UNIT-2 COMPUTER NETWORKS NOTES

Internetworking in Computer Network

In internetworking, routers are aware of each other's addresses as well as addresses outside of their network. They have two options: they can be statically set to operate on various networks, or they can learn by utilising the internetworking routing protocol.

What is Internetworking in a Computer Network?

The word "internetworking," which combines the words "inter" and "networking," denotes a connection between completely distinct nodes/segments. This connection is made possible by intermediary hardware like routers or gateways. Catenet was the initial title for associate degree internetwork. Private, public, commercial, industrial, and governmental networks frequently connect to one another. Therefore, a degree of internetwork could be a collection of several networks that operate as a single large network and are connected by intermediate networking devices. The trade, goods, and methods used to address the difficulty of creating and managing internet works are referred to as internetworking.

How Does Internetworking Work?

Every network node or phase is built using a similar protocol or a communication logic, such as TCP (Transfer Control Protocol) or IP (Internet Protocol), to enable communication. It is referred to as "internetworking" when a network interacts with another network using ongoing communication protocols. A packet of information must be delivered across numerous links, which is a problem that internetworking was created to address.

The distinction between expanding the network and internetworking is quite slight. A simple extension of a LAN is the use of a switch or hub to join two local area networks, but connecting them via a router is an example of internetworking. The OSI-ISO model's Layer 3 (Network Layer) enforces internetworking. The internet is the most prominent famous example of internetworking.

Types of Internetworking

Internetworking primarily consists of three units: Extranet, Internet, and Intranet. Internet connections may or may not be present on intranets and extranets. The computer network or the extranet area unit is typically protected from being accessed from the internet if it is not approved and if there is a link to the internet. Although it should serve as a portal for access to portions of the associate degree extranet, the internet is not considered to be a part of the computer network or extranet.

Extranet

It's a network of the internetwork with a confined scope to one organisation or institution but with limited links to one or more other networks on occasion; however, this is not always the

case. It is the lowest degree of internet usage and is typically prohibited in extremely private areas. An extranet may also be referred to as a MAN, WAN, or another type of network, but it cannot include a single local area network; rather, it must make at least one mention of an external network.

Internet

Internet is a specific internetworking that connects governmental, academic, public, and private networks on a global scale. It is based on the ARPANET, which was created by the ARPA (Advanced Research Projects Agency) of the U.S. Defense Department. It is also the location of the World Wide Web (WWW) and is referred to as the "Internet" to distinguish it from other generic internetworking. Internet users and their service providers utilise IP addresses obtained from address registries that control assignments.

Intranet

This computer network can be a collection of interconnected networks that employ the Internet Protocol and IP-based software like web browsers as well as FTP tools, all of which are controlled by a single body entity. This body entity blocks access to the computer network for the rest of the world and only allows a select few users. This network most frequently refers to the internal network of a business or other enterprise. To provide users with browse able data, a large computer network can typically have its own internet server.

Internetwork Addressing

The internetwork addresses set up devices singly or collectively. Depending on the protocol family and because of the OSI layer, addressing strategies vary. DLL, MAC addresses, and network-layer addresses are the three types of internetwork address area units that are typically employed.

DLL Addresses

All the physical network associations of network devices are clearly identified by a data-link layer address. Area units are frequently used as physical addresses or hardware addresses in data-link addresses. Data-link addresses can occasionally be found within a flat address space and are pre-configured with a fixed relationship to a particular device. End systems typically only have one data-link address since they only have one physical network association. As a result of having many physical network connections, routers and other internetworking equipment frequently have various data-link addresses.

MAC Addresses

Data-link layer addresses are included in MAC addresses. MAC addresses create network entities in LANs that use the data-link layer's IEEE MAC addresses. For each local area network interface, a unique MAC address designates a particular area unit. MAC addresses are expressed as twelve hexadecimal numbers and are forty-eight bits long. The Organisational Unique Identifier (OUI) is made up of the first 12 hexadecimal digits, which are typically managed by the IEEE and identify the maker or seller.

The interface serial variety or the other price set by a specific merchant would be represented by the final half a dozen positional notation digits. When an interface card initialises, MAC addresses are routinely traced into RAM from ROM, where they are known as burned-in addresses (abbreviated as BIAs).

Network Layer Addresses

The network addresses can occasionally be seen in both gradable address areas and the more common virtual or logical address area units. The relationship between the network address and the tool is logical and flexible; it typically depends either on the properties of the physical network or on groupings without any physical foundation. For each network-layer protocol that a finished system supports, a network-layer address is required. For each supported network-layer protocol, routers and other internetworking devices require a single network-layer address for every physical network association.

Challenges to Internetworking

There is no guarantee that useful internetwork will be implemented. There are many difficult fields, especially in the ones of dependability, connection, adaptability, and network management. However, each and every one of these fields is crucial to the creation of an efficient and cost-effective internetwork. The challenges to internetworking include:

- The first difficulty arises when we attempt to link several systems in order to allow communication among various technologies. For instance, completely distinct websites may employ various media or function at various speeds.
- Reliable service that must be maintained in the internetwork is another crucial consideration. Organisations as a whole and individual users alike rely on regular, dependable access to network resources.
- Centralised assistance and internet network troubleshooting should be provided via network management. For the network to operate smoothly, configuration, security, performance, and other issues need to be addressed properly.
- The most significant factor, flexibility, is crucial for network expansion as well as new applications and services.

Tunnelling:

Tunnelling is a protocol for transferring data securely from one network to another. Using a method known as *encapsulation*, Tunnelling allows private network communications to be sent across a public network, such as the Internet. Encapsulation enables data packets to appear general to a public network when they are private data packets, allowing them to pass unnoticed.

When data is tunnelled, it is split into smaller parts called *packets*, as it travels through the tunnel. The packets are encrypted via the tunnel, and another process known

as *encapsulation* takes place. For transmission, private network data and protocol details are encased in public network transmission units. The units have the appearance of public data, allowing them to be sent via the Internet. Encapsulation enables packets to reach their intended destination. De-capsulation and decryption take place at the final destination.

Tunnelling is possible thanks to a variety of procedures, including −

- Point-to-Point Tunnelling Protocol (PPTP)
- Layer Two Tunnelling Protocol (L2TP)

- PPTP (Point-to-Point Tunnelling Protocol)

  PPTP protects confidential information even when transmitted via public networks. An Internet service provider can provide authorized users with access to a private network called a virtual private network. Because it was built in a tunnelled environment, this is a "virtual" private network.

- Layer Two Tunnelling Protocol (L2TP)

  This tunnelling protocol combines PPTP with Layer 2 Forwarding.

  Tunnelling is a technique for communicating over a public network while going through a private network. This is especially beneficial in a corporate situation, and it also includes security measures like encryption.

  The IP packet in this scenario does not have to deal with the WAN, and neither do the hosts A and B. IP, and WAN packets will be understood by the multiprotocol routers M1 and M2. As a result, the WAN can be compared to a large tunnel connecting multiprotocol routers M1 and M2, and the process is known as Tunnelling.

  Tunnelling makes use of a layered protocol paradigm like the OSI or TCP/IP protocol suite. In other words, when data travels from host A to host B, it traverses all levels of the specified protocol (OSI, TCP/IP, and so on), and data conversion (encapsulation) to suit different interfaces of the particular layer is referred to as Tunnelling.

INTERNETWORKING ROUTING: https://www.youtube.com/watch?v=VFxlOra5NDc

Fragmentation Network layer in the Internet:

Fragmentation is an important function of network layer. It is technique in which gateways break up or divide larger packets into smaller ones called fragments. Each fragment is then sent as a separate internal packet. Each fragment has its separate header and trailer.

Sometimes, a fragmented datagram can also get fragmented further when it encounters a network that handles smaller fragments. Thus, a datagram can be fragmented several times

before it reaches final destination. Reverse process of the fragmentation is difficult. Reassembling of fragments is usually done by the destination host because each fragment has become an independent datagram.

The need of Fragmentation at Network Layer:

Fragmentation at the Network Layer is a process of dividing a large data packet into smaller pieces, known as fragments, to improve the efficiency of data transmission over a network. The need for fragmentation at the network layer arises from several factors:

1.Maximum Transmission Unit (MTU): Different networks have different Maximum Transmission Unit (MTU) sizes, which determine the maximum size of a data packet that can be transmitted over that network. If the size of a data packet exceeds the MTU, it needs to be fragmented into smaller fragments that can be transmitted over the network.

2.Network Performance: Large data packets can consume a significant amount of network resources and can cause congestion in the network. Fragmentation helps to reduce the impact of large data packets on network performance by breaking them down into smaller fragments that can be transmitted more efficiently.

3.Bandwidth Utilization: Large data packets may consume a significant amount of network bandwidth, causing other network traffic to be slowed down. Fragmentation helps to reduce the impact of large data packets on network bandwidth utilization by breaking them down into smaller fragments that can be transmitted more efficiently.

Fragmentation at the network layer is necessary in order to ensure efficient and reliable transmission of data over communication networks.

1.Large Packet Size: In some cases, the size of the packet to be transmitted may be too large for the underlying communication network to handle. Fragmentation at the network layer allows the large packet to be divided into smaller fragments that can be transmitted over the network.

2.Path MTU: The Maximum Transmission Unit (MTU) of a network defines the largest packet size that can be transmitted over the network. Fragmentation at the network layer allows the packet to be divided into smaller fragments that can be transmitted over networks with different MTU values.

3.Reliable Transmission: Fragmentation at the network layer increases the reliability of data transmission, as smaller fragments are less likely to be lost or corrupted during transmission.

What is IPv4?

IP stands for **Internet Protocol version v4** stands for **Version Four** (IPv4), is the most widely used system for identifying devices on a network. It uses a set of four numbers, separated by periods (like 192.168.0.1), to give each device a unique address. This address helps data find its way from one device to another over the internet.

Parts of IPv4

IPv4 addresses consist of three parts:

- **Network Part**: The network part indicates the distinctive variety that's appointed to the network. The network part conjointly identifies the category of the network that's assigned.
- **Host Part**: The host part uniquely identifies the machine on your network. This part of the IPv4 address is assigned to every host. For each host on the network, the network part is the same, however, the host half must vary.
- **Subnet Number**: This is the nonobligatory part of IPv4. Local networks that have massive numbers of hosts are divided into subnets and subnet numbers are appointed to that.

Characteristics of IPv4

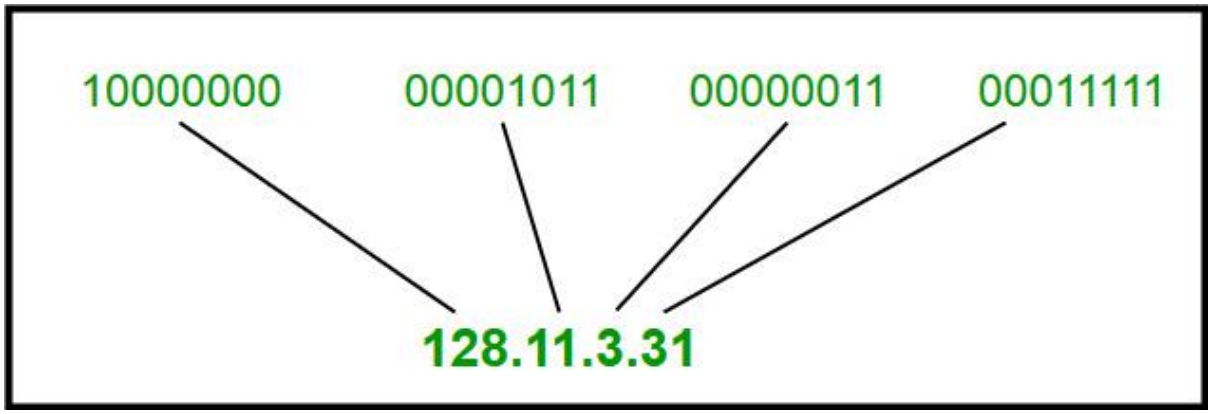
- IPv4 could be a 32-bit IP Address.
- IPv4 could be a numeric address, and its bits are separated by a dot.
- The number of header fields is twelve and the length of the header field is twenty.
- It has Unicast, broadcast, and multicast-style addresses.
- IPv4 supports VLSM (Virtual Length Subnet Mask).
- IPv4 uses the Post Address Resolution Protocol to map to the MAC address.
- RIP may be a routing protocol supported by the routed daemon.
- Networks ought to be designed either manually or with DHCP.
- Packet fragmentation permits from routers and causes host.

There are two notations in which the IP address is written, dotted decimal and hexadecimal notation.

Dotted Decimal Notation

Some points to be noted about dotted decimal notation:

- The value of any segment (byte) is between 0 and 255 (both included).
- No zeroes are preceding the value in any segment (054 is wrong, 54 is correct).



Dotted Decimal Notation

Hexadecimal Notation

Introduction of Classful IP Addressing

An **IP address** is an address that has 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 232.

Classful IP addressing is a way of organizing and managing IP addresses, which are used to identify devices on a network. Think of IP addresses like street addresses for houses; each device on a network needs its unique address to communicate with other devices.

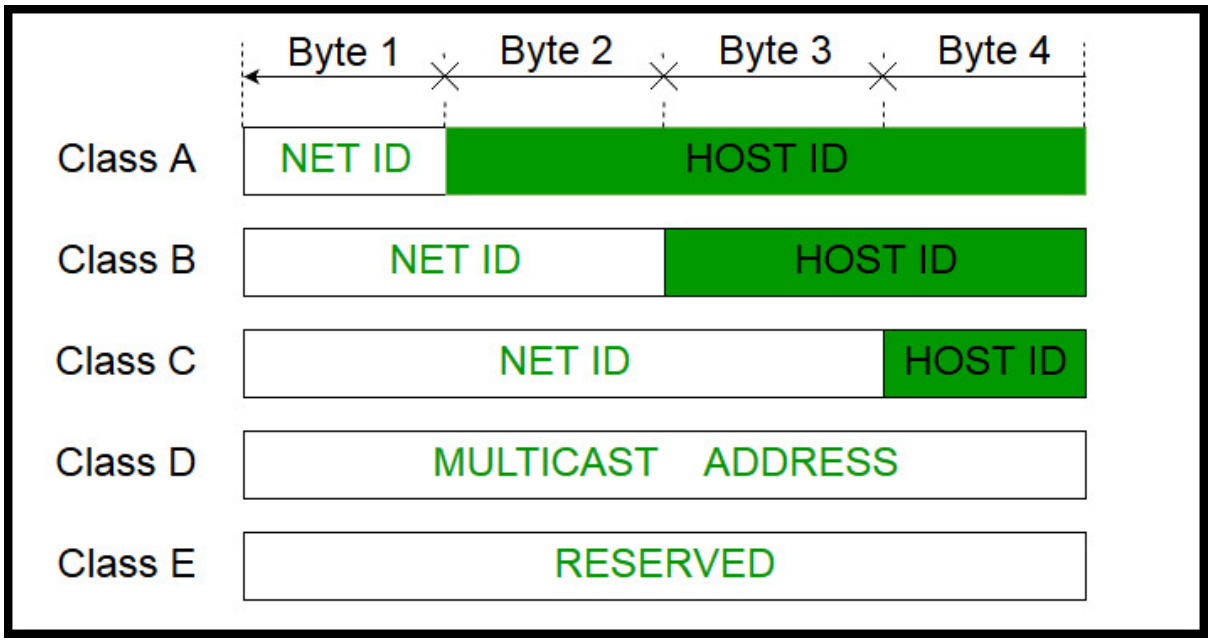
Classful Addressing

The 32-bit IP address is divided into five sub-classes. These are given below:

- 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 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.



Classful Addressing

Class A

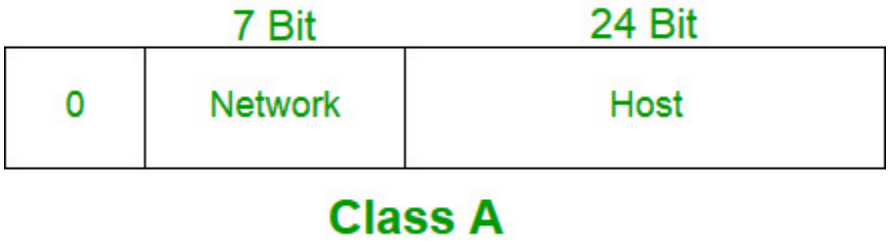
IP addresses belonging to class A are assigned to the networks that contain a large number of hosts.

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

- 2^24 – 2 = 16,777,214 host ID

IP addresses belonging to class A ranges from 0.0.0.0 – 127.255.255.255.



Class B

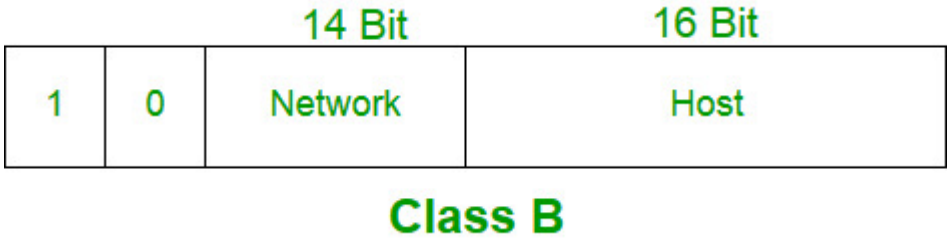
IP address belonging to class B is assigned to networks that range from medium-sized to large-sized networks.

- 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. The default subnet 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 128.0.0.0 – 191.255.255.255.



Class B

Class C

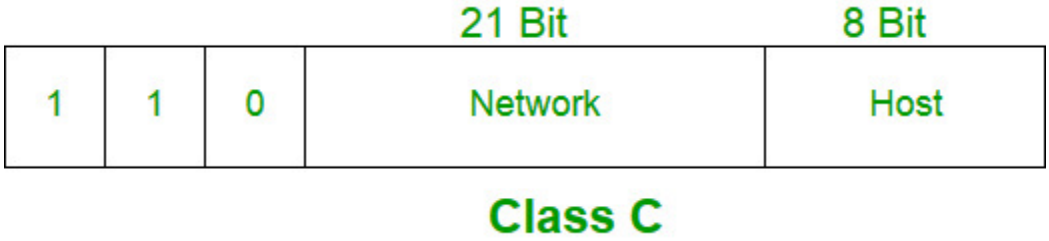
IP addresses belonging to class C are assigned to small-sized networks.

- 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. The default subnet 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 range from 192.0.0.0 – 223.255.255.255.

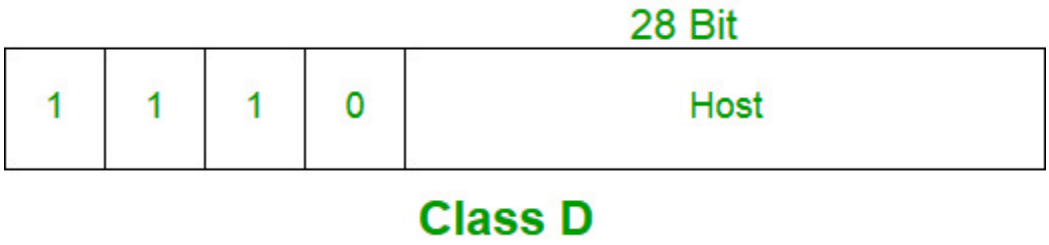


Class C

Class D

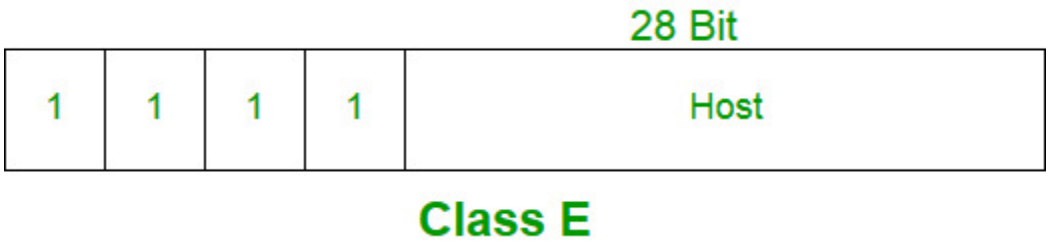
IP address belonging to class D is reserved for multi-casting. The higher-order bits of the first octet of IP addresses belonging to class D is always set to 1110. The remaining bits are for the address that interested hosts recognize.

Class D does not possess any subnet mask. IP addresses belonging to class D range from 224.0.0.0 – 239.255.255.255.



Class E

IP addresses belonging to class E are reserved for experimental and research purposes. IP addresses of class E range from 240.0.0.0 – 255.255.255.255. This class doesn't have any subnet mask. The higher-order bits of the first octet of class E are always set to 1111.



Rules for Assigning Host ID

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

- Within any network, the host ID must be unique to that network.
- A 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 the class A address and is reserved for internal loopback 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.

What is Classless Inter-Domain Routing (CIDR)?

CIDR or Class Inter-Domain Routing was introduced in 1993 to replace classful addressing. Classless Inter-Domain Routing (CIDR) is a method for efficiently allocating IP addresses and routing Internet Protocol (IP) packets. Unlike classful addressing, which divides IP addresses into fixed classes (A, B, C, etc.), CIDR allows for variable-length subnet masks (VLSM). This means that networks can be divided into smaller, more flexible subnets according to their specific needs, rather than being constrained by predefined class boundaries.

CIDR Notation

In CIDR subnet masks are denoted by /X. For example a subnet of 255.255.255.0 would be denoted by /24. To work a subnet mask in CIDR, we have to first convert each octet into its respective binary value.

Difference Between Classful Addressing and Classless Addressing

Parameter	Classful Addressing	Classless Addressing
Basics	In Classful addressing IP addresses are allocated according to the classes- A to E.	Classless addressing came to replace the classful addressing and to handle the issue of rapid exhaustion of IP addresses.
Practical	It is less practical.	It is more practical.
Network ID and Host ID	The changes in the Network ID and Host ID depend on the class.	There is no such restriction of class in classless addressing.

Parameter	Classful Addressing	Classless Addressing
VLSM	It does not support the Variable Length Subnet Mask (VLSM).	It supports the Variable Length Subnet Mask (VLSM).
Bandwidth	Classful addressing requires more bandwidth. As a result, it becomes slower and more expensive as compared to classless addressing.	It requires less bandwidth. Thus, fast and less expensive as compared to classful addressing.
CIDR	It does not support Classless Inter-Domain Routing (CIDR).	It supports Classless Inter-Domain Routing (CIDR).
Updates	Regular or periodic updates	Triggered Updates
Troubleshooting and Problem detection	Troubleshooting and problem detection are easy than classless addressing because of the division of network, host and subnet parts in the address.	It is not as easy compared to classful addressing.
Division of Address	• Network • Host • Subnet	• Host • Subnet

Introduction to Subnetting

Subnetting is a combination of two words i.e. Sub and Netting. Here Sub word means Substitute and netting word means Network. The Substitute Network created for a function to happen is known as Subnetting.

Subnetting is a technique for creating logical sub-networks from a single physical network (subnets). A company can grow its network via subnetting without asking for a new network number from its ISP. Subnetting hides network complexity while assisting in the reduction of network traffic. Here, a network which is unique has to provide its services to many Local Area Networks i.e. (LAN). So, for this reason Subnetting is extensively used.

Purpose of Subnetting in Computer Networks

- **Efficiency of the Network**

By removing the need for extra routers, subnetting makes network traffic simpler. This makes sure the data being transmitted can get to its destination as fast as possible, eliminating or avoiding any potential diversions that may slow it down.

- **Provides Network Security**

By isolating or removing vulnerable network regions and making it harder for intruders to move through a company's network, subnetting helps the network managers in reducing network-wide risks.

- **Internet Protocol (IP) Addressing Relocation**

Each class has a finite amount of possible host allocations; for instance, networks with more than 254 devices require a Class B allocation. Assume that you are a network administrator. Now, you have a task of allocating 150 hosts among three physical networks in three distinct cities for a Class B or C network. If so, we must either ask for additional address blocks for each network or split the single big network into small parts named subnets so that we could utilize a single address block across a number of physical networks.

We will learn about this concept deeper in the upcoming topics.

- **Reduction of Network Traffic**

Placing all of the computers on the same subnet can assist minimize network traffic if a significant amount of an organization's traffic is intended to be shared routinely among a number of devices. Without a subnet, all computers and servers on the network would be able to see data packets from every other machine.

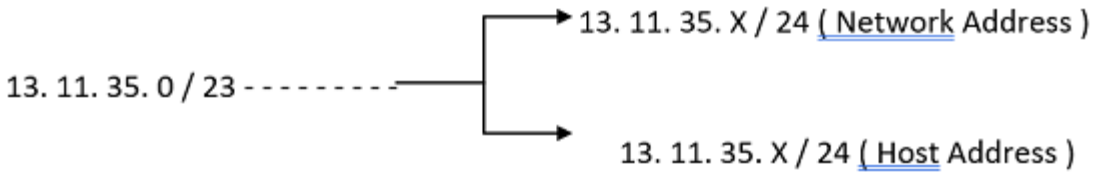
- **Network Speed Improvement**

The main network is divided into smaller subnets through the process of subnetting, and the goal of these smaller, linked networks is to split the large network into a collection of smaller, less-busy networks. Subnets reduce the need for traffic to use unnecessary routes, which speeds up the network.

- **Division of IP Addresses**

An IP address is split into its network address and host address via subnetting.

The split address may then be further divided into units using the subnet mask approach, and those units can be assigned to different network devices.



Here, X refers to the Host ID. This is the only thing which gets changed in the Internet Protocol Address

SUBNETTING: https://youtu.be/UHRPtNZ_Rz4

Network Layer Protocols

Network Layer is responsible for the transmission of data or communication from one host to another host connected in a network. Rather than describing how data is transferred, it implements the technique for efficient transmission. In order to provide efficient communication protocols are used at the network layer. The data is being grouped into packets or in the case of extremely large data it is divided into smaller sub packets. Each protocol used has specific features and advantages.

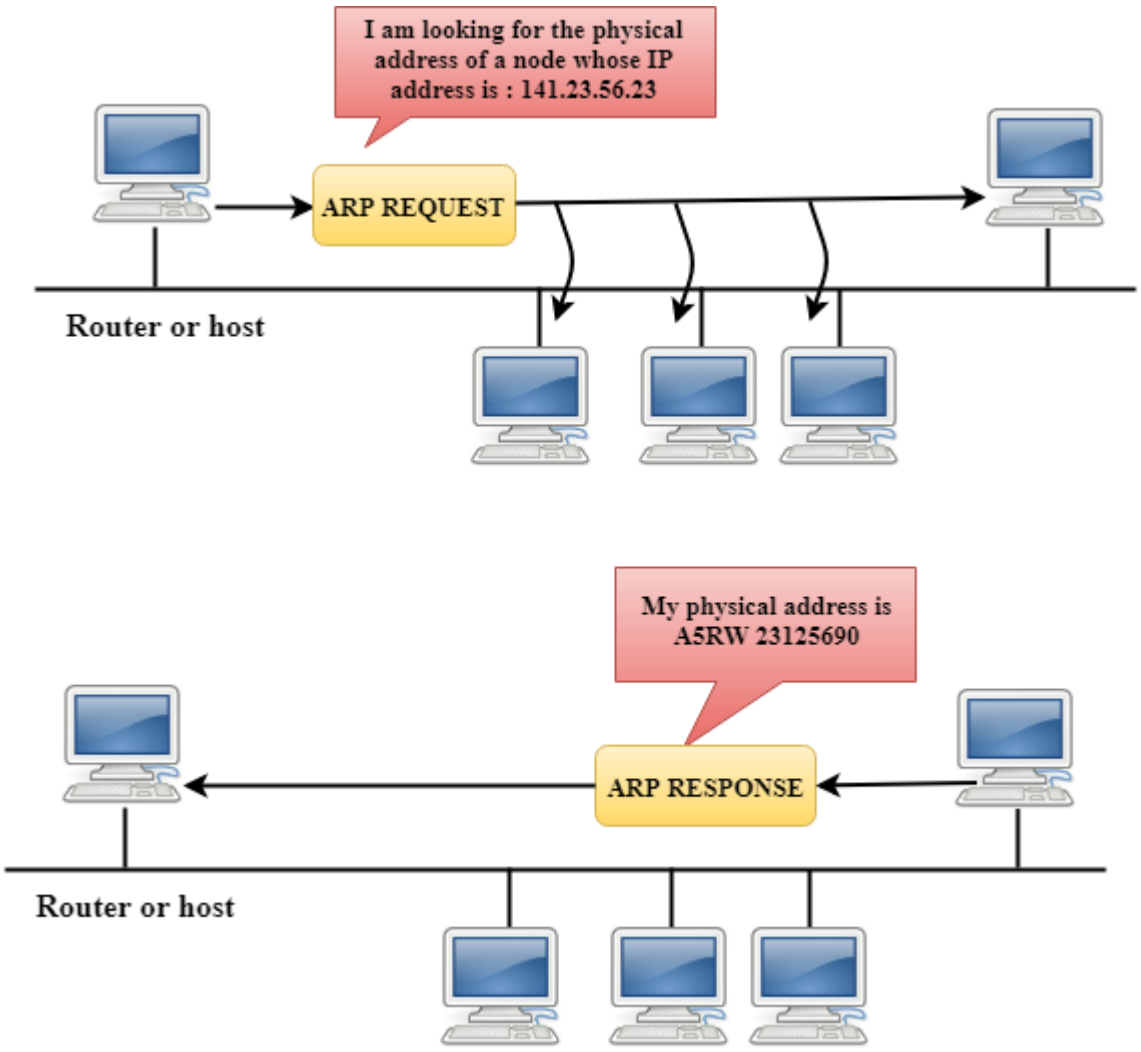
TCP/IP supports the following protocols:

ARP

- ARP stands for Address Resolution Protocol.
- It is used to associate an IP address with the MAC address.
- Each device on the network is recognized by the MAC address imprinted on the NIC. Therefore, we can say that devices need the MAC address for communication on a local area network. MAC address can be changed easily. For example, if the NIC on a particular machine fails, the MAC address changes but IP address does not change. ARP is used to find the MAC address of the node when an internet address is known.

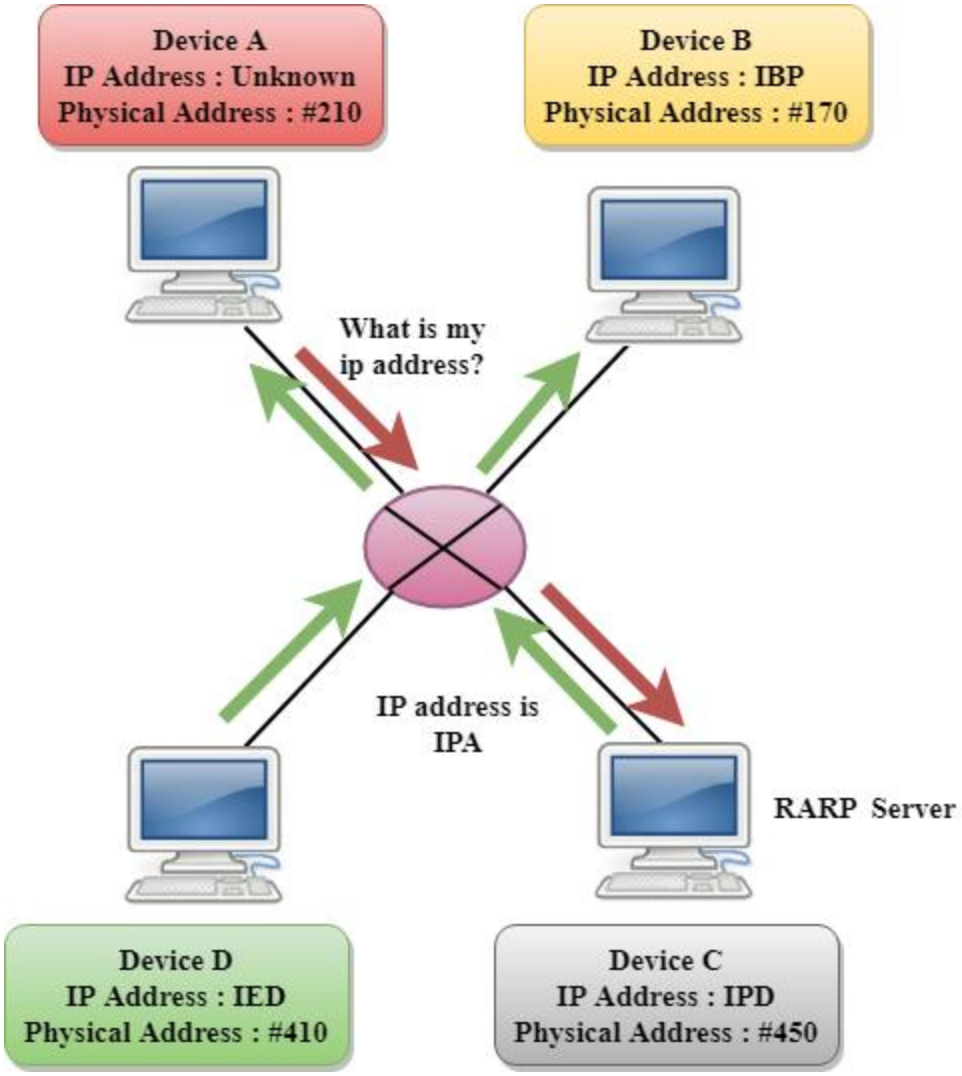
How ARP works

If the host wants to know the physical address of another host on its network, then it sends an ARP query packet that includes the IP address and broadcast it over the network. Every host on the network receives and processes the ARP packet, but only the intended recipient recognizes the IP address and sends back the physical address. The host holding the datagram adds the physical address to the cache memory and to the datagram header, then sends back to the sender.



RARP

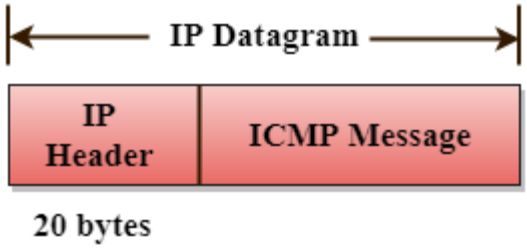
- RARP stands for **Reverse Address Resolution Protocol**.
- If the host wants to know its IP address, then it broadcast the RARP query packet that contains its physical address to the entire network. A RARP server on the network recognizes the RARP packet and responds back with the host IP address.
- The protocol which is used to obtain the IP address from a server is known as **Reverse Address Resolution Protocol**.
- The message format of the RARP protocol is similar to the ARP protocol.
- Like ARP frame, RARP frame is sent from one machine to another encapsulated in the data portion of a frame.



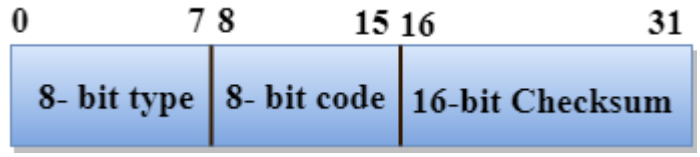
ICMP

- ICMP stands for Internet Control Message Protocol.
- The ICMP is a network layer protocol used by hosts and routers to send the notifications of IP datagram problems back to the sender.
- ICMP uses echo test/reply to check whether the destination is reachable and responding.
- ICMP handles both control and error messages, but its main function is to report the error but not to correct them.
- An IP datagram contains the addresses of both source and destination, but it does not know the address of the previous router through which it has been passed. Due to this reason, ICMP can only send the messages to the source, but not to the immediate routers.

- ICMP protocol communicates the error messages to the sender. ICMP messages cause the errors to be returned back to the user processes.
- ICMP messages are transmitted within IP datagram.



The Format of an ICMP message



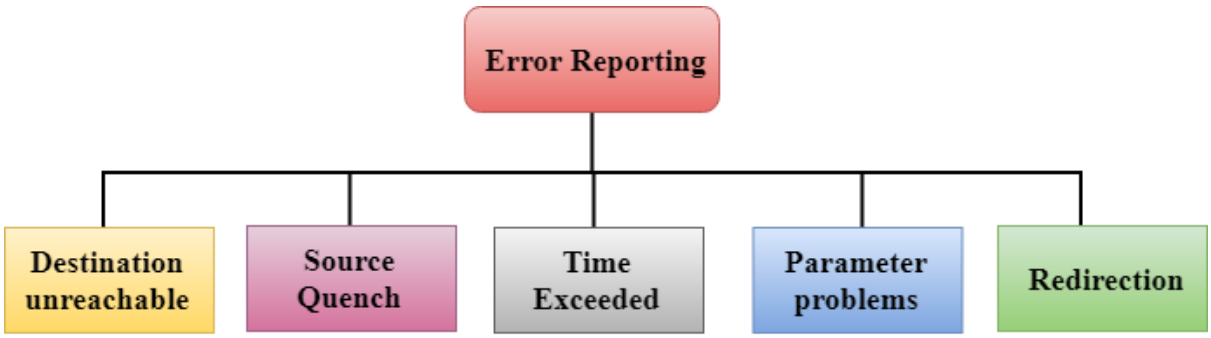
- The first field specifies the type of the message.
- The second field specifies the reason for a particular message type.
- The checksum field covers the entire ICMP message.

Error Reporting

ICMP protocol reports the error messages to the sender.

Five types of errors are handled by the ICMP protocol:

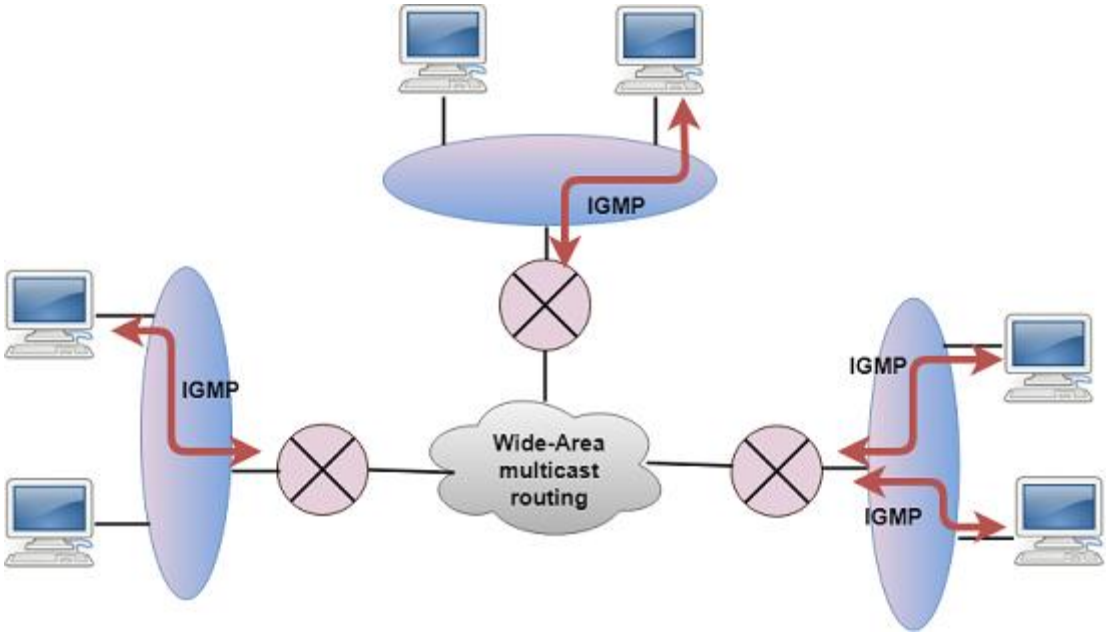
- Destination unreachable
- Source Quench
- Time Exceeded
- Parameter problems
- Redirection



- **Destination unreachable:** The message of "Destination Unreachable" is sent from receiver to the sender when destination cannot be reached, or packet is discarded when the destination is not reachable.
- **Source Quench:** The purpose of the source quench message is congestion control. The message sent from the congested router to the source host to reduce the transmission rate. ICMP will take the IP of the discarded packet and then add the source quench message to the IP datagram to inform the source host to reduce its transmission rate. The source host will reduce the transmission rate so that the router will be free from congestion.
- **Time Exceeded:** Time Exceeded is also known as "Time-To-Live". It is a parameter that defines how long a packet should live before it would be discarded.
- **Parameter problems:** When a router or host discovers any missing value in the IP datagram, the router discards the datagram, and the "parameter problem" message is sent back to the source host.
- **Redirection:** Redirection message is generated when host consists of a small routing table. When the host consists of a limited number of entries due to which it sends the datagram to a wrong router. The router that receives a datagram will forward a datagram to a correct router and also sends the "Redirection message" to the host to update its routing table.

IGMP

- IGMP stands for **Internet Group Message Protocol**.
- The IP protocol supports two types of communication:
    - **Unicasting:** It is a communication between one sender and one receiver. Therefore, we can say that it is one-to-one communication.
    - **Multicasting:** Sometimes the sender wants to send the same message to a large number of receivers simultaneously. This process is known as multicasting which has one-to-many communication.
- The IGMP protocol is used by the hosts and router to support multicasting.
- The IGMP protocol is used by the hosts and router to identify the hosts in a LAN that are the members of a group.



- IGMP is a part of the IP layer, and IGMP has a fixed-size message.
- The IGMP message is encapsulated within an IP datagram.

Difference Between IPv4 and IPv6

IPv4	IPv6
IPv4 has a 32-bit address length	IPv6 has a 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 4.29×10 9 address space	The address space of IPv6 is quite large it can produce 3.4×10 38 address space
The Security feature is dependent on the application	IPSEC is an inbuilt security feature in the IPv6 protocol

IPv4	IPv6
Address representation of IPv4 is in decimal	Address representation of IPv6 is in hexadecimal
Fragmentation performed by Sender and forwarding routers	In IPv6 fragmentation is performed only by the sender
In IPv4 Packet flow identification is not available	In IPv6 packet flow identification are Available and uses the flow label field in the header
In IPv4 checksum field is available	In IPv6 checksum field is not available
It has a broadcast Message Transmission Scheme	In IPv6 multicast and anycast message transmission scheme is available
In IPv4 Encryption and Authentication facility not provided	In IPv6 Encryption and Authentication are provided
IPv4 has a header of 20-60 bytes.	IPv6 has a header of 40 bytes fixed
IPv4 can be converted to IPv6	Not all IPv6 can be converted to IPv4
IPv4 consists of 4 fields which are separated by addresses dot (.)	IPv6 consists of 8 fields, which are separated by a colon (:)
IPv4's IP addresses are divided into five different classes. Class A , Class B, Class C, Class D , Class E.	IPv6 does not have any classes of the IP address.
IPv4 supports VLSM(Variable Length subnet mask).	IPv6 does not support VLSM.

IPv4	IPv6
Example of IPv4: 66.94.29.13	Example of IPv6: 2001:0000:3238:DFE1:0063:0000:0000:FEFB

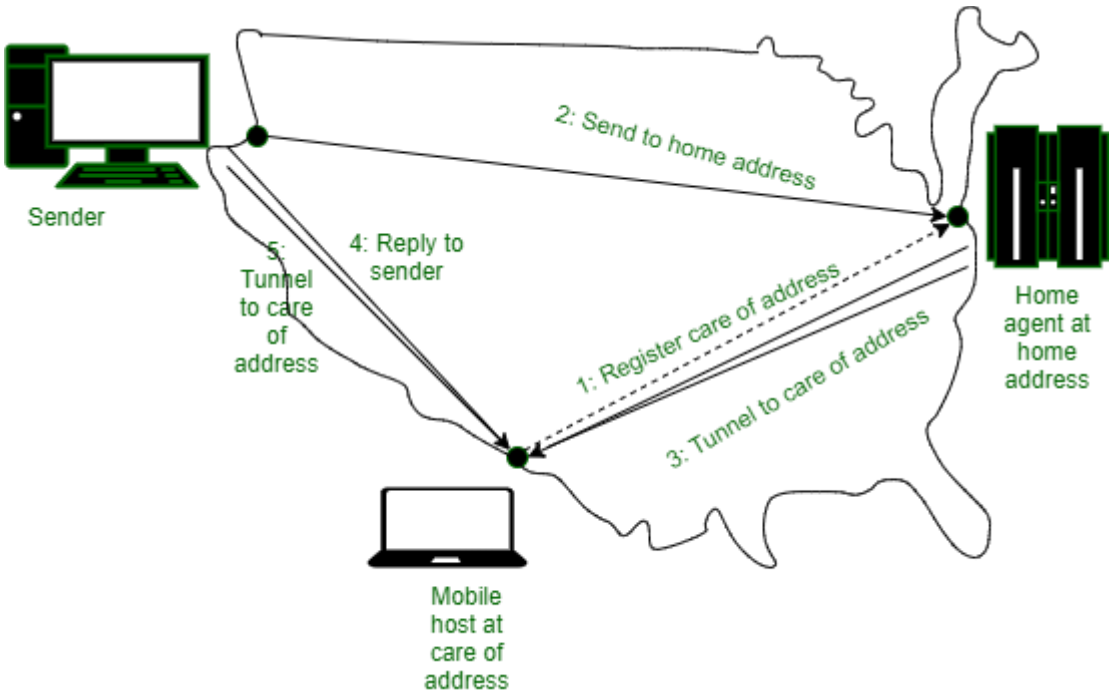
Routing for Mobile Hosts

Millions of people use computers while on go, from the truly mobile situations with a wireless device in moving cars, to nomadic situations in which laptop computers are used in a series of a different location. We use the term mobile hosts to mean either category, as distinct from stationary hosts that never move. The mobile hosts introduce a new complication to route packets to the mobile hosts, the network first has to find it.

Description of Diagram :

The message is shown with a dashed line in the figure indicate that it is a control message, not a data message. The sender sends a data packet to the mobile host using its permanent address. This packet is routed by the network to the host home location because the home addresses belong there. It encapsulates the packet with a new header and sends this bundle to the care-of address. This mechanism is called tunneling. It is very important on the internet, so we will look at it in more detail later.

Diagram :



- When the encapsulated packet arrives at the care-of address, the mobile host unwraps it and retrieves the packet from the sender.

- The overall route is called triangle routing because it way is circuitous if the remote location is far from the home location.
- As part of the step, 4 senders learns the current care-of address.
- Subsequent packets can be routed directly to the mobile host by tunneling them to the care-of address (step 5) bypassing the home location.
- If connectivity lost for any reason as the mobile moves, the home address can always be used to reach the mobile.

Mobile Internet Protocol (or Mobile IP)

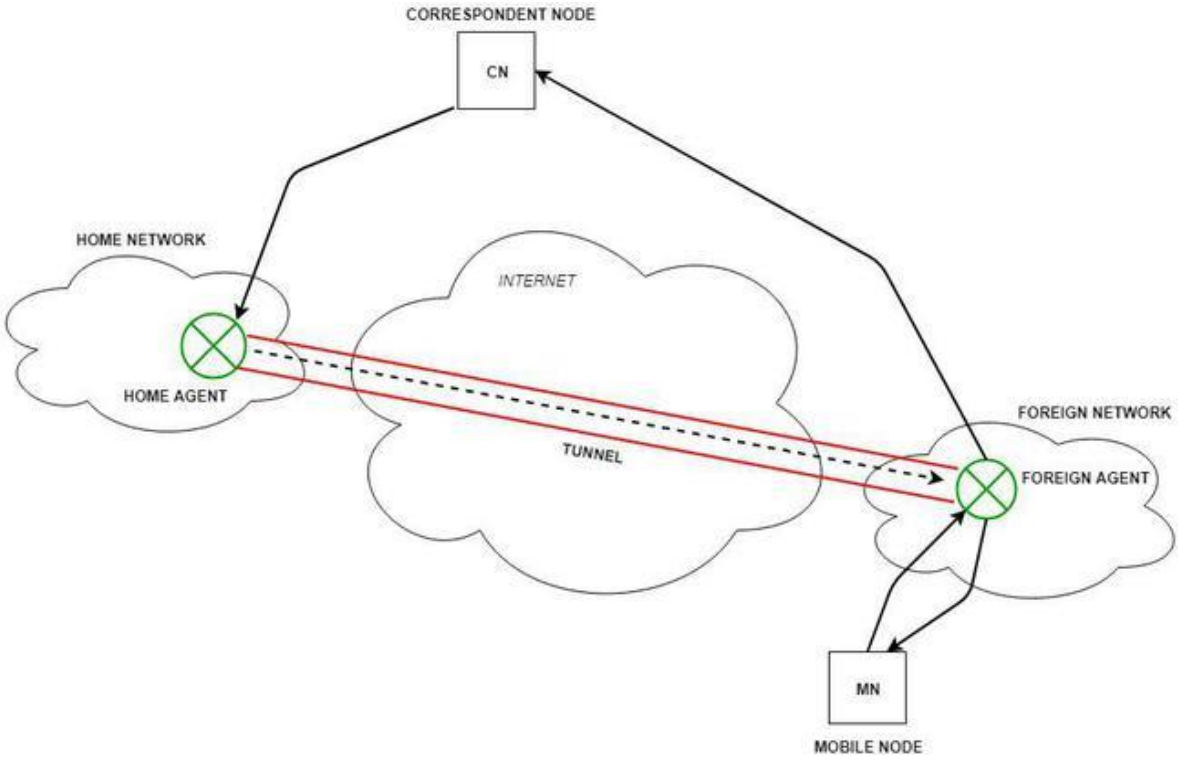
Mobile IP is a communication protocol (created by extending Internet Protocol, IP) that allows users to move from one network to another with the same IP address. It ensures that the communication will continue without the user's sessions or connections being dropped. Imagine having a phone number that stays the same no matter where you go. Mobile IP works similarly, ensuring that even if your device changes its network connection, it can still communicate without interruption.

This is particularly useful for mobile devices like smartphones, laptops, and tablets, which frequently switch between different networks, such as Wi-Fi and cellular. Mobile IP helps keep internet connections stable and reliable, making it easier to stay connected while on the move.

Basic Terminologies Related to Mobile IP

- **A Mobile Node (MN):** It is the hand-held communication device that the user carries e.g. Cell phone.
- **A Home Network:** It is a network to which the mobile node originally belongs as per its assigned IP address (home address).
- **Home Agent (HA):** It is a router in-home network to which the mobile node was originally connected
- **Home Address:** It is the permanent IP address assigned to the mobile node (within its home network).
- **Foreign Network:** It is the current network to which the mobile node is visiting (away from its home network).
- **A Foreign Agent (FA):** It is a router in a foreign network to which the mobile node is currently connected. The packets from the home agent are sent to the foreign agent which delivers them to the mobile node.
- **The Correspondent Node (CN):** It is a device on the internet communicating to the mobile node.

- **Care-of Address (COA):** It is the temporary address used by a mobile node while it is moving away from its home network.
- **Foreign Agent COA:** The COA could be located at the FA, i.e., the COA is an IP address of the FA. The FA is the tunnel end-point and forwards packets to the MN. Many MN using the FA can share this COA as a common COA.
- **Co-Located COA:** The COA is co-located if the MN temporarily acquires an additional IP address that acts as a COA. This address is now topologically correct, and the tunnel endpoint is at the MN. Co-located addresses can be acquired using services such as DHCP.



Mobile IP Topology

How Does Mobile IP Work?

The correspondent node sends the data to the mobile node. Data packets contain the correspondent node's address (Source) and home address (Destination). Packets reach the home agent. But now mobile node is not in the home network, it has moved into the foreign network. The foreign agent sends the care-of-address to the home agent to which all the packets should be sent. Now, a tunnel will be established between the home agent and the foreign agent by the process of tunneling.

Tunneling establishes a virtual pipe for the packets available between a tunnel entry and an endpoint. It is the process of sending a packet via a tunnel and it is achieved by a mechanism called encapsulation.

Now, the home agent encapsulates the data packets into new packets in which the source address is the home address and the destination is the care-of-address and sends it through

the tunnel to the foreign agent. Foreign agent, on another side of the tunnel, receives the data packets, decapsulates them, and sends them to the mobile node. The mobile node in response to the data packets received sends a reply in response to the foreign agent. The foreign agent directly sends the reply to the correspondent node.