(1) Devices

Page No.
Date: / /

Computer Networks - Nodes Connected to by wired or wireless links.

Basic characteristics of CN

(1) Fault tolerance
- → Continue working despite of failure
- → Ensure no loss of service

(2) Scalability
- → Grow based on needs
- → Have good performance after growth

(3) Quality of service
- → Ability to set priorities
- → Manage data traffic

(4) Security
- → ability to prevent
  - → unauthorized access
  - → forgery
  - → Misuse
- → ability to provide
  - → Confidentiality
  - → Integrity
  - → availability

(1) Data Communication

Data Communication are the exchange of data between two nodes via some form of link (transmission) such as a cable

Page No.
Date :

Data flow

Simplex (Unidirectional) Ex Keyboard

Half duplex (Both direction but not at same time) Ex. Walkie Talkie

Full duplex (Both direction at same time) Ex → telephone line

Protocols - network communication
(Elements of protocol →)

(1) Message encoding

Message source → Encoder → Transmitter → Transmission medium

Message destination ← Decoder ← Receiver ← (Signal)

(2) Message formatting & encapsulation
Agreed format.
Encapsulate the info to identify the sender & the receiver
properly

(3) Message size
Long messages must be broken into smaller pieces
to travel across a network

(4) Message timing
flow control. Response timeout

(5) Msg delivery options
(1) Unicast
(2) Multicast
(3) Broadcast

Protocols
It determines
(1) What is Communicated
(2) How it is —11—
(3) When it is —11—

Page No.
Date : / /

Peer to Peer Network
→ No Centralized administration
→ All peers are equal
→ Simple sharing application
→ Not scalable

Client Server Network
→ Centralized administration
→ Request - Response Model
→ Scalable
→ Server may be overloaded

Components of CN
(1) Nodes
- End nodes: Computers, VoIP Phones, Security Cameras
- Intermediary Nodes: Switches, Bridges, Hubs, Repeaters, Cell towers

(2) Media
- Wired Medium: Ethernet straight through Cable, Ethernet crossover cable, fiber Optic Cable, Coaxial Cable, USB Cable
- Wireless Medium: Infared - TV remote, Radio - Bluetooth, wifi, Micro waves - Cell Phones, Satellite - GPS

(3) Services

e-mail, online games, storage services, Voice over IP, file sharing, Video telephony

Page No.
Date: / /

Classification of CN

LAN — MAN — WAN

LAN: Wired - School Laboratory; Wireless - Wifi

MAN: Switches / Hub; Routers / Bridges

WAN: Internet

New trends
(1) Bring Your Own Device
(2) Online Collaboration
(3) Cloud Computing

SAN (Storage Area Network)
Cloud Computing

~~Ring~~	Number of Nodes	No of Cables	No. of ports/device	Total number of ports in the network
Ring	N	N	2	2×N
Star	N	N	1	2×N
Mesh	~~N·(N-1)~~ / 2	N·(N-1) / 2	N-1	N(N-1)

IP Address

Page No.
Date :

→ IP - Internet protocol
→ Every node in network is identified using IP address
→ 0.0.0.0 to 255.255.255.255 (32 bits)

Mac Address (Physical address)

→ (Media Access Control)
→ Every node in the LAN is identified with the help of MAC address
→ IP = location of a person
Mac = Name of person
→ Unique / Cannot be changed / Assigned by manufacturer
→ Ex: 70-20-84-00-ED-FC
→ Separator - hyphen, period, semicolon

Port Address

Friend sends you are parcel.
Reaching our city = Reaching our network (IP)
Reaching our apartment = Reaching the host (Mac)
Reaching right person = Reaching right process (Port)

→ In a node, many process will be running
Every process in a node is uniquely identified using port numbers
→ Port = Communication endpoint.

Key points

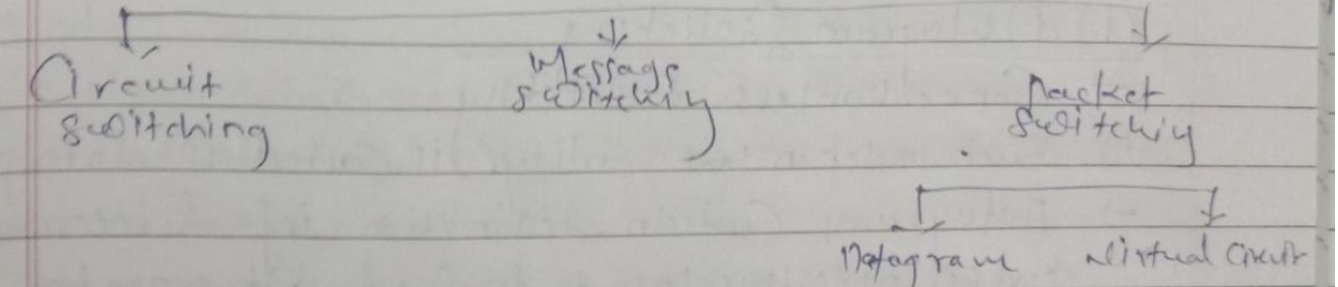
→ ~~Attach source IP address & destination~~

Switching techniques

→ Switching in CN helps in deciding the best route for data transmission if there are multiple routes in a larger network

→ One to one Connection

Switching techniques



(1) Circuit switching

3 phases

(1) Connection establishment
(2) Data transfer
(3) Connection disconnection

(2) Message switching

→ store & forward mechanism
→ Message is transferred as a complete unit & forwarded using store & forward mechanism at intermediary node
→ Not suited for streaming media & real-time application

(3) Packet switching

→ Internet is a packet switched network
→ Message is broken into individual chunks called as packets
→ Each packet sent individually

→ Each packet will have source & destination IP address with sequence number
→ Sequence number will help to receiver to Page No. Date:
- Reorder the packets
- Detects missing packet
- Sent acknowledgment

(i) Datagram Switching

→ Connectionless Switching
→ Each independent entity is called as datagram
→ Datagrams Contain destination info & intermediate device uses this info to forward datagram to right destination
→ ~~Here~~ Here path is not fixed
→ Intermediate nodes take the routing decisions to forward the packets

(ii) Virtual Circuit

→ Connection oriented Switching
→ A preplanned route is established before the messages are sent
→ Call request & Call accept packets are used to establish the Connection between Sender & receiver
→ Path is fixed for the duration of a logical Connection

Layering in CN

Layering - Decomposing the problem into more manageable Components
→ It provides more modular design
→ Easy to troubleshoot

Role of Protocols in layering

→ protocols is a set of rules that governs data Communication
→ protocols in each layer governs the activities of the data Communication

layered Architectures

OSI Model

→ Open system InterConnection
→ Made for understanding & designing network architecture i.e flexible robust & interoperable
→ Developed by ISO
→ Not a protocol
→ only a guideline hence refred as OSI referrance model
→ the purpose of OSI model is to show how to facilitate Communication between two machines having diff OS (linux, Ubuntu, Window etc)
→ Not ever fully implemented.

TCP/IP

→ TCP/IP = Transmission Control protocol / Internet protocol
→ Was developed prior to OSI
→ i.e layer here do not match all
→ It is a hierarchical protocol made of interactive modules, each of which provide a specific functionality.

OSI Reference Model

→ Purpose of the OSI Model is to facilitate Communication between diff systems without requiring changes to the logic of the underlying hardware & software

Please Do Not Throw Sausage Pizza Away

Physical layer	Data link layer	Network layer	Transport layer	Session layer	Presentation layer	Application layer

Application Layer

→ It enables the user to access the network resources
→ Services provided by Application Layer
- File transfer and Access Management
- Mail services
- Directory Services

Presentation layer

→ It is concerned with the syntax & semantics of the information exchanged between two systems
→ Services
- Translation
- Encryption
- Compression

Session layer

→ Establishes, maintains, & synchronizes the interaction among communicating devices
→ Services
- Dialog Control
- Synchronization

Transport layer

→ It is responsible for process to process delivery of the entire message
→ Services
- Port addressing
- Segmentation & Reassembly
- Connection Control
- End to End flow Control
- Error Control

Network Layer

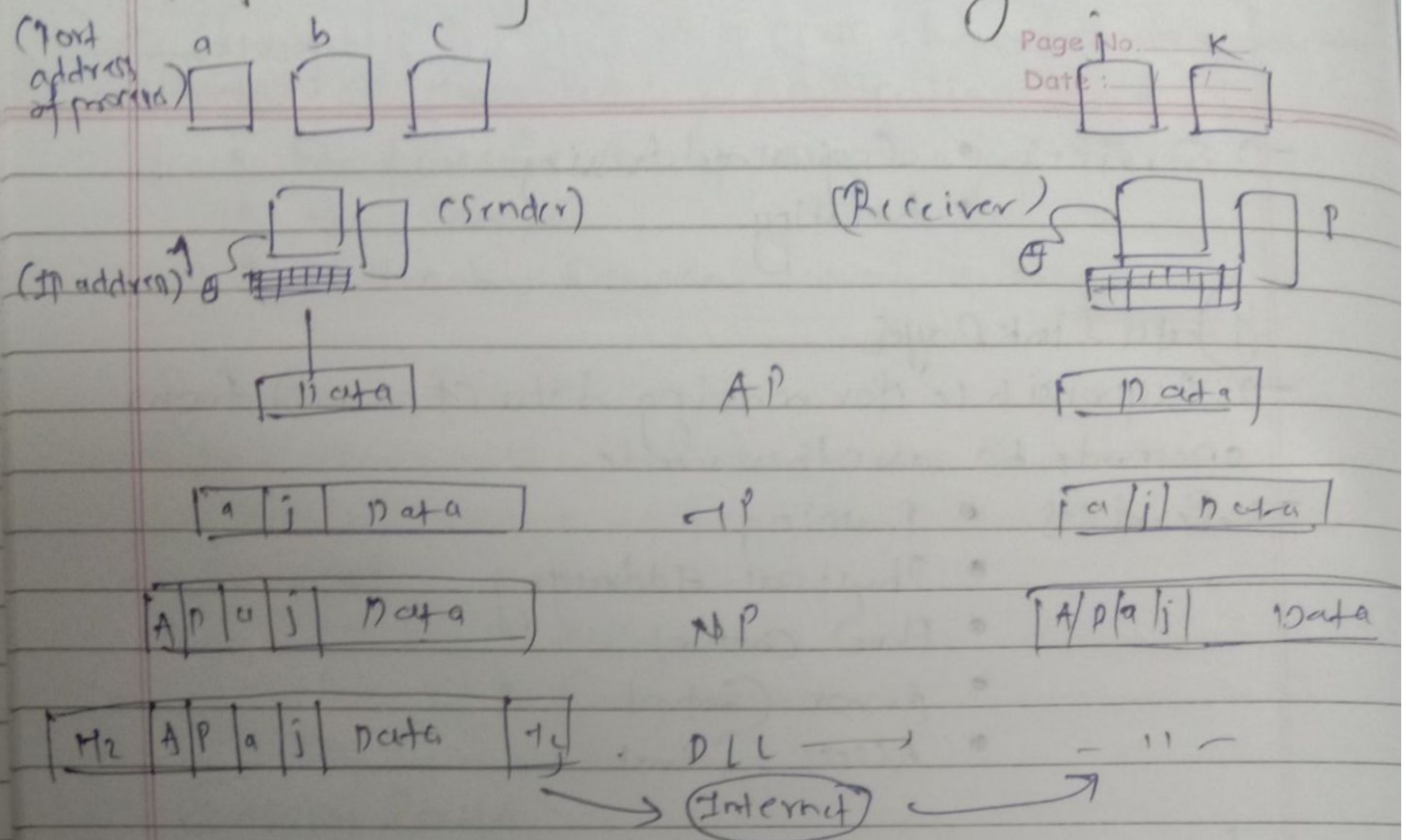
→ It is responsible for delivery of data from the original source to the destination network

→ Services • Logical addressing
• Routing

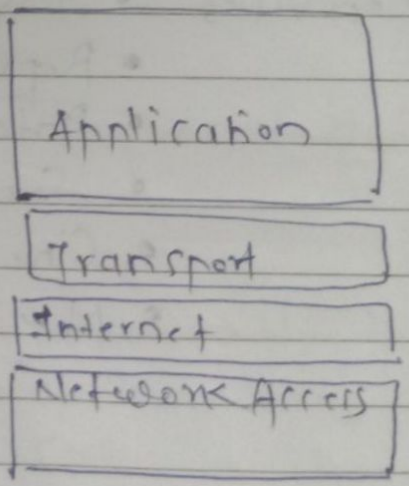
(1) Data link layer
→ Responsible for moving data (frames) from one node to another node.
→ Services • Framing
• Physical Addressing
• Flow Control
• Error Control
• Access Control

Physical layer
→ Responsible for transmitting bits over a medium. It also provides electrical & mechanical specifications
→ Services • Physical characteristics of the media
• Representation of bits
• Data rate
• Synchronization of bits
• Line Configuration
• Physical Topology

Port addressing and IP addressing



OSI Vs TCP/IP



Application	HTTP, DNS,
Presentation	DHCP, FTP
Session	
Transport	TCP, UDP
Network	IPV4, IPV6, ICMPV4, ICMPV6
Data link	PPP, Frame Relay
Physical	Ethernet

~~OSI Model~~

TCP/IP Model

Application - Represents data to the user, plus encoding & dialog control

Transport - Supports communication between diverse device across diverse networks

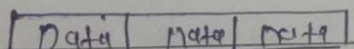
Internet - Determines the best path through the network

Network Access - Controls the hardware devices and media that make up the network

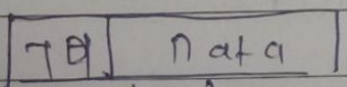
Protocol Data Unit (PDU)

Protocol Data Units (PDUs) are named according to the protocols of the TCP/IP suite: data, segment, packet, frame & bits

Email Data

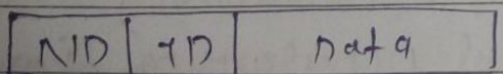


Data

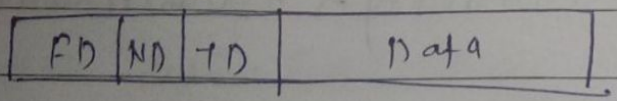


(Transport Header)

Segment



Packet.



Frame
(Medium Dependent)

1011000110010011

Bits.

Page No.
Date :

Basic Networking Commands

(1) ipconfig – Used to display and manage IP address assigned to the machine

(2) ipconfig /all – To show info about your network adapter

(3) ping – is the primary TCP/IP command used to troubleshoot connectivity, reachability & name resolution

(4) Tracert – for displaying the time it takes for a packet of info to travel between a local computer and distination IP address or domain

(5) Nslookup – To find info about another comp with the ip address

Basics of Cisco Packet tracer

→ Cisco – leading company in networking
→ An innovative & powerful networking simulation tool used for practice, discovery & troubleshooting

Hub

→ works at the physical layer
→ Used to set up LAN
→ Has multiple ports

→ Star topology

→ When a packet arrives at one port, it is copied to the other ports so that all segments of the LAN can see all packets

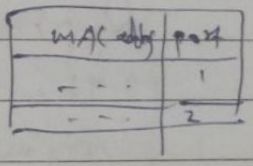
> Note - Different devices - Ethernet straight cable
> Same devices - Ethernet cross cable

Pros
(1) Cheaper than switches
(2) Works good for small network

Cons
(1) Issues in broadcast
(2) No memory

Switch

→ Networking hardware that connects devices on a computer network to establish a local area network.
→ Unlike hub, switch has memory
→ Stores MAC address table
→ Layer 2 device for setting up LAN



Hub	Switch
• Layer 1 devic (Physical layer)	Layer 2 device (Datalink layer)
• Has no memory	Stores MAC address table
• Not an intelligent device	Intelligent device
• Floods the network with broadcasting	Can do unicasting, multicasting, broadcasting
• Security risks are high	Security risks are low
• Less efficient	More efficient
• Half duplex	Full duplex

Basics of Router.

- → Networking device that forwards data packets between two Computer Network
- → A router is Connected to at least two networks, Commonly two LANs or WANs or a LAN and its ISP's network
- → It is a layer 3 (Network layer) device
- → Stores routing table

	Switch	Router
(1)	to connect many devices on a LAN	to connect one local networks to other n
(2)	operates at data link layer	Operates at Network layer
(3)	Has memory & stores MAC address	Has memory & stores routing table
(4)	decisions are taken based on mac address	— " — IP address
(5)	Half / full duplex	full duplex
(6)	LAN	LAN, MAN, WAN

Repeater

- → The data signals generally become too weak or corrupted if they tend to travel a long distance
- → Repeater regenerates the signal over the same network
- → It operates at the physical layer
- → They do not amplify the signal
- → It is a 2 port device

Basics of Bridge

- → Bridge = Repeater + functionality of reading MAC address
- → It is a layer 2 device
- → Used for interconnecting two LANs on the same protocol
- → It is a 2 port device

Page No.
Date : / /

Types of Bridges

(1) Transparent Bridges
→ These are the bridges in which the stations are completely unaware of the bridge's existence
→ Reconfiguration of the stations is unnecessary even if bridge is added or removed from network

(2) Source Routing Bridges
→ Here routing operation is performed by source station and frame specifies which route to follow

→ Various networking devices
Repeater, Hub, Switch, Bridge, Router, Multi-layer switch, Router, Modem, Firewall

Fundamental principles of physical layer
(1) Major function of the physical layer is to move data in the form of electromagnetic signal across a transmission medium
(2) The data usable to a person or an application are not in a form that can be transmitted over a network
(3) For ex, an image must first be changed to a form that transmission media can accept
(4) To be transmitted, data must be transformed to electromagnetic signals

Page No.
Date : / /

Signal

→ It is a function that represents the variation of a physical quantity with respect to time
→ Ex. Variation in temp of a city in one day i.e. 24 hrs
→ Analog and Digital Signal

Analog Signal

→ Signal that can take any value in defined range
→ All real life signals

Digital Signal

→ Signal that can take on of the finite values at any given time
→ Here we discretize both time & magnitude

Media	Physical Components	Signals
Copper Cable		electromagnetic signal
Fiber Optic Cable		• A light pulse equals 1 • No light pulse is 0
Wireless Media		Radio waves

Wired Media

Copper Cable (Ethernet Cable) | Copper Coaxial Cable | Fiber optic Cable

- Unshielded Twisted Pair
- Shielded Twisted Pair

Physical Layer

→ Responsible for transmitting bits over a medium
→ Services
- Physical characteristics of media
- Representation of bits
- Data rate
- Synchronization of bits
- Line Config
- Physical topology
- Transmission mode

Line Configuration

→ In a network two or more nodes are connected by a communication link that can be wired or wireless
→ for visualization links are imagined as a line between two points
→ for communication to happen, two nodes must be connected to the same link at the same time
→ This is called as line config or connection

Types → (1) Point to Point
(2) Multipoint Connection

Link Layer Services

Data Link Layer

Responsible for moving data (frame) from one node to another node
Services - framing, physical addressing, flow control, Error Control, Access Control

(1) Framing - The data link layer needs to pack bits into frames, so that each frame is distinguishable from one another

→ Our postal ~~service~~ system practices a type of framing
→ The simple act of inserting a letter into an envelope separates one piece of info from another; the envelope serves as the delimiter

(2) Physical Addressing
→ Encapsulation of the header & trailer info with the packet
→ In the header, the source & destination mac address are dealt

(3) Flow Control
→ Flow Control is one of the duties of data link Control sublayer.
→ The flow control in data link layer is end to end flow control
→ Speed matching mechanism
→ It co-ordinates the amount of data that can be sent before receiving an acknowledgment

(4) Access Control
→ Media Access Control

(5) Error Control
→ Error Detection & Correction

Sublayers of DLL

Page No.
Date : / /

Logical Link Sublayer

→ Takes the network protocol data & adds control info to help deliver the packet to the destination (Flow Control)

① Data Encapsulation

→ Frame assembly before transmission & frame disassembly upon reception of a frame

→ MAC layer adds a header & trailer to the network layer PDU

MAC Sublayer

→ Constituted the lower sublayer of data link layer

→ Implemented by hardware, typically in the computer NIC

→ Two primary responsibilities
- Data encapsulation
- Media Access Control
- Framing
- physical MAC addressing
- Error Control

→ Responsible for the placement of frames on the media & removal of frames in media

→ Communicates directly with physical layer

Framing

→ Framing in the data link layer separates a frame distinguishable from another frame

→ Frame = Header + Network layer PDU + Trailer

→ In packet switched network, the block of data called frames are exchanged between nodes, not bit streams

→ When node A wishes to transmit a frame to node B it tells its adaptor to transmit a frame from the node's memory

→ This results in a sequence of bits being sent over the link

→ The adaptor on node B then collects together the sequence of bits arriving on the link & deposits the corresponding frame in B's memory.

Types

Fixed size framing
→ Here the size of the frame is fixed so the frame length acts as delimiter of the frame
→ Consequently, it does not require additional boundary bits to identify the start & end of the frame

Variable size framing
→ Here the size of each frame to be transmitted may be diff
→ So additional mechanism are kept to mark the end of one frame & the beginning of other

Various Framing Approach

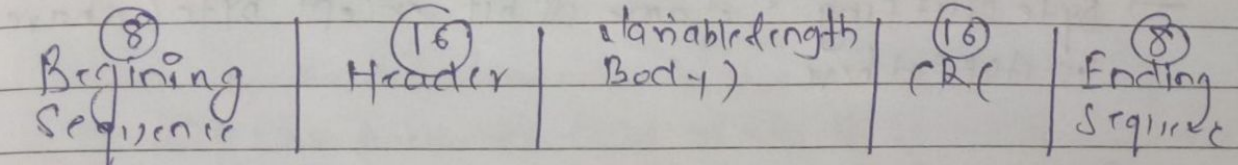
Bit oriented approach
1) It simply views the frame as a collection of bits
2) Data is transmitted as a sequence of bits that can be interpreted in the upper layers. both as text as well as multimedia data
3) Bit oriented protocol - HDLC ↔ High level Data link control

Byte oriented approach
1) Each frame is viewed as a collection of Byte
2) Byte oriented protocol - BISYNC, DDCMP, PPP

Clock Based framing
Ex. SONET (Synchronous Optical Network)

High level Data link Control (HDLC)

→ Developed by IBM
→ SDLC as later standardized by the ISO as the HDLC
→ Bit Oriented Protocol
→ Frame Format



Begining & ending sequence = 01111110
Header - Address & Control field
Body - Payload
CRC - Cyclic Redundancy check - Error Detection

→ types depending on control field.

I Frame	S-frame	U-frame
(Info frame)	Supervisory frame	Unnumbered frame
1st bit in control field is 0	— 11 — 10	— 11 — 11

Bit Stuffing
If the data part is any part of data is same as begining or ending sequence in HDLC i.e. 01111110 error is caused. So in data part 0 is stuffed after 5 consecutive ones.

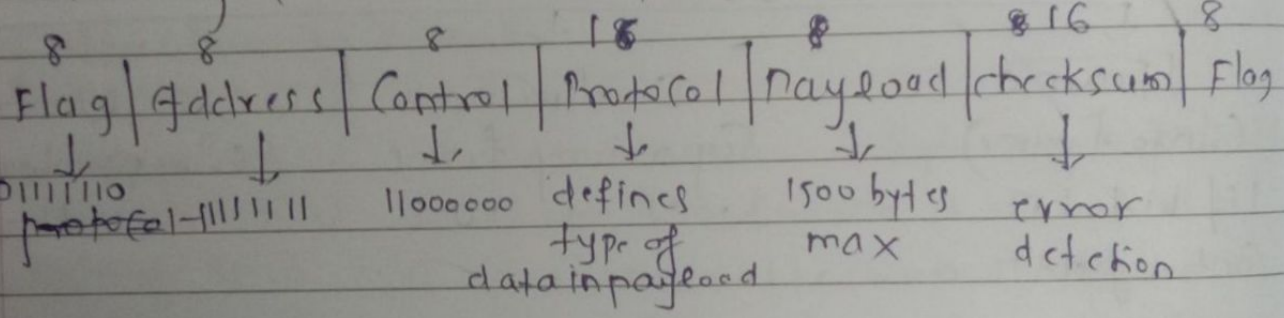
BISYNC Protocol
→ Sentinel approach
→ Developed by IBM
→ Also preferred as BSC

SYN	SYN	SOH	Header	STX	Body	ETX	CRC
8	8	8		8		8	16

→ Byte stuffing : Same as bit except byte (character) is stuffed here

Point to Point Protocol

1) WAN and data link layer protocol
2) Used in broadband communications having heavy loads and high speed
3) Used to transmit multiprotocol data bet^n two directly connected computers



4) Byte stuffing

DDCMP

1) Byte oriented communication protocol
2) Devised by digital Equipment Corporation
3) It is a byte counting approach.
4) Count field in the frame format.

SYN	SYN	Class (protocol like)	Count	Header	Body	CRC
8	8	8	14	42		16

* If the count field gets corrupted then the end of the frame would not be correctly detected by the receiver

Page No.
Date : / /

Error Detection.

Error - 1) Error caused during transmission is transmission error
2) Error detection & correction are implemented at data link or transport layer of the OSI model

Types of Error

(1) Bit error - Single bit ~~error~~ in data is changed
(2) Burst error - More than 1 bit in data is been corrupted.

How to detect the errors?

→ ~~Error detection~~ or Correct errors, need to send some extra bits with the data
→ the extra bits are called as redundant bits
→ Error detection means to decide whether the receiver data is correct or not without having a copy of the original msg
→ If the redundant bits are same in Sender & receiver side there is no error

Error Correction

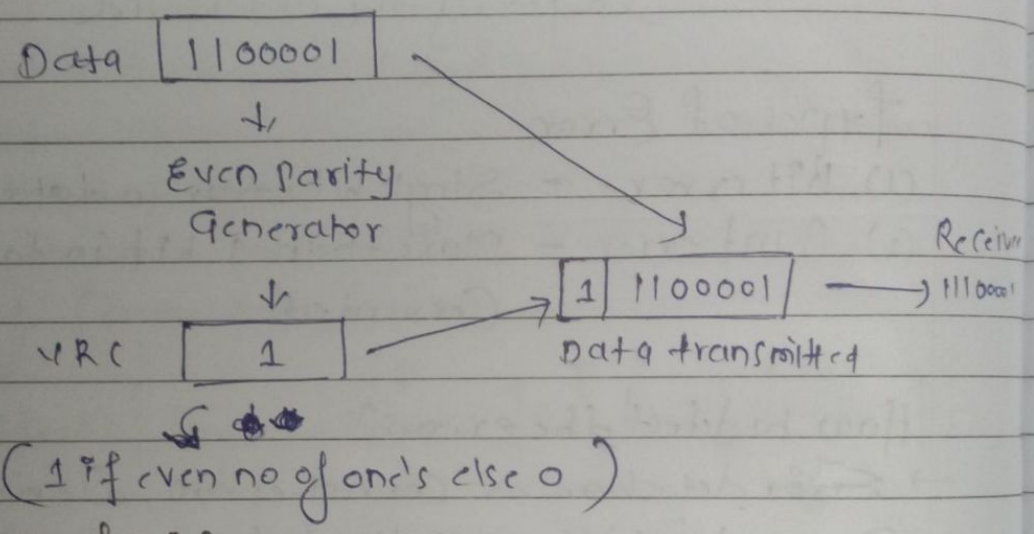
(1) Retransmission of the entire data unit
(2) Receiver can use an error-correcting code, which automatically corrects certain errors

Page No.
Date : / /

Error Detection Techniques

(1) Vertical Redundancy check (VRC)
(2) Longitudinal Redundancy check (LRC)
(3) Checksum
(4) Cyclic Redundancy check (CRC)

(VRC) Vertical Redundancy check (Parity check)



Performance of VRC

(1) It can detect single bit error
(2) It can detect burst error only if the numbers of errors is odd

Longitudinal Redundancy check (2d parity)

(1) Here, a block of bits is organized in row & column
(2) the parity bit is calculated for each column & sent along with the data
(3) The block of parity acts as the redundant bits

Page No.
Date : / /

Ex. Find LRC & data that should be transmitted for the data blocks 11100111 11011101 00111001 10101001

→ for each column even 1's — 0
odd 1's — 1

(1) Arrange data in Column

	1	1	1	0	0	1	1	1
	1	1	0	1	1	1	0	1
	0	0	1	1	1	0	0	1
	1	0	1	0	1	0	0	1
LRC →	1	0	1	0	1	0	1	0

Data transmitted =

10101010	10101001 ...
LRC	Data

Performance of LRC

→ LRC is the likelihood of detecting burst errors

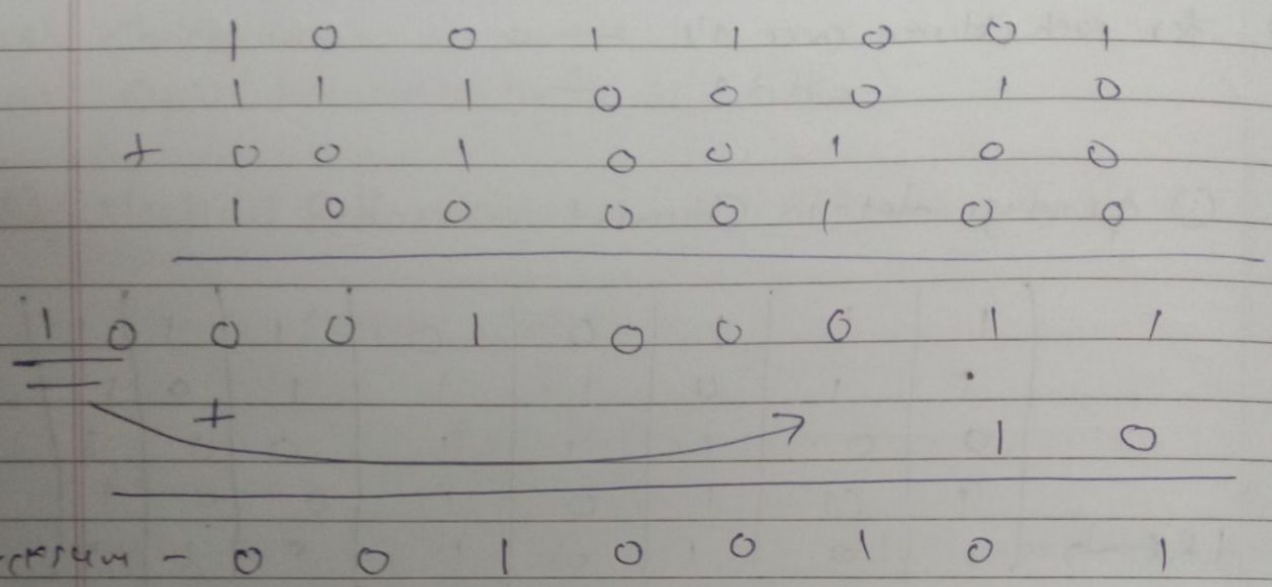
→ If two bits in one data unit are damaged & two bits in exactly the same position in another data unit are also damaged, the LRC checker will not detect an error

CheckSum

(1) Break the original message in to k number of blocks with n bits in each block
(2) Sum all the k datablocks
(3) Add the carry to the sum if any
(4) Do 1's Complement to the sum = checksum

Page No.
Date : / /

Ex. Data = 10011001 11100010 00100100 10000100



Checksum operation at receiver side,

- Sum all data blocks & checksum if the result is all 1's accept else reject

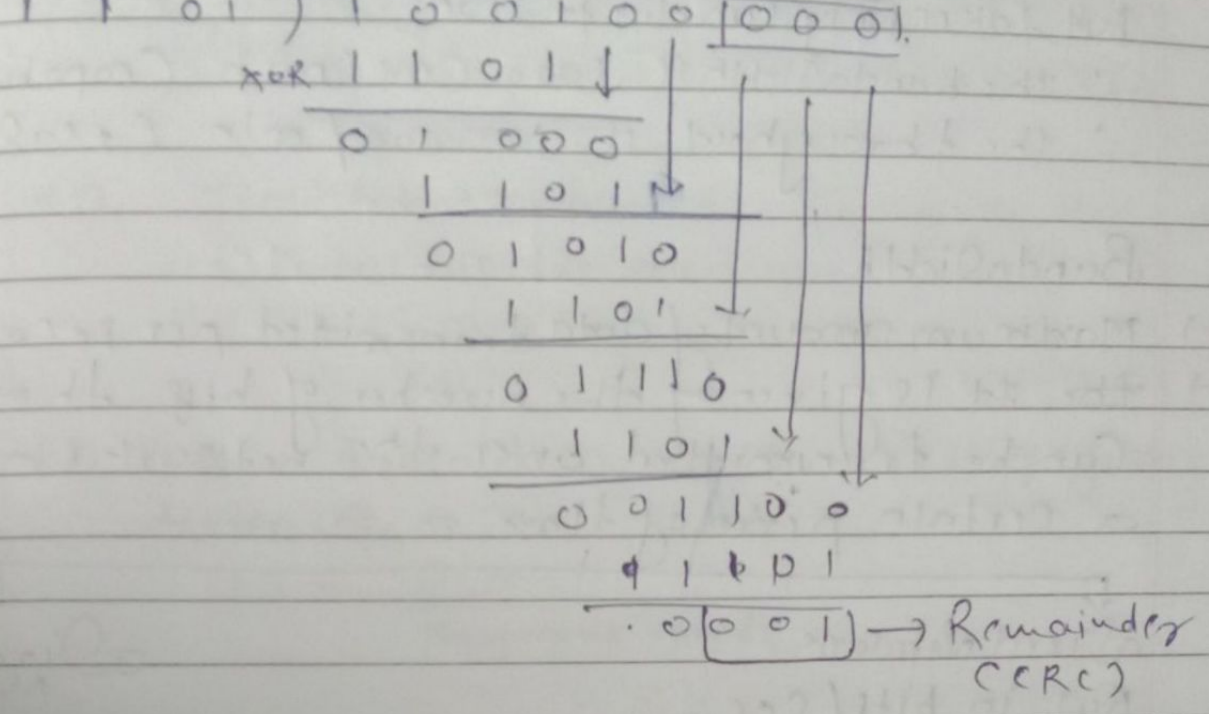
CRC (Cyclic Redundancy check)

Ex. Find the CRC for the data blocks 100100 with the divisor 1101. (Divisor will be known to both sender & receiver)

→ Steps.

(1) Find the length of the divisor L
(2) Append L-1 bits to the original message
(3) Perform binary division operation
(4) Remainder of the division = CRC.

Note - The CRC must of L-1 bits

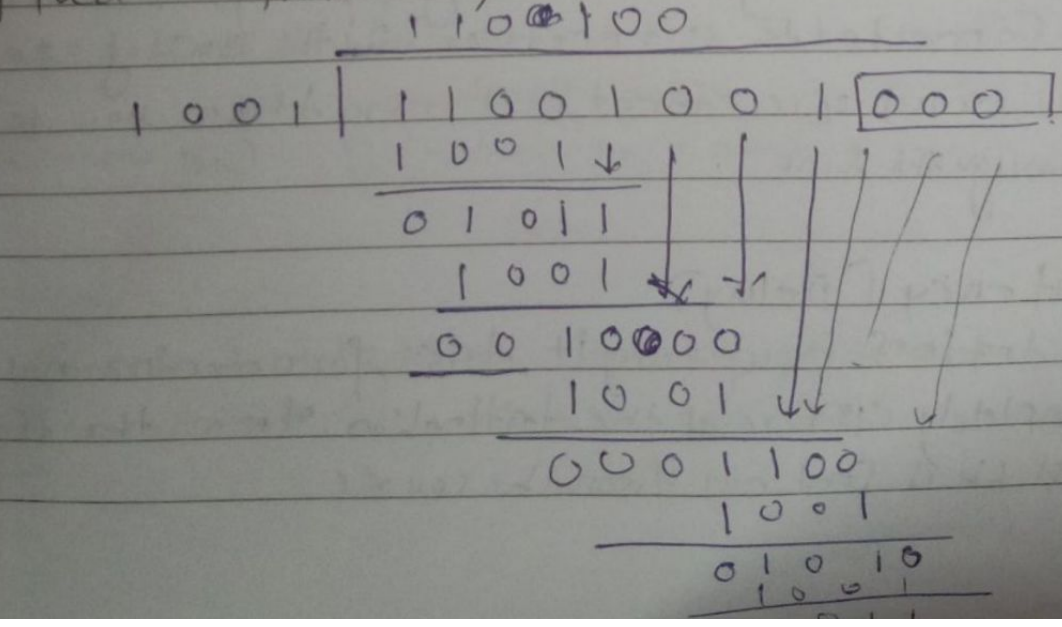


∴ Data transmitted = 1 0 0 1 0 0 0 0 1

Error detection in CRC

Divide divisor with data transmitted if the remainder is all zero receiver detects there are no errors

Q) the msg 1 1 0 0 1 0 0 1 is to be transmitted using CRC polynomial x^3+1 to protect it from errors. Find transmitted msg



Network Performance

It is measure by Bandwidth, Throughput, Latency (delay)

★ ~~that~~ of highway is designed to take load of 1000 cars but takes only 100 due to M2C.

∴ the bandwidth is 1000 cars/min (capability)

∴ the throughput is 100 cars/min (reality)

Bandwidth

→ Maximum amount of data transmitted per second

→ ~~the~~ It is given by the number of bits that can be transmitted over the network in a certain period of time.

Wired Networks
BW in bits/sec
Ex Gigabit Ethernet has bw of 1 Gbps

Wireless Network
BW in Hertz
Ex. Range of frequencies used to transmit signals which is measured in Hertz

Throughput

→ Actual amount of data that passes through the medium

→ It is a measure of how fast we can actually send the data through a network

→ In a link $T < B$ (T = throughput, B = Bandwidth)

→ The sender may have BW of 1 Mbps but may be connected to a receiver with BW of 200 kbps. This means we cannot send more than 200 kbps through this link.

Latency (Delay)

It defines how long it takes for an entire msg to completely arrive at the destination from the time the first bit is sent out from the source

Page No.
Date : / /

Latency = Transmission delay + propagation delay + Queuing delay + Processing delay

TD = Time taken to place the complete data packet on transmission medium

$TT = \frac{\text{Message size}}{\text{BW}}$

PD = time taken by ~~msg~~ a bit to go from device A to B

$PT = \frac{\text{Distance}}{\text{Propagation speed}}$.

QD = The time needed for each intermediate or end device to hold the msg before it can be processed

It is not a fixed factor, it changes with load imposed on network

It increase with heavy traffic in network

PD = time taken by node to process the msg

Bandwidth-Delay Product

It defines the number of bits that can fill the link

$\text{Length} = \text{delay}$

Cross section = BW $\left(\frac{\text{Volume} = \text{BW} \times \text{Delay}}{\text{link}}\right)$

Q. Consider that the link capacity of a channel is 512 kbps & round trip delay time is 1000 ms

→

Page No.
Date : / /

The bandwidth delay product = 512 kbps × 1000 ms
= 512 × 1000 bits/sec × 1000 × 10^{-3} sec
= 512000 bits
= 64000 bytes
= 62.5 Kilobytes (1024)

Q what is PT if distance btn two points is 12000 km
Assume propagation speed to be 2.4×10^8 m/s

→ PT = distance / PS

= $\frac{12000 \times 1000 \text{ m}}{2.4 \times 10^8 \text{ m/s}}$

= $\frac{121}{12500}$

PT = 0.005 sec

Round trip time

(1) It is the length of time it takes for a signal to be sent plus the length of time it takes to receive that signals acknowledgment.

RTT = 2 × PT

Flow Control

→ Speed matching mechanism
→ It is a set of procedures that tells the sender how much data it can transmit before it must wait for an acknowledgment from the receiver
→ Receiver has limited incoming speed & memory. It must inform the sender befor the limits are reached

Flow Control Protocols

Page No.
Date :

Noiseless channels
- Simplest
- stop & wait

Noisy channels
- stop & wait ARQ
- Sliding window protocols
  - Go-Back-N ARQ
  - Selective repeat ARQ

Stop & wait protocol

(1) It provides unidirectional data transmission with flow control facilities but without error control facilities

(2) Idea - after transmitting one frame, the sender waits for an acknowledgment before transmitting the next frame

Primitives of stop & wait protocol

Sender side - Rule (1) Send one data packet at a time
Rule (2) Send the next packet only after receiving ack for the previous

Receiver side - Rule (1) Receive & consume data packet
Rule (2) After that ack need to be sent

Problems

(1) Problems due to lost data (sender & receiver wait for ack for infinite number of time if any data packet is lost)

(2) Same to lost ack (-11-)

(3) Problems due to delayed ack / data
After timeout on sender side, a delayed ack might be wrongly considered as ack of some other data packet

Stop and Wait ARQ (Automatic Repeat Request)

→ Same as stop & wait but if the acknowledgement does not arrive after a certain period of time, the sender times out & retransmits the original frame

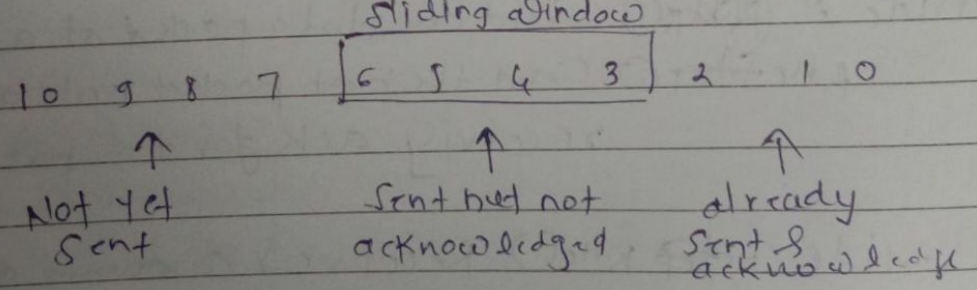
→ stop & wait ARQ = stop & wait + timeout timer + sequence number

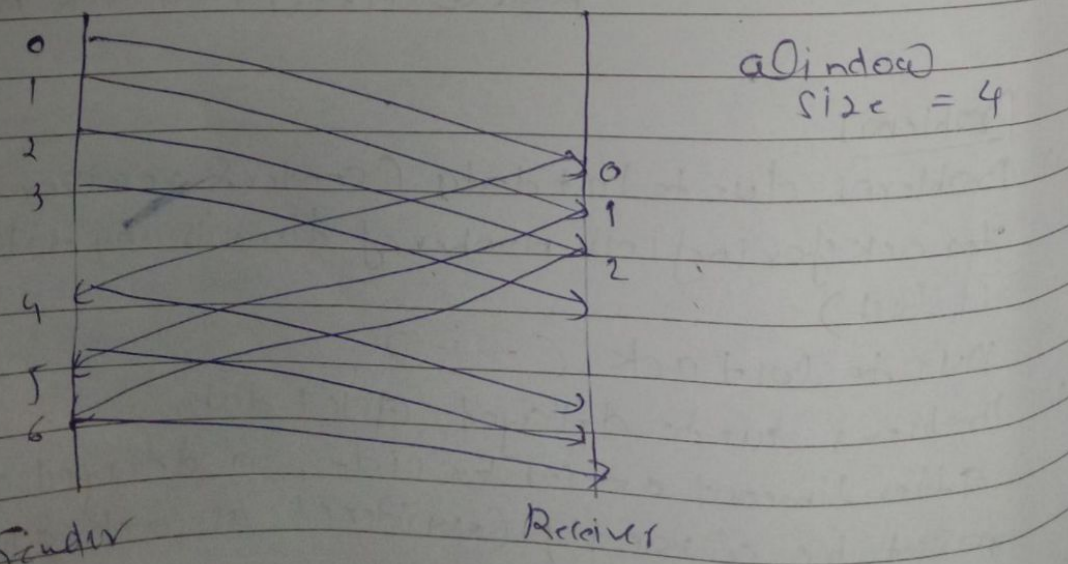
Sliding window Protocol

Drawbacks of ARQ (stop & wait) =>
1. One frame at a time
2. poor utilization of bandwidth
3. poor performance

Sliding window protocol

1. Can send multiple frames at a time
2. No. of frames to be sent is based on window size
3. Each frame is numbered → sequence number



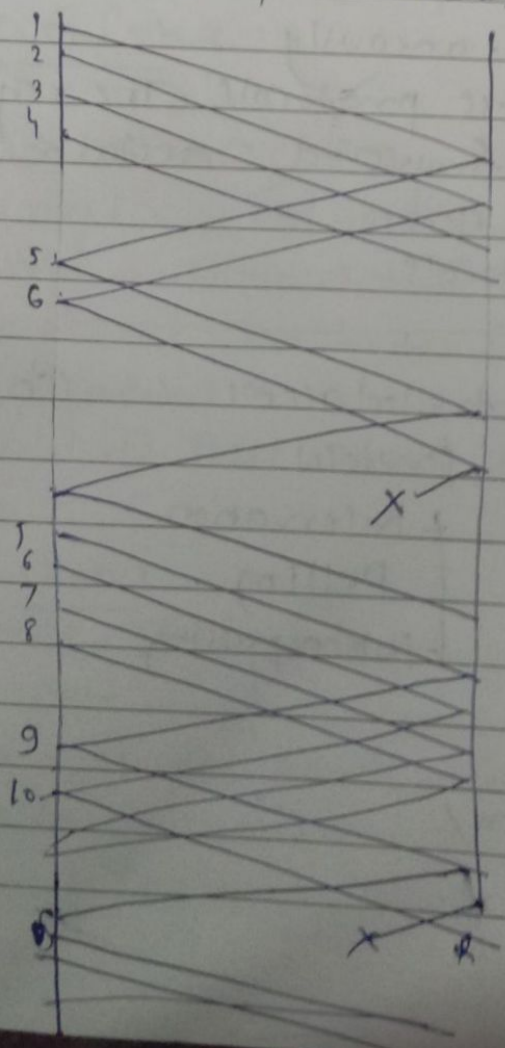


Go Back-N ARQ

1) N is sender window size.
2) If the acknowledgements of a frame is not received within an agreed upon time period, all frames in the current window are transmitted.
3) For Ex. if the sending window size is 4 (2^2) then the sequence numbers will be 0, 1, 2, 3, 0, 1, 2, 3, 0, 1, ...
4) The number of bits in the sequence number is 2. to generate the binary sequence 00, 01, 10, 11

Q. Host A want to send 10 frames to Host B. The both agreed to go with Go Back-4. How many number of frames are transmitted by Host A. If every 6th frame that is transmitted by Host A is either corrupted or lost

A)



17

Selective Repeat ARQ

(1) In selective Repeat ARQ, only the erroneous or lost frames are retransmitted, while correct frames are received & buffered

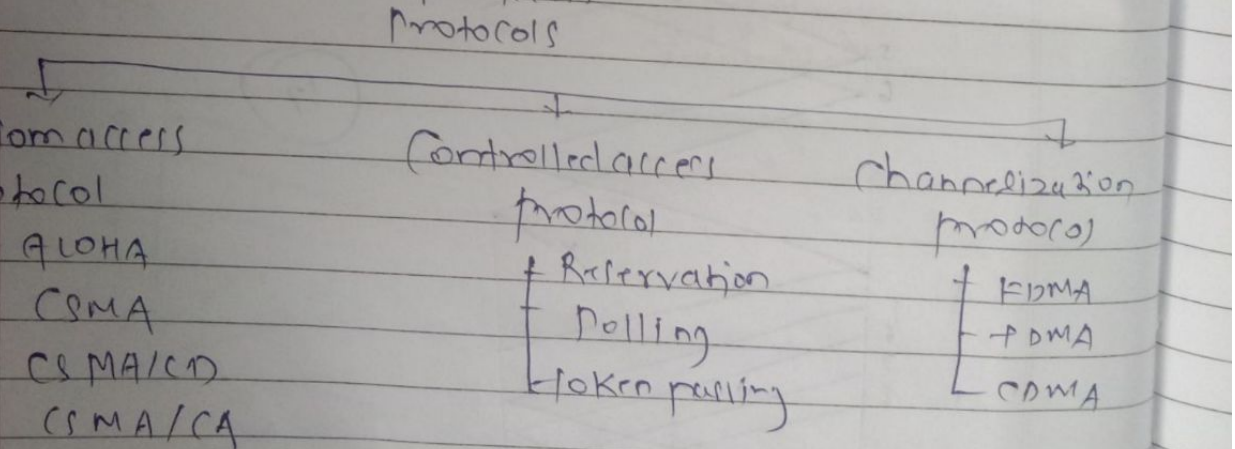
(2) The receiver while keeping track of sequence numbers buffers the frames in memory & sends NACK for only frame which is missing or damaged

Optimal Window Size = $\frac{\text{Bandwidth} \times \text{Delay}}{\text{Packet Size}}$

Multiple Access Protocol

(1) If there is a dedicated link bet^n the sender & the receiver then data link control layer is sufficient, However if there is no dedicated link present then multiple stations can access the channel simultaneously

(2) Hence multiple access protocol are required to decrease collision & avoid crosstalk



Random Access Protocol

(3) Every station is same
(4) If more than one station tries to send, there is an access conflict (collision) & the frames will be either destroyed or modified

Page no.
Date: / /

Controlled Access Protocols

(1) In controlled access, the stations consult one another to find which station has the right to send
(2) A station cannot send unless it has been authorized by other stations

Channelization

It is a multiple-access method in which the available bandwidth of a link is shared in time, frequency, or through code, between diff stations

Pure Aloha

(1) It was actually designed for WLAN but it is also applicable for shared medium.
(2) In this, multiple stations can transmit data at the same time & can hence lead to collision & data being garbled
Types ① Pure Aloha ② Slotted Aloha

Pure Aloha

(1) It allows stations to transmit whenever they have data to be sent
(2) When a station sends data it waits for an acknowledgment for a random amount of time called back-off time and re-sends the data

(3) Since diff stations wait for diff amount, the probability of further collision decreases

(4) The throughput of pure aloha is max when frames are of uniform length

(5) ~~Whenever two frames try to occupy~~ If the 1st bit of a new frame overlaps with just the last bit of a frame almost finished, both frames will be totally destroyed & both will have to be retransmitted later

Vulnerable time = $2 \times t_{fr}$

Throughput = $G \times e^{-2G}$, where G is the number of stations which transmit in the same time

Max throughput = 0.184 for $G = 0.5 (\frac{1}{2})$

Slotted Aloha

Pure Aloha	Slotted Aloha
(1) Any station can transmit the data at any time	Any station can transmit the data at the begining of any slot
(2) The time is continuous & not globally synchronized	The time is discrete & globally synchronized
(3) Vulnerable time in which collision may occur = $2 \times t_{fr}$	$= t_{fr}$
(4) Probability of successful transmission of data packet = $G \times e^{-2G}$	$= G \times e^{-G}$
(5) Max efficiency = 18.4% ($G = 1/2$)	= 36.8% ($G = 1$)
(6) Simplicity in Implementation	Reduces the no. of collisions to half & doubles the efficiency of pure aloha

CSMA Protocol

→ Carrier Sense Protocol

→ To minimize the chance of collision & therefore, the performance, the CSMA method was developed

→ Principle - Sense before transmit or listen before talk

→ Carrier can be busy or idle.

→ The possibility of collision still exists because of propagation delay; a station may sense the medium & find it idle, only because the first bit sent by another station has not yet been received.

Types

1 persistent
Sense continuously

Non persistent
Sense after every random slot of time

p persistent
when channel is idle it transmits with a probability p

CSMA/CD ⊕ Collisions can be detected by looking at the power or pulse width of the received signal & comparing it to the transmitted signal

① After a station detects a collision, it aborts its transmission, waits a random period of time & then tries again

② efficiency $= \frac{1}{1 + 6.44a}$ $\quad a = \frac{T_p}{T_t}$

③ distance ↑ ⇒ efficiency ↓

④ T_t) = RTT of 1 bit

T_t) $= 2 \times T_p$

CSMA/CA

→ Nodes attempt to avoid collisions by beginning transmission only after the channel is sensed to be idle

Reservation

→ Station needs to make reservation before sending data

Polling

→ One master node gives chance to every other node in round robin fashion to transmit the data they can

Token passing

When node receives a token, it holds onto the token only if it has some frames to transmit

Channelization

Available bandwidth of a link is shared in time, frequency or through code between diff stations

- Frequency Division MA (BW is divided into bands that are seperated by guard bands)
- Time Division MA The BW is just one channel that is time shared bet^n diff stations
- Code Division MA One channel carries all transmissions simultaneously (Multiplexing)

Ethernet

→ Most widely used wired LAN technologies

→ Operates in data link & physical layers

Ethernet frame format

Preamble : 56 bits of alternating 1s & 0s
SFD : Start frame delimiter, flag (10101011)

Preamble	SFD	Destination address	Source address	Length or type	Data & padding	CRC
7 bytes	1 byte	6 bytes	6 bytes	2 byte		4 byte

← physical layer header →

Data/padding - Min len = 46 bytes
Max len = 1500 bytes

Frame length - min = 64 bytes
Max = 1518 bytes

Ethernet Address Ex - 06:01:02:01:2C:2B - 6 bytes.

→ The least significant bit of the first byte defines the type of address
→ If the bit is 0, the address is unicast else multicast
→ If all bits are 1 then it is broadcast address

Hexadecimal to Binary

Hexadecimal	0	1	2	3	....	9	A	B	C	D	E	F
Decimal	0	1	2	3	....	9	10	11	12	13	14	15

Ex. 5BIC

5 → 0101
B → 11 → 1011

= 0101 1011

→ In an binary Ethernet address in each byte 1st 4 digits represents be a hexadecimal digit & the next four the other digit

Ethernet transmitter Algo

access protocol for Ethernet

→ the algo is commonly called Ethernet's Media Access Control (MAC) which is implemented in Hardware on the network adaptor

→ Access Method of ethernet : CSMA/CD

→ Encoding method : Manchester Encoding technique for converting data bits into signals

→ Ethernet transmitter algo - CSMA 1-persistent protocol

Runt frames - A frame with less than min length of 64 bytes

- Caused by collisions, malfunctioning network card, buffer underruns, duplex mismatch or software issues

Exponential backoff - Every time the adaptor detects collision it doubles the waiting time

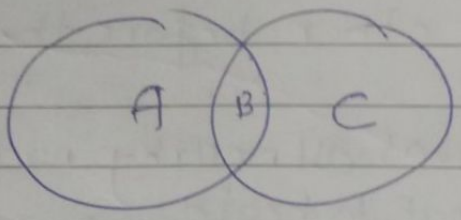
Ethernet Pros	Ethernet Cons
- Most widely used	- Under heavy loads too much of the Network's Capacity is wasted by collisions
- Inexpensive	- It does not hold good for real time & interactive applications
- All nodes are equal	- As network cannot set priority, it is not suitable for client-server architecture
- Simple maintenance & administration	- No ack
- Cable here is robust to noise	
- ∴ quality of data does not degrade	

Wireless Fidelity (Wi-Fi)
- CSMA/CA
- Modes → Infrastructure mode
  → Ad hoc & WiFi Direct
- Instead of all nodes being created equal some nodes are allowed to roam & some are connected to a wired network infrastructure, they are called access points (AP) & they are connected to each other by a so called distribution system
  Access points - towers etc
  Nodes - Devices

Active scanning - when node searches for access point
Passive scanning - when access points advertise themselves

WiFi frame format
See in video

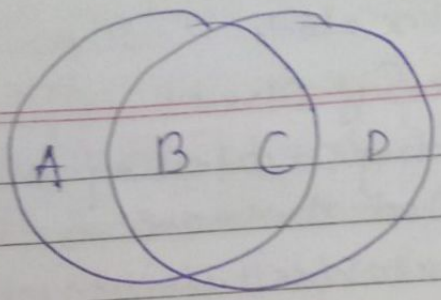
Hidden terminal Problem



- A & C both want to communicate to B & both are unaware of each other as they are out of each other's range
- Collision will happen at B (But unlike Ethernet, neither A nor C will be aware of this collision)
- A & C are said to be hidden nodes wrt each other

Solution - Multiple Access Collision Avoidance (MACA)
- RTS & CTS

Exposed terminal Problem



- Suppose B is sending to A. Node C is aware of this communication because it hear B's transmission
- It would be a mistake for C to conclude that it cannot transmit to anyone just because it can hear B's transmission
- Suppose C wants to transmit to node D
- This is not a problem since C's transmission to D will not interfere with A's ability to receive from B

Solution - MACA

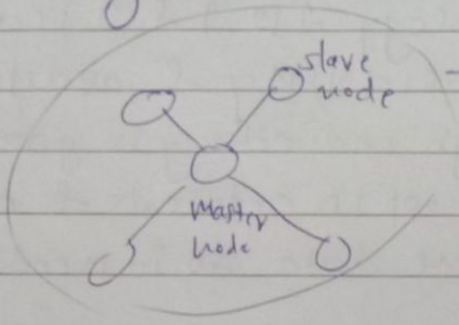
MACA
- Key idea - Sender & Receiver exchange control (RTS & CTS frame) frames with each other before the sender actually transmits any data
- this exchange informs all nearby nodes that a transmission is about to begin
- Sender transmits a Request to Send (RTS) which includes how long the sender wants to hold the medium, length of the data etc
- Receiver replies with a clear to send (CTS) this frame echoes this length field back to the Sender

☆ - The idea of using ack in MACA is proposed - MACAA
- receiver sends an ack to sender after receiving a frame
- All nodes must wait for ack before trying to transmit

— If RTS collision happens it will not be detected & exponential backoff algo will be used

IEEE 802.15 Bluetooth

— wireless technology for exchanging data for building Personal area Network (PANs)



→ Piconet

Collection of Piconet = Scatternet

Pros - Low cost, Easy to use, penetrate through walls, Locals can ad-hoc connection immediately without any cables, It is used for voice & data transfer

Cons - Low security, slow transfer, small range

Bluejacking - Unauthorized access of info from a wireless device through a bluetooth connection

VLAN

→ It is a logical partition of a layer 2 network

→ Multiple partitions can be created, allowing for multiple VLANs to co-exist

→ Each VLAN is a broadcast domain, usually with its own IP network

→ VLANs are mutually isolated & packets can only pass between them via a router

→ The partitioning of the layer 2 network takes place inside a layer 2 device, usually via a switch

→ The hosts grouped within a VLAN are unaware of the VLAN's existence

Benefits - Security, cost reduction, Better performance, shrink broadcast domains, improved IT efficiency, Simpler project & application management

~~Types of VLAN~~ - Data VLAN, default VLAN, Native VLAN etc

Spanning Tree Protocol

Redundancy - In technology 2 is 1 & 1 is none
↳ improves reliability & availability

Broadcast storm - Though redundancy is good it may form a loop in network & network may get flooded with the same data so it needs to be controlled

STP - was created to prevent loops
- Switches send probes into the network called (BPDU) Bridge protocol data unit to discover loops. If they receive these back, loop is present
- BPDU probes helps to elect the root bridge
- All switches will find the best way to reach the root bridge and the redundant links will be blocked
- This redundant links will only be active if the existing links or ports go down

Socket programming

(1) Socket function - Socket (address family of socket to be created, type of socket, protocol to be used)

(2) Connect function - Connect (Socket name, socket address, socket size)

(3) receive function - recv (socket name, address of data structure where info should be saved, size of ~~data~~ DS)

(4) close (sock name) - to close the socket