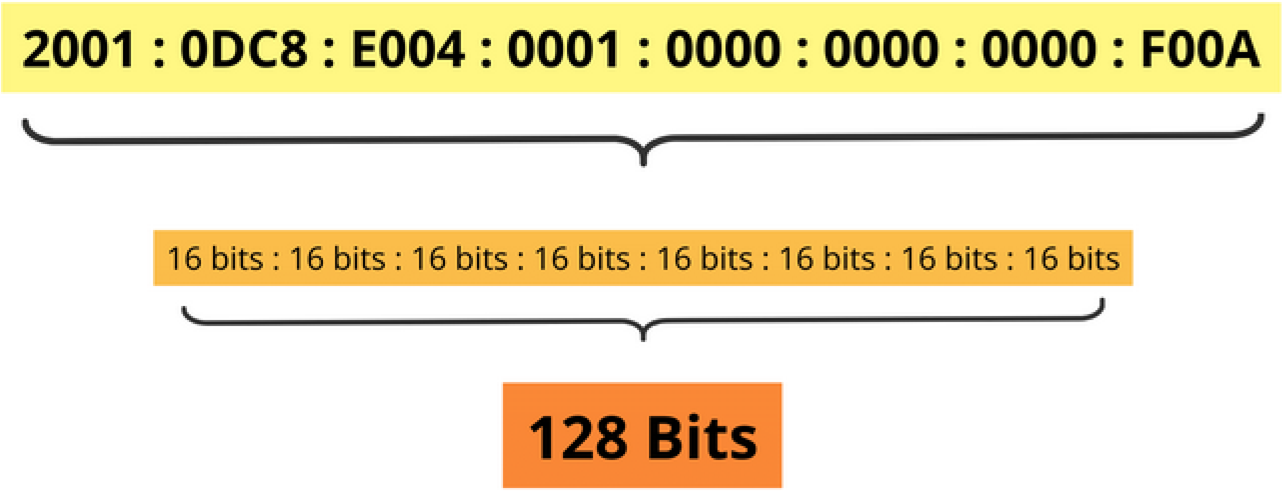
- IPV6
- IPv6 Packet Header Format
- The IPv6 protocol defines a set of headers, including the basic IPv6 header and the IPv6 extension headers.
- The following figure shows the fields that appear in the IPv6 header and the order in which the fields appear.
- Example of IPv6 Address

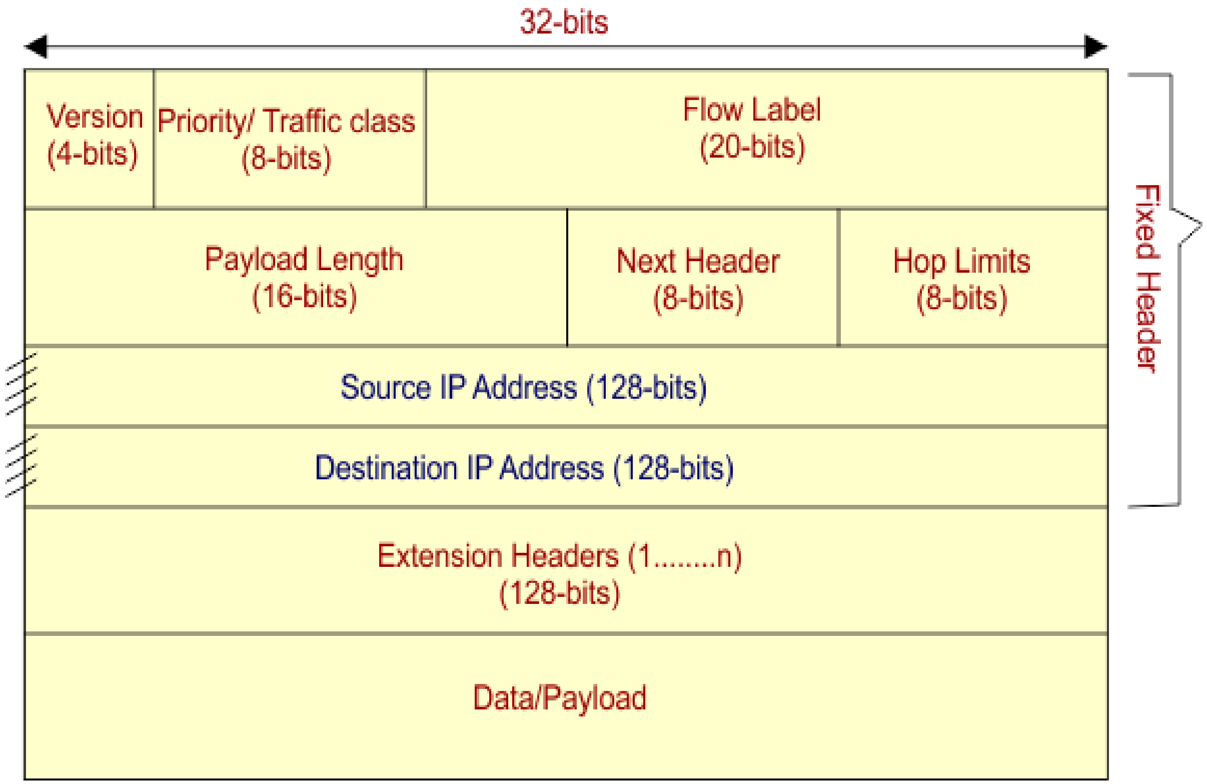


2001 : 0DC8 : E004 : 0001 : 0000 : 0000 : 0000 : F00A

16 bits : 16 bits : 16 bits : 16 bits : 16 bits : 16 bits : 16 bits : 16 bits

128 Bits

- IP version 6 is the new version of Internet Protocol, which is way better than IP version 4 in terms of complexity and efficiency. Let’s look at the header of IP version 6 and understand how it is different from the IPv4 header.



32-bits

Version (4-bits)

Priority/ Traffic class (8-bits)

Flow Label (20-bits)

Payload Length (16-bits)

Next Header (8-bits)

Hop Limits (8-bits)

Source IP Address (128-bits)

Destination IP Address (128-bits)

Extension Headers (1........n) (128-bits)

Data/Payload

Fixed Header

IPV6 Header

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

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

3. Flow Label (20-bits): This label is used to maintain the sequential flow of the packets belonging to a communication. The source labels the sequence to help the router identify that a particular packet belongs to a specific flow of information. This field helps avoid re-ordering of data packets. It is designed for streaming/real-time media.

- 4.Payload Length (16-bits): This field is used to tell the routers how much information a particular packet contains in its payload. Payload is composed of Extension Headers and Upper Layer data. With 16 bits, up to 65535 bytes can be indicated; but if the Extension Headers contain Hop-by-Hop Extension Header, then the payload may exceed 65535 bytes and this field is set to 0.

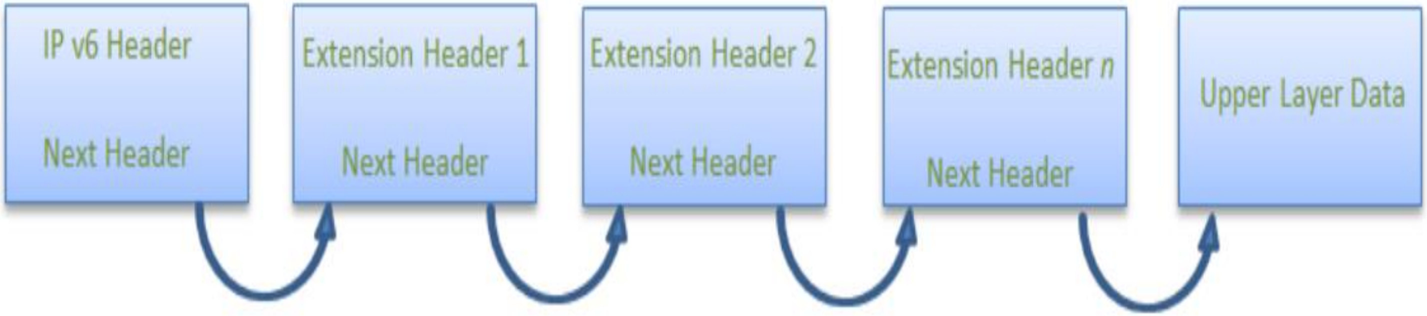
- 5. Next Header (8-bits): This field is used to indicate either the type of Extension Header, or if the Extension Header is not present then it indicates the Upper Layer PDU. The values for the type of Upper Layer PDU are same as IPv4's.

6. Hop Limit (8-bits): This field is used to stop packet to loop in the network infinitely. This is same as TTL in IPv4. The value of Hop Limit field is decremented by 1 as it passes a link (router/hop). When the field reaches infinitely.

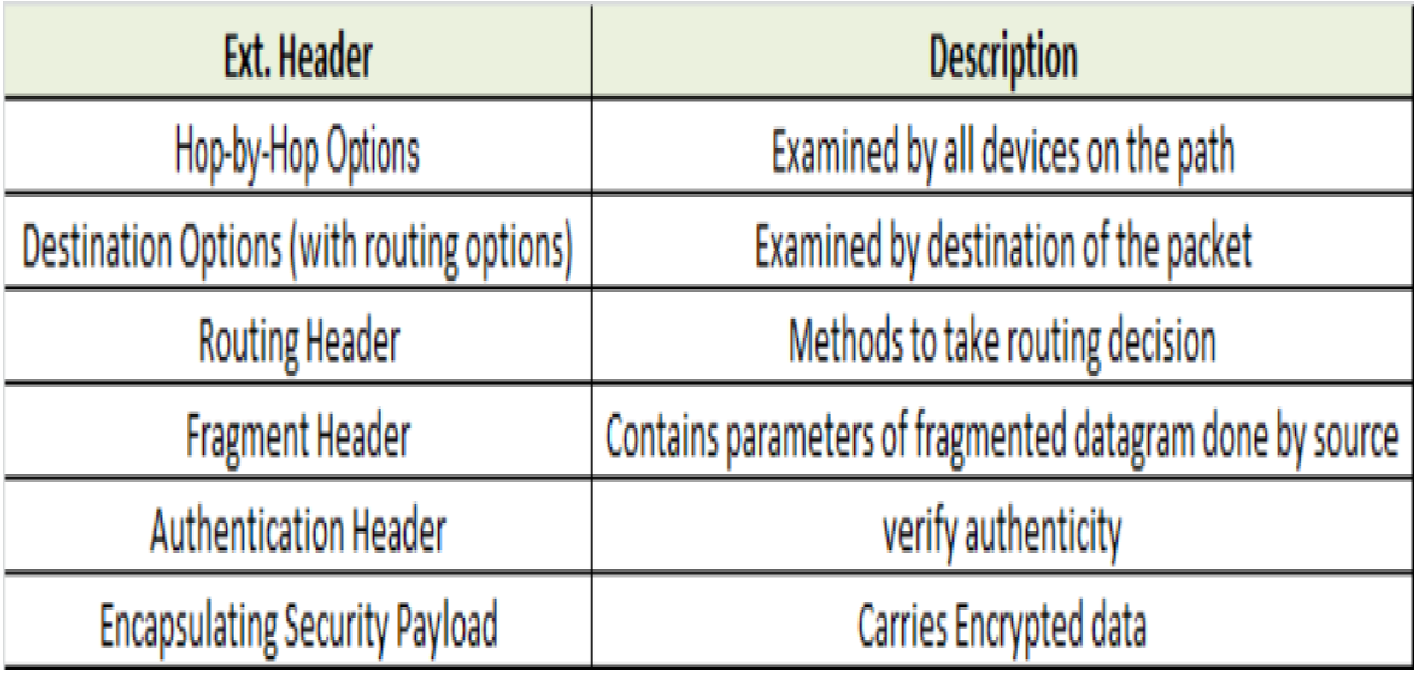
7. Source Address (128-bits): This field indicates the address of originator of the packet.

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



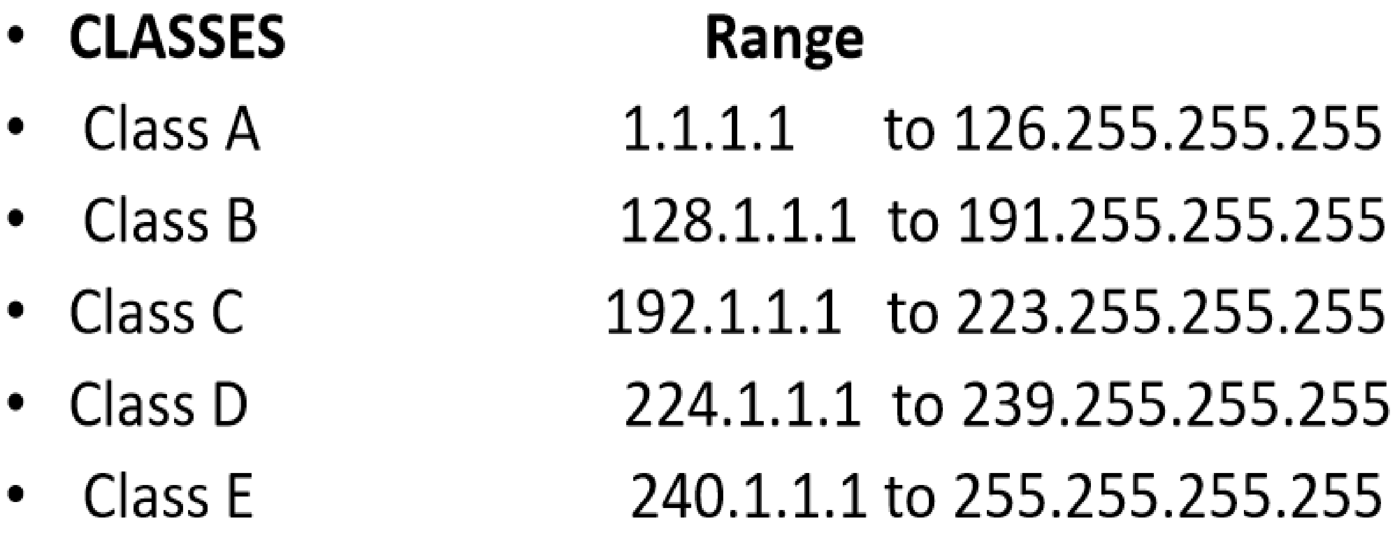
Header Extensions



Ext. Header	Description
Hop-by-Hop Options	Examined by all devices on the path
Destination Options (with routing options)	Examined by destination of the packet
Routing Header	Methods to take routing decision
Fragment Header	Contains parameters of fragmented datagram done by source
Authentication Header	verify authenticity
Encapsulating Security Payload	Carries Encrypted data

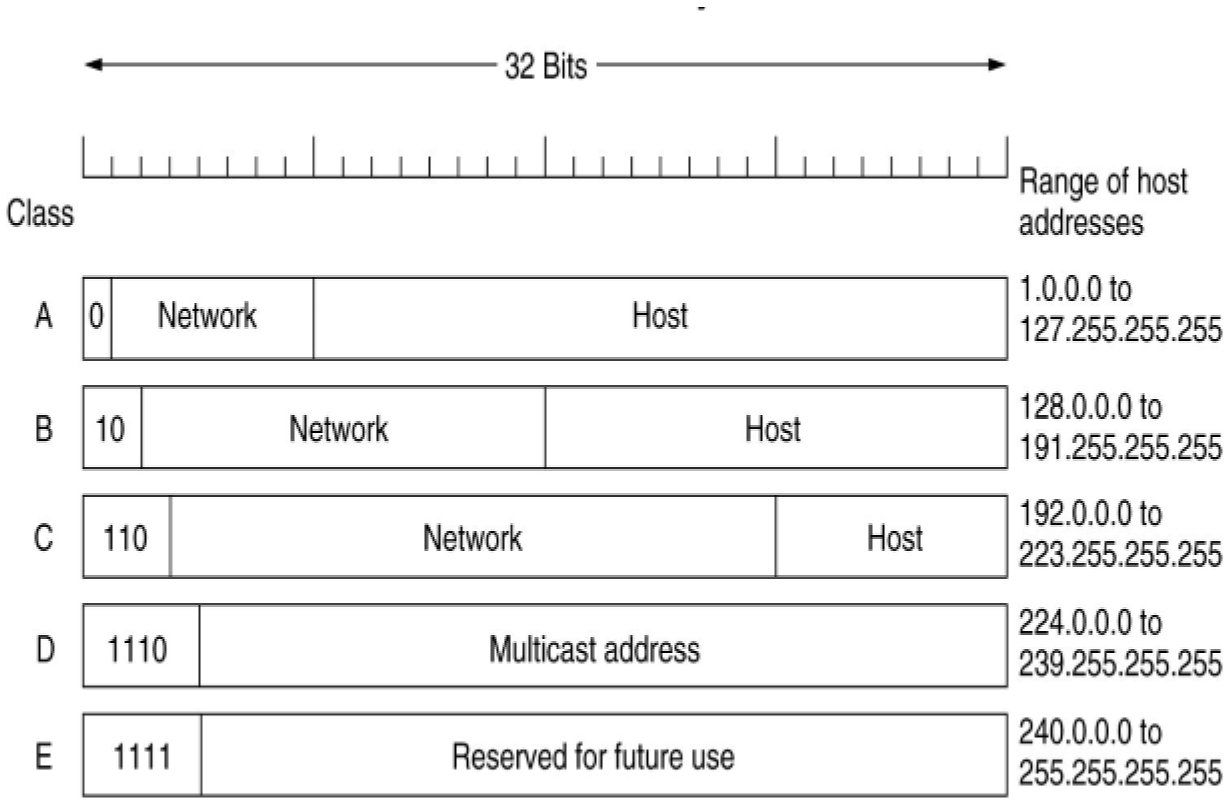
- IP Addresses
- In order to provide computer to computer communication via Internet, we need a global addressing scheme.
- Such an addressing is provided by Internet Protocol (IP) at the network layer.
- It is a 32-bit address This is called an IP address or logical address. Which is made up of the network ID, plus a unique host ID. This address is typically represented with the decimal value of each octet separated by a period (for example, 192.168.7.27). Every Host and router on the internet has an IP Address.

- Class of IP Address This IP address is unique and no two devices on the Internet can have the same address at the same time.



CLASSES	Range
Class A	1.1.1.1 to 126.255.255.255
Class B	128.1.1.1 to 191.255.255.255
Class C	192.1.1.1 to 223.255.255.255
Class D	224.1.1.1 to 239.255.255.255
Class E	240.1.1.1 to 255.255.255.255

These numbers are assigned by ISP (Internet Service Provider), and IP address can be used to identify the country or region from which a computer is connecting to the WEB. The IP address can either be Static or dynamic.



32 Bits

Class				Range of host addresses
A	0	Network	Host	1.0.0.0 to 127.255.255.255
B	10	Network	Host	128.0.0.0 to 191.255.255.255
C	110	Network	Host	192.0.0.0 to 223.255.255.255
D	1110	Multicast address		224.0.0.0 to 239.255.255.255
E	1111	Reserved for future use		240.0.0.0 to 255.255.255.255

- Classless Inter-Domain Routing (CIDR) is an IP address allocation method that improves data routing efficiency on the internet.
- Every machine, server, and end-user device that connects to the internet has a unique number, called an IP address, associated with it.
- Devices find and communicate with one another by using these IP addresses. Organizations use CIDR to allocate IP addresses flexibly and efficiently in their networks.
- An IP address has two parts:
- The *network address* is a series of numerical digits pointing to the network's unique identifier
- The *host address* is a series of numbers indicating the host or individual device identifier on the network

- Classful addresses
- An IPv4 address consists of 32 bits. Each string of numbers separated by the period consists of 8 bits, represented by 0 to 255 in numerical forms. Organizations could purchase three classes of IPv4 addresses.
- *Class A*
- A Class A IPv4 address has 8 network prefix bits. For example, consider 44.0.0.1, where 44 is the network address and 0.0.1 is the host address.
- *Class B*
- A Class B IPv4 address has 16 network prefix bits. For example, consider 128.16.0.2, where 128.16 is the network address and 0.2 is the host address.
- *Class C*
- A Class C IPv4 address has 24 network prefix bits. For instance, consider 192.168.1.100, where 192.168.1 is the network address and 100 is the host address.

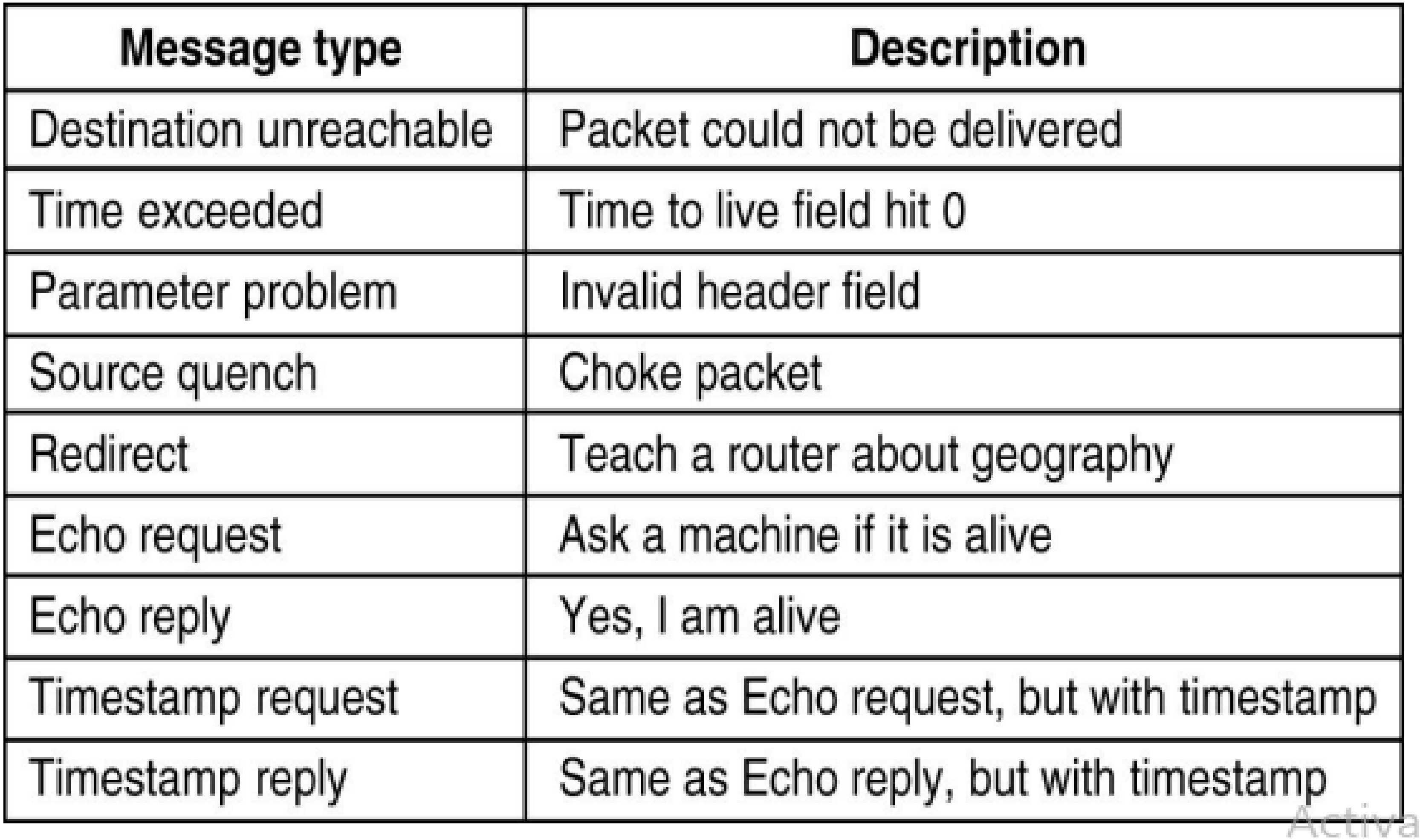
- Classless addresses
- Classless or Classless Inter-Domain Routing (CIDR) addresses use variable length subnet masking (VLSM) to alter the ratio between the network and host address bits in an IP address.
- A subnet mask is a set of identifiers that returns the network address’s value from the IP address by turning the host address into zeroes.
- For example, 192.0.2.0/24 is an IPv4 CIDR address where the first 24 bits, or 192.0.2, is the network address.

- Before Classless Inter-Domain Routing (CIDR), IP addresses were classful and created inefficiencies. We discuss some of these shortcomings next.
- Inflexible IP addressing
- In a classful addressing system, each class supported a fixed number of devices:
- Class A supported 16,777,214 hosts
- Class B supported 65,534 hosts
- Class C supported 254 hosts
- We will use here subnetting(Dividing the network).

- For example, an organization with 300 devices couldn’t have used a Class C IP address, which only permitted 254 devices.
- So, the organization would’ve been forced to apply for a Class B IP address, which provided 65,534 unique host addresses.
- However, only 300 devices would’ve been connected, which would’ve left 65,234 unused IP address spaces.

- Internet Control Message Protocol (ICMP)
- ICMP is network diagnostic and error reporting protocol. ICMP belongs to IP protocol suite and uses IP as carrier protocol.
- After constructing ICMP packet, it is encapsulated in IP packet. Because IP itself is a best-effort non-reliable protocol, so is ICMP.
- Any feedback about network is sent back to the originating host. If some error in the network occurs, it is reported by means of ICMP.
- ICMP contains dozens of diagnostic and error reporting messages

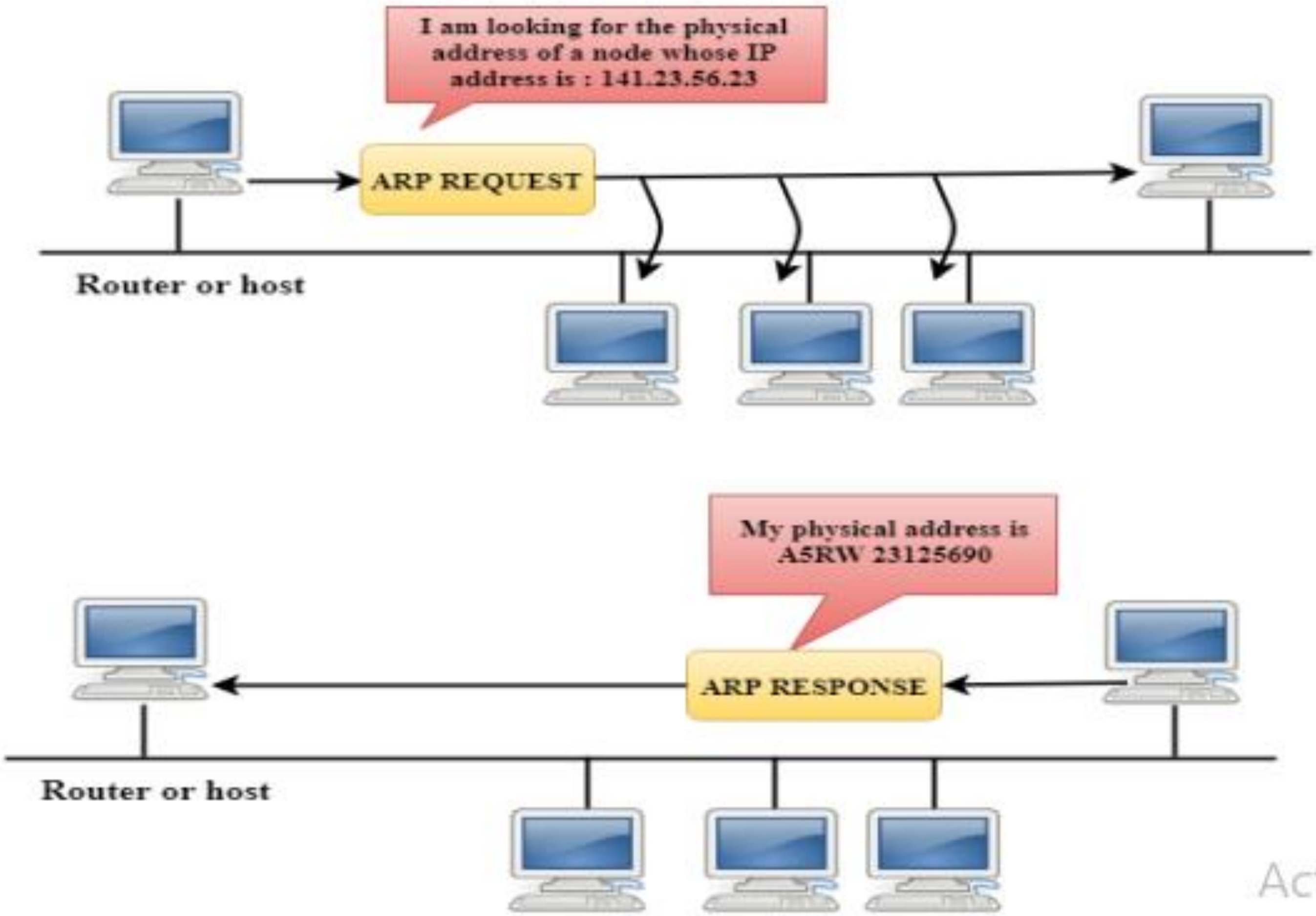
Internet Control Message Protocol parameters



Message type	Description
Destination unreachable	Packet could not be delivered
Time exceeded	Time to live field hit 0
Parameter problem	Invalid header field
Source quench	Choke packet
Redirect	Teach a router about geography
Echo request	Ask a machine if it is alive
Echo reply	Yes, I am alive
Timestamp request	Same as Echo request, but with timestamp
Timestamp reply	Same as Echo reply, but with timestamp

- Address Resolution Protocol (ARP) If a machine want to communicate to another machine in the same network, it requires its physical or MAC address. But ,since the application has given the destination's IP address it requires some mechanism to bind the IP address with its MAC address. This is done through Address Resolution protocol (ARP).

Address Resolution Protocol (ARP)

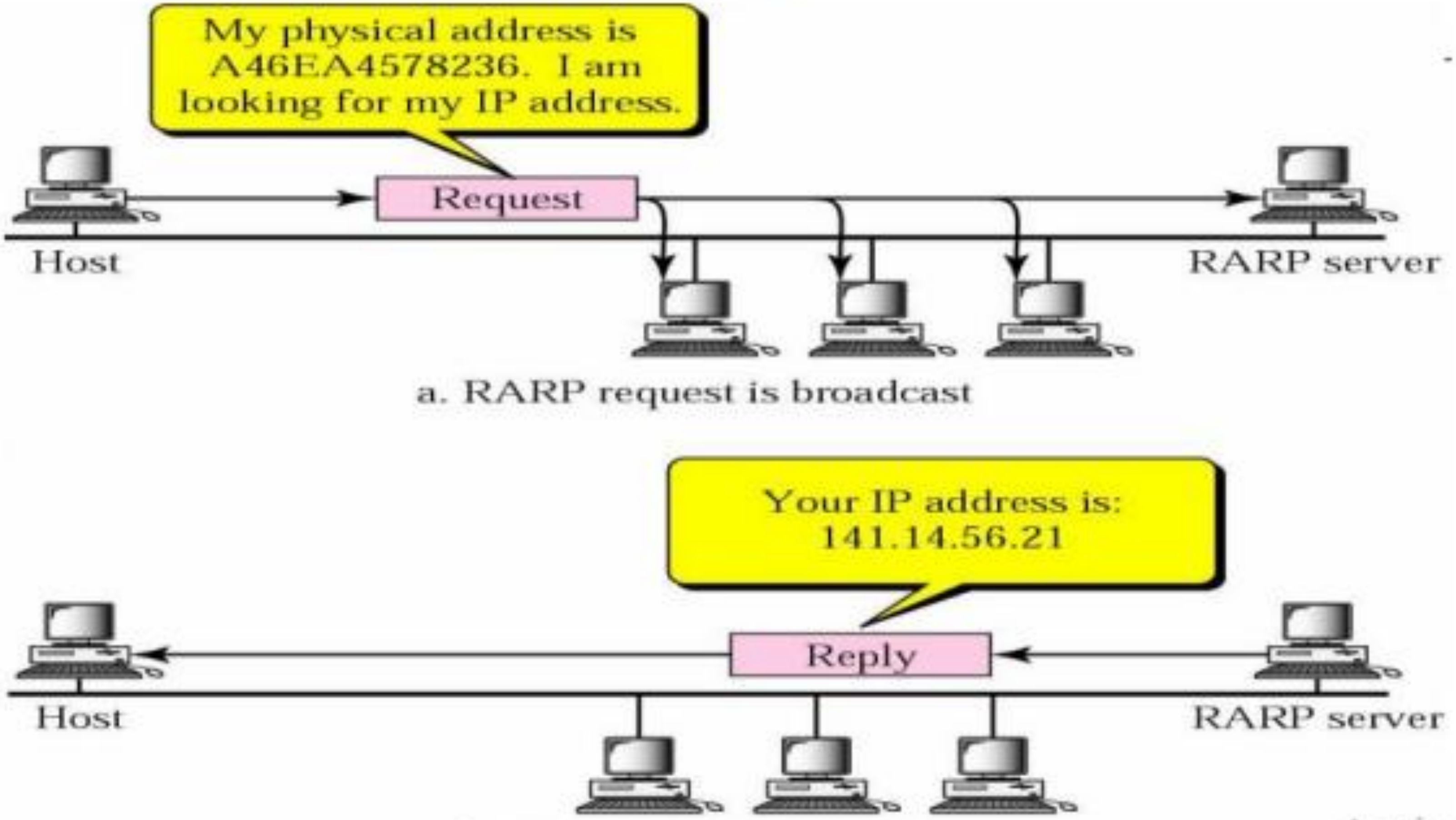


I am looking for the physical address of a node whose IP address is : 141.23.56.23

My physical address is A5RW 23125690

- Reverse Address Resolution Protocol
- RARP is a protocol by which a physical machine in a local area network can request to learn its IP address from a gateway server's Address Resolution Protocol table or cache. This is needed since the machine may not have permanently attached disk where it can store its IP address permanently.

RARP Operation

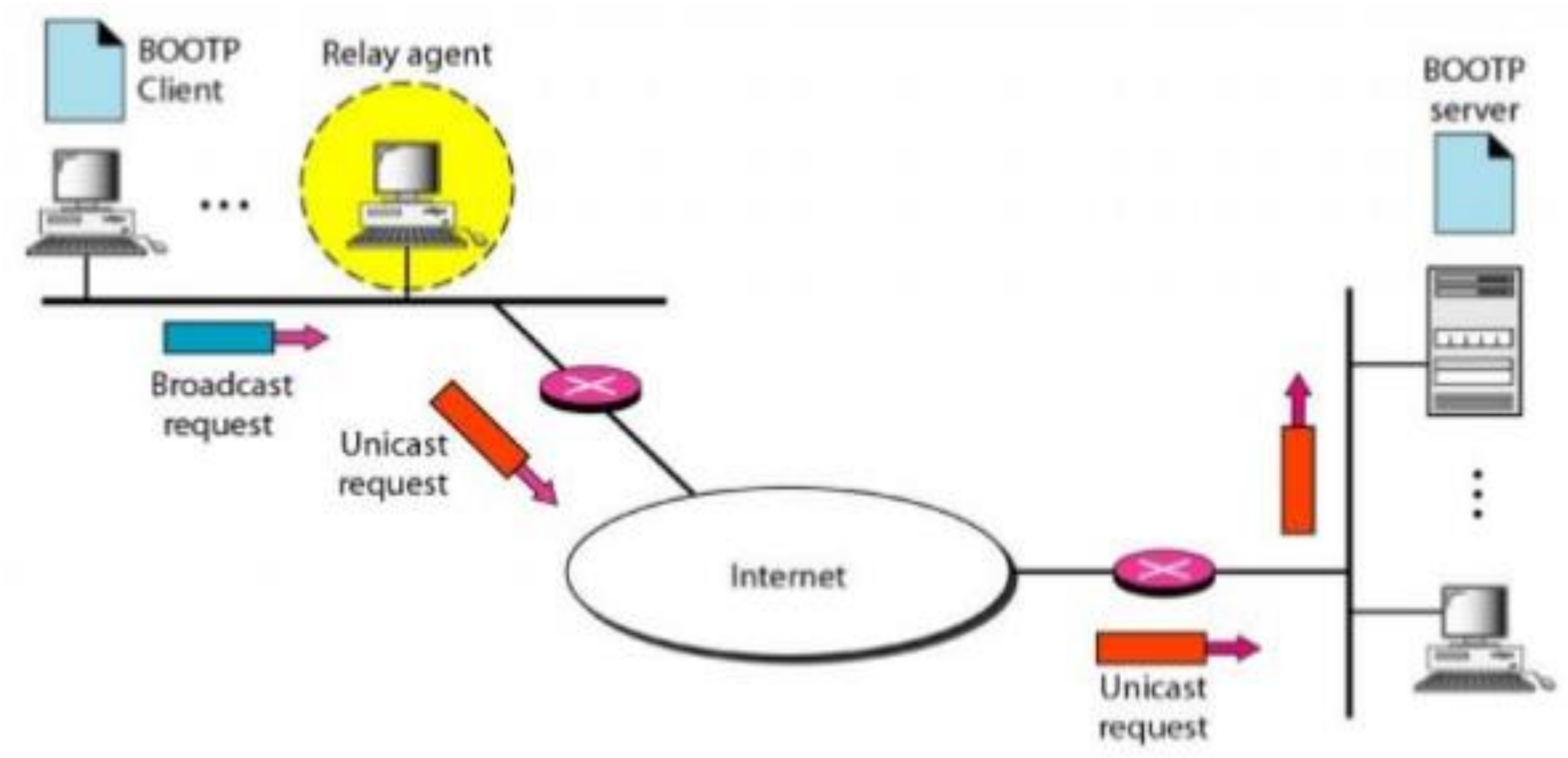

My physical address is A46EA4578236. I am looking for my IP address.
Request
Host
RARP server
Your IP address is: 141.14.56.21
Reply
Host
RARP server

a. RARP request is broadcast

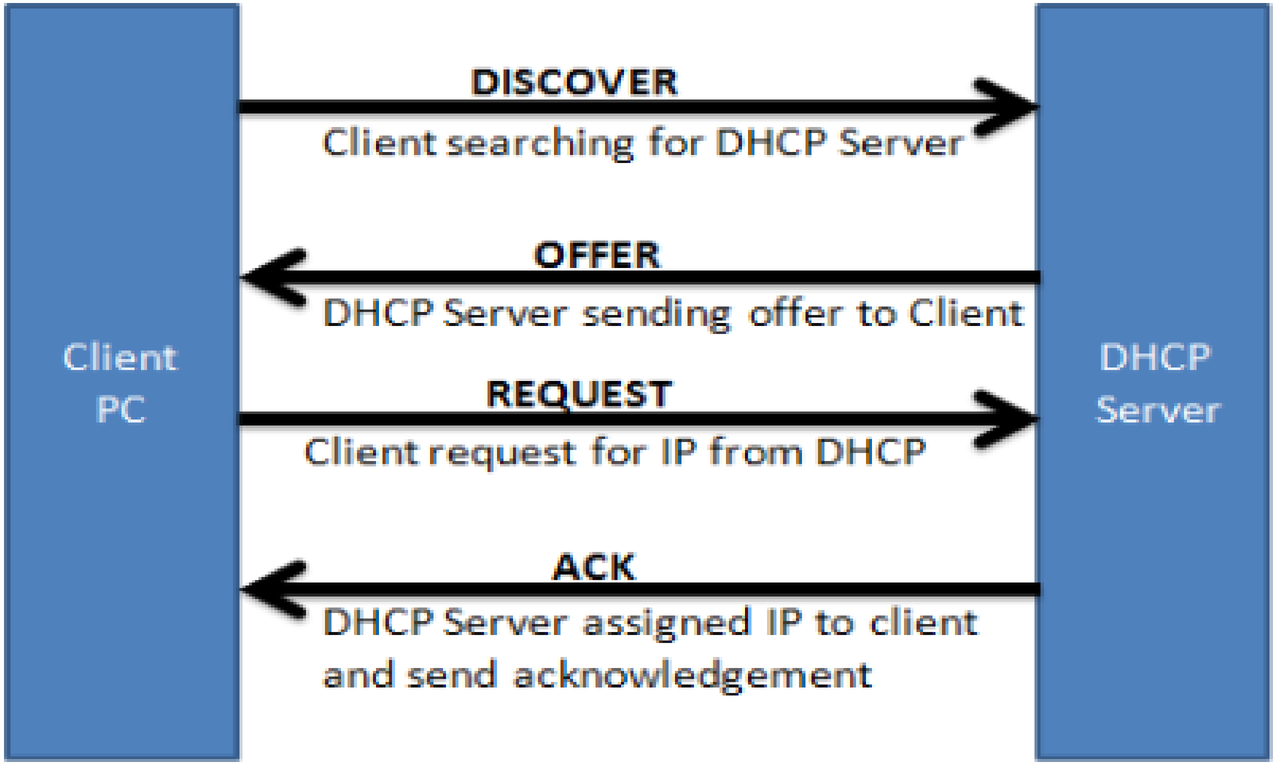
b. RARP reply is unicast

- Bootstrap Protocol (BOOTP)
- The Bootstrap Protocol is a networking protocol used to by a client for obtaining an IP address from a server. It was originally defined as specification RFC 951 and was designed to replace the Reverse Address Resolution Protocol (RARP), also known as RFC 903.
- Bootstrap protocol was intended to allow computers to find what they need to function properly after booting up.
- BOOTP uses a relay agent, which allows packet forwarding from the local network using standard IP routing, allowing one BOOTP server to serve hosts on multiple subnets

- The BOOTP request is broadcast because the client does not know the IP address of the server. An intermediate relay Agent is used in network which take request and encapsulate the message in unicast datagram and sends it to BOOTP server.

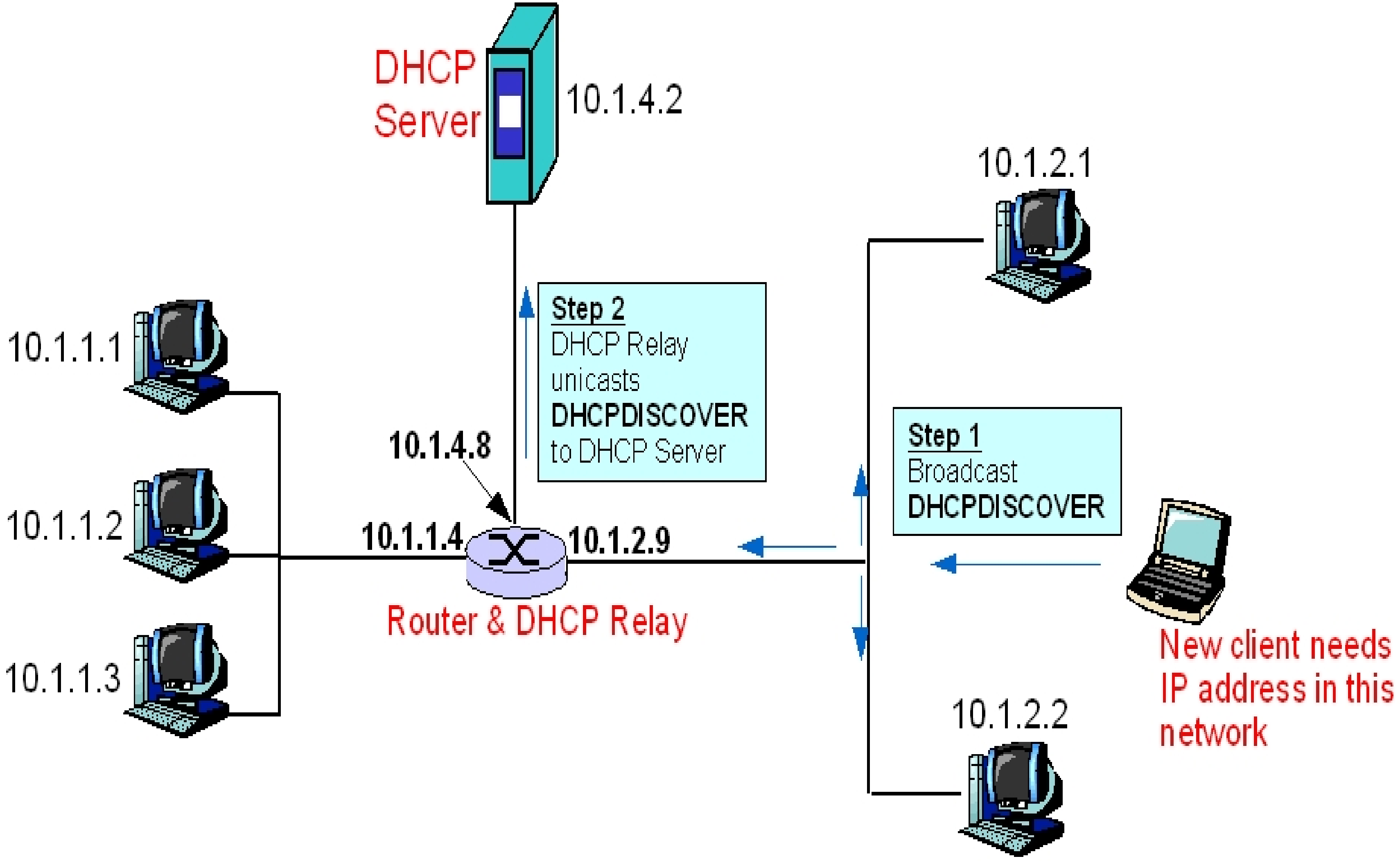


- DHCP (Dynamic Host Configuration Protocol) is a protocol used to provide quick, automatic, and central management • for the distribution of IP addresses within a network.


Client PC
DHCP Server
DISCOVER
Client searching for DHCP Server
OFFER
DHCP Server sending offer to Client
REQUEST
Client request for IP from DHCP
ACK
DHCP Server assigned IP to client and send acknowledgement

- How DHCP Works
- A DHCP server is used to issue unique IP addresses and automatically configure other network information.
- In most home and small businesses, the router acts as the DHCP server. In large networks, a single computer might act as the DHCP server.
- In short, the process goes like this: A device (the client) requests an IP address from a router (the host), after which the host assigns an available IP address to allow the client to communicate on the network. A bit more detail below..

- DHCP

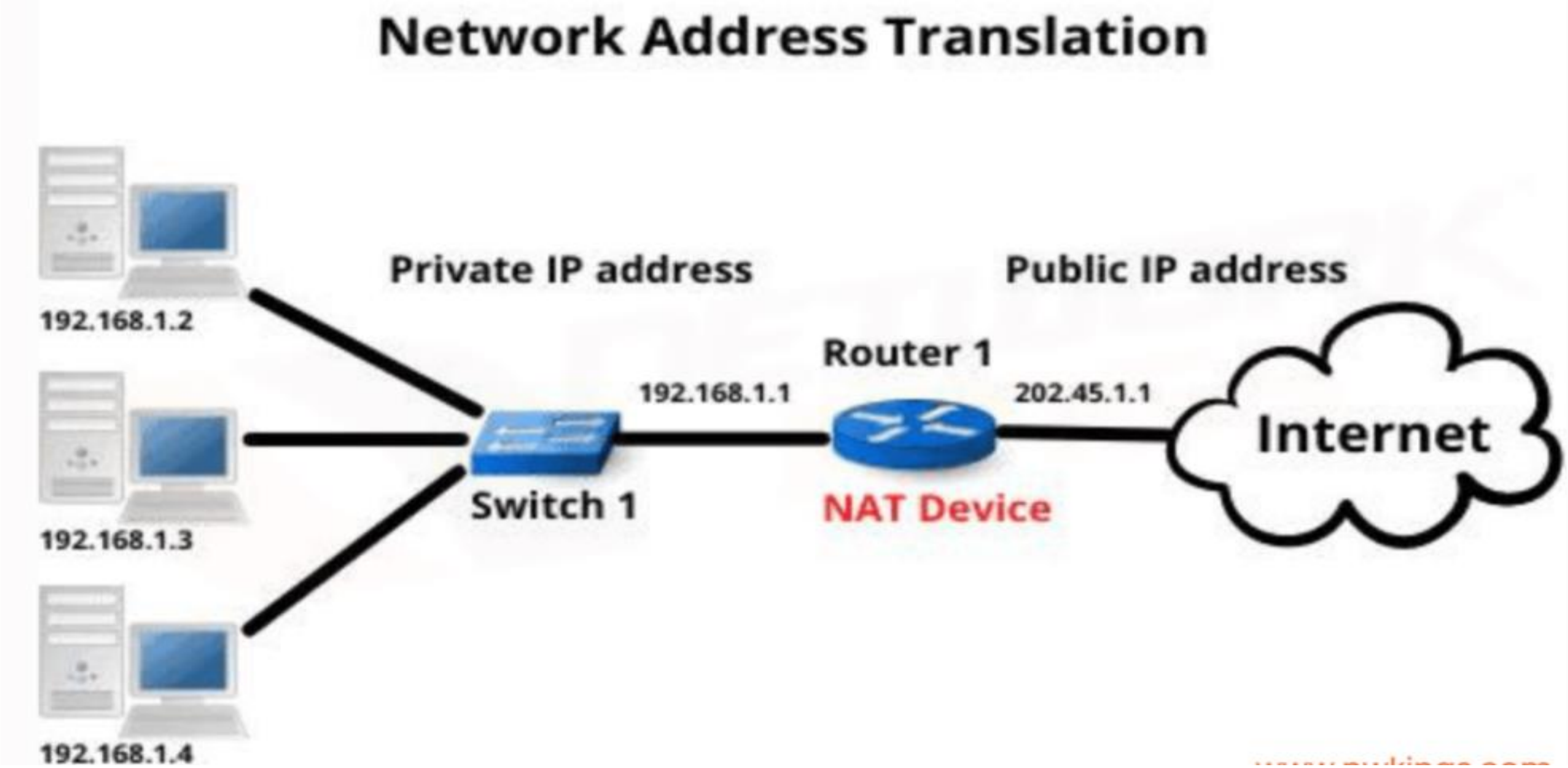


Step 2
DHCP Relay unicasts **DHCPDISCOVER** to DHCP Server

Step 1
Broadcast **DHCPDISCOVER**

- Network Address Translation
- NAT stands for network address translation. It's a way to map multiple private addresses inside a local network to a public IP address before transferring the information onto the internet. Organizations that want multiple devices to employ a single IP address use NAT, as do most home routers.
- **Network Address Translation (NAT) working –** Generally, the border router is configured for NAT i.e the router which has one interface in the local (inside) network and one interface in the global (outside) network.

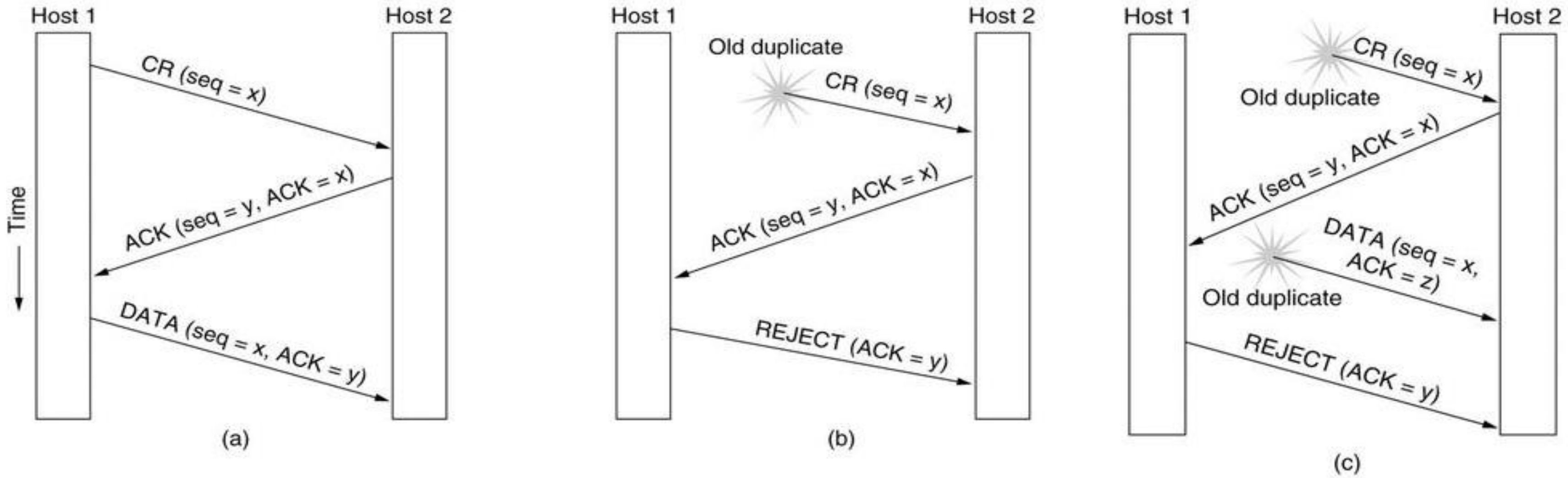
- When a packet traverse outside the local (inside) network, then NAT converts that local (private) IP address to a global (public) IP address. When a packet enters the local network, the global (public) IP address is converted to a local (private) IP address.



- Transport Layer
- The main role of the transport layer is to provide the communication services directly to the application processes running on different hosts.
- The transport layer provides a logical communication between application processes running on different hosts.
- Although the application processes on different hosts are not physically connected, application processes use the logical communication provided by the transport layer to send the messages to each other.
- The transport layer protocols are implemented in the end systems but not in the network routers.

- TCP Connection Establishment
- To make the transport services reliable, TCP hosts must establish a connection-oriented session with one another.
- Connection establishment is performed by using the three-way handshake mechanism. A three way handshake synchronizes both ends of a network by enabling both sides to agree upon original sequence numbers.
- This mechanism also provides that both sides are ready to transmit data and learn that the other side is available to communicate. This is essential so that packets are not shared or retransmitted during session establishment or after session termination.

- **TCP Connection establishment**



Three protocol scenarios for establishing a connection using a three-way handshake. CR denotes CONNECTION REQUEST.
(a) Normal operation,
(b) Old CONNECTION REQUEST appearing out of nowhere.
(c) Duplicate CONNECTION REQUEST and duplicate ACK.

- Connection Termination Protocol (Connection Release)
- While it creates three segments to establish a connection, it takes four segments to terminate a connection. During a TCP connection is fullduplex (that is, data flows in each direction independently of the other direction), each direction should be shut down alone.
- The termination procedure for each host is shown in the figure. The rule is that either end can share a FIN when it has finished sending data.

CONNECTION RELEASE:

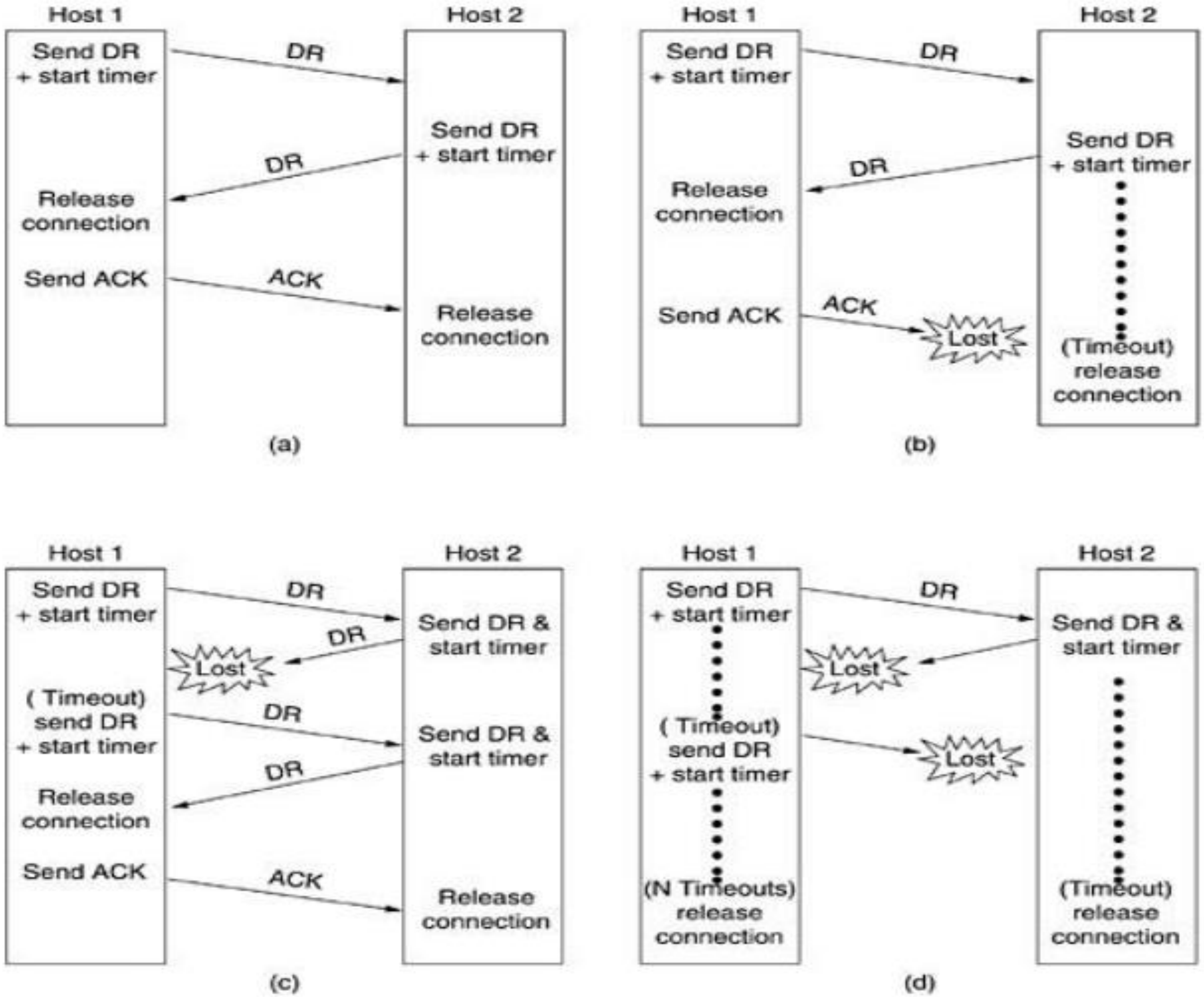


Fig-(a)	Fig-(b)	Fig-(c)	Fig-(d)
One of the user sends a DISCONNECTION REQUEST TPDU in order to initiate connection release. When it arrives, the recipient sends back a DR-TPDU, too, and starts a timer. When this DR arrives, the original sender sends back an ACK-TPDU and releases the connection. Finally, when the ACK-TPDU arrives, the receiver also releases the connection.	Initial process is done in the same way as in fig-(a). If the final ACK-TPDU is lost, the situation is saved by the timer. When the timer is expired, the connection is released.	If the second DR is lost, the user initiating the disconnection will not receive the expected response, and will timeout and starts all over again.	Same as in fig-(c) except that all repeated attempts to retransmit the DR is assumed to be failed due to lost TPDUs. After 'N' entries, the sender just gives up and releases the connection.

- Crash Recovery
- *Crash recovery* is the process by which the database is moved back to a consistent and usable state. This is done by rolling back incomplete transactions and completing committed transactions that were still in memory when the crash occurred When a database is in a consistent and usable state, it has attained what is known as a *point of consistency*.
- Network and Transport layers automatically handle network and router crashes. Issue here is how the transport layer recovers from host (end system) crashes. Want clients continue to be able to work if the server quickly reboots.