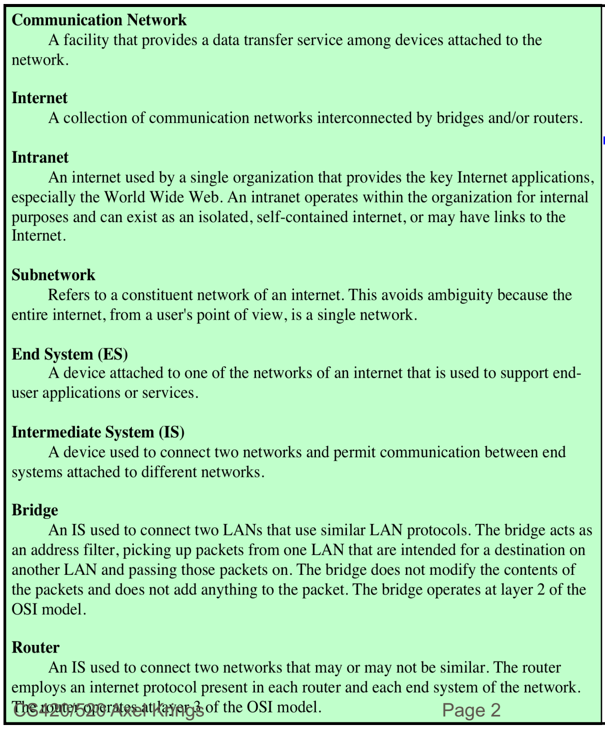
The Internet Protocol

Chapter 14 in Stallings 10th Edition



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.

Table 14.1

Internetworking Terms

(Table is on page 429 in the textbook)

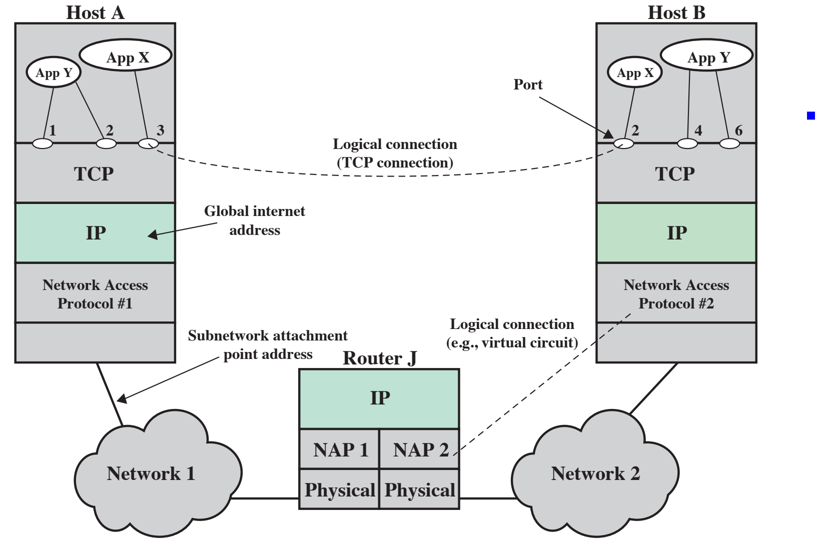
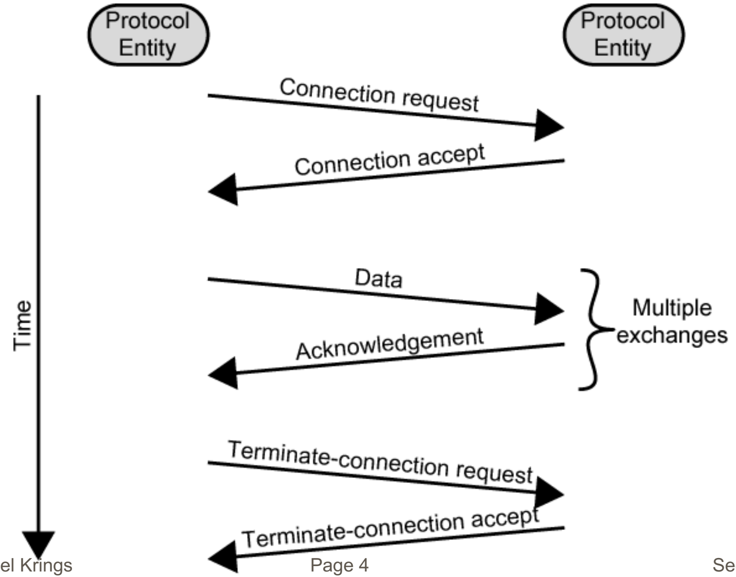


Figure 14.1 TCP/IP Concepts

Why we do not want Connection Oriented Transfer



Protocol Entity

Protocol Entity

Time

Connection request

Connection accept

Data

Acknowledgement

Multiple exchanges

Terminate-connection request

Terminate-connection accept

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

- Advantages
  - —Flexibility
  - —Robust
  - —No unnecessary overhead
- Unreliable
  - —Not guaranteed delivery
  - —Not guaranteed order of delivery
    - Packets can take different routes
  - —Reliability is responsibility of next layer up (e.g. TCP)

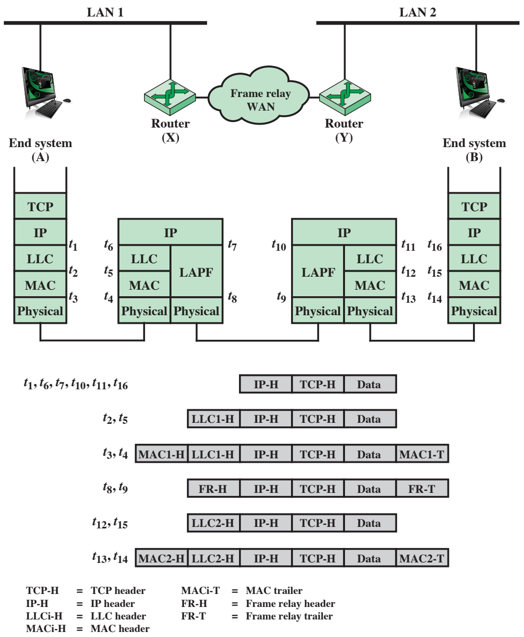

LAN 1
LAN 2
Frame relay WAN
Router (X)
Router (Y)
End system (A)
End system (B)
TCP
IP
LLC
MAC
Physical
LAPF
t_1 t_2 t_3 t_4 t_5 t_6 t_7 t_8 t_9 t_{10} t_{11} t_{12} t_{13} t_{14} t_{15} t_{16}
$t_1, t_6, t_7, t_{10}, t_{11}, t_{16}$ IP-H TCP-H Data
t_2, t_5 LLC1-H IP-H TCP-H Data
t_3, t_4 MAC1-H LLC1-H IP-H TCP-H Data MAC1-T
t_8, t_9 FR-H IP-H TCP-H Data FR-T
t_{12}, t_{15} LLC2-H IP-H TCP-H Data
t_{13}, t_{14} MAC2-H LLC2-H IP-H TCP-H Data MAC2-T
TCP-H = TCP header
IP-H = IP header
LLCi-H = LLC header
MACi-H = MAC header
MACi-T = MAC trailer
FR-H = Frame relay header
FR-T = Frame relay trailer

Figure 14.2 Example of Internet Protocol Operation

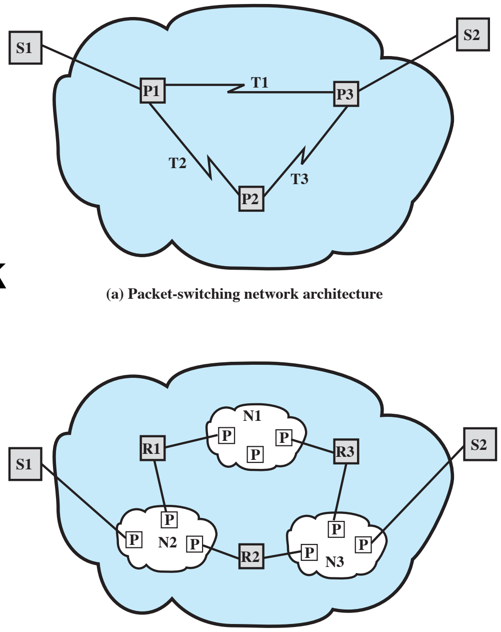
Connectionless Internetworking

- 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 Design Issues

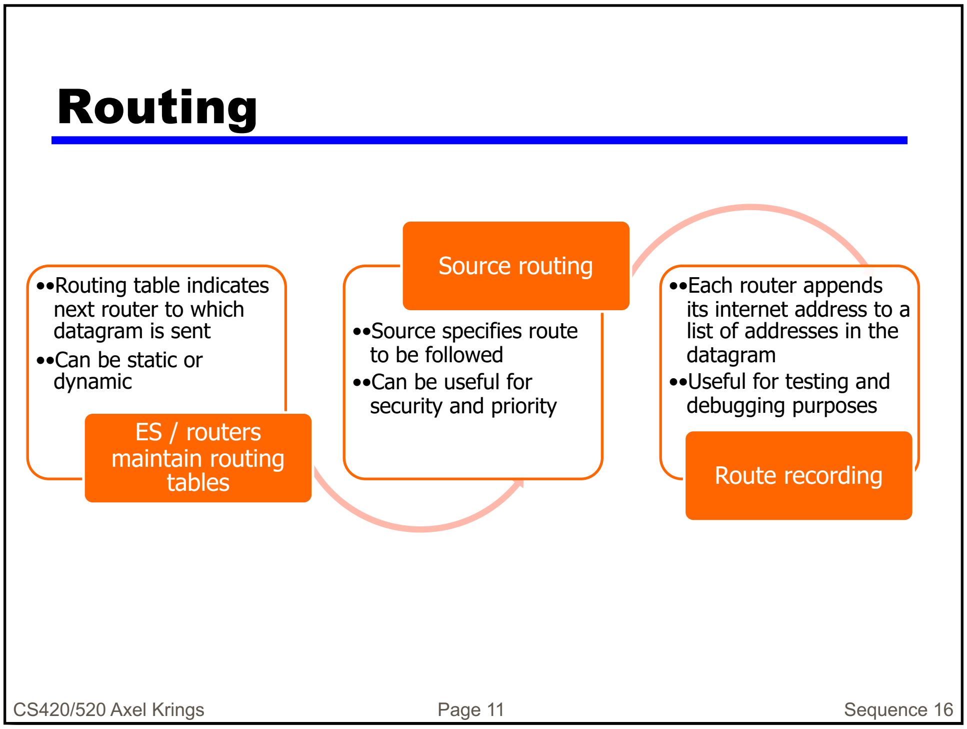
- Routing
- Datagram lifetime
- Fragmentation and reassembly
- Error control
- Flow control

The Internet as a Network



(a) Packet-switching network architecture

(b) Internetwork architecture



Routing

ES / routers maintain routing tables

••Routing table indicates next router to which datagram is sent

••Can be static or dynamic

Source routing

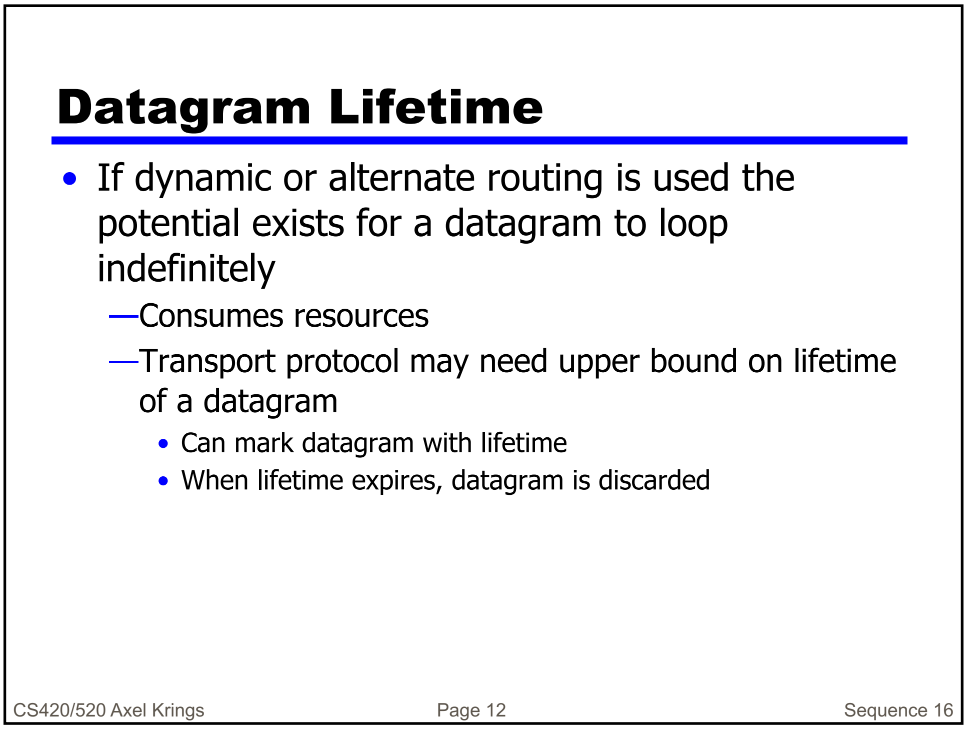
••Source specifies route to be followed

••Can be useful for security and priority

Route recording

••Each router appends its internet address to a list of addresses in the datagram

••Useful for testing and debugging purposes



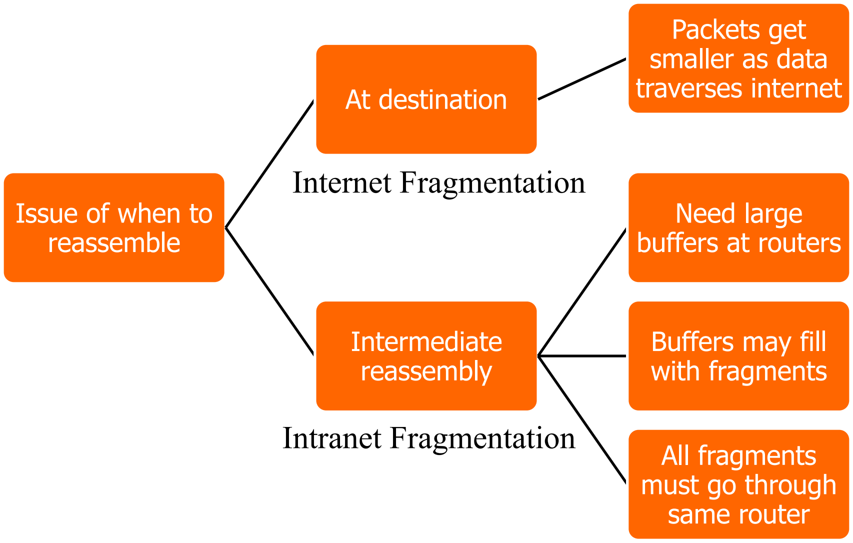
Datagram Lifetime

- If dynamic or alternate routing is used the potential exists for a datagram to loop indefinitely
  - —Consumes resources
  - —Transport protocol may need upper bound on lifetime of a datagram
    - Can mark datagram with lifetime
    - When lifetime expires, datagram is 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 and smaller retransmission units
  - Fairer access to shared facilities
  - Smaller buffers
- Disadvantages:
  - Smaller buffers
  - More interrupts and processing time

Fragmentation and Reassembly



Issue of when to reassemble

At destination

Packets get smaller as data traverses internet

Internet Fragmentation

Intermediate reassembly

Need large buffers at routers

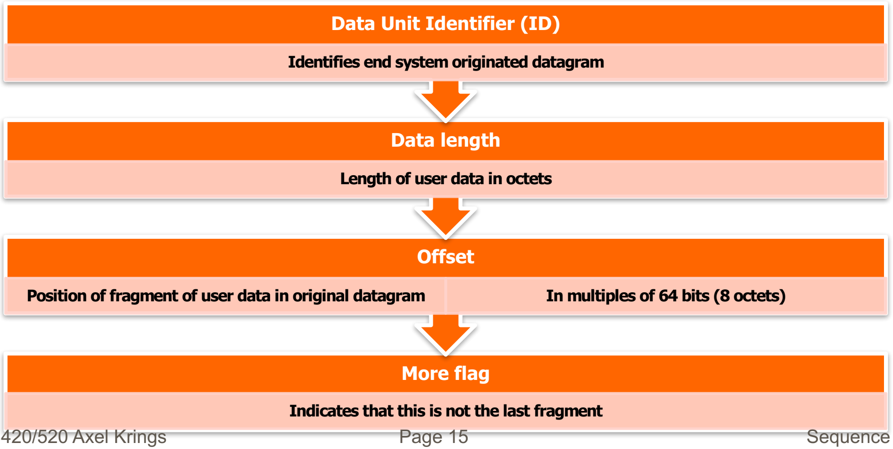
Buffers may fill with fragments

All fragments must go through same router

Intranet Fragmentation

IP Fragmentation

- IP reassembles 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

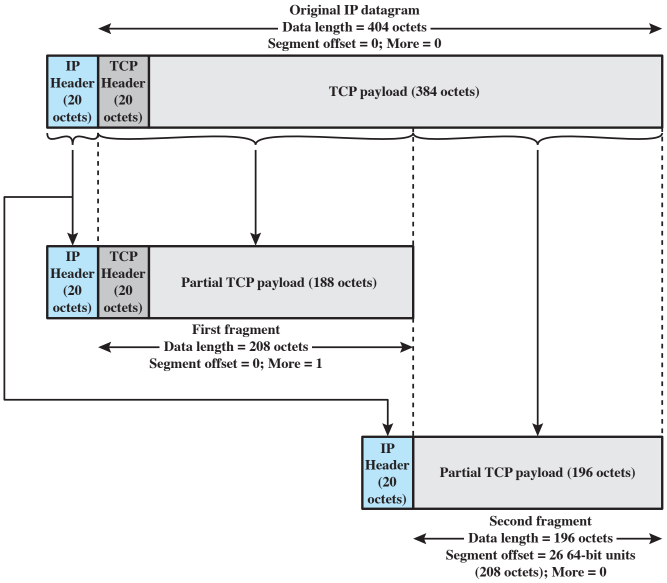


Figure 14.4 Fragmentation Example

Error and Flow Control

Error control

- Discarded datagram identification is needed
- Reasons for discarded datagrams include:
  - Lifetime expiration
  - Congestion
  - FCS error

Flow control

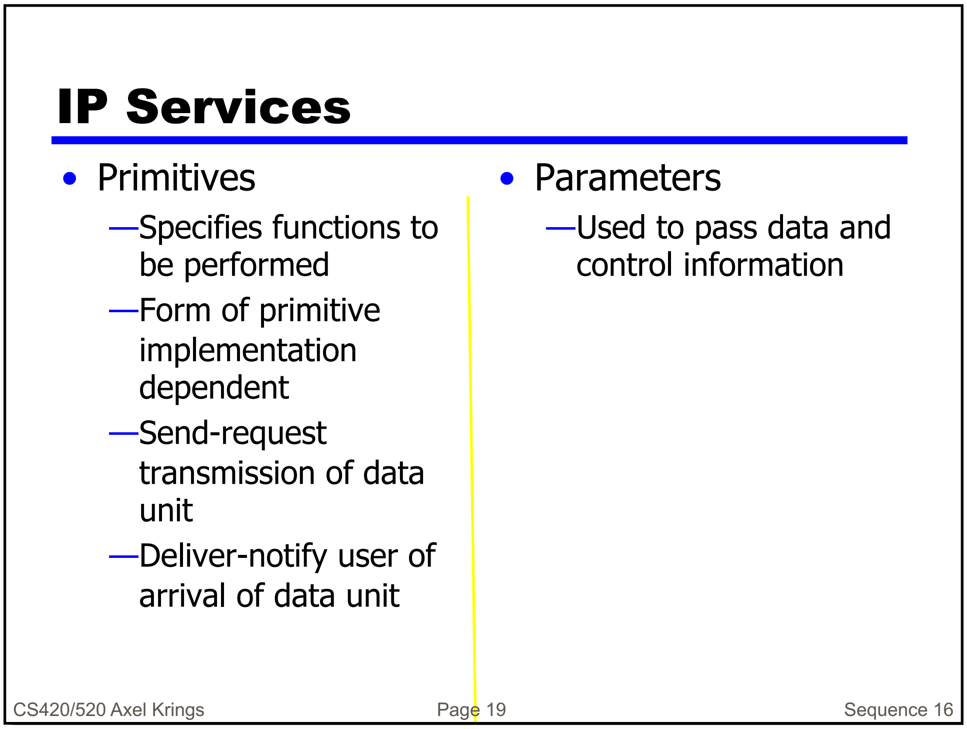
- Allows routers to limit the rate they receive data
- Send flow control packets requesting reduced data flow

Internet Protocol (IP) v4

- Defined in RFC 791
- Part of TCP/IP suite
- Two parts

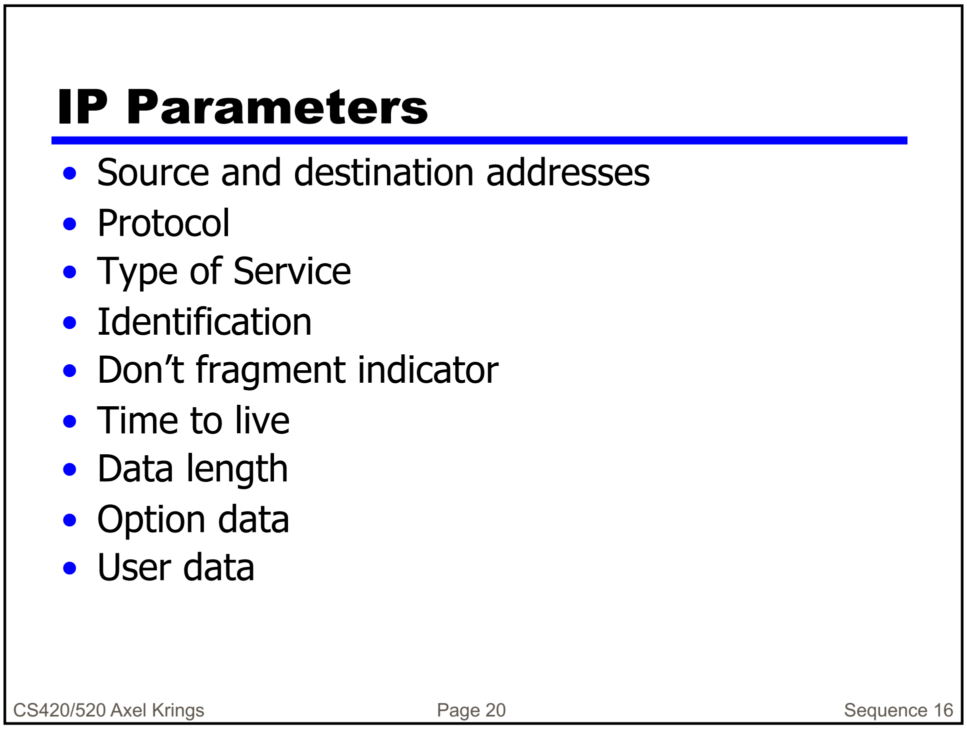
Specification of interface with a higher layer

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

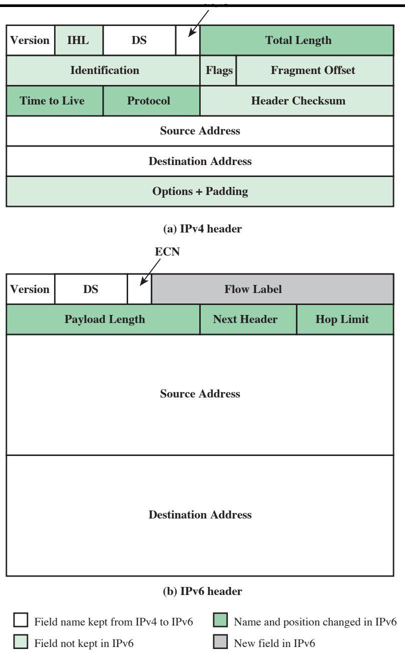


IP Parameters

- 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



(a) IPv4 header

(b) IPv6 header

Figure 14.5 IPv4 and IPv6 Headers

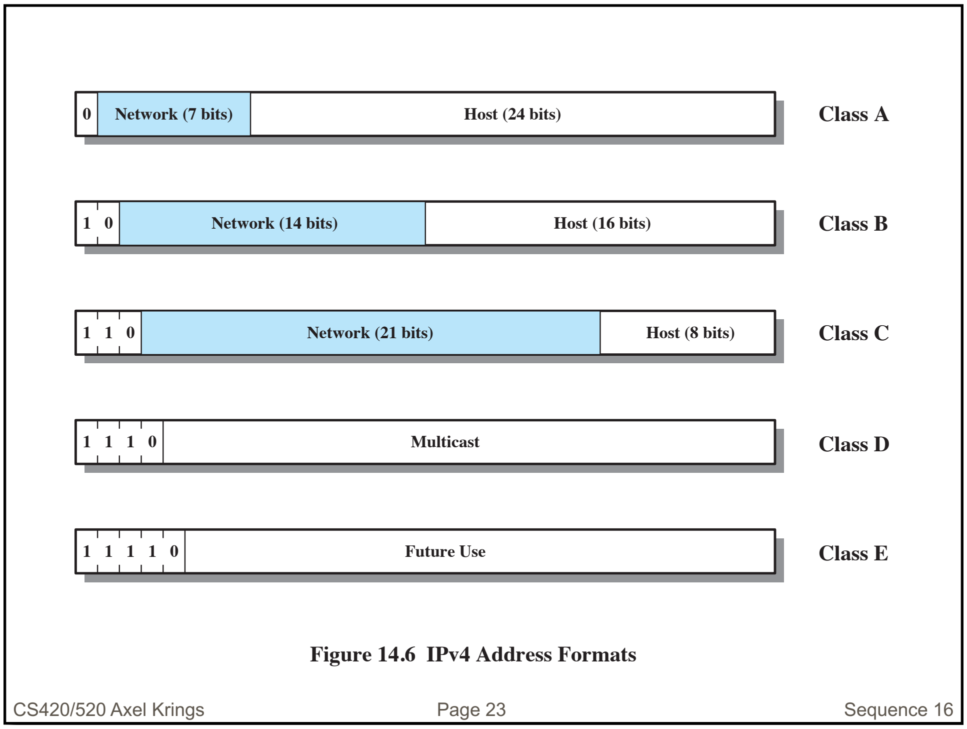
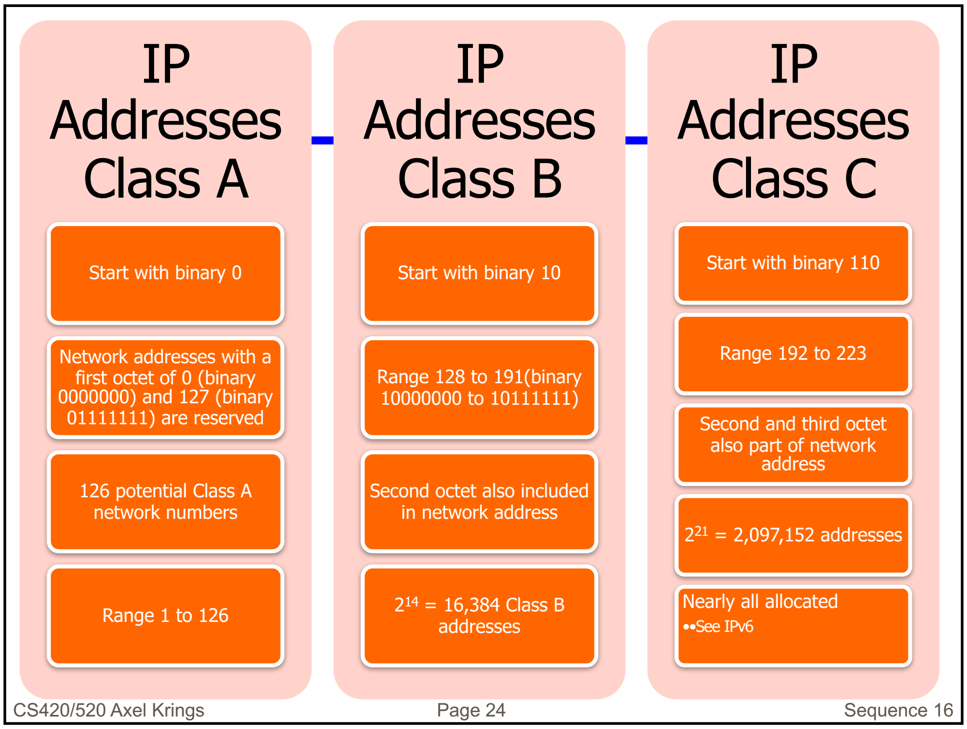


Figure 14.6 IPv4 Address Formats



IP Addresses Class A

- Start with binary 0
- Network addresses with a first octet of 0 (binary 0000000) and 127 (binary 01111111) are reserved
- 126 potential Class A network numbers
- Range 1 to 126

IP Addresses Class B

- Start with binary 10
- Range 128 to 191(binary 10000000 to 10111111)
- Second octet also included in network address
- 2^{14} = 16,384 Class B addresses

IP Addresses Class C

- Start with binary 110
- Range 192 to 223
- 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

Table 14.2

IPv4 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

(a) Dotted decimal and binary representations of IPv4 address and 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

(b) Default subnet masks

Inter-domain Routing

- Classless Inter-Domain Routing - CIDR
  - —Introduced in 1993 by the Internet Engineering Task Force
  - —Goal was to slow the growth of routing tables on routers across the Internet, and to help slow the rapid exhaustion of IPv4 addresses
  - —CIDR appends a "/" character to the address and the decimal number of leading bits of the routing prefix
  - —Example:
    - 192.168.1.0/24 for IPv4
    - 2001:db8::/32 for IPv6

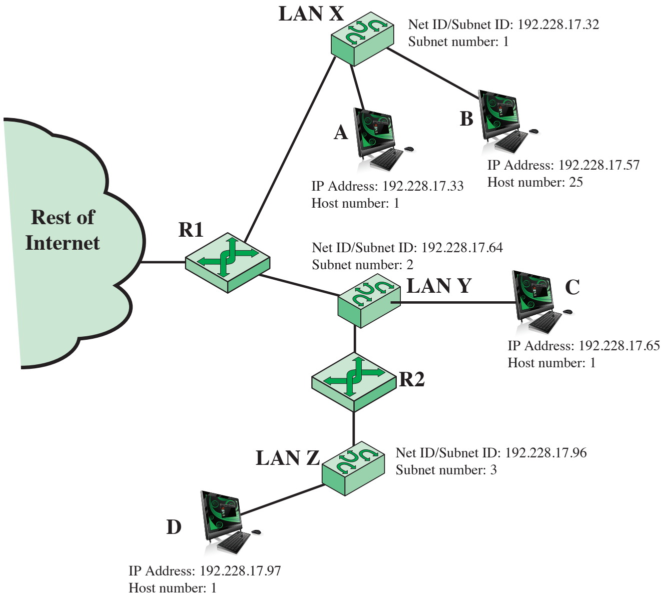

LAN X
Net ID/Subnet ID: 192.228.17.32
Subnet number: 1
A
B
IP Address: 192.228.17.33
Host number: 1
IP Address: 192.228.17.57
Host number: 25
Rest of Internet
R1
Net ID/Subnet ID: 192.228.17.64
Subnet number: 2
LAN Y
C
IP Address: 192.228.17.65
Host number: 1
R2
LAN Z
Net ID/Subnet ID: 192.228.17.96
Subnet number: 3
D
IP Address: 192.228.17.97
Host number: 1

Figure 14.7 Example of Subnetworking

Internet Control Message Protocol (ICMP)

- RFC 792
- Provides a means for transferring messages from routers and other hosts to a host
- 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

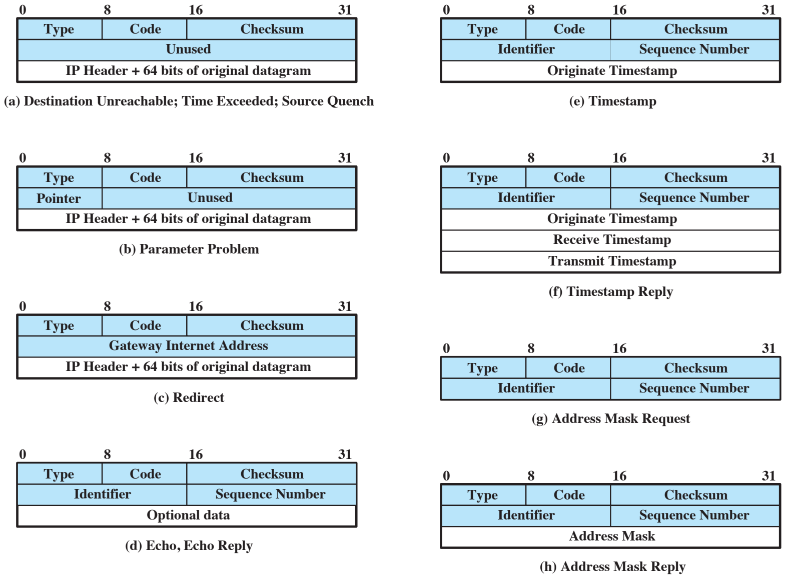


Figure 14.8 ICMP Message Formats

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

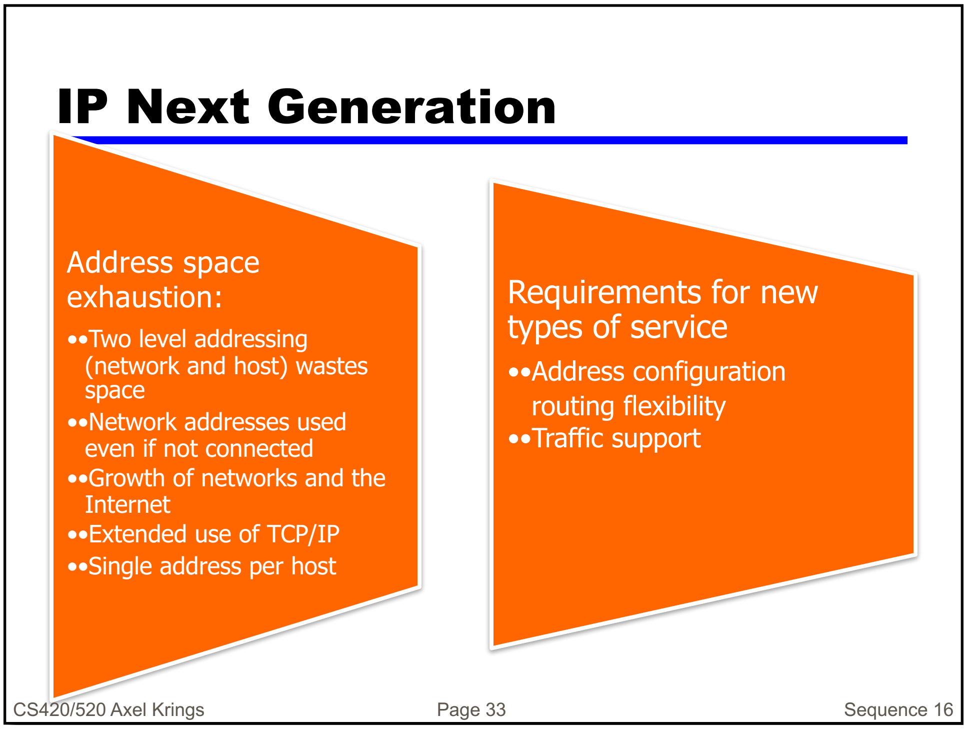
Address Resolution Protocol (ARP)

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 Next Generation

Address space exhaustion:

••Two level addressing (network and host) wastes space

••Network addresses used even if not connected

••Growth of networks and the Internet

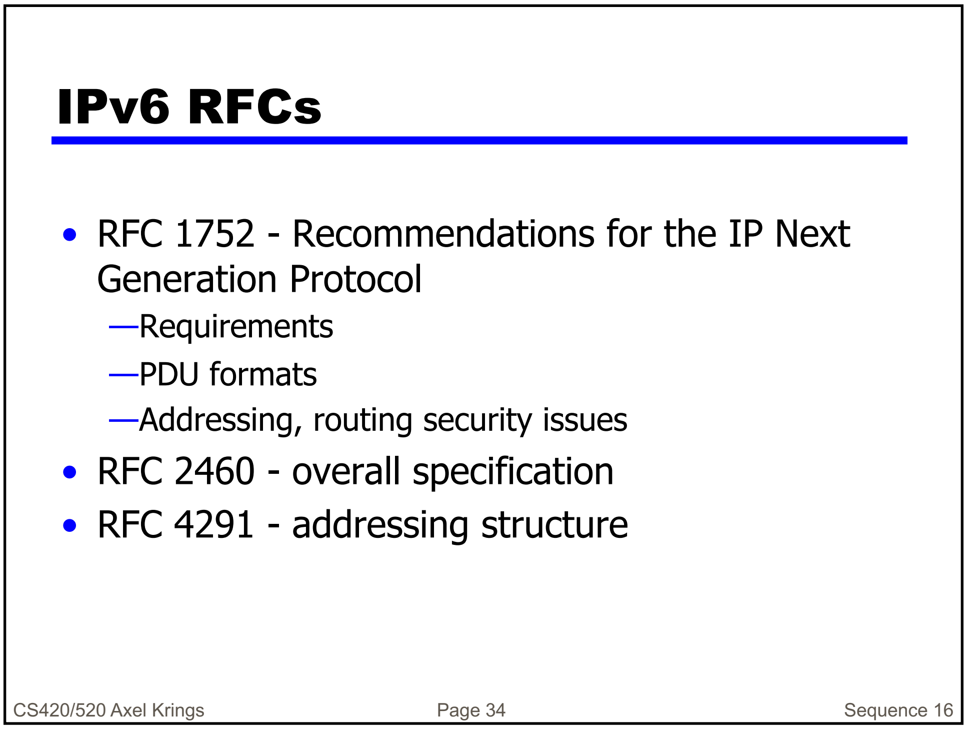
••Extended use of TCP/IP

••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** and multicast
- Support for resource allocation
  - —Labeled packet flows

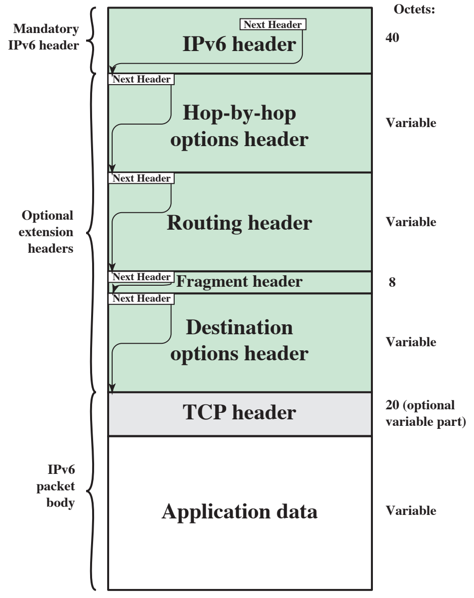
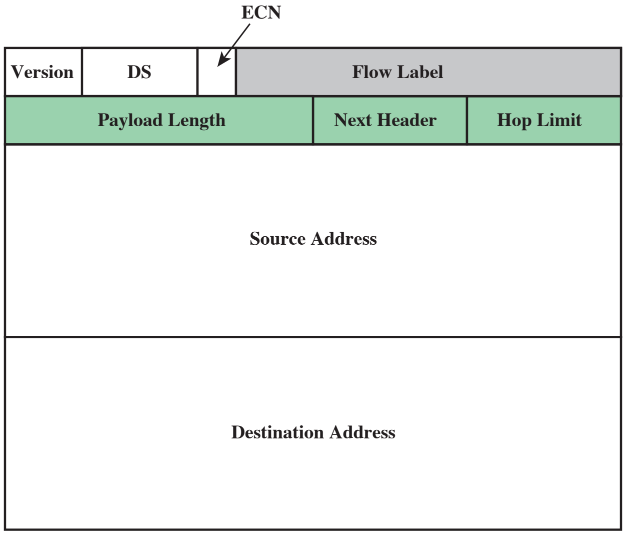


Figure 14.9 IPv6 Packet with Extension Headers (containing a TCP Segment)



(b) IPv6 header

□ Field name kept from IPv4 to IPv6

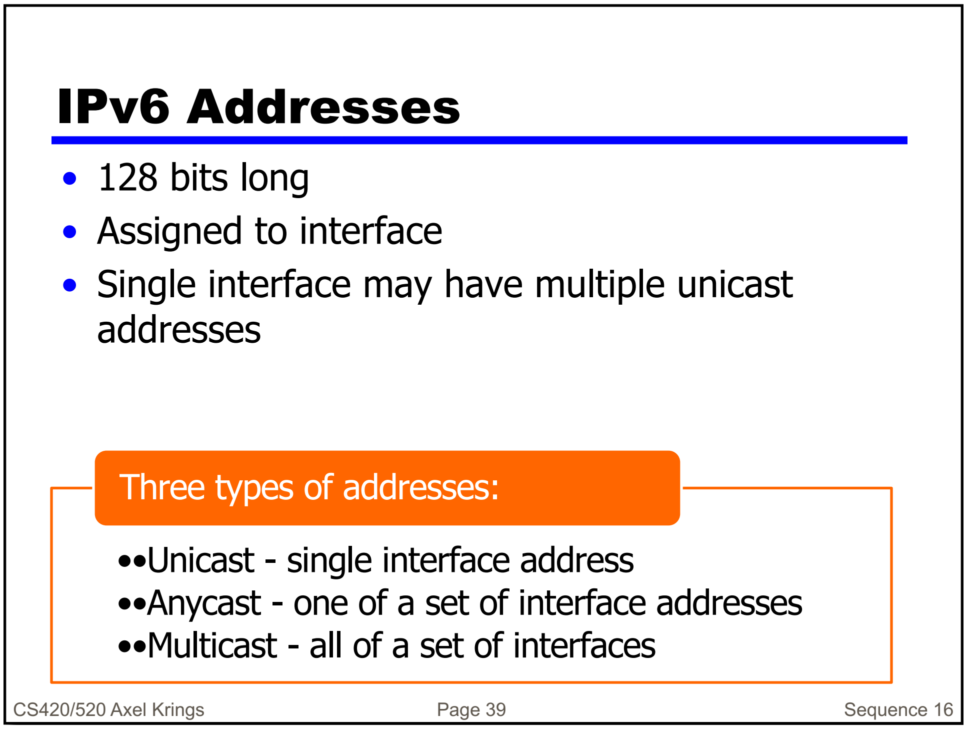
🟩 Name and position changed in IPv6

▢ Field not kept in IPv6

▨ New field in IPv6

IPv6 Flow Label

- Related sequence of packets
- Special handling
- Identified by source and destination address plus 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

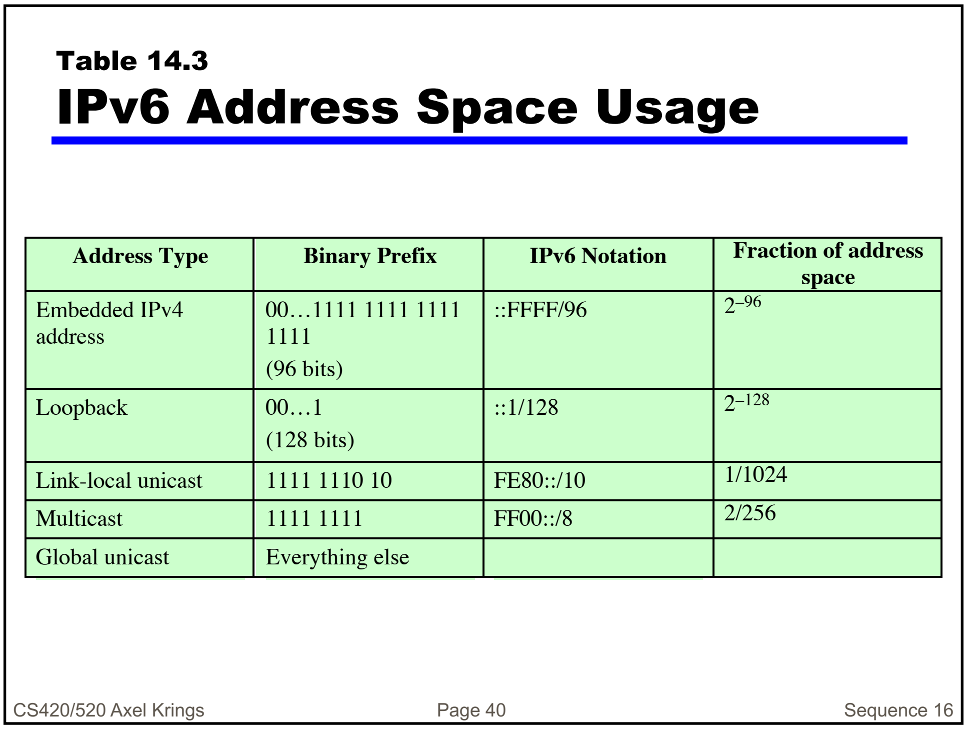
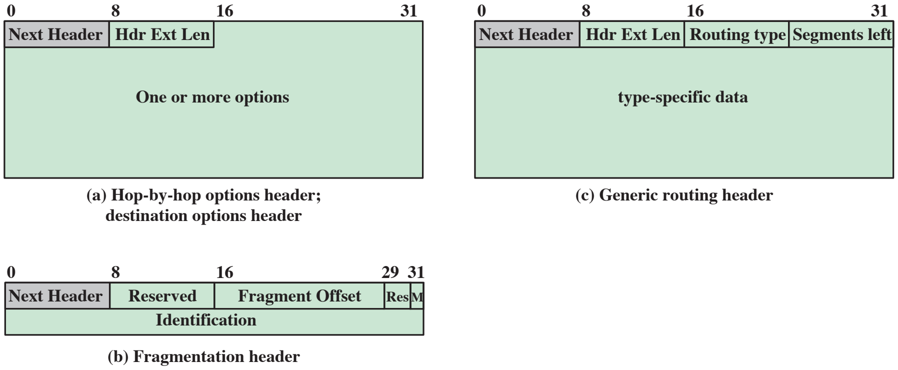


Table 14.3
IPv6 Address Space Usage

Address Type	Binary Prefix	IPv6 Notation	Fraction of address space
Embedded IPv4 address	00…1111 1111 1111 1111 (96 bits)	::FFFF/96	2^{-96}
Loopback	00…1 (128 bits)	::1/128	2^{-128}
Link-local unicast	1111 1110 10	FE80::/10	1/1024
Multicast	1111 1111	FF00::/8	2/256
Global unicast	Everything else		

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



0 8 16 31

Next Header | Hdr Ext Len

One or more options

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

0 8 16 31

Next Header | Hdr Ext Len | Routing type | Segments left

type-specific data

(c) Generic routing header

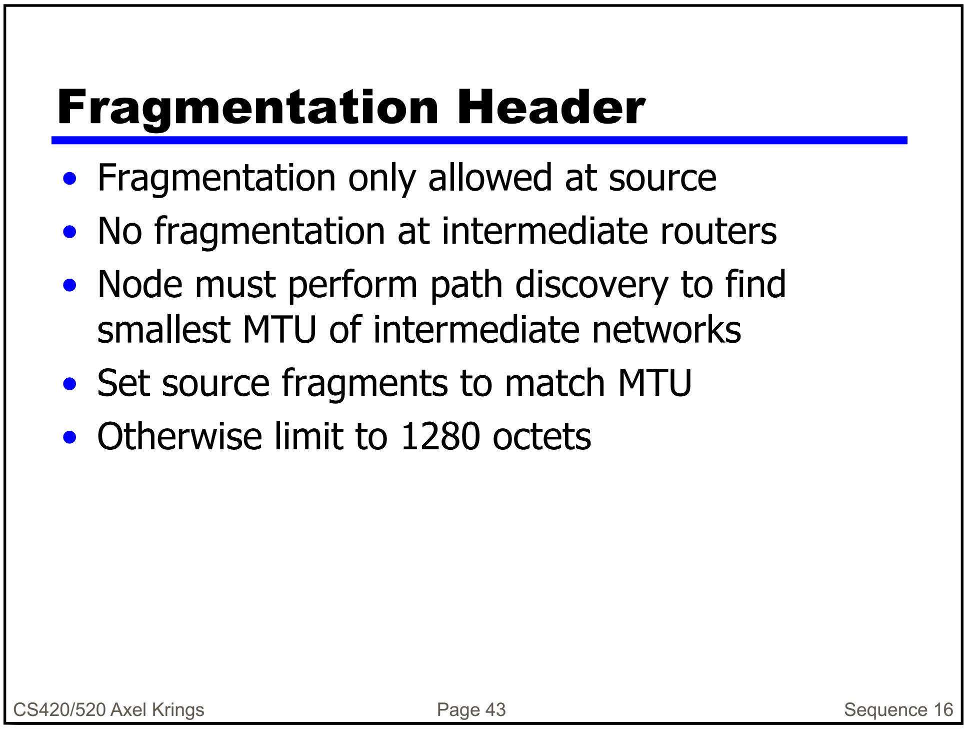
0 8 16 29 31

Next Header | Reserved | Fragment Offset | Res | M

Identification

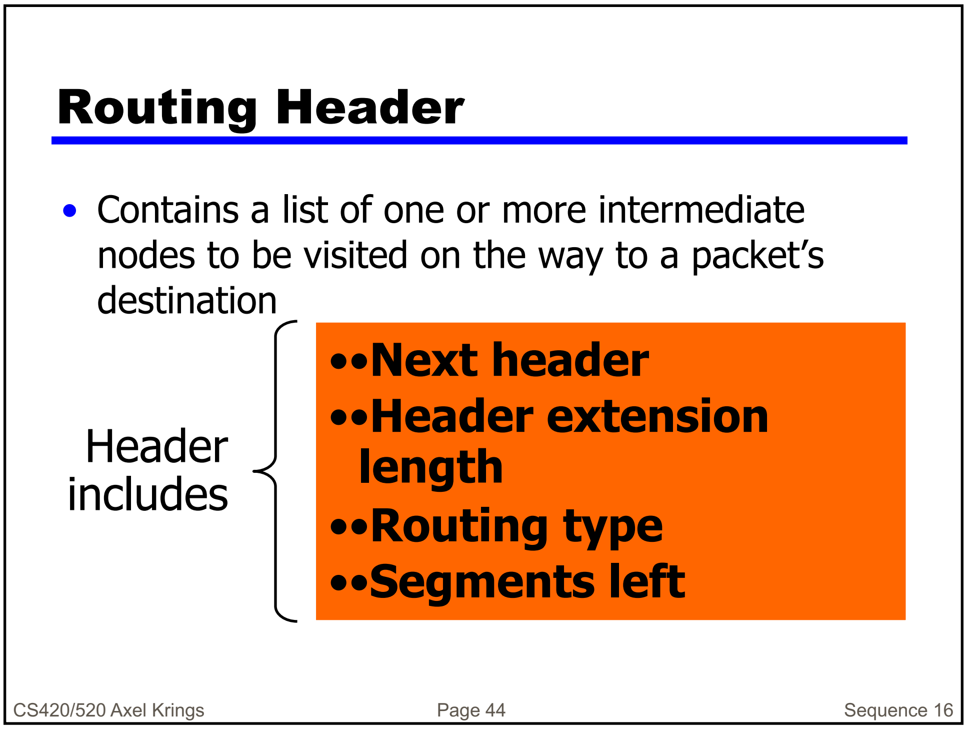
(b) Fragmentation header

Figure 14.10 IPv6 Extension Headers



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

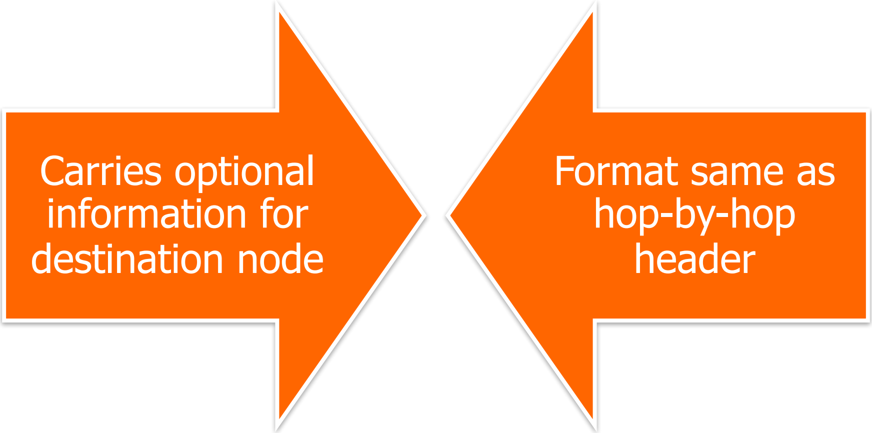
••Next header

••Header extension length

••Routing type

••Segments left

Destination Options Header



Carries optional information for destination node

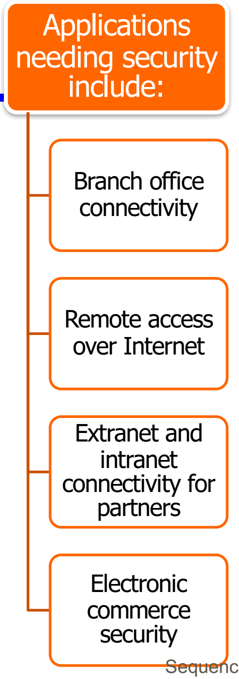
Format same as hop-by-hop header

Virtual Private Network (VPN)

- Set of computers interconnected using an unsecure network
  - e.g. linking corporate LANs over Internet
- Using encryption and special protocols to provide security
  - Eavesdropping
  - Entry point for unauthorized users
- Proprietary solutions are problematical
  - Development of IPSec standard

IPsec

- RFC 1636 (1994) identified security need
- Encryption and authentication necessary security features in IPv6
- Designed also for use with current IPv4



Applications needing security include:

- Branch office connectivity
- Remote access over Internet
- Extranet and intranet connectivity for partners
- Electronic commerce security

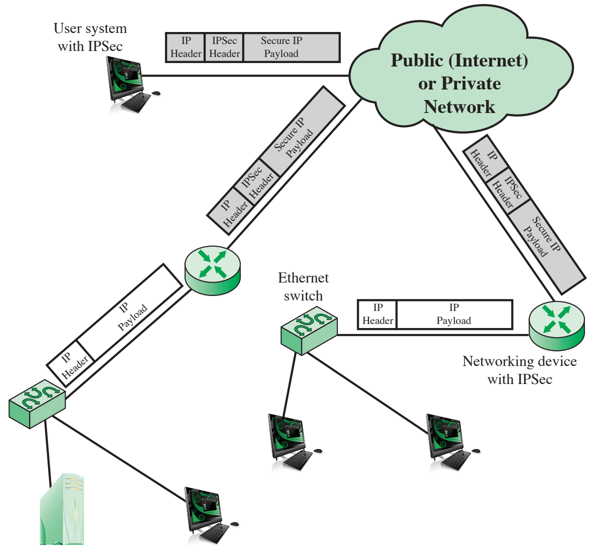
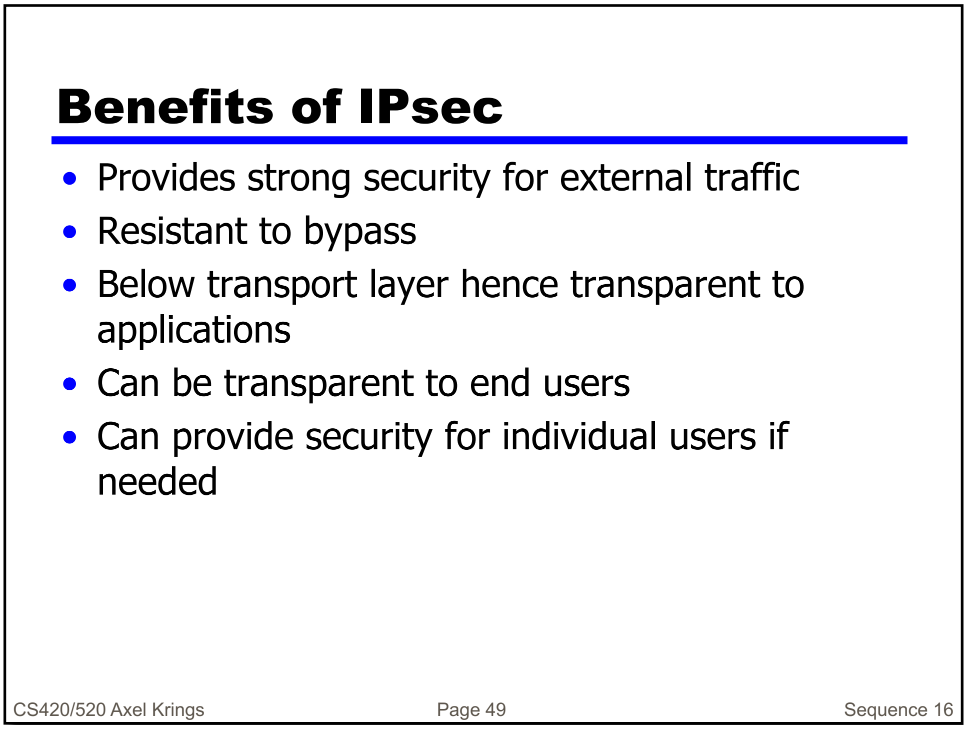
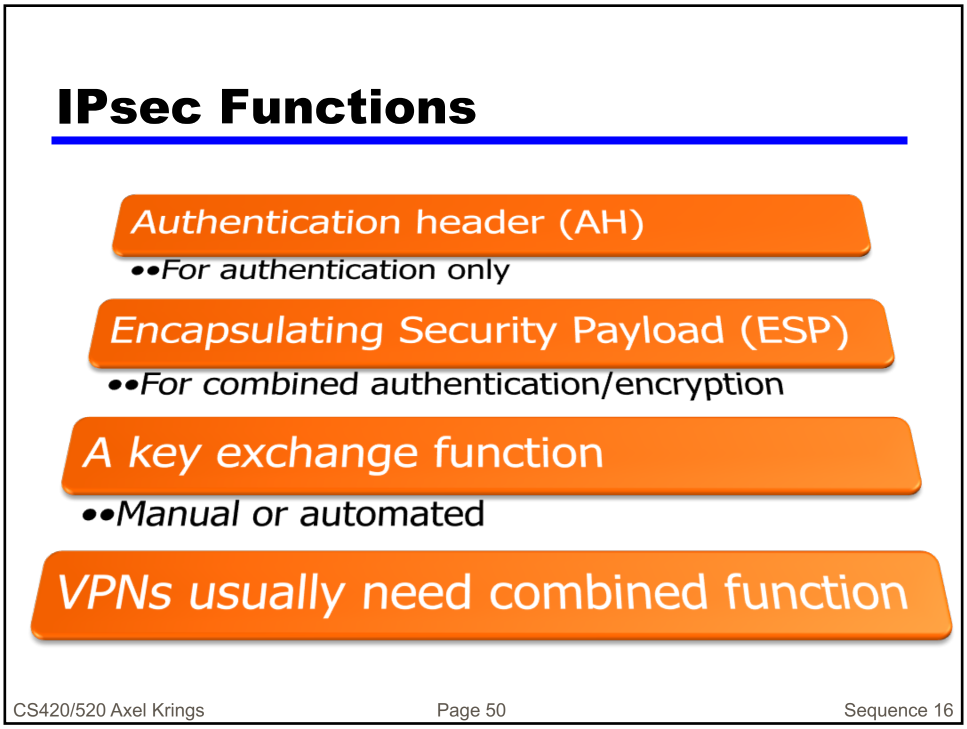


Figure 14.11 An IP Security Scenario



Benefits of IPsec

- Provides strong security for external traffic
- Resistant to bypass
- Below transport layer hence transparent to applications
- Can be transparent to end users
- Can provide security for individual users if needed



IPsec Functions

Authentication header (AH)

•• *For authentication only*

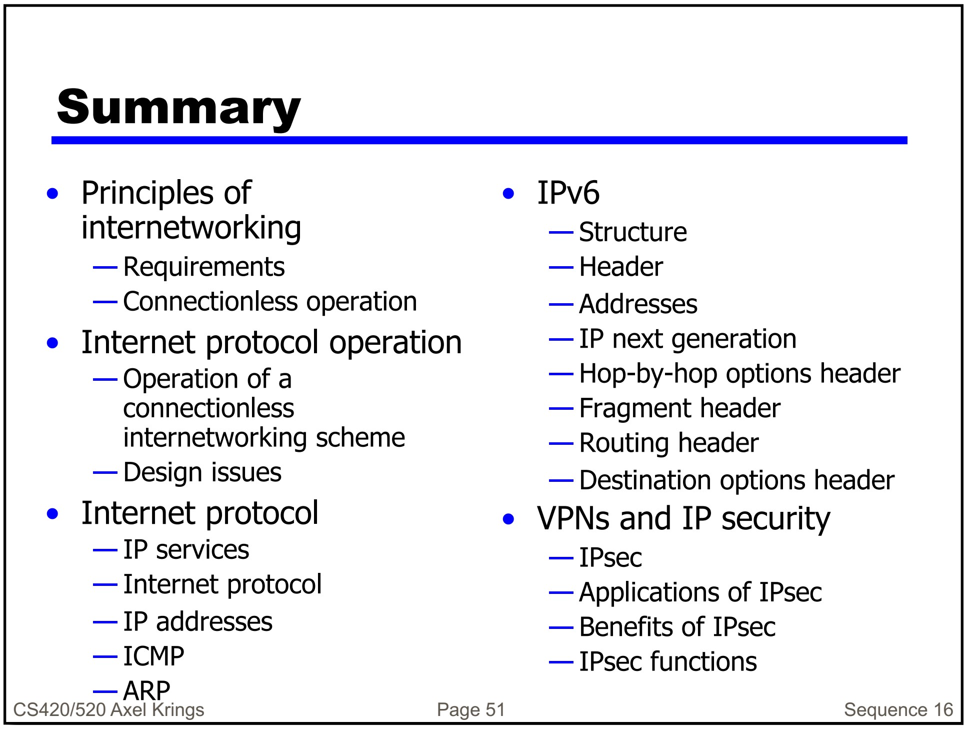
Encapsulating Security Payload (ESP)

•• *For combined authentication/encryption*

A key exchange function

•• *Manual or automated*

VPNs usually need combined function



Summary

- Principles of internetworking
  - Requirements
  - Connectionless operation
- Internet protocol operation
  - Operation of a connectionless internetworking scheme
  - Design issues
- Internet protocol
  - IP services
  - Internet protocol
  - IP addresses
  - ICMP
  - ARP
- IPv6
  - Structure
  - Header
  - Addresses
  - IP next generation
  - Hop-by-hop options header
  - Fragment header
  - Routing header
  - Destination options header
- VPNs and IP security
  - IPsec
  - Applications of IPsec
  - Benefits of IPsec
  - IPsec functions