UNIT II

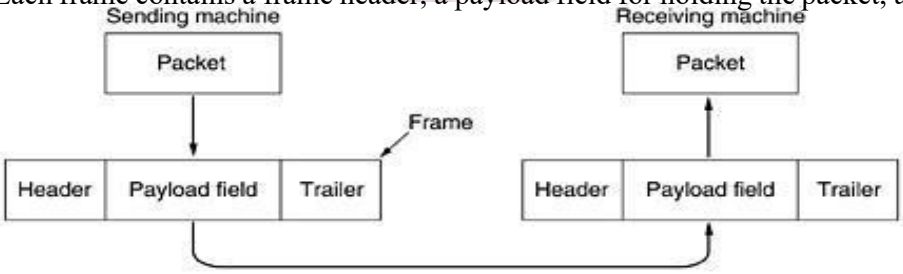
Data link layer: Design issues, framing, Error detection and correction.
Elementary data link protocols: simplex protocol, A simplex stop and wait protocol for an error-freechannel, A simplex stop and wait protocol for noisy channel.
Sliding Window protocols: A one-bit sliding window protocol, A protocol using Go-Back-N, Aprotocol using Selective Repeat, Example data link protocols.
Medium Access sub layer: The channel allocation problem, Multiple access protocols: ALOHA, Carrier sense multiple access protocols, collision free protocols. Wireless LANs, Data link layer switching.

Data link layer: Design issues

Design issues for data link layer are
1. Providing well defined service interface to the network layer.
2. Dealing with transmission errors.
3. Regulating the flow of data.

To achieve these goals, the data link layer takes the packets it gets from the network layer and changeas them into frames for transmission.

Each frame contains a frame header, a payload field for holding the packet, and a frame trailer.



Services provided to the Network layer:

The principal service of data link layer is transferring data from the network layer on the sourcemachine to the network layer on the destination machine.
Three commonly provided services are:

1. Unacknowledged connection less service.
2. Acknowledged connection less service.
3. Acknowledged connection-oriented service.

1. Unacknowledged connection less service:

- The source m/c sends independent frames to the destination m/c.
- No logical connection is established between source & destination.
- If a frame is lost, no attempt is made to detect the loss of the frame.
- This service is appropriate when the error rate is low.
- In this the destination m/c does not send any acknowledgement back to the sender.

- It is useful when an error rate is very low.
- Most LAN's are used unacknowledged connectionless services.

2. Acknowledged connectionless service:

- No logical connection is established between source &destination machine.
- But the receiver sends an acknowledgement back to the sender.
- By receiving the acknowledgement the sender knows that the frame has arrived correctly.
- If the acknowledgement is not received with in a specified time interval, it can be sent again.
- The network layer can always send a packet and wait for it to be acknowledged.
- If the acknowledgement is not forthcoming before the timer expires, thesender can just send the entire message again.
- The trouble of this strategy is that frames usually have a strict maximum length imposed by thehardware and network layer packets do.

3. Acknowledgement connection –oriented service:

- Before any data is transferred a connection is established between source & destinationmachines.
- It guarantees that each frame is received exactly once and that all frames are received in theright order.
- In this service the data transfer goes through three distinct phases.
- In the first phase, the connection is established variables are initiated & counters keep track ofwhich frames have been arrived &which once have not.
- In the second phase, one or more frames are actually transmitted.
- In the third phase, the connection is released freeing up the variables, buffer &other resources.
- Ex: In a WAN subnet consisting of routers connected by point-to-point leased telephone lines.
- When a frame arrives at a router, the hardware checks it for errors then passes the frame to thedata link layer software.
- The data link layer software checks to see if this is the frame expected, and if so, gives thepacket contained in the payload field to the routing software.
- The routing software then chooses the appropriate outgoing line and passes the packet backdown to the data link layer software.

FRAMING:

- In order to provide services to the network layer, the data link layer must use the services fromthe physical layer.
- The physical layer sends the bit stream to the data link layer.
- The no. of bits received may be different from the no. of bits transmitted.
- The data link layer convert the bit stream into data frames and compute the checksum for eachframe.
- At the destination, the check sum is recomputed.

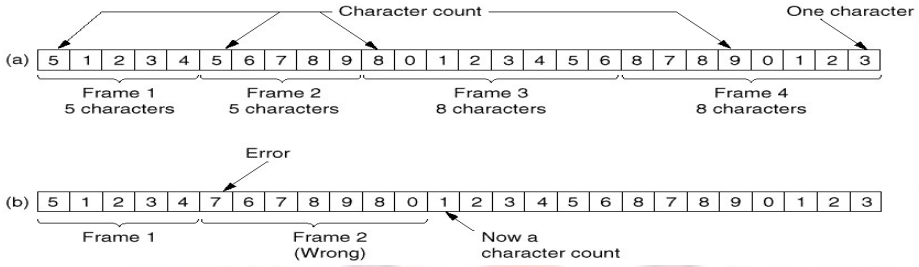
- If the recomputed check sum is different from the one contained in the frame.
- An error has occurred and the data link layer deals with the errors.
- To mark the start and end of each frame, we use *four methods*. They are

1. Character count.
2. Flag bytes with byte stuffing.
3. Starting and ending flags with bit stuffing.
4. Physical layer coding violations.

1. Character count:

This method uses a field in the header to specify the number of characters in the frame.

- At the destination the data link layer sees the character count, it knows how many characters followand where the end of the frame is



(a) With out error (b) with error

For example, if the characters count of 5 in the second frame becomes a 7.

- The destination will go out of synchronize and will be unable to locate the start of the next frame.

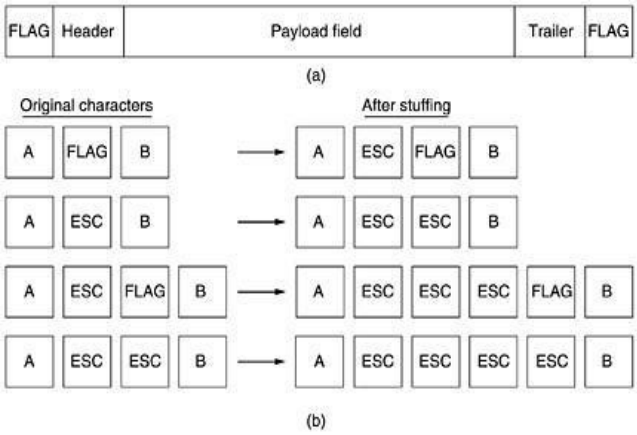
- The destination does not know how many characters to skip over to get to the start of the retransmission. For this reason, the character count is rarely used.

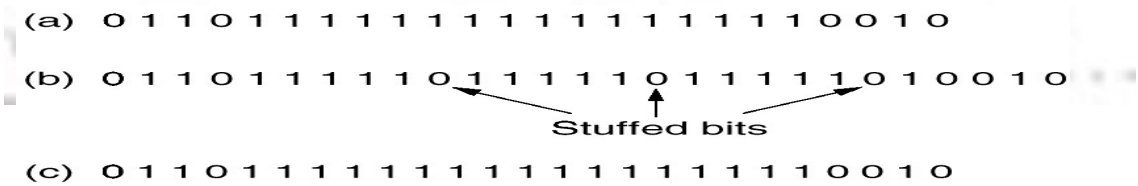
2. Flag bytes with byte stuffing:

- In this method, each frame start and end with special bytes.
- Most protocols have used the same byte called a flag byte as FLAG at both starting &ending ofthe frame.
- Even if the receiver ever loses synchronization, it can just search for the flag byte to find the endof the current frame.
- Two consecutive flag byte indicates the end of one frame and start of the next one.

Fig . (a) A frame delimited by flag bytes.

(b) Four examples of byte sequences before and after byte stuffing





- The sender's data link layer inserts a special escape byte "ESC"just before each flag byte the data.
- At the receiving end, the data link layer removes the escape byte before the data are given tothe network layer.
- This technique is called" byte stuffing" or "character stuffing".
- A framing flag byte can be identified by the absence or presence of an escape byte in the data.
- If an escape byte occurs in the middle of data that, too, is stuffed with an escape byte.
- Any single escape byte is part of an escape sequence, where as a doubled one indicates that asingle escape occurred naturally in the data.
- Examples of the byte sequences before &after byte stuffing.
- A major disadvantage of this framing method is it is used for 8-bit character only.
- Not all character codes use 8-bit characters, some use 16-bit characters, so a new technique hadto developed to allow sized characters.

3. Starting and ending flags, with bit stuffing:

- In this method, each frame begins and ends with a special bit pattern, 01111110 a flag byte.
- When the sender's data link layer encounters five consecutive 1's in the data, it automaticallystuffs a 0 bit into outgoing bit stream.
- This bit stuffing is similar to byte stuffing.
- When the receiver sees five consecutive incoming 1 bits, followed by a 0 bit, it automaticallydeletes the 0 bit.
- The boundary between two frames can be recognized by the flag pattern.
- If the receiver losses its track the receives has to scan the input for flag sequences.
- The flag sequences occur only at frame boundaries and never with in the data.

4. Physical layer coding violations:

This framing method is used in the networks in which physical medium contains someredundancy.
A 1 bit is a high –low pair & a 0 bit is a low-high pair. It means that every data bit has a transmissionin the middle. It makes easy for the receiver to locate the bit boundaries.

Error control:

- To make sure that all frames are eventually delivered to the network layer at the destination &in the proper order.
- The protocol calls for the receiver to send back special control frames bearing positive ornegative acknowledgements about the incoming frames.

- If a +ve acknowledgement is received the frame has arrived safely.
- If a – ve acknowledgement is received the frame has gone wrong & the frame must betransmitted again.
- If a frame is lost due to hardware failure the receiver will not react & does not send anyacknowledgement.
- Timers are introduced into the data link layer.
- When a frame is exacted the timer also starts, the frame will be correctly received & theacknowledgement will get back before the timer runs out.
- If the frame or acknowledgement is lost the timer will go off, here the frame is transmittedagain.
- If a frame is transmitted multiple times the receiver may accept the same and pass it to thenetwork layer more than once.
- To prevent this, sequence numbers are assigned to outgoing frames, so that the receiver candistinguish retransmission from originals.

Flow control:

- Flow control occurs when the sender wants to transmit frames faster than the receiver can acceptthem.
- Even if the transmission is error free, the receiver will simply be unable to handle the frames asthey arrive & will start to lose them.
- Feed back based flow control & rate based flow control are the two approaches that are commonlyused.
- In feedback –based flow control, the receiver sends back information to the sender giving itpermission to send more data.
- In rate based flow control, the protocol has a built – in –mechanism that limits the rate at whichsenders may transmit data, with out using feedback from the receiver.

Error detection and correction:

Data can be corrupted during transmission .for reliable communication; error must be detected&corrected.

Error correction: error correction can be done in two ways. When an error is discovered, the receivercan ask the sender to re –transmit the entire data unit.

- Or the receiver can be use an error- correcting code, which automatically corrects errors.

Error detecting codes:

For error detecting we use polynomial code also known as CRC is used. Polynomial codes are based upon treating bit strings as representations of polynomials with coefficients of 0 and 1 only.CRC cyclic redundancy check

1. Let us consider a data unit of ‘m’ bits.
2. A string of (n-1) 0’s is append to the data unit where ‘n’ is number of bits of the divisor. 3.The new data unit with m+ (n-1) bits is divided by divisor using modulo -2 division method.

The resulting remainder is having (n-1) bits .this remainder is called CRC remainder.

4. The CRC remainder of (n-1) bits obtained from step 3 replaces the already append 0’s in step2.
5. The data unit followed by CRC reaches the receiver.

6. The receiver divides the CRC appended data unit using the same divisor by the module -2division method.

If the data unit, received by the receiver is without any error then the remainder obtained from step6 will be zero.
Other wise the remainder will be non zero.
Ex: using error detecting code find the transmitted frame for a given frame of 1101011011 using thegenerator.

Frame: 1101011011
Generator it becomes 10011
In the given generator the highest power is 4, so we have to add 4 zero's to the frame.

Now, the transmitted frame is:
11010110111110
The frame is transmitted to the destination.
At the destination it again performs the same operation.
If the remainder is 0 the data is without errors & is accepted. Otherwise, the data is discarded.

Elementary data link protocols

Elementary data links protocols are 3 types:

1. An unrestricted simplex protocol.
2. A simplex stop-and – wait protocol.
3. A simplex protocol for a noisy channel.

1. An unrestricted simplex protocol:

- Data is transmitted in one direction only.
- transmitting and receiving network layers are always ready.
- processing time can be ignored.
- Infinite buffer space is available.
- Communication channel between the data link layers never damages ar loses frames.
- Here in this protocal, no sequence numbers as acknowledgements are used.

2) A Simple stop-and-wait Protocol:

- The communication channel is error free.
- Mai problem is how to prevent the sender from flooding the receiver with data faster than it is ableto process it.
- To prevent sender from sending more frames than the receiver can accept.
- After a packet is passed to the network layer, the receiver sends a little dummy frame back to thesender, so it gets permission to transmit the next frame.
- Sender sends one frame and then waits for an acknowledgement before proceeding is called "Stop-and-wait".
- This protocol has strict alternation of flow first the sender sends a frame, the receiver

sends anacknowledgement, then only the sender sends another frame, then the receiver sends &soon.

3) A Simplex protocol for a Noisy channel:

- The communication channel makes errors. Frames may be damaged or lost completely.
- If a frame is damaged the receiver hardware will detect the error when it computes the checksum.
- If a damaged frame arrived at the receiver, it would be discarded.
- The sender sends the frame again after the time out.
- The receiver must be able to distinguish a frame from retransmission.
- To achieve this sender put a sequence number in the header of each frame it sends.
- The receiver checks the sequence number of each arriving frame to see if it is a new frame.
- If it is duplicate frame, it is discarded.
- Protocols I which the sender waits for a positive acknowledgement before advancing to the next data is called (Positive Acknowledgement with Retransmission) PAR or (Automatic Repeat request) ARQ.

Sliding Window Protocol

In the previous protocols, data frames are transmitted in one direction only. There is need fortransmitting data in both directions.

- We have two separate physical circuits, each with a "forward" channel for transmitting data anda "reverse" channel for transmitting acknowledgements.
- The bandwidth of the reverse channel is entirely wasted as it sends only acknowledgements.
- To effectively use the bandwidth of the reverse channel. The receiver may wait for sometimefor the next data packet and with data pocket it sends the acknowledgement.
- The acknowledgement is attached to the outgoing data frame.
- The technique of temporarily delaying outgoing acknowledgements so that they can be attachedto the next outgoing data frame is known as "***Piggy Backing".***
- The advantage of using piggy backing is better use of the available channel bandwidth.
- All sliding window protocols maintains" sending window" and "receiving window"
- The sender maintain a set of sequence numbers corresponding to frames it is permitted to send
- These frames are in "sending windows"
- The receiver maintains a set of frames it is permitted to accept. These frames are in "receivingwindows"
- The three sliding windows protocols differ in terms of efficiency complexity and bufferrequirements.
- The three sliding windows protocol are
    1) A one bit sliding window protocol

2) A Protocol using go back n

3) A protocol using selective repeat

1) A one bit sliding window protocol

- Maximum windows size is one, search protocol uses stop- and –wait, here the sender transmitsa frame and wait form it's acknowledgement before sending the next one
- The starting machine fetcher the first packet from its network layer builds a frame from it andsender it.
- When the frame arrives the receiving data link layer checks to see if it is a duplicate.
- If it is the expected frame, it is passed to the network layer and the receiver's window is slidup.
- The acknowledgement field contains the number of the last frame received with out error.
- If it agrees with the sequence number of the frame it fetches the next packet from n/w layer.
- If the sequence number disagrees, it must continue trying to send the same frame.

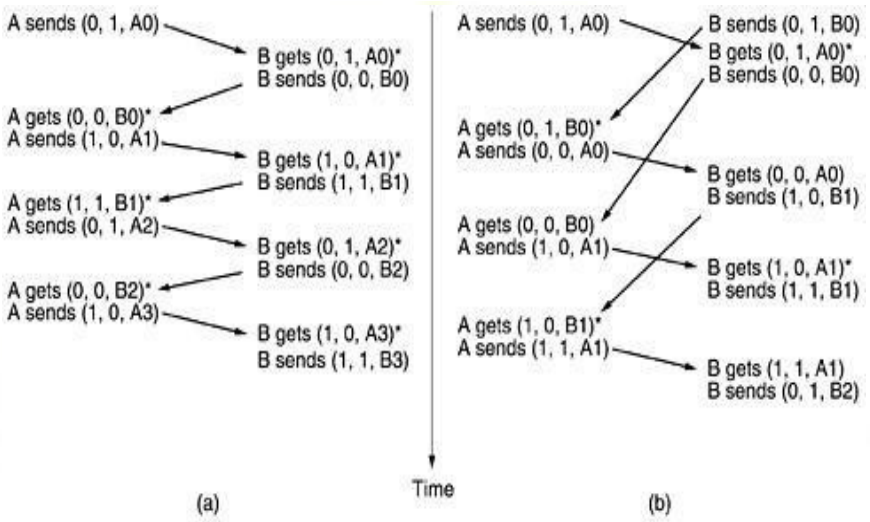


Fig. Two scenarios for protocol 4. (a) Normal case. (b)Abnormal case. The notation is (seq, ack, packet number). An asteriskindicates where a network layer accepts a packet.

2) A protocol using go back n

- To achieve better efficiency the solution is to allow the sender to transmit up to w frames before blocking instead of 1.
- If we take 'w' as 26, the sender begins sending frames 0 at t=520 it has finished sending 26 frames, the acknowledgement for frame 0 will have just arrived.
- Acknowledgements will arrive after every 20 m sec sender always get's permission to continues when it's it
- This technique is known as "pipelining"
- Pipelining frames over a communication channel has same problems. If a damaged frames occurs in the middle of a long steam frame.

- Go-back-n and selective repeat are the two ways to deal with errors in pipelining
- In Go-back-n the receiver simple discards all subsequent frames, sender no acknowledgements for the discarded frames.
- After the senders time out it retransmit all unacknowledged frames in order, starting with managed or lost one.
- It wastes a lost of band width, if error rate is high.

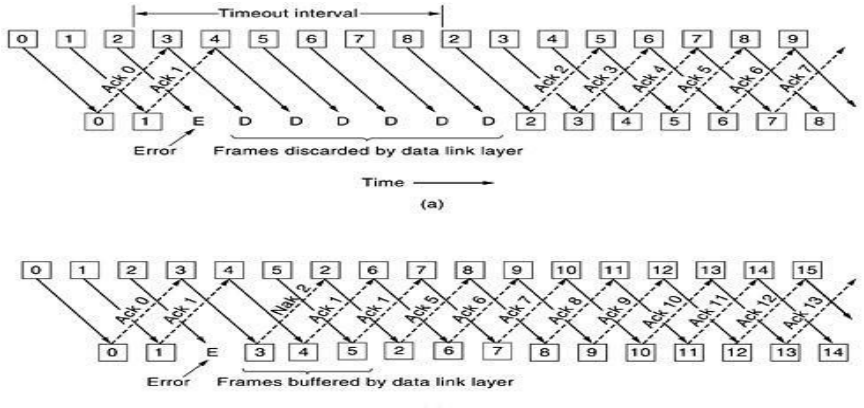
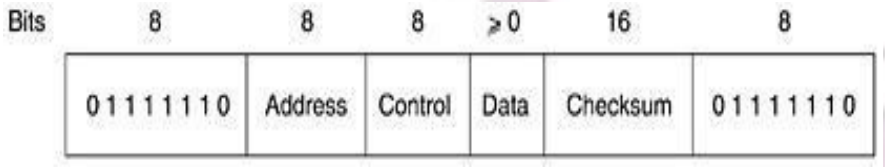


Fig. Pipelining and error recovery. Effect of an error when (a)receiver's window size is 1 and (b) receiver's window size is large.

A protocol using selective repeat:

- The receiver is allowed to accept and buffer the frames fallowing a damaged or lost frame.
- When a receiver suspects than an error has occurred, it sends a negative acknowledgment frameback to the sender.
- It is a request for retransmission of the frame in the NAK specified.
- After the time out the senders transmit the lost frame.
- After lost frame send to the network layer it transmit the other frames stored in the buffer to thenetwork layer in a sequence order.



Multiple access protocol:

A new and elegant method to solve the channel allocation problem is called the ALOHA system, used ground-based radio broadcasting, the basic idea is applicable to any system in which uncoordinated users are competing for the use of a single shared channel.

ALOHA 2 types PURE aloha & slotted aloha

PURE ALOHA: not divided according to time intervals do not require global time synchronization.***SLOTTED ALOHA***: divided according to time intervals. Slotted ALOHA need global time synchronization.

PURE ALOHA:

- When data is ready in it, it sends it directly.
- We do not know whether the channel is empty or not then the frames undergo collisions.
- All the frame lengths should be equal, then we get high throughput.

- Checksum recognizes if there is collision or not. It detects the collisions.
- If there is collision will wait for some random time & transmit the next frame. This is knownas retransmission.

Contention system: having single communication channel, where multiple users are competing for thatchannel then those systems are contention systems.

- Work load increasing.
- If N>1 , then we are unable to handle problems.

0<N<1, at least handle and transmit the frames.N-represents data frames which are to be sent. G-represents retransmit.
S-represents the total probability.

- When less no of data frames, then G=S (low loads) when load is over & over(high loads) G>S
- At low loads pure aloha is working well.
- Probability is given by S=GP0 (pure aloha)

P0-the frame which is transmitted without undergoing a collision.Pure aloha, S=Ge

Vulnerable period: the last bits of one frame is collided with the starting bits of another frame is calledvulnerable period.

- Here we have more collisions in aloha in this period.
- If we have 'K' frames which are to be sent then, position distribution equation

SLOTTED ALOHA:

- It need global time synchronization
- Slotted aloha is better than pure aloha in channel utilization.
- Probability of slotted aloha, S=
- If retransmission G increases, collision also increases if G decreases, graph falls down.
- Slotted aloha is not sensing the channel before transmit ion
- The total channel efficiency for pure aloha is S=1/2e.
- the total channel efficiency for slotted aloha is S=1/e.

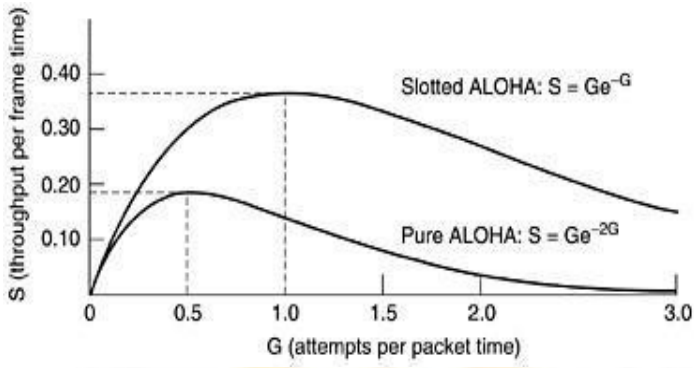


Fig. Throughput versus offered traffic for ALOHA systems.

carrier sense multiple access protocols:

protocols in which stations listen for a carrier and act accordingly are called carrier sense protocols.

1- persistent CSMA(carrier sense multiple access):

- when a station has data to send, it first listen to the channel to see if anyone else is transmitting at that moment.
- If the channel is busy, the station waits until it becomes idle.
- When the station detects an idle channel, it transmits the frame.
- This protocol is called 1-persistent because the station transmits with a probability of 1 when its finds the channel idle

Non persistent CSMA:

- Before sending the data , a station sends the channel.
- If no one else is sending, the station begins sending frames.
- If the channel is already in use, the station does not continuously sense it.
- It waits a random of time & then repeats the algorithm.
- This algorithm leads to better channel utilization than 1-persistant CSMA.

p-persistent CSMA:

- It applies to slotted channels
- When a station ready to sends it senses the channel.
- If it is idle, it transmits with a probability P.
- With a probability Q=1-p it differs until the next slot.
- This process repeat until either the frame has been transmitted.
- If the station initially senses the channel busy, it waits until the next slot& applies the algorithm.

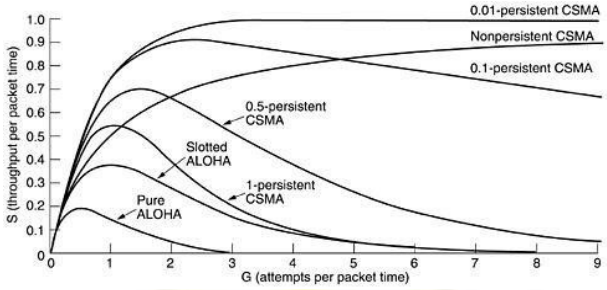


Fig. Comparison of the channel utilization versus load for various random access protocols.

CSMA/CD: (CSMA with collision detection.)

- Terminating damaged frames quickly saves time and bandwidth.
- At to, a station has finished transmitting its frame.
- Any other station having a frame to send may attempt now.
- If two or more stations decide to transmit simultaneously, there will be a collision.
- After a station detects a collision, it aborts its transmission waits a random time & then triesagain, assuming that no other station has X'ted in the meantime.
- Therefore, CSMA/CD consisting of alternating contension and transmission periods, with idleperiods occurring when all stations are quiet.
- Systems in which multiple users share a common channel in a way that can lead to conflicts areknown as contention systems.
- It works well on low loads.

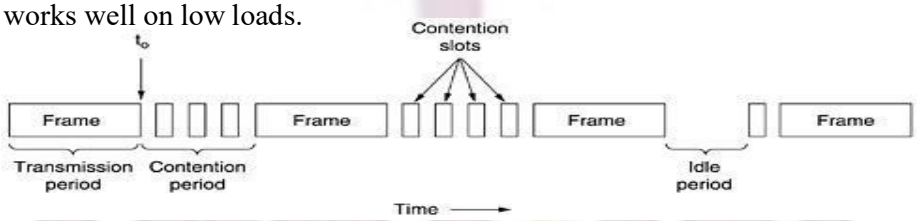


Fig: CSMA/CD can be in one of three states: contention, transmission, or idle

Collision free protocol

collisions do not occur with CSMA/CD. But it can occur during the contention period. These collisions affect the system performance, especially when the cable is long (i.e., large t) and the frames are short. some protocols that resolve the contention for the channel without any collisions at all, not even during the contention period. Most of these are not currently used in major systems, but in a rapidly.

Collision free protocols are:

1. **Bit map protocol.** **2.Binary count down protocol.**

BIT MAP protocol:

- Each contention period consists of exactly N slots.
- If station 0 has a frame to send, it transmits a 1 bit during the 0^{th} slot.
- No other station is allowed to transmit during this slot.
- In general, station J may announce that it has a frame to send by inserting a 1 bit into slot J.
- After all N slots have passed by each station has complete knowledge of which station andwish to transmit.
- At that point, they begin transmitting numerical order.
- Since every one agrees on who goes next, there will never be any collision.
- The protocols desire to transmit is broadcast before the actual transmission are calledreservation protocols.
- At low loads average waiting time 1.5N slots.
- At high loads average waiting time 0.5N slots.
- Efficiency at low loads = d/(N+d).
- Efficiency at high loads = d/(d+1).

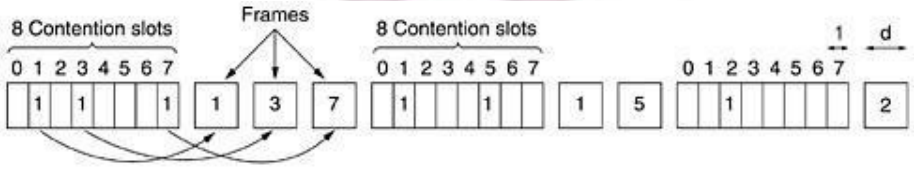


Fig: The basic bit-map protocol.

Binary cut down protocols:

- The station wants to use the channel now broadcasts its address as a binary bit string, startingwith the high order bit.
- All addresses are assumed to be the same length.this protocol is called binary cut down.
- To avoid conflicts, based on choice rule must be applied.
- As a station sees a high order bit position that is 0 in its address has ben overwritten with a 1.
- For example: if stations 0010, 0100, 1001 & 1010 are all trying to get the channel.
- In the first bit time the stations X'mit 0,0,1 & 1 respectively.
- Stations, 0010 & 1010 continue.
- The next bit is 0 & both stations continue.
- The next bit is 1 so station 1001 gives up.
- The winner is station 1010 because it has the highest address.
- It now transmits the frame.
- Channel efficiency=d/d+log.

Wireless LAN protocol

A system of portable computers that communicate by radio can be regarded as a wireless LAN.

- Wireless LAN are based on radio signals for transmission.
- The competitor who wants to access the channel is too far from the station so the problem iscalled hidden station problem.
- If two stations are out of the range the stations get bad reception the problem is called exposedstation problem.
- To overcome the problems we use MACA & MACAW protocols.

MACA-multiple access with collision avoidance

MACAW-MACA improve its performance & renamed their new protocol

MACAW.If A sends message RTS to B, if RTS is reached B it sends message

CTS to A. RTS→request to send.

CTS→ clear to send.

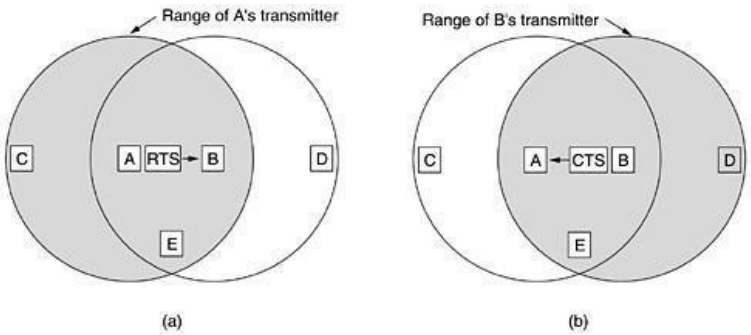


Fig: The MACA protocol. (a) *A* sending an RTS to *B*. (b) *B* responding with a CTS to *A*.

IEEE standards for LAN:

IEEE proposed some channel allocation protocols for LANs and MANs.

– logical link control protocol.

– Ethernet.

– token bus

– token ring

– distributed queue dual bus.

Ethernet:

- Ethernet refers to the cable.
- Four types of cabling are commonly used

Name	Cable	Max. seg.	Nodes/seg.	Advantages
10Base5	Thick coax	500 m	100	Original cable; now obsolete
10Base2	Thin coax	185 m	30	No hub needed
10Base-T	Twisted pair	100 m	1024	Cheapest system
10Base-F	Fiber optics	2000 m	1024	Best between buildings

Fig: The most common kinds of Ethernet cabling.

- 10 base 5 called as thick Ethernet.
- Connections are made using vampire taps.
- 10 base 5 means it operates at 10 mbps.uses baseband signaling & support segments of up to 500 meters.
- 10Base5, a **transceiver** is clamped securely around the cable its tap makes contact with the inner core.
- The transceiver contains the electronics that handle carrier detection and collision detection.

- When a collision is detected, the transceiver also puts a special invalid signal on the cable to ensure that all other transceivers also realize that a collision has occurred.
- With 10Base5, a **transceiver cable** or **drop cable** connects the transceiver to an interface boardin the computer.
- The transceiver cable may be up to 50 meters long and contains five
- individually shielded twisted pairs.
- Two of the pairs are for data in and data out, respectively.
- Two more are for control signals in and out. The fifth pair, which is not always used, allowsthe computer to power the transceiver electronics
- The transceiver cable terminates on an interface board inside the computer. The interface boardcontains a controller chip that transmits frames to, and receives frames from, the transceiver.
- The controller is responsible for assembling the data into the proper frame format, as well ascomputing checksums on outgoing frames and verifying them on incoming frames.
- 10 base 2 also called as thin Ethernet.
- Connections are made using industry standards BNC connectors to form T junctions, ratherthan using vampire taps.
- With 10 base2, the connection to the cable is just a passive BNC t-junction connector. BNCconnectors are easier to use and more reliable.
- Thin Ethernet is much cheaper and easier to install, but it can run for only 185 meters persegment, each of which can handle only 30 machines.
- Detecting cable breaks, excessive length, bad taps, or loose connectors can be a major problemwith both media.
- For this reason, techniques have been developed to track them down.
- A pulse of known shape is injected into the cable. If the pulse hits an obstacle or the end of thecable, an echo will be generated and sent back.
- By carefully timing the interval between sending the pulse and receiving the echo, it is possibleto localize the origin of the echo. This technique is called **time domain reflectometry**.
- 10 base T uses twisted pair cable.
- In 10 base T all stations have a cable running to a central hub.
- With 10 base T, there is no cable at all just hub.
- Adding or removing a station is simpler in this configuration, & cable breaks can be

detectedeasily.

- The advantage is the maximum cable run from the hub is only 100 meters.
- base F uses fiber optics.
- This is expensive due to the cost of the connectors and terminators.
- We use for different topologies they are linear, spine , tree, & segmented.
- To allow larger networks, multiple cable can be connected by repeaters.
- A repeater is a physical layer device it receives, amplifiers & retransmits signals in both directions.

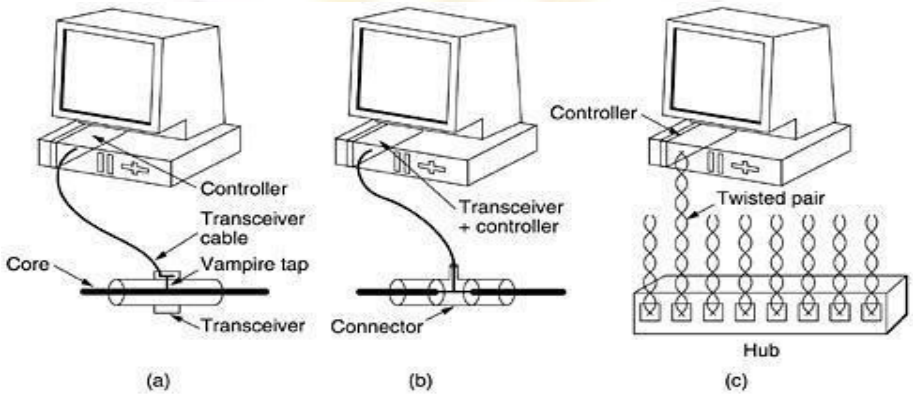


Fig: Three kinds of Ethernet cabling. (a) 10Base5. (b) 10Base2.(c) 10Base-T.

- A 0 bit is indicated by the presence of a transition at the start of the interval.

  In both cases, the transition in the middle.

- The high signal is + 0.85 volts & the low signal is _ 0.85 volts.

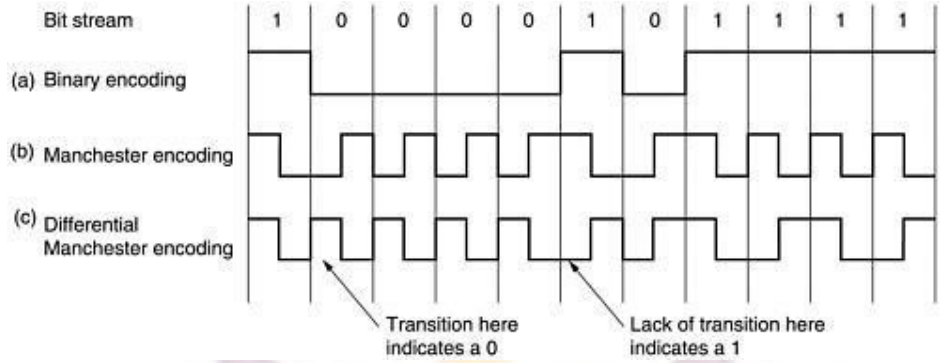


Fig: (a) Binary encoding. (b) Manchester encoding. (c)Differential Manchester encoding.

- Ethernet does not use differential Manchester encoding.
- All Ethernets use Manchester encoding.

MAC sublayer protocol:

- Each frame starts with a preamble of 7 bytes, each containing the bit pattern 10101010.
- Start of frame byte containing 10101011 to denote the start of the frame itself.
- The frame contains 2 addresses, one for the destination & and one for the source.
- It allows 2-byte & 6-byte addresses.
- The length field, tells how many bytes are present in the data field, from a min of 0 to a maxof 1500 bytes.
- The valid frames must be at least 64 bytes long, from destination address to checksum.
- If the data portion of a frame is less than 46 bytes, the pad field is used to fill out the frameto the minimum size.
- Frames with fewer bytes are padded out to 64 bytes.
- Checksum is used for error detection.

Binary exponential back of algorithem:

- This algorithm was chosen to dynamically adapt to the number of stations trying to send.
- After a collision, each station waits either 0 or 1 slot times before trying again.
- In general, after i collision, a random number between 0 and 2i-1 is chosen, & that noof slots is skipped.
- If the randomization interval for all collisions was 1023, the chance of two stationscolliding for a second time would be negligible.By having the randomization interval grow exponentially as more & more consecutive

collision occur.

- The algorithm ensures a low delay when only a few stations collide but also ensures thatthe collision is resolved in a reasonable interval when many stations colloid.
- All that needed is reserve the first contention slot fallowing successful X'ion for thedestination station.