DATE / /
PAGE

# Unit-I

## * Debugging Tools :-

→ ICMP uses two tools for debugging :-

(i) Ping
- we can send echo request & reply messages that check wheather the host / router is alive or running

(ii) Trace root
- is a tool that tracks the root taken by IP packet from source to destination
- → It records time taken by packet on each hop.
- → Uses ICMP messages & TTL values
  - zero ⇒ packet discarded
  - one ⇒ message produced by Router 1
  - Two ⇒ Router 2

## * Trace Root :-

e.g, A wants to send a packet to B. Bet^n A & B three routers exists

**Case 1 :-** TTL = 1

A sends the packet to R1 with TTL=1 as the packet reaches the R1 the value becomes 0. Host A gets to know that R1 is the first router in the path

**Case 2 :-** TTL = 2

A sends the packet to R1 with TTL=2 then the TTL values reduces by 1. then router 1 further sends the packet to R2 where TTL be values becomes 0.

As a result A gets to know R2 is 2nd router in the path.

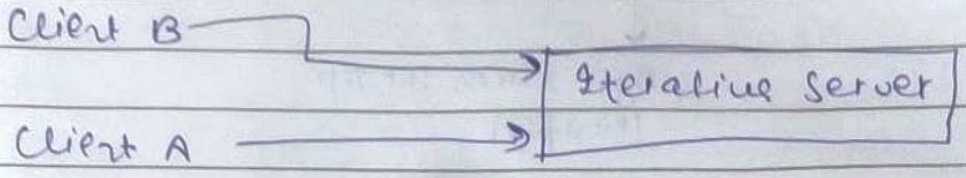
**Case 3 :-** TTL = 3

same as above.

Unit-2 :

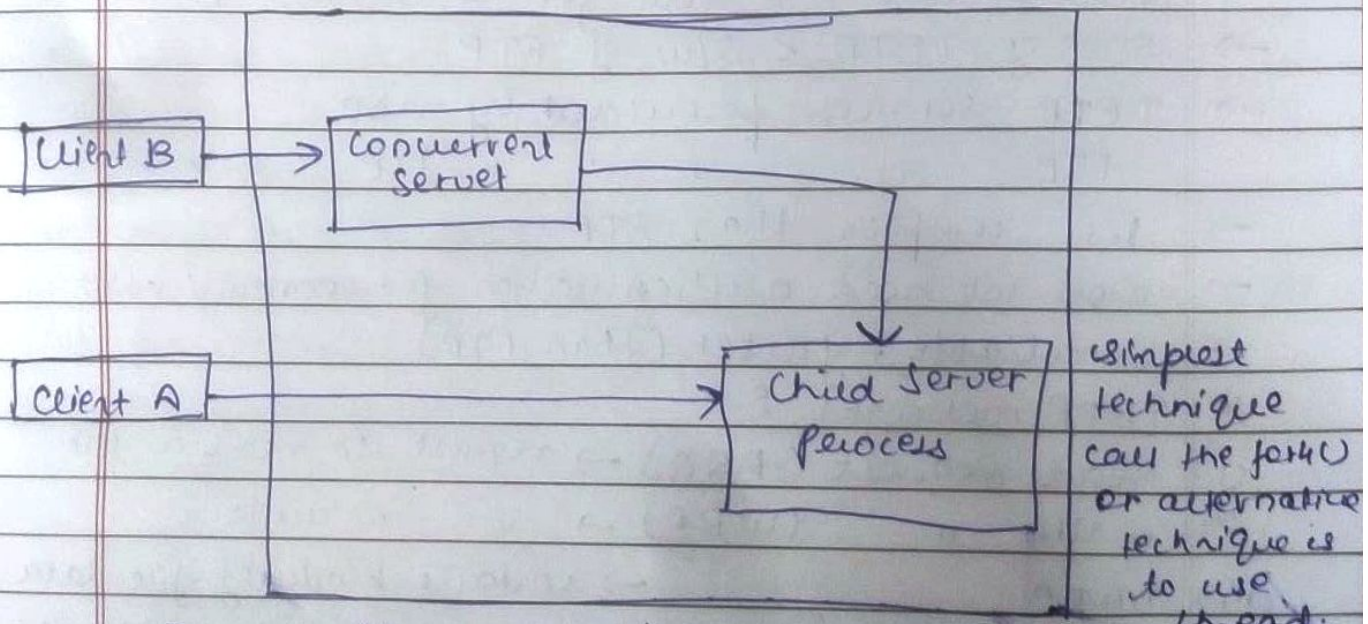
* Concurrent and Iterative Servers :-

* Iterative Server → handles each client one at a time
→ fairly simple and suitable for transaction that do not last long.
→ handles both connection request and transactions involved in the call itself.
→ If transaction ~~time~~ takes more time queues can build up quickly.




Client B cannot make a call until A has finished

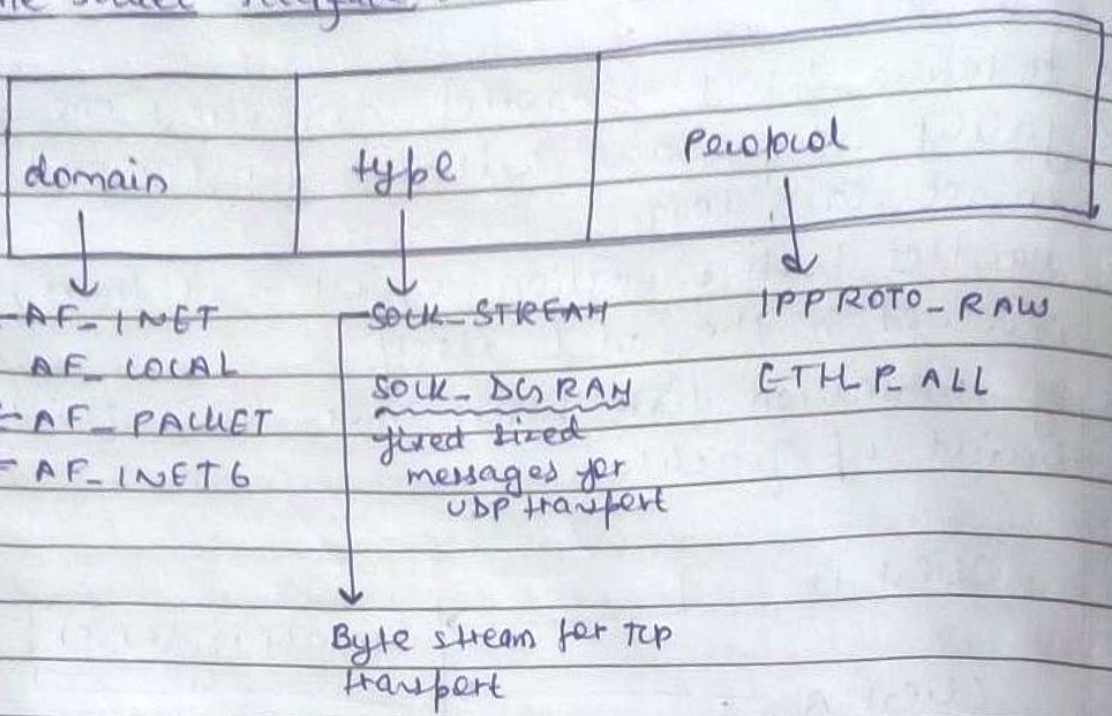
* Concurrent Server :-
→ handles multiple client at the same time.




→ more than one child server can be started in this way

DATE / /
PAGE

## * The Socket Interface :-




# Unit-3

## * TFTP :- (Trivial FTP)

→ not secure
→ read or write a file for a client
→ Slw of TFTP < Slw of FTP
→ TFTP services provided by UDP
FTP " " " TCP
→ less complex than FTP
→ Does not need authentication for communication
→ Unreliable, faster (than FTP)

## * TFTP messages :-

(i) Read Request (RRQ) → request to read a file
(ii) write " (WRQ) → " " write " "
(iii) DATA → contains block of file data
(iv) ACK → used to acknowledge each block of data
(v) Error → used to indicate error.

* WWW (World wide web) :-

→ Collection of info. that is linked together from points all over the world

→ provides flexibility, portability & user-friendly features.

→ ~~www~~ world wide collection of web-pages.

→ way of exchanging info. bet^n diff. computers on the internet.

→ Two components :-

(i) Structural — client, server, cache, internet

(ii) Semantic — HTTP, HTML, XHL (extensible Markup lang.), URL

→ Features :-

(i) Provides a system for Hypertext info.

(ii) Dynamic, interactive, cross platform, open source, distributed.

(iii) Provides info. for free.

(iv) Accessible from anywhere.

(v) We can exchange huge vol. of data

→ Disadvantages :-

(i) Difficult to prioritize & filter info.

(ii) No guarantee of finding what a person is looking for

(iii) No regulation

(iv) No quality control

(v) Danger in case of overload of info.

# Unit-4 •

* Auto-configuration :-

→ When a host in IPv6 joins a n/w, it can configure itself by the following process :-

(i) The host creates a link local address for itself (128-bit)

(ii) The host then tests to see LLA is unique and is not used for other hosts.

If this LLA is used by any other host then auto-configuration fails.

(iii) If the uniqueness of LLA is passed, the host still needs a global unicast Address for which it takes the help of the router, if the router cannot help the host with the configuration it informs the host then the host needs to use other means for configuration.

* Re-numbering :-

→ Related to auto-configuration.

→ Consists of replacing the n/w prefix with a different one

→ Routers advertise the existing prefix with small life time. At the same time, a new prefix is advertised with a long life-time.
Eventually the host sees to use old prefixes and employ only newly introduced one.

* IPV6 Routing Protocol :

(i) Interior Routing protocol => used within autonomous system or organization

(ii) Exterior " " => diff. autonomous systems.

Distance vector, link state, OSPF(V3), EIGRP, MP-BGP4, RIPng.

DATE / /
PAGE

* ~~Two forms of routi~~
* ~~IPv4 to IPv6 Tunnelling :-~~
* Protocols changed to Support IPv6 :-

(i) ICMP(V6) :-

→ upraded implementation of ICMP to accomodate IPv6 requirements.

(ii) DHCP(V6) :-

→ IPv4 requires DHCP for assigning IP addresses to the devices connecting over the n/w.
But, IPv6 allows auto-configuration for assigning IP address.

(iii) DNS :-

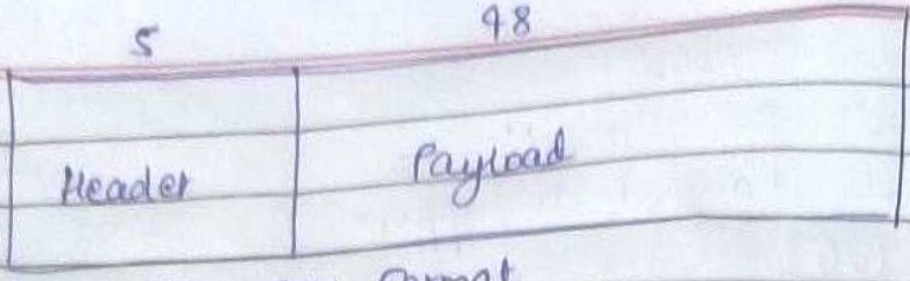
→ There has no new version, but it is now equipped with extensions to provide query support for IPv6 addresses.

## Unit-5

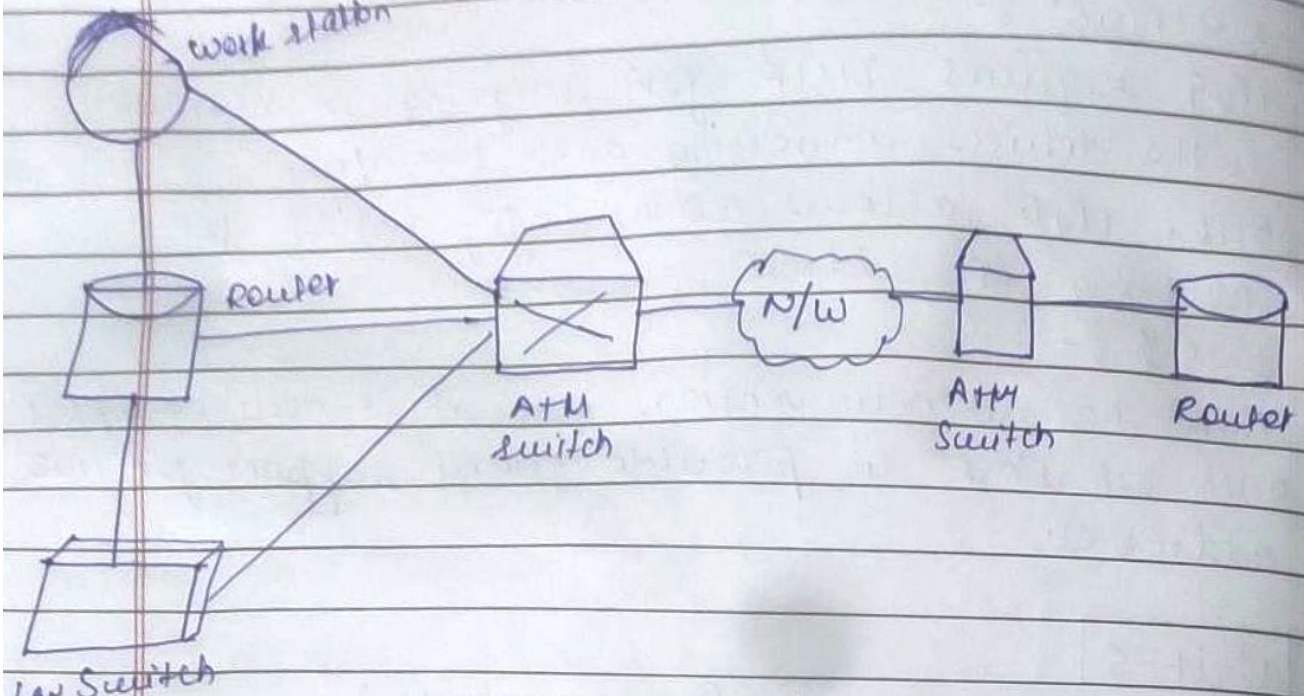
* ATM (Asynchronous Transfer Mode)

→ Wide Area Network (WAN) Technology.
→ Organizes i/p. i/to (cells) fixed length (53 bytes)
→ it can transfer all types of i/p. including data, video, image, voice etc.
→ it uses full duplex connection.
→ ATM networks are constructed using switches.
→ Before any data transfer begins end-end connection must be established.
→ ~~Bond~~ Connection oriented
→ Benefits :-

(i) Dynamic bandwidth (ii) Speed (fast) (iii) Scalable (iv) Small-sized header (v) Reduced Packet Overloading (vi) Uniform Packet size




ATH Cell Format




ATH Network

* VPN :- (Virtual Private Network)
→ Describes the opportunity to establish a protected n/w connection when using public networks.
→ VPN encrypts your internet traffic and disguise your online identity
→ This makes it difficult yor 3rd party do track your online activities & steal data
→ A VPN hides your IP address.
→ If you surf online with a VPN, the VPN server becomes the source of your data.
→ Your internet service provider & other 3rd party cannot see which websites you visit what data you send or receive online.

→ If your VPN connection is suddenly interrupted, your secure connection will also be interrupted. A good VPN can detect this and terminate pre-selected programs.

→ A strong VPN checks everyone who tries to login → Two factor authentication and authorization.

* Types of VPN :- 3-types

(i) SSL (Secure Socket Layer) :-

→ It enables individual users to access an organization's network.

→ It automatically uses most updated protocol that has been installed on the user's browser

(ii) Side-to-side VPN :-

→ Private network

→ Useful if you have multiple locations in your company each with its own LAN

→ Mainly used in large companies

→ complex implementation

→ Less flexible than SSL VPNs

(iii) Client-to-server VPN :-

→ connecting your home PC to the company with an extension cable.

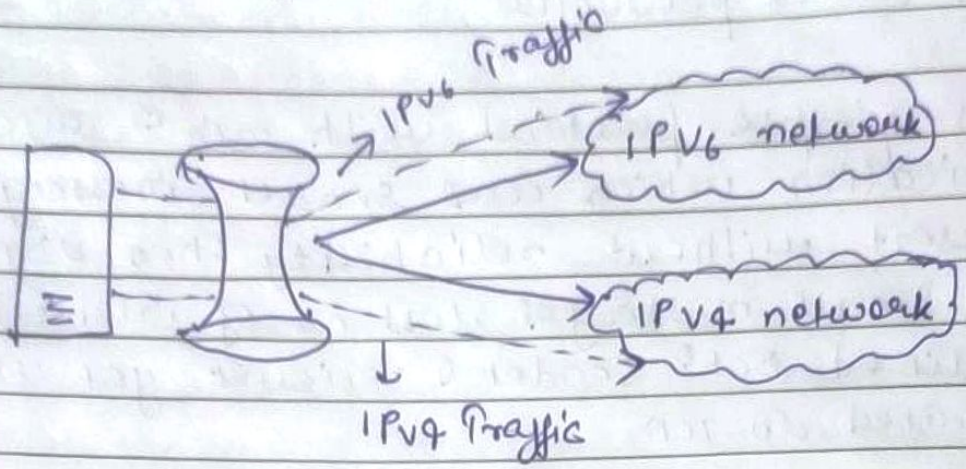
→ VPN client must first be installed and configured on the computer.

→ Greater efficiency

→ Universal access to company resources.

DATE / /
PAGE

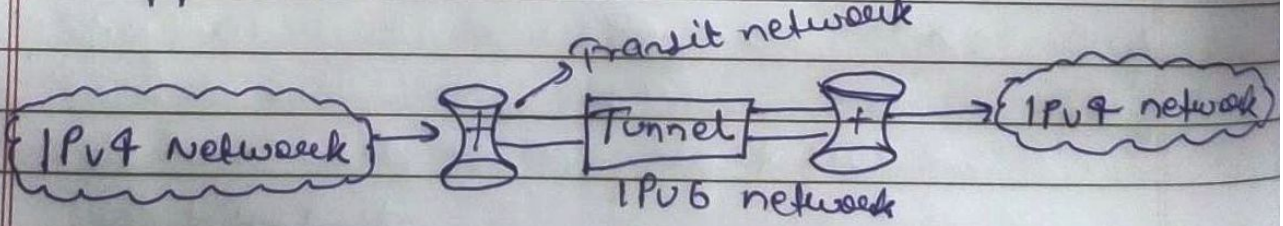
## * Transition from IPv4 to IPv6 :-




I ⇒ IPv6 as well IPv4 address configured for it can now speak with all the hosts on both the IPv4 as well as IPv6 network with the help of dual Stack Router → boundary router

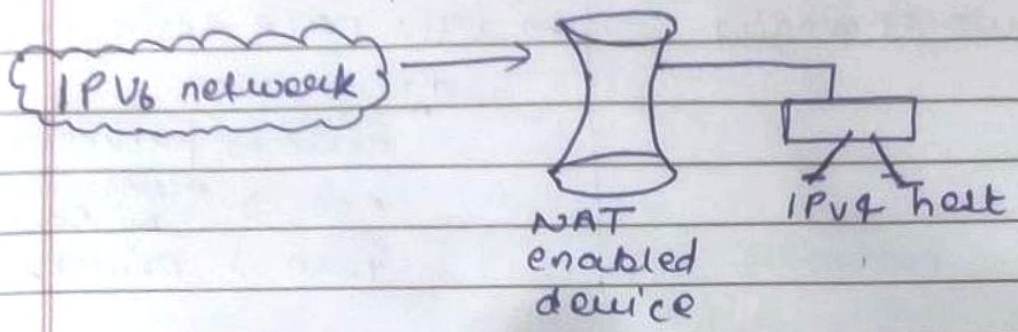
⇒ The Dual stack Router can communicate with both the network. It provides a medium for the hosts to access a server without changing their respective IP versions.

II Tunnelling :- where different IP versions exists on intermediate part or transmit networks. Tunnelling provides a better solution where user's data can pass through a non-supported IP version.



III. NAT Perotocol Translation :-

This is ~~the~~ another important method of transition enabled by a NAT-PT (Network Address Translation Perotocol) enabled device. With the help of NAT-PT device, actual can take place happens between IPv4 and IPV6 packet.




8. Which two IPv4 and IPv6 translation techniques manage the interconnection of IPv6 domain. (Choose two)

→ Trunking
✓→ Dual stack
→ encapsulation
✓→ Tunneling
→ multiplexing