CT-3

12M

Set-1

3. How do transition so occurs from IPV4 to IPV6.

4. HDLC transfer mode & frame structure.

Set-2

5. IPV6 Address types

4. PPP protocol.

Set-1

IPV6 packet format

Types of Addresses - IPV6.

importance of other DSL Technologies.

PPP frame format.

Set-2

Addressing modes of IPV6.

Compare IPV4 & IPV6

Services of SSL - 57

Features of VPN - 53.

12m

Transition from IPV4 to IPV6:

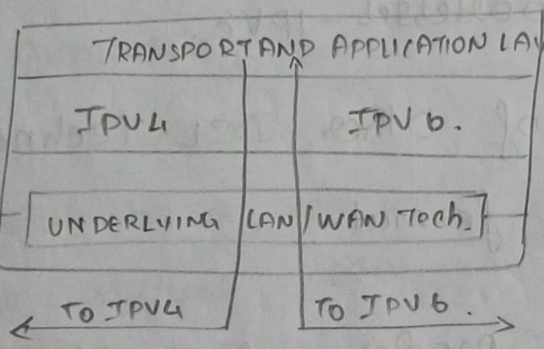
- IPV4 → 32 bit. range (0 to 255)
- IPV6 → 128 bit address

3 Strategies used.

→ Dual stack
→ Tunnelling
→ Header translation

Dual Stack:

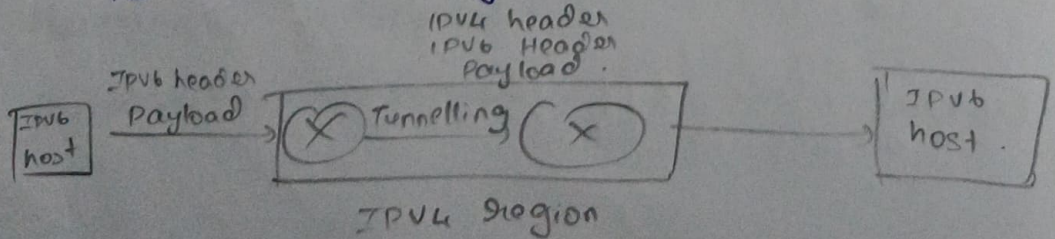
Before complete migration all station must run in dual mode. (Both)



- easiest method
- host able to gain access.
- IPV6 Doesnot work for all IPV4

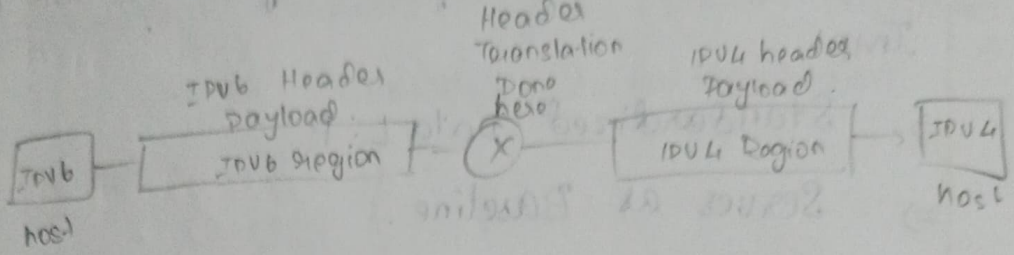
Tunnelling.

→ process happens when two IPV6 host wants to communicate through IPV4 channel.
→ to pass the channel, it requires IPV4 Addr.
→ IPV6 packet is encapsulated IPV4 packet to enter the region.



Header translation

- Header Translation requires when sender uses IPV6 & receiver uses IPV4, where IPV6 address needs to be translated to IPV4.



Rules:

- Addr of IPV6 to IPV4 by extracting the right most 32 bits.
- Value of IPV6 priority field is discarded.
- type of Service in IPV4 is set to zero.
- Checksum for IPV4 is calculated & inserted in the corresponding field.
- IPV6 flow label is ignored
- Compatible extension headers converted to options & inserted into IPV4 header (Drop)
- length of IPV4 header is calculated & inserted into the corresp. field.
- total length of the IPV4 packet is calculated & inserted in the corresp. field.

HDLC Transform Modes & frame structure

- high level Data link control.
- Exchange of Digital Data bet 2 Devices some form of Data link Contro

Imp:

⇒ Standardized Data L.P.

⇒ Serves as Baseline.

Char:

⇒ Defines 3 types of stations.

⇒ Two link config.

⇒ 3 - Data transfer modes of op.

Transfer Modes:

- Normal Response Mode (NRM)

→ unBalanced config.

→ Primary can only initiate transmission.

→ Second can't transmit Data, in response to command (poll) from primary

→ used on Multi - drop lines.

→ Host Computer as primary.

→ Terminale as Second.

* Asynchronous Balanced Mode (ABM)

⇒ unbalanced config

⇒ Second initiate transmission with permission from primary.

⇒ primary responsible for connect, disconnect, error recovery & initialization

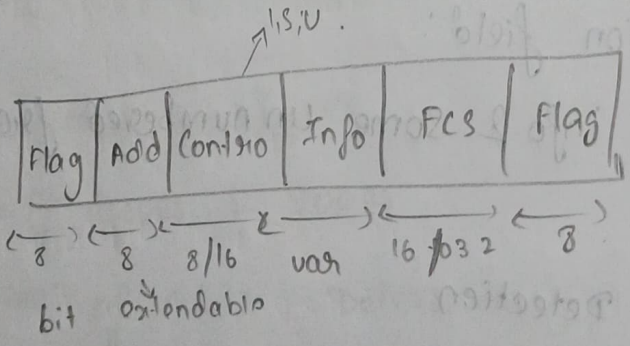
⇒ rarely used.

Frame structure.

* Synchronous transmission

⇒ All transmissions in frames

⇒ Single frame format for all Data & control exchanges.



* flag field:

⇒ Delimit Frame at Both sides.

⇒ 5 1's checks next bit

⇒ If 0 → Deleted

1 → seventh bit 0. (Accept)

* Bit stuffing:

* Address field:
  - ⇒ Identifies second station.
  - ⇒ 8 bit
  - ⇒ Multiples of 7.
* Control field
  - ⇒ I - frame (info)
  - ⇒ S - frame (Supervisory frame)
    - ↳ flow & error.
  - ⇒ U - frame (unnumbered frame)
    - ↳ Supplementary link control.
* final bit:
  - ⇒ Depends on context
* Information field:
  - ⇒ only info & some unnumbered frames.
* FCS
  - ⇒ Error Detection
  - ⇒ 16 bit CRC.
  - ⇒ Optional (32 bit)

IPV6 Address Types:

- IPV6 Larger Addresses: from 32 bit to 128 bits
- Improved options than IPV4

⇒ IPV6 Addressing Modes:

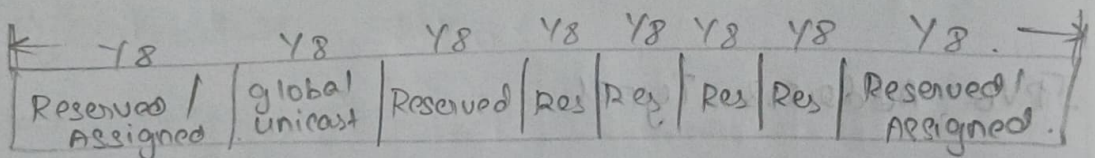
- 128bits → 4 times as long as its predecessor.
- 2^{128} → Abt 380billion billion billion billion diff. Addresses.
- Colon hexadecimal notation.
- 32 hexadecimal digits.
- 8 grps of 4 to improve readability.
  Separated grps by colons.
- Eg: 128.81.91.....

⇒ IPV6 Address Types.

- Diff types & scopes.
- Type: of Addr, Determines if packets are destined for one or for many machines.
- Scope: Which context address makes sense.
- Assigned to interface on nodes ⇒ IPV6.

* Unicast:
  - ⇒ Uniquely identifies an interface of a IPV6 node.
  - ⇒ is Delivered to the interface identified by that Address
* Multicast:
  - ⇒ identifies group of IPV6 interfaces.
  - ⇒ Sent, processed by all members in Multicast grp.
* Anycast:
  - ⇒ Multiple interfaces.
  - ⇒ Delivered to only one interface, nearest.

2^{128} -> Addr.



global unicast.

One - one comm.

equivalent to public IPV4 addr.

reach any host globally ⇒ Objective.

2^{125}

PPP protocol.

* PPP → point - to - point protocol.

⇒ telephone lines companies provide a physical link, but to control & manage the transfer of Data, there is a need for a special protocol. (PPP)

* Main Components.

⇒ A Method for encapsulating Multi-protocol diagrams.

⇒ Link control protol → estab. config & testing the Data link comm.

⇒ Network control protocol → estab. config diff n/w layer.

* Design principles.

→ Support Multi n/w p.
→ Link Config
→ Error Detect
→ Estab n/w addr.
→ Authentication
→ Extensibility.

* PPP - A protocol.

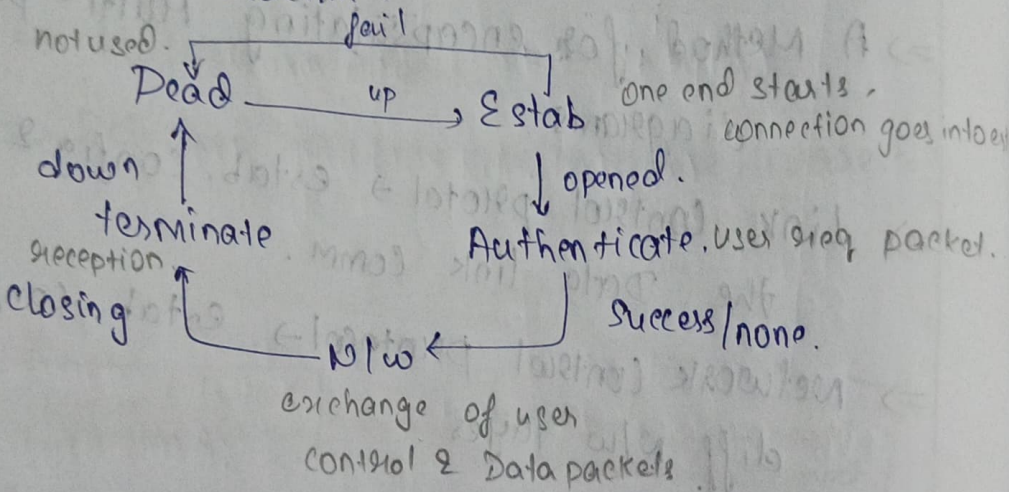
⇒ PPP relies on another DLP

⇒ HDLC → to perform some basic op.

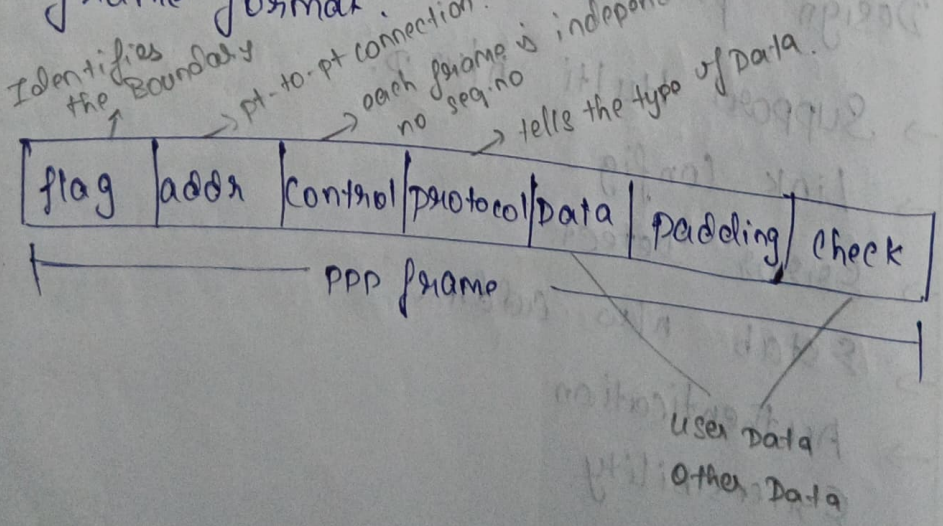
⇒ After initial handshake, PPP executes its own handshake.

⇒ PPP
- ↳ LCP
- ↳ NCP

* PPP state Machine.



* PPP - frame format.



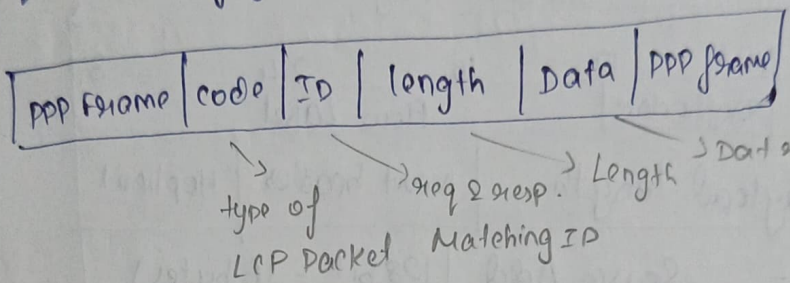
* LCP.

=> purpose.

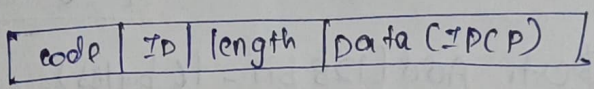
* Link estab.
* Link, maintenance, termination

=> classes:

* Link Config → Link termination → Link Monitoring



* NCP:



=> purpose.

→ Configure the N/w protocol.

→ Separate NCP for each. N/w.

=> Negotiation process:

→ Same Msg format, code nums, State Machines as LCP

* Un Supported options.

→ flow control.

* Overflow receiver's buffer are lost.

→ Error correction.

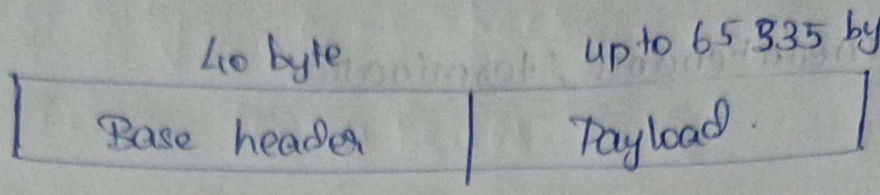
* includes only CRC.

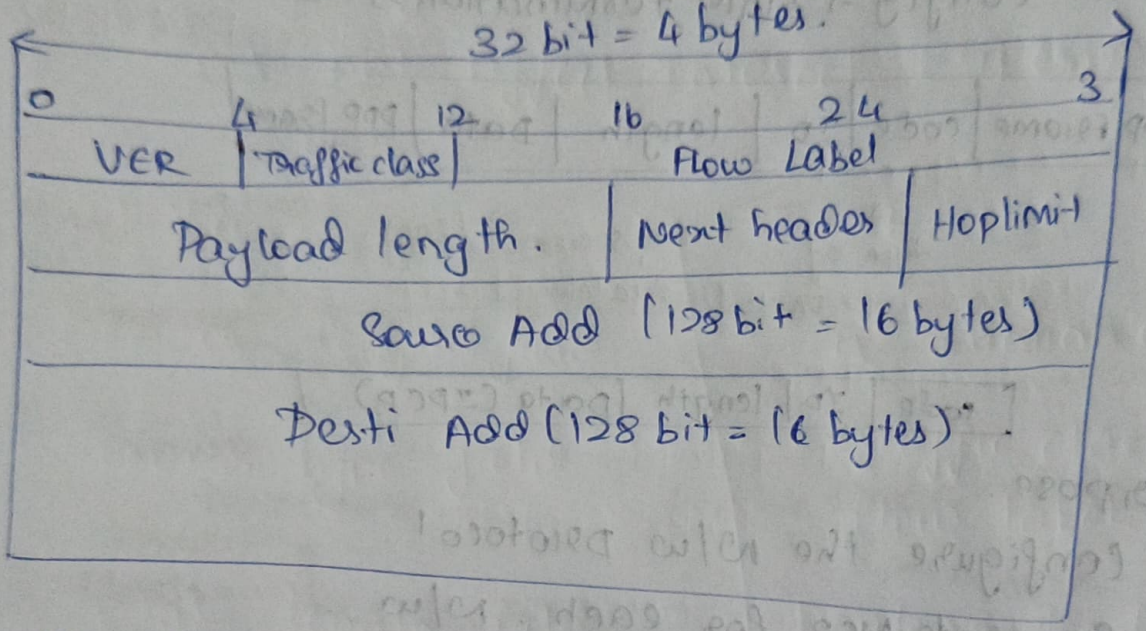
→ Re-sequencing.

* all frames sent & received.

4 masks:

IPV6 Packet format:





→ Version: whether IPV4 & IPV6.
→ Traffic class: Distinguish the payload.
→ flow label: Spl handling for particular flow of Data
→ Payload length: Defines length of IP Datagram
→ Next header: optional headers extension.
→ Hop limit: TTL
→ Source original source Addr.
→ Desti final dest.

Other DSL Technologies: → existing tele comm, residential users. not for Business.

* ~~SDSL~~ SDSL → Symmetric Digital Subscriber line.
* HDSL → high bit rate digital subscriber line.
  - → Alternative to T-line.
  - → using 2B1Q encoding.
  - → up to 3.6 KM
  - → using 2 twisted pair wires for
  - → full Duplex transmission.
* VDSL → Very high rate D.S.L
  - → using coaxial cable, fiber optic for Short Distances (300 to 1800m)
  - → using DMT with bit rate of 50 to 55 Mbps downstream & 1.5 to 2.5 Mbps up-stream

Features of VPN

* Virtual private N/w.
* N/w that is private not virtual.
* it guarantees privacy inside org.
* it is virtual beco2 not use real private WANS phy → public, virtually ~~Publi~~ → private

Features:

- Privacy → can't linked into comp
- Security → can't hack
- Access to websites.
- Anonymity
- Does not Affect Internet Experience.

IP V4	IPV6.
header length field	is eliminated.
Service type field	Traffic class & flow label.
Total length field	Payload len field.
Identification, flag, Offset.	Fag. extension header
TTL	Hop limit
protocol	Next - header
Header checksum	No checksum
Option fields	Extension headers.

Services of SSL:

⇒ Secure Socket layer

* Fragmentation: First SSL divides Data into blocks of 214 bytes or less

* Compression:
  Each fragment of Data is compressed using one of the lossless compression methods.
  negotiated bet client & Server → optional

* Msg integrity: To preserve the integrity of Data.