Network Layer - Introduction

- The role of the network layer is to move packets from a sending host to a receiving host. To do so, two important network layer functions can be identified as:
- Forwarding - When a packet arrives at a router's input link, the router must move the packet to the appropriate output link.
- Routing - The network layer must determine the route or path taken by packets as they flow from a sender to a receiver. The algorithms that calculate these paths are referred to as routing algorithms.

Network Layer - Introduction

- Packets transmitted by sending host may pass through several networks and require many hops at intermediate routers before reaching the destination host.
- Forwarding is router's local action of transferring a packet from an input link interface to the appropriate output link interface. Routing refers to the network wide process that determines the end-to-end paths that packets take from source to destination.
- Every router has a forwarding table. A router forwards a packet by examining the value of a field in the arriving packet's header, and then using this header value to index into the router's forwarding table. The value stored in the forwarding table entry for that header indicates the router's outgoing link interface to which that packet is to be forwarded.
- The values of the forwarding table are determined by routing algorithm. The routing algorithm can be centralized (e.g., executing on a central server) or decentralized (i.e., a distributed routing algorithm running in each router).
- In either case, a router receives routing protocol messages, which are used to configure its forwarding table.

The Internet Protocol (IP)

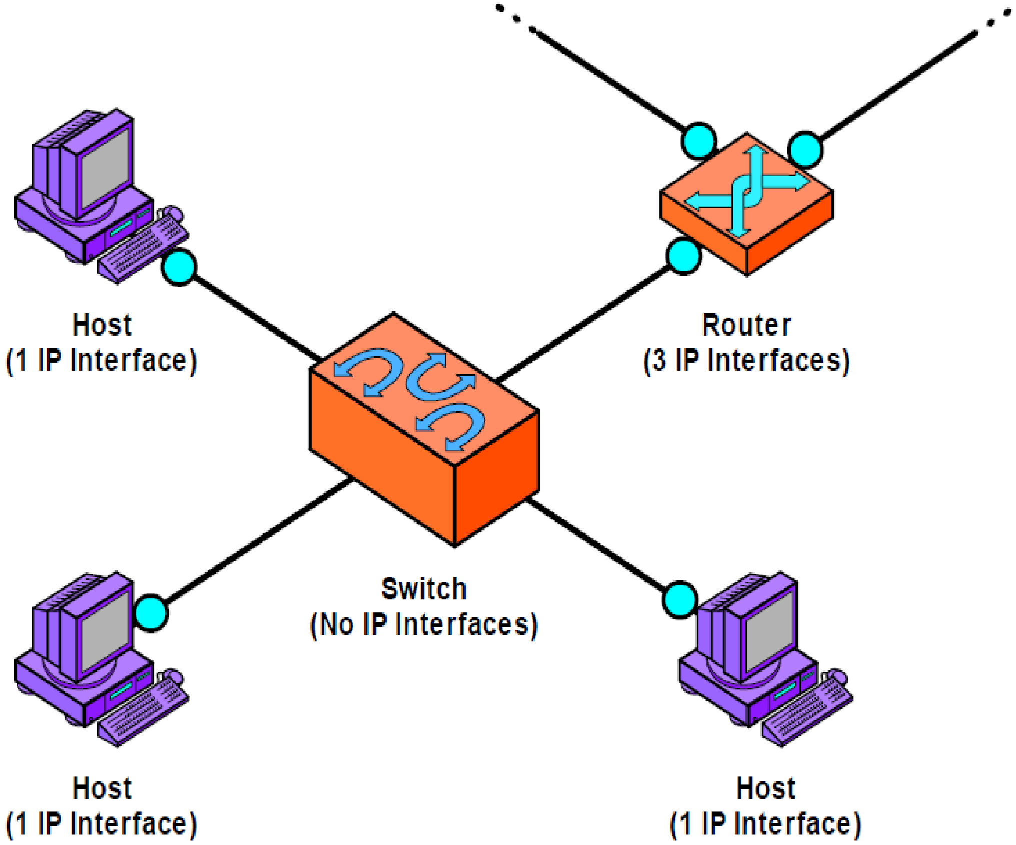
- The Internet Protocol (IP) is the core of the TCP/IP protocol suite and its main protocol at the network layer.
- IP has four basic functions:
- Addressing - In order to deliver datagrams, IP must know where to deliver them to. For this reason, IP includes a mechanism for host addressing.
- Data Encapsulation - IP accepts data from the transport layer protocols(UDP and TCP). It then encapsulates this data into an IP datagram using a special format prior to transmission.
- Fragmentation and Reassembly - IP datagrams are passed down to the data link layer for transmission on the local network. However, the maximum frame size of each data link network may be different. For this reason, IP includes the ability to fragment IP datagrams into pieces so they can each be carried on the local network. The receiving device uses the reassembly function to recreate the whole IP datagram again.
- Routing - When an IP datagram is sent to a destination on the same local network, this can be done easily using the network's underlying LAN protocol. However, when the destination is on a distant network not directly attached to the source, the datagram must be delivered by routing the datagram through intermediate devices (called routers). IP accomplishes this with support routing protocols.

IP Addressing

- IP address has following functions:
- Network Interface Identification - The IP address provides unique identification of the interface between a device and the network. This is required to ensure that the datagram is delivered to the correct recipients.
- Routing - When the source and destination of an IP datagram are not on the same network, the datagram must be delivered using intermediate nodes. The IP address is an essential part of the system used to route datagrams.

IP Addressing – What is an Interface?

- A host has only a single link into the network; when IP in the host wants to send a datagram, it does so over this link. The boundary between the host and the physical link is called an interface.
- A router's job is to receive a datagram on one link and forward the datagram on some other link, a router necessarily has two or more links to which it is connected. The boundary between the router and any one of its links is also called an interface.
- A router thus has multiple interfaces, one for each of its links.
- Because every host and router is capable of sending and receiving IP datagrams, IP requires each host and router interface to have its own IP address. Thus, an IP address is technically associated with an interface, rather than with the host or router containing that interface.

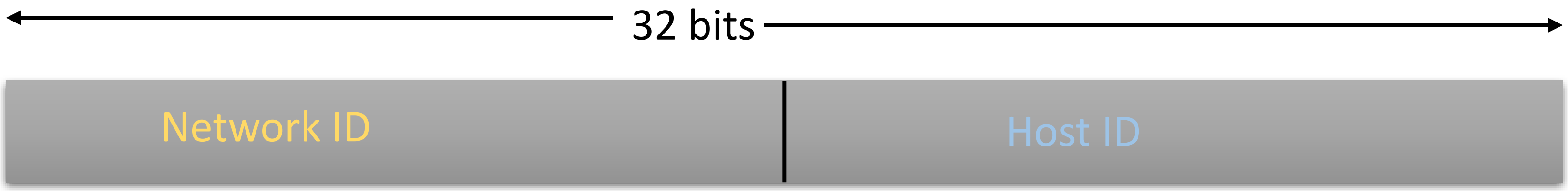


IP Addressing

- An IP address consists of 32 bits of information. These addresses are referred to as IPv4 (IP version 4) addresses.
- These addresses are unique i.e. each address defines one and only one connection to the internet.
- An IP address can be represented using one of the following methods:
  - Dotted decimal notation
  - Binary notation
  - Hexadecimal notation
- IP addresses are most commonly expressed in dotted decimal with each octet of 8 bits converted to a decimal number and the octets separated by a period (a "dot"). Each of the octets in an IP address can take on the values from 0 to 255 so the lowest value is theoretically 0.0.0.0 and the highest is 255.255.255.255.
- Since the IP address is 32 bits wide, this provides a theoretical address space of 2^{32}, or 4,294,967,296 addresses.

IP Address Structure

- The 32-bit IP address is a hierarchical address i.e. structured by network and host (two level hierarchy).



- Network Identifier (Network ID) - No. of bits, starting from the leftmost bit, used to uniquely identify a network where the host is located. Also called the network prefix. Every machine on the same network shares same network address.
- Host Identifier (Host ID) – No of bits used to uniquely identify a host on the network.
- Hierarchical addressing was chosen because, if every address were unique and flat addressing was used, all routers on the Internet would need to store the address of each and every machine on the Internet. This would make efficient routing impossible.
- Routers look at the network portion of the IP address to determine if the destination IP address is on the same network as the host IP address. Then routing decisions are made based on information the routers keep about where various networks are located. The host portion of the address is used by devices on the local portion of the network.

IP Address Classes

- IP addressing supports five different address classes: A, B, C, D, and E. Only classes A, B, and C are available for commercial use.
- Each class occupies some part of the address space.
- This architecture is called classful addressing.

	8 bits	8 bits	8 bits	8 bits
Class A	Network ID	Host ID	Host ID	Host ID
	8 bits	8 bits	8 bits	8 bits
Class B	Network ID	Network ID	Host ID	Host ID
	8 bits	8 bits	8 bits	8 bits
Class C	Network ID	Network ID	Network ID	Host ID

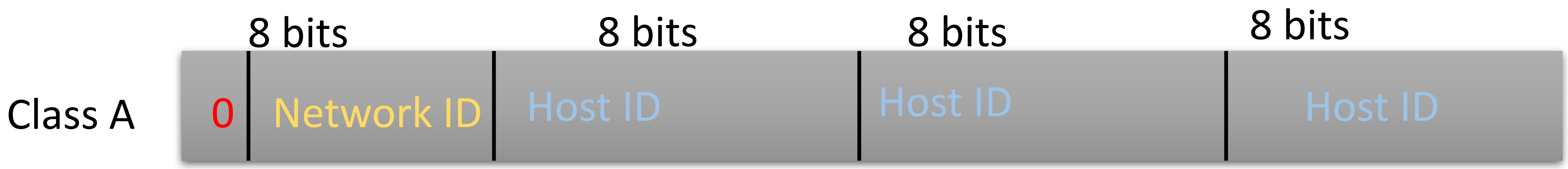
Network Address Range – Class A

- The first bit of the first byte in a Class A network address must always be off (0).
- If 0xxxxxxx then network address range will be:

  00000000 = 0

  01111111 = 127

- This means a Class A address must be between 0 and 127 in the first byte.



Class A

8 bits | 8 bits | 8 bits | 8 bits

0 | Network ID | Host ID | Host ID | Host ID

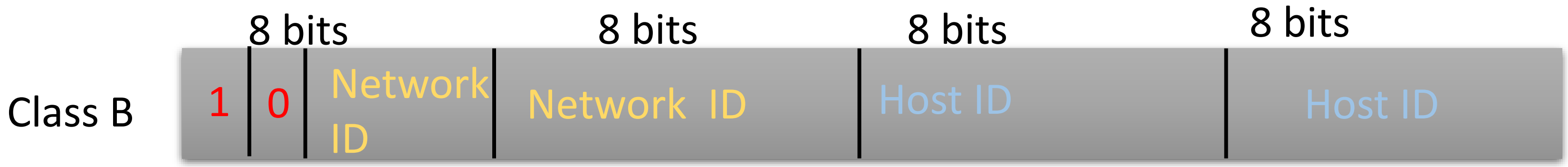
Network Address Range – Class B

- In a Class B network, the first bit of the first byte must always be turned on (1) but the second bit must always be turned off (0).
- If 10xxxxxx then network address range will be:

  10000000 = 128

  10111111 = 191

- This means a Class B network is defined when the first byte is configured from 128 to 191.



	8 bits			8 bits	8 bits	8 bits
Class B	1	0	Network ID	Network ID	Host ID	Host ID

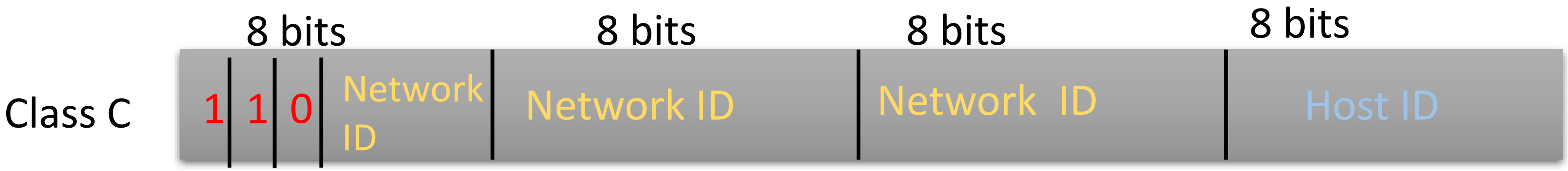
Network Address Range – Class C

- For Class C networks, the first 2 bits of the first octet are always turned on (1), but the third bit is off (0).
- If 110xxxxx then network address range will be:

  11000000 = 192

  11011111 = 223

- So, if you see an IP address that starts at 192 and goes to 223, then it is a Class C IP address.



8 bits | 8 bits | 8 bits | 8 bits

Class C | 1 | 1 | 0 | Network ID | Network ID | Network ID | Host ID

Reserved IP Addresses

- Some IP addresses are reserved for special purposes, so network administrators can't assign these addresses to nodes.

Address	Function
Network Address of all zeros (0.0.0.160)	Specified Host On This Network - This addresses a host on the current or default network.
Network Address 127.0.0.1	Reserved for loopback tests - Designates the local node and allows that node to send a test packet to itself without generating network traffic.
Node Address of all zeros (77.0.0.0)	The Specified Network - This notation, with a "0" at the end of the address, refers to an entire network.
Node Address of all ones (77.255.255.255)	All Hosts On The Specified Network - Used for broadcasting to all hosts on the local network.
Entire IP address set to all 0s (0.0.0.0)	Me - Used by a device to refer to itself when it doesn't know its own IP address. The most common use is when a device attempts to determine its address using a host configuration protocol like DHCP.
Entire IP address set to all 1s (255.255.255.255)	All Hosts On The Network - Broadcast to all nodes on the current network.

Class A Addresses

For Network ID

- 7 bits are used for Network ID as first bit is reserved as '0' for Class A.
  - ✓ No. of possible Network IDs = $2^7 - 2 = 126$ (Network address 0 and 127 are reserved and cannot be assigned to any network)

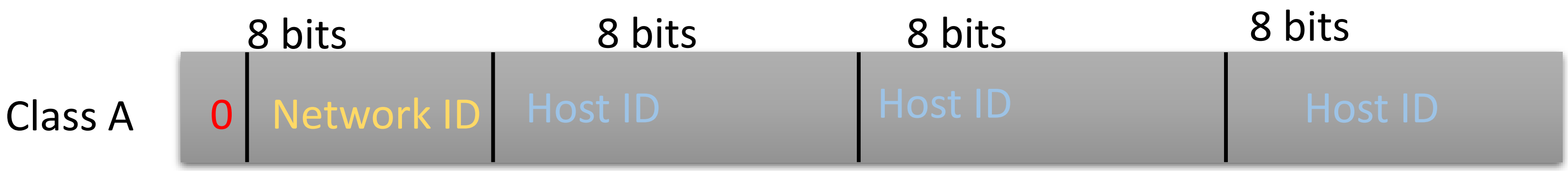
For Host ID

- 24 bits are used for Host ID
  - ✓ No of Host IDs per network ID = $2^{24} - 2 = 16,777,214$ (Host address of all 0's and all 1's is reserved)

E.g. All Host ID bits off is a network address 10.0.0.0

All Host ID bits on is a broadcast address 10.255.255.255

- Valid Host IDs are numbers between the network address and broadcast address i.e. 10.0.0.1 through 10.255.255.254



	8 bits	8 bits	8 bits	8 bits
Class A	0 Network ID	Host ID	Host ID	Host ID

Class B Addresses

For Network ID

- 14 bits are used for Network ID as first two bits are reserved as ‘10’ for Class B.
  - ✓ No. of possible Network IDs = $2^{14} = 16{,}384$

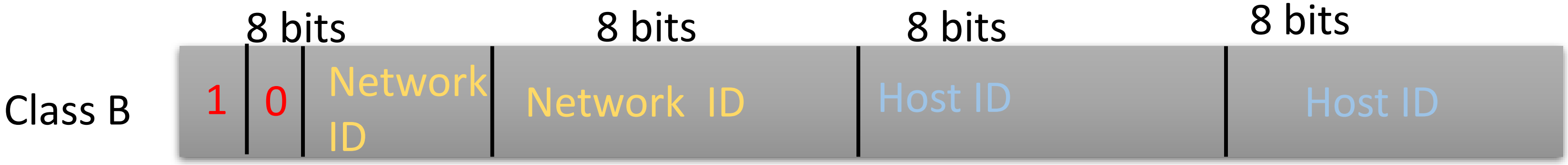
For Host ID

- 16 bits are used for Host ID
  - ✓ No of Host IDs per network ID = $2^{16} - 2 = 65{,}534$ (Host address of all 0’s and all 1’s is reserved)

E.g. All Host ID bits off is a network address 172.16.0.0

All Host ID bits on is a broadcast address 172.16.255.255

- Valid Host IDs are numbers between the network address and broadcast address i.e. 172.16.0.1 through 172.16.255.254



Class C Addresses

For Network ID

- 21 bits are used for Network ID as first three bits are reserved as ‘110’ for Class C.
  - ✓ No. of possible Network IDs = $2^{21} = 2{,}097{,}152$

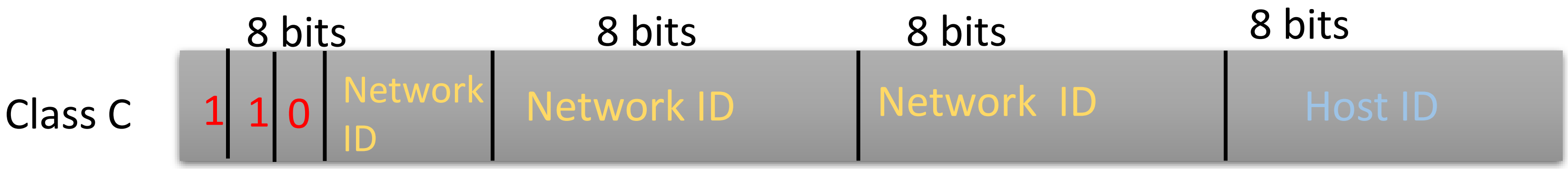
For Host ID

- 8 bits are used for Host ID
  - ✓ No of Host IDs per network ID = $2^8 - 2 = 254$ (Host address of all 0’s and all 1’s is reserved)

E.g. All Host ID bits off is a network address 192.168.100.0

All Host ID bits on is a broadcast address 192.168.100.255

- Valid Host IDs are numbers between the network address and broadcast address i.e. 192.168.100.1 through 192.168.100.254



Private IP Addresses

- Private IP addresses can be used on a private network, but they are not routable through the Internet.
- If every host on every network had to have real routable IP addresses then we would have run out of IP addresses.
- But by using private IP addresses, ISPs, corporations, and home users only need a relatively tiny group of IP addresses to connect their networks to the Internet. They can use private IP addresses on their inside networks and get along just fine.
- To accomplish this task, the ISP and the corporation use Network Address Translation (NAT), which basically takes a private IP address and converts it for use on the Internet.

Address Class	**Reserved Address Space**
Class A	10.0.0.0 through 10.255.255.255
Class B	172.16.0.0 through 172.31.255.255
Class C	192.168.0.0 through 192.168.255.255

IP Addresses Configuration

- There are two basic ways that IP addresses can be configured.
- Static configuration - each device is manually configured with an IP address that doesn't change. This is fine for small networks but becomes an administrative nightmare in larger networks when changes are required.
- Dynamic configuration - IP addresses are assigned to devices and changed under software control.

Dynamic Host Configuration Protocol

- DHCP allows a host to obtain an IP address automatically from a shared pool of IP addresses managed by DHCP server.
- A network administrator can configure DHCP so that a given host receives the same IP address each time it connects to the network (automatic allocation), or a host may be assigned a temporary IP address that will be different each time the host connects to the network(dynamic allocation).
- In addition to host IP address assignment, DHCP also allows a host to learn additional information, such as:
  - subnet mask,
  - the address of its first hop router (default gateway), and
  - the address of its local DNS server.
- DHCP is a client server protocol. A DHCP server is a network device that has been programmed to provide DHCP services to clients. They manage address information and other parameters and respond to client configuration requests. A DHCP client is any device that sends DHCP requests to a server to obtain an IP address or other configuration information.

Dynamic Host Configuration Protocol

- For a newly arriving host, the DHCP protocol is a four step process. The four steps are:
- DHCP server discovery - The first task of a newly arriving host is to find a DHCP server with which to interact. This is done using a DHCP discover message. The DHCP client creates an IP datagram containing its DHCP discover message along with the broadcast destination IP address of 255.255.255.255 and a "this host" source IP address of 0.0.0.0. The DHCP client passes the IP datagram to the link layer, which then broadcasts this frame to all nodes attached to the subnet.
- DHCP server offer - A DHCP server receiving a DHCP discover message responds to the client with a DHCP offer message that is broadcast to all nodes on the subnet, again using the IP broadcast address of 255.255.255.255. Each server offer message contains the transaction ID of the received discover message, the proposed IP address for the client, the network mask, and an IP address lease time which is the amount of time for which the IP address will be valid.
- DHCP request - The newly arriving client will choose from among one or more server offers and respond to its selected offer with a DHCP request message, echoing back the configuration parameters.
- DHCP ACK - The server responds to the DHCP request message with a DHCP ACK message, confirming the requested parameters.
- Once the client receives the DHCP ACK, the interaction is complete and the client can use the DHCP allocated IP address for the lease duration. DHCP also provides a mechanism that allows a client to renew its lease on an IP address in case of lease expiration.