Internetwork Protocols

Background to IP
IP, and related protocols

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

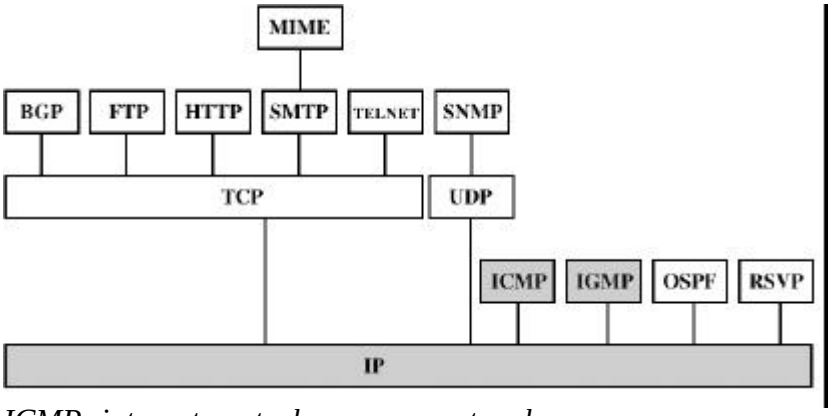
Internetworking Terms (2)

- 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)

- Repeater: used to connect link, retransmitting signals bidirectionally - OSI Layer 1
- Bridge
  - IS used to connect two LANs using similar protocols
  - Address filter passing on packets to the required network only
  - OSI layer 2 (Data Link)
- Router
  - IS connects two (possibly dissimilar) networks
  - Uses internet protocol present in each router and end system
  - OSI Layer 3 (Network)

Internetworking Protocols



ICMP: internet control message protocol
IGMP: internet group management protocol

Network Architecture Features

- These are generally all present, but different on different constituent networks
  - 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)

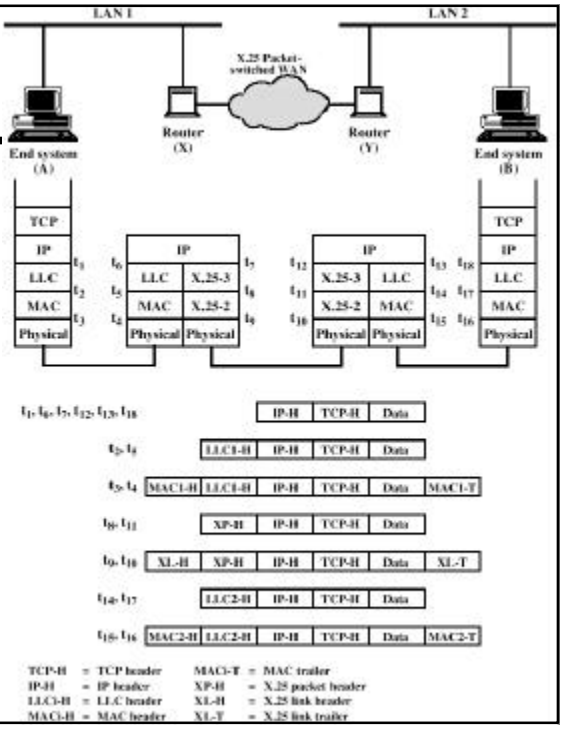
Connectionless Operation

- 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 (IP)
  - One such internet protocol developed for ARPANET
  - RFC 791
- 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 (already discussed)
- Datagram lifetime
- Fragmentation and re-assembly
- Error control
- Flow control

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
  - also important for timeouts at TCP level

Fragmentation and Re-assembly

- Different packet sizes used in different networks
- 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

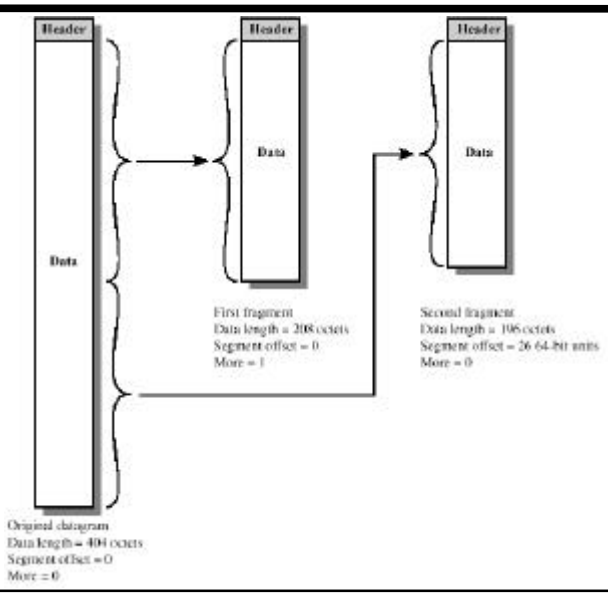
IP Fragmentation (1)

- 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

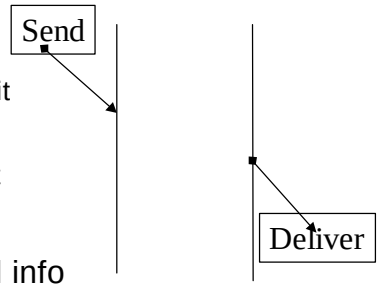
- Allows routers and/or stations to limit rate of incoming data
- Limited in connectionless systems
- Send flow control packets
  - Requesting reduced flow
- e.g. ICMP

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



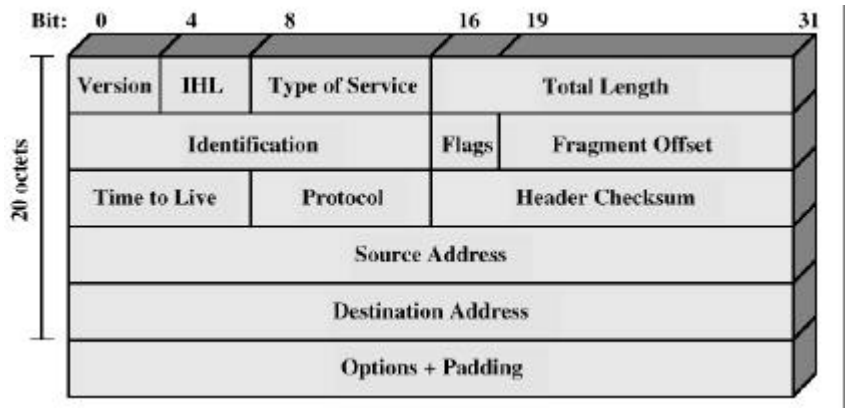
Parameters (1) (Send & Deliver)

- Source address
- Destination address
- Protocol
  - Recipient e.g. TCP
- Type of Service
  - Specify treatment of data unit during transmission through networks
  - Precedence (8 levels), Reliability (Normal or high), Delay (Normal or low), Throughput (Normal or high)
- Identification (Send only)
  - Uniquely identifies PDU
  - Needed for re-assembly and error reporting

Parameters (2) (Send & Deliver)

- Don t fragment indicator (Send only)
  - Can IP fragment data ?
  - If not, may not be possible to deliver
- Time to live (Send only)
  - in seconds
- Data length
- Option data
  - security, source routing, route recording, stream id, timestamping
- User data
  - and padding: length is 32 bit multiple

IP Protocol



Header Fields (1)

- Version
  - Currently 4 or 6
- IP 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
  - 4 bytes each in IPv4

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

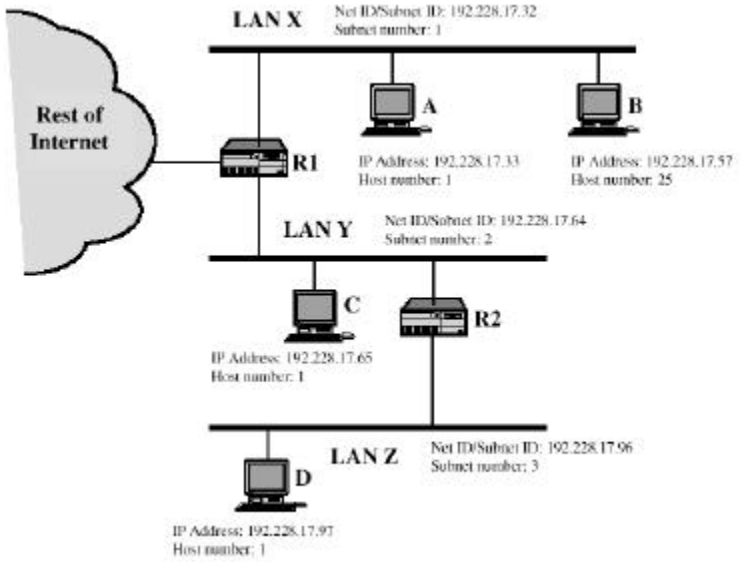
IP Addresses - Class C

- 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
- Transfer of (control) messages from routers and hosts to hosts
- Feedback about problems
  - e.g. destination unreachable, time to live expired, source quench (for flow control)
- Encapsulated in IP datagram
  - Not reliable

ICMP Message Formats