**Network Layer**

The Network Layer is the third layer of the OSI model.

* It handles the service requests from the transport layer and further forwards the service request to the data link layer.
* The network layer translates the logical addresses into physical addresses
* It determines the route from the source to the destination and also manages the traffic problems such as switching, routing and controls the congestion of data packets.
* The main role of the network layer is to move the packets from sending host to the receiving host.

The main functions performed by the network layer are:

* **Routing:** When a packet reaches the router's input link, the router will move the packets to the router's output link. For example, a packet from S1 to R1 must be forwarded to the next router on the path to S2.
* **Logical Addressing:** The data link layer implements the physical addressing and network layer implements the logical addressing. Logical addressing is also used to distinguish between source and destination system. The network layer adds a header to the packet which includes the logical addresses of both the sender and the receiver.
* **Internetworking:** This is the main role of the network layer that it provides the logical connection between different types of networks.
* **Fragmentation:** The fragmentation is a process of breaking the packets into the smallest individual data units that travel through different networks.

**Network Addressing:**

* Network Addressing is one of the major responsibilities of the network layer.
* Network addresses are always logical, i.e., software-based addresses.
* A host is also known as end system that has one link to the network. The boundary between the host and link is known as an interface. Therefore, the host can have only one interface.
* A router is different from the host in that it has two or more links that connect to it. When a router forwards the datagram, then it forwards the packet to one of the links. The boundary between the router and link is known as an interface, and the router can have multiple interfaces, one for each of its links. Each interface is capable of sending and receiving the IP packets, so IP requires each interface to have an address.
* Each IP address is 32 bits long, and they are represented in the form of "dot-decimal notation" where each byte is written in the decimal form, and they are separated by the period. An IP address would look like 193.32.216.9 where 193 represents the decimal notation of first 8 bits of an address, 32 represents the decimal notation of second 8 bits of an address.

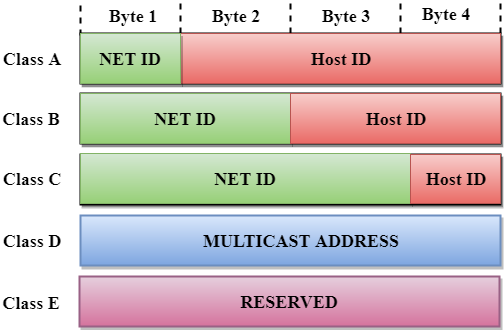
**Classful Addressing**

An IP address is 32-bit long. An IP address is divided into sub-classes:

* Class A
* Class B
* Class C
* Class D
* Class E

An ip address is divided into two parts:

* Network ID: It represents the number of networks.
* Host ID: It represents the number of hosts.



In the above diagram, we observe that each class have a specific range of IP addresses. The class of IP address is used to determine the number of bits used in a class and number of networks and hosts available in the class.

**Class A**

In Class A, an IP address is assigned to those networks that contain a large number of hosts.

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

In Class A, the first bit in higher order bits of the first octet is always set to 0 and the remaining 7 bits determine the network ID. The 24 bits determine the host ID in any network.

The total number of networks in Class A = 27 = 128 network address

The total number of hosts in Class A = 224 - 2 = 16,777,214 host address



**Class B**

In Class B, an IP address is assigned to those networks that range from small-sized to large-sized networks.

* The Network ID is 16 bits long.
* The Host ID is 16 bits long.

In Class B, the higher order bits of the first octet is always set to 10, and the remaining14 bits determine the network ID. The other 16 bits determine the Host ID.

The total number of networks in Class B = 214 = 16384 network address

The total number of hosts in Class B = 216 - 2 = 65534 host address



**Class C**

In Class C, an IP address is assigned to only small-sized networks.

* The Network ID is 24 bits long.
* The host ID is 8 bits long.

In Class C, the higher order bits of the first octet is always set to 110, and the remaining 21 bits determine the network ID. The 8 bits of the host ID determine the host in a network.

The total number of networks = 221 = 2097152 network address

The total number of hosts = 28 - 2 = 254 host address



**Class D**

In Class D, an IP address is reserved for multicast addresses. It does not possess subnetting. The higher order bits of the first octet is always set to 1110, and the remaining bits determines the host ID in any network.

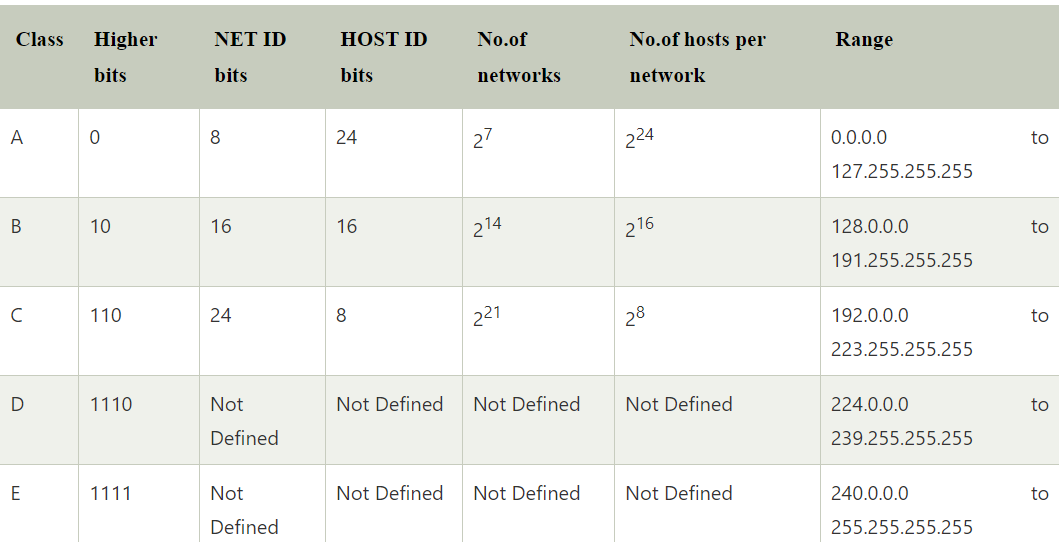


**Class E**

In Class E, an IP address is used for the future use or for the research and development purposes. It does not possess any subnetting. The higher order bits of the first octet is always set to 1111, and the remaining bits determines the host ID in any network.



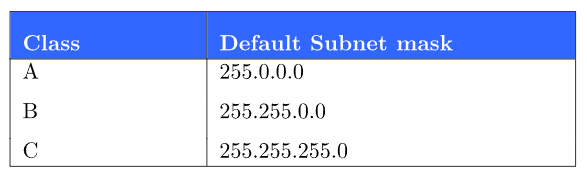
**Classful Network Architecture:**

****

**Subnet Mask:**

A subnet mask is used in a process known as subnetting, in which a large network is divided into smaller networks. More specifically, it’s like dividing a network into several contiguous network groups, and each group is known as a subnet. Furthermore, this process is implemented to reduce the wastage of IP addresses due to classful addressing.

A subnet mask is used to determine the network address and host address:

****

**Decimal to Binary Conversion and vice versa:**

The calculation of network address and the broadcast address involves decimal to binary conversion or vice versa. Hence, the following method may be helpful in calculating the network address and the broadcast address of an IP address.

**To convert the decimal number into binary numbers,**

* Divide the decimal number by 2.
* Store the remainder (either 0 or 1) repeatedly until the decimal number is completely divisible by 2.
* Note down the series of the remainder in 1 or 0 in reverse order.

For Example: **Convert (50)10 into binary format**

|  |  |
| --- | --- |
| **Division by 2** | **Remainder** |
| 50/2 = 25 | 0 |
| 25/2 = 12 | 1 |
| 12/2 = 6 | 0 |
| 6/2 =3 | 0 |
| 3/2 = 1 | 1 |
| 1/2 =0 | 1 |

Writing the remainder in reverse order, we get **(110010)2**

Since, IP address is represented in a block of 8 bits,

**(110010)2**is written as **(00110010)2**

Hence, **(50)10 =(00110010)2**

**To convert binary into decimal format**

* Multiply the binary number with the binary exponential of its place value.
* Add them all to give the decimal number.

For example, to convert **(00110010)2** into decimal format

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Binary Exponents | **27 = 128** | **26 = 64** | **25 = 32** | **24 = 16** | **23 = 8** | **22 = 4** | **21 = 2** | **20 = 1** |
| Binary Number | **0** | **0** | **1** | **1** | **0** | **0** | **1** | **0** |
|  | **128 x 0** | **64 x 0** | **32 x 1** | **16 x 1** | **8 x 0** | **4 x 0** | **2 x 1** | **1 x 0** |
| Decimal Number | **0 + 0 + 32 + 16 + 0 + 0 + 2 + 0 = (50)10** | | | | | | | |

Hence, the decimal equivalent of a binary number (**00110010)2**  is  **(50)10.**

**How to Calculate Network Address and Broadcast Address:**

Now, in order to calculate network and broadcast addresses, we need two pieces of information: the IP address of the device and the subnet mask of the network.

IP address **192.168.5.50 / 28** will have the network address and the broadcast address as the following

**To calculate the network address:**

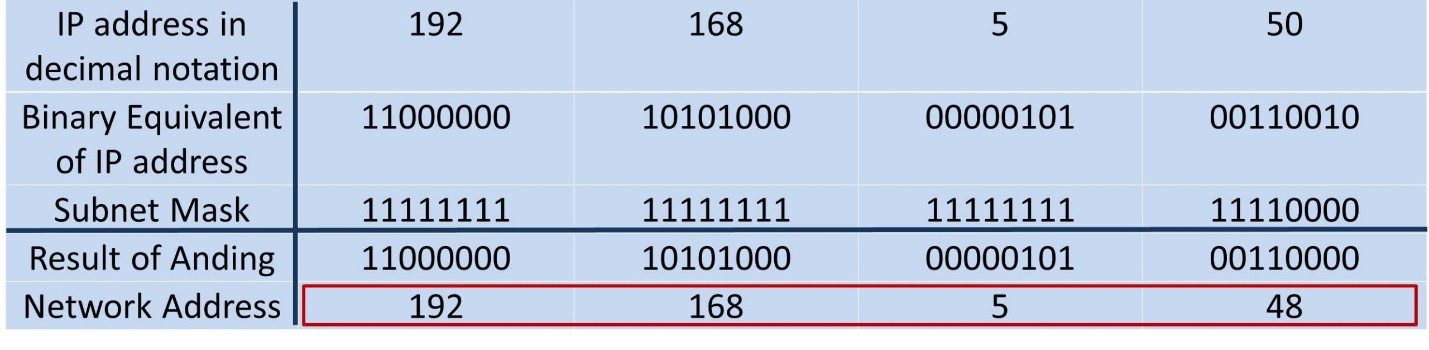
**Step1**: Write the given IP address in binary format.

**Step 2:** Write the subnet mask in binary form.

**Step:** Perform the logical  ANDing operation between the corresponding octets of the IP address and the subnet mask.

**Step 4:** Convert the result back to the decimal format and this will be the network address.

The following example illustrates the calculation of the network address.



Therefore, the network address will be: **192.168.5.48**

**To calculate the broadcast address**

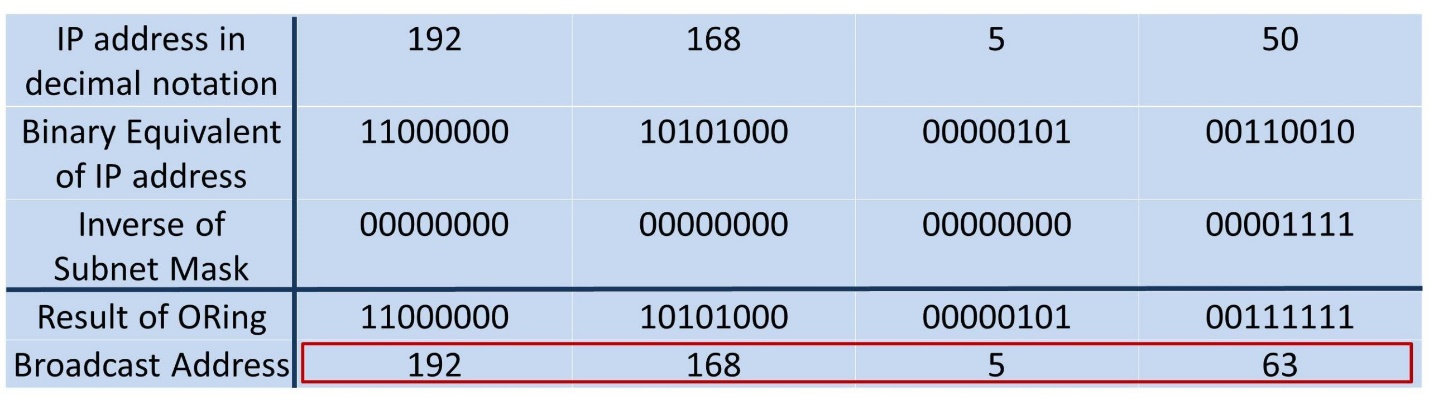
**Step1**: Write the given IP address in binary format.

**Step 2:** Write the inverse of the subnet mask in binary form.

**Step3:** Perform the logical ORing operation between the corresponding octets of the IP address and the inverse of the subnet mask.

**Step 4:** Convert the result back to the decimal format and this will be the network address.

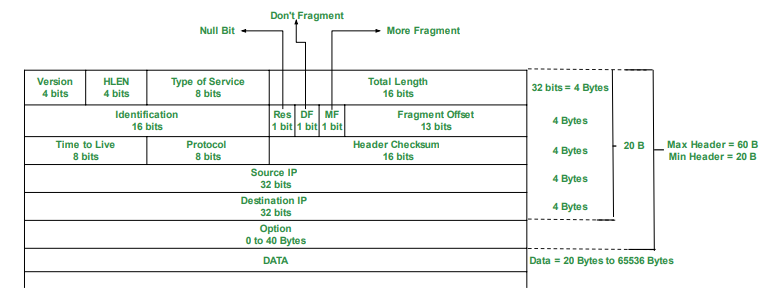
The following example illustrates the calculation of the broadcast address.

Therefore, the network address will be: **192.168.5.63**

The following tables show the subnet masks their corresponding CIDR values.

|  |  |
| --- | --- |
| **Subnet Mask** | **CIDR Value** |
| 255.0.0.0 | /8 |
| 255.128.0.0 | /9 |
| 255.192.0.0 | /10 |
| 255.224.0.0 | /11 |
| 255.240.0.0 | /12 |
| 255.248.0.0 | /13 |
| 255.252.0.0 | /14 |
| 255.254.0.0 | /15 |
| 255.255.0.0 | /16 |
| 255.255.128.0 | /17 |
| 255.255.192.0 | /18 |
| 255.255.224.0 | /19 |
| 255.255.240.0 | /20 |
| 255.255.248.0 | /21 |
| 255.255.252.0 | /22 |
| 255.255.254.0 | /23 |
| 255.255.255.0 | /24 |
| 255.255.255.128 | /25 |
| 255.255.255.192 | /26 |
| 255.255.255.224 | /27 |
| 255.255.255.240 | /28 |
| 255.255.255.248 | /29 |
| 255.255.255.252 | /30 |

**IPv4 header format:**



**VERSION:** Version of the IP protocol (4 bits), which is 4 for IPv4

**HLEN:** IP header length (4 bits), which is the number of 32 bit words in the header. The minimum value for this field is 5 and the maximum is 15.

**Type of service:** Low Delay, High Throughput, Reliability (8 bits)

**Total Length:** Length of header + Data (16 bits), which has a minimum value 20 bytes and the maximum is 65,535 bytes.

**Identification:** Unique Packet Id for identifying the group of fragments of a single IP datagram (16 bits)

**Flags:** 3 flags of 1 bit each: reserved bit (must be zero), do not fragment flag, more fragments flag (same order)

**Fragment Offset:** Represents the number of Data Bytes ahead of the particular fragment in the particular Datagram. Specified in terms of number of 8 bytes, which has the maximum value of 65,528 bytes.

**Time to live:** Datagram’s lifetime (8 bits), It prevents the datagram to loop through the network by restricting the number of Hops taken by a Packet before delivering to the Destination.

**Protocol**: Name of the protocol to which the data is to be passed (8 bits)

**Header Checksum:** 16 bits header checksum for checking errors in the datagram header

**Source IP address**: 32 bits IP address of the sender

**Destination IP address**: 32 bits IP address of the receiver

**Option:** Optional information such as source route, record route. Used by the Network administrator to check whether a path is working or not.

**Differences between IPv4 and Ipv6:**

|  |  |  |
| --- | --- | --- |
| **Address length** | IPv4 is a 32-bit address. | IPv6 is a 128-bit address. |
| **Fields** | IPv4 is a numeric address that consists of 4 fields which are separated by dot (.). | IPv6 is an alphanumeric address that consists of 8 fields, which are separated by colon. |
| **Classes** | IPv4 has 5 different classes of IP address that includes Class A, Class B, Class C, Class D, and Class E. | IPv6 does not contain classes of IP addresses. |
| **Number of IP address** | IPv4 has a limited number of IP addresses. | IPv6 has a large number of IP addresses. |
| **VLSM** | It supports VLSM (Virtual Length Subnet Mask). Here, VLSM means that Ipv4 converts IP addresses into a subnet of different sizes. | It does not support VLSM. |
| **Address configuration** | It supports manual and DHCP configuration. | It supports manual, DHCP, auto-configuration, and renumbering. |
| **Address space** | It generates 4 billion unique addresses | It generates 340 undecillion unique addresses. |
| **End-to-end connection integrity** | In IPv4, end-to-end connection integrity is unachievable. | In the case of IPv6, end-to-end connection integrity is achievable. |
| **Security features** | In IPv4, security depends on the application. This IP address is not developed in keeping the security feature in mind. | In IPv6, IPSEC is developed for security purposes. |
| **Address representation** | In IPv4, the IP address is represented in decimal. | In IPv6, the representation of the IP address in hexadecimal. |
| **Fragmentation** | Fragmentation is done by the senders and the forwarding routers. | Fragmentation is done by the senders only. |
| **Packet flow identification** | It does not provide any mechanism for packet flow identification. | It uses flow label field in the header for the packet flow identification. |
| **Checksum field** | The checksum field is available in IPv4. | The checksum field is not available in IPv6. |
| **Transmission scheme** | IPv4 is broadcasting. | On the other hand, IPv6 is multicasting, which provides efficient network operations. |
| **Encryption and Authentication** | It does not provide encryption and authentication. | It provides encryption and authentication. |
| **Number of octets** | It consists of 4 octets. | It consists of 8 fields, and each field contains 2 octets. Therefore, the total number of octets in IPv6 is 16. |