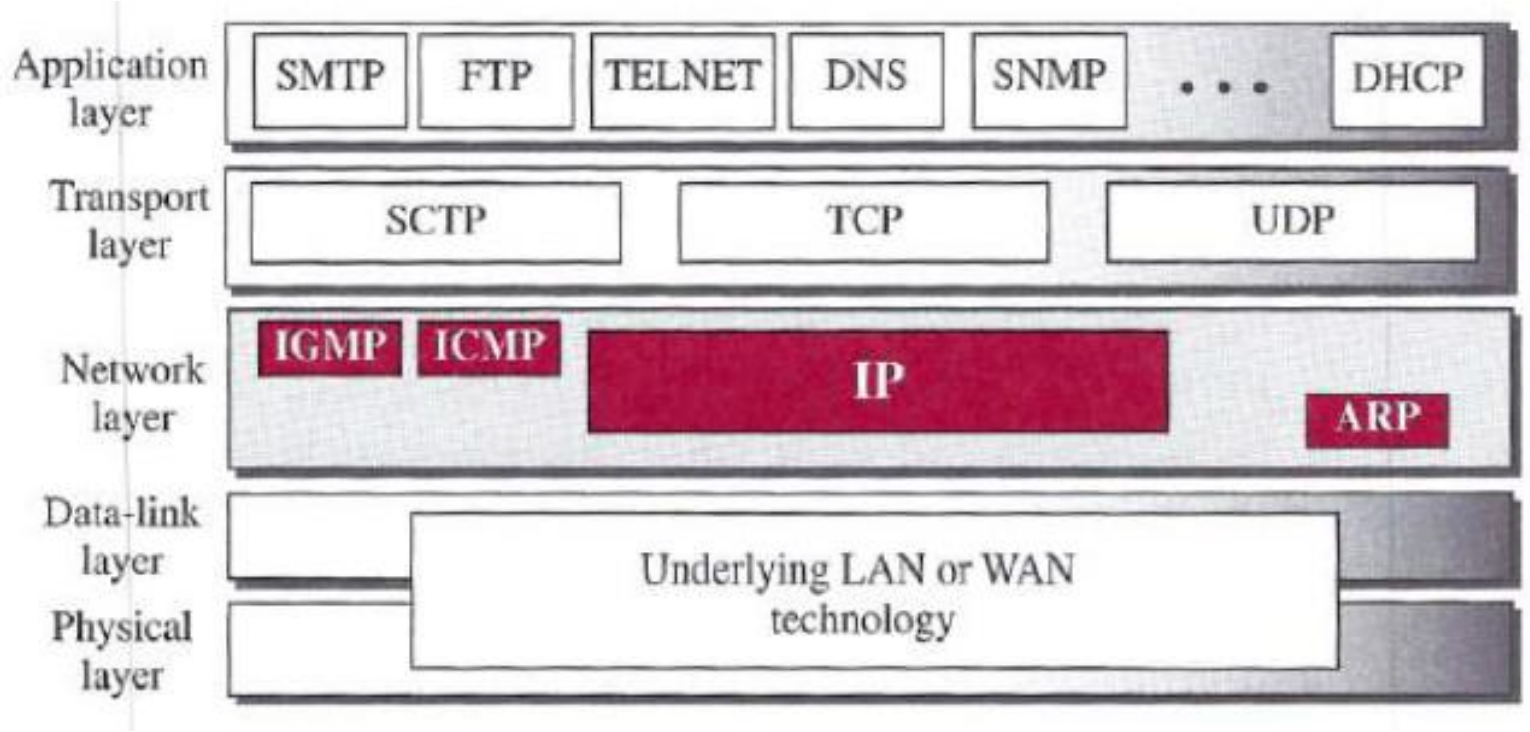
CS348: Computer Networks

IPv4 and IPv6

Dr. Manas Khatua
Assistant Professor
Dept. of CSE, IIT Guwahati
E-mail: manaskhatua@iitg.ac.in

TCP/IP Protocol Suite



- IP Addressing
- IP Packet format
- Routing Protocol
- Forwarding Rules

Internet's Network Layer

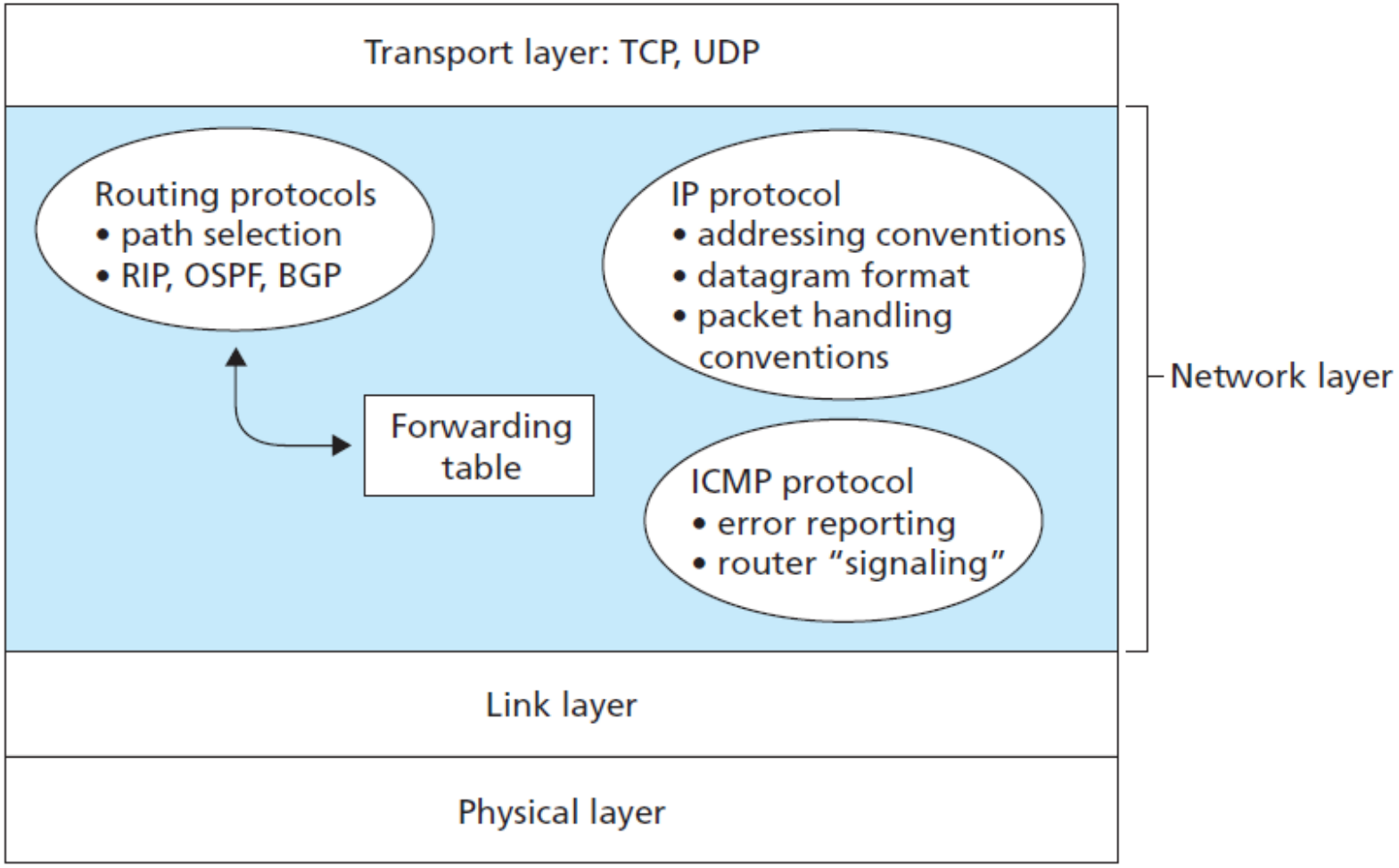
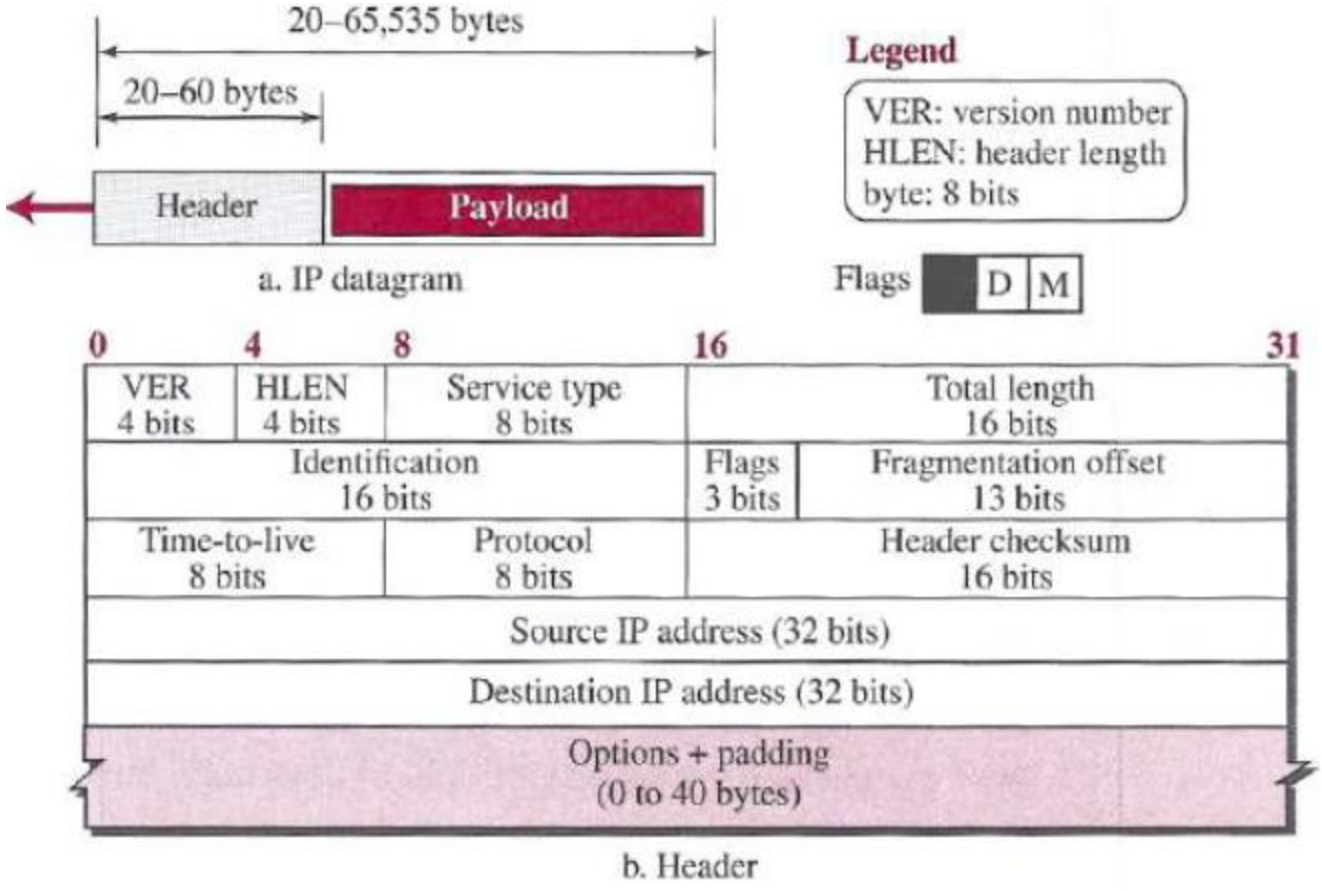


Figure 4.12 ♦ A look inside the Internet's network layer

IPv4 Header

- The most widely used protocol for internetworking is the Internet Protocol (IP).



IP Datagram Fields

- VER: version of the IPv4 protocol
- HLEN: total length of the datagram header
- ToS: provides *differentiated services* (DiffServ)
- Total length: header + data in byte

- Identification, Flags, Fragmentation Offset: These three fields are related to the fragmentation of the IP datagram
- TTL: control the maximum number of hops (routers) visited by the datagram

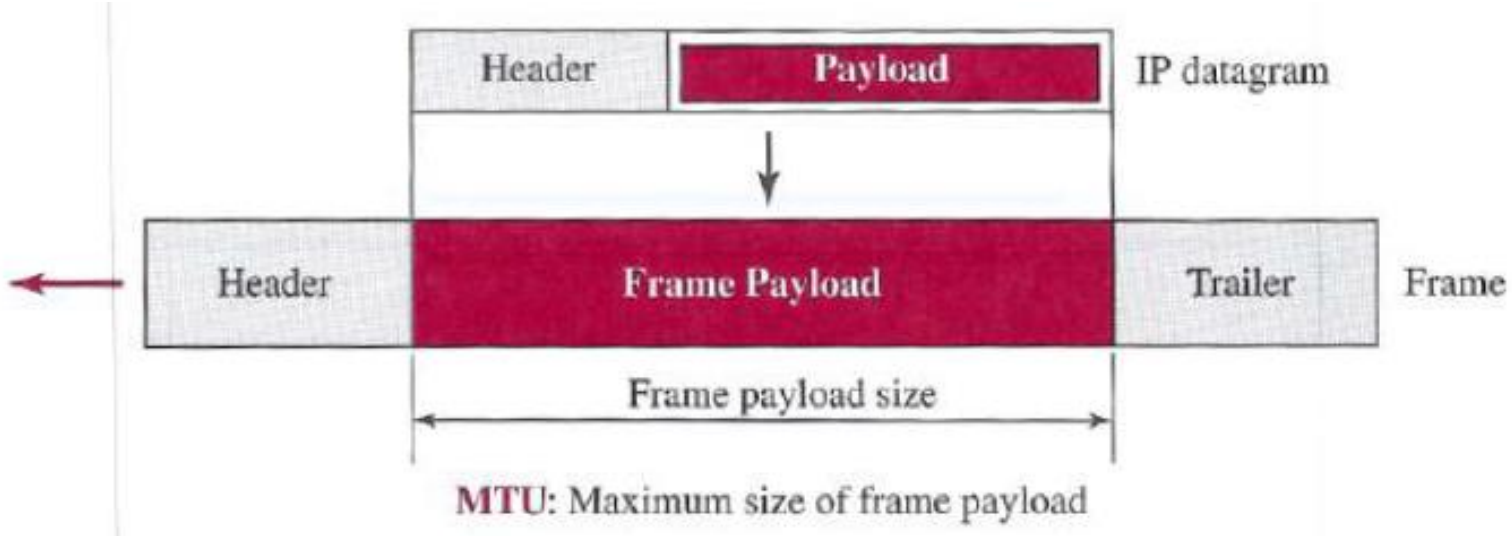
- Protocol: it defines to which protocol the payload should be delivered
- Checksum: helps to check the error in datagram header only
- Source & Destination Address: 32 bit IP addresses

- Options & Padding: used for network testing and debugging
- Payload: the packet coming from other protocols that use the service of IP

IP Fragmentation & Reassembly

- A datagram can travel through different networks.

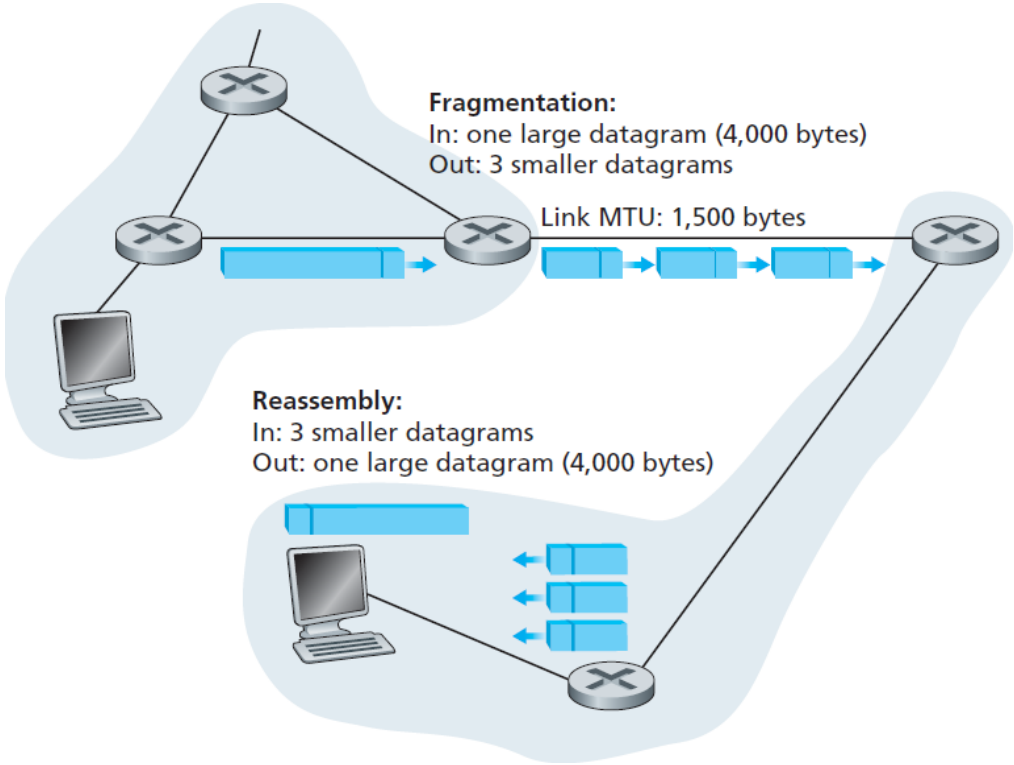
- Each router
  - decapsulates the IP datagram from the frame it receives,
  - processes it, and then
  - encapsulates it in another frame.



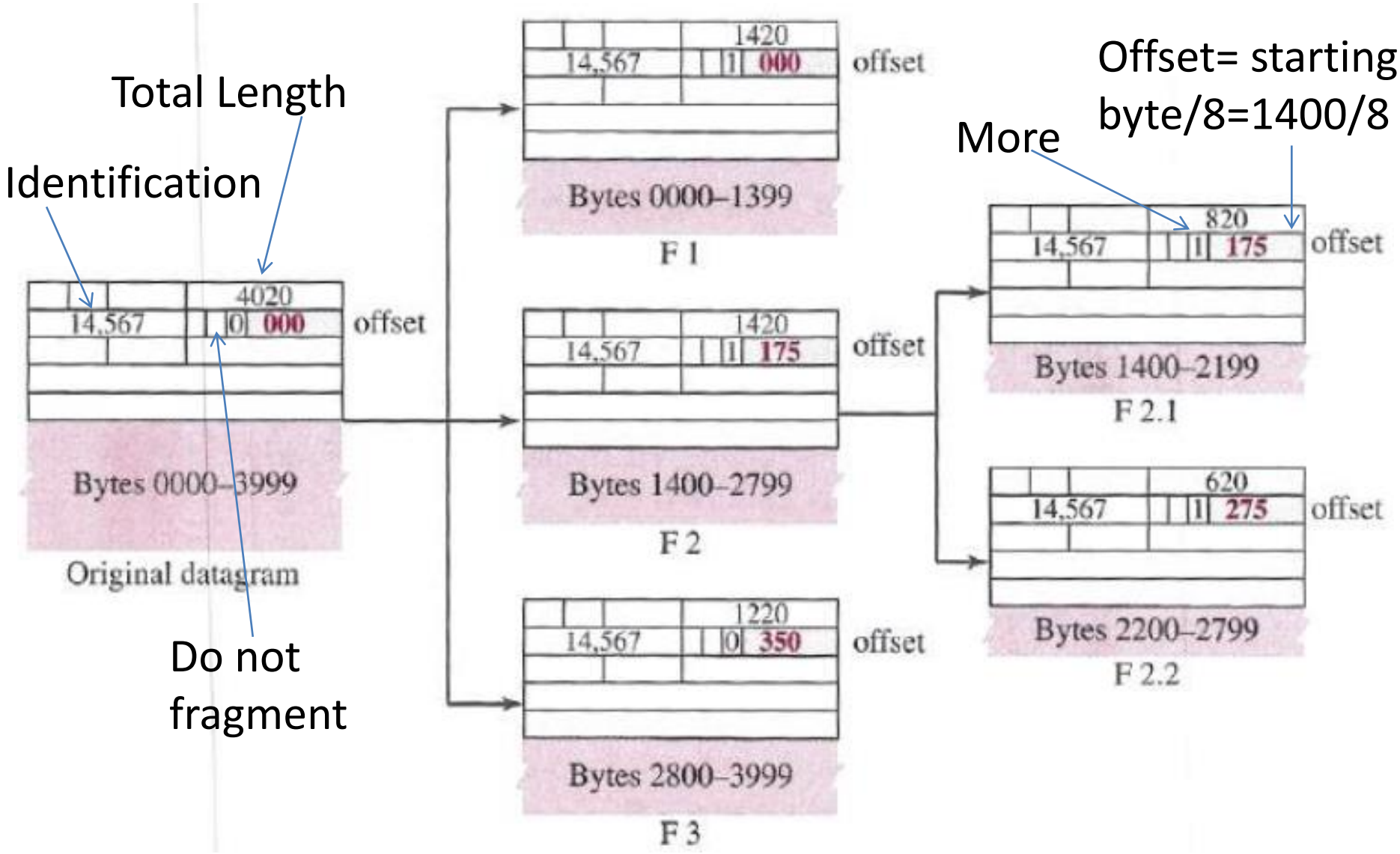
Cont…

- **Fragmentation** is done by the source host or intermediate router.
- But, **Reassembly** is done by the destination host only.

- 16-bit *identification field:* identifies a datagram uniquely. This is the present value of a counter maintained by sender.
- 3-bit flags *field:*
  - *Not used,*
  - *D: do not fragment,*
  - *M: more fragment*
- 13-bit *fragmentation offset field:* shows the relative position of a fragment w.r.t. the whole datagram



An Example

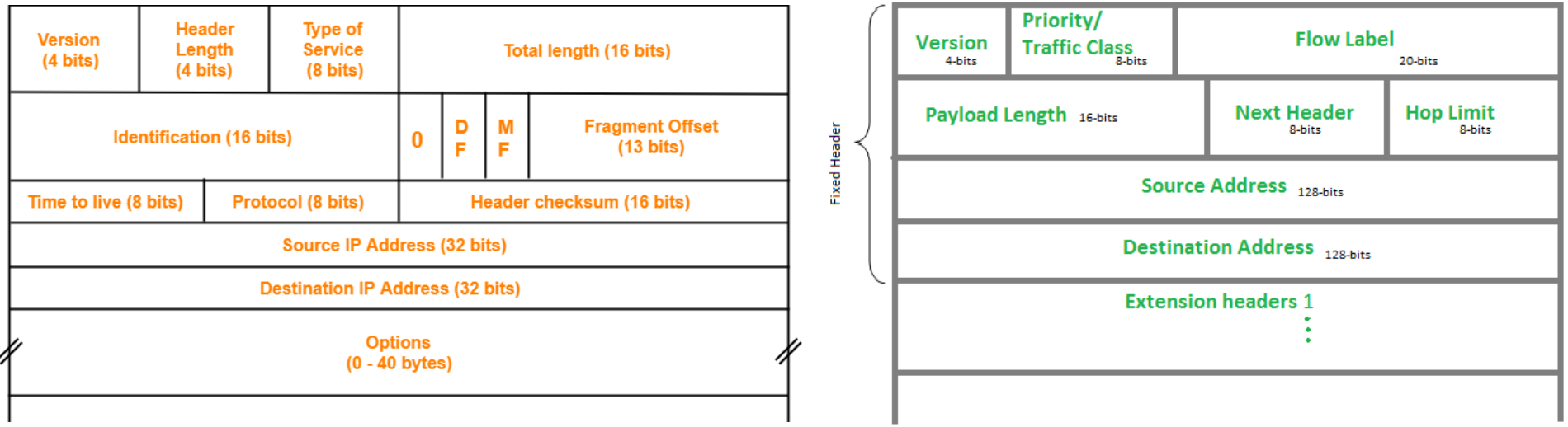

Total Length
Identification
Do not fragment
4020
14,567
0 000
offset
Bytes 0000–3999
Original datagram
1420
14,567
1 000
offset
Bytes 0000–1399
F 1
1420
14,567
1 175
offset
Bytes 1400–2799
F 2
1220
14,567
0 350
offset
Bytes 2800–3999
F 3
More
Offset= starting byte/8=1400/8
820
14,567
1 175
offset
Bytes 1400–2199
F 2.1
620
14,567
1 275
offset
Bytes 2200–2799
F 2.2

Introduction of IPv6

- In early 1990s, IETF began an effort to develop a successor to the IPv4 protocol
  - Motivation: 32-bit IP address space was beginning to be used up
  - Outcome: a new IP protocol, IPv6 with a large IP address space

- IPv6 is IP version 6 [RFC 2460]

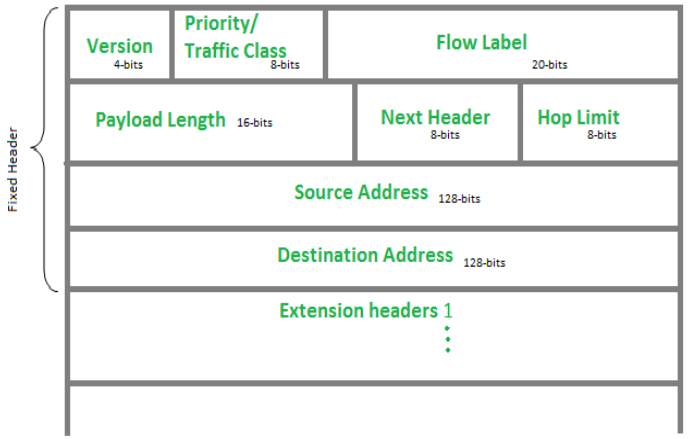
IPv4 → **IPv6**



Important Changes

- *Expanded addressing capabilities*
  - size of the IP address increased from 32 to 128 bits
  - anycast address has been introduced along with unicast and multicast addresses
- *Streamlined 40-byte header*
  - 40-byte fixed-length header allows for faster processing of the IP datagram
- *Flow labeling and priority*
  - labeling of packets belonging to particular flows for which the sender requests special handling
  - traffic class filed can be used to give priority to certain datagrams within a flow OR it can be used to give priority to datagrams from certain applications

IPv6 Datagram Format



- Version: IP version number
- Traffic class: used to give priority to certain datagram
- Flow label: used to identify a flow of datagrams
- Payload length: number of bytes in the IPv6 datagram following the fixed-length 40 byte header

- Next header: indicates Transport layer protocol (similar to as the protocol field in the IPv4 header)
- Hop limit: max. number of router a datagram can travel before reaching to destination
- Source and destination addresses: IPv6 128-bit address of source and des
- Data: payload portion of the IPv6 datagram

Few Other Changes

- Fragmentation/Reassembly
  - IPv6 does not allow for fragmentation and reassembly at intermediate routers; these operations can be performed only by the source and destination.
    - As fragmentation and reassembly are time-consuming operations
- Header checksum
  - It has been removed as transport-layer and link-layer protocols in the Internet layers perform checksumming
    - As the IPv4 header checksum needed to be recomputed atevery router due to modified value of TTL
- Options
  - no longer a part of the standard IP header. However, it can be added as next header
    - To make a fixed-length, 40 byte IP header

Transitioning from IPv4 to IPv6

- How will the public Internet, which is based on IPv4, be transitioned to IPv6?
  - One option would be to declare a flag day.
    - flag day is not possible!
  - RFC 4213 describes two other approaches
    - **dual-stack** approach, where IPv6 nodes also have a complete IPv4 implementation.
    - Such a node has the ability to send and receive both IPv4 and IPv6 datagrams
    - In the dual-stack approach, if either the sender or the receiver is only IPv4-capable, an IPv4 datagram must be used.

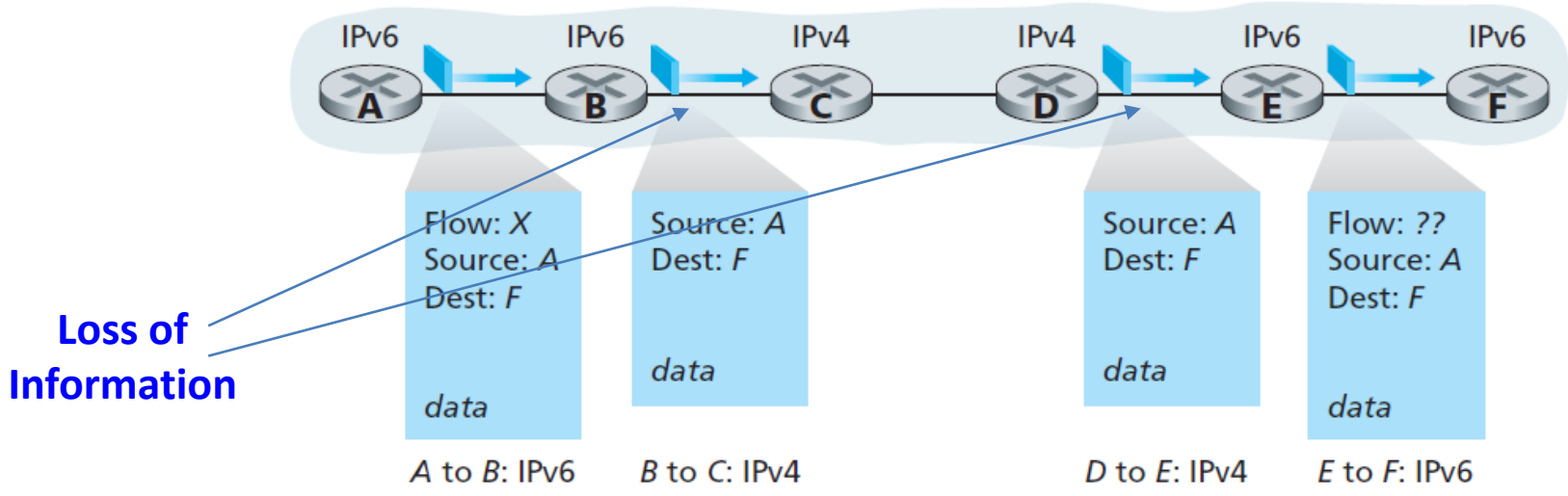


Figure 4.25 ♦ A dual-stack approach

Cont…

- An alternative to the dual-stack approach is known as **tunneling**.
  - It can solve the problem noted above (i.e. Loss of Information)

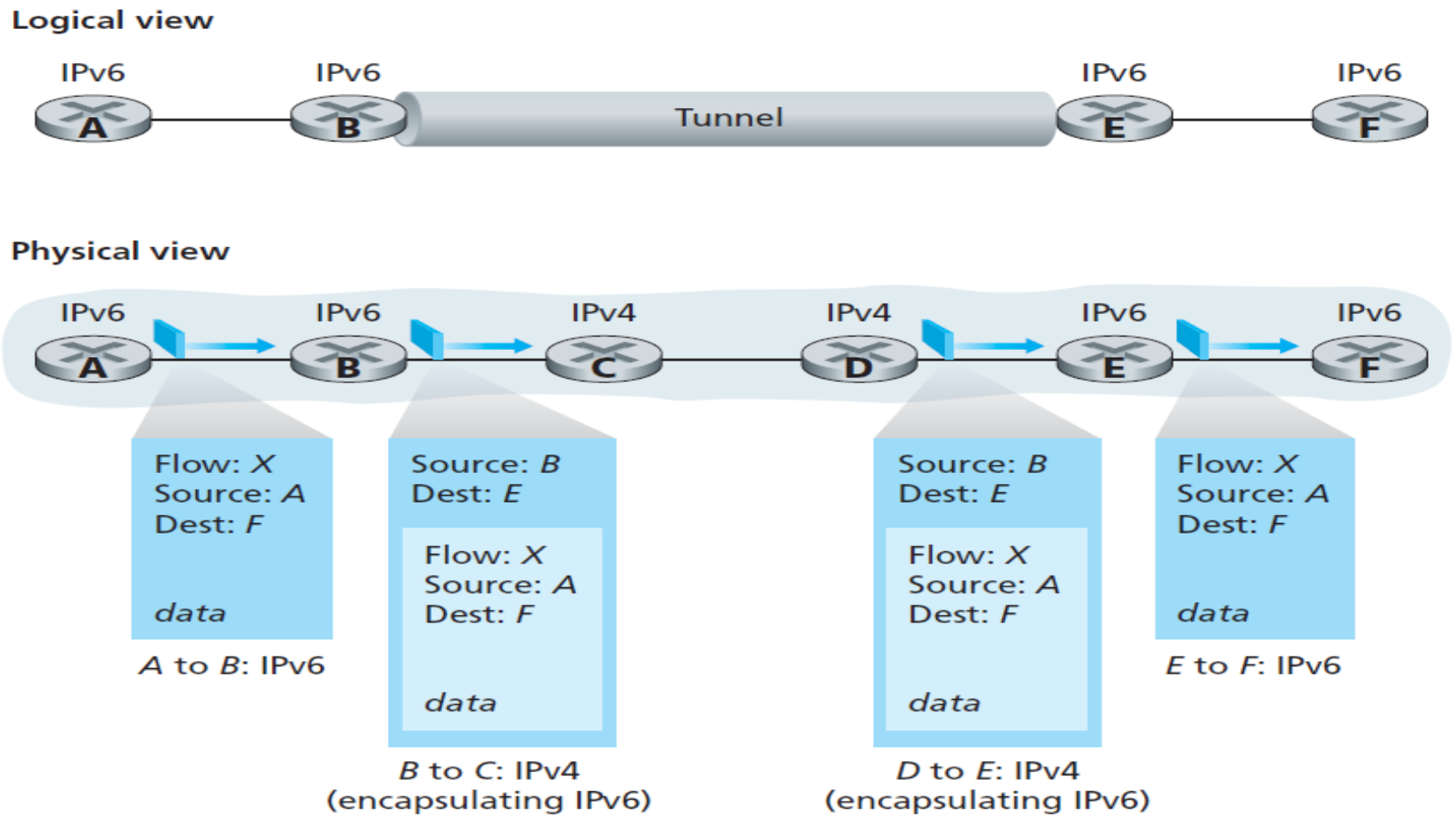


Figure 4.26 ◆ Tunneling

Cont…

- With tunneling, the IPv6 node on the sending side of the tunnel (for example, B) takes the *entire* IPv6 datagram and puts it in the data (payload) field of an IPv4 datagram.
- This IPv4 datagram is then addressed to the IPv6 node on the receiving side of the tunnel (for example, E) and sent to the first node in the tunnel (for example, C).
- So on.
- The IPv6 node on the receiving side of the tunnel eventually receives the IPv4 datagram (it is the destination of the IPv4 datagram!), determines that the IPv4 datagram contains an IPv6 datagram, extracts the IPv6 datagram, and then routes the IPv6 datagram exactly as it would if it had received the IPv6 datagram from a directly connected IPv6 neighbor.

Thanks!