Network Planning And Design

Terms you'll need to understand:

- √ Security
- √ Disaster recovery
- √ 10Base2
- √ 10Base5
- √ Coaxial cable
- √ Twisted-pair cable
- √ Fiber optic cable
- √ Ethernet
- √ Token Ring
- √ ARCNet
- √ Fault tolerance
- √ Repeaters
- √ Bridges
- √ Routers
- √ Brouters
- √ Gateways

Techniques you'll need to master:

- √ Understanding the concepts behind a successful network deployment
- √ Implementing fault tolerant features for network security

LAN communication functions are primarily performed by a combination of hardware and the firmware specifically designed to support it; therefore, the physical and logical implementations are essential to every network. Hardware can typically be defined as the network interface card (NIC), the cabling plant, and the hub or concentrator unit. To implement LANs successfully and logically, you must take into consideration user requirements, protocols, and a variety of architectures, which have strengths and weaknesses. We examine these topics throughout this chapter.

First, we cover what considerations must be taken into account when choosing a particular topology or network protocol. Next, we discuss topology requirements, including Ethernet and Token Ring—which we introduced in Chapter 5—and the restrictions of each media type. Then, we take a look at selecting an appropriate network architecture and network design principles. Finally, we review the guidelines for planning a successful deployment.

Network Layout Principles

There are several factors to consider when designing a network. Layout will be influenced by such elements as the following:

- Cost
- Distance limitations
- Potential growth
- Location
- Security
- Disaster recovery
- Capacity

Although you want the network to be as cheap, fast, unlimited, and secure as possible, the reality is that such a thing does not exist; you must achieve a balance among all the components. A matrix that takes design into consideration can be constructed. In this design, all factors can be numbered with the higher numbers taking priority over lower numbers. For example, if you are a designer for a small engineering firm that both expects little to no growth and has great capacity requirements due to bandwidth-intensive

applications, you would probably give greater weight to cost and capacity at the expense of disaster recovery and growth potential.

Cabling Considerations

The most basic networking component is the cabling plant. You should know how to select an appropriate cabling scheme, which we covered in detail in Chapter 4. You must take into consideration cost as well as distance limitations and restrictions. In the case of the engineering firm in the earlier example, a bus topology is appropriate because it is cheaper to implement than a star or ring topology. The trade-off is disaster recovery, because a single cable break affects all other workstations on the bus. Another consideration is media type. Your choices are twisted-pair, coaxial, or fiber optic cable—or wireless technology.

Here's what you need to know:

- Thinnet or 10Base2 networks use coaxial cable. The type is 50-ohm RG-58 A/U. Don't confuse it with RG-59A/U or RG-62A/U cables, used for cable television and ACRNet, respectively.
- Thinnet is used for relatively short-distance communication and is fairly flexible to facilitate routing between workstations. Thinnet connects directly to a workstation's network adapter card using a BNC T-connector, and uses the NIC's internal transceiver.
- Coaxial cable is also used for Thicknet or standard Ethernet cabling. It is less flexible, because it's about half-an-inch in diameter. Thicknet was traditionally used to connect several smaller Thinnet segments, because Thicknet was more expensive and difficult to install, and makes for a better backbone cable.
- Coaxial cable has the following advantages: low maintenance costs; simple to install; better resistance to signal noise over longer distances; and electronic support components are less expensive.
- Disadvantages of coaxial cable include limited distance and topology, low security (easily tapped); and it is difficult to make major changes to the cabling topology.
- To link two coaxial segments together, use a barrel or T-connector.

- Twisted-pair cable has the following advantages: It's well understood; it's easy to add computers to existing networks; it may already be installed in many buildings; and it is the least expensive cable medium.
- Twisted-pair cable has the following disadvantages: It's susceptible to noise, distance, and bandwidth limitations; it's least secure (easiest to tap); and it requires more expensive electronic support components (that is, hubs).
- Fiber optic cable advantages include: most secure (hardest to tap); highest bit rates; lowest loss over great distances; not subject to interference; supports voice, video, and data; smallest in size; and greatest longevity.
- Disadvantages of fiber optic cable are: most expensive medium in terms of installation and maintenance; somewhat delicate cable (can't be sharply bent); mostly limited to point-to-point applications because support components are expensive and not readily available.

Topology Requirements

Now that we've discussed media and how it affects the network topology, let's examine what the requirements are for the two most common topologies in use today: twisted-pair Ethernet and Token Ring. Token Ring is commonly used in large companies that need to network PCs with IBM mainframes and is less common in small businesses. It can have higher transmission speeds and can support more computers on a single network segment (up to 260, depending on the media type) than Ethernet. It is more expensive than Ethernet and is harder to install and maintain. We usually see its network cables diagrammed as a ring; but in reality, workstation cables radiate from a central hub to the computers, like a rimless spoke.

The layout for twisted-pair Ethernet looks like that of Token Ring, with computers attached to cables radiating from a central hub. As with Token Ring, the workstation cable runs up to 100 meters from a port in the hub to the network interface. The greatest advantage of twisted-pair Ethernet is that it is somewhat fault tolerant: If a transceiver starts jabbering or causing broadcast storms, the concentrator will usually be intelligent enough to shut down that port.

Also, the hub minimizes network failures. If a twisted-pair cable breaks, only that cable's computer is affected. If a thin Ethernet cable breaks,

the entire network stops functioning because 10Base2 is a bus topology. However, hubs complicate expansion: If you have an eight-port hub and want to add a ninth computer, you need a bigger hub (or another hub, with a maximum of four repeater levels). If you have eight computers on a thin Ethernet segment, you can add a ninth with an additional cable and T-connector. Again, a trade-off must be made between cost, distance limitations, potential growth, and capacity.

10BaseT Ethernet Restrictions

Here are some limitations of 10BaseT Ethernet:

- Workstations may be no more than 328 feet (100 meters) from the concentrator port.
- 1,024 stations are allowed on a segment without bridging.

10Base2 Ethernet Restrictions

Here are some limitations of 10Base2 Ethernet:

- The Ethernet 5-4-3 rule for connecting segments is 5 trunk segments can be connected, with 4 repeaters or concentrators, with no more than 3 populated segments (on coaxial cable).
- Length of trunk segment may be up to 607 feet (185 meters).
- A maximum of 30 workstations is allowed per trunk.
- There may be no more than 1,024 workstations per network.
- Entire network trunk length can't exceed 3,035 feet (925 meters).
- The minimum cable length between workstations is 20 inches.

10BaseFL Fiber Optic Inter-Repeater Link (FOIRL) Restrictions

10BaseFL is a standard defined by the IEEE 802.3 specification and is used over two fiber-optic links to transmit and receive data. It is highly resistant to noise and interference, and has a distance limitation of two kilometers.

Token Ring Restrictions

Here are some limitations of Token Ring:

- The maximum number of workstations is 260 on Type 1 or fiber optic cable at 16 Mbps.
- The maximum number of workstations is 72 on Type 3 cable at 4 Mbps.
- The distance between MSAUs (multistation access units) is 100 meters or 328 feet (Type 1 cabling) to 45 meters or 148 feet (Type 2 cabling).
- Each ring can have up to 33 MSAUs.
- Maximum distance of the ring is 4 kilometers with fiber optic cable.

ARCNet Restrictions

Here are some limitations of ARCNet:

- Bus segment length for coaxial cable is a maximum of 1,000 feet, with a limit of 8 workstations per coaxial segment.
- Bus segment length for twisted pair is a maximum of 400 feet.
- There is a maximum of 255 workstations per network.
- Workstations can be located up to 600 feet from the active hub.
- The maximum distance from passive hubs to active hubs is 100 feet; the maximum distance between two active hubs is 2,000 feet.
- The maximum distance allowed between workstations is 20,000 feet.
- There can be no more than 4 workstations on a passive hub, no more than 100 feet from a hub.
- Passive hubs cannot be connected to other passive hubs.

Selecting A Network Architecture

The network architect is guided first by the list of requirements, in order of priority, for the proposed network. When selecting a network architecture, you'll want to consider the following factors:

- Hardware requirements
- Software requirements

- Telecommunication needs
- Disaster recovery needs
- Corporate culture and organization
- Information analysis
- Environmental conditions

The types of hardware you need to consider include workstations, servers, backup systems, peripherals such as printers and CD-ROM towers, uninterruptible power supplies (UPSs), routers, bridges, hubs, minicomputers, and/or mainframes. If your network includes legacy systems, you'll need to integrate that technology smoothly with newer, open systems. It would not make sense to install a 155 Mbps ATM network in a company that still uses 486-class machines with ISA buses. Consider not only configuration, but usage as well. If your network utilization is very high and performance is slow, but your organization is expecting a growth spurt, consider replacing your aging Ethernet concentrators with high-powered switches to relieve congestion and create room for expansion and growth.

Software Considerations

What software will reside on the network? Perhaps your organization uses dumb terminals connected to a mainframe that runs proprietary, mission-critical applications. Perhaps several database programmers are on staff and the use of SQL Servers in your company is quite high.

Maybe your company uses only standard office applications, such as Microsoft Office. You may belong to a graphical design firm that uses bandwidth-intensive design software. Or you may work for Mr. Scrooge, who doesn't believe in spending money for network management, monitoring, or administration software tools. The choice of architecture will be different in each of these cases.

Telecommunications Considerations

The telecommunications needs that you need to consider include such things as PBXs, data links to the WAN, and remote access for a traveling sales force or a work-at-home initiative. If your company plans to use the same data link for voice as well as video and data, you'll need a T1-class connection. If this link is mission critical, you need to either establish a second, fail-safe link or make arrangements with your carrier for a virtual redundant link.

For example, if you must communicate primarily with the corporate headquarters in Atlanta, and you are in New York City, NetBEUI would not be an appropriate protocol for your network because it is not routable. If your work-at-home users all have 19.2 Kbps modems, the dial-in access will be an information bottleneck and you wouldn't need to put your communications server on a high-speed backbone.

Disaster Recovery And Fault-Tolerance Considerations

How important is disaster recovery to your organization? Consider a medical facility. Its network must be available 24 hours a day and it must be secure, to protect the confidentiality of patients' medical records. The network equipment should be protected by UPSs, and all file servers should be kept in locked closets, away from unauthorized personnel. The facility would probably need redundant equipment such as file servers, hubs, and routers even though redundancy is very expensive.

A bus topology wouldn't be appropriate because a cable break affects all workstations behind the break. Token Ring probably wouldn't be very effective either, because damage to a portion of the ring can knock several workstations off the network if the design isn't right.

Corporate Culture And Organizational Considerations

An effective, efficient network must also take into account the culture and organization of the company. For instance, if you belong to a small office that can't support a full-time MIS staff, you would probably choose a simple protocol, such as NWLink, and a fool-proof topology, such as twisted-pair Ethernet, which doesn't require a great deal of maintenance or administrative overhead. On the other hand, if you are designing for a law firm, where security is paramount, you'll need a file server for user-level security. A peer-to-peer network, such as Windows 98, that supports only share-level security would not be a good choice even though it is inexpensive.

You must also consider the following:

- What types of users will the network support and how will they use it?
- Will vendors and subcontractors be allowed to access your network?

- Will that access be local, through the Internet, or by way of dial-in access?

Share-level security, also called password-protected shares, assigns a password to each resource on the network. User-level security, also called access permissions, assigns rights to the network resources on a user-by-user basis. But, if your company requires high levels of security, encryption provides the best protection for user data.

If your network users are not computer-savvy, you would not want to choose an operating system such as NetWare or Unix, because they require a high level of understanding or ongoing, in-depth training. A simple, user-friendly network operating system (NOS) would be easier to understand and implement.

The best way to partition users is to identify how much latitude they need to successfully do their jobs. For example, someone who uses few applications and rarely upgrades software or hardware does not need a flexible and expandable environment. This is typical of task-oriented users. On the other hand, power or "knowledge-oriented" users—who need to use several different applications and upgrade hardware frequently—need more flexibility. Although it's obvious that centralized management leads to lower total cost of ownership and more security, the desire to centrally manage systems should not be more important than giving users the right tools for their jobs.

Information Analysis Considerations

Consider the informational needs of your network users. It may not be a matter of what they need to know, but *when* they need to know it. A bank or financial institution will probably use fast, dumb terminals that communicate with an off-site mainframe to access customers' records for loan processing. If the data is not immediately accessible during normal banking hours, the company stands to lose a substantial amount of money, as well as the goodwill of its customers.

In the case of a large governmental agency, on the other hand, data is usually updated through batch processing during the night, and information is not available in realtime. In most organizations of any size, there is such a substantial amount of data that sophisticated data warehousing and data mining tools are needed along with a cadre of analysts to extract the relevant information. In this case, the analysts would probably require faster machines and faster network access than the typical user, because information could be as old as 24 hours.

Environmental Considerations

Environmental conditions may include the obvious, such as space, electricity, cleanliness, and security, but these considerations may really be as simple as what's in place today. For instance, you would probably choose twisted-pair Ethernet if your building has CAT3 or better cabling already installed. However, if your manufacturing company plans to add another building to its campus and your existing buildings use a Token Ring network to access a mainframe, it wouldn't make sense to install Ethernet. Breaking that uniformity would result in higher installation costs, and a gateway would be required. Likewise, there's a higher cost of ownership for hybrid networks like this, which doubles the amount of hardware and knowledge you need to do your job.

Network Design Principles

Now that we've considered the elements of network design, let's consider the mechanisms involved. There is a truism in this business: Networks never shrink, they only grow. You must always design for growth whenever the budget allows. When a LAN has exceeded its limitations, you must start another LAN. For devices on one LAN to communicate with others on the second LAN, you must link the two. There are many ways to do this, depending on the architectures of the LANs, the cabling media, and the distance between the LANs.

Sometimes, your company may have merged with another. The two LANs to be interconnected may be dissimilar and geographically distinct. In this case, you might even be forced to link both LANs to a WAN. If your company has a large sales force always on the move, you should consider adding a communications server to provide dial-in access to the LAN/WAN.

Repeaters, Bridges, Routers, Brouters, And Gateways

In Chapter 5, you learned the difference between repeaters, bridges, routers, brouters, and gateways. It is important to remember their functions because it will affect which one you use to connect LANs to other LANs, to join LANs to WANs, to extend cable beyond its distance limitation, and to reduce network traffic.

Repeaters work at the Physical layer of the OSI model, bridges work at the Data Link layer, and routers work at the Network layer. Gateways tend to work at the Application layer performing protocol conversion, but they may act at all seven layers.

The distance limitations of various media types are due to signal attenuation, which is dictated by the media composition. Repeaters are used to extend the distance that a signal can travel by regenerating the signal before sending it to the neighboring cable segment. They perform no segmentation or traffic arbitration, but rather regenerate and pass along everything that comes in. Segments that are joined by a repeater must be of the same media access scheme, protocol, and transmission type, but can be of dissimilar media type (for example, a repeater could connect 10BaseT to 10Base2).

Bridges are needed to connect networks and to provide network segmentation. Bridges can connect dissimilar media and they maintain tables of MAC addresses. Bridges will not pass data across a segment if the source and destination are on the same segment. When a bridge handles error correction, performance improves because the bridge (rather than end devices) checks for errors that might lead to a request for retransmission. Therefore, a bridge is a good choice to improve network performance because it improves performance and is less expensive than a router.

Routers are often confused with bridges, but they perform more functions more intelligently. Routers are able to accommodate multiple paths between network segments, allowing packets to take the best possible route between sender and receiver. Bridges can't take advantage of multiple paths simultaneously. Routers also provide flow control, filtering, and broadcast management, so they are sometimes used to decrease network traffic propagation or for additional firewalling in a TCP/IP network. But routers, which work at higher layers of the OSI model, distinguish protocols and are not suitable in a NetBEUI network.

Brouters combine the characteristics of a bridge and a router, so they are a good choice for complex networks with several protocols because they can provide bridging functions for one protocol and routing functions for another.

Gateways are typically used to translate between dissimilar protocols, data structures, languages, or architectures. A gateway may be software or strictly hardware. The most common example would be setting up a Windows NT Server to act as a gateway for a Novell NetWare network, so that the Microsoft clients can access the NetWare resources without adding software to the workstation. Another common example would be connecting

email systems, such as Microsoft Mail and cc:Mail, so that users can send mail to other email users, regardless of what email package sender and receiver may use.

Finally, you would use a multiplexer to combine several data channels for transmission across a high-speed data link, such as a T1 or frame relay line. It is possible and sometimes cost effective to combine voice, data, and video on the same WAN link by using a multiplexer. The multiplexer will combine data streams from different sources into one feed for transmission over a WAN link.

Planning For Successful Deployment

Here are several factors to consider when planning for a network installation:

- Cabling
- Topology
- Network operating system
- Software and hardware
- Fault tolerance, disaster recovery, and security
- Protocols
- User requirements
- Administration

To plan for a successful network installation, you would:

1. **Conduct a survey of existing conditions.** This step is crucial to determining the parameters within which you must work. Remember each of the factors listed earlier. The existing conditions form the framework for any network design.
2. **Document the network requirements.** Again, using the already mentioned guidelines, be sure to document the following items:
   - How many computers are currently in use and how many are expected for the future?
   - What type of computers are involved?

- What special peripherals are required?
- Will the LAN be tied to a mainframe or a WAN?
- What software is in use or expected to be used?
- What type of administrative control is necessary?
- What level of resource sharing will be required?

3. **Select the network operating system (NOS).** This is the next step because it dictates what types of file server hardware you will need and which transport protocols you will support. Make sure the NOS can serve your existing and future network requirements and will be supported for a long time to come. Also, consider the administrative burden that the network operating system may create.
4. **Plan the logical network.** This involves choosing a transport protocol and data link technologies, dividing the network into subnets if necessary, and choosing security domains.
5. **Determine the network technology.** This is often the most difficult step, because it involves planning for unknowns. Estimating client loads and determining what technologies will support those loads is tough when you must estimate capacities. For instance, although a Token Ring network delivers a faster bit rate than an Ethernet network, workstations must wait for the token to begin transmission, which may make the Ethernet appear more responsive. Token Ring networks load in a simple, deterministic manner when clients are added, whereas overloaded Ethernet networks can cease functioning altogether.
6. **Plan the physical plant.** The environment, as well as the chosen network architectures, dictate what cabling media and topology are required. User and corporate requirements necessitate how and where the file servers, hubs, routers, and switches are stored and maintained.
7. **Select a file server hardware platform.** Make sure that all hardware is listed on Microsoft's Hardware Compatibility List (HCL), which you can find on the Web, on the TechNet CD, or supplied by your local Microsoft dealer or VAR. This simple step will save you a lot of grief when it's time for technical support.
8. **Determine storage requirements.** Again, this is tough to do for a new installation because there is no background data. Use the guidelines given for the network operating system

you've chosen and the manufacturer's data supplied with your file server hardware. Then, plan to double your storage every year. Make sure you have adequate RAM to support your storage requirements.

9. **Plan client support.** Use this planning time to focus on completing migration from 16-bit to 32-bit Windows-based applications. Make sure your clients can support new technology. To productively run databases, browsers, and other common applications, the majority of the desktops today should be Intel 486 (or equivalent) or higher, with a minimum of 16 MB of RAM and compatible hardware and software. Make sure your routers support all the protocols your network will need.

Practice Questions

Question 1

The Enormous Corporation is moving from NetWare 3.12 to Windows NT. Due to its terrible environmental record, the corporation is constantly involved in lengthy lawsuits. The company legal department is worried about confidential information placed on corporate file servers and would like to secure that information from everyone except itself. The company would also like to be able to use Internet email to share information, because it is a geographically diverse company, but it is afraid of hackers. What security measures should be implemented in this situation? [Check all correct answers]

- ❑ a. Gateway Service For NetWare
- ❑ b. Encryption
- ❑ c. User-level permissions
- ❑ d. File-level permissions

Both b and c are correct. User-level permissions imply that a file server has authenticated security based on a predefined set of criteria. Also, they are more secure than file-level permissions, answer d. Because user-level permissions don't trust even the network administrator with this information, encryption (answer b) would safeguard the files kept on the server as well as let the lawyers send Internet email securely. Gateway Service For NetWare would be required for access to the remaining NetWare servers, but it would not provide the required security.

Question 2

The XYZ Graphical Design firm is building a new, state-of-the-art facility to house its growing business. It is going to use a combination of NetWare and Windows NT servers on its network and would like all servers to reside on a 100 Mbps backbone. The rest of the company will be using 10 Mbps Ethernet for now, but may require higher bandwidths in the future. What is the appropriate cabling type for this situation?

- ❍ a. RG-58 A/U
- ❍ b. UTP CAT3
- ❍ c. UTP CAT4
- ❍ d. UTP CAT5

Answer d is the correct choice. CAT5 cabling is suitable for 100 Mbps bandwidth and is less expensive to install than fiber optics. RG-58 A/U is a coaxial cable used for Thinnet Ethernet networks and is not suitable for higher bandwidths. Therefore, answer a is incorrect. CAT3 unshielded twisted-pair is capable of carrying 10BaseT, but it's not recommended for higher bandwidths. Therefore, answer b is incorrect. CAT4 is not a deployed wiring standard. Therefore, answer c is incorrect.

Question 3

Consider the following situation:

You work for a medical clinic that supports patients around the clock. You are installing twisted-pair Ethernet in a new wing of the building. There will be 25 machines in the addition, but that number is expected to double in the first year. There has been some concern about disaster recovery due to recent events in the news. Due to patient confidentiality, tape backups are kept on site. Cost is not a consideration.

Required Result:

- Increase the level of fault tolerance for your file servers to the highest degree possible.

Optional Desired Results:

- You want to plan for the expected growth.
- You need to maintain a high level of security.

Proposed Solution:

- Implement a RAID 5 disk array for all file servers in the clinic.

Which results does the proposed solution produce?

❍ a. The proposed solution produces the required result and produces both of the optional desired results.

❍ b. The proposed solution produces the required result and produces only one of the optional desired results.

❍ c. The proposed solution produces the required result but does not produce any of the optional desired results.

❍ d. The proposed solution does not produce the required result.

The correct answer is d. The proposed solution would not be completely fault tolerant in the case of the failure of more than one drive. The correct solution would be to install RAID 1 array, which is complete disk mirroring. Another option would be to maintain hot spares for all network equipment.

Question 4

You want to connect a small Token Ring network with an Ethernet network, both of which use NetBEUI. You want to implement filtering to control network traffic. Which device should you use to accomplish this?

- ❍ a. A repeater
- ❍ b. A router
- ❍ c. A gateway
- ❍ d. A bridge

The correct answer is d because a bridge can connect two network segments and provide filtering to limit network traffic. The answer cannot be b because NetBEUI is not routable. A repeater cannot connect two dissimilar media access schemes and a gateway will not provide filtering. Therefore, answers a and c are also incorrect.

Question 5

You are the administrator for a small insurance office with a 27-node LAN. You currently have a single 10Base2 Ethernet segment installed in your office, running Novell NetWare 3.12, to which all networked devices are attached. Your boss announced at the last staff meeting that business is booming and your office will be adding four more agents next month. You plan to add four machines to the existing segment. How will you accomplish this?

- ❍ a. A T-connector
- ❍ b. A router
- ❍ c. A repeater
- ❍ d. A bridge

The correct answer is c, because there can be no more than 30 stations per 10Base2 segment. If you added a thirty-first station using a T-connector, as mentioned in answer a, you would have experienced intermittent problems or a complete network failure. A router or bridge, although they can link Ethernet segments, is not the best solution here.

Question 6

Your company has merged with the Enormous Corporation. You have implemented Microsoft Mail for the company's email and have spent a considerable amount of training dollars on your end-users. The new parent corporation email standard is cc:Mail. What device will be required to connect the dissimilar email systems, so that your users can retain their current mail system and communicate with the new administration?

- ❍ a. A gateway
- ❍ b. A router
- ❍ c. Microsoft Services For Lotus
- ❍ d. A MIME repeater

The correct answer is a. A gateway is needed to provide conversion because those functions would typically be performed at the highest layer of the OSI model, the Application layer. A router would simply route data packets, without application translation. Microsoft Services For Lotus and MIME repeaters do not exist.

Question 7

You have been hired as a consultant for the new Widget manufacturing company. This company will be moving into a pre-fabricated building in a month, and you must have the cabling in place for a twisted-pair Ethernet network. The four divisions of the company are Accounting, Administration, Sales, and Assembly Line. The company wants to give the employees a lot of latitude to use network resources freely, but accounting doesn't want anyone to see how much commission the sales staff makes. You have selected Microsoft Windows NT as your network operating system. Which security model should you implement?

- ❍ a. Domain-level security
- ❍ b. Inherited-rights security
- ❍ c. Share-level security
- ❍ d. User-level security

The correct answer is c, share-level security. This level of security involves assigning a password to selected shared resources, giving the owner of the

share control over access permissions for other users. Domain-level security and inherited-rights security do not exist in a Windows NT network. User-level security (access permissions) is very extensive, providing a great deal of control over access rights, but it usually requires administrative overhead that may not be appropriate for a small network, especially one where the culture supports less security, rather than more.

Question 8

The auditing firm of Dewie, Cheatam & Howe has hired you to install a temporary network for a two-month assignment. The company will be setting up seven computers in an unused boardroom that is not presently cabled for network use. What topology should you choose?

- ❍ a. Bus
- ❍ b. Mesh
- ❍ c. Ring
- ❍ d. Star-bus

The correct answer is a because a bus topology is the easiest and cheapest to install. There are no widely available commercial mesh topologies, which disqualifies b from further consideration. Both ring and star topologies usually require ancillary equipment, making them too expensive (and therefore less suitable) for a temporary network.

Question 9

Because its new operations in Las Vegas have been so successful, the Dewie, Cheatam & Howe accounting firm has decided to open another local office in Phoenix and relocate some of its employees from the corporate main offices in Hawaii. A high-speed data link will be needed to connect each of the mainland locations to the main offices on the islands. The company wants to take advantage of its low-cost T1 rates to link both voice and data on the same carrier signal. What type of device should the firm use?

- ❍ a. A repeater
- ❍ b. A bridge
- ❍ c. A gateway
- ❍ d. A multiplexer

A repeater will not aggregate various channels onto one data stream, which is the primary requirement. Neither a bridge nor a gateway will combine multiple signals over a single transmission link, but a multiplexer, answer d, will. This can be implemented in software, but is usually a combination of software and hardware.

Question 10

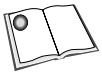
You have been managing a successful, efficient network for more than two years at your division of the Enormous Corporation. But because of the last mega-merger, your end-users have been complaining of slow network response times and strange, unrepeatable errors. Mr. Scrooge, your CFO, doesn't believe in spending money on frivolous software monitoring and administration tools. Fortunately, you have installed a Microsoft Windows NT network. What tools would you use to detect the potential problem(s)?

- ❍ a. A network analyzer
- ❍ b. Performance Monitor
- ❍ c. A cable tester
- ❍ d. User Manager For Domains

The correct answer is b. Performance Monitor is the only network monitoring tool that comes built-in to Windows NT. Although the User Manager For Domains is also built-in, it does not include problem diagnosis capabilities.

Need To Know More?

Chellis, James, Charles Perkins, and Matthew Strebe: *MCSE: Networking Essentials Study Guide, 2nd Edition*. Sybex Network Press, San Francisco, CA, 1998. ISBN 0-7821-2220-5. Chapter 5, "Designing the Local Area Network," contains excellent coverage of the various topics contained within this chapter.



Microsoft Press: *Networking Essentials, 2nd Edition*. Redmond, WA, 1997. ISBN 1-57231-527-X. Unit 1, Lesson 3, "Network Design," discusses all of the topics in this chapter in great detail.

Search the TechNet CD (or its online version through www.microsoft.com) using the keywords "Planning," "Token Ring," "Thinnet," and related product names. The Windows NT *Concepts and Planning Manual* also includes useful information on networking concepts.