UNIT 3

NETWORK LAYER

1.NETWORK LAYER SERVICES

The network layer in theTCP/IP protocol suite is responsible for the host-to-host delivery of datagrams.

Itprovidesservicestothetransportlayerandreceivesservicesfromthedata-link layer. Thenetwork layertranslates thelogical addressesinto physicaladdresses. Itdeterminestheroutefromthesourcetothedestinationandalsomanagesthetrafficpro blemssuchasswitching,routingand controls the congestion of data packets. Themainroleofthenetworklayeristomovethepacketsfromsendinghosttothereceivin g host.

Servicesprovidedbynetworklayerare

PACKETIZING

- Thefirst dutyof thenetwork layeris definitelypacketizing.
- Thismeansencapsulatingthepayload(data receivedfromupperlayer)inanetwork-layerpacketatthesourceanddecapsulatingthepayloadfromthenetwork-layerpacket atthe destination.
- Thenetworklayerisresponsiblefordeliveryofpackets fromasendertoa receiverwithoutchanging or using thecontents.

ROUTINGANDFORWARDING

Routing

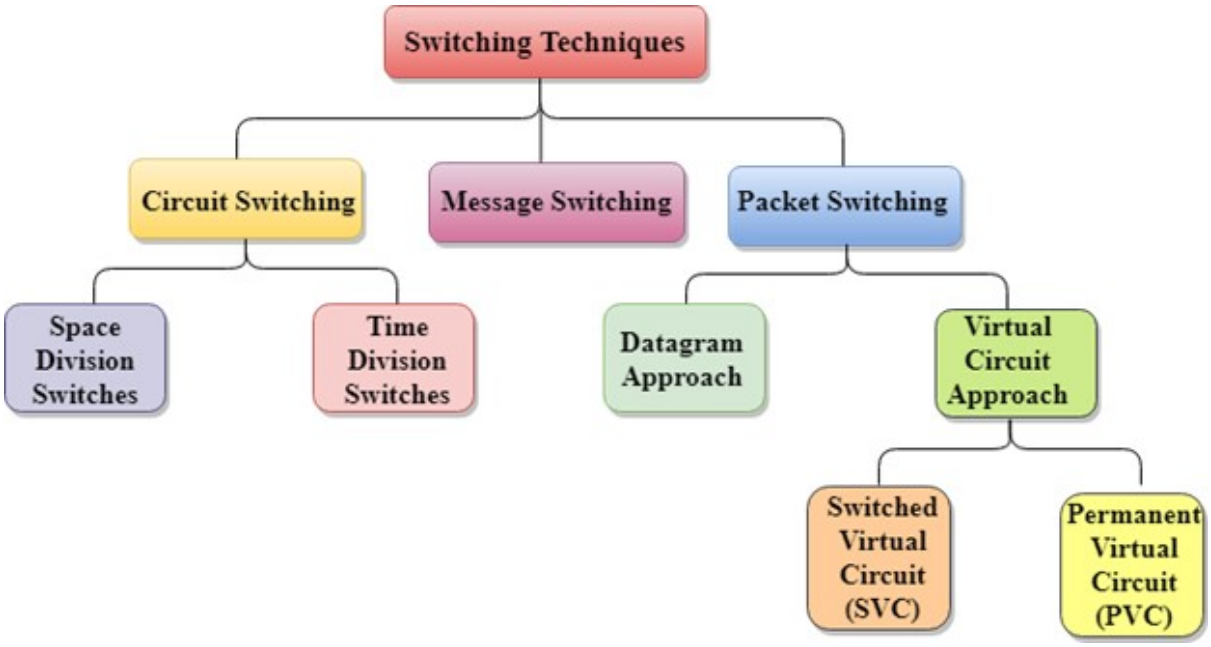
- Thenetworklayerisresponsibleforroutingthepacketfromitssourcetoth edestination.
- Thenetworklayerisresponsibleforfindingthebestoneamongthesepossi bleroutes.
- Thenetworklayerneedstohavesomespecificstrategiesfordefiningtheb estroute.
- Routingistheconceptofapplyingstrategiesandrunningroutingprotocol stocreatethe decision-making tables for each router.
- Thesetables arecalled asrouting tables.

Forwarding

- Forwardingcanbedefinedastheactionappliedbyeachrouterwhenapacketarrivesatone of its interfaces.
- Thedecision-makingtable,arouternormallyusesforapplyingthisactioniscalledthe forwarding table.
- Whenarouterreceivesapacketfromoneofitsattachednetworks,itneedstoforwardthe packet to another attached network.

2.SWITCHING

In large networks, there can be multiple paths from sender to receiver. The switching technique will decide the best route for data transmission.Switching technique is used to connect the systems for making one-to-one communication. Thetechniqueoftransferringtheinformationfromonecomputernetworktoanothernetwork is known as **switching**.Switchinginacomputernetworkisachievedbyusingswitches.Aswitchisa smallhardwaredevicewhichisusedtojoinmultiplecomputerstogetherwith one localarea network (LAN).

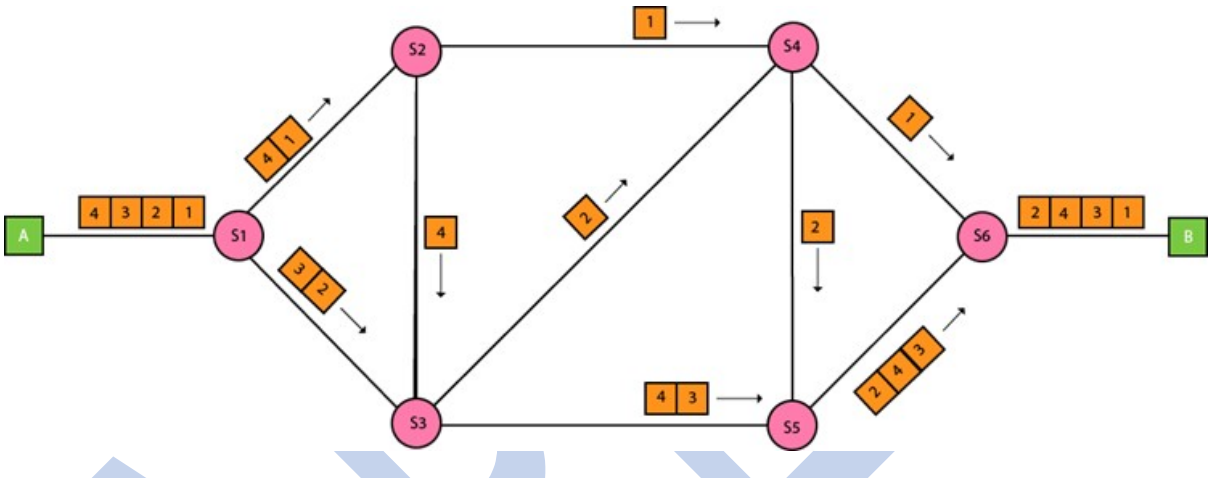


3.PACKET SWITCHING

The packet switching is a switching technique in which the message is sent in one go, but it is divided into smaller pieces, and they are sent

individually.The message splits into smaller pieces known as packets and packets are given a unique number to identify their order at the receiving end.

Every packet contains some information in its headers such as source address, destination address and sequence number.Packets will travel across the network, taking the shortest path as possible.All the packets are reassembled at the receiving end in correct order.If any packet is missing or corrupted, then the message will be sent to resend the message.If the correct order of the packets is reached, then the acknowledgment message will be sent.



Approaches Of Packet Switching:

There are two approaches to Packet Switching:

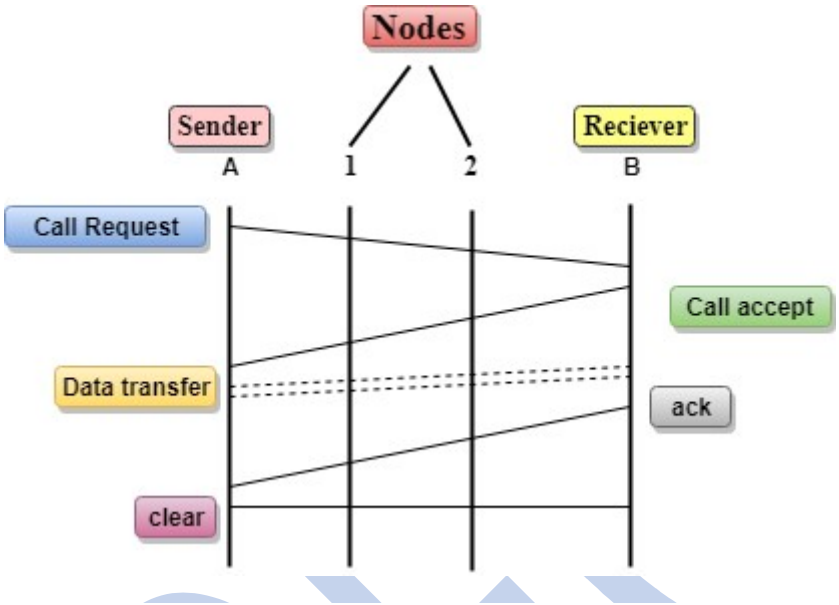
Datagram Packet switching:

It is a packet switching technology in which packet is known as a datagram, is considered as an independent entity. Each packet contains the information about the destination and switch uses this information to forward the packet to the correct destination.The packets are reassembled at the receiving end in correct order.In Datagram Packet Switching technique, the path is not fixed.Intermediate nodes take the routing decisions to forward the packets.Datagram Packet Switching is also known as connectionless switching.

Virtual Circuit Switching

Virtual Circuit Switching is also known as connection-oriented switching.In the case of Virtual circuit switching, a preplanned route is established before

the messages are sent.Call request and call accept packets are used to establish the connection between sender and receiver.In this case, the path is fixed for the duration of a logical connection.



Advantages Of Packet Switching:

Cost-effective: In packet switching technique, switching devices do not require massive secondary storage to store the packets, so cost is minimized to some extent. Therefore, we can say that the packet switching technique is a cost-effective technique.

Reliable: If any node is busy, then the packets can be rerouted. This ensures that the Packet Switching technique provides reliable communication.

Efficient: Packet Switching is an efficient technique. It does not require any established path prior to the transmission, and many users can use the same communication channel simultaneously, hence makes use of available bandwidth very efficiently.

Disadvantages Of Packet Switching:

Packet Switching technique cannot be implemented in those applications that require low delay and high-quality services.

The protocols used in a packet switching technique are very complex and requires high implementation cost.

If the network is overloaded or corrupted, then it requires retransmission of lost packets. It can also lead to the loss of critical information if errors are nor recovered.

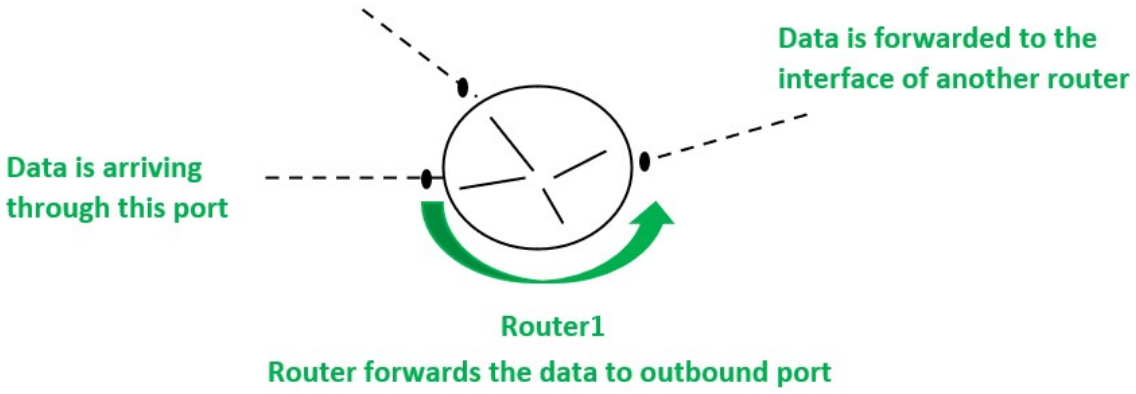
4.FORWARDING IP PACKETS

The process of packet forwarding simply implies the forwarding of incoming packets to their intended destination.

- Internet is made up of generally two terms- Interconnection and Network. So, it is a connection to a large collection of networks. A packet that is to be forwarded may be associated with the same network as the source host or may belong to a destination host in a different network. Thus, it depends on the destination how much a packet may need to travel before arriving at its destination.
- The router is responsible for the process of packet forwarding. It accepts the packet from the origin host or another router in the packet's path and places it on the route leading to the target host.
- The routing table is maintained by the router which is used for deciding the packet forwarding.

Packet Forwarding in Router:

Routers are used on the network for forwarding a packet from the local network to the remote network. So, the process of routing involves the packet forwarding from an entry interface out to an exit interface.



Working:

The following steps are included in the packet forwarding in the router-

- The router takes the arriving packet from an entry interface and then forwards that packet to another interface.
- The router needs to select the best possible interface for the packet to reach the intended destination as there exist multiple interfaces in the router.
- The forwarding decision is made by the router based on routing table entries. The entries in the routing table comprise destination networks and exit interfaces to which the packet is to be forwarded.
- The selection of exit interface relies on- firstly, the interface must lead to the target network to which the packet is intended to send, and secondly, it must be the best possible path leading to the destination network.

Packet Forwarding Techniques:

Following are the packet forwarding techniques based on the destination host:

- **Next-Hop Method:** By only maintaining the details of the next hop or next router in the packet's path, the next-hop approach reduces the size of the routing table. The routing table maintained using this method does not have the information regarding the whole route that the packet must take.
- **Network-Specific Method:** In this method, the entries are not made for all of the destination hosts in the router's network. Rather, the entry is made of the destination networks that are connected to the router.
- **Host-Specific Method:** In this method, the routing table has the entries for all of the destination hosts in the destination network. With the increase in the size of the routing table, the efficiency of the routing table decreases. It finds its application in the process of verification of route and security purposes.
- **Default Method:** Let's assume- A host in network N1 is connected to two routers, one of which (router R1) is connected to network N2 and the other router R2 to the rest of the internet. As a result, the routing table only has one default entry for the router R2.

5.IPV4

The identifier used in the IP layer of the TCP/IP protocol suite to identify the connection of each device to the Internet is called the Internet address or IP address. Internet Protocol version 4 (IPv4) is the fourth version in the development of the Internet Protocol (IP) and the first version of the protocol to be widely deployed. IPv4 is described in IETF publication in September 1981.The IP address is the address of the connection, not the host or the router.

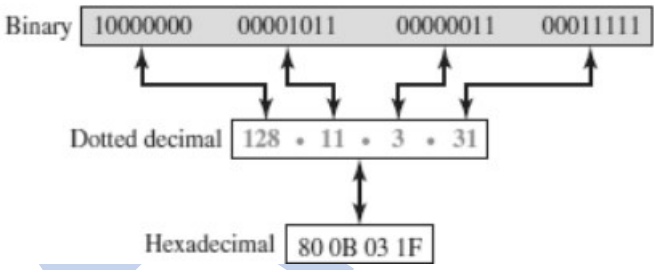
An IPv4 address is a 32-bit address that uniquely and universally defines the connection .

- If the device is moved to another network, the IP address may be changed.

IPv4 addresses are unique in the sense that each address defines one, and only one, connection to the Internet.If a device has two connections to the Internet, via two networks, it has two IPv4 addresses. Pv4 addresses are universal in the sense that the addressing system must be accepted by any host that wants to be connected to the Internet.

IPV4 ADDRESS SPACE

IPv4 defines addresses has an address space. An address space is the total number of addresses used by the protocol. If a protocol uses b bits to define an address, the address space is 2b because each bit can have two different values (0 or 1). IPv4 uses 32-bit addresses, which means that the address space is 232 or 4,294,967,296 (more than four billion). 4 billion devices could be connected to the Internet. IPV4 ADDRESS NOTATION There are three common notations to show an IPv4 address: (i) binary notation (base 2), (ii) dotted-decimal notation (base 256), and (ii) hexadecimal notation (base 16).

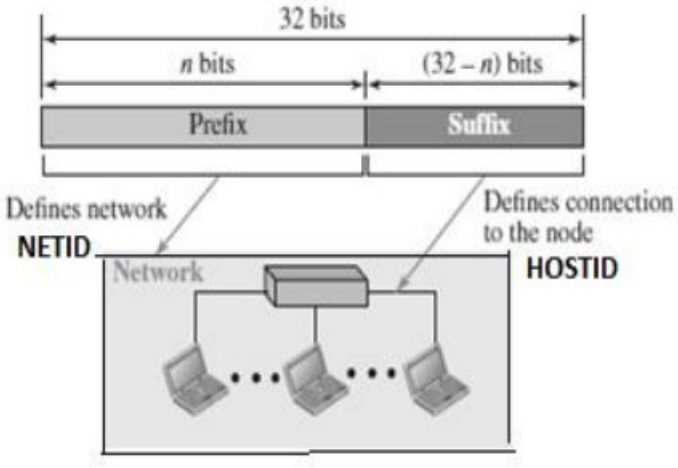


In binary notation, an IPv4 address is displayed as 32 bits. To make the address more readable, one or more spaces are usually inserted between bytes (8 bits). In dotted-decimal notation,IPv4 addresses are usually written in decimal form with a decimal point (dot) separating the bytes. Each number in the dotted-decimal notation is between 0 and 255. In hexadecimal notation, each hexadecimal digit is equivalent to four bits. This means that a 32-bit address has 8 hexadecimal digits. This notation is often used in network programming.

HIERARCHY IN IPV4 ADDRESSING

- In any communication network that involves delivery, the addressing system is hierarchical.A 32-bit IPv4 address is also hierarchical, but divided only into two parts.

- The first part of the address, called the prefix, defines the network(Net ID); the second part of the address, called the suffix, defines the node (Host ID). • The prefix length is n bits and the suffix length is (32- n) bits.
- A prefix can be fixed length or variable length.
- The network identifier in the IPv4 was first designed as a fixed-length prefix.
- This scheme is referred to as classful addressing.
- The new scheme, which is referred to as classless addressing, uses a variable length network prefix.

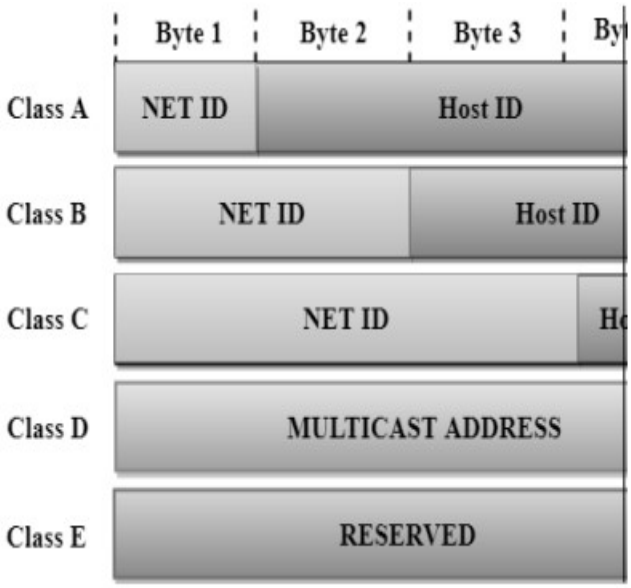


CATEGORIES OF IPV4 ADDRESSING

- There are two broad categories of IPv4 Addressing techniques.
- They are ¬ Classful Addressing ¬ Classless Addressing

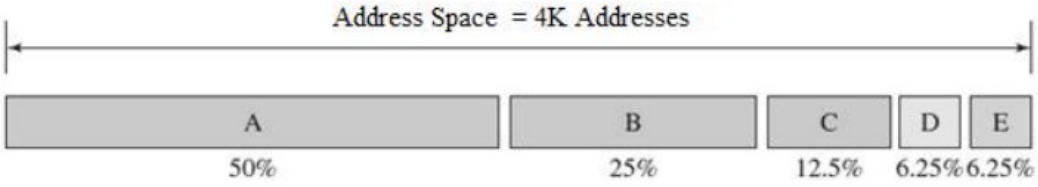
CLASSFUL ADDRESSING

An IPv4 address is 32-bit long(4 bytes). An IPv4 address is divided into sub-classes:



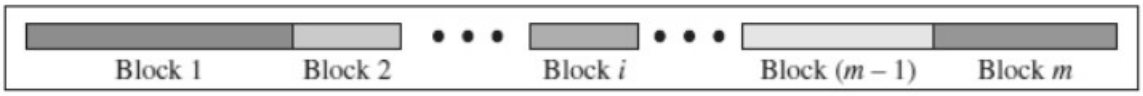
Class	Prefixes	First byte
A	n = 8 bits	0 to 127
B	n = 16 bits	128 to 191
C	n = 24 bits	192 to 223
D	Not applicable	224 to 239
E	Not applicable	240 to 255

Classful Network Architecture



Class	Higher bits	NET ID bits	HOST ID bits	No. of Networks	No.of hosts per network	Range
A	0	8	24	2^7	2^{24}	0.0.0.0 **to** 127.255.255.255
B	10	16	16	2^{14}	2^{16}	128.0.0.0 **to** 191.255.255.255
C	110	24	8	2^{21}	2^8	192.0.0.0 **to** 223.255.255.255
D	1110	Not Defined	Not Defined	Not Defined	Not Defined	224.0.0.0 **to** 239.255.255.255
E	1111	Not Defined	Not Defined	Not Defined	Not Defined	240.0.0.0 **to** 255.255.255.255

Address Depletion in Classful Addressing

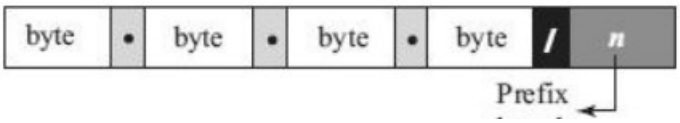
- The reason that classful addressing has become obsolete is address depletion
- Since the addresses were not distributed properly, the Internet was faced with the problem of the addresses being rapidly used up.
- This results in no more addresses available for organizations and individuals that needed to be connected to the Internet.
- To understand the problem, let us think about class A.
- This class can be assigned to only 128 organizations in the world, but each organization needs to have a single network with 16,777,216 nodes .
- Since there may be only a few organizations that are this large, most of the addresses in this class were wasted (unused).
- Class B addresses were designed for midsize organizations, but many of the addresses in this class also remained unused.
- Class C addresses have a completely different flaw in design. The number of addresses that can be used in each network (256) was so small that most companies were not comfortable using a block in this address class.
- Class E addresses were almost never used, wasting the whole class. Advantage of Classful Addressing
- 

- Although classful addressing had several problems and became obsolete, it had one advantage.
- To alleviate address depletion, two strategies were proposed and implemented: (i) Subnetting and (ii) Super netting.
- In subnetting, a class A or class B block is divided into several subnets. Each subnet has a larger prefix length than the original network.
- For example, if a network in class A is divided into four subnets, each subnet has a prefix of nsub = 10.
- At the same time, if all of the addresses in a network are not used, subnetting allows the addresses to be divided among several organizations.

CLASSLESS ADDRESSING

- In 1996, the Internet authorities announced a new architecture called classless addressing. In classless addressing, variable-length blocks are used that belong to no classes. We can have a block of 1 address, 2 addresses, 4 addresses, 128 addresses, and so on.
- In classless addressing, the whole address space is divided into variable length blocks.
- The prefix in an address defines the block (network); the suffix defines the

node (device). Theoretically, we can have a block of 20 , 21 , 22 , 232 addresses. The number of addresses in a block needs to be a power of 2. An organization can be granted one block of addresses.



Examples:
12.24.76.8/8
23.14.67.92/12
220.8.24.255/25

For example , 192.168.100.14 /24 represents the IP address 192.168.100.14 and, its subnet mask 255.255.255.0, which has 24 leading 1-bits. Address Aggregation

One of the advantages of the CIDR strategy is address aggregation (sometimes called address summarization or route summarization). When blocks of addresses are combined to create a larger block, routing can be done based on the prefix of the larger block. ICANN assigns a large block of addresses to an ISP. Each ISP in turn divides its assigned block into smaller subblocks and grants the subblocks to its customers. Special Addresses in IPv4 There are five special addresses that are used for special purposes: this-host address, limited-broadcast address, loopback address, private addresses, and multicast addresses

6.IPV6

IPv6 was evolved to solve address space problem and offers rich set of services. Some hosts and routers will run IPv4 only, some will run IPv4 and IPv6 and some will run IPv6 only.

DRAWBACKS OF IPV4

- Despite subnetting and CIDR, address depletion is still a long-term problem.
- Internet must accommodate real-time audio and video transmission that
- requires minimum delay strategies and reservation of resources.
- Internet must provide encryption and authentication of data for some
- applications

FEATURES OF IPV6

1. ***Better header format*** - IPv6 uses a new header format in which options areseparated from the base header and inserted, when needed, between the baseheader and the data. This simplifies and speeds up the routing process becausemost of the options do not need to be checked by routers.
2. ***New options*** - IPv6 has new options to allow for additional functionalities.
3. ***Allowance for extension*** - IPv6 is designed to allow the extension of the protocol if required by new technologies or applications.
4. ***Support for resource allocation*** - In IPv6, the type-of-service field has beenremoved, but two new fields, traffic class and flow label, have been added

toenable the source to request special handling of the packet. This mechanismcan be used to support traffic such as real-time audio and video.

Additional Features :

- Need to accommodate scalable routing and addressing
- Support for real-time services
- Security support
- Autoconfiguration -
- The ability of hosts to automatically configure themselves with such
- information as their own IP address and domain name.
- Enhanced routing functionality, including support for mobile hosts
- Transition from ipv4 to ipv6

ADDRESS SPACE ALLOCATION OF IPV6

- IPv6 provides a 128-bit address space to handle up to 3.4 × 1038 nodes.
- IPv6 uses *classless* addressing, but classification is based on MSBs.
- The address space is subdivided in various ways based on the leading bits.
- The current assignment of prefixes is listed in Table

Prefix	Use
00. . . 0 (128 bits)	Unspecified
00. . . 1 (128 bits)	Loopback
1111 1111	Multicast addresses
1111 1110 10	Link-local unicast
Everything else	Global Unicast Addresses

GLOBAL UNICAST

- Large chunks (87%) of address space are left *unassigned* for future use.
- IPv6 defines two types of *local* addresses for private networks.
  - *Link local* - enables a host to construct an address that need not be globally unique.
  - *Site local* - allows valid local address for use in a isolated site with several subnets.
- *Reserved* addresses start with prefix of eight 0's.
- *Unspecified address* is used when a host does not know its address
- *Loopback address* is used for testing purposes before connecting
- *Compatible address* is used when IPv6 hosts uses IPv4 network

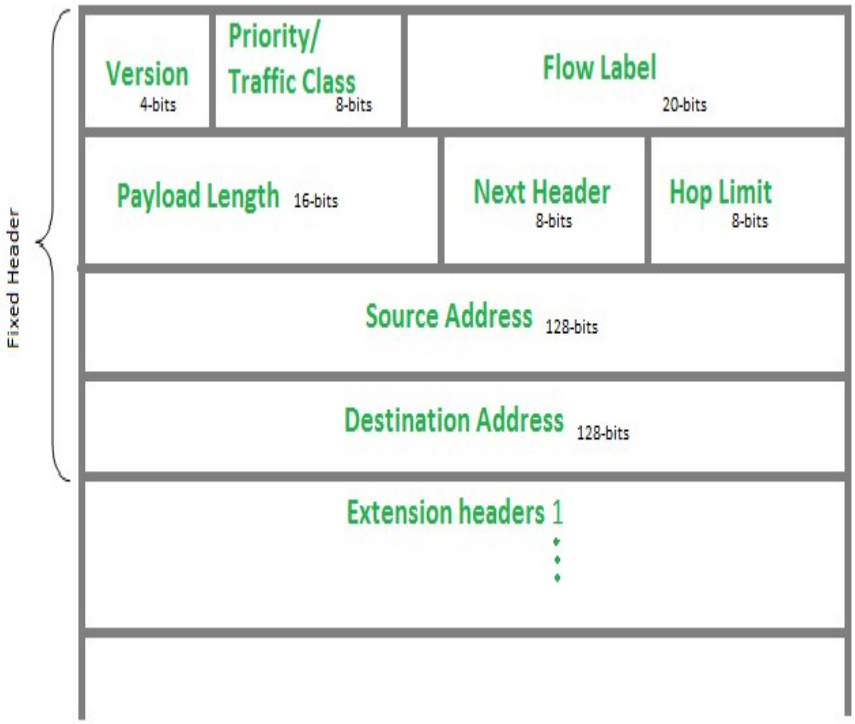
- M*apped address* is used when a IPv6 host communicates with a IPv4 host
- IPv6 defines *anycast* address, assigned to a set of interfaces.
- Packet with anycast address is delivered to only one of the nearest interface.
- Standard representation of IPv6 address is $x : x : x : x : x : x : x : x$ where x is a
- 16-bit hexadecimal address separated by colon (:).
- For example,

47CD :1234 : 4422 : ACO2 : 0022 : 1234 : A456 : 0124

IPV6 HEADER FORMAT

Version (4-bits): Indicates version of Internet Protocol which contains bit sequence 0110.

Traffic Class (8-bits): The Traffic Class field indicates class or priority of IPv6 packet which is similar to *Service Field* in IPv4 packet. It helps routers to handle the traffic based on the priority of the packet. If congestion occurs on the router then packets with the least priority will be discarded. As of now, only 4-bits are being used (and the remaining bits are under research), in which 0 to 7 are assigned to Congestion controlled traffic and 8 to 15 are assigned to Uncontrolled traffic.



Uncontrolled data traffic is mainly used for Audio/Video data. So we give higher priority to Uncontrolled data traffic.
The source node is allowed to set the priorities but on the way, routers can change it. Therefore, the destination should not expect the same priority which was set by the source node.

Flow Label (20-bits): Flow Label field is used by a source to label the packets belonging to the same flow in order to request special handling by intermediate IPv6 routers, such as non-default quality of service or real-time service. In order to distinguish the flow, an intermediate router can use the source address, a destination address, and flow label of the packets. Between a source and destination, multiple flows may exist because many processes might be running at the same time. Routers or Host that does not support the functionality of flow label field and for default router handling, flow label field is set to 0. While setting up the flow label, the source is also supposed to specify the lifetime of the flow.

Payload Length (16-bits): It is a 16-bit (unsigned integer) field, indicates the total size of the payload which tells routers about the amount of information a particular packet contains in its payload. The payload Length field includes extension headers(if any) and an upper-layer packet. In case the length of the payload is greater than 65,535 bytes (payload up to 65,535 bytes can be indicated with 16-bits), then the payload length field will be set to 0 and the jumbo payload option is used in the Hop-by-Hop options extension header.

Next Header (8-bits): Next Header indicates the type of extension header(if present) immediately following the IPv6 header. Whereas In some cases it indicates the protocols contained within upper-layer packets, such as TCP, UDP.

Hop Limit (8-bits): Hop Limit field is the same as TTL in IPv4 packets. It indicates the maximum number of intermediate nodes IPv6 packet is allowed to travel. Its value gets decremented by one, by each node that forwards the packet and the packet is discarded if the value decrements to 0. This is used to discard the packets that are stuck in an infinite loop because of some routing error.

Priority	Meaning
0	No Specific traffic
1	Background data
2	Unattended data traffic
3	Reserved
4	Attended bulk data traffic
5	Reserved
6	Interactive traffic
7	Control traffic

Source Address (128-bits): Source Address is the 128-bit IPv6 address of the original source of the packet.

Destination Address (128-bits): The destination Address field indicates the IPv6 address of the final destination(in most cases). All the intermediate nodes can use this information in order to correctly route the packet.

Extension Headers: In order to rectify the limitations of the *IPv4 Option Field*, Extension Headers are introduced in IP version 6. The extension header mechanism is a very important part of the IPv6 architecture. The next Header field of IPv6 fixed header points to the first Extension Header and this first extension header points to the second extension header and so on.

Advantages of IPv6 :

1. Realtime Data Transmission : Realtime data transmission refers to the process of transmitting data in a very fast manner or **immediately**. Example : Live streaming services such as cricket matches, or other tournament that are streamed on web exactly as soon as it happens with a maximum delay of 5-6 seconds.

2. IPv6 supports authentication: Verifying that the data received by the receiver from the sender is exactly what the sender sent and came through the sender only not from any third party. Example : Matching the hash value of both the messages for verification is also done by IPv6.

3. IPv6 performs Encryption: Ipv6 can encrypt the message at network layer even if the protocols of application layer at user level didn't encrypt the message which is a major advantage as it takes care of encryption.

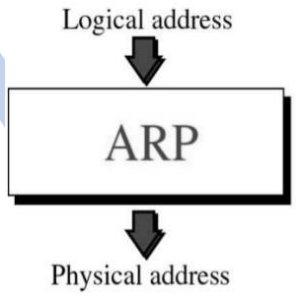
4. Faster processing at Router: Routers are able to process data packets of Ipv6 much faster due to smaller **Base header** of fixed size – 40 bytes which helps in decreasing processing time resulting in more efficient packet

transmission. Whereas in Ipv4, we have to calculate the length of header which lies between 20-60 bytes.

7.ARP

Address Resolution Protocol (ARP) is a protocol or procedure that connects an ever-changing Internet Protocol (IP) address to a fixed physical machine address, also known as a media access control (MAC) address, in a local-area network (LAN). This mapping procedure is important because the lengths of the IP and MAC addresses differ, and a translation is needed so that the systems can recognize one another. The most used IP today is IP version 4 (IPv4). An IP address is 32 bits long. However, MAC addresses are 48 bits long. ARP translates the 32-bit address to 48 and vice versa.There is a networking model known as the Open Systems Interconnection (OSI) model. First developed in the late 1970s, the OSI model uses layers to give IT teams a visualization of what is going on with a particular networking system. This can be helpful in determining which layer affects which application, device, or software installed on the network, and further, which IT or engineering professional is responsible for managing that layer.

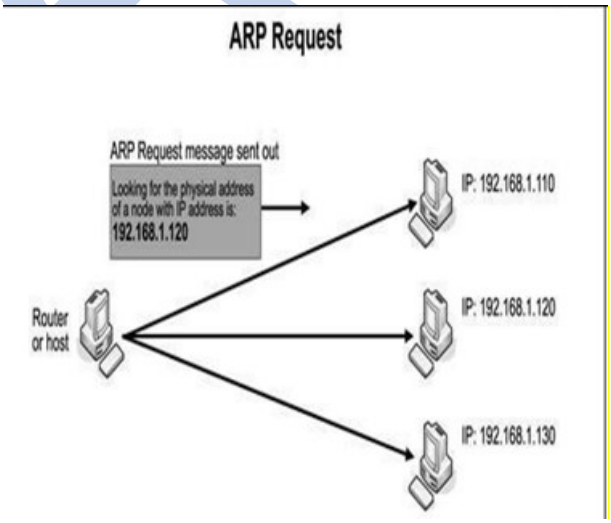
The MAC address is also known as the data link layer, which establishes and terminates a connection between two physically connected devices so that data transfer can take place. The IP address is also referred to as the network layer or the layer responsible for forwarding packets of data through different routers. ARP works between these layers.



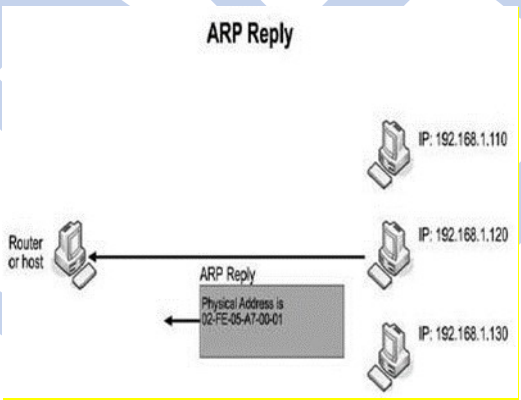
Packets of data arrive at a gateway, destined for a particular host machine. The gateway, or the piece of hardware on a network that allows data to flow from one network to another, asks the ARP program to find a MAC address that matches the IP address. The ARP cache keeps a list of each IP address and its matching MAC address. The ARP cache is dynamic, but users on a network can also configure a static ARP table containing IP addresses and MAC addresses.ARP caches are kept on all operating systems in an IPv4 Ethernet network.

Every time a device requests a MAC address to send data to another device connected to the LAN, the device verifies its ARP cache to see if the IP-to-MAC-address connection has already been completed. If it exists, then a new request is unnecessary. However, if the translation has not yet been carried out, then the request for network addresses is sent, and ARP is performed.An ARP cache size is limited by design, and addresses tend to stay in the cache for only a few minutes. It is purged regularly to free up space.

This design is also intended for privacy and security to prevent IP addresses from being stolen or spoofed by cyberattackers. While MAC addresses are fixed, IP addresses are constantly updated.In the purging process, unutilized addresses are deleted; so is any data related to unsuccessful attempts to communicate with computers not connected to the network or that are not even powered on.



ARP is the process of connecting a dynamic IP address to a physical machine's MAC address. As such, it is important to have a look at a few technologies related to IP.As mentioned previously, IP addresses, by design, are changed constantly for the simple reason that doing so gives users security and privacy. However changes on IP addresses should not be completely random. There should be rules that allocate an IP address from a defined range of numbers available in a specific network. This helps prevent issues, such as two computers receiving the same IP address. The rules are known as DHCP or Dynamic Host Configuration Protocol. IP addresses as identities for computers are important because they are needed to perform an internet search. When users search for a domain name or Uniform Resource Locator (URL), they use an alphabetical name. Computers, on the other hand, use the numerical IP address to associate the domain name with a server. To connect the two, a Domain Name System (DNS) server is used to translate an IP address from a confusing string of numbers into a more readable, easily understandable domain name, and vice versa



Hardware Type		Protocol Type
Hardware length	Protocol length	Operation Request:1, Reply:2
Source hardware address		
Source protocol address		
Destination hardware address (Empty in request)		
Destination protocol address		

8.RARP

The Reverse Address Resolution Protocol (RARP) is an obsolete computer communication protocol used by a client computer to request its Internet Protocol (IPv4) address from a computer network, when all it has available is its link layer or hardware address, such as a MAC address. The client broadcasts the request and does not need prior knowledge of the network topology or the identities of servers capable of fulfilling its request.

RARP is described in Internet Engineering Task Force (IETF) publication RFC 903.[1] It has been rendered obsolete by the Bootstrap Protocol (BOOTP) and the modern Dynamic Host Configuration Protocol (DHCP), which both support a much greater feature set than RARP.

RARP requires one or more server hosts to maintain a database of mappings of Link Layer addresses to their respective protocol addresses. Media Access Control (MAC) addresses need to be individually configured on the servers by an administrator. RARP is limited to serving only IP addresses.

Reverse ARP differs from the Inverse Address Resolution Protocol (InARP) described in RFC 2390, which is designed to obtain the IP address associated with a local Frame Relay data link connection identifier. InARP is not used in Ethernet.

Reverse Address Resolution Protocol (RARP) is a protocol a physical machine in a local area network (LAN) can use to request its IP address. It does this by sending the device's physical address to a specialized RARP server that is on the same LAN and is actively listening for RARP requests.

RARP WORKING:A network administrator creates a table in a RARP server that maps the physical interface or media access control (MAC) addresses to corresponding IP addresses. This table can be referenced by devices seeking to dynamically learn their IP address. When a new RARP-enabled device first connects to the network, its RARP client program sends its physical MAC address to the RARP server for the purpose of receiving an IP address in return that the device can use to communicate with other devices on the IP network. The RARP request is sent in the form of a data link layer broadcast. It is, therefore, important that the RARP server be on the same LAN as the devices requesting IP address information.Assuming an entry for the device's MAC address is set up in the RARP database, the RARP server returns the IP address associated with the device's specific MAC address.

The general RARP process flow follows these steps:

1. Device 1 connects to the local network and sends an RARP broadcast to all devices on the subnet. In the RARP broadcast, the device sends its physical MAC address and requests an IP address it can use.
2. Because a broadcast is sent, device 2 receives the broadcast request. However, since it is not a RARP server, device 2 ignores the request.
3. The broadcast message also reaches the RARP server. The server processes the packet and attempts to find device 1's MAC address in the RARP lookup table. If one is found, the RARP server returns the IP address assigned to the device. In this case, the IP address is 51.100.102.

DIFFERENCE BETWEEN ARP AND RARP

ARP	RARP
A protocol used to map an IP address to a physical (MAC) address	A protocol used to map a physical (MAC) address to an IP address
To obtain the MAC address of a network device when only its IP address is known	To obtain the IP address of a network device when only its MAC address is known
Client broadcasts its IP address and requests a MAC address, and the server responds with the corresponding MAC address	Client broadcasts its MAC address and requests an IP address, and the server responds with the corresponding IP address
IP addresses	MAC addresses
Widely used in modern networks to resolve IP addresses to MAC addresses	Rarely used in modern networks as most devices have a pre-assigned IP address
ARP stands for Address Resolution Protocol.	Whereas RARP stands for Reverse Address Resolution Protocol.

ARP	RARP
Through ARP, (32-bit) IP address mapped into (48-bit) MAC address.	Whereas through RARP, (48-bit) MAC address of 48 bits mapped into (32-bit) IP address.
In ARP, broadcast MAC address is used.	While in RARP, broadcast IP address is used.
In ARP, ARP table is managed or maintained by local host.	While in RARP, RARP table is managed or maintained by RARP server.
In Address Resolution Protocol, Receiver's MAC address is fetched.	While in RARP, IP address is fetched.
In ARP, ARP table uses ARP reply for its updation.	While in RARP, RARP table uses RARP reply for configuration of IP addresses .
Hosts and routers uses ARP for knowing the MAC address of other hosts and routers in the networks.	While RARP is used by small users having less facilities.

9.ICMP

Internet Control Message Protocol (ICMP) is a network layer protocol used to diagnose communication errors by performing an error control mechanism. Since 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 is used for reporting errors and management queries. It is a supporting protocol and is used by network devices like routers for sending error messages and operations information. For example, the requested service is not available or a host or router could not be reached.

Uses of ICMP

ICMP is used for error reporting if two devices connect over the internet and some error occurs, So, the router sends an ICMP error message to the source informing about the error. For Example, whenever a device sends any

message which is large enough for the receiver, in that case, the receiver will drop the message and reply back ICMP message to the source.Another important use of ICMP protocol is used to perform network diagnosis by making use of traceroute and ping utility. We will discuss them one by one.

Traceroute: Traceroute utility is used to know the route between two devices connected over the internet. It routes the journey from one router to another, and a traceroute is performed to check network issues before data transfer.

Ping: Ping is a simple kind of traceroute known as the echo-request message, it is used to measure the time taken by data to reach the destination and return to the source, these replies are known as echo-replies messages.

How Does ICMP Work?

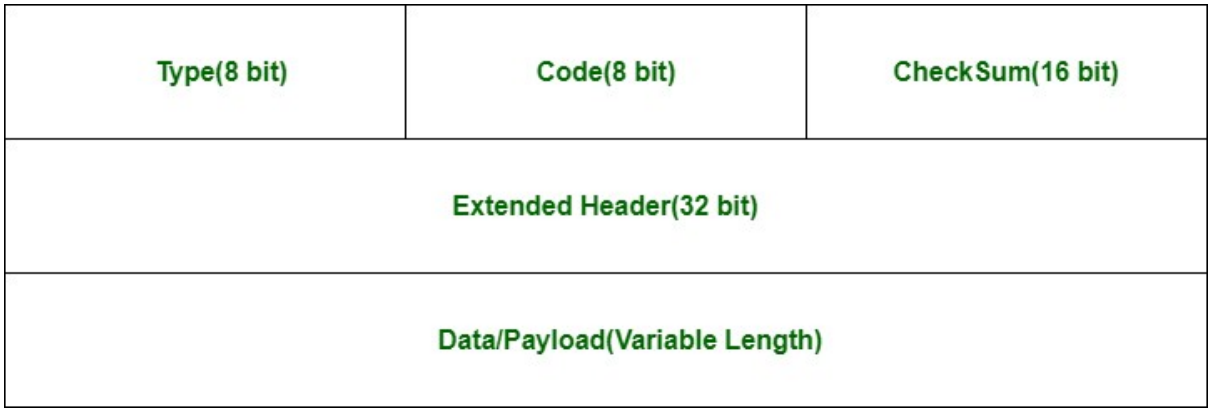
ICMP is the primary and important protocol of the IP suite, but ICMP isn't associated with any transport layer protocol (TCP or UDP) as it doesn't need to establish a connection with the destination device before sending any message as it is a connectionless protocol.

The working of ICMP is just contrasting with TCP, as TCP is a connection-oriented protocol whereas ICMP is a connectionless protocol. Whenever a connection is established before the message sending, both devices must be ready through a TCP Handshake.

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 Packet Format

ICMP header comes after IPv4 and IPv6 packet header.



In the ICMP packet format, the first 32 bits of the packet contain three fields:

Type (8-bit): The initial 8-bit of the packet is for message type, it provides a brief description of the message so that receiving network would know what kind of message it is receiving and how to respond to it. Some common message types are as follows:

- Type 0 – Echo reply
- Type 3 – Destination unreachable
- Type 5 – Redirect Message
- Type 8 – Echo Request
- Type 11 – Time Exceeded
- Type 12 – Parameter problem

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. Byte locations are identified by the pointer which causes the problem message and receiving device looks here for pointing to the problem.

The last part of the ICMP packet is Data or Payload of variable length. The bytes included in IPv4 are 576 bytes and in IPv6, 1280 bytes.

ICMP in DDoS Attacks

In Distributed DOS (DDoS) attacks, attackers provide so much extra traffic to the target, so that it cannot provide service to users. There are so many ways through which an attacker executes these attacks, which are described below.

Ping of Death Attack

Whenever an attacker sends a ping, whose size is greater than the maximum allowable size, oversized packets are broken into smaller parts. When the sender re-assembles it, the size exceeds the limit which causes a buffer overflow and makes the machine freeze. This is simply called a Ping of Death Attack. Newer devices have protection from this attack, but older devices did not have protection from this attack.

ICMP Flood Attack

Whenever the sender sends so many pings that the device on whom the target is done is unable to handle the echo request. This type of attack is called an ICMP Flood Attack. This attack is also called a ping flood attack. It stops the target computer's resources and causes a denial of service for the target computer.

Smurf Attack

Smurf Attack is a type of attack in which the attacker sends an ICMP packet with a spoofed source IP address. These type of attacks generally works on older devices like the ping of death attack.

Types of ICMP Messages

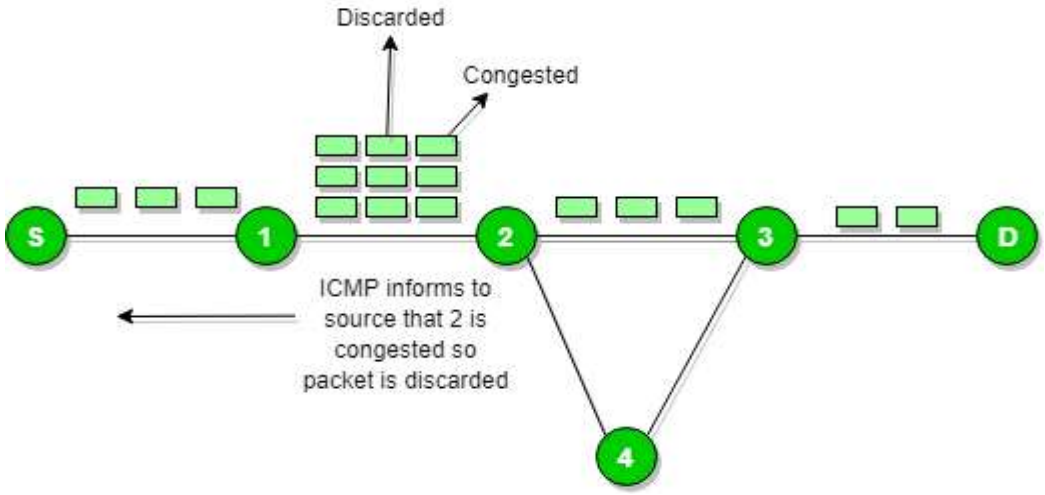
Type	Code	Description
0 – Echo Reply	0	Echo reply
3 – Destination Unreachable	0	Destination network unreachable
	1	Destination host unreachable
	2	Destination protocol unreachable
	3	Destination port unreachable
	4	Fragmentation is needed and the DF flag set
	5	Source route failed
5 – Redirect Message	0	Redirect the datagram for the network

Type	Code	Description
	1	Redirect datagram for the host
	2	Redirect the datagram for the Type of Service and Network
	3	Redirect datagram for the Service and Host
8 – Echo Request	0	Echo request
9 – Router Advertisement	0	Use to discover the addresses of operational routers
10 – Router Solicitation	0	
11 – Time Exceeded	0	Time to live exceeded in transit
	1	Fragment reassembly time exceeded.
12 – Parameter Problem	0	The pointer indicates an error.
	1	Missing required option
	2	Bad length
13 – Timestamp	0	Used for time synchronization

Type	Code	Description
14 – Timestamp Reply	0	Reply to Timestamp message

Source Quench Message

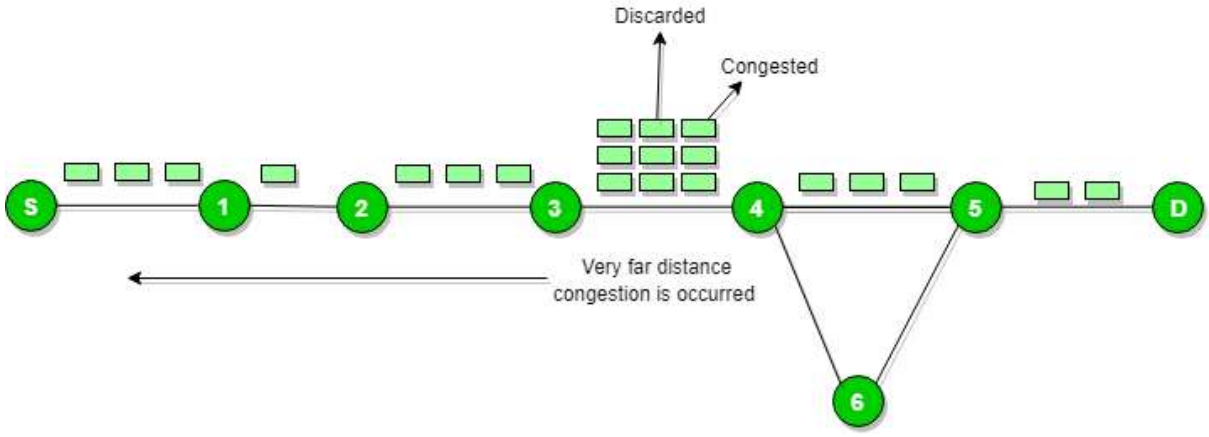
A source quench message is a request to decrease the traffic rate for messages sent to the host destination) or we can say when receiving host detects that the rate of sending packets (traffic rate) to it is too fast it sends the source quench message to the source to slow the pace down so that no packet can be lost.



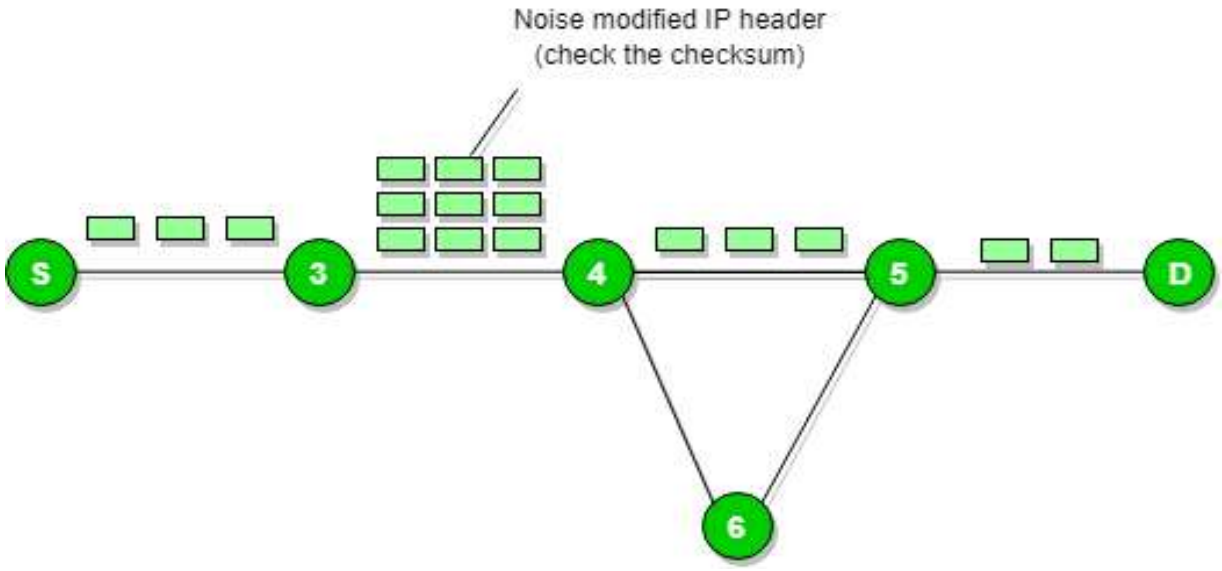
ICMP will take the source IP from the discarded packet and inform the source by sending a source quench message. The source will reduce the speed of transmission so that router will be free from congestion.

Parameter

Problem



Whenever packets come to the router then the calculated header checksum should be equal to the received header checksum then only the packet is accepted by the router.

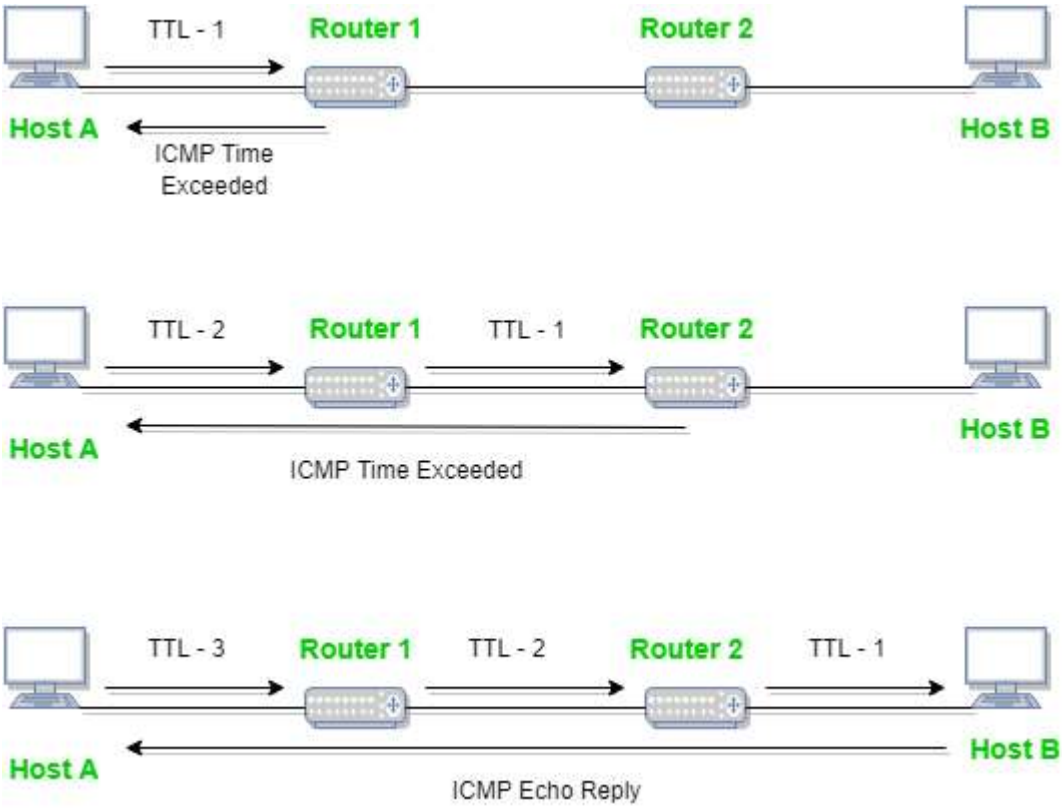


Parameter Problem

If there is a mismatch packet will be dropped by the router.

ICMP will take the source IP from the discarded packet and inform the source by sending a parameter problem message.

Time Exceeded Message

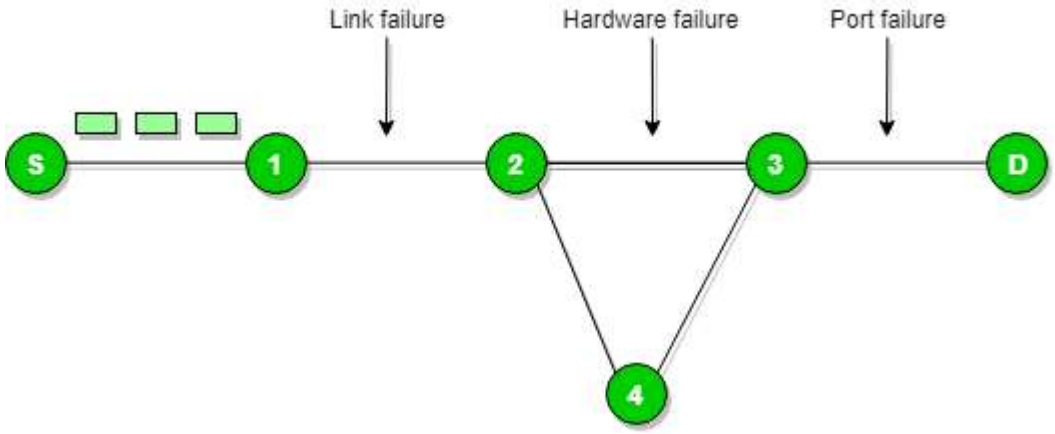


Time Exceeded Message

When some fragments are lost in a network then the holding fragment by the router will be dropped then ICMP will take the source IP from the discarded packet and informs the source, of discarded datagram due to the time to live field reaching zero, by sending the time exceeded message.

Destination Un-reachable

The destination is unreachable and is generated by the host or its inbound gateway to inform the client that the destination is unreachable for some reason.



Destination Un-reachable

There is no necessary condition that only the router gives the ICMP error message time the destination host sends an ICMP error message when any type of failure (link failure, hardware failure, port failure, etc) happens in the network.

Redirection Message

Redirect requests data packets are sent on an alternate route. The message informs a host to update its routing information (to send packets on an alternate route).

Example: If the host tries to send data through a router R1 and R1 sends data on a router R2 and there is a direct way from the host to R2. Then R1 will send a redirect message to inform the host that there is the best way to the destination directly through R2 available. The host then sends data packets for the destination directly to R2.
The router R2 will send the original datagram to the intended destination. But if the datagram contains routing information then this message will not be sent even if a better route is available as redirects should only be sent by gateways and should not be sent by Internet hosts.

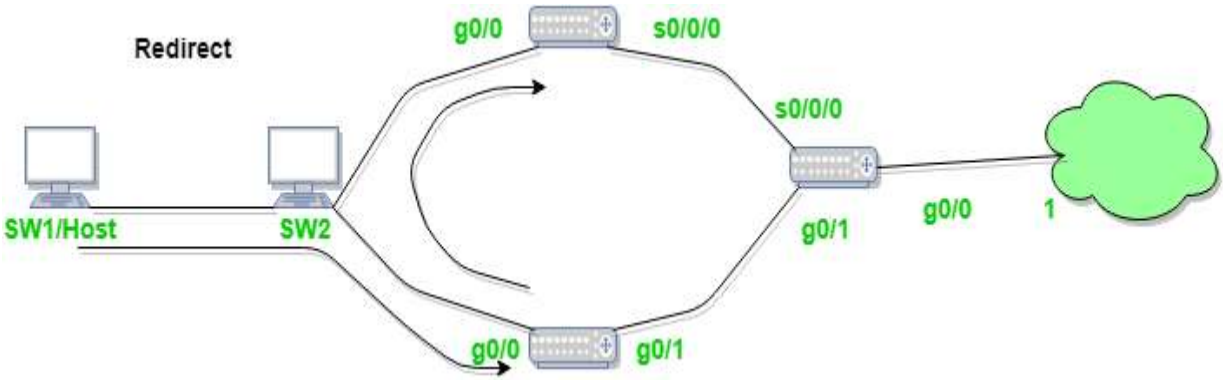


Figure - ICMP redirect Verification CCNP 2.0 100 - 101 (v - 71)

- ICMP Redirect
- ICMP Redirect for host
- ICMP Redirect for network
- How ICMP redirect work
- ICMP Redirect verification step by step

Redirection Message

Whenever a packet is forwarded in the wrong direction later it is re-directed in a current direction then ICMP will send a re-directed message.

10.DHCP

DHCP stands for Dynamic Host Configuration Protocol. It is the critical feature on which the users of an enterprise network communicate. DHCP helps enterprises to smoothly manage the allocation of IP addresses to the end-user clients' devices such as desktops, laptops, cell phones, etc. is an application layer protocol that is used to provide:

Why Use DHCP?

DHCP helps in managing the entire process automatically and centrally. DHCP helps in maintaining a unique IP Address for a host using the server. DHCP servers maintain information on TCP/IP configuration and provide configuration of address to DHCP-enabled clients in the form of a lease offer.

Components of DHCP

The main components of DHCP include:

- **DHCP Server:** DHCP Server is basically a server that holds IP Addresses and other information related to configuration.
- **DHCP Client:** It is basically a device that receives configuration information from the server. It can be a mobile, laptop, computer, or any other electronic device that requires a connection.
- **DHCP Relay:** DHCP relays basically work as a communication channel between DHCP Client and Server.
- **IP Address Pool:** It is the pool or container of IP Addresses possessed by the DHCP Server. It has a range of addresses that can be allocated to devices.
- **Subnets:** Subnets are smaller portions of the IP network partitioned to keep networks under control.
- **Lease:** It is simply the time that how long the information received from the server is valid, in case of expiration of the lease, the tenant must have to re-assign the lease.
- **DNS Servers:** DHCP servers can also provide DNS (Domain Name System) server information to DHCP clients, allowing them to resolve domain names to IP addresses.
- **Default Gateway:** DHCP servers can also provide information about the default gateway, which is the device that packets are sent to when the destination is outside the local network.
- **Options:** DHCP servers can provide additional configuration options to clients, such as the subnet mask, domain name, and time server information.

- **Renewal:** DHCP clients can request to renew their lease before it expires to ensure that they continue to have a valid IP address and configuration information.
- **Failover:** DHCP servers can be configured for failover, where two servers work together to provide redundancy and ensure that clients can always obtain an IP address and configuration information, even if one server goes down.
- **Dynamic Updates:** DHCP servers can also be configured to dynamically update DNS records with the IP address of DHCP clients, allowing for easier management of network resources.
- **Audit Logging:** DHCP servers can keep audit logs of all DHCP transactions, providing administrators with visibility into which devices are using which IP addresses and when leases are being assigned or renewed.

Operation Code	Hardware type	Hardware length	Hop count
Transition ID			
Number of seconds		Flags	
Client IP address			
Your IP address			
Server IP address			
Gateway IP address			
Client hardware address (16 bytes)			

Server name (64 bytes)
Boot file name (128 bytes)
Options (Variable length)

1. Hardware length:

This is an 8-bit field defining the length of the physical address in bytes. E.g. for Ethernet the value is 6.

2. Hop count: This is an 8-bit field defining the maximum number of hops the packet can travel.

3. Transaction ID:

This is a 4-byte field carrying an integer. The transaction identification is set by the client and is used to match a reply with the request. The server returns the same value in its reply.

4. Number of seconds:

This is a 16-bit field that indicates the number of seconds elapsed since the time the client started to boot.

5. Flag:

This is a 16-bit field in which only the leftmost bit is used and the rest of the bit should be set to os.

A leftmost bit specifies a forced broadcast reply from the server. If the reply were to be unicast to the client, the destination. IP address of the IP packet is the address assigned to the client.

6. Client IP address:

This is a 4-byte field that contains the client IP address. If the client does not have this information this field has a value of 0.

7. Your IP address:

This is a 4-byte field that contains the client IP address. It is filled by the server at the request of the client.

8. Server IP address:

This is a 4-byte field containing the server IP address. It is filled by the server in a reply message.

9. Gateway IP address:

This is a 4-byte field containing the IP address of a routers. IT is filled by the server in a reply message.

10. Client hardware address:

This is the physical address of the client .Although the server can retrieve this address from the frame sent by the client it is more efficient if the address is supplied explicitly by the client in the request message.

11. Server name:

This is a 64-byte field that is optionally filled by the server in a reply packet. It contains a null-terminated string consisting of the domain name of the server. If the server does not want to fill this filed with data, the server must fill it with all 0s.

12. Boot filename:

This is a 128-byte field that can be optionally filled by the server in a reply packet. It contains a null- terminated string consisting of the full pathname of the boot file. The client can use this path to retrieve other booting information. If the server does not want to fill this field with data, the server must fill it with all 0s.

13. Options:

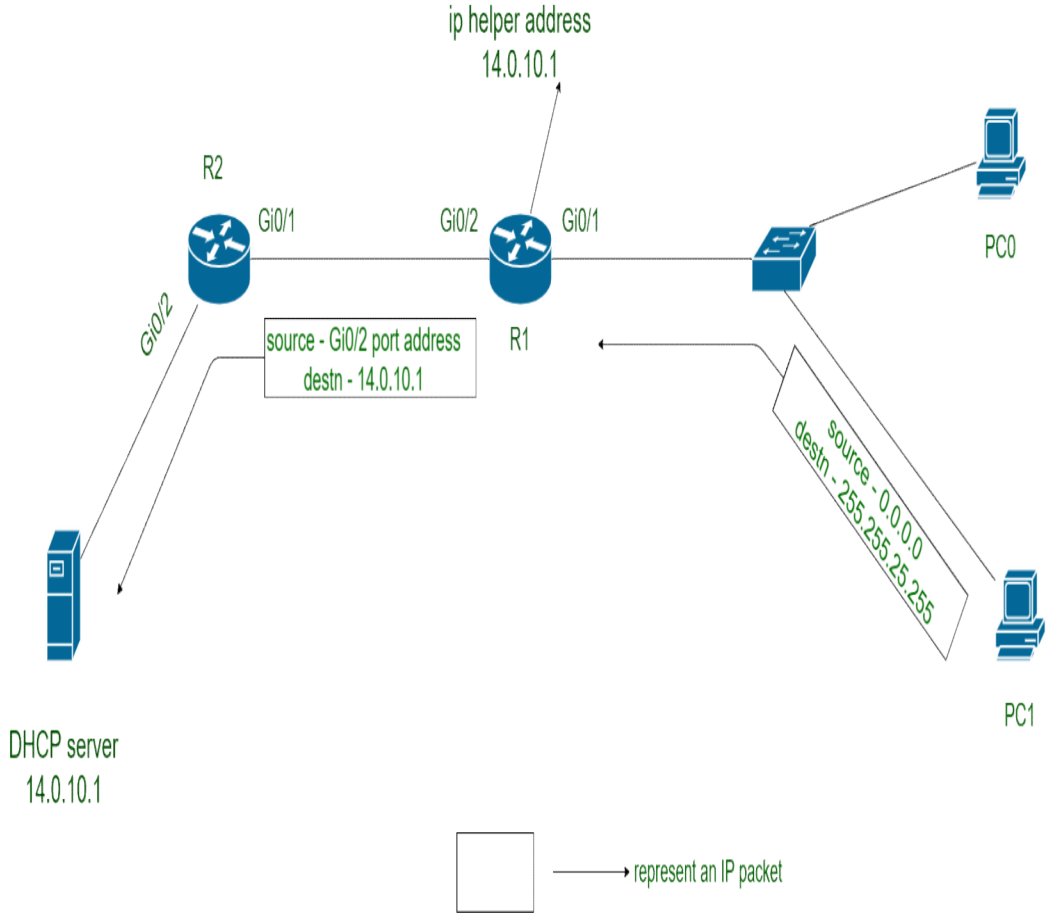
This is a 64-byte field with a dual purpose. IT can carry either additional information or some specific vendor information. The field is used only in a reply message. The server uses a number, called a magic cookie, in the format of an IP address with the value of 99.130.83.99. When the client finishes reading the message, it looks for this magic cookie. If present the next 60 bytes are options.

Working of DHCP

The working of DHCP is as follows:

DHCP works on the Application layer of the TCP/IP Protocol. The main task of DHCP is to dynamically assigns IP Addresses to the Clients and allocate information on TCP/IP configuration to Clients.

The DHCP **port number** for the server is 67 and for the client is 68. It is a client-server protocol that uses UDP services. An IP address is assigned from a pool of addresses. In DHCP, the client and the server exchange mainly 4 DHCP messages in order to make a connection, also called the DORA process, but there are 8 DHCP messages in the process.

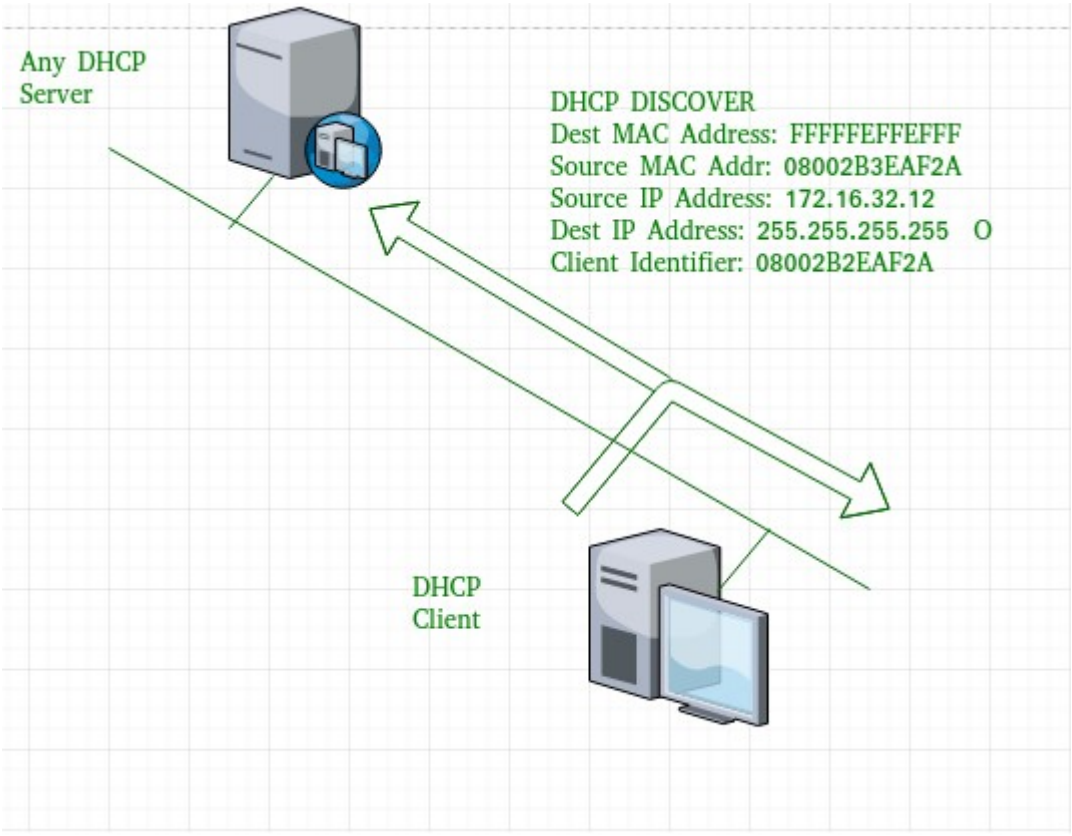


Working of DHCP

The 8 DHCP Messages:

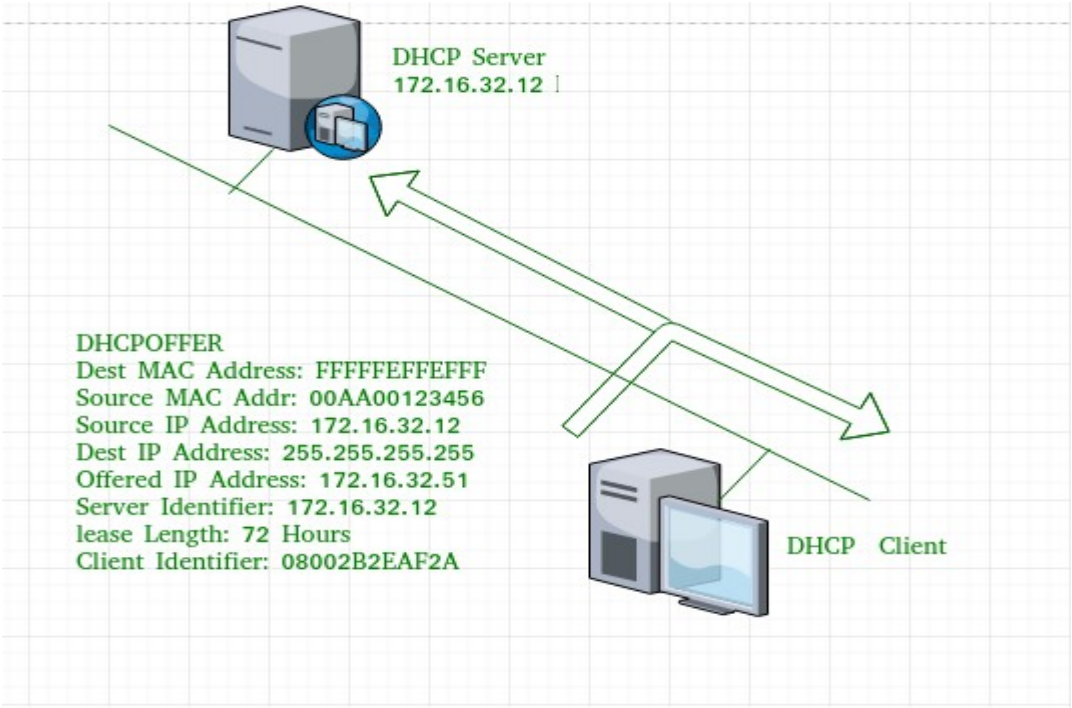
1. DHCP discover message: This is the first message generated in the communication process between the server and the client. This message is generated by the Client host in order to discover if there is any DHCP server/servers are present in a network or not. This message is broadcasted to

all devices present in a network to find the DHCP server. This message is 342 or 576 bytes long



As shown in the figure, the source MAC address (client PC) is 08002B2EAF2A, the destination MAC address(server) is FFFFFFFFFFFF, the source IP address is 0.0.0.0(because the PC has had no IP address till now) and the destination IP address is 255.255.255.255 (IP address used for broadcasting). As they discover message is broadcast to find out the DHCP server or servers in the network therefore broadcast IP address and MAC address is used.

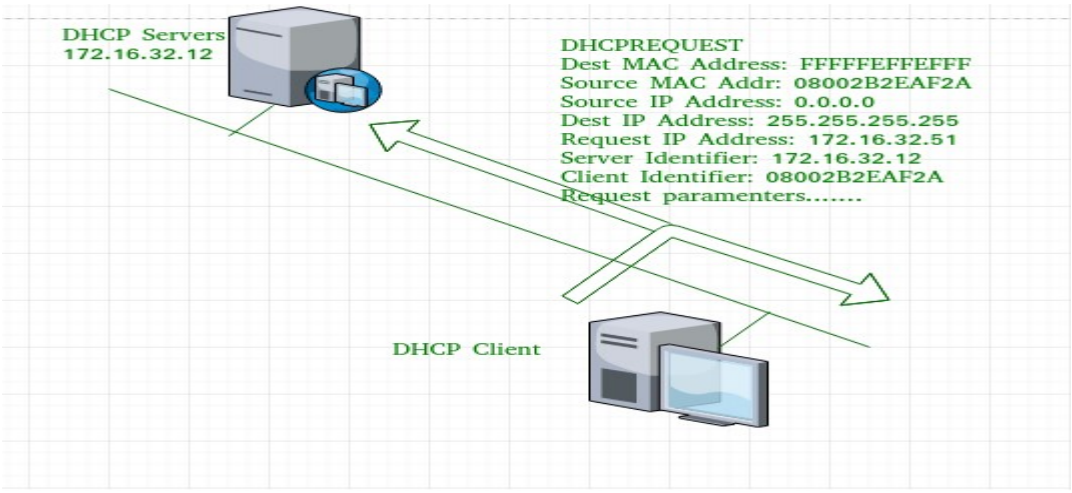
2. DHCP offers a message: The server will respond to the host in this message specifying the unleased IP address and other TCP configuration information. This message is broadcasted by the server. The size of the message is 342 bytes. If there is more than one DHCP server present in the network then the client host will accept the first DHCP OFFER message it receives. Also, a server ID is specified in the packet in order to identify the server.



Now, for the offer message, the source IP address is 172.16.32.12 (server's IP address in the example), the destination IP address is 255.255.255.255 (broadcast IP address), the source MAC address is 00AA00123456, the destination MAC address is FFFFFFFFFFFF. Here, the offer message is broadcast by the DHCP server therefore destination IP address is the broadcast IP address and destination MAC address is FFFFFFFFFFFF and the source IP address is the server IP address and the MAC address is the server MAC address.

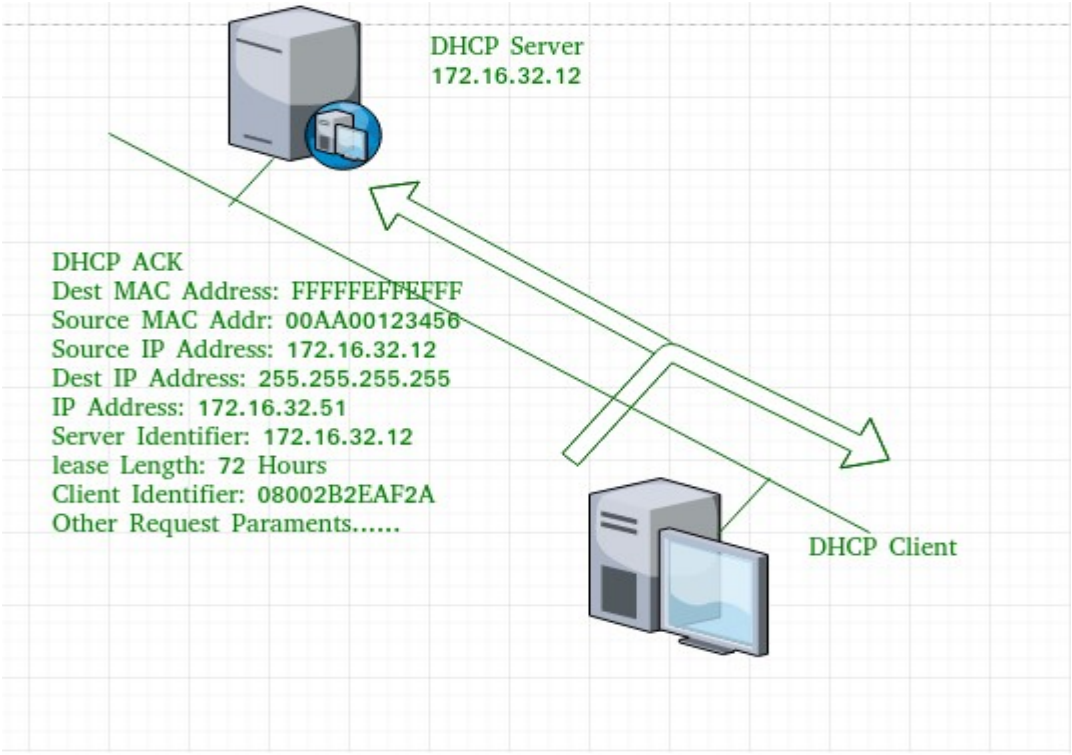
Also, the server has provided the offered IP address 192.16.32.51 and a lease time of 72 hours(after this time the entry of the host will be erased from the server automatically). Also, the client identifier is the PC MAC address (08002B2EAF2A) for all the messages.

3. DHCP request message: When a client receives an offer message, it responds by broadcasting a DHCP request message. The client will produce a gratuitous ARP in order to find if there is any other host present in the network with the same IP address. If there is no reply from another host, then there is no host with the same TCP configuration in the network and the message is broadcasted to the server showing the acceptance of the IP address. A Client ID is also added to this message.



Now, the request message is broadcast by the client PC therefore source IP address is 0.0.0.0(as the client has no IP right now) and destination IP address is 255.255.255.255 (the broadcast IP address) and the source MAC address is 08002B2EAF2A (PC MAC address) and destination MAC address is FFFFFFFFFFFF.

4. DHCP acknowledgment message: In response to the request message received, the server will make an entry with a specified client ID and bind the IP address offered with lease time. Now, the client will have the IP address provided by the server.



Now the server will make an entry of the client host with the offered IP address and lease time. This IP address will not be provided by the server to

any other host. The destination MAC address is FFFFFFFFFFFF and the destination IP address is 255.255.255.255 and the source IP address is 172.16.32.12 and the source MAC address is 00AA00123456 (server MAC address).

5. DHCP negative acknowledgment message: Whenever a DHCP server receives a request for an IP address that is invalid according to the scopes that are configured, it sends a DHCP Nak message to the client. Eg-when the server has no IP address unused or the pool is empty, then this message is sent by the server to the client.

6. DHCP decline: If the DHCP client determines the offered configuration parameters are different or invalid, it sends a DHCP decline message to the server. When there is a reply to the gratuitous ARP by any host to the client, the client sends a DHCP decline message to the server showing the offered IP address is already in use.

7. DHCP release: A DHCP client sends a DHCP release packet to the server to release the IP address and cancel any remaining lease time.

8. DHCP inform: If a client address has obtained an IP address manually then the client uses DHCP information to obtain other local configuration parameters, such as domain name. In reply to the DHCP inform message, the DHCP server generates a DHCP ack message with a local configuration suitable for the client without allocating a new IP address. This DHCP ack message is unicast to the client.

Note – All the messages can be unicast also by the DHCP relay agent if the server is present in a different network.

Advantages of DHCP

The advantages of using DHCP include:

- Centralized management of IP addresses.
- Centralized and automated TCP/IP configuration.
- Ease of adding new clients to a network.
- Reuse of IP addresses reduces the total number of IP addresses that are required.
- The efficient handling of IP address changes for clients that must be updated frequently, such as those for portable devices that move to different locations on a wireless network.
- Simple reconfiguration of the IP address space on the DHCP server without needing to reconfigure each client.

- The DHCP protocol gives the network administrator a method to configure the network from a centralized area.
- With the help of DHCP, easy handling of new users and the reuse of IP addresses can be achieved.

Disadvantages of DHCP

The disadvantage of using DHCP is:

- IP conflict can occur.
- The problem with DHCP is that clients accept any server. Accordingly, when another server is in the vicinity, the client may connect with this server, and this server may possibly send invalid data to the client.
- The client is not able to access the network in absence of a DHCP Server.
- The name of the machine will not be changed in a case when a new IP Address is assigned.

APEC