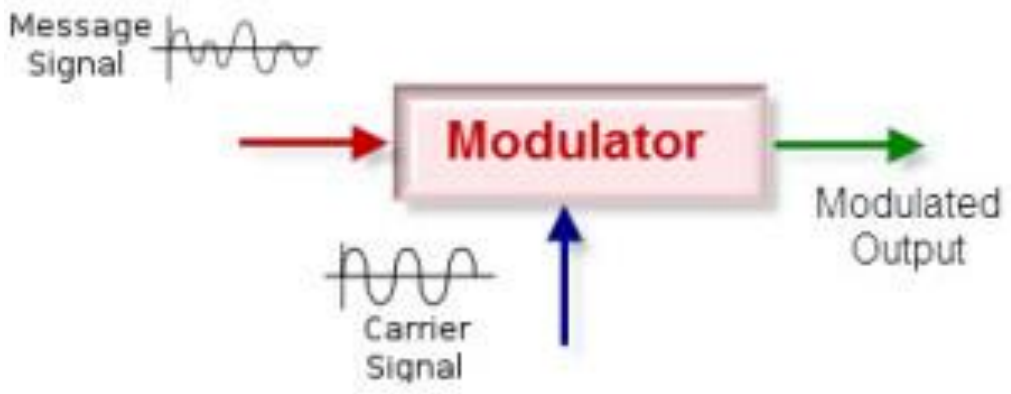
Computer Networks II

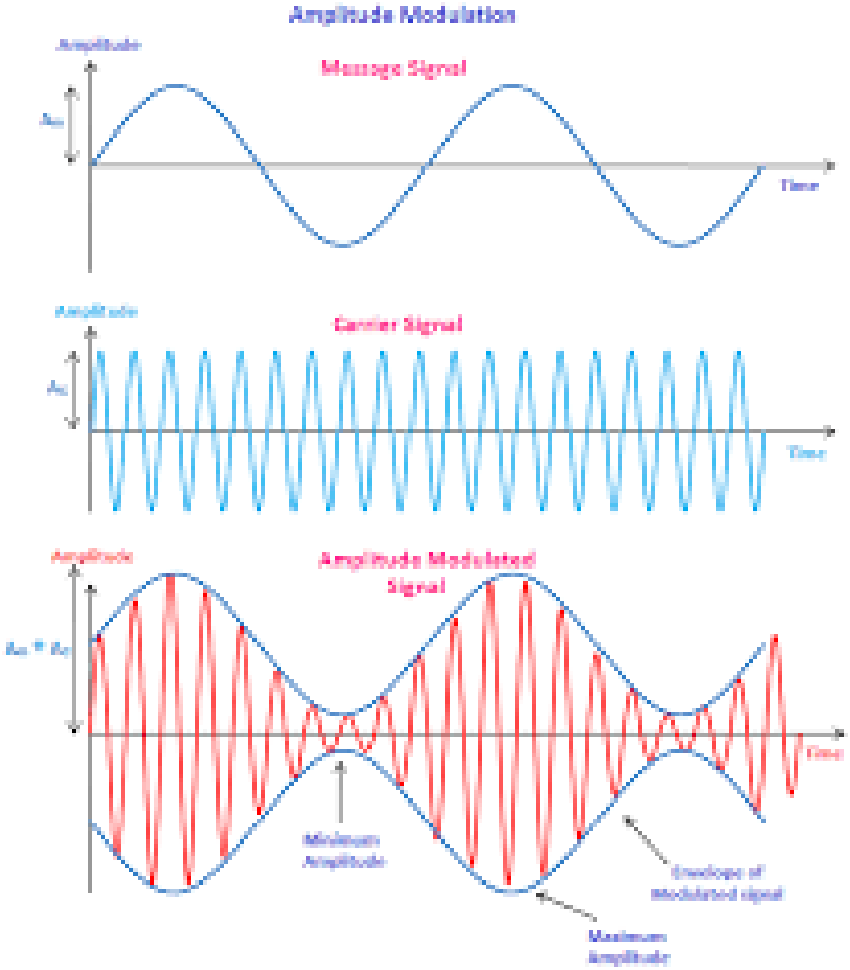
Modulation

- Modulation is a process of **changing the characteristics of the wave to be transmitted by superimposing the message signal on the high frequency signal.**
- In this process video, voice and other data signals modify high frequency signals – also known as carrier wave.
- This carrier wave can be DC or AC or pulse chain depending on the application used. Usually high frequency sine wave is used as a carrier wave signal.



Amplitude modulation

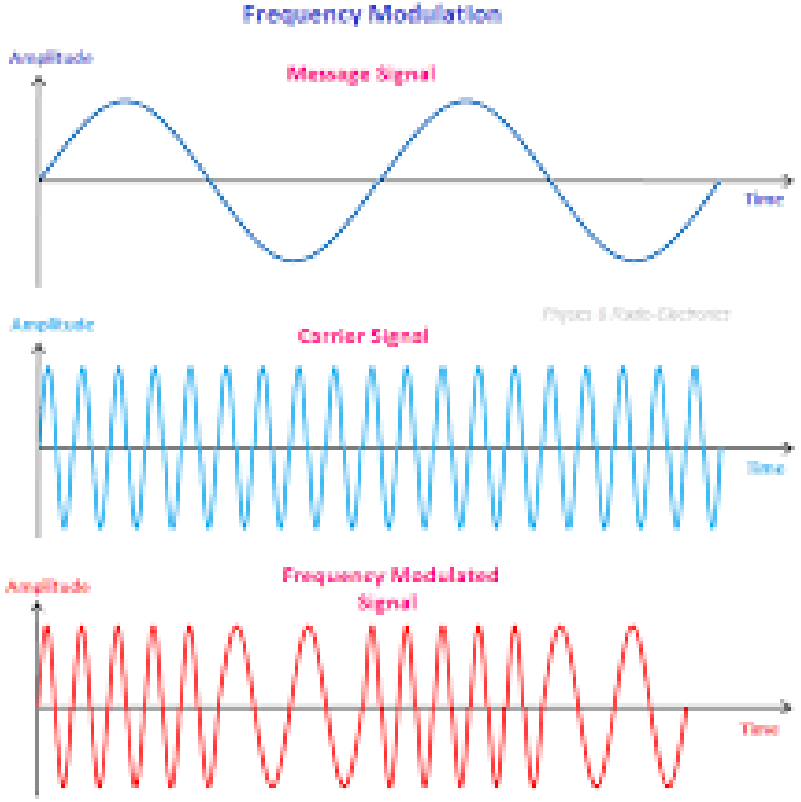
- In amplitude modulation, the **amplitude of the carrier wave is varied in proportion to the message signal**, and the other factors like frequency and phase remain constant.



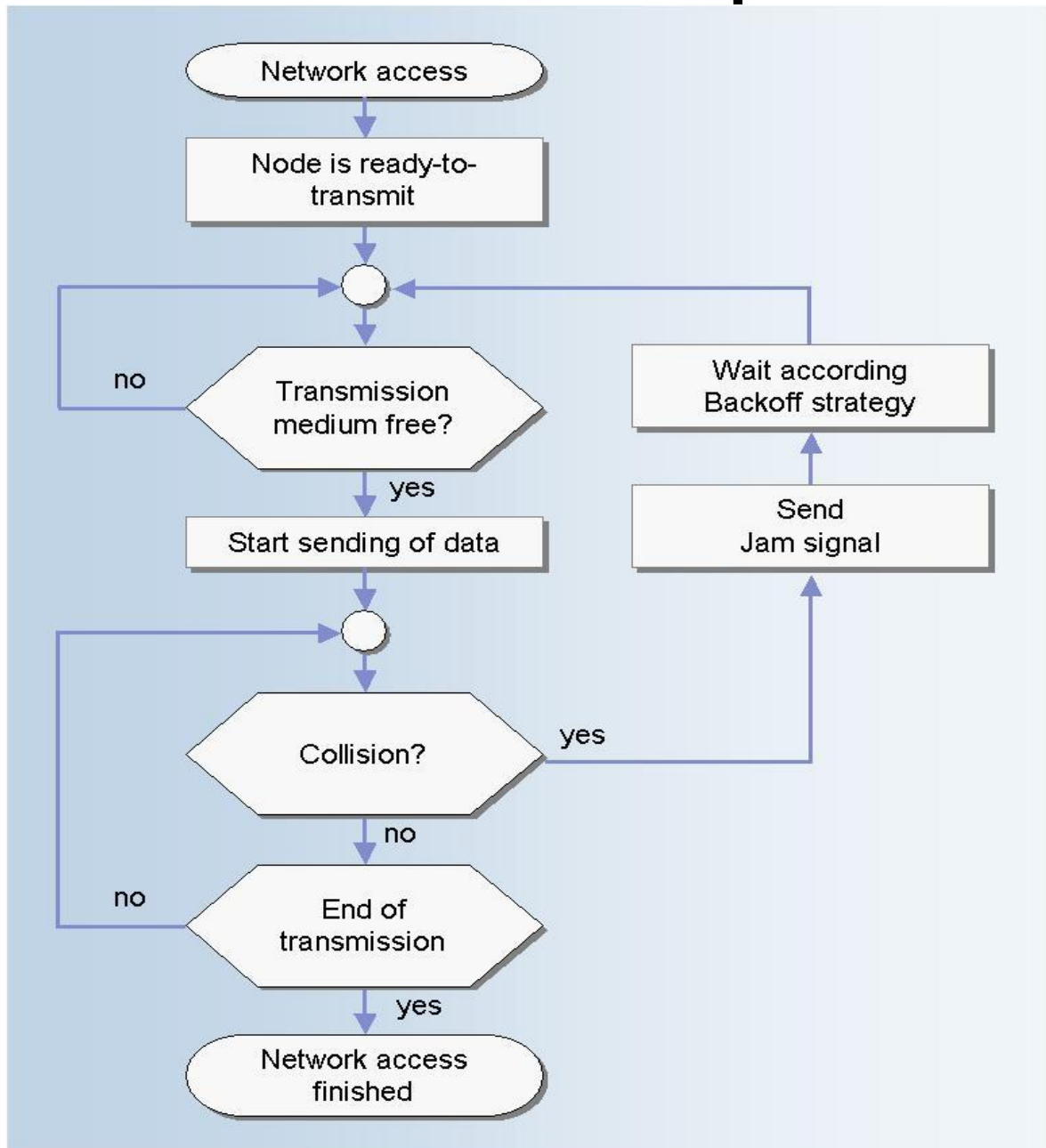
This type of modulation requires greater band width, more power. Filtering is very difficult in this modulation.

Frequency modulation

- It **varies the frequency of the carrier in proportion to the message** or data signal while maintaining other parameters constant.
- The advantage of FM over AM is the greater suppression of noise at the expense of bandwidth in FM. It is used in applications like radio, radar, telemetry seismic prospecting, and so on.



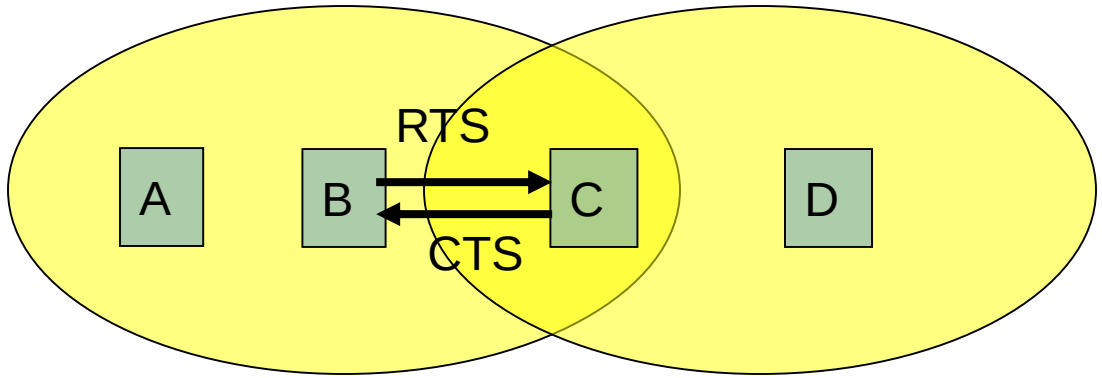
CSMA/CD(Carrier Sense Multiple Access/Collision detection)



CSMA/CA

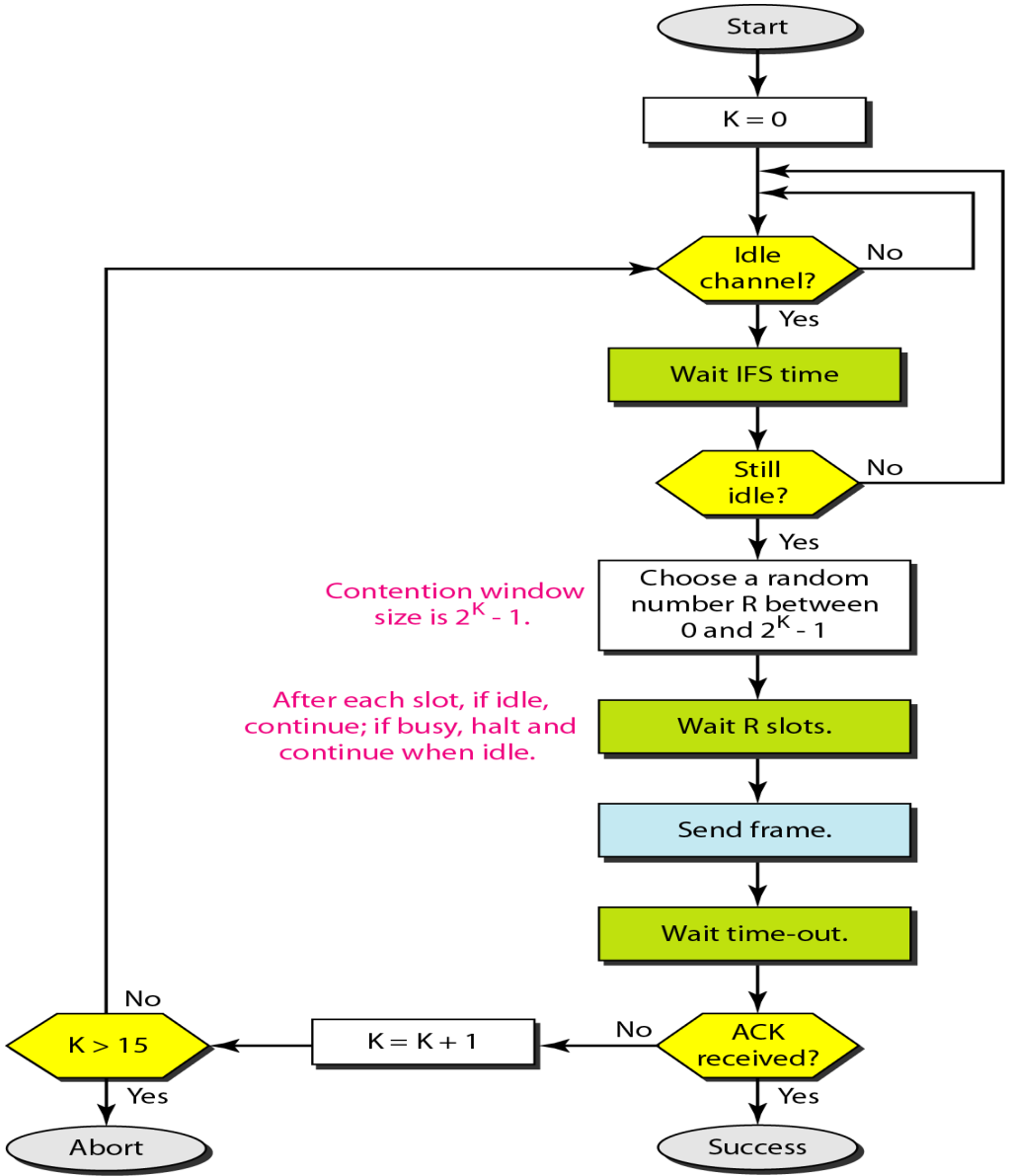
- Since we can’t detect collisions, we avoid them
  - CSMA/CA as opposed to CSMA/CD
  - Not greedy like Ethernet
- CS: listen before transmitting.
  - When medium busy, choose random backoff interval
  - Wait for that many idle timeslots to pass before sending
- CA: transmit short “jamming” signal before sending frame
  - essentially reserves medium, let’s others know your intent to transmit

CSMA/CA with RTS / CTS Protocols



1. B stimulates C with Request To Send (RTS)
2. A hears RTS and defers to allow the CTS
3. C replies to B with Clear To Send (CTS)
4. D hears CTS and defers to allow the data
5. B sends to C

CSMA/CA with ACK



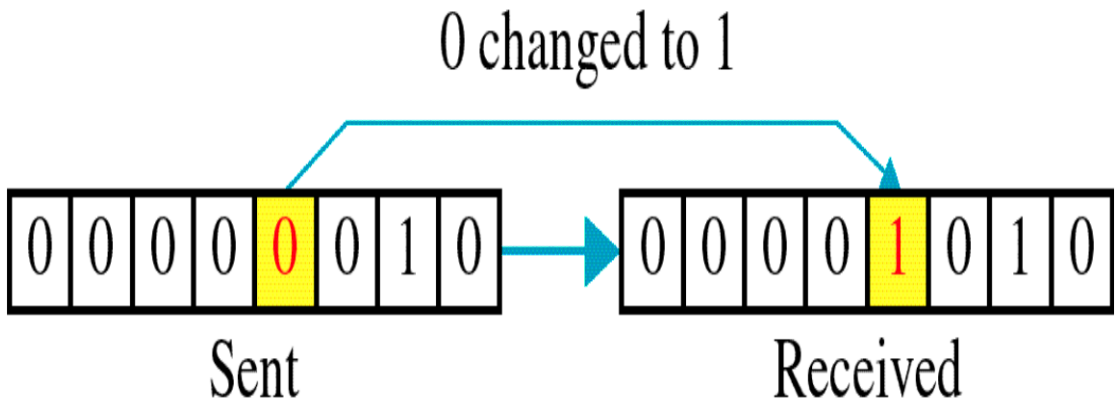
Channel idle? Don't transmit yet!
Wait IFS(Inter Frame Space) time.

Still idle after IFS? Don't transmit yet!
Now in Contention Window.
Choose random number and wait that many slots.

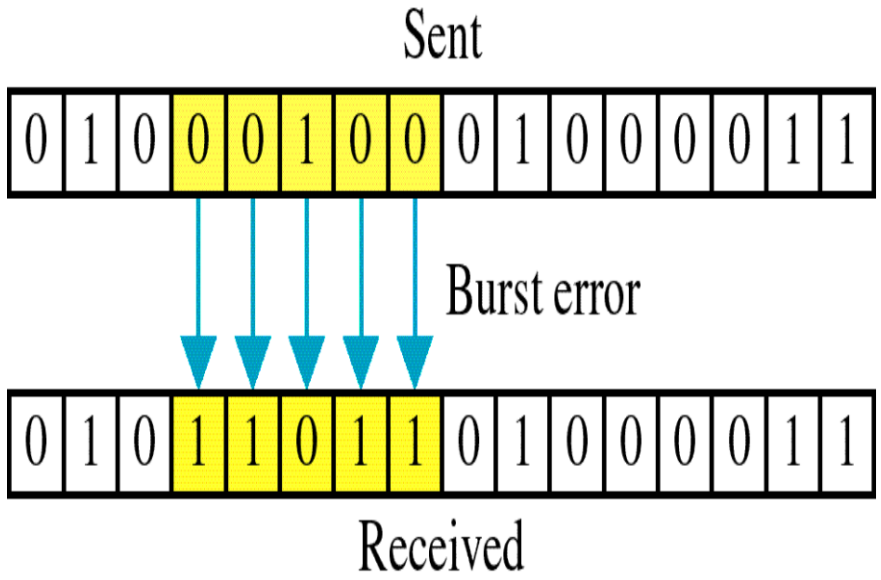
Did you wait R slots and all slots were available? Go ahead, transmit.
Now, wait time-out for a response.

Types of Errors

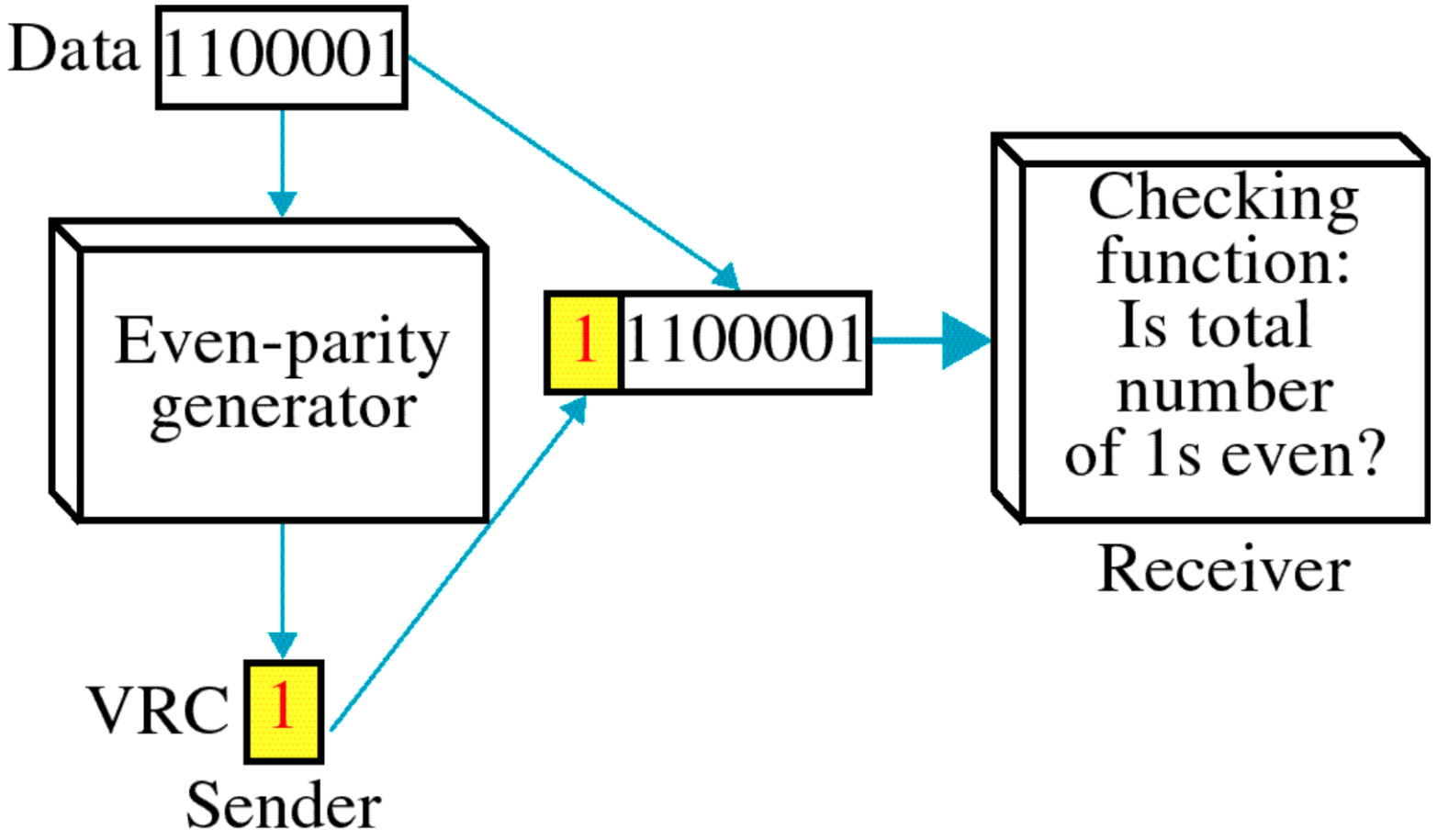
Single Bit Error



Burst Error



Single bit Parity

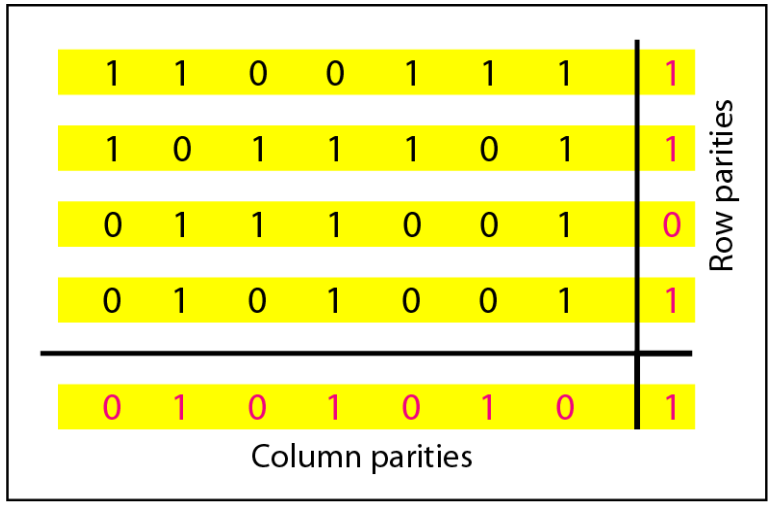


Disadvantages

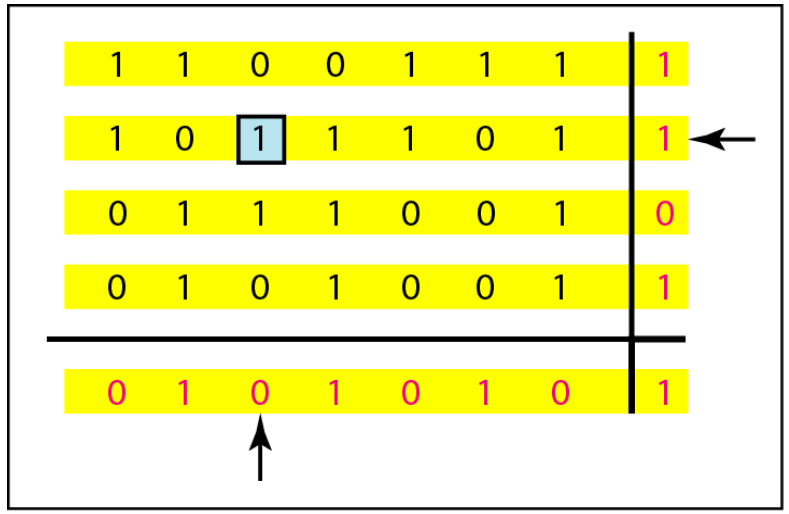
➔It can detect single bit error

➔It can detect burst errors only if the total number of errors is odd.

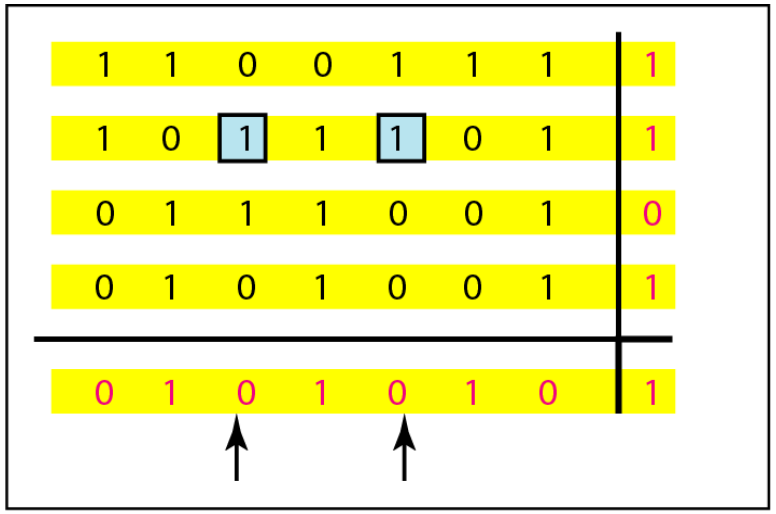
Tw Dimensional Parity checking



a. Design of row and column parities

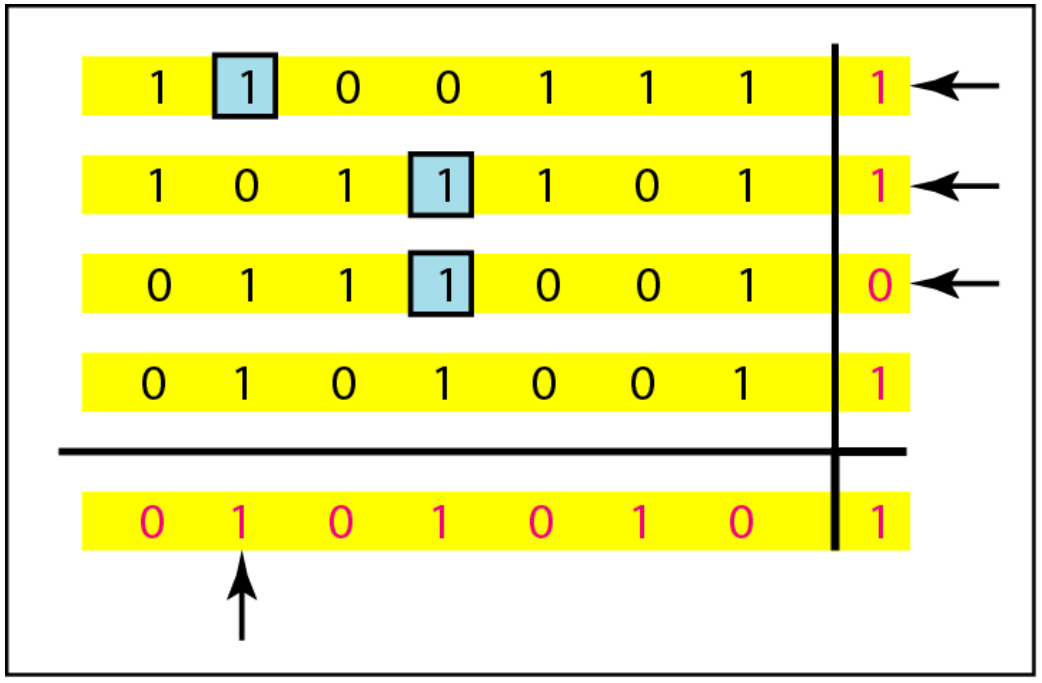


b. One error affects two parities

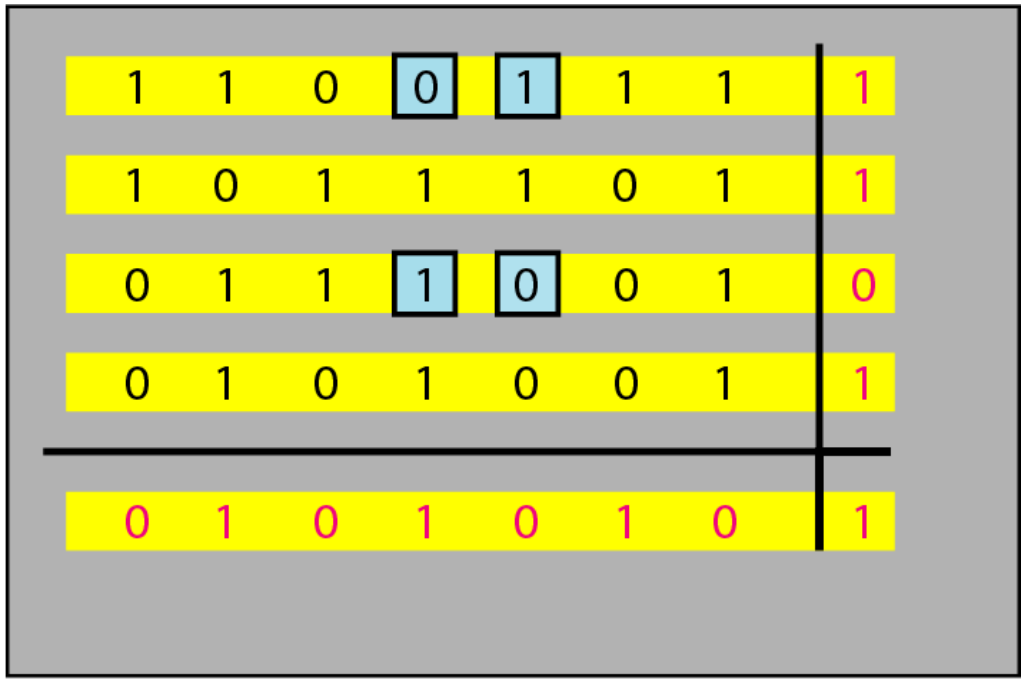


c. Two errors affect two parities

2D Parity Checking



d. Three errors affect four parities



e. Four errors cannot be detected

CheckSum

At sender side,

•If m bit checksum is used, the data unit to be transmitted is divided into segments of m bits.
•All the m bit segments are added.
•The result of the sum is then complemented using 1's complement arithmetic.
•The value so obtained is called as **checksum**.

•The data along with the checksum value is transmitted to the receiver.

At receiver side,

•If m bit checksum is being used, the received data unit is divided into segments of m bits.
•All the m bit segments are added along with the checksum value.
•The value so obtained is complemented and the result is checked.

Original Data

10011001	11100010	00100100	10000100
1	2	3	4

k=4, m=8

Sender

```
1    10011001
2    11100010
     --------
    (1)01111011
           1
     --------
     01111100
3    00100100
     --------
     10100000
4    10000100
     --------
    (1)00100100
           1
     --------
Sum: 00100101
     --------
CheckSum: 11011010
```

Reciever

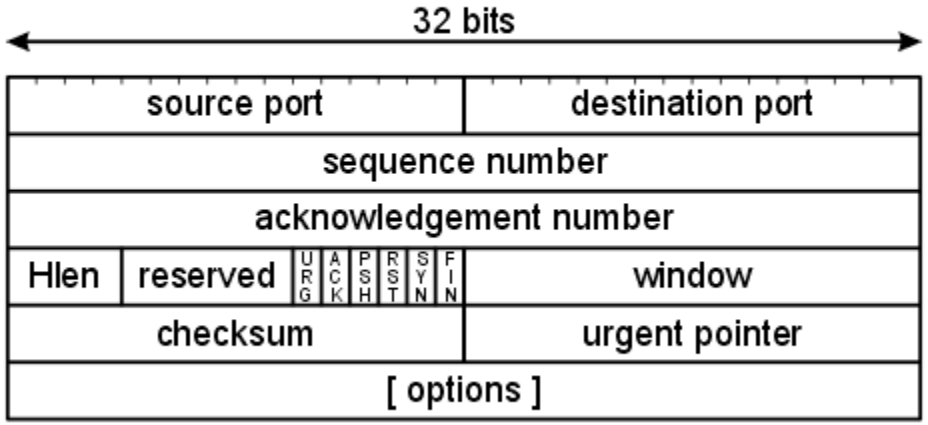
```
1    10011001
2    11100010
     --------
    (1)01111011
           1
     --------
     01111100
3    00100100
     --------
     10100000
4    10000100
     --------
    (1)00100100
           1
     --------
     00100101
     11011010
     --------
Sum: 11111111
Complement: 00000000
```

Conclusion: Accept Data

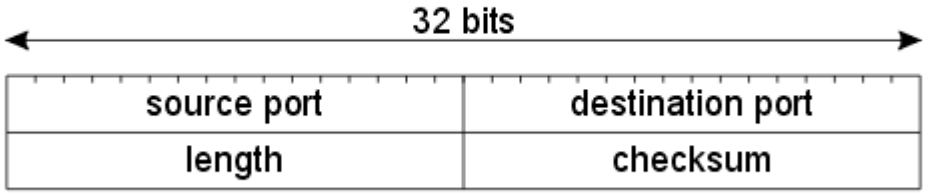
TRANSMISSION CONTROL PROTOCOL (TCP)	USER DATAGRAM PROTOCOL (UDP)
TCP is a connection-oriented protocol. Connection-orientation means that the communicating devices should establish a connection before transmitting data and should close the connection after transmitting the data.	UDP is the Datagram oriented protocol. This is because there is no overhead for opening a connection, maintaining a connection, and terminating a connection. UDP is efficient for broadcast and multicast type of network transmission.
TCP is reliable as it guarantees delivery of data to the destination router.	The delivery of data to the destination cannot be guaranteed in UDP.
TCP provides extensive error checking mechanisms. It is because it provides flow control and acknowledgment of data.	UDP has only the basic error checking mechanism using checksums.
Sequencing of data is a feature of Transmission Control Protocol (TCP). this means that packets arrive in-order at the receiver.	There is no sequencing of data in UDP. If ordering is required, it has to be managed by the application layer.
TCP is comparatively slower than UDP.	UDP is faster, simpler and more efficient than TCP.
Retransmission of lost packets is possible in TCP, but not in UDP.	There is no retransmission of lost packets in User Datagram Protocol (UDP).
TCP header size is 20 bytes.	UDP Header size is 8 bytes.
TCP is heavy-weight.	UDP is lightweight.
TCP is used by HTTP, HTTPs, FTP, SMTP and Telnet	UDP is used by DNS, DHCP, TFTP, SNMP, RIP, and VoIP.

TCP and UDP Headers

TCP header format

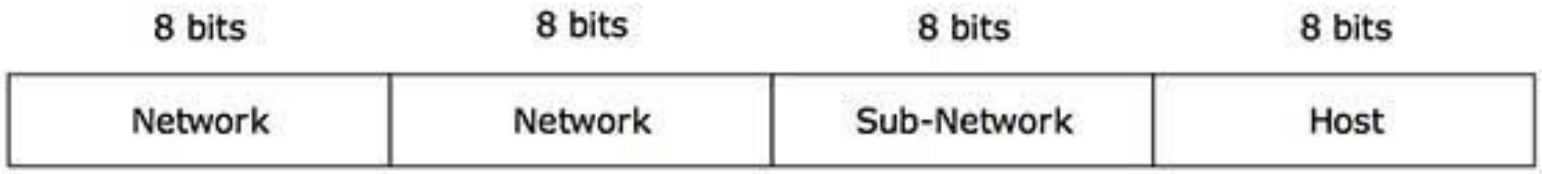


UDP header format



IPv4

- IP provides a mechanism to uniquely identify hosts by an IP addressing scheme. IP uses best effort delivery, i.e. it does not guarantee that packets would be delivered to the destined host, but it will do its best to reach the destination. Internet Protocol version 4 uses 32-bit logical address.
- An IP address, which is 32-bits in length, is divided into two or three parts as depicted −
- No of Networks=2^Network bits
- No of hosts=2^Hosts bits-2

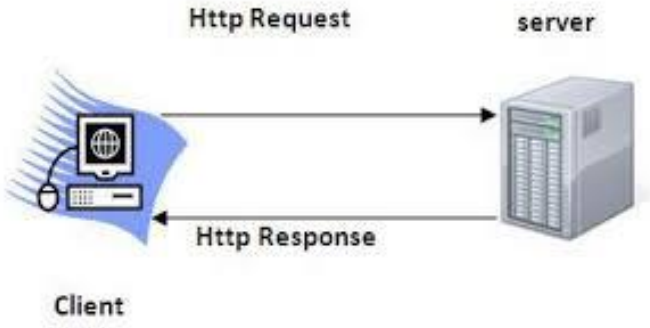


IPv4

- If IP address is 172.3.16.123
- That means network address is:172.3.0.0
- First Host:172.3.0.1
- Last Host:172.3.255.254
- Broadcast address for network is:172.3.255.255
- Loopback testing address:127.0.0.0

HTTP-Hyper Text Transfer Protocol

- Basically, HTTP is a TCP/IP based communication protocol, that is used to deliver data (HTML files, image files, query results, etc.) on the World Wide Web.
- The default port is TCP 80.
- HTTP functions as a request–response protocol in the client–server computing model.
- A web browser, for example, may be the *client* and an application running on a computer hosting a website may be the *server*. The client submits an HTTP *request* message to the server.
- The server, which provides *resources* such as HTML files and other content, or performs other functions on behalf of the client, returns a *response* message to the client. The response contains completion status information about the request and may also contain requested content in its message body.



FTP

- File Transfer Protocol (FTP) is a standard Internet protocol for transmitting files between computers on the Internet over TCP/IP connections.
- FTP is a client-server protocol where a client will ask for a file, and a local or remote server will provide it.
- FTP is a client-server protocol that relies on two communications channels between client and server: a command channel for controlling the conversation and a data channel for transmitting file content.
- Clients initiate conversations with servers by requesting to download a file. Using FTP, a client can upload, download, delete, rename, move and copy files on a server.
- A user typically needs to log on to the FTP server, although some servers make some or all of their content available without login, known as anonymous FTP
- PORT NO:20(Data connection) and 21(Control Connection)

POP

- Post Office Protocol (POP) is a type of computer networking and Internet standard protocol that extracts and retrieves email from a remote mail server for access by the host machine.
- POP uses the TCP/IP protocol stack for network connection and works with Simple Mail Transfer Protocol (SMTP) for end-to-end email communication, where POP pulls messages and SMTP pushes them to the server.
- POP is a protocol used to retrieve e-mail from a mail server. Most e-mail applications (sometimes called an *e-mail client*) use the POP protocol, although some can use the newer IMAP
- PORT NO:110 or 995

IMAP

- IMAP is the better option - and the recommended option - when you need to check your emails from multiple devices, such as a work laptop, a home computer, or a tablet, smartphone, or other mobile device. Tap into your synced (updated) account from any device with IMAP.

- POP3 downloads email from a server to a single computer, then deletes it from the server. Because your messages get downloaded to a single computer or device and then deleted from the server, it can appear that mail is missing or disappearing from your Inbox if you try to check your mail from a different computer.

SMTP

- SMTP stands for Simple Mail Transfer Protocol.
- It is a TCP protocol used for sending messages to other computer users based on e-mail addresses.
- It provides a mail exchange between users on the same or different computers, and it also supports:
  - It can send a single message to one or more recipients.
  - Sending message can include text, voice, video or graphics.
  - It can also send the messages on networks outside the internet.
- The main purpose of SMTP is used to set up communication rules between servers. The servers have a way of identifying themselves and announcing what kind of communication they are trying to perform.
- They also have a way of handling the errors such as incorrect email address. For example, if the recipient address is wrong, then receiving server reply with an error message of some kind.
- PORT NO:25

SMTP and POP/IMAP