COMP2001J Computer Networks

# Lecture 9 – Network Layer
## (protocols)

Dr. Shen WANG (王燊)

shen.wang@ucd.ie

# 5 weeks to go!

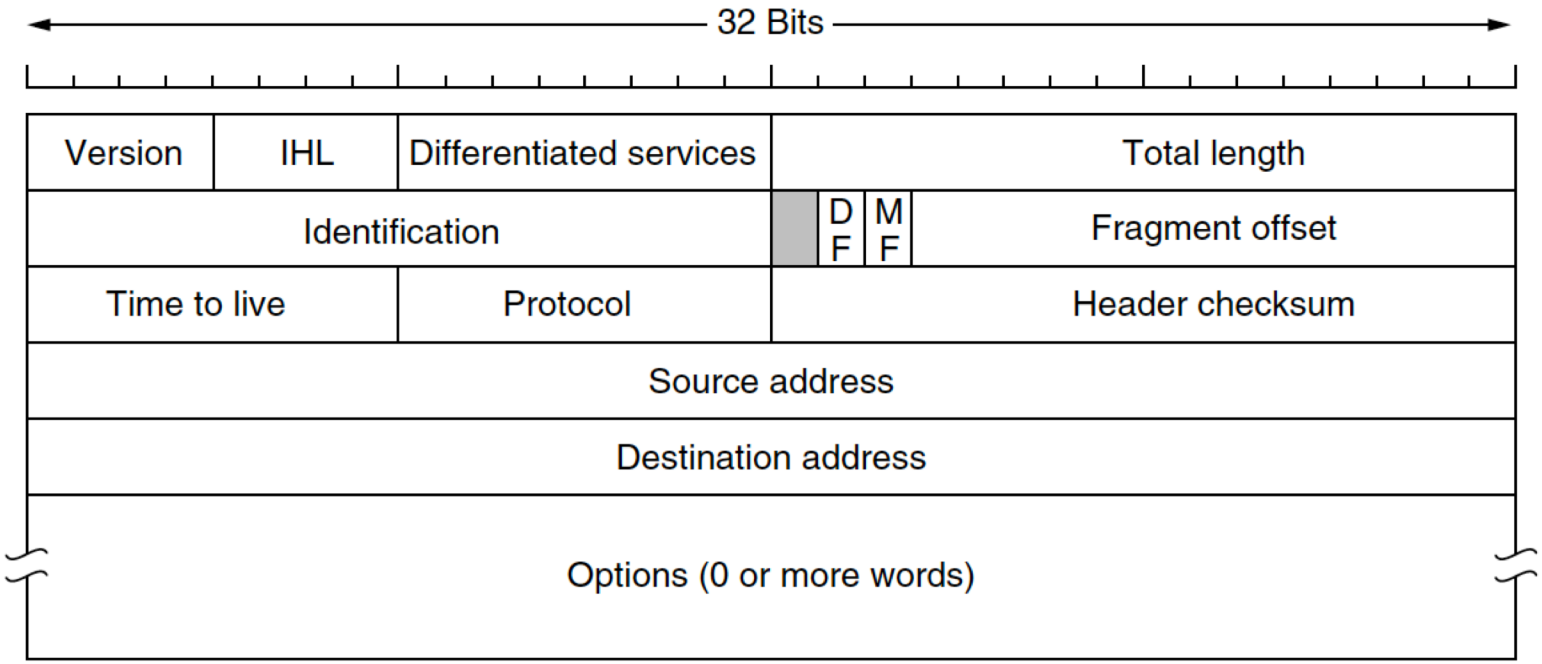
- Week 10:
  - Lecture: 25th April
- ~~Week 11:~~
  - Reading week
- Week 12:
  - Lab: 6th May (Monday), 15:25, Room 218, TB-4
  - Lab: 7th May
  - Lecture: 9th May
- Week 13, 14, 15

# Outline

- IPv4
  - Header Structure
  - Checksum
  - Fragmentation
- NAT
- IPv6
  - Compared to IPv4
- Tunnelling
- Mobile IP

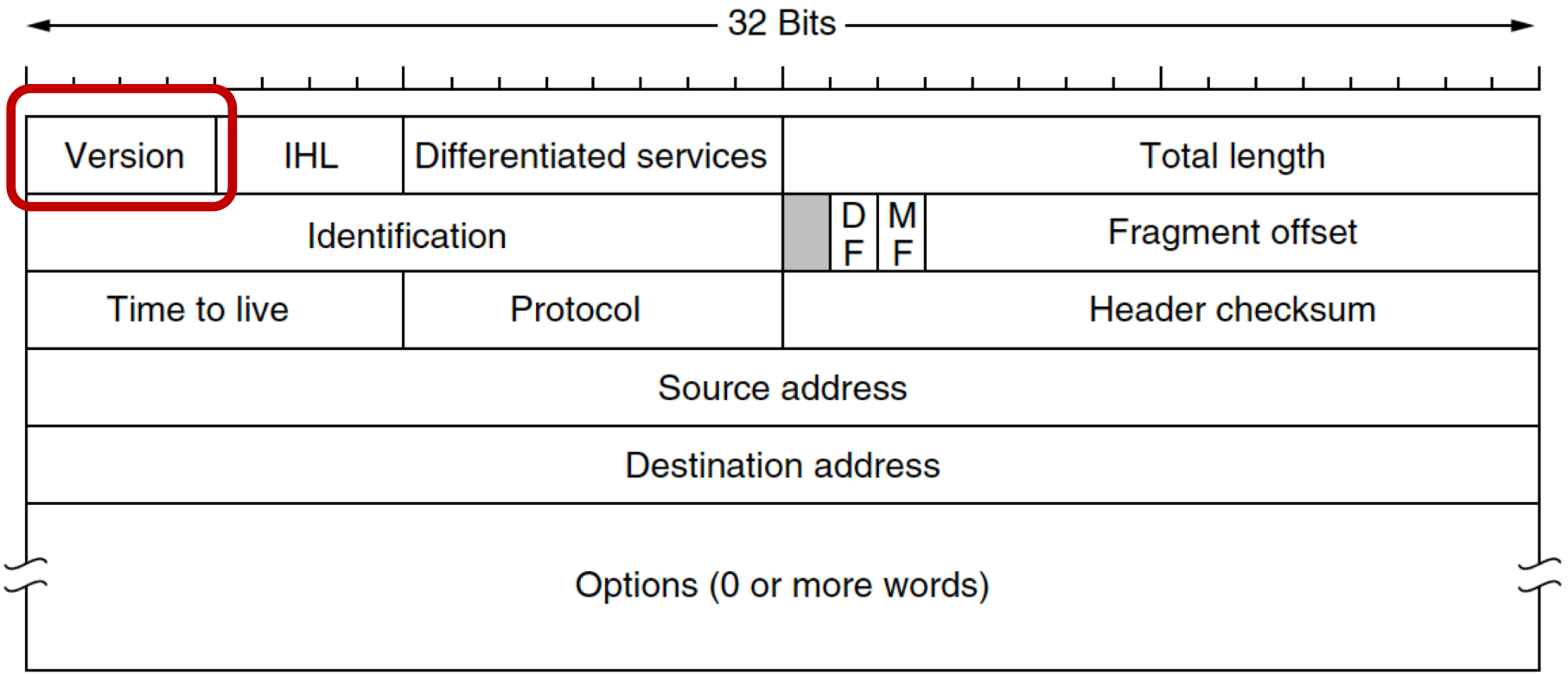
# IPv4 Header

- IPv4 (Internet Protocol) header is carried on all packets and has fields for the key parts of the protocol:



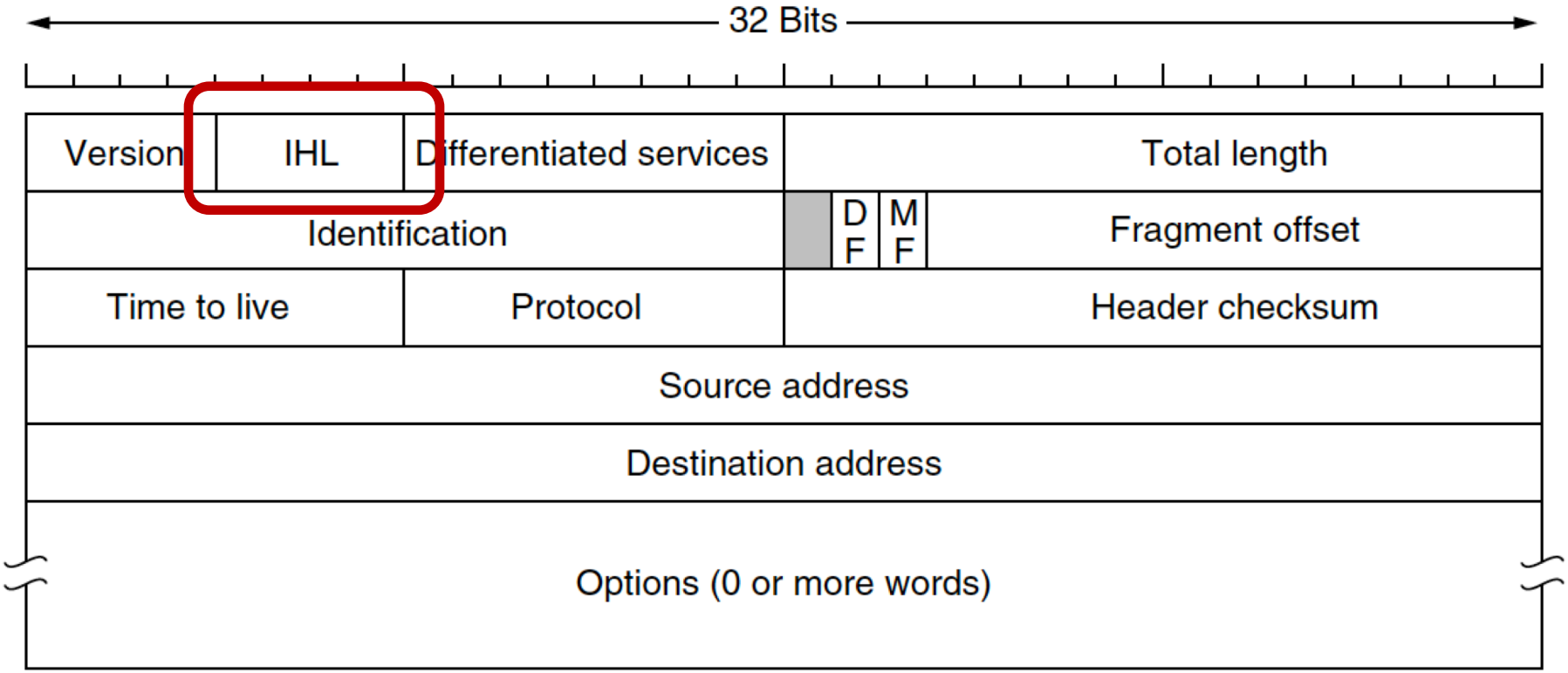
# IPv4 Header

- Version: IPv4 or v5 or v6



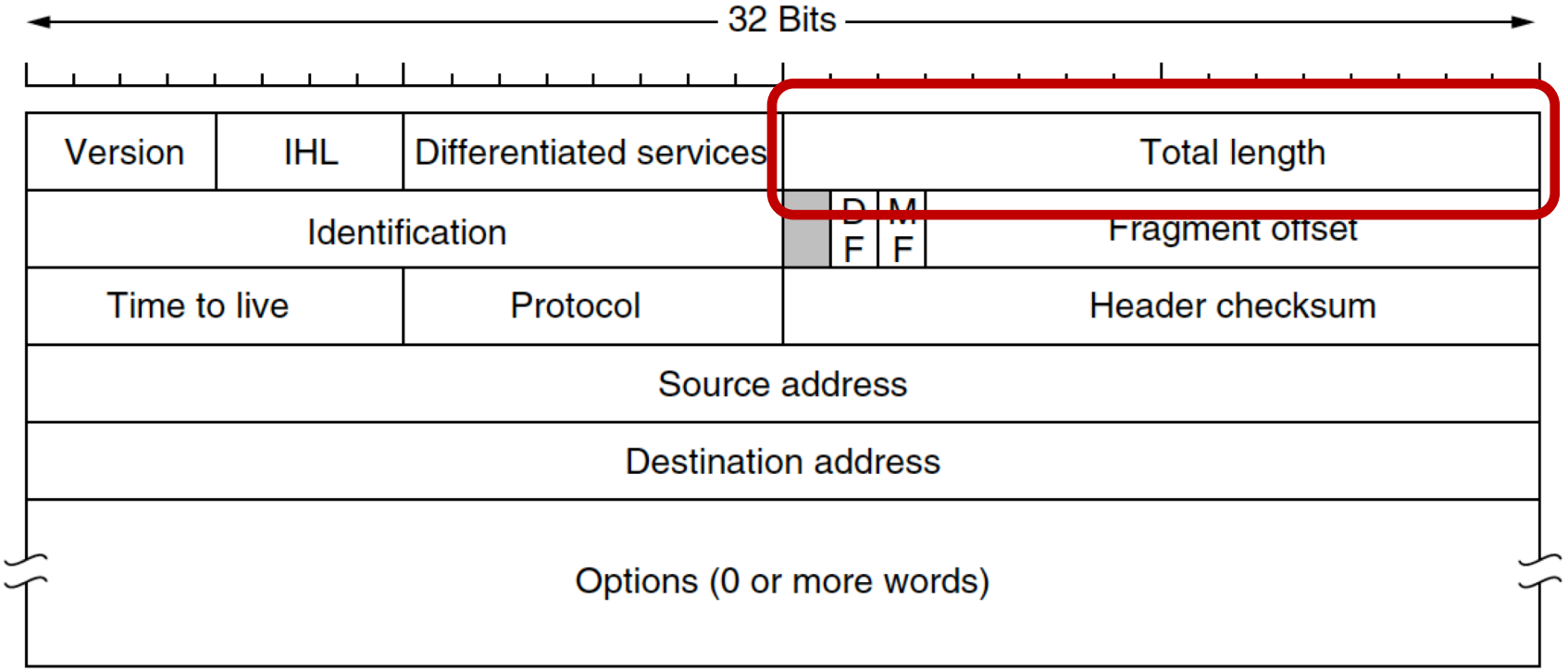
# IPv4 Header

- IHL: IP Header Length
  - 5~15, max:15*__4bytes__ = 60bytes



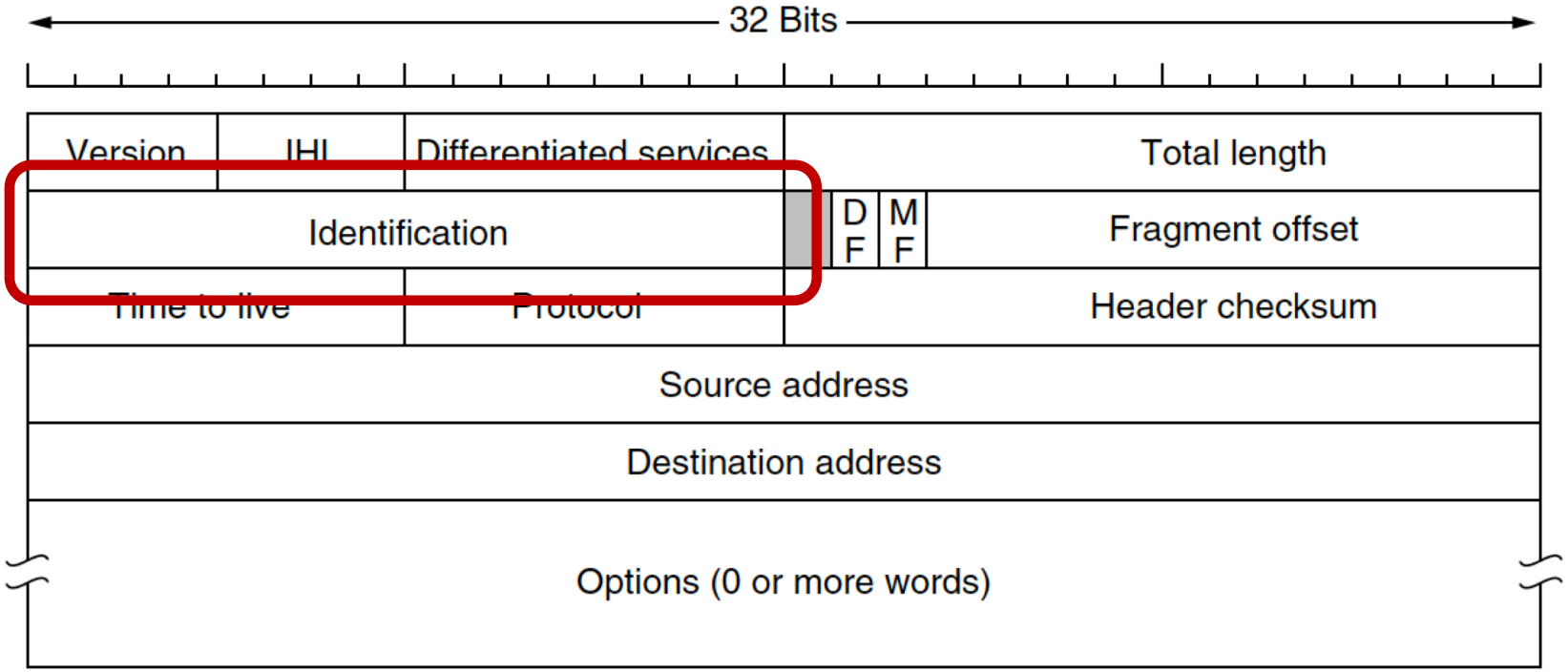
# IPv4 Header

- Total length: header and data, max: 65,535 bytes
  - should not exceed Maximum Transmission Unit (MTU)
  - E.g. Ethernet MTU = 1500B



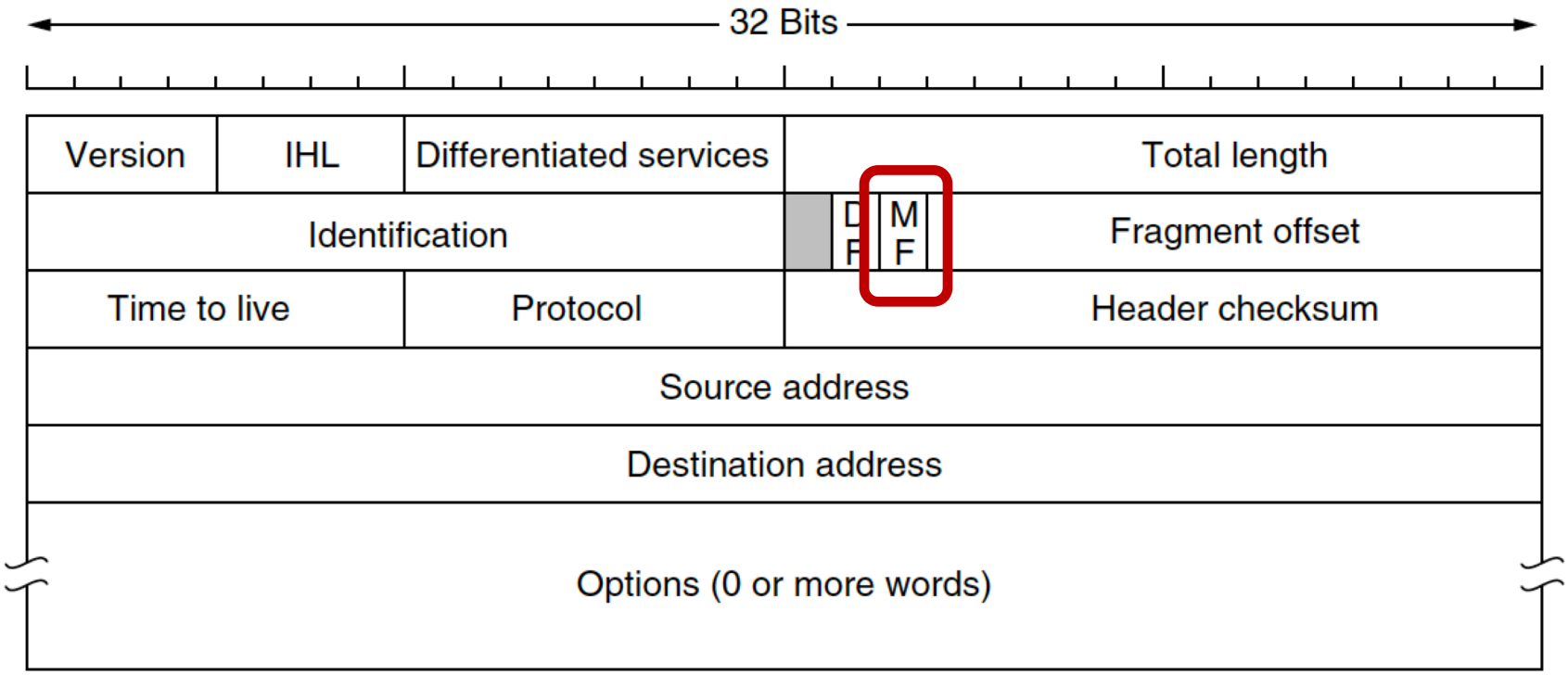
# IPv4 Header

- Identification: all fragments of an IP packet have the same value
  - Like a counter, this is 100, the next should be 101
  - But not a sequence number, IP provides connectionless service



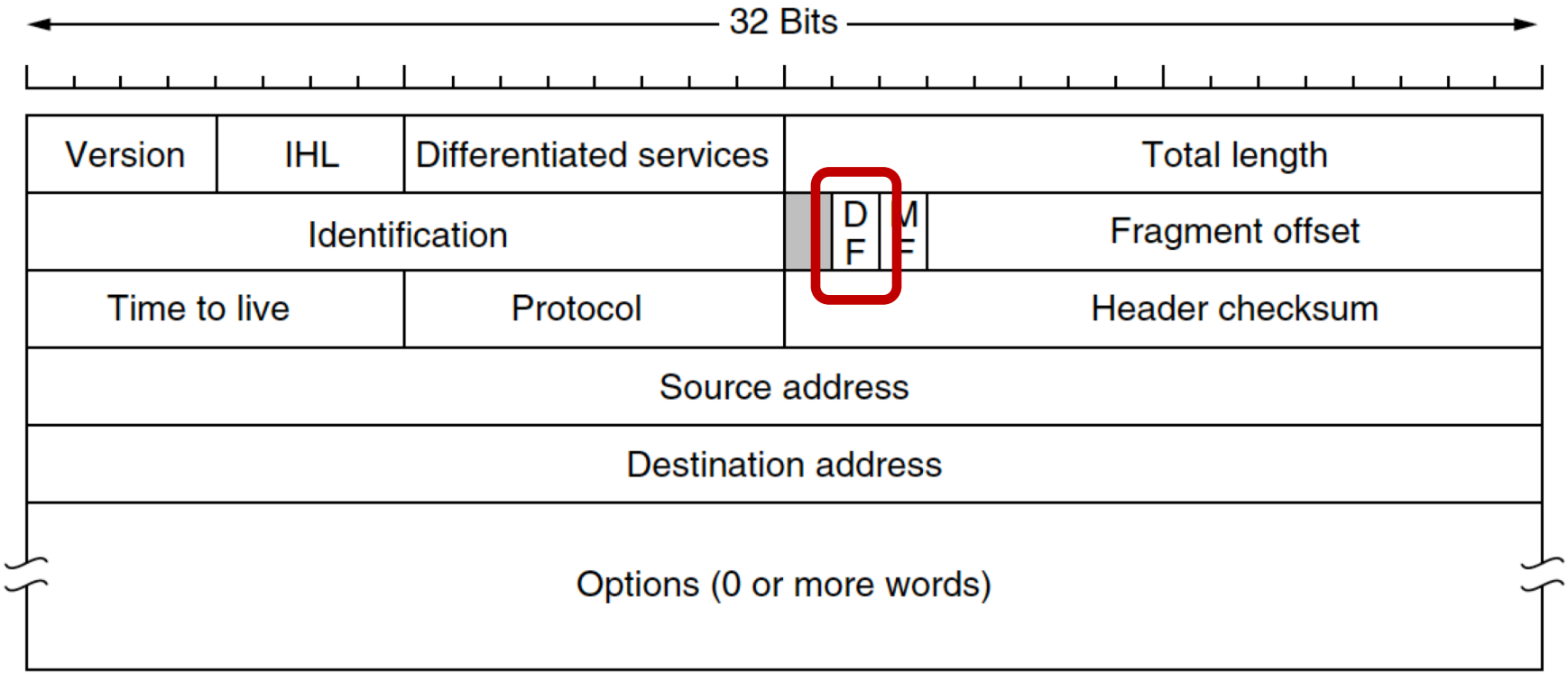
# IPv4 Header

- MF: More fragment, for IP packets that have the same identification
  - MF=1: more fragments afterwards
  - MF=0: last fragment



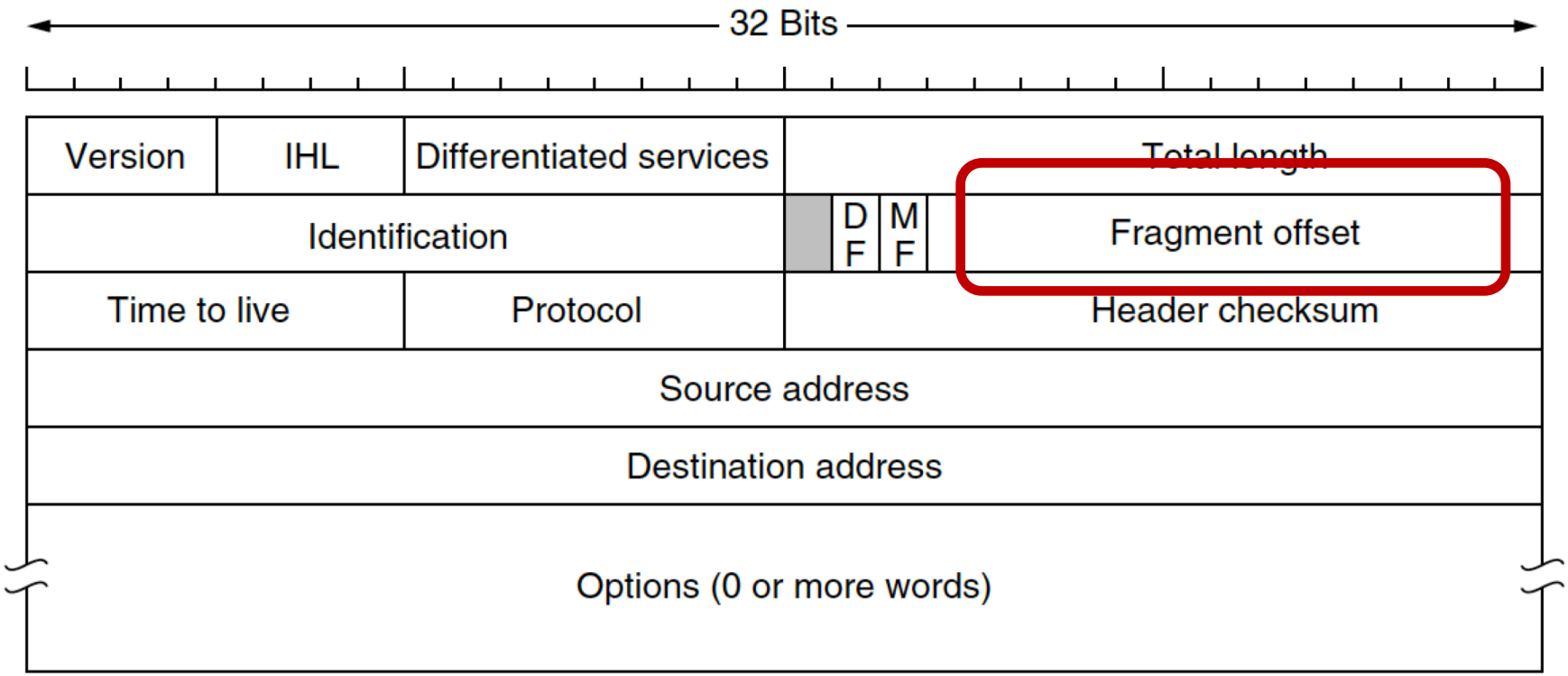
# IPv4 Header

- DF: Don’t Fragment. IP fragmentation is allowed when DF = 0



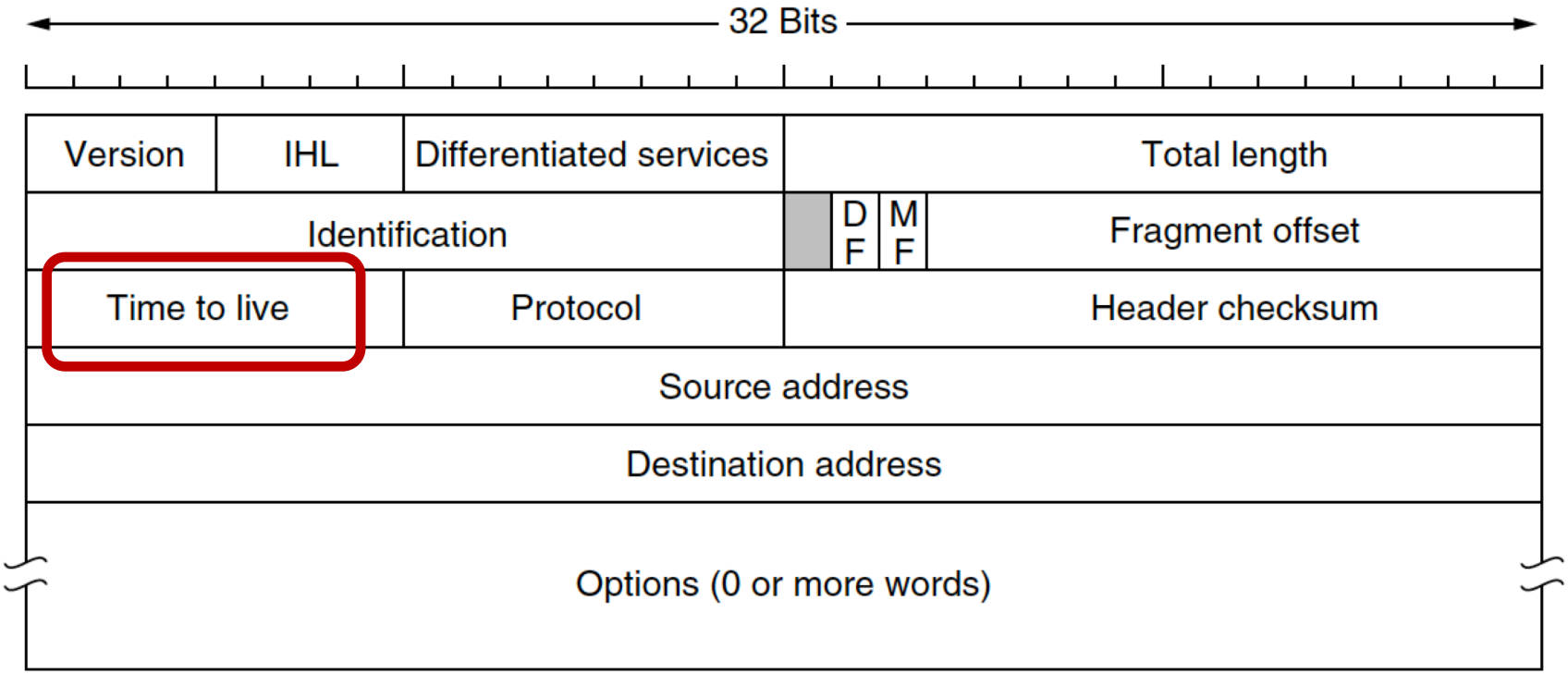
# IPv4 Header

- Fragment offset: relative starting position in all IP fragments that have the same identification.
  - Unit: **8 bytes**



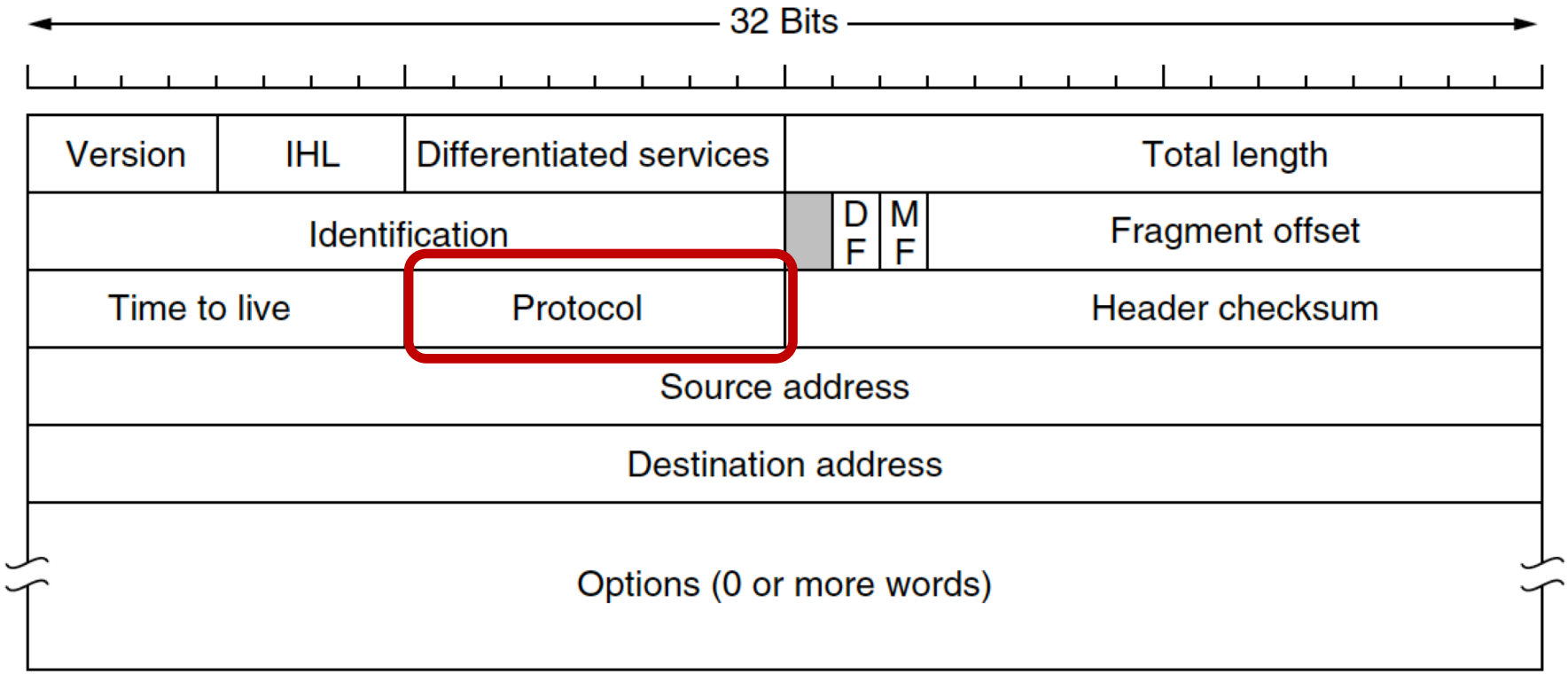
# IPv4 Header

- Time to live (TTL): a counter used to limit packet lifetimes.
  - In practice, it just counts hops and must be decremented on each hop of router.



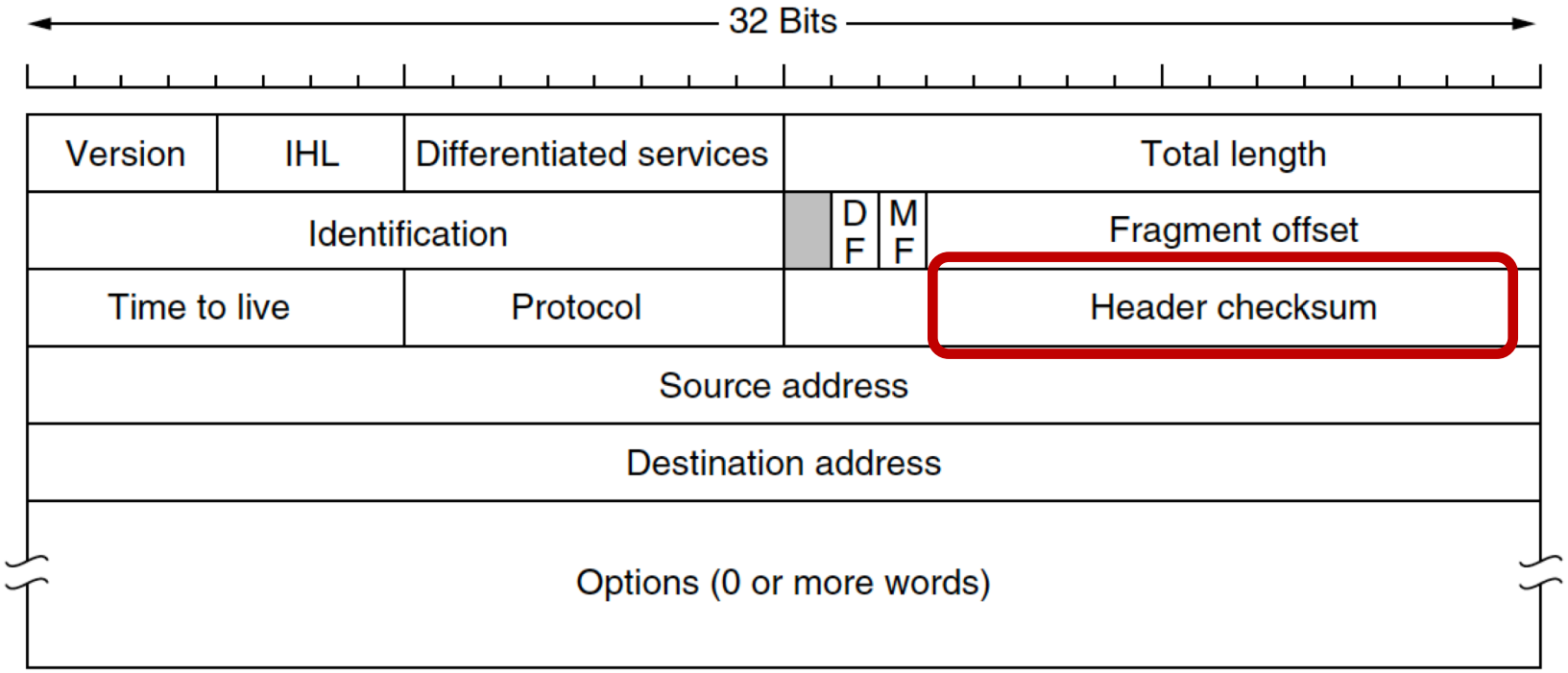
# IPv4 Header

- Protocol: which protocol used in the upper layer, transport layer.
  - E.g. TCP, UDP



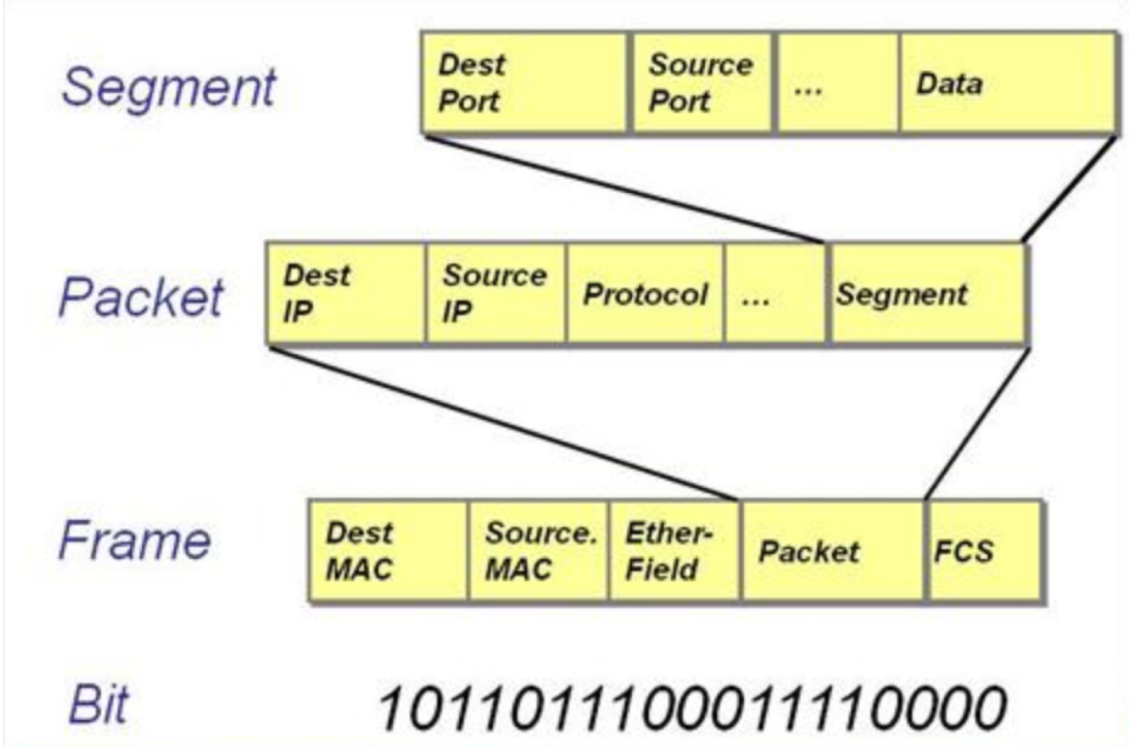
# IPv4 Header

- Checksum: header, not data; updates at each new hop
  - An error in the header is much more serious than an error in the data.
  - Data is sometimes not checksummed because doing so is expensive, and upper layers often do it anyway, making it redundant here.



# PDU – Protocol Data Unit

- Transport Layer
  - Packet (shared with network layer)
  - TCP: segment
  - UDP: datagram
- Network Layer
  - Packet(shared with transport layer)
  - Datagram
- Data link Layer
  - frame
- Physical Layer
  - bit

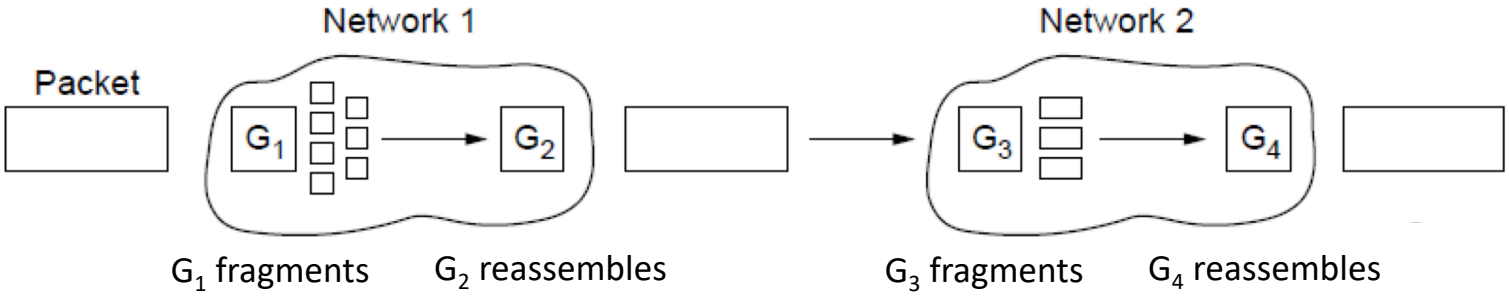


# Fragmentation

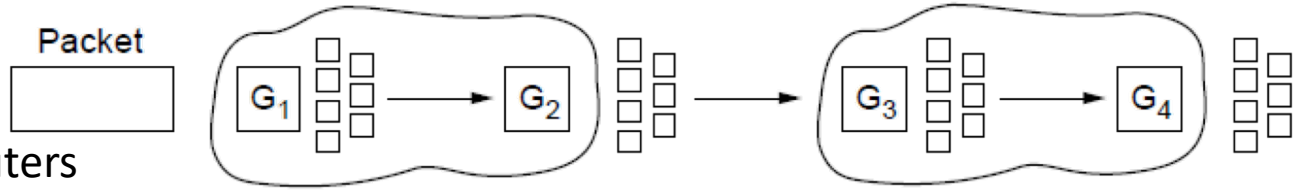
- MTU limits Transmission Unit on network link
  - Larger MTU less overhead, smaller MTU less delay
- Varies on different physical transmission links
- Fragmentation - split a long IP datagram into some short IP fragments to send
- Reassemble – to receive correctly, reassemble multiple IP fragments into one original long IP datagram

# Packet Fragmentation

- Networks have different packet size limits for many reasons
  - Large packets sent with fragmentation & reassembly




Transparent – packets fragmented / reassembled in each network

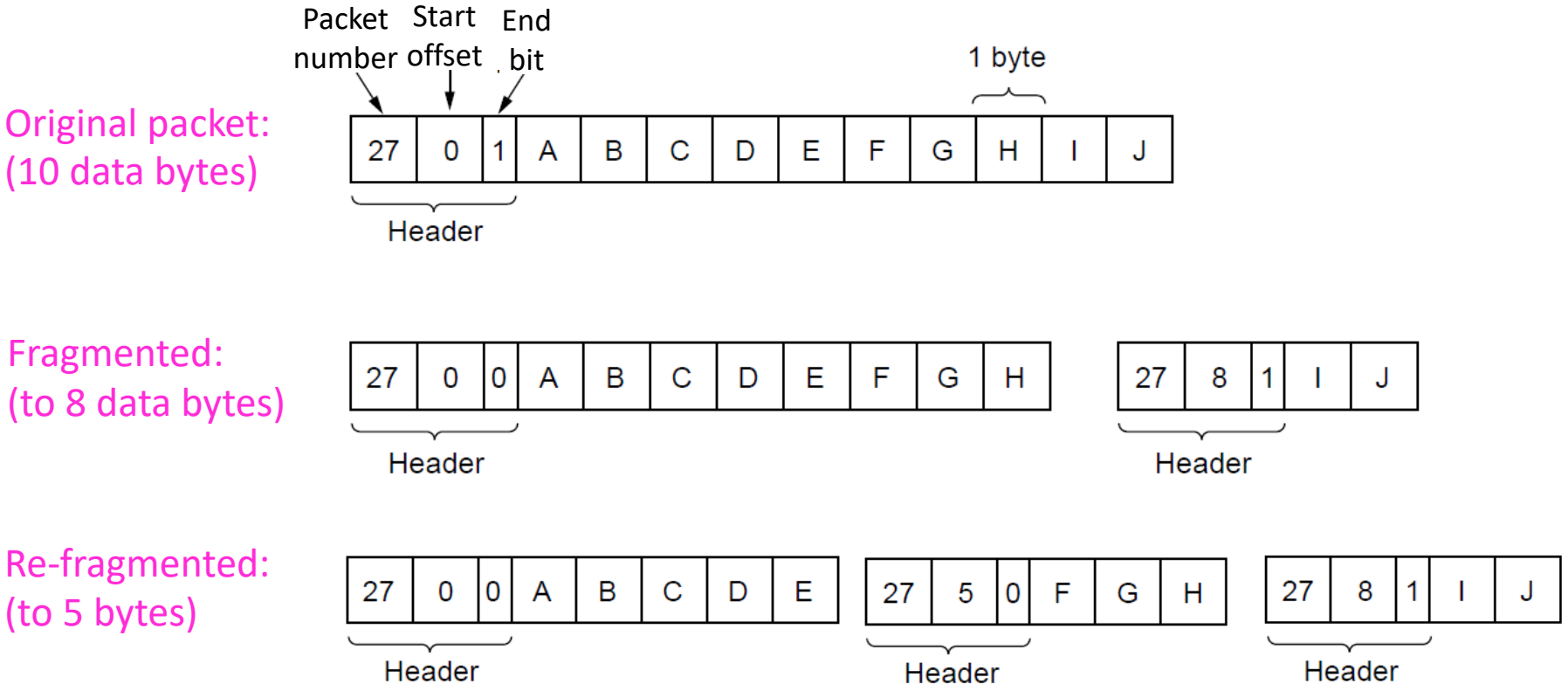



It requires routers
to do less work.
IP works this way.

**Non-transparent** – fragments are reassembled at destination

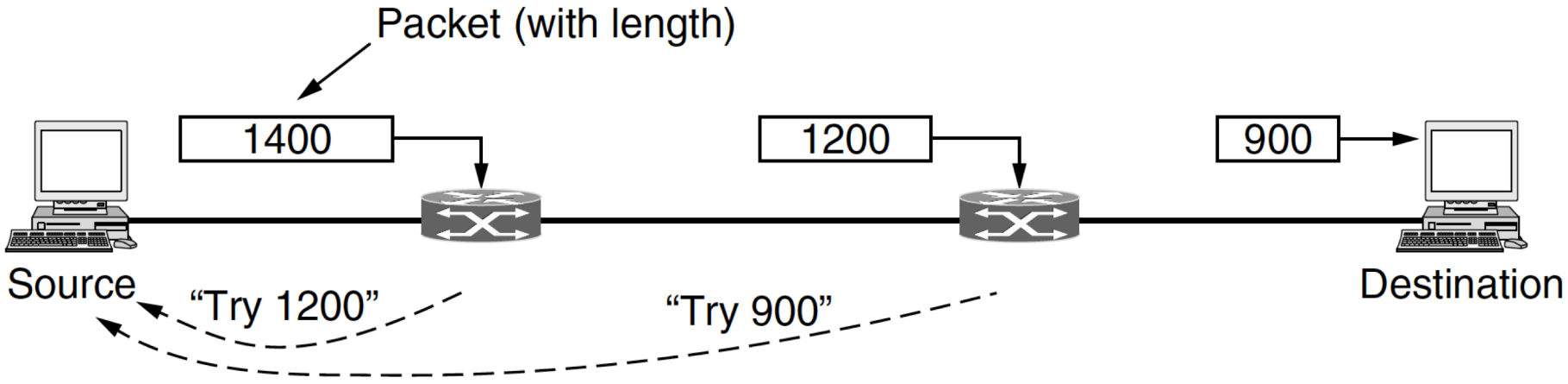
# Packet Fragmentation

- Example of IP-style fragmentation:



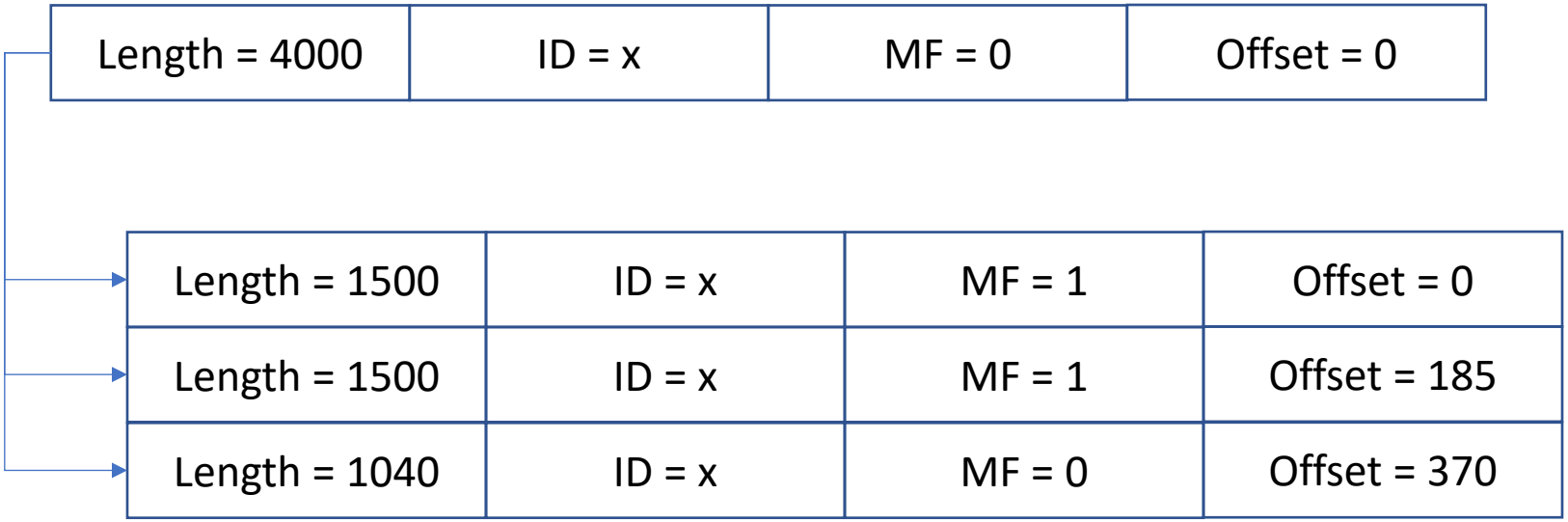
# Packet Fragmentation

- Path MTU Discovery avoids too many fragmentations over the network
  - Each IP packet is sent with its header bits set to indicate that no fragmentation is allowed to be performed.
  - If a router receives a packet that is too large, it generates an error packet, returns its MTU (Max. Transmission Unit) to the source, and drops the packet.



# Fragmentation - example

- IP header: 20 bytes, 4000 bytes IP datagram to send over a transmission link that has MTU = 1500 bytes



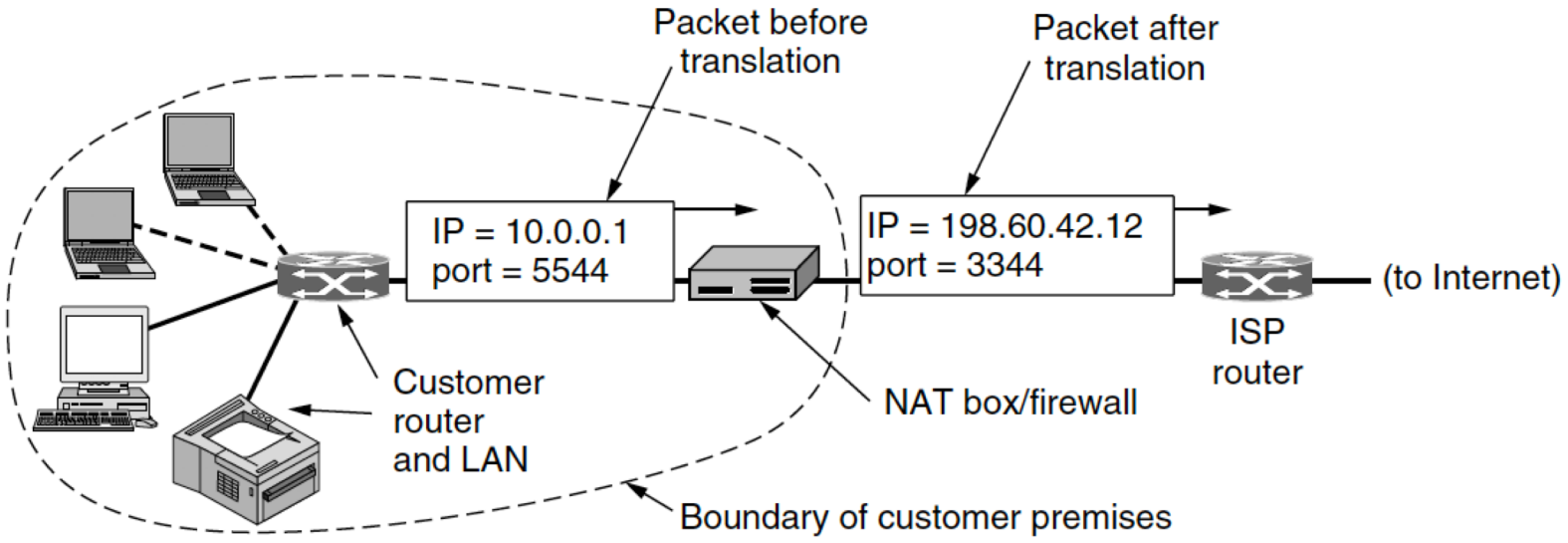

- Two more headers: 2 x 20 bytes
- Offset: 185 = 1480 / 8bytes

# NAT – Network Address Translation

- The outside networks only know one IPv4 address (assigned by ISP) for a whole internal network
- The internal network allocates IP address freely to all internal devices
- No packets containing these addresses, in the three reserved ranges, may appear on the Internet itself.
  - 10.0.0.0 – 10.255.255.255/8 16,777,216 hosts
  - 172.16.0.0 – 172.31.255.255/12 1,048,576 hosts
  - 192.168.0.0 – 192.168.255.255/16 65,536 hosts

# NAT – Network Address Translation

- NAT box maps one external IP address to many internal IP addresses
  - Use IP address + port number (UDP/TCP) locates one host in this internal network to communicate with outside network.

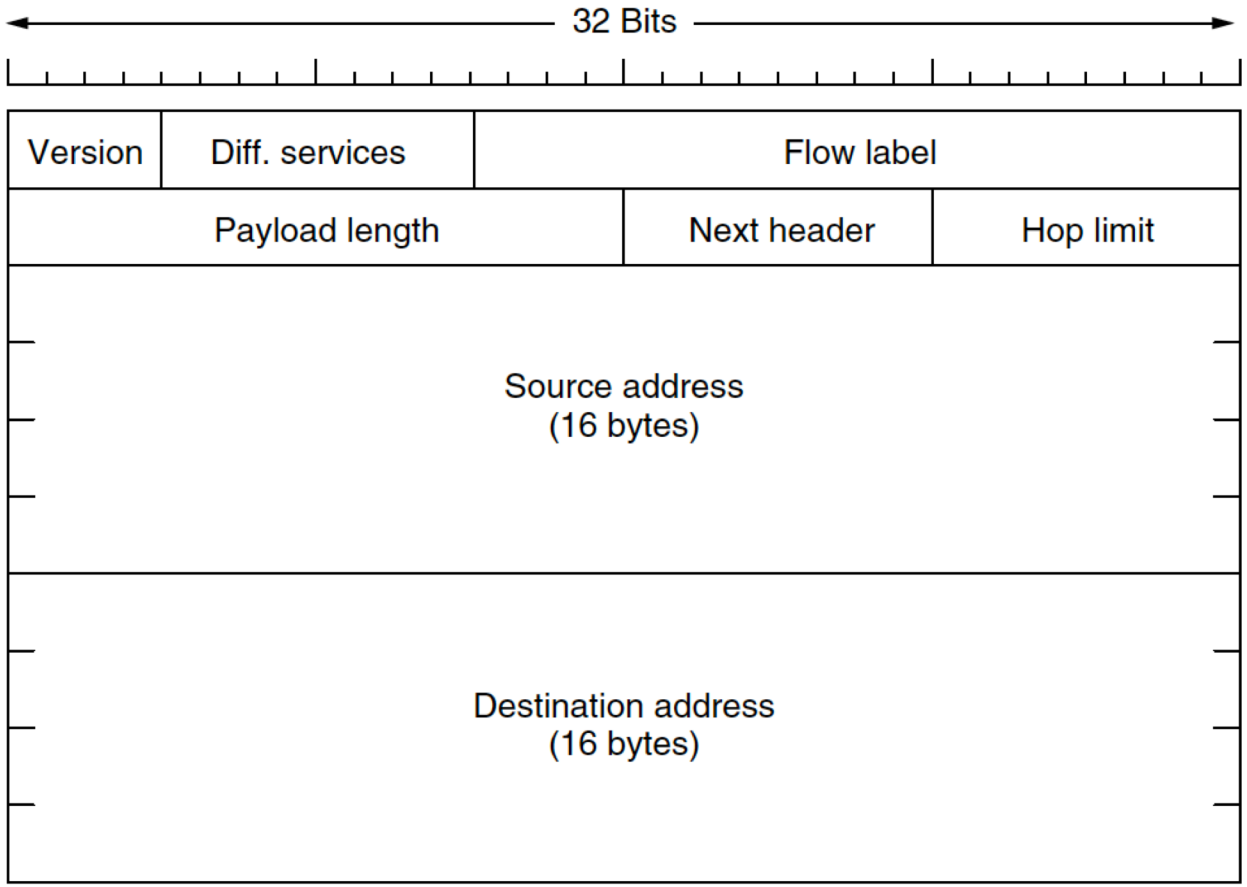


# NAT – Network Address Translation

- The mapping in the NAT box is set up when a connection is established.
- The connections can only be made from inside the house to the Internet!
  - You can't run a server in your home without special configuration.
- Violates layering (each layer should be independent).
  - What if the transport layer is not using UDP/TCP?
- Very common in homes network.
- Can also be used as a firewall to protect internal computers

# IPv6 Header

- IPv6 address: 4 x 32bits = **128 bits** (e.g. 2001:db8:0:0:0:ff00:42:8329)
  - $2^{128}$, or approximately $3.4\times10^{38}$



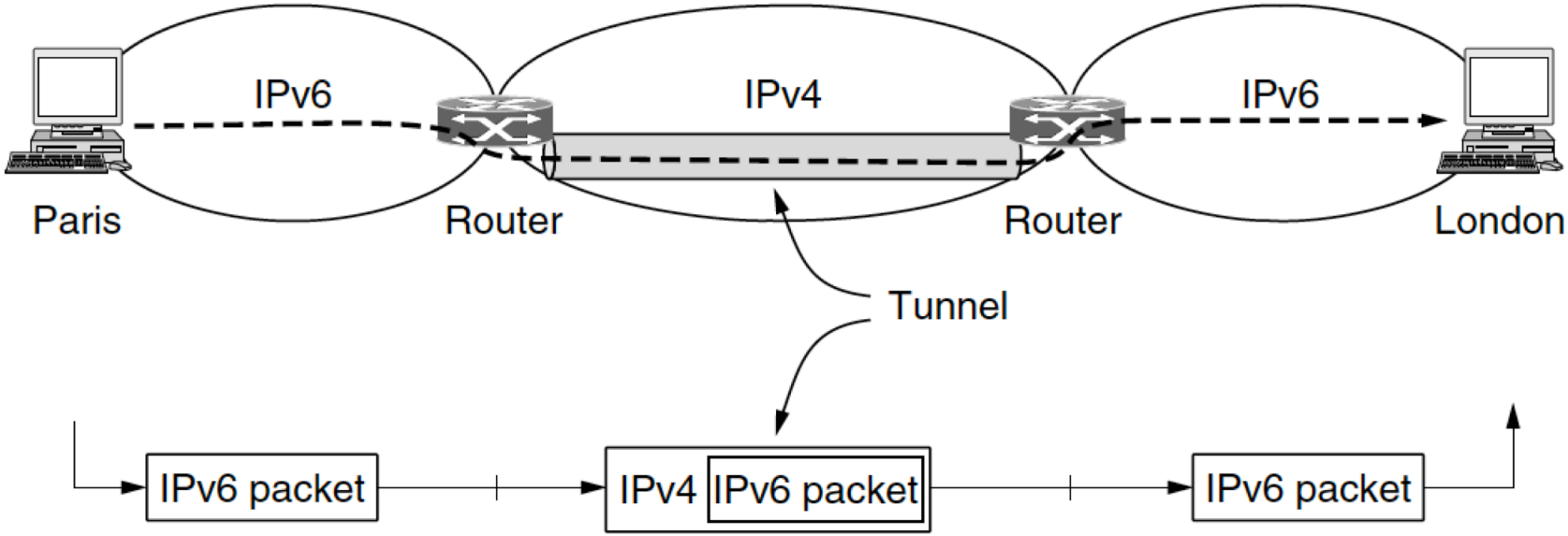
# IPv6

- Deployment has been slow & painful, but may pick up pace now that addresses are all but exhausted
- IPv6 protocol header has much longer addresses (128 vs. 32 bits) and is simpler (by using extension headers)
- IPv6 extension headers handles other functionality

| Extension header | Description |
|---|---|
| Hop-by-hop options | Miscellaneous information for routers |
| Destination options | Additional information for the destination |
| Routing | Loose list of routers to visit |
| Fragmentation | Management of datagram fragments |
| Authentication | Verification of the sender's identity |
| Encrypted security payload | Information about the encrypted contents |

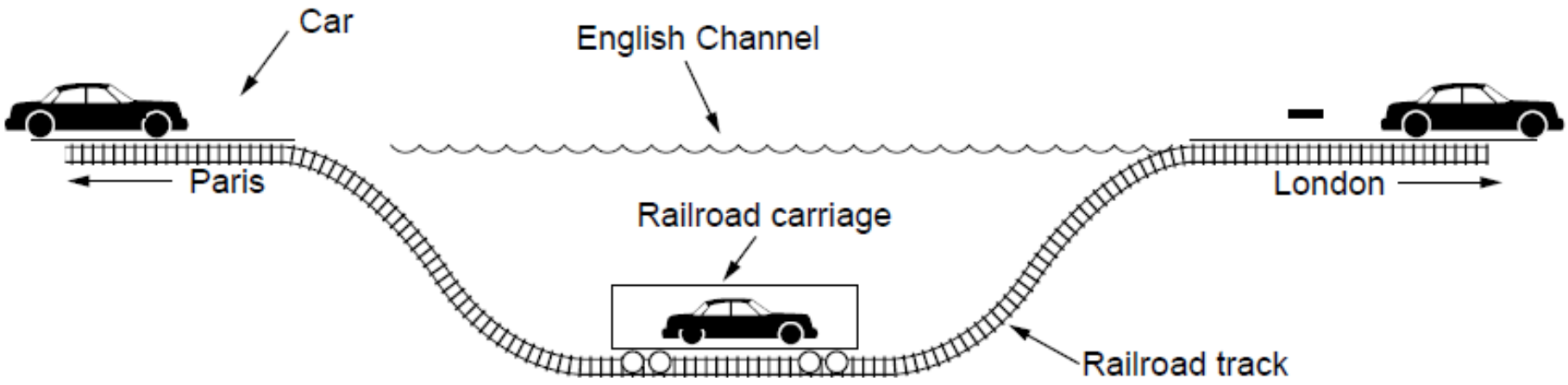
# Tunnelling

- Tunnelling protocol allows a network user to access or provide a network service that the underlying network does not support or provide directly.
  - E.g: IPv6 over IPv4
- Connects two networks through a middle one
  - Packets are encapsulates over the middle



# Tunnelling

- Tunneling analogy:
  - tunnel is a link
  - packet can only enter/exit at ends



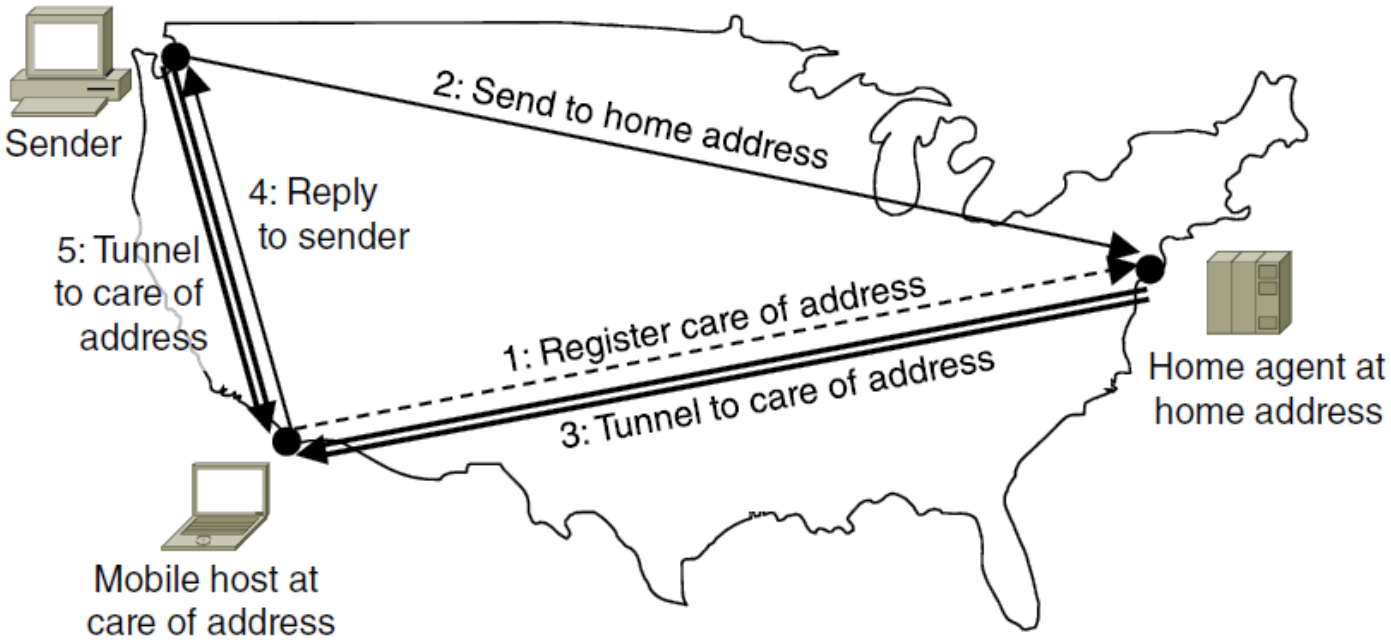
# Tunnelling

- The disadvantage of tunnelling is that none of the hosts on the network that is tunnelled over can be reached because the packets cannot escape in the middle of the tunnel.

- However, this limitation of tunnels is turned into an advantage with VPNs (Virtual Private Networks). A VPN is simply an overlay that is used to provide a measure of security.

# Mobile IP

- **Mobile hosts** can be reached via a **home agent**
  - Fixed home agent **tunnels** packets to reach the mobile host
  - Reply can optimize path for subsequent packets after registration
  - No changes to routers or fixed hosts



# Mobile IP

- To keep the TCP connection between a mobile host and a static host
  - reducing the effects of location changes while the mobile host is moving around
  - without having to change the underlying TCP/IP.
  - Often in wireless network, e.g. changing a wi-fi router connection
  - Not for cellular network, e.g. 3G or 4G, base station handover is done already
- No matter how Care of address (CoA),or local address changes, Mobile IP keeps a fixed Home address.

# Summary

- What are key fields in the header of IPv4? Why? How do they work?
- It seems IP addresses are not enough, how IPv6 and NAT is designed for solving this problem?
- What is the key technology for VPN? Any other applications for this technology?
  - Although moving around different places (wireless LANs) on campus, I can use my computer for Internet without losing connection.
- How does it work without changing any IP address settings?