Back To Course

LIVE BATCHES

Learn

Classroom

Theory

Quiz

Learn Quiz Filter

We have combined Classroom and Theory tab and created a new Learn tab for easy access. You can access Classroom and Theory from the left panel.

Network Layer

Network layer works for the transmission of data from one host to the other located in different networks. It also takes care of packet routing i.e. selection of the shortest path to transmit the packet, from the number of routes available. The sender & receiver's IP address are placed in the header by the network layer.

The functions of the Network layer are:

1. **Routing:** The network layer protocols determine which route is suitable from source to destination. This function of network layer is known as routing.
2. **Logical Addressing:** In order to identify each device on internetwork uniquely, network layer defines an addressing scheme. The sender & receiver's IP address are placed in the header by network layer. Such an address distinguishes each device uniquely and universally.

* *Segment* in Network layer is referred as **Packet**.

** Network layer is implemented by net devices such as routers.

Let's look at some primary needs of the Network layer and why it is so important to implement:

1. **Internetworking:** Made possible using Routers. This can be across various types like 802.11, 3G, Ethernet etc

2. **Addressing:** This involves processing of IP Adresses

3. **Routing and Forwarding:** A routing table is maintained by the routers to decide how a packet must be transmitted globally to its specific IP addresses. This process does the global connection is called routing. Forwarding is more of a local concept instead of global.

4. **Scalability (Using hierarchy in Networks):** This refers to the hierarchial organisation of packets.

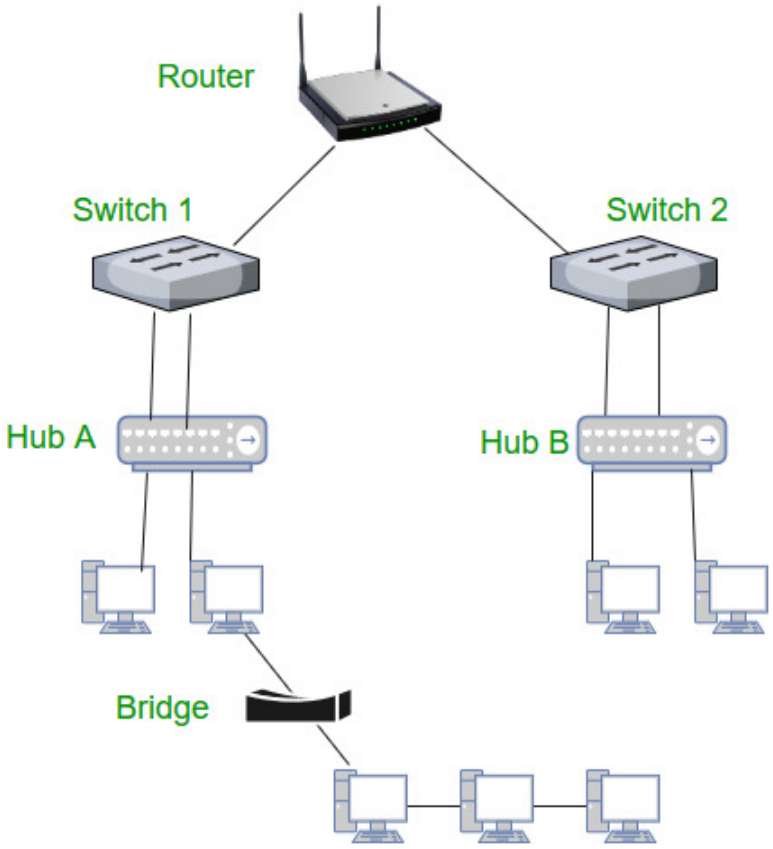
5. **Bandwidth Control:** There must be a good utilisation of Bandwidth.

6. **Fragmentation and Re-assembly:** Division of bigger packets into multiple small packets and rearranging them to get the original packet is called Fragmentation and Re-assembly respectively.

Before understanding the working at the Networking layer, let's get familiar with a few technical devices that has a great role to play in this system:

1. **Switch** - A switch is a multiport bridge with a buffer and a design that can boost its efficiency(a large number of ports imply less traffic) and performance. The switch is a data link layer device. The switch can perform error checking before forwarding data, that makes it very efficient as it does not forward packets that have errors and forward good packets selectively to correct port only. In other words, switch divides collision domain of hosts, but broadcast domain remains the same.

2. **Routers** - A router is a device like a switch that routes data packets based on their IP addresses. The router is mainly a Network Layer device. Routers normally connect LANs and WANs together and have a dynamically updating routing table based on which they make decisions on routing the data packets. Router divide broadcast domains of hosts connected through it.



3. **Brouter** - It is also known as the bridging router is a device which combines features of both bridge and router. It can work either at the data link layer or a network layer. Working as a router, it is capable of routing packets across networks and working as a bridge, it is capable of filtering local area network traffic.

4. **Repeater** - A repeater operates at the physical layer. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted so as to extend the length to which the signal can be transmitted over the same network. An important point to be noted about repeaters is that they do not amplify the signal. When the signal becomes weak, they copy the signal bit by bit and regenerate it at the original strength. It is a 2 port device.

5. **Hub** - A hub is basically a multiport repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations. Hubs cannot filter data, so data packets are sent to all connected devices. In other words, the collision domain of all hosts connected through Hub remains one. Also, they do not have the intelligence to find out the best path for data packets which leads to inefficiencies and wastage.

   Types of Hub

   - **Active Hub:-** These are the hubs which have their own power supply and can clean, boost and relay the signal along with the network. It serves both as a repeater as well as wiring centre. These are used to extend the maximum distance between nodes.

- **Passive Hub:-** These are the hubs which collect wiring from nodes and power supply from active hub. These hubs relay signals onto the network without cleaning and boosting them and can't be used to extend the distance between nodes.

6. **Bridge** - A bridge operates at data link layer. A bridge is a repeater, with add on the functionality of filtering content by reading the MAC addresses of source and destination. It is also used for interconnecting two LANs working on the same protocol. It has a single input and single output port, thus making it a 2 port device.

   Types of Bridges

   - **Transparent Bridges:-** These are the bridge in which the stations are completely unaware of the bridge's existence i.e. whether or not a bridge is added or deleted from the network, reconfiguration of the stations is unnecessary. These bridges make use of two processes i.e. bridge forwarding and bridge learning.

   - **Source Routing Bridges:-** In these bridges, routing operation is performed by source station and the frame specifies which route to follow. The hot can discover frame by sending a special frame called discovery frame, which spreads through the entire network using all possible paths to destination.

7. **Gateway** - A gateway, as the name suggests, is a passage to connect two networks together that may work upon different networking models. They basically works as the messenger agents that take data from one system, interpret it, and transfer it to another system. Gateways are also called protocol converters and can operate at any network layer. Gateways are generally more complex than switch or router.

Functions of Network Layer: 1) It helps in the delivery of data in the form of packets.

2) It helps in the delivery of packets from source host to the destination host.

3) The network layer is basically used when we want to send data over a different network.

4) In this logical addressing is used ie. when data is to be sent in the same network we need an only physical address but if we wish to send data outside network we need a logical address.

5) It helps in routing ie. routers and switches are connected at this layer to route the

packets to its final destination.

- Differences between IPv4 and IPv6

IPv4 and IPv6 are internet protocol version 4 and internet protocol version 6, IP version 6 is the new version of Internet Protocol, which is way better than IP version 4 in terms of complexity and efficiency.

Difference Between IPv4 and IPv6:

IPv4	IPv6
IPv4 has 32-bit address length	IPv6 has 128-bit address length
It Supports Manual and DHCP address configuration	It supports Auto and renumbering address configuration
In IPv4 end to end connection integrity is Unachievable	In IPv6 end to end connection integrity is Achievable
It can generate $4.29x10^9$ address space	Address space of IPv6 is quite large it can produce $3.4x10^{38}$ address space
Security feature is dependent on application	IPSEC is inbuilt security feature in the IPv6 protocol
Address representation of IPv4 is in decimal	Address Representation of IPv6 is in hexadecimal
Fragmentation performed by Sender and forwarding routers	In IPv6 fragmentation performed only by sender

IPv4	IPv6
In IPv4 Packet flow identification is not available	In IPv6 packetflow identification are Available and uses flow label field in the header
In IPv4 checksumfield is available	In IPv6 checksumfield is not available
It has broadcast Message Transmission Scheme	In IPv6 multicast and any cast message transmission scheme is available
In IPv4 Encryption and Authentication facility not provided	In IPv6 Encryption and Authentication are provided
IPv4 has header of 20-60 bytes.	IPv6 has header of 40 bytes fixed

- IP Addressing | Classless Addressing

We have introduced IP addressing and classful addressing in the previous post.

Network Address and Mask

Network address - It identifies a network on internet. Using this, we can find range of addresses in the network and total possible number of hosts in the network.

Mask - It is a 32-bit binary number that gives the network address in the address block when AND operation is bitwise applied on the mask and any IP address of the block.

The default mask in different classes are :

Class A - 255.0.0.0

Class B - 255.255.0.0

Class C - 255.255.255.0

Example : Given IP address 132.6.17.85 and default class B mask, find the beginning address (network address).

Solution : The default mask is 255.255.0.0, which means that the only the first 2 bytes are preserved and the other 2 bytes are set to 0. Therefore, the network address is 132.6.0.0.

Subnetting: Dividing a large block of addresses into several contiguous sub-blocks and assigning these sub-blocks to different networks is called subnetting. It is a

practice that is widely used when classless addressing is done.

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.

Some values calculated in subnetting :

1. Number of subnets : Given bits for mask - No. of bits in default mask

2. Subnet address : AND result of subnet mask and the given IP address

3. Broadcast address : By putting the host bits as 1 and retaining the network bits as in the IP address

4. Number of hosts per subnet : $2^{(32 - \text{Given bits for mask})} - 2$

5. First Host ID : Subnet address + 1 (adding one to the binary representation of the subnet address)

6. Last Host ID : Subnet address + Number of Hosts

Example : Given IP Address - 172.16.0.0/25, find the number of subnets and the number of hosts per subnet. Also, for the first subnet block, find the subnet address, first host ID, last host ID and broadcast address.

Solution : This is a class B address. So, no. of subnets = $2^{(25-16)} = 2^9 = 512$.

No. of hosts per subnet = $2^{(32-25)} - 2 = 2^7 - 2 = 128 - 2 = 126$

For the first subnet block, we have subnet address = 0.0, first host id = 0.1, last host id = 0.126 and broadcast address = 0.127

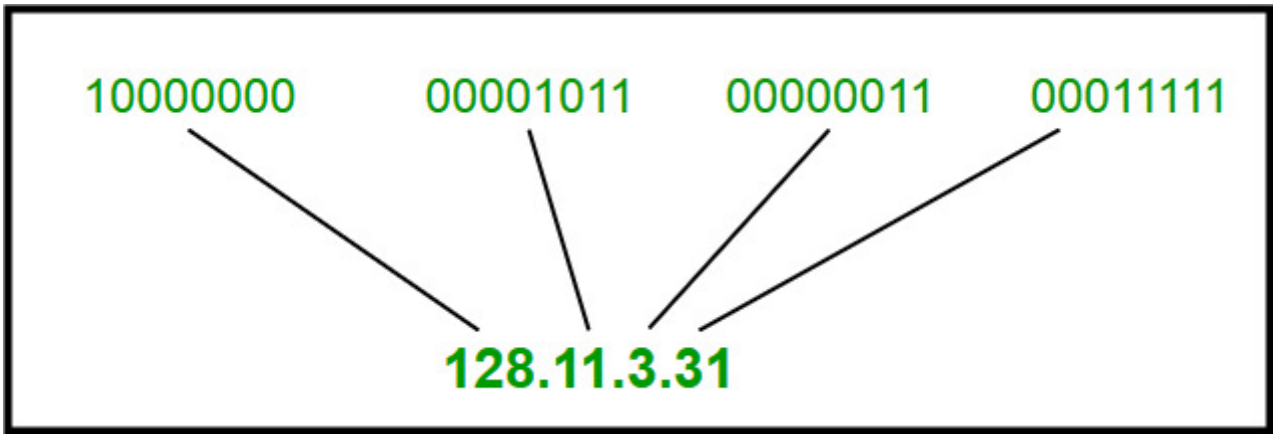
Below questions have been asked in previous GATE exam on above topics.
GATE | GATE CS 2003 | Question 82 GATE | GATE CS 2006 | Question 45 GATE | GATE CS 2007 | Question 67 GATE | GATE CS 2008 | Question 57 GATE | GATE CS 2010 | Question 47 GATE | GATE CS 2012 | Question 21 GATE | GATE CS 2015 Set 3 | Question 48

Please write comments if you find anything incorrect, or you want to share more information about the topic discussed above

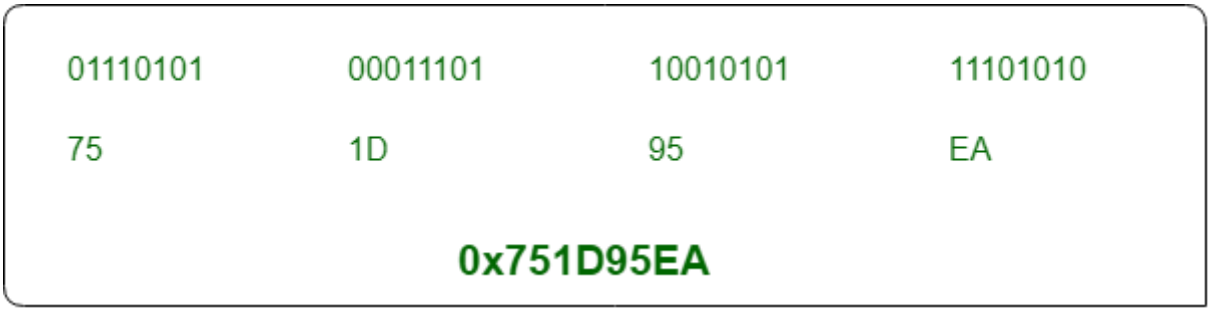
Introduction of Classful IP Addressing

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:



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).

Classful Addressing The 32 bit IP addre ided into five sub-classes. These are:

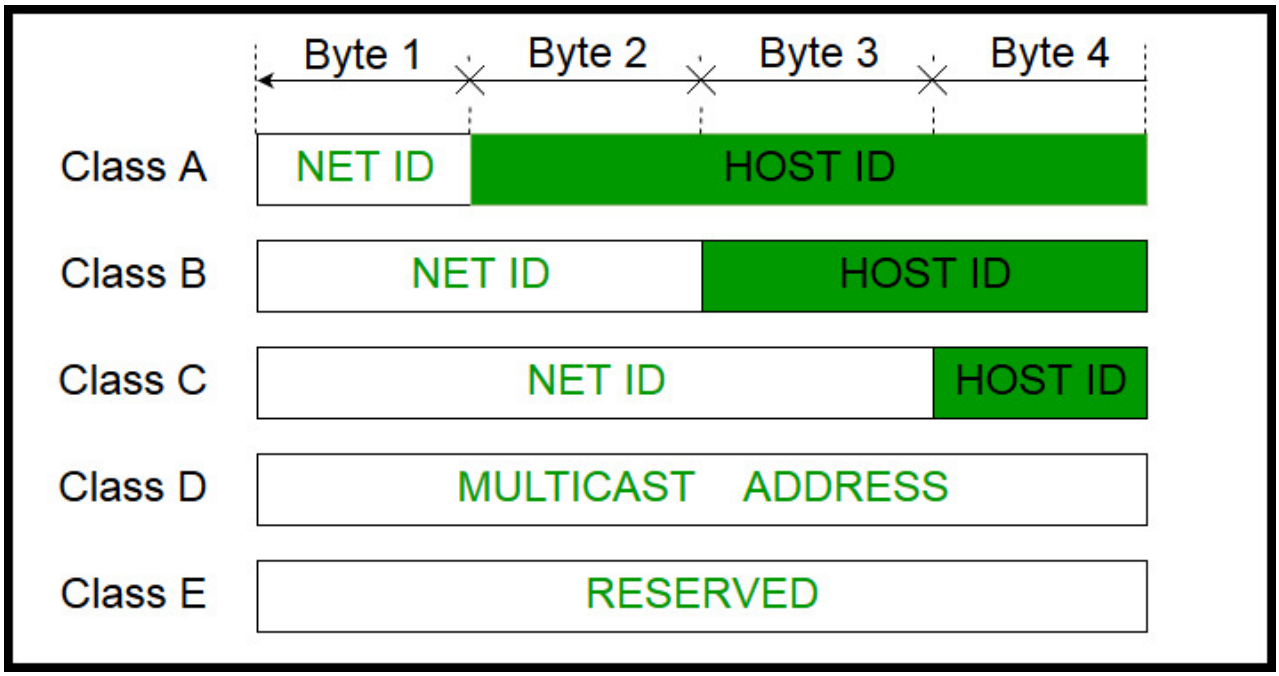
- Class A

- 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).

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.

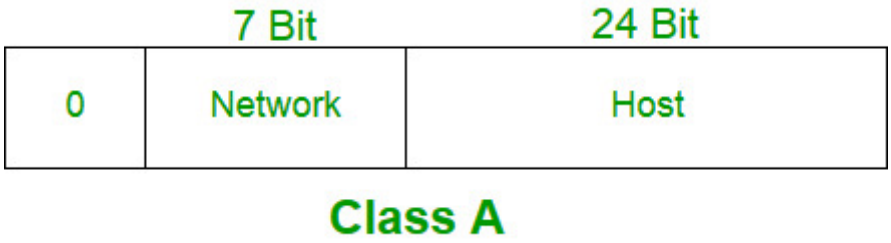
IP address belonging to class A are assigned to the networks that contain a large number of hosts.

- 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 subnet mask for class A is 255.x.x.x. Therefore, class A has a total of:

- 2^7-2= 126 network ID(Here 2 address is subracted because 0.0.0.0 and 127.x.y.z are special address.)
- 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:

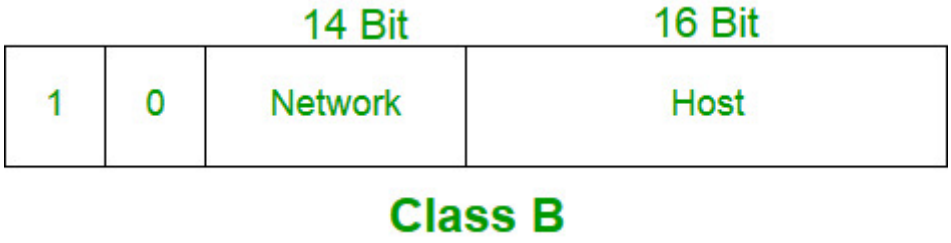
IP address belonging to class B are assigned to the networks that ranges from medium-sized to large-sized networks.

- 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.



Class C:

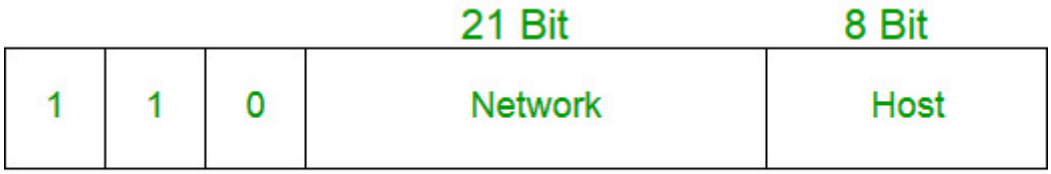
IP address belonging to class ssigned to small-sized networks.

- 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.

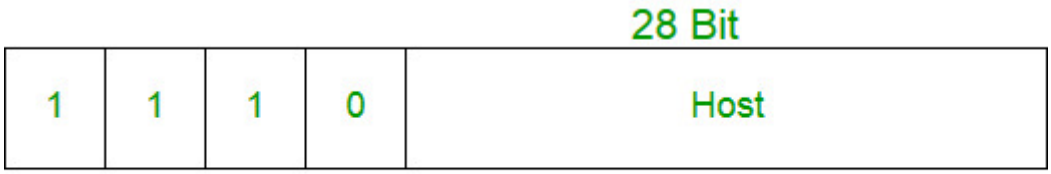


Class C

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.

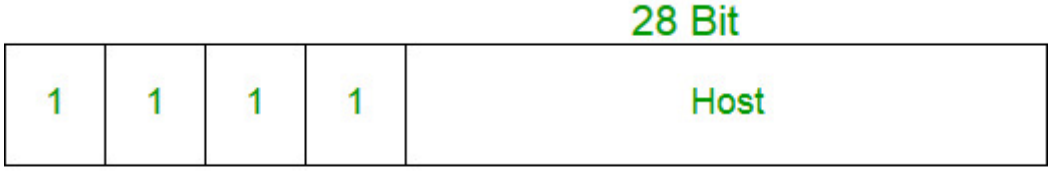
Class D does not posses any sub-net mask. IP addresses belonging to class D ranges from 224.0.0.0 - 239.255.255.255.



Class D

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.



Class E

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.

Rules for assigning Host ID:

Host ID's are used to identify a host within a network. The host ID are assigned based on the following rules:

- Within any network, the host ID must be unique to that network.
- Host ID in which all bits are set to 0 cannot be assigned because this host ID is used to represent the network ID of the IP address.
- Host ID in which all bits are set to 1 cannot be assigned because this host ID is reserved as a broadcast address to send packets to all the hosts present on that particular network.

Rules for assigning Network ID:

Hosts that are located on the same physical network are identified by the network ID, as all host on the same physical network is assigned the same network ID. The network ID is assigned based on the following rules:

- The network ID cannot start with 127 because 127 belongs to class A address and is reserved for internal loop-back functions.
- All bits of network ID set to 1 are reserved for use as an IP broadcast address and therefore, cannot be used.
- All bits of network ID set to 0 are used to denote a specific host on the local network and are not routed and therefore, aren't used.

Summary of Classful addressing :

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 availab ass 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. We will be discussing Classless addressing in next post.

References: https://en.wikipedia.org/wiki/Classful_network TechNet - Microsoft Classful network - Wikipedia
This article is contributed by **Mayank Kumar** and **Gaurav Miglani**. If you like GeeksforGeeks and would like to contribute, you can also write an article using contribute.geeksforgeeks.org or mail your article to contribute@geeksforgeeks.org. See your article appearing on the GeeksforGeeks main page and help other Geeks.

Please write comments if you find anything incorrect, or you want to share more information about the topic discussed above.

- Network Address Translation (NAT)

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.

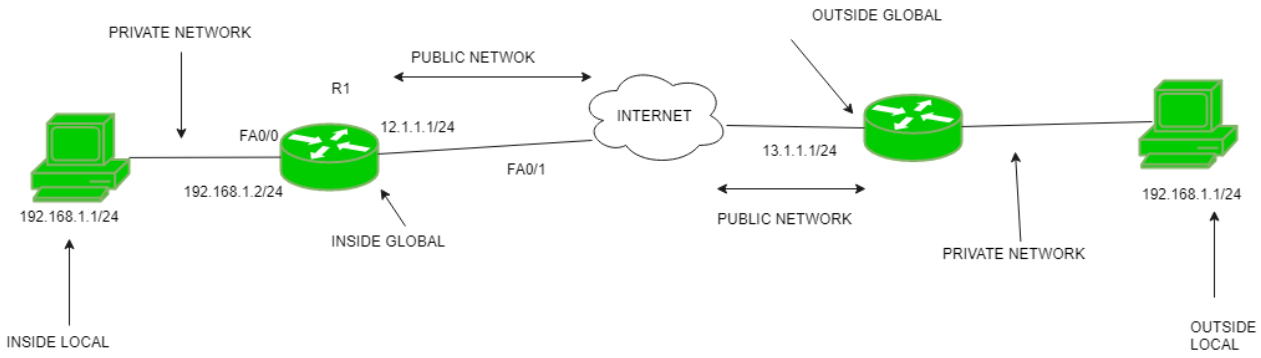
Network Address Translation (NAT) working - Generally, the border router is configured for NAT i.e the router which has one interface in local (inside) network and one interface in the global (outside) network. When a packet traverse outside the local (inside) network, then NAT converts that local (private) IP address to a global (public) IP address. When a packet enters the local network, the global (public) IP address is converted to a local (private) IP address.

If NAT run out of addresses, i.e., no address is left in the pool configured then the packets will be dropped and an Internet Message Protocol (ICMP) host

unreachable packet to the destination is sent.

Why mask port numbers?
Suppose, in a network, two hosts A and B are connected. Now, both of them request for the same destination, on the same port number, say 1000, on the host side, at the same time. If NAT does an only translation of IP addresses, then when their packets will arrive at the NAT, both of their IP addresses would be masked by the public IP address of the network and sent to the destination. Destination will send replies on the public IP address of the router. Thus, on receiving a reply, it will be unclear to NAT as to which reply belongs to which host (because source port numbers for both A and B are same). Hence, to avoid such a problem, NAT masks the source port number as well and makes an entry in the NAT table.

NAT inside and outside addresses - Inside refers to the addresses which must be translated. Outside refers to the addresses which are not in control of an organisation. These are the network Addresses in which the translation of the addresses will be done.



- **Inside local address -** An IP address that is assigned to a host on the Inside (local) network. The address is probably not a IP address assigned by the service provider i.e., these are private IP address. This is the inside host seen from the inside network.
- **Inside global address -** IP address that represents one or more inside local IP addresses to the outside world. This is the inside host as seen from the outside network.
- **Outside local address -** This is the actual IP address of the destination host in the local network after translation.
- **Outside global address -** This is the outside host as seen form the outside network. It is the IP address of the outside destination host before translation.

Network Address Translation (NAT) Types - There are 3 ways to configure NAT:

1. **Static NAT -** In this, a single unregistered (Private) IP address is mapped with a legally registered (Public) IP address i.e one-to-one mapping between local and global address. This is generally us Web hosting. These are not used in

organisations as there are many devices who will need Internet access and to provide Internet access, the public IP address is needed.

Suppose, if there are 3000 devices who need access to the Internet, the organisation have to buy 3000 public addresses that will be very costly.

2. **Dynamic NAT -** In this type of NAT, an unregistered IP address is translated into a registered (Public) IP address from a pool of public IP address. If the IP address of pool is not free, then the packet will be dropped as an only a fixed number of private IP address can be translated to public addresses.

   Suppose, if there is a pool of 2 public IP addresses then only 2 private IP addresses can be translated at a given time. If 3rd private IP address wants to access Internet then the packet will be dropped therefore many private IP addresses are mapped to a pool of public IP addresses. NAT is used when the number of users who wants to access the Internet is fixed. This is also very costly as the organisation have to buy many global IP addresses to make a pool.

3. **Port Address Translation (PAT) -** This is also known as NAT overload. In this, many local (private) IP addresses can be translated to a single registered IP address. Port numbers are used to distinguish the traffic i.e., which traffic belongs to which IP address. This is most frequently used as it is cost-effective as thousands of users can be connected to the Internet by using only one real global (public) IP address.

Advantages of NAT -

- NAT conserves legally registered IP addresses .
- It provides privacy as the device IP address, sending and receiving the traffic, will be hidden.
- Eliminates address renumbering when a network evolves.

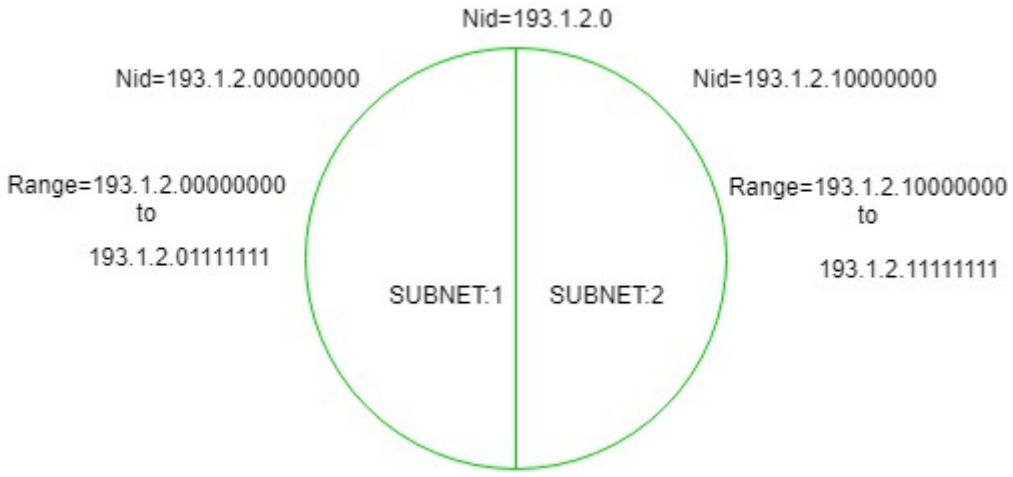
Disadvantage of NAT -

- Translation results in switching path delays.
- Certain applications will not function while NAT is enabled.
- Complicates tunneling protocols such as IPsec.
- Also, router being a network layer device, should not tamper with port numbers(transport layer) but it has to do so because of NAT.

- Introduction To Subnetting

When a bigger network is divided into smaller networks, in order to maintain security, then that is known as Subnetting. so, ma ce is easier for smaller networks.

Now, let's talk about dividing a network into two parts: so to divide a network into two parts, you need to choose one bit for each Subnet from the host ID part.



In the above diagram, there are two Subnets.

Note: It is a class C IP so, there are 24 bits in the network id part and 8 bits in the host id part.

- **For Subnet-1:** The first bit which is chosen from the host id part is zero and the range will be from (193.1.2.00000000 till you get all 1's in the host ID part i.e, 193.1.2.01111111) except for the first bit which is chosen zero for subnet id part.

  Thus, the range of subnet-1:

  ```
  193.1.2.0 to 193.1.2.127
  ```

- **For Subnet-2:** The first bit chosen from the host id part is one and the range will be from (193.1.2.100000000 till you get all 1's in the host ID part i.e, 193.1.2.11111111).

  Thus, the range of subnet-2:

  ```
  193.1.2.128 to 193.1.2.255
  ```

Note:

1. To divide a network into four (2^2) parts you need to choose two bits from host id part for each subnet i.e, (00, 01, 10, 11).

2. To divide a network into eight (2^3) parts you need to choose three bits from host id part for each subnet i.e, (000, 001, 010, 011, 100, 101, 110, 111) and so on.

- Classless Inter Domain Routing (CIDR)

As we have already learned about Classful Addressing, so in this article, we are going to learn about Classless Inter-Domain Routing. which is also known as Classless addressing. In the Classful addressing the no of Hosts within a network always remains the same depending upon the class of the Network.

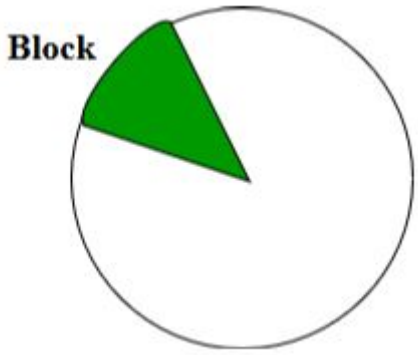
```
Class A network contains 2^24 Hosts,

Class B network contains 2^16 Hosts,

Class C network contains 2^8 Hosts
```

Now, let's suppose an Organization requires 2^{14} hosts, then it must have to purchase a Class B network. In this case, 49152 Hosts will be wasted. This is the major drawback of Classful Addressing.

In order to reduce the wastage of IP addresses a new concept of **Classless Inter-Domain Routing** is introduced. Now a days *IANA* is using this technique to provide the IP addresses. Whenever any user asks for IP addresses, IANA is going to assign that many IP addresses to the User.



Representation: It is as also a 32-bit address, which includes a special number which represents the number of bits that are present in the Block Id.

```
a . b . c . d / n
```

Where, n is number of bits that are present in Block Id / Network Id.

Example:

```
20.10.50.100/20
```

Rules for forming CIDR Blocks:

1. All IP addresses must be contiguous.
2. Block size must be the power of 2 (2^n).
   If the size of the block is the power of 2, then it will be easy to divide the Network.
   Finding out the Block Id is very easy if the block size is of the power of 2.
   Example: If the Block size is 2^5 then, Host Id will contain 5 bits and Network will contain 32 - 5 = 27 bits.

3. First IP address of the Block must be evenly divisible by the size of the block. in simple words, the least significant part should always start with zeroes in Host Id. Since all the least significant bits of Host Id is zero, then we can use it as Block Id part.

Example: Check whether 100.1.2.32 to 100.1.2.47 is a valid IP address block or not?

1. All the IP addresses are contiguous.
2. Total number of IP addresses in the Block = 16 = 2^4.
3. 1st IP address: 100.1.2.00100000
   Since, Host Id will contains last 4 bits and all the least significant 4 bits are zero.
   Hence, first IP address is evenly divisible by the size of the block.

All the three rules are followed by this Block. Hence, it is a valid IP address block.

- Distance Vector Routing (DVR) Protocol

A **distance-vector routing (DVR)** protocol requires that a router inform its neighbors of topology changes periodically. Historically known as the old ARPANET routing algorithm (or known as Bellman-Ford algorithm).

Bellman Ford Basics - Each router maintains a Distance Vector table containing the distance between itself and ALL possible destination nodes. Distances,based on a

chosen metric, are computed using information from the neighbors' distance vectors.

```
Information kept by DV router -
   • Each router has an ID
   • Associated with each link connected to a router,
     there is a link cost (static or dynamic).
   • Intermediate hops


Distance Vector Table Initialization -
   • Distance to itself = 0
   • Distance to ALL other routers = infinity number.
```


Distance Vector Algorithm -

1. A router transmits its distance vector to each of its neighbors in a routing packet.
2. Each router receives and saves the most recently received distance vector from each of its neighbors.
3. A router recalculates its distance vector when:
    - It receives a distance vector from a neighbor containing different information than before.
    - It discovers that a link to a neighbor has gone down.

The DV calculation is based on minimizing the cost to each destination

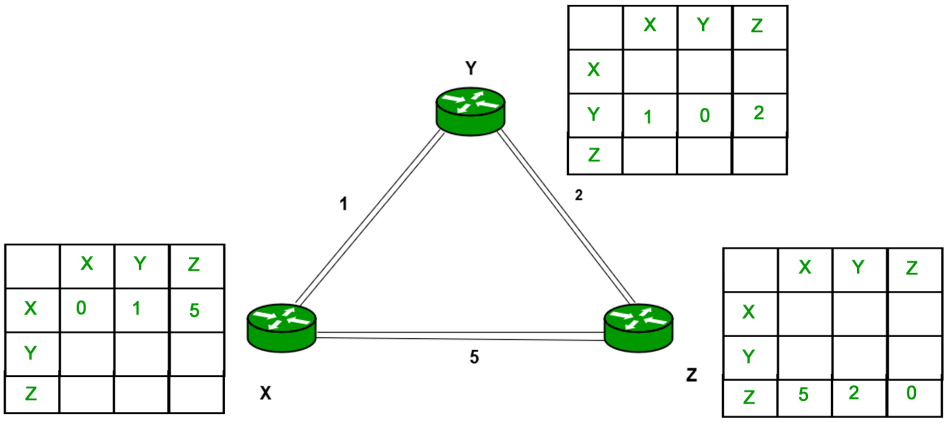
```
Dx(y) = Estimate of least cost from x to y
C(x,v) =  Node x knows cost to each neighbor v
Dx   =  [Dx(y): y ∈ N ] = Node x maintains distance vector
Node x also maintains its neighbors' distance vectors
- For each neighbor v, x maintains Dv = [Dv(y): y ∈ N ]
```

Note -

- From time-to-time, each node sends its own distance vector estimate to neighbors.
- When a node x receives new DV estimate from any neighbor v, it saves v's distance vector and it updates its own DV using B-F equation:

  ```
  Dx(y) = min { C(x,v) + Dv(y), Dx(y) } for each node y ∈ N
  ```

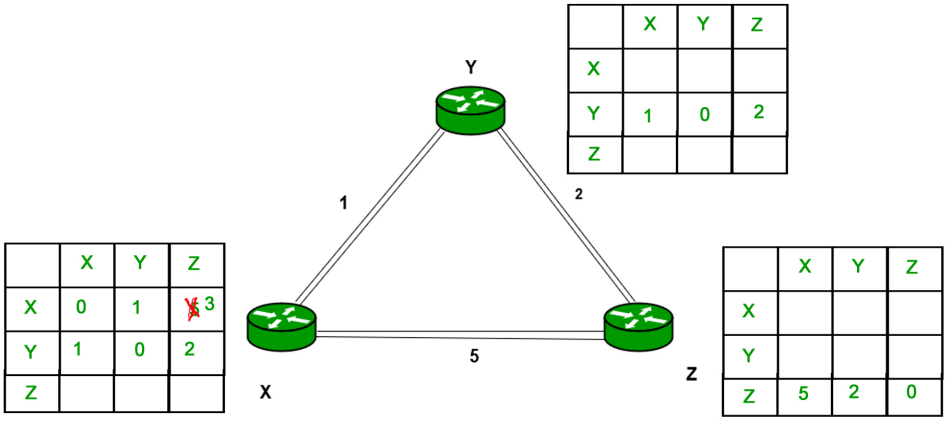
Example - Consider 3-routers X, Y and Z as shown in figure. Each router have their routing table. Every routing table will contain distance to the destination nodes.



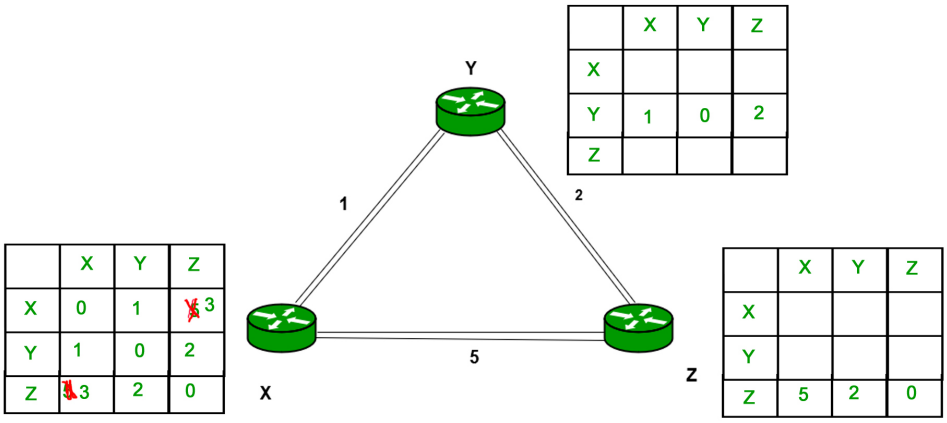
Consider router X , X will share it routing table to neighbors and neighbors will share it routing table to it to X and distance from node X to destination will be calculated using bellmen- ford equation.

```
Dx(y) = min { C(x,v) + Dv(y)} for each node y ∈ N
```

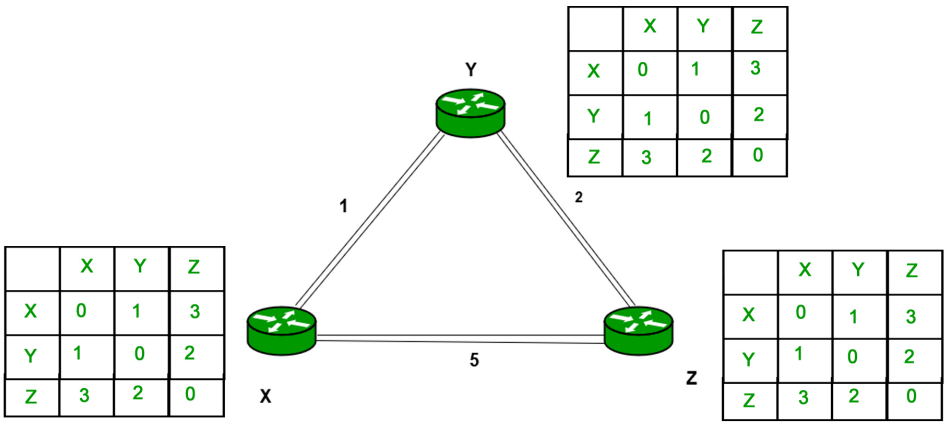
As we can see that distance will be less going from X to Z when Y is intermediate node(hop) so it will be update in routing table X.



Similarly for Z also -



Finally the routing table for all -



Advantages of Distance Vector routing -

- It is simpler to configure and maintain than link state routing.

  Disadvantages of Distance Vector routing -
  - It is slower to converge than link state.
  - It is at risk from the count-to-infinity problem.
  - It creates more traffic than link state since a hop count change must be propagated to all routers and processed on each router. Hop count updates take place on a periodic basis, even if there are no changes in the network topology, so bandwidth-wasting broadcasts still occur.
  - For larger networks, distance vector routing results in larger routing tables than link state since each router must know about all other routers. This can also lead to congestion on WAN links.

Note - Distance Vector routing use User datagram protocol) for

transportation.

GATE CS Corner Questions

Practicing the following questions will help you test your knowledge. All questions have been asked in GATE in previous years or in GATE Mock Tests. It is highly recommended that you practice them.

1. GATE CS 2011, Question 52
2. GATE CS 2011, Question 53
3. GATE CS 2010, Question 54
4. GATE CS 2010, Question 55
5. GATE IT 2005, Question 28
6. GATE CS 2014 (Set 1), Question 33
7. GATE IT 2008, Question 65
8. GATE CS 2014 (Set 2), Question 65

References -

Distance vector routing - wikipedia www.eecs.yorku.ca

This article is contributed by **Akash Sharan**. If you like GeeksforGeeks and would like to contribute, you can also write an article using contribute.geeksforgeeks.org or mail your article to contribute@geeksforgeeks.org. See your article appearing on the GeeksforGeeks main page and help other Geeks.

Please write comments if you find anything incorrect, or you want to share more information about the topic discussed above.

Company

About Us

Careers

Privacy Policy

Contact Us

Terms of Service

Learn

Algorithms

Data Structures

Languages

CS Subjects

Video Tutorials

LIVE BATCHES

Practice

Courses

Company-wise

Topic-wise

How to begin?

Contribute

Write an Article

Write Interview Experience

Internships

Videos

▲