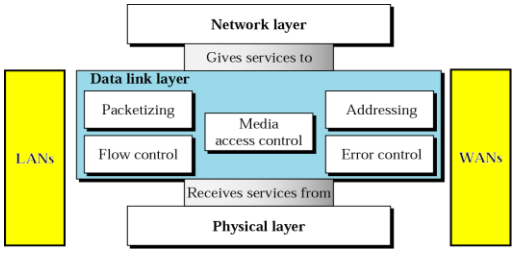
Data Link Layer

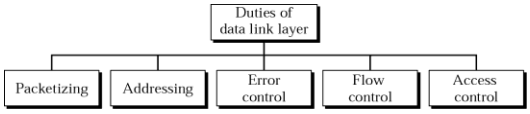
Learning Objectives

- To introduce the design issues of data link layer.
- To discuss different error control methods and flow control protocols
- To discuss protocols of medium access control sublayer
- To discuss Ethernet and Wireless Lan's s
- To discuss Bluetooth

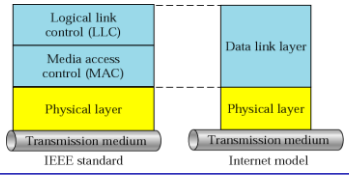
Position of the data-link layer



Data Link Layer Duties



LLC and MAC Sublayers



The data link control is responsible for reliable transmission of message over transmission channel by using techniques like framing, error control and flow control.

MAC sub layer is required if there is no dedicated link present then multiple stations can access the channel simultaneously. Hence multiple access protocols are required to decrease collision and avoid crosstalk.

Topics

Error Detection and Correction

Data Link Control and Protocols

Multiple Access

Local Area Networks

Wireless LANs

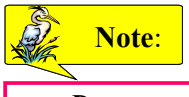
Switching

Error Detection and Correction

Learning Objectives

- To introduce the types of errors.
- To discuss different error detection methods.
- To discuss parity check, CRC and checksum.
- To discuss different error detection methods.

Cont ....



Data can be corrupted during transmission. For reliable communication, errors must be detected and corrected.

Types of Error

Single-Bit Error

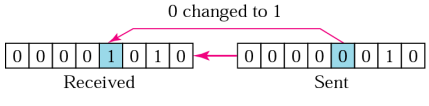
Burst Error

Cont ....

Note:

In a single-bit error, only one bit in the data unit has changed.

Single-Bit Error

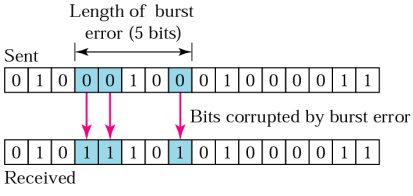


Cont ....

Note:

A burst error means that 2 or more bits in the data unit have changed.

Burst Error of Length 5



The length of the burst error is measured from the first corrupted bit to the last corrupted bit. Some bits in between may not be corrupted.

Detection

Redundancy

Parity Check

Cyclic Redundancy Check (CRC)

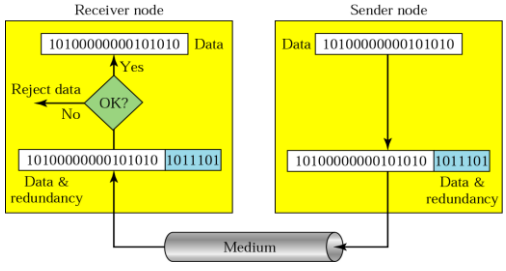
Checksum

Cont ....

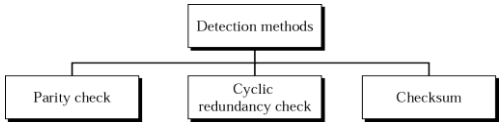
Note:

Error detection uses the concept of redundancy, which means adding extra bits for detecting errors at the destination.

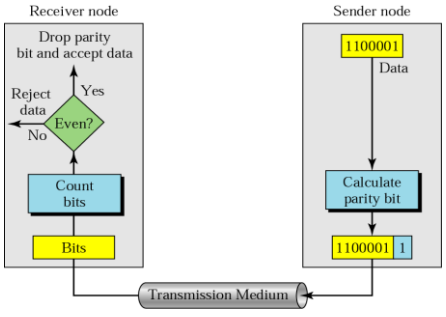
Redundancy



Detection Methods



Even-Parity Concept



Cont ....

Note:

In parity check, a parity bit is added to every data unit so that the total number of 1s is even (or odd for odd-parity).

Cont ....

Note:

Simple parity check can detect all single-bit errors. It can detect burst errors only if the total number of errors in each data unit is odd.

Cont ....

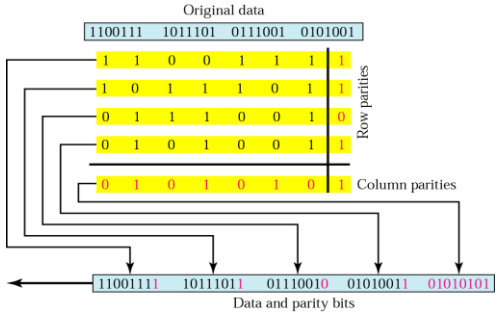
Let Sender sends data 10110, to make it even parity sender send the data 10110 1

Now, Receiver receives 01110 1,

The receiver will accept this data

Thus, errors in more than one bit cannot be detected with single parity bit.

Two-Dimensional Parity



Cont ....

Note:

In two-dimensional parity check, a block of bits is divided into rows and a redundant row of bits is added to the whole block.

Cont ....

Let Sender sends data 11001100 and 10101100.

11001100	**0**
10101100	0
01100000	0

If first bit and second from last bits in each of them is changed, making the data units as 01001110 and 00101110.

01001110	**0**
00101110	0
01100000	0

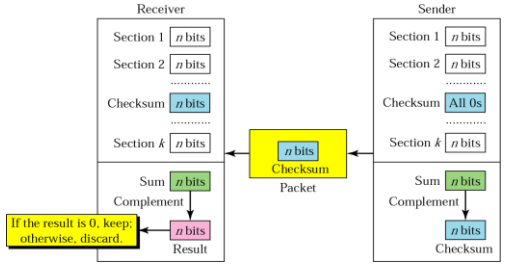
The receiver will accept this data

Cont ....

Note:

If two bits in one data unit are damaged and two bits in exactly same position in another data unit are also damaged, the 2-D Parity check checker will not detect an error.

Checksum



Cont ....

Note:

The sender follows these steps:

- *The unit is divided into k sections, each of n bits.*
- *All sections are added using one's complement to get the sum.*
- *The sum is complemented and becomes the checksum.*
- *The checksum is sent with the data.*

Cont ....

Note:

The receiver follows these steps:

- *The unit is divided into k sections, each of n bits.*
- *All sections are added using one's complement to get the sum.*
- *The sum is complemented.*
- *If the result is zero, the data are accepted: otherwise, rejected.*

Cont ....

Example:

k=4, m=8

```
  10110011
  10101011
 ↶ 01011110
         1
  01011111
  01011010
  10111001
  11010101
 ↶ 10001110
         1
  10001111
  01110000
```

Sum :
Checksum

Sender

Example: Received data

```
  10110011
  10101011
 ↶ 01011110
         1
  01011111
  01011010
  10111001
  11010101
 ↶ 10001110
         1
  10001111
  01110000
```

Sum: 11111111

Complement = 00000000

Conclusion = Accept data

Receiver

Cont ....

Suppose the following block of 16 bits is to be sent using a checksum of 8 bits.

10101001 00111001

The numbers are added using one's complement

10101001
00111001

Sum 11100010

Checksum **00011101**

The pattern sent is 10101001 00111001 **00011101**

Cont ....

Now suppose the receiver receives the pattern sent and there is no error.

10101001 00111001 00011101

When the receiver adds the three sections, it will get all 1s, which, after complementing, is all 0s and shows that there is no error.

10101001
00111001
00011101
Sum 11111111

Complement 00000000 means that the pattern is OK.

Cont ....

Now suppose there is a burst error of length 5 that affects 4 bits.

10101**111 11**111001 00011101

When the receiver adds the three sections, it gets

10101111
11111001
00011101
Partial Sum **1** 11000101

Carry **1**

Sum 11000110

Complement **00111001 the pattern is corrupted**.

Cont ....

The checksum detects all errors on odd number of bits.

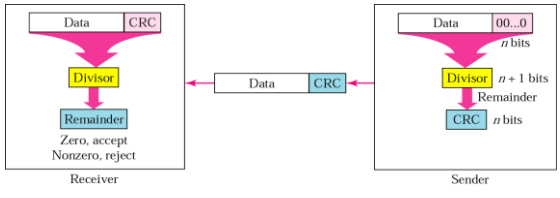
It detects most errors on even no of bits.

But, If one or more bits of a segment is damaged and the bits of opposite value at same position in second segment is also damaged, then the sum of the column is not changed, and receiver will not detect the error.

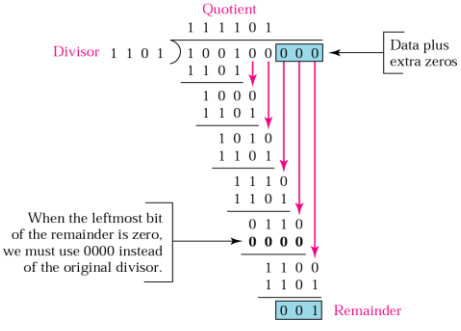
Sender	
	11001100
	10101100
Add	01111000
Add carry	1
Sum=	01111001
Check sum	10000110

Receiver	
	10101100
	11001100
Add	01111000
Add carry	1
Sum=	01111001
Check sum	10000110

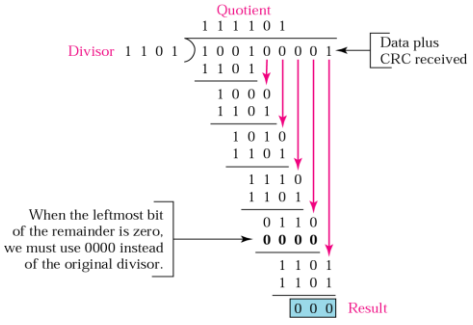
CRC Generator and Checker



Binary Division in a CRC



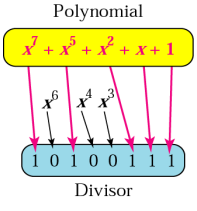
Binary division in CRC checker



A polynomial

$$x^7 + x^5 + x^2 + x + 1$$

A Polynomial Representing a Divisor



A Polynomial Representing a Divisor

- All the values can be expressed as polynomials of a dummy variable X.
- For example, for P = 11001 the corresponding polynomial is X^4+X^3+1.
- A polynomial is selected to have at least the following properties:
  - It should not be divisible by X.
  - It should not be divisible by (X+1).

A Polynomial Representing a Divisor

- Commonly used divisor polynomials are:
  - CRC-16 = $X^{16} + X^{15} + X^2 + 1$
  - CRC-CCITT = $X^{16} + X^{12} + X^5 + 1$
  - CRC-32 = $X^{32} + X^{26} + X^{23} + X^{22} + X^{16} + X^{12} + X^{11} + X^{10} + X^8 + X^7 + X^5 + X^4 + X^2 + 1$

Name	Polynomial	Application
CRC-8	x^8+x^2+x+1	ATM header
CRC-10	$x^{10}+x^9+x^5+x^4+x^2+1$	ATM AAL
ITU-16	$x^{16}+x^{12}+x^5+1$	HDLC
ITU-32	$x^{32}+x^{26}+x^{23}+x^{22}+x^{16}+x^{12}+x^{11}+x^{10}+x^8+x^7+x^5+x^4+x^2+x+1$	LANs

CRC Performance

- CRC is a very effective error detection technique.
- If the divisor is chosen according to the previously mentioned rules, its performance can be summarized as follows:
  - ✓ CRC can detect all single-bit errors
  - ✓ CRC can detect all double-bit errors
  - ✓ CRC can detect any odd number of errors
  - ✓ CRC can detect all burst errors of less than the degree of the polynomial.
  - ✓ CRC detects most of the larger burst errors with a high probability.
  - ✓ For example, CRC-12 detects 99.97% of errors with a length 12 or more.

Error Correction

- The techniques that we have discussed so far can detect errors, but do not correct them.
- Error Correction can be handled in two ways.
  - Backward Error Correction: when an error is discovered; the receiver can have the sender retransmit the entire data unit.
  - Forward Error Correction: Receiver can use an error-correcting code, which automatically corrects certain errors

Error Correction

- Error-correcting codes are more sophisticated than error detecting codes and require more redundant bits
- The number of bits required to correct multiple-bit or burst error is so high that in most of the cases it is inefficient to do so.
- For this reason, most error correction is limited to one, two or at the most three-bit errors.

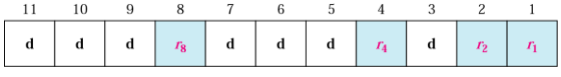
Error Correction: Signal Bit Error Correction

- A single-bit error can be detected by addition of a parity bit (VRC) with the data, which needed to be sent.
- A single additional bit can detect error, but it's not sufficient to correct that error too.
- For correcting an error, one has to know the exact position of error, i.e., exactly which bit is in error
- To this, we must add some additional redundant bits.

Error Correction: Signal Bit Error Correction

- A technique developed by *R. W. Hamming* provides a practical solution.
- The solution or coding scheme he developed is commonly known as Hamming Code.
- Hamming code can be applied to data units of any length and uses the relationship between the data bits and redundant bits.

Positions of Redundancy Bits



Positions of Redundancy Bits

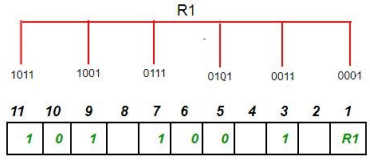
- The number of redundant bits can be calculated using the following formula:

$2^r >= m+r+1$ Where m= data bit and r=redundant bit

- Suppose the number of data bits is 7, then the number of redundant bits can be calculated using:
  = 2^4 ≥ 7 + 4 + 1
  Thus, the number of redundant bits= 4
- **Determining the position of redundant bits**
  - These redundancy bits are placed at the positions which correspond to the power of 2.

Positions of Parity Bits

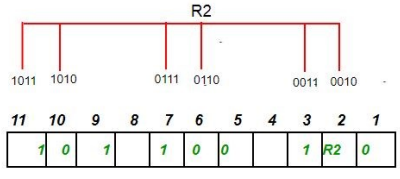
- R1 bit is calculated using parity check at all the bits positions whose binary representation includes a 1 in the least significant position.



https://www.geeksforgeeks.org/hamming-code-in-computer-network/

Positions of Parity Bits

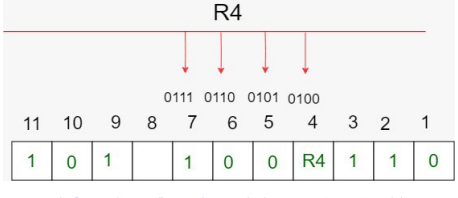
- R2 bit is calculated using parity check at all the bits positions whose binary representation includes a 1 in the second position from the least significant bit.



https://www.geeksforgeeks.org/hamming-code-in-computer-network/

Positions of Parity Bits

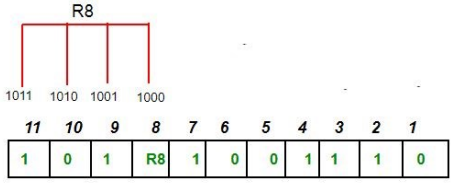
- R4 bit is calculated using parity check at all the bits positions whose binary representation includes a 1 in the third position from the least significant bit. R4: bits 4, 5, 6, 7



https://www.geeksforgeeks.org/hamming-code-in-computer-network/

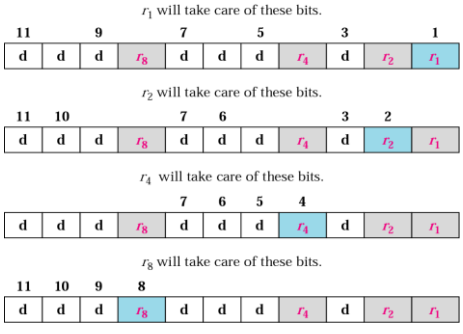
Positions of Parity Bits

- R8 bit is calculated using parity check at all the bits positions whose binary representation includes a 1 in the fourth position from the least significant bit.

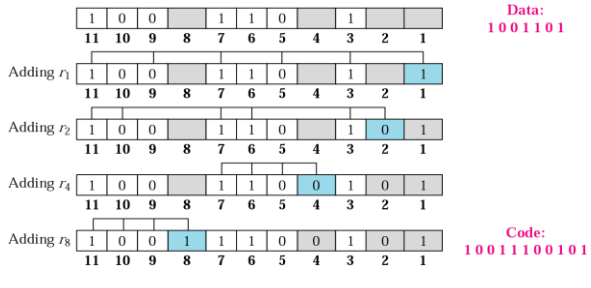


https://www.geeksforgeeks.org/hamming-code-in-computer-network/

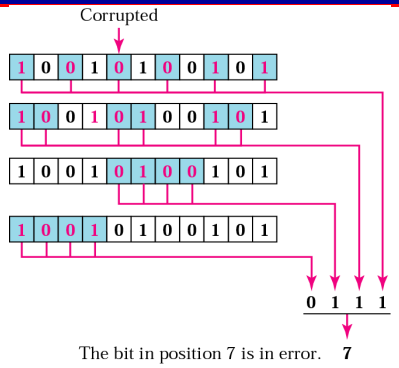
Redundancy Bits Calculation



Example of Redundancy



Error Detection using Hamming



Conclusion

- Errors can be single bit or burst errors
- Three common redundancy methods are parity check, CRC and checksum
- Errors can be corrected by retransmission
- Hamming code is error correction through retransmission

Topic

Flow Control Protocols

Learning Objectives

- To introduce the protocols for error and flow control.
- To discuss Stop and wait, Go back N and selective repear ARQ
- To discuss concept of piggybacking and pipelining
- To discuss HDLC protocol and its various frames

Cont ....

Note:

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

Cont ....

Note:

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

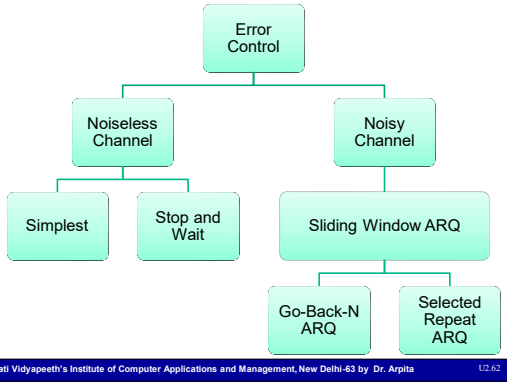
Cont ....

Error Control Techniques

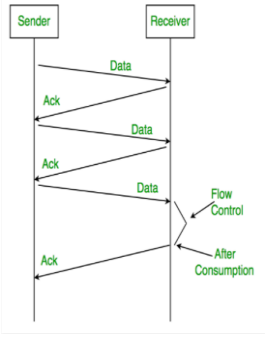
When an error is detected in a message, the receiver sends a request to the transmitter to retransmit the ill-fated message or packet.

The most popular retransmission scheme is known as Automatic-Repeat-Request (ARQ). Such schemes, where receiver asks transmitter to re-transmit if it detects an error, are known as reverse error correction techniques.

Cont ....

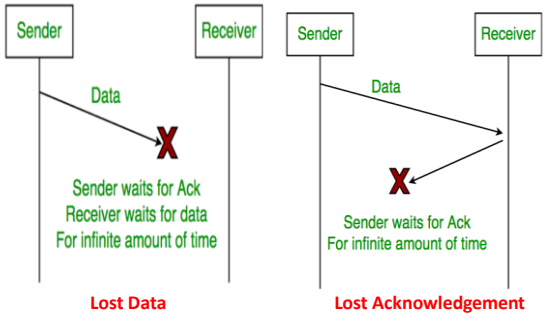


Stop-and-Wait



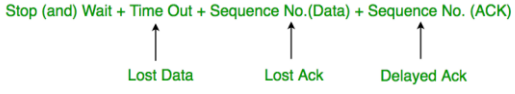
- **Sender:**
  - Send one data frame at a time.
  - Send the next frame only after receiving acknowledgement for the previous.
- **Receiver:**
  - Send acknowledgement after receiving and consuming a data packet.
  - After consuming frame acknowledgement need to be sent (Flow Control)

Stop-and-Wait: Problems



Stop-and-Wait: Problems

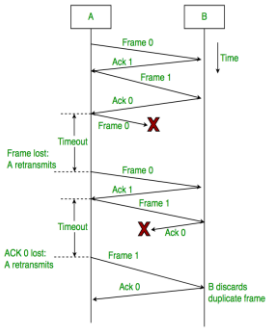
- **Delayed Acknowledgement/Data:**
  - After a timeout on the sender side, a long-delayed acknowledgement might be wrongly considered as acknowledgement of some other recent packet.
- The solution of all three problems is given by Stop-and-Wait ARQ (Automatic Repeat Request)



Automatic Repeat Request

- **Automatic Repeat Request**
- The most common techniques for error correction are based on some or all the following principles.
  - Error detection
  - Positive acknowledgement
  - Retransmission after time-out
  - Negative acknowledgement and retransmission
- Collectively these mechanisms are all referred to as Automatic Repeat Request (ARQ)

Stop-and-Wait ARQ



- Sender A sends a data frame or packet with sequence number 0.
- Receiver B, after receiving the data frame, sends an acknowledgement with sequence number 1 (the sequence number of the next expected data frame or packet)
- There is only a one-bit sequence number that implies that both sender and receiver have a buffer for one frame or packet only.

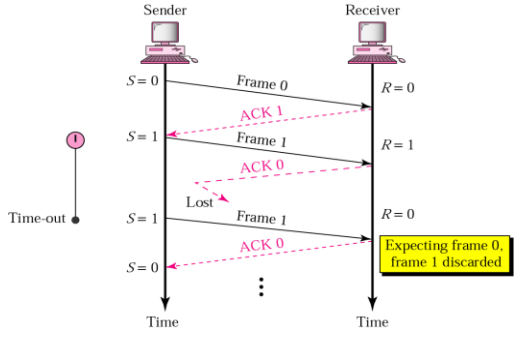
Cont ....

In Stop-and-Wait ARQ, which is simplest among all protocols, the sender (say station A) transmits a frame and then waits till it receives positive acknowledgement (ACK) or negative acknowledgement (NACK) from the receiver (say station B).

Station B sends an ACK if the frame is received correctly, otherwise it sends NACK.

Station A sends a new frame after receiving ACK; otherwise it retransmits the old frame, if it receives a NACK.

Stop-and-Wait ARQ, Lost ACK

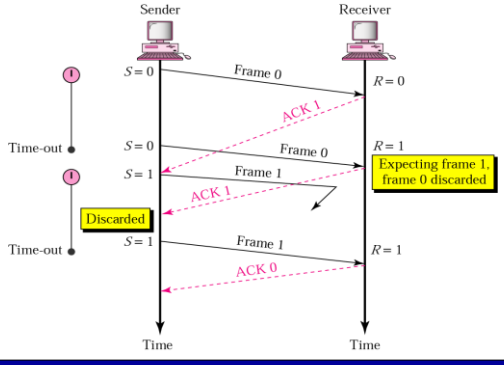


Cont ....

Note:

In Stop-and-Wait ARQ, numbering frames prevents the retaining of duplicate frames.

Stop-and-Wait , Delayed ACK



Cont ....

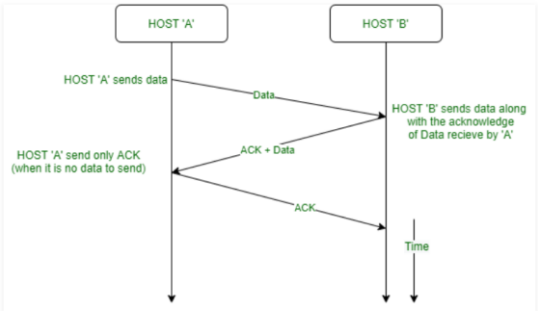
Note:

Numbered acknowledgments are needed if an acknowledgment is delayed and the next frame is lost.

Cont ....

- The Stop and Wait ARQ solves the main three problems but may cause big performance issues as the sender always waits for acknowledgement even if it has the next packet ready to send.
- Stop and Wait ARQ may work fine where propagation delay is very less for example LAN connections
- But, performs badly for distant connections like satellite connections.
- Poor Bandwidth Utilization
- One Frame at a time

Piggy Backing



Cont ....

What is piggybacking? What is its advantage?

In practice, the link between receiver and transmitter is full duplex and usually both transmitter and receiver stations send data to each over.

So, instead of sending separate acknowledgement packets, a portion (few bits) of the data frames can be used for acknowledgement. This phenomenon is known as piggybacking.

The piggybacking helps in better channel utilization. Further, multi-frame acknowledgement can be done.

Cont ....

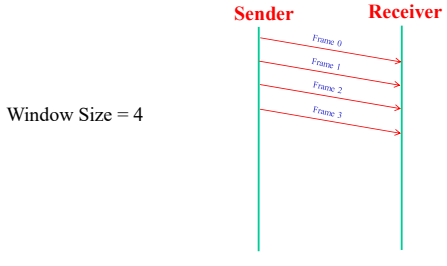
- **Advantages of piggybacking :**
  - Better use of available channel bandwidth. This happens because an acknowledgment frame needs not to be sent separately.
  - Usage cost reduction
  - Improves latency of data transfer

- **Disadvantages of piggybacking :**
  - The disadvantage of piggybacking is the additional complexity.
  - If the data link layer waits long before transmitting the acknowledgment (block the ACK for some time), the frame will rebroadcast.

Sliding Window ARQ

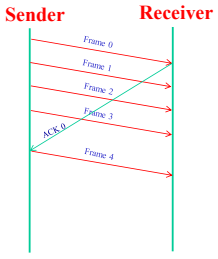
- Sliding Window protocol sends more than one packet at a time with a larger sequence number.
- Number of frames that can be sent at a time is called Window Size.
- Once sender receives the Ack for packet 0, window slides and the next packet can be assigned sequence number 0.
- Sequence numbers are reused so that so that header size can be kept minimum.
  - *Don't confuse with frame number and Sequence number*

Sliding Window ARQ



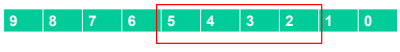
Sliding Window ARQ

Window Size = 4

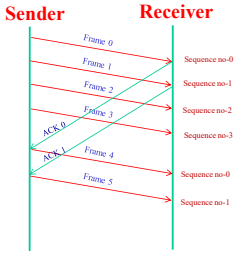


 U2.79

Sliding Window ARQ



Window Size = 4



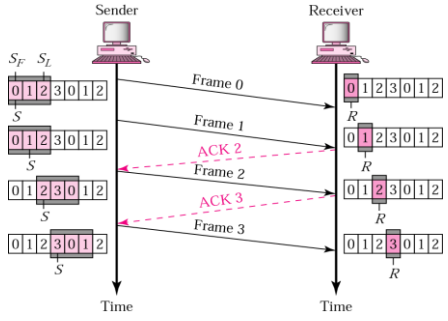
 U2.80

Go-Back-N

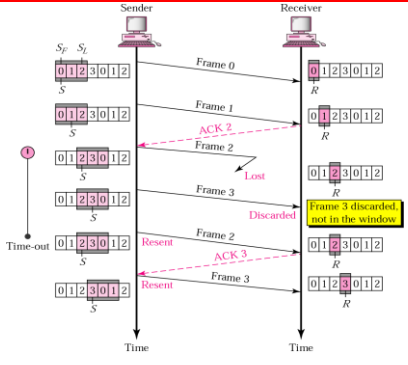
- The most popular ARQ protocol is the go-back-N ARQ, where the sender sends the frames continuously without waiting for acknowledgement.
- That is why it is also called as *continuous ARQ*. As the receiver receives the frames, it keeps on sending ACKs or a NACK, in case a frame is incorrectly received.
- When the sender receives a NACK, it retransmits the frame in error plus all the succeeding frames as shown in Fig..
- Hence, the name of the protocol is go-back-N ARQ. If a frame is lost, the receiver sends NAK after receiving the next frame

 U2.81

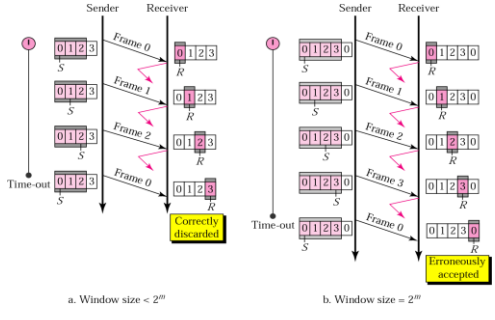
Go-Back-N , Normal Operation



Go-Back-N , Lost Frame



Go-Back-N : Sender Window Size



a. Window size < 2^m b. Window size = 2^m

m= No of bits allowed in header

Cont ....

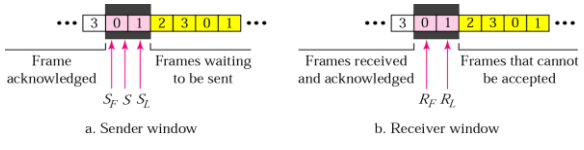
Note:

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

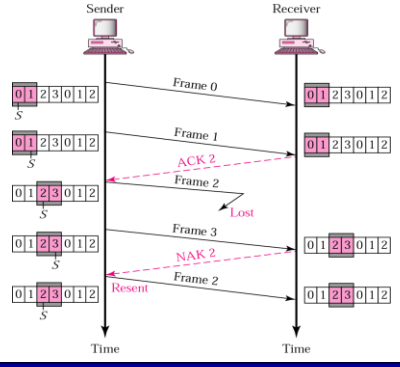
Selective Repeat

- The selective-repetitive ARQ scheme retransmits only those for which NAKs are received or for which timer has expired, this is shown in the Fig
- This is the most efficient among the ARQ schemes, but the sender must be more complex so that it can send out-of-order frames.
- The receiver also must have storage space to store the post-NAK frames and processing power to reinsert frames in proper sequence.

Selective Repeat



Selective Repeat , Lost Frame

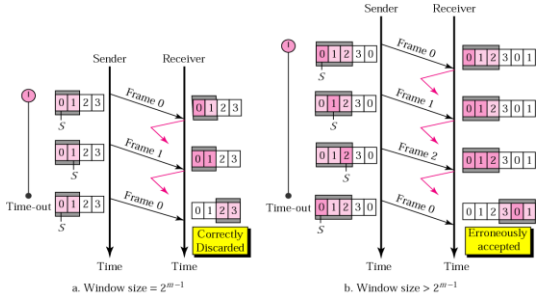


Cont ....

Note:

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

Selective Repeat



Selective Repeat

How the inefficiency of Stop-and-Wait protocol is overcome in sliding window protocol?

- The Stop-and-Wait protocol is inefficient when large numbers of small packets are sent by the transmitter since the transmitter has to wait for the acknowledgement of each individual packet before sending the next one.
- This problem can be overcome by sliding window protocol. In sliding window protocol multiple frames (up to a fixed number of frames) are send before receiving an acknowledgement from the receiver.

 U2.91

Switching

- When there are many devices, it is necessary to develop suitable mechanism for communication between any two devices.
- In the switched network methodology, the network consists of a set of interconnected nodes, among which information is transmitted from source to destination via different routes, which is controlled by the switching mechanism.

 U2.92

Switching

- The end devices that wish to communicate with each other are called stations. The switching devices are called nodes. Some nodes connect to other nodes and some are to connected to some stations.
- The switching performed by different nodes can be categorized into the following three types:
  - Circuit Switching
  - Packet Switching
  - Message Switching

 U2.93

Circuit Switching

- Communication via circuit switching implies that there is a dedicated communication path between the two stations.
- The path is a connected through a sequence of links between network nodes.
- On each physical link, a logical channel is dedicated to the connection.
- Circuit switching is commonly used technique in telephony, where the caller sends a special message with the address of the callee (i.e. by dialing a number) to state its destination.

Circuit Switching

It involved the following three distinct steps:

Circuit Establishment: *To establish an end-to-end connection before any transfer of data.*

Some segments of the circuit may be a dedicated link, while some other segments may be shared.

Data transfer:

- Transfer data is from the source to the destination.
- The data may be analog or digital, depending on the nature of the network.
- The connection is generally full-duplex.

Circuit Switching

Circuit disconnect:

- Terminate connection at the end of data transfer.
- Signals must be propagated to deallocate the dedicated resources.

Thus the actual physical electrical path or circuit between the source and destination host must be established before the message is transmitted.

This connection, once established, remains exclusive and continuous for the complete duration of information exchange and the circuit becomes disconnected only when the source wants to do so.

Message Switching

- In this switching method, a different strategy is used, where instead of establishing a dedicated physical line between the sender and the receiver, the message is sent to the nearest directly connected switching node.
- This node stores the message, checks for errors, selects the best available route and forwards the message to the next intermediate node.

Message Switching

The line becomes free again for other messages, while the process is being continued in some other nodes.

Due to the mode of action, this method is also known as *store-and-forward technology where the message hops from node to node to its final destination. Each node stores the full message, checks for errors and forwards it.*

In this switching technique, more devices can share the network bandwidth, as compared with circuit switching technique.

Message Switching

Temporary storage of message reduces traffic congestion to some extent.

Higher priority can be given to urgent messages, so that the low priority messages are delayed while the urgent ones are forwarded faster.

Through broadcast addresses one message can be sent to several users.

Last of all, since the destination host need not be active when the message is sent, message switching techniques improve global communications.

Message Switching

- Each network node receives and stores the message
- Determines the next leg of the route, and
- Queues the message to go out on that link.

Advantages:

- Line efficiency is greater (sharing of links).
- Data rate conversion is possible.
- Even under heavy traffic, packets are accepted, possibly with a greater delay in delivery.
- Message priorities can be used, to satisfy the requirements, if any.

Disadvantages:

- Message of large size monopolizes the link and storage

 U2.100

Packet Switching

- The basic approach is not much different from message switching. It is also based on the same 'store-and-forward' approach. However, to overcome the limitations of message switching, messages are divided into subsets of equal length called *packets.*
- In packet switching approach, data are transmitted in short packets (few Kbytes). A long message is broken up into a series of packets

 U2.101

Packet Switching

- Main difference between Packet switching and Circuit Switching is that the communication lines are not dedicated to passing messages from the source to the destination.
- In Packet Switching, different messages (and even different packets) can pass through different routes, and when there is a "dead time" in the communication between the source and the destination, the lines can be used by other sources.

 U2.102

Packet Switching

- Main difference between Packet switching and Circuit Switching is that the communication lines are not dedicated to passing messages from the source to the destination.
- In Packet Switching, different messages (and even different packets) can pass through different routes, and when there is a "dead time" in the communication between the source and the destination, the lines can be used by other sources.

 U2.103

Packet Switching

- There are two basic approaches commonly used to packet Switching: **virtual-circuit packet switching and datagram packet switching.**
- In virtual-circuit packet switching a virtual circuit is made before actual data is transmitted, but it is different from circuit switching in a sense that in circuit switching the call accept signal comes only from the final destination to the source while in case of virtual-packet switching this call accept signal is transmitted between each adjacent intermediate node

 U2.104

Packet Switching

- There are two basic approaches commonly used to packet Switching: **virtual-circuit packet switching and datagram packet switching.**
- In virtual-circuit packet switching a virtual circuit is made before actual data is transmitted, but it is different from circuit switching in a sense that in circuit switching the call accept signal comes only from the final destination to the source while in case of virtual-packet switching this call accept signal is transmitted between each adjacent intermediate node

 U2.105

Packet Switching

- An initial setup phase is used to set up a route between the intermediate nodes for all the packets passed during the session between the two end nodes.
- In each intermediate node, an entry is registered in a table to indicate the route for the connection that has been set up.
- Thus, packets passed through this route, can have short headers, containing only a *virtual circuit identifier (VCI), and not their destination.*
- *Each intermediate node passes the packets according to the information that was stored in it, in the setup phase.*

 U2.106

Packet Switching

Datagram Packet Switching Networks

- This approach uses a different, more dynamic scheme, to determine the route through the network links.
- Each packet is treated as an independent entity, and its header contains full information about the destination of the packet.
- The intermediate nodes examine the header of the packet, and decide to which node to send the packet so that it will reach its destination.

 U2.107

Packet Switching

- Thus, in this method, the packets don't follow a pre-established route, and the intermediate nodes (the routers) don't have pre-defined knowledge of the routes that the packets should be passed through.
- Packets can follow different routes to the destination, and delivery is not guaranteed (although packets usually do follow the same route, and are reliably sent).

 U2.108

Packet Switching

- Due to the nature of this method, the packets can reach the destination in a different order than they were sent, thus they must be sorted at the destination to form the original message.
- This approach is time consuming since every router has to decide where to send each packet.
- The main implementation of Datagram Switching network is the Internet, which uses the IP network protocol.

Packet Switching

Advantages :

- Call setup phase is avoided (for transmission of a few packets, datagram will be faster).
- Because it is more primitive, it is more flexible.
- Congestion/failed link can be avoided (more reliable).

Problems:

- Packets may be delivered out of order.
- If a node crashes momentarily, all of its queued packets are lost.

Switching

Circuit Switching	Datagram Packet	Virtual Circuit Packet
Dedicated path	No dedicated path	No dedicated path
Path established for entire conversation	Route established for each packet	Route established for entire conversation
Call set up delay	Packet transmission delay	Call set up delay, Packet transmission delay
Overload may block call set up	Overload increases packet delay	Overload may block call set up and increases packet delay
No speed or code conversion	Speed or code conversion	Speed or code conversio
Fixed bandwidth	Dynamic bandwidth	Dynamic bandwidth
No overhead bits after call set up	Overhead bits in each packet	Overhead bits in each packet

TOPIC

Multiple Access

Channel Allocation Problem

- Channel allocation is a process in which a single channel is divided and allotted to multiple users in order to carry user specific tasks.
- If there are N number of users and channel is divided into N equal-sized sub channels, Each user is assigned one portion.
- When multiple users use a shared network and want to access the same network. Then channel allocation problem in computer networks occurs.

Channel Allocation Problem

- To allocate the same channel between multiple users, different Channel Allocation Techniques are used.
  - Static channel allocation
  - Dynamic Channel Allocation
  - Hybrid Channel Allocation

Static Channel Allocation

- It is the classical or traditional approach of allocating a single channel
- Frequency Division Multiplexing (FDM) or Time Division Multiplexing is used.
- If there are N users, the bandwidth is divided into N equal sized portions.
- Each user is assigned one portion.
- No interface between users

Dynamic Channel Allocation

- The technique in which channels are not permanently allocated to the users is called dynamic channel allocation.
- The allocation depends upon the traffic.
- This technique optimizes bandwidth usage and provides fast data transmission.
- There are two approaches
  - Centralized dynamic channel allocation
  - Distributed dynamic channel allocation

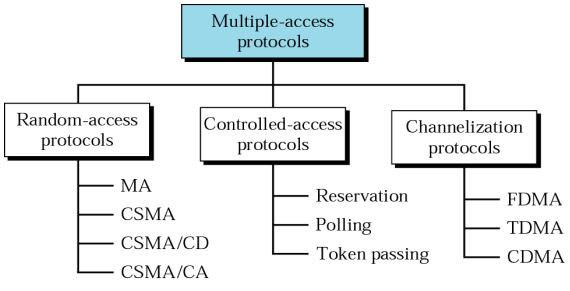
Assumptions in Dynamic Channel Allocation

- **Station Model:** N independent stations with a program for transmission.
- **Single Channel:** A single channel is available for all communication.
- **Collision:** If frames are transmitted at the same time by two or more stations, then the collision occurs.
- **Continuous or slotted time:** There is no master clock that divides time into discrete time intervals.
- **Carrier Sense:** Stations sense the channel before transmission.

Hybrid Channel Allocation

- The mixture of fixed channel allocation and dynamic channel allocation is called **Hybrid Channel Allocation**.
- The total channels are divided into two sets, fixed and dynamic sets.
- A fixed set of channels is used when the user makes a call.
- If all fixed sets are busy, then dynamic sets are used.
- When there is heavy traffic in a network, then hybrid channel allocation is used.

Multiple-Access Protocols



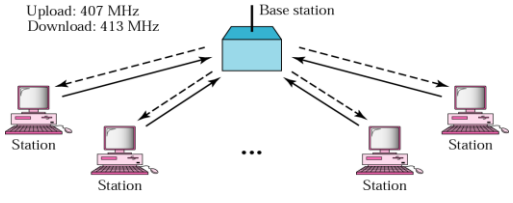
Random Access

- In random access or contention methods, no station is superior to another station and none is assigned the control over another.
- No station permits, or does not permit, another station to send.
- The decision to send data depends on the state of the medium (busy or idle).
- In random access method, each station has the right to the medium without being controlled by any other station.
- However, if more than one station tries to send, there is an access conflict- collision- and the frames will be either destroyed and modified.

Random Access

- Followings are the major concern to implement the random access protocols
  - When can a station access the medium?
  - If the channel is busy, what will station do?
  - How can a station decide the success or failure of the transmission?
  - What can be done if there is access conflict?

ALOHA Network



ALOHA Network

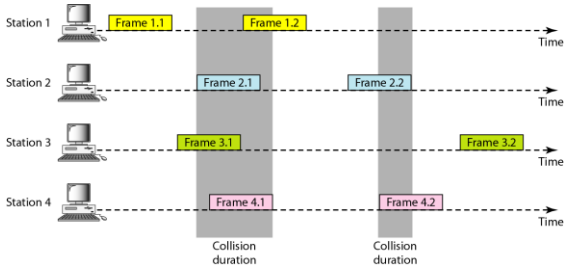
- The ALOHA scheme was invented by Abramson in 1970 for a packet radio network connecting remote stations to a central computer and various data terminals at the campus of the university of Hawaii.
- It was designed for a radio (Wireless LAN) , but it can be used on any shared medium.
- Users are allowed random access of the central computer through a common radio frequency band *f1* and the computer centre broadcasts all received signals on a different frequency band *f2*.

ALOHA network

Pure ALOHA

- The original ALOHA protocol is called pure ALOHA.
- The idea is that each station sends a frame whenever it has a frame to send.
- However, since there is only one channel to share, there is the possibility of collision between frames from different stations.
- If one bit of a frame coexists on the channel with one bit from another frame, there is collision, and both will be destroyed.

ALOHA Network



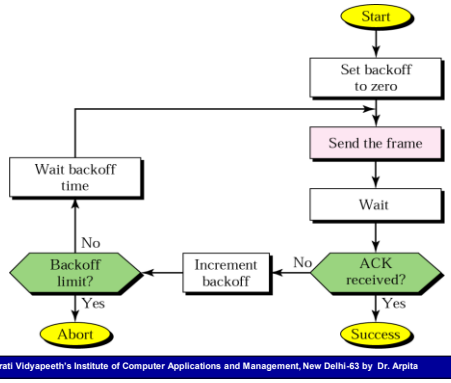
ALOHA Network

- The pure ALOHA protocol relies on acknowledgment from the receiver.
- When a station sends a frame, it expects the receiver to send an acknowledgement .
- If the acknowledgment does not arrive after a time-out period, the station assumes that the frame has been destroyed and resends the frame.

ALOHA network

- A collision involves two or more stations.
  - If all these stations try to resend their frames after the time-out, the frame will collide again.
  - Pure ALOHA dictates that when the time-out period passes, each station waits a random amount of time before resending its frame.
  - The randomness will help avoid more collisions.
  - We call this time the back-off time.

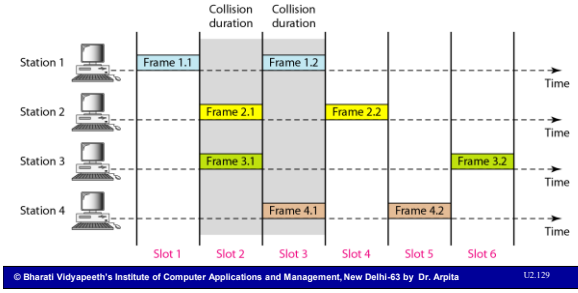
Procedure for ALOHA protocol



ALOHA Network

Slotted ALOHA

In slotted ALOHA, we divide the time into slots and force the station to send only at the beginning of the time slot.



Pure Aloha Vs Slotted Aloha

Pure Aloha	Slotted Aloha
In this aloha, any station can transmit the data at any time.	In this, any station can transmit the data at the beginning of any time slot.
In this, The time is continuous and not globally synchronized.	In this, The time is discrete and globally synchronized.
Vulnerable time for pure aloha = 2 x Tt	Vulnerable time for Slotted aloha = Tt
In Pure Aloha, Probability of successful transmission of data packet= G x e^{-2G} , *where G is number of stations wants to transmit in Tt slot*	In Slotted Aloha, Probability of successful transmission of data packet= G x e^{-G} , *where G is number of stations wants to transmit in Tt slot*
In pure aloha, Maximum efficiency= 18.4%	In slotted aloha, Maximum efficiency= 36.8%
Pure aloha doesn't reduces the number of collisions to half.	Slotted aloha reduces the number of collisions to half and doubles the efficiency of pure aloha.

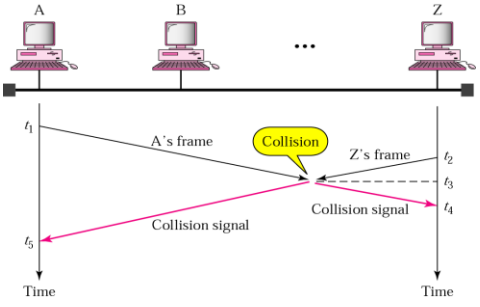
CSMA

- CSMA: Carrier Sense Multiple Access
- The poor efficiency of the ALOHA scheme can be attributed to the fact that a node start transmission without paying any attention to what others are doing.
- Carrier Sense multiple access requires that each station first check the state of the medium before sending.

CSMA

- In this scheme, a node having data to transmit first listens to the medium to check whether another transmission is in progress or not.
- The node starts sending only when the channel is free, that is there is no carrier.
- That is why the scheme is also known as *listen-before-talk.*

Collision in CSMA



Persistence strategies

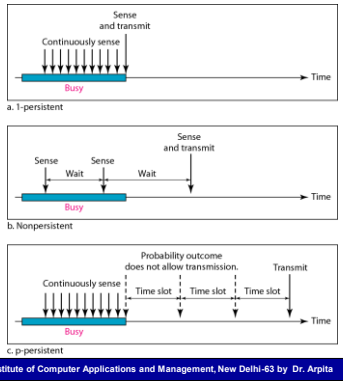
- There are three variations of this basic scheme as outlined below.

(i) 1-persistent CSMA: In this case, a node having data to send, start sending, if the channel is sensed free. If the medium is busy, the node continues to monitor until the channel is idle. Then it starts sending data.

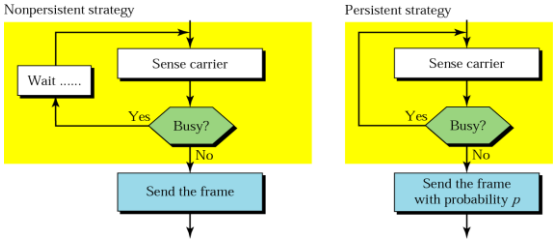
(ii) Non-persistent CSMA: If the channel is sensed free, the node starts sending the packet. Otherwise, the node waits for a random amount of time and then monitors the channel.

(iii) p-persistent CSMA: If the channel is free, a node starts sending the packet. Otherwise the node continues to monitor until the channel is free and then it sends with probability *p*.

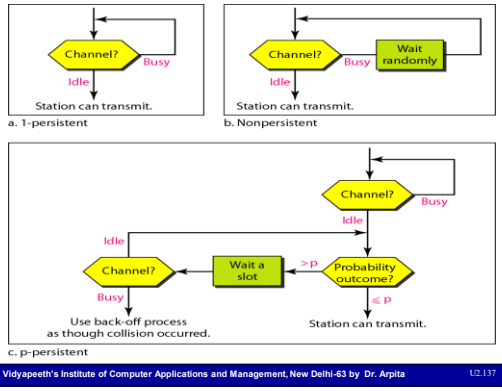
Behavior of three persistant methods



Persistence strategies



Persistence Strategies



CSMA/CD

- The CSMA method does not specify the procedure following a collision.
- Carrier sense multiple access with collision detection (CSMA/CD) augments the algorithm to handle the collision.
- In this method, a station monitors the medium after it sends a frame to see if the transmission was successful.
- If so, the station is finished..
- If, however, there is a collision, the frame is sent again.
- CSMA/CD does not use an 'acknowledgment' system. It checks for successful and unsuccessful transmissions through collision signals.

CSMA/CD

- CSMA/CD protocol can be considered as a refinement over the CSMA scheme.
- It has evolved to overcome one glaring inefficiency of CSMA.
- In CSMA scheme, when two packets collide the channel remains unutilized for the entire duration of transmission time of both the packets.
- If the propagation time is small (which is usually the case) compared to the packet transmission time, wasted channel capacity can be considerable.

CSMA/CD

- This wastage of channel capacity can be reduced if the nodes continue to monitor the channel while transmitting a packet and immediately cease transmission when collision is detected.
- This refined scheme is known as *Carrier Sensed Multiple Access with Collision Detection* (CSMA/CD) or *Listen-While-Talk*.
- CSMA/CD is not used in Wireless Networks

CSMA/CD

On top of the CSMA, the following rules are added to convert it into CSMA/CD:

(i) If a collision is detected during transmission of a packet, the node immediately ceases transmission, and it transmits jamming signal for a brief duration to ensure that all stations know that collision has occurred.

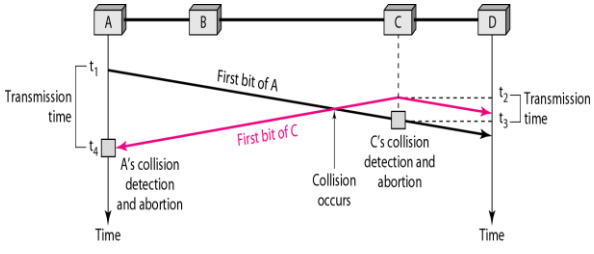
(ii) After transmitting the jamming signal, the node waits for a random amount of time and then transmission is resumed.

CSMA/CD

- The random delay ensures that the nodes, which were involved in the collision are not likely to have a collision at the time of retransmissions.
- To achieve stability in the back off scheme, a technique known as *binary exponential back off* is used.
- A node will attempt to transmit repeatedly in the face of repeated collisions, but after each collision, the mean value of the random delay is doubled.
- After 15 retries (excluding the original try), the unlucky packet is discarded and the node reports an error.

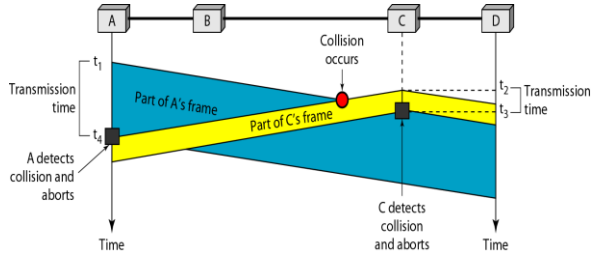
CSMA/CD

Collision of the first bit in CSMA/CD

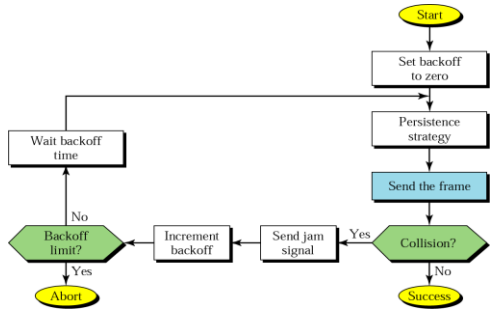


CSMA/CD

Collision and abortion in CSMA/CD



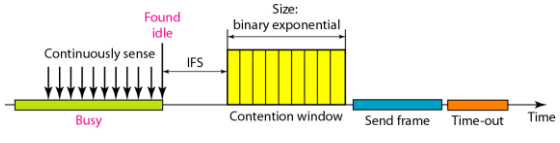
CSMA/CD procedure



CSMA/CA procedure

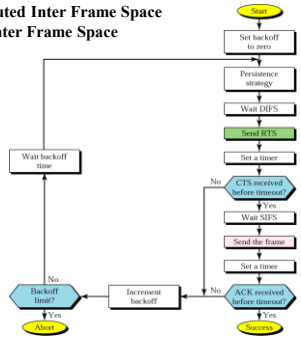
- Carrier sense multiple access with collision avoidance (CSMA/CA) is CSMA with procedures that avoid a collision.
- In CSMA/CA, the IFS (interframe space) can also be used to define the priority of a station or a frame.
- In CSMA/CA, if the station finds the channel busy, it does not restart the timer of the contention window; it stops the timer and restarts it when the channel becomes idle.
- It can be used in Wireless Networks
- It uses acknowledgement method to confirm the successful transmission.

Timing in CSMA/CA



CSMA/CA flowchart

DIFS: Distributed Inter Frame Space
SIFS: Short Inter Frame Space



CSMA/CA Process

1. Before sending a frame, the source station senses the medium by checking the energy level at the carrier frequency.
   a. The channel use a persistence strategy with back-off until the channel is idle.
   b. After the station is found to be idle, the station waits for a period of time called distribution interframe space (DIFS); then the station sends a control frame called the request to send (RTS).

CSMA/CA Process

2. After receiving the RTS and waiting a period of time called the short interframe space (SIFS) , the destination sends a control frame, called the clear to send (CTS), to the source station. This control frame indicates that the destination station is ready to receive data.
3. The source station sends data after waiting an amount of time equal to SIFS.
4. The destination station, after waiting an amount of time equal to SIFS, sends an ACK to show that the frame has been received.
5. ACK is needed in this protocol because the station does not have any means to check for the successful arrival of its data at the destination.

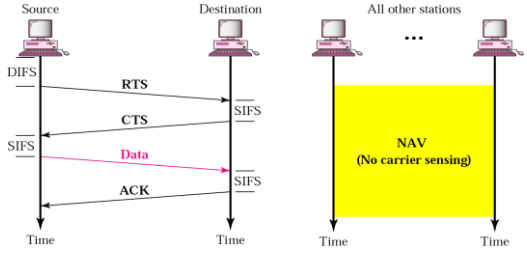
CSMA/CA Process

If one station has acquired access of the channel, how do other stations decide the waiting time?

NAV

- When a station send a RTS frame, it includes the duration of time that it needs to occupy the channel.
- The stations that are affected by this transmission create a time called 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 RTS frame, other stations start their NAV.
- In other words, each station, before sensing the physical medium to see if it is idle, first checks its NAV to see if it has expired.

CSMA/CA and NAV



Comparison

How performance is improved in CSMA/CD protocol compared to CSMA protocol?

- In CSMA scheme, a station monitors the channel before sending a packet. Whenever a collision is detected, it does not stop transmission leading to some wastage of time.
- On the other hand, in CSMA/CD scheme, whenever a station detects a collision, it sends a jamming signal by which other station comes to know that a collision occurs. As a result, wastage of time is reduced leading to improvement in performance.

Collision Free Protocols

- Almost collisions can be avoided in CSMA/CD, they can still occur during the contention period.
- Contention period: period of time when a station starts transmitting before other stations know that the line is busy.
- These collisions adversely affect the efficiency of transmission.
- Hence some protocols have been developed which are contention free.

Collision Free Protocols

- Contention Free Protocols
  - Bit-Map Method
  - Binary Countdown
  - Token Passing
  - Adaptive tree walk method

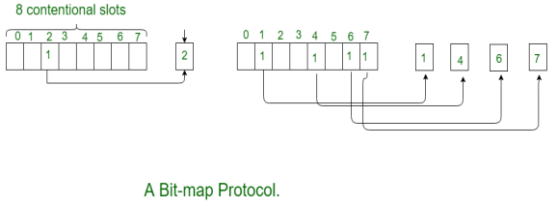
Bit-Map Method

- Bit map protocol is collision free Protocol in bitmap protocol method, each contention period consists of exactly N slots.
- If node 0 has a frame to send, it transmit a 1 bit during the first slot.
- No other node is allowed to transmit during this period.
- Next node 1 gets a chance to transmit 1 bit if it has something to send, regardless of what node 0 had transmitted.

Bit-Map Method

- In general node j may declare the fact that it has a frame to send by inserting a 1 into slot j.
- Hence after all nodes have passed, each node has complete knowledge of who wants to send a frame.
- Now, they begin transmitting in numerical order.
- Since everyone knows who is transmitting and when, there could never be any collision.

Bit-Map Method



A Bit-map Protocol.

https://www.geeksforgeeks.org/collision-free-protocols-in-computer-network/

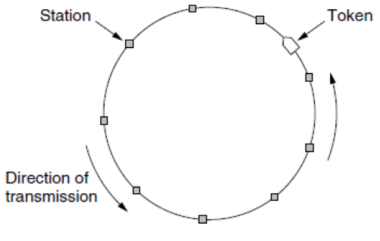
Bit-Map Method

- **Disadvantage**:
- It is inefficiency during low load.
- If a node has to transmit and no other node needs to do so, even then it has to wait for the bitmap to finish.
- Hence the bitmap will be repeated over and over again if very few nodes want to send wasting valuable bandwidth.

Token Passing

- The bit-map protocol is that it lets every station transmit a frame in turn in a predefined order.
- The same thing can be accomplished through passing a small message called a token from one station to the next in the same predefined order.
- The token represents permission to send.
- A node can send the frame, once it receives the token. After transmission, it passes the token to the next node.
- If a node don't have the frame to send, it simply passes the token.

Token Passing



Token Passing

- Note that we do not need a physical ring to implement token passing.
- The channel connecting the stations might instead be a single long bus.
- This protocol is called **token bus.**
- **Even when demand is light, a station wishing to transmit must wait for the token, increasing latency.**

 U2.163

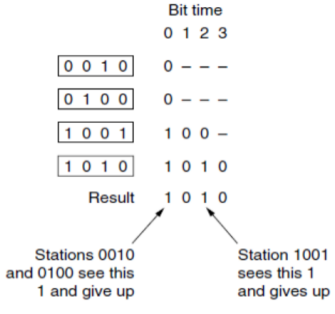
Binary Countdown

- All nodes are assigned with binary address.
- All addresses are assumed of the same length.
- A station wanting to use the channel broadcast its address as binary bit string starting with the high order bit.
- When any node sees the higher bit than itself, it gives up.
- If two or more nodes have the same higher bit, then next higher bit is sent.
- This process continues until any one of them wins.

 U2.164

Binary Countdown

- .



 U2.165

Binary Countdown

- The problem with this protocol is that the nodes with higher address always wins.
- Hence this creates a priority which is highly unfair and hence undesirable.

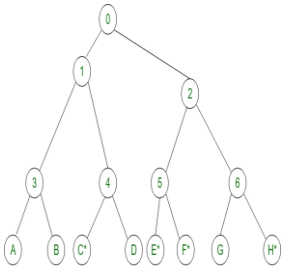
Limited Contention Protocols

- Collision based protocols (pure and slotted ALOHA, CSMA/CD) are good when the network load is low.
- Collision free protocols (bitmap, binary Countdown) are good when load is high.
- Limited contention protocol combines advantages of two-
  - Behave like the ALOHA scheme under light load
  - Behave like the bitmap scheme under heavy load.

Adaptive Tree Walk Protocol

- Initially all the nodes are allowed to try to acquire the channel.
- If it is able to acquire the channel, it sends its frame.
- If there is collision, then the nodes are divided into two equal groups and only one of these groups compete for slot 1.
- If one of its member acquires the channel, then the next slot is reserved for the other group.
- if there is a collision then that group is again subdivided, and the same process is followed.

Adaptive Tree Walk Protocol



https://www.geeksforgeeks.org/collision-free-protocols-in-computer-network/

- **Slot-0:** C*, E*, F*, H* (all nodes under node 0 can try which are going to send), conflict
- **Slot-1:** C* (all nodes under node 1can try}, C sends
- **Slot-2:** E*, F*, H*(all nodes under node 2 can try}, conflict
- **Slot-3:** E*, F* (all nodes under node 5 can try to send), conflict
- **Slot-4:** E* (all nodes under E can try), E sends
- **Slot-5:** F* (all nodes under F can try), F sends
- **Slot-6:** H* (all nodes under node 6 can try to send), H sends.

Topic

Local Area Networks:
Ethernet

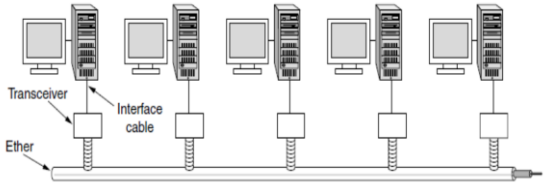
Learning Objectives

- To introduce the three generation of ethernet
- To describe the different stages in these three generations
- Traditional Ethernet
- Fast Ethernet
- Gigabit Ethernet

Learning Objectives

- Ethernet is the most widely used LAN technology, which is defined under IEEE standards 802.3.
- The reason behind its wide usability is Ethernet is easy to understand, implement, maintain, and allows low-cost network implementation.
- Ethernet operates in two layers of the OSI model, Physical Layer, and Data Link Layer.
- In order to handle collision, the Access control mechanism used in Ethernet is 1-persistent CSMA/CD.

Traditional Ethernet

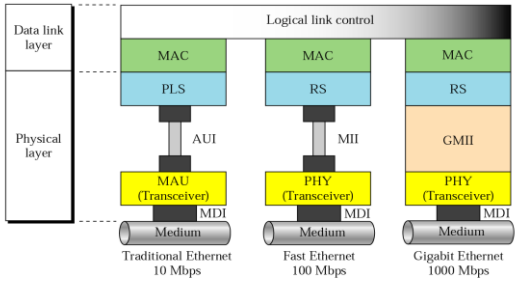


Three generations of Ethernet

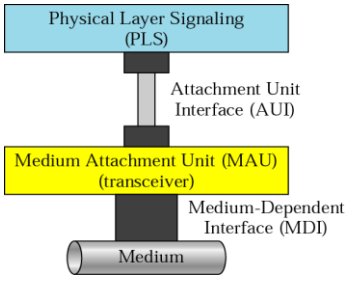
AUI: Attachment Unit Interface
MAC: Media Access Control
MAU: Medium Attachment Unit

MDI: Medium-Dependent Interface
MII: Medium-Independent Interface
GMII: Gigabit Medium-Independent Interface

PHY: Physical Layer Entity
PLS: Physical Layer Signaling
RS: Reconciliation Signaling

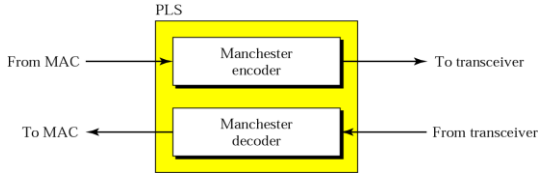


Physical layer



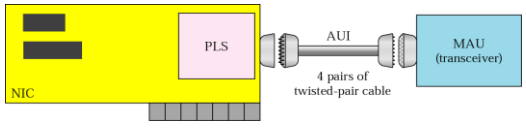
PLS

- The PLS (Physical Layer Signaling) encodes and decodes the data.



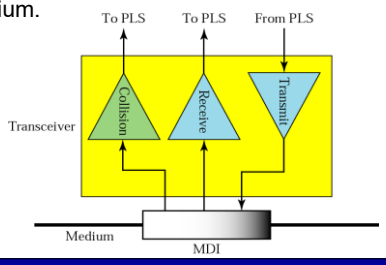
AUI

- The attachment unit interface is a specification that defines interface between PLS and MAU.
- This is designed to provide the facility to connect the PLS to different MAU. This makes PLS to be medium independent.



MAU (transceiver)

- Medium Attachment Unit (MAU) is medium dependent.
- It creates the appropriate signal for each particular medium.



Ethernet MAC Sublayer Protocol

PREAMBLE	SFD	DESTINATION ADDRESS	SOURCE ADDRESS	LENGTH	DATA	CRC
7 Bytes	1 Byte	6 Bytes	6 Bytes	2 Bytes	46 - 1500 Bytes	4 Bytes

- Preamble :
  - Ethernet frame starts with 7-Bytes Preamble.
  - It indicates the receiver that frame is coming and allow the receiver to lock onto the data stream before the actual frame begins.
- Start of frame delimiter (SFD):
  - This is a 1-Byte field which is always set to 10101011.
  - SFD indicates that upcoming bits are starting of the frame, which is the destination address.

Ethernet MAC Sublayer Protocol

PREAMBLE	SFD	DESTINATION ADDRESS	SOURCE ADDRESS	LENGTH	DATA	CRC
7 Bytes	1 Byte	6 Bytes	6 Bytes	2 Bytes	46 - 1500 Bytes	4 Bytes

- Source Address :
  - This is a 6-Byte field which contains the MAC address of source machine.
  - As Source Address is always an individual address (Unicast), the least significant bit of first byte is always 0.
- Length:
  - Length is a 2-Byte field, which indicates the length of entire Ethernet frame. This 16-bit field can hold the length value between 0 to 65534, but length cannot be larger than 1500 because of some own limitations of Ethernet.

Ethernet MAC Sublayer Protocol

PREAMBLE	SFD	DESTINATION ADDRESS	SOURCE ADDRESS	LENGTH	DATA	CRC
7 Bytes	1 Byte	6 Bytes	6 Bytes	2 Bytes	46 - 1500 Bytes	4 Bytes

- Destination Address : This is 6-Byte field which contains the MAC address of machine for which data is destined.

06-01-02-01-2C-4B

  - Unicast: LSB (least significant bit) of first octet of an address is set to zero.
  - Multicast: If the LSB (least significant bit) of first octet of an address is set to One
  - Broadcast: Ethernet frames with ones in all bits of the destination address (FF-FF-FF-FF-FF-FF) are referred as broadcast address.

Ethernet MAC Sublayer Protocol

PREAMBLE	SFD	DESTINATION ADDRESS	SOURCE ADDRESS	LENGTH	DATA	CRC
7 Bytes	1 Byte	6 Bytes	6 Bytes	2 Bytes	46 - 1500 Bytes	4 Bytes

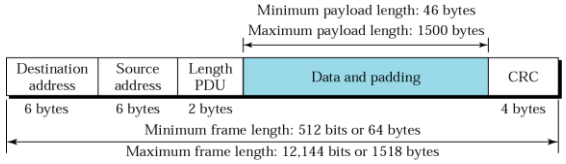
- Data:
  - This is the place where actual data is inserted, also known as Payload. Both IP header and data will be inserted here if Internet Protocol is used over Ethernet.
  - The maximum data present may be as long as 1500 Bytes.
  - In case data length is less than minimum length i.e. 46 bytes, then padding 0's is added to meet the minimum possible length.

Ethernet MAC Sublayer Protocol

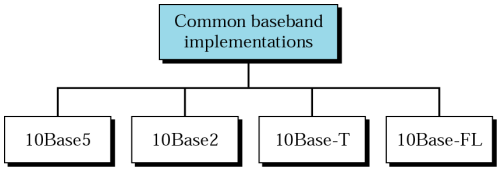
PREAMBLE	SFD	DESTINATION ADDRESS	SOURCE ADDRESS	LENGTH	DATA	CRC
7 Bytes	1 Byte	6 Bytes	6 Bytes	2 Bytes	46 - 1500 Bytes	4 Bytes

- Cyclic Redundancy Check (CRC)
  - CRC is 4 Byte field.
  - This field contains a 32-bits hash code of data, which is generated over the Destination Address, Source Address, Length, and Data field.
  - If the checksum computed by destination is not the same as sent checksum value, data received is corrupted.

Minimum and maximum length



Categories of traditional Ethernet

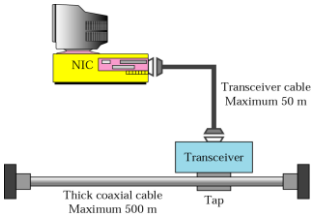


Categories of traditional Ethernet

- **Ethernet cables** likewise are manufactured to any of several standard specifications.
  - The most popular Ethernet cable in current use, Category 5 or CAT5, supports both traditional and Fast Ethernet.
  - The Category 5e (CAT5e) cable supports Gigabit Ethernet.
  - To connect Ethernet cables to a computer, a person normally uses a network adapter, also known as a network interface card (NIC).
  - Ethernet adapters interfaces directly with a computer's system bus. The cables, in turn, utilize connectors that in many cases look like the RJ-45 connector used with modern telephones.

10Base5 : Thick Ethernet

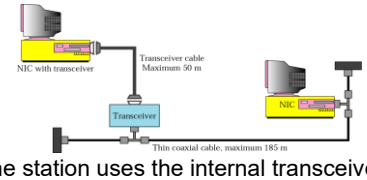
- This is the first Ethernet specification.
- It uses bus topology with an external transceiver connected via a tap to a thick coaxial cable.



 U2.187

10Base2:Thin Ethernet or Cheapernet

- Uses Bus topology with an internal transceiver
- Point to Point connection with external transceiver.

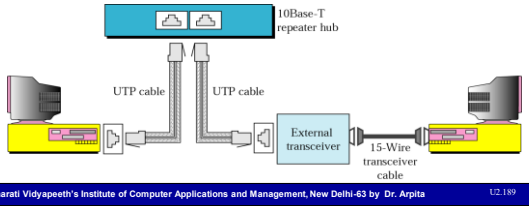


- If the station uses the internal transceiver, No need for AUI cable.
- If the station lack the transceiver, external transceiver is used with AUI

 U2.188

10Base-T: Twisted Pair Ethernet

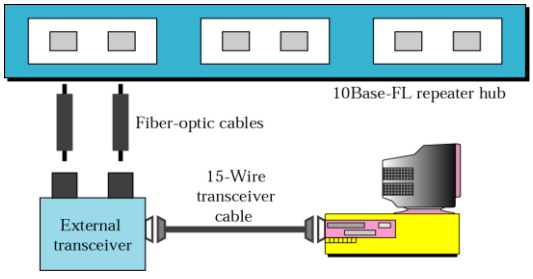
- It uses physical star topology.
- Stations are connected to hub with an internal transceiver or external transceiver.



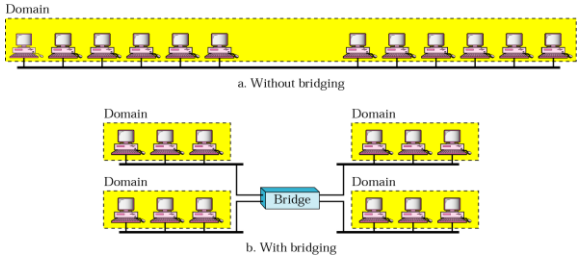
 U2.189

10Base-FL: Fiber Link Ethernet

- Uses the star topology to connect stations to hub.



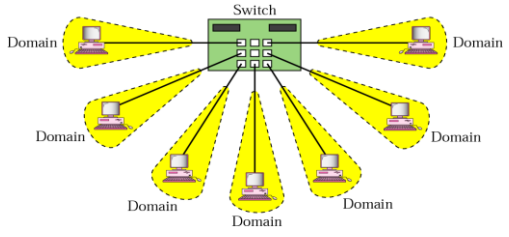
Bridged Ethernet



Bridged Ethernet

- The bridge is used to divide the LAN.
- There are two benefits to divide the Ethernet LAN.
  - The Raise of Bandwidth: In unbridged Ethernet LAN, the bandwidth is shared between all stations. If we divide the Ethernet LAN, each segment can use same bandwidth.
  - Separate Collision Domain: As the Ethernet LAN is divided into smaller segments using bridge, the collision domain shrinks.

Switched Ethernet

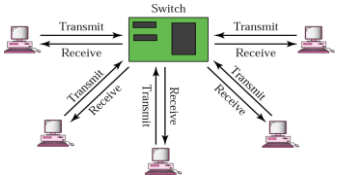


Switched Ethernet

- An Ethernet switch is a bridge which can connect more than two segments together.
- The idea behind a switch is that it removes all unneeded traffic from each segment by only forwarding the traffic needed on that segment, which provides better performance on the network.

Full-duplex switched Ethernet

- Two links are used: One to transmit and One to receive.
- No need for CSMA/CD



Fast Ethernet

- In the mid-1990s, Fast Ethernet technology matured and met its design goals of
  - increasing the performance of traditional Ethernet while avoiding the need to completely re-cable existing Ethernet networks.
  - Only supports star topology.
- Fast Ethernet comes in two major varieties:
  - 100Base-T (using unshielded twisted pair cable)
  - 100Base-FX (using fiber optic cable)

 U2.196

Gigabit Ethernet

- Whereas Fast Ethernet improved traditional Ethernet from 10 Megabit to 100 Megabit speed,
- Gigabit Ethernet boasts the same order-of-magnitude improvement over Fast Ethernet by offering speeds of 1000 Megabits (1 Gigabit).
- Gigabit Ethernet was first made to travel over optical and copper cabling, but the 1000Base-T standard successfully supports it as well.
- 1000Base-T uses Category 5 cabling similar to 100 Mbps Ethernet, although achieving gigabit speed requires the use of additional wire pairs.

 U2.197

Topic

Wireless LANs

 U2.198

IEEE 802.11

Architecture

Physical Layer

MAC Layer

Addressing Mechanism

Wireless LANs

Some of the advantages are mentioned below :

- **Availability of low-cost portable equipment:** Due to the technology enhancements, the equipment cost that are required for WLAN set-up have reduced a lot.

- **Mobility:** An increasing number of LAN users are becoming mobile. These mobile users require that they are connected to the network regardless of where they are because they want simultaneous access to the network. This makes the use of cables, or wired LANs, impractical if not impossible. Wireless LAN can provide users mobility, which is likely to increase productivity, user convenience and various service opportunities

Wireless LANs

- **Installation speed and simplicity:** Wireless LANs are very easy to install. There is no requirement for wiring every workstation and every room. This ease of installation makes wireless LANs inherently flexible.
- **Installation flexibility:** If a company moves to a new location, the wireless system is much easier to move than ripping up all of the cables that a wired system would have snaked throughout the building. This also provides portability. Wireless technology allows network to go anywhere wire cannot reach.

Wireless LANs

Reduced cost of ownership: While the initial cost of wireless LAN can be higher than the cost of wired LAN hardware, it is envisaged that the overall installation expenses and life cycle costs can be significantly lower. Long-term cost-benefits are greater in dynamic environment requiring frequent moves and changes.

Scalability: Wireless LAN can be configured in a variety of topologies to meet the users need and can be easily scaled to cover a large area with thousands of users roaming within it.

IEEE 802.11 Architecture

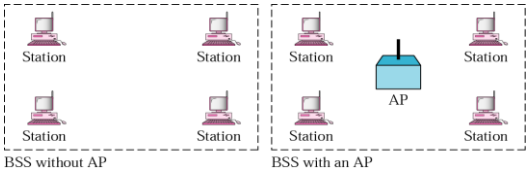
IEEE has defined the specifications for a Wireless LAN, called IEEE 802.11, which covers the physical and data link layers.

The standard defines two kinds of services :

•BSS (Basic Service Set)

•ESS (Extended Service Set)

BSSs



BSS without AP BSS with an AP

IEEE 802.11 Architecture

BSS

- IEEE 802.11defines the BSS as the building block of a wireless LAN.
- A basic service set is made of stationary or mobile wireless stations and an optional central base station, known as the access point (AP).
- BSS without an AP is stand alone network and can not send data to other BSSs.
- It is called an **ad-hoc network** architecture.

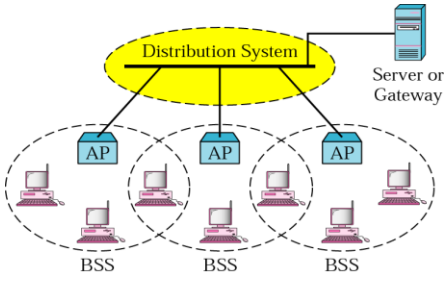
 U2.205

IEEE 802.11 Architecture

- In this architecture, stations can form a network without the need of an AP.
- They can locate one another and agree to be part of a BSS.
- A BSS with an AP is sometimes referred to as an **infrastructure network.**

 U2.206

ESS



 U2.207

IEEE 802.11 Architecture

ESS

- An ESS is made up of two or more BSSs with APs.
- In this case, the BSSs are connected through a distribution system, which is usually a wired LAN.
- The distribution system connects the APs in the BSSs.
- IEEE 802.11 des not restrict the distribution system; it can be any IEEE LAN such as Ethernet.

IEEE 802.11 Architecture

The extended service set uses two types of stations :

Mobile :- Mobile stations are normal stations inside a BSS.

Stationary :- Stationary stations are AP stations that are part of a wired LAN.

ESS

- When BSSs are connected, the stations within reach of one another can communicate without the use of an AP.
- However, communication between two stations in two different BSSs usually occurs via two APs.
- The idea is similar to communication in a cellular network if we consider each BSS to be cell.
- Each AP to be a base station.
- Note that a mobile station can belong to more than one BSS at the same time.

Station Types

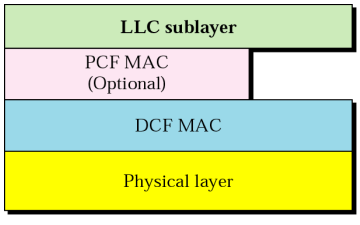
IEEE 802.11, defines three types of satations based on their mobility in a wireless Lan

•**No-transition** – A station with no-transition mobility is either stationary or moving only inside a BSS

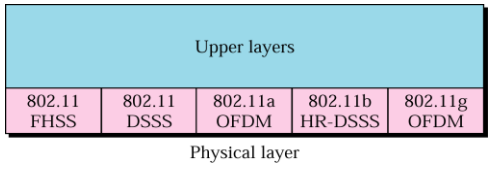
•**BSS-transition** – A station with BSS-transition mobility can move from one BSS to another, but the movement is confined inside one ESS.

•**ESS-transition** – A station with ESS-transition mobility can move from one ESS to another.

MAC layers in IEEE 802.11 standard



Physical Layer Specifications



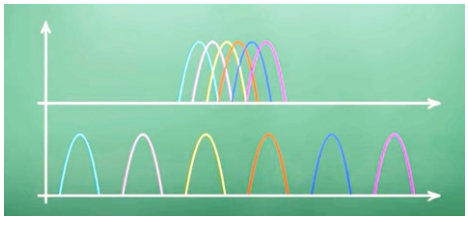
FHSS

- This is somewhat similar to sending different parts of one song over several FM channels.
- Eavesdroppers hear only unintelligible blips and any attempt to jam the signal results in damaging a few bits only.
- The modulation technique in this specification is either two-level FSK or four-level FSK with 1 or 2 bits/baud, which results in a **data rate of 1 or 2 Mbps**

DSSS

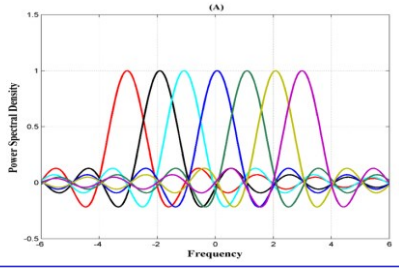
- With **direct sequence spread spectrum** the transmission signal is spread over an allowed band (for example 25MHz).
- A random binary string is used to modulate the transmitted signal. This random string is called the ***spreading code***.
- The data bits are mapped to into a pattern of "chips" and mapped back into a bit at the destination.
- The number of chips that represent a bit is the ***spreading ratio***.
- The modulation technique in this specification is PSK at 1 Mbaud/s. The system allows 1 or 2 bits/baud (BPSK or QPSK), which results in a data rate **of 1 or 2 Mbps**

OFDM



Orthogonal means that the peak of one signal occurs at the null of other signals

OFDM



Orthogonal means that the peak of one signal occurs at the null of other signals

https://www.researchgate.net/publication/321278034_An_implementation_of_peak_to_average_power_ratio_reduction_for_multicarrier_system_orthogonal_frequency_division_multiplexing

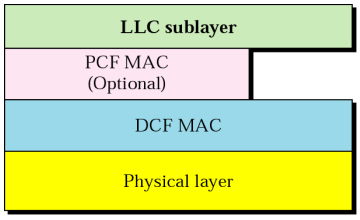
OFDM

- IEEE 802.11a OFDM describes the orthogonal frequency-division multiplexing (OFDM) method for signal generation in a 5.725–5.850 GHz band.
- OFDM is similar to FDM.
- OFDM uses PSK and QAM for modulation.
- The common data rates are 18 Mbps (PSK) and 54 Mbps (QAM).

HR-DSSS

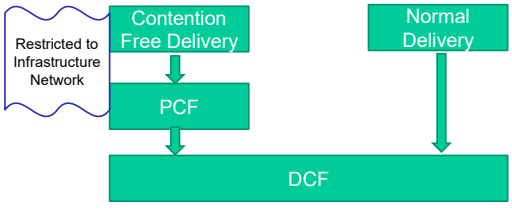
- High-rate direct-sequence spread spectrum (HRDSSS) method for signal generation in the 2.400–4.835 GHz band.
- HR-DSSS is similar to DSSS except for the encoding method.
- ***Complementary code keying (CCK) is used instead of BPSK or QPSK that are used in DSSS.***
  - CCK includes a pair of codes called chipping sequences which are complementary to each other.
  - CCK has a shorter chipping sequence of 8 bits
- Data Rates: Upto 11Mbps

MAC layers in IEEE 802.11 standard



MAC layers in IEEE 802.11 standard

- IEEE 802.11 defines two MAC sublayers:
  - Distributed Coordination Function (DCF)
  - Point Coordination Function (PCF)



MAC layers in IEEE 802.11 standard

- Distributed Coordination Function (DCF)
  - DCF is the basis of the standard CSMA/CA access mechanism
  - It first checks to see that the radio link is clear before transmitting.
  - To avoid collisions, stations use a random backoff after each frame, with the first transmitter seizing the channel.
  - It may use the CTS/RTS clearing technique to further reduce the possibility of collisions.
  -

MAC layers in IEEE 802.11 standard

- Distributed Coordination Function (DCF)
  - Transmission can be initiated immediately if the medium is idle for greater than DIF period. Carrier sensing is performed with both PHY layer as well as with NAV.
  - The medium is said to be free for at least the period equivalent to DIFS if the previous frame was received without errors.
  - If there was errors, then the medium must be free for the duration equal to **Extended Interframe space** (EIFS).

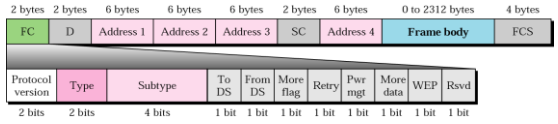
MAC layers in IEEE 802.11 standard

- Point Coordination Function (PCF)
  - PCF is restricted to infrastructure networks.
  - Contention-free service is not provided full-time.
  - When the PCF is used, time on the medium is divided into the contention-free period (CFP) and the contention period.
  - Access to the medium in the former case is controlled by the PCF, while access to the medium in the latter case is controlled by the DCF

PCF

- To give priority to PCF over DCF, another set of interframe spaces has been defined : PIFS and SIFS.
- SIFS is as same as DCF
- PIFS (PCF IFS) – is shorter than the DIFS.
- This means that if, at the same time, a station wants to use only DCF and an AP wants to use PCF, the AP has priority.

Frame Format



 U2.228

Frame format

FC	**Frame Control-**The FC field is used to define the type of frame and some control information.
D	This field defines the duration of the transmission. That is used to set the value of NAV. In control frame, this field defines the ID of the frame.
Addresses	Depends upon To DS and from DS
Sequence control	Defines sequence number of the frame to be used in flow control.
Frame body	Data
FCS	CRC-32

 U2.229

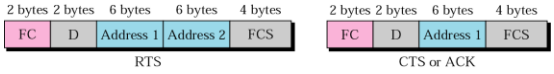
Subfields in FC field

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

 U2.230

Control Frames

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



Cont ....

Table Values of subfields in control frames

Subtype	*Meaning*
1011	Request to send (RTS)
1100	Clear to send (CTS)
1101	Acknowledgment (ACK)

Cont ....

Table Subfields in FC field

To DS	*From DS*	*Address 1*	*Address 2*	*Address 3*	*Address 4*
0	0	Destination station	Source station	BSS ID	N/A
0	1	Destination station	Sending AP	Source station	N/A
1	0	Receiving AP	Source station	Destination station	N/A
1	1	Receiving AP	Sending AP	Destination station	Source station

DS: Distribution System **DS=1** means AP **DS=0** means Normal station

Bluetooth

 U2.234

Bluetooth

Architecture

Radio Layer

Baseband Layer

L2CAP Layer

Other Upper Layers

 U2.235

Bluetooth

- Bluetooth wireless technology is a short-range radio technology, which is developed for Personal Area Network (PAN).
- It is mainly used as an alternative to wire connections, to exchange files between nearby portable devices and connect cell phones and music players with wireless headphones.
- It is an ad hoc type network operable over a small area such as a room.
- In the most widely used mode, transmission power is limited to 2.5 milliwatts, giving it a very short range of up to 10 metres.

 U2.236

Bluetooth

- The name "Bluetooth“ was named after the name of the 10th-century Danish king Harald Bluetooth.
- The IEEE standardized Bluetooth as IEEE 802.15.1, but no longer maintains the standard.
- The Bluetooth SIG (Bluetooth Special Interest Group) oversees development of the specification, manages the qualification program, and protects the trademarks.
- The Bluetooth SIG published the Bluetooth Core Specification Version 5.3 on July 13, 2021

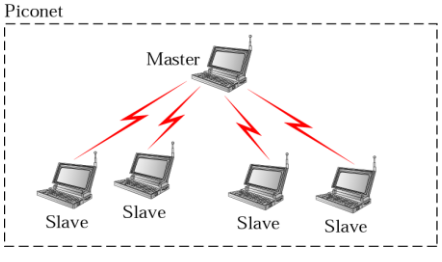
Bluetooth

There are two types of topology for Bluetooth
- Piconet
- Scatternet.

The Piconet is a small ad hoc network of devices (normally 8 stations) as shown in Fig. It has the following features:

- One is called Master and the others are called Slaves
- All slave stations synchronizes their clocks with the master
- Possible communication - One-to-one or one-to-many
- Each piconet has a unique hopping pattern/ID
- Each master can connect to 7 simultaneous or 200+ inactive (parked) slaves per piconet.

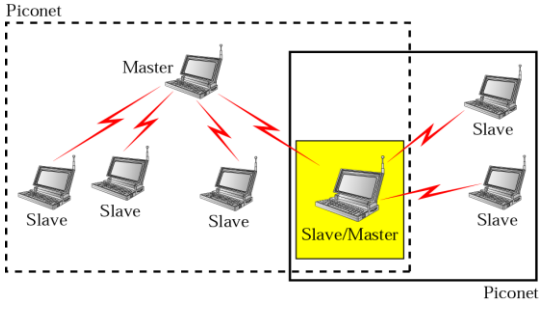
Piconet



Scatternet

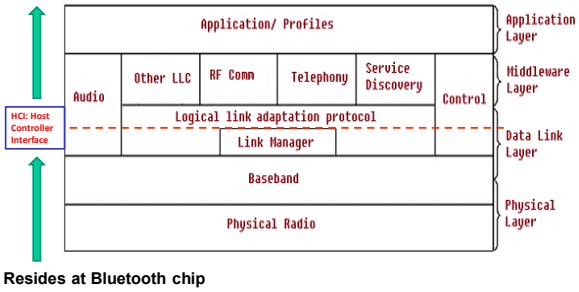
- By making one slave as master of another Piconet, Scatternet is formed by combining several Piconets. Key features of the scatternet topology are mentioned below:
  - A Scatternet is the linking of multiple co-located piconets through the sharing of common master or slave devices.
  - A device can be both a master and a slave.
  - Radios are symmetric (same radio can be master or slave).
  - High capacity system, each piconet has maximum capacity (720 Kbps)

Scatternet



Bluetooth Layers

Implemented on the Bluetooth device that hosts the chip



Resides at Bluetooth chip

Bluetooth Layers: Radio

- The Radio layer defines the requirements for a Bluetooth transceiver operating in the 2.4 GHz ISM band.
- Bluetooth devices are low-power and have a range of 10 m.
- Bluetooth uses the frequency-hopping spread spectrum (FHSS) method.
- To transform bits to a signal, Bluetooth uses a sophisticated version of FSK, called GFSK (FSK with Gaussian bandwidth filtering).

 U2.243

Bluetooth Layers: Radio

- GFSK has a carrier frequency.
- Bit 1 is represented by a frequency deviation above the carrier;
- Bit 0 is represented by a frequency deviation below the carrier.

 U2.244

Bluetooth Layers: Baseband

- The baseband layer is roughly equivalent to the MAC sublayer in LANs.
- The primary and secondary stations communicate with each other using time slots.
- The access method is TDD-TDMA (time-division duplex TDMA).
  - TDD-TDMA is a kind of half-duplex communication in which the sender and receiver send and receive data, but not at the same time.

 U2.245

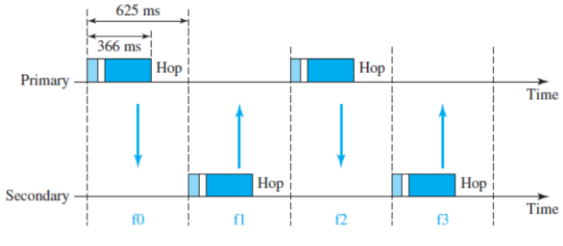
Bluetooth Layers: Baseband

- There can be two type of communication in Bluetooth.
  - Single-Secondary Communication
    - ✓If the piconet has only one secondary (Slave)
  - Multiple-Secondary Communication
    - ✓if there is more than one secondary in the piconet

Bluetooth Layers: Baseband

- Single-Secondary Communication: If the piconet has only one secondary, the TDMA operation is very simple.
- The primary uses even-numbered slots (0,2,4, . .); the secondary uses odd-numbered slots (1,3,5, . .).
- In slot 0, the primary sends, and the secondary receives;
- In slot 1, the secondary sends and the primary receives. The cycle is repeated.

Bluetooth Layers: Baseband



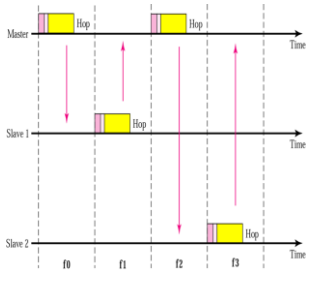
Single Secondary Communication

259 μs is needed for hopping and control mechanisms. This means that a one-slot frame can last only 625 − 259, or 366 μs.

Bluetooth Layers: Baseband

- Multiple-Secondary Communication : if there is more than one secondary in the piconet.
  - The primary (Master) uses the even-numbered slots
  - A Secondary (Slave) sends in the next odd-numbered slot, if the packet in the previous slot was addressed to it.
  - All secondaries listen on even-numbered slots, but only one secondary sends in any odd-numbered slot

Bluetooth Layers: Baseband



Multiple Secondary Communication

- In slot 0, the primary sends a frame to secondary 1.
- In slot 1, only secondary 1 sends a frame to the primary because the previous frame was addressed to secondary 1; other secondaries are silent.
- In slot 2, the primary sends a frame to secondary 2.
- In slot 3, only secondary 2 sends a frame to the primary because the previous frame was addressed to secondary 2; other secondaries are silent.
- The cycle continues.

Bluetooth Layers: Baseband

- There are two types of Links can be created between a primary and a secondary.
  - Synchronous Connection-oriented (SCO) Link
    - ✓Used when avoiding latency (delay in data delivery) is more important than integrity (error-free delivery).
    - ✓In an SCO link, a physical link is created between the primary and a secondary by reserving specific slots at regular intervals.
    - ✓If a packet is damaged, it is never retransmitted.
    - ✓SCO is used for real-time audio where avoiding delay is all-important.
    - ✓Data Rate: 64 kbps

Bluetooth Layers: Baseband

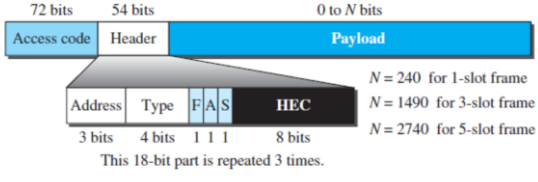
- There are two types of Links can be created between a primary and a secondary.
  - Asynchronous Connectionless Link (ACL)
    - ✓Used when data integrity is more important than avoiding latency.
    - ✓if a payload encapsulated in the frame is corrupted, it is retransmitted.
    - ✓Data rate: 721 kbps

Bluetooth Layers: Baseband

- Frame Format
  - One-slot, Three-slot, Or Five Slot Frames.
  - One Slot:
    - ✓In one-slot frame exchange, 259 μs is needed for hopping and control mechanisms. This means that a one-slot frame can last only 625 − 259, or 366 μs.
  - Three Slot:
    - ✓A three-slot frame occupies three slots.
    - ✓Only one hop number is used, three hop numbers are consumed.
    - ✓Since 259 μs is used for hopping, the length of the frame is 3 × 625 − 259 = 1616 μs or 1616 bits.
  - Five Slot: Only one hop number is used, five numbers are consumed. Length of the frame is 5 × 625 − 259 = 2866 bits

Bluetooth Layers: Baseband

- Frame Format (Three Slot)



Bluetooth Layers: Baseband

Access code	Contains synchronization bits and the identifier of the primary to distinguish the frame of one piconet from that of another.	
Header	This 54-bit field is a repeated 18-bit pattern	
	Address	The 3-bit address subfield can define up to seven secondaries
	Type.	Identifies the frame type (ACL, SCO, poll, or null), the type of error correction used in the data field, and how many slots long the frame is.
	F	When set (1), it indicates that thedevice is unable to receive more frames
	A	1-bit subfield is for acknowledgment. Bluetooth uses Stop-and-Wait ARQ
	S	This 1-bit subfield holds a sequence numbering
	HEC	The 8-bit header error correction subfield is a checksum to detect errors
Payload	This subfield can be 0 to 2740 bits long. It contains data or control information coming from the upper layers.	

Bluetooth Layers: L2CAP

- Link Manager:
  - The link manager handles the establishment of logical channels between devices, including power management, pairing and encryption.
  - Link Manager Protocol is used to take care of all services for Link manager.
  - It lies below the host controller interface.
- Host Controller Interface (HCI) :
  - HCI provides a command interface for the controller and the link manager.
  - It discovers the other Bluetooth devices that are within the coverage radius.

Bluetooth Layers: L2CAP

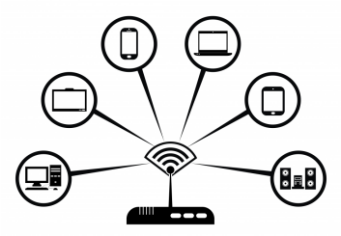
- The Logical Link Control and Adaptation Protocol, or L2CAP (L2 here means LL), is roughly equivalent to the LLC sublayer in LANs.
- It is used for data exchange on an ACL link;
- SCO channels do not use L2CAP.
- L2CAP provides following services
  - Multiplexing
    - ✓At the sender site, it accepts data from one of the upper-layer protocols, frames them, and delivers them to the baseband layer.
    - ✓At the receiver site, it accepts a frame from the baseband layer, extracts the data, and delivers them to the appropriate protocol layer.

Bluetooth Layers: L2CAP

- Segmentation and Reassembly
  - ✓The L2CAP divides 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 them at the destination.
- QoS (Quality-of-Service)
  - ✓Bluetooth allows the stations to define a quality-of-service level.
  - ✓Bluetooth defaults to what is called best-effort service; it will do its best under the circumstances.
- Group Management
  - ✓L2CAP is to allow devices to create a type of logical addressing between themselves like multicasting.

 U2.258

WiFi =Wireless Fidelity?



 U2.259

WiFi

- Wi-Fi is based on the IEEE 802.11 family of standards, which are commonly used for local area networking of devices and Internet access.
- The different versions of Wi-Fi are specified by various IEEE 802.11 protocol standards

Generational name	Technology supported
Wi-Fi 7	802.11be (in development)
Wi-Fi 6	802.11ax
Wi-Fi 5	802.11ac
Wi-Fi 4	802.11n

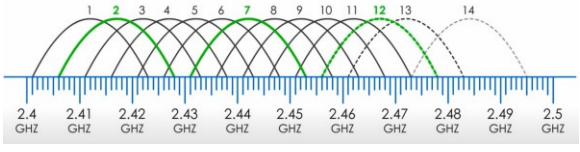
 U2.260

WiFi

Generation	IEEE Standard	Maximum Linkrate (Mbit/s)	Adopted	Radio Frequency (GHz)	Modulation
Wi-Fi 6E	802.11ax	600 to 9608	2020	6	MIMO-OFDM
Wi-Fi 6	802.11ax	600 to 9608	2019	2.4/5	MIMO-OFDM
Wi-Fi 5	802.11ac	433 to 6933	2014	5	MIMO-OFDM
Wi-Fi 4	802.11n	72 to 600	2008	2.4/5	MIMO-OFDM
(Wi-Fi 3*)	802.11g	6 to 54	2003	2.4	OFDM
(Wi-Fi 2*)	802.11a	6 to 54	1999	5	OFDM
(Wi-Fi 1*)	802.11b	1 to 11	1999	2.4	DSSS
(Wi-Fi 0*)	802.11	1 to 2	1997	2.4	DSSS, FHSS

https://en.wikipedia.org/wiki/IEEE_802.11

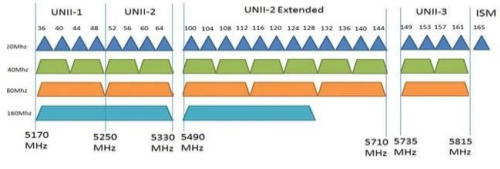
WiFi: 2.4 GHz



- Gap between Adjacent Channel=5MHz
- Only non-overlapping channels are used.
- The band is overcrowded as this band is used by many devices like Microwave oven, Bluetooth etc.
- More Susceptible for interference.

https://www.youtube.com/watch?v=QIJnZFeKIRA&list=PLSNNzog5eydvJG48PYnWnNY7-tQIfkTRb&index=9

WiFi: 5 GHz



- 5 GHz consists of 24 unlicensed band, each 20 MHz wide.
- There is no overlapping among 24 channels.
- In theory, it can support up to 1 Gbps data rate.
- To increase bandwidth channel bonding is used.

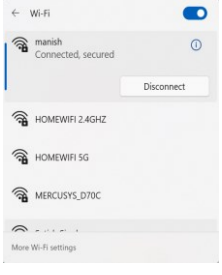
UNII: Unlicensed National Information Infrastructure

WiFi: 5 GHz Vs 2.4 GHz

- 5GHz band provides better data transfer rate than 2.4GHz band.
- 5GHz band is less congested than 2.4GHz band.
- 5GHz band has greater attenuation than 2.4GHz band.
- 2.4 GHz range is greater than 5GHz band.
- 2.4 GHz band is highly prone to interfence as many devices used.

WiFi: Common Terms

- SSID (Service Set Identifier): Name of your wireless network, also known as Network ID.



- SSIDs can be up to 32 alphanumeric characters long.
- They are also case-sensitive.
- The SSID can be changed in the software configuration pages for your wireless modem
- Users can assign more than one SSID to an access point.
- Using multiple SSIDs allows users to access different networks, each with different policies and functions.
- The two networks might use the same physical infrastructure, but they would have two different SSIDs

WiFi: Hotspot

- Hotspot: A hotspot is a physical location where people can access the Internet, typically using Wi-Fi.
- Mobile hotspot: A mobile hotspot (sometimes called a portable hotspot) is a hotspot that's just that—mobile.
- Tethering:
  - Sharing of a mobile device's Internet connection with other connected computers.
  - Connection of a mobile device with other devices can be done over wireless LAN (Wi-Fi), over Bluetooth or by physical connection using a cable, for example USB.

WiFi: Hotspot

- Access point (wireless access point): A wireless access point (WAP) is a networking device that allows a Wi-Fi compliant device to connect to a wired network.

Conclusion

- Medium Access control can be random access, controlled or channelised.
- In CSMA station must listen to the medium first
- CSMA/CD is CSMA with post collision procedure
- CSMA/CA is CSMA with procedure that avoids collision

Summary

- Medium Access control can be random acess, controlled or channelised.
- In CSMA station must listen to the medium first
- CSMA/CD is CSMA with post collision procedure
- CSMA/CA is CSMA with procedure that avoids collision

Review Questions (OBJ)

1. In cyclic redundancy checking, the divisor is _____ the CRC.
A) The same size as
B) one bit less than
C) one bit more than
D) none of the above

2. The _____of errors is more difficult than the _____.
A) correction; detection
B) detection; correction
C) creation; correction
D) creation; detection

Review Questions (OBJ)

3. The checksum of 1111 and 1111 is _____.
A) 1111
B) 0000
C) 1110
D) 0111

4. The divisor in a cyclic code is normally called the _____.
A) degree
B) generator
C) redundancy
D) none of the above

Review Questions (OBJ)

5. In a Go-Back-N ARQ, if the window size is 63, what is the range of sequence numbers?
A) 0 to 63
B) 0 to 64
C) 1 to 63
D) 1 to 64

6. In Go-Back-N ARQ, if frames 4, 5, and 6 are received successfully, the receiver may send an ACK _____ to the sender.
A) 5
B) 6
C) 7
D) any of the above

Review Questions (OBJ)

7. HDLC is an acronym for _____.
A) High-duplex line communication
B) High-level data link control
C) Half-duplex digital link combination
D) Host double-level circuit
8. Both Go-Back-N and Selective-Repeat Protocols use a _____.
A) sliding frame
B) sliding window
C) sliding packet
D) none of the above

Review Questions (OBJ)

9. In Selective Repeat ARQ, if 5 is the number of bits for the sequence number, then the maximum size of the send window must be _____
A) 15
B) 16
C) 31
D) 1

10. ARQ stands for _____.
A) Automatic repeat quantization
B) Automatic repeat request
C) Automatic retransmission request
D) Acknowledge repeat request

Review Questions (Short)

1. What is advantage of controlled access over random access?
2. How do two persistence strategies differ?
3. What is purpose of Jam signal in CSMA/CD?
4. Why is token passing a controlled access procedure?
5. Compare and contrast Go Back N and Selective repeat
6. Define piggybacking and its usefulness
7. What is access method used in wireless lans?
8. Find the checksum of the following bi sequence. Assume 8-bit segment size
   10010011 10010011 1001100 01001101

Review Questions (Short)

9. How are a lost acknowledgement a lost frame handled at the sender site in Go-Back-N ARQ ?
11. What is Frequency Hopping Spread Spectrum . Explain.
12. Construct the Hamming code for the bit sequence 1001101.
13. What is the relationship between AMPS and D-AMPS in Mobile Phones?
14. Explain the procedure of CSMA/CD

Review Questions (Long)

1. Differentiate between Go-back n and Selective repeat .sliding window?
2. What is purpose of NAV?

Recommended reading

1. Forozun, Data Communication and Networking, TMH
2. Tanenbaum , A computer Networks: Prentice Hall
3. Stallings , High speed Networks :Prentice Hall
4. Comer D. Computer Networks: Prentice hall
5. Kurose, J and ross , Computer Networking : Addison Wesley