CSC8004 Computer Networks

The Network Layer

Ellis Solaiman

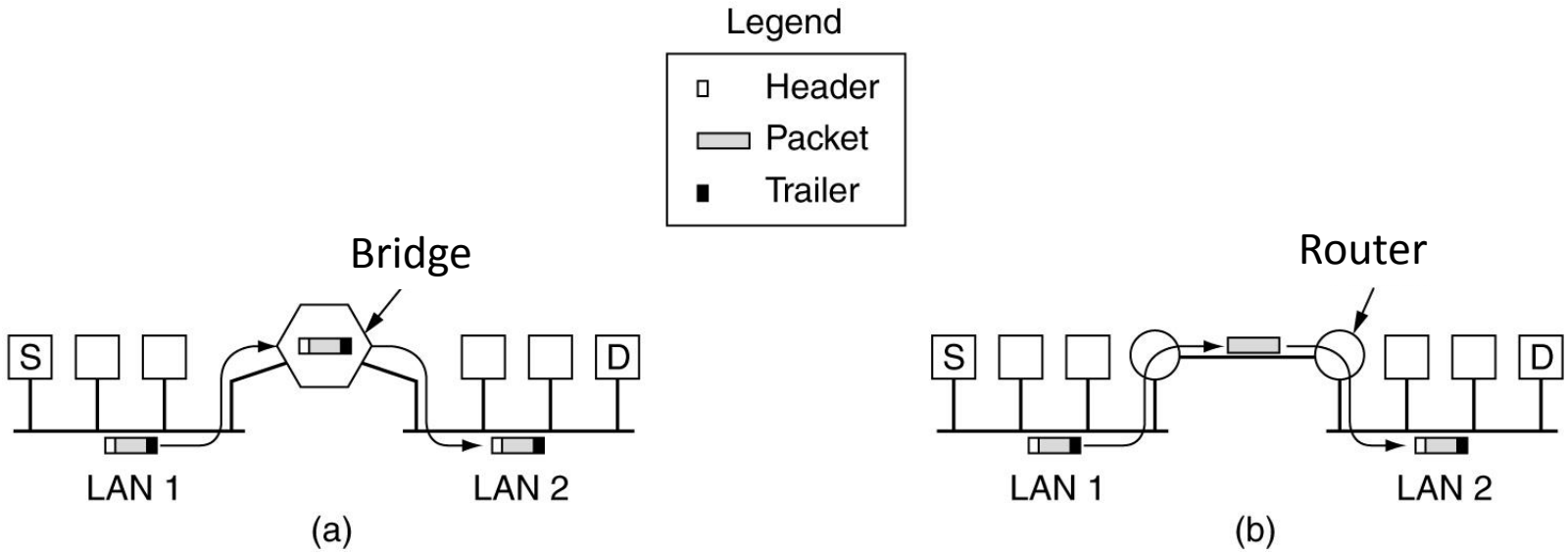
The Internet and internetworking

- **Internetworking** is the process of forming connections between different networks to provide internet services.

Heterogeneous systems

- Different address schemes
- Different maximum packet size
- Different network access mechanisms
- Different timeouts
- Different Error recovery mechanisms
- Different Routing techniques
- Different User access control mechanisms
- Connections and connectionless communication

How networks can be connected



Bridge uses Ethernet MAC header to decide on destination

Router extracts packet and uses its header to decide on destination.
More work to do than bridge

Tunneling

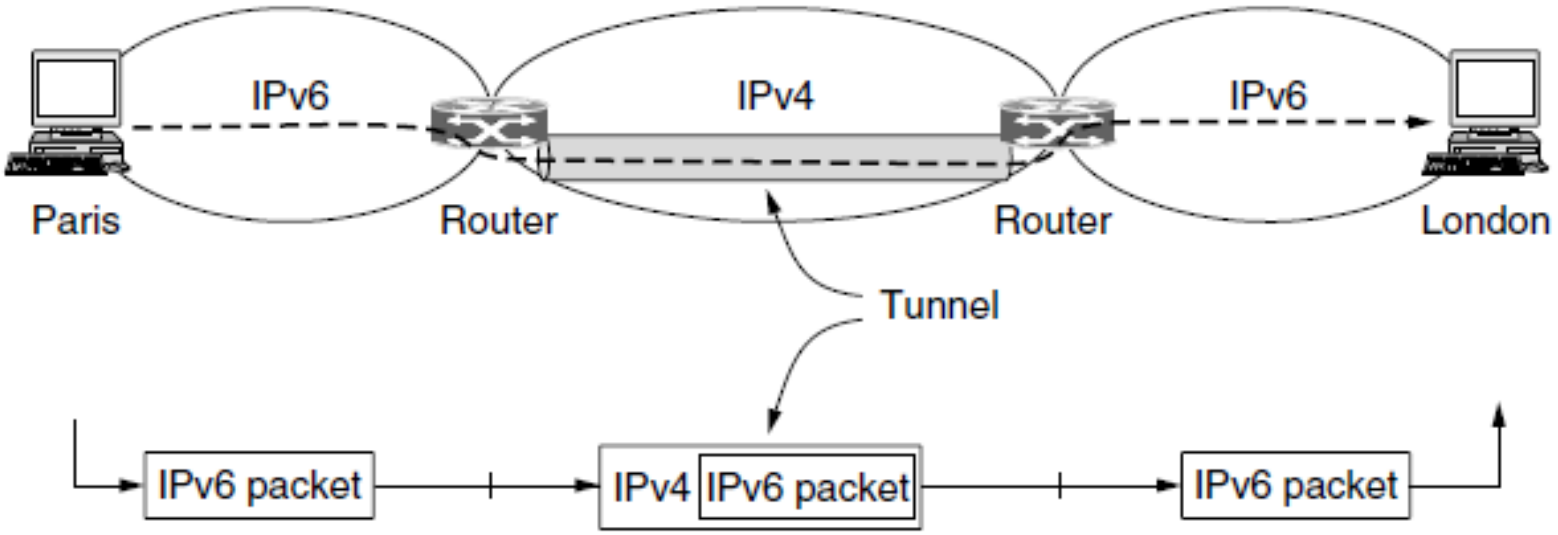
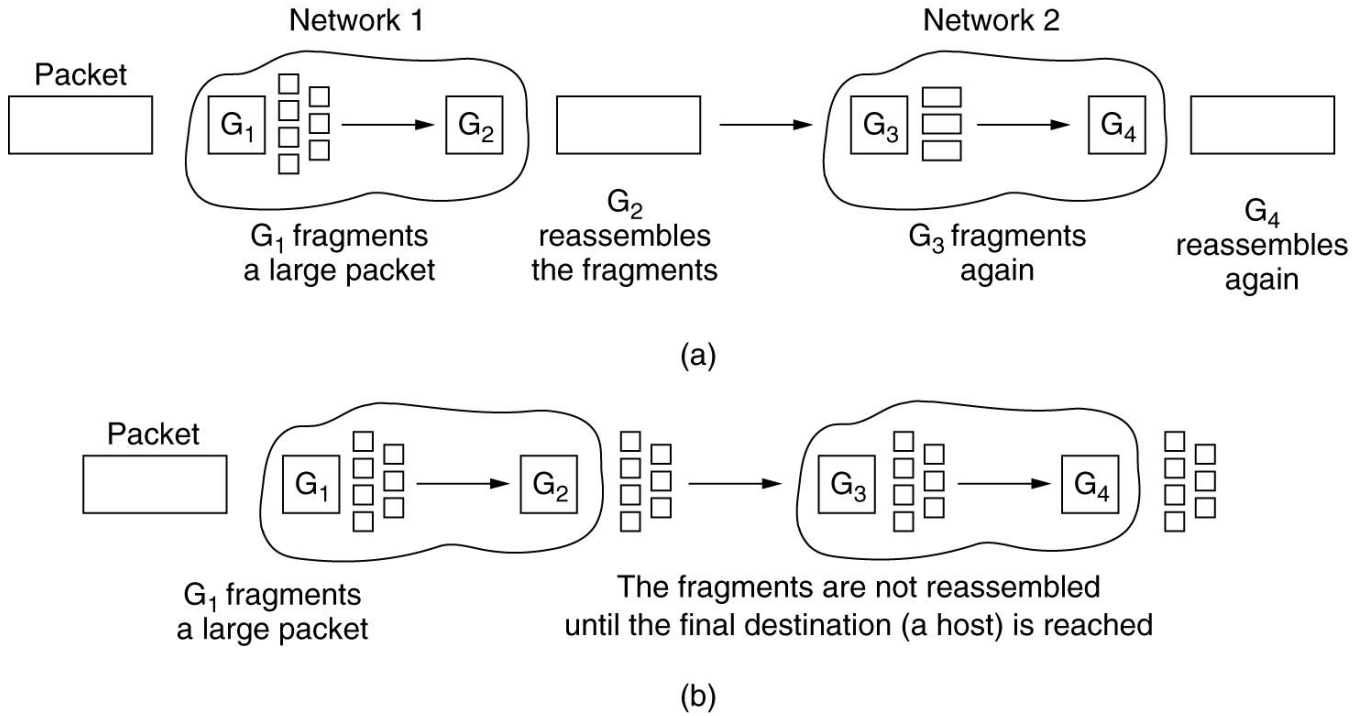


Figure 5-40. Tunneling a packet from Paris to London.

Fragmentation



Incoming packet too large for intermediate networks

Packets broken down by multi-protocol routers (G)

In (a) multi-protocol routers reassemble packet at boundary (transparent fragmentation)

In (b) packet is only reassembled at destination (non-transparent fragmentation)

Fragmentation (2)

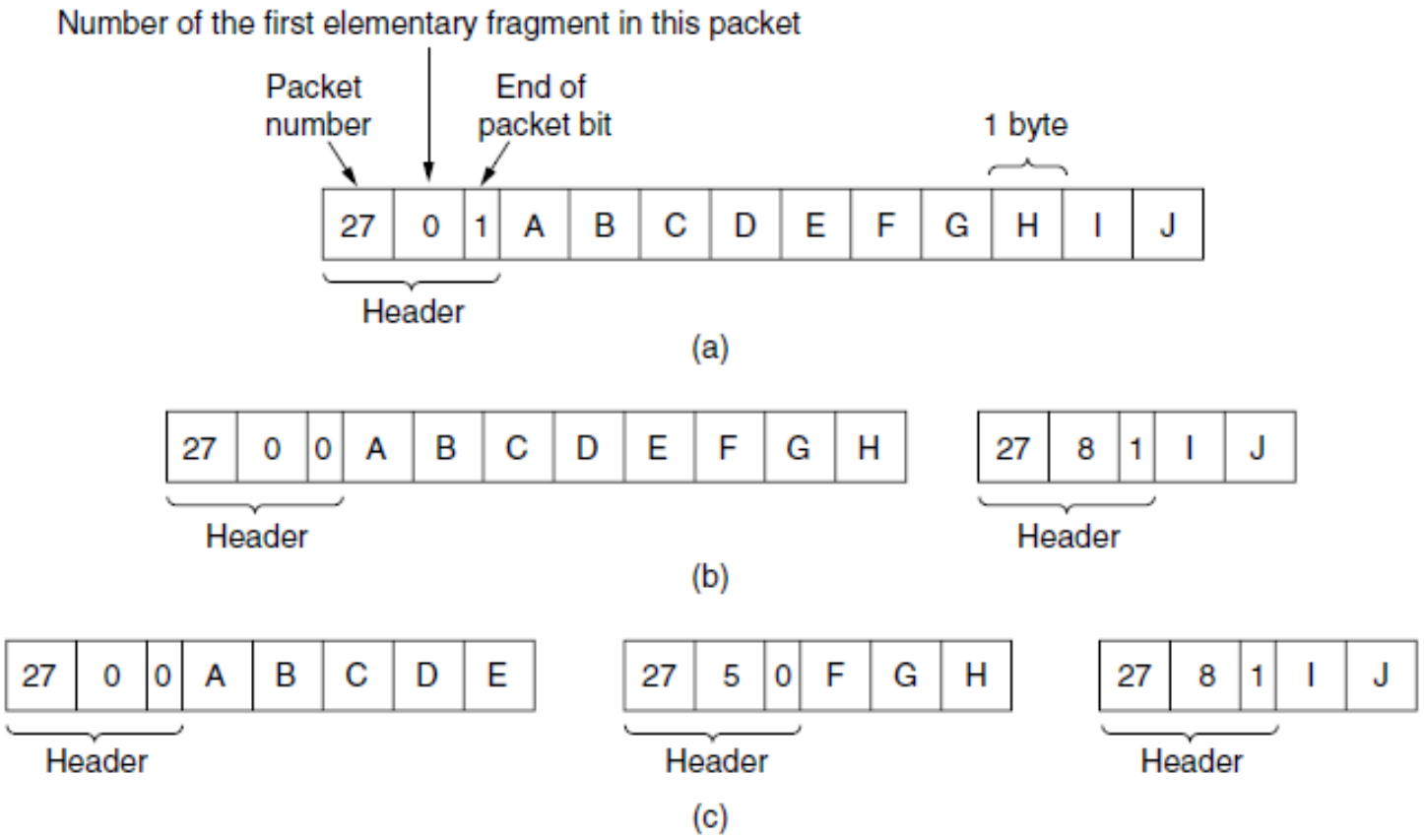


Figure 5-43. Fragmentation when the elementary data size is 1 byte. (a) Original packet, containing 10 data bytes. (b) Fragments after passing through a network with maximum packet size of 8 payload bytes plus header. (c) Fragments after passing through a size 5 gateway.

No Fragmentation

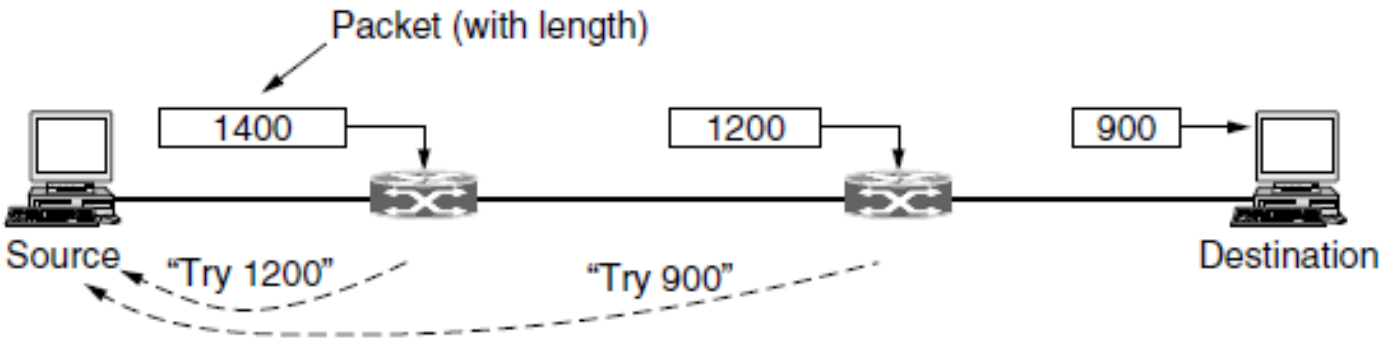


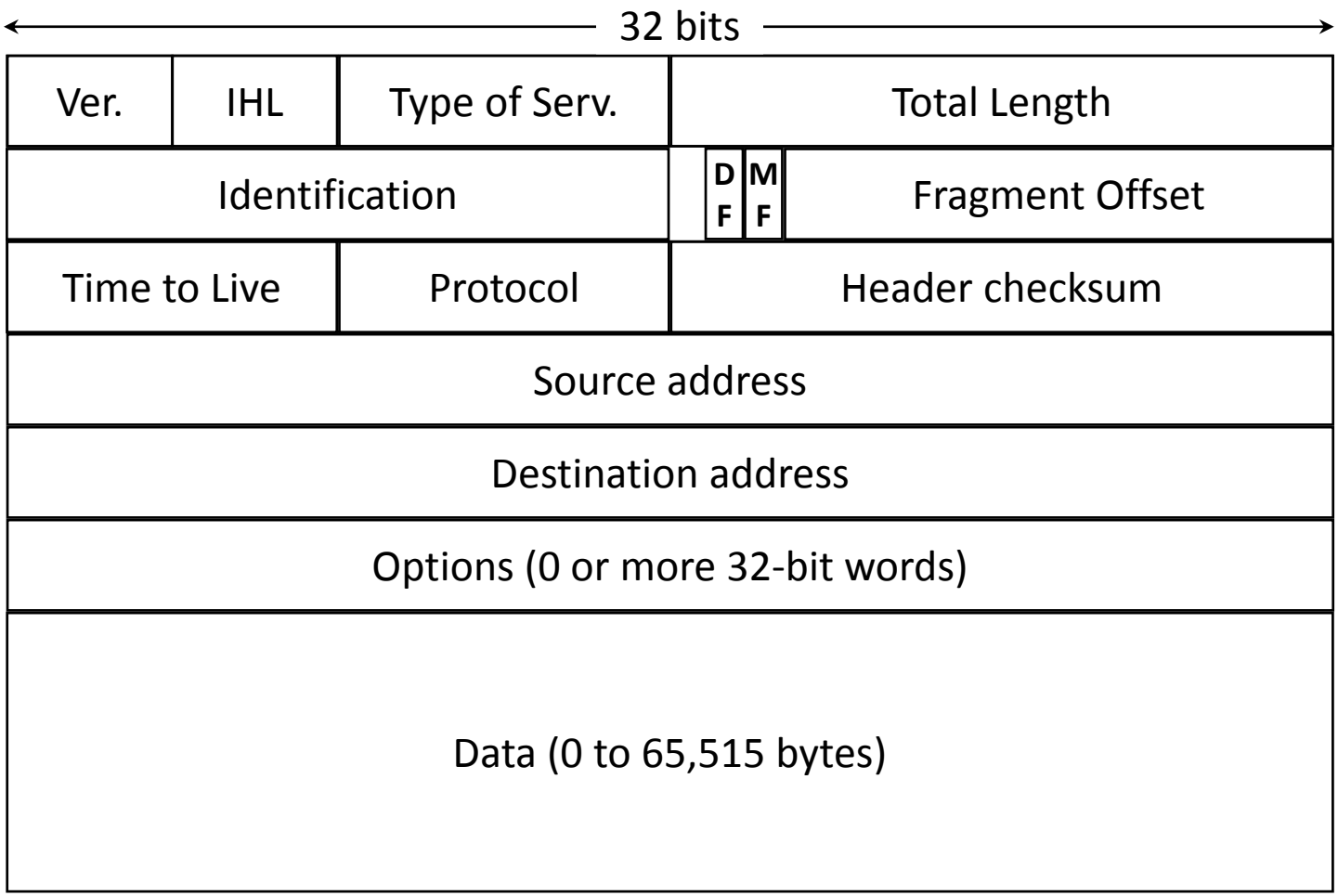
Figure 5-44. Path MTU discovery.

MTU: Maximum Transmission Unit

The Internet Protocol (IP)

- The Internet is a (very large) collection of different kinds of subnets.
- IP is the “glue” that allows all these subnets to exchange data – giving the impression of a single, global net.
- IP provides delivery of packets from one host in The Internet to any other host in The Internet, even if the hosts are on different networks (with possibly different protocols).
- Internet packets may be up to 64 kilobytes in length (although they are typically much smaller).
- Typically a maximum frame size will be 1500 bytes (Ethernet).

The IPv4 format



The IPv4 format (2)

- Version: The IP version number, currently 4, called IPv4. A new version, IPv6, is already in use.
- IHL: IP Header Length.
- Type of Service: Contains priority information.
- Total Length: The total length of the datagram including header.
- Identification: when an IP packet is segmented into multiple fragments, each fragment is given the same identification. This field is used to reassemble the fragments.

The IPv4 format (3)

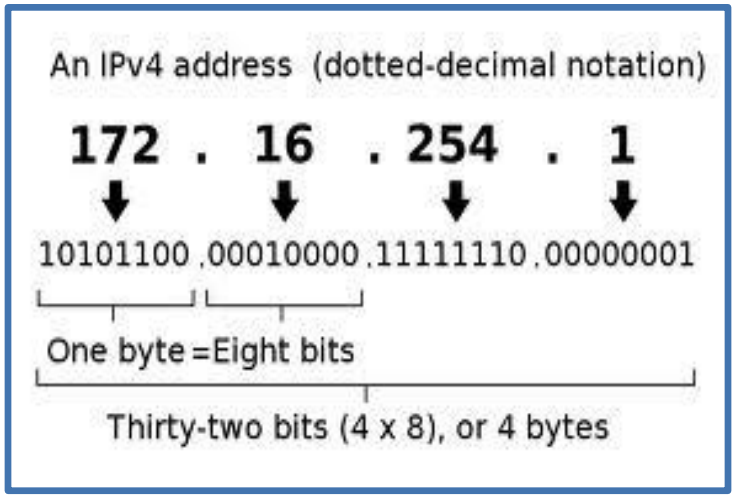
- DF: Don’t Fragment. Packets must be sent in one piece.
- MF: More Fragments. When a packet is fragmented, all fragments except the last one have this bit set.
- Fragment offset: The fragment’s position within the original packet.
- Time to Live: Hop count, decremented each time the packet reaches a new router. When hop count = 0, the packet is discarded.
- Protocol: Identifies which transport layer protocol is being used for this packet.

The IPv4 format (4)

- Header Checksum: Verifies the contents of the IP header.
- Source and Destination Addresses: Uniquely identify sender and receiver of the packet.
- Options: Used to extend the functionality of IP. Examples: source routing, security.

Addressing

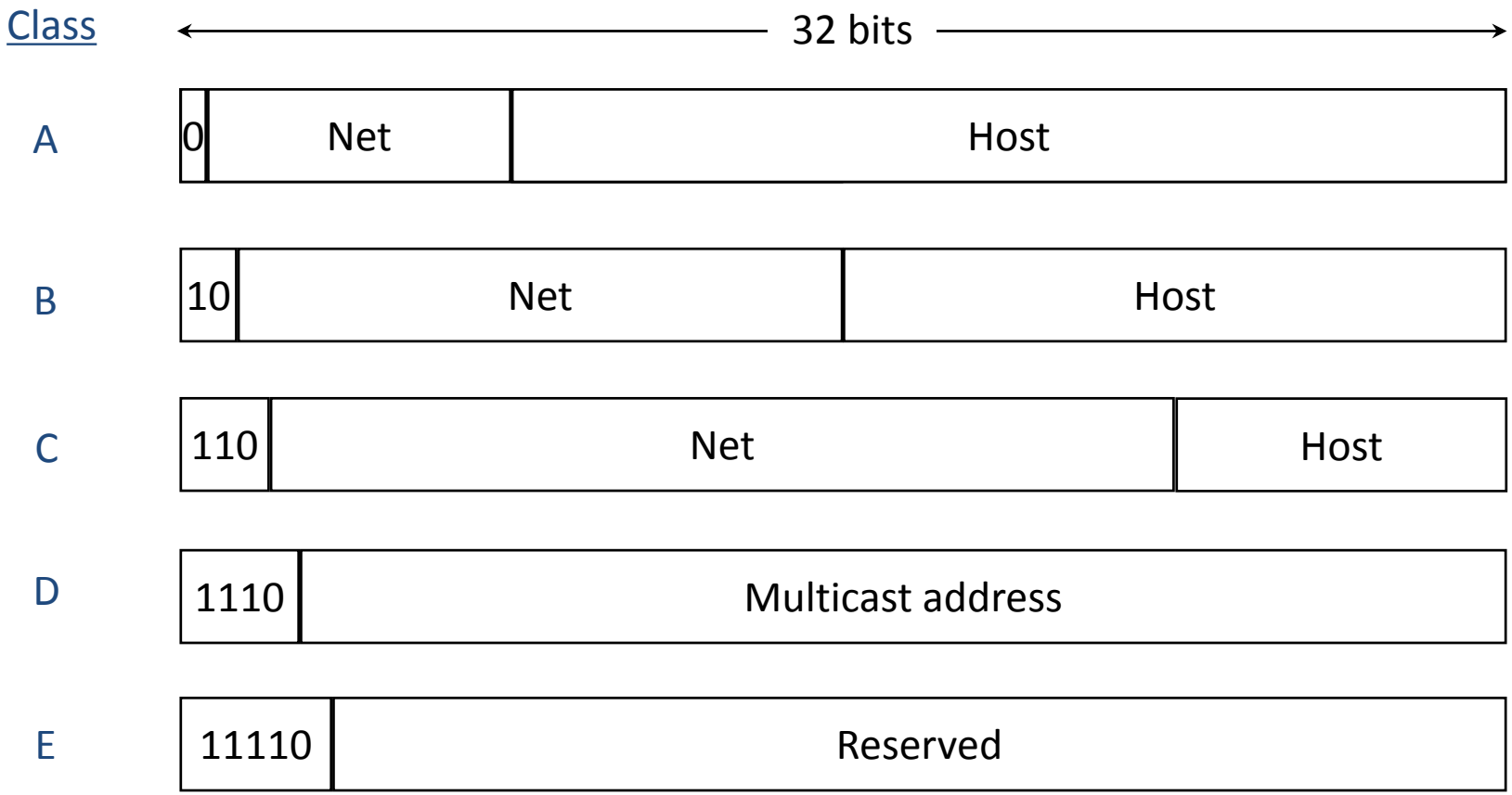
- Each host is assigned a unique 32-bit Internet (IP) address that is used in all communication with that host.
- Each address consists of a (netid,hostid) pair where ***netid*** **identifies a network** and ***hostid*** **identifies the host** on that network by its connection to the network.
- IP addresses are binary numbers, usually displayed in human readable notation



Addressing

- There are three primary classes of identifier distinguished by the two higher order bits of the address:
  - Class A: first bit 0. Used for very large networks with a very large number of hosts: 7 bit *netid* and 24 bit *hostid*. Over 16 million hosts per net, 1.0.0.0 to 127.255.255.255.
  - Class B: first bit 1 second bit 0. Used for moderate to large sized networks with between 2^8 and 2^{16} hosts: 14 bit *netid* and 16 bit *hostid*. About 65 thousand hosts, 128.0.0.0 to 191.255.255.255.
  - Class C: first bit 1, second bit 1, and third bit 0. Used for small networks with up to 2^8 (256) hosts: 21 bit *netid* and 8 bit *hostid*. 192.0.0.0 to 223.255.255.255.
  - Class D: Special case (multicast), 224.0.0.0 to 239.255.255.255.
  - Class E: Broadcast: 255.255.255.255 (i.e all '1's in binary).

IPv4 address classes



Addressing

Class	Total # of bits for Net ID/H ID	Leading bits of address (binary)	Range of first decimal	Usable # of network ID bits	# of possible network IDs	# of host IDs per network ID
A	8/24	**0**xxx xxxx	0-127	8-1=7	2^7 = 128	2^{24} = 16 777 216
B	16/16	**10**xx xxxx	128-191	16-2=14	2^{14}=16384	2^{16} = 65536
C	24/8	**110**x xxxx	192-223	24-3=21	2^{21}= ~2mil	2^8 = 256

http://en.wikipedia.org/wiki/List_of_assigned_/8_IPv4_address_blocks

Addressing

Deciding the class of an IP address of echo.ncl.ac.uk

175 . 50 . 12 . 2

10101111.00110010.00001100.00000010

Class B

Classless Inter-Domain Routing (CIDR)

- In order to make the remaining address space last longer; CIDR was introduced instead of the previous 3 classes.
- CIDR has no class structure, instead each network
  - Is assigned a block of addresses as big (or small) as needed

http://en.wikipedia.org/wiki/List_of_assigned_/8_IPv4_address_blocks

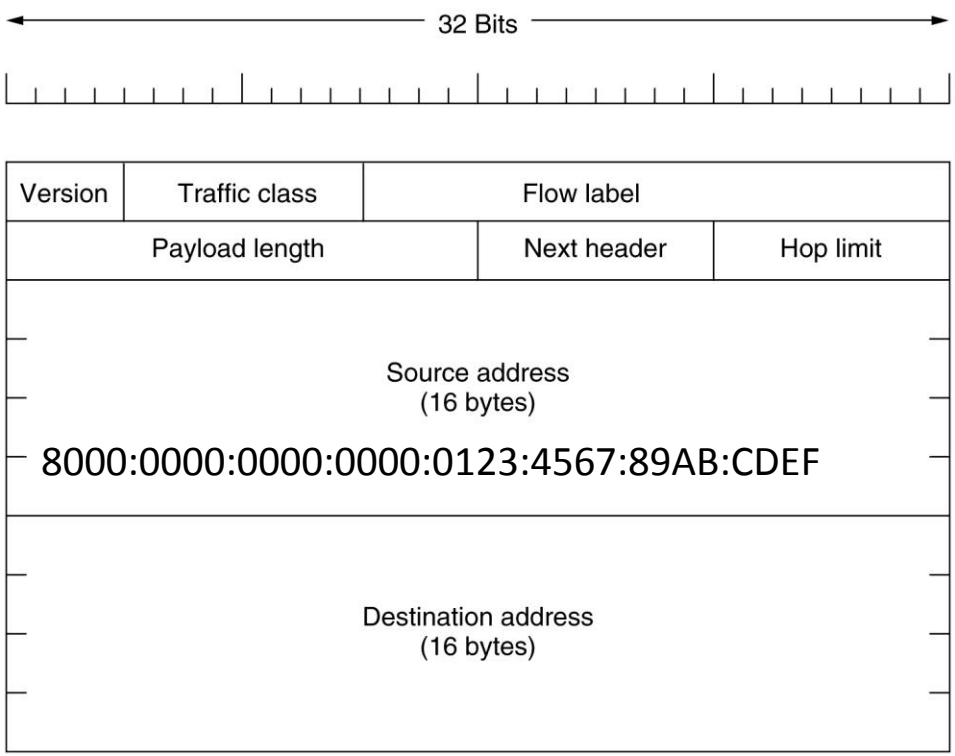
Network Address Translation (NAT)

- Most networks only communicate through a single point (the firewall).
- As a result most of their address space is unused on the Internet itself.
- NAT exploits this by only assigning one (or very few) addresses to an entire network.
- All incoming and outgoing messages must therefore go through this address.
- The network must translate this address into the host destination:
  - Private IP address space inside the network, e.g 10.0.0.0 to 10.255.255.255
  - Actual host stored in TCP header.

Network Address Translation (NAT)

- How does a machine (echo.ncl.ac.uk) which has the address 10.4.127.133 connect to the Internet?
- Addresses in the range 10.0.0.0 to 10.255.255.255 are private IP address space inside the network, they are not used for communication on the public Internet.
- The internal machine (echo) cannot connect directly outside its private network without going through a proxy server. This involves a process referred to as Network Address Translation (NAT).
- The private IP address (10.4.127.133) is stored in the TCP pseudo header and the source in the IP header will give the IP address of the proxy server.
- When a reply arrives back at the proxy server, the internal private IP address is recovered from the TCP proxy header and the datagram delivered to echo.

The IPv6 format



Header has fixed length

Flexibility through “next header”

Class field supports prioritization/QoS

Flow label not yet fully defined

Payload length refers to data

Hop limit same as time to live in IPv4

Source/destination addresses are

16 bytes each (4 bytes in IPv4)

- one IP address per molecule on Earth!
- addresses with first 12 bytes as zero are interpreted as IPv4 addresses so IPv4 and IPv6 can coexist

Note no CRC – this is assumed to be handled by other layers