SNS COLLEGE OF TECHNOLOGY

Coimbatore-35
An Autonomous Institution

Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A+' Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

DEPARTMENT OF ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

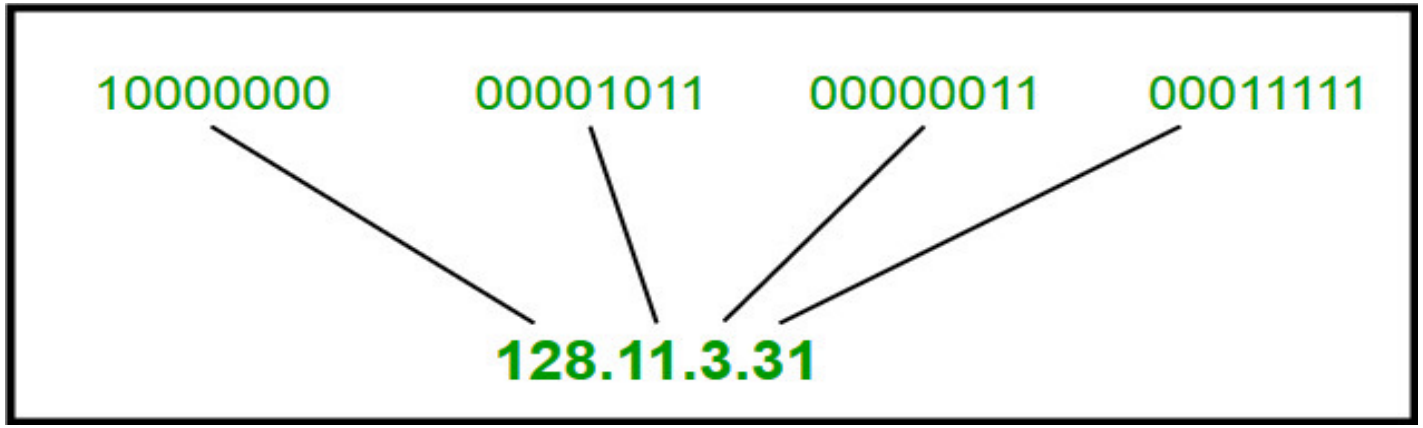
19CSB302- COMPUTER NETWORKS

UNIT-3 INTERNETWORKING AND ROUTING

IP ADDRESSING

An 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}.

DOTTED DECIMAL /BINARY NOTATION



CLASSFUL ADDRESSING

The 32-bit IP address is divided into five sub-classes.

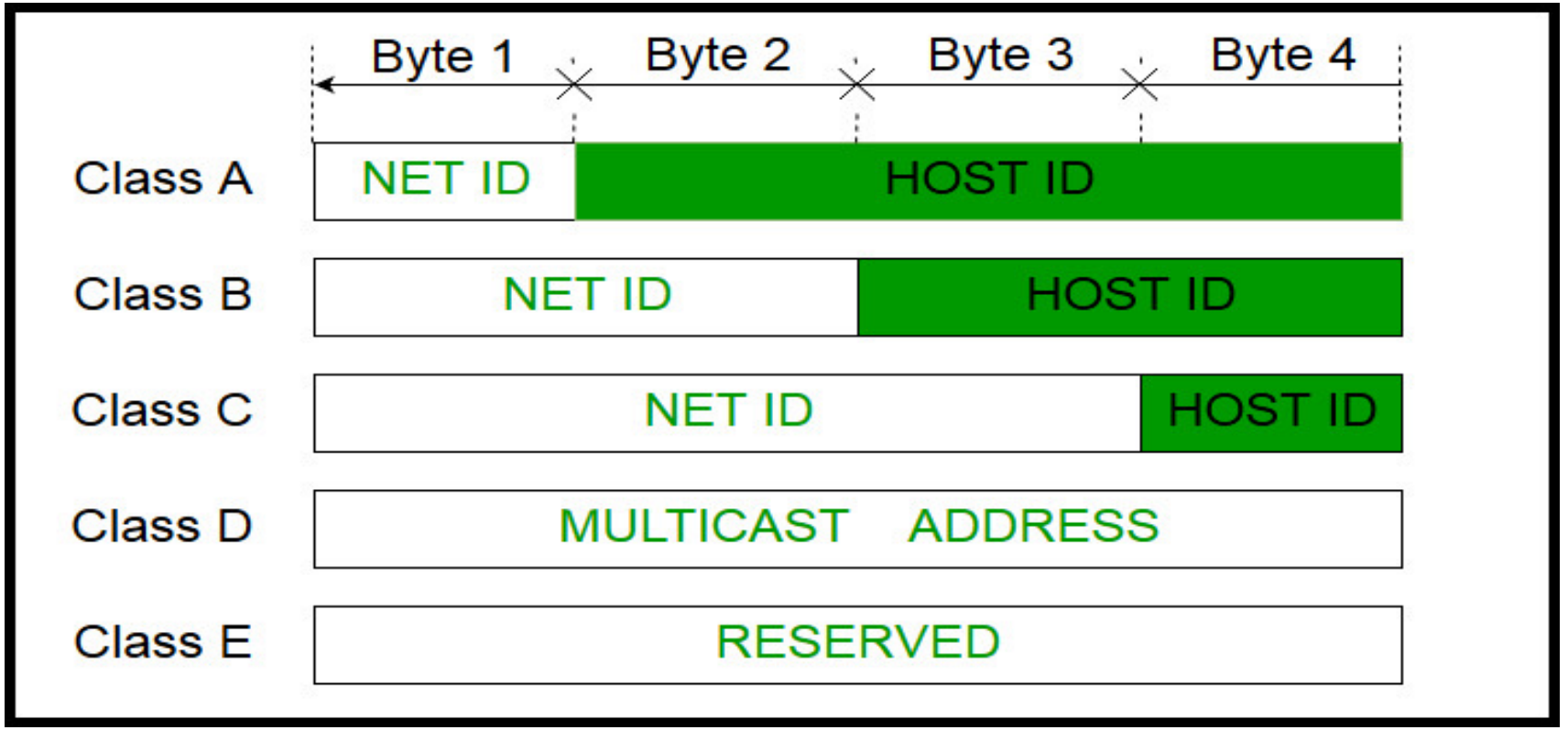
- Class A
- Class B
- Class C
- Class D
- Class E

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 determines the classes of the IP address.

The IPv4 address is divided into two parts:

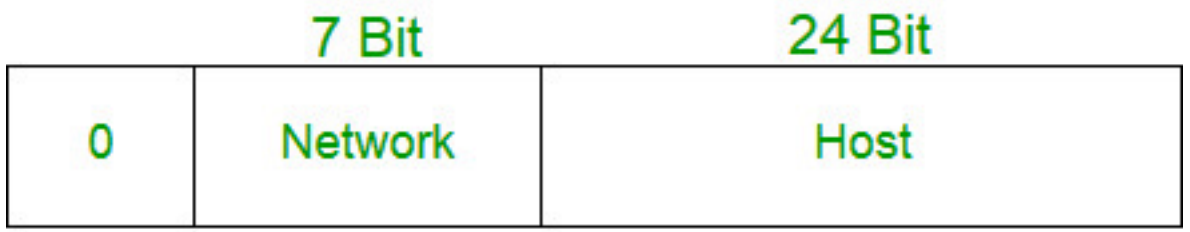
- Network ID
- Host ID

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 an IP address to each device that is connected to its network.


Byte 1
Byte 2
Byte 3
Byte 4
Class A
NET ID
HOST ID
Class B
NET ID
HOST ID
Class C
NET ID
HOST ID
Class D
MULTICAST ADDRESS
Class E
RESERVED

Class A

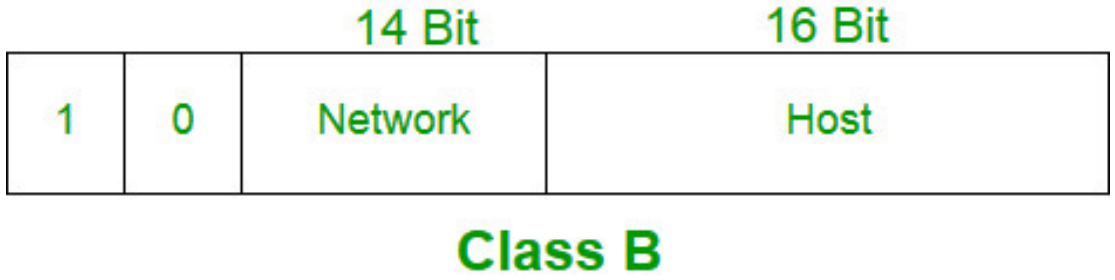
- IP addresses belonging to class A are assigned to the networks that contain a large number of hosts.
- The network ID is 8 bits long.
- The host ID is 24 bits long. The higher-order bit of the first octet in class A is always set to 0. The remaining 7 bits in the first octet are used to determine network ID. The 24 bits of host ID are used to determine the host in any network.



Class A

Class B

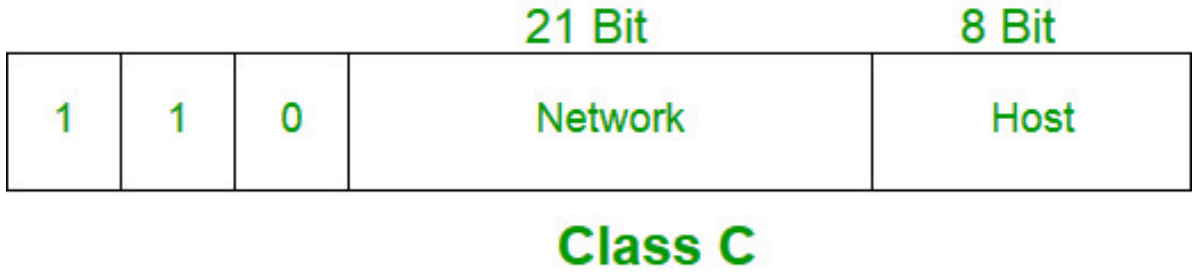
- IP address belonging to class B is assigned to networks that range from medium-sized to large-sized networks.
- The network ID is 16 bits long.
- The host ID is 16 bits long.
- The higher-order bits of the first octet of IP addresses of class B are always set to 10. The remaining 14 bits are used to determine the network ID. The 16 bits of host ID are used to determine the host in any network.



Class B

Class C

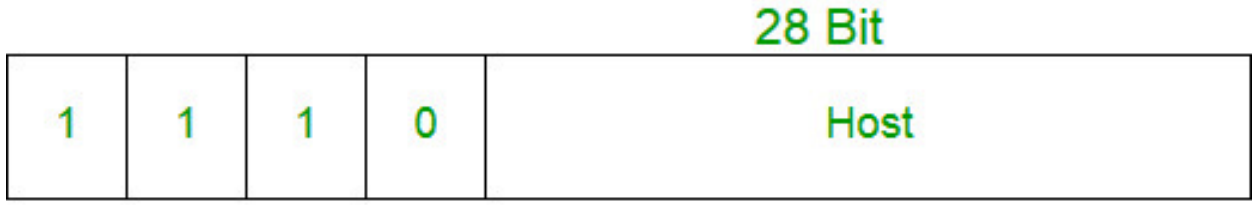
- IP addresses belonging to class C are assigned to small-sized networks.
- The network ID is 24 bits long.
- The host ID is 8 bits long.
- The higher-order bits of the first octet of IP addresses of class C is always set to 110. The remaining 21 bits are used to determine the network ID. The 8 bits of host ID are used to determine the host in any network



Class C

Class D

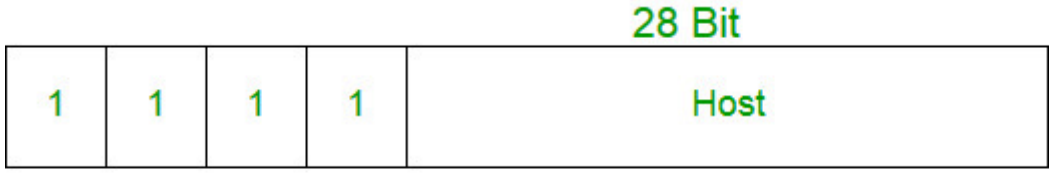
- IP address belonging to class D is reserved for multi-casting. The higher-order bits of the first octet of IP addresses belonging to class D is always set to 1110.



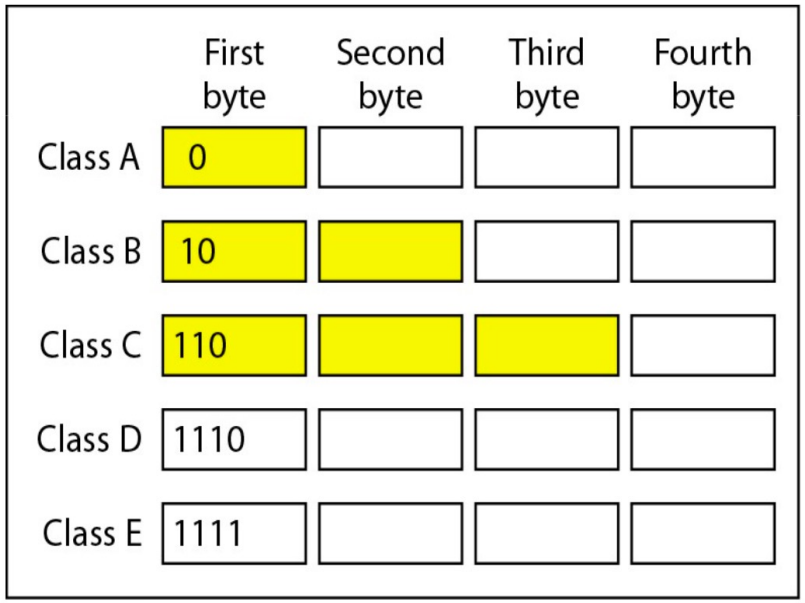
Class D

Class E

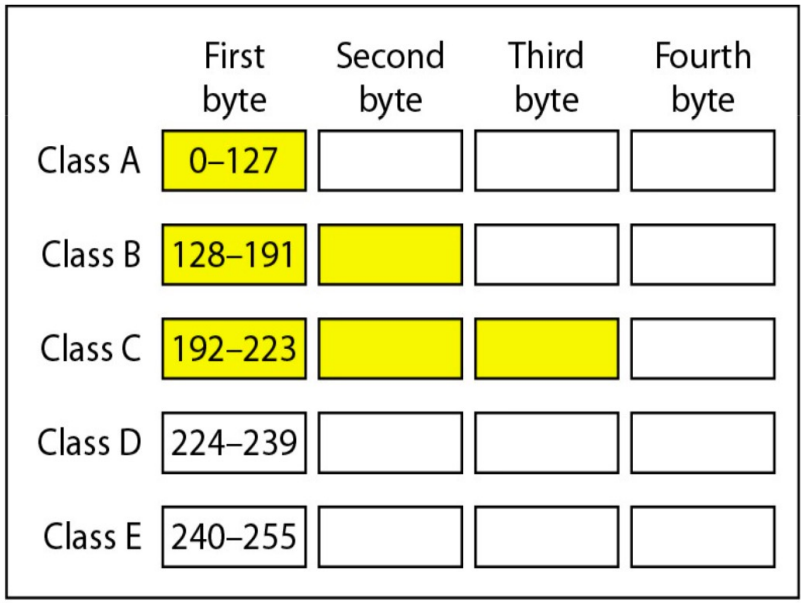
- IP addresses belonging to class E are reserved for experimental and research purposes.



Class E



a. Binary notation



b. Dotted-decimal notation

Subnet Mask

- When you connect a device to a network, the network assigns an IP address to the device. That IP address consists of two parts: the **network portion** and the **host portion**. The network portion of the IP address identifies the overall network while the host portion identifies the device. The subnet mask is obtained by making all the network bits 1 and host bits 0.

Class A
Subnet Mask

Netwok	Host	Host	Host
255	0	0	0

Class B
Subnet Mask

Netwok	Network	Host	Host
255	255	0	0

Class C
Subnet Mask

Netwok	Network	Network	Host
255	255	255	0

Classes of IPv4 address

Address Class	1st Octet range in decimal	1st Octet bits (Blue Dots do not change)	Network (N) and Host (H) Portion	Default mask (Decimal)	Number of possible networks and hosts per network
A	0–127	00000000 - 01111111	N.H.H.H	255.0.0.0	128 Nets (2^7) 16,777,214 hosts ($2^{24}-2$)
B	128–191	10000000 - 10111111	N.N.H.H	255.255.0.0	16,384 Nets (2^{14}) 65,534 hosts ($2^{16}-2$)
C	192–223	11000000 - 11011111	N.N.N.H	255.255.255.0	2,09,150 Nets (2^{21}) 254 hosts (2^8-2)
D	224–239	11100000 - 11101111	NA (Multicast)	-	-
E	240–255	11110000 - 11111111	NA (Experimental)	-	-

nesoacademy.org

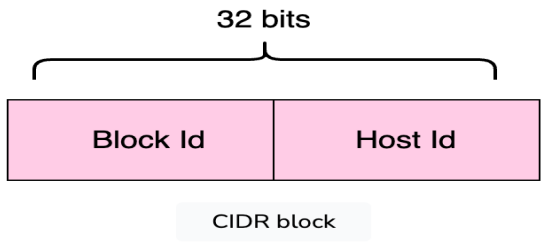
In Classful addressing, a large part of available addresses were wasted

Classless Addressing

- **Classless Inter-Domain Routing (CIDR)** is another name for classless addressing.
- This addressing type aids in the more efficient allocation of IP addresses.
- This technique assigns a block of IP addresses based on specified conditions when the user demands a specific amount of IP addresses. This block is known as a "CIDR block", and it contains the necessary number of IP addresses.

Structure

The CIDR block comprises two parts. These are as follows:



Block id is used for the network identification

Host id is used to identify the host part of the network.

Notation

CIDR IP addresses look as follows:

w.x.y.z/n

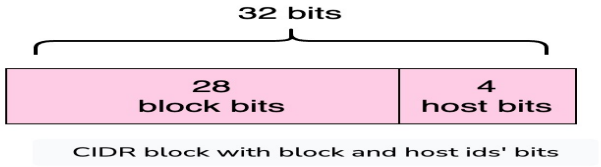
- In the example above *w,x,y,z* each defines an 8-bit binary number, while *n* tells us about the number of bits used to identify the network and is called an **IP network prefix** or **mask**.

Rules

- Addresses should be contiguous.
- The number of addresses in the block must be in the power of 2.
- The first address in the block can be found by setting the rightmost 32-n bits to 0s
- The last address in the block can be found by setting the rightmost 32-n bits to 1s

Given the following IP address, let's find the network and host bits.

- 200.56.23.41/28



CIDR block with block and host ids' bits

- $n_h=2^{32-n}$
- This particular case, in which *n* equals 28, represents the block id bits, so subtracting it with 32 leaves us with the total number of hosts expected in the network.
- $n_h=2^{32-28}$
- $n_h=2^4$

Therefore there are 16 hosts in this network

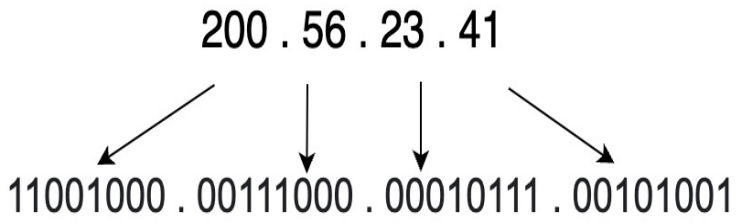
Subnet Mask

- The 32-bit IP address contains information about the host and its network. It is very necessary to distinguish both. For this, routers use Subnet Mask, which is as long as the size of the network address in the IP address. Subnet Mask is also 32 bits long. If the IP address in binary is ANDed with its Subnet Mask, the result yields the Network address.

Network address

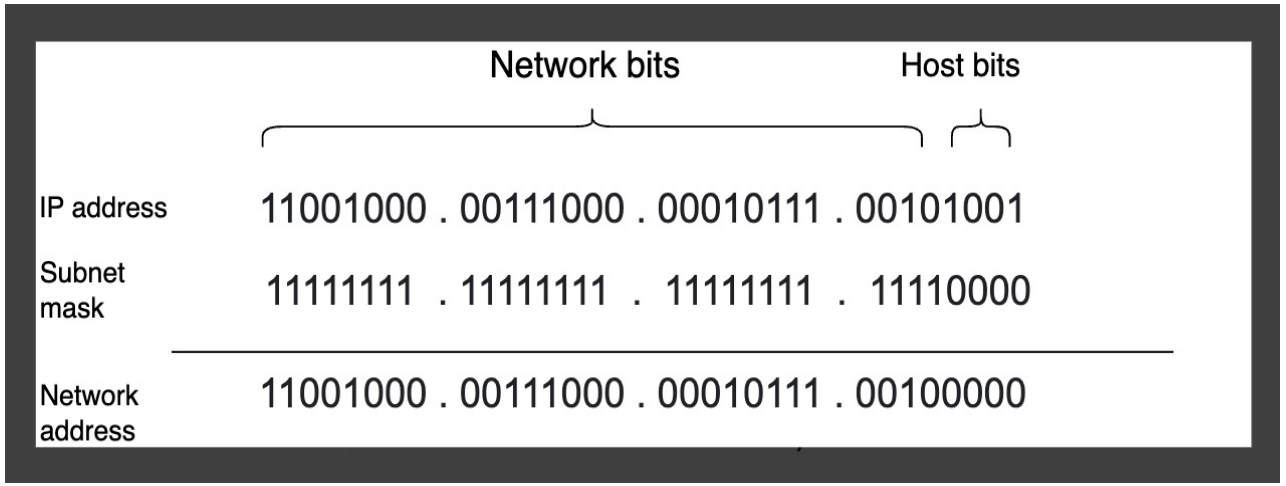
- To find the network address of a particular IP address, apply the AND operation to the IP address with its subnet mask. The subnet mask is obtained by making all the network bits 1 and host bits 0.

- To obtain the network address of the classless IP address 200.56.23.41/28, the following steps are needed:
- Convert the address into binary notation, as follows:

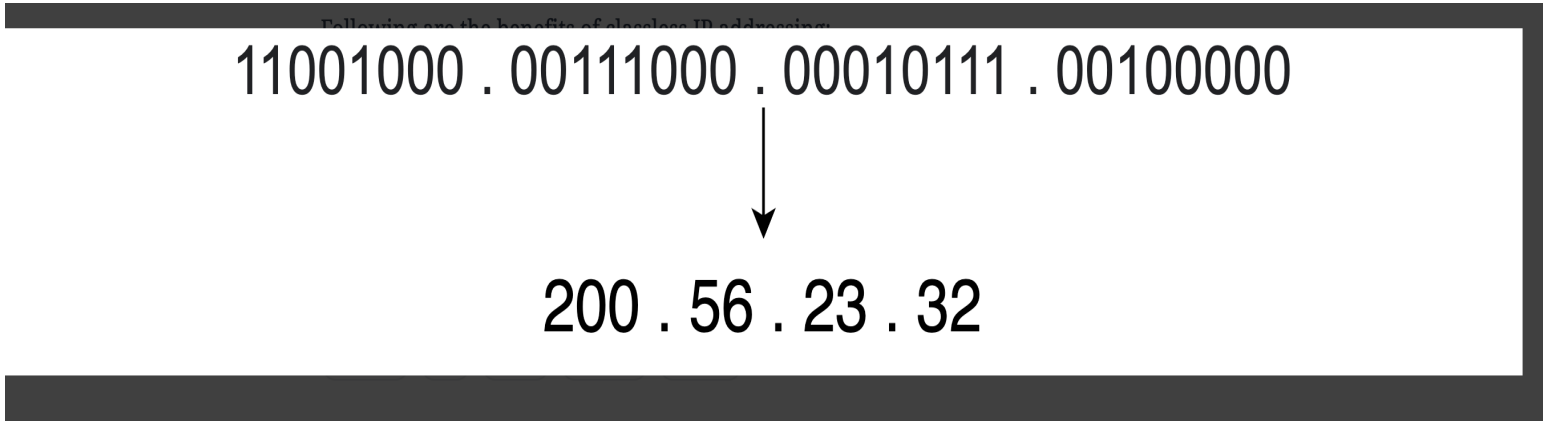


IP address into binary notation

Now apply the AND operation on the converted IP address and its subnet mask. The resultant will be the network address in binary format.



Convert the network address into decimal.



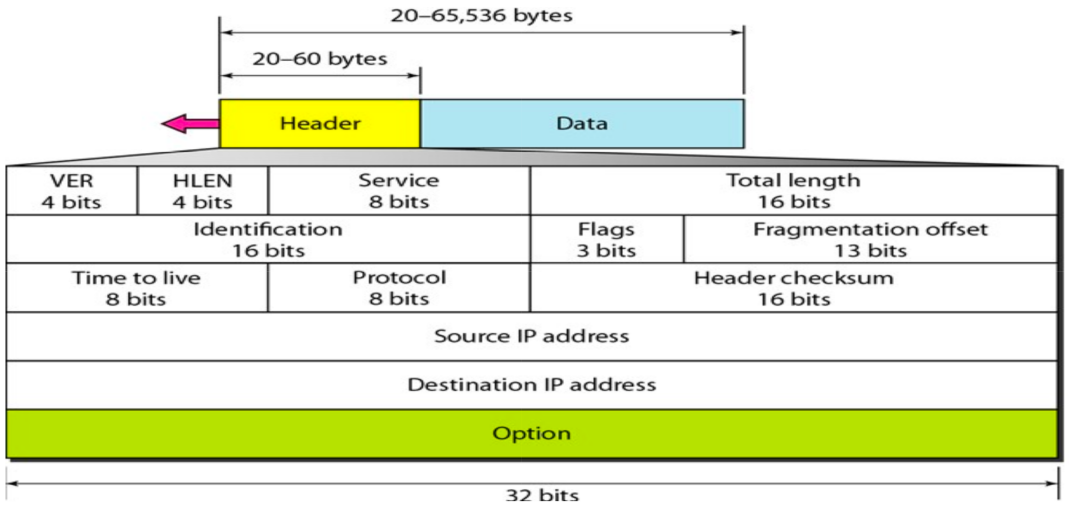
IPV4-Internet Protocol Version 4

- Internet Protocol being a layer-3 protocol (OSI) takes data Segments from layer-4 (Transport) and divides it into packets. IP packet encapsulates data unit received from above layer and add to its own header information.

(IP Encapsulation)

The encapsulated data is referred to as IP Payload. IP header contains all the necessary information to deliver the packet at the other end.

IPv4 datagram format



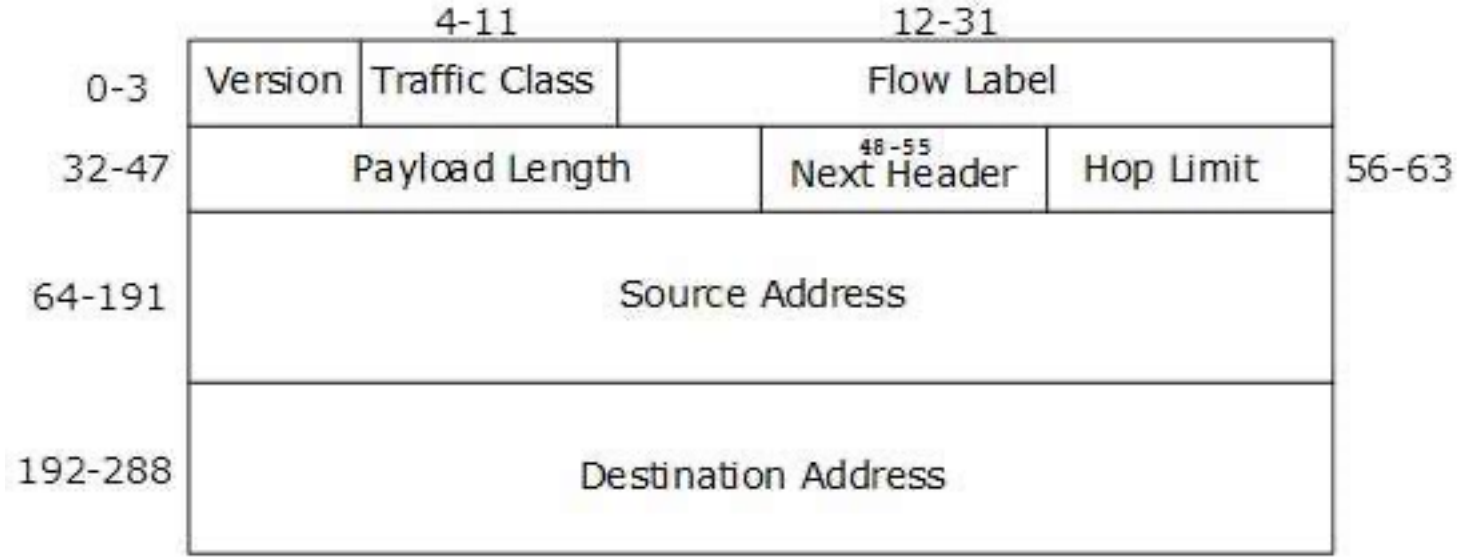
- **Version** – Version no. of Internet Protocol used (e.g. IPv4).
- **IHL** – Internet Header Length; Length of entire IP header.
- **Service DSCP** – Differentiated Services Code Point; this is Type of Service.

  ECN – Explicit Congestion Notification; It carries information about the congestion seen in the route.
- **Total Length** – Length of entire IP Packet (including IP header and IP Payload).
- **Identification** – If IP packet is fragmented during the transmission, all the fragments contain same identification number, to identify original IP packet they belong to.
- **Flags** – As required by the network resources, if IP Packet is too large to handle, these 'flags' tells if they can be fragmented or not.

- **Fragment Offset** − This offset tells the exact position of the fragment in the original IP Packet.
- **Time to Live** − To avoid looping in the network, every packet is sent with some TTL value set, which tells the network how many routers (hops) this packet can cross. At each hop, its value is decremented by one and when the value reaches zero, the packet is discarded.
- **Protocol** − Tells the Network layer at the destination host, to which Protocol this packet belongs to, i.e. the next level Protocol. For example protocol number of ICMP is 1, TCP is 6 and UDP is 17.
- **Header Checksum** − This field is used to keep checksum value of entire header which is then used to check if the packet is received error-free.
- **Source Address** − 32-bit address of the Sender (or source) of the packet.
- **Destination Address** − 32-bit address of the Receiver (or destination) of the packet.
- **Options** − This is optional field, which is used if the value of IHL is greater than 5. These options may contain values for options such as Security, Record Route, Time Stamp, etc.

IPV6

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



- IPv6 fixed header is 40 bytes long and contains the following information.

Version (4-bits): It represents the version of Internet Protocol, i.e. 0110.

Traffic Class (8-bits): These 8 bits are divided into two parts. The most significant 6 bits are used for Type of Service to let the Router Known what services should be provided to this packet. The least significant 2 bits are used for Explicit Congestion Notification (ECN).

Flow Label (20-bits): This label is used to maintain the sequential flow of the packets belonging to a communication.

Payload Length (16-bits): This field is used to tell the routers how much information a particular packet contains in its payload.

Next Header (8-bits): This field is used to indicate either the type of Extension Header

Hop Limit (8-bits): This field is used to stop packet to loop in the network infinitely. This is same as TTL in IPv4.

Source Address (128-bits): This field indicates the address of originator of the packet.

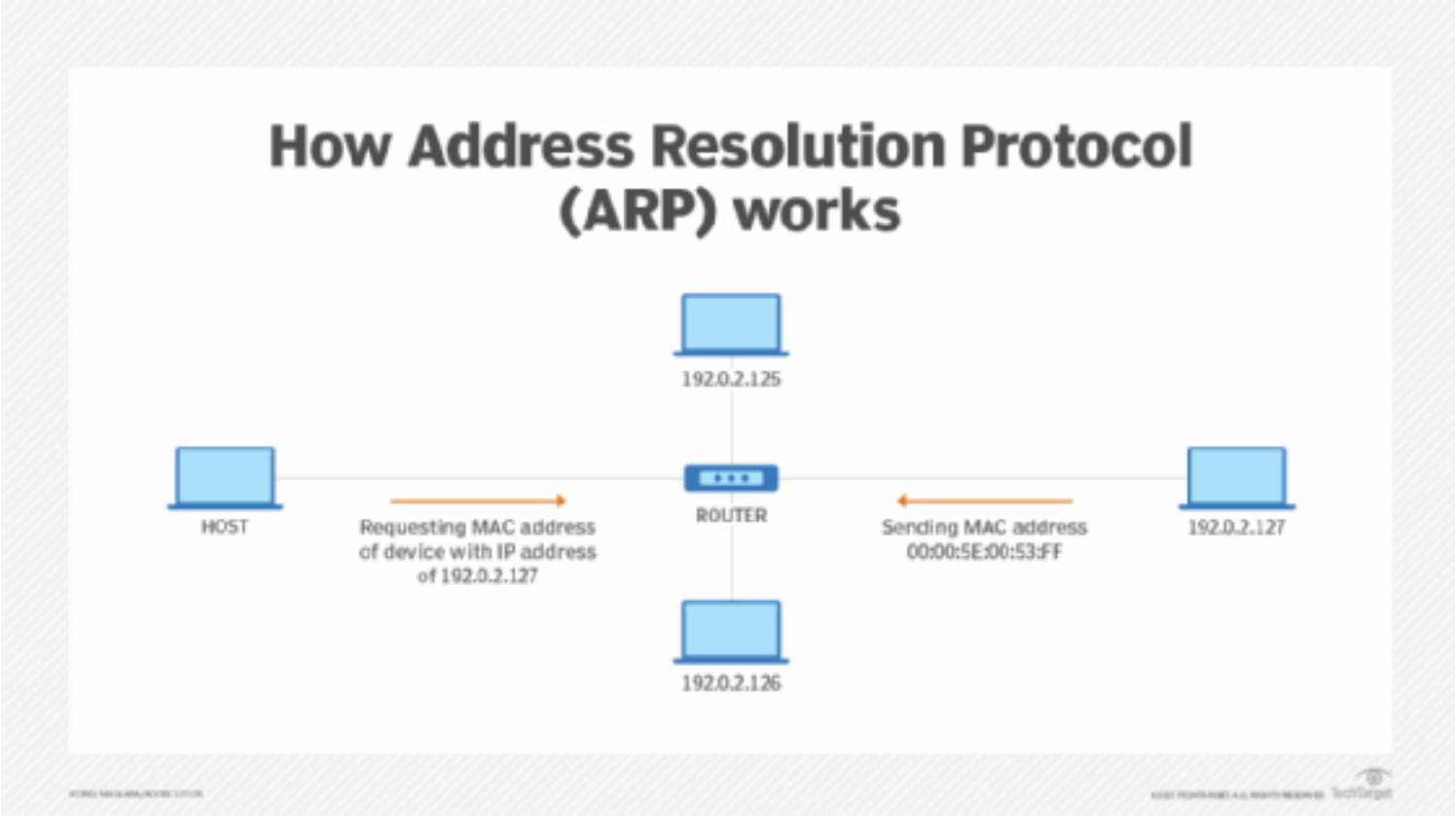
Destination Address (128-bits): This field provides the address of intended recipient of the packet.

Difference between IPV4 and IPV6

IPv4	IPv6
IPv4 stands for Internet Protocol Version 4.	IPv6 stands for Internet Protocol Version 6.
IPv4 uses numeric addressing.	IPv6 uses alphanumeric addressing.
IPv4 consists of 32-bits in the form of four octets.	IPv6 consists of 128-bits in the form of 8 segments.
IPv4 can generate 4 billion unique addresses.	IPv6 can generate over 340 un-decillion (3.4□10383.4x1038) unique addresses.
IPv4 uses periods (.) to separate the octets of the address.	IPv6 uses colons (:) to separate the segments of the address.
IPv4 can perform unicast, broadcast, and multicast.	IPv6 can perform unicast, anycast, and multicast. (No broadcasting).
IPv4 is divided into 5 classes ranging from class A to class E.	There are no classes in IPv6.
IPv4 header is large and contains 12 fields.	IPv6 has a smaller header consisting of 8 fields only.
IPv4 header length is 20-bits.	IPv6 header field is 40-bits.
IPv4 header contains checksum field.	IPv6 header does not contain the checksum field.
In the case of IPv4, the fragmentation is performed by the sending and forwarding routes.	In the case of IPv6, the fragmentation is performed by the sender itself.
IPv4 supports Variable Length Subnet Mask.	IPv6 does not support Variable Length Subnet Mask.

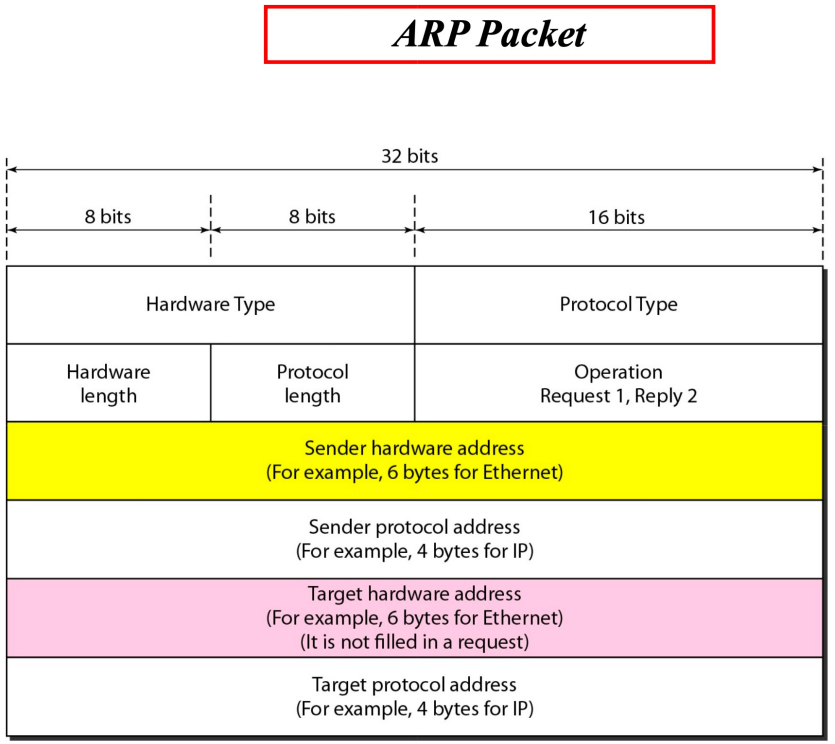
ARP-Address Resolution Protocol

- Address Resolution Protocol (ARP) is a procedure for mapping a dynamic IP address to a permanent physical machine address in a local area network (LAN). The physical machine address is also known as a media access control (**MAC)** address.
- The job of ARP is essentially to translate 32-bit addresses to 48-bit addresses and vice versa. This is necessary because IP addresses in IP version 4 (IPv4) are 32 bits, but MAC addresses are 48 bits.


How Address Resolution Protocol (ARP) works
192.0.2.125
HOST
Requesting MAC address of device with IP address of 192.0.2.127
ROUTER
Sending MAC address 00:00:5E:00:53:FF
192.0.2.127
192.0.2.126

- When an incoming packet destined for a host machine on a particular LAN arrives at a gateway, the gateway asks the ARP program to find a MAC address that matches the IP address.
- A table called the **ARP cache** maintains a record of each IP address and its corresponding MAC address.
- ARP broadcasts a request packet to all the machines on the LAN and asks if any of the machines are using that particular IP address. When a machine recognizes the IP address as its own, it sends a reply so ARP can update the cache

ARP Packet Format



Hardware type: This is 16 bits field defining the type of the network on which ARP is running. Ethernet is given type 1.

Protocol type: This is 16 bits field defining the protocol.

Hardware length: This is an 8 bits field defining the length of the physical address in bytes. Ethernet is the value 6.

Protocol length: This is an 8 bits field defining the length of the logical address in bytes. For the IPv4 protocol, the value is 4.

Operation (request or reply): This is a 16 bits field defining the type of packet. Packet types are ARP request (1), and ARP reply (2).

- **Sender hardware address:** This is a variable length field defining the physical address of the sender. For example, for Ethernet, this field is 6 bytes long.
- **Sender protocol address:** This is also a variable length field defining the logical address of the sender For the IP protocol, this field is 4 bytes long.
- **Target hardware address:** This is a variable length field defining the physical address of the target. For Ethernet, this field is 6 bytes long. For the ARP request messages, this field is all **0's** because the sender does not know the physical address of the target.
- **Target protocol address:** This is also a variable length field defining the logical address of the target. For the IPv4 protocol, this field is 4 bytes long.

RARP

Reverse Address Resolution Protocol (RARP) is a network-specific standard protocol. Some network hosts, such as a diskless workstation, do not know their own IP address when they are booted. To determine their own IP address, they use a mechanism similar to ARP

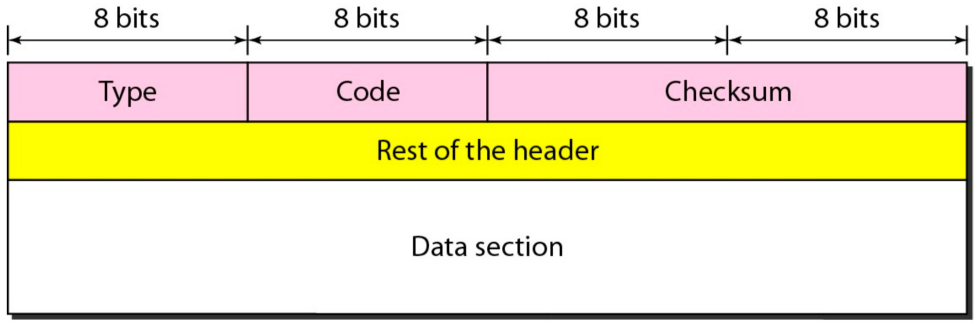
- The reverse address resolution is performed the same way as the ARP address resolution. The same packet format is used for the ARP.
- An exception is the operation code field that now takes the following values−
  - **3 for RARP request**
  - **4 for RARP reply**

Internet Control Message Protocol (ICMP)

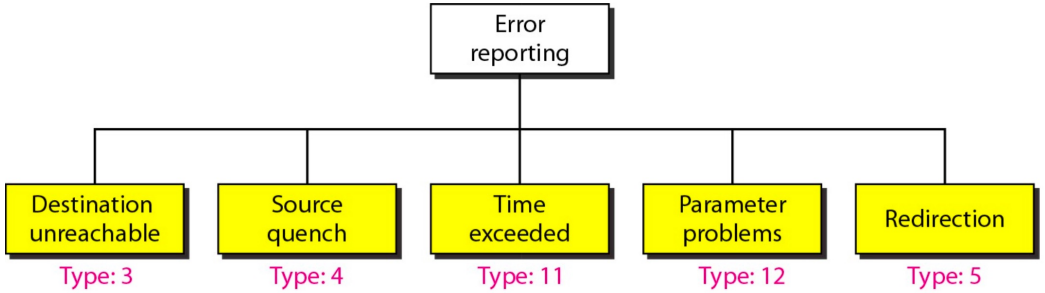
- Internet Control Message Protocol (ICMP) is a network layer protocol used to diagnose **communication errors** by performing an error control mechanism
- IP does not have an inbuilt mechanism for sending error and control messages. It depends on Internet Control Message Protocol(ICMP) to provide error control.
- ICMP packets are transmitted in the form of datagrams that contain an IP header with ICMP data. ICMP datagram is similar to a packet, which is an independent data entity.

ICMP Header

General format of ICMP messages



Type (8-bit): The initial 8-bit of the packet is for message type



- **Code (8-bit):** Code is the next 8 bits of the ICMP packet format, this field carries some additional information about the error message and type.

- **Checksum (16-bit):** Last 16 bits are for the checksum field in the ICMP packet header. The checksum is used to check the number of bits of the complete message and enable the ICMP tool to ensure that complete data is delivered.
- The next 32 bits of the ICMP Header are **Extended Header** which has the work of pointing out the problem in IP Message.
- The last part of the ICMP packet is Data or Payload of variable length.

Types of ICMP messages

- **Information Messages** – In this message, the sender sends a query to the host or router and expects an answer. For example, A host wants to know if a router is alive or not.
- **Error-reporting message** – This message report problems that a router or a host (destination) may encounter when it processes an IP packet.
- **Query Message** – It helps a router or a network manager to get specific information from a router or another host.

Category	Type	Message
Error-Reporting Messages	3	Destination unreachable
	4	Source quench
	11	Time Exceeded
	12	Parameter Problem
	5	Redirection
Query Message	8 or 0	Echo request or reply
	13 or 14	Timestamp request or reply
	17 or 18	Address mask request or reply
	10 or 9	Router Solicitation or advertisement

Echo-request and echo-reply message

- A router or a host can send an echo-request message. It is used to ping a message to another host that "Are you alive". If the other host is alive, then it sends the echo-reply message.

Timestamp-request and timestamp-reply message

- The timestamp-request and timestamp-reply messages are also a type of query messages. Suppose the computer A wants to know the time on computer B, so it sends the timestamp-request message to computer B. The computer B responds with a timestamp-reply message.

Address Mask Request

- The ICMP Address Mask Request and Address Mask Reply query messages provide a host with the ability to determine the subnet mask in use on the local network.

Router Solicitation

- The ICMP Router Solicitation message is sent from a computer host to any routers on the local area network to request that they advertise their presence on the network.