Module 5 (Chap 6 & 7)

PAGE No.
DATE / /

Designing an IP Addressing Plan.

Introduction to IPV6

Routing Protocol Features

Routing Protocols for the Enterprise

Routing Protocol Deployment

Route Redistribution.

Route Filtering

Redistributing and Filtering with BGP.

Route Summarization.

Private and Public IPV4 Addresses.

Private IP addresses

→ Reserved IP addresses that are used internally within a company's network and not on the internet

→ When sending anything on the internet, private IP addresses must be mapped to a company's external registered address.

→ RFC 1918, Address allocation for Private Internets, defines the Private IP addresses as follows:

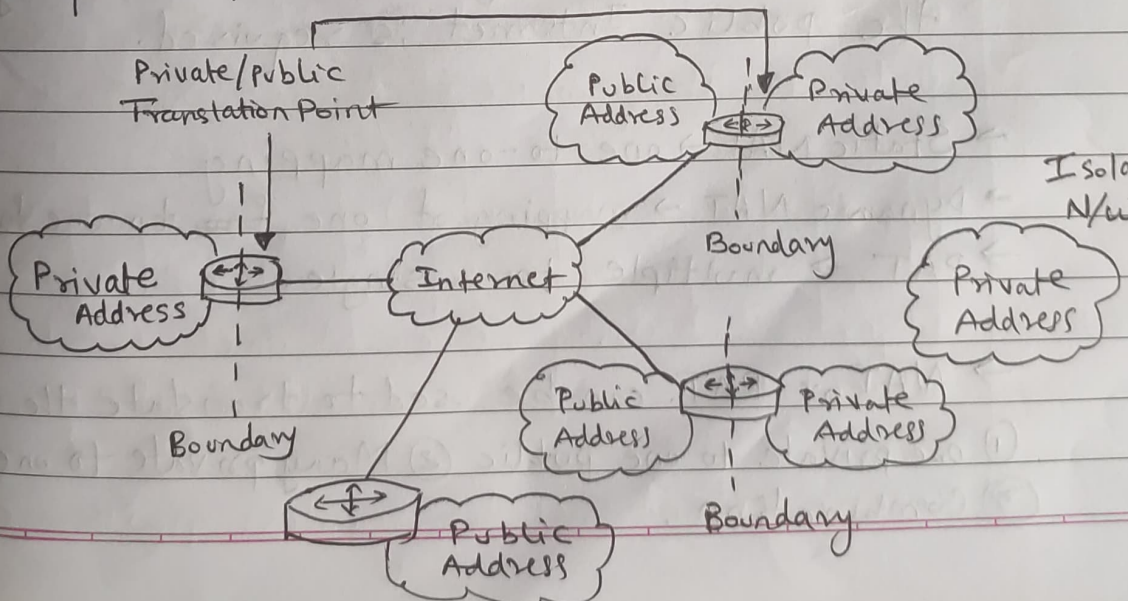
- 10.0.0.0 to 10.255.255.255
- 172.16.0.0 to 172.31.255.255
- 19.168.0.0 to 192.168.255.255

→ The remaining addresses are public addressed.

Public IP addresses

→ Public IP address can be accessed over the internet

→ They are provided for external communication



(*) Selection Criteria

→ There are a very few public IP addresses currently available, hence ISPs can assign only a subset of class C addresses to their customers.

→ Hence, number of public IP addresses assigned to an organization is very less.

→ Solution is to use Private IP addressess within the internal n/w and translate these to public addresses when Internet connectivity is required.

(*) Interconnecting Private & Public Addresses

→ When private addresses are used in a network for addressing and this network must be connected to internet, Network Address Translation (NAT) or Port Address Translation (PAT) must be used for translation.

→ NAT or PAT is required if accessibility to the public Internet is required.

→ Static NAT → one-to-one mapping

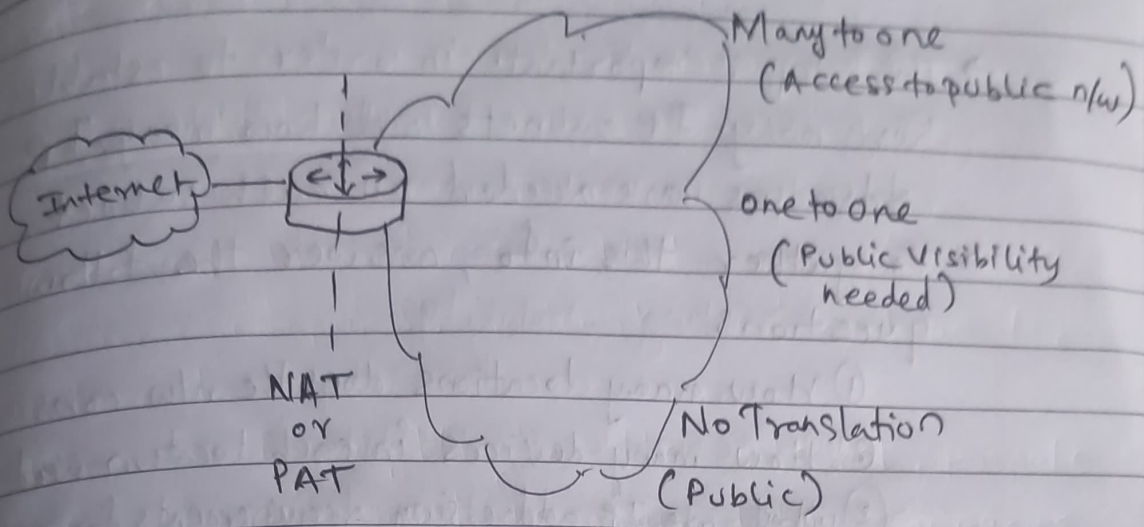
→ Dynamic NAT → mapping of one to one from many.

→ PAT → multiple to a single.

→ NAT or PAT can be used to translate the following:

① one private to one public ② Many private to one public ③ Combination.

Private to Public Address Translation.



Usage of Private and Public Addresses in an Enterprise N/w.

Private IP addresses:
- → Enterprise Campus
- → Enterprise Branch
- → Enterprise Teleworker.

Public IP addresses.
- → Enterprise Edge
  - Internet connectivity Module
  - E-commerce Module
  - Remote Access and VPN module
- → Enterprise Data Center.

PAGE No.
DATE / /

(*) Determining Size of the n/w.

→ This step is important in order to establish how many IP subnets and how many IP addresses are needed on each subnet.
→ To gather this info, answer the following questions
① How many locations does the n/w consist of?
② How many devices in each location need addresses?
③ What are IP addressing requirements for each local?
④ What subnet size is appropriate?

(*) Determining N/w topology.

→ Acquiring a general picture of n/w topology helps determine the correct information to gather about n/w size and its relation to IP addressing.
→ This helps the designer to determine the number of locations, location types and their correlation.

(*) Size of individual locations

→ N/w size in terms of IP addressing plan relates to the number of devices and interfaces that need an IP address.
→ The designer determines the approximate number of workstations, servers, router, interfaces, Layer-3 interfaces, etc. at each location which gives a minimum overall no. of IP addresses needed.
→ Reserve IP addresses for seamless growth are kept.

⑥ Planning the IP Addressing Hierarchy

→ IP address uses hierachical addressing scheme.
→ A single IP address can contain information about the network, its sub-network and ultimately the host.
→ The network and the sub-network part is the prefix part of an IP address.
→ The router has to only know how to reach the next hop; it does not ~~know~~ have to know the details of how to reach an end node that is not local.
→ Routers use the prefix to determine the path for a destination address not local.
→ host part is used to reach local hosts.

⑦ Route Summarization.

→ One route in routing table represents many other routes
→ Route summarization reduces the routing update traffic and reduces number of routes in routing table and overall router overhead in the router receiving the routes.
→ In a hierarchical network design, effective use of route summarization can limit the impact of topology changes to the routers in one section of the network.
→ eg: (Page 416 ciscobook.pdf)

Side NoTE : Go through CIDR

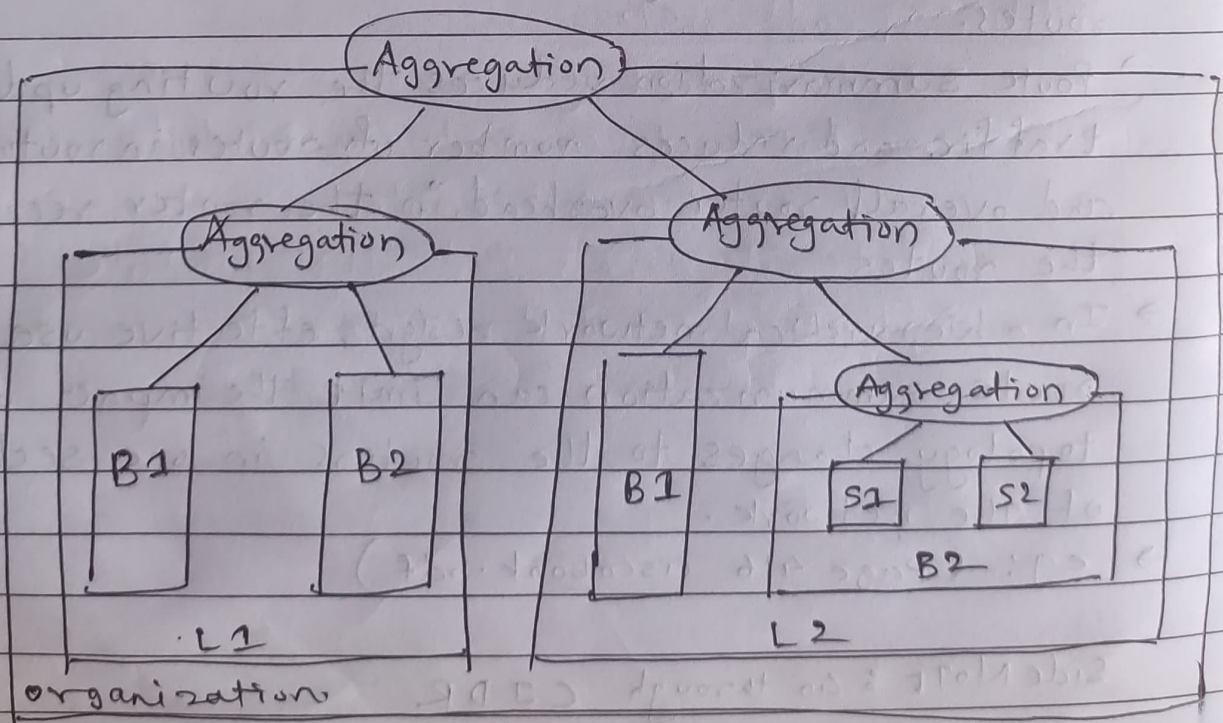
PAGE No.
DATE / /

(*) Benefits of Hierarchical Addressing.

→ Decreases Burden on Routers
→ Reduces the size of Routing Table
→ Helps in Route Summarization.
→ Enhances network's overall
  (i) routing stability
  (ii) service availability
  (iii) network scalability.
→ Supports modular design.

(*) Summarization Groups.

→ To reduce routing overhead in a large nlw, a multilevel hierarchy might be required.
→ The depth of hierarchy depends on the network size and the size of the highest-level summarization group.



→ 3 levels of hierarchy:

① First Level: group of summarized subnets known as summarization groups (Location)

② Second Level: within first level summarization groups. (Location divided in buildings)

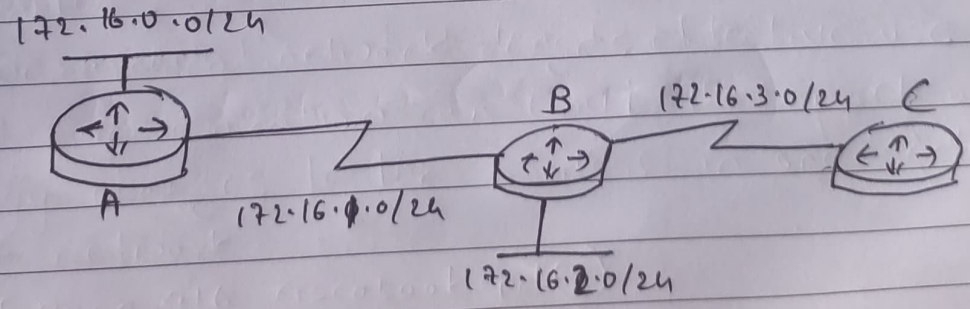
③ Third Level: within the second-level summarization group (Building divided in sections or floors)

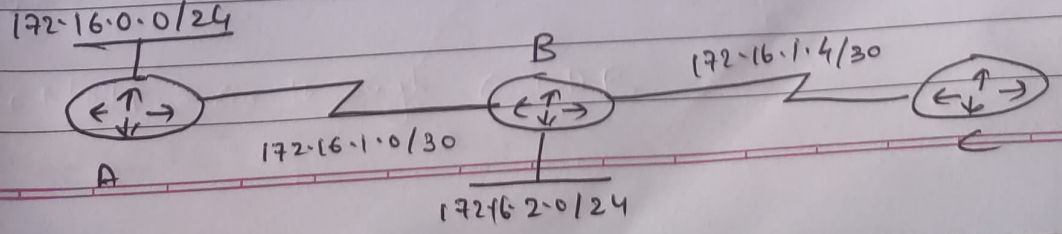
✱ Impacts of Poorly Designed IP Addressing.

→ Excess routing traffic consumes bandwidth
→ Increased Routing table recalculation.
→ Possibility of routing loops.

✱ Fixed & Variable length Subnet Masks.

FLSM: all subnet mask in a major n/w must be same.
VLSM: subnet masks within a n/w can be different.





→ To use VLSM, routing protocol must be classless.
→ Classful routing protocols permit only FLSM.

Classful and Classless Routing Protocols.

Static Versus Dynamic IP Address Assignment Methods.

Static IP Address Assignment.

→ Statically / Manually assigned to a system.
→ NA configures IP address, default gateway and name servers manually.
→ extra burden for the NA especially on large-scale n/w.

Dynamic IP Address Assignment.

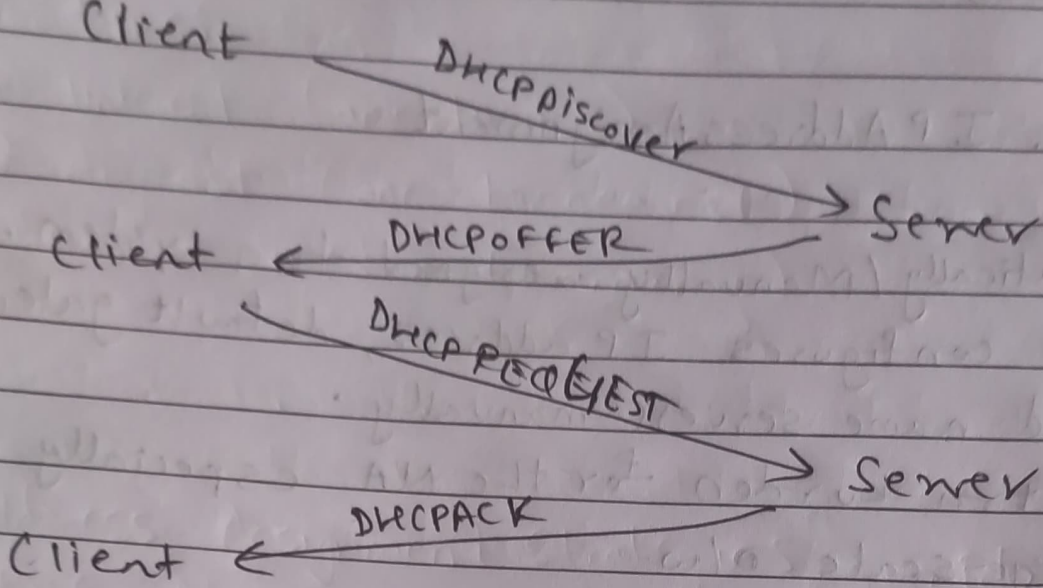
→ Dynamically assigned to the end system.
→ NA must set up a server to assign the addresses.
→ on that server, the NA defines the parameters to send to the host.
→ On the host, the administrator enables the host to acquire the address Dynamically.

④ When to use Static or Dynamic

Parameter	Static.	Dynamic
Node Type	Routers & switches	Enduserdevices (PCs)
No. of End Systems	< 30	> 30
Renumbering	No.	Yes
Address Tracking	easier	additional config.
High Availability	Yes	No
Security	Minor risk	Riskier.

⑤ Page (429) Ciscobook pdf

(*) Using DHCP to Assign IP Addresses



→ DHCP supports three possible address allocation mechanisms:

① Manual (specific MAC address)
② Automatic (permanent to a host)
③ Dynamic (limited time to a host)

(*) Static v/s Dynamic Name Resolution
(*) When to use Static or Dynamic Name Resolution
(*) Using DNS for Name Resolution
(*) DHCP & DNS server location in a N/W

(431 - 435) ciscobook.pdf.

IPV6 (Introduction)

→ developed to overcome limitations of the current IPv4

→ The basics of IPv6 are similar to those of IPv4 with slight variations

→ Features of IPv6.

1. Larger Address space : 128 bits.
2. Globally unique IP Addresses.
3. Site multihoming
4. Header format Efficiency.
5. Improved privacy & security
6. Increased mobility & multicast capabilities.
7. Flow labelling capabilities.

→ Format

x:x:x:x:x:x:x:x. (x: 16 bit Hexadecimal)

→ 2035:0001:2BC5:0000:0000:087C:0000:000A

→ 2035:1:2BC5::87C:0:A

Version (4)	Traffic Class (8)	Flow Label (20)
Payload length (16)	Next Header (8)	Hop Limit (8)
Source Address (128)		
Destination Address (128)		
Extension Headers		

(Stay Edu)

→ IPv6 Address Types. (Star Edu)

→ 3 types

(1) Unicast (one-to-one)
(2) Anycast (one-to-neavest)
(3) Multicast (one-to-many)

(4) Address Assignment Strategies } Star Edu.
(5) IPv6 Name Resolution

(8) IPv4 v/s IPv6

Characteristics	IPv4	IPv6
Address Length	32-bit	128-bit
Types of Addresses	Unicast, broadcast, multicast	Unicast, Anycast, multicast
Address Representation	Decimal	Hexadecimal.
Checksum	Not Available	Available
End-to-End connection integrity	Unachievable	achievable.
Fragmentation	it is done by sending and forwarding routes	is done by the sender.

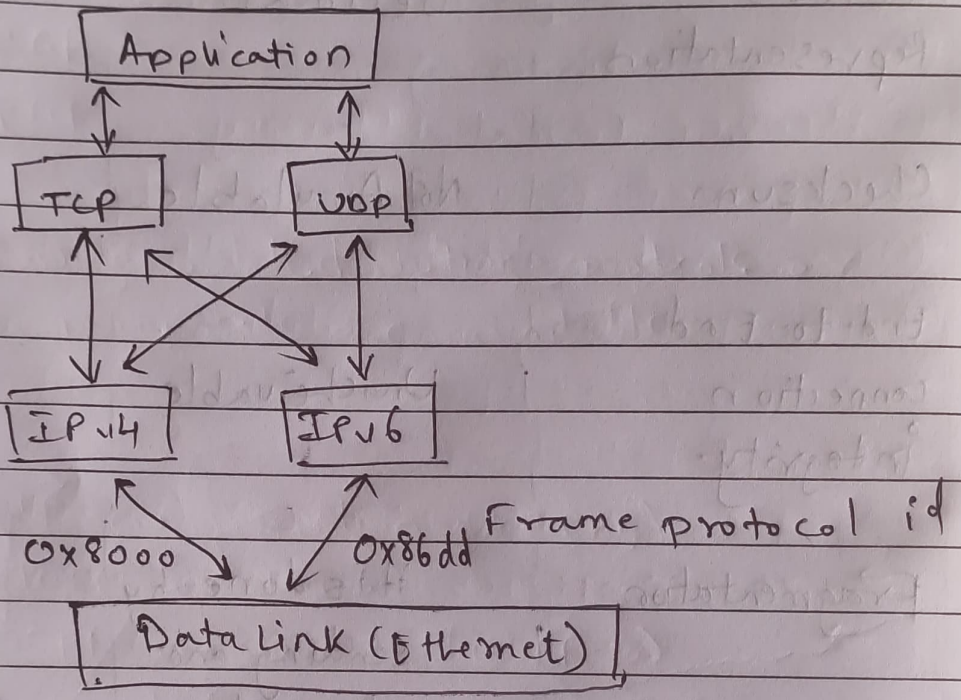
④ IPv4-to-IPv6 Transition:

→ The transition from IPv4 to IPv6 can be done by these 3 primary Mechanisms.

(i) Dual Stack

→ Both IPv4 & IPv6 stacks run on a system that communicate with both IPv6 and IPv4 devices.

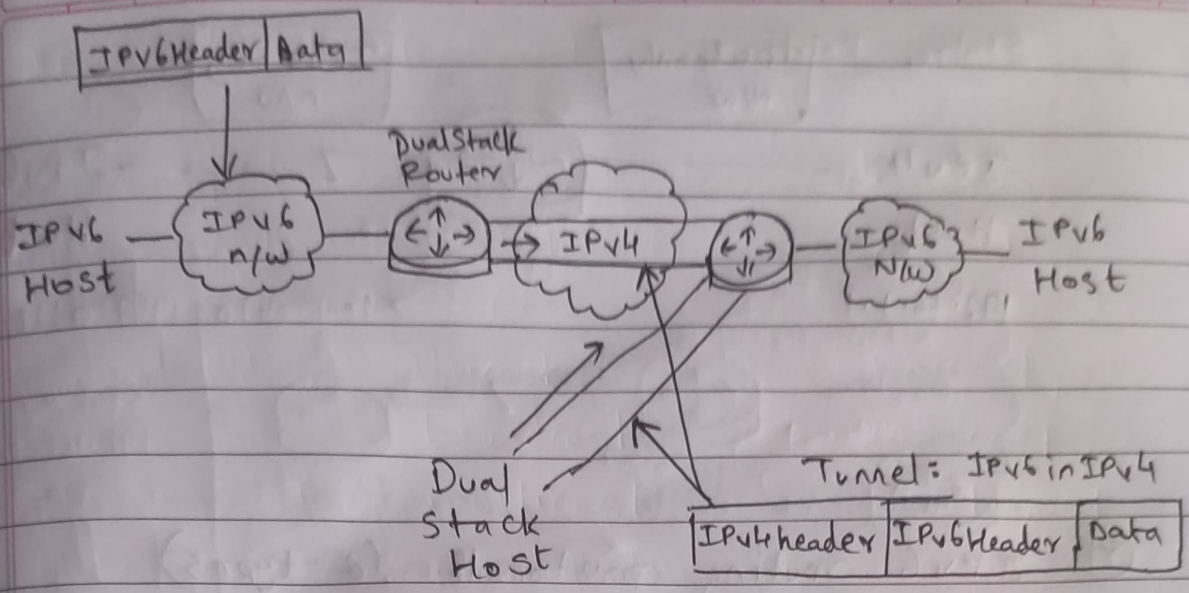
→ IP choice is based on name lookup and application prefere



(ii) Tunnelling Transition Mechanism.

→ The purpose of tunneling is to encapsulate packets of one type in packets of another.

→ When transitioning to IPv6, tunneling encapsulates IPv6 in IPv4 packets.



→ Tunnel can be established by following techniques.

(i) Manually configured

(ii) semi-automated

(iii) Automatic

→ By using tunneling mechanism, IPv6 n/w can communicate without having to upgrade IPv4 infrastructure between them.

(ii) Translation Transition Mechanism.

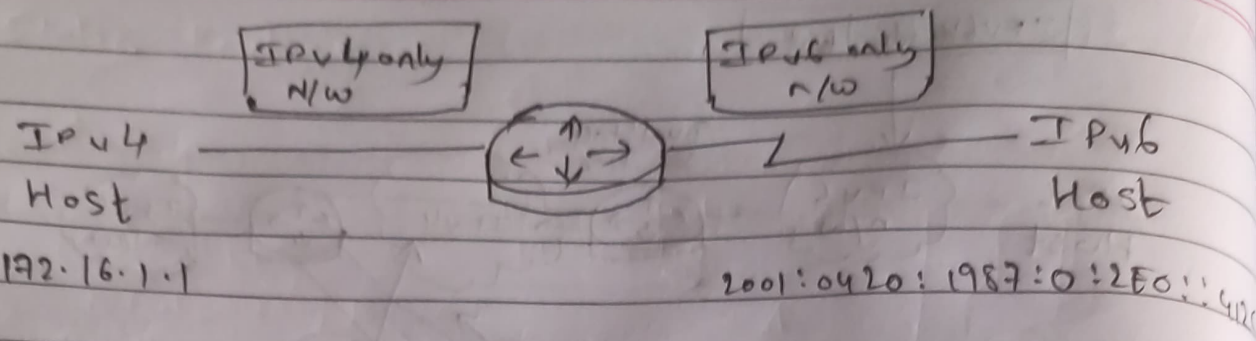
→ Dual Stack and Tunneling manage the interconnection of IPv6 domains.

→ For certain deployment scenarios, techniques are available for connecting IPv4-only nodes to IPv6-only nodes, using translation.

→ There are two types of translation techniques which are similar to NAT techniques

(i) NAT-PT (Network Address Translation - Protocol Translation)

(ii) DSTM (Dual-Stack Transition Mechanism)



(*) IPv6 routing protocols (2-types)

- IGP
- EGP

The following updated routing protocols or draft proposals are available:

IGP:

- RIP new generation (RIPng)
- EIGRP for IPv6
- OSPF version 3 (OSPF-3)
- Integrated IS-IS version 6 (IS-ISv6)

EGP:

- Multiprotocol extensions to BGP version 4 (BGP 4+)

(*) Routing Protocol Features.

→ Routing is the process of selecting a path for traffic in a network or between or across multiple networks.

→ A routing protocol specifies how routers communicate with each other, distributing information that enables them to select routes between any two nodes on a computer network.

→ There are many ways to characterize routing protocols, such as.

(i) Static v/s dynamic routing
(ii) Interior v/s exterior routing protocols
(iii) Distance vector v/s link state v/s hybrid
(iv) Flat v/s Hierarchical routing protocols

(*) Routing Protocols for the Enterprise

- EIGRP
- OSPF
- Integrated IS-IS
- BGP

(*) Routing Protocol Deployment (493 Fig 7-14) ciscobook

PAGE No.
DATE / /

Routing Protocol Metric.

→ A metric is a value (such as path length) that routing protocols use to measure paths to a destination.

→ Different protocols calculate routing metrics from different parameters and with different formulas.

EIGRP Metric calculation

→ It uses minimum blw & accumulated delay of the path toward the destination network.

$$\text{Metric} = (K1 * \text{blw}) + (K2 * \text{blw}) / (256 - \text{load}) + (K3 * \text{delay})$$

if $K5 \neq 0$, then:

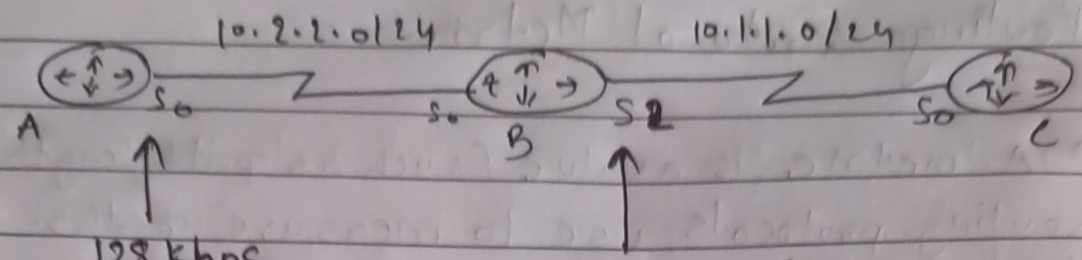
$$\text{Metric} = \text{Metric} * [K5 / (\text{reliability} + K4)]$$

K values are constant with default values $K1 = K3 = 1$ and $K2 = K4 = K5 = 0$, Therefore, formula is.

$$\boxed{\text{Metric} = \text{Blw} + \text{DELAY}}$$

(i) Blw is the smallest/slowest between source & destination. in kbps.
(ii) 10^7 is divided by that value and multiplied by 256
(iii) Delay is sum of delays in the path from source to destination in tens of microseconds multiplied by 256.

eg:



Metric that Router B advertises for 10.1.1.0/24 is

$B|w = (10^7 / 1544) * 256 = 1658031$

$Delay = (20000/10) * 256 = 512000$

$\therefore$ Metric = B|w + DELAY

= 2,170,031

Metric that Router A advertises for 10.1.1.0/24.

$B|w = (10^7 / 128) * 256 = 20,000,000$

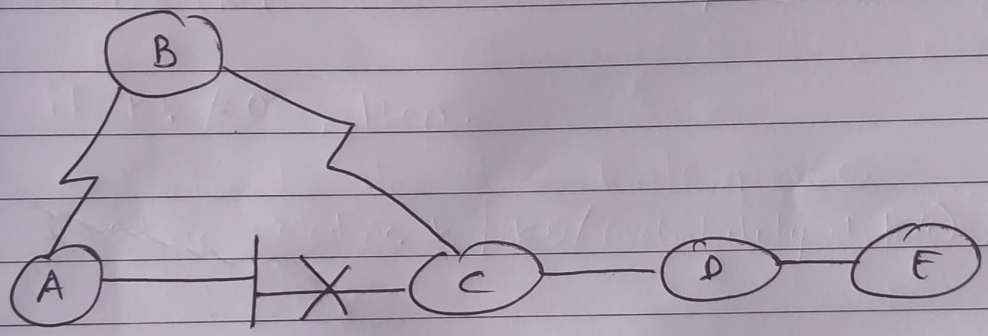
$Delay = ((20,000+20000)/10) * 256 = 1,024,000$

$\therefore$ Metric = B|w + Delay

= 21,024,000

Routing Protocol Convergence.

- Whenever change occurs in a n/w topology, all routers in that n/w must learn the new topology
- routers share info with each other, but they must calculate impact of topology change independently.
- Because they develop independent agreement on the new topology, they are said to converge on this consensus.
- The quicker the convergence, the more optimal the routing protocol.



Protocol	Convergence time to Router E
RIP	Hold-down + 1 or 2 update Intervals
IGRP	Hold-down + 1 or 2 update Intervals
EIGRP	Matter of seconds
OSPF	Matter of seconds.