Chapter 1

Networking fundamentals

Learning Objectives

Upon reading this chapter, students should be able to:

\* Trace the development of PC networks and the Internet.

\* Describe the different network models and components.

\* Identify communication components and protocols used in a network.

\* Understand the differences in the different types of networks commonly in use today.

\* Recognize the trends that are changing the way businesses and organizations use networking technologies.

Chapter Summary

PC networks grew out of a traditional mainframe environment utilizing dumb terminals and a central mainframe computer. The PC revolutionized how businesses operated, but presented challenges in the areas of data isolation and security. PC networks rose out of a need to address these issues.

Network benefits include resource and data sharing, improved communication and support, and security control through authentication methods that range from username/password authentication to the use of biometric devices. Network concerns include information security and maintenance and support. Networks require ongoing maintenance and support, typically through the role of a dedicated network administrator.

The Internet plays a key role in many modern networking configurations, growing from the four original Department of Defense ARPANET servers to up to 500 million computers today. It has been a breeding ground for the design and development of new information and communication technologies, with many PC network innovations tracing their roots directly to the Internet.

There are three basic network components: servers, clients, and the circuit (cable plant). The circuit is the pathway through which the messages travel.

Network devices include network adapters, hubs, switches, routers, bridges, brouters, and gateways. Switches are similar to hubs in connecting many PCs and servers to a LAN, but switches are more sophisticated at managing traffic. A router connects multiple networks together. A network adapter, or network interface card (NIC) is hardware that connects a computer to a network and determines the low-level protocol used by the computer to communicate on the network.

There are two basic network models: client/server and peer-to-peer. In the client/server network model, one or more computers are designated as servers, providing resources to the network. The rest of the computers are clients, consuming those resources. The identifying feature of a client/server network is centralized control over network security. In a directory services network, everything on the network, including users, computers, and shared resources, is maintained in a centralized directory.

In a peer-to-peer network, the network client computers act as both clients and servers and are sometimes referred to as peer servers. Peer servers are not limited to peer-to-peer networks. You can deploy peer servers on client/server and directory services-based networks to provide additional resources.

The basic difference between clients and servers is the software they run: client operating systems (Windows 2000, XP, Vista and Windows 7) or server/network operating systems (Windows 2000 Server, Server 2003, Server 2008 and most Linux versions).

Data communications is the movement of computer information from one point to another by means of electrical, optical, or radio frequency transmission systems. The broader term telecommunications includes the transmission of voice and video (images and graphics) as well as data and usually implies longer distances. The line between the two has tended to blur in recent years, with telecommunications often a key part of data communications.

The Internet was based from the beginning on Transmission Control Protocol/Internet Protocol (TCP/IP), which is actually a suite of different protocols, each supporting different communication roles. In the past several years, TCP/IP has become the de facto standard for all computer networking applications, including PC networks.

There are three main categories of networks: LANS, MANs, and WANs. A LAN connects computers and other network devices so that the devices can communicate with each other to share resources. Devices on a wired LAN are connected using inexpensive cable. Due to limitations in distance, performance, and manageability, a LAN is usually confined to a single office or floor of a building. Many new LANs are being installed using wireless technologies. Wireless networks commonly use an access point, which acts as a central access point (working similarly to a hub or switch) and can also connect a wireless network to a wired network. A MAN is made up of LANs that are interconnected across a city or metropolitan area, typically spanning up to 75 miles. Although MANs are very expensive to implement, they offer a high-speed alternative to the slower connections often available in WANs because of the MAN’s higher-performance cable plant and equipment. Traditional MANs connect through a backbone network. Backbone networks typically span up to several miles and provide high-speed communication, commonly up to 100 Mbps to 1,000 Mbps. In recent years, there has been a tendency toward linking LANs through high-bandwidth Internet connections instead of building or buying MANs. A WAN interconnects two or more LANs or MANs. Traditionally, a LAN becomes a WAN when it connects across the public telephone network—often using lines (long-haul transmission lines) leased from local telephone companies. The majority of WANs communicate at speeds between 56 Kbps and 1.5 Mbps, although speeds up to 9.953 Gbps are available. At one time, WANs were considered low-speed connections, but this is rapidly changing as the availability of high-bandwidth connections increases and the associated costs drop. Internet technologies have driven the evolution of LANs, particularly in the development of intranets and extranets.

Future trends driving the future of networking involving integration of video, voice, and data; as well as new information services commonly provided by ASPs.

Key Terms

**Access point** A designated point of entry within a network where wireless devices send and receive transmissions.

**Addressing** How computers are able to identify and recognize each other on a network.

**Application service providers (ASPs)**

Companies that develop and sell applications that are used over the Internet.

**ARCNET** Acronym for Attached Resource Computer Network. ARCNET is an outdated networking protocol that was used in the 1980s for office automation tasks.

**Authentication mechanisms** Ways that the network can validate who is and who isn’t allowed access to the network.

**Backbone network** A large, central network that can be used to connect LANs to form MANs, and also connect other backbone networks, MANs, and even WANs.

**Bandwidth** The capacity on a given network for data transmission.

**Biometric device** Device that uses physical features such as fingerprint or retinal pattern, to authenticate network users.

**Bridge** A network communication device used to connect physical networks and provide a level of filtering between networks.

**Broadband** A type of high-speed data transmission circuit.

**Brouter** A network communication device that combines the functionality of routers and bridges.

**Client operating system** The control program installed on the client PC.

**Client/server network** Network model that connects multiple PCs, called clients, to a single computer, called a server, which distributes data and resources to the network.

**Connection** The process of having two computers recognize each other and open a communication channel between them.

**Convergence** Integration of voice, video, and data communication.

**Data communications** Movement of computer information from one point to another by means of electrical or optical transmission systems.

**Directory services network** A network model in which everything on the network, including users, computers, and shared resources, is maintained in a centralized directory. Also known as a directory-based network.

**Dumb terminal** A screen and a keyboard with all data storage, processing, and control occurring at the mainframe.

**Ethernet** A protocol defining the wired connections within a network. Most commonly used networking standard with support for speeds ranging from 10 Mbps to 10 Gbps in current implementations.

**Extranet** A private network that allows specific external users access over the Internet.

**Fiber optic** Transmission media using glass or plastic fibers to carry light (laser) signals.

**File server** A server on a network whose primary function is to serve as a repository for network user files.

**Gateway** A connection device that is used to connect networks and devices that would not otherwise be able to communicate with each other.

**Handshaking** The process used by computers for establishing a connection to each other.

**High-level protocol** The rules for how data is transferred from one device to another.

**Hub** A connection device that allows multiple connections to the network.

**Information utilities** Companies that sell information services.

**Internet service provider (ISP)** Companies providing Internet access for a fee.

**Intranet** A closed private LAN used for internal communication.

**Local area network (LAN)** A relatively small network of computers, printers, and other devices covering a small geographic area.

**Long-haul transmission lines** Telephone cables within a wide area network used to transmit over long distances.

**Low-level protocol** A system of rules for how network connection is achieved.

**Media player** Small portable digital device used for playing audio and video files.

**Metropolitan area network (MAN)**

A high-speed internetwork of LANs deployed in a metropolitan area.

**Modem** Devices that enables computers to communicate over dial-up telephone lines.

**NetBEUI** High-level protocol originally used on Microsoft networks.

**Network** Computers connected in such a way that they can communicate with each other.

**Network adapter** The hardware that enables a computer to connect to a network.

**Network administrator** An IT expert specializing in the upkeep and support of networks.

**Network interface card (NIC)** Another name for a network adapter; the hardware that enables a computer to connect to a network.

**Network system** The path over which servers and clients communicate.

**Node** A uniquely identifiable device.

**Packet** Block of data formatted for transmission over a network.

**Peer server** The PCs in a peer-to-peer network that act as both client and server.

**Peer-to-peer network** A small network architecture in which individual computers are connected directly to one another and can act as both a server and a client.

**Print server** A server on a network whose primary function is to control network user access to shared printers.

**Protocol** Rules or standards that define the way in which devices communicate on a network, such as signal strength and format.

**Regional carriers** Regional telephone companies.

**Router** A network communication device used to connect two or more networks or network types.

**Server** A computer that stores and provides resources and data to the network.

**Server operating system** The control program installed on the server. Also known as a network operating system.

**Smart phone** Any device capable of placing phone calls and advanced computing functions including web browsing, e-mail transmission, media playing, document viewing, and schedule maintenance.

**Smart terminal** A connection device that has onboard memory and processing capabilities.

**Switch** A connection device similar to a hub but more sophisticated including functionality that allows it to control and manage data transmissions.

**Telecommunications** The transmission of voice and video (images and graphics) as well as data; usually implies longer distances.

**Token ring** A topology in which a data packet is sent around a ring of computers until it reaches its intended destination.

**Transmission Control Protocol/ Internet Protocol (TCP/IP)**

High-level protocol suite developed for use on the Internet and currently the de facto standard PC network protocol.

**Transmission media** The media that carries network signals—either copper wire, fiber optic line, or radio transmission.

**Virtual private network (VPN)** An private communication path over the public Internet acting as a secure network within a larger or public network.

**Voice over IP (VOIP)** The technology that enables Internet-based telephone services.

**Web browser** Software that enables a computer to render and display documents published from a Web server.

**Web server** Network server that stores documents and graphics published to the Internet.

**Wide area network (WAN)** LANs connected over a wide large geographic area, traditionally connecting LANs using the public switched telephone network but more commonly connecting through the Internet.

**Wired network** A network consisting of PCs and servers, which are physically connected by cables.

**Wireless network** Use radio transmission instead of cables to communicate.

**Workgroup** A logical peer-to-peer network grouping.

Lecture Notes

1. Identify a local network administrator either in your college or the local business community and ask them to describe the networks they use in their business, the topologies of those networks, and the protocols used.

2. Divide the class into two or more groups. Ask each group to develop a list of products that they use in their every-day life that are illustrative of the growing trend of convergence. After 20 minutes, ask a representative from each group to present their findings.

3. Ask the students to prepare a short research paper with examples of 1-2 pages on the three different types of networks (LANs, MANs, and WANs).

4. Ask all students to think of and list all network devices they utilize each day.

5. Ask students to do a brief research report on the importance of security for PC networks.

Suggestions for Learning Activities

1. Assign Project 1.1, Understanding Key Concepts, in conjunction with Sections 1.1 and 1.2 of the text. This Project helps students become more familiar with key terms and concepts related to networking basics, network components and network types.

2. Assign Project 1.2, Identifying Basic Components, in conjunction with Sections 1.2 and 1.3 of the text. This Project allows students to practice recognizing common network components and differentiating wired and wireless networks.

3. Assign Project 1.3, Understanding Network Types, in conjunction with Section 1.4 of the text. This Project helps students to practice comparing and contrasting network types and choosing a network type based on organizational requirements.

4. Assign Project 1.4, Preparing for Network Installation, after students have completed the chapter. This Project allows students to practice identifying minimum wired network hardware requirements, installing a network adapter, and connecting to a wired network.

5. Assign Project 1.5, Installing Windows Server 2008, after students have completed the chapter. This Project allows students to practice installing Windows Server 2008, configuring network parameters and verifying successful installation.

Suggestions for Additional Resources

1. Microsoft TechNet: Network Basics and Overview (<http://www.microsoft.com/technet/network/evaluate/technol/networks.mspx>)

2. Linksys.com – Learning Center/Network Basics (<http://www.linksys.com/servlet/Satellite?c=L_Content_C1&childpagename=US%2FLayout&cid=1114037291160&pagename=Linksys%2FCommon%2FVisitorWrapper&lid=9116080198N01>)

3. Articles and Tutorials: Network Protocols (<http://www.windowsnetworking.com/articles_tutorials/Network_Protocols/>)

Answers to Self-Check Questions

**Answers may vary, but should address the same general concepts as the sample answers.**

**Section 1.1**

1. List two benefits of modern networks.

**The primary benefits are resource sharing, communication, and security.**

2. How are PC networks similar to older mainframe networks? How are they different?

**Mainframe systems have all processing power and storage located within the central mainframe while each PC and server has its own processor, memory and disk storage. Client/server and mainframe share similar architecture in terms of resource flow.**

3. Why is security for PC networks a concern?

**Hackers and ID thieves have tools that can easily penetrate PC and server operating systems and retrieve sensitive information. Encryption methods and access prevention tools can mitigate this threat.**

4. What are some of the access control methods used to protect networked information?

**Some access control methods include usernames, passwords, and biometrics such as fingerprint scanners or retinal scanners.**

**Section 1.2**

1. Compare the roles of network clients and network servers.

**Network servers provide resources to the network. Network clients consume the resources provided by servers.**

2. How is a router used in a network?

**A router is used to connect two or more networks.**

3. Compare the client/server, directory services, and peer-to-peer network models.

**The client/server model uses computers acting specifically in client and server roles and provides centralized security. The directory services model maintains everything in the network in a central directory and also provides centralized security. The peer-to-peer model uses peer-servers and does not have centralized security control.**

**Section 1.3**

1. Define data communications.

**The movement of computer information from one point to another.**

2. How have newer systems taken advantage of the merging of data communications and telecommunications?

**Data communications networks facilitate more efficient use of computers and improve the day-to-day control of a business by providing faster information flow. They also provide message transfer services to allow computer users to talk to one another via electronic mail, chat, and video streaming.**

3. Compare the role of low-level and high-level protocols.

**Low-level protocols define hardware-level communication standards such as signal strength and physical connection hardware. High-level protocols operate at the software level and handle activities such as establishing connections and formatting data for transmission.**

**Section 1.4**

1. Compare characteristics of LANs, CANs, MANs, and WANs:

**LAN:**

**\* Used within small areas (such as in an office building).**

**\* Offer high-speed communication—typically, 100Mbps or faster.**

**\* Provide access for many devices.**

**\* Use LAN-specific equipment such as hubs and network interface cards.**

**CAN:**

**\* Connects several LANs within a building or small geographical area**

**\* Larger than a LAN but smaller than a WAN**

**MAN:**

**\* Sites are dispersed across a city and perhaps the surrounding area as well.**

**\* Historically slow connections (56Kbps–1.5Mbps) have given way to communication at hundreds of megabits per second and even gigabit speeds.**

**\* Provide single points of connection between each LAN.**

**\* Use devices such as routers, telephone switches, and microwave antennas as parts of their communication infrastructure.**

**WAN**

**\* Can cover a very large geographical area—even span the world.**

**\* Usually communicate at slow speeds (compared to LANs).**

**\* Access to the WAN is limited—a LAN usually has only one WAN link that is shared by all devices.**

**\* Use devices such as routers, modems, and WAN switches, connectivity devices specific to LANs and used to connection to long-haul transmission media.**

2. How are intranets and extranets similar? How are they different?

**Intranets and extranets are similar because they are both based on Internet technologies. They differ because intranets use Internet technology to facilitate internal communications while extranets provide connectivity for external users.**

**Section 1.5**

1. Describe the process of convergence.

**Convergence is the integration of voice, video, and data communications. Carriers such as AT&T provide telecommunication services that support data and voice transmission over the same circuits—instead of transmitting video, voice, and data signals separately on different networks—and hardware manufacturers provide the infrastructure needed to meet the changing definition of data.**

2. What is an information utility and how has it evolved?

**An information utility is a company that provides a wide range of standardized information services.**

3. What challenges do organizations face in relation to the information made available by the Internet?

**\* Assessing the accuracy and value of information**

**\* Assimilating the information we decide is useful**

**\* Using the information effectively.**

Answers to Summary Questions

1. Broadband includes a wide range of frequencies to increase the volume of data communication. True or false?

**True**

2. Which of the following refers to a network deployed in the smallest geographic area?

(a) WAN

(b) MAN

(c) CAN

(d) **LAN**

3. What is the primary shared resource on large PC networks?

(a) **Data**

(b) Audio speakers

(c) Scanners

(d) None of the above

4. A \_\_\_\_\_\_\_\_\_\_\_\_\_\_ is a device used to connect network devices like computers and printers.

(a) Node

(b) Router

(c) **Switch**

(d) Gateway

5. What is the device used to connect two or more LANs?

(a)node

(b) **router**

(c) hub

(d) gateway

6. Which network model does not support centralized security?

(a) Client/server

(b) Directory services

(c) **Peer-to-peer**

7. Microsoft Internet Explorer is an example of a Web server. True or false?

**False**

8. What is distinctive about fiber-optic cable compared to other transmission media types?

(a) It carries digital data.

(b) It uses radio-frequency communication transmissions.

(c) It contains copper wire.

(d) **It uses glass or plastic to carry the data signal**.

9. What is the term used to refer to any uniquely identifiable device on a network?

(a) **Node**

(b) Host

(c) Server

(d) Gateway

10.What is the device that makes a physical connection between a computer and the network cable in a traditional wired network?

(a) Switch

(b) **Network interface card**

(c) Brouter

(d) Access point

11. What is the most commonly used low-level protocol on PC networks?

(a) ARCNET

(b) Token Ring

(c) **Ethernet**

(d) NetBEUI

12. Which of the following is defined by a high-level protocol?

(a) Physical connection to the network

(b) Signal strength

(c) **Connection procedures**

(d) Cable plant structure

13. Which protocol is the de facto standard for PC networking?

(a) IPX/SPX

(b)AppleTalk

(c) NetBEUI

(d) **TCP/IP**

14. What type of network would you use to connect various locations in San Francisco through existing phone company-owned cables?

(a) CAN

(b) LAN

(c) **MAN**

(d) WAN

15. An extranet is a network that uses Internet technologies to allow access to invited users from outside the organization. True or false?

**True**

16. What is the term referring to the integration of voice, video, and data communications?

(a) **Convergence**

(b) Pervasive networking

(c) Information utility

(d) Extranet

17. What is an ASP?

(a) A company that provides public access to the Internet.

(b) **A company that develops specific systems and services.**

(c) A company that provides telecommunication infrastructure for purchase or lease.

(d) A company the designs and develops connection devices.

18. Which of the following refers to a private communication path over a public network?

(a) BN

(b) MAN

(c) ASP

(d) **VPN**

19. What is the device used to connect a wireless and wired network?

(a) **Access point**

(b) Switch

(c) Gateway

(d) Modem

20. Why would you deploy a peer server on a peer-to-peer network?

(a) Peer services provide centralized access authentication.

(b)Peer servers are dedicated sources services optimized for peer-to-peer use.

(c) **Peer servers act in the role of both server and client.**

(d) Peer servers cannot be used on other types of networks.

Answers to Apply: What Would You Do? Questions

**Answers may vary, but should address the same general concepts as the sample answers.**

You are working with a team designing a network for a large organization. The team is gathering information about network requirements and trying to make some initial design considerations. The company has five offices in St. Louis and additional offices in Dallas, Los Angeles, and Seattle.

1. What are issues that will help determine the types of connections needed between the offices?

**Major issues would include the amount of data you need to move between the offices, communication speed, security requirements, cost, and how difficult it will be to deploy and maintain the network.**

1. Describe the general network design and the role of connectivity devices.

**Each office would be configured as a separate LAN, possibly a routed LAN, depending on the office layout and number of users. The offices in St. Louis would be connected using either a MAN or WAN infrastructure, depending on the best fit. The remaining offices would be interconnected through a WAN infrastructure. Hubs, switches, or both would likely be used to connect devices on the LANs. Routers would be used to connect the LANs to each other.**

1. Why would a directory services network more likely meet the organization’s needs that a peer-to-peer network?

**A directory services network provides centralized management and control. Also, peer-to-peer networks are designed to support a very small number of users (usually no more than 12).**

Answers to Be a Network Configuration Engineer Questions

**Answers will vary, but should address the same general concepts as the sample answers.**

You are a consultant currently specializing in small-to-medium businesses. You want to expand your business to include home network design and implementation.

1. What network issues are similar in small businesses and home networks?

**Family members will want to share data, but more likely photos, audio files, and videos than traditional data files. They will want to share hardware resources, such as printers. A likely justification for the network would be the desire to share a single Internet connection.**

1. What are additional issues might you need to deal with in a home network?

**There is a good chance that some of the family members will not be very computer literate. They also may not recognize or even understand the need for network security to protect sensitive information.**

1. What is the potential impact of pervasive computing developments on home network design?

**Many of the devices being developed are consumer devices, that is, devices meant to be bought by “plain folks” and used in and around the home. Having made the investment in the devices, family members will want to integrate them with the network and will probably have no idea of what this will entail.**

1. Why might you configure the network as an intranet?

**Family members may want to set up a private Web server for use in the house. This would give busy families a way of keeping in touch, leaving notes for each other, and so forth. It’s also a way to display photos and home movies.**