UNIT 1
COMPUTER NETWORKS

CONTENTS

- **Introduction-** Perspectives Business Domains: Networks. Applications: Resource Sharing, Client Server programming, e-commerce and digital communications.
- **Introduction**: Networks, Network types.
- **Network Models:** TCP / IP protocol suite, Addressing, The OSI Model.
- **Transmission Modes:** Parallel Transmission and Serial Transmission. Link Layer: Data Link Control(DLC): DLC Services, Data Link Layer Protocols, High Level Data Link Control (HDLC), Point-to- Point Protocol (PPP): Framing, Transition phases. Media Access Control (MAC): Random Access: CSMA/CD,CSMA/CA.

PERSPECTIVES

- **An application programmer** would list the services that his or her application needs—for example, a guarantee that each message the application sends will be delivered without error within a certain amount of time or the ability to switch gracefully among different connections to the network as the user moves around.
- **A network operator** would list the characteristics of a system that is easy to administer and manage—for example, in which faults can be easily isolated, new devices can be added to the network and configured correctly, and it is easy to account for usage.
- **A network designer** would list the properties of a cost-effective design—for example, that network resources are efficiently utilized and fairly allocated to different users. Issues of performance are also likely to be important.

NETWORKS

- A **network** is the interconnection of a set of devices capable of communication. In this definition, a device can be a host (or an end system as it is sometimes called) such as a large computer, desktop, laptop, workstation, cellular phone, or security system.
- A device in this definition can also be a connecting device such as a router, which connects the network to other networks, a switch, which connects devices together, a modem (modulator-demodulator), which changes the form of data, and so on.
- These devices in a network are connected using wired or wireless transmission media such as cable or air.

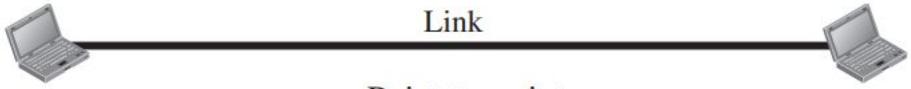
Network Criteria

- A network must be able to meet a certain number of criteria. The most important of these are **performance, reliability, and security.**
- **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. Performance is often evaluated by **two networking metrics: throughput and delay.**
- 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**

- 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.

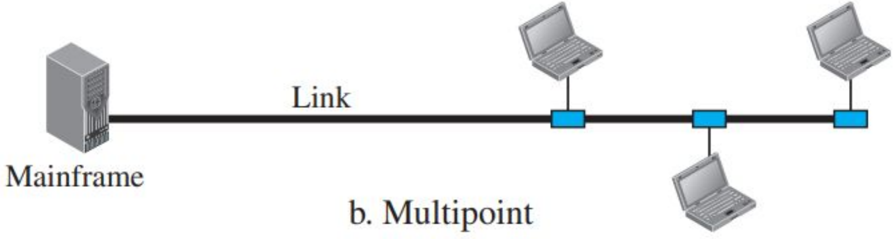
Physical Structures: **Type of Connection:**

- There are two possible types of connections: **point-to-point and multipoint.**
- 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**



a. Point-to-point

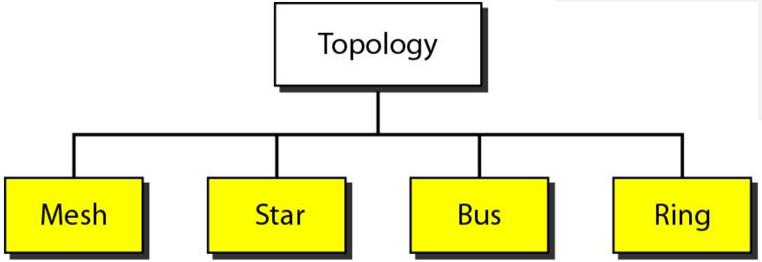
- A **multipoint** (also called multidrop) connection is one in which **more than two specific devices share a single link**
- In a multipoint environment, the c**apacity of the channel is shared, either spatially or temporally.**
- If several devices can use the link simultaneously, it is a **spatially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



b. Multipoint

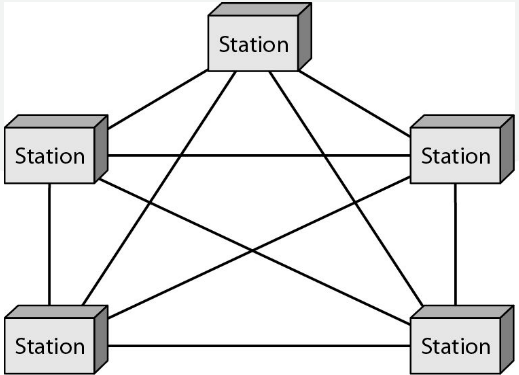
Network Topology

- The term physical topology refers to the **way in which a network is laid out physically.**
- **Two 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**



Mesh Topology

- **Every device has a dedicated point-to-point link to every other device**
- We need **n (n – 1) physical links** to connect n nodes if the links are simplex mode.
- If the links are in duplex mode we need **n (n – 1)/2** links
- To accommodate that many links, every device on the network must have **n – 1 input/output (I/O) ports** to be connected to the **other n – 1 stations.**



Advantages of Mesh topology :

- each connection **can carry its own load**
  → traffic between devices is not shared
- **robust**
- **high privacy / security**
- **ease of fault identification** / isolation

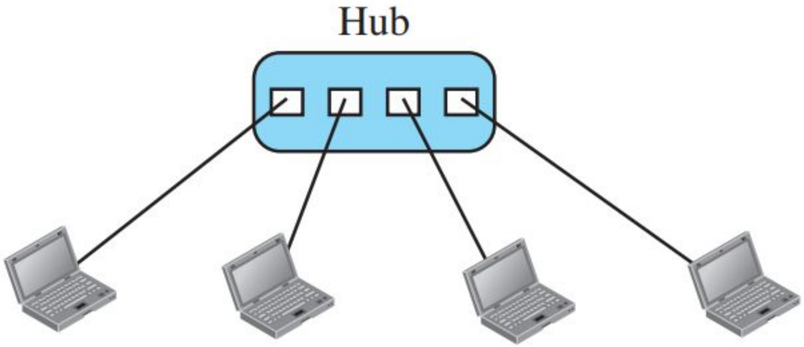
Disadvantages :

- **large amount of cabling and I/O ports**
- unwieldy cabling, **difficult to install / reinstall**
- **expensive**

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.**

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 device wants to send data to another, it sends the data to the controller, which then relays the data to the other connected device**



Advantages star topology:

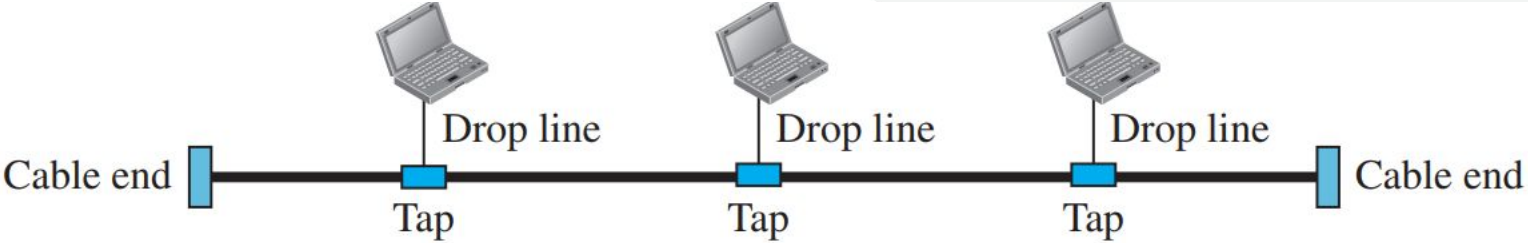
- **less cabling, less I/O ports, less expensive**
- **easy to install and re-configure**
- **robust** → only failed link is affected
- **ease of fault identification** / isolation

Disadvantage :

- **the hub is a single point of failure**

Bus Topology

- 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 connection running between the device and the main cable.**



Advantages of Bus topology:

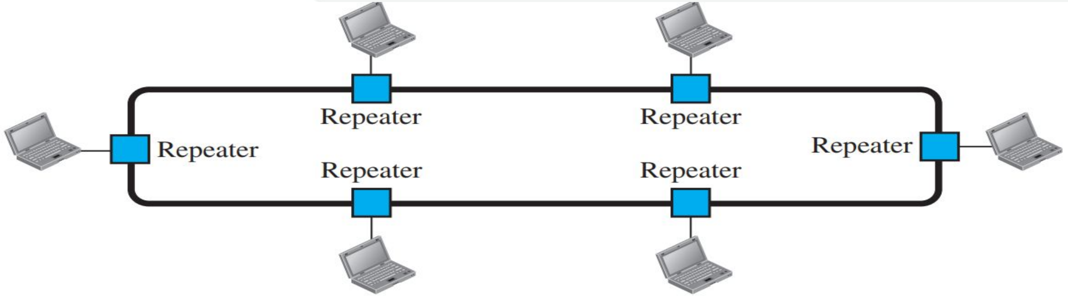
- **uses much less cabling**
- **ease of installation**

Disadvantages :

- **difficult reconnection** / fault isolation
- **difficult to add new devices** - may require
- **modification / replacement of backbone**
- **signal reflection at taps** → quality
- **degradation → limit on lengths / nodes**
- **break in bus cable stops all transmissions**

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 r**eaches 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**



Advantages of ring topology:

- **easy to install, reconfigure, add, delete**
- simplified **fault isolation**

Disadvantages:

- **limitation on maximum ring length / number of nodes**
- a **break in the ring can bring the entire network down**

- 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.

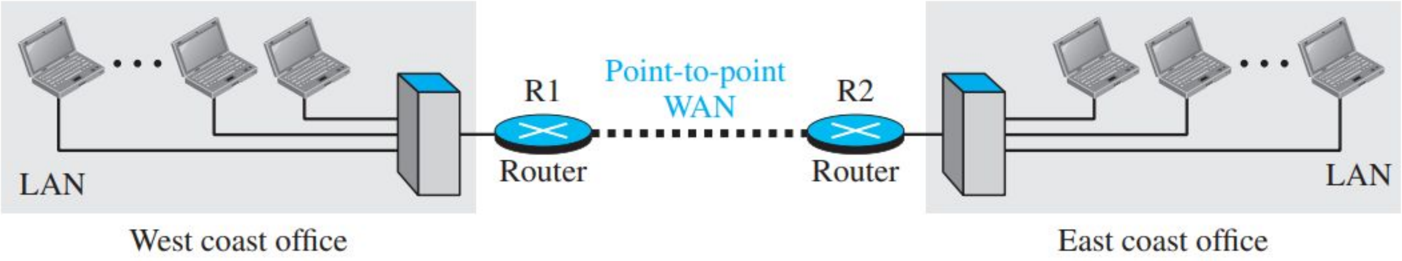
NETWORK TYPES

Local Area Network:

- A local area network (LAN) is usually privately owned and connects some hosts in a single office, building, or campus.
- Depending on the needs of an organization, 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 devices.
- Each host in a LAN has an identifier, an address, that uniquely defines the host in the LAN.
- A packet sent by a host to another host carries both the source host’s and the destination host’s addresses.

Internetwork

- Today, it is very rare to see a **LAN or a WAN in isolation; they are connected to one another.**
- When **two or more networks are connected, they make an internetwork, or internet**. As an example, assume that an o**rganization has two offices,** one on the e**ast coast and the other on the west coast.**
- Each office has a **LAN that allows all employees in the office to communicate with each other.**
- To make the communication between employees at different offices possible, the management leases a point-to-point dedicated **WAN** from a service provider, such as a telephone company, and connects the two LANs.
- Now the company has an internetwork, or a **private internet** (with lowercase i). Communication between offices is now possible



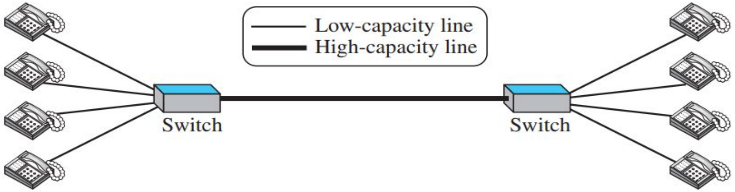
- When a host in the west coast office sends a message to another host in the **same office,** the router blocks the message, but the switch directs the message to the destination.
- On the other hand, when a host on the west coast sends a message to a host on the east coast, r**outer R1 routes the packet to router R2,** and the packet reaches the destination.

Switching

- An **internet is a switched network** in which a switch connects at least two links together.
- A **switch needs to forward data from a network to another network when required.**
- The two most common types of switched networks are **circuit-switched** and **packet-switched networks**.

Circuit-Switched Network

- In a circuit-switched network, a **dedicated connection, called a circuit,** is a**lways available between the two end systems; the switch can only make it active or inactive.**
- circuit switching was very common **in telephone networks in the past,** although **part of the telephone network today is a packet-switched network**
- Thick line is a high-capacity communication line that can handle four voice communications at the same time; the capacity can be shared between all pairs of telephone sets.

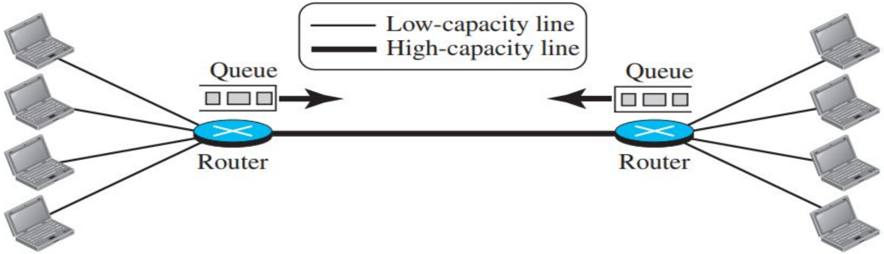


- In the **first case,** all telephone sets are busy; four people at one site are talking with four people at the other site; **the capacity of the thick line is fully used.** In the second case, only one telephone set at one side is connected to a telephone set at the other side; only one-fourth of the capacity of the thick line is used.
- **This means that a circuit-switched network is efficient only when it is working at its full capacity; most of the time, it is inefficient because it is working at partial capacity.**

- Now assume that the capacity of the thick line is only twice the capacity of the data line connecting the computers to the routers.
- If only two computers (one at each site) need to communicate with each other, there is no waiting for the packets.
- However, if packets arrive at one router when the thick line is already working at its full capacity, the **packets should be stored and forwarded in the order they arrived.**
- **The two simple examples show that a packet-switched network is more efficient than a circuit switched network, but the packets may encounter some delays**

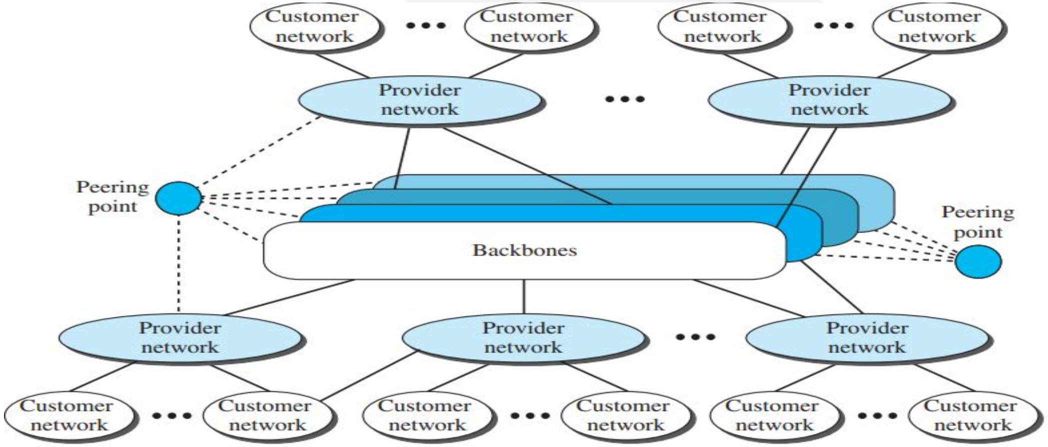
Packet-Switched Network

- In a computer network, the **communication between the two ends is done in blocks of data called packets.**
- In other words, **instead of the continuous communication we see between two telephone sets when they are being used, we see the exchange of individual data packets between the two computers.**
- This allows us to make the **switches function for both storing and forwarding** because **a packet is an independent entity that can be stored and sent later**.



The Internet

- An **internet (note the lowercase i) is two or more networks that can communicate with each other.**
- The most notable **internet is called the Internet (uppercase I), and is composed of thousands of interconnected networks.**



- The **Internet as several backbones, provider networks, and customer networks.**
- At the top level, the **backbones are large networks owned by some communication companies** such as Sprint, Verizon (MCI), AT&T, and NTT.
- The **backbone networks are connected through some complex switching systems, called peering points.**
- At the **second level, there are smaller networks, called provider networks, that use the services of the backbones for a fee.**
- The **provider networks are connected to backbones and sometimes to other provider networks.**
- **The customer networks are networks at the edge of the Internet that actually use the services provided by the Internet.**
- They **pay fees to provider networks for receiving services.** Backbones and provider networks are also called **Internet Service Providers** (ISPs).
- The backbones are often referred to as **international ISPs; the provider networks are often referred to as national or regional ISPs.**

Accessing the Internet

- The Internet today is an internetwork that allows any user to become part of it.
- The user, however, needs to be physically connected to an ISP.
- The physical connection is normally done through a point-to-point WAN.

1. Using Telephone Networks: Since most telephone networks have already connected themselves to the Internet, one option for residences and small businesses to connect to the Internet is to **change the voice line between the residence or business and the telephone center to a point-to-point WAN.**

- **Dial-up service** :converts data to voice
- **DSL Service**: also allows the line to be used simultaneously for voice and data communication

2. Using Cable Networks: The **cable companies** have been upgrading their cable networks and connecting to the Internet. A residence or a small business can be connected to the Internet by using this service.

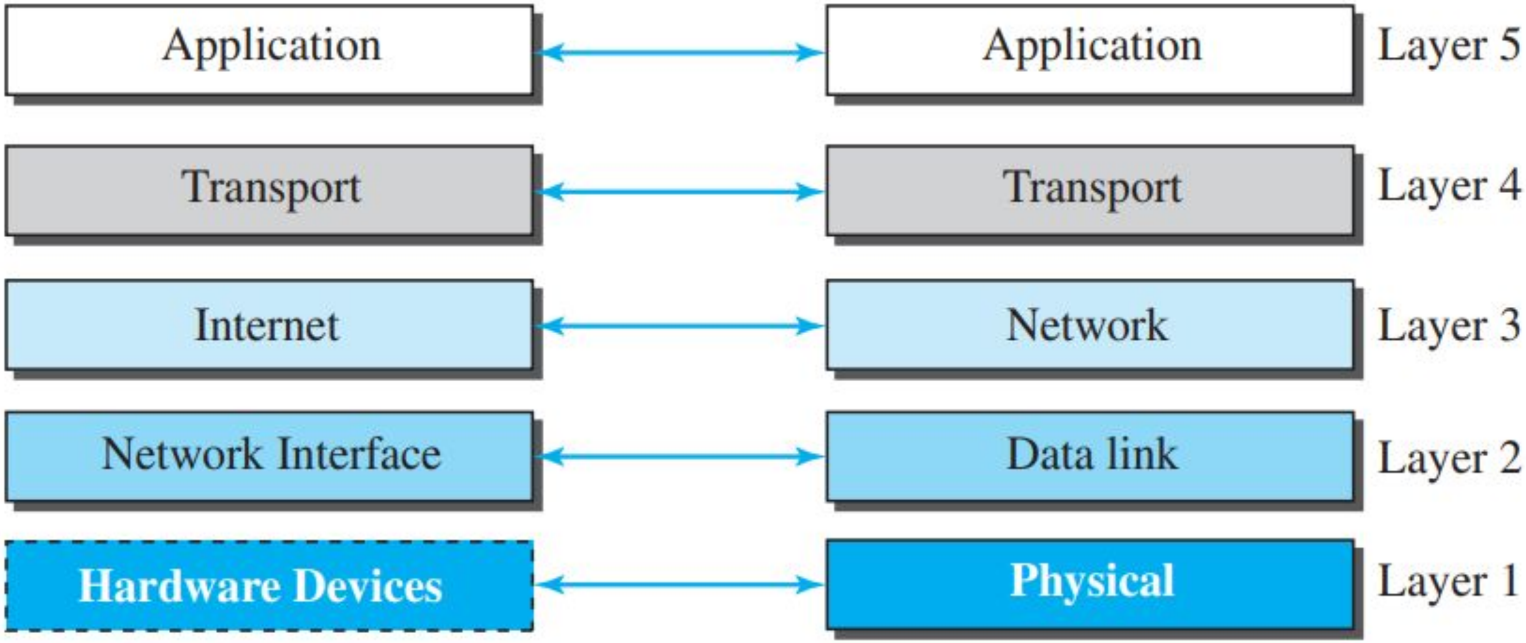
3. Using Wireless Networks: With the **growing wireless WAN access,** a household or a small business can be connected to the Internet through a wireless WAN

4. Direct Connection to the Internet: A **large organization or a large corporation can itself become a local ISP** and be **connected to the Internet.** This can be done if the organization or the corporation **leases a high-speed WAN from a carrier provider and connects itself to a regional ISP.**

For example, a **large university with several campuses can create an internetwork and then connect the internetwork to the Internet.**

TCP/IP PROTOCOL SUITE

- 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.
- The term hierarchical means that 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.
- Today, however, TCP/IP is thought of as a five-layer model



Application | Application | Layer 5

Transport | Transport | Layer 4

Internet | Network | Layer 3

Network Interface | Data link | Layer 2

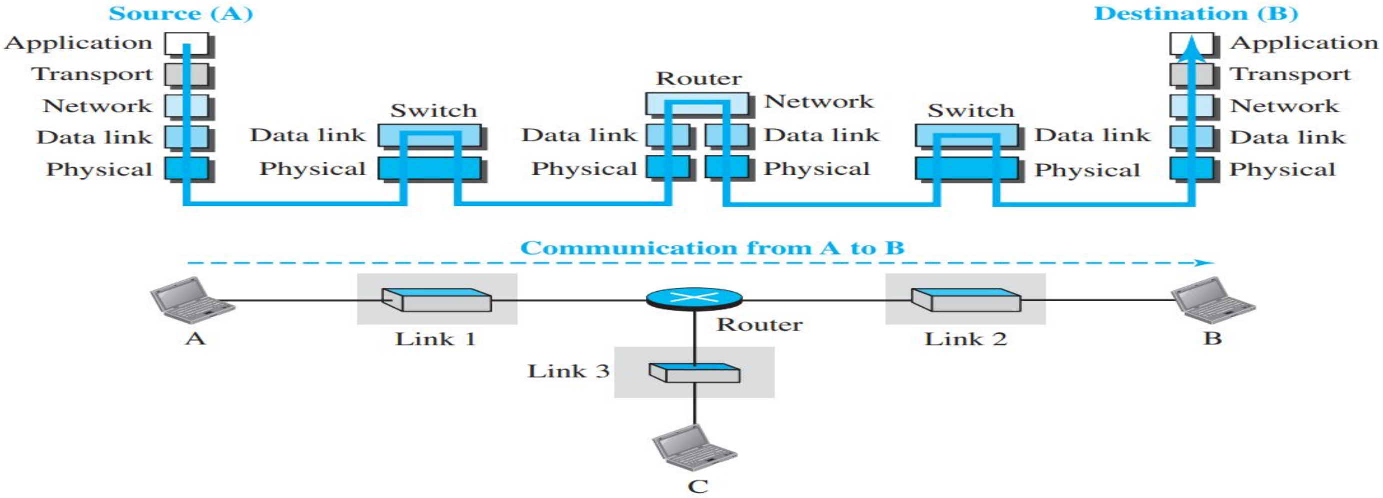
Hardware Devices | Physical | Layer 1

a. Original layers

b. Layers used in this book

Layered Architecture

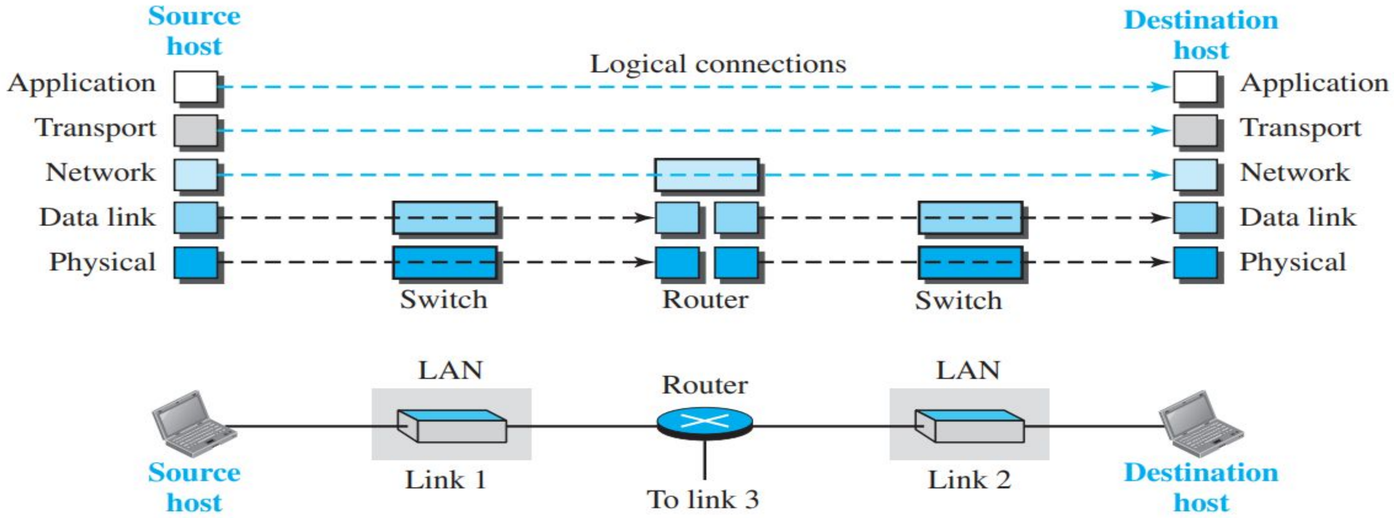
- To show how the layers in the TCP/IP protocol suite are involved in communication between two hosts, we assume that we want to use the suite in a small internet made up of three LANs (links), each with a link-layer switch. We also assume that the links are connected by one router,



- Let us assume that computer A communicates with computer B.
- As the figure shows, we have five communicating devices in this communication: source host (computer A), the link-layer switch in link 1, the router, the link-layer switch in link 2, and the destination host (computer B).
- Each device is involved with a set of layers depending on the role of the device in the internet.
- The two hosts are involved in all five layers; the source host needs to create a message in the application layer and send it down the layers so that it is physically sent to the destination host.
- The destination host needs to receive the communication at the physical layer and then deliver it through the other layers to the application layer.

Layers in the TCP/IP Protocol Suite

- We briefly discuss the functions and duties of layers in the TCP/IP protocol suite
- To better understand the duties of each layer, we need to think about the logical connections between layers.



- The duty of the application, transport, and network layers is end-to-end.
- However, the duty of the data-link and physical layers is hop-to-hop, in which a hop is a host or router.
- In other words, the domain of duty of the top three layers is the internet, and the domain of duty of the two lower layers is the link.
- **Note that**, although the logical connection at the network layer is between the two hosts, we can only say that identical objects exist between two hops in this case because a router may fragment the packet at the network layer and send more packets than received

Description of Each Layer: Physical Layer

- the physical layer is responsible for carrying individual bits in a frame across the link
- Two devices are connected by a transmission medium (cable or air).
- We need to know that 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.
- The data-link layer takes a datagram and encapsulates it in a packet called a **frame**
- Some 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.
- 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. This means that if any of theses services is required for an application, the application should rely only on the transport-layer protocol.

- The network layer also includes unicast (one-to-one) and multicast (one-to-many) routing protocols.
- 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 logical connection at the transport layer is also end-to-end.
- The transport layer at the source host gets the message from the application layer, encapsulates it in a transport layer packet (called a segment or a user datagram in different protocols) and sends it, through the logical (imaginary) connection, to the transport layer at the destination host
- 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, error control, and congestion control to reduce the loss of segments due to congestion in the network.

- The other common protocol, **User Datagram Protocol** (UDP), is a connectionless protocol that transmits user datagrams without first creating a logical connection.
- In UDP, each user datagram is an independent entity without being related to the previous or the next one (the meaning of the term connectionless).
- UDP is a simple protocol that does not provide flow, error, or congestion control.
- Its simplicity, which means small overhead, is attractive to an application program that needs to send short messages and cannot afford the retransmission of the packets involved in TCP, when a packet is corrupted or lost.
- A new protocol, **Stream Control Transmission Protocol** (SCTP) is designed to respond to new applications that are emerging in the multimedia

Application Layer

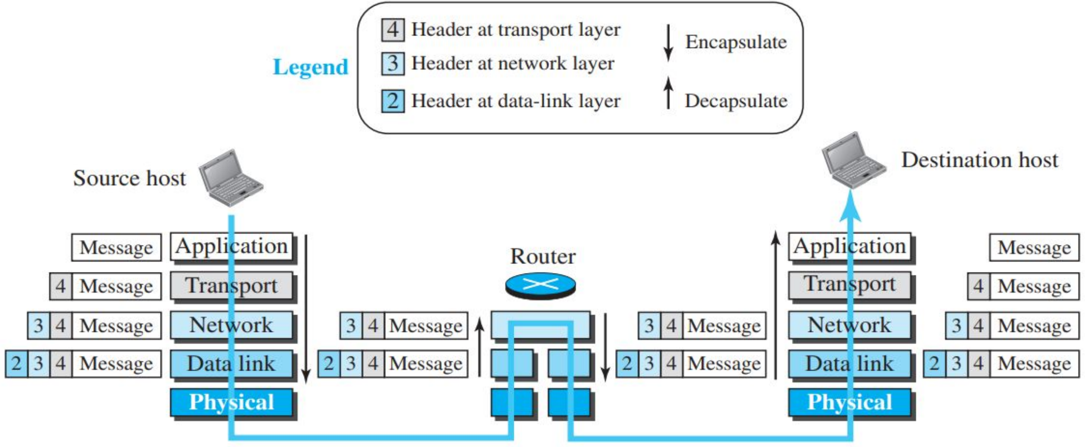
- The two application layers exchange messages between each other as though there were a bridge between the two layers.
- Communication at the application layer is between two processes
- To communicate, a process sends a request to the other process and receives a response. Process-to-process communication is the duty of the application layer.
- The application layer in the Internet includes many predefined protocols, but a user can also create a pair of processes to be run at the two hosts.
- HTTP, WWW,SMTP, FTP, TELNET, SSH, SNMP, DNS etc are application layer protocols

Encapsulation and Decapsulation

Encapsulation at the Source Host: At the source, we have only encapsulation.

1. At the application layer, the data to be exchanged is referred to as a message. A message normally does not contain any header or trailer
2. The transport layer takes the message as the payload, the load that the transport layer should take care of. It adds the transport layer header to the payload, which contains the identifiers of the source and destination application programs that want to communicate plus some more information that is needed for the end-to-end delivery of the message, such as information needed for flow, error control, or congestion control.
3. The result is the transport-layer packet, which is called the segment (in TCP) and the user datagram (in UDP).

The transport layer then passes the packet to the network layer.



3. The network layer takes the transport-layer packet as data or payload and adds its own header to the payload. The header contains the addresses of the source and destination hosts and some more information used for error checking of the header, fragmentation information, and so on. The result is the network-layer packet, called a datagram. The network layer then passes the packet to the data-link layer.

4. The data-link layer takes the network-layer packet as data or payload and adds its own header, which contains the link-layer addresses of the host or the next hop (the router). The result is the link-layer packet, which is called a frame. The frame is passed to the physical layer for transmission.

Decapsulation and Encapsulation at the Router

At the router, we have both **decapsulation and encapsulation** because the router is connected to two or more links.

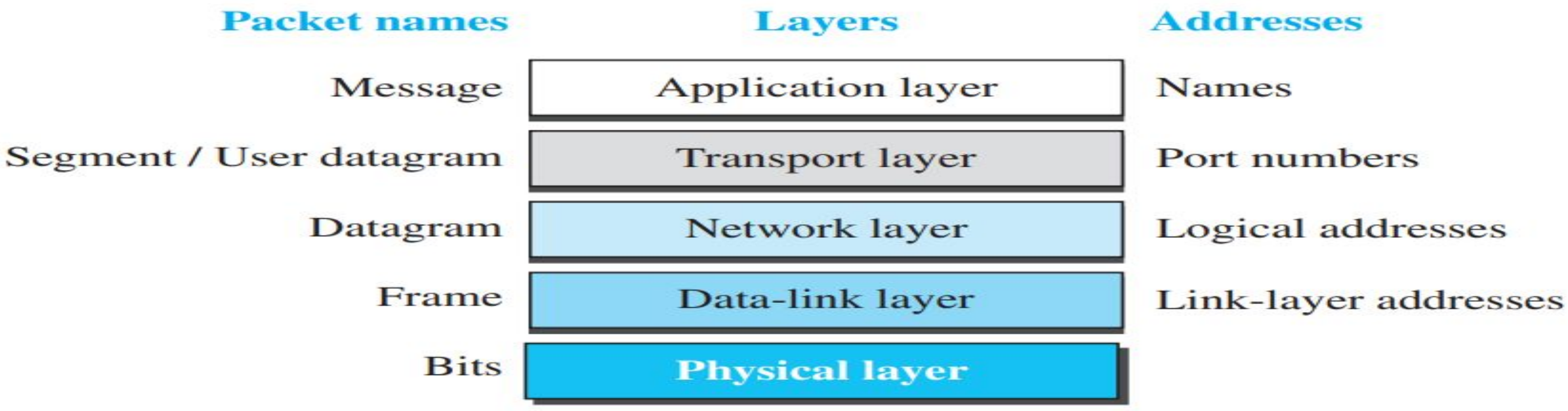
1. After the set of bits are delivered to the data-link layer, this layer decapsulates the datagram from the frame and passes it to the network layer.
2. The network layer only inspects the source and destination addresses in the datagram header and consults its forwarding table to find the next hop to which the datagram is to be delivered. The contents of the datagram should not be changed by the network layer in the router unless there is a need to fragment the datagram if it is too big to be passed through the next link. The datagram is then passed to the data-link layer of the next link.
3. The data-link layer of the next link encapsulates the datagram in a frame and passes it to the physical layer for transmission

Decapsulation at the Destination Host

- At the destination host, each layer only decapsulates the packet received, removes the payload, and delivers the payload to the next-higher layer protocol until the message reaches the application layer.
- It is necessary to say that decapsulation in the host involves error checking.

Addressing

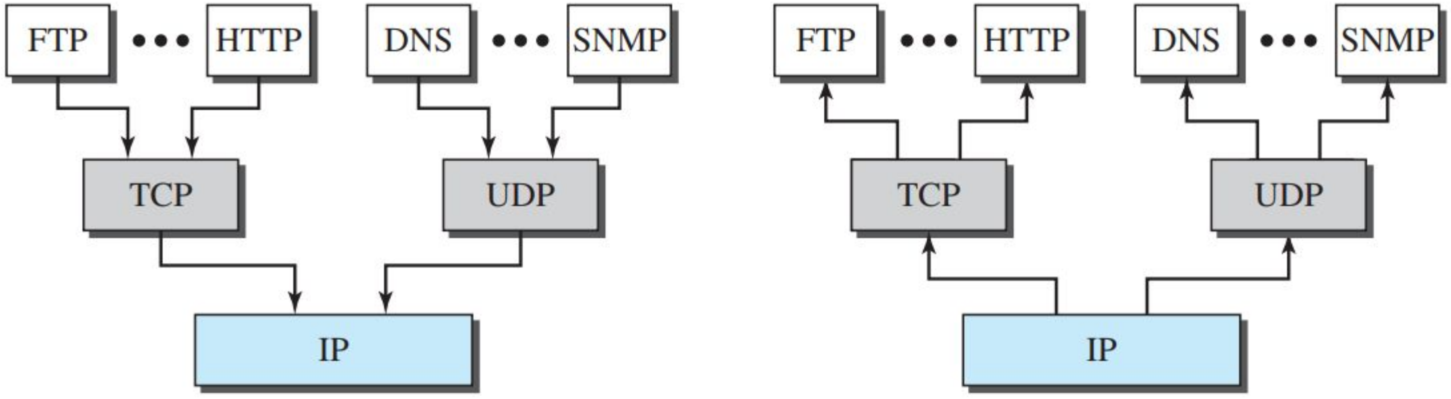
- Any communication that involves two parties needs two addresses: source address and destination address.
- Although it looks as if we need five pairs of addresses, one pair per layer, we normally have only four because the physical layer does not need addresses; as bits cannot have addresses



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

- As the figure shows, there is a relationship between the layer, the address used in that layer, and the packet name at that layer. At the application layer, we normally use names to define the site that provides services, such as someorg.com.
- At the transport layer, addresses are called port numbers, and these define the application-layer programs at the source and destination
- At the network-layer, the addresses are global, with the whole Internet as the scope. IP addresses.
- The link-layer addresses, sometimes called MAC addresses, are locally defined addresses, each of which defines a specific host or router in a network (LAN or WAN).

Multiplexing and Demultiplexing: with respect to layers



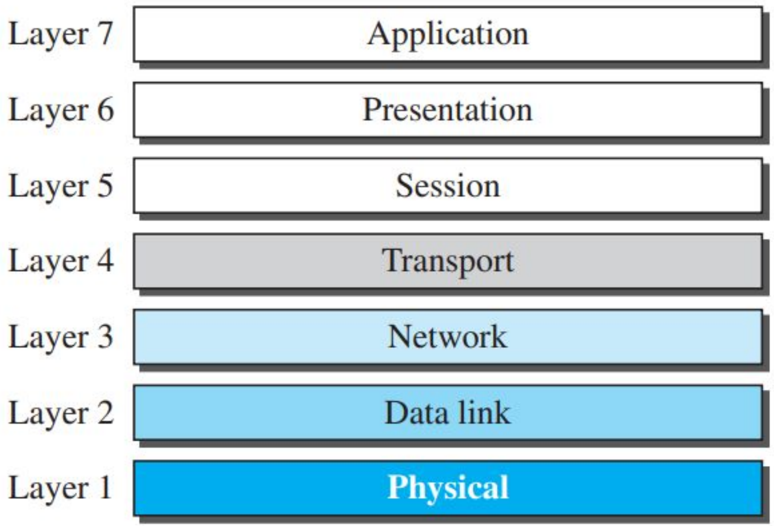
a. Multiplexing at source

b. Demultiplexing at destination

THE OSI MODEL

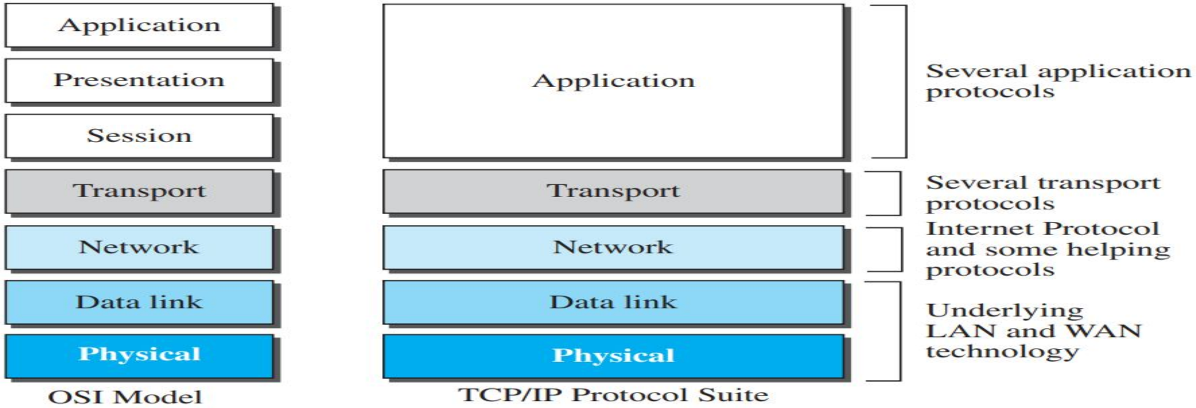
- An ISO standard that covers all aspects of network communications is the Open Systems Interconnection (OSI) model.
- It was first introduced in the late 1970s.
- An open system is a set of protocols that allows any two different systems to communicate regardless of their underlying architecture.
- The 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 understanding and designing a network architecture that is flexible, robust, and interoperable.
- The OSI model was intended to be the basis for the creation of the protocols in the OSI stack.

- OSI consists of seven separate but related layers, each of which defines a part of the process of moving information across a network.



Layer 7	Application
Layer 6	Presentation
Layer 5	Session
Layer 4	Transport
Layer 3	Network
Layer 2	Data link
Layer 1	**Physical**

- When we compare the two models, we find that 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.
- The application layer in the suite is usually considered to be the combination of three layers in the OSI model,



Application
Presentation
Session
Transport
Network
Data link
Physical
OSI Model

Application
Transport
Network
Data link
Physical
TCP/IP Protocol Suite

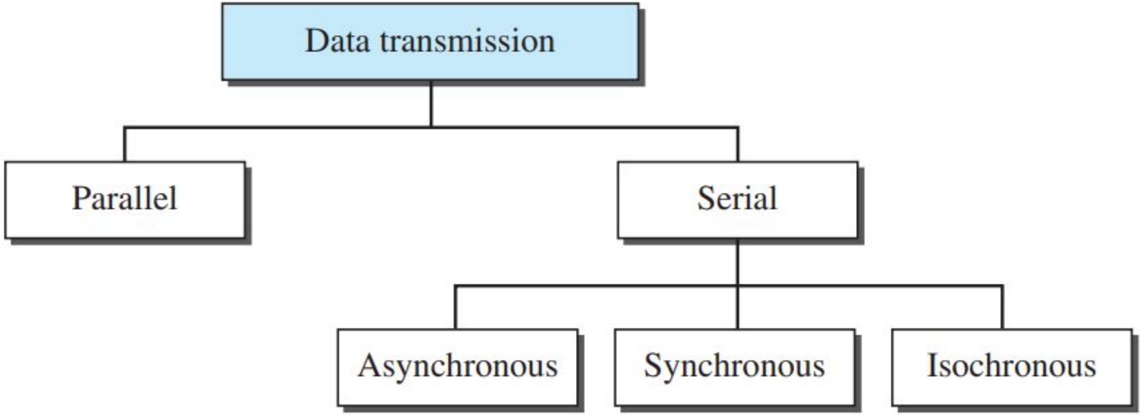
Several application protocols
Several transport protocols
Internet Protocol and some helping protocols
Underlying LAN and WAN technology

OSI versus TCP/IP

- Two reasons were mentioned for this decision. First, 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.

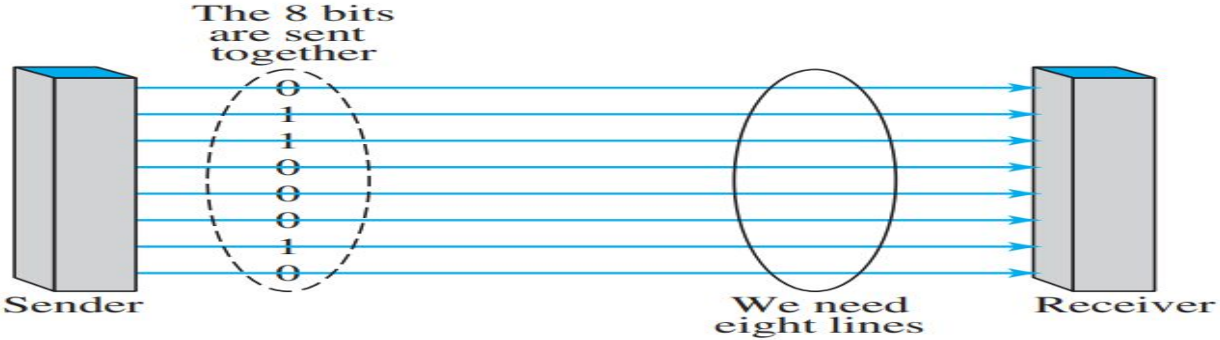
TRANSMISSION MODES

- The transmission of binary data across a link can be accomplished in either parallel or serial mode.
- In parallel mode, multiple bits are sent with each clock tick. In serial mode, 1 bit is sent with each clock tick.



Parallel Transmission

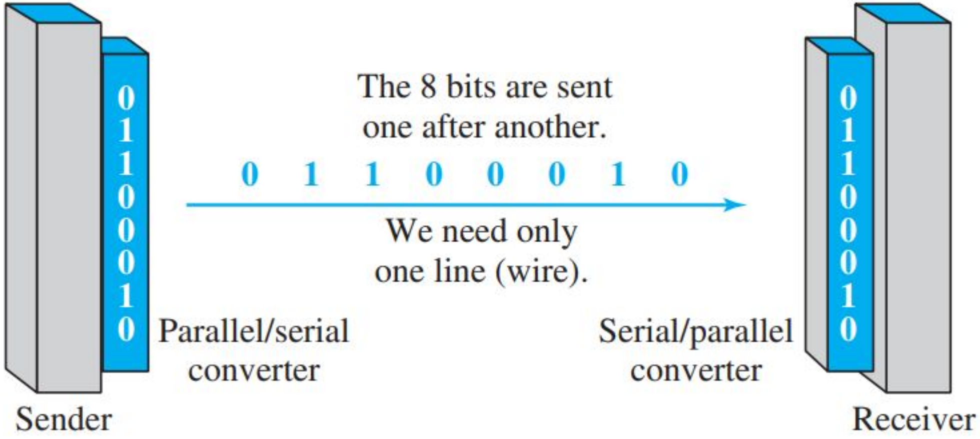
- By grouping, we can send data n bits at a time instead of 1.
- This is called parallel transmission.
- The mechanism for parallel transmission is a conceptually simple one: **Use n wires to send n bits at one time.**
- That way each bit has its own wire, and all n bits of one group can be transmitted with each clock tick from one device to another.



- The **advantage** of parallel transmission is **speed**.
- All else being equal, parallel transmission can increase the transfer speed by a factor of *n* over serial transmission.
- But there is a significant **disadvantage**: **cost**.
- Parallel transmission requires *n* communication lines (wires in the example) just to transmit the data stream.
- Because this is expensive, parallel transmission is usually limited to short distances

Serial Transmission

- In serial transmission one bit follows another, so we need only one communication channel rather than n to transmit data between two communicating devices


The 8 bits are sent one after another.
0 1 1 0 0 0 1 0
We need only one line (wire).
0 1 1 0 0 0 1 0
Parallel/serial converter
Sender
0 1 1 0 0 0 1 0
Serial/parallel converter
Receiver

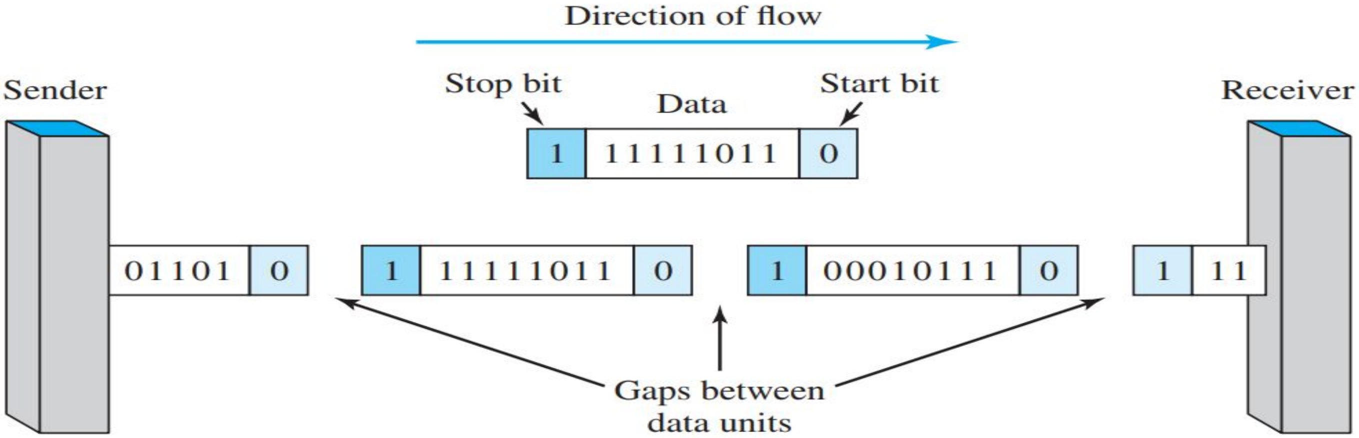
- The advantage of serial over parallel transmission is that with only one communication channel, serial transmission reduces the cost of transmission over parallel by roughly a factor of ***n***
- Since communication within devices is parallel, conversion devices are required at the interface between the sender and the line (parallel-to-serial) and between the line and the receiver (serial-to-parallel).

Serial transmission occurs in one of three ways: **asynchronous, synchronous, and isochronous.**

Asynchronous Transmission:

- It is so named because the **timing of a signal is unimportant**. Instead, information is received and translated by agreed upon **patterns**.
- **Patterns** are based on grouping the bit stream into bytes. Each group, usually **8 bits**, is sent along the link as a unit.
- To alert the receiver to the arrival of a new group, therefore, an extra bit is added to the beginning of each byte.
- This bit, **usually a 0, is called the start bit**.
- To let the receiver know that the byte is finished, **1 or more additional bits are appended** to the end of the byte.
- These bits, usually 1s, are called **stop bits**.
- By this method, each byte is increased in size to at least 10 bits, of which 8 bits is information and 2 bits or more are signals to the receiver.
- In addition, the transmission of each byte may then be **followed by a gap of varying duration**.

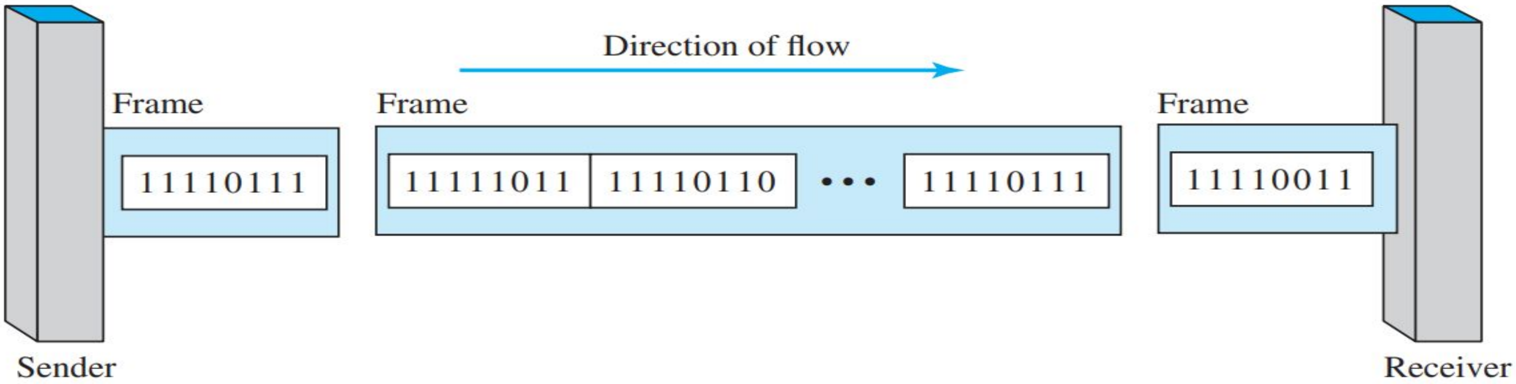
- Asynchronous here means “asynchronous at the byte level,” but the bits are still synchronized; their durations are the same.
- When the receiver detects a start bit, it sets a timer and begins counting bits as they come in. After n bits, the receiver looks for a stop bit.
- As soon as it detects the stop bit, it waits until it detects the next start bit



- The addition of stop and start bits and the insertion of gaps into the bit stream make asynchronous transmission slower than forms of transmission that can operate without the addition of control information.
- But it is cheap and effective, two advantages that make it an attractive choice for situations such as low-speed
- For example, the connection of a keyboard to a computer is a natural application for asynchronous transmission.

Synchronous Transmission

- In synchronous transmission, we send bits one after another without start or stop bits or gaps. It is the responsibility of the receiver to group the bits.
- If the sender wishes to send data in separate bursts, the gaps between bursts must be filled with a special sequence of 0s and 1s that means idle.
- The receiver counts the bits as they arrive and groups them in 8-bit units.



- Without gaps and start and stop bits, there is no built-in mechanism to help the receiving device adjust its bit synchronization midstream.
- Timing becomes very important, therefore, because the accuracy of the received information is completely dependent on the ability of the receiving device to keep an accurate count of the bits as they come in.
- The **advantage** of synchronous transmission is **speed.**
- For this reason, it is more useful for high-speed applications such as the transmission of data from one computer to another. Byte synchronization is accomplished in the data-link layer.
- Although there is no gap between characters in synchronous serial transmission, there may be uneven gaps between frames.

Isochronous

- In real-time audio and video, in which uneven delays between frames are not acceptable, synchronous transmission fails.
- For example, TV images are broadcast at the rate of 30 images per second; they must be viewed at the same rate.
- If each image is sent by using one or more frames, there should be no delays between frames.
- For this type of application, synchronization between characters is not enough; **the entire stream of bits must be synchronized**.
- The isochronous transmission guarantees that the data arrive at a fixed rate.

Link Layer

Data Link Control(DLC): DLC Services

Data Link Layer Protocols

High Level Data Link Control (HDLC)

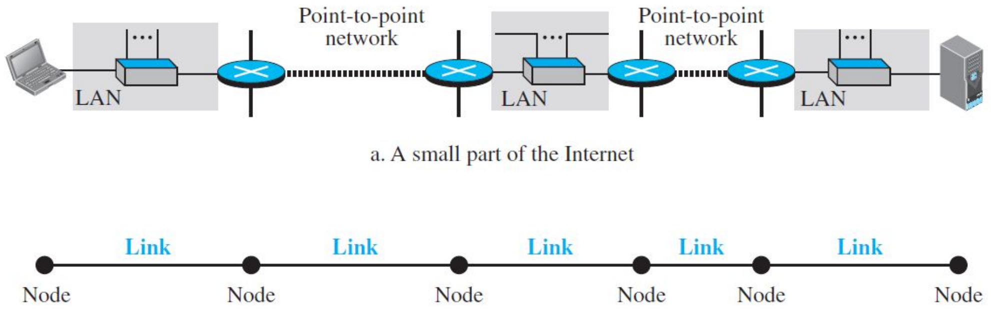
Point-to- Point Protocol (PPP): Framing, Transition phases.

Media Access Control (MAC):

Random Access: CSMA/CD,CSMA/CA

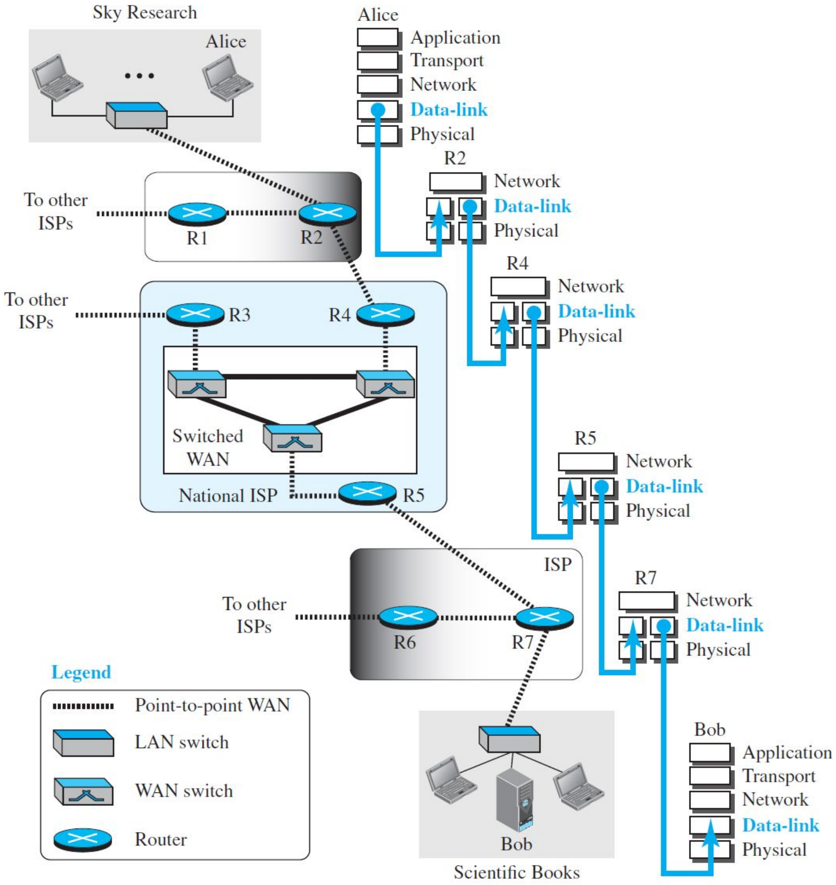
Introduction to Data Link Layer

- The Internet is a combination of networks glued together by connecting devices (routers or switches)
- Communication at the data-link layer is node-to-node.
- End hosts and routers are nodes and network in between are links



a. A small part of the Internet

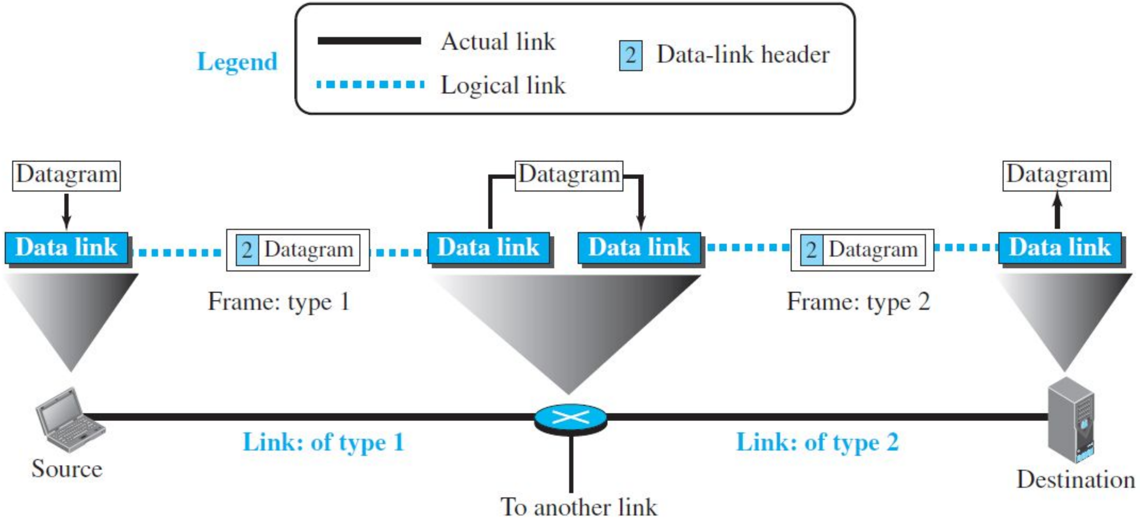
b. Nodes and links


Sky Research
Alice
To other ISPs
R1
R2
To other ISPs
R3
R4
Switched WAN
National ISP
R5
ISP
To other ISPs
R6
R7
Bob
Scientific Books
Legend
Point-to-point WAN
LAN switch
WAN switch
Router
Alice
Application
Transport
Network
Data-link
Physical
R2
Network
Data-link
Physical
R4
Network
Data-link
Physical
R5
Network
Data-link
Physical
R7
Network
Data-link
Physical
Bob
Application
Transport
Network
Data-link
Physical

Services

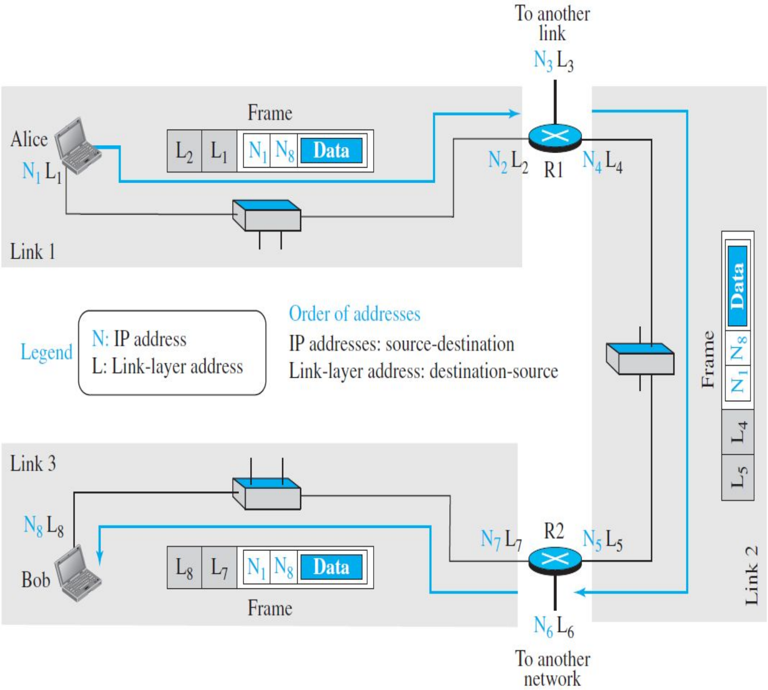
- The data link layer provides services to the network layer; it receives services from the physical layer.
- When a packet is travelling in the Internet, the data-link layer of a node (host or router) is responsible for delivering a datagram to the next node in the path.
- The data-link layer of the 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.
- Each intermediate node needs to do both encapsulate and decapsulate.
- Why encapsulation and decapsulation?
  - Different protocol with a different frame format in each link
  - Link layer addresses are different.

- The datagram received by the data-link layer of the source host is encapsulated in a frame.
- The frame is logically transported from the source host to the router.
- The frame is decapsulated at the data-link layer of the router and encapsulated at another frame.
- The new frame is logically transported from the router to the destination host.



Addressing

- To better understand the functionality of and the services provided by the link layer, the data-link layer is divided into two sublayers: **data link control (DLC) and media access control (MAC).**
- The data link control sublayer deals with all issues common to both point-to-point and broadcast links; the media access control sublayer deals only with issues specific to broadcast links.
- A link-layer address is sometimes called a link address, sometimes a physical address, and sometimes a MAC address.
- **Address Resolution Protocol (ARP)** is a network layer protocol that accepts an IP address from the IP protocol, maps the address to the corresponding link-layer address, and passes it to the data-link layer.



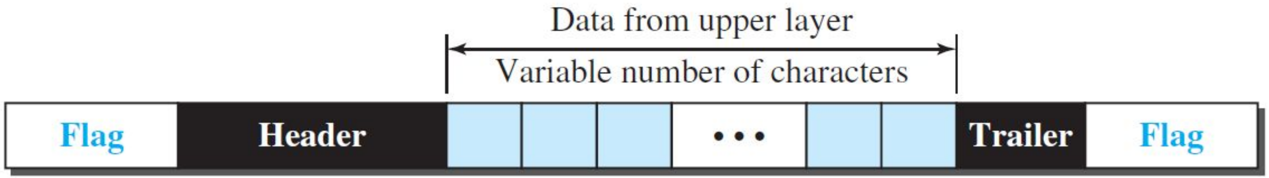
Services by Data Link Control (DLC)

- Framing:
  - A packet at the data-link layer is normally called a frame.
  - Different data-link layers have different formats for framing.
  - Framing in the data-link layer separates a message from one source to a destination by adding a sender address and a destination address
  - When a message is divided into smaller frames, a single-bit error affects only that small frame.

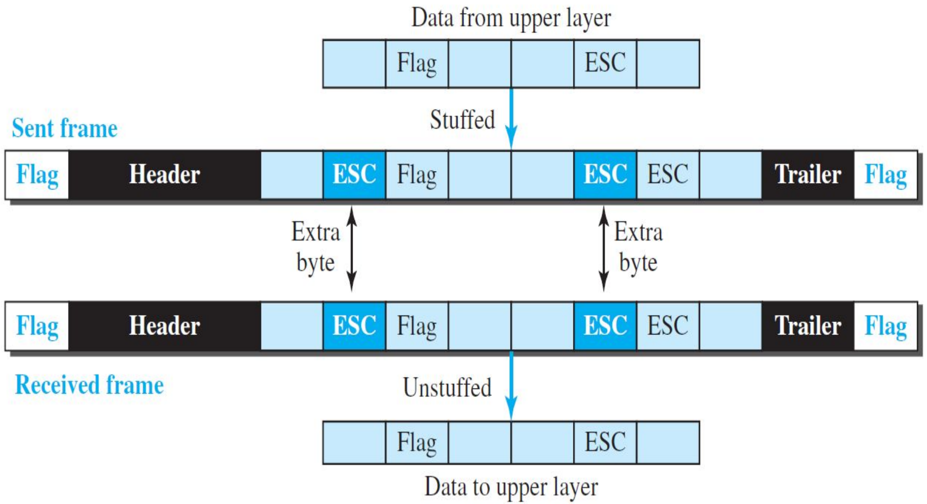
- Frames can be of fixed or variable size
  - In fixed-size framing, there is no need for defining the boundaries of the frames; the size itself can be used as a delimiter.
  - In variable-size framing, we need a way to define the end of one frame and the beginning of the next. Two approaches: a character-oriented approach and a bit-oriented approach

Framing

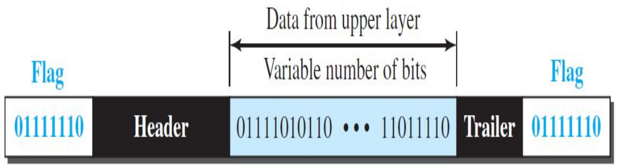
- In **character-oriented (or byte-oriented) framing**, data to be carried are 8-bit characters from a coding system such as ASCII.
- To separate one frame from the next, an 8-bit (1-byte) flag is added at the beginning and the end of a frame.
- The flag could be selected to be any character not used for text communication.
- Byte stuffing (or character stuffing) is a strategy wherein a special byte is added to the data section of the frame when there is a character with the same pattern as the flag.
- This byte is usually called the escape character (ESC) and has a predefined bit pattern.

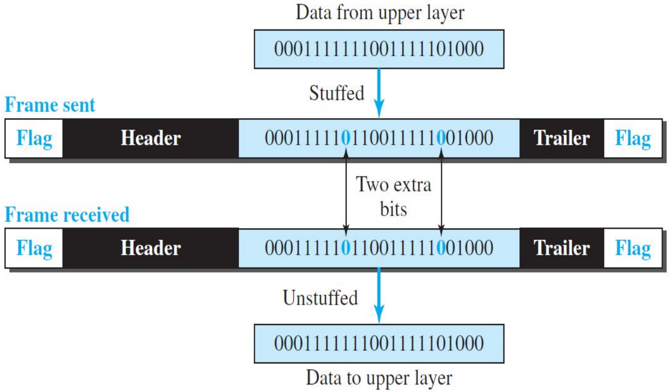


- If the escape character is part of the text, an extra one is added to show that the second one is part of the text.

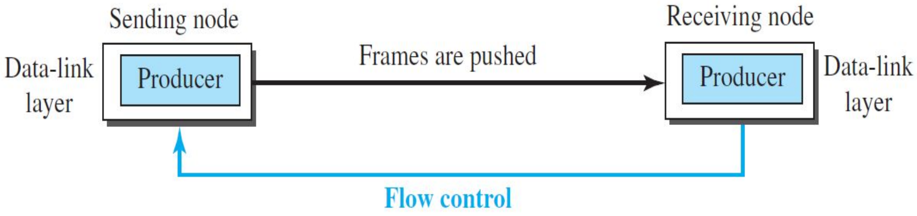


- In **bit-oriented framing**, the data section of a frame is a sequence of bits to be interpreted by the upper layer as text, graphic, audio, video, and so on.
- A special 8-bit pattern flag, 01111110, is used as the delimiter to define the beginning and the end of the frame.
- If the flag pattern appears in the data, we need to somehow inform the receiver that this is not the end of the frame: Bit Stuffing
- Bit stuffing is the process of adding one extra 0 whenever five consecutive 1s follow a 0 in the data, so that the receiver does not mistake the pattern 0111110 for a flag.
- This means that if the flag like pattern 01111110 appears in the data, it will change to 011111010 (stuffed) and is not mistaken for a flag by the receiver.





Flow Control:



- The data-link layer at the sending node tries to push frames toward the data-link layer at the receiving node. If the receiving node cannot process and deliver the packet to its network at the same rate that the frames arrive, it becomes overwhelmed with frames.
- Flow control in this case can be feedback from the receiving node to the sending node to stop or slow down pushing frames.
- Use of two buffers; one at the sending data-link layer and the other at the receiving data-link layer.
- When the buffer of the receiving data-link layer is full, it informs the sending data-link layer to stop pushing frames.
- What if the Buffer size is of only one slot that can hold only one frame?
    - When this single slot in the receiving data-link layer is empty, it sends a note to the network layer to send the next frame.

Error Control

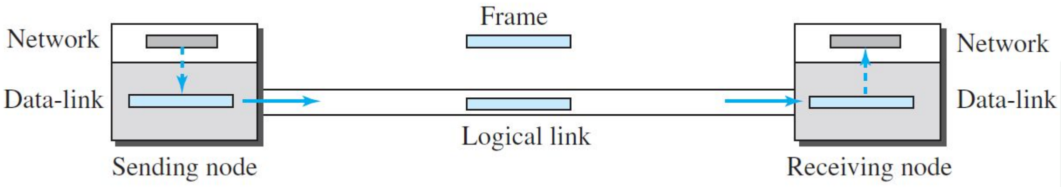
- Error control at the data-link layer is implemented to prevent the receiving node from delivering corrupted packets to its network layer.
- Two methods to implement error control.
  - If the frame is corrupted, it is silently discarded; if it is not corrupted, the packet is delivered to the network layer. - Ethernet
  - If the frame is corrupted, it is silently discarded; if it is not corrupted, an acknowledgment is sent to the sender.
- In both methods, a Cyclic Redundancy Checksum (CRC) is added to the frame header by the sender and checked by the receiver.
- Combination of Flow and error control:
  - The acknowledgment that is sent for flow control can also be used for error control to tell the sender the packet has arrived uncorrupted. The lack of acknowledgment means that there is a problem in the sent frame.

DLC Protocol - Connectionless and Connection Oriented

- Connectionless:
  - 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.
  - Eg: Data link protocols of LANs
- Connection Oriented:
  - 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).
  - The frames are numbered and sent in order.
  - Eg: Point to point protocols, some LANs and some WANs.

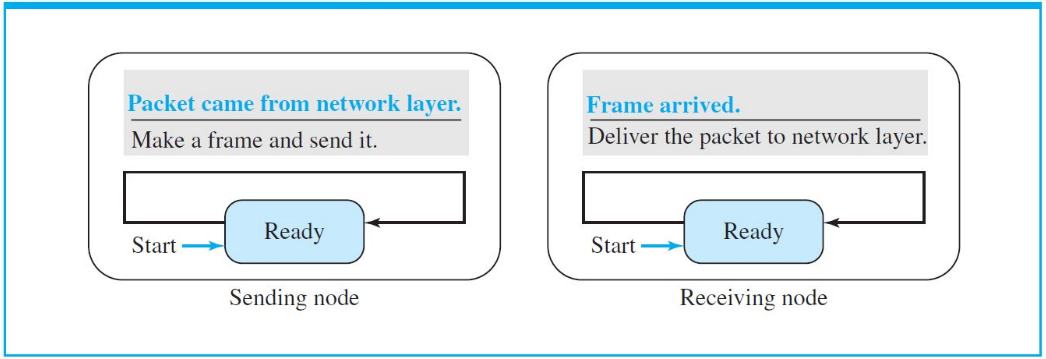
Data Link Layer Protocol

- Four Protocols are defined to deal with flow control and error control:
  - **Simple Protocol, Stop- and- wait**, Go- Back-N and Selective-repeat.
- **Simple Protocol:** With neither flow control nor error control.

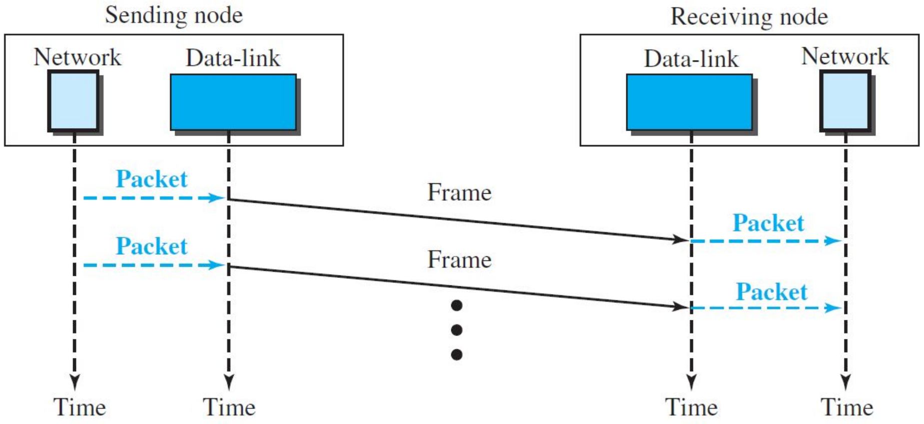


- Finite State machine (FSM):
  - The sender site should not send a frame until its network layer has a message to send.
  - The receiver site cannot deliver a message to its network layer until a frame arrives.

- FSM has only one state i.e. Ready

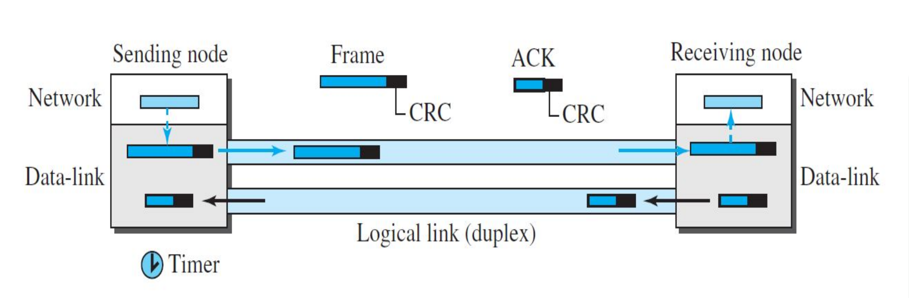

Packet came from network layer.
Make a frame and send it.
Start
Ready
Sending node
Frame arrived.
Deliver the packet to network layer.
Start
Ready
Receiving node

- The flow diagram is simple with sender sending frames one after the other without thinking of the receiver.



Stop-and-Wait Protocol

- It has both flow control and error control.
- The sender sends one frame at a time and waits for an acknowledgment before sending the next one. It starts the timer.
- Data frame has CRC to detect error. The receiver on receiving frame, checks CRC, if it is incorrect indicating the frame is corrupted then it will be discarded otherwise it will be sent to network layer after decapsulation and an acknowledgement will be sent to the sender node.
- The sender node on receiving acknowledgement from receiver before expiration of timer, discards the current frame and sends next frame.
- If the timer at the sender expires and there is no acknowledgement received from the receiver then, it resends the frame.

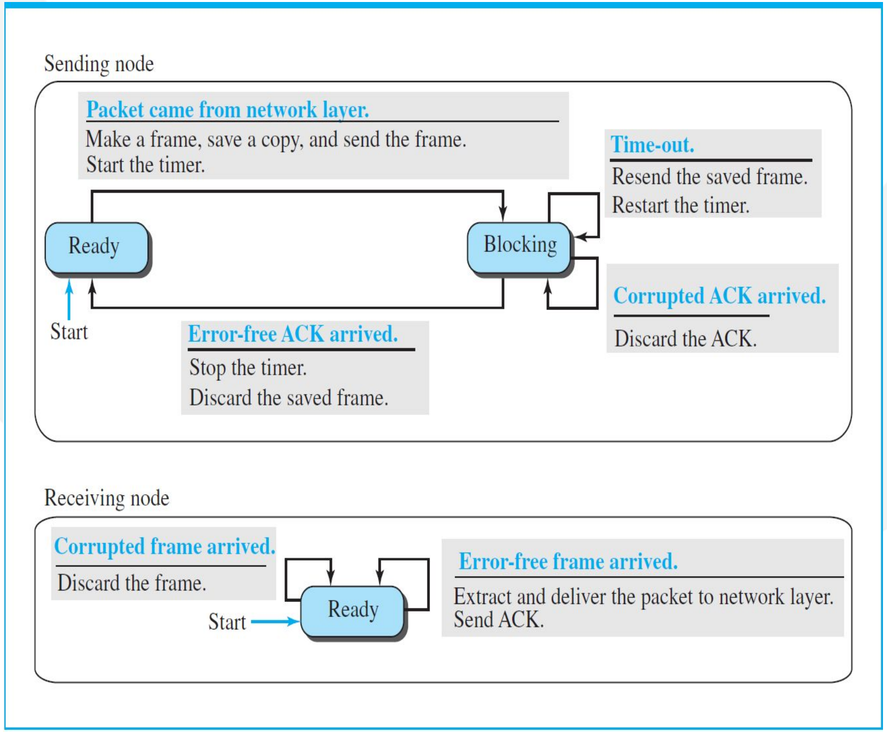


FSM of Stop-and-Wait protocol

Sender States: Ready and Blocking states.

- Ready State: Sender is waiting for a packet from network layer. On receiving packet, the sender encapsulates it into frame, makes a copy of it, sends the frame and starts the timer. Then moves to blocking state.

- Blocking state:
  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.



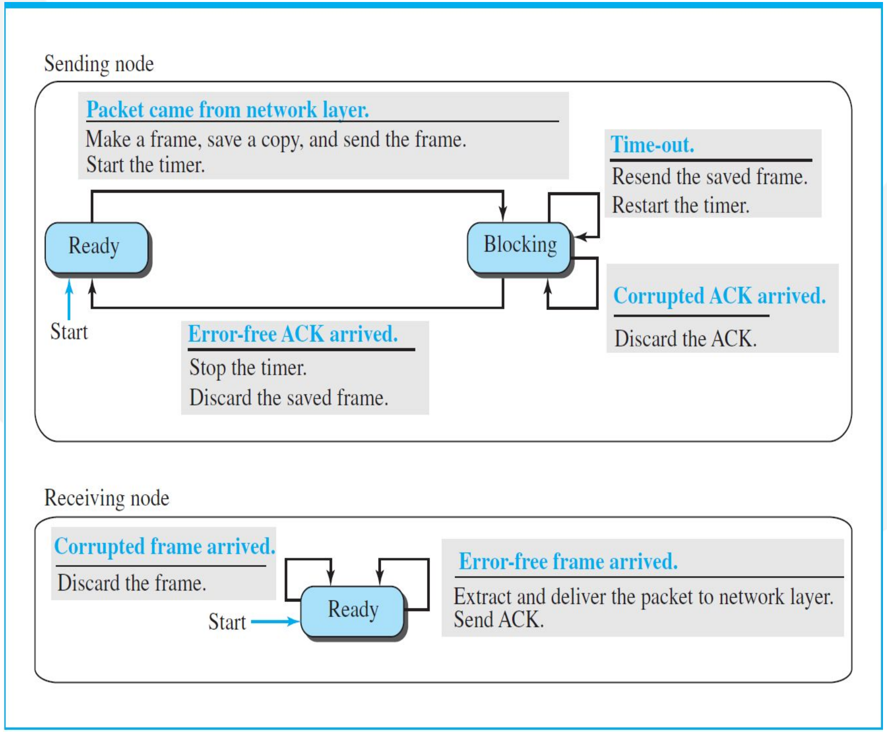
FSM of Stop-and-Wait protocol

Receiver State: Ready

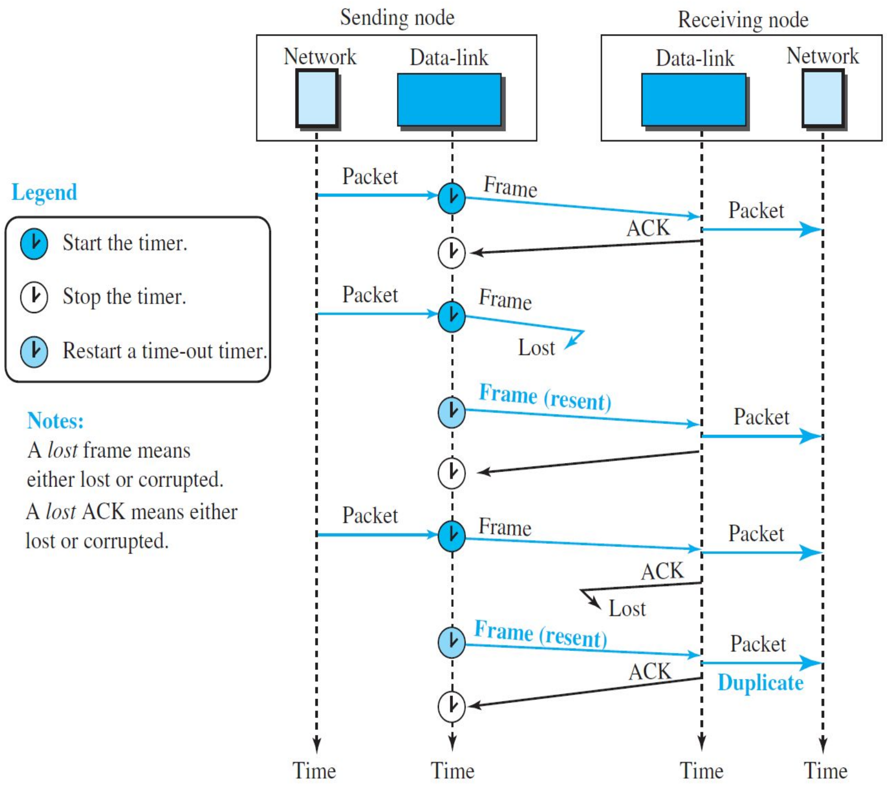
- Ready State:

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

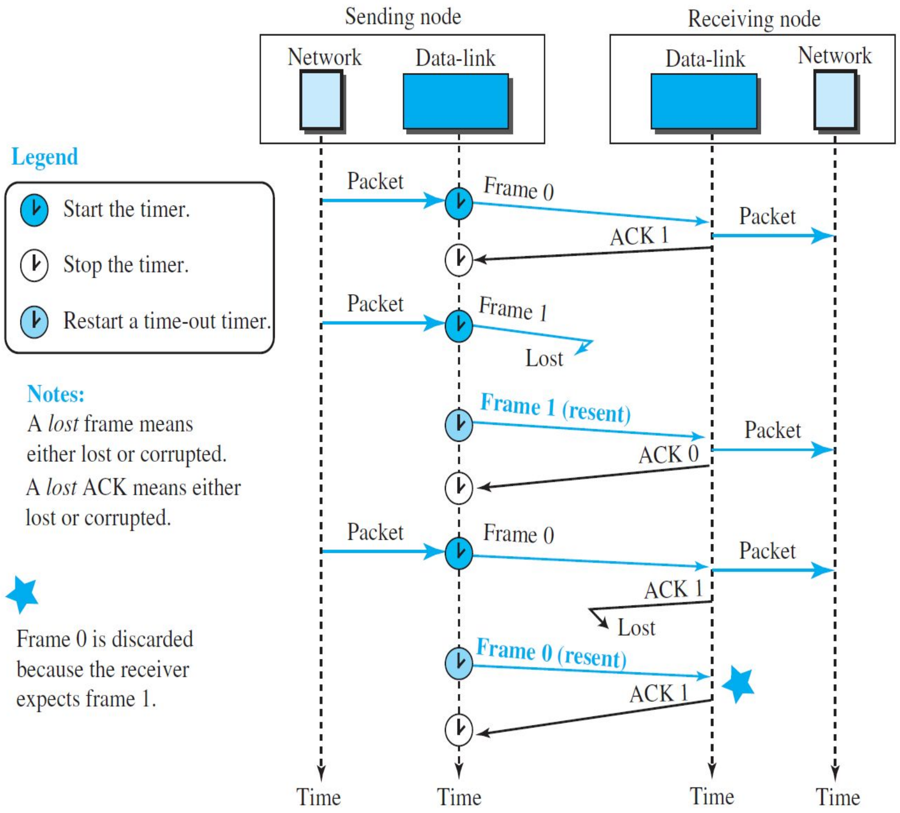
  b. If a corrupted frame arrives, the frame is discarded.



- The network layer at the receiver site receives two copies of the third packet, which is not right.
- Solution: addition of sequence numbers to the data frames and acknowledgment numbers to the ACK frames.
- In this case, Sequence numbers are 0, 1, 0, 1, 0, 1, . . . ; the acknowledgment numbers can also be 1, 0, 1, 0, 1, 0.
- An acknowledgment number always defines the sequence number of the next frame to receive.
- **Piggybacking:** When node A is sending data to node B, Node A also acknowledges the data received from node B. Complex in data link layer.



Notes:
A *lost* frame means either lost or corrupted.
A *lost* ACK means either lost or corrupted.



Legend

- Start the timer.
- Stop the timer.
- Restart a time-out timer.

Notes:

A *lost* frame means either lost or corrupted.

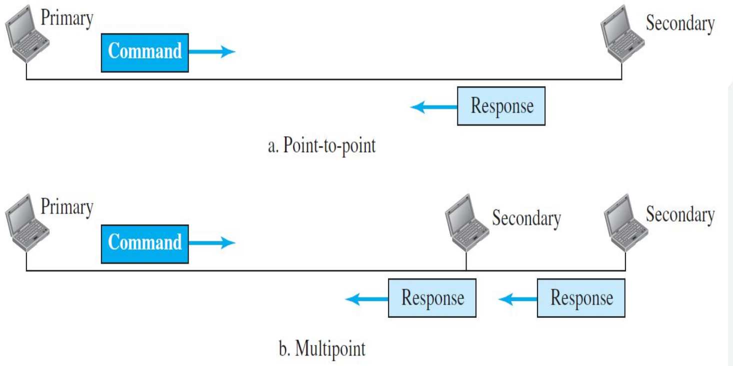
A *lost* ACK means either lost or corrupted.

★ Frame 0 is discarded because the receiver expects frame 1.

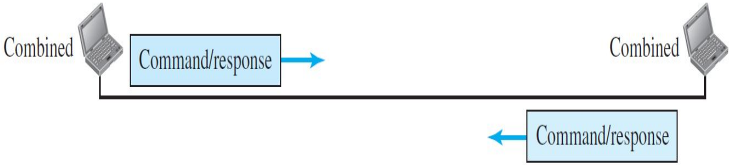
HDLC: High-Level Data Link Control

- High-level Data Link Control (HDLC) is a bit-oriented protocol for communication over point-to-point and multipoint links.
- It uses Stop-and-wait protocol.
- Configuration and Transfer modes: Two transfer modes that can be used in different configurations.
    - Normal Response Mode (NRM): The station configuration is unbalanced. We have 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
    - Asynchronous Balanced mode (ABM): The configuration is balanced. The link is point-to-point, and each station can function as a primary and a secondary (acting as peers).

NRM

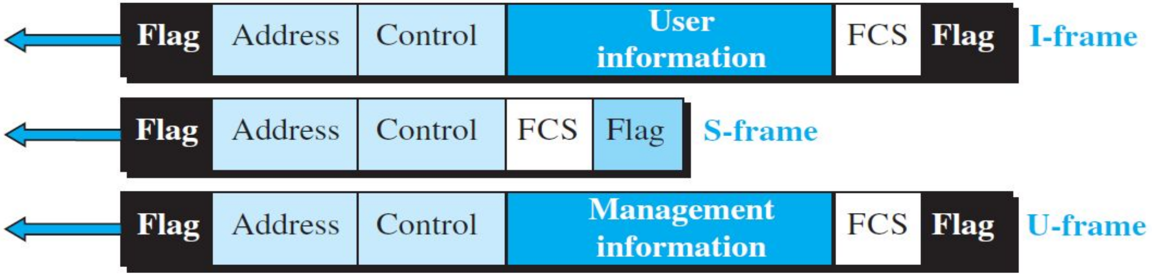


ABM

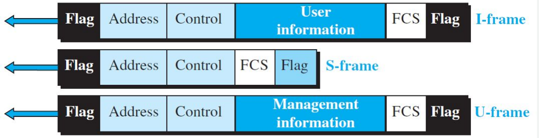


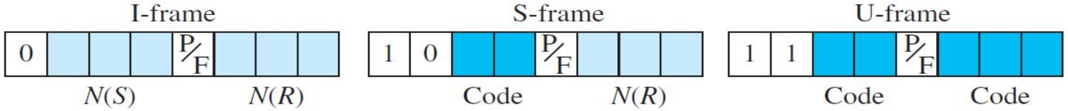
HDLC - Framing

- Three types of frames:
  - Information frames (I-frames): Data-link user data and control information relating to user data (piggybacking).
  - Supervisory frames (S-frames): Used only to transport control information.
  - Unnumbered frames (U-frames): system management, managing the link itself.



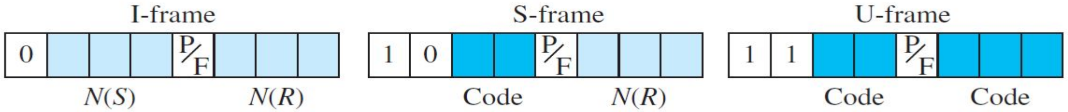
- **Flag field:** Has synchronization pattern 01111110, which identifies both the beginning and the end of a frame.
- **Address field:** This field contains the address of the secondary station. If a primary station created the frame, it contains a ‘to’ address. If a secondary station creates the frame, it contains a ‘from’ address.
- **Control field:** The control field is one or two bytes used for flow and error control. It determines the type of the frame.
- **Information field:** It 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.





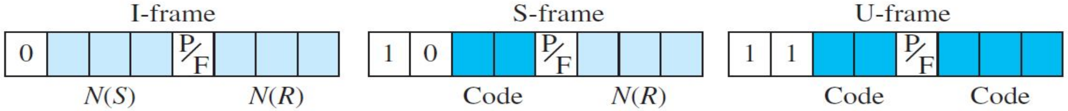
Control field for I-frames:

- I-frames are designed to carry user data from the network layer. In addition, they can include flow- and error-control information (piggybacking).
- 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 (0 to 7).
- The last 3 bits, called N(R), correspond to the acknowledgment number when piggybacking is used.
- The P/F field 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.
- 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.
    - **Receive Ready (RR):** code = 00. This kind of frame acknowledges the receipt of a safe and sound frame or group of frames. N(R) is acknowledgment number.
    - **Receive Not Ready (RNR):** code= 10. 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. N(R) is acknowledgment number.
    - **Reject (REJ):** code= 01. It is a NAK that can be used in Go-Back-N ARQ to improve the efficiency of the process by informing the sender, before the sender timer expires, that the last frame is lost or damaged. N(R) is negative acknowledgment number.
    - **Selective Reject (SREJ):** code=11. This is a NAK frame used in Selective Repeat ARQ. N(R) is negative acknowledgment number.

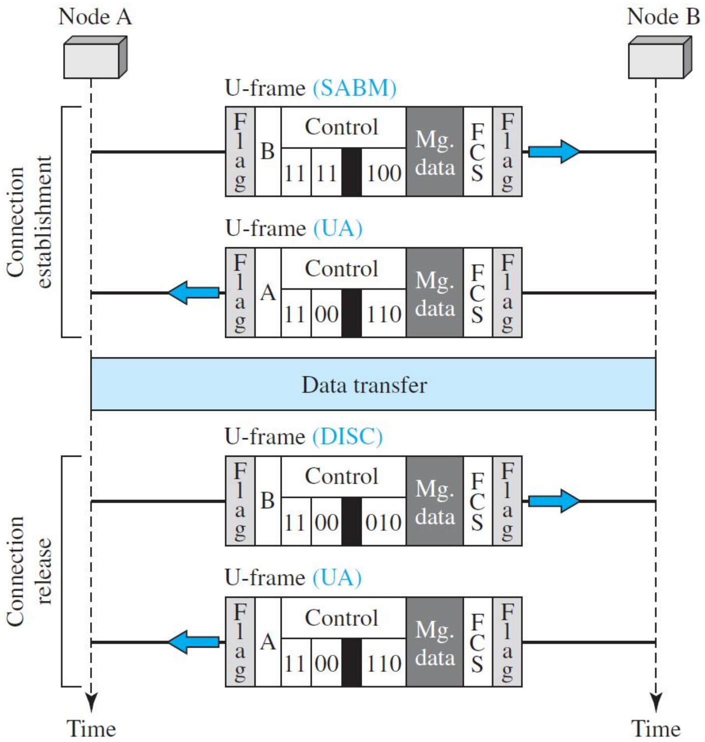


Control field for U-frames:

- Unnumbered frames are used to exchange session management and control information between connected devices.
- Information field in the frame is the system management information.
- 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.

Example of connection and disconnection

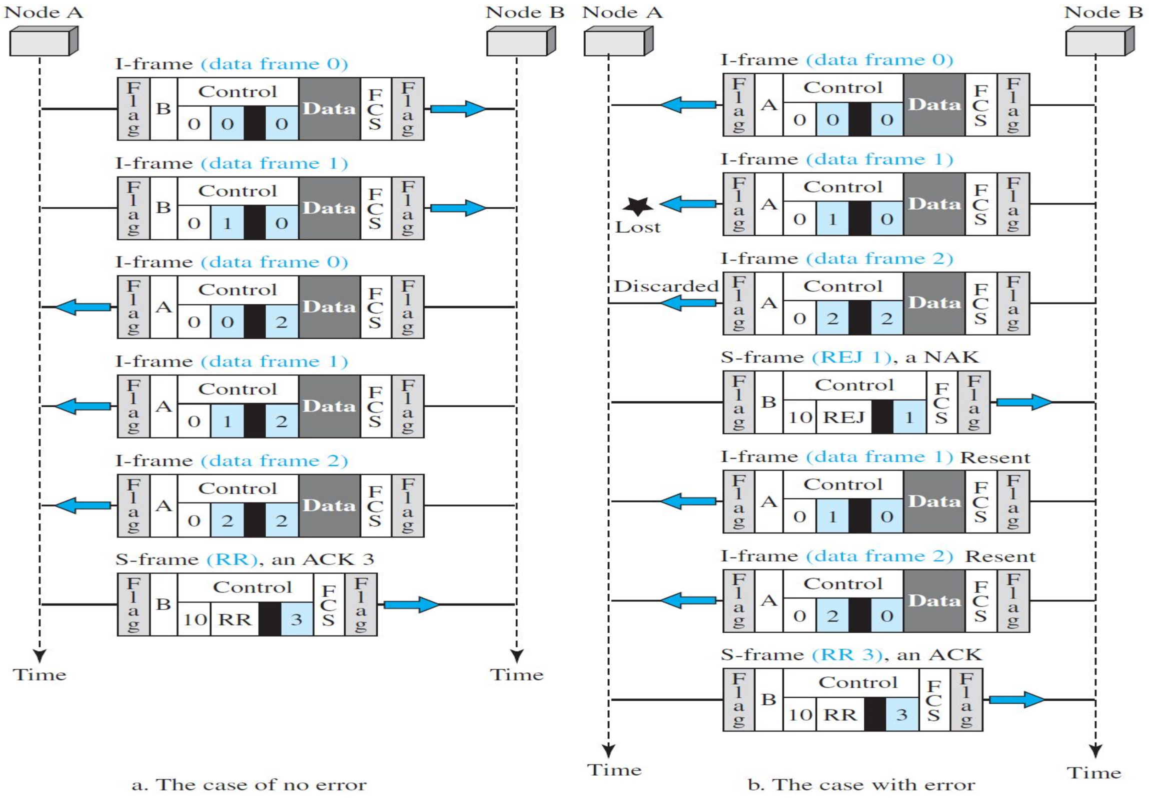
- Node A asks for a connection with a set asynchronous balanced mode (SABM) frame; node B gives a positive response with an unnumbered acknowledgment (UA) frame.
- After these two exchanges, data can be transferred between the two nodes (not shown in the figure).
- After data transfer, node A sends a DISC (disconnect) frame to release the connection; it is confirmed by node B responding with a UA (unnumbered acknowledgment).



The first is the case where no error has occurred;

the second is the case where an error has occurred and some frames are discarded.

Figure 11.19 *Example of piggybacking with and without error*



POINT-TO-POINT PROTOCOL

PPP provides several services:

1. PPP defines the format of the frame to be exchanged between devices.

2. PPP defines how two devices can negotiate the establishment of the link

3. PPP defines how network layer data are encapsulated in the data link frame.

4. PPP defines how two devices can authenticate each other.

5. PPP provides multiple network layer services

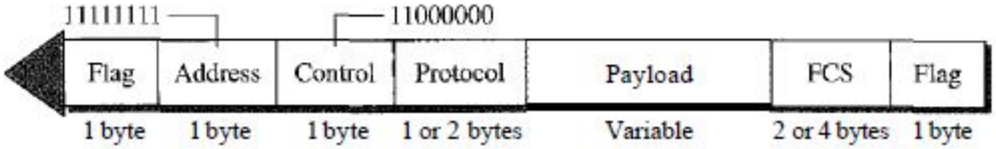
6. PPP provides connections over multiple links.

7. PPP provides network address configuration. This is particularly useful when a home user needs a temporary network address to connect to the Internet.

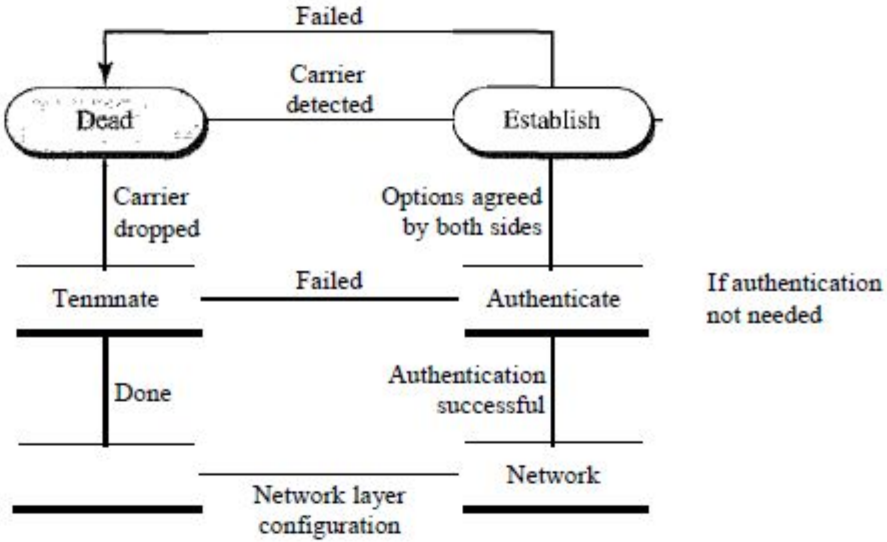
Missing services

1. PPP has a very simple mechanism for error control.
2. PPP does not provide flow control.
3. PPP does not provide a sophisticated addressing mechanism to handle frames in a multipoint configuration.

Framing



Transition phases



Random Access

Carrier Sense Multiple Access (CSMA)

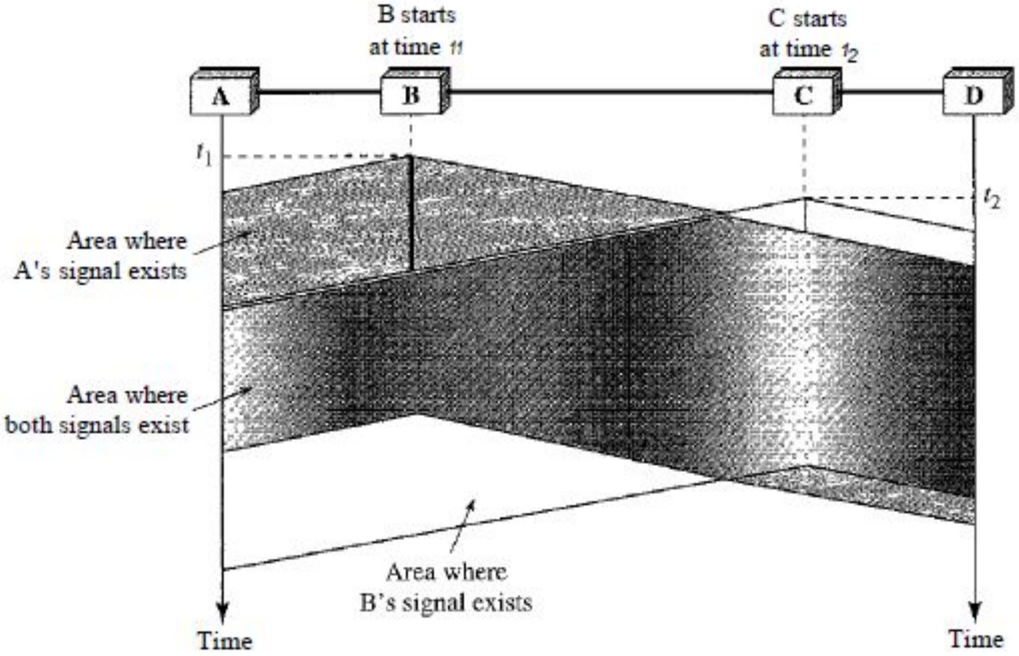
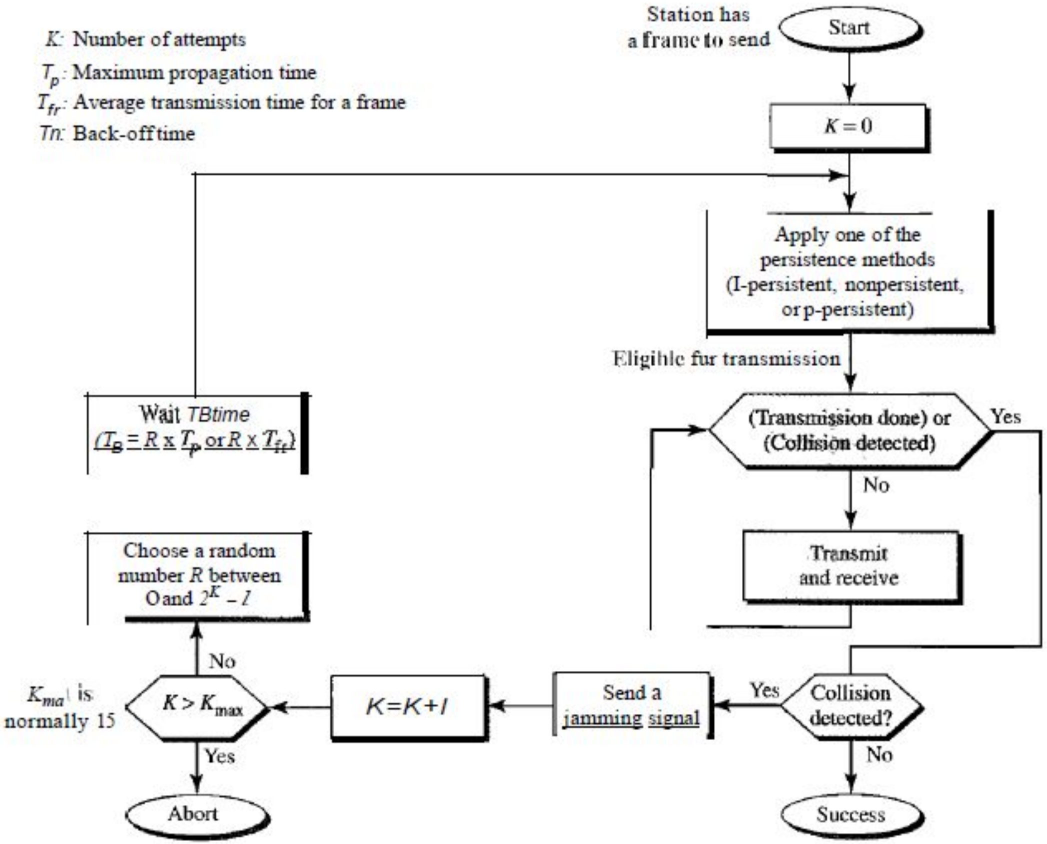

B starts at time t1
C starts at time t2
A
B
C
D
t_1
t_2
Area where A's signal exists
Area where both signals exist
Area where B's signal exists
Time
Time

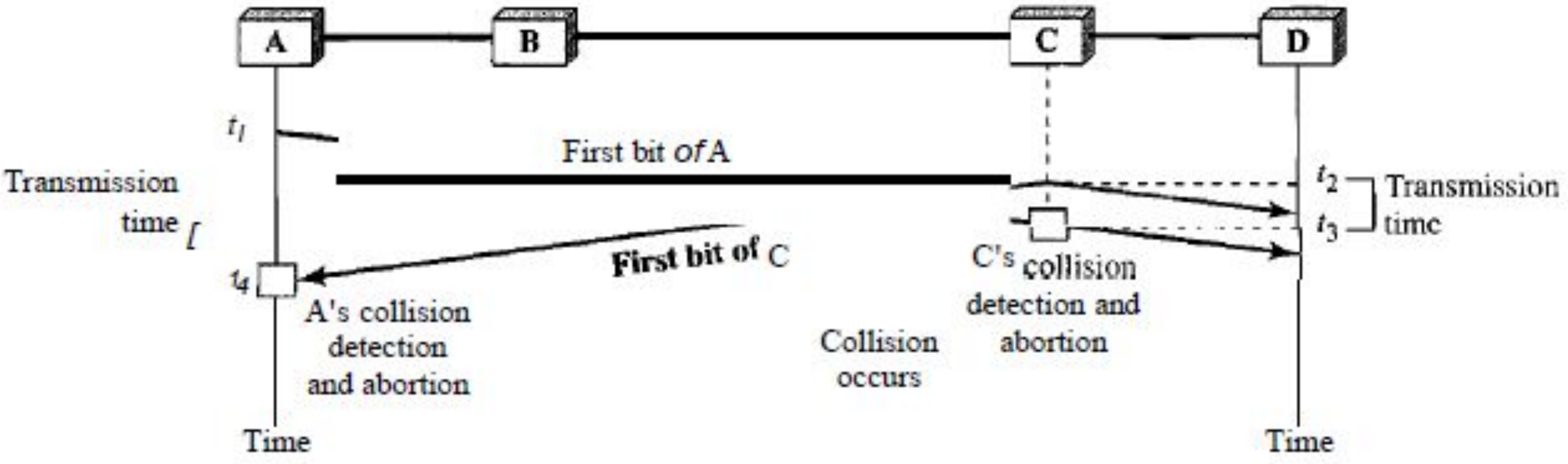
Fig. Space/time model of the collision in CSMA

Flow diagram for the CSMAICD

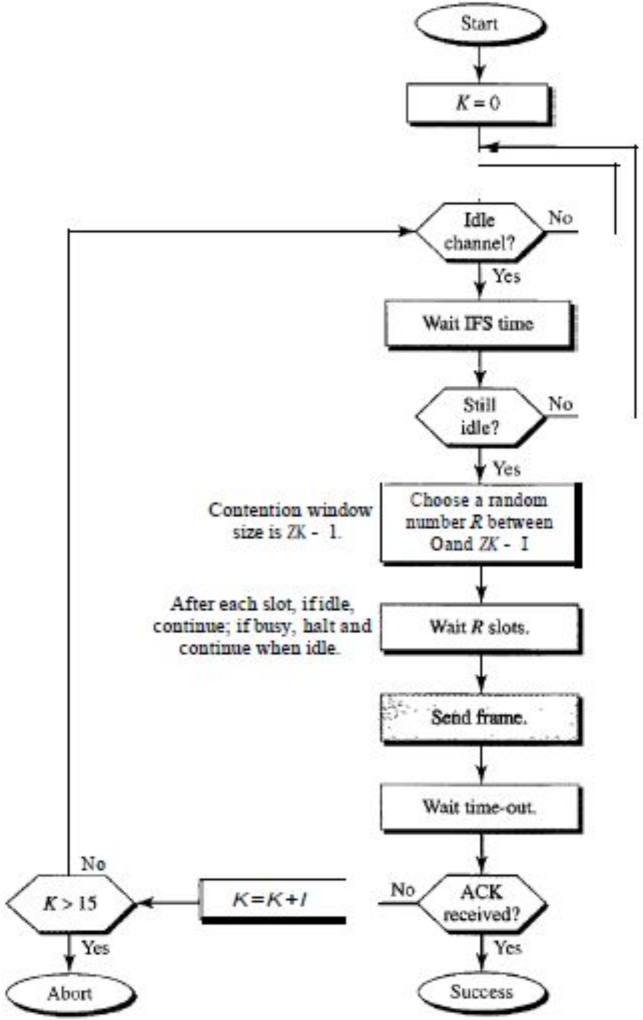

K: Number of attempts
T_p: Maximum propagation time
T_{fr}: Average transmission time for a frame
Tn: Back-off time
Station has a frame to send
Start
K = 0
Apply one of the persistence methods (I-persistent, nonpersistent, or p-persistent)
Eligible fur transmission
(Transmission done) or (Collision detected)
Yes
No
Transmit and receive
Collision detected?
Yes
No
Success
Send a jamming signal
K=K+I
K > Kmax
Kmax is normally 15
No
Yes
Abort
Choose a random number R between 0 and 2^K – 1
Wait TBtime
(TB = R x Tp or R x Tfr)

CSMA

Collision in CSMA



CSMA/CA


Start
K = 0
Idle channel?
No
Yes
Wait IFS time
Still idle?
No
Yes
Contention window size is ZK - 1.
Choose a random number R between Oand ZK - 1
After each slot, if idle, continue; if busy, halt and continue when idle.
Wait R slots.
Send frame.
Wait time-out.
No
K > 15
K=K+I
No
ACK received?
Yes
Yes
Abort
Success

Thank you