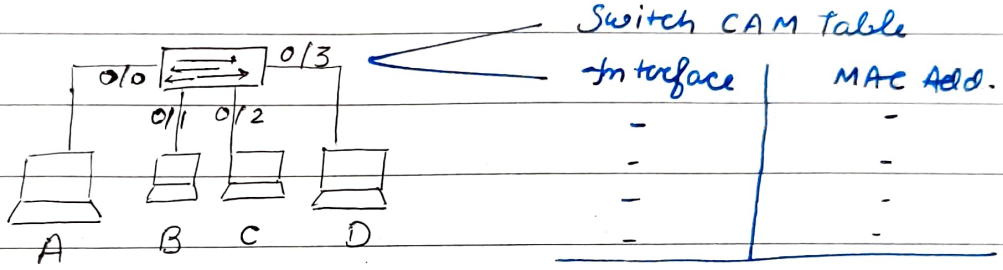
SWITCHING (L2)

Functions of Switches:

① Address Learning:

For keeping MAC addresses, Switches use MAC filter tables (CAM Tables).



② Forwarding Decisions:

Again Switch uses CAM to choose appropriate exit interface.

③ Loop Avoidance:

Switches use Spanning Tree Protocol (STP) for detecting loops.

Advantage of Switches:

- Hardware Based Bridging (ASICs)
- Wire Speed
- Low cost & latency

Port Security:

Physically avoiding suspected MAC addresses from connecting.

→ Ports should not be 'DYNAMICALLY' accessible.

PROTECT : Drops packets with unknown source MAC address

RESTRICT: Drops packets and send SNMP trap

SHUTDOWN: (Default) Puts interface into 'error-disable' state immediately.

VLAN Range * 1 to 1005 (NORMAL)

—— x —— * 1006 to 4094 (EXTENDED)

1002 - 1005 (reserved for FDDI & token Ring)

VLANS

- Used to divide switch.
- Virtual LANs (Separation of Network)

NEED & BENEFITS

① Broadcast Control: Increases no of broadcast domains while decreasing their size.

② Security: We can create multiple broadcast groups. We can apply restrictions on H/W addresses, routers, protocols & applicatio

③ Flexibility & Scalability ✓

TYPES OF PORTS

A> ACCESS PORTS: It belongs to and carries the traffic of only 1 VLAN. There is no tagging at all.

B> VOICE ACCESS PORT: A switch allows you to add a second VLAN to access port for VOICE TRAFFIC. It is also called an 'aux' VLAN.

It allows us to connect both a phone & PC device to one switch port but still have each device in different VLAN.

classmate
Date
Page

C > TRUNK PORT: carries traffic of multiple VLAN.

→ Tag - Untag: switches will tag the traffic if it (client) is on different switch & different VLAN.

Native VLAN: VLAN 1 is always native by default. Any untagged traffic will go to & throu. of the Native VLAN.

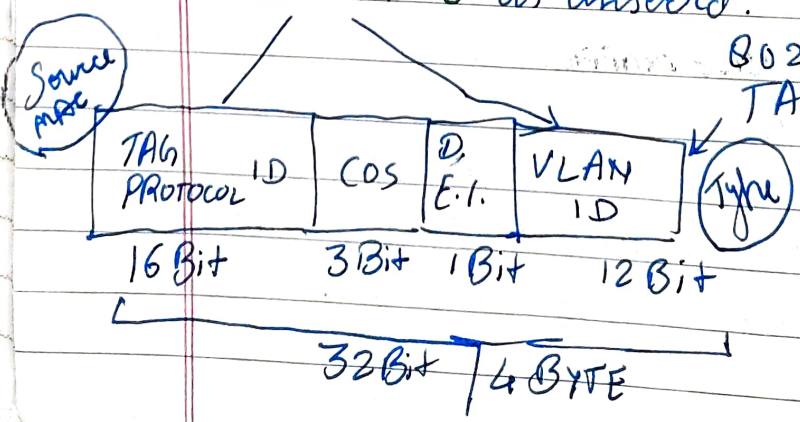
UNTAGGED = NATIVE

PROTOCOLS FOR VLAN IDENTIFICATION:

1. ISL (Inter Switch Linking): This will allow VLANs to be multiplexe over a trunk link through external encapsulation method.

- ISL is proprietary to CISCO but CISCO has moved towards using only 802.1q.

2. IEEE 802.1q: In this a field is inserted into the frame for identificatio 12 bit VLAN ID is inserted.



classmate
Date
Page

ROUTING BETWEEN VLAN:

Method 1 (ROAS) Router on a stick:
In this we create sub interfaces for every VLAN (one for each VLAN)

Method 2 (SVI) Switched Virtual Interface
In this, we use a L3 switch to do the routing.

Trunking modes:
① Access: non-trunking mode
② Dynamic Auto: If neighbor sends DTP, it will become trunk.
③ Dynamic Desirable: Actively send DTP to his neighbor requesting to trunk.
④ Trunk: permanent trunk mode.

* No Negotiate: Prevents DTP packets, you can use this only if ports are configured as 'access' or 'trunk'.

- DTP is Cisco's proprietary to automatic trunk initiation.

STP

NEED:

- Prevention of Network Loops.
  - Broadcast storm
  - Multiple frame copies
  - MAC table thrashing

Root Bridge: Switch with lowest Bridge ID.
LOWER = BETTER

BPDU
- Bridge Protocol Data Units
- Used to exchange data / information between switches.

COST		
	10 Mb/s	100
	100 Mb/s	19
	1 Gb/s	4
	10 Gb/s	2

TYPES OF PORTS:

① ROOT PORT: Lowest path cost to the ROOT
↓ (if equal)
Bandwidth
↓ (if equal)
LOWEST PORT NUMBER

(2) DESIGNATED PORT: determined to have best cost to get to the other ports on the network.

(3) FORWARDING: ✓ forwarding frames

(4) BLOCKED: X No info. transfer.

• ALTERNATE • BACKUP • NON DESIGNATED

STATUS OF PORTS (STP)

A> DISABLED: Not in use / Shutdown (RSTP)

B> BLOCKING: Won't forward frames. (STP)

C> LISTENING: prepares to forward frames without populating MAC add. table (STP)

D> LEARNING: populates MAC a. table. (RSTP) + (STP)

E> FORWARDING: things are ✓. (RSTP) + (STP)

***

CONVERGENCE: Occurs when all ports are in either FORWARDING or BLOCKING mode. No data is forwarded until convergence is completed.

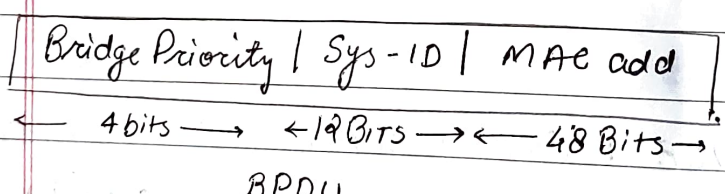
***

Date
Page

TYPES OF STPs:

① CST (802.1d): After the election of ROOT, the elected bridge will become ROOT of all VLAN, Network & bridges.
- All bridge will create a single path to ROOT.

② PVST+(CISCO Default): Per VLAN spanning tree creates a per VLAN STP instance.
- Eat up much memory resources than STP.
- STP tree will be optimized for the traffic of each VLAN.
- To allow PVST+ to operate, there is a field inserted into BPDU to accomodate extended system ID.



③ RSTP (802.1w): • Reduce the convergence time.
- The resource are used much more than CST but less than PVST+.
- Iteration of BPDU exchange enhanced.

④ Rapid PVST+ (CISCO's RSTP): Creates instance per VLAN but at a speed of 802.1w

Date
Page

3) MSTP (802.1s): Multiple Spanning tree protocol gives us the same fast convergence as RSTP but reduce the number of STP instances.

- Allow us to create VLAN sets & a STP on the top of another STP.

PROCESS OF STP: R. / PVST+ R. →

→ ELECTING ROOT by bridge ID.

→ Determine ROOT PORTS by finding lowest path cost to the ROOT Bridge.

→ Find DESIGNATED PORTS by looking at Bridge IDs.

Bridge ID
↓ COST
MAC Address
} for ROOT PORTS DESIGNATED

PRIORITIES
↓
LOWER PORT NUMBER

STP FAILURE CONSEQUENCE :

A > Bandwidth consumption / load

B > MAC table is unusable

C > 100% CPU use will lead to failure.

PORT FAST: If some important devices like server can't wait for STP to happen and we are sure that they won't create a loop in network we can leave those ports to forwarding state forever using PORT FAST.

BPDU Guard: If a port that has PORTFAST enabled, recives any BPDU on the port, it will place that port on error disabled state (for prevention) So configuring BPDU-Guard is a must.

- Sh spanning-tree summary
- Spanning-tree vlan _ priority 102
  root pri/sec.
- Spanning-tree mode rapid-PVST

- LABS + THEORY
- RPVST+

ETHERCHANNEL

NEED:

* Redundancy.
* Resiliency.

- a port-channel technology.
- used to aggregate links.

IEEE 802.3ad LACP: → Automatic creation of Ether Channel.

Cisco PAgP :

USE:

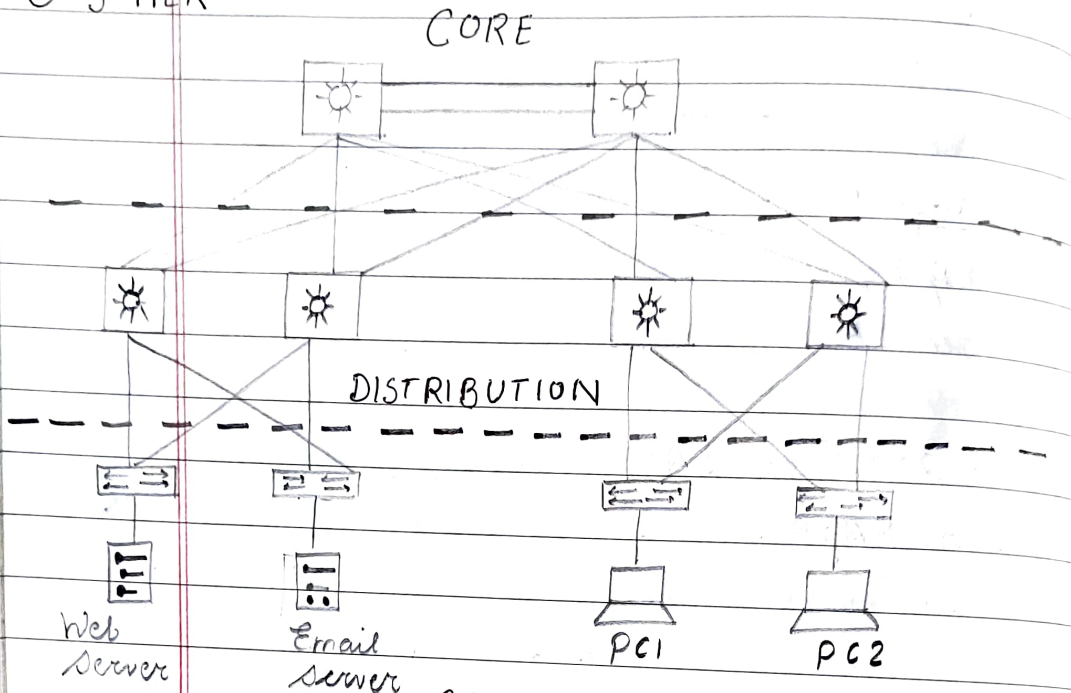
A> Port Channeling: Combining 2-8 fast Ethernet or 2 Giga Ethernet port into 1 logical link.

PAgP	LACP
Auto / Desirable	Active / Passive
→ 8 CHANNEL TOGETHER	→ 16 CHANNEL TOGETHER

- 1 LAB.

NETWORK TOPOLOGY ARCHITECTURE

① 3-TIER



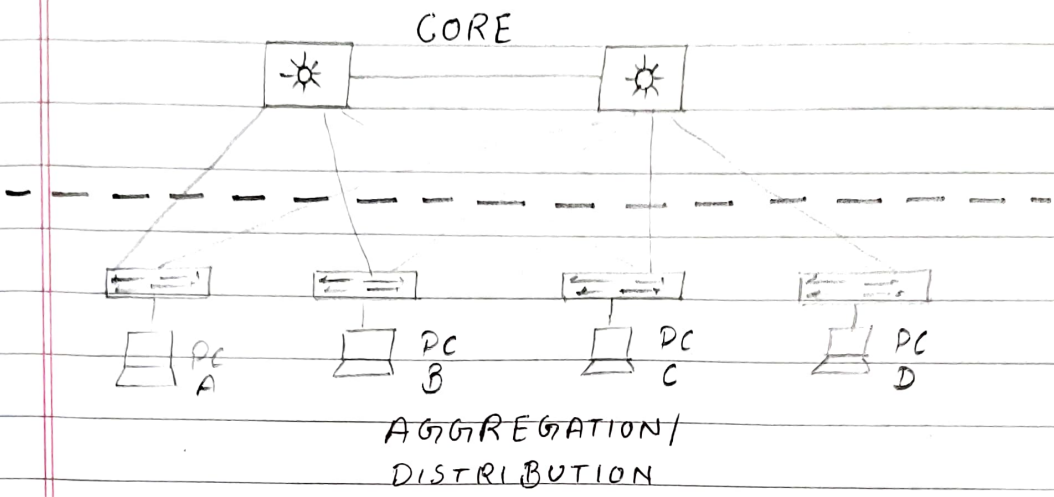
CORE:
- Core of the network.
- Never should slow down.
- No workgroup support & access.
- Avoid expanding CORE.
- High Reliability and high speed.

DISTRIBUTION:
- Aggregation layer
- Routing, Packet Filtering
- NAT, firewalls
- Routing between VLANs.

ACCESS:
- User & Workgroup access.
- Desktop layer, QoS, Device connectivity.

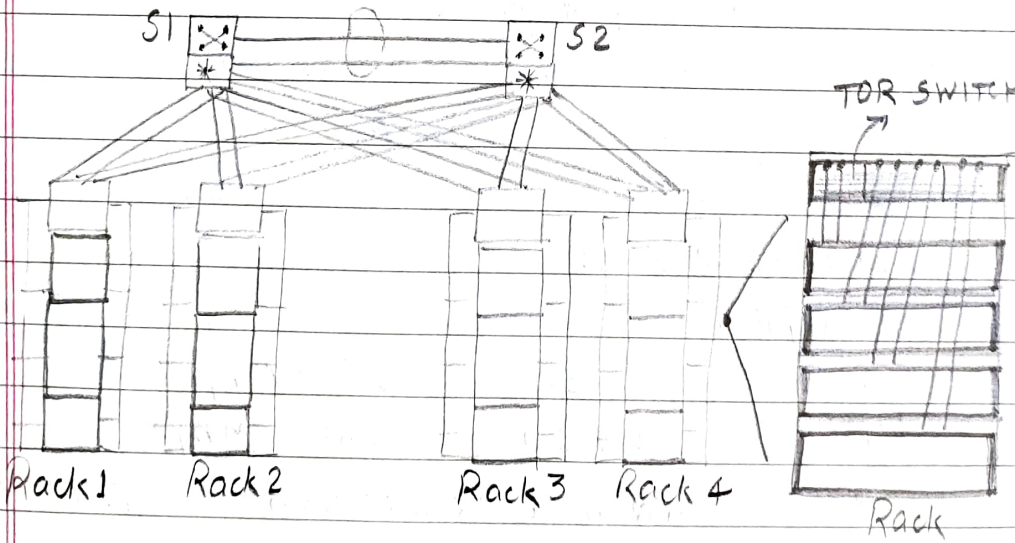
classmate
Date
Page

(ii) 2TIER (COLLAPSED CORE)



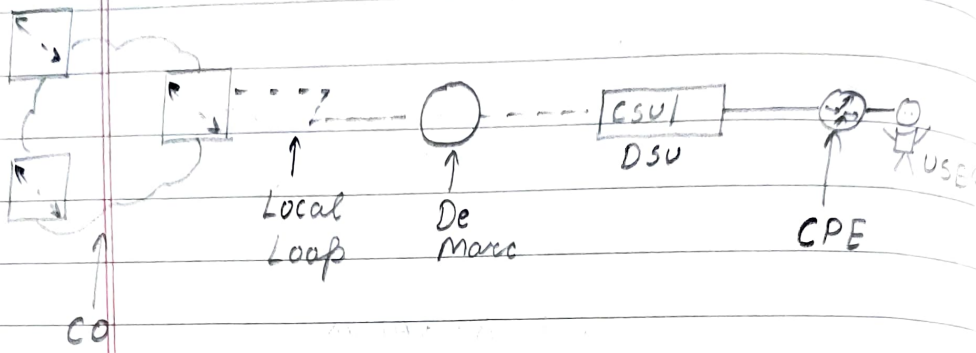
- less expansive, greater for small organization
- max performance & user availability.
- economical & functional for CAN.

(iii) SPINE - LEAF



- created for data centres.
- TOR (Top of Rack design). → Leaf
- Spine Switches (S1 & S2).
- Redundancy & speed ✓

(iv) WAN: • Large geographic area.
• require to connect local sites.



CPE: Customer Premises equipment

CSU/DSU: Channel / Data Service Unit used to connect a DTE to a digital circuit like a T1/T3 line.
CSU/DSU provides clocking of the line to the router.

Demarcation Point: Spot where ISP is responsibility begins.

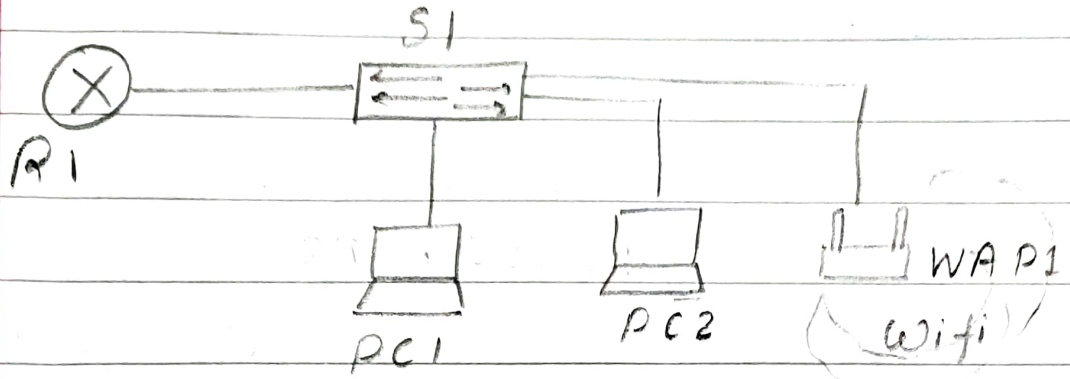
CO: Central office connects user's network to provider's network.

WAN Connections:

DS0/E0		
T1	24 DS0	1.544 Mbps
E1	30 DS0	2.048 Mbps
T3	28 DS1 OR 672 DS0	44.736 Mbps
OC3	155 Mbps	
OC12	622.08 Mbps	
OC48	2488.32 Mbps	

Fiber

(V) SOHO : Small office / Home office



(VI) On Premise & Cloud

↓ ↑

Straight Through :→ Same Devices
Cross over : ↘ Diff. Devices

CABLE ISSUES:

- Miswire
- Dead Wire
- Length
- Interference
- Exposure

T568A | T568B

gGoBbO brBR

oOgBbG brB

RUNT: Frames smaller than 64 Bytes
GIANTS: Frames larger than 1518 Bytes
CRC: Frames where CRC/FCS was wrong

PoE:
- Central Power
- Central Backup
- Network switch
- Power Negotiation occurs (802.3)

802.3 AF → 15.4 W.
802.3 AT → 30W.
802.3 BT T3 → 60W.
802.3 BT T4 → 100 W.

- show power inline -

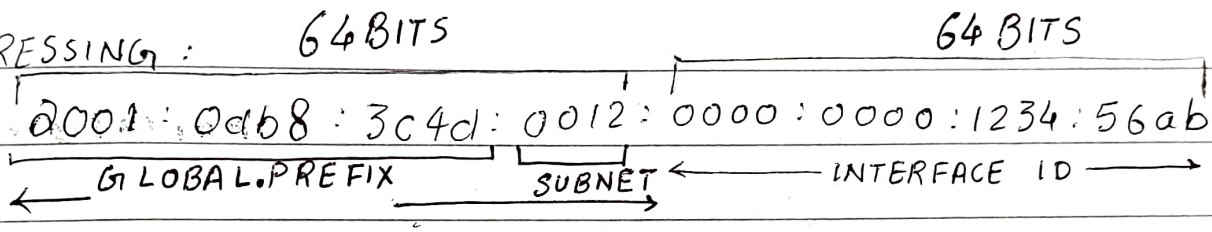
* non data wires (4-5, 7-8)

IPV6:

BENIFITS • 3.4×10^{38} Addresses

- lighter than IPV4 (half the fields)
- faster processing speeds
- lookup happens at light speed.
- IPV6 has no broadcasts. IPV6 has anycast for same problem.

ADDRESSING:



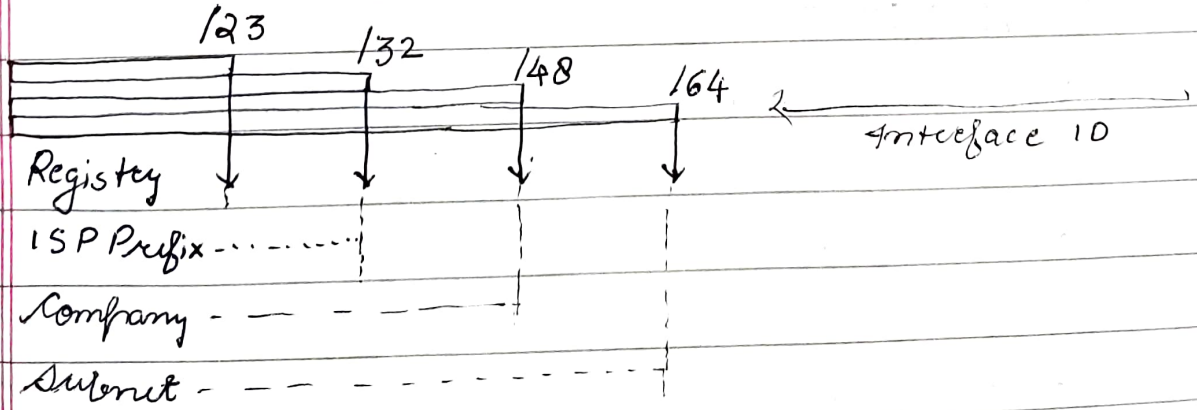
TYPES OF IPV6 ADDRESSES:

① UNICAST: Delivered to a single interface.

- Global Unicast address
- Link-Local address
- Unique-Local address

A) Global Unicast: public routable address

2000 ::/3



B> LINK LOCAL ADDRESS :

- These are like APIPA of IPV4.
- non-routable but can share & access files locally.

FE80 :: /10

C> UNIQUE LOCAL ADDRESS:

- Also non-routable.
- nearly global Unique.
  do almost exactly like PRIVATE ADD. of IPV4.

FC00 :: /7

(II) MULTCAST

- Used for multicasting.
- always start with FF.

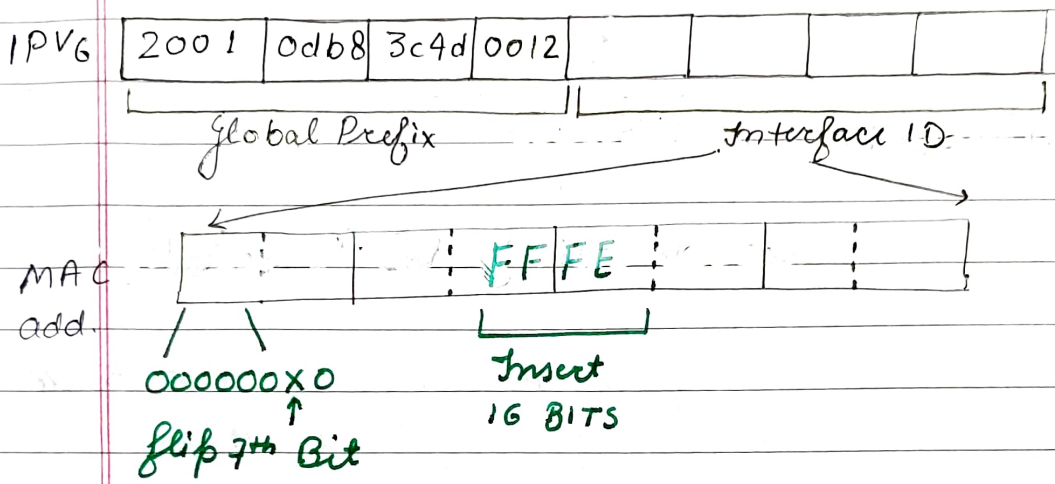
FF00 :: /8

(III) ANYCAST

- Identifies multiple interface on multiple device.
- typically only configured on routers, never on hosts.
- IETF reserved top 128 addresses for each /64 for use with anycast.

IPV6 address assignment :

(1) STATELESS AUTOCONF. (EUI-64)



Example : MAC = 0b 34 : ba 12 : 1234

0b = 00001011

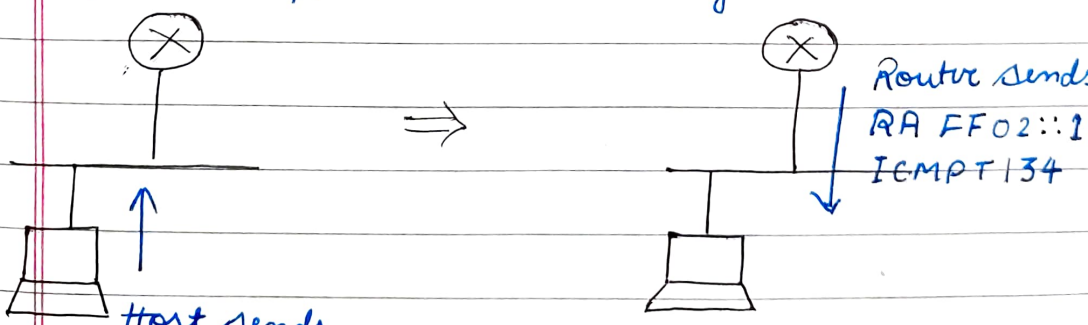
↓

0

flip = 00001001 → 0934 : ba12 : 1234

IPV6 after EUI-64 2001:0db8:3c4d:0012:0934:baff:fe12:1234

This process happens automatically :



STEP A

STEP B

(11) DHCP V6 (STATEFULL):

- It works same as IPV4 but the process differs:

→ In IPV4, upon booting client used to send DHCP DISCOVER message. But because in IPV6, RS & RA happens first,

If DHCP V6 is on the network is available, the RA will come back to the client and tell that DHCP is available to use.

→ If a router is not found, client will respond by sending DHCP solicit message which is actually a multicast with destination FF02::1:2 & calls out all DHCP agents both server & relay.

PRIVATE IP Address Class A → 10.0.0.0 / 8

B → 172.16.0.0 / 172.31.255.255

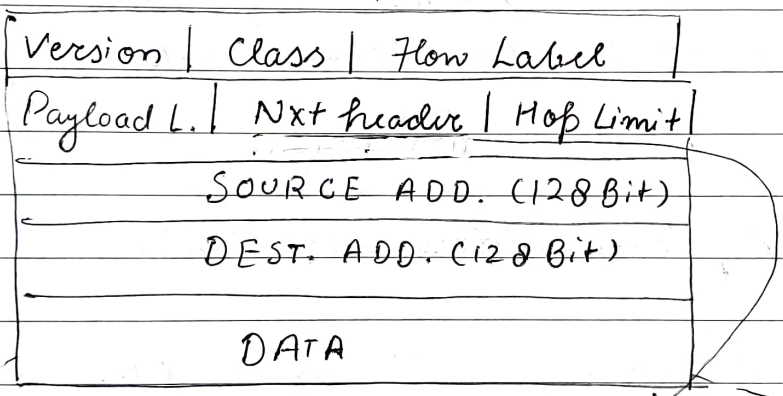
C → 192.168.0.0 / 16

Date

Page

ICMP V6 : • It is not a separate like in IPV4 Now ICMP is an integral part of IP header.

- By default, it prevents any fragmentation by using a process called 'path MTU discovery'.
- ICMP packet is identified by value 58 in the next header field of IPV6.



In ICMP → Nxt header = 58

DATA =

ICMPV6 TYPE	ICMPV6 CODE	CHECKSUM
ICMPV6 DATA		

ICMP V6

ICMP V6 CODE →

1	Destination Unreachable
128	Echo Request
129	Echo Reply
133 / 134	RS / RA
135	Neighbor Solicitation
136	Neighbor Adv.

Neighbor Discovery Protocol (NDP):

- NDP is ARP of IPV6.
- Process is achieved via a multicast address called solicited Node Address.

FF02:0:0:0:0:1:FF__:____ /104

Last part of IPV6 is added.

- When this address is queried, host will send its L2 address back.

DAD (Duplicate Address Detection):

- DAD is a function of NS/NA.