Year	Subject Title	Sem	Sub Code
2018 -19 Onwards	**Core: COMPUTER NETWORKS**	**IV**	**18BIT42C**

UNIT III: The Data Link layer - Data link layer Design Issues – Error Detection and Correction- Elementary Data link protocols. Medium Access Sub Layers The channel allocation problem – Multiple access protocols Carrier sense multiple access protocols, collision –free protocols, Limited contention protocols.

UNIT IV: The Network Layer – Network Layer Design Issues – Routing Algorithms The optimality principle, shortest path routing, flooding, and distance vector routing, routing for mobile hosts.

TEXT BOOKS

1. Andrew S. Tanenbaum, “Computer Networks”, 4th Edition, Pearson Education Publ. 2014.

.

Prepared by : Mrs. G. Shashikala, Asst. prof., PG and Research Dept of InformationTechnology

Data Link Layer

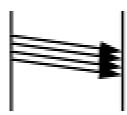
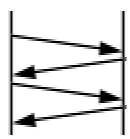
- Provides a *well-defined service interface* to the network layer.
- Determines how the bits of the physical layer are grouped into frames *(framing)*.
- Deals with transmission errors *(CRC and ARQ)*.
- Regulates the flow of frames.
- Performs general link layer management.

Data Link Layer Design Issues

- Services provided to the Network Layer
- Framing
- Error Control
- Flow Control

Datalink Layer Services

- Unacknowledged connectionless service
  - No acks, no connection
  - Error recovery up to higher layers
  - For low error-rate links or voice traffic
- Acknowledged connectionless service
  - Acks improve reliability
  - For unreliable channels. E.g.: Wireless Systems

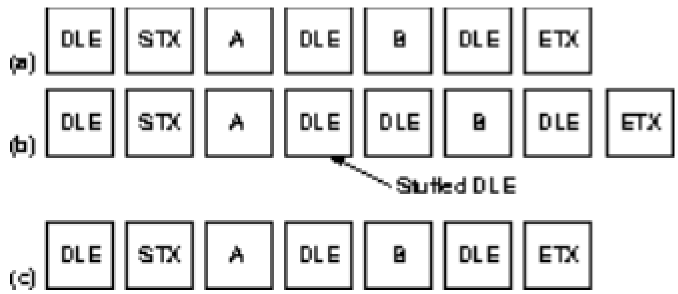



Framing

- Framing = How to break a bit-stream into frames
- Need for framing: Error Detection/Control work on chunks and not on bit streams of data
- Framing methods:
  - Timing : risky. No network guarantees.
  - Character count: may be garbled by errors
  - Character stuffing: Delimit frame with special characters
  - Bit stuffing: delimit frame with bit pattern
  - Physical layer coding violations

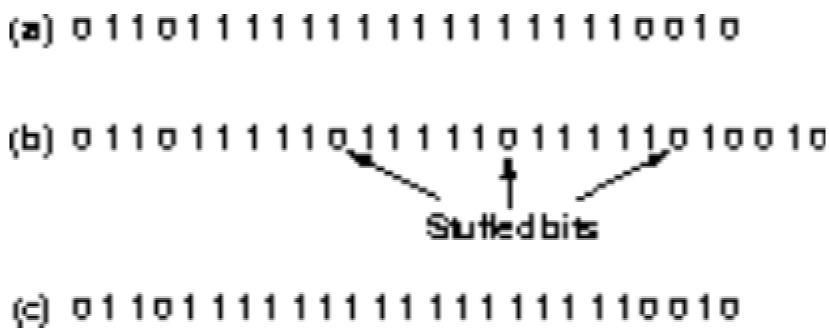
Character Stuffing

- Delimit with DLE STX or DLE ETX character flags
- Insert 'DLE' before accidental 'DLE' in data
- Remove stuffed character at destination



Bit Stuffing

- Delimit with special bit pattern (bit flags)
- Stuff bits if pattern appears in data
- Remove stuffed bits at destination



Physical Coding Violations

- On networks having coding redundancy on physical medium

Error Control

- Error Control = Deliver frames without error, in the proper order to network layer
- Error control Mechanisms:
  - Ack/Nak: Provide sender some feedback about other end
  - Time-out: for the case when entire packet or ack is lost
  - Sequence numbers: to distinguish retransmissions from originals

Flow Control

- Flow Control = Sender does not flood the receiver, but maximizes throughput
- Sender throttled until receiver grants permission

Error Detection and Correction

- Transmission errors: common on local loops, wireless links
- Single bit-errors vs Burst Errors
- n-bit codeword = m message bits + r check bits
- Hamming Distance = number of bit positions in which two code words differ
- Distance D code = minimum hamming distance between any two code words written in the code
- To detect d errors, distance d+1 code required
- To correct d errors, distance 2d+1 code required

Error-Correcting Codes

- Enough redundant information in a frame to detect and correct the error
- Lower limit on number of check bits to correct 1 error: $(m+r+1) <= 2^r$
- Hamming's method: (corrects 1-bit errors)
  - Bit positions in powers of 2 (1,2,4 ...) = check bits
  - Other bit positions data
  - Every bit included in several parity computations (See text)

Burst Error Correction

- Arrange code words as matrix
- Transmit one column at a time
- Uses kr check bits to immunize blocks of km data bits to single burst error of length k or less

Char.	ASCII	Check bits
H	1001000	00110010000
a	1100001	10111001001
m	1101101	11101010101
m	1101101	11101010101
i	1101001	01101011001
n	1101110	01101010110
g	1100111	11111001111
	0100000	10011000000
c	1100011	11111000011
o	1101111	00101011111
d	1100100	11111001100

Error-Detecting Codes

- Enough redundant information in a frame to detect error
- Request retransmission from source to correct the error
- Parity checks
- Cyclic Redundancy Code (CRC) checks

Cyclic Redundancy Check (CRC)

- **Binary Check Digit Method**
- Make number divisible by P=110101 (n+1=6 bits)

Example: M=1010001101 is to be sent

1. Left-shift M by n bits $2^n M$= 101000110100000
2. Divide $2^n M$ by P, find remainder: R=01110
3. Subtract remainder from P
4. Add the result of step 2 to step 1 : T=101000110101110
5. Check that the result T is divisible by P.

Modulo 2 Division

```
        Q=1101010110
P=110101)101000110100000=2^nM
         110101
          111011
          110101
           011101
           000000
            111010
            110101
             011111
             000000
              111110
              110101
               010110
               000000
                101100
                110101
                 110010
                 110101
                  001110
                  000000
                   01110 = R
```

Checking At The Receiver

```
       1101010110
110101)101000110101110
       110101
        111011
        110101
         011101
         000000
          111010
          110101
           011111
           000000
            111110
            110101
             010111
             000000
              101111
              110101
               110101
               110101
                00000
```

Cyclic Redundancy Check (CRC)

Polynomial Division Method

Make $T(x)$ divisible by $P(x) = x^5+x^4+x^2+1$ (Note: n=5)

Example: M=1010001101 is to be sent

$M(x) = x^9+x^7+x^3+x^2+1$

1. Multiply M(x) by x^n, $x^nM(x) = x^{14}+x^{12}+x^8+x^7+x^5+$ ....
2. Divide $x^nM(x)$ by $P(x)$, find remainder: $R(x)$=01110=x^3+x^2+x

- 3. Add the remainder $R(x)$ to $x^nM(x)$: $T(x) = x^{14}+x^{12}+x^8+x^7+x^5+x^3+x^2+x$
- 4. Check that the result $T(x)$ is divisible by $P(x)$.
- Transmit the bit pattern corresponding to $T(x)$: 101000110101110

Elementary Data Link Protocols

- Unrestricted Simplex Protocol
  - Framing only
  - No error or flow control
- Simplex Stop-and-Wait
  - Send one packet
  - Wait for Ack before proceeding
- Simplex Protocol for a Noisy Channel
  - Automatic Repeat request (ARQ) protocols
  - Positive Ack
  - 1-bit sequence number in frames (not in acks)
  - Timeout to detect lost frames/acks
  - Retransmission
  - Can fail under early timeout conditions
- Full Duplex Communication
  - Piggybacking of acks

- Receiver window
  - Packets outside window discarded
  - Window advances when sequence number = low edge of window received
  - Receiver window always constant
- Sender transmits W frames before blocking (pipelining)

The medium access control sublayer

- The protocols used to determine who goes next on a multi-access channel belong to a sublayer of the data link layer called the **MAC (Medium Access Control)** sublayer.
- The MAC sublayer is especially important in LANs, particularly wireless ones because wireless is naturally a broadcast channel.
- WANs, in contrast, use point-to-point links, except for satellite networks.

THE CHANNEL ALLOCATION PROBLEM

- **Static Channel Allocation**
- If there are *N users, the bandwidth is divided into N equal-sized* portions, with each user being assigned one portion. Since each user has a private frequency band, there is now no interference among users.
- When there is only a small and constant number of users, each of which has a steady stream or a heavy load of traffic, this division is a simple and efficient allocation mechanism.
- A wireless example is FM radio stations. Each station gets a portion of the FM band and uses it most of the time to broadcast its signal.

- *We assume that the frames arrive randomly* with an average arrival rate of λ frames/sec, and that the frames vary in length with an average length of 1/*μ bits. With these parameters, the service rate* of the channel is μ*C* *frames/sec.*
- *A standard queueing theory result is*
- $T = 1/(\mu C - \lambda)$
- Now let us divide the single channel into *N independent subchannels, each* with capacity *C /N bps. The mean input rate on each of the subchannels will now* be λ/*N*. *Recomputing T, we get*

  $T_N = 1/(\mu(C/N) - (\lambda/N)) = N/(\mu C - \lambda) = NT$

- The mean delay for the divided channel is *N times worse than that of without dividing.* $(T_N = NT)$

- (a) Continuous Time
  - Frame transmission can begin at any time
  - There is no master clock dividing the time into discrete intervals

  (b) Slotted Time
  - Time is divided into discrete intervals called slots.
  - Frame transmission begins at the beginning of the slot
  - A slot may be idle, may have one frame (legal) and may have multiple frames (collision)
- (a) Carrier Sense
  - Stations can tell if the channel is in use before trying to use it
  - If channel is in use, no station will attempt to use it before goes idle

  (b) No Carrier Sense
  - Stations can't sense the channel before trying to use it
  - They go ahead and transmit … only later they can say it was an error

Dynamic Channel Allocation (1)

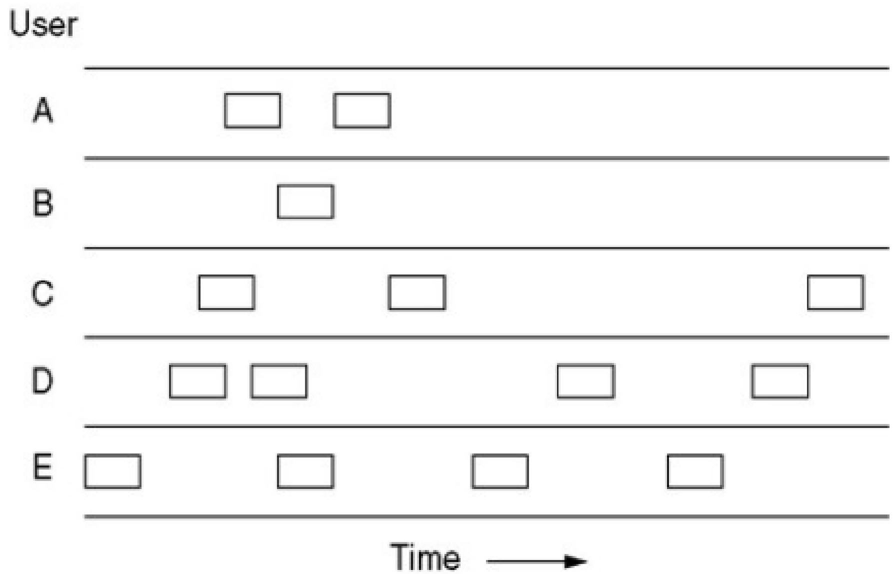
- Station Model.
  - The model consists of N independent stations
- Single Channel Assumption.
  - A single channel is available for all communications
- Collision Assumption.
  - If two frames are transmitted simultaneously , they overlap in time and the resulting signal is garbled. This event is called a ***collision***.
  - All station can detect collisions
  - A collided frame must be transmitted again latter
  - There are no errors other than those generated by collisions

Multiple Access Protocols

- ALOHA
- Carrier Sense Multiple Access Protocols
- Collision-Free Protocols

Pure ALOHA (1)

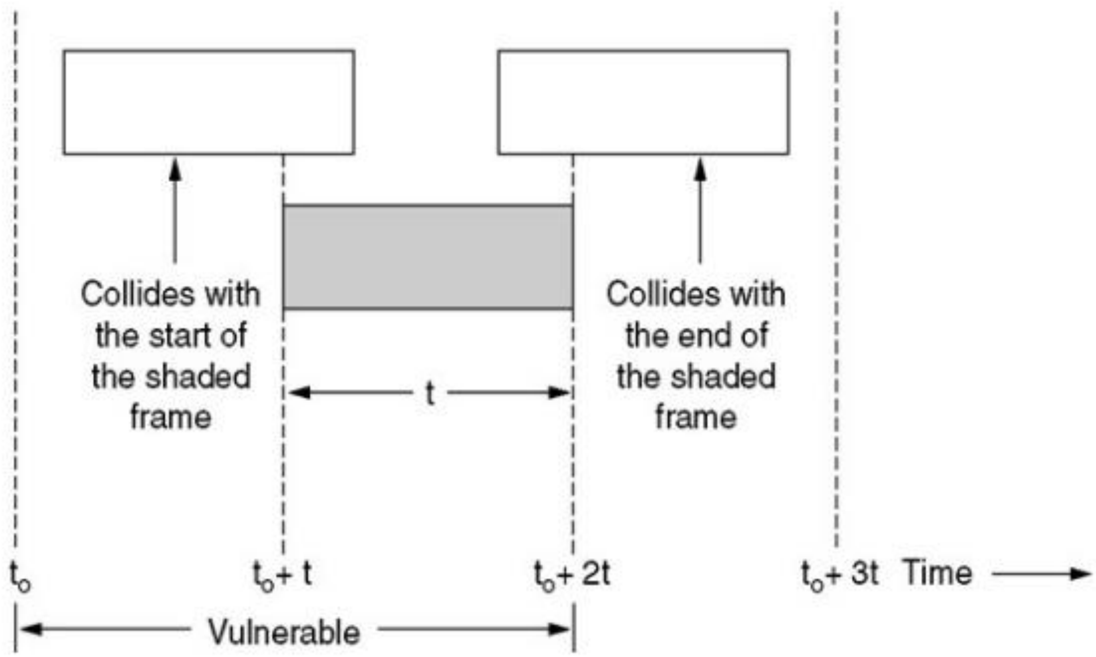
In pure ALOHA, frames are transmitted at completely arbitrary times.



- Frame time – the amount of time needed to transmit the standard fixed length frame
- An infinite population of users generates new frames according to a Poisson distribution, with mean N frames per time frame.
  - If N >1 than more frames than the channel can handle
  - 0<N<1 for reasonable throughput

- In addition to new frames, stations generate retransmissions. The probability of k transmission attempts per frame time, old and new combined, is also Poisson, with mean G per frame
  - G >= N (equal when there are no retransmissions)
- Throughput of a channel is:
  - S = G P0, where P0 is the probability that a frame doesn't suffer collisions

Vulnerable period for the shaded frame.



Slotted ALOHA

Assumptions

- all frames same size
- time is divided into equal size slots, time to transmit 1 frame
- nodes start to transmit frames only at beginning of slots
- nodes are synchronized
- if 2 or more nodes transmit in slot, all nodes detect collision

Operation

- when node obtains fresh frame, it transmits in next slot
- no collision, node can send new frame in next slot
- if collision, node retransmits frame in each subsequent slot with prob. p until success

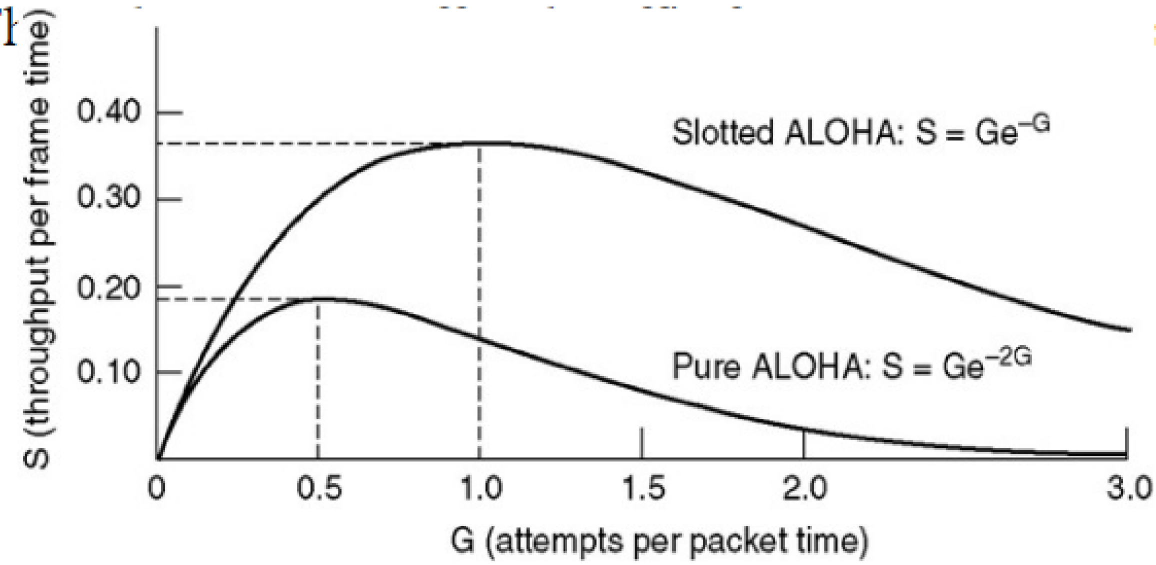
Slotted ALOHA

- The time is divided into discrete intervals, each interval corresponding to one frame.
- The users will need to be synchronized with the beginning of the slot
  - Special station can emit a pip at the start of each interval
- A computer is not allowed to send data at any arbitrary times, it will be forced to wait until the next valid time interval
- Since the vulnerable period is now halved, the throughput of this method would be:
- Slotted ALOHA peaks at G=1 :: so S=1/e=.368 (i.e. 37 % success)…..a small increase in channel load will drastically reduce its performance.

$$S = Ge^{-G}$$

Pure ALOHA vs. Slotted ALOHA

Th s.



CSMA Protocols

- Are protocols in which stations listen for a carrier (i.e. transmission) and act accordingly
- Networks based on these protocols can achieve better channel utilization than 1/e
- Protocols
  - 1 persistent CSMA
  - Non persistent CSMA
  - p persistent CSMA
  - CSMA CD

1 Persistent CSMA

- 1 persistent CSMA
  - When a station has data to send, it first listens to the channel
  - If channel is busy, the station waits until the channel is free. When detects an idle channel, it transmits the frame
  - If collision occurs, it will wait an random amount of time and starts again
  - The protocol is called 1 persistent, because the station sends with probability of 1 when finds the channel idle, meaning that is continuously listening
  - Propagation delay

Non Persistent CSMA

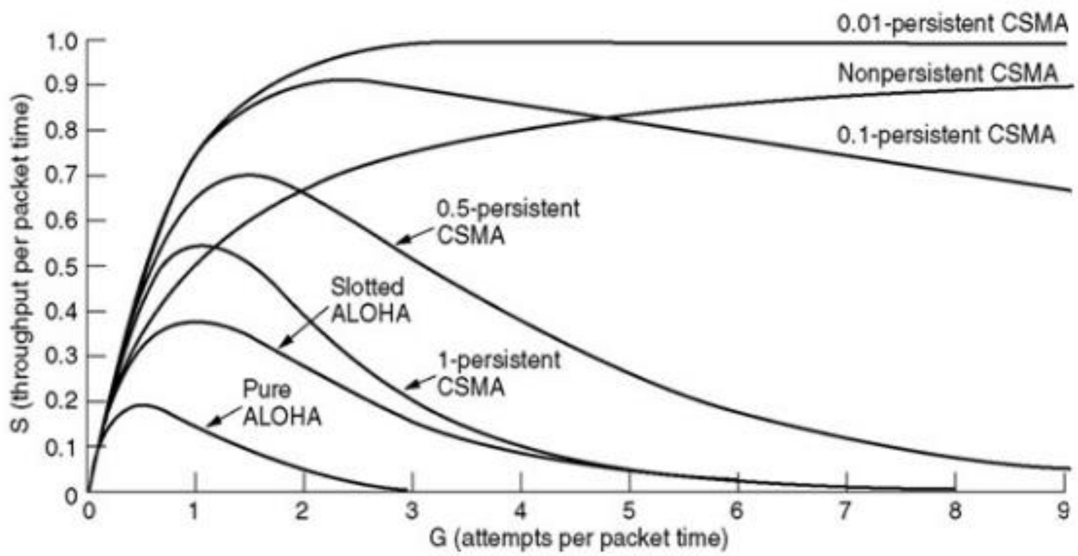
- Before sending a station senses the channel. If no activity, it sends its frame
- If channel is busy, then will not continue to sense the channel until it becomes idle, but it will retry at a latter time (waiting a random period of time and repeating the algorithm)
- With this algorithm, fewer collisions will happen; thus better channel utilization but with longer delays than 1 persistent CSMA algorithm

p Persistent CSMA

- It applies to slotted channels
- When a station becomes ready to send, it senses the channel. If it is idle will transmit with a probability of p. With a probability of q it defers to the next slot.
- If next slot is also idle, it transmits or it defers again with probabilities of p and q
- This process is repeated until the frame gets either transmitted or another station it began transmission
- For latter case, the unlucky station acts the same as it would have been a collision (waits a random time and starts again)

Persistent and Non-persistent CSMA

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



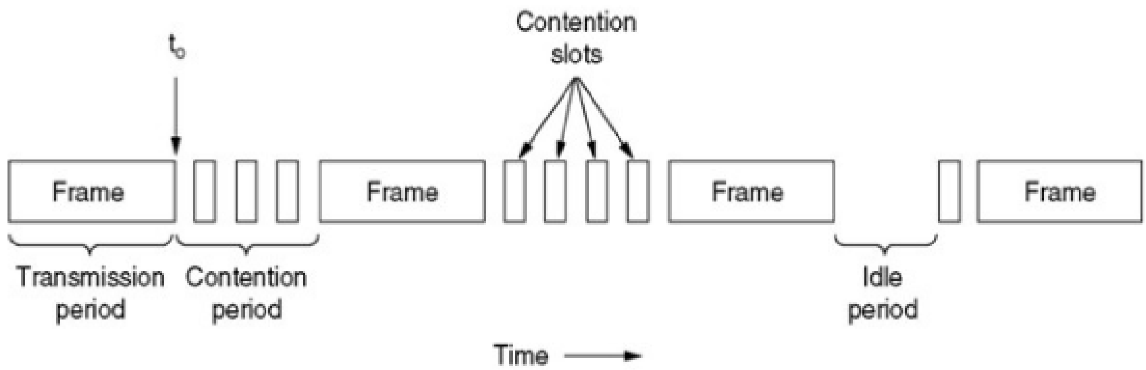
CSMA with Collision Detection

- An improvement over CSMA protocols is for a station to abort its transmission when it senses a collision.
- If two stations sense the channel idle and begin transmission at the same time, they will both detect the collision immediately; there is no point in continuing to send their frames, since they will be garbled.
- Rather than finishing the transmission, they will stop as soon as the collision is detected
  - Saves time and bandwidth

CSMA/CD

- CSMA method that we've learnt just now doesn't specify the procedure following a collision.
- CSMA/CD augments the algorithm to handle the collision
- In the CSMA/CD method, a station monitors the medium after it sends a frame to see of the transmission was a successful. If so, the station is finished. If, however, there is a collision, the frame is sent again.
- To better understand CSMA/CD, see fig 12.12

CSMA with Collision Detection



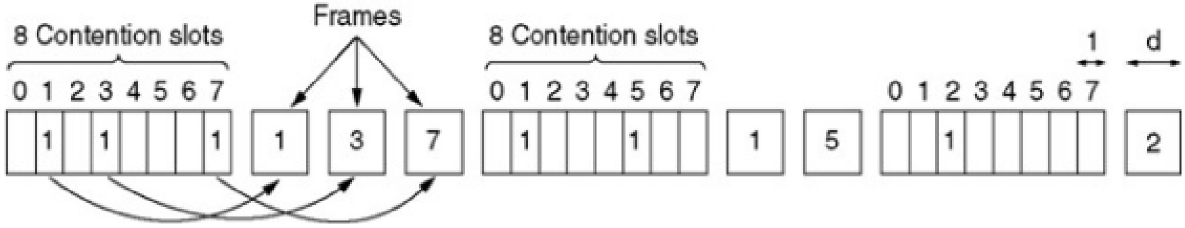
CSMA/CD can be in one of three states:
contention, transmission, or idle.

Collision Free Protocols

- Collisions adversely affect the system performance, especially if the cable is long and the frames are short
- The collision free protocols solve the contention for the transmission channel without an collisions at all
- N stations are assumed to be connected to the same transmission channel
- Protocols
  - Bit-Map Protocol
  - Binary Countdown

Collision-Free Protocols (1)

The basic bit-map protocol.



If station j has a frame to send, it will transmit a 1 in j-th contention slot

Collision-Free Protocols (2)

The binary countdown protocol. A dash indicates silence.