CHAPTER 1

Networking in the Enterprise

Objectives

Upon completion of this chapter, you should be able to answer the following questions:

- What is an enterprise?
- How does traffic flow in an enterprise network?
- How is traffic handled in an enterprise?
- How does an extranet compare to an intranet?
- What is a telecommuter, and what services does a telecommuter require?
- What is the importance of a VPN?

Key Terms

This chapter uses the following key terms. You can find the definitions in the Glossary.

business enterprise   page 4

enterprise   page 4

enterprise network   page 5

converged   page 5

mission-critical   page 5

enterprise-class   page 5

failover   page 5

hierarchical design model   page 6

access layer   page 6

distribution layer   page 6

core layer   page 6

Enterprise Composite Network Model (ECNM)   page 8

edge device   page 9

intrusion detection system (IDS)   page 9

intrusion prevention system (IPS)   page 9

failure domain   page 9

downtime   page 10

back-end network   page 10

intranet   page 12

extranet   page 12

packet sniffer   page 13

latency   page 14

Jitter   page 14

Quality of service (QoS)   page 14

Teleworking   page 15

telecommuting   page 15

teleworker   page 15

telecommuter   page 15

teleconferencing   page 15

virtual private network (VPN)   page 16

Enterprise networks provide application and resource support to local and remote users anywhere and at any time. Intranets and extranets form the structure of these networks and often incorporate both LAN and WAN technologies. Traffic flow patterns, both internal and external, must be controlled to provide an efficient and secure network. The enterprise network uses advanced security and networking technology to enable telecommuters to work securely and productively while away from the office.

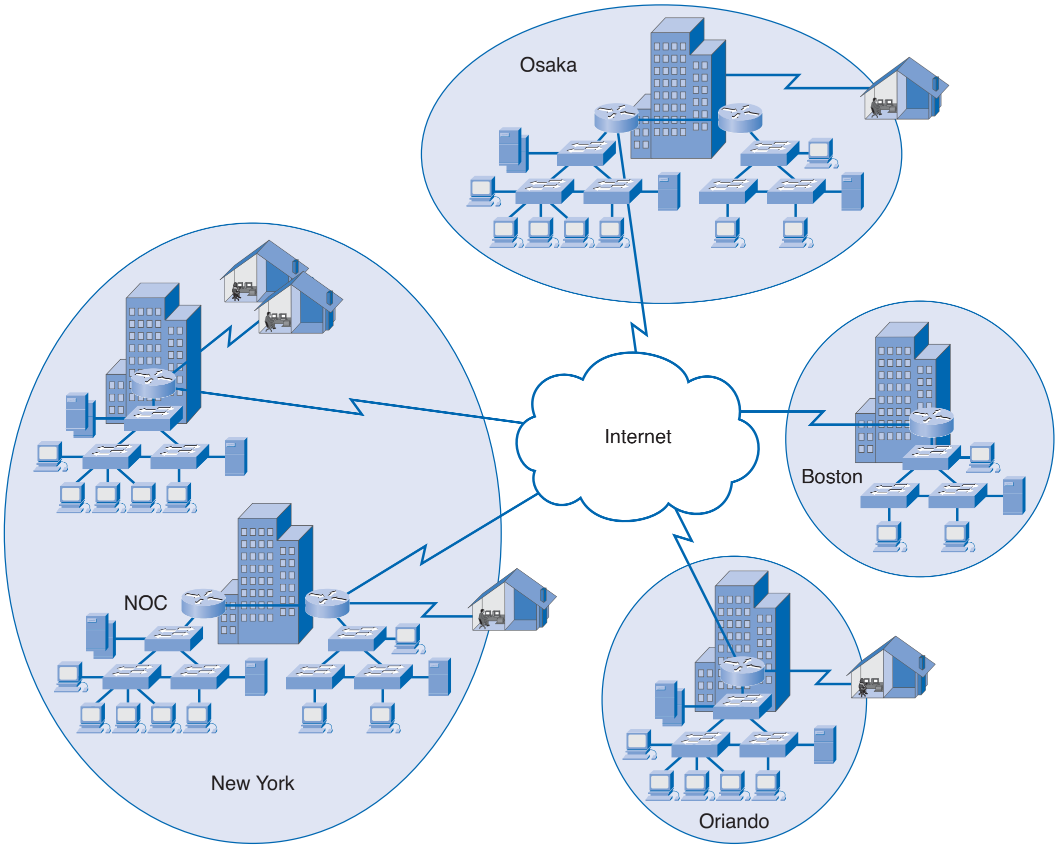
Part II of this book includes the corresponding labs for this chapter.

Describing the Enterprise Network

As businesses grow and evolve, so do their networking requirements. A large business environment with many users and locations, as shown in Figure 1-1, or one with many systems, is referred to as a ***business enterprise*** or more simply an ***enterprise***. Common examples of enterprise environments include the following:

- Manufacturers
- Large retail stores
- Restaurant and service franchises
- Utilities and government agencies
- Hospitals
- School systems

Figure 1-1 An Enterprise



These enterprises rely on their networks to provide access to shared resources and information. Without the network, many of the normal activities of the enterprise cannot be completed, resulting in substantial financial and customer base losses. Enterprise networks must be properly designed and maintained to reduce the chances of any outage.

Supporting the Business Enterprise

The network used to support the business enterprise is called an ***enterprise network***. Enterprise networks are designed to provide support for diverse business requirements and critical applications. They support the exchange of various types of network traffic, including data files, e-mail, voice, and video applications for multiple business units. To efficiently handle this ***converged*** network traffic, enterprise networks must have centralized control of devices and traffic.

Businesses increasingly rely on their network infrastructure to provide ***mission-critical*** services. Outages in the enterprise network can prevent the business from performing its normal activities, which can result in lost revenue and lost customers. Users are very intolerant of any outages in network services. In the enterprise environment, users have come to expect that network services will be available as designed 99.999 percent of the time. This means a maximum of just over five minutes of network outage in a year. Many service providers guarantee this level of service and enter into contractual agreements that result in severe financial penalties if this level of service is not maintained.

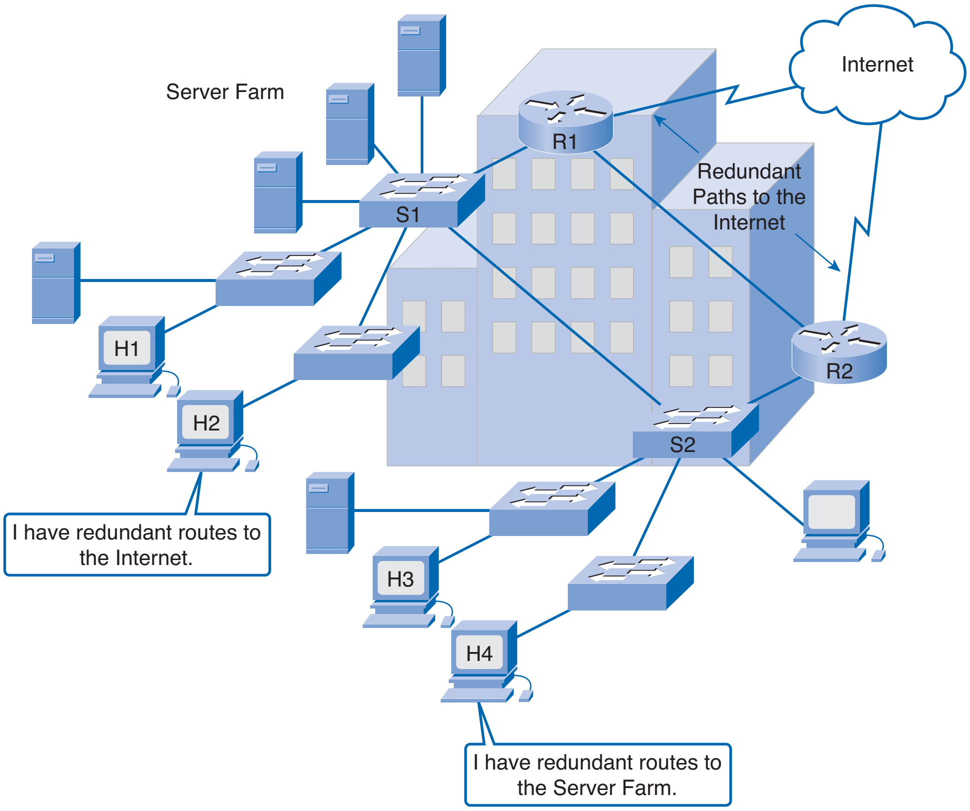
To obtain this level of reliability, high-end equipment is commonly installed in the enterprise network environment. Equipment installed in an enterprise network normally moves large volumes of network traffic, whereas the volume of traffic that moves in a nonenterprise environment is substantially less. This ***enterprise-class*** equipment is designed for reliability and stability, with features such as redundant power supplies and ***failover*** capabilities. Enterprise-class equipment is designed and manufactured to more stringent standards than lower-end devices.

Purchasing and installing enterprise-class equipment does not eliminate the need for proper network design. One objective of good network design is to prevent any single point of failure that could compromise network performance. This is accomplished by building redundancy into the network design as shown in Figure 1-2. When incorporating redundancy into a network design, it is important to consider not only the equipment but also all links. Other key factors in network design include optimizing bandwidth utilization, ensuring security, and network performance.

Traffic Flow in the Enterprise Network

To optimize available bandwidth on an enterprise network, the network must be organized so that traffic stays localized and is not propagated onto unnecessary portions of the network. Allowing traffic to flow onto network segments where it is not required or desired has many negative affects. The traffic consumes valuable bandwidth, thus decreasing network performance. If this decreased performance is not acceptable, additional bandwidth must be installed to compensate for the unwanted traffic, resulting in increased network costs. In addition, this traffic presents a security hazard in that it may contain confidential information or information about the structure of the network itself. An unscrupulous individual with sufficient technical knowledge could intercept this traffic and use it to compromise the integrity of the network or gain valuable information that could be financially devastating to the organization.

Figure 1-2 Redundancy in Network Design


Server Farm
Internet
R1
S1
Redundant Paths to the Internet
R2
S2
H1
H2
H3
H4
I have redundant routes to the Internet.
I have redundant routes to the Server Farm.

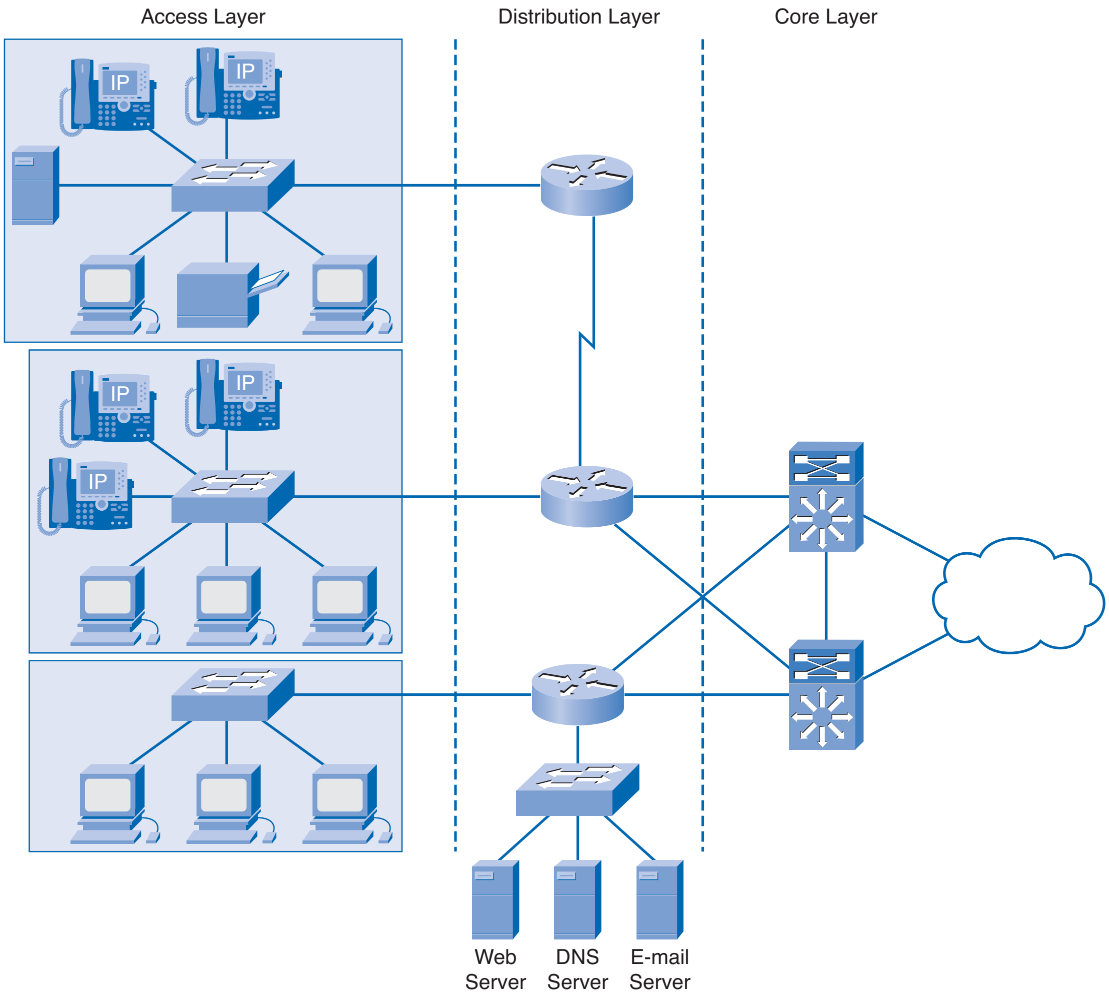
Using the three-layer ***hierarchical design model*** helps organize the network. This model divides the network functionality into three distinct layers: ***access layer***, ***distribution layer***, and ***core layer***, as shown in Figure 1-3.

Each layer is designed to meet specific functions. The access layer provides connectivity for the users. The distribution layer is used to forward traffic from one local network to another. Finally, the core layer represents a high-speed backbone layer between dispersed end networks. User traffic is initiated at the access layer and passes through the other layers only if the functionality of those layers is required. Even though the hierarchical model has three layers, some enterprise networks use the core layer services offered by an Internet service provider (ISP) to reduce costs.

Each layer is designed to meet specific functions. The access layer performs the following functions:

- Provides a connection point for end-user devices to the network
- Allows multiple hosts to connect to other hosts through a network device such as a switch
- Exists on the same logical network
- Confines traffic destined for a host on the same network to the access layer
- Passes traffic to the distribution layer for delivery if the message is destined for a host on another network

Figure 1-3 Three-Layer Hierarchical Design Model



The distribution layer performs the following functions:

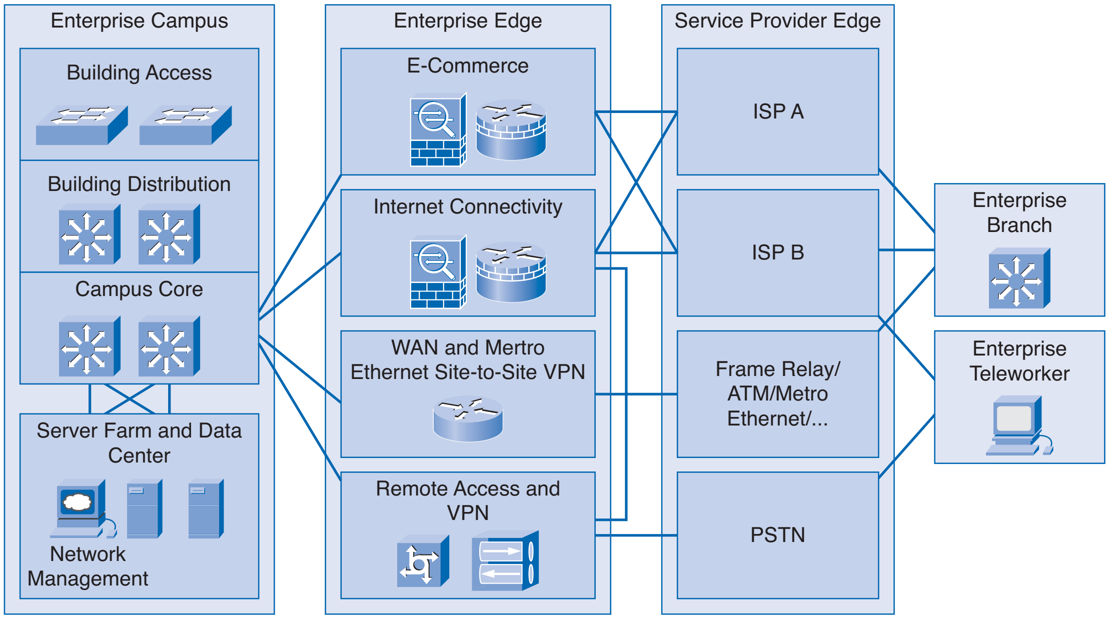
- Provides a connection point for separate local networks
- Ensures that traffic between hosts on the same local network stays local
- Passes on traffic destined for other networks
- Filters incoming and outgoing traffic for security and traffic management purposes
- Contains more powerful switches and routers than the access layer
- Passes data to the core layer for delivery to a remote network if the destination network is not directly connected

The core layer performs the following functions:

- Provides a high-speed backbone layer with redundant (backup) connections
- Transports large amounts of data between multiple end networks
- Includes very powerful, high-speed switches and routers
- Transports data quickly and reliably

The Cisco ***Enterprise Composite Network Model (ECNM)*** divides the network into functional components while still maintaining the concept of core, distribution, and access layers. The functional components of this model are the Enterprise Campus, Enterprise Edge, and Service Provider Edge, as shown in Figure 1-4.

Figure 1-4 Cisco Enterprise Composite Network Model



Enterprise Campus

The Enterprise Campus component consists of the campus infrastructure with server farms and network management. The Building Access module contains both Layer 2 and Layer 3 switches to provide the correct port density for the environment. This module is responsible for the implementation of VLANs and trunk links to the Building Distribution module.

The Building Distribution module uses Layer 3 devices to aggregate traffic from building access layers. Routing, access control, and quality of service (QoS) are all implemented by this module.

Redundancy of devices and links are important design considerations. The Campus Core module provides high-speed connectivity between Building Distribution modules, data center server farms, and the Enterprise Edge. Redundancy, fast convergence, and fault tolerance are the design goals of this module.

Network management continually monitors devices and network performance to ensure optimum operation. The server farm provides high-speed connectivity and protection for servers. It is important to provide redundancy, security, and fault tolerance in this area.

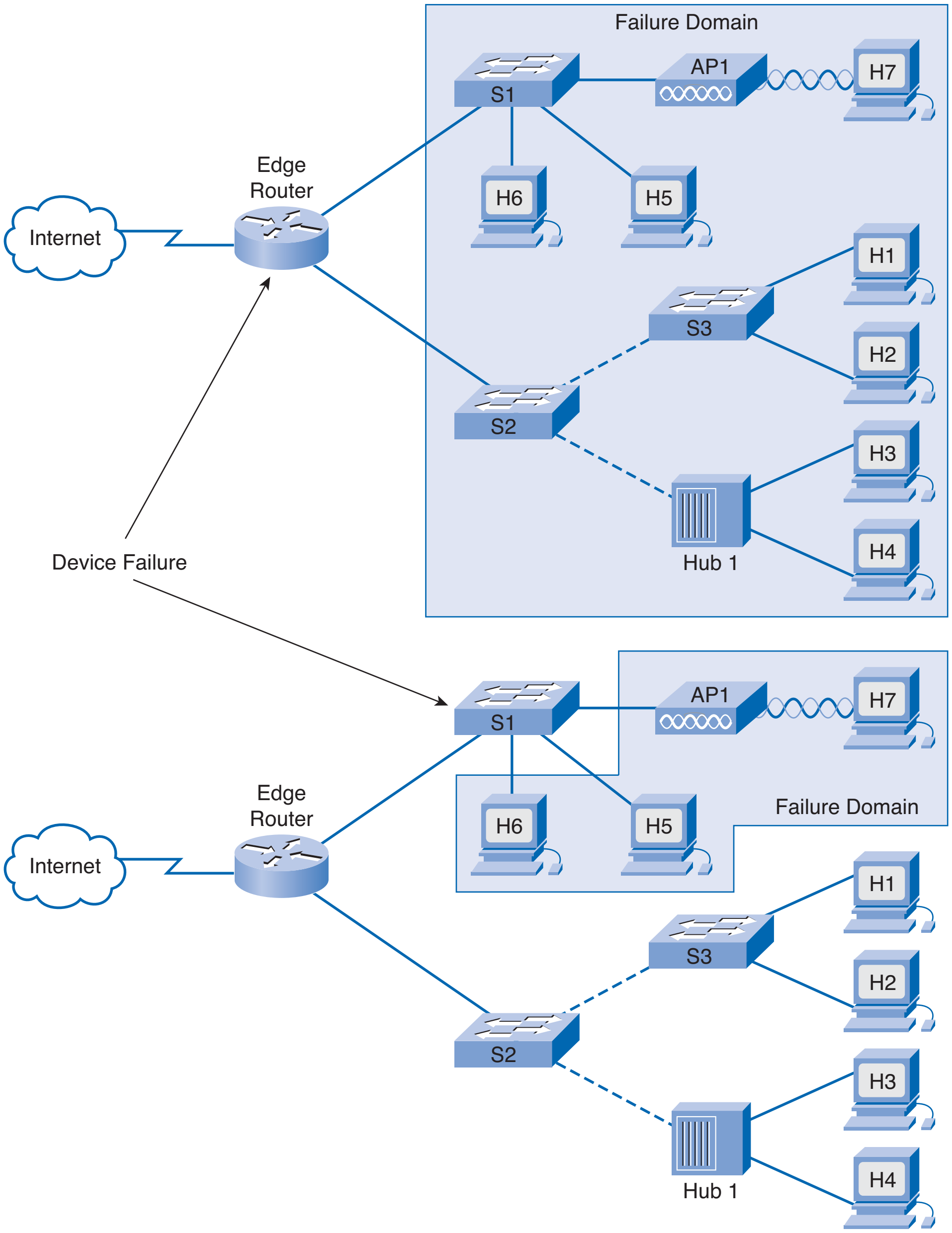
Enterprise Edge

The Enterprise Edge component consists of the Internet, E-commerce, VPN, and WAN modules connecting the enterprise with the service provider's network. This module extends the enterprise services to remote sites and enables the enterprise to use Internet and partner resources. It provides QoS, policy enforcement, service levels, and security.

All data that enters or exits the ECNM passes through an ***edge device***. This is the point at which all packets can be examined and a decision made as to whether the packet should be allowed on the enterprise network. For this reason, this is the location at which an ***intrusion detection system (IDS)*** or ***intrusion prevention system (IPS)*** is normally configured. These systems help protect the network against malicious activity.

A well-designed network not only controls traffic but also limits the size of failure domains. A ***failure domain*** is the area of a network impacted when a key device or service experiences problems. The function of the device that initially fails determines the impact of a failure domain. For example, a malfunctioning switch on a network segment normally impacts only hosts on that segment. However, if the router that connects this segment to others fails, the impact is much greater, as shown in Figure 1-5.

Figure 1-5 Failure Domains



The use of redundant links and reliable enterprise-class equipment minimizes the chance of disruption in a network. Smaller failure domains reduce the impact of a failure on company productivity. They also simplify the troubleshooting process, thereby shortening the ***downtime*** for all users.

Service Provider Edge

The Service Provider Edge component provides Internet, public switched telephone network (PSTN), and WAN services to the enterprise. This functional area represents connections to resources external to the campus. It facilitates communications to WAN and ISP technologies.

Packet Tracer
□ **Activity**

Observing the Traffic Flow in an Enterprise Network (1.1.2)

In this activity, you observe the flow of traffic through a network. Use file d3-112.pka on the CD-ROM that accompanies this book to perform this activity using Packet Tracer.

Enterprise LANs and WANs

Enterprise networks incorporate both traditional LAN and WAN technologies. In a typical enterprise network, multiple local networks at a single campus interconnect at either the distribution layer or the core layer to form a LAN. These LANs interconnect with other sites that are more geographically dispersed to form a WAN.

LANs are private and under the control of a single organization. The organization installs, manages, and maintains the wiring and devices that are the functional building blocks of the LAN. Some WANs are privately owned; however, because the development and maintenance of a private WAN is expensive, only very large organizations can afford to maintain a private WAN. Most companies purchase WAN connections from a service provider or ISP. The ISP is then responsible for maintaining the ***back-end network*** connections and network services between the LANs. Figure 1-6 shows a typical enterprise network.

When an organization has many global sites, establishing WAN connections and service can be complex. For example, the major ISP for the organization might not offer service in every location or country in which the organization has an office. As a result, the organization must purchase services from multiple ISPs. Using multiple ISPs often leads to differences in the quality of services provided. In many emerging countries, for example, network designers find differences in equipment availability, WAN services offered, and encryption technology available for security. To support an enterprise network, it is important to have uniform standards for equipment, configuration, and services.

With LAN technology, the organization has the responsibility of installing and managing the infrastructure. This technology functions mainly at the access and distribution layers, with Ethernet being the most commonly deployed LAN technology. The LAN connects users and provides support for localized applications and server farms. Connected devices are usually in the same local area, such as a building or a campus.

With WANs, connected sites are usually geographically dispersed. Connectivity to the WAN requires a device such as a modem or CSU/DSU to put the data in a form acceptable to the network of the service provider. Although some large organizations maintain their own WANs, these services are often provided by an ISP who has the responsibility of installing and managing the infrastructure. WAN services include T1/T3, E1/E3, digital subscriber line (DSL), cable, Frame Relay, and ATM. Figure 1-7 shows how edge devices convert between Ethernet encapsulation and serial WAN encapsulation as the traffic moves from the LAN to the WAN.

Figure 1-6 An Enterprise Network

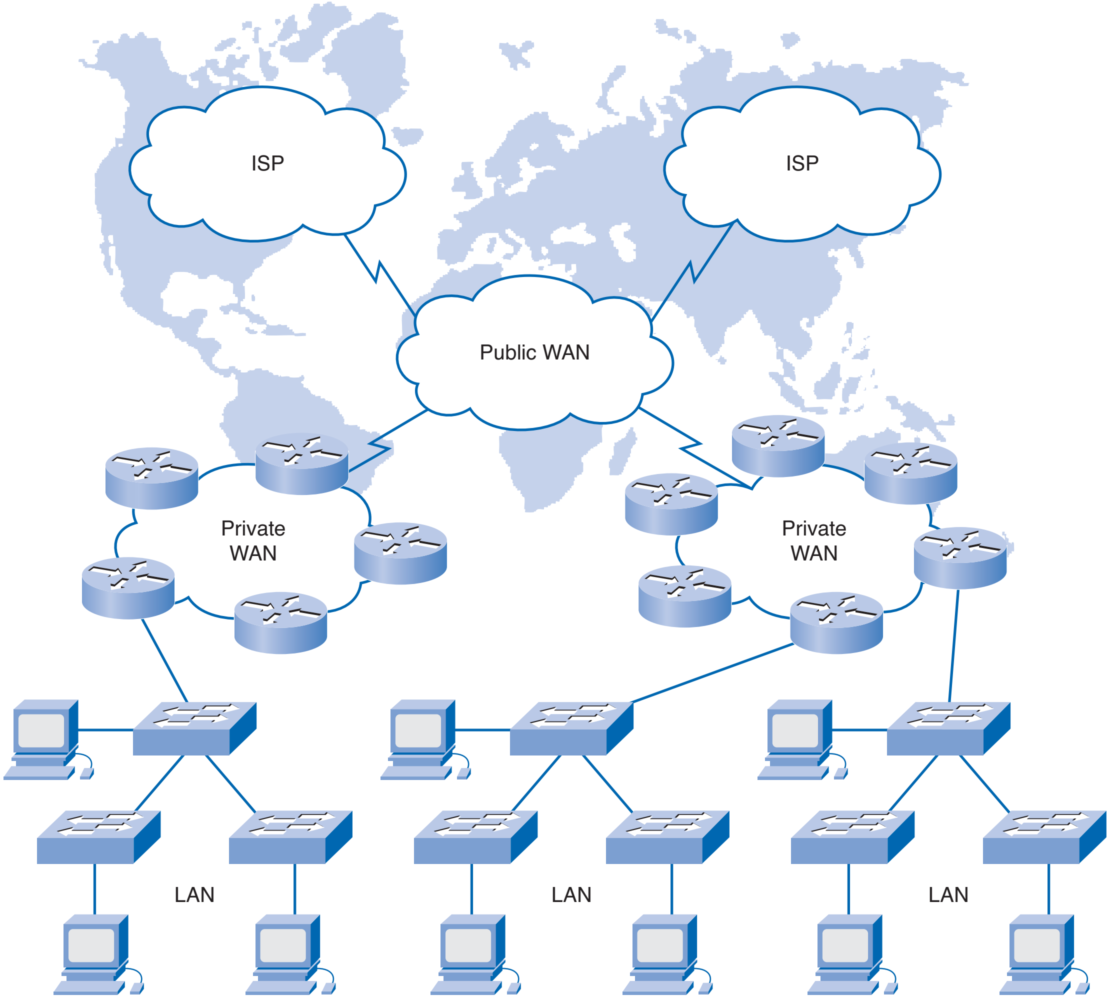
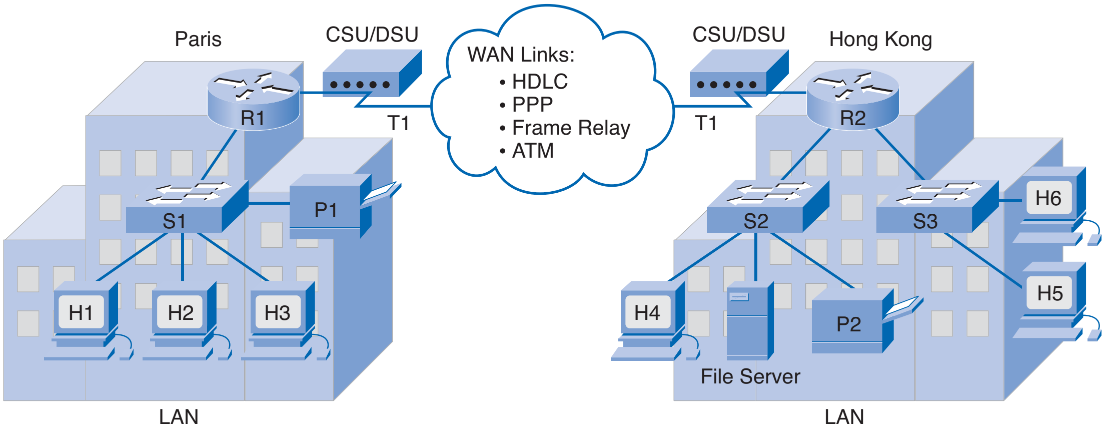


Figure 1-7 WAN Services



Interactive Activity 1-1: LAN and WAN Terminology (1.1.3)

In this activity, you identify the terms relating to LANs and WANs. Use file d3ia-113 on the CD-ROM that accompanies this book to perform this interactive activity.

Intranets and Extranets

Enterprise networks contain both WAN and LAN technologies. These networks provide many of the services associated with the Internet, including the following:

- E-mail
- Web
- FTP
- Telnet/SSH
- Discussion forums

Many companies use this private network or ***intranet*** to provide access for local and remote employees via both LAN and WAN technologies. Intranets may have links to the Internet. If connected to the Internet, firewalls control the traffic that enters and exits the intranet. Intranets contain confidential information and are designed for company employees only. The intranet should be protected by a firewall. Remote employees who are not physically connected to the enterprise LAN must authenticate before gaining access to the resources it provides.

In some situations, businesses extend privileged access to their network to key suppliers and customers. This access may be through direct WAN connections, remote login to key application systems, or through virtual private network (VPN) access into a protected network. An ***extranet*** is a private network (intranet) that allows controlled access to individuals and companies such as suppliers and contractors, outside the organization. An extranet is not a public network.

Identifying Enterprise Applications

Many different applications are required to support the modern enterprise. Each of these has very specific requirements of the underlying network. Regardless of the type of application, traffic generated by the application should be allowed only on portions of the network where it is required.

Traffic Flow Patterns

A properly designed enterprise network has well-defined and predictable traffic flow patterns. In some circumstances, traffic stays on the LAN portion of the enterprise network, and at other times it traverses the WAN links. When determining how to design the network, it is important to consider the amount of traffic destined for a specific location and where that traffic most often originates.

Some common traffic types that should remain local to users on the LAN include file sharing, printing, internal backup, mirroring, and intracampus voice. System updates, company e-mail, and transaction processing are also normally seen on a local network but are also sent across the enterprise WAN. In addition to WAN traffic, external traffic is traffic that originates from or is destined for the Internet. VPN and Internet traffic is considered external traffic flow.

Controlling the flow of traffic on a network optimizes available bandwidth and introduces a level of security through monitoring. By understanding traffic patterns and flows, the network administrator can predict the types and amount of traffic to expect on each portion of the network or through each device. When traffic is detected in an area of the network where it is unexpected, that traffic can be filtered and the source of the traffic investigated.

Interactive Activity 1-2: Traffic Flow Patterns (1.2.1)

In this activity, you identify the flow pattern for each type of traffic. Use file d3ia-121 on the CD-ROM that accompanies this book to perform this interactive activity.

Applications and Traffic on an Enterprise Network

At one time, voice, video, and data each traveled on separate networks, which could be optimized for the specific type of traffic. Now technology supports a converged network, where voice, video, and data flow across the same medium. This convergence presents many design and bandwidth management challenges. Enterprise networks must support the business enterprise by allowing traffic from a variety of applications, including the following:

- Database transaction processing
- Mainframe or data center access
- File and print sharing
- Authentication services
- Web services
- E-mail and other communications
- VPN services
- Voice calls and voicemail
- Video and videoconferencing

In addition, network management traffic and the control processes required for the underlying operation of the network must also travel across the network.

When trying to determine how to manage network traffic, it is important to understand the type of traffic that is crossing the network and the current traffic flow pattern. If the types of traffic are unknown, a technician can use a ***packet sniffer*** to capture traffic for analysis. To determine traffic flow patterns, it is important to capture traffic during peak utilization times to get a good representation of the different traffic types and to perform the capture on different network segments, because some traffic will be local to a particular segment.

Using the information obtained from the packet sniffer, network technicians can determine traffic flows. Technicians analyze this information based on the source and destination of the traffic and the type of traffic being sent. Technicians then use this analysis to decide how to manage the traffic more efficiently, such as filtering unnecessary traffic flows or changing flow patterns altogether by relocating a server or service to a different location on the network. Optimizing the network performance might require major redesign and intervention.

Lab 1-1: Capturing and Analyzing Network Traffic (1.2.2)

In this lab, you use Wireshark to capture and analyze protocol data packets as they cross the network. Refer to the hands-on lab in Part II of this *Learning Guide*. You may perform this lab now or wait until the end of the chapter.

Network Traffic Prioritization

Not all types of network traffic have the same requirements or behave in the same manner. For example, voice traffic is much less tolerant to loss and delay than is data traffic. The characteristics of the various types of network traffic must be clearly understood to design and construct a network capable of carrying converged network traffic.

Data Traffic

Most network applications use data traffic. Some types of online applications transmit data that is sporadic. Other types, such as data storage applications, transmit high volumes of traffic for a sustained period. Some data applications are more concerned about time sensitivity than reliability, and most data applications can tolerate delays. For this reason, data traffic usually uses TCP. TCP uses acknowledgments to determine when lost packets must be retransmitted and thus guarantees delivery. Although the use of acknowledgments makes TCP a more reliable delivery protocol, it also introduces a delay in the delivery of the data.

Voice and Video Traffic

Voice traffic and video traffic differ from data traffic. Voice and video applications require an uninterrupted stream of data to ensure high-quality conversations and images. The acknowledgment process in TCP introduces delays, which break these streams and degrade the quality of the application. Therefore, voice and video applications use the User Datagram Protocol (UDP) rather than TCP. Because UDP does not incorporate mechanisms for retransmitting lost packets, it minimizes delays.

In addition to understanding the delays of TCP versus UDP, it is necessary to understand the delay, or ***latency***, caused by the networking devices that must process the traffic on its path to the destination. Open Systems Interconnection (OSI) Layer 3 devices create more delay than Layer 2 devices because of the number of headers they have to process. Therefore, routers introduce a longer delay than switches. ***Jitter***, caused by network congestion, is the variation in the length of time packets take to travel from the source to the destination. It is important to reduce the impact of delay, latency, and jitter on time-sensitive traffic.

Quality of service (QoS) is a process used to guarantee adequate bandwidth to a specified data flows. QoS mechanisms sort traffic into different queues, based on priority. For example, voice traffic is given priority over ordinary data. The following list describes this process:

1. Inbound traffic is classified based on type. The traffic type is normally related to the application that generated the traffic and includes things such as voice, video, FTP, and Telnet. Some traffic may be discarded (filtered) at this step.

2. Classified traffic is placed into priority queues based on preconfigured priority levels. For example, voice traffic is very sensitive to delay, so it is placed in a higher-priority queue than FTP data.

3. Traffic in higher-priority queues is sent before traffic in lower-priority queues.

Interactive Activity 1-3: Traffic Prioritization Terminology (1.2.3)

In this activity, you match the traffic prioritization term to the correct definition. Use file d3ia-123 on the CD-ROM that accompanies this book to perform this interactive activity.

Supporting Remote Workers

The development of enterprise networks and remote connection technology has changed the way we work. ***Teleworking***, also referred to as ***telecommuting*** and e-commuting, allows employees to use telecommunications technology to work from their homes or other remote locations. The remote worker using the technology is called a ***teleworker*** or ***telecommuter***.

Teleworking

An increasing number of companies encourage their employees to consider teleworking. Teleworking provides many advantages and opportunities for both employer and employee. From the employer perspective, when employees work from home, the company does not have to provide them with dedicated physical office space. A single office space can be set up for shared use by employees who need to spend time in the physical office. This arrangement reduces real estate costs and the associated support services. Some companies have even reduced the expense of air travel and hotel accommodations to bring their employees together by using ***teleconferencing*** and collaboration tools. People from all over the world can work together as if they were in the same physical location.

Employees also benefit from teleworking. Employees save time and money, and reduce stress, by eliminating the daily travel to and from the office. Employees can dress casually at home, and thus save money on business attire. Working from home allows employees to spend more time with their families. Reduced travel for employees also has a favorable effect on the environment. Less airplane and automobile traffic means less pollution.

Not all individuals are suited to a teleworking environment. Teleworkers need to be self-directed and disciplined. Some teleworkers miss the social environment of an office setting and find it difficult to work in physical isolation. Not all jobs can take advantage of teleworking. Some positions require a physical presence in the office during a set period of time. However, more enterprises are taking advantage of technology to increase the frequency of telecommuting. Some of the basic teleworker tools follow:

- **E-mail**: Delivers a written message to a remote user for viewing and response at a later time
- **Chat**: Delivers a written message to a remote user in real time for immediate viewing and response
- **Desktop and Application Sharing**: Allows multiple uses to view and interact with the same applications simultaneously
- **FTP**: Transfers files between computers
- **Telnet**: Connects and starts a terminal session on a remote device
- **VoIP**: Allows real-time voice communication between users over the Internet
- **Videoconferencing**: Allows users in multiple locations to communicate face to face in real time

Application- and screen-sharing tools have improved, and it is now possible to integrate both voice and video into these applications. New technology has enabled more sophisticated levels of online collaboration. Using the enterprise network, this technology creates an environment in which individuals from remote locations meet as though they were in the same room. By combining large video displays and high-quality audio in specially designed rooms, it appears as if all participants, regardless of their physical location, are sitting across the boardroom table from each other.

Interactive Activity 1-4: Telecommuting Opportunities (1.3.1)

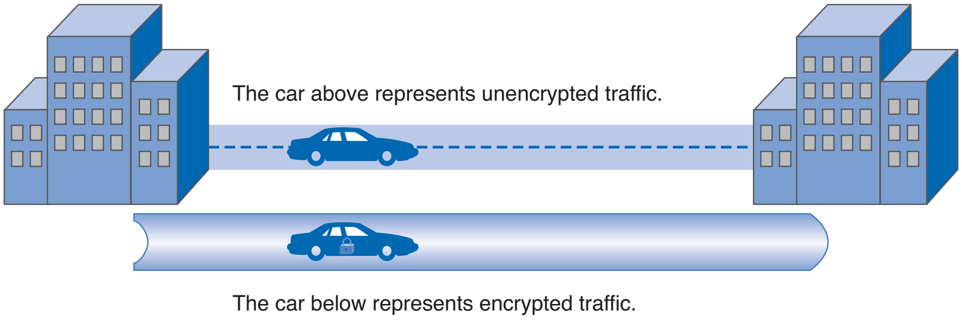
In this activity, you identify scenarios appropriate for telecommuting. Use file d3ia-131 on the CD-ROM that accompanies this book to perform this interactive activity.

Virtual Private Networks

One obstacle that teleworkers must overcome is the fact that most of the tools available for working remotely are not secure. Using nonsecure tools allows data to be intercepted or altered during transmission. One solution is to always use the secure forms of applications, if they exist. For example, instead of using Telnet, use Secure Shell (SSH). Unfortunately, secure forms of all applications may not be available. A much easier choice is to encrypt all traffic moving between the remote site and the enterprise network using a ***virtual private network (VPN)***.

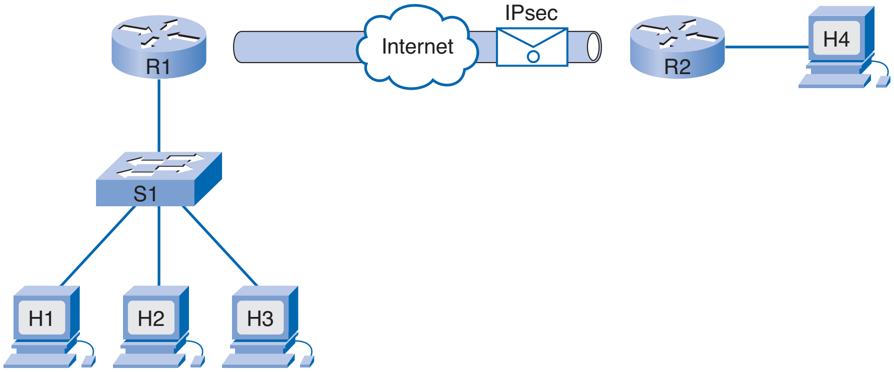
VPNs are often described as tunnels. Consider the analogy of an underground tunnel versus an open road between two points, as shown in Figure 1-8. Anything that uses the underground tunnel to travel between the two points is surrounded and protected from view. The underground tunnel represents the VPN encapsulation and virtual tunnel.

Figure 1-8 VPN Analogy


The car above represents unencrypted traffic.
The car below represents encrypted traffic.

When using a VPN, a virtual tunnel is created by linking the source and destination addresses. All data flow between the source and destination is encrypted and encapsulated using a secure protocol such as IPsec, as shown in Figure 1-9. This secure packet is transmitted across the network. When it arrives at the receiving end, it is de-encapsulated and unencrypted.

Figure 1-9 VPN Tunnel



VPNs are a client/server application; therefore, telecommuters must install the VPN client on their computers to form a secure connection with the enterprise network. When telecommuters are connected to the enterprise network through a VPN, they become part of that network and have access to all services and resources that they would have if they were physically attached to the LAN.

Note

One of the most common encapsulating protocols for VPNs is IPsec, which is short for IP Security. IPsec is a suite of protocols that provide many services, including the following:

- Data encryption
- Integrity validation
- Peer authentication
- Key management

Summary

Modern business enterprises rely on their networks for many business-critical applications. Failure of the network can result in both lost customers and lost revenue. For this reason, enterprise-class networks incorporate high-end, enterprise-class equipment and redundancy in their design. Enterprise-class networks are designed to provide an uptime of at least 99.999 percent.

Enterprise networks are composed of both LAN and WAN technology. They must provide services both to those physically connected to the network and to those working remotely. Intranets provide services only to employees of a company or organization. Extranets are intranets that have been extended to provide services to others directly involved in the business of the enterprise but who are not employees.

Enterprise networks can often span continents. Traffic flow patterns in these large enterprise networks must be carefully analyzed and controlled to optimize the available bandwidth and provide a reasonable level of security.

Networks carry many different types of traffic, each of which has different requirements for delivery. Some traffic, such as voice, is very intolerant to delay and must be given priority over more-tolerant traffic such as data packets. QoS is used to provide the prioritization of traffic.

Current network technology and security processes enable network services to be extended outside of the physical boundaries of the corporate office. These services can be made available to anyone at any time, thus enabling many individuals to work from remote locations. This working arrangement is known as teleworking or telecommuting. When working remotely, teleworkers should use the secure form of all applications such as SSH and HTTPS to minimize the possibility that data could be intercepted. Not all applications have a secure form, so VPN technology should be used to encrypt all traffic being sent across a nonsecure network.

Activities and Labs

Interactive Activities on the CD-ROM:

Interactive Activity 1-1: LAN and WAN Terminology (1.1.3)

Interactive Activity 1-2: Traffic Flow Patterns (1.2.1)

Interactive Activity 1-3: Traffic Prioritization Terminology (1.2.3)

Interactive Activity 1-4: Telecommuting Opportunities (1.3.1)

Packet Tracer
□ **Activity**

Packet Tracer Activities on the CD-ROM:

Observing the Traffic Flow in an Enterprise Network (1.1.2)

Hands-On Labs in Part II of This Book:

Lab 1-1: Capturing and Analyzing Network Traffic (1.2.2)

Check Your Understanding

Complete all the review questions listed here to check your understanding of the topics and concepts in this chapter. Appendix A, “Check Your Understanding and Challenge Questions Answer Key,” lists the answers.

1. Which type of network allows a customer to connect to a secure company website to check on a delivery date?

   A. LAN
   B. WAN
   C. Intranet
   D. Extranet

2. Which layer of the three-layer hierarchical design model is used to filter FTP traffic from a specific host?

   A. Access
   B. Distribution
   C. Core
   D. Aggregation

3. In the ECNM, where should an IPS or IDS be configured?

   A. Enterprise Campus
   B. Enterprise Edge
   C. Service Provider Edge
   D. WAN Edge

4. In the ECNM, where should QoS be implemented?

   A. Building Access module
   B. Building Distribution module
   C. Campus Core module

5. Which tool would enable a teleworker to communicate in real time with a colleague?

   A. FTP
   B. E-mail
   C. Chat
   D. Telnet

6. What type of traffic, if found on an enterprise WAN link, indicates a problem with the network design? Choose all that apply.

   A. Departmental file sharing
   B. Printing
   C. Internal backup
   D. Intracampus voice

7. Why should remote workers use VPN technology to connect to the home network?

8. Why does voice traffic use UDP but FTP uses TCP?

9. What should be done if unexpected traffic types are found on a network segment?

10. Why is it important to limit the size of failure domains when designing a network?

Challenge Questions and Activities

These questions require a deeper application of the concepts covered in this chapter. You can find the answers in Appendix A.

1. You have just been hired by AnyCompany, and your first task is to determine why end users are reporting that the company network is "slow." You quickly analyze the traffic moving on the distribution layer and notice a large number of print requests. What could be causing this, and how would you correct it?

2. You are the network manager for AnyCompany. Company management has decided that they want to allow some people in the accounting department to work from home and have asked you whether this might present any problems. They are especially concerned about the security of their financial data. What recommendations would you make and why?