An Introduction to Networking

© Cengage Learning 2016

Objectives

- Identify types of applications and protocols used on a network
- Distinguish between the client-server and peer-to-peer models used to control access to a network
- Describe various networking hardware devices and the most common physical topologies
- HVAC system and protecting against ESD

© Cengage Learning 2016

How Networks Are Used

- A network is a group of computers and other devices connected by some type of transmission media.
- Network services - the resources a network makes available to its users
  - Includes applications and the data provided by these applications
- Types of applications found on most networks:
  - Client-Server
  - File and Print Services
  - Communications Services

© Cengage Learning 2016

Client-Server Applications

- Client computer requests data or a service from a second computer, called the server
- List of several popular client-server applications:
  - Web service
  - Email services
  - FTP service
  - Telnet service
  - Remote Desktop
  - Remote applications

© Cengage Learning 2016

Client-Server Applications- Web services

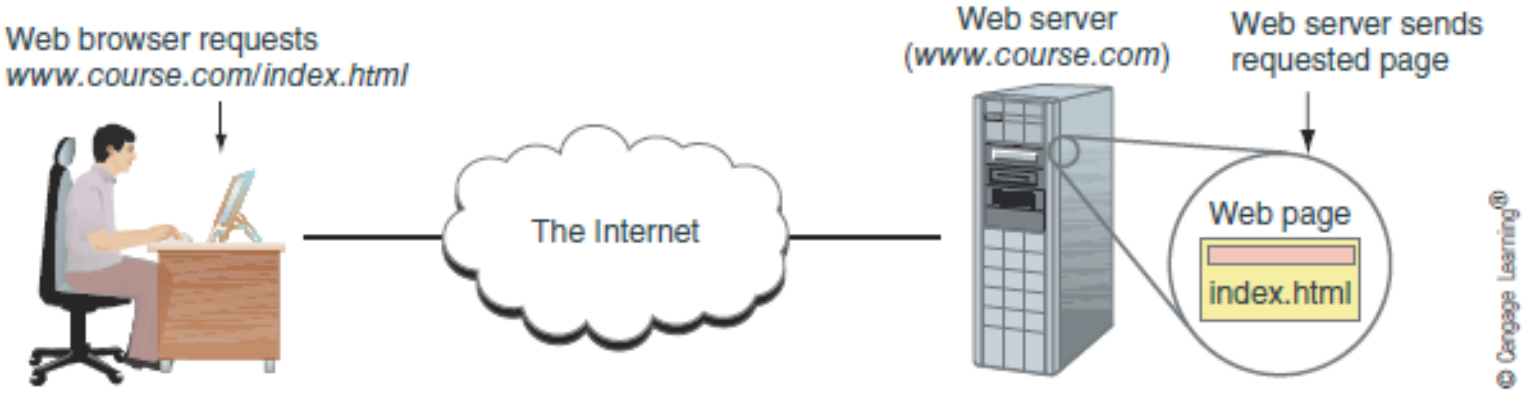

Figure 1-1 A Web browser (client application) requests a Web page from a Web server (server application); the Web server returns the requested data to the client

- HTTP HyperText Transfer Protocol:protocol used between server and clients (browser), if layered on top of SSL (Secure Socket Layer) or TLS(Transport Layer Security) result is HTTPS.
- Example of web server: Apache (Unix), IIS(Windows server)

© Cengage Learning 2016

Client-Server Applications - email services

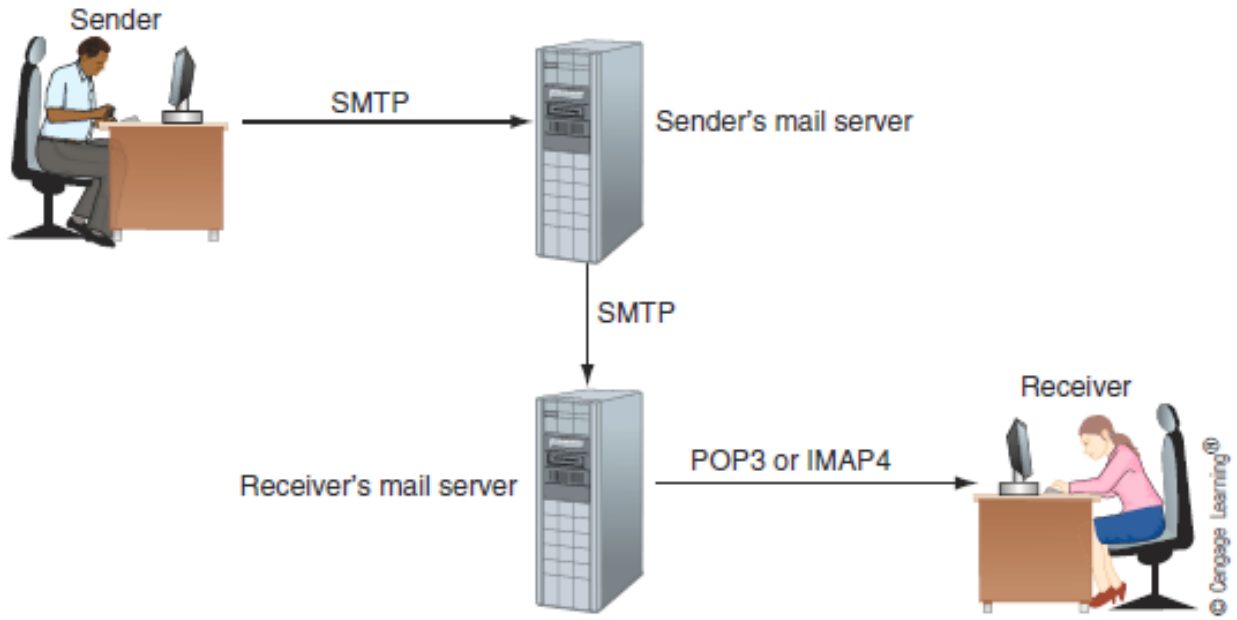

Figure 1-2 SMTP is used to send email to a recipient's mail server, and POP3 or IMAP4 is used by the client to receive email

- A Client server application that involves two servers

SMTP(Simple Mail Transfer Protocol): used to send an email message to a server

- POP3(Post Office Protocol), IMAP4(Internet Message Access Protocol):

deliver the message to the receiving client.

© Cengage Learning 2016

Client-Server Applications

- FTP service: Transfers files between two computers, using File transfer protocol, FTP, SFTP
- Telnet service: A command-line used to control a computer remotely, not secured, Linux uses SSH protocol (Secure Shell)
- Remote Desktop: secure transmission usually used by vendor technician to access Client computer, both use RDP to establish a client-server communication
- Remote Applications: Application installed on a server, easy for maintenance and backup of applications.

© Cengage Learning 2016

File and Print Services

- File services - a server's ability to share data files and disk storage space
- File server - a computer that provides file services
- Print services - ability to share printers across a network
  - With one printer, less time is spent on maintenance and management

© Cengage Learning 2016

Communication Services

- Convergence - using the same network to deliver multiple types of communications services (video, voice, fax)
- A similar term-Unified communication (UC) - refers to the centralized management of multiple network-based communications- one software for long-distance calls and intra-office phone calls.
- Three types of communication services:
  - Conversational voice - VoIP (Voice over IP): Can use point-to-point model (skype,..) or point-to-multipoint model (on Conference call).
  - Streaming live audio and video (Skype, Google Talk, or live sport:client-server model)
  - Streaming stored audio and video (YouTube:client-server model)

© Cengage Learning 2016

Communication Services

- Voice and video transmissions are delay-sensitive
  - You don’t want to hear or see breaks in transmission
- Voice and video transmission are considered loss-tolerant (accept skipping video frames)
- Network administrators must pay attention to the quality of service (QoS) a network provides for voice and video
- Bandwidth - the amount of traffic, or data transmission activity, on the network

© Cengage Learning 2016

Controlling Network Access

- Topology - how parts of a whole work together
- Physical topology - mostly applies to hardware and describes how computers, other devices, and cables fit together to form the physical network
- Logical topology - has to do with software and describes how access to the network is controlled
  - How users and programs initially gain access to the network (how applications and databases are shared on the network)
- Network operating system - controls access to the entire network (Windows server 2012R2.. 2016, Ubuntu, Red Hat)
  - Required by client-server models

© Cengage Learning 2016

Peer-to-Peer Model

- Peer-to-peer (P2P) network model - the OS of each computer on the network is responsible for controlling access to its resources
  - No centralized control
- Computers, called hosts, form a logical group of computers and users
  - May share resources
  - May prevent access to resources
- Each computer user has a Windows local account
  - Works only on that one computer

© Cengage Learning 2016

Peer-to-Peer Model

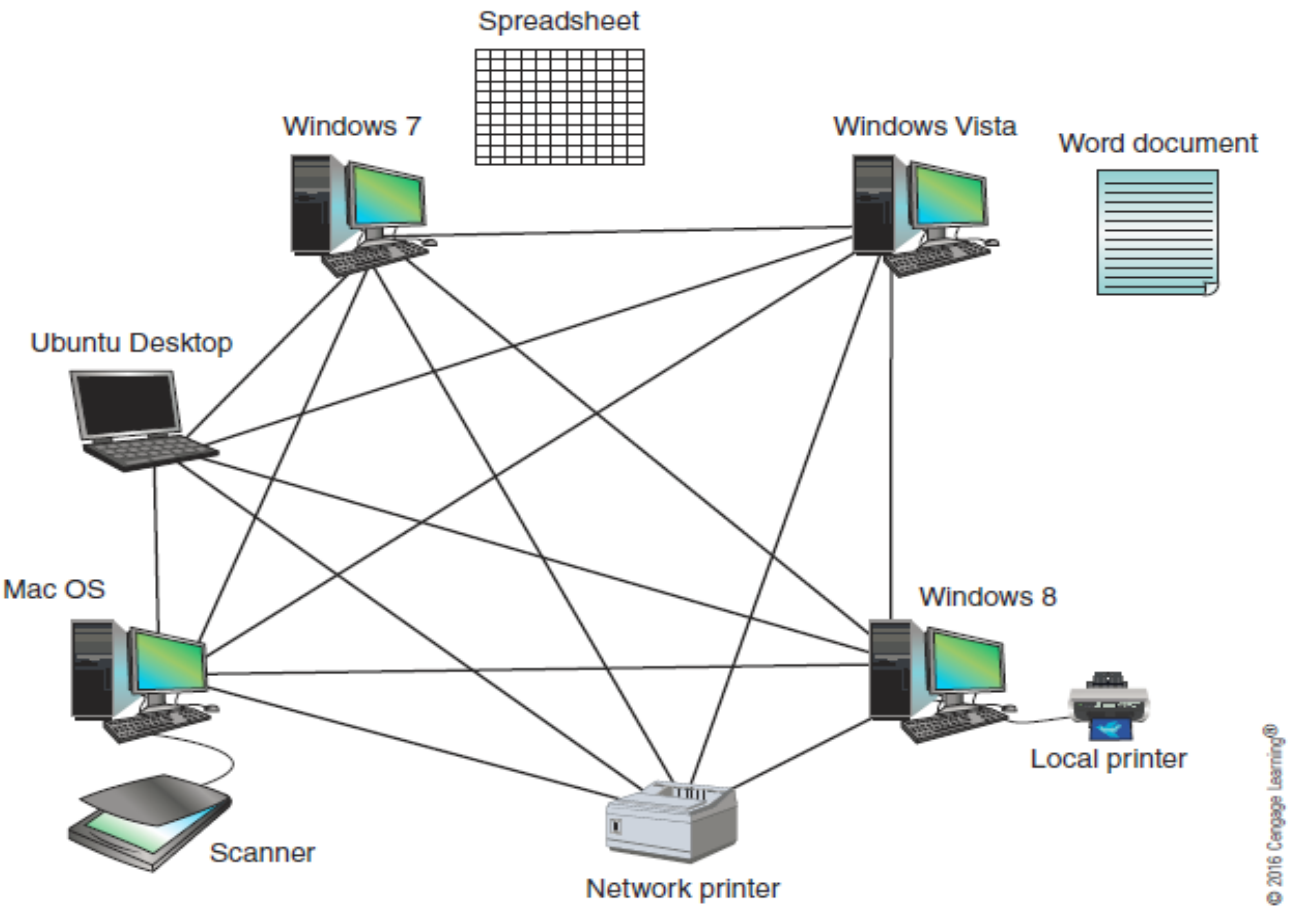

Figure 1-4 In a peer-to-peer network, no computer has more authority than another; each computer controls its own resources, and communicates directly with other computers

© Cengage Learning 2016

Peer-to-Peer Model

- Advantages
  - Simple configuration (using Homegroup)
  - Less expensive
    - Compared to other network models
- Disadvantages
  - Not scalable
  - Not necessarily secure
  - Not practical for large installations

© Cengage Learning 2016

Client-Server Network Model

- Resources are managed by the network operating system (NOS) via a centralized directory database
- Windows domain - a logical group of computers that a Windows Server can control
- Active Directory (AD) - the centralized directory database that contains user account information and security for the entire group of computers
- Global account (a.k.a. global username or network ID) - a domain-level account assigned by the network administrator and is kept in AD

© Cengage Learning 2016

Client-Server Network Model

- A user can sign on to the network from any computer on the network and gain access to the resources that AD allows
  - This process is managed by Active Directory Domain Services (AD DS)
- Clients don’t share their resources directly with each other
  - Access is controlled by entries in the centralized domain database

© Cengage Learning 2016

Client-Server Network Model

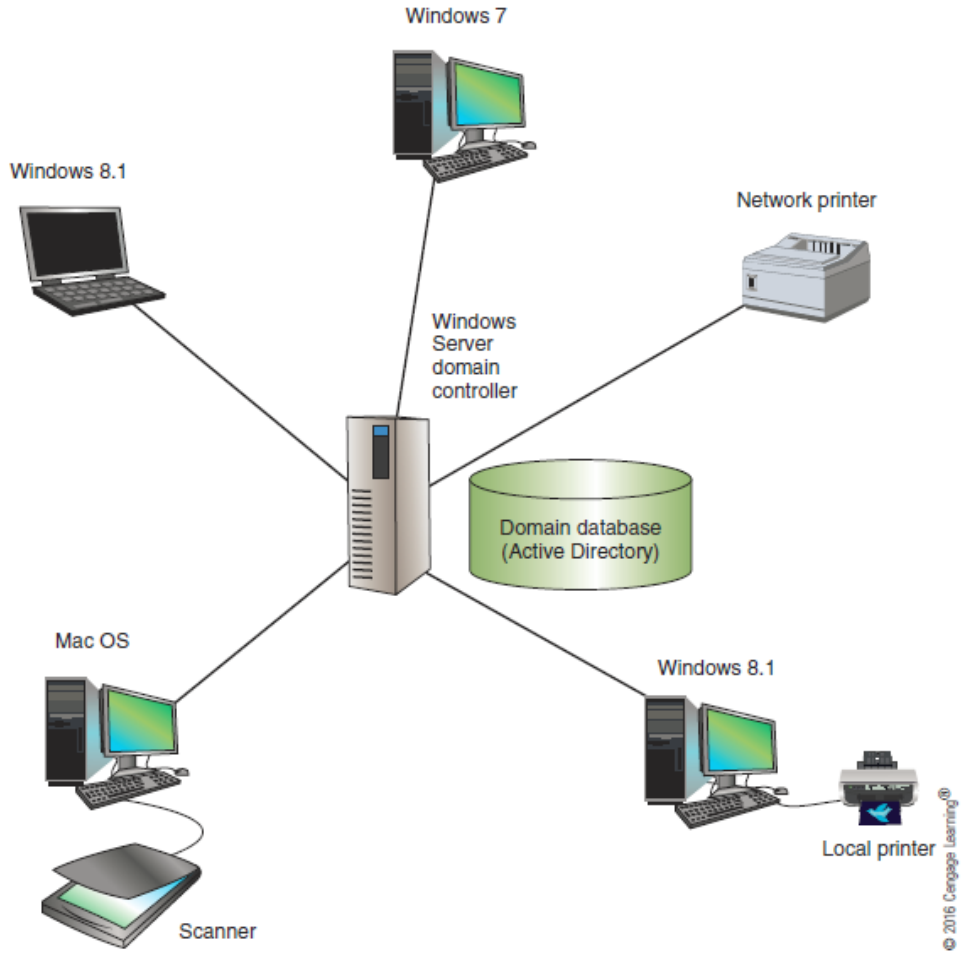

Figure 1-5 A Windows domain uses the client-server model to control access to the network, where security on each computer or device is controlled by a centralized database on a domain controller

© Cengage Learning 2016

Client-Server Network Model

- The NOS is responsible for:
  - Manages client data, resources
  - Ensures authorized user access
  - Controls user file access
  - Restricts user network access
  - Dictates computer communication rules
  - Supplies application to clients
- Server examples
  - Windows Server 2012 R2, Ubuntu Server, or Red Hat Linux

© Cengage Learning 2016

Client-Server Network Model

- Servers that have a NOS installed require:
  - More memory, processing, storage capacity
  - Equipped with special hardware
    - Provides network management functions
- Advantages relative to peer-to-peer networks
  - User credential assigned from one place
  - Multiple shared resource access centrally controlled
  - Central problem monitoring, diagnostics, correction capabilities
  - More scalable

© Cengage Learning 2016

Networking Hardware and Physical Topologies

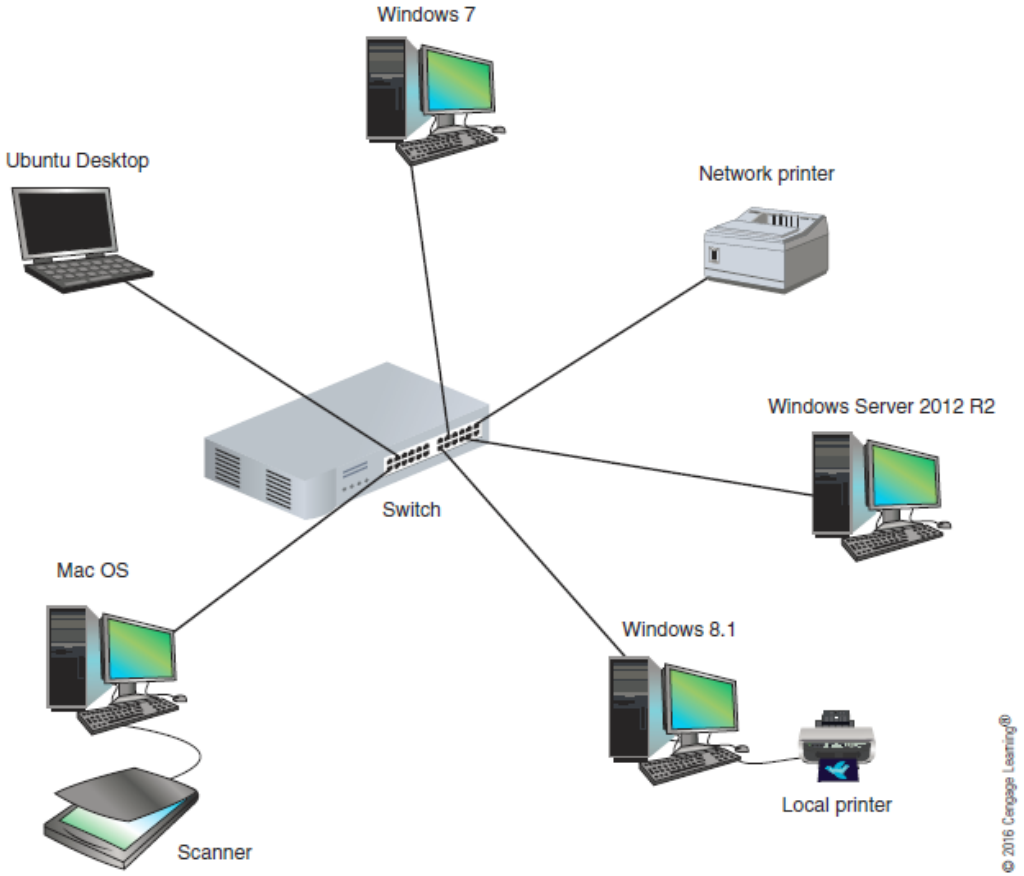

Figure 1-6 This LAN has five computers, a network printer, a local printer, a scanner, and a switch, and is using a star topology

© Cengage Learning 2016

LANs and Their Hardware

- Local area network (LAN) - usually contained in a small space
  - Such as an office or building
- Switch - receives incoming data from one of its ports and redirects it to another port or multiple ports
  - Will send the data to its intended destination
- Star topology - all devices connect to one central device (usually a switch)
- Network interface card (NIC) - a network port used to attach a device to a network

© Cengage Learning 2016

LANs and Their Hardware

- A LAN can have several switches
- Backbone - a central conduit that connects the segments (pieces) of a network
  - Might use higher transmission speeds and different cabling than network cables connected to computers

© Cengage Learning 2016

LANs and Their Hardware

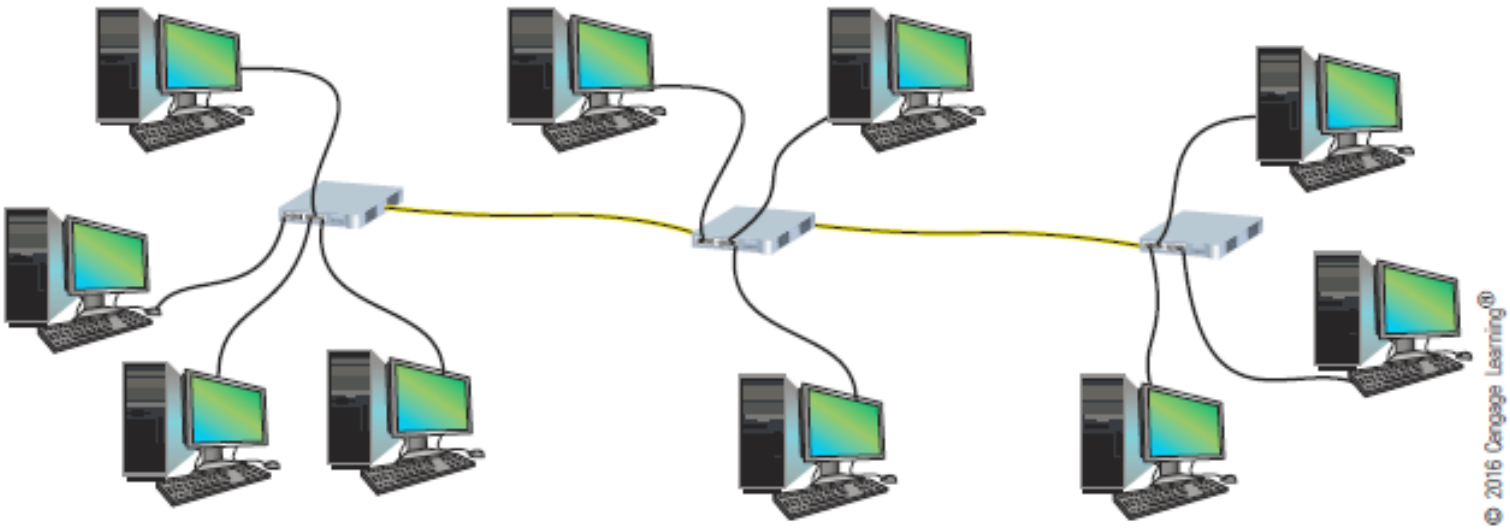

Figure 1-10 This local network has three switches, and is using a star-bus topology

Three switches daisy-chained together in a single line is said to use a bus topology

- However, each switch is connected to computers via a star topology, making it a star-bus topology
- A topology that combines topologies is known as a hybrid topology

© Cengage Learning 2016

LANs and Their Hardware

- Router - a device that manages traffic between two or more networks
  - Can help find the best path for traffic to get from one network to another
- Routers can be used in small home networks to connect the home LAN to the Internet
- Industrial-grade routers can have several network ports, one for each network it connects to
- Difference between router and switch:
  - Router is like a gateway between networks

© Cengage Learning 2016

LANs and Their Hardware

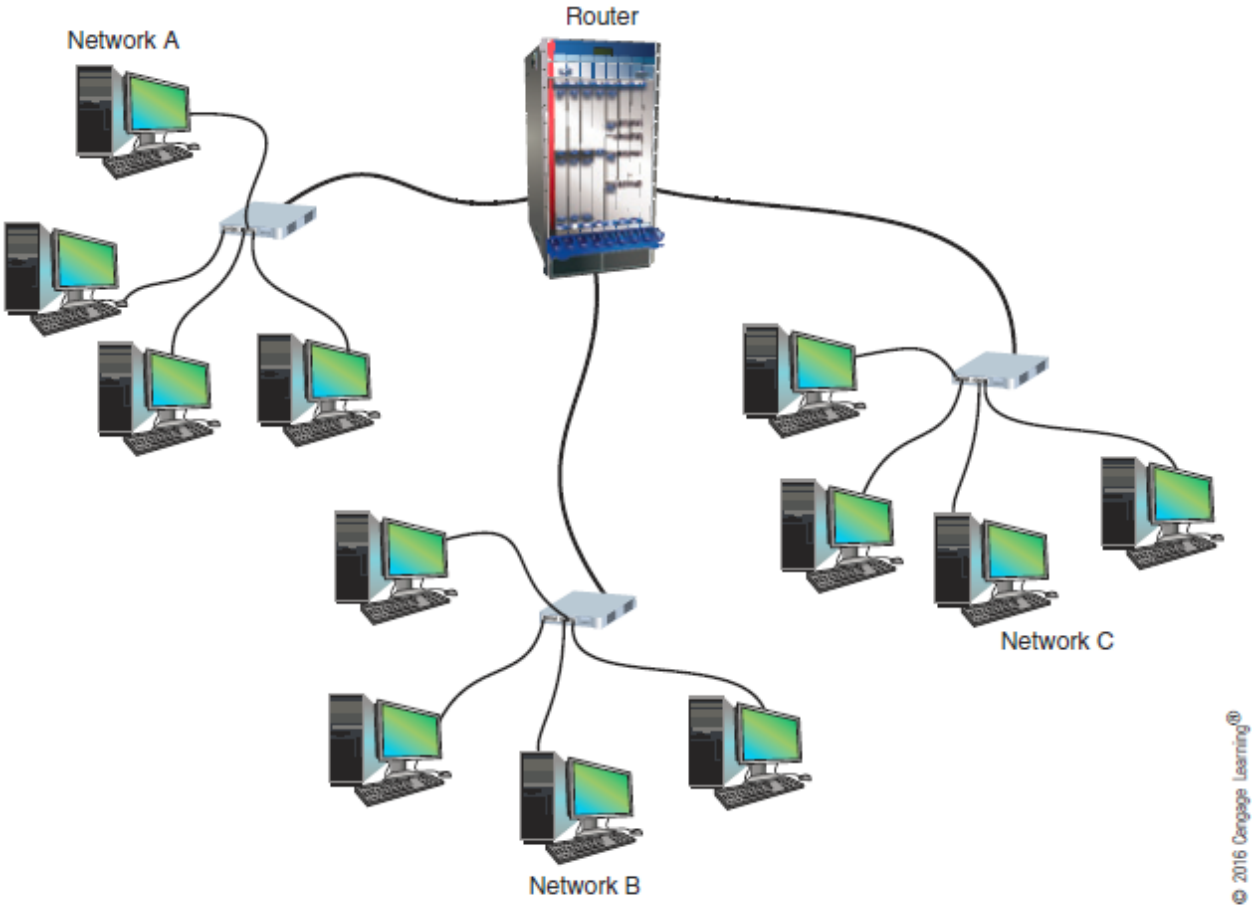

Figure 1-13 Three LANs connected by a router

© Cengage Learning 2016

MANs and WANs

- Metropolitan area network (MAN) - a group of connected LANs in the same geographical area
  - Also known as a campus area network (CAN)
- WAN (wide area network) - a group of LANs that spread over a wide geographical area
  - Internet is the largest and most varied WAN
- MANs and WANs often use different transmission methods and media than LANs
- PAN (personal area network) - smallest network
  - A network of personal devices

© Cengage Learning 2016

MANs and WANs

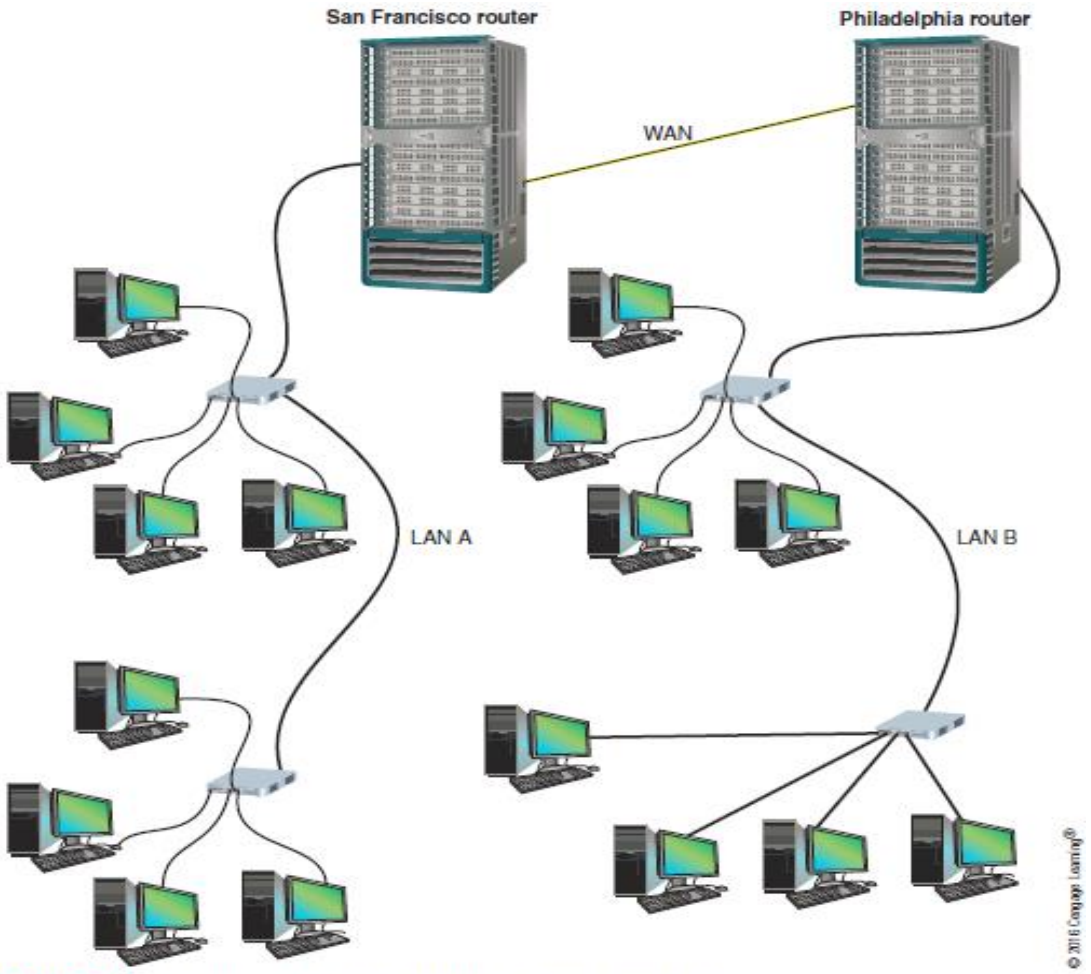

Figure 1-14 A WAN connects two LANs in different geographical areas

© Cengage Learning 2016

Staying Safe When Working with Networks and Computers

- Network and computer technicians need to know how to protect themselves
  - As wells as protect sensitive electronic components
- This section takes a look at some best practices for safety

© Cengage Learning 2016

Emergency Procedures

- Know the best escape route or emergency exit
- Fire Suppression Systems - have a fire suppression system in the data center that includes:
  - Emergency alert system
  - Portable fire extinguishers
  - Emergency power-off switch
  - Suppression agent
- Fail Open or Fail Close - does the security system allow access during a failure (fail open) or deny access during the failure (fail close)

© Cengage Learning 2016

HVAC Systems

- Heating, ventilation, and air conditioning (HVAC) system - controls the environment in a data center
  - Including the temperature, humidity, airflow, and air filtering
- HVAC system must provide acceptable temperature and humidity ranges for devices that might overheat or fail due to high humidity
- HVAC systems and network cabling often occupy the space above the ceiling or below the floor in a data center
  - Called the plenum

© Cengage Learning 2016

Protecting Against Static Electricity

- Computer components are grounded inside a computer case
- Sensitive electronic components can be damaged by electrostatic discharge (ESD)
- Static electricity can cause two types of damage:
  - Catastrophic failure - destroyed beyond use
  - Upset failure - shorten the life of a component

© Cengage Learning 2016

Protecting Against Static Electricity

- Before touching a component, ground yourself by:
  - Wearing an ESD strap around your wrist that clips onto the chassis or computer case
  - Touching the case before touching any component inside the case
  - Storing a component inside an antistatic bag
- In addition to protecting against ESD, always shut down and unplug a computer before working inside it

© Cengage Learning 2016

Troubleshooting Network Problems

- Troubleshooting steps used by most expert networking troubleshooters:
  - Identify problem
    - Gather information
    - Identify symptoms
    - Question users
    - Determine if anything has changed
  - Establish theory of probable cause
    - Question the obvious

© Cengage Learning 2016

Troubleshooting Network Problems

- Troubleshooting steps (cont'd)
  - Test theory to determine cause
    - If theory confirmed, determine next steps
    - If theory not confirmed, establish new theory or escalate
  - Establish action plan
  - Implement solution or escalate the problem
  - Verify full functionality
    - Implement preventative measures if applicable
  - Document findings, actions, outcomes

© Cengage Learning 2016

Summary

- Networks provide a wide range of services, including client-server applications, file and print services, and communications services
- File and print services enable multiple users to share data, storage areas, and printers
- Traditional peer-to-peer networks are usually simple and inexpensive to set up
- The client-server model for access control relies on a centrally administered server using a NOS that manages shared resources for multiple clients
  - More complex and expensive to install

© Cengage Learning 2016

Summary

- A LAN is a network of computers and other devices that can directly address all other nodes
- In a star topology, all computers and network devices connect to one central device
- A backbone is a central conduit that connects parts of a network and might use the bus topology
- A router manages traffic between two or more LANS
- LANS can be interconnected to form WANS, which traverse longer distances in two or more geographical areas
- When working with sensitive components, protect against ESD by using an ESD strap

© Cengage Learning 2016