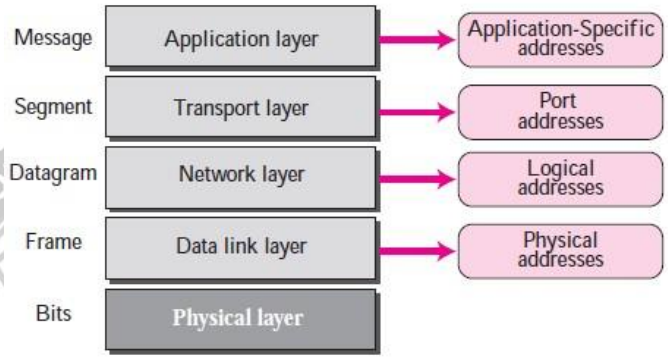
UNIT I

FOUNDATIONS OF COMPUTER NETWORKS

Addresses used in the TCP/IP protocol.

Four levels of addresses are used in the TCP/IP protocol: physical address, logical address, port address, and application-specific address as shown in Figure.



Physical Addresses

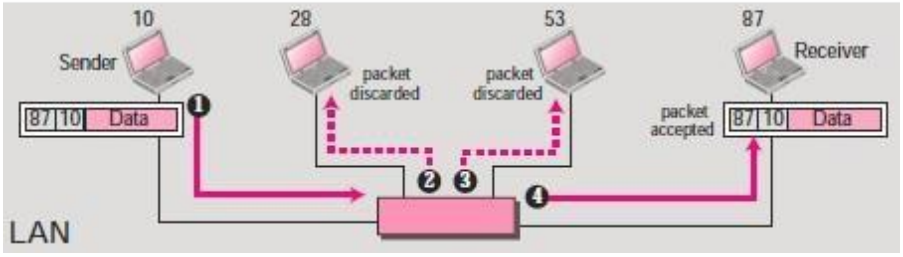
- The physical address, also known as the link address, is the address of a node as defined by its LAN or WAN.
- The size and format of these addresses vary depending on the network. For example, Ethernet uses a 6-byte (48-bit) physical address.
- Physical addresses can be either unicast (one single recipient), multicast (a group of recipients), or broadcast (to be received by all systems in the network.
- Example: Most local area networks use a 48-bit (6-byte) physical address written as

  12 hexadecimal digits; every byte (2 hexadecimal digits) is separated by a colon, as shown below: A 6-byte (12 hexadecimal digits) physical address 07:01:02:01:2C:4B

07:01:02:01:2C:4B
A 6-byte (12 hexadecimal digits) physical address

In Figure below a node with physical address 10 sends a frame to a node with physical address 87. The two nodes are connected by a link (a LAN). At the data link layer, this frame contains physical (link) addresses in the header. These are the only addresses needed. The rest of the header contains other information needed at this level. The trailer usually contains extra bits needed for error detection. The data link layer at the sender receives data from an upper layer. It encapsulates the data in a frame, adding a header and a trailer. The header, among other pieces of information, carries the receiver and the sender physical (link) addresses.

Note that in most data link protocols, the destination address 87 in this case, comes before the source address (10 in this case). The frame is propagated through the LAN. Each station with a physical address other than 87 drops the frame because the destination address in the frame does not match its own physical address. The intended destination computer, however, finds a match between the destination address in the frame and its own physical address. The frame is checked, the header and trailer are dropped, and the data part is decapsulated and delivered to the upper layer.



Unicast, Multicast, and Broadcast Physical Addresses

Physical addresses can be either unicast (one single recipient), multicast (a group of recipients), or broadcast (to be received by all systems in the network). Some networks support all three addresses.

A source address is always a unicast address—the frame comes from only one station. The destination address, however, can be unicast, multicast, or broadcast. The least significant bit of the first byte defines the type of address.

Q: Define the type of the following destination addresses:

1. 4A:30:10:21:10:1A
2. 47:20:1B:2E:08:EE
3. FF:FF:FF:FF:FF:FF

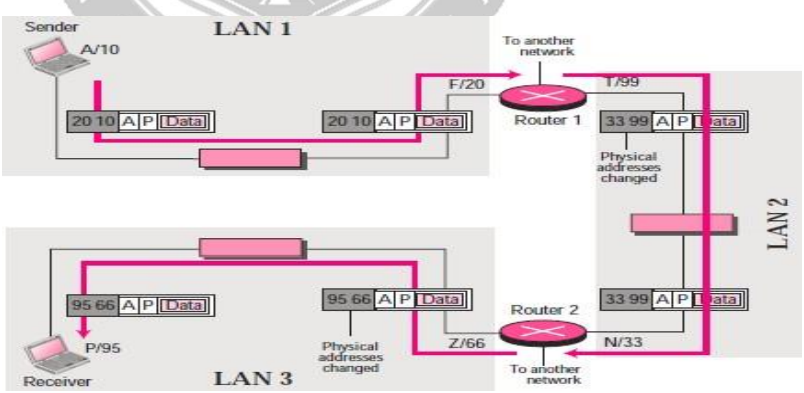
Logical Addresses

- Logical addresses are used by networking software to allow packets to be independent of the physical connection of the network, that is, to work with different network topologies and types of media.
- A logical address in the Internet is currently a 32-bit address that can uniquely define a host connected to the Internet. An internet address in IPv4 in decimal numbers 132.24.75.9
- No two publicly addressed and visible hosts on the Internet can have the same IP address.
- The physical addresses will change from hop to hop, but the logical addresses remain the same.
- The logical addresses can be either unicast (one single recipient), multicast (a group of recipients), or broadcast (all systems in the network). There are limitations on broadcast addresses.

- Logical addresses are necessary for universal communications that are independent of underlying physical networks. Physical addresses are not adequate in an internetwork environment where different networks can have different address formats. A universal addressing system is needed in which each host can be identified uniquely, regardless of the underlying physical network. The logical addresses are designed for this purpose. A logical address in the Internet is currently a 32- bit address that can uniquely define a host connected to the Internet. No two publicly addressed and visible hosts on the Internet can have the same IP address.

Example (2)

- The Figure below shows a part of an internet with two routers connecting three LANs. Each device (computer or router) has a pair of addresses (logical and physical) for each connection. In this case, each computer is connected to only one link and therefore has only one pair of addresses. Each router, however, is connected to three networks (only two are shown in the figure). So each router has three pairs of addresses, one for each connection. Although it may be obvious that each router must have a separate physical address for each connection, it may. The computer with logical address A and physical address 10 needs to send a packet to the computer with logical address P and physical address 95. The sender encapsulates its data in a packet at the network layer and adds two logical addresses (A and P). Note that in most protocols, the logical source address comes before the logical destination address (contrary to the order of physical addresses). The network layer, however, needs to find the physical address of the next hop before the packet can be delivered. The network layer consults its routing table and finds the logical address of the next hop (router 1) to be F.



- Another protocol, Address Resolution Protocol (ARP) finds the physical address of router 1 that corresponds to its logical address (20). Now the network layer passes this address to the data link layer, which in turn, encapsulates the packet with physical destination address 20 and physical source address 10. The router decapsulates the packet from the frame to read the logical destination address P. Since the logical destination address does not match the router's logical address, the router knows that the packet needs to be forwarded. The router consults its routing table and ARP to find the physical destination

address of the next hop (router 2), creates a new frame, encapsulates the packet, and sends it to router 2.

- Note the physical addresses in the frame. The source physical address changes from

10 to 99. The destination physical address changes from 20 (router 1 physical address) to 33 (router 2 physical address). The logical source and destination addresses must remain the same; otherwise the packet will be lost. At router 2 we have a similar scenario. The physical addresses are changed, and a new frame is sent to the destination computer. When the frame reaches the destination, the packet is decapsulated. The destination logical address P matches the logical address of the computer. The data are decapsulated from the packet and delivered to the upper layer. Note that although physical addresses will change from hop to hop, logical addresses remain the same from the source to destination.

The physical addresses will change from hop to hop, but the logical addresses remain the same.

Unicast, Multicast, and Broadcast Addresses

The logical addresses can be either unicast (one single recipient), multicast (a group of recipients), or broadcast (all systems in the network).

Port Addresses

- There are many application running on the computer. Each application run with a port no.(logically) on the computer.
- A port number is part of the addressing information used to identify the senders and receivers of messages.
- Port numbers are most commonly used with TCP/IP connections.
- These port numbers allow different applications on the same computer to share network resources simultaneously.
- The physical addresses change from hop to hop, but the logical and port addresses usually remain the same.
- Example: a port address is a 16-bit address represented by one decimal number 753

The IP address and the physical address are necessary for a quantity of data to travel from a source to the destination host. However, arrival at the destination host is not the final objective of data communications on the Internet. Computers are devices that can run multiple processes at the same

time. The end objective of Internet communication is a process communicating with another process. For example, computer A can communicate with computer C by using TELNET. At the same time, computer A communicates with computer B by using the File Transfer Protocol (FTP). For these processes to receive data simultaneously, we need a method to label the different processes.

In other words, they need addresses. In the TCP/IP architecture, the label assigned to a process is called a port address. A port address in TCP/IP is 16 bits in length.

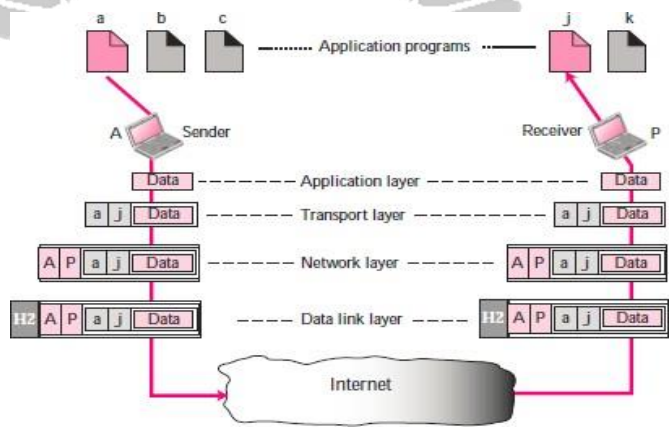
A port address is a 16-bit address represented by one decimal number as shown.

753

A 16-bit port address represented as one single number

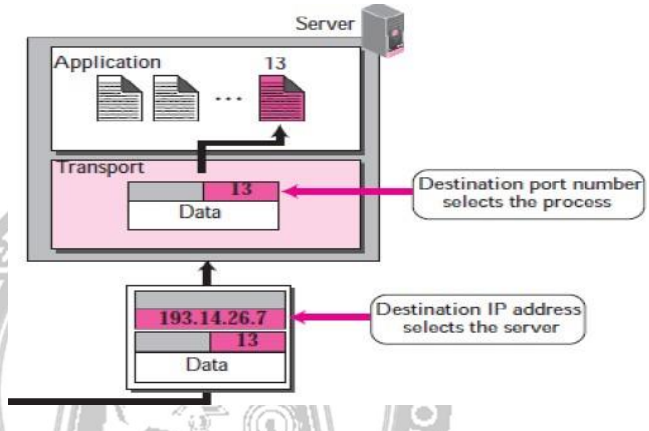
Example (3)

The following Figure shows two computers communicating via the Internet. The sending computer is running three processes at this time with port addresses a, b, and c. The receiving computer is running two processes at this time with port addresses j and k. Process a in the sending computer needs to communicate with process j in the receiving computer. Note that although both computers are using the same application, FTP, for example, the port addresses are different because one is a client program and the other is a server program.



To show that data from process a need to be delivered to process j, and not k, the transport layer encapsulates data from the application layer in a

packet and adds two port addresses (a and j), source and destination. The packet from the transport layer is then encapsulated in another packet at the network layer with logical source and destination addresses (A and P). Finally, this packet is encapsulated in a frame with the physical source and destination addresses of the next hop. We have not shown the physical addresses because they change from hop to hop inside the cloud designated as the Internet. Note that although physical addresses change from hop to hop, logical and port addresses remain the same from the source to destination.



- In the TCP/IP protocol suite, the port numbers are integers between 0 and 65,535.
- The client program defines itself with a port number, called the ephemeral port number (chosen randomly). The word ephemeral means short lived.
- The server process must also define itself with a port number (called well-known port numbers). This port number, however, cannot be chosen randomly.

ICANN Ranges (Internet Corporation for Assigned Names and Numbers)

ICANN has divided the port numbers into three ranges: well-known, registered, and dynamic (or private)

- Well-known ports: The ports ranging from 0 to 1,023 are assigned and controlled by ICANN..

- Registered ports: The ports ranging from 1,024 to 49,151 are not assigned or controlled by ICANN. They can only be registered with ICANN to prevent duplication.

Dynamic ports: The ports ranging from 49,152 to 65,535 are neither controlled nor registered. They can be used as temporary or private port numbers. The original recommendation was that the ephemeral port numbers for clients be chosen from this range. However, most systems do not follow this recommendation.

Application-Specific Addresses

- Some applications have user-friendly addresses that are designed for that specific application.
- Examples include the e-mail address (for example, forouzan@fhda.edu) and the Universal Resource Locator (URL) (for example, www.mhhe.com). The first defines the recipient of an e-mail; the second is used to find a document on the World Wide Web.

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.

TCP/IP Addressing Scheme:

TCP/IP uses a 32 bit addressing scheme to identify the devices on a network. These 32 bits are divided into four octets, of eight bits each. Each of these four octets is represented in a decimal form, and separated by a dot. For example, 198.172.168.10 is an IP address. This format of representing IP address is called the dotted decimal format.

The octets in an IP address can take a decimal value from 9 to 255 because the largest decimal value that can be represented by eight binary bits is 255(11111111 in binary). For example, the 32 bit binary address 11000110.10101100.1010100.0001010 represents the IP address 198.172.168.10.

The addressing provided by a network layer protocol to a device is called its network address. For example, 198.172.168.10 is the network address of a device. This is different from the MAC address which is the hardware address of the NIC or the device (routers or switch). The network addresses in a TCP/IP network are also known as IP addresses. Therefore, 198.172.168.10 is also known as the IP address.

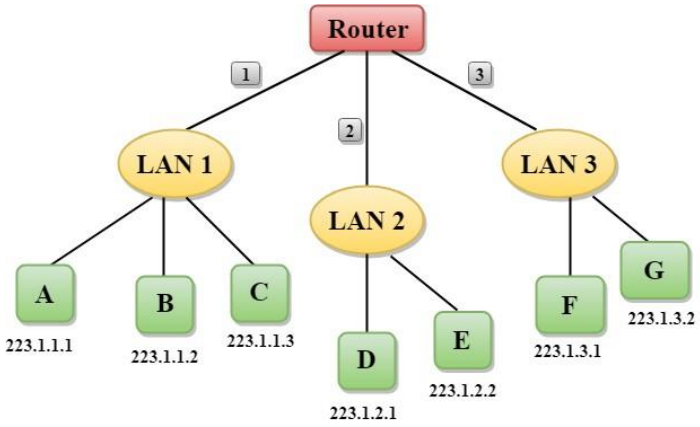
Components of IP address:

For continence sake we use IP address dotted-decimal notation, while the computer converts this into binary. However, even though these sets of 32 bits are considered a single
–they have an internal structure containing two components:

- Network Identifier (Network ID): A certain number of bits, starting from the left- most bit, is used to identify the network where the host or other network interface is located. This is also sometimes called the network prefix or even just the prefix. This is the address of the network itself, and is used by other networks to identify this network.

- Host Identifier (Host ID): The remainder of the bits is used to identify the host on the network. This is the address of the device with in the network.

The fundamental division of the bits of an IP address is into a network ID and host ID. Here, the network ID is 8 bits long and the host ID is 24 bits in length.



- In the above figure, a router has three interfaces labeled as 1, 2 & 3 and each router interface contains its own IP address.
- Each host contains its own interface and IP address.
- All the interfaces attached to the LAN 1 is having an IP address in the form of
  223.1.1.xxx, and the interfaces attached to the LAN 2 and LAN 3 have an IP address in the form of 223.1.2.xxx and 223.1.3.xxx respectively.
- Each IP address consists of two parts. The first part (first three bytes in IP address) specifies the network and second part (last byte of an IP address) specifies the host in the network.

Classful Addressing

IP Address Classes:

Internet addresses are allocated by the InterNIC the organization that administers the internet. These IP addresses are divided into classes. The most common of these are classes A, B, and C. Classes D and E exist, but are not generally used by end users. Each of the address classes has a different default subnet mask. You can identify the class of an IP address by looking at its first octet. Following are the ranges of class A, B and C Internet addresses, each with an example address:

· Class A networks use a default subnet mask of 255.0.0.0 and have 0-127 as their first octet. The address 10.52.36.11 is a class A address. Its first octet is 10, which is between 1 and 126, inclusive.

· Class B networks use a default subnet mask of 255.255.0.0 and have 128-191 as their first octet. The address 172.16.52.63 is a class B address. Its first octet is 172, which is between 128 and 191, inclusive.

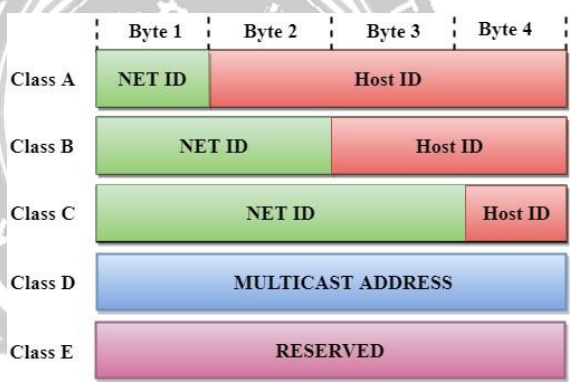
· Class C networks use a default subnet mask of 255.255.255.0 and have 192-223 as their first octet. The address 192.168.123.132 is a class C address. Its first octet is
192, which is between 192 and 223, inclusive.

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 = 2^7 = 128 network address

The total number of hosts in Class A = 2^{24} - 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 = 2^{14} = 16384 network address

The total number of hosts in Class B = 2^{16} - 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 = 2^{21} = 2097152
network address
The total number of hosts = 2^{8} - 2 = 254 host
address

Clas s 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.

Cla ss 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.

Rules for assigning Host ID:

The Host ID is used to determine the host within any network. The Host ID is assigned based on the following rules:

- The Host ID must be unique within any network.
- The Host ID in which all the bits are set to 0 cannot be assigned as it is used to represent the network ID of the IP address.
- The Host ID in which all the bits are set to 1 cannot be assigned as it is reserved for the multicast address.

Rules for assigning Network ID:

If the hosts are located within the same local network, then they are assigned with the same network ID. The following are the rules for assigning Network ID:

- The network ID cannot start with 127 as 127 is used by Class A.

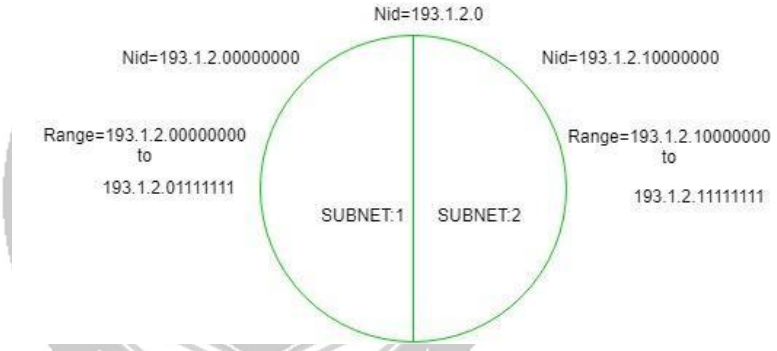
- The Network ID in which all the bits are set to 0 cannot be assigned as it is used to specify a particular host on the local network.
- The Network ID in which all the bits are set to 1 cannot be assigned as it is reserved for the multicast address.

Introduction To Subnetting

When a bigger network is divided into smaller networks, in order to maintain security, then

that is known as Subnetting. so, maintenance 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.



IP Subnetting:

Subnets are an efficient method for logically dividing a network into segments, such that the network performance is optimized. Subnets are defined as the segments of a network that use schemes different from one another but corresponding to the addressing schemes different from one another but corresponding to the addressing scheme used by the main network. Therefore, devices in one subnet cannot directly communicate with devices represented by 192.168.30.0, in which 192.168.30 represents the network address, and the value in the fourth octet would represent the host on the network. For example, the address of a particular host in this network would be 192.168.30.4. The fourth octet in a Class C address can take a value between 0 and 225, and therefore, this network can have up to 256 hosts. However, configuring 255 components in a single network would significantly degrade the performance of the network as well as the network router. Therefore, the network, 192.168.30.x can be divided into subnets, with each subnet consisting of, say, 16 computers.

On a network without subnets, a device outside the network can identify a host eith the help of the network and host addresses. On a network with subnets, however, an additional piece of information, called the subnet mask, is needed to identify a host. The network address helps determine the network in which is located, whereas the subnet mask responsible for locating the subnet on the network to which the host belongs. The host address identifies the individual host.

However, the addressing scheme used by IP has only four octets that can be used to represent the network address or the host depending on the IP address class. It is not possible to include information on the subnet in the IP address itself, and therefore, the subnet mask is a separate 32bit address, accompanying the IP address of a device.

The default subnet mask values for a class A, class B, class C IP addresses are listed in
Table.

IP Address Class	Default Subnet Mask
Class A	255.0.0.0
Class B	255.255.0.0
Class C	255.255.255.0

The default subnet masks are used when a network does not have any subnets. For creating subnets, the default values are modified to obtain customized, only the octets that denote the host address are modified, and not the octet(s) that represent the network address. For example 255.244.0.0 is a valid subnet mask for a class A network but not
252.124.0.0 in fact, 252.124.0.0 is not a valid subnet mask for a network of any IP address class.

The subnet masks and IP addresses on the network are dependent on one another because of network that belongs to a particular IP addresses class can accommodate only a particular number of devices irrespective of the number of subnets. For example, a class B network can have a maximum of only 65,536 devices irrespective of the number subnets that are created. Therefore, the subnet mask values are derived from the IP address of the network. Fig. 6.19, represents divided to depict the subnet address.

As represented in Fig.6.19, the bits of the octet (s) representing the host address are subdivided to represent the subnet address and the host address. For example, In class C IP address, the bits of the last octet represent the subnet address as well as the host address. The number of bits used by the subnet address, and the number of bits used by the host address are determined by the

subnet mask. The following sub-topic explains the steps involved in creating subnets.

Supernetting in Network Layer

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

There are some points which should be kept in mind while supernetting:

1. All the Networks should be contiguous.
2. The block size of every networks should be equal and must be in form of 2^n.
3. First Network id should be exactly divisible by whole size of supernet.

Example – Suppose 4 small networks of class C:

200.1.0.0,

200.1.1.0,

200.1.2.0,

200.1.3.0

Build a bigger network which have a single Network Id.

Explanation – Before Supernetting routing table will be look like as:

NETWORK ID	SUBNET MASK	INTERFACE
200.1.1.0	255.255.255.0	B
200.1.2.0	255.255.255.0	C
200.1.3.0	255.255.255.0	D

First, lets check whether three condition are satisfied or not:

1. Contiguous: You can easily see that all network are contiguous all having size 256 hosts.
   Range of first Network from 200.1.0.0 to 200.1.0.255. If you add 1 in last IP address of first network that is 200.1.0.255 + 0.0.0.1, you will get the next network id that is
   200.1.1.0. Similarly, check that all network are contiguous.
2. Equal size of all network: As all networks are of class C, so all of the have a size of
   256 which in turn equal to 2^8.
3. First IP address exactly divisible by total size: When a binary number is divided by
   2^n then last n bits are the remainder. Hence in order to prove that first IP address is exactly divisible by while size of Supernet Network. You can check that if last n v=bits
   are 0 or not.
   In given example first IP is 200.1.0.0 and whole size of supernet is $4*2^8 = 2^{10}$. If last 10 bits of first IP address are zero then IP will be divisible.

11001000	00000001	00000000	00000000
200	1	0	0

Last 10 bits of first IP address are zero (highlighted by green color). So 3rd condition is also satisfied.

Therefore, you can join all these 4 networks and can make a Supernet. New Supernet Id will be 200.1.0.0.

Advantages of Supernetting –

1. Control and reduce network traffic
2. Helpful to solve the problem of lacking IP addresses
3. Minimizes the routing table

Disadvantages of Supernetting –

- It cannot cover different area of network when combined
- All the networks should be in same class and all IP should be contiguous

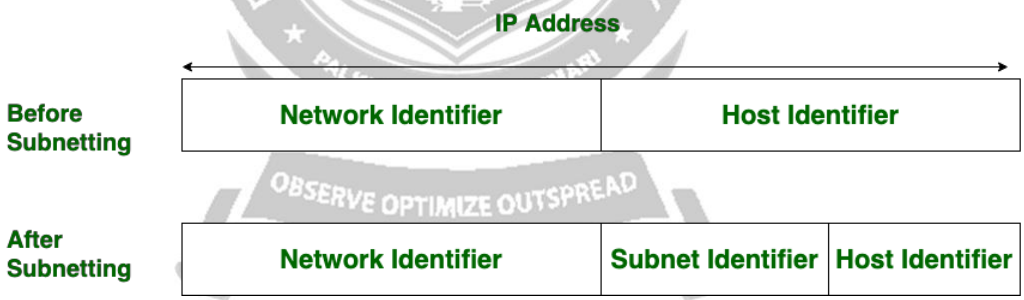
- Difference between Subnetting and Supernetting

Subnetting:

Subnetting is the procedure to divide the network into sub-networks or small networks.

Supernetting:

Supernetting is the procedure of combine the small networks into larger space. In subnetting, Network addresses's bits are increased. on the other hand, in subnetting, Host addresses's bits are increased. Subnetting is implemented via Variable-length subnet masking, While supernetting is implemented via Classless interdomain routing.



Difference between Subnetting and Supernetting:

S.N	SUBNE	SUPERN
1.	Subnetting is the procedure to divide the	While supernetting is the procedure of combine the
2.	In subnetting, Network addresses's	While in subnetting, Host addresses's bits are
3.	In subnetting, The mask bits are moved towards	While In supernetting, The mask bits are moved
4.	Subnetting is implemented via Variable-length subnet	While supernetting is implemented via Classless

5.	In subnetting, Address depletion is reduced or	While It is used for simplify routing process

IPv4 datagram format

The Internet Protocol version 4 (IPv4) is a protocol for use on packet-switched Link Layer networks (e.g. Ethernet). IPv4 provides an addressing capability of approximately 4.3 billion addresses.

- Version number: These 4 bits specify the IP protocol version of the datagram. It determines how to interpret the header. Currently the only permitted values are 4 (0100) or 6 (0110).
- Header length: Specifies the length of the IP header, in 32-bit words.
- Type of service: The type of service (TOS) bits were included in the IPv4 header to allow different types of IP datagrams (for example, datagrams particularly requiring low delay, high throughput, or reliability) to be
- distinguished from each other.
- Datagram length: This is the total length of the IP datagram (header plus data), measured in bytes.
- Identifier: Uniquely identifies the datagram. It is incremented by 1 each time
- a datagram is sent. All fragments of a datagram contain the same identification value. This allows the destination host to determine which fragment belongs to which datagram.
- Flags: In order for the destination host to be absolutely sure it has received the last fragment of the original datagram, the last fragment has a flag bit set to 0, whereas all the other fragments have this flag bit set to 1.
- Fragmentation offset: When fragmentation of a message occurs, this field specifies the offset, or position, in the overall message where the data in this fragment goes. It is specified in units of 8 bytes (64 bits).

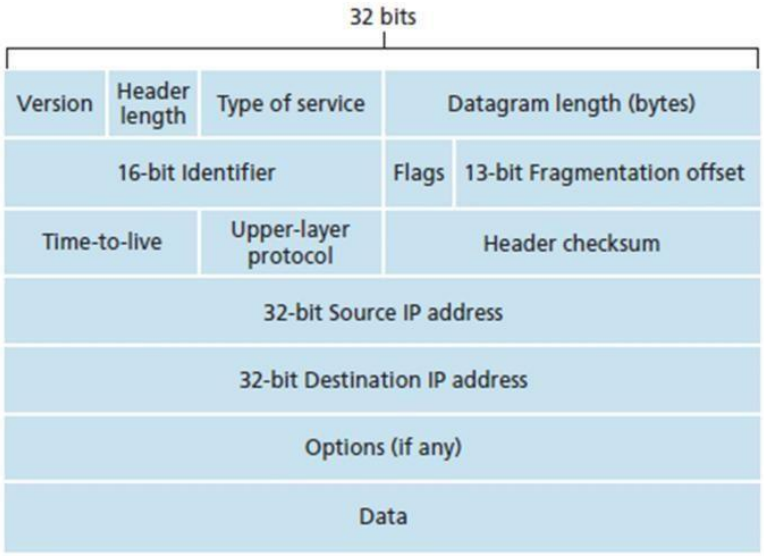


Fig. 7 IPv4 datagram format

- Time-to-live: Specifies how long the datagram is allowed to ―live‖ on the network. Each router decrements the value of the TTL field (reduces it by one) prior to transmitting it. If the TTL field drops to zero, the datagram is assumed to have taken too long a route and is discarded.
- Protocol: This field is used only when an IP datagram reaches its final destination. The value of this field indicates the specific transport-layer protocol to which the data portion of this IP datagram should be passed. For example, a value of 6 indicates that the data portion is passed to TCP, while a value of 17 indicates that the data is passed to UDP.
- Header checksum: The header checksum aids a router in detecting bit errors in a received IP datagram.
- Source and destination IP addresses: When a source creates a datagram, it inserts its IP address into the source IP address field and inserts the address of the ultimate destination into the destination IP address field.
- Options: The options fields allow an IP header to be extended.
- Data (payload): The data to be transmitted in the datagram, either an entire higher-layer message or a fragment of one.
- IP addressing: introduction
- IP address: It is 32-bit identifier for host, router interface
- Interface: It is a connection between host/router and physical link. A router's typically have multiple interfaces A host typically has one or two interfaces

- There is an IP addresses associated with each interface.
- Subnets: To determine the subnets, detach each interface from its host or router, creating islands of isolated networks, with interfaces terminating the end points of the isolated networks. Each of these isolated networks is called a subnet.
- Subnet part: high order bits defines subnet
- Host part: low order bits defines host.

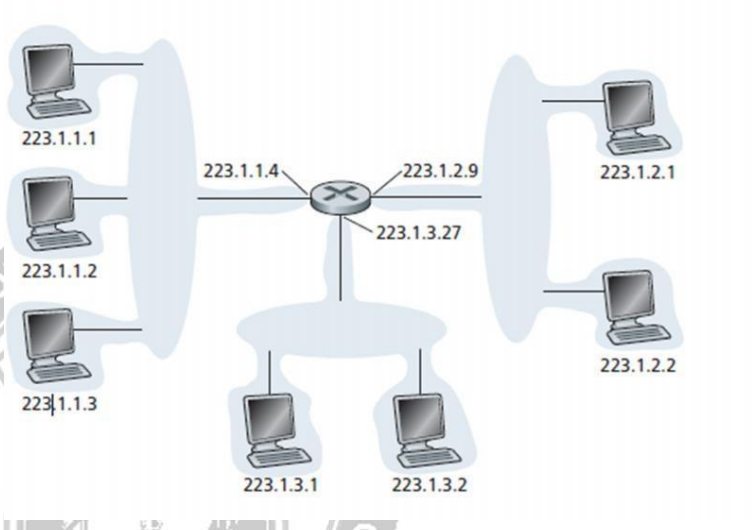


Fig. 8 Interface addresses and subnets

IPv6 Datagram Format

The Internet Protocol version 6 (IPv6) is more advanced and has better features compared to IPv4.

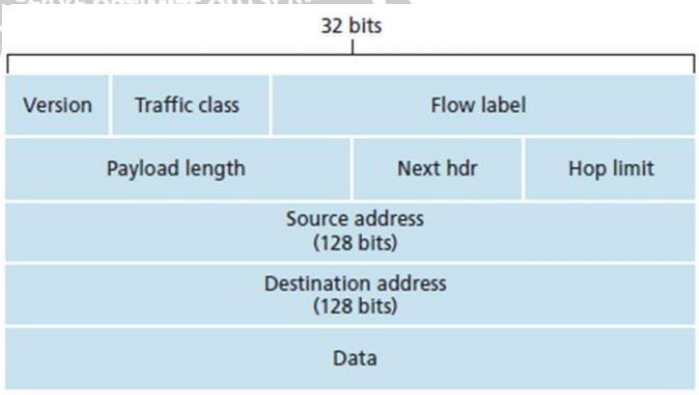


Fig. 12 IPv6 datagram format

- Version: The size of the Version field is 4 bits. The Version field shows the version of IP and is set to 6.

- Traffic Class: The size of Traffic Class field is 8 bits. Traffic Class field is similar to the IPv4 Type of Service (ToS) field. The Traffic Class field indicates the IPv6 packet's class or priority.
- Flow Label: The size of Flow Label field is 20 bits. The Flow Label field provide additional support for real-time datagram delivery and quality of service features. The purpose of Flow Label field is to indicate that this packet belongs to a specific sequence of packets between a source and destination and can be used to prioritized delivery of packets for services like voice.
- Payload Length: The size of the Payload Length field is 16 bits. The Payload Length field shows the length of the IPv6 payload, including the extension headers and the upper layer protocol data
- Next Header: The size of the Next Header field is 8 bits. The Next Header field shows either the type of the first extension (if any extension header is available) or the protocol in the upper layer such as TCP, UDP, or ICMPv6.
- Hop Limit: The size of the Hop Limit field is 8 bits The Hop Limit field shows the maximum number of routers the IPv6 packet can travel. This Hop Limit field is similar to IPv4 Time to Live (TTL) field.
- Source Address: The size of the Source Address field is 128 bits. The Source Address field shows the IPv6 address of the source of the packet.
- Destination Address: The size of the Destination Address field is 128 bits. The Destination Address field shows the IPv6 address of the destination of the packet.
- Data: The data to be transmitted in the datagram, either an entire higher-layer message or a fragment of one.

Difference between IPv4 and IPv6

IPv4	IPv6
IPv4 addresses are 32 bit length.	IPv6 addresses are 128 bit length.
Fragmentation done by sender is forwarding	Fragmentation is done only by sender.
No packet flow identification.	Packet flow identification is available within the
Checksum field is available in	No checksum field in header.
Options fields are available in header.	No option fields, but Extension headers are

Address Resolution Protocol (ARP)is available to map IPv4	Address Resolution Protocol (ARP) is replaced with
Broadcast messages are available.	Broadcast messages are not
Manual configuration (Static) of IP addresses or DHCP (Dynamic configuration)	Auto-configuration of addresses is available.