# Internet Protocols (chapter 18)

CSE 3213

Fall 2011

**Communication Network**
A facility that provides a data transfer service among devices attached to the network.

**Internet**
A collection of communication networks interconnected by bridges and/or routers.

**Intranet**
An internet used by a single organization that provides the key Internet applications, especially the World Wide Web. An intranet operates within the organization for internal purposes and can exist as an isolated, self-contained internet, or may have links to the Internet.

**Subnetwork**
Refers to a constituent network of an internet. This avoids ambiguity because the entire internet, from a user's point of view, is a single network.

**End System (ES)**
A device attached to one of the networks of an internet that is used to support end-user applications or services.

**Intermediate System (IS)**
A device used to connect two networks and permit communication between end systems attached to different networks.

**Bridge**
An IS used to connect two LANs that use similar LAN protocols. The bridge acts as an address filter, picking up packets from one LAN that are intended for a destination on another LAN and passing those packets on. The bridge does not modify the contents of the packets and does not add anything to the packet. The bridge operates at layer 2 of the OSI model.

**Router**
An IS used to connect two networks that may or may not be similar. The router employs an internet protocol present in each router and each end system of the network. The router operates at layer 3 of the OSI model.

Internetworking Terms

# TCP/IP Concepts

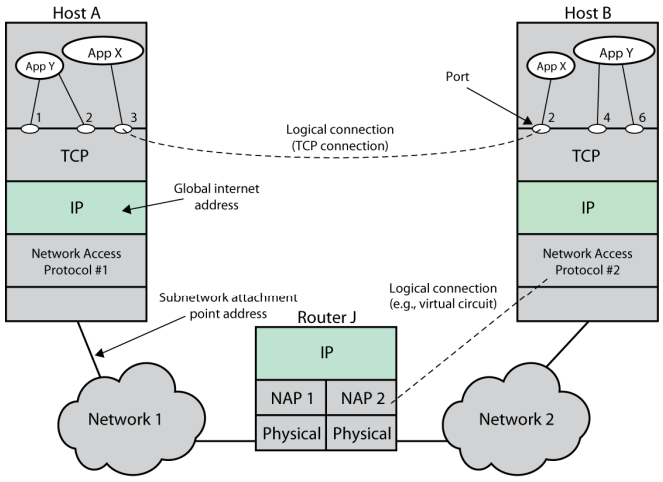



Figure 18.1 TCP/IP Concepts

# Connectionless Operation

- Internetworking involves connectionless operation at the level of the Internet Protocol (IP)

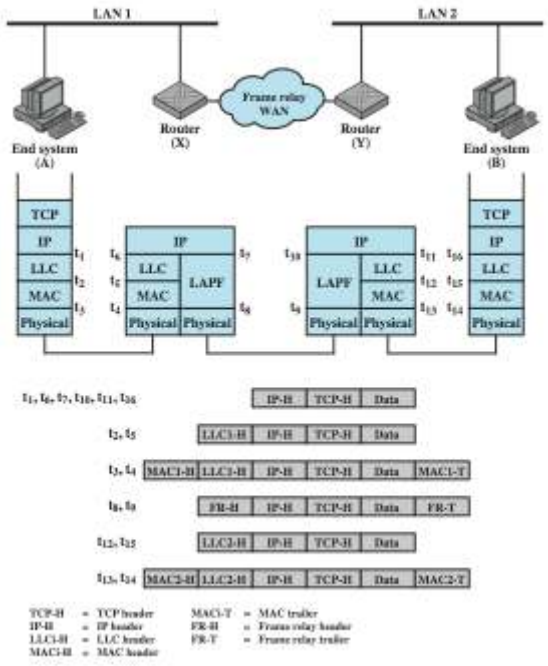
IP

- initially developed for the DARPA internet project
- protocol is needed to access a particular network

# Connectionless Internetworking

- Connectionless internet facility is flexible
- IP provides a connectionless service between end systems.
  - Advantages:
    - is flexible
    - can be made robust
    - does not impose unnecessary overhead

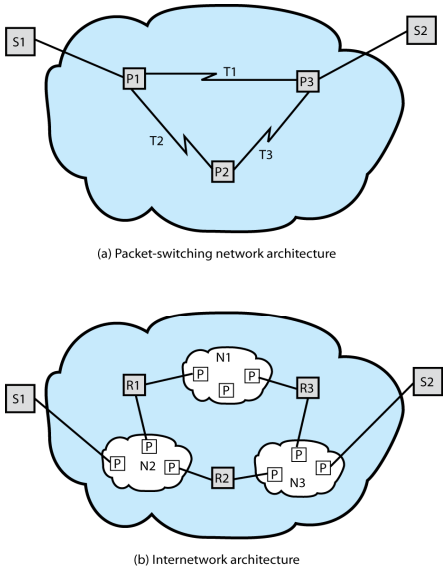
# IP Operation



# IP Design Issues

- routing
- datagram lifetime
- fragmentation and reassembly
- error control
- flow control

# The Internet as a Network

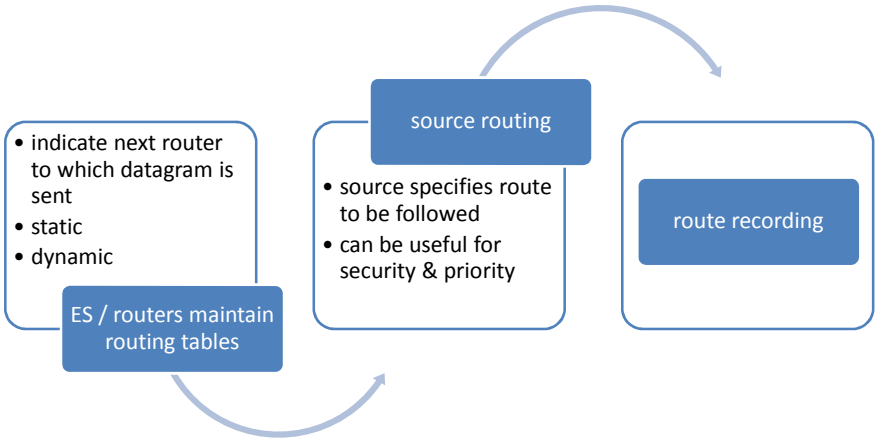



(a) Packet-switching network architecture

(b) Internetwork architecture

Figure 18.3 The Internet as a Network

# Routing



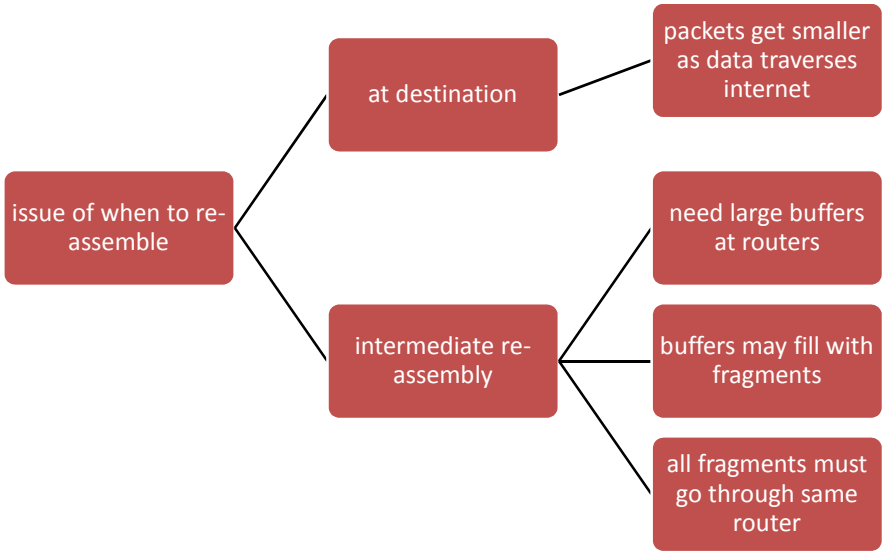

# Datagram Lifetime

- datagrams could loop indefinitely
  - consumes resources
  - transport protocol may need upper bound on lifetime of a datagram
    - can mark datagram with lifetime
    - when lifetime expires, datagram discarded

# Fragmentation and Re-assembly

- protocol exchanges data between two entities
- lower-level protocols may need to break data up into smaller blocks, called fragmentation
- reasons for fragmentation:
  - network only accepts blocks of a certain size
  - more efficient error control & smaller retransmission units
  - fairer access to shared facilities
  - smaller buffers
- disadvantages:
  - smaller buffers
  - more interrupts & processing time

# Fragmentation and Re-assembly



# IP Fragmentation

- IP re-assembles at destination only
- uses fields in header
  - Data Unit Identifier (ID)
    - identifies end system originated datagram
  - Data length
    - length of user data in octets
  - Offset
    - position of fragment of user data in original datagram
    - in multiples of 64 bits (8 octets)

*More* flag

- indicates that this is not the last fragment

# Fragmentation Example

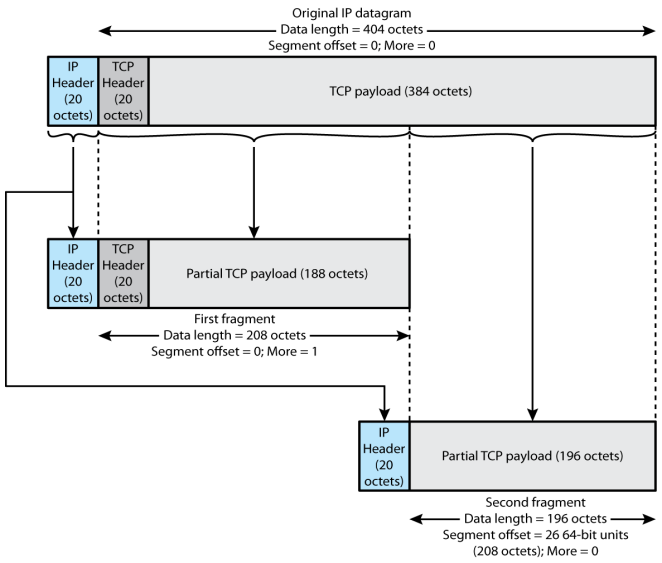



Figure 18.4 Fragmentation Example

# Error and Flow Control

- Error control
  - discarded datagram identification is needed
  - reasons for discarded datagrams include:
    - lifetime expiration
    - congestion
    - FCS error

➢Flow control

- allows routers to limit the rate they receive data
- send flow control packets requesting reduced data flow

# Internet Protocol (IP) v4

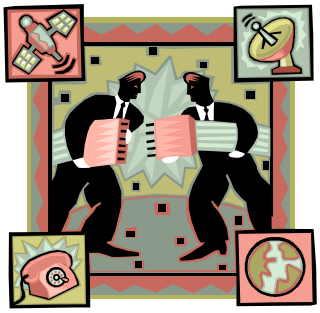
- defined in RFC 791
- part of TCP/IP suite
- two parts

specification of interface with a higher layer

specification of actual protocol format and mechanisms

# IP Services

- Primitives
  - specifies functions to be performed
  - form of primitive implementation dependent
  - Send - request transmission of data unit
  - Deliver - notify user of arrival of data unit
- Parameters
  - used to pass data and control information



# IP Parameters

- source and destination addresses
- protocol
- type of service
- identification
- don't fragment indicator
- time to live
- data length
- option data
- user data

# IP Options

- security
- route recording
- source routing
- stream identification
- timestamping

# IPv4 Header

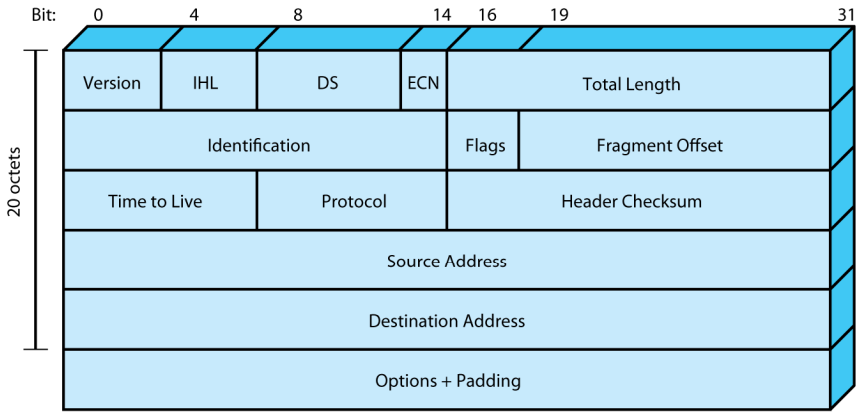
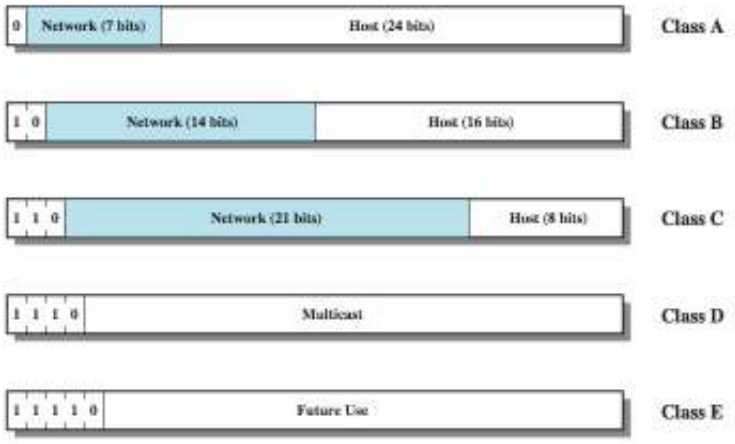



Figure 18.5 IPv4 Header

# IPv4 Address Formats




# IP Addresses - Class A

- start with binary 0
- all 0 reserved
- 01111111 (127) reserved for loopback
- range 1.x.x.x to 126.x.x.x

## IP Addresses - Class B

- start with binary 10
- range 128.x.x.x to 191.x.x.x
- second octet also included in network address
- $2^{14}$ = 16,384 class B addresses

## IP Addresses - Class C

- start with binary 110
- range 192.x.x.x to 223.x.x.x
- second and third octet also part of network address
- $2^{21}$ = 2,097,152 addresses
- nearly all allocated
  - see IPv6

# Subnets and Subnet Masks

- allows arbitrary complexity of internetworked LANs within 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 number and host number
- local routers route within subnetted network
- subnet mask indicates which bits are subnet number and which are host number

# IP Addresses and Subnet Masks

(a) Dotted decimal and binary representations of IP address 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 |

# Internet Control Message Protocol (ICMP)

- RFC 792
- transfer messages from routers and hosts to hosts
- 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 not reliable

# ICMP Message Format

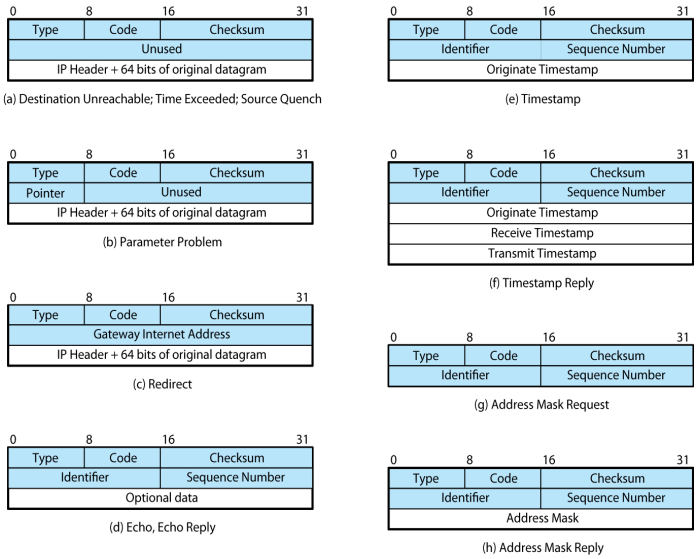



Figure 18.8 ICMP Message Formats

## Common ICMP Messages

- destination unreachable
- time exceeded
- parameter problem
- source quench
- redirect
- echo and echo reply
- timestamp and timestamp reply
- address mask request and reply

## Address Resolution Protocol (ARP)

need MAC address to send to LAN host

- manual
- included in network address
- use central directory
- use address resolution protocol

ARP (RFC 826) provides dynamic IP to Ethernet address mapping

- source broadcasts ARP request
- destination replies with ARP response

# IP Versions

- IP v 1-3 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)

# Why Change IP?

address space exhaustion:

- two level addressing (network and host) wastes space
- network addresses used even if not connected
- growth of networks and the Internet
- extended use of TCP/IP
- single address per host

requirements for new types of service

- address configuration routing flexibility
- traffic support

# IPv6 RFCs

- RFC 1752 - Recommendations for the IP Next Generation Protocol
  - requirements
  - PDU formats
  - addressing, routing security issues
- RFC 2460 - overall specification
- RFC 4291 - addressing structure

# IPv6 Enhancements

- expanded 128 bit address space
- improved option mechanism
  - most not examined by intermediate routes
- dynamic address assignment
- increased addressing flexibility
  - anycast & multicast
- support for resource allocation
  - labeled packet flows

# IPv6 PDU (Packet) Structure

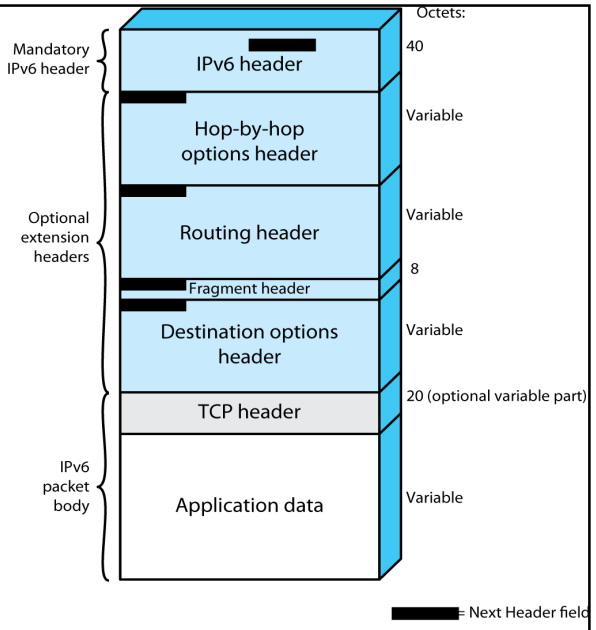
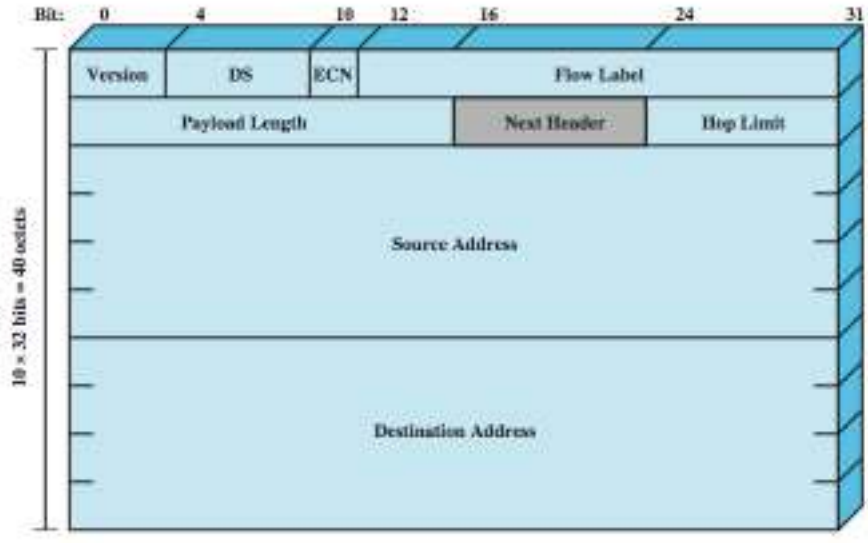



Figure 18.9 IPv6 Packet with Extension Headers (containing a TCP Segment)

# IP v6 Header



# IP v6 Flow Label

- related sequence of packets
- special handling
- identified by source and destination address + flow label
- router treats flow as sharing attributes
- may treat flows differently
- alternative to including all information in every header
- have requirements on flow label processing

# IPv6 Addresses

- 128 bits long
- assigned to interface
- single interface may have multiple unicast addresses

three types of addresses:

- unicast - single interface address
- anycast - one of a set of interface addresses
- multicast - all of a set of interfaces

## Hop-by-Hop Options

- must be examined by every router
  - if unknown discard/forward handling is specified
- next header
- header extension length
- options
  - Pad1
  - PadN
  - Jumbo payload
  - Router alert

## Fragmentation Header

- fragmentation only allowed at source
- no fragmentation at intermediate routers
- node must perform path discovery to find smallest MTU of intermediate networks
- set source fragments to match MTU
- otherwise limit to 1280 octets

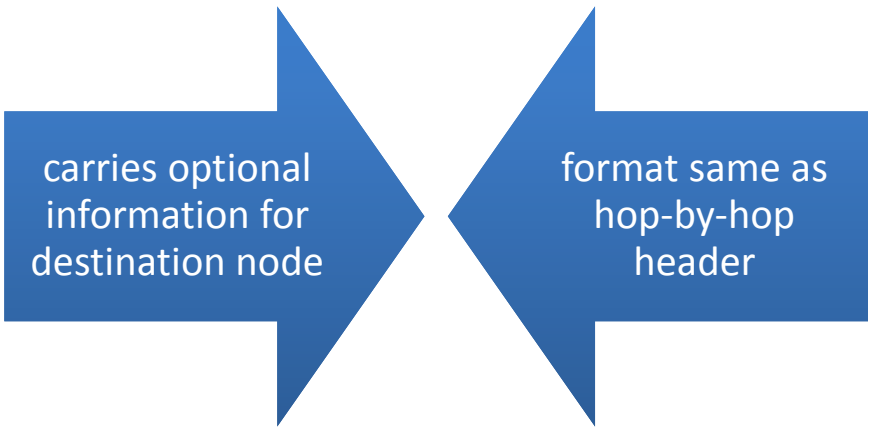
# Routing Header

- contains a list of one or more intermediate nodes to be visited on the way to a packet's destination

header includes
- **next header**
- **header extension length**
- **routing type**
- **segments left**

Type 0 routing provides a list of addresses
- **initial destination address is first on list**
- **current destination address is next on list**
- **final destination address will be last in list**

# Destination Options Header



# IPv6 Extension Headers

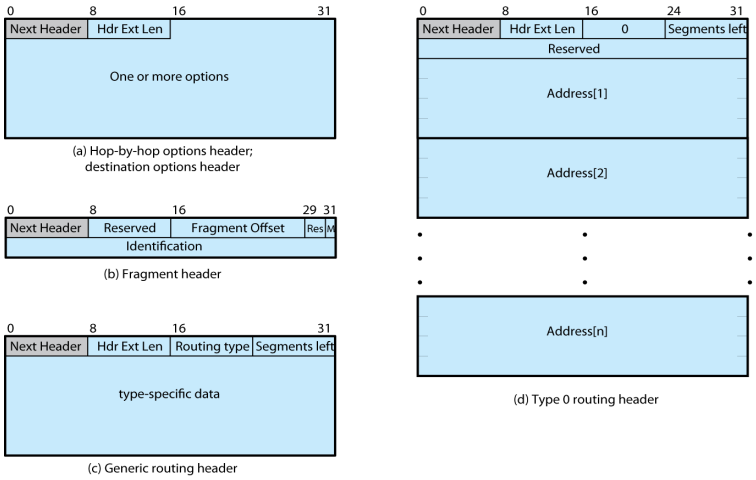



Figure 18.11 IPv6 Extension Headers

# Reading

- Chapter 18, Stallings
- Next lecture: Internetworking Operation (Chapter 19)