mood-book

UNIT I

Introduction to Data Communications

- Introduction
- Components,
- Data Representation,
- Data Flow
- Networks-Distributed processing
- Network Criteria
- Physical Structures
- Network Models
- Categories of Networks
- interconnection of Networks
- The internet- A brief History
- The Internet Today
- Protocol and Standards-protocols
- standards, standards Organizations
- **Internet** standards
- network models
- Layered Tasks,
- OSI models,
- Layers in OSI model
- TCP/IP Protocol Suite,
- Addressing
- Introduction,
- Wireless Links and Network Characteristics
- WIFI:802.11
- Wireless LANs-The 802.11 Architecture.

Introduction to Data Communication

In the process of communication, the sharing of information takes place. This sharing can be local or remote. between individuals, local communication usually occurs face to face, while remote communication takes place over distance. The term *telecommunication*, which includes telephony, telegraphy, and television, means communication at a distance *(tele* is Greek for "far").

Note: The word ***data*** refers to information presented in whatever form is agreed upon by the parties creating and using the data.

In Data Communications, data generally are defined as information that is stored in digital form. Data communications is the process of transferring digital information between two or more points. Information is defined as the knowledge or intelligence. Data communications can be summarized as the transmission, reception, and processing of digital information. For data communications to occur, the communicating devices must be part of a communication system made up of a combination of hardware (physical equipment) and software (programs). The effectiveness of a data communications system depends on four fundamental characteristics:

i. Delivery,
ii. Accuracy
iii. Timeliness
iv. Jitter

i. ***Delivery:*** The system must deliver data to the correct destination. Data must be received by the intended device or user and only by that device or user.

ii. ***Accuracy:*** The system must deliver the data accurately. Data that have been altered in transmission and left uncorrected are unusable.

iii. ***Timeliness*****:** The system must deliver data in a timely manner. Data delivered late are useless. In the case of video and audio, timely delivery means delivering data as they are produced, in the same order that they are produced, and without significant delay. This kind of delivery is called *real-time* transmission.

iv Jitter: Jitter refers to the variation in the packet arrival time. It is the uneven delay in the delivery of audio or video packets. For example, let us assume that video packets are sent every 3D ms. If some of the packets arrive with 3D-ms delay and others with 4D-ms delay, an uneven quality in the video is the result.

1. **List and Explain the fundamental characteristics of required for Data Communication Systems.**

Components:

A data communications system has five components

1. ***Message*****:** The message is the information (data) to be communicated. Popular forms of information include text, numbers, pictures, audio, and video.

2. ***Sender*****:** The sender is the device that sends the data message. It can be a computer, workstation, telephone handset, video camera, and so on.

3. Receiver: The receiver is the device that receives the message. It can be a computer, workstation, telephone handset, television, and so on.

4. ***Transmission medium*****:** The transmission medium is the physical path by which a message travels from sender to receiver. Some examples of transmission media include twisted-pair wire, coaxial cable, fiber-optic cable, and radio waves.

5. ***Protocol:*** A protocol is a set of rules that govern data communications. It represents an agreement between the communicating devices. Without a protocol, two devices may be connected but not communicating.

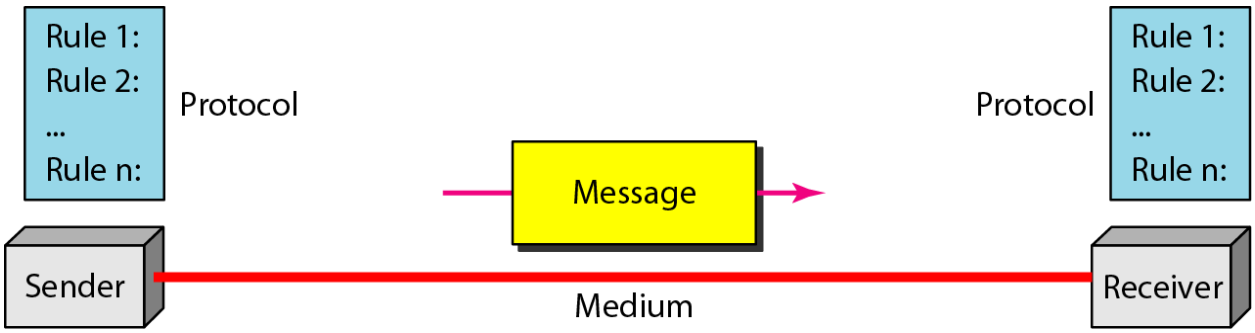


Figure 1: Components of Data Communications

1. With a neat diagram list and explain various components of Data Communication System.

Data Representation:

Information today comes in different forms such as

i. Text,

ii. Numbers,

iii Images,

iv Audio, and

v.Video.

i.Text

In data communications, text is represented as a bit pattern, a sequence of bits (0s or 1s). Different sets of bit patterns have been designed to represent text symbols. Each set is called a code, and the process of representing symbols is called coding. Today, the prevalent coding system is called Unicode, which uses 32 bits to represent a symbol or character used in any language in the world. The American Standard Code for Information Interchange (ASCII), developed some decades ago in the United States, now constitutes the first 127 characters in Unicode and is also referred to as Basic Latin.

ii.Numbers

Numbers are also represented by bit patterns. However, a code such as ASCII is not used to represent numbers; the number is directly converted to a binary number to simplify mathematical operations..

iii.Images

Images are also represented by bit patterns. In its simplest form, an image is composed of a matrix of pixels (picture elements), where each pixel is a small dot. The size of the pixel depends on the *resolution.* For example, an image can be divided into 1000 pixels or 10,000 pixels. In the second case, there is a better representation of the image (better resolution), but more memory is needed to store the image.

After an image is divided into pixels, each pixel is assigned a bit pattern. The size and the value of the pattern depend on the image. For an image made of only black and- white dots (e.g., a chessboard), a 1-bit pattern is enough to represent a pixel. If an image is not made of pure white and pure black pixels, you can increase the size of the bit pattern to include gray scale. For example, to show four levels of gray scale, you can use 2-bit patterns. A black pixel can be represented by 00, a dark gray pixel by 01, a light gray pixel by 10, and a white pixel by 11.

There are several methods to represent color images. One method is called RGB, so called

because each color is made of a combination of three primary colors: *red*, green, and blue. The intensity of each color is measured, and a bit pattern is assigned to it. Another method is called YCM, in which a color is made of a combination of three other primary colors: yellow, cyan, and magenta.

IV. Audio

Audio refers to the recording or broadcasting of sound or music. Audio is by nature different from text, numbers, or images. It is continuous, not discrete. Even when we use a microphone to change voice or music to an electric signal, we create a continuous signal.

V. Video

Video refers to the recording or broadcasting of a picture or movie. Video can either be produced as a continuous entity (e.g., by a TV camera), or it can be a combination of images, each a discrete entity, arranged to convey the idea of motion.

1. **List out the forms of data representation and Explain**

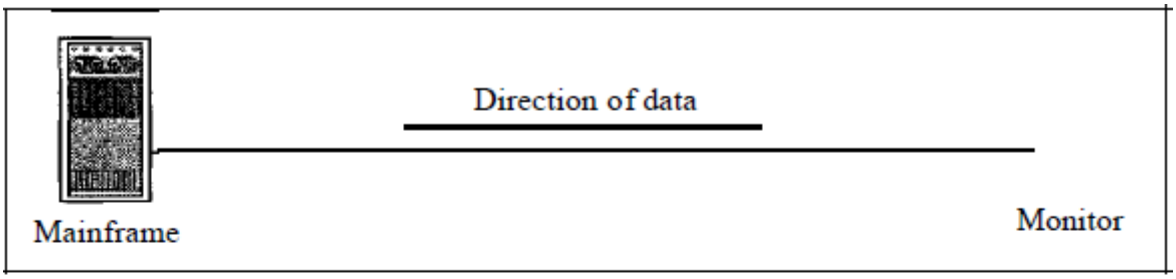
Data Flow:

The Data flow can as following modes

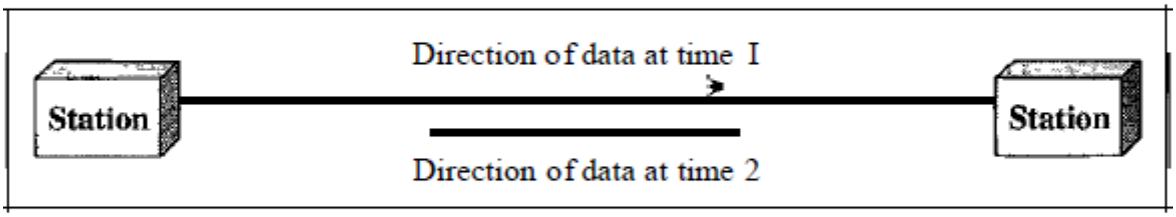
i.simplex,

ii. half-duplex, and

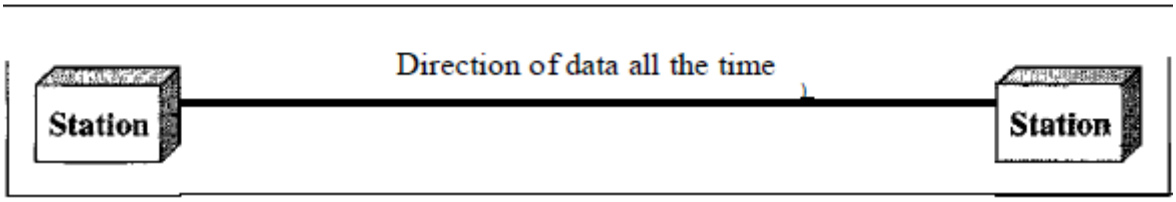
iii. full-duplex)



a. Simplex



b. Half-duplex



c. Full-duplex

i.Simplex

In simplex mode, the communication is unidirectional, as on a one-way street. Only one of the two devices on a link can transmit; the other can only receive. Keyboards and traditional monitors are examples of simplex devices. The keyboard can only introduce input; the monitor can only accept output. The simplex mode can use the entire capacity of the channel to send data in one direction.

ii.Half-Duplex

In half-duplex mode, each station can both transmit and receive, but not at the same time. When one device is sending, the other can only receive, and vice versa.

The half-duplex mode is like a one-lane road with traffic allowed in both directions. When cars are traveling in one direction, cars going the other way must wait.

In a half-duplex transmission, the entire capacity of a channel is taken over by whichever of the two devices is transmitting at the time. Walkie-talkies and CB (citizens band) radios are both half-duplex systems. The half-duplex mode is used in cases where there is no need for communication in both directions at the same time; the entire capacity of the channel can be utilized for each direction.

iii.Full-Duplex

In full-duplex mode, both stations can transmit and receive simultaneously.

The full-duplex mode is like a two-way street with traffic flowing in both directions at the same time. In full-duplex mode, signals going in one direction share the capacity of the link: with signals going in the other direction.

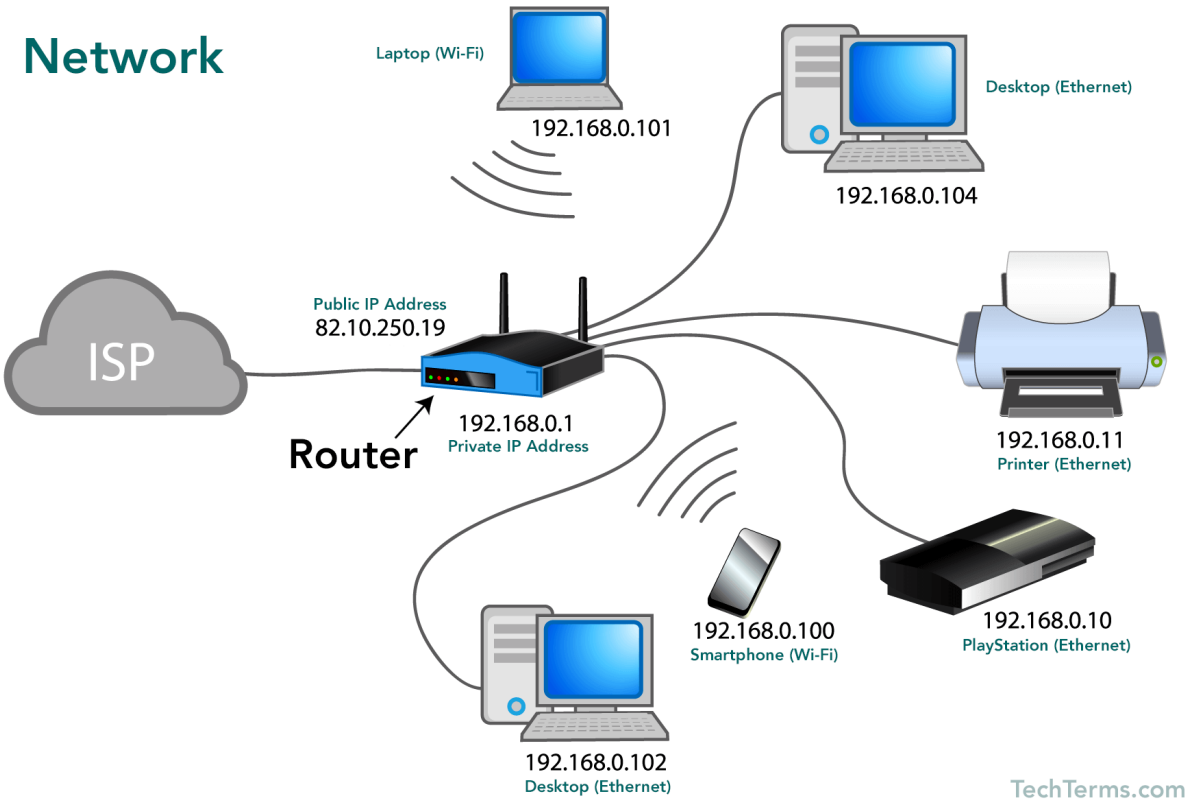
This sharing can occur in two ways: Either the link must contain two physically separate transmission paths, one for sending and the other for receiving; or the capacity of the channel is divided between signals traveling in both directions.

One common example of full-duplex communication is the telephone network. When two people are communicating by a telephone line, both can talk and listen at the same time.

1. **Mention and explain the various data flow methods with examples**

NETWORKS:

Definition: A network is a set of devices (often referred to as *nodes)* connected by communication links. A node can be a computer, printer, or any other device capable of sending and/or receiving data generated by other nodes on the network.



Distributed Processing

Most networks use distributed processing, in which a task is divided among multiple computers. Instead of one single large machine being responsible for all aspects of a process, separate computers (usually a personal computer or workstation) handle a subset.

1. **Define network and give diagrammatic representation of network**
2. **What is network and explain distributed processing used in networks.**

NETWORK CRITERIA:

A network must be able to meet a certain number of criteria. The most important of these are

i. Performance,
ii. Reliability, and
iii. Security.

i. Performance

Performance can be measured in many ways, including transit time and response time. Transit time is the amount of time required for a message to travel from one device to another. Response time is the elapsed time between an inquiry and a response. The performance of a network depends on a number of factors, including the number of users, the type of transmission medium, the capabilities of the connected hardware, and the efficiency of the software.

Performance is often evaluated by two networking metrics: throughput and delay.
We often need more throughput and less delay. However, these two criteria are often contradictory. If we try to send more data to the network, we may increase throughput but we increase the delay because of traffic congestion in the network.

ii. Reliability

In addition to accuracy of delivery, network reliability is measured by the **frequency of failure**, the time it takes a link to recover from a failure, and the network's robustness in a catastrophe.

iii. Security

Network security issues include protecting data from unauthorized access, protecting data from damage and development, and implementing policies and procedures for recovery from breaches and data losses.

1. **Discuss the important criterions a network should meet.**

PHYSICAL STRUCTURES:

The following are the network attributes.

i. Type of Connection

A network is two or more devices connected through links. A link is a communications pathway that transfers data from one device to another. For visualization purposes, it is simplest to imagine any link as a line drawn between two points. For communication to occur, two devices must be connected in some way to the same link at the same time. There are two possible types of connections: point-to-point and multipoint.

a. Point-to-Point A point-to-point connection provides a dedicated link between two devices. The entire capacity of the link is reserved for transmission between those two devices. Most point-to-point connections use an actual length of wire or cable to connect the two ends, but other options, such as microwave or satellite links, are also possible.

Example : changing of television channels by infrared remote control, by this a point-to-point connection between the remote control and the television's control system is established.

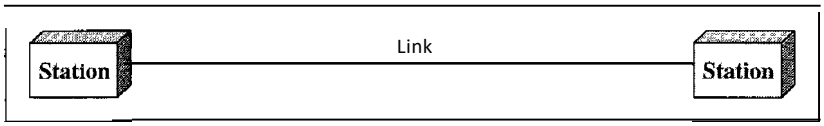


Figure : Point to Point Connection

b. Multipoint: A multipoint (also called multidrop) connection is one in which more than two specific devices share a single link . In a multipoint environment, the capacity of the channel is shared, either spatially or temporally. If several devices can use the link simultaneously, it is a *spatially shared* connection. If users must take turns, it is a *timeshared* connection.

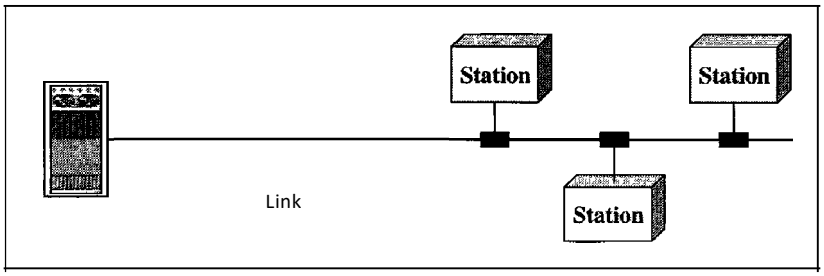


Figure : A Multipoint Connection

ii. Physical Topology

The term *physical topology* refers to the way in which a network is laid out physically or more devices connect to a link; two or more links form a topology. The topology of a network is the geometric representation of the relationship of all the links and linking devices (usually called nodes) to one another. There are four basic topologies possible:

a. Mesh, b. Star, c. Bus, and d. Ring.

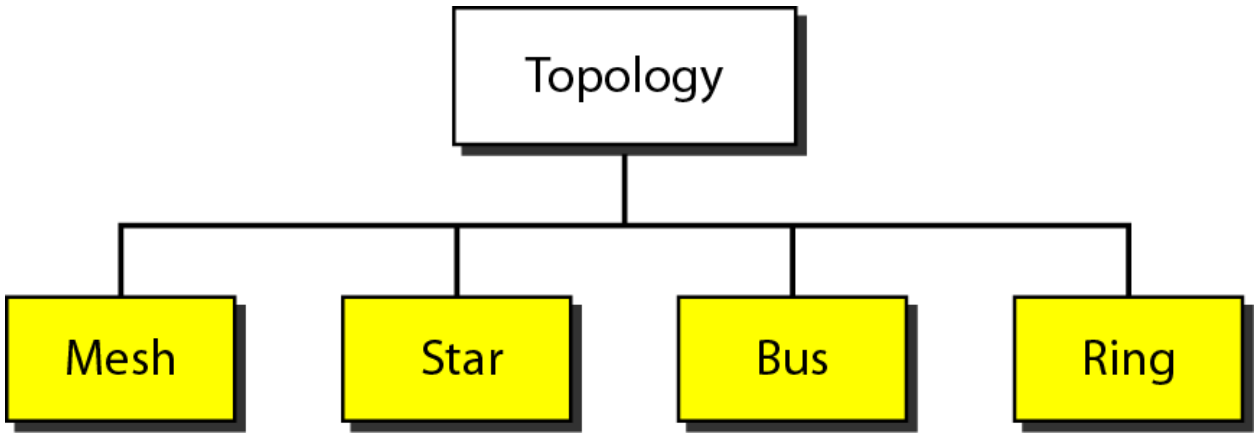


Figure: The categories of topology

a. Mesh: In a mesh topology, every device has a dedicated point-to-point link to every other device. The term *dedicated* means that the link carries traffic only between the two devices it connects. To find the number of physical links in a fully connected mesh network with *n* nodes, we first consider that each node must be connected to every other node. Node 1 must be connected to *n* - I nodes, node 2 must be connected to *n* - 1 nodes, and finally node *n* must be connected to *n* - 1 nodes. We need *n*(*n* - 1) physical links. However, if each physical link allows communication in both directions (duplex mode), we can divide the number of links by 2. In other words, we can say that in a mesh topology, we need *n*(*n* -1) /2 duplex-mode links.

To accommodate that many links, every device on the network must have *n* - 1 input/output *(VO)* ports to be connected to the other *n* - 1 stations.

A mesh offers several **advantages** over other network topologies. First, the use of **dedicated links** guarantees that each connection can carry its own data load, thus eliminating the traffic problems that can occur when links must be shared by multiple devices. Second, a mesh topology is **robust**. If one link becomes unusable, it does not incapacitate the entire system.

Third, there is the advantage of privacy or security. When every message travels along a dedicated line, only the intended recipient sees it. Physical boundaries prevent other users from gaining access to messages. Finally, **point-to-point links make** fault identification and fault isolation easy. Traffic can be routed to avoid links with suspected problems. This facility enables the network manager to discover the precise location of the fault and aids in finding its cause and solution.

Disadvantages

The main disadvantages of a mesh are related to the **amount of cabling and the number of I/O ports** required. First, because every device must be connected to every other device, installation and reconnection are difficult. Second, the **sheer bulk of the wirin**g can be greater than the available space (in walls, ceilings, or floors) can accommodate. Finally, the **hardware required to connect each link** (I/O ports and cable) can be prohibitively expensive. For these reasons a mesh topology is usually implemented in a limited fashion, for example, as a backbone connecting the main computers of a hybrid network that can include several other topologies.

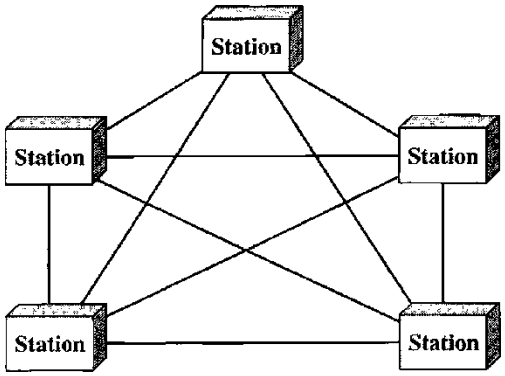


Figure: A fully connected mesh topology (five devices)

One practical example of a mesh topology is the connection of telephone regional offices in which each regional office needs to be connected to every other regional office.

a. **Star Topology:** In a star topology, each device has a dedicated point-to-point link only to a central controller, usually called a hub. The devices are not directly linked to one another. Unlike a mesh topology, a star topology does not allow direct traffic between devices. The controller acts as an exchange: If one device wants to send data to another, it sends the data to the controller, which then relays the data to the other connected device. A star topology is less

expensive than a mesh topology. In a star, each device needs only one link and one I/O port to connect it to any number of others. This factor also makes it easy to install and reconfigure. Far less cabling needs to be housed, and additions, moves, and deletions involve only one connection: between that device and the hub.

Other advantages include robustness. If one link fails, only that link is affected. All other links remain active. This factor also lends itself to easy fault identification and fault isolation. As long as the hub is working, it can be used to monitor link problems and bypass defective links.

One big disadvantage of a star topology is the dependency of the whole topology on one single point, the hub. If the hub goes down, the whole system is dead.

Although a star requires far less cable than a mesh, each node must be linked to a central hub. For this reason, often more cabling is required in a star than in some other topologies (such as ring or bus).

High-speed LANs often use a star topology with a central hub.

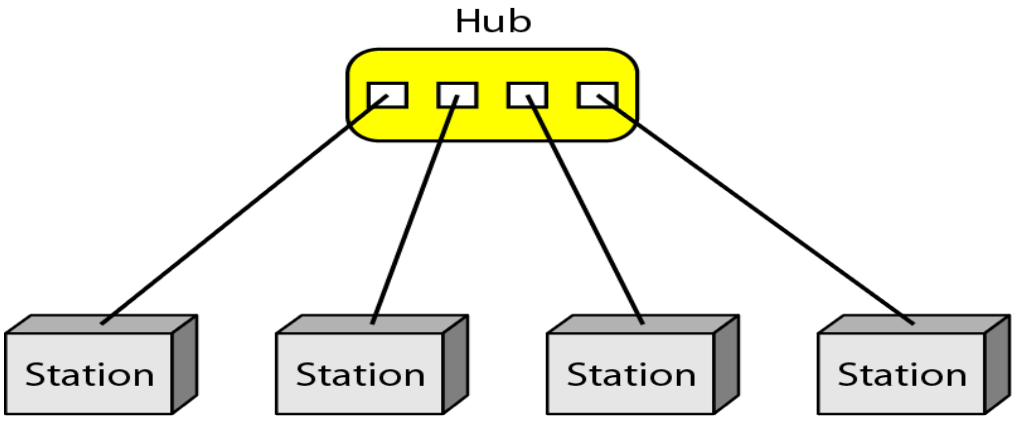


Figure : A star topology connecting four stations

b. **Bus Topology:** The preceding examples all describe point-to-point connections. A **bus topology,** on the other hand, is multipoint. One long cable acts as a **backbone** to link all the devices in a network.

Nodes are connected to the bus cable by drop lines and taps. A drop line is a con• nection running between the device and the main cable. A tap is a connector that either splices into the main cable or punctures the sheathing of a cable to create a contact with the

metallic core. As a signal travels along the backbone, some of its energy is transformed into heat. Therefore, it becomes weaker and weaker as it travels farther and farther. For this reason there is a limit on the number of taps a bus can support and on the distance between those taps.

Advantages of a bus topology include ease of installation. Backbone cable can be laid along the most efficient path, then connected to the nodes by drop lines of various lengths. In this way, a bus uses less cabling than mesh or star topologies. In a star, for example, four network devices in the same room require four lengths of cable reaching all the way to the hub. In a bus, this redundancy is eliminated. Only the backbone cable stretches through the entire facility. Each drop line has to reach only as far as the nearest point on the backbone.

Disadvantages include difficult reconnection and fault isolation. A bus is usually designed to be optimally efficient at installation. It can therefore be difficult to add new devices. Signal reflection at the taps can cause degradation in quality. This degradation can be controlled by limiting the number and spacing of devices connected to a given length of cable. Adding new devices may therefore require modification or replacement of the backbone.

In addition, a fault or break in the bus cable stops all transmission, even between devices on the same side of the problem. The damaged area reflects signals back in the direction of origin, creating noise in both directions.

Bus topology was the one of the first topologies used in the design of early local area networks. Ethernet LANs can use a bus topology, but they are less popular now for reasons.

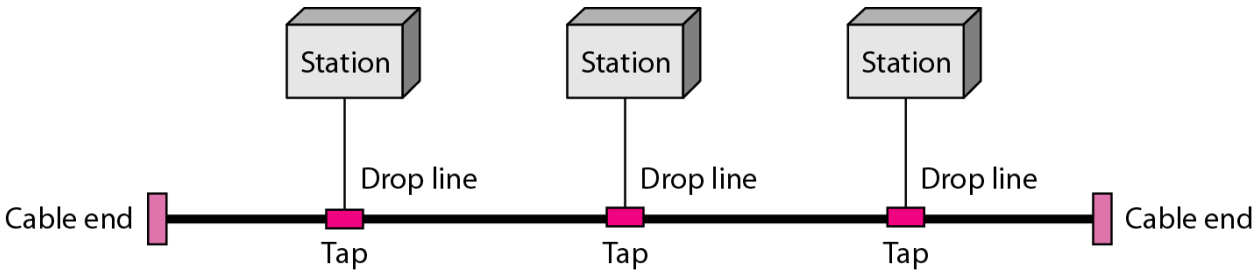


Figure : A bus topology connecting three stations

c. ***Ring Topology:*** In a ring topology, each device has a dedicated point-to-point connection with only the two devices on either side of it. A signal is passed along the ring in one direction, from device to device, until it reaches its destination. Each device in the ring incorporates a repeater. When a device receives a signal intended for another device, its repeater regenerates the bits and passes them along.

A ring is relatively easy to install and reconfigure. Each device is linked to only its immediate neighbors (either physically or logically). To add or delete a device requires changing only two connections. The only constraints are media and traffic considerations (maximum ring length and number of devices). In addition, fault isolation is simplified. Generally in a ring, a signal is circulating at all times. If one device does not receive a signal within a specified period, it can issue an alarm. The alarm alerts the network operator to the problem and its location.

However, unidirectional traffic can be a disadvantage. In a simple ring, a break in the ring (such as a disabled station) can disable the entire network. This weakness can be solved by using a dual ring or a switch capable of closing off the break.

Ring topology was prevalent when IBM introduced its local-area network Token Ring. Today, the need for higher-speed LANs has made this topology less popular.

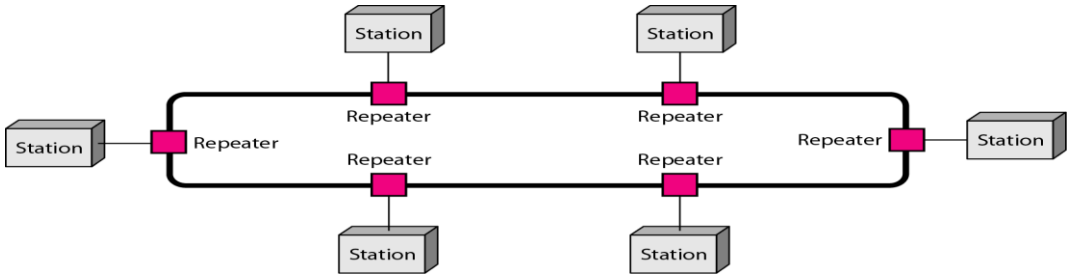


Figure: Ring Topology

d. ***Hybrid Topology*****:** A network can be hybrid. For example, we can have a main star topol• ogy with each branch connecting several stations in a bus topology as shown in Figure

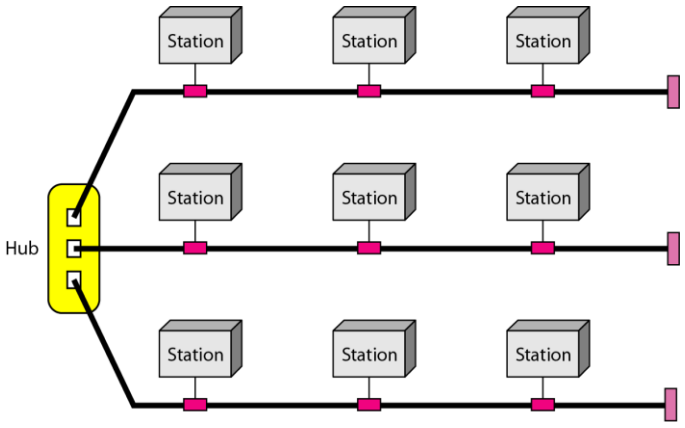


Figure: Hybrid Topology

1. **Explain various topologies with neat diagrams, mention the area of application and also discuss the importance of hybrid topology.**

NETWORK MODELS:

Computer networks are created by different entities. Standards are needed so that these heterogeneous networks can communicate with one another. The two best-known standards are the OSI model and the Internet model. The OSI (Open Systems Interconnection) model defines a seven-layer network; the Internet model defines a five-layer network.

Categories of Networks

Today when we speak of networks, we are generally referring to two primary categories: local-area networks and wide-area networks. The category into which a network falls is determined by its size. A LAN normally covers an area less than 2 mi; a WAN can be worldwide. Networks of a size in between are normally referred to as metropolitan area networks and span tens of miles.

i. Local Area Network

A local area network (LAN) is usually privately owned and links the devices in a single office, building, or campus. Depending on the needs of an organization and the type of technology used, a LAN can be as simple as two PCs and a printer in someone's home office; or it can extend throughout a company and include audio and video peripherals. Currently, LAN size is limited to a few kilometers.

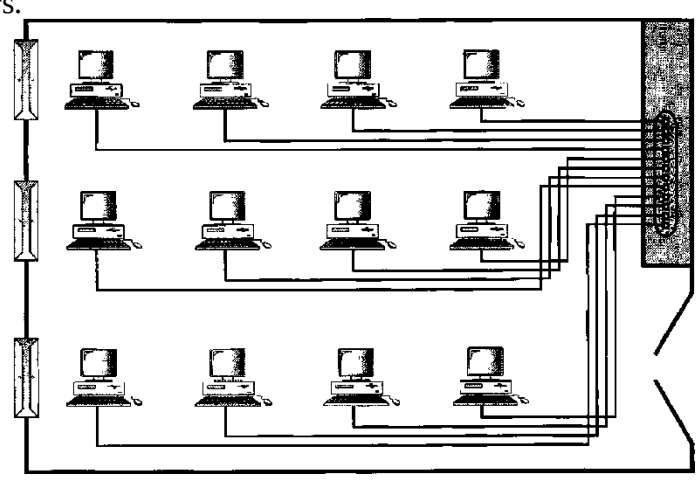


Figure: An isolated IAN connecting 12 computers to a hub in a closet

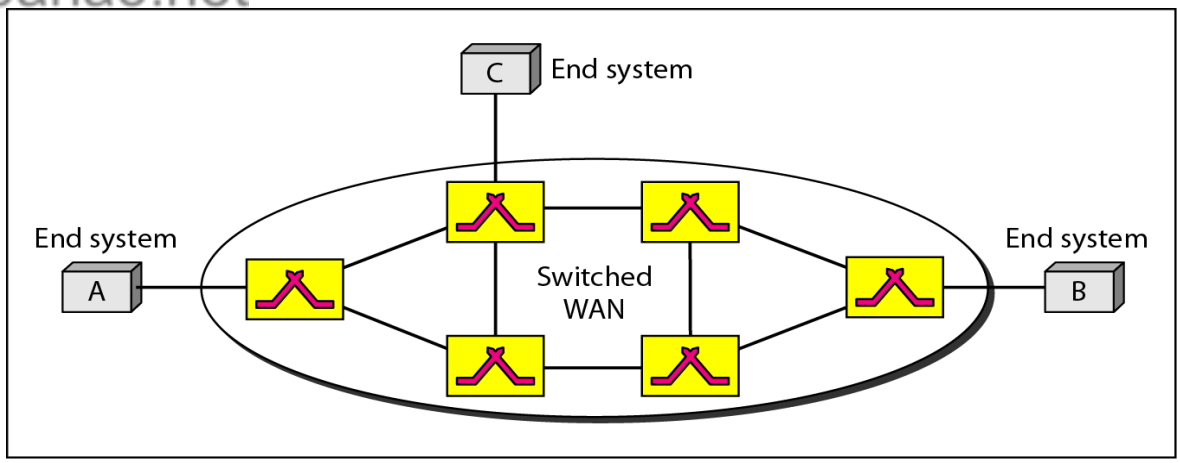
LANs are designed to allow resources to be shared between personal computers or workstations. The resources to be shared can include hardware (e.g., a printer), software (e.g., an application program), or data. A common example of a LAN, found in many business environments, links a workgroup of task-related computers, for example, engineering workstations or accounting PCs. One of the computers may be given a large capacity disk drive and may become a server to clients. Software can be stored on this central server and used as needed by the whole group. In this example, the size of the LAN may be determined by licensing restrictions on the number of users per copy of software, or by restrictions on the number of users licensed to access the operating system.

In addition to size, LANs are distinguished from other types of networks by their transmission media and topology. In general, a given LAN will use only one type of transmission medium. The most common LAN topologies are bus, ring, and star.

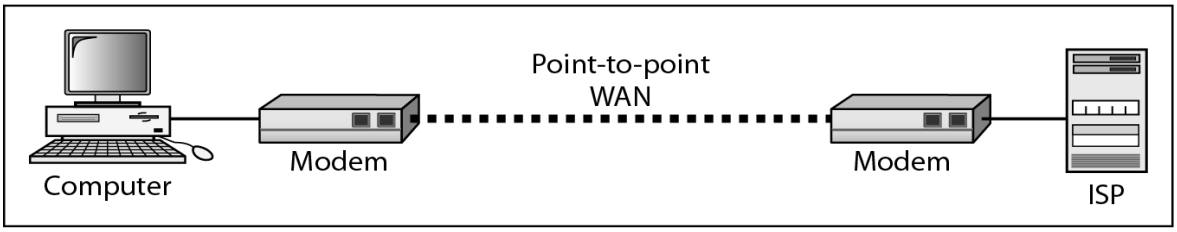
Early LANs had data rates in the 4 to 16 megabits per second (Mbps) range. Today, however, speeds are normally 100 or 1000 Mbps. Wireless LANs are the newest evolution in LAN technology.

ii. Wide Area Network

A wide area network (WAN) provides long-distance transmission of data, image, audio, and video information over large geographic areas that may comprise a country, a continent, or even the whole world. A WAN can be as complex as the backbones that connect the Internet or as simple as a dial-up line that connects a home computer to the Internet. We normally refer to the first as a switched WAN and to the second as a point-to-point WAN. The switched WAN connects the end systems, which usually comprise a router (internet working connecting device) that connects to another LAN or WAN. The point-to-point WAN is normally a line leased from a telephone or cable TV provider that connects a home computer or a small LAN to an Internet service provider (lSP). This type of WAN is often used to provide Internet access.



a. Switched WAN



b. Point-to-point WAN

Fig: WANs: a switched WAN and a point-to-point WAN

An early example of a switched WAN is X.25, a network designed to provide connectivity between end users. X.25 is being gradually replaced by a high-speed, more efficient network called Frame Relay. A good example of a switched WAN is the asynchronous transfer mode (ATM) network, which is a network with data unit packets called cells.

iii. Metropolitan Area Networks

A metropolitan area network (MAN) is a network with a size between a LAN and a WAN. It normally covers the area inside a town or a city. It is designed for customers who need a high-speed connectivity, normally to the Internet, and have endpoints spread over a city or part of city. A good example of a MAN is the part of the telephone company network that can provide a high-speed DSL line to the customer. Another example is the cable TV network that originally was designed for cable TV, but today can also be used for high-speed data connection to the Internet.

1. **Explain various network connections with neat Diagrams**
2. **Explain about switched WAN network.**

INTERCONNECTION OF NETWORKS: INTERNETWORK:

Today, it is very rare to see a LAN, a MAN, or a LAN in isolation; they are connected to one another. When two or more networks are connected, they become an internetwork, or internet.

As an **example,** assume that an organization has two offices, one on the east coast and the other on the west coast. The established office on the west coast has a bus topology LAN; the newly opened office on the east coast has a star topology LAN. The president of the company lives somewhere in the middle and needs to have control over the company from her horne. To create a backbone WAN for connecting these three entities (two LANs and the president's computer), a switched WAN (operated by a service provider such as a telecom company) has been leased. To connect the LANs to this switched WAN, however, three point-to-point WANs are required. These point-to-point WANs can be a high-speed DSL line offered by a telephone company or a cable modern line offered by a cable TV provider as shown in Figure.

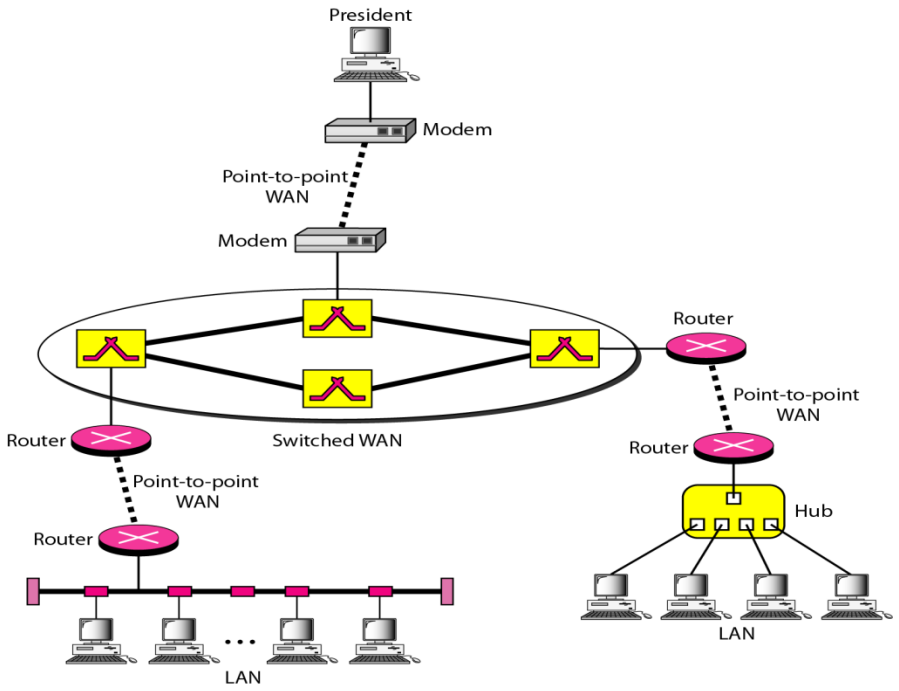


Figure: A heterogeneous network made of four WANs and two LANs

1. **Explain interconnection of networks.**

THE INTERNET

The Internet has revolutionized many aspects of our daily lives. It has affected the way we do business as well as the way we spend our leisure time. Count the ways you've used the Internet recently. Perhaps you've sent electronic mail (e-mail) to a business associate, paid a utility bill, read a newspaper from a distant city, or looked up a local movie schedule-all by using the Internet. Or maybe researched a medical topic, booked a hotel reservation, chatted with a fellow Trekkie, or comparison-shopped for a car. The Internet is a communication system that has brought a wealth of information to our fingertips and organized it for our use. The Internet is a structured, organized system.

A Brief History

A network is a group of connected communicating devices such as computers and printers. An internet (note the lowercase letter i) is two or more networks that can communicate with each other. The most notable internet is called the Internet (uppercase letter I), a collaboration of more than hundreds of thousands of interconnected networks. Private individuals as well as various organizations such as government agencies, schools, research facilities, corporations, and libraries in more than 100 countries use the Internet. Millions of people are users. Yet this extraordinary communication system only came into being in 1969.

In the mid-1960s, mainframe computers in research organizations were stand• alone devices. Computers from different manufacturers were unable to communicate with one another. The **Advanced Research Projects Agency** (ARPA) in the Department of Defense (DoD) was interested in finding a way to connect computers so that the researchers they funded could share their findings, thereby reducing costs and eliminating duplication of effort.

In 1967, at an Association for Computing Machinery (ACM) meeting, ARPA presented its ideas for ARPANET, a small network of connected computers. The idea was that each host computer (not necessarily from the same manufacturer) would be attached to a specialized computer, called an *interface* ***message processor*** **(IMP**). The IMPs, in turn, would be connected to one another. Each IMP had to be able to communicate with other IMPs as well as with its own attached host.

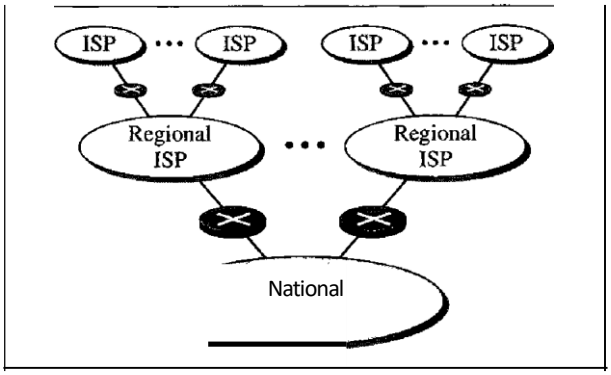
By 1969, ARPANET was a reality. Four nodes, at the University of California at Los Angeles (UCLA), the University of California at Santa Barbara (UCSB), Stanford Research Institute (SRI), and the University of Utah, were connected via the IMPs to form a network. Software called the ***Network Control Protocol*** (NCP) provided communication between the hosts.

In 1972, Vint Cerf and Bob Kahn, both of whom were part of the core ARPANET group, collaborated on what they called the ***Internetting Project*** Cerf and Kahn's landmark 1973 paper outlined the protocols to achieve end-to-end delivery of packets. This paper on Transmission Control Protocol (TCP) included concepts such as encapsulation, the datagram, and the functions of a gateway.

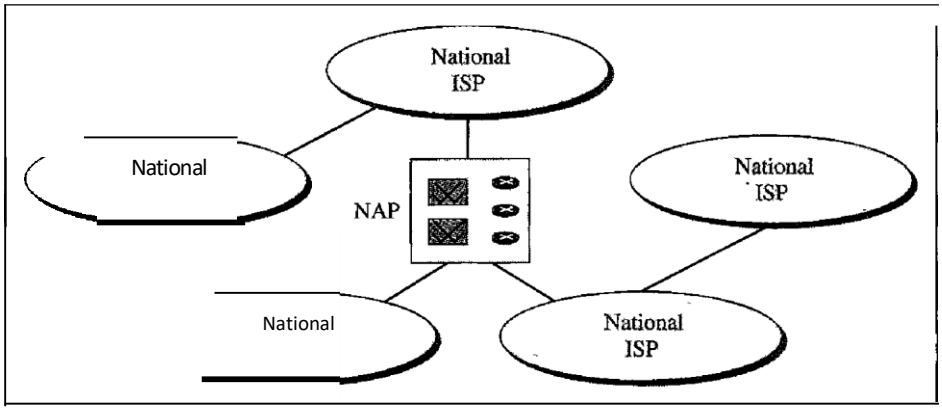
Shortly thereafter, authorities made a decision to split TCP into two protocols: Transmission Control Protocol (TCP) and Internetworking Protocol (lP). IP would handle datagram routing while TCP would be responsible for higher-level functions such as segmentation, reassembly, and error detection. The internetworking protocol became known as TCPIIP.

The Internet Today

The Internet has come a long way since the 1960s. The Internet today is not a simple hierarchical structure. **It is made up of many wide- and local-area networks joined by connecting devices and switching stations.** It is difficult to give an accurate representation of the Internet because it is continually changing-new networks are being added, existing networks are adding addresses, and networks of defunct companies are being removed. Today most end users who want Internet connection use the services of Internet service providers (lSPs). There are international service providers, national service providers, regional service providers, and local service providers. The Internet today is run by private companies, not the government. Below fig shows a conceptual (not geographic) view of the Internet.



a. Structure of a national ISP



b. Interconnection of national ISPs

International Internet Service Providers

At the top of the hierarchy are the international service providers that connect nations together.

National Internet Service Providers

The national Internet service providers are backbone networks created and maintained by specialized companies. There are many national ISPs operating in North America; some of the most well known are SprintLink, PSINet, UUNet Technology, AGIS, and internet Mel. To provide connectivity between the end users, these back bone networks are connected by complex switching stations (normally run by a third party) called network access points (NAPs). Some national ISP networks are also connected to one another by private switching stations called *peering points.* These normally operate at a high data rate (up to 600 Mbps).

Regional Internet Service Providers

Regional internet service providers or regional ISPs are smaller ISPs that are connected to one or more national ISPs. They are at the third level of the hierarchy with a smaller data rate.

Local Internet Service Providers

Local Internet service providers provide direct service to the end users. The local ISPs can be connected to regional ISPs or directly to national ISPs. Most end users are connected to the local ISPs. Note that in this sense, a local ISP can be a company that just provides Internet services, a corporation with a network that supplies services to its own employees, or a nonprofit organization, such as a college or a university, that runs its own network. Each of these local ISPs can be connected to a regional or national service provider.

PROTOCOLS AND STANDARDS

Protocols

In computer networks, communication occurs between entities in different systems. An entity is anything capable of sending or receiving information. However, two entities can• not simply send bit streams to each other and expect to be understood. For communication to occur, the entities must agree on a protocol. A protocol is a set of rules that govern data communications. A protocol defines what is communicated, how it is communicated, and when it is communicated. The key elements of a protocol are syntax, semantics, and timing.

Syntax: The term *syntax* refers to the structure or format of the data, meaning the order in which they are presented. For example, a simple protocol might expect the first 8 bits of data to be the address of the sender, the second 8 bits to be the address of the receiver, and the rest of the stream to be the message itself.

Semantics: The word *semantics* refers to the meaning of each section of bits. How is a particular pattern to be interpreted, and what action is to be taken based on that interpretation? For example, does an address identify the route to be taken or the final destination of the message?

Timing: The term *timing* refers to two characteristics: when data should be sent and how fast they can be sent. For example, if a sender produces data at 100 Mbps but the receiver can process data at only 1 Mbps, the transmission will overload the receiver and some data will be lost.

Standards

Standards are essential in creating and maintaining an open and competitive market for equipment manufacturers and in guaranteeing national and international interoperability of data and telecommunications technology and processes. Standards provide guidelines to manufacturers, vendors, government agencies, and other service providers to ensure the kind of interconnectivity necessary in today's marketplace and in international com• munications. Data communication standards fall into two categories: *de facto* (meaning "by fact" or "by convention") and *de jure* (meaning "by law" or "by regulation").

Standards Organizations

Standards are developed through the cooperation of standards creation committees, forums, and government regulatory agencies.

Standards Creation Committees

While many organizations are dedicated to the establishment of standards, data telecommunications in North America rely primarily on those published by the following:

International Organization for Standardization (ISO):

The ISO is a multinational body whose membership is drawn mainly from the standards creation committees of various governments throughout the world. The ISO is active in developing cooperation in the realms of scientific, technological, and economic activity.

International Telecommunication Union-Telecommunication Standards

Sector (ITU-T). By the early 1970s, a number of countries were defining national standards for telecommunications, but there was still little international compati• bility. The United Nations responded by forming, as part of its International Telecommunication Union (ITU), a committee, the Consultative Committee for International Telegraphy and Telephony (CCITT). This committee was devoted to the research and establishment of standards for telecommunications in general and for phone and data systems in particular. On March 1, 1993, the name of this committee was changed to the International Telecommunication Union Telecommunication Standards Sector (ITU-T).

American National Standards Institute (ANSI).

Despite its name, the American National Standards Institute is a completely private, nonprofit corporation not affili• ated with the U.S. federal government. However, all ANSI activities are undertaken with the welfare of the United States and its citizens occupying primary importance.

Institute of Electrical and Electronics Engineers (IEEE).

The Institute of Electrical and Electronics Engineers is the largest professional engineering society in the world. International in scope, it aims to advance theory, creativity, and product quality in the fields of electrical engineering, electronics, and radio as well as in all related branches of engineering. As one of its goals, the IEEE oversees the develop ment and adoption of international standards for computing and communications.

Electronic Industries Association (EIA).

Aligned with ANSI, the Electronic Industries Association is a nonprofit organization devoted to the promotion of electronics manufacturing concerns. Its activities include public awareness education and lobbying efforts in addition to standards development. In the field of information technology, the EIA has made significant contributions by defining physical connection interfaces and electronic signaling specifications for data communication.

Forums

Telecommunications technology development is moving faster than the ability of stan• dards committees to ratify standards. Standards committees are procedural bodies and by nature slow-moving. To accommodate the need for working models and agreements and to facilitate the standardization process, many special-interest groups have

devel-

oped **forums** made up of representatives from interested corporations. The forums work with universities and users to test, evaluate, and standardize new technologies. By concentrating their efforts on a particular

technology, the forums are able to speed acceptance and use of those technologies in the telecommunications community. The forums present their conclusions to the standards bodies.

Regulatory Agencies

All communications technology is subject to regulation by government agencies such as the **Federal Communications Commission** (FCC) in the United States. The pur• pose of these agencies is to protect the public interest by regulating radio, television, and wire/cable communications. The FCC has authority over interstate and interna• tional commerce as it relates to communications.

Internet Standards

An **Internet standard** is a thoroughly tested specification that is useful to and adhered to by those who work with the Internet. It is a formalized regulation that must be followed. There is a strict procedure by which a specification attains Internet standard status. A specification begins as an Internet draft. An **Internet draft** is a working document (a work in progress) with no official status and a 6-month lifetime. Upon recommendation from the Internet authorities, a draft may be published as a **Request for Comment** (RFC). Each RFC is edited, assigned a number, and made available to all interested parties. RFCs go through maturity levels and are categorized according to their requirement level.

Network Models

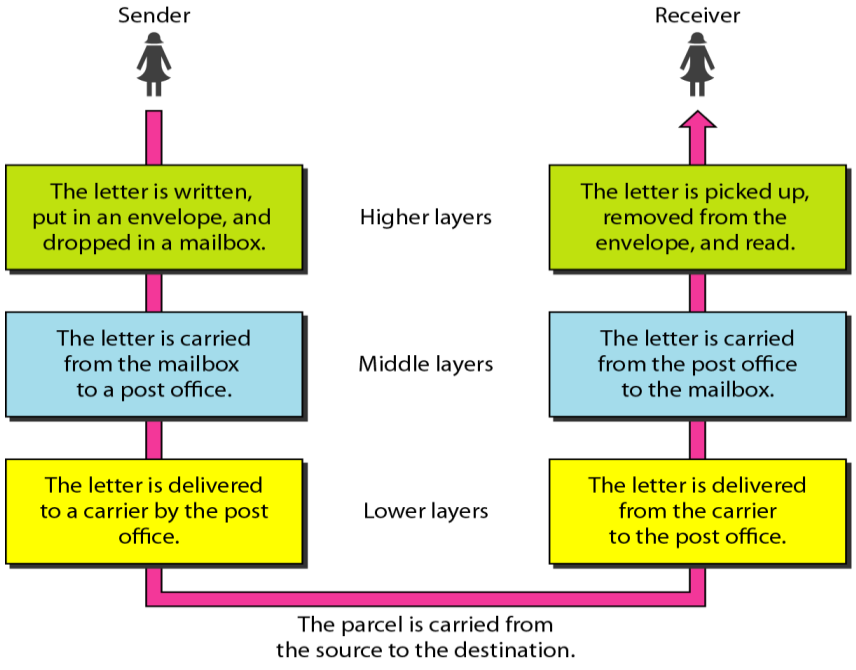
A network is a combination of hardware and software that sends data from one location to another. The hardware consists of the physical equipment that carries signals from one point of the network to another. The software consists of instruction sets that make possible the services that we expect from a network.

We can compare the task of networking to the task of solving a mathematics problem with a computer. The fundamental job of solving the problem with a computer is done by computer hardware. However, this is a very tedious task if only hardware is involved. We would need switches for every memory location to store and manipulate data. The task is much easier if software is available. At the highest level, a program can direct the problem-solving process; the details of how this is done by the actual hardware can be left to the layers of software that are called by the higher levels.

Compare this to a service provided by a computer network. For example, the task of sending an e-mail from one point in the world to another can be broken into several tasks, each performed by a separate software package. Each software package uses the services of another software package. At the lowest layer, a signal, or a set of signals, is sent from the source computer to the destination computer.

LAYERED TASKS

We use the concept of layers in our daily life. As an example, let us consider two friends who communicate through postal maiL The process of sending a letter to a friend would be complex if there were no services available from the post office. Figure shows the steps in this task.



Sender, Receiver, and Carrier

In above figure we have a sender, a receiver, and a carrier that transports the letter. There is a hierarchy of tasks.

At the Sender Side the activities that take place at the sender site.

Higher layer. The sender writes the letter, inserts the letter in an envelope, writes the sender and receiver addresses, and drops the letter in a mailbox.

Middle layer: The letter is picked up by a letter carrier and delivered to the post office.

Lower laye:. The letter is sorted at the post office; a carrier transports the letter.

on the Way:

The letter is then on its way to the recipient. On the way to the recipient's local post office, the letter may actually go through a central office. In addition, it may be trans• ported by truck, train, airplane, boat, or a combination of these.

At the Receiver Site

Lower layer: The carrier transports the letter to the post office.

Middle layer: The letter is sorted and delivered to the recipient's mailbox.

Higher layer: The receiver picks up the letter, opens the envelope, and reads it.

Hierarchy

According to our analysis, there are three different activities at the sender site and another three activities at the receiver site. The task of transporting the letter between the sender and the receiver is done by the carrier. Something that is not obvious immediately is that the tasks must be done in the order given in the hierarchy. At the sender site, the letter must be written and dropped in the mailbox before being picked up by the letter carrier and delivered to the post office. At the receiver site, the letter must be dropped in the recipient mailbox before being picked up and read by the recipient.

Services

Each layer at the sending site uses the services of the layer immediately below it. The sender at the higher layer uses the services of the middle layer. The middle layer uses the services of the lower layer. The lower layer uses the services of the carrier.

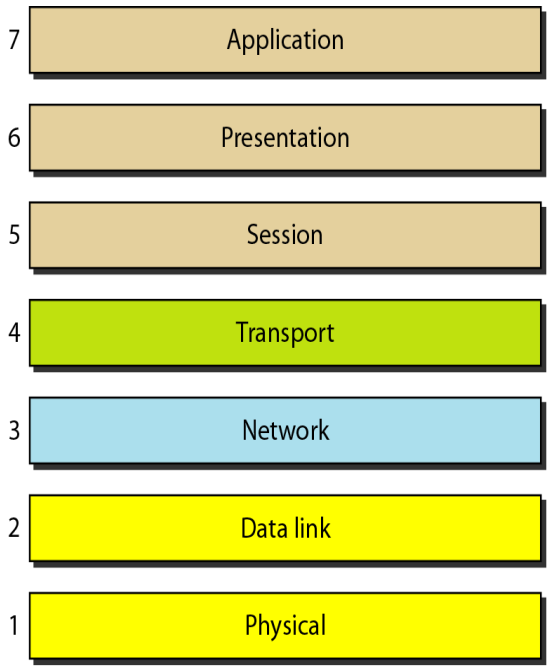
The layered model that dominated data communications and networking literature before 1990 was the Open Systems Interconnection (OSI) model. Everyone believed that the OSI model would become the ultimate standard for data communications, but this did not happen. The TCPIIP protocol suite became the dominant commercial architecture because it was used and tested extensively in the Internet; the OSI model was never fully implemented.

In this chapter, first we briefly discuss the OSI model, and then we concentrate on TCPIIP as a protocol suite.

THE OSI MODEL

Established in 1947, the International Standards Organization (ISO) is a multinational body dedicated to worldwide agreement on international standards. An ISO standard that covers all aspects of network communications is the Open Systems Interconnection 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 archi• tecture. The purpose of the OSI model is to show how to facilitate communication between different systems without requiring changes to the logic of the underlying hard• ware and software. 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 is a layered framework for the design of network systems that allows communication between all types of computer systems. It consists of seven sep• arate but related layers, each of which defines a part of the process of moving information across a network (see Figure 2.2). An understanding of the fundamentals of the OSI model provides a solid basis for exploring data communications.



Layered **Architecture**

The OSI model is composed of seven ordered layers: physical (layer 1), data link (layer 2), network (layer 3), transport (layer 4), session (layer 5), presentation (layer 6), and application (layer 7). Figure 2.3 shows the layers involved when a message is sent from device A to device B. As the message travels from A to

B, it may pass through many intermediate nodes. These intermediate nodes usually involve only the first three layers of the OSI model.

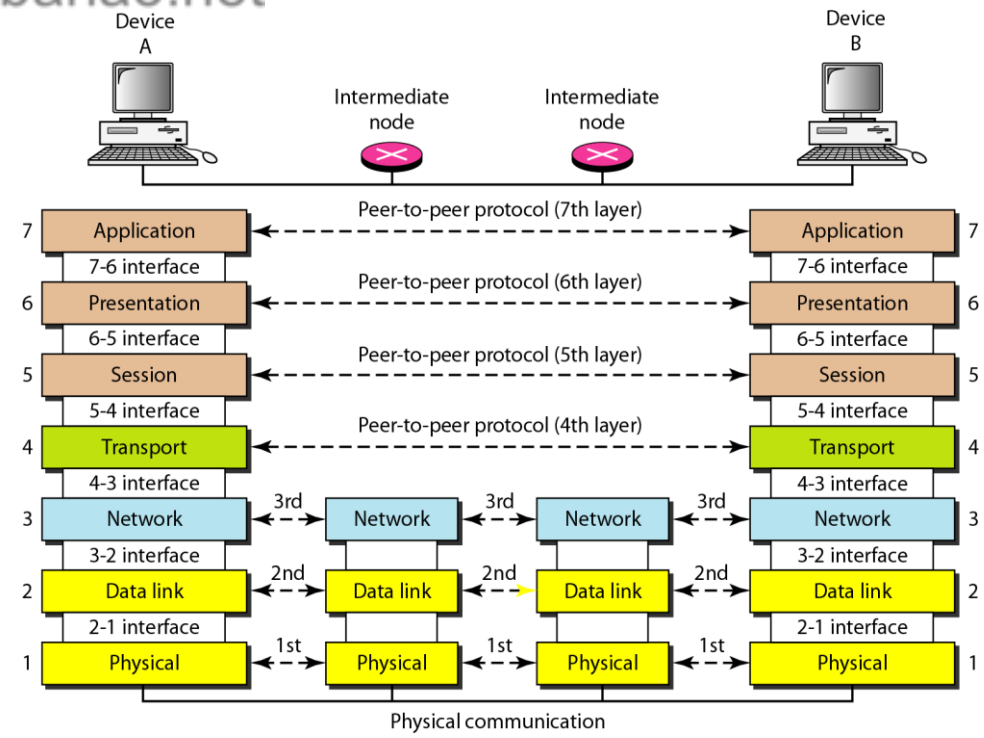
In *developing* the model, the designers distilled the process of transmitting data to

its most fundamental elements. They identified which networking functions had related uses and collected those functions into discrete groups that became the layers. Each layer defines a family of functions distinct from those of the other layers. By defining and localizing functionality in this fashion, the designers created an architecture that is both comprehensive and flexible. Most importantly, the OSI model allows complete interoperability between otherwise incompatible systems.

Within a single machine, each layer calls upon the services of the layer just below it. Layer 3, for example, uses the services provided by layer 2 and provides services for layer 4. Between machines, layer *x* on one machine communicates with layer *x* on another machine. This communication is governed by an agreed-upon series of rules and conventions called protocols. The processes on each machine that communicate at a given layer are called peer-to-peer processes. Communication between machines is therefore a peer-to-peer process using the protocols appropriate to a given layer.

Peer-to-Peer Processes

At the physical layer, communication is direct: In Figure 2.3, device A sends a stream of bits to device B (through intermediate nodes). At the higher layers, however, com• munication must move down through the layers on device A, over to device B, and then back up through the layers. Each layer in the sending device adds its own information to the message it receives from the layer just above it and passes the whole package to the layer just below it.
At layer I the entire package is converted to a form that can be transmitted to the receiving device. At the receiving machine, the message is unwrapped layer by layer, with each process receiving and removing the data meant for it. For example, layer 2 removes the data meant for it, then passes the rest to layer 3. Layer 3 then removes the data meant for it and passes the rest to layer 4, and so on.



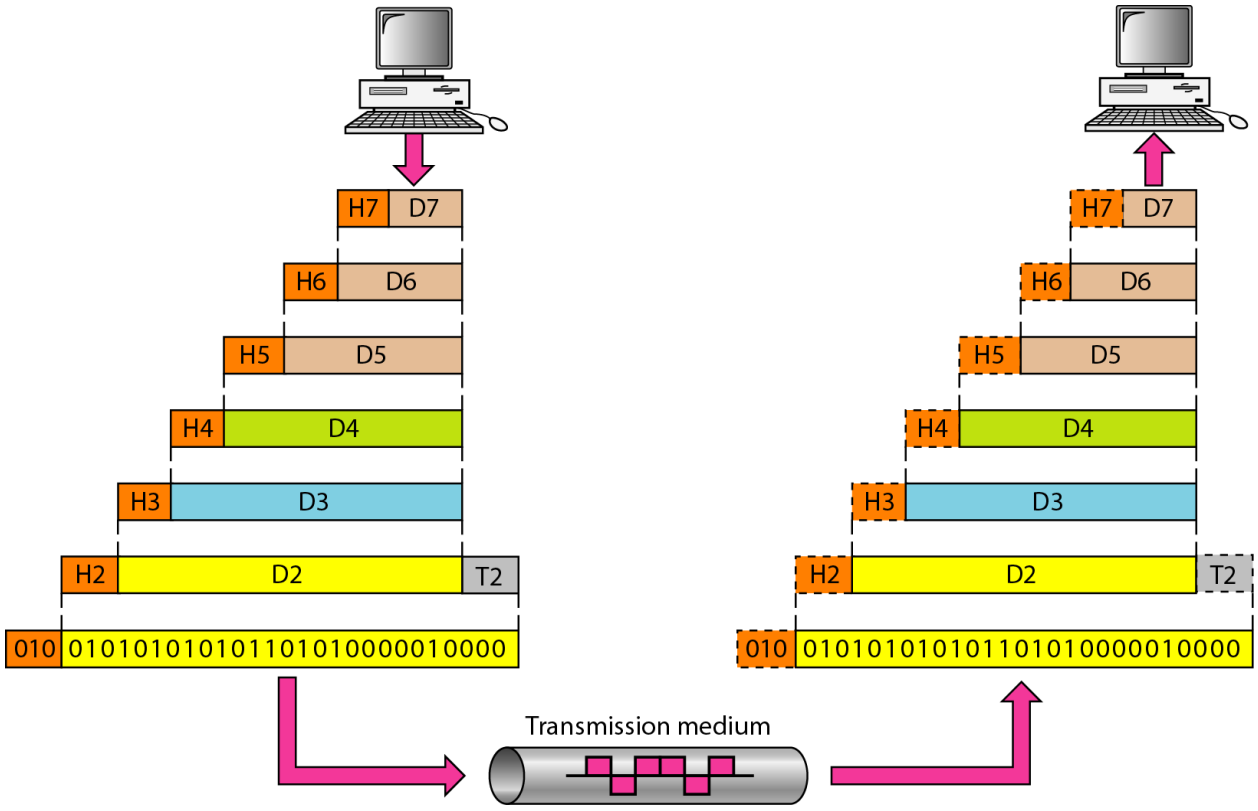
Interfaces Between Layers

The passing of the data and network information down through the layers of the send• ing device and back up through the layers of the receiving device is made possible by an interface between each pair of adjacent layers. Each interface defines the informa• tion and services a layer must provide for the layer above it. Well-defined interfaces and layer functions provide modularity to a network. As long as a layer provides the expected services to the layer above it, the specific implementation of its functions can be modified or replaced without requiring changes to the surrounding layers.

Organization ofthe Layers

The seven layers can be thought of as belonging to three subgroups. Layers I, 2, and 3-physical, data link, and network-are the network support layers; they deal with
the physical aspects of moving data from one device to another (such as electrical specifications, physical connections, physical addressing, and transport timing and reliability). Layers 5, 6, and 7-session, presentation, and application-can be thought of as the user support layers; they allow interoperability among unrelated software systems. Layer 4, the transport layer, links the two subgroups and ensures that what the lower layers have transmitted is in a form that the upper layers can use. The upper OSI layers are almost always implemented in software; lower layers are a combination of hardware and software, except for the physical layer, which is mostly hardware.
In Figure 2.4, which gives an overall view of the OSI layers, D7 means the data unit at layer 7, D6 means the data unit at layer 6, and so on. The process starts at layer 7 (the application layer), then moves from layer to layer in descending, sequential order. At each layer, a **header,** or possibly a **trailer,** can be added to the data unit. Commonly, the trailer is added only at layer 2. When the formatted data unit passes through the physical layer (layer 1), it is changed into an electromagnetic

signal and transported along a physical link.



Upon reaching its destination, the signal passes into layer 1 and is transformed back into digital form. The data units then move back up through the OSI layers. As each block of data reaches the next higher layer, the headers and trailers attached to it at the corresponding sending layer are removed, and actions appropriate to that layer are taken. By the time it reaches layer 7, the message is again in a form appropriate to the application and is made available to the recipient.

Encapsulation

Figure 2.3 reveals another aspect of data communications in the OSI model: encapsula• tion. A packet (header and data) at level 7 is encapsulated in a packet at level 6. The whole packet at level 6 is encapsulated in a packet at level 5, and so on.

In other words, the data portion of a packet at level *N* - 1 carries the whole packet (data and header and maybe trailer) from level *N*. The concept is called *encapsulation;* level *N* - 1 is not aware of which part of the encapsulated packet is data and which part is the header or trailer. For level *N* - 1, the whole packet coming from level *N* is treated as one integral unit.

Physical Layer

The physical layer coordinates the functions required to carry a bit stream over a physical medium. It deals with the mechanical and electrical specifications of the interface and transmission medium. It also defines the procedures and functions that physical devices and interfaces have to perform for transmission to Occur. Figure below shows the position of the physical layer with respect to the transmission medium and the data link layer.

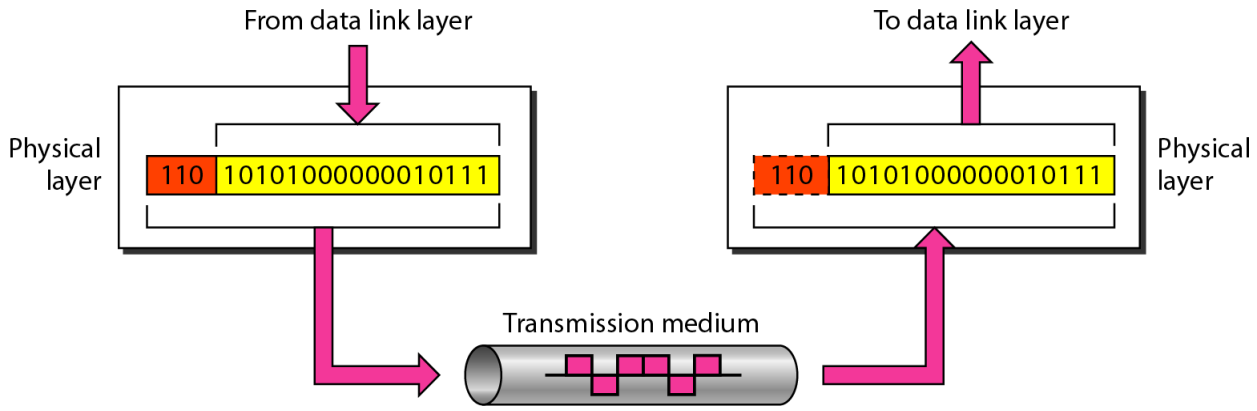


Figure: ***Physical layer***

The physical layer is also concerned with the following: o Physical characteristics of interfaces and medium. The physical layer defines the characteristics of the interface between the devices and the transmission medium. It also defines the type of transmission medium.

o **Representation of bits**: The physical layer data consists of a stream of bits (sequence of Os or 1s) with no interpretation. To be transmitted, bits must be encoded into signals--electrical or optical. The physical layer defines the type of encoding (how Os and Is are changed to signals).

o Data rate: The transmission rate-the number of bits sent each second-is also defined by the physical layer. In other words, the physical layer defines the duration of a bit, which is how long it lasts.

o Synchronization of bits. The sender and receiver not only must use the same bit rate but also must be synchronized at the bit level. In other words, the sender and the receiver clocks must be synchronized. o Line configuration. The physical layer is concerned with the connection of devices to the media. In a point-to-point configuration, two devices are connected through a dedicated link. In a multipoint configuration, a link is shared among several devices.

o Physical topology. The physical topology defines how devices are connected to make a network. Devices can be connected by using a mesh topology (every device is connected to every other device), a star topology (devices are connected through a central device), a ring topology (each device is connected to the next, forming a ring), a bus topology (every device is on a common link), or a hybrid topology (this is a combination oftwo or more topologies).

o Transmission mode. The physical layer also defines the direction of transmission between two devices: simplex, half-duplex, or full-duplex. In simplex mode, only one device can send; the other can only receive. The simplex mode is a one-way communication. In the half-duplex mode, two devices can send and

receive, but not at the same time. In a full-duplex (or simply duplex) mode, two devices can send and receive at the same time.

Data Link Layer

The data link layer transforms the physical layer, a raw transmission facility, to a reliable link. It makes the physical layer appear error-free to the upper layer (network layer). Figure below shows the relationship of the data link layer to the network and physical layers.

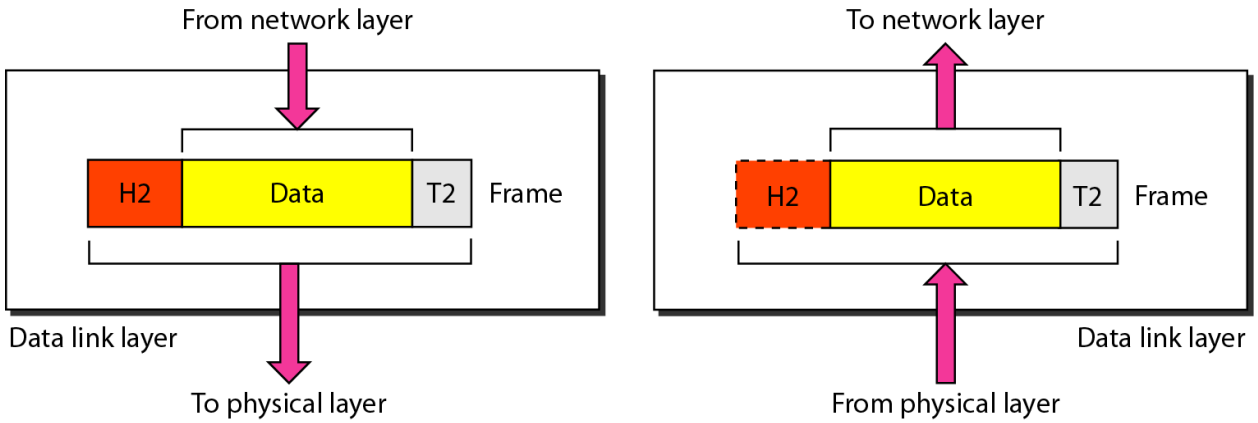


Figure: data link layer

Framing. The data link layer divides the stream of bits received from the network layer into manageable data units called frames. o Physical addressing. If frames are to be distributed to different systems on the network, the data link layer adds a header to the frame to define the sender and/or receiver of the frame. If the frame is intended for a system outside the sender's network, the receiver address is the address of the device that connects the network to the next one.

Data Flow control. If the rate at which the data are absorbed by the receiver is less than the rate at which data are produced in the sender, the data link layer imposes a flow control mechanism to avoid overwhelming the receiver.

Error control. The data link layer adds reliability to the physical layer by adding mechanisms to detect and retransmit damaged or lost frames. It also uses a mechanism to recognize duplicate frames. Error control is normally achieved through a trailer added to the end ofthe frame.

Data Access control. When two or more devices are connected to the same link, data link layer protocols are necessary to determine which device has control over the link at any given time. Figure 2.7 illustrates hop-to-hop (node-to-node) delivery by the data link layer.

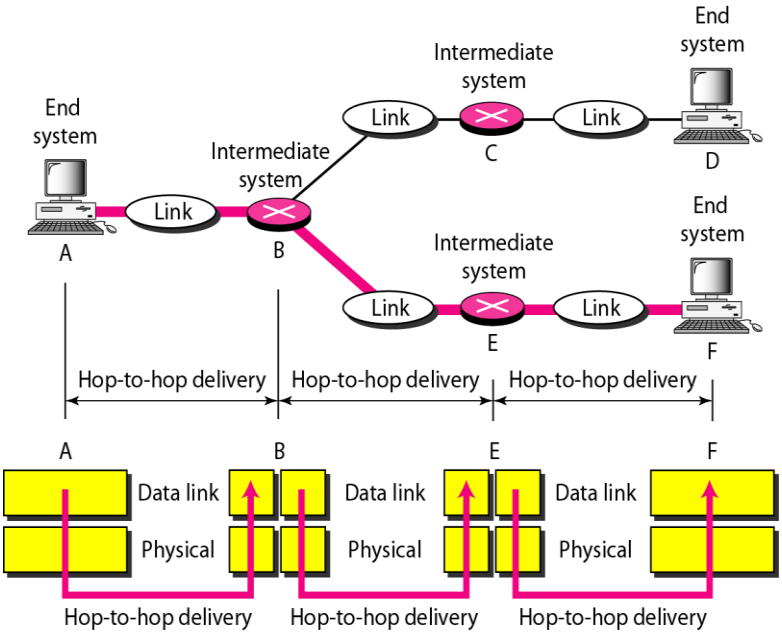
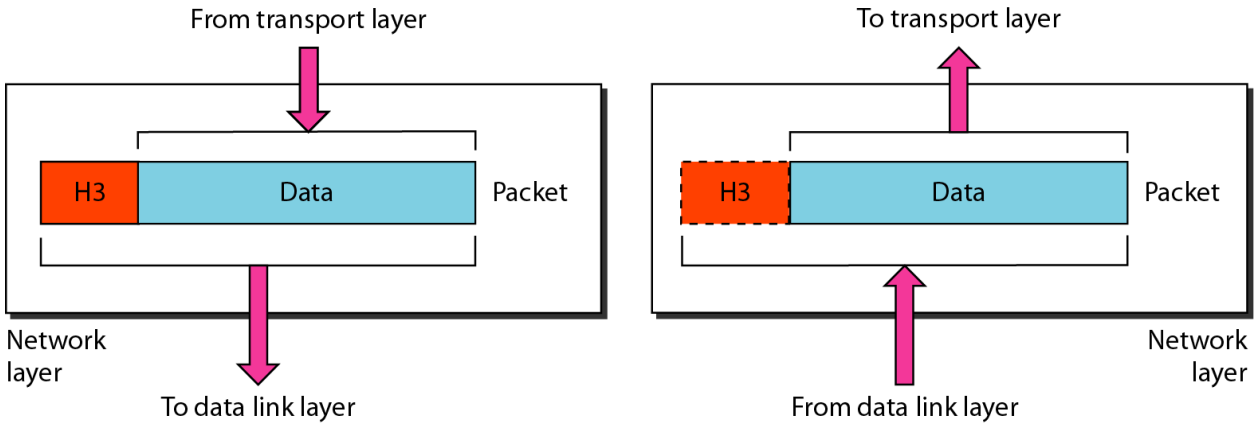


Figure: Hop-to hop delivery

As the figure shows, communication at the data link layer occurs between two adjacent nodes. To send data from A to F, three partial deliveries are made. First, the data link layer at A sends a frame to the data link layer at B (a router). Second, the data link layer at B sends a new frame to the data link layer at E. Finally, the data link layer at E sends a new frame to the data link layer at F. Note that the frames that are exchanged between the three nodes have different values in the headers. The frame from A to B has B as the destination address and A as the source address. The frame from B to E has E as the destination address and B as the source address. The frame from E to F has F as the destination address and E as the source address. The values of the trailers can also be different iferror checking includes the header ofthe frame.

Network Layer

The network layer is responsible for the source-to-destination delivery of a packet, possibly across multiple networks (links). Whereas the data link layer oversees the delivery of the packet between two systems on the same network (links), the network layer ensures that each packet gets from its point of origin to its final destination. Iftwo systems are connected to the same link, there is usually no need for a network layer. However, ifthe two systems are attached to different networks (links) with connecting devices between the networks (links), there is often a need for the network layer to accomplish source-to-destination delivery. Figure below shows the relationship of the network layer to the data link and transport layers.



The network layer is responsible for the delivery of individual packets from the source host to the destination host.

Other responsibilities of the network layer include the following:

i) Logical addressing. The physical addressing implemented by the data link layer handles the addressing problem locally. If a packet passes the network boundary, we need another addressing system to help distinguish the source and destination systems. The network layer adds a header to the packet coming from the upper layer that, among other things, includes the logical addresses of the sender and receiver.

ii) Routing. When independent networks or links are connected to create intemet works (network of networks) or a large network, the connecting devices (called routers or switches) route or switch the packets to their final destination. One of the functions of the network layer is to provide this mechanism.

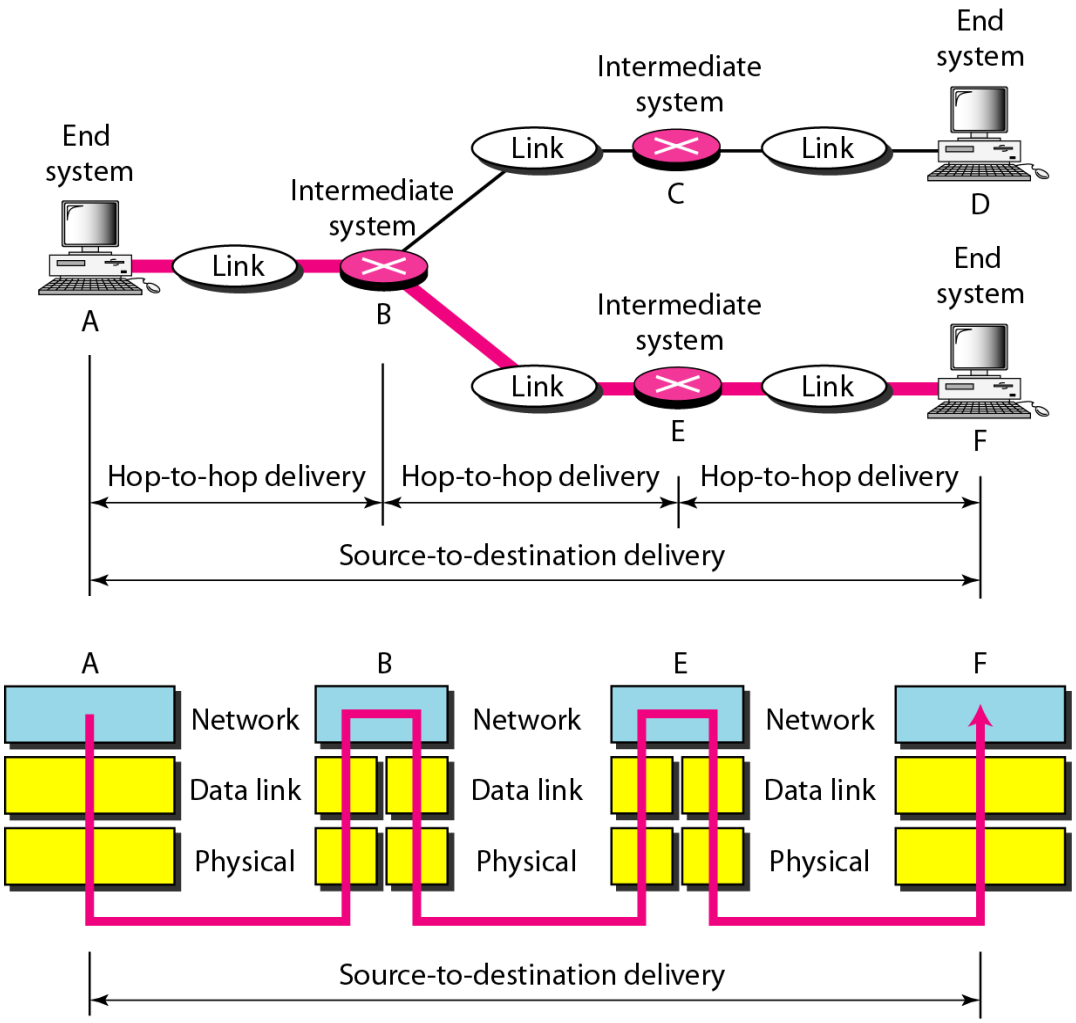


Figure ***Source-to-destination delivery***

As the figure shows, now we need a source-to-destination delivery. The network layer at A sends the packet to the network layer at B. When the packet arrives at router B, the router makes a decision based on the final destination (F) ofthe packet. As we will see in later chapters, router B uses its routing table to find that the next hop is router E. The network layer at B, therefore, sends the packet to the network layer at E. The network layer at E, in tum, sends the packet to the network layer at F.

Transport Layer :

The transport layer is responsible for process-to-process delivery of the entire message. A process is an application program running on a host. Whereas the network layer oversees source-to-destination delivery of individual packets, it does not recognize any relationship between those packets. It treats each one independently, as though each piece belonged to a separate message, whether or not it does. The transport layer, on the other hand, ensures that the whole message arrives intact and in order, overseeing both error control and flow control at the source-to-destination level.

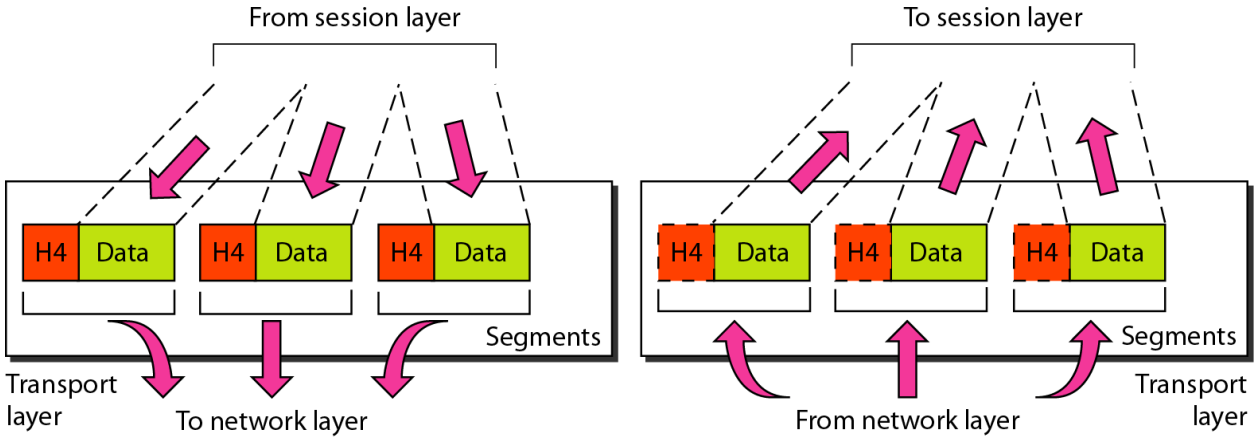


Figure: Transport Layer

The transport layer is responsible for the delivery of a message from one process to another.

Other responsibilities ofthe transport layer include the following:

(i) **Service-point addressing**. Computers often run several programs at the same time. For this reason, source-to-destination delivery means delivery not only from one computer to the next but also from a specific process (running program) on one computer to a specific process (running program) on the other. The transport layer header must therefore include a type of address called a service-point address (or port address). The network layer gets each packet to the correct computer; the transport layer gets the entire message to the correct process on that computer.

(ii) **Segmentation and reassembly**. A message is divided into transmittable segments, with each segment containing a sequence number. These numbers enable the transport layer to reassemble the message correctly upon arriving at the destination and to identify and replace packets that were lost in transmission.

(iii)Connection control. The transport layer can be either connectionless or connectionoriented. A connectionless transport layer treats each segment as an independent packet and delivers it to the transport layer at the destination machine. A connection oriented transport layer makes a connection with the transport layer at the destination machine first before delivering the packets. After all the data are transferred, the connection is terminated.

(iv) Flow control. Like the data link layer, the transport layer is responsible for flow control. However, flow control at this layer is performed end to end rather than across a single link.

(v) Error control. Like the data link layer, the transport layer is responsible for error control. However, error control at this layer is performed process-to process rather than across a single link. The sending transport layer makes sure that the entire message arrives at the receiving transport layer without error (damage, loss, or duplication). Error correction is usually achieved through retransmission.

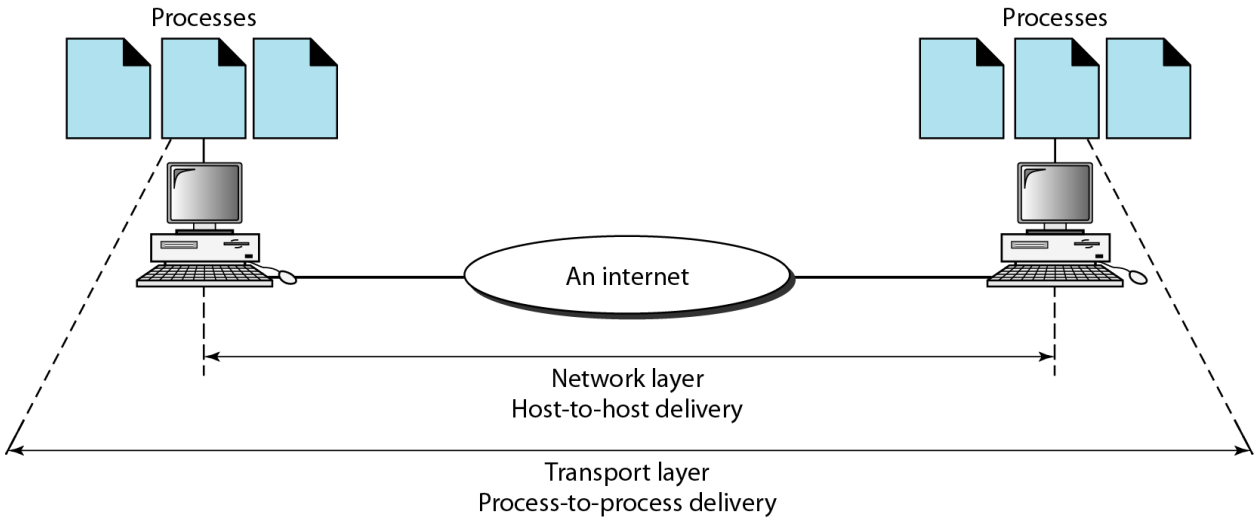


Figure : ***Reliable process-to-process delivery of a message***

Session Layer:

The services provided by the first three layers (physical, data link, and network) are not sufficient for some processes. The session layer is the network dialog controller. It establishes, maintains, and synchronizes the interaction among communicating systems.

The session layer is responsible for dialog control and synchronization.

Specific responsibilities of the session layer include the following: o Dialog control. The session layer allows two systems to enter into a dialog. It allows the communication between two

processes to take place in either halfduplex (one way at a time) or full-duplex (two ways at a time) mode. o Synchronization. The session layer allows a process to add checkpoints, or synchronization points, to a stream of data. For example, if a system is sending a file of2000 pages, it is advisable to insert checkpoints after every 100 pages to ensure that each 100-page unit is received and acknowledged independently. In this case, if a crash happens during the transmission of page 523, the only pages that need to be resent after system recovery are pages 501 to 523. Pages previous to 501 need not be resent. Figure illustrates the relationship of the session layer to the transport and presentation layers.

Presentation Layer:

The presentation layer is concerned with the syntax and semantics of the information exchanged between two systems. Figure shows the relationship between the presentation layer and the application and session layers.

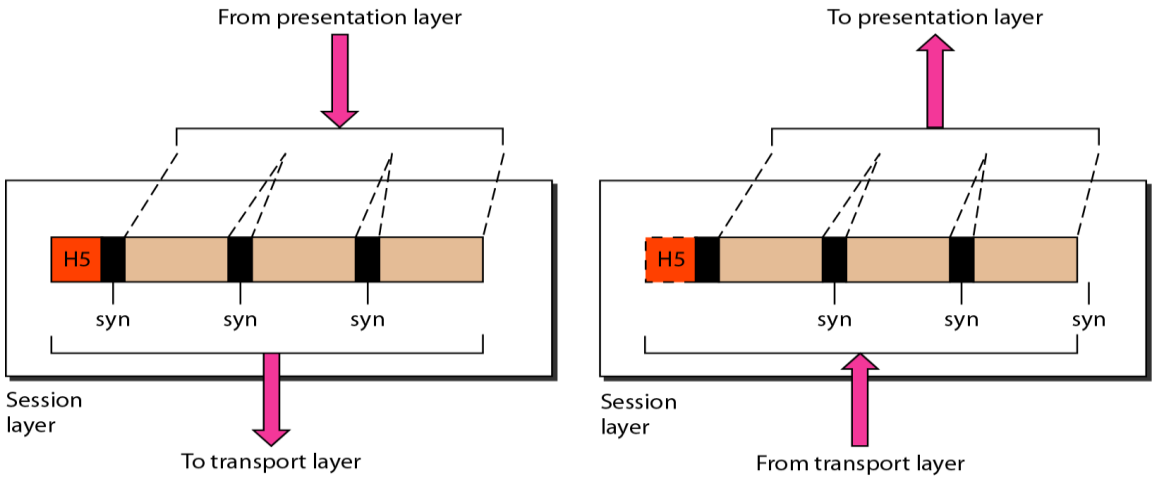


Figure : ***Session layer***

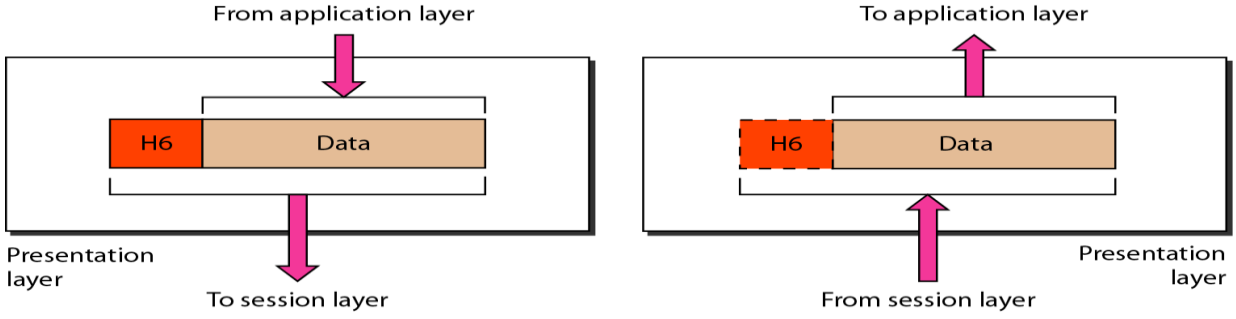


Figure : ***Presentation layer***

The presentation layer is responsible for translation, compression, and encryption.

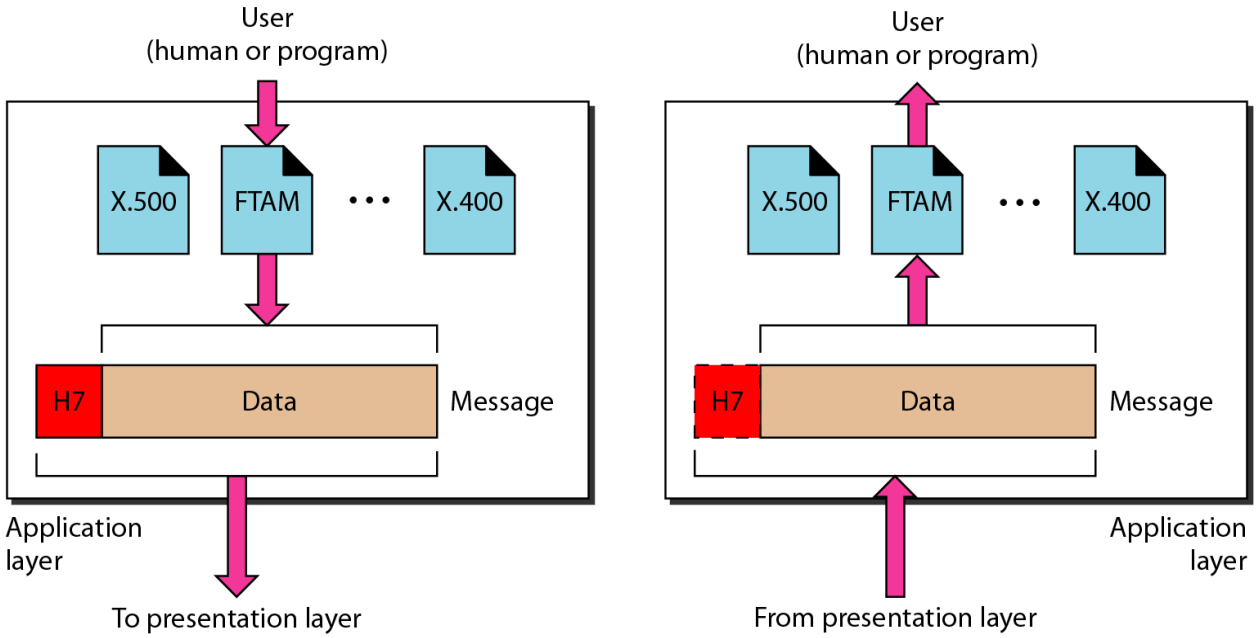
Specific responsibilities of the presentation layer include the following:

(i) **Translation.** The processes (running programs) in two systems are usually exchanging information in the form of character strings, numbers, and so on. The information must be changed to bit streams before being transmitted. Because different computers use different encoding systems, the presentation layer is responsible for interoperability between these different encoding methods. The presentation layer at the sender changes the information from its sender-dependent format into a common format. The presentation layer at the receiving machine changes the common format into its receiver-dependent format.

(ii) **Encryption.** To carry sensitive information, a system must be able to ensure privacy. Encryption means that the sender transforms the original information to another form and sends the resulting message out over the network. Decryption reverses the original process to transform the message back to its original form.

(iii) **Compression.** Data compression reduces the number of bits contained in the information. Data compression becomes particularly important in the transmission of multimedia such as text, audio, and video.

Application Layer



The application layer is responsible for providing services to the user.

Specific services provided by the application layer include the following:

(i) **Network virtual terminal.** A network virtual terminal is a software version of a physical terminal, and it allows a user to log on to a remote host. To do so, the application creates a software emulation of a terminal at the remote host. The user's computer talks to the software terminal which, in turn, talks to the host, and vice versa. The remote host believes it is communicating with one of its own terminals and allows the user to log on.

(ii) **File transfer, access, and management.** This application allows a user to access files in a remote host (to make changes or read data), to retrieve files from a remote computer for use in the local computer, and to manage or control files in a remote computer locally.

(iii) **Mail services.** This application provides the basis for e-mail forwarding and storage.

(iv) **Directory services.** This application provides distributed database sources and access for global information about various objects and services.

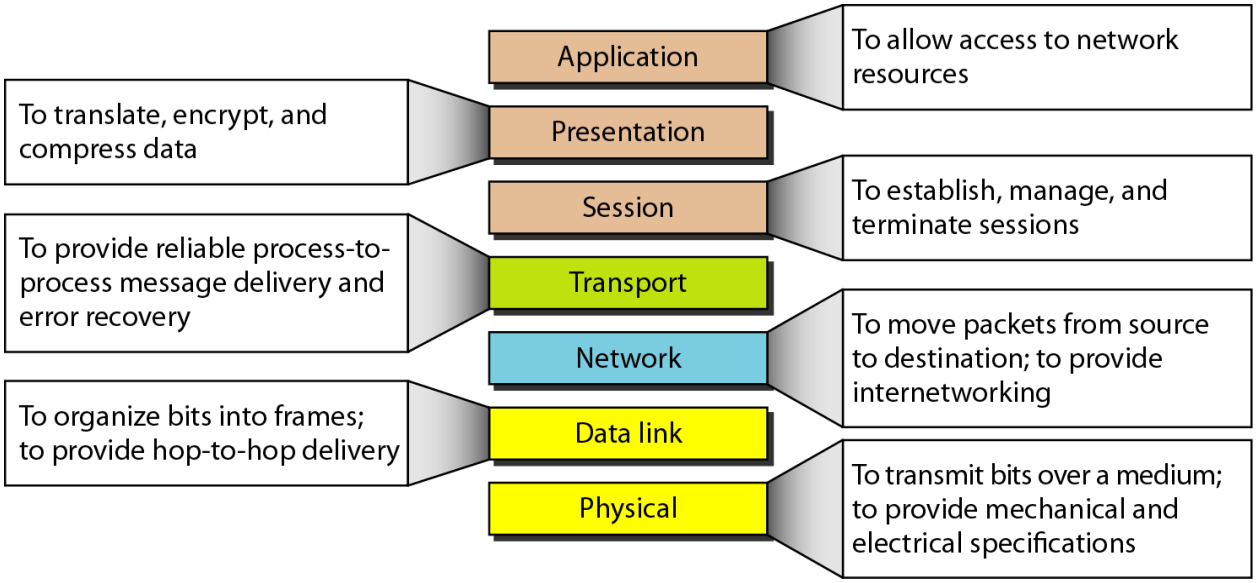


Figure Summary of layers

TCP/IP PROTOCOL SUITE :

The TCPIIP protocol suite was developed prior to the OSI model. Therefore, the layers in the TCP/IP protocol suite do not exactly match those in the OSI model. The original TCP/IP protocol suite was defined as having four layers: host-to-network, internet, transport, and application. However, when TCP/IP is compared to OSI, we can say that the host-to-network layer is equivalent to the combination of the physical and data link layers. The internet layer is

equivalent to the network layer, and the application layer is roughly doing the job of the session, presentation, and application layers with the transport layer in TCPIIP taking care of part of the duties of the session layer. we assume that the TCPIIP protocol suite is made of five layers: physical, data link, network, transport, and application. The first four layers provide physical standards, network interfaces, internetworking, and transport functions that correspond to the first four layers of the OSI model. The three topmost layers in the OSI model, however, are represented in TCPIIP by a single layer called the application layer.

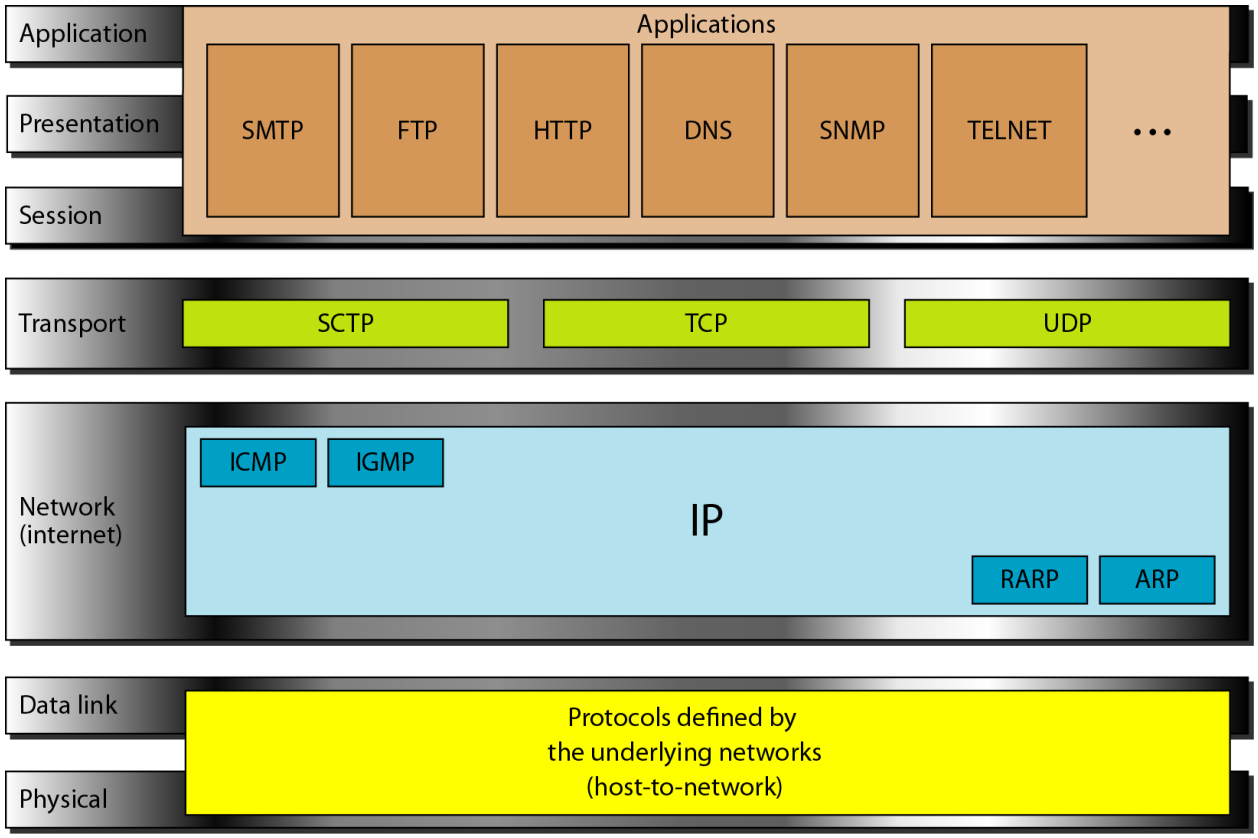


Figure : ***TCP/IP and OSI model***

TCP/IP is a hierarchical protocol made up of interactive modules, each of which provides a specific functionality; however, the modules are not necessarily interdependent. Whereas the OSI model specifies which functions belong to each of its layers, the layers of the TCP/IP protocol suite contain relatively independent protocols that can be mixed and matched depending on the needs of the system. The term hierarchical means that each upper-level protocol is supported by one or more lower-level protocols. At the transport layer, TCP/IP defines three protocols: Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Stream Control Transmission Protocol (SCTP). At the network layer, the main protocol defined by TCP/IP is the Internetworking Protocol (IP); there are also some other protocols that support data movement in this layer.

Physical and Data Link Layers

At the physical and data link layers, TCP/IP does not define any specific protocol. It supports all the standard and proprietary protocols. A network in a TCP/IP internetwork can be a local-area network or a wide-area network.

Network Layer

At the network layer (or, more accurately, the internetwork layer), TCP/IP supports the Internetworking Protocol. IP, in turn, uses four supporting protocols: ARP, RARP, ICMP, and IGMP.

Internetworking Protocol (IP)

The Internetworking Protocol (IP) is the transmission mechanism used by the TCP/IP protocols. Itis an unreliable and connectionless protocol-a best-effort delivery service. The term best effort means that IP provides no error checking or tracking. IP assumes the unreliability of the underlying layers and does its best to get a transmission through to its destination, but with no guarantees. IP transports data in packets called datagrams, each of which is transported separately. Datagrams can travel along different routes and can arrive out of sequence or be duplicated. IP does not keep track of the routes and has no facility for reordering datagrams once they arrive at their destination. The limited functionality of IP should not be considered a weakness, however. IP provides bare-bones transmission functions that free the user to add only those facilities necessary for a given application and thereby allows for maximum efficiency.

Address Resolution Protocol

The Address Resolution Protocol (ARP) is used to associate a logical address with a physical address. On a typical physical network, such as a LAN, each device on a link is identified by a physical or station address, usually imprinted on the network interface card (NIC). ARP is used to find the physical address of the node when its Internet address is known. Reverse Address Resolution Protocol

The Reverse Address Resolution Protocol (RARP) allows a host to discover its Internet address when it knows only its physical address. It is used when a computer is connected to a network for the first time or when a diskless computer is booted. Internet Control Message Protocol

The Internet Control Message Protocol (ICMP) is a mechanism used by hosts and gateways to send notification of datagram problems back to the sender. ICMP sends query and error reporting messages. Internet Group Message Protocol

The Internet Group Message Protocol (IGMP) is used to facilitate the simultaneous transmission of a message to a group of recipients.

Transport Layer

Traditionally the transport layer was represented in TCP/IP by two protocols: TCP and UDP. IP is a host-to-host protocol, meaning that it can deliver a packet from one physical device to another. UDP and TCP are transport level protocols responsible for delivery of a message from a process (running program) to another process. A new transport layer protocol, SCTP, has been devised to meet the needs of some newer applications.

User Datagram Protocol

The User DatagramProtocol (UDP) is the simpler ofthe two standard TCPIIP transport protocols. It is a process-to-process protocol that adds only port addresses, checksum error control, and length information to the data from the upper layer.

Transmission Control Protocol

The Transmission Control Protocol (TCP) provides full transport-layer services to applications. TCP is a reliable stream transport protocol. The term stream, in this context, means connection-oriented: A connection must be established between both ends of a transmission before either can transmit data. At the sending end of each transmission, TCP divides a stream of data into smaller units called segments. Each segment includes a sequence number for reordering after receipt, together with an acknowledgment number for the segments received. Segments are carried across the internet inside of IP datagrams. At the receiving end, TCP collects each datagram as it comes in and reorders the transmission based on sequence numbers.

Stream Control Transmission Protocol

The Stream Control Transmission Protocol (SCTP) provides support for newer applications such as voice over the Internet. It is a transport layer protocol that combines the best features ofUDP and TCP.

Application Layer :

The application layer in TCPIIP is equivalent to the combined session, presentation, and application layers in the OSI model Many protocols are defined at this layer.

ADDRESSING

Four levels of addresses are used in an internet employing the TCP/IP protocols: physical (link) addresses, logical (IP) addresses, port addresses, and specific addresses

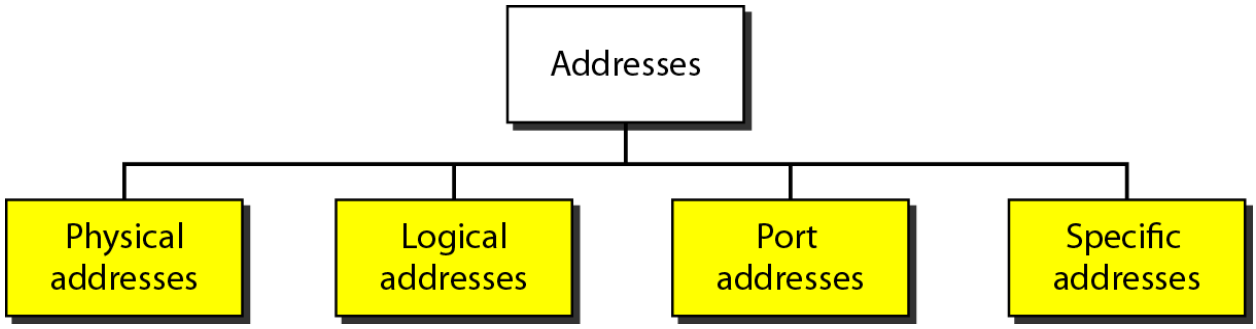


Figure ***Addresses in TCP/IP***

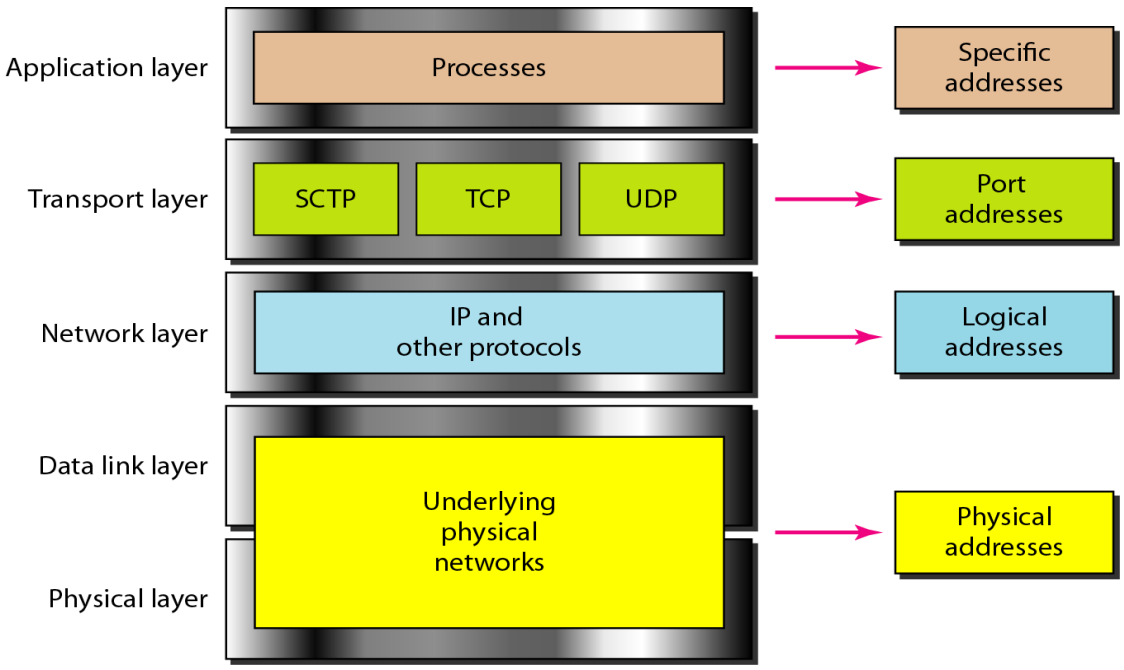


Figure ***Relationship of layers and addresses in TCP/IP***

Physical Addresses

The physical address, also known as the link address, is the address of a node as defined by its LAN or WAN. It is included in the frame used by the data link layer. It is the lowest-level

address. The physical addresses have authority over the network (LAN or WAN). The size and format of these addresses vary depending on the network. For example, Ethernet uses a 6-byte (48-bit) physical address that is imprinted on the network interface card (NIC). LocalTalk (Apple), however, has a I-byte dynamic address that changes each time the station comes up.

Example

In Figure a node with physical address 10 sends a frame to a node with physical address 87. The two nodes are connected by a link (bus topology LAN). At the data link layer, this frame contains physical (link) addresses in the header. These are the only addresses needed. The rest of the header contains other information needed at this level. The trailer usually contains extra bits needed for error detection. As the figure shows, the computer with physical address lO is the sender, and the computer with physical address 87 is the receiver. The data link layer at the sender receives data from an upper layer. It encapsulates the data in a frame, adding a header and a trailer. The header, among other pieces of information, carries the receiver and the sender physical (link) addresses. Note that in most data link protocols, the destination address, 87 in this case, comes before the source address (10 in this case). A bus topology for an isolated LAN. In a bus topology, the frame is propagated in both directions (left and right). The frame propagated to the left dies when it reaches the end of the cable if the cable end is terminated appropriately. The frame propagated to the right is sent to every station on the network. Each station with a physical addresses other than 87 drops the frame because the destination address in the frame does not match its own physical address. The intended destination computer, however, finds a match between the destination address in the frame and its own physical address. The frame is checked, the header and trailer are dropped, and the data part is decapsulated and delivered to the upper layer.

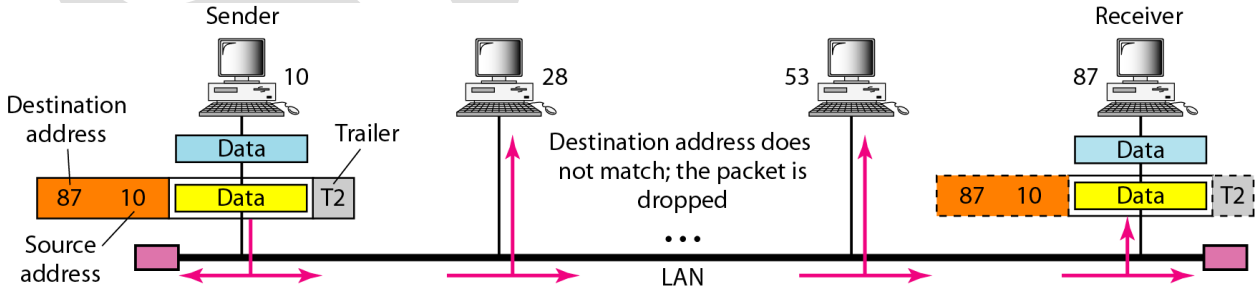


Figure: ***Physical addresses***

‘

Logical Addresses

Logical addresses are necessary for universal communications that are independent of underlying physical networks. Physical addresses are not adequate in an internetwork environment where different networks can have different address formats. A universal addressing system is needed in which each host can be identified uniquely, regardless of the underlying physical network. The logical addresses are designed for this purpose. A logical address in the Internet is currently a 32-bit address that can uniquely define a host connected to the Internet. No two publicly addressed and visible hosts on the Internet can have the same IP address.

Example

Figure below shows a part of an internet with two routers connecting three LANs. Each device (computer or router) has a pair of addresses (logical and physical) for each connection. In this case, each computer is connected to only one link and therefore has only one pair of addresses. Each router, however, is connected to three networks (only two are shown in the figure). So each router has three pairs of addresses, one for each connection. Although it may obvious that each router must have a separate physical address for each connection, it may not be obvious why it needs a logical address for each connection.

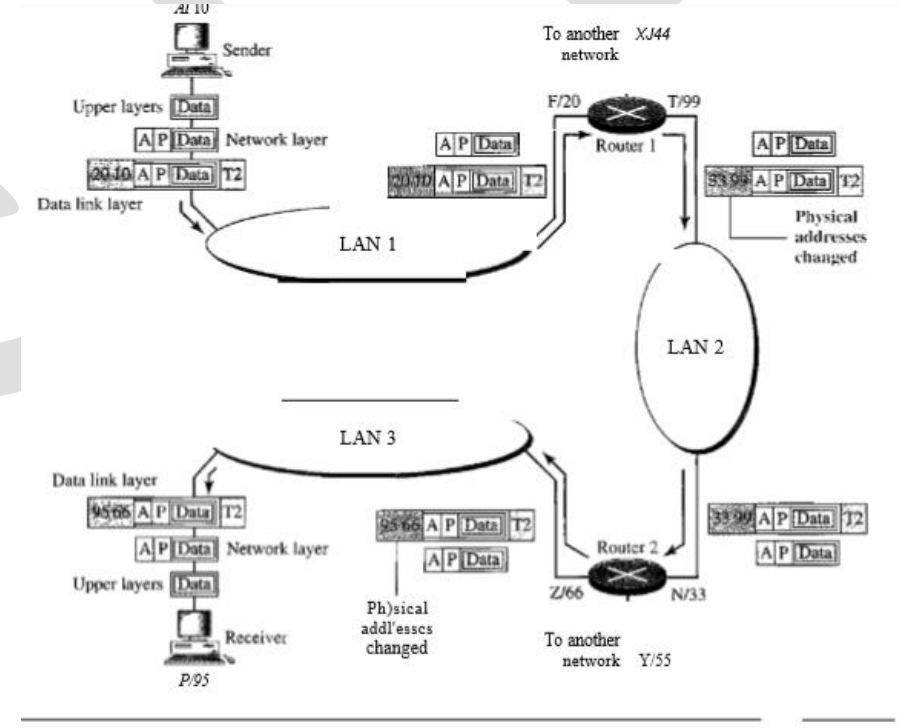


Figure: IP address

The computer with logical address A and physical address 10 needs to send a packet to the computer with logical address P and physical address 95. letters are used to show the logical addresses and numbers for physical addresses, but note that both are actually numbers, as we will see later in the chapter. The sender encapsulates its data in a packet at the network layer and adds two logical addresses (A and P). Note that in most protocols, the logical source address comes before the logical destination address (contrary to the order of physical addresses). The network layer, however, needs to find the physical address ofthe next hop before the packet can be delivered. The network layer consults its routing table and finds the logical address of the next hop (router I) to be F. The ARP discussed previously finds the physical address of router 1 that corresponds to the logical address of 20. Now the network layer passes this address to the data link layer, which in tum, encapsulates the packet with physical destination address 20 and physical source address 10. The frame is received by every device on LAN 1, but is discarded by all except router 1, which finds that the destination physical address in the frame matches with its own physical address. The router decapsulates the packet from the frame to read the logical destination address P. Since the logical destination address does not match the router's logical address, the router knows that the packet needs to be forwarded. The router consults its routing table and ARP to find the physical destination address of the next hop (router 2), creates a new frame, encapsulates the packet, and sends it to router 2. Note the physical addresses in the frame. The source physical address changes from 10 to 99. The destination physical address changes from 20 (router 1 physical address) to 33 (router 2 physical address). The logical source and destination addresses must remain the same; otherwise the packet will be lost. At router 2 we have a similar scenario. The physical addresses are changed, and a new frame is sent to the destination computer. When the frame reaches the destination, the packet is decapsulated. The destination logical address P matches the logical address ofthe computer. The data are decapsulated from the packet and delivered to the upper layer. *Note that although physical addresses will change from hop to hop, logical addresses remain the same from the source to destination*.

Port Addresses

The IP address and the physical address are necessary for a quantity of data to travel from a source to the destination host. However, arrival at the destination host is not the final objective of data communications on the Internet. A system that sends nothing but data from one computer to another is not complete. Today, computers are devices that can run multiple processes at the same time. The end objective of Internet communication is a process communicating with another process. For example, computer A can communicate with computer C by using TELNET. At the same time, computer A communicates with computer B by using the File Transfer Protocol (FTP). For these processes to receive data simultaneously,

we need a method to label the different processes. In other words, they need addresses. In the TCPIIP architecture, the label assigned to a process is called a port address. A port address in TCPIIP is 16 bits in length.

The physical addresses change from hop to hop, but the logical and port addresses usually remain the same.

Wireless Networks

CSE 3461: Introduction to Computer Networking

Reading: § § 6.1–6.3, Kurose and Ross (≤ 6th ed.); § § 7.1–7.3, Kurose and Ross (7th ed.)

Questions

- How do you use wireless network technology in daily life?
- How many of you have smartphones? Laptops?
  - Smartphones: iOS or Android?
  - Laptops: MS Windows, macOS, or Linux?
- Have you have set up a wireless LAN? What was the experience like?

Wireless Networks

Background:

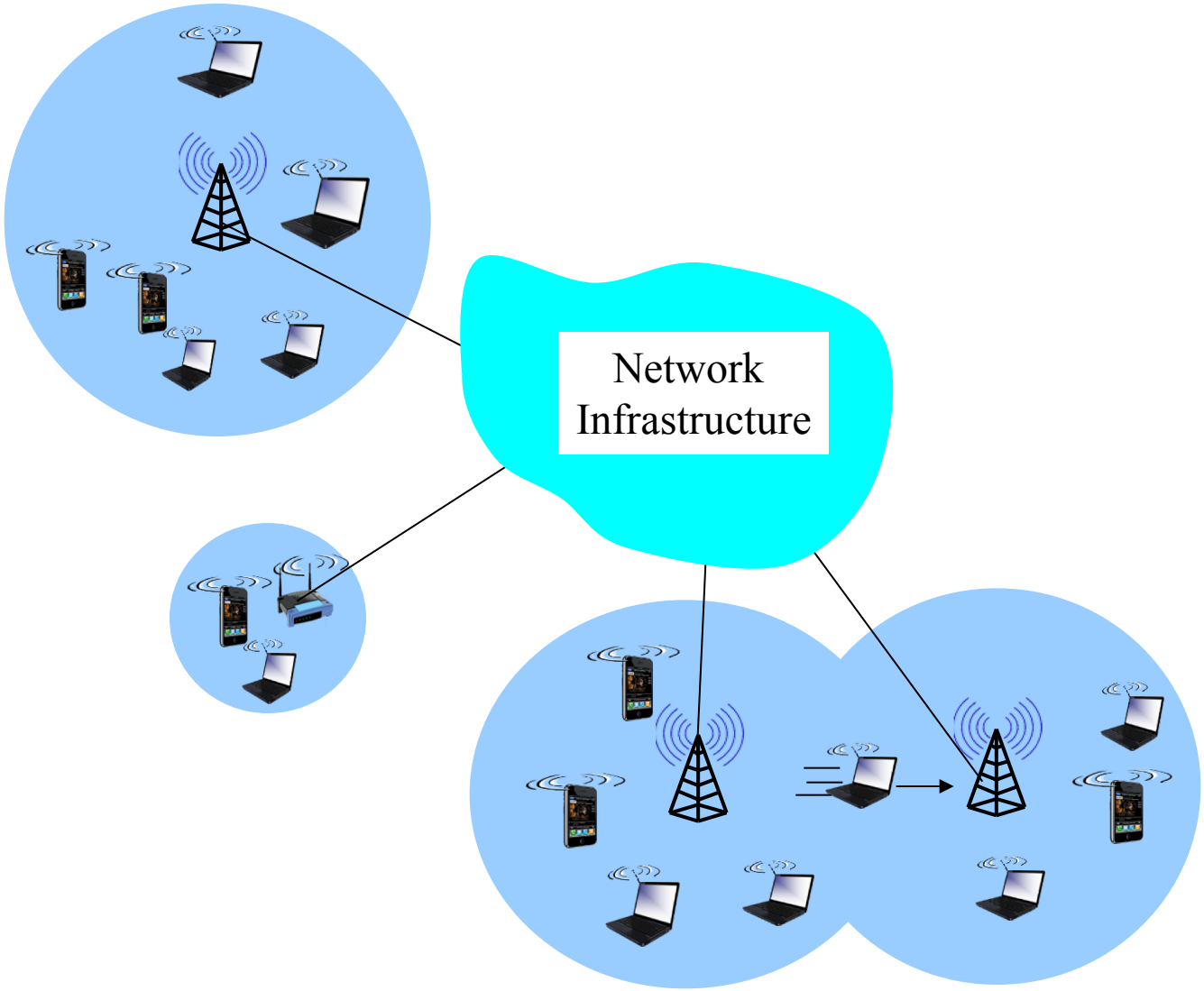
- Number of wireless (mobile) phone subscribers now exceeds number of wired phone subscribers
  - 4.3 billion mobile broadband subscriptions worldwide (ITU, 2017) [1]
  - 334.6 million smartphones sold in Q1 2016 alone [2]
- Number of wireless Internet-connected devices equals number of wireline Internet-connected devices
  - Laptops, smartphones promise anytime untethered Internet access
- Key idea: ***Wireless:*** communication over wireless link

[1] ITU, https://www.itu.int/en/mediacentre/Pages/2017-PR37.aspx
[2] D. Van Boom, "It's not just Apple: Global smartphone market shrinks for the first time ever," 27 Apr. 2016, *CNET* / CBS Interactive, https://cnet.co/2mldOa3

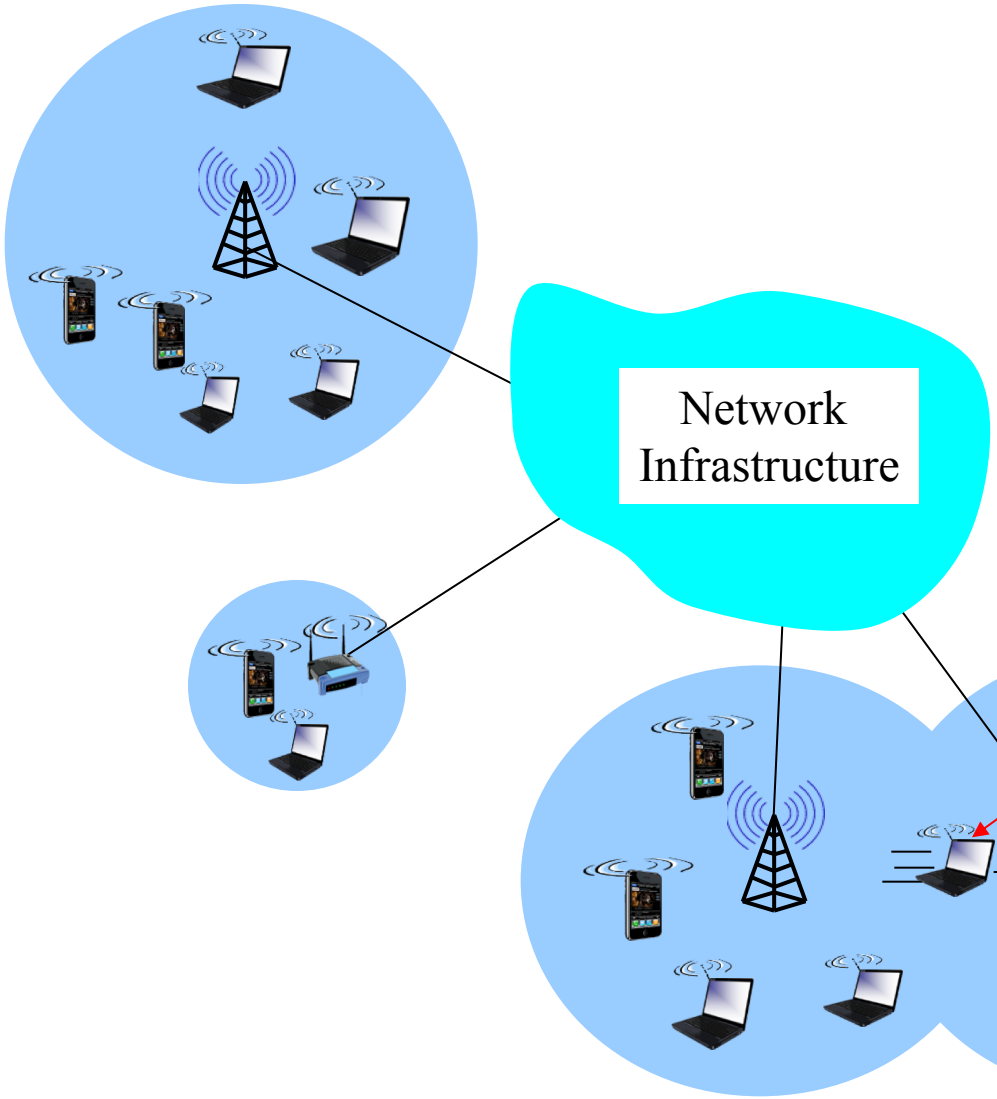
Outline

- **Introduction**
- Wireless links, characteristics
  - CDMA
- IEEE 802.11 wireless LANs (“Wi-Fi”)
- Tools of the Trade

Elements of a Wireless Network (1)



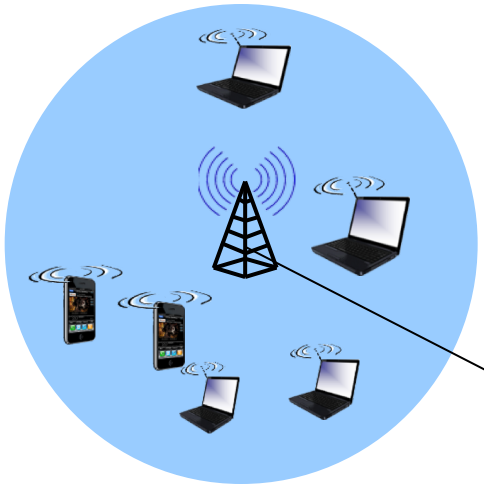
Elements of a Wireless Network (2)

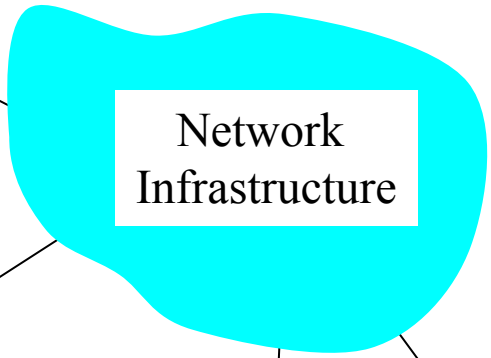


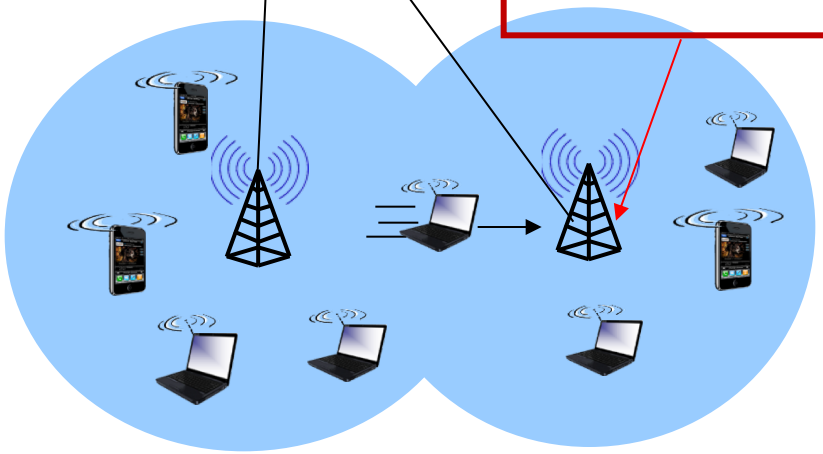
Wireless Hosts

- Laptop, smartphone
- Run applications
- May be stationary (non-mobile) or mobile
  - Wireless does *not* always mean mobility

Elements of a Wireless Network (3)



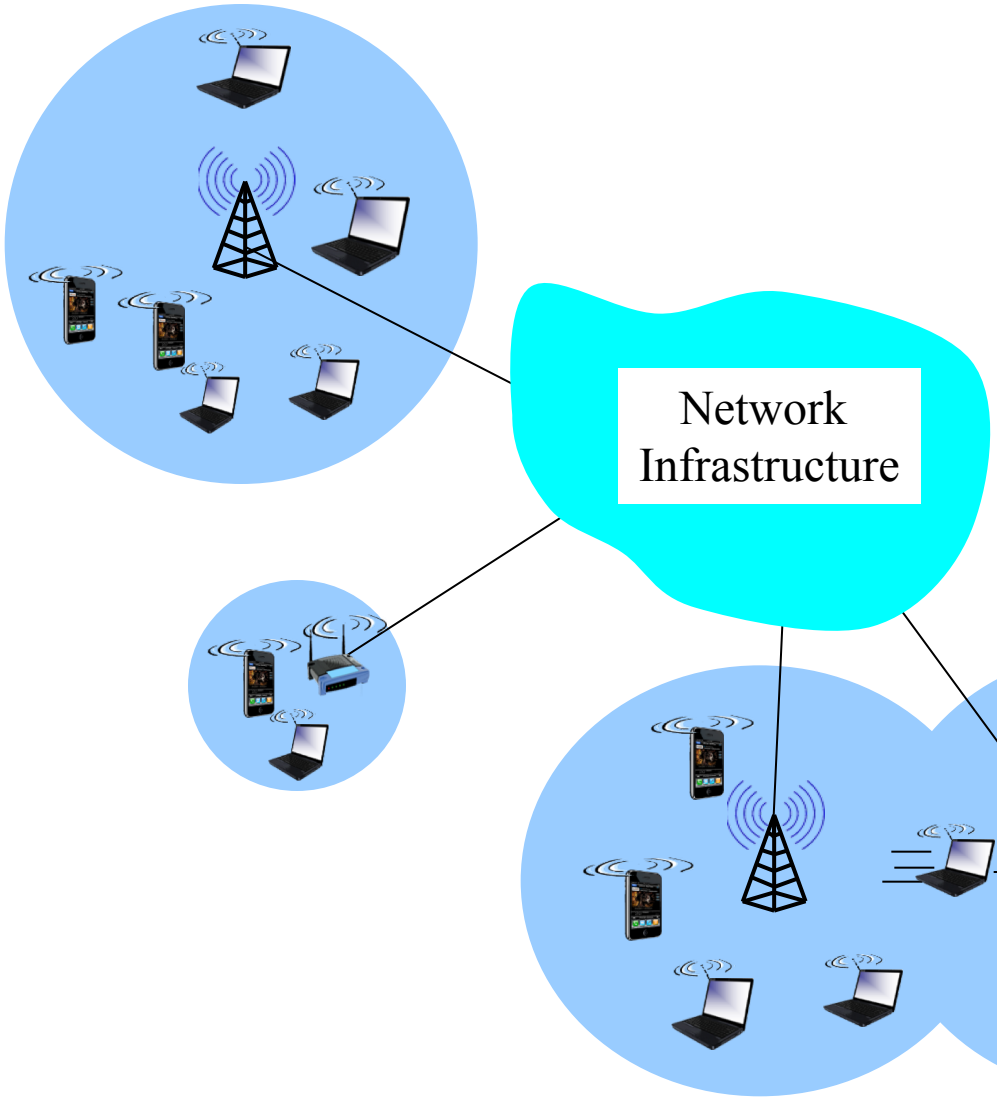




Base Station

- Typically connected to wired network
- Relay - responsible for sending packets between wired network and wireless host(s) in its "area"
  - e.g., cell towers, 802.11 access points

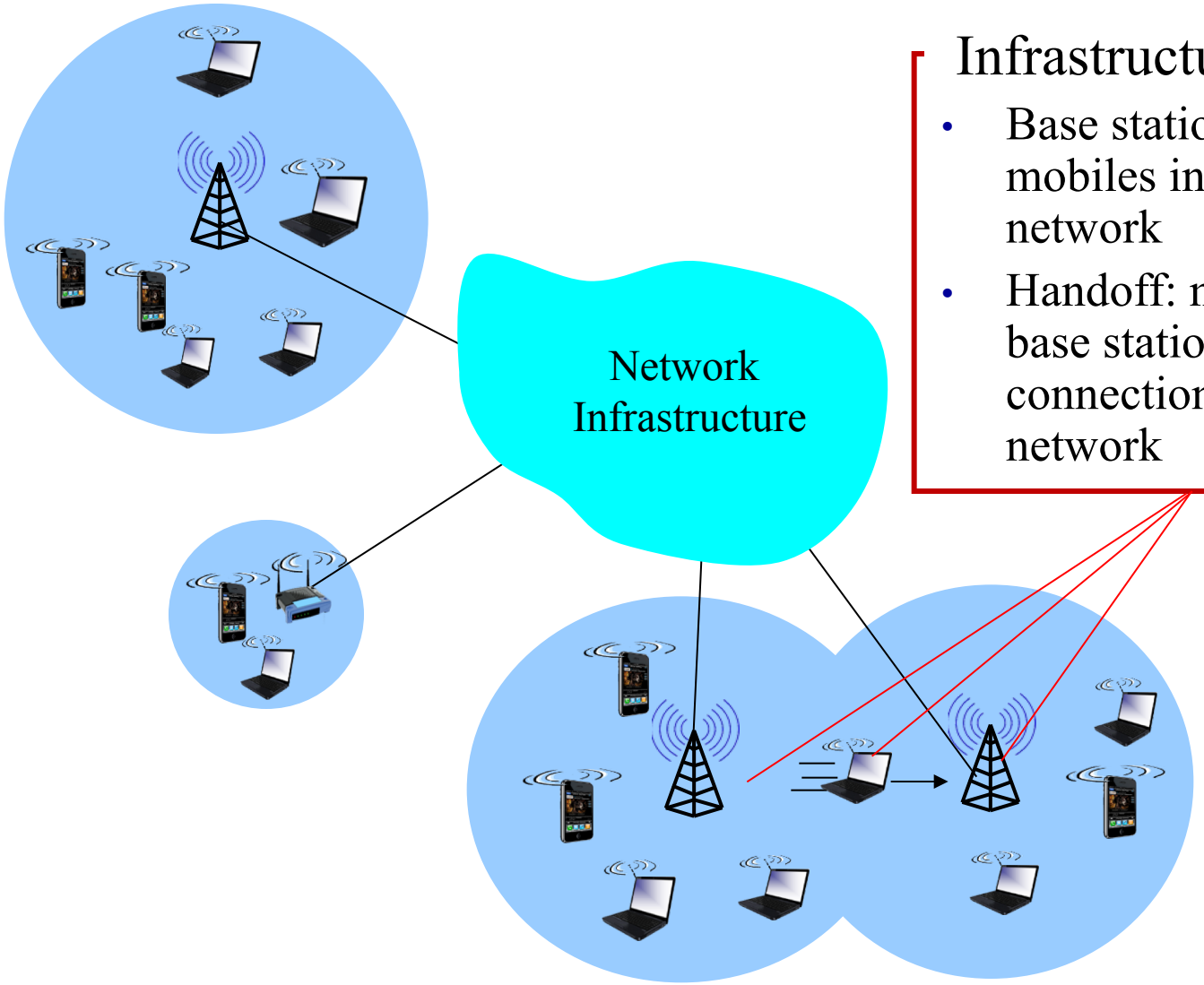
Elements of a Wireless Network (4)



Wireless link

- Typically used to connect mobile(s) to base station
- Also used as backbone link
- Multiple access protocol coordinates link access
- Various data rates, transmission distance

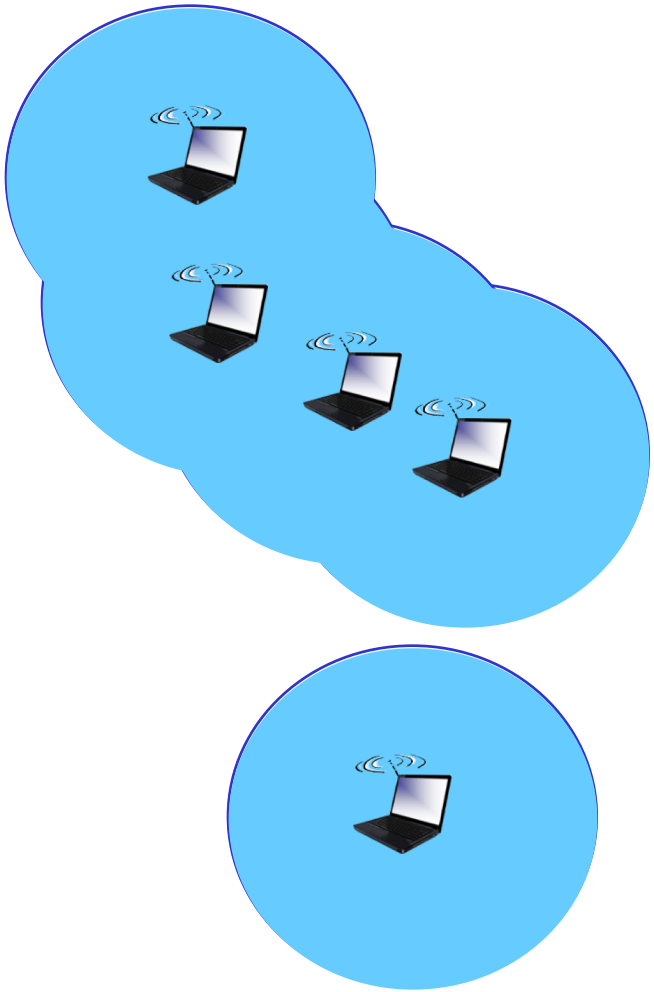
Elements of a Wireless Network (5)



Infrastructure mode

- Base station connects mobiles into wired network
- Handoff: mobile changes base station providing connection into wired network

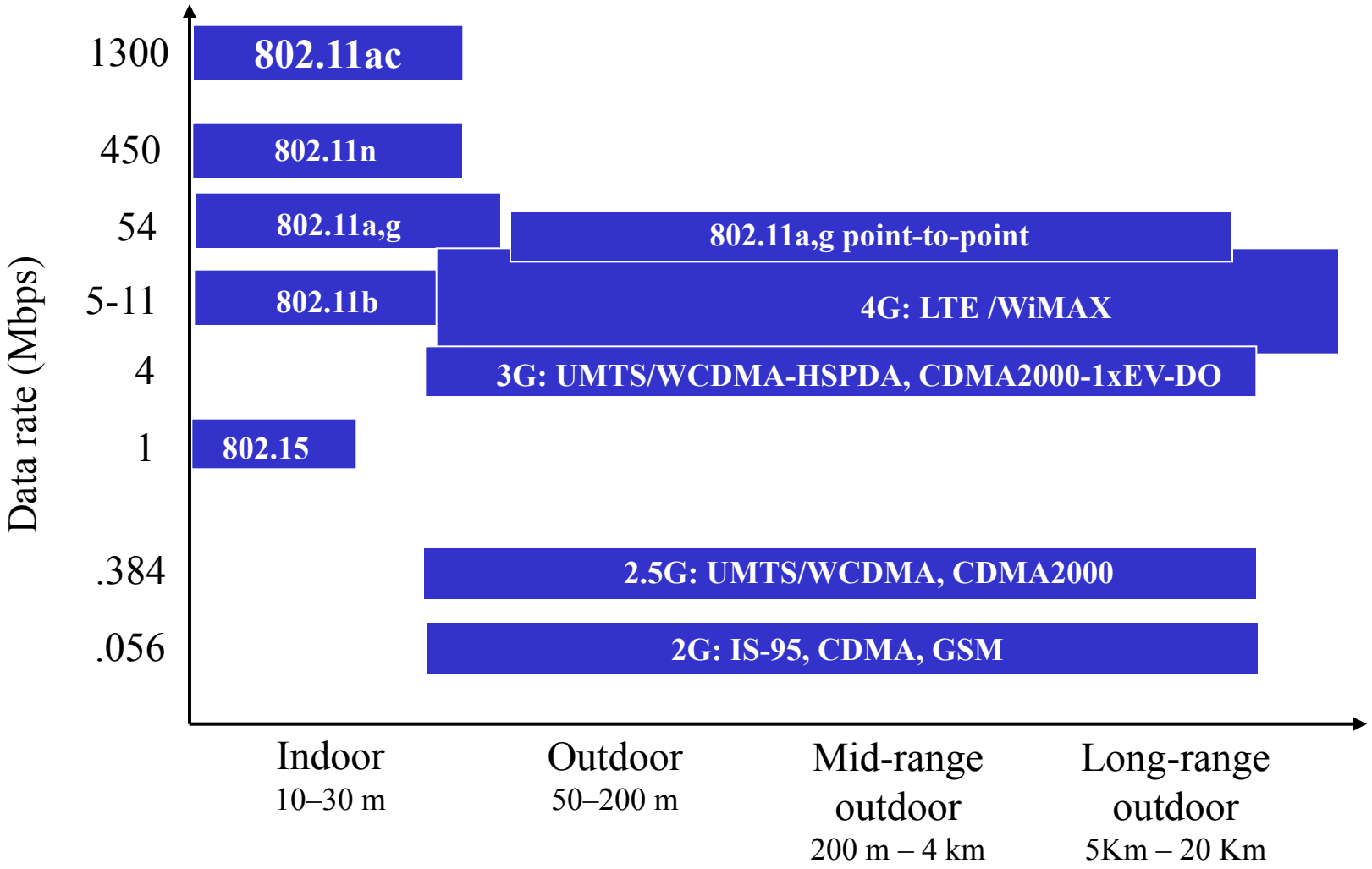
Elements of a Wireless Network (6)



Ad Hoc Mode

- No base stations
- Nodes can only transmit to other nodes within link coverage
- Nodes organize themselves into a network: route among themselves

Characteristics of Selected Wireless Links



Wireless Network Taxonomy

	Single Hop	Multiple Hops
Infrastructure (e.g., APs)	Host connects to base station (WiFi, WiMAX, cellular), which connects to larger Internet	Host may have to relay through several wireless nodes to connect to larger Internet: *mesh net*
No Infrastructure	No base station, no connection to larger Internet (*Bluetooth, ad hoc nets*)	No base station, no connection to larger Internet. May have to relay to reach another given wireless node (MANET, VANET)

Outline

- Introduction
- **Wireless links, characteristics**
  - **CDMA**
- IEEE 802.11 wireless LANs (“Wi-Fi”)
- Tools of the Trade

Wireless Link Characteristics (1)

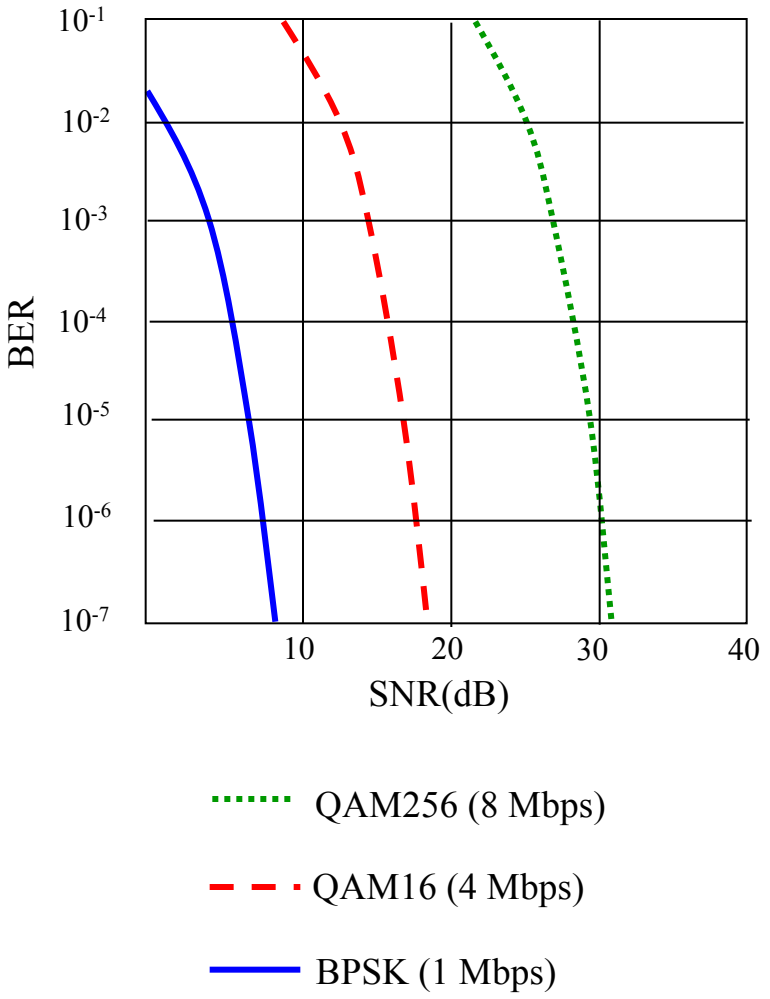
Important differences from wired link …

- ***Decreased signal strength:*** Radio signal attenuates as it propagates through matter (*path loss*)
- ***Interference from other sources:*** Standardized wireless network frequencies (e.g., 2.4 GHz) shared by other devices (e.g., phones); devices (motors, microwaves, etc.) interfere as well
- ***Multipath propagation:*** Radio signal reflects off objects ground, arriving ad destination at slightly different times

…. make communication across (even a point to point) wireless link much more "difficult"

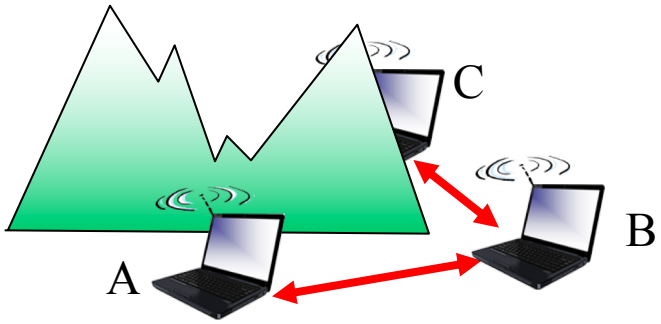
Wireless Link Characteristics (2)

- SNR: signal-to-noise ratio
  - Larger SNR ⟹ easier to extract signal from noise ("good thing")
- BER: bit error rate
- ***SNR versus BER tradeoffs:***
  - ***Given physical layer:*** increase power ⟹ increase SNR ⟹ decrease BER
  - ***Given SNR:*** choose physical layer that meets BER requirement, giving highest throughput
    - SNR may change with mobility: dynamically adapt physical layer (modulation technique, data rate)
- Details:
  - QAM: quadrature amplitude modulation
  - BPSK: binary phase shift keying



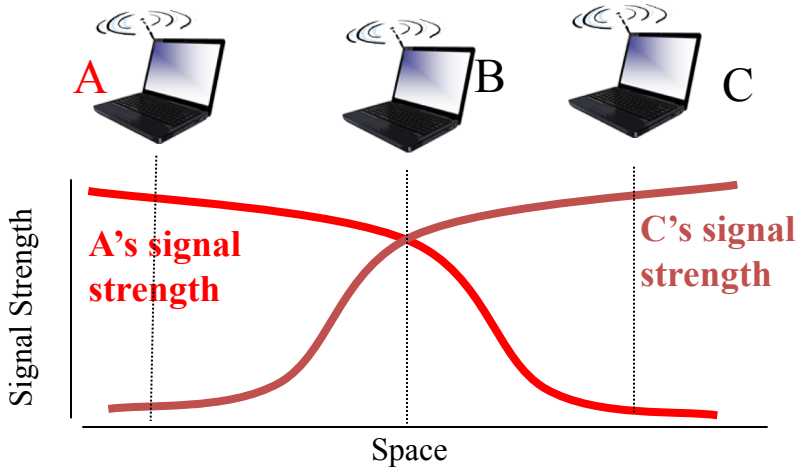
Wireless Network Characteristics

Multiple wireless senders and receivers create additional problems (beyond multiple access):



Hidden terminal problem

- B, A hear each other
- B, C hear each other
- A, C cannot hear each other means A, C unaware of their interference at B



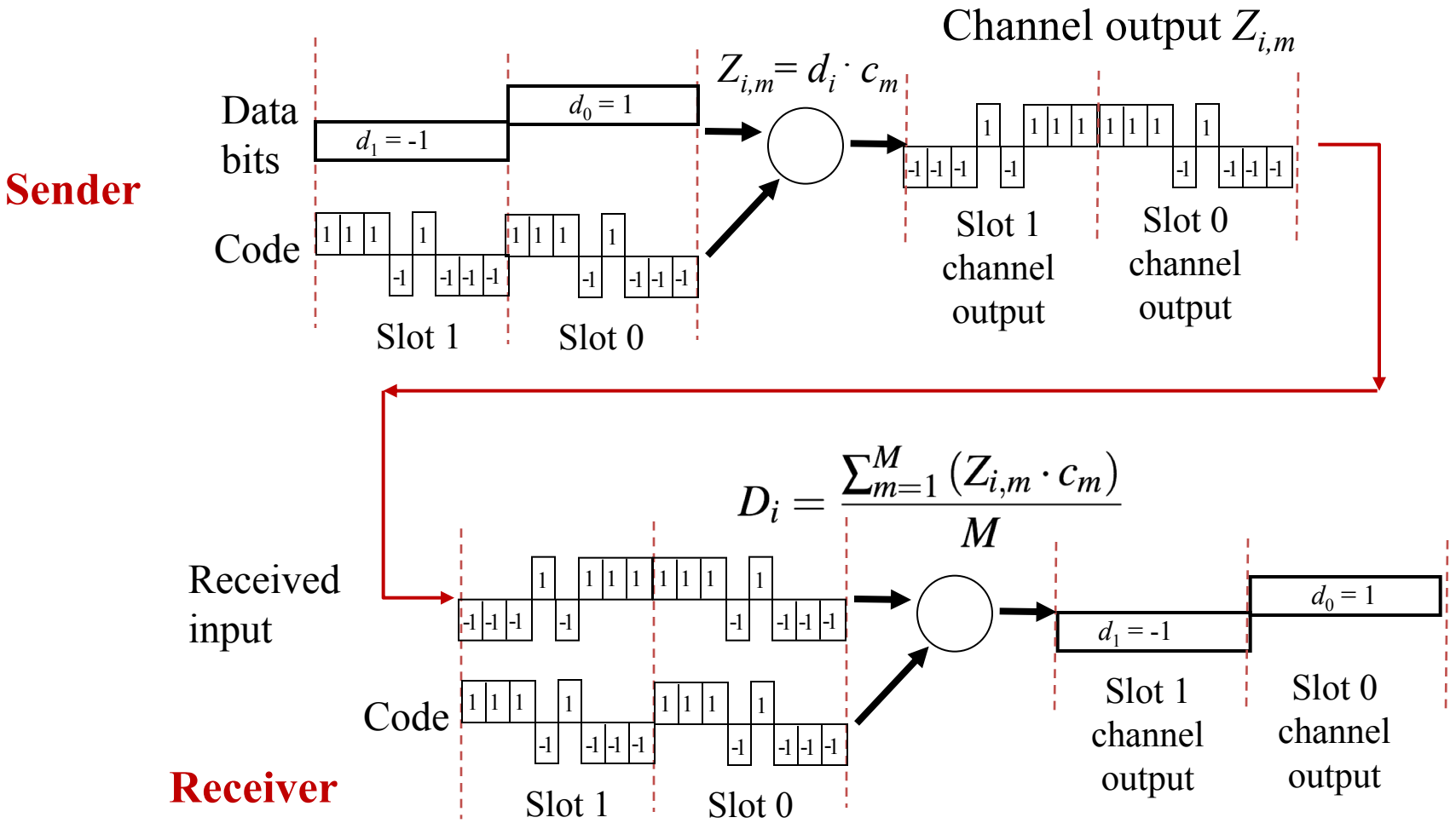
Signal attenuation:

- B, A hear each other
- B, C hear each other
- A, C cannot hear each other interfering at B

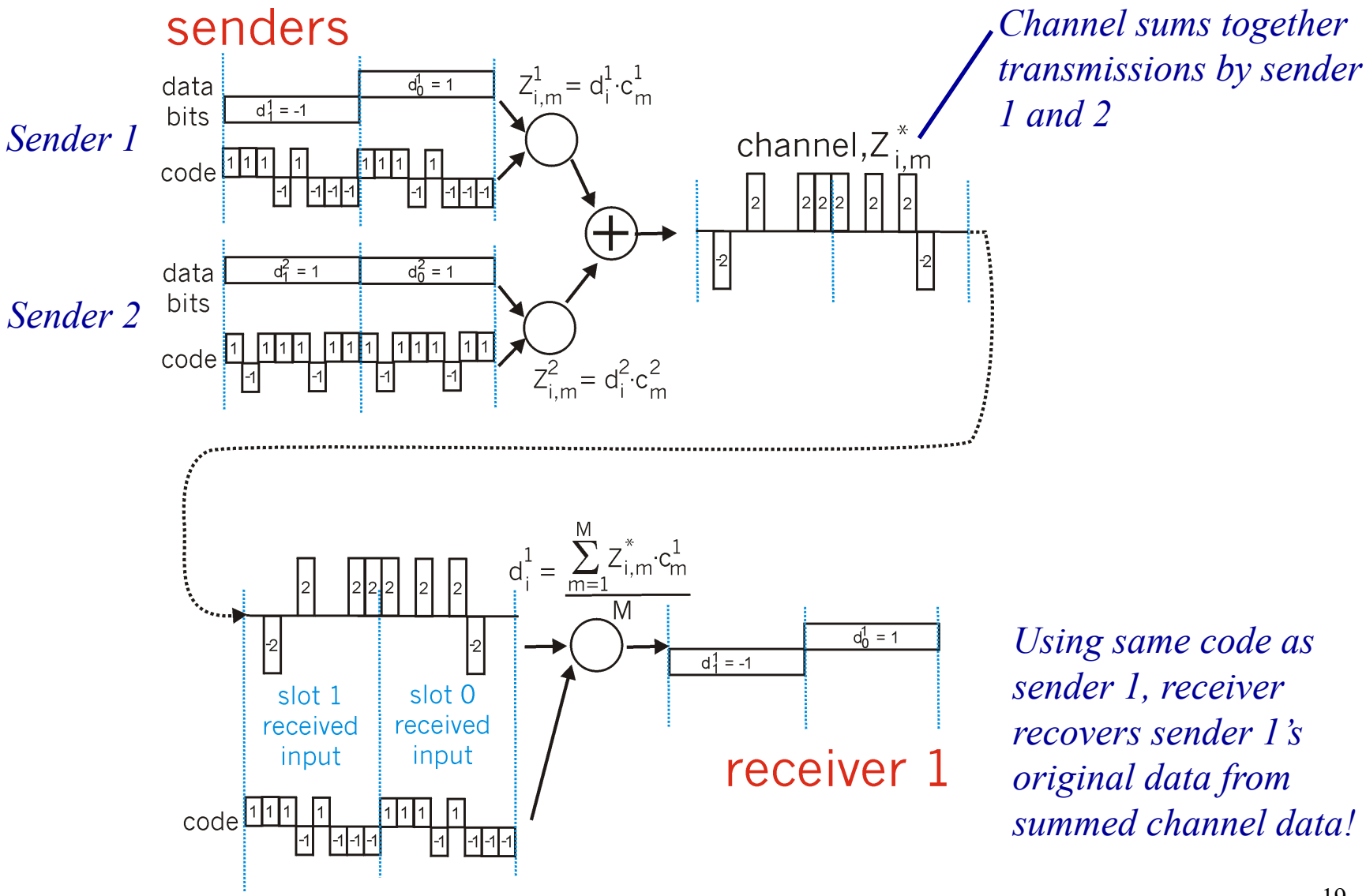
Code Division Multiple Access (CDMA)

- Unique "pseudo-noise code" (PN code) assigned to each user; i.e., code set partitioning
  - All users share same frequency, but each user has own "chip" sequence (i.e., PN code) to encode data
  - Allows multiple users to "coexist" and transmit simultaneously with minimal interference (if codes are "orthogonal")
- ***Encoded signal*** = (original data) × (chip sequence)
- ***Decoding:*** inner product of encoded signal and chip sequence

CDMA Encoding/ Decoding



CDMA: Two-Sender Interference



Outline

- Introduction
- Wireless links, characteristics
  - CDMA
- **IEEE 802.11 wireless LANs (“Wi-Fi”)**
- Tools of the Trade

IEEE 802.11 Wireless LAN (WLAN)

802.11a

- Freq.: 5–6 GHz
- Data rate: up to 54 Mbps

802.11b

- 2.4, 5 GHz unlicensed spectrum
- Data rate: up to 11 Mbps
- Direct sequence spread spectrum (DSSS) in physical layer
  - All hosts use same chip code

802.11g

- Freq.: 2.4, 5 GHz
- Data rate: up to 54 Mbps

802.11n: multiple antennas

- 2.4, 5 GHz range
- Data rate: up to 450 Mbps

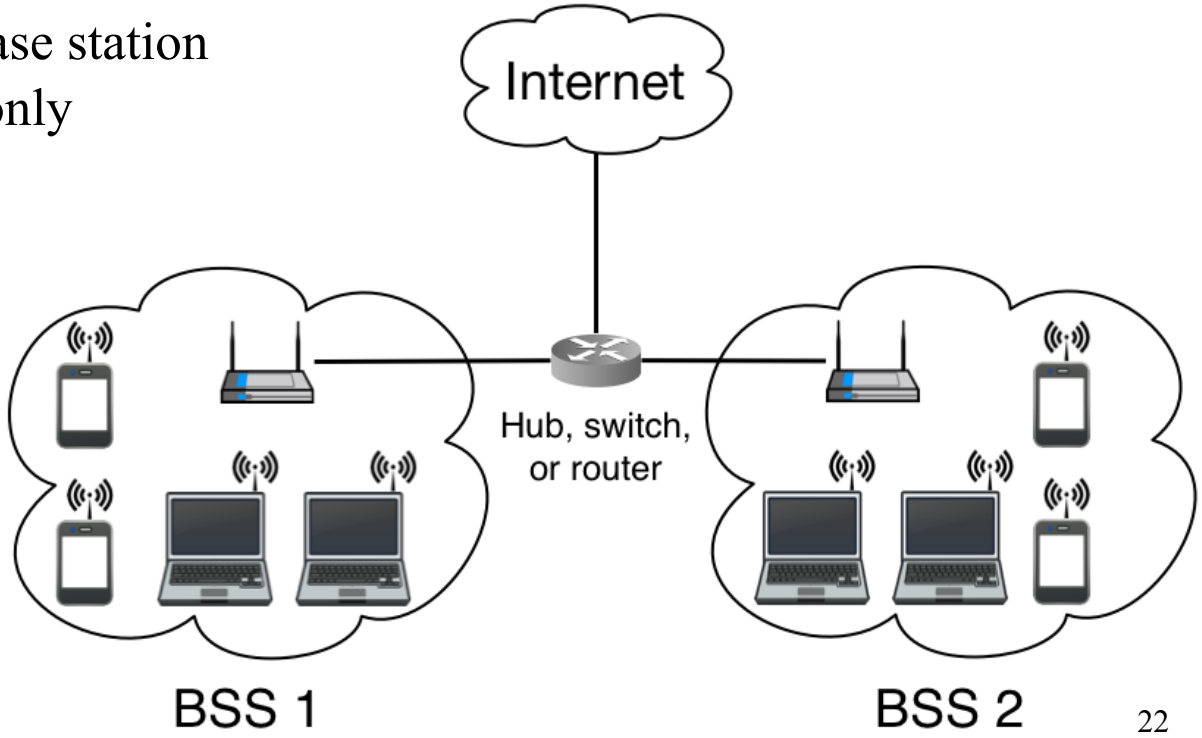
802.11ac: higher data rate (> 400 Mbps), 5-GHz only

802.11ad: ≥ 1 Gbps data rate, 60-GHz band, range: 10s of cm

- All use CSMA/CA for multiple access
- All have base-station and ad-hoc network versions

802.11 WLAN Architecture

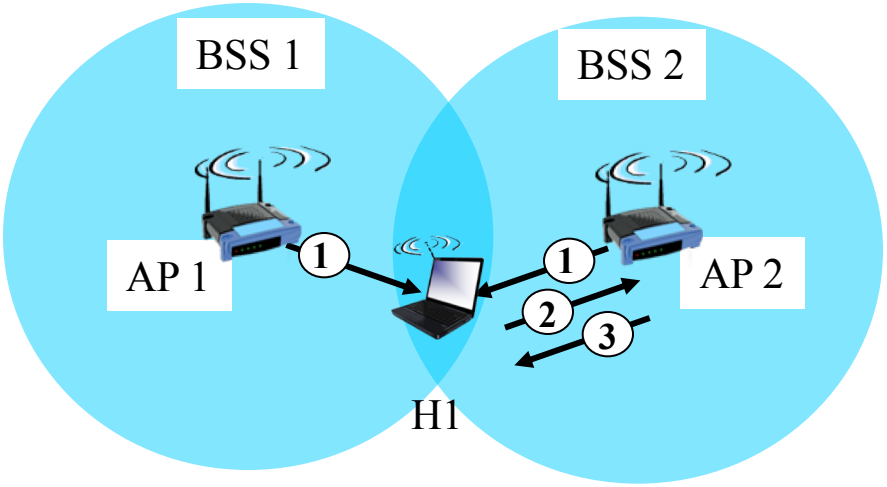
- Wireless hosts communicate with base station
  - **Base station: access point (AP)**
- **Basic Service Set (BSS)** (aka "cell") in infrastructure mode contains:
  - Wireless hosts
  - Access point (AP): base station
  - Ad hoc mode: hosts only

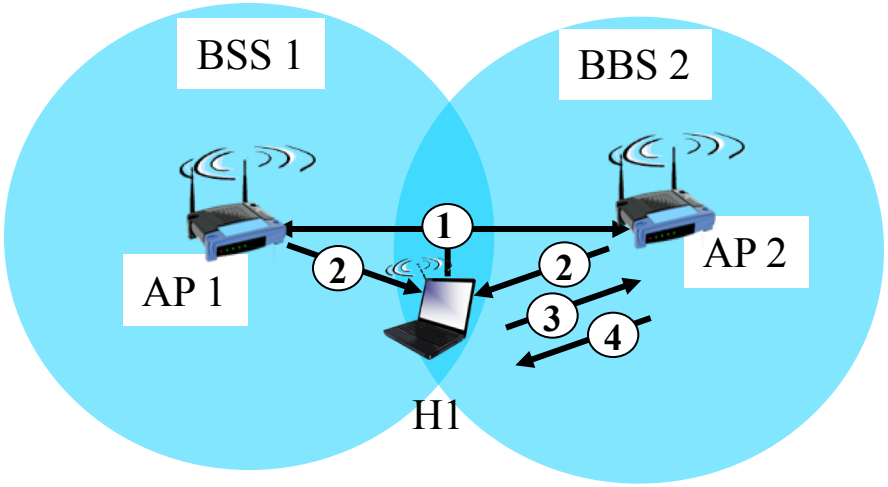


802.11: Channels and Association

- 802.11: 2.4–2.485 GHz spectrum divided into 11 channels at different frequencies
  - AP admin chooses frequency for AP
  - Interference possible: channel can be same as that chosen by neighboring AP!
  - Numerous channels in 5-GHz frequency band
- Host must ***associate*** with an AP
  - Scans channels, listening for ***beacon frames*** containing AP's name (SSID) and MAC address
  - Selects AP to associate with
  - May perform authentication
  - Typically runs DHCP to get IP address in AP's subnet

802.11: Passive/Active Scanning





Passive scanning:

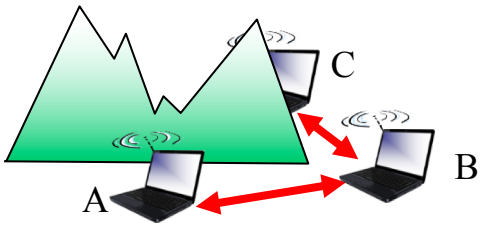
1. Beacon frames sent from APs
2. Association Request frame sent: H1 to selected AP
3. Association Response frame sent from selected AP to H1

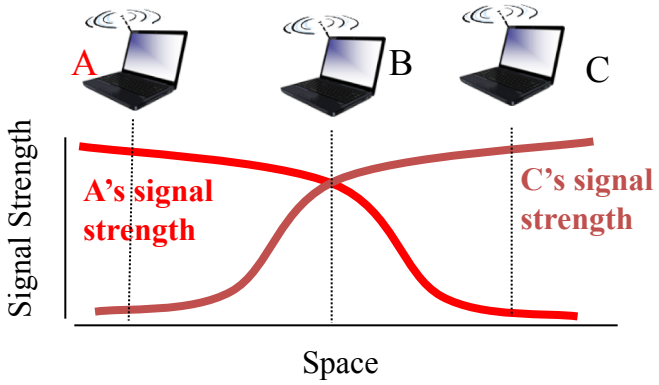
Active scanning:

1. Probe Request frame broadcast from H1
2. Probe Response frames sent from APs
3. Association Request frame sent: H1 to selected AP
4. Association Response frame sent from selected AP to H1

IEEE 802.11: Multiple Access

- Avoid collisions: 2 or more nodes transmitting at same time
- 802.11: CSMA – sense before transmitting
  - Don't collide with ongoing transmission by other node
- 802.11: *no* collision detection!
  - Difficult to receive (sense collisions) when transmitting due to weak received signals (fading)
  - Can't sense all collisions in any case: hidden terminal, fading
  - Goal: ***avoid collisions:*** CSMA/CA (Collision Avoidance)





IEEE 802.11 MAC Protocol: CSMA/CA

802.11 sender

1. **if** sense channel idle for **DIFS*** **then**

   transmit entire frame (no CD)

2. **if** sense channel busy **then**

   start random backoff time

   timer counts down while channel idle

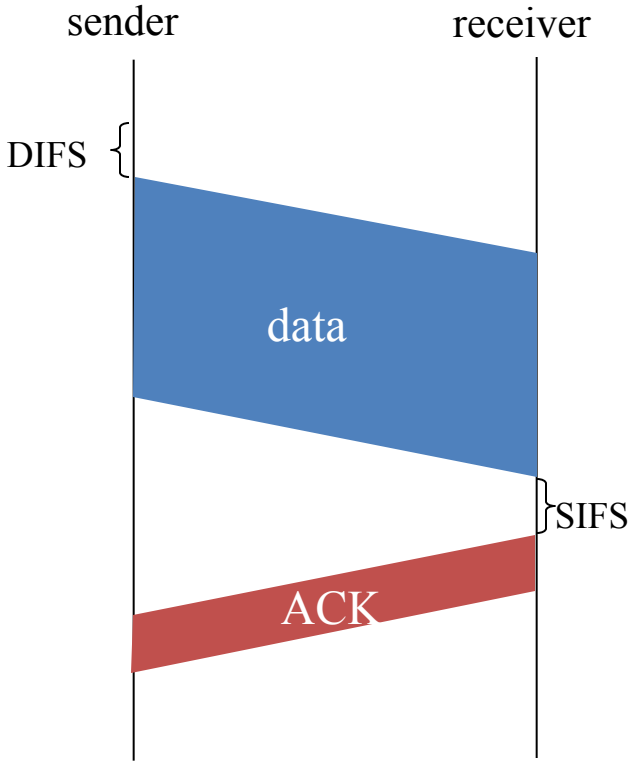
   transmit when timer expires

   if no ACK, **then** increase random backoff interval; **repeat** 2

802.11 receiver

1. **if** frame received OK:

   return ACK after **SIFS*** (ACK needed due to hidden terminal problem)



* DIFS: DCF Inter-Frame Space; SIFS: Short Inter-Frame space; DCF: Distributed Coordination Function

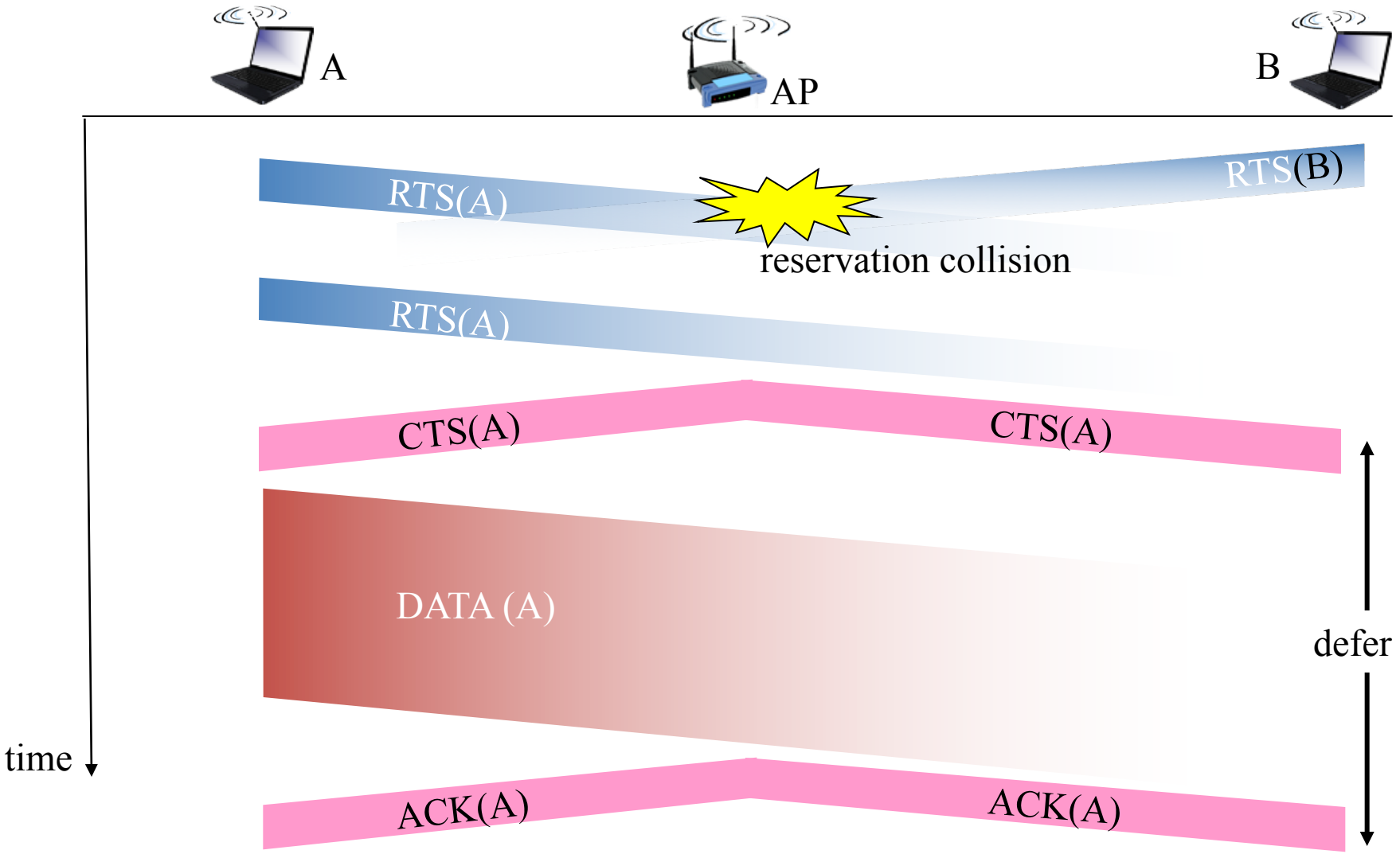
802.11: Collision Avoidance

Idea: allow sender to "reserve" channel rather than random access of data frames: avoid collisions of long data frames

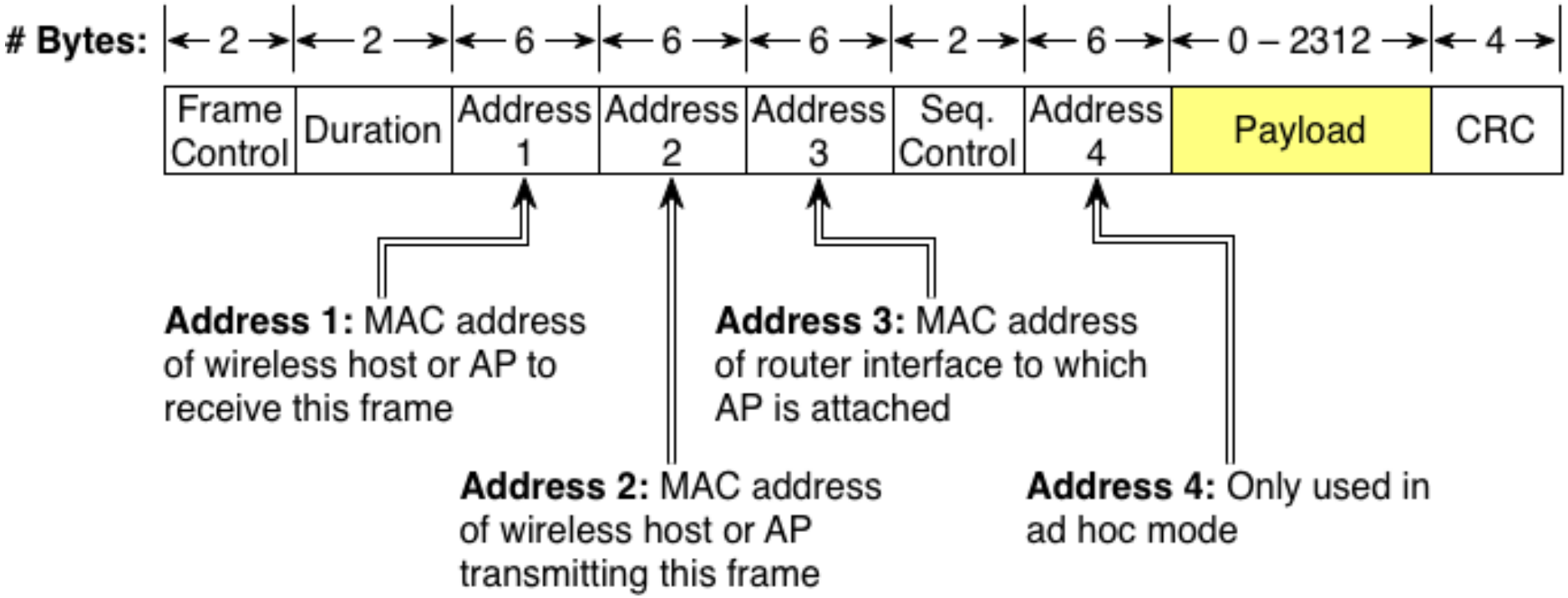
- Sender first transmits *small* request-to-send (RTS) packets to BS using CSMA
  - RTSs may still collide with each other (but they're short)
- BS broadcasts clear-to-send CTS in response to RTS
- CTS heard by all nodes
  - Sender transmits data frame
  - Sther stations defer transmissions

Avoid data frame collisions completely using small reservation packets!

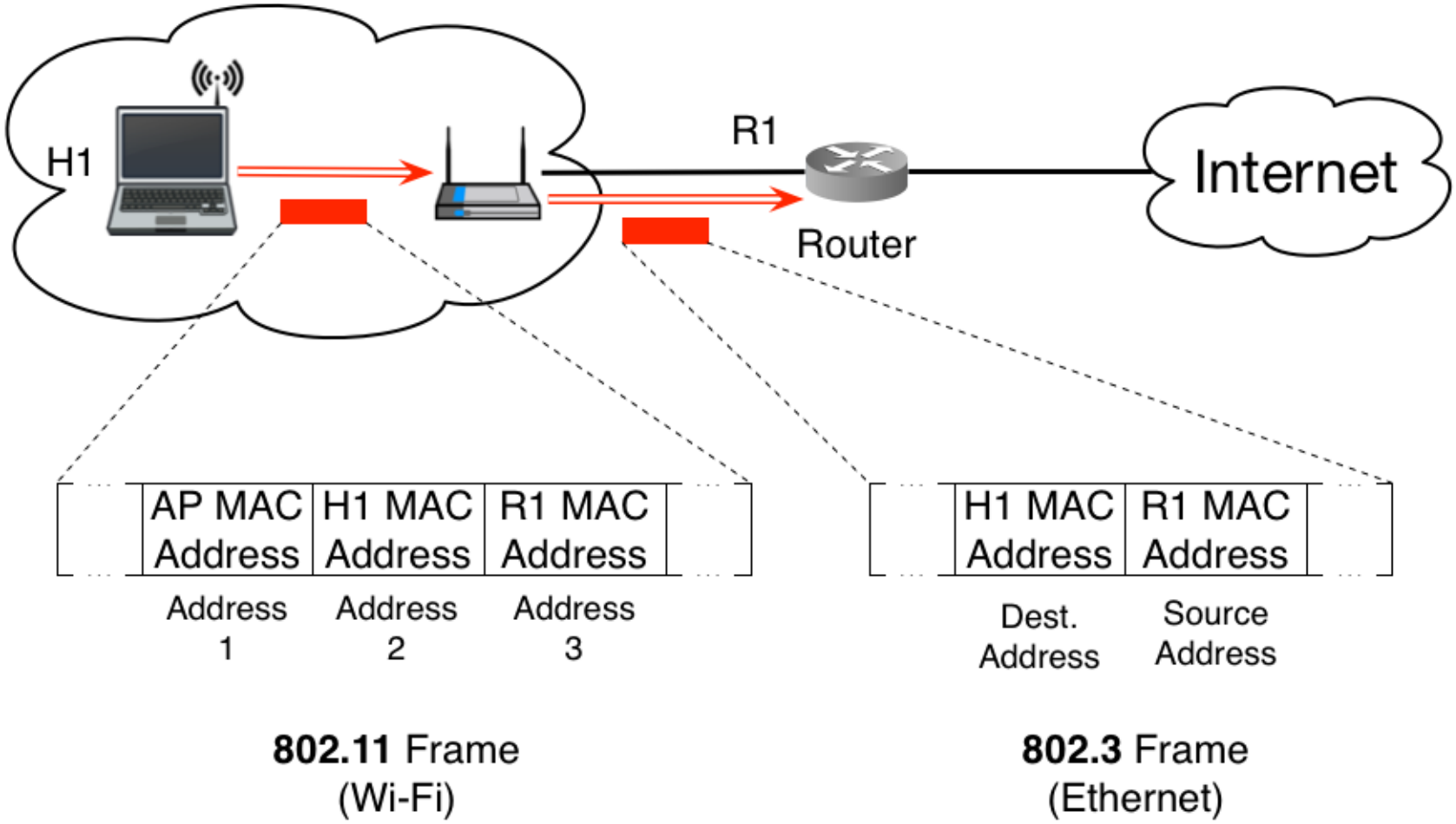
802.11: Collision Avoidance: RTS-CTS Exchange



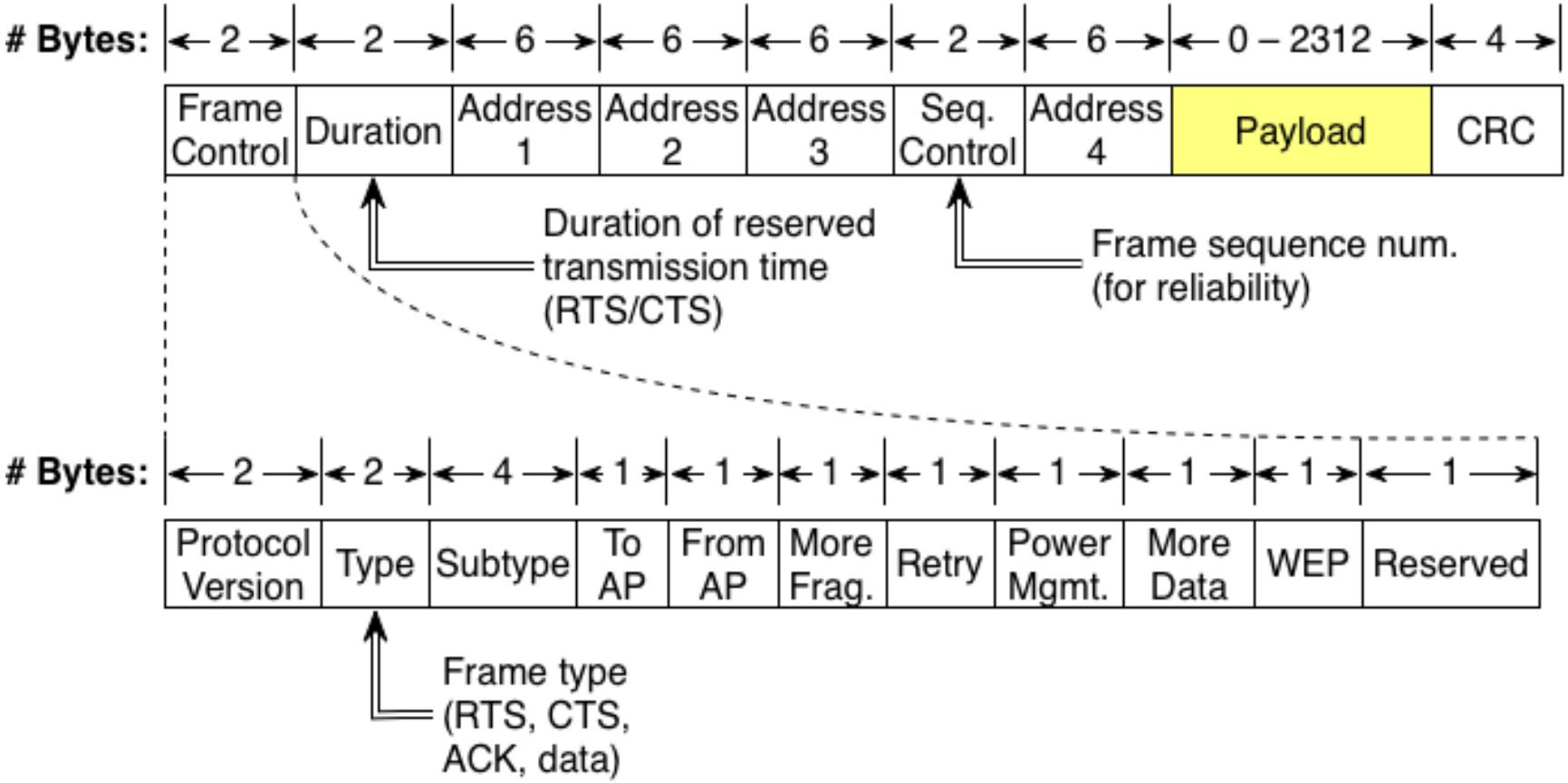
802.11 Frame: Addressing (1)



802.11 Frame: Addressing (2)

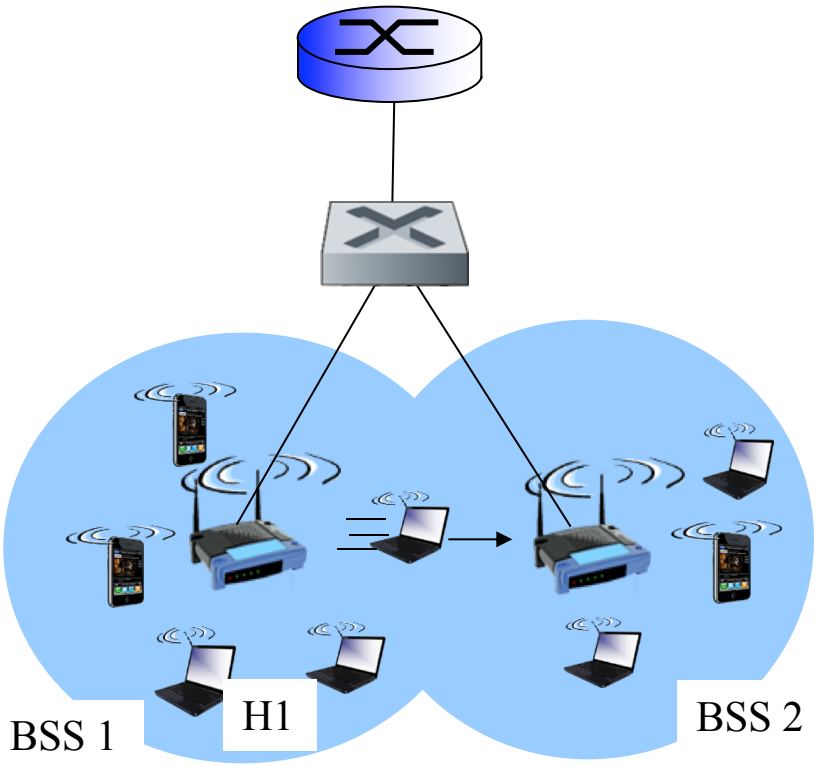


802.11 Frame: More Details



802.11: Mobility in the Same Subnet

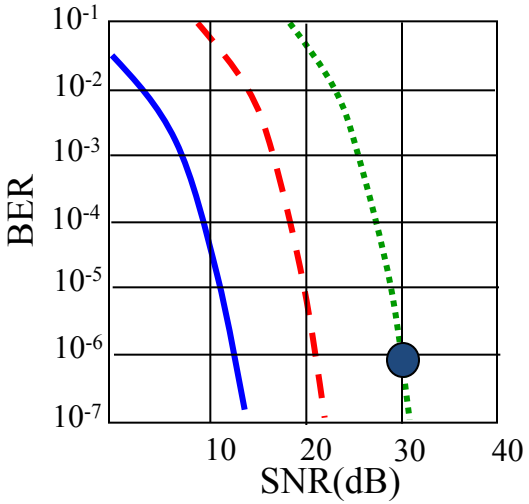
- H1 remains in same IP subnet: IP address can remain same
- Switch: which AP is associated with H1?
  - Self-learning (Ch. 5): switch will see frame from H1 and "remember" which switch port can be used to reach H1

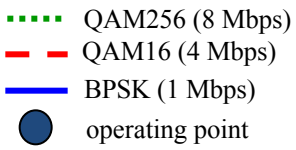


802.11: Advanced Capabilities (1)

Rate Adaptation

- Base station, mobile dynamically change transmission rate (physical layer modulation technique) as mobile moves, SNR varies





1. SNR decreases, BER increase as node moves away from base station

2. When BER becomes too high, switch to lower transmission rate but with lower BER

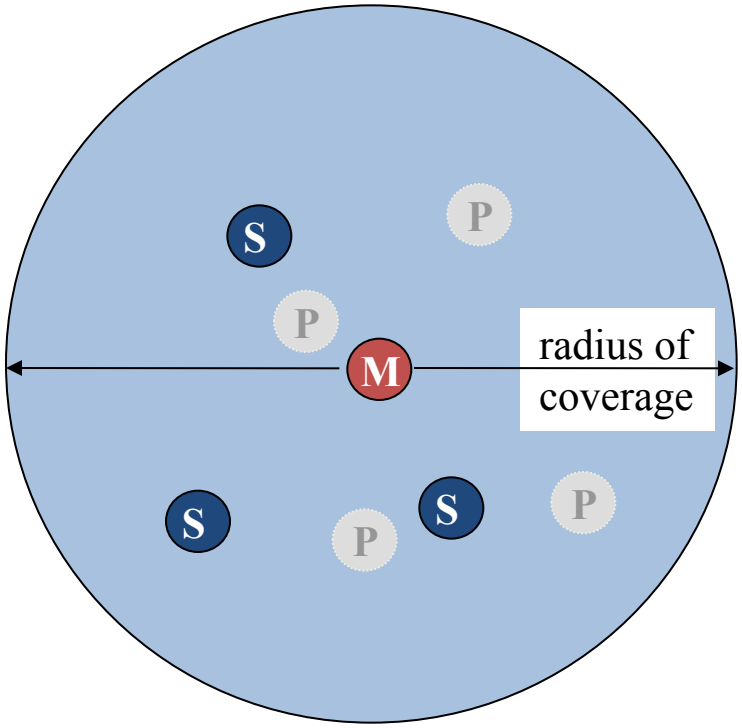
802.11: Advanced Capabilities (2)

Power Management

- Node-to-AP: "I am going to sleep until next beacon frame"
  - AP knows not to transmit frames to this node
  - Node wakes up before next beacon frame
- Beacon frame: contains list of mobiles with AP-to-mobile frames waiting to be sent
  - Node will stay awake if AP-to-mobile frames to be sent; otherwise sleep again until next beacon frame

802.15: Personal Area Network

- 10-meter diameter
- Replacement for cables (mouse, keyboard, headphones)
- Ad hoc: no infrastructure
- Master/slaves:
  - Slaves request permission to send (to master)
  - Master grants requests
- 802.15: evolved from Bluetooth specification
  - 2.4–2.5 GHz radio band
  - Data rate: up to 721 kbps



Outline

- Introduction
- Wireless links, characteristics
  - CDMA
- IEEE 802.11 wireless LANs (“Wi-Fi”)
- **Tools of the Trade**

Tools of the Trade (Linux) (1)

- `iw`: Scan for WLANs and configure them (https://wireless.wiki.kernel.org/en/users/documentation/iw)

```
adam@mactop-debian: ~
adam@mactop-debian: ~ 80x24
[adam]~ $ sudo iw dev wlan1 scan
BSS 34:12:98:0a:7c:a6(on wlan1)
        TSF: 1216774355687 usec (14d, 01:59:34)
        freq: 2437
        beacon interval: 100 TUs
        capability: ESS Privacy SpectrumMgmt ShortSlotTime RadioMeasure (0x1511)
        signal: -65.00 dBm
        last seen: 7732 ms ago
        Information elements from Probe Response frame:
        SSID: champnet
        Supported rates: 1.0* 2.0* 5.5* 11.0* 18.0 24.0 36.0 54.0
        DS Parameter set: channel 6
        Country: US     Environment: Indoor/Outdoor
                Channels [1 - 11] @ 30 dBm
        Power constraint: 0 dB
        TPC report: TX power: 25 dBm
        ERP: Barker_Preamble_Mode
        RSN:     * Version: 1
                 * Group cipher: CCMP
                 * Pairwise ciphers: CCMP
                 * Authentication suites: PSK
                 * Capabilities: 1-PTKSA-RC 1-GTKSA-RC (0x0000)
        Extended supported rates: 6.0 9.0 12.0 48.0
        HT capabilities:
```

Examples run on Debian Linux 9 (`amd64` machine architecture).

Tools of the Trade (Linux) (2)

- `iw` (cont'd): Wi-Fi scan at OSU (Au2017):
  - 13 `osuwireless` SSIDs (plus many more, e.g., `WiFi@OSU`)
  - Frequencies: 2.412, 2.462 GHz; 5.220, 5.3 GHz; 5.52, 5.54, 5.56, 5.6, 5.62, 5.66, 5.7, 5.785, 5.8 GHz
  - Signal strengths: –84 dBm to –53 dBm (0 dBm corresponds to 1 mW; –3 dBm corresponds to 0.5 mW, and so on)

Tools of the Trade (Linux) (3)

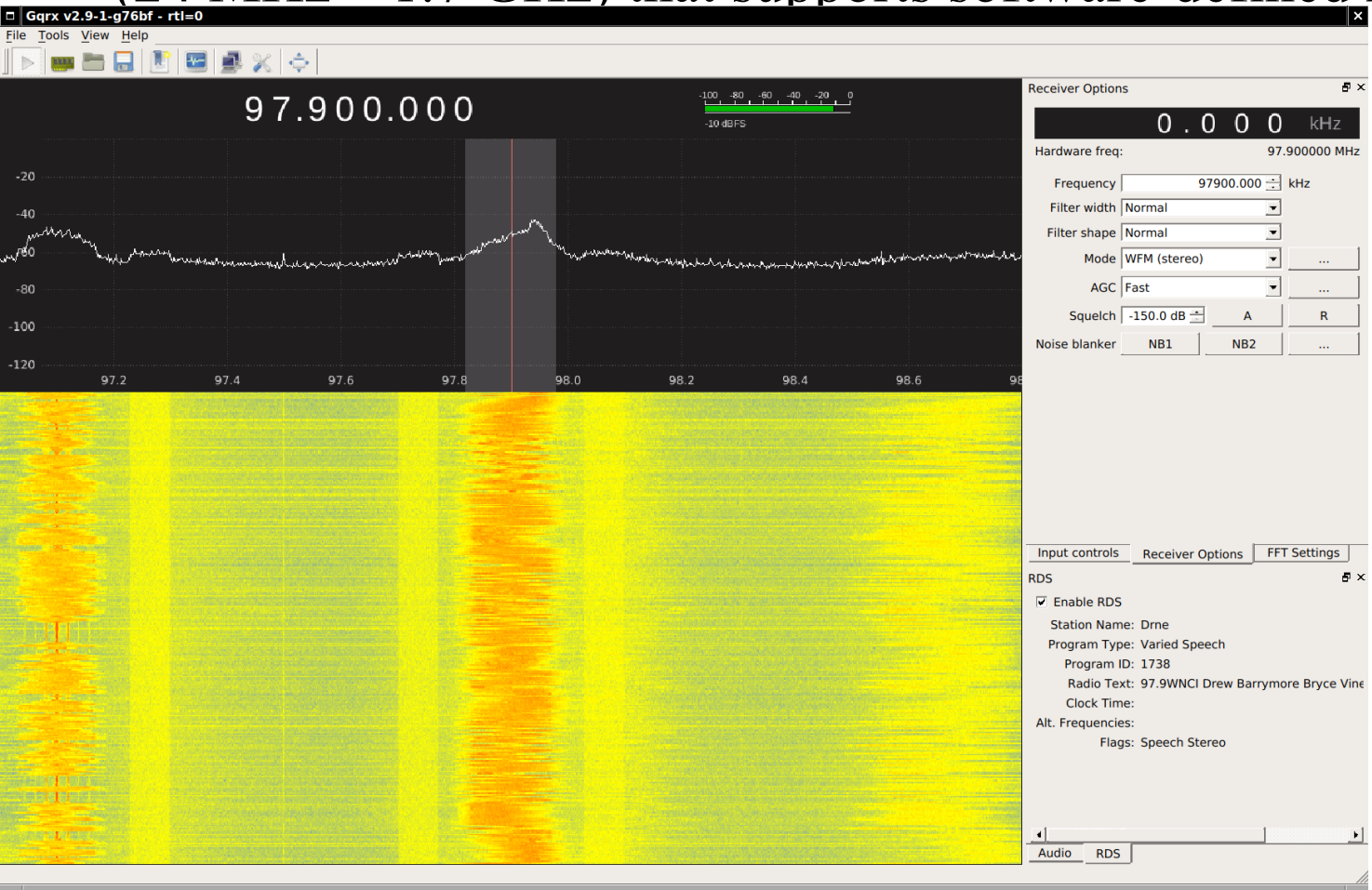
- `hcitool`: Scan for nearby Bluetooth devices
  - Both "Classic" Bluetooth and Bluetooth Low Energy
  - Part of Linux BlueZ suite (http://www.bluez.org)

```
adam@mactop-debian: ~
adam@mactop-debian: ~ 80x24
[adam]~ $ hcitool scan --flush
Scanning ...
        28:39:5E:21:93:14       [TV] UN32J5500
[adam]~ $
```

```
adam@mactop-debian: ~
adam@mactop-debian: ~ 80x24
[adam]~ $ sudo hcitool -i hci1 lescan
LE Scan ...
28:39:5E:21:93:14 (unknown)
28:39:5E:21:93:14 [TV] UN32J5500
D8:E0:E1:B5:DC:54 (unknown)
28:39:5E:21:93:14 (unknown)
28:39:5E:21:93:14 [TV] UN32J5500
D8:E0:E1:B5:DC:54 (unknown)
28:39:5E:21:93:14 (unknown)
28:39:5E:21:93:14 [TV] UN32J5500
D8:E0:E1:B5:DC:54 (unknown)
28:39:5E:21:93:14 (unknown)
28:39:5E:21:93:14 [TV] UN32J5500
D8:E0:E1:B5:DC:54 (unknown)
28:39:5E:21:93:14 (unknown)
28:39:5E:21:93:14 [TV] UN32J5500
D8:E0:E1:B5:DC:54 (unknown)
D8:E0:E1:B5:DC:54 (unknown)
28:39:5E:21:93:14 (unknown)
D8:E0:E1:B5:DC:54 (unknown)
28:39:5E:21:93:14 (unknown)
28:39:5E:21:93:14 [TV] UN32J5500
D8:E0:E1:B5:DC:54 (unknown)
28:39:5E:21:93:14 (unknown)
```

Tools of the Trade: Hardware

- RTL-SDR (https://www.rtl-sdr.com/): $25 receiver (24 MHz – 1.7 GHz) that supports software-defined radio (SDR)



GQRX: Free SDR program (http://www.gqrx.dk)

Summary

- Introduction
- Wireless links, characteristics
  - CDMA
- IEEE 802.11 wireless LANs (“Wi-Fi”)
- Tools of the Trade