CHAPTER 9
WIDE AREA NETWORKS

Chapter Summary

The Wide Area Network (WAN) is a key part of the enterprise edge. Most organizations do not build their own WAN communication circuits, preferring instead to lease them from common carriers or to use the Internet. This chapter focuses on the WAN architectures and telecommunications services offered by common carriers for use in enterprise WANs, not the underlying technology that the carriers use to provide them. We discuss the three principal types of WAN services that are available: dedicated-circuit services, packet-switched services, and virtual private network (VPN) services. We conclude by discussing how to improve WAN performance and how to select services to build WANs.

Learning Objectives

After reading this chapter, students should:

- Understand dedicated-circuit services and architectures
- Understand packet-switched services and architectures
- Understand Internet-based VPN services and architectures
- Understand the best practice recommendations for WAN design
- Be familiar with how to improve WAN performance

Key Terms

access VPN
Canadian Radio-Television and Telecommunications Commission (CRTC)
channel service unit/data service unit (CSU/DSU)
committed information rate (CIR)
common carrier
dedicated-circuit services
discard eligible (DE)
Ethernet services
Encapsulating Security Payload (ESP)
extranet VPN
Federal Communications Commission (FCC)
fractional T1 (FT1)
frame relay
full-mesh architecture
interexchange carrier (IXC)
Internet Service Provider (ISP)
intranet VPN
IPSec
L2TP
latency
layer-2 VPN
layer-3 VPN
local exchange carrier (LEC)
maximum allowable rate (MAR)
mesh architecture
multiprotocol label switching (MPLS)
packet assembly/disassembly (PAD)
packet services
Packet-switched services
partial-mesh architecture
permanent virtual circuits (PVC)
point of presence (POP)
public utilities commission (PUC)
ring architecture
star architecture
switched virtual circuit (SVC)
synchronous digital hierarchy (SDH)
synchronous optical network (SONET)
T carrier circuit
T1, T2, T3, T4 circuits
virtual private network (VPN)
VPN gateway
VPN software

Chapter Outline

1. Introduction
2. Dedicated-Circuit Networks
   a. Basic Architecture
   b. T Carrier Services
   c. SONET Services
3. Packet-Switched Networks
   a. Basic Architecture
   b. Frame Relay Services
   c. Ethernet Services
   d. MPLS Services
   e. IP Services
4. Virtual Private Networks
   a. Basic Architecture
   b. VPN Types
   c. How VPNs Work
5. The Best Practice WAN Design
6. Improving WAN Performance
   a. Improving Device Performance
   b. Improving Circuit Capacity
   c. Reducing Network Demand
7. Implications for Management

8. Summary

Answers to Textbook Exercises

Answers to End-of-Chapter Questions

1. What are common carriers, local exchange carriers, and interexchange carriers?

   A common carrier is a private company that sells or leases communication services and facilities to the public. Common carriers are profit-oriented, and their primary products are services for voice and data transmissions, both over traditional wired circuits as well as cellular services. Common carriers often supply a broad range of computer-based services, such as the manufacturing and marketing of specialized communication hardware and software. Common carriers that provide local telephone services are commonly called local exchange carriers (LEC), while carriers that provide long distance services (e.g., Sprint) are commonly called interexchange carriers (IXC). As the LECs move into the long distance market and IXCs move into the local telephone market, this distinction may disappear.

2. Who regulates common carriers and how is it done?

   Most countries have a federal government agency that regulates data and voice communications. In the United States, the agency is the Federal Communications Commission (FCC); in Canada it is the Canadian Radio-Television and Telecommunications Commission (CRTC). The FCC regulates interstate and international communications to and from the United States. State Public Utilities Commissions (PUCs) regulate intrastate communications within their states. Regulation is achieved on the basis of tariffs filed and approved (or disapproved) by the FCC and PUCs.

   Most countries have a federal government agency that regulates data and voice communications. In the United States, the agency is the Federal Communications Commission (FCC); in Canada it is the Canadian Radio-Television and Telecommunications Commission (CRTC). Each state or province also has its own public utilities commission (PUC) to regulate communications within its borders.

   The FCC/CRTC differs from the state PUCs in the following way:

   - The FCC has regulatory powers to compel common carriers to conform to the Federal Communications Act of 1934 and its revisions. It regulates the tariffs for interLATA and international (calls to and from the United States) communications. These usually are referred to as long distance communications.
   - A state PUC sets the rules and regulates the tariffs for all communications in its individual state boundary.

   Note to the instructor: There may be some overlap between federal and state jurisdictions because you can have both intraLATA and interLATA communications take place entirely within one state.

3. How does MPLS work?

   It is sometimes called a layer 2.5 technology because it inserts four-byte header that contains its own information between the layer 2 frame and the layer 3 IP packet. With MPLS, the customer connects to the common carrier's network using any common layer 2 service (e.g., T carrier, SONET, ATM, frame relay, Ethernet). The carrier's switch at the network entry point examines the incoming frame and converts the incoming layer 2 or layer 3 address into an MPLS address label. This label and some other control information (e.g., quality of service (QoS)) form the MPLS header, which is inserted into the layer 2 frame for transmission inside the carrier's network.

4. Compare and contrast dedicated-circuit services, and packet-switched services.

   With dedicated circuit networks, a circuit is established between the two communicating computers. This circuit provides a guaranteed data transmission capability that was available for use by only those two computers and is assigned solely to that transmission. No other transmission is possible until the circuit is closed. In contrast, packet switched services enable multiple connections to exist simultaneously between computers over the same physical circuit or even over different physical circuits.

   With a *dedicated circuit network*, you lease circuits from common carriers for their exclusive use twenty-four hours per day, seven days per week. All connections are point to point, from one building in one city to another building in the same or a different city. The carrier installs the circuit connections at the two end points of the circuit and makes the connection between them. The circuits still run through the common carrier's cloud, but the network behaves as if you have your own physical circuits running from one point to another:

   - Dedicated circuits are billed at a flat fee per month and the user has unlimited use of the circuit.
   - Once you sign a contract, making changes can be expensive because it means rewiring the buildings and signing a new contract with the carrier. Therefore, dedicated circuits require more care in network design than switched circuits both in terms of locations and the amount of capacity you purchase.

   With *packet switched services*, the user again buys a connection into the common carrier cloud). The user pays a fixed fee for the connection into the network (depending upon the type and capacity of the service) and is charged for the number of packets transmitted.

5. Is a WAN that uses dedicated circuits easier or harder to design than one that uses packet-switched circuits? Explain.

   A WAN using dedicated circuits is harder to design than one that uses packet-switched circuits. With dedicated circuits, once you sign a contract, making changes can be expensive because it means rewiring the buildings and signing a new contract with the carrier. Dedicated circuits therefore require more care in network design than using packet-switched circuits. In addition, packet-switched networks enable packets from separate messages with different destinations to be interleaved for transmission, unlike dedicated circuits.

6. Compare and contrast ring architecture, star architecture, and mesh architecture.

A *ring architecture* connects all computers in a closed loop, with each computer linked to the next. The circuits are full duplex circuits. Computers in the ring may send data in one direction or the other depending upon which direction is the shortest to the destination.

Properties of the ring architecture (assuming a double ring structure):

- Messages can take a long time to travel from the sender to the receiver. Considering there are only two routes from any one computer to another, if one part of the circuit or any one computer becomes overloaded, traffic delays can build up very quickly.

- The double-ring structure offers redundancy. If a circuit fails, messages can travel to their destinations in the opposite direction (probably with a time and distance penalty). If the network is operating close to its capacity, this will dramatically increase transmission times because the traffic on the remaining part of the network may come close to doubling (because all traffic originally routed in the direction of the failed link will now be routed in the opposite direction through the longest way around the ring).

A *star architecture* connects all computers to one central computer that routes messages to the appropriate computer.

Properties of the star architecture:

- It is easy to manage because the central computer receives and routes all messages in the network.

- It can be faster than the ring network since, in general any message needs to travel through fewer circuits to reach its destination than is the case in the ring network). However, the star topology is the most susceptible to traffic problems because the central computer must process all messages on the network. The central computer must have sufficient capacity to handle traffic peaks or it may become overloaded and network performance will suffer.

- In general, the failure of any one circuit or computer affects only the one computer on that circuit.

- If the central computer fails, the entire network fails because all traffic must flow through it. It is critical that the central computer be extremely reliable.

In a *mesh architecture* (usually implemented as partial mesh architecture), every computer may be connected to any other computer. Typically many, but not all, computers are connected.

Properties of the mesh architecture:

- The effects of the loss of computers or circuits in a mesh network depend entirely upon the circuits available in the network. If there are many possible routes through the network, the loss of one or even several circuits or computers may have few effects beyond the specific computers involved. However, if there are only few circuits in the network, the loss of even one circuit or computer may seriously impair the network.

- In general, mesh networks combine the performance benefits of both ring networks and star networks. Mesh networks usually provide relative short routes through the network (compared to ring networks) and provide many possible routes through the network to prevent any one circuit or computer from becoming overloaded when there is a lot of traffic (compared to star networks in which all traffic goes through one computer).

- Since mesh networks use decentralized routing, each computer in the network performs its own routing. This requires more processing by each computer in the network than in star or ring networks as well as the "overhead" transmission of network status information (e.g., how busy each computer is), reducing network capacity.

7. What are the most commonly used T carrier services? What data rates do they provide?

T-Carrier Designation	**DS Designation**	**Speed**
	DS-0	64 Kbps
T-1	DS-1	1.544 Mbps
T-2	DS-2	6.312 Mbps
T-3	DS-3	33.375 Mbps
T-3	DS-4	274.176Mbps

8. Distinguish among T-1, T-2, T-3, and T-4 circuits.

A T-1 circuit (sometimes called a DS-1 circuit) provides a data rate of 1.544 Mbps. T-1 circuits can be used to transmit data, but often are used to transmit both data and voice. In this case, a time division multiplexer (TDM) provides 24 64 Kbps circuits. Digitized voice using pulse code modulation (PCM) requires a 64 Kbps circuit so a T-1 circuit enables 24 simultaneous voice channels.

A T-2 circuit transmits data at a rate of 6.312 Mbps. Basically, it is a multiplexed bundle of four T-1 circuits. A T-3 circuit allows transmission at a rate of 44.376 Mbps, although most articles refer to this rate as 45 megabits per second. This is equal to the capacity of 28 T-1 circuits. T-3 circuits are becoming popular as the transmission medium for corporate WANs because of their higher data rates. At low speed, these T-3 circuits can be used as 672 different 64 Kbps channels or voice channels. A T-4 circuit transmits at 274.176 Mbps, which is equal to the capacity of 178 T-1 circuits. Obviously, an organization using either T-3 or T-4 circuits must have a tremendous need to transmit very large quantities of data.

9. Describe SONET. How does it differ from SDH?

The synchronous optical network (SONET) has recently been accepted by the U.S. standards agency (ANSI), as a standard for optical transmission at gigabit per second speeds. The international telecommunications standards agency (ITU-T) also recently standardized a version of SONET under the name of synchronous digital hierarchy (SDH). SONET and SDH are very similar and can be easily interconnected. The SONET standard includes more data rates than the SDH standard. As with T carrier services, a CSU/DSU is needed to connect the user's network into the SONET/SDH circuit.

SONET transmission speeds begin at the OC-1 level (optical carrier level 1) of 51.84 Mbps. Each succeeding rate in the SONET fiber hierarchy is defined as a multiple of OC-1, with SONET data rates defined as high as OC-192 or about 10 Gbps. Each level above OC-1 is created by multiplexing. Although not yet available in all locations, SONET/SDH is available in most large cities worldwide.

10. How do packet-switching services differ from other wide area networks services?

Packet switched services are quite different from the other types of network services. For each of these three, dialed circuit services, dedicated circuit services, and circuit switched services, a physical circuit was established between the two communicating computers. This circuit provided a guaranteed data transmission capability that was available for use by only those two computers.

In contrast, packet switched services enable multiple connections to exist simultaneously between computers. With packet switched services, the user again buys a connection into the common carrier network. The user pays a fixed fee for the connection into the network and charged for the number of packets transmitted.

11. Where does packetizing take place?

Splitting messages into individual packets (packetizing) takes place at a packet assembly/disassembly device (PAD), which can be owned and operated by the customer or by the common carrier.

The PAD converts the sender's data into the network layer and data link layer packets used by the packet network and sends them through the packet switched network. At the other end, another PAD reassembles the packets back into the network layer and data link layer protocols expected by the destination and delivers it to the appropriate computer. This "packetizing" and re-assembly is almost instantaneous, and data are transmitted continuously. The PAD can translate between different data link layer protocols between the sender and the destination (e.g., ethernet at the sender and token ring at the receiver). It may also provide conversion from one code to another (i.e., ASCII to EBCDIC).

12. Compare and contrast frame relay, MPLS, SMDS, and Ethernet services.

Frame relay differs from traditional networks in three important ways. First, frame relay operates only at the data link layer. Frame relay, like other packet switched networks takes the incoming packets from the user network and converts them to its own packet structure for internal transmission. Frame relay uses variable length packets which adapt to the size of the incoming packet (up to 8K).

Second, frame relay networks do not perform error control. Virtually all other types of networks perform error checking at each computer in the network. Any errors in transmission are corrected immediately, so that the network layer and application software can assume error-free transmission. However, this error control is one of the most time consuming processes in a network. Most networks today are relatively error-free, so frame relay networks do not ensure error-free delivery of the packets (they do perform error checking, but simply discard packets with errors; they do not generate NAKs and ask for retransmission). It is up to the software at the source and destination to perform error correction and to control for lost messages. Since the user's data link packet remains intact, it is simple for the devices at the edge of the frame relay network to check the error control information in the user's data link layer packet to ensure that no errors have occurred and to request transmission of damaged or lost packets.

A third major difference is that frame relay defines two connection data rates that are negotiated per connection and for each virtual circuit as it is established. The committed information rate (CIR) is the data rate the circuit must guarantee to transmit. If the network accepts the connection, it guarantees to provide that level of service. Most connections also specify a maximum allowable rate (MAR), which is the maximum rate that the frame relay network will attempt to provide, over and above the CIR. The circuit will attempt to transmit all packets up to the MAR, but all packets that exceed the CIR are marked as discard eligible (DE). If the network becomes overloaded, DE packets are discarded. So while can transmit faster than the CIR, they do so at a risk of lost packets.

Switched Multimegabit Data Service (SMDS) is an unreliable packet service like ATM and frame relay. SMDS encapsulates incoming packets from the user's network with ATM-like 53-byte cells, although the address is different than an ATM address. The user's data link layer address is mapped to the SMDS address, which is used for transmission through the SMDS network. The SMDS cell is stripped off at the destination and the user's data link layer packet reassembled. Like ATM and frame relay, SMDS does not perform error checking; the user is responsible for error checking. SMDS provides only a connectionless datagram service.

Ethernet service networks bypass the PSTN; companies offering Ethernet/IP packet networks have laid their own gigabit Ethernet fiber optic networks in large cities. When an organization signs up for service, the packet network company installs new fiber optic cables from their city-wide WAN backbone into the organization's office complex and connect it to an Ethernet switch. The organization simply plus their network into their Ethernet switch and begins using the service. All traffic entering the packet network must be Ethernet using IP. Since most organizations today use Ethernet and IP in the LAN and BN environment, Ethernet/IP avoids the need to translate or encapsulate to generate addresses for LAN or BN traffic and gains in throughput. It avoids complexity, meaning that companies do not have to add staff knowledgeable in the different WAN protocols, software, and hardware these technologies require. This technology is offered by relatively new startup companies like Yipes.com.

MPLS is different in that it is designed to work with a variety of commonly used layer-2 protocols. The customer connects to the common carrier's network using any common layer-2 service. MPLS offers a wide range of speeds because it can run on a variety of physical circuits such as T-carrier and SONET.

13. Which likely to be the longer term winner, IP, MPLS, or Ethernet services?

    Each of these technologies has benefits and an argument could be made for each. As such, student answers will vary. IP seems to be a contender because the Internet utilizes TCP/IP. Ethernet has the advantage of being used heavily on LANs, so the protocol conversion doesn't have to occur. MPLS is a relatively new option and has the benefit of being able to work so closely with Layer 2 and Layer 3 protocols.

14. Explain the differences between CIR and MAR.

The committed information rate (CIR) is the data rate the circuit must guarantee to transmit. If the network accepts the connection, it guarantees to provide that level of service. Most connections also specify a maximum allowable rate (MAR), which is the maximum rate that the frame relay network will attempt to provide, over and above the CIR. The circuit will attempt to transmit all packets up to the MAR, but all packets that exceed the CIR are marked as discard eligible (DE). If the network becomes overloaded, DE packets are discarded. So while can transmit faster than the CIR, they do so at a risk of lost packets.

15. How do VPN services differ from common carrier services?

A type of VAN, called a virtual private network (VPN) (or sometimes software defined network) has emerged. VPNs provide circuits that run over the Internet but appear to the user to be private networks. Internet access is inexpensive compared to the cost of leasing dedicated circuits, circuit switched services, or packet switched services from a common carrier.

Different VPNs provide different services, but most offer packet switching hardware that will communicate via the Internet, or VPN services which you lease from the VPN in much the same way as leasing a service from a common carrier. These VPN hardware (or services) take your data, encrypt it, and send it through the Internet through a series of "tunnels" -- a virtual circuit through the Internet which constrains the source and destination to only those within the VPN.

16. Explain how VPN services work.

A virtual private network (VPN) provides the equivalent of private packet switched network over the public Internet. You establish a series of PVCs that run over the Internet, so that the network acts like a set of dedicated circuits over a private packet network.

With a VPN, you first lease an Internet connection at whatever access rate and access technology you choose for each location you want to connect. For example, you might lease a T-1 circuit from a common carrier that runs from your office to your Internet service provider (ISP). You pay the common carrier for the circuit and the ISP for Internet access. Then you connect a VPN device (a specially designed router or switch) to each Internet access circuit to provide access from your networks to the VPN. The VPN devices enable you to create PVCs through the Internet that are called *tunnels.*

The VPN device at the sender takes the outgoing packet and encapsulates it with a protocol that is used to move it through the tunnel to the VPN device on the other side (a technology focus box later in this chapter describes this process in more detail). The VPN device at the receiver, strips off the VPN packet and delivers the packet to the destination network. The VPN is transparent to the users; it appears as though a traditional packet switched network PVC is in used. The VPN is also transparent to the ISP and the Internet as a whole; there is a simply a stream of Internet packets moving across the Internet.

The primary advantages of the VPNs is low cost and flexibility. Because they use the Internet to carry messages, the major cost is Internet access, which is inexpensive compared to the cost of circuit switched services, dedicated circuit services, or packet switched services from a common carrier. Likewise, anywhere you can establish Internet service, you can quickly put a VPN.

There are two important disadvantages.

- Since traffic on the Internet is unpredictable, sometimes packets travel quickly and at other times they take a long time to reach their destination.
- Second, because the data travels on the Internet, security is always a concern. Most VPN networks encrypt the packet at the source VPN device before it enters the Internet and decrypt the packet at the destination VPN device.

17. Compare the three types of VPN.

Three types of VPN are in common use: intranet VPN, extranet VPN and access VPN.

- An *intranet VPN* provides virtual circuits between organization offices over the Internet. Each location has a VPN device that connects the location to another location through the Internet.
- An *extranet VPN* is the same as an intranet VPN except that the VPN connects several different organizations, often customers and suppliers, over the Internet.
- An *access VPN* enables employees to access an organization's networks from a remote location. Employees have access to the network and all the resources on it in the same way as employees physically located on network. The user connects to a local ISP that supports the VPN service via POTS, ISDN, or other circuit. The VPN device at the ISP accepts the user's login, establishes the tunnel to the VPN device at the organization's office, and begins forwarding packets over the Internet. An access VPN provides a more less expensive connection than having a national toll-free 800 number that connects directly into large sets of modems at the organization's office. Compared to a typical ISP-based remote connection, the access VPN is secure connection than simply sending packets over the Internet.

18. How can you improve WAN performance?

Improving the performance of WANs is handled in the same way as improving LAN performance. You begin by checking the devices in the network, by upgrading the circuits between the computers, and by changing the demand placed on the network. Below is the performance checklist for improving WANs.

Increase Computer and Device Performance

- Upgrade devices
- Change to a more appropriate routing protocol (either static or dynamic)

Increase Circuit Capacity

- Analyze message traffic and upgrade to faster circuits where needed
- Check error rates

Reduce Network Demand

- Change user behavior
- Analyze network needs of all new systems
- Move data closer to users

19. Describe five important factors in selecting WAN services.

Five important factors in selecting WAN services are vendor capabilities, network capacity, flexibility, control, and reliability. The best vendors provide high quality service, quickly respond to network problems, adapt to changing customer needs, and provide useful network management services along with the data transmission services.

There are a variety of services available at many different data transmission rates. Try to estimate the general capacity you need at each network site, and be aware that users' needs change. In general, dedicated circuits are much less flexible than switched services. Control is another important issue. With dedicated circuits, you have more control over how you messages get routed in the network because your computers do the routing. With switched services, the service provider is responsible for the routing, and, your messages get intermixed with those of other network users. The reliability of a network service both in terms of average error rates and any circuit failures is also important.

20. Are Ethernet services a major change in the future of networking or a technology blip?

It is reasonable to expect major changes in the future of networking with Ethernet services. Several carriers have announced that they intend to stop offering all services except Ethernet and Internet services. With the advent of Ethernet services such as YIPES, this offers a significant approach to networking because it offers a way to "slice" fiber services down to the 1 Mbit level. Thus the customer can dynamically allocate slices and pay for what is used without the costs of infrastructure change. Further, as organizational LANs heavily use Ethernet and IP in the LAN and BN environment, and the WAN packet network services (X.25, ATM, Frame Relay, and SMDS) use layer-2 protocols, it is likely that Ethernet services would be more attractive. Any LAN or BN traffic must be translated or encapsulated into a new protocol and destination addresses generated for the new protocol. This takes time, slowing network throughput. Thus, the advantage of Ethernet services in networking is that there is no translation prior to transmission, making the service appealing. Ethernet services will represent a new and very attractive WAN technology in the future.

21. Are there any WAN technologies that you would avoid if you were building a network today? Explain.

FDDI because of bandwidth issues and high hardware costs, Integration of transport favors technologies using IP addressing. At this point, the avoidance of ATM in newer networks is suggested since so much new development is using Ethernet.

22. Suppose you joined a company that had a WAN composed of SONET, T carrier and frame relay services, each selected to match a specific network need for a certain set of circuits. Would you say this was a well-designed network? Explain.

This depends on how suitable the various technologies are for the applications supports. Today, increasingly, network designers make decisions to reduce costs, gain reliability, and increase performance through network integration, dynamic allocation so that unused capacity much not be paid for, and failover capabilities.

23. It is said that frame relay services and dedicated-circuit services are somewhat similar from the perspective of the network designer. Why?

    They are both based on a single connection to the common carrier and provide similar transmission speed and reliability.

Mini-Cases

I. Cookies Are Us

Cookies are Us runs a series of 100 cookie stores across the Midwestern U.S. and central Canada. At the end of each day, the stores sends sales and inventory data to headquarters, which uses the data to ship new inventory and plan marketing campaigns. They have decided to move to a WAN. What type of a WAN architecture and WAN service would you recommend?

Based on limited application requirements, VPN or T-carrier services will work well. Each of these are relatively cheap and will suffice for the file transfers required daily at the headquarters site.

II. MegaCorp

MegaCorp is large manufacturing firm that operates 5 factories in Dallas, 4 factories in Los Angeles, and 5 factories in Albany, New York. It operates a tightly connected order management system that coordinates orders, raw materials, and inventory across all 14 factories. What type of a WAN architecture and WAN service would you recommend?

Student answers can vary on this one based on some assumptions that can be made related to the volume of data and current costs. T carrier services would be a good option, as these would provide the necessary bandwidth at a reasonable price. .

III. Sunrise Consultancy

Sunrise Consultancy is a medium-sized consulting firm that operates 17 offices around the world (Dallas, Chicago, New York, Atlanta, Miami, Seattle, Los Angeles, San Jose, Toronto, Montreal, London, Paris, Sao Paulo, Singapore, Hong Kong, Sydney, and Bombay). They have been using Internet connections to exchange email and files, but the volume of traffic has increased to the point that they now want to connect the offices via a WAN. Volume is low but expected to grow quickly once they implement a new knowledge management system. What type of a WAN topology and WAN service would you recommend? Why?

With Sunrise moving from the Internet to a Wide Area Network (WAN), I would suggest a Cloud-based design, as that will be the simplest method for the network manager to network in the nine independent offices.

IV. Cleveland Transit

Reread Management Focus 9-1. What other alternatives do you think Cleveland Transit considered? Why do you think they did what they did?
Cleveland Transit probably considered many of the packet-switched services. One of the main reasons they chose a SONET ring was because of the full-duplex ring which enables communication to continue even in the event of a circuit cut. Resiliency of the network is key due to the 24/7 requirement for the types of services that they require.

V. Air China

Reread Management Focus 9-2. What other alternatives do you think Air China considered? Why do you think they did what they did?
They probably considered many of the packet-switched services as they offer some of the same benefits. The selection of Frame Relay is not surprising because it is one of the more common world-wide and operates at sufficient speeds for this type of application.

VI. Marietta City Schools

Reread Management Focus 9-3. What alternatives do you think Marietta City Schools considered? Why do you think they did what they did?
They probably considered many of the packet-switched services as they offer some of the same benefits. They probably selected Ethernet because they probably are using Ethernet on their LANs so no protocol translation is required. In addition, the 1-10 Gbps speeds offer the service they need for the new application types they are considering.

VII. Cisco

Reread Management Focus 9-4. What other alternatives do you think that Cisco considered? Why do you think they did what they did?
They probably considered many of the packet-switched services as they offer some of the same benefits. They probably selected the MPLS option because they were able to utilize this option to provide a full mesh architecture to increase reliability, while at the same time increasing capability and flexibility, while keeping costs about the same.

Next Day Air Service Case Study

1. With your knowledge of NDAS's network, what service would you recommend for the future to connect the remote offices to the hubs at Atlanta and New Orleans and the hubs to the corporate office in Tampa? Will the current facilities be adequate?

Based on the traffic volume analyses done for this case study in earlier chapters, the existing facilities seem adequate for reasonable workload increases in the existing offices. As Next Day Air Service grows into a nationwide operation, however, the multiplexed circuits between Tampa/Atlanta and Tampa/New Orleans will have to be replaced. Additional offices can be handled by adding another circuit between the new office and the appropriate multiplexer hub in Atlanta or New Orleans. Also, more multiplexers might be added, as was discussed previously.

The current trend is to combine both voice and data communications onto a single network. To combine voice and data, the students might recommend acquisitions of an ISDN facility with basic 2B + D channel service linking each remote office to the appropriate hub. Each hub should be connected to the Tampa office using primary 23B + D channel service

Another alternative might be the acquisition of Megacom or WATS circuits, This would require incoming and outgoing Megacom circuits for interstate calling, as well as incoming and outgoing Megacom circuits for interstate calling.

Answers may vary. Encourage student discussion of other digital services, such as T-1 circuits, or packet switched services. Accept any reasonably justified alternative answer.

2. President Coone has just informed you that NDAS is considering placing several new offices in Chicago and Los Angeles. Each office would have its own LAN. What factors would

determine the use of a metropolitan area network (MAN) to connect NDAS offices in a single city together?
The key factors in determining the use of a MAN to interconnect NDAS offices in a single city are:

a. the availability of MAN services within the city
b. the cost of the MAN service (using the common carrier or even construction of NDAS's own MAN)
c. the estimated volume of the data to be transmitted between and among the LANs linked via MAN service
d. the need for dial-in and dial-out service on the LANs
e. the actual distances between LANs
f. the nature and cost of interfacing software and equipment needed to access the MAN
g. network management requirements for MAN integrated LANs
h. network reliability considerations for MAN integrated LANs
i. network security on MAN integrated LANs

The topic of MAN-linked LANs should lead to an interesting class discussion, especially if a local Bell Operating Company representative, knowledgeable about MAN services offered in your city, can be invited as class discussion moderator.

3. As the network plans become more global, what security issues become more of a concern?

The international nature of the expanded network creates a greater security concern for the company. Many countries overseas do not have the same security and privacy laws as we seen in the U.S. , making it much more difficult to capture and prosecute those attempting to breach security. Similarly, some cultures abroad don't consider hacking, copyright infringement, etc to be such a bad thing. Thus, as operations expand into these countries, more potential attacks are likely to occur.

Additional Content

Teaching Notes

I cover the material in this chapter evenly, but I omit the selecting WAN services. My primary goal is to have students understand the major differences between the general categories of services and to have some familiarity with the specific services offered. In many ways, dialed services and circuit switched services are the same and I point this out to students. Likewise, the data rates for many services are similar so I point out that most of the internal network "plumbing" uses 64 Kbps PCM circuits and this is why the data rates are similar. The primary differences are the connection features (dedicated, circuit switched, packet switched) and the way in which the services are marketed to the users.

Dedicated circuit services have remained mostly stable of the past few years, with the exception of ever increasing data rates. The only new entrant is DSL and its derivatives (e.g., ADSL, VDSL) and competitors (cable modems). This is an area to watch. There will be many new developments over the next few years as this technology matures.

Circuit switched technologies (i.e., ISDN) have now entered the main stream. I'm not sure ISDN will be that important over the next three years. If the RBOCs deploy ADSL as rapidly as some are planning to, then ADSL may eclipse ISDN. I read an article in a telecommunications magazine entitled "ISDN: We Hardly Knew You." There may be some truth in this.

War Stories

Installing ISDN

(Objective: illustrate the problems with ISDN)

A friend of mine who worked for AT&T attended a 2-day seminar on installing ISDN in New York. The entire first day (except for some introductory remarks) was spent watching the instructor call six different organizations to get provisioning information needed to connect the ISDN card to the telephone network and have it talk to the training organization's server over the ISDN line. I'm not joking. After six hours worth of phone calls and several incorrect responses to the instructor's questions requiring additional calls, the computer was finally able to talk with the organization's server. With stories like this, it is no wonder that organizations are looking toward ADSL rather than ISDN.