ET4254 – Communications and Networking 1

Topic 9 Internet Protocols

Aims:-

- *basic protocol functions*
- internetworking principles
- connectionless internetworking
- IP
- IPv6
- IPSec

Protocol Functions

- have a small set of functions that form basis of all protocols
  - encapsulation
  - fragmentation and reassembly
  - connection control
  - ordered delivery
  - flow control
  - error control
  - addressing
  - multiplexing
  - transmission services

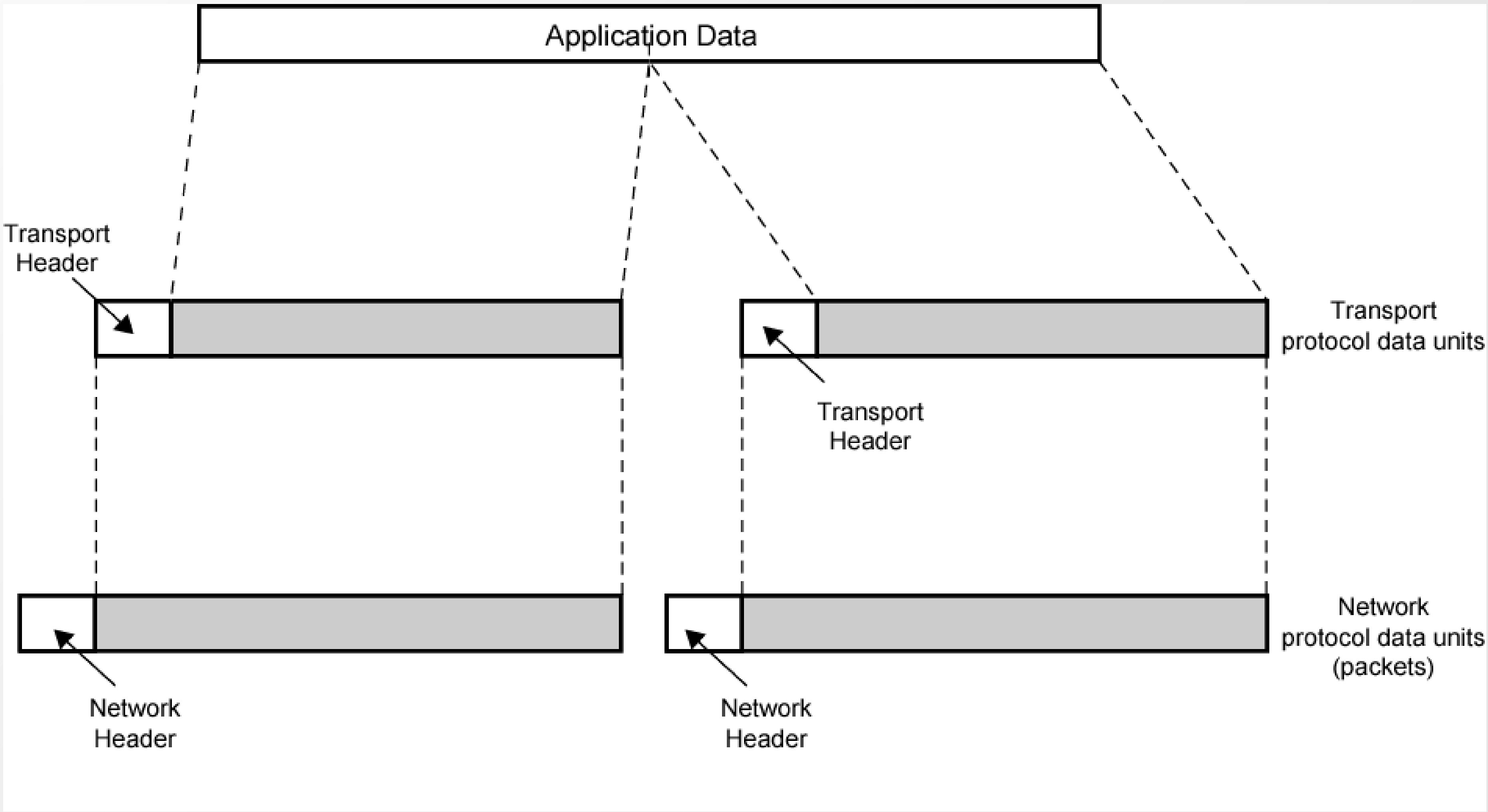
Encapsulation

- data usually transferred in blocks
- called Protocol Data Units (PDUs)
- have three categories of control
  - address
  - error-detecting code
  - protocol control
- encapsulation is addition of control information to data
- have many examples of PDU’s in previous chapters
  - e.g. TFTP, HDLC, frame relay, ATM, AAL5, LLC, IEEE 802.3, IEEE 802.11

Fragmentation and Reassembly

- protocol exchanges data between two entities
- lower-level protocols may need to break data up into smaller blocks, called fragmentation
- for various reasons
  - 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

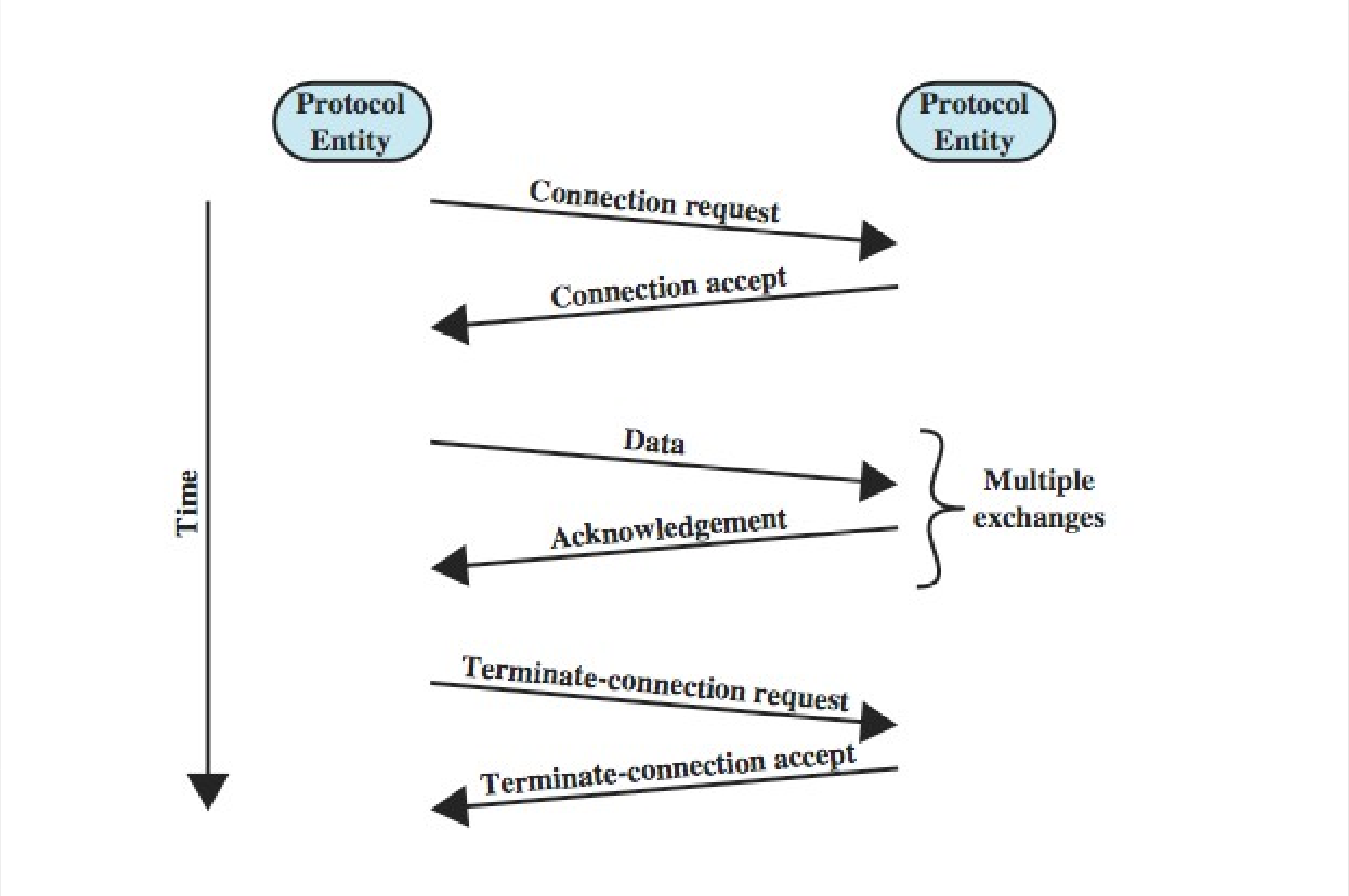
PDUS and Fragmentation



Connection Control

- have connectionless data transfer
  - where each PDU treated independently
- and connection-oriented data transfer
  - involves a logical association, or connection, established between entities
  - preferred (even required) for lengthy data exchange
  - or if protocol details are worked out dynamically
- three phases occur for connection-oriented
  - connection establishment
  - data transfer
  - connection termination

Phases of Connection Oriented Transfer



Connection Establishment

- entities agree to exchange data
- typically, one station issues connection request
- may involve central authority
- receiving entity accepts or rejects (simple)
- may include negotiation
- syntax, semantics, and timing
- both entities must use same protocol
- may allow optional features
- must be agreed

Data Transfer and Termination

- both data and control information exchanged
- data flow and acknowledgements may be in one or both directions
- one side may send termination request
- or central authority might terminate

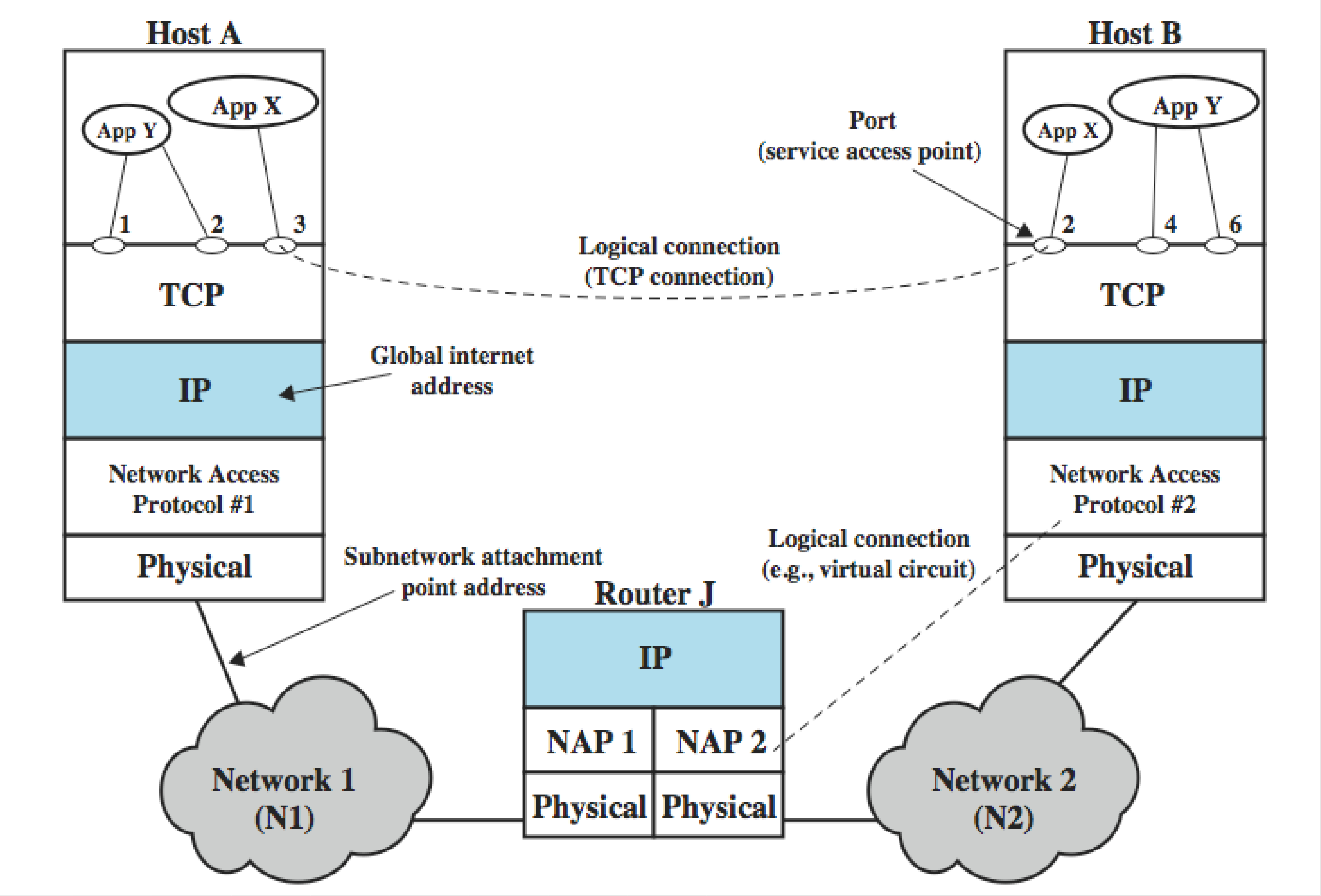
Sequencing

- used by many, but not all, connection-oriented protocols
  - e.g. HDLC, IEEE 802.11
- connection-oriented protocols include some way of identifying connection
- have PDUs numbered sequentially
- each side tracks seq numbers in and out
- to support three main functions
  - ordered delivery
  - llow control
  - error control

Ordered Delivery

- risk PDUs may arrive out of order
- require PDU order must be maintained
- hence number PDUs sequentially
- easy to reorder received PDUs
- use finite sequence number field
  - numbers repeat modulo maximum number
  - max sequence number greater than max number of PDUs that could be outstanding

TCP/IP Concepts



Flow Control

- receiving entity limits amount / rate of data sent
- simplest protocol is stop-and-wait
- more efficient protocols use concept of credit
  - amount of data sent without acknowledgment
- must be implemented in several protocols
  - network traffic control
  - buffer space
  - application overflow

Error Control

- to guard against loss or damage
- implemented as separate error detection and retransmission functions
  - sender inserts error-detecting code in PDU
  - receiver checks code on incoming PDU
  - if error, discard
  - if transmitter doesn’t get acknowledgment in reasonable time, retransmit
- can use an error-correction code
  - enables receiver to detect and possibly correct errors
- performed at various protocol layers

Addressing

- addressing level
- addressing scope
- connection identifiers
- addressing mode

Addressing Level

- level in architecture where entity is named
- have a unique address for each intermediate and end system
- usually a network-level address to route PDU
  - e.g. IP address or internet address
  - e.g. OSI - network service access point (NSAP)
- at destination data must routed to some process
  - e.g. TCP/IP port
  - e.g. OSI service access point (SAP)

Addressing Scope

- global address which identifies unique system
  - unambiguous
  - synonyms permitted
  - system may have more than one global address
  - global applicability
  - enables internet to route data between any two systems
- need unique address for each interface on network
  - MAC address on IEEE 802 network and ATM host address
  - enables network to route data units through network
- only relevant for network-level addresses
- port or SAP above network level is unique within system

Connection Identifiers

- is used by both entities for future transmissions
- advantages:
  - reduced overhead since smaller
  - routing using a fixed route tagged by connection ID
  - multiplexing of multiple connections
  - use of state information

Addressing Mode

- address usually refers to single system
  - individual or unicast address
- can refer to more than one system for
  - multiple simultaneous recipients for data
  - broadcast for all entities within domain
  - multicast for specific subset of entities

Multiplexing

- multiple connections into single system
  - e.g. frame relay, can have multiple data link connections terminating in single end system
  - e.g. multiple TCP connections to given system
- upward multiplexing
  - have multiple higher level connections over a single lower level connection
- downward multiplexing
  - have single higher level connection built on multiple lower level connections

Transmission Services

- may have additional services to entities:
  - priority on connection basis or message basis
  - quality of service
    - *e.g. minimum throughput or maximum delay threshold*
  - security mechanisms, restricting access
- these depend on underlying transmission system and lower-level entities

Internetworking Terms

- communications Network
- internet
- the Internet
- intranet
- End System (ES)
- Intermediate System (IS)
- bridge
- router

Requirements of Internetworking

- link between networks
- routing and delivery of data between processes on different networks
- accounting services and status info
- independent of network architectures

Network Architecture Features

- addressing
- packet size
- access mechanism
- timeouts
- error recovery
- status reporting
- routing
- user access control
- connection based or connectionless

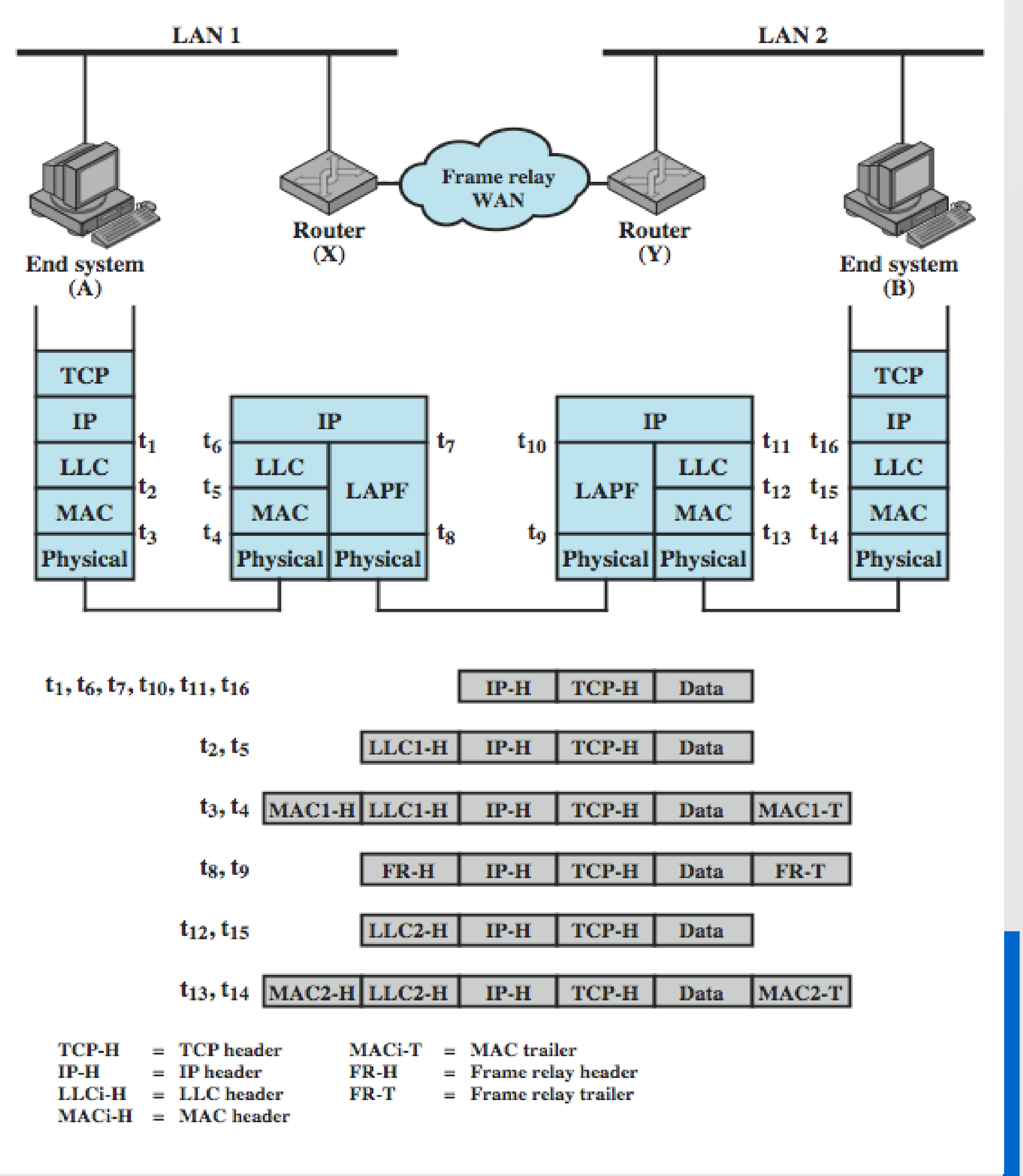
Architectural Approaches

- connection oriented
  - virtual circuit
- connectionless
  - datagram
  - PDU’s routed independently from source ES to dest ES through routers and networks
  - share common network layer protocol, e.g. IP
  - below have network access on each node

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)

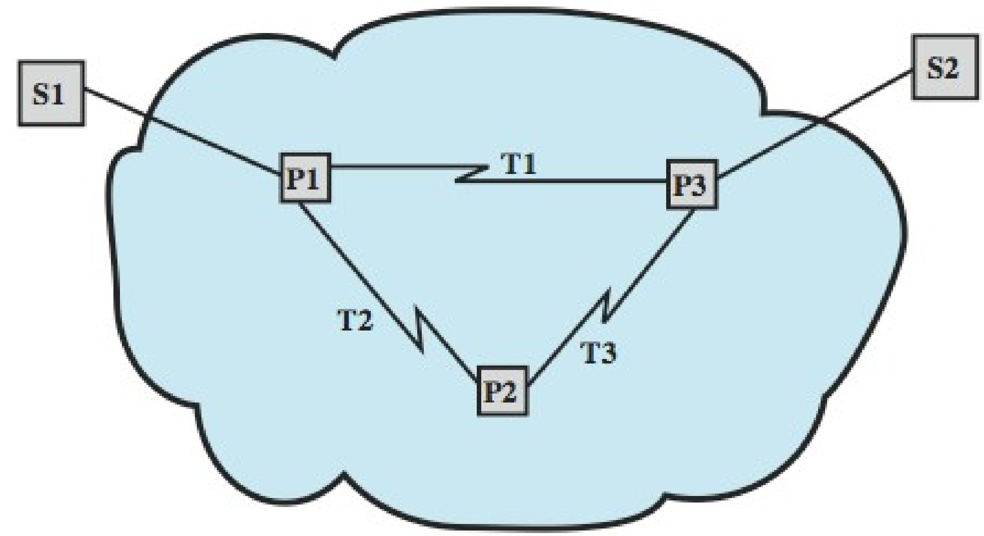
IP Operation



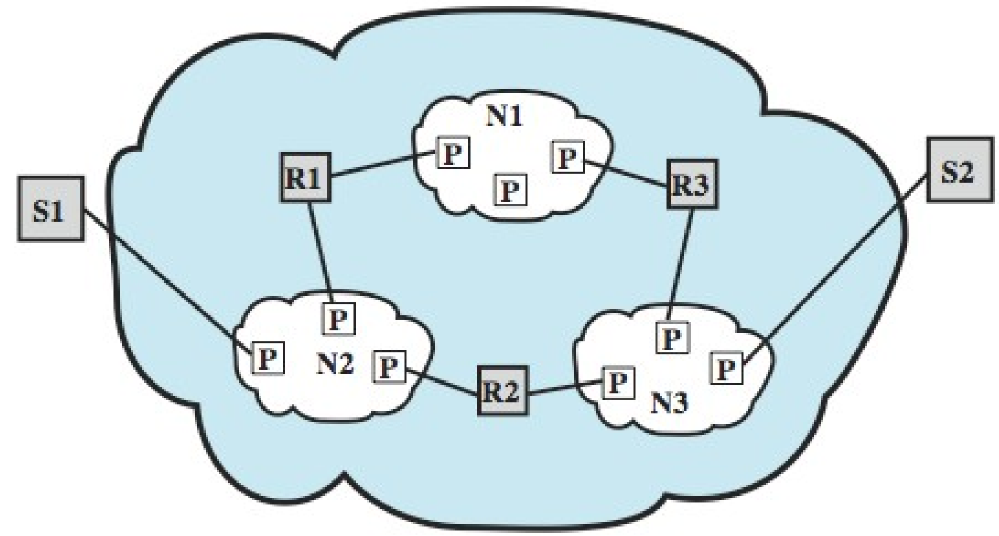
Design Issues

- routing
- datagram lifetime
- fragmentation and re-assembly
- error control
- flow control

The Internet as a Network



(a) Packet-switching network architecture



(b) Internetwork architecture

Routing

- ES / routers maintain routing tables
  - indicate next router to which datagram is sent
  - static
  - dynamic
- source routing
  - source specifies route to be followed
  - can be useful for security & priority
- route recording

Datagram Lifetime

- datagrams could loop indefinitely
  - consumes resources
  - transport protocol may need upper bound on lifetime of a datagram
- can mark datagram with lifetime
  - Time To Live field in IP
  - when lifetime expires, datagram discarded
  - simplest is hop count
  - or time count

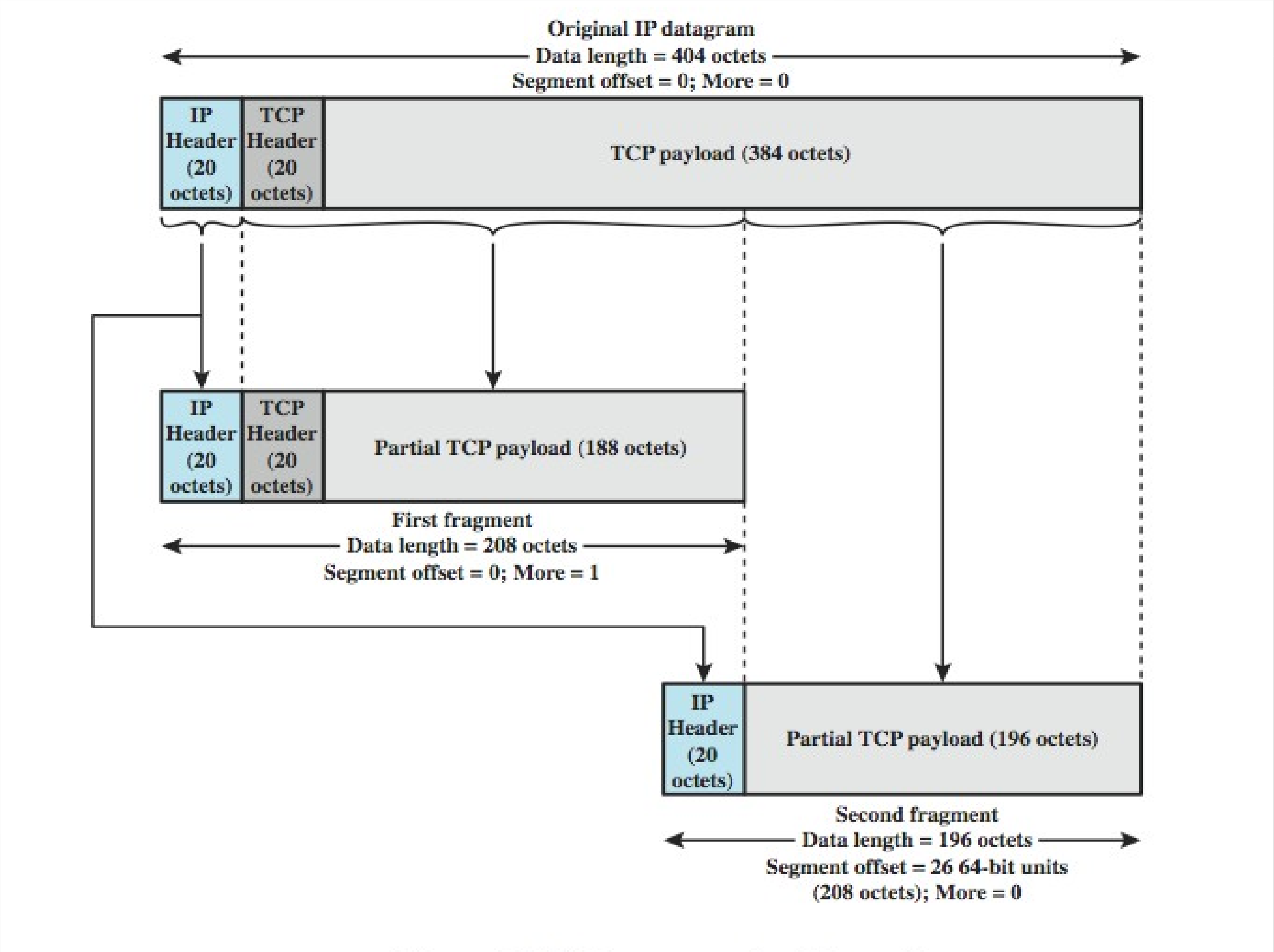
Fragmentation and Re-assembly

- may have different packet sizes
  - on networks along path used by datagram
- issue of when to re-assemble
  - at destination
    - *packets get smaller as data traverses internet*
  - intermediate re-assembly
    - *need large buffers at routers*
    - *buffers may fill with fragments*
    - *all fragments must go through same router*

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



Dealing with Failure

- re-assembly may fail if some fragments get lost
- need to detect failure
- re-assembly time out
  - assigned to first fragment to arrive
  - if timeout expires before all fragments arrive, discard partial data
- use packet lifetime (time to live in IP)
  - if time to live runs out, kill partial data

Error Control

- no guaranteed delivery
- router should attempt to inform source if packet discarded
- source may modify transmission strategy
- may inform high layer protocol
- need datagram identification
- see ICMP in next section

Flow Control

- allows routers and/or stations to limit rate of incoming data
- limited in connectionless systems
- send flow control packets to request reduced flow
- see ICMP in next section

Internet Protocol (IP) v4

- IP version 4
- defined in RFC 791
- part of TCP/IP suite
- two parts
  - specification of interface with a higher layer
    - *e.g. TCP*
  - specification of actual protocol format and mechanisms
- will (eventually) be replaced by IPv6

IP Services

- Primitives
  - 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 info

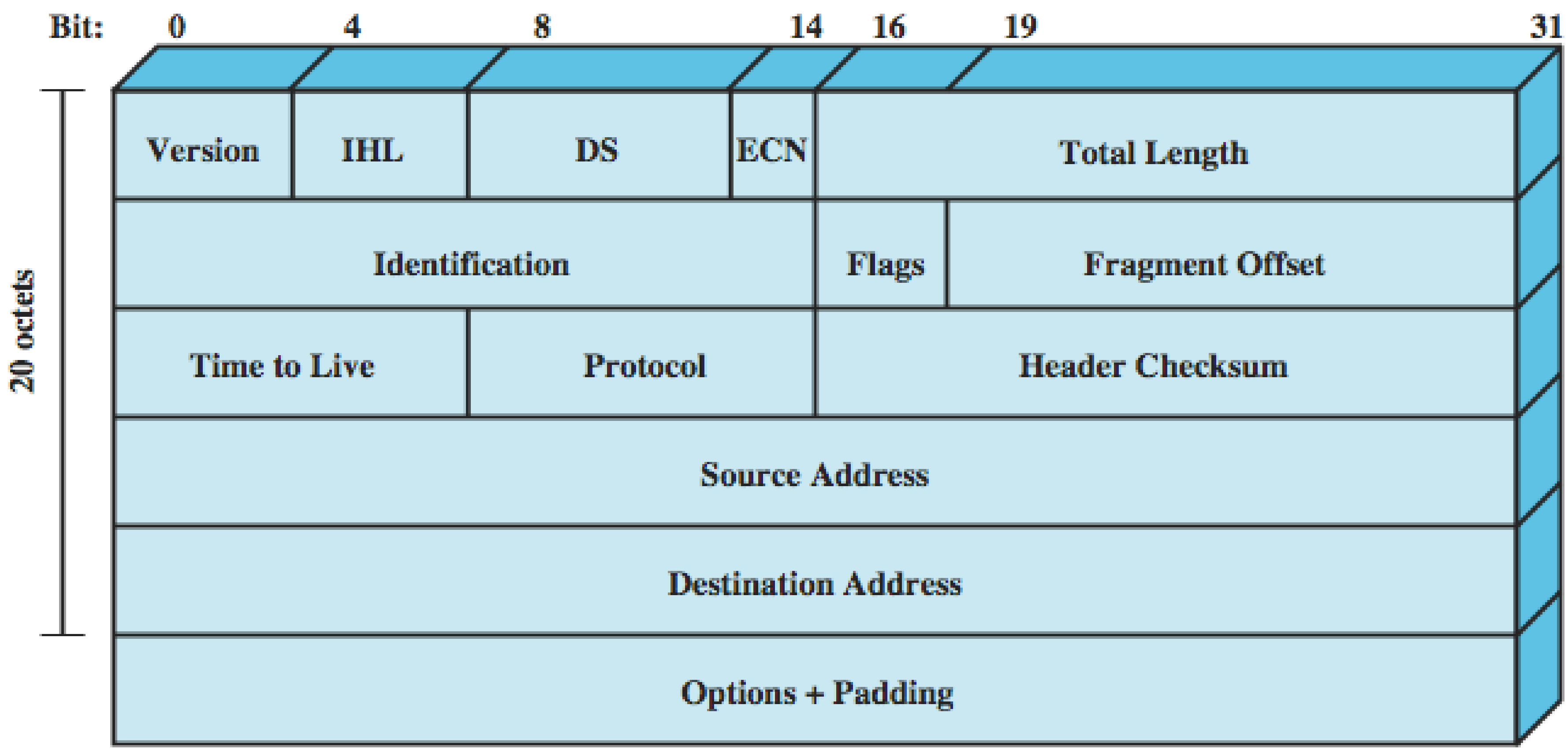
IP Parameters

- source & destination addresses
- protocol
- type of Service
- identification
- don’t fragment indicator
- time to live
- data length
- option data
- user data

IP Options

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

IPv4 Header



Bit:
0
4
8
14
16
19
31
20 octets
Version
IHL
DS
ECN
Total Length
Identification
Flags
Fragment Offset
Time to Live
Protocol
Header Checksum
Source Address
Destination Address
Options + Padding

Header Fields (1)

- Version
  - currently 4
  - IP v6 - see later
- Internet header length
  - in 32 bit words
  - including options
- DS/ECN (was type of service)
- total length
  - of datagram, in octets

Header Fields (2)

- Identification
  - sequence number
  - identify datagram uniquely with addresses / protocol
- Flags
  - More bit
  - Don’t fragment
- Fragmentation offset
- Time to live
- Protocol
  - Next higher layer to receive data field at destination

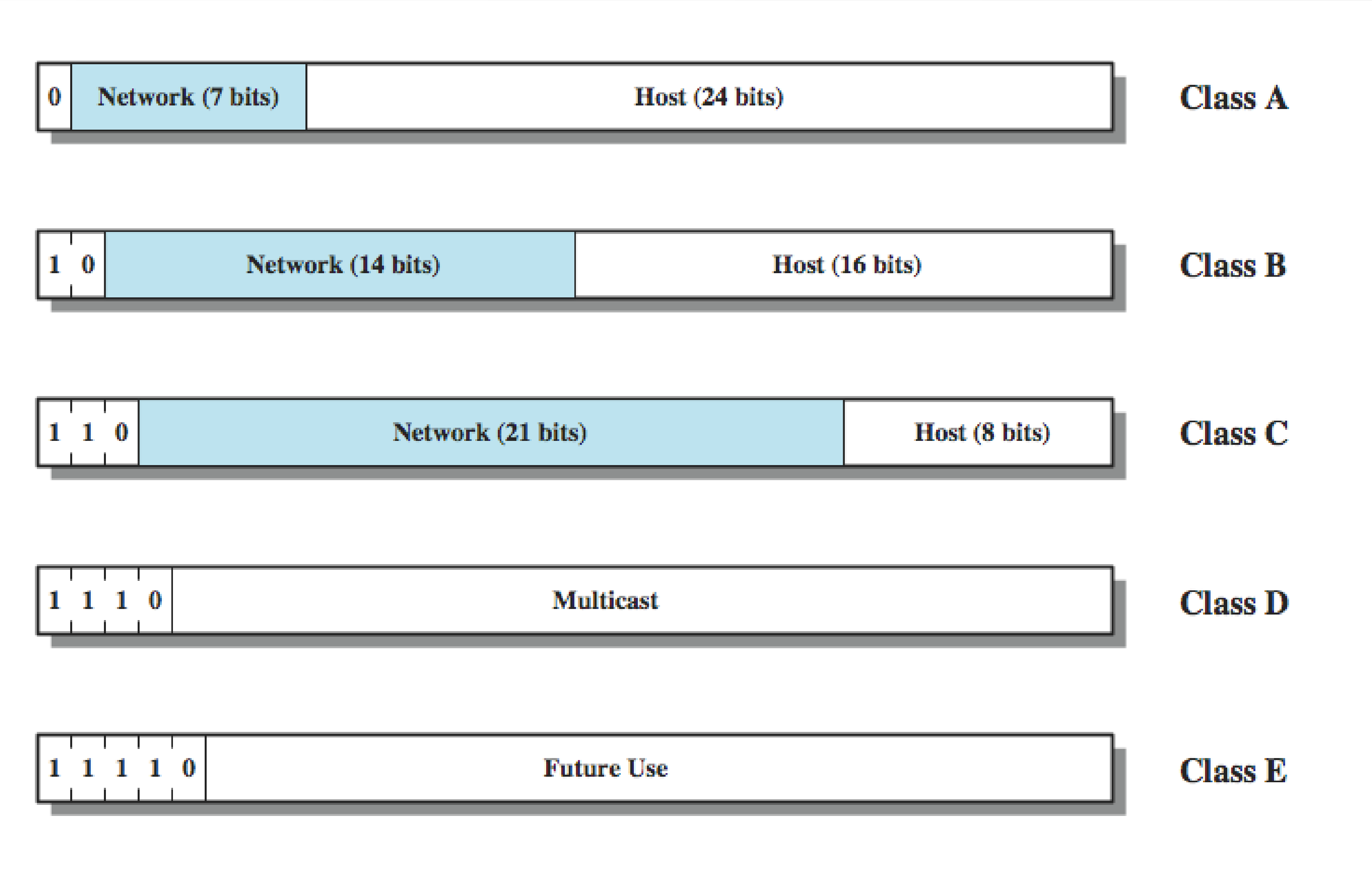
Header Fields (3)

- Header checksum
  - reverified and recomputed at each router
  - 16 bit ones complement sum of all 16 bit words in header
  - set to zero during calculation
- Source address
- Destination address
- Options
- Padding
  - to fill to multiple of 32 bits long

Data Field

- carries user data from next layer up
- integer multiple of 8 bits long (octet)
- max length of datagram (header plus data) is 65,535 octets

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
- all allocated

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
- all allocated

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

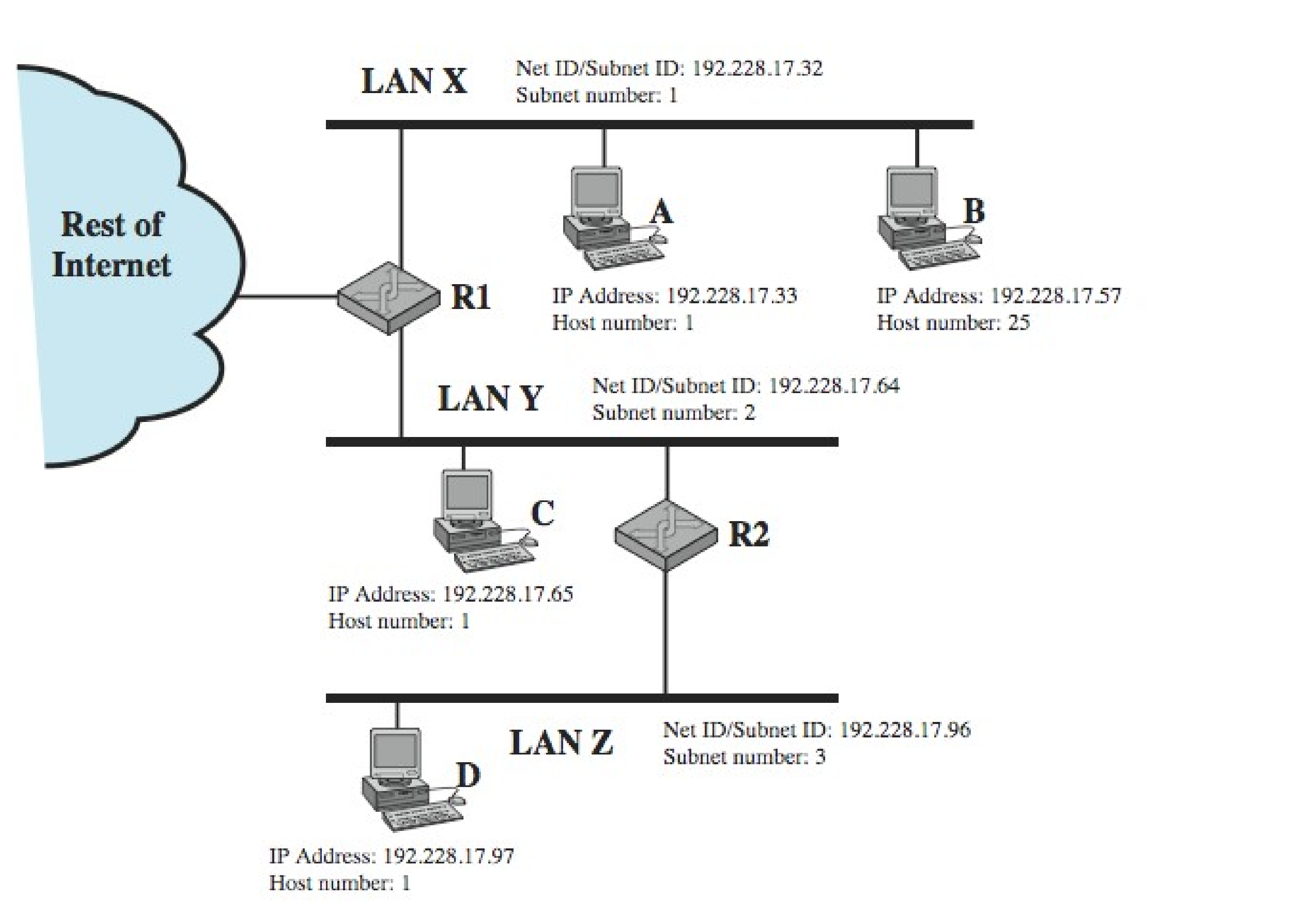
Subnets and Subnet Masks

- 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

Subnet Mask Calculation

	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

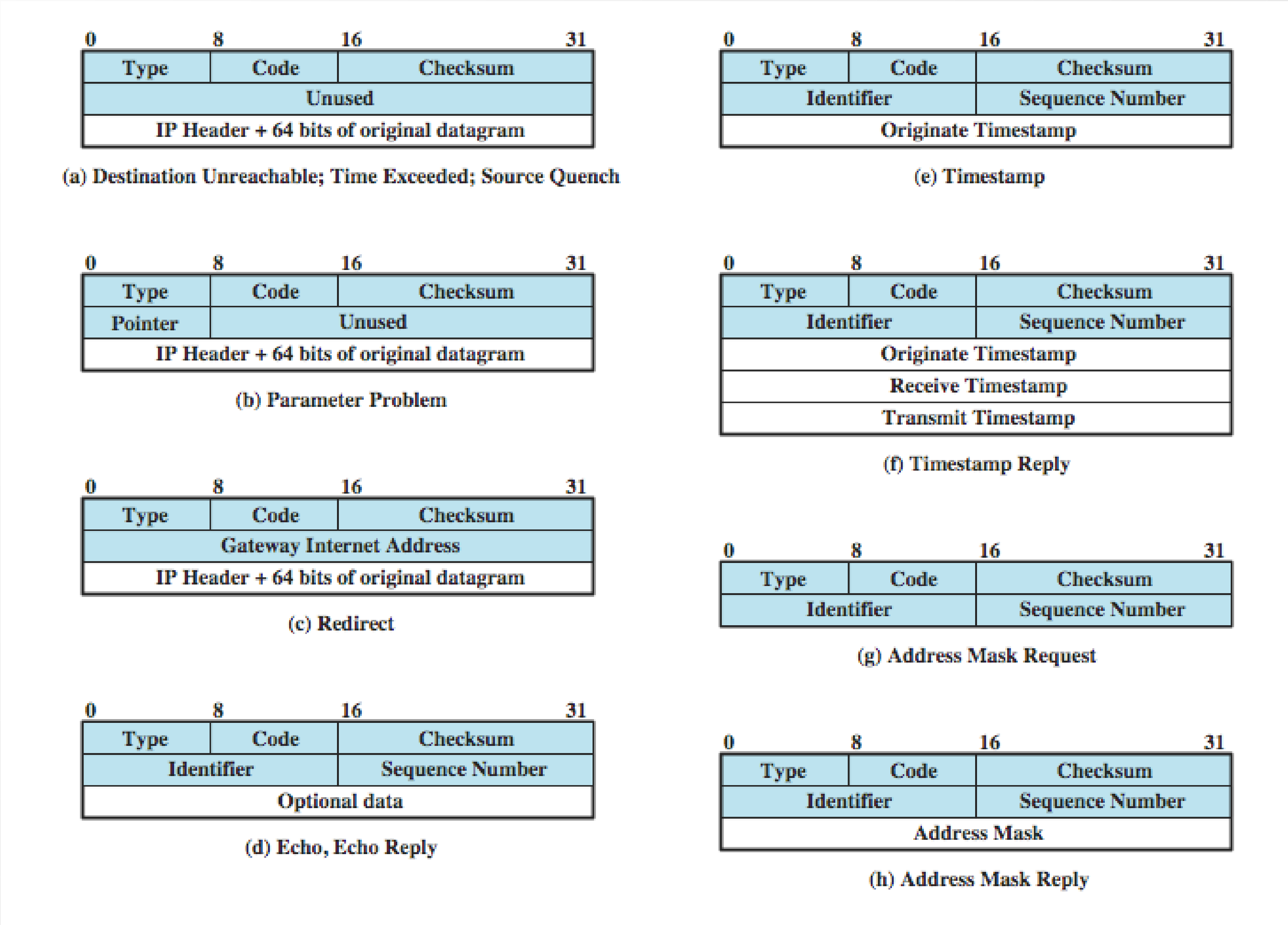
Routing Using Subnets



ICMP

- Internet Control Message Protocol
- RFC 792 (get it and study it)
- transfer of (control) messages from routers and hosts to hosts
- feedback about problems
  - e.g. time to live expired
- encapsulated in IP datagram
  - hence not reliable

ICMP Message Formats



Common ICMP Messages

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

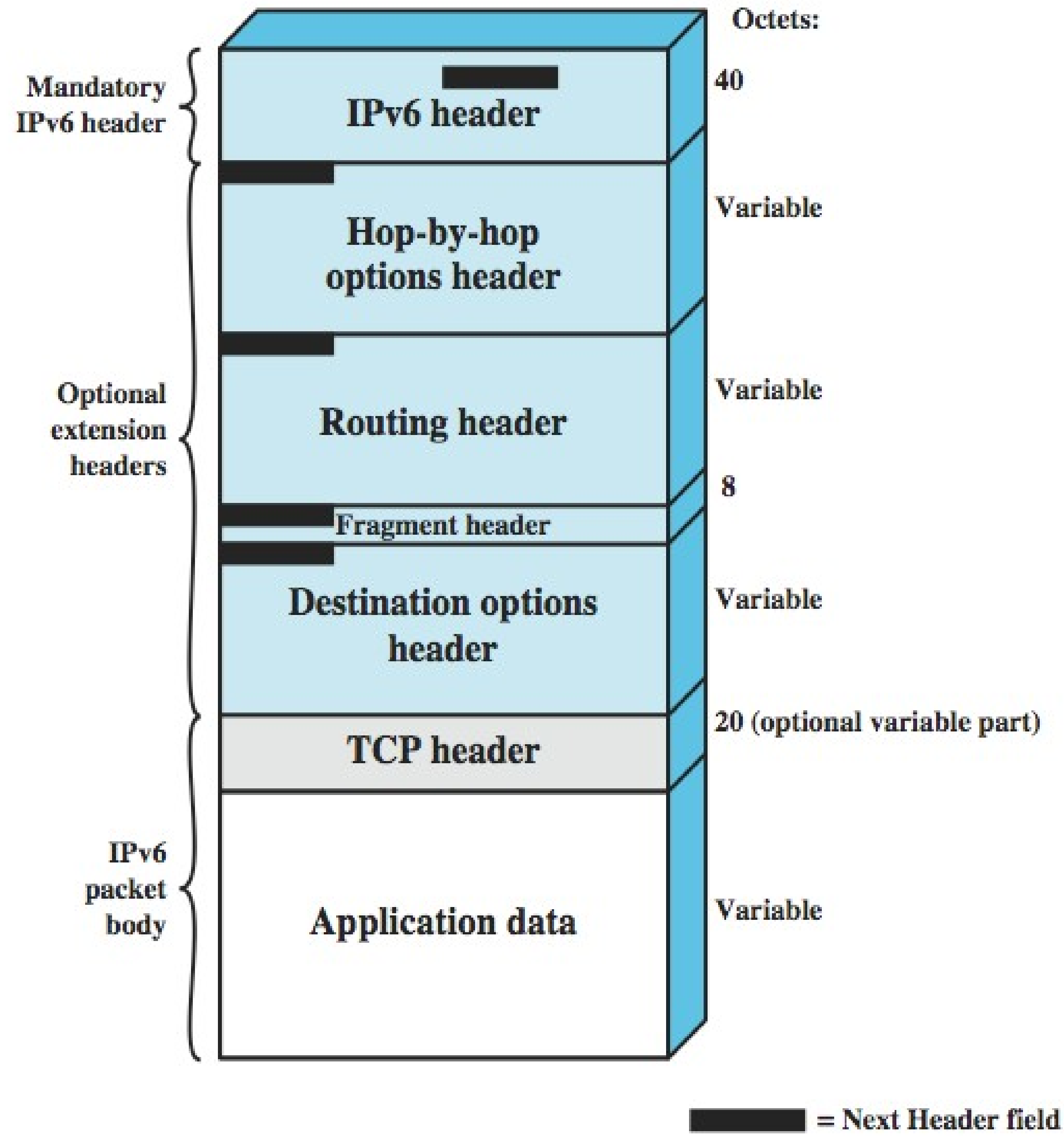
IPv6 RFCs

- RFC 1752 - Recommendations for the IP Next Generation Protocol
  - requirements
  - PDU formats
  - addressing, routing security issues
- RFC 2460 - overall specification
- RFC 2373 - addressing structure
- many others

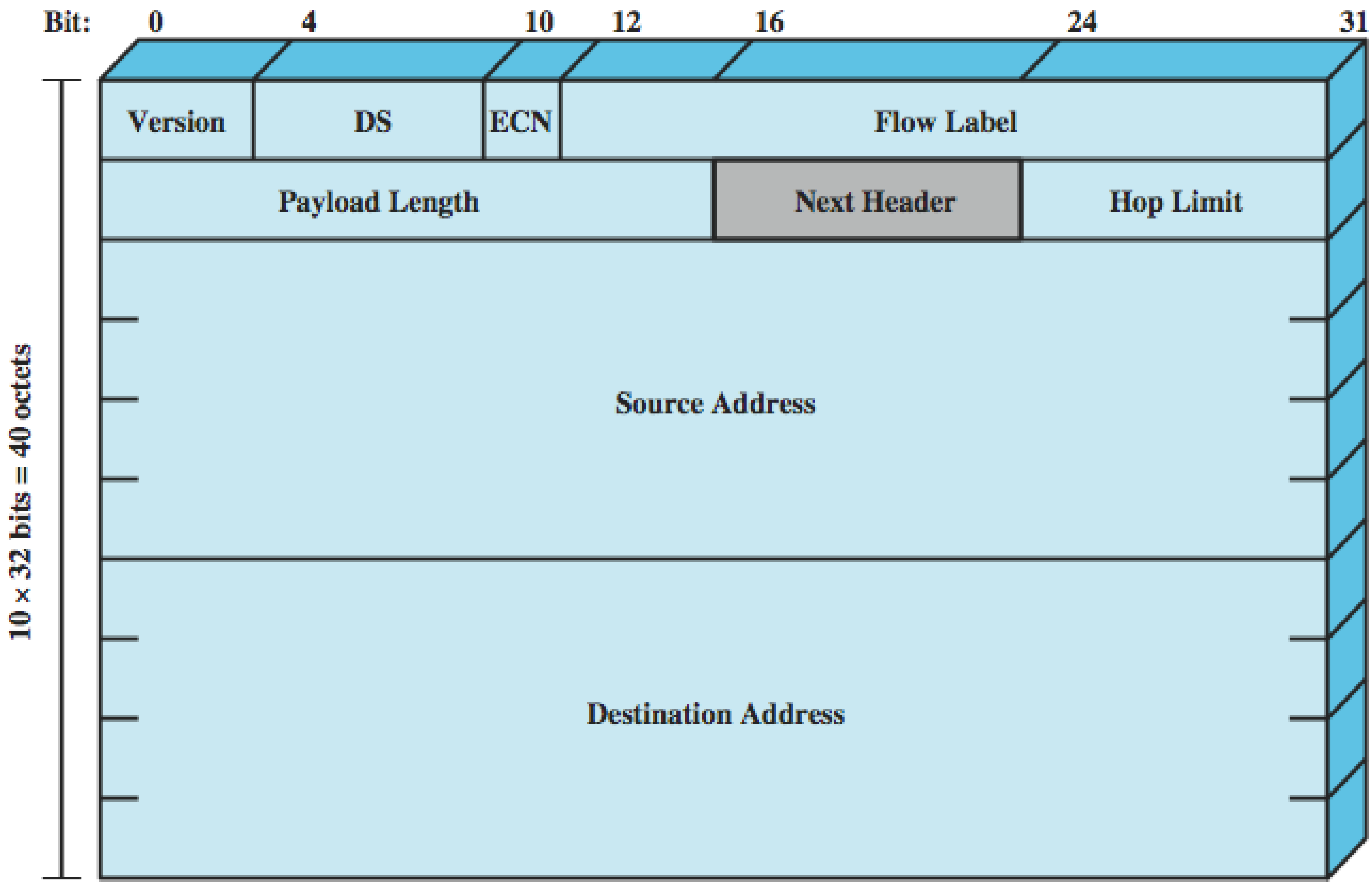
IPv6 Enhancements

- 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



IP v6 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

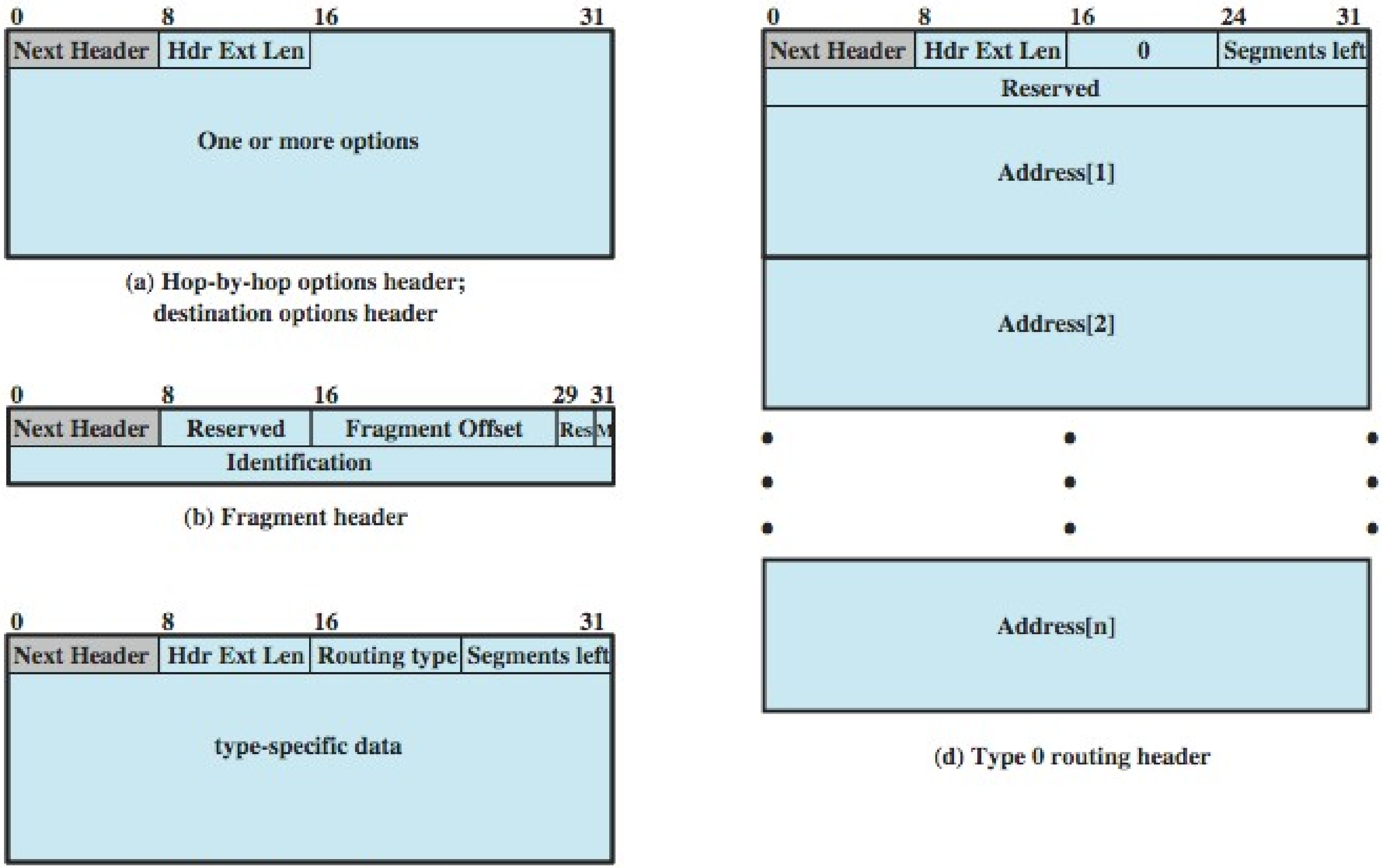
IP v6 Flow Label

- related sequence of packets
- needing special handling
- identified by src & dest addr + flow label
- router treats flow as sharing attributes
  - e.g. path, resource allocation, discard requirements, accounting, security
- may treat flows differently
  - buffer sizes, different forwarding precedence, different quality of service
- alternative to including all info 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

IPv6 Extension Headers



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

(b) Fragment header

(c) Generic routing header

(d) Type 0 routing header

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
- header includes
  - fragment offset
  - more fragments bit
  - identification

Routing Header

- list of one or more intermediate nodes to visit
- 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

- carries optional info for destination node
- format same as hop-by-hop header

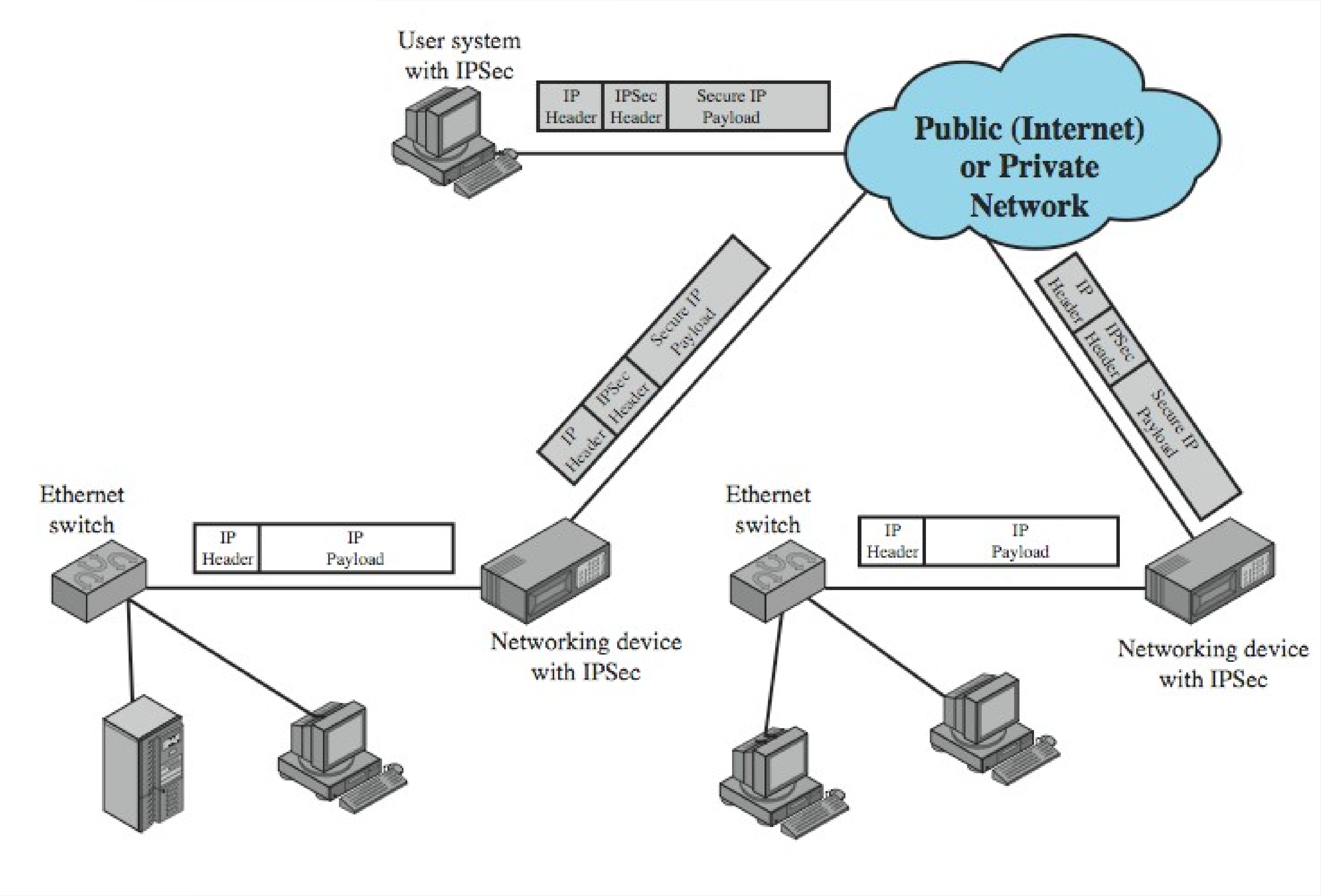
Virtual Private Networks

- set of computers interconnected using an insecure network
  - e.g. linking corporate LANs over Internet
- using encryption & special protocols to provide security
  - to stop eavesdropping & unauthorized users
- proprietary solutions are problematical
- hence development of 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
  - remote access over Internet
  - extranet & intranet connectivity for partners
  - electronic commerce security

IPSec Scenario



IPSec Benefits

- 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
  - for authentication only
- Encapsulating Security Payload (ESP)
  - for combined authentication/encryption
- a key exchange function
  - manual or automated
- VPNs usually need combined function
- see chapter 21

Summary

- basic protocol functions
- internetworking principles
- connectionless internetworking
- IP
- IPv6
- IPSec