BUS3150 - Computer Facilities Network Management

10 - Internet Protocols

Faculty of Information Technology
Monash University

This Lecture

- Principles of internetworking.
- Internet Protocol Version 4 (IPv4).
- IPv4 Address structure including subnetworking.

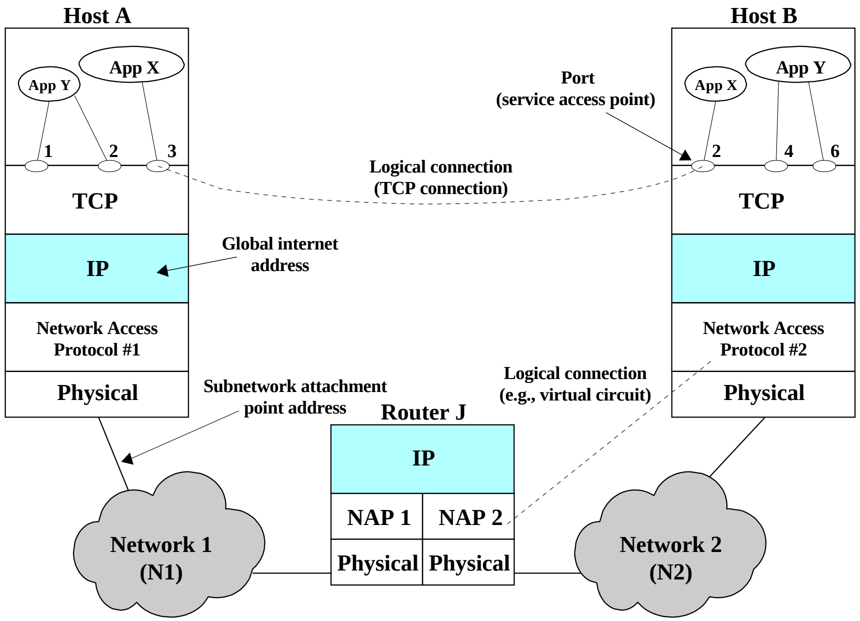
Internetworking

- Techniques to connect various sub-networks so that services can be shared and appear to users as a single large network.
- Establish seamless communication links among machnines operating at distant locations, connected to varying types of sub-networks (e.g. LANs) and using different operating systems.
- Require a globally accepted method for connecting networks.

Internetworking

- 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 Using TCP/IP



Internetworking

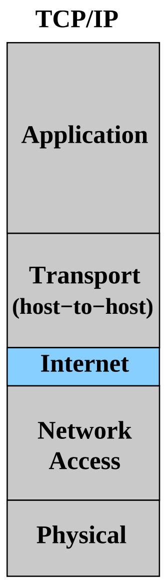
- End System (ES)
  - Device attached to one of the networks of an internet.
  - Supports end-user applications or services.
  - Example: Host A and Host B in the previous slide.
  - Includes workstations, PDA, etc.
- Intermediate System (IS)
  - Device used to connect two networks.
  - Permits communication between end systems attached to different networks.
  - Example: Router J in the previous slide.
  - Includes routers (using IP layer) and bridges (using MAC layer).

Internetworking

- Modes of Operation:
  - Connectionless data transfer
    - Each PDU treated independently.
    - Without connection establishment or termination.
    - Datagram service.
  - Connection-oriented data transfer
    - Involves establishment and termination of a connection.
    - Circuit and virtual circuit connections.
  - Connection-oriented preferred for lengthy exchanges of data.

Internet Protocol (IP) Version 4

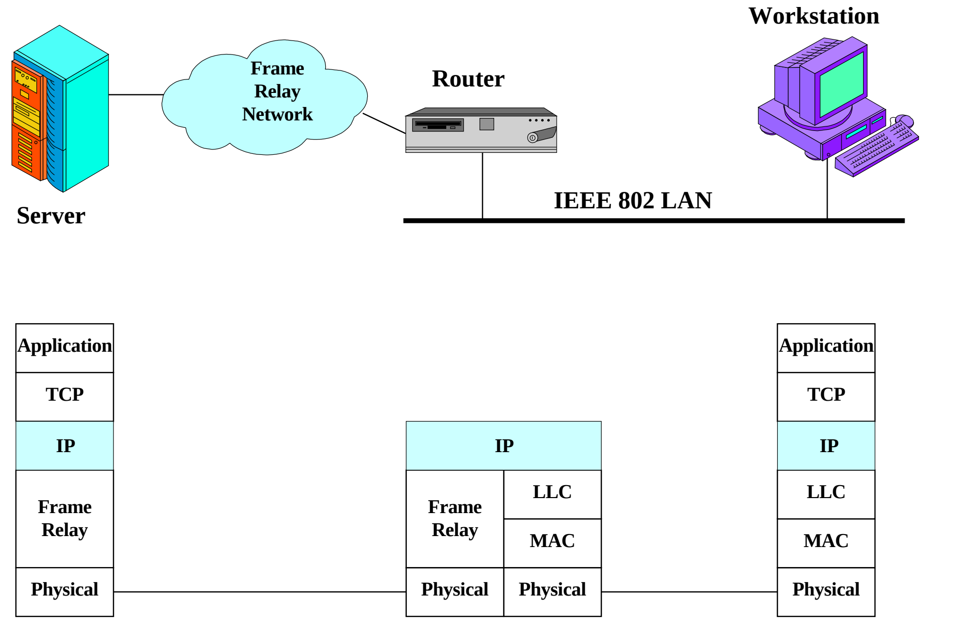
- IPv4 (RFC791) is part of the TCP/IP suite.
- Specifies interface with higher layers (e.g. TCP, UDP).
- Specifies protocol format and mechanisms.
- Will (eventually) be replaced by IPv6.
- Recall the five layers of the TCP/IP suite ⟶
- We are concerned with the Internet layer.



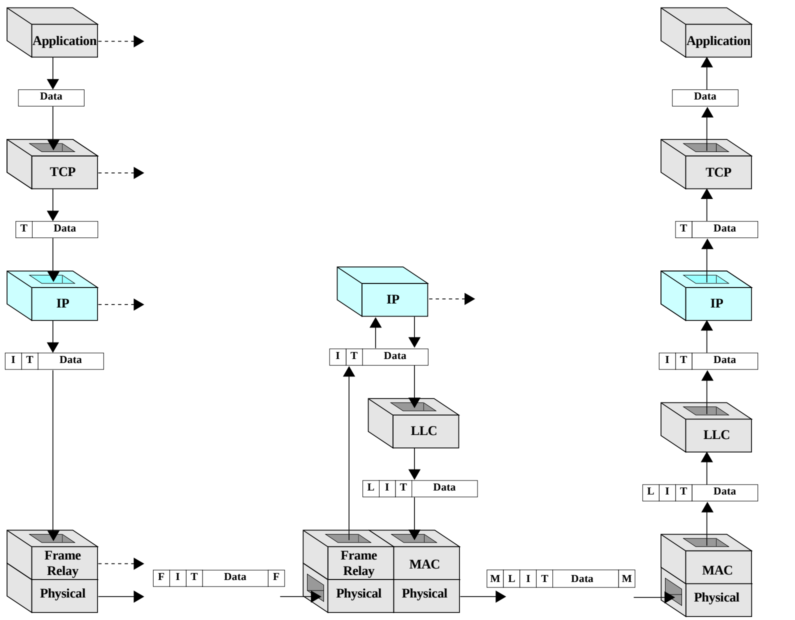
Internet Protocol

- Not all networks within the Internet are reliable.
- The transport layer should deal with reliablity issues.
- IP Operation:
  - The transport layer breaks messages into 64kbyte datagrams.
  - Datagrams delivered through Internet routers which may further fragment the datagrams.
  - Uses a best-effort connectionless service to transport datagrams over multiple paths to destination.
  - Transport layer at destination re-orders and re-assembles all datagrams.
- Two protocols in the network layer of each end system and router:
  - Upper layer: internetworking (common over the entire internet).
  - Lower layer: network access (specific to the type of network).

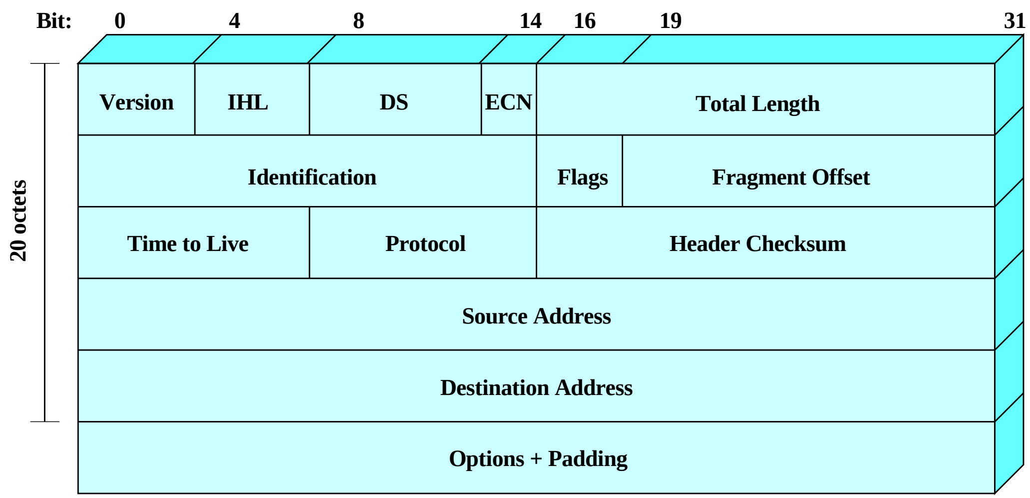
A TCP/IP Example Using Frame Relay and IEEE 802 LAN



A TCP/IP Example Using Frame Relay and IEEE 802 LAN



IPv4 Protocol Header



IHL : Internet header length.
DS : Differentiated services field.
ECN : Explicit congestion notification field.

IP Header Fields

- Version (4 bits)
  - Currently value is 4 for IPv4.
  - For IPv6 the value is 6 and the header is larger (40 octets).
- Internet header length – IHL (4 bits)
  - Multiple of 32 bit words including options.
  - Minimum value of 5 for a minimum header length of 20 octets.
- DS/ECN (8 bits) – precedence, reliability, delay, throughput
  - 6 bits (differentiated services) + 2 congestion notification
- Total length (16 bits)
  - Of the datagram (header and data), in octets.

IP Header Fields

- Identification (16 bits)
  - Sequence number.
  - Used with addresses and user protocol to identify datagram uniquely.
- Flags (3 bits) – Two are only defined.
  - More bit – indicates more datagrams to follow for defragmentation.
  - Don't fragment – If set and datagram is larger than network can handle, then the datagram is dropped. If not set, datagram can be fragmented.
- Fragment offset (13 bits) – multiples of 64 bit words.
  - Each datagram (except the last) should be multiple of 64 bits.
- Time to live (8 bits) – seconds (Each router will decrease time on its way).
- Protocol (8 bits)
  - Next higher layer to receive data field at destination e.g. TCP.

IP Header Fields

- Header checksum (16 bits)
  - Header may change at each node.
  - Re-verified and recomputed at each router.
  - 16 bit ones complement addition of all 16 bit words in header.
  - Set to zero during calculation.
- Source address (32 bits).
- Destination address (32 bits).
- Options – encodes user options (variable length) such as security labels, source routing lists, route recording, etc.
- Padding
  - To ensure the total header length is a multiple of 32 bits.

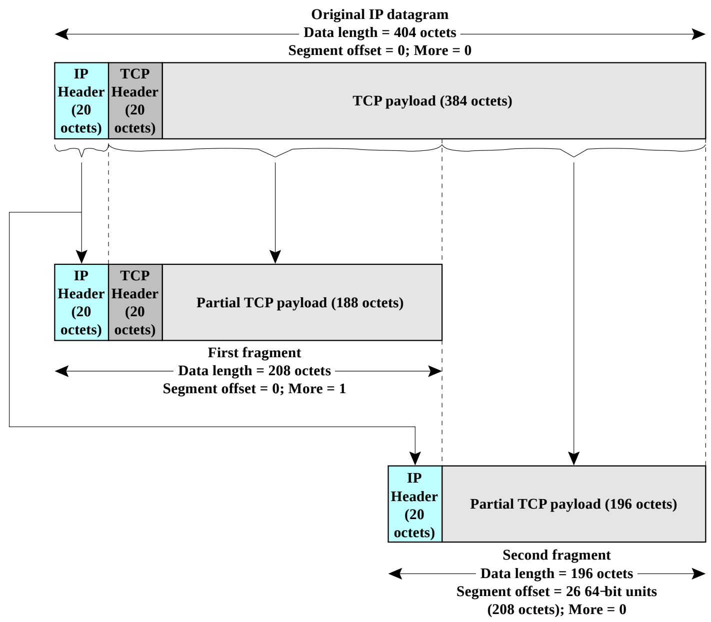
IP Data Field

- Carries user data from next layer up.
- Integer multiple of 8 bits (octet) in length.
- Max length of datagram (header plus data) 65,535 octets.
  - The total length field is 16 bits ($2^{16} - 1 = 65{,}535$).

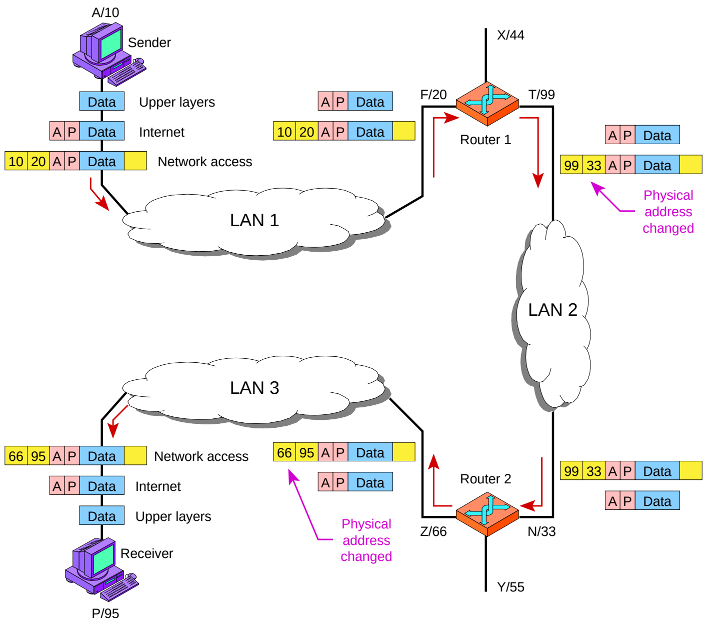
IP Fragmentation

- Different networks have different maximum packet sizes.
- Fragment larger packets – where to we re-assemble fragments?
  - Intermediate systems: need large buffers at each router and require all fragments to follow the same path through the network.
  - Destination: packets get smaller as they traverse the internet.
- IP fragmentation uses re-assembly at destination with:
  - Data unit identifier – use addresses, protocol and identification fields.
  - Data length – length of user data.
  - Fragment offset – position of fragment of user data in original datagram.
  - More flag – indicates this is not the last fragment.

IP Fragmentation Example

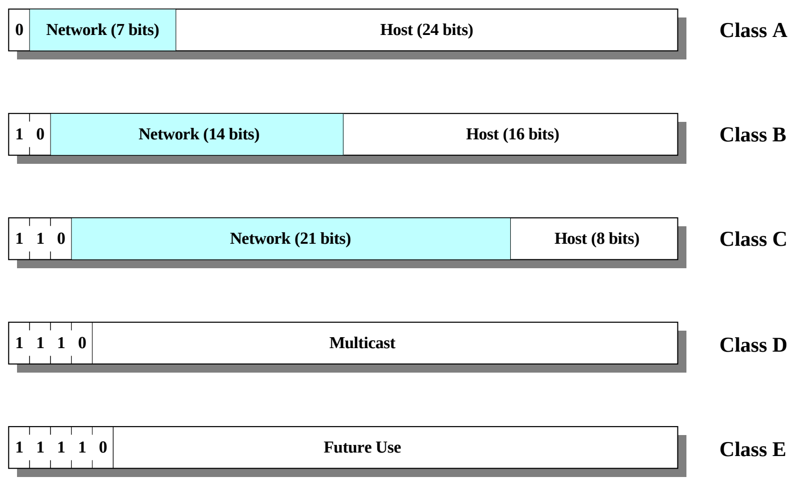


IP Address



IPv4 Address Formats

- 32-bit global address is partitioned into a network (address a subnetwork) and a host (address a host on that subnetwork) identifier.



IPv4 Addresses: Network Class A

- A few networks, each with many hosts.
- Starts with a binary 0.
- Adress with all 0 reserved.
- First octet 01111111_2 (127) reserved for loopback.
- Range 1.x.x.x to 126.x.x.x

0	**Network (7 bits)**	**Host (24 bits)**	**Class A**

IPv4 Addresses : Network Class B

- Medium number of networks each with a medium number of hosts.
- Starts with a binary 10.
- Range 128.x.x.x to 191.x.x.x
- Second Octet also included in network address:
  – 6 bits from first octet and 8 bits from second octet (6+8=14).
- 2^{14} = 16,384 class B addresses.
- For example:
  – 130.194.x.x (10000010.11000010.x.x) Monash network.
  – 130.194.11.x Monash ITS managed services.
  – 130.194.11.149 (www.monash.edu.au)

1	**0**	**Network (14 bits)**	**Host (16 bits)**	**Class B**

IPv4 Addresses : Network Class C

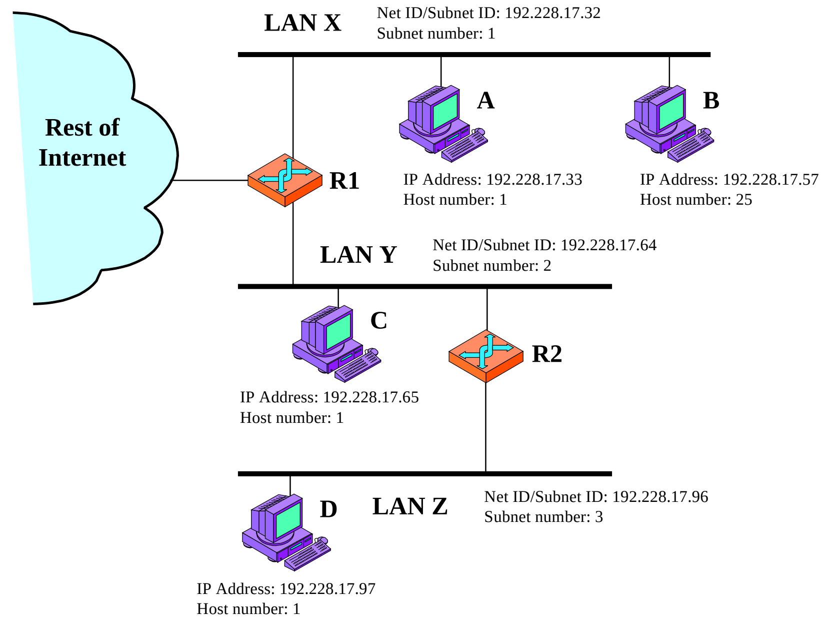
- Many networks, each with a few hosts.
- Starts with a binary 110.
- Range 192.x.x.x to 223.x.x.x
- Second and third octet also part of network address.
- 2^{21} = 2,097,152 addresses.

1	**1**	**0**	**Network (21 bits)**	**Host (8 bits)**	**Class C**

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 Subnetworking



Routing Using Subnetworking

- Uses class C address 192.228.17.x for entire network.
- Upper three bits of host are used to specify the LAN.

	Dotted Decimal	Binary Representation
IP Address	192.228.17.57	11000000.11100100.00010001.00111001
Subnet mask	255.255.255.224	11111111.11111111.11111111.11100000
Bitwise AND of above (network/subnet number)	192.228.17.57	11000000.11100100.00010001.00100000
Subnet number	1 (LAN X)	11000000.11100100.00010001.001
Host number	25 (Host B)	00000000.00000000.00000000.00011001

- Subnet mask 255.255.255.0 (class C) delivers to network, while subnet mask 255.255.255.224 delivers to a particular LAN.

Further Reading

- Stallings, W. Data and Computer Communications, Prentice Hall. Chapter 18.
- Stallings, W. Business Data Communications, Prentice Hall. Chapters 4 and 5.
- Forouzan, B. Data Communications and Networking, McGraw-Hill. Parts of Chapters 2, 19 and 20.