

Please read these important Navigation Notes

About the Online Instructor's Manual: The Online Instructor's Manual is an electronically enhanced version of the printed Instructor's Manual. Using Adobe Acrobat Reader, you can easily browse the Online Instructor's Manual to find material that will help you prepare for class at a moment's notice. A predefined list of bookmarks allows you to quickly link to chapter overviews, chapter outlines, technical notes, lecture notes, additional assignments, solutions, and more.

Navigating the Online Instructor's Manual: The easiest way to navigate through the pages of the Online Instructor's Manual is by using the bookmark list prepared by Course Technology. To use the bookmark list:

1. First, take a moment to expand the overview area so that the bookmark list is fully visible. To do so, drag the **Window Splitter** control (see Fig. 1) to the right. This setting will be retained until you close the document.

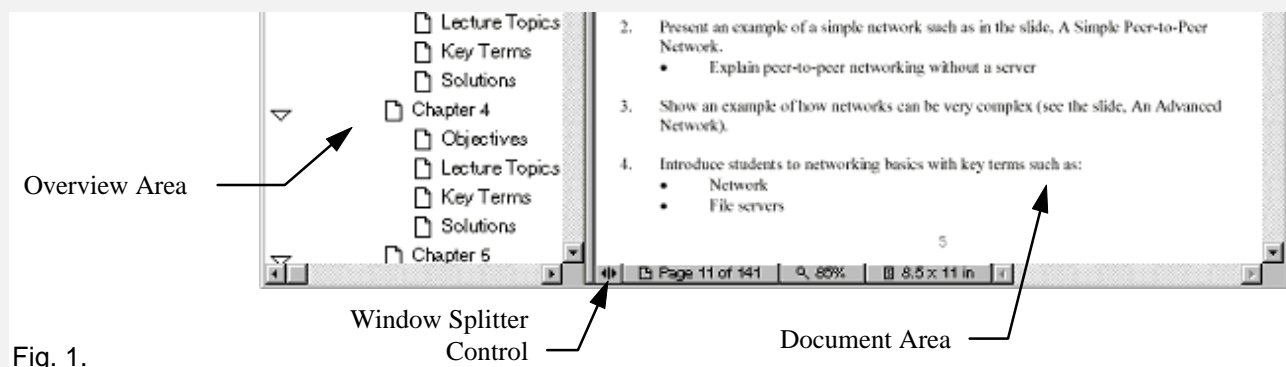


Fig. 1.

2. Use the scrollbar to the right of the Overview Area to view the bookmarks for each chapter. Click on a bookmark to go to the topic indicated.
3. To expand the document page to the full width of the Acrobat Reader for easier reading, click on the **Page Only** button on the toolbar (see Fig. 2).
4. To return to the bookmark list from Page Only view, click the **Bookmarks and Page** button on the toolbar (see Fig. 2).



Fig. 2.

5. If you would like to return to your previous location in the document, use the **Go Back** button on the toolbar (see Fig. 2). The **Go Forward** button will return you from this previous location.

COURSE TECHNOLOGY

Printing the Online Instructor's Manual: You have the option of printing out either the entire Online Instructor's Manual or just the pages you find particularly useful. To print pages from the Online Instructor's Manual:

1. Choose **Print** from the File menu.
2. Choose the range of pages you would like to print, if necessary.
3. Click **OK** or follow the steps as you normally would to print a document

Enhancing the Online Instructor's Manual: The Instructor's Notes in the Online Instructor's Manuals merely offer *suggestions* for teaching the material covered in the texts. You will undoubtedly have your own style of teaching. The Faculty Online Companion for your text can be found by following the Teaching Resources link on the Course Technology Homepage (<http://www.course.com/>).

You also have the option of bringing text from the online manuals into your own documents for editing. To copy text from the Online Instructor's Manual into another document:

1. Click the **Text Selection** tool on the toolbar (see Fig. 3). Your pointer will become an I-bar.
2. Click and drag the pointer to highlight the text that you would like to copy.
3. Choose **Copy** from the Edit menu to copy the selected text to the clipboard.



Fig.3. Text Selection Tool

4. Open a document in another application, such as Microsoft Word.
5. Choose **Paste** from the Edit menu of that application to insert the text from the Online Instructor's Manual.

Instructor's Manual to Accompany

A Guide to Networking Essentials



Instructor's Materials prepared by

David Johnson
LANWrights

Instructor's Manual to accompany *A Guide to Networking Essentials* is published by Course Technology.

*Associate Product Manager
Manufacturing*

Cover Designer

Lisa Ayers
Sean Marr
Elizabeth Martinez
Susannah Lean

©1998 Course Technology

All rights reserved. This publication is protected by federal copyright law. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, or be used to make any derivative work (such as translation or adaptation), without prior permission in writing from Course Technology

Trademarks

Course Technology and the open book logo are registered trademarks of Course Technology.

Some of the product names used in this book have been used for identification purposes only and may be trademarks or registered trademarks of their respective manufacturers and sellers.

Disclaimer

Course Technology reserves the right to revise this publication and make changes from time to time in its content without notice.

ISBN 0-7600-5869-5

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

Introduction

This manual is intended to prepare the instructor to teach the Networking Essentials class. The class is geared toward providing the students the knowledge necessary to pass the Microsoft certification test Networking Essentials, Exam # 70-058.

Content Outline

Each of the chapters in this manual contain the following sections:

Objectives – Outlines what will be covered in the chapter

Teaching Tips – Provides the instructor information on the contents of the Guide to Networking Essentials as well as tips and examples related to the text.

Additional Case Projects – Provides the instructor additional projects which can be assigned to students to enhance their knowledge of the material in the chapter.

Solutions – Includes answers to the Review Questions and discussion of the Hands-on Projects and Case Projects at the end of each chapter.

Table of Contents

Chapter 1: Introduction to Networks and Networking Concepts	3
Chapter 2: Network Design Essentials	12
Chapter 3: Networking Media.....	21
Chapter 4: Network Interface Cards	32
Chapter 5: Making Networks Work.....	40
Chapter 6: Network Communications and Protocols	47
Chapter 7: Network Architectures.....	56
Chapter 8: Simple Network Operations.....	66
Chapter 9: Understanding Complex Networks	75
Chapter 10: Network Administration and Support	81
Chapter 11: Enterprise and Distributed Networks	91
Chapter 12: Wide Area and Large-Scale Networks	99
Chapter 13: Solving Network Problems	107
Chapter 14: The Internet: A World-Wide Resource.....	116

Chapter 1: Introduction to Networks and Networking Concepts

Objectives

After reading the chapter and completing the exercises, the students should be able to:

- Understand basic networked communications
- Identify essential network components
- Describe the benefits of networking
- Understand peer-to-peer and server-based networks and their differences
- Apply their knowledge when selecting an appropriate network type for small business use
- Suggest possible redesigns for a small, but expanding network

Teaching Tips

What Is Networking?

Networking Fundamentals

- 1 Describe the very basic concept that any two connected computers comprise a network. This connection provides the basis for networked communications. Most network communication, in fact, consist of conversations between two computers.
- 2 Discuss the primary reason for implementing a network: sharing resources. Whether sharing data or sharing printers, networks are created to share resources.
- 3 Remind the students that, when it comes to sharing data, no standalone computer is as powerful or convenient as a group of networked computers.

Local and Wide Area Networks

- 1 Define Local Area Network and how it fits into today's networks. LAN defines a small, localized network. As the network grows and more computers are added, the LAN forms the basis for an internetwork.
- 2 Describe how a number of LANs in multiple locations can be connected to form a WAN. These types of networks are generally created when LANs in different cities or countries are connected to each other.
- 3 Mention the less-often referred-to Metropolitan Area Network (MAN) and Campus Area Network. These

network types are often implemented as a middle state between a LAN and a WAN. MANs use WAN technologies to connect LANs within a fairly small geographic region, such as a city. Campus Area Networks sometimes use these same technologies or longer-distance LAN technologies to connect multiple buildings in a campus.

- 4 Demonstrate how the Internet is, in fact, an intricate WAN connecting thousands of LANs.

A Networking Lexicon

- 1 Mention that, because computer networking is a very specialized field, there are many terms which have been created or adapted for use in networking terminology. It is imperative that the students understand these terms to fully understand networking.

Clients, Peers, and Servers

- 1 Define the client/server relationship: Clients make requests from a server, the server then fulfills (services) those requests. This type of request/response is standard throughout both client/server networks and peer-to-peer networks.
- 2 Describe the peer-to-peer network environment: Each computer acts as both a client and a server, depending on the requests being made. When a request is made for a local resource, the computer is acting as a server. When the computer requests data from another computer, it is acting as a client. These are called peer-to-peer (or just peer) networks because all computers share and request resources from each other.

The Network Medium Carries Network Messages

- 1 Describe the term network medium. This generally refers to the physical cable connecting the computers. However, in some networks (infra-red or radio, for example), air is the network medium.
- 2 Describe the role of the medium in networking. Its sole purpose is to carry messages from one computer to another.
- 3 Describe the role of the network interface card (NIC)/network adapter. This adapter provides the connection from the computer to the medium.
- 4 Describe how the medium can affect the number of computers, speed, and layout (topology) of the network.

Network Protocols

- 1 Define the term protocol in regard to networking. Just as when two dignitaries meet at the UN, certain rules apply to communication. These rules, or protocols, define how the computers are identified, how they place data on the medium, and how they initiate and manage communications sessions.

- 2 Describe how protocols are used in networking. For two computers to communicate, they must use the same rules. Say, for example, that two ambassadors met at the UN, one who speaks French, and one who speaks Russian. If they do not share a common language, communication is impossible without a translator. The same applies to computers on a network. They must use the same “language” to communicate.

Network Software

- 1 Demonstrate that, even though two computers may be using a common medium and protocol, they must have networking software to communicate with each other. The client networking software decides whether network access is needed. The server networking software controls who has access to the information on the server and handles sharing resources.
- 2 The most prominent NOSs today are Microsoft’s Windows NT and Novell’s NetWare (IntranetWare).
- 3 Mention the layered approach to networking. For example, the client NOS instructs the protocol to access the medium through the NIC to exchange information with another computer. Each layer depends on the layers below and above to supply particular pieces in the network communication model.

Network Types

Peer-to-Peer Networking

- 1 Tie this section into the previous description of peer computers. In these networks, not only does each computer act as both a client and a server, but each user administers their own machine. Resource sharing is handled by the individual users.
- 2 Be sure to mention the implications of this model:
 - As a network grows larger, it becomes more difficult to manage.
 - Each resource can have a different password.
 - There is no way to control who has access to a resource, just what the password is. If a person who does not need access to a particular resource learns the password to that resource, they have access.
 - Data organization is exceptionally difficult. If each computer can act as a server, how many copies of a document can exist? Which copy is the most current?
- 3 Describe the best time and place to use peer-to-peer networks. Generally, these are small companies or working groups in which every person is fairly computer savvy and security is not essential.

- 4 Mention that peer-to-peer networks are the cheapest and easiest to install. They generally only require the operating system on the computers to cooperate. A perfect example is the Windows family of operating systems. Windows for Workgroups, Windows 95, and Windows NT Workstation can all support peer-to-peer networks.

Server-Based Networks

- 1 Again, tie this information to the earlier section. The server's sole purpose is to respond to client requests. This type of network represents the vast majority of networks installed today.
- 2 Describe the key differences between peer networks and server-based networks: centralized management and higher levels of security.
- 3 Describe the password structure in a server-based network: Each user is assigned a username and password which grants them access to the server and controls what resources the user can use. This implements a much higher level of security than peer-to-peer networks, where any user with the correct password can access the resource.
- 4 Describe the Windows NT domain model and how it is used in server-based networks. Before the user is granted access to the network, their username and password must be validated by a domain controller. The domain controllers restrict access to any computers within the domain. By doing this, users can logon only once and access any number of services.
- 5 Mention that server-based networks gracefully increase in size. When more users are supported, more servers are added and the network grows. This is opposed to peer-to-peer networks where management becomes a problem after around 20 users.

Hybrid Networks

- 1 Describe how hybrid networks combine the best of both peer-to-peer and server-based networks. Again, a good example is a network with the Microsoft Windows family. Windows for Workgroups, Windows 95, and Windows NT Workstation computers can all act as both peers and clients in a Windows NT Server network. The peer computers can share resources when necessary, but utilize the server for most networking requests.

Server Hardware Requirements

- 1 Mention that because servers perform very specialized functions, their hardware requirements are significantly greater. Table 1-1 is especially helpful in detailing the differences between client and server requirements.
- 2 Make special note of the differences between Microsoft's "minimum" requirements and the accepted industry standard, especially in regard to memory and hard drive space.

Specialized Servers

- 1 Describe the basic role of specialized servers. As networks grow larger, it often becomes necessary to divide the tasks of a server between two or more machines. This is especially true when dealing with connections to the outside world such as communications servers or Internet servers.

Selecting the Right Type of Network

- 1 Recap the pros and cons of each type of network, describing the best situations in which to use each. Peer-to-peer networks are best suited to small workgroups where security is not important. Server-based networks are best when large numbers of clients are to be supported and centralized control of resources is imperative.

Additional Case Projects

Case A

A River City Printing company occupies three buildings around the city, an administrative office, a warehouse, and a print shop. Currently, there are a few standalone computers, but no network. The company plans to implement a network linking all the offices in the next few months and has asked you to help design it. There are plans for a total of 20 computers at all three sites. Security is not an issue, and the users are fairly computer savvy. What type of network should be installed and why?

Solution

A metropolitan area network (MAN) will be installed because the all locations are in a single city. A peer-to-peer network is best suited to this situation because there are very few computers and security is not an issue.

Case B

Conglamo, a large, multi-national company is currently running a peer-to-peer network at each of its 35 sites. The sites are not currently connected, but they are planning to do so. To keep costs low, management would like to continue to use the peer-to-peer network. However, as the sites are linked together data will need to be shared between the users and security is very important. Should the company continue to use peer-to-peer networking? What arguments could you use to convince management to switch to a server-based network?

Solution

Conglamo should definitely switch from peer-to-peer to a server-based network. The number of users dictates that the peer-to-peer network be abolished. In your letter to management, note that the computers would not have to be changed, only a server would have to be added. The current desktop operating system could easily fit into a server-based network. In addition, administration of users and resources would be significantly easier in a server-based network, security would be vastly improved, and all data could easily be backed up at a single location.

Solutions

Answers to Chapter Review Questions

Question	Answer	Page
1	b. wide area network	4
2	a. Windows NT Workstation, b. Windows 95, d. Windows NT Server, e. Windows for Workgroups	9 – 10
3	b. peer-to-peer	10
4	a. medium	6
5	b. network interface card (NIC)	6
6	a. easy to install, b. inexpensive c. user-managed resources, e. network is unaffected by one failed computer	10
7	True	5
8	a. LAN	4
9	c. WAN	4
10	d. A collection of standalone machines is the only possible answer (no network is mentioned in the question, so none appears in the answer). It might seem tempting to guess a. LAN, but since no network is mentioned, it's incorrect.	3
11	d. internetwork	4
12	d. peers	6
13	a. fax servers, b. communication servers, c. file and print servers, d. application servers	14
14	b. server-based, c. peer-to-peer	8
15	d. protocol	6
16	c. Individual resources may each have their own unique passwords on a peer-to-peer network, d. There is no centralized security on a peer-to-peer network	10
17	a. share	2
18	c. peripheral devices	2
19	True	2
20	False	8-10
21	a. administrator	8-10
22	a. Tight security is required, c. Budget is the primary concern.	8-10
23	c. server-based	11
24	True	11-12
25	a. specialized servers	14
26	a. combination network	12-13
27	a. RAM, b. disk space, c. faster CPU, d. more CPUs. Some students may not include answer d. Although more CPUs are not necessary, more is always better for CPUs and other system resources.	13
28	a. Windows 95, b. Windows for Workgroups, c. Windows NT Workstation. All of these computers can play limited server roles, and some NT Workstation product provide full-blown specialized server capabilities. But the Microsoft official line is that only Windows NT Server is a full-blown server operating system.	11-12
29	c. fax server. Note: While Windows 95 includes built-in fax software, Windows NT does not.	15

Hands-on Projects Discussion

For the Hands-on Projects that follow, the computers must be running either Windows 95 or Windows NT and will need to be networked. Project 1-1 shows the students how to view network information using the NET VIEW command, whereas Project 1-2 shows the students how to share their resources. As an addition to Project 1-2, let the students view the information on another computer through the Network Neighborhood.

Project 1-1

There are over 20 NET commands available under Windows NT. In this exercise, the students will learn about the NET VIEW and NET HELP commands. The former permits users to view resources active on their networks, in varying levels of detail. The latter provides information about NET commands in general, and syntax and examples for individual NET commands (for example, you used NET HELP VIEW to get the details on the NET VIEW command). Over time, most savvy NT administrators find the NET commands invaluable for obtaining network status information, for troubleshooting balky or errant networks, and for automating all kinds of routine tasks. (For example, the NET ACCOUNTS command can be used to create accounts, establish or change passwords, and logon limitations of all kinds. These can be included in a batch file and run in the background, instead of requiring lots of fiddling with GUI utilities.)

Project 1-2

Sharing resources is one of the fundamental reasons for networking. In this project the students learn how to share a directory across the network; in a later chapter, they will learn how to do the same thing with a printer. In either case, this is a fundamental step toward creating a functioning network. The students will make heavy use of this capability as a network or systems administrator. Please note also that NET VIEW <computername> is a great way to check the status of share assignments and availability; they will probably make heavy use of this utility for that very reason as well.

Case Projects Discussion

Case 1

The requirements for XYZ's network include support for up to 18 people, and to maintain file security on a per-project basis. They also include a requirement that the network be easy to manage and back up. All of these requirements argue strongly for a server-based network, including the requirement for 10 or more users, the need for centralized, secure access to project files, and also for centralized management and back up. These are among the key reasons that Microsoft presents as the rationale for using server-based networks.

Case 2

Widgets requirements include the cheapest possible implementation, minimal training for employees, and a need for employees to be able to control resources on their own machines. All of these requirements are hallmarks of peer-to-peer networks; therefore, Widgets should use the networking services built into Windows 95 or Windows NT Workstation to construct a peer-to-peer network.

Case 3

American Tool and Die's requirements include characteristics that call for a server-based network and other characteristics that call for a peer-to-peer network. Because both kinds of functionality are needed, a combination network is the answer here. The factors that call for a server-based network include the need to share a single database between both locations, plus requirements for network faxing and dial-up services for each location. The factor that calls for a peer-to-peer network is the need for users to have some control over individual resources, on a per-machine basis. Taken together, all these factors argue that a combination network is the right solution.

Case 4

The specialized servers that will be required at American Tool and Die, above and beyond a standard file and print server (which is always safe to assume as part of a server-based network), include the following:

- A database server, to provide access to the single database available at both locations, that managers will use to exchange work orders and monitor inventory.
- A fax server at each location, to support faxing for all users on the LAN. The only reason that two fax servers might be needed, in fact, is to permit easier access to incoming faxes in both locations. Under the right circumstances, however, only a single fax server would be required, provided that users in one office were savvy enough to check a status screen for incoming faxes at the other location. In that case, they would only need access to a local printer to obtain copies of faxes, or they could even read them on-screen, and save a few trees.
- A communications server at one location to support dial-in access to the LAN. Because it's safe to assume that some kind of network link exists between Towson and Beltsville (how else could the managers share a single database at both locations?), users can traverse that link when they dial into Towson, if they need access to resources in Beltsville (or vice-versa, if the server resides in Beltsville).
- Although it's not specifically stated in the requirements for American Tool and Die, a savvy network administrator would also ask the question "What about e-mail?" In most multi-site organizations, e-mail is the biggest productivity booster of all. Sometimes networking knowledge can help elicit requirements (and funding for servers) even when those requirements aren't initially stated.

Chapter 2: Network Design Essentials

Objectives

After reading the chapter and completing the exercises, the students should be able to:

- Design a network layout
- Understand the various networking topologies
- Learn how to integrate the use of hubs into a network
- Explore the variations of the standard networking topologies
- Select the best network topology for the environment
- Construct a network layout

Teaching Tips

Network Design

Designing a Network Layout

- 1 Emphasize the different terms for a network design or layout. Topology, diagram, map, and layout all refer to the physical installation of the network as well as the protocols and communications methods used.

Standard Topologies

Bus

- 1 Describe the bus topology as the simplest of all networking topologies. All computers are connected to a single backbone, over which all communication takes place.
- 2 Emphasize that a single cable break in a bus topology network can cause all network communication to cease.
- 3 Describe the procedure computers use to send data across the network. When a computer has data to send, it addresses the data and places it on the wire. The data is received by all computers, but only the computer the data is destined for accepts the data packets.

- 4 Note that only one computer can send data at a time. Because of this, the larger a bus network gets, the slower communication is.
- 5 Emphasize that the bus topology is a passive topology. This means that the computers on the bus listen for data being sent. They do not take an active role in forwarding data to the destination computer.
- 6 Describe how a signal continues through the network until it is absorbed by a terminator. If a cable break occurs, there is no termination, and the signal continues to bounce indefinitely.
- 7 Note that, although it is very easy to expand a bus network, the topology is still limited to the maximum cable distance of the network architecture. This is discussed in more detail in Chapter 3.
- 8 As the cable reaches its maximum distance, a phenomenon called attenuation occurs. This means that the signal is weakened over distance. However, a repeater can be placed on the segment to increase the strength of the signal.

Star

- 1 Note that the star topology network connects all computers at a central point, the hub. This is convenient for administration, but requires a more intricate cabling installation.
- 2 Also note that one of the biggest attractions of the star topology network is that, if a cable run from a workstation to the hub fails, only that workstation is effected, it does not effect the rest of the network.

Ring

- 1 Briefly discuss the token passing method of communicating on a ring. This will be discussed in more detail in Chapter 7.
- 2 Note that, as opposed to bus and star topologies, rings are active topologies. This is because each computer in the network is responsible for transmitting the data to the next computer in line.
- 3 It is important to note that not all ring networks are physically wired as rings. Token ring networks are generally wired as stars, whereas FDDI network are wired as true rings.
- 4 Note that, like bus networks, a single computer or cable failure effects communication on the entire network.

Hubs

- 1 Describe the difference between active and passive hubs. Active hubs regenerate the signal, whereas passive hubs do not. Passive hubs do not require power.

Variations of the Major Topologies

- 1 Describe each of the three major variations of the major topologies: mesh, star-bus, and star-ring.
 - The mesh network topology provides exceptional fault-tolerance, but at a much higher cost. In actuality, the Internet is an example of a mesh topology network. Many thousands of routers provide multiple paths through the Internet to ensure that data reaches its destination, even in the event of a failure.
 - The star-bus topology connects a series of hubs together via a bus backbone. This is often used to connect hubs on different floors of a building.
 - As mentioned previously, the star-ring topology is used when the network is physically wired as a star, but uses ring communication.

Selecting a Topology

- 1 Discuss the advantages and disadvantages of each topology and the best time to use each.

Constructing a Network Layout

- 1 Discuss the process for constructing a network layout. Each of the questions on page 45 must be answered to create an effective network map. Each of the questions will have an effect on which network topology is used, whether the network will be peer-to-peer or server-based, what type of cabling, protocols, and wide-area technologies will be used.

Additional Case Projects

Case A

The 15 computers in Cindy's office are scattered over two floors of a single building. Each floor has a central telephone room with access to the other floor. She has been asked to connect the computers in a peer-to-peer network. What type of network should Cindy implement?

Solution

Considering that the telephone room is centered on the floor and provides access to the other floors, a star-bus topology would be best. This way, cables don't have to be strung from one computer to the next, as with a standard bus network. All computers could be connected to hubs in the telephone rooms and the hubs could be connected using Thinnets.

Case B

A set of five shared database servers is being developed by your software department. These systems rely on each other for redundancy and are fault-tolerant of each other. Design a network which will provide these computers full redundancy, no matter the cost.

Solution

These five servers should be connected using a mesh topology with at least two connections to the outside network. In this configuration, if one device fails, there are still multiple paths to the users.

Solutions

Answers to Chapter Review Questions

Question	Answer	Page
1	Topology	34
2	c. It requires significantly more cabling than a bus network.	39
3	False	37
4	b. It provides equal access to all computers on the network.	40-41
5	Mesh	42
6	The discussion of star topology mentions the inherent centralization of resources, and resilience in the face of a single computer or cable failure.	38-39
7	Thinnet, 10Base2, coaxial cable	35
8	False	38
9	Signal bounce	36-37
10	Bus	35
11	The disadvantages of a bus topology network include: cable failure leads to network failure, coaxial cable can be expensive and difficult to install and reconfigure.	35-38, 44
12	Star	38-39
13	Signal bounce	36-37
14	The more computers attached to a bus topology network, the slower network communications. This is due to the fact that only one computer can communicate at a time.	36
15	Answers include: a single computer failure on a single-ring topology can impact the rest of the network, it can sometimes be difficult to isolate problems on a ring, adding or removing computers disrupts network operations.	39-41, 44
16	Passive, because computers that do not have data to send are not responsible for ensuring data is delivered.	36
17	There are many reasons to keep a network diagram current, but the most important one is to maintain a record of a network's true layout, configuration, and of the devices and cables that comprise it. This is a key troubleshooting tool, and is often among the first resources that a network administrator will consult when problems arise. Other reasons include: it keeps an accurate inventory of equipment, cables and ancillary equipment; it maintains indicators of what construction activities might impact the network; it provides a complete record of a network's carrying capacity; and it can be used as a tool for planning for growth and expansion.	45-46
18	Attenuation	38
19	Token	40
20	True, for all computers except for the one attached to the broken cable	39
21	Ring (dual counter-rotating rings, in fact)	40
22	Active	39
23	Star	39
24	Active	41

Hands-on Projects Discussion

Project 2-1

The worksheet for this project could be completed as follows:

Will this be a peer-to-peer or server-based network? The brokerage application demands a server, as does the need for sharing sensitive data, and controlling access to files. There are no compelling needs that indicate a combination network is needed, so a straightforward server-based network appears best for Joe's needs.

If server-based, how many servers will be attached to the network? At least one, to handle the brokerage software, and possibly another to handle file and print services. The actual answer will depend on how resource-intensive the brokerage application is. We know of many networks of up to 100 users that are served for all needs by a single server (but usually, a heavy-duty machine with 128 MB RAM or more, 4 GB of disk space or more, and often, 2 or more CPUs).

How many computers will be attached to the network? At least 25, with needs to expand in the near future (planning on 40 to 50 client machines in the near term sounds like a good idea).

What applications will the computers be running? New brokerage software that runs on a server, plus standard word-processing and spreadsheet programs.

How many printers will be attached to the network? 5, with possible needs for expansion

What fault-tolerance level is required by the applications? No requirements for fault-tolerance are stated in the project description.

What funding is available for this network design? According to the specifications, Joe "doesn't want to spend a lot of money."

Given this information and what we know about Joe's office layout—namely, two floors in a building, wiring closets available, and conduit between floors—a hybrid star-bus topology makes the most sense. Following this approach, you'd run coaxial cable through the conduit between floors, and attach to one or more hubs on each floor, then make use of the wiring closets to centralize twisted-pair wiring to the desktops and servers. The need for file security and the existence of sensitive data also argue strongly for physical server security, so you'll want to make sure that servers are housed in a locked room with limited access and adequate power and ventilation to keep them running smoothly.

Case Projects Discussion

Note: The first paragraph of the Case Projects section should be labeled Case 1.

Case 1

The mid-sized engineering firm's needs are somewhat similar to Joe's from the Hands-on project: multiple floors in an office building, a need for all desktops to be networked, and multiple servers that users must access. One major difference is a need for high reliability. The solution is also similar to Joe's with some additional stipulations:

- Keep the hybrid bus-star topology, but run dual links between floors (in different conduits if possible; noisy environments will require fiber rather than coax), so that if one backbone link fails, another can be connected to maintain connectivity. If traffic levels are high, or reliability needs truly extreme, using a fault-tolerant topology like FDDI for the backbone might make sense.
- Use intelligent hubs in the star portion of the network; these will automatically reconfigure themselves in the event of a cable break, and prevent unnecessary interruptions of service.
- Place all servers and hubs in locked, well-ventilated facilities. For maximum availability, this argues for a server room for each of the three floors, with a server and one or more hubs in each room. If the servers are configured to fill in for each other's functions, the floors may be able to function independently even if the bus backbone is broken at any point. For reliability's sake, it's also important to put all servers and hubs on UPSs to maintain the network through power glitches, and to permit graceful server shutdowns in the event of power outages.
- Use Category 5 cable between the hubs and the workstations; not only is it more immune to interference, but it can also support higher bandwidth technologies, should network speed become an issue at any time in the future.

Case 2

Two ways to implement a server farm would be as follows:

Plan 1: Construct a network with two backbones: one through which all desktop traffic flows, and to which all servers are attached. This provides the medium for communications between clients and servers on the network. Create a second backbone, to which only servers are attached. This second backbone can be used to carry replication and synchronization traffic between servers, and will keep this traffic from affecting users' access to the servers. In a pinch, the secondary backbone could be turned into a primary by connecting all the hubs or routers that aggregate the client traffic to that backbone, should the primary ever fail.

The advantages of this approach include:

- The secondary backbone can be implemented locally, using the fastest available technology to maximize the server's abilities to communicate with one another.
- The design isolates client-server traffic from server-to-server traffic, and maximizes network access for both communities.

The disadvantages of this approach include:

- Each server requires multiple network interfaces, incurring more costs for equipment, and more work for installation and configuration (also introduce more points of potential failure).
- The aggregate throughput for each server still includes both client-server and server-to-server traffic, which may overload some systems, unless they're heavy-duty machines with multiple CPUs and lots of RAM (this approach would be recommended, in any case).

Plan 2: Use special mirrored servers for each individual server, or server clustering technology for the server farm. Use a high-speed network switch to aggregate and distribute client-server traffic, and a secondary, high-speed backbone to coordinate server-to-server traffic.

The advantages of this approach include:

- Server mirroring or clustering technologies offer the highest server throughputs available, and create some of the most reliable server systems possible with today's technologies.
- This design also isolates client-server traffic from server-to-server traffic, and maximizes network access for both communities, but its design supports much higher traffic levels and network utilization rates.

The disadvantages of this approach include:

- Both mirrored servers and server clusters are exotic technologies, and demand extraordinarily skilled installation and configuration activities. They are also more difficult to upgrade and maintain. Likewise, these technologies are quite expensive, sometimes as much as two to three times the costs of equivalent, conventional standalone servers.
- The network design requires the purchase and integration of expensive, high-speed equipment. It will add significantly to the costs of the network (but also add significantly to its overall capabilities). As server farms go, this second approach represents the closest most organizations come to matching the state of the art.

Case 3

For classes we've actually taught, the two most common configurations are:

Case 1: a permanent classroom facility, where servers and computers remain set up between classes, ready for reconfiguration and reuse. In this case, a star topology is the most common configuration, with optional access to a local backbone that may lead to other servers (for configuring classroom servers and workstations) or to the Internet (for those classes that require such access). Its benefits appear in the list that follows:

- The network remains a constant in this situation, as do the machines. Cables can be routed out of harm's way, yet provide students with ready access to machines, for practicing hardware installation and configuration.
- This approach offers maximum flexibility and capability, because a second NIC in the classroom server can permit the instructor (or students) to attach other networking devices as class content may dictate, including routers, raid arrays, protocol analyzers, and other equipment.
- Access to the building backbone makes it easy for instructors or administrators to create download images for classroom servers and workstations. Once a class is completed, classroom machines can be wiped clean, and reloaded with the download image necessary for the next scheduled class. This practice is common in most permanent computer teaching facilities.

Case 2: A traveling classroom facility, where servers and computers must be torn down and packed up between classes, ready for reconfiguration and reuse. In this case, a simple 10Base2 bus topology is the most common configuration, because wiring can be routed around the classroom as needed, and because widely available modular components make it easy to set up and tear down). In most cases, all machines are laptops, or all student machines are laptops, and instructor machines/servers are portable lunchbox style computers.

As long as the course operator spends the money necessary for high-quality, padded shipping cases, this setup works extremely well. Its major downside is that network devices fail from time to time, making classroom troubleshooting a part of the customary setup routine. Its benefits appear in the list that follows.

- The network is designed to be easy to set up and tear down. Cables must be routed out of harm's way, and students must be warned about the fragility of PC Card cable attachments.
- This approach also offers good flexibility and capability, because a second NIC in the classroom server still permits the instructor (or students) to attach other networking devices as class content may dictate, including routers, raid arrays, protocol analyzers, and other equipment. Transport may become an issue, but connectivity remains good.
- Instructors must spend time developing scripts and setup utilities to configure student machines for classes. Normally, we'd begin classroom setup by installing software on two machines (the instructor machine and one other), and setting up two independent networks to copy the setup software to other student machines. This bisection of the network keeps traffic on each half to acceptable levels (we've learned it's hard to load Windows NT Workstation on Server onto more than six machines at any one time, using conventional 10 MB Ethernet). Once the downloads are complete, the network can be completely connected, and the class will be ready to go. Barring the need to troubleshoot network cables or NICs, this normally takes between 1.5 and 2.5 hours, for anywhere from 8 to 12 student machines.

Chapter 3: Networking Media

Objectives

After reading the chapter and completing the exercises, the students should be able to:

- Define and understand the technical terms related to cabling, including attenuation, crosstalk, shielding, and plenum
- Identify three major types of both network cabling and wireless network technologies
- Understand baseband and broadband transmission technologies and when each may be used
- Decide what kinds of cabling and connections are appropriate for particular networking environments
- Describe wireless transmission techniques used in LANs
- Describe signaling technologies used for mobile computing

Teaching Tips

Network Cabling: Tangible Physical Media

- 1 Remind the students that the interface between the computer and the media is responsible for making the translation from binary signaling.
- 2 Note that of the two types of transmission media, cabling is by far the most prevalent.

Primary Cable Types

- 1 Mention that cables fall into three basic categories: coaxial, twisted-pair, and fiber-optic.

General Cable Characteristics

- 1 Note that all cables, no matter what type, share the same basic characteristics, listed on pages 53 through 55.
- 2 Briefly discuss each of the fundamental cable characteristics. Make special note of bandwidth, maximum segment length, insertion loss, plenum rating, and costs.

Baseband and Broadband Transmission

- 1 It is important for the students to understand baseband and broadband transmission not only to fully comprehend the technology, but also to supply a basis for the naming conventions used in Ethernet.
- 2 Describe baseband transmission. This method uses a digital encoding and a fixed signal. The entire bandwidth of the cable is used to transmit a single data signal. Using baseband, only one computer can send data at a time.
- 3 Discuss the role of repeaters in baseband networks. They are used to counter the effects of attenuation by strengthening the signal and sending it on.
- 4 Describe broadband transmission. This method uses analog encoding. Because of this, when the cable has sufficient bandwidth, multiple transmissions can be sent at the same time. Cable television uses broadband transmission to send many channels down a single cable.
- 5 Note that broadband transmission is one-way. This means that two channels are necessary for computers to communicate.
- 6 Note that in broadband networks, amplifiers, not repeaters, are used to strengthen signals.
- 7 Discuss the two forms of two-way broadband communication: mid-split and dual-cable. Mid-split communication uses a single cable and divides the bandwidth for two-way communication. Conversely, dual-cable uses two cables, one to transmit and one to receive.
- 8 Note that historically, broadband systems provide greater bandwidth than baseband systems.

Coaxial Cable

- 1 Describe the structure of coaxial cable. The conductor core is wrapped with insulation, shielding, and an outer covering.
- 2 Describe the role of shielding for all cables. This protective layer reduces the influence of external interference, such as EMI or RFI.
- 3 Describe the two basic types of coax (Thinnet and Thicknet) and their IEEE specifications when used with Ethernet (10Base2 and 10Base5).
- 4 Describe the method for naming used with IEEE specifications. 10Base2 translates into 10Mbps, baseband transmission, 200 meters (in actuality its 185 meters, but this will be discussed in greater detail in Chapter 7).
- 5 Discuss the components used to attach a computer to a Thinnet segment. The BNC cable connector is attached to a BNC T-connector, which is connected to the BNC port on the network adapter card.

- 6 Note that many cable specifications follow the Radio Government (RG) guidelines. Thinnet is RG-58 cable. Note also that CATV cable is actually RG-59. These are not the same and CATV cable cannot be used for Ethernet networks.
- 7 Be sure to mention the note included with Table 3-2. BNC is defined a number of different ways. If the students plan to take the Microsoft certification test, BNC is defined as British Naval Connector. However, the other names listed are used as often.
- 8 Mention that Thicknet is often described as “Standard Ethernet” because it was used for the first implementation of Ethernet.
- 9 Note that, because Thicknet is thicker, it has a larger maximum cable length and is less susceptible to interference.
- 10 Note the comparison shown in Figures 3-3 and 3-4. Computers attached to Thinnet networks are connected via T-connectors. However, there are significantly more parts when connecting a computer to a Thicknet network.
- 11 Discuss the role of terminators in coaxial networks. These terminators absorb signals so that they do not bounce along the cable indefinitely. Without proper termination, computers will not be able to communicate on a network.

Twisted-Pair Cable

- 1 Discuss the role of the twists in twisted-pair wire. The twists cause the magnetic fields created when signals are passed through the wires to wrap around each other, which increases the wire’s resistance to interference.
- 2 Define crosstalk and its effect on network communication.
- 3 Briefly discuss the two types of twisted-pair cable: UTP and STP.
- 4 Mention that UTP is the basis for the 10BaseT specification. Because it can be used for telephone as well as computer connections, it is rapidly becoming the most popular cable type.
- 5 Discuss the cooperation of EIA, TIA, and ANSI which defined the categories of UTP. The ANSI/EIA/TIA 568 Commercial Building Wiring Standard defines how UTP is constructed (number of twists per foot, etc.), how it is used, and the maximum transmission speeds for the cable.
- 6 Briefly discuss all categories of cable, concentrating on Category 3 and Category 5 because they are the most prevalent in Ethernet installations.
- 7 Note that because of its shielding, STP is far more resistant to interference and crosstalk than UTP. However, it is also more expensive.
- 8 Also note that although there are no standards for STP cables, they are generally measured against the ANSI/EIA/TIA 568 standard.

- 9 Discuss the connectors used in twisted-pair cabling, RJ-11 and RJ-45, and their differences. RJ-45 connectors are used in network cabling and contain eight wire traces, as opposed to the four wire traces in RJ-11 connectors.
- 10 Discuss the pieces of a twisted-pair wiring center.
- 11 The caption for Figure 3-8 has the connectors backward. The punchdown block is shown on the right and the patch panel is on the left.

Fiber-Optic Cable

- 1 Note that fiber-optic cable uses pulses of light rather than electricity. Because of this, it is essentially immune to interference and has much longer maximum cable lengths, in some cases as long as 100 kilometers.
- 2 Also note that because fiber-optic cables use light, they are also immune to eavesdropping. Electric media can be “listened to” because they emit external signals. This is not the case with fiber-optic cable.
- 3 Mention that fiber-optic cable also supports much higher bandwidths than copper cables.
- 4 Note that the benefits of fiber-optic cable come at a price. It is the most expensive cabling option and care must be taken during installation with regard to bending the cable to the point the inner conductor, which is usually made of glass, breaks.
- 5 Discuss the structure of the fiber-optic cable and the role of the cladding and shielding. Every part of the fiber-optic cable exists to ensure the core does not break.
- 6 Note that fiber-optic communication is a one-way street. This means that two cables are required for computers to communicate.
- 7 Discuss the connector types used with fiber-optic cables.

Cable Selection Criteria

- 1 Discuss each of the questions listed on pages 69 and 70. These questions are integral in choosing the correct cable type for a network.

The IBM Cabling System

- 1 Discuss the fact that IBM created its own cabling system which divides the cables into type according to their structure and role in the network.
- 2 Note that the IBM cable connector is neither male nor female, which requires special faceplates and distribution panels.

- 3 Note that the IBM cabling system uses the American Wire Gauge (AWG) standard which uses the diameter of the conductor as its measurement. The smaller the AWG number, the larger the conductor.
- 4 Also mention that there is no IBM Type 4 definition.

Wireless Networking: Intangible Media

- 1 Make it clear to the students that wireless does not mean without cables of any kind. Wireless networks are most often combined with a normal wired network, creating a hybrid network.

The Wireless World

- 1 Discuss the cases where wireless networks are common. Other examples include: users in warehouses that need access to the network, but cannot use a cabled computer to verify stock; two buildings on opposite sides of a river where physical cable runs are impossible.

Types of Wireless Networks

- 1 Discuss the three types of wireless networks. Mention that mobile computing is a carrier-based network because it relies upon a communications carrier such as AT&T or GTE.

Wireless LAN Applications

- 1 Note that the only difference between cabled computers and wireless computers on a LAN is how they are connected. Wireless users are able to access the network as if they were physically wired to it.
- 2 Discuss the role of the access point device in wireless LANs. This is the component which connects the wireless computers to the physical network. In essence, it is a hub for wireless computers.

Wireless LAN Transmission

- 1 Discuss the measurement of electronic signals transmitted through the air: the number of cycles per second, or Hertz.
- 2 Note that this measurement affects the amount of data and the speed at which the data is sent. Generally, lower-frequency transmissions carry data more slowly over longer distances, whereas higher-frequency transmissions carry data more quickly over shorter distances.
- 3 Discuss the frequency bands used by radio, microwave, and infrared wireless systems.
- 4 Note that high frequency technologies often require a clear line of sight between the sender and the receiver.
- 5 Mention each of the four types of wireless LAN technologies: infrared; laser; narrowband, single-frequency radio; and spread-spectrum radio.

- 6 Describe the different types of infrared networks. These are often used in LAN environments because they are able to transmit at up to 10Mbps.
- 7 Note that spread-spectrum radio technologies use multiple frequencies simultaneously. This reduces the susceptibility to interference and also limits the possibility of eavesdropping.
- 8 Discuss frequency hopping and direct-sequence modulation techniques for ensuring data arrives intact and it is not intercepted on the way. When discussing direct-sequence modulation, mention the practice of sending dummy chips on some channels to confuse anyone who may be attempting to eavesdrop on the transmission.

Wireless Extended LAN Technologies

- 1 Discuss the role of wireless technologies in extending networks. This applies most to connecting buildings where physical cabling is impossible, such as the earlier example with the river.

Microwave Networking Technologies

- 1 Note that microwave communications are broken up into two categories: terrestrial and satellite. Note that even satellite microwave communication requires "line of sight." Microwave devices just see farther than humans.
- 2 Mention that, although it is fast, it is also very expensive to use microwave communication, especially satellite.

Trends in Wireless Networking

- 1 Discuss the 802.11 Wireless Networking Standard which is expected to be approved by the IEEE in 1998.
- 2 Also discuss cellular packet radio and CDPD. These technologies are proving to be some of the most exciting in wireless networking.
- 3 Each of these wireless technologies is growing quickly and the industry expects bandwidth to increase and costs to decrease faster than any other networking technology in history.

Additional Case Projects

Case A

You are developing a workgroup network for your design department. There are nine computers which need to be connected and one printer. All lie are situated in a rough circle around a central wiring closet on one floor of a building. There is no great need for speed and costs should be kept low. Discuss the advantages of using both Thinnet and UTP in this configuration.

Solution

Because there is no real need for speed and the users are fairly close together on a single floor, 10Base2 is a good solution. It is inexpensive and easy to implement. Because all computers are centered around a wiring closet, a 10BaseT implementation could also be used. This type of configuration is easy to troubleshoot and also inexpensive to implement and maintain. The ultimate decision centers around upgradability. Knowing there is no current need for speed, it may not be necessary to go with UTP. However, knowing the way businesses operate, an upgrade is inevitable. UTP is probably the best solution for this network.

Case B

Steve's boss has asked him to suggest alternatives for connecting his company's two buildings. They are currently leasing a T1 from the phone company and it's getting expensive. He would rather incur a large one-time cost than keep paying the phone company. He is leaning toward microwave because the buildings have line-of-sight. However, the entire half mile between the buildings is owned by Steve's company and Steve feels fiber-optic would be the best option. What arguments can Steve use to convince his boss fiber-optic is the way to go?

Solution

Again, it comes down to a matter of upgradability. Steve knows that microwave will only operate up to 10Mbps, whereas fiber-optic can reach a theoretical speed of 2.4 Gbps. Even using 100 Mbps fiber-optic is a better solution than microwave. In addition, fiber-optic is not susceptible to any interference or eavesdropping, whereas microwave is very susceptible to both.

Solutions

Answers to Chapter Review Questions

Question	Answer	Page
1	d. optical fiber	56-57
2	c. short	57
3	d. insulating layer	56-57
4	c. backbone	59-61
5	d. attenuation	53
6	a. core	56
7	d. plenum	54
8	d. PVC	54
9	d. plenum	54
10	d. fiber-optic cable	68
11	a. Category 1	64
12	b. RJ-45	65
13	True	58-61
14	d. fiber-optic	67-68
15	d. Category 5, e. Fiber-optic	64, 68
16	d. crosstalk	62
17	b. is the official answer. There have been cases where RG-62 has been used in an RG-58 network, but it is not recommended.	59
18	c. wire braid	67
19	b. lowers susceptibility to interference, c. increases maximum segment length	64
20	d. Note that two 10BaseT NICs can sometimes be connected with a single STP cable (answer a) but that is not always the case.	58
21	a. vampire tap	60
22	b. digital	55
23	a. analog	55
24	a. access points	73
25	d. wireless bridge	78
26	All answers (a., b., c., d.)	74-78
27	b. frequency-hopping, d. direct-sequence	77-78
28	a. reflective infrared, e. low-power, single-frequency radio	75-76
29	c. propagation delay	79-80
30	d. spread-spectrum radio	77-78

Hands-on Projects Discussion

Project 3-1

For this project, it is a good idea to get as many different types of media as you can find. Variations of thin coax such RG-58, RG-59, and RG-62, both shielded and unshielded twisted-pair, IBM Type 1 and Type 2 cables, and fiber-optic. It is also a good idea to only have one end of these cables terminated. The unterminated end can be cut back to reveal the core and, where applicable, shielding.

Project 3-2

Scenario 1: A Noisy Stretch

If any kind of conductive cable has to pass through an interference-rich environment—and the shop floor at XYZ sounds “noisy” in the extreme—it must be routed through metal conduit to deflect most of the interference. Even so, close proximity to intense sources of interference could still impede network traffic, so care must be taken when routing the conduit to avoid coming closer than 25 feet to intense sources of interference, such as arc-welders or metal stampers. The only medium that’s guaranteed to be immune to such interference is fiber-optic cable. In this kind of environment, we’d still recommend running it through conduit anyway, to protect it from errant forklifts and the vagaries of heavy machinery.

Scenario 2: Going the Distance

A single segment of either Thickwire Ethernet or fiber-optic cable will go the distance from the front office to the loading dock (10Base5 can cover 500 meters, or over 1,500 feet; 10BaseF can cover over 2 km, or over 6,500 feet). But two segments of Thinnet could be connected through a repeater, and cover the same distance as well. As long as this doesn’t violate the 5-4-3 rule for Thinnet (only three cable segments may have network devices attached, a maximum of 4 repeaters between any two cable segments, and no more than 5 segments in total), this configuration will also work.

Scenario 3: Build a Better Backbone

Given that most inter-floor gaps in office buildings seldom exceed more than 20 feet, the maximum distance from the ninth to the eleventh floor is around 60 feet. Figuring an additional 40 feet at both ends for runs between the elevator shaft and wiring closets, this only eliminates TP from contention. But if either Thinnet or Thickwire coax is to be used in an elevator shaft, it must be routed through conduit for additional shielding (elevators can be rich, if intermittent, sources of EMI and even RFI). Of these two options, Thickwire’s higher resistance to interference makes it the better choice. But of all available options, fiber-optic remains the best because of its relative immunity to interference. Because of the temperature and humidity conditions in elevator shafts, we’d still recommend running fiber-optic cable through conduit in that kind of environment. And when it comes to open-ended bandwidth, nothing beats fiber-optic cable: recently reported tests have measured actual throughput on fiber optic cable of 10 Gbps—today, no conductive cable even comes close to this kind of bandwidth!

Case Projects Discussion

Case 1

Whenever cables go through the ground, differences in ground potential between one location and another can cause current to flow. Because this will interfere with, if not block, networked communications, most network engineers recommend using fiber-optic cable for in-ground cable runs. Likewise, only fiber has the ability to accommodate increasingly large amounts of bandwidth, leaving room for higher-speed technologies to use the existing in-ground cable. Thus, of the possible answers to this case project, both c and d are correct, but c is the most compelling technical justification for using fiber-optic cable, rather than Thinnet.

Case 2

Here, TVBCA is moving new facilities, where they want to use a fiber-optic backbone to interlink all three buildings. Because fiber-optic cable easily meets the 100 Mbps speed requirement, the proposed solution achieves the required result. Because fiber-optic cable is as immune from eavesdropping as it's possible to get, it also obtains the first of the optional desired results. But because fiber-optic cable and the associated backbone access equipment are expensive, this solution fails to meet the second optional desired result of creating a network that's as inexpensive as possible. Thus, answer b is correct.

Case 3

The advertising firm's decision to use Category 5 wiring and hubs, presumably with 100 Mbps Ethernet, certainly delivers the required result, of providing a network that operates at speeds of up to 100 Mbps. Of all twisted pair cable varieties, however, Cat 5 is the most expensive, so the cabling will not be as cheap as it gets—but to meet the 100 Mbps requirement, Cat 5 is required, so this is one of those Microsoft questions that requires careful reading. The exact wording is “as inexpensive as it can be”—as long as you buy a reasonably priced grade of Cat 5 cable, this requirement cannot help but be met, despite appearances. As for ease of installation, only someone on-site can decide what's easy and what's not. However, professional TP cable installation usually requires wall plates and routing cables through ceilings and into walls. These fail to qualify as easy, unless you're a full-time cable installer. Therefore, the answer to this question is b, because the required result and only one of the optional desired results is met.

Case 4

XYZ Corp.'s quest for mobile computing for its field engineers depends on use of cellular modems to connect remote computers with the organization's LAN. Because the plan also includes encryption fees, even though the traffic is broadcast, it's safe to assume that encryption makes eavesdropping a waste of time. But because cellular technologies are not the cheapest, the solution fails to meet the requirement that it be as cheap as possible. Thus, the answer is b because the required result and one of the optional desired results is met.

Case 5

Back at TVBCA, they're trying to bridge the Susquehanna electronically. The solution they've chosen is a pair of infrared laser wireless bridges. These will definitely meet the required result, because the bridges will link the two LANs. They will also meet the need for security from electronic eavesdropping, because the clear line of sight must be intercepted to grab any traffic. Infrared emissions more than three or four meters from the devices would be extremely hard to intercept and decode, so as long as TVBCA can keep interlopers with snooping equipment off their buildings' roofs, they should be OK. And finally, because infrared emissions are immune to EMI, as long as TVBCA shields the cable that connect to the bridges as heavily as possible, the bridges themselves shouldn't suffer from their proximity to the substation. Thus, the answer to this question is a, because the required result and both optional desired results are met.

Chapter 4: Network Interface Cards

Objectives

After reading the chapter and completing the exercises, the students should be able to:

- Describe what role a network adapter card plays in networked communications
- Explain how network adapters prepare data for transmission, accept incoming network traffic, and control how networked communications flow
- Understand the variety of configurable options for network adapters and describe common settings
- Describe important characteristics for selecting adapter cards
- Recount network adapter enhancements that can improve performance
- Explain the role of driver software in network adapters

Teaching Tips

Network Interface Card (NIC) Basics

- 1 Note that the sole purpose of a network interface card is to mediate the connection between the computer and the network medium. This includes managing the physical connection as well as translating data from the computer into signals appropriate for the network medium.
- 2 Note that network interface cards go by many names including network adapter, NIC, and just plain network card.

From Parallel to Serial, and Vice Versa

- 1 Describe parallel transmission. Data is sent along a number of lines at the same time. This is the transmission method used within the computer.
- 2 Describe serial transmission. Data is sent in a linear sequence. This is the transmission method used by most network media. One of the jobs of the NIC is to convert the data it receives in parallel to serial for transmission across the network, and perform the reverse operation for incoming data. Figure 4-1 illustrates this function very well.

- 3 Define bus width. This is the number of parallel lines that make up the computer's bus. This width is measured in the number of bits which can be moved in a single bus transfer. Although buses are discussed in greater detail in the next section, mention here that the first PCs used an 8-bit bus. The second generation of PCs move to 16-bit, which became the Industry Standard Architecture (ISA).
- 4 Describe the role of the transceiver in network communication. As the students learned in Chapter 3, the transceiver for a Thickwire network is connected directly to the backbone. The computer is then attached to the transceiver via a drop cable. However, most other types of NICs include a transceiver directly on the card. It is also very common to include multiple transceivers on the NIC to accommodate different media.
- 5 Note that the NIC is responsible for packaging data into packets, which are the fundamental units of data for network communication. The NIC is also responsible for correcting packet-level errors.
- 6 Describe the NIC's role as "gatekeeper" for the computer. It examines all packets on the network as they are sent and determines whether the computer is the destination of any packet. It does this by examining the destination network address of the packet and comparing it to its own network address. This process is discussed in more detail in Chapter 5.

PC Busses

- 1 Note that there are four types of PC busses: Industry Standard Architecture (ISA), Enhanced Industry Standard Architecture (EISA), Micro Channel Architecture (MCA), and Peripheral Component Interface (PCI).
- 2 Describe each of the busses and their speeds (8-bit, 16-bit, or 32-bit). Note that EISA slots can accommodate ISA cards. Also note that MCA is not often found in PCs.

Principles of NIC Configuration

- 1 Mention Plug and Play and its ideal configuration strategy. Also mention, however, that it often does not work. The more devices in your computer, the less likely it is that Plug and Play will work.
- 2 Note that many cards are software configurable, but some cards, especially older cards, require setting be made via jumpers or DIP switches.

Setting IRQs

- 1 Define interrupt and interrupt request line (IRQ). These are used by the devices in a computer to get the attention of the CPU.
- 2 It is very important the students understand that each device must have its own IRQ. If two devices are configured to use the same IRQ, problems occur. Depending on the conflict, the machine may not even boot.
- 3 Note that diagnostic software such as MSD or WINMSD can be used to view the interrupts being used in a computer. If you run MSD before you install the NIC, you will know which IRQs are available.

- 4 For purposes of the Microsoft certification test, it is important the students know which IRQs are assigned by default to which devices. There may be questions which say “Your computer has a floppy drive, two serial ports and one printer port. Which IRQ can be used for a network adapter?”

Base I/O Ports

- 1 Define I/O ports. Again, it is important for the students to know which I/O ports are available for use by peripherals such as NICs.

Base Memory Address (membase)

- 1 Define base memory address and how it is used by the NIC to communicate with the CPU.
- 2 Also describe the high memory area. This goes back to the earliest days of the PC when, according to Bill Gates in a speech in 1981, “640K ought to be enough for anybody.”

Making the Network Attachment

- 1 Note that the network card must match the medium. Some cards, like Ethernet, are able to accommodate a number of media, whereas the more advanced and specialized cards are only able to support one media.

Choosing Network Adapters for Best Performance

- 1 Discuss each of the methods listed for increasing the speed of adapter cards. There are a number of questions on the Microsoft certification test which require the students to know how server speed can be increased. The questions are phrased “Which of the following network adapter card configurations will provide the highest throughput? ISA with DMA, EISA with shared system memory, PCI with DMA, or MCA with bus mastering?”

Special-Purpose NICs

Wireless Adapters

- 1 As mentioned in Chapter 3, network adapters for wireless communication are different than those for wired communication. Note that these are available for most operating systems.

Remote Boot Adapters

- 1 Discuss the need for specialized network adapters to be used in diskless computers. Often, for security reasons, computers are installed without disk drives of any nature. The network adapters in these computers use a Boot PROM to connect to the network to load the operating system.

Driver Software

- 1 Discuss the role of the device driver in network communications. This driver is used by the computer to control the NIC.
- 2 Note that in the early days of networking, a driver was compiled for each variation of the network card. For example, a driver was created for a card using IRQ 5 and I/O port 300h. Then, if the card was move to another machine or reconfigured for any reason, a new driver was compiled with the new settings. As you can image, this was an exceptionally tedious task.
- 3 Discuss the NDIS and ODI standards which allow more than one protocol to run on a NIC and, in the case of ODI, simplify driver development. It is important for the students to be familiar with these standards for the Microsoft test.

Additional Case Projects

Case A

Develop an example of how bus width effects communication.

Solution

There are many different things the students could use for this example. The key is that when there are more lines to access a component, communication is faster. Some examples might include waiting in line at the grocery store or a concert.

Case B

Your company often employs temporary workers to input sensitive data. As your network and database have grown, concern has mounted that the information these workers enter may not be safe, or may be taken off the premises. Your boss has asked you to implement a hardware-based solution to ensure that nothing happens to the data in the system.

Solution

The best option for this scenario is to install remote boot adapters in diskless workstations. This way, the workers are able to input the data, but are not able to damage the data with viruses or remove information on diskette. It is important that the students understand that changes will need to be made on the workstation side and also on the server to support remote boot systems.

Solutions

Answers to Chapter Review Questions

Note: Question 25 should read: “Which of the following are the most common I/O port assignments for NICs?”

Question	Answer	Page
1	d. IRQ 11	110
2	a. PCI, b. MCA, c. EISA	106
3	a. A driver is a small program that mediates between the computer’s operating system and a hardware device. Some students may choose b. Although a driver may act like part of the operating system, it is really a separate piece of software.	115
4	a. agree with	115-116
5	False	102-103
6	d. 16-bit and 32-bit	105-107
7	d. on-board RAM	102-103
8	All answers (a., b., c., d.)	112
9	All answers (a., b., c., d., e.)	110
10	5	110
11	c. Neither device will work.	109
12	d. Permit the CPU and a peripheral device to exchange messages.	110
13	All answers (a., b., c., d.)	112
14	b. EISA, c. MCA	106
15	c. Windows 95	107
16	c. To inform the CPU that some event requiring its attention has occurred.	109
17	a. ISA, b. EISA	106
18	All answers (a., b., c., d.)	113
19	b. IRQ, c. base I/O port, d. base memory address	109-111
20	b. transceiver	103
21	All answers (a., b., c., d., e.)	102-105
22	a. Networks got faster, so buses did; too, b. Increased CPU speeds demanded faster, wider busses; c. Increased application sophistication increased user’s demands for data; d. More applications needed network support.	105-107
23	a. Check the CPU, motherboard, and peripherals at PC boot time.	107
24	a. Macintosh OS 8.0 and higher, e. Windows NT Server and Workstation	109
25	c. 280h, d. 300h	110
26	False	111

Hands-on Projects Discussion

The Hands-on projects for this chapter involve installing a network interface card in a computer. The projects assume the students will be using Windows 95 or Windows NT machines. It is important during the second project that students ground themselves properly and work with the equipment very carefully.

Project 4-1

Throughout this project, the students use Microsoft programs to document the machine's current configuration. This is a very important step in installing any new hardware in a computer and the students should be very familiar with the process.

Project 4-2

In this project, the students actually take apart the computer and install the new adapter. Any hardware configuration must be done at this time and the students must be extremely careful with the hardware.

Project 4-3

The students are now ready to power their machines on. It is important to note that some computers may not boot because the configuration settings of the new adapter may conflict with a previously installed adapter. If this is the case, the student should move to another computer and check the adapter there. If the student was not properly grounded, there is a chance the card or motherboard could be damaged.

Project 4-4

Once the computer has restarted, it is time to install the adapter software. If the student is using a Windows 95 computer, and it is a Plug and Play adapter, the student will be asked to install the software as the computer boots. If the student is using a Windows NT computer, they must go through the Control Panel to install the software.

Project 4-5

Once the NIC and software are installed, the students use the NET VIEW command to verify configuration and that the adapter is working properly.

Case Projects Discussion

Case 1

The hardware that's installed in the PC includes a serial mouse and an internal modem, this does away with both serial ports, so there go IRQs 3 and 4. The two SCSI controllers will probably take up IRQs 10 and 11. Also, IRQs 0 (system time), 1 (keyboard), 2 (IRQ cascade), 6 (floppy drive), 7 (LPT1:), 8 (real time clock), 9 (IRQ cascade), 13 (math coprocessor), and 14 (IDE controller) are often taken. This leaves only IRQ 5 available from the list shown, which is why it's also the most common factory default setting for NICs anyway.

Case 2

Because a 32-bit bus mastering NIC with additional onboard RAM gives you about as much speed as you can get when attaching a server to a cable segment, it definitely produces the required result of handling network traffic with reasonable response time. This also helps to guarantee that the server won't slow the network down. But because it would be cheaper (in fact half the cost) to use plain-vanilla NICs on the relatively idle segments, this solution fails to keep the hardware costs of a minimum. Thus, the correct answer is b, which produces the required result but only one of the optional desired results.

Case 3

The real issue with Bob's PC is that it is painfully slow. This will affect the network only when he's transmitting data, however. Therefore replacing his NE1000 with an NE2000 is probably the most practical solution (answer a). Replacing the card with an EISA version does no good because an EISA card won't work in an ISA slot (although ISA cards can work in EISA slots, it doesn't work the other way around). If Bob generates a lot of traffic on the network, however slowly, answer c will indeed isolate other users from his influence; in that case, this answer makes the most sense. Because you can't replace Bob's old PC with a new one, a PCI card won't work in his machine, either, so answer d. is completely incorrect. Because a is more practical than c, we think the correct answer to this question should be a, but it's a close call.

Case 4

Dealing with interrupt conflicts gets to be a way of life when installing NICs, especially for heavily loaded end user machines. The only real solution to the problem that doesn't diminish the machine's current capabilities is to follow the strategy outline in answer a, and try to change the IRQ for some other device, to free up an IRQ that the NIC can use. Answer b implies that whatever devices can't be made to work can be omitted, which the user may not appreciate. Answer c may work, but the PC Card NIC will still need an IRQ, too—you may be spending more money, just to wind up with the same problem you were trying to solve. Answer d limits the speed of the network attachment to serial port speeds; unless you spend real money (\$150 or more) for a high-speed serial interface, you'll wind up with a network attachment that runs significantly slower than a NIC attachment. This is a solution that's only worth considering if all other options have been exhausted and the machine still can't be connected to the network.

Chapter 5: Making Networks Work

Objectives

After reading the chapter and completing the exercises, the students should be able to:

- Understand and explain the OSI reference model
- Understand and explain the IEEE 802 networking model and related standards
- Explain the OSI reference model's layers and their relationships to networking hardware and software

Teaching Tips

OSI and 802 Networking Models

- 1 Note that these theoretical models are extremely important in understanding how networks work. In terms of the Microsoft tests, there is significant coverage of the OSI model and IEEE 802 specifications. Questions range from “Which of the following devices operates at the Network layer of the OSI model” to “Which of the following IEEE 802 specifications concerns itself with high-speed networking.”

Role of a Reference Model

- 1 Discuss reference models in general and, in particular, the OSI reference model. It provides a standard framework to discuss what takes place when two devices communicate.
- 2 Also note that “Open Systems” is the ultimate goal of the OSI model. It has provided a basis for non-proprietary devices and protocols.

OSI Network Reference Model

- 1 Note that the OSI reference model is made up of layers. These layers are centered around the idea that every function in a network can be broken up into a series of related tasks.
- 2 Another example which can be used to illustrate layers is vehicle production. Each team has its own function (design, engineering, production) and relies on the others to complete the task—putting a quality automobile in your garage. It would be a good idea to have the students come up with other examples to facilitate their understanding of layers.

OSI Reference Model Structure

- 1 Note that the OSI reference model is divided into seven layers, shown on page 139 in Figure 5-1. Each layer performs a specific tasks in network communication and will be discussed in detail momentarily.
- 2 Discuss the interconnection between the layers. Each layer interacts with the layer above and below it. For example, the Session layer works with both the Transport layer (immediately below), and the Presentation layer (immediately above).
- 3 Note that the layers can be generally grouped together according to function. Layers 1 and 2 are concerned with the physical media, signaling, etc. Layers 3 and 4 deal with getting the data to the destination across the network. Layers 5 through 7 handle conversations between the computers.
- 4 Note that each layer communicates with its peer layer on the other computer which is often called logical or virtual communication. This means that the Transport layer on the sending computer communicates, by using the services of the lower layers, with the Transport layer on the receiving computer.
- 5 The mnemonics listed in the Note on page 141 are very, very handy for remembering the layers and their order.
- 6 Mention that as data is passed down through the protocol stack, each layer adds its own information to be used by its peer layer on the receiving computer. When the data is received and passed up through the layers, each layer removes the information attached by its peer on the sending computer.
- 7 Describe PDUs and their function in the OSI model.
- 8 Describe each of the layers of the OSI model. Be sure to note the following:
 - The Application layer provides the interface to the user and makes decisions on whether or not network access is needed.
 - The Presentation layer handles data compression/decompression and encryption/decryption.
 - The Session layer manages the “conversation” between applications and is responsible for synchronization
 - The Transport layer is responsible for segmenting the stream of data from the upper layers into manageable pieces. It is also concerned with error-free delivery and thus manages flow control and error handling.
 - The Network layer’s responsibility is to direct data in an internetwork. It is also responsible for logical network address to physical network address conversion.
 - The Data Link layer is responsible for addressing the packets and defining the structure of the packets. This structure is called the frame and is discussed in more detail in Chapter 6.
 - The Physical layer converts bits into signals to be sent across the network.

IEEE 802 Networking Specifications

- 1 Note that IEEE Project 802 was started to define a set of LAN standards to ensure that network interfaces and cabling from multiple manufacturers would be compatible. As an interesting side note, 802 stands for February (2), 1980.
- 2 It is also important to note that although the 802 standards predate the OSI model, they were developed collaboratively and are compatible with each other.
- 3 Note that the majority of Project 802's work was done in the Physical and Data Link layers.
- 4 Mention that there are currently 12 standards from Project 802 (802.1 through 802.12). The IEEE recognizes that networks are constantly changing and have provided mechanisms for expanding the project as necessary. For the purposes of this class and the Microsoft tests, the students should focus on the 801.1 through 802.5 standards, with some attention to 802.11. and 802.12, the newest standards.

IEEE Extensions to the OSI Reference Model

- 1 It is very important to note that the IEEE divided the Data Link layer into two sublayers: Logical Link Control (LLC) and Media Access Control (MAC). There are questions on the Microsoft test which are directly related to where these two sublayers fit into the OSI model.
- 2 Describe LLC and its use of Service Access Points.
- 3 Mention that the MAC sublayer provides shared access for multiple NICs at the Physical layer. Although it will be mentioned later, note that the MAC sublayer is responsible for the physical addressing. Each network card has a MAC address that identifies it on the network.

Additional Case Projects

Case A

Develop an example for how layers work.

Solution

There are many different things the students could use as examples of layers. The key is that each layer performs a specific function. Some examples might include driving a car to the store or any type of communication, phone calls, meetings, etc. Each of these has a specific set of guidelines which govern what takes place.

Case B

Using your example in the Case 3, assign names to your layers and specify their specific tasks.

Solution

The solution for this Case study depends entirely upon the example used in Case 3. It is important that the students understand how the steps are applied to situations. Stress that the layers they create should apply to situations similar to the example they developed in Case 3.

Solutions

Answers to Chapter Review Questions

Question	Answer	Page
1	c. seven	139
2	False	137-139
3	a. formatting, d. addressing	141-142
4	d. peers	140-141
5	a. 6, b. 2, c. 5, d. 1	139
6	Data Link	144
7	c. Network	144
8	Physical	145
9	c. Network	144
10	Presentation	142-143
11	c. Session	143
12	Transport	143
13	b. protocol suite	139
14	b. control information for frame type, routing, and segmentation; c. payload data; d. CRC, a data integrity check	144-145
15	b. Cyclical Redundancy Check	144
16	c. Twice; once before transmission and again on receipt	144
17	c. 802.3, d. 802.4, e. 802.5, f. 802.12	149
18	b. Data Link	148
19	b. Logical Link Control (LLC), d. Media Access Control (MAC)	148
20	b. Logical Link Control (LLC)	148
21	b. 802.3	147
22	d. 802.5	147
23	c. 802.4	147
24	e. 802.11	147
25	b. 12	147
26	a. IPX/SPX, b. TCP/IP	139-140

Case Projects Discussion

Case 1

All of the available answers are correct and can be used as arguments against ARCNet. The fact that Ethernet is accepted as a standard means that it is widely supported and, consequently, equipment and drivers are very easy to find. The availability of different network media makes the cost of Ethernet negligible in comparison to ARCNet. Of course, higher speed is always preferable. If, after all of these arguments, your boss still disagrees, it might be a good idea to demonstrate each technology, to give him a real feel for the differences.

Case 2

Again, all of these are reasonable arguments. It may not matter to your boss whether it is an “accepted industry standard,” but it will make drivers and devices easier to find. Speed is always an issue and the fact that, at a minimum, Ethernet moves at 10Mbps should be an incentive. Of course, 100Mbps is available and prices are dropping, so it is an even more attractive technology. The fact the Ethernet can run on many media that are resistant to interference makes it a likely choice for getting the shop floor connected.

Chapter 6: Network Communications and Protocols

Objectives

After reading the chapter and completing the exercises, the students should be able to:

- Understand the function and structure of packets in a network and be able to analyze and understand those packets
- Understand the function of protocols in a network, discuss the layered architecture of protocols, and describe common protocols and their implementation
- Understand channel access methods

Teaching Tips

Function of Packets in Network Communications

- 1 Note that data is divided into packets for manageability and reliability. Smaller chunks of data are easier to manage and if the packet is damaged during transmission, just a small piece of the original data will need to be resent.

Packet Structure

- 1 Note that the exact structure of a packet is determined by the protocol and media being used. As you'll see in Chapter 7, different protocols use different packet structures or frames. However, all packets have three basic parts: the header, data, and trailer.

Packet Creation

- 1 Figure 6-3 shows the process of creating a packet. As the data is passed through the layers of the OSI model, each layer on the sending computer adds its own header or trailer information, whereas this information is removed on the receiving end.

Understanding Packets

- 1 Note here that, as mentioned in Chapter 4, it is the job of the NIC to determine which packets on the network are destined for the computer.

Protocols

- 1 State that, by definition, protocols are rules for communication. This term, of course, was used when discussing rules for meeting and communicating with people. This also applies to communication between computers.

The Function of Protocols

- 1 Define protocol suite. There is no single protocol which encompasses all aspects of network communication. When a group of protocols is designed to work together to communicate effectively over a network, it is called a protocol suite or protocol stack.
- 2 Describe connectionless and connection-oriented protocols. Connectionless protocols assume that the data will get to its destination by relying on the other protocols in the suite. Connectionless protocols are generally very fast because of this assumption. Connection-oriented protocols, on the other hand, establish a connection to ensure reliable delivery of the data. This comes at a price, however, because connection-oriented protocols are slower.
- 3 Describe routable and non-routable protocols. It is very important for the students to understand that some protocols, most particularly NetBEUI, do not contain Network layer information and, consequently, are not routable. This is addressed in questions on the Microsoft certification test.

Protocols in a Layered Architecture

- 1 Discuss the division of protocols by function into three basic groups: network protocols, transport protocols, and application protocols.
- 2 Describe the general function of each of these types of protocols.

Common Protocols

NetBIOS and NetBEUI

- 1 Discuss the history of NetBIOS and NetBEUI. NetBIOS was developed by Microsoft and IBM for workgroup environments with less than 200 computers.
- 2 It is very important to note that NetBIOS can use many protocols for transport. The Microsoft operating systems require NetBIOS naming to function, but they can use IPX/SPX or TCP/IP.
- 3 Discuss the architecture of the Microsoft protocol suite and how it maps to the OSI model.
- 4 Briefly discuss each of the protocols in the Microsoft suite.

NWLink (IPX/SPX)

- 1 NWLink (IPX/SPX) and its related protocols should actually be listed in their own section. This is a misprint in the text.
- 2 Note that NWLink is Microsoft's implementation of IPX/SPX which is used in Novell NetWare networks.
- 3 Discuss the architecture of the NWLink protocol suite and its relation to the OSI model.
- 4 Briefly discuss each of the protocols in the NWLink protocol suite. Be sure to note that NWLink is often the preferred protocol for large Microsoft networks because addressing is automatic, unlike TCP/IP, and it is a routable protocol.

Transmission Control Protocol/Internet Protocol (TCP/IP)

- 1 Discuss the history of TCP/IP and its role in networking. TCP/IP is the most commonly used protocol suite because of its cross-platform compatibility and its use in today's Internet.
- 2 Discuss the architecture of the TCP/IP suite and its relation to the OSI model.
- 3 Note that, more than any other protocol suite, the TCP/IP suite is made up of small, specialized protocols. For example, in the NWLink suite, many functions are handled by IPX. However, in the TCP/IP suite, the FTP protocol is responsible for file manipulation, the SMTP protocol is responsible for e-mail transfer, the RIP protocol is used to distribute routing information, etc.
- 4 Briefly discuss each of the protocols listed. Note that there are many, many more protocols in the TCP/IP suite. For more detailed information on TCP/IP, we recommend the *TCP/IP Illustrated* series of books from Addison Wesley.

IP Addressing

- 1 Note that, unlike NetBEUI and NWLink, IP addresses are assigned by the user or administrator. These addresses are 32 bits long and are written in dotted-decimal format with each byte separated from the next by a period (192.156.118.1). It is very important the students understand the IP addressing system. Microsoft has a completely separate class and test dedicated to TCP/IP, but the students here must understand the basics.
- 2 Note that each byte, also called an octet, is a decimal notation of a binary number. For example, an octet in which the bits are 11011011 is written as 219 (128+64+16+8+2+1). Remember that when transmitting over a network medium, everything that is sent is binary, either a 1 or a 0. Thus, the IP address is actually 32 1s or 0s. However, it's much easier for people to understand 192.156.118.1 than 1100000010011100111011000000001.
- 3 Note that the decimal numbers 0 (00000000) and 255 (11111111) are reserved for broadcasts and special packets. Hosts on a network cannot use these numbers in their address.

- 4 Discuss the class system for defining which bits of the address denote the host and which bits denote the network the host is on. This information is used to determine whether the destination of a packet is on the local network or a remote network.
- 5 Note that any address beginning with 127, such as 127.115.1.10, is considered the loopback address. If a packet contains this information in the destination address section, the packet is not placed on the network. This is very useful when troubleshooting TCP/IP problems. If the user PINGS the loopback address and receives no response, TCP/IP is not properly loaded or the NIC has failed.
- 6 Discuss the private addresses that are available for computer networks not connecting to the Internet. Note that if packets with these addresses are placed on the Internet, they are immediately dropped.
- 7 Discuss CIDR (pronounced cider). This method for defining which portion of the address is the host and which is the network is very detailed. It is important for the students to know that it exists and that it is the method used today to make this distinction.
- 8 Note that the subnet mask is used to determine which part of the address is the host and which part is the network. The following examples will help illustrate its function. Ones in the binary section denote network ID, while zeros denote host ID.

```

IP address:      202.100.99.230
Subnet Mask:    255.255.255.0 (Class C)
Binary Address: 11001010 01100100 01100011 11100110
Binary Mask:    11111111 11111111 11111111 00000000
Binary Network ID: 11001010 01100100 01100011
Binary Host ID:                               11100110
Decimal Network ID: 202.100.99
Decimal Host ID:  230

```

```

IP address:      152.98.212.156
Subnet Mask:    /26 (CIDR)
Binary Address: 10011000 01100010 11010100 10011100
Binary Mask:    11111111 11111111 11111111 11000000
Binary Network ID: 10011000 01100010 11010100 10
Binary Host ID:                               011100
Decimal Network ID: 152.98.212.128
Decimal Host ID:  28

```

- 10 Note that for computers on one network segment to communicate with each other using TCP/IP, they must have the same subnet mask.
- 11 Note that the DHCP protocol can be used to automatically configure computer's TCP/IP information including address, subnet mask, and default gateway.

Other Protocols

- 1 Briefly discuss AppleTalk, XNS, DECNet, and X.25. Note that XNS is the basis for IPX/SPX and, consequently, NWLink. These protocols are still used in networking today, but are not mentioned in the Microsoft test.

Putting Data on the Cable: Channel Access Methods

Function of Access Methods

- 1 Note that channel access methods are used to ensure data that is sent reaches its destination. These rules are used to prevent or minimize collisions which destroy data and slow down communication.

Major Access Methods

- 1 Note that early networks used contention access methods. Whenever a computer had data to send, it sent it. However, it quickly became evident that this would not work for large networks.
- 2 Discuss CSMA/CD's method for minimizing collisions. When a computer has data to send, it listens to the network to see if any other computer is sending data. If not, it sends its data. If so, it waits a random amount of time and checks again. This is called collision detection. CSMA/CD is one of the most popular channel access methods, especially for LANs.
- 3 Discuss CSMA/CA's method for minimizing collisions. When a computer has data to send, it sends an "intent to transmit" signal. Then, all the other computers on the network know that they cannot send data immediately. This is called collision avoidance. Only AppleTalk uses CSMA/CA.
- 4 Discuss the token-passing channel access method. Collisions are non-existent on token-passing networks because only the computer with the token, a special packet used to manage network communication, is able to transmit data. Token-passing networks also guarantee that every computer on the network will have the opportunity to send data. For this reason, they expand easily and are well-suited to time-sensitive environments.

- 5 Discuss the demand-priority channel access method. This method is only used by 100VG-AnyLAN networks, which are discussed in detail in Chapter 7. Intelligent hubs control access to the network in demand-priority networks. When a computer has data to send, it sends a demand signal to the hub. The hub then sends an acknowledgment that the computer can begin sending data. One feature of this access method is that priority levels can be assigned to particular computers, such as servers, to allow them more time on the network; hence, demand-priority.
- 6 Discuss the polling channel access method. This method has its roots in mainframe computing and is seldom used today. A central device polls the network allowing the network devices to communicate only when polled.

Choosing an Access Method

- 1 Outline the advantages and disadvantages of each of the access methods. This information is included on the Microsoft test, but only briefly. Be certain to note that token-passing networks guarantee access to all computers and scale better than contention-based networks.

Additional Case Projects

Case A

You have been asked to design a network for a small advertising firm. They are currently running a mix of Windows 95 and Macintosh computers, and are interested in installing a Windows NT Server. Except for the price of the server, they would like to keep costs low. Describe the channel access method and protocols which could be used in this environment.

Solution

In this situation, the best solution is to install an Ethernet network, which uses CSMA/CD. If the Macintosh computers are new, they will have a built-in EtherTalk port; otherwise, an external EtherTalk adapter will need to be added. The Windows 95 machines will all need Ethernet cards. When the server is configured to communicate with the Macintosh computers, it will use the AppleTalk protocol suite, whereas on the Windows 95 side, any protocol could be used. Because of the small number of machines, NetBEUI is the best solution.

Case B

Your network includes three subnets connected through a router. It is necessary for you to use TCP/IP for connectivity to a UNIX system, but it has not yet been installed on the computers. Your network will not be connecting to the Internet. Describe an IP addressing system which will provide your computers the connectivity they need.

Solution

Because the computers do not need access to the Internet, any of the private addresses could be used. The most likely candidate would be the 192.168 series. This will provide support for up to 256 subnets without having to subnet an existing address. For example, segments A, B, and C may have addresses of 192.168.100.0, 192.168.150.0, and 192.168.200.0, respectively. This will allow room for growth and would provide the easiest implementation.

Solutions

Answers to Chapter Review Questions

Question	Answer	Page
1	False	175
2	a. packet, c. frame, d. datagram	160, 163
3	c. defines which part of the address specifies the network and which part specifies the host ID.	174
4	b. Data Link, d. Physical, e. Network	165
5	b. 172.19.243.254	174
6	Transport	164
7	Token passing	180
8	False	167-168
9	a. works well in high-traffic environments, d. allows certain computers to be assigned a higher priority than others	183
10	e. ARP	171
11	a. IPX, b. UDP	169, 172
12	b. equal access to the medium for all computers on the network, d. allows for priority assignment	182
13	Token passing	180
14	b. error-checking information	161
15	a. NCP	170
16	c. have the same subnet mask	174
17	c. demand priority	181
18	False	163
19	d. different frame types	169
20	e. DHCP	175

Hands-on Projects Discussion

Each of these projects is geared toward familiarizing the students with the Network applet in the Control Panel. As discussed, this applet is used to configure all functions of networking on a Windows NT or Windows 95 system, although the applets are slightly different for each OS.

Project 6-1

The goal of this project is to ensure you are familiar with the settings one of the most prevalent protocol suites in use today. It is assumed that you will be working on a Windows NT 4.0 system, but similar settings are available for Windows 95. It is especially important to know how IP addresses are assigned (via DHCP or manually), and what settings are available.

Project 6-2

As discussed in the introduction to the Hands-on section, the DLC protocol is used to print to Hewlett-Packard printers directly connected to the network. However, the same principals used in this exercise can be applied to install any protocol on a Windows NT system.

Project 6-3

Again, although this exercise deals specifically with removing the DLC protocol, these steps are used to remove any protocols from the system.

Case Projects Discussion

Case 1

Although the company is small at the present time, the expansion plans make this network design decision crucial. If there were no plans for expansion, the best option might be NetBEUI and Ethernet. However, with plans to at least double the size of the network in the near future, the best solution for this situation is IPX/SPX over Token Ring.

Although NetBEUI works well in small environment, remember that, because it is not routable and utilizes broadcasts extensively, it is not a good option for an expanding network. Because of this, IPX/SPX is by far the best choice for this network. IPX/SPX is supported by Windows NT, is routable and handles large networks fairly well, and does not have the configuration headaches of TCP/IP.

If cost had been listed as an issue in making a decision, Ethernet may be considered again. However, because it was not mentioned, it can be assumed that the marginal difference in cost is acceptable to achieve a network that operates smoothly with twice as many computers. Remember that Ethernet works well with few computers, but slowly degrades as computers are added to the network. Token-ring, however, is able to guarantee access to the network for each computer and scales well to large networks.

Case 2

This is the fun one! No money limitations! To design this dream of a network, the best and brightest should be installed. Demand priority channel access is the best way to ensure that all traffic gets where its going in a timely manner. TCP/IP is a necessity because of the UNIX systems, but should be considered as the protocol regardless.

Chapter 7: Network Architectures

Objectives

After reading the chapter and completing the exercises, the students should be able to:

- Understand the different major network architectures, including Ethernet, Token Ring, ARCNet, AppleTalk, and FDDI
- Understand the standards governing those architectures
- Understand the limitations, advantages, and disadvantages of each standard

Teaching Tips

Ethernet

Overview

- 1 Discuss the research at the ALOHA network project at the University of Hawaii and how this research led Xerox at the PARC to develop an early version of Ethernet. (3 Mbps among 100 computers over 1 km)
- 2 Discuss the teaming of Digital Equipment Corp., Intel, and Xerox (DIX) in further developing the Ethernet standard (10Mbps).
- 3 Describe how the DIX standard led to the IEEE 802.3 specification in 1990.
- 4 Describe how the address is “burned in” to an Ethernet card when it is produced, ensuring that all cards have universally unique addresses.

The 10Mbps IEEE Standards

- 1 Define the four basic 10Mbps Ethernet standards:
 - 10Base5
 - 10Base2
 - 10BaseT
 - 10BaseF

- 2 Describe the naming convention used for IEEE standards. The name is split into three parts:
 - Transmission speed (generally 10 or 100)
 - Transmission type (baseband or broadband)
 - Distance (in hundreds of meters) or Media type (twisted-pair or fiber-optic)

For example: 10Base2 = 10Mbps, baseband transmission, 200 meters (actually 185, but close enough for standards work). 10BaseF = 10Mbps, baseband transmission, fiber-optic cable.

10Base5

- 1 Discuss the layout of a 10Base5 network: Thicknet backbone is pierced by vampire taps which connect the backbone to the transceiver. The transceiver is connected to an AUI or DIX connector on the computer via a drop cable.
- 2 Discuss the strict distance limitations of 10Base5:
 - Maximum backbone segment length = 500 meters
 - Transceivers must be more than 2.5 meters apart.
 - Drop cable from computer to transceiver must be less than 50 meters. (Drop cable is not figured into total network length.)
- 3 Discuss the 5-4-3 rule for coaxial networks (both 10Base5 and 10Base2):
 - A network can have **five** backbone segments connected by **four** repeaters, but only **three** segments can be populated.

10Base2

- 1 Discuss the differences between 10Base5 and 10Base2: Thinnet instead of Thicknet, 185 meters instead of 500 meters.
- 2 Describe the terminators, T-connectors, and barrel connectors used with Thinnet.
- 3 Note that, because 10Base2 uses coaxial cable, it is subject to the 5-4-3 rule.

10BaseT

- 1 Along with the cabling which can be used in 10BaseT, discuss the topology of the network: 10BaseT is wired as a star, but operates as a bus. Because 10BaseT uses active hubs, the 5-4-3 rule does not apply.
- 2 Briefly discuss the fact that 10BaseT supports Category 3, 4, or 5 UTP, but most new installations will use Category 5 to support the upgrade to 100Mbps Ethernet.
- 3 The biggest limitation to 10BaseT is distance (100 meters from hub to end-node). Discuss this limitation and how it will affect network installations.

10BaseF

- 1 Discuss the three implementations of 10BaseF:
 - 10BaseFL—Used to link computers in a LAN environment (fiber to the desktop)
 - 10BaseFP—Used to link computers via passive hubs
 - 10BaseFB—Uses fiber-optic cable as a backbone between hubs
- 2 Discuss the fact that because of its cost and difficult installation, 10BaseF is generally limited to interconnections between hubs.

The 100Mbps IEEE Standards

Overview

- 1 Discuss that there are two 100Mbps standards: 100VG-AnyLAN, and 100BaseT. These high-speed networks are very well-suited for video, CAD/CAM, and imaging.

100VG-AnyLAN

- 1 Although discussed with the Ethernet specifications, 100VG-AnyLAN encompasses both Ethernet and Token Ring technologies; hence the term AnyLAN.
- 2 Discuss the fact that AnyLAN is currently still in development and is the only architecture to use the demand priority channel access method discussed in Chapter 6.
- 3 Discuss the performance advantages gained by having intelligent hubs control network communication, rather than each computer handling the process for itself.
- 4 Compare the cable requirements for AnyLAN with 10BaseT. Both support Category 3 UTP, but if Category 5 is used with an AnyLAN installation, the maximum cable length is increased to 150 meters. 100VG-AnyLAN is also able to use fiber-optic cable.

100BaseT (Fast Ethernet)

- 1 Describe 100BaseT as an extension of the 802.3 specification which raises transmission speeds to 100Mbps.
- 2 Discuss the three implementations of Fast Ethernet and their cabling specifications:
 - 100BaseT4—Uses all four pairs of Category 3, 4, or 5 UTP
 - 100BaseTX—Uses two pairs of Category 5 UTP
 - 100BaseFX—Uses two-strand fiber-optic cables.

Ethernet Frame Types

- 1 Describe the Ethernet frame and discuss how the frame type varies from specification to specification.
- 2 Discuss the four Ethernet frame types and which protocols they are each generally used for:
 - Ethernet 802.3: IPX/SPX on Novell NetWare 2.x and 3.x networks
 - Ethernet 802.2: IPX/SPX on Novell NetWare 3.12 and 4.x networks
 - Ethernet SNAP: EtherTalk and mainframe networks
 - Ethernet II: TCP/IP
- 3 Compare all Ethernet frame types, particularly 802.2 and 802.3. Emphasize that 802.3 is not in compliance with the IEEE specification; 802.2 is.

Segmentation

- 1 Discuss the role of segmentation in an Ethernet network. Emphasize that through network segmentation, throughput is increased.

Token Ring

Overview

- 1 Discuss the origin of Token Ring at IBM and the eventual IEEE 802.5 standard.

How Token Ring Works

- 1 Discuss the token-passing method employed by Token Ring networks. A computer receives the token from its NAUN and passes it to its NADN. If the token is not in use and the computer has data to send, it attaches its data to the token. The receiving computer toggles two bits in the data packet and sends it back to the sending computer to verify receipt.
- 2 Be sure to make it clear that collisions do not occur on a Token Ring network because only the computer with the token is able to send data. This feature also ensures that all computers are granted equal access to the network, which means that Token Ring networks gracefully increase in size.

Beaconing

- 1 Describe the beaconing process used in Token Ring networks to identify network failures. Be sure to emphasize that the first computer powered on is the active monitor and is responsible for managing the beaconing process.

Hardware Components

- 1 Discuss the role of the MAU and SMAU in the Token Ring network. IBM's implementation of Token Ring is by far the most popular, but varies slightly from the IEEE standard. IBM hardware is most often associated with Token Ring.
- 2 Stress that, to ensure ring continuity, the RO port on one MAU must be connected to the RI port on the next MAU. In the IBM implementation, 33 hubs can be connected this way.

Cabling in a Token Ring Environment

- 1 Discuss the fact that Token Ring cabling is based on the American Wire Gauge (AWG) standard.

AppleTalk and ARCNet

The AppleTalk Environment

- 1 Discuss the distinction between AppleTalk and LocalTalk. AppleTalk refers to the architecture while LocalTalk refers to the cabling system.
- 2 Discuss the dynamic addressing scheme used by AppleTalk. When a computer is turned on, it broadcasts a request to use a particular address. If the address is already in use, it picks another number at random and broadcasts a request to use that address.
- 3 Compare AppleTalk Phase 1 with AppleTalk Phase 2. Phase 2 introduced EtherTalk and TokenTalk which allow AppleTalk protocols to operate over Ethernet and Token Ring networks.

LocalTalk

- 1 Discuss the layout of the AppleTalk architecture and how it is dictated by the way the connectors are constructed. This creates a tree-like look, while actually operating as a bus.
- 2 Describe in detail the CSMA/CA method of channel access used in the LocalTalk environment.

EtherTalk and TokenTalk

- 1 Discuss the additional requirements for EtherTalk or TokenTalk, as well as the increased performance. Each of these implementations require a new NIC be added to the workstation. However, performance is increased from 230.4 Kbps to 10Mbps for Ethernet, 4 Mbps or 16 Mbps for Token Ring.

The ARCNet Environment

- 1 Discuss the operation of ARCNet vs. the cabling of ARCNet. It operates in a virtual ring, but can be wired as a bus, star, or combination.
- 2 Describe the process for addressing ARCNet NICs. Unlike Ethernet or Token Ring, the address (Station ID or SID) for the NIC is set using jumpers on the NIC itself.
- 3 Note that the token is passed from computer to computer according to the SID. The location of the computer in the network, then, can have an effect on communication.
- 4 Discuss the Next station Identifier (NID) and its role in ARCNet communication. The NID is determined through a broadcast method in which the computer sends a message requesting a response from the computer with a SID one greater than its own. If no computer answers, it increases the SID by one. It repeats this process until a computer responds to the broadcast.

ARCNet Hubs

- 1 Discuss the roles of active and passive hubs in an ARCNet network. Note that passive hubs can only be connected to active hubs or computers, whereas active hubs can be connected to other active hubs as well as passive hubs or computers.
- 2 Also note the distance limitations in regards to active and passive hubs:
 - Active hubs connected to active hubs can be no more than 600 meters (2,000 feet) apart.
 - Passive hubs can be no more than 30 meters (100 feet) from an active hub.

ARCNet Cabling

- 1 Note that, when using coaxial cable in an ARCNet star-topology network, the BNC connector is connected directly to the hub without using a BNC T-connector.

FDDI

- 1 Discuss the fact that, unlike Token Ring, FDDI is wired in a physical ring. Generally, there is no central connection point, but concentrators sometimes provide this functionality.
- 2 Discuss the token-passing process employed by FDDI. Multiple tokens can be on the network at one time and a computer does not have to wait for confirmation before passing the token on to the next computer.
- 3 Describe the role of the dual counter-rotating rings in FDDI. The primary ring is always used to send data. The secondary ring takes over only when there is a failure in the primary ring.
- 4 Describe the differences between Single Attachment Stations and Dual Attachment Stations and when each would be used.

Other Networking Alternatives

- 1 Briefly discuss the broadband, broadcast, and gigabit technologies. Although their implementation is limited, they are very useful and, especially in the case of gigabit technologies, exciting technological developments.

Additional Case Projects

Case A

Your boss has decided to network his house. He wants everything, lights, television, etc., to be controlled by a server in the basement. He has asked you to wire his house and make sure everything works. Knowing your boss, you anticipate that he will want to keep costs down, but have a high-speed network. Describe the networking solution you will put in place.

Solution

Considering the boss's attitudes toward speed and cost, installing a 100BaseTX network with Category 5 UTP is best. This cable can be used for all connections in the house, including phone, network, ISDN, etc., and will support very high transmission speed.

Case B

You have been hired by a state agency to provide connectivity between their existing Token Ring network and a new database server cluster. The cluster will need a network with transmission speeds of 100Mbps. The cluster's network must support prioritization and should be redundant. This particular agency has very deep pockets and there is no concern for cost. What network architecture, or combination of architectures best suits this installation?

Solution

This is another case where 100VG-AnyLAN is the perfect solution. The cluster can have 100Mbps transmission and prioritization, as well as easily support Token Ring packets.

Solutions

Answers to Chapter Review Questions

Question	Answer	Page
1	a. 100BaseT4, b. 100BaseTX, c. 100BaseFX	204
2	d. Token Passing	215
3	b. two	219
4	b. Ethernet_II	207
5	The active monitor manages the beaconing process in a token ring environment.	209
6	3	196
7	a. jumpers	216
8	230.4 Kbps	214
9	Error checking	206
10	c. concentrator	219
11	a. active hubs, b. Computers	218
12	c. American Wire Gauge (AWG)	211
13	a. one	210
14	802.2	206
15	100VG-AnyLAN	202
16	According to node number, which is assigned manually.	216
17	b. 10Base5	195
18	c. 2.5 Mbps	215
19	a. Type 1	211
20	c. Token Ring, d. FDDI	210, 219
21	Primary	220
22	A vampire tab is used to attach a transceiver to a Thicknet cable by piercing the shielding.	195
23	a. MAU, b. MSAU	210
24	FDDI is very fast, reliable, covers long distances and is highly secure.	221
25	c. CSMA/CA	214

Case Projects Discussion

Case 1

This Case project should include an extensive outline of the student's plans to implement this network, starting with connecting the buildings. The distance and speed limitations dictate that fiber-optic cable be used. Generally, this leans toward FDDI. 100BaseFX is a possibility, but would be better suited for the backbone in each building. So, the best option is to put a router on the first floor of each building, with an FDDI connection to the other buildings, and a 100BaseFX connection for each of the floors.

On each floor of each building, place an Ethernet switch which has a 100BaseFX port and can handle either 10Mbps or 100Mbps. The 10/100 option allows you to make the transition from 10Mbps easily. A decision needs to be made on the 100Mbps standard which will be used on the desktop. 100BaseTX will require rewiring Buildings 1 and 3, whereas 100BaseT4 can use the CAT 3 already installed. Building 2 can be wired with CAT 5 and still use the T4 standard for wiring the RJ-45 connectors.

The second floor of Building 3 is a special consideration. It could use 100BaseT4 like the rest of the building, but, this would provide no fault tolerance. The best option here, again, is a separate FDDI ring for the servers. It means that the router for building three should reside on the second floor rather than the first, which affects the cabling of the building, but all decisions made so far will support this change.

The drawing included in Figure 7-18 is a good basis, but should be expanded to include cable segment lengths and media types.

Case 2

Although it is not mentioned, you have to assume that the Macintosh network is running LocalTalk in a peer-to-peer environment. To connect to the PC network, a shift must be made to EtherTalk or TokenTalk, depending on the existing PC network. In addition, Service for Macintosh should be loaded on a Windows NT Server on the PC network to allow the PCs and the Macs to share files and printers. By making the switch to EtherTalk, for example, the cabling will need to be replaced, but the speed will be increased to 10Mbps.

Case 3

In actuality, this configuration is very similar to Case 1. The biggest difference is that there is no call for fault tolerance between the buildings. In this case, 100BaseFX is sufficient. It is still a good idea to use routers in each building, to avoid breaking the 5-4-3 rule (it only applies to hubs, not routers). Again, because CAT 3 is already installed, it would be a good idea to use the 100BaseT4 standard rather than TX, which would require new cabling.

Case 4

For this type of environment, ease of installation and cost are key, not speed. The recommended solution here is to utilize 10Base2 (Thinnet) to connect all the computers in the classroom. In addition, it would be a good idea to use notebook computers with PCMCIA network cards, rather than large, desktop systems. Because of its size, any protocol could be used and, depending on the class, NetBEUI may be preferable.

Chapter 8: Simple Network Operations

Objectives

After reading the chapter and completing the exercises, the students should be able to:

- Explain how network operating systems work
- Understand the various networking software components
- Install a network operating system
- Define and implement network services
- Install and configure network applications

Teaching Tips

Network Operating Systems

Network Operating System Overview

- 1 Note that in the early days of networking, the software used to communicate over the network was added on to the original operating system. True network operating systems, i.e., those designed specifically for networking, have only come into being very recently. MS LAN Manager and NetWare Lite are examples of this type of networking system.
- 2 Also note, purely for curiosity's sake, that it is accepted in the industry to refer to a network operating system either as an N.O.S., or as a NOS (nôs, näs).

Demands of a NOS

- 1 Describe multitasking and its role in network computing. To get the most out of a set of computer hardware, many operating systems multitask, that is run numerous processes at the same time.
- 2 Define time slicing. Time slicing occurs when the computing cycles of a CPU are divided between tasks. Because of the speed of the CPU, it seems as though it is working on multiple processes at once, when in reality each process is started, processed for a certain number of cycles, then stopped while the CPU moves on to the next process.

- 3 Describe the two types of multitasking, preemptive and cooperative. With preemptive multitasking, the operating system controls which process gets CPU access and for how long. However, in cooperative multitasking, each process has control of the CPU for as long as it needs it. While a cooperative multitasking process has control of the CPU, no other process is given access.
- 4 Note that nearly all operating systems use preemptive multitasking, especially network operating systems.

Software Components of Networking

Client Network Software

- 1 Recall that client computers in a network request services from servers and, in special cases from each other.
- 2 Note that the function of the redirector is to accept requests from applications and determine whether network access is needed. If so, it sends the request over the network to the server or resource host. However, if the request is for local resources, the redirector hands the request off to the CPU for processing.
- 3 Note that this function is performed by the redirector in Microsoft networks. However, other types of operating systems call this process different things. In Novell networks, it is the requestor that performs these functions, in other operating systems, it is the network shell.
- 4 Note that one of the original functions of the redirector and designator was to “fake out” the underlying operating system. For example, MS-DOS expects all drive letters to be A: through Z: and printers to be on LPT1 or LPT2. The redirector is able to assign “normal” drive letters to network resources so that MS-DOS thinks it is part of the local system. The same applies to printers on the network. The redirector can direct output intended for LPT1 to a printer on the network. This does not apply as dramatically to network-aware operating systems like Windows 95, but the principal is the same.
- 5 Ensure that the students understand the Universal Naming Convention. This convention permeates modern networking, especially Microsoft networking, and the students must understand how it works.

Server Network Software

- 1 Note that, as discussed in previous chapters, the role of a server is to share resources and control access to those resources. This includes management of resources, management of users and groups, logon authentication, and often fault tolerance systems to protect the data.

Client and Server

- 1 Recall that in some environments, computers are able to act as both client and server. Peer networks allow users to access resources on other computers and share the resources on their computer. Windows NT Workstation is a good example of this type of operating system.

Installing a Network Operating System

Installation Preparation

- 1 Briefly discuss each of the considerations listed when installing a network operating system. The size and topology of the network will not be addressed as the operating system is installed, but should be considered when choosing a NOS and in determining hardware requirements.
- 2 Discuss how a computer's job requirements will affect the installation. The obvious question is: Will the computer be a client or a server? One of the key points when dealing with a Windows NT Server installation is the role domain management role the server will play. Will the server be a primary domain controller, backup domain controller, member server, or standalone server? This question is especially important because a server's domain role cannot be changed once the operating system is installed. To change from a member server to a domain controller, the operating system must be reinstalled.
- 3 Note that it is very important to have a network naming convention established before proceeding with the operating system installation. This naming convention is often governed by the type of operating system installed. For example, client computers in a Novell NetWare environment generally do not have names and the server names can be up to 47 characters. However, in a Windows networking environment, all computers names, clients and servers alike, are limited to 15 characters, in accordance with NetBIOS standards.
- 4 Note that the network naming convention applies not only to computers, but to users, groups, and shared network devices such as printers.
- 5 Describe each of the configurations for storage devices. Note that a single-boot, single-partition installation is the most secure, but is not always desirable. With multiple partitions, the user data can easily be separated from the operating system files.
- 6 Recall from Chapter 4 that the configuration of the network adapter is very important to computer performance. There may be a time during the NOS installation that IRQ, I/O port, and memory address settings for each NIC are required.
- 7 Discuss each protocol and protocol selection for the network. This choice should be made long before the server's operating system is installed. However, it is usually very easy to add or remove protocols from network computers.
- 8 Note that, especially in the case of Windows NT Server, it is important to use hardware that is compatible with the operating system. Microsoft's Hardware Compatibility List (HCL) is used to determine whether hardware is supported by Windows NT. Note that if the hardware installed in the server is not on the HCL, Microsoft will not provide support for the installation.

Installing Microsoft Windows NT Server 4.0

- 1 Discuss each of the types of installation. The decision whether to baseline the system or use the existing OS could very well be based on whether the CD-ROM in the system is supported by Windows NT. If the CD-ROM is not supported by NT, the existing operating system will have to be used.
- 2 It is important to note that, when installing Windows NT 4.0 from an existing NT operating system (such as

NT Workstation 3.51), WINNT32.EXE can be used. However, this only works in the 32-bit environment of Windows NT and cannot be used when upgrading from other operating systems.

- 3 Note that there are three sections to the Windows NT Server 4.0 installation: text-based, GUI, and networking. During the text-based portion of the installation, hard drives are configured and formatted, the license is confirmed, and the system directory name is specified. During the GUI phase, the computer and domain names are defined, the server type is selected, the working environment (desktop settings, etc.) is configured, and the Administrator account is assigned a password. During the networking portion, NICs are defined, drivers and protocols are installed and configured, and bindings are reviewed.
- 4 Note that the installation is not complete until the computer is rebooted and the Administrator logs on successfully.

Installing Novell NetWare 4.11/IntranetWare

- 1 Discuss the choices of where to install the NOS from: over the network, CD-ROM, and floppy.
- 2 Note that INSTALL.NLM is the module which drives the NetWare load process. Because of the way NetWare operates, the entire installation is text-based, but the steps are similar to Windows NT. The server is assigned a name, the volumes are defined and formatted, and the NICs are configured.
- 3 Note that, unlike Windows NT, no login is required to complete the NetWare installation. Once the server reboots successfully, the installation process is complete.

Network Services

- 1 Describe network services. These services provide functionality on a network, including, but not limited to, file and printer sharing, Internet services, and gateway services.

Installing, Removing, and Configuring Network Services

- 1 Describe the process of adding, removing, and configuring network services in Windows NT. As with all things related to the network, services are managed through the Network applet of the Control Panel. There are some cases, such as Microsoft's Internet Information Server and Remote Access Service, which are managed through a separate application which is installed when the service is installed.

Network Bindings

- 1 Describe the process of binding network components. This process is centered around binding protocols to NIC device drivers. The order in which the protocols are bound to the card has an effect on how the protocols perform. The most frequently used protocol should be bound first.

Network Printing

- 1 Describe the role of network printing. This allows multiple users to share a printer. By doing this, a company is able to purchase fewer printers, which saves money. Note that this is one of the most important functions of computer networking.
- 2 Discuss the steps necessary to install a network printer. Also discuss the steps which must be taken on the client side to utilize the network printer.
- 3 Briefly discuss printer management. Beyond just changing the paper in the printer, printer management includes controlling printer access, monitoring the print queues, and keeping track of printer drivers.

Network Directory Shares

- 1 Note that sharing files and directories is the second major piece of networking.
- 2 Note the three ways a network share can be accessed: mapping a driver letter, using the UNC, selecting the share from a list of available shares (such as when using the Network Neighborhood to browse the network).

Network Applications

- 1 Note that the difference between network applications and regular desktop applications is that network applications were designed for multiple simultaneous users on numerous computers connected over a network. Discuss the benefits of using network applications. Note specifically the version control problems for both documents and programs that are avoided.
- 2 Discuss the three types of network applications: centralized, file-system sharing, and client/server.

E-Mail or Messaging

- 1 Briefly discuss e-mail messaging programs. This is by far the most recognized network application.
- 2 Briefly discuss the e-mail protocols which are used for communication over the network.

Scheduling or Calendaring

- 1 Briefly discuss scheduling and calendaring programs. These programs simplify meeting coordination, task lists, and address books. Note that to work effectively, most scheduling programs integrate into e-mail packages. This way, when a meeting reminder is sent, it is sent as an e-mail message.

Groupware

- 1 Briefly discuss groupware applications. These applications are relatively new and allow many users to work on a single document or project.

Additional Case Projects

Case A

Suppose the following situation exists: Jaime is planning a network installation for his medium-sized company. There are 43 computers, three servers, and 10 printers which will be installed. All computers will be installed in four divisions of the company: Administration (#1420), Accounting (#1982), Development (#0300), and Projects (#2256). Jaime is installing Windows NT servers and Windows 95 workstations.

Required result: The naming convention must provide a unique name for each user and device on the network.

Optional desired results: The naming convention should be easy to understand and administer.

Proposed solution: Usernames will consist of the first four letters of first name of the user, followed by their department number (DAVI1982). Computer names will follow the same naming convention, first four letters of the primary user's first name followed by their department number. Server names will be SERVER1, SERVER2, and SERVER3. Printer names consist of the type of printer (HPLJ), the department number (0300), and the printer number (1, 2, etc.).

Which of the following does the proposed solution provide:

- a The proposed solution provides both the required result and the optional result.
- b The proposed solution provides only the required result.
- c The proposed solution does not provide the required result.

Solution

The answer here is b. The proposed solution does provide a unique name for each user and device on the network. However, it is not easy to understand or administer.

Case B

You have just purchased a new computer with no operating system installed. You would like to install Windows NT Server, Windows NT Workstation, and Windows 95. Describe the order in which you would perform the installation and why.

Solution

Windows 95 should be installed first because it will provide CD-ROM support for the other operating systems. Windows 95 can easily configure Plug and Play devices, at which point the user can write down the configuration for use in the Workstation and Server installations. It does not matter which operating system is installed next, though it is generally Workstation. Be sure to note that Server and Workstation must be installed in separate directories.

Solutions

Answers to Chapter Review Questions

Question	Answer	Page
1	True	232
2	b. Whether or not it servers as a domain controller or a member server.	237
3	a. Windows NT Workstation, b. Windows 95, d. Novell NetWare, e. Windows NT Server	232
4	b. single-partition, single NOS	238
5	b. the illusionary method of computer where multiple processes operate simultaneously by sharing the CPU.	233
6	True	239
7	False	233
8	a. IP address, c. subnet mask	239
9	All answers (a., b., c., d., e.)	232
10	a. not all hardware is supported by the high-performance requirements of a NOS	240
11	c. accessing network shares	234
12	a. CD-ROM based, b. over the network, c. floppy-based only	240, 242
13	d. to forward requests to local or remote resources hosts	234
14	d. It can provide access to a CD-ROM otherwise not supported by the NOS itself	240
15	a. requestor, c. designator	234
16	a. character-based	242
17	b. Error! Reference source not found.	235
18	c. network services	243
19	All answers (a., b., c., d.)	235
20	All answers (a., b., c., d., e.)	244
21	False	234-236
22	c. e-mail	248
23	a. responsibilities of the server, c. naming conventions, e. organization of storage devices	236-240
24	True	246
25	a. servers and clients, b. users, c. directory shares, e. printer shares	237-238

Hands-on Projects Discussion

Project 8-1

The intent of this project is to familiarize the user with the steps required to connect to a networked printer using Windows NT or Windows 95. From the client perspective, connecting to a previously shared printer is rather easy. These steps can be used to connect any number of printers. As discussed in the text, the printer can easily be removed from the system configuration.

Project 8-2

Similar to Project 8-1, this project highlights the steps necessary to map a drive letter to a networked share. Removing this mapping is also very simple. Remember that, in most cases, it is necessary for the computer to have a drive letter assigned to a resource before it can be accessed. This goes back to the fact that, historically, local drives were assigned letters (A:\, B:\, C:\, etc.) and most applications still require this kind of notation.

Case Projects Discussion

Case 1

In a networking environment, a server machine is no more likely to crash than any desktop computer. However, it is true that the crashing of a server is usually more severe than the failure of a workstation. But even this possible drawback, the benefits of a client/server system far outweigh the small chance of a server crash. Some of the benefits are:

- Centralized administration of network resources
- Centralized storage of important files for backup purposes
- A serious and reliable security scheme
- Shared or collaborative applications

In addition to these benefits, the hardware and software that are combined to create a server computer are specifically designed to be robust, reliable, and high performance. Manufacturers understand that a server is more important than a workstation and have taken steps to ensure that your server is the most reliable system within your network.

Case 2

Control over access is a function of a client/server system where a user account security scheme has been implemented. If an employee leaves the organization, no matter what access level they enjoyed previously, their user account can be simply and easily disabled, deleted, or just changed for the new user by an administrator. Disabling the account will preserve it for future security audits while preventing it from being used to gain access to the network. Deleting the account will remove the account from the system and obviously not allow the user account access to the network. Changing the account involves renaming and changing the password for another user, this allows another user to enjoy the security privileges and access settings without requiring the tedious recreation by a system administrator. This also prevents the old user from gaining access to the system because they would no longer know the username or password for the account.

Case 3

Improving the performance of a CPU can only be affected in a few ways:

- Adding additional physical RAM
- Adding L2 cache
- Reducing the number of services and applications running simultaneously

Of these actions, the adding additional RAM will most likely provide the desired results. If you are still experiencing problems, you may need to upgrade the CPU itself.

Chapter 9: Understanding Complex Networks

Objectives

After reading the chapter and completing the exercises, the students should be able to:

- Discuss interconnectivity issues in a multivendor environment
- Define the various options to implement a multivendor network environment
- Discuss the differences between centralized and client/server computing
- Define the client/server networking environment

Teaching Tips

Interconnectivity in Multivendor Environments

- 1 Discuss the interconnectivity problems that come with implementing complex networks. Seldom, if ever, are all desktop computers and servers made by the same hardware manufacturer or run the same brand of operating system. This poses a special set of problems that the major networking vendors have attempted to address.

Implementing Multivendor Solutions

- 1 Note that there are two methods which can be used to implement multivendor network environments, client-based and server-based. The solution chosen depends on the vendors involved.

Client-Based Solution

- 1 Discuss the client-based multivendor networking solution. By implementing multiple redirectors (or requestors), the client's NOS is able to determine to which network's resource the request should be sent.
- 2 The label for the Client for NetWare Networks in Figure 9-2 is incorrect. The component of the NetWare client operating system that performs the tasks of the Microsoft redirector is called the requestor.

Server-Based Solution

- 1 Discuss the server-based multivendor solution. Servers, such as Windows NT Server 4.0, can load services specifically designed for other vendor's client systems. For example, Services for Macintosh or File and Print Services for NetWare can be installed on a Windows NT server to provide connectivity to Macintosh and NetWare clients.

Vendor Options

- 1 Discuss the steps taken by Microsoft, Novell, and Apple to provide connectivity across all platforms.
- 2 Recap the role of the Microsoft redirector.
- 3 Discuss the Client Service for NetWare (CSNW) which allows Windows NT Workstation computers to attach to Novell NetWare servers. Also mention the Gateway Service (GSNW) for NetWare which provides similar connectivity to Windows NT Server computers.
- 4 Note that MS-DOS clients can easily connect to any of the major NOSs. In the case of MS-DOS client on a AppleTalk network, additional hardware is required.
- 5 Briefly discuss Novell's and Apple's connectivity solutions. Note that by installing the Service for Macintosh on a Windows NT Server, Apple clients are able to utilize the full services available on the server.

Centralized vs. Client/Server Computing

- 1 Discuss the evolution of computing from a centralized environment to a client/server environment.

Client/Server Environment

- 1 Discuss the roles of both clients and servers in a true client/server environment. Note especially the distributed processing involved in client/server networking. With client/server networks, some processing occurs on the server, and some on the client. A good example of this is an application server which runs a groupware product. The server manages the clients' requests for files and controls the groupware processing.
- 2 Note that a server which performs only shared file services is often not considered a client/server configuration. This is called a shared-file storage system.

Client/Server Model in a Database Environment

- 1 Note that a DBMS environment is the penultimate example of client/server processing. The client makes a request for data to the server. The server searches through the database to get the information requested and returns it to the client. The client, then, is able to perform calculations, sorting, and filtering on the data.
- 2 Note that in all client/server environments, the front-end is the client, and the back-end is the server. Briefly describe their specific roles in a DBMS environment.

Client/Server Architecture

- 1 Briefly discuss the single database server and distributed database architectures. When establishing these types of networking environments, the client must be properly configured to support the server structure. When distributed databases are installed, the servers often act as a single entity, so that client configuration may actually be the same as with a single-server network.

Advantages of Working in a Client/Server Environment

- 1 Briefly discuss the advantages of using a client/server model rather than a centralized computing model. The primary reason is distributed processing. This utilizes the superior computing power of the server for the most arduous tasks, but also uses the CPU on the client to perform minor calculations.

Additional Case Projects

Case A

You have been asked to design a network for a small advertising firm. They are currently running Macintosh and Windows 95 computers, and are interested in installing a Windows NT Server. Costs for this project must be kept to a minimum. Describe the configurations of all computers in this network.

Solution

The center of this configuration is the NT Server. By installing Services for Macintosh on the server, Macintosh users can share information with Windows 95 users. In addition, the Macintosh computers must be able to connect to the NT Server, which means installing EtherTalk or TokenTalk cards. In this case, because of the size of the network and cost considerations, EtherTalk is best. The Windows 95 computers will easily interface with the Windows NT Server, so no configuration changes are necessary.

Solutions

Answers to Chapter Review Questions

Question	Answer	Page
1	NWLink	265
2	a. Microsoft, b. Novell, d. Apple	264
3	Centralized Computing	266
4	a. client	263
5	Client	268
6	b. server	267
7	Server	268
8	False	267
9	Client/Server, Centralized	266
10	Centralized	267
11	Client Service for NetWare	265
12	MS-DOS, OS/2, and Windows NT	266
13	True	264
14	a. client	267
15	b. server	263
16	Front-end	268
17	Windows NT, Windows 95, and Windows for Workgroups	265
18	Services for NetWare Directory Services	265
19	SQL	268
20	b. client/server	267

Hands-on Projects Discussion

Project 9-1

As mentioned in the text, the Services for Macintosh can be added to a Windows NT Server to provide Macintosh computers access to Windows NT resources including file and print sharing. This project is intended to familiarize the user with the steps necessary to install Services for Macintosh and configure the Service once it has been installed. As with most network services, it is installed through the Network applet in the Control Panel.

Project 9-2

As mentioned in the text, the Client for NetWare Networks allows Windows 95 computers to easily access NetWare resources, including file and print sharing. This client service is also installed through the Network applet in the Control Panel.

Case Projects Discussion

Case 1

Perhaps the easiest way to make this transition is to do most of the work on the Windows NT Server machines. Because it was not mentioned in the Case outline, we have to assume that your company is running either NetBEUI or TCP/IP (IPX is generally only used in special situations). So, first and foremost, you have to install NWLink on one or both Windows NT Servers. This will allow the NetWare clients and servers to see your servers. Then, by loading the appropriate redirector, such as Client for Microsoft Networks in Windows 95, on the NetWare clients, those devices will be able to take full advantage of your NT network. But, how will the clients on your network access the information on the other side?

Again, the easiest way is to install Gateway Services for NetWare on one Windows NT Server. After establishing a GATEWAY user on the NetWare servers, the GSNW will be able to attach to the NetWare network and utilize its resources.

Case 2

Yet again, the best bet will be to install a Windows NT Server. Although protocols have not been discussed, NWLink is the minimum because of the NetWare clients in Engineering. It does not specify what type of clients (Windows for Workgroups or Windows 95), but the correct redirector will have to be loaded. By installing Service for Macintosh, you are ensured the Mac clients will have access. The Windows for Workgroups and Windows 95 clients in Accounting will only need a minor configuration change to attach to the Windows NT Server.

Chapter 10: Network Administration and Support

Objectives

After reading the chapter and completing the exercises, the students should be able to:

- Create, disable, and delete user accounts
- Configure group accounts to make them most effective
- Describe all aspects of network monitoring
- Create a network security plan
- Protect their servers from data loss

Teaching Tips

Managing Networked Accounts

- 1 Briefly describe the role of user and group accounts in network administration. Note that this chapter deals with the generalities of network administration and support, but focuses on the Windows NT Server 4.0 operating system.

Creating User Accounts

- 1 Note that two accounts are created by default when NT Server is installed: Administrator and Guest. It is a very good idea to rename or disable the Administrator account after the network is running because hackers use this account to gain access.
- 2 Note that before creating any accounts, a network administration plan should be in place which includes the naming convention for users and groups, the password policy for user accounts, a policy regarding logon hours and event auditing, and group account guidelines.
- 3 Discuss the different settings for user account passwords. Strictly speaking, all a user needs to logon to the network is a valid username. Of course, this is not very secure. By requiring a password, security is increased. Security is also increased by requiring passwords to be a certain length (at least six characters), requiring users to change their password regularly (every 30 to 60 days), and require users to use unique passwords. In addition, the password policy should state that passwords include mixed case characters and numbers. This virtually eliminates the possibility of a dictionary attack.
- 4 Note that to further prevent attack, the user's account should automatically be disabled if they fail to logon three times in a row.

- 5 Discuss the use for logon hours. By only allowing users access to the network during certain hours of the day, the network is more secure and regular processes, such as backups, can be run without concern for user intervention.
- 6 Discuss the role of event auditing. This process keeps track of both successful and unsuccessful logon attempts, object accesses, logoffs, and changes to security information. Note that the log that tracks these events can grow rather quickly. In a very secure network environment, this information is often sent directly to a Microsoft SQL Server system for storage in a database.
- 7 Briefly discuss setting users' rights on the network and the role of the local and global groups in Windows NT Server. A user's rights define which network resources they have access to and what they can do with those resources. It is often easier to create a group, assign specific rights to that group, and include users in the group than to assign rights to each user individually.
- 8 Briefly discuss the Windows NT automatic groups. It is important to remember that these groups exist and, although users cannot be added manually, they have certain rights which you may or may not want all users to have.

Managing Group Accounts

- 1 Discuss the role of local groups and global groups. In addition, discuss the reason local groups can include global groups, but not vice versa.
- 2 Describe trust relationships and how they provide cross-domain access. This is often a very confusing process. First, a domain must allow itself to be trusted, then a trust is established (either one-way or two-way). Note that this process must take place on both sides of the trust, even if the trust will ultimately be one-way.
- 3 Note that after the trust is established, users or groups must be added to provide access for the users of the other domain. Briefly discuss each of the methods for implementing these accounts.

Disabling and Deleting User Accounts

- 1 Briefly discuss disabling and deleting users accounts and when each should be done. This policy should be established when the network is setup and may be something like "In the event that a user leaves the company, their account will be disabled for 30 days to provide the administrator time to ensure all data and security settings are available for their replacement. After 30 days, the account will be deleted."

Renaming and Copying User Accounts

- 1 Note that it is often easier to rename or copy an existing account than to create a new one. This ensures that all settings are the same for the new user account.

Managing Network Performance

Data Reads and Writes

- 1 Discuss the effects of reads and writes, both successful and unsuccessful, on network performance. If the server refuses to accept large streams of raw data, it is an indication of memory problems in the server.

Queued Commands

- 1 Discuss how the number of queued commands affects a server's performance. If the number of queued commands is more than the number of NICs in the server, there is a bottleneck.

Collisions per Second

- 1 Recap what must happen when a collision occurs. Discuss how too many collisions effect network performance.
- 2 Also discuss how the number of collisions per second may indicate a bigger problem in the network, such as cable segment lengths that are too long.

Security Errors

- 1 Discuss how a large number security errors may indicate attempts to illegally access your network.

Server Sessions

- 1 Discuss server sessions and how they may be used to indicate an overloaded server.

Network Performance

- 1 Note that there are three tools provided with the Windows NT Server 4.0 operating system which can be used to monitor network performance: the Event Viewer, the Performance Monitor, and the Network Monitor.
- 2 Briefly discuss the Event Viewer and how it can be used to track events such as unsuccessful logon attempts. Note that for the Security log to track logon/logoff events, the filters must be enabled in User Manager for Domains.
- 3 Briefly discuss the Performance Monitor and its role in monitoring network and server performance. Note that the Chart view monitors events in real-time and displays the information in a graphical format.
- 4 Note that Performance Monitor uses large amounts of resources. For this reason, it is a very good idea to run Performance Monitor remotely.

- 5 Briefly discuss the Network Monitor and its ability to monitor network performance. Note that it is not installed automatically when the operating system is installed. It is added through the Network Neighborhood Services tab.
- 6 Note that, again, the Network Monitor utilizes a large number of resources and should be run remotely.
- 7 Note that the Network Monitor is able to capture data packets and track a conversation between computers. This information can be very helpful when diagnosing a network problem. For example, with Network Monitor capturing data going between two computers, the administrator might find that a response to a query is being sent, but after the allotted timeout period.
- 8 Note that for security reasons, the Network Monitor checks for other occurrences of Network Monitor and reports the name of the account logged on, what the monitor is doing, the adapter address, and the version number.

Total System Management

- 1 Discuss using Performance Monitor to check hard drive information. Note that to use Performance Monitor in this way, the DISKPERF command must be run from a command prompt.
- 2 Discuss the difference between soft page faults and hard page faults and how they are indicative of memory problems in a server. Be sure to note that hard page faults are the biggest concern.

Maintaining a Network History

- 1 Briefly discuss the use of a network history in troubleshooting and how to utilize the information obtained from the Performance Monitor and Event Viewer to create a network history document.
- 2 Note that it is very important to know what network performance looks like under normal conditions.

Managing Network Data Security

Planning for Network Security

- 1 Briefly discuss the considerations when deciding on a network security plan. It is important to mention that all situations are different and that the same security measures are not necessary in all instances.

Security Models

- 1 Briefly discuss physical and data security. Note that physical security may be as simple as installing the servers in a locked room and ensuring that only authorized personnel have access.

- 2 Note that the data security models roughly correspond to the network models, i.e., peer-to-peer networks use share-oriented security whereas server-based networks use user-oriented security. This should be considered in all phases of network planning. The level of security required has a large impact on the network operating system chosen.

Implementing Security

- 1 Briefly discuss setting up a security system and the user training that goes along with it. Note that the more a user understands why you have implemented a particular system, the less likely they are to cause problems. For example, if a user doesn't understand that their password has to be changed every 60 days, then, when they can't logon because their password has expired, they will become frustrated and come to the administrator. However, if the user does understand that the security plan requires them to change their password, when they receive the message from the server telling them its time, they will do so willingly.

Maintaining Security

- 1 Briefly discuss maintaining the security plan through periodic review and amendment of the original plan.

Avoiding Data Loss

- 1 Note that one of the key aspects of networking, and, indeed, one of the major selling points, is the ability to protect data. Aspiring network administrators are often able to convince their bosses that a network is in order by showing them that the chances of losing a document are greatly reduced when a network is installed.

Tape Backup

- 1 Briefly discuss the five types of backups and when to use each. Make special note of the difference between an incremental backup and a differential backup. Both of these methods can be used in a backup plan for daily backups, but, although incremental backups are faster later in the week, they are harder to use for recovery purposes.
- 2 Note that it is very important to create a backup schedule and stick to it. Make sure that everyone responsible for the backups knows what needs to happen and when. It is often best to assign this task to one person to ensure it is done the same way every day.
- 3 Note that a backup log is very important when it comes to disaster recovery. By keeping a log, an administrator can easily see which tapes contain the data he needs and so he will not waste time searching through tapes. Many new backup programs, such as ARCserve, perform this function automatically.
- 4 Discuss using test restorations to ensure the backups are running properly. It would be of no use to anyone if, when the hard drive in the server crashed, the data on the full backup could not be restored.

Uninterruptible Power Supply

- 1 Discuss how an uninterruptible power supply (UPS) can prevent data loss by ensuring the server has enough power to shutdown gracefully.
- 2 Note that a UPS is also able to condition the power coming from the wall outlet and provide surge protection.
- 3 Also note that many UPS systems provide connections for 10BaseT, RJ-45, or RJ-11 connections to prevent surges from damaging network cards, ISDN interfaces, and modems.

Fault-Tolerant Systems

- 1 Briefly discuss disk mirroring and duplexing and how these methods prevent data loss. Note that, with mirroring, if the hard drive controller fails, data is still lost. However, with duplexing, if the primary controller fails, the secondary drive and controller still ensure that data is safe.
- 2 Note that disk mirroring and disk duplexing are RAID level one.
- 3 Briefly discuss disk striping with parity. This is actually RAID (redundant array of independent, or inexpensive, disks) level 5. This system insures data against data loss by writing parity information for the data written on a different drive than the data is on. When a drive fails, this parity information can be used to reconstruct the data.
- 4 Note that the Windows NT operating system will perform disk striping with parity without extra adapter cards or software. This is one unique feature of Windows NT.
- 5 Note that when using RAID 5, all partitions in the stripe set must be the same size, and the equivalent of one disk is used for parity information. For example, if a stripe set consists of six 600 MB drives, the total usable space is 3 GB (5x600) while the parity space will equal 600 MB. Be sure to stress that the parity information is *not* located on a single hard drive.
- 6 Briefly discuss the benefits of each type of fault-tolerant system and when each would be used. Note that disk mirroring is less expensive, but makes less efficient use of the drive space available. Disk striping with parity makes more efficient use of the drives available, but requires many more resources than mirroring.

Additional Case Projects

Case A

The administration manager has taken a leave of absence and will not return for nearly a year. Her temporary replacement needs to have all access to the network that she had. What is the best way to ensure her replacement has the correct level of access? How will you ensure that no one uses the manager's account while she is gone?

Solution

Because the administration manager will eventually be returning, the best option is to copy her user account to an account assigned to her replacement. After that, the manager's account should be disabled. If the manager were not returning, the user could easily rename the account and change the password to give the replacement the exact access the manager had.

Case B

Your network has three servers and 15 workstations. You have been tasked with implementing a backup policy that will ensure against data loss, provide a fast backup, and provide the fastest recovery in the event of a failure. Outline a backup policy to suit your needs.

Solution

The best solution here is to back each server up independently every week night. To ensure that time is saved, a full backup should be done every Friday, with differential backups Monday through Thursday. By doing this, the backups at the backups on Monday through Thursday are fairly quick and, in the event of a failure, only two tapes will have to be restored.

Solutions

Answers to Chapter Review Questions

Question	Answer	Page
1	SECURITY or SAM (Security Accounts Manager)	287
2	b. Guest, c. Administrator	284
3	Disabled	289
4	128, 14	285
5	b. Global groups may not contain other global groups, c. There are three predefined global groups	288
6	a. one	291
7	b. The server might be experiencing a shortage of RAM	291
8	True	291
9	a. Performance Monitor	294
10	System	294
11	c. User Manager for Domains	294
12	8 MB	296
13	a. Performance Monitor	297
14	a. copy, c. differential (Although it is not stated in the text, the differential backup does not reset the archive bit. In this manner, everything since the last full backup is backed up.)	301
15	False	303
16	b. all currently logged-on user accounts accessing the server via the network	287
17	d. on all disks	303
18	b. 500 MB	303
19	32	303
20	d. 500 MB	303
21	False	287
22	RDISK /s	309
23	a. Permit MANAGEMENT to trust SALES, b. Make Joe a member of a local group in the MANAGEMENT domain.	289
24	b. System log	294

Hands-on Projects Discussion

Project 10-1

It cannot be stressed enough how important the Emergency Repair Disk can be in times of trouble. Familiarity with the RDISK utility can save you time and headaches.

Project 10-2

A network security plan is important for many reasons. Before embarking on a new network or server installation, having a plan already approved and in place makes the installation run more smoothly. In addition, if your network

is ever audited, the security plan can be used to assure the auditing staff of the solidity of your network.

The first question addressed in the project is role assignment and user/group creation. As stated, having this information before you start will make your life easier in the long run. Along with creating the users and groups, a password policy must be established. It is highly recommended that a minimum password length be established (usually six characters), and that users be required to change their passwords periodically (usually 60 days). There may be situations where it is preferable that users only logon to the network during certain hours. This is also part of the security plan and should be in place before work on the network begins.

When using Windows NT or a similar NOS where auditing options are available, decide what types of events you want to track. Do successful logon attempts mean as much to you as unsuccessful logon attempts? What about changes to the user and group objects?

Finally, a backup policy is imperative. Chances are you will probably never have a catastrophic network crash. But, guaranteed, if you don't have a good backup policy, it will happen.

Project 10-3

As mentioned in the text, Windows NT supports a number of RAID levels which are used to ensure against data loss. RAID 5, or disk striping with parity is the most secure and fastest RAID level supported by Windows NT. The steps outlined in this project will not only provide you with a better understanding of how RAID is setup on a Windows NT server, but give you the tools to save your data. Remember that each partition in the stripe set must be the same size and that the equivalent of one partition will be used for parity information.

Case Projects Discussion

Case 1

The correct answer to this question is "c. You accomplished your optional goal, but not your required goal." This is because the two-way trust relationship opens up ALPHA as well as OMEGA. The better option here is to setup a one-way trust between OMEGA and ALPHA, which will allow the ALPHA users access to the OMEGA resources, but not vice-versa.

Case 2

There is always a chance you will lose data. In this case, the most likely place data will be lost is the workstation. The server is adequately protected against data loss due to power failure. However, in the event of a power failure, you must be sure to take the server down gracefully to completely ensure no data is lost. The other information listed (the mirrored partition, the backups, etc.) are all very good ideas and should be implemented on all networks, they have no bearing on what happens when the power goes out.

Chapter 11: Enterprise and Distributed Networks

Objectives

After reading the chapter and completing the exercises, the students should be able to:

- Understand how modems are used in network communications
- Survey the different types of carriers used in network communications
- Explain how larger networks are implemented with devices such as repeaters, bridges, routers, gateways, and switches

Teaching Tips

Modems in Network Communications

- 1 Define modem and the function a modem performs. Note that modem stands for MODulator/DEModulator. They convert digital signals to analog signals (modulation) for transmission over phone lines, and upon receipt convert analog signals to digital signals (demodulation).
- 2 Note that modems can be either internal or external. This is important as modem speeds increase. A serial port (RS-232) on a computer can only communicate at 115 Kbps. ISDN, which is discussed in detail in Chapter 12, has a maximum speed of 128 Kbps. For this reason, it is often best to have an internal ISDN adapter.
- 3 Discuss the role of the Hayes modem in establishing the standard against which modems are measured.

Modem Speed

- 1 Briefly discuss the ITU standards for measuring modem speed. Use the example on page 316 to demonstrate how modem speed actually affects communication. A V.22bis modem will transmit a 1,000 word document in 25 seconds, whereas a V.42bis modem with compression will transmit it in one second.
- 2 Define baud. Note that originally, baud and bits per second were interchangeable. A modem that had 2,400 oscillations per second could transmit 2,400 bits per second. However, this has changed dramatically and now a modem transmitting 28,800 bps may only be using 9,600 oscillations per second.

Types of Modems

- 1 Discuss asynchronous communication and the method used by asynchronous modems to delineate each byte in a transmission. Async separate each byte with a start and stop bit.

- 2 Note that to ensure data integrity, a parity bit is added to each byte in an asynchronous communication stream. This parity bits works much the same way a CRC works in Ethernet.
- 3 Note that to increase communication throughput, many modems use compression such as Microcom's MNP 5.
- 4 Discuss synchronous communication and the method used by synchronous modems to coordinate data transmission. Sync modems, as opposed to async modems, rely on timing to ensure that data frames are correctly delineated. Because of this, sync modems must be "in sync" to communicate.
- 5 Note that sync modems are significantly faster than async modems.
- 6 Also mention that there are three synchronous communications protocols, SDLC, HDLC, and bisync.
- 7 It is very important to note that synchronous modems cannot operate over regular phone lines the way async modems can. Synchronous modems generally require a leased-line environment, which will be discussed in the next chapter. This increases the costs of using synchronous modems.
- 8 Briefly discuss digital "modems." In fact, these are not modems, but rather interfaces to connect computers to digital networks such as ISDN.

Carriers

- 1 Briefly discuss the PTSN and the three types of carriers available: dial-up, ISDN, and leased-lines.
- 2 Note that dial-up is the standard for home use and provides a temporary connection.
- 3 Briefly discuss ISDN, it will be discussed in greater detail in Chapter 12.
- 4 Also briefly discuss dedicated leased-lines; they will also be discussed in detail in Chapter 12.

Remote Access Networking

- 1 Briefly discuss the Remote Access Service included with Windows NT. Note that computers using RAS to connect to the network act as if they were directly attached, albeit significantly slower.
- 2 Note that there are two client connection programs, the RAS client and Dial-Up Networking (DUN) software. The connection software used depends on the operating system.

Serial Line Internet Protocol (SLIP)

- 1 Note that SLIP is the older of the two connection protocols and was intended for Internet connections. Because of this, it only supports TCP/IP.

Point-to Point Protocol (PPP)

- 1 Note that PPP provides a more dynamic mechanism for connecting remote clients. It supports TCP/IP, NWLink, and NetBEUI. It also supports dynamic IP address assignment, which SLIP does not.

Creating Larger Networks

Repeaters

- 1 Note that a repeater is used to regenerate a signal. However, also note that a repeater does not work above the Physical layer so they have no knowledge of the protocols and their structure. If a packet is damaged, but the signal is good, the repeater will regenerate the bad packet.
- 2 Also note that repeaters cannot be used to connect different protocols. An Ethernet segment must be connected to an Ethernet segment. However, repeaters are able to connect different cable types, such as Thinnet to UTP.
- 3 Briefly discuss propagation delay and its effect on networks using repeaters. It is because of propagation delay that the 5-4-3 rule exists for coaxial networks.

Bridges

- 1 Note that, in addition to connecting network segments and dissimilar physical media, bridges filter traffic and can connect different network architectures.
- 2 Discuss the filtering bridges perform. Bridges operate at the Data Link layer of the OSI model. Recall that the MAC sublayer of the Data Link layer is where physical addressing takes place. Using the information contained in packets it processes, a bridge learns which devices reside on each cable segment. It then forwards packets it receives according to the physical destination address of the packet. This process is used by transparent or learning bridges.
- 3 Discuss source-routing bridges. These bridges use information provided by the packet's source to determine the path the packet takes. In a source routing network, the stations do the majority of the work, whereas in a transparent bridging network, the bridge handles determines the packet's path.
- 4 Discuss broadcasts and note that bridges do not filter broadcast packets. This information is queried on the Microsoft test and it is important the students understand that bridges will not limit broadcasts and will not prevent broadcast storms.
- 5 Briefly discuss translation bridges which provide connectivity between different network architectures.

Routers

- 1 Discuss routers and their role in networks. Routers are used to create internetworks, or collections of networks. These internetworks function independently, but are able to share information.

- 2 Note that routers are able to provide fault-tolerance in networks by choosing between multiple paths. If a network is designed with more than one path from Office A to Office B, the router will choose the best path for the packets. However, if the best path is no longer available, the router is able to select another path.
- 3 Note that routers can connect multiple network segments and filter traffic like bridges. It is important to mention that, unlike bridges, routers do not forward broadcasts and can be used to prevent broadcast storms.
- 4 Mention that routers operate at the Network layer of the OSI model. Because of this, not all protocols can be routed, only those with Network information.
- 5 Also note that because routers operate at the Network layer, they can easily perform the function of translation bridges, i.e., sending information over different network architectures. This is very often the primary task for a router. A good example of this is illustrated in an internetwork which consists of two separate buildings on a campus. The buildings use Ethernet and are connected using FDDI. In this configuration, the router is used to send data between the two buildings and converts all data from Ethernet to FDDI and back to Ethernet.
- 6 Note that routers handle unknown destinations and broadcasts differently than bridges. When a router receives a packet whose destination it does not know, it discards the packet. Routers also do not forward broadcasts or corrupted packets. This is very useful in limiting the effect of network failures and broadcast storms.
- 7 Briefly discuss how routing tables are used by routers to determine the path a packet must take.
- 8 Briefly discuss both methods of populating these tables, static routing and dynamic routing.
- 9 Discuss both distance-vector and link-state route discovery algorithms. Use the following example to illustrate the differences between the two types of route discovery.

Consider a network between three sites as shown in the figure. Site A is connected to Site B via a T-1 line, Site B is connected to Site C via a T-1 line, and Site A is connected to Site C via a 56 Kbps line. When a distance-vector algorithm is used to determine the best path for a packet to take, traffic from Site A destined for Site C will be sent directly over the 56K line. However, because link-state algorithms take into consideration network speed as well as the number of hops, when OSPF is used to determine the best path, it will send the traffic through the router at Site B because two T-1 lines are faster than a 56K line.

- 10 Briefly discuss the spanning tree algorithm and how it is used to eliminate redundant routes. For more information on this topic, refer the students to *Interconnections: Bridges and Routers* by Radia Perlman. Ms. Perlman wrote the spanning tree algorithm and explains the topic in detail and very well. This book is highly recommended.
- 11 Briefly discuss routable and non-routable protocols. It is very important for the students to understand that NetBEUI is not a routable protocol. Because of this, it is only suited for small networks using bridges. If a router is installed in a network using NetBEUI, traffic will not be passed between the network segments.

Brouters

- 1 Briefly discuss brouters. Note that almost all hardware marketed as a router is, in fact, a brouter. Brouters, when correctly configured, are able to perform the functions of both routers and bridges. These devices are very useful in networks using a mix of routable and non-routable protocols, especially those using NetBEUI.

Gateways

- 1 Briefly discuss gateways. These are intricate pieces of equipment which operate at all layers of the OSI model to convert data from one format to another. They are most often found when connecting PC networks to mainframe computers.
- 2 Note that because of the detail involved in making these types of conversions, gateways are slower and more expensive than other networking equipment.

Switches

- 1 It is important to mention switches, as they are being marketed as a new technology. In fact, a switch is a high-speed, multiport bridge. Switches determine path according to the destination MAC address of the packet.
- 2 Note that the big difference between bridges and switches is that switches dedicate bandwidth to each connection. For example, in a typical repeater or bridge, all ports in the device share 10Mbps. However, with a switch, each port has what is known as “dedicated 10Mbps.”

Additional Case Projects

Case A

You have just been hired to administer a TCP/IP network that consists of seven segments in two buildings connected using routers and a T1 circuit. In an effort to alleviate network congestion, you have added a new segment in each building and have moved 20 computers to each segment. You are positive the computers and the routers are configured correctly, but the new segments can only see the existing segments, not each other. In addition, none of the original segments can see the new segment in the other building. You find that the routing tables on include the new segment information in their building, but not in the other building. What is the problem?

Solution

The routers have been manually configured using static routing. This being the case, each router will need to be updated with the information for the new segment in the other building.

Solutions

Answers to Chapter Review Questions

Question	Answer	Page
1	c. link-state	329
2	Propagation delay (or excessive propagation delay)	323
3	d. source routing	325
4	a. repeater	323
5	False	326
6	Non-routable	329
7	PPP or point-to-point protocol	321
8	d. Data Link	324
9	False	337
10	b. broadcast storm	325
11	a. bits per second	316
12	b. distance-vector	329
13	c. modem	316
14	SLIP or Serial Line Interface Protocol	321
15	False	317
16	Repeater	322
17	a. static routing	328
18	a. router	327
19	Routable	329
20	V.42bis	316
21	a. Transparent	324
22	b. Synchronous	318
23	Ter or terbo	316
24	False	325
25	c. gateway	331

Hands-on Projects Discussion

These projects are very straight forward in that they require only a Windows NT (Project 11-1) and a Windows 95 (Project 11-2) computer. Although a modem is required to use the RAS server and DUN clients, it is not necessary for installing the software.

Case Projects Discussion

Case 1

Because Windows NT includes the built-in RAS service, it provides an affordable and practical remote access solution. Even better, by using the RAS Point-to-Point Tunneling Protocol (PPTP), your remote users can simply dial an Internet ISP, and use PPTP to connect to the RAS server across the Internet, yet still maintain secure communications (PPTP encrypts all traffic between remote senders and the RAS server, and vice-versa).

RAS supports network access with full network capabilities, so that users can do remotely what they can do when directly attached to the network (only slower). Thus, in addition to e-mail access, are also able to use file, print, and applications services that would normally be available to them only if directly attached to the network.

To provide access to the NetWare resources, we recommend installing Gateway Services for NetWare on one or more of the Windows NT Servers. This will permit dial-in clients to access NetWare file and print services as if they were native Windows NT services. For native NetWare clients, it will be necessary to ensure that RAS forwards their IPX/SPX traffic to the proper NetWare servers, but RAS has proven itself quite able to handle such communication needs. If the native NetWare users need access to file and print services from the Windows NT Server machines, it may also become necessary to purchase the add-on File and Print Services for NetWare (FPNW) module from Microsoft for that reason.

Case 2

In this case, the presence of NetBEUI provides a clue that excessive broadcasts from the two combined 10Base2 segments may be slowing the overall network down. Because a repeater cannot filter traffic, it will be necessary to replace the repeater with a filtering device to block unnecessary traffic from passing between the two cable segments. Because the two networks functioned acceptably when they were not interconnected, it's safe to assume that most of the resources that users need reside on "their" sides of the interconnection device. This also makes it safe to assume that blocking broadcast traffic from transmitting the interconnection device will not impose undue hardships on network users. Because neither a bridge nor a repeater can block broadcasts, it will be necessary to replace the repeater with a router.

Case 3

LAN-to-host connectivity is an important consideration in many networks, especially those where employees need regular or occasional access to a legacy system such as a mainframe. In addition to providing connectivity between the LAN topology and the type of connection that the mainframe supports, it's also necessary to provide a common protocol across the two environments so that network clients on the LAN can communicate with the mainframe. Because the proposed solution calls for "possible reconfiguration of the mainframe" this provides a clue that adding a protocol to the mainframe might be the best solution.

The two ingredients that this solution requires are:

- 1 A physical connection between the Token Ring LAN and the Ethernet backbone to which the mainframe is attached. This requires a bridge or a router to connect the two dissimilar networking technologies, as shown in Figure 11-3. The actual choice of the device will depend on whether the interconnection must filter traffic (in which case a router is preferable) or not (in which case a bridge will work quite nicely). For most such situations, a router would be used because filtering traffic destined for the backbone is by far the most common practice.
- 2 A shared protocol between the Token Ring LAN and the Ethernet backbone. Although solutions for a variety of protocols are available, including IPX/SPX, SNA, and others, we recommend adding TCP/IP to the mainframe, because it will provide ready access to applications and services in that environment. With the appropriate software, the mainframe could serve files using FTP, Web pages using HTTP, and terminal emulation through a Telnet daemon or an IP-based 3270 terminal emulation service. Because LAN users will either already be using TCP/IP, or have ready access to its protocols and services, this creates the most usable shared protocol across the two environments.

Chapter 12: Wide Area and Large-Scale Networks

Objectives

After reading the chapter and completing the exercises, the students should be able to:

- Describe the base concepts associated with Wide Area Networks (WANs)
- Understand the differences between analog, digital, and packet-switching WAN technologies
- Identify the uses, benefits, and drawbacks of advanced WAN technologies such as ISDN, ATM, Frame Relay, FDDI, SONET, and SMDS.

Teaching Tips

Wide Area Network Transmission Technologies

- 1 Briefly discuss wide area networks. Be sure to mention that these technologies are often very expensive and most companies rely on third-party vendors, such as the phone company, to provide these services.

Analog Connectivity

- 1 Briefly discuss analog transmission over POTS/PSTN. Note that this network was originally intended to carry voice traffic only. Consequently, data communication can be a hit-and-miss proposition.
- 2 Note also that the PSTN may not be completely reliable because it is a switched network. Each time a call is placed, a different path is taken through the network. This means that the quality of each call is inconsistent.
- 3 Briefly discuss the line types used in the PSTN. Note that Types 5 and higher are able to transmit data.
- 4 Note that a line can be leased which ensures the quality of the line and provides for easy troubleshooting in the event that something goes wrong. However, this configuration is much more costly than regular dial-on-demand phone lines.
- 5 Briefly discuss the method used to decide whether to use leased-line or dial-on-demand analog circuits.

Digital Connectivity

- 1 Briefly discuss digital services and their benefits. The biggest benefit of digital service is that it is nearly 100% error-free. DDS circuits guarantee line quality and transmission rates.

- 2 Describe CSU/DSUs and their role in wide area networking. These devices perform similar functions to modems, but for digital, rather than analog, transmission.
- 3 Briefly discuss T1 circuits. Note that this is one of the most popular WAN solutions today. It provides 1.544 Mbps transmission at a fairly reasonable price. Note that when lower bandwidth is acceptable, a portion of a T1 can be used.
- 4 Discuss multiplexing and demultiplexing and how it is used over a T1 link to combine data transmissions. By using multiplexing, companies can use a single T1 and still provide separate channels for many different connections.
- 5 Briefly discuss T1 channels and the DS notation system. Note that each channel supports 64 Kbps transmission. Channels are then combined to form T1s, T3s, etc.
- 6 Note that T3 and T4 cannot be run over standard copper cable, but require fiber-optic.
- 7 Briefly discuss switched 56K lines. These lines provide digital communication on-demand and are charged according to the number of minutes used.

Packet-Switching Networks

- 1 Briefly discuss packet-switching networks and how they work. Note that this type of transmission does not rely on a single pathway. In fact, two packets may not even take the same path through the network.
- 2 Note that because the packets are small, their transmission is very fast. If a packet is lost or damaged, the time lost in retransmission is minimal.
- 3 Discuss virtual circuits, both switched and permanent, and how they are used in packet-switching networks.
- 4 Briefly discuss virtual private networks. This type of connectivity is becoming more and more popular as systems are able to support VPN connections over the Internet. Note that Windows NT 4.0 and Windows 95 support PPTP which can be used to create VPNs.

Advanced WAN Technologies

X.25

- 1 Briefly discuss X.25. Note that X.25 is a packet-switched technology that includes extensive error-checking.

ISDN (Integrated Services Digital Network)

- 1 Briefly discuss ISDN which provides support for both voice and data over digital lines. Discuss the differences between BRI and PRI and how they are used. It is important for the students to know which type of circuit is installed in the home or office and how many channels are available with each circuit type.

Frame Relay

- 1 Briefly discuss frame relay which uses packet-switching with limited error-checking and variable-length packets. Note that frame relay uses PVC communication techniques which means that the same pathway is used for all communication.

ATM (Asynchronous Transfer Mode)

- 1 Briefly discuss ATM which uses packet-switching but with fixed-length packets. Fixed-length packets provide for faster communication because the devices on the network are not concerned about the amount of data in the packet. If a packet is too small or too large, it was damaged during transmission and must be resent.
- 2 Note that ATM works at very high transmission speeds, 155 Mbps to a theoretical 2.4 Gbps.
- 3 Also note that ATM can easily interface with other WAN technologies such as T3, FDDI and SONET.

FDDI (Fiber Distributed Data Interface)

- 1 Briefly discuss FDDI and its use in both LAN and WAN configurations. Note that FDDI uses dual counter-rotating rings to provide fault-tolerance. All data is sent over the primary ring. However, if the primary ring fails, the traffic is rerouted around the failure on the secondary ring.
- 2 Note that FDDI operates at 100 Mbps at up to 100 kilometers. This distance means that FDDI is often used to create metropolitan area networks.

SONET (Synchronous Optical Network)

- 1 Briefly discuss SONET which uses fiber-optic cable to transmit voice, data, and video from 51.84 Mbps to 2.48 Gbps.

SMDS (Switched Multimegabit Data Service)

- 1 Note that SMDS is a high-speed WAN technology which uses fixed-length cells to provide communication speeds 1.544 45 Mbps.

Additional Case Projects

Case A

John's company needs to connect its 15 offices in the U.S. However, there is concern about cost and they would like to get the most from their money. Because of the centralized database they will be using, transmission must be over 1 Mbps. What type of WAN solution should John choose?

Solution

For this situation, frame relay is the best choice. It provides transmission speeds up to 1.544 Mbps and is relatively inexpensive.

Case B

Charlie's network consists of four buildings on a campus in suburban Philadelphia. As a company, they have decided to be on the cutting edge of technology and want to install a new inter-building network which will support video and voice, as well as data at speeds up to 1 Gbps. Which WAN solution should Charlie use?

Solution

ATM is the only WAN solution which will provide the services and speed Charlie requires. Because they are in a campus environment, installing the fiber-optic cable should be relatively inexpensive and they will not have to rely on a service provider, such as the local phone company.

Solutions

Answers to Chapter Review Questions

Question	Answer	Page
1	d. SONET	356
2	False	344
3	c. X.25	352
4	All answers (a., b., c., d., e.)	344
5	b. It transmits variable-length packets at the Data Link layer through the most cost-effective path.	353
6	d. PSTN	345
7	c. ATM	354
8	True	344
9	b. ISDN	352
10	a. limited bandwidth, b. inconsistent quality of equipment, d. originally designed for voice-only communications.	345
11	c. establishing calls and maintaining the connection	353
12	All answers (a., b., c., d.)	346
13	b. T1	347
14	a. 2.4 Kbps, b. 4.8 Kbps, c. 9.6 Kbps, d. 56 Kbps	347
15	c. 99%	347
16	c. CSU/DSU	347
17	All answers (a., b., c., d.)	348
18	c. Multiplexing is a technology that enables several communications to travel simultaneously over the same cable segment.	348
19	b. 24	348
20	b. 2	348
21	a. ATM, c. SONET	354, 356
22	c. packet-switching	322
23	True	322
24	b. frame relay, c. ATM	353, 354
25	a. 100 Kilometers distance	355

Hands-on Projects Discussion

As mentioned in the text, these projects demonstrate using the TCP/IP utilities TRACERT and PING. The computers the students are using must have TCP/IP installed and have access to the Internet. It is always interesting to watch the path a packet takes through the Internet when traveling to **Error! Reference source not found.** or someplace similar.

Case Projects Discussion

Case 1

With the information provided for this case study, the fractional T1 does indeed make the most sense. The bandwidth will always be available when needed (whereas some setup time would be necessary to add a second dial-up ISDN line when peak demand occurred), and the price tag fits exactly within the monthly budget for communications costs. The frame relay solution might be more appealing to businesses that wanted to keep costs as low as possible, but this approach would also impose some slight delay when usage needed to jump from 128 Kbps to 256 Kbps (but nothing like the time required to “add in” the dial-up ISDN connection). Note that the “average \$660 monthly charge” is determined by multiplying the 128 Kbps charge (\$550) by 120% (or, complete use of two 64 Kbps links, plus 20% use of two more 64 Kbps links).

As the following case study should indicate, however, this consideration only tells part of the story involved in selecting a WAN link type. Please note that over time, monthly recurring costs for most communications links quickly outweigh the financial implications of up-front costs: the higher the bandwidth, the more expensive the equipment that goes with it, to be sure, but higher bandwidth also costs more on a per-month basis. Over time, recurring costs usually comprise the bulk of the outlays involved for most systems (just as toner cartridges, repairs, and paper will usually cost more than a printer if compounded across a printer’s entire usage history).

Case 2

This case study is meant to point out that two factors contribute to up-front costs for communications links: equipment costs, plus installation and setup costs. For the scenarios described in this question, the economics argue most heavily in favor of the cheapest alternative—namely, ISDN. But because frame relay fits within the \$5,000 range stipulated for both equipment and installation costs, and provides peak-level bandwidth much more quickly and automatically than ISDN, if the \$5,000 ceiling truly can’t be broken, then frame relay would make the most sense, considering up-front costs, and average monthly communication costs.

But if network growth is possible, and the size of the channel might need to be upgraded in the next year or two, it’s also noteworthy that a mere \$200 may seem insignificant should it become necessary to switch from ISDN or frame relay to T1 in the future. In some cases, the same equipment that supports a fractional T1 can also support a full T1 link, so it would be possible to upgrade the T1 link from 256 Kbps to 1.544 Mbps without replacing the link attachment equipment. Given this consideration, management might be willing to find another \$200 to buy some potentially valuable additional bandwidth now, instead of having to pay to replace the frame relay equipment in the future.

This helps explain why it’s not only important to understand current communication requirements when planning WAN links, but to take account of anticipated growth requirements. Sometimes spending a little extra at the beginning can avoid being forced to spend significantly more later on when bandwidth needs exceed the capabilities of your current configuration.

Case 3

The best way to understand the implications of these prospective designs is to build a budget for each one. That's what's shown in Table 12-1. Here's how the table was created:

- 1 The total for all the videoconferencing equipment was added across all four sites in the first data line in the table. These costs contribute substantially to the monthly amortization costs for all three scenarios. But because they don't vary, we simply added them in for all three scenarios in the line that reads "TOTAL monthly costs, including all amortization."
- 2 For each scenario, we computed the costs for the NYC office separately, because it has triple the bandwidth needs. We calculated equipment plus installation for all three other offices as a single figure. Note that although equipment and installation costs may seem high as line items, when amortized over three years, they pale by comparison to communications costs.
- 3 Notice also that although there's a big cost differential between Scenario 1 and both Scenarios 2 and 3, that there's little monetary difference between Scenarios 2 and 3. We'd recommend choosing Scenario 2 only because of its modest cost savings; if reliability or alternate use of the bandwidth is possible, it might make more sense to contract with more than one communications provider for the T1 lines in Scenario 3: that way, if one provider goes down, the system could continue to function, albeit at reduced capacity.
- 4 If it weren't for the reliability and availability issues, Scenarios 2 and 3 are more or less a wash. To save a little money and reduce the amount of equipment to manage, choose Scenario 2; to increase availability and reliability of the system, choose Scenario 3. The real world will be full of interesting choices like these—working through the numbers gives you an excellent opportunity to discover where the best solutions lie.

	NYC	SanFran	Boston	Seattle	Total	Monthly Amort cost
video conference equipment	250,000.00	250,000.00	250,000.00	250,000.00	1,000,000.00	27,777.78
Scenario 1						
3 T2s for NYC						
monthly	36,000.00					36,000.00
equipment + installation	32,400.00					900.00
1 T2 for other sites						
monthly		12,000.00	12,000.00	12,000.00		36,000.00
equipment + installation	32,400.00					900.00
TOTAL Monthly costs, including all amortization						101,577.78
Yearly cost						1,218,933.33
Net costs (after deducting 1,000,000 travel savings)						218,933.33
Scenario 2						
T3 for NYC						
monthly	24,000.00					24,000.00
equipment + installation	55,000.00					1,527.78
1 T2 for other sites						
monthly		12,000.00	12,000.00	12,000.00		36,000.00
equipment + installation	32,400.00					900.00
TOTAL Monthly costs, including all amortization						90,205.56
Yearly cost						1,082,466.67
Net costs (after deducting 1,000,000 travel savings)						82,466.67
Scenario 3						
T3 for NYC						
monthly	24,000.00					24,000.00
equipment + installation	55,000.00					1,527.78
4 T1s for each add'l site						
monthly	36,000.00					36,000.00
equipment + installation	37,200.00					1,033.33
TOTAL Monthly costs, including all amortization						90,338.89
Yearly cost						1,084,066.67
Net costs (after deducting 1,000,000 travel savings)						84,066.67

Chapter 13: Solving Network Problems

Objectives

After reading the chapter and completing the exercises, the students should be able to:

- Discuss the benefits of network management and planning
- Understand the necessity for networking standards, policies and procedures, and documentation
- Troubleshoot the network following a structured approach
- Discuss the types of specialized equipment and other resources that are available for troubleshooting

Teaching Tips

Preventing Problems with Network Management and Planning

- 1 Briefly discuss the two ways to resolve network problems: preventing problems through planning and repairing damage that already exists. Note that these two forms of troubleshooting must work together to form a cohesive network management plan.

Backing Up Network Data

- 1 Recap that a successful backup plan must include a list of which files are to be backed up and how often, a schedule for backups, a person to perform the backups, scheduled testing of the backup system, a backup log, and a storage plan.
- 2 Briefly recap the backup methods.

Setting Security Policies

- 1 Note that it is very important to have a security policy in place as users are added to the network. This security plan should be detailed and followed closely to insure the security of the network.
- 2 Briefly discuss all security enhancements such as minimum password lengths, forced periodic password changes, etc.
- 3 One of the most important aspects of security is ensuring that only a few individuals have sufficient access to administer the network. The fewer people who have administrative access to the network, the safer the network is.

Setting Hardware and Software Standards

- 1 Discuss implementing hardware and software standards. It is very important that the students understand how to express the reasons for choosing certain hardware or software to their users. From an administrative and support standpoint, standardization is imperative. Users must understand that, although Word Perfect may do exactly the same things as Microsoft Word, if the policy is that MS Word is installed on all machines, it is that way for a reason and must remain that way.

Establishing Upgrade Guidelines

- 1 Discuss upgrades and implementing policies to govern them. It is very important that the students understand that, although it may work on paper, every upgrade should be tested and, whenever possible, a pilot upgrade system should be used. This means that, after testing, a few users are upgraded and use the system for a specified time before the entire organization is upgraded. By using this type of pilot system, the kinks of the upgrade can be worked out with a small group of kindhearted individuals before tackling the rest of the network.

Maintaining Documentation

- 1 Note that, although it is quite possibly the most boring aspect of network management, thorough documentation is a necessary evil. When it comes time to upgrade the network, purchase additional equipment, or troubleshoot a problem, a complete set of network documents is priceless.
- 2 Discuss each of the documents in the network documentation set.
- 3 Note that all documents should be kept in both hard and soft copy, and that it is imperative this information be updated regularly on both copies.

Performing Preemptive Troubleshooting

- 1 Briefly discuss each of the ISO's preemptive troubleshooting network management categories.

Using Network Monitoring Utilities

- 1 Note that it is very important to establish a baseline of "normal" network activity. This gives the user a point of reference when something on the network goes awry. Without a baseline, the user cannot as easily see what is wrong.
- 2 Briefly discuss the types of information that are gathered by network monitoring utilities and how they are used to identify network anomalies.
- 3 Note that measurement should be taken on a regular basis to ensure the network is performing adequately and that the baseline is accurate.

- 4 Discuss SNMP and how it is used in TCP/IP networks to manage and monitor devices. SNMP uses software agents which are loaded on network devices to monitor their performance and configuration. This information is kept in a management information base (MIB).
- 5 Note that an SNMP manager is used to retrieve information in a device's MIB. This information can then be logged or graphed to provide a baseline for the device's performance.
- 6 Mention that SNMP can also be used to manage and configure network devices. These functions are controlled by through security groups called communities. For example, one community may be given access only to view MIB information, whereas another may be allowed to configure the device. This limited security insures against unauthorized reconfiguration of network devices.

Network Troubleshooting

Troubleshooting Methodology

- 1 Note that most network problems can be corrected by verifying the state of the computer. The two key steps are eliminating user error and verifying the physical connections. The vast majority of problems fall into these two categories.
- 2 Remember, if all else fails, reboot. Some problems that occur are true anomalies and can be corrected simply by rebooting the computer.
- 3 Note that the structured approach in the text is recommended by Microsoft and will be referred to on the certification exam. After going through the four basic steps, this approach ensures that nothing is missed in the melee to locate and correct the problem.
- 4 Briefly discuss each of the five steps in the structured troubleshooting approach. Each of these steps is extremely important and the students must be able to ask the correct questions of users when the fateful call comes in.
- 5 Note that, when collecting information, specific questions are the key. Rather than asking "What's wrong?" ask the user "Is the network slower than normal?" or "Is your screen blank, or can you move your mouse?"
- 6 Note that the biggest question when collecting information is "What has changed?" This is often the key to any problem.
- 7 Note that after a problem seems to be fixed, it must be tested to ensure that the correct solution was used.

Using Special Tools

- 1 It is very important the students understand the applications and limitations of each device for the Microsoft exam. Knowing when to use a DVM and when to use a TDR is key to passing the troubleshooting portion of test.

- 2 Note that most network problems occur at the Physical layer of the OSI model and, consequently, most troubleshooting tools operate at this layer.
- 3 Discuss how a DVM works and how it can be used to determine whether the cable is intact. If the DVM finds no resistance or resistance within the cable's limitations (50-ohms for Thinnet, for example), the cable is fine. However, if the DVM shows infinite resistance, there is a cable break preventing electronic flow.
- 4 Discuss using a TDR to locate a short or break in the cable. Note that a TDR can provide an approximate location for the cable break.
- 5 Briefly discuss advanced cable testers and oscilloscopes. Cable testers operate at higher layers of the OSI model and therefore provide more detailed information. O-scopes can be used to identify crimps, bends, breaks, and even attenuation problems.
- 6 Briefly discuss network monitors, such as Windows NT's Performance Monitor and Network Monitor, and how they are used to troubleshoot network problems. These programs are able to capture and decode network traffic, which qualifies them as software-only protocol analyzers.
- 7 Discuss protocol analyzers. These hardware and software combinations provide the most advanced network troubleshooting and are by far the most expensive equipment available. Perhaps the most well-known protocol analyzer is the Network General Sniffer which can decode frames from more than 14 protocols.

Network Support Resources

Microsoft TechNet

- 1 Briefly discuss TechNet which is a subscription service provided by Microsoft. Note that this service is fairly expensive, but well worth it for administrators supporting Microsoft-based networks.

Microsoft Knowledge Base

- 1 Since the manuscript was produced, Microsoft has changed the format for the Knowledge Base. The new URL is <http://www.microsoft.com/support>. This page is a search engine through the Knowledge Base and provides support for networking questions.

Bulletin Board Services (BBSs) and Newsgroups

- 1 Briefly discuss BBSs and their role in gathering information and drivers. The MSDL is used to retrieve the latest software and drivers for Microsoft products. Many other hardware and software manufacturers provide a BBS for these services as well.
- 2 Discuss newsgroups and how to use them to gain knowledge and ask questions regarding problems the students may be experiencing.

Periodicals

- 1 Note that periodicals such as *LAN Times* and *Network Computing* are invaluable resources for information regarding new and current technology.

Common Troubleshooting Situations

Cabling and Related Components

- 1 Discuss troubleshooting Physical layer problems, such as those involving cables, connectors, and NICs.

Power Fluctuations

- 1 Note that power fluctuations can not only cause data to be lost, but can physically damage hardware. The best way to prevent this is to connect computers to UPSs or, at the very least, surge suppressers.

Upgrades

- 1 Discuss implementing upgrades and troubleshooting problems with upgrades. The most important thing, which cannot be stressed often enough, is to test every upgrade thoroughly. Also, always inform your users that an upgrade is being performed and when it is. This way, when problems occur, the users will know why and will be able to help troubleshoot problems.

Poor Network Performance

- 1 Note that most network performance problems occur because of changes in the network. A new computer is added which extends the cable beyond its maximum segment length, or new equipment has been added which is not performing as expected. In addition, users playing networked games often cause large amounts of traffic on the network, bogging it down and making other communication impossible.

Additional Case Projects

Case A

A computer on your network has started sending large amounts of bad packets, which are bogging down your 10Base2 network. What could be causing the problem? What is the solution?

Solution

The most likely problem in this situation is a bad T-connector or NIC. The first solution to try is replacing the connector. If the problem persists, replace the card in the computer.

Solutions

Answers to Chapter Review Questions

Question	Answer	Page
1	b. Microsoft Knowledge Base, d. Microsoft Download Library	384, 385
2	c. time-domain reflectometer	382
3	a. Physical	381
4	b. volt-ohm meter	381
5	a. Accounting management, b. Configuration management, d. Performance management, f. Security management, g. Fault management	375
6	a. rebooting the computer	379
7	a. Stay calm or b. Eliminate user error	378
8	True	379
9	c. Network Monitor	382
10	Thorough planning	370
11	b. TechNet	384
12	c. protocol analyzer	383
13	a. Test to isolate the cause, b. Study the results of the test to identify a solution, e. Collect information about the problem, f. Set the problem's priority, g. Develop a list of possible causes	379
14	c. cabling problems	381
15	b. UPS	387
16	d. Verify the physical connections.	379
17	b. MIBs	377
18	True	375
19	b. SNMP	377
20	True	385

Hands-on Projects Discussion

Project 13-1

For this project, the students will need to define a list of documents required for their network. If the students do not have a real-world network to work from, propose a sample document plan that still requires security, upgrade, hardware, and software policies.

Project 13-2

For this project, the students will install Network Monitor on their Windows NT Server system. They will need the NT Server CD-ROM or the installation files (the I386 directory from the CD-ROM) to perform the installation.

Project 13-3

For this project, the students will install and configure the SNMP agent software for Windows NT. They will again need the CD-ROM or the installation files.

Case Projects Discussion

Case 1

The first thing to recognize here is that both symptoms indicate a fundamental inability to access the network. The five step-method is as follows, which we annotate here with specific remarks:

- 1 **Set the problem's priority.**
The user is unable to function on the network. As long as nothing more pressing is in your in-basket, this is about as serious as things get for a network administrator. It's time to start troubleshooting!
- 2 **Collect information about the problem.**
You already know she can't get to e-mail, and she can't print. When you get to her office, check the network cable on her machine first. If it's properly connected, try a basic access tool like PING or NETSTAT to see if any kind of network access is working. If it is, you'll need to find out what's changed recently on that machine, and see if some configuration problems might be at work.
- 3 **Develop a list of possible causes.**
Network connectivity is compromised.
Configuration changes have affected network access.
- 4 **Test each hypothesis to isolate the actual cause.**
Examine the cable for basic connectivity.
Test network access with simple PING or NETSTAT commands.
Ask user about recent changes to system.
Attempt other forms of network access or use.
- 5 **For each potential cause, attempt at least one solution.**
Reseat the cable and/or run NIC diagnostics software.
Run PC/desktop diagnostics to check basic system functionality.
Restore configuration to earlier settings.
Bring a laptop and check to see if a known good working machine can connect.

Case 2

The network topology uses a Thickwire backbone to connect two subnets on Thinnet. When the other Thinnet segment drops out of sight completely, the first place to start checking is on the Thickwire segment that connects the two buildings. Begin with the protocol analyzer to see if any network traffic is visible on that cable segment at all. If the segment is active, analyze a trace to see what addresses are responsible for whatever traffic does appear thereupon. If the traffic is from “your” building, chances are good that there’s a break between the backbone and the “other” buildings backbone connection; if the traffic is from “their” building, check your building’s backbone connection. If there’s no traffic on the backbone at all, given that it’s Thickwire, this usually indicates a cable break, a short, or a missing terminator. Your cable tester should help you isolate and locate such problems in fairly short order.

On the other hand, higher layer problems have been known to cause such symptoms, too. If there are no basic connectivity problems evident, ask if any routers have been reconfigured lately. We’ve seen the same symptoms appear when misconfiguration caused all traffic from one segment to be filtered out (rather than only the broadcasts that the filter was supposed to block). This is another case where your protocol analyzer will come in handy, because it will show you exactly what kind of traffic is active on the backbone, and let you determine where it’s coming from and what kind of traffic it is.

Case 3

The bisection method is a great way to proceed when trying to isolate low-level connectivity problems. Make sure you have a portable protocol analyzer, or at least a laptop with a 10Base2 connection active and working, and two extra terminators. Start at one end of the network and terminate the end-most cable segment on both ends, with one other computer attached. If your problem lies in this neighborhood, you’ll soon realize it, and should be able to take appropriate steps: Replace one or both terminators, replace the cable, replace the other computer’s NIC.

Once this small network is working, add an additional cable and computer, and test again. You’ll repeat this until the problem appears. When it does, verify its location by isolating the most recently added segment and computer, and testing it by itself. If the problem persists, zero in on the potential culprits on that segment: the cable, the other terminator, and the computer’s NIC. If it doesn’t back up from your current configuration, and reverse your path to add back in segments you’ve already tested. Should this happen, also test the cables to make sure their impedance is correct (and that it’s the right kind of cable; we’ve seen this happen when an RG-62 segment got mixed in with a bunch of RG-59 A/U segments by mistake).

What’s at work here is a process of elimination. By carefully checking each element in the network segment, you’re able to isolate and eliminate the problem. Access to basic test equipment (a VOM) and a working laptop or protocol analyzer will make this job much easier.

Chapter 14: The Internet: A World-Wide Resource

Objectives

After reading the chapter and completing the exercises, the students should be able to:

- Discuss the Internet and its available services
- Access resources on the Internet and understand its addressing methods
- Make and use an Internet connection

Teaching Tips

What's on the Internet?

- 1 Note that today's Internet began as a the Department of Defense's Advanced Research Projects Agency Network (ARPANET or eventually DARPA-NET). This network was used primarily to share information among an elite group of universities and research labs.
- 2 Note that the Internet uses the TCP/IP protocol suite and is at least partially responsible for its prominence in networking today.

E-mail

- 1 Discuss e-mail and its ramifications for business and personal communications today. This is the most popular function of the Internet because messages are nearly instantaneous and are often less expensive than faxes, overnight services, or regular mail.
- 2 Discuss addressing e-mail. Note the @ symbol which is used to delineate between the addressee and their organization.
- 3 Note that most e-mail uses the SMTP protocol for transport and the MIME standard to govern how files are attached to messages.

File Transfer Protocol Servers

- 1 Note that along with BBSs, FTP servers are often the best way to retrieve the latest driver or software from a particular vendor.
- 2 Discuss the different FTP clients available. Note that the FTP client included with the Microsoft operating systems is character-based, but there are many FTP clients available that are GUI-based.

- 3 Note that most Web browsers, including Internet Explorer and Netscape, support FTP access and are easier to work with than character-based clients. However, often browsers only support anonymous logons, which are not supported at many FTP sites.

Gopher

- 1 Briefly discuss Gopher which is a menu-driven program which is often used in academic environments. It allows users to browse files without knowing their exact location.
- 2 Note that Gopher is often used in the University environment to distribute information, but does not have a large installation in the business environment.

Newsgroups

- 1 Discuss USENET newsgroups, their content, and use. The USENET system is extensive and provides readers with a discussion forum on any topic. From a networking perspective, users can take part in discussions on any topic and can pose questions to other users and administrators who may have more experience in the area.

Telnet

- 1 Briefly discuss Telnet and its application in networking and the Internet. Telnet can be used within a network to manage and configure many types of equipment, including routers and bridges, as well as interact with remote systems.
- 2 Note that Telnet is also often used on the Internet to provide text-only connectivity to ISPs and other systems for e-mail and account management.
- 3 Note that Windows NT Server does not include a Telnet daemon, but a beta version is available which will allow an administrator to manage an NT server.

World Wide Web

- 1 Discuss the World Wide Web and its use in networking today. Direct students to the Microsoft home page and discuss the information that can be found there.
- 2 Discuss using search engines such as Yahoo and Alta Vista to determine which Web pages have information on a particular subject.

Locating Internet Resources

Internet Resource Names

- 1 Describe the Uniform Resource Locator (URL) convention and how it is used to name Internet resources. Note that a true URL includes the protocol used. For example, many people use **Error! Reference source not found.** as a URL when, in fact, the URL is <http://www.microsoft.com>. This is because it is not necessary for a site to include www or ftp in their name. For example, the CNN site is cnn.com. If a user wanted to go to the FTP site for CNN, which does not exist by the way, the user would enter <ftp://cnn.com>.

Domain Name System (DNS)

- 1 Describe the Domain Name System and how it is used to assign names to IP addresses.
- 2 Briefly discuss the basic domains used on the Internet. Note that this domain system is currently being revised to include much more specific domain names. Direct the students to the domain name registration authorities at <http://www.uninett.no/navn/domreg.html>.

Making an Internet Connection

- 1 Note that the type of Internet connection used is determined by the amount of bandwidth needed and the cost. Many companies that utilize the Internet extensively have T1 or even T3 access to the Internet; many home and SOHO users get by with ISDN or dial-up connections.

Dial-Up Connections

- 1 Discuss making a dial-up connection to the Internet and the selection of protocols. Recap that PPP supports dynamic IP addressing, which is used by most ISPs.

ISDN

- 1 Briefly discuss ISDN implementations and their competition, cable modems and DSL services.

Connection Considerations

- 1 Recap that the primary considerations in choosing an Internet connection are cost and bandwidth. Most individuals cannot afford to install a T1 to their homes, whereas most businesses cannot rely on dial-up connections.
- 2 Discuss implementing proxy servers and firewalls to provide secure Internet access for businesses. A proxy server, such as Microsoft Proxy Server 2.0, acts as a gateway between the network and the Internet. A firewall, on the other hand, restricts access by filtering packets it receives.

Additional Case Projects

Case A

One of your Windows NT Workstation computers has been experiencing intermittent crashes and has caused some data to be lost. Which Internet resources could you use to try to fix the problem?

Solution

The first place to look is the Microsoft Knowledge Base Web site. By entering a search string, you will be able to find information about your problem. In addition, one of the Microsoft newsgroups may provide you with some information. If no one is experiencing the same problems, posting a question to the group may provide an answer.

Solutions

Answers to Chapter Review Questions

Question	Answer	Page
1	b. ISDN	414
2	c. Gopher	408
3	c. HTML	411
4	True	411
5	c. .org	413
6	b. HTTP	411
7	c. PPP	414
8	a. NNTP	409
9	Search engine	411
10	b. @	405
11	b. modem	414
12	d. the Department of Defense	404
13	c. ISP	406
14	True	412
15	c. DNS	413

Hands-on Projects Discussion

For each of the Hands-on Projects, the students will need computers with access to the Internet and a Web browser. The exercises assume Microsoft Internet Explorer will be used, but Netscape or another browser will also work. Each of the projects give the students exposure to services available on the Internet.

Case Projects Discussion

Case 1

Given the problem description, starting at Novell's (www.novell.com) and Microsoft's (www.microsoft.com) and using their search engines with a string like "troubleshooting Token Ring" seems like a good place to start. If your NICs come from a single vendor or a small group of vendors, check their Web sites for bug reports, driver update information, and troubleshooting tips. We also recommend checking Yahoo! (www.yahoo.com) and Excite (www.excite.com) and searching on strings like "troubleshooting Token Ring" and "Token Ring troubleshooting." It would probably be worthwhile looking for general Token Ring information by searching there for entries like "Token Ring tutorial" or "Token Ring networking overview" as well.

Case 2

What this exercise should tell you is that a Web browser and Internet access is all you really need these days to keep your configurations current, and to keep up with trouble and bug reports for your systems. We don't configure a new system any more without visiting the vendor's site to see what's new by way of drivers for all the components in the system. We strongly suggest that you follow the same approach from here on out!

Case 3

Using this search string on the Microsoft site took us straight where we wanted to go: "Windows NT" and "SP3"

This is called a Boolean search, because it uses the logical AND operator to instruct the search engine to return only documents that contain the literal string "Windows NT" and the literal string "SP3." This is the kind of search approach you want to use to keep from reading too much irrelevant material in your search for the "right stuff." Total elapsed time for this approach: about 30 seconds, most of it spent waiting for the search response to be returned.

On the other hand, here's how we got to the same location by deliberate navigation:

- 1 Starting at the Microsoft home page at www.microsoft.com, we clicked the Products button at the top of the page.
- 2 Next, we selected the BackOffice products family, then clicked the Product Information button at the bottom of the page.
- 3 Then we clicked on the download button for the Microsoft Windows NT Server page
- 4 Then, we searched for about five minutes before we realized this was the wrong path, and hit the back button four times to jump to the Windows Product Family pages instead.
- 5 Then, we clicked on the Windows NT Server 4.0 home page. This took us to the same page, we'd jumped out of from the products family.
- 6 This time, we tried the "Hot News" listing, and scrolled through four screens of data before seeing pointers to post SP3 hotfixes, and then eventually, a pointer to SP3 itself

Total elapsed time for this approach: nearly 15 minutes, most of it reading frantically to figure out where to go next.

The moral of this story is: if there's a search engine, learn how to use it as well as you can. It will save you hours of wasted time, in very short order.