FRANCIS XAVIER ENGINEERING COLLEGE
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

19CS5602 COMPUTER NETWORKS

UNIT II DATA LINK LAYER

Link Layer Addressing - ARP - Error Detection and Correction - Data Link Control Services - Data Link Layer Protocols - HDLC - PPP - Media Access Control - Ethernet - Wireless LANs: IEEE 802.11, Bluetooth - Connecting Devices.

2.1 Introduction

What isDLL (Data LinkLayer)?

The Data Link Layer is the second layer in the OSI model, above the Physical Layer, whichensures that the error free data is transferred between the adjacent nodes in the network. It breaksthe datagram passed down by above layers and converts them into frames ready for transfer. Thisiscalled**Framing.**

Itprovidestwomainfunctionalities

 Reliabledatatransferservicebetweentwopeer networklayers

 Flow Control mechanism which regulates the flow of frames such that data congestion is notthereat slow receivers dueto fast senders.

2.2 LINK-LAYERADDRESSING

In a connectionless internetwork such as the Internet we cannot make a datagram reach itsdestination using only IP addresses. The reason is that each datagram in the Internet, from the same source host to the same destination host, may take a different path. The source and destination IP addresses define the two ends but cannot define which links the datagram shouldpassthrough.

ThreeTypesofaddresses

Somelink-layer protocols define three types of addresses: unicast, multicast, and brodcast.

UnicastAddress

Each host or each interface of a router is assigned a unicast address. Unicasting meansone-to-one communication. A frame with a unicast address destination is destined onlyforoneentityin thelink.

A3:34:45:11:92:F1

MulticastAddress

Some link-layer protocols define multicast addresses. Multicasting means one-to-many communication. However, the jurisdiction is local(insidethe link).

A2:34:45:11:92:F1

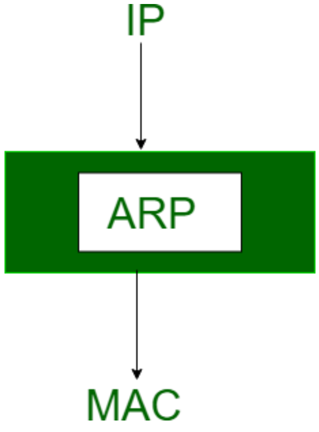
Broadcast Address

Some link-layer protocols define a broadcast address. Broadcasting means one-to-allcommunication. A frame with a destination broadcast address is sent to all entities inthelink. FF:FF:FF:FF:FF:FF

AddressResolutionProtocols(ARP):

Most of the computer programs/applications use logical address (IP address) to send/receivemessages,howevertheactualcommunicationhappensoverthephysicaladdress (MACaddress)

i.e from layer 2 of OSI model. So our mission is to get the destination MAC address which helpsin communicating with other devices. This is where ARP comes into the



picture, its functionalityisto translateIPaddresstophysical address.

Most of the computer programs/applications use **logical address (IP address)** to send/receive messages, however the actual communication happens over the **physical address (MACaddress)** i.e from layer 2 of OSI model. So our mission is to get the destination MAC addresswhich helps in communicating with other devices. This is where ARP comes into the picture, its functionality is to translate IP address to physical address.

The acronym ARP stands for Address Resolution Protocol which is one of the most important protocols of the Networklayer in the OSImodel.

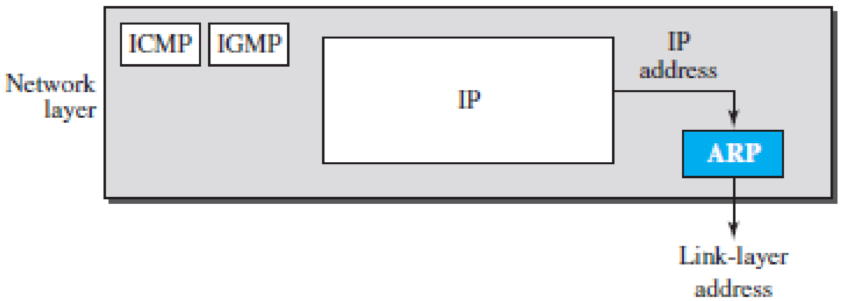
Note:ARP finds the hard wareaddress, also known as Media Access Control (MAC) address, of a host from its knownIPaddress.

Let'slook at how ARP works.

Imagine a device wants to communicate with the other over the internet. What ARP does? Is itbroadcastapacket to all the devices ofthesourcenetwork?

The devices of the network peel the header of the data link layer from the protocol data unit(PDU) called frame and transfers the packet to the network layer (layer 3 of OSI) where the network ID of the packet is validated with the destination IP's network ID of the packet and if it's equal then it responds to the source with the MAC address of the destination, else the packetreaches the gateway of the network and broadcasts packet to the devices it is connected with andvalidatestheir networkID.

Position of ARP in TCP/IP protocol suite

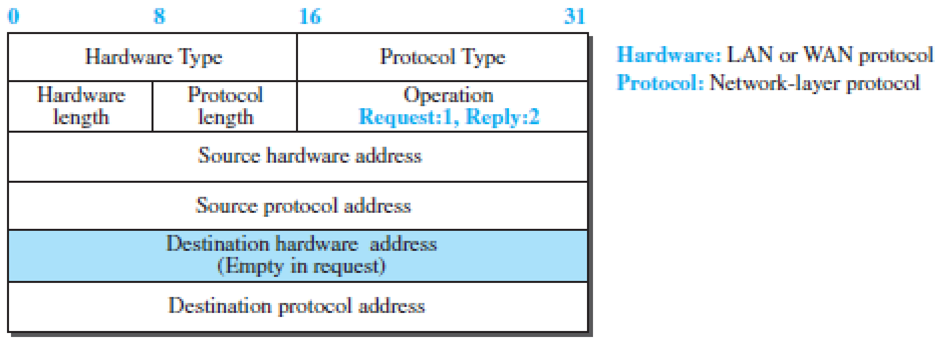


Anytime a host or a router needs to find the link-layer address of another host or router in itsnetwork, it sends an ARP request packet. The packet includes the link-layer and IP addresses of the sender and the IP address of the receiver. Because the sender does not know the link-layeraddress of the receiver,the query is broadcast over the link using thelink-layer broadcast address, which we discuss for each protocol later.

Caching

A question that is often asked is this: If system A can broadcast a frame to find the linklayeraddressofsystemB,why can’t system A send the datagram for system Busing abroad castframe? In otherwords, instead of sending one broadcast frame (ARPrequest), one unicast frame (ARP response), and another unicastframe (for sending the datagram), system A can encapsulate the datagram and send it to the network. System B receives it and keep it; other systems discard it.

ARP packet



Hardware Type		Protocol Type
Hardware length	Protocol length	Operation Request:1, Reply:2
Source hardware address		
Source protocol address		
Destination hardware address (Empty in request)		
Destination protocol address		

Hardware: LAN or WAN protocol
Protocol: Network-layer protocol

2.3 DLCServices.

The data link control (DLC) deals with procedures for communication between two adjacentnodes—node-to-node communication—no matter whether the link is

dedicatedor broadcast.Data link control functions include framing and flow and error control. In this section, we firstdiscuss framing, or how to organize the bits that are carried by the physical layer. We then discuss flow and error control.

Datalinkcontrolfunctionsincludes

(1) Framing.

(2) ErrorControl.

(3) FlowControl.

Framing

Data transmission in the physical layer means moving bits in the form of a signal from the source tothe destination. The physical layer provides bit synchronization to ensure that the sender and receiveruse the same bit durations and timing. The data-link layer, on the other hand, needs to pack bits intoframes, so that each frame is distinguishable from another. Our postal system practices a type of framing. The simple act of inserting aletter into an envelope separates one piece of information from another; the envelope serves as the delimiter. In addition, each envelope defines the sender and receiver addresses, which is necessary since the postal system is a many-to-many carrier facility.

Framing in the data-link layer separates a message from one source to a destination by adding asender address and a destination address. The destination address defines where the packet is to go; the sender address helps the recipient acknowledge the receipt.

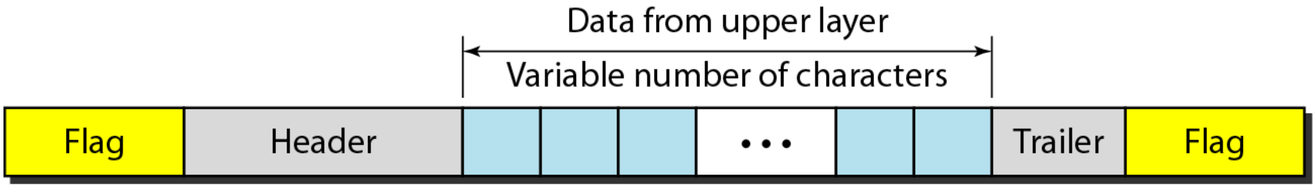
Although the whole message could be packed in one frame, that is not normally done. One reason is that a frame can be very large, making flow and error control very inefficient. When a message iscarried in one very large frame, even a single-bit error would require the retransmission of the wholeframe. When a message is divided intosmaller frames, a single-bit error affects only that smallframe.

FrameSize:

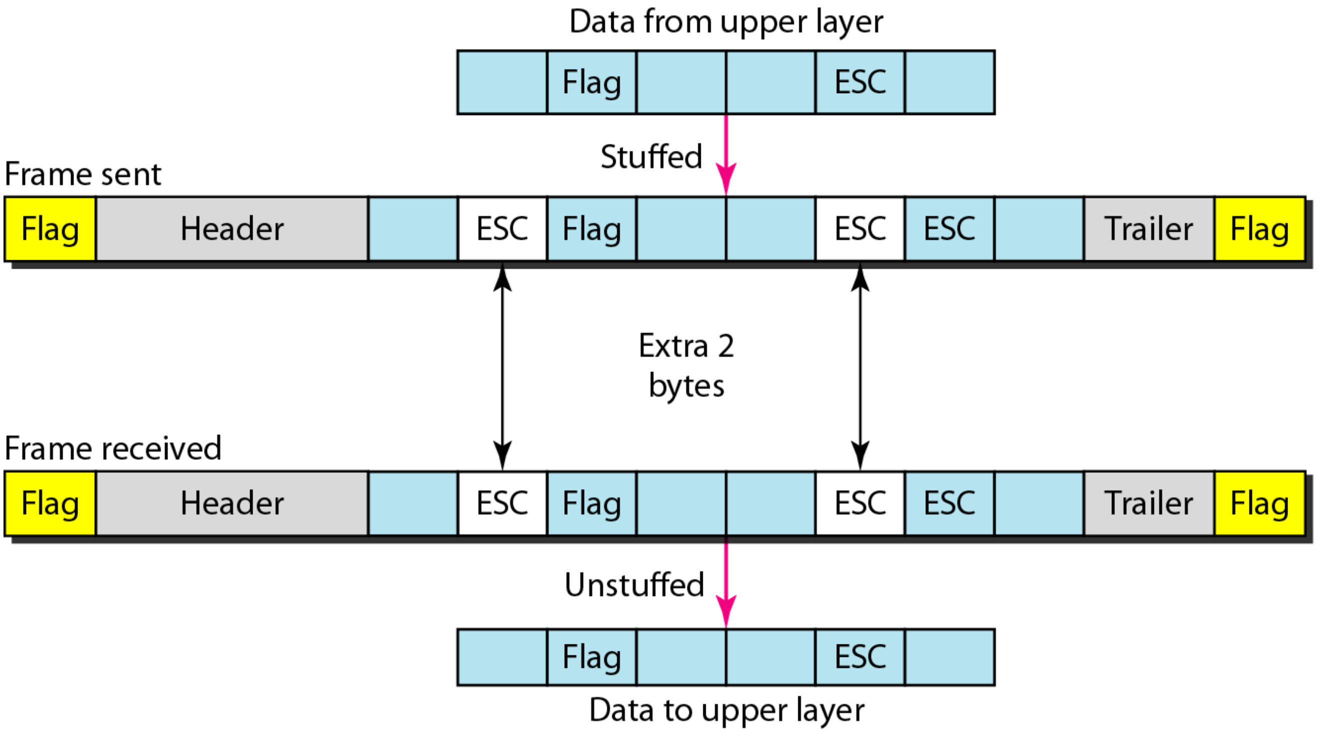
Frames can be of fixed or variable size. In fixed-size framing, there is no need for defining theboundaries of the frames; the size itself can be used as a delimiter. An exampleof this type offraming is the ATM WAN, which uses frames of fixed size called cells. Our main discussion in thischapter concerns variable-size framing, prevalent in local-area networks. In variable-size framing, we need a way to define the end of one frame and the beginning of the next. Historically, two approaches were used for this purpose: a character – oriented approach and a bit-oriented approach.

Character-OrientedFraming:

In character-oriented (or byte-oriented) framing, data to be carried are 8-bit characters from a codingsystem such as ASCII. The header, which normally carries the source and destination addresses andother control information, and thetrailer, which carries error detection redundant bits, are alsomultiples of 8 bits. To separate one frame from the next, an 8-bit (1-byte) flag is added at thebeginning and the end of a frame. The flag, composed of protocol-dependent special characters,signalsthestart or end ofa frame.



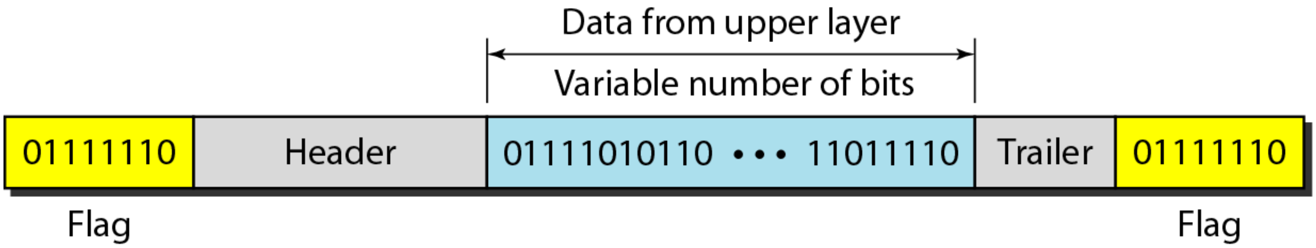
Byte stuffing and unstuffing



Byte stuffing is the process of adding 1 extra byte whenever there is a flag or escape character in the text.

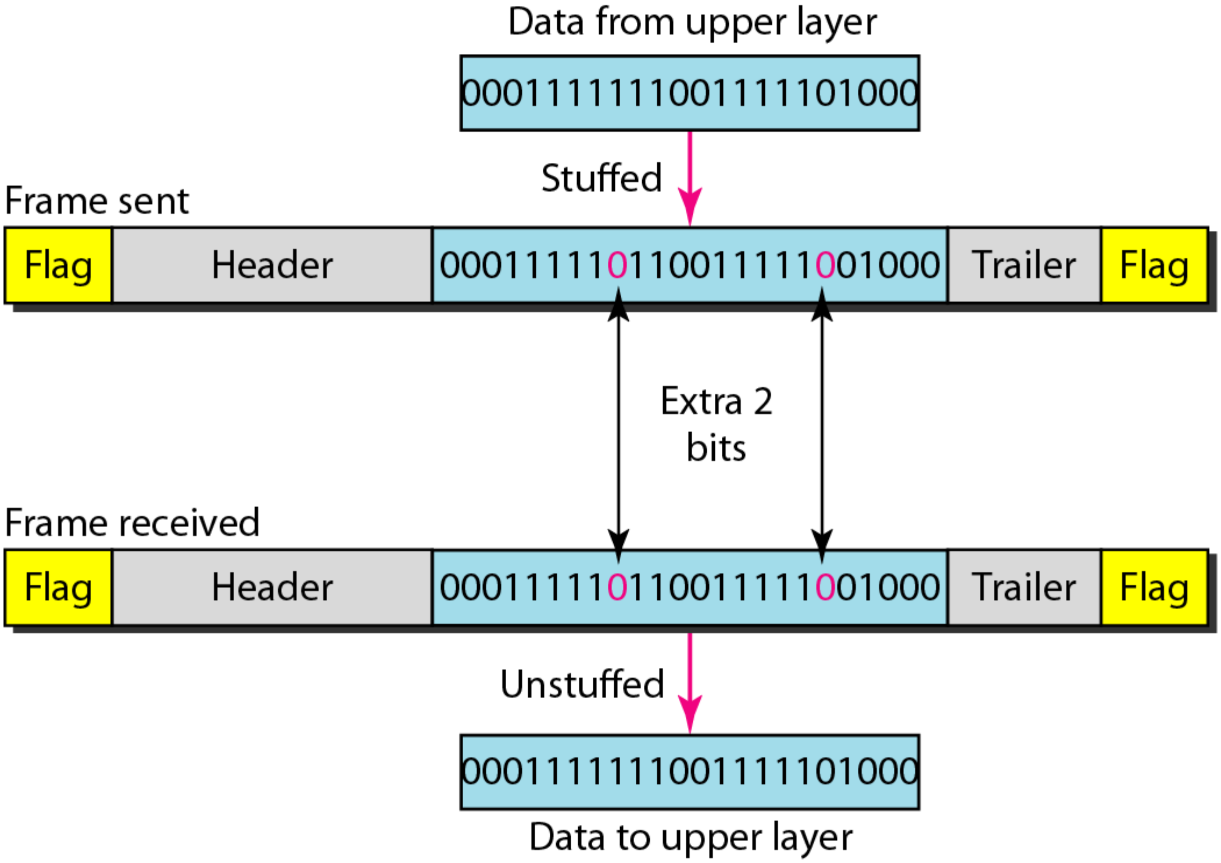
Bit-OrientedFraming:

Inbit-oriented framing,thedatasection ofaframeis a sequenceof bitstobeinterpreted by the upper layer as text, graphic, audio, video, and so on. However, in addition to headers (andpossible trailers), we still need a delimiter to separate one frame from the other. Most protocolsuse a special 8-bit pattern flag, 01111110, as the delimiter to define the beginning and the end oftheframe.



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 mistakethe pattern 0111110 for a flag.



FLOW AND ERROR CONTROL

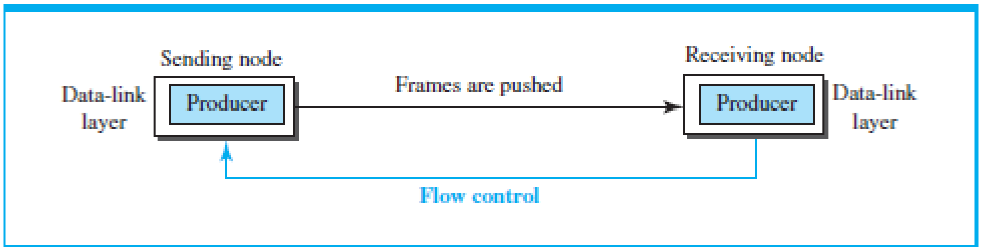
The most important responsibilities of the data link layer are flow control and error control. Collectively, these functions are known as data link control

FlowControl

Flow control refers to a set of procedures used to restrict the amount of data that the sender can send beforewaiting for acknowledgment.

Whenever an entity produces items and another entity consumes them, there should be a balance between production and consumption rates. If the items are produced faster than they can beconsumed, the consumer can be overwhelmed and may need to discard some items. If the items are produced more slowly than they can be consumed, the consumer must wait, and the systembecomes less efficient. Flow control is related to the first issue. We need to prevent losing the data items at the consumer site. In communication at the data-link layer, we are dealing with fourentities: network and data-link layers at the sending node and network and data-link layers at the receiving node. Although we can have a complex relationship with more than one producer
and consumer, weignore the relationships between networks and data-link layers and concentrate on the relationship between two data-link layers.

Flow control at the data-link layer



Buffers

Although flow control can be implemented in several ways, one of the solutions is normally to use two buffers; one at the sending data-link layer and the other at the receiving data-link layer. A buffer is a set of memory locations that can hold packets at the sender and receiver. The flowcontrol communication can occur by sending signals from the consumer to the producer. When the buffer of the receiving data-link layer is full, it informs the sending data-link layer to stoppushingframes.

ErrorControl:

Error control in the data link layer is based on automatic repeat request, which is the retransmission of data.

Error control at the data-link layer is normally very simple andimplemented using one of the following two methods. In both methods, a CRC is added to theframeheader bythe sender and checked bythe receiver.

❑ Inthe first method, if the frame is corrupted, it is silently discarded; if it is not corrupted,

the packet is delivered to the network layer. This method is used mostly in wired LANs such asEthernet.

❑ In the second method, if the frame is corrupted, it is silently discarded; if it is not corrupted, an acknowledgment is sent (for thepurposeof both flowand errorcontrol)to thesender.

CombinationofFlow andErrorControl

Flow and error control can be combined. In a simple situation, the acknowledgment that is sentfor 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. Weshow this situation when we discuss some simple protocols in the next section. A frame that carries an acknowledgment is normally called an ACK to distinguish it from the data frame.

ConnectionlessandConnection-Oriented

ADLCprotocolcanbeeitherconnectionlessor connection-oriented.

ConnectionlessProtocol

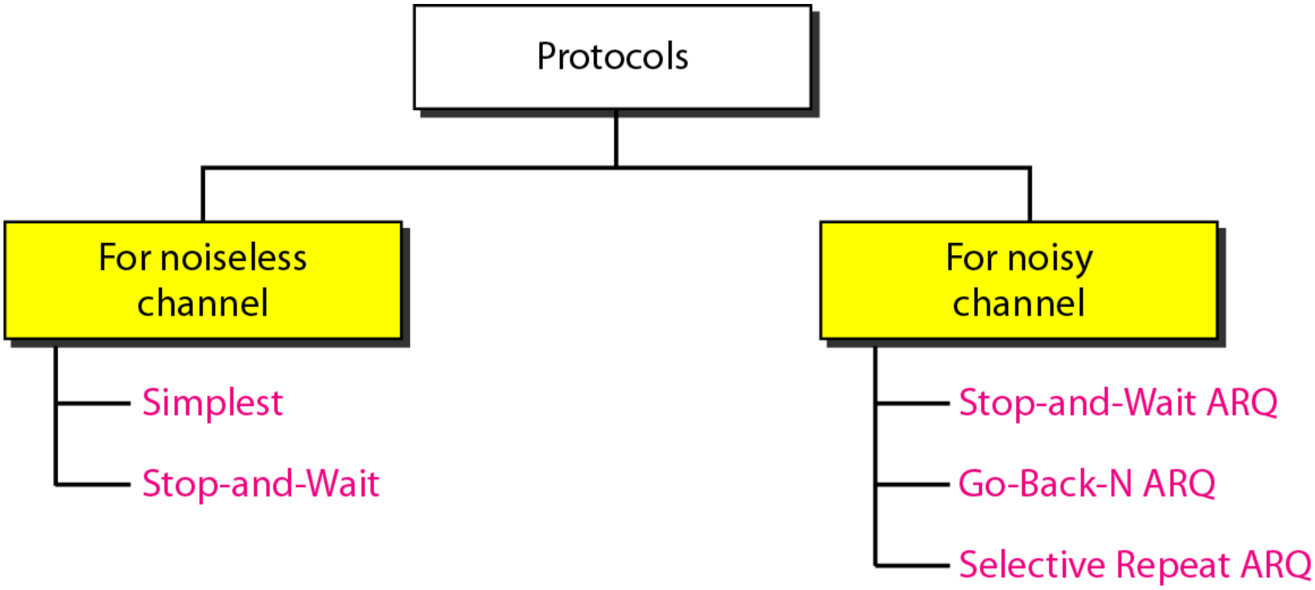
In a connectionless protocol, frames are sent from one node to the next without any relationship between the frames; each frame is independent. Note that the term connectionless here does notmean that there is no physical connection (transmission medium) between the nodes; it meansthat there is no connection between frames. The frames are not numbered and there is no sense ofordering.Most of thedata-linkprotocols for LANs areconnectionlessprotocols.

Connection-OrientedProtocol

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 (transferphase), the logical connection is terminated(teardownphase). In this type of communication, the frames are numbered and sent in order. If they are not received in order, thereceiver needs to wait until all frames belonging to the same set are received and then deliver them in order to the network layer. Connection oriented protocols are rare in wired LANs, but we can see the min somepoint-to-pointprotocols, somewireless LANs,andsome WANs.

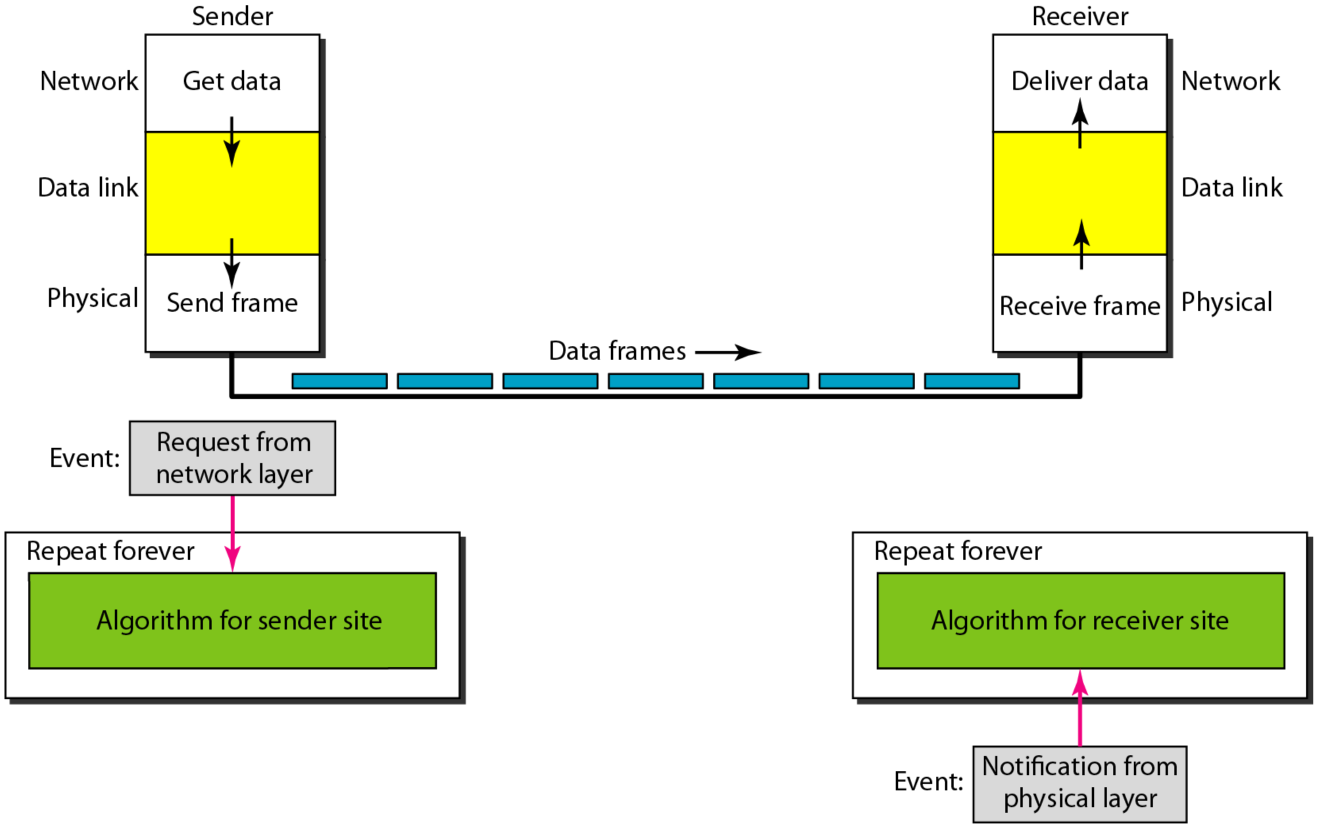
2.4 Data-LinkLayerProtocols

Traditionally four protocols have been defined for the data-link layer to deal with flow and error control: Simple, Stop-and-Wait, Go-Back-N, and Selective-Repeat.

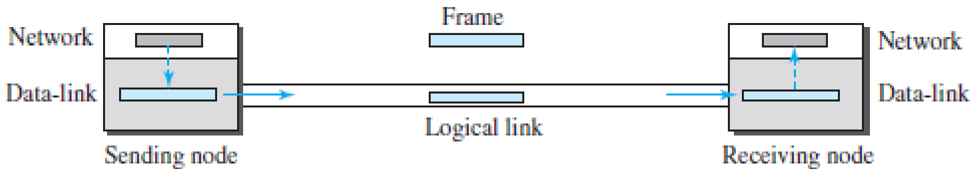


SimpleProtocol

Our first protocol is a simple protocol with neither flow nor error control. We assume that thereceiver can immediately handle any frame it receives. In other words, the receiver can never beoverwhelmedwith incomingframes.

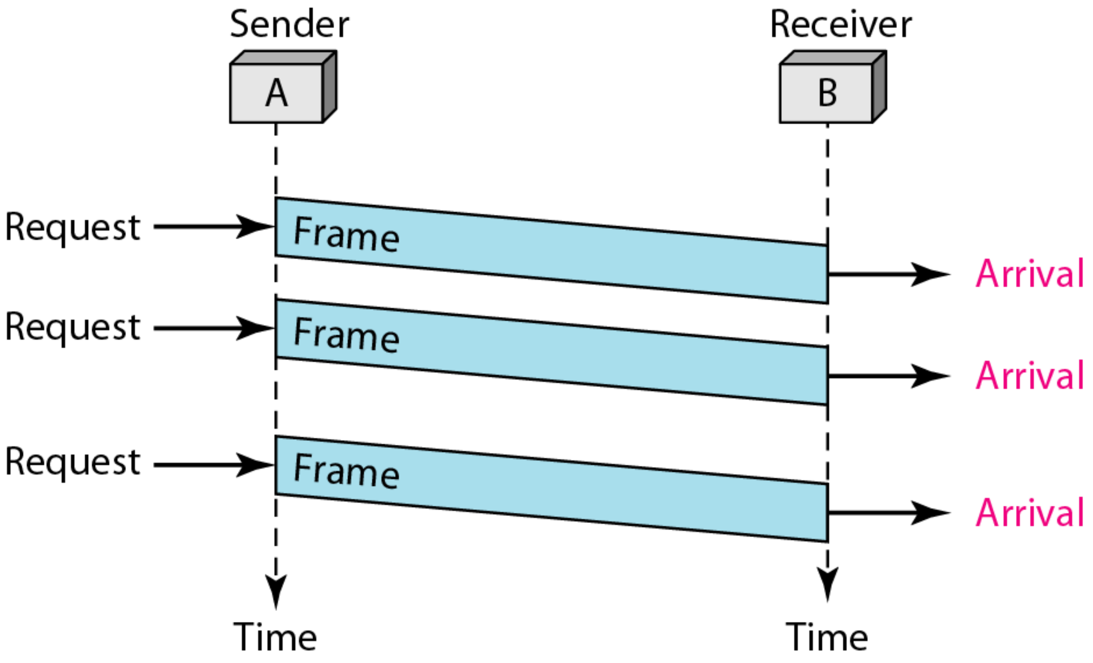


Simple protocol



The data-link layer at the sender gets a packet from its network layer, makes aframe out of it,and sends the frame. The data-link layer at the receiver receives a frame from the link, extractsthe packet from the frame, and delivers the packet to its networklayer. The data-link layers ofthesenderand receiver provide transmission services for their network layers.

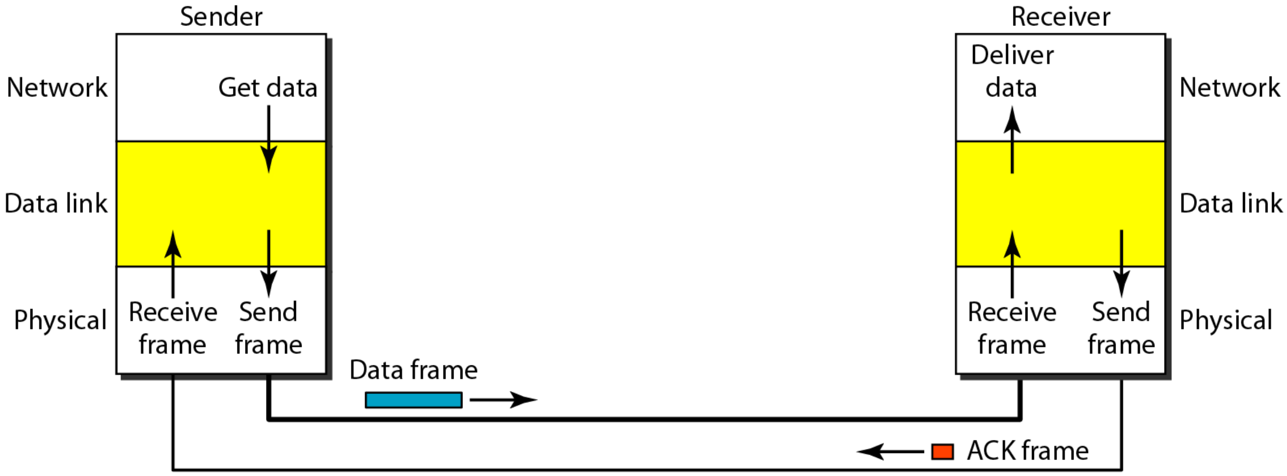
Flow Diagram:

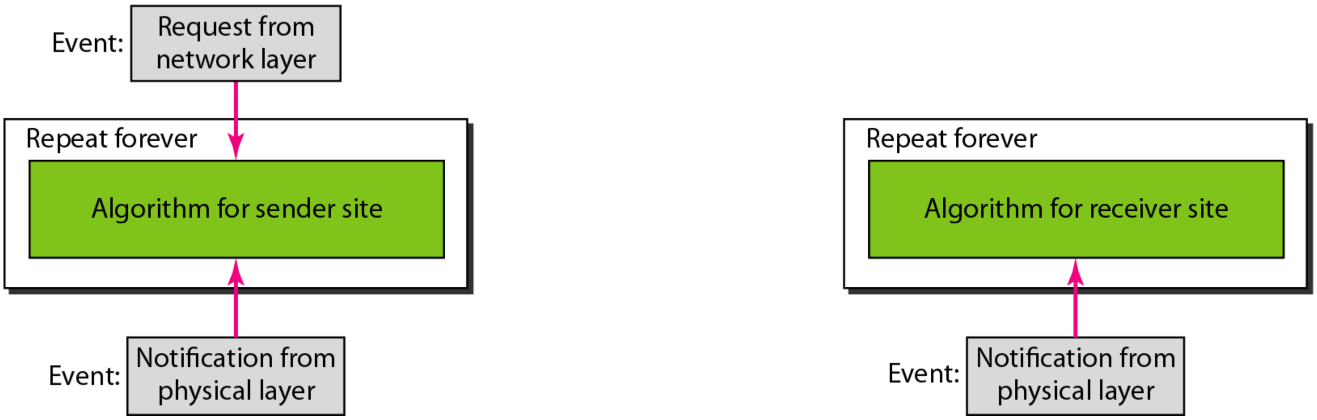


Stop-and-WaitProtocol

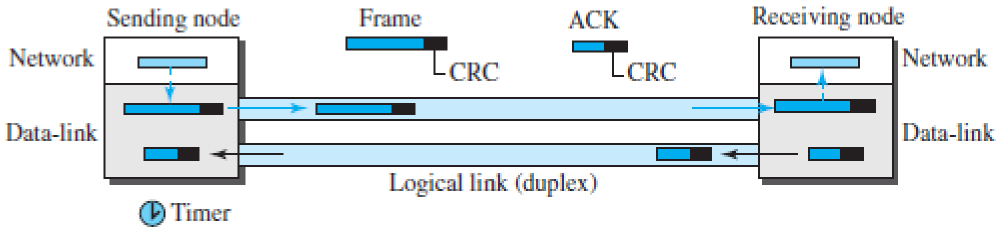
Our secondprotocoliscalledthe Stop-and-Wait protocol, which uses both flow and error control. In this protocol, the sendersends one frame at a time and waits for an acknowledgment before sending the next one. Todetect corrupted frames, we need to add a CRC to each data frame. When aframe arrives at the receiver site, it is checked. If its CRC is incorrect, the frame is corrupted andsilently discarded. The silence of the receiver is a signal for the sender that a frame was eithercorrupted 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 thenext frame(if ithas one to send). If the timer expires, the sender resends the previous frame,

assuming that theframe was either lost or corrupted. This means that the sender needs to keep a copy of the frameuntil its acknowledgment arrives. When the corresponding acknowledgment arrives, the senderdiscardsthecopyand sends thenext frame if it is ready.




Event:
Request from network layer
Repeat forever
Algorithm for sender site
Event:
Notification from physical layer
Repeat forever
Algorithm for receiver site
Event:
Notification from physical layer

Stop-and-Wait protocol



SenderStates

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 networklayer. If a packet comes from the network layer, the sender creates a frame, saves a copy of theframe,starts the onlytimer and sends theframe. 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.

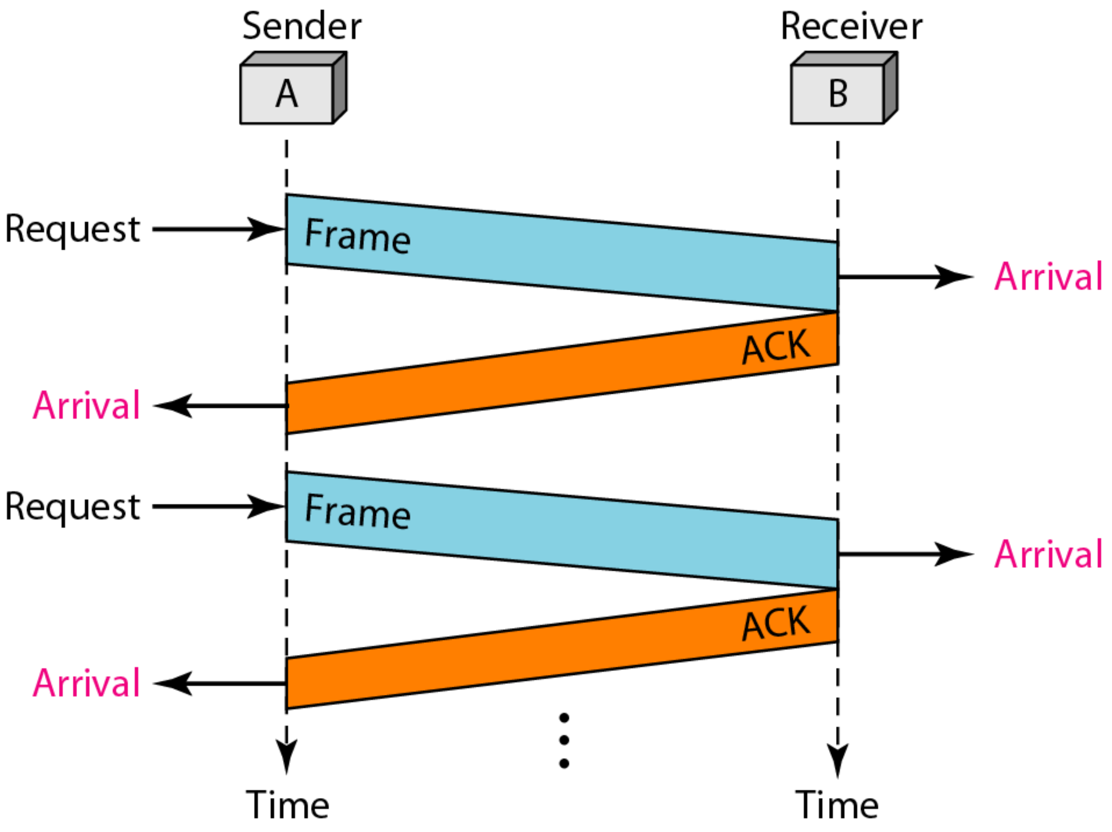
Receiver

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.

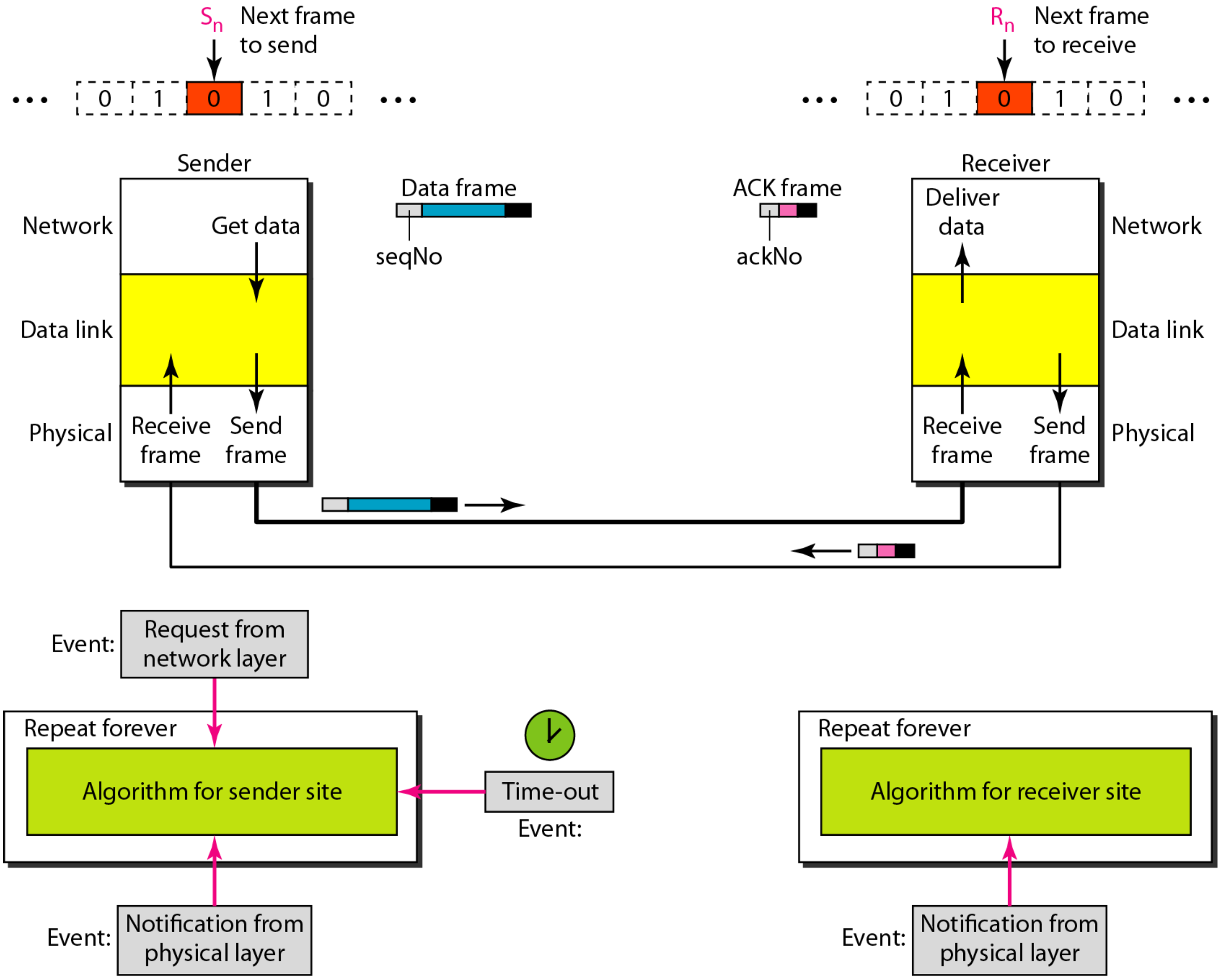
Flow Diagram:



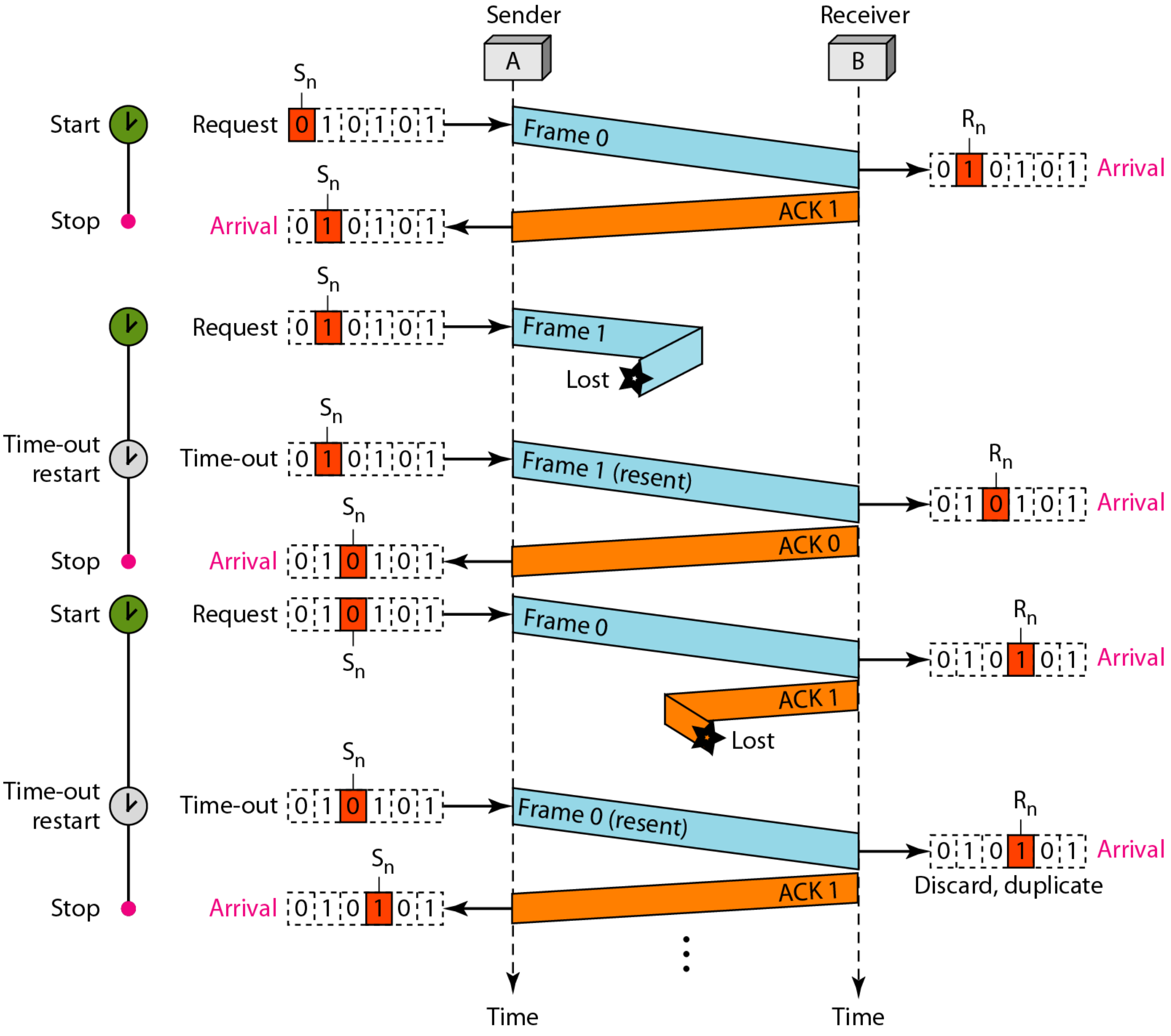
Stop-and-Wait Automatic Repeat Request

Error correction in Stop-and-Wait ARQ is done by keeping a copy of the sent frame and retransmitting of the frame when the timer expires.

In Stop-and-Wait ARQ, we use sequence numbers to number the frames.The sequence numbers are based on modulo-2 arithmetic. The acknowledgment number always announces in modulo-2 arithmetic the sequence number of the next frame expected.



Flow Diagram:

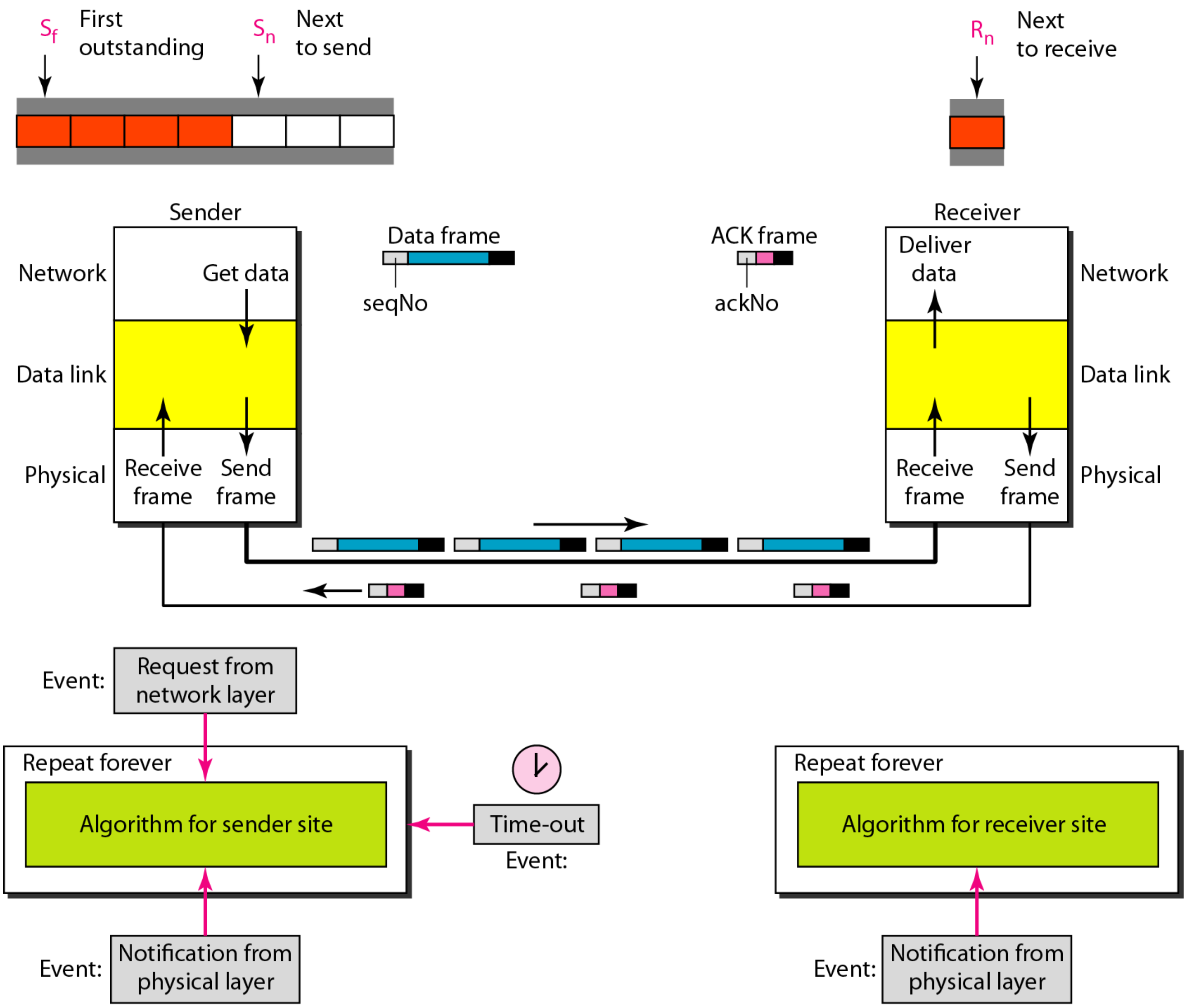


Go-Back-N Protocol

In the Go-Back-N Protocol, the sequence numbers are modulo 2^m,where m is the size of the sequence number field in bits.

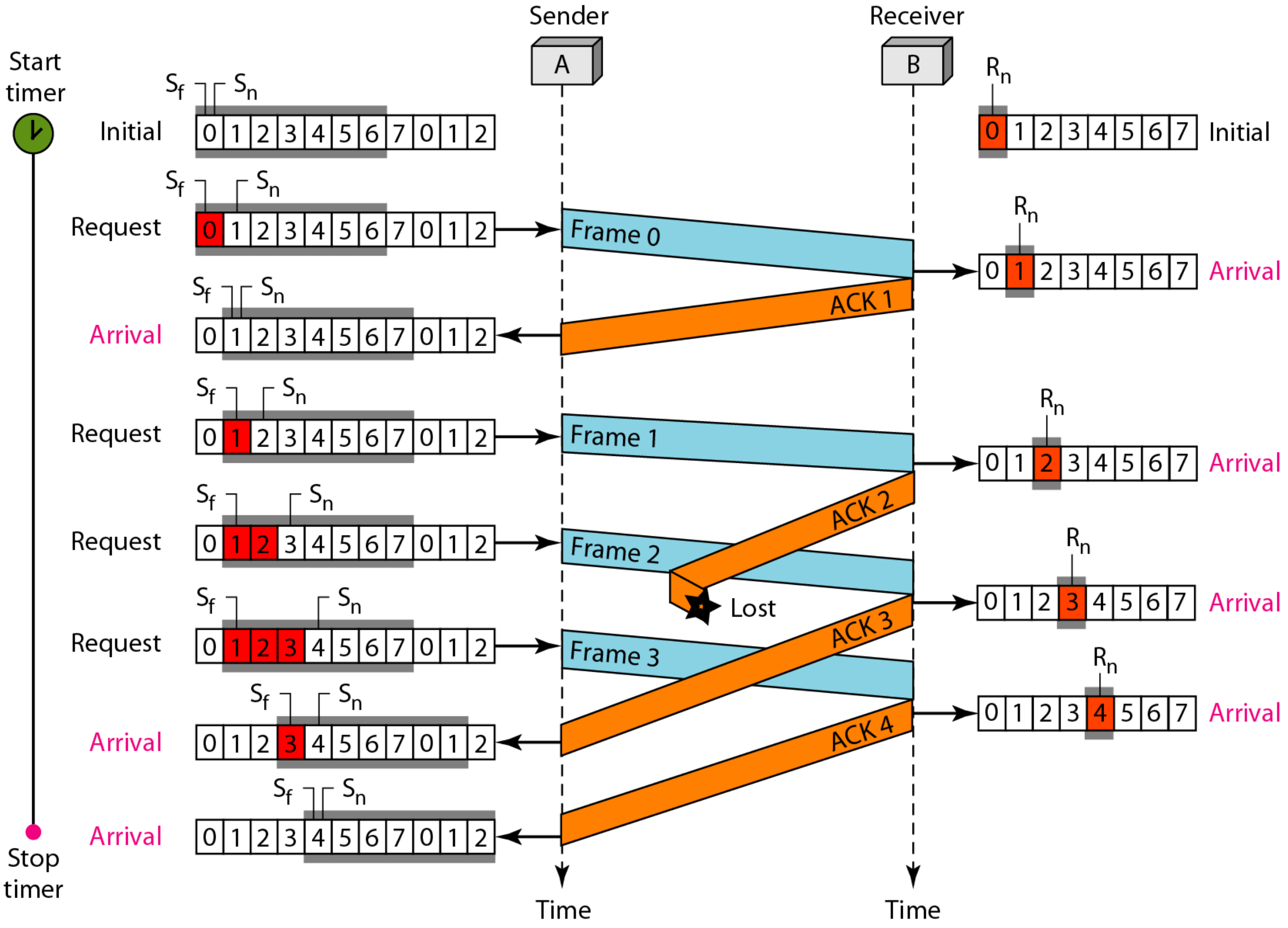
The send window can slide oneor more slots when a valid acknowledgment arrives.

The receive window is an abstract concept defining an imaginary box of size 1 with one single variable Rn. The window slideswhen a correct frame has arrived; sliding occurs one slot at a time.



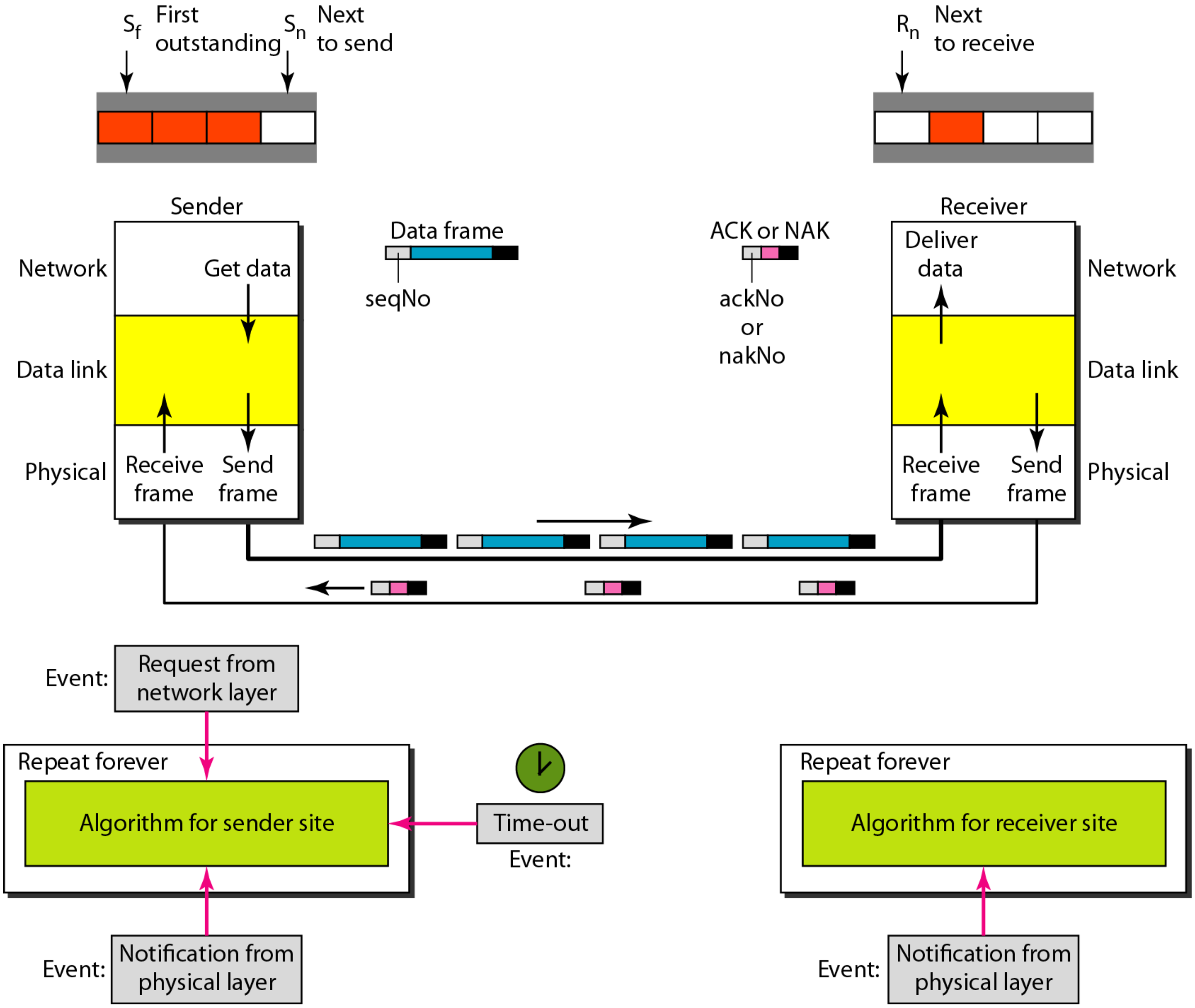
In Go-Back-N ARQ, the size of the send window must be less than 2m;the size of the receiver window is always 1.

Flow Diagram:

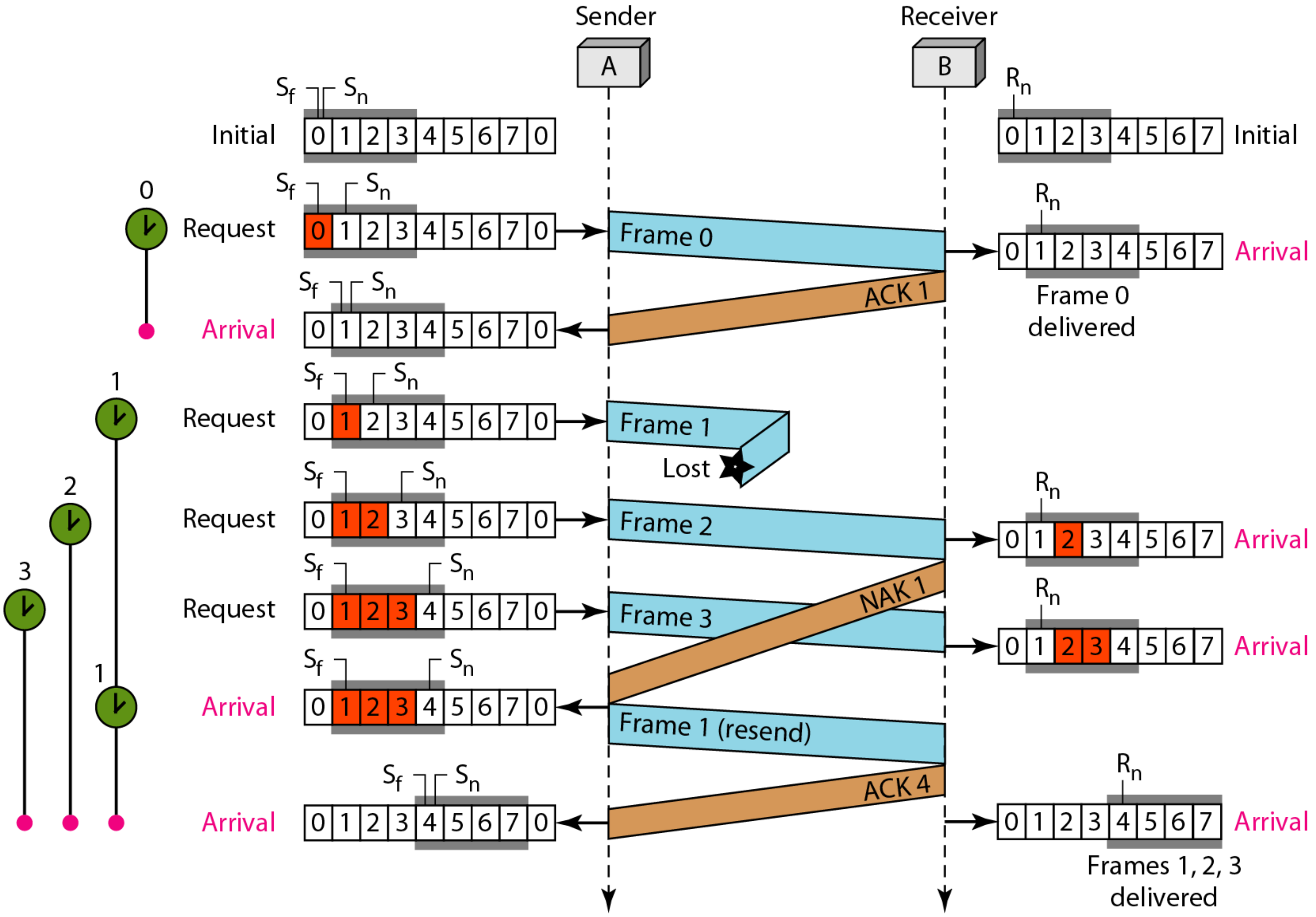


Selective Repeat ARQ

In Selective Repeat ARQ, the size of the sender and receiver window must be at most one-half of 2^m.

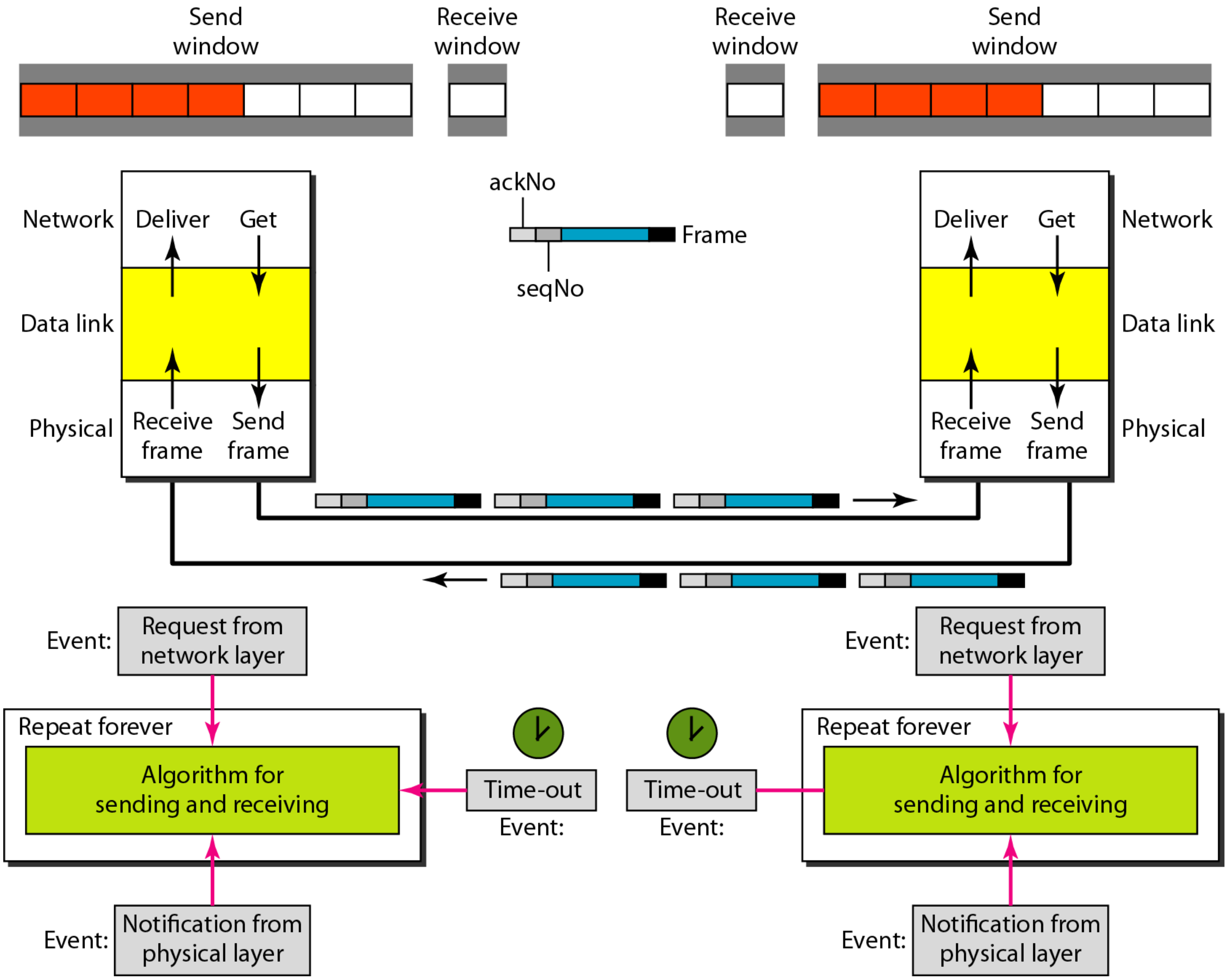


Flow diagram:



Piggybacking

Protocols have been designed in the past to allow data to flow in both directions.However, to make the communication more efficient, the data in one direction is piggy backed with the acknowledgment in the other direction. In other words, when node A is sending data tonode B, Node A also acknowledges the data received from node B. Because piggybacking makes communication at the data link layer more complicated, it is not a common practice.



2.5 HDLC

HDLC - Short for High-level Data Link Control, a transmission protocol used at the data linklayer (layer 2) of the OSI seven layer model for data communications.

High-level Data Link Control (HDLC) is a bit-oriented protocol for communication over point-to-point and multipoint links. It implements the ARQ mechanisms.The HDLC protocolembeds information in a data frame that allows devices to control data flow and correct errors.HDLC is an ISO standard developed from the Synchronous Data Link Control (SDLC) standard proposed by IBM in the 1970's. HDLC NRM (also knownas SDLC).

TypesofFramesinHDLC

HDLCdefinesthreetypesofframes:

1. Informationframes(I-frame)

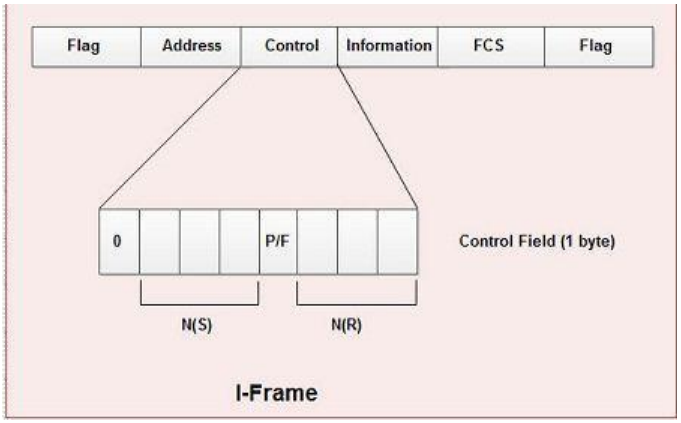
2. Supervisoryframe(S-frame)

3. Unnumberedframe(U-frame)

1. Informationframes

• I-frames carry user's data and control information about user's data.

• I-frame carries user data in the information field.



• The first bit of control field is always zero, *i.e*. the presence of zero at this place indicates that itisI-frame.

• Bit number 2, 3 & 4 in control field is called N(S) that specifies the sequence number of theframe. Thus it specifies the number of the frame that is currently being sent. Since it is a 3.bitfield,onlyeight sequencenumbers arepossible 0,1,2,3,4,5,6, 7 (000 to 111).

• Bit number 5 in control field is P/F i.e. Poll/Final and is used for these two purposes. It has,meaningonlywhenit is seti.e. whenP/F=1.Itcanrepresent thefollowing two cases.

(i) It means poll when frame is sent by a primary station to secondary (when address fieldcontainsthe address of receiver).

(ii) It means final when frame is sent by secondary to a primary (when the address field containstheaddress of thesender).

• Bit number 6, 7, and 8 in control field specifies N(R) i.e. the sequence number of the frameexpectedin return in two-waycommunication.

If last frame received was error-free then N(R) number will be that of the next frame is sequence.If the last frame was not received correctly, the N(R) number will be the number of the damagedframe, asking forits retransmission.

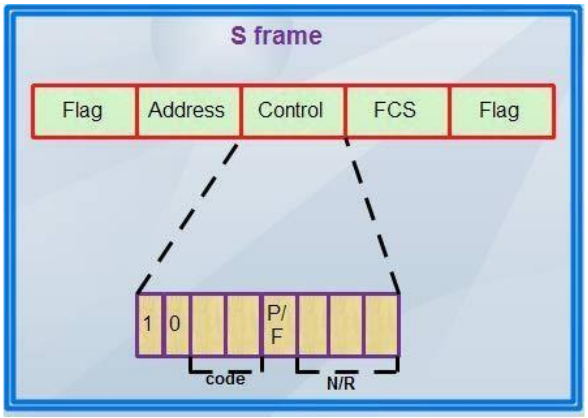
2. Supervisoryframe

• S-frame carries control information, primarily data link layer flow and error controls.

• It does not contain information field.

• The format of S-frame is shown in diagram.

•



• The first two bits in the control field of S-frame are always10.

• Then there is a bitcode field that specifies four types of S-frame with combination 00, 01, 10, 11 as shown in table :-

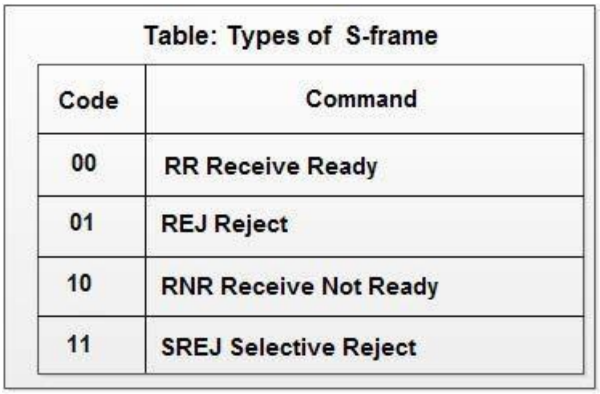


Table: Types of S-frame

Code	Command
00	RR Receive Ready
01	REJ Reject
10	RNR Receive Not Ready
11	SREJ Selective Reject

1. RR, Receive Ready-used to acknowledge frames when no I-frames are availab1e to piggyback the acknowledgement.

2. REJReject - used by the receiver to send a NAK when error has occurred.

3. RNRReceive Not Ready-used for flow control.

4. SREJ SelectiveReject-indicates to the transmitter that it should retransmit the frame indicated in the N(R) subfield.

- There is no N(S) field in control field of S-frame as S-frames do not transmit data.
- *P/F* bit is the fifth bit and serves the same purpose as discussed earlier.
- Last three bits in control field indicates N(R) *i.e.* they correspond to the ACK or NAK value.

3.Unnumberedframe

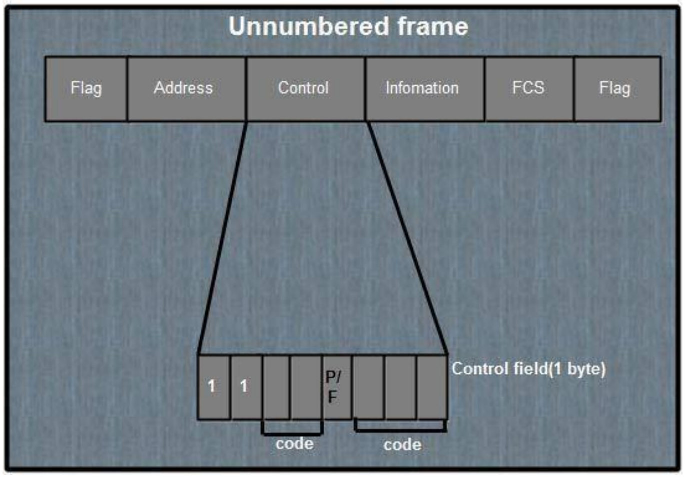
- U-frames are used to exchange session management and control information

between the two connected devices.

- Information field in U-frame does not carry user information rather, it carries

system management information.

- The frame format of U-frame is shown in diagram.
- U-frame is identified by the presence of 11 in the first and second bit position in control field.
- These frames do not contain N(S) or N(R) in controlfield.



- U-frame contains two code fields, one two bit and other three bit.
- These five bits can create upto 32 different U-frames.
- .*P/F* bit in control field has same purpose in I-frame.

Protocol Structure - HDLC: High Level Data Link ControlFlag-

The value of theflagis always (0x7E).

Address field - Defines the address of the secondary station which is sending the frame or thedestination of the frame sent by the primary station. It contains Service Access Point (6bits), aCommand/Response bit to indicate whether the frame relates to information frames (I-frames)being sent from the node or received by the node, and an address extension bit which is usuallyset to true to indicate that the address is of length one byte. When set to false it indicates anadditionalbyte follows.

Extended address - HDLC provides another type of extension to the basic format. The address field may be extended to more than one byte by agreement between the involved parties.

Controlfield- Serves to identify the type of the frame. In addition, it includes sequence numbers, control features and error tracking according to theframe type.

FCS - The Frame Check Sequence (FCS) enables a high level of physical error control byallowingthe integrityof thetransmitted framedatato be checked.

2.6 POINT-TO-POINTPROTOCOL(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 anInternet service provider use PPP. The majority of these users have a traditional modem; they areconnected to the Internet through a telephone line, which provides the services of the physicallayer. But to control and manage the transfer of data, there is a need for a point-to-point protocolatthedata-link layer. PPP is byfar themost common.

Services

The designers of PPP have included several services to make it suitable for a point-to pointprotocol,but have ignored some traditional services to make it simple.

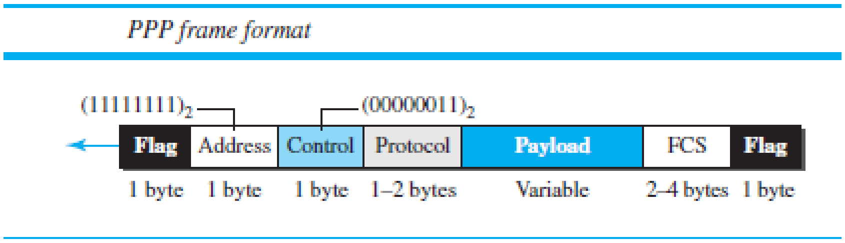
Services ProvidedbyPPP

PPP defines the format of the frame to be exchanged between devices. It also defines how twodevices can negotiate the establishment of the link and the exchange of data. PPP is designed toaccept payloads from several network layers (not only IP). Authentication is also provided in theprotocol, but it is optional. The new version of PPP, called Multilink PPP, provides connections over multiple links. One interesting feature of PPP is that it provides network address configuration. This is particularly useful when a home user need satemporary network address to connect to theInternet.

Framing

PPP uses a character – oriented (orbyte-oriented) frame. Figure shows the format of a PPP frame. The description of each field follows:

❑ ***Flag.***A PPP frame startsand ends with a1-byte flag with the bit pattern 01111110.



PPP frame format

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

❑ ***Control.*** This field is set to the constant value 00000011 (imitating unnumbered frames inHDLC). PPP does not provide any flow control. Error control is alsolimitedto 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; butthis can be changed during negotiation. The data field is byte-stuffed if the flag byte patternappears 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.

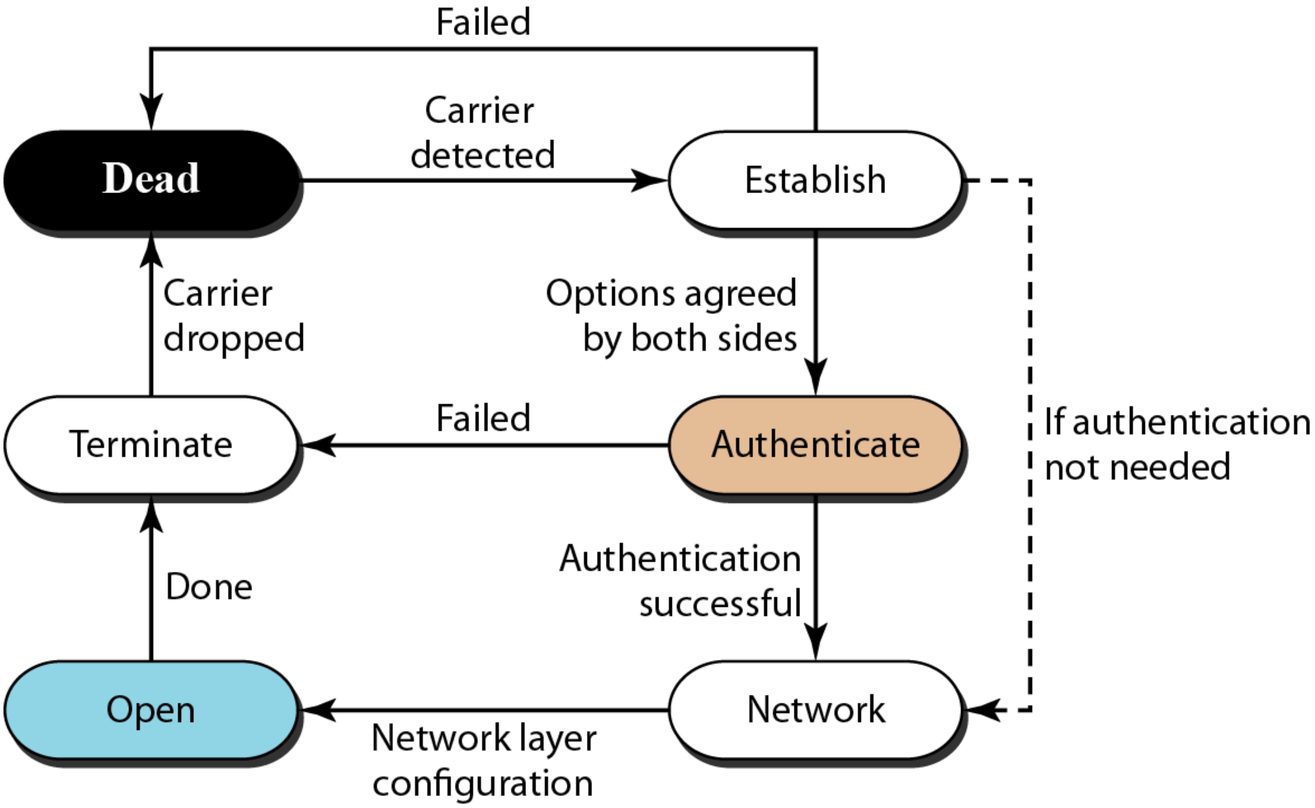
❑ ***FCS.***Theframecheck sequence(FCS)is simplya2-byteor4-bytestandard CRC.

ByteStuffing

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 meansthat every time the flag like pattern appears in the data, thisextra byteisstuffed totell thereceiver that the next byte is not a flag. Obviously, the escape byte itself should be stuffed with another escape byte.

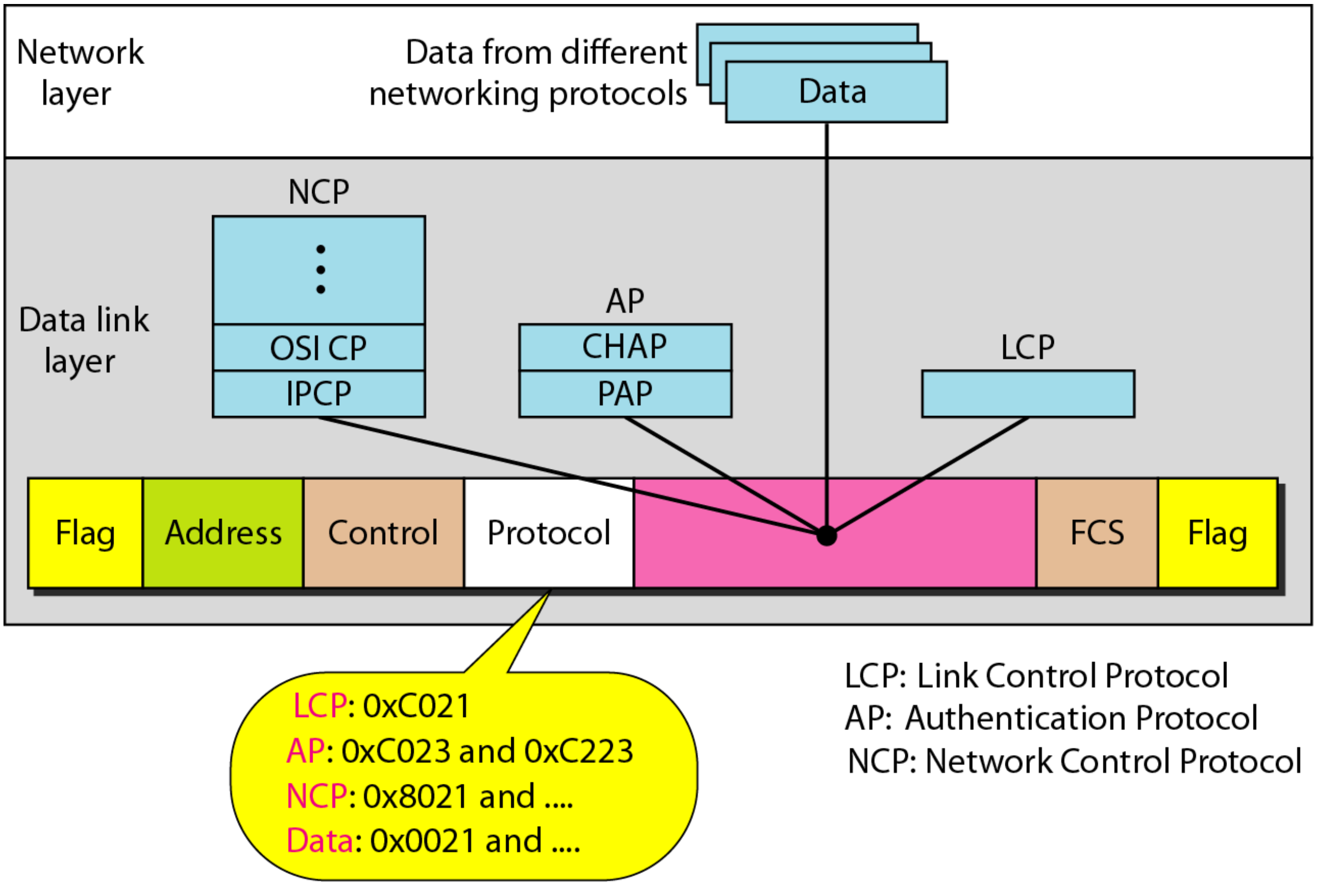
TransitionPhases

A PPP connection goes through phases which can be shown in a *transition phase* diagram. Thetransition diagram, which is an FSM, starts with the *dead* state. In this state, there is no activecarrier (atthe physicallayer) andthe line isquiet.Whenoneof 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,ifthey donotknow eachother), thenthe system needs to do authentication(an extra step); otherwise, the parties can simply start communication. The link-control protocol packets, discussed shortly, are used for this purpose. Several packets may be exchanged here. Data transfer takes place in the *open* state. When a connection reaches this state, the exchange of datapackets can be started. The connection remains in this state until one of the endpoints wants toterminate the connection. In this case, the system goes to the *terminate* state. The system remainsin this state until the carrier (physical-layer signal) is dropped, which moves the system to the *dead* state again.


Failed
Carrier detected
Dead
Establish
Carrier dropped
Options agreed by both sides
Terminate
Failed
Authenticate
If authentication not needed
Done
Authentication successful
Open
Network
Network layer configuration

Multiplexing

Although PPP is a link-layer protocol, it uses another set of protocols to establish the link,authenticate the parties involved, and carry the network-layer data. Three sets of protocols aredefined to make PPP powerful: the Link Control Protocol (LCP), two Authentication Protocols(APs), and several Network Control Protocols (NCPs). At any moment, a PPP packet can carrydata from one of these protocols in its data field. Data mayalso comefromseveral different networklayers.



2.7 MediaAccessControl

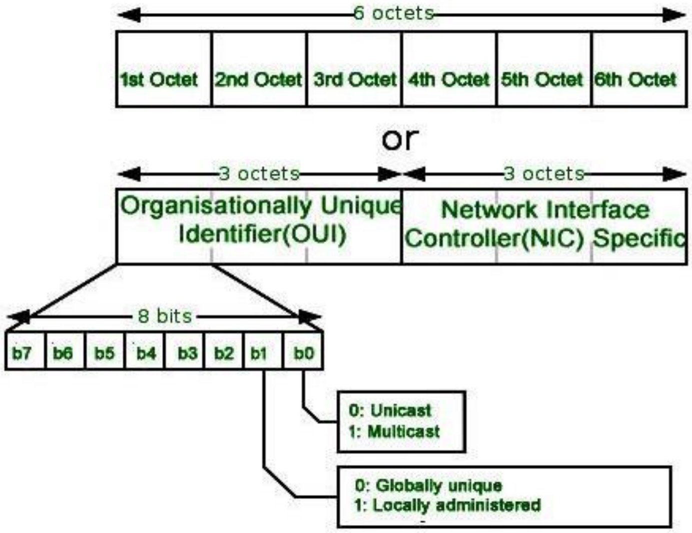
In order to communicate or transfer the data from one computer to another computer we needsome address. In Computer Network various types of address are introduced; each works at different layer. Media Access Control Address is a physical address which works at Data LinkLayer. In thisarticle, we will discuss about addressing in DLL, which is MAC Address.

MediaAccessControl(MAC)Address –

MAC Addresses are unique 48-bits hardware number of a computer, which is embedded into network card(known as Network Interface Card) during the time of manufacturing. MAC Address is also known as Physical Address of a network device. In IEEE802 standard, DataLink Layer is divided into two sublayers–

1. Logical Link Control(LLC) Sublayer
2. Media Access Control(MAC) Sublayer

MAC address is used by Media Access Control (MAC) sublayer of Data-Link Layer. MACAddress is word wide unique, since millions of network devices exists and we need to uniquelyidentifyeach.



FormatofMACAddress–

MAC Address is a 12-digit hexadecimal number (6-Byte binary number), which is mostly represented by Colon-Hexadecimal notation. First 6-digits (say 00:40:96) of MAC Address identifies the manufacturer, called as OUI (Organizational Unique Identifier). IEEE Registration Authority Committeeassign these MAC prefixes to its registered vendors.

Here are some OUIof well known manufacturers :

CC:46:D6-Cisco

3C:5A:B4 - Google,

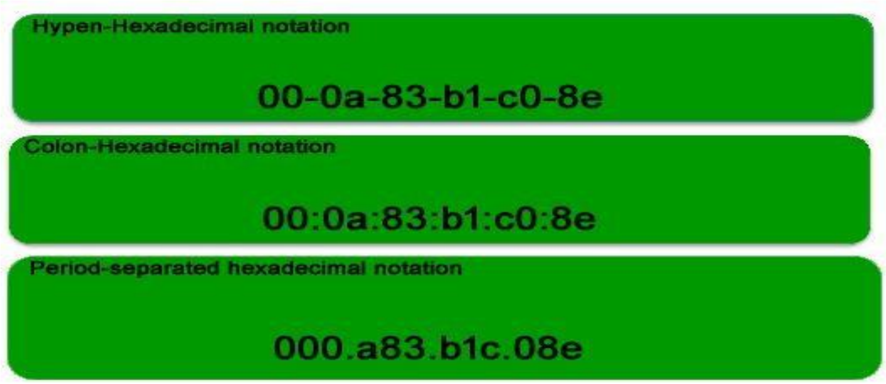
Inc.3C:D9:2B - Hewlett Packard

00:9A:CD – HUAWEI TECHNOLOGIES CO., LTD

The right most six digits represents Network Interface Controller, which is assigned by manufacturer.

As discussed above, MAC address is represented by Colon-Hexadecimal notation. But this is justa conversion, not mandatory. MAC address can be represented usingany of the following formats

–



Hypen-Hexadecimal notation

00-0a-83-b1-c0-8e

Colon-Hexadecimal notation

00:0a:83:b1:c0:8e

Period-separated hexadecimal notation

000.a83.b1c.08e

Note: Colon – Hexadecimal notation is used by *Linux OS* and Period-separated Hexadecimal notation is used by *Cisco Systems*.

How to find MAC address–

Command for UNIX/Linux -

ifconfig -aiplink list

ipaddress show

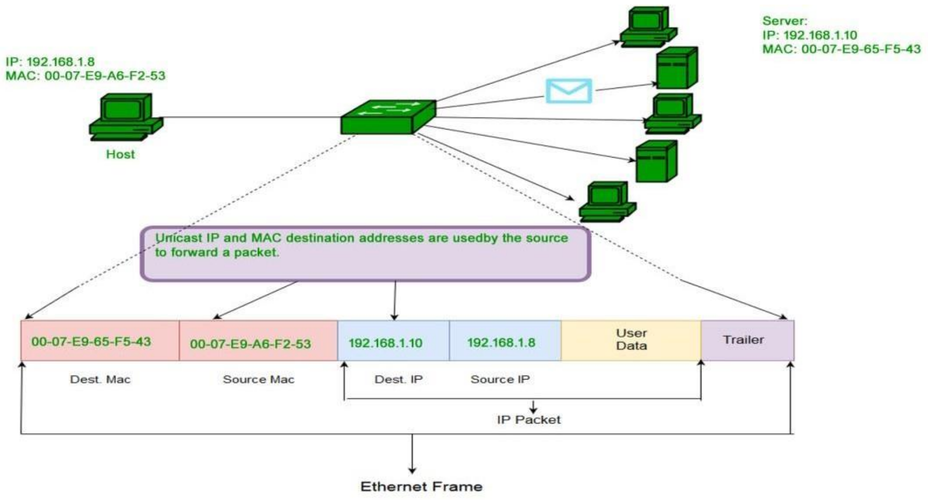
Command for Windows OS-*ipconfig/all*

Mac OS - *TCP/IP Control Panel*

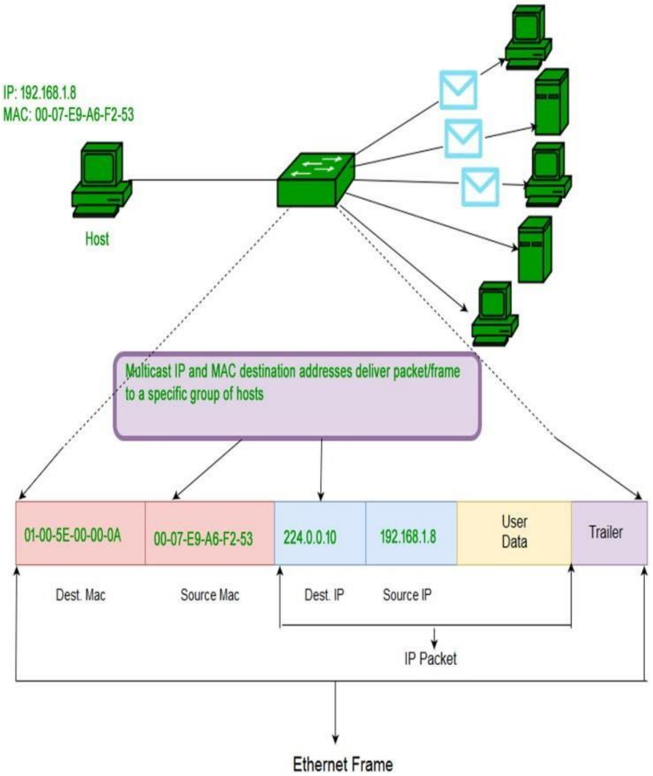
Note – LAN technologies like Token Ring, Ethernet use MAC Address as their Physical address but there are some networks (AppleTalk) which does not use MAC address.

Typesof MACAddress–

1. Unicast – A Unicast addressed frame is only sent out to the interface leading to specific NIC. If the LSB (least significant bit) of first octe to fan address is set to zero, the frame is meant to reach only one receiving NIC. MAC Address of source machine is always Unicast.

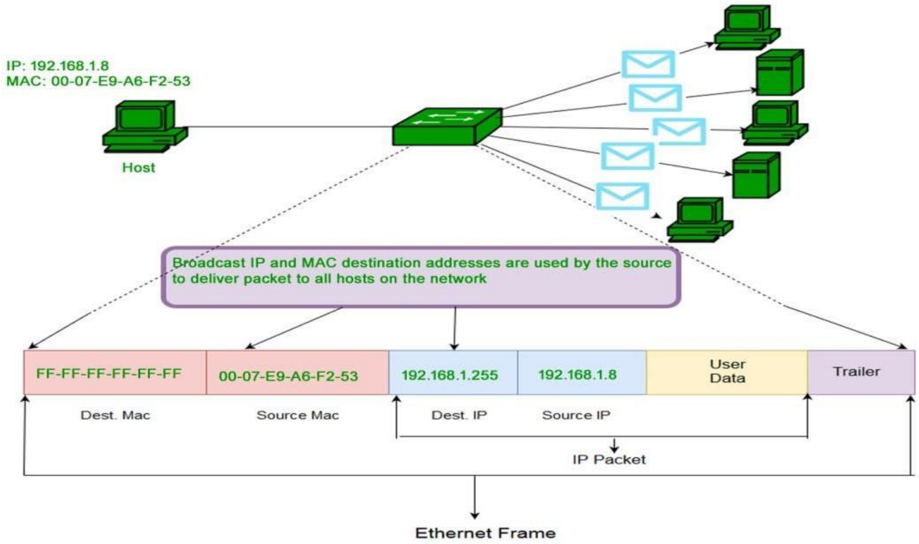


2. **Multicast –** Multicast address allow the source to send a frame to group of devices. InLayer-2(Ethernet) Multicast address, LSB(least significant bit) of first octetofan address is set to one. IEEE has allocated the address block 01-80-C2-xx-xx-xx (01-80-C2-00-00-00to01-80-C2-FF-FF-FF)for group addresses for use by standard protocols.



3. **Broadcast –** Similar to Network Layer, Broadcast is also possible on underlying layer(DataLink Layer). Ethernet frames with ones in all bits of

the destination address(FF-FF-FF-FF-FF-FF) are referred as broadcast address. Frames which are destined with MAC address FF-FF-FF-FF-FF-FF will reach to every computer belong to that LAN segment.



Whatis MACCloning –

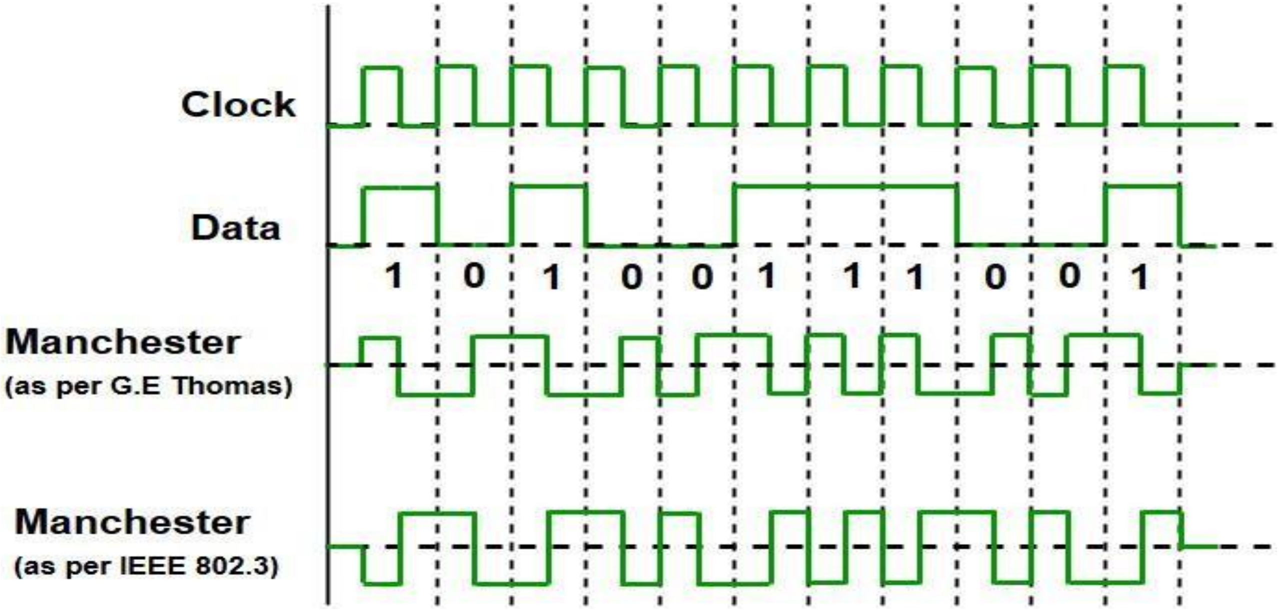
Some ISPs use MAC address inorder to assign IP address to gateway device. When deviceconnects to the ISP, DHCP server records the MAC address and then assign IP address. Now thesystem will be identified through MAC address. When the device get disconnected, it looses theIP address. If user wants to reconnect, DHCP server checks if the device is connected before. Ifso, then server tries to assign same IP address (in case lease period not expired). In case userchanged the router, user has to inform the ISP about new MAC address because new MACaddress is unknown to ISP, so connection cannot be established.Or the other option is Cloning, user can simply clone the registered MAC address with ISP. Now router keeps reporting old MAC address to ISP and there will be no connection issue.

2.8 WiredLANs: Ethernet

Local Area Network (LAN) is a data communication network connecting various terminals orcomputers within a building or limited geographical area. The connection among the devicescould be wired or wireless. Ethernet, Token Ring and Wireless LAN using IEEE 802.11 areexamplesof standardLAN technologies.

Ethernet:-

Ethernet is most widely used LAN Technology, which is defined under IEEE standards 802.3.The reason behind its wideusabilityis Ethernet is easyto understand,implement, maintain and allow slow-cost network implementation. Also,Ethernet offers flexibility in terms of topologies which are allowed. Ethernet operates in two layers of the OSI model, Physical Layer, and DataLink Layer. For Ethernet, the protocol data unit is Frame since we mainly deal with DLL. Inorder to handle collision, the Access control mechanism used in Ethernet is CSMA/CD.Manchester EncodingTechnique is used in Ethernet.



Since we are talking about IEEE 802.3 standard Ethernet therefore, 0 is expressed by a high-to-low transition, a 1 by the low-to-high transition. In both Manchester Encoding and DifferentialManchester,EncodingBaud rate is doubleof bit rate.

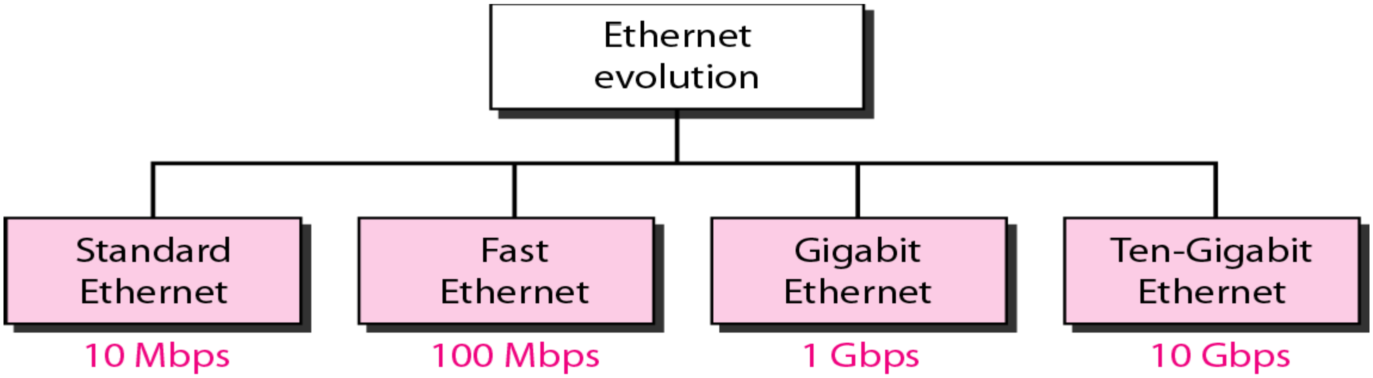
Baudrate=2*Bit rate

Ethernet LANs consist of network nodes and interconnecting mediaor link. The network nodes can beof two types:

- Data Terminal Equipment (DTE):- Generally, DTEs are the end devices that convert the userinformation into signals or reconvert the received signals. DTEs devices are: personal computers,workstations, file servers or print servers also referred to as end stations. These devices are eitherthe source or the destination of data frames. The data terminal equipment may be a single piece of equipment or multiple pieces of equipment that are interconnected and perform all the required functions to allow the user to communicate. A user can interact to DTE or DTE may beauser.

- DataCommunicationEquipment(DCE):-DCEs are the inter mediate network devices that receive and forward frames across the network. They may be either standalone devices such asrepeaters, network switches, routers or maybe communications interface units such as interfacecards and modems. The DCE performs functions such as signal conversion, coding and may be apartofthe DTE or intermediate equipment.

Ethernet evolution through four generations



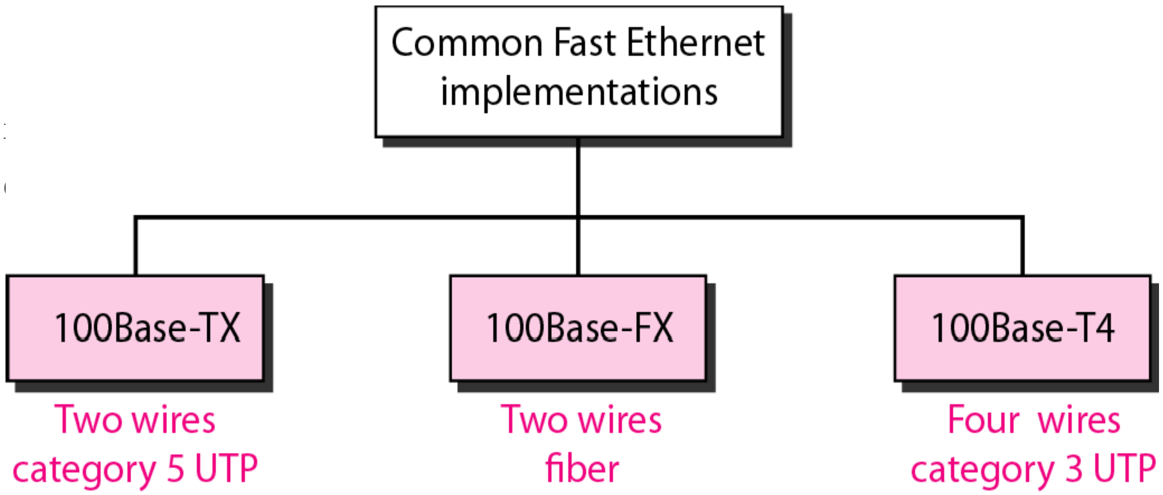
i) Standard Ethernet

- Transfer data at a rate of 10 Mbps.

Characteristics	*10Base5*	*10Base2*	*10Base-T*	*10Base-F*
Media	Thick coaxial cable	Thin coaxial cable	2 UTP	2 Fiber
Maximum length	500 m	185 m	100 m	2000 m
Line encoding	Manchester	Manchester	Manchester	Manchester

ii) FastEthernet

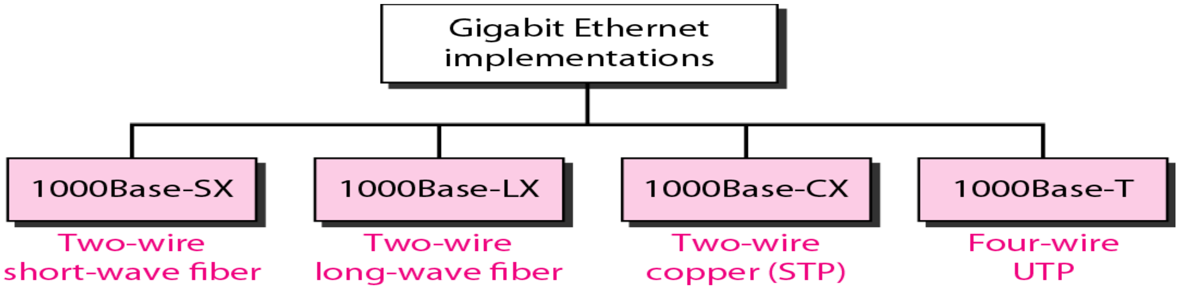
Fast Ethernet refers to an Ethernet network that can transfer data at a rate of 100Mbit/s.

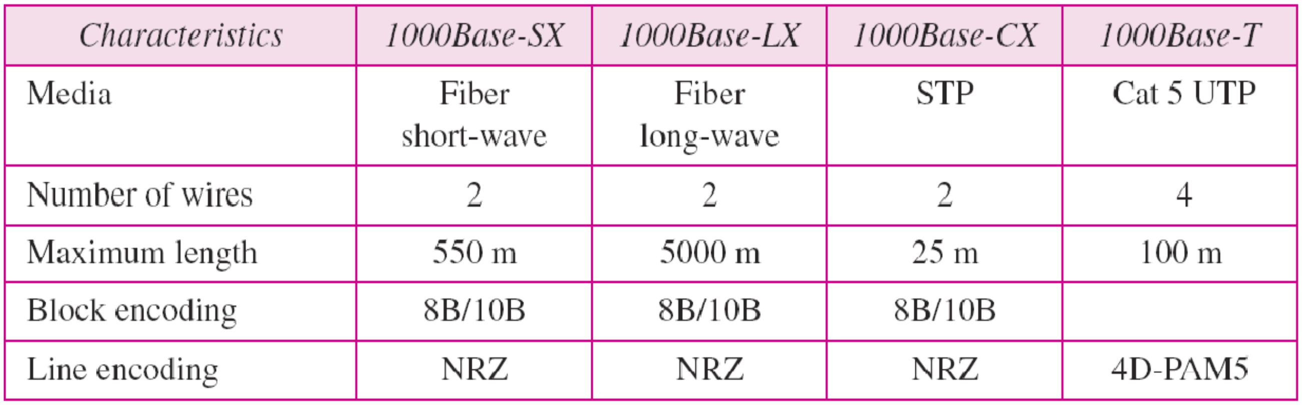


Characteristics	*100Base-TX*	*100Base-FX*	*100Base-T4*
Media	Cat 5 UTP or STP	Fiber	Cat 4 UTP
Number of wires	2	2	4
Maximum length	100 m	100 m	100 m

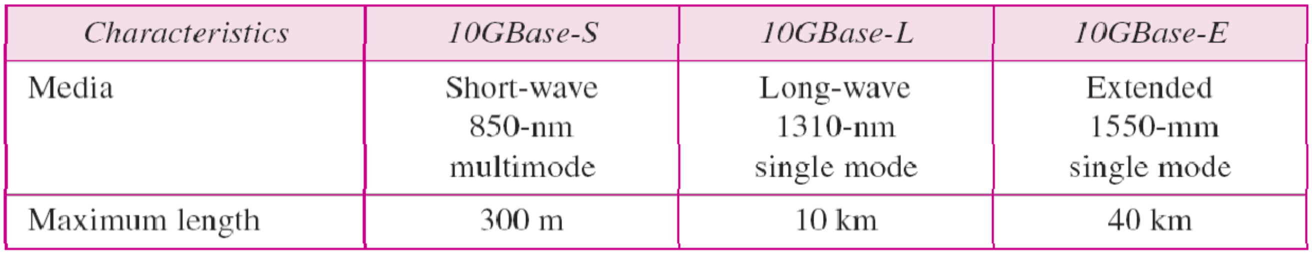
iv. 10GigabitEthernet

10 Gigabit Ethernet is the recent generation and delivers a data rate of 10 Gbit/s (10,000 Mbit/s).Itisgenerallyused for backbonesin high-end applicationsrequiringhigh datarates.





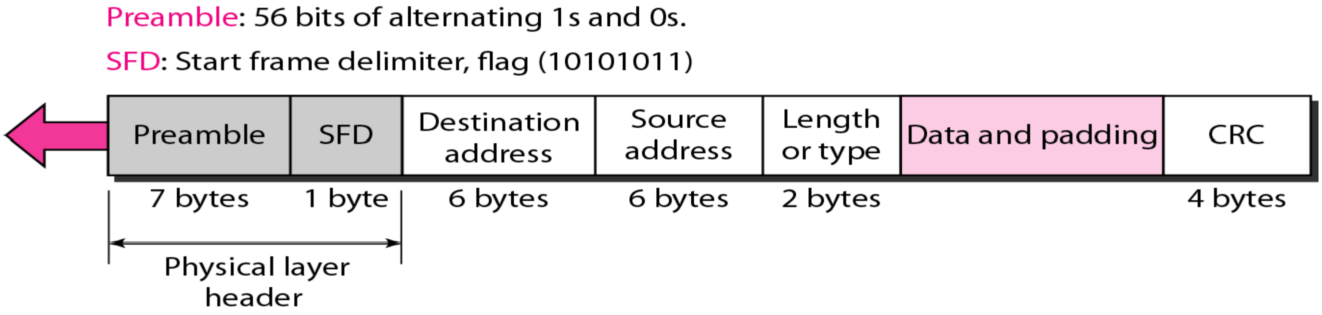
Characteristics	*1000Base-SX*	*1000Base-LX*	*1000Base-CX*	*1000Base-T*
Media	Fiber short-wave	Fiber long-wave	STP	Cat 5 UTP
Number of wires	2	2	2	4
Maximum length	550 m	5000 m	25 m	100 m
Block encoding	8B/10B	8B/10B	8B/10B	
Line encoding	NRZ	NRZ	NRZ	4D-PAM5



Characteristics	*10GBase-S*	*10GBase-L*	*10GBase-E*
Media	Short-wave 850-nm multimode	Long-wave 1310-nm single mode	Extended 1550-mm single mode
Maximum length	300 m	10 km	40 km

802.3 MAC Frame Format:

The Ethernet frame contains seven fields: preamble, SFD, DA, SA, length or type of protocol data unit (PDU), upper-layer data, and the CRe. Ethernet does not provide any mechanism for acknowledging received frames, making it what is known as an unreliable medium. Acknowledgments must be implemented at the higher layer.



- **Preamble.** The first field of the 802.3 frame contains 7 bytes (56 bits) of alternating Os and 1s that alerts the receiving system to the coming frame and enables it tosynchronize its input timing. 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 theframe. The preamble is actually added at the physical layer and is not (formally)part of the frame.
- **Start frame delimiter (SFD)**. The second field (l byte: 10101011) signals thebeginning of the frame. The SFD warns the station or stations that this is the lastchance for synchronization. The last 2 bits is 11 and alerts the receiver that the nextfield is the destination address.
- Destination address (DA). The DA field is 6 bytes and contains the physical address of the destination station or stations to receive the packet.
- Source address (SA). The SA field is also 6 bytes and contains the physical address of the sender of the packet.
- Length or type. This field is defined as a type field or length field. The original Ethernet used this field as the type field to define the upper-layer protocol using the MAC frame. The IEEE standard used it as the length field to define the number of bytes in the data field. Both uses are common today.
- Data. This field carries data encapsulated from the upper-layer protocols. It is a minimum of 46 and a maximum of 1500 bytes.
- CRC. The last field contains error detection information, in this case a CRC-32

2.9 WirelessLANs-Introduction

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 oncollege campuses, in office buildings, and in many public areas. Before we discuss a specificprotocolrelated to wirelessLANs, let ustalkabout them ingeneral.

ArchitecturalComparison

Let us first compare the architecture of wired and wireless LANs to give some idea of what we need to look for when we study wireless LANs.

Medium

The first difference we can see between a wired and a wireless LAN is the medium. In a wired LAN, we use wires to connect hosts. In Chapter 7, we saw that we moved frommultiple accessto point-to-point access through the generation of the Ethernet. In a switched LAN, with a link-layer switch, the communication between the hosts is point-to-point and full-duplex(bidirectional). In a wireless LAN, the medium is air, the signal is generally broadcast. Whenhosts in a wirelessLAN communicate with each other, they are sharing the same medium(multipleaccess). In a very rare situation, we may be able to create a point-to-point communication between two wireless hosts by using a very limited bandwidth and two- directional antennas. Our discussion in this chapter, however, is about the multiple-accessmedium, which means we need to use MAC protocols.

Hosts

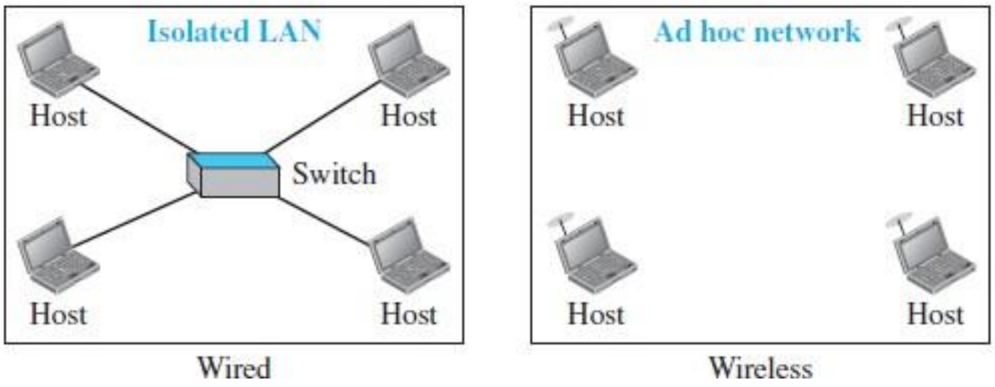
In a wired LAN, a host is always connected to its network at a point with a fixed link layer address related to its network interface card (NIC). Of course, a host can move from one point in the Internet to another point. In this case, its link-layer address remains the same, but its network-layer address will change (Mobile IP section). However, before the host can use theservices of the Internet, it needs to be physically connected to the Internet. In a wireless LAN, ahost is not physically connected to the network; it can move freely (as we'll see) and can use theservicesprovided bythenetwork.

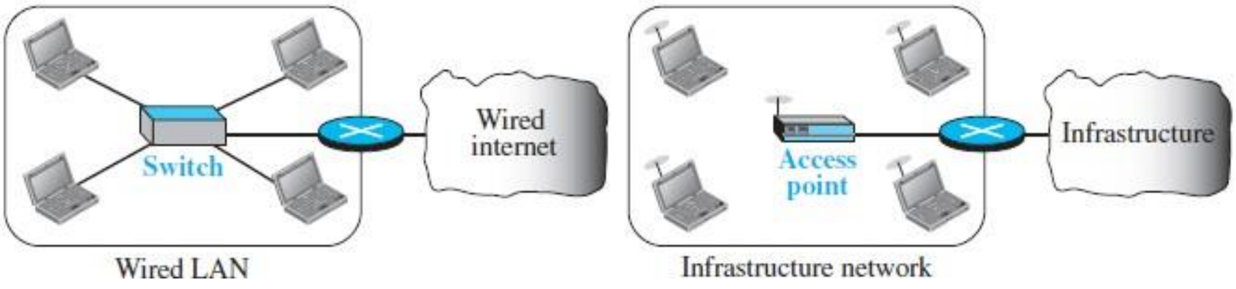
IsolatedLANs

The concept of a wired isolated LAN also differs from that of a wireless isolated LAN. A wired isolated LAN is a set of hosts connected via a link-layer switch (in the recent generation of Ethernet). A wireless isolated LAN, called an *adhocnetwork* in wireless LAN terminology, is a set of hosts that communicate freely with each other. The concept of a link-layer switch does notexistin wirelessLANs. Figure15.1 showstwo isolatedLANs, onewired andonewireless.

Connection to Other Networks

A wired LAN can be connected to another network or an internet work such as the Internet using a router. A wireless LAN may be connected to a wired infrastructure network, to a wireless infrastructure network, or to another wireless LAN. The first situation is the one that we discuss in this section: connection of a wireless LAN to a wired infrastructure network.


Isolated LANs: wired versus wireless


Connection of a wired LAN and a wireless LAN to other networks

2.10IEEE 802.11

IEEE has defined the specifications for a wireless LAN, called IEEE 802.11, which covers the physical and data-link layers. It is sometimes called *wireless Ethernet*.

In some countries, including the United States, the public uses the term *WiFi*(short for wireless fidelity) as a synonym for *wireless LAN*. WiFi, however, is a wireless LAN that is certified by the WiFi Alliance, a global, non profit industry association of more than 300 member companies devoted to promoting the growth of wirelessLANs.

Architecture

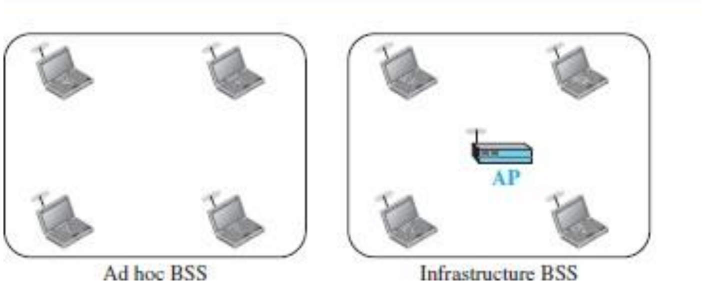
The standard defines two kinds of services: the basic service set(BSS) and the extended service set (ESS).

BasicServiceSet

IEEE 802.11 defines the basic service set (BSS) as the building blocks of a wireless LAN. Abasic service set is made of stationary or mobile wireless stations and an optional central basestation,known as the *accesspoint (AP)*. Figure15.4shows two sets inthisstandard.

The BSS without an AP is a stand-alone network and cannot send data to other BSSs. It is calledan *ad hoc architecture*. In this architecture, stations can form a network without the need of anAP; they can locate one another and agree to be part of a BSS. A BSS with an AP is sometimesreferredtoas an *infrastructure BSS*.

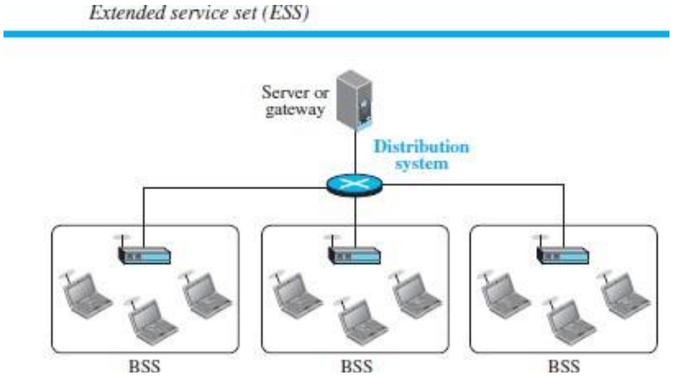
Basic service sets (BSSs)



ExtendedServiceSet

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 distributionsystem; it can be any IEEE LAN such as an Ethernet. Note that the extended service set uses twotypes of stations: mobile and stationary. The mobile stations are normal stations inside a BSS.ThestationarystationsareAP stations that arepart of awiredLAN.

When BSSs are connected, the stations within reach of one another can communicate without theuse of an AP. However, communication between a station in a BSS and the outside BSS occursvia the AP. The idea is similar to communication in a cellular network if we consider each BSS to be a cell and each AP to be a basestation.


Extended service set (ESS)

StationTypes

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** iseither stationary (not moving) or moving only inside a BSS. A station with **BSS-transitionmobility** can move from one BSS to another, but the movement is confined inside one ESS. Astationwith**ESS-transitionmobility**canmovefromoneESStoanother.However,IEEE 802.11doesnot guaranteethatcommunication iscontinuousduringthemove.

MACSublayer

IEEE 802.11 defines two MAC sublayers: the distributed coordination function (DCF) and pointcoordination function (PCF). Figure shows the relationship between the two MAC sublayers, theLLCsublayer, and the physical layer.

DistributedCoordinationFunction

OneofthetwoprotocolsdefinedbyIEEEattheMACsublayeriscalledthe***distributedcoordinationfunction (DCF)***. DCFuses CSMA/CA asthe access method

Frame Exchange TimeLine

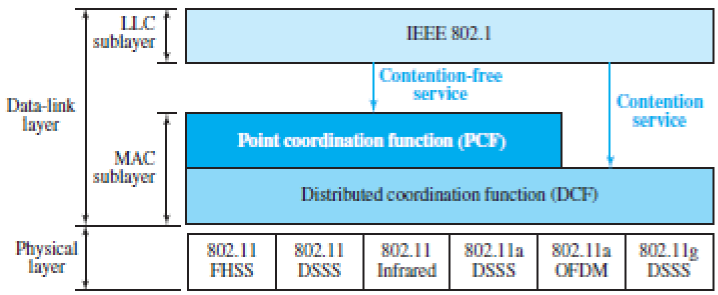
Figure shows the exchange of data and controlframes intime.

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 inter frame space(DIFS);*** then the station sends a control frame called the *request to send(RTS)*.

MAC layers in IEEE 802.11 standard

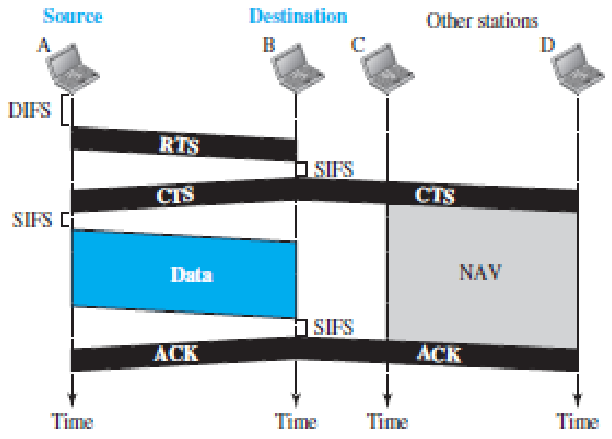


2. After receiving the RTS and waiting a period of time called the ***short interframe space(SIFS),*** the destination station sends a control frame, called the *clear to send (CTS)*, to the sourcestation.This control frame indicates that the destination station is readytoreceivedata.

3. The source stations ends 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 itsdata at the destination. On the other hand, the lack ofcollision in CSMA/CD is a kind of indication to the source that data have arrived.

CSMA/CA and NAV



NetworkAllocationVector

How do other stations defer sending their data if one station acquires access? In otherwords,how is the *collision avoidance* aspect of this protocol accomplished*?* The key is a feature calledNAV.

When a station sends an RTS frame, it includes the duration of time that it needs to occupy thechannel. The stations that are affected by this transmission create a timercalled a ***network allocation vector(NAV)*** that shows how much time must pass before these stations are allowed to check the channel for idleness. Each time a station accesses the system and sends an RTSframe, other stations start their NAV. In other words, each station, before sensing the physicalmedium to see if it is idle, first checks its NAV to see if it has expired. ***Collision DuringHandshaking*** What happens if there is a collision during the time when RTS or CTS control frames are intransition, often called the *handshaking period*? Two or more stations may try to send RTS frames at the same time. These control frames may collide. However,because there isnomechanism for collision detection, the sender assumes there has been a collision if it has notreceived a CTS frame from the receiver. The backoff strategy is employed, and the sender tries again.

Hidden-StationProblem

The solution to the hidden station problem is the use of the handshake frames (RTS and CTS).Figure also shows that the RTS message from B reaches A, but not C. However, because both BandCare within the range of A, the CTS message, which contains the duration of data transmission from B to A, reaches C. Station C knows that some hidden station is using the channel and refrains from transmitting until that duration is over.

2.11 Bluetooth

Bluetooth is a wireless LAN technology designed to connect devices of different functions suchas telephones, notebooks, computers (desktop and laptop), cameras, printers, and even coffeemakers when they are at a short distance from each other. A BluetoothLAN is an ad hocnetwork, which means that the network is formed spontaneously; the devices, sometimes calledgadgets, find each other and make a network called a piconet. A Bluetooth LAN can even beconnected to the Internet if one of the gadgets has this capability. A Bluetooth LAN, by nature,cannotbe large.If there aremanygadgetsthat tryto connect, thereischaos.

Bluetooth technology has several applications. Peripheral devices such as a wireless mouse orkeyboard can communicate with the computer through this technology. Monitoring devices cancommunicate with sensor devices in a small health care center. Home security devices can usethis technology to connect different sensors to the main security controller. Conference attendeescansynchronizetheirlaptop computers at a conference.

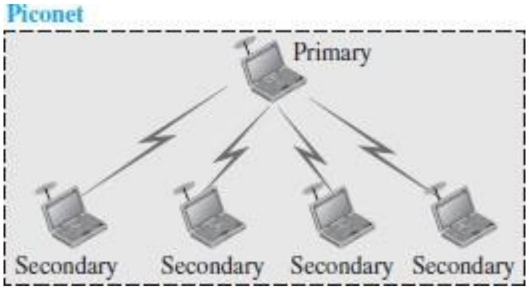
Bluetooth was originally started as a project by the Ericsson Company. It is named for Harald Blaatand, the king of Denmark(940-981)who united Denmark and Norway. *Blaatand* translates to *Bluetooth* in English. Today, Bluetooth technology is the implementation of a protocol definedby the IEEE 802.15 standard. The standard defines a wireless personal-area network (PAN)operablein an area the sizeof a room or a hall.

Architecture

Bluetooth defines two types of networks: piconet and scatternet.

Piconets

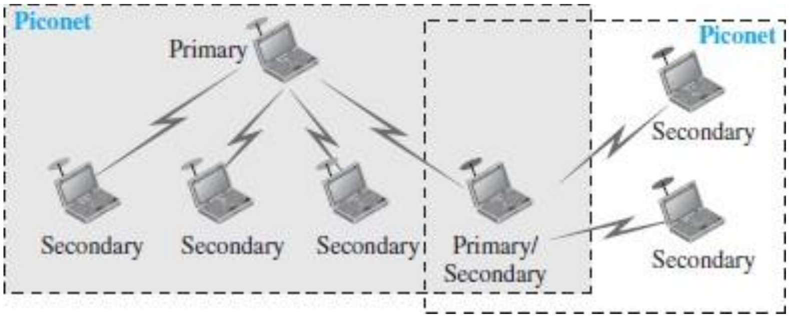
A Bluetooth network is called a ***piconet,*** or a smallnet. A piconet can have upto eightstations, one of which is called the *primary;* the rest are called *secondaries.* All the secondary stations synchronize their clocks and hopping sequence with the primary. Note that a piconet can have only one primary station. The ommunication 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. Because only eight stations can be active in a piconet, activating a station from the parked state means that an active station must goto the parked state.

Scatternet

Piconets can be combined to form what is called a ***scatternet.*** A secondary station in one piconetcan be the primary in another piconet. This station can receive messages from the primary in thefirst piconet (as a secondary) and, acting as a primary, deliver them to secondaries in the secondpiconet.A station can beamember oftwo piconets.

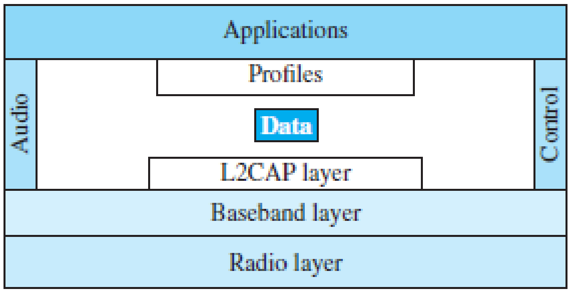


BluetoothDevices

A Bluetooth device has a built-in short-range radio transmitter. The current data rate is 1 Mbpswith a 2.4-GHz bandwidth. This means that there is a possibility of interference between theIEEE802.11b wirelessLANs and BluetoothLANs.

Bluetooth Layers

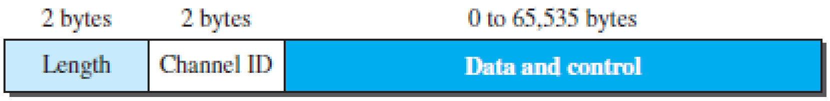
Bluetooth uses several layers that donot exactly match those of the Internet model.



L2CAP

The **Logical LinkControl andAdaptation Protocol,**or **L2CAP** (L2here meansLL),isroughly equivalent to the LLC sublayer in LANs. It is used for data exchange on an The 16-bitlength field defines the size of the data, in bytes, coming from the upper layers. Data can be up to65,535 bytes. The channel ID (CID) defines a unique identifier for the virtual channel created at this level.

L2CAP data packet format



The L2CAP has specific duties : multiplexing, segmentation and reassembly, quality of service(QoS), and group management.

Multiplexing

The L2CAP can do multiplexing. At the sender site, it accepts data from one of the upper-layerprotocols, frames them, and delivers them to the baseband layer. At the receiver site, it accepts aframe from the baseband layer, extracts the data, and delivers them to the appropriate protocollayer.

Segmentation and Reassembly

The maximum size of the payload field in the baseband layer is 2774 bits, or 343 bytes. Thisincludes 4 bytes to define the packet and packet length. Therefore, the size of the packet that canarrive from an upper layer can only be 339 bytes. However, application layers sometimes need tosend a data packet that can be up to 65,535 bytes (an Internet packet, for example). The L2CAPdivides these large packets into segments and adds extra information to define the location of the segments in the original packet. The L2CAP segments the packets at the source and reassembles thedestination.

QoS

Bluetooth allows the stations to define a quality-of-service level. For the moment, it is sufficientto know that if no quality-of-service level is defined, Bluetooth defaults to what is called *best-effort*service; it will do its best under thecircumstances.

2.12 ConnectingDevices(Hub,Repeater,Bridge,Switch,Router,GatewaysandBrouter)

1. **Repeater** – A repeater operates at the physical layer. Its job is to regenerate the signal over thesame network before the signal becomes too weak or corrupted so as to extend the length towhich the signal can be transmitted over the same network. An important point to be noted aboutrepeaters is that they do not amplify the signal. When the signal becomes weak, they copy the signal bit by bit and regenerate it at the original strength. It is a 2 port device.

2. Hub –A hub is basically a multiport repeater. A hub connects multiple wires coming fromifferent branches, for example, the connector in star topology which connects different stations.Hubs cannot filter data, so data packets are sent to all connected devices.In other words,collision domainof all hosts connected through Hub remains one.Also, they do not haveintelligence to find out best path for data packets which leads to inefficiencies and wastage.**TypesofHub**

- **Active Hub :-**These are the hubs which have their own power supply and can clean ,boost and relay the signal along the network. It serves both as a repeater as well as wiring center.Theseareused toextend maximum distancebetweennodes.
- **Passive Hub :-**These are the hubs which collect wiring from nodes and power supplyfrom active hub. These hubs relay signals onto the network without cleaning and boostingthemand can't beused to extend distancebetween nodes.

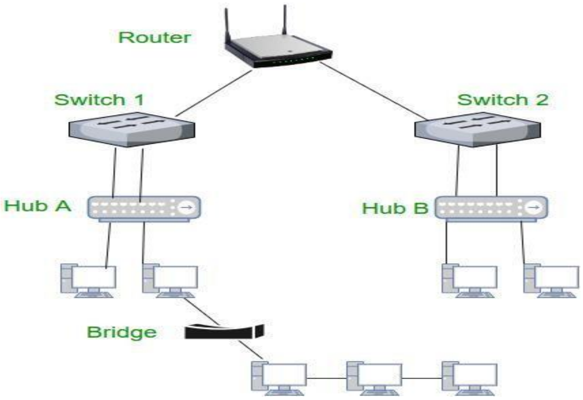
3. Bridge – A bridge operates at data link layer. A bridge is a repeater, with add on functionalityof filtering content by reading the MAC addresses of source and destination. It is also used forinterconnecting two LANs working on the same protocol. It has a single input and single outputport,thus makingit a2 port device.

TypesofBridges

- **Transparent Bridges :-**These are the bridge in which the stations are completely unaware of the bridge's existence i.e. whether or not a bridge is added or deleted from the network, reconfiguration of the stations is unnecessary. These bridges makes use of two processes i.e. bridge for warding and bridge learning.
- **Source Routing Bridges :-**In these bridges, routing operation is performed by source station and the frame specifies which route to follow. The hot can discover frame by sending a specical frame called discovery frame, which spreads through the entire network using all possible paths to destination.

4. **Switch** – A switch is a multi port bridge with a buffer and a design that can boost itsefficiency(large number of ports imply less traffic) and performance. Switch is data link layerdevice. Switch can perform error checking before forwarding data, that makes it very efficient asit does not forward packets that have errors and forward good packets selectively to correct port only.In other words, switch divides collision domain of hosts, but broadcast domain remains same.

5. **Routers** – A router is a device like a switch that routes data packets based on their IPaddresses.Router ismainly aNetworkLayerdevice.Routersnormally connectLANsandWANs togetherand have adynamically updating routing table basedon whichthey makedecisionsonrouting the data packets.Routerdivide broadcastdomainsof hostsconnectedthroughit.



6. **Gateway** – A gateway, as the name suggests, is a passage to connect two networks together that may work upon different networking models. They basically works as the messenger agents that take data from one system, interpret it, and transfer it to another system. Gateways are also called protocol converters and can operate at any network layer. Gateways are generally more complex than switch or router.

7. **Brouter**– It is also known as bridging router is a device which combines features of both bridge and router. It can work either at datalink layer or at network layer. Working as router, it is capable of routing packets across networks and working as bridge, it is capable of filtering local area network traffic.