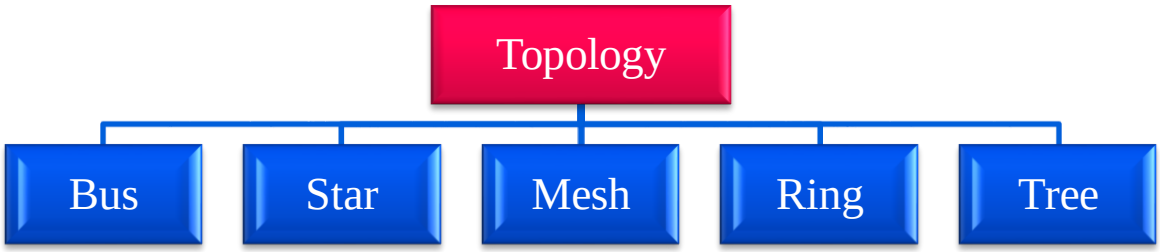
➢ Advanced Question

1. Explain Network Topologies.

The Geometric representation of such a nodes and links relationship is called network topology.

- ➢ The network topology is on the physical layer topology.
- ➢ It show or explain the how computers and network devices are connected over the network.
- ➢ Physical establishment of network.
- ➢ Types of Network topologies:



a) Bus Topology:

This topology is used when the establishment small network, not for live longer means short time and simple or temporary.

- Bus topology is the passive topology because it does not use any electronics to amplify signal pass through simple cable from one computer to another.

- The bus topology is the slower because when single computer sends the message then other computer cannot be transfer message in the network.
- When one computer send the message then the massage is send to all address and all computer check the destination add and destination address is not match then reject and match then accept it.
- It require proper termination at both ends of cable, it avoid reflections.
- Broadband or coaxial cable is used
- If bus fails, whole network fails.

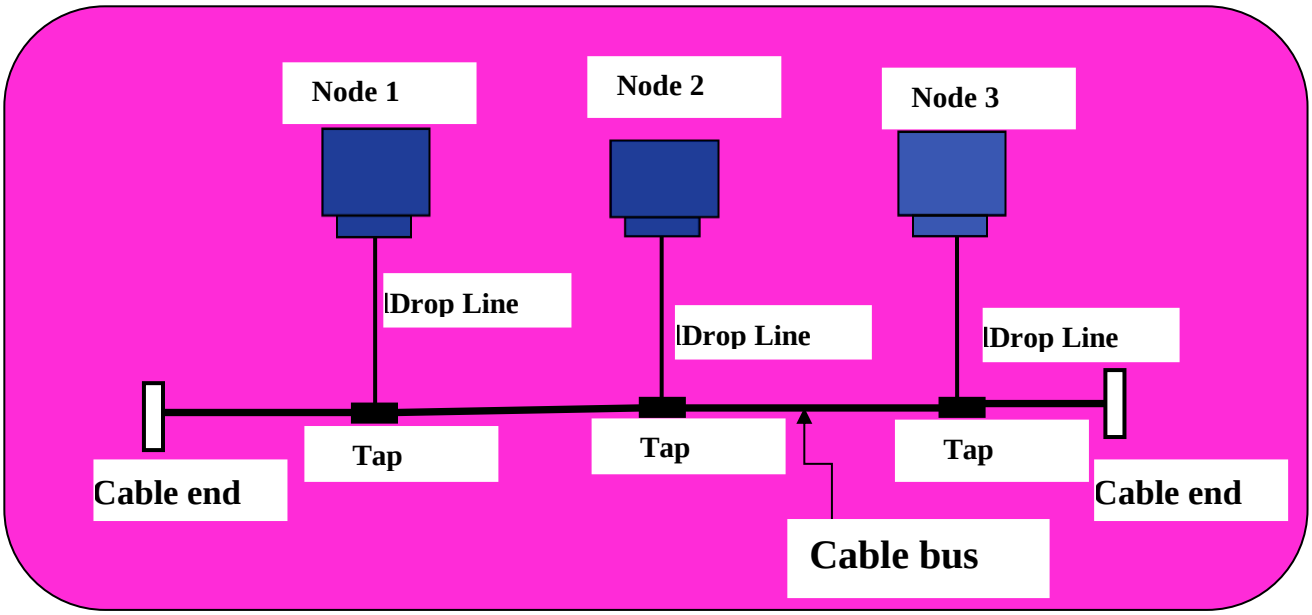


Fig.: Bus Topology

b) Ring Topology:

In the topology, all and every computer connected to the next computer.

When one computer send the transmit token (short) to other computer then the token send to next computer until the

destination address receive that message and after that send message in reply.

- It is one way direction message flow.
- It is active topology.
- When the one node defected then network become down.
- High performance topology
- Large bandwidth necessary
- Relatively difficult to reconfiguration
- Difficult to troubleshoot

c) Star topology:

In this the all computers are connected to central devices such as hub via cable.

- It is used in concentrated network
- Twisted, coaxial or optical cable used
- When central device faulty then whole network fails.
- Adding new system is become easy
- Fault diagnose is easy
- When computer is fail then it cannot be affect the network.

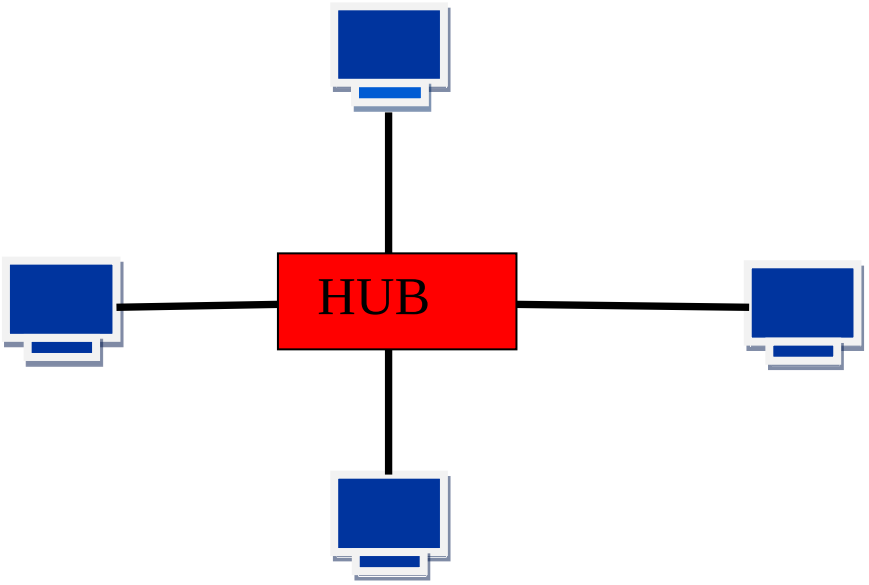


Fig: Star Topology

d) Mesh topology:

Mesh topology is the topology in which all computers are connected each other with point to point dedicated link.

- The link carries data only between two computer that's why number of cables is used.
- If devices connected in network = n

  No. of cables = n (n-1) / 2

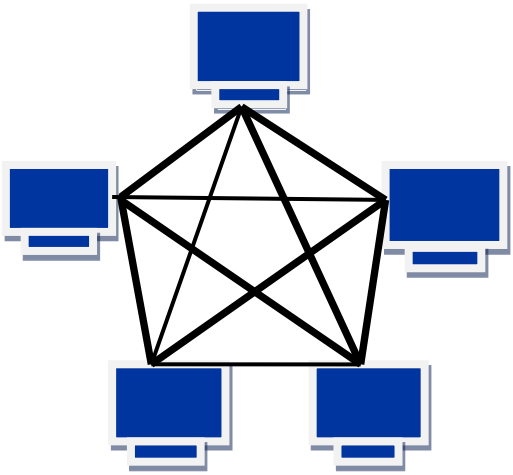


Fig: Mesh Topology

e) Tr

A variation of star topology is called Tree topology.

In which the computers is connected to the hub (secondary hub) but it is not central hub.

- Central hub is controls the whole network and all computers are no directly connected with central hub.
- The all secondary hub connected to the central hub.
- The central hub in this topology is an active hub which contains repeater
- The repeater which amplifies the signal and signal can be travel long distance.
- Secondary hub is passive or active.

2. Explain TCP/IP Networking Model.

The TCP/IP networking model is shown in below figure.

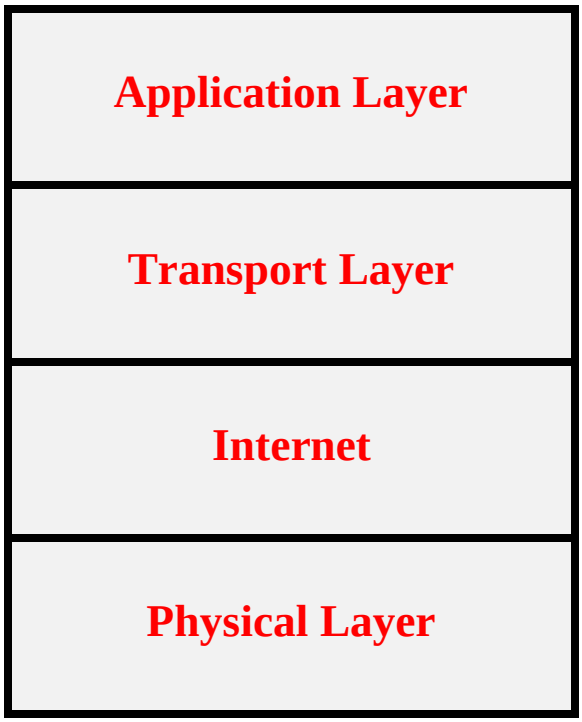


Fig.: TCP/IP reference model

- It has four (4) layers.
- In this transport layer delivery the packets is not guaranteed.
- Vertical approach
- Only connection less services provided at the network layer
- TCP/IP model s not capable to identify services, protocols and interfaces.
- Protocol replacement is not easy while technology change.
- This model doesn't fit any other protocol stack.
- It cannot be used in other application.

3. Explain LAN and WAN Network.

LAN Network:

LAN network is designed for operates over the small physical area such as office, between two or more buildings.

All the computers are connected via single cable.

Topologies used in LAN:

i. Bus, ii. Ring, iii. Star and iv. Tree etc…

- ✓ It is used in different application variety.
- ✓ It is uses layered architecture.
- ✓ They are 100 mbps capability of operating.
- ✓ Via LAN computer and workstation interconnected in the offices.
- ✓ Easy to design and troubleshoot.
- ✓ In the LAN network, one server computer which serving all the remaining clients.
- ✓ Nowadays share of file, Information and resources are too easy because of LAN.
- ✓ It is privately owned network.
- ✓ Distances cover: few kilometers
- ✓ It also capable to connect computers, server and printer also.
- ✓ Many companies also connect voice, audio and video peripheral.
- ✓ It different from MAN and WAN on the base of topology and transmission media.
- ✓ Data rates: 10 Mbps to 16 Gbps

LAN is stands for Local Area Network.

WAN:

When network become extended as per requirement become gradually increase then network expand.

The WAN network connects the networks all over the world and use for the communication from one country to another.

The different user communication in wan established using leased telephone lines or satellite links and similar channel.

- ✓ Cheaper and more efficient for use phone network for the links.
- ✓ Large block data from existing records or files transfer
- ✓ Terminal located all over the country
- ✓ In WAN network is Large distance covered, that's why it may be face major problems like propagation delay and variable signal travel times.
- ✓ For avoiding this problem it decides that
  All terminal use same centralized common data provided by the central resolution computer.
- ✓ Example:
  Airline Reservation System
- ✓ Host: large computer
  Host provides the service to many computers.
  Provided services are:
  I} providing computing capabilities
  II} Providing access to database
- ✓ WAN contains the machine collection used for running users (i.e. application) programs.
- ✓ By communicating subnets, all the hosts are connected in WAN.
- ✓ Without internet network we cannot access or transfer the information from one host to another.

✓ Subnets function:

Carry messages from one host to host

- ❖ Subnet consist of two components i.e.:
  1] Transmission lines
  2] Switching elements
- ❖ It use public leased or private communication devices and can spread over a wide geographical area.
- ❖ Most WAN network contains large number of cables or telephone lines each one connecting a pair of router.

4. Explain Operation of Switch.

Switch is the device which is used in the network.

Switch providing bridging functionality with high efficiency.

- ❖ Switch connects multiple devices or segments in a LAN means it act as multiport bridge.
- ❖ It has a buffer – for check each links are connected or not
- ❖ When the data send then it store the data packets in the buffer of receiving link
- ❖ Then it checks the destination address for search outgoing link.
- ❖ Whenever it gets the information about outgoing link is free then it sends the frame to a designated address.

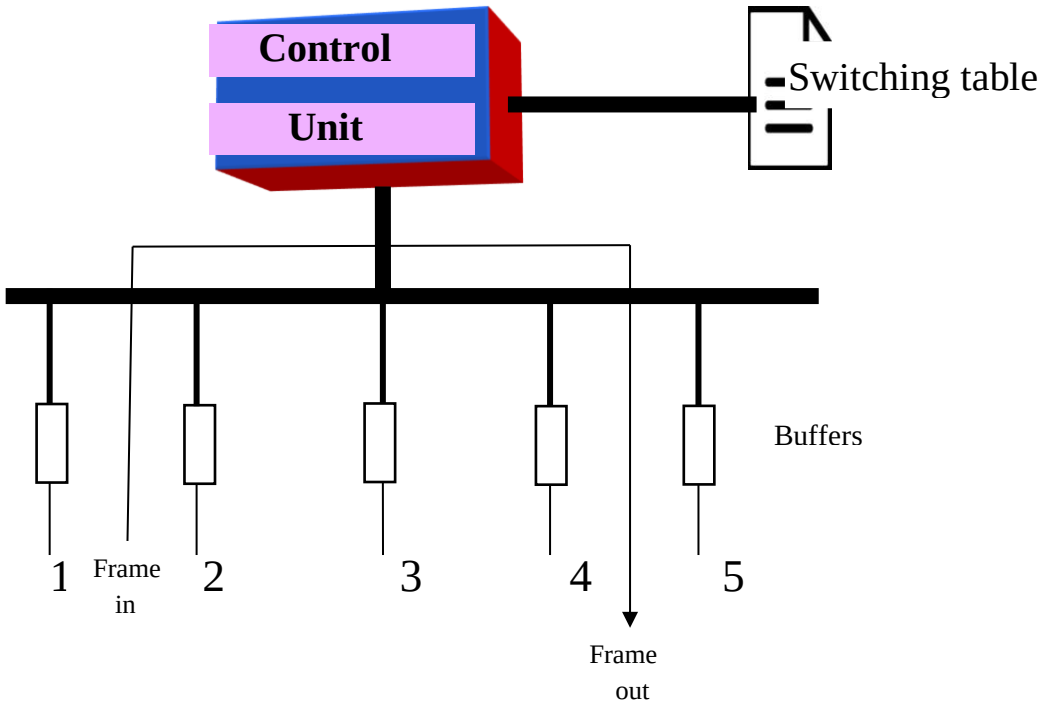


Fig.: Switch

In the figure see that the frame arrives at port no. 2 and it store into the buffer.

To find output port: The CPU and Control unit using the information in the frame consult the switching table.

Then the frame is sent to the port 5 for transmission.

TYPES of SWITCHES:

A. Store and forward Switch:

It store the frames input buffer until the it received whole packet.

B. Cut through switch:

It forward the packets to the output buffer as soon as destination address found.

5. Describe the purpose and functions of various network devices.

6. Make list of the appropriate media, cables, ports, and connectors to connect switches to other.

7. Define Network devices and hosts.

NETWORK DEVICES:

Network devices are the devices which used for the connection establishment of network for communicate between two or more systems.

HOST:

Host is the most important part of network without host we cannot be provides services to many computers.

Other words host is the end devices system which is connected in the network.

8. What are Ethernet Standard (802.3) and Frame Formats?

➢ Intermediate Question

1. Comparison between UTP, MM and SM Ethernet Cabling

2. Make Cross cable.

The cross cable is used for connects same types of network devices (computer to computer).

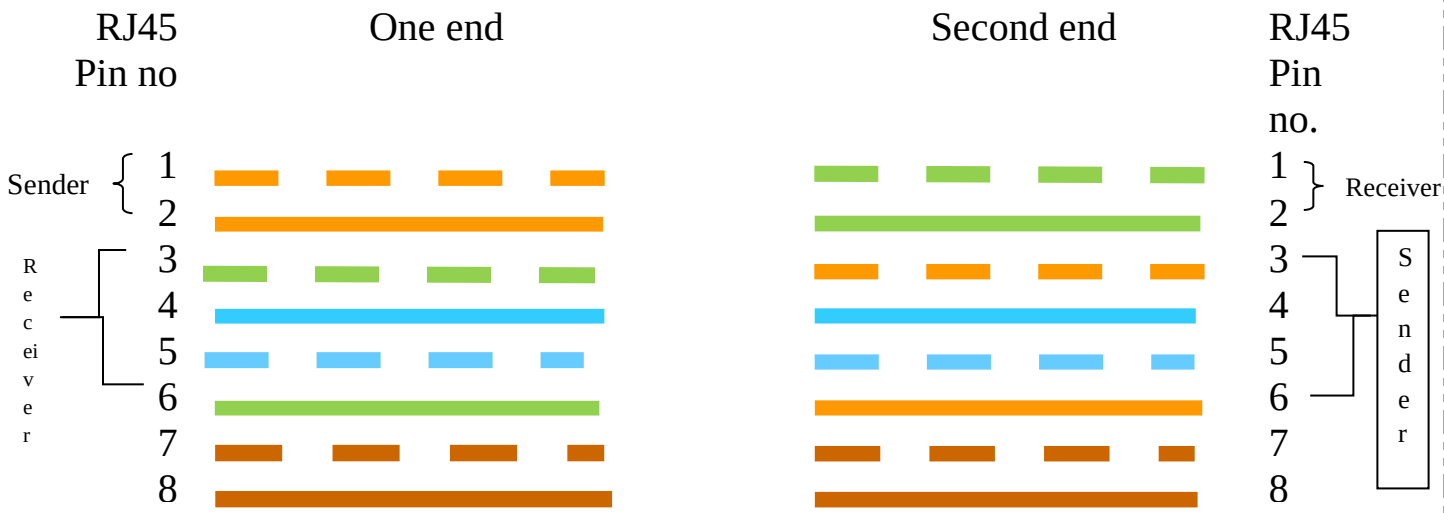
Examples like

a) Computer to Computer
b) Router to computer

The following steps for make Cross Cable:

i. Take a twisted pair cable
ii. Cut and strip the wire using striping tool
iii. Twisted pair having eight wire cable inside and see the all the in the pair of two wire twisted each other like
    - ✓ Orange + white wire twisted with Orange wire
    - ✓ Green + white wire twisted with Green wire
    - ✓ Blue + white wire twisted with Blue wire
    - ✓ Brown + white wire twisted with Brown wire
iv. Open the all wire means untwisted the wire from one another
v. Take RJ45 connector
    - RJ45 stands for Registered Jack 45
    - It is standard interface which used for the LAN network devices connection to one another
    - It has 8 pin

vi. Arrange the Cable as per the colour coding of the cross cable requirement shown in below



vii. All the wires are inserted into RJ45 connector.

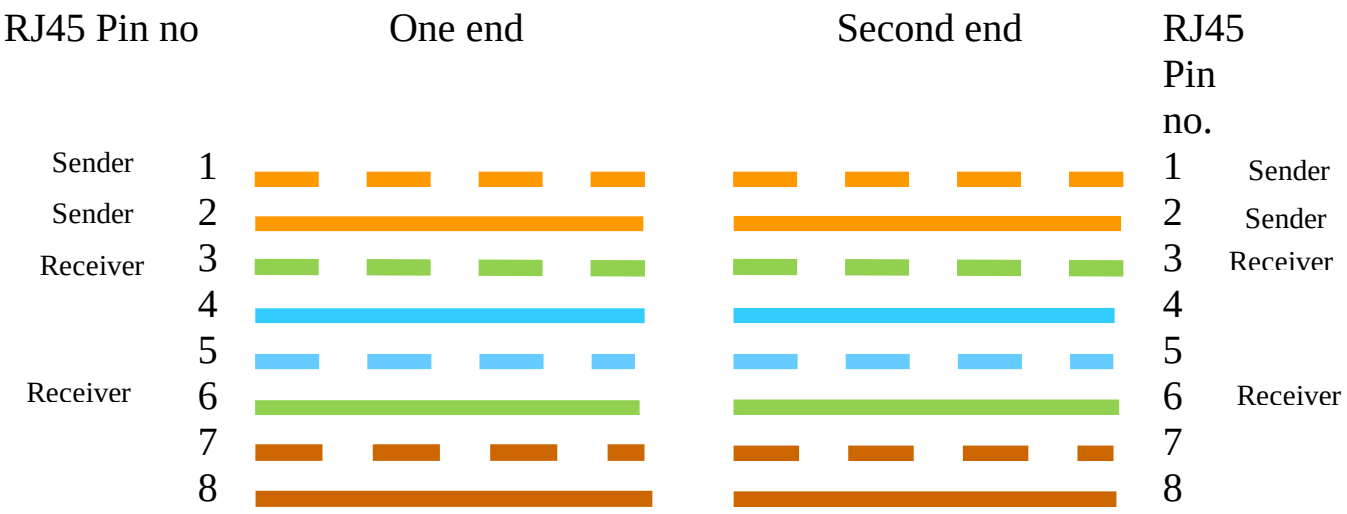
viii. Then crimping the connector using crimp tool at both end of the cable.

3. Make Straight-Through Cable.

The Straight-through cable is used for connects different types of devices such as computer to switch switch/hub to router etc….

The following steps for make Straight-Through Cable:

Colour coding for the make Straight Cable:



4. Differentiate between LAN/WAN operation and features.

5. Explain ARP, ICMP and Domain name.

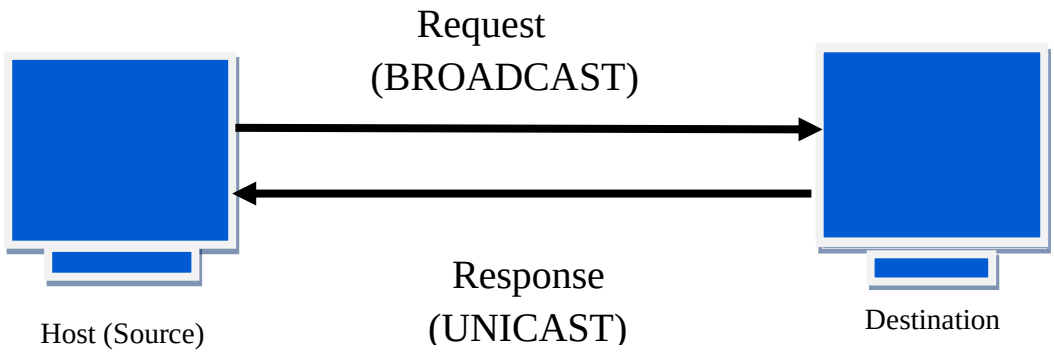
ARP:

ARP is stands for Address Resolution Protocol.

- It is work on the DATA LINK LAYER means second layer of OSI model.

- It is used for the find out physical address (MAC/ System name) of the system with the help of logical address (IP).
- It is layer 2 protocol because MAC address work on layer 2.
- ARP used only IPv4 not IPv6.
- ARP generated in only same network not different network.
- ARP procedure shown in the below figure:

ARP Req	Source IP add	Destination IP add	Source MAC Add	Dest. MAC Add (FF:FF:FF:FF:FF)



ARP Reply	Source IP add	Destination IP add	Source MAC Add	Dest. MAC Add

Fig.: Address Resolution Protocol

- Same network ID is used.

- Types of ARP:
  a. ARP

b. RARP (Reverse Address Resolution Protocol)
c. Proxy ARP
d. Gratuitous ARP

ICMP:

ICMP is stand for Internet Control Massage Protocol.

- It is internet layer protocol.
- It is used for the find out error between network management and network devices communication.
- It is also used for the data will be received by the destination at a time or not.
- When the data cannot be approach to destination while IP package cannot be work properly then router can be send error message to the host that
    a. Request service not available
    b. Destination not reachable
- It is not transport protocol means it cannot be transfer data from one system to another.
- It is helpful for the network diagnostic as a
    - Ping
    - Traceroute

DOMAIN NAME:

The name of website is known as domain name.

- Without domain name we can use the website using the IP address but the IP address of the different and multiple website cannot be remember easily that's why the domain name will be used.
- For example:

6. Describe the components required for network and Internet communications.

The components required for network and internet communications are

a) Hub, Repeater and Ethernet Cable Connector:

Both the devices are work on Layer 1 of OSI model means Physical Layer device.

HUB:

Hub is the device which use for connect more than two computer in the network.

- ✓ Hub is broadcast device that cannot be able to store MAC Address.

REPEATER:

Repeater is the device which use for when signal travel for long distance in between repeater will be used because of repeater regenerate the signal strength and pass through it for the receiver.

Ethernet Cable Connector:

Ethernet Cable connector which is the physical device which used for the transmit data from one device to another device.

- ✓ For the transmitting data through this it is more secure than the Wireless transmission device.

b) Switch and Bridge:

Both the devices are used at Data Link Layer means Layer 2 devices of OSI model.

SWITCH:

Switch is the active device which is used for connect more than two devices will be communicate in the network.

- ✓ It is maintain CAM (Content Addressable Memory) in which store the information about the MAC address of the devices.
- ✓ It is broadcast device but when it is receives the MAC addresses of the devices.
- ✓ It supports unicast as well as multicast.
- ✓ Error checking is possible.
- ✓ It has buffers.

BRIDGE:

Bridge is the device which used for the divide single network into various network segment.

- ✓ It takes the decision about the incoming network traffics will be filtering or forwarding.
- ✓ It is use only 2 or 4 ports.
- ✓ It is also maintain the MAC address Table.
- ✓ But it cannot capable for Error check.
- ✓ It has not buffer.

c) MLS and Router:

Both the devices work on the Layer 3: Network Layer of OSI model.

MLS SWITCH:

MLS is stands for Multi-Layer Switching which is the network device that can be responsible for the connecting network devices and also capable for the routing of the network.

- ✓ It works on the switches packets with the help of IP address as well as MAC address.

ROUTER:

Router is a network device which is maintain the routing table that capable for choose best path for the transmission of the data.

- ✓ It is used for connects different networks.

7. Explain Encapsulation and DE capsulation in OSI Reference model.

Encapsulation and De-Capsulation in OSI reference model is shown in below:

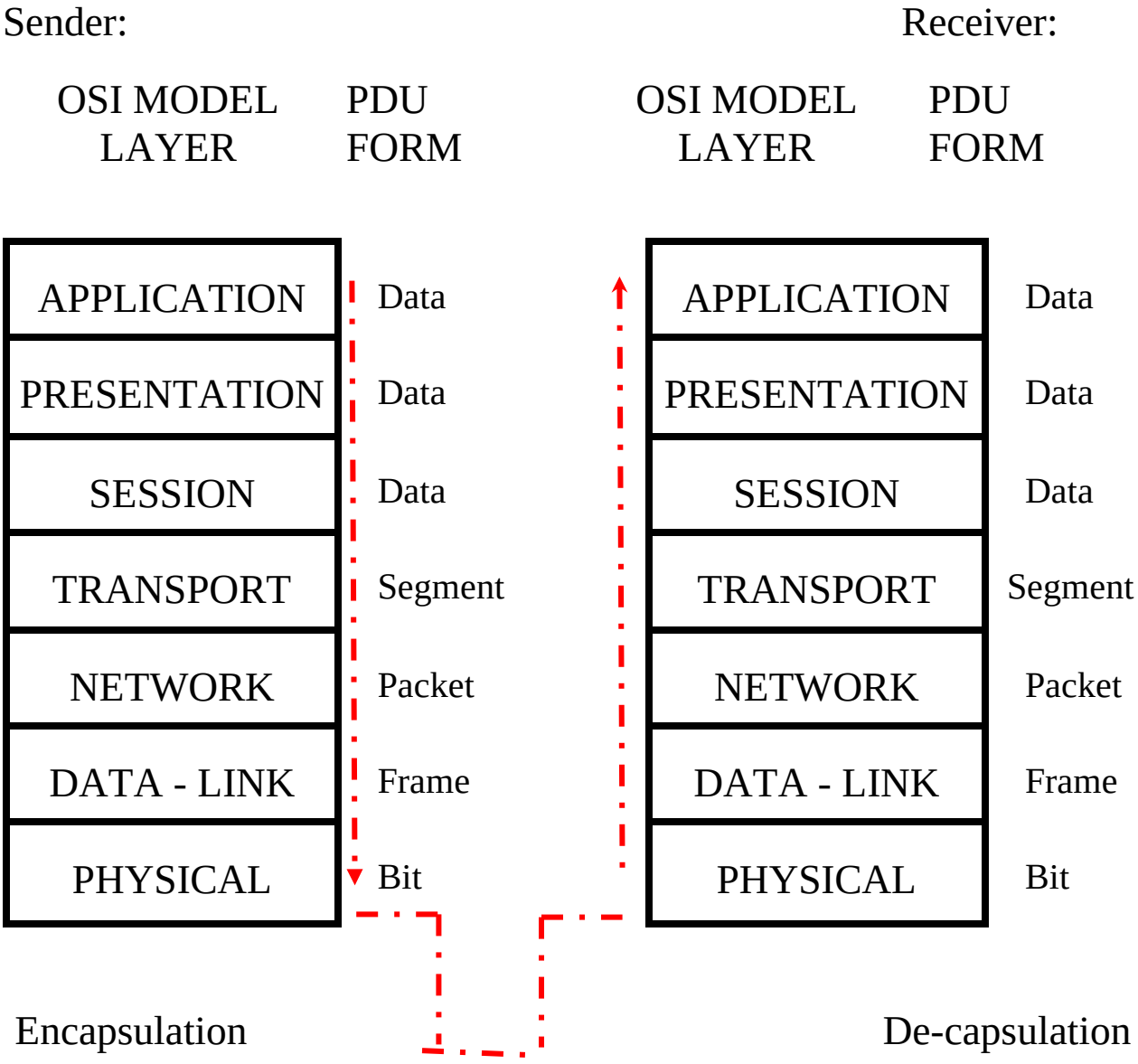
ENCAPSULATION:

In the process of data travel at sender side in OSI reference model from top to bottom layer and each layer adds the information like IP Header is called as Encapsulation.

DECAPSULATION:

In OSI reference model, when data at the receiver side travel from bottom to top layers and when it move up then released the header one by one each layer is called DE-capsulation.

The process of Encapsulation and DE capsulation is shown in below figure:



8. Explain network segmentation and basic traffic management concepts.

Network Segmentation:

9. What is flow control and acknowledgment?

Flow Control and Acknowledgement:

In the computer network, when data sent from sender to receiver in between data will be loss or may be interrupt that's why the flow control is necessary for the communication.

When the data will be reaches or not to the receiver about this sender will have no any idea. And sometimes the data is also loss that could be important packet of the information. And the big question for receiver is that how they inform to the sender that the packet will be loss or send me repeat.

For the overcome of this problems Acknowledgement service is available in the communication.

- Data link layer provides flow control.
- Also Transport layer provides flow control but it performed end to end and not across a single link.
- Acknowledgement is the services in which receiver send the ACK packet in which say that the packet will be received successfully or not.
- ACK is for positive response
- NACK is the negative response means that data packet cannot be received and send it repeatedly.

There are different services are available for the Flow control and ACK:

a) Stop and Wait Protocol
b) Sliding Window Protocol

c) GO-back-N ARQ

➢ Advance question

1. Use the OSI and TCP/IP models and their associated protocols to explain how data flows in a network.

2. Identify and explain at layers 1, 2, 3, and 7 using a layered model approach.

3. Explain CSMA/CD and CSMA/CA.

CSMA/CD:

CSMA/CD stands for Carrier Sense Multiple Access/ Collision Detection.

- CSMA/CD is the protocol which used in an Ethernet network or wired network while we use the cable like copper cable, fibre optic cable etc. for the transmission of data from one system to another system.
- CSMA/CD implemented on SWITCH.

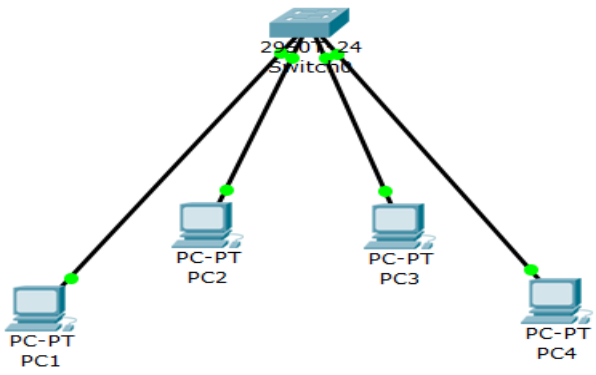


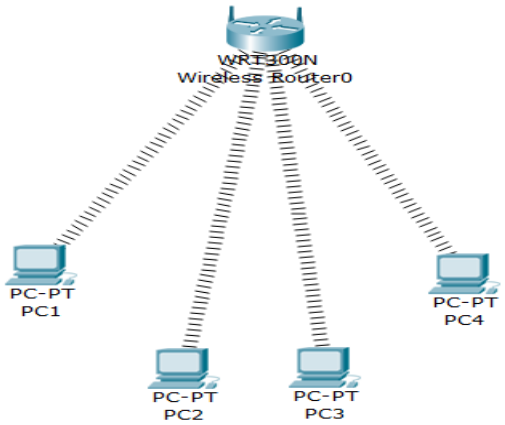
Figure: for CDMA/CD concept understanding

- When all the number of different systems are connected in a network through one switch.
- When all system will be communicate with each other means when PC1 send file to the PC4 at a time other side PC3 send files to the PC2 and PC2 send a file to the PC4. This situation is create in all networks that time when two data will be meet with other means collides with each other than data will be loss.
- That why the CSMA/CD protocols will be introduced for the overcome from this situation.
- The CSMA/CD protocol will be implemented on Switch. It predetermined that at which place the collision will be occurs than it will be communication channel full duplex to half duplex then collision not occurs but when situation not overcome then half duplex to simplex mode communication will be work on for the transmission data from the one system to another.

CSMA/CA:

CSMA/CA is stands for Carrier Sense Multiple Access/ Collision Avoidance.

- CSMA/CD is the protocol which is used in the wireless technology for the avoiding collision data which share by the different system at a time.
- Standards which use this protocol is 802.11x technology.
- CSMA/CA will be implemented on the ROUTER in wireless connection.



- In this protocol, when multiple systems will be connect with the router at a same time then router will the avoiding the system connection because of avoiding collision.
- Sometimes we can see that when we connect mobile/PC/laptop to the wi-fi but we cannot enable to establish connection this is one example of the CSMA/CA protocol.
- This protocol is not implemented on the wired network.

4. Explain this frame and find layer.

Ethernet (802.3) Frame Format

7 bytes	1 byte	6 bytes	6 bytes	2 bytes	42 to 1500 bytes	4 bytes	12 bytes
Preamble	Start of Frame Delimiter	Destination MAC Address	Source MAC Address	Type	Data (payload)	CRC	Inter-frame gap

An Ethernet IEEE 802.3 standard is widely used in LAN (Local Area network).

- It is physical layer technology.
- Ethernet – CSMA/CD access method

Preamble:

- Preamble used for the synchronization purpose in Ethernet frame.
- ✓ It has 7 bytes information.
- ✓ 7 bytes means that 56 bits.
- ✓ In preamble 56 bits of alternating of 1s and 0s (101010101010…….).

Start of Frame Delimiter:

- Start of Frame Delimiter is also used for the reason of synchronization and SFD is acts as flower.
- In SFD, Flag is fixed i.e., 10101011
- Size: 1 Byte (8 bits).

Destination and Source MAC address:

- Both destination and source MAC address is 6 bytes in size individually.
- Layer 2 protocol is deals with the physical address that is MAC address.

- MAC address is 48 bits.
- The next six bytes followed by the SFD is the destination MAC address.
- MAC Address generated from the Source it has to put on the SOURCE ADDRESS field.
- MAC Address of the destination that the system MAC address it receives the data. So the upper layer network it receives to encapsulate header of the trailer.
- Source and destination are residing in the same local area network it has the Source and Destination MAC address.
- Otherwise when Destination address is not available or unknown then ARP protocol works for the finding or get MAC address of the destination.

Type:

- 2 bytes
- It is decides the types of data that is what upper layer protocol.

DATA:

Whatever it receive from the upper layer i.e., network layer that information is placed in the field (data field).

CRC:

- CRC stand for the Cyclic Redundancy Check
- It is used for the error detection
- Size: 4 bytes

5. Draw and explain Cisco hierarchical model.

CISCO Hierarchical Model:

Cisco hierarchical model is the industrial adopted model used for the designing scalable, reliable and cost-efficient internetwork.

Three layer Hierarchical Model shown in below figure:

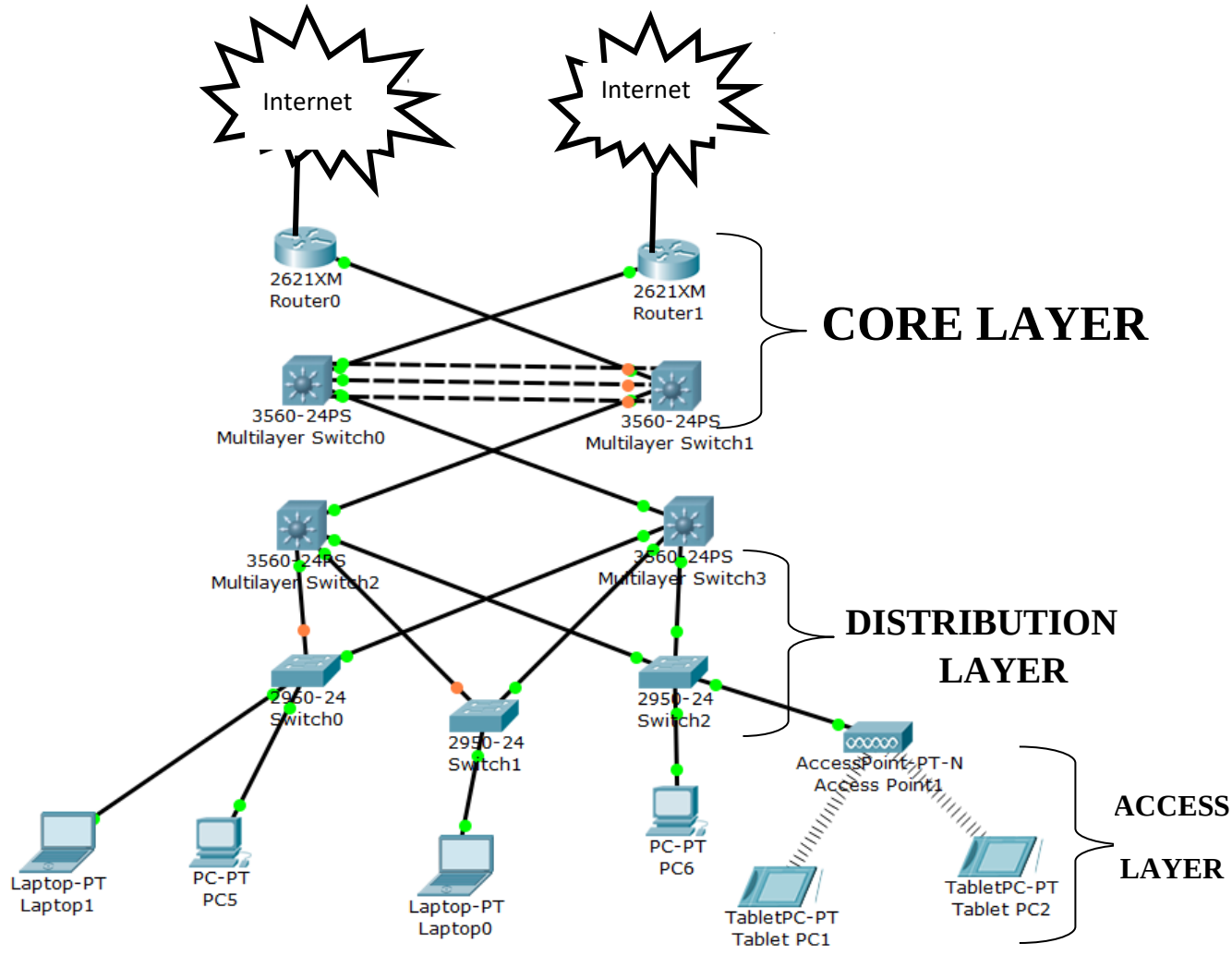


Fig.: Cisco Hierarchical Model

When all the host (users) access the internet service with the help of hierarchical model architecture.

Three Layer of Hierarchical Model:

1. CORE LAYER
2. DISTRIBUTION LAYER
3. ACCESS LAYER

1. CORE LAYER:

On the Core Layer of Cisco Hierarchical Model Router and switches networking devices will be used.

Switch used in core layer that is the layer 3 switch namely Multi Layer Switch and Router which is used for the routing in the network as well as the different-different WAN networks because of establishing proper communication and users receives the proper data.

Router and MLS switch will be used in the WAN network.

For the maintaining of Core devices we can use the core network and it is also used for the when one network will be down or break then other network will be continuously work without any breakage.

Features and working:

- Provides high-speed switching like fast transport
- Provides reliability and fault tolerance
- Scaling by using faster and not more, equipment
- Avoiding CPU-intensive packet manipulation caused by security, inspection
- QoS classification or other processes

2. Distribution Layer:

Distribution layer of this model, in this layer multiple switches i.e. both layer 3 and layer 2 are connected and at this point provided services to the hosts.

Layer 2 switches used for the establishment local area network and in this network more configuration will be not required. It is used for the simple internet access and network services like file transfer and communication between devices.

Distribution process will be works on this layer.

It is the mediator between the Core Layer and Access Layer and it is distributes an information between both layers.

Feature and Workings:

- LAN or WAN links aggregation:

  Its create link between Access layer (LAN) and Core layer (WAN). Its work on distribution and communication between them.
- ACLs and Filtering used as a Policy-based Security
- Routing services between LANs and WANs and also between routing domains e.g., EIGRP to OSPF
- Redundancy and load balancing
- A boundary for route aggregation and summarization configured on interfaces toward the core layer.
- Broadcast Domain Control because routers or multilayer switches do not forward broadcasts.

The devices acts as the demarcation point between broadcast domains.

3. ACCESS LAYER:

ACCESS LAYER of this model will be more near to the user work on it.

Devices used for the access information in this layer are PC, laptop, mobile devices, Voice IP phone.

Feature and Workings:

- Layer 2 switching
- High availability
- Port security
- QoS classification and marking and trust boundaries
- ARP inspection
- Manage Virtual Access Control Lists (VACLs)
- Manage Spanning Tree:
  For multiple switches management
- Power over Ethernet (PoE) which is used single cable for the power & data and auxiliary VLANs for VoIP

6. Drawing of a typical wired and wireless enterprise LAN.

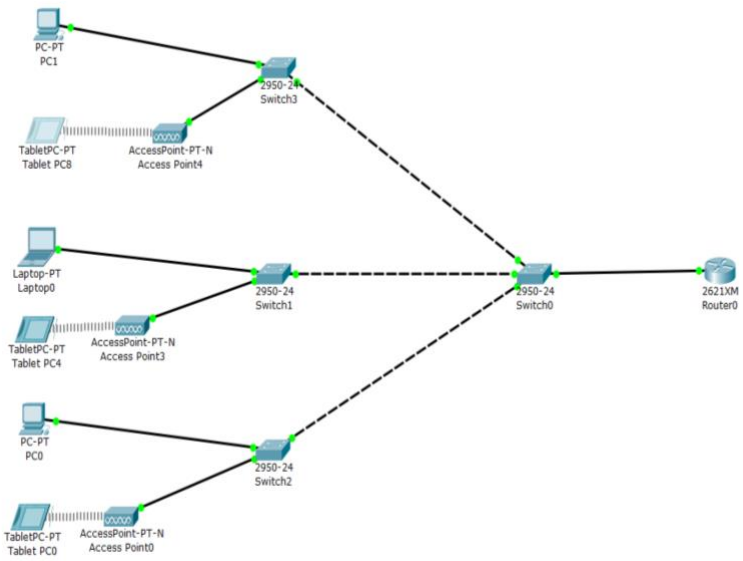


Fig.: typical wired and wireless enterprise LAN

7. Describe the uses of straight-through and crossover Ethernet cables.

   Uses of Straight-through Ethernet Cable:

It is used for connecting different networking devices.

a) it connects host (PC, laptop) to switch/hub
b) connection establishment between switch and router
c) connects server to switch
d) also connects layer 3 switch to layer 2 switch
e) connection between layer 3 switch to router
f) switch to networks LAN modems
g) connects computer to a cable/DSL modem's LAN port
h) connects two hub/switch with one switch/hub using uplink port and other one using normal port

Uses of Crossover Ethernet Cable:

It is used for connecting Same networking devices.

a) It establish connection between router and router
b) It connects switch to switch network
c) For connecting both computer device with each other
d) It also connects computer and router connection

8. Explain Layer 2 and Layer 3 switch.

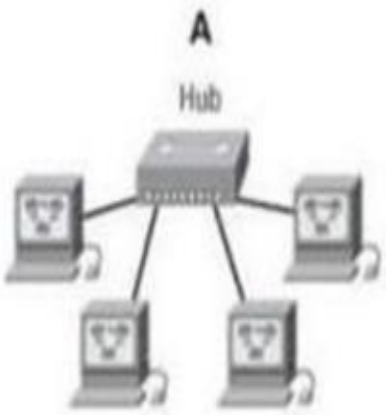
Layer 2 and layer 3 switch:

Features	Layer 2 Switch	Layer 3 switch
1. OSI model layer	Works on Data Link Layer of OSI model	Works on Network layer of OSI model
2. MAC/IP	It is supported MAC address for the transfer data from one system to another system.	It is supported IP and MAC address for the transfer data from one to another system
3. Routing	It is not responsible for routing.	It is also capable for routing.
4. Tables	It contain MAC table.	It contains MAC as well as routing table.
5. Inter-vlan	In this switch, inter-vlan is not supported for the communication between two VLANs used router or Layer 3 switch is needed.	In this switch, inter-vlan is supported for the communication between two VLANs.
6. other	Layer 2 switch is used for distribute information on distribution layer of Cisco Hierarchical model.	Layer 3 switch is the device works on core layer of Cisco Hierarchical model.
7. End device	End devices are directed connected to the layer 2 switch.	When end devices are directed connected to the layer 3 switch then it will be simply work as a layer 2 switch.
8. Port	Each port on a switch is a separate collision domain, that's why no packet collision should be occur.	

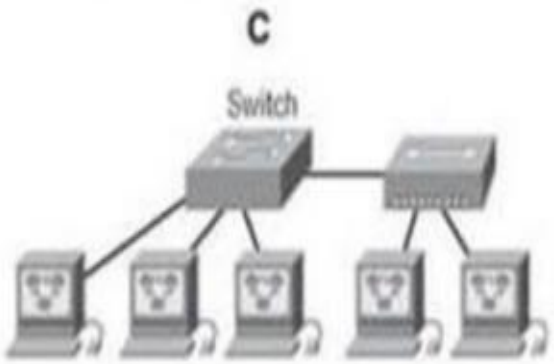
9. Identifying Collision and Broadcast Domains

Collision Domain: 1

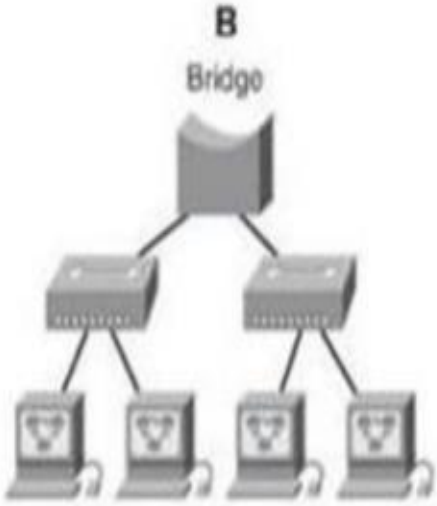
Broadcast Domain: 1



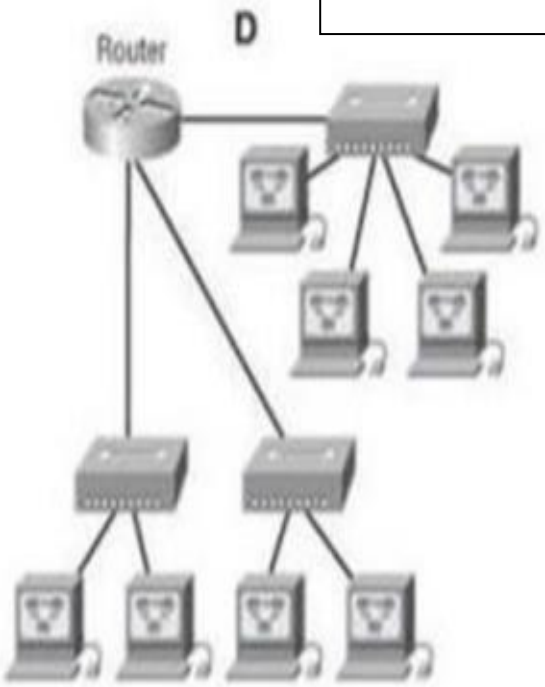
Collision Domain: 1
Broadcast Domain: 1



Collision Domain: 4
Broadcast Domain: 1



Collision Domain: 2
Broadcast Domain: 1



Collision Domain: 3
Broadcast Domain: 3

9. Explain Spanning Tree Protocol.

Spanning Tree Protocol:

Spanning Tree Protocol is also famous name STP.

- ✓ STP is the Layer – 2 protocol.
- ✓ Purpose: 1. It ensuring to not creating loops in network when network choose redundant path
  2. Break the loop (loop free technology)
- ✓ In a network when loop is create then whole network will be either down or death.
- ✓ It is works on bridge and switch.
- ✓ That's why the STP is introduced.
- ✓ It is the protocol which break the loop will be created in network while two or more than two switches connected.

Works:

When all switches connected into the network they will be thing that the master switch is itself. Then

1. Switch send the BPDU packets to all devices that connected with the port.
   BPDU: Bridge Protocol Data Unit which is contain the information about the STP.
2. All switches gives the MAC into the BPDU packet.
3. BPDU packet store all the MAC address of different switches and ensure that which MAC address Bridge ID is the higher or lower.
4. After that from the MAC Address it decided which switch is master and non - designated switch.
   Lower MAC address: Master Switch and
   Higher MAC Address: Non-designated Switch
   Other MAC address: Slave Switches

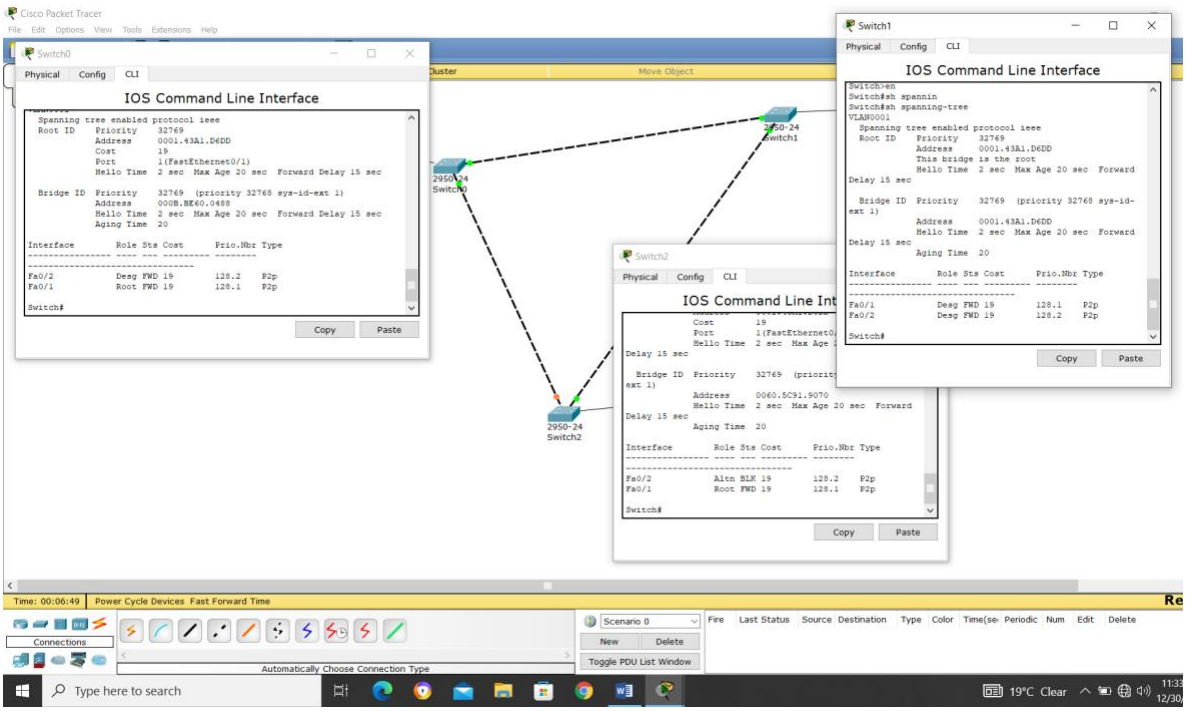


Image: Spanning Tree Protocol

In this Image, we can see that the switches are connected in the network. In the table see that in IOS common Line interface:/

Interface of Switch0:

Fa0/2	Desg	It means that the switch is Root Bridge / Master switch.
Fa0/1	Root	

Interface:

Fa0/1	Desg	It means that switch is the slave switch.
Fa0/2	Desg	

Interface:

Fa0/2	Altn	It means that the switch is Non-designated switch.

Altn means block

Fa0/1 Root

11. Explain unicast, Multicast and Broadcast.

Unicast, Multicast and Broadcast are the Transmission Method in the network.

UNICAST:

Unicast is the one to one network.

Unicast transmission sends the data between two networks in which single sender (one host) of the network 1 sends data to the only single receiver of the other network.

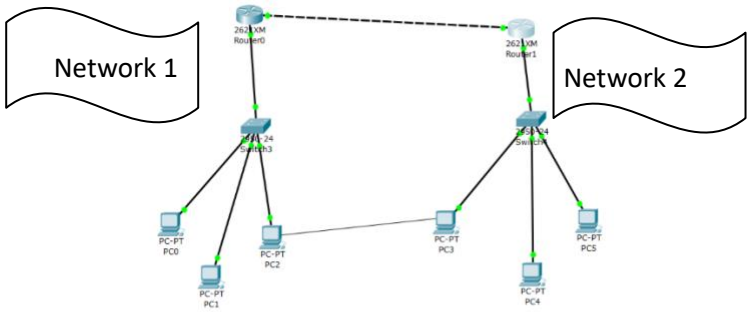


Fig: Unicast transmission

(in which PC2 only sends data to PC3)

Multicast Transmission:

Multicast is the one to many.

In multicast Transmission the any single host of the one network send the data to the more than one in another network host.

In network 1, only one sender but in network 2, more than one receiver. In the below figure see that the 2 receiver will be connect with the network 1 host.

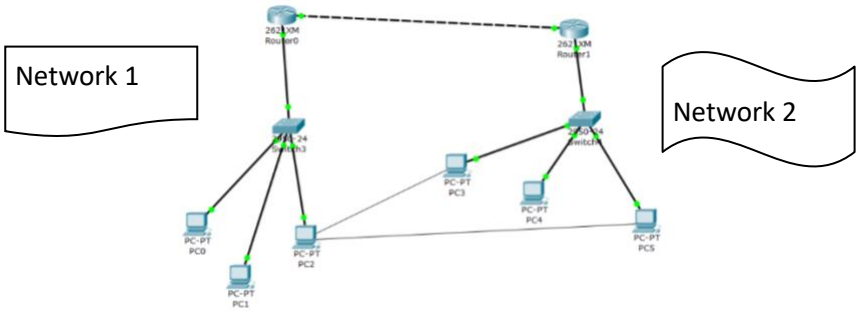


Figure: Multicast Transmission

Broadcast:

Broadcast is the one to ALL.

In this transmission one sender of the one network send the information to the all host of the another network or same network is called Directed or Limited Broadcast respectively.

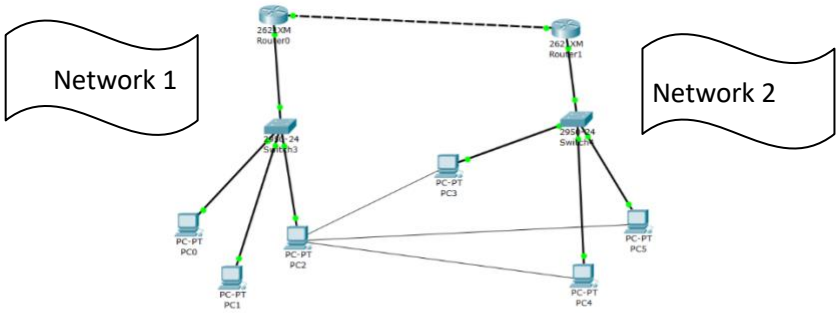


Figure: Multicast transmission

12. Explain CAM (Content Addressable Memory).

CAM is stands for the Content Address Memory.

It is the memory which used in the Switch. In the memory we can store the data like MAC address of the host (computer, laptop, other network devices) which is connected to the ports of that switch. Also, store the MAC address with the port number of switch and VLAN database means which port of the switch support which number of VLAN.

CAM Table

MAC Address	Port	VLAN
0000.0000.1111	1	1
0000.0000.2222	2	1
0000.0000.6666	6	1
0000.0000.5555	5	1
0000.0000.3333	3	20
0000.0000.4444	4	1

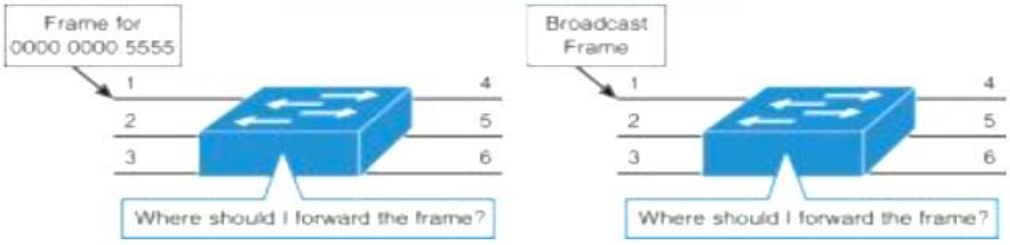


Table: CAM

13. Explain CAM (Ternary Content Addressable Memory).

Ternary Content Addressable Memory is the memory which store the information about which switch port connected to the host MAC address and also VLAN and port number.

This TCAM table is different from the CAM table because in TCAM table which store the information about the policies means which port of the switch which has the permission granted or deny to communicate with the MAC address as well as IP address of the host or services.

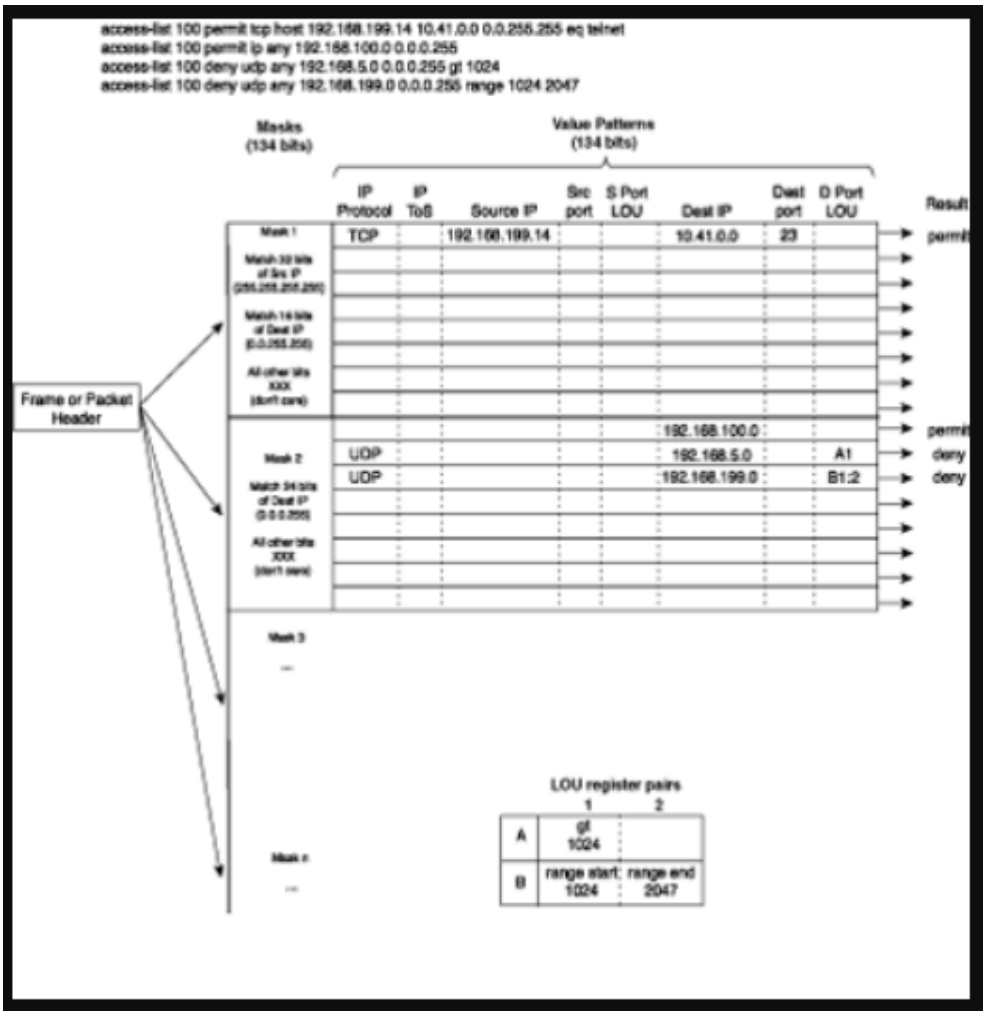


Table: TCAM

14. Which command use of Show MAC TABLE?

The below Command use for show MAC Table:

1. Switch(config)# mac address-table aging-time seconds
2. Switch(config)# mac address-table static mac-address vlan vlan-id interface type mod/num