not write.

—David Groth

Acknowledgments
It takes many people to put a book together and this book is no exception. First, I would like to thank my coauthors, David Wall and Michael de Beer. They should be proud of the work they have done here. Thanks also to my technical editors, Robert Gradante and Don Fuller. They were responsible for making sure the information in this book is technically accurate and as up-to-date as possible.

This book would not have existed if not for the efforts of Linda Lee, this book’s developmental and acquisitions editor at Sybex. Thank you for putting up with all my phone calls and e-mails! Additionally, thanks go out to Rebecca Rider for her work as project editor and Judy Flynn for turning my collection of chicken-scratchings into a cohesive, useful study guide. The production department at Sybex also deserves my thanks. Thanks to Bill Gibson, electronic publishing specialist, for making this book look the way it does; to Leslie Higbee, production team leader, for making the production end of things run so smoothly; and to Molly Glover, proofreader, for her time reading every word.

I would also like to acknowledge my wife, family, and friends. My wife, Linda, tirelessly wrote and edited the appendices as well as kept me on the right track. She was a real trooper because she did it while taking care of our new daughter, Alison. Thanks to Alison, too, for being fussy when I needed a break (or when she thought I needed a break) or cute when I needed a laugh. Thank you to my family and friends who understood when I couldn’t do something because I had to work on the book. I really appreciate that.

Finally, I 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 the i-Net+ exam or this book, feel free to e-mail me at dgroth@corpcomm.net. All three of us worked very hard on this book to make it the best i-Net+ study guide available. I hope you agree that it is.

—David Groth

I’d like to thank the Sybex team for their support, especially Linda Lee, my acquisitions and developmental editor, for her insightful suggestions and guidance. Also, thanks goes to my coworkers at IGC, especially Steve Fram, Scott Weikart, and Marci Lockwood, who have all provided me with opportunities to deepen my understanding of the Internet.

—Michael de Beer

I would like to thank the hard-working staff at Sybex. Linda Lee, Judy Flynn, and Rebecca Rider provided editorial guidance, while Robert Gradante and Donald Fuller did a great technical edit. Bill Gibson did super layout and design work, while Leslie Higbee and Molly Glover put many hours of work into making this project flow smoothly. I also want to thank my family and friends, particularly Adam Bergman and Joy Kinsey, for their kindness and support.

—David Wall

Introduction

If you are like the rest of the networking community, you’ve probably taken certification exams. Becoming certified is one of the best things you can do for your career in the computer or networking field. It proves that you are knowledgeable in the area in which you are certified.

In this book, you’ll find out what the i-Net+ exam is all about. Each chapter covers part of the exam, and
at the end of each chapter, there are review questions to help you prepare for the exam.

What Is the i-Net+ Certification?

i-Net+ is a certification developed by the Computing Technology Industry Association (CompTIA). This organization exists to provide resources and education for the computer and technology community. This is the same body that developed the A+ and Network+ exams for computer and networking technicians. In 1997, members of CompTIA convened to develop a new certification that tests skills for Internet professionals. To ensure industry-wide support, it is sponsored by many IT industry leaders, including:

- Association of Internet Professionals
- IBM
- Microsoft
- Novell

The i-Net+ exam was designed to test the skills of Internet professionals who are responsible for implementing and maintaining Internet, intranet, and extranet infrastructure and services as well as development of related applications.

The exam tests areas of Internet technologies such as the TCP/IP protocol, the various types of servers, and the concepts of Internet design and implementation, such as which items are required for an easy-to-read Web site and the prerequisites for its installation. In addition, it covers troubleshooting concepts and various how-tos.

Why Become i-Net+ Certified?

As this book is being written, the i-Net+ certification is brand-new. But i-Net+ is the next certification in a line of CompTIA certifications, starting with A+ certification and Network+ certification. Because CompTIA is a well-respected developer of industry vendor-neutral certifications, getting i-Net+ certified indicates that you are competent in the specific areas tested by the exam.

Two major benefits are associated with becoming i-Net+ certified:

- Proof of professional achievement
- Opportunity for advancement

Proof of Professional Achievement

Networking professionals are competing these days to see who can get the most certifications. And technicians want the i-Net+ certification because it is broad, covering the entire field of Internet-related technical knowledge, rather than only development or security, for example. Thus, it can be a challenge to prepare for the i-Net+ exam. Passing the exam, however, certifies that you have achieved a certain level of knowledge about vendor-independent Internet-related subjects.
Opportunity for Advancement

We all like to get ahead in our careers. With advancement comes more responsibility, to be sure, but usually it means more money and greater opportunities. In the information technology area, this can usually be accomplished by obtaining multiple technology certifications, including i-Net+.

i-Net+, because of its wide-reaching industry support, is recognized as a base line of Internet and networking information. Some companies will specify that i-Net+ certification will result in a pay raise at review time. And some companies will specify that i-Net+ certification, in conjunction with A+ Certification, is required as a condition of employment before an employee’s next review.

How to Become i-Net+ Certified

The simplest way to find out how to become i-Net+ certified is to take the exam. It is administered by Sylvan Prometric, with which most of you are familiar if you have taken any other computer certification exams. It is administered by computer. To register to take the exam, call Sylvan (not the testing center) at 877-803-6867 and tell them you want to take the i-Net+ exam. You must pay for the exam at registration time with a major credit card (for example, Visa or MasterCard). The cost is $135 for CompTIA members and $185 for non-members. Special incentive pricing may be in effect when you take the exam—check CompTIA’s Web site for details.

Tip You can also register on the Internet through Sylvan Prometric at www.sylvanprometric.com or www.2test.com.

The exam itself consists of approximately 75 questions. You have 1 hour and 30 minutes for the test. At the end of the exam, your score report will be displayed on screen and printed so that you have a hard copy.

Who Should Buy This Book?

If you are one of the many people who want to pass the i-Net+ exam, you should buy this book and use it to study for the exam. The i-Net+ exam is designed for Internet professionals with six months of experience in a variety of entry-level, Internet-related technical job functions. This book was written with one goal in mind: to prepare you to pass the i-Net+ exam by describing in detail the concepts on which you’ll be tested.

How to Use This Book and CD

This book includes several features that will make studying for the i-Net+ exam easier. First, at the beginning of the book (right after this introduction, in fact) is an assessment test you can use to check your readiness for the actual exam. Take this test before you start reading the book. It will help you to determine the areas you may need to “brush up” on. You can then focus on those areas while reading the book. The answers to this test appear on a separate page after the last question. Each answer also includes an explanation and a note telling you in which chapter this material appears.

In addition, there are review questions at the end of each chapter. As you finish each chapter, answer the questions and then check your answers, which will appear on the page after the last question. If you answered any question(s) incorrectly, you’ll know that you may need some additional study in that particular area of the exam. You can go back and reread the section in the chapter that deals with each
question you got wrong to ensure that you “know your stuff.”

Appendix A includes a practice exam. Take this exam when you have finished reading all the chapters and answering all the review questions and you feel you are ready for the i-Net+ exam. Take the practice exam as if you were actually taking the i-Net+ exam (i.e., without any reference material). The answers to the practice exam can be found at the end of the test on the last page of Appendix A. If you get more than 90 percent of the answers correct, you’re ready to go ahead and take the real exam.

On the CD-ROM that is included with this book, there are several “extras” you can use to bolster your exam “readiness”:

**Electronic "flashcards"** You can use these 150 flashcard-style questions to review your knowledge of i-Net+ concepts on your PC. Additionally, you can download the questions into your Palm device (if you own one) for reviewing anywhere, anytime, without a PC!

**Test engine** This portion of the CD-ROM includes all of the questions that appear in the text of this book: the assessment questions at the end of this introduction, the chapter review questions, and the Practice Exam questions from Appendix A. In addition, it includes a set of bonus questions that only appear on the CD-ROM. The book questions will appear similarly to the way they did in the book, and they will also be randomized. This random test will allow you to pick a certain number of questions and will simulate an actual exam. Combined, these test engine elements will allow you to test your readiness for the “real” i-Net+ exam.

**Full text of the book** If you are going to travel but still need to study for the i-Net+ exam, and you have a laptop with a CD-ROM drive, you can take this entire book with you on the CD-ROM. The book is in PDF (Adobe Acrobat) format so it can be read easily on any computer.

### Conventions Used in This Book

To understand the way this book is put together, you must learn about a few of the special conventions we used. Following are some of the items you will commonly see.

**Italicized words** indicate new terms. After each italicized term, you will find a definition.

Lines formatted in this font refer to the output of a program. You will usually see several of these lines together indicating what the output of a text-based program usually looks like. This font is also used in Web addresses.

Tip **Tips** will be formatted like so. A tip is a special piece of information that can make either your work or your test-taking experience easier.

Note **Notes** are formatted with this symbol and this box. When you see a note, it usually indicates some special circumstance to make note of. Notes usually include information that is somewhat out of the ordinary and relates to the exam.

Warning **Warnings** are found within the text whenever there is a technical situation that arises that may cause damage to a component or cause a system failure of some kind. Additionally, warnings are placed in the text to call particular attention to a potentially dangerous situation.

Sidebars
Exam Objectives

The i-Net+ exam objectives were developed by a group of Internet industry professionals through the use of an industry-wide job task analysis. CompTIA asked groups of Internet professionals to fill out a survey rating the skills they felt were important in their jobs. The results were grouped into objectives for the exam. This section includes the outline of the exam objectives for the i-Net+ exam and the weight of each objective category.

Warning The objectives and weighting percentages given in this section can change at any time. Check CompTIA’s Web site at www.comptia.org for a list of the most current objectives.

i-Net Basics (10%)

1.1 Describe a URL, its functions and components, different types of URLs, and use of the appropriate type of URL to access a given type of server. Content may include the following:

- Protocol
- Address
- Port

1.2 Identify the issues that affect Internet site functionality (e.g., performance, security, and reliability). Content may include the following:

- Bandwidth
- Internet connection points
- Audience access
- Internet Service Provider (ISP)
- Connection types
- Corrupt files
- Files taking too long to load
- Inability to open files
1.3 Describe the concept of caching and its implications. Content may include the following:

- Server caching
- Client caching
- Proxy caching
- Cleaning out client-side cache
- Server may cache information as well
- Web page update settings in browsers

1.4 Describe different types of search indexes—static index/site map, keyword index, full-text index. Examples could include the following:

- Searching your site
- Searching content
- Indexing your site for a search

**i-Net Clients (20%)**

2.1 Describe the infrastructure needed to support an Internet client. Content could include the following:

- TCP/IP stack
- Operating system
- Network connection
- Web browser
- E-mail
- Hardware platform (PC, handheld device, WebTV, Internet phone)

2.2 Describe the use of Web browsers and various clients (e.g., FTP clients, Telnet clients, e-mail clients, all-in-one clients/universal clients) within a given context of use. Examples of context could include the following:

- When you would use each
- The basic commands you would use (e.g., put and get) with each client (e.g., FTP, Telnet)
2.3 Explain the issues to consider when configuring the desktop. Content could include the following:

- TCP/IP configuration (NetBIOS name server such as WINS, DNS, default gateway, subnet mask)
- Host file configuration
- DHCP versus static IP
- Configuring browser (proxy configuration, client-side caching)

2.4 Describe MIME types and their components. Content could include the following:

- Whether a client can understand various e-mail types (MIME, HTML, uuencode)
- The need to define MIME file types for special download procedures such as unusual documents or graphic formats

2.5 Identify problems related to legacy clients (e.g., TCP/IP sockets and their implication on the operating system). Content could include the following:

- Checking revision date, manufacturer/vendor
- Troubleshooting and performance issues
- Compatibility issues
- Version of the Web browser

2.6 Explain the function of patches and updates to client software and associated problems. Content could include the following:

- Desktop security
- Virus protection
- Encryption levels
- Web browsers
- E-mail clients

2.7 Describe the advantages and disadvantages of using a cookie and how to set cookies. Content could include the following:

- Setting a cookie without the knowledge of the user
- Automatically accepting cookies versus query
- Remembering everything the user has done
Security and privacy implications

Development (20%)

3.1 Define programming-related terms as they relate to Internet applications development. Content could include the following:

- API
- CGI
- SQL
- SAPI
- DLL—dynamic linking and static linking
- Client and server-side scripting

3.2 Describe the differences between popular client-side and server-side programming languages. Examples could include the following:

- Java
- JavaScript
- Perl
- C
- C++
- Visual Basic
- VBScript
- JScript
- XML
- VRML
- ASP

Content could include the following:

- When to use the languages
- When they are executed
3.3 Describe the differences between a relational database and a non-relational database.

3.4 Identify when to integrate a database with a Web site and the technologies used to connect the two.

3.5 Demonstrate the ability to create HTML pages. Content could include the following:

- HTML document structure
- Coding simple tables, headings, forms
- Compatibility between different browsers
- Difference between text editors and GUI editors
- Importance of creating cross-browser coding in your HTML

3.6 Identify popular multimedia extensions or plug-ins. Examples could include the following:

- QTVR (QuickTime VR)
- Flash
- Shockwave
- RealPlayer
- Windows Media Player

3.7 Describe the uses and benefits of various multimedia file formats. Examples could include the following:

- GIF
- GIF89a
- JPEG
- PNG
- PDF
- RTF
- TIFF
- PostScript
- EPS
3.8 Describe the process of pre-launch site/application functionality testing. Content could including the following:

- Checking hot links
- Testing different browsers
- Testing to ensure it does not corrupt your e-commerce site
- Load testing
- Access to the site
- Testing with various speed connections

**Networking (25%)**

4.1 Describe the core components of the current Internet infrastructure and how they relate to each other. Content may include the following:

- Network access points
- Backbone

4.2 Identify problems with Internet connectivity from source to destination for various types of servers. Examples could include the following:

- E-mail
- Slow server
- Web site

4.3 Describe Internet domain names and DNS. Content could include the following:
DNS entry types
Hierarchical structure
Role of root domain server
Top level or original domains—edu, com, mil, net, gov, org
Country level domains—UK

4.4 Describe the nature, purpose, and operational essentials of TCP/IP. Content could include the following:
- What addresses are and their classifications (A, B, C, D)
- Determining which ones are valid and which ones are not (subnet masks)
- Public versus private IP addresses

4.5 Describe the purpose of remote access protocols. Content could include the following:
- SLIP
- PPP
- PPTP
- Point-to-point/multipoint

4.6 Describe how various protocols or services apply to the function of a mail system, Web system, and file transfer system. Content could include the following:
- POP3
- SMTP
- HTTP
- FTP
- NNTP (news servers)
- TCP/IP
- LDAP
- LPR
- TELNET
4.7 Describe when to use various diagnostic tools for identifying and resolving Internet problems. Content could include the following:

- Ping
- winipcfg
- ipconfig
- ARP
- Trace Routing Utility
- Network Analyzer
- netstat

4.8 Describe hardware and software connection devices and their uses. Content could include the following:

- Network interface card
- Various types of modems including analog, ISDN, DSL, and cable
- Modem setup and commands
- Adapter
- Bridge
- Internet-in-a-box
- Cache-in-a-box
- Hub
- Router
- Switch
- Gateway
- NOS
- Firewall

4.9 Describe various types of Internet bandwidth technologies (link types). Content could include the
following:

- T1/E1
- T3/E3
- Frame Relay
- X.25
- ATM
- DSL

4.10 Describe the purpose of various servers—what they are, their functionality, and features. Content could include the following:

- Proxy
- Mail
- Mirrored
- Cache
- List
- Web (HTTP)
- News
- Certificate
- Directory (LDAP)
- E-commerce
- Telnet
- FTP

**i-Net Security (15%)**

5.1 Define the following Internet security concepts: access control, encryption, auditing and authentication, and provide appropriate types of technologies currently available for each. Examples could include the following:

- Access control: Access Control List, firewall, packet filters, proxy
Authentication: Certificates, digital signatures, nonrepudiation

Encryption: public and private keys, Secure Sockets Layer (SSL), S/MIME, digital signatures, global versus country-specific encryption standards

Auditing: Intrusion detection utilities, log files, auditing logs

SET (Secure Electronic Transactions)

5.2 Describe VPN and what it does. Content could include the following:

- VPN in encrypted communications
- Connecting two different company sites via an Internet VPN (extra net)
- Connecting a remote user to a site

5.3 Describe various types of suspicious activities. Examples could include the following:

- Multiple login failures
- Denial of service attacks
- Mail flooding/spam
- Ping floods
- SYN floods

5.4 Describe access security features for an Internet server (e.g., e-mail server, Web server). Examples could include the following:

- User name and password
- File level
- Certificate
- File-level access: read, write, no access

5.5 Describe the purpose of antivirus software and when to use it. Content could include the following:

- Browser/client
- Server

5.6 Describe the differences between the following as they relate to security requirements:

- Intranet
Business Concepts (10%)

6.1 Explain the issues involved in copyrighting, trademarking, and licensing. Content could include the following:

- How to license copyright materials
- Scope of your copyright
- How to copyright your material anywhere
- Consequences of not being aware of copyright issues and not following copyright restrictions

6.2 Identify the issues related to working in a global environment. Content could include the following:

- Working in a multivendor environment with different currencies, etc.
- International issues—shipping, supply chain
- Multilingual or multicharacter issues (Unicode)
- Legal and regulatory issues

6.3 Define the following Web-related mechanisms for audience development (i.e., attracting and retaining an audience):

- Push technology
- Pull technology

6.4 Describe the differences between the following from a business standpoint:

- Intranet
- Extranet
- Internet

6.5 Define e-commerce terms and concepts. Content could include the following:

- EDI
- Business to business
- Business to consumer
Internet commerce
Merchant systems
Online cataloging
Relationship management
Customer self-service
Internet marketing

How to Contact the Authors

If you have any questions while you are reading this book, feel free to contact any of the authors. David Groth can be reached via e-mail (the best way to reach him) at dgroth@corpcomm.net. Michael de Beer can be reached at madebeer@igc.org, and David Wall can be reached at david@davidwall.com.

Test-Taking Tips

The i-Net+ exam is a new standard (as this book is being written) and should gain wide acceptance among Internet professionals. Remember a few things when taking your test:

- Get a good night’s sleep the night before.
- Take your time on each question. Don’t rush it.
- Arrive at the testing center a few minutes early so that you can review your notes.
- Answer all questions, even if you don’t know the answer. (Unanswered questions are considered wrong.)
- If you don’t know the answer to a question, mark it and come back to it later.
- Read each question twice and make sure you understand it.

Good luck on your i-Net+ exam and in your future in the Internet industry.

Assessment Test

1. How does a certificate differ from a public key?
   A. A certificate is itself encrypted.
   B. A certificate is necessarily issued by an independent authority.
   C. A certificate has a time limit.
   D. A certificate does not change over time.
2. What is not true about installing an update?
   A. It can corrupt your system.
   B. It can close important security holes in your desktop security.
   C. Updates must be installed in every case.
   D. It can provide added functionality.

3. Which is true of full-text reverse indexes?
   A. They really shine for sites that update infrequently.
   B. They are primarily governed by ROBOTS.TXT spider rules.
   C. They speed queries.
   D. They provide concept-based functionality.

4. Copyright law provides protection for software but allows for _______.
   A. Limited use
   B. Educational use
   C. Nonprofit use
   D. Fair use

5. The test server is a Pentium-100 with 500MB of RAM running Apache on Linux. Each child of
   the Web server uses 5MB of RAM. The server has a dedicated T1 line and serves an unlimited
   number of clients that download its 100K static pages at 10 K/s. Given this test server, at what
   rate of incoming requests will the Web server start increasing its queue length?
   1. 2
   2. 6
   3. 11
   4. 16

6. Which networking component requests resources from a server?
   A. Workstation
   B. Server
   C. Router
   D. Firewall

7. What is Microsoft’s modular software architecture called?
   A. Object-orientation
B. C++

C. The Microsoft Foundation Classes (MFC)

D. The Component Object Model (COM)

8. Which component of a Web browser contains all the menus for the program?
   A. Button bar
   B. Menu bar
   C. Status Bar
   D. Activity indicator

9. One difference between patent and copyright is _______.
   A. Patent protection is available only in the United States.
   B. There is no implicit patent; you must apply for and be granted one.
   C. Two independent inventors of a product or process may both enjoy patents on it.
   D. Copyright does not allow for corporate ownership.

10. What do HTTP response codes in the 4 xx range mean?
    A. There has been a server error.
    B. There has been a client error.
    C. The request has been redirected.
    D. Everything went as planned.

11. During an SMTP communications session, which command does the sender use to indicate to the server that it is ready to send the body of the message?
    A. PUT
    B. rcpt to
    C. body
    D. HELO

12. Of the people who view a banner ad, the percentage that follow its link to an advertiser’s site is called _______.
    A. The clickthrough rate
    B. The passthrough rate
C. The yield

D. The drawing power

13. How many host IP addresses are available with the CIDR designation /21?
   A. 128
   B. 1,024
   C. 2,046
   D. 9,128

14. What is not true about installing an update?
   A. It can corrupt your system.
   B. It can close important security holes in your desktop security.
   C. Updates must be installed in every case.
   D. It can provide added functionality.

15. True or false. Telnet servers are somewhat of a security risk.
   A. True
   B. False

16. True or False. X.25 is a WAN transmission method.
   A. True
   B. False

17. Virtual shopping cart services are a function of which type of HTTP server?
   A. Internet
   B. Intranet
   C. FTP
   D. E-commerce

18. If someone claims she got an error message on your site, what is the first thing you should do?
   A. Ask her to try again and give you the exact error message.
   B. Look in the access log for verification that she went to your server.
   C. Check to see if the server is up.
   D. Ask remote staff to check the firewall connectivity.
19. True or False. You must have a PC in order to browse the Internet?
   A. True
   B. False

20. Which part of the URL http://www.novell.com/index.html is the actual DNS name of the server being accessed?
   A. http://
   B. www.novell.com
   C. index.html
   D. novell

21. What is the program that interprets Java programs called?
   A. The Java Interpreter
   B. The Java Compiler
   C. The Java Virtual Machine
   D. The Java Grinder

22. True or False. You can use Telnet to access the console of a Unix host?
   A. True
   B. False

23. When browsing the Internet with a Web browser, what is the text that links you to another page on the Web called?
   A. Hypertext
   B. Hyperlink
   C. Hyperactive
   D. Hyperbole

24. True or False. Before assigning any IP address, you must apply for a registered IP address from either the IANA or your ISP.
   A. True
   B. False.

25. Which of the following is not needed before transferring a file from an FTP server using an FTP client?
   A. FTP Server name
   B. DNS MX record
C. username

D. password

26. Dynamic packet filtering relies upon _______.
   A. Blocking certain kinds of traffic, like ICQ transmissions
   B. Requiring packets inbound from the Internet to pass through a firewall
   C. Tracking open TCP/IP connections and only allowing the packets related to those transmissions to pass through in sequence
   D. Detecting multiple login attempts

27. What is the default subnet mask for a Class B address?
   A. 255.255.0.0
   B. 0.0.0.0
   C. 255.255.255.0
   D. 255.0.0.0

28. Access control measures limit the damage that can be done by an attacker. How do they do this?
   A. By making brute force attacks more difficult
   B. By imposing an extra layer of password protection
   C. By encrypting stored data en masse
   D. By giving users of a computer access only to those resources they need to access in order to do their jobs

29. What should people doing quality control on a Web site look for?
   A. Pages that look ugly and don’t work visually
   B. Conformity with the storyboard
   C. Anything on their checklist
   D. Functionality errors only

30. A tunneling protocol is used to facilitate _______.
   A. Secure e-commerce
   B. Firewalls
   C. Dial-up Internet connections
31. The process of establishing a relationship between two tables in a relational database is called doing a _____.
   A. Link
   B. Join
   C. Pivot
   D. Combo

32. Which two network utilities are the most similar?
   A. Ping and winipcfg
   B. ARP and tracert
   C. Ping and tracert
   D. Ping and ARP

33. QUALCOMM Eudora is an example of a ______ client.
   A. Mail
   B. Web
   C. FTP
   D. Telnet

34. A database management system (DBMS) is primarily responsible for what?
   A. Storing data in a database and handling queries sent to it
   B. Backing up a database
   C. Integrating a database with the Internet
   D. Providing Perl support

35. When planning the content of a Web site, it is most important to _____.
   A. Use the latest technologies so the site won't need to get reinvented soon.
   B. Only use technologies that won't be roadblocks for potential users.
   C. Follow the local policy, based on the goals of the site and the audience profile.
   D. Choose technology the development team enjoys and is good at.

36. An object is likely to be in a cache if _____.
A. The object was requested a long time ago.
B. The object is fresh; it was requested just before the cache was last cleared.
C. The object has high value because it has never before been requested.
D. The object has been requested recently.

37. Licensing always allows for ______ .
   A. One party’s use of another party’s copyrighted material under certain terms
   B. A payment of money to the copyright holder
   C. A limited period of use
   D. Mandatory review of the terms by a judge

38. If you want to buy your sister either black high heels or purple tennis shoes, which query will be most useful?
   A. A full-text search for “black high heels or purple tennis shoes”
   B. A keyword search for “black high heels or purple tennis shoes”
   C. A full-text search for (black and “high heels”) or (purple and “tennis shoes”)
   D. A keyword search for “high heels or sneakers”

39. What do HTTP response codes in the 4xx range mean?
   A. There has been a server error.
   B. There has been a client error.
   C. The request has been redirected.
   D. Everything went as planned.

40. Which Internet access link technology is a point-to-point link that sends digital signals over the standard POTS phone lines installed in most homes, is inexpensive, but is not widely available in all areas as yet?
   A. Frame Relay
   B. T1
   C. DSL
   D. ATM

41. A company that receives income from products it sells to foreign nationals is ______ .
   A. Not liable for taxes on the income in its home country
B. Usually responsible for paying duties on services provided over the Internet
C. Liable for taxes on the income in its home country
D. Usually eligible for special tax benefits

42. __________ servers allow Internet clients to search for people along with their addresses and phone numbers.
   A. Proxy
   B. FTP
   C. NNTP
   D. LDAP

43. Which T-series Internet bandwidth technology has a maximum throughput of 1.544Mbps?
   A. T1
   B. T2
   C. T3
   D. T4

44. Which FTP command produces the output “Type set to A”?
   A. put
   B. ascii
   C. get
   D. ls

45. True or False. The POP3 protocol is used to send e-mail between Internet e-mail servers.
   A. True
   B. False

46. Netscape’s server-side scripting language, LiveScript, is similar to _____.
   A. VBScript.
   B. JavaScript.
   C. Perl.
   D. Java.

47. Access Control Lists (ACLs) are built into routers. They serve to ______.
A. Define who may access a system
B. Support the operations of a proxy server
C. Prevent SYN floods
D. Determine which machines may send packets in which direction over the router

Answers to Assessment Test

1. C. A certificate guarantees that someone is who he or she claims to be but guarantees its validity for only a certain time period. For more information on certificates, see Chapter 7.

2. C. Updates have both benefits and risks. The cost and benefit need to be weighed, so installing an upgrade is not required. For more information on patches and updates, see Chapter 10.

3. C. The table mapping words to files allows direct lookups on where a word is used. For more information about searching and indexing, see Chapter 9.

4. D. The doctrine of fair use describes circumstances in which someone may use copyrighted material without explicit permission. For more information of fair use, see Chapter 11.

5. C. If there are 100 processes, and each finishes serving a request every 10 seconds, 10 requests a second will be fulfilled. At 11 requests a second, one request is added to the queue every second. For more information about planning server capacity and performance, see Chapter 9.

6. A. Of all the components listed, workstations are the only ones to request resources (e.g., files, information). For more information on servers, see Chapter 1.

7. D. The Component Object Model (COM) allows for modularity in Windows code. For more on COM, see Chapter 8.

8. B. The menu bar is the only component of a Web browser that contains the menus for the program. The button bar contains all the control buttons for browsing, the status bar shows the status of the browsing session, and the activity indicator shows that Internet activity is occurring. For more information on Web browser components, see Chapter 5.

9. B. You must apply for and be granted a patent in order to be able to defend an invention from infringement. For more information on patents, see Chapter 11.

10. B. The client could be asking for a file that is forbidden or does not exist. For more on HTTP response codes, see Chapter 10.

11. C. PUT is used for HTTP requests, rcpt to indicates the message recipient, and HELO starts the communications session. For more information on the SMTP communications process, refer to Chapter 2.

12. A. The percentage of ad viewers that choose to visit the underlying site is called the clickthrough rate. For more information on the clickthrough rate, see Chapter 11.
13. C. /21 indicates that there are 21 bits used for the network address of an IP address and that there are 11 bits left over for host addresses, corresponding to a decimal number of 2,048 (subtract 2 for addresses with all 0s and all 1s, leaving 2,046). For more information on CIDR, see Chapter 3.

14. C. Updates have both benefits and risks. The cost and benefit need to be weighed, so installing an upgrade is not required. For more information on patches and updates, see Chapter 10.

15. A. Because you are giving a user from the Internet access to the server console, the user could theoretically run unauthorized programs. For more information on Telnet servers, see Chapter 4.

16. B. Actually, X.25 is an access method and assumes that a path from sender to receiver exists. For more information on X.25, see Chapter 1.

17. D. E-commerce servers provide virtual shopping cart services to help customers shop online. For more information on e-commerce servers, see Chapter 4.

18. A. You need to find out exactly what she claims to be experiencing before you can test the problem. For more information on troubleshooting, see Chapter 10.

19. B. False. It is also possible to use an Internet appliance. See Chapter 5 for more on Internet appliances.

20. B. A is the protocol, C is the name of the resource being accessed, and D doesn’t represent a specific part of a URL. For more information on URLs, refer to Chapter 2.

21. C. The Java Virtual Machine (JVM) interprets Java programs. For more on Java, see Chapter 8.

22. A. True. The primary function of Telnet is to access the console of a Unix host. For more information on Telnet, see Chapter 5.

23. B. A Hyperlink is a line of text that, when clicked, will take you to another page. For more information on hyperlinks, see Chapter 6.

24. B. You don’t have to apply for a registered IP address if your network isn’t connected to the Internet. For more information on registered IP addresses, refer to Chapter 3.

25. B. For more information on FTP client, see Chapter 6.

26. C. Dynamic packet filtering keeps track of open connections and prevents people from breaking in while transmissions are in progress. For more information on dynamic packet filtering, see Chapter 7.

27. A. 255.255.255.0 is for a Class C address, and 255.0.0.0 is for a Class A address. For more information on default masks, see Chapter 3.

28. D. Access control measures limit the resources available to individual users, meaning that even if they get into the system, they can only do a certain degree of damage. For more information on access control measures, see Chapter 7.

29. B and C. Each site should establish a testing methodology, including a list of bugs to check for.
For more information about testing a site before rolling it out to the public, see Chapter 10.

30. D. Tunneling protocols encapsulate VPN data in Internet packets, using encryption to keep it secure. For more information on tunneling protocols, see Chapter 7.

31. B. To establish a relationship between two tables in a relational database is to do a join. For more on relational databases, see Chapter 8.

32. C. Ping and tracert both send packets to a destination host. Ping is used primarily to see if the host will respond. You could use tracert for a similar job, but it is better suited to seeing the path to a host. For more information on troubleshooting utilities, see Chapter 10.

33. A. Eudora is one of the many Internet mail clients available. It doesn’t perform any other of the functions listed. For more information on mail clients, see Chapter 5.

34. A. Though DBMSes may do the other tasks listed, their primary job is to store data and allow users to access it. For more on DBMSes, see Chapter 8.

35. C. Although all enjoy some truth, B is most likely to lead to a successful Web site. For more information about planning which content types to use on a Web site, see Chapter 9.

36. D. The object has been put into the cache by a recent request. Because it is recent, it is likely it hasn't expired in the cache or been pushed out by other cached content. For more information about caching, see Chapter 9.

37. A. Licensing is one party’s use of another party’s copyrighted material under certain terms, which may or may not be granted in exchange for payment.

38. C. The full-text search will look through the details of more pages. The search terms will not find purple high heels or black tennis shoes. For more information on searching, see Chapter 9.

39. B. The client could be asking for a file that is forbidden or does not exist. For more on HTTP response codes, see Chapter 10.

40. C. Of the answers listed, only DSL is inexpensive and not widely available in all areas. For more information on Internet access link technologies, see Chapter 1.

41. C. The income you receive from foreign customers is taxable income like any other. For more information on this subject, see Chapter 11.

42. D. Of all the types listed, only LDAP servers (such as www.switchboard.com) facilitate searching for people and their phone numbers. For more information on directory servers, see Chapter 4.

43. A. T1 is 1.544Mbps, T3 is 44.736Mbps, and T2 and T4 are actually valid T-series connections, but they aren’t widely used and discussed in Internet circles. For more information on T-series Internet bandwidth technologies, see Chapter 1.

44. B. The ascii command changes the file type to A and thus produces the specified output. The others all produce different outputs. For more information on FTP use, see Chapter 6.
45. B. SMTP is used for this purpose. For more information on POP3 and SMTP, refer to Chapter 2.

46. B. LiveScript sometimes is called “server-side JavaScript.” For more on scripting languages, see Chapter 8.

47. D. ACLs determine which machines can send packets to what machines over a router. An ACL might allow local machines to send packets out to the Internet but allow inbound traffic only in response to a request. For more information on Access Control Lists, see Chapter 7.

Chapter 1: i-Net+ Networking Basics

Overview

i-Net+ Exam Objectives Covered in This Chapter:

- **Describe hardware and software connection devices and their uses. Content could include the following:**
  - Network interface card
  - Various types of modems including analog, ISDN, DSL, and cable
  - Modem setup and commands
  - Adapter
  - Bridge
  - Internet-in-a-box
  - Cache-in-a-box
  - Hub
  - Router
  - Switch
  - Gateway
  - NOS
  - Firewall

- **Describe various types of Internet bandwidth technologies (link types). Content could include the following:**
  - T1/E1
  - T3/E3
By most accounts, the Internet is a big network. It contains many of the same components as any corporate network. To that end, before discussing the Internet, it is helpful to understand some of the basic components and concepts of a network. Many of the concepts involved in understanding networks will cross over to understanding the inner workings of the Internet. This chapter will introduce you to some of the more common networking topics you must understand when working with Internet technologies. Some of those topics include definitions of servers and protocols, hardware and software connection devices, and the various bandwidth technologies used to connect Internet sites to one another. This chapter will introduce you to these and other networking components and concepts so that you may have a better understanding of the Internet’s underpinnings.

What Is a Network?

In the computer world, the term network describes two or more connected computers that can share a resource such as data, a printer, an Internet connection, applications, or a combination of these. Today, networks can be classified into two main types:

- Local area network (LAN)
- Wide area network (WAN)

The type used depends on the number of computers (and people) who need access, the geographical and physical layout of the enterprise, and of course, financial resources. In this section, we’ll discuss each type and describe the situation that is most appropriate for its use.

Local Area Network (LAN)

By definition, a local area network, or 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 to 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 who share the same files and databases over the LAN, such as, for example, the sales department. Figure 1.1 shows an example of a LAN and its workgroups.
Theoretically, a LAN could connect a maximum of 1,024 computers at a maximum distance of 900 meters (around 2,700 feet, assuming thinnet cable is used). These figures are based on using one area of the network for the majority of network traffic (in what is known as a backbone configuration), other network areas (called segments) connecting workstations to the main cabling portion using special devices to extend the overall range of the network, and finally, very light network traffic. If you use a different type of cabling, these maximums decrease to 30 computers, with the most distant computer connected at a maximum of 100 meters (about 300 feet) from a central point.

Cabling Topologies

As shown in Figure 1.1, network cabling can be laid out in many different ways. The specific way network cables are arranged is known as the cabling topology. There are four main types: bus, star, ring, and mesh. A bus topology connects all computers to a single cable. In a bus topology, the network cable run starts at one computer and goes to the next, then to the next, and so on. A star topology, on the other hand, has cable runs from each device on the network to a central device (known as a hub). Although not very common, ring topologies connect each computer to two others to form a ring. Finally, a mesh topology connects every computer directly to every other computer. In mathematical terms, if there were \( n \) computers, there would be \( n \times (n-1)/2 \) cables in a mesh topology.

Wide Area Network (WAN)

Chances are, you are an experienced WAN user and didn’t know it. If you have ever connected to the Internet, you have used the largest WAN on the planet. A wide area network, or 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.
- LANs are limited in size and scope; WANs are not.
- WANs can be connected on demand or can be permanently connected. LANs have permanent
connections between stations.

- WANs can use public or private network transports. LANs primarily use private network transports.

The Internet is actually a specific type of WAN. It is a collection of networks that are interconnected and is therefore 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*.

**Network Hardware Components**

Networks are made up of many entities, both hardware and software. Each hardware device on the network has a different function to perform. In this section, you will learn about some of these devices and the specific functions they perform.

**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)* that are available to users. In the network environment, the term *workstation* normally refers to any computer connected to the network and used by a user to do work.

Note It is important to distinguish between workstations and clients. A client is any network entity that can request resources of 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 its 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*, which you will learn about later in this chapter.

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 and uses the Hypertext Transfer Protocol (HTTP) to deliver them.

**Mail server** Hosts and delivers e-mail. It is 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** Hosts modems for inbound requests to connect to the network. Remote access servers provide remote users (working at home or on the road) with a connection to the network.

**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(s) each server plays, they all (should) have the following in common:

1. Hardware and/or software for data integrity (such as backup hardware and software)
2. The ability to support a large number of clients

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.

Warning 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.

![Sample Network Diagram](image)

Figure 1.2: A sample network including servers and workstations Specific types of Internet servers will be discussed in more detail in Chapter 4.

**The Network Interface Card (NIC)**

The *network interface card (NIC)*, as its name suggests, is the device in your computer that connects (interfaces) your computer to the network. This device provides the physical, electrical, and electronic connections to the network media. It is responsible for converting the information your computer needs to send to the network into the special electrical signals for the type of network technology your network
uses. Also occasionally called a network adapter, a NIC is either an expansion card (the most popular implementation) or built into the motherboard of the computer. Figure 1.3 shows a sample NIC.

![Figure 1.3: A sample NIC](image)

In most cases, a NIC must be added to the computer. It is usually installed into some kind of expansion slot on the computer's motherboard. In some notebook computers, NIC adapters can be connected to the printer port or through a built-in PC card slot.

Note In order to be used on a network, the NIC must have at least one protocol bound to it within the operating system. Binding a protocol means to logically associate a particular protocol with that instance of a NIC within an operating system so that the OS can communicate with the rest of the network using that protocol.

The important thing to remember when buying a NIC for your computer is to buy one that not only matches the bus type in your computer, but also matches the type of network you have. It sounds rather obvious, but you can’t get a Token Ring card to communicate on an Ethernet network, no matter how hard you try. It just won’t work because a Token Ring NIC wasn’t designed to work on an Ethernet network. The electrical signals are in a completely different format.

One other thing to remember about NIC cards: All NIC cards contain a “burned-in” address (sometimes known as the hardware address, or MAC address) from the manufacturer. This address is used at the header of a packet to identify a node on the network. This address, in most NICs, cannot be changed.

**Network Cables**

Although it is possible to use several forms of wireless networking, such as radio and infrared, most networks communicate via some sort of cable. Although the i-Net+ exam doesn’t test you on cabling technologies, it is important that we at least make an attempt to discuss network cabling because, without cabling, the network has no pathway to transmit data. In this section, we’ll look at three types of cables commonly found in LANs:

- Coaxial
- Twisted-pair
Fiber-optic

Coaxial Cable

Coaxial cable (or coax) contains a center conductor made of copper and surrounded by a plastic jacket, with a braided shield over the jacket (as shown in Figure 1.4). A plastic such as either PVC or Teflon covers this metal shield. The Teflon-type covering is frequently referred to as a plenum-rated coating. That simply means that the coating does not produce toxic gas when burned and is rated for use in air plenums that carry breathable air. This type of cable is more expensive but may be mandated by electrical code whenever cable is hidden in walls or ceilings.

Figure 1.4: Construction of a coaxial cable

Coaxial cable is available in different specifications that are rated according to the RG Type system. Different cables have different specifications and, therefore, different RG grading designations (according to the U.S. military specification MIL-C-17). Distance and cost are considerations when selecting coax cable. The thicker the copper, the farther a signal can travel—and with that comes higher costs and a less-flexible cable.

There are two main categories of coaxial cable, Thick Ethernet (or thicknet) and Thin Ethernet (or thinnet). The primary difference between the two is the diameter of the cable and the distance they can carry a signal in a single segment. Thinnet coaxial can carry a signal 185 meters in a single segment, and thicknet can carry a signal 500 meters in a single segment. Thicknet cable has approximately the same diameter as a small garden hose and is difficult to bend. Thinnet cable, on the other hand, has approximately the same diameter as a pencil, is much more flexible, and thus easier to install. Of the two, thinnet is much more common in newer installations.

The main consideration with the installation of coaxial cable is the phenomenon of signal bounce. With coaxial cable, the signal travels up and down the entire length of the wire. When the signal reaches the end of the wire, the electrical change from copper to air prevents the conversation from simply falling out the end. So the signal bounces back down the wire it just traversed. This creates an echo, just as if you were yelling into a canyon. These additional signals on the wire make communication impossible. To prevent this, you must place a terminator on each end of the wire to absorb the unwanted echo.

Warning Proper termination requires that one terminator be connected to a ground. Connecting both terminators to a ground can create a ground loop, which can produce all kinds of bizarre, ghostlike activity, for example, a network share that appears and disappears.

Coaxial cable primarily uses BNC connectors. BNC has many definitions in the computer world. Some think British Naval Connector, citing its origins. Others would say Bayonet Nut Connector, after its function. Still others would say Bayonet Neill Concelman, after its authors. Suffice it to say, it’s just easier to call it a BNC connector and know that it’s used on 10Base-2 Ethernet connections to RG-58 cable.
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 with no outer shielding, called *unshielded twisted-pair (UTP)*. UTP is commonly used in 10BaseT, star-wired networks.

The wires in twisted-pair cable are twisted to minimize electromagnetic interference. When electromagnetic signals are conducted on copper wires that are in close proximity (such as inside a cable), some electromagnetic interference occurs. In cabling parlance, 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, the more common type of twisted-pair cable, is rated in the following categories:

- **Category 1** Two twisted-pair (4 wires). Voice grade (not rated for data communications). This is the oldest category of UTP and it is 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).
- **Category 2** Four twisted-pair (8 wires). Suitable for up to 4Mbps.
- **Category 3** Four twisted-pair (8 wires), with three twists per foot. Acceptable for 10Mbps. A popular cable choice for a long time.
- **Category 4** Four twisted-pair (8 wires) and rated for 16Mbps.
- **Category 5** Four twisted-pair (8 wires) and rated for 100Mbps.
- **Category 6** Four twisted-pair (8 wires) and rated for 1000Mbps. (Became a standard in December 1998.)

Frequently, you will hear *Category* shortened to *Cat*. Today, any cable that you install should be a minimum of Cat 5. We say “a minimum” because some cable is now certified to carry a bandwidth signal of 350MHz or beyond. This allows unshielded twisted-pair cables to reach a speed of 1Gbps, which is fast enough to carry broadcast-quality video over a network.

UTP cables use RJ (Registered Jack) connectors rather than BNC connectors. The connector used with UTP cable is called RJ-45, which is similar to the RJ-11 connector used on most telephone cables, except RJ-45 is larger. The RJ-11 has 4 wires, or 2 pair, and the network connector RJ-45 has 4 pair, or 8 wires.
Signaling Methods

How much of a cable’s available bandwidth (overall capacity, such as 10Mbps) is used by each signal depends on whether the signaling method is baseband or broadband. Baseband uses the entire bandwidth of the cable for each signal (using one channel). It is typically used with digital signaling.

In broadband, multiple signals can be transmitted on the same cable simultaneously by means of frequency division multiplexing (FDM). Multiplexing is dividing a single medium into multiple channels. With FDM, the cable’s band width is divided into separate channels (or frequencies), and multiple signals can traverse the cable on these frequencies simultaneously. FDM is typically used for analog transmissions. Another method, time division multiplexing (TDM), can also be used to further divide each individual FDM frequency into individual time slots. Additionally, TDM can be used on baseband systems.

Fiber-Optic Cable

If your data runs are measured in kilometers, or if you have gigabits of data to move each second, fiber-optic is your cable of choice because copper cannot reach more than 500 meters (around 1600 feet—that’s six football fields to you and me) without electronics regenerating the signal. Additionally, fiber-optic is the only cabling technology that can support the high data transfer speeds that the backbone of the Internet requires. 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. The most common use of fiber-optic cable these days is for high-speed telephone lines.

Note Ethernet running at 10Mbps over fiber-optic cable is normally designated 10BaseF; the 100Mbps version of this implementation is 100BaseFX.

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

The pros are as follows:

- It’s completely immune to EMI or RFI.
- It can transmit up to 4 kilometers.

Here are the cons:

- It’s difficult to install.
- It requires a bigger investment in installation and materials.

Fiber-optic technology was initially very expensive and difficult to work with, but it is now being installed in more and more places. Some companies with high bandwidth requirements plan to bring fiber-optic speeds to the desktop.

The Hub

After the NIC, a hub is probably the next most common device found on networks today. A hub (also called a concentrator) serves as a central connection point for several network devices. At its basic
level, a hub simply repeats everything it receives on one port to all the other ports on the hub, thus providing a communication pathway for all stations connected to it. Figure 1.5 shows an example of a hub.

![Figure 1.5: A standard hub](image)

Hubs are found on every twisted-pair Ethernet network, including those found at ISPs. Hubs are used to connect multiple network devices together. ISPs may have several Internet servers connected to a hub, which is in turn connected to the ISP’s Internet connection, allowing the servers to communicate with each other as well as with the Internet.

There are many classifications of hubs, but two of the most important are active and passive:

- An active hub is electrically powered and actually amplifies and cleans up the signal it receives, thus doubling the effective segment distance limitation for the specific topology (for example, extending an Ethernet segment another 100 meters).

- A passive hub typically is unpowered and makes only physical, electrical connections. Normally, the maximum segment distance of a particular topology is shortened because the hub takes some power away from the signal strength in order to do its job.

**The Switch**

In the past few years, the *switching hub* has received a lot of attention as a replacement for the standard hub. The switching hub is more intelligent than a standard hub in that it can actually understand some of the traffic that passes through it. A switching hub (or *switch* for short) listens to all the stations connected to it and records their network cards’ hardware addresses (see Figure 1.6). Then, when one station on a switch wants to send data to a station on the same switch, the data gets sent directly from the sender to the receiver. This is different from the way hubs operate. Hubs, if you will remember, don’t care what stations are connected and simply repeat anything they receive on one port out to all the other ports. Because of this difference, there is much less overhead on the transmissions and the full bandwidth of the network can be used between sender and receiver.

Switches have received a lot of attention because of this ability. If a server and several workstations were connected to the same 100Mbps Ethernet switch, each workstation would need a dedicated 100Mbps channel to the server, and there would never be any collisions.
Figure 1.6: A switch builds a table of all addresses of all connected stations.

The Bridge

A bridge is a network device, operating at the Data Link layer of the Open Systems Interconnection (OSI) model, that logically separates a single network into two segments but lets the two segments appear to be one network to connected workstations. The primary use for a bridge is to keep traffic meant for stations on one side on that side of the bridge and not let it pass to the other side. For example, if you have a group of workstations that constantly exchange data on the same network segment as a group of workstations that don’t use the network much, the busy group will slow down the performance of the network for the other users. If you put in a bridge to separate the two groups, only traffic destined for a workstation on the other side of the bridge will pass to the other side. All other traffic stays local. Figure 1.7 shows a network before and after bridging. Notice how the network has been divided into two segments; traffic generated on one side of a bridge will never cross the bridge unless a transmission has a destination address on the opposite side of the bridge.

Figure 1.7: A sample network before and after bridging
The Router

Routers play a major part in the Internet. As a matter of fact, the structure of the Internet is made up of two major items: routers and phone connections (phone connections are discussed later in this chapter). A router is a network device that connects multiple, often dissimilar, network segments into an internetwork. The router, once connected, can make intelligent decisions about how best to get net work data to its destination based on network performance data that it gathers from the network itself. Because the router is somewhat intelligent, it is much more complex and thus more expensive than other types of network connectivity devices.

Router Ports

A router is not much to look at. Most routers have metal cases and are roughly 19 inches wide, approximately 14 inches deep, and anywhere from 1.5 inches high to 2 feet high with the more complex models. A typical router has multiple ports, or connection points, so that it can connect to all kinds of different network segments and route traffic between them. But at the bare minimum, most routers have at least three ports, and each has a different use.

Each port connects to a different device. For example, the most common port found on a router (there may be many of these ports) is a high-speed serial port (usually labeled something like WAN 0 or Serial 0). This port usually connects to either a modem bank or a WAN connection device like a Channel Service Unit / Data Service Unit (CSU/DSU), which is used to connect a router to a T1 phone line, discussed later in this chapter.

The second type of port is the port that connects the router to the LAN. It is usually an Ethernet port that you would connect to a hub so that the router could communicate with the rest of the LAN. It is usually labeled something like LAN 0 or Eth0 (for an Ethernet router).

The third type of port that some routers have is what is called an out-of-band management port. This port is a serial port (that most often uses an RJ-45 connector) that you connect to a terminal or PC running terminal software so you can configure the router. Some routers forgo this port in favor of in-band management, meaning that you run the management software on a PC connected to the network and configure the router over the network. Some routers have one or the other, but many high-end routers have both to allow you the most flexibility in configuration.
Figure 1.8 shows an example of a router and some of the most common items found on routers today. Note that the router shown in Figure 1.8 has two serial ports, a LAN port, and an out-of-band management port.

Figure 1.8: A sample router

**Router Use on the Internet**

As mentioned, the Internet is a web of interconnected routers. An ISP’s LAN is connected to a router, which is connected by some kind of leased telephone connection to the router at the ISP’s ISP (called an *upstream provider*). That ISP is connected to another ISP, and so on. Routers are also capable of providing multiple, redundant links between two routers. If one connection fails, the router will send all traffic over the other connection.

In addition to providing LAN-to-Internet connectivity, a router can provide a way for dial-up clients to connect to the Internet. When you connect your home computer to the Internet via a modem, your modem is dialing another modem attached to a router of some kind. The router then routes the requests from the connected computer to the Internet and routes the associated responses back to the original requesting computer.

Figure 1.9 shows a sample router with two serial ports and one LAN port and how it might be used in an ISP. Note what devices are connected to each port. Note that the modems that customers will dial into and the WAN connections are connected to a router’s serial port (because they are serial devices) and the LAN port connects to the rest of the LAN.

Figure 1.9: A sample router and how it might be used in an ISP

**The Firewall**

Networks that are connected to the Internet are subject to possible attacks from outside malicious
entities located elsewhere on the Internet. To protect a network against attacks, a device called a firewall is employed. Firewalls reside between a company’s LAN and the Internet and monitor all traffic going into and out of the network. Any suspicious or unwanted activity is monitored and, if necessary, quelled. Firewalls are usually combinations of hardware and software with multiple NICs (one for the Internet side, another for the LAN side, and possibly a third for a DMZ, discussed in a moment). Some firewalls are stand-alone hardware devices; others consist of special software that turns the server computer on which it runs into a firewall. Both types can be generalized as firewalls. The major difference between the two is that the latter may run a commercially available NOS, like NT, NetWare, or Unix, whereas the former is running its own highly specialized operating system.

Most firewalls in use today implement a feature called a demilitarized zone (DMZ), which is a network segment that is neither public nor local, but halfway between. People outside your network primarily access your Web servers, FTP servers, and mail-relay servers. Because hackers tend to go after these servers first, place them in the DMZ. A standard DMZ setup has three network cards in the firewall computer. The first goes to the Internet. The second goes to the network segment where the aforementioned servers are located, the DMZ. The third connects to your intranet.

When hackers break into the DMZ, they can see only public information. If they break into a server, they are breaking into a server that holds only public information. Thus, the entire corporate network is not compromised. In addition, no e-mail messages are vulnerable; only the relay server can be accessed. All actual messages are stored and viewed on e-mail servers inside the network. As you can see in Figure 1.10, the e-mail router, the FTP server, and the Web server are all in the DMZ, and all critical servers are inside the firewall.

![Figure 1.10: A firewall with a DMZ](image)

The Modem

The device most commonly used to connect computers over a public analog phone line is a modem (a contraction of modulator/demodulator). A modem changes digital signals from the computer into analog signals that can be transmitted over phone lines and other analog media. On the receiving end, the modem changes the analog signals back to digital signals.

Modems change the digital ones and zeros into analog signals. The pattern of these analog signals encodes the data for transmission to the receiving computer. The receiving modem then takes the analog
signals and turns them back into ones and zeros. Using this method, which is slower than completely
digital transmissions, data can travel over longer distances with fewer errors.

A modem can be either internal or external. The key difference between the two is the amount of
configuration required. You must configure internal modems with an IRQ and an I/O address as well as
a virtual COM port address to ensure that they function properly. External modems simply hook to a
serial port and don’t require nearly as much configuration.

In addition to being either internal or external, some modems can connect either by using the telephone
system or through your local cable TV cable. Analog telephone modems are the most common, but in
larger metropolitan areas, cable modems are becoming more popular because they offer higher speed at
a lower price. This is attractive because people will always pay less for more bandwidth.

Note For information on how to set up and configure a modem, see Chapter 6.

Internet Gateways

There are a couple of definitions for the term gateway. A gateway, in the classical sense, is any
combination of hardware and software that translates one protocol or technology into another. The best
element of this is an e-mail gateway. There are different types of e-mail systems, including Simple Mail
Transfer Protocol (SMTP), Exchange, GroupWise, and others. When you want to connect a proprietary
e-mail system (like MS Exchange or Novell GroupWise) to the Internet, you will need to use an e-mail
gateway that translates the native e-mail system’s mail into Internet (SMTP) mail format. When a
message is sent to the Internet, the mail system will send it first to the e-mail gateway, which will
translate the mail to SMTP format and then send it on to the Internet. Figure 1.11 shows how an e-mail
gateway is used. Notice how the e-mail message is translated from GroupWise format to SMTP format.

Figure 1.11: Example of how gateways work

The other popular definition of a gateway is used when configuring the TCP/IP protocol (discussed in
Chapter 3) on a network. In TCP/IP parlance, a gateway is another name for a router. When setting up
TCP/IP on a workstation, you may have to configure a default gateway. A default gateway is the router
your workstation will send all TCP/IP traffic to when the workstation can’t determine the destination IP
address.

A router is acting as a gateway in the sense of protocol conversion as well. For example, if your Ethernet
10BaseT network is connected to the Internet over a packet-switched Frame Relay line, you send an
Ethernet packet to the router, which then encapsulates the Ethernet packet into a format the Frame Relay
data link can understand. In this sense, a router does act as a gateway, performing the conversion of the
Ethernet protocol to the packet-switching protocol. That is why the first routers were called gateways,
and the “default gateway” configuration for IP clients has remained.
Network Software Components

In addition to all the hardware components, networks use some software components to tie together the functions of the different hardware components. Each software component has a different function on the network. In this section, you will learn about some of the software often found on a network. The most important network software components that you’ll learn about include:

- Network operating system (NOS)
- Protocols

Each software component runs on a computer and provides the network with some service.

Network Operating System (NOS)

Every network today uses some form of software to manage the resources of the network. This software runs on the servers and is called a network operating system (or NOS, for short). NOSes are, first and foremost, computer operating systems, which means they manage and control the functions of the computer they are running on. NOSes are more complex than computer operating systems because they manage and control the functions of the network as well. A NOS gives a network its “soul” because each NOS works a bit differently. Different NOSes will need to be administered differently.

The three most popular network operating systems that you will need to know about are:

- Microsoft Windows NT/Windows 2000
- Novell NetWare
- Unix

In the following sections, you will learn background information on each NOS, its current version, its applicability to the Internet/its strength as a NOS for an Internet server, and its system requirements.

Microsoft Windows NT

There has been a buzz in the computer industry as of late about Windows NT, produced by Microsoft Corporation. Everyone’s asking, “Should I be installing it?” With the same graphical interface as other versions of Windows and simple administration possible from the server console, it is a force to be reckoned with. Microsoft has put its significant marketing muscle behind it, and Windows NT has become a viable alternative in the network operating system market, previously dominated by Novell NetWare and the various flavors of Unix.

As this book is being written, Windows NT 4 is the current version of Windows NT, but Windows 2000 is scheduled to be released very soon (and may have been released by the time you are reading this book). Windows 2000 is the next generation of Windows and is designed to eventually replace both Windows 95/98 and Windows NT. Windows 2000 is the biggest release of Windows to date and has the most features, including a new directory service and Plug-and-Play support.

Note For more information on Windows NT, visit Microsoft’s Web site at www.microsoft.com.
Microsoft’s Windows NT Server has become the predominant general-purpose server for the industry. Its versatility and familiar graphical user interface (it’s the same as Windows 95/98 in NT 4 and 2000) belie its complexity. Using TCP/IP and other protocols, Windows NT can communicate and be integrated with NetWare and Unix servers. Additionally, it is the preferred NOS for the intranet and Internet services of small companies because it’s easy to set up and manage for Internet services. Again, this ease comes from the familiarity people have with the client OS, Windows 95/98. Also, Internet services can be installed during NOS setup with a few mouse-clicks and a minimal amount of configuration. The only downside to Windows NT is that it’s sometimes unstable and it has much larger hardware requirements than the other NOSes discussed in this chapter (as listed in Table 1.1).

Table 1.1: Windows NT Server 4 Hardware Requirements

<table>
<thead>
<tr>
<th>Hardware</th>
<th>Minimum</th>
<th>Recommended</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>Intel 80486 or higher (I386 architecture) or a supported RISC processor (MIPS R4x00, Alpha AXP, or Power PC)</td>
<td>Pentium 90MHz or higher (the faster the better)</td>
</tr>
<tr>
<td>Display</td>
<td>VGA</td>
<td>SVGA</td>
</tr>
<tr>
<td>Hard disk space</td>
<td>120MB free</td>
<td>300MB free</td>
</tr>
<tr>
<td>Memory</td>
<td>16MB</td>
<td>32MB or greater</td>
</tr>
<tr>
<td>Network card</td>
<td>At least one that matches the topology of your network</td>
<td>At least one that matches the topology of your network</td>
</tr>
<tr>
<td>CD-ROM</td>
<td>None</td>
<td>8x or greater</td>
</tr>
<tr>
<td>Mouse</td>
<td>Required</td>
<td>Required</td>
</tr>
</tbody>
</table>

Novell NetWare

NetWare, made by Novell, Inc., was the first NOS developed specifically for use with PC networks. It was introduced in the late ‘80s and quickly became the software people chose to run their networks. NetWare is one of the more powerful network operating systems on the market today. It is almost infinitely scalable and has support for multiple client platforms. Although most companies larger than a few hundred stations are running NetWare, this NOS enjoys success in many different types of networks.

Currently, NetWare is at version 5 and includes workstation management support, Internet connectivity, Web proxy, and native TCP/IP protocol support, as well as continued support for its award-winning directory service, Novell Directory Services (NDS).

As an Internet and intranet NOS, NetWare sees use in large networks for secure intranets. In our tests, with similarly configured servers, NetWare had the best Web server performance over NT and Unix (using the included Netscape Enterprise Server for NetWare). Plus, its Web page security is integrated with Novell’s directory service (NDS). Hardware requirements are listed in Table 1.2.

Note For more information on NetWare, check out Novell, Inc.’s Web site at www.novell.com.

Table 1.2: NetWare 5 Hardware Requirements and Recommendations

<table>
<thead>
<tr>
<th>Hardware</th>
<th>Minimum</th>
<th>Recommended</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>Pentium</td>
<td>Pentium 90MHz or faster.</td>
</tr>
<tr>
<td>Display</td>
<td>VGA</td>
<td>SVGA.</td>
</tr>
</tbody>
</table>
Unix

Of the network operating systems other than Windows NT and NetWare, the various forms of Unix are probably the most popular. It is also among the oldest of the network operating systems. Bell Labs developed Unix, in part, in 1969—in part because there are now so many iterations, commonly called flavors, of Unix that it is almost a completely different operating system.

Although the basic architecture of all flavors is the same (32-bit kernel, command-line based, capable of having a graphical interface, as in X Windows), the subtle details of each make one flavor better than another in a particular situation.

Unix flavors incorporate a kernel, which constitutes the core of the operating system. The kernel can access hardware and communicate with various types of user interfaces. The two most popular user interfaces are the command-line interface (called a shell) and the graphical interface (X Windows). The Unix kernel is similar to the core operating system components of Windows NT and NetWare. In Unix, the kernel is typically simple and, therefore, powerful. Additionally, the kernel can be recompiled to include support for more devices. As a matter of fact, some flavors include the source code so that you can create your own flavor of Unix.

As an Internet platform, Unix has many advantages, mainly because the Internet was first and foremost a Unix-based network. Many services available for the Internet (like Usenet news) work best on the Unix platform because these technologies were first developed on Unix. Additionally, Unix is powerful enough to scale to service hundreds of thousands of Web requests per second. Many of the most popular Web sites run on Unix.

Each flavor of Unix has widely varied hardware requirements. Some flavors can run on any processor/hardware combination. Others can only run on certain combinations. As an example, hardware requirements for the common PC-based Unix flavor Red Hat Linux 6 are covered in Table 1.3. If you need to install any flavor of Unix onto a computer, check the software’s packaging or documentation for its respective hardware requirements.

Tip Unix hardware requirements vary from vendor to vendor. As such, they are not currently tested for in the exam.

Table 1.3: Red Hat 6 Linux Hardware Requirements

<table>
<thead>
<tr>
<th>Hardware</th>
<th>Minimum</th>
<th>Recommended</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>Intel 80486 or higher (I386 architecture), 680x0, or a supported RISC processor (MIPS, AP1000+, Alpha AXP, SPARC, or PowerPC)</td>
<td>Pentium 90MHz or higher (the faster the better)</td>
</tr>
<tr>
<td>Display</td>
<td>VGA</td>
<td>SVGA</td>
</tr>
</tbody>
</table>
All network entities must communicate to gain the benefits of being networked. In order to communicate, each device on the network must understand the same basic rules of that communication. For example, each node must understand a common “language” and the types of “words” to use. Not to imply that computers speak English, but they do need a set of rules to communicate. These rules are called protocols. Multiple protocols operating together are called a protocol suite. Finally, a software implementation of a protocol is called a protocol stack.

There is really only one protocol suite used on the Internet, the Transmission Control Protocol/Internet Protocol (TCP/IP) suite. It was developed at approximately the same time the Internet was developed. When it was being designed, its designers wanted a protocol that could reconfigure itself around possible breaks in the communication channel. Today, TCP/IP is almost ubiquitous because almost every operating system includes a TCP/IP protocol stack so that the operating system can communicate with the Internet. That feature, along with its relatively decent performance, makes TCP/IP a very popular protocol. We’ll discuss TCP/IP in more detail in Chapter 3.

Other Protocols

In addition to TCP/IP, there are other protocols available for use on LANs. The protocol suite Internetwork Packet eXchange/Sequenced Packet eXchange (IPX/SPX), developed by Novell for use with NetWare, is probably the second most popular protocol. It is used with both NetWare and Windows NT and is a popular choice because of its ease of configuration. Some other protocol suites you may encounter are the NetBIOS Enhanced User Interface (NetBEUI), DEC Networking (DECNet), and Systems Network Architecture (SNA) protocols, but these see much more limited use in LANs today when compared to TCP/IP and IPX/SPX.

Combination Components

Some network devices don’t fit well into any category. They perform several special Internet access and performance functions without any kind of standard NOS. These devices are optimized such that they do one particular operation and do it very efficiently and very quickly. The following are two examples of combination components:

- Internet-in-a-box
- Cache-in-a-box

In the following sections, you will learn about the various combination components available; a basic
description of how each one works and common applications for each one are included.

**Internet-in-a-Box**

With its exponential growth in the last few years, many more people are getting on the Internet and it is becoming less convenient to access it with a modem. Any company that has a network already in place can theoretically give everyone on that network Internet access by directly connecting the LAN to the Internet using a router and some kind of dedicated point-to-point or public switched connection (discussed later). The need for a faster (greater than 56Kbps), multiuser connection at an inexpensive price has arisen.

To fill this need, some router and Internet access companies (like Bay, Cisco, and 3Com) have developed "Internet-in-a-box" devices that provide Internet access to an entire network over a single Internet connection. These devices are typically “black boxes” that have a single phone line connection and a single network connection. Installation is very simple. Hook the LAN to the LAN port, hook a phone line to the phone port, and configure the box using an included configuration software package. Obviously, there is a little more to it than that, but it is still very simple. Once configured, the device will provide Internet access for everyone connected to the network.

These boxes are available with a variety of connection methods, including regular phone modem, ISDN, DSL, and T1 connections. However, most only include one connection method and can only support a limited number of users (usually fewer than 20). Any more than that would require a true router with a CSU/DSU or modem combination that can support higher throughput and a larger number of users. [Figure 1.12] shows a network configured with one of these devices. The Internet-in-a-box provides a single point of access to the Internet for this network.

Figure 1.12: Internet connection with an Internet-in-a-box device

**Cache-in-a-Box**

One other “in-a-box” technology that is catching on is “cache-in-a-box.” A cache-in-a-box is a “black box” that you plug into your network to increase Internet surfing by caching portions of frequently accessed Web sites. Internet caching systems are used to increase Internet access performance. These “preconfigured caching systems” are just hardwired versions of caching servers. Caching servers work by keeping track of every Web site that is visited and caching portions of them. The next time someone on the same network visits that same Web site, the response to the request for that Web page comes from the cache located on the local network, not from the actual Internet Web server that is hosting it. The performance benefit is realized because the cached entries are delivered at LAN speeds (10-100Mbps) and are coming from a local server (not one that is located across several routed links). [Figure 1.13] illustrates this process.
This technology has become so important and popular that some vendors are selling preconfigured cache boxes. Again, the benefit to these caches is performance and ease of setup. Basically, you plug the cache box into your network, give it a TCP/IP address, configure it using the included software, and configure all Web clients to use it. Generally speaking, these “caches-in-a-box” include high-powered processors and are designed to dedicate all their resources to caching Internet content.

Compaq’s ICS (based on Novell’s Internet Caching System) is one example of a cache-in-the-box.

**Local Area Network Link Types**

Local area networks (LANs) have many ways of delivering data from point A to point B. These “link types” include specifications that dictate how the stations will transmit their data, how the data will travel on the network, and how much data can be transmitted. The majority of networks installed today (including the ones at ISPs) use these link types. There are two popular LAN link types you will see on almost every network:

- **Ethernet**
- **Token Ring**

Most servers and workstations connect using one of these link types.

**Ethernet**

Ethernet, the most popular network specification, was originally the brainchild of Xerox Corporation. Introduced in 1976, it quickly became the network of choice for small LANs. The Unix market was the first to embrace this easy-to-install network.

Ethernet uses the CSMA/CD (Carrier Sense Multiple Access with Collision Detection) media access method, which means that only one workstation can send data across the network at a time. It functions much like the old party line telephone systems used in rural areas. If you wanted to use the telephone, you picked up the line and listened to see if anyone was already using it. If you heard someone on the
line, you didn’t try to dial or speak; you simply hung up and waited a while before you picked up the phone to listen again.

If you picked up the phone and heard a dial tone, you knew the line was free. You and your phone system operated by carrier sense. You sensed the dial tone or carrier, and if it was present, you used the phone. Multiple access means that more than one party shared the line. Collision detection means that if two people picked up the phone at the same time and dialed, they would “collide” and both would need to hang up the phone and try again. The first one back on the free line gains control and is able to make a call.

In the case of Ethernet, workstations send signals (frames) across the network. When a collision takes place, the workstations transmitting the frames stop transmitting and wait for a random period of time before retransmitting. Using the rules of this model, the workstations must contend for the opportunity to transmit across the network. For this reason, Ethernet is referred to as a contention-based system.

Current implementations of Ethernet allow for connection speeds of either 10 or 100Mbps. There are, however, standards being developed for Gigabit Ethernet (one thousand megabits per second).

**Token Ring**

Token Ring was developed by IBM as a robust, highly reliable network. It is more complex than Ethernet because it has self-healing properties. Token Ring is an IEEE 802.5 standard whose topology is physically a star but logically a ring. Workstations connect to the bus by means of individual cables that connect to a multistation access unit (MSAU) or controlled-access unit (CAU). MSAUs and CAUs are similar to Ethernet hubs in that they exist at the center of the star, but they are for Token Ring networks. The difference between an MSAU and a CAU is that an MSAU is a passive device that has no power plug and no intelligence, whereas a CAU has intelligence and a power plug. A CAU can perform physical network management operations.

The original Token Ring cards were 4Mbps. These were later replaced by 16Mbps cards. The 16Mbps cards are manufactured to work at 4Mbps (for compatibility), but the 4Mbps cards only run at 4Mbps. The 4Mbps version will allow only one token on the ring at a time. The 16Mbps version will allow a card to retransmit a new free token immediately after the last bit of a frame. The term for this is early token release.

Warning When configuring a Token Ring network, you must remember that all Token Ring cards must be set to either 4Mbps or 16Mbps. You cannot mix the speeds on the same segment.

In a Token Ring, although the cards attach like a star to the MSAU or CAU, they function logically in a ring. A free token (a small frame with a special format) is passed around the ring in one consistent direction. A node receives the token from its nearest active upstream neighbor (NAUN) and passes it to its nearest active downstream neighbor (NADN). If a station receives a free token, it knows that it can attach data and send it on down the ring. This is called media access. Each station is given an equal chance to have the token and take control in order to pass data.

Each station in the ring receives the data from the busy token and repeats the data, exactly as it received it, on to the next active downstream neighbor on the ring. The addressed station (the station the data is intended for) keeps the data and passes it on up to its upper-layer protocols. It then switches 2 bits of the frame before it retransmits the information back on to the ring to indicate that it received the data. The data is sent repeatedly until it reaches the source workstation, and then the process begins again.
Each station in the ring basically acts as a repeater. The data is received and retransmitted by each node on the network until it has gone full circle. This is something like the party game called Rumor or Telephone, in which one person whispers something into one player’s ear, who in turn whispers it into someone else’s ear, and so on until it has gone full circle. The only difference is, in the party game, when the person who initiated the message receives it back, it has usually undergone substantial permutations. When the originating node on the network receives the message, it is normally intact except that 2 bits have been flipped to show that the message made it to its intended destination.

Note Token Ring computers act as repeaters, in contrast to computers in an Ethernet network, where they are passive and therefore not relied on to pass data. This is why Token Ring networks can experience periods of latency when a computer fails and Ethernet networks will not. Also, the token-passing access method will not have collisions because only one token is on the cable at one time; Ethernet networks with CSMA/CD do have collisions.

### Internet Bandwidth Link Types

An Internet bandwidth technology (or link) is the communications pathway between the various LANs that make up the Internet. These links are typically specific types of analog or digital telephone lines that carry data for a corporate WAN and for the Internet. They are leased from the telephone companies that serve the cities at the ends of the link. Hence, these WAN links are often called leased lines.

In addition to connecting networks together, the same WAN link technologies are also used to connect entire networks to the Internet and to provide the Internet with its structure by connecting multiple ISPs together. Wide area network links are commonly grouped into two main types:

- Point-to-point
- Public switched networks

### Point-to-Point WAN Connections

Point-to-point WAN connections are WAN links that exist directly between two locations. Point-to-point connections are typically used for WAN connections between a central office and a branch office or from these locations to an ISP for Internet connectivity. These connections come in a variety of connection speeds. The main advantage of point-to-point connections to the Internet is that there is only one “hop” between the two locations, thus much less latency in each transmission, which means more data can be transmitted. The main downside is that these connections are often more expensive than their switched counterparts.

There are seven main point-to-point WAN connections in use today:

- DDS/56Kbps
- T1/E1
- T3/E3
- Asynchronous Transfer Mode (ATM)
Each connection type differs primarily in the data throughput rates offered and in the cost. In this section, you will learn about the most popular point-to-point WAN (and Internet) connection types.

**DDS/56Kbps**

The Dataphone Digital Service (DDS) line from AT&T is a dedicated, point-to-point connection with throughput anywhere from 2400bps to 56Kbps. The 56Kbps digital connection is the most common, and this type of line has since obtained the moniker *56K line*. This type of line is used most often for small office connections to the central office. Some small companies may use this for their connection to their ISP for an Internet connection.

Note If a phone company other than AT&T provides this service, the line is known as a Digital Data Service line. The abbreviation is still DDS, however.

**T1/E1**

A T1 is a 1.544Mbps digital connection that is typically carried over two pair of UTP wires. This 1.544Mbps connection is divided into 24 discrete, 64Kbps channels (called DS0 channels). Each channel can carry either voice or data. In the POTS world, T1 lines are used to bundle analog phone conversations over great distances, using much less wiring than would be needed if each pair carried only one call. This splitting into channels allows a company to combine voice and data over one T1 connection. You can also order a fractional T1 channel that uses fewer than the 24 channels of a full T1. An E1 is the same style channel, but it is a European standard and is made up of 32 64Kbps channels for a total throughput of 2.048Mbps.

A T1 connection is used very often to connect a medium-size company (50 to 250 workstations) to the Internet. It is usually cost prohibitive to have a T1/E1 connection for any company smaller than that, and it doesn’t have the bandwidth that larger companies would require for high-speed WAN connections. Smaller ISPs that mainly provide residential dial-up connections may only have a T1 connection.

**T3/E3**

A T3 line and a T1 connection work similarly, but a T3 line carries a whopping 44.736Mbps. This is equivalent to 28 T1 channels (or a total of 672 DS0 channels). E3 is a similar technology for Europe that uses 480 channels for a total bandwidth of 34.368Mbps. Currently these services require fiber-optic cable or microwave technology. Many local ISPs have T3 connections to the major ISPs, such as SprintNet, AT&T, and MCI. Also, very large, multinational companies use T3 connections to send voice and data between their major regional offices.

**Asynchronous Transfer Mode (ATM)**

Of the link types we have discussed so far, Asynchronous Transfer Mode (ATM) is one link type that is used on both LANs and WANs. ATM uses cell-switching technology, which means that it works by dividing all data to be transmitted into special 53-byte packets called cells and sending them over a
switched, permanent virtual circuit. Because all the packets are the same length, and because they are very small, ATM is a highly efficient, and very fast, set of WAN standards. It can support transmissions of voice and video in addition to data at speeds of from 1.5 to 2488Mbps. Additionally, ATM supports the ability to reserve bandwidth to ensure Quality of Service (QoS) so that voice and data transmissions won’t interfere with each other. Several Internet backbone ISPs use ATM to move massive amounts of Internet data quickly.

ISDN

ISDN is a digital, point-to-point network capable of maximum transmission speeds of about 1.4Mbps, although speeds of 128Kbps are more common. Because it is capable of much higher data rates, at a fairly low cost, ISDN is becoming a viable remote Internet connection method, especially for those who work out of their homes and require high-speed Internet access but can’t afford a T1 or higher. ISDN uses the same UTP wiring as your residential or business telephone wiring (also known as Plain Old Telephone Service, or POTS), but it can transmit data at much higher speeds. That’s where the similarity ends, though. What makes ISDN different from a regular POTS line is how it uses the copper wiring. Instead of carrying an analog (voice) signal, it carries digital signals. This is the source of several differences.

A computer connects to an ISDN line via an ISDN terminal adapter (often incorrectly referred to as an ISDN modem). An ISDN terminal adapter is not a modem because it does not convert a digital signal to an analog signal; ISDN signals are digital.

A typical ISDN line has two types of channels. The first type of channel is called a Bearer, or B, channel, which can carry 64Kbps of data. A typical ISDN line has two B channels. One channel can be used for a voice call while the other is being used for data transmissions, and this occurs on one pair of copper wire. The second type of channel is used for call setup and link management and is known as the Signal, or D, channel (also referred to as the Delta channel). This third channel has only 16Kbps of bandwidth.

In many cases, to maximize throughput, the two Bearer channels are combined into one data connection for a total bandwidth of 128Kbps. This is known as bonding or inverse multiplexing. This still leaves the Delta channel free for signaling purposes. In rare cases, you may see user data such as e-mail on the D line. This was introduced as an additional feature of ISDN, but it hasn’t caught on.

ISDN has three main advantages:

- Fast connection.
- Higher bandwidth than POTS. Bonding yields 128KB bandwidth.
- No conversion from digital to analog.

ISDN does have a few disadvantages:

- It’s more expensive than POTS.
- Specialized equipment is required at the phone company and at the remote computer.
- Not all ISDN equipment can connect to each other.
DSL

Digital Subscriber Line (DSL) is a hot topic for home Internet access because it is relatively cheap (less than $100/month in most areas), fast (greater than 128Kbps), and available in most major cities in the United States. xDSL is a general category of copper access technologies that is becoming popular because it uses regular, POTS phone wires to transmit digital signals and is extremely inexpensive compared with the other digital communications methods. xDSL implementations cost hundreds instead of the thousands of dollars that you would pay for a dedicated, digital point-to-point link (such as a T1). They include Digital Subscriber Line (DSL), High Data Rate Digital Subscriber Line (HDSL), Single Line Digital Subscriber Line (SDSL), Very High Data Rate Digital Subscriber Line (VDSL), and Asymmetric Digital Subscriber Line (ADSL), which is currently the most popular. It is beyond the scope of this book to cover all the DSL types. Ask your local telephone company which method they provide.

ADSL is winning the race because it focuses on providing reasonably fast upstream transmission speeds (up to 640Kbps) and very fast downstream transmission speeds (up to 9Mbps). This makes downloading graphics, audio, video, or data files from any remote computer very fast. The majority of Web traffic, for example, is downstream. The best part is that ADSL works on a single phone line without losing the ability to use it for voice calls. This is accomplished with what is called a splitter, which enables the use of multiple frequencies on the POTS line.

As with ISDN, communicating via xDSL requires an interface to the PC. All xDSL configurations require a modem, called an endpoint, and a NIC. Often the modem and NIC are on a single expansion card.

SONET

Some of the fastest WAN connections are those employed in the Synchronous Optical Network (SONET). SONET is a high-speed, fiber-optic system that provides a standard method for transmitting digital signals over a fiber-optic network. Multiple transmission types (i.e., 64Kbs channels, T1/E1 channels) can be multiplexed together to provide SONET speeds.

SONET is able to achieve maximum transmission speeds of up to 2.488 gigabits per second. It does so by using a fixed frame size of 810 bytes. This fixed frame size makes transmissions very efficient, and thus they can carry more data.

SONET speeds are rated as channels. They are designated with an OC (Optical Character) number. The OC lines are designated OC-1 through OC-768. OC-1 channels communicate at 51.84Mbps, OC-3 channels communicate at 155.52Mbps, and OC-768 channels communicate at 40Gbps.

Public Switched Network WAN Connections

The other type of WAN link most commonly in use is the public switched network WAN connection. These connections use the telephone company’s analog switched network to carry digital transmissions. Your network traffic is combined with other network traffic from other companies. Essentially, you are sharing the bandwidth with all other companies. The upside to this type of WAN connection is that it is cheaper than point-to-point connections, but because you share the bandwidth with other traffic, it isn’t necessarily as efficient.

Let’s take a brief look at some of the public switched network connections that companies use to
connect to the Internet, including:

- Public Switched Telephone Network (PSTN)
- X.25
- Frame Relay

**Public Switched Telephone Network (PSTN)**

Almost everyone outside the phone companies themselves refers to PSTN (Public Switched Telephone Network) as POTS (Plain Old Telephone Service). This is the wiring system that runs from most people’s houses to the rest of the world. It is the most popular method for connecting to the Internet because of its low cost, ease of installation, and simplicity. The majority of the houses in the U.S. that have Internet connections connect to their ISP via PSTN and a modem.

The phone company runs a UTP (unshielded twisted-pair) cable (called the local loop) from your location (called the demarcation point or demarc, for short) to a phone company building called the Central Office. All the pairs from all the local loop cables that are distributed throughout a small regional area come together at a central point, similar to a patch panel in a UTP-based LAN.

This centralized point has a piece of equipment called a switch attached. The switch functions almost exactly like the switches we mentioned earlier, in that a communications session, once initiated when the phone number of the receiver is dialed, exists until the conversation is closed. The switch can then close the connection. On one side of the switch is the neighborhood wiring. On the other side are lines that may connect to another switch or to a local set of wiring. The number of lines on the other side of the switch depends on the usage of that particular exchange. **Figure 1.14** shows a PSTN system that utilizes these components.

![Figure 1.14: A local PSTN (POTS) network](image)

Warning Use caution when working with bare phone wires because they may carry a current. In POTS, the phone company uses a battery to supply power to the line, which is sometimes referred to as self-powered. It isn’t truly self-powered; the power comes from the phone system.

POTS has many advantages, including:

- It is inexpensive to set up. Almost every home in the United States has or can have a telephone connection.
- There are no LAN cabling costs.
Connections are available in many countries throughout the world.

POTS is the most popular remote access connection method for the Internet because only two disadvantages are associated with it: limited bandwidth and thus a limited maximum data transfer rate. At most, 64Kbps data transmissions are possible, though rarely achieved by anyone connecting from home to the Internet.

**X.25**

X.25 was developed by the International Telecommunications Union (ITU) in 1974 as a standard interface for WAN packet switching. It does not specify any thing about the actual data transmission, however. It only makes specifications about the access to the WAN and just assumes that a route from sender to receiver exists. The original X.25 specification supported transmission speeds of up to 64Kbps, but the 1992 revision supports transmission speeds of up to 2Mbps. It is currently one of the most widely used WAN interfaces.

**Frame Relay**

Similar to X.25, Frame Relay is a WAN technology in which packets are transmitted by switching. Packet switching involves breaking messages into chunks at the sending router. Each packet can be sent over any number of routes on its way to its destination. The packets are then reassembled in the correct order at the receiver. Because the exact path is unknown, a cloud is used when creating a diagram to illustrate how data travels throughout the service. Figure 1.15 shows a Frame Relay WAN connecting smaller LANs.

![Figure 1.15: A typical frame relay configuration](image)

Frame Relay uses permanent virtual circuits (PVCs). PVCs allow virtual data communications circuits between sender and receiver over a packet-switched network. This ensures that all data that enters a Frame Relay cloud at one side comes out at the other over a similar connection.

The beauty of using a shared network is that sometimes you can get much better throughput than you are paying for. When signing up for one of these connections, you specify and pay for a Committed Information Rate (CIR), or in other words, a minimum bandwidth. If the total traffic on the shared
network is light, you may get much faster throughput without paying for it. Frame Relay begins at the CIR speed and can reach as much as 1.544Mbps, the equivalent of a T1 line, which was discussed earlier.

However, the major downside to Frame Relay is that you share traffic with all other people within the Frame Relay cloud. If you aren’t paying for a CIR, your performance can vary widely. Despite this disadvantage, Frame Relay is a popular Internet connection method because of its low cost.

Table 1.4 shows all these point-to-point connections and their respective performance, availability, and cost.

Table 1.4: Point-to-point WAN and Internet connection types

<table>
<thead>
<tr>
<th>Connection</th>
<th>Max Throughput</th>
<th>U.S. Availability</th>
<th>Relative Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>56K/DDS</td>
<td>56Kbps</td>
<td>Widely available</td>
<td>Low</td>
</tr>
<tr>
<td>T1/E1</td>
<td>1.544Mbps/ 2.048Mbps</td>
<td>Widely available</td>
<td>Medium</td>
</tr>
<tr>
<td>T3/E3</td>
<td>44.736Mbps/ 34.368Mbps</td>
<td>Widely available</td>
<td>High</td>
</tr>
<tr>
<td>ATM</td>
<td>2488Mbps</td>
<td>Moderately available</td>
<td>Very high</td>
</tr>
<tr>
<td>ISDN</td>
<td>Around 2Mbps</td>
<td>Moderately available</td>
<td>Low</td>
</tr>
<tr>
<td>DSL</td>
<td>Greater than 128Kbps</td>
<td>Available in larger cities, becoming more available in rural areas</td>
<td>Low</td>
</tr>
<tr>
<td>Frame Relay</td>
<td>1.544Mbps or slower</td>
<td>Widely available</td>
<td>Low</td>
</tr>
<tr>
<td>OC-1</td>
<td>51.84Mbps</td>
<td>Moderately available</td>
<td>Very, very high</td>
</tr>
<tr>
<td>OC-3</td>
<td>155.52Mbps</td>
<td>Moderately available</td>
<td>Very, very high</td>
</tr>
<tr>
<td>OC-48</td>
<td>2.488Gbps</td>
<td>Slim availability</td>
<td>Don’t ask</td>
</tr>
</tbody>
</table>

Summary

In this chapter, you learned about some of some of the LAN and WAN networking technologies that apply to the business of the Internet. Because most networks are connected to the Internet these days, the concepts contained in this chapter will be valuable to you as an Internet professional. You learned the definitions of a LAN and a WAN as well as the differences between them. You also learned about some of the hardware components that exist on the network, including workstations, servers, NICs, network cables, hubs, switches, bridges, routers, firewalls, and modems. In addition to learning about the hardware components, you learned about some of the software components that work on the network to provide Internet (and other) services, including network operating systems (NOSes) and protocols. Then there are those components that don’t fall easily into either category. Those components are known as combination components, and there are really only two components in this category on the i-Net+ exam, the Internet-in-a-box and the cache-in-a-box. Both components are “black boxes” you can add to your network without a large amount of configuration.

This chapter included a discussion about the link types that carry data from point A to point B on a network. LAN link types include Ethernet and Token Ring. Ethernet is the most common LAN link type. WAN link types include DDS/ 56Kbps, T1/E1, T3/E3, ATM, ISDN, DSL, and Frame Relay. The WAN link types can be used for connecting to the Internet and vary in speed and link cost.
You also learned about many different kinds of hardware and software connection technologies. The following list includes the most important ones to know for the i-Net+ exam:

**Network interface card**  Also called a network adapter or NIC, this device provides a computer with its electrical and physical connection to a network.

**Various types of modems, including analog, ISDN, DSL, and cable**  A modem is a device that converts the digital signals your computer uses into analog signals that can be transmitted over longer distances (typically over house phone lines). Modems can be either internal or external. Of the two types, internal modems are cheaper but require more configuration. External modems are more expensive but typically have status displays that can aid in connection troubleshooting.

**Bridge**  A bridge is a hardware connection device that connects two network segments into a single network. It can also divide a single network into two network segments while at the same time maintaining a unified network. Network traffic that originates on one side of a bridge for a destination on the same segment will never cross the bridge. A bridge will only pass traffic that originates on one side and is destined for a station on the other side.

**Hub**  This network device connects all network devices together on a twisted-pair Ethernet network. It repeats all signals it receives on one port to all other ports. This device is the central device in a star topology Ethernet network.

**Router**  A router is the device that connects multiple network segments into an internetwork. Routers are intelligent devices that are responsible for making routing decisions about the best path for data packets to take when traveling through an internetwork. Routers are used in ISPs to connect modem users to the Internet in addition to connecting the ISP’s LAN to the Internet.

**Switch**  A switching hub (or switch for short) is a network connectivity device that listens to all the stations connected to it and records their network card’s hardware addresses. Then, when one station on a switch wants to send data to a station on the same switch, the data gets sent directly from the sender to the receiver. The full bandwidth of the network can be used between sender and receiver.

**Gateway**  A gateway is any combination of hardware and software that translates one protocol or technology into another. The most common use of gateways on the Internet is for e-mail. Gateway is also another name for a router.

**Network operating system**  A Network Operating System (NOS) is the software that controls and manages both the server and the network. The most popular NOSes include Novell NetWare, Microsoft Windows NT, and Unix.

- NetWare is a PC-based NOS—and the first PC-based NOS for LANs. It is a high-performance NOS with low hardware requirements
- Windows NT is an easy-to-use NOS that implements the Windows “look and feel.” It is a great NOS for Internet content hosting
- Unix is the oldest NOS that is available for many hardware platforms. Linux is a PC-based flavor of Unix that has become popular as an Internet server NOS.

**Firewall**  Firewalls reside between a company’s LAN and the Internet and monitor all traffic going
into and out of the network. Any suspicious or unwanted activity is monitored and quelled, if necessary.

**Internet-in-a-box** This technology allows small networks to be connected to the Internet simply. The Internet-in-a-box device has one connection that connects to the LAN and another that connects to a phone line or other Internet connection type. The box can then be configured using special software and will allow all users on the LAN access to the Internet without having to do a lot of configuration of routers, CSU/DSUs, and so on.

**Cache-in-a-box** This is a “black box” that you plug into your network to increase Internet Web surfing performance by caching portions of frequently accessed Web sites. You simply plug it into your network and configure the browsers on your network to use it. Some cache boxes don’t require Web browser configuration and cache all Internet traffic.

**Internet link technologies** These are the links between LANs and the Internet or used as WAN connections. They are typically lines leased from the local telephone companies. Each type differs based on its speed, availability, and relative cost.

**Review Questions**

1. Which network hardware device connects dissimilar network topologies into an internetwork?
   A. Hub
   B. Bridge
   C. Switch
   D. Router

2. Which Internet bandwidth technology is the primary technology used on the Internet backbone?
   A. Token Ring
   B. Ethernet
   C. X.25
   D. ATM

3. Which of the following is a standard interface for Frame Relay?
   A. X.25
   B. ISDN
   C. T1
   D. xDSL

4. Which network hardware device is required for the computer in order to connect it to a network?
   A. Bridge
5. Which network hardware device protects a LAN against malicious attacks from the Internet?
   A. Bridge
   B. Switch
   C. NIC
   D. Firewall

6. Which of the following is the fastest possible Internet communications technology?
   A. Ethernet
   B. ATM
   C. T1
   D. T3

7. A T3 connection has a maximum bandwidth of _______ Mbps?
   A. 1.544
   B. 2.048
   C. 34.368
   D. 44.736

8. An E1 connection has a maximum bandwidth of _______ Mbps?
   A. 1.544
   B. 2.048
   C. 34.368
   D. 44.736

9. Of the following, which Internet connection type for home users is taking off and offers fairly high speed (>128Kbps) for a fairly reasonable price?
   A. DSL
   B. ISDN
   C. Frame Relay
10. A T1 WAN connection has a maximum speed of ______ Mbps.
   A. 1.544
   B. 2.048
   C. 34.368
   D. 44.736

11. Which protocol is the Internet based on?
   A. IPX/SPX
   B. NetBEUI
   C. TCP/IP
   D. DECNet

12. Which network hardware device is used to segment a single network into multiple segments?
   A. Hub
   B. Firewall
   C. NIC
   D. Bridge

13. Which component of the network is responsible for providing network services to the rest of the network?
   A. Server
   B. Bridge
   C. Workstation
   D. NIC

14. What is the most widely available Internet connection method in the United States?
   A. ISDN
   B. DSL
   C. POTS
   D. X.25

15. Which network hardware device will increase your Web browsing performance?
A. Firewall
B. Cache
C. Bridge
D. Router

16. Which NOS is the oldest NOS currently in use?
   A. Unix
   B. NetWare
   C. Windows NT
   D. OS/2

17. A ___________ is used in firewalls to provide a safe area for public data that is not part of the public or private networks.
   A. Firewall
   B. Internet-in-a-box
   C. DMZ
   D. Router

18. Based on speed and cost, which Internet bandwidth link type would be the best choice for a small ISP serving 100 dial-up users?
   A. 56K/DDS
   B. T1
   C. T3
   D. ATM

19. Which NOS was developed, in part, by Bell Labs and currently has several hundred different “flavors”?
   A. OS/2
   B. Windows NT
   C. NetWare
   D. Unix

20. Which network connectivity device translates one protocol or technology into another and is used to connect dissimilar network technologies?
   A. Firewall
B. Hub
C. Gateway
D. DSL

Answers to Review Questions

1. D. Hubs, bridges, and switches connect only the same network topologies. Routers are the only devices that connect different topologies (e.g., Ether net to Token Ring).

2. D. Although Token Ring and Ethernet are found in ISPs, ATM is the primary WAN technology used on the Internet backbone. X.25 is only a WAN access technology.

3. A. ISDN, T1, and xDSL are all Internet bandwidth technologies, whereas X.25 is the interface for Frame Relay.

4. B. The other devices (bridge, router, and firewall) are all different network connectivity devices, but you absolutely must have a NIC installed in a computer in order to connect the computer to a network.

5. D. Bridges, switches, and routers are all simply network connectivity devices. Some routers can perform packet filtering, but firewalls are designed specifically to protect a network against malicious activity from the Internet.

6. B. ATM has maximum speeds of 2488Mbps. Ethernet has a maximum transmission speed of 100Mbps. T1 lines are 1.544Mbps, and T3s are 44.736Mbps.

7. D. A T1 connection has a maximum transmission speed of 1.544Mbps. The 2.048 is E1 speed, 34.368 is E3 speed, and 44.736 is T3 speed.

8. B. An E1 connection communicates at 2.048Mbps. T1 connections are 1.544Mbps, E3 connections are 34.368Mbps, and T3 connections are 44.736.

9. A. Frame Relay and ATM normally aren’t for home users (unless you happen to be Bill Gates). ISDN is more expensive than DSL and offers more bandwidth.

10. A. T1 connections have a maximum speed of 1.544Mbps. B is for E1, C is for E3, and D is for T3.

11. C. TCP/IP is the only protocol allowed on the Internet and was developed about the same time as the Internet.

12. D. A bridge is the only device of those listed that is used to segment a network. Hubs and NICs are only connection devices and don’t divide a network. Firewalls perform security checks on network traffic but don’t do any segmenting.

13. A. A server provides network services to the rest of the network. Bridges, workstations, and NICs do not. Bridges segment a network, workstations request the resources a server provides, and NICs allow a workstation to get access to a network.
14. C. Almost every home in the United States already has a PSTN (POTS) phone line. ISDN and DSL have limited availability in major metropolitan areas. X.25 isn’t available in every home without additional cost.

15. B. Of the devices listed, a cache is the only device that can increase a network’s Web browsing performance. All the others can actually introduce delay into Internet communications.

16. A. Although NetWare, NT, and OS/2 have been in use for some time, Unix is, in fact, the oldest.

17. C. The demilitarized zone (DMZ) is the network segment connected to a firewall where public data is placed so that it is available to both public and private networks. A, B, and D are incorrect because they are all examples of other Internet hardware and software technologies.

18. B. Because the maximum connection speed of today’s modems is 56Kbps and the ISP is serving a maximum of 100 users, the maximum throughput needed is 100 x 56, or 5600Kbps (5.6Mbps). A 56K/DDS link would be too slow and a T3 or ATM connection would be way too fast (and probably way too expensive for a small ISP). A T1 (at 1.544Mbps) would be slower than the throughput number figured above, but it is extremely unlikely that all 100 users would be on at the same time. Plus, you can buy multiple T1s for the cost of a single T3.

19. D. The only one of these listed that was developed in any part by Bell Labs is Unix. The others were all developed by other companies, like IBM (OS/2), Novell (NetWare), and Microsoft (NT).

20. C. A gateway is the only device listed here that can connect dissimilar network technologies and perform protocol and technology translation. Firewalls and hubs are network connectivity devices, but they can’t do protocol translation. DSL is actually an Internet link type.

**Chapter 2: Internet Basics**

**Overview**

**i-Net+ Objectives Covered in This Chapter:**

- Describe a URL, its functions and components, different types of URLs, and use of the appropriate type of URL to access a given type of server. Content may include the following:
  - Protocol
  - Address
  - Port

- Describe the core components of the current Internet infrastructure and how they relate to each other. Content may include the following:
  - Network access points
  - Backbone

- Identify problems with Internet connectivity from source to destination for various types of
servers. Examples could include the following:
- E-mail
- Slow server
- Web site

Describe Internet domain names and DNS. Content could include the following:
- DNS entry types
- Hierarchical structure
- Role of root domain server
- Top level or original domains—edu, com, mil, net, gov, org
- Country level domains—UK

The Internet is a very complex entity. To understand the topics found in later chapters in this book, you must first understand the underlying layout and technologies of the Internet so that you have a common reference point for those discussions. In this chapter, you will learn the following:

- What the Internet is
- Internet layout
- Domain Name Services (DNS)
- Uniform Resource Locators (URLs)
- Internet communications process

Throughout this chapter, you will also learn the terminology of the devices and processes used on the Internet. Let’s begin the discussion of these topics with the definition of the Internet.

**What Is the Internet?**

The simplest definition of the Internet is that it is a collection of local area networks connected together by high-speed public WAN connections. Servers on these LANs provide information to the rest of the Internet in the form of documents, images, and multimedia content. The information delivered by these servers is generally called Internet content. For a small fee, anyone with a computer and a modem can access the Internet and get access to this content. Figure 2.1 shows a graphical representation of the Internet. Notice how individual users and LANs connect to Internet Service Providers (ISPs), which in turn can connect to other ISPs that connect to backbone ISPs. Backbone ISPs are ISPs with very high-speed connections between them (several hundred megabits per second). You will learn about ISPs in the sections to follow.
History of the Internet

The Internet started out as a project of the U.S. government’s Defense Advanced Research Projects Agency (DARPA) in 1973. They wanted to design a network that could reconfigure itself around breaks and faults in case one of its nodes were taken out during a war. The architects of this network, called ARPAnet, took this into consideration and developed a suite of protocols (called TCP/IP) and a network that could do just that.

Another network was developed in 1980 to connect IBM mainframes in university data centers. This network was called BITnet, and it allowed universities to communicate with one another, thus facilitating collaboration among professors at those universities with the first, primitive e-mail system.

In 1983, the Internet Architecture Board (IAB) was formed to guide the development of the TCP/IP protocol suite (the protocol used on the Internet) and to provide research data for the Internet. The IAB consists of two organizations, the Internet Engineering Task Force (IETF) and the Internet Research Task Force (IRTF). The IETF is responsible for the ongoing development of the TCP/IP protocol. When a new TCP/IP protocol is proposed, the IETF issues a Request for Comments (RFC) that details the specifications of the new protocol and how it is to be used. The IRTF, on the other hand, is responsible for researching new Internet technologies and their possible implications on the Internet as a whole.

In 1986, the National Science Foundation (NSF) developed NSFnet as a backbone for the now-emerging Internet. It would connect the old ARPAnet, BITnet, and a bunch of other networks together to form the Internet. At this point, the Internet became very far reaching and very powerful as thousands of people who were now connected to it could all communicate and collaborate.

The Internet Today

Since the days of the NSFnet, ARPAnet, BITnet, and all the others, Internet use has grown exponentially. No longer do only geeks and professors know about it; it has become a part of popular culture. Every television commercial ends with the company name and the address of the company’s Web site so you can visit it and get even more information. One measure of a company’s success is how many hits the company’s Web site gets per day.

It is estimated that in September 1999, there were more than 201 million people worldwide on the Internet, and that number is estimated to double by 2001. Currently, more than 75 percent of all
metropolitan areas in the United States have Internet access. Basically, any household that has a phone line can get access to the Internet (with either a local or a long distance phone call). With each passing year, Internet access technologies allow faster access to the Internet. Home access speeds are available from 33.6Kbps (modems) to 512Kbps (ISDN and DSL access). At these speeds, Internet content can include streaming audio and video.

**The Layout of the Internet**

Even though the Internet is a constantly evolving entity, its areas can be broken down into several basic classifications:

- Access points (ISPs)
- WAN connections
- Backbone providers

Each classification deals with a particular section of the Internet, as shown in Figure 2.2. Notice how the Internet areas connect to each other and what types of connections are used between them.

![Figure 2.2: Layout of the Internet](image)

In the following sections, you will learn the details of each Internet area and the responsibilities each area has within the Internet. You will also learn which areas end users interact with and the different types of ISPs.

**Access Points (ISPs)**

As previously mentioned, anyone can get access to the information found on the Internet, but first they must be connected to the Internet. The Internet has often been called the “Information Superhighway.” I’d actually describe it as an “Internet Toll way.” To get the benefits of the “highway,” you have to pay to get on. Thus, in order to get on the Internet, you have to pay the people who have set up access points to it (similar to the on-ramps of the toll highways). These access points are called Internet Service Providers (ISPs). An ISP has a very high-speed connection (usually capable of transmitting several megabits per second) to the Internet. The ISP then sells slower (several kilobits per second) dial-up or dedicated connections.

ISPs usually have a high-speed LAN, with a large, complex router to connect the LAN to the Internet. Then, on the ISP’s “backbone” (as shown in Figure 2.3) are the ISP’s mail, news, and Web servers, as
well as the routers that provide dial-up and dedicated leased-line access to the Internet for the ISP’s customers. Additionally, some ISPs sell “space” on their backbone to companies so that those companies can place their Web servers directly on the ISP’s backbone for the best possible performance. This practice is called server hosting. In Figure 2.3, notice where the ISP’s backbone is and what items connect to it within an ISP. Also notice that the backbone connects to a router that, in turn, connects the ISP to its own ISP.

Figure 2.3: A typical ISP setup

ISPs can be found in every major city in the U.S. and in almost every rural area. In Europe and the Asian countries, ISPs can be found in the larger cities. However, the Internet’s reach is expanding more and more every day. Very soon it will be possible to get Internet access anywhere on (or off) Earth.

Note To find an ISP in your area, you can look in the Yellow Pages under “Internet providers,” or, if you can get to a machine connected to the Internet, check out The List of ISPs at [http://thelist.internet.com](http://thelist.internet.com).

**WAN Connections**

If the Internet were a living entity, the ISPs would be its appendages and the WAN connections would be the arterial connections between them. A wide area network (WAN) connection is a special phone line that is leased from the local telephone company and used to carry data between two LANs. For our discussion, WAN connections connect two ISPs to provide the Internet with its structure.

WAN connection speeds range from 9600bps to hundreds of megabits per second (Mbps). These WAN connections were covered in detail in Chapter 1, but to summarize, Table 2.1 illustrates some WAN technologies and their associated speeds.

**Table 2.1: Common WAN Connection Technologies**

<table>
<thead>
<tr>
<th>WAN Connection</th>
<th>Common Speed(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>DDS</td>
<td>56Kbps</td>
</tr>
<tr>
<td>Frame Relay</td>
<td>56Kbps-1.544Kbps</td>
</tr>
<tr>
<td>T1</td>
<td>1.544Kbps</td>
</tr>
<tr>
<td>T3</td>
<td>44.736Mbps</td>
</tr>
<tr>
<td>ISDN</td>
<td>128Kbps-2Mbps</td>
</tr>
<tr>
<td>ATM</td>
<td>155Mbps</td>
</tr>
</tbody>
</table>
Backbone Providers

Although the Internet is essentially a network of ISPs, there are a few select ISPs that connect to each other with high-speed WAN connections to provide the Internet with a “backbone.” These ISPs are known as backbone providers (as shown earlier in Figure 2.2) and connect to each other at speeds from 100Mbps to 1Gbps. The Internet backbone is the set of high-speed WAN connections, servers, and ISPs that provide the structure for the Internet.

Many ISPs claim to be backbone providers, but this is usually a marketing gimmick and means that they connect directly to an actual backbone provider but are not actually part of the Internet backbone. Most backbone providers are divisions of telephone companies and are called Network Access Points (NAPs). Sprint and Pacific Bell are examples of NAPs. Originally, there were four major NAPs that connected the Internet. Since that time, several new NAPs have been added, like ICS and Worldcom.

Internet 2—The Next Generation

The current Internet has seen many advancements, but there are even more Internet technologies waiting to be developed, technologies such as IPv6, Quality of Service (QoS), Telemedicine, video multicasting, and many others. A number of them will improve collaboration abilities and directly benefit higher education (as did the technologies of the current Internet). For this reason, a consortium of higher education institutions have gotten together and formed the University Corporation for Advanced Internet Development (UCAID). One of UCAID’s projects is Internet2 (I2), the collection of next-generation Internet applications and technologies being developed for use with the Internet infrastructure in use today. Internet2 is not its own network, as some people incorrectly assume. It is only the name given to the ongoing research of these technologies and their possible applications. Just as the current Internet technologies have their roots in the collaboration efforts of education, it is the hope of the UCAID that the work done with Internet2 will increase the Internet’s usability. For more information, visit UCAID at www.ucaid.edu.

Domain Name Services (DNS)

Domain Name Services (DNS) is a network service that associates alphanumeric host names with the TCP/IP address of a particular Internet host. When surfing the Web, you could refer to a host by its IP address (for example, 201.35.124.12), but it is more common to use a DNS host name (www.sybex.com). Internet host names are used because they are easier to remember than long, dotted-decimal IP addresses. In this section, you will learn what a domain is, how domains are organized within DNS, and the specifics of how to use DNS.

What Are Domains?

Host names are typically the name of a device that has a specific IP address, and on the Internet, they are part of what is known as a fully qualified domain name. A fully qualified domain name consists of a host name and a domain name.
Although you have a Social Security number and can remember it when you need it, life would be difficult if you had to remember the Social Security numbers of all your friends and associates. You might be able to remember the Social Security numbers of as many as 10 friends and relatives, but after that things would get a bit difficult. Likewise, it’s easier to remember www.microsoft.com than it is to remember 198.105.232.6.

The process of finding the host name for any given IP address is known as name resolution, which can be performed in several ways, and we’ll look at all of them in the next few sections. But first you need to understand Internet domains and how they are organized.

Internet Domain Organization

On the Internet, domains are arranged in a hierarchical tree structure. There are seven top-level domains currently in use:

com A commercial organization. Most companies will end up as part of this domain.

edu An educational establishment, such as a university.

gov A branch of the U.S. government.

int An international organization, such as NATO or the United Nations.

mil A branch of the U.S. military.

net A network organization.

org A nonprofit organization.

Warning Unfortunately, the word domain is used in several ways, depending on the context. When the topic is the Internet, a domain refers to a collection of network host computers.

U.S. Domains

Your local ISP is probably a member of the net domain, and your company is probably part of the com domain. The gov and mil domains are reserved strictly for use by the government and the military within the United States. The com domain is by far the largest, followed by the edu domain, and well over 130 countries are represented on the Internet.

New U.S. Domains

Because the com domain is so popular, almost every company has a Web address that ends with .com. Additionally, there are no divisions in any of the domains, especially the com domain. For these reasons, the Internet Assigned Numbers Authority (IANA) has come up with some new top-level domains to further segment the U.S. Internet DNS space, for example:

firm Designed for naming businesses or firms
shop Domain for online shopping centers

web Domain for Web sites relating to information about the WWW

info Domain used for Web sites that provide some useful information to a community (like a community billboard)

arts Domain for cultural and entertainment organizations

rec Domain for completely recreational Web sites

nom Domain for an individual person’s name

.

International Domains

In other parts of the world, the final part of a domain name represents the country in which the server is located: ca for Canada, jp for Japan, uk for Great Britain, and ru for Russia, for example. Figure 2.4 shows an example of the layout of the Internet DNS hierarchy. Notice how the com, edu, and international domains are all at the same level.

![Figure 2.4: Internet DNS domain hierarchy](image)

If you want to contact someone within one of these domains by e-mail, you just add that person’s e-mail name to his domain name, separated by an at sign (@). For example, if you want to e-mail the president of the United States, send your e-mail to this address:

President@whitehouse.gov

InterNIC assigns all Internet domain names and makes sure no names are duplicated. Names are assigned on a first-come, first-served basis, but if you try to register a name that infringes on someone else’s registered trademark, your use of that name will be rescinded if the trademark holder objects.

Now that we have detailed how Internet domain names work and where they came from, we can return to our discussion of name-resolution methods.

Using DNS

The abbreviation DNS stands for Domain Name Services. You use DNS to translate host names and domain names to IP addresses, and vice versa, by means of a standardized lookup table that the network administrator defines and configures. The system works just like a giant telephone directory.
Suppose you are using your browser to surf the Web and you enter the URL http://www.microsoft.com to go to the Microsoft home page. Your Web browser then asks the TCP/IP protocol to ask the DNS server for the IP address of www.microsoft.com. When your Web browser receives this address, it connects to the Microsoft Web server and downloads the home page. DNS is an essential part of any TCP/IP network, simplifying the task of remembering addresses; all you have to do is simply remember the host name and domain name.

The DNS tables that are used to resolve the host name to an IP address are composed of records. Each record is composed of a host name, a record type, and an address. There are several record types, including the address record, the mail exchange record, and the CNAME record.

The **address record**, commonly known as the **A record**, directly maps a host name to an IP address. The example below shows the address record for a host called mail in the company.com domain:

```
mail.company.com. IN A 204.176.47.9
```

The **mail exchange (MX)** record points to the mail exchanger for a particular host. DNS is structured so that you can actually specify several mail exchangers for one host. This feature provides a higher probability that e-mail will actually arrive at its intended destination. The mail exchangers are listed in order in the record, with a priority code that indicates the order in which the mail exchangers should be accessed by other mail delivery systems.

If the first priority doesn’t respond in a given amount of time, the mail delivery system tries the second one, and so on. Here are some sample mail exchange records:

```
host.company.com. IN MX 10 mail.company.com.
host.company.com. IN MX 20 mail2.company.com.
host.company.com. IN MX 30 mail3.company.com.
```

In this example, if the first mail exchanger, mail.company.com, does not respond, the second one, mail2.company.com, is tried, and so on.

The **CNAME record**, or canonical name record, is also commonly known as the **alias record** and allows hosts to have more than one name. For example, your Web server has the host name www, and you want that machine also to have the name ftp so that users can easily FTP in to manage Web pages. You can accomplish this with a CNAME record. Assuming you already have an address record established for the host name www, a CNAME record adding ftp as a host name would look something like this:

```
www.company.com. IN A 204.176.47.2
```

When you put all these record types together in a file, its called a DNS table, and it might look like this:

```
mail.company.com. IN A 204.176.47.9
mail2.company.com. IN A 204.176.47.21
mail3.company.com. IN A 204.176.47.89
host.company.com. IN MX 10 mail.company.com.
host.company.com. IN MX 20 mail2.company.com
host.company.com. IN MX 30 mail3.company.com.
www.company.com. IN A 204.176.47.2
```
You can establish other types of records for specific purposes, but we won’t go into those in this book. DNS can become very complex very quickly, and entire books are dedicated to the DNS system.

Obtaining Your Own Domain Name

It seems like you can’t watch a television commercial these days without seeing at the bottom of the screen a domain name that matches the company name (for example, pizzahut.com for Pizza Hut, ibm.com for IBM, etc.). You may wonder how these names are obtained. It is easy and almost anyone can do it. It costs around $100.00 for a single domain name. The steps are as follows:

1. Choose a domain name (e.g., bobsroom.com).

2. Using your Web browser, go to www.networksolutions.com/ and use their search engine to see if the domain name you want has been taken. If the name you want is available, proceed to step 3. If not, go back to step 1 and start over.

3. Use Network Solution’s Web interface to fill out your contact information as well as the hosting information for the domain. “Hosting” a domain name means that a server has been configured to tell the rest of the Internet where your domain’s servers are. Your ISP can host your new domain name (providing you make arrangements beforehand) or, for a fee, Network Solutions will host it.

4. Complete the form and wait for confirmation of your domain name.

That’s it!

Uniform Resource Locators (URLs)

Everyone who has ever used the World Wide Web (WWW) has more than likely used a Uniform Resource Locator (URL). A URL is a standard way of referring to an Internet resource when making Internet connections and requests. You will primarily use URLs in Web clients (like Navigator and Internet Explorer) and other Internet utilities. A URL consists of several components, including:

- Protocol designation
- DNS name of host
- Path
- Resource name

For all intents and purposes, a URL is an address that tells a utility where to go on the Internet to get a resource and what protocol to use when retrieving it.

Figure 2.5 shows an example of a URL. Notice that there are different parts of the URL.
Figure 2.5: A sample URL

Protocol Designation

The first part of a URL that we are going to discuss is the leftmost portion (immediately to the left of the ://, as shown in Figure 2.6), the protocol designation. The protocol designation tells the utility you are using (in most cases, an Internet browser like Internet Explorer or Navigator) what protocol to use when connecting. Some of the most popular protocols found in URLs include:

- HTTP
- FTP
- FILE
- TELNET

HTTP

The HTTP protocol designation portion of a URL stands for Hypertext Transfer Protocol, which is the transport protocol used for Web content on the Internet. By placing the http:// at the start of the URL, you are indicating to the Web browser that you are making a request of a Web server and that you want to use the HTTP protocol to request and deliver the information.

This is the default protocol designation for most Web browsers. When you enter an address without a protocol designation (e.g., www.yahoo.com) into the Go To or Address line of the Web browser, the Web browser will default to the HTTP protocol designation.

FTP

The FTP protocol designation indicates that the browser will use the File Transfer Protocol (FTP) to transfer files between the specified FTP server and the workstation. When you add ftp:// to the beginning of the URL, the browser will act as an FTP client and will be able to download and upload files using the FTP protocol designation.

TELNET

The TELNET protocol designation indicates that the Web browser will try to connect to the specified host using the TCP/IP Terminal Emulation protocol (TELNET). TELNET allows a user to enter commands on a host without actually typing the commands on the host’s keyboard.

When you specify a URL using telnet://, the browser will actually open another program to provide the
actual Telnet functions because an Internet browser doesn’t have the ability to send TELNET commands. The TELNET protocol designation tells the browser to open up the Telnet client.

**FILE**

The FILE protocol designation is a special one. It actually doesn’t tell the browser what protocol to use, but rather it tells the browser to go and get a file stored either locally on the computer or over a LAN. Typically, this protocol designation would look something like this:

FILE://E:\studeweb\Page.htm

The browser would then display the selected file (if possible).

Note The FILE protocol syntax might look slightly different in different browsers.

**DNS Name of Host**

The next part of a URL is the DNS name of host (as shown in Figure 2.7). This name is the actual DNS name of the host you are connecting to. Refer back to the discussion of DNS earlier in the chapter for an explanation of DNS. A DNS host name for a Web server is most often something like `aaa.something.xxx`, where `aaa` is the local host name (www, ftp, etc.), `something` is the domain name, and `xxx` is a .com, .edu, .net, or other domain extension.

![Figure 2.7: The DNS name of host in a URL](http://www.sybex.com/test/index.html)

Note A TCP/IP address can be used in place of the DNS name of host in a URL.

**Path**

The path portion of a URL (Figure 2.8) indicates the path on the host where the requested resource can be found. This path is relative to the hosting directory on the Internet server. For example, the URL `www.yahoo.com/homes/fargo` points to the /homes/fargo directory under the Web software directory on the `www.yahoo.com` Web server.

![Figure 2.8: The path portion of a URL](http://www.sybex.com/test/index.html)

Note It is important to note that the path portion of a URL can either be short (one directory) or long (more than one directory).

**What the Heck Is a Tilde?**

Sometimes you will see a URL listed like `http://www.somewhere.com/~dgroth/`. Every thing in that URL makes sense except the tilde (~) character. This character has a special purpose. In Web servers
that provide Web hosting for multiple users’ home pages, the ~ indicates to the Web server to get the Web pages from the specified user’s (in our example, dgroth) home directory on that server. Whenever you sign up with an ISP, you are given a user account, a password, and a home directory on a Web server. You can then set up your own home page by placing the HTML files in your home directory (or in a special subdirectory under your home directory). When this method is used, the Web pages are kept relatively secure from other users, but the Web server can still access them.

Resource Name

The last part of a URL (shown in Figure 2.9) is the actual name of the resource you are requesting from the server specified in the URL. For most Web URLs, this name will be the name of an HTML file that is stored on a Web server and that you want to download and display on your computer.

Figure 2.9: The resource name within a URL

There are some URLs that have the name and location of a program here, for example:

http://search.yahoo.com/bin/search?p=Books

This URL is an example of a search performed at www.yahoo.com. In this case, the resource you are requesting is the script program called search, and the search parameter "books" is being passed to the script to perform a search for books. The key to identifying that this is a script is that there is no .html ending on the resource you are requesting and that there is a question mark after the name of the resource along with some search parameters.

Internet Communications Process

The i-Net+ exam tests your knowledge of the behind-the-scenes processes that happen during Internet communications from an Internet client to the various types of servers that exist. Here are the two most common Internet communications process that people discuss:

- HTTP (Web) requests and responses
- SMTP (e-mail) traffic

HTTP (Web) Requests and Responses

The most common type of communication on the Internet is that between a Web browser and a Web server. This communication is known as an HTTP communications session because the request is made using the HTTP protocol. An HTTP communication consists of both a request for data (also known as an HTTP GET) and a response that includes the requested data. Figure 2.10 illustrates the process that occurs when a Web browser makes a request of an HTTP server.
As shown in Figure 2.10, the HTTP communications session consists of four major processes:

1. The browser submits the URL request to the Web server.
2. The browser communicates via TCP/IP and TCP port 80 to the Web server.
3. The Web server receives the request, decodes it, and locates the requested documents.
4. The server returns the requested documents and the Web browser displays them.

Let’s take a brief look at each step.

**Step 1: The Browser Request**

There are two entities involved in any HTTP Web request: the client and the server. The client is most often a Web browser, although other Internet utilities are starting to use HTTP as a request method. The server component is almost always a Web (HTTP) server.

With a Web browser, you make a request of a Web server by entering a URL in the address line and pressing Enter or by clicking a hypertext link in an HTML document. This process initiates a request to the Web server. The request looks something like this:

```
GET http://www.accn.com/index.html HTTP/1.0
```

The GET portion of this request is known as the *HTTP request method*. This can be one of several different options. Some options for the request method are detailed in Table 2.2.

<table>
<thead>
<tr>
<th>Request Method</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>GET</td>
<td>Primary method of retrieving data from a Web server. This method requests a certain document or file from a Web server.</td>
</tr>
<tr>
<td>PUT</td>
<td>A method by which a client can upload a file to a Web server.</td>
</tr>
<tr>
<td>HEAD</td>
<td>A method that instructs an HTTP server to return only header information about a requested resource, not the actual resource itself.</td>
</tr>
</tbody>
</table>

**Step 2: Browser Communication**

Because HTTP is part of the TCP/IP protocol suite, it uses part of the TCP/IP protocol suite as a transport method. Specifically, HTTP uses the Transmission Control Protocol (TCP) as its main
transport protocol. When a Web browser makes an HTTP request of a Web server, HTTP uses TCP port 80 during its communications. A TCP port identifies which TCP/IP process on the server machine the request is destined for. TCP port 80 is the default port address that specifies that the request is destined for an HTTP server process. Other port addresses can be used, but both client and server must be set up specifically to use them.

Note TCP/IP and its protocols are covered in more detail in Chapter 3.

In addition, HTTP requests include information like what (HTML document or multimedia content) is being requested as well as what version of HTTP is being used (HTTP 1.0 in most cases).

**Step 3: Web Server Receives Request**

The third step in the communications process is when the Web server receives the HTTP request and processes it. During this step, the Web server decodes the request and tries to determine exactly what the browser is asking for. Once the browser has determined what the request is, it locates the file(s) asked for in the request and proceeds to the next step, returning the requested information to the client.

**Step 4: The Requested Document Is Returned**

Once the server has found the requested information, it can send it back to the client that requested it. The server sends the data back using TCP or its “cousin,” User Datagram Protocol (UDP). Which protocol is used depends on the type of content being sent. Most HTML documents are sent back using the TCP protocol.

**E-Mail (SMTP and POP3)**

E-mail, like the Web, is almost everywhere these days. All corporate business cards now have e-mail addresses on them. Communications have been enhanced to the point where large amounts of information can be conveyed almost instantaneously as well as efficiently.

E-mail is just a logical, digital version of the U.S. postal system. Digital messages are sent from a computer on one end to a recipient computer. But the message doesn’t go directly from sender to recipient; instead, it passes through several computers on its way to its destination. Internet e-mail is a store-and-forward messaging system, which means the message sits in one location (stored) until a server process moves it to the next location (forwarded). This process repeats until the message arrives at its destination. Figure 2.11 shows a sample Internet mail setup.

![Internet mail setup](image)

Figure 2.11: An Internet mail setup

Internet e-mail consists of two major components:

- Simple Mail Transfer Protocol (SMTP)
- Post Office Protocol 3 (POP3)
Let’s discuss each protocol and how they work together within the Internet to provide the Internet with its messaging system.

**Simple Mail Transfer Protocol (SMTP)**

The Simple Mail Transfer Protocol, as its name suggests, is the TCP/IP suite protocol used to transfer mail between Internet hosts. SMTP is most commonly used between mail clients and mail servers as well as between mail servers.

Like HTTP, SMTP uses TCP. SMTP initiates communications on TCP port 25. All SMTP conversations (either between client and server or between servers) work basically the same way. The sender opens a connection on TCP port 25, and the recipient responds that it is ready by sending back its name, address, and SMTP mail program version. The mail-sending process can then begin. During this process, SMTP uses special SMTP commands to send the mail. Each command has a special function within the SMTP communications process. To illustrate some of the most common SMTP commands, let’s examine a simple SMTP communication:

```
220 mail.somewhere.net ESMTP Sendmail 8.9.3/8.9.3;
Tue, 3 Aug 1999 08:52:14 -0500 (CDT)
HELO corpcomm.net
250 ns1.corpcomm.net Hello fgo1-a9.corpcomm.net
       [209.74.93.19], pleased to meet you
mail from:dgroth@corpcomm.net
250 dgroth@corpcomm.net... Sender ok
rcpt to:llee@sybex.com
250 llee@sybex.com... Recipient ok
data
354 Enter mail, end with "." on a line by itself
Test
Please ignore this message.
David G.
.
250 IAA22065 Message accepted for delivery
```

The first line (the line starting with 220) is the line that the SMTP server responds with, indicating that it is ready to start the conversation. As previously mentioned, this line includes the version of the SMTP service the recipient is running (in this case, Sendmail). The next line (starting with HELO) indicates what domain the sending computer is from. The receiving computer will then verify that the sending computer is actually at the domain it says it is from. This particular feature is fairly new. It was implemented to prevent unauthorized users from using an SMTP mail server to send mail without permission.

Once the receiving computer has verified that it is who it says it is, the sender then uses the mail from command to indicate who sent the mail. The e-mail address that appears after the mail from command is the address that appears in the From line in the header of the sent e-mail. The rcpt to: line tells the receiving computer who the mail’s intended recipient is. This line specifies the e-mail address that appears on the To line of an e-mail.

The last part of this conversation begins with the data command, which indicates to the receiving computer that what follows is the actual body of the e-mail. After the data command, the sending system sends all the data that is part of that e-mail. To signify the end of the data, the sending computer sends a . on a line by itself.
The final line indicates that the mail was sent successfully.

**POP3**

When an e-mail gets sent over the Internet, it uses SMTP until it reaches the mail server at its destination. The e-mail then is stored on the mail server until the client is ready to download it. From there, Post Office Protocol 3 (POP3) is the protocol used to download the mail from the server to the mail client.

Most Internet e-mail clients today use SMTP for sending e-mail and the POP3 protocol for downloading received mail.

Note For more information on POP3, see RFC 1081, which can be found at [www.cis.ohio-state.edu/htbin/rfc/rfc1081.html](http://www.cis.ohio-state.edu/htbin/rfc/rfc1081.html).

**Summary**

In this chapter, you learned the basics of the Internet, including such concepts as the following:

**What the Internet is** The Internet is a collection of local area networks connected together by high-speed public WAN connections. Also, the Internet consists of servers that store Internet content (HTML, graphics, etc.) until it is requested by a client.

**Internet layout** The Internet is completely interconnected. Access points (ISPs) connect to each other using high-speed public telephone lines (WAN connections). Those ISPs then connect to Internet backbone (the highest-speed WAN connections, several gigabits per second).

**Domain Name Services (DNS)** DNS is the service used to translate user-friendly host names into their respective IP addresses. Domain suffixes fall into two categories: U.S. domains (such as com, org, and edu) and international domains (named after their two-letter country code, like .jp for Japan and .de for Germany).

**Uniform Resource Locator (URL)** A URL is the universal way of referring to an Internet resource. They consist of a protocol designation (http:// or ftp://), followed by the DNS name of the host being accessed, then ending with the path of the resource being accessed.

**Internet communications process** The last topic you learned about is the process that happens “behind the scenes” for both Web (HTTP) requests and Internet e-mail (SMTP and POP3) requests. Basically, both processes use a request-response mechanism. The client makes a request; the server processes the request and sends back a response.

**Review Questions**

1. Which protocol is used between a Web server and a Web browser when HTML documents are downloaded during a Web browsing session?
   A. HTML
2. What does URL stand for?
   A. Universal Residence Location
   B. Uniform Resource Locator
   C. Universal Reaction Language
   D. Uniform Residence Language

3. What TCP port do HTTP requests use by default?
   A. 80
   B. 25
   C. 13
   D. 8

4. What TCP port do SMTP requests use by default?
   A. 13
   B. 21
   C. 25
   D. 80

5. Which TCP/IP suite protocol is primarily used to download Internet e-mail from an e-mail server?
   A. SMTP
   B. HTTP
   C. HTML
   D. POP3

6. Which TCP/IP service resolves host names into IP addresses and vice versa?
   A. HTTP
   B. DNS
   C. POP3
7. Which command during an SMTP communications session indicates the actual e-mail recipient to the receiving computer?
   A. `rcpt to`
   B. `data`
   C. `hello`
   D. `mail to`

8. Which items are sent by the receiving server to the sending entity during an SMTP communications session?
   A. IP address of receiving server
   B. DNS name of receiving server
   C. Name and version of receiving server
   D. Name and version of sending entity

9. Which part of the URL `http://www.novell.com/index.html` indicates the protocol that should be used to retrieve the Web document?
   A. `www`
   B. `http://`
   C. `index.html`
   D. `www.novell.com`

10. Which protocol(s) can be used to download files from an Internet server?
    A. HTTP
    B. TELNET
    C. FTP
    D. FILE

11. To which component of the Internet can individual users buy modem connections so that they can get on the Internet?
    A. Backbone ISP
    B. Access point ISP
    C. WAN connection

12. Which part of the URL `http://www.novell.com/index.html` indicates the actual resource being
requested by the Web browser?
A. http://
B. www.novell.com
C. index.html
D. .com

13. Which HTTP request method allows a browser to indicate that it wants a specific file?
A. GET
B. PUT
C. HOLD
D. HEAD

14. Which HTTP request method allows a browser to upload a file to a Web server?
A. GET
B. PUT
C. HOLD
D. HEAD

15. Which DNS root-level domain is classified for schools, colleges, and other educational institutions?
A. sch
B. col
C. edu
D. com

16. Which DNS root-level domain is classified for commercial entities?
A. com
B. edu
C. org
D. gov

17. Which part of the SMTP communications session indicates the e-mail address of the sender?
A. rcpt to
B. HELO
C. data
D. mail from

18. You can send e-mail, but you can’t receive it. Which protocol is most likely to blame?
   A. POP3
   B. SMTP
   C. LDAP
   D. TCP

19. Which HTTP request method allows a browser to request only the header of a document?
   A. GET
   B. PUT
   C. HOLD
   D. HEAD

20. Which protocol designation in a URL is used for viewing a file from the local hard disk in a Web browser?
   A. disk://
   B. file://
   C. http://
   D. C://

Answers to Review Questions

1. B. HTTP is the protocol used for this process. Although FTP can be used for downloads, it is generally not used during the Web browsing session to download HTML files to the browser. HTML and TELNET are invalid answers.

2. B. In Internet parlance, URL is short for Uniform Resource Locator.

3. A. HTTP is used on TCP port 80 (by default). Port 25 is used for SMTP and ports 13 and 8 are for other uses not discussed in this chapter.

4. C. SMTP uses TCP port 25, HTTP uses port 80, FTP uses port 21, and TCP port 13 is used for a special purpose called Daytime (not discussed in this chapter).

5. D. POP3 is the protocol used to download mail from an e-mail server. SMTP is used to send
(upload) mail to an e-mail server. HTTP and HTML generally do not get involved in the client-server e-mail process.

6. B. Domain Name Services (DNS) resolves host names into IP addresses (and vice versa). HTTP is used for Web requests, and POP3 and SMTP are used for receiving and sending e-mail.

7. A. data designates the body of the message, helo starts the communication session. mail to is not an actual command.

8. A, C. The only items that are sent during an SMTP communications session are the IP address of the receiving server and the name and version of the receiving server.

9. B. All the other parts are part of either the DNS host name or the path to the resource being requested.

10. A, C. Both HTTP and FTP can be used to download files from an Internet server. TELNET is used to control a Unix host remotely, and FILE tells the browser to go and get a file stored either locally on the computer or over a LAN.

11. B. Backbone ISPs and WAN connections form the main structure of the Internet. Generally speaking, it is prohibitively expensive to get either a connection to a backbone ISP or your own WAN connection.

12. C. http:// is the protocol designation, www.novell.com is the host being accessed, and .com is the top-level domain of the host being accessed.

13. A. PUT is used to send a request to a Web server.

14. B. PUT is used for uploading files, HEAD is used to retrieve only the header information, and HOLD is not a valid answer.

15. C. edu is used for educational institutions, com is for commercial companies, and the other two don’t exist.

16. A. edu is used for educational institutions, org is generally for nonprofit organizations, and gov is for government institutions.

17. D. rcpt to indicates the recipient, HELO starts the communication session, and data indicates the body of the message.

18. A. POP3 is used to download new mail from an e-mail server. SMTP is used for sending Internet e-mail. LDAP is used for directory queries, and TCP is a transport protocol.

19. D. GET is for retrieving the entire body, PUT is for uploading files, and HOLD doesn’t exist.


Chapter 3: Protocols
Overview

I-Net+ Exam Objectives Covered in This Chapter:

- Describe the nature, purpose, and operational essentials of TCP/IP. Content could include the following:
  - What addresses are and their classifications (A, B, C, D)
  - Determining which ones are valid and which ones are not (subnet masks)
  - Public versus private IP addresses

- Describe the purpose of remote access protocols. Content could include the following:
  - SLIP
  - PPP
  - PPTP
  - Point-to-point/multipoint

- Describe how various protocols or services apply to the function of a mail system, Web system, and file transfer system. Content could include the following:
  - POP3
  - SMTP
  - HTTP
  - FTP
  - NNTP (news servers)
  - TCP/IP
  - LDAP
  - LPR
  - TELNET
  - Gopher

This chapter is about the protocols in use on the Internet. A protocol is nothing more than a set of rules that govern a particular operation. The Internet has many protocols, but the ones you're interested in are those having to do with network communications. Network communications take place using network communications protocols. A network communications protocol is a set of rules that govern network communications. If two computers are going to communicate, they both must be using the same protocol.
The Internet uses many different protocols (most of which are a subset of the TCP/IP protocol suite, which is discussed below). Each protocol governs a specific function (like e-mail, Web browsing, and file transfer). In this chapter, you will learn about protocols, their functions, and which protocols are used on the Internet.

**The TCP/IP Protocol Suite**

The Transmission Control Protocol/Internet Protocol (TCP/IP) suite is a collection, or suite, of protocols that operate together to provide data transport services for the Internet. The TCP/IP protocol suite is the only protocol suite used on the Internet. Because TCP/IP is so central to working with the Internet and with intranets, we’ll discuss it in detail, and then we’ll discuss some of the protocols that make up the TCP/IP protocol suite. We’ll start with some background on TCP/IP and how it came about and then describe the technical goals defined by the original designers.

**A Brief History of TCP/IP**

The TCP/IP protocol was first proposed in 1973, but it was not until 1983 that a standardized version was developed and adopted for wide area use. In that same year, TCP/IP became the official transport mechanism for all connections to ARPAnet, a forerunner of the Internet.

Much of the original work on TCP/IP was done at the University of California, Berkeley, where computer scientists were also working on the Berkeley version of Unix (which eventually grew into the Berkeley Software Distribution [BSD] series of Unix releases). TCP/IP was added to the BSD releases, which in turn was made available to universities and other institutions for the cost of a distribution tape. Thus, TCP/IP began to spread in the academic world, laying the foundation for today’s explosive growth of the Internet, and of intranets as well.

During this time, the TCP/IP family continued to evolve and add new members. One of the most important aspects of this growth was the continuing development of the certification and testing program carried out by the U.S. government to ensure that the published standards, which were free, were met. Publication ensured that the developers did not change anything or add any features specific to their own needs. This open approach has continued to the present day; use of the TCP/IP family of protocols virtually guarantees a trouble-free connection between many hardware and software platforms.

**TCP/IP Design Goals**

When the U.S. Department of Defense began to define the TCP/IP network protocols, their design goals included the following:

- It had to be independent of all hardware and software manufacturers. Even today, this is fundamentally why TCP/IP makes such good sense in the corporate world; it is not tied to IBM, Novell, Microsoft, DEC, or any other specific company.

- It had to have good built-in failure recovery. Because TCP/IP was originally a military proposal, the protocol had to be able to continue operating even if large parts of the network suddenly disappeared from view, say after an enemy attack.

- It had to handle high error rates and still provide completely reliable end-to-end service.
It had to be efficient with a low data overhead. The majority of data packets using the IP protocol have a simple, 20-byte header, which means better performance when compared with other networks. A simple protocol translates directly into faster transmissions, giving more efficient service.

It had to allow the addition of new networks without any service disruptions.

As a result, TCP/IP was developed with each component performing unique and vital functions that allowed all the problems involved in moving data between machines over networks to be solved in an elegant and efficient way. The popularity that the TCP/IP family of protocols enjoys today did not arise just because the protocols were there or even because the U.S. government mandated their use. They are popular because they are robust, solid protocols that solve many of the most difficult networking problems and do so elegantly and efficiently.

Let’s now examine the two major components of the TCP/IP protocol suite, the Transmission Control Protocol and the Internet Protocol, as well as their makeup and functions.

Benefits of Using TCP/IP Rather Than Other Networking Protocols for the Internet

There are several reasons why TCP/IP was chosen as the primary protocol for the Internet:

• TCP/IP is a widely published open standard and is completely independent of any hardware or software manufacturer. Of all the protocols in use today, it is the most ubiquitous and, because of its widespread availability, is a natural choice for the Internet.

• TCP/IP can send data between different computer systems running completely different operating systems, from small PCs all the way to mainframes and everything in between.

• TCP/IP is separated from the underlying hardware and will run over Ethernet, Token Ring, or X.25 networks and even over dial-up telephone lines. Because of this feature, the Internet can use many different types of physical media, including phone lines and network links.

• TCP/IP is a routable protocol, which means it can send datagrams over a specific route, thus reducing traffic on other parts of the network.

• TCP/IP has reliable and efficient data-delivery mechanisms. This is a major advantage on the Internet when links constantly go up and down.

• TCP/IP uses a common addressing scheme. Therefore, any system can address any other system, even in a network as large as the Internet. (This addressing scheme will be covered in “Understanding IP Addressing” later in this chapter.)

The Transmission Control Protocol

The Transmission Control Protocol (TCP) serves to ensure reliable, verifiable data exchange between
hosts on a network. TCP breaks data into pieces, wrapping it with the information needed to route it to its destination, and reassembling the pieces at the receiving end of the communications link. The wrapped and bundled pieces are called datagrams. TCP puts on the datagram a header that provides the information needed to get the data to its destination. The most important information in the header includes the source and destination port numbers, a sequence number for the datagram, and a checksum. Because it can ensure delivery, TCP is known as a connection-oriented protocol.

The source port number and the destination port number allow the data to be sent back and forth to the correct process running on each computer. The sequence number allows the datagrams to be rebuilt in the correct order in the receiving computer, and the checksum allows the protocol to check whether the data sent is the same as the data received. It does this by first totaling the contents of a datagram and inserting that number in the header. This is when IP enters the picture. Once the header is in the datagram, TCP passes the datagram to IP to be routed to its destination. The receiving computer then performs the same calculation, and if the two calculations do not match, an error occurred somewhere along the line and the datagram is resent.

Figure 3.1 shows the layout of the datagram with the TCP header in place.

![Figure 3.1: A datagram with its TCP header](image)

In addition to the source and destination port numbers, the sequence number, and the checksum, a TCP header contains the following information:

**Acknowledgment Number** Indicates that the data was received successfully. If the datagram is damaged in transit, the receiver throws the data away and does not send an acknowledgment back to the sender. After a predefined time-out expires, the sender retransmits data for which no acknowledgment was received.

**Offset** Specifies the length of the header.

**Reserved** Variables set aside for future use.

**Flags** Indicates that this packet is the end of the data or that the data is urgent.

**Window** Provides a way to increase packet size, which improves efficiency in data transfers.

**Urgent Pointer** Gives the location of urgent data.

**Options** A set of variables reserved for future use or for special options as defined by the user of the protocol.

**Padding** Ensures that the header ends on a 32-bit boundary.

The data in the packet immediately follows this header information.
A Summary of TCP Communications

You must remember a few things specifically about TCP communications:

• Flow control allows two systems to cooperate in datagram transmission to prevent overflows and lost packets.

• Acknowledgment lets the sender know that the recipient has received the information.

• Sequencing ensures that packets arrive in the proper order.

• Checksums allow easy detection of lost or corrupted packets.

• Retransmission of lost or corrupted packets is managed in a timely way.

The Internet Protocol

The network routing and addressing portion of TCP/IP is called Internet Protocol. This protocol is what actually moves the data from point A to point B, in a process that is called routing.

IP is referred to as connectionless; that is, it does not swap control information (or handshaking information) before establishing an end-to-end connection and starting a transmission. The Internet Protocol must rely on TCP to determine that the data arrived successfully at its destination and to retransmit the data if it did not. IP’s only job is to route the data to its destination. In this effort, IP inserts its own header in the datagram once it is received from TCP. The main contents of the IP header are the source and destination addresses, the protocol number, and a checksum.

Note You may sometimes hear IP described as unreliable because it contains only minimal error detection or recovery code.

Without the header provided by IP, intermediate routers between the source and destination, commonly called gateways, would not be able to determine where to route the datagram. Figure 3.2 shows the layout of the datagram with the TCP and IP headers in place.

![Figure 3.2: A datagram with TCP and IP headers](image)

Take a look at the fields in the IP header:

Version Defines the IP version number. Version 4 is the current standard, and values of 5 or 6 indicate that special protocols are being used.

IHL (Internet Header Length) Defines the length of the header information. The header length can
vary; the default header is five 32-bit words, and the sixth word is optional.

**TOS (Type of Service)** Indicates the kind or priority of the required service.

**Total Length** Specifies the total length of the datagram, which can be a minimum of 576 bytes and a maximum of 65,536 bytes.

**Identification** Provides information that the receiving system can use to reassemble fragmented datagrams.

**Flags** The first flag bit specifies that the datagram should not be fragmented and must therefore travel over subnetworks that can handle the size without fragmenting it; the second flag bit indicates that the datagram is the last of a fragmented packet.

**Fragmentation Offset** Indicates the original position of the data and is used during reassembly.

**Time to Live** Originally, the time in seconds that the datagram could be in transit; if this time was exceeded, the datagram was considered lost. Now interpreted as a *hop count* and usually set to the default value 32 (for 32 hops), this number is decreased by each router through which the packet passes.

**Protocol** Identifies the protocol type, allowing the use of non-TCP/IP protocols. A value of 6 indicates TCP, and a value of 17 indicates User Datagram Protocol (UDP).

**Header Checksum** An error-checking value that is recalculated at each stop over point; necessary because certain fields change.

**TCP Header** The header added by the TCP part of the protocol suite.

The data in the packet immediately follows this header information.

**Gateways and Routing**

As we mentioned, routing is the process of getting your data from point A to point B. Routing datagrams is similar to driving a car. Before you drive off to your destination, you determine which roads you will take to get there. And along the way, you sometimes have to change your mind and alter your route.

The IP portion of the TCP/IP protocol inserts its header in the datagram, but before the datagram can begin its journey, IP determines whether it knows the destination. If it does, IP sends the datagram on its way. If it doesn’t know and can’t find out, IP sends the datagram to the host’s default gateway.

Each host on a TCP/IP network has a default gateway, an off-ramp for datagrams not destined for the local network. They’re going somewhere else, and the gateway’s job is to forward them to that destination if it knows where it is. Each gateway has a defined set of routing tables that tell the gateway the route to specific destinations.

Because gateways don’t know the location of every IP address, they have their own gateways that act just like any TCP/IP host. In the event that the first gateway doesn’t know the way to the destination, it forwards the datagram to its own gateway. This forwarding, or routing, continues until the datagram reaches its destination. The entire path to the destination is known as the *route*. 
Datagrams intended for the same destination may actually take different routes to get there. Many variables determine the route. For example, overloaded gateways may not respond in a timely manner or may simply refuse to route traffic and time out. That time-out causes the sending gateway to seek an alternate route for the datagram.

Routes can be predefined and made static, and alternate routes can be predefined, providing a maximum probability that your datagrams travel via the shortest and fastest route.

**Ports and Sockets Explained**

On a TCP/IP network, data travels from a port on the sending computer to a port on the receiving computer. A **port** is an address that identifies the application associated with the data. The **source port number** identifies the application that sent the data, and the **destination port number** identifies the application that receives the data. All ports are assigned unique 16-bit numbers in the range 0 through 32,767.

Today, the very existence of ports and their numbers is more or less transparent to the users of the network because many ports are standardized. Thus, a remote computer can know which port it should connect to for a specific service. For example, all servers that offer Telnet services do so on port 23, and Web servers normally run on port 80. This means that when you dial up the Internet to connect to a Web server, you automatically connect to port 80, and when you use Telnet, you automatically connect to port 23. The TCP/IP protocol uses a modifiable lookup table to determine the correct port for the data type. **Table 3.1** lists some of the well-known port numbers for common protocols.

**Table 3.1: Well-Known Port Numbers for Common Protocols**

<table>
<thead>
<tr>
<th>Number</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>21</td>
<td>File Transfer Protocol (FTP)</td>
</tr>
<tr>
<td>23</td>
<td>Telnet</td>
</tr>
<tr>
<td>25</td>
<td>Simple Mail Transfer Protocol (SMTP)</td>
</tr>
<tr>
<td>70</td>
<td>Gopher</td>
</tr>
<tr>
<td>79</td>
<td>Finger</td>
</tr>
<tr>
<td>80</td>
<td>Hypertext Transfer Protocol (HTTP)</td>
</tr>
<tr>
<td>110</td>
<td>Post Office Protocol 3 (POP3)</td>
</tr>
<tr>
<td>119</td>
<td>Network News Transfer Protocol (NNTP)</td>
</tr>
</tbody>
</table>

In multiuser systems, a program can define a port on-the-fly if more than one user requires access to the same service at the same time. Such a port is known as a **dynamically allocated** port and is assigned only when needed, for example, when two remote computers dial in to a third computer and simultaneously request Telnet services on that system.

The combination of an IP address (more on IP addresses in a moment) and a port number is known as a **socket**. A socket identifies a single network process in terms of the entire Internet. You may hear or see the words **socket** and **port** used as if they were interchangeable terms, but they are not. Two sockets, one on the sending system and one on the receiving host, are needed to define a connection for connection-oriented protocols, such as TCP.

Sockets were first developed as a part of the BSD Unix system kernel, in which they allow processes
that are not running at the same time or on the same system to exchange information. You can read data from or write data to a socket just as you can with a file. Socket pairs are bidirectional so that either process can send data to the other.

Understanding IP Addressing

As you saw in “The Internet Protocol” earlier in this chapter, IP moves data between computer systems in the form of a datagram, and each datagram is delivered to the destination port number that is contained in the datagram header. This destination port number, or address, is a standard 16-bit number that contains enough information to identify the receiving network as well as the specific host on that network for which the datagram is intended.

In this section, we’ll go over what IP addresses are, why they are so necessary, and how they are used in TCP/IP networking. But first, we need to clear up a possible source of confusion—Ethernet addresses and IP addresses.

Ethernet Addresses Explained

You may remember that in an earlier section we mentioned that TCP/IP is independent of the underlying network hardware. If you are running on an Ethernet-based network, be careful not to confuse the Ethernet hardware address and the IP address required by TCP/IP.

Each Ethernet network card (and any other NIC, for that matter) has its own unique hardware address, known as the media access control (MAC) address. This hardware address is predefined and preprogrammed on the NIC by the manufacturer of the board as a unique 48-bit number.

The first three parts of this address are called the OUI (Organizationally Unique Identifier) and are assigned by the Institute of Electrical and Electronics Engineers (IEEE). Manufacturers purchase OUIs in blocks and then assign the last three parts of the MAC address, making each assignment unique. Remember, the Ethernet address is predetermined and is hard-coded onto the NIC. A MAC address is a Data Link layer address used in the header of an Ethernet frame. An IP address is a Network layer address. IP addresses are very different; let’s take a look.

IP Addresses Explained

TCP/IP requires that each computer on a TCP/IP network have its own unique IP address. An IP address is a 32-bit number, usually represented as a four-part number with each of the four parts separated by a period or decimal point. You may also hear this method of representation called dotted decimal or quad decimal. In the IP address, each individual byte, or octet as it is sometimes called, can have a usable value in the range 1 through 255.

Note The term octet is the Internet community’s own term for an 8-bit byte, and it came into common use because some of the early computers attached to the Internet had bytes of more than 8 bits; some of DEC’s early systems had bytes of 18 bits.

The way these addresses are used varies according to the class of the network, so all you can say with certainty is that the 32-bit IP address is divided in some way to create an address for the network and an address for each host. In general, though, the higher-order bits of the address make up the network part of the address, and the rest constitutes the host part of the address. In addition, the host part of the
address can be divided further to allow for a subnetwork address. We’ll be looking at all this in more detail in the “IP Address Classifications” and “Understanding Subnets” sections later in this discussion.

Some host addresses are reserved for special use. For example, in all network addresses, host numbers cannot be all 0s or all 255s. An IP host address with all host bits set to 0 identifies the network itself; so 52.0.0.0 refers to network 52. An IP address with all host bits set to 255 is known as a broadcast address. The broadcast address for network 204.176 is 204.176.255.255. A datagram sent to this address is automatically sent to every individual host on the 204.176 network.

Note When addressing nodes, you can never give a host an address where the host portion of the IP address is all zeros or all ones.

InterNIC (Internet Network Information Center) assigns and regulates IP addresses on the Internet; you can get one directly from InterNIC, or you can ask your Internet Service Provider (ISP) to secure an IP address on your behalf. Another strategy is to obtain your address from InterNIC and only use it internally until you are ready to connect to the Internet.

\section*{Intranets and Private IP Addresses}

If you are setting up an intranet and you don’t want to connect to the outside world through the Internet, you don’t need to register with InterNIC the IP addresses you use on your intranet. These IP addresses are called private IP address because they are only valid on the local intranet. Registering your addresses with InterNIC simply ensures that the addresses you propose to use are unique over the entire Internet. These addresses are known as public IP addresses because they are known and valid across the entire Internet. If you never connect to the Internet, there’s no reason to worry about whether your private addresses are redundant with a computer that isn't on your network.

\section*{IP Address Classifications}

The current TCP/IP addressing scheme version is known as IP version 4, or IPv4 (there is a new revision that hasn’t been universally accepted yet, called IPv6, but you’ll learn about that later in this chapter). In the 32-bit IPv4 address, the number of bits used to identify the network and the host vary according to the network class of the address. You’ll need to know that the several classes are as follows:

- **Class A** is used for very large networks only. The high-order bit in a Class A network is always 0, which leaves 7 bits available to define 127 networks. The remaining 24 bits of the address allow each Class A network to hold as many as 16,777,216 hosts. Examples of Class A networks include General Electric, IBM, Hewlett-Packard, Apple, Xerox, DEC, Columbia University, and MIT. All the possible Class A networks are in use, and no more are available.

- **Class B** is used for medium-sized networks. The two high-order bits are always 10, and the remaining bits are used to define 16,384 networks, each with as many as 65,534 hosts attached. Examples of Class B networks include Microsoft and Exxon. All the Class B networks are in use, and no more of them are available either.
Class C is for smaller networks. The three high-order bits are always 110, and the remaining bits are used to define 2,097,152 networks, but each network can have a maximum of only 254 hosts. Class C networks are still available from some ISPs.

Class D is a special multicast address and cannot be used for networks. The four high-order bits are always 1110, and the remaining 28 bits allow access to more than 268 million possible addresses.

Class E is reserved for experimental purposes. The first four bits in the address are always 1111.

Figure 3.3 illustrates the relationships among these classes and shows how the bits are allocated by InterNIC.

Because the bits used to identify the class are combined with the bits that define the network address, you can draw the following conclusions from the size of the first octet, or byte, of the address:

- A value of 126 or less indicates a Class A address. The first octet is the network number; the next three, the host address.
- A value of exactly 127 is reserved as a loopback test address. If you send a message to 127.0.0.1, it should get back to you unless something is wrong with your computer. Using this number as a special test address has the unfortunate effect of wasting more than 24 million possible IP addresses.
- A value of 128 through 191 is a Class B address. The first two octets are the network number, and the last two are the host address.
- A value of 192 through 223 is a Class C address. The first three octets are the network address, and the last octet is the host address.
- A value greater than 223 indicates a reserved address.

Tip Another special address is 192.168.xxx.xxx, an address specified in RFC 1918 as being available for anyone who wants to use IP addressing on a private network but does not want to connect to the Internet. If you fall into this category, you can use this address without the risk of compromising someone else’s registered network address. RFC 1918 also reserves the 10.xxx.xxx.xxx networks and the 172.16.xxx.xxx through 172.32.xxx.xxx networks.

IPv4 vs. IPv6—The Next Generation
With the explosive growth of the Internet, very few public IP addresses are left. There are no Class A addresses left; few, if any, Class Bs; and the Class C addresses that are available are strictly regulated. We are experiencing this shortage of public IP addresses mainly because the current IP addressing scheme, IP version 4 (IPv4 for short), uses a 32-bit addressing scheme that allows for around 17 million node addresses. Because of this short age of IP addresses, a new version of IP, designated IPv6, has been specified. It uses a 128-bit addressing scheme that will allow for more than 70 octillion (70 followed by 27 zeros). That’s enough for each person on earth to have more than a million IP addresses. Should be enough, don’t you think? As this book was being written (Fall 1999), IPv6 had still not received widespread use.

### Understanding Subnets

The current IP addressing scheme provides a flexible solution to the task of addressing thousands of networks, but it is not without problems. The original designers did not envision the Internet growing as large as it has; at that time, a 32-bit address seemed so large that they quickly divided it into different classes of net works to facilitate routing rather than reserving more bits to manage the growth in network addresses. (Who ever thought we would need a PC with more than 640KB of memory?) To solve this problem, and to create a large number of new network addresses, another way of dividing the 32-bit address, called subnetting, was developed.

An IP subnet modifies the IP address by using host address bits as additional network address bits. In other words, the dividing line between the network address and the host address is moved to the right, creating additional networks but reducing the number of hosts that can belong to each network.

When IP networks are subnetted, they can be routed independently, which allows a much better use of address space and available bandwidth. To subnet an IP network, you define a bit mask known as a subnet mask, in which a bit pattern cancels out unwanted bits so that only the bits of interest remain.

Working out subnet masks is one of the most complex tasks in network administration and is not for the faint of heart. If your network consists of a single segment (in other words, there are no routers on your network), you will not have to use this type of subnetting, but if you have two or more segments (or subnets), you will have to make some sort of provision for distributing IP addresses appropriately. You can do just that by using a subnet mask.

The subnet mask is similar in structure to an IP address in that it has four parts, or octets, but now it defines three elements (network, subnet, and host) rather than two (network and host). It works a bit like a template that, when superimposed on top of the IP address, indicates which bits in the IP address identify the network and which bits identify the host. If a bit is on in the mask, that equivalent bit in the address is interpreted as a network bit. If a bit is off in the mask, the bit is part of the host address. The 32-bit value is then converted to dotted-decimal notation. In general, you will only use one subnet mask on your network.

A subnet is only known and understood locally; to the rest of the Internet, the address is still interpreted as a standard IP address. Table 3.2 shows how this all works for the most commonly used standard IP address classes.

### Table 3.2: Default Subnet Masks for Standard IP Address Classes

<table>
<thead>
<tr>
<th>Class</th>
<th>Default Subnet Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>255.0.0.0</td>
</tr>
<tr>
<td>B</td>
<td>255.255.0.0</td>
</tr>
<tr>
<td>C</td>
<td>255.255.255.0</td>
</tr>
</tbody>
</table>
Routers then use the subnet mask to extract the network portion of the address so that they can send the data packets along the proper route on the network.

Because all the Class A and Class B networks are taken, you are most likely to encounter subnet-related issues when working with a Class C network. In the next section, we’ll describe in detail how to subnet a Class C network.

<table>
<thead>
<tr>
<th>Class</th>
<th>Subnet Mask Bit Pattern</th>
<th>Subnet Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>11111111 00000000 00000000 00000000</td>
<td>255.0.0.0</td>
</tr>
<tr>
<td>B</td>
<td>11111111 11111111 00000000 00000000</td>
<td>255.255.0.0</td>
</tr>
<tr>
<td>C</td>
<td>11111111 11111111 11111111 00000000</td>
<td>255.255.255.0</td>
</tr>
</tbody>
</table>

Routers then use the subnet mask to extract the network portion of the address so that they can send the data packets along the proper route on the network.

Because all the Class A and Class B networks are taken, you are most likely to encounter subnet-related issues when working with a Class C network. In the next section, we’ll describe in detail how to subnet a Class C network.

The Advantages of Subnetting

Although subnetting is complex, it does have some advantages:

1. It reduces the size of routing tables.
2. It minimizes network traffic.
3. It isolates networks from others.
4. It maximizes performance.
5. It optimizes IP address space.
6. It enhances the ability to secure a network.

How to Subnet a Class C Network

You can subnet any class IP address, but the most common practice today is to subnet a Class C IP address block, so we’ll discuss that process here. How do you find out the values you can use for a Class C network subnet mask? Remember from the previous discussion that InterNIC defines the leftmost three octets in the address, leaving you with the rightmost octet for your own network addresses? If your network consists of a single segment, you have the following subnet mask:

11111111 11111111 11111111 00000000

When expressed as a decimal number, your address is as follows:

255.255.255.0

Because all of your addresses must match these leftmost 24 bits, you can do what you like with the last 8 bits, given a couple of exceptions that we’ll look at in a moment.
You might decide to divide your network into two equally sized segments, say with the numbers 1 through 127 as the first subnet (00000001 through 01111111 in binary) and the numbers 128 through 255 as the second subnet (10000000 through 11111111 in binary). Now the number inside the subnets can vary only in the last seven places, and the subnet mask becomes:

255.255.255.128

In binary this is:

11111111.11111111.11111111.10000000

Tip Use the Windows Calculator in scientific mode (choose View Ý Scientific) to look at binary-to-decimal and decimal-to-binary conversions. Click the Bin (binary) button, and then type the bit pattern that you want to convert. Click the Dec (decimal) button to display its decimal value; you can also go the other way and display a decimal number in binary form.

Now let’s get back to the exceptions we mentioned. The network number is the first number in each range, so the first subnet’s network number is X.Y.Z.0, and the second’s is X.Y.Z.128 (X, Y, and Z are the octets assigned by InterNIC). The default router address or default gateway is the second number in each range, X.Y.Z.1 and X.Y.Z.129, and the broadcast address is the last address, or X.Y.Z.127 and X.Y.Z.255. You can use all the other addresses within the range as you see fit on your network.

Table 3.3 describes how you can divide a Class C network into four equally sized subnets with a subnet mask of 255.255.255.192. This gives you 61 IP addresses on each subnet once you have accounted for the network, router, and broadcast default addresses.

<table>
<thead>
<tr>
<th>Network Number</th>
<th>Router Address</th>
<th>Broadcast Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>X.Y.Z.0</td>
<td>X.Y.Z.1</td>
<td>X.Y.Z.63</td>
</tr>
<tr>
<td>X.Y.Z.64</td>
<td>X.Y.Z.65</td>
<td>X.Y.Z.127</td>
</tr>
<tr>
<td>X.Y.Z.128</td>
<td>X.Y.Z.129</td>
<td>X.Y.Z.191</td>
</tr>
<tr>
<td>X.Y.Z.192</td>
<td>X.Y.Z.193</td>
<td>X.Y.Z.255</td>
</tr>
</tbody>
</table>

Table 3.4 describes how you can divide a Class C network into eight equally sized subnets with a subnet mask of 255.255.255.224. This gives you 29 IP addresses on each subnet once you have accounted for the network, router, and broadcast default addresses.

<table>
<thead>
<tr>
<th>Network Number</th>
<th>Router Address</th>
<th>Broadcast Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>X.Y.Z.0</td>
<td>X.Y.Z.1</td>
<td>X.Y.Z.31</td>
</tr>
<tr>
<td>X.Y.Z.32</td>
<td>X.Y.Z.33</td>
<td>X.Y.Z.63</td>
</tr>
<tr>
<td>X.Y.Z.64</td>
<td>X.Y.Z.65</td>
<td>X.Y.Z.95</td>
</tr>
<tr>
<td>X.Y.Z.96</td>
<td>X.Y.Z.97</td>
<td>X.Y.Z.127</td>
</tr>
<tr>
<td>X.Y.Z.128</td>
<td>X.Y.Z.129</td>
<td>X.Y.Z.159</td>
</tr>
<tr>
<td>X.Y.Z.160</td>
<td>X.Y.Z.161</td>
<td>X.Y.Z.191</td>
</tr>
<tr>
<td>X.Y.Z.192</td>
<td>X.Y.Z.193</td>
<td>X.Y.Z.223</td>
</tr>
</tbody>
</table>
Classless Inter-Domain Routing (CIDR)

InterNIC no longer gives out addresses under the Class A, B, or C designations. Instead, it uses a method called Classless Inter-Domain Routing (CIDR), usually pronounced “cider.” CIDR networks are described as “slash x” networks; the x represents the number of bits in the IP address range that InterNIC controls. This allows InterNIC to define networks that fall between the old classifications and means that you can get a range of addresses much better suited to your needs than in times past. In CIDR terms, a network classified as a Class C network under the old scheme becomes a slash 24 network because InterNIC controls the leftmost 24 bits and you control the rightmost 8 bits. Table 3.5 shows some example slash x network types.

Table 3.5: Example CIDR Network Types

<table>
<thead>
<tr>
<th>InterNIC Network Type</th>
<th>Subnet Mask</th>
<th>Approximate Number of IP Addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td>slash 8</td>
<td>255.0.0.0</td>
<td>16,000,000</td>
</tr>
<tr>
<td>slash 12</td>
<td>255.240.0.0</td>
<td>1,000,000</td>
</tr>
<tr>
<td>slash 16</td>
<td>255.255.0.0</td>
<td>65,536</td>
</tr>
<tr>
<td>slash 20</td>
<td>255.255.240.0</td>
<td>4,096</td>
</tr>
<tr>
<td>slash 21</td>
<td>255.255.248.0</td>
<td>2,048</td>
</tr>
<tr>
<td>slash 22</td>
<td>255.255.252.0</td>
<td>1,024</td>
</tr>
<tr>
<td>slash 23</td>
<td>255.255.254.0</td>
<td>512</td>
</tr>
<tr>
<td>slash 24</td>
<td>255.255.255.0</td>
<td>256</td>
</tr>
<tr>
<td>slash 25</td>
<td>255.255.255.128</td>
<td>128</td>
</tr>
<tr>
<td>slash 26</td>
<td>255.255.255.192</td>
<td>64</td>
</tr>
<tr>
<td>slash 27</td>
<td>255.255.255.224</td>
<td>32</td>
</tr>
<tr>
<td>slash 28</td>
<td>255.255.255.248</td>
<td>16</td>
</tr>
<tr>
<td>slash 29</td>
<td>255.255.255.248</td>
<td>8</td>
</tr>
<tr>
<td>slash 30</td>
<td>255.255.255.254</td>
<td>4</td>
</tr>
</tbody>
</table>

TCP/IP Remote Access Protocols

The most common way of accessing the Internet for the majority of the people connected is to use some kind of remote access protocol. A remote access protocol manages the connection between a remote computer and a remote access server. Each remote access protocol allows a remote computer to access a remote network in some fashion. In the case of Internet connections, the remote network is the Internet and the remote access protocols allow the remote computer to submit requests and receive data from the Internet.

Three primary remote access protocols are in use today:

- Serial Line Internet Protocol (SLIP)
Point-to-Point Protocol (PPP)

Point-to-Point Tunneling Protocol (PPTP)

Serial Line Internet Protocol (SLIP)

In 1984, students at the University of California, Berkeley, developed SLIP for Unix as a way to transmit TCP/IP over serial connections (such as modem connections over POTS). SLIP operates at both the Physical and Data Link layers of the OSI model. Today, SLIP is found in many network operating systems in addition to Unix. It is being used less frequently with each passing year, though, because it lacks features when compared with other protocols. Although a low overhead is associated with using SLIP and you can use it to transport TCP/IP over serial connections, it does not support encrypted password methods. SLIP is used today primarily to connect a workstation to the Internet or to another network running TCP/IP.

Setting up SLIP for a remote connection requires a SLIP account on the host machine and usually a batch file or a script on the workstation. When SLIP is used to log in to a remote machine, a terminal mode must be configured after login to the remote site so that the script can enter each parameter. If you don’t use a script, you will have to establish the connection and then open a terminal window to log in to the remote access server manually.

Warning: It is difficult to create a batch file that correctly configures SLIP. Our advice is to avoid SLIP when possible and use PPP instead.

Point-to-Point Protocol (PPP)

PPP is used to implement TCP/IP over point-to-point connections (for example, serial and parallel connections). It is most commonly used for remote connections to ISPs and LANs.

PPP uses the Link Control Protocol (LCP) to communicate between a PPP client and a host. LCP tests the link between a client and a PPP host and specifies PPP client configuration. PPP can support several network protocols, and, because it features error checking and flow control and can run over many types of physical media, PPP has almost completely replaced SLIP. In addition, PPP can automatically configure TCP/IP and other protocol parameters. On the down side, high overhead is associated with using PPP, and it is not compatible with some older configurations.

From the technician’s standpoint, PPP is easy to configure. Once you connect to a router using PPP, the router assigns all other TCP/IP parameters. This is typically done with DHCP (Dynamic Host Configuration Protocol). Within the TCP/IP protocol stack, DHCP is the protocol that is used to assign TCP/IP addressing information, including host IP address, subnet mask, and DNS (Domain Name Services) configuration. This information can be assigned over a LAN connection or a dial-up connection. When you connect to an ISP, you are most likely getting your IP address from a DHCP server.

Point-to-Point Tunneling Protocol (PPTP)

PPTP is the Microsoft-created sibling to PPP. It is used to create virtual connections across the Internet using TCP/IP and PPP so that two networks can use the Internet as their WAN link yet retain private network security. PPTP is both simple and secure.
To use PPTP, set up a PPP session between the client and server, typically over the Internet. Once the session is established, create a second dial-up session that uses PPTP to dial through the existing PPP session. The PPTP session tunnels through the existing PPP connection, creating a secure session. In this way, you can use the Internet to create a secure session between the client and the server. Also called a virtual private network, this type of connection is very inexpensive when compared with a direct connection.

PPTP is a good idea for network administrators who want to connect several LANs but don’t want to pay for dedicated leased lines. But, as with any network technology, there can be disadvantages, including the following:

- PPTP is not available on all types of servers.
- PPTP is not a fully accepted standard.
- PPTP is more difficult to set up than PPP.
- Tunneling can reduce throughput.

You can implement PPTP in two ways. First, you can set up a server to act as the gateway to the Internet and to do all the tunneling. The workstations will run normally without any additional configuration. You would usually use this method to connect entire networks. **Figure 3.4** shows two networks connected using PPTP. Notice how the TCP/IP packets are tunneled through an intermediate TCP/IP network (in this case, the Internet).

![Figure 3.4: A PPTP implementation connecting two LANs over the Internet](image)

The second way to use PPTP is to configure a single, remote workstation to connect to a corporate network over the Internet. The workstation is configured to connect to the Internet via an ISP, and the VPN client is configured with the address of the VPN remote access server. The VPN then exists between the VPN client and VPN server. PPTP is often used to provide VPN functions to connect remote workstations to corporate LANs when a workstation must communicate with a corporate network over a dial-up PPP link through an ISP and the link must be secure. An example of this configuration is shown in **Figure 3.5**.
Layer 2 Tunneling Protocol (L2TP)—The Next-Generation Tunneling Protocol

PPTP has been around for awhile as part of Windows NT’s Internet offerings. With the advent of the Secure IP (IPSec) technology (a method of encrypting IP traffic), a new tunneling protocol has been suggested to the IETF (in RFC 2661). This new technology (known as the Layer 2 Tunneling Protocol) uses PPP to tunnel across an intermediate IP network. It takes the best features of the two most common tunneling protocols—PPTP from Microsoft and L2F from Cisco—and merges them into a single tunneling protocol.

Other Internet Protocols

In addition to TCP and IP, the TCP/IP protocol suite has provisions for several different protocols that each have a different function. The i-Net+ exam will test your basic knowledge of these protocols. The other TCP/IP protocols include (but are not limited to):

- HTTP
- FTP
- POP3
- SMTP
- NNTP
- LPR
- LDAP
- TELNET
- Gopher

Many of these protocols are covered in more detail in other chapters, but in the following sections,
you’ll gain a basic understanding of what each protocol does.

**Hypertext Transfer Protocol (HTTP)**

The Hypertext Transfer Protocol (HTTP) is the command and control protocol used to manage communications between a Web browser and a Web server. When you access a Web page on the Internet or on a corporate intranet, you see a mixture of text, graphics, and links to other documents or other Internet resources. HTTP is the protocol that initiates the transport of each of the components of a Web page.

Note For more info on the HTTP communications process, see Chapter 2. Also, the HTTP server is covered in Chapter 4, and the HTTP client is covered in both Chapters 5 and 6.

**File Transfer Protocol (FTP)**

The File Transfer Protocol is a TCP/IP protocol that provides a mechanism for single or multiple file transfers between computer systems; FTP is also the name of the client software used to access the FTP server running on the remote host. The FTP package provides all the tools needed to look at files and directories, change to other directories, and transfer text and binary files from one system to another. File Transfer Protocol uses TCP through port 21 to actually move the files. We’ll look at how to transfer files using FTP in detail in Chapter 6.

**Simple Mail Transfer Protocol (SMTP)**

The Simple Mail Transfer Protocol (SMTP) is the protocol responsible for moving messages from one e-mail server to another. It is also the protocol used to send e-mail from a client to an e-mail server. The e-mail servers run either Post Office Protocol (POP3) or Internet Mail Access Protocol (IMAP) to distribute e-mail messages to users. All e-mail servers that send e-mail to the Internet must be using TCP/IP and an e-mail program that can send e-mail using SMTP.

Note The SMTP communications process is covered in more detail in Chapter 2. Also, SMTP servers are discussed in Chapter 4 and SMTP clients are discussed in more detail in Chapters 5 and 6.

**Post Office Protocol 3 (POP3)**

POP3 is the protocol used to download mail from an Internet (SMTP) mail server. POP3 servers provide a storage mechanism for incoming mail. When a client connects to a POP3 server, all the messages addressed to that client are downloaded; messages cannot be downloaded selectively. Once the messages are downloaded, the user can delete or modify messages without further interaction with the server. In some locations, POP3 is being replaced by another standard, Internet Mail Access Protocol (IMAP).

**Network News Transfer Protocol (NNTP)**

This is the protocol used to transport Internet news (also called Usenet news) between news servers. It is also the protocol used to transport these news articles between news servers and news clients. This protocol is often confused with the Network Time Protocol (NTP), which serves a different purpose.

**Line Printer (LPR) Protocol**
This protocol is used primarily on Unix systems, although Windows NT uses it as well. It is the protocol used to send commands to network printers over TCP/IP. Its name suggests it works only for line printers (also called dot-matrix printers). That’s mainly because, when it was being developed, the majority of the printers in use were line printers.

**Lightweight Directory Access Protocol (LDAP)**

This protocol is seeing increased use as network directories see increased use. The Lightweight Directory Access Protocol is the protocol used to make simple requests of a network directory (like NDS, X.500, or Active Directory). LDAP requests can consist of requests for names, locations, and other information like phone numbers and e-mail addresses. Many Web browsers (including Navigator and Internet Explorer) contain LDAP clients so they can request information from directory servers.

**TELNET**

This protocol is a terminal emulation protocol that allows a workstation to perform a remote logon to another host over the network. It is used primarily to allow users at workstations to access a Unix server and run commands just as if they were sitting at the server’s console.

**Gopher**

Gopher is a text-based utility that was used in the early years of the Internet to search for data and news. It would present selections in a hierarchical format. Gopher was developed from work done at the University of Minnesota; their mascot was the gopher, so they named this technology Gopher. It was the best way to search for information before the Web came along and made everything “friendly.”

Figure 3.6 shows how some of the components we’ve been discussing fit together within the TCP/IP protocol suite. The top layers are the various Internet server applications. Notice that the top layers rely on different bottom layers for transport and other functions.

**Summary**

The TCP/IP protocol suite is the protocol used for all communications on the Internet. In this chapter, you learned about the following concepts:

**The nature, purpose, and operational essentials of TCP/IP** You learned that the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite is the primary protocol suite in use on the Internet. Stations that use TCP/IP are assigned (either manually or automatically) a 32-bit, dotted-decimal number called an IP address. It is represented as four three-digit numbers, like so: `xxx.xxx.xxx.xxx`, where each digit can be any number from 0 to 255.

**Classes of IP addresses** IP addresses are characterized by their class. Table 3.6 details the classes of IP addresses based on the range of the first octet.
Table 3.6: IP Address Classes, Address Ranges, and Default Subnet Masks

<table>
<thead>
<tr>
<th>Class</th>
<th>First Octet Address Range</th>
<th>Default Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>0-126</td>
<td>255.0.0.0</td>
</tr>
<tr>
<td>B</td>
<td>128-191</td>
<td>255.255.0.0</td>
</tr>
<tr>
<td>C</td>
<td>192-223</td>
<td>255.255.255.0</td>
</tr>
</tbody>
</table>

**Remote access protocols** You learned the details of the three most popular remote access TCP/IP protocols: SLIP, PPP, and PPTP. SLIP is the most primitive with the fewest features. PPP is the most often used remote access protocol because it supports protocols other than TCP/IP and it supports error checking and flow control. Finally, PPTP is the protocol used to provide VPN services over TCP/IP.

**Various protocols that make up the TCP/IP protocol suite** The TCP/IP protocol suite is made up of many different individual protocols, each with a different purpose and use. Table 3.7 outlines each protocol and its function.

Table 3.7: TCP/IP Suite Protocols

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Function/Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP</td>
<td>Transporting requests for Internet content from browsers to Web servers and transporting content back to requesting browser</td>
</tr>
<tr>
<td>FTP</td>
<td>Transferring files</td>
</tr>
<tr>
<td>SMTP</td>
<td>Sending e-mail</td>
</tr>
<tr>
<td>TELNET</td>
<td>Terminal emulation</td>
</tr>
<tr>
<td>NNTP</td>
<td>Transporting Internet news between client and server</td>
</tr>
<tr>
<td>LPR</td>
<td>TCP/IP printing</td>
</tr>
<tr>
<td>LDAP</td>
<td>Internet directory queries</td>
</tr>
<tr>
<td>Gopher</td>
<td>Searching Internet data in a hierarchical format</td>
</tr>
</tbody>
</table>

**Review Questions**

1. What is the default subnet mask for a Class C IP address?
   A. 255.0.0.0
   B. 255.255.0.0
   C. 255.255.255.0
   D. 255.255.255.255

2. Which TCP/IP suite protocol is used to transfer text and multimedia content between a Web browser and a Web server?
   A. SMTP
   B. HTTP
   C. POP3
3. The subnet mask 255.255.255.0 corresponds to what CIDR designation?
   A. /8
   B. /24
   C. /29
   D. /30

4. Which TCP/IP suite protocol is used for reliable, point-to-point TCP/IP remote access connections?
   A. PPP
   B. PPTP
   C. CIDR
   D. TCP

5. If you were given an IP address of 176.58.24.1 for your machine, but no subnet mask, what subnet mask could you use by default?
   A. 255.0.0.0
   B. 255.255.0.0
   C. 255.255.255.0
   D. 255.255.255.255

6. Which of the following addresses is an invalid TCP/IP address to assign to a host?
   A. 204.67.129.1
   B. 7.21.1.1
   C. 170.200.1.1
   D. 191.260.42.1

7. Which TCP/IP protocol(s) can be used for Internet mail?
   A. LDAP
   B. SMTP
   C. NNTP
   D. FTP
8. Which subnet mask corresponds to a CIDR designation of /8?
   A. 255.0.0.0
   B. 255.240.0.0
   C. 255.255.0.0
   D. 255.255.240.0

9. Which remote access technology allows secure TCP/IP network connections over the Internet?
   A. PPP
   B. SLIP
   C. SMTP
   D. PPTP

10. Which of the following TCP/IP addresses are considered broadcast addresses?
    A. 201.123.45.255
    B. 34.1.0.0
    C. 107.28.94.1
    D. 79.0.0.0

11. What is the default TCP port number for a POP3 connection?
    A. 21
    B. 25
    C. 80
    D. 110

12. Which protocol is used for Internet directory queries?
    A. SMTP
    B. LDAP
    C. POP3
    D. NNTP

13. What is the default subnet mask for the IP address 18.204.37.112?
    A. 255.0.0.0
    B. 255.255.0.0
14. Which TCP/IP protocol is used for sending print jobs to TCP/IP printers?
   A. POP3
   B. SMTP
   C. LPR
   D. NNTP

15. Which of the following addresses could you assign to an Internet host?
   A. 192.168.10.2
   B. 208.34.109.255
   C. 67.22.22.22
   D. 255.12.37.109

16. What is the default subnet mask for a Class B IP address?
   A. 255.255.0.0
   B. 0.0.0.255
   C. 255.255.255.0
   D. 255.0.0.0

17. If your ISP gave you a TCP/IP address of 204.153.129.0/24, what subnet mask would you use?
   A. 255.255.0.0
   B. 255.255.255.0
   C. 255.0.0.0
   D. 0.0.0.0

18. What is the TCP/IP protocol used for sending and receiving Internet news?
   A. FTP
   B. HTTP
   C. LDAP
   D. NNTP
19. Which TCP/IP protocol is the primary protocol used to transfer text and binary files on the Internet?
   A. SMTP
   B. FTP
   C. LDAP
   D. LPR

20. Which TCP/IP protocol is used to search Internet text and news for information?
   A. SMTP
   B. Gopher
   C. Telnet
   D. FTP

Answers to Review Questions

1. C. 255.0.0.0 is Class A, 255.255.0.0 is Class B, and 255.255.255.255 is a broadcast address.

2. B. SMTP is used for sending e-mail, POP3 is used for downloading e-mail, and LDAP is used for directory queries.

3. B. A designation of /24 means the leftmost 24 bits refer to the network portion of a TCP/IP address and the rightmost 8 bits (the remainder) are used to assign host addresses. The leftmost 24 bits out of 32 bits corresponds to a subnet mask of 255.255.255.0.

4. A. Of all the answers listed, PPP is the only remote access protocol used for reliable, TCP/IP, point-to-point communications.

5. B. Because the IP address begins with 176, your address would be a Class B address. The default subnet mask for a Class B address is 255.255.0.0.

6. D. The largest number you can use in a TCP/IP address is 255. 260 is larger than 255, so it is invalid.

7. B. LDAP is used for Internet directory queries, NNTP is used for Internet news, and FTP is used for file transfer.

8. A. A CIDR designation of /8 means that the leftmost 8 bits of an address refer to the network portion. This would correspond to a subnet mask of 255.0.0.0

9. D. PPTP is used for secure communications over the Internet. PPP and SLIP are primarily used for point-to-point communications, and SMTP is used for sending e-mail.

10. A. 201.123.45.255 is the only broadcast address because all host bits are set to 1 (255 in decimal).
107.28.94.1 is a valid IP address, and 34.1.0.0 and 79.0.0.0 are IP addresses that refer to a specific network.

11. D. 110 is used for POP3 communications. Port 21 is used for FTP communications, 25 is used for SMTP, and 80 is used for HTTP.

12. B. SMTP is used for sending Internet e-mail, POP3 is used to download Internet e-mail, and NNTP is used to send and receive Internet news.

13. A. 18.204.37.112 is a Class A address. 255.0.0.0 is the default subnet mask for a Class A address. 255.255.0.0 is for a Class B, 255.255.255.0 is for a Class C, and 255.255.255.255 is a reserved address.

14. C. POP3 is used for downloading mail, SMTP is the protocol for sending mail, and NNTP is used for sending and receiving Internet news.

15. C. 208.34.109.255 and 255.12.37.109 are reserved addresses for broadcasts. 192.168.10.2 is a reserved address for intranets and cannot be routed on the Internet.

16. A. Of the answers listed, 255.255.0.0 is the default subnet mask for a Class B IP address.

17. B. A /24 CIDR designation is equivalent to a standard Class C address with a default subnet mask of 255.255.255.0.

18. D. FTP is used for uploading and downloading files, HTTP is the protocol used for transferring HTML documents and images from a Web server, and LDAP is used for making directory queries.

19. B. SMTP is used for sending Internet e-mail, LDAP is used to make Internet directory queries, and LPR is used to send print jobs to TCP/IP printers.

20. B. Gopher is the protocol used to search the Internet for text and news. SMTP is used for sending Internet mail, Telnet is used for remotely accessing a Unix host, and FTP is used for downloading and uploading files.

Chapter 4: Servers and Their Functions

Overview

i-Net+ Exam Objectives Covered in This Chapter:

- Describe the purpose of various servers—what they are, their functionality, and features. Content could include the following:
  - Proxy
  - Mail
  - Mirrored
Web (HTTP) Servers

Web servers make up a specific class of servers that use a special program or service to provide HTML and other Internet content to clients via TCP/IP. Web servers get their name from the World Wide Web (WWW), which is a network of servers that provide Internet content from a server back end to a graphical client (also known as a browser). Actually, Web server is somewhat of a misnomer because all servers that serve up some kind of graphical content to a Web browser using the Hypertext Transfer Protocol (HTTP) are generically called Web servers. Although, more specifically, they should be called HTTP servers because that's really what they are. Only HTTP servers that are on the WWW should be called Web servers. For the purpose of this discussion, unless otherwise noted, an HTTP server and a Web server are the same thing.

Note Because the i-Net+ exam focuses more on Web servers than it does other types of servers, they will receive the most coverage in this chapter.

How Web (HTTP) Servers Work

Web servers are actually fairly simple compared to some other types of specialized servers (e.g., database servers). First of all, Web servers run a specialized program or service called an HTTP daemon (pronounced “dee-mon” or “day-mon,” depending on whom you ask). This process is really what makes a Web server a Web server. The daemon runs as a process within the NOS and is responsible for responding to all requests from a Web browser. These responses include negotiation for an HTTP connection and the actual delivery of files. HTTP daemons are made by several different companies and
for several different NOS platforms. The different brand names are covered in “Examples of Web Server Software” later in this chapter.

In addition to HTTP daemons, Web servers may have capabilities for running scripts. A script is simply a small program that the server executes when a particular action is requested on a Web page. For example, some Web pages have forms that you can fill out to send information to the owner of the Web site. Most often, a script will gather the information from the form, compress it into a readable message, then e-mail it to a predetermined e-mail address. Scripts will be covered in more detail in Chapter 8.

Basically, an HTTP server works something like this: The HTTP daemon sits idle until it receives a request from a Web browser. When the daemon receives a request, it decodes it, locates the requested document, file, or script, and returns the requested information to the requesting Web browser.

Note For more information on the specifics of HTTP, see RFC 2068 at www.ietf.org.

Uses for Web Servers

Even though Web servers are relatively simple in how they operate, they are used for a variety of applications. The Web’s greatest power is its ability to deliver all kinds of information in an easy-to-use, consistent manner. Because Web browsers are fairly ubiquitous on computers these days, and so many employees have access to them, many companies are trying to leverage their investment in a Web server by using it to deliver a variety of information, including:

- Company information
- Public advertisements
- Technical information
- Stock quotes
- Classified ads
- Statistical data

Web servers can deliver all this information quickly and easily. Many software developers have realized this, and as such, more and more software programs (primarily office suite applications) give the user the ability to save data to HTML for mat so that it can be viewed using a Web browser.

Web servers can be classified into three major categories, based on their use and the type of data they deliver:

- Internet servers
- Intranet servers
- E-commerce server

In the following sections, you’ll learn about each type of Web server and the differences between them.
Internet Servers

Everyone that has ever “surfed the Web” has accessed an Internet Web server. An Internet Web server is just a Web server that serves public HTML and other content to all clients on the Internet. Public content is information that is published to the Internet for everyone to read. Content might include the following:

- Company location and contact information
- Product catalogs
- Stock quotes

Mainly, what differentiates an Internet Web server from other types of Web servers is that an Internet Web server serves public content over the Internet. You could say that it serves public content over a public medium (the Internet).

Additionally, Internet servers are usually supported by high-powered hardware to make it possible for a large amount of people to visit a site and retrieve public company and product information. This translates into company revenue because the more powerful the Web server’s hardware, the more simultaneous connections the server can support, and thus, more people can be simultaneously looking at a company’s Web site.

Note For an example of an Internet server, check out www.sybex.com and note all the public information.

Intranet Servers

Intranet servers are HTTP servers that are located on a company’s LAN and serve information only to employees of that company or other users who have been given authority to view it. Intranet servers serve private company information and content and usually require that the user requesting the information log in with a username and password. Private content includes information you wouldn’t want a competitor to have access to, including:

- Company policy manual
- Company memos
- Company news (not for general release)
- Human resources information
- Corporate e-mail
- Corporate phone directory

Intranet servers generally serve this private content over a private medium, the LAN. All users on the LAN access this Web server and this information using their Web browsers from a machine located inside the company firewall.

Note In some cases, a company will use some kind of secure authentication method to make private
When the term *intranet* was first introduced, most people thought it was a misspelling of *Internet*. But companies soon saw that it was valuable to have a standard way of accessing company information. Rather than using several different programs to disseminate information (for example, Word processing, spreadsheet, and e-mail programs), they could place the information in a central repository (the intranet server), and it could be accessed using a standard program (the Web browser) that everyone already knew how to use.

In smaller companies with limited budgets, the company Internet server doubles as an intranet server. In larger companies, the Internet server and intranet server are usually two different machines and are most often located on two different areas of the network.

Note If you work for a company that has an intranet Web server, you know what kind of information is available. In this case, we can’t give you a URL because the information on most intranets is private!

**E-Commerce Servers**

E-commerce is a relatively new term coined by industry analysts. It is the exchange of money and goods just as commerce is, but with e-commerce, the Internet is the exchange medium. A great number of consumers are gravitating toward making more and more of their purchases via the Internet. This trend is occurring because most companies who sell over the Internet can provide their products in a one- or two-day time frame and at a much lower cost than those selling through more traditional retail methods. This appeals to people with an “instant gratification” purchase mentality. For example, suppose you needed an Ethernet print server for your laser printer. You check with a few local vendors, but no one has it in stock, and you would have had to wait four to five days for it to be ordered. You can order it through an online vendor and receive it the next day. If you have a problem with it, you can call the company’s customer service line and receive the replacement the next day. In an era where “retail customer service” is an oxymoron, e-commerce is proving to be profitable for many companies.

To provide e-commerce, a company needs to implement an e-commerce server. An e-commerce server is basically an Internet Web server that provides e-commerce services through Web server scripts or programs. Some of the e-commerce services commonly found on an e-commerce server include:

- **Catalog search service**  A search service allows a prospective customer to search a “virtual catalog” of the products being sold on the Web site. The customer simply types some words or a part number in a form and clicks a button to start the search. The catalog search service returns items that match the search and displays them in a list. The customer can then select the item she wants to view or perform a different search.

- **Virtual shopping cart services** A potential Web customer can select items one at a time, and the shopping cart service remembers each item as if it were in a “virtual shopping cart.” When the customer is done shopping, he clicks a Check Out button (or something similar). The server then tallies up all the items and displays a list in invoice format, along with a subtotal, taxes (if applicable), and shipping costs. The customer can modify his virtual shopping cart by removing items, adding additional items, and choosing appropriate shipping methods. When the customer is satisfied, he chooses an Accept button. The customer is then asked to provide personal (address, phone, and e-mail, usually) and payment information, and the order is processed. This service is the heart of the e-commerce server.
credit card authentication Many payment options are available over the Internet, including C.O.D., check, cashier’s check, and credit cards. However, using a credit card is the most efficient method of payment; money is transferred more quickly, and thus, the order is processed quickly. Customers can pay for their products immediately, and their order is processed immediately without human intervention. Credit card authentication is usually performed with a script that runs alongside all the other e-commerce services on a Web server. When a customer wants to pay with a credit card, she enters the card number and expiration date along with the order amount on a secure Web page. This information is submitted to the Web server over a secure connection. The Web server then sends the card information to the credit card authentication service, which acts like the little credit card machines in a common retail store. The authentication service contacts (either via a dial-up connection or via the Internet) the appropriate credit card company’s server and indicates that the customer wants to make a purchase for a certain amount. The credit card company then returns either a rejection or a confirmation with an authorization number. The Web server’s credit card authentication service returns that information to both the company’s accounts receivable database and the user’s Web browser. These programs also indicate to the shopping cart service that the purchase was successful and the order can be initiated.

E-mail order verification Once the order has been placed, the e-commerce server (usually the virtual shopping cart program) will display the complete order in a Web browser window along with an order number so that the order can be tracked. The user can print this information for his records. To ensure that the user gets the information, a copy is sent to the e-mail address specified when the user entered his personal information. Most e-commerce Web sites will not let you place an order unless you enter at least your name, phone number, and e-mail address (along with appropriate payment information).

Note For secure orders, some e-commerce sites may use certificate servers (discussed in the sidebar “Secure Connections Using Certificate Authorities”) to prove customers’ identities.

E-commerce Web sites are currently a hot trend. To make money to offset the cost of putting up their Web site, some companies will sell items even if the primary purpose of the site is to disseminate information.


Secure Connections Using Certificate Authorities

More and more Internet sales transactions are taking place. The number of sales increases exponentially every day, so it stands to reason that there are people who make it their business to intercept sales communications and (criminally) use the information they gain to their advantage. It is therefore necessary to provide a method for private, secure communications. Today, this is done on the Internet with either secure transmissions using Secure Sockets Layer (SSL) or public key/private key cryptography using digital certificates and certificate servers. Web sites that use SSL have addresses that begin with https://.

Certificates, on the other hand, allow both the client and the server to prove their identity by presenting a digital version of an identity card. Using a special key, this digital identity card (called a digital certificate) is “signed” by a server that both the sender and receiver trust. The server is known as a certificate authority (also called a certificate server). The certificate server uses information from the requester and other third parties (like credit card companies) to verify the identity of the requester and to create the digital certificate. A server that provides e-commerce through the use of certificate authorities or other third-party security is known as a Commercially Secured Server (CSS).
Examples of Web Server Software

Since the growth of the Internet exploded, there have been a multitude of Web server platforms available. The most common software available for a NOS is currently an HTTP daemon (Web server) of some type. Web server software comes in many different types and interfaces. Each type differs in the platforms it supports and the way it is administered. To prepare you for the i-Net+ exam, this section will cover a few of the most commonly used HTTP daemons, including:

- HTTPd
- IIS
- Apache

We’ll discuss the features of each type of HTTP daemon and the platforms each supports.

NCSA HTTPd

The first HTTP daemon was developed by the National Center for Supercomputing Applications (NCSA) at the University of Illinois at Urbana-Champaign. It is known as HTTPd (short for HTTP daemon) and is the HTTP daemon that most other Web daemons are based on. HTTPd is free; you can download it from the NCSA Web site along with all documentation and source code. It was developed for use on Unix systems and is available for use on most Unix platforms.

Note For more information on HTTPd, visit www.ncsa.uiuc.edu or www.cern.ch.

Microsoft IIS

When Microsoft finally realized the value of the Internet, they hastily threw together an HTTP daemon for their Windows NT operating system. This daemon is known as Microsoft Internet Information Server (IIS). Over time, it has developed into a robust HTTP server platform. The two main advantages of IIS are its cost and ease of use. IIS comes free with Windows NT and with some service packs. IIS version 2 comes free with NT Server 4 (IIS 2 is upgraded to version 3 with service pack 2 or later), and IIS version 4 is available free of charge on the NT Option Pack CD. As this book is being written, all versions of IIS are free of charge. The most current version of IIS, IIS 5, is included in Windows 2000 Server. Additionally, it is extremely easy to configure this Web server because the administration program is fully graphical and Windows based. The graphical utility used to administer IIS is known as the Microsoft Internet Service Manager (ISM), and it’s used to administer all of the Microsoft Internet services running on the same NT server as the ISM. Most first-time administrators configure IIS with out a great deal of training or knowledge of the inner workings of Windows NT.

Unfortunately, these advantages don’t come without a price. IIS only runs on Windows NT. That’s fine if all you have are Windows NT servers, but if you want to run IIS and you don’t have an NT server on your network, you must install one.

Note For more information on IIS, check out www.microsoft.com/backoffice/.
**Apache**

As this book is being written, the Linux operating system is gaining popularity in the corporate network as a Web server platform. The main reason for this is the Apache Web server. Supposedly, Apache got its name because it is “a patchy” version of the NCSA HTTPd. In reality, Apache is based on the NCSA HTTPd, but it has been rewritten and has had features added so that it is now its own HTTP daemon. According to a recent survey (www.netcraft.com/Survey/), Apache is the most commonly used Web server.

Apache was developed first for the Linux operating system. But, because the source code for Apache is freely available, Apache versions can be found for many other NOSes, including most versions of Unix as well as Windows NT and OS/2.

Apache’s main advantage is that it is a freely available, stable, HTTP daemon. The downside is that it can be relatively difficult for the average administrator to configure, especially if he isn’t familiar with the administration of Unix daemons.

Note For more information about Apache, check out www.apache.org.

**“Mirrored” Web Sites**

A Web site mirror is an exact copy of a Web site that is located at a different domain name. Web sites are mirrored for a variety of reasons. Occasionally, a Web site is extremely popular, and the Web server hosting the site can’t keep up with all the traffic. So the owner places copies of the Web site in different geographic areas so that people in those areas can access the mirror instead of the actual site. For example, Yahoo.com is probably one of the biggest search engines in use today. It has mirrors in many countries, and it is usually faster for people to obtain information from their “local” mirror than to go to the main site.

Popular FTP sites are mirrored as well. This is done so that popular files are available for download from multiple locations, thus spreading the load across multiple servers.

**FTP Servers**

An FTP server is any server that provides files to clients using the FTP protocol (a subset of the TCP/IP protocol suite, as discussed in Chapter 3). An FTP server is usually the next server that a company will set up once their Web server is installed and operational. HTTP and FTP are complimentary technologies. When you visit a computer company Web site and look for technical support information, there will often be an area where you can download support files (for example, patches, documentation, and so on). As a matter of fact, many Web software companies have FTP server software that compliments their HTTP server nicely. For example, when you install Microsoft’s IIS, you have the option of installing the IIS FTP server as well.

In this section, you’ll learn how an FTP server works and some uses for them. We’ll also give you some examples of FTP servers.
How FTP Servers Work

FTP servers are similar in function to HTTP servers in that FTP servers also use a daemon (called an FTP daemon) to respond to client requests. FTP servers are a bit more complex than HTTP servers, however. Whereas HTTP daemons respond to a very limited set of commands, FTP daemons respond to a wide array of commands. These commands will be covered in more detail in Chapter 5.

FTP daemons run on a server and wait until they receive a request for an FTP connection from an FTP client. The FTP daemon then responds to the client and asks the user to log in. The user sends a username and password to tell the server who is requesting the file. Because most Internet sites don’t need to regulate who can download files, many sites allow Anonymous or FTP as a username and will accept any text as the password. Anonymous users are generally not allowed to upload or delete files, but they can download files.

Once the user logs in, she can request a file. When the FTP daemon receives this request, it sends the requested file back to the requesting client.

Note The FTP process will be covered in more detail in Chapter 5, where FTP clients are discussed.

Uses for FTP Servers

As already stated, FTP servers are typically used for supplemental file delivery from a company’s Web site. They are more flexible than Web servers for file delivery because they allow files to be uploaded as well as downloaded and at the same time maintain security.

The biggest use of FTP servers on both the Internet and intranets is for archival file storage and delivery. For example, there are many Web sites on the Internet that store shareware and make it available for anyone to download. These “software warehouses” store many gigabytes of software and usually have a Web interface that allows people to get descriptions of the software they’re looking for and then click a link to download the file. An example of this type of FTP site is ftp.cdrom.com, which hosts thousands of files and can be searched via the Web site.

Examples of FTP Servers

Just as with HTTP servers, there are myriad FTP daemons. Some come free with the NOS (as in the case of FTPd), whereas others must be purchased. The two most popular FTP daemons are the Unix daemon, FTPd, and Microsoft’s IIS. Here, you’ll learn the differences between the two and the platforms they run on.

FTPd

The FTP Daemon (FTPd) is the FTP daemon used on most Unix-based servers. As is the case with the other Unix-based daemons (like HTTPd and Telnet), it was the first FTP daemon platform developed. The majority of software companies that make FTP daemon software base it on FTPd. Most versions of Unix include a version of FTPd for free.

IIS

Microsoft has included an FTP server in Internet Information Server (IIS). When you install IIS onto a Windows NT machine, you have the option of installing the FTP server component of IIS. During the
installation, the IIS installation program asks you which directory you want to “publish” to the Internet so that people can download files. Once it’s installed, people on the Internet will be able to download files from the specified directory.

IIS has the benefit of being the easiest FTP server to install and administer. The same administration program used to administer the HTTP server component of IIS (Microsoft Internet Service Manager) is also used to administer the FTP daemon portion.

**News (NNTP) Servers**

Most ISPs today have at least one news server to allow their subscribers access to Internet news articles. *News servers* are those Internet servers that store and distribute Usenet news articles using the Network News Transfer Protocol (NNTP). As discussed in Chapter 3, NNTP is one of the protocols in the TCP/IP protocol suite. The following sections will discuss the details of NNTP servers, including how they work, some common uses, and some examples.

**How News (NNTP) Servers Work**

Just like the other Internet servers, news servers use a daemon to respond to requests and to deliver news messages. NNTP clients communicate with the NNTP daemon to send and receive news articles. These news articles are simply text messages that are organized by subject into categories (called newsgroups). For example, there is a newsgroup called alt.autos.studebaker. The messages contained in this newsgroup pertain primarily to Studebaker automobiles. When you want to post a message to the Internet about Studebakers, you send the message to your local news server and designate that it belongs in the alt.autos.studebaker newsgroup. Then, those with similar interests can look at the alt.autos.studebaker newsgroup, see your message, and respond. They can respond by either posting a message back to the newsgroup or e-mailing you directly.

The individual newsgroups are stored in directories on the news server. When a client first connects to the news server, it requests a list of all newsgroups stored on the server. The server responds with a complete list of the names of all the newsgroups it stores. This can take a while because, typically, thousands of individual newsgroups exist (a typical ISP lists over 50,000). Once the client chooses a newsgroup to view, it sends a request to the news server to retrieve all the headers (that is, the Subject line, the To line, and the From line) of the messages in the newsgroup. You might be asking, “Why not download all of the message?” Well, you may not want to read every message, so it downloads only the headers so you can decide which message(s) you want to read. Then, when you click a particular message in the client, the client requests the remainder of the message. The server then locates the full message body and returns it to the client.

In addition to allowing clients to read messages, NNTP servers will send out messages that they receive, either from clients or from other servers. NNTP servers can be configured to send all their messages to other NNTP servers. Additionally, the servers that “push” news messages can also receive messages. In this way, messages that get posted to one news server will be propagated throughout the Internet. Because of this distribution mechanism, newsgroups are among the most powerful collaboration tools on the Internet.

**Uses for News Servers**

News servers have two main uses; both of them have to do with providing an area for discussions to take place. First, as described earlier, newsgroups provide an area for discussions to take place on the
Internet. Users from all over the world can discuss their favorite topics (like Studebakers) just as if they were talking in the same room.

Second, newsgroups provide a discussion area for LAN (not Internet) users only. Users within a company can discuss company issues in a secure environment without having to meet face-to-face. You can do this by implementing a news server on your LAN without allowing it to communicate with Internet news servers. The advantage is the same as it is for Internet news servers: collaboration among several people without face-to-face contact. This use is not as common as the Internet variety, but it is useful and it is done.

Examples of News Servers

There are several Internet news daemons available, but the majority of them are available for Unix only. There are very few news daemons for NT, NetWare, or other platforms, mainly because NNTP is a bit more complex and difficult to configure. In addition, because of the performance and hardware support required to host 50,000+ newsgroups and upload and download all those messages, the NOS that scales the best for this application is Unix.

Note Don’t get us wrong. News daemons do exist for other platforms besides Unix, but most ISPs run their news daemon on a Unix box.

The most common news daemon is the Internet News Daemon (INND, also referred to as simply INN). Versions of it are available for free download from the Internet for most versions of Unix, including Solaris, AIX, SVR4, and BSD. Originally written by Rich Salz, INND development was taken over in 1996 by the Internet Software Consortium (ISC, a group of people dedicated to developing free, open source Internet software). INND is a stable news server with many features, including:

- Binary message support
- Scalability
- Technical support contracts available (not bad for freeware)

As this book is being written, INND version 2.2.1 has just been released and is available for FTP download from the ISC. Their Web site is at www.isc.org, where you can find more detailed information on INND.

Mail (SMTP) Servers

Apart from Web servers, Internet mail (SMTP) servers are the second most-installed servers that companies will implement when setting up their Internet presence. An SMTP mail server will allow all the users within a company to send and receive e-mail across the Internet using the Simple Mail Transfer Protocol (SMTP). As you most likely know, e-mail servers allow people to communicate quickly, efficiently, and cheaply. It’s no wonder they’re popular.

How Mail (SMTP) Servers Work

As other types of Internet servers do, SMTP servers use a daemon to perform all operations. The daemon waits until someone wants to send mail to it. Once an entity makes a TCP connection to the
SMTP daemon using TCP port 25, the daemon responds and indicates its readiness to receive the mail. The sender then tells the SMTP daemon who the mail is from and who it’s for and sends the body of the message. Once the body of the message is sent, the daemon verifies the integrity of the message and makes sure it is being sent to a valid address. The daemon will then perform a DNS lookup to find the IP address of the mail host for the recipient’s domain (for example, if you’re sending mail to bob@somewhere.com, the daemon tries to find the mail host for the somewhere.com domain). If the DNS server reports that no such host exists, the entire message is returned to the sender indicating that it was "undeliverable."

If the DNS query finds the IP address of the recipient’s domain’s SMTP mail server, the sending SMTP daemon will open a connection to the destination mail server and try to send the message. If it can’t, the sending daemon will hold it in its “waiting to send” queue and try again at some later time (exactly when is a configurable parameter). If it can’t deliver it after a specified amount of time has passed (another configurable parameter), it will return it to the sender with a message saying that the message was undeliverable after multiple retries.

When the message arrives at the destination daemon, the destination daemon will deliver it to the appropriate directory where the message will wait until it is read by the end user (either using a terminal client, like Pine, or through a POP3 client, discussed in Chapter 5).

Uses for Mail Servers

Obviously, the main use for mail servers is to send and receive e-mail. However, within that general definition, mail servers can play many different roles. First of all, a mail server can be a host mail server for an ISP. That means all the mail for the users on that ISP gets sent to and is stored on that mail server.

Also, mail servers can perform a function known as SMTP relaying. SMTP relay servers are servers that perform SMTP relaying by simply forwarding e-mail that is coming from any SMTP client or server to a destination SMTP server. They are used when a client can’t send e-mail directly to its destination on the Internet.

Finally, some mail servers are used as e-mail list servers. List servers are servers that facilitate discussion among various people using e-mail to communicate. List servers are e-mail servers that use special add-on software configured with a special e-mail address (something like majordomo@domain.com) and a list of the e-mail addresses of the people who want to participate in the discussion. Any e-mail sent to the list server’s e-mail address gets forwarded to all e-mail addresses in the list. The forwarded message contains the list server’s e-mail address as the "reply to" address so that, when any member of the list replies to a message, the reply gets sent to all others on the list.

Warning Using list servers is a great way to communicate ideas to a large amount of people, but it’s also a great way to overload your mail server.

Examples of SMTP Mail Servers

The most commonly used SMTP daemon (and, therefore, probably the best example) is the Unix SMTP daemon, Sendmail. Sendmail is freely available over the Internet for most versions of Unix, including SVR4, BSD, Solaris, and Linux. Other SMTP mail servers are available for Unix and other NOS platforms, but Sendmail is the most popular and the one used by most ISPs. It was the first SMTP daemon developed, and most current SMTP daemons are based on the technology found in Sendmail.
Sendmail is very complex. It requires extensive configuration to function properly. Because of its complexity, many books have been written on the configuration of the Sendmail daemon, so we won’t devote a great deal of time to it here.

SMTP Gateways

You may be asking, “Well, my company doesn’t use Sendmail; we use _______ (fill in the blank with any commercial e-mail product), but my company’s e-mail software can e-mail to and from the Internet just fine. What’s up?” Commercial e-mail software like Microsoft’s Exchange and Novell’s GroupWise can also connect to the Internet and be mail servers, but they are primarily designed to be LAN e-mail servers only. To provide SMTP functionality, both require an add-on SMTP gateway to allow them to communicate with the Internet. However, once an SMTP gateway is installed, these two e-mail packages can do everything described in this section, including acting as a mail relay host (although this is configurable).

Proxy Servers

A proxy server is one of several solutions to the problems associated with connecting your intranet or corporate network to the Internet. A proxy server is a program that handles traffic to external host systems on behalf of the client software running on the protected network. This means that clients access the Internet through the proxy server. It’s a bit like those one-way mirrors—you can see out of it, but a potential intruder cannot see in.

Many proxy servers can cache documents, which is particularly useful if a number of clients request the same document independently; the client request is filled more quickly, and Internet traffic is reduced. Caching can be of the following types:

**Active caching** The proxy server uses periods of low activity to go out and retrieve documents it thinks will be requested by clients in the near future.

**Passive caching** The proxy server waits for a client to make a request, retrieves the document, and then decides whether to cache it.

Note Some documents, such as those from a paid subscription service or those requiring specific authentication, cannot be cached.

**How Proxy Servers Work**
A proxy server sits between a user on your network and a server out on the Internet. Instead of communicating with each other directly, each talks to the proxy (in other words, to a “stand-in”). From the user’s point of view, the proxy server presents the illusion that the user is dealing with a genuine Internet server. To the real server on the Internet, the proxy server gives the illusion that the real server is dealing directly with the user on the internal network. So depending on which way you are facing, a proxy server can be both a client and a server. The point to remember here is that the user is never in direct contact with the Internet server, as Figure 4.1 illustrates.

However, the proxy server doesn’t just forward requests from your users to the Internet and back. Because it examines and makes decisions about the requests that it processes, it can control what your users can do. Depending on the details of your security policy, client requests can be approved and forwarded, or they can be denied. Rather than requiring that the same restrictions be enforced for all users, many advanced proxy server packages can offer different capabilities to different users.

There are two types of proxies: Winsock proxies and HTTP proxies. Winsock proxies make any kind of TCP/IP request (including FTP, HTTP, etc.) on behalf of client stations. Winsock proxies require a special piece of software on the client station. These proxies also allow TCP/IP requests to be made at the workstation using any protocol. You don’t have to have TCP/IP installed or configured on the workstation to use a Winsock proxy. Most proxies fall into this category. HTTP proxies, on the other hand, simply make Web requests on behalf of a Web browser. Both types are often implemented on networks.

Warning A proxy server can only be effective if it is the only connection between an internal network and the Internet. As soon as you allow another connection that does not go through a proxy server, your network is at risk.

Uses for Proxy Servers

Proxy servers are commonly found on networks that are connected to the Internet. Because proxies examine every packet going between the Internet and the stations on the LAN, they make great firewalls. Many proxy servers have the capability to configure “allowed traffic types.” This may slow down performance, but for companies without the resources to implement a separate firewall, a proxy with this capability may be the best choice.

If the proxy server does caching, it can improve Internet “surfing” and download performance. Many companies will implement a proxy to increase total Internet performance if they only have a 56Kbps connection to the Internet (like a slow Frame Relay, ISDN, or dial-up connection). In our company, we
have a 56Kbps modem connected to an NT server and Microsoft Proxy Server installed. With all 
browsers on our home network configured to use the proxy, all the computers on the network can surf 
the Internet with pretty good performance (and only use one phone line and, thus, one Internet 
connection).

Examples of Proxy Servers

Because of the popularity of proxy servers, many software companies are selling proxy server software. 
There are even a few proxy servers available for free download. Here, you’ll learn about two examples 
of proxy servers: Microsoft Proxy Server and the proxy server component of the Apache Web server. 
You’ll learn the differences between the two and the platforms they support.

Microsoft Proxy Server

One of the most popular proxy servers is Microsoft Proxy Server (usually abbreviated MS Proxy 
Server). Its popularity is due to its dependence on the Windows NT platform. Currently at version 2, MS 
Proxy Server is available only for Windows NT systems. Because many companies have chosen 
Windows NT for their Internet server platform, the advantage here is that you don’t have to learn 
another NOS.

Another of MS Proxy Server’s features is its ease of administration. Just like the Microsoft FTP and 
HTTP server, you can use the Microsoft Internet Service Manager to administer the properties of MS 
Proxy Server. Once you have learned how to use the Internet Service Manager to administer one Internet 
service, it’s simply a matter of learning the specifics for each particular service. You don’t need to learn 
how to use a different administration tool for each service. Additionally, because most MS Proxy Server 
properties are configured correctly during installation, you should rarely have to do much administration 
after installation.

Unlike many of the components discussed in this chapter, MS Proxy Server isn’t free; it must be 
purchased either from Microsoft or a distributor of Microsoft products. However, as this book is being 
written, you can buy MS Proxy Server for $995.00 retail (you should be able to find it at a reduced price 
through software clearing houses and warehouse stores). You can download a free trial version from 
Microsoft’s Web site at [www.microsoft.com](http://www.microsoft.com), but it will expire and be nonfunctional after 90 days.

MS Proxy Server is a great proxy server if you have Windows NT already installed, although it may not 
make financial sense to put in a Windows NT server if you don’t already have one.

Note More information on Microsoft Proxy Server can be found at the proxy portion of the Microsoft 

Apache

The freeware Apache HTTP server discussed earlier includes a proxy server module so that the server 
running the Apache HTTP daemon can also be a proxy server. This functionality is possible with 
versions only after version 1.2. Because Apache is mainly available for Unix, its caching server has the 
same NOS requirement.

Apache costs less than MS Proxy Server (it’s free), and because, by most people’s account, Unix is a 
higher-performance operating system, Apache will have better performance as a proxy server as well. It 
should be noted, however, that different combinations of hardware and software can produce different
performance results. Keeping this in mind, although there are exceptions, it is generally accepted that a
Unix-based HTTP or Winsock proxy is faster than an NT-based one.

Directory Servers

The buzzword in the information technology business these days is directory. A directory, as it applies
to networking, is a centralized repository of network resource information. This information can be used
for network management purposes or other useful applications. A network directory contains
information such as what kind of users, servers, printers, and so on exist on a network. Each item
(usually called an object) and its associated properties (for example, phone number, department,
address, etc.) can be searched through a standard query language. For example, if you had a network of
250 people and you wanted to e-mail some one but didn’t know her e-mail address, you could use a
program to query the directory and find the e-mail address.

Directories have been around for years. Only recently have they been popular with the Internet crowd.
The biggest use for directories on the Internet is repositories of personal information. A directory server
is a server that stores directory information and makes it available to the Internet for searches. A great
example of a directory server is Switchboard (www.switchboard.com). With it, you can look for
anyone or any business. To look for people, for example, all you need to know is their last name
(although you may want to supply the server with more information).

There are many public directory servers on the Internet and each one is slightly different. For this
reason, a standard request and access protocol was developed. This protocol is the Lightweight
Directory Access Protocol (LDAP), and it is used to provide a common access method for the myriad of
directories that exist. Additionally, there is a standard method of organizing and naming entries in these
directories. This standard is known as the X.500 directory naming scheme, and many Internet directories
conform to this naming standard.

Note It is important to note that LDAP is not a directory, but a directory access method. There is no
such thing as an LDAP directory. A more plausible moniker would be an LDAP-compliant
directory service.

Note For more information on LDAP, refer to the University of Michigan’s (the developers of LDAP)
Web site, www.umich.edu/~dirsvcs/ldap/doc/. More information on X.500 can be found at

How Directory (LDAP) Servers Work

Most public directory servers use two daemons to provide directory services to the network and to the
Internet. The first daemon (which has different names depending on the directory service used) is
responsible for managing the directory itself. A directory is, for the most part, a large, relational
database that requires maintenance to stay current. This first daemon indexes the entire directory so
searches can be performed. It also responds to directory calls in its own (non-LDAP) query language
and protocol. The second daemon is used to provide LDAP access to the directory. The LDAP daemon
waits until an LDAP query is received. The LDAP daemon formats the query in the directory’s native
query language and passes the query on to the directory service daemon. The directory service daemon
retrieves the requested information and passes it back to the LDAP daemon, which in turn returns the
information to the requesting client.

Uses for Directory Servers
As previously mentioned, directory servers on the Internet are primarily used to look up information about people. On servers like those at www.four11.com and www.whowhere.com, you can search for addresses, phone numbers, and e-mail addresses of people you know using only part of their name for the query. For example, if you had a friend in high school that you lost touch with over the years and you know his name and the state you think he lives in, you could go to one of these directory servers and type in the information you know. The directory server would return the pertinent contact information for the people who match the query. Of course, there’s no guarantee that your old high school friend will be among those listed, but the chances are pretty good.

Some companies use directory servers on their intranet as a company telephone directory. Rather than referring to a paper book or list of hundreds of names and telephone numbers, employees can type their requests into an LDAP client of some kind and query their company’s directory server to find the phone number (and other information) of any other employee. The advantage to the company is that it saves paper and is much more efficient.

Examples of Directory Servers

The best example of a directory server is any server running Novell Directory Services (NDS), the default directory service for Novell NetWare versions 4.x and above. NDS LDAP functionality is provided by an additional module (LDAP Services for NDS) that can be downloaded from Novell’s software download Web site (www.novell.com/download/) for free. NDS is the most widely used directory service, and it is also the most flexible.

For Internet servers, there are a number of choices, each with different advantages for different applications. But one of the most common LDAP servers in use is the Netscape Directory Server. It is available for many platforms, including various flavors of Unix and Windows NT. It’s popular because many people use the Netscape Enterprise server as their main Internet or intranet Web server, or they use the Netscape Web browser and they are already familiar with the administration of Netscape’s products.


Telnet Servers

A Telnet server is any server that uses the Telnet daemon and protocol to allow a user to access the console of a machine over a TCP/IP network as though she were sitting at the console. In the context of Internet sites, there are very few dedicated Telnet servers. Most Internet users prefer to receive their information in the graphical Web browser. Plus, allowing any user on the Internet access to a server’s console is a large security breach!

In the following sections, you’ll learn how Telnet servers work. We’ll also give you the most common examples of Telnet servers.

How Telnet Servers Work
Servers that can be accessed via Telnet are usually running some form of a Telnet daemon. The Telnet daemon runs on the Unix server and waits for Telnet connections. When you telnet in to a Unix box, you run a Telnet client and connect to the Telnet daemon over a TCP/IP connection. When you type on the keyboard, each keystroke is sent from the client to the Telnet daemon. The Telnet daemon sends the keystroke on to the Unix kernel, just as if you were sitting at the Unix server’s console typing the commands. The Unix kernel then returns the display of the character that was typed to the Telnet daemon, which in turn sends it back to the Telnet client, where it is displayed on the screen.

Each keystroke is displayed in this manner. As mentioned, the Unix server doesn’t know whether a client is “telnetted in” or is sitting at the keyboard of the Unix server.

Note Telnet is primarily a feature of Unix machines, although third-party utilities allow telnetting into any machine that has a text interface and can run a Telnet daemon.

Uses for Telnet Servers

There are two primary uses for a Telnet server. The first is to allow remote administration of any server running the Telnet daemon. If the server running the Telnet daemon is connected to the Internet, an administrator could use a Telnet client to connect to the server and perform various administrative tasks like adding users, deleting users, running programs, and shutting down the system.

The other use is to provide LAN and Internet users access to text-based Unix applications through a Telnet client. In this application, a client can connect to a Unix server and run the application as though she were sitting at the machine. This use is not very popular because this approach opens up the server to potential security threats. Potential hackers would have access to the server’s console—not a very desirable situation.

Examples of Telnet Servers

Because the great majority of Telnet servers are Unix-based servers, it’s no surprise that the most popular Telnet daemon is the Unix Telnet daemon, TELNETd. When you install any brand of Unix, the installation program will install several Unix components, and the Telnet daemon is almost always included. This service will automatically be started when Unix boots, and you will be able to telnet in to the server from any client on the network.

Summary

In this chapter, you learned about all the different kinds of Internet servers in use today (and covered on the i-Net+ exam), as well as how they work and their common use(s). The chapter also included some examples of each type of server. All these Internet servers use some kind of daemon (a network service that runs on the server and waits for a connection from a client of some kind). Table 4.1 lists the various types of servers and the names of the most common daemons for each.

<table>
<thead>
<tr>
<th>Server</th>
<th>Common Daemon Name(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web (HTTP) server</td>
<td>NCSA HTTPd, Microsoft IIS</td>
</tr>
<tr>
<td>FTP server</td>
<td>NCSA FTPd, Microsoft IIS, Apache</td>
</tr>
<tr>
<td>News (NNTP) server</td>
<td>INND</td>
</tr>
</tbody>
</table>
HTTP servers

HTTP servers are the most popular type of server on the Internet. They are most commonly used for delivering documents and other content to Web browsers using the Hypertext Transfer Protocol (HTTP). Additionally, they are used to provide e-commerce services (buying products and services over the Internet).

FTP servers

FTP servers allow people to download files over the Internet. Often, these servers are used in conjunction with HTTP servers so that users can use the Web to search for the files and then use FTP to download them.

News servers

News servers provide an area for discussions to take place over the Internet. They store and forward news messages and deliver them using the Network News Transfer Protocol (NNTP). News messages are organized by topic into discussion groups called newsgroups.

Mail (SMTP) servers

Mail servers provide messaging services over the Internet by storing and forwarding Internet e-mail messages. When forwarding messages, Internet mail servers use the Simple Mail Transfer Protocol (SMTP).

Proxy servers

Proxy servers provide Internet services on behalf of their clients. Clients make requests to an Internet server, but the request goes to the proxy server first. The proxy server then makes the request on behalf of the requesting client. The response comes back to the proxy server, which returns it to the requesting client. To increase performance, proxy servers can also cache the responses; then, the next time a Web browser makes a similar request, the proxy responds at a much faster speed than the requested server would.

Directory servers

Directory servers provide directory information to requesting clients using the Lightweight Directory Access Protocol (LDAP). Directory servers can provide names, e-mail addresses, phone numbers, and location information to requesting clients.

Telnet servers

Telnet servers are most often Unix machines and run a Telnet daemon, which allows clients to access the console as if they were using the keyboard of the Telnet server itself.

Table 4.2: Some Examples of Common Servers

<table>
<thead>
<tr>
<th>Type of server</th>
<th>Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web (HTTP)</td>
<td><a href="http://www.sybex.com">http://www.sybex.com</a></td>
</tr>
<tr>
<td>FTP</td>
<td>FTP://ftp.cdrom.com</td>
</tr>
<tr>
<td>News (NNTP)</td>
<td><a href="http://www.dejanews.com">http://www.dejanews.com</a></td>
</tr>
</tbody>
</table>

Table 4.2 lists the URLs of some Web sites that offer examples of some of the types of servers discussed in this chapter. You could also visit your ISP’s home page for a list of some of these servers it may have.
Review Questions

1. Which protocol is used by Internet mail servers for delivering Internet mail?
   A. HTTP
   B. FTP
   C. SMTP
   D. NNTP

2. Which of the following is an example of an HTTP server?
   A. IIS
   B. Sendmail
   C. TELNETd
   D. INN

3. Which server, when implemented, would allow you to perform searches for information on people and their e-mail addresses?
   A. Directory server
   B. FTP server
   C. Mail server
   D. Telnet server

4. Which protocol is used by Internet Web servers to deliver content to Web browsers?
   A. FTP
   B. HTTP
   C. LDAP
   D. NNTP

5. Which Internet server(s) can function in more than one capacity (i.e., serve more than one type of client)?
   A. IIS
   B. Apache
6. Which Internet server can increase the performance of Web surfing?
   A. Proxy server
   B. HTTP server
   C. FTP server
   D. SMTP server

7. Which HTTP server(s) is/are available for free download from the Internet?
   A. NDS
   B. FTPd
   C. Apache
   D. INN

8. Which protocol is most often used for file transfer?
   A. SMTP
   B. LDAP
   C. NNTP
   D. FTP

9. In order to be an e-commerce server, a Web server must offer what service(s)?
   A. File transfer
   B. credit card authentication
   C. Virtual shopping cart services
   D. Directory queries

10. Which FTP daemon is available for Unix?
    A. IIS
    B. FTPd
    C. INN
    D. LDAP
11. Telnet daemons are installed by default on which NOS platform(s)?
   A. NetWare
   B. Windows NT
   C. Unix
   D. OS/2

12. Apache is an example of which kind of Internet server?
   A. HTTP
   B. FTP
   C. News
   D. SMTP

13. What TCP/IP protocol is used to access directory servers?
   A. NNTP
   B. FTP
   C. SMTP
   D. LDAP

14. What is the default TCP/IP suite protocol used to communicate between Internet news servers?
   A. NNTP
   B. FTP
   C. SMTP
   D. LDAP

15. Which of the following is an example of a Unix Internet news daemon?
   A. FTPd
   B. INN
   C. IIS
   D. HTTPd

16. What is the name of the utility used to administer IIS?
   A. Services Manager
   B. Internet Service Manager
C. Internet Information Server Manager

D. Services Control Panel

17. Which of the following Internet servers does not run on Windows NT?
   A. IIS
   B. INN
   C. Apache
   D. Microsoft Proxy Server

18. A __________ is an SMTP server that sends any e-mails it receives to a list of e-mail recipients, thus forming a kind of “discussion group.”
   A. List server
   B. E-commerce server
   C. News server
   D. Web server

19. Novell’s NDS can be used as a __________ server.
   A. Web
   B. FTP
   C. Directory
   D. News

20. A __________ server is a type of Internet server that is used for e-commerce and facilitates secure transactions.
   A. FTP
   B. Certificate
   C. Directory
   D. Telnet

Answers to Review Questions

1. C. SMTP is the only protocol used by Internet mail servers to deliver mail. The other protocols are used for different Internet services.

2. A. The other daemons listed are used for other Internet services.
3. A. None of the other servers can perform this kind of search.

4. B. The Hypertext Transfer Protocol (HTTP) is used to deliver content from Web servers to Web browsers. FTP is used to transfer files, LDAP is for directory access, and NNTP is used by news servers.

5. A, B. IIS has components for HTTP, FTP, and proxy serving. Apache has components for HTTP and proxy serving. INN is for Internet news and SMTP is for Internet mail.

6. A. Proxy servers can cache the responses to Internet requests and provide them (at a much faster rate) to other clients when they make the same request.

7. C. Of all the answers listed, Apache is the only Web server and, consequently, the correct answer. NDS is a directory server, FTPd is an FTP server, and INN is a news server.

8. D. Although SMTP and NNTP might be used to transfer files as attachments to messages, FTP is the protocol used to directly transfer files from server to client.

9. B, C. These two services are the key services that, apart from content, make a regular HTTP server into an e-commerce server. File transfer and directory queries are functions of other types of servers.

10. B. Of those listed, FTPd is the only FTP daemon available for Unix.

11. C. Unix is the only platform that currently installs a Telnet daemon by default. The other NOSes listed may have Telnet capability, but it is an add-on feature.

12. A. Apache is a free HTTP server.

13. D. LDAP is the protocol used to access directory servers over the Internet. NNTP is used for Internet news, FTP is used for file transfer, and SMTP is used for e-mail.

14. A. NNTP is the TCP/IP protocol used to deliver Internet news. LDAP is the protocol used to access directory servers over the Internet, FTP is used for file transfer, and SMTP is used for e-mail.

15. B. The Internet News Daemon (INN) is the only daemon listed that can provide access to Internet news. FTPd is for FTP; HTTPd and IIS are for Web services.

16. B. The Microsoft Internet Service Manager is used to administer IIS and all its components.

17. B. The Internet News Daemon is only available for Unix (although attempts are being made to recompile it for Windows NT).

18. A. List servers are the only servers that perform this function.

19. C. Novell Directory Services (NDS), when used only with LDAP Services for NDS, can be used as a directory server. NDS is a directory service and cannot be used as a Web, FTP, or news server.
20. B. Certificate servers are used in conjunction with e-commerce servers to ensure that both sender and receiver in an e-commerce transaction are who they say they are.

Chapter 5: Internet Clients

Overview

i-Net+ Exam Objectives Covered in This Chapter:

1. Describe the infrastructure needed to support an Internet client. Content could include the following:
   • TCP/IP stack
   • Operating system
   • Network connection
   • Web browser
   • E-mail
   • Hardware platform (PC, handheld device, WebTV, Internet phone)

In Chapter 4, you learned about all the different types of servers that can be found on the Internet, how they work, and what they are used for, and you looked at some examples of each type of server. You’ll remember from earlier chapters that the server is only one half of the client-server equation. You’ve learned about the server portion of the equation; now it’s time to learn about the other half: Internet clients.

Of the Internet components, Internet clients are the most visible. An Internet client is the combination of hardware and software that allows a user to interact with servers on the Internet. The Internet client formats server requests, sends the requests to the server, and displays the results when they are received from the server.

In this chapter, you’ll learn about the most common clients used on the Internet and the requirements for using them.

Internet Client Requirements

In order to use a client to make requests of the Internet, you must have a few items in place. These items make it possible for you to run the client application and use it for Internet requests:

1. Hardware
1. Operating system
1. TCP/IP
Internet connection

Without these items, you won’t be able to use the Internet at all. Agreed—some of them are pretty obvious, but you should at least know that they are required. In this section, you will learn what items are required to run a client and use it to connect to the Internet.

Hardware

Hardware is any computer item that you can touch. Internet clients do require some type(s) of hardware in order to run. The following sections will discuss all of the hardware issues relating to Internet clients, including the following:

- Hardware requirements
- Internet client hardware platforms
- Connection hardware

You’ll learn the impact each item has on Internet client use.

Hardware Requirements

Each client software package has its own hardware requirements, usually listed on the side of the box or on the manufacturer’s Web site. If the hardware requirements aren’t met, the software either won’t run at all or will run poorly. The following list includes some of the hardware requirements you’ll come across for client software:

Minimum processor speed Specifies the slowest possible processor (CPU) the client will run on. Although the software will run if the processor in your PC is the same as this value, to realize the best possible performance, it is commonly recommended that you have a processor in your computer that is newer (faster) than the specified processor.

Minimum RAM Specifies the minimum amount of memory (RAM) you must have installed in your PC for the client software to run correctly. The specification is usually given in megabytes (MB). However, for best performance, make sure the RAM configuration in your computer exceeds this requirement.

Hard disk space required Signifies how much disk space (megabytes, or MB) the client will require in order to be installed on your system. This number is usually pretty accurate, but it’s never a bad idea to have a bit more than the requirement.

Tip Because many software companies are realizing that software won’t run well at the “minimum” requirements, some are now releasing “suggested” configurations. When at all possible, ensure that your computer is at the suggested hardware level rather than the minimum.

Internet Client Hardware Platforms

Internet clients have to run on some type of electronic hardware device. These devices fall into one of two categories, each with its own merits and disadvantages. We’ll describe two of the platforms: the personal computer (PC) and the Internet appliance.
Personal Computer

Many homes have personal computers today. A personal computer (PC) is the most common Internet client hardware platform—mainly because it is so flexible. In addition to supporting Internet clients, a PC can be used to play games and use productivity applications (like a word processor or a spreadsheet program). Therefore, a PC’s main advantage is its flexibility. Its main disadvantage is its cost, which is, however, continuing to drop. In fact, nowadays, it’s possible to buy a PC for less than $1,000 for the entire system, including a printer.

Internet Appliance

Those that can’t (or won’t) buy a PC for their home may instead have an Internet appliance like Microsoft’s WebTV. An Internet appliance is a device that you connect to your television and to a phone line to provide Internet access without a computer. Internet appliances usually come with a wireless keyboard so you can type information into forms and search engines. If your main reason for owning a PC is to search the Web, an Internet appliance may be a better choice. However, there are a few drawbacks:

- It has limited upgradability.
- You are required to sign up with the Internet appliance manufacturer’s Internet Service Provider (ISP).
- There is little support for JavaScript or other client-side scripting technologies.
- It can’t be used for other applications (for example, word processing).
- You can’t install third-party utilities on it. If it’s not built in to the “box,” the box probably can’t run it.

Other Devices

These days, many devices can be used as Internet hardware platforms, including cellular phones, Internet phones, and handheld PCs. Many different hardware devices are being created to allow different ways of accessing the Internet.

Connection Hardware

The other item of hardware you must consider when setting up an Internet client is the connection hardware. Connection hardware is the device(s) you use to connect your computer to your ISP. If you are connecting to the Internet via a regular phone line, you’ll need a modem. As discussed in Chapter 1, a modem is a device that converts the digital signals (electrical impulses) from your computer into analog signals (tones) that can be transmitted over the telephone. When these signals reach the other end, the receiving modem converts the analog signals back to digital signals so the computer can understand what’s being transmitted. Most computers you buy today come with a modem and Internet connection software already installed.

If you are connecting your computer to a LAN that is already connected to the Internet, you must install a device known as a network interface card (NIC) in order to get your PC on the Internet. As discussed in Chapter 1, the NIC converts the signals from your computer into a format the network can understand. The network administrator has already installed the hardware (i.e., routers, CSU/DSUs, and
so on) that are required to connect the LAN to the Internet, so the NIC just connects your PC to the LAN and, thus, to the Internet.

**Operating System (OS)**

In addition to having a computer of some sort, you must have an operating system installed on your computer so the computer knows how to run applications and do “useful” things (like browsing the Internet). An operating system controls and manages all the functions of the computer on which it is installed. Additionally, it provides the interface between the user and the computer and its applications.

For the i-Net+ exam, you must know that the computer you are using to connect to the Internet must have an operating system installed on it (you can’t use the computer without an OS). Furthermore, you must understand that for any Internet clients you install, your computer must be running the required OS version or the client won’t install properly (or at all). For example, if you are installing a Web browser and the OS requirements say, “For Windows 95/98,” that means this client only runs on the Windows 95 or Windows 98 operating system. If you try to install it on a Macintosh, it won’t work (it actually won’t even install).

**TCP/IP Protocol Stack**

Another requirement that all Internet clients have in common is that the TCP/IP protocol must be installed and running. The TCP/IP protocol stack is one of several protocol stacks. A protocol stack is a collection, or suite, of protocols that work together. As discussed in Chapter 3, the Internet is based on the Transmission Control Protocol/Internet Protocol (TCP/IP) suite of protocols. If the TCP/IP protocol is not installed and configured correctly, the Internet clients will be unable to send data to and receive data from the Internet. Thankfully, most operating systems (including Windows 95, 98, and NT and the MacOS) include TCP/IP support.

Note The software that provides TCP/IP support for Windows applications is known as WINSOCK.DLL. You may hear about commercial TCP/IP software that requires "Winsock compliance." This just means that the software will use the Winsock DLL to connect to the Internet. Most (if not all) Windows Internet clients are Winsock clients.

**Internet Connection**

This requirement for an Internet client almost goes without saying. If you’re going to use an Internet client, you must have a connection to the Internet. There is one exception, however. If you have your own intranet and you’re going to use your Internet clients as clients for your intranet, then you don’t need an Internet connection. Many companies that do this also have an Internet connection because it is a valuable tool to offer employees.

The type of Internet connection you should have varies depending on your Internet needs. If you are in charge of connecting your company to the Internet and you have hundreds of computers that need access, you may want a leased-line connection of some kind between your network and your ISP. If you are setting up your computer to connect to the Internet from home, it may only be feasible to have a slower-speed (and thus, cheaper) connection to the Internet like a Plain Old Telephone Service (POTS) dial-up, Integrated Services Digital Network (ISDN), or Digital Subscriber Line (xDSL) connection.

Note Chapter 1 details the different types of Internet connections and their merits.
Types of Internet Clients

Just as there are many types of Internet content servers, there are many different types of Internet clients. For the most part, each client allows access to a different type of server. In this section, you’ll learn about the different types of Internet clients and what they are used for, and we’ll give you at least one example of each type of client.

Web Browser

When most people think of the Internet, they think of a graphical environment with lots of pictures, audio, and text. It wouldn’t be possible to display this content from Web servers without the Web client (more commonly called a Web browser). A Web browser is an application that you use to submit requests for Internet content (i.e., Web pages, graphics, and so on) to a Web server using the Hypertext Transfer Protocol (HTTP). The Web browser also displays the responses to those requests on the screen.

Before we give you some examples of Web browsers, we’ll discuss some of the components Web browsers have in common.

Web Browser Components

Although there are a few different Web browsers available, they all share a similar “look.” Because Web browsers today are based, in some way, on the work done by the National Center for Supercomputing Applications (NCSA), they all have at least a few items in common (as shown in Figure 5.1):

Browser window This is the main part of the Web browser, where the text and graphics of a Web page are displayed.

Location bar The location bar is the component that displays the location of the Web page currently showing in the browser window. If you type the address of a Web site into this area and press Enter, the Web browser locates the Web site and displays its home page.

Menu bar As its name implies, this is the part of the browser that contains the menus. Click a word and a menu appears with choices that control the way you use the Web browser.

Button bar This bar contains buttons that help you navigate within the WWW. The buttons are normally user-friendly and usually perform the operation indicated by their label (for example, the Back button takes you back to the page that was displayed before the current page).

Activity indicator In most Web browsers, this indicator will be animated when a user has made a request and is waiting for the requested Web page or Internet content to display.

Status bar At the bottom of the browser window, there is an area called the status bar (see Figure 5.1). It shows what’s happening during the request-response sequence of a Web browsing session. It will show whether the site has responded and the progress of the response to the original request (usually with an indication of the percentage downloaded).
Examples of Web Browsers

In the early days of the World Wide Web, there was only one Web browser, NCSA Mosaic. It was a very basic Web browser in that it could only display HTML text and GIF-formatted graphics. It was a free browser that you could download from the NCSA (although development rights were later sold to Spyglass). As the Internet grew, so did the number of browsers available. Every browser could display basic HTML and GIF graphics, but some could display the newer graphic format, JPEG (Joint Photographic Experts Group). Problems emerged when a Web site designed for one browser couldn’t be displayed in another. Out of this chaos, two clear leaders emerged: Netscape Navigator and Microsoft Internet Explorer, both in some way based on NCSA Mosaic.

Netscape Navigator

Netscape Navigator was the first browser (apart from NCSA Mosaic) to gain widespread commercial acceptance. Navigator is extremely similar in both appearance and function to Mosaic. This is because it was developed by some of the members who originally developed NCSA Mosaic, including Marc Andreessen. In 1994, Marc left NCSA and, together with James Clark (formerly of Silicon Graphics), started Netscape Communications Corporation. Their first major product was a “Mosaic-killer” called Netscape Navigator, nicknamed Mozilla (after the name of an animated dragon that appeared in the activity indicator).

One of the features that made Netscape Navigator more popular than Mosaic was its support for document streaming. That is, Netscape Navigator would display items as it would receive them rather than waiting until it received all the items on a page before displaying them (as Mosaic did).

Figure 5.2 shows an example of what Netscape Navigator looks like (actually part of Communicator version 4). Notice the large N in the upper-right corner of the browser window (the activity indicator). This indicator is one characteristic that can help you identify which browser you are using. Also, when you are sending and receiving data on the Internet, the N will be animated with stars moving in the background.

Currently, Netscape Navigator has been incorporated into a full Internet communications suite known as Netscape Communicator. Communicator includes the standard Navigator component as well as components for reading and composing e-mail, reading and composing Internet news, and a collaboration tool.
Microsoft was late to the “Internet game.” They were too busy working on their operating system and application platforms to worry about this “passing fad” called the Internet. But once they saw how popular the Netscape browser was, they had to have a piece of the market (actually, they wanted all of it). So, to quickly get their Internet market share, Microsoft now includes their Internet Explorer browser for free in all versions of their operating system, and it is difficult to remove (which was the source of the Microsoft/Department of Justice antitrust case). It is also available for free download from the Internet.

Microsoft had to put together a browser in a hurry. What they ultimately did was purchase the licensing rights to the majority of the original Mosaic code from Spyglass, then added a few tweaks and released it as Internet Explorer 1. While Netscape Navigator dominated the browser market, Microsoft was going to make up for lost time by releasing a modification to Windows 95 called the Windows 95 Plus Pack. This software package included a few neat utilities, some games, and the new browser, Internet Explorer (nicknamed IE). Additionally, Microsoft included IE in the OEM release of Windows 95 and NT for distribution to computer manufacturers.

Figure 5.3 shows the Microsoft Internet Explorer window (version 5). Again, the distinguishing feature of this browser is the activity indicator. Note that it is now a Windows icon rather than a big N.
FTP Program

As mentioned in earlier chapters, FTP utilities are used to upload and download files to and from FTP servers. Unlike Web browsers, there are many different types of FTP clients. Some clients use text commands on a command line to transfer files. Other FTP clients display directories and files in a graphical interface and use mouse-clicks and menu commands to perform the file transfer functions.

There are three main FTP utilities in use today:

- Unix FTP
- Windows 95/98 FTP
- Web browsers

In this section, you’ll get a general overview of the types of FTP clients in use today and how they look. In Chapter 6, you’ll learn how to use an FTP client to upload and download files.

Unix FTP

The first FTP utility that was ever used was the Unix FTP utility. It’s a pretty simple program. The user starts the program by typing FTP at a Unix command prompt. Once the program begins, a command line appears that usually looks something like this:

FTP>

At the command line, the user types commands to tell the FTP program which file to get, where to get it, and how to get it. Table 5.1 lists some of the popular commands you might use when you’re using the Unix command-line FTP utility to download or upload a file. How you use these commands to transfer
files is covered in “Using FTP to Download and Upload Files” in Chapter 6. Also, Figure 5.4 shows a command-line FTP utility in use.

Table 5.1: Unix FTP Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>open</td>
<td>open &lt;address&gt;</td>
<td>Opens an FTP session with an FTP server (for example, open ftp.sybex.com).</td>
</tr>
<tr>
<td>ls</td>
<td>ls</td>
<td>Used to list all the files and directories in the current directory (similar to the MS-DOS DIR command).</td>
</tr>
<tr>
<td>cd</td>
<td>cd &lt;dirname&gt;</td>
<td>Used to change the current directory. Used almost exactly like the MS-DOS CD command.</td>
</tr>
<tr>
<td>get</td>
<td>get &lt;filename&gt;</td>
<td>Specifies the name of the file on the remote host to download and then begins to download the specified file to the local computer.</td>
</tr>
<tr>
<td>mget</td>
<td>mget &lt;wildcards&gt;</td>
<td>Specifies multiple files (through the use of a filter) to download and starts downloading them one at a time.</td>
</tr>
<tr>
<td>put</td>
<td>put &lt;filename&gt;</td>
<td>Specifies the name of the file on the local computer to upload and then begins to upload the file to the remote computer.</td>
</tr>
<tr>
<td>mput</td>
<td>mput &lt;wildcards&gt;</td>
<td>Specifies multiple files (through the use of a filter) to upload to the remote computer and then starts to upload them one at a time.</td>
</tr>
<tr>
<td>binary</td>
<td>binary</td>
<td>Sets the transfer mode for files to binary. This must be set in order to transfer binary files (any file that is not composed of ASCII text) correctly.</td>
</tr>
<tr>
<td>ascii</td>
<td>ascii</td>
<td>Sets the transfer mode for files to ASCII text mode for transferring HTML and other ASCII text documents.</td>
</tr>
<tr>
<td>hash</td>
<td>hash</td>
<td>Toggles the printing of hash marks for each 8K downloaded.</td>
</tr>
<tr>
<td>prompt</td>
<td>prompt</td>
<td>Toggles prompting between each file upload or download using the mput or mget commands, respectively.</td>
</tr>
<tr>
<td>quit</td>
<td>quit</td>
<td>Ends the current FTP session and closes the FTP program.</td>
</tr>
</tbody>
</table>
Every release of Windows since (and including) Windows 95 has included a command-line FTP program that almost exactly duplicates the Unix FTP utility. The commands and their uses are the same. Additionally, the “look and feel” is almost identical (as shown in Figure 5.5).

You can start the Windows FTP utility one of two ways. You can run the Windows Command Prompt (Start → Programs → MS-DOS or Start → Programs → Command Prompt) and type FTP to start the FTP utility. You could also start it by choosing Start → Run, typing FTP, and clicking OK. Once it starts, it will work almost exactly the same as its Unix counterpart. The main difference is that, in the Windows version, local path names are shown in DOS format instead of Unix format.

Graphical FTP Utilities

Although FTP was historically a command-line utility, many companies have made graphical interfaces to make the process of transferring files to and from the Internet easier. Of the FTP utilities available for purchase or download, graphic FTP utilities are the most popular. Figure 5.6 shows an example of one such FTP utility, WS_FTP by Ipswitch Software. Rather than using complex command-line commands, graphical FTP utilities such as these represent both the local and host systems on the screen and use buttons and icons for some of the commands you can perform. For example, remember the binary FTP command that changed the transfer mode to binary. Notice in Figure 5.6 that the graphic utility has a radio button for that function.
A graphical FTP utility that you have used but may not know it is your Web browser. Most Web browsers (including Netscape Navigator and Microsoft Internet Explorer) support transferring files using the FTP protocol. If you access an FTP server with a Web browser (either by typing in an FTP URL or clicking a link that leads to an FTP server), the browser will display the files in a list and allow you to navigate the FTP server’s directory structure as well as download the file by clicking it. Figure 5.7 shows what Netscape Navigator looks like during a typical FTP transaction.

Terminal (Telnet) Client

Telnet clients allow you enter commands on a Unix server without actually sitting at that server’s console. A Telnet client takes the keystrokes from the client’s keyboard and sends them to the Telnet daemon running on the Unix computer. The Telnet daemon sends the screen displays back to the Telnet client. The Telnet client then displays the screen updates within the Telnet client window on the client computer.

The most popular Telnet client is the Windows 95/98/NT Telnet client, mainly because it comes free with all versions of Windows since (and including) Windows 95. Figure 5.8 shows what a sample Telnet session would look like using the Windows Telnet program. Notice that the first thing you must do when telnetting into a Unix server is log in. This is a function of the Unix server and not of the Telnet program because Unix requires you to log in before you do anything else. The Telnet program just
displays the login and lets you log in as though you were sitting at the console.

Figure 5.8: The Windows Telnet client

News Client

News clients (also called newsreaders) allow you to read and post Internet news messages from an Internet news server using the NNTP protocol. Using the news client, you can view a list of all the newsgroups that exist on a specified news server. If you like a particular newsgroup (alt.autos.studebaker, for example), you can configure your news client to show you all the headers (subject lines) of all the messages in that newsgroup. Then, if a particular message looks interesting, you can click that message to read it and, if you wish, to respond to it.

Figure 5.9 shows one example of a newsreader: Microsoft Outlook Newsreader (it comes free with Microsoft Internet Explorer or Microsoft Outlook). As you can see, this client’s screen is divided into four main areas. Across the top of the window are the menu and navigation bars. Below that, along the left side of the window, is the list of news servers and newsgroups you are subscribed to on those servers. To the right of that, in the top pane, is the list of headers of all the messages for the newsgroup that is selected in the left pane. If you click one of these headers, the client downloads the message to your machine and displays the contents of the message in the message display pane (the largest portion of this client, immediately to the right of the newsgroup list).

Figure 5.9: Microsoft Outlook Newsreader
Most news clients work in a similar fashion. They may not all look exactly the same, but there will be a list of news servers along with the list of newsgroups you subscribe to on each server, and there will be a window with a list of the headers of the messages for each newsgroup and a window where you can view the body of the message.

Note Some other examples of newsreaders include Netscape News and Free Agent. Again, like Microsoft Outlook Newsreader, they will function similarly.

E-Mail Client

Internet e-mail clients are those software programs used to send and receive e-mail and communicate with SMTP servers. E-mail clients send mail using the SMTP protocol. They also download e-mail from SMTP servers using the POP3 protocol. E-mail clients are the second most-popular Internet client software installed on computers today (as you might imagine, Web browsers are the most popular).

E-mail clients typically include a couple of standard features:

**Inbox** The Inbox is a location where all incoming mail resides. Typically, new mail in the Inbox has some kind of designation to differentiate it from mail that hasn’t been read. Some software packages use an unopened envelope icon next to the message to indicate a new message and an opened envelope to indicate a message that has been read.

**Outbox** The Outbox is a folder where all messages go as soon as you hit the Send button. The messages stay in this folder until they are sent to the server. This feature allows you to see what items are waiting to be sent. The main reason this feature exists is for people who send a lot of e-mail and may want to make a last-minute change after they click Send. However, once the message has been sent to the mail server, it disappears from this folder and can no longer be edited.

**Sent items** This feature is a folder that keeps a duplicate copy of all messages that have been sent. When you send a message, a copy gets sent to the SMTP server and another copy gets placed into this folder. The Sent items folder allows you to keep track of what you have sent and to whom.

**Address book** No e-mail program would be complete without an address book. This feature is a small database of the e-mail addresses of all the people you frequently send e-mail to. You can either type a person’s e-mail address in every time you send e-mail to him or simply select his name from the address book. The program will read the selected person’s e-mail address from the address book and put it in the To line of the new e-mail message, which is much more efficient.

There are two major examples of e-mail clients in use today: Microsoft Outlook and Netscape Messenger. A version of each is available with the associated manufacturer’s Web browser product (Internet Explorer and Navigator, respectively). In this section, we’ll briefly cover these two popular e-mail clients and explain what their interfaces look like. Configuration and use will follow in the next chapter.

Microsoft Outlook

Microsoft Outlook is one of the most popular e-mail clients for several reasons. First, it is included with the Microsoft Office 97 and Office 2000 office productivity suites, so it is readily available on many computers. Also, it is easy to use because many people are familiar with the Microsoft Office suite of products and it has a similar interface, so using it is second nature. Finally, it includes many other
features besides e-mail, including a powerful contact management feature and an integrated calendar and task list.

Figure 5.10 shows the screen of Outlook 98. There are a few things to note about this graphic. The bar on the left of the screen is known as the Outlook bar, and it contains icons for your Inbox (where mail is received and stored until you move it to another folder), your Contacts folder (basically, a very powerful address book), your Calendar, and other folders. To the right of that is the display of what ever folder happens to be selected in the Outlook bar (in this case, the Inbox). If you select a different folder on the left, a different window will display on the right. Above these two windows are the menu bar and button bar. Items on these two bars are used to perform the various functions in Outlook, like creating new mail, checking for new mail, replying to mail, and organizing mail, to name a few. We’ll cover how to use Outlook to send and receive mail in the next chapter.

![Figure 5.10: Microsoft Outlook window](image)

Netscape Messenger

Unlike Microsoft Outlook, Netscape Messenger (also called Netscape Mail in older versions of Netscape) is just a mail program, although the folks at Netscape may not like us for saying so. It does include a basic address book and the ability to read HTML embedded in the body of an e-mail message. Plus, it is available for free download along with Netscape Navigator.

Figure 5.11 shows what Netscape Messenger looks like. Notice that the layout of Netscape Messenger is somewhat similar to the layout of Outlook Newsreader. The list of messages (i.e., the Inbox) is at the top of the screen, and the selected message is viewed in a pane below that. Additionally, Netscape Messenger can display messages in HTML format. Apart from those items, Netscape Messenger is pretty similar to most other mail programs in functionality.
No discussion of e-mail products would be complete without a discussion of the most popular shareware, Eudora, made by QUALCOMM. There are actually two separate versions of Eudora, Eudora Pro and Eudora Light. The Eudora Pro product is a full-featured, powerful, commercial version that you can buy. Eudora Light is a stripped-down (although it still maintains many advanced features) version of Eudora Pro and is available for download for free from the QUALCOMM Web site (eudora.qualcomm.com).

As you can see in Figure 5.12, Eudora looks similar to the other Internet mail clients (especially Outlook). You can select a folder on the left and view its contents in the window on the right. Individual messages are listed, and you can view their contents by double-clicking them.

Summary

In this chapter, you learned about the infrastructure needed to support an Internet client. The items
needed to support an Internet client include not only hardware but software as well. There are five main items:

**Hardware platform** To get on the Internet, you need to use a hardware device of some kind. You can use either a PC or an Internet appliance. A PC is the most common choice, but more and more you’ll find people using Internet appliances (like the WebTV device) to surf the Internet. Internet appliances are inexpensive, but they can only perform certain Internet tasks (like browsing the Web and sending and receiving e-mail). If you use a PC, you may need additional hardware (for example, a modem or NIC) to support your connection to the Internet.

**Operating system** Every hardware platform must have an operating system. This isn’t so much an Internet requirement as simply a requirement of the hard ware. If you want to do anything on a computer or appliance, you must have an operating system installed. Windows 95/98 is the most common Internet client operating system.

**Network connection** This requirement means you must have a connection to the Internet in some form. Whether you use a modem in your PC or your entire network is connected to the Internet, you must have some kind of connection to an ISP to support your Internet clients.

**Web browser** A Web browser is the Internet client that creates HTTP requests and displays the Internet content it receives. It is the tool used to view all the content on the World Wide Web (WWW). The two most popular browsers in use today are Netscape Navigator and Microsoft Internet Explorer. They both are based on the Mosaic Web browser developed at the National Center for Supercomputing Applications (NCSA) at the University of Illinois at Urbana-Champaign, so they are similar in appearance and function. The main difference in their appearance is the activity indicator. IE has a Windows icon and Navigator has an animated N.

**E-mail** An e-mail client is an Internet client that can send and receive e-mail using the SMTP and POP3 (or IMAP) TCP/IP protocols, respectively. The two most popular Internet e-mail clients in use today are Netscape Messenger (also called Netscape Mail) and Microsoft Outlook.

### Review Questions

1. Which item is not required in order to use a Web browser to browse the Internet?
   - A. TCP/IP address
   - B. Internet connection
   - C. Some kind of hardware (PC or other) Internet device
   - D. FTP client

2. Which component of a Web browser indicates activity when animated?
   - A. Menu bar
   - B. Button bar
   - C. Activity indicator
3. Which Internet client(s) can be used to transfer files from an FTP server?
   A. FTP client
   B. Web browser
   C. Mail client
   D. Internet news client

4. Which Internet client(s) can be used to send, receive, and read SMTP mail?
   A. FTP client
   B. Web browser
   C. Mail client
   D. Internet news client

5. Which Internet client(s) can be used to read Internet news?
   A. FTP client
   B. Web browser
   C. Mail client
   D. Internet news client

6. Which FTP command is used to download a single file?
   A. get
   B. mget
   C. put
   D. mput

7. What should your FTP client be set to in order to successfully download an EXE file?
   A. ls
   B. binary
   C. exe
   D. ascii

8. Suppose you need to set up someone to use the Internet, but she doesn’t have a great deal of money to spend on a computer. What device could you install so she could still send and receive
9. What protocol must be installed in order for Internet clients to function?
   A. IPX/SPX
   B. NetBEUI
   C. TCP/IP
   D. HTTP

10. Which feature of an e-mail client allows you to keep track of the e-mail addresses of the people you commonly send e-mail to?
    A. Send and Receive
    B. Inbox
    C. Outbox
    D. Address book

11. Which network hardware device connects a computer to an ISP and the Internet via a standard phone line?
    A. PC
    B. Modem
    C. Internet appliance
    D. Processor

12. Which protocol(s) can the Microsoft Outlook e-mail client use to send and receive e-mail over the Internet?
    A. IPX/SPX
    B. POP3
    C. SMTP
    D. FTP

13. Which Internet client allows you to perform Unix commands on another computer just as if you were sitting at the console?
A. Web client
B. FTP client
C. Internet news client
D. Telnet client

14. Internet news clients run on which protocol?
   A. FTP
   B. HTTP
   C. NNTP
   D. POP3

15. Which Internet client(s) allows you to view Internet HTML and multimedia content?
   A. FTP client
   B. Web client
   C. Mail client
   D. News client

16. What is the name of Netscape’s Internet e-mail program?
   A. E-Mail
   B. Outlook
   C. Messenger
   D. Navigator

17. Internet Explorer is an example of what type of Internet client?
   A. Internet news client
   B. Internet e-mail
   C. FTP client
   D. Web browser

18. Microsoft Outlook is an example of what type of Internet client?
   A. Internet mail client
   B. FTP client
C. Telnet client
D. Web browser

19. Which component of a Web browser shows what, exactly, is happening during the request-response sequence of a Web browsing session?
   A. Status bar
   B. Button bar
   C. Menu bar
   D. Activity indicator

20. A(n) ________________ is the combination of hardware and software combined in one package that allows a user to interact with servers on the Internet without using a PC.
   A. Web browser
   B. Modem
   C. Internet appliance
   D. Operating system

Answers to Review Questions

1. D. Answers A, B, and C are all required before you can use a Web browser. You do not need an FTP client to browse the Web.

2. C. The activity indicator animates when the Web browser is either sending or receiving data.

3. A and B. Both an FTP client and a Web browser can be used to transfer files from an FTP server. Mail clients and news clients are used to view text messages from other users.

4. C. Of the clients listed, an Internet mail client is the only one that can be used to send and receive SMTP mail.

5. D. Of the clients listed, the Internet news client is the only one that can read Internet news.

6. A. Although mget can also be used to download files, it is used for multiple files, not for single files. The put and mput commands are used to upload files.

7. B. The ls command is used to list files, the ascii command sets the ASCII mode for text files only. The exe command isn’t a real command.

8. D. The Internet appliance is the best choice because it can be used to access the Internet but it doesn’t cost as much as a PC. A modem and a telephone won’t work without a PC, and a PC would be too expensive for this person.
9. C. All Internet clients require that the TCP/IP protocol be installed before they will function. The other protocols listed perform different functions, but generally speaking, they are not required by all Internet clients.

10. D. The address book allows you to keep track of people and their e-mail addresses. You can send e-mail to them by selecting their name rather than having to type in their e-mail address every time.

11. B. A modem connects a computer to the Internet via a standard phone line. An Internet appliance can connect to the Internet, but it won’t connect a computer to the Internet. A PC and a computer are the same thing, and a processor is part of a PC, so both A and D would be incorrect.

12. B and C. POP3 and SMTP are protocols used by Outlook to download and upload mail, respectively. IPX/SPX is a transport protocol used on LANs, and FTP is the file transfer protocol used to upload and download files from an FTP server.

13. D. Of the clients listed, the only one that allows you to perform Unix commands as if you were sitting at the console of the computer is a Telnet client.

14. C. The Network News Transfer Protocol is used to download Internet news from news servers. FTP, HTTP, and POP3 are protocols used for other Internet clients.

15. B. A Web client is the client primarily used to view HTML and Internet content, although it is possible for some mail and news clients.

16. C. Messenger is the Internet e-mail component of Netscape Communicator. Outlook is the only other e-mail program listed, and it’s Microsoft’s Internet e-mail program.

17. D. Internet Explorer is Microsoft’s Web browser product. Although it can transfer files with the FTP protocol, it is primarily a Web browser. It is not a news client, e-mail client, or FTP client.

18. A. Microsoft Outlook is used to send, receive, and read Internet e-mail. It cannot perform any functions of the other three clients listed.

19. A. The status bar at the bottom-left corner of the Web browser window shows exactly what is taking place during the session. Although the activity indicator does show activity, it doesn’t show exactly what is going on. The menu bar and the button bar don’t show any activity, but rather they allow the user to perform actions within the browser.

20. C. An Internet appliance is the device that’s a combination of hardware and software that allows a user to surf the Web without the need for a PC. A modem is only a piece of hardware, and a Web browser and an operating system are both software.

Chapter 6: Internet Client Configuration and Use

Overview
i-Net+ Exam Objectives Covered in This Chapter:

1. **Describe the use of Web browsers and various clients (e.g., FTP clients, Telnet clients, e-mail clients, all-in-one clients/universal clients) within a given context of use. Examples of context could include the following:**
   - When you would use each
   - The basic commands you would use (e.g., put and get) with each client (e.g., FTP, Telnet)

2. **Explain the issues to consider when configuring the desktop. Content could include the following:**
   - TCP/IP configuration (NetBIOS name server such as WINS, DNS, default gateway, subnet mask)
   - Host file configuration
   - DHCP versus static IP
   - Configuring browser (proxy configuration, client-side caching)

3. **Describe MIME types and their components. Content could include the following:**
   - Whether a client can understand various e-mail types (MIME, HTML, uuencode)
   - The need to define MIME file types for special download procedures such as unusual documents or graphic formats

4. **Describe the advantages and disadvantages of using a cookie and how to set cookies. Content could include the following:**
   - Setting a cookie without the knowledge of the user
   - Automatically accepting cookies versus query
   - Remembering everything the user has done
   - Security and privacy implications

In **Chapter 5**, you learned about the different types of clients that exist and the requirements for using them. In this chapter, you’ll learn how to configure and use each of these clients. The topics covered include both client PC and client software configuration as well as the steps you need to take to use the most popular Internet clients.

Now that you understand the basic look and features of each type of Internet client, you must learn how to configure and use them. Notice, however, that we will not be covering the installation of clients. If you are taking the i-Net+ exam, you should already know how to install software. Most software installations are similar (i.e., run SETUP.EXE, click Next a bunch of times, fill out the appropriate information when prompted, click Finish to finish the setup), so we won’t devote space to them here.

**Client Configuration**
When client software is installed, it doesn’t always work immediately. Most client software requires some kind of configuration before it will work correctly. In the following sections, you’ll learn the basic steps needed to configure at least one of each type of Internet client discussed in the preceding chapter. In addition, you’ll learn how to properly configure a client computer for use as an Internet client.

**Basic Client Computer Configuration**

Before configuring each Internet client software package, you must configure the computer running the software to support it. Although there are many client platforms, for the i-Net+ exam, you will only have to know how to configure Windows 95/98 clients, so we will cover only those in this section. Take note, however, that in the “real world,” it is to your advantage to know about the many different client platforms available (including Windows 95/98, Windows NT, Linux, MacOS, OS/2, and so on) and how to configure each to connect to the Internet.

There are several items you must configure on a client computer so that it can support Internet clients:

- TCP/IP addresses
- Name resolution
- Dial-up connection

The first two are configured using the properties of the TCP/IP protocol in the Network Control Panel. To start configuring any of these items, you first must ensure that TCP/IP has been installed on the client. You can double-check that it has been installed by following these steps:

1. Open the Network Control Panel (found in Start → Settings → Control Panel in Windows 95/98) and see if TCP/IP is listed (as shown in the following screen shot).

![Network Configuration Screen Shot](image)

2. If TCP/IP isn’t listed, click Add, and the Select Network Component Type dialog box appears.
3. Select Protocol from the list of components and click Add. Once you do, the Select Network Protocol window appears and you can pick the manufacturer and the appropriate protocol. For TCP/IP, select Microsoft from the list on the left and TCP/IP from the list on the right. Click OK to install the protocol.

Once the TCP/IP protocol is installed, you can proceed to configure its properties, starting with the TCP/IP addresses.

**TCP/IP Addresses**

In addition to requiring a TCP/IP stack, an Internet client computer must be configured with a few special TCP/IP addresses:

- Client TCP/IP address
- Subnet mask
- Default gateway

You can begin the configuration of these addresses by following these steps:

1. Choose Start → Settings → Control Panel and double-click the Network Control Panel.

2. To view the properties of TCP/IP from this window, select TCP/IP by clicking it, then click the Properties button. This will bring up the window shown in the following screen shot. Here, you can enter or change all TCP/IP-related properties contained on the various pages within this window. You will learn what all of these items mean, and how to configure them, in the sections that follow.
Client TCP/IP Address

The first address that needs to be configured is the address you must assign to the client PC so it can send and receive data on the Internet. This address is known as the client IP address. As discussed in Chapter 3, it is a 12-digit, dotted decimal number that uniquely identifies the client PC on the Internet. All clients that will send and receive data on the Internet must have a client IP address.

Client IP addresses are assigned from the IP Address tab of the TCP/IP protocol Properties window. You can assign them either manually or automatically. To assign an address manually, select the Specify an IP address radio button and type in the IP address you want to assign (as shown in Figure 6.1). You must ensure that the address you enter follows the IP addressing conventions (which were discussed in Chapter 3).

![Figure 6.1: Assigning an IP address manually](image)

To assign an IP address to a client PC automatically, select the Obtain an IP Address Automatically radio button on the IP Address tab of the TCP/IP Properties window and let the PC obtain its own IP address information from a Dynamic Host Configuration Protocol (DHCP) server. This is the default setting. If TCP/IP is installed on the client PC and this option is enabled, the client PC will query a DHCP server for its TCP/IP address. If you set up a DHCP server on your network, you can give all
your client computers (at least the ones with a TCP/IP stack that supports DHCP) IP address information automatically.

Note DHCP servers can assign to clients information other than TCP/IP addresses, such as subnet masks, default gateways, DNS information, and WINS server information.

The process by which a client PC requests its IP address begins when the client PC boots up. The TCP/IP stack has been configured to obtain its IP address automatically, so it sends out a broadcast on the local network segment, basically saying, “I need an IP address.” Any DHCP servers on the network segment will respond by saying, “I’ve got one for you.” The DHCP server will then assign an IP address (and any other pertinent information) to that client PC. This process is illustrated in Figure 6.2.

Figure 6.2: A DHCP server assigning an address

The decision on whether or not to statically address your computer or use DHCP is going to be based on the type of network you have. If you are using a connection to the Internet through an ISP, the majority of the time, you will be using DHCP to get an address. If you are unsure, check with your ISP or network administrator. Also, many ISPs automatically install and configure these network settings on a PC as part of the installation of their software (for example, if you use AT&T WorldNet to access the Internet, when you install the WorldNet CD, it automatically configures the network settings).

Note If you want to check your TCP/IP configuration, use the winipcfg program. To start this program, choose Start → Run, type in winipcfg, and click OK. The utility that appears will allow you to view your entire TCP/IP configuration.

Subnet Mask

If you selected Specify an IP Address and entered an IP address manually at the TCP/IP configuration screen, you must also enter the correct subnet mask (in the specified field) for the IP address you enter or the client won’t be able to communicate properly. However, if you selected Obtain an IP Address Automatically, the subnet mask will be specified by the DHCP server. For a detailed explanation of subnet masks, refer back to Chapter 3.

Default Gateway

The default gateway is the address of the router to which the client will send all TCP/IP traffic that is not addressed to a specific station on the local network. The default gateway address should be entered on any client PC that is attached to a network that is connected to the Internet via a router. The address of the default gateway is another piece of configuration information that can be distributed using a DHCP server.

Name Resolution
In addition to specifying the IP addresses for the client, you must specify how the client will resolve host names into IP addresses and vice versa. If you’ll remember from Chapter 2, host names are logical, alphanumeric names given to computers to identify them on a network without using cryptic sequences of numbers that a user would have to remember to access that host. Host names make accessing TCP/IP hosts more “friendly” because it is easier to remember www.sybex.com than it is to remember 10.45.89.129 (at least for most people).

There are three ways to configure name resolution on a client PC:

1. HOSTS file configuration
2. Domain Name Services (DNS)
3. Windows Internet Name Service (WINS)

DNS has been covered in previous chapters, but in this chapter, we will discuss where to find the other name resolution methods and how to configure them properly.

HOSTS File Configuration

The HOSTS file configuration is a name given to any file (usually named HOSTS.TXT or simply HOSTS, or something along those lines) that performs host name to IP address mapping. It must be manually edited by the user to add different hosts. For example, if you have a network with five PCs on it, each with its own name and HOSTS file configuration, and then you add a sixth PC, you would have to edit the HOSTS file on each PC and add the new host name of the new PC in order to refer to that new PC by its host name from any PC on the network.

This file exists in various locations on different PCs. On Windows PCs, it can generally be found in the Windows directory (usually C:\WINDOWS) or in the Windows NT directory in C:\WINNT\SYSTEM32\DRIVERS\ETC and is named HOSTS.SAM. Figure 6.3 shows a sample HOSTS.SAM file from a Windows 98 PC. This happens to be a hosts file from a PC on a home network. Notice that there are only two entries: 127.0.0.1 is mapped to the local PC (localhost), and the IP address 10.0.0.2 is mapped to the host name S1. This PC will translate the host name S1 back to the IP address 10.0.0.2.

Figure 6.3: A sample HOSTS.SAM file from a Windows 98 PC

# Copyright (c) 1998 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP stack for Windows95
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a `#'
# symbol
#
# For example:
#
# 102.54.94.97 rhino.acme.com # source server
# 38.25.63.10 x.acme.com # x client host

127.0.0.1 localhost
10.0.0.2 S1
What happens, though, when a second server, S2 (with an IP address of 10.0.0.3), is added to the network? You must edit this HOSTS file (and all the HOSTS files on client PCs on the network) to include the information for the new server. In our example, then, you must start up a text editor (for example, MS-DOS EDIT.COM or Windows Notepad) and open the HOSTS.SAM file. Then, at the end of the file, insert an entry with the IP address of the new server (10.0.0.3) followed by a tab or a few spaces and then the host name you want to assign to that IP address (in this case, S2). Save the file and reboot the computer. After the reboot, the computer will be able to access server S2 by name. Figure 6.4 shows the edited HOSTS.SAM file with the new entry. Notice that the new entry follows the pattern of the other entries.

Figure 6.4: Updated HOSTS.SAM file

Domain Name Services (DNS)

The functions of Domain Name Services (DNS) were discussed in earlier chapters, but in this chapter, you’ll learn how to configure a client PC to make DNS requests. If you are using DNS (and not HOSTS files) to resolve host names to IP addresses and vice versa, you must tell your client PC’s TCP/IP stack the IP address of a DNS server to use to resolve these names.

To start configuring DNS on a Windows 95/98 PC, use the following steps:

1. Open the Network Control Panel (as discussed earlier).
2. Open the TCP/IP Properties window (as discussed earlier).
3. Click the DNS Configuration tab. From this screen, you can configure the IP address of the DNS server(s) that your client PC should use to resolve DNS names to IP addresses.
4. To configure DNS resolution on this Windows 95/98 client PC, you must first enable DNS resolution by clicking the radio button labeled Enable DNS.

5. Once you click the Enable DNS radio button, the bottom half of the property page will brighten and allow you to enter values for DNS configuration. There are four areas that you can configure on this tab:

   **Host** This field allows you to set the actual host name of the Windows 95/98 PC. The default name for this field is the actual name of the PC. This name is usually specified during the installation of Windows. Windows will, by default, make the name of your computer, as seen in the identification tab of the Network Control Panel applet, the same as your host name. It is recommended you keep these the same.

   **Domain** In this field, enter the Internet DNS domain name that represents this entire network.

   **DNS Server Search Order** This field is the most important field on this tab. This is where you specify the IP addresses of the DNS server(s) for the domain specified in the Domain field. More than one server IP address can be specified. If more than one IP address is specified, the client will query the DNS servers in order (from top to bottom).

   **Domain Suffix Search Order** If you type a host name in a Web browser and leave out the
somewhere.com domain name, the entries in this field will be appended to the host name and the client will try to make DNS queries with the new name. For example, suppose you type just “snoopy” in the address line of a Web browser; that isn’t a DNS domain name, so the Windows TCP/IP stack will try to resolve the name by appending whatever domain names are in this list. If somewhere.com is in this list, the TCP/IP stack will append somewhere.com to snoopy and try to resolve snoopy.somewhere.com into an IP address.

6. At a minimum, to configure DNS on a Windows 95/98 client, you must enter a host name, a domain name, and at least one DNS server IP address. Simply type in the values in the appropriate fields. For the DNS server IP address, you must first type the IP address of the DNS server in the appropriate field, then click the Add button.

7. Once you have entered the appropriate values, you can click OK to close the TCP/IP Properties window and then click OK to close the Network Control Panel. Windows will ask you to reboot the client PC. Once rebooted, the client PC will be able to access hosts by DNS name as well as by TCP/IP addresses.

Note The i-Net+ exam doesn’t cover the details of setting up a DNS server, and thus it is outside the scope of this book. For an excellent reference on DNS servers and their setup, check out DNS and BIND from O’Reilly & Associates.

Windows Internet Name Service (WINS)

The Windows Internet Name Service is a name resolution service commonly found on Windows NT networks that are using TCP/IP. WINS is used in conjunction with TCP/IP and maps NetBIOS names to IP addresses. For example, suppose you have a print server on your LAN that you have come to know as PrintServer1. In the past, to print to that server, you needed only to remember its name and to select that name from a list. However, TCP/IP is a completely different protocol and doesn’t understand NetBIOS names; therefore, it has no way of knowing the location of that server or its address. That’s where WINS comes in.

Each time you access a network resource on a Windows NT network using TCP/IP, your system needs to know the host name or IP address. If WINS is installed, you can continue using the NetBIOS names that you have previously used to access the resources because WINS provides the cross-reference from name to address for you.
Configuring WINS name resolution is also done through the TCP/IP Properties window. There is a tab, WINS Configuration, on the TCP/IP Properties window that allows you to configure the addresses of WINS servers (shown in Figure 6.5). These addresses are stored with the configuration, and TCP/IP uses them to query for Net BIOS host names and addresses when necessary. WINS is similar to DNS in that it cross-references host names to addresses; however, as we mentioned earlier, WINS references NetBIOS names to IP addresses, and DNS references TCP/IP host names to IP address. To view the NetBIOS name of your Microsoft computer, go to the identification tab of the Network Control Panel.

Another major difference between WINS and DNS is that WINS builds its own reference tables dynamically and you have to configure DNS manually. When a workstation running TCP/IP is booted and attached to the network, it uses the WINS address settings in the TCP/IP configuration to communicate with the WINS server. The workstation gives the WINS server various pieces of information about itself, such as the NetBIOS host name, the actual username logged on to the workstation, and the workstation’s IP address. WINS stores this information for use on the network and periodically refreshes it to maintain accuracy.

Microsoft, however, has developed a new DNS record that allows the DNS server to work in perfect harmony with a WINS server. The Microsoft DNS Server software currently ships with Windows NT. Here’s how it works. When a DNS query returns a WINS record, the DNS server then asks the WINS server for the host name address. Thus, you need not build complex DNS tables to establish and configure name resolution on your server; Microsoft DNS relies entirely on WINS to tell it the addresses it needs to resolve. And because WINS builds its tables automatically, you don’t have to edit the DNS tables when addresses change; WINS takes care of this for you.

You can use both WINS and DNS on your network, or you can use one without the other. Your choice is determined by whether your network is connected to the Internet and whether your host addresses are dynamically assigned. When you are connected to the Internet, you must use DNS to resolve host names and addresses because TCP/IP depends on DNS service for address resolution.

WINS is disabled by default (as shown previously in Figure 6.5). To configure WINS, follow these steps:

1. First select one of the radio buttons shown, either Enable WINS Resolution or Use DHCP for
WINS Resolution. If you select Use DHCP for WINS Resolution, the client PC will get its WINS server information from a DHCP server, along with its IP address information.

2. If you select Enable WINS Resolution as shown in the following screen shot, you can manually specify which WINS server(s) to use for NetBIOS host name to TCP/IP address resolution.

3. When you choose Enable WINS Resolution, configuration is much the same as it is with DNS configuration. Simply enter the IP addresses of the WINS servers, one at a time, and click Add to add them to the list of WINS servers.

4. When you’re finished entering the IP addresses, click OK to close the TCP/IP Properties window. Then click OK to save the changes and close the Network Control Panel. Windows will ask you to reboot.

5. After the reboot, the client PC will be able to perform WINS resolution.

Note We didn’t discuss the Scope ID field in this book because it is not often used. However, for your information, it is used to “group” NetBIOS entities together. All entities on a network with the same Scope ID value can send NetBIOS data (e.g., share lists and domain information) to one another. If you enter a scope ID of 12, this station can only communicate with other NetBIOS entities that have their scope ID set to 12. Most often, this field is left blank so that all computers can communicate with all other NetBIOS entities without restriction.

Configuring a Dial-Up Connection

The most popular way to connect a client PC to the Internet is with a standard phone line and a modem (what is known as a dial-up Internet connection). Because a dial-up Internet connection is the most popular way of connecting clients to the Internet, the i-Net+ exam will test your knowledge of configuring a computer to make this type of connection.

To connect your Windows 95/98 computer to the Internet over a regular modem connection, you must have a few items in place, including:

- A modem
Windows Dial-Up Networking (DUN) software

A valid access account with an ISP

A configured Dial-Up Networking connection

In the following sections, we’ll cover each item in more detail. Once you get your client connected, you can install a Web browser or another client and communicate with the Internet.

**Modem**

In order to have a dial-up connection, you must have one critical piece of hardware installed on your computer: a modem. As mentioned in Chapter 1, a modem converts the digital signals that your computer uses into analog signals that can be sent over telephone lines. Dial-up connections can use either an internal or external modem.

When installing a modem into a Windows 95/98 machine, you must have the correct Windows 95/98 driver for the modem. A modem driver is the software component that manages and controls the modem. Without the correct driver installed, the dial-up connection software would not be able to communicate with the modem and thus would not be able to dial up to the ISP.

Drivers include several embedded strings of characters called **modem initialization commands**, which are the commands sent to the modem by the communications program to “initialize” it. These commands tell the modem things like how many rings to wait before answering, how long to wait between detecting the last keystroke and disconnecting, and the speed at which to communicate.

For a while, each manufacturer had its own set of commands, and every communications program had to have settings for every particular kind of modem available. In particular, every program had commands for the Hayes line of modems (mainly because Hayes made good modems and their command language was fairly easy to program). Eventually, other modem manufacturers began using the “Hayes-compatible” command set. This set of modem-initialization commands became known as the Hayes command set. It is also known as the “AT command set” because each Hayes modem command started with the letters **AT** (presumably calling the modem to **AT**ention).

Each AT command does something different. The letters **AT** by themselves (when issued as a command) will ask the modem if it’s ready to receive commands. If it returns “ok,” that means that the modem is ready to communicate. If you receive “error,” it means there is an internal modem problem that may need to be resolved before communication can take place.

**Table 6.1** details some of the most common modem commands. Notice that we’ve included a couple of extra commands that aren’t AT commands. These items are characters used to affect how the phone number is dialed (including pauses and turning off call-waiting).

**Table 6.1: Common Modem Initialization Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>AT</td>
<td>Tells the modem that what follows the letters AT is a command that should be interpreted</td>
<td>Used to precede most commands.</td>
</tr>
</tbody>
</table>
If you are going to connect your computer to the Internet via a modem and telephone line, aside from configuring the various aspects of the TCP/IP protocol, you will have to configure a Dial-Up Networking connection on Windows 95. The Windows Dial-up Networking software is used to connect Windows 95/98 to various networked systems and is included as part of Windows 95/98. It is not installed by default unless you have a modem installed in the computer when Windows 95/98 is being installed. It is also installed whenever you install a modem in the computer. Bottom line: you cannot connect your Windows 95/98 PC to an ISP (and thus, to the Internet) unless the Windows 95/98 Dial-Up Networking software is installed.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATDT nnnnnnn</td>
<td>Dials the number nnnnnnn as a tone-dialed number</td>
<td>Used to dial the number of another modem if the phone line is set up for tone dialing.</td>
</tr>
<tr>
<td>ATDP nnnnnnn</td>
<td>Dials the number nnnnnnn as a pulse-dialed number</td>
<td>Used to dial the number of another modem if the phone line is set up for rotary dialing.</td>
</tr>
<tr>
<td>ATA</td>
<td>Answers an incoming call manually</td>
<td>Places the line off-hook and starts to negotiate communication with the modem on the other end.</td>
</tr>
<tr>
<td>ATH0 (or +++ and then ATH0)</td>
<td>Tells the modem to hang up immediately</td>
<td>Places the line on-hook and stops communication. (Note: The 0 in this command is a zero.)</td>
</tr>
<tr>
<td>AT&amp;F</td>
<td>Resets modem to factory default settings</td>
<td>This command works as the initialization string when others don’t. If you have problems with modems hanging up in the middle of a session or failing to establish connections, use this string by itself to initialize the modem.</td>
</tr>
<tr>
<td>ATZ</td>
<td>Resets modem to power-up defaults</td>
<td>Almost as good as AT&amp;F, but may not work if power-up defaults have been changed with S-registers.</td>
</tr>
<tr>
<td>ATS0-n</td>
<td>Waits n rings before answering a call</td>
<td>Sets the default number of rings that the modem will detect before taking the modem off-hook and negotiating a connection. (Note: The 0 in this command is a zero.)</td>
</tr>
<tr>
<td>ATS6-n</td>
<td>Waits n seconds for a dial tone before dialing</td>
<td>If the phone line is slow to give a dial tone, you may have to set this register to a number higher than 2.</td>
</tr>
<tr>
<td>comma (,)</td>
<td>Pauses briefly</td>
<td>When placed in a string of AT commands, the comma will cause a pause to occur. Used to separate the number for an outside line (many businesses use 9 to connect to an outside line) and the real phone number (e.g., 9, 555-1234).</td>
</tr>
<tr>
<td>*70 or 1170</td>
<td>Turns off call-waiting</td>
<td>The “click” you hear when you have call-waiting (a feature offered by the phone company) will interrupt modem communication and cause the connection to be lost. To disable call-waiting for a modem call, place these commands in the dialing string like so: *70, 555-1234. Call-waiting will resume after the call is terminated.</td>
</tr>
</tbody>
</table>
ISP Account

In addition to the software and hardware components involved in a dial-up connection, you must have a valid access account with an ISP. An ISP account includes a username and password you can use to gain access to the ISP’s servers and to the Internet. ISPs charge a small fee (typically anywhere from $10-$30 per month) for access to the Internet through a modem connection.

When you do get an ISP account, they will give you a “configuration sheet” that contains all the information you will need to configure your Dial-Up Networking connection. Some ISPs have a preconfigured software installation disk with all this information already entered. In that case, all you need to do is install the software and your client PC will be configured. If your ISP doesn’t have a sheet or a disk like this, you can make a “cheat sheet” by asking them a few questions and writing down the answers:

- What is the dial-up phone number?
- What is my username and password?
- What are the DNS names of your e-mail servers (outgoing and incoming)?
- What are the IP addresses or DNS names?
- What is the DNS name of your news server?

The answers to these questions will be needed in the next section, where you need to create a Dial-Up Networking connection (the last three will be used in sections that follow, where you configure the other clients, including Web browsers).

Dial-Up Networking Connection

The final component of a dial-up connection is a Dial-Up Networking connection script. This script is an icon that represents a collection of preconfigured settings for dialing up to a specific ISP. This Dial-Up Networking script is a function of Windows 95/98 Dial-Up Networking and includes settings like ISP phone number, ISP TCP/IP settings, username and password, and connection name.

To create a Dial-Up Networking connection on a Windows 95/98 client, follow these steps:

1. First ensure that all the previously listed items are in place (i.e., modem, dial-up networking software, and an ISP account).

2. To start the process, have your information sheet from your ISP (or your “cheat sheet”) handy and open the Dial-Up Networking folder. You can access this folder either by opening My Computer or by choosing Start ➤ Programs ➤ Accessories ➤ Dial-Up Networking in Windows 95 (Start ➤ Programs ➤ Accessories ➤ Communications ➤ Dial-Up Networking in Windows 98). This folder normally lists any Dial-Up Networking connections you have already configured, but you haven’t configured one yet, so it should be blank.
3. Once you have this window open, you can start to configure a new connection by double-clicking the Make New Connection icon.

4. In the first screen (the following screen shot is from Windows 98), there are two fields. The first asks you to give a name to this connection (the default is My Connection). You should type in the name of your ISP or some name that indicates to you that this is a Dial-Up Networking connection to your ISP. In this sample case, we’ll use TestISP. The second field asks you which modem this connection should use. This field has a drop-down list that includes more than one modem (if more than one modem is installed). The default for this field is the first modem that’s installed. In this case, the only modem that’s installed is a 56K U.S. Robotics and it’s already selected, so you don’t have to do anything with this field unless you have another modem installed and you want to use that modem. Once you have finished entering the connection name and selecting a modem, click the Next button.

Tip You can click the Cancel button at any point during this process to cancel the configuration of this connection.

Note The Configure button displayed in the first screen allows you to configure the modem settings, like modem speaker volume, modem connection speed, and manual dialing capabilities. Most often, the defaults for the modem only need to be changed with the more troublesome connections. You will also have a chance to configure these options later after
5. The next screen is where you’ll enter the phone number of the ISP’s modem bank. The Area Code field should default to your area code (you should have entered it when you installed the modem). If not, you can change it on this screen. In the Telephone Number field, you should enter the telephone number given to you by the ISP for the ISP’s modem bank. You can also choose the dialing prefix for long distance numbers by selecting your country from the drop-down list labeled Country or Region Code. But you shouldn’t have to select anything because hopefully your ISP is a local phone call!