UNIT I NETWORK MODELS AND DATALINK LAYER 9

Overview of Networks and its Attributes – Network Models – OSI, TCP/IP, Addressing – Introduction to Datalink Layer – Error Detection and Correction – Ethernet(802.3)- Wireless LAN – IEEE 802.11, Bluetooth – Flow and Error Control Protocols – HDLC – PPP.

Overview of Networks and its Attributes

Data communications are the exchange of data between two devices via some form of transmission medium such as a wire cable. 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)

Fundamental characteristics of Data communication systems:

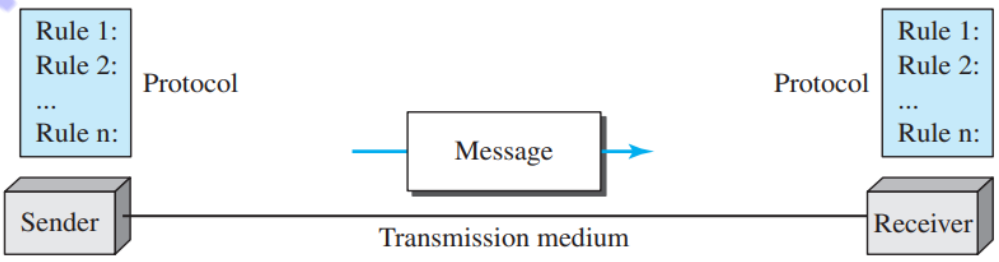
1. Delivery. The system must deliver data to the correct destination. Data must be received by the only by that device

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

3. 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.

4. Jitter. Jitter refers to the variation in the packet arrival time. It is the uneven delay in the delivery of audio or video packets.

Components of Data communication systems



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.

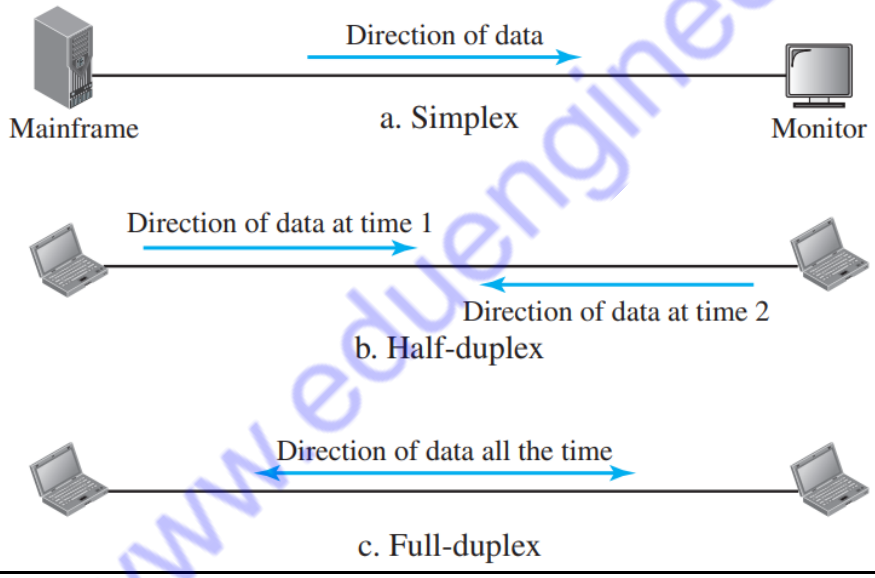
3. Receiver. The receiver is the device that receives the message. It can be a computer, workstation, telephone handset, television, and so on.

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

Data Flow

Communication between two devices can be simplex, half-duplex, or full-duplex



Simplex

In simplex mode, the communication is unidirectional, as on a one-way street.
Eg: Monitor, Keyboard

Half-Duplex

In half-duplex mode, each station can both transmit and receive, but not at the same time.
Eg: Walkie-talkies and CB (citizens band) radios

Full-Duplex

In full-duplex mode (also called duplex), both stations can transmit and receive simultaneously
Eg: Telephone, Mobile Phone

NETWORKS

A network is the interconnection of a set of devices capable of communication

Host is a large computer

Eg: Desktop, laptop, workstation, cellular phone, or security system

Network Criteria

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.

Eg: The number of users, the type of transmission medium, the capabilities of the connected hardware, and the efficiency of the software

Performance is evaluated by two networking metrics: throughput and delay.

Reliability

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.

Security

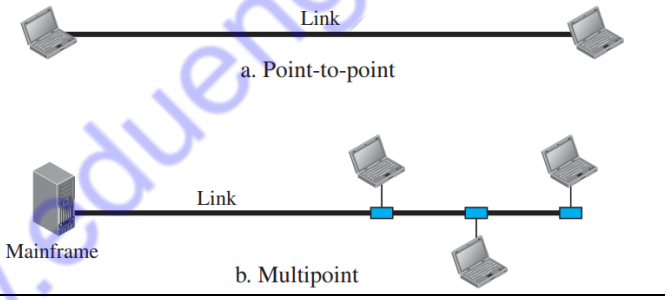
Network security issues include protecting data from unauthorized access, protecting data from damage and development, and implementing policies and procedures for recovery from breaches and data losses.

Physical Structures

A network is two or more devices connected through links. A link is a communications pathway that transfers data from one device to another

Point-to-Point: A point-to-point connection provides a dedicated link between two devices

Multipoint: A multipoint (also called multidrop) connection is one in which more than two specific devices share a single link

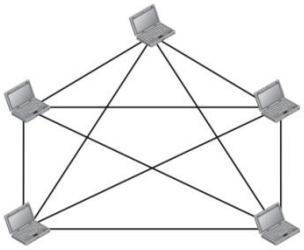


Physical Topology

The term physical topology refers to the way in which a network is laid out physically. It is a geometric representation of the relationship of all the links and linking devices (usually called nodes) to one another. There are four basic topologies possible: mesh, star, bus, and ring.

Mesh Topology

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.

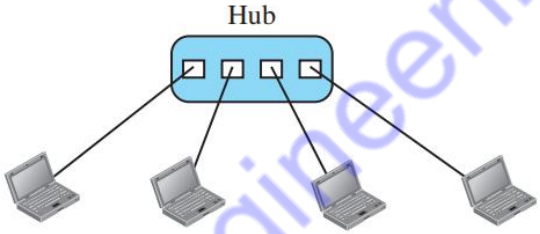


The use of dedicated links guarantees that each connection can carry its own data load, thus eliminating the traffic problems. If one link becomes unusable, it does not incapacitate the entire system. High privacy and security

The main disadvantages of a mesh are related to the amount of cabling and the number of I/O ports required.

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



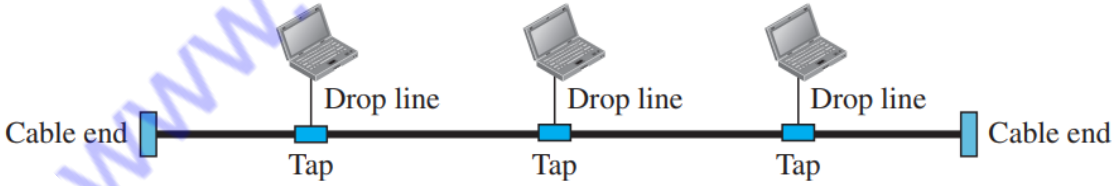
If one link fails, only that link is affected.

One big disadvantage of a star topology is the dependency of the whole topology on one single point, the hub

The star topology is used in local-area networks (LANs)

Bus Topology

One long cable acts as a backbone to link all the devices in a network

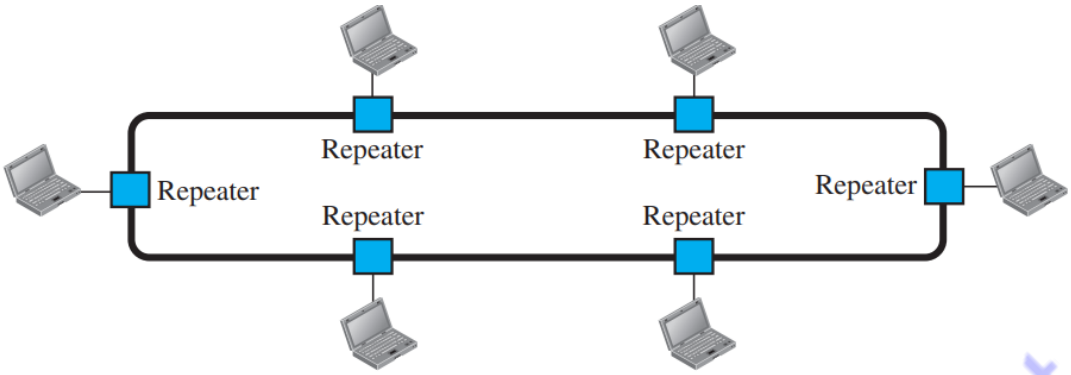


Advantages of a bus topology include ease of installation

Disadvantages include difficult reconnection and fault isolation.

Ring Topology

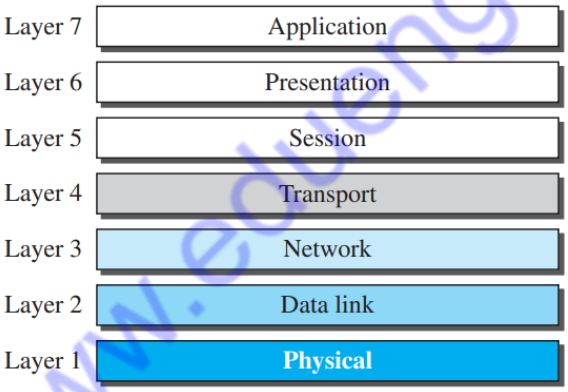
In a ring topology, each device has a dedicated point-to-point connection with only the two devices on either side of it. A signal is passed along the ring in one direction, from device to device, until it reaches its destination.



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.

THE OSI MODEL:

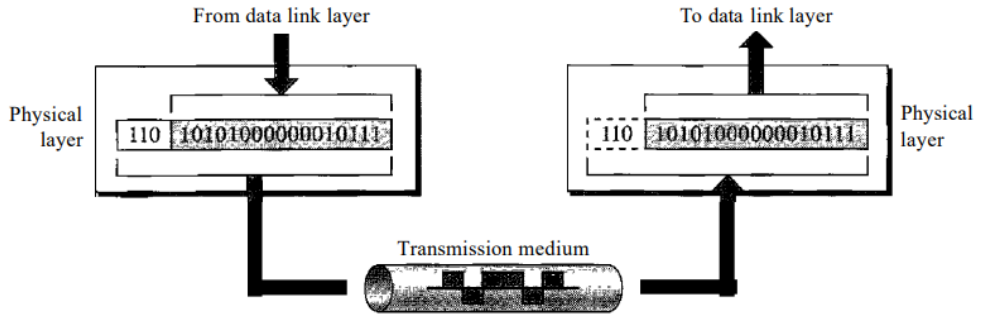
- Established in 1947, the International Organization for Standardization (ISO) is a multinational body dedicated to worldwide agreement on international standards.
- An ISO standard that covers all aspects of network communications is the Open Systems Interconnection (OSI) model. It was first introduced in the late 1970s.
- 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 hardware and software
- The OSI model is not a protocol; it is a model for flexible, robust, and interoperation
- It consists of seven separate but related layers, each of which defines a part of the process of moving information across a network



Layers in the OSI Model:

Physical Layer:

- 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

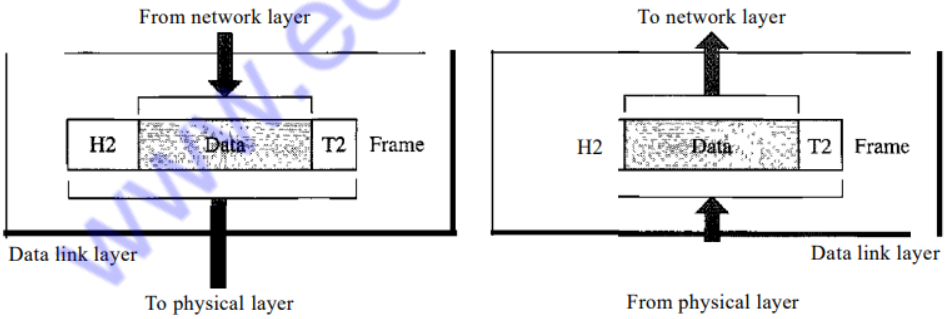


Responsibilities of Physical Layer:

- **Data rate.**
  The transmission rate-the number of bits sent each second-is also defined by the physical layer.
- **Synchronization of bits.**
  The sender and receiver not only must use the same bit rate but also must be synchronized at the bit level.
- **Line configuration**.
  It defines the connection is whether the connection is point-to-point or point to multipoint like broadcasting
- **Physical topology.**
  The physical topology defines how devices are connected to make a network. Devices can be connected by using a mesh topology , a star topology , a ring topology , a bus topology, or a hybrid topology (
- **Transmission mode.**
  The physical layer also defines the direction of transmission between two devices: simplex, half-duplex, or full-duplex.

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



- **Framing:**
  The data link layer divides the stream of bits received from the network layer into manageable data units called frames.
- **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.
- **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.
- **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

Network Layer

- The network layer is responsible for the source-to-destination delivery of a packet, possibly across multiple networks (links).
- 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.
- If two systems are connected to the same link, there is usually no need for a network layer.

Resposibilities of Network Layer

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.

Routing.

When independent networks or links are connected to create internetworks (network of networks) or a large network, the connecting devices route or switch the packets to their final destination.

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.

Responsibilities of Transport Layer:

- **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.
- **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.

- **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 connectionoriented 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.
- **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.
- **Error control.**
  Like the data link layer, the transport layer is responsible for error control.
  However, error control at this layer is performed process-toprocess rather than across a single link.
  Error correction is usually achieved through retransmission

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

Responsibilities of Session Layer:

- **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.
- **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 of 2000 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 2.12 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
- **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
- **Encryption.** To carry sensitive information, a system must be able to ensure privacy
- **Compression.** Data compression reduces the number of bits contained in the information

Application Layer

- The application layer enables the user, whether human or software, to access the network.
- It provides user interfaces and support for services such as electronic mail, remote file access and transfer, shared database management, and other types of distributed information services

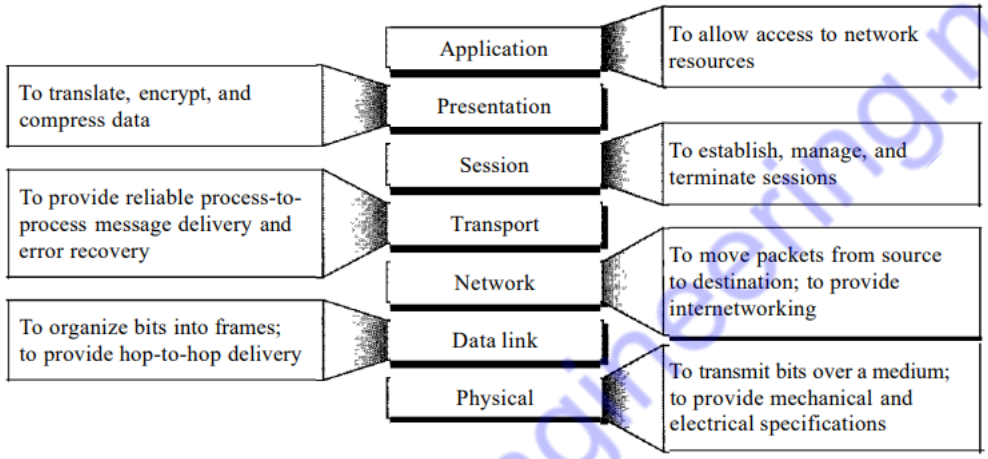
Network virtual terminal.

A network virtual terminal is a software version of a physical terminal, and it allows a user to log on to a remote host.

File transfer, access, and management.

Mail services. This application provides the basis for e-mail forwarding and storage.

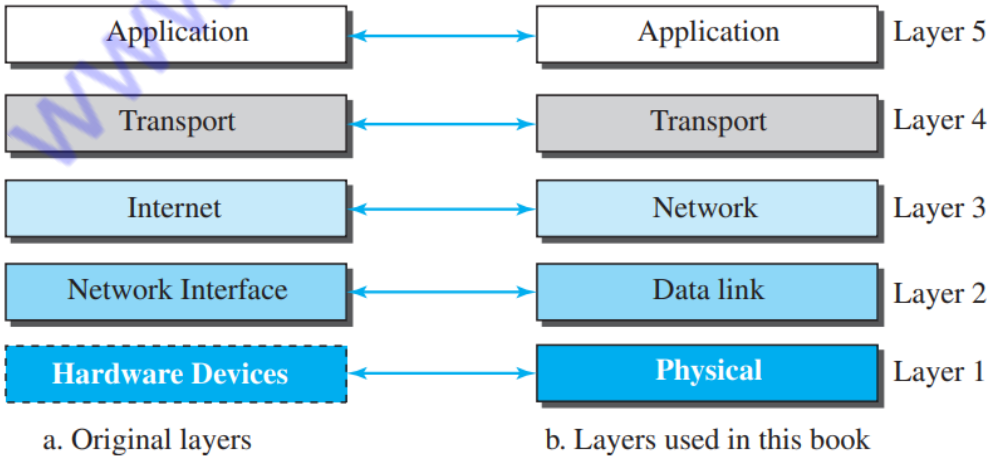
Directory services. This application provides distributed database sources and access for global information about various objects and services.

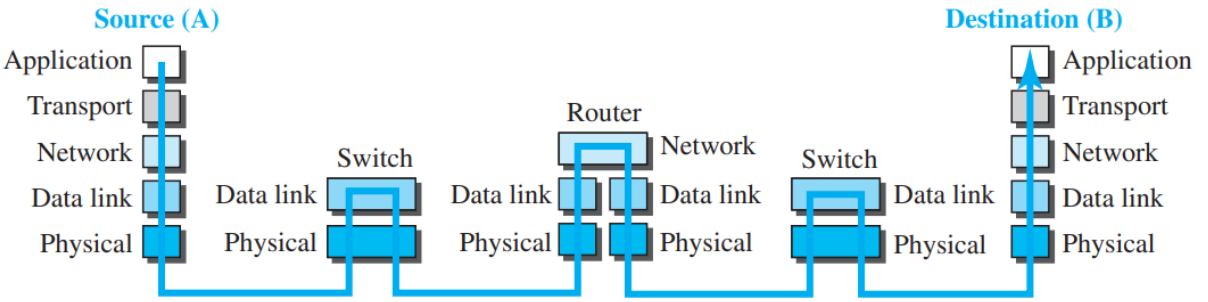


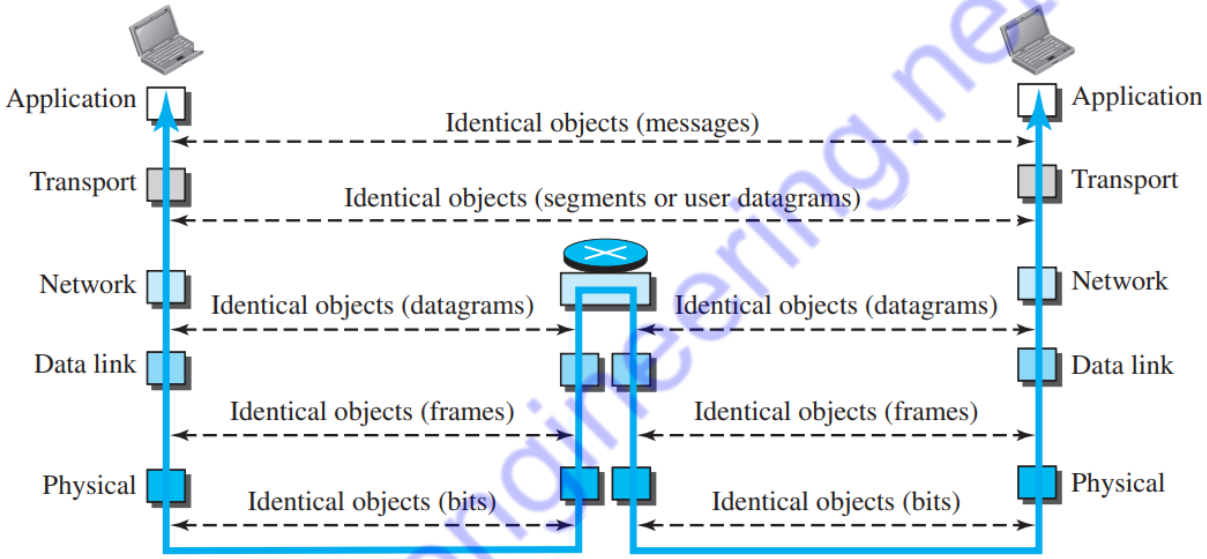
TCP/IP is a protocol suite

- A set of protocols organized in different layers) used in the Internet today.
- It is a hierarchical protocol made up of interactive modules, each of which provides a specific functionality.
- Each upper level protocol is supported by the services provided by one or more lower level protocols. The original TCP/IP protocol suite was defined as four software layers built upon the hardware

Layers in TCP/IP Protocol Suite







Physical Layer

- The physical layer is responsible for carrying individual bits in a frame across the link.
- It is the lowest level in the TCP/IP protocol suite
- The communication between two devices at the physical layer is still a logical communication because there is another, hidden layer, the transmission media, under the physical layer.
- Two devices are connected by a transmission medium (cable or air).
- The transmission medium does not carry bits; it carries electrical or optical signals. So the bits received in a frame from the data-link layer are transformed and sent through the transmission media, but we can think that the logical unit between two physical layers in two devices is a bit. There are several protocols that transform a bit to a signal.

Data-link Layer

- There may be several overlapping sets of links that a datagram can travel from the host to the destination.
- The routers are responsible for choosing the best links. However, when the next link to travel is determined by the router, the data-link layer is responsible for taking the datagram and moving it across the link.
- The link can be a wired LAN with a link-layer switch, a wireless LAN, a wired WAN, or a wireless WAN. We can also have different protocols used with any link type.

- TCP/IP does not define any specific protocol for the data-link layer. It supports all the standard and proprietary protocols.
- Some data link-layer protocols provide complete error detection and correction, some provide only error correction

Network Layer

- The network layer is responsible for creating a connection between the source computer and the destination computer.
- The communication at the network layer is host-to-host. However, since there can be several routers from the source to the destination, the routers in the path are responsible for choosing the best route for each packet.
- Since there can be several routers from the source to the destination, the routers in the path are responsible for choosing the best route for each packet
- The network layer in the Internet includes the main protocol, Internet Protocol (IP), that defines the format of the packet, called a datagram at the network layer
- IP is a connectionless protocol that provides no flow control, no error control, and no congestion control services
- A routing protocol does not take part in routing (it is the responsibility of IP), but it creates forwarding tables for routers to help them in the routing process.
- The network layer also has some auxiliary protocols that help IP in its delivery and routing tasks.
- The Internet Control Message Protocol (ICMP) helps IP to report some problems when routing a packet.
- The Internet Group Management Protocol (IGMP) is another protocol that helps IP in multitasking.
- The Dynamic Host Configuration Protocol (DHCP) helps IP to get the network-layer address for a host.
- The Address Resolution Protocol (ARP) is a protocol that helps IP to find the link-layer address of a host or a router when its network-layer address is given.

Transport Layer

- The transport layer at the source host gets the message from the application layer, encapsulates it in a transportlayer packet and sends it, through the logical connection, to the transport layer at the destination host.
- The transport layer is responsible for giving services to the application layer
- The transport layer should be independent of the application layer
- The main protocol, Transmission Control Protocol (TCP), is a connection-oriented protocol that first establishes a logical connection between transport layers at two hosts before transferring data. It creates a logical pipe between two TCPs for transferring a stream of bytes
- TCP provides flow control and error control Mechanisms
- User Datagram Protocol (UDP), is a connectionless protocol that transmits user datagrams without first creating a logical connection
- UDP is a simple protocol that does not provide flow, error, or congestion control.

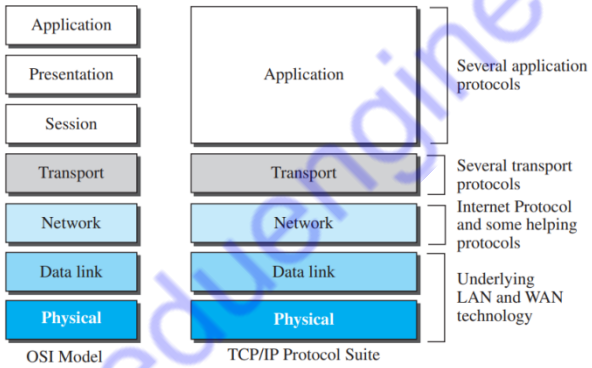
Application Layer

- The two application layers exchange messages between each other as though there were a bridge between the two layers.

- To communicate, a process sends a request to the other process and receives a response.
- Process-to-process communication is the duty of the application layer. The a user can also create a pair of processes to be run at the two hosts
- The Hypertext Transfer Protocol (HTTP) is a vehicle for accessing the World Wide Web (WWW).
- The Simple Mail Transfer Protocol (SMTP) is the main protocol used in electronic mail (e-mail) service.
- The File Transfer Protocol (FTP) is used for transferring files from one host to another.
- The Terminal Network (TELNET) and Secure Shell (SSH) are used for accessing a site remotely.
- The Simple Network Management Protocol (SNMP) is used by an administrator to manage the Internet at global and local levels.
- The Domain Name System (DNS) is used by other protocols to find the network-layer address of a computer

OSI versus TCP/IP:

- There are two layers, session and presentation, are missing from the TCP/IP protocol suite.
- These two layers were not added to the TCP/IP protocol suite after the publication of the OSI model



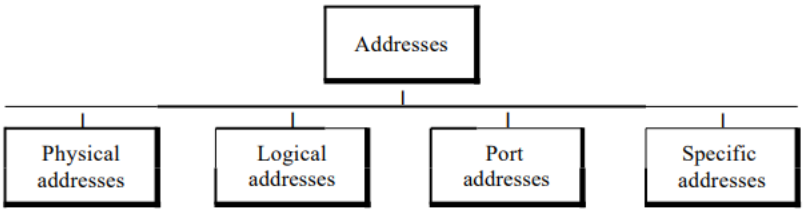
- TCP/IP has more than one transport-layer protocol. Some of the functionalities of the session layer are available in some of the transport-layer protocols.
- Second, the application layer is not only one piece of software. Many applications can be developed at this layer
- If some of the functionalities mentioned in the session and presentation layers are needed for a particular application, they can be included in the development of that piece of software.

Lack of OSI Model's Success:

- First, OSI was completed when TCP/IP was fully in place and a lot of time and money had been spent on the suite
- Second, some layers in the OSI model were never fully defined. For example, although the services provided by the presentation and the session layers were listed in the document, actual protocols for these two layers were not fully defined.
- Third, when OSI was implemented by an organization in a different application, it did not show a high enough level of performance

Addressing:

There are 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



Physical Address or Link Address:

- It 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.

  Eg: Ethernet uses a 6-byte (48-bit) physical address that is imprinted on the network interface card (NIC).

07:01:02:01:2C:4B

A 6-byte (12 hexadecimal digits) physical address

Logical Address:

- 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
- The physical addresses will change from hop to hop, but the logical addresses usually remain the same.

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. H
- However, arrival at the destination host is not the final objective of data communications on the Internet.
- 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
- Port address is used to address different processes for receiving the data simultaneously

Specific Addresses

- Some applications have user-friendly addresses that are designed for that specific address.

  Eg: E-mail address (for example, forouzan@fhda.edu)

  Universal Resource Locator (URL) (for example, www.mhhe.com).

Data Link Layer:

- Data link control functions include framing, flow and error control, and softwareimplemented protocols that provide smooth and reliable transmission of frames between nodes
- The duty scope of the data-link layer is node-to-node.
- When a packet is travelling in the Internet, the data-link layer of a node (host or router) is responsible for delivering a datagram to the next node in the path.
- For this purpose, the data-link layer of the sending node needs to encapsulate the datagram received from the network in a frame, and the data-link layer of the receiving node needs to decapsulate the datagram from the frame.

Framing:

- A packet at the data-link layer is normally called a frame.
- The first service provided by the data-link layer is framing
- The data-link layer at each node needs to encapsulate the datagram in a frame before sending it to the next node
- The node also needs to decapsulate the datagram from the frame received on the logical channel.
- Framing in the data link layer separates a message from one source to a destination, or from other messages to other destinations, by adding a sender address and a destination address.
- The destination address defines where the packet is to go; the sender address helps the recipient acknowledge the receipt

Flow Control:

- Flow control refers to a set of procedures used to restrict the amount of data that the sender can send before waiting for acknowledgment.
- The flow of data must not be allowed to overwhelm the receiver.
- Any receiving device has a limited speed at which it can process incoming data and a limited amount of memory in which to store incoming data.
- The receiving device must be able to inform the sending device before those limits are reached and to request that the transmitting device send fewer frames or stop temporarily.
- Incoming data must be checked and processed before they can be used.

Error Control:

- At the sending node, a frame in a data-link layer needs to be changed to bits, transformed to electromagnetic signals, and transmitted through the transmission media.
- At the receiving node, electromagnetic signals are received, transformed to bits, and put together to create a frame.
- Since electromagnetic signals are susceptible to error, a frame is susceptible to error. The error needs first to be detected.
- After detection, it needs to be either corrected at the receiver node or discarded and retransmitted by the sending node.
- Error control in the data link layer is based on automatic repeat request, which is the retransmission of data

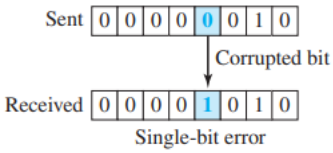
Error Detection and Correction:

Types of Errors

Whenever bits flow from one point to another, they are subject to unpredictable changes because of interference. This interference can change the shape of the signal.

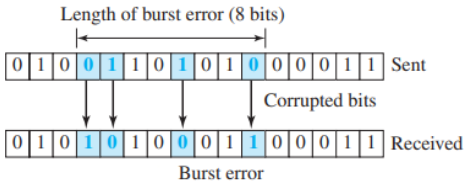
Single bit Error:

In this only 1 bit of a given data unit (such as a byte, character, or packet) is changed from 1 to 0 or from 0 to 1.



Burst Error:

The term burst error means that 2 or more bits in the data unit have changed from 1 to 0 or from 0 to 1.



A burst error is more likely to occur than a single-bit error because the duration of the noise signal is normally longer than the duration of 1 bit, which means that when noise affects data, it affects a set of bits.

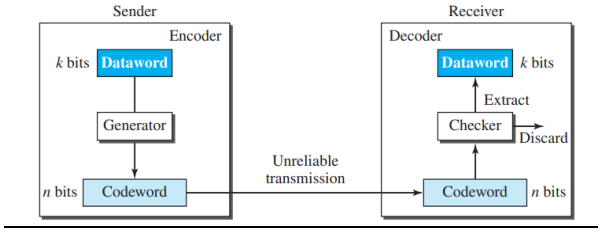
Redundancy:

The central concept in detecting or correcting errors is redundancy. To be able to detect or correct errors, we need to send some extra bits with our data. These redundant bits are added by the sender and removed by the receiver. The number of errors and the size of the message are important factors. There are two coding techniques are commonly available- Block coding and Convolutional coding

BLOCK CODING:

- In block coding, the total message is divided into blocks, each of k bits, called **data words.**
- There are r redundant bits are added to each block to make the length n = k + r. The resulting n-bit blocks are called **code words.**
- With k bits, we can create a combination of 2^k data words; with n bits, we can create a combination of 2^n code words.
- Since n > k, the number of possible code words is larger than the number of possible data words. The block coding process is one-to-one; the same dataword is always encoded as the same code word. This means that we have $2^n - 2^k$ code words that are not used.
- If the receiver receives an invalid code word, this indicates that the data was corrupted during transmission.
- The sender creates codewords out of data words by using a generator that applies the rules and procedures of encoding.
- Each code word sent to the receiver may change during transmission. If the received code word is the same as one of the valid code words, the word is accepted; the corresponding data word is extracted for use.

- If the received codeword is not valid, it is discarded. However, if the code word is corrupted during transmission but the received word still matches a valid code word, the error remains undetected



Hamming Distance:

- **The Hamming distance between two words is the number of differences between the corresponding bits**.The Hamming distance between two words x and y as d(x, y).
- It is distance between the received code word and the sent code word is the number of bits that are corrupted during transmission.
  Eg: If the codeword 00000 is sent and 01101 is received, 3 bits are in error and the Hamming distance between the two is d(00000, 01101) = 3.
- The Hamming distance can easily be found by applying the XOR operation (⊕) on the two words and count the number of 1s in the result.
  Eg: . The Hamming distance d(000, 011) is 2 because (000 ⊕ 011) is 011 (two 1s). 2.
  The Hamming distance d(10101, 11110) is 3 because (10101 ⊕ 11110) is 01011 (three 1s).
- In a set of codewords, the **minimum Hamming distance** is the smallest Hamming distance between all possible pairs of code words
- If s errors occur during transmission, the Hamming distance between the sent codeword and received code word is s. If our system is to detect up to s errors, the minimum distance between the valid codes must be (s + 1).

$$d_{min} = s + 1.$$

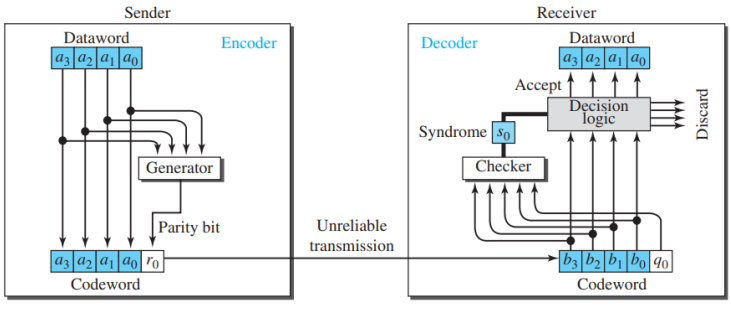
Linear Block Codes:

- Almost all block codes used today belong to a subset of block codes called linear block codes.
- In this an exclusive OR (addition modulo-2) of two valid code words creates another valid code word.

Parity-Check Code

- It is the most familiar error-detecting code is the parity-check code.
- This code is a linear block code.
- In this code, a k-bit data word is changed to an n-bit code word where n = k + 1. The extra bit, called the parity bit, is selected to make the total number of 1s in the code word even.
- Parity check code is a single bit error detection code

Dataword	*Codeword*
0000	**00000**
0001	**00011**
0010	**00101**
0011	**00110**
0100	**01001**
0101	**01010**



Cyclic codes:

- Cyclic codes are special linear block codes with one extra property.
- In a cyclic code, if a code word is cyclically shifted (rotated), the result is another code word.

  Eg: if 1011000 is a code word and we cyclically left-shift, then 0110001 is also a Code word.

$b_1 = a_0$ $b_2 = a_1$ $b_3 = a_2$ $b_4 = a_3$ $b_5 = a_4$ $b_6 = a_5$ $b_0 = a_6$

Cyclic Redundancy Check:

- A subset of cyclic codes called the cyclic redundancy check (CRC), which is used in networks such as LANs and WANs
- It is based on binary division.

Sender Side:

- A string of n 0's is appended to the data unit to be transmitted.
- Here, n is one less than the number of bits in CRC generator.
- Binary division is performed of the resultant string with the CRC generator.
- After division, the remainder so obtained is called as CRC.
- It may be noted that CRC also consists of n bits.
- The newly formed code word (Original data + CRC) is transmitted to the receiver.

At receiver side:

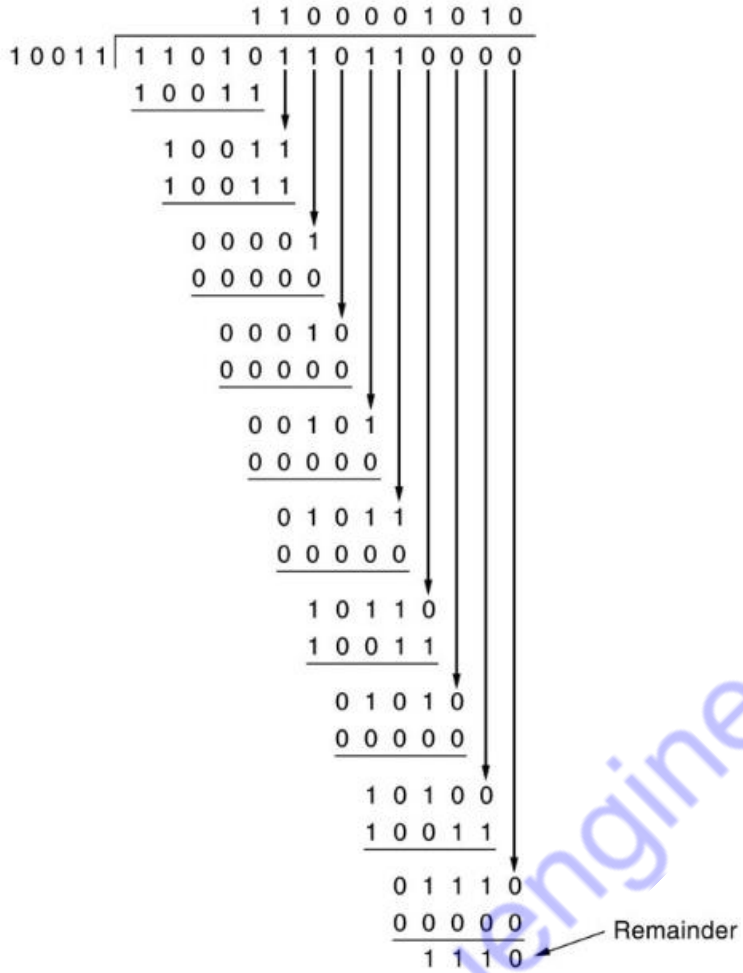
- The transmitted code word is received.
- The received code word is divided with the same CRC generator.
- On division, the remainder so obtained is checked.

Problems:

A bit stream 1101011011 is transmitted using the standard CRC method. The generator polynomial is x4+x+1. What is the actual bit string transmitted?

The generator polynomial G(x) = x4 + x + 1 is encoded as 10011.

Clearly, the generator polynomial consists of 5 bits. So, a string of 4 zeroes is appended to the bit stream to be transmitted. The resulting bit stream is 11010110110000.



Now,

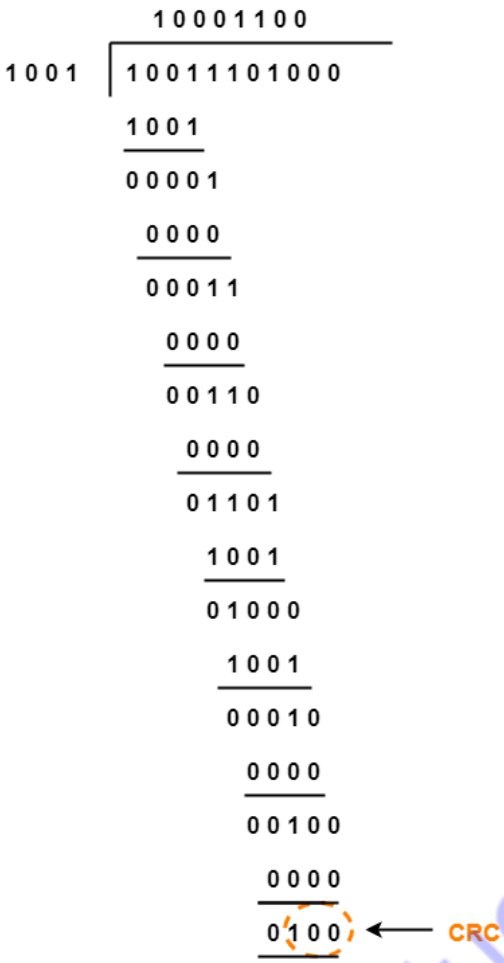
- The code word to be transmitted is obtained by replacing the last 4 zeroes of 11010110110000 with the CRC.
- Thus, the code word transmitted to the receiver = 11010110111110.

A bit stream 10011101 is transmitted using the standard CRC method. The generator polynomial is x3+1.

1. What is the actual bit string transmitted?

The generator polynomial G(x) = x3 + 1 is encoded as 1001.
Clearly, the generator polynomial consists of 4 bits.
So, a string of 3 zeroes is appended to the bit stream to be transmitted.
The resulting bit stream is 10011101000.

Now, the binary division is performed as



From here, CRC = 100.

Now,

- The code word to be transmitted is obtained by replacing the last 3 zeroes of 10011101000 with the CRC.
- Thus, the code word transmitted to the receiver = 10011101100.

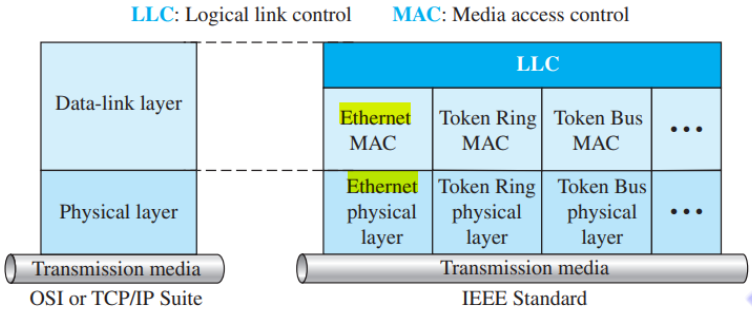
Ethernet Protocol:

- In 1985, the Computer Society of the IEEE started a project, called Project 802, to set standards to enable intercommunication among equipment from a variety of manufacturers
- Project 802 does not seek to replace any part of the OSI model or TCP/IP protocol suite. Instead, it is a way of specifying functions of the physical layer and the data-link layer of major LAN protocols
- The IEEE has subdivided the data-link layer into two sub layers: logical link control (LLC) and media access control (MAC). IEEE has also created several physical-layer standards for different LAN protocols

Logical Link Control (LLC)

- The data link control handles framing, flow control, and error control.

- In IEEE Project 802, flow control, error control, and part of the framing duties are collected into one sub layer called the logical link control (LLC).
- Framing is handled in both the LLC sub layer and the MAC sub layer.
- The LLC provides a single link-layer control protocol for all IEEE LANs.

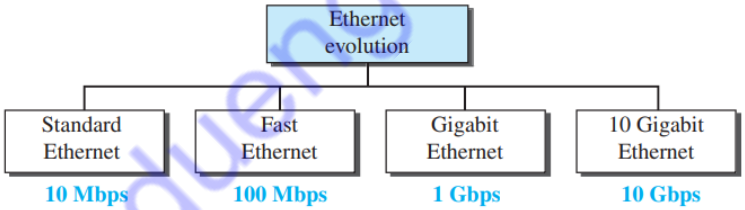


Media Access Control (MAC)

- IEEE Project 802 has created a sub layer called media access control that defines the specific access method for each LAN.

Ethernet Evolution

- The Ethernet LAN was developed in the 1970s by Robert Metcalfe and David Boggs.
- It has gone through four generations: Standard Ethernet (10 Mbps), Fast Ethernet (100 Mbps), Gigabit Ethernet (1 Gbps), and 10 Gigabit Ethernet (10 Gbps),



Standard Ethernet:

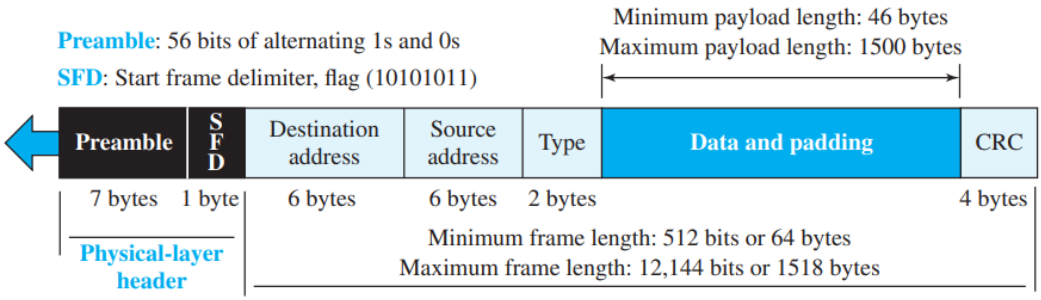
The original Ethernet technology with the data rate of 10 Mbps as the Standard Ethernet

Connectionless and Unreliable Service

- Ethernet provides a connectionless service, which means each frame sent is independent of the previous or next frame.
- Ethernet has no connection establishment or connection termination phases.
- The sender sends a frame whenever it has it; the receiver may or may not be ready for it.
- The sender may overwhelm the receiver with frames, which may result in dropping frames. If a frame drops, the sender will not know about it.
- If the transport layer is also a connectionless protocol, such as UDP, the frame is lost and salvation may only come from the application layer.
- However, if the transport layer is TCP, the sender TCP does not receive acknowledgment for its segment and sends it again.
- Ethernet is also unreliable like IP and UDP.

Frame Format

The Ethernet frame contains **seven fields**



Preamble

- This field contains 7 bytes (56 bits) of alternating 0s and 1s that alert the receiving system to the coming frame and enable it to synchronize its clock if it's out of synchronization.
- The pattern provides only an alert and a timing pulse.
- The 56-bit pattern allows the stations to miss some bits at the beginning of the frame.
- The preamble is actually added at the physical layer and is not (formally) part of the frame

Start frame delimiter (SFD)

- This field (1 byte: 10101011) signals the beginning of the frame.
- The SFD warns the station or stations that this is the last chance for synchronization.
- The last 2 bits are (11)2 and alert the receiver that the next field is the destination address.
- This field is actually a flag that defines the beginning of the frame.
- It needs to remember that an Ethernet frame is a variable-length frame.
- It needs a flag to define the beginning of the frame. The SFD field is also added at the physical layer.

Destination address (DA):

- This field is six bytes (48 bits) and contains the linklayer address of the destination station or stations to receive the packet.
- When the receiver sees its own link-layer address, or a multicast address for a group that the receiver is a member of, or a broadcast address, it decapsulates the data from the frame and passes the data to the upper layer protocol defined by the value of the type field.

Source address (SA).

- This field is also six bytes and contains the link-layer address of the sender of the packet.

Type.

- This field defines the upper-layer protocol whose packet is encapsulated in the frame.
- It is used for multiplexing and demultiplexing.

Data

- This field carries data encapsulated from the upper-layer protocols.
- It is a minimum of 46 and a maximum of 1500 bytes.
- If the data coming from the upper layer is more than 1500 bytes, it should be fragmented and encapsulated in more than one frame.
- If it is less than 46 bytes, it needs to be padded with extra 0s. A padded data frame is delivered to the upper-layer protocol as it is (without removing the padding), which means that it is the responsibility of the upper layer to remove or, in the case of the sender, to add the padding.
- The upper-layer protocol needs to know the length of its data.

Addressing

- Each station on an Ethernet network has its own network interface card (NIC).
- The NIC fits inside the station and provides the station with a link-layer address.
- The Ethernet address is 6 bytes (48 bits), normally written in hexadecimal notation, with a colon between the bytes.

4A:30:10:21:10:1A

Access Method

- The standard Ethernet chose CSMA/CD with 1-persistent method
- Assume station A has a frame to send to station D.
- Station A first should check whether any other station is sending (carrier sense).
- Station A measures the level of energy on the medium (for a short period of time, normally less than 100 µs).
- If there is no signal energy on the medium, it means that no station is sending (or the signal has not reached station A).
- Station A interprets this situation as idle medium.
- It starts sending its frame.
- On the other hand, if the signal energy level is not zero, it means that the medium is being used by another station.
- Station A continuously monitors the medium until it becomes idle for 100 µs. It then starts sending the frame.
- However, station A needs to keep a copy of the frame in its buffer until it is sure that there is no collision.
- The medium sensing does not stop after station A has started sending the frame. Station A needs to send and receive continuously.

Efficiency of standard Ethernet:

The efficiency of the Ethernet is defined as the ratio of the time used by a station to send data to the time the medium is occupied by this station.

$$\text{Efficiency} = 1 / (1 + 6.4 \times a)$$

"a" is the number of frames that can fit on the medium. It can be calculated as

a = (propagation delay)/(transmission delay)

In the Standard Ethernet with the transmission rate of 10 Mbps, we assume that the length of the medium is 2500 m and the size of the frame is 512 bits. The propagation speed of a signal in a cable is normally 2×10^8 m/s.

Propagation delay = $2500/(2 \times 10^8) = 12.5$ µs	**Transmission delay = $512/(10^7) = 51.2$ µs**
$a = 12.5/51.2 = 0.24$	**Efficiency = 39%**

Wireless LAN:

- Wireless communication is one of the fastest-growing technologies. The demand for connecting devices without the use of cables is increasing everywhere. Wireless LANs can be found on college campuses, in office buildings, and in many public areas.

Architectural Comparison:

Activity/Category	Wireless Network	Wired Network
Freedom of movement for users	Users can access network from anywhere within range.	Users location limited by need to use cable and/or connect to a port.
Sharing Files	Easier with wireless network as you do not need to be cabled to network, though transfer speeds may be slower.	Generally less convenient as you have to be cabled in, but transfer speeds often faster.
Cables	Far less complicated, disruptive, and untidy cabling needed.	Lots of cables and ports needed which can be a headache.
Business	For businesses dealing with public, customers like and often expect wireless, so wireless can increase income.	Wired networks are not convenient for public use, but sometimes acceptable for a traditional office.
Connection speeds	Usually slower than wired.	Usually faster than wireless.
Security	Less secure than wired. Both bandwidth and information can sometimes be accessed.	More secure than wireless.
Set up	Upgrading to a wireless network can be difficult and expensive.	Can also be difficult and expensive to set up.

Characteristics of Wireless LAN:

Attenuation

- The strength of electromagnetic signals decreases rapidly because the signal disperses in all directions; only a small portion of it reaches the receiver. The situation becomes worse with mobile senders that operate on batteries and normally have small power supplies.

Interference

- A receiver may receive signals not only from the intended sender, but also from other senders if they are using the same frequency band.

Multipath Propagation

- A receiver may receive more than one signal from the same sender because electromagnetic waves can be reflected back from obstacles such as walls, the ground, or objects.
- The result is that the receiver receives some signals at different phases (because they travel different paths). This makes the signal less recognizable

Error

- The errors and error detection are more serious issues in a wireless network than in a wired network.
- Error level is measured using signal-to-noise ratio (SNR). If SNR is high, it means that the signal is stronger than the noise (unwanted signal), so we may be able to convert the signal to actual data.
- On the other hand, when SNR is low, it means that the signal is corrupted by the noise and the data cannot be recovered.

Access Control

- The Standard Ethernet uses the CSMA/CD algorithm. In this method, each host contends to access the medium and sends its frame if it finds the medium idle.
- If a collision occurs, it is detected and the frame is sent again. Collision detection in CSMA/CD serves two purposes. If a collision is detected, it means that the frame has not been received and needs to be resent. If a collision is not detected, it is a kind of acknowledgment that the frame was received.

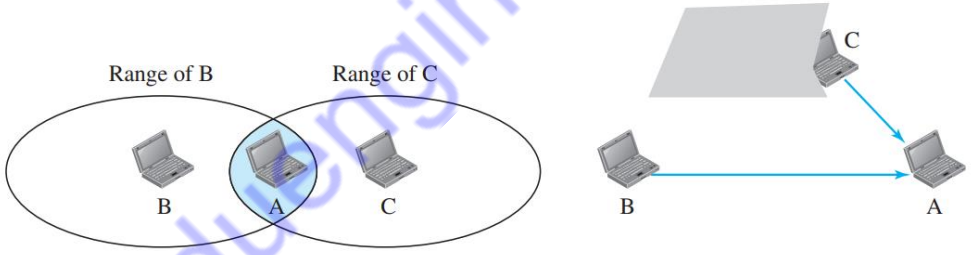
The CSMA/CD algorithm does not work in wireless LANs for three reasons:

- To detect a collision, a host needs to send and receive at the same time, which means the host needs to work in a duplex mode. Wireless hosts do not have enough power to do so (the power is supplied by batteries). They can only send or receive at one time
- Because of the hidden station problem, in which a station may not be aware of another station's transmission due to some obstacles or range problems, collision may occur but not be detected

  Example:

  Consider the circuit shown in Figure. Station B has a transmission range shown by the left oval (sphere in space); every station in this range can hear any signal transmitted by station B. Station C has a transmission range shown by the right oval (sphere in space); every station located in this range can hear any signal transmitted by C.

  Station C is outside the transmission range of B; likewise, station B is outside the transmission range of C. Station A, however, is in the area covered by both B and C; it can hear any signal transmitted by B or C. The figure also shows that the hidden station problem may also occur due to an obstacle.



a. Stations B and C are not in each other's range.

b. Stations B and C are hidden from each other.

  Assume that station B is sending data to station A. In the middle of this transmission, station C also has data to send to station A. However, station C is out of B's range and transmissions from B cannot reach C. Therefore C thinks the medium is free. Station C sends its data to A, which results in a collision at A because this station is receiving data from both B and C. In this case, we say that stations B and C are hidden from each other with respect to A. Hidden stations can reduce the capacity of the network because of the possibility of collision
- The distance between stations can be great. Signal fading could prevent a station at one end from hearing a collision at the other end.

IEEE 802.11 PROJECT(or) WIRELESS ETHERNET:

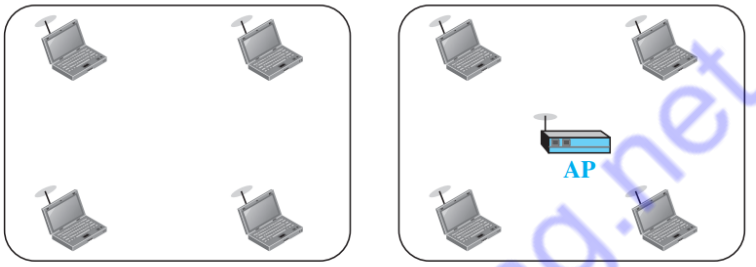
- IEEE has defined the specifications for a wireless LAN, called IEEE 802.11, which covers the physical and data-link layers
- The term WiFi (Wireless Fidelity) as a synonym for wireless LAN

Architecture

- The standard defines two kinds of services: the basic service set (BSS) and the extended service set (ESS).

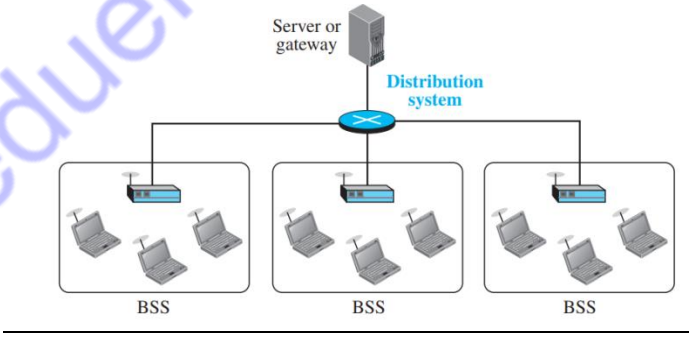
Basic Service Set :

- A basic service set is made of stationary or mobile wireless stations and an optional central base station, known as the access point (AP).
- The BSS without an AP is a stand-alone network and cannot send data to other BSSs. It is called an **ad hoc architecture.**
- A BSS with an AP is sometimes referred to as an **Infrastructure BSS**



Extended Service Set

- An extended service set (ESS) is made up of two or more BSSs with APs.
- In this case, the BSSs are connected through a distribution system, which is a wired or a wireless network.
- The distribution system connects the APs in the BSSs.
- IEEE 802.11 does not restrict the distribution system; it can be any IEEE LAN such as an Ethernet.
- The mobile stations are normal stations inside a BSS.
- The stationary stations are AP stations that are part of a wired LAN.



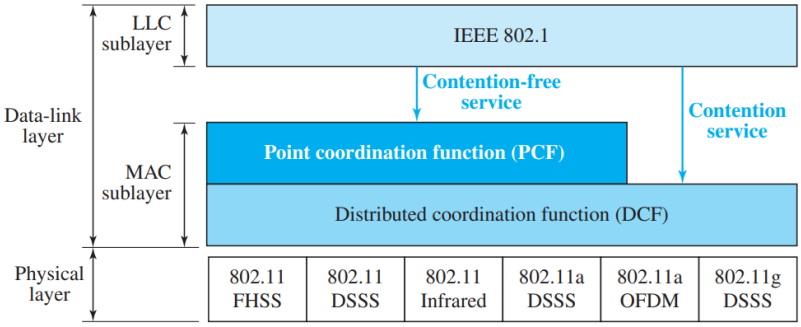
Station Types

IEEE 802.11 defines three types of stations based on their mobility in a wireless LAN: no-transition, BSS-transition, and ESS-transition mobility.

- A station with no-transition mobility is either stationary (not moving) or moving only inside a BSS.
- A station with BSS-transition mobility can move from one BSS to another, but the movement is confined inside one ESS.
- A station with ESS-transition mobility can move from one ESS to another

MAC Sublayer:

IEEE 802.11 defines two MAC sublayers: the distributed coordination function (DCF) and point coordination function (PCF).



Distributed Coordination Function:

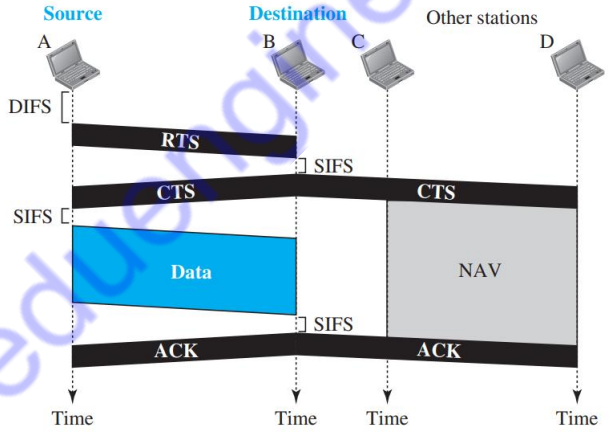
- One of the two protocols defined by IEEE at the MAC sub layer is called the distributed coordination function (DCF).
- DCF uses CSMA/CA as the access method

Frame Exchange Time Line:

1. Before sending a frame, the source station senses the medium by checking the energy level at the carrier frequency.

a. The channel uses a persistence strategy with backoff until the channel is idle.

b. After the station is found to be idle, the station waits for a period of time called the distributed interframe space (DIFS); then the station sends a control frame called the request to send (RTS).

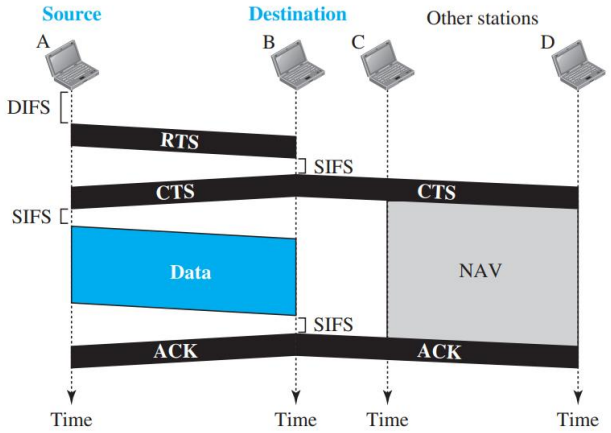


2. After receiving the RTS and waiting a period of time called the short interframe space (SIFS), the destination station sends a control frame, called the clear to send (CTS), to the source station. This control frame indicates that the destination station is ready to receive data.

3. The source station sends data after waiting an amount of time equal to SIFS.

4. The destination station, after waiting an amount of time equal to SIFS, sends an acknowledgment to show that the frame has been received. Acknowledgment is needed in this protocol because the station does not have any means to check for the successful arrival of its data at the destination. On the other hand, the lack of collision in CSMA/CD is a kind of indication to the source that data have arrived.

When a station sends an RTS frame, it includes the duration of time that it needs to occupy the channel. The stations that are affected by this transmission create a timer called a **Network Allocation Vector (NAV) that shows how much time must pass before these stations are allowed to check the channel for idleness.**

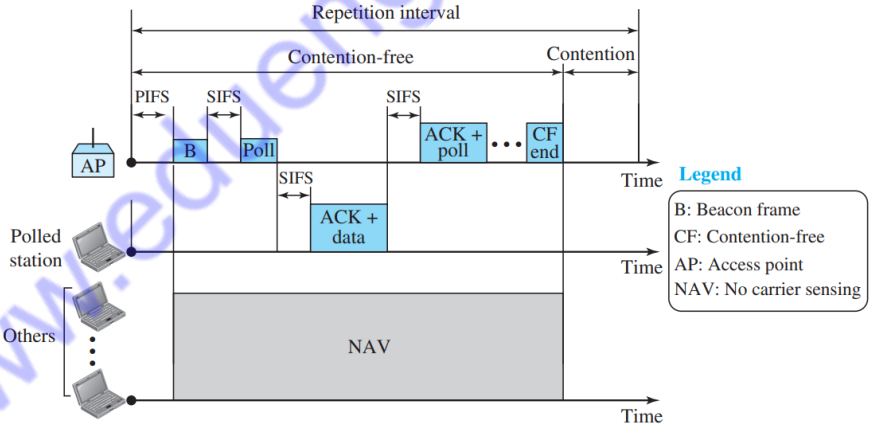


Collision During Handshaking

- Two or more stations may try to send RTS frames at the same time. These control frames may collide. However, because there is no mechanism for collision detection, the sender assumes there has been a collision if it has not received a CTS frame from the receiver.

Point Coordination Function (PCF):

- The point coordination function (PCF) is an optional access method that can be implemented in an infrastructure network
- It is implemented on top of the DCF and is used mostly for time-sensitive transmission.
- The AP performs polling for stations that are capable of being polled. The stations are polled one after another, sending any data they have to the AP.

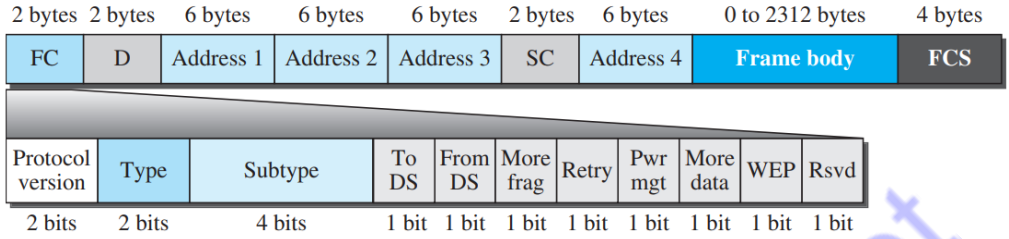


- To give priority to PCF over DCF, another interframe space, PIFS, has been defined.
- PIFS (PCF IFS) is shorter than DIFS.
- Due to the priority of PCF over DCF, stations that only use DCF may not gain access to the medium.
- To prevent this, a repetition interval has been designed to cover both contention-free PCF and contention-based DCF traffic. The repetition interval, which is repeated continuously, starts with a special control frame, called a beacon frame.
- When the stations hear the beacon frame, they start their NAV for the duration of the contention-free period of the repetition interval

- At the end of the contention-free period, the PC sends a CF end (contention-free end) frame to allow the contention-based stations to use the medium.

Frame Format

The MAC layer frame consists of nine fields



Frame control (FC).

The FC field is 2 bytes long and defines the type of frame and some control information.

Field	*Explanation*
Version	Current version is 0
Type	Type of information: management (00), control (01), or data (10)
Subtype	Subtype of each type (see Table 15.2)
To DS	Defined later
From DS	Defined later
More frag	When set to 1, means more fragments
Retry	When set to 1, means retransmitted frame
Pwr mgt	When set to 1, means station is in power management mode
More data	When set to 1, means station has more data to send
WEP	Wired equivalent privacy (encryption implemented)
Rsvd	Reserved

D.This field defines the duration of the transmission that is used to set the value of NAV. In one control frame, it defines the ID of the frame.

Addresses. There are four address fields, each 6 bytes long.

Sequence control. This field, often called the SC field, defines a 16-bit value. The first four bits define the fragment number; the last 12 bits define the sequence number, which is the same in all fragments.

Frame body. This field, which can be between 0 and 2312 bytes, contains information based on the type and the subtype defined in the FC field.

FCS. The FCS field is 4 bytes long and contains a CRC-32 error-detection sequence

Frame Types

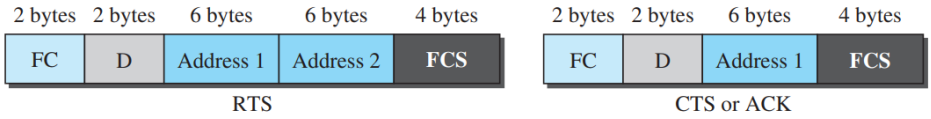
- A wireless LAN defined by IEEE 802.11 has three categories of frames: management frames, control frames, and data frames.

Management Frames

Management frames are used for the initial communication between stations and access points.

Control Frames

Control frames are used for accessing the channel and acknowledging frames.



Data Frames

Data frames are used for carrying data and control information.

BLUETOOTH

- Bluetooth is a wireless LAN technology designed to connect devices of different functions such as telephones, notebooks, computers ,cameras, printers, and even coffee makers when they are at a short distance from each other.
- A Bluetooth LAN is an ad hoc network, which means that the network is formed spontaneously; the devices, sometimes called gadgets, find each other and make a network called a piconet.
- A Bluetooth LAN can even be connected to the Internet if one of the gadgets has this capability. A Bluetooth LAN, by nature, cannot be large.

Applications:

- Peripheral devices such as a wireless mouse or keyboard can communicate with the computer through this technology.
- Monitoring devices can communicate with sensor devices in a small health care center.
- Home security devices can use this technology to connect different sensors to the main security controller.
- Conference attendees can synchronize their laptop computers at a conference.

Bluetooth was originally started as a project by the Ericsson Company. It is named for Harald Blaatand, the king of Denmark (940-981) who united Denmark and Norway.

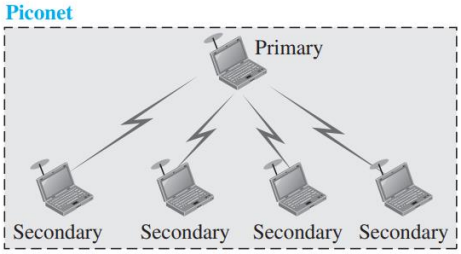
Today, **Bluetooth technology is the implementation of a protocol defined by the IEEE 802.15 standard.** The standard defines a wireless personal-area network (PAN) operable in an area the size of a room or a hall.

Architecture

Bluetooth defines two types of networks: piconet and scatternet.

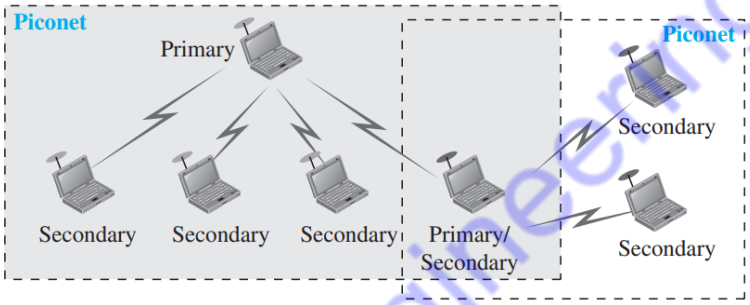
Piconets :

- A Bluetooth network is called a piconet, or a small net.
- A piconet can have up to eight stations, one of which is called the primary; the rest are called secondaries.
- All the secondary stations synchronize their clocks and hopping sequence with the primary.
- A piconet can have only one primary station.
- The communication between the primary and secondary stations can be one-to-one or one-to-many
- Although a piconet can have a maximum of seven secondaries, additional secondaries can be in the parked state.
- A secondary in a parked state is synchronized with the primary, but cannot take part in communication until it is moved from the parked state to the active state



Scatternet:

- Piconets can be combined to form what is called a scatternet.
- A secondary station in one piconet can be the primary in another piconet.
- This station can receive messages from the primary in the first piconet (as a secondary) and, acting as a primary, deliver them to secondaries in the second piconet.
- A station can be a member of two piconets



Bluetooth Layers

L2CAP :The Logical Link Control and Adaptation Protocol, or L2CAP (L2 here means LL), is roughly equivalent to the LLC sublayer in LANs. It is used for data exchange on an ACL link; SCO channels do not use L2CAP

- The 16-bit length field defines the size of the data, in bytes, coming from the upper layers. Data can be up to 65,535 bytes.
- The channel ID (CID) defines a unique identifier for the virtual channel created at this level.
- The L2CAP has specific duties: multiplexing, segmentation and reassembly, quality of service (QoS), and group management.

TDMA:

- Bluetooth uses a form of TDMA that is called TDD-TDMA (time-division duplex TDMA).
- TDD-TDMA is a kind of half-duplex communication in which the sender and receiver send and receive data, but not at the same time (half-duplex)
- The communication for each direction uses different hops. This is similar to walkie-talkies using different carrier frequencies

Links

Two types of links can be created between a primary and a secondary: SCO links and ACL links.

SCO:

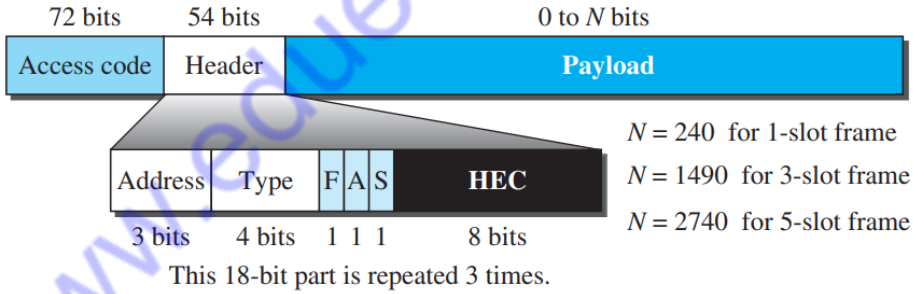
- A synchronous connection-oriented (SCO) link is used when avoiding latency (delay in data delivery) is more important than integrity (error-free delivery).
- In an SCO link, a physical link is created between the primary and a secondary by reserving specific slots at regular intervals.
- The basic unit of connection is two slots, one for each direction. If a packet is damaged, it is never retransmitted

ACL:

- An asynchronous connectionless link (ACL) is used when data integrity is more important than avoiding latency.
- In this type of link, if a payload encapsulated in the frame is corrupted, it is retransmitted.
- A secondary returns an ACL frame in the available odd-numbered slot if the previous slot has been addressed to it. ACL can use one, three, or more slots and can achieve a maximum data rate of 721 kbps

Frame Format

- A frame in the baseband layer can be one of three types: **one-slot, three-slot, or fiveslot**. A slot, as we said before, is 625 µs.
- In a one-slot frame exchange, 259 µs is needed for hopping and control mechanisms. This means that a one-slot frame can last only 625 − 259, or 366 µs.
- With a 1-MHz bandwidth and 1 bit/Hz, the size of a oneslot frame is 366 bits.
- A three-slot frame occupies three slots. However, since 259 µs is used for hopping, the length of the frame is 3 × 625 − 259 = 1616 µs or 1616 bits. A device that uses a three-slot frame remains at the same hop for three slots.
- A five-slot frame also uses 259 bits for hopping, which means that the length of the frame is 5 × 625 − 259 = 2866 bits.



Access code. This 72-bit field normally contains synchronization bits and the identifier of the primary to distinguish the frame of one piconet from that of another.

Header. This 54-bit field is a repeated 18-bit pattern. Each pattern has the following subfields:

a. **Address-**The 3-bit address subfield can define up to seven secondary (1 to 7). If the address is zero, it is used for broadcast communication from the primary to all secondaries.
b. **Type-**The 4-bit type subfield defines the type of data coming from the upper layers.
c. **F.** This 1-bit subfield is for flow control. When set (1), it indicates that the device is unable to receive more frames (buffer is full).
d. **A.** This 1-bit subfield is for acknowledgment. Bluetooth uses Stop-and-Wait ARQ; 1 bit is sufficient for acknowledgment.

e. **S**. This 1-bit subfield holds a sequence number. Bluetooth uses Stop-and-Wait ARQ; 1 bit is sufficient for sequence numbering.

f. **HEC.** The 8-bit header error correction subfield is a checksum to detect errors in each 18-bit header section. The header has three identical 18-bit sections. The receiver compares these three sections, bit by bit. If each of the corresponding bits is the same, the bit is accepted; if not, the majority opinion rules. This is a form of forward error correction. This double error control is needed because the nature of the communication, via air, is very noisy. Note that there is no retransmission in this sublayer.

Payload. This subfield can be 0 to 2740 bits long. It contains data or control information coming from the upper layers.

Band Bluetooth uses a 2.4-GHz ISM band divided into 79 channels of 1 MHz each.

FHSS Bluetooth uses the frequency-hopping spread spectrum (FHSS) method in the physical layer to avoid interference from other devices or other networks

Modulation To transform bits to a signal, Bluetooth uses a sophisticated version of FSK, called GFSK (FSK with Gaussian bandwidth filtering)

Flow and Error Control Protocols:

The Data Link Control (DLC) protocol can be either connectionless or connection-oriented.

Connectionless Protocol:

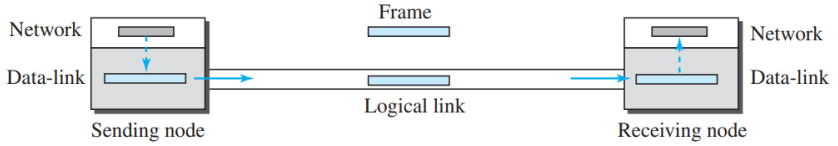
- In a connectionless protocol, frames are sent from one node to the next without any relationship between the frames; each frame is independent.
- The frames are not numbered and there is no sense of ordering.
- Most of the data-link protocols for LANs are connectionless protocols.

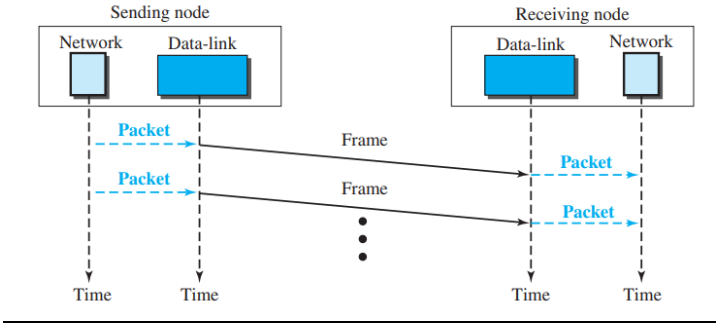
Connection-Oriented Protocol

- In a connection-oriented protocol, a logical connection should first be established between the two nodes (setup phase).
- After all frames that are somehow related to each other are transmitted (transfer phase), the logical connection is terminated (teardown phase).
- In this type of communication, the frames are numbered and sent in order.
- If they are not received in order, the receiver needs to wait until all frames belonging to the same set are received and then deliver them in order to the network layer.
- Connectionoriented protocols are rare in wired LANs, but we can see them in some point-to-point protocols, some wireless LANs, and some WANs.

Simple Protocol

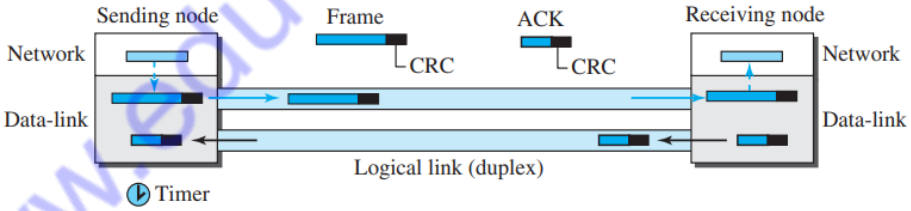
- First protocol is a simple protocol with neither flow nor error control.
- The receiver can immediately handle any frame it receives. In other words, the receiver can never be overwhelmed with incoming frames
- The sender site should not send a frame until its network layer has a message to send.
- The receiver site cannot deliver a message to its network layer until a frame arrives.





Stop-and-Wait Protocol

- Our second protocol is called the Stop-and-Wait protocol, which uses both flow and error control
- In this protocol, the sender sends one frame at a time and waits for an acknowledgment before sending the next one.
- To detect corrupted frames, we need to add a CRC to each data frame.
- When a frame arrives at the receiver site, it is checked. If its CRC is incorrect, the frame is corrupted and silently discarded.
- The silence of the receiver is a signal for the sender that a frame was either corrupted or lost. Every time the sender sends a frame, it starts a timer.
- If an acknowledgment arrives before the timer expires, the timer is stopped and the sender sends the next frame.
- If the timer expires, the sender resends the previous frame, assuming that the frame was either lost or corrupted. This means that the sender needs to keep a copy of the frame until its acknowledgment arrives.
- When the corresponding acknowledgment arrives, the sender discards the copy and sends the next frame if it is ready.



Sender States

The sender is initially in the ready state, but it can move between the ready and blocking state

Ready State:

- When the sender is in this state, it is only waiting for a packet from the network layer. If a packet comes from the network layer, the sender creates a frame, saves a copy of the frame, starts the only timer and sends the frame.
- The sender then moves to the blocking state.

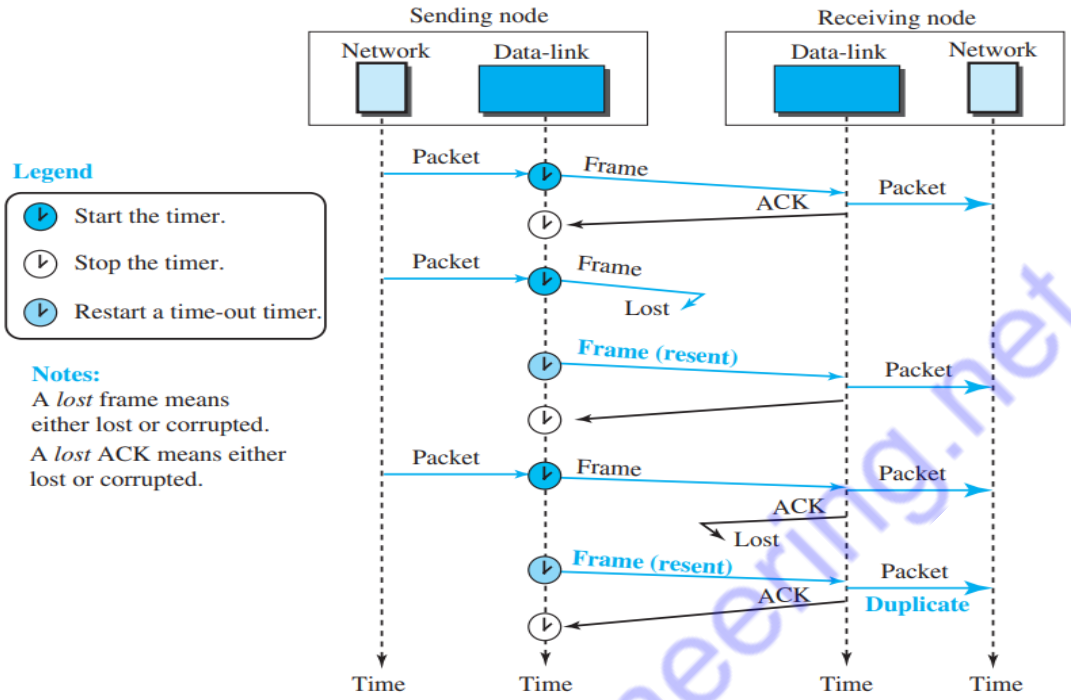
Blocking State:

When the sender is in this state, three events can occur:

a. If a time-out occurs, the sender resends the saved copy of the frame and restarts the timer.

b. If a corrupted ACK arrives, it is discarded.

c. If an error-free ACK arrives, the sender stops the timer and discards the saved copy of the frame. It then moves to the ready state.



Receiver

- The receiver is always in the ready state. Two events may occur:

  a. If an error-free frame arrives, the message in the frame is delivered to the network layer and an ACK is sent.

  b. If a corrupted frame arrives, the frame is discarded.

HDLC (High-level Data Link Control)

HDLC is a bit-oriented protocol for communication over point-to-point and multipoint links.

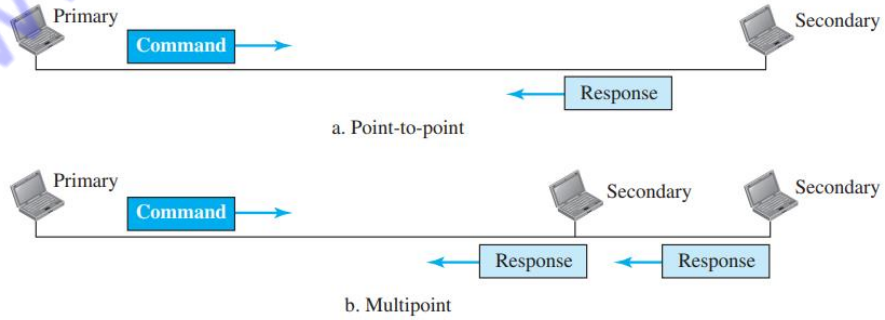
It implements the Stop-and-Wait protocol

Configurations and Transfer Modes

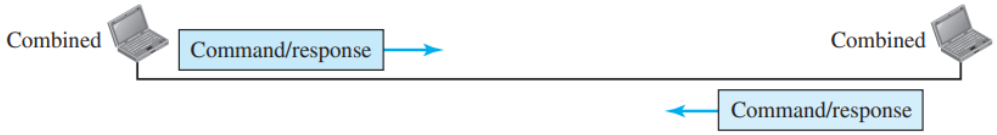
HDLC provides two common transfer modes that can be used in different configurations:

Normal response mode (NRM) and asynchronous balanced mode (ABM).

In normal response mode (NRM), the station configuration is unbalanced. Assume one primary station and multiple secondary stations. A primary station can send commands; a secondary station can only respond. The NRM is used for both point-to-point and multipoint links



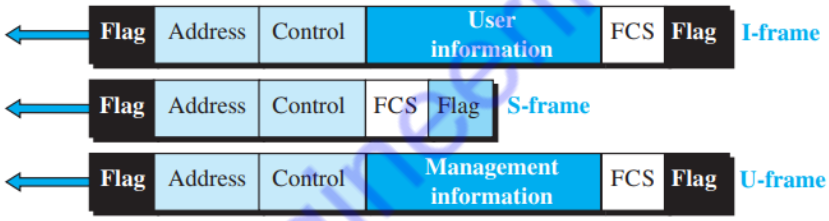
In ABM, the configuration is balanced. The link is point-to-point, and each station can function as a primary and a secondary



Framing

HDLC defines three types of frames:
information frames (I-frames), supervisory frames (S-frames), and
unnumbered frames (U-frames).

- Each type of frame serves as an envelope for the transmission of a different type of message. Iframes are used to data-link user data and control information relating to user data (piggybacking).
- S-frames are used only to transport control information. U-frames are reserved for system management.
- Information carried by U-frames is intended for managing the link itself



Flag field

- This field contains synchronization pattern 01111110, which identifies both the beginning and the end of a frame.

Address field

- This field contains the address of the secondary station. If a primary station created the frame, it contains a to address. If a secondary station creates the frame, it contains a from address. The address field can be one byte or several bytes long, depending on the needs of the network.

Control field.

- The control field is one or two bytes used for flow and error control.

Information field.

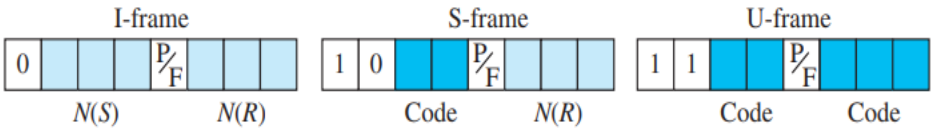
- The information field contains the user's data from the network layer or management information. Its length can vary from one network to another.

FCS field.

- The frame check sequence (FCS) is the HDLC error detection field. It can contain either a 2- or 4-byte CRC.

Control Field:

The control field determines the type of frame and defines its functionality



Control Field for I-Frames:

- I-frames are designed to carry user data from the network layer.
- In addition, they can include flow- and error-control information (piggybacking).
- The subfields in the control field are used to define these functions.
- The first bit defines the type. If the first bit of the control field is 0, this means the frame is an I-frame.
- The next 3 bits, called N(S), define the sequence number of the frame.
- The last 3 bits, called N(R), correspond to the acknowledgment number when piggybacking is used.
- The single bit between N(S) and N(R) is called the P/F bit.
- The P/F field is a single bit with a dual purpose. It has meaning only when it is set (bit = 1) and can mean poll or final.
- It means poll when the frame is sent by a primary station to a secondary (when the address field contains the address of the receiver).
- It means final when the frame is sent by a secondary to a primary (when the address field contains the address of the sender).

Control Field for S-Frames

Supervisory frames are used for flow and error control whenever piggybacking is either impossible or inappropriate.

S-frames do not have information fields.

If the first 2 bits of the control field are 10, this means the frame is an S-frame. The last 3 bits, called N(R), correspond to the acknowledgment number (ACK) or negative acknowledgment number (NAK), depending on the type of S-frame.

The 2 bits called code are used to define the type of S-frame itself.

With 2 bits, there are four types of S-frames possible

- **Receive ready (RR).** If the value of the code subfield is 00, it is an RR S-frame. This kind of frame acknowledges the receipt of a safe and sound frame or group of frames. In this case, the value of the N(R) field defines the acknowledgment number
- **Receive not ready (RNR).** If the value of the code subfield is 10, it is an RNR Sframe. It acknowledges the receipt of a frame or group of frames, and it announces that the receiver is busy and cannot receive more frames. It acts as a kind of congestion-control mechanism by asking the sender to slow down. The value of N(R) is the acknowledgment number.
- **Reject (REJ).** If the value of the code subfield is 01, it is an REJ S-frame. This is a NAK frame, but not like the one used for Selective Repeat ARQ. The value of N(R) is the negative acknowledgment number.
- **Selective reject (SREJ)**. If the value of the code subfield is 11, it is an SREJ Sframe. This is a NAK frame used in Selective Repeat ARQ. The value of N(R) is the negative acknowledgment number.

Control Field for U-Frames

- Unnumbered frames are used to exchange session management and control information between connected devices.
- U-frames contain an information field, but one used for system management information, not user data.
- U-frame codes are divided into two sections: a 2-bit prefix before the P/ F bit and a 3-bit suffix after the P/F bit. Together, these two segments (5 bits) can be used to create up to 32 different types of U-frames.

POINT-TO-POINT PROTOCOL (PPP)

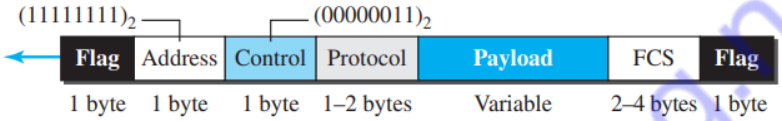
One of the most common protocols for point-to-point access is the Point-to-Point Protocol (PPP). Today, millions of Internet users who need to connect their home computers to the server of an Internet service provider use PPP

Services Provided by PPP:

- PPP defines the format of the frame to be exchanged between devices.
- It also defines how two devices can negotiate the establishment of the link and the exchange of data. PPP is designed to accept payloads from several network layers.
- Authentication is also provided in the protocol, but it is optional.
- The new version of PPP, called Multilink PPP, provides connections over multiple links.

Framing

PPP uses a character-oriented (or byte-oriented) frame.



Address. The address field in this protocol is a constant value and set to 11111111 (broadcast address).

Control. This field is set to the constant value 00000011.PPP does not provide any flow control. Error control is also limited to error detection.

Protocol. The protocol field defines what is being carried in the data field: either user data or other information. This field is by default 2 bytes long, but the two parties can agree to use only 1 byte.

Payload field. This field carries either the user data or other information. The data field is a sequence of bytes with the default of a maximum of 1500 bytes; but this can be changed during negotiation. The data field is byte-stuffed if the flag byte pattern appears in this field. Because there is no field defining the size of the data field, padding is needed if the size is less than the maximum default value or the maximum negotiated value.

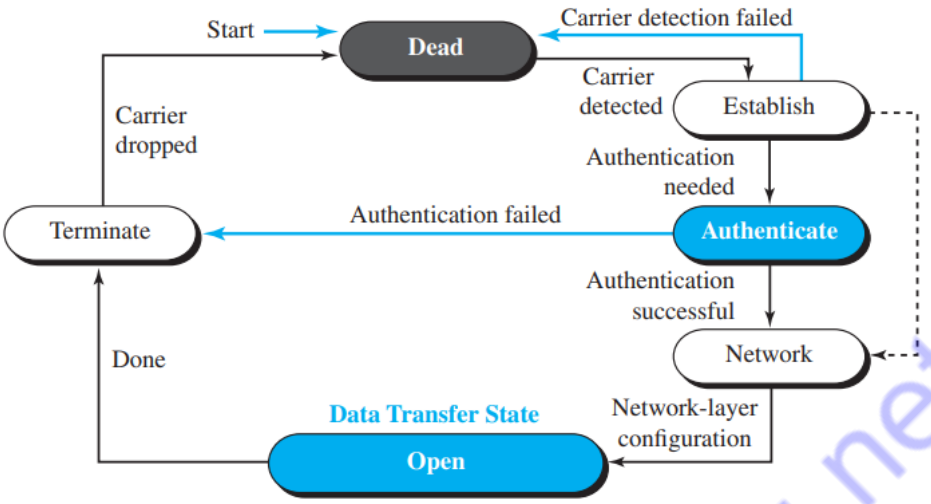
FCS. The frame check sequence (FCS) is simply a 2-byte or 4-byte standard CRC

Byte Stuffing

Since PPP is a byte-oriented protocol, the flag in PPP is a byte that needs to be escaped whenever it appears in the data section of the frame. The escape byte is 01111101, which means that every time the flag like pattern appears in the data, this extra byte is stuffed to tell the receiver that the next byte is not a flag.

Transition Phases

- A PPP connection goes through phases which can be shown in a transition phase diagram
- The transition diagram, which is an FSM, starts with the dead state.
- In this state, there is no active carrier and the line is quiet.
- When one of the two nodes starts the communication, the connection goes into the establish state. In this state, options are negotiated between the two parties.



- If the two parties agree that they need authentication (for example, if they do not know each other), then the system needs to do authentication (an extra step); otherwise, the parties can simply start communication.

EDU ENGINEERING

PIONEER OF ENGINEERING NOTES

TAMIL NADU'S BEST EDTECH PLATFORM FOR ENGINEERING

CONNECT WITH US

WEBSITE: www.eduengineering.net

TELEGRAM: @eduengineering

INSTAGRAM: @eduengineering

- **Regular Updates for all Semesters**
- **All Department** Notes AVAILABLE
- **Handwritten** Notes AVAILABLE
- **Past Year** Question Papers AVAILABLE
- **Subject wise** Question Banks AVAILABLE
- **Important Questions** for Semesters AVAILABLE
- Various **Author Books** AVAILABLE