Data and Computer Communications

CHAPTER 14

The Internet Protocol

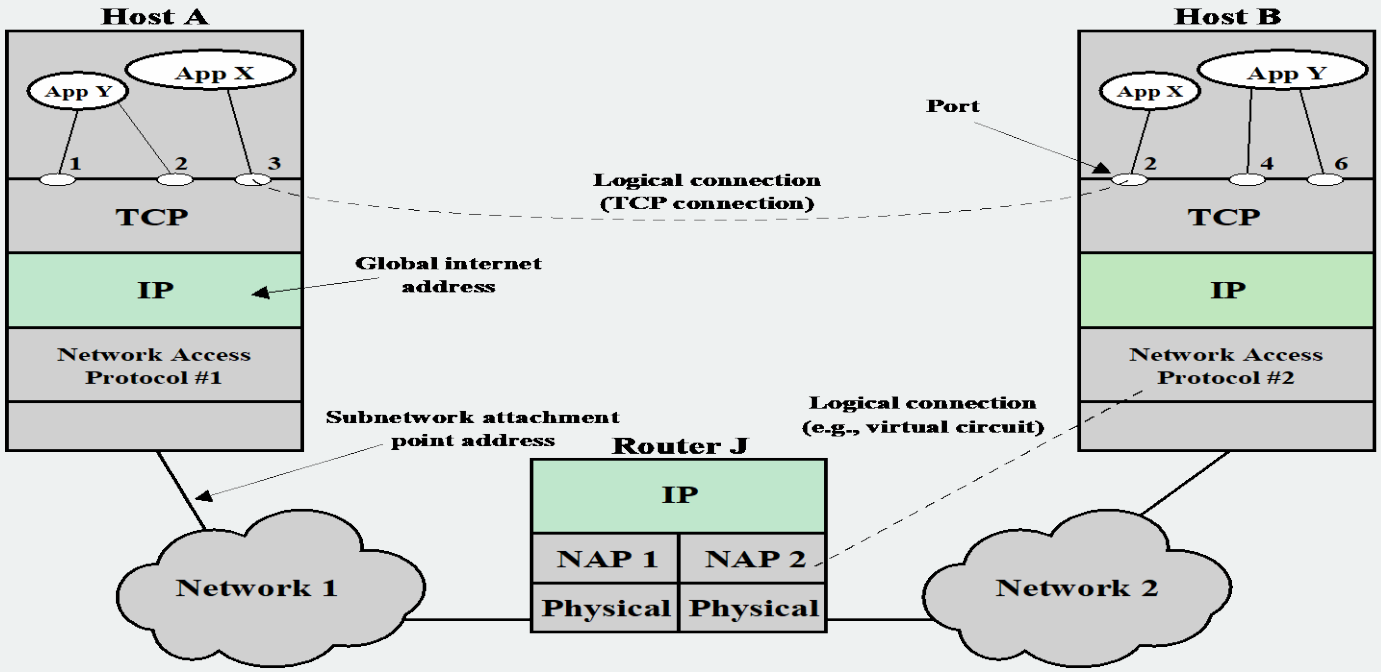


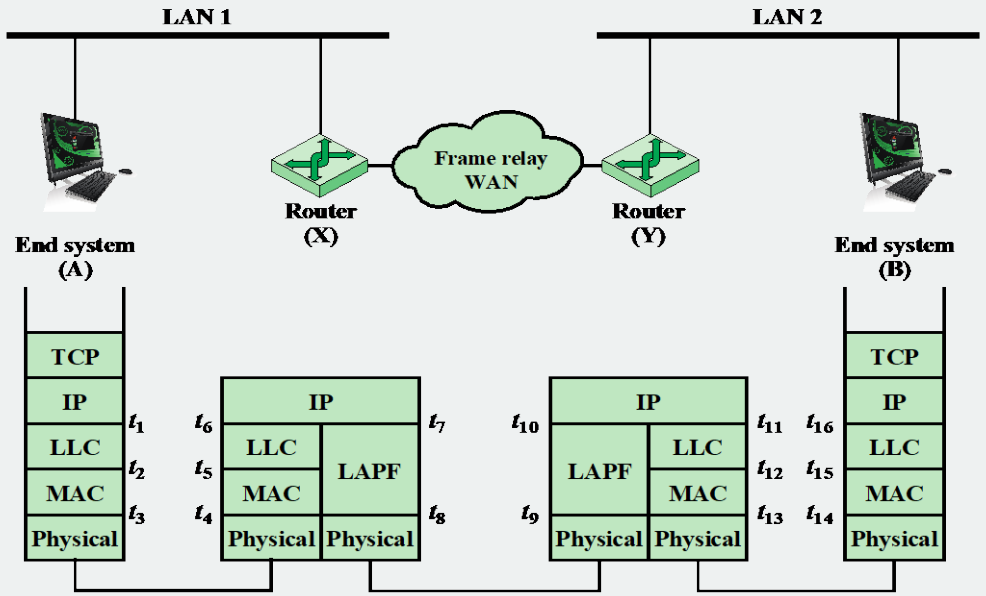
Figure 14.1 TCP/IP Concepts

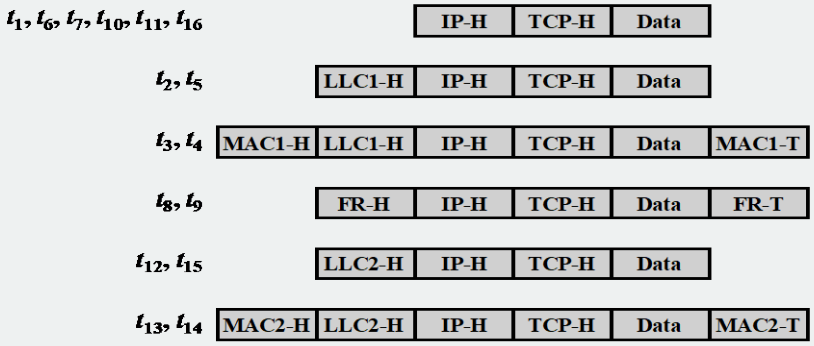
Connectionless Operation

- 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





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

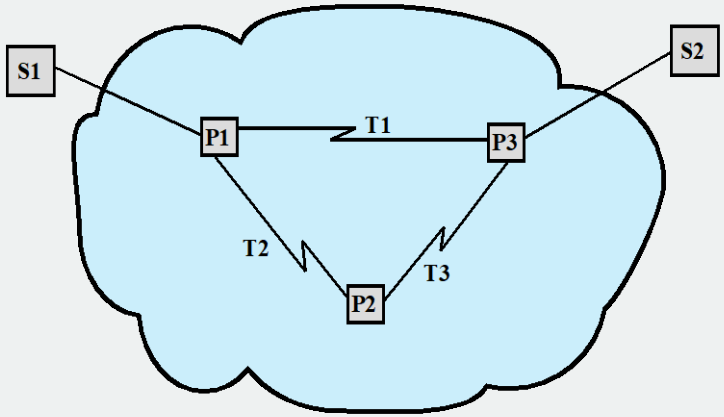
Figure 14.2 Example of Internet Protocol Operation

Connectionless Internetworking

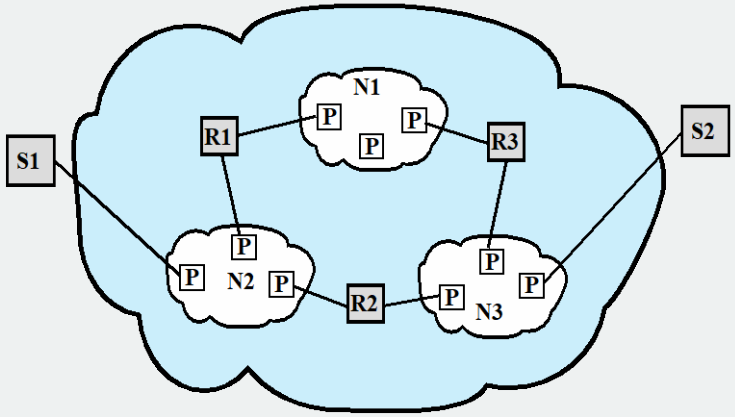
- Connectionless internet facility is flexible
- IP provides a connectionless service between end systems
  - Advantages:
    - Is flexible
    - Can be made robust
    - Does not impose unnecessary overhead

IP Design Issues

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



(a) Packet-switching network architecture



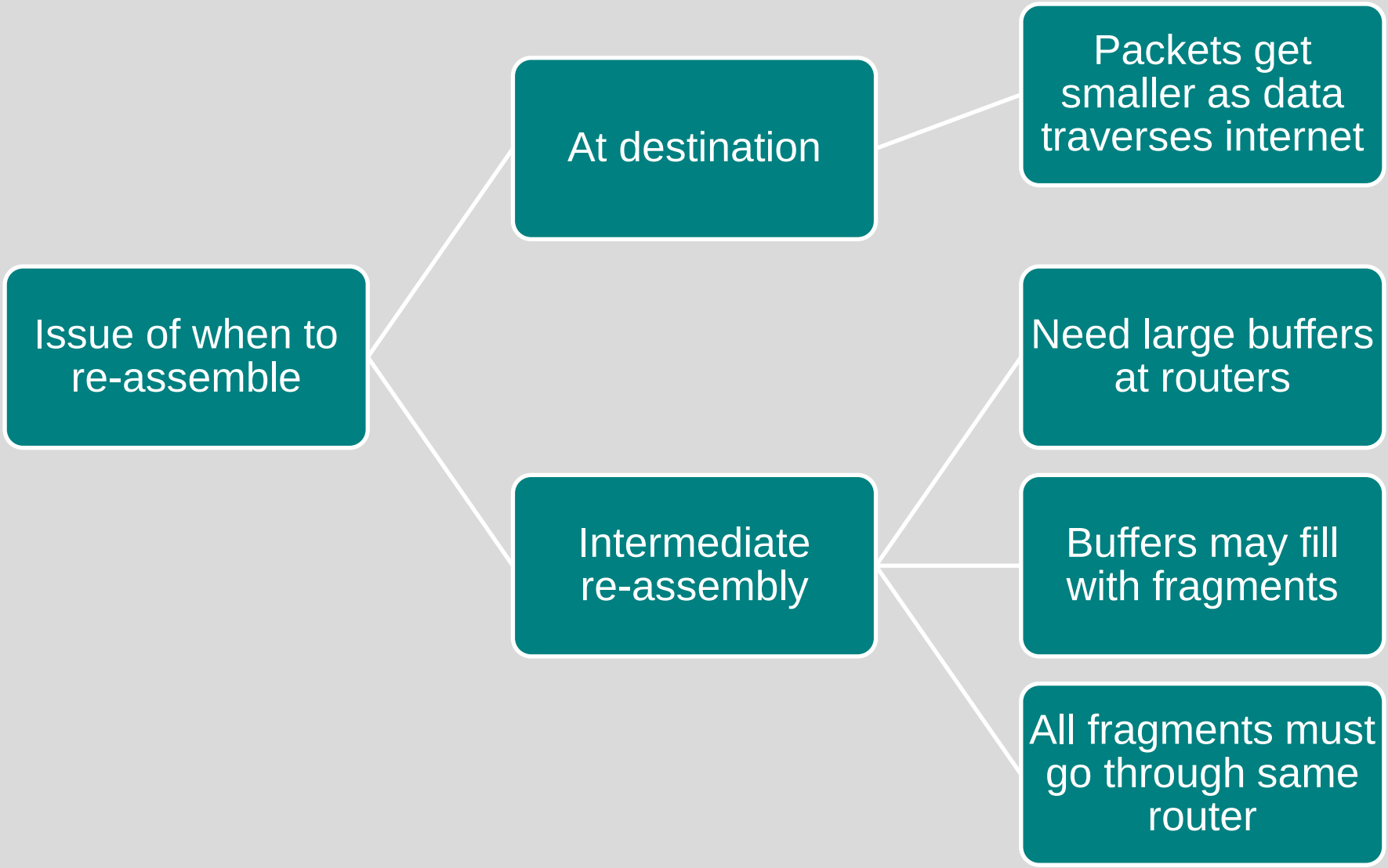
(b) Internetwork architecture

Figure 14.3 The Internet as a Network

Fragmentation and Re-assembly

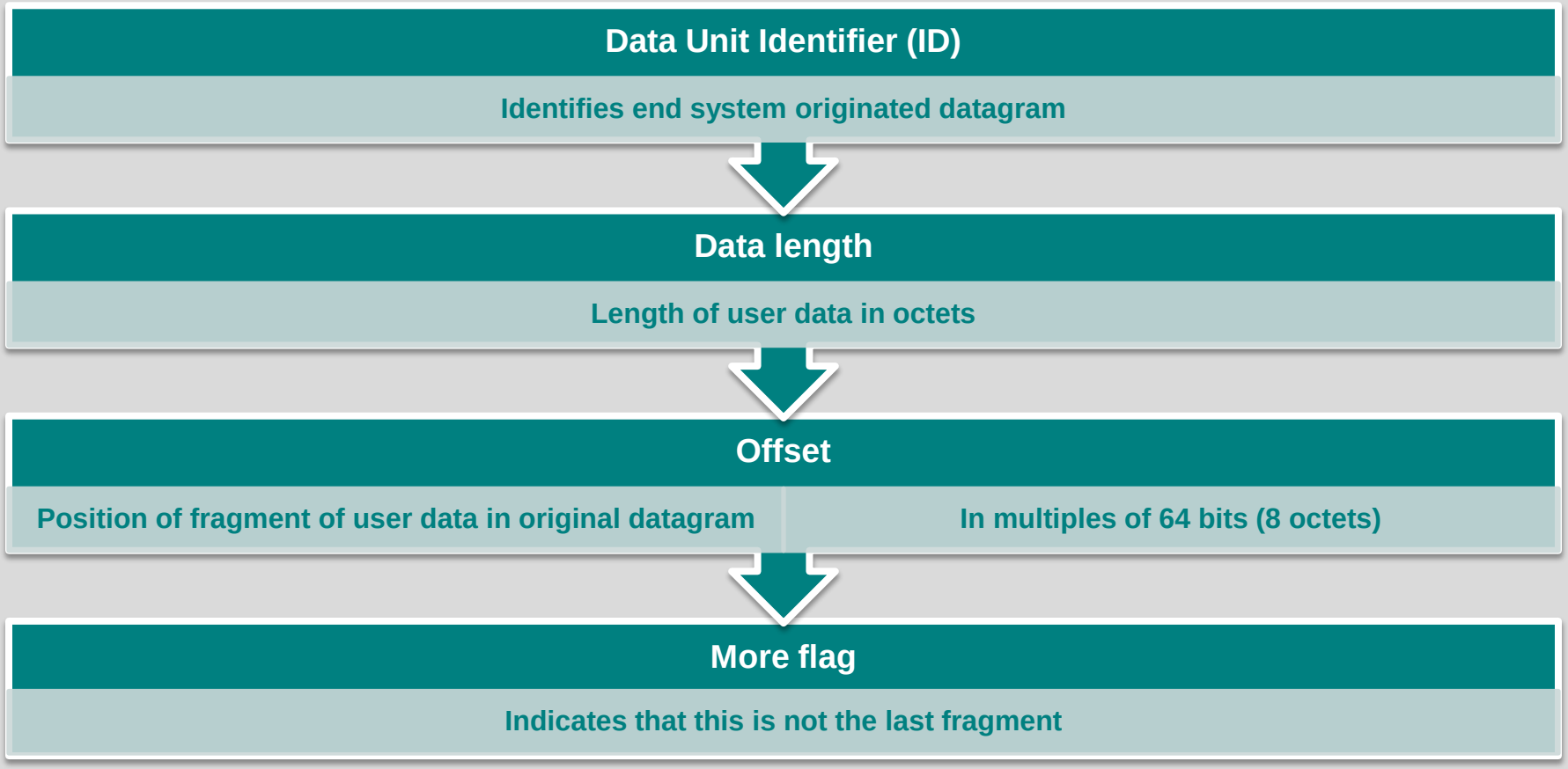
- Protocol exchanges data between two entities
- Lower-level protocols may need to break data up into smaller blocks, called fragmentation
- Reasons for fragmentation:
  - Network only accepts blocks of a certain size
  - More efficient error control and smaller retransmission units
  - Fairer access to shared facilities
  - Smaller buffers
- Disadvantages:
  - Smaller buffers
  - More interrupts and processing time

Fragmentation and Re-assembly



IP Fragmentation

- IP re-assembles at destination only
- Uses fields in header



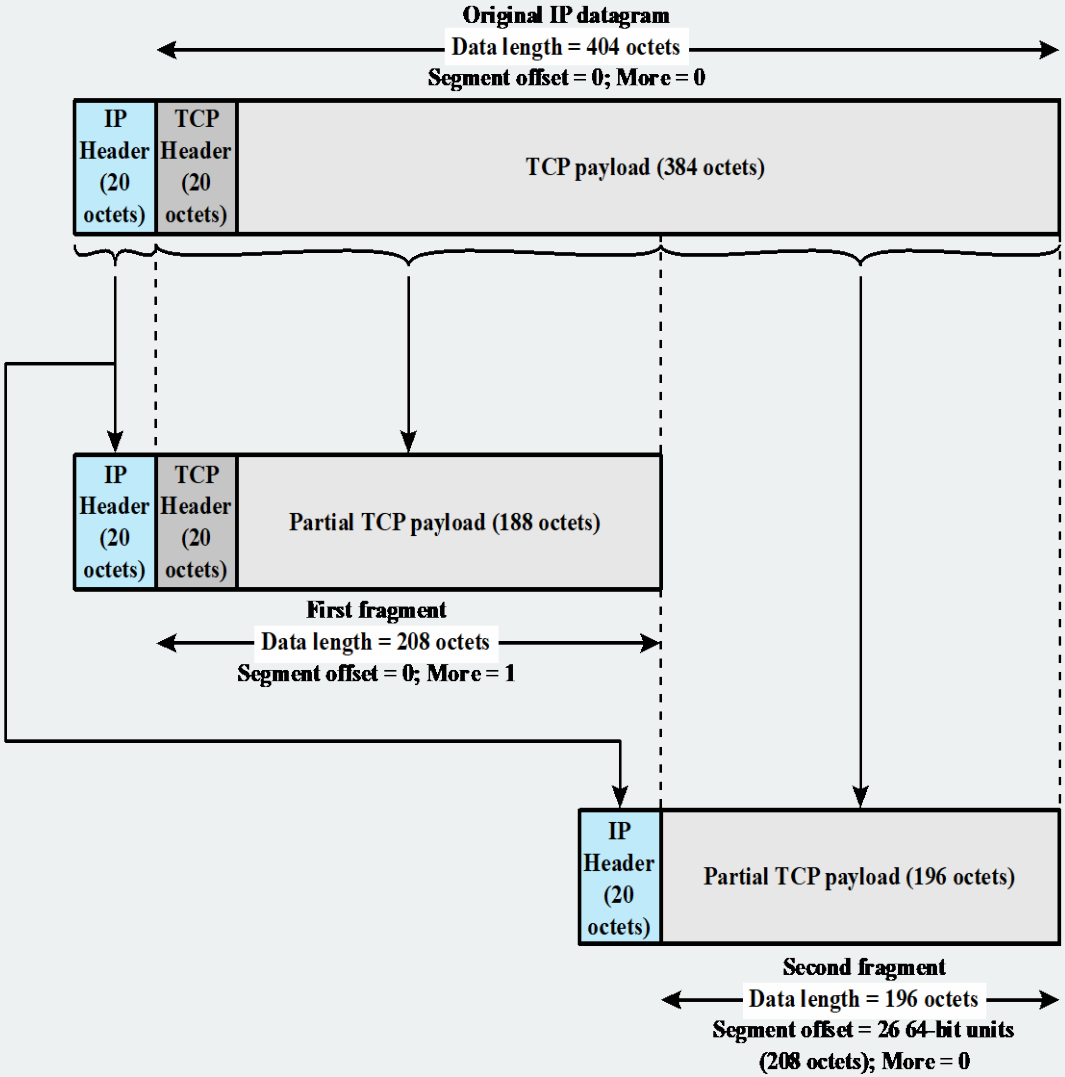


Figure 14.4 Fragmentation Example

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 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

Time stamping

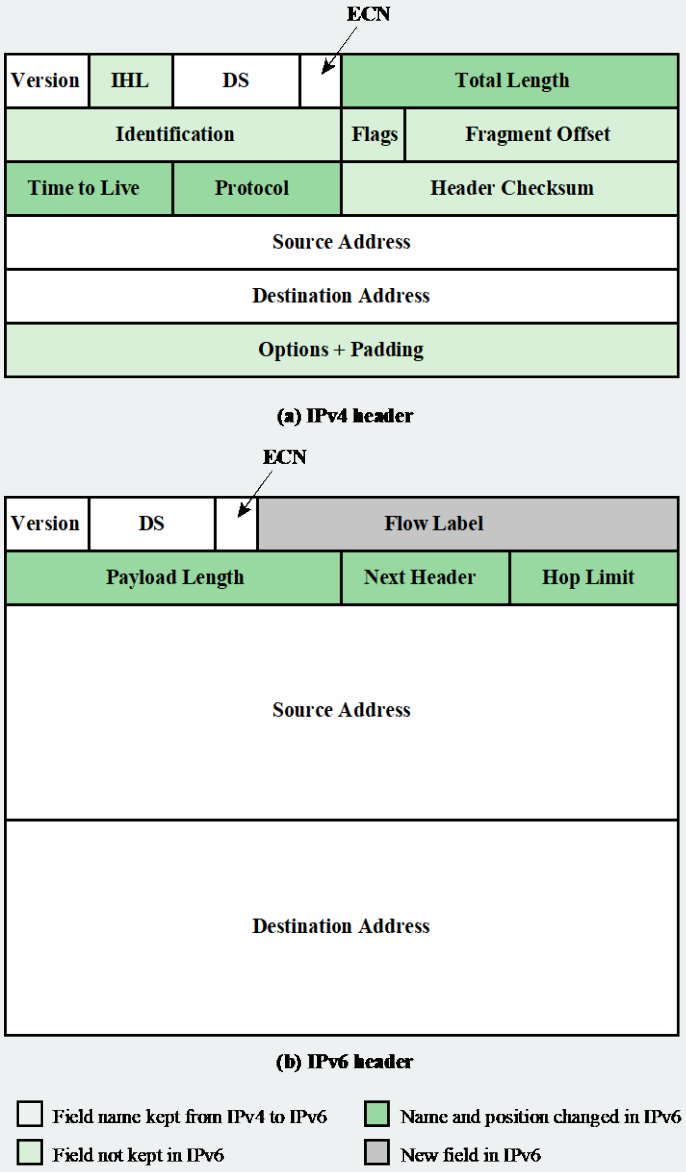


Figure 14.5 IPv4 and IPv6 Headers

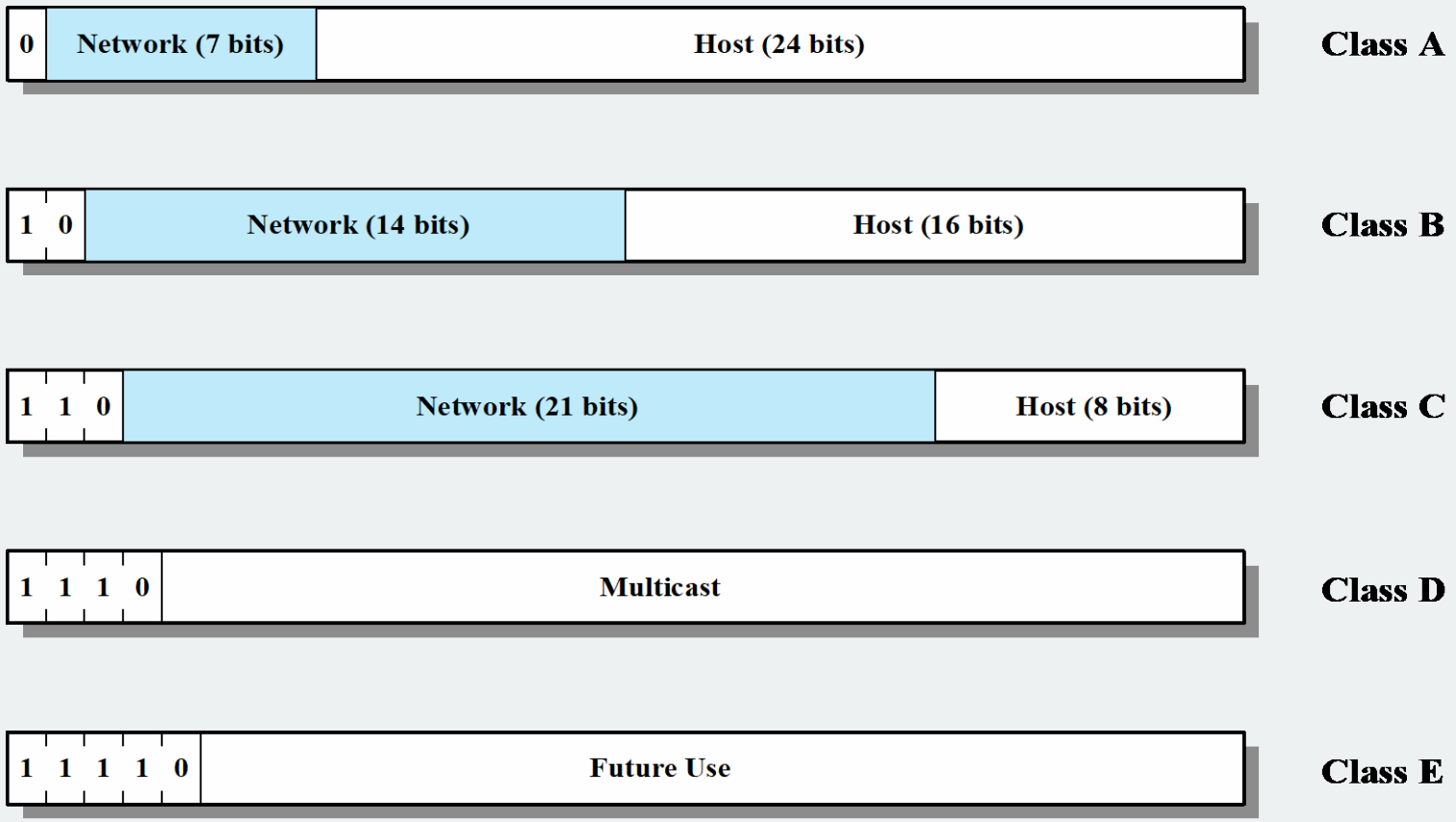


Figure 14.6 IPv4 Address Formats

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	00000000.00000000.000 00000.00011001	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

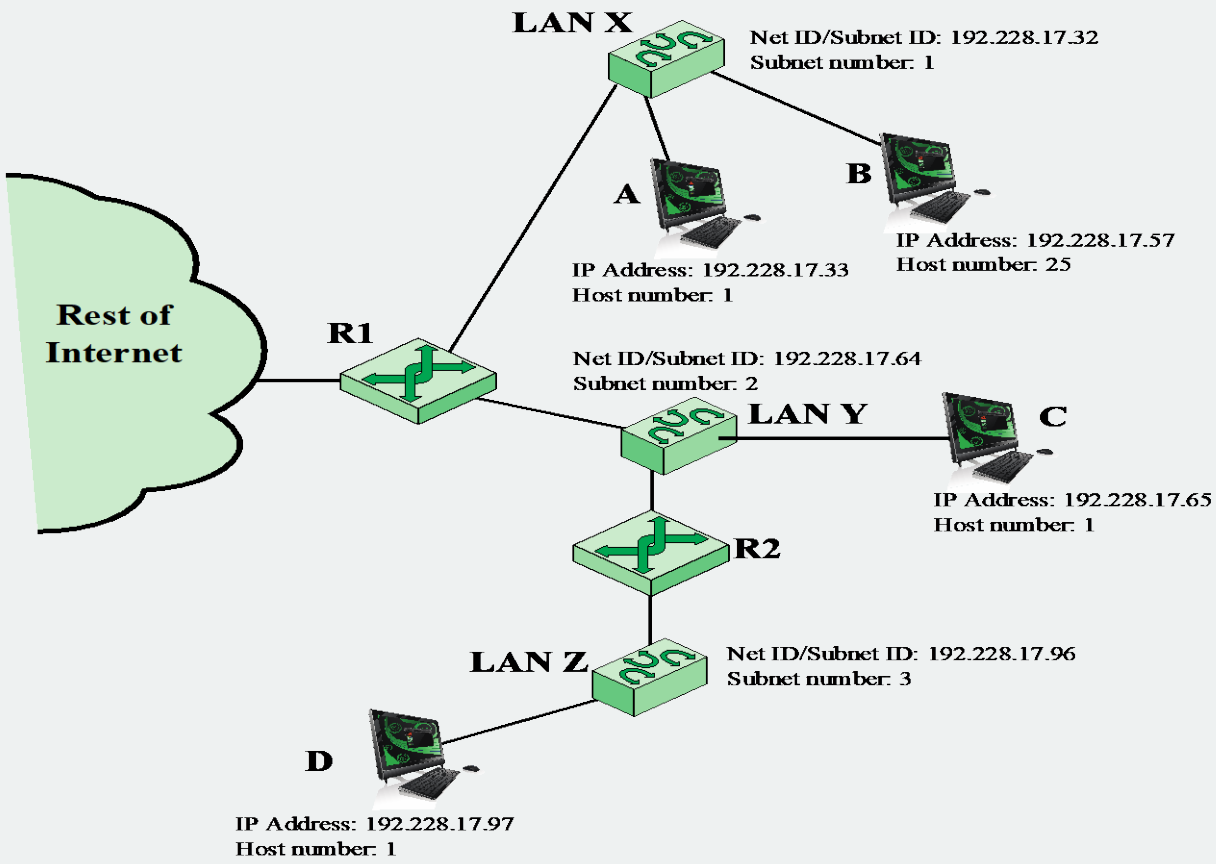


Figure 14.7 Example of Subnetworking

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

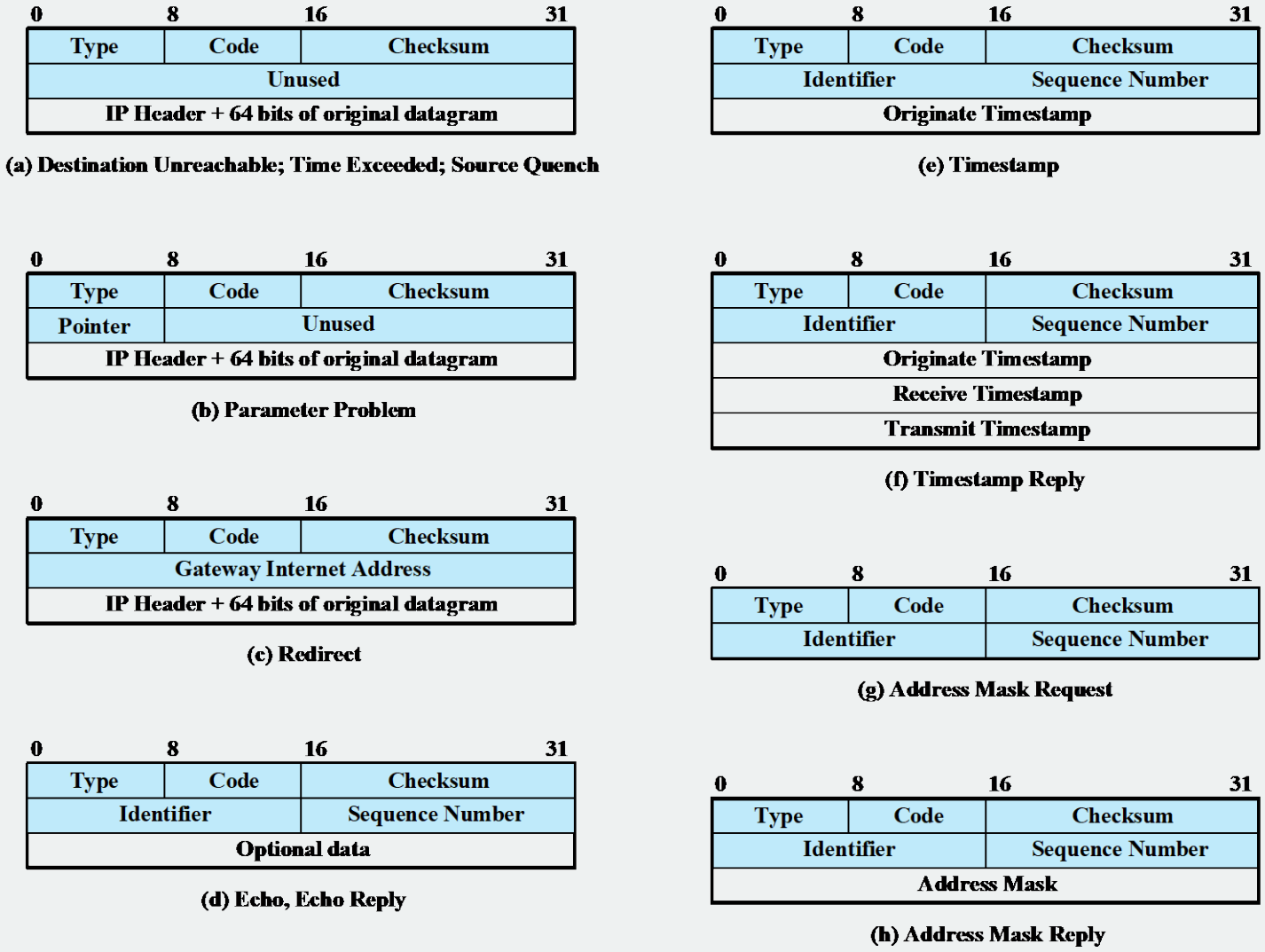


Figure 14.8 ICMP Message Formats

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

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

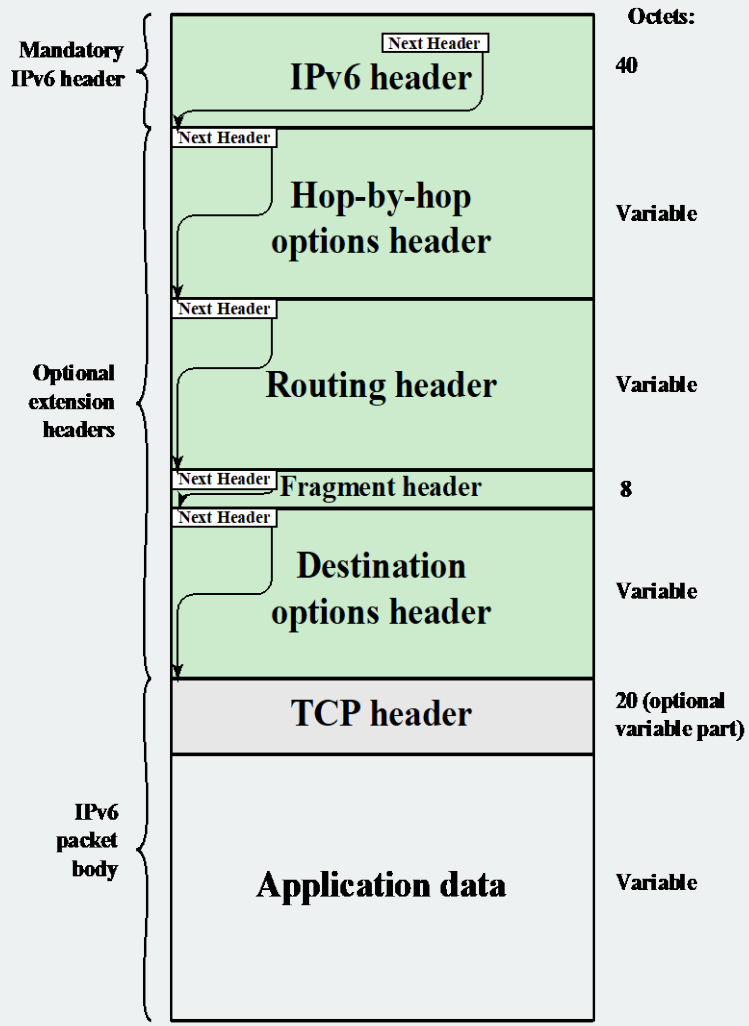


Figure 14.9 IPv6 Packet with Extension Headers (containing a TCP Segment)

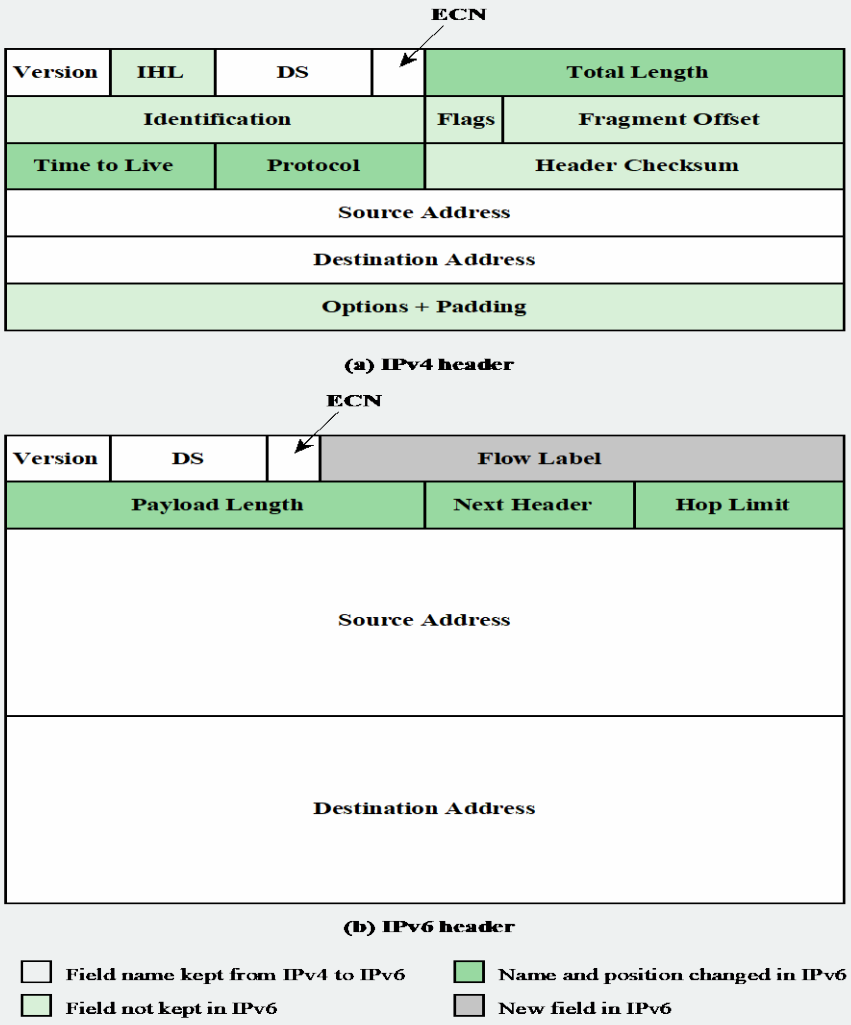


Figure 14.5 IPv4 and IPv6 Headers

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

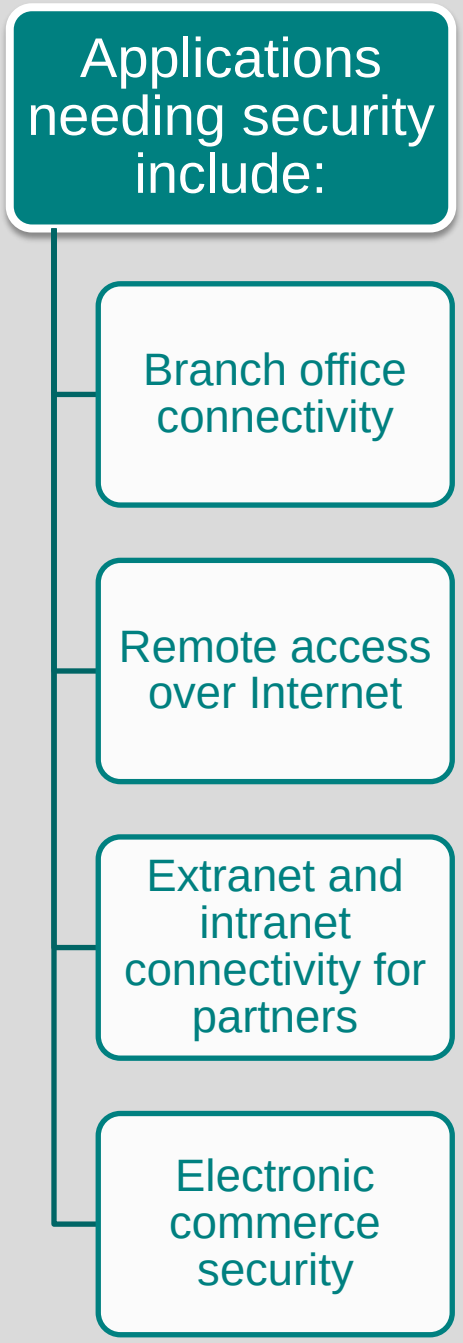
Address Type	Binary Prefix	IPv6 Notation	Fraction of address space
Embedded IPv4 address	00…1111 1111 1111 1111 (96 bits)	::FFFF/96	2^{-96}
Loopback	00…1 (128 bits)	::1/128	2^{-128}
Link-local unicast	1111 1110 10	FE80::/10	1/1024
Multicast	1111 1111	FF00::/8	2/256
Global unicast	Everything else		

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



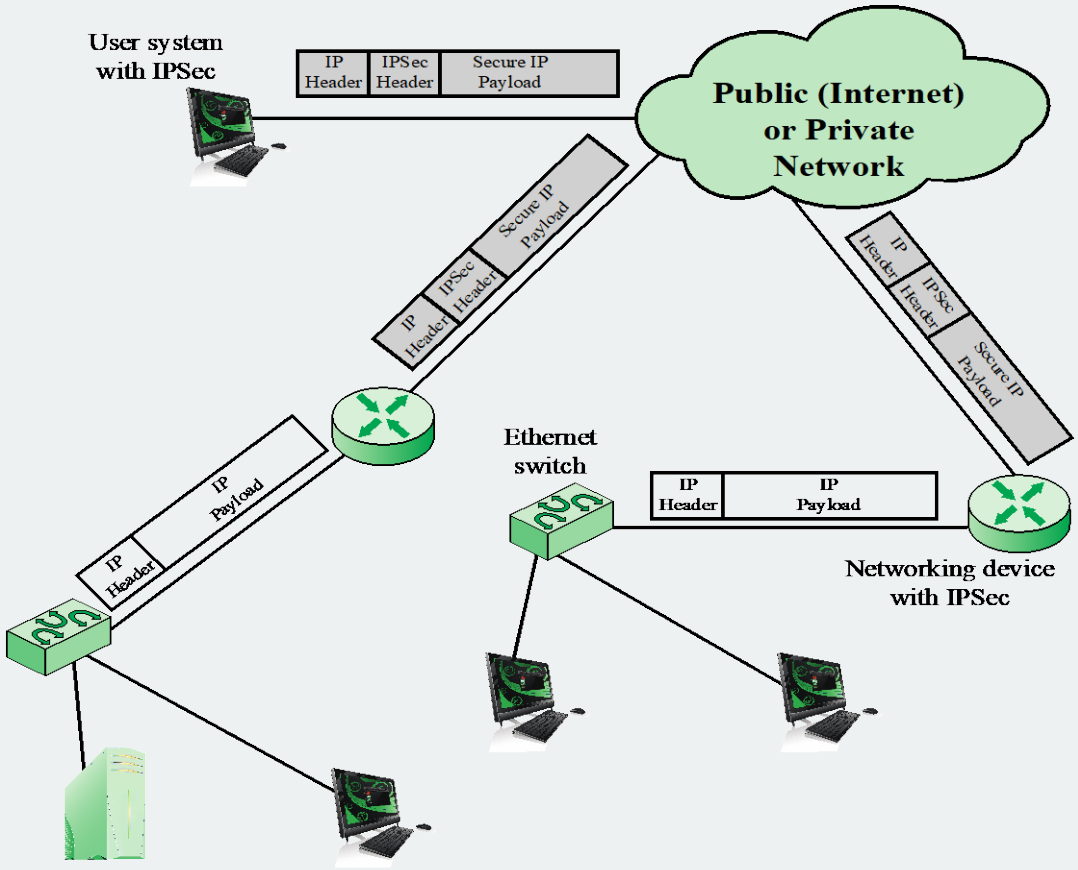


Figure 14.11 An IP Security Scenario

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