Redes e Comunicações

Intranetworking

Internetworking Terms (1)

- Communications Network
  - Facility that provides data transfer service
- An internet
  - Collection of communications networks interconnected by bridges and/or routers
- The Internet - note upper case I
  - The global collection of thousands of individual machines and networks
- Intranet
  - Corporate internet operating within the organization
  - Uses Internet (TCP/IP and http)technology to deliver documents and resources

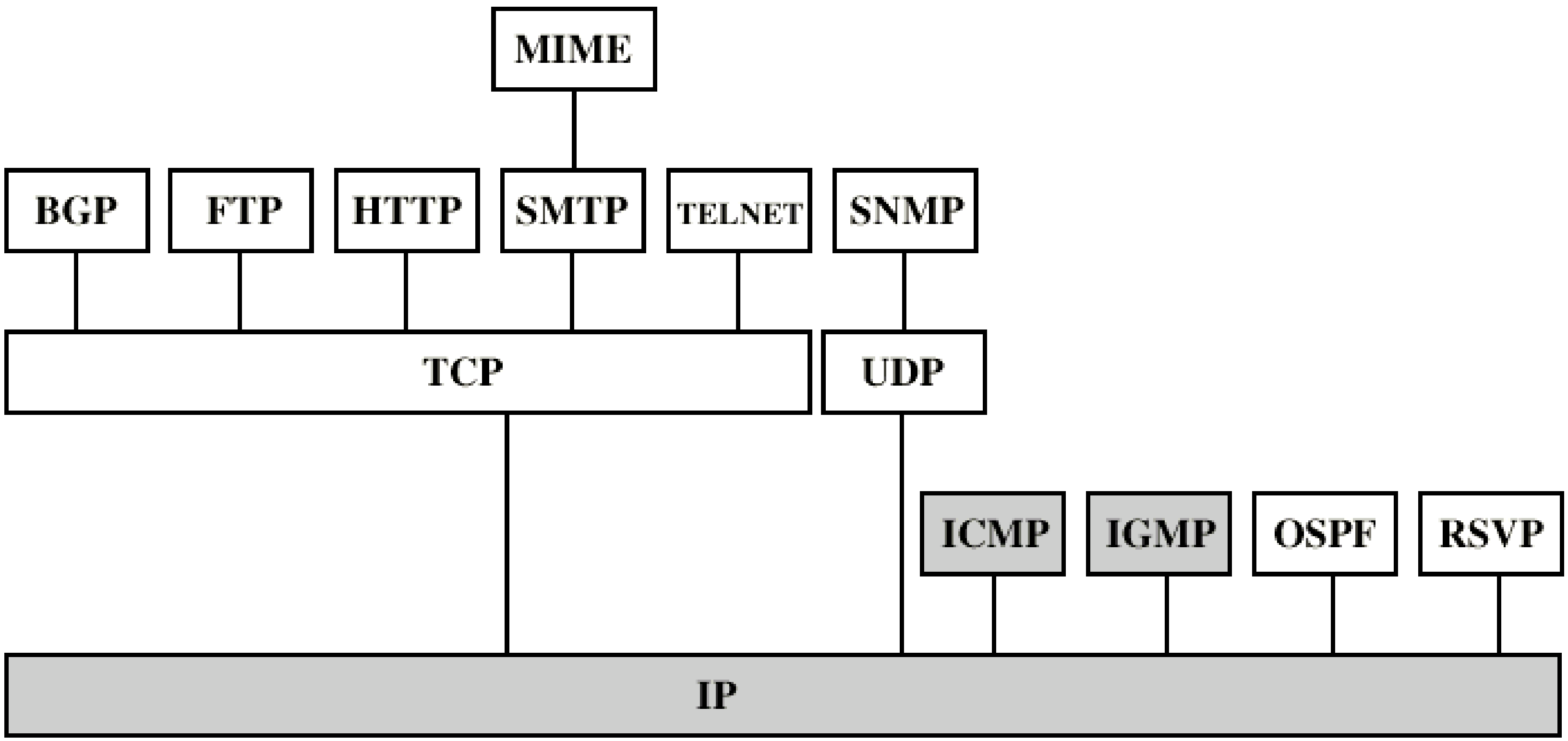
Internetworking Terms (2)

- End System (ES)
  - Device attached to one of the networks of an internet
  - Supports end-user applications or services
- Intermediate System (IS)
  - Device used to connect two networks
  - Permits communication between end systems attached to different networks

Internetworking Terms (3)

- Bridge
  - IS used to connect two LANs using similar LAN protocols
  - Address filter passing on packets to the required network only
  - OSI layer 2 (Data Link)
- Router
  - Connects two (possibly dissimilar) networks
  - Uses internet protocol present in each router and end system
  - OSI Layer 3 (Network)

Internetworking Protocols



Requirements of Internetworking

- Link between networks
  - Minimum physical and link layer
- 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
- Connectionless

Connection Oriented

- Assume that each network is connection oriented
- IS connect two or more networks
  - IS appear as DTE to each network
  - Logical connection set up between DTEs
    - Concatenation of logical connections across networks
  - Individual network virtual circuits joined by IS
- May require enhancement of local network services
  - 802, FDDI are datagram services

Connection Oriented IS Functions

- Relaying
- Routing

- e.g. X.75 used to interconnect X.25 packet switched networks

- Connection oriented not often used
  - (IP dominant)

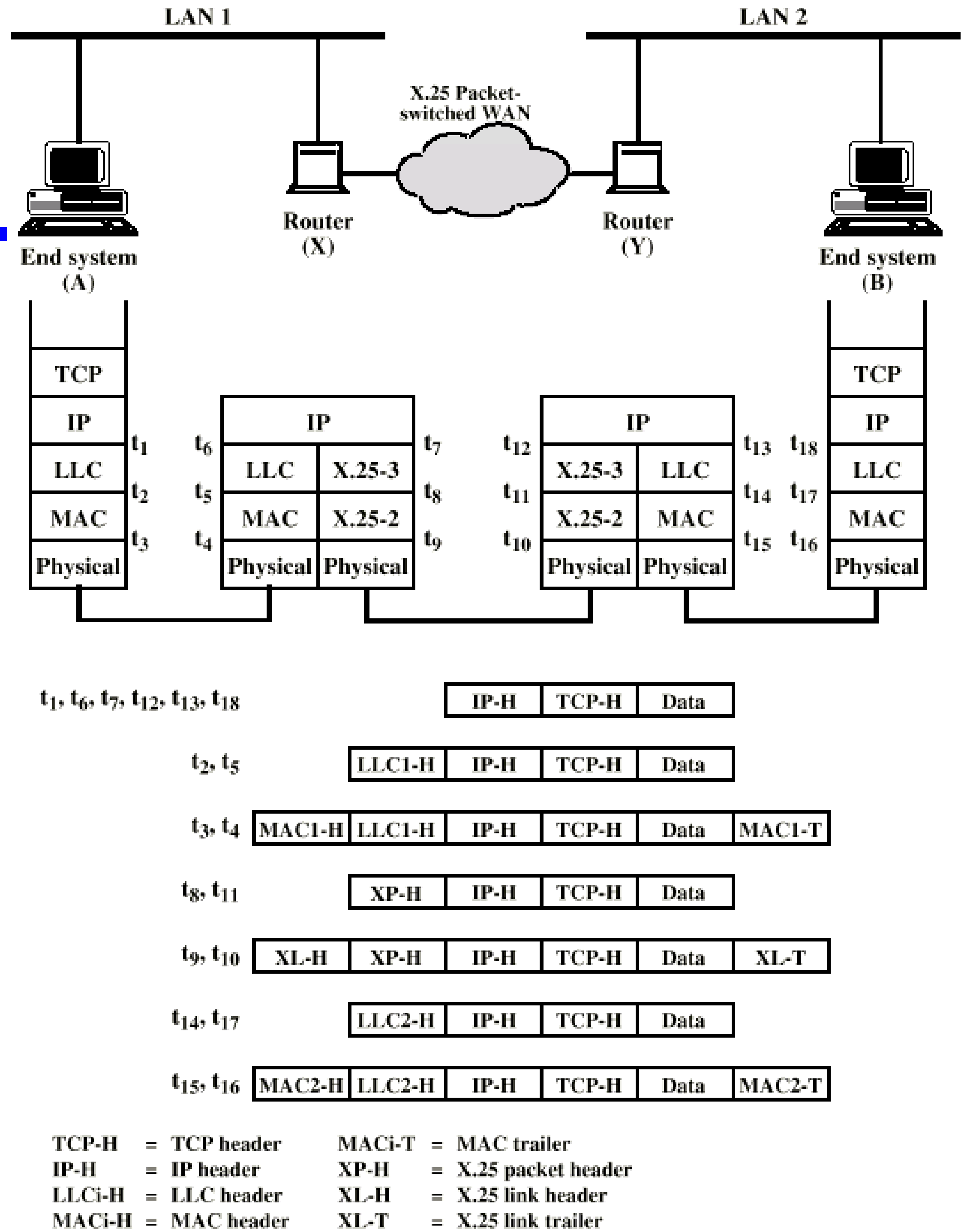
Connectionless Operation

- Corresponds to datagram mechanism in packet switched network
- Each NPDU treated separately
- Network layer protocol common to all DTEs and routers
  - Known generically as the internet protocol
- Internet Protocol
  - One such internet protocol developed for ARPANET
  - RFC 791 (Get it and study it)
- Lower layer protocol needed to access 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)

IP Operation



Design Issues

- Routing
- Datagram lifetime
- Fragmentation and re-assembly
- Error control
- Flow control

Routing

- End systems and routers maintain routing tables
  - Indicate next router to which datagram should be sent
  - Static
    - May contain alternative routes
  - Dynamic
    - Flexible response to congestion and errors
- Source routing
  - Source specifies route as sequential list of routers to be followed
  - Security
  - Priority
- Route recording

Datagram Lifetime

- Datagrams could loop indefinitely
  - Consumes resources
  - Transport protocol may need upper bound on datagram life
- Datagram marked with lifetime
  - Time To Live field in IP
  - Once lifetime expires, datagram discarded (not forwarded)
  - Hop count
    - Decrement time to live on passing through a each router
  - Time count
    - Need to know how long since last router
- (Aside: compare with Logan's Run)

Fragmentation and Re-assembly

- Different packet sizes
- When to re-assemble
  - At destination
    - Results in packets getting 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
      - Inhibits dynamic routing

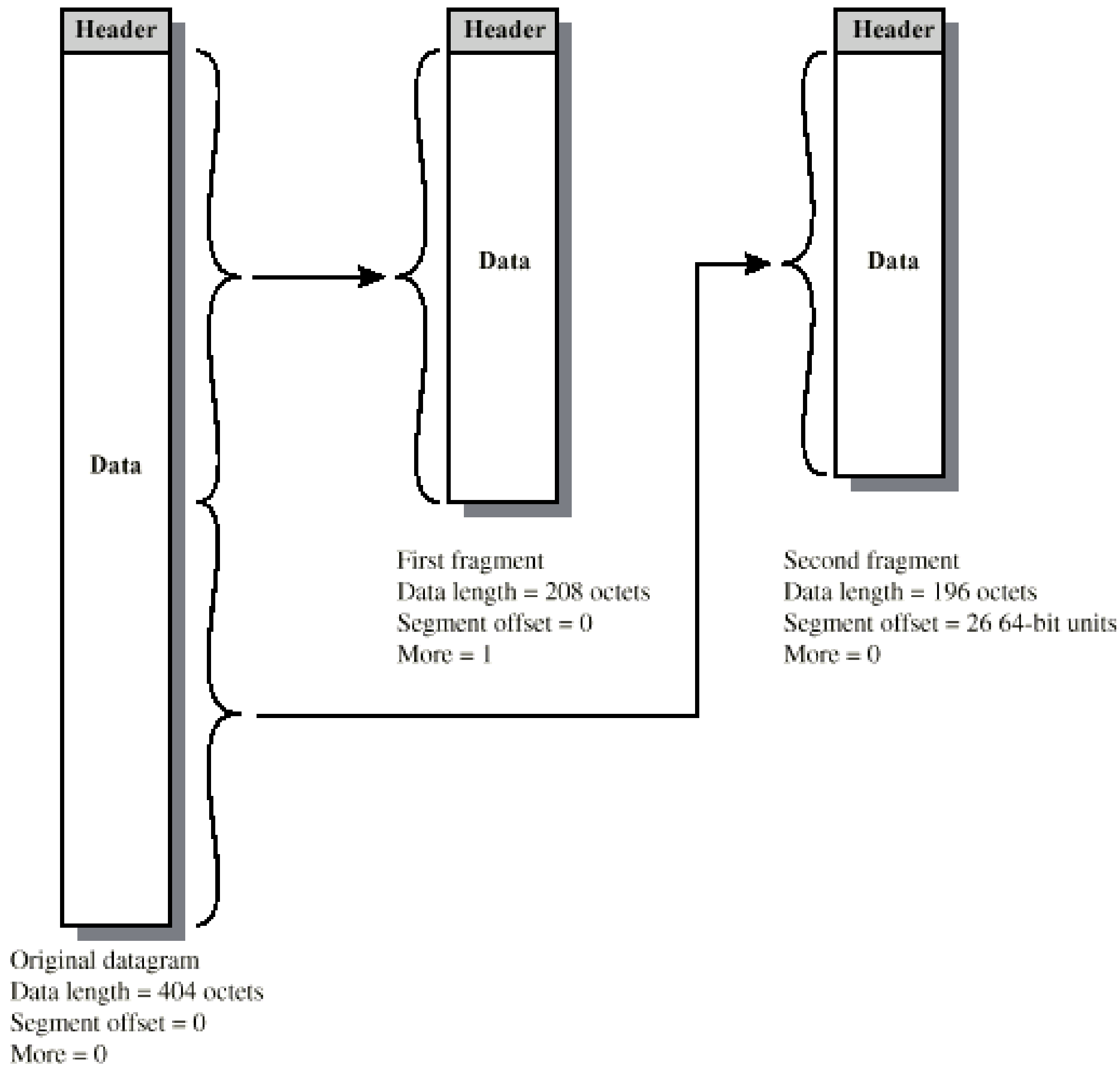
IP Fragmentation (1)

- IP re-assembles at destination only
- Uses fields in header
  - Data Unit Identifier (ID)
    - Identifies end system originated datagram
      - Source and destination address
      - Protocol layer generating data (e.g. TCP)
      - Identification supplied by that layer
  - Data length
    - Length of user data in octets

IP Fragmentation (2)

- 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

- Not guaranteed delivery
- Router should attempt to inform source if packet discarded
  - e.g. for time to live expiring
- Source may modify transmission strategy
- May inform high layer protocol
- Datagram identification needed
- (Look up ICMP)

Flow Control

- Allows routers and/or stations to limit rate of incoming data
- Limited in connectionless systems
- Send flow control packets
  - Requesting reduced flow
- e.g. ICMP

Internet Protocol (IP)

- Part of TCP/IP
  - Used by the Internet
- Specifies interface with higher layer
  - e.g. TCP
- Specifies protocol format and mechanisms

IP Services

- Primitives
  - Functions to be performed
  - Form of primitive implementation dependent
    - e.g. subroutine call
  - Send
    - Request transmission of data unit
  - Deliver
    - Notify user of arrival of data unit
- Parameters
  - Used to pass data and control info

Parameters (1)

- Source address
- Destination address
- Protocol
  - Recipient e.g. TCP
- Type of Service
  - Specify treatment of data unit during transmission through networks
- Identification
  - Source, destination address and user protocol
  - Uniquely identifies PDU
  - Needed for re-assembly and error reporting
  - Send only

Parameters (2)

- Don’t fragment indicator
  - Can IP fragment data
  - If not, may not be possible to deliver
  - Send only
- Time to live
  - Send onl
- Data length
- Option data
- User data

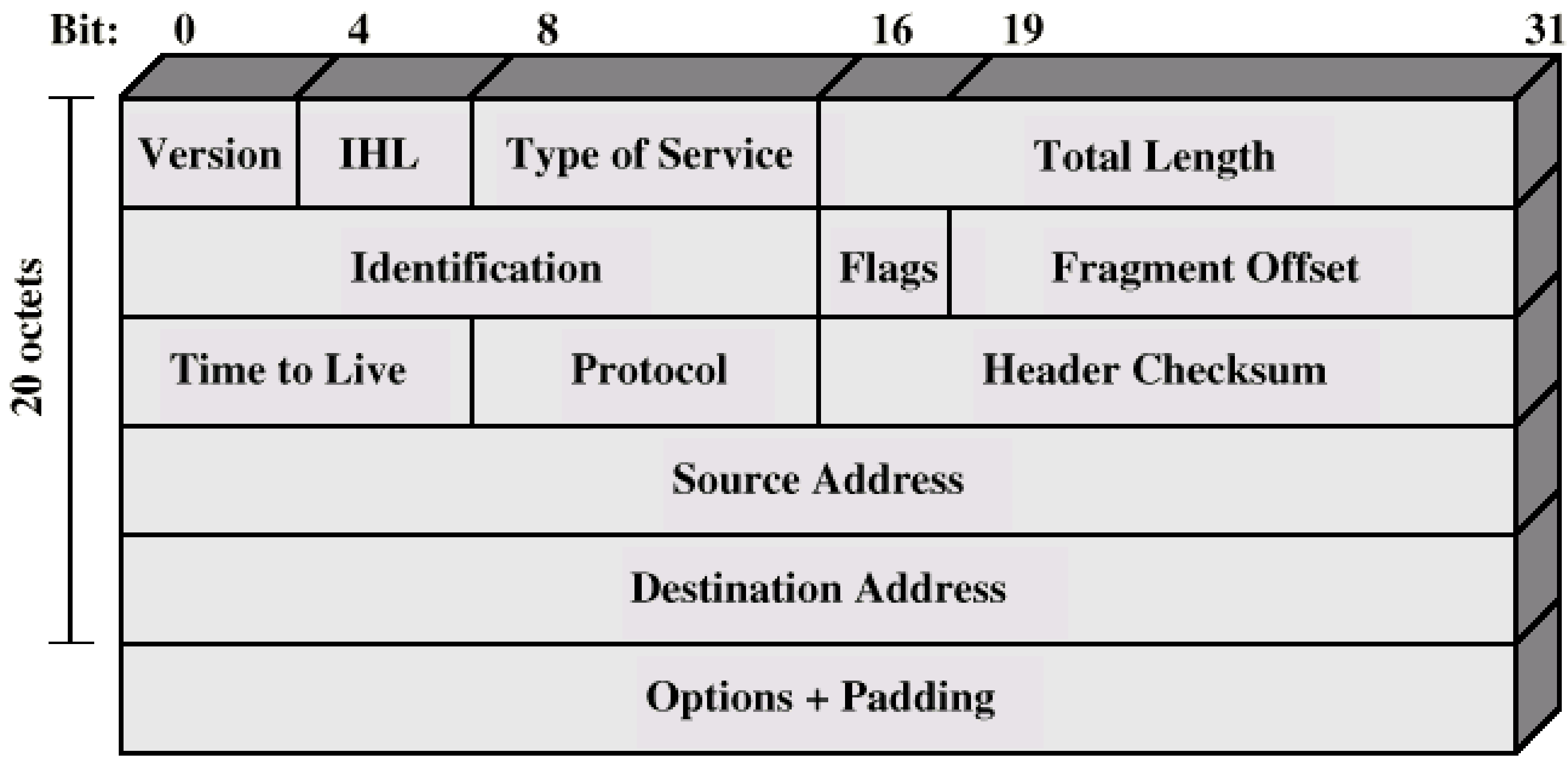
Type of Service

- Precedence
  - 8 levels
- Reliability
  - Normal or high
- Delay
  - Normal or low
- Throughput
  - Normal or high

Options

- Security
- Source routing
- Route recording
- Stream identification
- Timestamping

IP Protocol



Bit: 0 4 8 16 19 31
20 octets
Version
IHL
Type of Service
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
- Type of service
- Total length
  - Of datagram, in octets

Header Fields (2)

- Identification
  - Sequence number
  - Used with addresses and user protocol to identify datagram uniquely
- 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) 65,535 octets

IP Addresses - Class A

- 32 bit global internet address
- Network part and host part
- 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 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

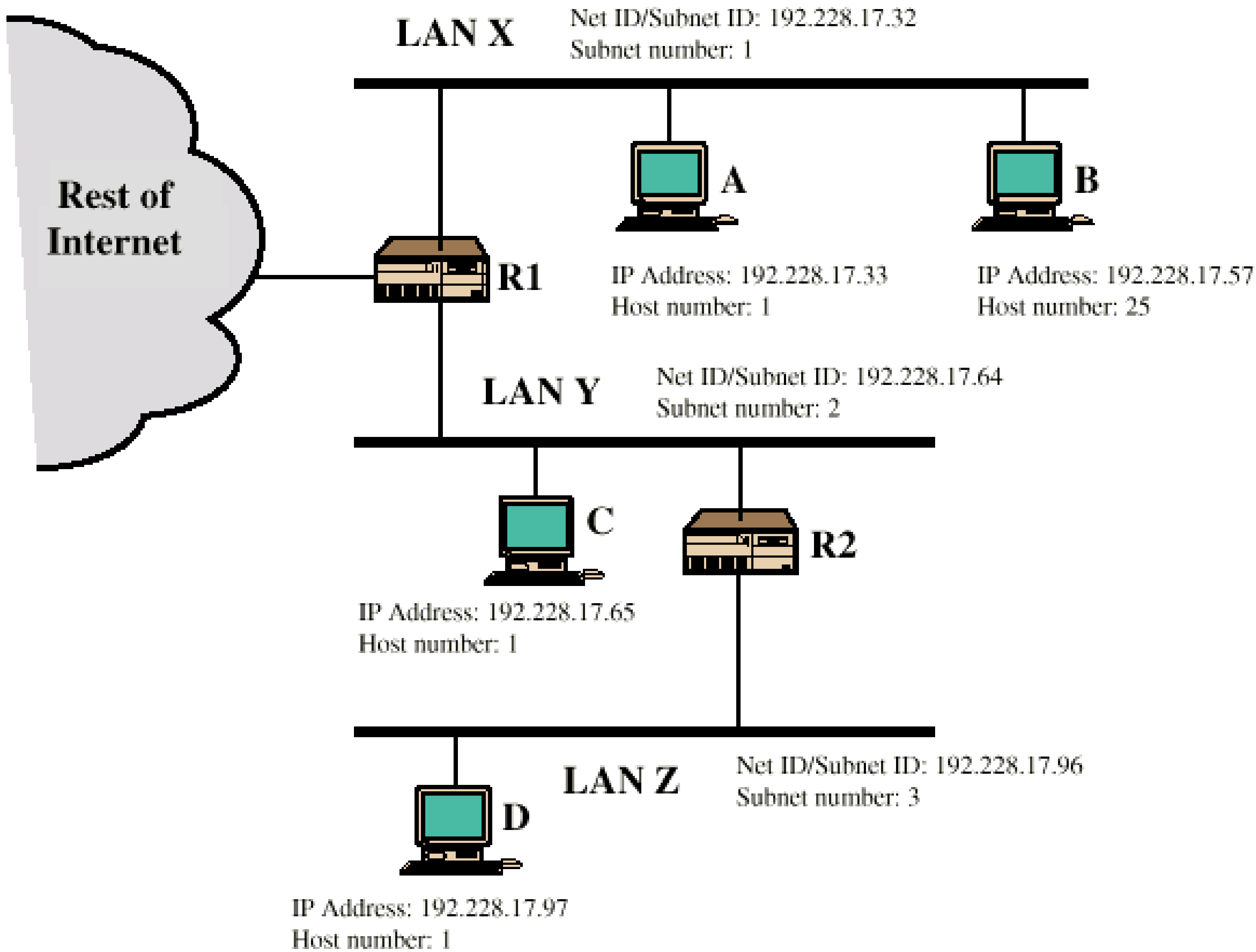
IP Addresses - Class C

- Start 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

- Allow 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

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
  - Not reliable

ICMP Message Formats

0	8	16	31
Type	Code	Checksum	
Unused			
IP Header + 64 bits of original datagram			

(a) Destination Unreachable; Time Exceeded; Source Quench

0	8	16	31
Type	Code	Checksum	
Pointer	Unused		
IP Header + 64 bits of original datagram			

(b) Parameter Problem

0	8	16	31
Type	Code	Checksum	
Gateway Internet Address			
IP Header + 64 bits of original datagram			

(c) Redirect

0	8	16	31
Type	Code	Checksum	
Identifier		Sequence Number	
Optional data			

(d) Echo, Echo Reply

0	8	16	31
Type	Code	Checksum	
Identifier		Sequence Number	
Originate Timestamp			

(e) Timestamp

0	8	16	31
Type	Code	Checksum	
Identifier		Sequence Number	
Originate Timestamp			
Receive Timestamp			
Transmit Timestamp			

(f) Timestamp Reply

0	8	16	31
Type	Code	Checksum	
Identifier		Sequence Number	

(g) Address Mask Request

0	8	16	31
Type	Code	Checksum	
Identifier		Sequence Number	
Address Mask			

(h) Address Mask Reply

IP v6 - Version Number

- 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
  - Next Generation

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
  - Extended use of TCP/IP
  - Single address per host
- Requirements for new types of service

IPv6 RFCs

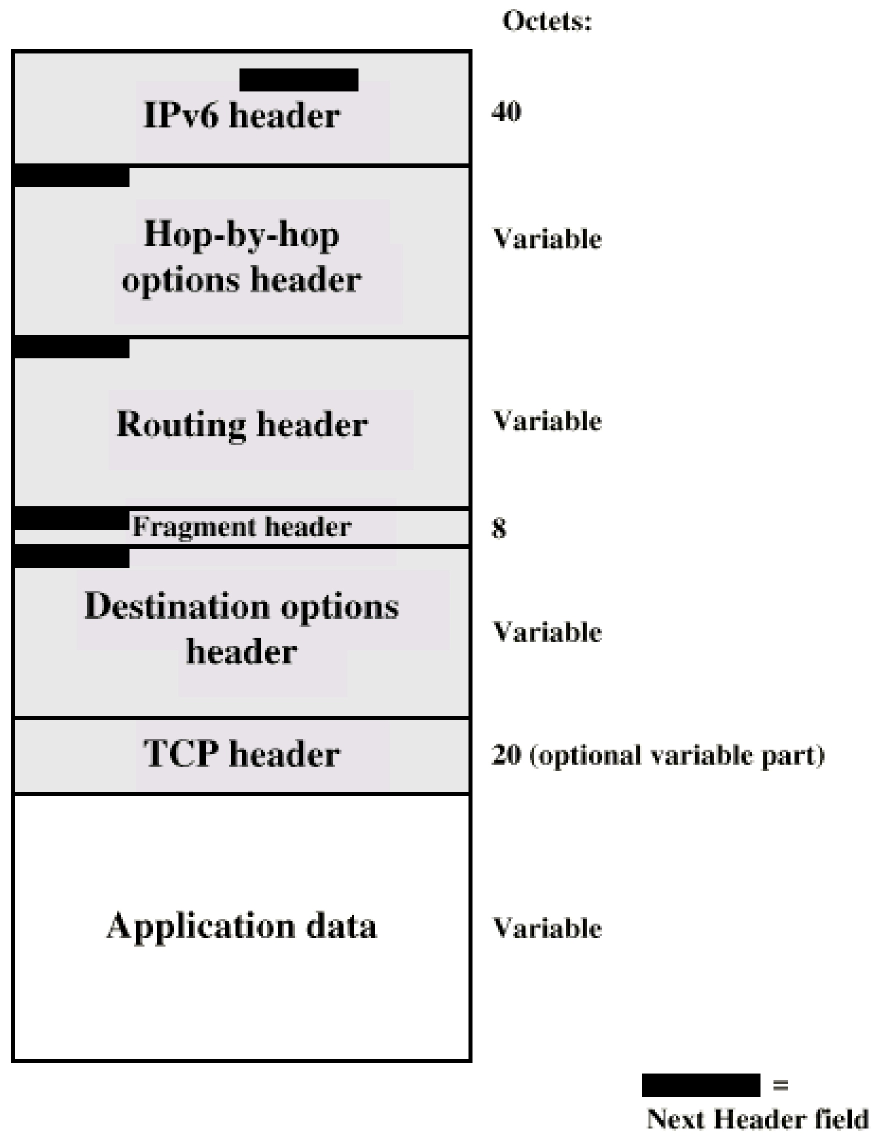
- 1752 - Recommendations for the IP Next Generation Protocol
- 2460 - Overall specification
- 2373 - addressing structure
- others (find them)

- 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
    - Improved speed and simplified router processing
    - Easier to extend options
- Address autoconfiguration
  - Dynamic assignment of addresses

IPv6 Enhancements (2)

- Increased addressing flexibility
  - Anycast - delivered to one of a set of nodes
  - Improved scalability of multicast addresses
- Support for resource allocation
  - Replaces type of service
  - Labeling of packets to particular traffic flow
  - Allows special handling
  - e.g. real time video

Structure

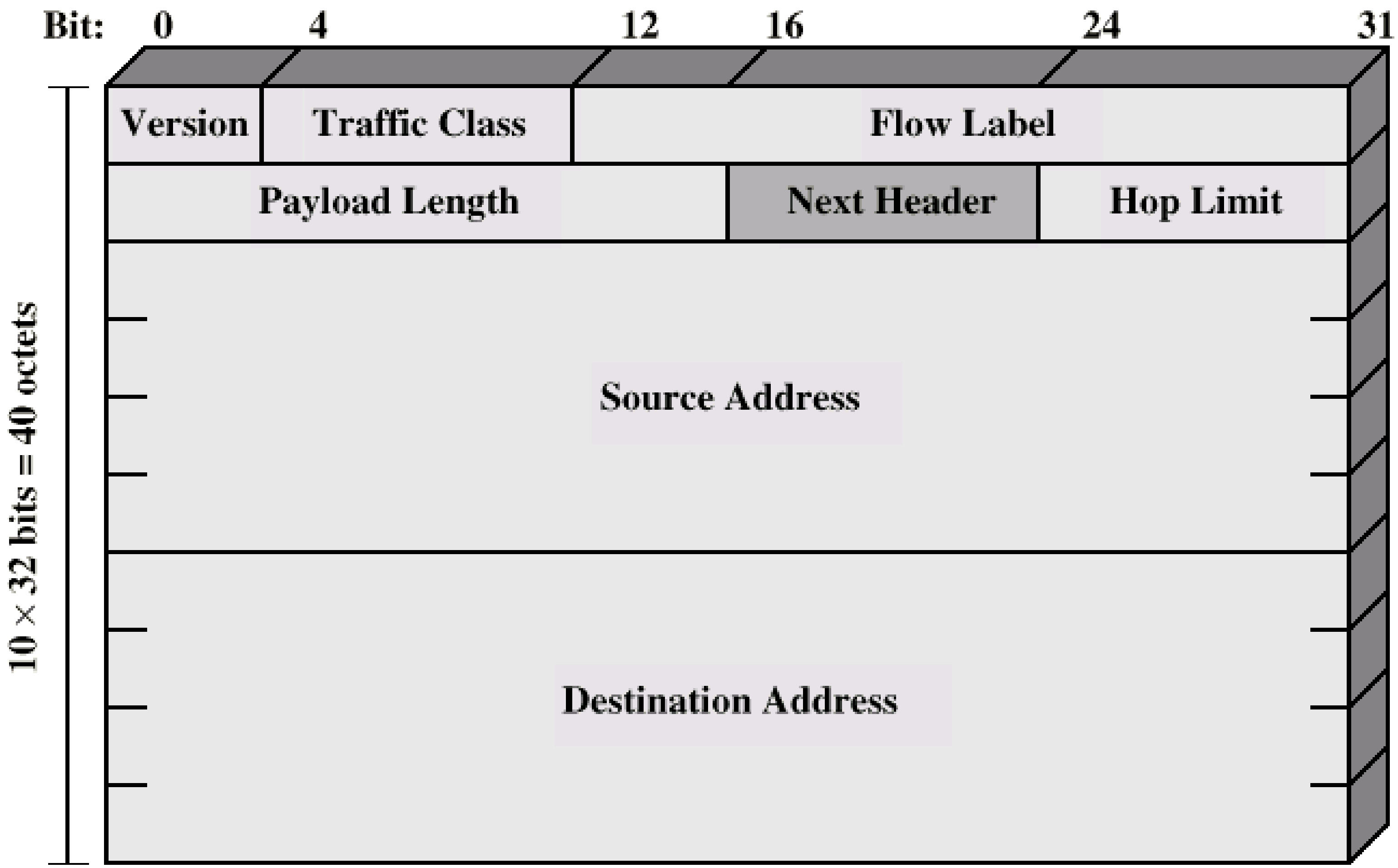


Octets:
IPv6 header
40
Hop-by-hop options header
Variable
Routing header
Variable
Fragment header
8
Destination options header
Variable
TCP header
20 (optional variable part)
Application data
Variable
= Next Header field

Extension Headers

- Hop-by-Hop Options
  - Require processing at each router
- Routing
  - Similar to v4 source routing
- Fragment
- Authentication
- Encapsulating security payload
- Destination options
  - For destination node

IP v6 Header



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

IP v6 Header Fields (1)

- Version
  - 6
- Traffic Class
  - Classes or priorities of packet
  - Still under development
  - See RFC 2460
- Flow Label
  - Used by hosts requesting special handling
- Payload length
  - Includes all extension headers plus user data

IP v6 Header Fields (2)

- Next Header
  - Identifies type of header
    - Extension or next layer up
- Source Address
- Destination address

IPv6 Addresses

- 128 bits long
- Assigned to interface
- Single interface may have multiple unicast addresses
- Three types of address

Types of address

- Unicast
  - Single interface
- Anycast
  - Set of interfaces (typically different nodes)
  - Delivered to any one interface
  - the “nearest”
- Multicast
  - Set of interfaces
  - Delivered to all interfaces identified

Hop-by-Hop Options

- Next header
- Header extension length
- Options
  - Jumbo payload
    - Over 2^{16} = 65,535 octets
  - Router alert
    - Tells the router that the contents of this packet is of interest to the router
    - Provides support for RSPV (chapter 16)

Fragmentation Header

- Fragmentation only allowed at source
- No fragmentation at intermediate routers
- Node must perform path discovery to find smallest MTU of intermediate networks
- Source fragments to match MTU
- Otherwise limit to 1280 octets

Fragmentation Header Fields

- Next Header
- Reserved
- Fragmentation offset
- Reserved
- More flag
- Identification

Routing Header

- List of one or more intermediate nodes to be visited
- Next Header
- Header extension length
- Routing type
- Segments left
  - i.e. number of nodes still to be visited

Destination Options

- Same format as Hop-by-Hop options header

Multicasting

- Addresses that refer to group of hosts on one or more networks
- Uses
  - Multimedia “broadcast”
  - Teleconferencing
  - Database
  - Distributed computing
  - Real time workgroups

Requirements for Multicasting (1)

- Router may have to forward more than one copy of packet
- Convention needed to identify multicast addresses
  - IPv4 - Class D - start 1110
  - IPv6 - 8 bit prefix, all 1, 4 bit flags field, 4 bit scope field, 112 bit group identifier
- Nodes must translate between IP multicast addresses and list of networks containing group members
- Router must translate between IP multicast address and network multicast address

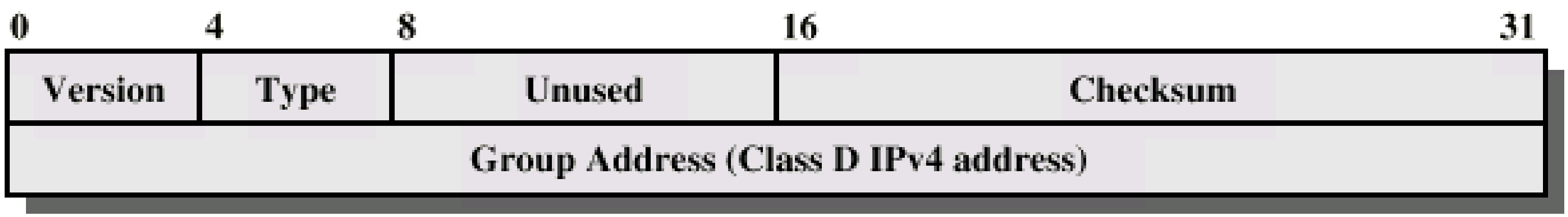
Requirements for Multicasting (2)

- Mechanism required for hosts to join and leave multicast group
- Routers must exchange info
  - Which networks include members of given group
  - Sufficient info to work out shortest path to each network
  - Routing algorithm to work out shortest path
  - Routers must determine routing paths based on source and destination addresses

IGMP

- Internet Group Management Protocol
- RFC 1112
- Host and router exchange of multicast group info
- Use broadcast LAN to transfer info among multiple hosts and routers

IGMP Format


0
4
8
16
31
Version
Type
Unused
Checksum
Group Address (Class D IPv4 address)

IGMP Fields

- Version
  - 1
- Type
  - 1 - query sent by router
  - O - report sent by host
- Checksum
- Group address
  - Zero in request message
  - Valid group address in report message

IGMP Operation

- To join a group, hosts sends report message
  - Group address of group to join
  - In IP datagram to same multicast destination address
  - All hosts in group receive message
  - Routers listen to all multicast addresses to hear all reports
- Routers periodically issue request message
  - Sent to all-hosts multicast address
  - Host that want to stay in groups must read all-hosts messages and respond with report for each group it is in

Group Membership in IPv6

- Function of IGMP included in ICMP v6
- New group membership termination message to allow host to leave group