Technology in Action

Alan Evans • Kendall Martin

Mary Anne Poatsy

Eleventh Edition

Technology in Action

Chapter 10

Behind the Scenes:
Networking and Security in the
Business World

Chapter Topics

- Client/Server Networks and Topologies
  - Client/Server Network Basics
  - Servers and Network Topologies
- Setting Up Business Networks
  - Transmission Media
  - Network Adapters and Network Navigation Devices
  - Network Operating Systems
  - Client/Server Network Security

Basics of Client/Server Networks

- A network is a group of two or more computing devices (nodes)

- Configured to share information and resources

  - Printers, files and databases

- Businesses gain advantages from deploying networks

3

Basics of Client/Server Networks
Networking Advantages

Benefits of Business Networks

Enable resource sharing
- Expensive peripherals, such as printers, can be shared
- Networks can share a single internet connection

Facilitate knowledge sharing
- Data can be accessed by multiple people

Enable software sharing
- Software can be delivered to client computers from a server

Enhance communication
- Information sharing is more effective when employees are connected

Basics of Client/Server Networks
Networking Disadvantages

- Disadvantages to using networks
  - Additional personnel required to maintain network
  - Require special equipment and software
- Cost savings and advantages usually outweigh the disadvantages

Basics of Client/Server Networks
Comparing Client/Server and Peer-to-Peer Networks

- Where to find client/server networks
    - Majority of computer networks are client/server
    - Tasks can be handled centrally at server
    - Client/server is considered centralized
    - Peer-to-peer (P2P) is decentralized

Basics of Client/Server Networks
Comparing Client/Server and Peer-to-Peer Networks

- Why businesses use client/server networks

  - Make data flow more efficiently than P2P

  - Responds to requests from large number of clients at same time

  - Can be configured to perform specific tasks efficiently

Basics of Client/Server Networks
Comparing Client/Server and Peer-to-Peer Networks

- Why P2P networks aren't used more in business settings

    - Difficult to administer beyond 10 users

    - Inefficient with large number of computers

    - Security can't be implemented centrally

    - Client computers are freed up for processor-intensive tasks

Basics of Client/Server Networks
Types of Client/Server Networks

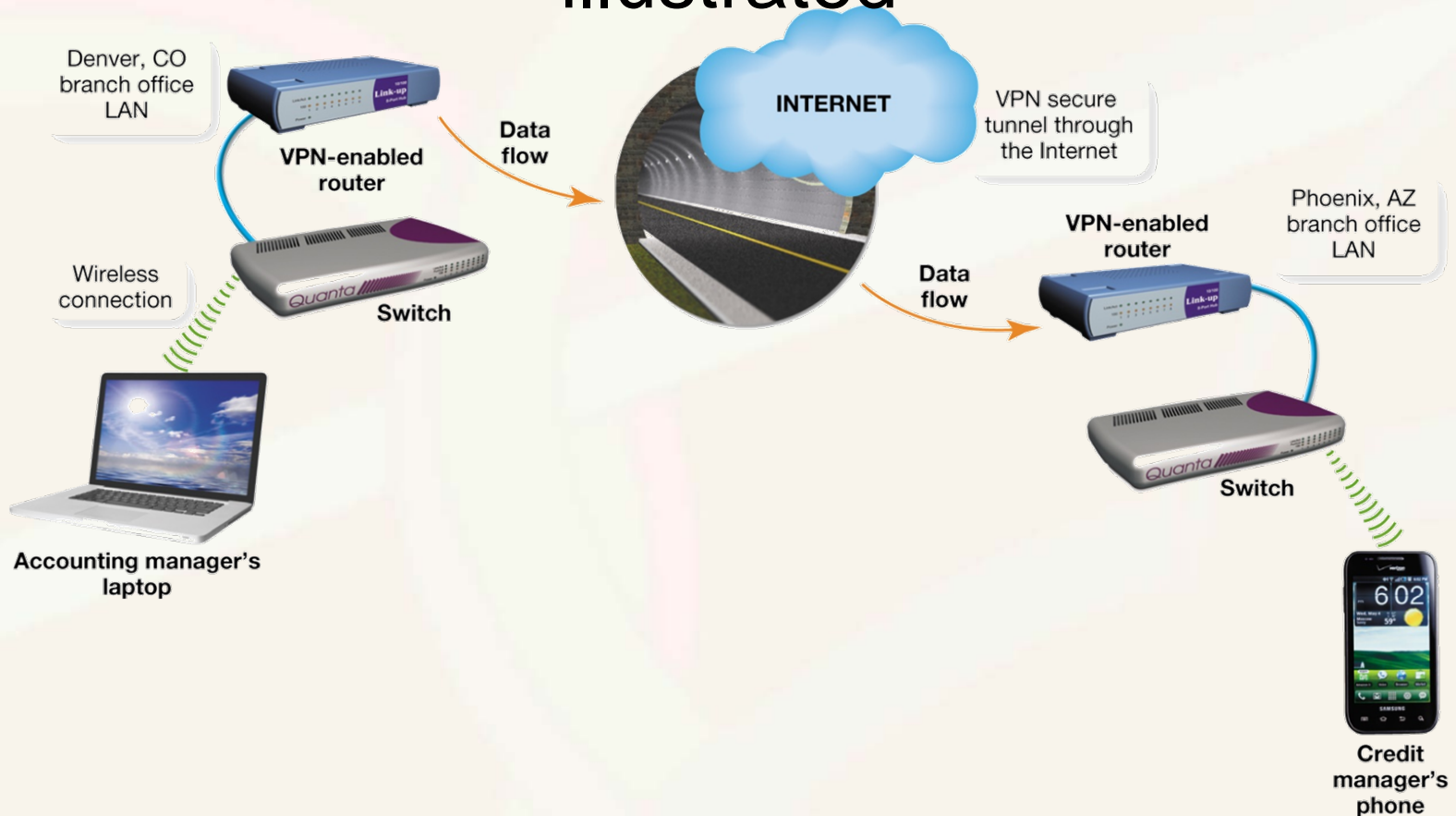|		
LAN (Local Area Network)	A network consisting of nodes covering a small geographic area	In small businesses or self-contained units of a large business (such as one or more floors of the same office building)
WAN (Wide Area Network)	Two or more LANs connected together, often over long distances	Connecting business LANs over long distances such as between branches in two cities
MAN (Metropolitan Area Network)	WANs constructed by municipalities to provide connectivity in a specific geographic area	Although not deployed by businesses, employees often use them while traveling

Basics of Client/Server Networks
Types of Client/Server Networks

- Virtual Private Networks (VPNs) keep information secure

- VPNs work using tunneling
  - Data packets placed into other data packets
  - Encrypted so only understood by sending and receiving hardware (tunnel interface)
  - Hardware is optimized for efficiency
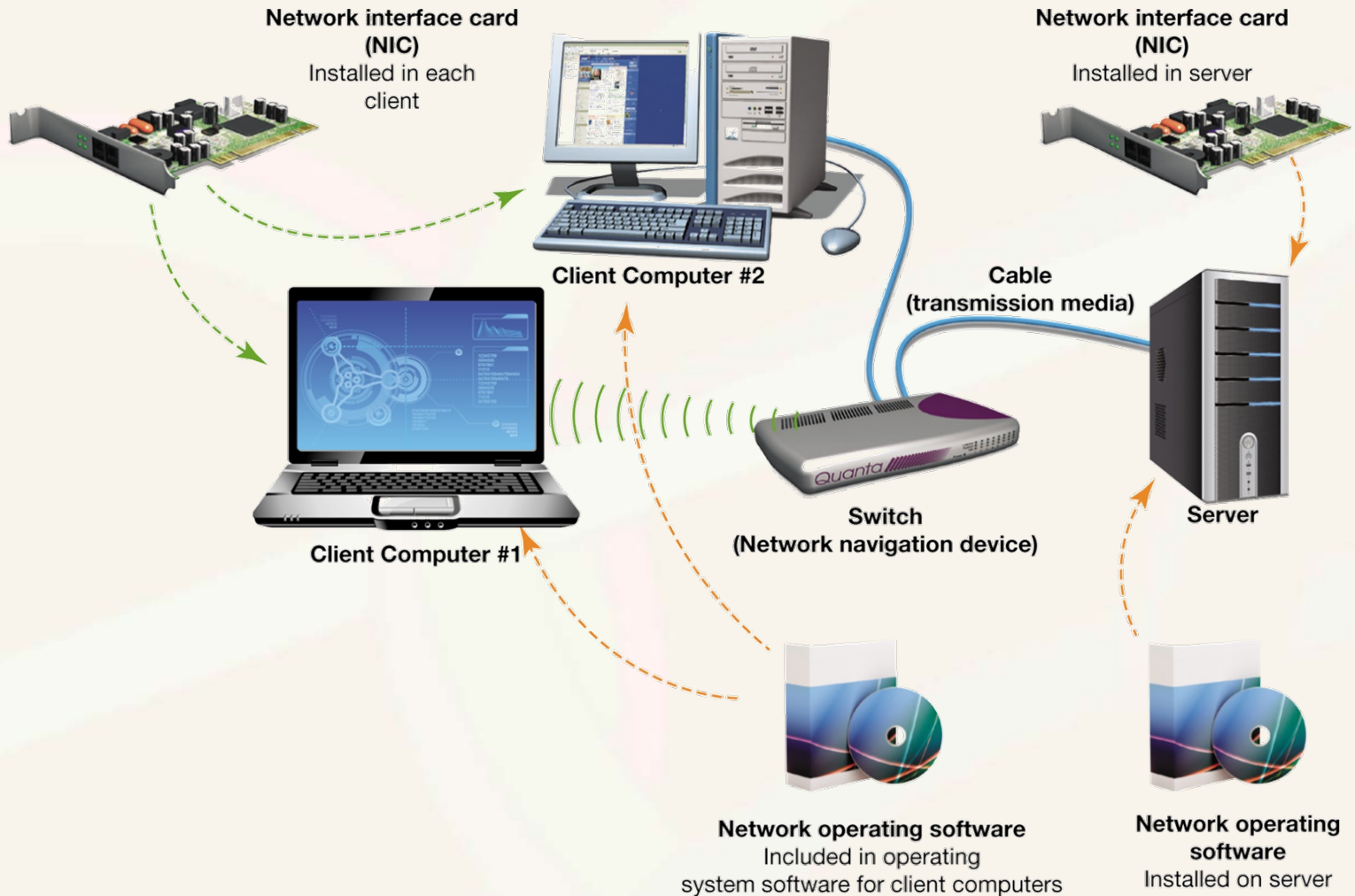
Basics of Client/Server Networks
Types of Client/Server Networks

- Virtual Private Network (VPN) illustrated

Basics of Client/Server Networks
Key Components

Network interface card (NIC)
Installed in each client

Network interface card (NIC)
Installed in server

Client Computer #2

Cable (transmission media)

Client Computer #1

Switch (Network navigation device)

Server

Network operating software
Included in operating system software for client computers

Network operating software
Installed on server

Servers

- Workhorses of client/server network
- Interface with many network users
- Assist with variety of tasks
- Number and types of servers depend on network size and workload

Major Categories of Servers

Print Servers
Manage all printing jobs for client computers

Application Servers
Serve as a repository for application software

Database Servers
Provide client computers with database access

Authentication Servers
Keep track of users logged onto the network

File Servers
Store and manage files for network user

E-Mail Servers
Process and deliver incoming and outgoing e-mail

Communications Servers
Handle all communications between the network and other networks

Web/Cloud Servers
Host websites to make them available through the Internet

Servers
Authentication and File Servers

- Authentication servers
  - Keep track of who is logging on to network
  - Keep track of which services are available to each user
  - Act as overseers for the network
  - Manage and coordinate services provided by dedicated servers
- File servers
  - Store and manage files for network users

Servers
Print Servers

- Manage all client-requested printing jobs

  - Help computers be more productive

  - Free up CPU to do other jobs

- Print queue (print spooler) is a holding area for print jobs

  - Each printer has its own named print queue

  - Jobs print in order

  - Queue can be set to prioritize jobs

Servers
Application Servers

- An application server:
  - Acts as repository for application software
  - Delivers software when client computer makes request
  - Eases installation and upgrading
  - Application is installed or upgraded on application server

Servers
Database Servers

- Provides clients with information stored in databases

- Many people can access the database at one time

- Database resides only on the database server

Servers
E-Mail Servers

- How e-mail is handled on a large client/ server network

  – Processes and delivers incoming and outgoing e-mail

  – Large volume could overwhelm a server that handled other tasks

  – Handles routing and delivery of messages

Servers
Communications Servers

- Handle communications between network and other networks

- Manage Internet connectivity

- Have a heavy workload in most organizations

- Are only devices connected directly to Internet

- Provide single point of contact, make it easier to secure network from hackers

Servers
Web Servers

- Functions of a web server

  - Hosts a website

  - Makes it available to the Internet

  - Runs specialized software

  - Many businesses use hosting company instead

Servers
Cloud Servers

- Cloud servers

    - Not physically located at company office

    - Maintained by hosting companies

    - Connected to networks via the Internet

    - Can be used for any type of server
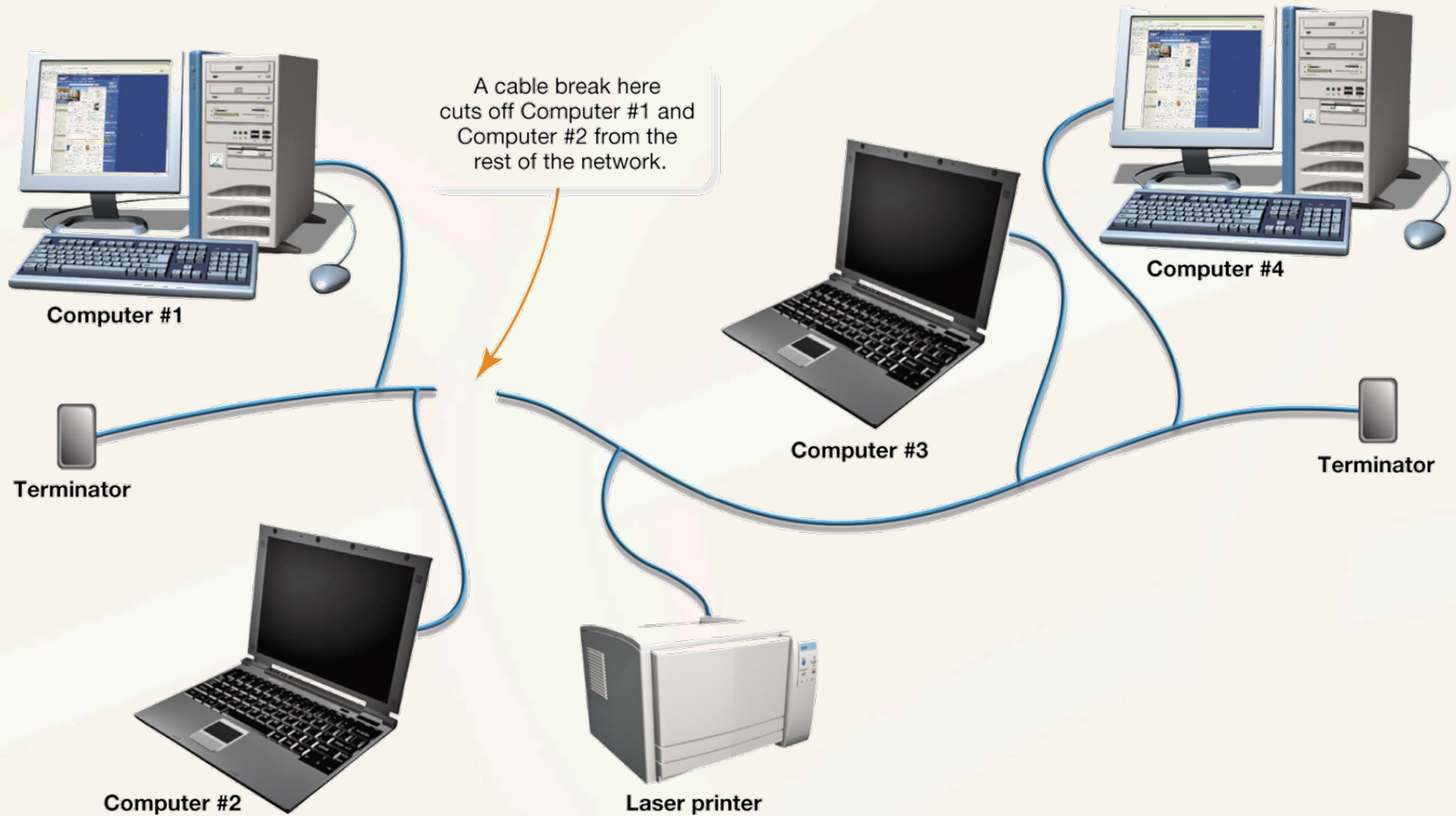
    - Can save money for small businesses

Network Topologies

- Physical: layout of the "real" components of the network

- Logical: virtual connections among network nodes

  – Determined by protocols instead of physical layout or paths that signals follow

Network Topologies

- Network protocols

  – Sets of rules for exchanging information

  – Most common topologies are bus, ring, and star

  – Type of topology affects a network's performance and scalability

Network Topologies
Bus Topology

A cable break here cuts off Computer #1 and Computer #2 from the rest of the network.

Computer #1

Computer #4

Terminator

Computer #3

Terminator

Computer #2

Laser printer

Network Topologies
Bus Topology

- Bus (linear) topology
  - All computers are connected in sequence with single cable
  - Data collisions happen when two computers send data at same time
  - Data is broadcast to all devices on network in packets
  - Passive topology (when each node does nothing to move data along)

Network Topologies
Bus Topology

- Advantages
  - Simplicity
  - Low cost

- Disadvantages
  - If cable breaks, the network is disrupted
  - Adding a large number of nodes limits performance and causes delays

Network Topologies
Ring Topology

STEP 1: The token travels around the ring until a computer needs to transmit data.

STEP 2: Computer #2 needs to print and grabs the token.

STEP 3: Computer #2 completes the transmission and releases the token.

STEP 4: A cable break stops movement of the token and data transmission.

Computer #1

Computer #4

Computer #2

Computer #3

Token Ring

Printer
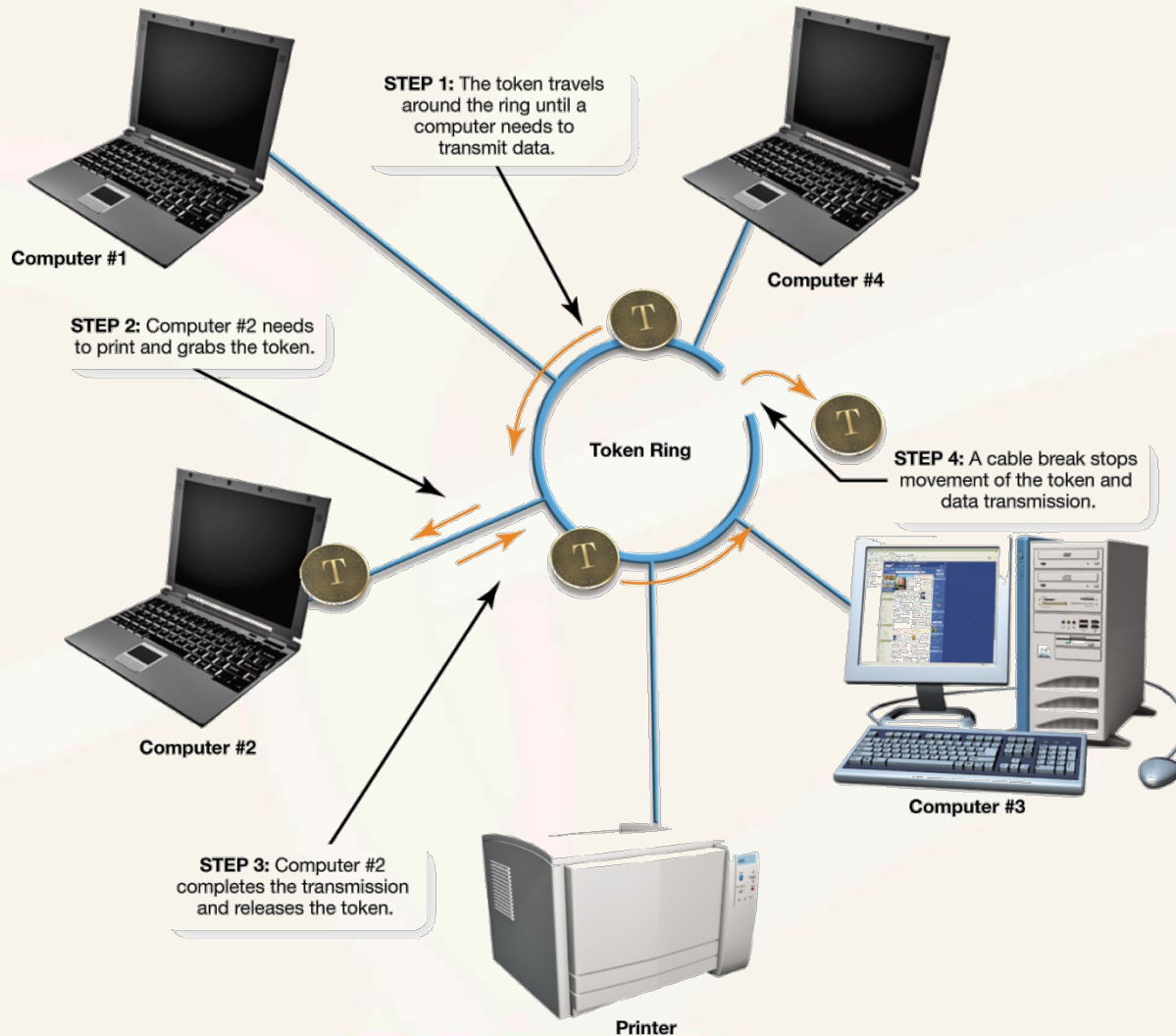
Network Topologies
Ring Topology

- Configuration resembles a loop

- Data flows around the circle in one direction in special packets (tokens)

- Token is passed until grabbed by a computer that needs to transmit data

- Computer "holds" token until finished transmitting data

Network Topologies
Ring Topology

- Advantages of a ring topology
  - Provides fairer allocation of resources
  - Enables nodes to have equal chance
  - Acceptable performance with many users
- Disadvantages of a ring topology
  - If one computer fails, entire network can fail
  - Problems can be hard to find
  - Ceases to function while node is installed

Network Topologies
Star Topology

Printer

Server

Computer #1

Computer #6

A cable break here means Computer #1 cannot communicate with the network. However, all other computers and devices can still communicate with each other.

Switch

Computer #5

Computer #2

Computer #3

Computer #4
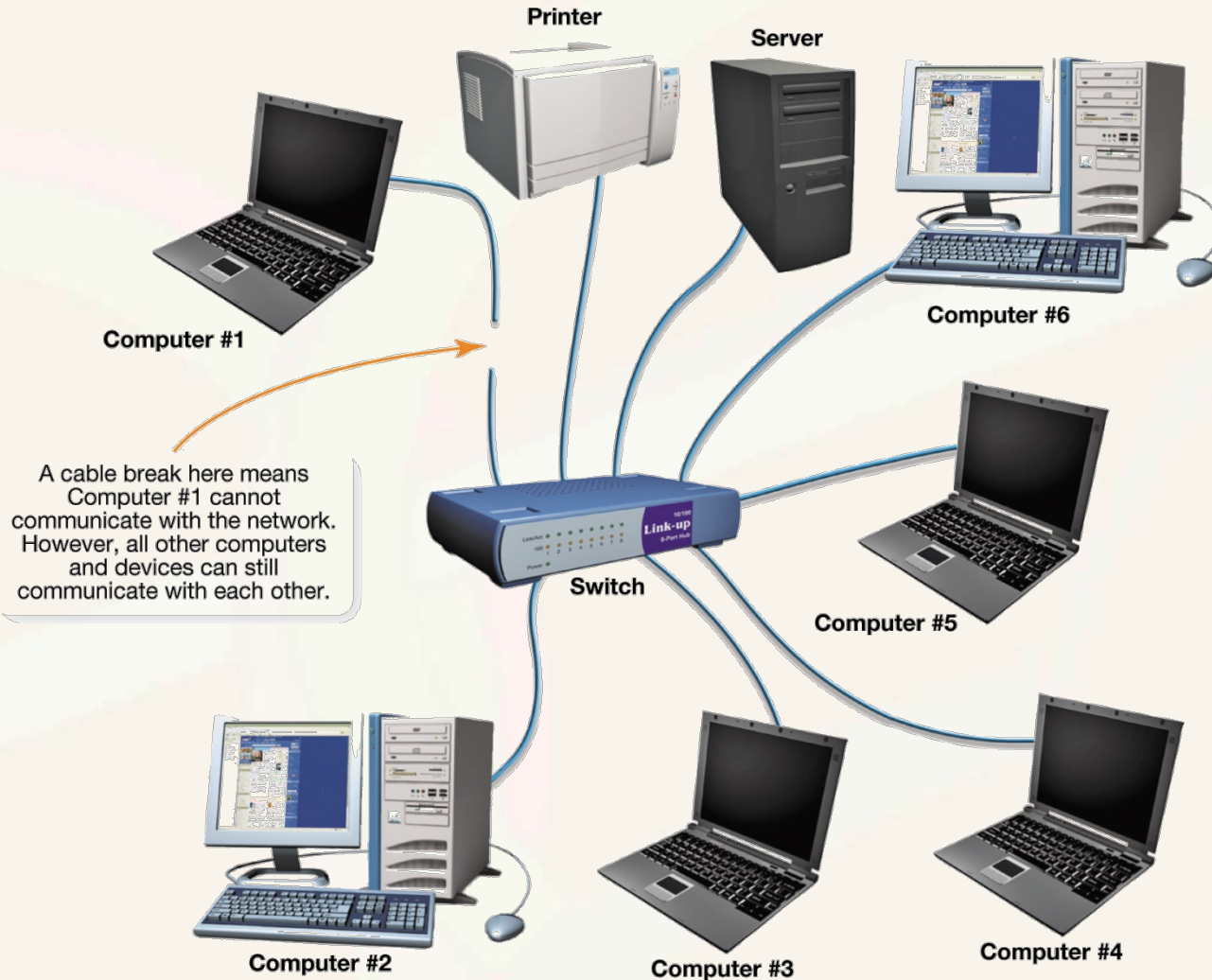
Network Topologies
Star Topology

- Nodes connect to central device in a star pattern
  - Node picks up transmissions addressed to it
  - Jam signal causes original nodes to stop transmitting when data collides
    - After random amount of time nodes try transmitting again

Network Topologies
Star Topology

- Advantages
  - Failure of one computer doesn't affect rest of network
  - Easy to add nodes
  - Performance remains acceptable even with large number of nodes
- Disadvantage
  - Requires more cable

Network Topologies
Comparing Topologies

Advantages and Disadvantages of Bus, Ring, and Star Topologies		
TOPOLOGY	**ADVANTAGES**	**DISADVANTAGES**
Bus	• Uses a minimal amount of cable. • Installation is easy, reliable, and inexpensive.	• Breaks in the cable can disable the network. • Large numbers of users decrease performance because of high volumes of data traffic.
Ring	• Allocates access to the network fairly. • Performance remains acceptable even with many users.	• Adding/removing nodes disables the network. • Failure of one node can bring down the network. • Problems in data transmission can be difficult to find.
Star	• Failure of one node doesn't affect other nodes on the network. • Centralized design simplifies troubleshooting and repairs. • High scalability: Adding computers is easy. • Performance remains acceptable even with many users.	• Requires more cable (and possibly higher installation costs) than a bus or ring topology. • The switch is a single point of failure; if it fails, all computers connected to it are affected.

Check Your Understanding

- What are the advantages of a business network?

- Resources (such as printers) can be shared

- Facilitation of knowledge sharing

- Software can be shared

- Information sharing is more effective

Check Your Understanding

- How does a client/server network differ from a peer-to-peer network?

- Servers exercise control over the network

- Data flows more efficiently in client/server networks

- Client/server networks are more scalable

Check Your Understanding

- What are the main classifications of client/server networks?

- Local area networks (LANs)

- Wide area networks (WANs)

- Metropolitan area networks (MANs)

Check Your Understanding

- What components are needed to construct a client/server network?

- Servers
- Topology
- Transmission media
- Network adapters
- Network navigation devices
- Network operating system (NOS) software

Check Your Understanding

- What do the various types of servers do?

- Authentication servers – control access
- File servers – store and manage user files
- Print servers – manage printing jobs
- Application servers – provide access to application software
- Database servers – store database files
- E-mail servers – manage e-mail traffic
- Communications servers – control flow of information to other networks
- Web servers – host websites
- Cloud servers – provide storage and access to data on the Internet

Check Your Understanding

- What are the various network topologies?

- Bus

- Ring

- Star

- Hybrid – blending of two or more topologies

Transmission Media

- Transmission media
  - Comprise the physical system that data travels between devices on the network
  - Network devices would be unable to communicate without transmission media
  - Most corporate networks use a combination of wired and wireless media

Transmission Media
Wired Transmission Media

- Why wired connections are used in business networks

  - Provide higher throughput and better security

  - Desktop computers are still popular choices

  - Permanence of desktop installation lends itself to wired connections

- Three main cable types (twisted-pair, coaxial, fiber-optic)

Transmission Media
Wired Transmission Media

- Six factors need to be considered
  - Maximum run length
  - Bandwidth
  - Bend radius (flexibility)
  - Cable cost
  - Installation cost
  - Interference

Maximum run length
- How far a cable can run before data signal degrades
- Distance between nodes determines run length needed

Bandwidth
- Amount of data transmitted across medium
- Measured in bits per second (BPS)

Flexibility (bend radius)
- How much a cable can be bent before it is damaged
- Lots of corners? Need cable with a high bend radius.

Cable cost
- Cost is different for each cable type
- Budget may limit choice of cable type

Installation cost
- Twisted-pair and coaxial cable are inexpensive to install (low $)
- Fiber-optic cable requires special training and equipment (high $)

Interference
- Twisted-pair most susceptible to interference
- Fiber-optic immune to interference

Transmission Media
Wired Transmission Media

- Causes of interference with data signals

  - Electromagnetic interference (EMI)

  - Radio frequency interference (RFI)

 - Fiber-optic cable is virtually immune to interference

Transmission Media
Twisted-Pair Cable

- Twisting the wires:
    - Causes magnetic fields to intermingle
    - Reduces amount of crosstalk
    - Shielded twisted-pair (STP) has foil shielding
    - Unshielded twisted-pair (UTP) is more susceptible to interference
    - Because of lower cost UTP is most often used

Transmission Media
Twisted-Pair Cable Anatomy
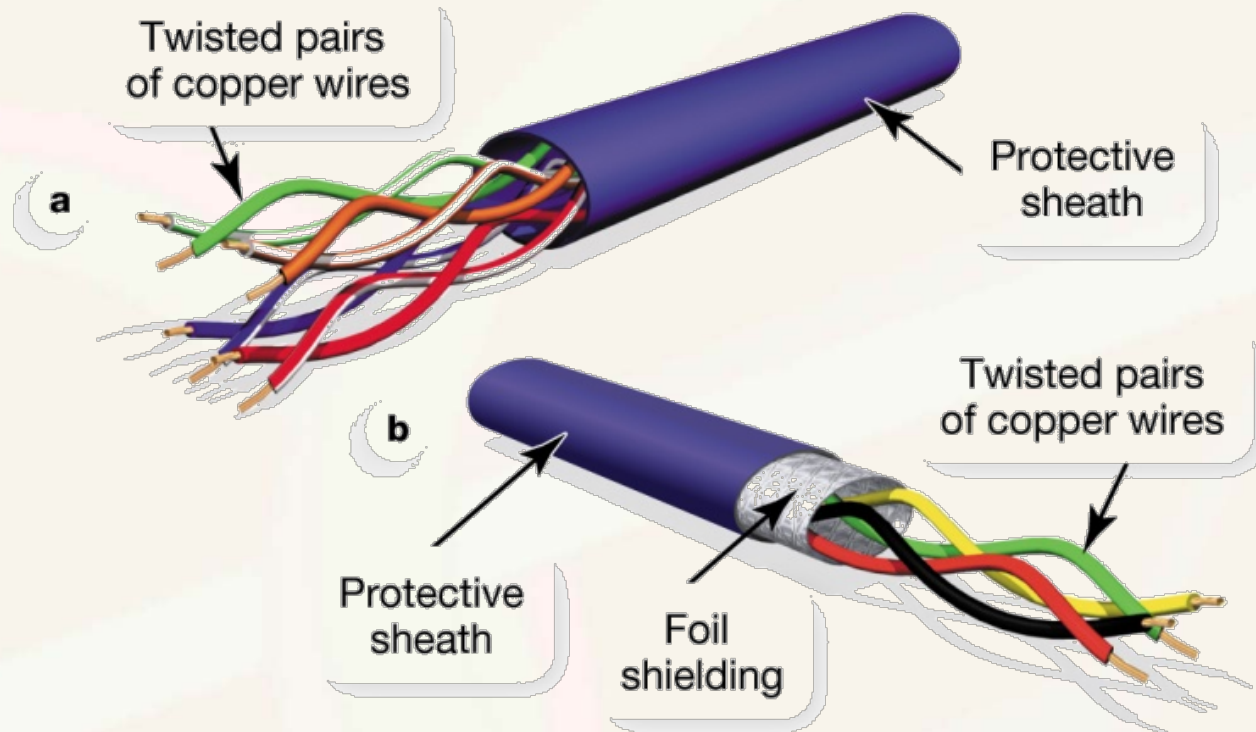
(a) unshielded twisted-pair (UTP) cable
(b) shielded twisted-pair (STP) cable

Transmission Media
Coaxial Cable

- Coaxial cable in business networks

  - Not as popular, but still used when there is heavy electrical interference

Plastic jacket

Plastic insulation

Copper core

Braided metal for shielding
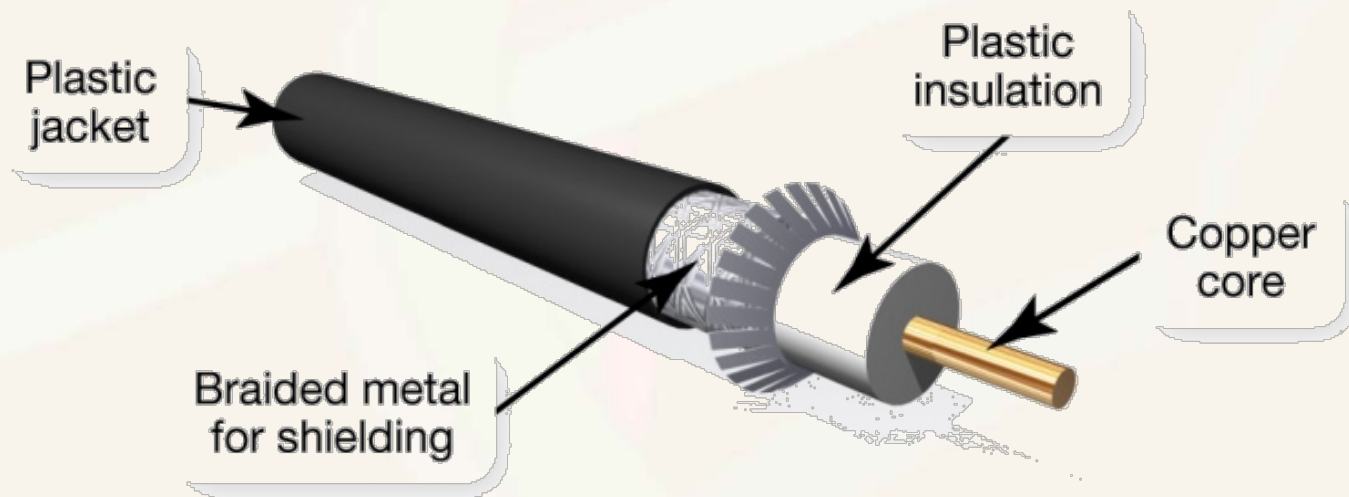
Transmission Media
Coaxial Cable

- Four main components of coax cable

  - Core for transmitting signal

  - Solid layer of nonconductive insulating material surrounds core

  - Layer of metal shielding covers insulation to reduce interference

  - External jacket covers protect internal cable components from damage

Transmission Media
Fiber-Optic Cable

- What fiber-optic cable looks like
  - Three major components
    - Glass (or plastic) fiber (or bundle of fibers) through which data is transmitted
    - Protective layer of glass or plastic wrapped around core to protect it
    - Outer jacket (sheath) made of durable material
  - Transmission passes in only one direction, so most cables have at least two fibers (cores)

Transmission Media
Fiber-Optic Cable Anatomy

Optical glass fiber

Protective sheath

Glass or plastic cladding
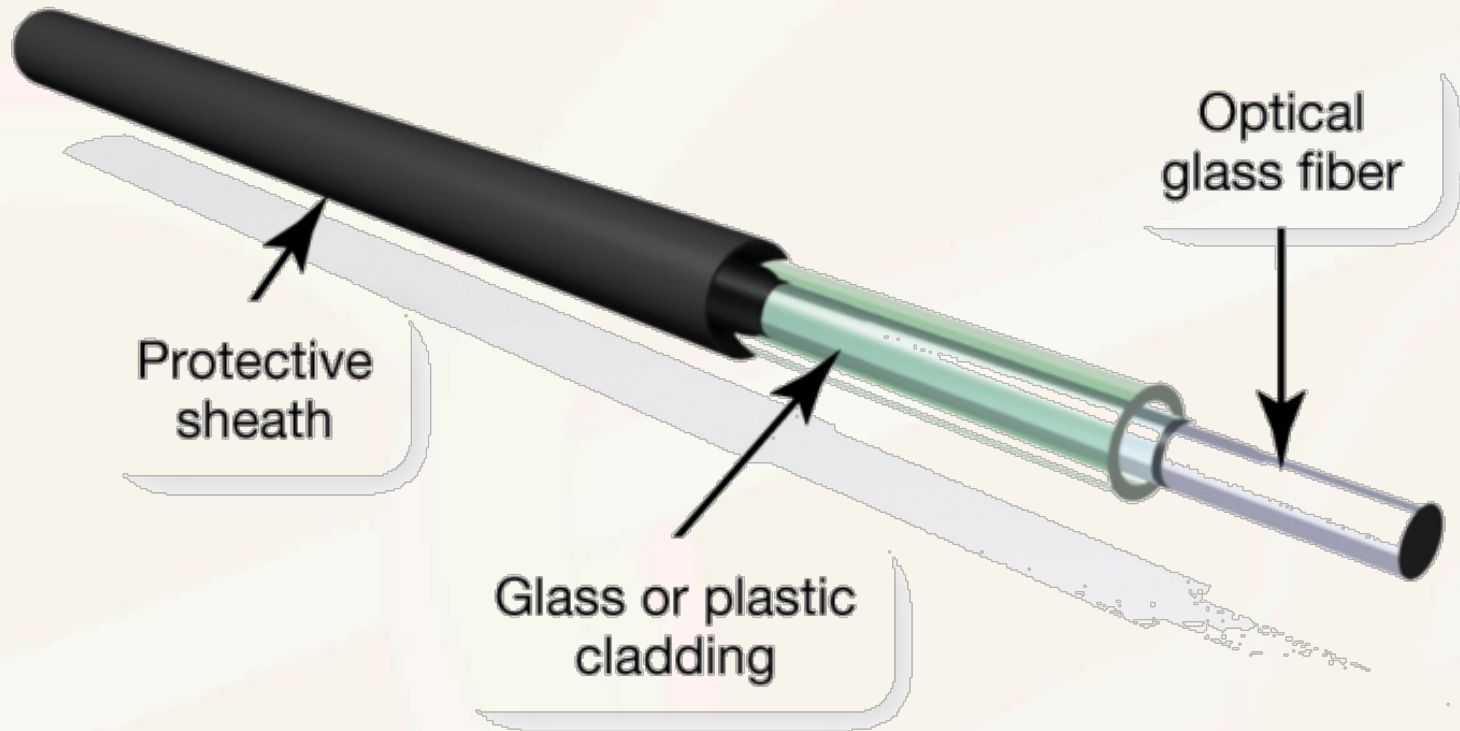
Transmission Media
Wireless Media Options

- Wireless media options
  - Most businesses use the same Ethernet standards as home networks
  - Wireless access points provide coverage wherever portable devices will be used

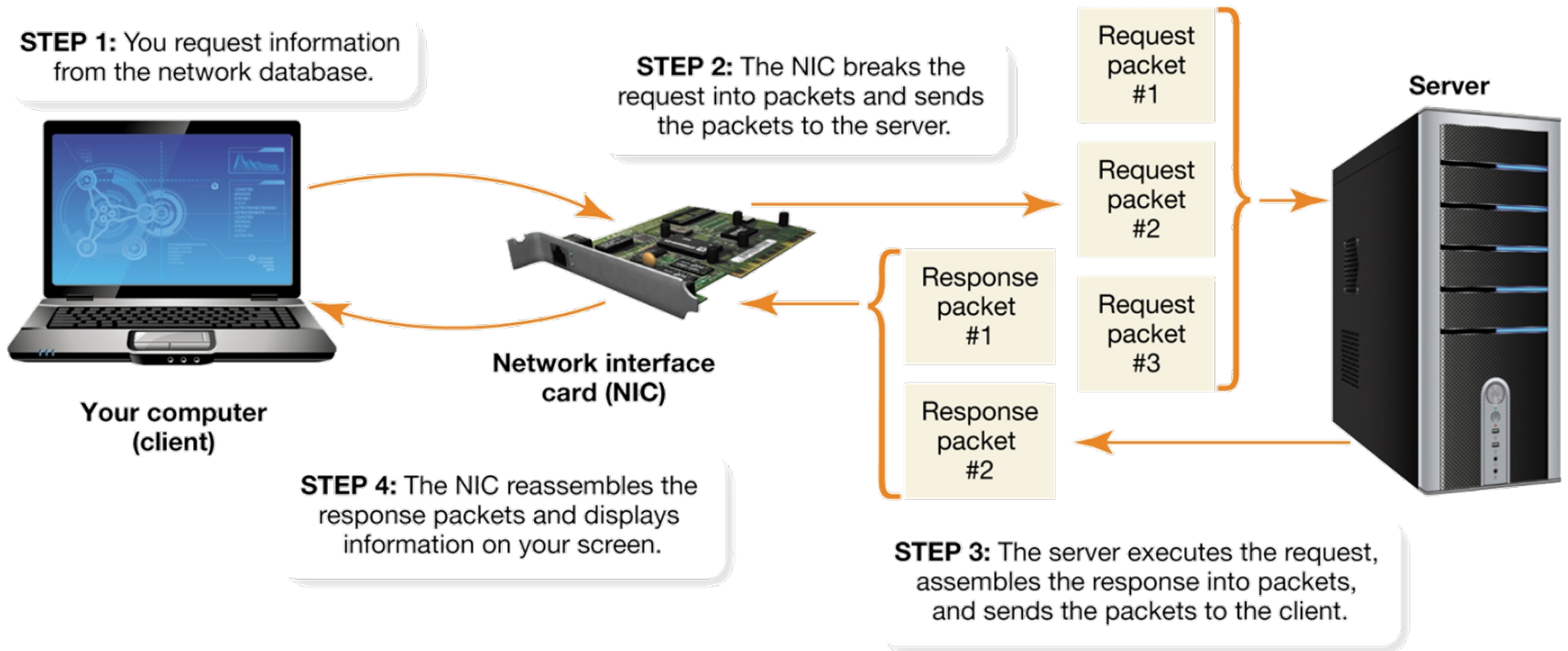# Transmission Media
Comparing Transmission Media

- Best medium for business networks
  - Network engineers are responsible for selecting the appropriate topologies and media
    - Topology to be used
    - Length of cable runs
    - Amount of interference
    - Need for wireless connectivity
  - Most use a mix of media types

Network Adapters

- Network adapters
  - Perform specific tasks
  - Enable nodes to communicate on network
  - Referred to as network interface cards (NICs)
  - Break data into packets
  - Act as gatekeepers for information flowing to and from client computer

Network Adapters
What Do They Do?

STEP 1: You request information from the network database.

STEP 2: The NIC breaks the request into packets and sends the packets to the server.

Request packet #1

Request packet #2

Request packet #3

Response packet #1

Response packet #2

Server

Network interface card (NIC)

Your computer (client)

STEP 4: The NIC reassembles the response packets and displays information on your screen.

STEP 3: The server executes the request, assembles the response into packets, and sends the packets to the client.

Network with Wireless Access Point

Desktop computer

Cat 6 cable

Server

Laptop computer
with wireless NIC

Switch

Link-up

Radio waves

Smartphone
with wireless NIC

Link-up

Wireless access point
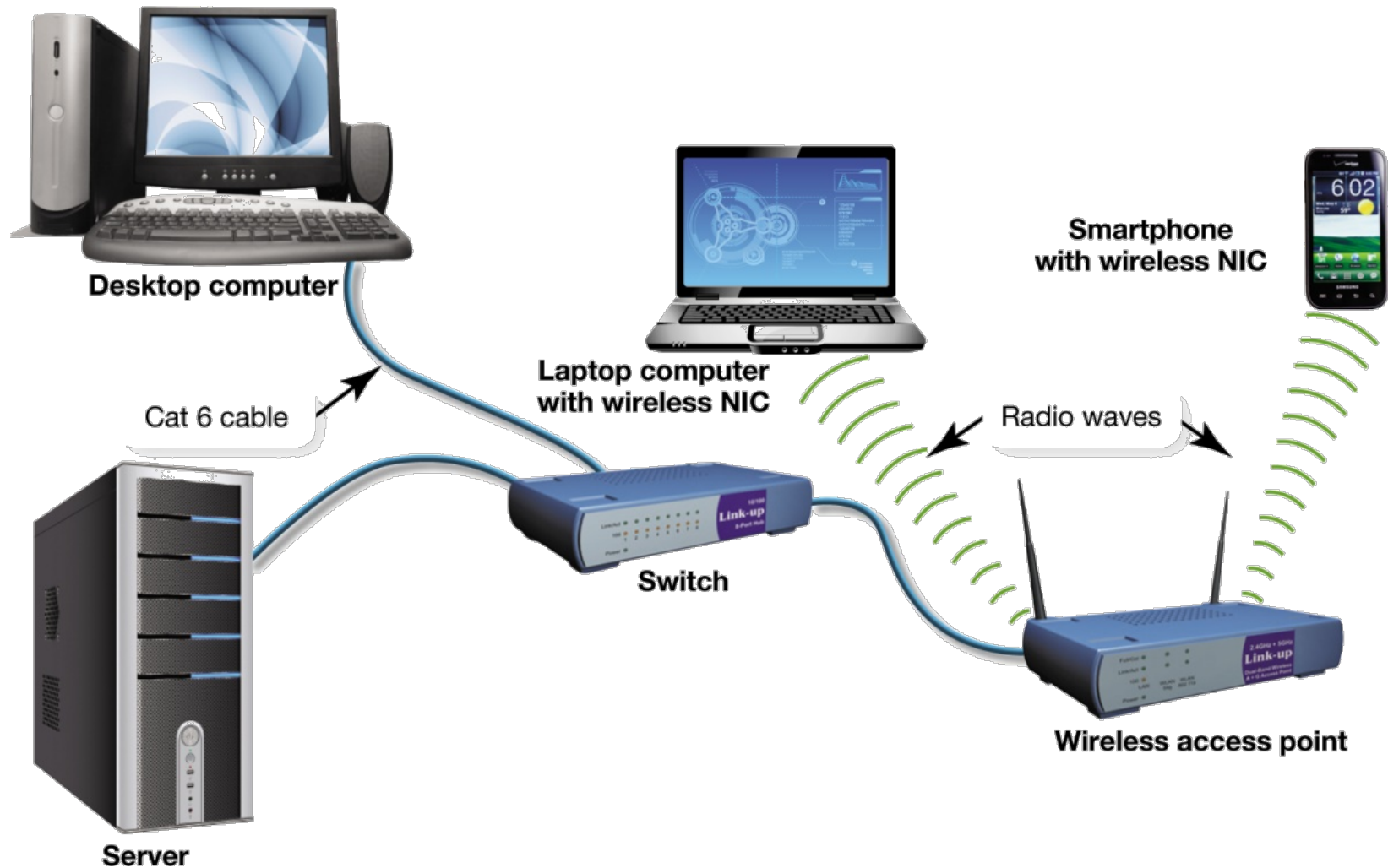
Network Navigation Devices
MAC Addresses

- How network adapters know where to send data packets
  - Network adapters have physical address, called a media access control (MAC) address
  - Institute of Electrical and Electronics Engineers (IEEE) allocates MAC addresses to adapter manufacturers
  - Not the same as IP addresses

Network Navigation Devices
Switches and Bridges

- Devices used to route signals through a single network
  - Switches rebroadcast data on specific route
  - Switches make decisions using MAC address
  - Improve network efficiency by ensuring node only receives intended data
  - Switches are not sufficient for moving data efficiently across networks of all sizes
  - Bridges are used to connect network segments (collision domains)

Network Navigation Devices
How a Switch Functions

Message for Computer #3

Switch

Server

Computer #1

Rebroadcast of message for Computer #3

Computer #2
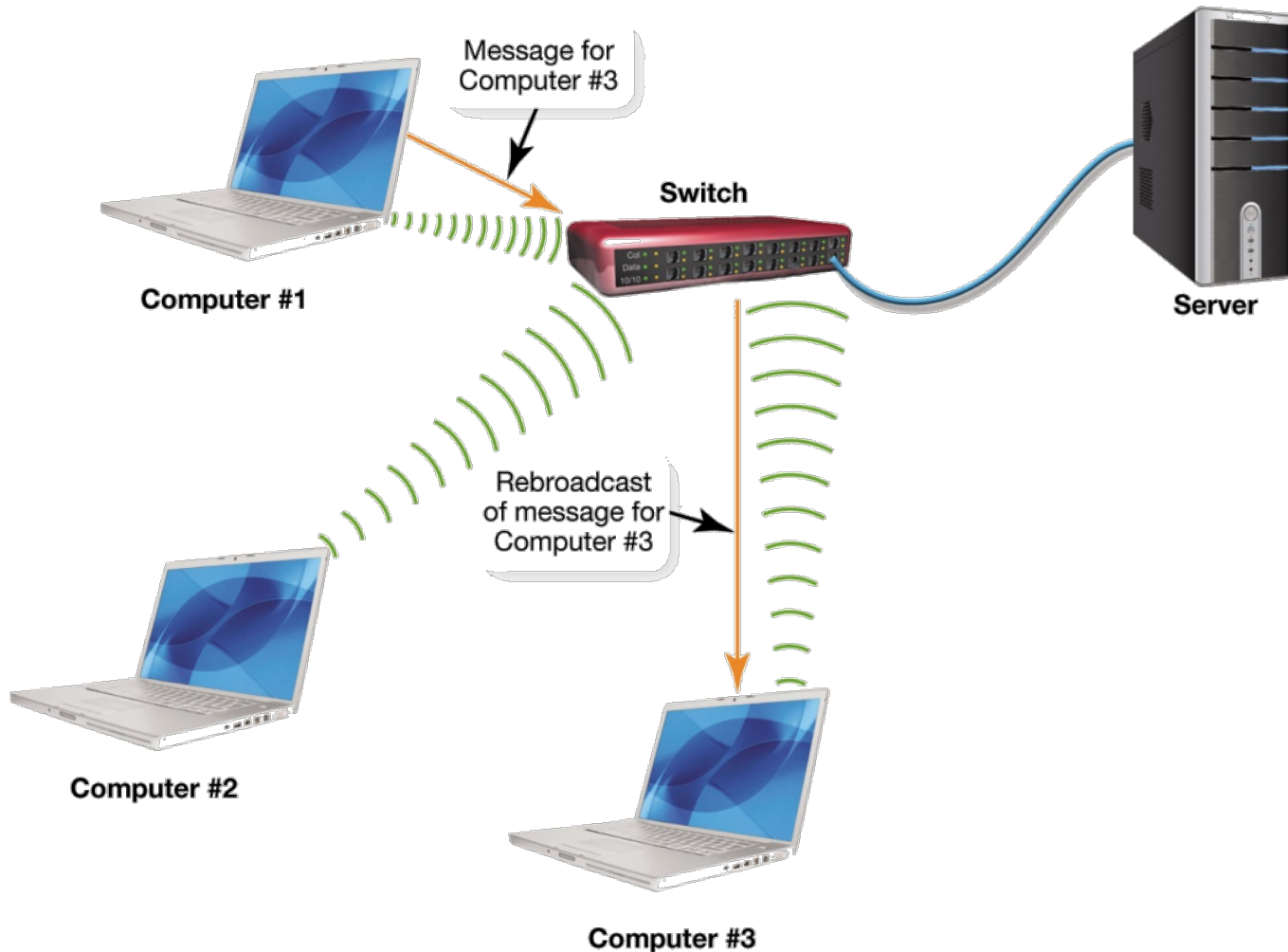
Computer #3

Network Navigation Devices Routers

- Routers move data between networks
  - Looks at higher level network addresses
  - When data address is not on network it sends data to another network, or Internet

Network Operating Systems

- Connecting computers doesn't automatically create client/server network
- Network operating system (NOS) is needed
- Modern operating systems include NOS software for peer-to-peer networking
- Client/server networks usually require sophisticated NOS software

Network Operating Systems

- How the NOS controls network communications
  - Each NOS has proprietary:
    - Communications language
    - File management structure
    - Device management structure
  - Sets and controls protocols for all devices
  - Internet uses open protocol (TCP/IP)
  - Modern NOSs support TCP/IP

Network Security for Client/Server Networks

- Sources of security threats

  - Human errors and mistakes

  - Malicious human activity

  - Natural events and disasters

Network Security for Client/Server Networks
Authentication

- Authentication is the process of approving which users can use a network

- Hackers can use people's accounts improperly to log into a network

Network Security for Client/Server Networks
Access Privileges

- Access privileges are granted when your account is set up

- Restricting access privileges protects a network

- Portable storage devices (such as flash drives) facilitate data theft

- Network administrators must protect networks from portable storage devices

Network Security for Client/Server Networks
Physical Protection Measures

Access card reader

Retinal scanning

Fingerprint/palm scanning

Facial recognition
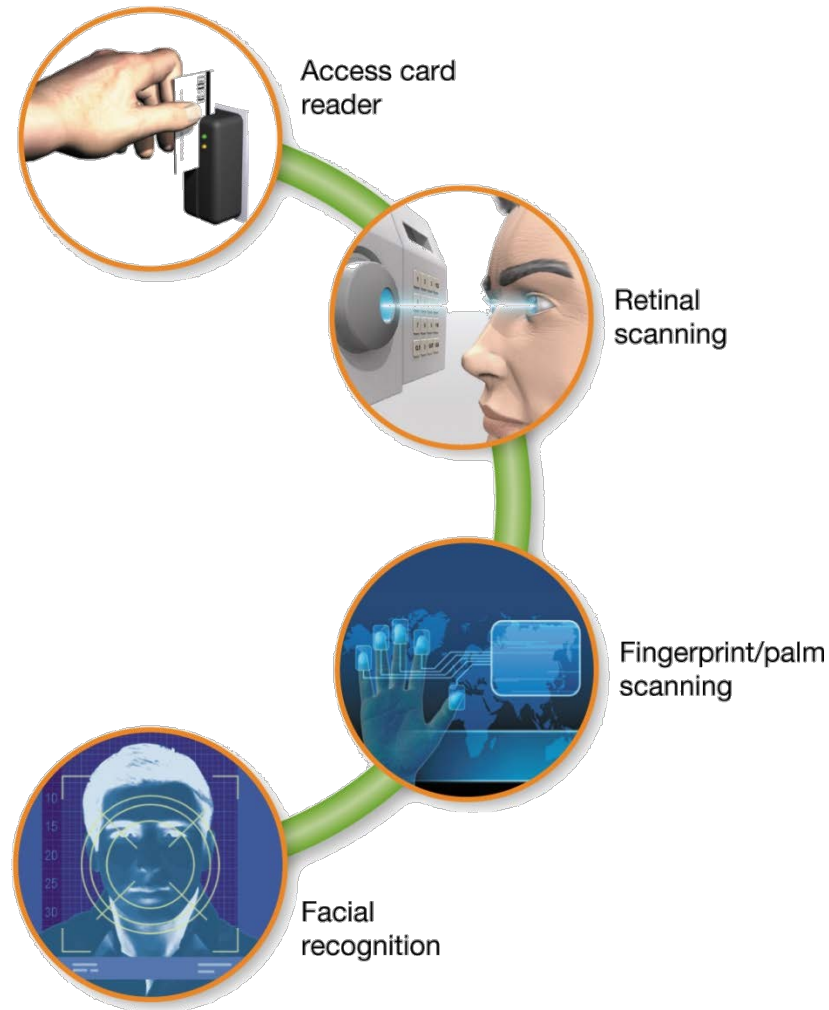
Network Security for Client/Server Networks Physical Protection Measures

- Biometric authentication devices use unique characteristic of human biology to identify users

- Problems with biometric devices

  - Don't always function as intended

  - Future fingerprint readers will use algorithms

  - Future retinal readers might check for blinks or whether pupils contract

Network Security for Client/Server Networks
Firewalls

- Internet connections on client/server networks are vulnerable to hackers

- Firewalls on a client/server network provide protection similar to a personal firewall installed on a home network

- Firewalls on client/server networks are usually more sophisticated than personal firewalls

Network Security for Client/Server Networks
Firewalls (cont.)

- A bastion host is a heavily secured server on a perimeter network
  - Honey pot
  - Configured as a Proxy server
    - Acts as go-between connecting internal computers with external network

Network Security for Client/Server Networks
Firewalls (cont.)
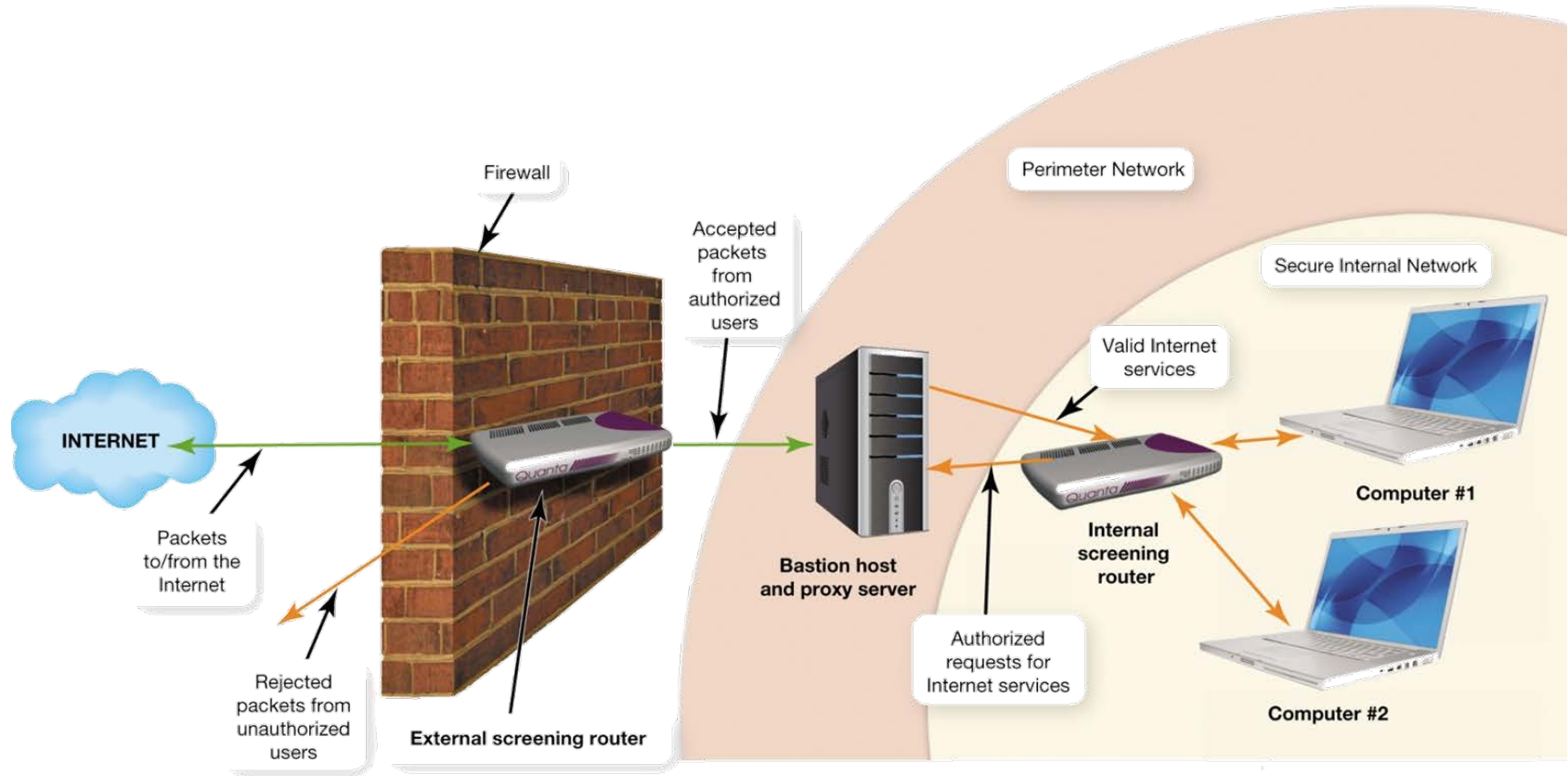
Check Your Understanding

- What types of transmission media are used in client/server networks?

- Wireless media
  - Uses radio waves
- Wired media
  - Twisted-pair cable
  - Coaxial cable
  - Fiber-optic cable

Check Your Understanding

- How do network adapters enable computers to participate in a client/server network?

- Network adapters
  - Convert low-power signals from the computer to high-power signals that can traverse media
  - Breaks data into packets
  - Control the flow of data to and from the computer

Check Your Understanding

- What devices assist in moving data around a client/server network?

- Switches – transmit data from node to node on a network

- Bridges – transmit data between two segments (collision domains) on the same network

- Routers – move data between two networks

Check Your Understanding

- What software needs to run on computers attached to a client/server network, and how does this software control network communications?

- Network operating system (NOS) software
- NOS provides common rules (protocols) that control communications between nodes

Check Your Understanding

- What measures are employed to keep large networks secure?

- Authentication procedures restrict access to authorized users

- Access privileges restrict users only to data and systems they need to access

- Access to networking equipment is physically restricted by locked doors and biometric devices