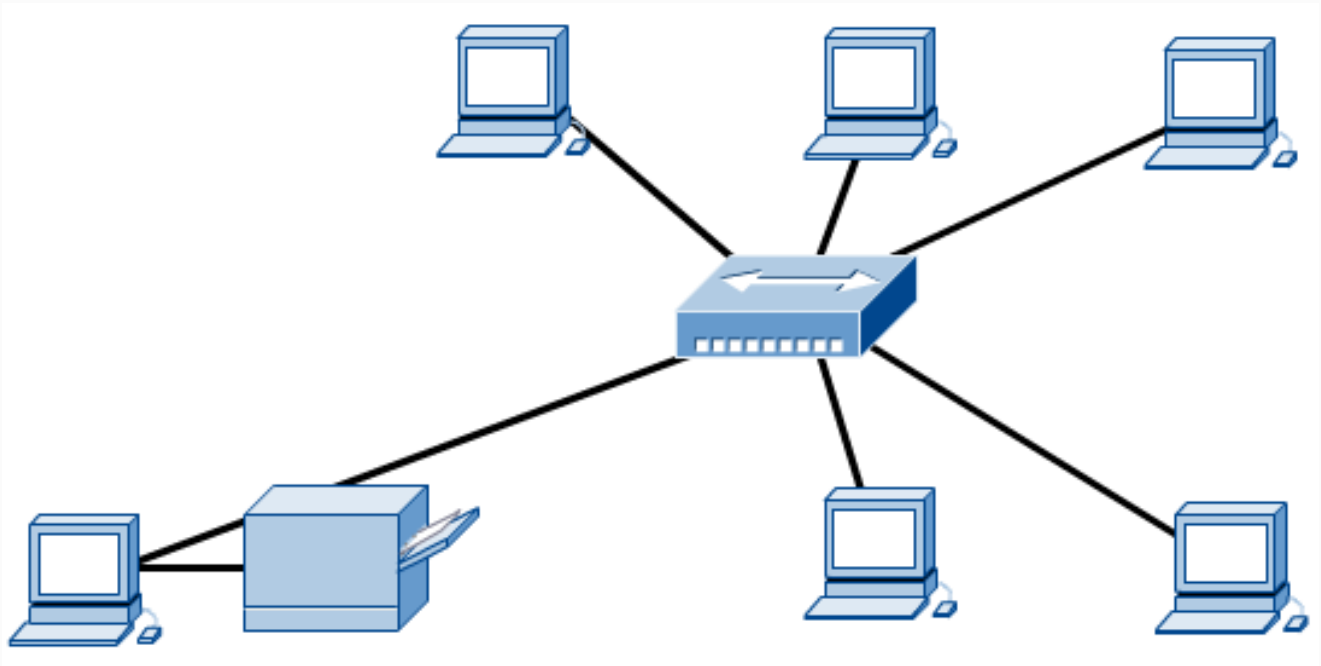
Telecommunications & Networking

Networking Fundamentals

Computer Networks

- A computer network is defined as having two or more devices (such as workstations, printers, or servers) that are linked together for the purpose of sharing information, resources, or both.



Why Do We Need Networking?

If you own multiple PCs, you have probably thought about how great it would be if your computers could talk to each other. With your computers connected, you could:

- Share a single printer between computers
- Share a single Internet connection among all the computers in your home
- Access shared files such as photographs, MP3s, spreadsheets and documents on any computer in the house. The need to share information is an important part of the development of computer networks.

Why Do We Need Networking? (cont…)

- It avoids duplication, conserves resources, and allows for the management and control of key information.
- Play games that allow multiple users at different computers
- Send the output of a device like a DVD player or Webcam to your other computer(s)

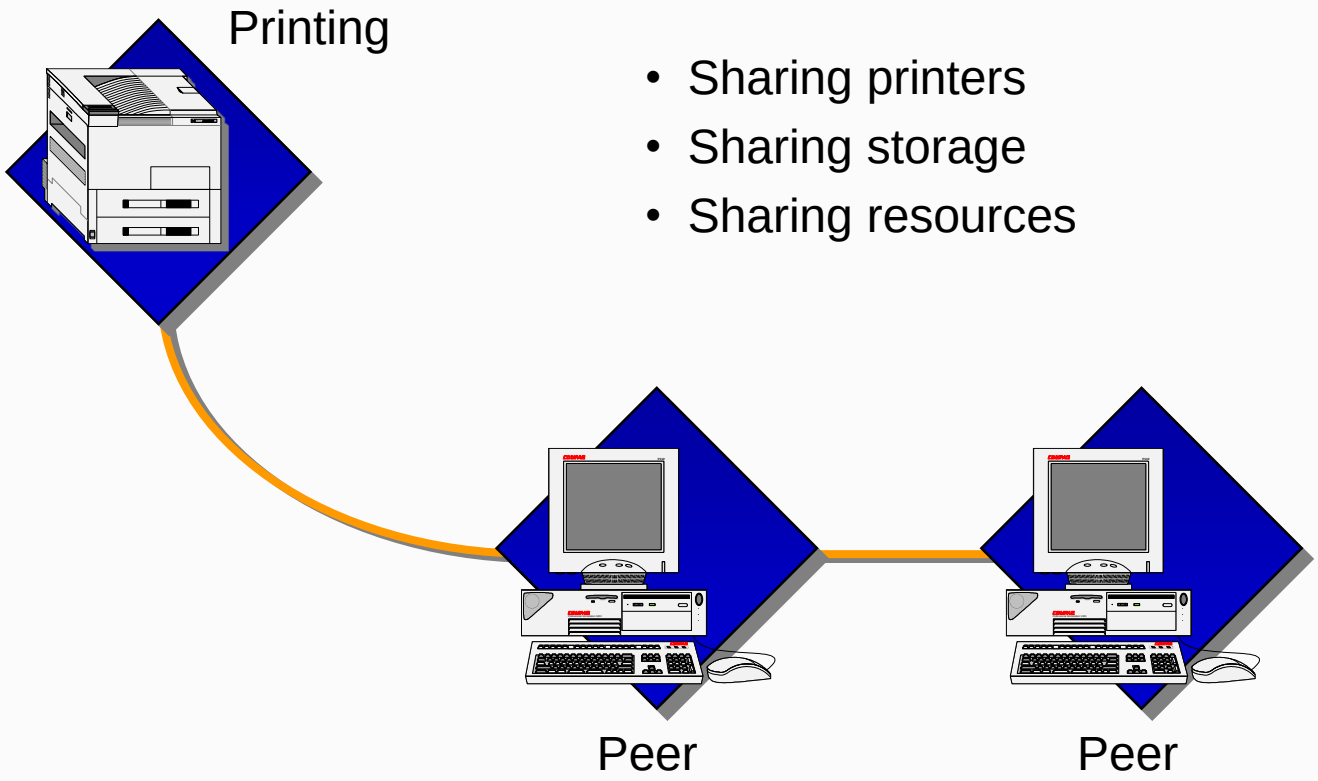
Network Administration

- The ongoing task of maintaining and adapting the network to changing conditions belongs to network administrators and support personnel.
- Network administrator responsibilities include setting up new user accounts and services, monitoring network performance, and repairing network failures.
- They evaluate new technologies and requirements, administrators must measure the benefits of the new features against the issues, costs, and problems that they may introduce to the network.

Overview of Networks

- In providing services, networked computers take on different roles or functions in relation to each other.
  - Two computers typically communicate with each other by using request/response protocols. The requester takes on the role of a client, and the responder takes on the role of a server. Then they switch roles (peer-to-peer).
  - Some computers take the role of server all the time to manage resources, share files, manage security, and provide services to all other computer on the network (client/server).
  - By using local-area network (LAN) and wide-area network (WAN) technologies, many computers are interconnected to provide services to their users.

A Peer-to-Peer Network



- Sharing printers
- Sharing storage
- Sharing resources

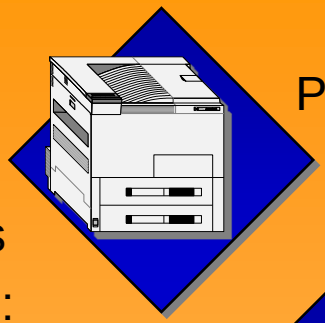
A Peer-to Peer Network

- In a peer-to-peer network, the networked computers act as equal partners, or peers, to each other. As peers, each computer can take on the client function or the server function alternately.
- In a peer-to-peer network, individual users control their own resources. They may decide to share certain files with other users and may require passwords before they allow others to access their resources.
- A peer-to-peer network works well with a small number of computers, perhaps 10 or fewer.

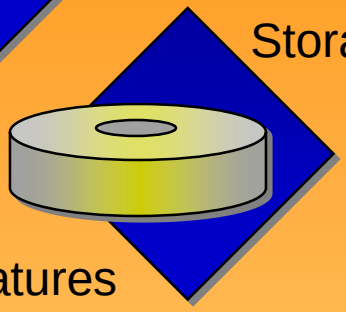
A Client/Server Network

Servers provide clients with access to:

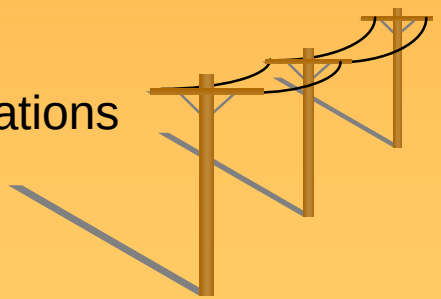
- Shared printers
- Network storage
- Network security features
- Other network resources



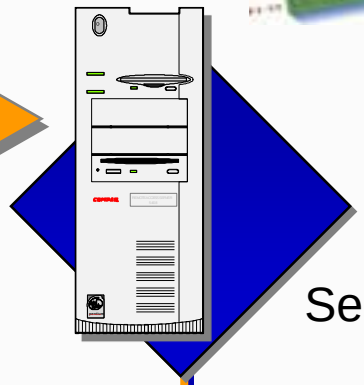
Printing



Storage

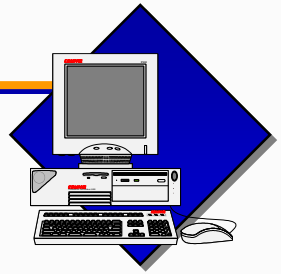


Communications



Server

Client

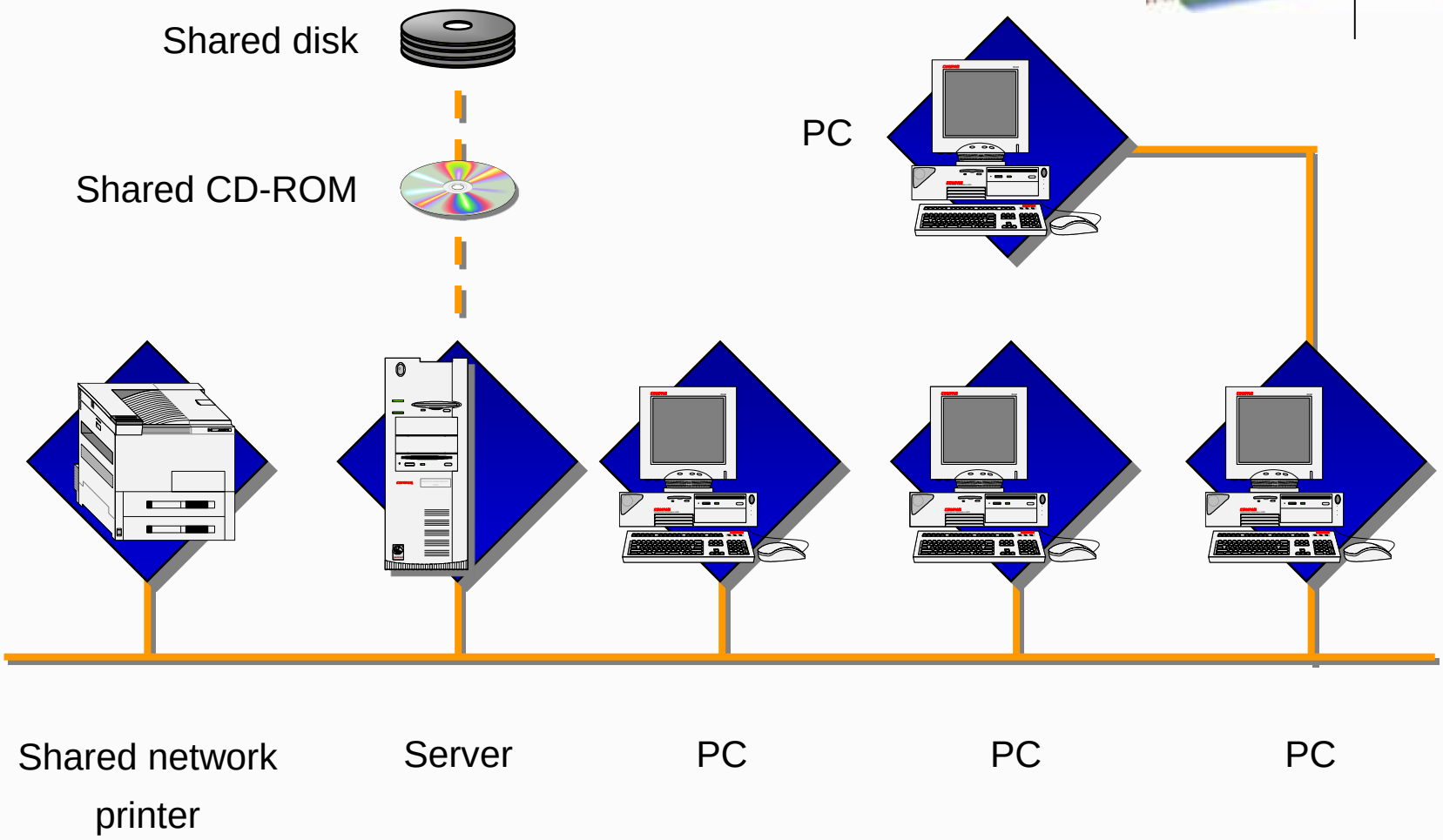


Client

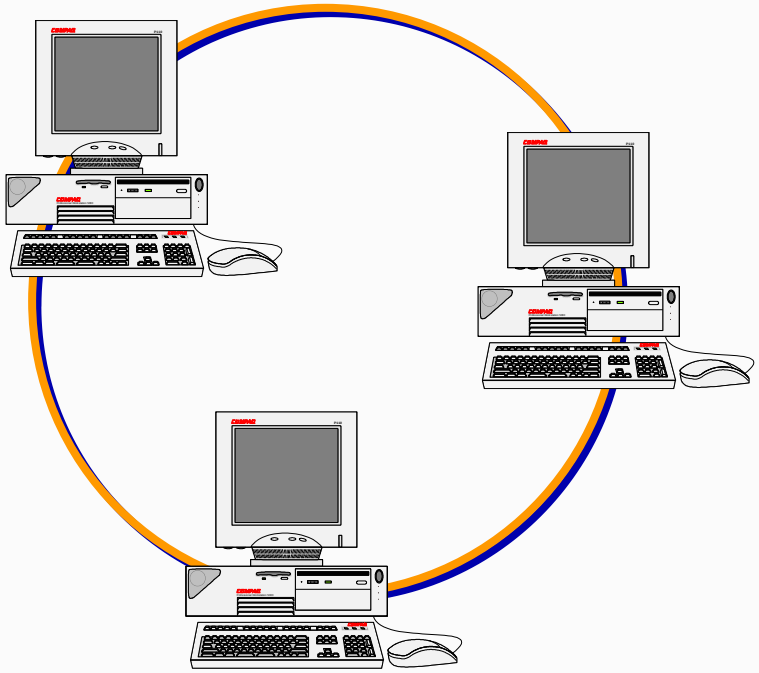
A Client/Server Network

- In a client/server network arrangement, network services are located in a dedicated computer whose only function is to respond to the requests of clients.
- The server contains the file, print, application, security, and other services in a central computer that is continuously available to respond to client requests.
  - Multiple computers can use a single installed application as long as you have purchased a user license for maximum number that will access the application at one time.
- Typically, desktop computers function as clients and one or more computers with additional processing power, memory, and specialized software function as servers.

A Typical Network



Since modern networks are based on protocols, **different OS's can communicate** and share information.



Local Area Network (LAN)
Small geographical area

Wide Area Network (WAN)
Large geographical area

Local-Area Networks

- The general shape or layout of a network is called its topology. A topology can refer to either a logical or physical layout.
- LANs connect many computers in a relatively small geographical area such as a home, an office, a building, or a campus.
- LANs require the networked computers to share the communications channel that connects them. The communications channel that they all share is called the medium.

Wide-Area Networks

- WANs connect computers in a large geographical area such as cities, states, and countries.
- Wide area connections between computers use point-to-point, **serial** communications lines. These lines are called point-to-point because they connect only two computers, one on each side of the line.
- Wide area connections make use of the communications facilities put in place by the utility companies, called common carriers, such as the telephone company.
- WANs typically connect fewer computers than LANs and normally operate at lower speeds than LANs. WANs, however, provide the means for connecting single computers and many LANs over large distances.

Circuit-switched vs. Packet-switched

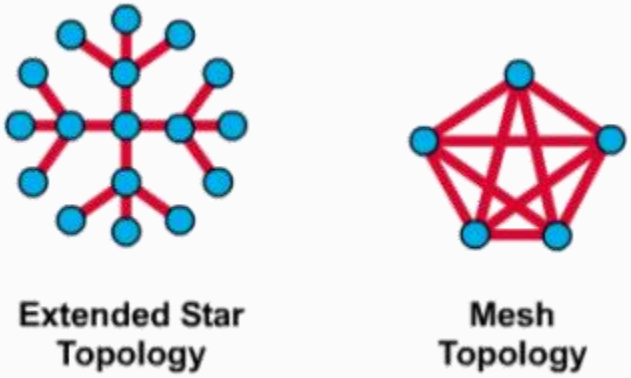
- In a **circuit-switched network**, a connection is established and all data is transmitted over that circuit (telephone system).
  - A modem connected to the phone system uses a circuit.
  - Connect one POTS (Plain Old Telephone System) to another
  - Any dial-up connection
- In a **packet-switched network**, each individual packet of data can take a different path.
  - Any always-on connection
  - Cable, DSL, T1
  - Internet traffic uses packet-switching technology.

Data Transmission

- The data channels over which a signal is sent can operate in one of three ways: simplex, half-duplex, or full-duplex.
  - **Simplex** is a single one-way baseband transmission that only travels in one direction.
  - **Half-duplex** transmission is an improvement over simplex because the traffic can travel in both directions but only in one direction at a time (transmit or receive).
    - Typically, a modem uses a half-duplex transmission
  - **Full-duplex** transmission operates like a two-way, two-lane street. Traffic can travel in both directions at the same time.

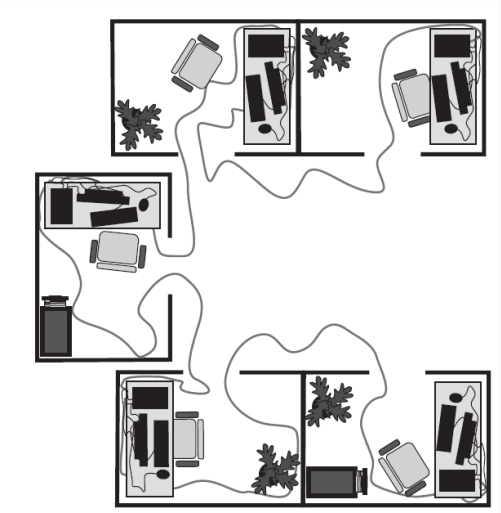
Physical Topologies

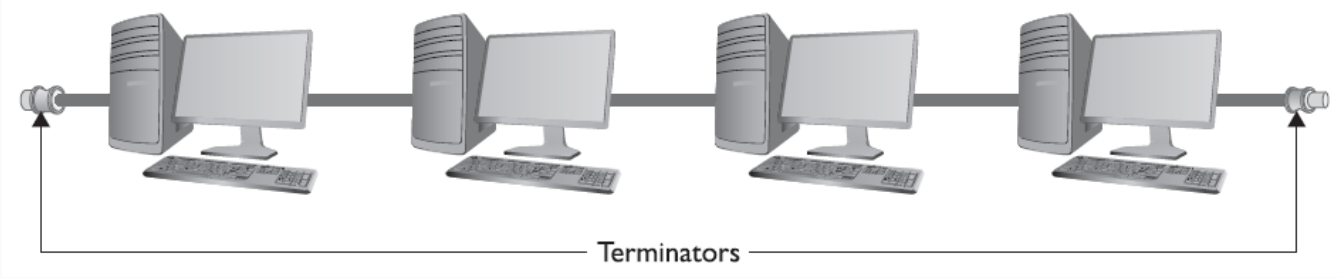
- The physical topology defines the way computer and other devices are connected.



Bus Networks

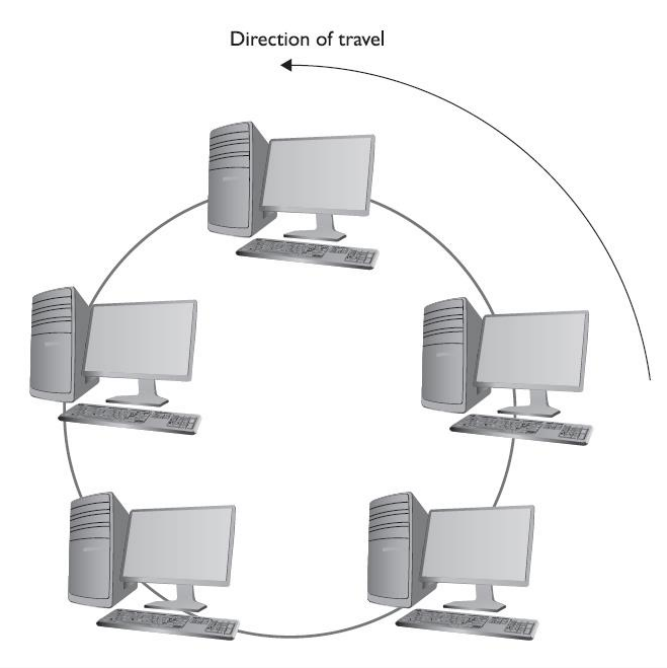
- First Generation of Network
- Required Terminators at each end
  - Prevent signal reflection
- Point of failures





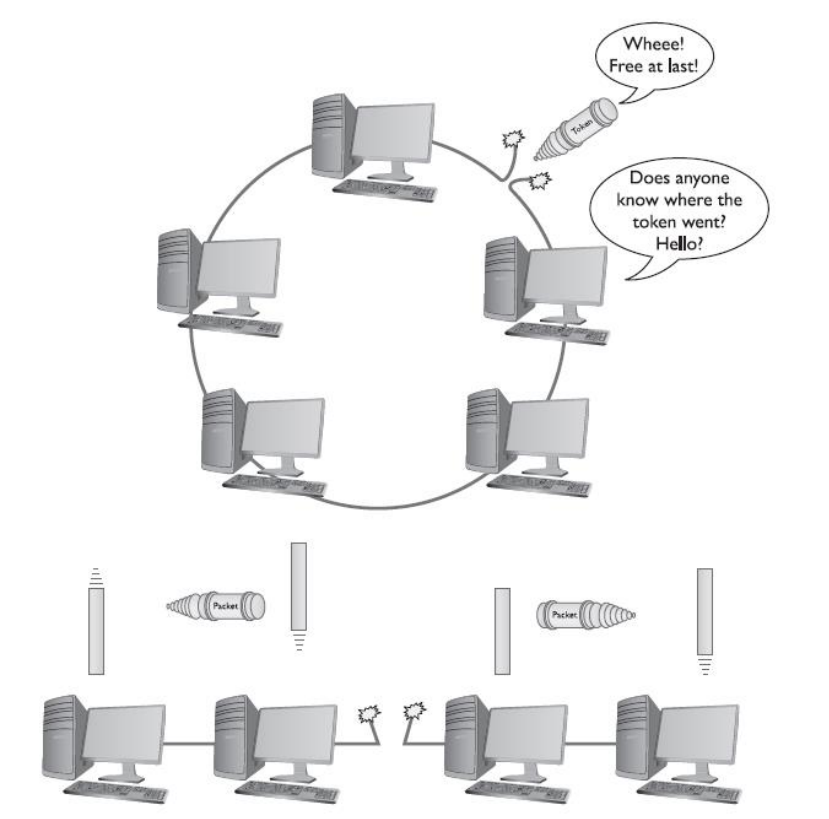
Token Ring Networks

- Data Moves in a Circle
- Token moves from computer to computer
  - Computer with token can "talk"



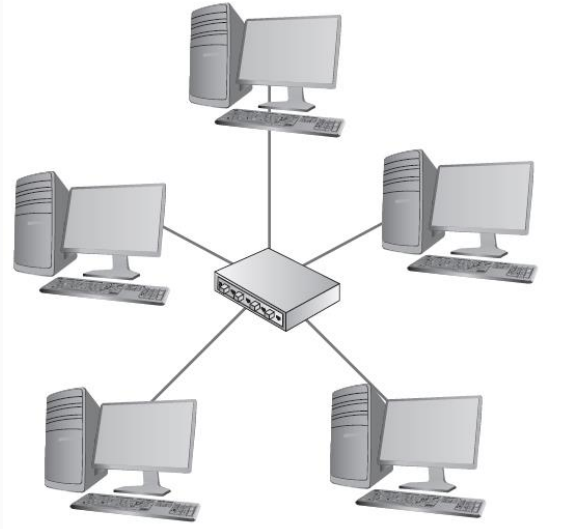
Star and Bus

- Suffers same problems in network faults



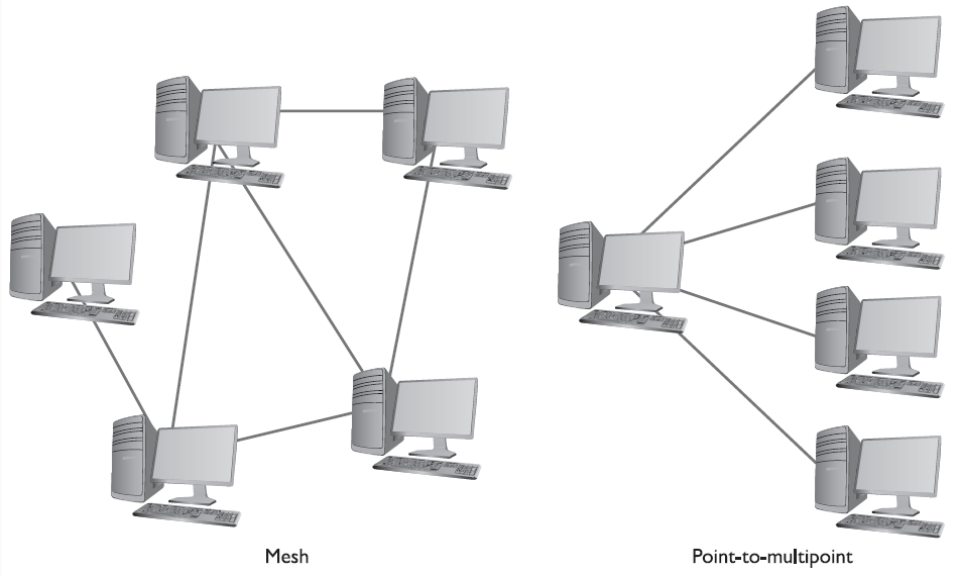
Star Networks

- Uses a central connection box for all networked computers
- Offers fault tolerance
  - One computer doesn't affect network



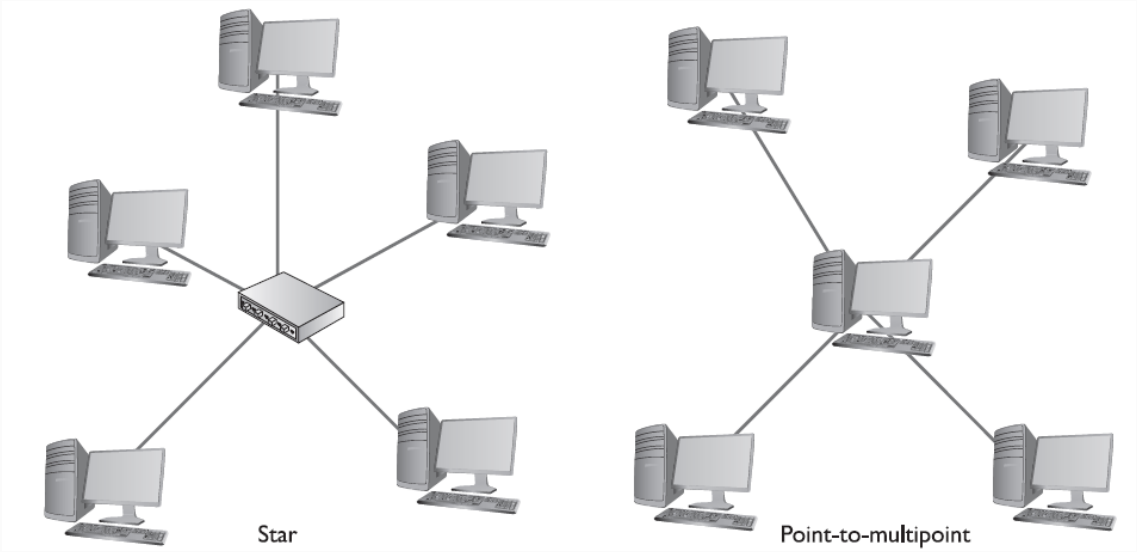
Mesh / Multipoint Networks

- Both used in most wireless networks
- Mesh has redundant connections



Mesh / Multipoint Networks

- Star and Point-to-multipoint not to be confused



Point to Point

- Two computers connect directly
- No central device

Physical vs. Logical Topology

- Networks can have both a physical and logical topology.
- Physical topology – Refers to the layout of the devices and media.
- Logical topology – Refers to the paths that signals travel from one point on the network to another. That is, the way in which data accesses media and transmits packets across it.
- A network can have a one type of physical topology and a completely different type of logical topology or they can be the same.

Types of Media

- Coaxial cable - copper-cored cable surrounded by a heavy shielding. Uses BNC connector.
- Twisted pair - Shielded and Unshield
  - Shielded - Shielded Twisted-Pair (STP) cable combines the techniques of cancellation and the twisting of wires with shielding. Uses STP connector
  - Unshielded Twisted-Pair (UTP) cable is used in a variety of networks. It has two or four pairs of wires. Uses RJ45 connector
- Fiber-optic cable is a networking medium capable of conducting modulated light transmissions.

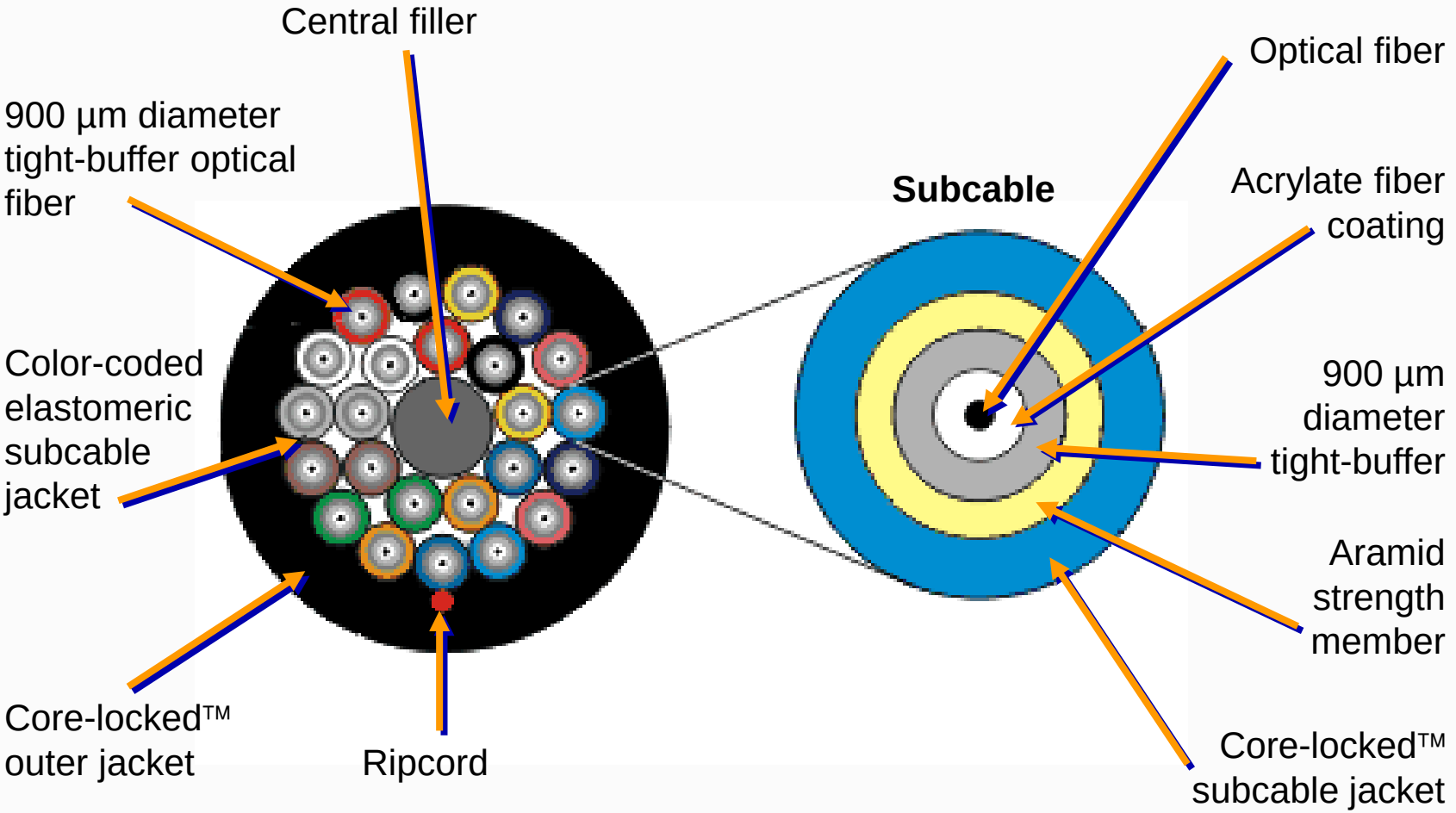
Network Cabling

10Base2 (ThinNet)	10 Mbps	Coaxial uses a BNC connector	185 meters or 607 feet
10Base5 (ThickNet)	10 Mbps	Coaxial uses an AUI 15-pin D-shaped connector	500 meters or 1,640 feet
10BaseT and 100BaseT (Twisted-pair)	10 or 100 Mbps	UTP or STP uses an RJ-45 connector	100 meters or 328 feet
10BaseF, 10BaseFL,	10 Mbps,	Fiber-optic cable uses an	500 meters up to

Ethernet UTP with RJ-45 Connectors

Coaxial Cable and BNC Connectors

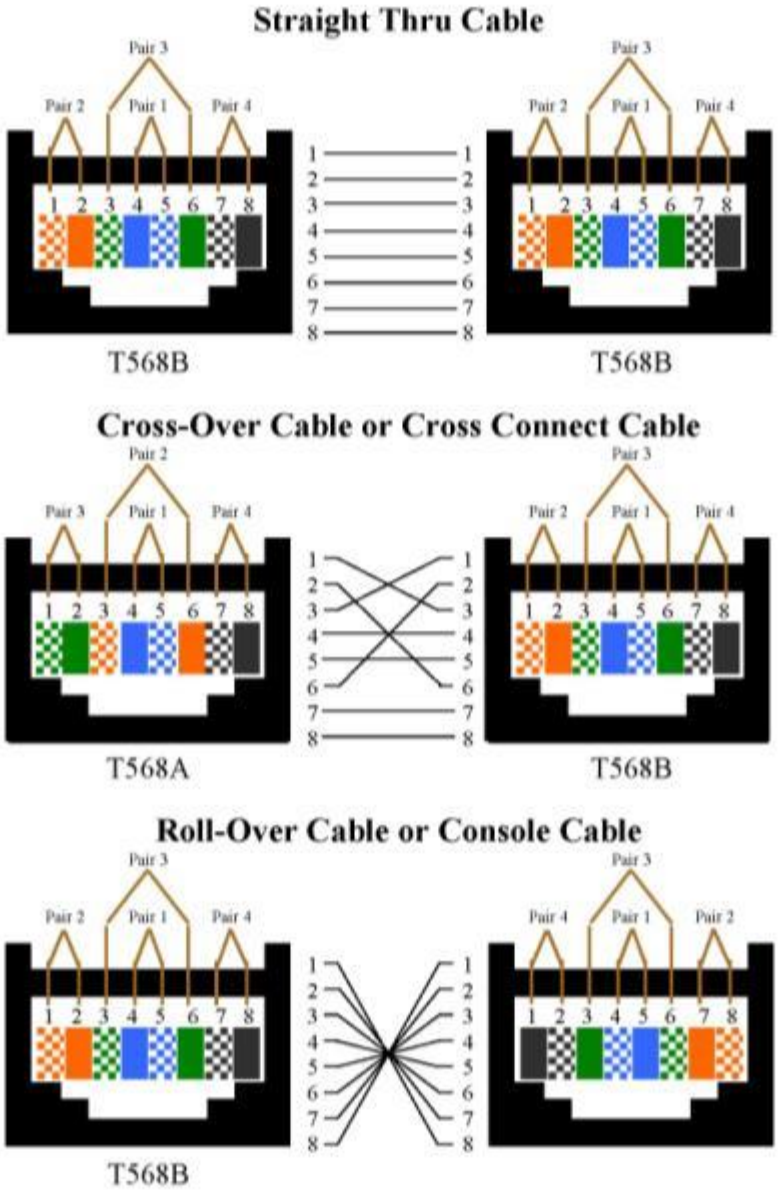
Fiber-optic Cable



RJ45 Pinouts

568A Scheme

- G/W
- G
- O/W
- B
- B/W
- O
- Br/W
- Br



568B Scheme

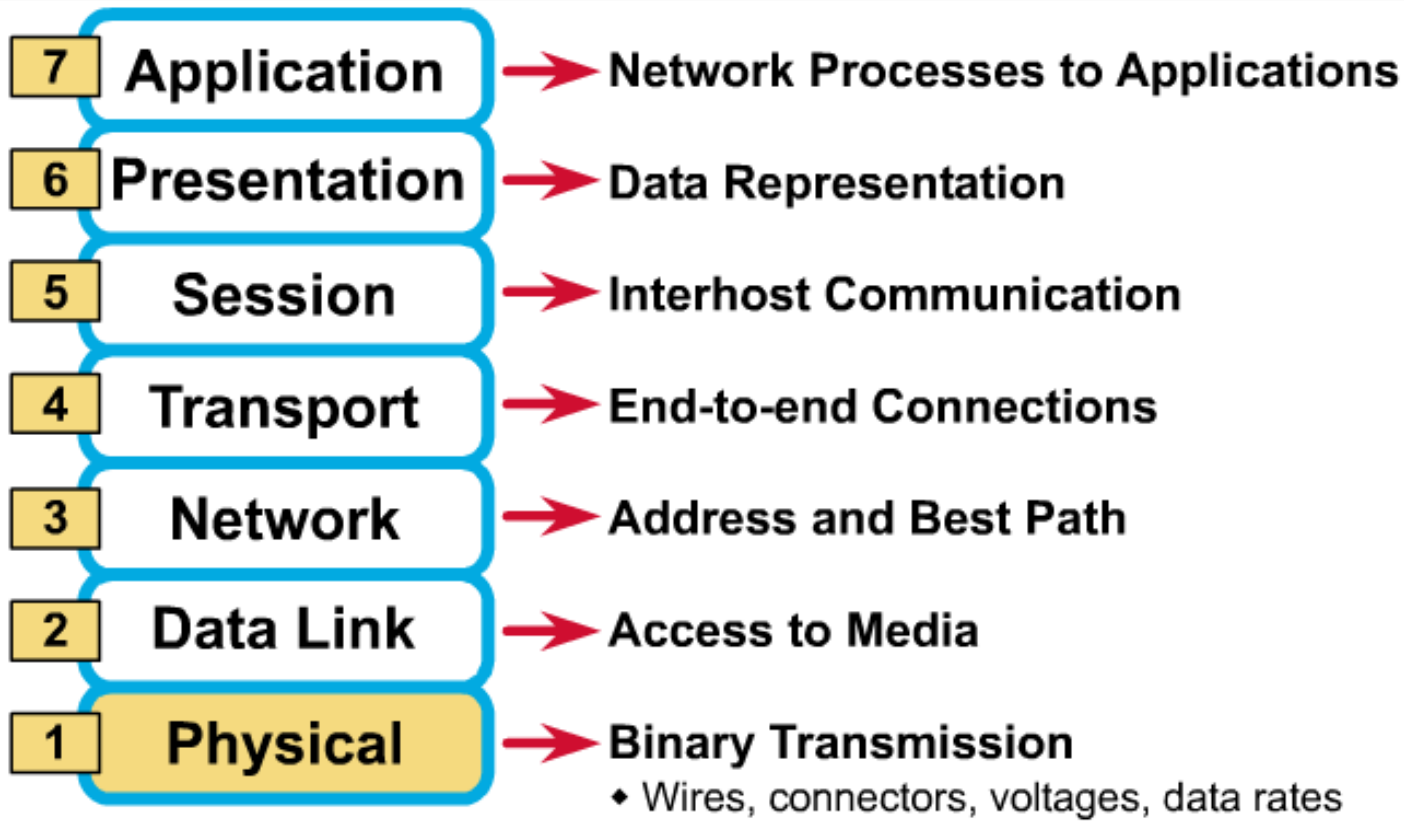
- O/W
- O
- G/W
- B
- B/W
- G
- Br/W
- Br

STANDARD

Networking Devices

OSI Model

- The Open Systems Interconnection (OSI) reference model is an industry standard framework that is used to divide the functions of networking into seven distinct layers.



Common Networking Devices

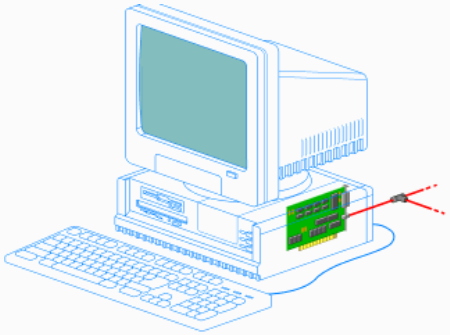
- **A Network Interface Card (NIC)** - a device that plugs into a motherboard and provides ports for the network cable connections. It is the computer's interface with the LAN.
- **Repeater** – a device that is used to extend an Ethernet wire to allow more devices to communicate with each other.
- **Hub** – A multi-port repeater. May be active (amplify and clean up the signal) or passive (signal is just split)

Common Networking Devices

- **Bridge**- connect network segments. The basic functionality of the bridge resides in its ability to make intelligent decisions about whether to pass signals on to the next segment of a network.
- **Switch** - sometimes described as a multi-port bridge. A switch is a more sophisticated device than a bridge.
- **Router** - the most sophisticated internetworking devices discussed so far. They are slower than bridges and switches, but make "smart" decisions on how to route (or send) packets received on one port to a network on another port.
- **Firewall** - a program or hardware device that filters the information coming through the Internet connection into your private network or computer system

Network Interface Card

- There are several important considerations to bear in mind when selecting a NIC to use on a network:
  - The type of network – NICs are designed for Ethernet LANs, Token Ring, FDDI, and so on.
  - The type of media –such as twisted-pair, coaxial, fiber-optic, or wireless.
  - The type of system bus –PCI or ISA.
- Today its common to find the network connected to USB.



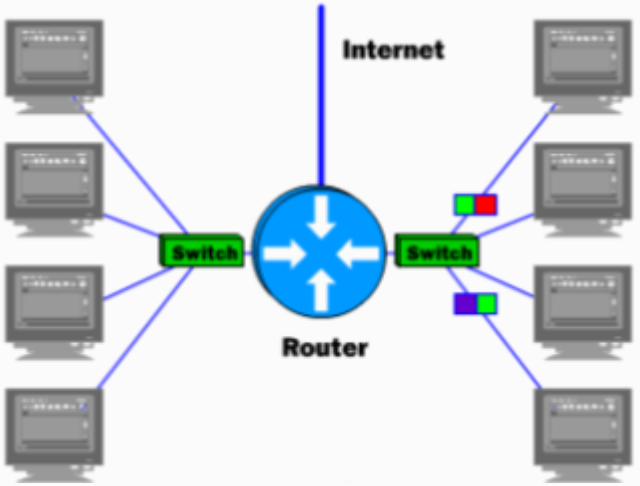
Switches

Switches are a vital part of today's LANs. Switches allow out high speed networks (100/1000Mbps) to travel without collisions. A switches main functions are:

1. Make intelligent decisions based on a computers MAC address (layer2)
2. It is primarily used to connect network segments.
3. Break collision domains
4. Interconnect different switches with a high speed backbone.

Routers

Much of the work required to get information from one computer network to another is done by **routers** -- they're the crucial devices that let information flow between, rather than within, networks. Routers are specialized computers that send your messages, and those of every other Internet user, speeding to their destinations along thousands of pathways. When information needs to travel between networks, routers determine how to get it there. A router bases all of its decisions on IP addresses (layer 3).



Routers

A router has two separate but related jobs:

1. It ensures that information doesn't go where it's not needed. This is crucial for keeping large volumes of data from clogging the connections of "innocent bystanders."
2. It makes sure that information makes it to the intended destination(s).

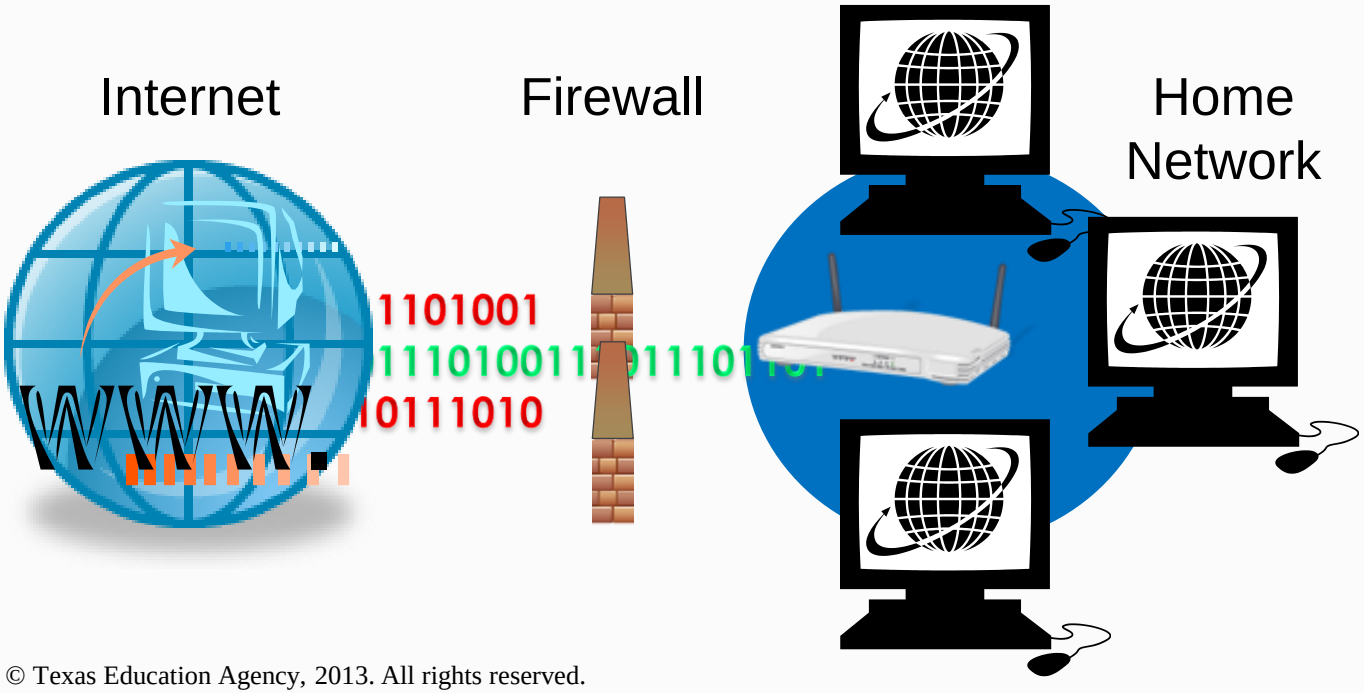
In performing these two jobs, a router is extremely useful in dealing with two separate computer networks. It joins the two networks, your home network and the Internet in this case, passing information from one to the other. It also protects the networks from one another, preventing the traffic on one from unnecessarily spilling over to the other. Regardless of how many networks are attached, the basic operation and function of the router remains the same. Since the Internet is one huge network made up of tens of thousands of smaller networks, routers are an absolute necessity.

Firewalls

- Whether you are one of the growing number of computer users with fast, always-on Internet access or you're still using a dial-up connection, you may want to consider implementing a **firewall**. A firewall is simply a program or hardware device that filters the information coming through the Internet connection into your private network or computer system. You use a firewall to protect your home network and family from offensive Web sites and potential hackers. If an incoming packet of information is flagged by the filters, it is not allowed through.
- You should note that some spam is going to get through your firewall as long as you accept e-mail. And, while some firewalls offer virus protection, it is worth the investment to install anti-virus software on each computer.

Firewalls

- Hardware firewalls are incredibly secure and not very expensive. One of the best things about a firewall from a security standpoint is that it stops anyone on the outside from logging onto a computer in your private network.



Networking Standards

IEEE 802 Standards

- 802.1: High-level interface
- 802.2: Logical link control
- 802.3: CSMA/CD (Ethernet)
- 802.4: Token Bus
- 802.5: Token Ring
- 802.6: MANs
- 802.7: Broadband LANs
- 802.8: Fiber-optic LANs
- 802.9: Integrated data and voice networks
- 802.10: Security
- 802.11: Wireless networks

Most Popular Physical Network Architectures

- Ethernet (most popular)
- Token ring
- FDDI (Fiber Distributed Data Interface)
- Wireless LAN technology

Ethernet

- The Ethernet architecture is now the most popular type of LAN architecture.
- The Ethernet architecture is based on the IEEE 802.3 standard. The IEEE 802.3 standard specifies that a network implements the Carrier Sense Multiple Access with Collision Detection (CSMA/CD) access control method.
- Wireless and Satellite both use Ethernet
  - Satellites are located over the equator
  - Weather can effect its performance

Ethernet Networking

Ethernet has many advantages:

- It is the fastest home-networking technology (100 Mbps).
- It can be inexpensive if the computers are close to one another.
- It is extremely reliable.
- It is easy to maintain after it is set up.
- The number of devices that can be connected is virtually unlimited.
- There is a great deal of technical support and information available.

And a few disadvantages:

- If you have more than two computers, you'll need additional equipment.
- It can be expensive if wiring and jacks need to be installed.
- Set-up and configuration can be difficult.
- The technical jargon and the number of options can be confusing.

Ethernet Networking

- To connect the computers, you will need **Unshielded Twisted Pair** (UTP) Category 5e cable. This type of cabling is designed to handle speeds up to 1000-Mbps needed by Ethernet. The RJ-45 connector at the end of the cable looks very similar to the RJ-11 connector on a phone cord but is slightly bigger (and not compatible).
- You can buy Cat 5e cables in predetermined lengths with the connectors already attached (expensive).
- If you plan to install the Cat 5e cabling in the walls of your house, you can buy the cable in rolls, cut it to length and connect the cable to special RJ-45 wall boxes. UTP has a maximum usable length of 100 meters.

Ethernet Networking

*Note: If you want to connect **just two computers**, you can avoid the hub or switch and use a **crossover Cat 5 cable**. With a crossover cable, you directly connect one NIC card to the other without a hub or switch. This only works for two computers -- to connect more than two you need a hub or switch.

Ethernet Variations, Distinguished by Speed

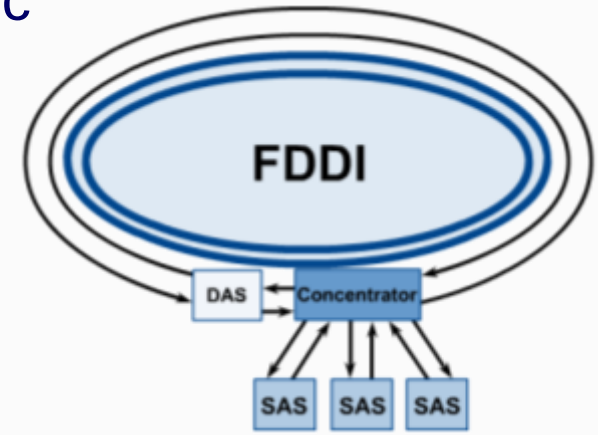
- 10-Mbps Ethernet
  - Uses either shielded twisted-pair (STP) cable, unshielded twisted-pair (UTP) cable (CAT3 or higher), or coaxial cable
- 100-Mbps Ethernet or Fast Ethernet
  - Uses UTP (CAT5 or higher) or STP cable
  - 100BaseFX uses fiber-optic cable (single-mode, multi-mode, and plastic)
- 1000-Mbps or Gigabit Ethernet
  - Uses twisted-pair (CAT5e or higher) and fiber-optic cable

Token Ring

- Token Ring was developed as a reliable network architecture based on the token-passing access control method
- Token Ring standards are defined in IEEE 802.5
- Physical star; logical ring
- Transmits data at 4 Mbps or 16 Mbps
- Uses centralized device called a MAU (Multi-station Access Unit)
- Less popular than Ethernet

Fiber Distributed Data Interface

- FDDI is a type of Token Ring network. Its implementation and topology differ from the Token Ring LAN architecture, which IEEE 802.5 governs.
- As its name implies, FDDI runs on fiber-optic cable, and thus combines high-speed performance with the advantages of the token-passing ring topology.
- Multiple nodes can have data on the ring at the same time
- Often used for a large LAN in a large company or as a backbone network to connect several LANs in a large building



Wireless LANs (WLANs)

- Make connections using a wireless NIC
- Communicate directly or connect to a LAN by way of a wireless access point (AP)
- Popular where cables are difficult to install
- Slower than wired networks
- Security is an issue
- Standards
  - IEEE 802.11b (11Mbps at 2.4GHz) - 1999
  - IEEE 802.11a (54Mbps at 5GHz) - 2001
  - IEEE 802.11g (54Mbps at 2.4GHz) - 2003
  - IEEE 802.11n (100Mbps at 2.4Ghz) - 2006
  - Bluetooth

Protocols on a Network

- Supports three suites of protocols
  - TCP/IP (Transmission Control Protocol/Internet Protocol)
    - Protocol suite for the Internet
  - IPX/SPX (Internetwork Packet Exchange/Sequenced Packet Exchange)
    - Designed for use with networks
    - Not supported on Internet
  - NetBEUI (NetBIOS Extended User Interface)
    - Proprietary protocol for use on networks isolated from the Internet

Bandwidth Technologies

service		personal and business mobile telephones
Regular telephone (POTS, for Plain Old Telephone Service)	Up to 56 Kbps	Home and small business access to an ISP using a modem
X.25	56 Kbps	Provides communication between mainframes and terminals
ISDN	64 Kbps to 128 Kbps	Small to medium size business access to an ISP
IDSL	128 Kbps	(ISDN Digital Subscriber Line) Home and small business access to an ISP

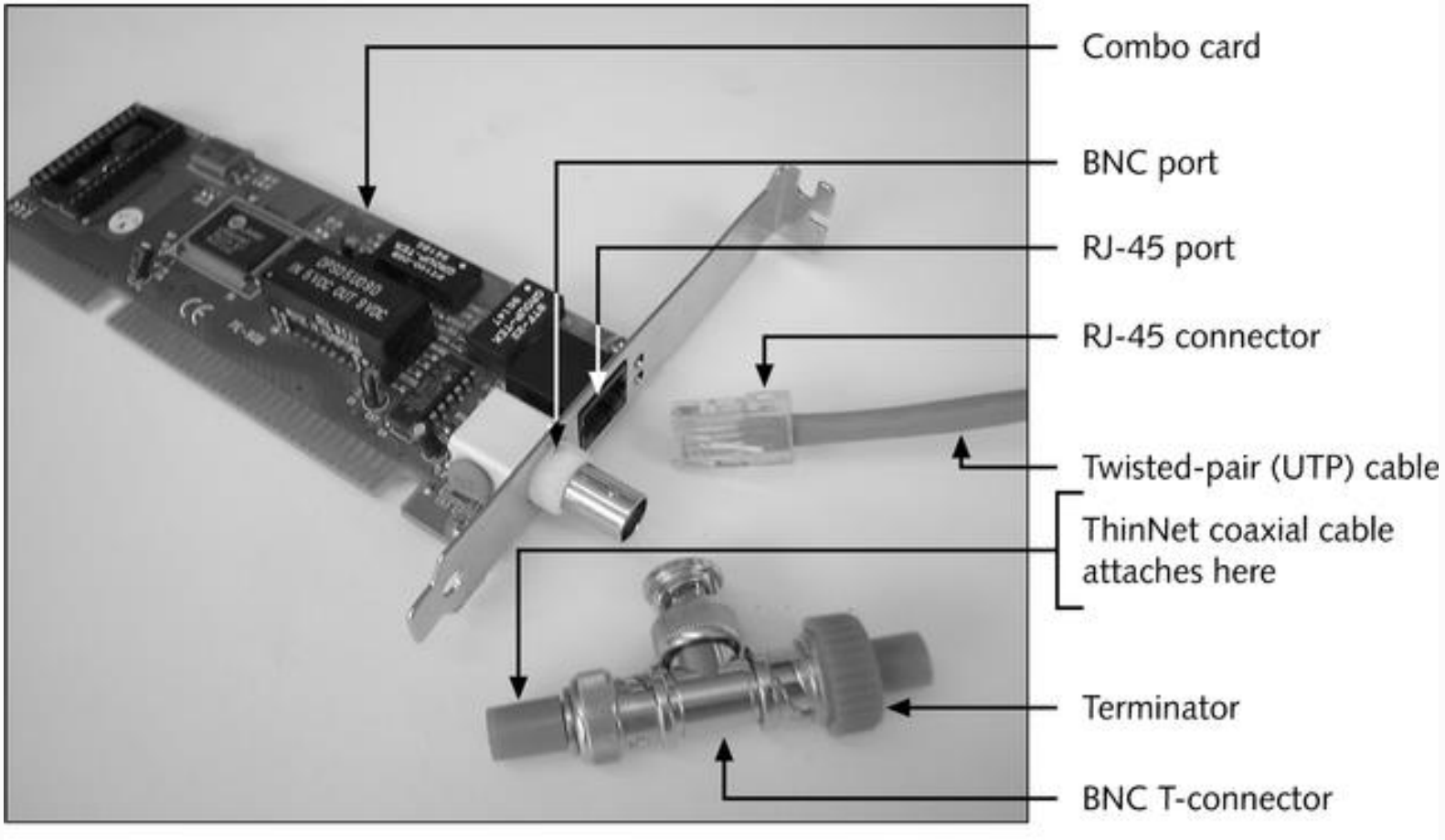
Bandwidth Technologies

Technology	Maximum Throughput Speeds	Common Uses
ADSL (Asymmetric Digital Subscriber Line)	640 Kbps upstream and up to 6.1 Mbps downstream	Most bandwidth is from ISP to user
SDSL (Symmetric DSL)	1.544 Mbps	Equal bandwidths in both directions
HDSL (High-bit-rate DSL)	Up to 3 Mbps	Equal bandwidths in both directions
Cable modem	512 Kbps to 5 Mbps	Home or small business to ISP
VDSL (Very-high-rate DSL)	Up to 55 Mbps over short distances	Future technology of DSL under development
802.11b wireless	5.5 Mbps or 11 Mbps	Most popular wireless
802.11a wireless	Up to 54 Mbps	Not readily available
Frame Relay	56 Kbps to 45 Mbps	Businesses that need to communicate internationally or across the country
Fractional T1	*n* times 64 Kbps (where *n* = number of channels or portions of a T1 leased)	Companies expecting to grow into a T1 line, but not yet ready for a T1
T1	1.544 Mbps	To connect large companies to branch offices or an ISP
Token Ring	4 or 16 Mbps	Used for local network
Ethernet	10 or 100 Mbps 1Gbps up to 40Gbps	Most popular technology for a local network

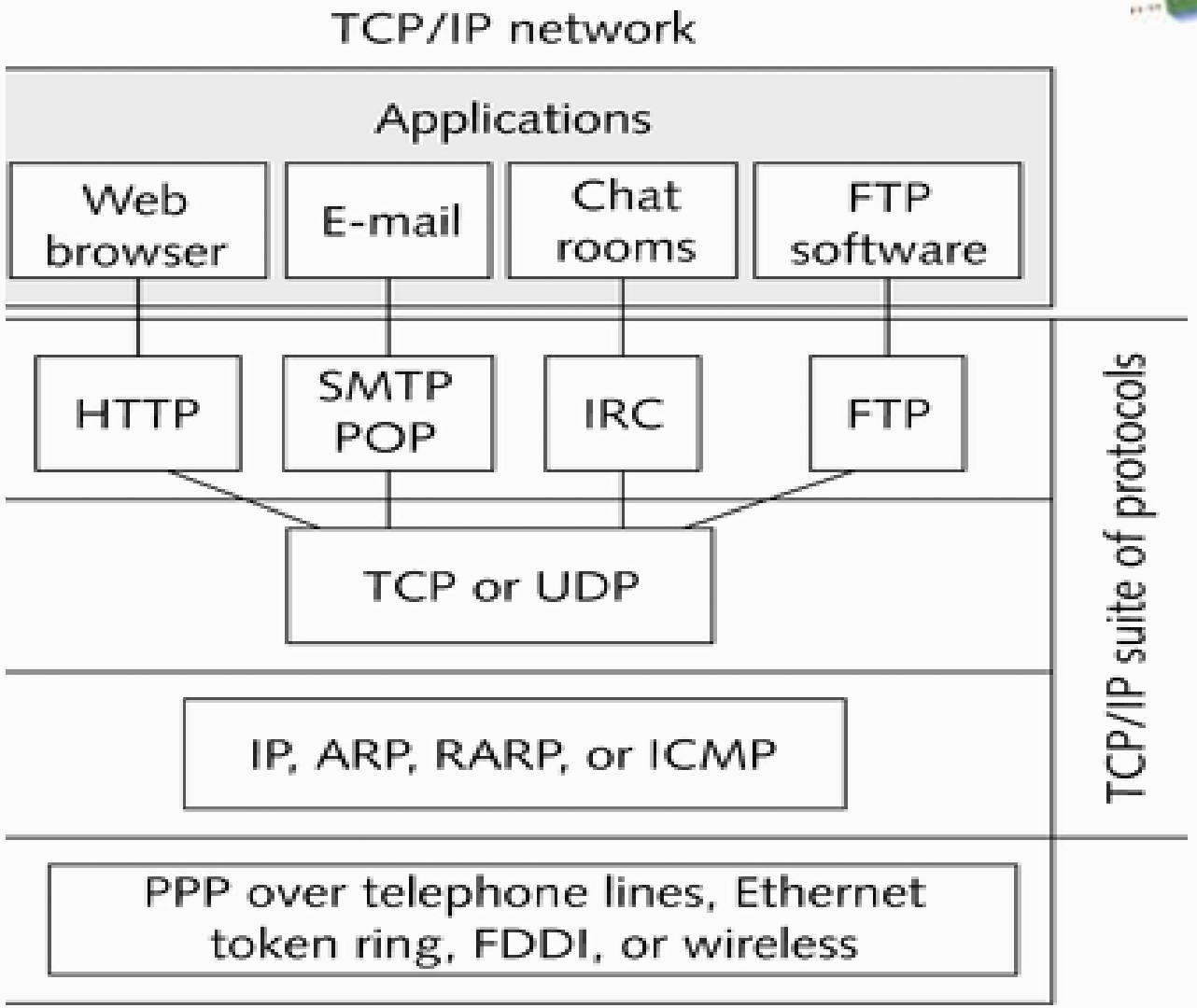
Bandwidth Technologies

Technology	Maximum Throughput Speeds	Common Uses
T3	45 Mbps	Large companies that require a lot of bandwidth and transmit extensive amounts of data
OC-1	52 Mbps	ISP to regional ISP
FDDI	100 Mbps	Supports network backbones from the1980s and early 1990s; also used to connect LANs across multiple buildings
ATM	25, 45, 155, or 622 Mbps	Large business networks and LAN backbones
OC-3	155 Mbps	Internet or large corporation backbone
OC-24	1.23 Gbps	Internet backbone, uses optical fiber
OC-256	13 Gbps	Major Internet backbone, uses optical fiber
SONET (Synchronous Optical Network)	51, 155 , 622, 1244, or 2480 Mbps	Major backbones

Ethernet Combo Card



TCP/IP Protocol Suite



TCP/IP Utilities

- TCP/IP is used to exchange information on the Internet.
- **Ping** is a simple but highly useful command-line utility that is included in most implementations of TCP/IP.
  - Ping works by sending an ICMP echo request to the destination computer. The receiving computer then sends back an ICMP echo reply message.
- **Tracert** is a utility that displays the route a packet takes on its journey from source computer to destination host.

TCP/IP Utilities

- **Address Resolution Protocol** (ARP) is the means by which networked computers map Internet Protocol (IP) addresses to physical hardware (MAC) addresses that are recognized in a local network.
- The ARP cache is the means by which a correlation is maintained between each MAC address and its corresponding IP address.
- The command arp –a is used to display the arp cache.
- The command arp –d deletes the arp cache.

TCP/IP Utilities

- **Reverse Address Resolution Protocol** (RARP), a protocol used to obtain IP address information based on the physical or MAC address.
- RARP provides the rules by which the physical machine in a LAN can request to learn its IP address from a gateway server ARP table or cache.

TCP/IP Utilities

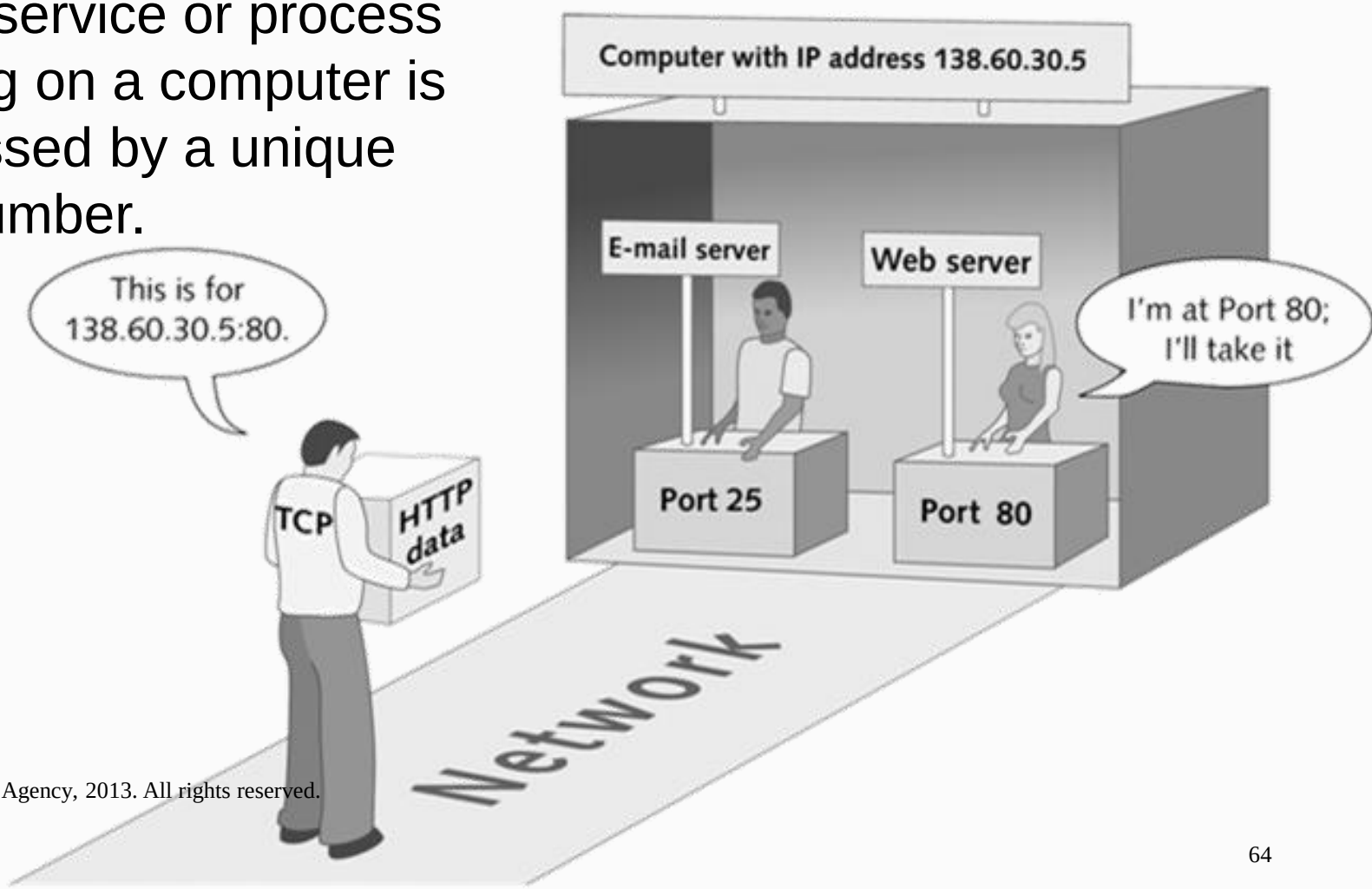
- TCP/IP configuration information can be displayed using different utilities, depending on the operating system:
  - **ipconfig**
  - **inipcfg**
  - **ifconfig**
  - **config**

Utilities and Applications

- **Telnet -** used to access remote devices for configuration, control, and troubleshooting.
- **Nbtstat** – Displays current information about TCP/IP and NetBEUI when both are being used on the same network.
- **Netstat** – Displays information about current TCP/IP connections.
- **Route** – Allow you to manually control network routing tables.

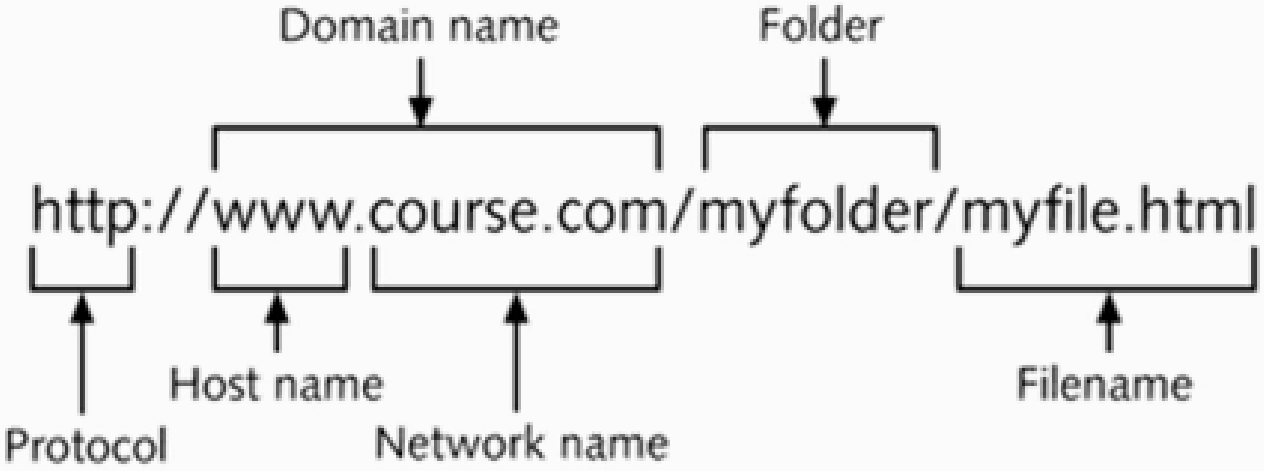
Port Numbers

Every service or process running on a computer is addressed by a unique port number.



How a URL Is Structured

- URL (Uniform Resource Locator)
  - Address for a Web page file or other resource on the Internet



A URL contains the protocol used, the host name of the web sever, the network name, and the path and filename of the requested file.

Top-Level Domain Names

.coop	Business cooperatives
.edu	Educational institutions
.gov	Government institutions
.info	General use
.int	Organizations established by international treaties between governments
.mil	U.S. military
.museum	Museums
.name	Individuals
.net	Internet providers or networks