PACKET ENCAPSULATION

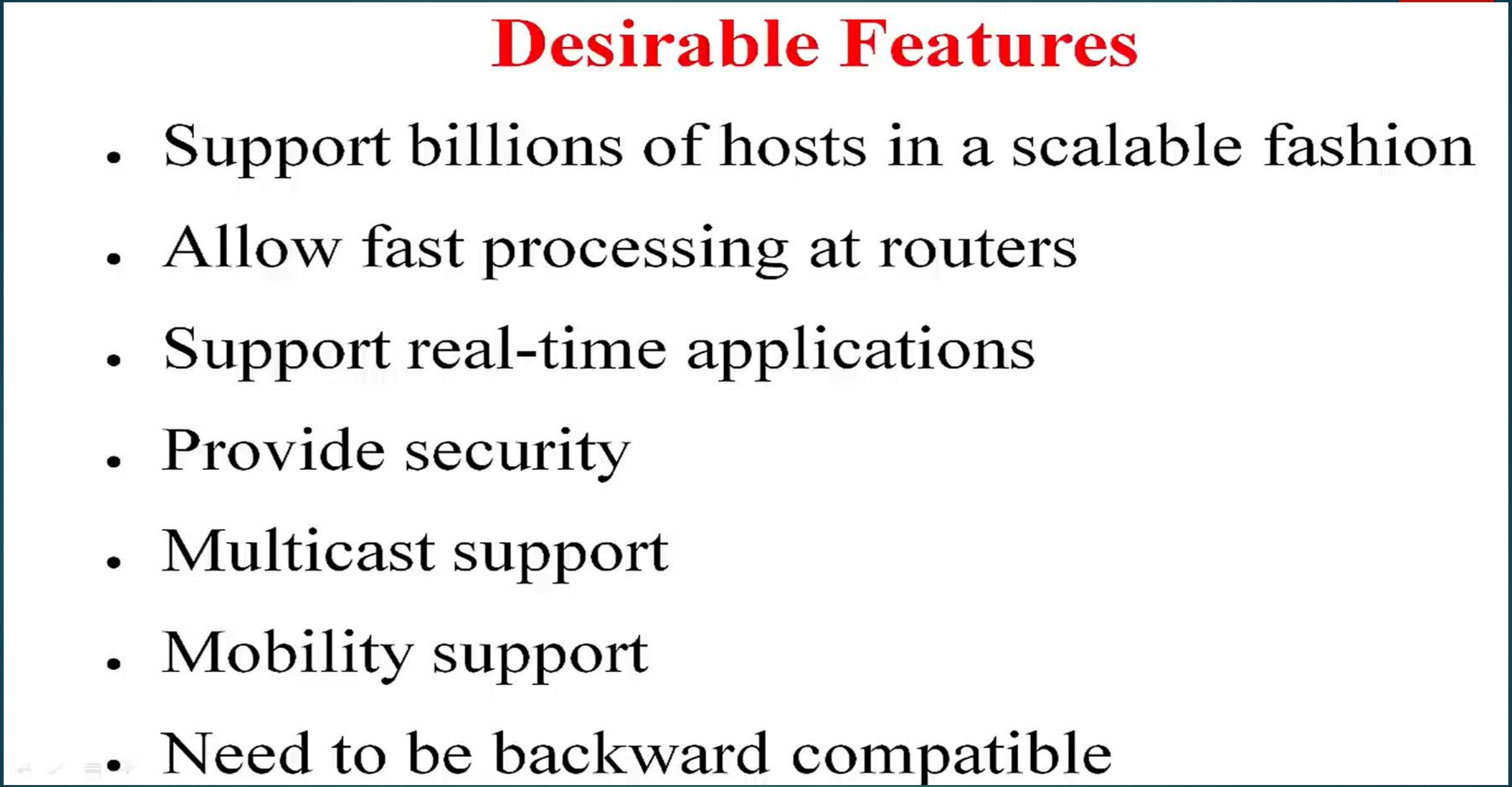
Introduction

- Encapsulation means Hiding something inside.
- Encapsulation is also called as Tunneling
- Data traveling over a network is divided into packets.
- A typical packet has two parts: the header, which indicates the packet's destination and which protocol it uses, and the payload, which is the packet's actual contents.

- An encapsulated packet is essentially a packet inside another packet.
- In an encapsulated packet, the header and payload of the first packet goes inside the payload section of the surrounding packet.
- The original packet itself becomes the payload.

Why Encapsulation?

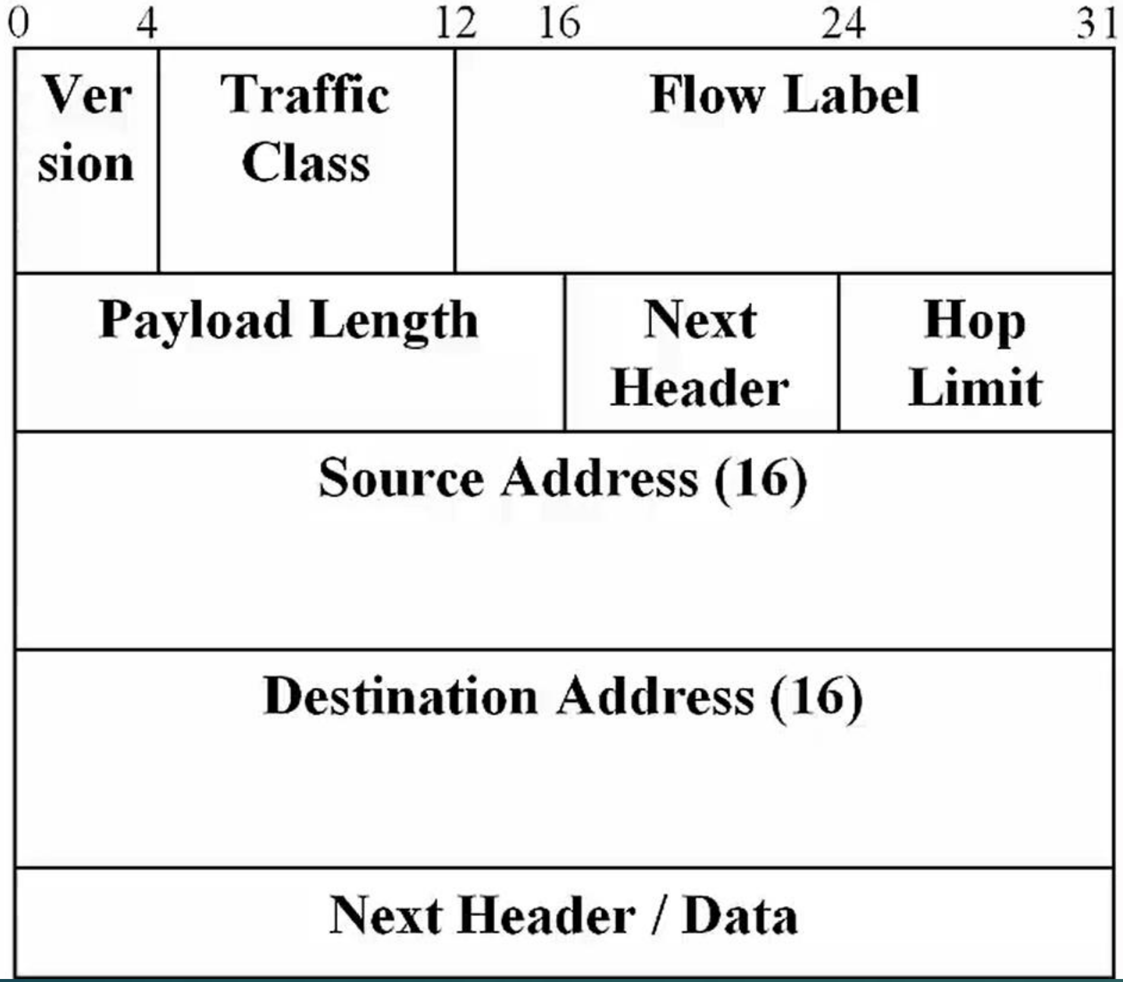
- All packets use networking protocols — standardized ways of formatting data — to get to their destinations. However, not all networks support all protocols. Imagine a company wants to set up a WAN connecting Office A and Office B.
- The company uses the IPv6 protocol, which is the latest version of the Internet Protocol, but there is a network between Office A and Office B that only supports IPv4.
- By encapsulating their IPv6 packets inside IPv4 packets, the company can continue to use IPv6 while still sending data directly between the offices.
- Encapsulation is also useful for encrypted network connections.
- If a packet is completely encrypted, including the header, then network routers will not be able to forward the packet to its destination since they do not have the key and cannot see its header.
- By wrapping the encrypted packet inside another unencrypted packet, the packet can travel across networks like normal.



Desirable Features

- Support billions of hosts in a scalable fashion
- Allow fast processing at routers
- Support real-time applications
- Provide security
- Multicast support
- Mobility support
- Need to be backward compatible

IPv6 Header



0 4 12 16 24 31

Version | Traffic Class | Flow Label

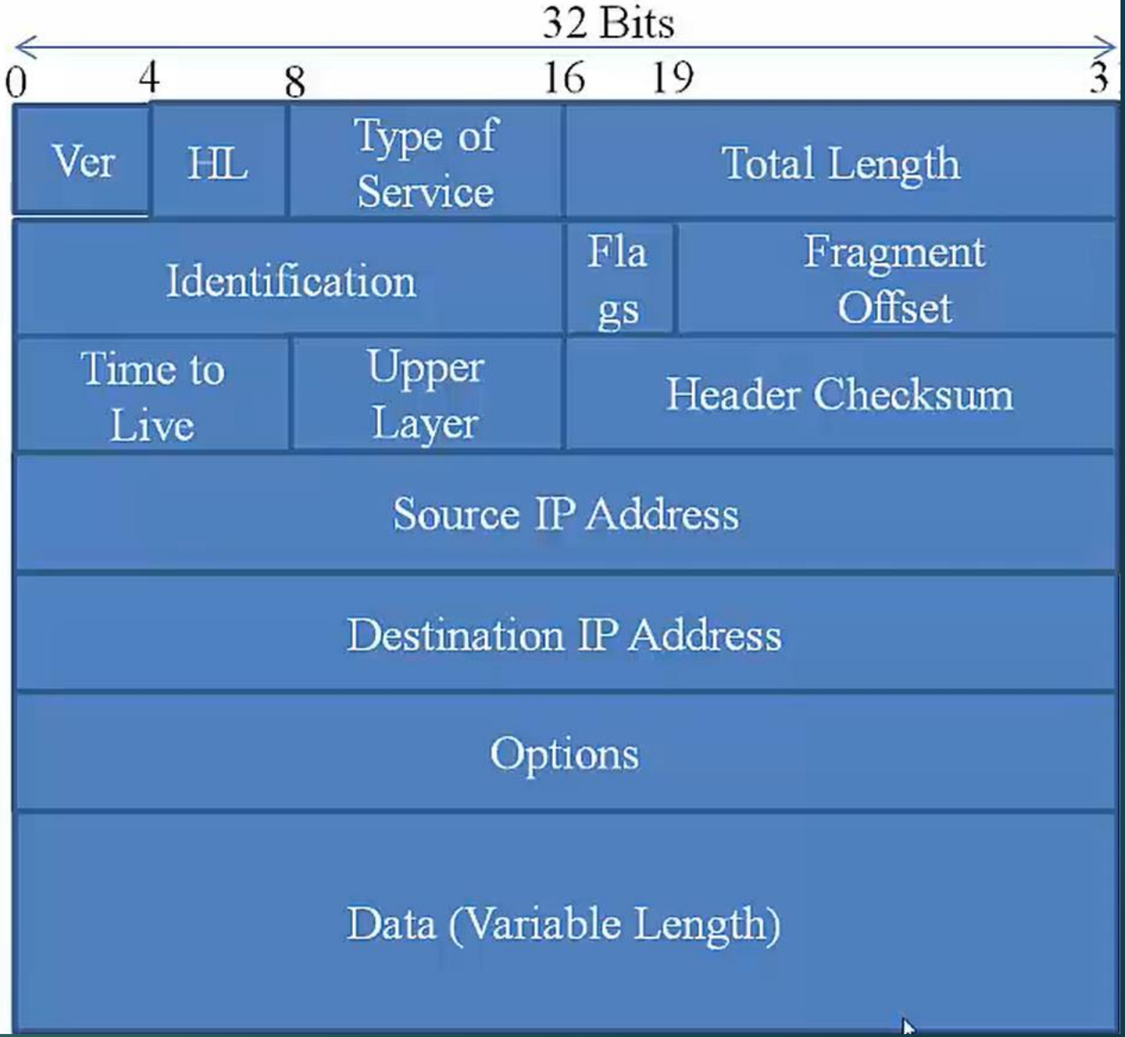
Payload Length | Next Header | Hop Limit

Source Address (16)

Destination Address (16)

Next Header / Data

IPv4 Header



32 Bits

0 4 8 16 19 3

Ver | HL | Type of Service | Total Length

Identification | Flags | Fragment Offset

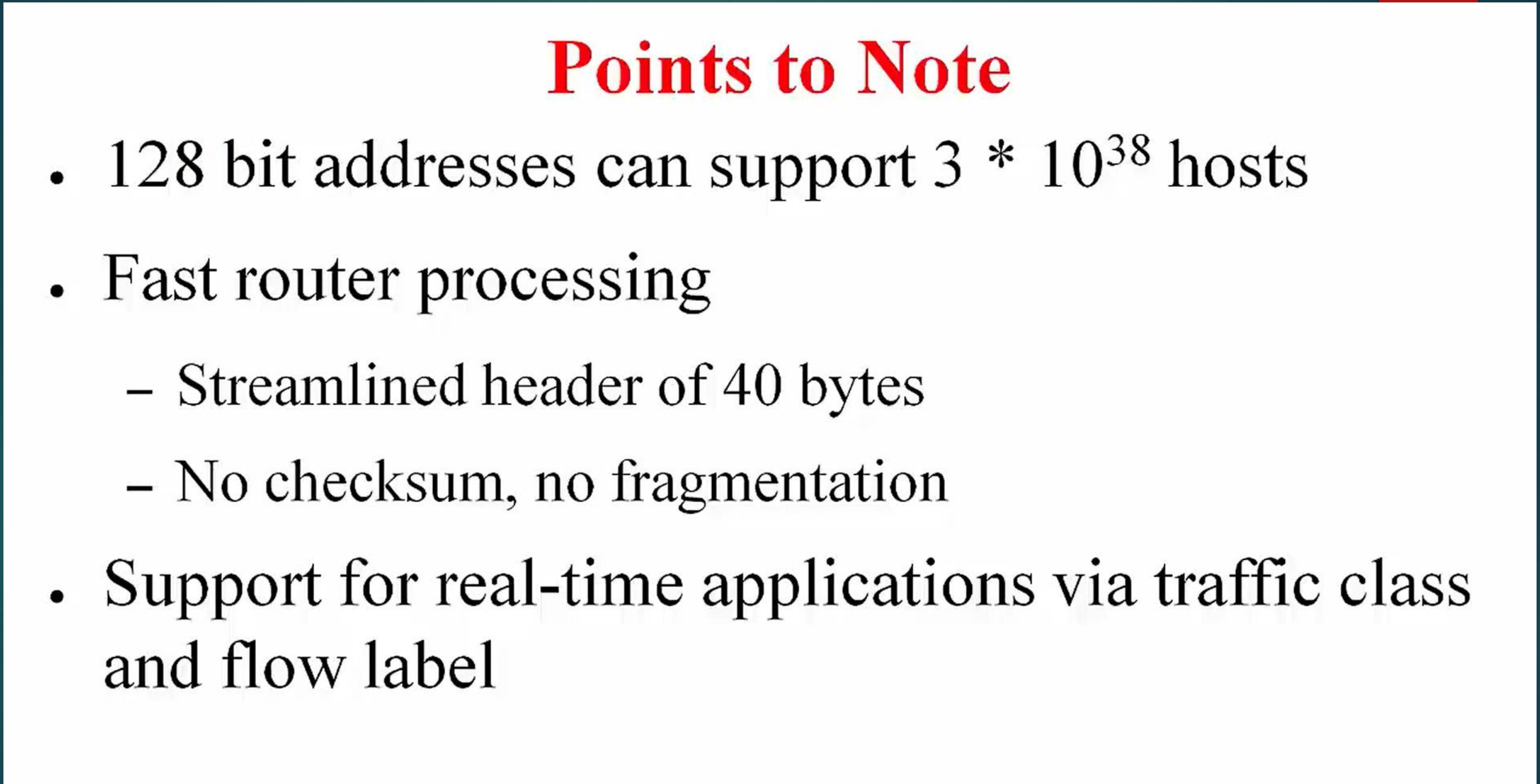
Time to Live | Upper Layer | Header Checksum

Source IP Address

Destination IP Address

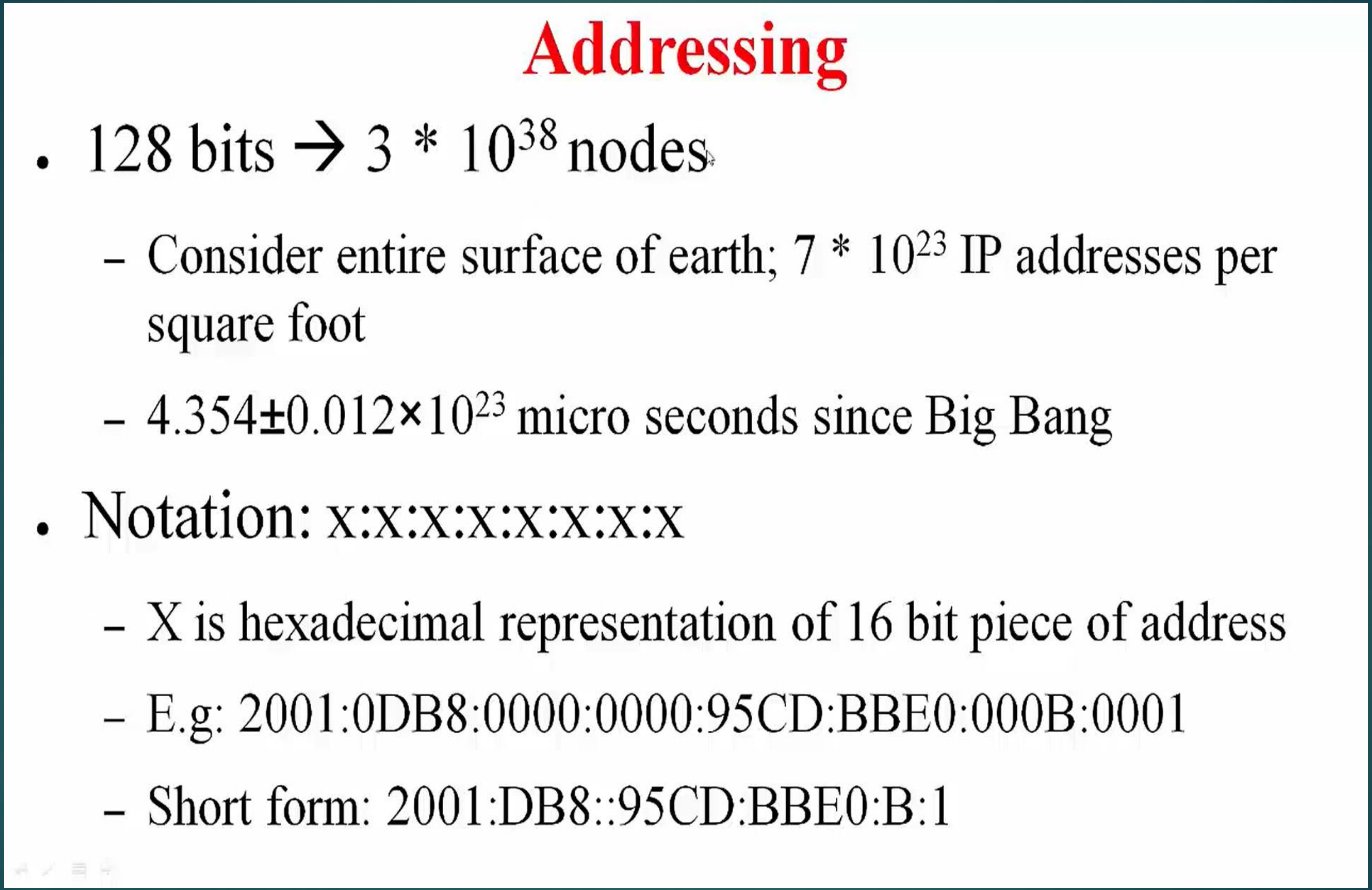
Options

Data (Variable Length)



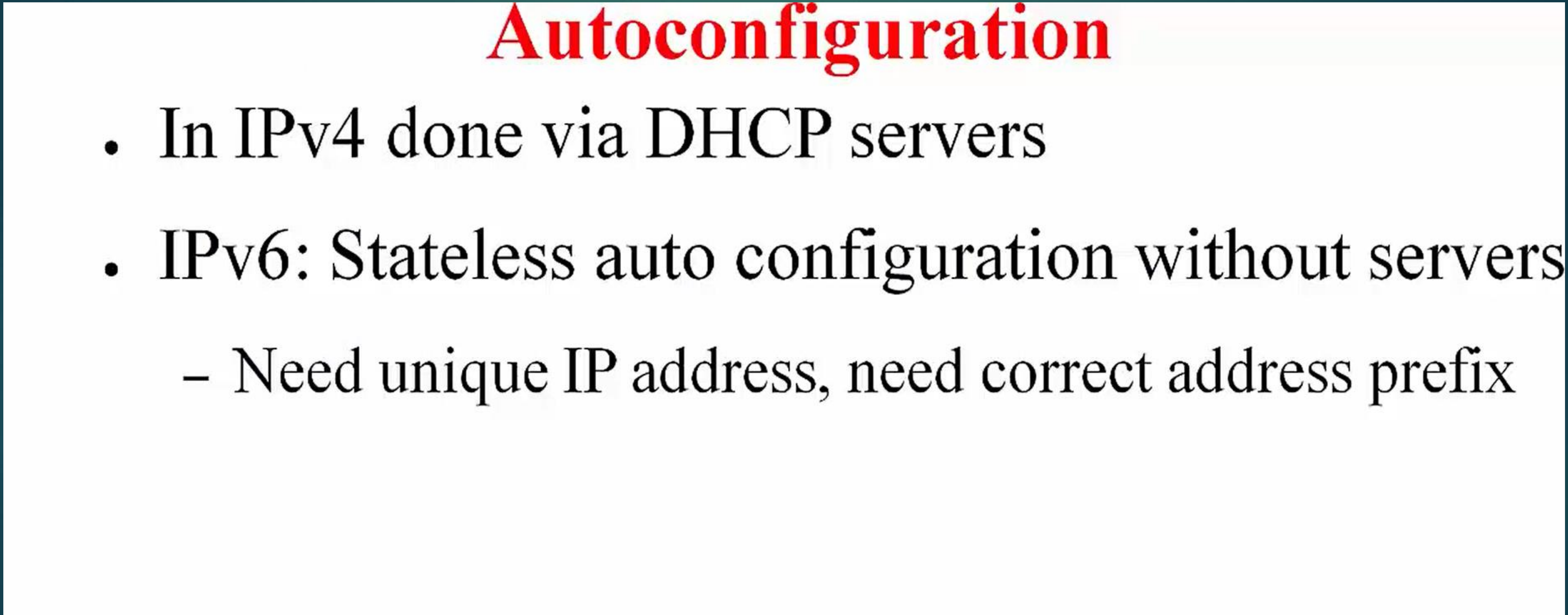
Points to Note

- 128 bit addresses can support 3 * 10^{38} hosts
- Fast router processing
  - Streamlined header of 40 bytes
  - No checksum, no fragmentation
- Support for real-time applications via traffic class and flow label



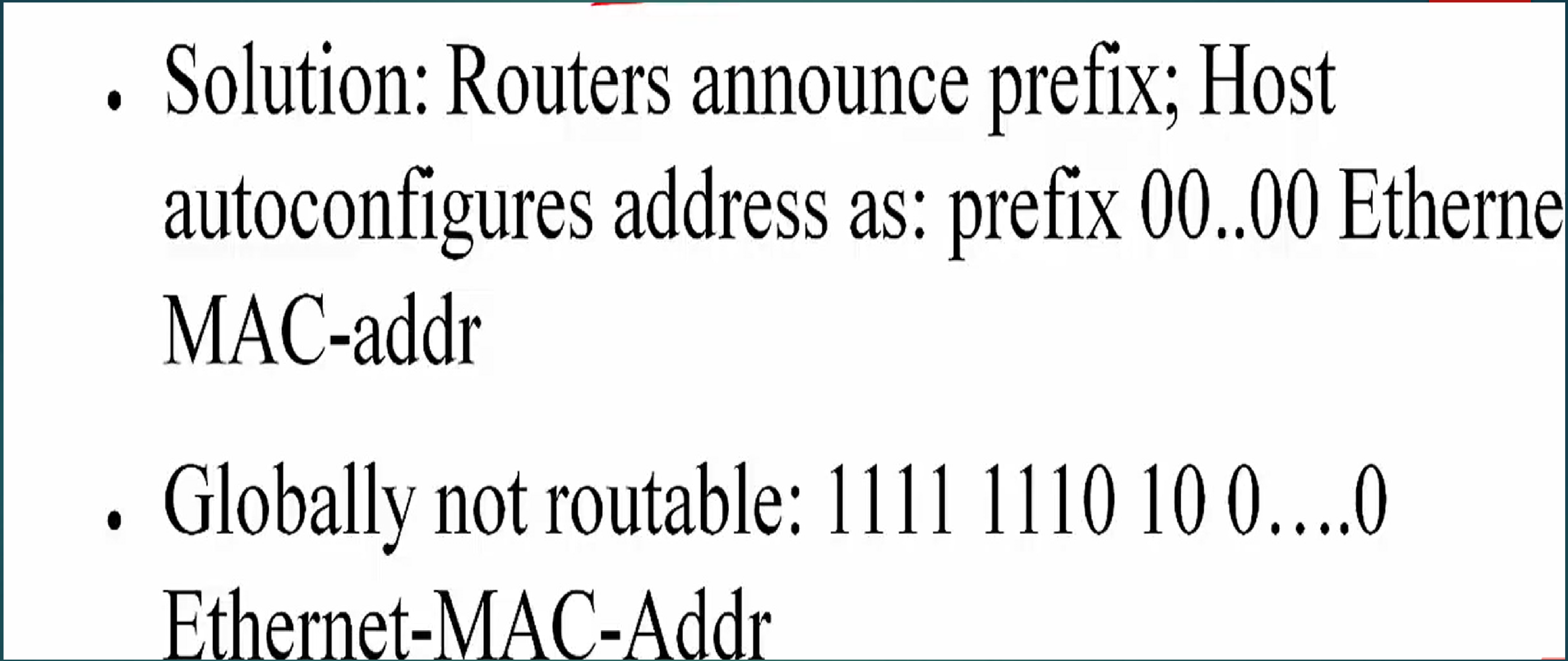
Addressing

- 128 bits → $3 * 10^{38}$ nodes
  - Consider entire surface of earth; $7 * 10^{23}$ IP addresses per square foot
  - $4.354 \pm 0.012 \times 10^{23}$ micro seconds since Big Bang
- Notation: x:x:x:x:x:x:x:x
  - X is hexadecimal representation of 16 bit piece of address
  - E.g: 2001:0DB8:0000:0000:95CD:BBE0:000B:0001
  - Short form: 2001:DB8::95CD:BBE0:B:1

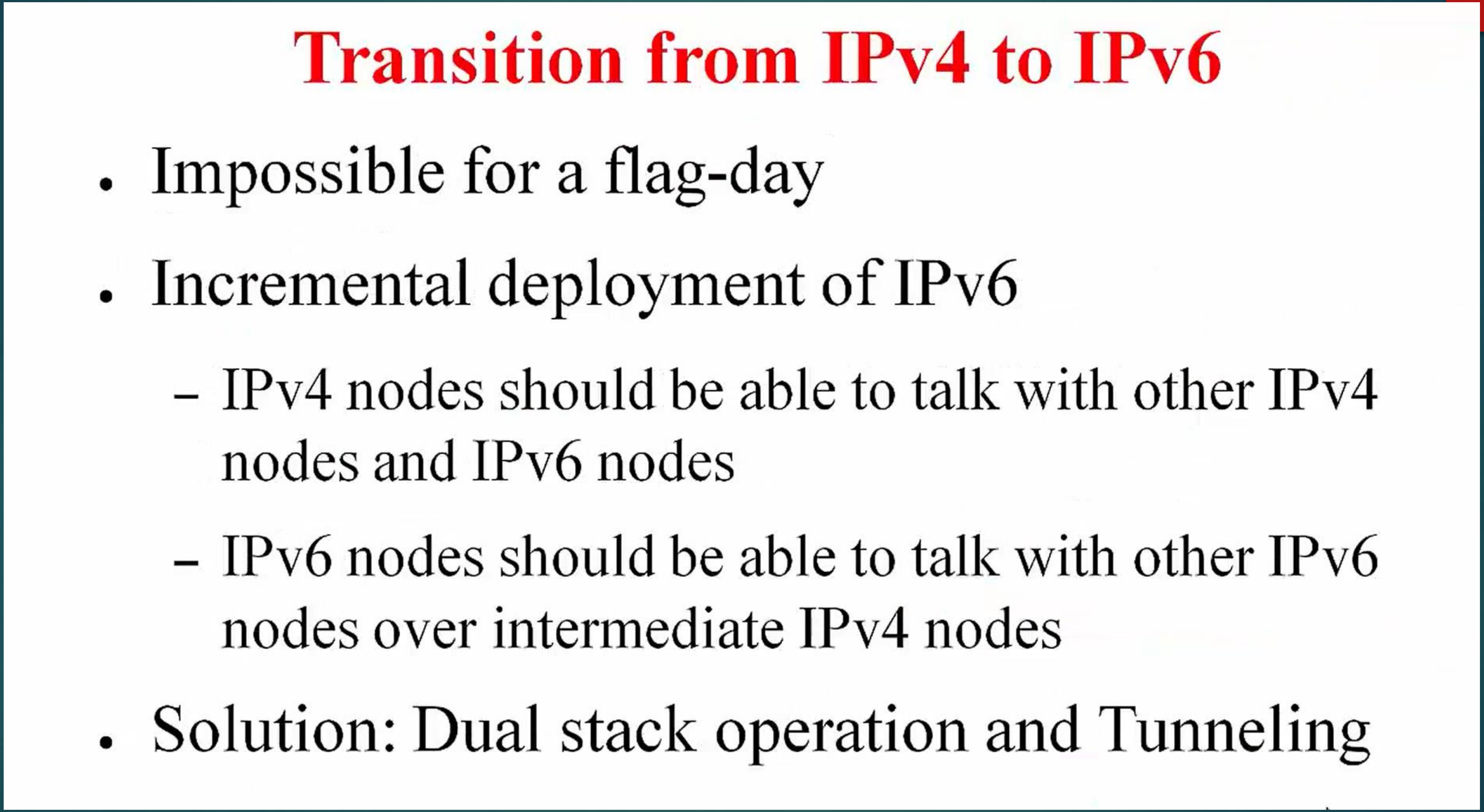


Autoconfiguration

- In IPv4 done via DHCP servers
- IPv6: Stateless auto configuration without servers
  - Need unique IP address, need correct address prefix

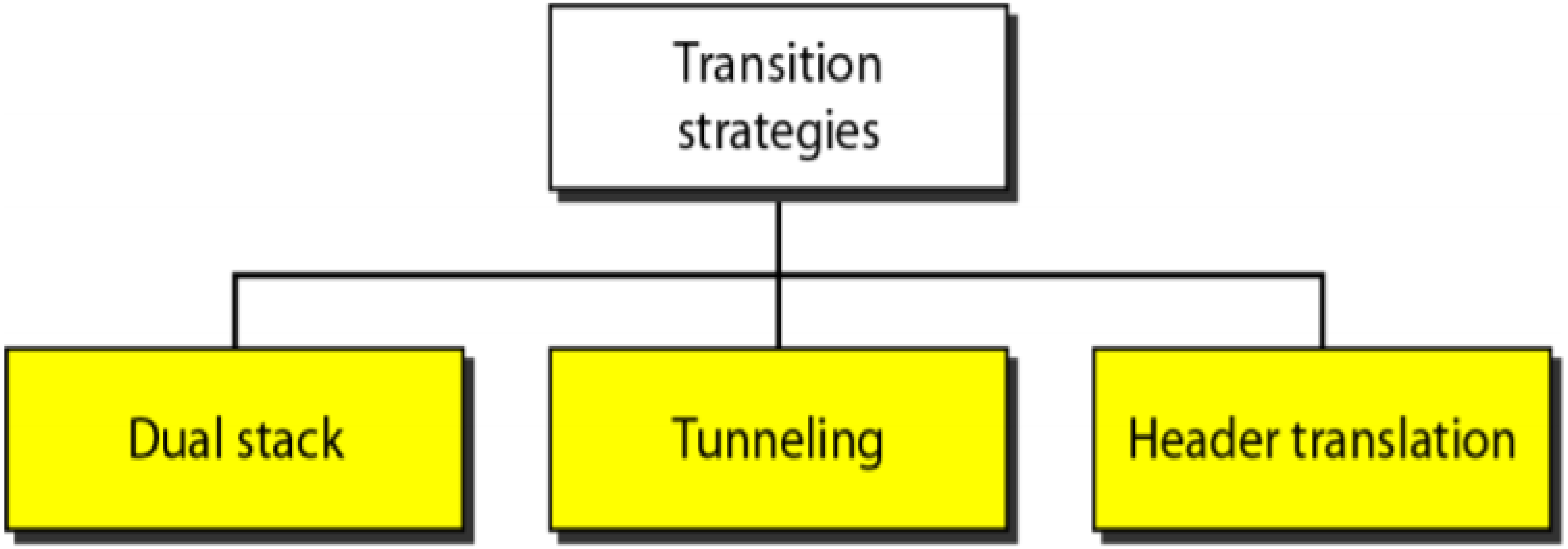


- Solution: Routers announce prefix; Host autoconfigures address as: prefix 00..00 Etherne MAC-addr
- Globally not routable: 1111 1110 10 0….0 Ethernet-MAC-Addr



Transition from IPv4 to IPv6

- Impossible for a flag-day
- Incremental deployment of IPv6
  - IPv4 nodes should be able to talk with other IPv4 nodes and IPv6 nodes
  - IPv6 nodes should be able to talk with other IPv6 nodes over intermediate IPv4 nodes
- Solution: Dual stack operation and Tunneling



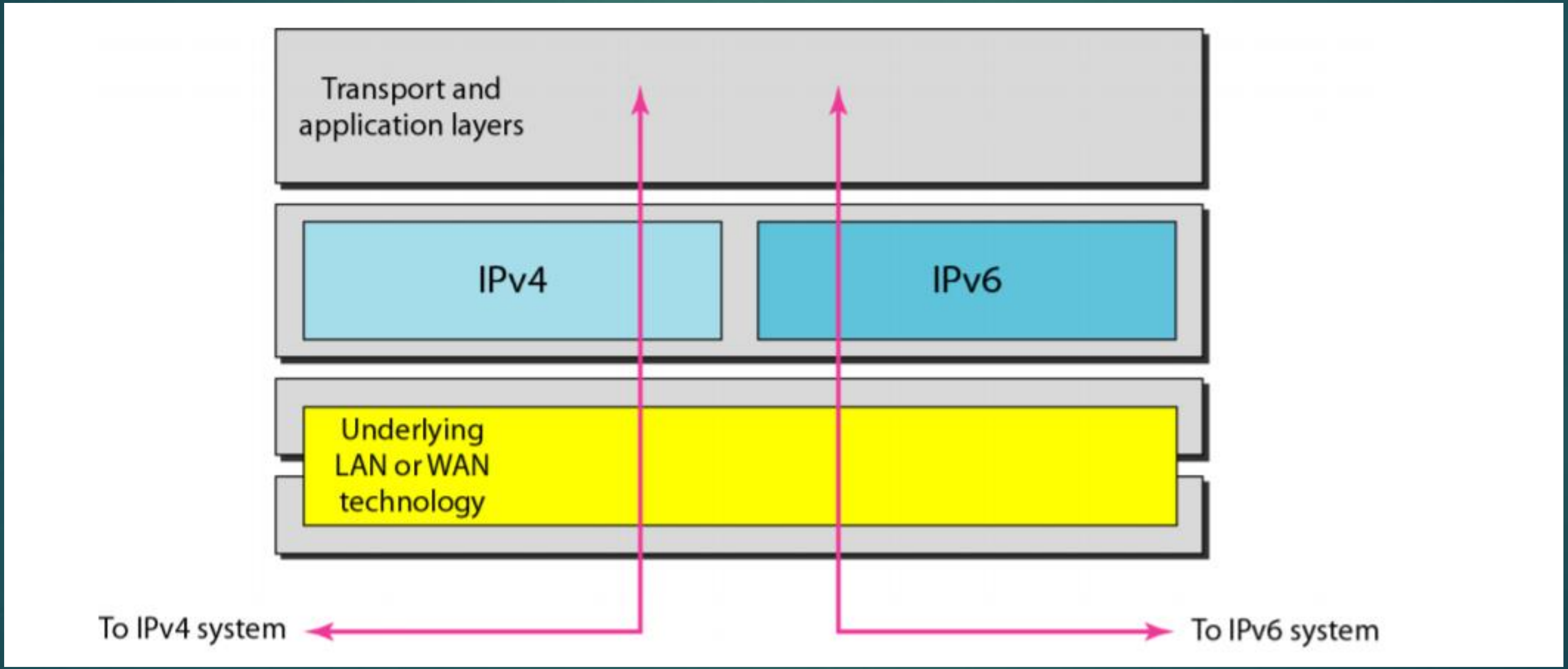
Transition strategies

Dual stack

Tunneling

Header translation

Dual Stack


Transport and application layers
IPv4
IPv6
Underlying LAN or WAN technology
To IPv4 system
To IPv6 system

IP Tunneling

- In the physical world, tunneling is a way to cross terrain or boundaries that could not normally be crossed.
- Similarly, in networking, tunnels are a method for transporting data across a network using protocols that are not supported by that network.
- Tunneling works by encapsulating packets: wrapping packets inside of other packets. (Packets are small pieces of data that can be re-assembled at their destination into a larger file.)
- Tunneling is often used in virtual private networks
- It can also set up efficient and secure connections between networks, enable the usage of unsupported network protocols, and in some cases allow users to bypass firewalls.

IPv6 over IPv4 Tunneling

- Point-to-point tunnels made by encapsulating IPv6 packets within IPv4 headers
- Allows isolated IPv6 end systems to communicate without the need to upgrade the IPv4 infrastructure
- Transition mechanisms:

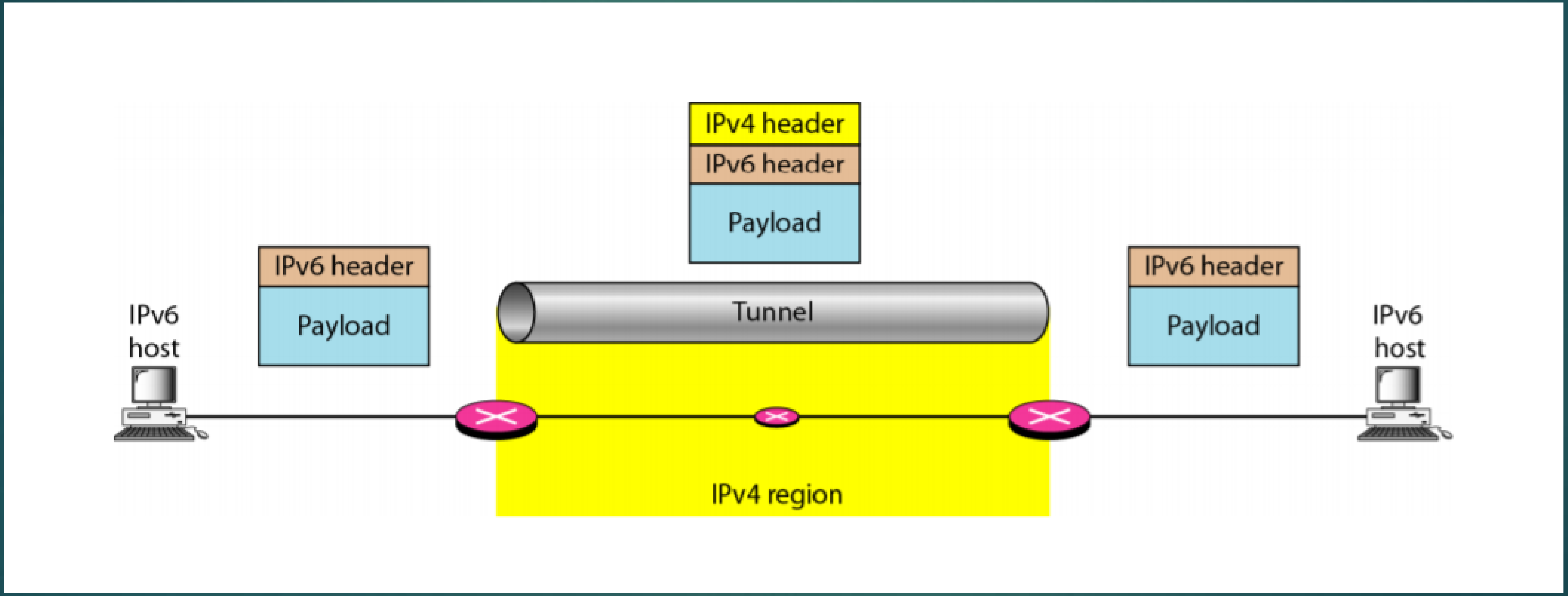
i. Manually configured IPv6 over IPv4 tunnelling

ii. IPv6 over IPv4 GRE tunneling

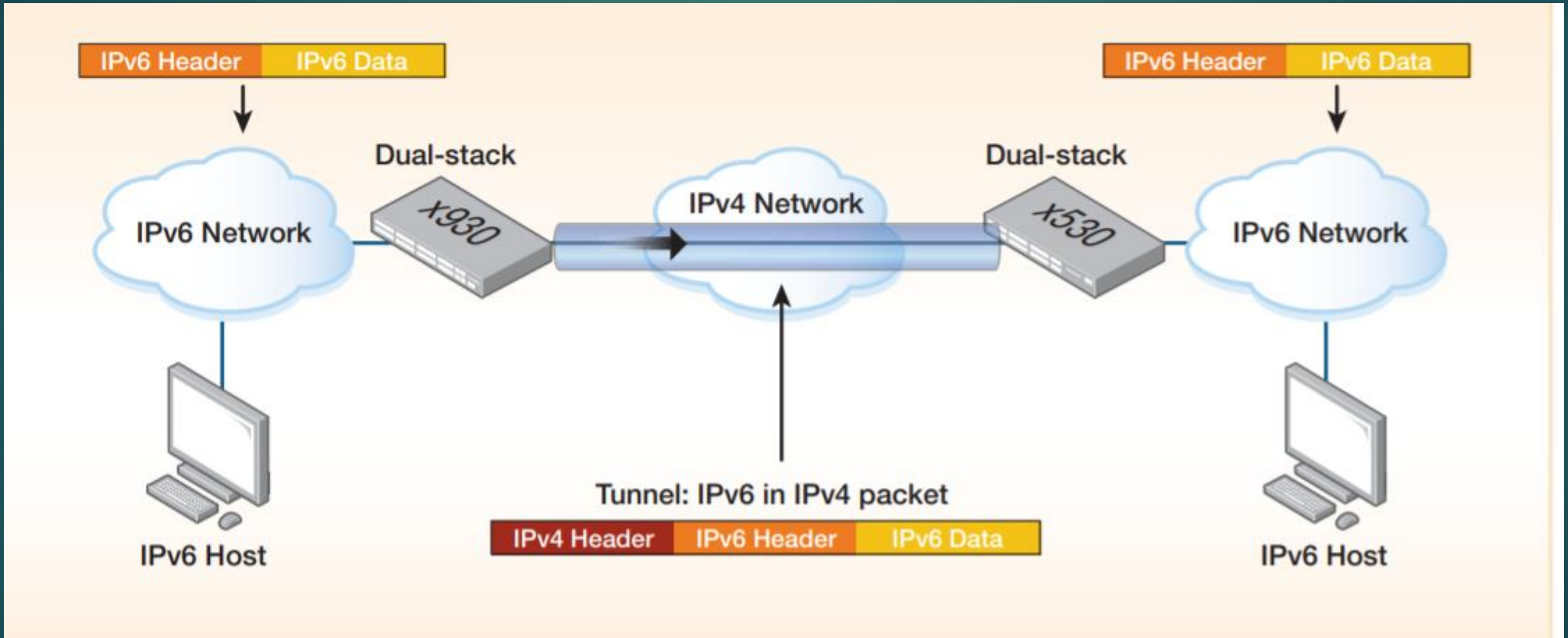
iii. Semi-automatic tunneling

iv. Fully automatic tunneling

Tunneling


IPv4 header
IPv6 header
Payload
IPv6 header
Payload
Tunnel
IPv6 header
Payload
IPv6 host
IPv6 host
IPv4 region

Deploying IPv6 over IPv4 tunnels

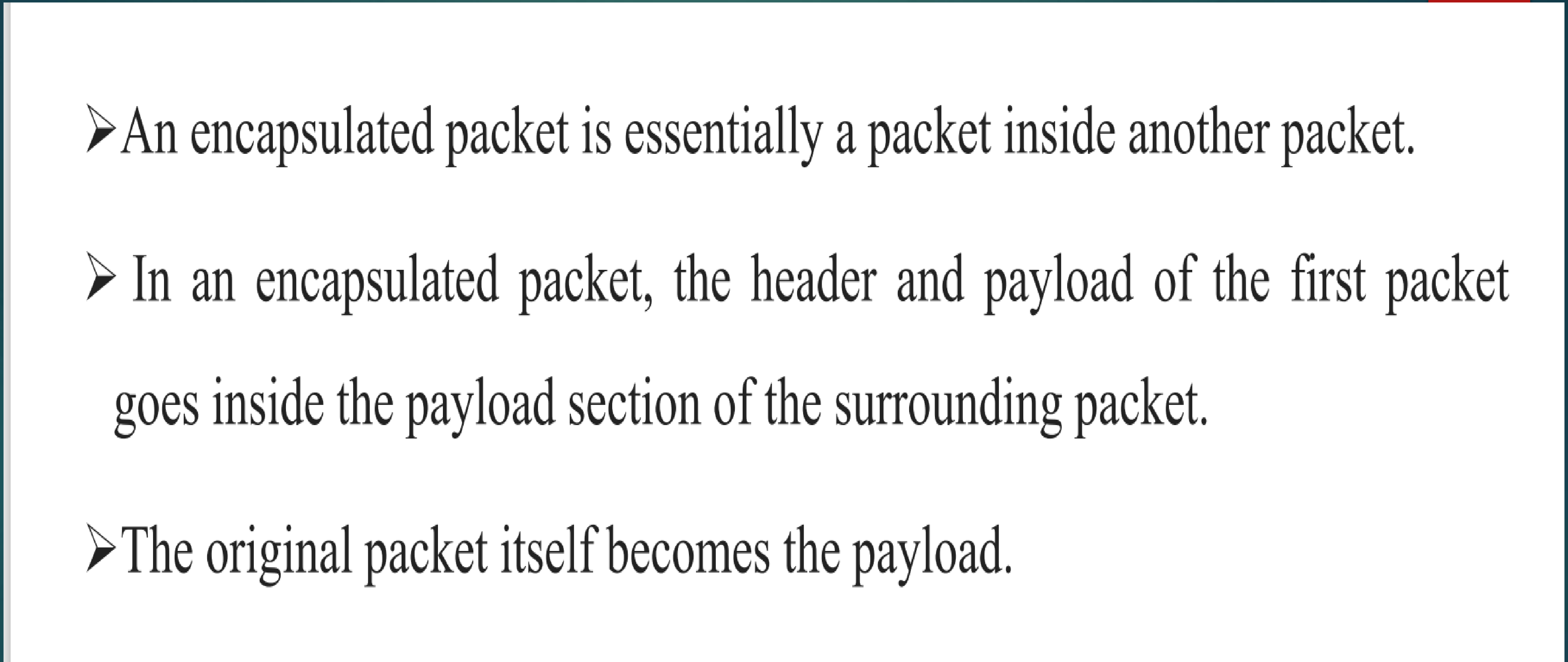


Tunneling requirements

- Endpoints must run in dual-stack mode
- Appropriate entries in a DNS that map between host names and IP addresses for both IPv4 and IPv6

Packet Encapsulation

- ➢Encapsulation means Hiding something inside.
- ➢Encapsulation is also called as Tunneling
- ➢Data traveling over a network is divided into packets.
- ➢ A typical packet has two parts: the header, which indicates the packet's destination and which protocol it uses, and the payload, which is the packet's actual contents.



- An encapsulated packet is essentially a packet inside another packet.
- In an encapsulated packet, the header and payload of the first packet goes inside the payload section of the surrounding packet.
- The original packet itself becomes the payload.

IP Encapsulation protocols

- GRE, IPsec, IP-in-IP, and SSH
- Point-to-Point Tunneling Protocol (PPTP)
- Secure Socket Tunneling Protocol (SSTP)
- Layer 2 Tunneling Protocol (L2TP)

GRE Encapsulation Protocol

- Generic Routing Encapsulation (GRE) is one of several tunneling protocols.
- GRE encapsulates data packets that use one routing protocol inside the packets of another protocol.
- GRE is one way to set up a direct point-to-point connection across a network, for the purpose of simplifying connections between separate networks.
- GRE adds two headers to each packet: GRE header and an IP header.
- The GRE header indicates the protocol type used by the encapsulated packet.
- The IP header encapsulates the original packet's IP header and payload.

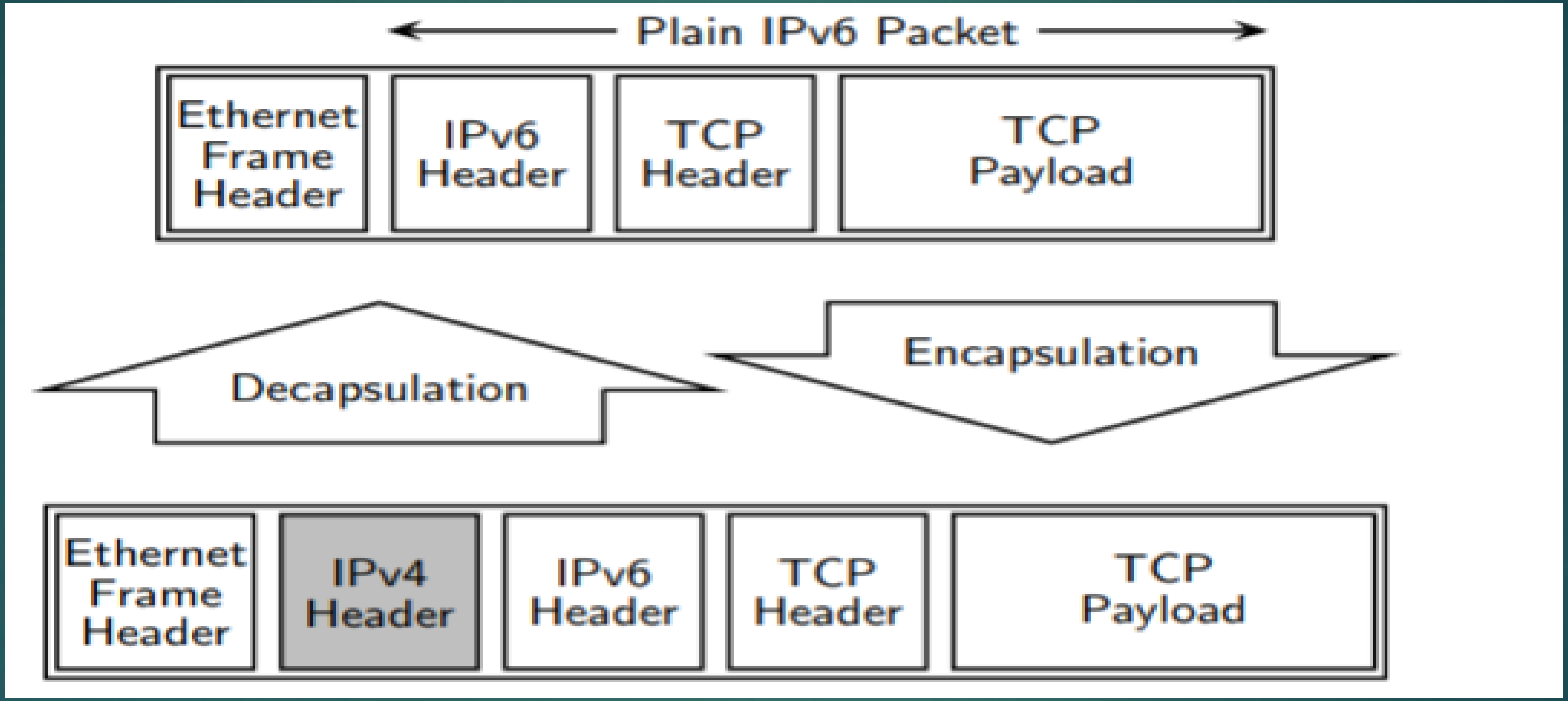
IP Sec

- IPsec is a group of protocols that are used together to set up encrypted connections between devices.
- It helps keep data sent over public networks secure.
- IPsec is often used to set up VPNs and it works by encrypting IP packets, along with authenticating the source where the packets come from.
- Within the term "IPsec," "IP" stands for "Internet Protocol" and "sec" for "secure."
- The Internet Protocol is the main routing protocol used on the Internet; it designates where data will go using IP addresses.
- IPsec is secure because it adds encryption* and authentication to this process

IP in IP Encapsulation

- IP-in-IP is a tunneling protocol for encapsulating IP packets inside other IP packets.
- Its main use is setting up network routes that would not normally be available.

IP in IP Encapsulation

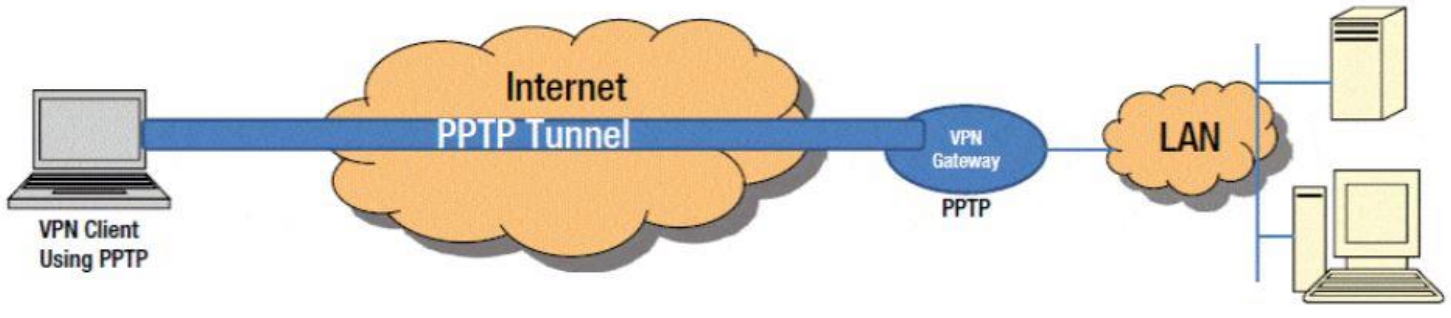


SSH

- The Secure Shell (SSH) protocol sets up encrypted connections between client and server, and can also be used to set up a secure tunnel.
- SSH operates at layer 7 of the OSI model, the application layer.

Point to Point Tunneling protocol

- PPTP is a data-link layer protocol for wide area networks (WANs) based on the Point-to-Point Protocol (PPP) and developed by Microsoft that enables network traffic to be encapsulated and routed over an unsecured public network such as the Internet.
- Remote users can securely access corporate local area network (LAN) resources using the Internet instead of having to use direct modem connections over the Public Switched Telephone Network (PSTN) or dedicated leased-line connections.



Point-to-Point Tunneling Protocol (PPTP)

- Point-to-Point Tunneling Protocol (PPTP) allows the creation of virtual private networks (VPNs), which tunnel TCP/IP traffic through the Internet.

Secure Socket Tunneling Protocol

- Secure Socket Tunneling Protocol (SSTP) is a form of virtual private network (VPN) tunnel that provides a mechanism to transport PPP traffic through an SSL/TLS channel.

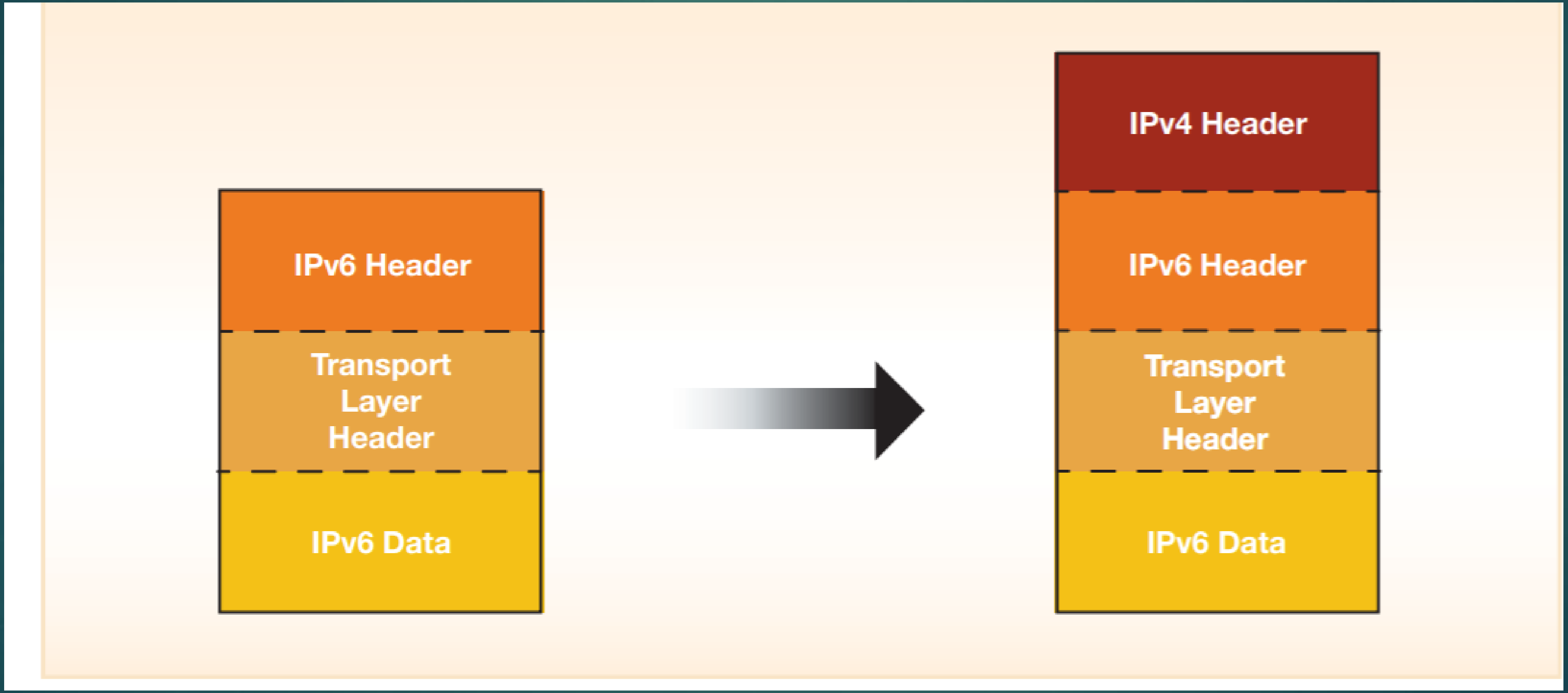
- SSL/TLS provides transport-level security with key negotiation, encryption and traffic integrity checking.

Layer2 Tunneling protocol

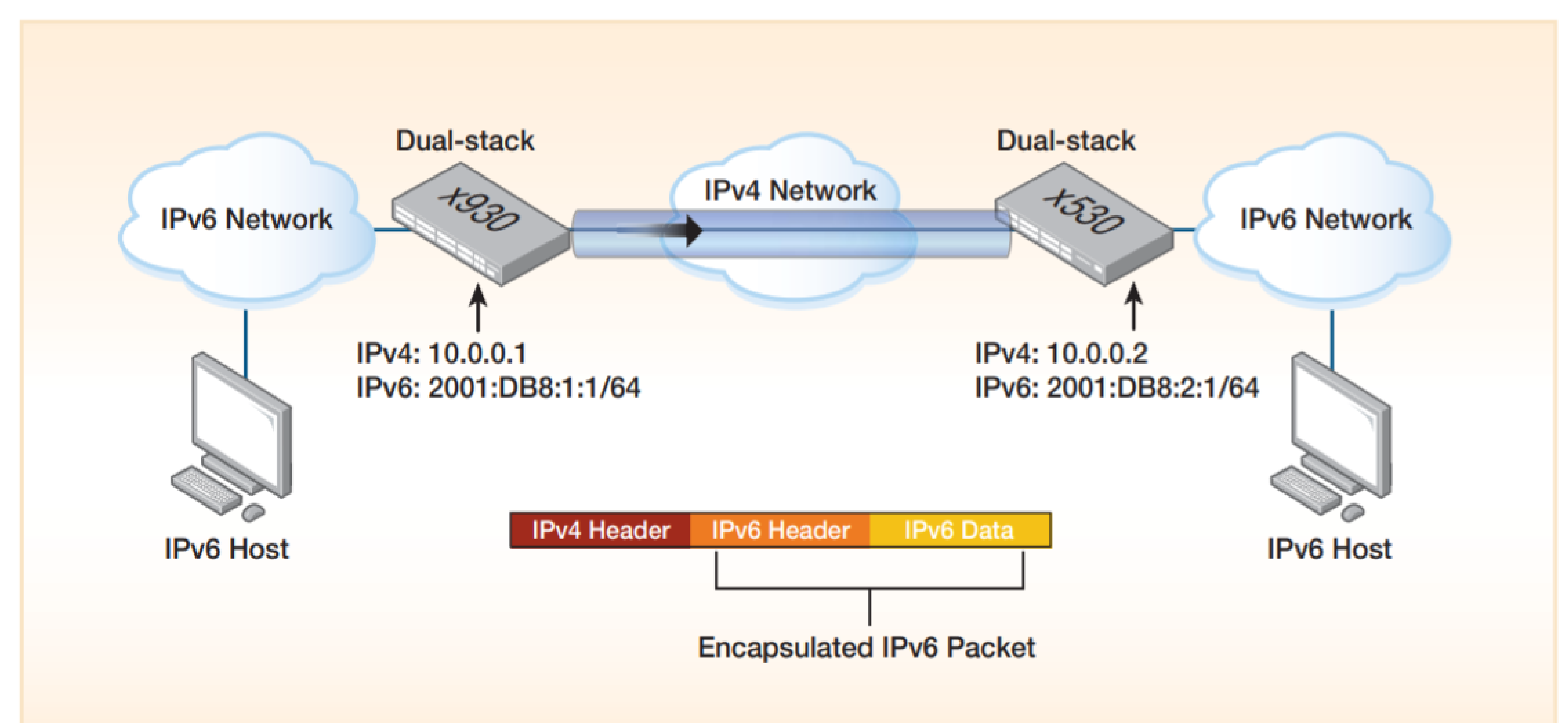
- Layer 2 Tunneling Protocol (L2TP) is a computer networking protocol used by Internet service providers (ISPs) to enable virtual private network (VPN) operations.
- L2TP is similar to the Data Link Layer Protocol in the OSI reference model, but it is actually a session layer protocol.

  A User Datagram Protocol (UDP) port is used for L2TP communication.
- Because it does not provide any security for data such as encryption and confidentiality, an encryption protocol such as Internet Protocol security (IPsec) is often used with L2TP.

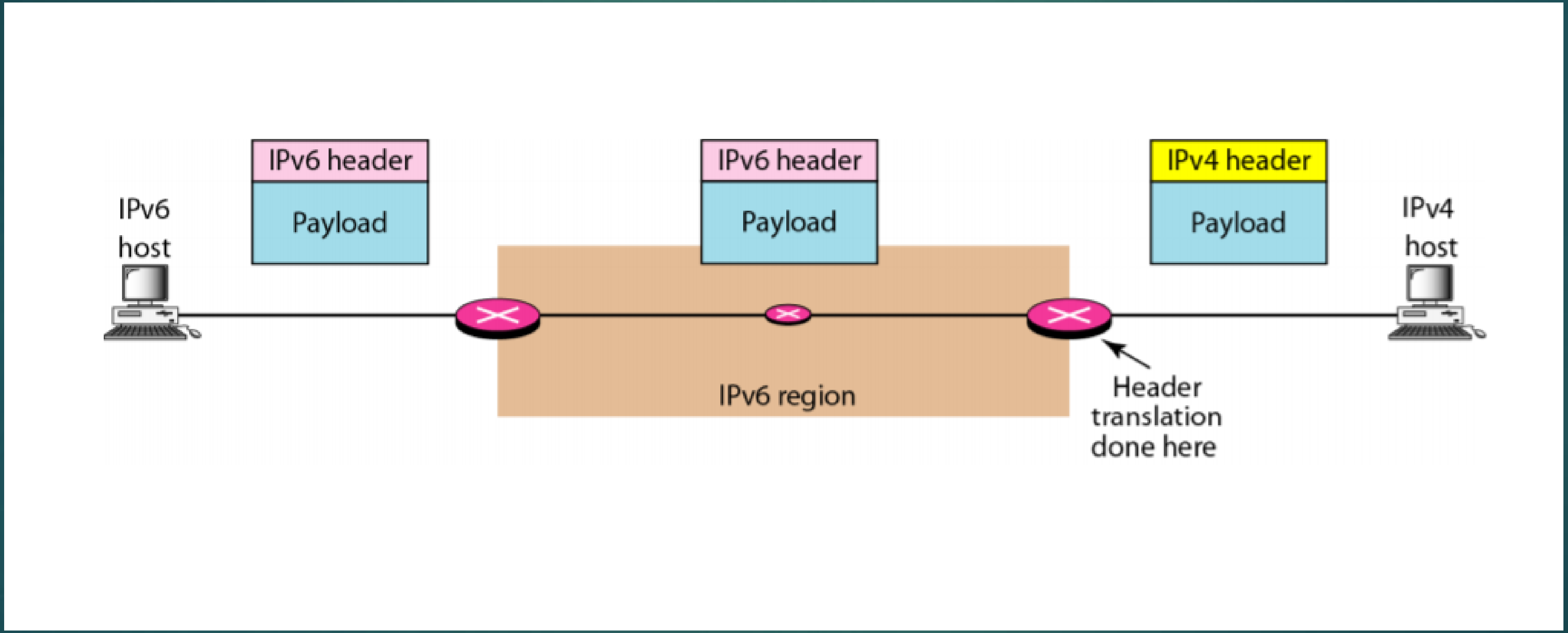
Encapsulation

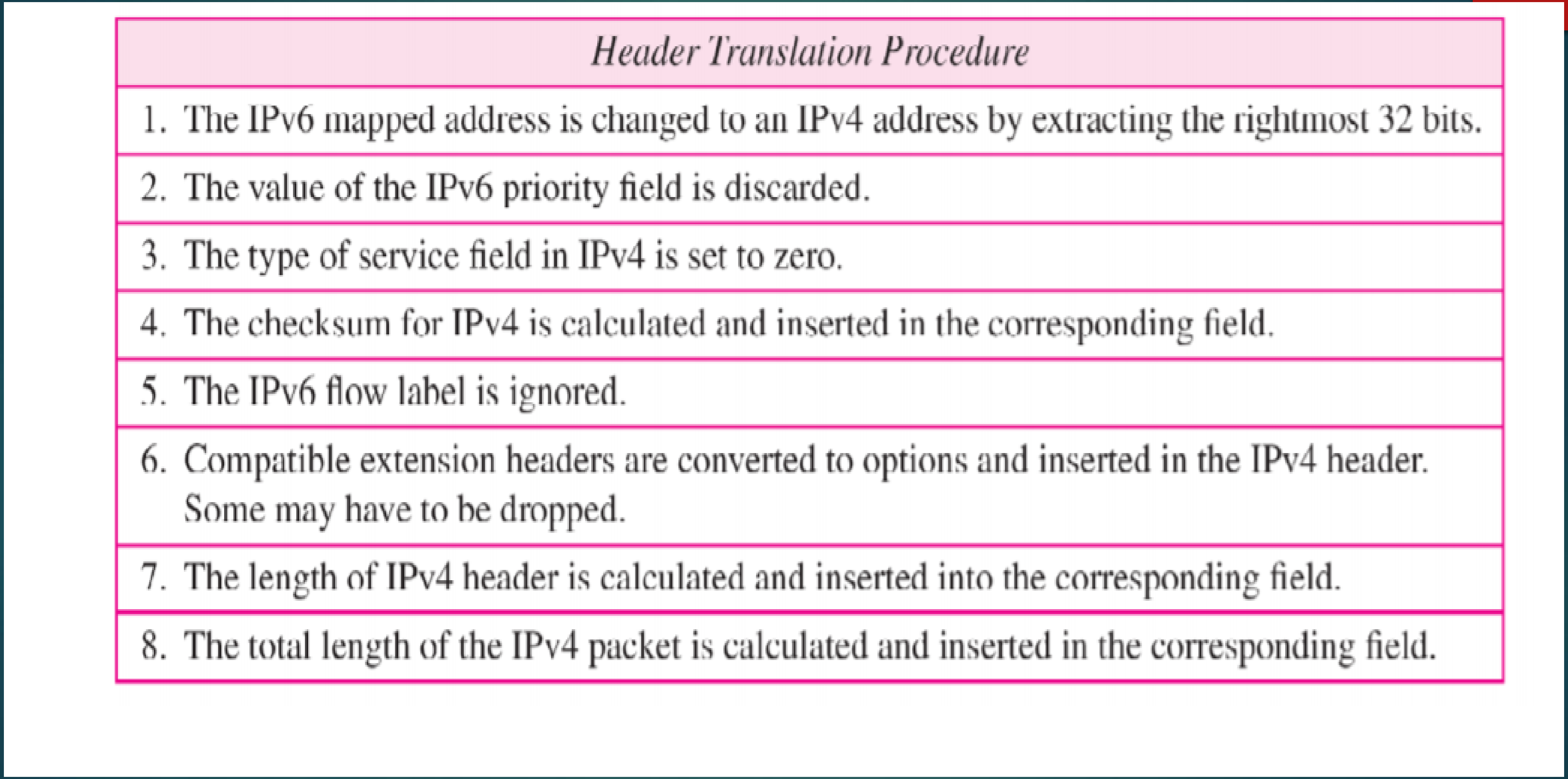


Configuration Example



Header Translation





Header Translation Procedure
1. The IPv6 mapped address is changed to an IPv4 address by extracting the rightmost 32 bits.
2. The value of the IPv6 priority field is discarded.
3. The type of service field in IPv4 is set to zero.
4. The checksum for IPv4 is calculated and inserted in the corresponding field.
5. The IPv6 flow label is ignored.
6. Compatible extension headers are converted to options and inserted in the IPv4 header. Some may have to be dropped.
7. The length of IPv4 header is calculated and inserted into the corresponding field.
8. The total length of the IPv4 packet is calculated and inserted in the corresponding field.

Thank You