Network : Internet Protocol (2)

Jae Hyeon Kim

Reference

William Stalling, Data and Computer Communications 10/E, Prentice Hall

Subnets and Subnet Masks

- Aims to save the IP addresses by sharing an address with a set of physical networks
- Allows arbitrary complexity within an organization
  - Insulate overall Internet from growth of network numbers and routing complexity
  - Site looks to rest of internet like single network
- Each LAN assigned subnet number
  - Host portion of address partitioned into subnet # and host #
  - Local routers route within subnetted network
- Subnet mask indicates which bits are subnet number and which are host number

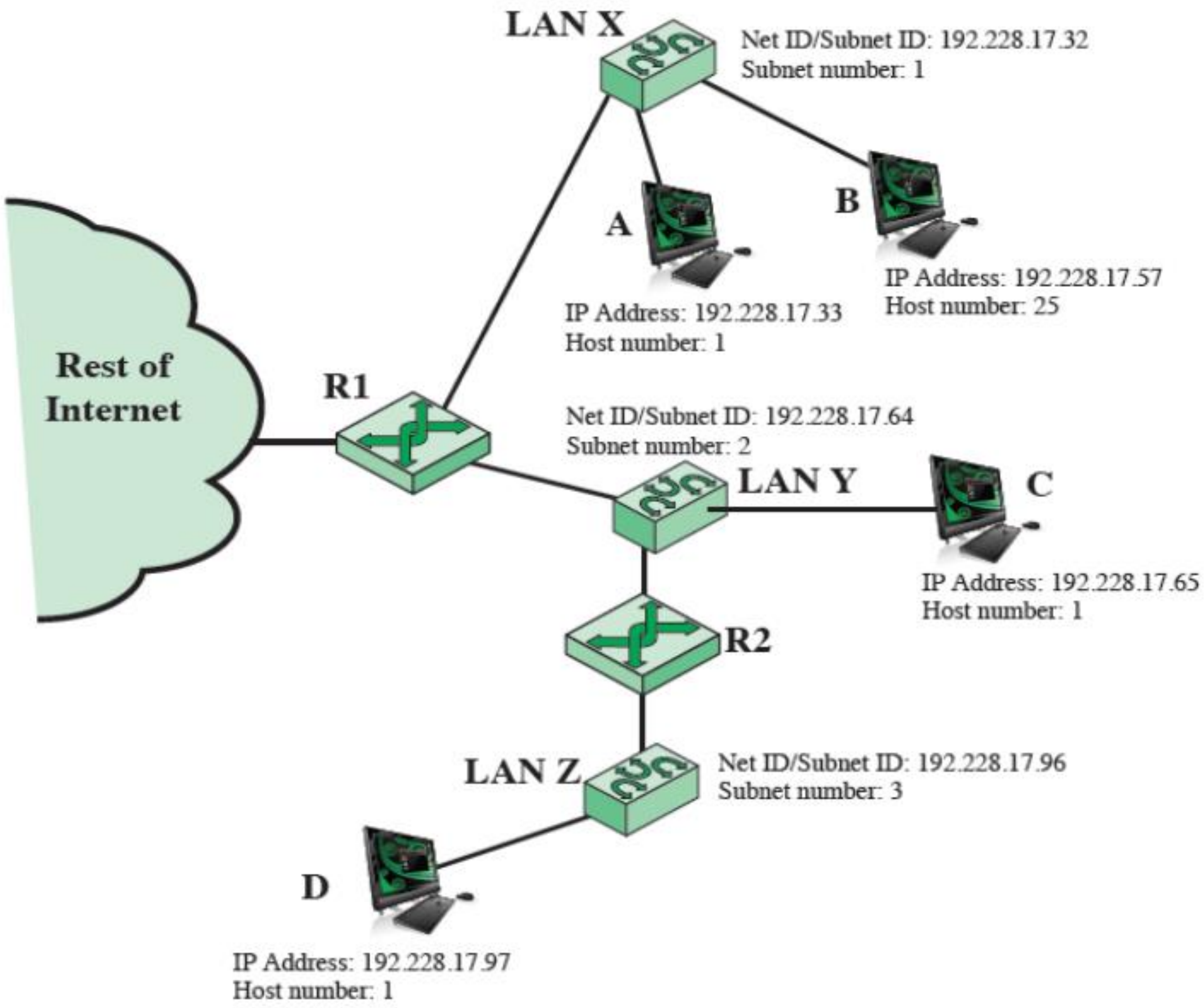
– IP Addresses and Subnet Masks

	Binary Representation	Dotted Decimal
IP address	11000000.11100100.00010001.00111001	192.228.17.57
Subnet mask	11111111.11111111.11111111.11100000	255.255.255.224
Bitwise AND of address and mask (resultant network/subnet number)	11000000.11100100.00010001.00100000	192.228.17.32
Subnet number	11000000.11100100.00010001.001	1
Host number	00000000.00000000.00000000.00011001	25

(b) Default subnet masks

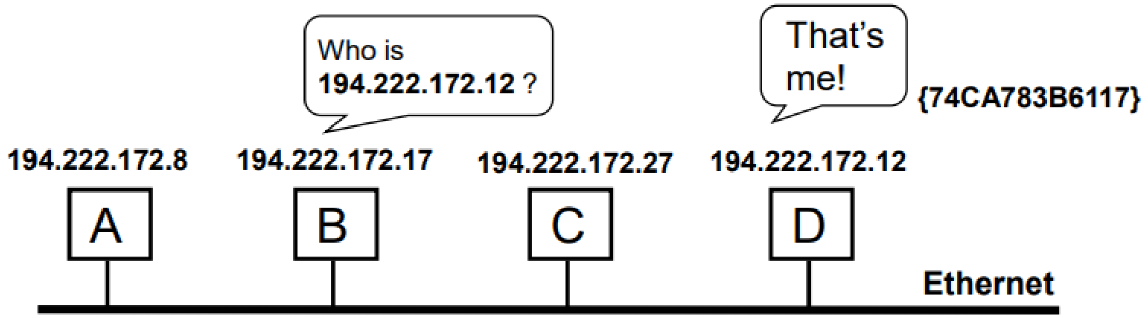
	Binary Representation	Dotted Decimal
Class A default mask	11111111.00000000.00000000.00000000	255.0.0.0
Example Class A mask	11111111.11000000.00000000.00000000	255.192.0.0
Class B default mask	11111111.11111111.00000000.00000000	255.255.0.0
Example Class B mask	11111111.11111111.11111000.00000000	255.255.248.0
Class C default mask	11111111.11111111.11111111.00000000	255. 255. 255.0
Example Class C mask	11111111.11111111.11111111.11111100	255. 255. 255.252

– An Example : Routing Using Subnets



Mapping IP Addresses to the DL

- Consider an Ethernet(IEEE802.3) LAN running IP
  - Recall data link layer has it's own 48-bit addresses
  - Network layer provide it's own 32-bit IP address space
  - Data link layer knows nothing about IP addresses
- How do these two sets of addresses get mapped?
  - ARP(Address Resolution Protocol, RFC 826) build a query message and broadcast it
  - All hosts in the network receive it and one says "that's me!"



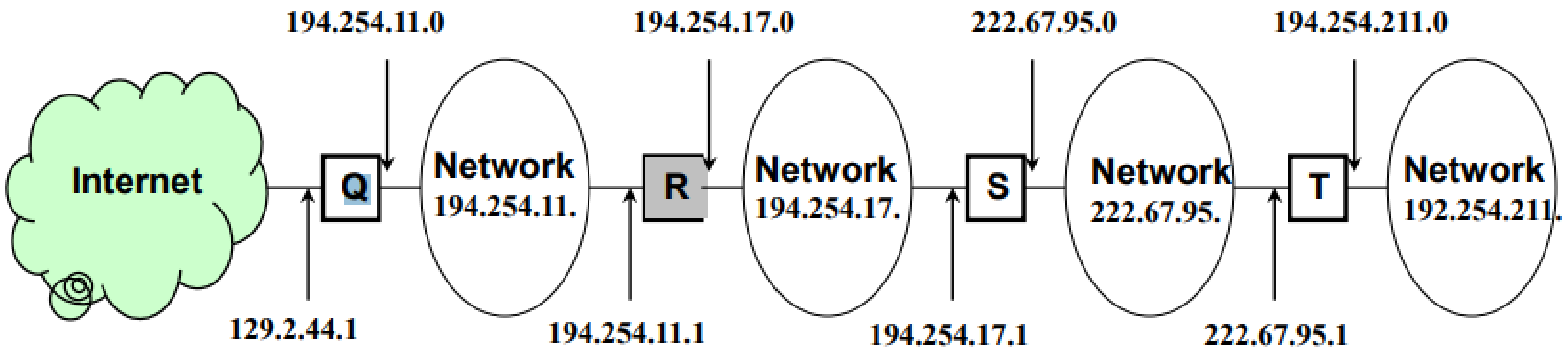
Address Resolution Protocol (ARP)

- ARP is a part of the physical network system
  - But it is not a part of the IP
- ARP is a low-level protocol that hides the underlying network physical addressing
  - And permits a machine to assign an arbitrary IP address
- Now, the broadcasting is too expensive, how can it be solved?
  - When a host receives an ARP reply, it saves the sender's IP address and its physical address in its cache for successive lookups
- Is it be possible more refinement?
  - The sender's IP-to-physical address binding is included in every ARP broadcast; receivers update the binding in their cache

Table Driven IP Routing

- IP routing employs an routing table on host and router
  - The routing table contains information about the possible destinations and how to reach them
  - IP consults the table to decide where to send the datagram
- Then, what information should be kept in routing tables?
  - Minimal information principle : keep network prefix only
  - Information hiding principle : specifies one step along the path from the router to a destination
  - Default routing : if no route appears in the table, the routing routines send the datagram to a default router

– Table Driven IP Routing (An Example)



To reach hosts on network	Route to this address
194.254.11	Deliver Directly
194.254.17	Deliver Directly
222.67.95	194.254.17.1
192.254.211	194.254.17.1
Default	194.254.11.0

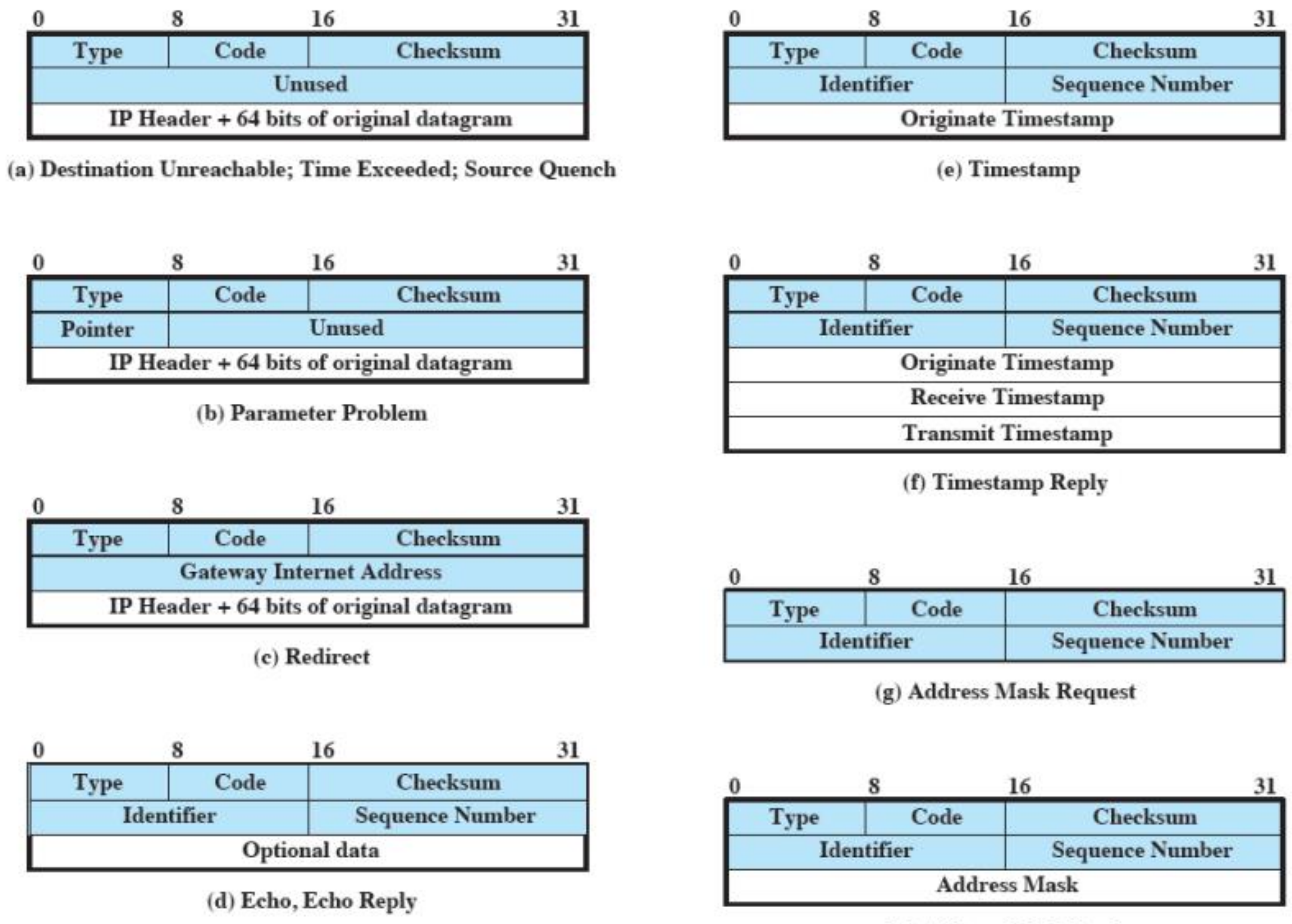
Routing Protocols in IPv4

- IP routing is based on the destination network ID alone?
  - All IP traffic for a given network tales the same path regardless to the delay or throughput of physical network
  - Only the final router can determine if the destination exists or is operational, the router only can report the delivery to the sender
  - Each router routes traffic independently – someone should find out if two-way communication is always possible
- IP routing selects the next hop to be sent the datagram
  - IP simply passes the datagram and the next hop IP address to the network interface software (so-called network driver)
  - The driver software responsible to bind the next hop IP address to a physical address, forms a frame, and sends it

Internet Control Message Protocol (ICMP)

- RFC 792
- Provides a means for transferring message from routers and other hosts to a host
- Mainly provides feedback about problems
  - Datagram cannot reach its destination
  - Router does not have buffer capacity to forward
  - Router can send traffic on a shorter route
- Encapsulated in IP datagram
  - Hence net reliable

– ICMP Message Format



(a) Destination Unreachable; Time Exceeded; Source Quench

(b) Parameter Problem

(c) Redirect

(d) Echo, Echo Reply

(e) Timestamp

(f) Timestamp Reply

(g) Address Mask Request

(h) Address Mask Reply

Why Change IP?

- Address space exhaustion
  - Two level addressing (network and host) wastes space
  - Network addresses used even if not connected to Internet
  - Growth of networks and the Internet
  - Single address per host
- Requirement for new types of service
  - Address configuration
  - Routing flexibility
  - Traffic support
- Security
- mobility

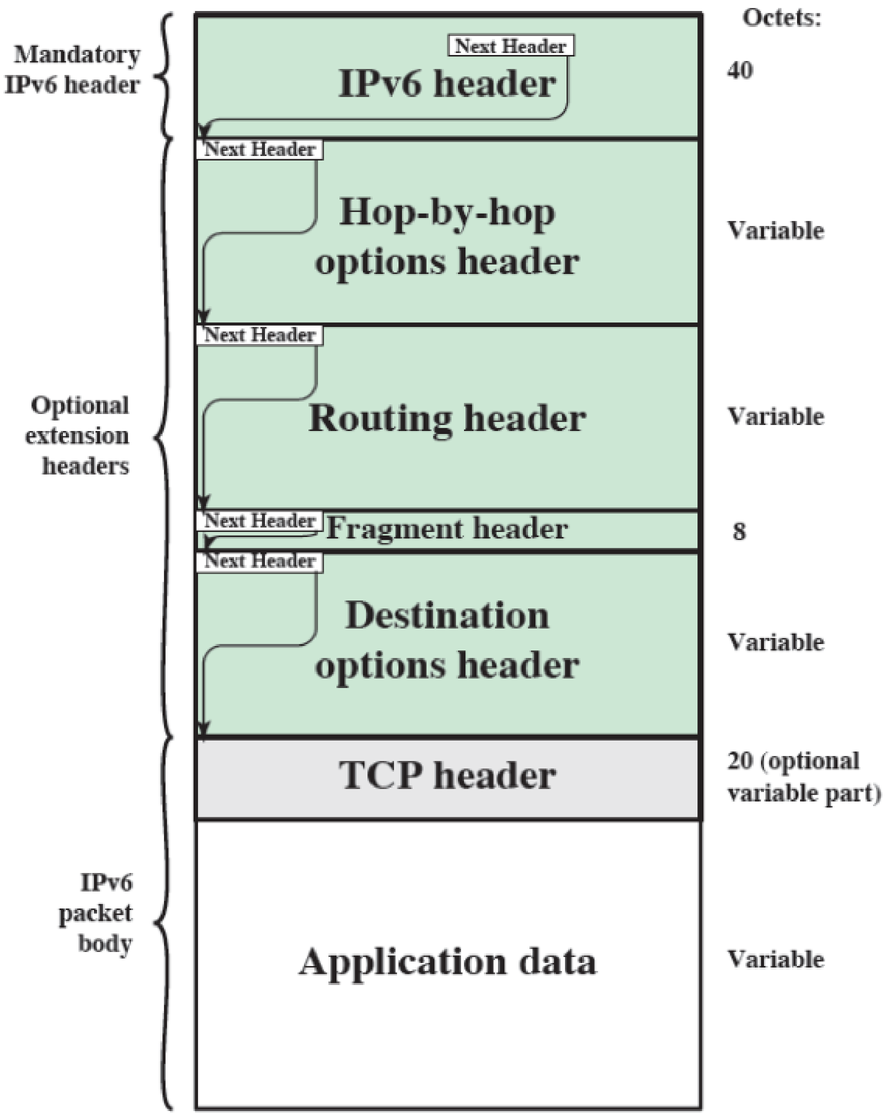
IPv6 RFCs

- IP versions
  - IP v1-3 defined and replaced
  - IP v4 - current version
  - IP v5 - streams protocol
  - IP v6 - replacement for IP v4 : during development it was called IPng(IP Next Generation)
- RFC 1752 – recommendations for the IPng
  - Requirements
  - Addressing, routing security issues
- RFC 2460 – overall specification
- RFC 4291 – addressing structure

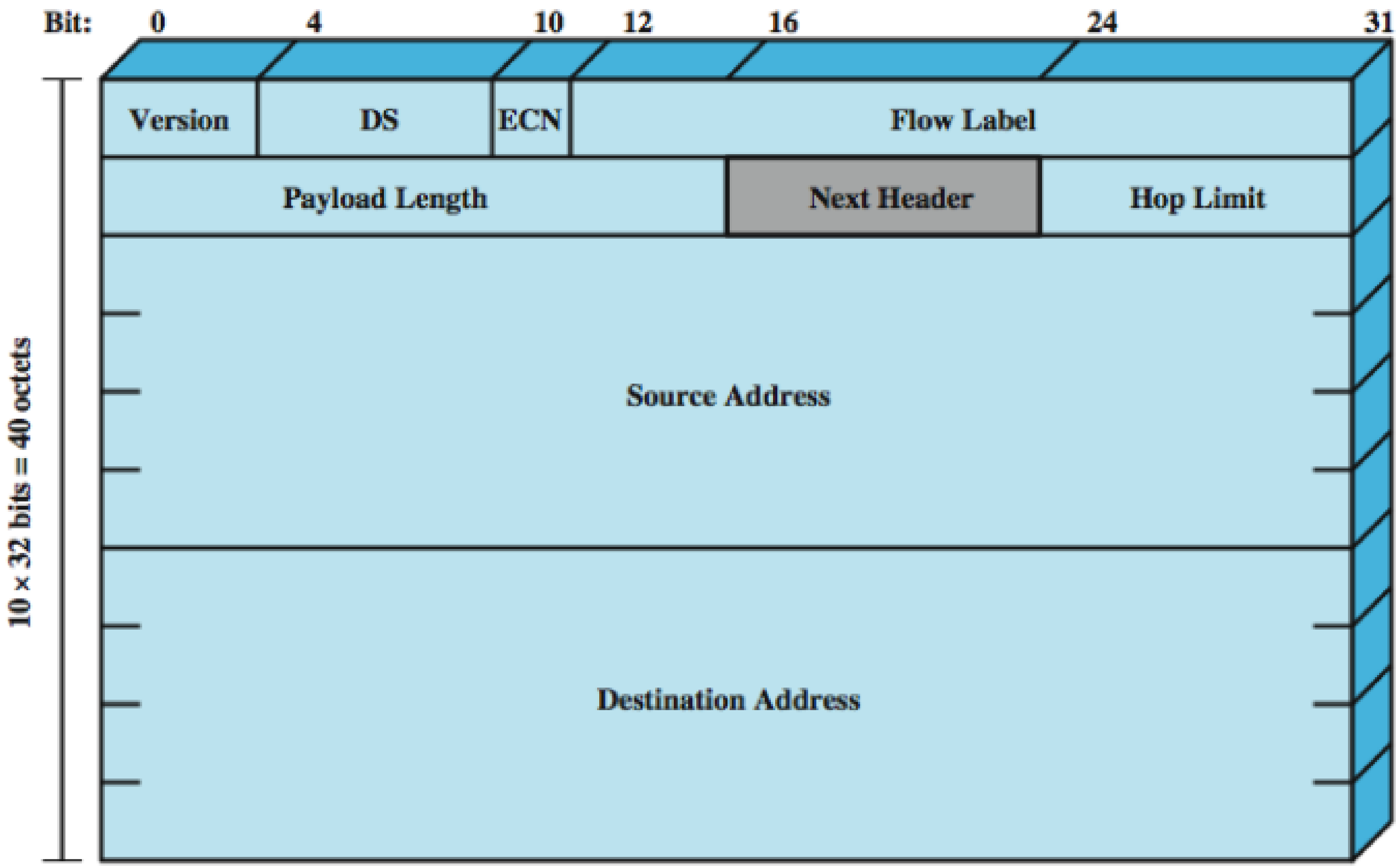
IPv6 Enhancements

- Expanded address space
  - 128 bit
- Improved option mechanism
  - Separate optional headers between IPv6 header and transport layer header (most are not examined by intermediate routes)
- Dynamic address assignment
- Increased addressing flexibility
  - Anycast – delivered to one of a set of nodes
- Support for resource allocation
  - Labeling of packets to particular traffic flow

– IPv6 Packet with Extension Headers



IPv6 Header



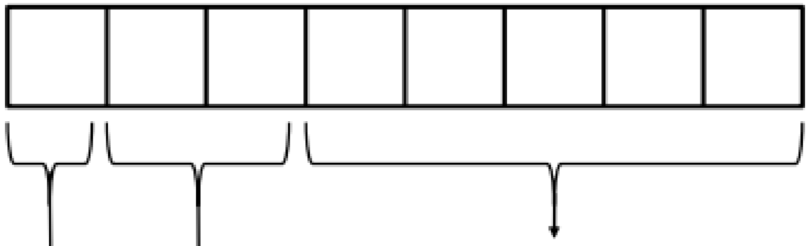
Bit: 0 4 10 12 16 24 31
Version
DS
ECN
Flow Label
Payload Length
Next Header
Hop Limit
Source Address
Destination Address
10 × 32 bits = 40 octets

IPv6 Flow Label

- Related sequence of packets
  - Needs a special handling for a specific packet
  - Identified by source and destination address + flow label
- Router treats flow as sharing attributes
  - E.g. path, resource allocation, discard requirements, security
- May treat flows differently
  - Buffer sizes, different forwarding precedence, different QoS
- Flow requirements are defined prior to flow start and a unique flow level is assigned to the flow
  - Alternative to including all info in every header

Next Header

It consists as:



option type : specify a particular option (including TCP/UDP)

indicate the action to be taken by a node that does't recognize this option type

00 : skip over this option and continue processing the header
01 : discard the packet
10 : discard the packet and send an ICMP parameter problem message to the packet source
11: discard the packet and send an ICMP parameter problem message to the packet source, for not a multicast address

specifies whether the Option Data field does't change(0), may change (1) on route from source to destination

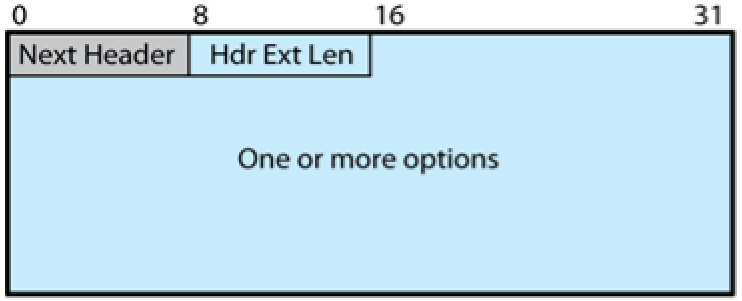
IPv6 Addresses

- 128 bits long
- Assigned to an interface rather than a host
  - Single interface may have multiple unicast addresses
- Three types of address
  - Unicast : single interface
  - Anycast : set of interfaces (typically different nodes), delivered to any one interface, usually the “nearest”
  - Multicast : set of interfaces, delivered to all interfaces identified

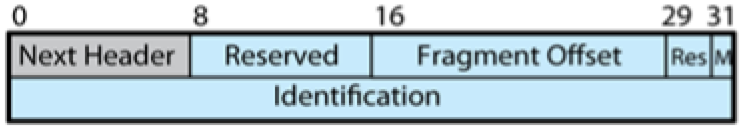
Extension Headers

- Hop-by-hop options
  - Require processing at each router
- Routing options
  - Similar to v4 source routing
- Fragmentation options
  - Only allowed at source, no fragmentation at intermediate routers
- Authentication options
  - Encapsulating security payload
- Destination options
  - Carries optional information for destination node

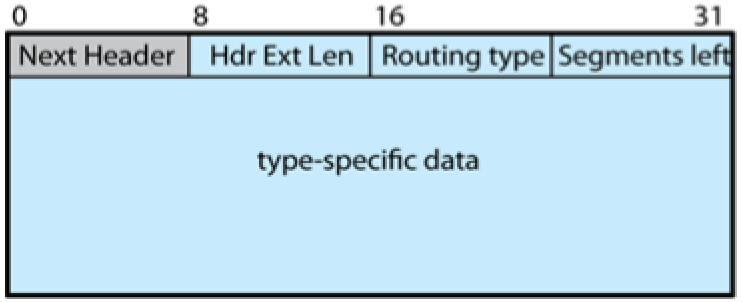
IPv6 Extension Headers



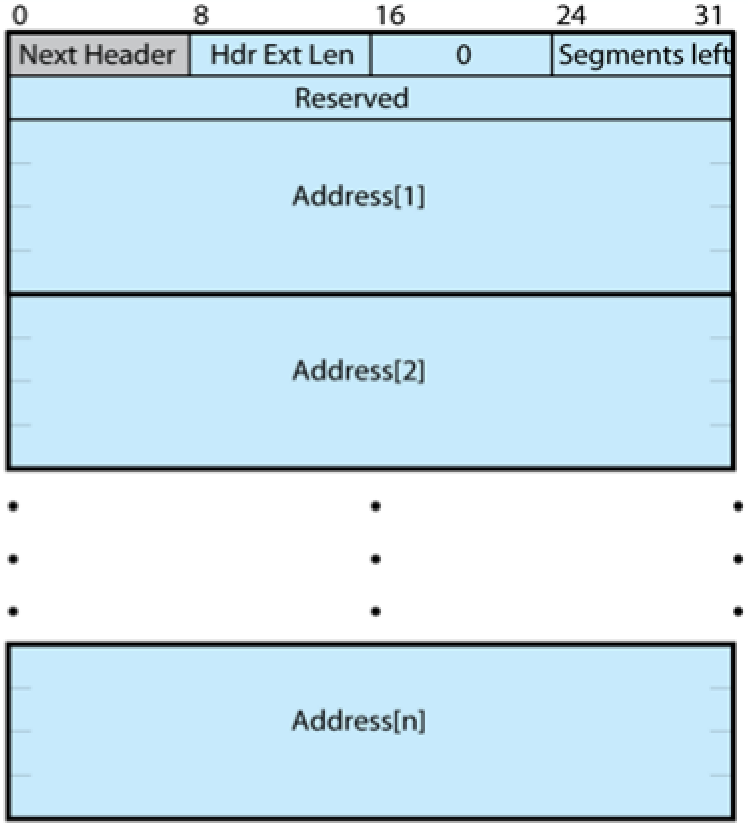
(a) Hop-by-hop options header;
destination options header



(b) Fragment header



(c) Generic routing header



(d) Type 0 routing header

Virtual Private Network (VPN)

- Set of computers interconnected using an unsecure network, as Internet
  - But they provide a secure channel between the organizations, much like as a private network
- Using encryption & special protocols to provide security
  - Eavesdropping (cryptography)
  - Entry point for unauthorized users (authentication)
- Proprietary solutions are problematical
  - Hence, develop the IPSec standard

IPSEC

- RFC 1636 (1994) identified security need
- Encryption & authentication to be IPv6
  - But designed also for use with current IPv4
- Applications needing security include:
  - Branch office connectivity
  - Electronic commerce security
- Benefits
  - Provides strong security for external traffic
  - Resistant to bypass
  - Can be transparent to applications as well as end users

IPSEC Function

- Authentication header
  - For authentication only
- Encapsulating Security Payload (ESP)
  - For combined authentication/encryption
- A key exchange function
  - Manual or automated
- VPNs usually need combined functions

– IPSEC Scenario : VPN