CN

U-4

* NAT

→ To access internet on public device we need an IP address

→ The NAT allows multiple devices to access the internet through a single public address

→ NAT (Network Address Translation) is the process in which one or more local IP address are translated into one or more Global IP address and vice-versa.

Working of NAT

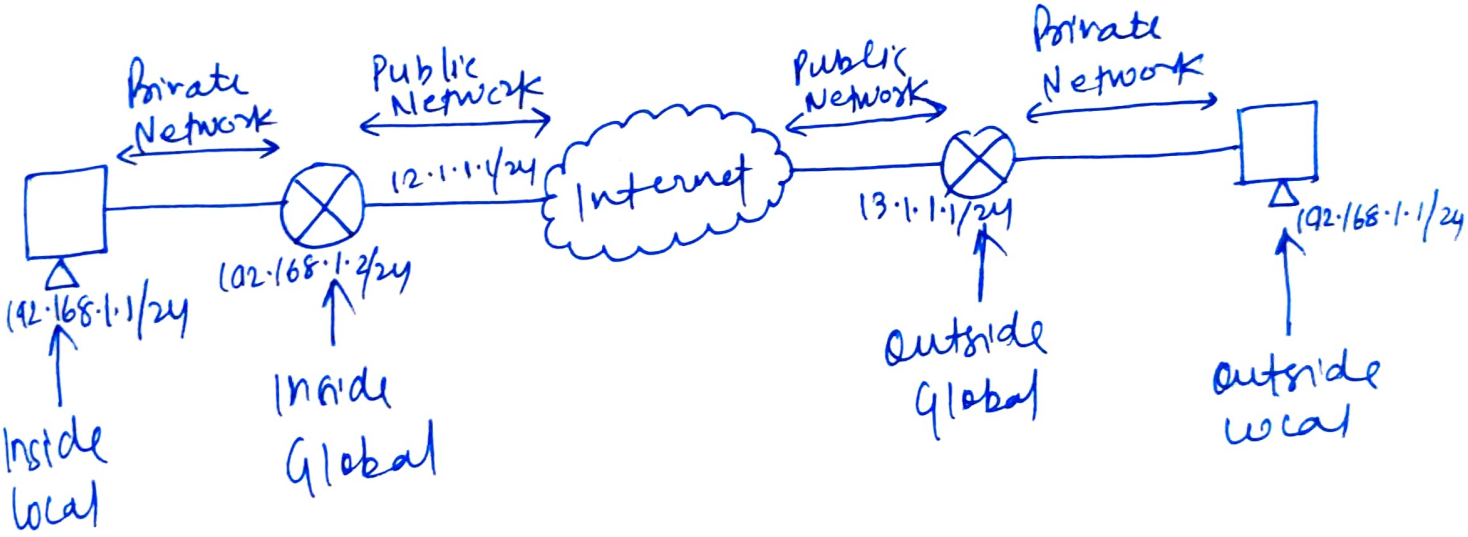
→ Here, generally the Border Router is configured

→ Border Router is the router which has one interface in local (inside) network and one interface in global (outside) network.

→ When packet travels outside of local (inside) network, then nat converts that local IP address to global (public) IP address. (public)

→ When packets enters into the local network, the global (public) IP addresses is converted into the local (private) IP address.

→ If NAT run out of address, i.e no addresses are left then packets will be dropped and Internet Control Message Protocol (ICMP) is sent to destination



Types of NAT

1) Static NAT
2) Dynamic NAT
3) Post Address Translation (PAT)

1) Static Nat

→ If a Private IP address is mapped with Public Address i.e. one to one mapping b/w local and global Addres, This is Static NAT

2) Dynamic NAT

→ Here, the Private IP address is translate into of Public IP address from pool of public IP. address.

3) Port Address Translation (PAT)

→ In this Many local (private) IP address can be translated to a single registered IP address.

→ Port Number is used to distinguish Traffic.

Advantages

* Provides Privacy
* Conserves legal IP address
* Eliminates address renumbering.

Disadvantages

* Cause Delay
* Some application won't work
* Complicates Tunelling protocols.

* Transistion from IPV4 to IPV6

Three stratigies are used:

(1) Dual stack

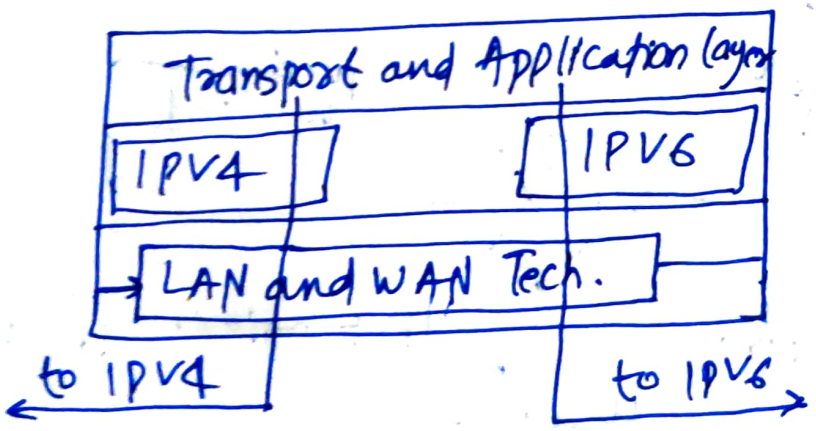
(2) Tunneling

(3) Header Translation

(1) Dual stack

→ Before completing Migration, all the station should run in dual mode i.e. IPV4 and IPV6

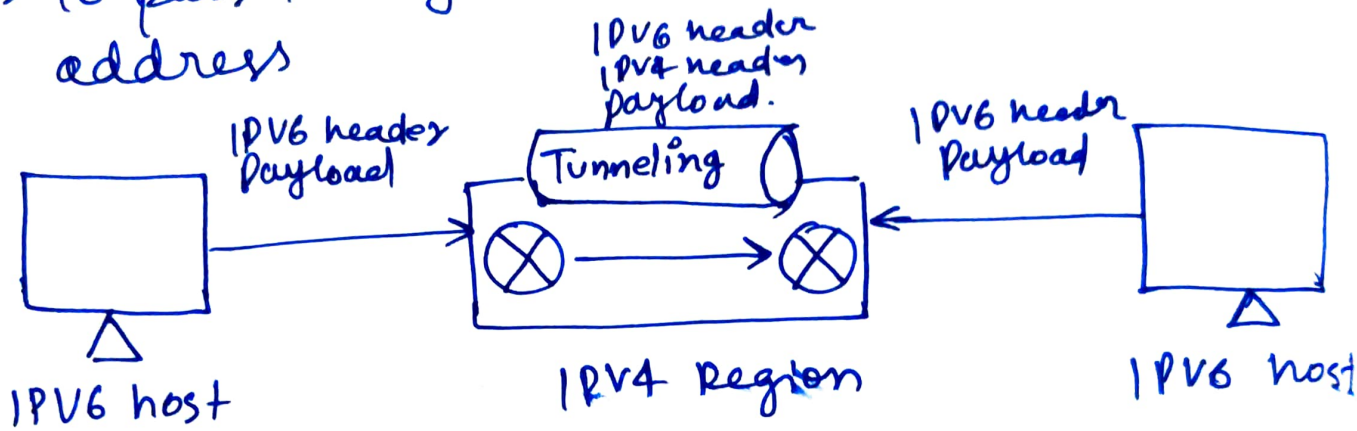
→ Before sending packet to destination the source needs DNS, if it returns IPV4 then source sends IPV4 packet else sends IPV6.



(2) Tunneling { Automatic : configured using IPV4
Configured : configured manually.

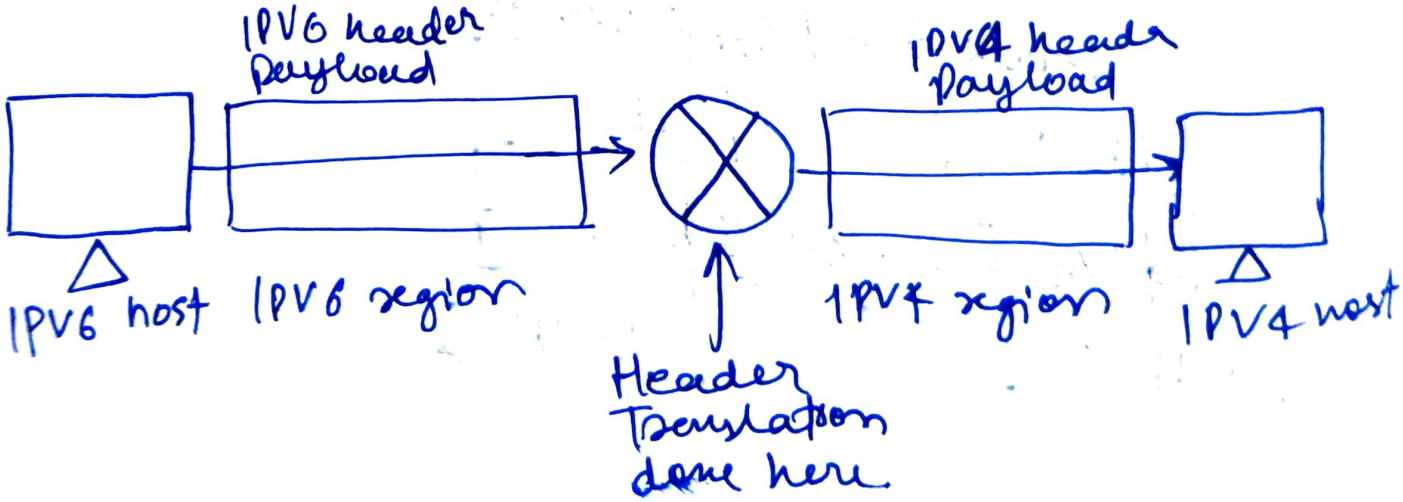
→ It is the process when two IPV6 host wants to communicate through IPV4 channel

→ To pass through this channel it requires IPV4 address



(3) Header Translation

→ It is the process in which sender uses IPV6 and receiver uses IPV4, where the IPV6 address needs to be translated to IPV4



* IPV6 Addressing Modes

→ 128 bits or 16 bytes long
  → four times as long as its predessor
→ 2^{128}
  → about 340 billion billion billion different addresses.
→ Colon Hexadecimal Notation
  → addresses are written using 32 hexadecimal digit
  → digits are arranged into 8 groups to improve readibility
  → Groups are seperated by colons.

2001:0718:1c01:0016:020d:56ff:fe77:52a3

→ Zero Suppression Rule
  (1) count the number of blocks
  (2) (-) subtract this number by 8
  (3) (*) multiply result by 16.

example FF02::2

No. of Blocks = 2

No. of bits seperated = (8-2) x 16
= 6 x 16
= 96

* Difference b/w IPV4 and IPV6

IPV4	IPV6
* 32 bit address length	* 128 bit address length
* Manual Config	* Auto config
* Connection integrity is unachievable	* Achieveable.
* Address rep. in decimal	* Address rep. in hexadecimal
* Checksum field is available	* Checksum field is not available.
* Can be converted to IPV6	* Cannot be converted to IPV4
* It has five diff Class. class A, B, C, D, E	* It doesn't have any classes.
* Separated by (.)	* Separated by (:)

*IPV6 Address Type

→ There are three types of Addsess in IPV6:-

(1) Unicast

→ A unicast address uniquely identifies the interface of IPV6 node.

→ A packet sent to the unicast address is delivered to interface identified by that address.

(2) Multicast

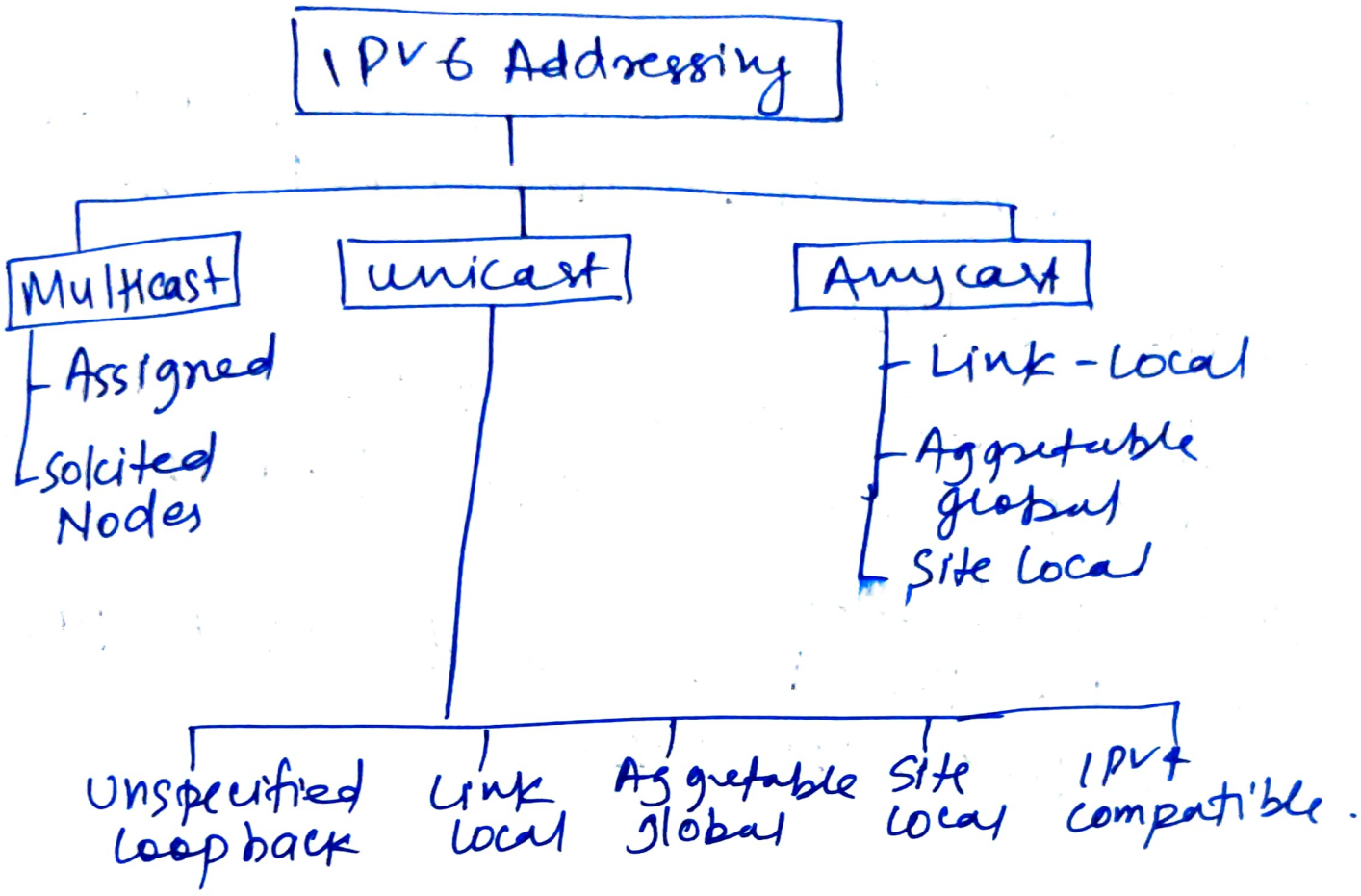
→ A Multicast address identifies the group of IPV6 interfaces

→ A packet sent to multicast address is process by all members of multicast group.

(3) Anycast

→ An Anycast is assigned to multiple interfaces.

→ A packet sent to Anycast address, will be delivered to only one of these interfaces.



* IPV4 to IPV6 tunneling.

→ Basic idea behind tuneling method is that IPV6 will be tunneled over an existing IPV4 network

→ IPV4 to IPV6 tuneling can be done in variety of ways:

(1) Router to Router

→ IPV6 or IPV4 routers are interconnected by IPV4 infrastructure and IPV6 packet.

(2) Host to Router

→ IPV6 or IPV4 host can tunel IPV6 packets to IPV6 or IPV4 routers.

(3) Host to Host

→ IPV6 or IPV4 host can tunnel IPV6 packets to an intermediary IPV6 or IPV4 host

(3) Host to Host

→ IPV6 or IPV4 routers are interconnected by IPV4 infrastructure and IPV6 packets.

(4) Router to Host

→ IPV4 or IPV6 Routers can tunnel IPV6 packets to IPV4 or IPV6 host

CN U5

* PPP protocol

→ The telephone line or cable provide a physical link, but to control and manage transfer of data, PPP is used.

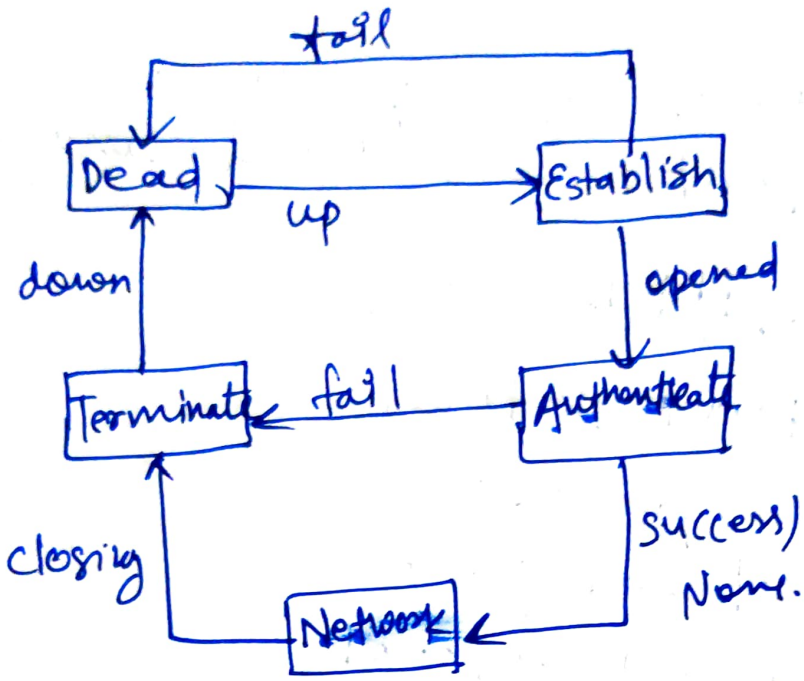
→ PPP is Point to Point Protocol.

→ PPP has three components:
  (1) Multi protocol Datagram
  (2) LCP - Link control Protocol
  (3) NCP - Network control Protocol.

→ PPP design principle
  (i) supports multiple link layer
  (ii) Link configuration
  (iii) Error Detection
  (iv) Establish network Addresses.
  (v) Authentication
  (vi) Extensibility.

→ PPP protocols
  (i) HDLC - to perform base operations
  (ii) LCP - Link control protocol
  (iii) NCP - Network control protocol.

→ PPP state Machines.



Dead :- Link is not being used.

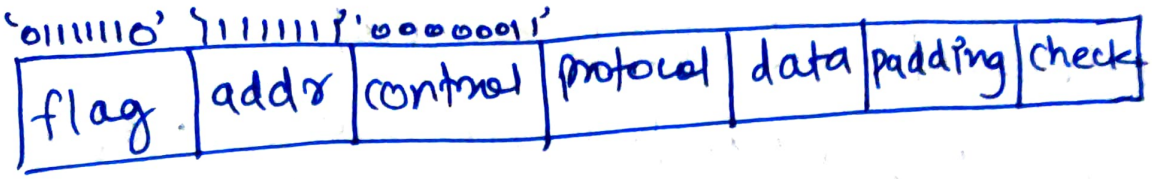
Establish :- When one machine starts communication, the connection goes into establishing state.

Authenticating :- User sends Authenticate req. packet includs user name & password.

Networking :- Exchange of data packets.

Terminating :- User sends the terminate link.

→ PPP format. (For 4-mark as well)



① Flag field
→ Boundaries of PPP frame
→ Value is 01111110

② Address field
→ It uses Broad cast address
→ Value is 11111111

③ Control field
→ Frame has no sequence no. and each frame is Independent.
→ Value is 00000011

④ Data field
→ This field carries data and informations

⑤ FCS
→ Frame check sequence
→ It is 2byte or 4byte
→ CRC used for error detection.

*HDLC

→ High level Data Link control.

→ It manages node to node transfer of data b/w two connected machines.

→ Exchange the Data b/w two devices

→ It is a widely used Data Link control protocol.

→ HDLC station types:

(i) Primary stations

→ Control operation of Links

→ Issues ~~frames~~ commands

(ii) Secondary stations

→ under control of primary stations

→ Issues ~~frames~~ responses.

(iii) Combined station

→ May issue commands and responses

→ HDLC configuration

(i) Balanced

→ one primary station and one or more secondary station

→ supports half duplex or full duplex

(ii) Unbalanced
→ Two combined stations
→ supports half duplex and full duplex.

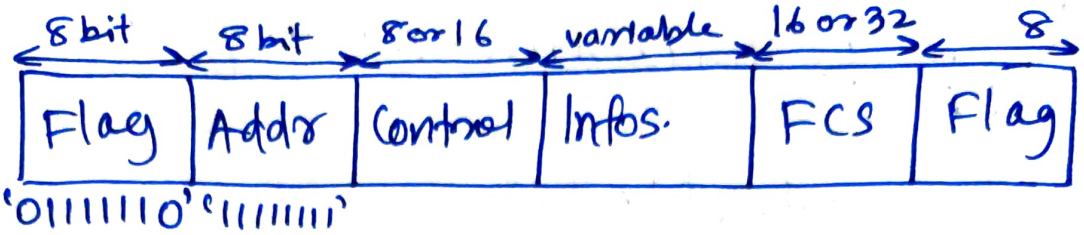
→ HDLC Transfer Modes

→ Normal Response Mode
(i) Unbalanced configuration
(ii) Primary can initiate transmission
(iii) Secondary can transmit data

→ Asynchrous Balance Mode
(i) Balanced configuration
(ii) Any station can initiate transmission.
(iii) Most widely used.

→ Asynchrous Response Mode
(i) Unbalanced configuration
(ii) Secondary may initiate transmission without any permission
(iii) Primary is used for connect, disconnect, error recovery
(iv) Rarely used.

→ Frame Structure



(1) Flag Field

→ surrounds frame at both sides

→ Bit stuffing is used to avoid confusion

→ Value is 01111110

Bit stuffing : Insert 0 bit after every sequence of five 1s

ex Patton

111111111110101111101111110

after bit stuffing

11111 0 11111 0 0101111 0 1110111110 0 10

(2) Address Field

→ uses sencondary station

→ 8 bits long

→ value is 11111111

(3) Control Field

→ I-Frame : Information frame data is transmitted to user

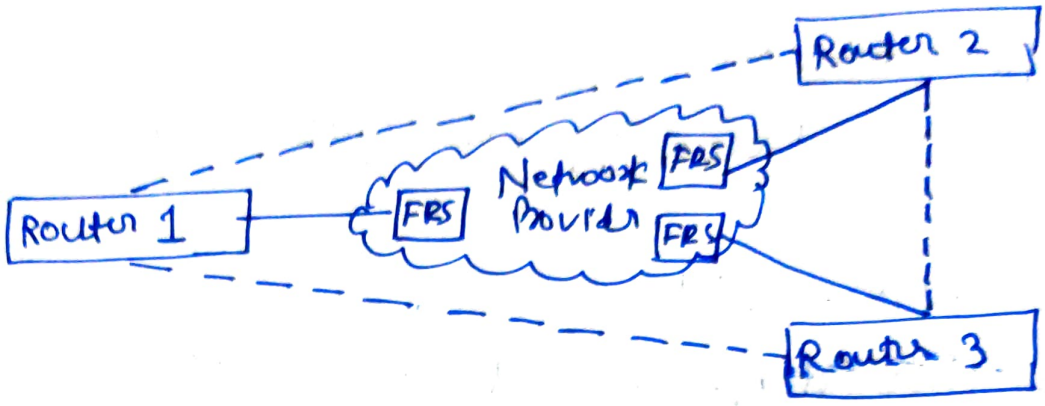
→ S-frame : Supervisory frame
used for flow & error control

→ U-frame : Unnumbered frame
Recovery, connect/disconnect

(4) Information field
→ only information and some unnumbered frames
→ variable length

(5) FCS - Frame check sequence
→ Error detection
→ 16 bit CRC
→ optional 32 bit CRC

* Frame Relaying



FRS: frame relay switch

→ Frame Relay is connection-oriented service

→ It uses High Level DataLink Control (HDLC) protocol

→ It is used to connect LANs and transmit data across WANs

→ Frame relay transfer data between LAN across WANs by dividing data into packets

→ Does not have any error control or flow control.

→ LAN will send data packets. The packet sent by LAN will be checked by frame relay switch. Frame Relay switch will already have the info about the LAN. This LAN will send data packets to other LAN. And in this way multiple LANs can share data.

* VPN - Virtual Private Network
→ VPN gives you the protected network when you are using Public Network
→ VPN encrypts the internet traffic.
→ VPN hides your IP address.

features:

(1) Secure encryption
→ Hide the online activities

(2) Access to regional content
→ By changing location, you can access the content of other countries which is not available in our country.

(3) Secure Data Transfer
→ VPN connects you to pvt server and let you transfer the imp. files

(4) Improve online gaming
→ can access to the games which are banned in our country.

* ATM

→ Asynchronous Transfer Mode

→ Replaces most existing WAN technologies

→ Improves performance of frame Relay

→ 53 bytes cell = 48 byte data + 5 header

→ Rates of 155-622 Mbps are achieved

→ compatible with twisted pair, ~~coaxial~~ coax and fiber.