20MCA104
ADVANCED COMPUTER NETWORKS

Module 1- Part1

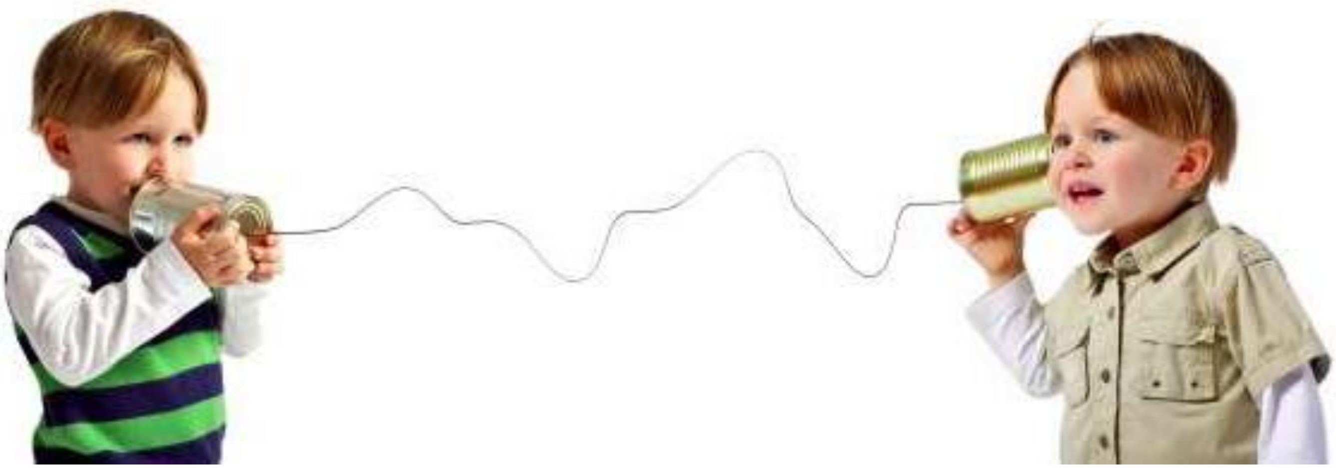
Jane George
Asst. Professor
Dept. of MCA
RIT Kottayam

Module 1- Part1

OVERVIEW OF COMPUTER NETWORKS AND THE INTERNET

Network

- A group or system of interconnected people or things.



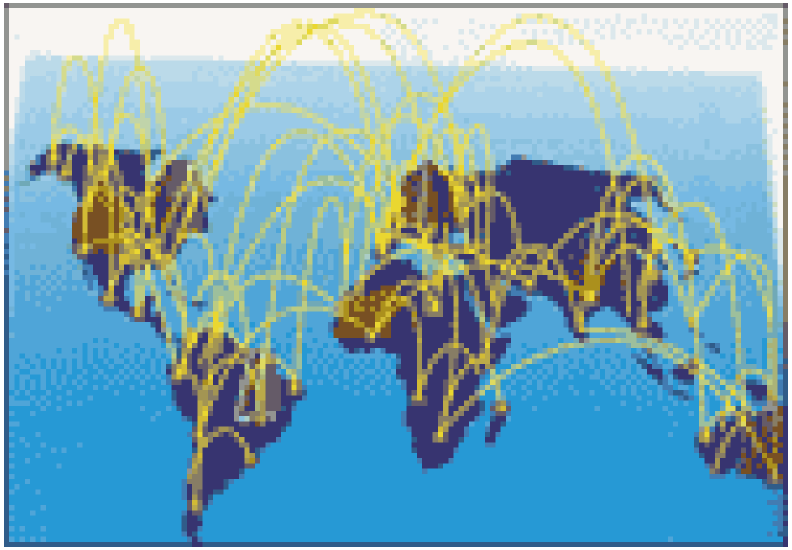
Computer Network

- A group of computers linked to each other.
- Enables communication with another computer.
- Share resources, data, and applications.

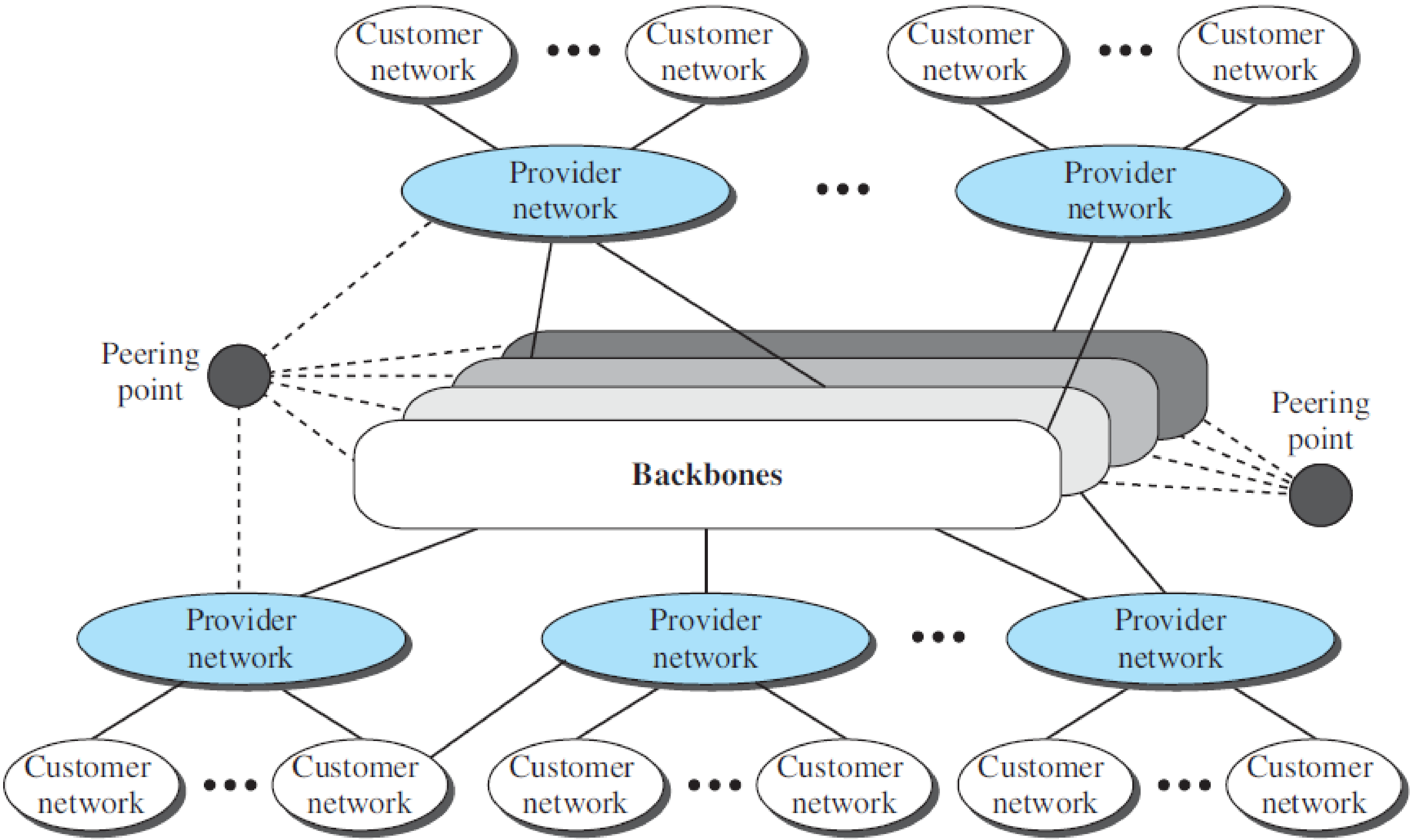

20 35

Internet

- A network of networks.
- Connects millions of people all over the world.
- Collection of computers, servers, mainframes, network devices, peripherals, or other devices.



Internet today



- The **Backbones** are large networks owned by some communication companies such as Sprint, Verizon (MCI), AT&T, and NTT.
  - The backbone networks are connected through some complex switching systems, called **peering points**.
- The **Provider networks** use the services of the backbones for a fee.
  - The provider networks are connected to backbones and sometimes to other provider networks.
- The **Customer networks** are networks at the edge of the Internet that actually use the services provided by the Internet.
  - They pay fees to provider networks for receiving services.

- Backbones and provider networks are also called **Internet Service Providers** (ISPs).
- The **backbones** are often referred to as **International ISPs**.
- The **provider networks** are often referred to as **national or regional ISPs**.

Examples of network devices

- Desktop computers, laptops, mainframes, and servers.
- Consoles and thin clients.
- Firewalls
- Bridges
- Repeaters
- Network Interface cards
- Switches, hubs, modems, and routers.
- Smart phones and tablets.
- Webcams

https://youtu.be/vvrdgwDnMQA

Hub

Gateway

Router

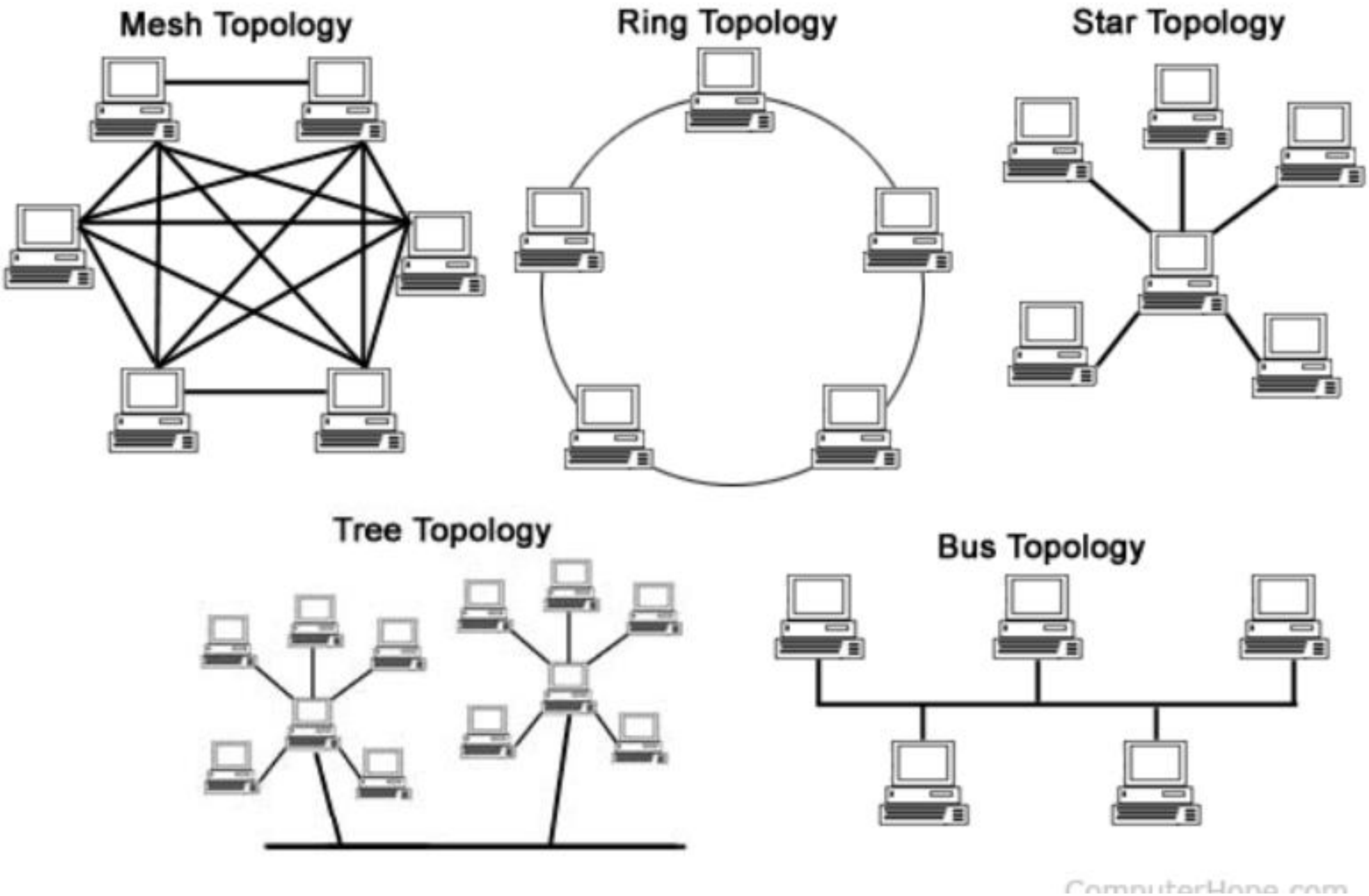
Repeater

Bridge

Switch

Network Topology

- Physical configuration of a network.
- Determines how the network's computers are connected.
- Typical network configurations include
  - Bus topology,
  - Mesh topology,
  - Ring topology,
  - Star topology,
  - Tree topology and
  - Hybrid topology.


Mesh Topology
Ring Topology
Star Topology
Tree Topology
Bus Topology
ComputerHope.com

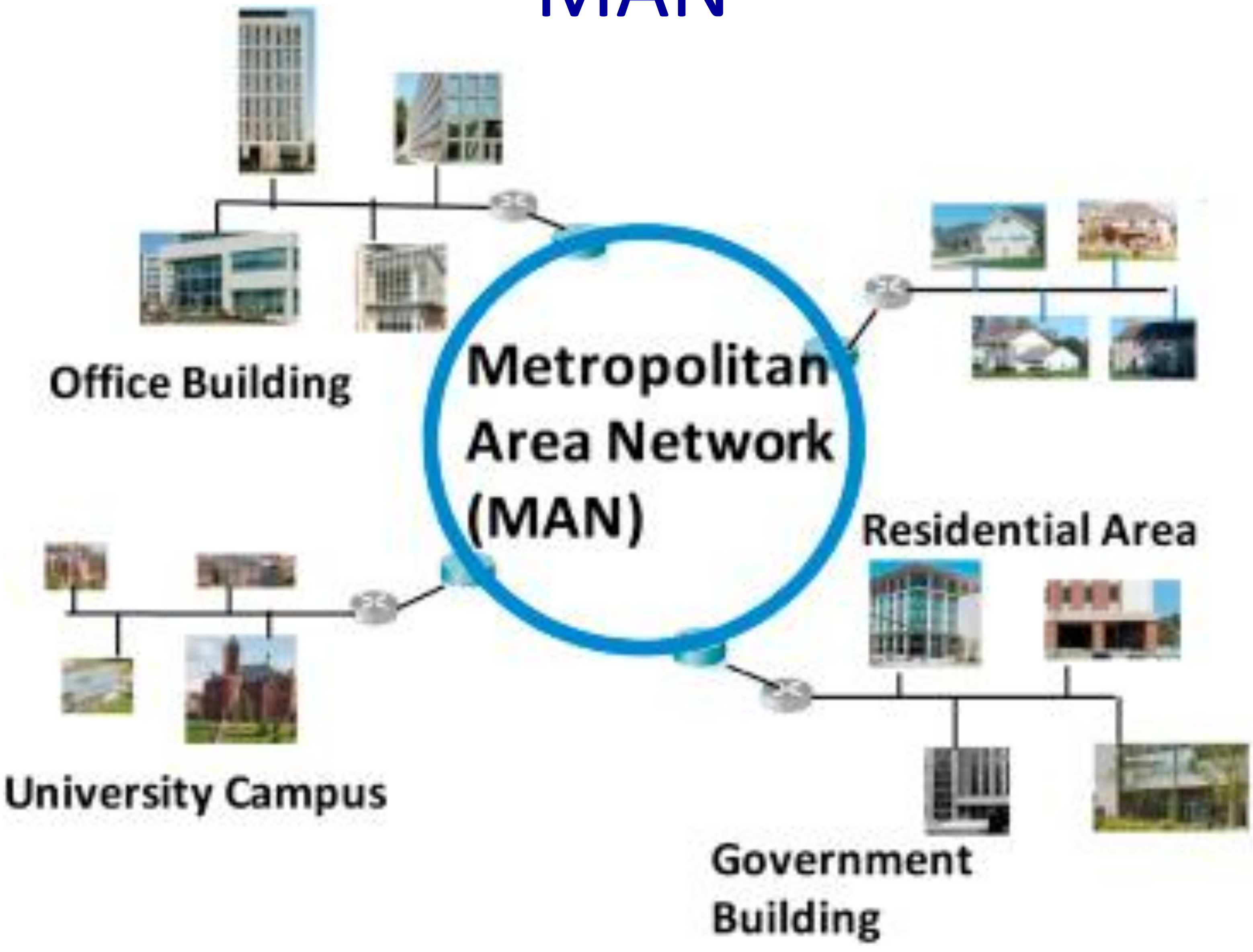
Types of Network

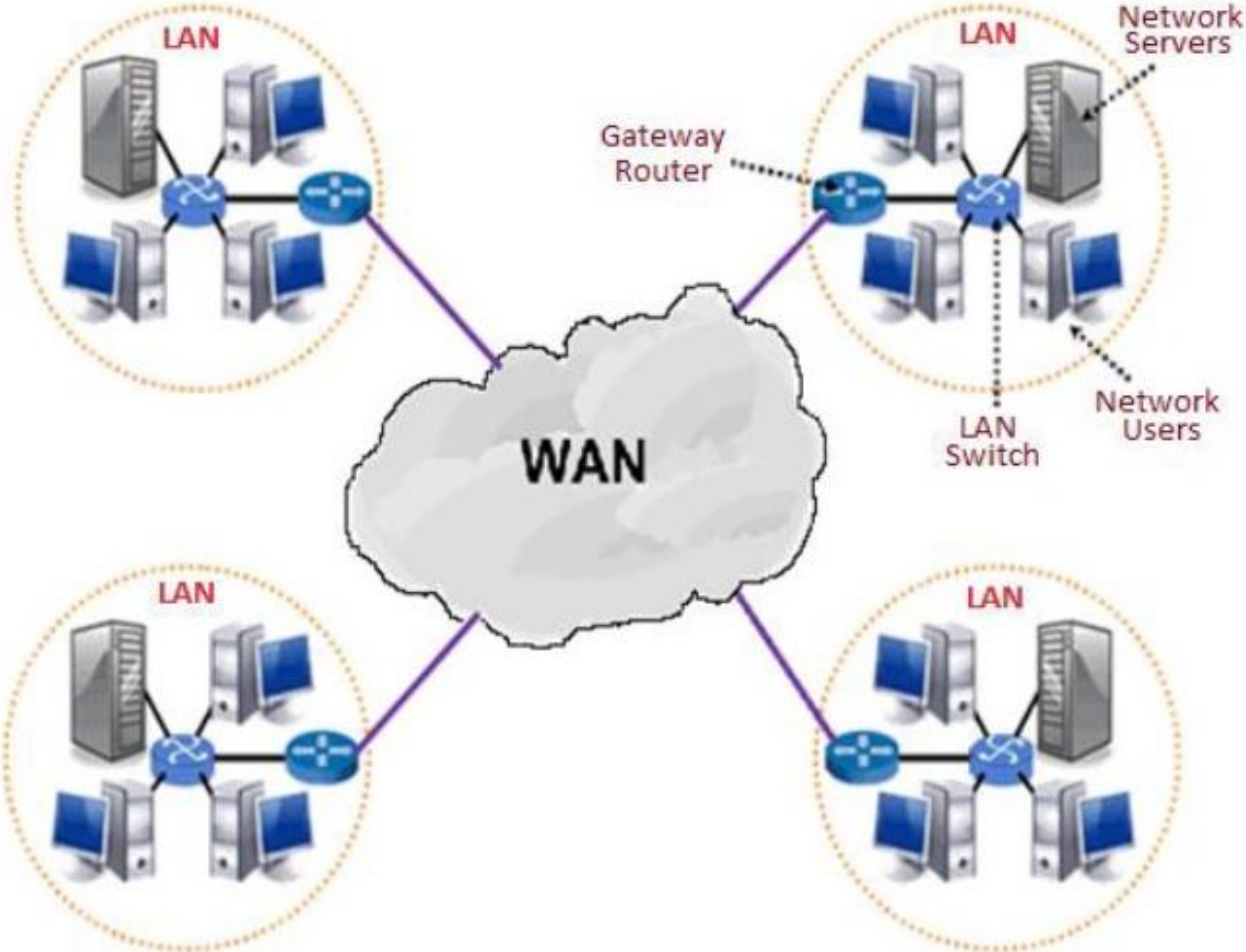
- Based on distance
  - Personal Area Network (PAN)
  - Local Area Network (LAN), 0-2 km
  - Metropolitan Area Network (MAN), 2-50 km,
  - Wide Area Network (WAN), 50+ km

PAN


LAN

MAN

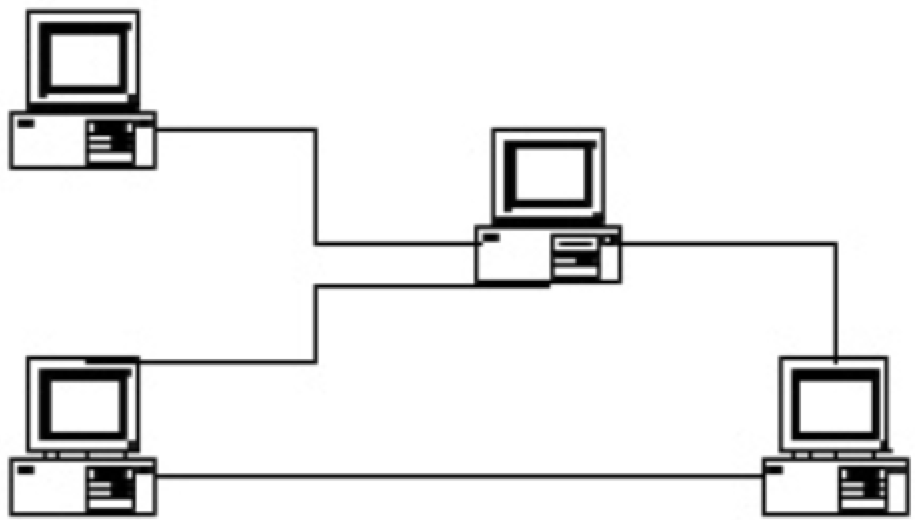

Office Building
Metropolitan
Area Network
(MAN)
Residential Area
University Campus
Government
Building


LAN
LAN
Network Servers
Gateway Router
WAN
LAN Switch
Network Users
LAN
LAN

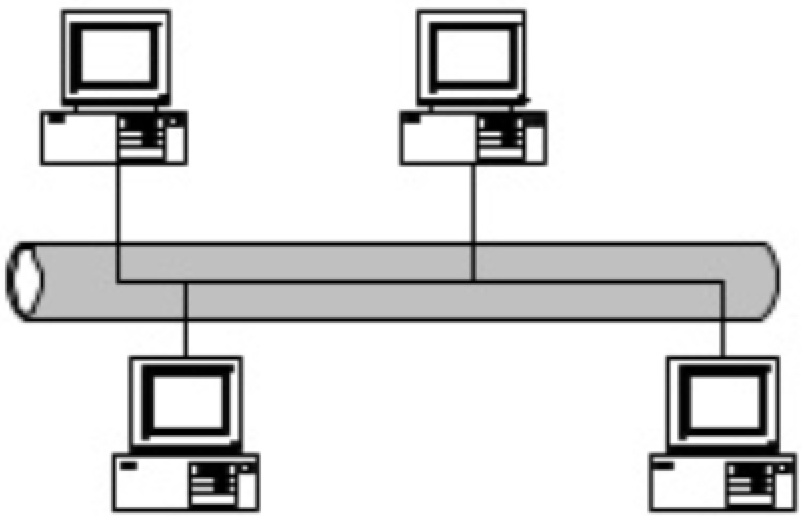
WAN

Types of Networks

- Based on Transmission Technology
  - Point-to-Point Networks: Pairs of hosts are directly connected.
  - Broadcast Networks: All stations share a single communication channel.



Point-to-Point Network

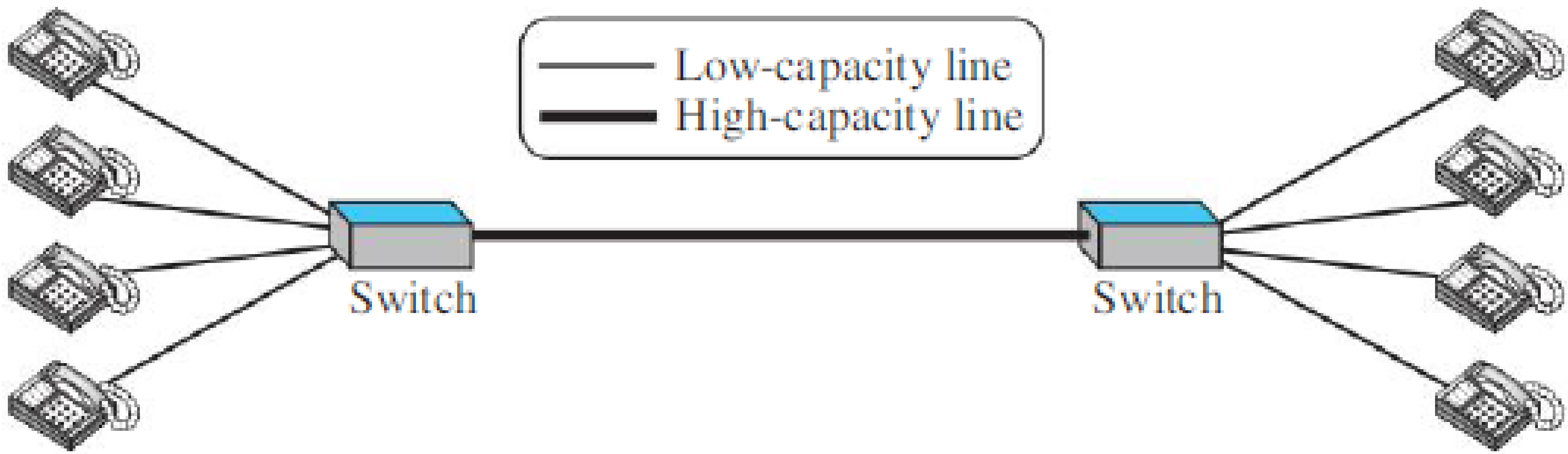


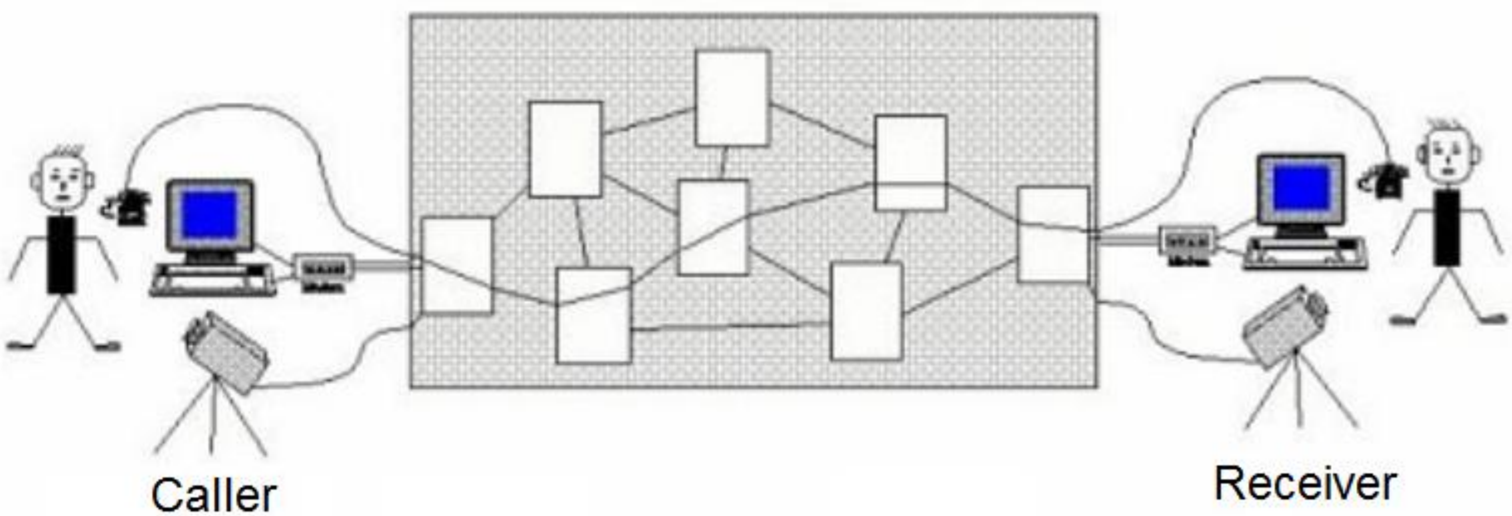
Broadcast Network

Types of Networks

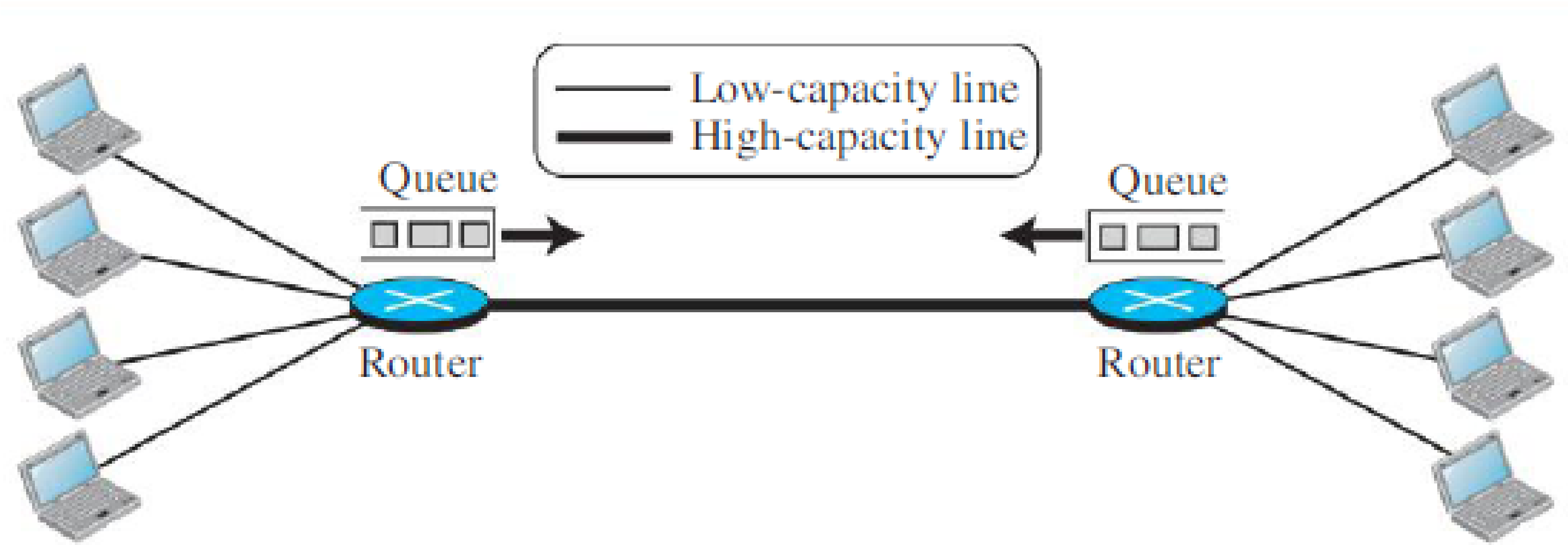
- Based on switching technique
  - Circuit Switched Networks
    - A dedicated path (circuit) is setup before transmission.
    - All bits follow the same path, e.g., Phone.
  - Packet Switched Networks
    - Packets of bits are forwarded individually.

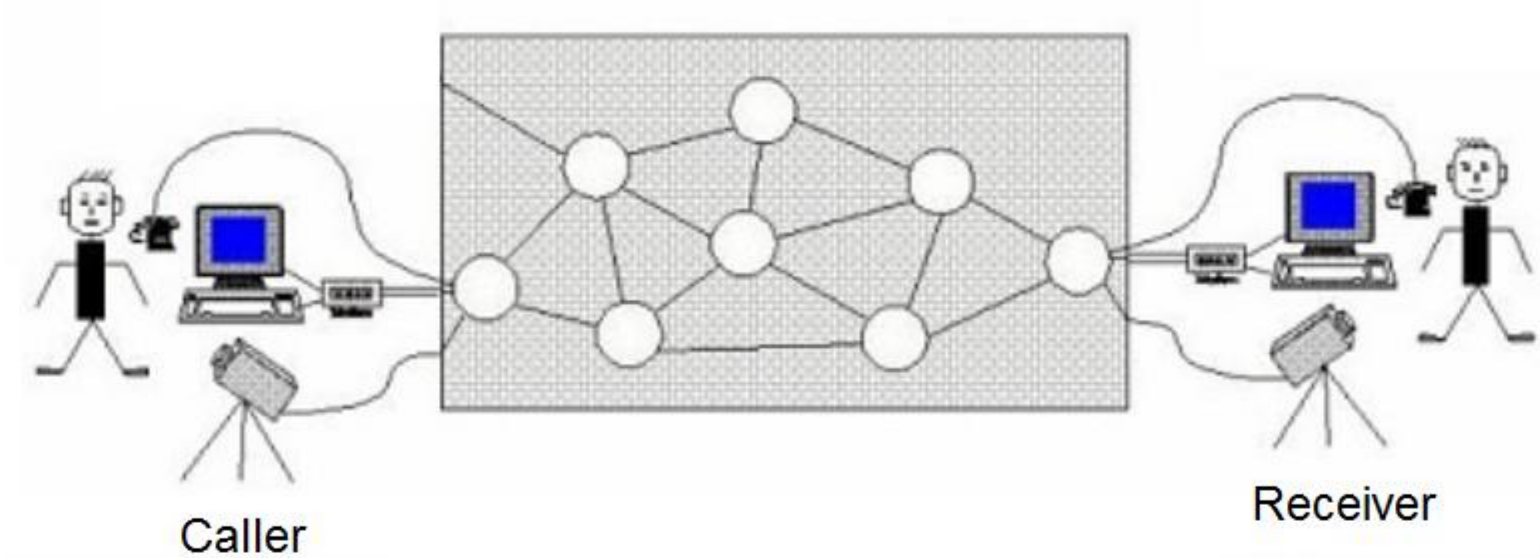
Circuit Switched Network

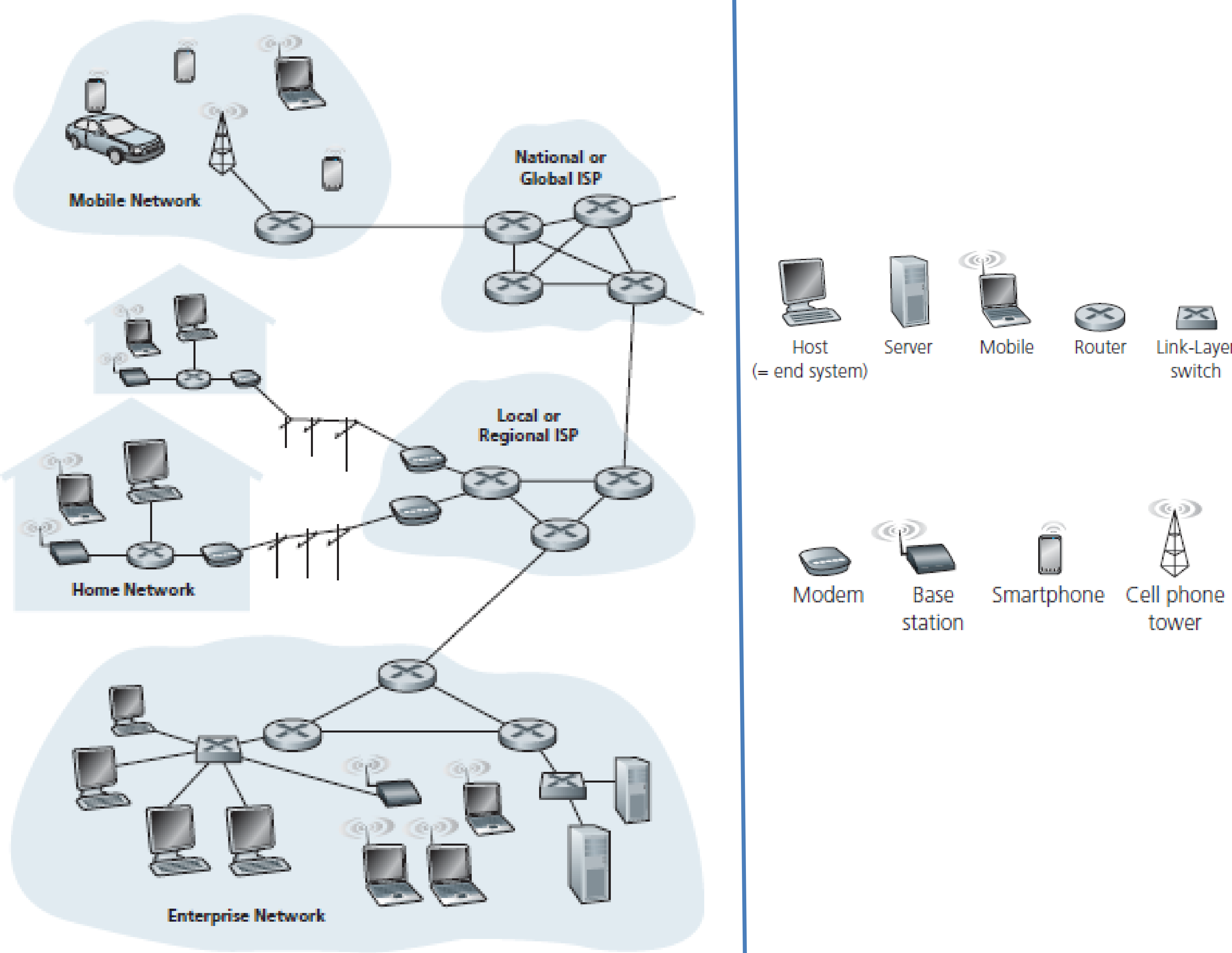




Packet Switched Network







Mobile Network
National or Global ISP
Local or Regional ISP
Home Network
Enterprise Network
Host (= end system)
Server
Mobile
Router
Link-Layer switch
Modem
Base station
Smartphone
Cell phone tower

Terminology

- **Hosts** or **end systems –** computing devices
  - Laptops,
  - smart phones,
  - tablets,
  - TVs,
  - gaming consoles,
  - Web cams,
  - automobiles,
  - environmental sensing devices,
  - picture frames, and
  - home electrical and security systems.

Terminology…

- End systems are connected together by a network of **communication links** and **packet switches.**
- Many types of **communication links**, which are made up of different types of physical **media**, including
  - Coaxial cable,
  - Copper wire,
  - Optical fiber, and
  - Radio spectrum.
- Different links can transmit data at different rates, with the **transmission rate** of a link measured in bits/second.

- When one end system has data to send to another end system,
  - The sending end system segments the data and adds header bytes to each segment.
  - The resulting packages of information, known as **packets.**
  - Packets are then sent through the network to the destination end system.
  - Destination end system reassemble the packets into the original data.

Terminology…

- A **packet switch**
  - takes a packet arriving on one of its incoming communication links and
  - forwards that packet on one of its outgoing communication links.
- Mainly 2 types
  - **Routers** and
  - **Link-layer switches.**

Terminology…

- End systems access the Internet through **Internet Service Provider (ISPs).**
- Each ISP is in itself a network of packet switches and communication links.

Terminology…

- **Protocols - ** Rules.

> Definition: *A **protocol** defines the <u>format and the order of messages</u> exchanged between two or more communicating entities, as well as <u>the actions taken</u> on the transmission and/or receipt of a message or other event.*

  – 2 main protocols in internet-
    - **Transmission Control Protocol (TCP)**
    - **Internet Protocol (IP)**

  – The Internet's principal protocols are collectively known as **TCP/IP**.

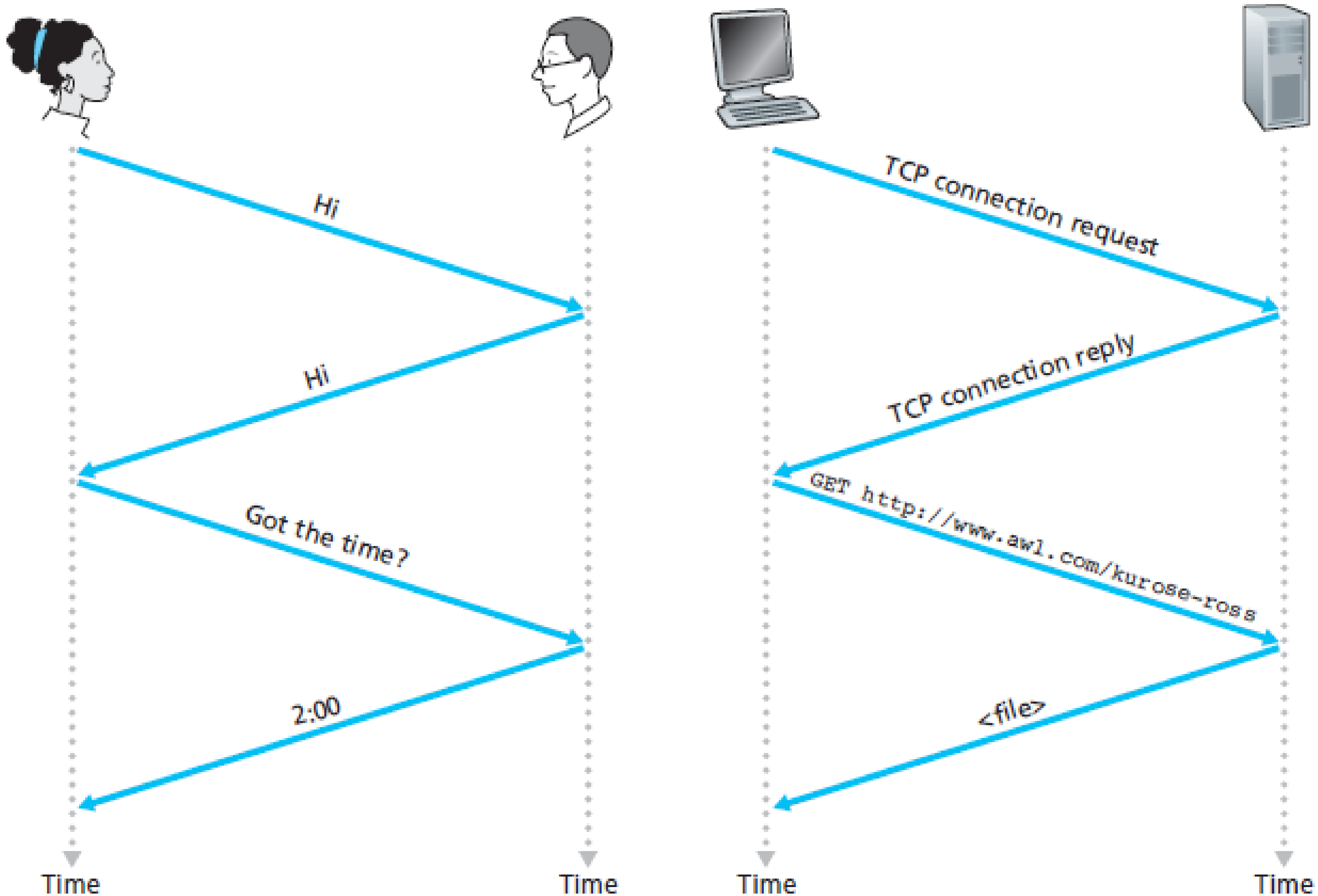


Figure ♦ A human protocol and a computer network protocol

Terminology…

- **Internet standards**
  - Everyone should agree on what each and every protocol does.
  - Developed by the **Internet Engineering Task Force (IETF)**.
  - The IETF standards documents are called **requests for comments** **(RFCs)**.
    - They define protocols such as TCP, IP, HTTP (for the Web), and SMTP (for e-mail).
    - There are currently more than 6,000 RFCs.

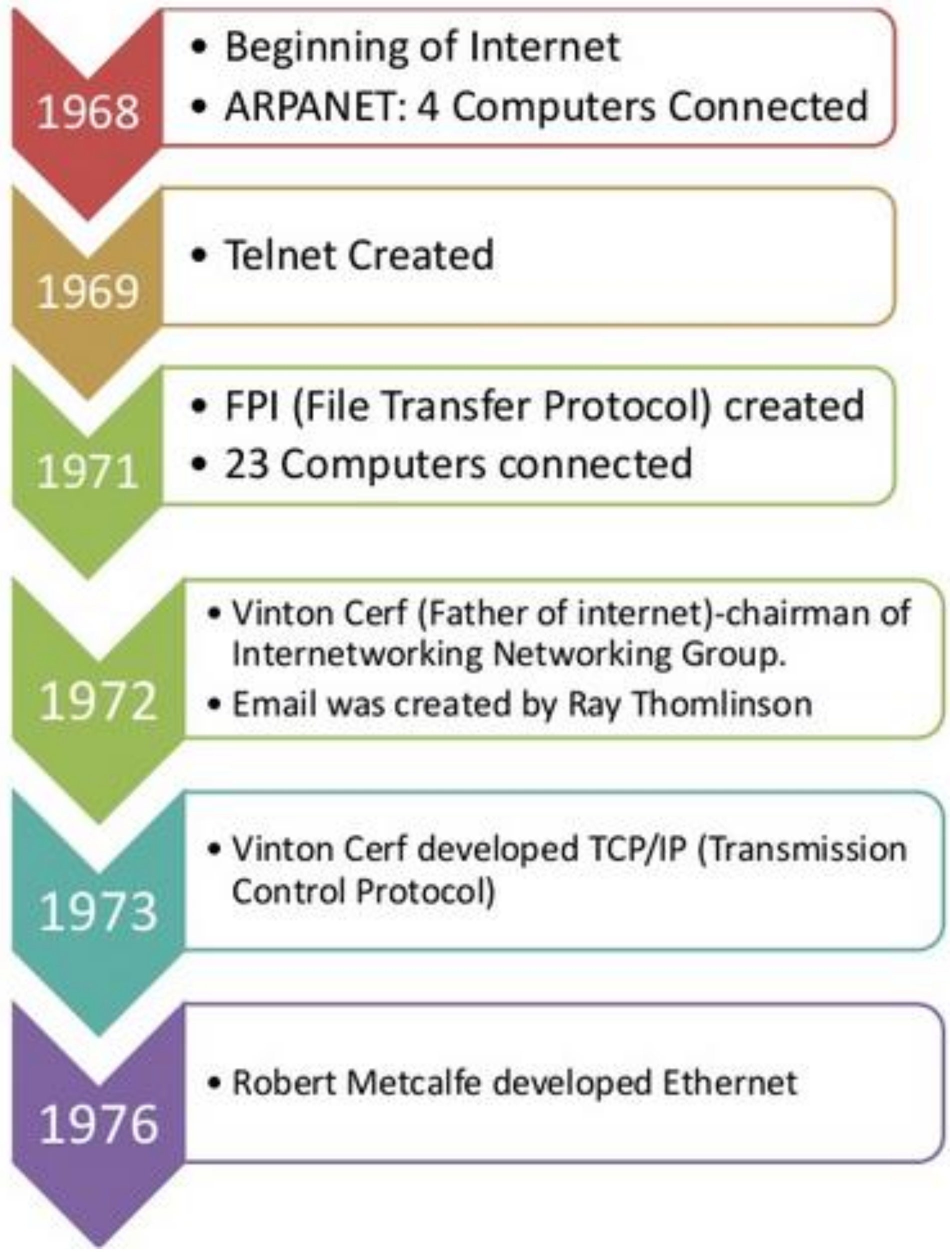
Internet : A service view

- ***Internet** - An infrastructure that provides services to applications.*
- These applications include
  - Electronic mail,
  - Web surfing,
  - Social networks,
  - Instant messaging,
  - Voiceover- IP (voip),
  - Video streaming,
  - Distributed games,
  - Peer-to-peer (P2P) file sharing,
  - Television over the internet,
  - Remote login, etc…
- The applications are said to be **distributed applications,** since they involve multiple end systems that exchange data with each other.

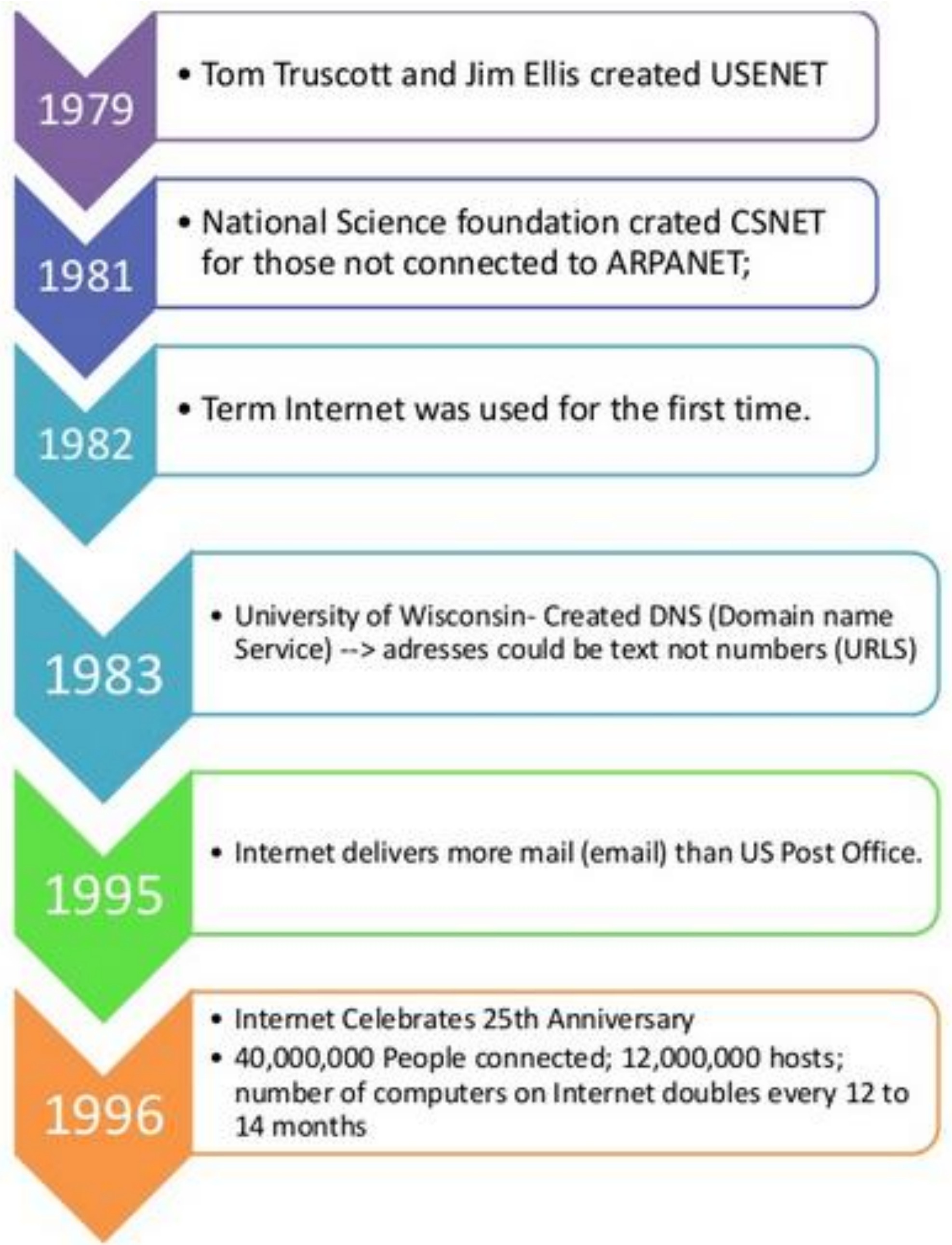
Internet : A service view…

- End systems attached to the Internet provide an **Application Programming Interface** **(API)**
  - *Specifies how a program running on one end system asks the Internet infrastructure to deliver data to a specific destination program running on another end system.*
  - A set of rules.

History


1968
• Beginning of Internet
• ARPANET: 4 Computers Connected
1969
• Telnet Created
1971
• FPI (File Transfer Protocol) created
• 23 Computers connected
1972
• Vinton Cerf (Father of internet)-chairman of Internetworking Networking Group.
• Email was created by Ray Thomlinson
1973
• Vinton Cerf developed TCP/IP (Transmission Control Protocol)
1976
• Robert Metcalfe developed Ethernet

History…


1979
• Tom Truscott and Jim Ellis created USENET
1981
• National Science foundation crated CSNET for those not connected to ARPANET;
1982
• Term Internet was used for the first time.
1983
• University of Wisconsin- Created DNS (Domain name Service) --> adresses could be text not numbers (URLS)
1995
• Internet delivers more mail (email) than US Post Office.
1996
• Internet Celebrates 25th Anniversary
• 40,000,000 People connected; 12,000,000 hosts; number of computers on Internet doubles every 12 to 14 months

The Network Edge

End Systems

- The computers and other devices connected to the Internet are often referred to as **end systems.**

End Systems

- The computers and other devices connected to the Internet are often referred to as **end systems.**

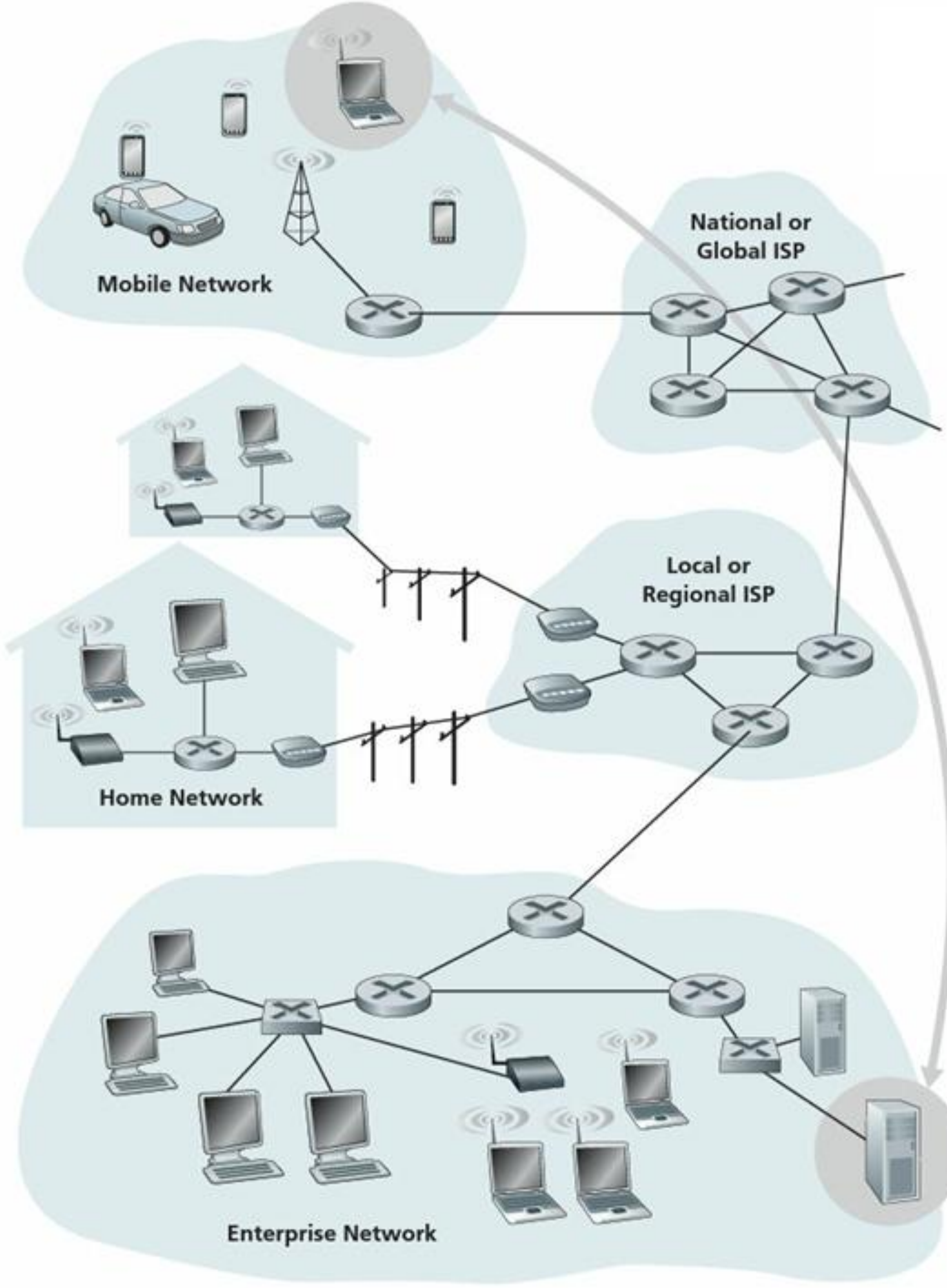
- WHY THEY ARE CALLED SO?

End Systems

- The computers and other devices connected to the Internet are often referred to as **end systems**.

- WHY THEY ARE CALLED SO?

- They are referred to as end systems because they sit at the edge of the Internet.


Mobile Network
National or
Global ISP
Local or
Regional ISP
Home Network
Enterprise Network

End Systems

- End systems are also referred to as **hosts.**

End Systems

- End systems are also referred to as **hosts.**

- Why?

End Systems

- End systems are also referred to as **hosts.**

- Why?

- Because they host (that is, run) application programs.

End Systems

- End systems are also referred to as **hosts.**
- Why?
- Because they host (that is, run) application programs such as :

  - a Web browser program,

  - a Web server program,

  - an e-mailclient program, or

  - an e-mail server program.

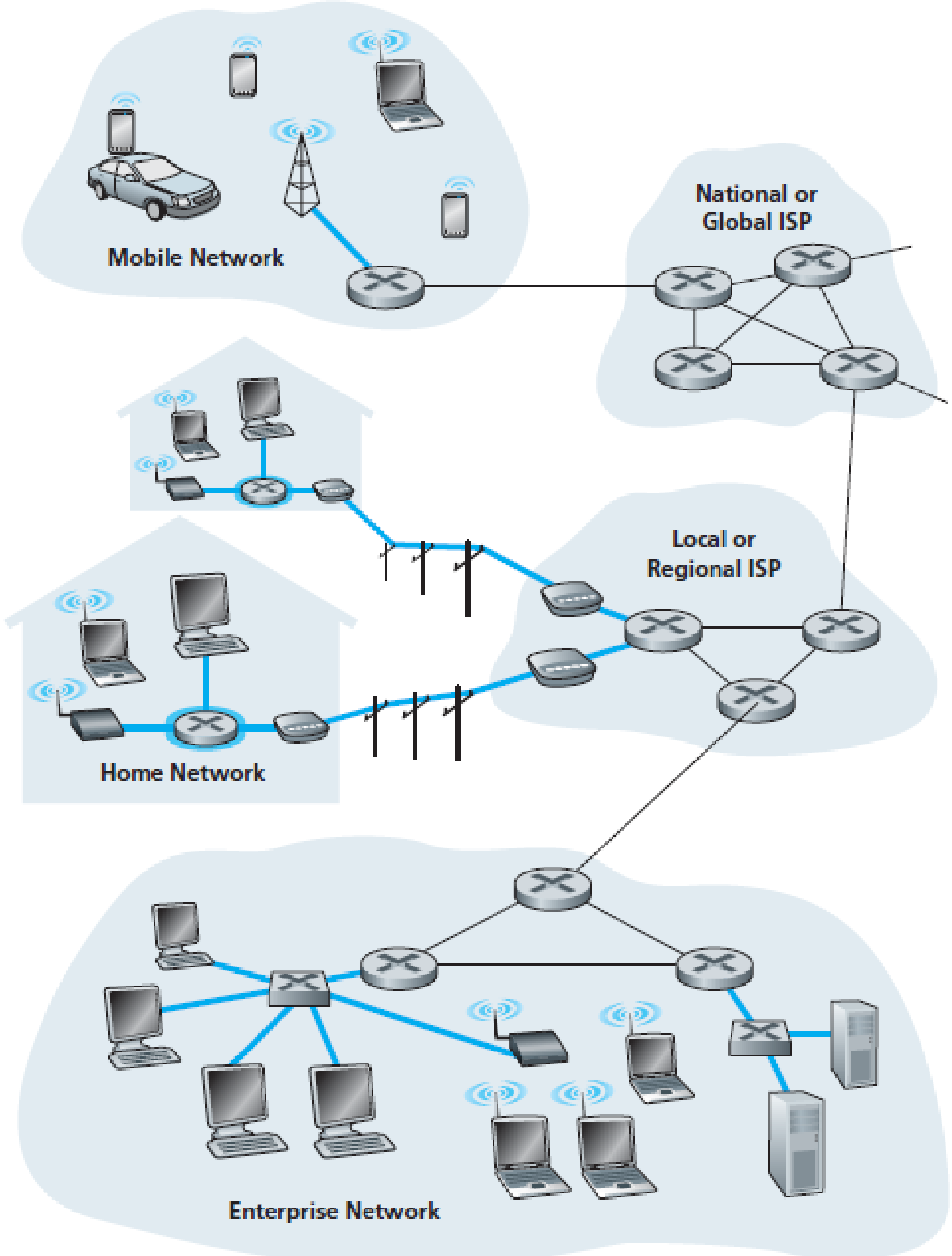
End Systems

- Hosts classified into 2
  - **Clients and**
  - **Servers.**

Access Networks

- The network that physically connects an end system to the first router on a path from the end system to any other distant end system.

- First router is also known as the “edge router”.



Mobile Network
National or Global ISP
Local or Regional ISP
Home Network
Enterprise Network

Types of Access Networks

1. **Home Access:**
   - DSL,
   - Cable,
   - FTTH,
   - Dial-Up, and
   - Satellite
2. **Enterprise Access :**
   - Ethernet and
   - WiFi
3. **Wide-Area Wireless Access:**
   - 3G and
   - LTE

Digital Subscriber Line (DSL)

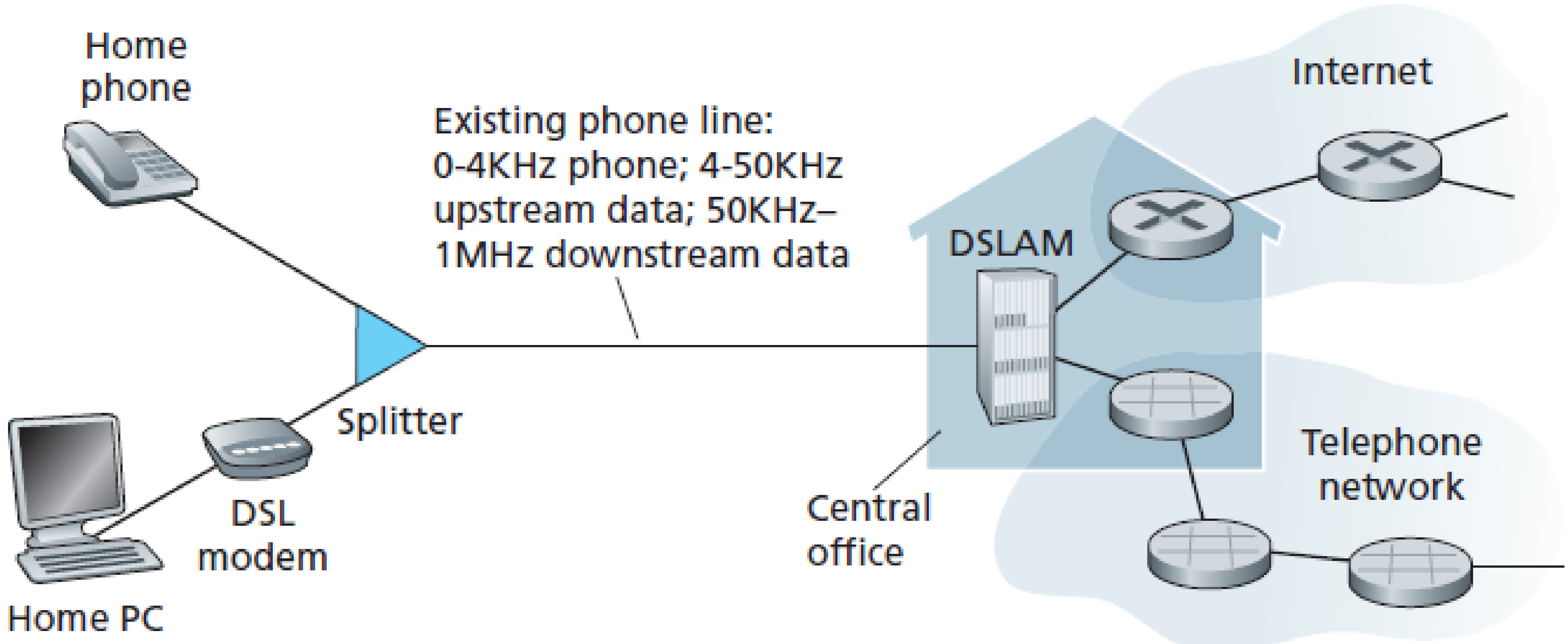


Figure ♦ DSL Internet access

Digital Subscriber Line Access Multiplexer (DSLAM)

Cable Internet Access

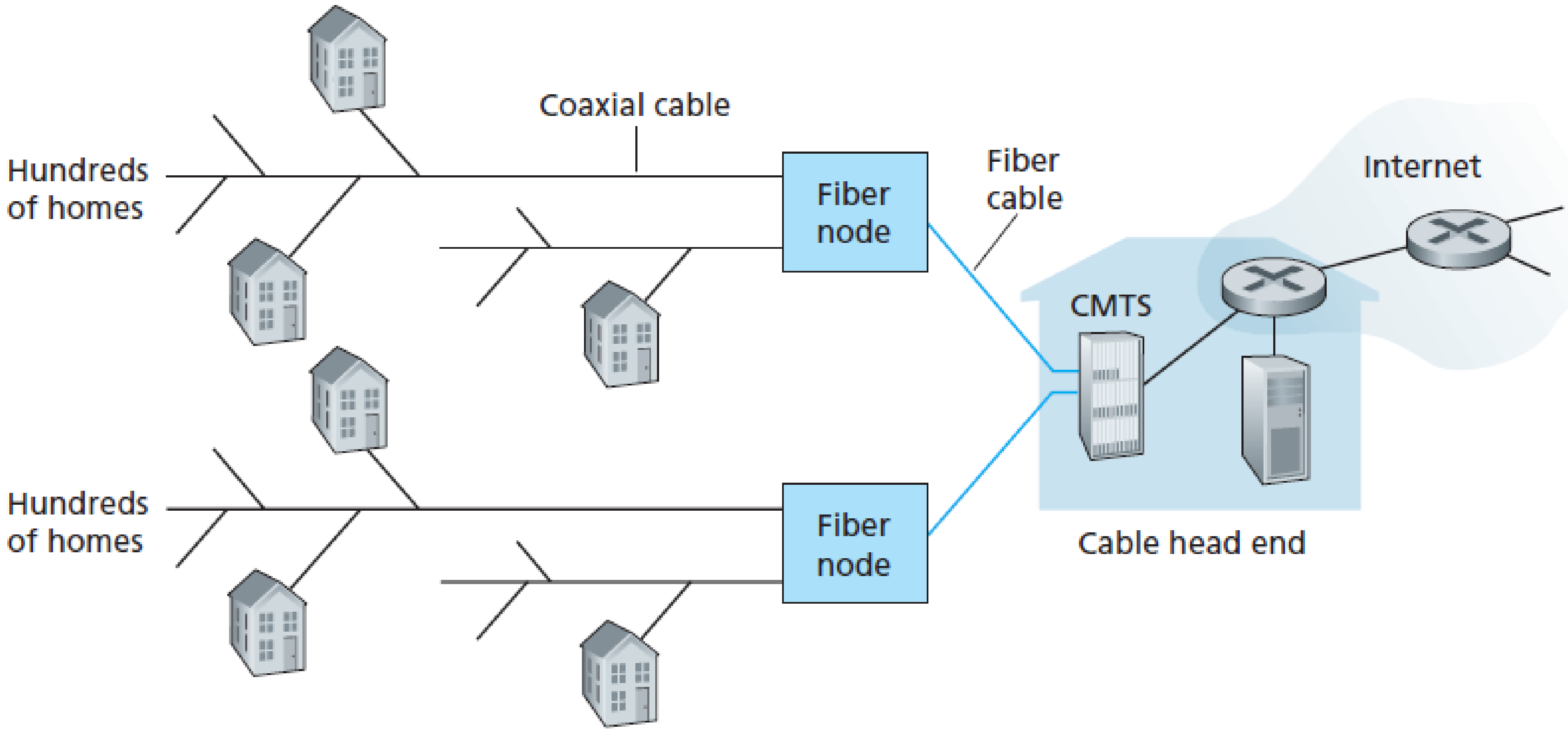


Figure ♦ A hybrid fiber-coaxial access network

Cable Modem Termination System (CMTS)

Because both fiber and coaxial cable are employed in this system, it is often referred to as **Hybrid Fiber Coax (HFC)**.

Fiber To The Home (FTTH)

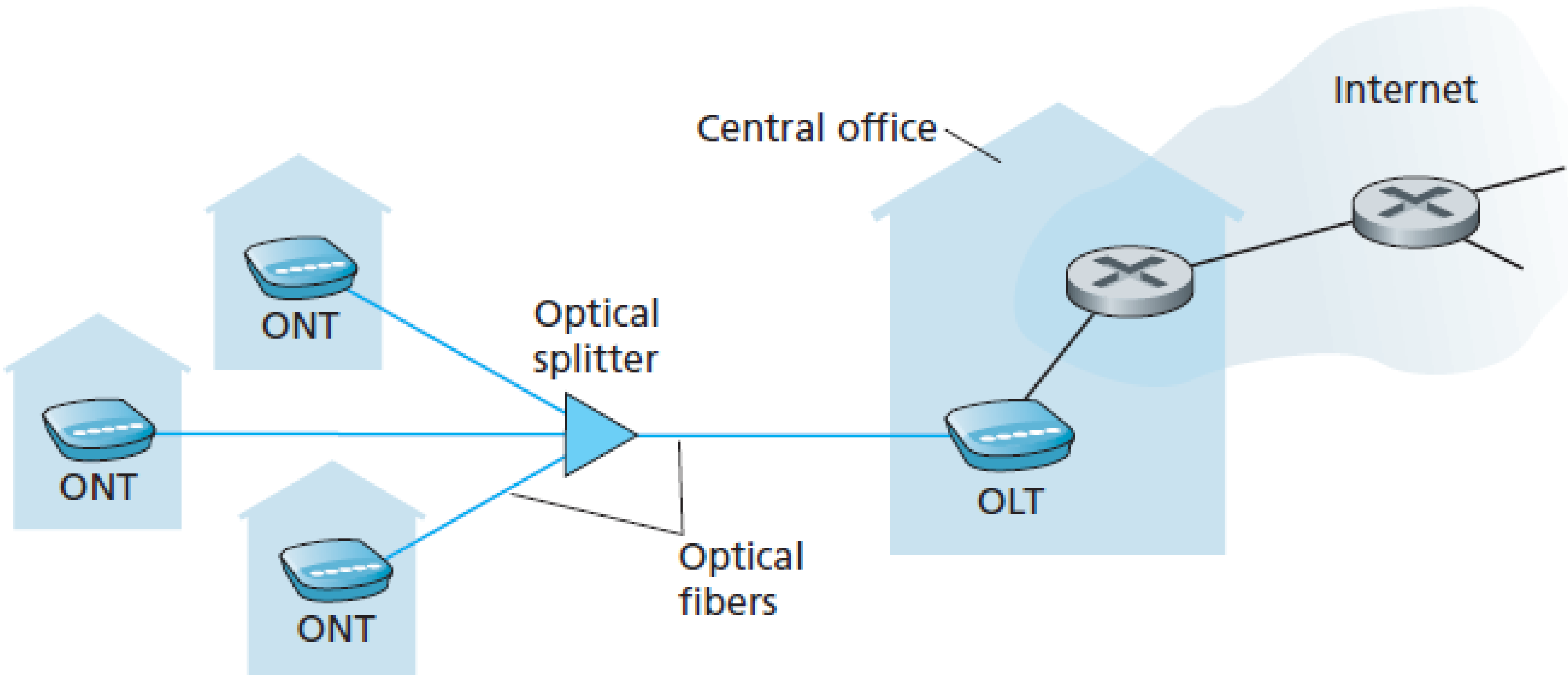


Figure ♦ FTTH Internet access

Optical Network Terminator (ONT)
Optical Line Terminator (OLT)

Fiber To The Home (FTTH)…

- Optical Distribution Network
  - Direct Fiber
    - One fiber leaving the CO for each home.
  - Using Splitter
    - Active Optical Networks (AONs) and
    - Passive Optical Networks (PONs)

Other Home Access Network Technologies

- Satellite link
  - Speed - more than 1 Mbps;
  - 2 satellite access providers.
    - StarBand and
    - HughesNet
- Dial-up access
  - over traditional phone lines
  - Speed - 56 kbps

Ethernet :

Wired(IEEE 802.3) and Wireless(IEEE 802.11)

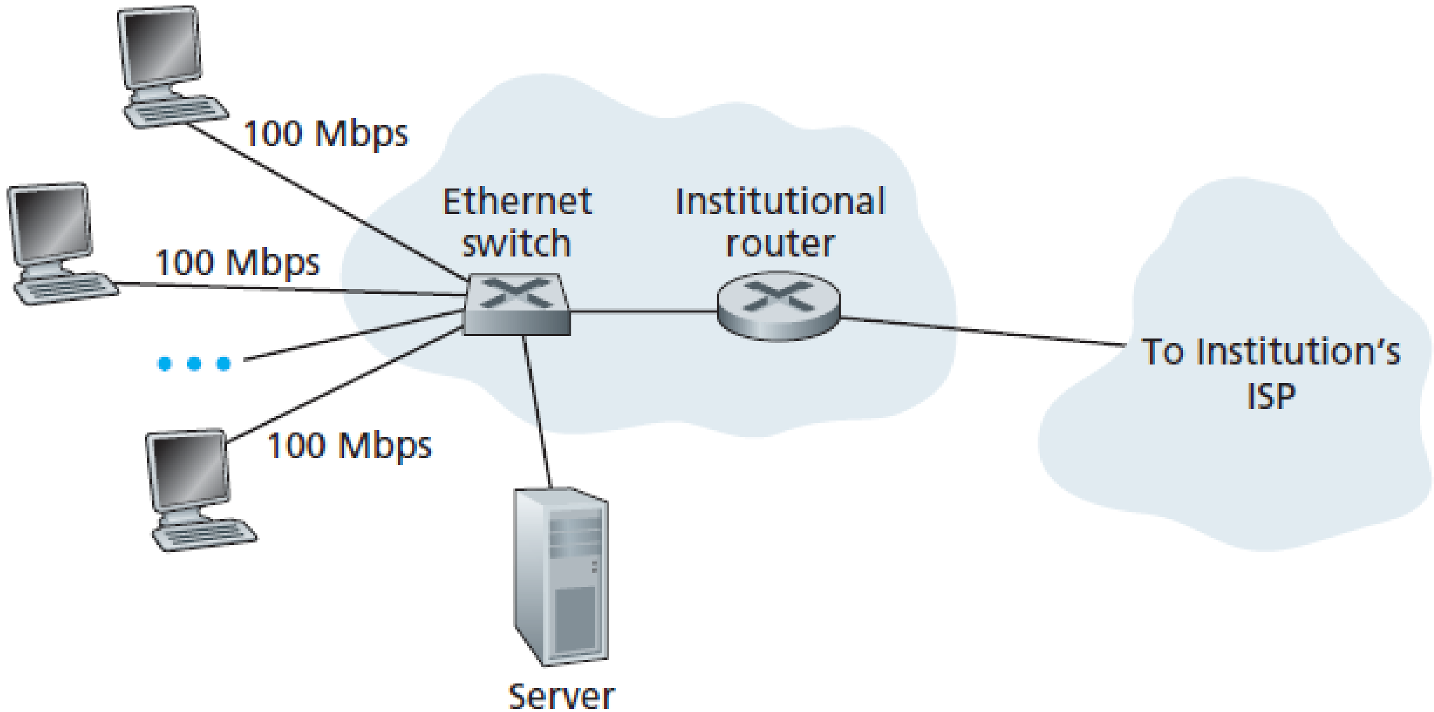


Figure ♦ Ethernet Internet access

Users have 100 Mbps access to the Ethernet switch, whereas servers may have 1 – 10 Gbps access.

WiFi Access Networks

- 802.11b (Wi-Fi 1) - 11 Mbps
- 802.11a (Wi-Fi 2) - 1.5-54 Mbps
- 802.11g (Wi-Fi 3) - 54 Mbps
- 802.11n (Wi-Fi 4)
  - 450 - 600 Mbps
- 802.11ac (Wi-Fi 5) - 1.73 Gbps
- 802.11ax (Wi-Fi 6)
  - *High Efficiency* Wi-Fi
  - 2.4 Gbps

WiFi ALLIANCE™

Wireless Fidelity

Combined Broadband and Wireless Network

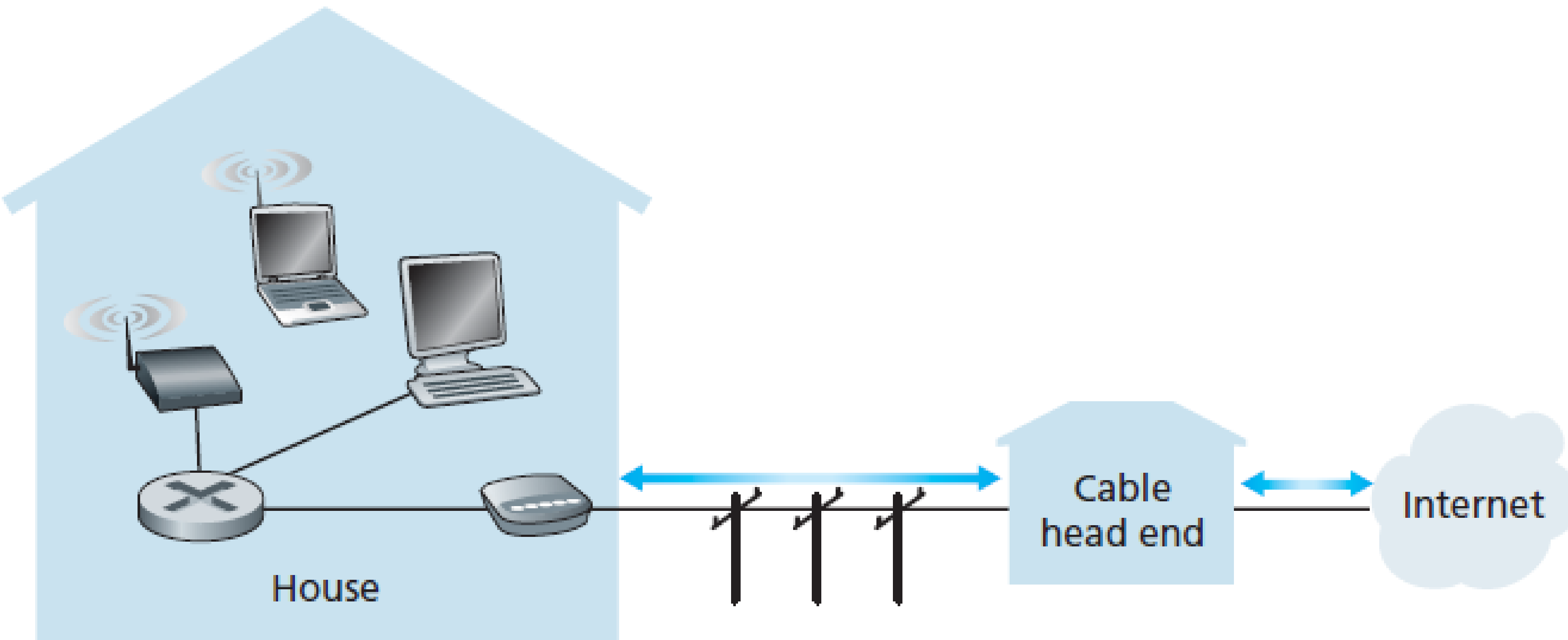


Figure ♦ A typical home network

Wide-Area Wireless Access

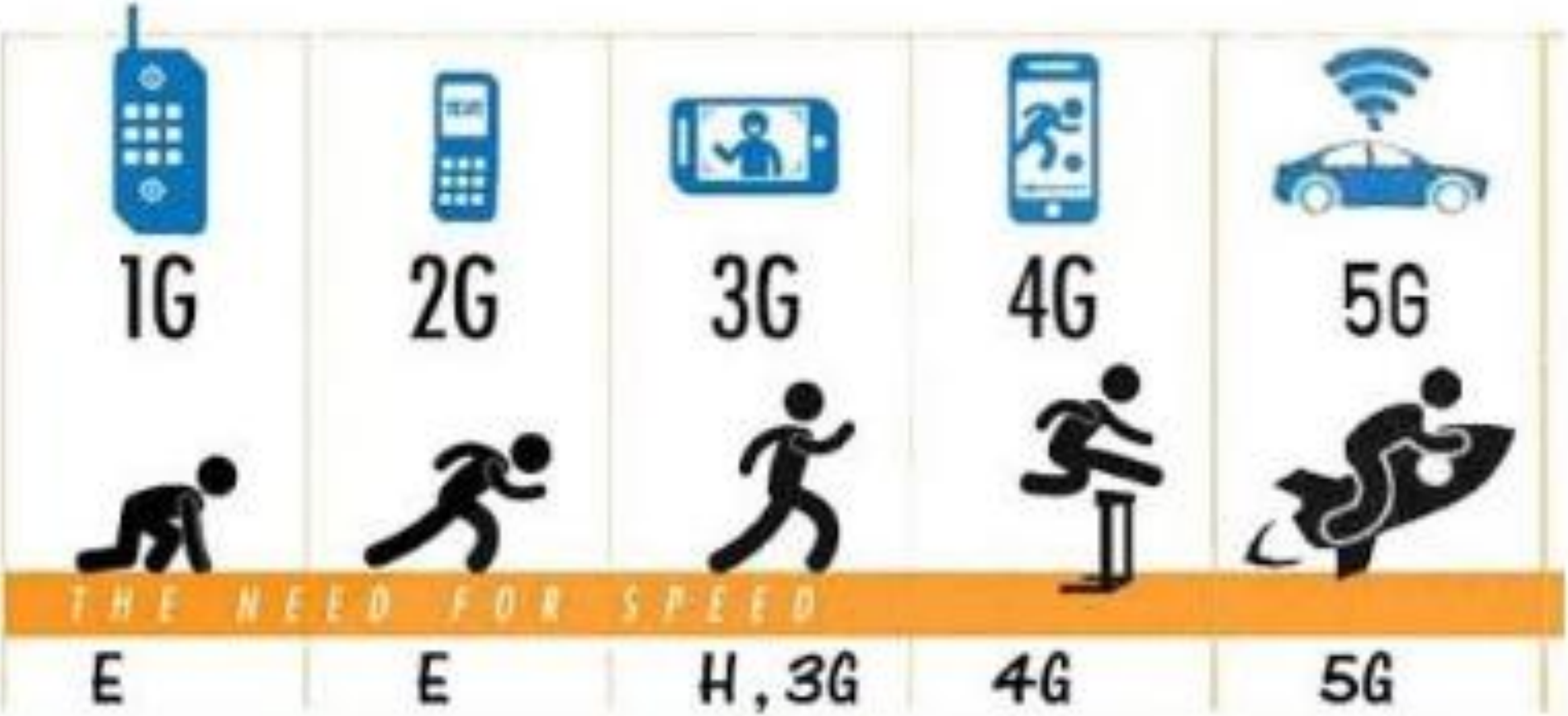
3G

- Packet-switched wide-area wireless Internet access
- Speed - 1 Mbps

LTE

- "Long-Term Evolution"
- Speed - 10 Mbps

(**Worldwide Interoperability for Microwave Access**)

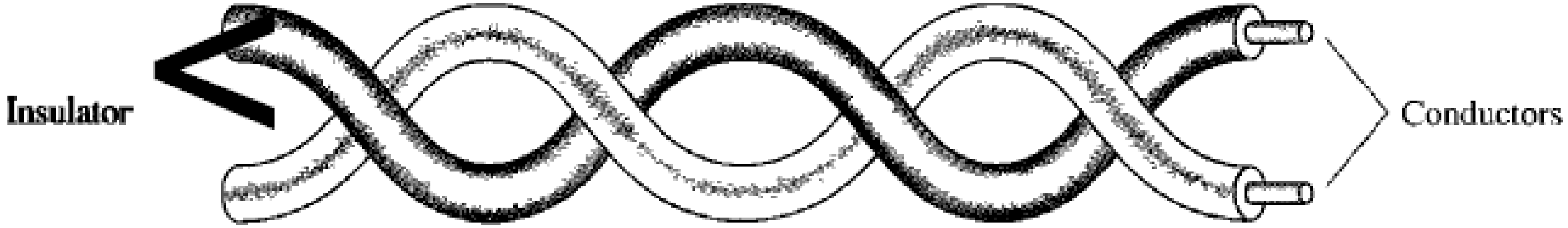

1G
2G
3G
4G
5G
THE NEED FOR SPEED
E
E
H, 3G
4G
5G

Transmission/Physical Media

- **Guided**: waves are guided along a solid medium
  - Twisted Pair
  - Coaxial cable
  - Optical fiber
- **Unguided**: waves propagate in the atmosphere and in outer space
  - Microwave
  - Satellite

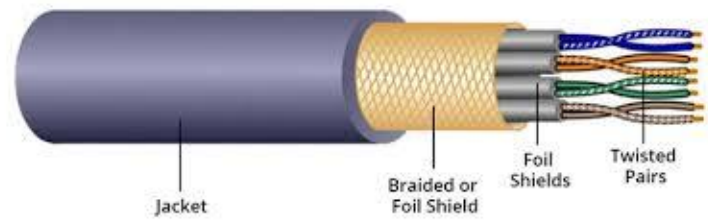
Twisted Pair (TP)

- Twisted pair consists of two insulated copper wires, each about 1 mm thick, arranged in a regular spiral pattern.
- The wires are twisted together to reduce the electrical interference from similar pairs close by.

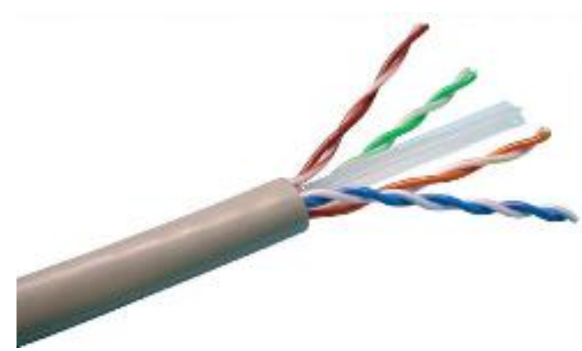


Shielded and Unshielded TP

- **Shielded Twisted Pair (STP)**
  - Metal braid or sheathing that reduces interference
  - More expensive
  - Harder to handle (thick, heavy)
  - Used in token rings

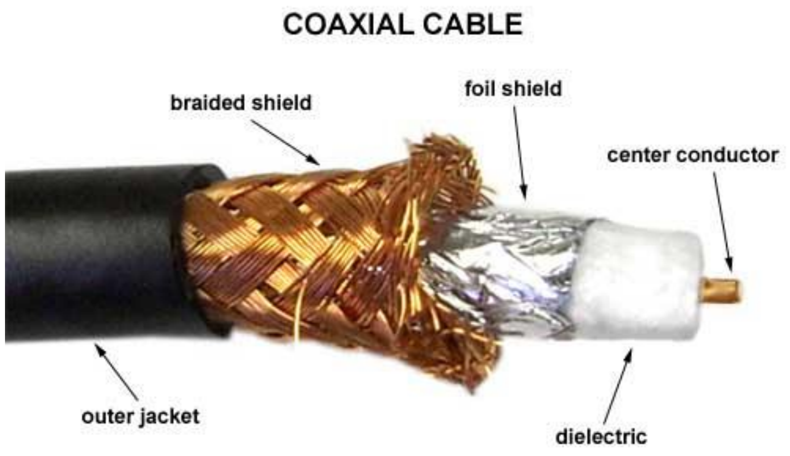


- **Unshielded Twisted Pair (UTP)**
  - Ordinary telephone wire
  - Cheap, Flexible
  - Easiest to install
  - No shielding
  - Suffers from external interference
  - Used in Telephone and Ethernet



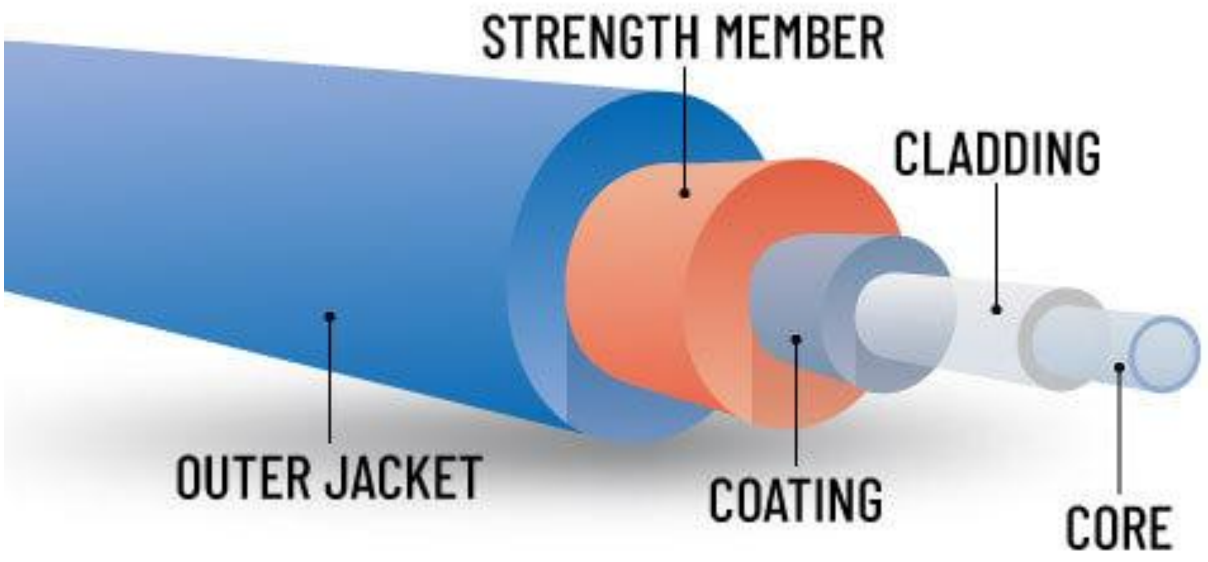
Coaxial Cable

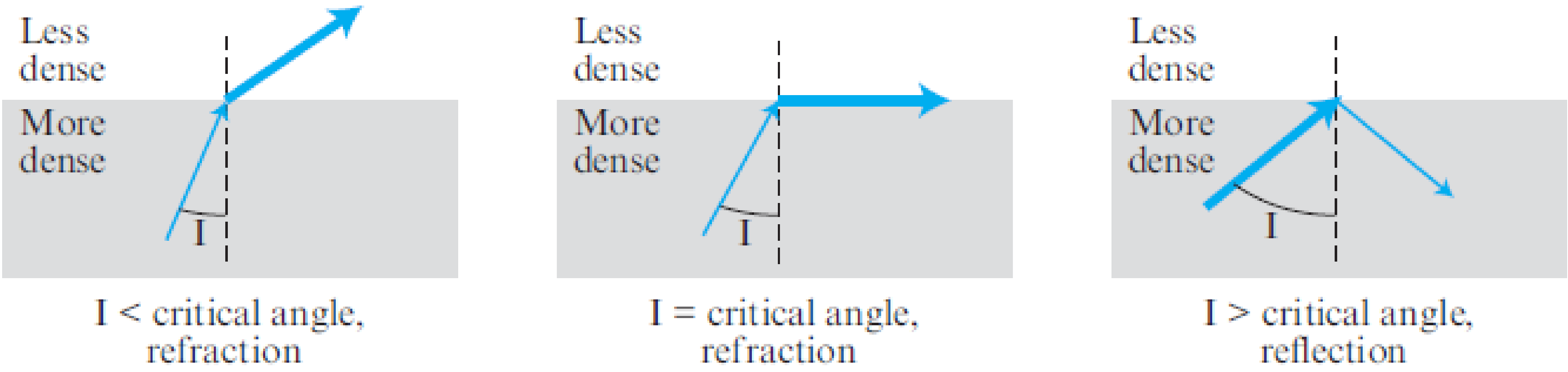
- Coaxial cable (or coax) has a central core conductor of solid or stranded wire
  - – enclosed in an insulating sheath, which is, encased in an outer conductor of metal foil, braid, or a combination of the two.
- The outer metallic wrapping serves both as a shield against noise and as the second conductor, which completes the circuit.



Fiber-Optic Cable

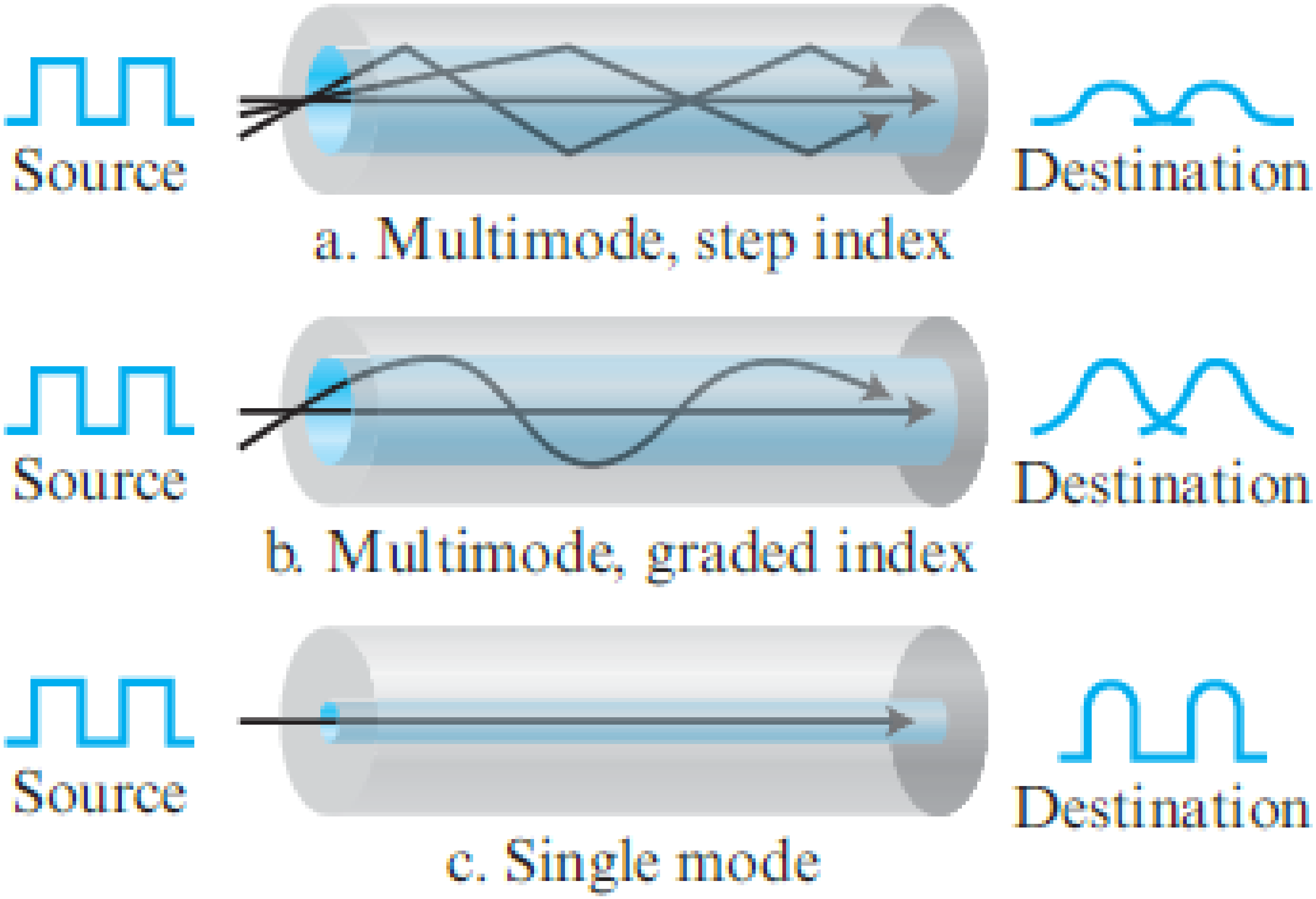
- A fiber-optic cable is made of glass or plastic and transmits signals in the form of light.
- Optical fibers use reflection to guide light through a channel.



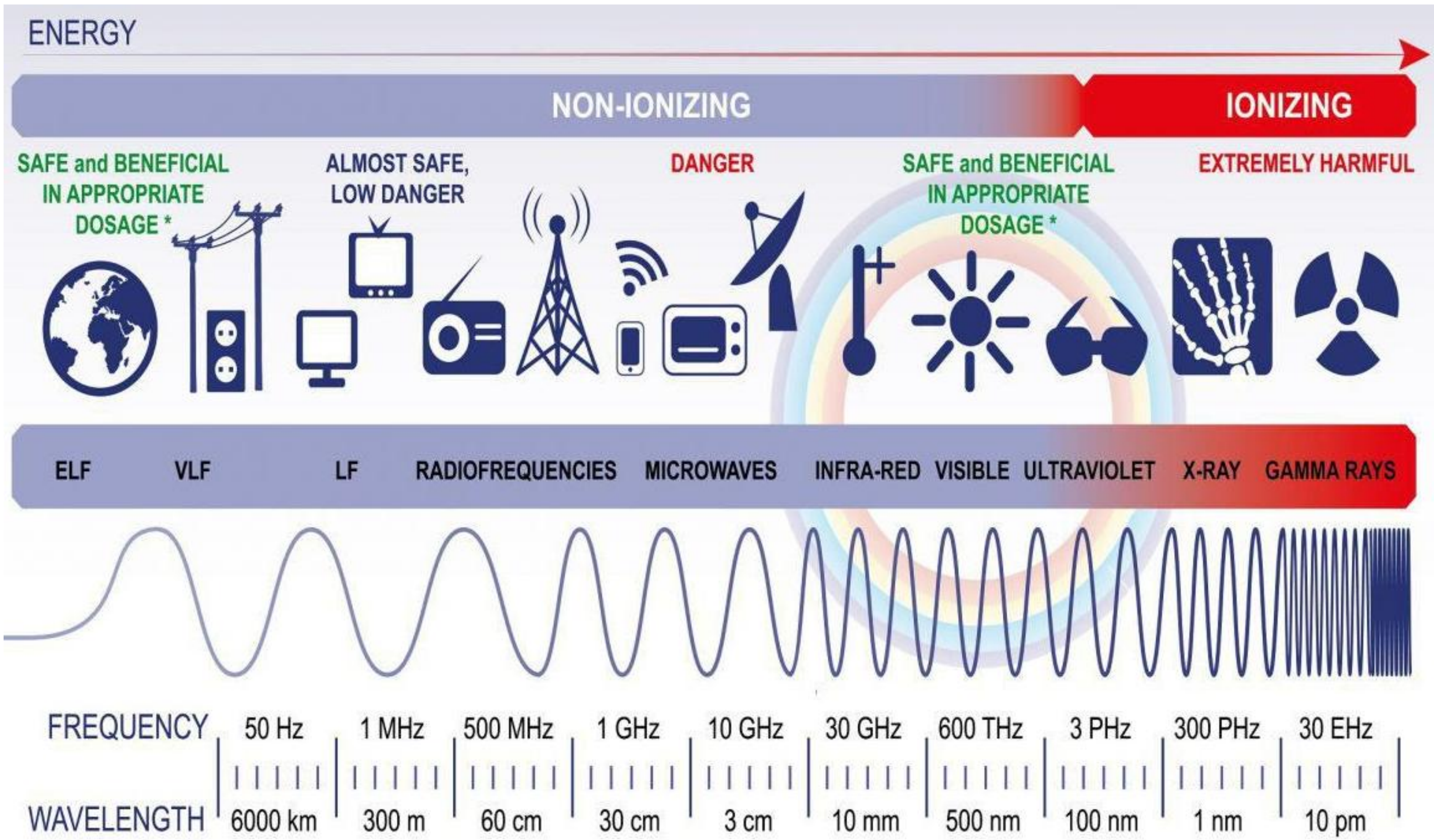


Bending of light ray

Propagation Modes



Electromagnetic Spectrum



Terrestrial Radio Channels

- 3 groups:
  - Operate over very short distance (e.G., With one or two meters).
  - Operate in local areas, (spanning from ten to a few hundred meters).
  - Operate in the wide area (spanning tens of kilometers).

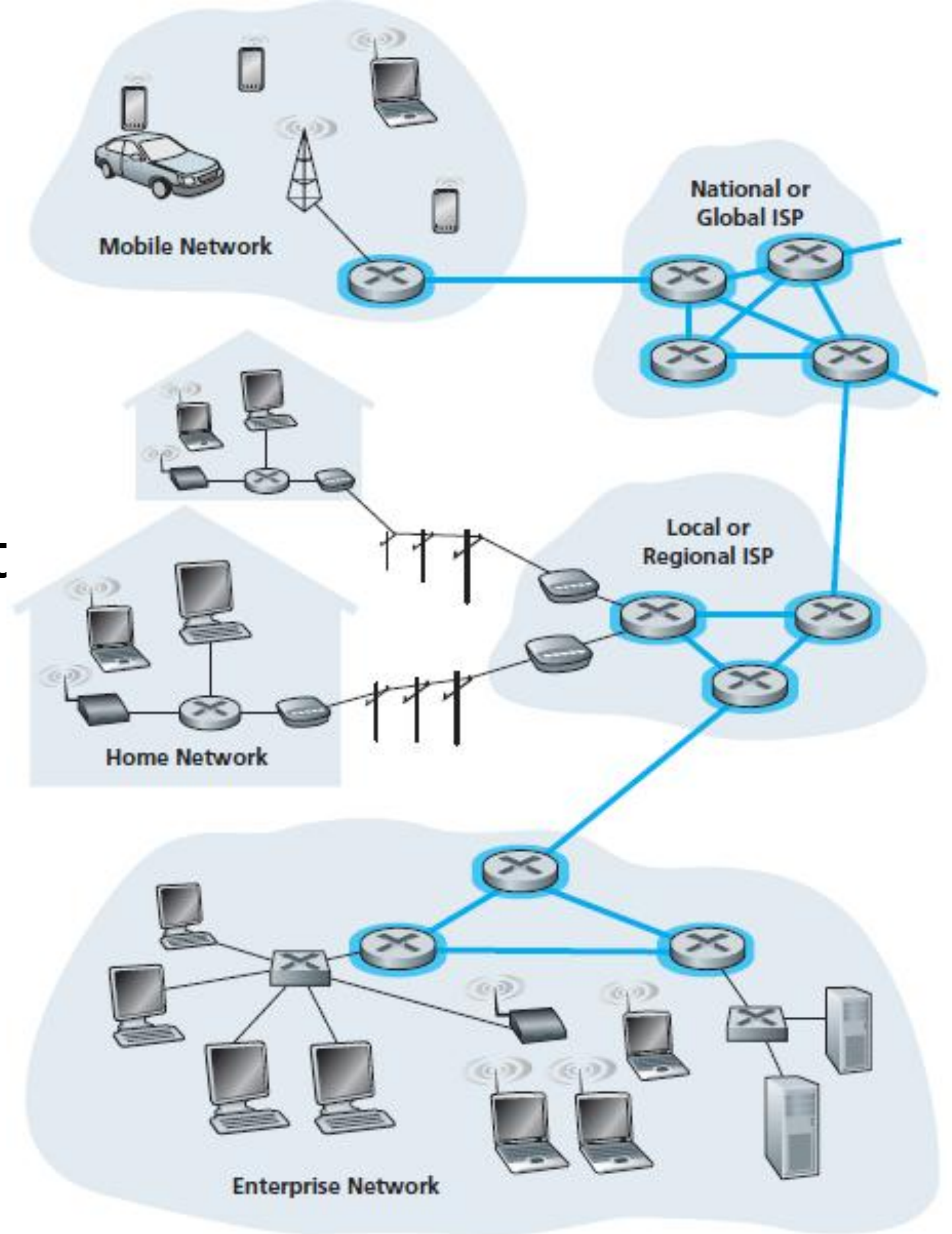
Satellite Radio Channels

- Two types of satellites are used in communications:
  - **Geostationary satellites**
    - Permanently remain above the same spot on Earth.
    - Placed in orbit at 36,000 km above Earth's surface.
    - Signal propagation delay of 280 milliseconds.
  - **Low-earth orbiting (LEO) satellites.**
    - Placed much closer to Earth and do not remain permanently above one spot on Earth.
    - They rotate around Earth.

The Network Core

The Network Core

- The mesh of packet switches and links that interconnects the Internet's end systems.



Packet Switching

- End systems exchange **messages** with each other.
- To send a message from a source end system to a destination end system,
  - The source breaks long messages into smaller chunks of data known as **packets.**
  - Between source and destination, each packet travels through **communication links** and **packet switches** (routers and link-layer switches).

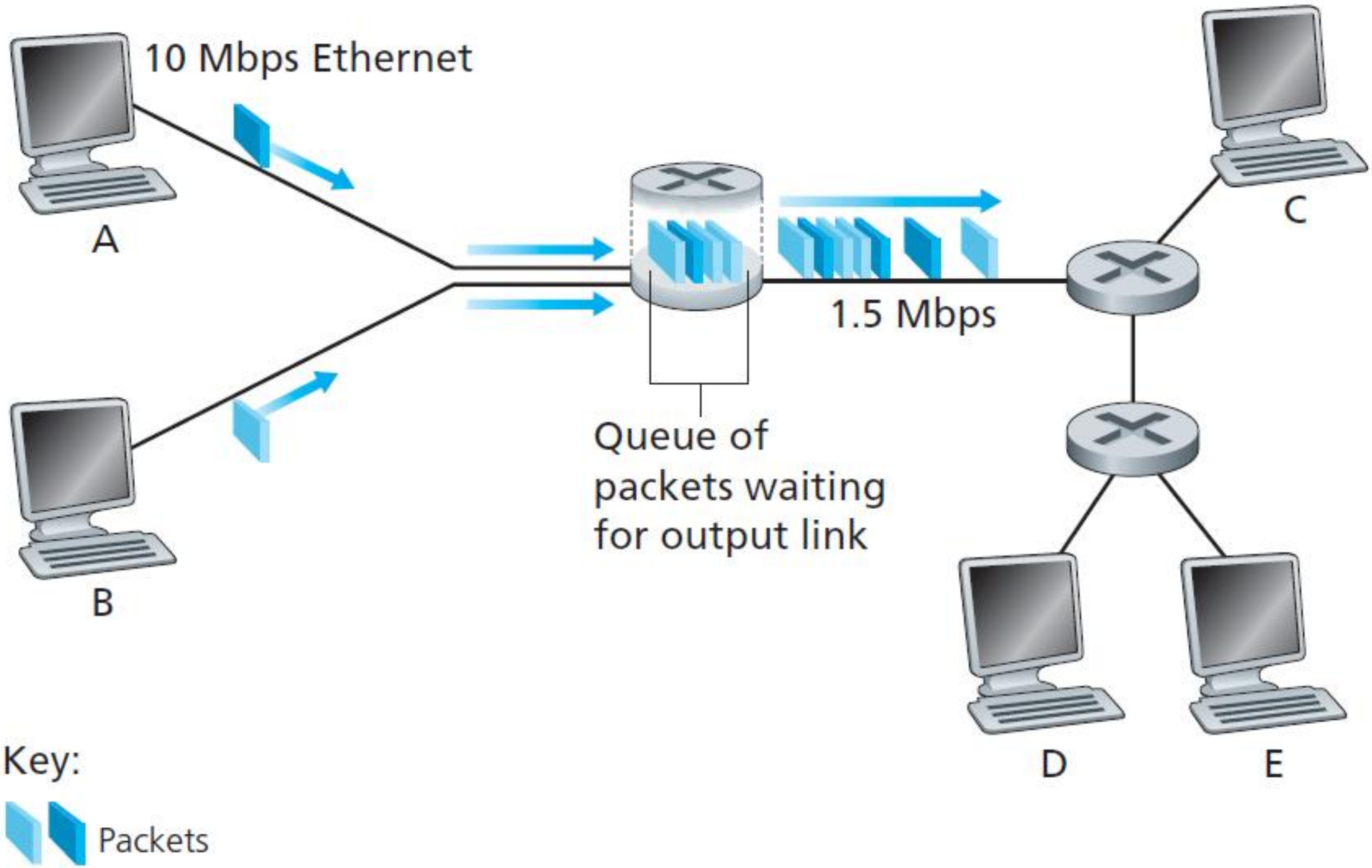


Figure ♦ Packet switching

Packet Switching…

- The Packets are transmitted over each communication link at a rate equal to the *full* ***transmission rate*** *of the link.*
- So, if a source end system or a packet switch is sending a packet of *L bits* over a link with *transmission rate R bits/sec*, then the time to transmit the packet is *L/R seconds.*

Store-and-Forward Transmission

- Packet switching method.
- Store-and-forward transmission means
  - The packet switch must receive the entire packet before it can begin to transmit the first bit of the packet onto the outbound link.

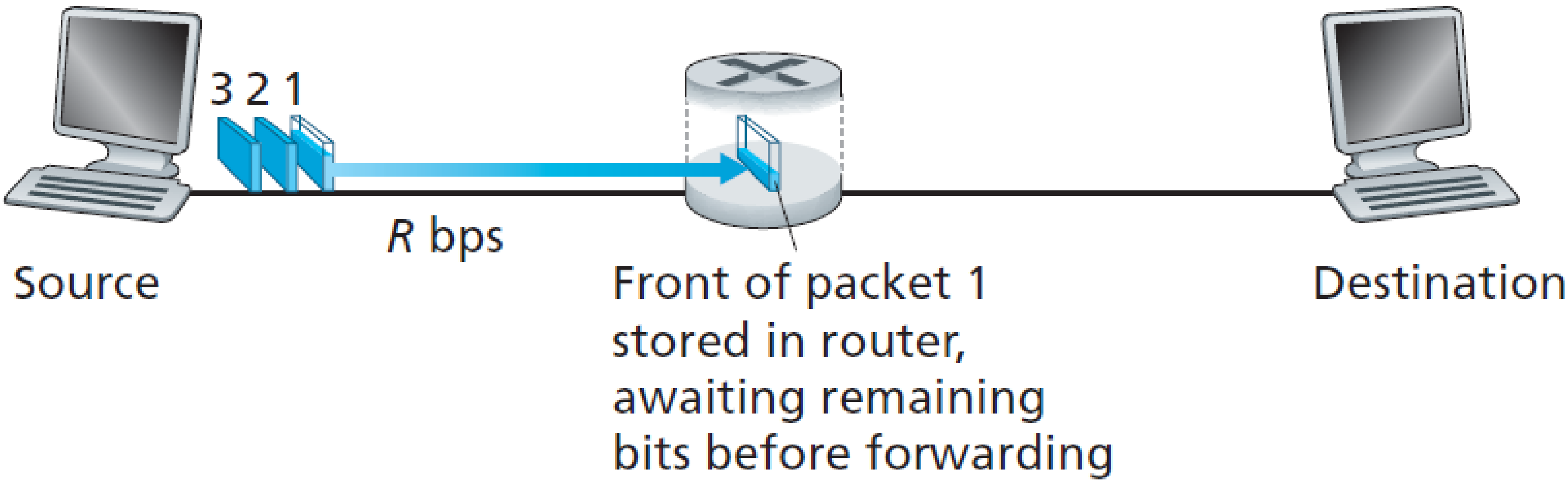


Figure ♦ Store-and-forward packet switching

- The source has transmitted some of packet 1, and the front of packet 1 has already arrived at the router.
- The router cannot transmit the bits it has received; instead it must first buffer (i.e., "store") the packet's bits.
- After receiving *all* of the packet's bits, the router *begin to transmit (i.e., "forward")* the packet onto the outbound link.

- <u>Amount of time for transmitting 1 packet</u>
  - Time 0 : source begins to transmit
  - Time L/R seconds *:*
    - Source has transmitted the entire packet.
    - The entire packet has been received and stored at the router.
    - Begin to transmit the packet onto the outbound link.
  - Time 2L/R *:*
    - The router has transmitted the entire packet, and
    - The entire packet has been received by the destination.
- Thus, the total delay is $2L/R$.

- Amount of time for transmitting 3 packets
  - Time 0 : source begins to transmit
  - Time L/R seconds *:*
    - Router begins to forward the first packet.
    - Source will begin to send the second packet.
  - Time 2L/R *:*
    - The destination has received the first packet
    - The router has received the second packet.
  - Time 3L/R *:*
    - The destination has received the first two packets
    - The router has received the third packet.
  - Time 4L/R *:*
    - Destination has received all three packets.
- Thus, the total delay is $4L/R$.

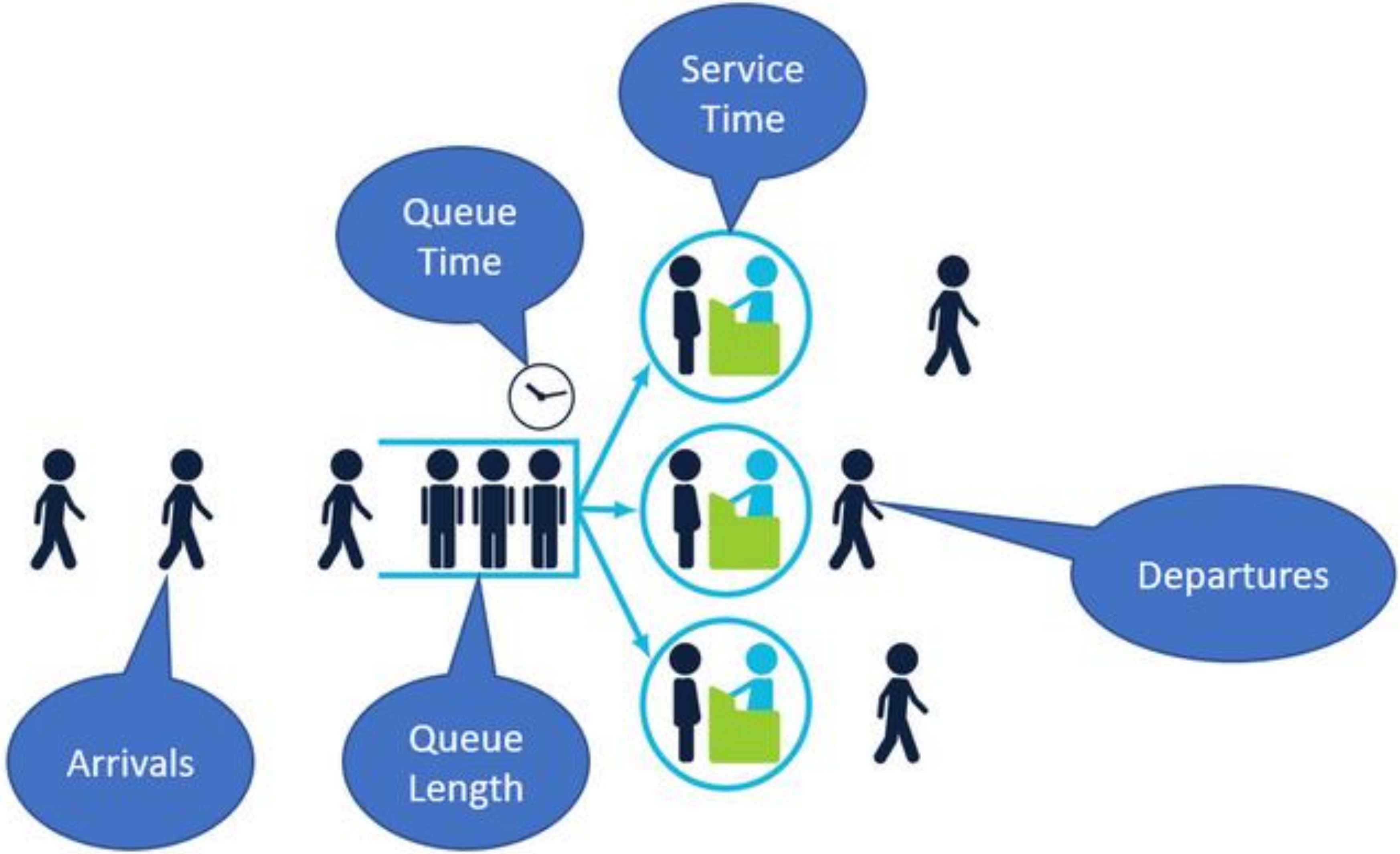
- General case
  - Sending one packet from source to destination
  - Over a path consisting of *N links* each of *rate R*
    - (There are *N-1 routers* between source and destination.)

$$d_{\text{end-to-end}} = N\frac{L}{R}$$

- General case
  - Sending one packet from source to destination
  - Over a path consisting of *N links* each of *rate R*
    - (There are *N-1 routers* between source and destination.)

$$d_{\text{end-to-end}} = N\frac{L}{R}$$

  - What will be the delay for sending P packets over a series of N links?

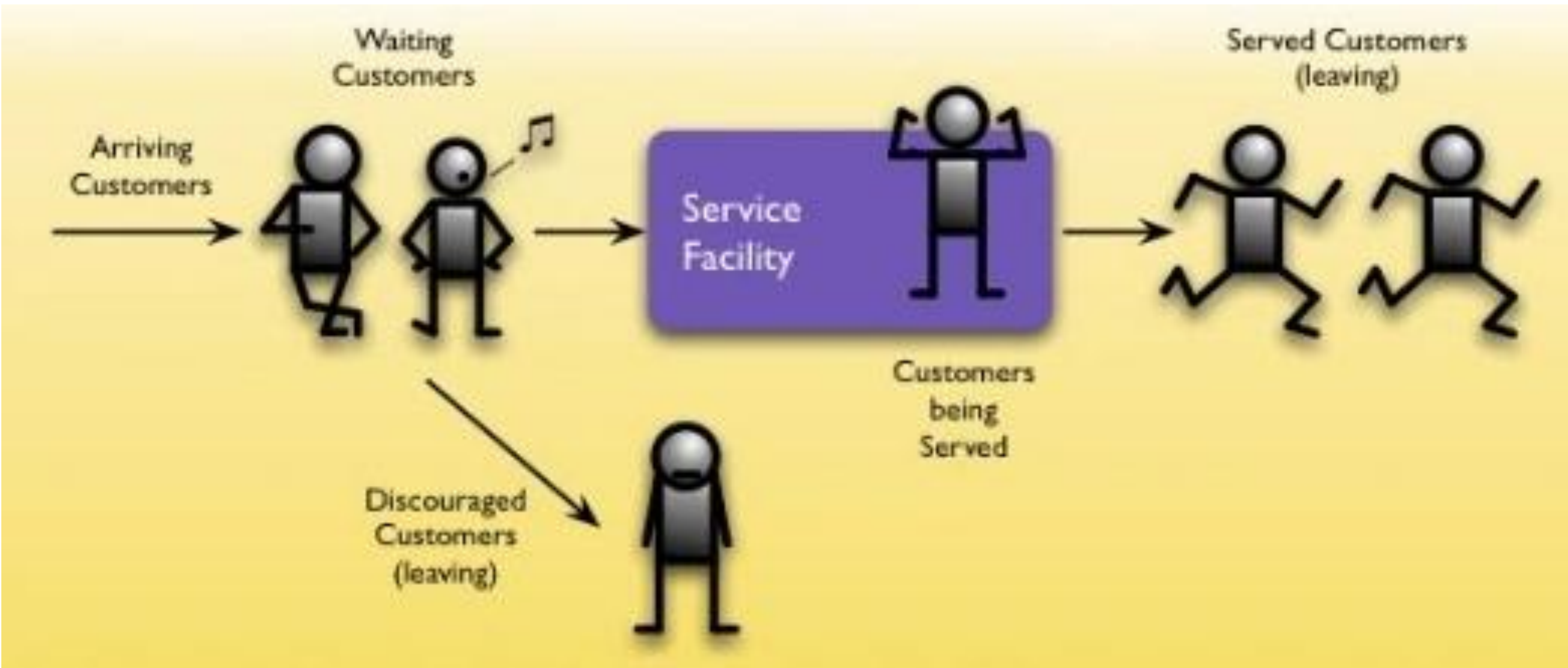

Service Time
Queue Time
Departures
Arrivals
Queue Length

Output Buffer

- Each packet switch has multiple links attached to it.
- For each attached link, the packet switch has an **output buffer (**or **output queue),**
  - which stores packets that the router is about to send into that link.

Queuing Delays

- If an arriving packet, finds the link is busy with the transmission of another packet, the arriving packet must wait in the output buffer.
- Thus, in addition to the store-and-forward delays, packets suffer output buffer **queuing delays.**
- These delays are
  - variable.
  - depend on the level of congestion in the network.



Waiting Customers
Served Customers (leaving)
Arriving Customers
Service Facility
Customers being Served
Discouraged Customers (leaving)

Packet Loss

- The amount of output buffer space is finite
- An arriving packet may find that the buffer is completely full with other packets waiting for transmission.
- In this case, **packet loss** will occur.
  - Packets will be dropped.
    - either the arriving packet
    - or one of the already-queued packets.

Types of Delay

- As a packet travels from one node to another node along a path, the packet suffers from several types of delays at *each node along the path*.
- The most important of these delays are the
  - **Nodal processing delay,**
  - **Queuing delay,**
  - **Transmission delay, and**
  - **Propagation delay.**
- Together, these delays accumulate to give a **total nodal delay**.

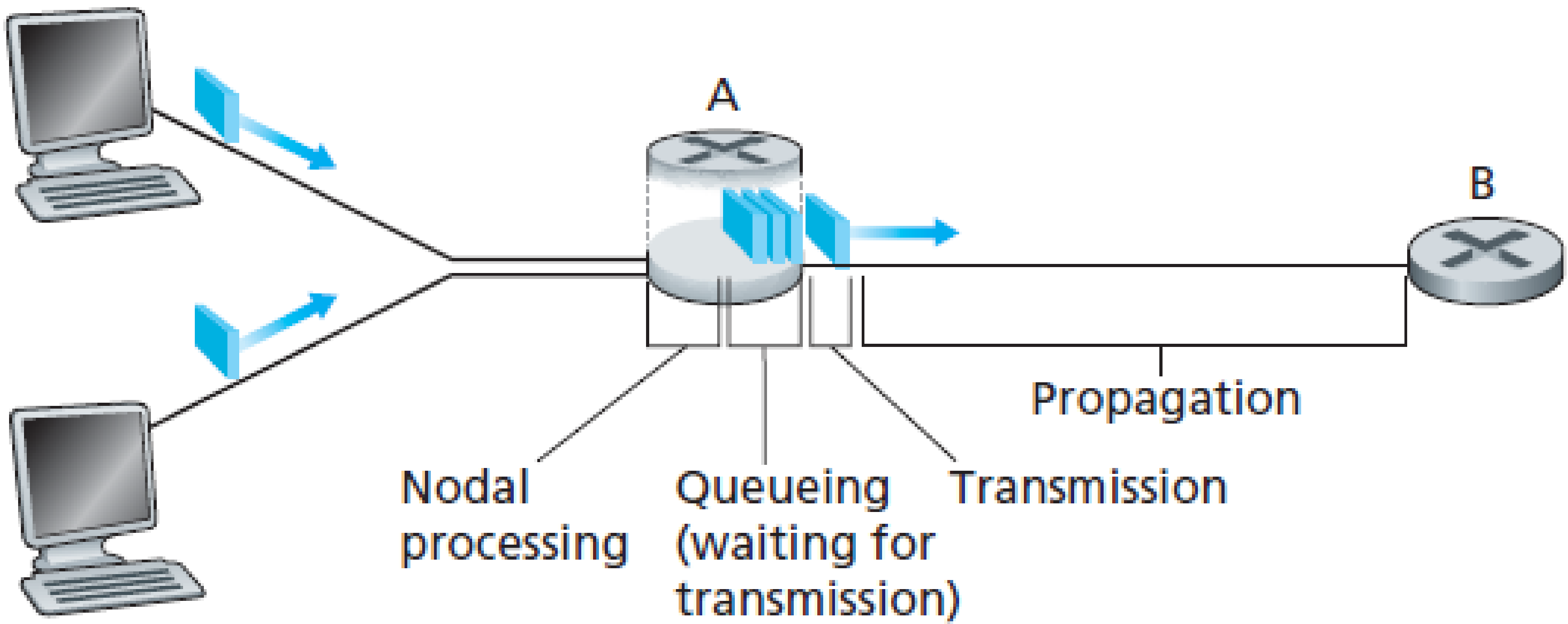


Fig. The nodal delay at router A

Processing Delay

- The time required to
  - examine the packet's header and
  - determine where to direct the packet.
  - check for bit-level errors in the packet that occurred in transmitting from the previous node.
- Processing Delay is microseconds or less in high-speed routers

Queuing Delay

- Time to wait in a queue before transmitted onto the next link.
- Depend on the number of earlier-arriving packets that are queued.
- If the queue is empty, delay will be zero.
- if the traffic is heavy, delay will be long.
- On the order of microseconds to milliseconds.

Transmission Delay

- The transmission delay is ***L/R*.**
  - *This is the amount of time required to push (transmit) all of the packet's* bits into the link.
  - L : length of the packet in bits.
  - R : transmission rate of the link.
- Transmission delays are on the order of microseconds to milliseconds.

Propagation Delay

- The time required to propagate from the beginning of the link to next node.
- The bit propagates at the propagation speed of the link.
- The propagation speed
  - Depends on the physical medium of the link and
  - In the range of $2*10^8$ - 3 $*10^8$ meters/sec
- The propagation delay is the distance between two routers divided by the propagation speed d/s.
  - d : distance between nodes and
  - *s :* propagation speed of the link.

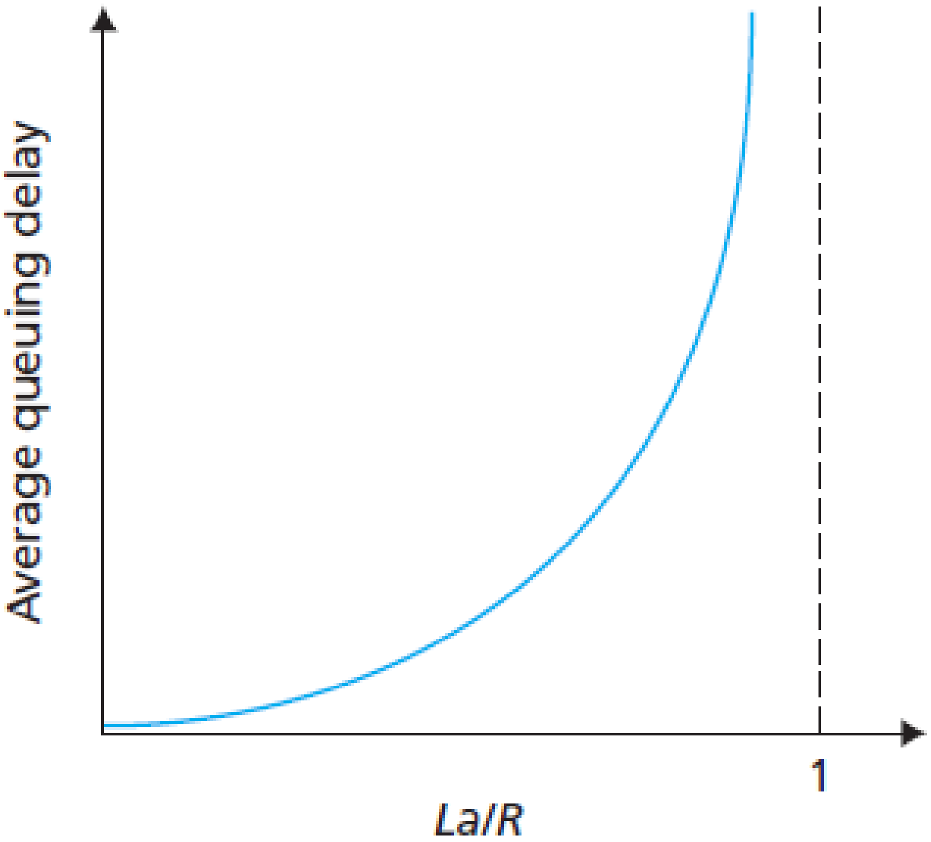
- The total nodal delay is given by

$$d_{\text{nodal}} = d_{\text{proc}} + d_{\text{queue}} + d_{\text{trans}} + d_{\text{prop}}$$

Traffic Intensity

- Let ***a*** denote the average rate at which packets arrive at the queue.
  - in units of *packets/sec.*
- Let **R** is the transmission rate.
  - the rate (in *bits/sec*) at which bits are pushed out of the queue.
- Assume that, all packets consist of ***L*** *bits.*
- The average rate at which bits arrive at the queue is ***La*** *bits/sec.*
- Then the ratio ***La/R****, called the* ***traffic intensity.***

- Case : *La/R > 1*
  - the queuing delay will approach infinity!
- Case : *La/R ≤ 1*
  - if packets arrive periodically—
    - that is, one packet arrives every *L/R seconds*
    - *then every packet will arrive at an empty queue and* there will be no queuing delay.
  - if packets arrive in bursts but periodically,
    - there can be a significant average queuing delay.



- Typically, the arrival process to a queue is *random.*

Example

- Suppose *N packets* arrive simultaneously every *(L/R)N seconds.*
- Then the first packet transmitted has no queuing delay;
- The second packet transmitted has a queuing delay of *L/R seconds;*

•

•

- The nth packet transmitted has a queuing delay of *(n -1)L/R seconds*.

End-to-End Delay

- Let's now consider the total delay from source to destination.
- Suppose there are *N -1 routers* between the source host and the destination host.
- Let's also suppose that the network is uncongested.
- The end-to-end delay for an uncongested network is,

$$d_{\text{end-end}} = N\,(d_{\text{proc}} + d_{\text{trans}} + d_{\text{prop}})$$

Throughput

- Definitions
  - The rate at which a node can forward packets.
  - Throughput at any point in a network is the number of bits passing through the point in a second,
    - which is actually the transmission rate of data at that point.

End-to-end throughput

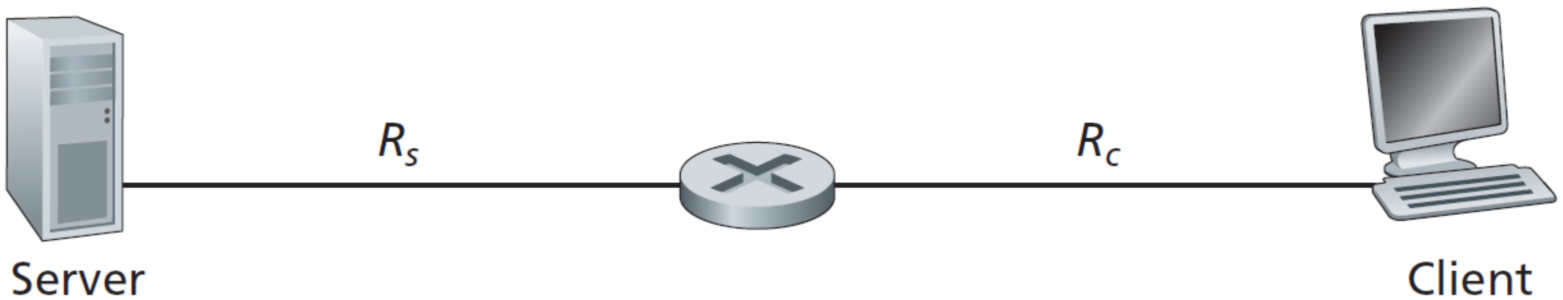
- Consider transferring a large file from Host A to Host B across a computer network.

- The **instantaneous throughput** at any instant of time is the rate(in bits/sec) at which Host B is receiving the file.

- If the file consists of *F* bits and the transfer takes *T* seconds for Host B to receive all F bits, then the **average throughput** of the file transfer is ***F/T*** *bits/sec.*

Example 1

- Consider the throughput for a file transfer from the server to the client.

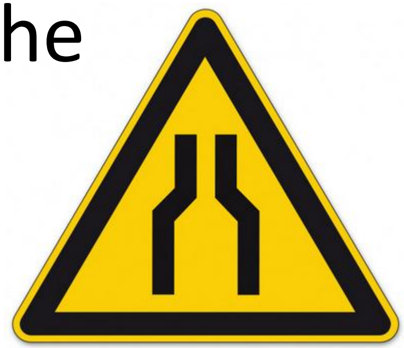


  - R_s - rate of the link between server and router.
  - R_c - rate of the link between router and client.

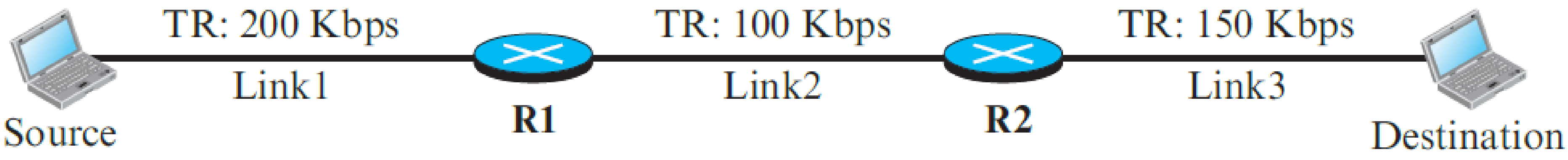
- Scenario
  a) $Rs < Rc$
  b) $Rc < Rs$

- Scenario
  a) $Rs < Rc$
  b) $Rc < Rs$

- Thus, for this simple two-link network, the throughput is min{R_c, R_s},
- That is, it is the transmission rate of the **bottleneck link.**

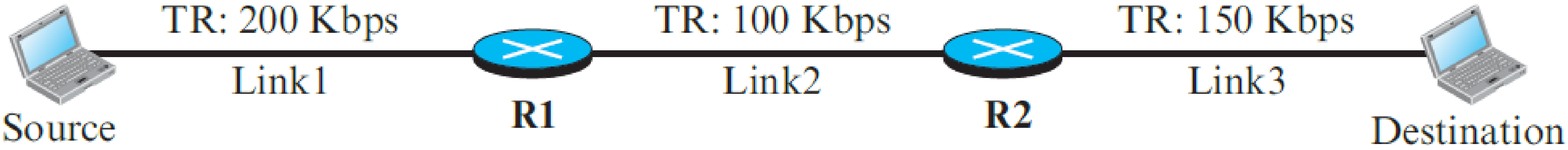


Example 2



TR: 200 Kbps
Link1
TR: 100 Kbps
Link2
TR: 150 Kbps
Link3
Source
R1
R2
Destination

Example 2



a. A path through three links

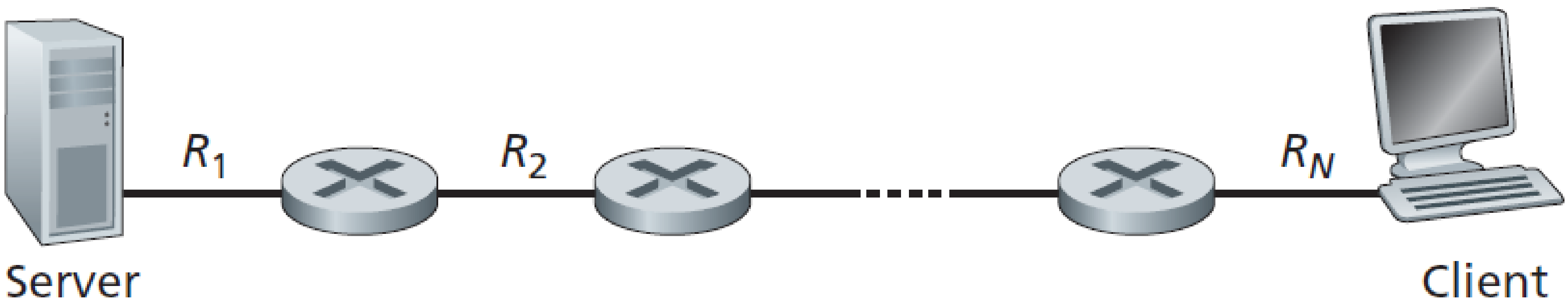
TR: Transmission rate

b. Simulation using pipes

Throughput, T= 100Kbps,
rate of the bottleneck link

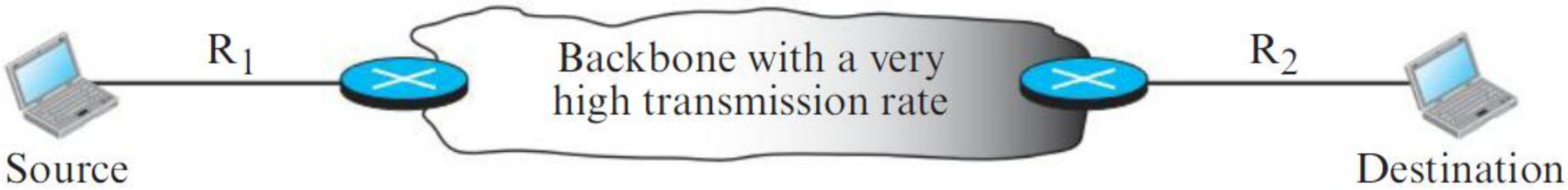
Example 3

- Consider a network with *N links between the server and the* client, with the transmission rates of the *N links being* $R_1, R_2, \ldots, R_N$.



- **Throughput** = **min{$R_1, R_2, \ldots, R_N$}**

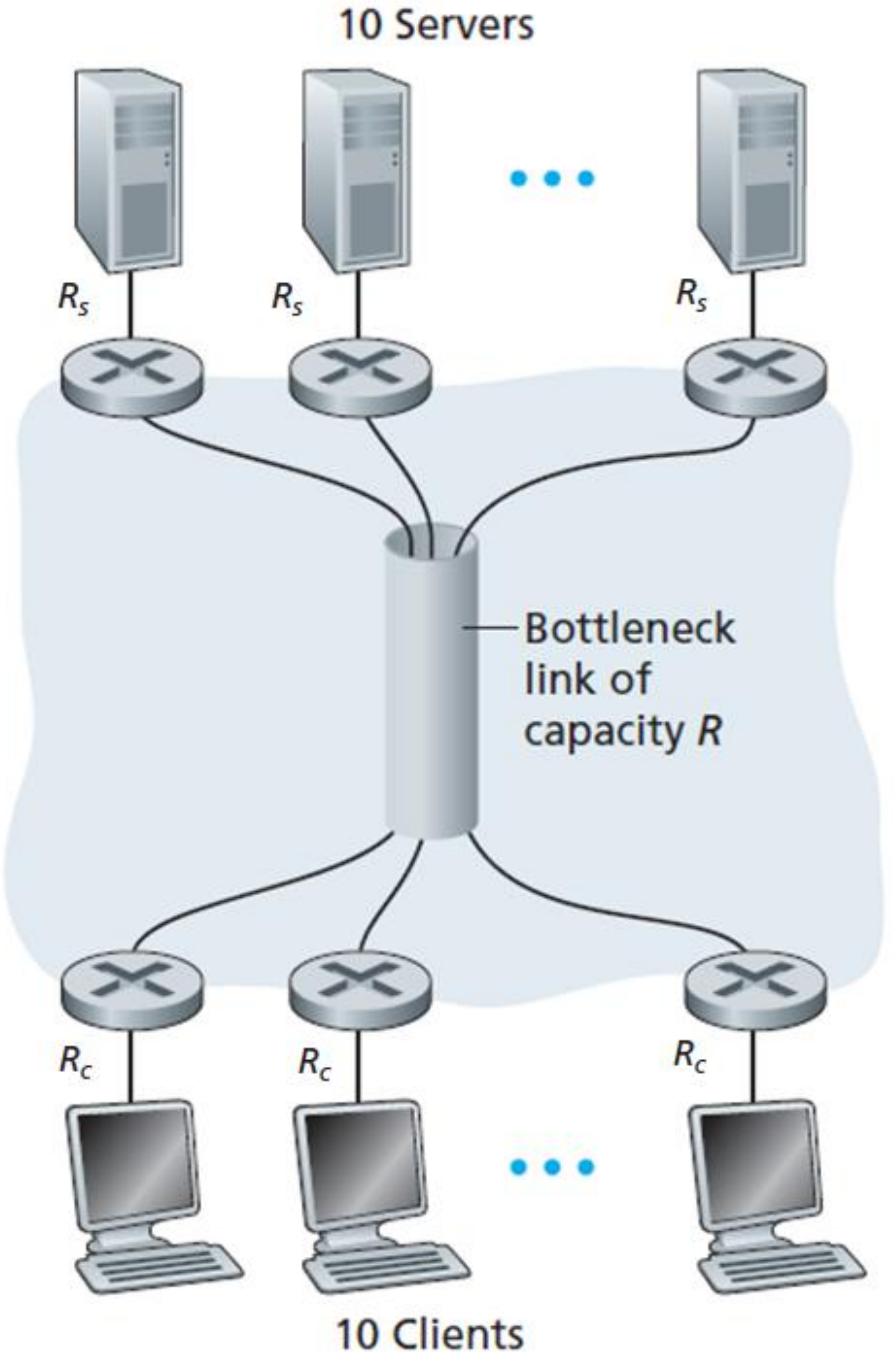
Example 4



What is the throughput here?

- Since the backbone n/w has high transmission rate, throughput depends on rates of end links only.

$$T = \min(R_1, R_2)$$



Example 5

- Throughput?
  - $R >> Rs$ & Rc
    - $T = \min\{Rs, Rc\}$.
  - $R = Rs$ & Rc

- Suppose
  - *Rs = 2 Mbps,*
  - *Rc = 1 Mbps,*
  - *R = 5 Mbps*

  - Find the end-to-end throughput?
    - 10 connections are sharing the link R.
    - Therefore, T=5 Mbps/10.

T = 500 kbps

In a summary…

- Throughput depends
  1. on the transmission rates of the links along the path and
  2. on the intervening traffic.

Protocol Layering

The airline system

- Ticketing agents,
- baggage checkers,
- gate personnel,
- pilots,
- airplanes,
- air traffic control, and
- a worldwide system for routing airplanes

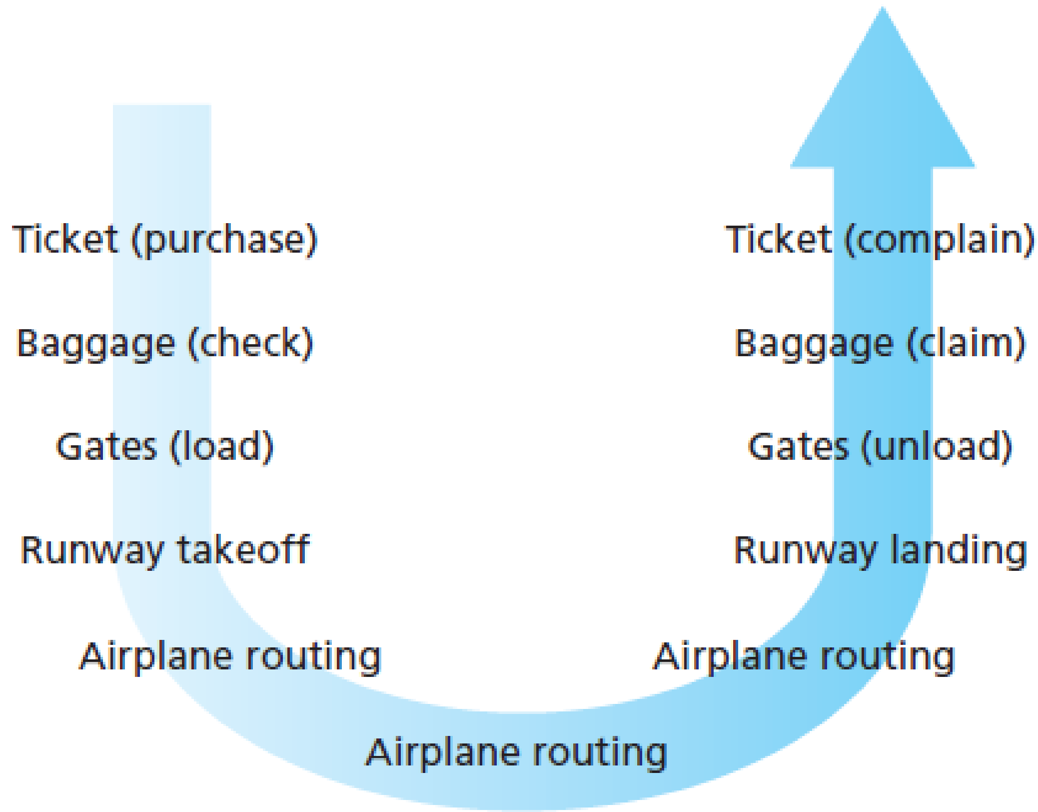


Figure ♦ Taking an airplane trip: actions

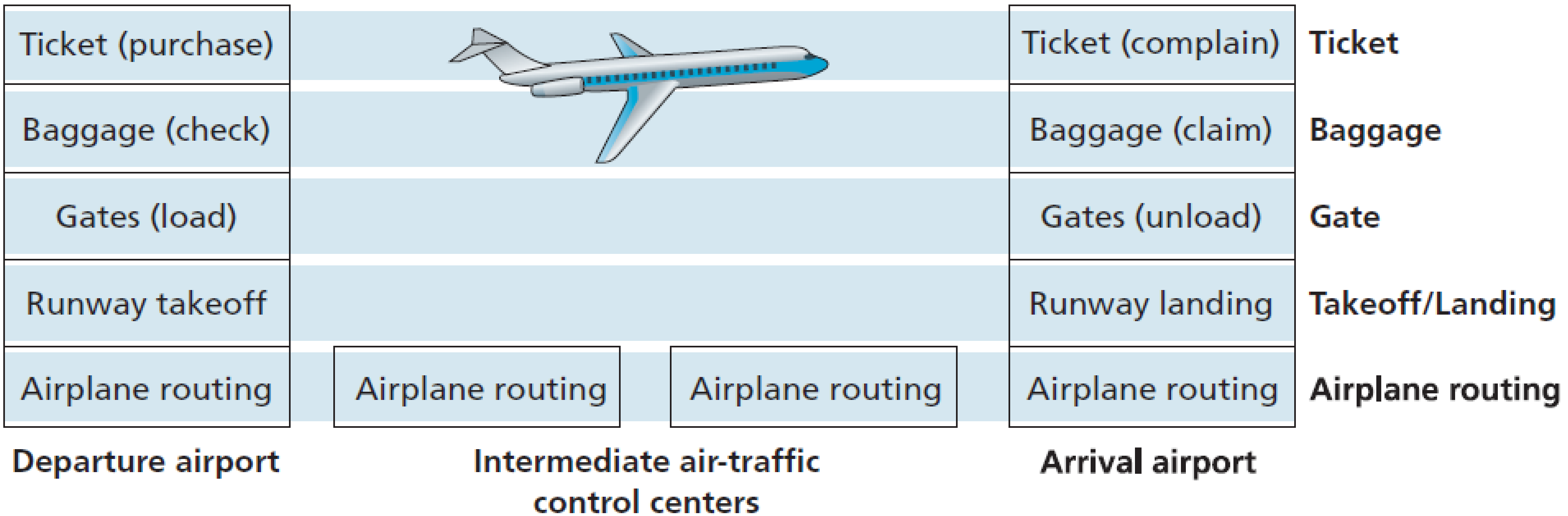


Figure ♦ Horizontal layering of airline functionality

Protocol Layering

Protocol

- defines the rules that both the sender and receiver and all intermediate devices need to follow to be able to communicate effectively.

- When communication is simple,
  - need only one simple protocol.

Protocol layering

- When the communication is complex,
  - divide the task into different layers,
  - need a protocol at each layer,
  - each layer offers a **service**.

Figure: *A single-layer protocol*

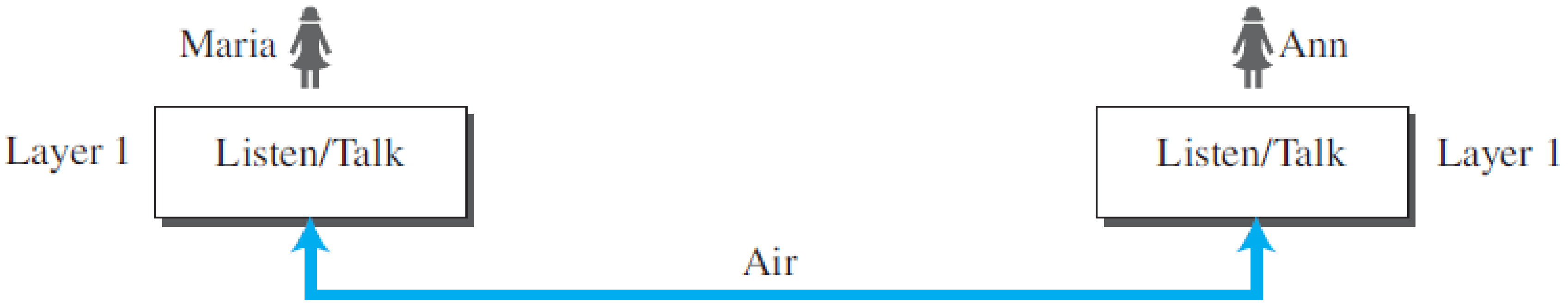
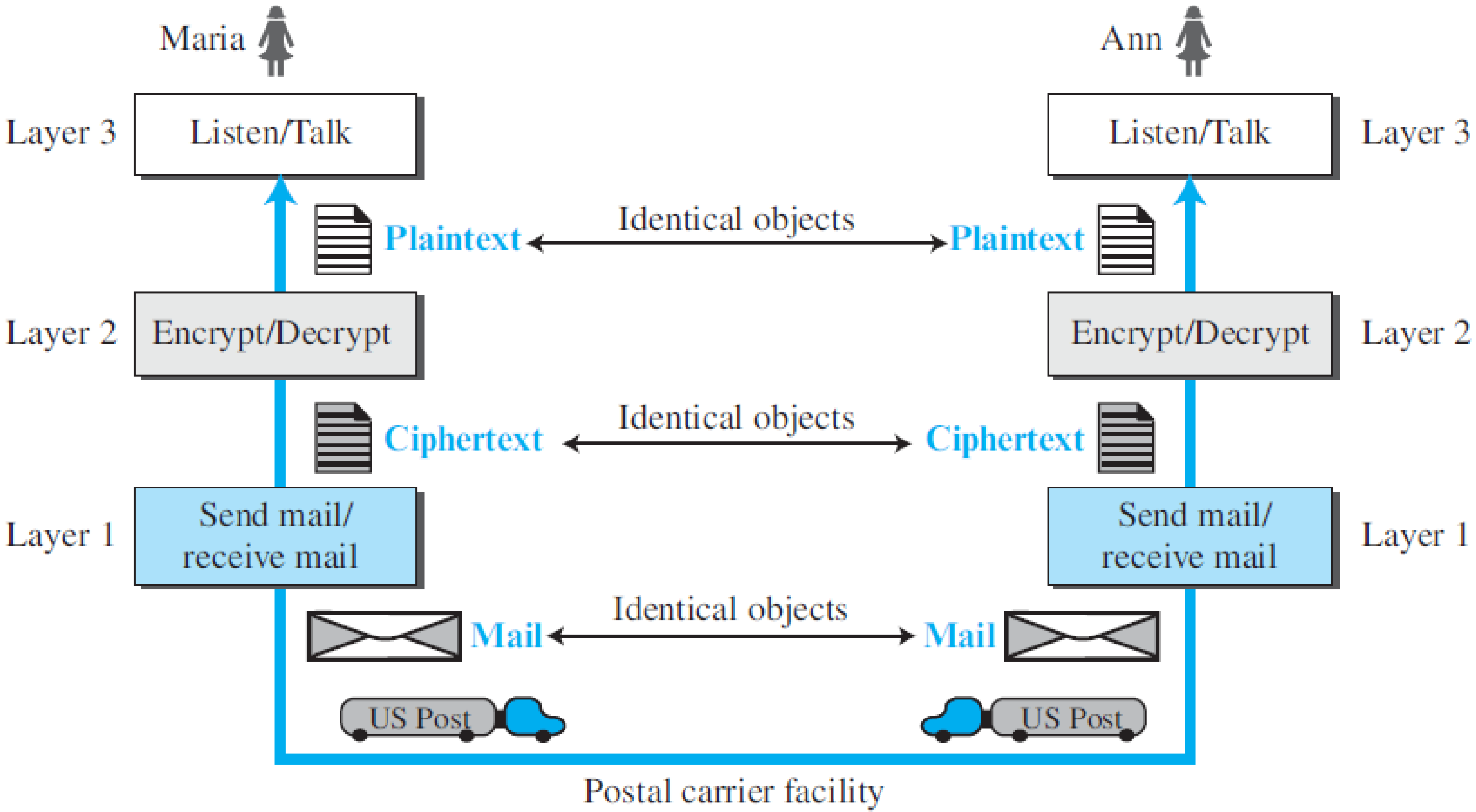


Figure: *A three-layer protocol*



Protocol Layering…

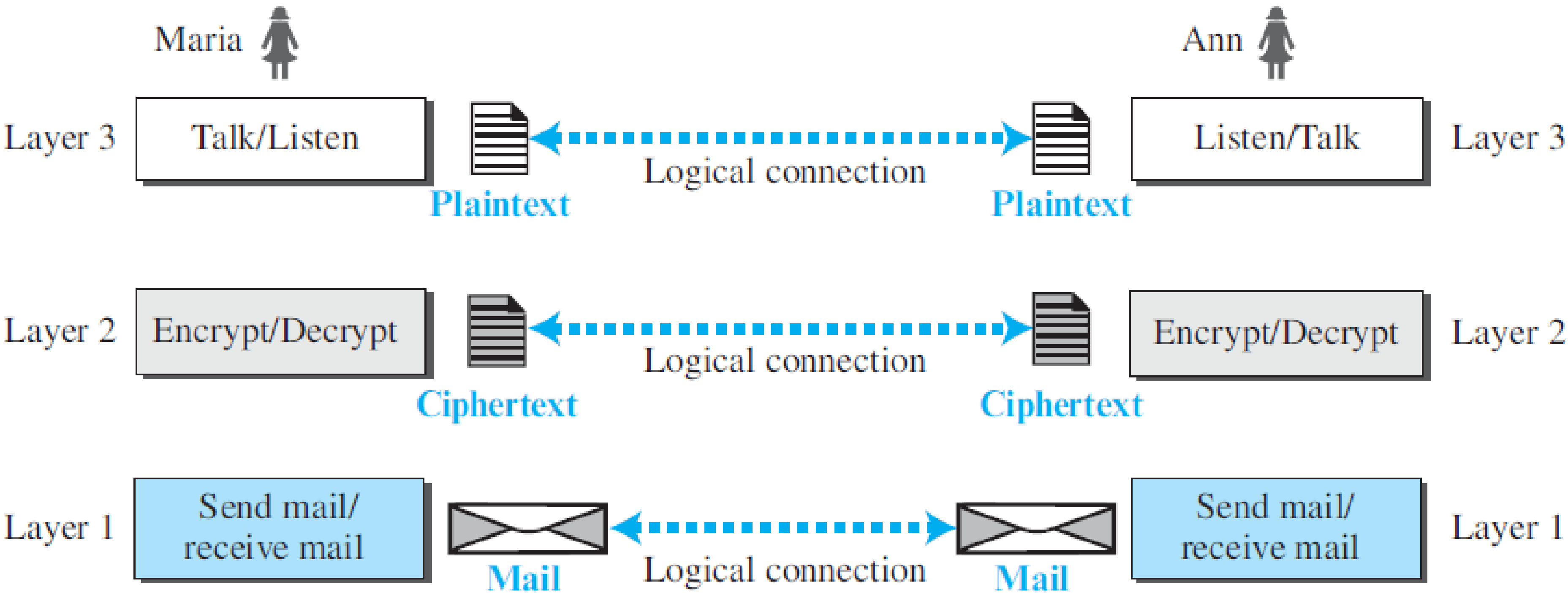
- A protocol layer can be implemented
  - in software,
  - in hardware, or
  - in a combination of the two.

Principles of Protocol Layering

1. If we want bidirectional communication, we need to make each layer so that it is able to perform two opposite tasks, one in each direction.
2. The two objects under each layer at both sites should be identical.

Logical Connections

- There is a logical (imaginary) connection at each layer.



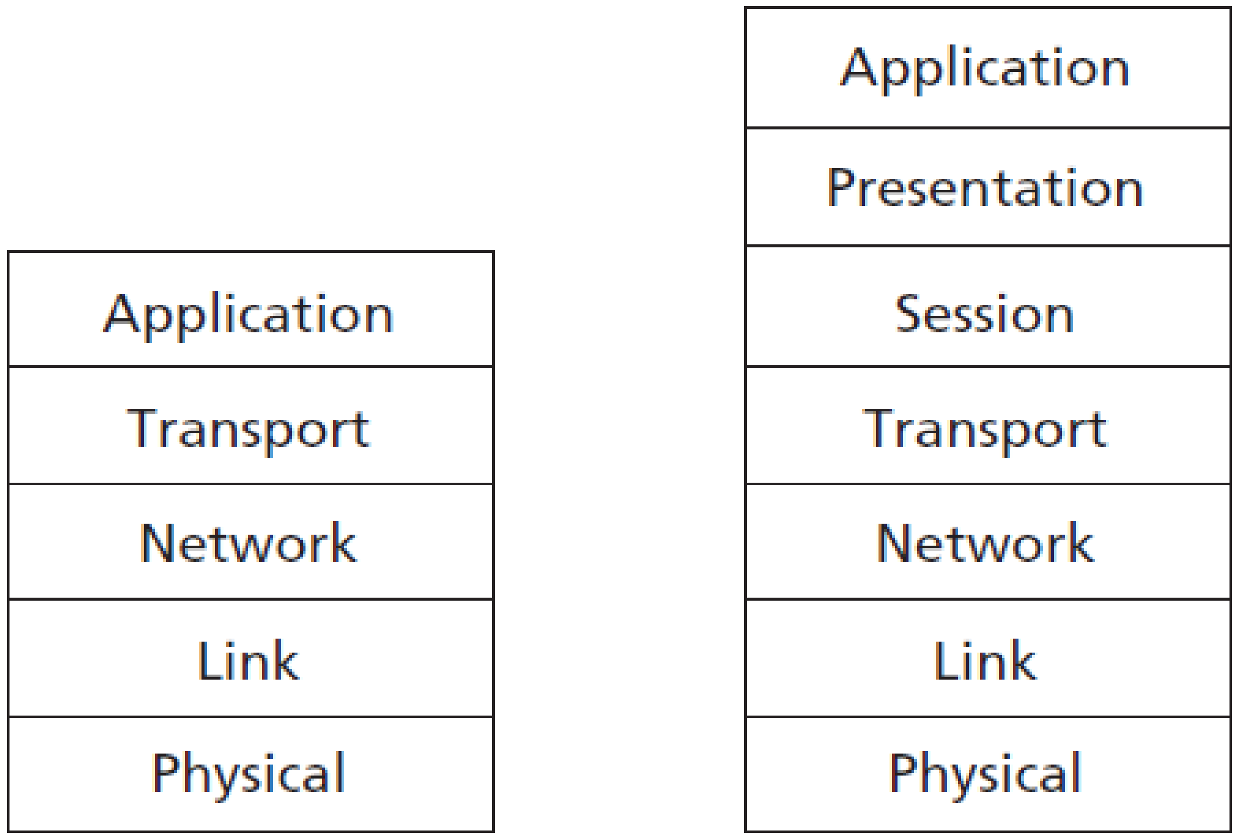
Advantages of protocol layering

- Divide a complex task into several smaller and simpler tasks.
- Gives modularity.
- Separate the services from the implementation.
- Intermediate systems need only some layers.

Drawbacks

1. One layer may duplicate lower-layer functionality.
2. Functionality at one layer may need information that is present only in another layer; this violates the goal of separation of layers.
   – for example, a timestamp value.

Protocol Stack



a. Five-layer Internet protocol stack

b. Seven-layer ISO OSI reference model

TCP/IP Protocol Suite

- TCP/IP (Transmission Control Protocol/Internet Protocol).
- TCP/IP is a protocol suite –
  - A set of protocols organized in different layers.
  - Used in the internet today.
- A hierarchical protocol made up of interactive modules, each of which provides a specific functionality.
  - The term hierarchical means that each upper level protocol is supported by the services provided by one or more lower level protocols.

Figure: *Layers in the TCP/IP protocol suite*

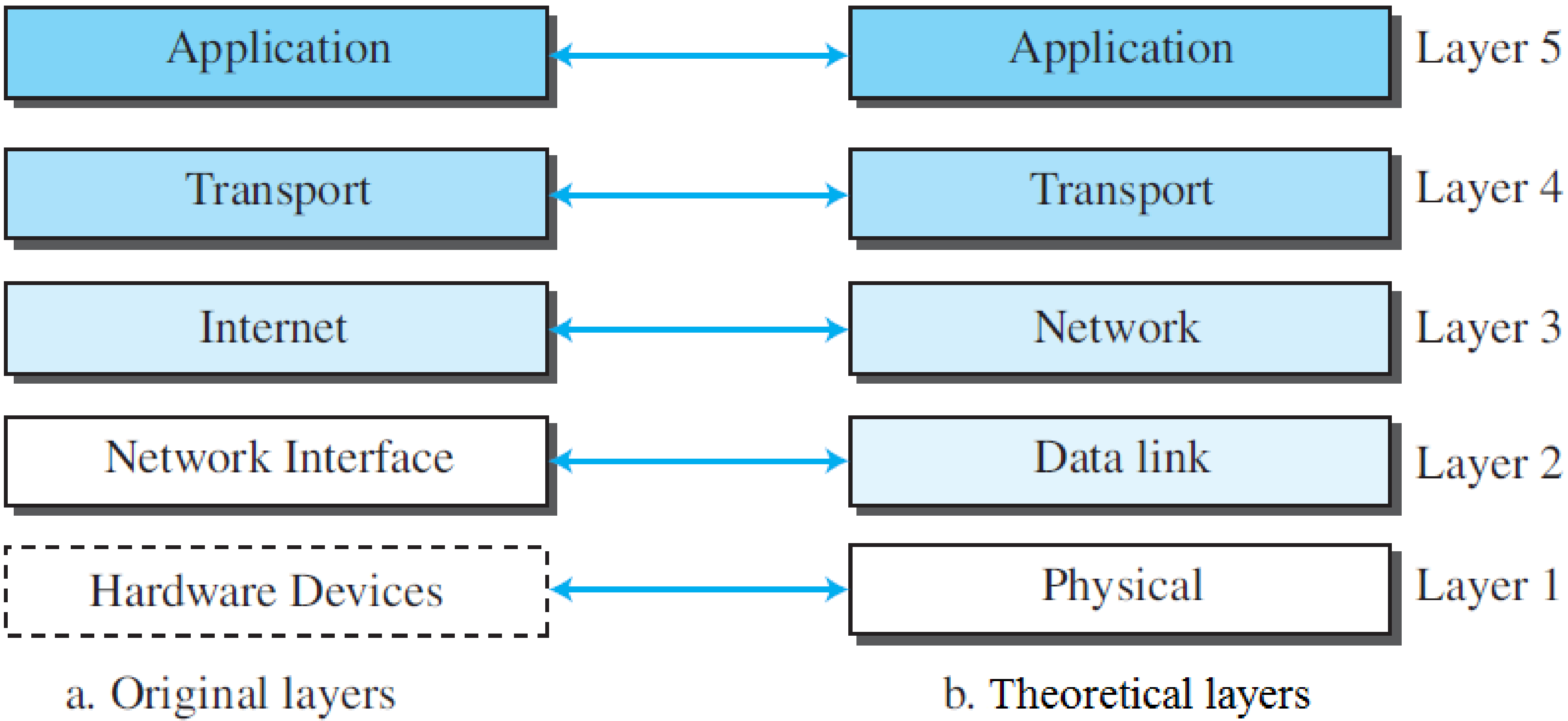
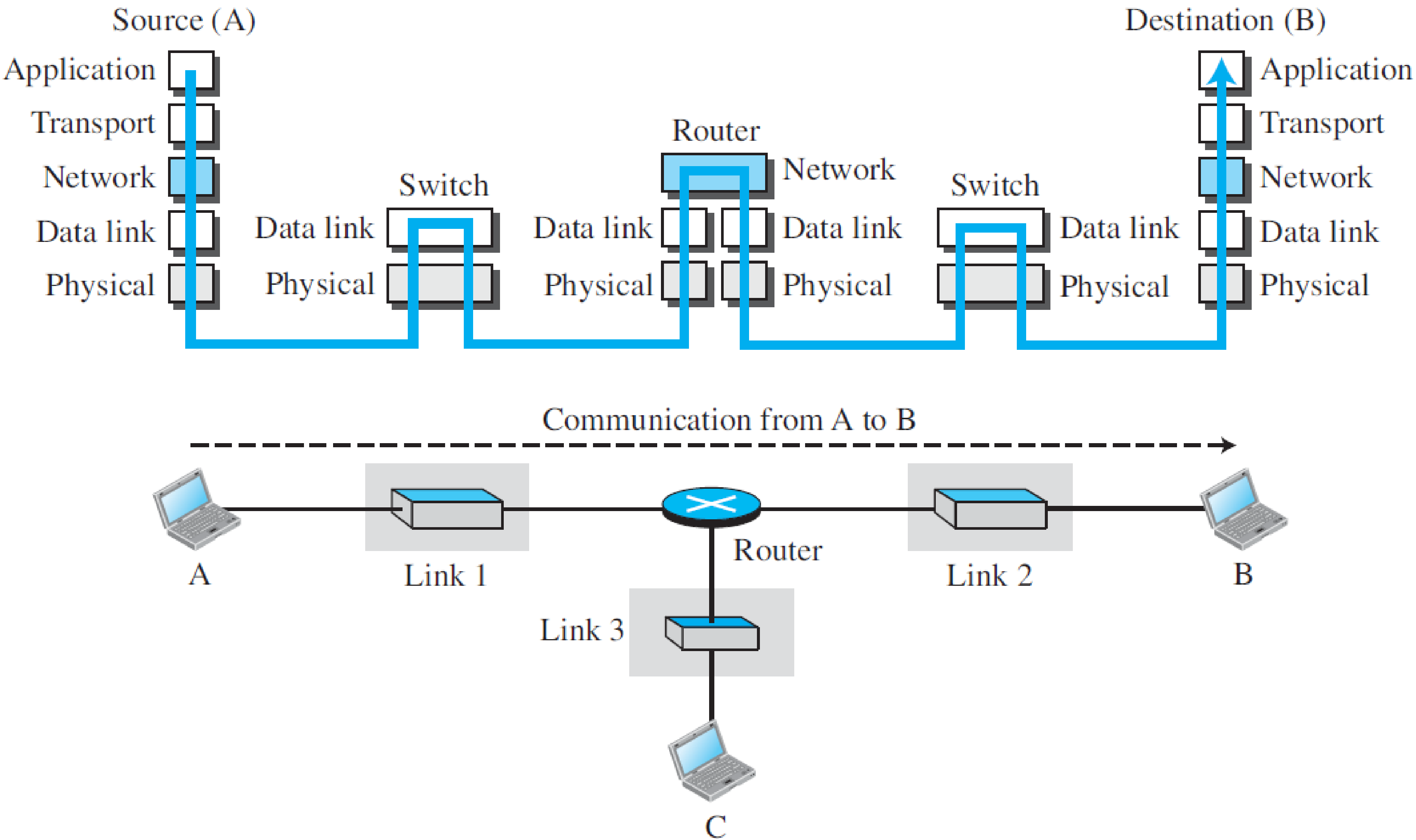


Figure : *Communication through an internet*



- Each device is involved with a set of layers depending on the role of the device in the internet.
- The two hosts are involved in all five layers.
- The router is involved only in three layers.
  - A router is always involved in one network layer.
  - It is involved in n combinations of data link and physical layers in which n is the number of links the router is connected to.
- A link-layer switch in a link is involved only in two layers, data-link and physical.

Figure: *Logical connections between layers of the TCP/IP protocol suite*

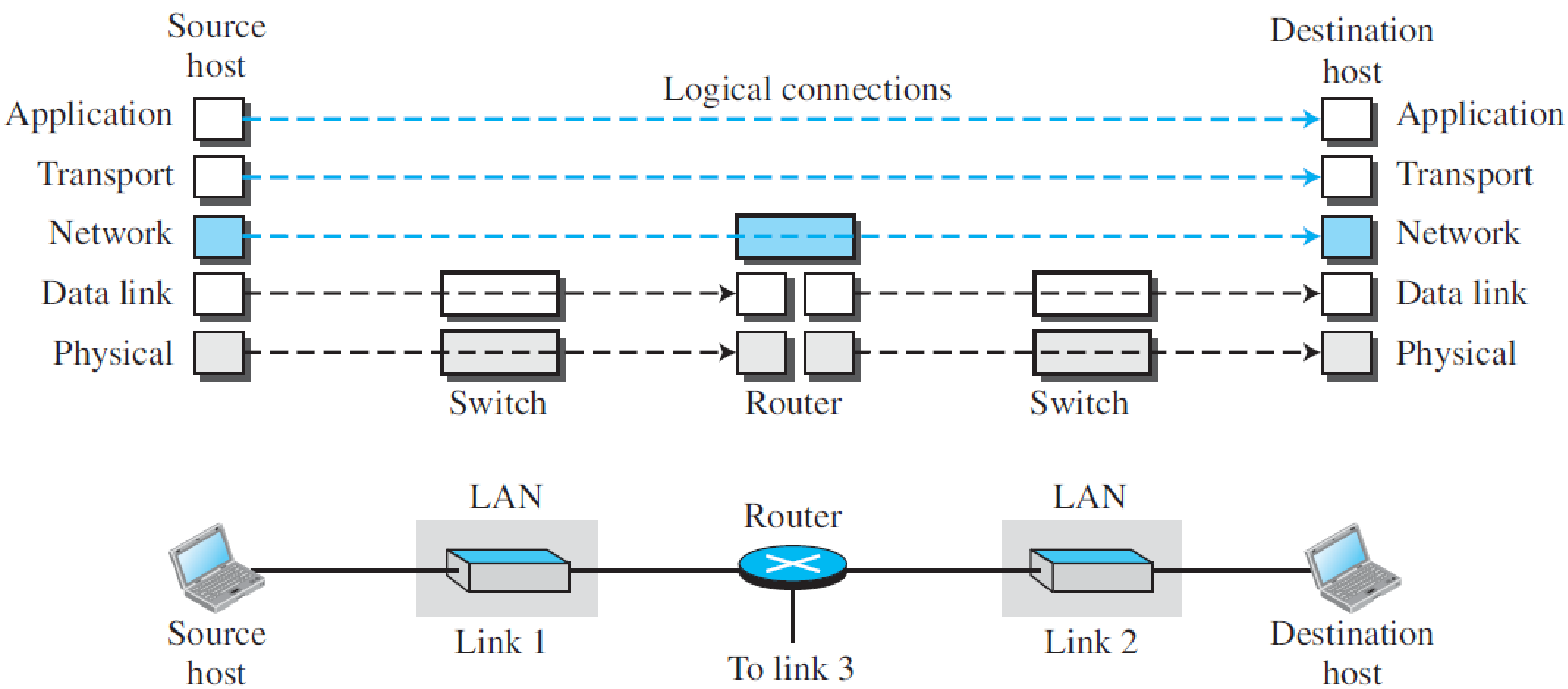
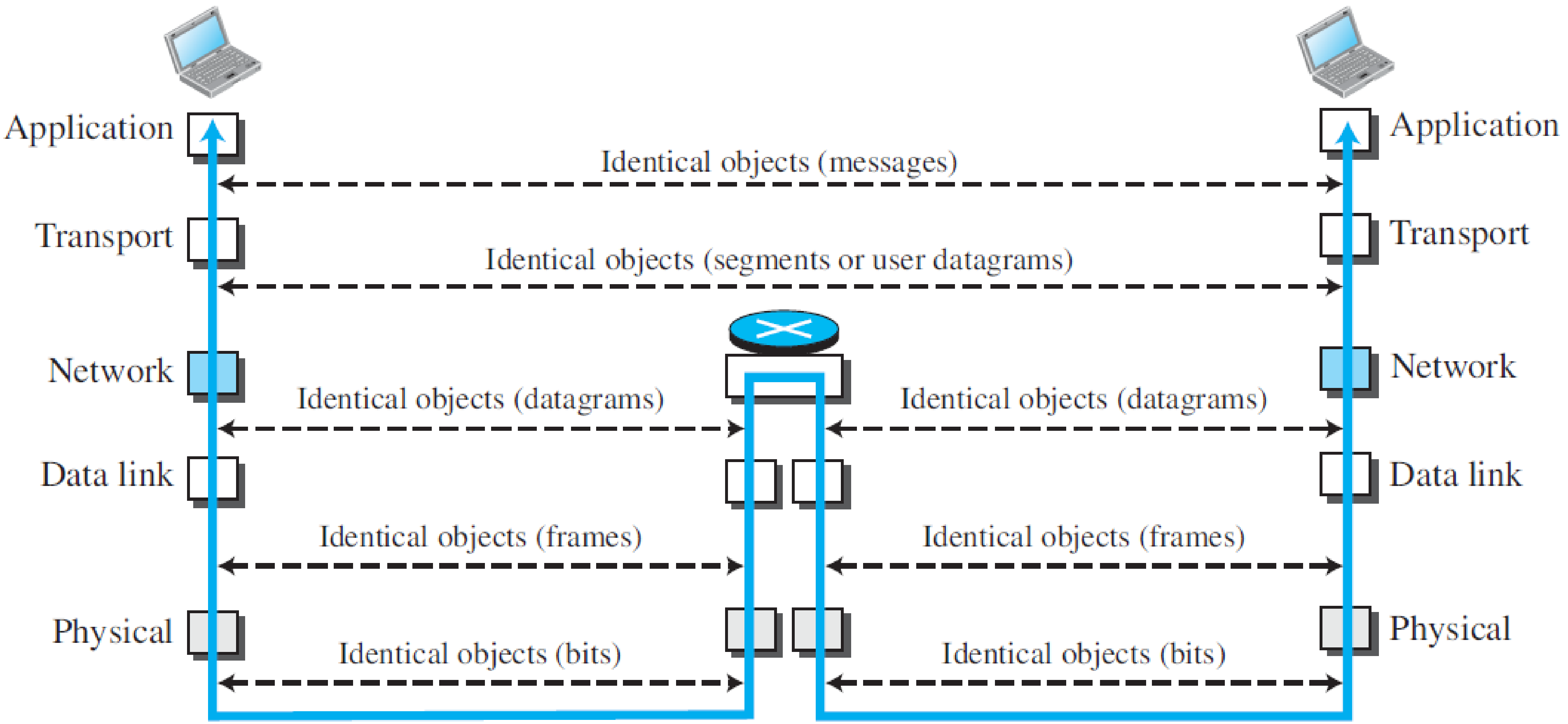


Figure: *Identical objects in the TCP/IP protocol suite*



Application Layer

- The two application layers exchange messages between each other.
- Communication at the application layer is between two processes (two programs running at this layer).
- To communicate, a process sends a request to the other process and receives a response.
- Process-to-process communication is the duty of the application layer.

- Protocols in application layer:
  - The Hypertext Transfer Protocol (HTTP) is a vehicle for accessing the World Wide Web (WWW).
  - Simple Mail Transfer Protocol (SMTP) is the main protocol used in electronic mail (e-mail) service.
  - The File Transfer Protocol (FTP) is used for transferring files from one host to another.
  - The Terminal Network (TELNET) and Secure Shell (SSH) are used for accessing a site remotely.
  - The Simple Network Management Protocol (SNMP) is used by an administrator to manage the Internet at global and local levels.
  - The Domain Name System (DNS) is used by other protocols to find the network-layer address of a computer.
  - The Internet Group Management Protocol (IGMP) is used to collect membership in a group.

Transport Layer

- The logical connection at the transport layer is also end-to-end.
- The transport layer at the source host
  - gets the message from the application layer,
  - encapsulates it in a transport layer packet (called a segment or a user datagram) and
  - sends it, through the logical (imaginary) connection, to the transport layer at the destination host.
- The transport layer is responsible for giving services to the application layer:
  - to get a message from an application program running on the source host and
  - deliver it to the corresponding application program on the destination host.

- Protocols in transport layer:
  - Transmission Control Protocol (TCP)
  - User Datagram Protocol (UDP)
  - Stream Control Transmission Protocol (SCTP)

- Transmission Control Protocol (TCP)
  - Connection-oriented protocol –
    - First establishes a logical connection between transport layers at two hosts before transferring data.
  - TCP provides
    - Flow control - matching the sending data rate of the source host with the receiving data rate of the destination host to prevent overwhelming the destination.
    - Error control - to guarantee that the segments arrive at the destination without error and resending the corrupted ones.
    - Congestion control - to reduce the loss of segments due to congestion in the network.

- <u>User Datagram Protocol (UDP)</u>
  - Connectionless protocol
    - Transmits user datagrams without first creating a logical connection.
  - In UDP, each user datagram is an independent entity without being related to the previous or the next one.
  - UDP is a simple protocol that does not provide flow, error, or congestion control.
  - Small overhead compared to TCP.
  - Used to send short messages and cannot afford the retransmission of the packets when a packet is corrupted or lost.

- <u>Stream Control Transmission Protocol (SCTP)</u>
  - is designed to respond to new applications that are emerging in the multimedia.

Network Layer

- The network layer is responsible for creating a connection between the source computer and the destination computer.
- The communication at the network layer is host-to-host.
- Since there can be several routers from the source to the destination, the routers in the path are responsible for choosing the best route for each packet.
- Network layer is responsible for host-to-host communication and routing the packet through possible routes.

- Protocols in network layer:
  - Internet Protocol (IP)
  - Internet Control Message Protocol (ICMP)
    - helps IP to report some problems when routing a packet.
  - The Internet Group Management Protocol (IGMP)
    - helps IP in multitasking.
  - The Dynamic Host Configuration Protocol (DHCP)
    - helps IP to get the network-layer address for a host.
  - The Address Resolution Protocol (ARP)
    - helps IP to find the link-layer address of a host or a router when its network-layer address is given.

- Internet Protocol (IP)
  - Defines the format of the packet, called a datagram at the network layer.
  - Defines the format and the structure of addresses used in this layer.
  - Responsible for routing a packet from its source to its destination.
  - Connectionless protocol.
  - Includes unicast (one-to-one) and multicast (one-to-many) routing protocols.

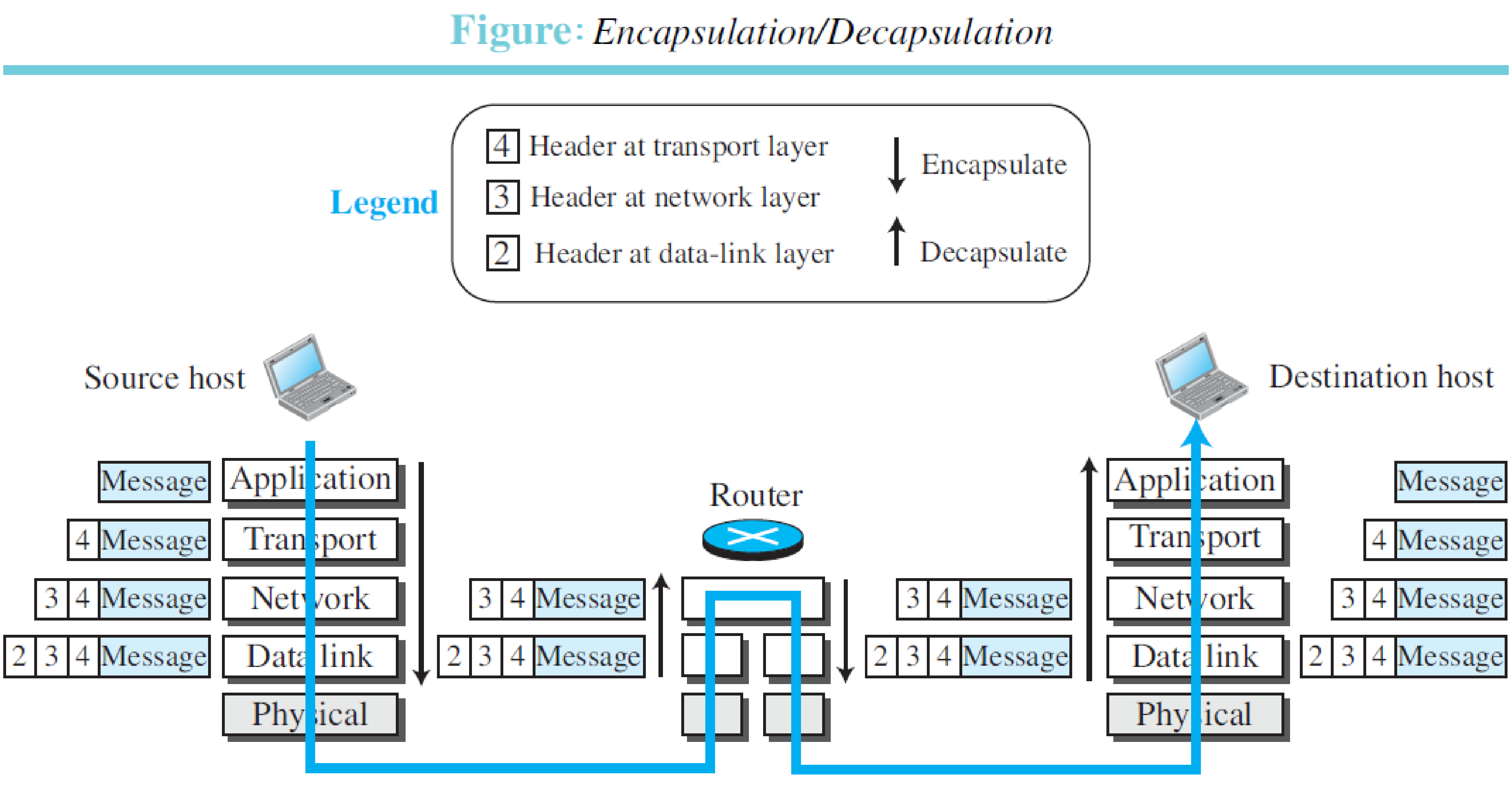
Data-link Layer

- Responsible for taking the datagram and moving it across the link.
- The link can be a wired LAN with a link-layer switch, a wireless LAN, a wired WAN, or a wireless WAN.
  - Different protocols used with different link type.
- The data-link layer takes a datagram and encapsulates it in a packet called a frame.
- Each link-layer protocol may provide a different service.
  - Some link-layer protocols provide complete error detection and correction,
  - Some provide only error correction.

Physical Layer

- Responsible for carrying individual bits in a frame across the link.
- The bits received in a frame from the data-link layer are transformed and sent through the transmission media.
  - Transmission medium does not carry bits; it carries electrical or optical signals.

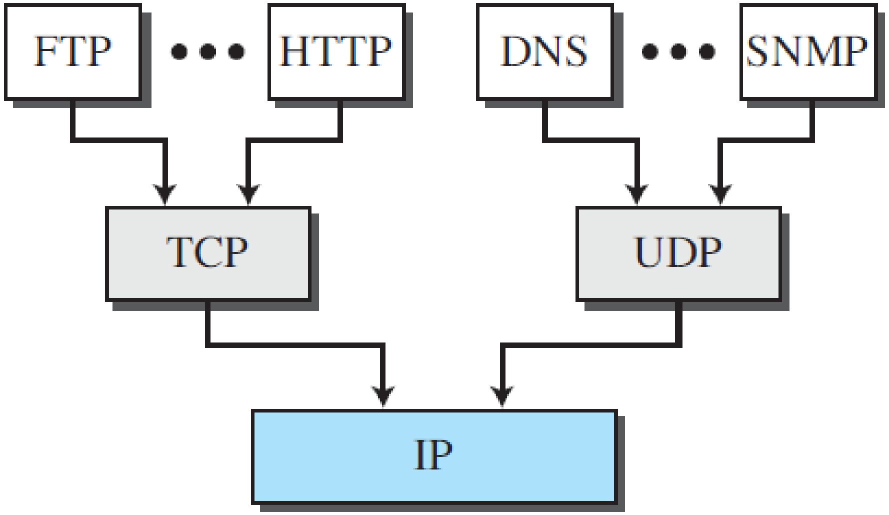
Encapsulation and Decapsulation



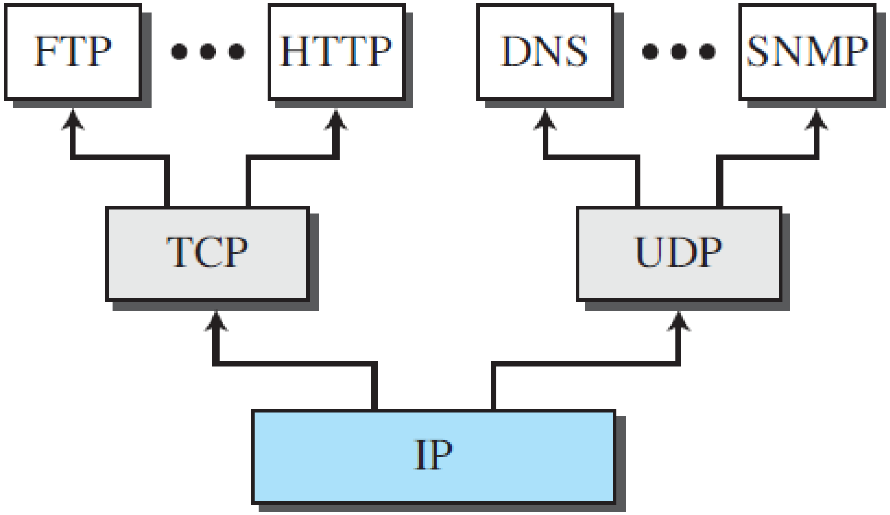
Addressing

Packet names	Layers	Addresses
Message	Application layer	**Names**
Segment / User datagram	Transport layer	**Port numbers**
Datagram	Network layer	**Logical addresses**
Frame	Data-link layer	**Link-layer addresses**
Bits	Physical layer	

Multiplexing and Demultiplexing



a. Multiplexing at source

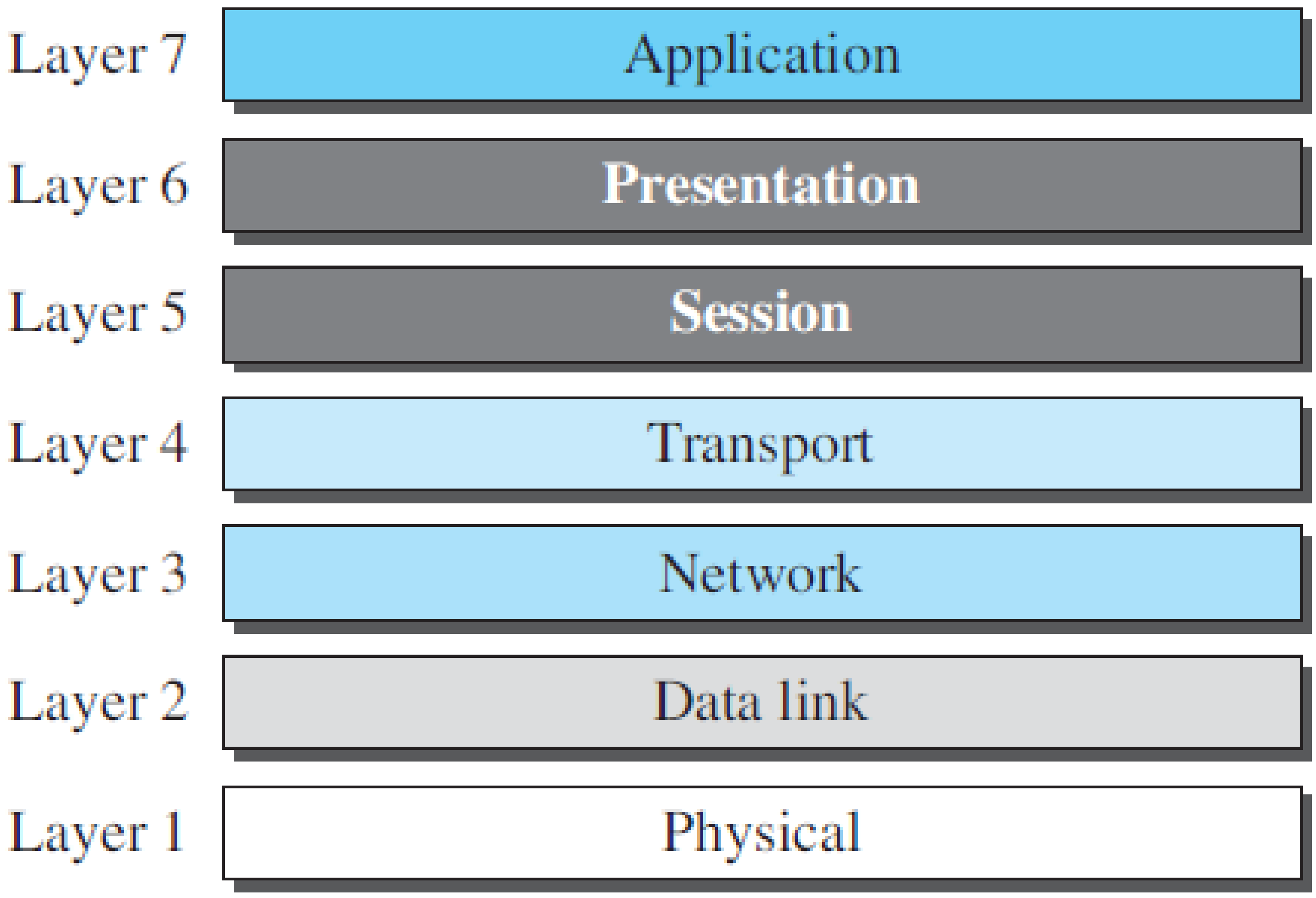


b. Demultiplexing at destination

The OSI Model

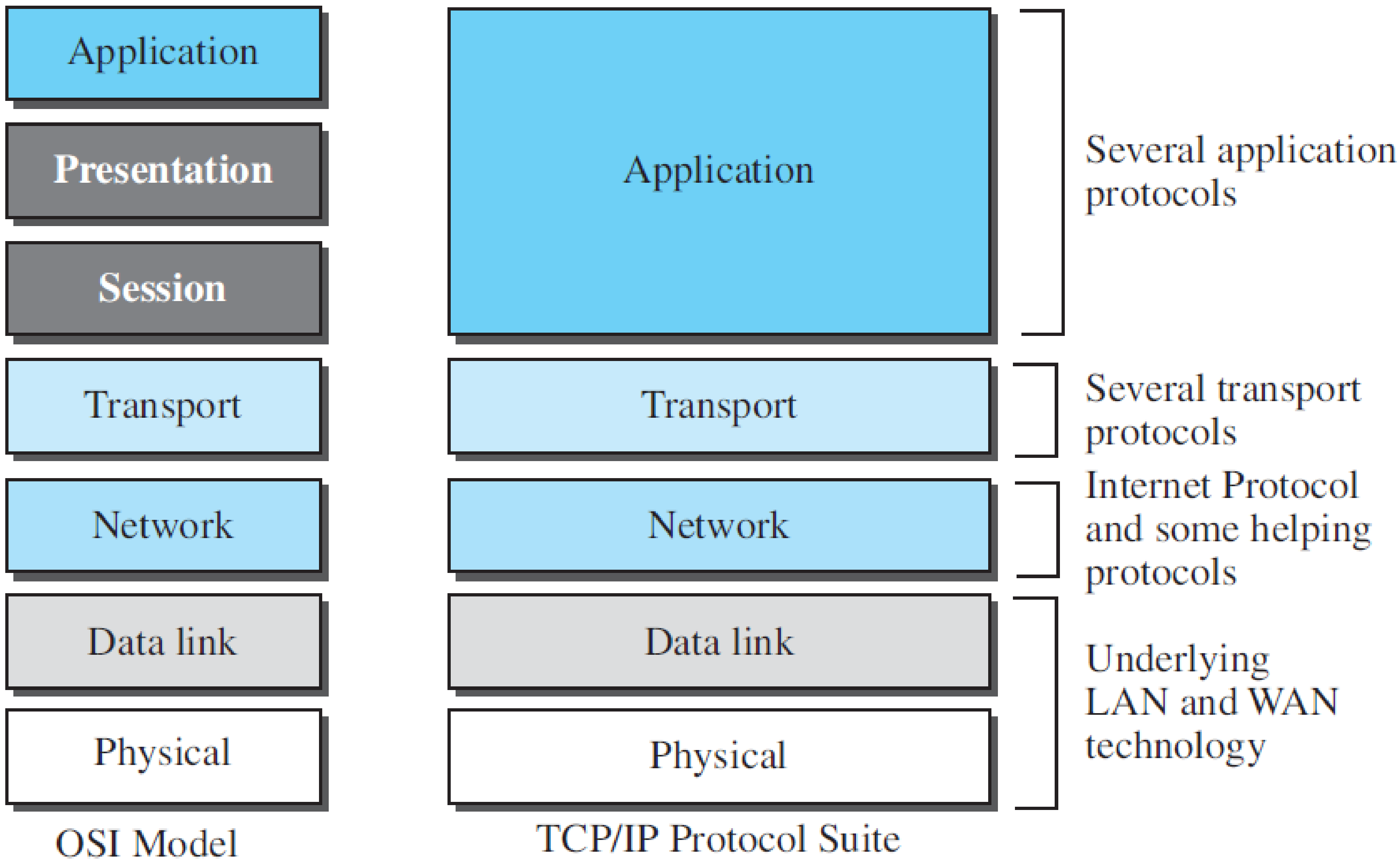
- **An ISO standard that covers all aspects of network communications is the Open Systems Interconnection (OSI) model.**
- It was first introduced in the late 1970s.
- An open system is a set of protocols that allows any two different systems to communicate regardless of their underlying architecture.
- The OSI model is not a protocol.
- It is a model for understanding and designing a network architecture that is flexible, robust, and interoperable.

The OSI Model



Please **D**o **N**ot **T**ake **S**ales **P**ersons **A**dvice

OSI versus TCP/IP



- Consider the two additional layers present in the OSI reference model -
- Presentation Layer
  - Provides services that allow communicating applications to interpret the meaning of data exchanged.
  - These services include
    - Data Compression
    - Data Encryption
    - Data Description
- Session Layer
  - Delimiting and synchronization of data exchange,
  - Building check pointing and recovery scheme.

- Internet lacks two layers found in the OSI reference model.
  - Are the services provided by these layers unimportant?
  - What if an application *needs* one of these services?

It’s up to the application developer.

- To decide if a service is important.
- If the service *is important*, build that functionality into the application.

Lack of OSI Model's Success

1. OSI was completed when TCP/IP was fully in place and a lot of time and money had been spent on the suite; changing it would cost a lot.
2. The presentation and the session layers in the OSI model were never fully defined.
3. Low level of performance.