* LOAD SDEDDING:

- **Load shedding** is a way that when routers are being inundated by packets that they cannot handle, they just throw them away.
- When buffer becomes full routers simply discard packets.
- Which packet to discard may depend on the applications running.
- Example:

  -For file transfer, an old packet is worth more than a new one. We cannot discard older packets since this will cause a gap in received data

  -For real time voice or video it is probably better to throw away old data and keep new packets.
- Co-operation from the sender is required while discarding the packets.
- For many applications, some packets are more important than others.
- An example is packets that carry routing information. These packets are more important than regular data packets because they establish routes; if they are lost, the network may lose connectivity.
- So the application itself has to mark packets with priority.
- To implement an intelligent discarding policy, application must mark their packets in priority to indicate how important they are.

RANDOM EARLY DETECTION:

- This is an approach in which the router discards one or more packets before the buffer becomes completely full.
- To determine when to start discarding, routers maintain a running average of their queue length.
- Each time a packet arrives, the RED algorithm computes the average queue length.
- If the average queue length on some link is lower than threshold, the link is said to be with minimal congestion or non-existent and the packets are queued.
- If the average queue length on some link exceeds a threshold, the link is said to be congested and a small fraction of the packets are dropped at random.

- If the average queue length is between the two thresholds, this might indicate the onset of congestion. The probability of congestion is then calculated.
- In this way the buffer is prevented from getting full by discarding packets and congestion is prevented.
- The ideal number of packets to drop depends on how many senders need to be notified of congestion.
- ECN is the preferred option if it is available. It works in exactly the same manner, but delivers a congestion signal explicitly rather than as a loss; RED is used when hosts cannot receive explicit signals.

IP ADDRESSES

- An IP address is numeric identifier assigned to each machine on an IP network.
- An IP address is made up of 32 bits of information.
- These bits are divided into four parts containing 8 bits each.
- There are three methods for representing an IP address:
    1. Dotted decimal: 131.57.30.58
    2. Binary: 10000010.00111001.00011110.00111000
    3. Hexadecimal:8B.39.C2.43
- Every host and router on the Internet has an IP address that can be used in the Source address and Destination address fields of IP packets.
- It is important to note that an IP address does not actually refer to a host.
- It really refers to a network interface, so if a host is on two networks, it must have two IP addresses.
- Most hosts are on one network and thus have one IP address.
- In contrast, routers have multiple interfaces and thus multiple IP addresses.

* Classful and Special Addressing:

- The 32 bit IP address is a structured or hierarchical address.

- The key advantage of prefixes is that routers can forward packets based on only the network portion of the address, as long as each of the networks has a unique address block.
- The host portion does not matter to the routers because all hosts on the same network will be sent in the same direction.

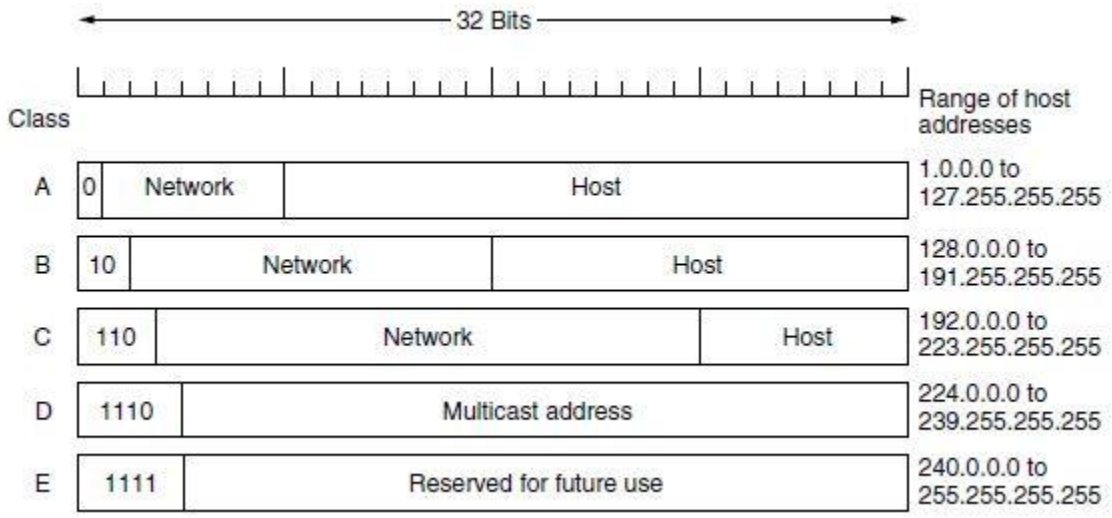


Fig: IP address formats.

- **Class A:**

Number of bits for network id	- 8 bits
Number of bits for host id	- 24 bits
Prefix	- 0(1 bit)
Number of IP addresses	- 2^31 bits (as 1 bit is prefix)
Number of networks	- 2^7 -2 (as 1 bit is prefix)
Number of hosts	- 2^24-2
Range	- 1 to 127
Default Subnet mask	-255.0.0.0 [representing network id bits with 1's and host id bits with 0's. For a class A it is 11111111.00000000.00000000.00000000 (as network id is 8 bits and host id is 24 bits)]

- **Class B:**

Number of bits for network id	- 16 bits
Number of bits for host id	-16 bits
Prefix	-10(2 bits)
Number of IP addresses	-2^30 bits (as 2 bits are prefix)
Number of networks	- 2^14 (as 2 bits are prefix)
Number of hosts	-2^16-2
Range	-128 to 191
Default Subnet mask	-255.255.255.0 [representing network id bits with 1's and host id bits with 0's. For a class B-11111111.11111111.00000000.00000000 (as network id is 16 bits and host id is 16 bits)]

- **Class C:**

Number of bits for network id	- 24 bits
Number of bits for host id	- 8 bits
Prefix	-110(3 bits)
Number of IP addresses	-2^29 bits (as 3 bits are prefix)
Number of networks	- 2^21 (as 3 bits are prefix)
Number of hosts	-2^8-2
Range	- 192 to 223
Default Subnet mask	-255.255.255.0 [representing network id bits with 1's and host id bits with 0's. For a class C-11111111.11111111.11111111.00000000 (as network id is 24 bits and host id is 8 bits)]

- **Class D:**

Prefix	-1110(4 bits)
Number of IP addresses	-2^28 bits (as 4 bits are prefix)
Range	- 224 to 239

- **Class E:**

Prefix	-1111(4 bits)
Number of IP addresses	-2^28 bits (as 4 bits are prefix)
Range	- 240 to 255

- IP address can be identified by the range of each class.

- **Example:** Find the class of the following address

  (Q1) 1.22.200.10

  Solution: Class A IP Address

  (Q2) 241.240.200.2

  Solution: Class E IP Address

  (Q3) 180.170.0.2

  Solution: Class B IP Address

- **Example:** Find the network id and host id

  (a) 19.34.21.5

  - Network id - 19 Host id - 34.21.5

  (b) 246.3.4.10

  - No network id and host id as 246.3.4.10 belongs to class E address.

  (c) 201.2.4.2

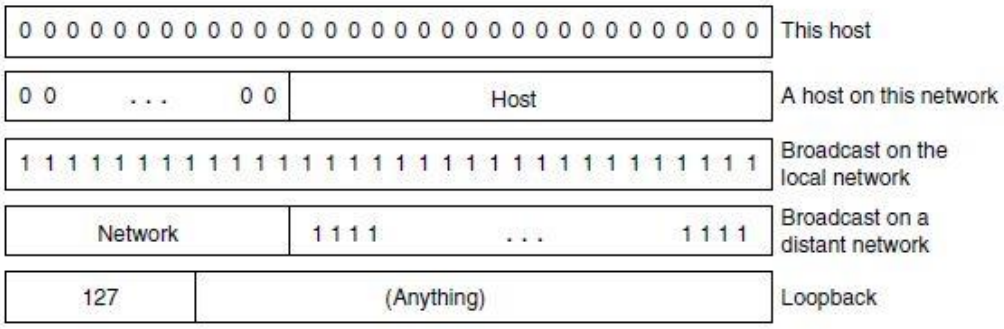
  - Network id – 201.2.4 Host id - 2

- **Special address:**

  -Network address of all 0's.

  -Network address of all 1's.

  -Network 127



* Subnetting:

- Network numbers are managed by a nonprofit corporation called **ICANN** (**Internet Corporation for Assigned Names and Numbers**), to avoid conflicts.
- In turn, ICANN has delegated parts of the address space to various regional authorities, which dole out IP addresses to ISPs and other companies.
- This is the process by which a company is allocated a block of IP addresses.
- **Subnetting** is the practice of dividing a network into two or more smaller networks.
- Small networks are known as subnets.
- Benefits of subnetting:
    1. Easily maintained
    2. security
    3. Reduce network traffic
- **Subnet mask:**

  A **Subnet mask** is a 32-bit number that **masks** an IP address, and divides the IP address into network address and host address. **Subnet Mask** is made by setting network bits to all "1"s and setting host bits to all "0"s.
- **How to divide a network into subnets , find the range of subnet, subnet mask**

  [Present in pdf]

Example:

(Q) Find the subnet address for the following

Solution:

IP Address: 140.11.36.22

Mask: 255.255.255.0

Step1: Convert the IP address and mask into binary

Step 2: Then perform the AND operation and convert it into decimal

IP Address: 10001100.00001011.00100100.00010110

Mask: 11111111.11111111.11111111.00000000

Performing AND operation the value is:

10001100.00001011.00100100.00000000=140.11.36.0 is the sub network address.

* CIDR—Classless Inter Domain Routing:

- Blocks of IP addresses are allocated so that the addresses are used efficiently.
- CIDR IP addresses can be described as consisting of two groups of bits.
- The most significant group of bits denotes the prefix i.e., a network address that is used for the identification of a network or sub-network.
- The least significant group of bits is known as host identifier that determines the total number of bits in the address.
- CIDR **notation**

  a.b.c.d/n

- **Rules for forming CIDR Blocks:**
  1. All IP addresses must be contiguous.
  2. Block size must be the power of 2 (2^n).
- **For example**, a CIDR block is shown below

  192.168.1.0/28

  -Here /28 signifies the total number of 1's bits in the routing mask (network mask).

  -This IP address can be shown as below in the binary format:

  11111111.11111111.11111111.11110000

  Here the first 28 bits are marked as 1.

  -It would be equivalent to a network mask of 255.255.255.240

  -Now for finding the subnetwork address of 192.168.1.10/28

  - We have perform AND operation for subnet mask and the given address

11111111.11111111.11111111.11110000

11000000.10101000.00000001.00001010

Performing AND operation the value is:

11100000.10101000.00000001.00000000=192.168.1.0 is the sub network address.

* NAT:

- NAT stands for "Network Address Translation."
- To access the Internet, one public IP address is needed, but we can use a private IP address in our private network.
- The idea of NAT is to allow multiple devices to access the Internet through a single public address.
- To achieve this, the translation of private IP address to a public IP address is required.
- **Network Address Translation (NAT)** is a process in which one or more local IP address is translated into one or more Global IP address and vice versa in order to provide Internet access to the local hosts.
- Also, it does the translation of port numbers i.e. masks the port number of the host with another port number, in the packet that will be routed to the destination.
- It then makes the corresponding entries of IP address and port number in the NAT table. NAT generally operates on router or firewall.