3. TCP/IP ADDRESSING

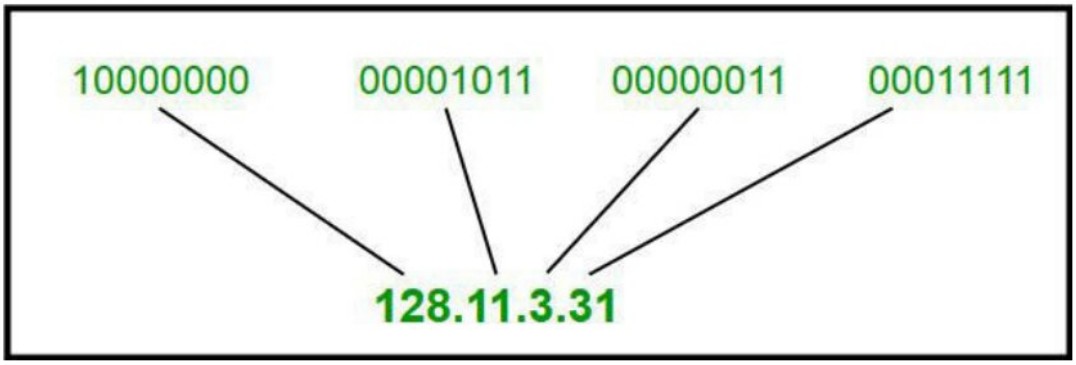
3.1 Learning Objectives

- To know about IP addressing
- Elaborate classful and classless addressing
- Discuss subnetting and supernetting
- Know about IPV4 and IPV6 header formats
- Elaborate comparison between them

3.2 IP Addressing

IP address is an address having information about how to reach a specific host, especially outside the LAN. An IP address is a 32 bit unique address having an address space of 2^{32}.
Generally, there are two notations in which IP address is written, dotted decimal notation and hexadecimal notation.

Dotted Decimal Notation



Hexadecimal Notation

Scanned with CamScanner

Some points to be noted about dotted decimal notation :
1. The value of any segment (byte) is between 0 and 255 (both included).
2. There are no zeroes preceding the value in any segment (054 is wrong, 54 is correct).

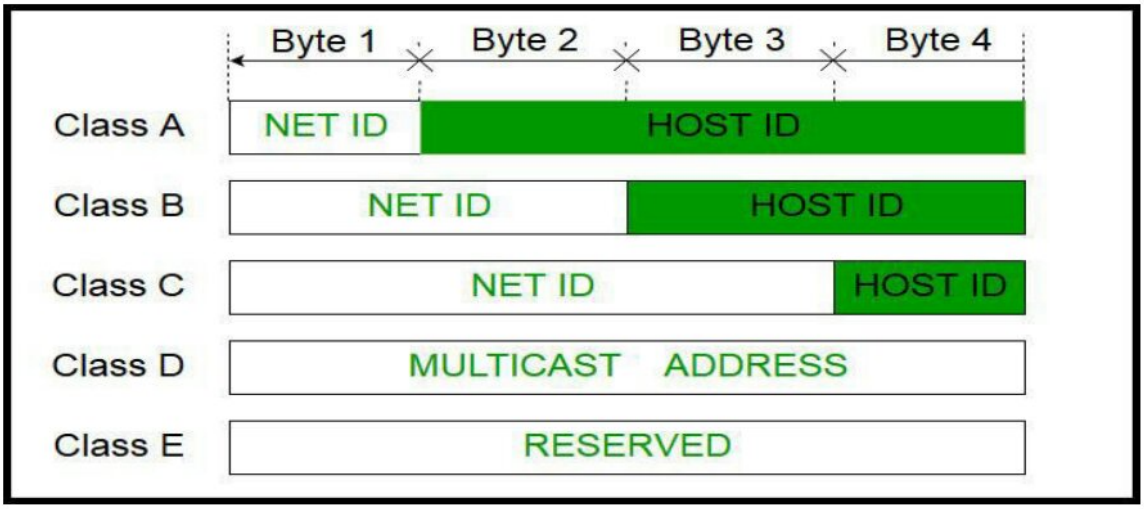
3.2.1 Classful Addressing
The 32 bit IP address is divided into five sub-classes. These are:

- Class A
- Class B
- Class C
- Class D
- Class E

Each of these classes has a valid range of IP addresses. Classes D and E are reserved for multicast and experimental purposes respectively. The order of bits in the first octet determine the classes of IP address.
IPv4 address is divided into two parts:

- Network ID
- Host ID

The class of IP address is used to determine the bits used for network ID and host ID and the number of total networks and hosts possible in that particular class. Each ISP or network administrator assigns IP address to each device that is connected to its network.



Note: IP addresses are globally managed by Internet Assigned Numbers Authority(IANA) and regional Internet registries(RIR).

Scanned with CamScanner

Note: While finding the total number of host IP addresses, 2 IP addresses are not counted and are therefore, decreased from the total count because the first IP address of any network is the network number and whereas the last IP address is reserved for broadcast IP.

Class A:

IP address belonging to class A are assigned to the networks that contain a large number of hosts.

- The network ID is 8 bits long.
- The host ID is 24 bits long.

The higher order bit of the first octet in class A is always set to 0. The remaining 7 bits in first octet are used to determine network ID. The 24 bits of host ID are used to determine the host in any network. The default sub-net mask for class A is 255.x.x.x. Therefore, class A has a total of:

- 2^7= 128 network ID
- 2^24 – 2 = 16,777,214 host ID

IP addresses belonging to class A ranges from 1.x.x.x – 126.x.x.x

Class B:

IP address belonging to class B are assigned to the networks that ranges from medium-sized to large-sized networks.

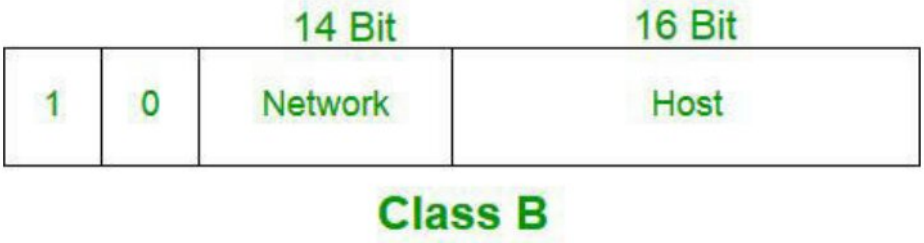
- The network ID is 16 bits long.
- The host ID is 16 bits long.

The higher order bits of the first octet of IP addresses of class B are always set to 10. The remaining 14 bits are used to determine network ID. The 16 bits of host ID is used to determine the host in any network. The default sub-net mask for class B is 255.255.x.x. Class B has a total of:

- 2^14 = 16384 network address
- 2^16 – 2 = 65534 host address

IP addresses belonging to class B ranges from 128.0.x.x – 191.255.x.x.

Scanned with CamScanner



Class C:

IP address belonging to class C are assigned to small-sized networks.

- The network ID is 24 bits long.
- The host ID is 8 bits long.

The higher order bits of the first octet of IP addresses of class C are always set to 110. The remaining 21 bits are used to determine network ID. The 8 bits of host ID is used to determine the host in any network. The default sub-net mask for class C is 255.255.255.x. Class C has a total of:

- 2^21 = 2097152 network address
- 2^8 – 2 = 254 host address

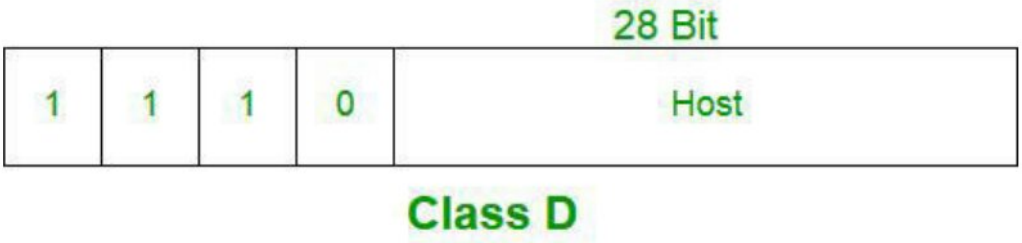
IP addresses belonging to class C ranges from 192.0.0.x – 223.255.255.x.

Class D:

IP address belonging to class D are reserved for multi-casting. The higher order bits of the first octet of IP addresses belonging to class D are always set to 1110. The remaining bits are for the address that interested hosts recognize.

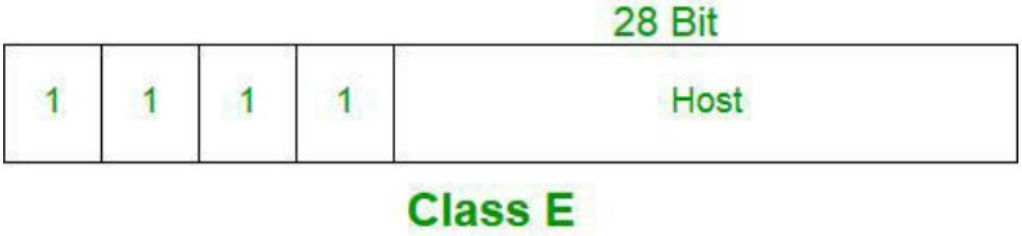
Class D does not posses any sub-net mask. IP addresses belonging to class D ranges from 224.0.0.0 – 239.255.255.255.

Scanned with CamScanner



Class E:

IP addresses belonging to class E are reserved for experimental and research purposes. IP addresses of class E ranges from 240.0.0.0 – 255.255.255.254. This class doesn't have any sub-net mask. The higher order bits of first octet of class E are always set to 1111.



Range of special IP addresses:

169.254.0.0 – 169.254.0.16 : Link local addresses
127.0.0.0 – 127.0.0.8 : Loop-back addresses
0.0.0.0 – 0.0.0.8 : used to communicate within the current network.

Summary of Classful addressing :

Scanned with CamScanner

CLASS	LEADING BITS	NET ID BITS	HOST ID BITS	NO. OF NETWORKS	ADDRESSES PER NETWORK	START ADDRESS	END ADDRESS
CLASS A	0	8	24	2^7 (128)	2^{24} (16,777,216)	0.0.0.0	127.255.255.255
CLASS B	10	16	16	2^{14} (16,384)	2^{16} (65,536)	128.0.0.0	191.255.255.255
CLASS C	110	24	8	2^{21} (2,097,152)	2^8 (256)	192.0.0.0	223.255.255.255
CLASS D	1110	NOT DEFINED	NOT DEFINED	NOT DEFINED	NOT DEFINED	224.0.0.0	239.255.255.255
CLASS E	1111	NOT DEFINED	NOT DEFINED	NOT DEFINED	NOT DEFINED	240.0.0.0	255.255.255.255

Problems with Classful Addressing:

The problem with this classful addressing method is that millions of class A address are wasted, many of the class B address are wasted, whereas, number of addresses available in class C is so small that it cannot cater the needs of organizations. Class D addresses are used for multicast routing, and are therefore available as a single block only. Class E addresses are reserved.

Since there are these problems, Classful networking was replaced by Classless Inter-Domain Routing (CIDR) in 1993

3.2.3 Classless Addressing

To reduce the wastage of IP addresses in a block, we use sub-netting. What we do is that we use host id bits as net id bits of a classful IP address. We give the IP address and define the number of bits for mask along with it (usually followed by a '/' symbol), like, 192.168.1.1/28. Here, subnet mask is found by putting the given number of bits out of 32 as 1, like, in the given address, we need to put 28 out of 32 bits as 1 and the rest as 0, and so, the subnet mask would be 255.255.255.240.

3.3. Subnetting

Subnetting: Dividing a large block of addresses into several contiguous sub-blocks and

Scanned with CamScanner

assigning these sub-blocks to different smaller networks is called subnetting. It is a practice that is widely used when classless addressing is done.

3.4 Supernetting

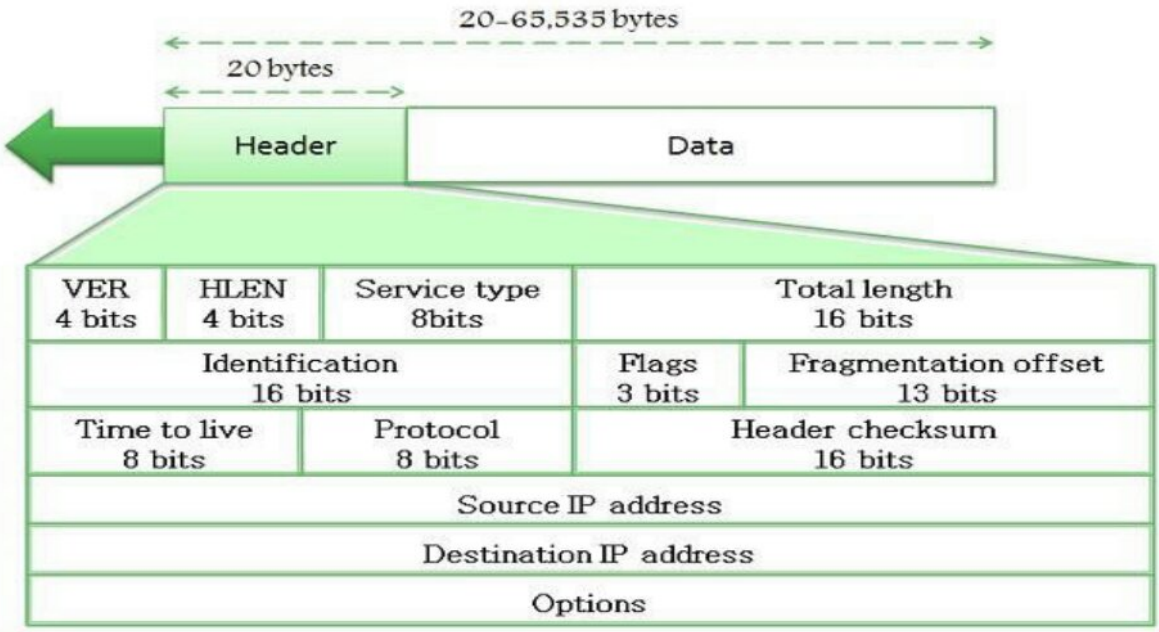
Supernetting is the opposite of Subnetting. In subnetting, a single big network is divided into multiple smaller subnetworks. In Supernetting, multiple networks are combined into a bigger network termed as a Supernetwork or Supernet.

Supernetting is mainly used in Route Summarization, where routes to multiple networks with similar network prefixes are combined into a single routing entry, with the routing entry pointing to a Super network, encompassing all the networks. This in turn significantly reduces the size of routing tables and also the size of routing updates exchanged by routing protocols.

More specifically,

- When multiple networks are combined to form a bigger network, it is termed as super-netting
- Super netting is used in route aggregation to reduce the size of routing tables and routing table updates

3.5 IPV4 Header Format



Base Header

Scanned with CamScanner

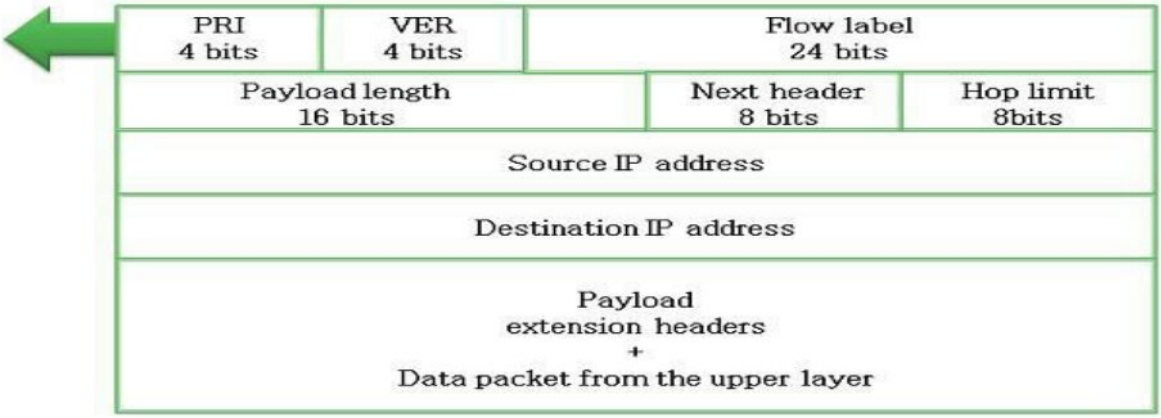
Version: It defines the version number of IP, i.e., in this case, it is 4 with a binary value of 0100.
Header length (HLEN): It represents the length of the header in multiple of four bytes.
Service type: It determines how datagram should be handled and includes individual bits such as level of throughput, reliability, and delay.
Total length: It signifies the entire length of the IP datagram.
Identification: This field is used in fragmentation. A datagram is divided when it passes through different networks to match the network frame size. At that time each fragment is determined with a sequence number in this field.
Flags: The bits in the flags field handles fragmentation and identifies the first, middle or last fragment, etc.

Fragmentation offset: It's a pointer that represents the offset of the data in the original datagram.
Time to live: It defines the number of hops a datagram can travel before it is rejected. In simple words, it specifies the duration for which a datagram remains on the internet.
Protocol: The protocol field specifies which upper layer protocol data are encapsulated in the datagram (TCP, UDP, ICMP, etc.).
Header checksum: This is a 16-bit field confirm the integrity of the header values, not the rest of the packet.
Source address: It's a four-byte internet address which identifies the source of the datagram.
Destination address: This is a 4-byte field which identifies the final destination.
Options: This provides more functionality to the IP datagram. Furthermore can carry fields like control routing, timing, management, and alignment.
IPv4 is a two-level address structure (net id and host id) classified into five categories (A, B, C, D, and E).

3.6 IPV6 Header Format

An IPv6 address is a 128-bit binary value, which can be displayed as 32 hexadecimal digits.

Format of an IPv6 datagram



Base Header

Version: This four-bit field specifies the version of the IP, i.e., 6 in this case.
Priority: It defines the priority of the packet concerning traffic congestion.

Scanned with CamScanner

Flow label: The reason for designing this protocol is to facilitate with special controlling for a certain flow of data.
Payload length: It defines the total length of the IP datagram excepting the base header.

Next header: It's an eight-bit field describe the header that trails the base header in the datagram. The next header is one of the optional extension headers which IP uses or the header for an upper layer protocol such as UDP or TCP.
Hop limit: This eight-bit hop limit field assists with the same functions at the TTL field in IPv4.
Source address: It is a 16 bytes internet address identifies the source of the datagram.
Destination address: This is 16-byte internet address that generally describes the final destination of the datagram.

3.7 Comparison Between IPV4 and IPV6

BASIS OF COMPARISON	IPV4	IPV6
Address Configuration	Supports Manual and DHCP configuration.	Supports Auto-configuration anc renumbering
End-to-end connection integrity	Unachievable	Achievable
Address Space	It can generate 4.29 x 10^9 addresses.	It can produce quite a large num addresses, i.e., 3.4 x 10^{38}.
Security features	Security is dependent on application	IPSEC is inbuilt in the IPv6 prot
Address length	32 bits (4 bytes)	128 bits (16 bytes)
Address Representation	In decimal	In hexadecimal

Scanned with CamScanner

Fragmentation performed by	Sender and forwarding routers	Only by the sender
Packet flow identification	Not available	Available and uses flow label field in the header
Checksum Field	Available	Not available
Message Transmission Scheme	Broadcasting	Multicasting and Anycasting
Encryption and Authentication	Not Provided	Provided

VERY SHORT QUESTIONS

1. Define IP address.
2. Masking is used in subnetting(T/F)?
3. Name the five class of classfull addressing?
4. Mention the range of addresses included in each class of IP address?
5. What is the full form of IPV4 and IPV6?
6. Which address is used for loop back test?
7. What is TCP/IP

SHORT QUESTIONS

1. Explain the various types of ip address?
2. What is subnetting?
3. What is supernetting?

Scanned with CamScanner

4. Draw the table for various address class of IP address?
5. What is the disadvantage of classful addressing and why classless addressing was opted?

LONG QUESTION

1. Explain IPV4 Header format?
2. Explain IPV6 header format?
3. Compare IPV4 and IPV6 header format?
4. Explain IP addressing in detail?

Scanned with CamScanner