Experiment-1

CSE 3034	Computer Networking	4	1

Computer Networks : Physical Layer, Data Link, The Medium Access Control Sublayer, Network Layer, The Transport, Application Layer, Network Security, Introduction to Networks Labs : Networking Today, Basic Switch and End Device Configuration, Protocols and Models, Physical Layer, Number Systems, Data Link Layer, Ethernet Switching, Network Layer, Address Resolution, Basic Router Configuration, IPv4 Addressing, IPv6 Addressing, ICMP, Transport Layer, Application Layer, Network Security Fundamentals, Build a Small Network

Textbooks

- Computer Networks by Tannenbaum, Pearson India
- Introduction to Networks Labs and Study Guide by Allan Johnson, Cisco

Course Format : 3 Classes/Week, 1 hr/Class; 1 Lab/Week, 2 hrs/Lab = 4 Credits

Aim: Study of network components, network representations and topologies, types of networks, and network IP address.

Objectives:

To learn basics of:

1. Network Components

Host Roles

Peer-to-Peer

End Devices

Intermediary Devices

Network Media

2. Network Representations and Topologies

Network Representations

Topology Diagrams

3. Common Types of Networks

LANs and WANs

The Internet

Intranets and Extranets

4. Network IP Address

IPv4 addressing

Introduction

- Networks are all around us. They provide us with a way to communicate and share information and resources with individuals in the same location or around the world.
- Networks require an extensive array of technologies and procedures that can readily adapt to varying conditions and requirements.
- Advancements in networking technologies are perhaps the most significant changes in the world today.
- They are helping to create a world in which national borders, geographic distances, and physical limitations become less relevant and present ever- diminishing obstacles.

- The internet has changed the manner in which our social, commercial, political, and personal interactions occur.
- The immediate nature of communications over the internet encourages the creation of global communities.
- The creation of online communities for the exchange of ideas and information has the potential to increase productivity opportunities around the globe.

Network Components

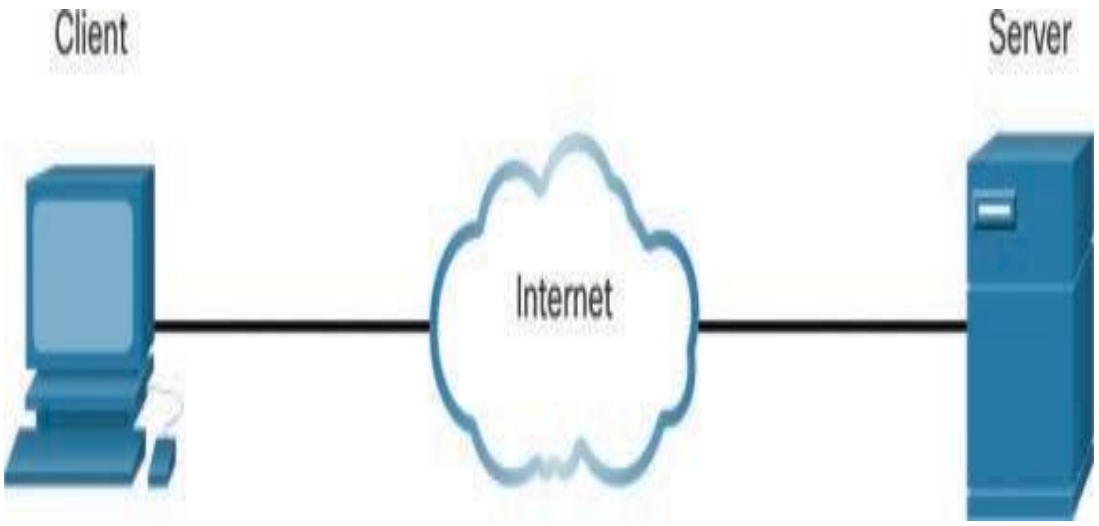
- Many different components are required to enable a network to provide services and resources.
- These various components work together to ensure that resources are delivered in an efficient manner to those requiring the services.

Host Roles

- If you want to be part of a global online community, your computer, tablet, or smart- phone must first be connected to a network. That network must be connected to the internet.
- Any computer that is connected to a network and that participates directly in network communication is classified as a host.
- Hosts can be called end devices. Some hosts are also called clients.
- However, the term *host* specifically refers to a device on a network that is assigned a number for communication purposes.

- This number, which identifies the host within the particular network, is called the Internet Protocol (IP) address. An IP address identifies the host and the network to which the host is attached.
- ***Servers*** are computers with software that allows them to provide information, such as email or web pages, to other end devices on the network.
- Each service requires separate server software. For example, a server requires web server software in order to provide web services to the network.
- A computer with server software can simultaneously provide services to many different clients.
- A client is a type of host. ***Clients*** have software for requesting and displaying the information obtained from the server.

- **Figure 1-1** A Client and a Server



- An example of client software is a web browser, such as Chrome or Firefox. A single computer can also run multiple types of client software.

Table 1-1 Common Server Software

Software Type	Description
Email	An email server runs email server software. Clients use mail client software, such as Microsoft Outlook, to access email on the server.
Web	A web server runs web server software. Clients use browser software, such as Windows Internet Explorer, to access web pages on the server.
File	A file server stores corporate and user files in a central location. The client devices access these files with client software such as Windows File Explorer.

Peer-to-Peer

- Client and server software usually run on separate computers, but it is also possible for one computer to be used for both roles at the same time.
- In small businesses and homes, many computers function as both servers and clients on the network. This type of network, called a peer-to-peer network.

- **Figure 1-2 Peer-to-Peer Network**

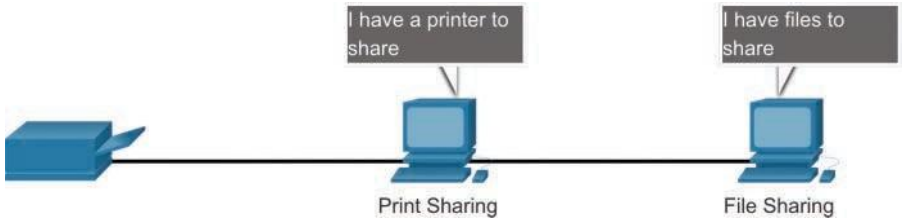
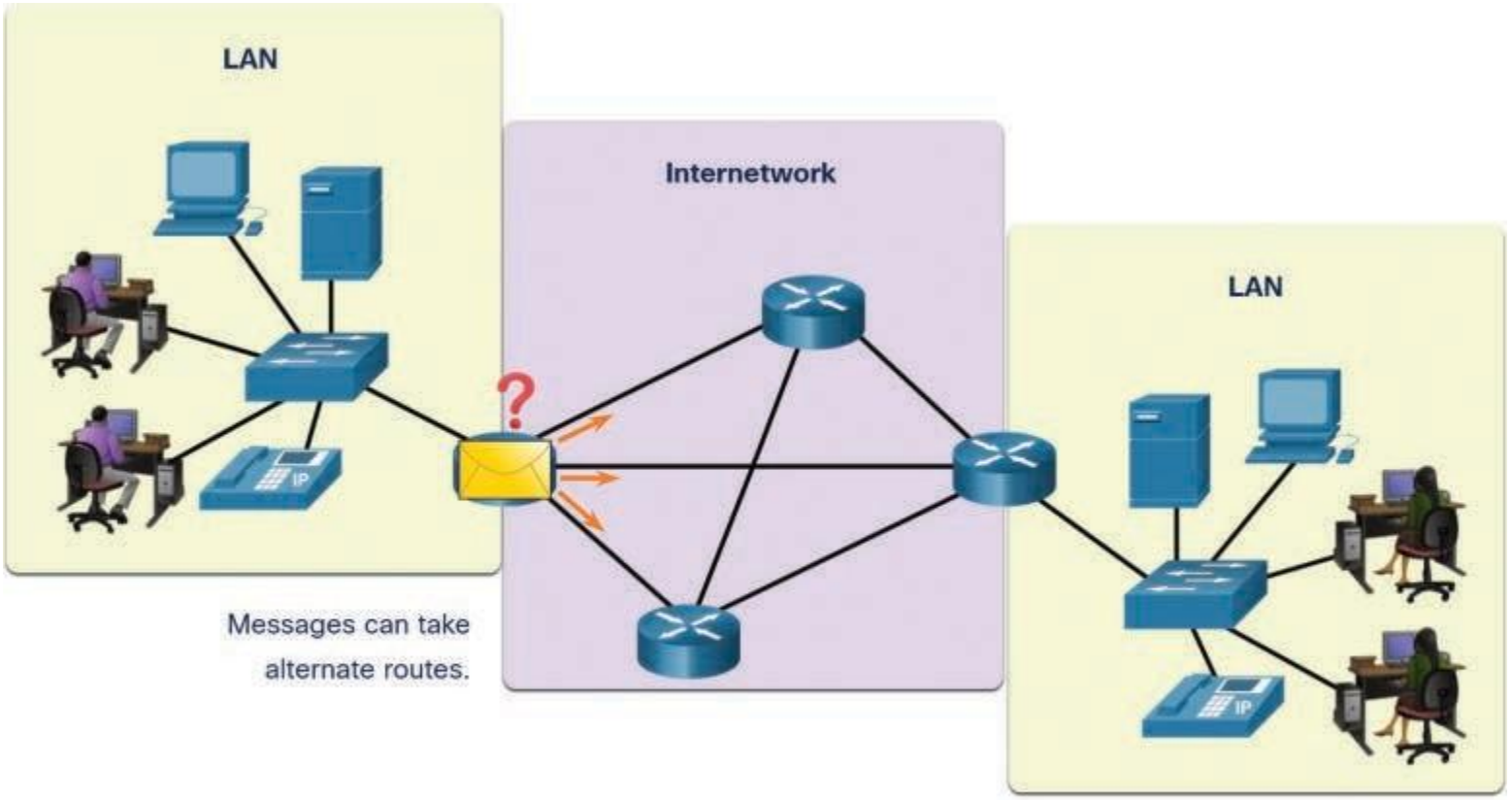


Table 1-2 Peer-to-Peer Networking Advantages and Disadvantages

Advantages	Disadvantages
Easy to set up	No centralized administration
Less complex	Not as secure
Lower cost because network devices and dedicated servers may not be required	Not scalable
Can be used for simple tasks such as transferring files and sharing printers	All devices may act as both clients and servers, which can slow their performance

End Devices

- The network devices that people are most familiar with are end devices. To distinguish one end device from another, each end device on a network has an address.
- When an ***end device*** initiates communication, it uses the address of the destination end device to specify where to deliver the message.
- An end device is either the source or destination of a message transmitted over the network.

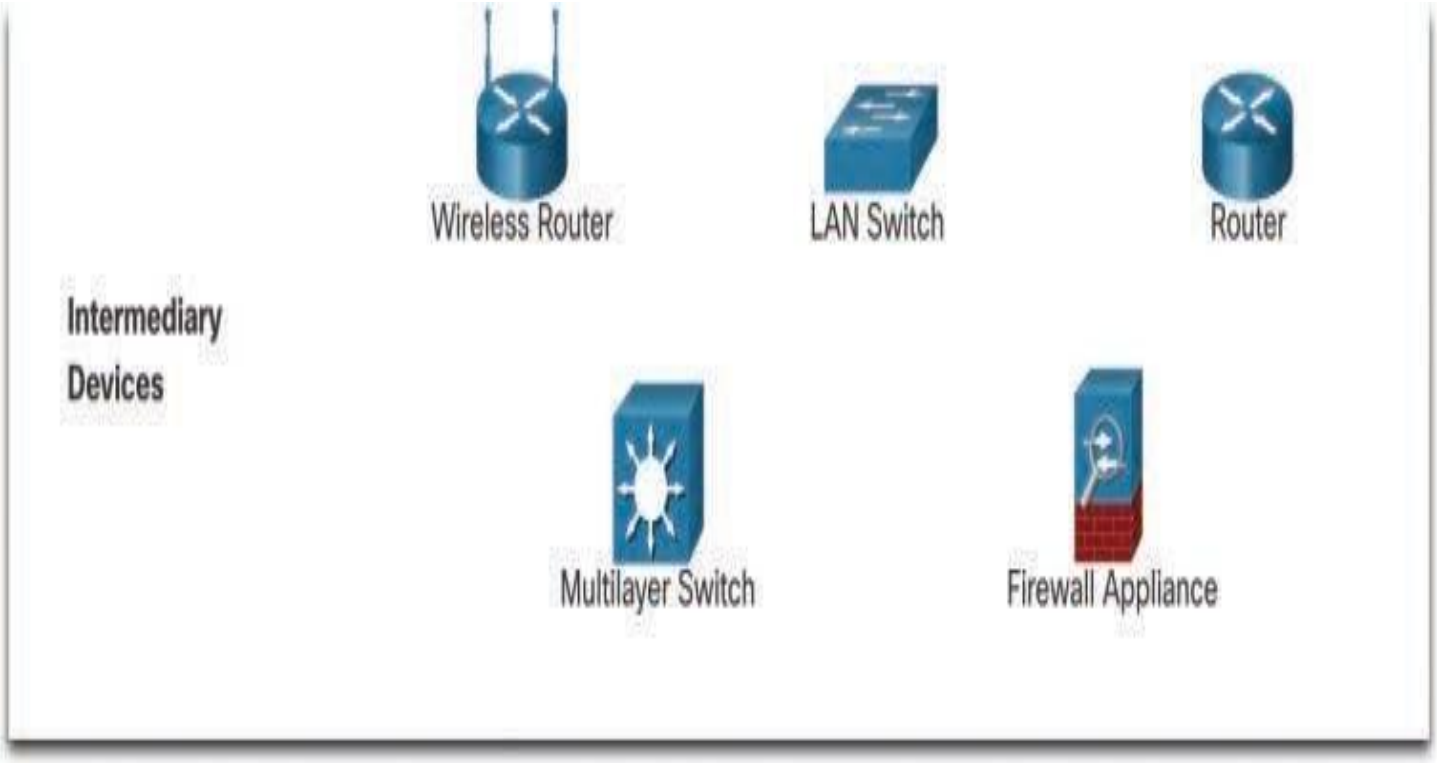


Data originates with an end device, flows through the network, and arrives at an end device.

Intermediary Devices

- *Intermediary devices* connect individual end devices to a network. They can connect multiple individual networks to form an internetwork.
- These intermediary devices provide connectivity and ensure that data flows across the network.
- Intermediary devices use the destination end device address, in conjunction with information about the network interconnections, to determine the path that messages should take through the network.

- **Figure 1-4** Common Intermediary Devices



- Intermediary network devices perform some or all of these functions:

- Regenerate and retransmit communication signals
- Maintain information about what pathways exist through the network and internetwork
- Notify other devices about errors and communication failures
- Direct data along alternate pathways when there is a link failure
- Classify and direct messages according to priorities
- Permit or deny the flow of data, based on security settings

- **Repeater:** A device that regenerates weak signals to extend the distance a signal can travel.
- It receives a signal and retransmits it at a higher level and/or higher power, or on to the other side of an obstruction, so that the signal can cover longer distances.
- **Hub:** A device that extends the reach of a network by regenerating the electrical signal.
- It also receives data on one port and then sends it out to all other active ports.
- It is used for connecting multiple twisted pair or fiber optic Ethernet devices together and making them act as a single network segment.
- The device is a form of multi port repeater.

- **Switch:** A network switch or switching hub is a computer networking device that connects network segments.
- It connects multiple devices on a network by receiving data and using filtering and forwarding to send the data to the intended destination device.
- **Router:** A network layer device that forwards data packets between networks. Routers use IP addresses to forward traffic to other networks.
- It interconnects two or more computer networks, and selectively interchanges packets of data between them.
- Each data packet contains address information that a router can use to determine if the source and destination are on the same network, or if the data packet must be transferred from one network to another.
- Where multiple routers are used in a large collection of interconnected networks, the routers exchange information about target system addresses, so that each router can build up a table showing the preferred paths between any two systems on the interconnected networks.

- **Gate Way:** Normally, a relatively general term that refers to different kinds of networking devices. Historically, when routers were created, they were called gateways.
- A gateway is a hardware device that acts as a "gate" between two networks.
- A gate way may contain devices such as protocol translators, impedance matching devices, rate converters, fault isolators, or signal translators as necessary to provide system interoperability.

Network Media

- Communication transmits across a network on media. The media provide the channel over which a message travels from source to destination.
- Modern networks primarily use three types of media to interconnect devices:

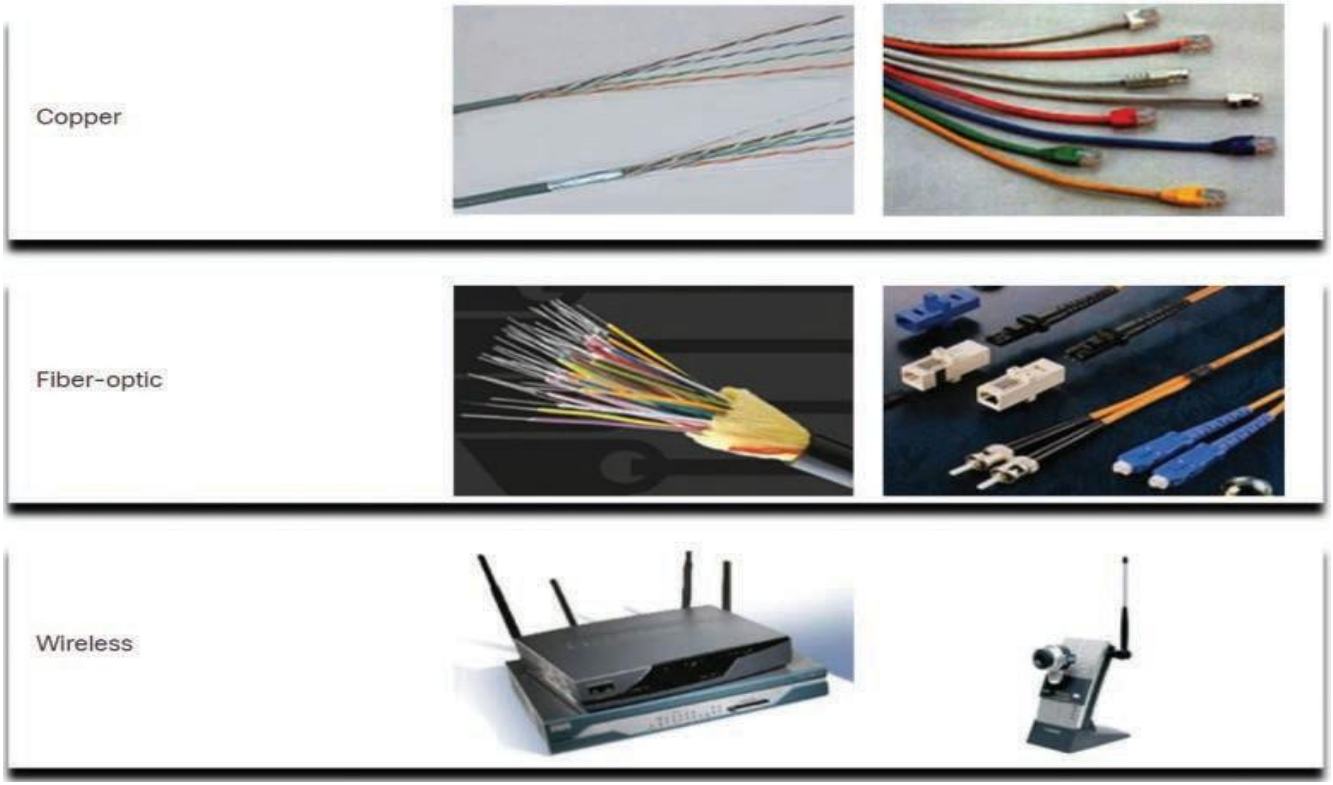
➢ **Metal wires within cables:** Data is encoded into electrical impulses.

➢ **Glass or plastic fibers within cables (fiber-optic cable):** Data is encoded into pulses of light.

➢ **Wireless transmission:** Data is encoded via modulation of specific frequencies of electromagnetic waves.

- Different types of network media have different features and benefits. Not all net- work media have the same characteristics, and they are not all appropriate for the same purpose.

- Figure 1-5 Network Media



- ***Unshielded twisted-pair (UTP)*** cabling is the most common networking medium.
- UTP cabling is used for interconnecting network hosts with intermediary networking devices, such as switches and routers.
- Different situations may require UTP cables to be wired according to different wiring conventions.

■■ Straight-through UTP: This is the most common type of networking cable, commonly used to interconnect a host to a switch and a switch to a router.

■■ Crossover UTP: This cable is used to interconnect similar devices—for example, to connect a switch to a switch, a host to a host, or a router to a router.

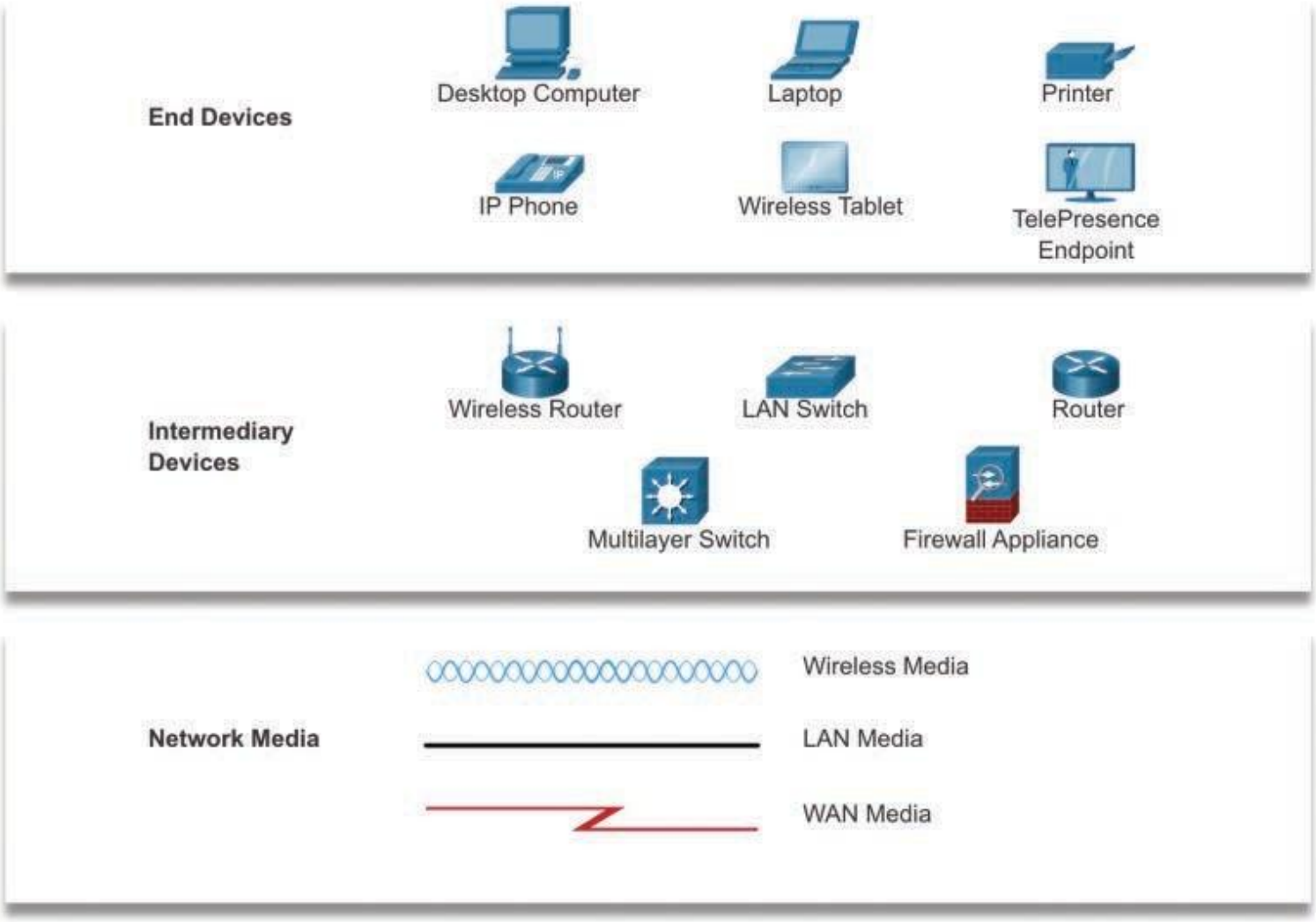
2. Network Representations and Topologies

- A network's infrastructure is documented using commonly used symbols to represent devices and different types of diagrams to represent the interconnection of these devices in the network.
- Understanding these symbols and diagrams is an important aspect of understanding network communications.

Network Representations

- Network architects and administrators must be able to show what their networks look like.
- They need to be able to easily see which components connect to other components, where they are located, and how they are connected.
- Diagrams of networks often use symbols, to represent the different devices and connections in a network.
- A diagram provides an easy way to understand how devices connect in a network. This type of "picture" of a network is known as a *topology diagram*.
- The ability to recognize the logical representations of the physical networking components is critical to being able to visualize the organization and operation of a network.

Figure 1-6 Network Symbols for Topology Diagrams



- In addition to these representations, specialized terminology is used to describe how each of these devices and media connect to each other:
- **Network interface card (NIC):** A NIC physically connects an end device to a network.
- **Physical port:** A port is a connector or an outlet on a networking device where a medium connects to an end device or another networking device.
- **Interface:** An interface is a specialized port on a networking device that connects to a network. Because routers connect networks, the ports on a router are referred to as *network interfaces*.

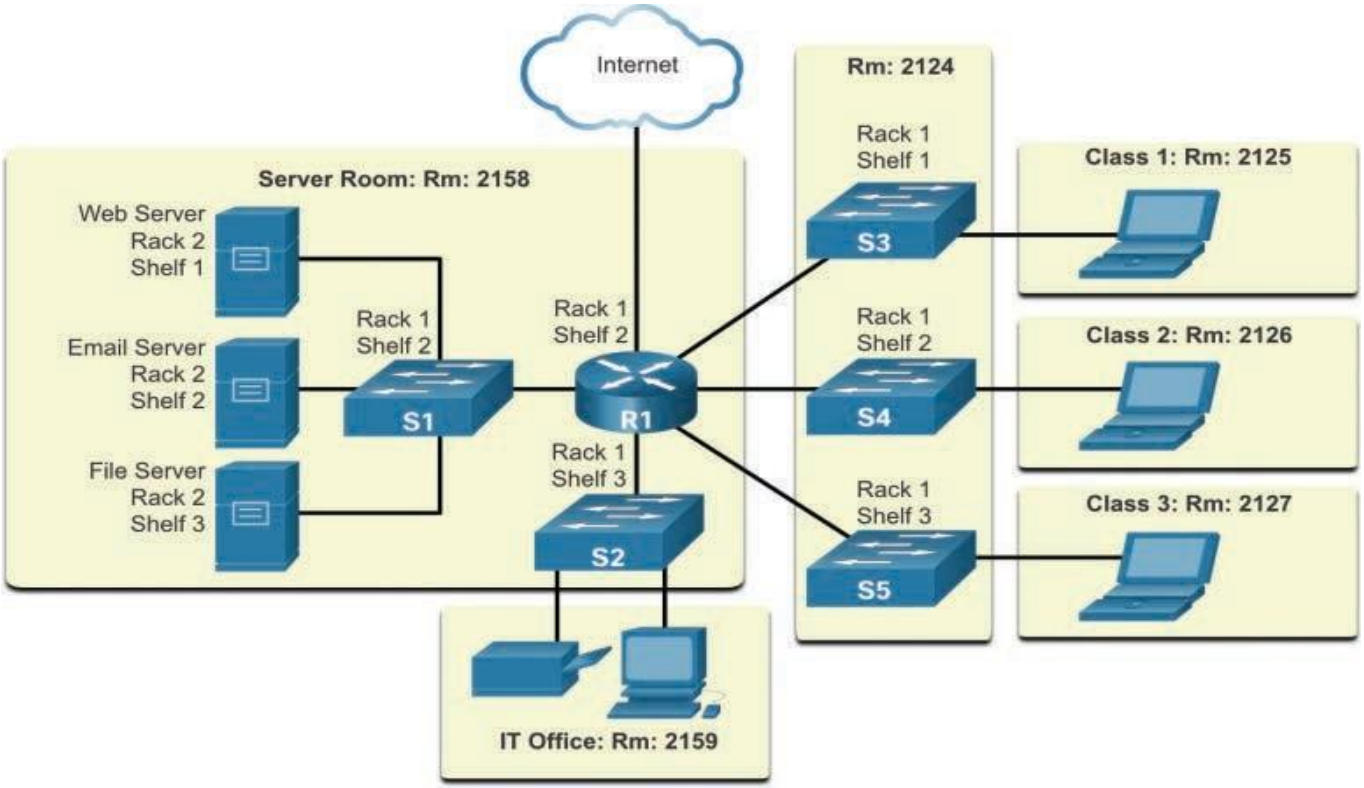
Topology Diagrams

- ***Topology*** diagrams are mandatory documentation for anyone working with a network. Such a diagram provides a visual map of how the network is connected.
- There are two types of topology diagrams: physical and logical.

Physical Topology Diagrams

- A physical topology diagram illustrates the physical locations of intermediary devices and cable installation.

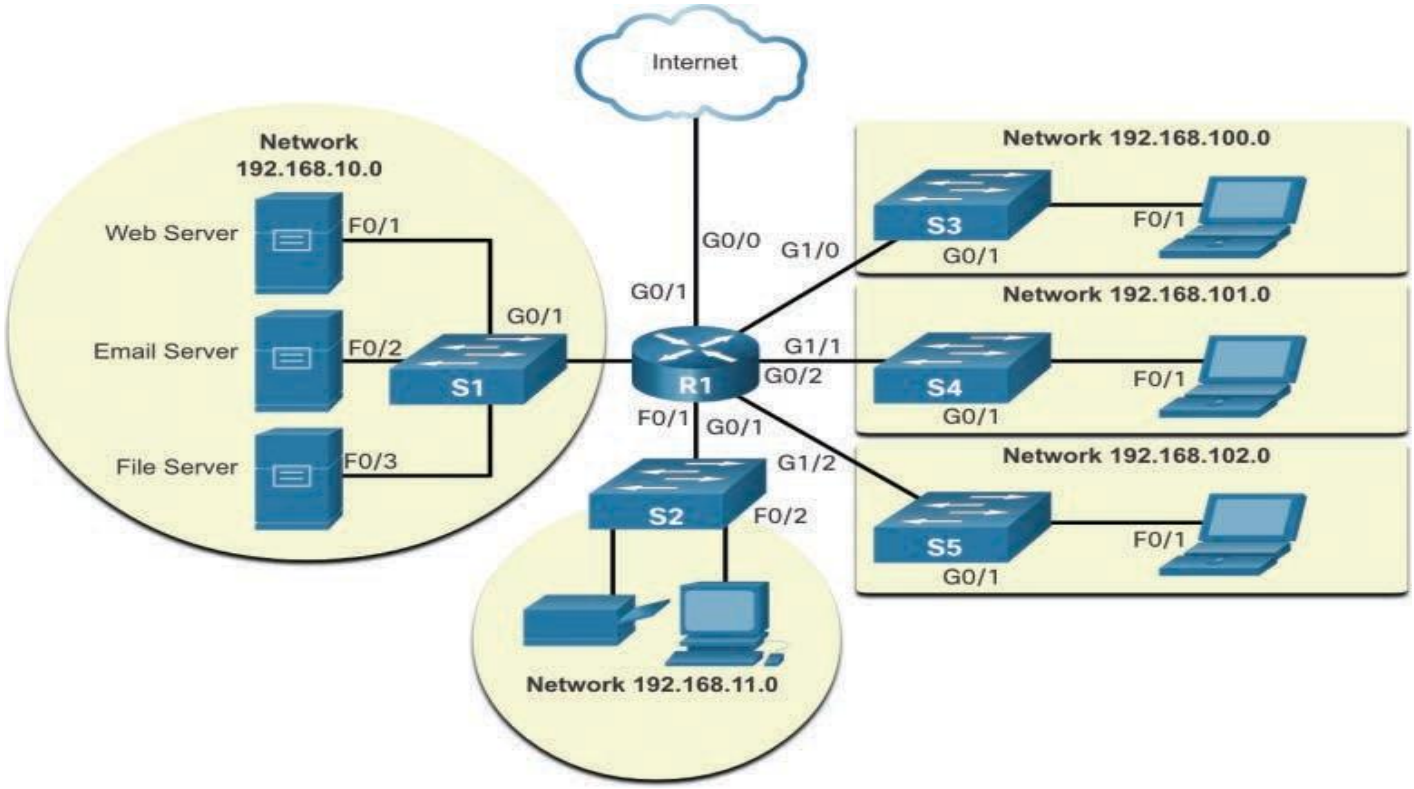
Figure 1-7 Physical Topology Example



Logical Topology Diagrams

- A logical topology diagram illustrates devices, ports, and the addressing scheme of a network.

Figure 1-8 Logical Topology Example



Common Types of Networks

- Networks can be categorized in various ways, including by size, by location, or by function.
- Networks come in all sizes. They range from simple networks consisting of two computers to networks connecting millions of devices.
- The internet is the largest network in existence. In fact, the term *internet* means a “network of networks.” The internet is a collection of interconnected private and public networks.
- In small businesses and homes, many computers function as both servers and clients on the network. This type of network is called a peer-to-peer network.

There are networks of varying sizes that can be categorized in various ways, including the following:

- **Small home networks:** Small home networks connect a few computers to each other and to the internet.
- ***Small office and home office (SOHO) networks*:** A SOHO network allows computers in a home office or a remote office to connect to a corporate network or access centralized, shared resources.
- **Medium to large networks:** Medium to large networks, such as those used by corporations and schools, can have many locations with hundreds or thousands of interconnected hosts.
- **Worldwide networks:** The internet is a network of networks that connects hundreds of millions of computers worldwide.

LANs and WANs

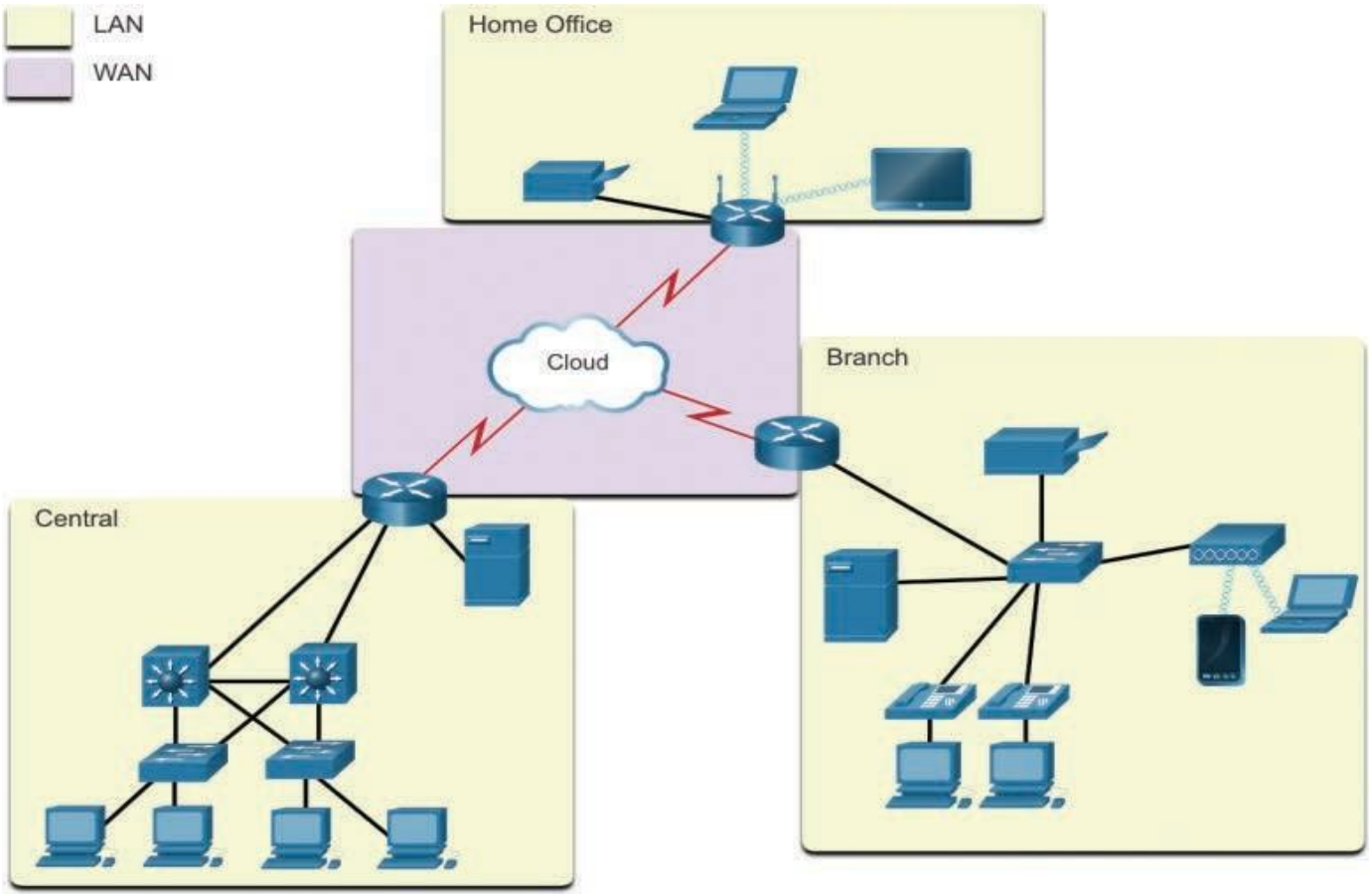
- Network infrastructures vary greatly in terms of:

- Size of the area covered
- Number of users connected
- Number and types of services available
- Area of responsibility

- The two most common types of network infrastructures are *local-area networks* ***(LANs)*** and *wide-area networks* ***(WANs)***.

- A **LAN** is a network infrastructure that provides access to users and end devices in a small geographic area. A LAN is typically used in a department within an enterprise, a home, or a small business network.
- A **WAN** is a network infrastructure that provides access to other networks over a wide geographic area, which is typically owned and managed by a larger corporation or a telecommunications service provider.

Figure 1-9 LANs connected to a WAN.



LANs

- A LAN is a network infrastructure that spans a small geographic area. LANs have specific characteristics:

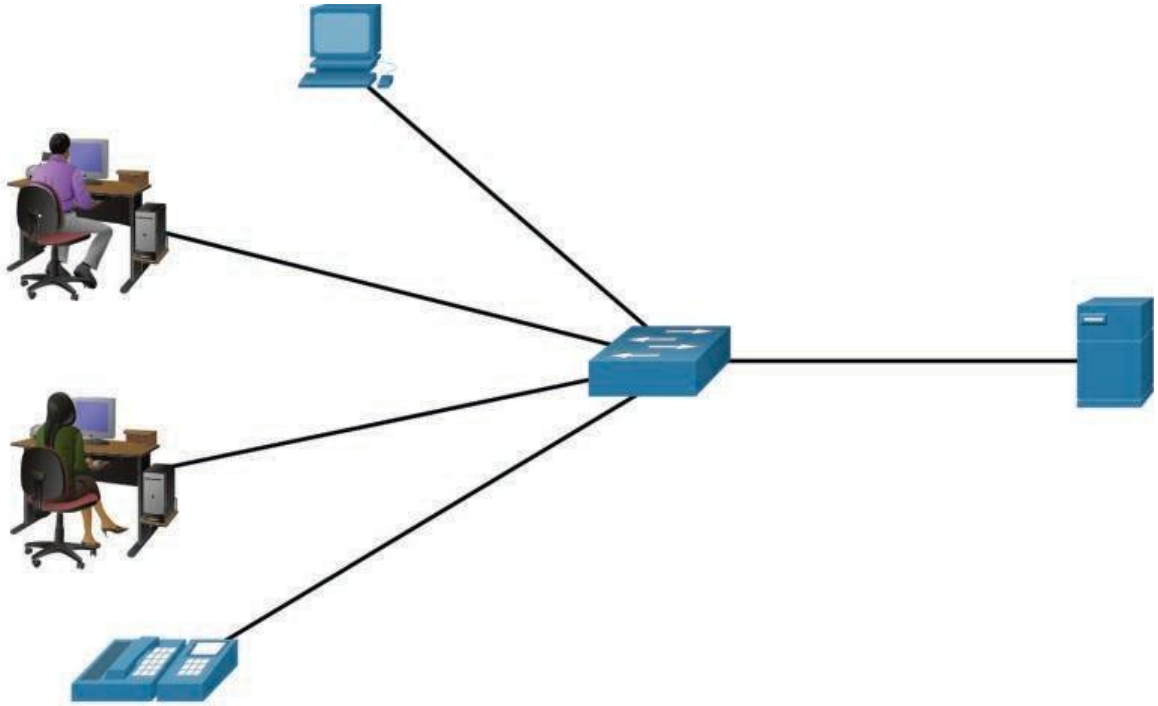
➢ LANs interconnect end devices in a limited area such as a home, school, office building, or campus.

➢ A LAN is usually administered by a single organization or individual.

➢ Administrative control is enforced at the network level and governs the security and access control policies.

➢ LANs provide high-speed bandwidth to internal end devices and intermediary devices.

Figure 1-10 Example of a LAN



A network serving a home, small building, or a small campus is considered a LAN.

WANs

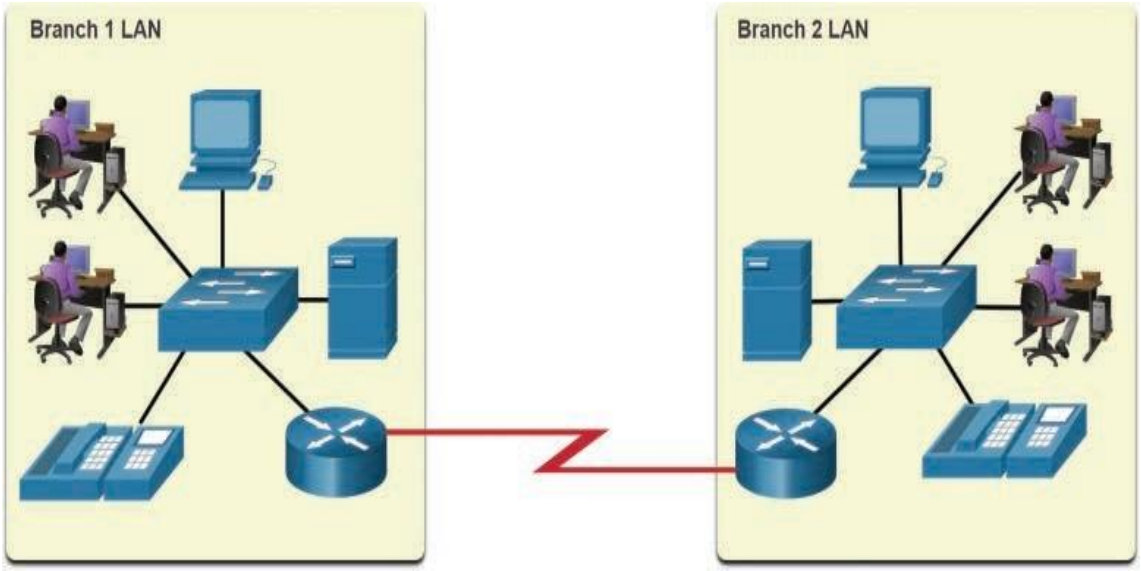
- A WAN is a network infrastructure that spans a wide geographic area. WANs are typically managed by service providers (SPs) or internet service providers (ISPs).
- WANs have specific characteristics:

➢ WANs interconnect LANs over wide geographic areas such as between cities, states, provinces, countries, or continents.

➢ WANs are usually administered by multiple service providers.

➢ WANs typically provide slower-speed links between LANs.

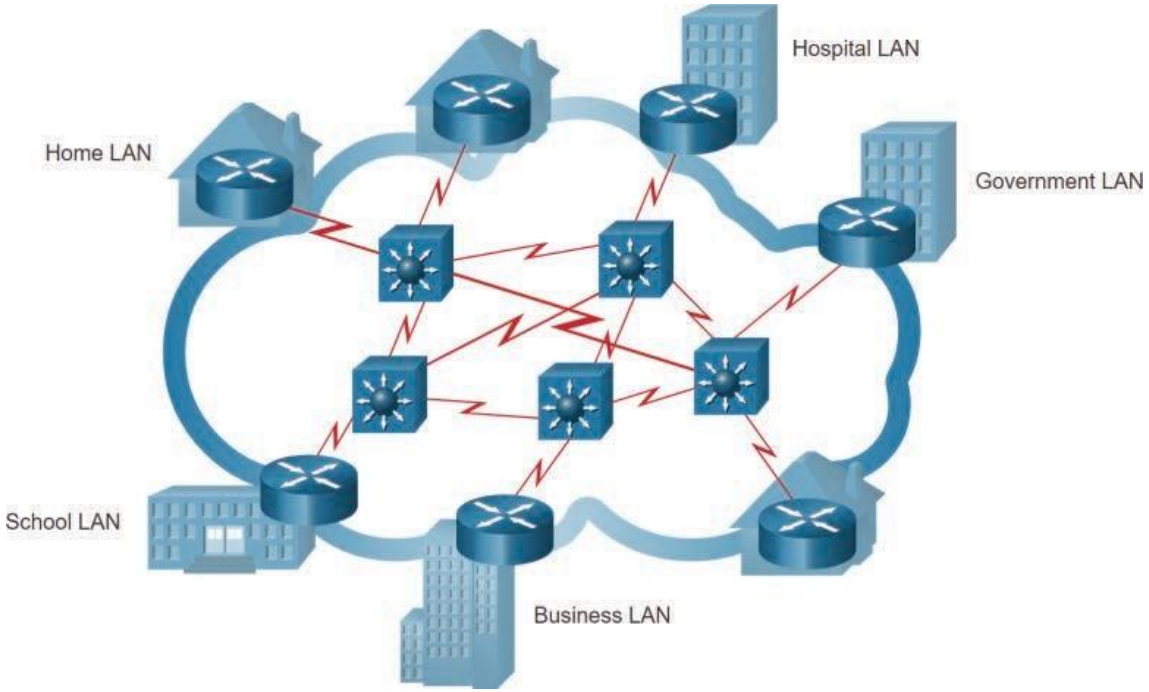
- Figure 1-11 Example of a WAN Link



The Internet

- The ***internet*** is a worldwide collection of interconnected networks (*internetworks*, or *internet* for short). Internet is a collection of interconnected LANs and WANs.

Figure 1-12 Example of a View of the Internet



- Some of the LAN examples in Figure 1-12 are connected to each other through a WAN connection. WANs are then connected to each other.
- The WAN connection lines (which look like lightning bolts) represent the varieties of ways we connect networks. WANs can connect through copper wires, fiber-optic cables, and wireless transmissions.
- The internet is not owned by any individual or group.
- Ensuring effective communication across this diverse infrastructure requires the application of consistent and commonly recognized technologies and standards as well as the cooperation of many network administration agencies.

Intranets and Extranets

- Two other terms are similar to the term internet: intranet and extranet.
- The term ***intranet*** is often used to refer to a private connection of LANs and WANs that belongs to an organization.
- An intranet is designed to be accessible only by the organization's members, employees, or others with authorization.
- An organization may use an ***extranet*** to provide secure and safe access to individuals who work for a different organization but require access to the organization's data.

- Some examples of extranets:

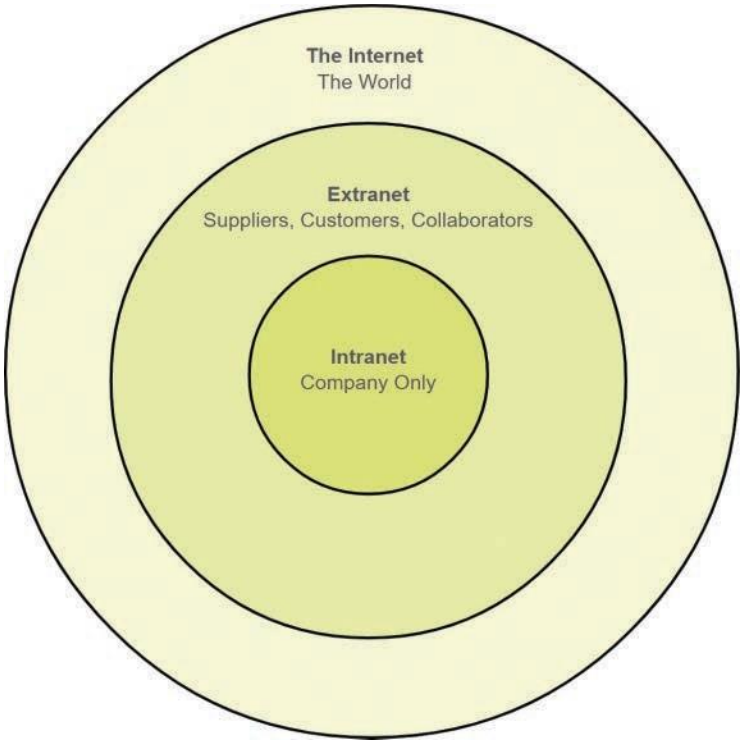
➢ A company that is providing access to outside suppliers and contractors

➢ A hospital that is providing a booking system to doctors so they can make appointments for their patients

➢ A local education office that is providing budget and personnel information to the schools in its district

- Figure 1-13 illustrates the levels of access that different groups have to a company intranet, a company extranet, and the internet.

Figure 1-13 Levels of Access from Intranet to Internet



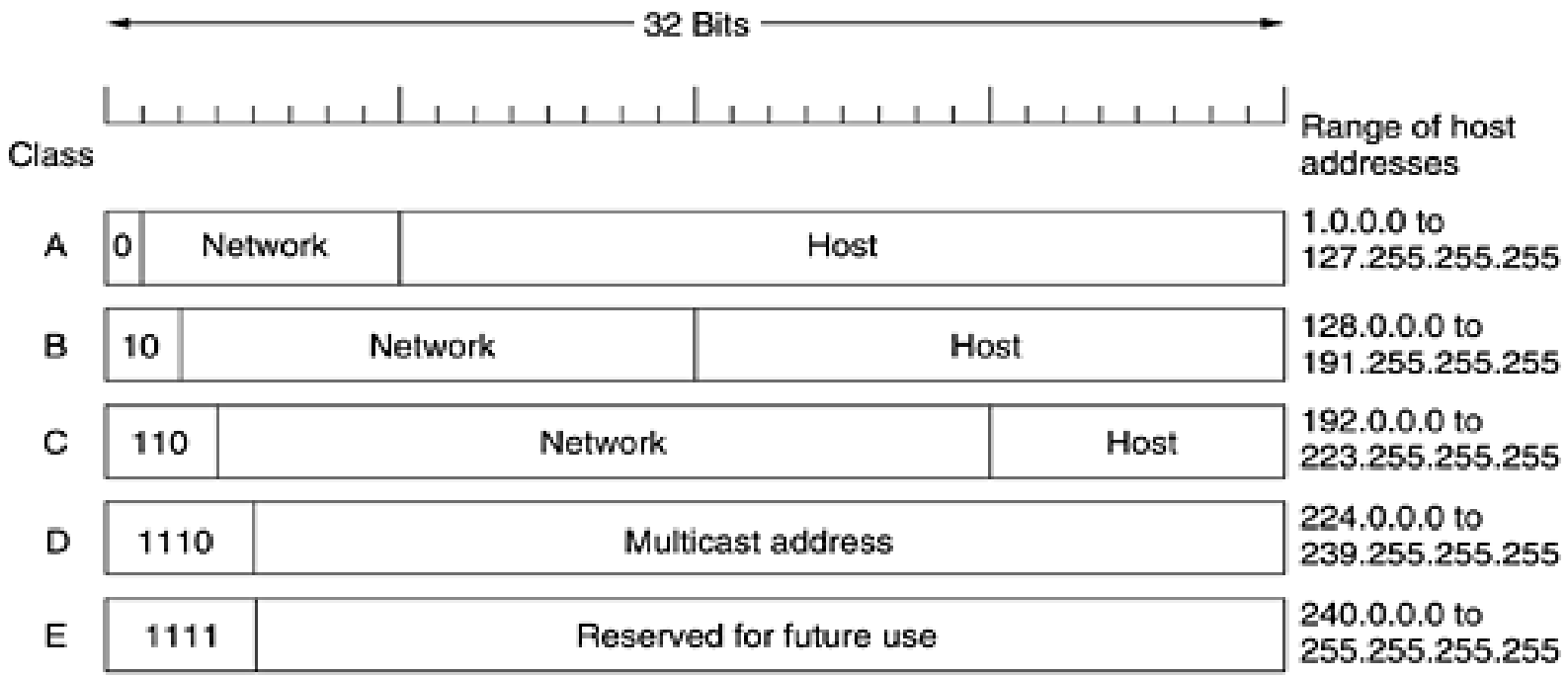
Network IP Address

- Every host and router on the Internet has an IP address, which encodes its network number and host number.
- The combination is unique: in principle, no two machines on the Internet have the same IP address.
- In the TCP/IP protocol, the unique identifier for a computer is called its IP address.
- There are two standards for IP addresses: **IP Version 4 (IPv4)** and **IP Version 6 (IPv6).**

IPv4 addressing

- Format of IP address IPv4 is made up of four parts, in the pattern as w.x.y.z.
- Each part has 8 binary bits and the values in decimal can range from 0 to 255.
- IP addresses are divided into different classes. These classes determine the maximum number of hosts per network ID.

- **IP address formats**



Class	Address Range	Supports
Class A	1.0.0.1 to 126.255.255.254	Supports 16 million hosts on each of 127 networks.
Class B	128.1.0.1 to 191.255.255.254	Supports 65,000 hosts on each of 16,000 networks.
Class C	192.0.1.1 to 223.255.254.254	Supports 254 hosts on each of 2 million networks.
Class D	224.0.0.0 to 239.255.255.255	Reserved for multicast groups.
Class E	240.0.0.0 to 254.255.255.254	Reserved.

- For networks of different size, The first one (for large networks) to three (for small networks) octets can be used to identify the **network**, while the rest of the octets can be used to identify the **node** on the network.
- The class A formats allow for up to 128 networks with 16 million hosts each,
- The class B formats allow 16,384 networks with up to 64K hosts, and
- The class C formats allow 2 million networks (e.g., LANs) with up to 256 hosts each (although a few of these are special).

Reference:

- Introduction to Networks Labs and Study Guide by Allan Johnson, Cisco
- Computer Networks by Andrew S. Tannenbaum, Pearson India