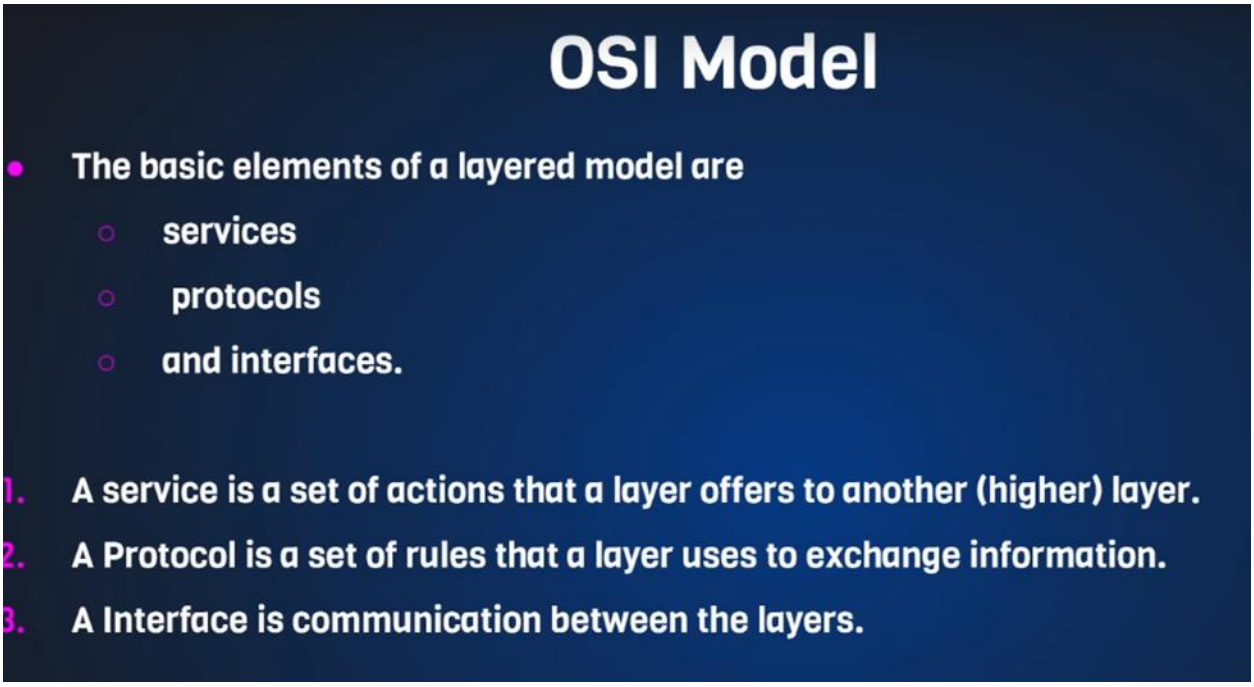
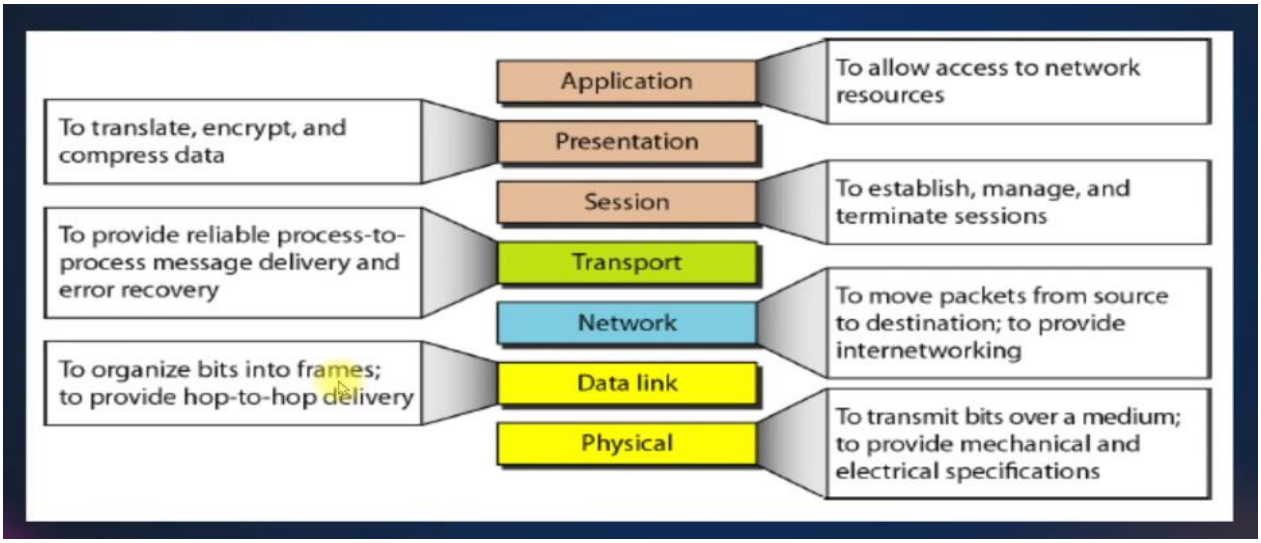
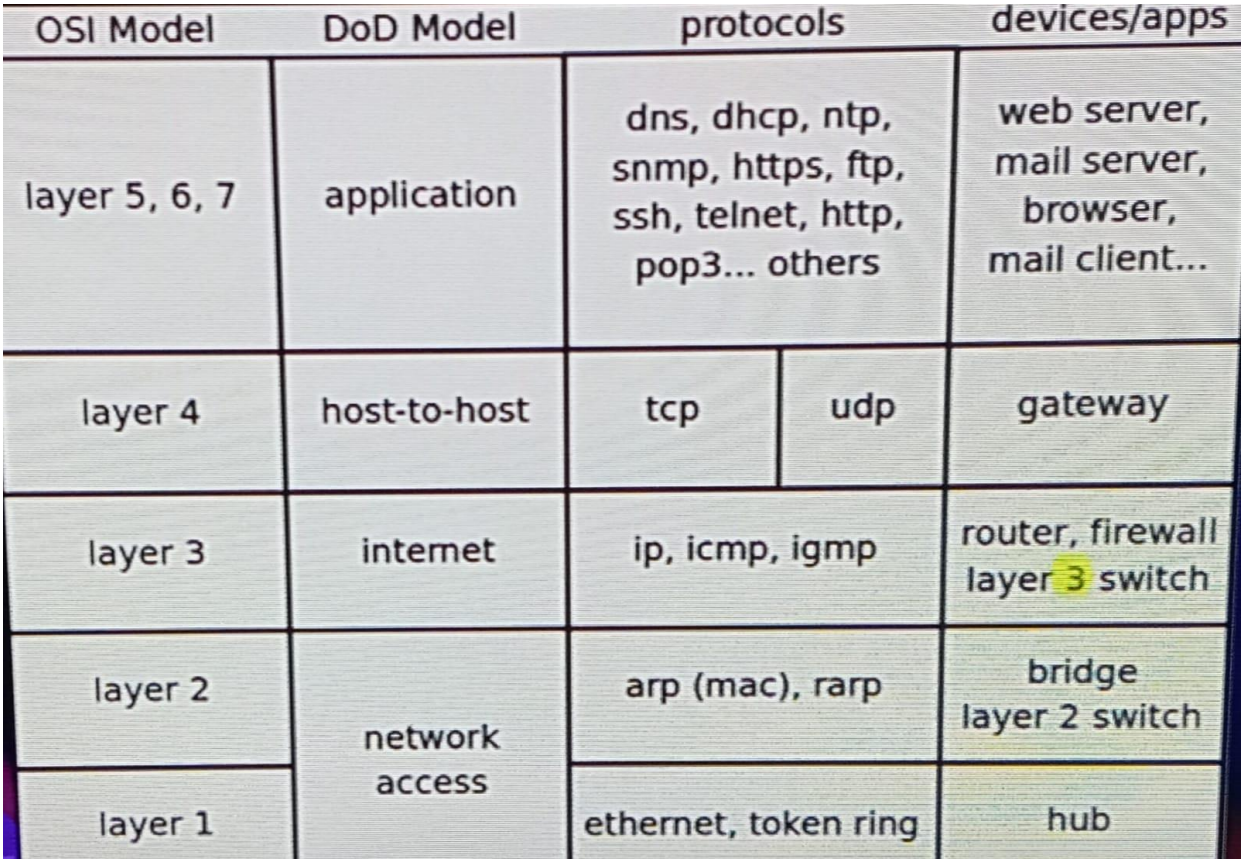
A set of standard follow by everyone in computer networking, ISO (International organization of standard) has developed this standard



OSI – (Open system Interconnection) model is a seven layer architecture developed in 1984





OSI Model	DoD Model	protocols		devices/apps
layer 5, 6, 7	application	dns, dhcp, ntp, snmp, https, ftp, ssh, telnet, http, pop3... others		web server, mail server, browser, mail client...
layer 4	host-to-host	tcp	udp	gateway
layer 3	internet	ip, icmp, igmp		router, firewall layer 3 switch
layer 2	network access	arp (mac), rarp		bridge layer 2 switch
layer 1		ethernet, token ring		hub

VLAN (VIRTUAL LAN)

Suppose we need 5 local area network with few devices in each local area network, so we need 5 switches to create such scenario. If it established with a single switch is called VLAN

In this scenario I am going to create 3 virtual local area network that is 3 vlan (yellow, blue, green)

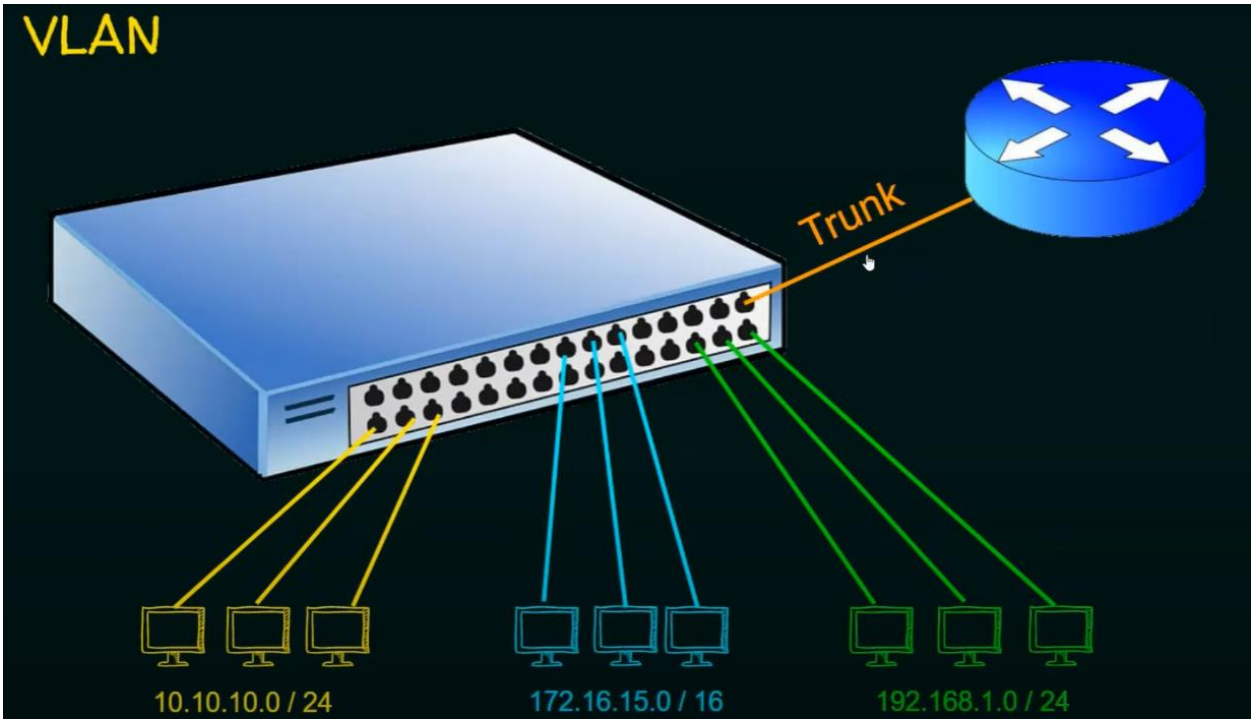
which have ip of 10.10.10.0/24 (yellow vlan) → /24 represent the subnet →

- will decide that ip address range,
- at what ip it will start & how many ip address do you get it and
- what will be the network and broadcast address

ex:-
255.255.255.0
10.10.10.0 => network ip
10.10.10.1 _____ …….. Total ip we get 254 we can assign it
10.10.10.254
10.10.10.255 => broad cost ip
Similarly we assign ip for blue and green

❖ Suppose device 1 in yellow vlan wants to send some packet, only another 2 devices in yellow vlan can receive similarly for blue and green vlan

- Yellow vlan 10.10.10.1 send broadcast only that vlan will recive this broadcast. it will not disrupt with other 2 vlan



suppose yellow vlan device wants to communicate with blue vlan device both are in 2 different network then router will come into the picture I am bringing the router connecting it to one of the freely available ports and this port is carry the traffic of all the vlan this port is called trunk port

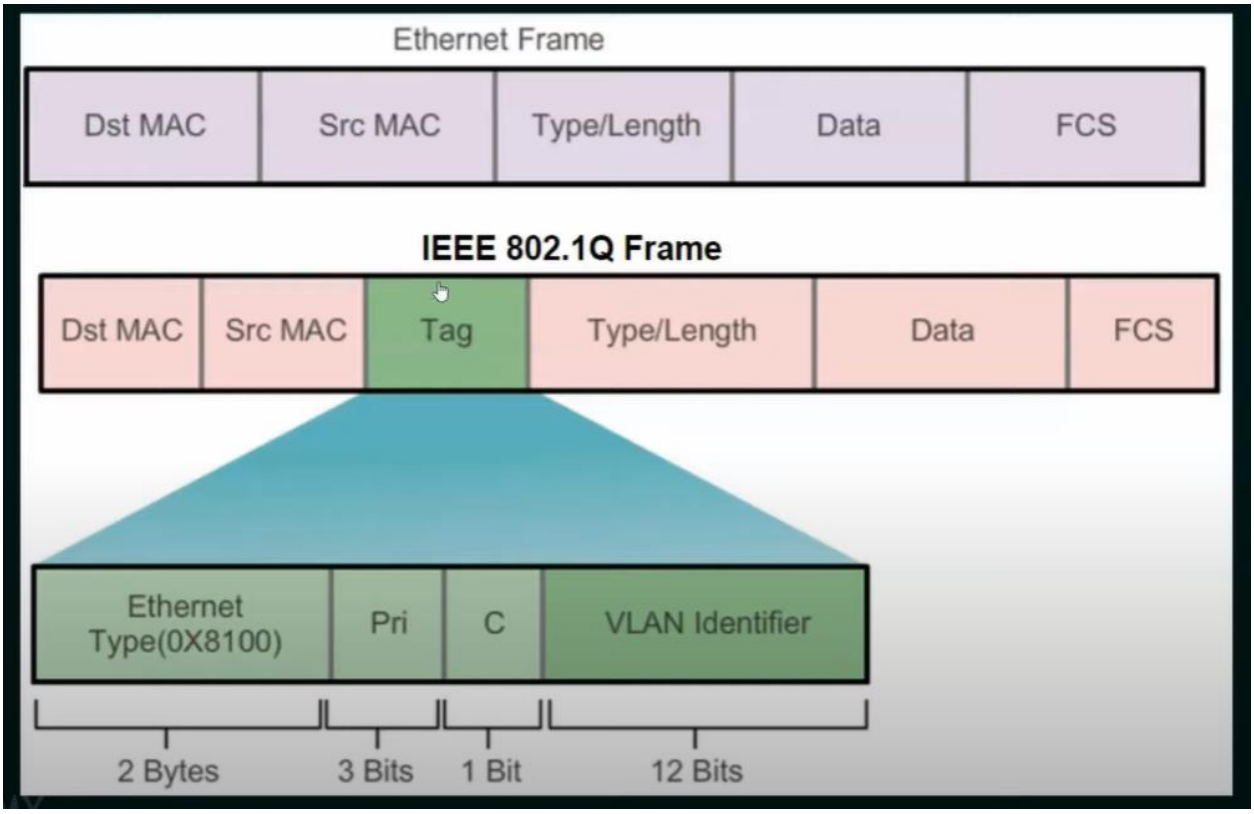
VLAN:----
* vlan is a logical partition of a layer 2 network (In a single switch we are creating 3 vlan)
* each vlan is a broadcast domain, usually with its own IP network (Yellow vlan 10.10.10.1 send broadcast only that vlan will receive this broadcast)
* The partitioning of the layer 2 network takes place inside a layer2 device, usually via a switch.

BENEFITS OF VLAN:-
Security
Cost reduction
Shrink broadcast domain

Types of VLAN: -
Data VLAN
Default VLAN
Native VLAN
Management VLAN
Voice VLAN

VLAN FRAME TAGGING:-

Dst MAC- destination mac Src MAC – source mac address FCS- frame check sequence (error detection potion) between Dst MAC and Src MAC we have tag this tag only responsible for identifying the vlan. This tagging is done by a switch whenever a host sends a packet the switch will receive that packet and it puts a vlan tag to its frame so that whenever the frame is passed through multiple switches every switch can recognize to which vlan it has to send and this tagging is called as ieee 802.1 cure frame tagging



- It is used to properly transmit multiple VLAN frames through a trunk link.

Suppose yellow VLAN device want to transfer data to Blue VLAN device then switch will put the VLAN tag to the Ethernet Frame and that tag frame is send to the trunk and router receive it and then router forward this to blue VLAN device

- Different tagging protocols exist, IEEE 802.1Q is a very popular

What happen with VLAN: ----

- They are good. To some extent
- In some cases it's not sufficient:

1) Limited vlanID
2) The use of STP protocol → only one link is active
3) Handling many ARP table

- Some cases: Datacenter,ISP

Introducing VxLAN

- Virtual eXtensible Local Area Network (VXLAN)
- RFC7348
- Using UDP protocol
- Terminology:
  - **VNI**: VXLAN Network Identifier (or VXLAN Segment ID)
  - **VTEP**: VXLAN Tunnel End Point. An entity that originates and/or terminates VXLAN tunnels
  - **VXLAN Segment**: VXLAN Layer 2 overlay network over which VMs communicate
  - **VXLAN Gateway**: an entity that forwards traffic between VXLANs

VXLAN Benefit : ---

- Not bounded on layer 2 devices
- More scalable (more IDs). Vlan id only 4096
- No limited by STP
- Suitable for multi tenant environment (cloud provider)
- Eliminate problem: Inadequate Table Sizes at ToR Switch