OSI MODEL

OSI-1

Easy Engineering Classes – Free YouTube Lectures

EEC Classes GGSIPU, UPTU, Mumbai Univ., Pune Univ., GTU, Anna Univ., PTU and Others EEC Classes

Data Communication and Networking

Open System Interconnection (OSI) Model

It is a layered framework for the design of NIw systems that allows Comm^n between all types of Computer Systems.

↳ '7' Seven Separate Layers.

IMP.. → Each Layer calls upon the services of the Layer just below it. (All people Seems to Near Dominos Pizza)

Layers in OSI Model

Layer 7 - Application Layer

Layer 6 - Presentation Layer

Layer 5 - Session Layer

Layer 4 - Transport Layer

Layer 3 - Network Layer

Layer 2 - Data Link Layer

Layer 1 - Physical Layer

(i) Physical Layer:- It is responsible for moving individual bits from one (node) to the next.

Functions:-

(i) Transmission Media

(ii) Types of Encoding

(iii) Data Rate [no. of bits sent each sec.]

(iv) Synchronization of bits

(v) Line Configuration → Point-to-Point, Multipoint

(vi) Topology → Mesh, Star, Bus, Ring

(vii) Transmission Mode → Simplex, Half-duplex, Full-duplex.

OSI-2

Easy Engineering Classes – Free YouTube Lectures

EEC Classes GGSIPU, UPTU, Mumbai Univ., Pune Univ., GTU, Anna Univ., PTU and Others EEC Classes

Data Communication and Networking

OSI MODEL

(ii) Data Link Layer:- It transforms the physical layer into a reliable link.

Functions:- (i) Framing :- Conversion of bits → Frames.

(ii) Physical Addressing → Header is added to frame

IMP.. (iii) Flow Control

(iv) Error Control

(v) Access Control

(iii) Network Layer:- Responsible for Source-to destination delivery of Packet.

Functions:- (i) Logical Addressing → Header to the Packet Coming from Upper.

IMP.. (ii) Routing → Routing algorithms.

(iv) Transport Layer:- Responsible for Process-to-Process delivery.

Functions:-

(i) Service-point Addressing (Port Address)

(ii) Segmentation and Reassembly → Sending → Receiving.

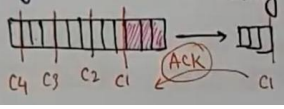
(iii) Connection Control → Connectionless. Connection Oriented.

(iv) Flow and Error Control

(v) Session Layer:- Functions:-

(i) Dialog Control → Half Duplex (One Way at a time) Full Duplex (two ways at a time)

(ii) Synchronization :- Adding checkpoints



OSI-3

Easy Engineering Classes – Free YouTube Lectures

EEC Classes GGSIPU, UPTU, Mumbai Univ., Pune Univ., GTU, Anna Univ., PTU and Others EEC Classes

Data Communication and Networking

OSI MODEL

(vi) Presentation Layer:- It deals with the Syntax and Semantics of the Info" exchanged b/w two Systems.

Functions:- (i) Translation :- Converting a message to Compatible bit stream.

(ii) Encryption :- Converting Plaintext to Ciphertext. → Decryption (receiving side).

(iii) Compression :- Reducing no. of bits contained in the info".

(vii) Application Layer:- It enables the users (Human/SW) to access the N/w.

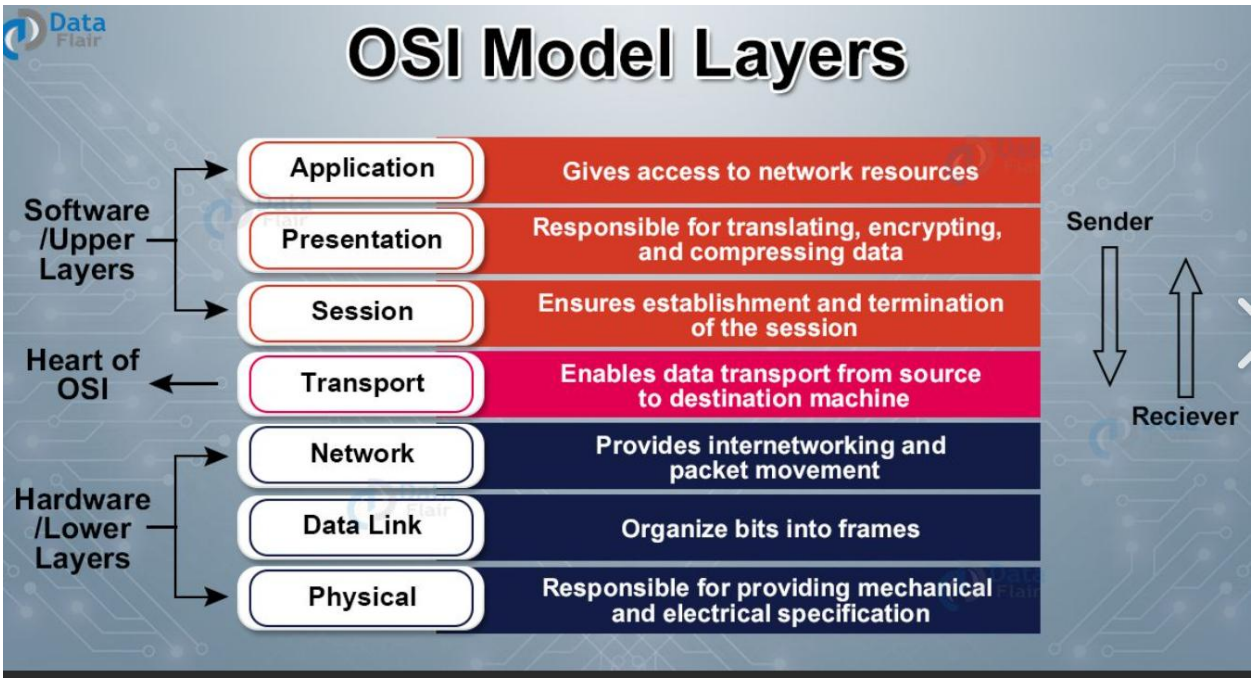
Functions:-

(i) N/w Virtual Terminal :- S/w version of Physical terminal. (Remote Host Login is facilitated)

(ii) File Transfer, access and Management

(iii) E-mail Services

(iv) Directory Services



Data Communication and Networking

TCP/IP Reference Model:-

It is developed before OSI model.

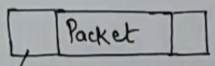
→ Contains Four Layers but now it Contain 5 Layers.

Layer 1 →	Application	Application
Layer 2 →	Transport	Transport
Layer 3 →	Internet	Network
Layer 4 →	Network Interface	Data Link
Layer 5 →		Physical

Application
Presentation
Session
} OSI

(i) Physical Layer:- Unit of Comm^n is Single bit.
→ No specific Protocol
→ Comm^n b/w two hops, nodes, Computer.

(ii) Data Link Layer:-
↳ No specific Protocol.
→ Comm^n b/w two hops/nodes
→ Unit of Comm^n is Frame.



Source and destination address of fr

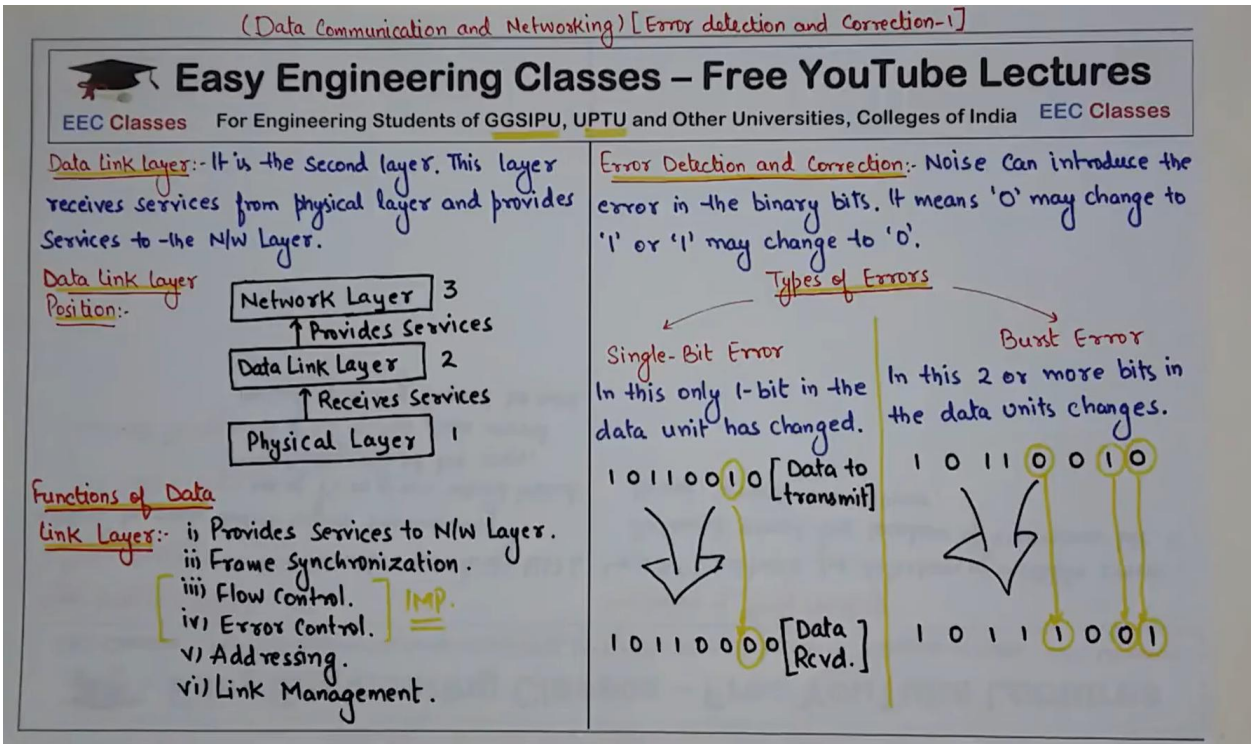
(iii) Network Layer:- Internet Protocol (IP) is used for transmission mechanism.
↳ Unit of Comm^n is called datagram.
→ Comm^n is end to end.

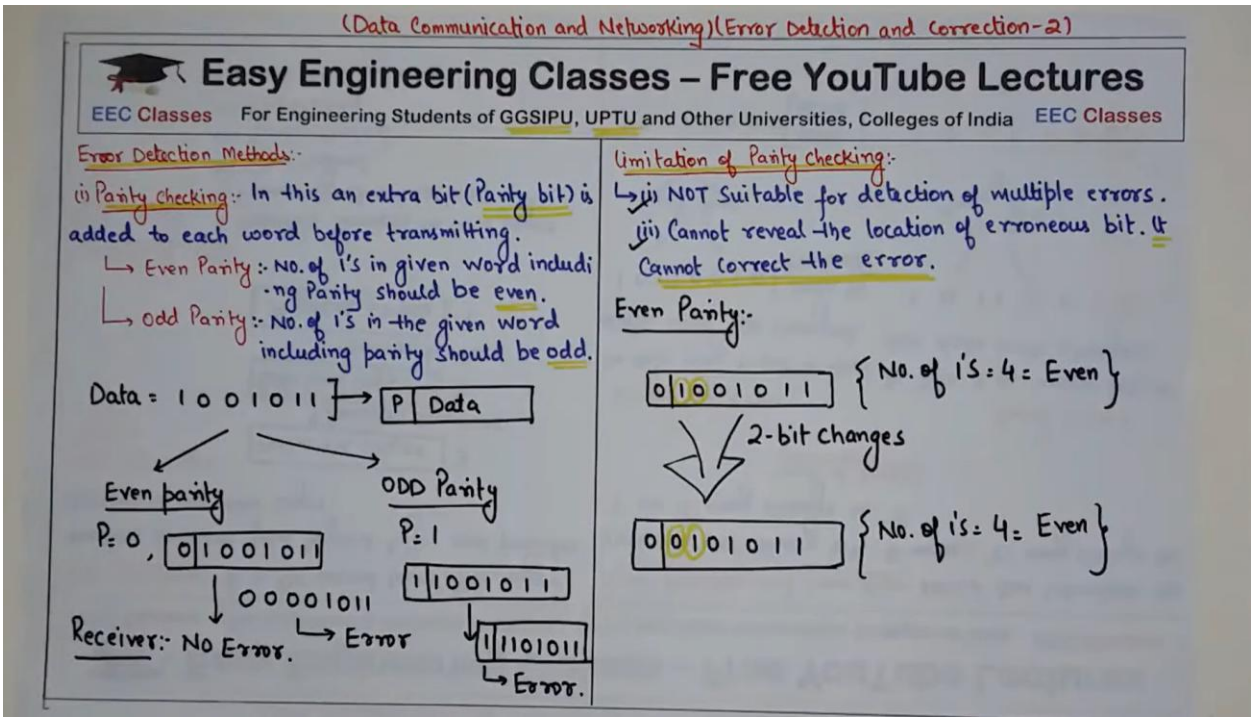
(iv) Transport Layer:-
→ Responsible for delivering whole message.
↳ Unit of Comm^n is called Segment.
→ Two Protocols

TCP	UDP
Transmission Control Protocol.	User datagram Protocol
(Connection Oriented)	(Connection Less)

(v) Application Layer:- It is Comb^n of Session, Presentation and Application Layers in OSI model.
Unit of Comm^n is Message.

ERROR DETECTION





(Data Communication and Networking) [Checksum-1]

Easy Engineering Classes – Free YouTube Lectures

EEC Classes For Engineering Students of GGSIPU, UPTU and Other Universities, Colleges of India EEC Classes

Checksum for Error Detection:- In this each word is added to the previous word and total sum [Checksum] is calculated. Then the checksum is transmitted along with the data.

Idea of checksum:- (7, 11, 12, 0, 6) to send.

W1 ..... W5

W1 + W2 + ... + W5 → Checksum

7 + 11 + 12 + 0 + 6 = 36

(Transmitter) Data | C.S → (Receiver) Data | C.S

Calculate Checksum (Compare) → C.S1

if C.S = C.S1 → No Error

7, 11, 12, 0, 6 | -36 (TR) → 7, 11, 12, 0, 6 | -36 (RE)

Calculate checksum (7 + 11 + 12 + 0 + 6) = 36

-36 + 36 = 0 ✓ No = Error.

Checksum using one's complement:-

Checksum = 36

10 0 1 0 0] 36

10

0 1 1 0 (6)

Inverse 1 0 0 1 (9)

7, 11, 12, 0, 6 | 9

7 + 11 + 12 + 0 + 6 + (9) = 45

10 1 1 0 1] 45

10

1 1 1 1

Inverse 0 0 0 0 } No = Error

(Data Communication and Networking) (Error-detection and Correction) (CRC-1)

Easy Engineering Classes – Free YouTube Lectures

EEC Classes For Engineering Students of GGSIPU, UPTU and Other Universities, Colleges of India EEC Classes

Cyclic Redundancy Check (CRC):- It is based on the concept of Binary Division.

CRC Generator:- (Data)

i) Append string of n 0s to the data unit.

ii) Divide newly generated data unit in (i) by the divisor.

iii) Remainder after (ii) is n bit CRC.

iv) The CRC will replace n 0s to get codeword to be transmitted.

'n' bits

Data | 00..... 0

Divisor (n+1)

CRC 'n bits'

Data | CRC (Codeword)

Transmitted

Same divisor to be used

CRC Checker:- Here the receiver divides the data unit by the same divisor which was used by the transmitter. The remainder of the divison is then checked → Remainder is '0' [Accepted]; → Remainder is not '0' [Rejected]

Data | CRC } Data Unit

Divisor

Remainder → 0 [No Error]; → Not '0' [Error]

CRC Example:- Dataset = 1001, Divisor = 1011.

Data = 1001

Divisor = 1011 [n+1 bits]

XOR

0 ⊕ 0	0
0 ⊕ 1	1
1 ⊕ 0	1
1 ⊕ 1	0

```
        1010
1011 ) 1001000
       1011
       -----
        0100
        0000
        ----
        1000
        1011
        ----
        0110
        0000
        ----
         110   <- Remainder
```

CRC

Receiver Side:- 1001110

```
        1010
1011 ) 1001110
       1011
       -----
        0101
        0000
        ----
        1011
        1011
        ----
        0000
        0000
        ----
         000   <- Remainder
```

No Error

Hamming Codes:- They are Linear Block Codes. (n, K) Hamming codes for $m \geq 3$ is defined by the following equations:

i) Block Length, $n = 2^m - 1$

ii) No. of message bits : $K = 2^m - m - 1$

iii) No. of Parity bits : $(n-K) = m$

iv) Minimum distance, $d_{min} = 3$

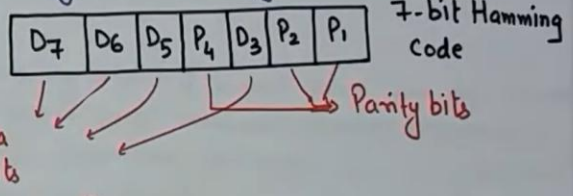
v) Efficiency $= \frac{K}{n} = \frac{2^m - m - 1}{2^m - 1}$

$$= \boxed{1 - \frac{m}{2^m - 1}}$$

Hamming Code Structure:- Error Correcting Code.

→ Parity bits are inserted in b/w data bits.

→ Commonly 7-bits Hamming code is used.



Selection of Parity Bits:-

i) $P_1 \rightarrow 1, 3, 5, 7$

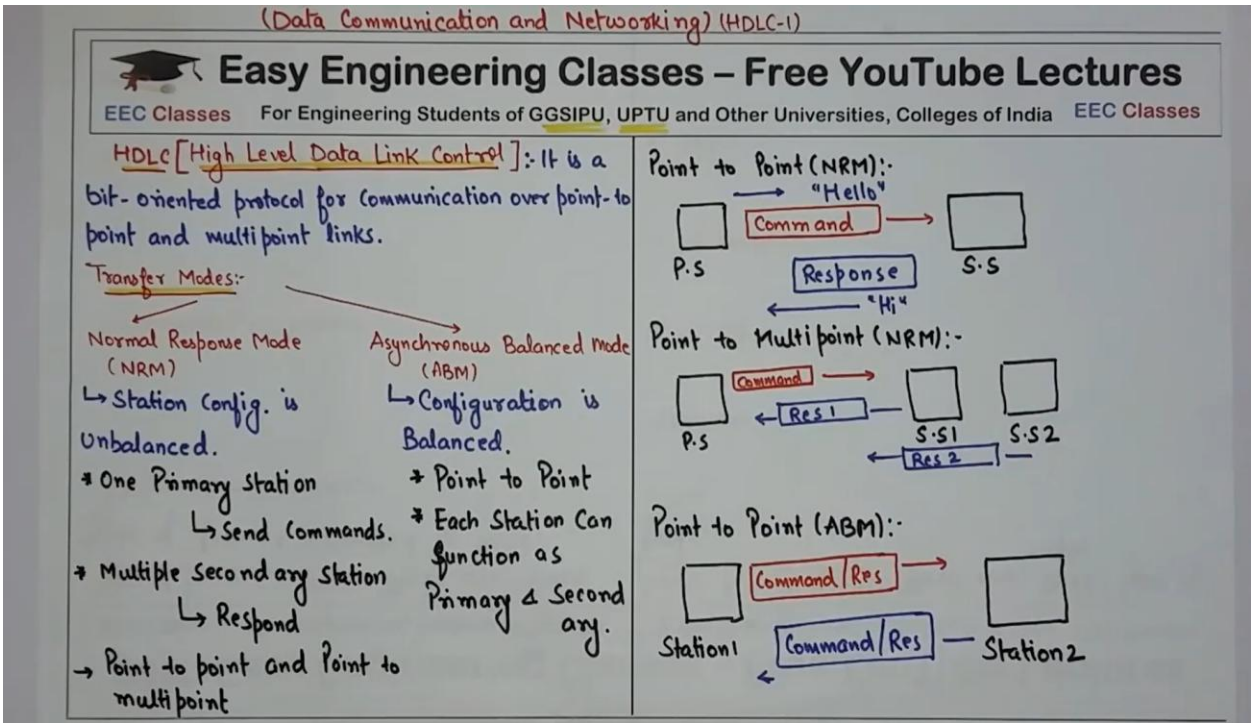
ii) $P_2 \rightarrow 2, 3, 6, 7$

iii) $P_4 \rightarrow 4, 5, 6, 7$

} Adjusted to '0' or '1' depending on the condition.

FLOW CONTROL

HDLC



(Data Communication and Networking) (HDLC-2)

Easy Engineering Classes – Free YouTube Lectures

EEC Classes For Engineering Students of GGSIPU, UPTU and Other Universities, Colleges of India EEC Classes

Types of Frames in HDLC:- There are three types of frames supported by HDLC.

i) Information (I) Frames:- Transport → user data / Control info"

Flag	Add.	Control	User Info"	FCS	Flag

ii) Supervisory (S) Frames:- Transport only Control Inf

Flag	Add.	Control	FCS	Flag

iii) Unnumbered (U) Frames:- Reserved for System Mgmt.

Flag	Addr.	Control	Mgmt Info"	FCS	Flag

Frame Format of HDLC:- There are (upto) Six (6) types of fields.

i) Flag → Beginning / End] of the Frame. | Serves as Synchronization pattern for receiver.

ii) Address → Contains the Address of the Station (Secondary) P.S — 'to' S.S — 'from'

iii) Control → used for Error and Flow Control.

iv) Information → User's data or Management Info".

v) FCS → Frame Check Sequence.
↳ HDLC Error detection field.

PPP

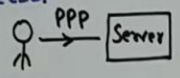
(Data Communication and Networking) (PPP-1)

Easy Engineering Classes – Free YouTube Lectures

EEC Classes For Engineering Students of GGSIPU, UPTU and Other Universities, Colleges of India EEC Classes

Point-to-Point Protocol (PPP):- It is the most common protocol for point-to-point access.

Services provided by PPP:-



i) Defines format of frames.
ii) Defines Link establishment process.
iii) Defines Data exchange process.
iv) Defines How N/w Layer data are encapsulated in data link frame.
v) Defines Authentication process b/w two devices.

Services Not provided by PPP:-

i) Flow Control.
ii) Very Simple mechanism for Error Control.
iii) No addressing mechanism to handle frames in multipoint configuration.

Frame Format of PPP:-

Flag	Address	Control	Protocol	Pay load	FCS	Flag

i) Flag: → Start / end] of the frame] Byte-Oriented Protocol.

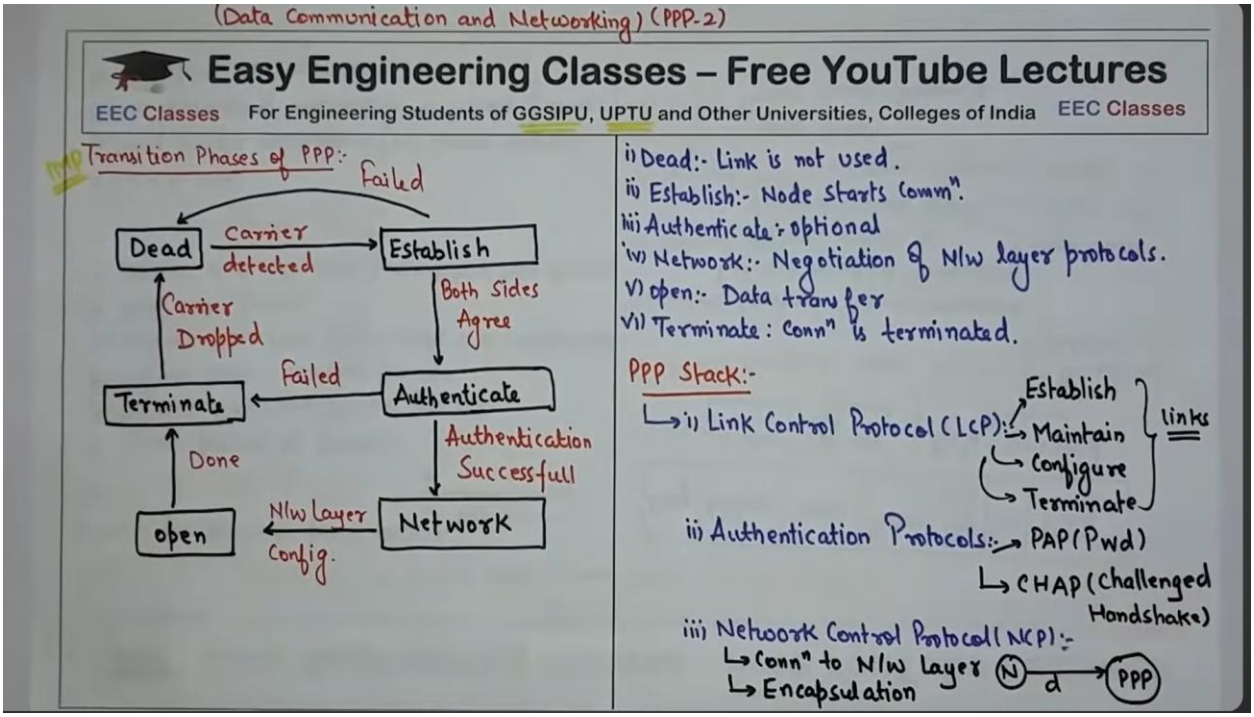
ii) Address: Constant Value 11111111] → Broadcast Address.

iii) Control: Constant Value 11000000
↳ Not needed Generally.

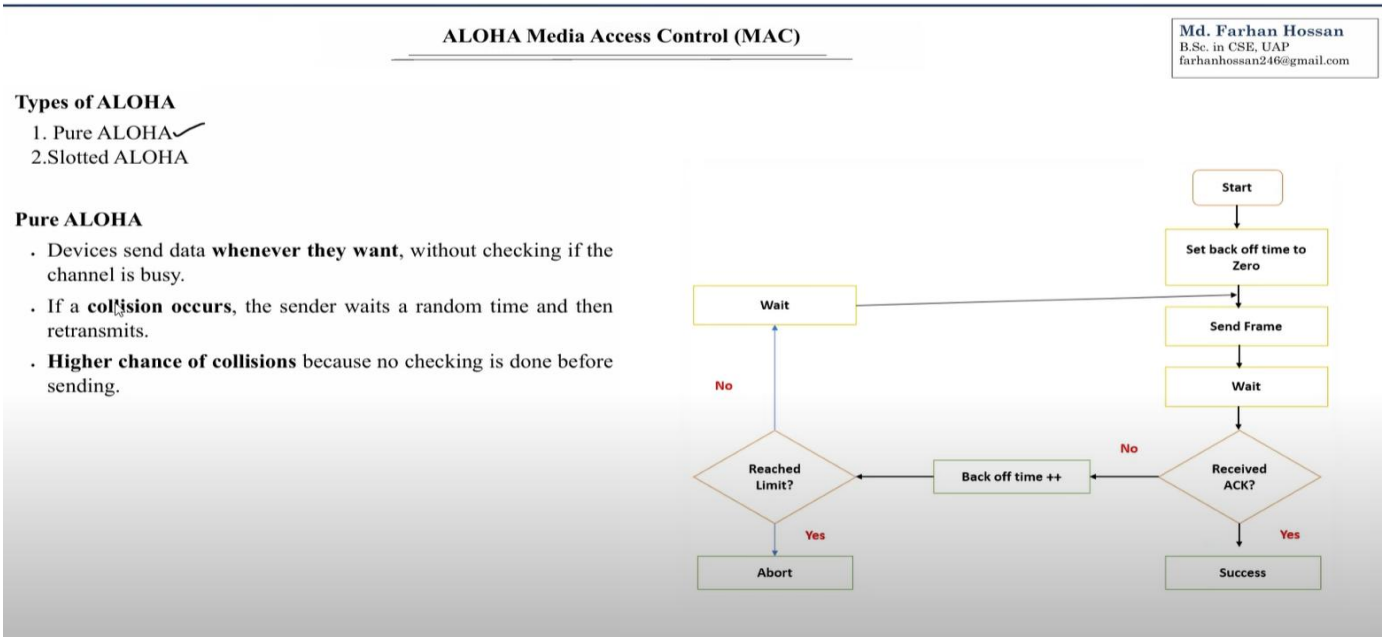
iv) Protocol: defines what is Carried in data field → user data / other Info".

v) Payload Field: → Carry either userdata or other Info".

vi) FCS: Frame check Sequence


(Data Communication and Networking) (PPP-2)
Easy Engineering Classes – Free YouTube Lectures
EEC Classes For Engineering Students of GGSIPU, UPTU and Other Universities, Colleges of India EEC Classes
Transition Phases of PPP:-
Dead
Carrier detected
Establish
Both Sides Agree
Authenticate
Authentication Successfull
Network
N/w Layer Config.
open
Done
Terminate
Carrier Dropped
Failed
Failed
i) Dead:- Link is not used.
ii) Establish:- Node starts Comm".
iii) Authenticate:- optional
iv) Network:- Negotiation of N/w layer protocols.
v) open:- Data transfer
vi) Terminate: Conn" is terminated.
PPP Stack:-
i) Link Control Protocol (LCP):-
Establish
Maintain
Configure
Terminate
links
ii) Authentication Protocols:- PAP (Pwd)
CHAP (Challenged Handshake)
iii) Network Control Protocol (NCP):-
Conn" to N/w Layer
Encapsulation
N
d
PPP

ALOHA


ALOHA Media Access Control (MAC)
Md. Farhan Hossan
B.Sc. in CSE, UAP
farhanhossan246@gmail.com
Types of ALOHA
1. Pure ALOHA
2.Slotted ALOHA
Pure ALOHA
. Devices send data whenever they want, without checking if the channel is busy.
. If a collision occurs, the sender waits a random time and then retransmits.
. Higher chance of collisions because no checking is done before sending.
Start
Set back off time to Zero
Wait
Send Frame
Wait
No
No
Reached Limit?
Back off time ++
Received ACK?
Yes
Yes
Abort
Success

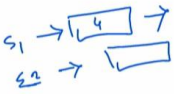
Slotted ALOHA

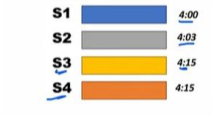
Md. Farhan Hossan
B.Sc. in CSE, UAP
farhanhossan246@gmail.com

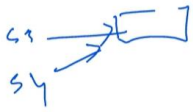
Slotted ALOHA is a network protocol used to manage data transmission and avoid collisions in a shared communication channel.

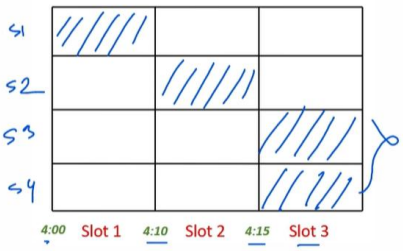
How It Works

1. Time is Divided into Slots
2. Send Only at the Beginning of a Slot
3. If Two Packets Collide, They Try Again









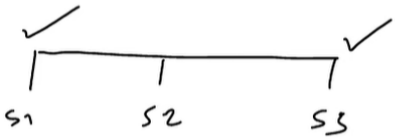
CSMA

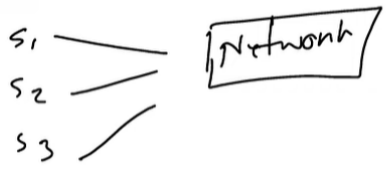
Carrier Sense Multiple Access (CSMA)

What is CSMA?

Carrier Sense Multiple Access (CSMA) is a protocol used in network communication where multiple devices share a common transmission channel. Before sending data, devices check whether the channel is free. If it is free, they send data; otherwise, they wait.

Now, let's dive into CSMA/CD (used in wired networks) and CSMA/CA (used in wireless networks).





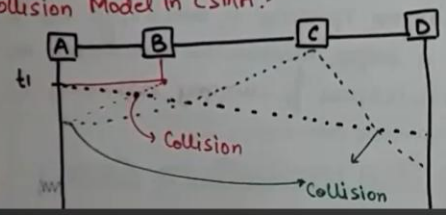
Carrier Sense Multiple Access with Collision Detection (CSMA/CD)

In this technique, station senses the medium before trying to use it.

CSMA → Sense before transmit
CSMA → Listen before Talk

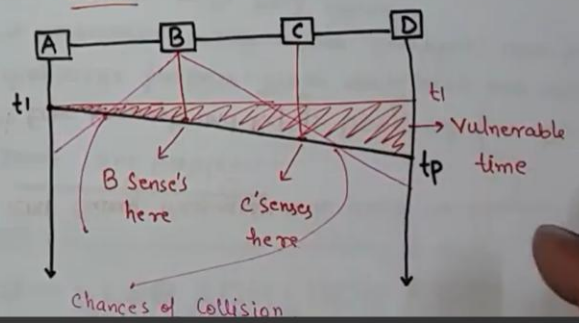
[CSMA requires that each station first listen to the medium before sending the packet.]

Collision Model in CSMA:-



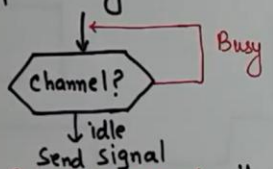
Vulnerable Time:- It is the Propagation Time (Tp). This is the time needed for a signal to propagate from one end of the medium to the other end.

Diagramatic Representation of Vulnerable Time in CSMA:-

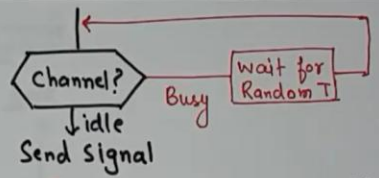


Persistence Methods in CSMA:-

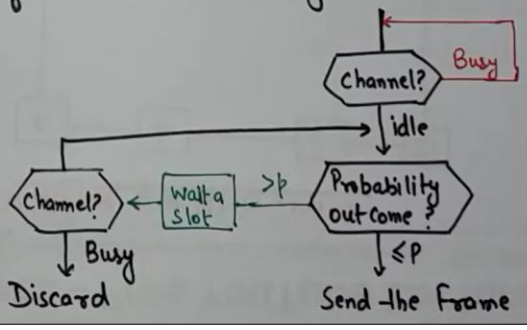
(i) 1-Persistent Method:- if the station finds the line idle, it sends frame immediately (with probability 1).

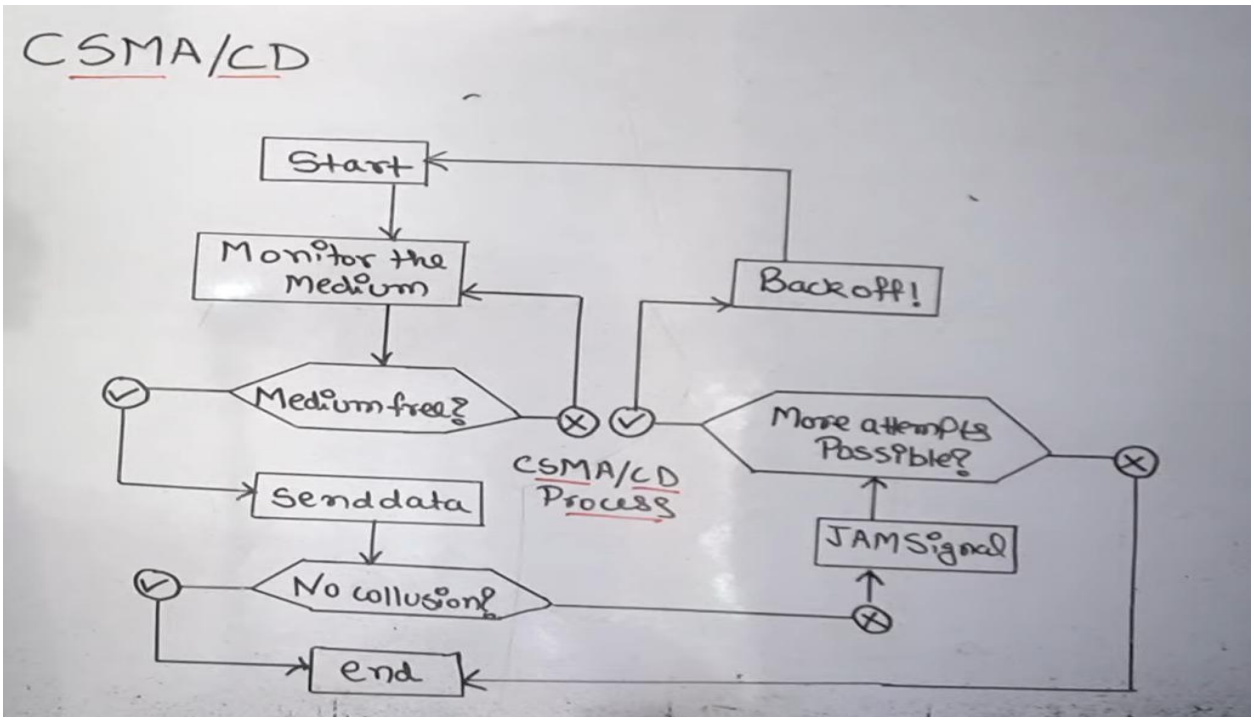


(ii) Non-Persistent Method:- if the line is idle, Station sends the frame immediately. if the line is not idle, it waits for a random amount of time and then senses the line again.



(iii) p-Persistent Method:- It combines the advantages of the other two strategies.





CSMA/CD (Collision Detection)

CSMA/CD (Collision Detection) – Used in Wired Networks like Ethernet

CSMA/CD is designed to detect and handle **collisions** in a shared wired network.

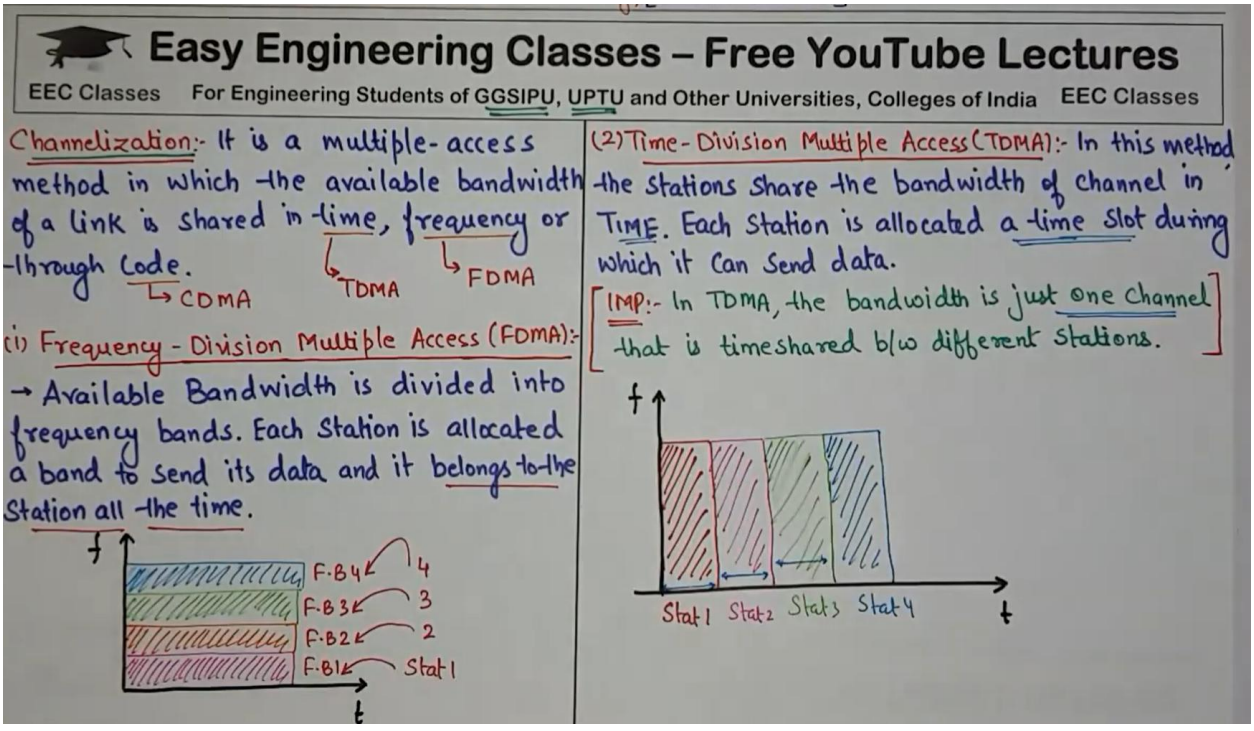
How It Works:

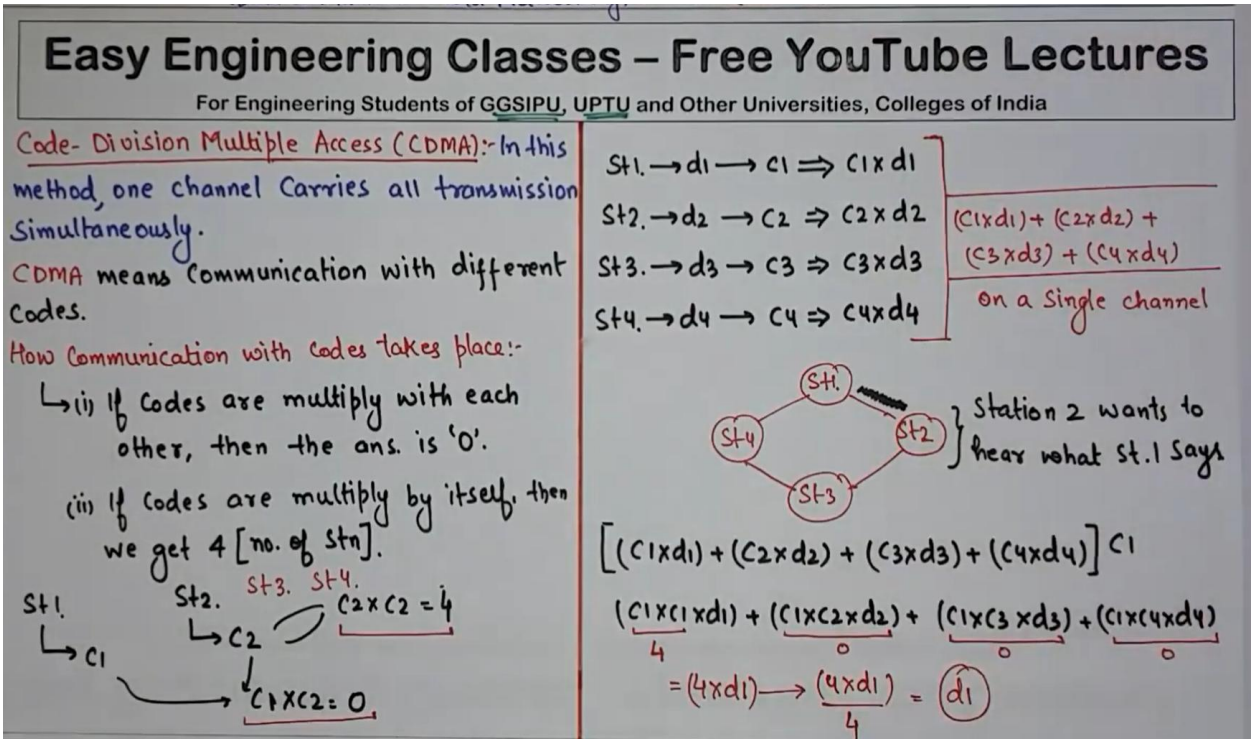
1. **Carrier Sense (Listen First)**
   - The device listens to the network to check if the channel is **free**.
2. **Transmit Data**
   - If the channel is free, the device sends data.
3. **Collision Detection**
   - If two devices send data at the same time, a **collision** occurs, corrupting the data.
4. **Jam Signal**
   - The devices detect the collision and send a **jam signal** to notify all other devices that a collision has happened.
5. **Backoff (Wait & Retry)**
   - The devices stop transmitting and wait for a **random amount of time** before trying again.
6. **Retry Transmission**
   - After waiting, they start the process again from step 1.

FDMA,TDMA,CDMA(chanalization)

Comparison of FDMA, TDMA, CDMA

Feature	FDMA	TDMA	CDMA
High carrier frequency stability	Required	Not necessary	Not necessary
Timing/synchronization	Not required	Required	Required
Near-far problem	No	No	Yes,power control tech.
Variable transmission rate	Difficult	Easy	Easy
Fading mitigation	Equalizer not needed	Equalizer may be needed	RAKE receiver possible
Power monitoring	Difficult	Easy	Easy
Zone size	Any size	Any size	Large size difficult





Network Device

Hub/ripitor

Network Device

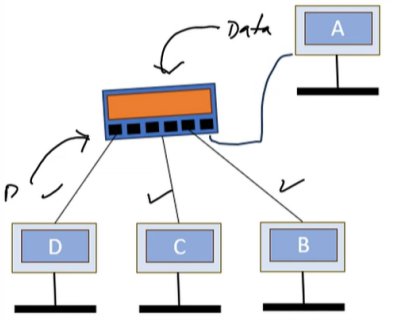
Md. Farhan Hossan
B.Sc. in CSE, UAP
farhanhossan246@gmail.com

HUB Network Device:

A HUB is a basic networking device used to connect multiple devices (like computers, printers, or other network devices) in a local area network (LAN). It is a central connection point in the network, allowing devices to communicate with each other.

Key Features of a HUB:

1. **Central Connection Point**:
   - A hub acts as a "meeting place" where all the devices in a network plug in using Ethernet cables.
2. **Broadcasting Data**:
   - When a hub receives data from one device, it broadcasts (sends) the data to all connected devices.
   - Only the intended recipient processes the data, while others ignore it.
3. **Layer 1 Device**:
   - It operates at the **Physical Layer** (Layer 1) of the OSI model.
   - It doesn't filter or direct data packets; it simply forwards them.
4. **Simple and Affordable**:
   - Hubs are inexpensive and easy to set up, making them ideal for small networks or learning purposes.



Network Device

Types of HUBs:

1. **Active HUB**:
   - Requires power and amplifies the incoming signals before broadcasting them.
2. **Passive HUB**:
   - Doesn't require power. It simply forwards data as it is.
3. **Intelligent HUB**:
   - Adds management features like monitoring traffic or diagnosing issues.

Limitations of a HUB:

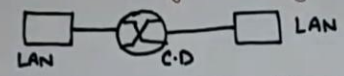
1. **No Filtering**:
   - A hub doesn't know which device the data is intended for, so it sends data to all devices, creating unnecessary traffic.
2. **Collisions**:
   - If two devices send data at the same time, a collision occurs, and data must be resent. This slows down the network.
3. **Outdated Technology**:
   - Modern networks use **switches** instead of hubs because switches are smarter and more efficient.

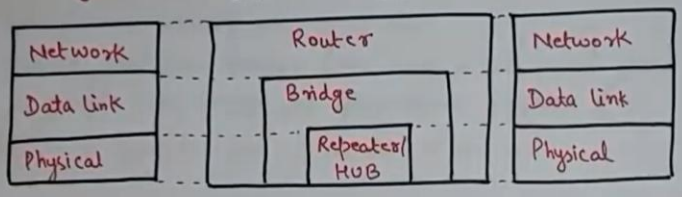
Data Communication and Networking – Connecting Devices-1

Easy Engineering Classes – Free YouTube Coaching

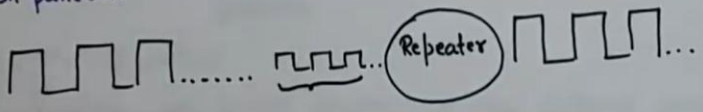
For Engineering Students of GGSIPU, UPTU and Other Universities, Colleges of India

Connecting Devices:-

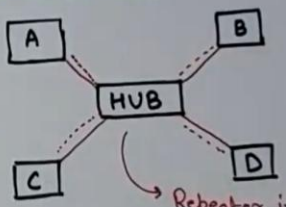




(i) Repeaters:- This devices operates Only in the physical Layer. A repeater receives a signal and, before it becomes too weak / Corrupted, regenerates and retimes original bit pattern.



HUB:- In Star topology, Repeater is Called HUB.



Repeater in Star topology.

NOTE:- Repeater/HUB forwards every bit. They don't have the intelligence to filter data.

Network Device

Md. Farhan Hossan
B.Sc. in CSE, UAP
farhanhossan246@gmail.com

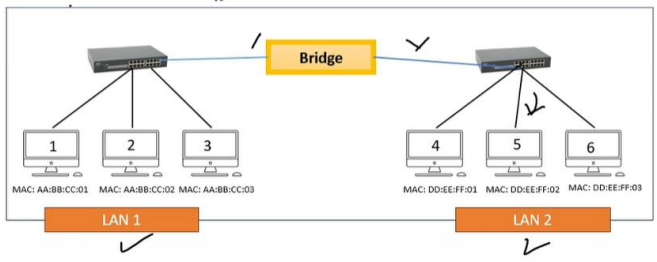
Bridge in Computer Networks

A **bridge** is a network device that connects two or more local area network (LAN) segments to create a single, unified network. It operates at the **Data Link Layer (Layer 2)** of the OSI model and uses **MAC addresses** to decide whether to forward or filter data packets (frames).

Features of a Bridge:

- ✓ Traffic Control
- ✓ Collision Domain Segmentation

Source Device	Destination Device	Source LAN	Destination LAN
PC2 (AA:BB:CC:01)	PC5 (DD:EE:FF:02)	LAN 1	LAN 2



Network Device

SWITCH Network Device:

A **Switch** is a more advanced networking device than a hub. It connects multiple devices (like computers, servers, or printers) in a network and ensures that data is sent only to the intended device, making it faster and more efficient.

Key Features of a Switch:

1. **Smart Data Handling**:
   - Unlike a hub, a switch doesn't broadcast data to all devices. It sends the data directly to the specific device it's meant for.
2. **MAC Address Table**:
   - A switch keeps a table of MAC addresses (unique identifiers for devices on the network).
   - When a device sends data, the switch learns where the device is and updates its table.
3. **Layer 2 Device**:
   - Switches operate at the **Data Link Layer** (Layer 2) of the OSI model.
4. **Collision-Free Communication**:
   - Switches create a separate communication path for each pair of devices, eliminating data collisions.

Network Device

Md. Farhan Hossan
B.Sc. in CSE, UAP
farhanhossan246@gmail.com

Scenario Setup

1. **Devices and Ports**:
   - **PC** is connected to **Port 1** of the switch.
   - **Laptop** is connected to **Port 2** of the switch.
   - **Printer** is connected to **Port 3** of the switch.
2. **MAC Address Table (Initially)**:
   - When the switch powers on, its **MAC address table** is **empty** because it hasn't learned any MAC addresses yet.

Step 1: PC Sends Data to Laptop

- The **PC** wants to send data to the **Laptop**.
- The **PC** knows the **MAC address** of the laptop (AA:BB:CC:DD:EE:02), so it includes this in the Ethernet frame:
  - **Source MAC**: AA:BB:CC:DD:EE:01 (PC's MAC)
  - **Destination MAC**: AA:BB:CC:DD:EE:02 (Laptop's MAC)

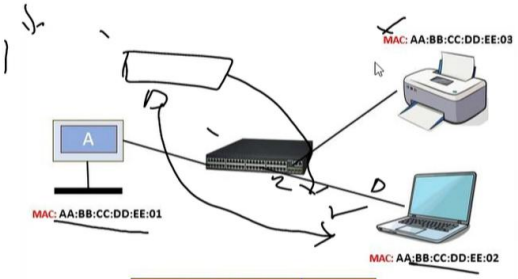
Step 2: Data Reaches the Switch

- The Ethernet frame arrives at the **switch** on **Port 1**.
- The switch examines the **source MAC address** (AA:BB:CC:DD:EE:01) and learns that:
  - Device with MAC address AA:BB:CC:DD:EE:01 is connected to **Port 1**.

Step 3: Switch Updates the MAC Address Table

Step 4: Switch Looks for the Destination MAC

Step 5: Laptop Responds to PC



Mac Address	Port
AA.BB.CC.DD.EE.01	1
AABB.CC.DD.EE.02	2

Network Device

Md. Farhan Hossan
B.Sc. in CSE, UAP
farhanhossan246@gmail.com

Router:

A **router** is a networking device that connects multiple networks. It acts as a traffic director, ensuring data travels efficiently from one network to another, typically between a local network (LAN) and the internet (WAN).

Scenario Flow (With Private and Public Ports):

Step 1: Laptop Sends a Request to Google:

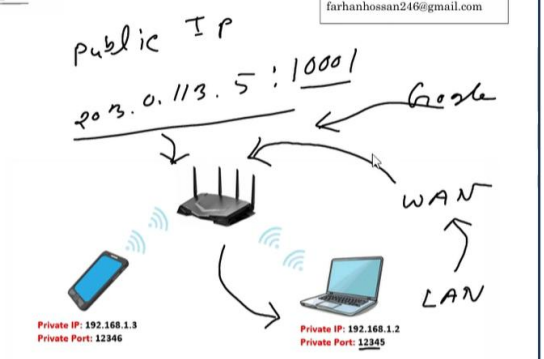
1. The **laptop** with private IP 192.168.1.2 wants to visit **Google** (which is at IP 8.8.8.8).
2. The **laptop** sends an HTTP request to Google.

Step 2: Router Performs NAT (Private to Public Translation):

1. The **router** receives the request from the laptop.
2. Since 192.168.1.2 is a **private IP** (which can't be routed on the internet), the router needs to replace the **private IP** with its **public IP** (203.0.113.5).
3. The router **assigns a public port number** (e.g., 10001) to the session, mapping the laptop's private port 12345 to the public port 10001.
4. The **router** now sends the request to Google with **public IP** (203.0.113.5) and **public port** (10001).

Step 3: Responses Come Back from Google:

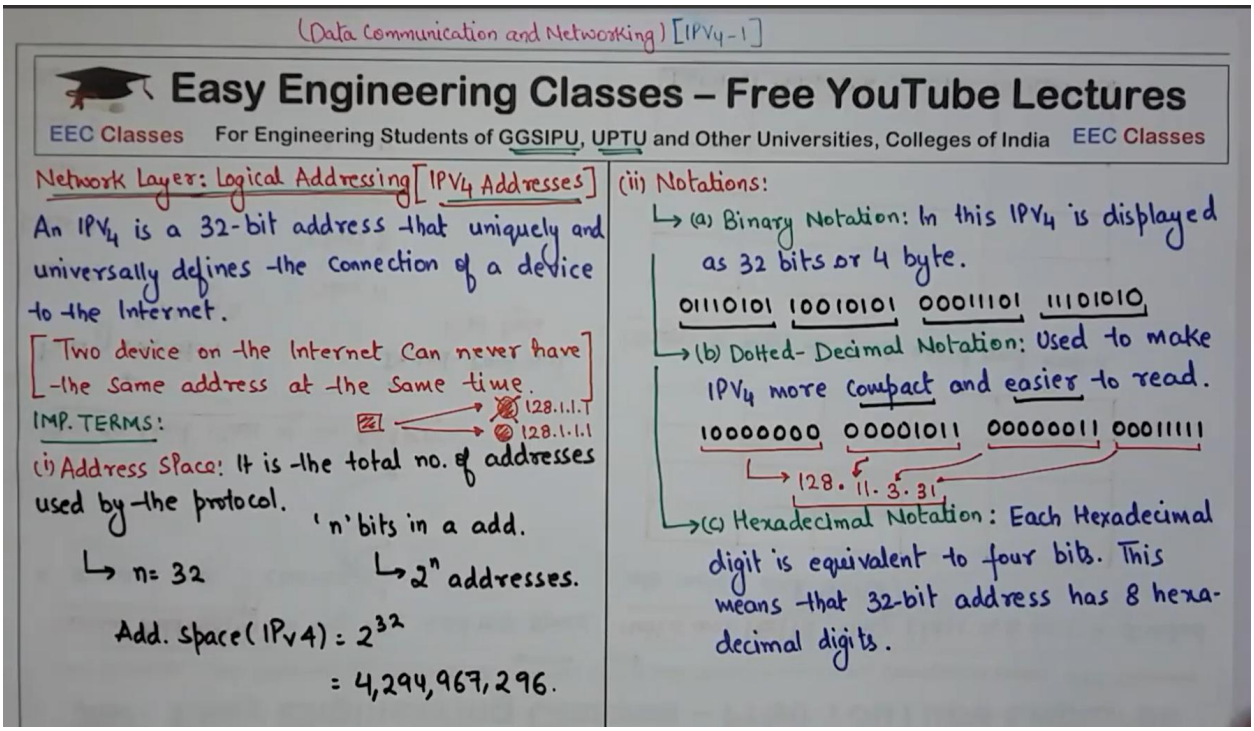
1. Google's server responds to the requests from ~~both devices~~ (laptop ~~and phone~~).
   - Google's response for the **laptop** goes to 203.0.113.5:10001 (public IP and port assigned to the laptop).
2. The router looks at its **NAT table**, checks the port numbers (10001 and 10002), and forwards the responses back to the correct device (laptop or phone).



Private IP	Private Port	Public IP	Public Port
192.168.1.2	12345	203.0.113.5	10001

Network Address Translation (NAT) Table

IP ADRESS



Classful Addressing: In this the address space is divided into 5 classes → Class A, Class B, Class C, Class D, Class E

IMP:

How to find Class of an Address:-

Binary Notation (First Byte)	IMP: Dotted-Decimal (First Byte)
Class A 0....	Class A 0–127
Class B 10....	Class B 128–191
Class C 110....	Class C 192–223
Class D 1110....	Class D 224–239
Class E 1111....	Class E 240–255

Netid and Hostid: Only class A, B or C is divided into netid and hostid.

class	Byte1	Byte2	Byte3	Byte 4
classA	Netid	Hostid	Hostid	Hostid
ClassB	Netid	Netid	Hostid	Hostid
Class C	Netid	Netid	Netid	Hostid

n bits = 1
(32-n) = 0
A: n = 8
B: n = 16
C: n = 24

Mask: It helps to find netid and hostid.

class	Binary (Mask)	Decimal
classA	11111111 00000000 00000000 00000000	255.0.0.0
class B	11111111 11111111 00000000 00000000	255.255.0.0
classC	11111111 11111111 11111111 00000000	255.255.255.0

DEFAULT MASK FOR CLASSFUL ADDRESSING

Easy Engineering Classes – Free YouTube Lectures
EEC Classes For Students Studying Programming with C++ in Class XI and XII (CBSE, NCERT) and B.Tech Courses

Classless Addressing:- In this, Variable length blocks are used that belongs to no class.

Restrictions:-

↳ (i) Addresses in a Block must be Contiguous.

(ii) No. of Addresses in a Block must be a power of 2 [1, 2, 4, 8, 16, ...]

(iii) The first address must be evenly divisible by the no. of addresses.

Block
First → 205.16.37.32 → 205.16.37.33 → 205.16.37.34 ... Last → 205.16.37.47

16 = 2^4 =

Mask in classless Addressing can take any Value from 0 to 32. (n) + (32-n) = 0.

↳ Slash/CIDR Notation.

x.y.z.t/n → defines the mask.

IMP Points:

(i) First Address in block can be found by setting the rightmost (32-n) bits to 0s.

(ii) Last address can be found by setting the rightmost (32-n) bits to 1s.

(iii) No. of Addresses = 2^{32-n}

Example:- One of the Addresses is 205.16.37.39/28. Find first, last and total no. of addresses.

11001101 00010000 00100101 00100111 → 00101111

F.A:- 11001101 00010000 00100101 00100000 N.A: 2^4

= 205.16.37.32 L.A = 205.16.37.47 = 16

One More Way of Extracting Block Info^n :-

↳ (i) No. of Addresses, $N = 2^{32-n}$.

(ii) First Address = (Address) AND (MASK)

(iii) Last Address = (Address) OR (COMPLEMENT of MASK)

Example:- For a Address 205.16.37.39/28, Find

i) First Address

ii) Last Address

iii) No. of Addresses. $= 2^{32-28}$

$= 2^4$

$= 16$

Address:- 11001101 00010000 00100101 00100111

Mask:- 11111111 11111111 11111111 11110000

First Add. 11001101 00010000 00100101 00100000

AND

1+1=1

Mask (comp.) 00000000 00000000 00000000 00001111

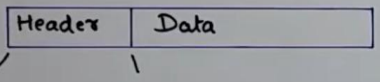
11001101 00010000 00100101 00101111

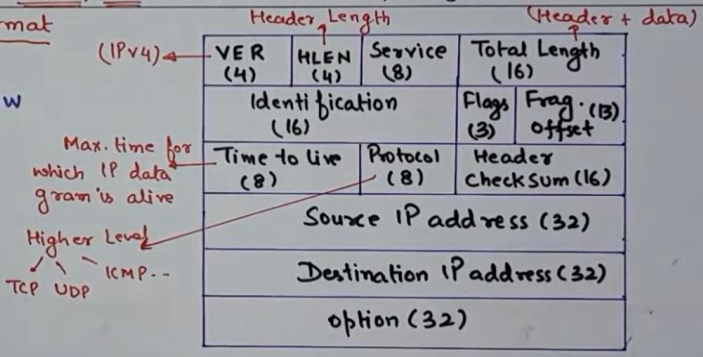
IPv4 Protocol: IP Packet/Datagram Format

IMP Points:-

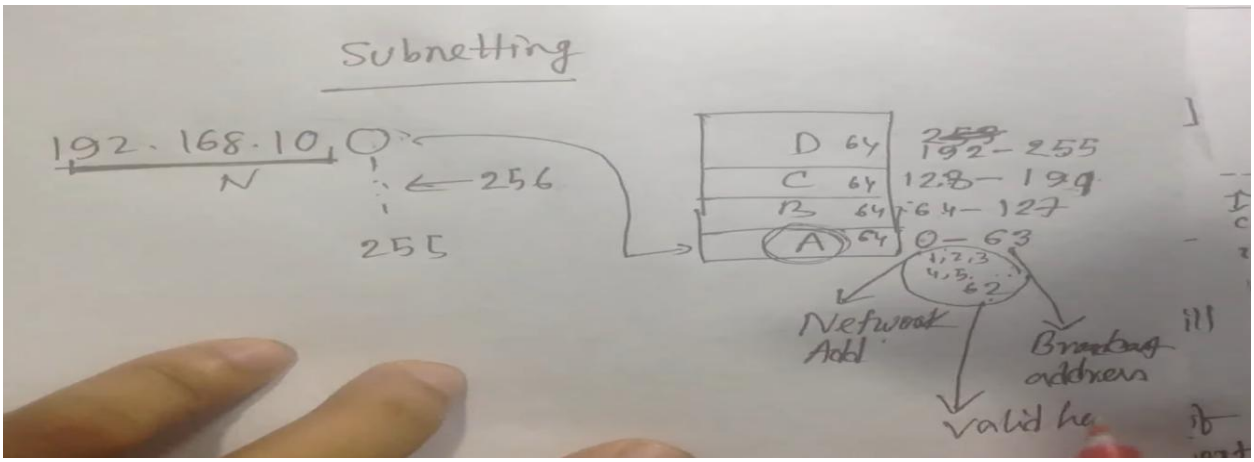
(i) Used by TCP/IP protocols at N/W Layer.

(ii) Unreliable and Connectionless





(Header) [32 bits]



IP → 192.168.10.0

subnet mask : 255.255.255.224

Find out

1. Block size ?
2. Number of subnets ?
3. Number of valid hosts ?
4. what are the valid subnets or subnets ID ?
5. what are the first valid host & Last valid host ?
6. what's the Broadcast address ?

Easy Engineering Classes – Free YouTube Lectures

2^{128}

For Engineering Students of GGSIPU, UPTU and Other Universities, Colleges of India

IPv6 Addresses:- It is of 128 bits or 16 bytes.

↳ Length is (4) -times -the length address of IPv4.

Notations:-

(i) **Dotted- Decimal:-** It is used for IPv4 Compa--libility. 221.14.65.11.105.45.170.34.12.234.18.0.14.0.115.255](16)

(ii) **Colon Hexadecimal:-** It is used -to make -the address more readable. In this notation, the 128 bits are divided into 8 sections, each of 2 bytes in length. [Two bytes in Hexadecimal req. 4 Hexadecimal digits].

FDEC: BA98: 7654: 3210: ADBF: BBFF: 2922: FFFF

Abbreviation:- It is a technique -to reduce the length of IPv6 address. It is done by omitting/removing the leading zeros of a section.

[NOTE:- Only the leading Zeros can be dropped]

[Zero-Compression]

FDEC: 0074: 0000: 0000: 0000: B0FF: 0000: FFF0

omitting these Zeros

FDEC: 74: 0: 0: 0: B0FF: 0: FFF0 } Abbreviated Address

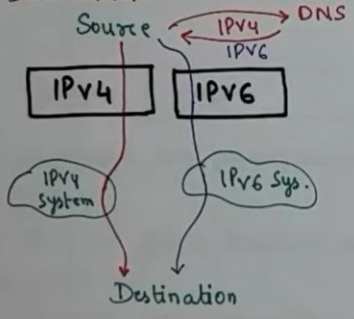
↓

FDEC: 74: : B0FF: 0: FFF0

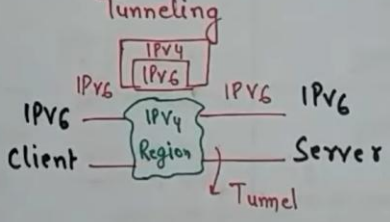
↳ GAP.

Transition from IPv4 to IPv6:- There are three transition Strategies.

Dual Stack



Tunneling



IPv6 Packet is encapsulated in an IPv4 Packet when it enters the IPv4 Region.

Header Translation

When most of system are on IPv6 but some still uses IPv4.