UNIT-4

MEDIUM ACCESS CONTROL SUBLAYER

- Data link layer in the OSI model is divided into two layers,
  - Logical Link control Sublayer
  - Medium Access Control Sublayer
- Medium Access Control Sublayer is responsible for
  - Physical Addressing (MAC address)
  - Access Control (Channel Allocation)

4.1 MAC ADDRESSING:

- A media access control address (MAC address) is a unique identifier assigned to network interfaces for communications on the physical network segment. • MAC addresses are used for numerous network technologies and most IEEE 802 network technologies, including Ethernet.
- Logically, MAC addresses are used in the media access control protocol sub layer of the OSI reference model.
- MAC addresses are most often assigned by the manufacturer of a network interface card (NIC) and are stored in its hardware, such as the card's read-only memory or some other firmware mechanism.
- A network node may have multiple NICs and each must have one unique MAC address per NIC.
- MAC address is 48-bit address space contains potentially 2^{48} or 281,474,976,710,656 possible MAC addresses.
- Addresses can either be **universally administered addresses** or **locally administered addresses**.

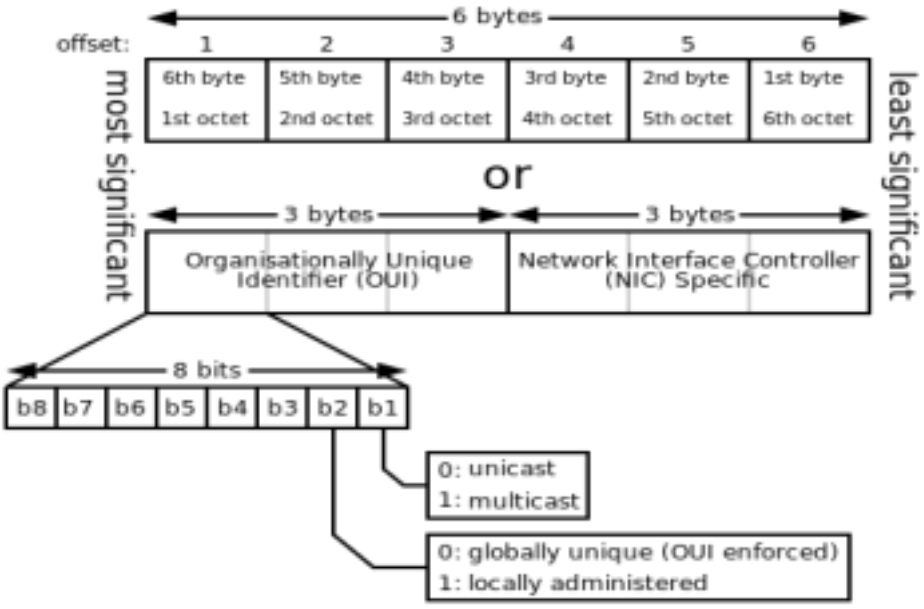


Figure: MAC address format

• The first three octets (in transmission order) identify the organization that issued the identifier and are known as the **Organizationally Unique Identifier (OUI).** • Remaining 3 octets represent the address of the **Network Interface Card.** • Universally administered and locally administered addresses are distinguished by setting the second-least-significant bit of the most significant byte of the address. This bit is also referred to as the U/L bit, short for Universal/Local, which identifies how the address is administered.

- If the bit is 0, the address is universally administered.
- If it is 1, the address is locally administered.

Ex: 06-00-00-00-00-00 the most significant byte is 06 (hex), the binary form of which is 00000110, where the second-least-significant bit is 1. Therefore, it is a locally administered address. Consequently, this bit is 0 in all OUIs.

- If the least significant bit of the most significant octet of an address is set to 0 (zero), the frame is meant to reach only one receiving NIC. This type of transmission is called unicast.
- A unicast frame is transmitted to all nodes within the collision domain, which typically ends at the nearest network switch or router.
- Only the node with the matching hardware MAC address will accept the frame; network frames with non-matching MAC-addresses are ignored, unless the device is in promiscuous mode.

4.2 CHANNEL ALLOCATION PROBLEM:

- Networks can be divided into two categories:
  - Networks those are using point-to-point connections and
  - Networks those using broadcast channels.
- In any broadcast network, the key issue is how to determine who gets to use the channel when there is competition for it.
- Broadcast channels are sometimes referred to as **multi-access channels** or **random access channels**.
- The MAC sub layer is especially important in LANs, many of which use a multi access channel as the basis for communication. WANs, in contrast, use point-to-point links, except for satellite networks.
- **Static Channel Allocation in LANs and MANs**
  - ***Frequency Division Multiplexing (FDM):*** If there are *N* users, the bandwidth is divided into *N* equal-sized portions, each user being assigned one portion.

    Drawback of FDM: FDM is a simple and efficient allocation mechanism. But, when the number of senders is large and continuously varying or the traffic is bursty.

  - ***Time Division Multiplexing:*** Each user is statically allocated every *N*th time slot. If a user does not use the allocated slot. The same holds if we split up the networks physically.

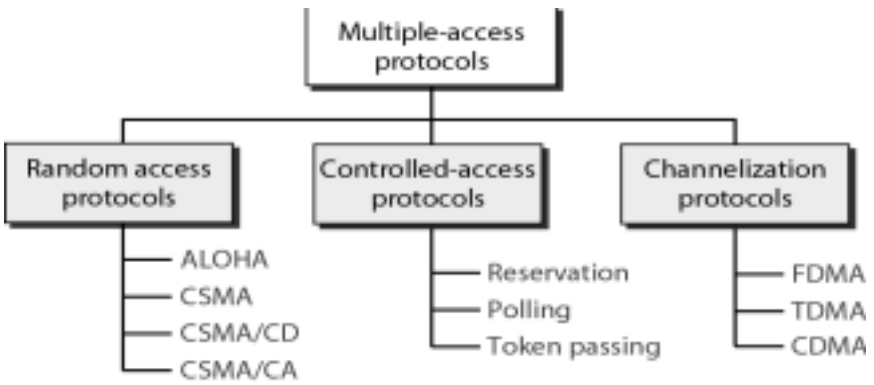
Prepared by K.SRIVIDYA

Medium Access Sub layer

- **Dynamic Channel Allocation in LANs and MANs**

Dynamic channel allocation problems have five key assumptions:

1. **Station Model.** The model consists of N independent stations (e.g., computers, telephones, or personal communicators), each with a program or user that generates frames for transmission. Stations are sometimes called terminals. Once a frame has been generated, the station is blocked and does nothing until the frame has been successfully transmitted.
2. **Single Channel Assumption.** A single channel is available for all communication. All stations can transmit on it and all can receive from it. As far as the hardware is concerned, all stations are equivalent, although protocol software may assign priorities to them.
3. **Collision Assumption.** If two frames are transmitted simultaneously, they overlap in time and the resulting signal is garbled. This event is called a collision. All stations can detect collisions. A collided frame must be transmitted again later. There are no errors other than those generated by collisions.
4. **a. Continuous Time.** Frame transmission can begin at any instant. There is no master clock dividing time into discrete intervals.
   Slotted Time. Time is divided into discrete intervals (slots). Frame transmissions always begin at the start of a slot. A slot may contain 0, 1, or more frames, corresponding to an idle slot, a successful transmission, or a collision, respectively.
5. **a. Carrier Sense.** Stations can tell if the channel is in use before trying to use it. If the channel is sensed as busy, no station will attempt to use it until it goes idle.
   b. No Carrier Sense. Stations cannot sense the channel before trying to use it. They just go ahead and transmit. Only later can they determine whether the transmission was successful.



4.2.1 ALOHA

- ALOHA, the earliest random access method, was developed at the University of Hawaii in early 1970.
- It was designed for a radio (wireless) LAN, but it can be used on any shared medium.

Prepared by K.SRIVIDYA

Medium Access Sub layer

• It is obvious that there are potential collisions in this arrangement. • The medium is shared between the stations. When a station sends data, another station may attempt to do so at the same time. The data from the two stations collide and become garbled.

• There are two forms of ALOHA

1. Pure ALOHA
2. Slotted ALOHA

• **Pure ALOHA**

▪ The original ALOHA protocol is called pure ALOHA. This is a simple, but elegant protocol.

▪ ***The idea is that each station sends a frame whenever it has a frame to send.*** ▪ Since there is only one channel to share, there is the possibility of collision between frames from different stations.

▪ A collision involves two or more stations.

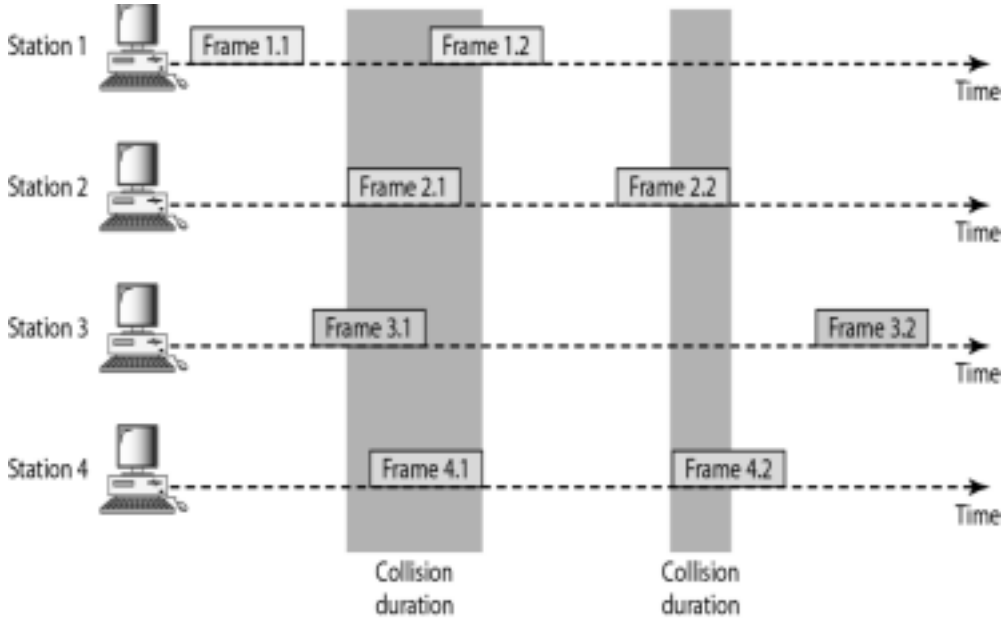


Figure: Pure ALOHA

▪ The pure ALOHA protocol relies on ***acknowledgments*** from the receiver.

- When a station sends a frame, it expects the receiver to send an acknowledgment.
- If the acknowledgment does not arrive after a time-out period, the station assumes that the frame (or the acknowledgment) has been destroyed and resends the frame.
- If all these stations try to resend their frames after the time-out, the frames will collide again.

▪ **Collision Prevention in Pure ALOHA:**

- Pure ALOHA dictates that when the time-out period passes, each station waits a random amount of time before resending its frame.
- After a maximum number of retransmission attempts Kmax' a station must give up and try later.

Prepared by K.SRIVIDYA

Medium Access Sub layer

- **Vulnerable Time:** The length of the collision is given by the Vulnerable Time.

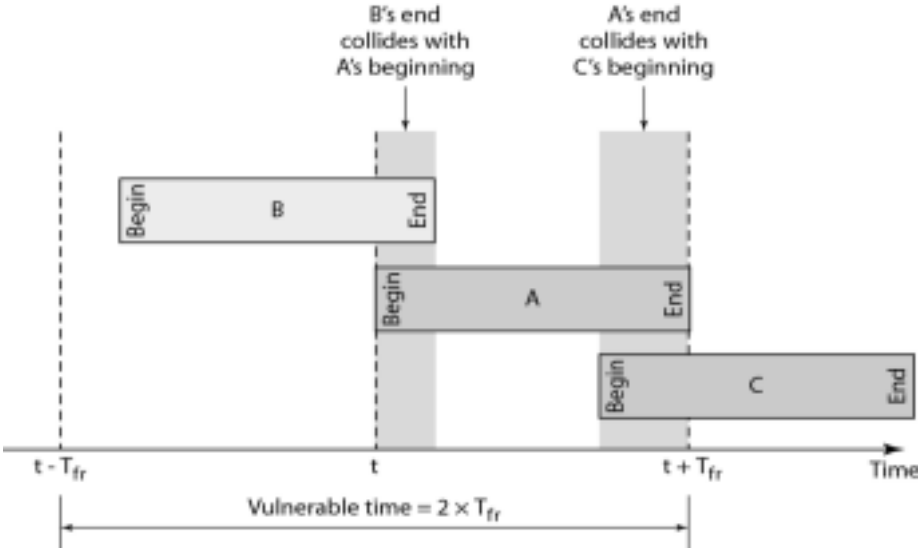


Figure: Vulnerable Time of Pure ALOHA

- Let us assume that the stations send fixed-length frames with each frame taking T_{fr} s to send.
- The Above figure gives the vulnerable time of the Station A, Station A sends a frame at time *t*. Now imagine station B has already sent a frame between $t - T_{fr}$ and *t*. This leads to a collision between the frames from station A and station B. The end of B's frame collides with the beginning of A's frame.
- On the other hand, suppose that station C sends a frame between *t* and $t+T_{fr}$. Here, there is a collision between frames from station A and station C. The beginning of C's frame collides with the end of A's frame.
- The vulnerable time, during which a collision may occur in pure ALOHA, is 2 times the frame transmission time.

Pure ALOHA vulnerable time = 2 x T_{fr}

- **Slotted ALOHA**
  - Slotted ALOHA was invented to improve the efficiency of pure ALOHA. In slotted ALOHA we divide the time into slots of T_{fr} s and force the station to send only at the beginning of the time slot.
  - Because a station is allowed to send only at the beginning of the synchronized time slot, if a station misses this moment, it must wait until the beginning of the next time slot. This means that the station which started at the beginning of this slot has already finished sending its frame.
  - There is still the possibility of collision if two stations try to send at the beginning of the same time slot.

Prepared by K.SRIVIDYA

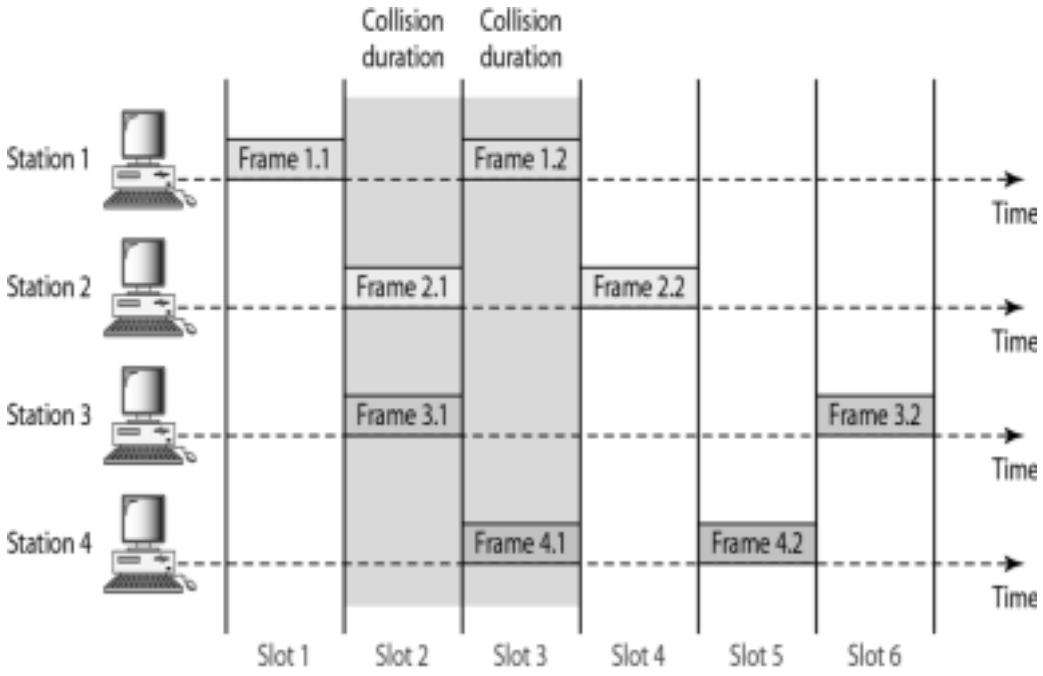


Figure: Slotted ALOHA

- **Vulnerable Time:** The vulnerable time for slotted ALOHA is one-half that of pure ALOHA.

Slotted ALOHA vulnerable time = T_{fr}

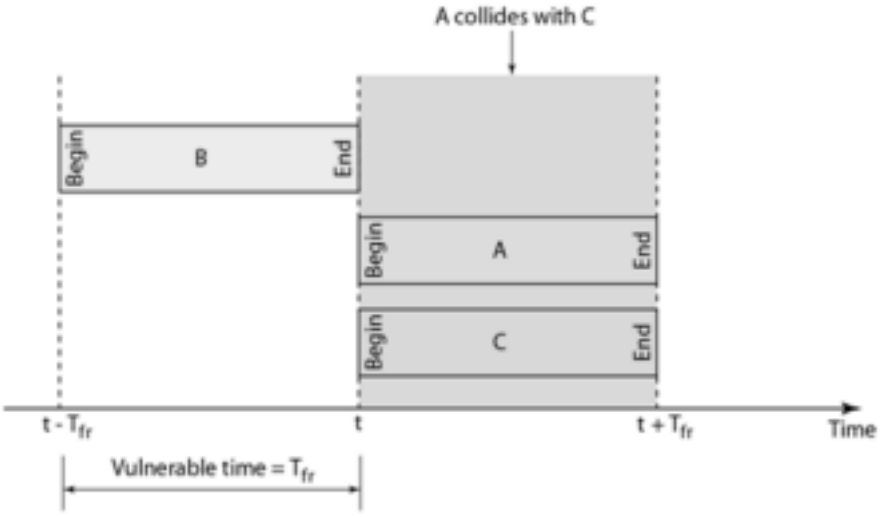


Figure: Vulnerable Time of Slotted ALOHA

Prepared by K.SRIVIDYA

Medium Access Sub layer

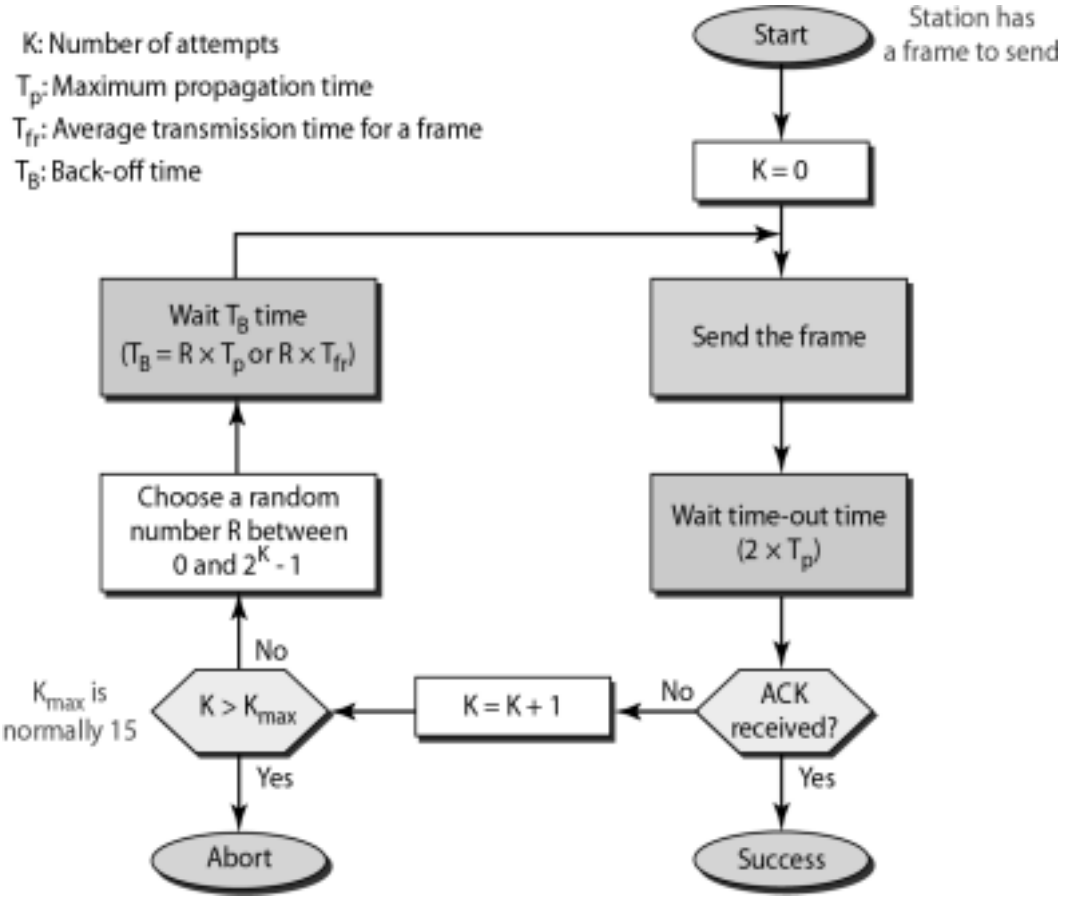


Figure: Flow Diagram for ALOHA

- **Throughput:**
  - The average number of successful transmissions for slotted ALOHA is $S = G \times e^{-G}$.
  - The maximum throughput Smax is 0.368, when G = 1. In other words, if a frame is generated during one frame transmission time, then 36.8 percent of these frames reach their destination successfully. This result can be expected because the vulnerable time is equal to the frame transmission time.
  - If a station generates only one frame in this vulnerable time (and no other station generates a frame during this time), the frame will reach its destination successfully.

The throughput for slotted ALOHA is $S =: G \times e^{-G}$.

The maximum throughput S_{max} == 0.368 when G=1.

4.2.2 CSMA:(Carrier Sense Multiple Access)

- To minimize the chance of collision and, therefore, increase the performance, the CSMA method was developed.
- The chance of collision can be reduced if a station senses the medium before trying to use it.
- Carrier sense multiple access (CSMA) requires that each station first listen to the medium (or check the state of the medium) before sending. In other words, CSMA is based on the principle "sense before transmit" or "listen before talk."

• CSMA can reduce the possibility of collision, but it cannot eliminate it. • Stations are connected to a shared channel (usually a dedicated medium). • The possibility of collision still exists because of ***propagation delay***; when a station sends a frame, it still takes time (although very short) for the first bit to reach every station and for every station to sense it.

- In other words, a station may sense the medium and find it idle, only because the first bit sent by another station has not yet been received.

• At time $t_1$station B senses the medium and finds it idle, so it sends a frame. • At time *t2* $(t_2 > t_1)$ station C senses the medium and finds it idle because, at this time, the first bits from station B have not reached station C. Station C also sends a frame. • The two signals collide and both frames are destroyed.

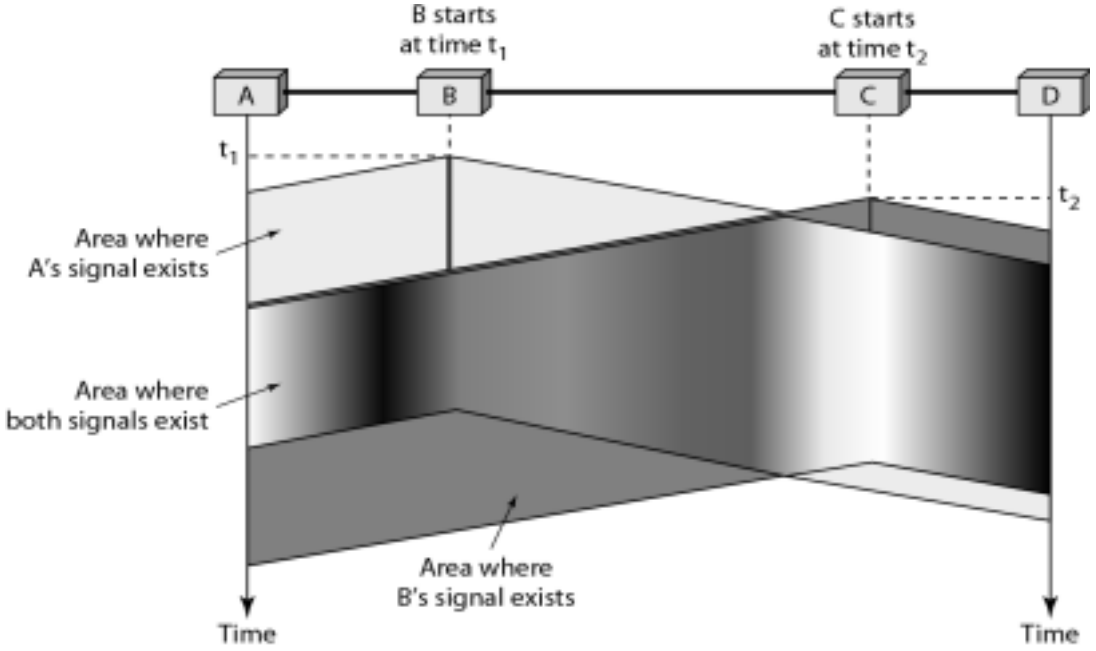


Figure: Collision in CSMA

- **Vulnerable Time of CSMA:**
  - The vulnerable time for CSMA is the **propagation time T_p**. This is the time needed for a signal to propagate from one end of the medium to the other. ▪ When a station sends a frame, and any other station tries to send a frame during this time, a collision will result. But if the first bit of the frame reaches the end of the

medium, every station will already have heard the bit and will refrain from sending.

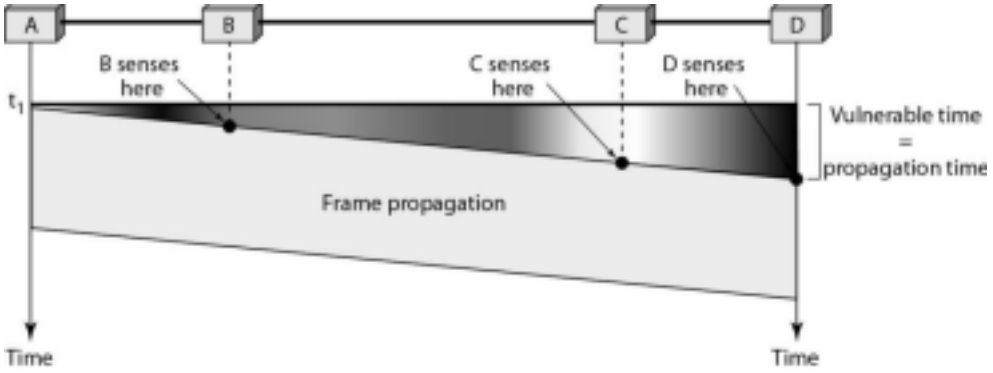


Figure: Vulnerable Time of CSMA

- **Persistence Methods of CSMA:**
  - There are three methods for CSMA persistence
    1. **1-persistent CSMA**
    2. **Non Persistent CSMA**
    3. **P-persistent CSMA**
  - **1-Persistennt CSMA:**
    - The **I-persistent method** is simple and straightforward.
    - **In** this method, after the station finds the line idle, it sends its frame immediately (with probability 1).

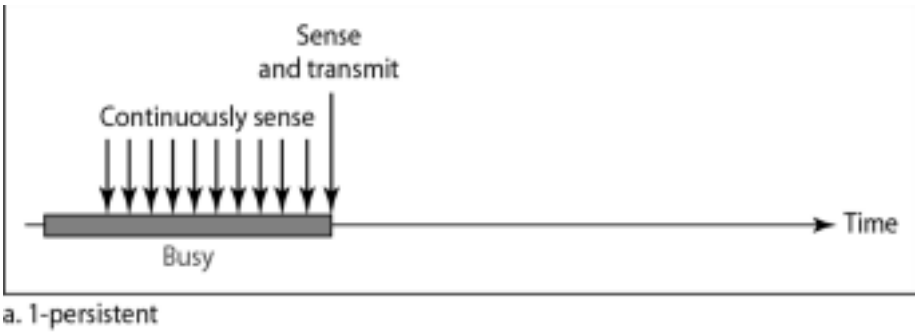


Figure: 1-Persistent CSMA

- This method has the highest chance of collision because two or more stations may find the line idle and send their frames immediately.

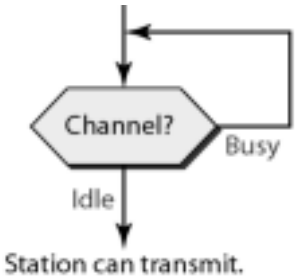
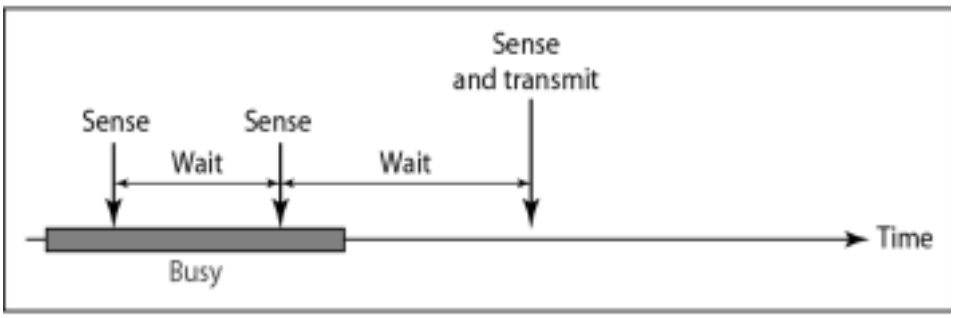


Figure: Flow Diagram of 1-Persistent CSMA

  - **Non Persistent CSMA:**
    - In the Non Persistent Method, a station that has a frame to send
    - senses the line. If the line is idle, it sends immediately. If the line is not idle, it waits a random amount of time and then senses the line again.

- The Non Persistent approach reduces the chance of collision because it is unlikely that two or more stations will wait the same amount of time and retry to send simultaneously.
- This method reduces the efficiency of the network because the medium remains idle when there may be stations with frames to send.



b. Nonpersistent

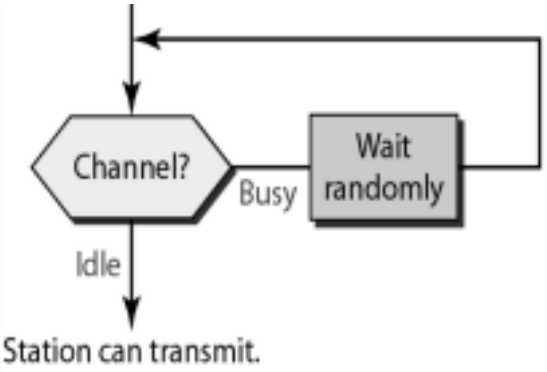
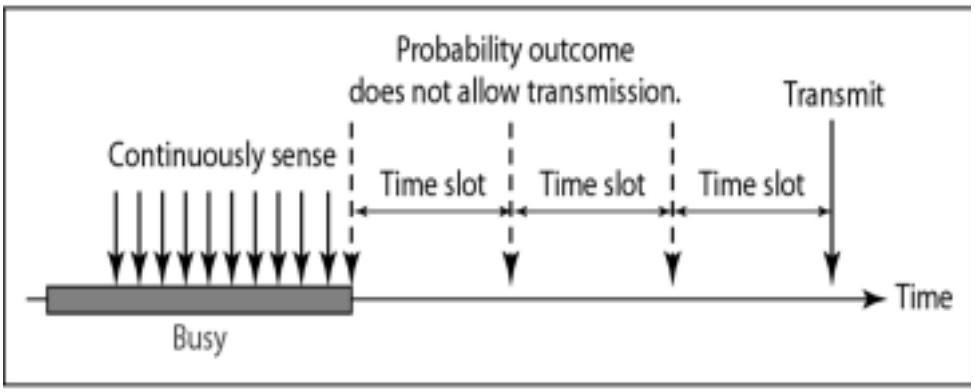


Figure: Flow diagram for Non Persistent CSMA

- **P-Persistent CSMA:**
  - The p-persistent method is used if the channel has time slots with a slot duration equal to or greater than the maximum propagation time.
  - The p-persistent approach combines the advantages of the other two strategies.
  - It reduces the chance of collision and improves efficiency.

  - In this method, after the station finds the line idle it follows these steps:
    1. With probability *p,* the station sends its frame.
    2. With probability $q = 1 - p$, the station waits for the beginning of the next time slot and checks the line again.
       a. If the line is idle, it goes to step 1.
       b. If the line is busy, it acts as though a collision has occurred and uses the back-off procedure.



c. p-persistent

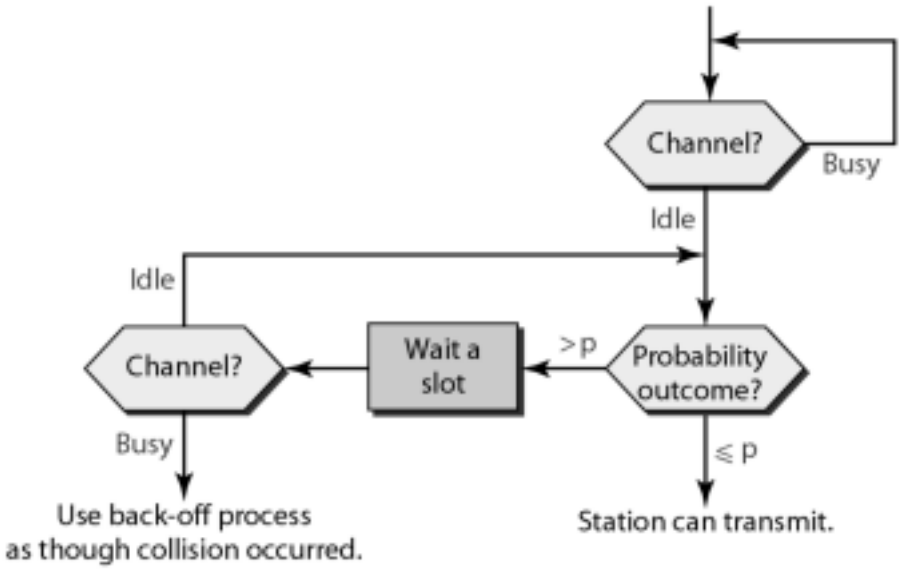


Figure: Flow Diagram for P-Persistent CSMA

4.2.3 CSMA/CD (Carrier Sense Multiple Access with Collision Detection): • 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.

• To better understand CSMA/CD, let us look at the first bits transmitted by the two stations involved in the collision. Although each station continues to send bits in the frame until it detects the collision.

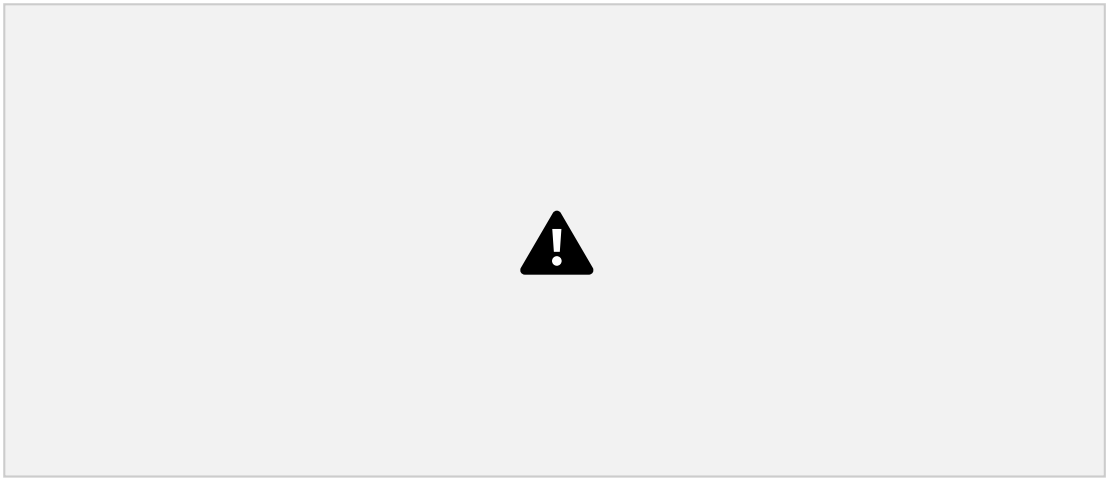


Figure: Collision of the first bit in CSMA/CD

• At time t_1, station A has executed its persistence procedure and starts sending the bits of its frame.

• At time t_2, station C has not yet sensed the first bit sent by A. Station C executes its persistence procedure and starts sending the bits in its frame, which propagate both to the left and to the right. The collision occurs sometime after time t_2 Station C detects a

collision at time *t3* when it receives the first bit of A's frame. Station C immediately (or after a short time, but we assume immediately) aborts transmission. • **Minimum Frame Size:** Each frame must be large enough for a sender to detect a collision.

• **Energy Level:**

▪ The level of energy in a channel can have three values: zero, normal, and abnormal.

▪ At the zero level, the channel is idle. This level is also called ***Idle Period.*** ▪ At the normal level, a station has successfully captured the channel and is sending its frame. This level is called ***Transmission Period.***

▪ At the abnormal level, there is a collision and the level of the energy is twice the normal level. This is called ***Contention Period.***

▪ A station that has a frame to send or is sending a frame needs to monitor the energy level to determine if the channel is idle, busy, or in collision mode.

Figure: Energy levels in CSMA/CD

Prepared by K.SRIVIDYA

Medium Access Sub layer

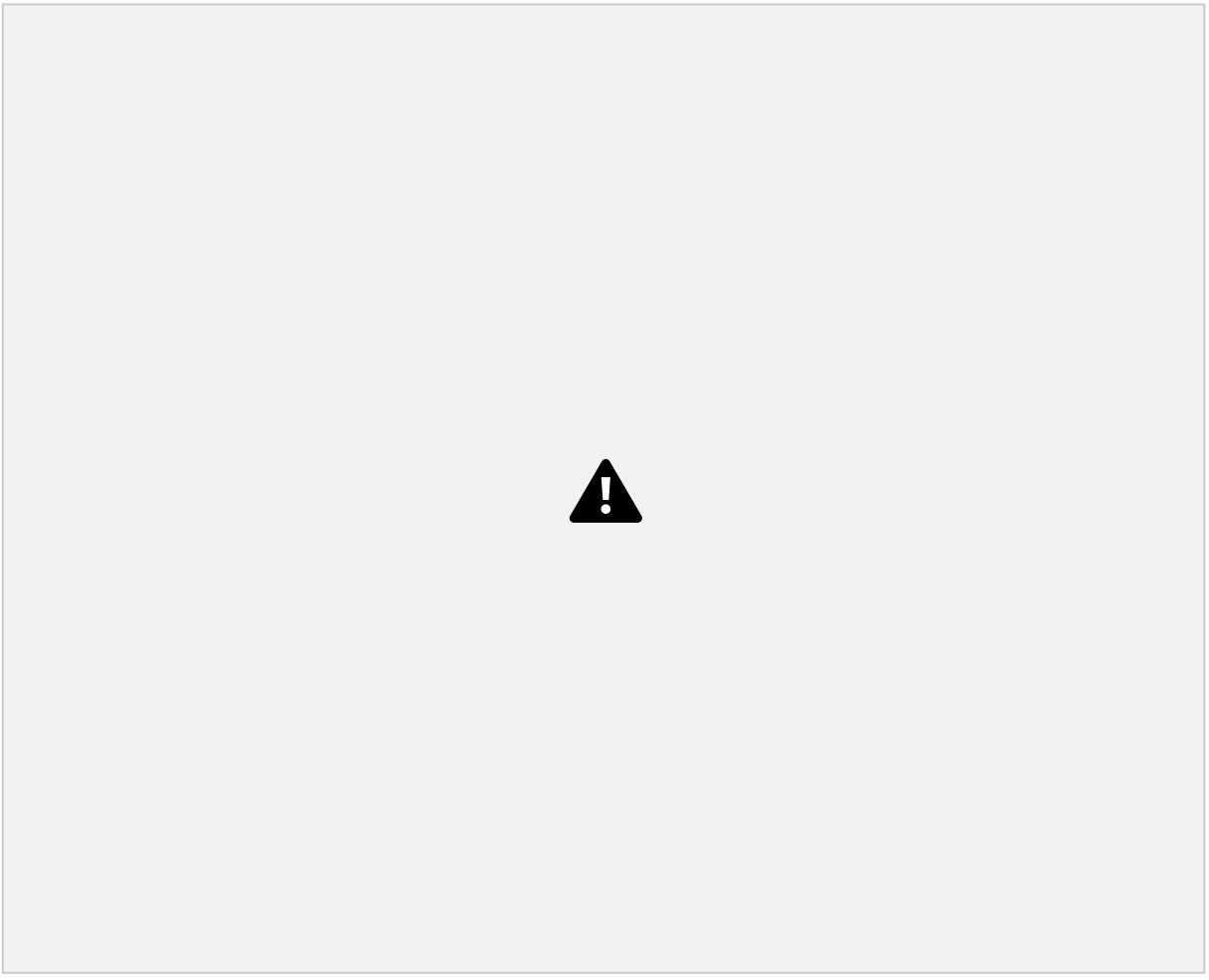
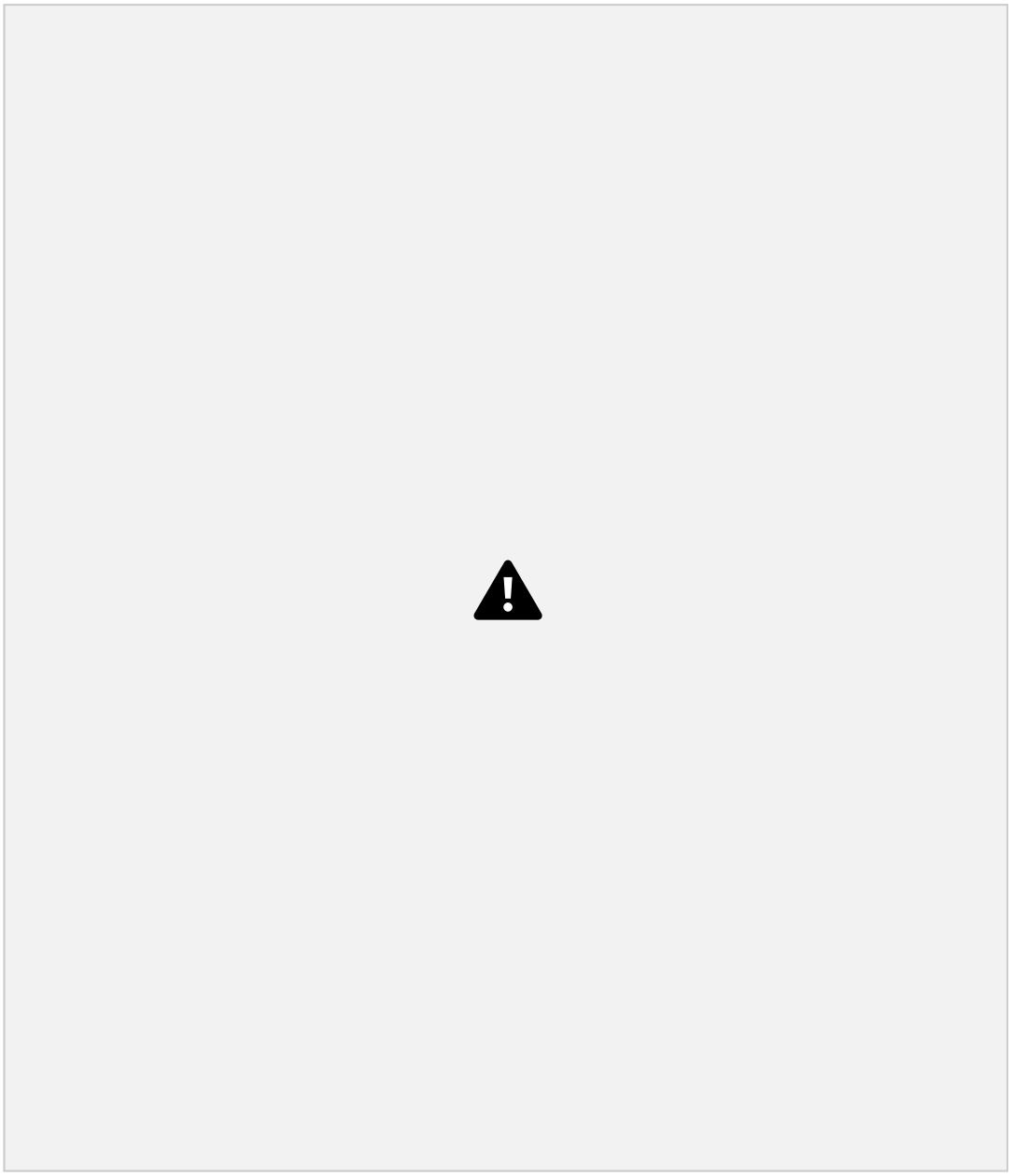


Figure: Flow Diagram for CSMA/CD



4.2.4 CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance): • The basic idea behind *CSMA/CD* is that a station needs to be able to receive while transmitting to detect a collision. The signal from the second station needs to add a significant amount of energy to the one created by the first station.

- In a wired network, the received signal has almost the same energy as the sent signal because either the length of the cable is short or there are repeaters that amplify the energy between the sender and the receiver. This means that in a collision, the detected energy almost doubles.
- In a wireless network, much of the sent energy is lost in transmission. The received signal has very little energy. Therefore, a collision may add only 5 to 10 percent additional energy. This is not useful for effective collision detection.
- Carrier sense multiple access with collision avoidance *(CSMA/CA)* was invented for this network.
- Collisions are avoided through the use of CSMA/CA's three strategies: ***The Interframe Space, The Contention Window, and Acknowledgments*** ▪ **Interframe Space:**

- Collisions are avoided by deferring transmission even if the channel is found idle.
- When an idle channel is found, the station does not send immediately.
- It waits for a period of time called the interframe space or IFS.
- The IFS time allows the front of the transmitted signal by the distant station to reach this station.
- If after the IFS time the channel is still idle, the station can send, but it still needs to wait a time equal to the contention time.
- The IFS variable can also be used to prioritize stations or frame types. For example, a station that is assigned a shorter IFS has a higher priority.

▪ **The Contention Window:**

- The contention window is an amount of time divided into slots.
- A station that is ready to send chooses a random number of slots as its wait time. The number of slots in the window changes according to the binary exponential back-off strategy. This means that it is set to one slot the first time and then doubles each time the station cannot detect an idle channel after the IFS time. This is very similar to the p persistent method except that a random outcome defines the number of slots taken by the waiting station.
- The contention window is that the station needs to sense the channel after each time slot.
- If the station finds the channel busy, it does not restart the process; it just stops the timer and restarts it when the channel is sensed as idle. This gives priority to the station with the longest waiting time.

▪ **Acknowledgements:**

- The data may be corrupted during the transmission. The positive acknowledgment and the time-out timer can help guarantee that the receiver has received the frame.

Figure: The Interframe Space, The Contention Window, and Acknowledgments

• ***CSMA/CA*** was mostly intended for use in **wireless networks.**

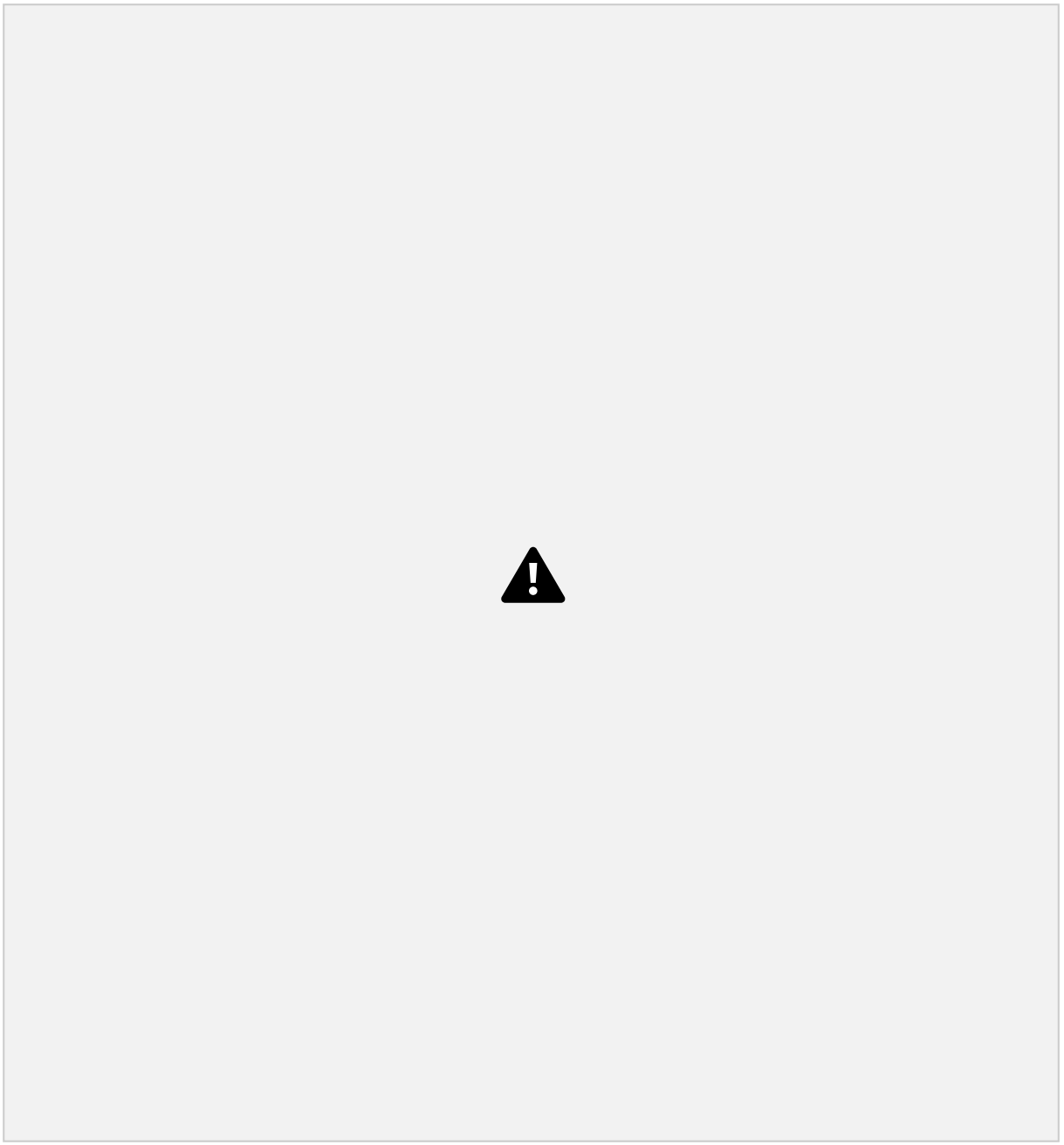


Figure: Flow Diagram of CSMA/CA

4.3 ETHERNET:

• Ethernet is IEEE 802.3 standard. This is a dominant LAN technology and cheaper. • Ethernet is used for Wired LANs.

• **Ethernet Frame Format:**

Figure: Ethernet Frame

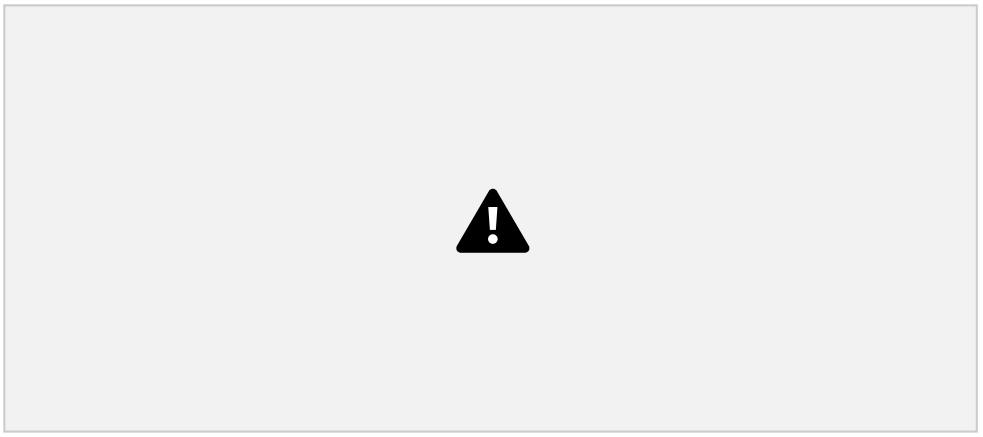
The field defined as

- **Preamble:** The first field of the 802.3 frame contains 7 bytes (56 bits) of alternating 0s and 1s that alerts the receiving system to the coming frame and enables it to synchronize its input timing. The preamble is actually added at the physical layer and is not (formally) part of the frame.
- **Start frame delimiter (SFD):** The second field (l byte: 10101011) signals the beginning of the frame. The SFD warns the station or stations that this is the last chance for synchronization. The last 2 bits is 11 and alerts the receiver that the next field is the destination address.
- **Destination address (DA):** The DA field is 6 bytes and contains the physical address of the destination station or stations to receive the packet.
- **Source address (SA):** The SA field is also 6 bytes and contains the physical address of the sender of the packet.
- **Length or type:** This field is defined as a type field or length field. The original Ethernet used this field as the type field to define the upper-layer protocol using the MAC frame. The IEEE standard used it as the length field to define the number of bytes in the data field.
- **Data:** This field carries data encapsulated from the upper-layer protocols. It is a minimum of 46 and a maximum of 1500 bytes.
- **CRC:** The last field contains error detection information, in this case a CRC 32

• Ethernet has gone through 4 generations.

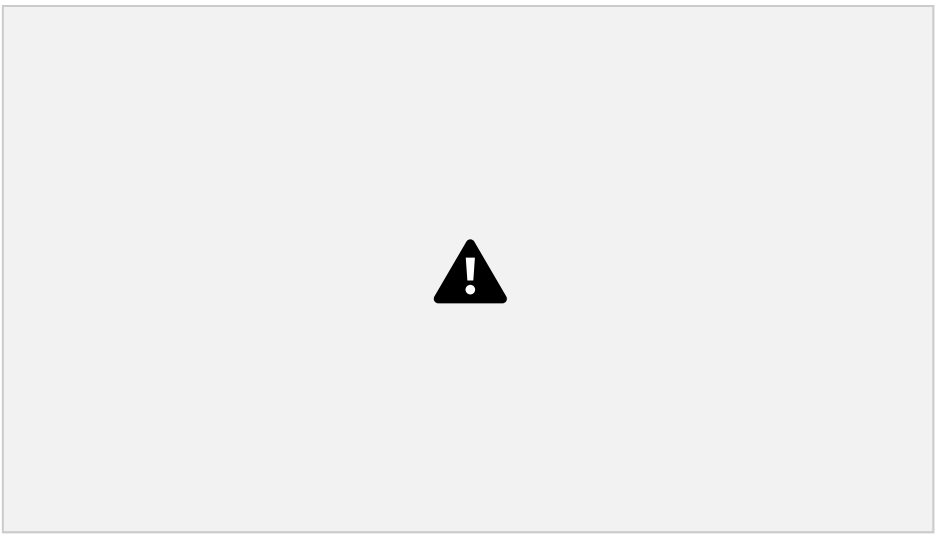
Figure: Four Versions of Ethernet.

• **Standard Ethernet:**



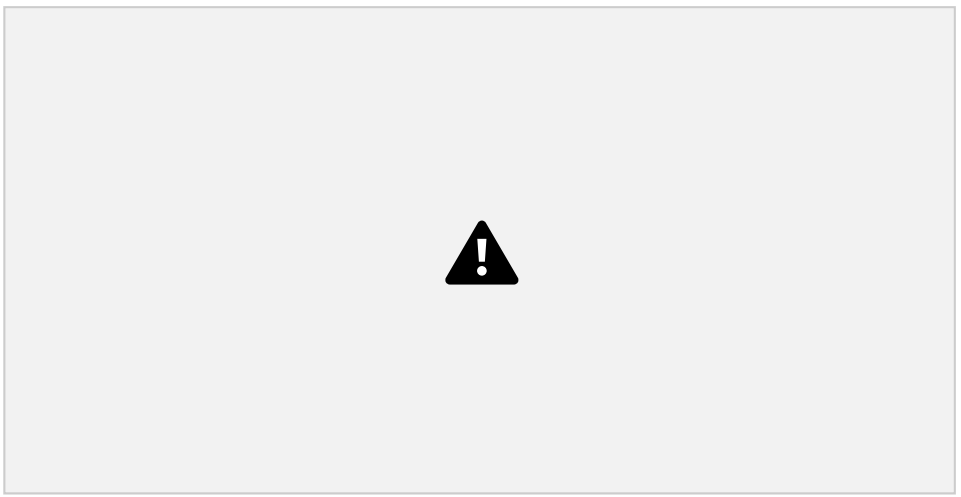
▪ **10 Base 5:** ***Thick Ethernet***

- The first implementation is called 10BaseS, thick Ethernet, or Thicknet. The name derived from the size of the cable, which is roughly the size of a garden hose and too stiff to bend with your hands.
- 10Base5 was the first Ethernet specification to use a bus topology with an external transceiver (transmitter/receiver) connected via a tap to a thick coaxial cable.
- The transceiver is responsible for transmitting, receiving, and detecting collisions. The transceiver is connected to the station via a transceiver cable that provides separate paths for sending and receiving. This means that collision can only happen in the coaxial cable.
- The maximum length of the coaxial cable must not exceed ***500*m,** otherwise, there is excessive degradation of the signal. If a length of more than *500* m is needed, up to five segments, each a maximum of 500-meter, can be connected using repeaters.



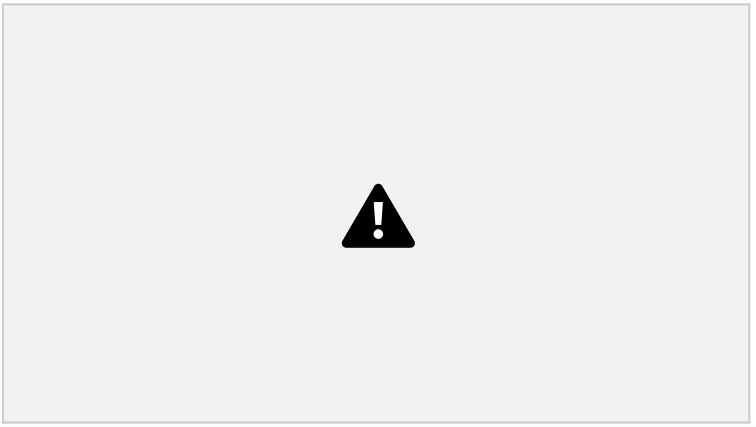
▪ **10 Base 2:** ***Thin Ethernet***

- The second implementation is called 10Base2, thin Ethernet, or Cheapernet.
- 10Base2 also uses a bus topology, but the cable is much thinner and more flexible.
- The cable can be bent to pass very close to the stations. In this case, the transceiver is normally part of the network interface card (NIC), which is installed inside the station.
- This cable is less expensive than 10Base5. Installation is also simple.



▪ **10 Base T:** ***Twisted-Pair Ethernet***

- The third implementation is called 10Base-T or twisted-pair Ethernet. 10Base-T uses a physical star topology.

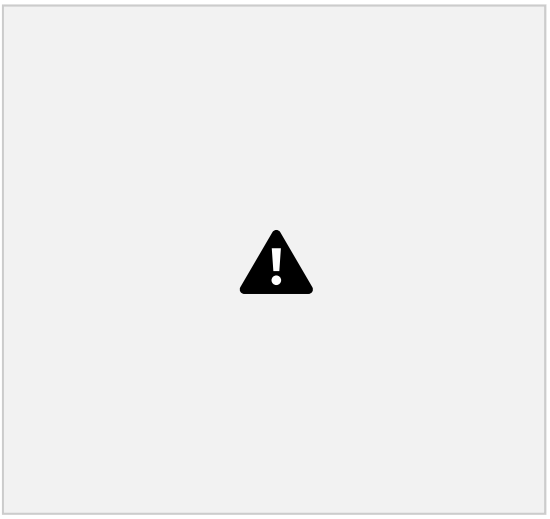


- The stations are connected to a hub via two pairs of twisted cable. ○ Two pairs of twisted cable create two paths (one for sending and one for receiving) between the station and the hub.
- Any collision here happens in the hub.

- Compared to 10BaseS or 10Base2, we can see that the hub actually replaces the coaxial cable as far as a collision is concerned.
- The maximum length of the twisted cable here is defined as 100 m, to minimize the effect of attenuation in the twisted cable.

▪ **10 Base F:** ***Fiber Ethernet***

- 10Base-F uses a star topology to connect stations to a hub. The stations are connected to the hub using two fiber-optic cables.



- **Manchester Encoding:**
  - All standard implementations use digital signaling (baseband) at 10 Mbps.
  - At the sender, data are converted to a digital signal using the Manchester scheme.
  - at the receiver, the received signal is interpreted as Manchester and decoded into data.
  - Manchester encoding is self-synchronous, providing a transition at each bit interval.

Figure: Encoding and Decoding in Standard Ethernet

Medium Access Sub layer

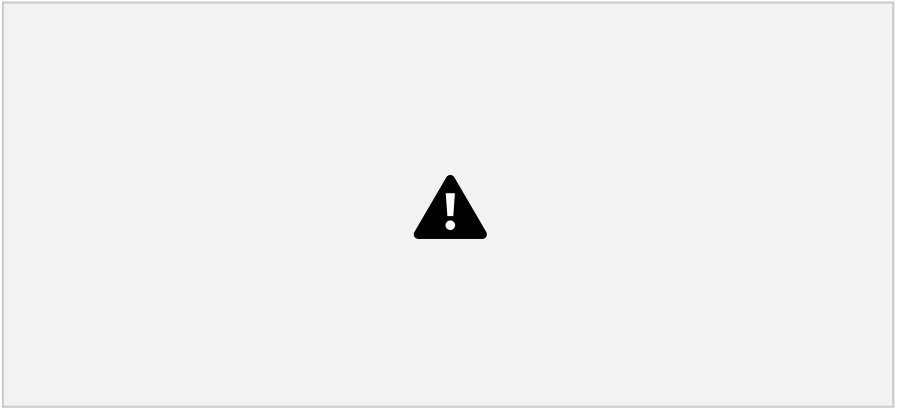
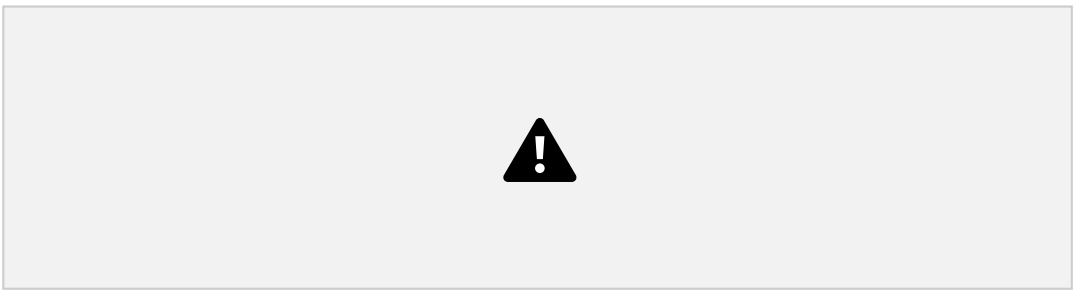
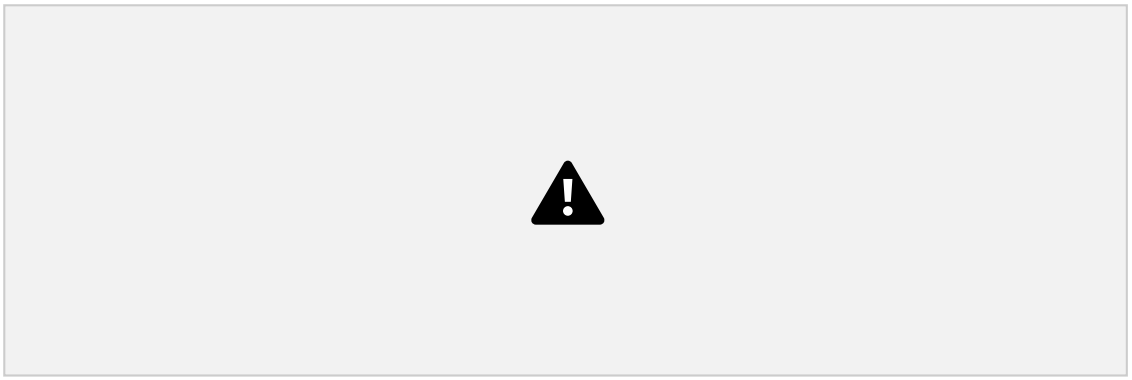


Figure: Manchester Encoding

▪ **Comparison of Standard Ethernet Implementations:**



• **Fast Ethernet: IEEE 802.3u**



▪ **100 Base-TX:**

- 100 Base-TX uses two pairs of twisted-pair cable (either category 5 UTP or STP).For encoding **4B/5B** block coding is used to provide bit synchronization by preventing the occurrence of a long sequence of 0s and 1s. This creates a data rate of 125 Mbps, which is fed into **MLT-3** for encoding.

Figure: Encoding and Decoding in 100 Base-TX

▪ **100 Base-FX:**

- 100Base-FX uses two pairs of fiber-optic cables.
- Optical fiber can easily handle high bandwidth requirements by using simple encoding schemes.
- The designers of 100Base-FX selected the NRZ-I encoding scheme for this implementation. **NRZ-I** has a bit synchronization problem for long sequences of 0s (or 1s, based on the encoding). To overcome this problem, the designers used **4B/5B.**

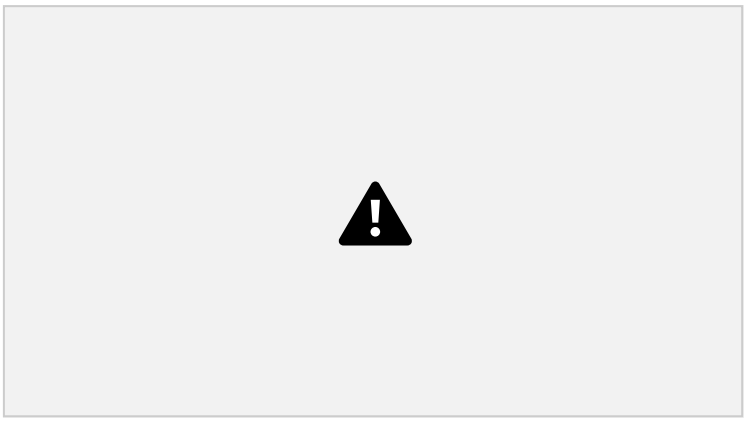


Figure: Encoding and Decoding in 100 Base-FX

- **100 Base-T4:**
  - 100 Base-T4, was designed to use category 3 or higher UTP. The implementation uses four pairs of UTP for transmitting 100 Mbps. Encoding/decoding in 100Base-T4 is more complicated. Each twisted pair cannot easily handle more than 25 Mbaud.
  - Three pairs of UTP category 3, can handle only 75 Mbaud (25 Mbaud) each.
  - 100 Base-T4 uses **8B/6T** encoding. In 8B/6T, eight data elements are encoded as six signal elements. This means that 100 Mbps uses only (6/8) x 100 Mbps, or 75 Mbaud.

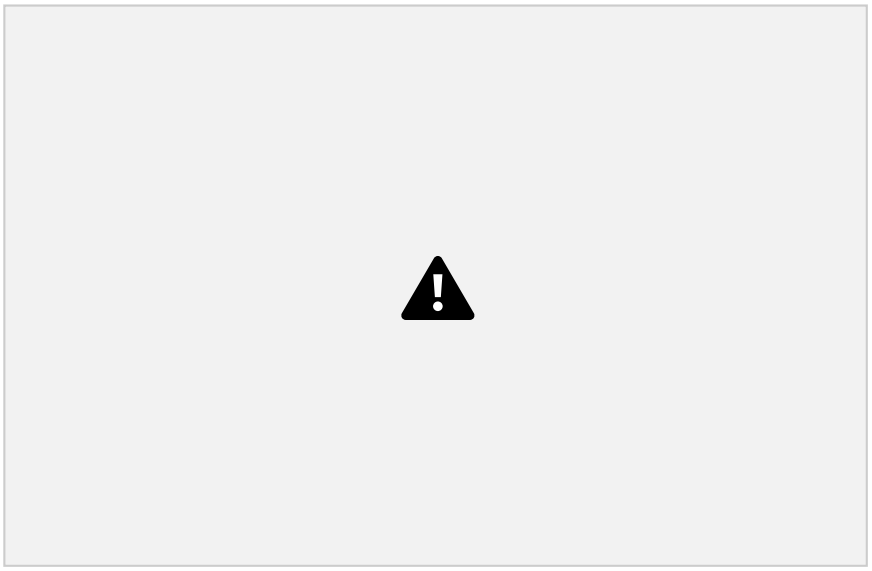
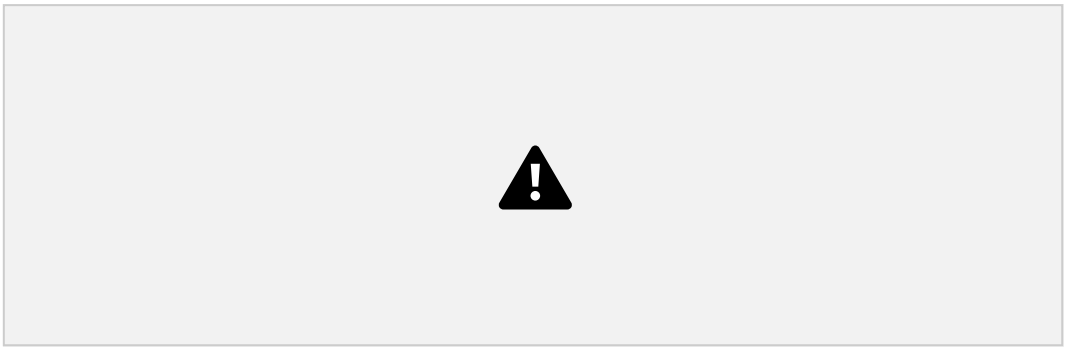
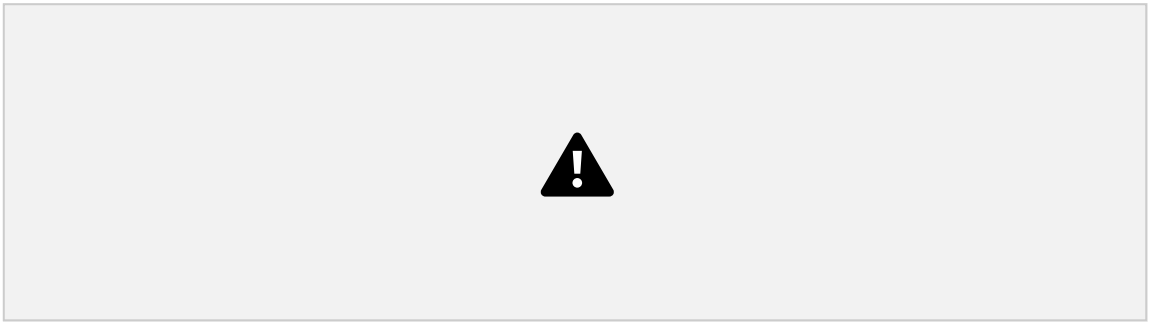


Figure: Encoding and Decoding in 100 Base-T4

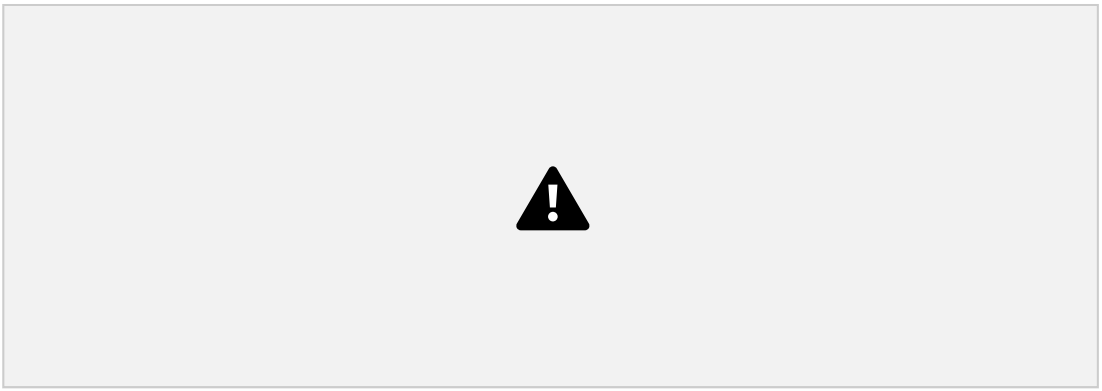
- **Fast Ethernet Summary:**



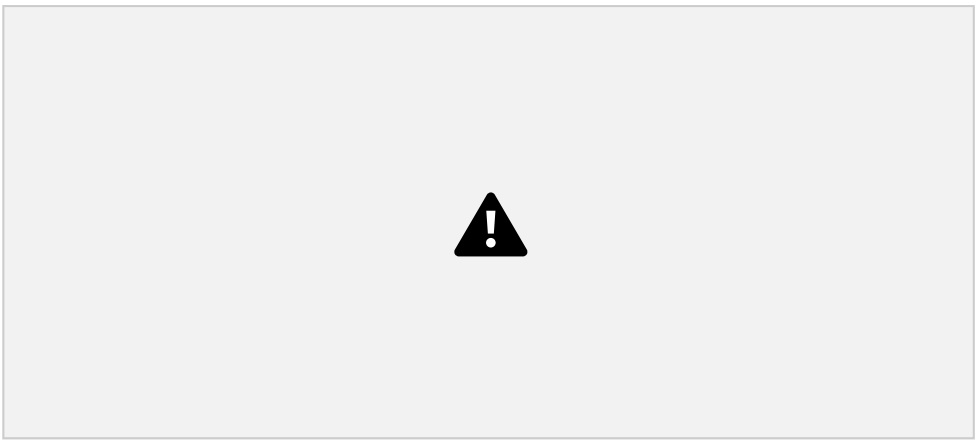
- **Gigabit Ethernet: IEEE 802.3z, 802.3ab**
  - The Data rate is 1Gbps



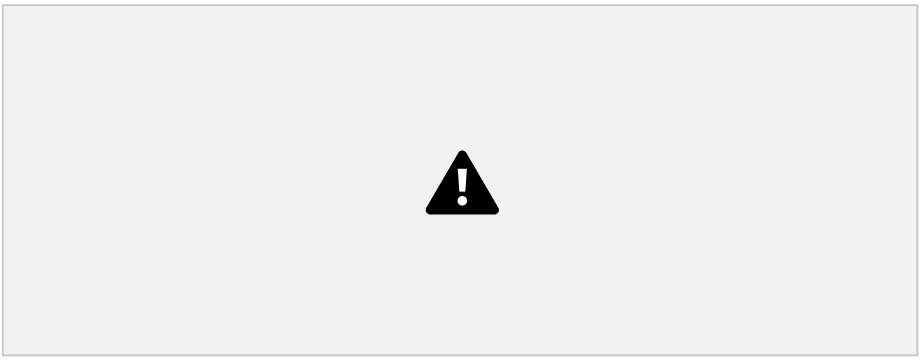
  - **Gigabit Ethernet Summary:**



  - **1000Base-SX:**



  - **1000Base T:**



• **10 Gigabit Ethernet: IEEE 802.3ae, 802.3ak, 802.3an**

1. Upgrade the data rate to 10 Gbps.
2. Make it compatible with Standard, Fast, and Gigabit Ethernet.
3. Use the same 48-bit address.
4. Use the same frame format.
5. Keep the same minimum and maximum frame lengths.
6. Allow the interconnection of existing LANs into a metropolitan area network (MAN) or a wide area network (WAN).
7. Make Ethernet compatible with technologies such as Frame Relay and ATM

▪ **10Gigabit Ethernet Summary:**

4.4. WIRELESS LANS

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

• **Architecture:**

▪ The standard defines two kinds of services:
The Basic Service Set (BSS) and **The extended service set (ESS).**

▪ ***Basic Service Set***

- IEEE 802.11 defines the basic service set (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).
- The BSS without an AP is a stand-alone network and cannot send data to other BSSs. It is called an ***ad hoc 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.***

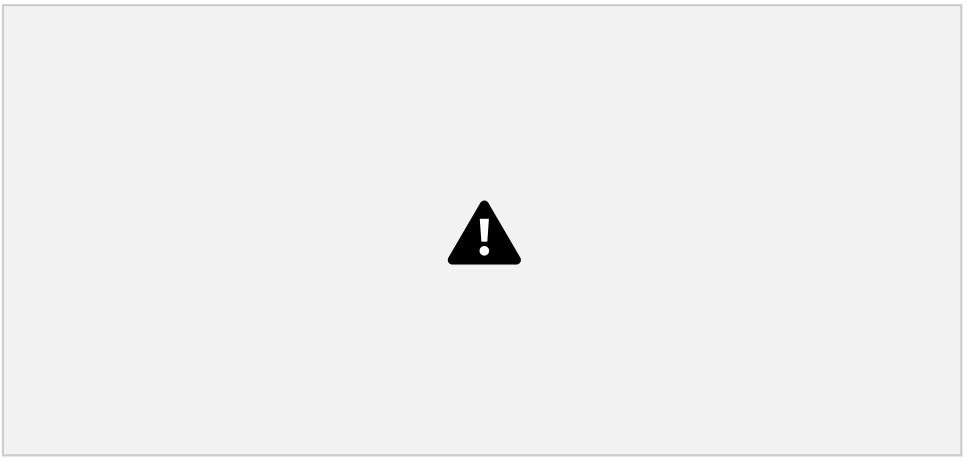


Figure: BSS with AP and Without AP

- **Extended Service Set:**
  - An extended service set (ESS) is made up of two or more BSSs with APs. In this case, the BSSs are connected through a *distribution system,* which is usually a wired LAN.
  - The distribution system connects the APs in the BSSs.
  - IEEE 802.11 does not restrict the distribution system; it can be any IEEE LAN such as an Ethernet.
  - The extended service set uses two types of stations: ***mobile and stationary.***
  - ***The mobile stations*** are normal stations inside a BSS.
  - ***The stationary stations*** are AP stations that are part of a wired LAN.
  - When BSSs are connected, the stations within reach of one another can communicate without the use of an AP. 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 a cell and each AP to be a base station.
  - A mobile station can belong to more than one BSS at the same time.

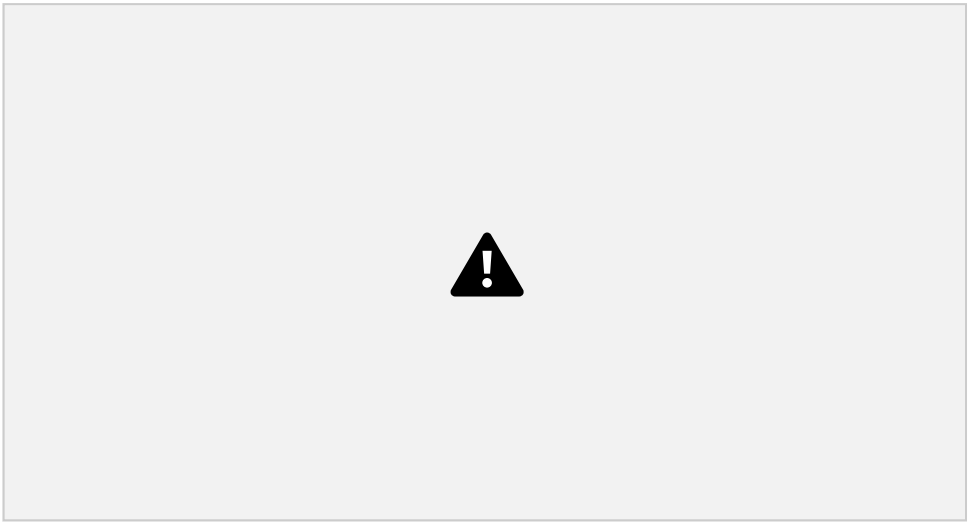
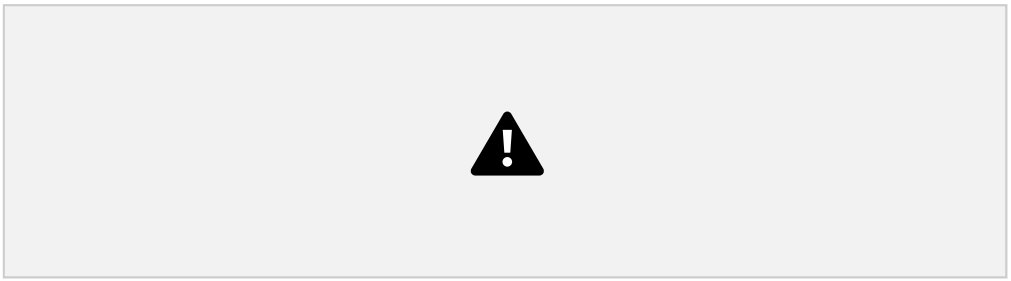
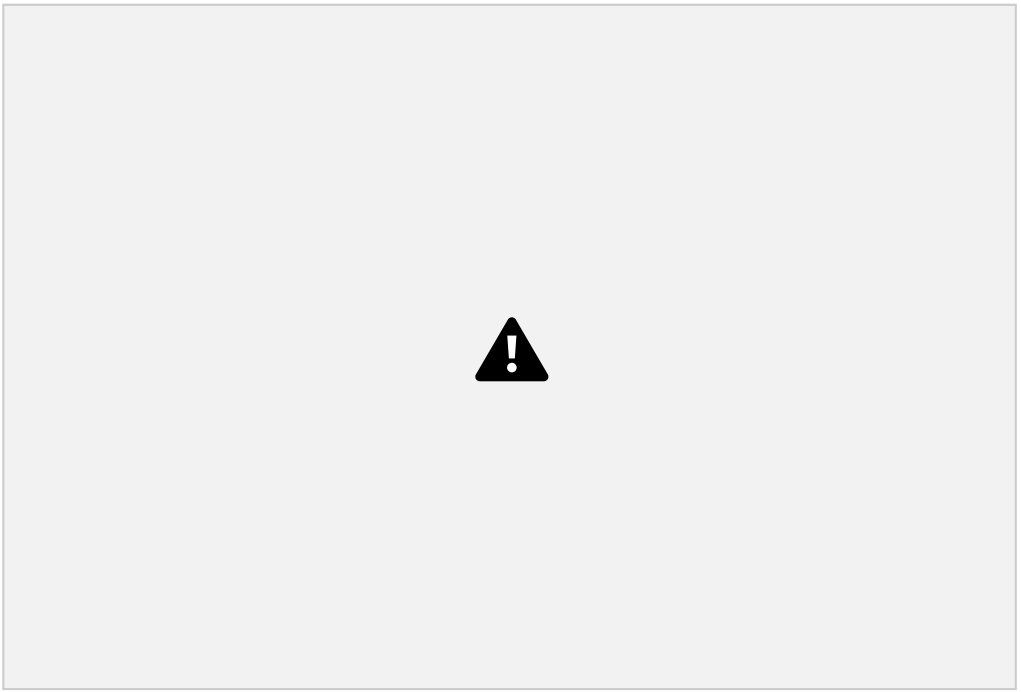


Figure: Extended Service Set.

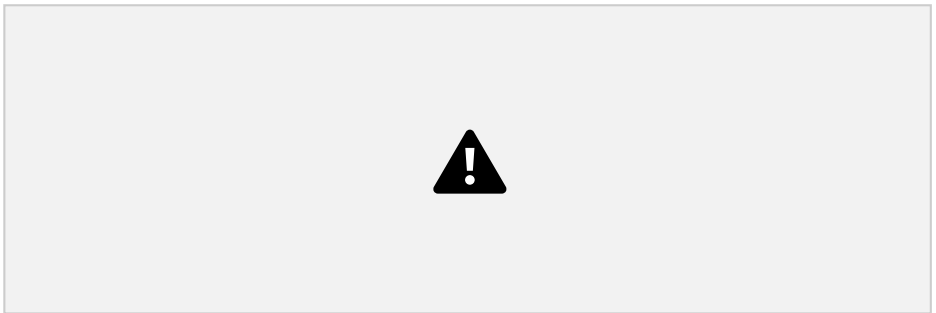
- **Frame Format:**



- **Frame control (FC):** The FC field is 2 bytes long and defines the type of frame and some control information.
  The Subfields of FC:



- **Addresses:** There are four address fields, each 6 bytes long. The meaning of each address field depends on the value of the ***To*** **DS** and ***From*** **DS** subfields.



- **Sequence control:** This field defines the sequence number of the frame to be used in flow control.
- **Frame body:** This field, which can be between 0 and 2312 bytes,

contains information based on the type and the subtype defined in the FC field.

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

Medium Access Sub layer

- ***Frame Types***
  - A wireless LAN defined by IEEE 802.11 has three categories of frames: ***management frames, control frames, and data frames.*** ***Management Frames:*** Management frames are used for the initial communication between stations and access points.
  - ***Control Frames:*** Control frames are used for accessing the channel and acknowledging frames.

  - ***Data Frames:*** Data frames are used for carrying data and control information.
- **Hidden Station Problem:**

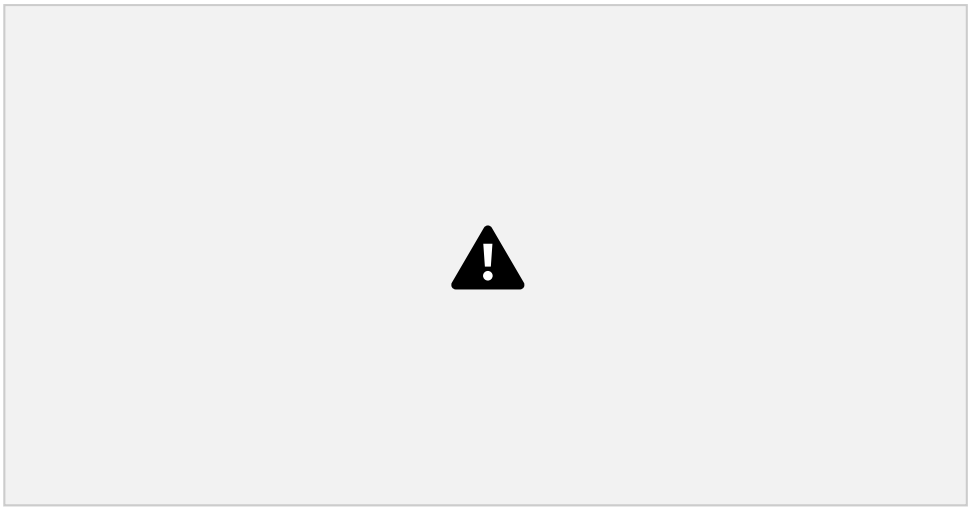


Figure: Hidden Station Problem

  - Figure shows an example of the hidden station problem.
  - Station B has a transmission range shown by the left oval (sphere in space); every station in this range can hear any signal transmitted by station B.
  - Station C has a transmission range shown by the right oval (sphere in space); every station located in this range can hear any signal

transmitted by C.

- Station C is outside the transmission range of B; likewise, station B is outside the transmission range of C.
- Station A, is in the area covered by both Band C; it can hear any signal transmitted by B or C.

- Assume that station B is sending data to station A. In the middle of this transmission, station C also has data to send to station A. Station C is out of B's range and transmissions from B cannot reach C. Therefore C thinks the medium is free.
- Station C sends its data to A, which results in a collision at A because this station is receiving data from both B and C.
- In this case, we say that stations ***Band C are hidden*** from each other with respect to A.
- Hidden stations can reduce the capacity of the network because of the possibility of collision.
- **Solution:**
  - ➢ Hidden Station Problem can be solved using the handshake frames (RTS and CTS).

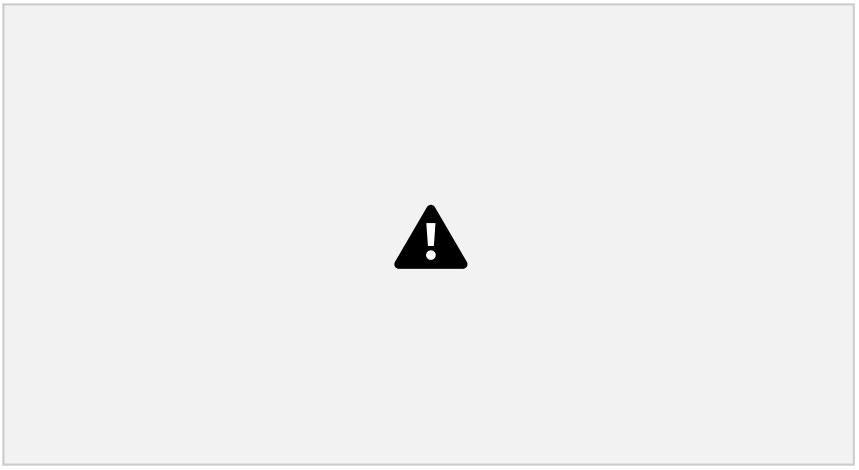


Figure: Use of handshaking to prevent hidden station problem

- ➢ Figure shows that the RTS message from B reaches A, but not C.
- ➢ Because both Band C are within the range of A, the CTS message, which contains the duration of data transmission from B to A reaches C.
- ➢ Station C knows that some hidden station is using the channel and refrains from transmitting until that duration is over.

▪ **Exposed Station Problem:**

- In this problem a station refrains from using a channel when it is, available.
- In Figure, station A is transmitting to station B.

- Station C has some data to send to station D, which can be sent without interfering with the transmission from A to B.
- Station C is exposed to transmission from A; it hears what A is sending and thus refrains from sending. In other words, C is too conservative and wastes the capacity of the channel.

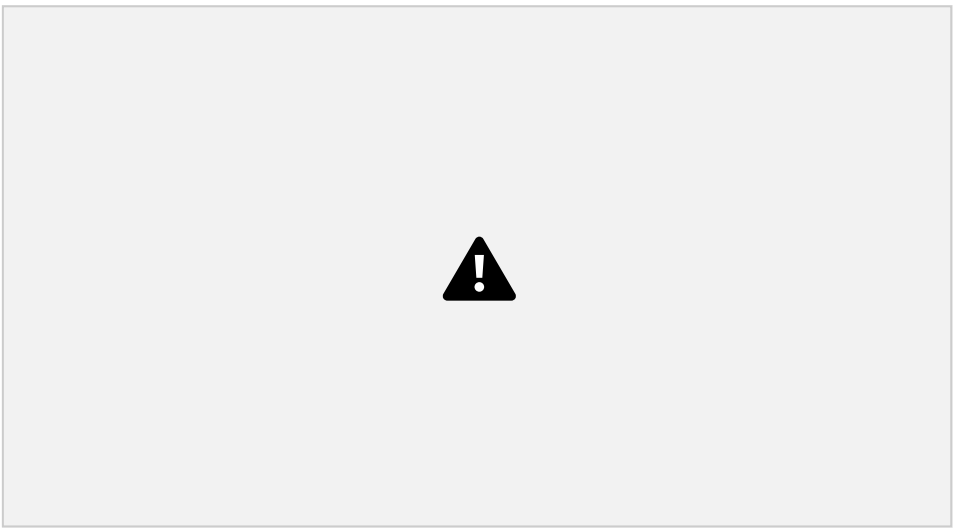


Figure: Exposed Station Problem

- **Solution:**

➢ The handshaking messages RTS and CTS cannot help in this case, despite what you might think.

➢ Station C hears the RTS from A, but does not hear the CTS from B. Station C, after hearing the RTS from A, can wait for a time so that the CTS from B reaches A; it then sends an RTS to D to show that it needs to communicate with D. Both stations B and A may hear this RTS, but station A is in the sending state, not the receiving state.

➢ Station B, responds with a CTS. The problem is here. If station A has started sending its data, station C cannot hear the CTS from station D because of the collision; it cannot send its data to D.

➢ It remains exposed until A finishes sending its data.

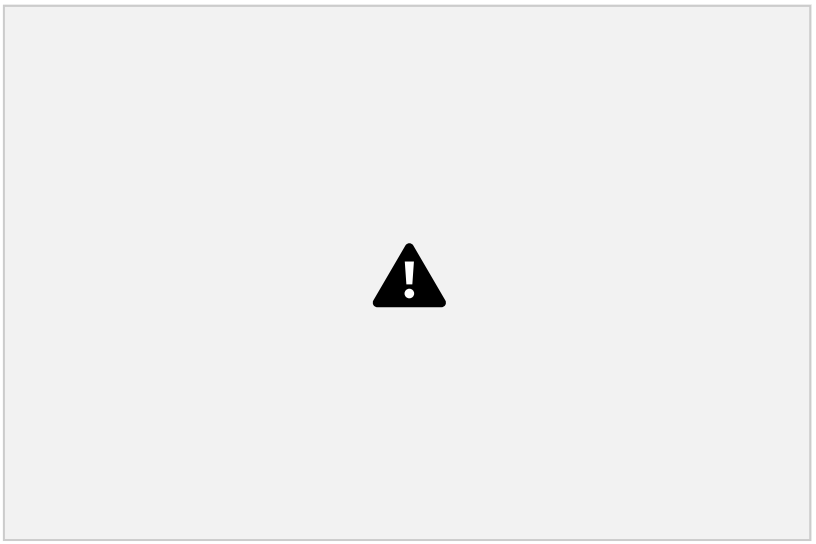


Figure: Use of handshaking in exposed station problem

4.6 BRIDGES

- A bridge operates in both the physical and the data link layer.
- In physical layer it regenerates the signal it receives.

- In data link layer, the bridge can check the physical (MAC) addresses (source and destination) contained in the frame.
- **Functions of a Bridge**

  The functions of the bridge are few and simple:
  - The bridge makes no modification to the content or format of the frames it receives, nor does it encapsulate them with an additional header.
  - Each frame to be transferred is simply copied from one LAN and repeated with exactly the same bit pattern on the other LAN. Because the two LANs use the same LAN protocols, it is permissible to do this.
  - The bridge should contain enough buffer space to meet peak demands. Over a short period of time, frames may arrive faster than they can be retransmitted. ▪ The bridge must contain addressing and routing intelligence. At a minimum, the bridge must know which addresses are on each network to know which frames to pass. Further, there may be more than two LANs interconnected by a number of bridges. In that case, a frame may have to be routed through several bridges in its journey from source to destination.
  - A bridge may connect more than two LANs.
- **Filtering:** A bridge has filtering capability. It can check the destination address of a frame and decide if the frame should be forwarded or dropped. If the frame is to be forwarded, the decision must specify the port. A bridge has a table that maps addresses to ports.
- The bridge is designed for use between local area networks (LANs) that use identical protocols for the physical and link layers (e.g., all conforming to IEEE 802.3). Because the devices all use the same protocols, the amount of processing required at the bridge is minimal.

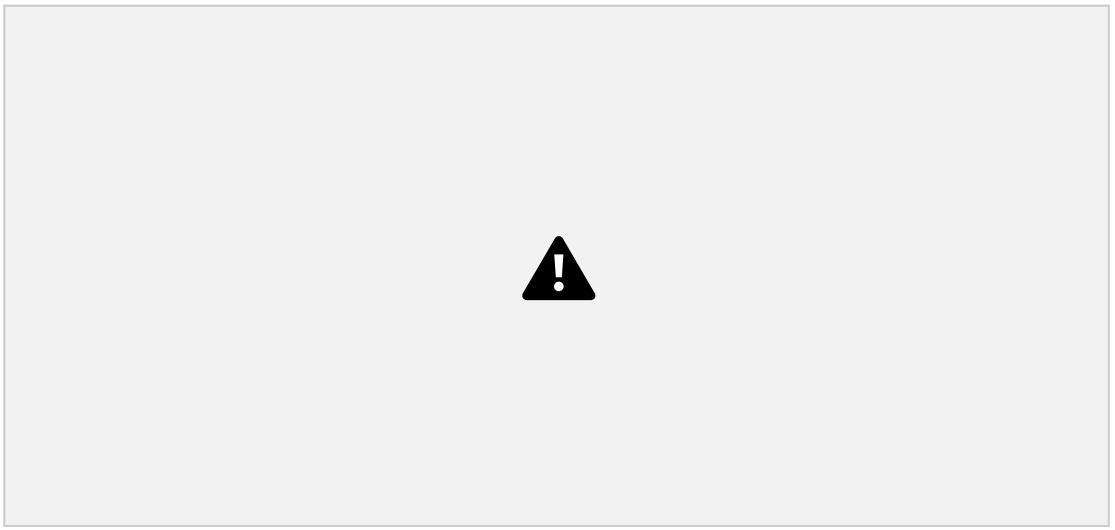


Figure: Multiple LANs connected by a backbone to handle a total load higher than the capacity of a single LAN using a Bridge

- ***More sophisticated bridges are capable of mapping from one MAC format to another (e.g., to interconnect an Ethernet and a token ring LAN).***

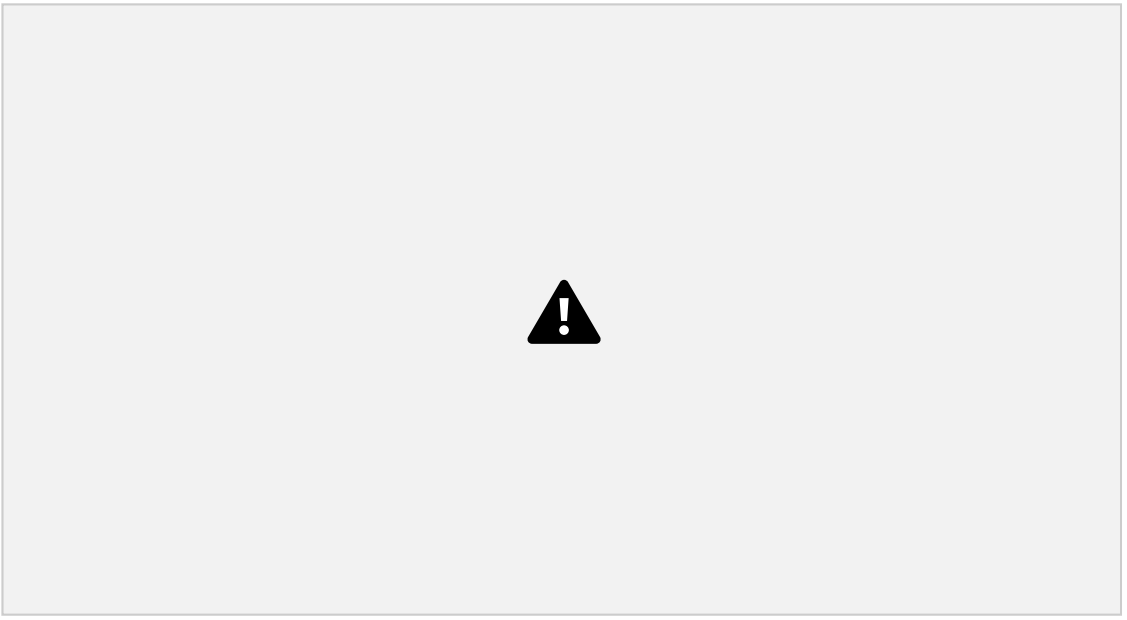


Figure: Bridge between two different LANS

- **Spanning Tree Bridges:**
  - To increase reliability, some sites use two or more bridges in parallel between pairs of LANs as shown in the figure. This arrangement, also introduces some additional problems because it creates loops in the topology.

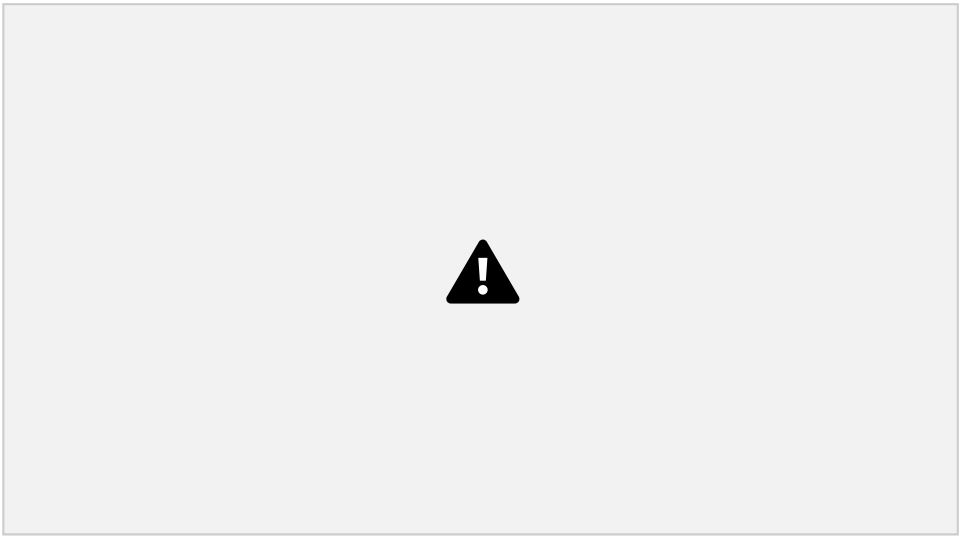


Figure: Looping in Transparent Bridges

▪ Each bridge, following the normal rules for handling unknown destinations, uses flooding, which in this example just means copying it to LAN 2. ▪ Bridge 1 sees F_2, a frame with an unknown destination, which it copies to LAN 1, generating F_3 (not shown). Similarly, bridge 2 copies F_1 to LAN 1 generating F_4 (also not shown). Bridge 1 now forwards F_4 and bridge 2 copies F_3. This cycle goes on forever.

▪ **Solution:** Some potential connections between LANs are ignored in the interest of constructing a fictitious loop-free topology.

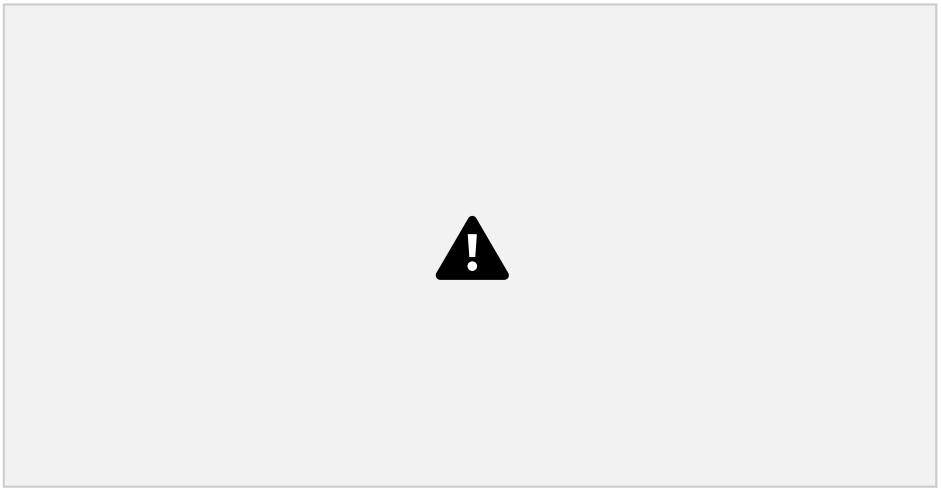


Figure: Spanning Tree Bridges

- For example, in the above figure, we see nine LANs interconnected by ten bridges. This configuration can be abstracted into a graph with the LANs as the nodes. An arc connects any two LANs that are connected by a bridge. The graph can be reduced to a spanning tree by dropping the arcs shown as dotted lines in right hand side figure. Using this spanning tree, there is exactly one path from every LAN to every other

LAN. Once the bridges have agreed on the spanning tree, all forwarding between LANs follows the spanning tree. Since there is a unique path from each source to each destination, loops are impossible.

- **Building Spanning Tree:**

  ➢ To build the spanning tree, first the bridges have to choose one bridge to be the root of the tree. The bridge with the lowest serial number becomes the root.

  ➢ Next, a tree of shortest paths from the root to every bridge and LAN is constructed. This tree is the spanning tree.

  ➢ If a bridge or LAN fails, a new one is computed.

- The result of this algorithm is that a unique path is established from every LAN to the root and thus to every other LAN. Although the tree spans all the LANs, not all the bridges are necessarily present in the tree (to prevent loops). Even after the spanning tree has been established, the algorithm continues to run during normal operation in order to automatically detect topology changes and update the tree.
- The distributed algorithm used for constructing the spanning tree was invented by Radia Perlman and is described in detail in (Perlman, 2000). It is standardized in IEEE 802.1D.

• **Remote Bridges:**

▪ A common use of bridges is to connect two (or more) distant LANs. For example, a company might have plants in several cities, each with its own LAN. Ideally, all the LANs should be interconnected, so the complete system acts like one large LAN.

▪ **Remote Bridges** can be used to create a wide area network (WAN) link between LANs. Remote bridges, where the connecting link is slower than the end networks, largely have been replaced with routers.

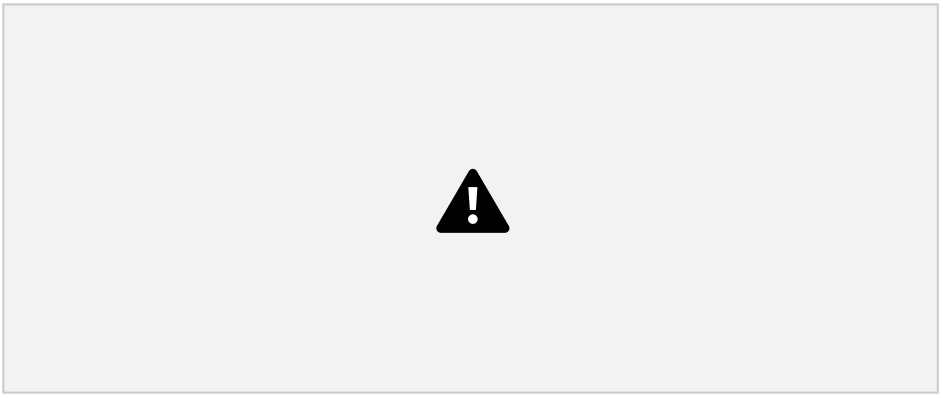


Figure: Remote Bridge

▪ Various protocols can be used on the point-to-point lines. One possibility is to choose some standard point-to-point data link protocol such as PPP, putting complete MAC frames in the payload field.