UNIT III - NETWORK LAYER

Switching: Packet Switching - Internet protocol - IPV4 – IP Addressing – Subnetting - IPV6, ARP, RARP, ICMP, DHCP

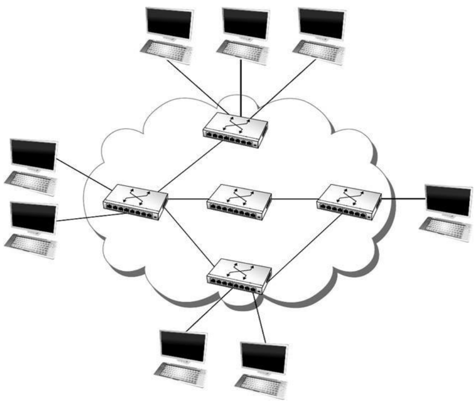
- The network layer works for the transmission of data from one host to the other located in different networks.
- It provides end to end communication by forwarding packets from source to destination.
- It also takes care of packet routing i.e., selection of the shortest path to transmit the packet, from the number of routes available.
- The sender & receiver’s IP addresses are placed in the header by the network layer.

NETWORK LAYER SERVICES:

- Packeting
- Routing and forwarding
- Addressing
- Error control
- Flow control
- Congestion control
- Quality of service

SWITCHING

- The technique of transferring the information from one computer network to another network is known as **switching**.
- Switching in a computer network is achieved by using switches.
- A switch is a small hardware device which is used to join multiple computers together with one local area network (LAN).
- Switches are devices capable of creating temporary connections between two or more devices linked to the switch.
- Switches are used to forward the packets based on MAC addresses.
- A Switch is used to transfer the data only to the device that has been addressed. It verifies the destination address to route the packet appropriately.
- It is operated in full duplex mode.
- It does not broadcast the message as it works with limited bandwidth.



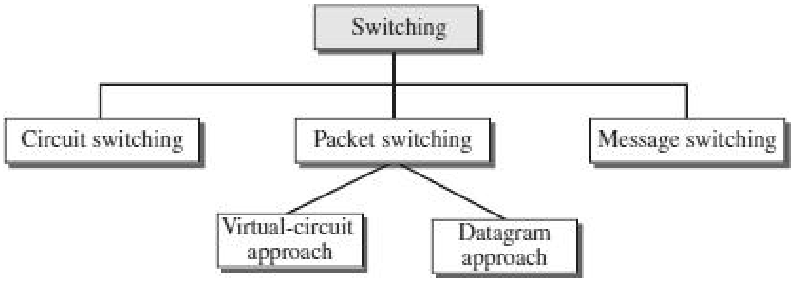
Advantages of Switching:

- Switch increases the bandwidth of the network.
- It reduces the workload on individual PCs as it sends the information to only that device which has been addressed.
- It increases the overall performance of the network by reducing the traffic on the network.
- There will be less frame collision as switch creates the collision domain for each connection.

Disadvantages of Switching:

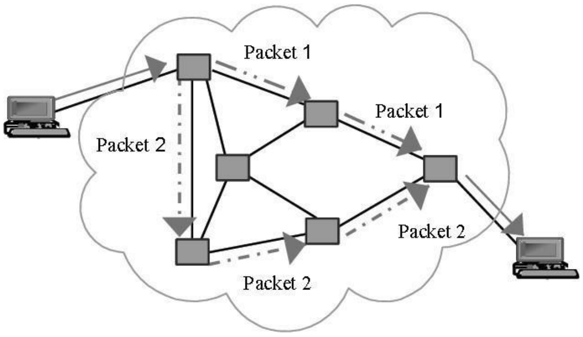
- A Switch is more expensive than network bridges.
- A Switch cannot determine the network connectivity issues easily.
- Proper designing and configuration of the switch are required to handle multicast packets.

Types of Switching Techniques



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.



***Advantages of Packet Switching*:**

- **Cost-effective**
- **Reliable**
- **Efficient**

APPROACHES OF PACKET SWITCHING

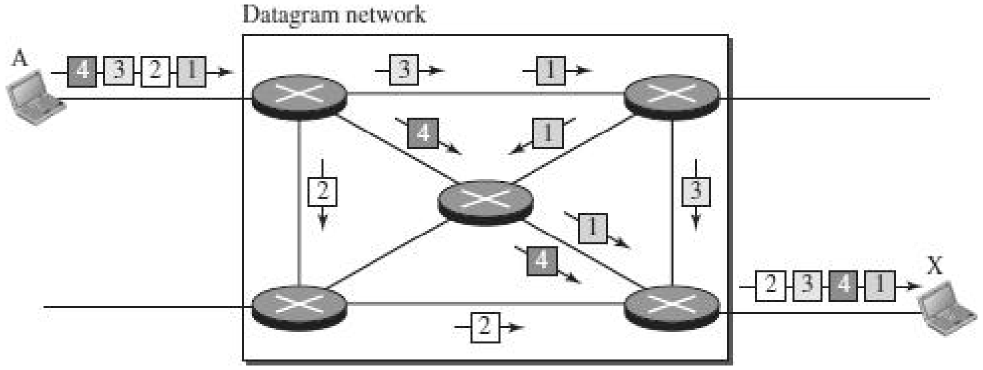
There are two approaches to Packet Switching:

- Datagram Packet switching (Connectionless service)
- Virtual Circuit Switching (Connection oriented service)

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.

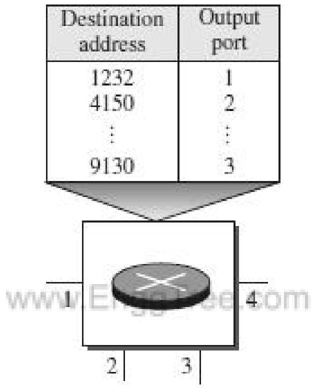
- In Datagram Packet Switching technique, the path is not fixed.
- Intermediate nodes take the routing decisions to forward the packets.
- Datagram Packet Switching is also known as connectionless switching.
- There are no setup or teardown phases.
- Each packet is treated the same by a switch regardless of its source or destination.



In this example, all four packets (or datagrams) belong to the same message, but may travel different paths to reach their destination.

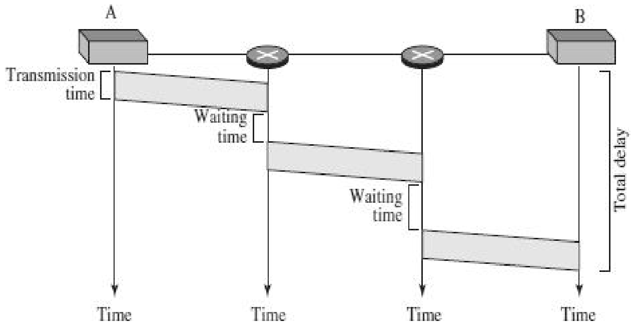
Routing Table

In this type of network, each switch (or packet switch) has a routing table which is based on the destination address. The routing tables are dynamic and are updated periodically. The destination addresses and the corresponding forwarding output ports are recorded in the tables.



Destination address	Output port
1232	1
4150	2
⋮	⋮
9130	3

Delay in a datagram network



- The packet travels through two switches.
- There are three transmission times (3*T*), three propagation delays (slopes 3t of the lines), and two waiting times (*w*1 + *w*2).
- We ignore the processing time in each switch.

Total delay = $3T + 3t + w1 + w2$

<u>Virtual Circuit Switching</u>

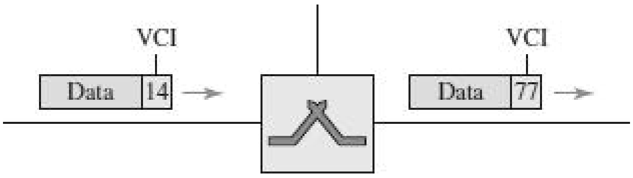
- Virtual Circuit Switching is also known as connection-oriented switching.
- In the case of Virtual circuit switching, a virtual connection is established before

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.

Virtual Circuit Identifier (VCI)

A virtual circuit identifier (VCI) that uniquely identifies the connection at this switch. A VCI, unlike a global address, is a small number that has only switch scope; it is used by a frame between two switches. When a frame arrives at a switch, it has a VCI; when it leaves, it has a different VCI.



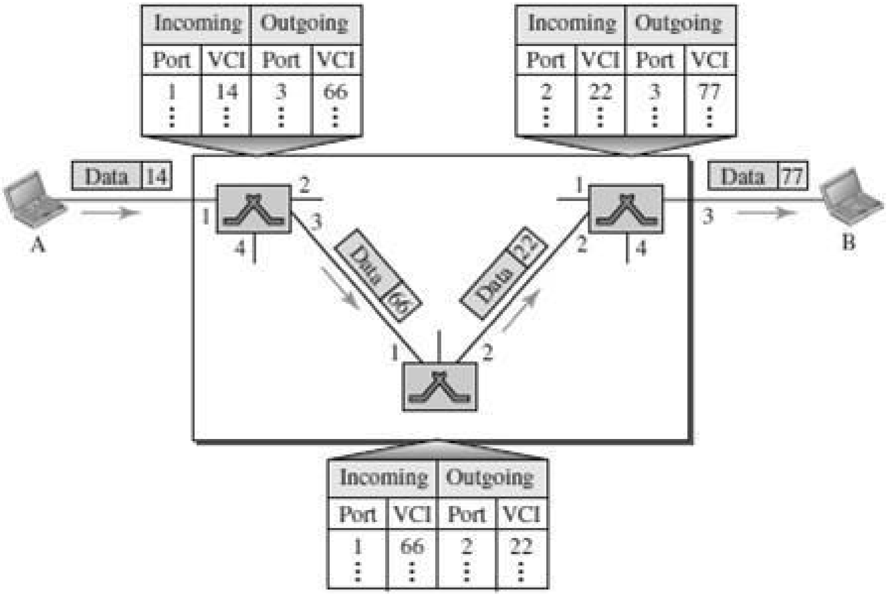
Virtual Circuit Table

Every Virtual Circuit (VC) maintains a table called Virtual Circuit table. One entry in the VC table on a single switch contains the following:

- An incoming interface on which packets for this VC arrive at the switch
- An outgoing interface in which packets for this VC leave the switch
- An outgoing VCI that will be used for outgoing packets

Example:

Source A sends a frame to Source B through Switch 1, Switch 2 and Switch 3.



Incoming		Outgoing	
Port	VCI	Port	VCI
1	14	3	66
⋮	⋮	⋮	⋮

Incoming		Outgoing	
Port	VCI	Port	VCI
2	22	3	77
⋮	⋮	⋮	⋮

Incoming		Outgoing	
Port	VCI	Port	VCI
1	66	2	22
⋮	⋮	⋮	⋮

IPV4 ADDRESSES

- 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.
- IPv4 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

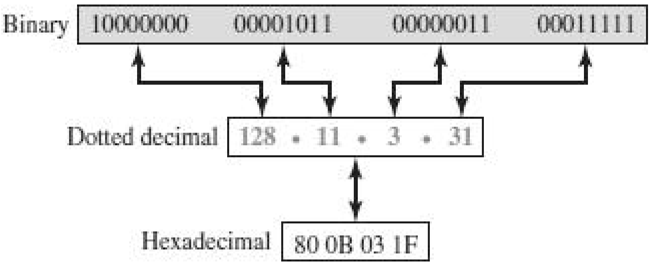
- IPv4 defines addresses has an address space.
- An address space is the total number of addresses used by the protocol.
- If a protocol uses *b* bits to define an address, the address space is 2^b because each bit can have two different values (0 or 1).
- IPv4 uses 32-bit addresses, which means that the address space is 2^{32} 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).



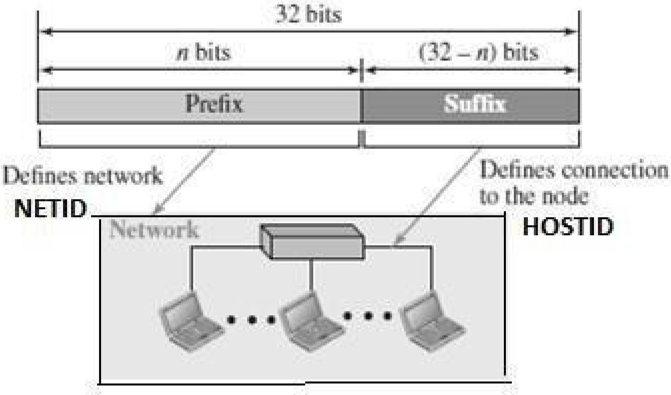
In *binary notation,* an IPv4 address is displayed as 32 bits. To make the address more readable, one or more spaces are usually inserted between bytes (8 bits).

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.



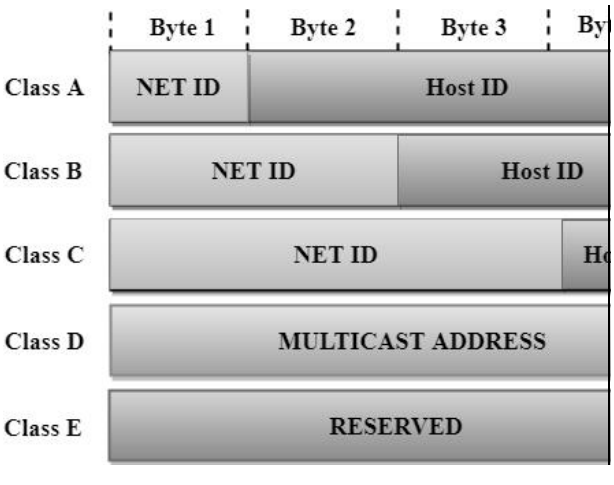
- A prefix can be fixed length or variable length.
- The network identifier in the IPv4 was first designed as a fixed-length prefix.
- This scheme is referred to as classful addressing.
- The new scheme, which is referred to as classless addressing, uses a variable- length network prefix.

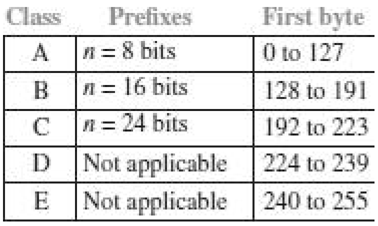
CATEGORIES OF IPV4 ADDRESSING

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

CLASSFUL ADDRESSING

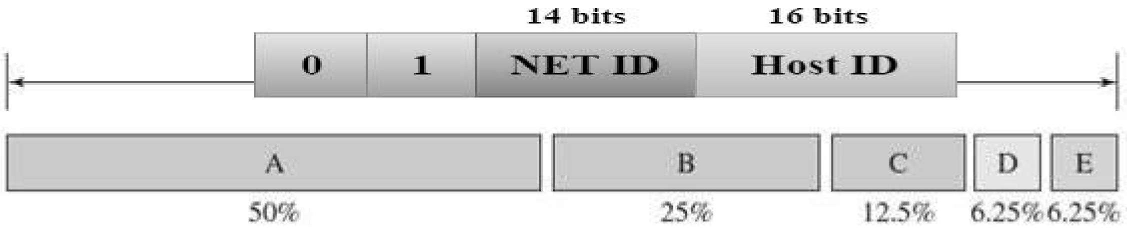
- An IPv4 address is 32-bit long (4 bytes).
- An IPv4 address is divided into sub-classes:

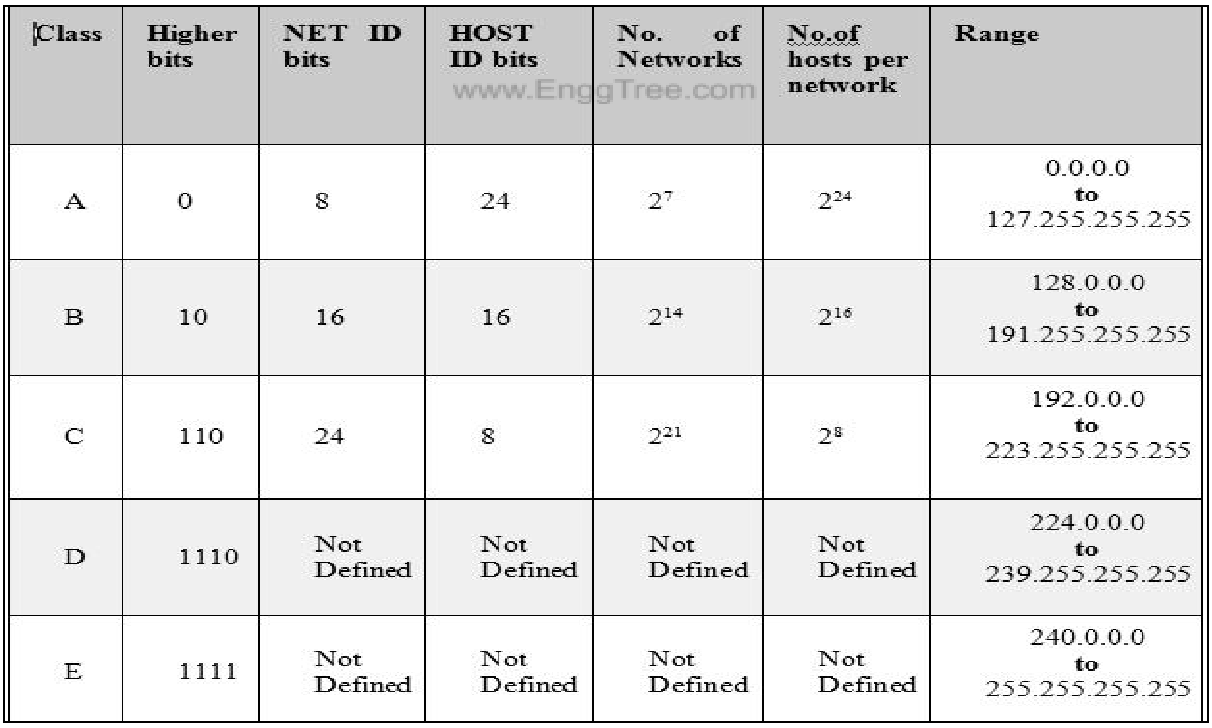




Class	Prefixes	First byte
A	n = 8 bits	0 to 127
B	n = 16 bits	128 to 191
C	n = 24 bits	192 to 223
D	Not applicable	224 to 239
E	Not applicable	240 to 255

Classful Network Architecture

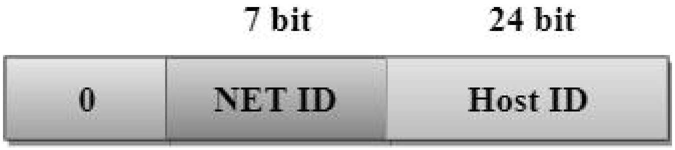




Class	Higher bits	NET ID bits	HOST ID bits	No. of Networks	No.of hosts per network	Range
A	0	8	24	2^7	2^{24}	0.0.0.0 to 127.255.255.255
B	10	16	16	2^{14}	2^{16}	128.0.0.0 to 191.255.255.255
C	110	24	8	2^{21}	2^8	192.0.0.0 to 223.255.255.255
D	1110	Not Defined	Not Defined	Not Defined	Not Defined	224.0.0.0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

Class A

- In Class A, an IP address is assigned to those networks that contain a large number of hosts.
  - The network ID is 8 bits long.
  - The host ID is 24 bits long.
- In Class A, the first bit in higher order bits of the first octet is always set to 0 and the remaining 7 bits determine the network ID.
  - The 24 bits determine the host ID in any network.
  - The total number of networks in Class A = 2^7 = 128 network address
  - The total number of hosts in Class A = 2^{24} - 2 = 16,777,214 host address

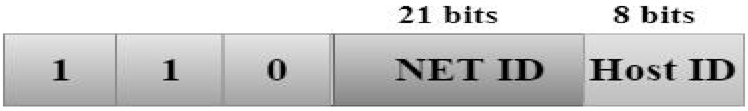


Class B

- In Class B, an IP address is assigned to those networks that range from small- sized to large-sized networks.
  - The Network ID is 16 bits long.
  - The Host ID is 16 bits long.
- In Class B, the higher order bits of the first octet is always set to 01, and the remaining14 bits determine the network ID.
  - The other 16 bits determine the Host ID.
  - The total number of networks in Class B = 2^{14} = 16384 network address
  - The total number of hosts in Class B = 2^{16} - 2 = 65534 host address

Class C

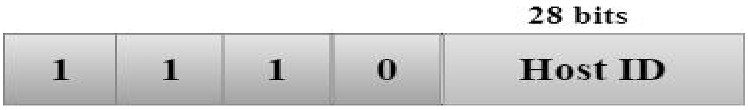
- In Class C, an IP address is assigned to only small-sized networks.



- The Network ID is 24 bits long.
- The host ID is 8 bits long.
- In Class C, the higher order bits of the first octet is always set to 110, and the remaining 21 bits determine the network ID.
- The 8 bits of the host ID determine the host in a network.
- The total number of networks = 2^{21} = 2097152 network address
- The total number of hosts = 2^{8} - 2 = 254 host address

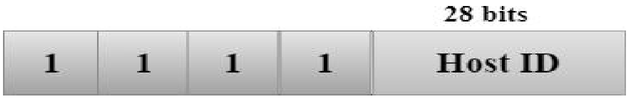
Class D

- In Class D, an IP address is reserved for multicast addresses.
- It does not possess subnetting.The higher order bits of the first octet are always set to 1110, and the remaining bits determines the host ID in any network.



Class E

- In Class E, an IP address is used for the future use or for the research and development purposes.
- It does not possess any subnetting.
- The higher order bits of the first octet are always set to 1111, and the remaining bits determines the host ID in any network.



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.

Subnetting and Supernetting

- To alleviate address depletion, two strategies were proposed and implemented:

(i) Subnetting and (ii) Supernetting.

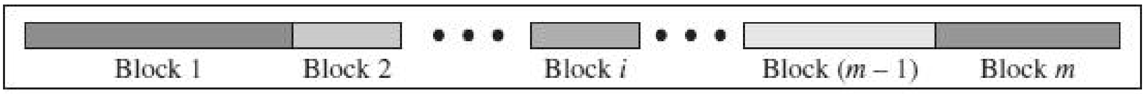
Subnetting

- 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 $n_{sub} = 10$.
- 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 $2^{0}, 2^{1}, 2^{2}, \ldots, 2^{32}$ addresses.
- The number of addresses in a block needs to be a power of 2. An organization can be granted one block of addresses.

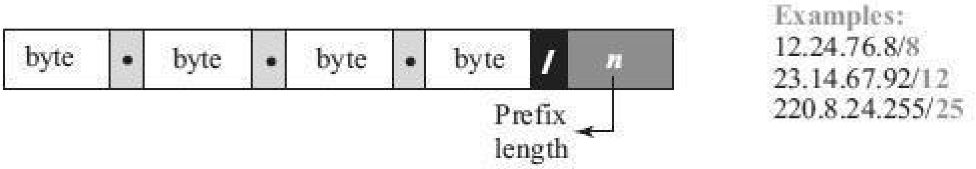


Address space

- The prefix length in classless addressing is variable.
- We can have a prefix length that ranges from 0 to 32.
- The size of the network is inversely proportional to the length of the prefix.
- A small prefix means a larger network; a large prefix means a smaller network.
- The idea of classless addressing can be easily applied to classful addressing.
- An address in class A can be thought of as a classless address in which the prefix length is 8.
- An address in class B can be thought of as a classless address in which the prefix is 16, and so on. In other words, classful addressing is a special case of classless addressing.

Notation used in Classless Addressing

- The notation used in classless addressing is informally referred to as *slash notation* and formally as ***classless interdomain routing*** or ***CIDR.***



- 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.

This-host Address

✓ The only address in the block **0.0.0.0**/**32** is called the *this-host* address.

✓ It is used whenever a host needs to send an IP datagram but it does not know its own address to use as the source address.

Limited-broadcast Address

✓ The only address in the block **255.255.255.255**/**32** is called the *limited- broadcast* address.

✓ It is used whenever a router or a host needs to send a datagram to all devices in a network.

✓ The routers in the network, however, block the packet having this address as the destination; the packet cannot travel outside the network.

Loopback Address

✓ The block **127.0.0.0/8** is called the *loopback* address.

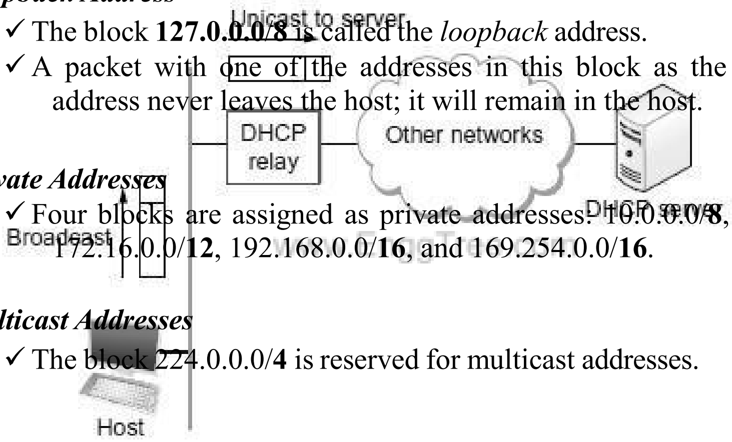
✓ A packet with one of the addresses in this block as the destination address never leaves the host; it will remain in the host.

Private Addresses

✓ Four blocks are assigned as private addresses: 10.0.0.0/**8**, 172.16.0.0/**12**, 192.168.0.0/**16**, and 169.254.0.0/**16**.

Multicast Addresses

✓ The block 224.0.0.0/**4** is reserved for multicast addresses.



DHCP – DYNAMIC HOST CONFIGURATION PROTOCOL

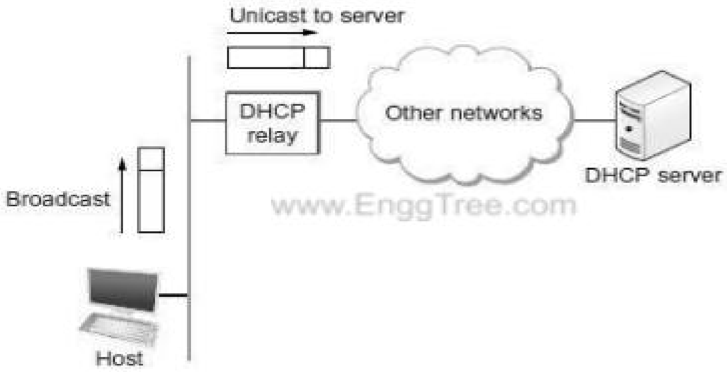
- ➢ The dynamic host configuration protocol is used to simplify the installation and maintenance of networked computers.
- ➢ DHCP is derived from an earlier protocol called BOOTP.
- ➢ Ethernet addresses are configured into network by manufacturer and they are unique.
- ➢ IP addresses must be unique on a given internetwork but also must reflect the structure of the internetwork
- ➢ Most host Operating Systems provide a way to manually configure the IP information for the host

➢ **Drawbacks of manual configuration:**

1. A lot of work to configure all the hosts in a large network
2. Configuration process is error-prune.

➢ It is necessary to ensure that every host gets the correct network number and that no two hosts receive the same IP address.

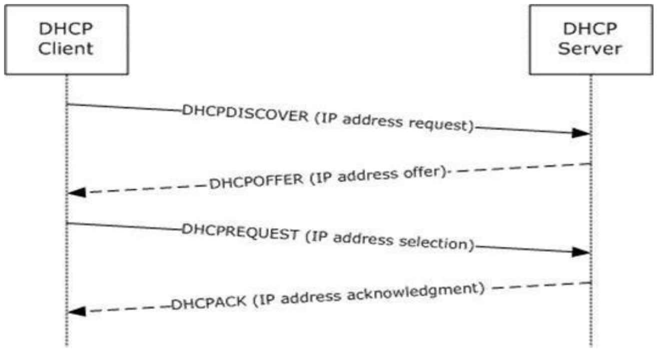
- For these reasons, automated configuration methods are required.
- The primary method uses a protocol known as the *Dynamic Host Configuration Protocol* (DHCP).
- The main goal of DHCP is to minimize the amount of manual configuration required for a host.
- If a new computer is connected to a network, DHCP can provide it with all the necessary information for full system integration into the network.
- DHCP is based on a client/server model.
- DHCP clients send a request to a DHCP server to which the server responds with an IP address
- DHCP server is responsible for providing configuration information to hosts.
- There is at least one DHCP server for an administrative domain.
- The DHCP server can function just as a centralized repository for host configuration information.
- The DHCP server maintains a pool of available addresses that it hands out to hosts on demand.

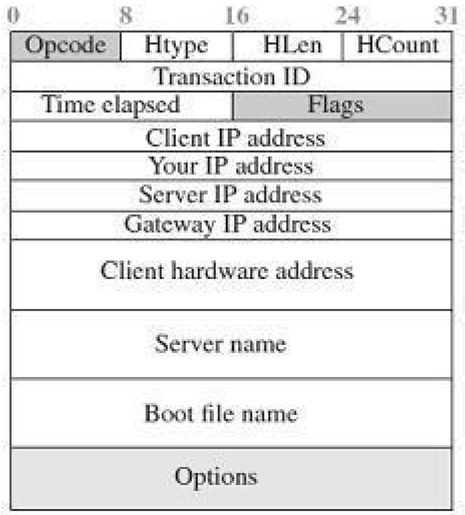


- A newly booted or attached host sends a DHCPDISCOVER message to a special IP address (255.255.255.255., which is an IP broadcast address.
- This means it will be received by all hosts and routers on that network.
- DHCP uses the concept of a *relay agent.* There is at least one relay agent on each network.
- DHCP relay agent is configured with the IP address of the DHCP server.
- When a relay agent receives a DHCPDISCOVER message, it unicasts it to the DHCP server and awaits the response, which it will then send back to the requesting client.

DHCP Message Format

- A DHCP packet is actually sent using a protocol called the *User Datagram Protocol* (UDP).


DHCP Client
DHCP Server
DHCPDISCOVER (IP address request)
DHCPOFFER (IP address offer)
DHCPREQUEST (IP address selection)
DHCPACK (IP address acknowledgment)



Opcode: Operation code, request (1) or reply (2)
Htype: Hardware type (Ethernet, ...)
HLen: Length of hardware address
HCount: Maximum number of hops the packet can travel
Transaction ID: An integer set by the client and repeated by the server
Time elapsed: The number of seconds since the client started to boot
Flags: First bit defines unicast (0) or multicast (1); other 15 bits not used
Client IP address: Set to 0 if the client does not know it
Your IP address: The client IP address sent by the server
Server IP address: A broadcast IP address if client does not know it
Gateway IP address: The address of default router
Server name: A 64-byte domain name of the server
Boot file name: A 128-byte file name holding extra information
Options: A 64-byte field with dual purpose described in text

INTERNET PROTOCOL

- The Internet Protocol is the key tool used today to build scalable, heterogeneou
  - IP runs on all the nodes (both hosts and routers) in a collection of networks
  - IP defines the infrastructure that allows these nodes and networks to function as a single logical internetwork.

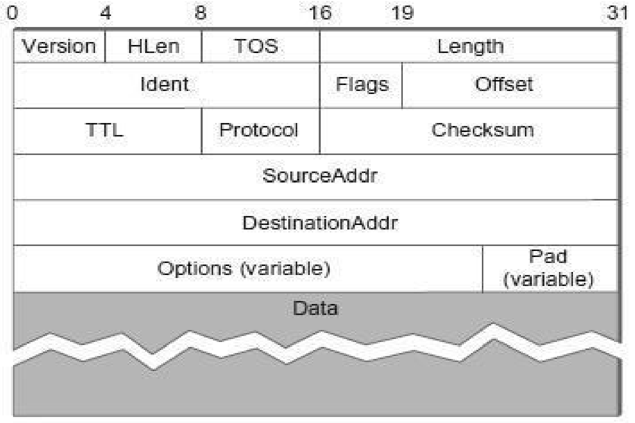
IP SERVICE MODEL

- Service Model defines the host-to-host services that we want to provide
- The main concern in defining a service model for an internetwork is that we can provide a host-to-host service only if this service can somehow be provided over each of the underlying physical networks.
- The Internet Protocol is the key tool used today to build scalable, heterogeneous internetworks.

- The **IP service model** can be thought of as having **two parts**:
  - A ***GLOBAL ADDRESSING SCHEME*** - which provides a way to identify all hosts in the internetwork
  - A ***DATAGRAM DELIVERY MODEL*** – A connectionless model of data delivery.

IP PACKET FORMAT / IP DATAGRAM FORMAT

- A key part of the IP service model is the type of packets that can be carried.
- The IP datagram consists of a header followed by a number of bytes of data.



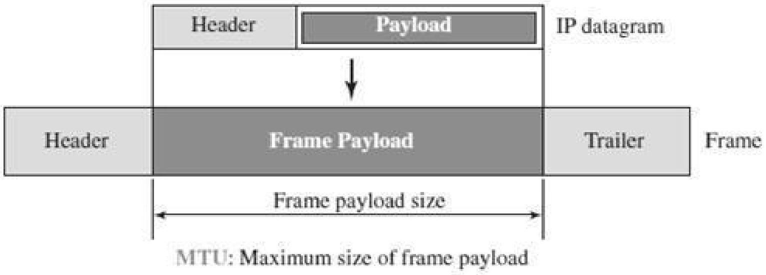
FIELD	DESCRIPTION
Version	Specifies the version of IP. Two versions exist – IPv4 and IPv6.
HLen	Specifies the length of the header
TOS *(*Type of Service)	An indication of the parameters of the quality of service desired such as Precedence, Delay, Throughput and Reliability.
Length	Length of the entire datagram, including the header. The maximum size of an IP datagram is 65,535(2^{10}) bytes
Ident (Identification)	Uniquely identifies the packet sequence number. Used for fragmentation and re-assembly.
Flags	Used to control whether routers are allowed to fragment a packet. If a packet is fragmented, this flag value is 1. If not, flag value is 0.
Offset (Fragmentation offset)	Indicates where in the datagram, this fragment belongs. The fragment offset is measured in units of 8 octets (64 bits). The first fragment has offset zero.
TTL **(Time to Live)**	Indicates the maximum time the datagram is allowed to remain in the network. If this field contains the value zero, then the datagram must be destroyed.
Protocol	Indicates the next level protocol used in the data portion of the datagram
Checksum	Used to detect the processing errors introduced into the packet

Source Address	The IP address of the original sender of the packet.
Destination Address	The IP address of the final destination of the packet.
Options	This is optional field. These options may contain values for options such as Security, Record Route, Time Stamp, etc
Pad	Used to ensure that the internet header ends on a 32-bit boundary.The padding is zero.

IP DATAGRAM - FRAGMENTATION AND REASSEMBLY

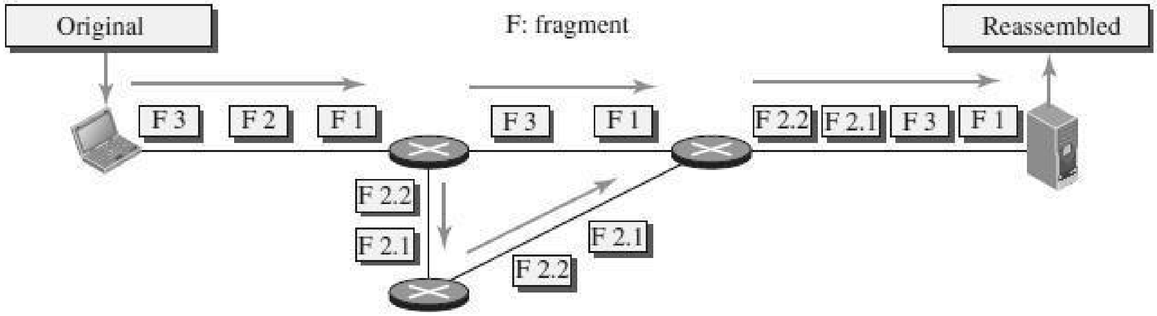
Fragmentation:

- Every network type has a ***maximum transmission unit*** (MTU), which is the largest IP datagram that it can carry in a frame.



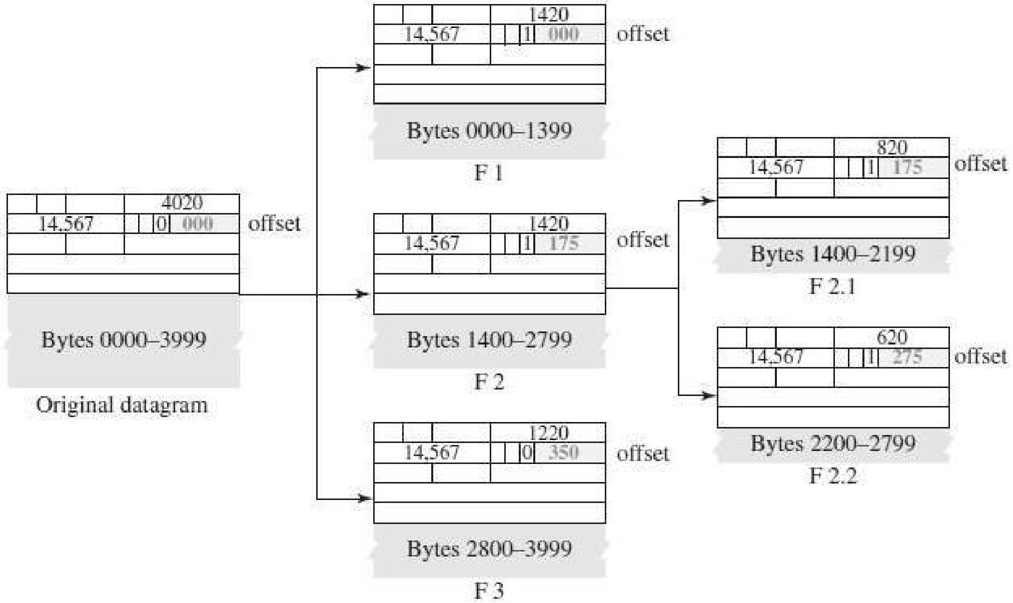
- Fragmentation of a datagram will only be necessary if the path to the destination includes a network with a smaller MTU.
- When a host sends an IP datagram, it can choose any size that it wants.
- Fragmentation typically occurs in a router when it receives a datagram that it wants to forward over a network that has an MTU that is smaller than the received datagram.
- Each fragment is itself a self-contained IP datagram that is transmitted over a sequence of physical networks, independent of the other fragments.
- Each IP datagram is re-encapsulated for each physical network over which it travels.
- For example, if we consider an Ethernet network to accept packets up to 1500 bytes long.
- This leaves two choices for the IP service model:
  - Make sure that all IP datagrams are small enough to fit inside one packet on any network technology
  - Provide a means by which packets can be fragmented and reassembled when they are too big to go over a given network technology.
- Fragmentation produces smaller, valid IP datagrams that can be readily reassembled into the original datagram upon receipt, independent of the order of their arrival.

Example:



- The original packet starts at the client; the fragments are reassembled at the server.
- The value of the identification field is the same in all fragments, as is the value of the flags field with the more bit set for all fragments except the last.
- Also, the value of the offset field for each fragment is shown.
- Although the fragments arrived out of order at the destination, they can be correctly reassembled.

- The value of the offset field is always relative to the original datagram.



- Even if each fragment follows a different path and arrives out of order, the final destination host can reassemble the original datagram from the fragments received (if none of them is lost) using the following strategy:
    1) The first fragment has an offset field value of zero.
    2) Divide the length of the first fragment by 8. The second fragment has an offset value equal to that result.
    3) Divide the total length of the first and second fragment by 8. The third fragment has an offset value equal to that result.
    4) Continue the process. The last fragment has its M bit set to 0.
    5) Continue the process. The last fragment has a *more* bit value of 0.

Reassembly:

- Reassembly is done at the receiving host and not at each router.
- To enable these fragments to be reassembled at the receiving host, they all carry the same identifier in the Ident field.
- This identifier is chosen by the sending host and is intended to be unique among all the datagrams that might arrive at the destination from this source over some reasonable time period.
- Since all fragments of the original datagram contain this identifier, the reassembling host will be able to recognize those fragments that go together.
- For example, if a single fragment is lost, the receiver will still attempt to reassemble the datagram, and it will eventually give up and have to garbage- collect the resources that were used to perform the failed reassembly.
- Hosts are now strongly encouraged to perform "path MTU discovery," a process by which fragmentation is avoided by sending packets that are small enough to traverse the link with the smallest MTU in the path from sender to receiver.

IP SECURITY

There are three security issues that are particularly applicable to the IP protocol:

(1) Packet Sniffing (2) Packet Modification and (3) IP Spoofing.

Packet Sniffing

- An intruder may intercept an IP packet and make a copy of it.
- Packet sniffing is a passive attack, in which the attacker does not change the contents of the packet.
- This type of attack is very difficult to detect because the sender and the receiver may never know that the packet has been copied.
- Although packet sniffing cannot be stopped, encryption of the packet can make the attacker's effort useless.
- The attacker may still sniff the packet, but the content is not detectable.

Packet Modification

- The second type of attack is to modify the packet.
- The attacker intercepts the packet, changes its contents, and sends the newpacket to the receiver.
- The receiver believes that the packet is coming from the original sender.
- This type of attack can be detected using a data integrity mechanism.
- The receiver, before opening and using the contents of the message, can use this mechanism to make sure that the packet has not been changed during the transmission.

IP Spoofing

- An attacker can masquerade as somebody else and create an IP packet that carries the source address of another computer.
- An attacker can send an IP packet to a bank pretending that it is coming from one of the customers.
- This type of attack can be prevented using an origin authentication mechanism

IP Sec

- The IP packets today can be protected from the previously mentioned attacks using a protocol called IPsec (IP Security).
- This protocol is used in conjunction with the IP protocol.
- IPsec protocol creates a connection-oriented service between two entities in which they can exchange IP packets without worrying about the three attacks such as Packet Sniffing, Packet Modification and IP Spoofing.
- IP Sec provides the following four services:

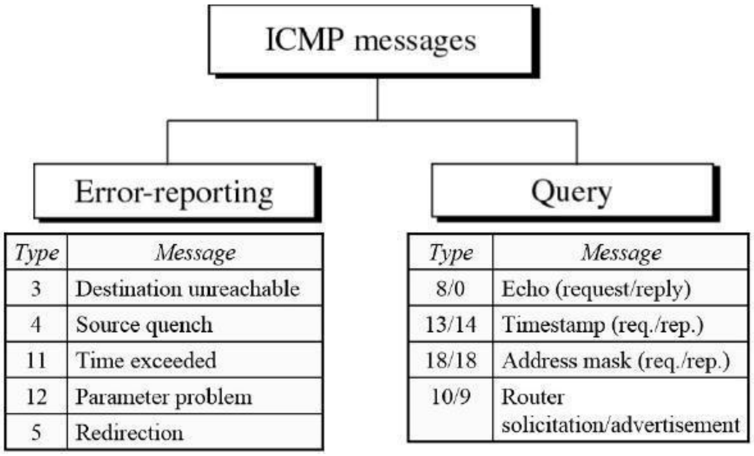
1) **Defining Algorithms and Keys:** The two entities that want to create a secure channel between themselves can agree on some available algorithms and keys to be used for security purposes.
2) **Packet Encryption:** The packets exchanged between two parties can be encrypted for privacy using one of the encryption algorithms and a shared key agreed upon in the first step. This makes the packet sniffing attack useless.
3) **Data Integrity:** Data integrity guarantees that the packet is not modified during the transmission. If the received packet does not pass the data integrity test, it is discarded. This prevents the second attack,packet modification.
4) **Origin Authentication:** IPsec can authenticate the origin of the packet to be sure that the packet is not created by an imposter. This can prevent IP spoofing attacks.

ICMPV4 - INTERNET CONTROL MESSAGE PROTOCOL VERSION 4

- ICMP is a network-layer protocol.
- It is a companion to the IP protocol.
- Internet Control Message Protocol (ICMP) defines a collection of error messages that are sent back to the source host whenever a router or host is unable to process an IP datagram successfully.

ICMP MESSAGE TYPES

- ICMP messages are divided into two broad categories: *error-reporting messages* and *query messages.*
- The error-reporting messages report problems that a router or a host (destination) may encounter when it processes an IP packet.
- The query messages help a host or a network manager get specific information from a router or another host.



Type	*Message*
3	Destination unreachable
4	Source quench
11	Time exceeded
12	Parameter problem
5	Redirection

Type	*Message*
8/0	Echo (request/reply)
13/14	Timestamp (req./rep.)
18/18	Address mask (req./rep.)
10/9	Router solicitation/advertisement

ICMP Error – Reporting Messages

- ICMP error messages report error conditions
- Typically sent when a datagram is discarded
- Error message is often passed from ICMP to the application program

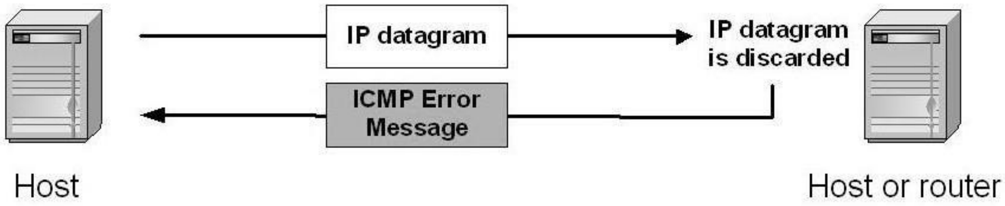
➢ ***Destination Unreachable*—**When a router *cannot route* a datagram, the datagram is discarded and sends a destination unreachable message to source host.

➢ ***Source Quench*—**When a router or host discards a datagram due to *congestion*, it sends a source-quench message to the source host. This message acts as flow control.

➢ ***Time Exceeded*—**Router discards a datagram when TTL field becomes 0 and a time exceeded message is sent to the source host.

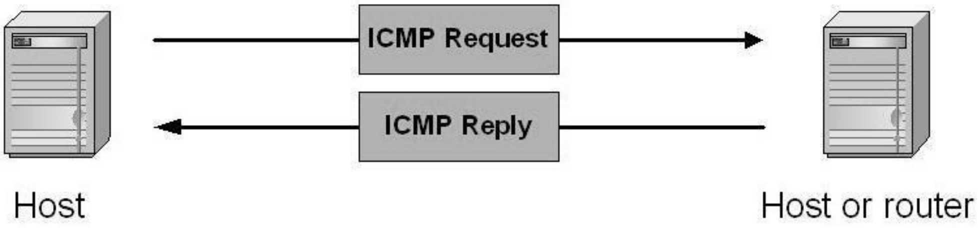
➢ ***Parameter Problem*—**If a router discovers ambiguous or *missing* value in any field of the datagram, it discards the datagram and sends parameter problem message to source.

➢ ***Redirection*—**Redirect messages are sent by the default router to inform the source host to *update* its forwarding table when the packet is routed on a wrong path.



ICMP Query Messages

- Request sent by host to a router or host
- Reply sent back to querying host



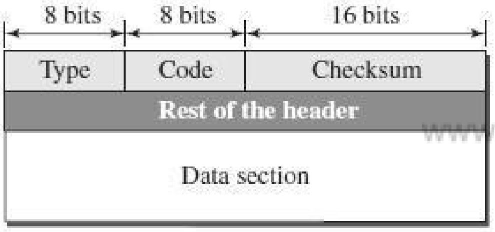
➢ ***Echo Request & Reply*—**Combination of echo request and reply messages determines whether two systems communicate or not.

➢ ***Timestamp Request & Reply*—**Two machines can use the timestamp request and reply messages to determine the round-trip time (RTT).

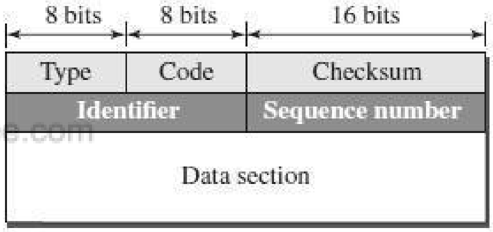
- ***Address Mask Request & Reply*—**A host to obtain its subnet mask, sends an address mask request message to the router, which responds with an address mask reply message.
- ***Router Solicitation/Advertisement*—**A host broadcasts a router solicitation message to know about the router. Router broadcasts its routing information with router advertisement message.

ICMP MESSAGE FORMAT

- An ICMP message has an 8-byte header and a variable-size data section.



Error-reporting messages



Query messages

Type	Defines the type of the message
Code	Specifies the reason for the particular message type
Checksum	Used for error detection
Rest of the header	Specific for each message type
Data	Used to carry information
Identifier	Used to match the request with the reply
Sequence Number	Sequence Number of the ICMP packet

ICMP DEBUGGING TOOLS

Two tools are used for debugging purpose. They are (1) Ping (2) Traceroute

Ping

- The *ping* program is used to find if a host is alive and responding.
- The source host sends ICMP echo-request messages; the destination, if alive, responds with ICMP echo-reply messages.
- The *ping* program sets the identifier field in the echo-request and echo-reply message and starts the sequence number from 0; this number is incremented by 1 each time a new message is sent.
- The *ping program* can calculate the round-trip time.
- It inserts the sending time in the data section of the message.
- When the packet arrives, it subtracts the arrival time from the departure time to get the round-trip time (RTT).

```
$ ping google.com
```

Traceroute or Tracert

- The *traceroute* program in UNIX or *tracert* in Windows can be used to trace the path of a packet from a source to the destination.
- It can find the IP addresses of all the routers that are visited along the path.
- The program is usually set to check for the maximum of 30 hops (routers) to be visited.
- The number of hops in the Internet is normally less than this.

```
$ traceroute google.com
```

IPV6 - NEXT GENERATION IP

- 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.

FEATURES OF IPV6

1. ***Better header format* -** IPv6 uses a new header format in which options are separated from the base header and inserted, when needed, between the base header and the data. This simplifies and speeds up the routing process because most 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 been removed, but two new fields, traffic class and flow label, have been added to enable the source to request special handling of the packet. This mechanism can be used to support traffic such as real-time audio and video.

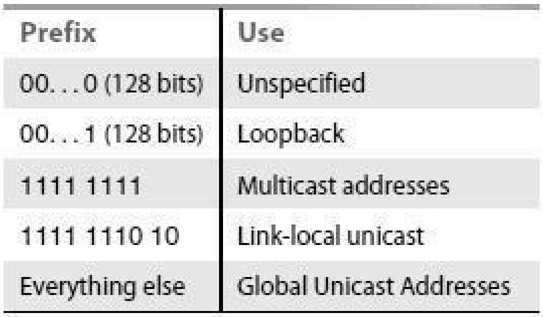
Additional Features:

1. Need to accommodate scalable routing and addressing
2. Support for real-time services
3. Security support
4. Autoconfiguration

   The ability of hosts to automatically configure themselves with such information as their own IP address and domain name.
5. Enhanced routing functionality, including support for mobile hosts
6. Transition from ipv4 to ipv6

ADDRESS SPACE ALLOCATION OF IPV6

□ IPv6 provides a 128-bit address space to handle up to 2^{128}
□ 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

□ A node may be assigned an “IPv4-compatible IPv6 address” by zero-extending a 32-bit IPv4 address to128 bits.

□A node that is only capable of understanding IPv4 can be assigned an “IPv4- mapped IPv6 address” by prefixing the 32-bit IPv4 address with 2 bytes of all 1s and then zero-extending the result to 128 bits.

ADDRESS NOTATION OF IPV6

- 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

<u>Discards leading Zeros</u>

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

To

47CD **:** 1234 **:** 4422 **:** ACO2 **:** 22 **:** 1234 **:** A456 **:** 0124

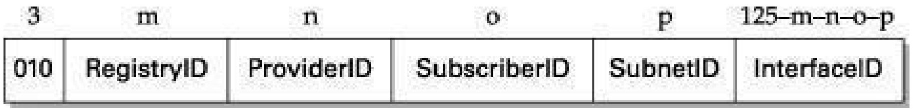
<u>Consecutive Zeros can be replaced by colon</u>

For example,

47CD **:** 0000 **:** 0000 **:** 0000 **:** 0000 **:** 0000 **:** A456 **:** 0124 → 47CD **: :** A456 **:** 0124

ADDRESS AGGREGATION OF IPV6

- IPv6 provides *aggregation* of routing information to reduce the burden on routers.
- Aggregation is done by assigning prefixes at *continental* level.
- For *example*, if all addresses in Europe have a common prefix, then routers in other continents would need one routing table entry for all networks in Europe.



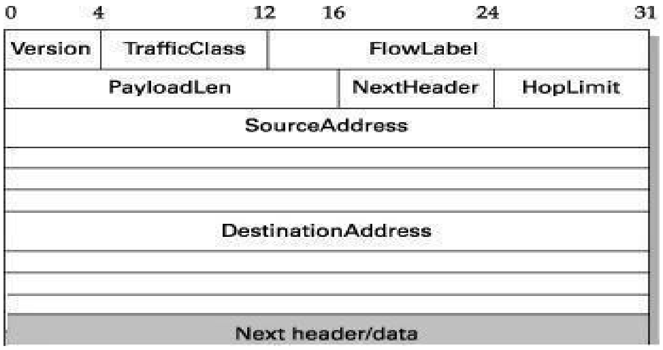
- ❖ ***Prefix*** - All addresses in the same continent have a common prefix
- ❖ ***RegistryID* —** identifies the continent
- ❖ ***ProviderID* —** identifies the provider for Internet access, i.e., ISP.
- ❖ ***SubscriberID* —** specifies the subscriber identifier
- ❖ ***SubntID* —** contains subnet of the subscriber.
- ❖ ***InterfaceID* —**contains link level or physical address.

PACKET FORMAT OF IPV6

- IPv6 base header is 40 bytes long.

Version — specifies the IP version, i.e., 6.

- ❖ ***Traffic Class*** — defines priority of the packet with respect to traffic congestion. It is either congestion-controlled or non-congestion controlled
- ❖ ***Flow Label*** — provides special handling for a particular flow of data. Router handles different flows with the help of a flow table.



- ❖ ***Payload Len*** — gives length of the packet, excluding IPv6 header.(Actual data)
- ❖ ***Next Heade***r — Options are specified as a header following IP header. NextHeader contains a pointer to optional headers.
- ❖ ***Hop Limit*** — Gives the TTL value of a packet.
- ❖ ***Source Address / Destination Address*** — 16-byte addresses of source and destination host

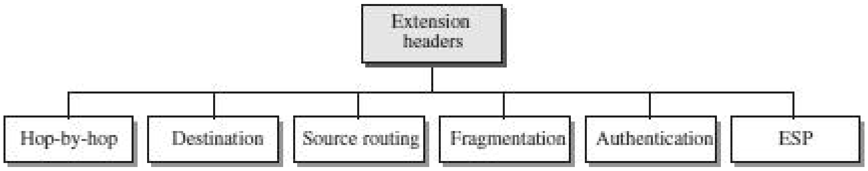
Extension Headers

□ Extension header provides greater functionality to

□ IPv6. Base header may be followed by six

□ extension headers.

Each extension header contains a NextHeader field to identify the header following it.



- ❖ ***Hop-by-Hop*** — source host sends information to all routers visited by the packet
- ❖ ***Destination*** — source host information is passed to the destination only.
- ❖ ***Source Routing*** — routing information provided by the source host.
- ❖ ***Fragmentation*** — In IPv6, only the source host can fragment. Source uses a path MTU discovery technique to find smallest MTU on the path.
- ❖ ***Authentication*** — used to validate the sender and ensures data integrity.
- ❖ ***ESP (Encrypted Security Payload)*** — provides confidentiality against eaves dropping.

ADVANCED CAPABILITIES OF IPV6

□ **Auto Configuration** — Auto or stateless configuration of IP address to hosts without the need for a DHCP server, i.e., plug and play.

□ **Advanced Routing** — Enhanced routing support for mobile hosts is provided.

□ **Additional Functions —** Enhanced routing functionality with support for mobile hosts.

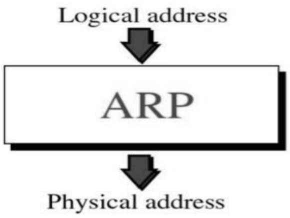
□ **Security —** Encryption and authentication options provide confidentiality and integrity.

□ **Resource allocation —** Flow label enables the source to request special handling of real-time audio and video packets

ARP stands for Address Resolution Protocol.

ADDRESS RESOLUTION PROTOCOL(ARP)

- o ARP is the most important protocol of the Data Link Layer.
- o ARP is a network layer protocol used to **convert a IP address (Network/Logical address) into a MAC Address (Hardware /Physical address).**



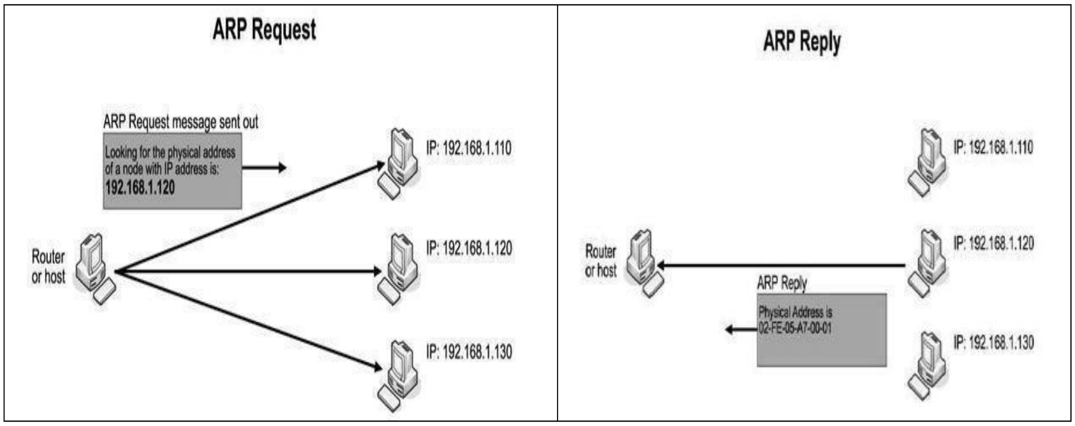
- The computer programs/applications use logical address (IP address) to send/receive messages, however the actual communication happens over the physical address (MAC address).
- To send a datagram over a network, we need both the logical and physical address.
- IP addresses are made up of 32 bits whereas MAC addresses are made up of 48 bits.
- ARP enables each host to build a table of IP address and corresponding physical address.
- ARP relies on broadcast support from physical networks.
- The Address Resolution Protocol is a request and response protocol.
- The types of ARP messages are:
    1. ARP request
    2. ARP reply

ARP Operation

- ARP maintains a cache table in which MAC addresses are mapped to IP addresses.
- If a host wants to send an IP datagram to a host,it first checks for a mapping in the cache table.
- If no mapping is found, it needs to invoke the Address Resolution Protocol over the network.
- It does this by broadcasting an ARP query onto the network.

- This query contains the target IP address.
- Each host receives the query and checks to see if it matches its IP address.
- If it does match, the host sends a response message that contains its link- layer address (MAC Address) back to the originator of the query.
- The originator adds the information contained in this response to its ARP table.
- For example,

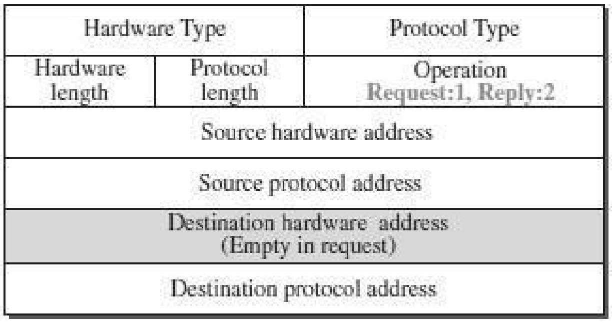
To determine system B's physical (MAC) address, system A broadcasts an ARP request containing B's IP address to all machines on its network.



- All nodes except the destination discard the packet but update their ARP table.
- Destination host (System B) constructs an ARP Response packet
- ARP Response is unicast and sent back to the source host (System A).
- Source stores target Logical & Physical address pair in its ARP table from ARP Response.

- If target node does not exist on same network, ARP request is sent to default router.

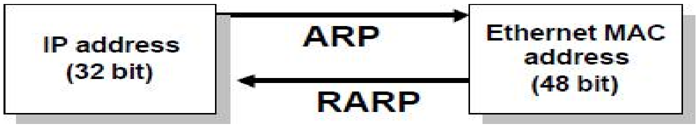
ARP Packet



<table>
<tr><td colspan="2">Hardware Type</td><td>Protocol Type</td></tr>
<tr><td>Hardware length</td><td>Protocol length</td><td>Operation
Request:1, Reply:2</td></tr>
<tr><td colspan="3">Source hardware address</td></tr>
<tr><td colspan="3">Source protocol address</td></tr>
<tr><td colspan="3">Destination hardware address
(Empty in request)</td></tr>
<tr><td colspan="3">Destination protocol address</td></tr>
</table>

RARP – Reverse ARP

- Reverse Address Resolution protocol (RARP) allows a host to convert itsMAC address to the corresponding IP address.



Reverse Address Resolution Protocol

Introduction

Reverse Address Resolution Protocol, also known as reverse ARP, is a networking protocol used to link a MAC address with an Internet Protocol (IP) address. It is the inverse of the Address Resolution Protocol (ARP), which links an IP address with a MAC address. RARP was originally developed in the stages of computer networking as a means to assign IP addresses to diskless workstations or other devices that were unable to store their IP addresses. In this blog, we will explain the RARP protocol, its purpose, and how it works, along with its advantages and disadvantages.

What is Reverse Address Resolution Protocol?

Reverse Address Resolution Protocol or RARP is the inverse of the more commonly used Address Resolution Protocol (ARP). ARP is a protocol that maps an IP address to a MAC address, which is needed for data link layer communication. RARP, on the other hand, maps a MAC address to an IP address, which is needed for network layer communication.

During its inception, Reverse Address Resolution Protocol was designed specifically for devices such as diskless workstations that lacked the capability to store their IP addresses. In this scenario, these devices would broadcast their MAC addresses and request an IP address. A RARP server on the network would then respond with an IP address corresponding to that MAC address.

The functionality and operation of RARP are documented in RFC 903. It functions within the data link layer of the OSI model. ARP and DHCP have largely replaced it in networks. It had a significant impact on the evolution of computer networking protocols and is still utilized in specific situations.

Purpose of Reverse Address Resolution Protocol

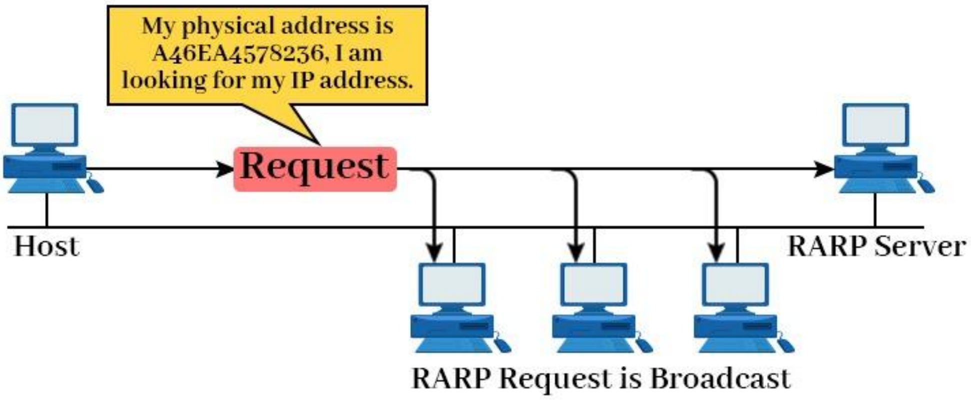
The primary goal of the Reverse Address Resolution Protocol (RARP) is to allocate IP addresses to devices that lack storage or configuration files to store their IP addresses. These devices include workstations, embedded systems, network printers, routers, and switches.

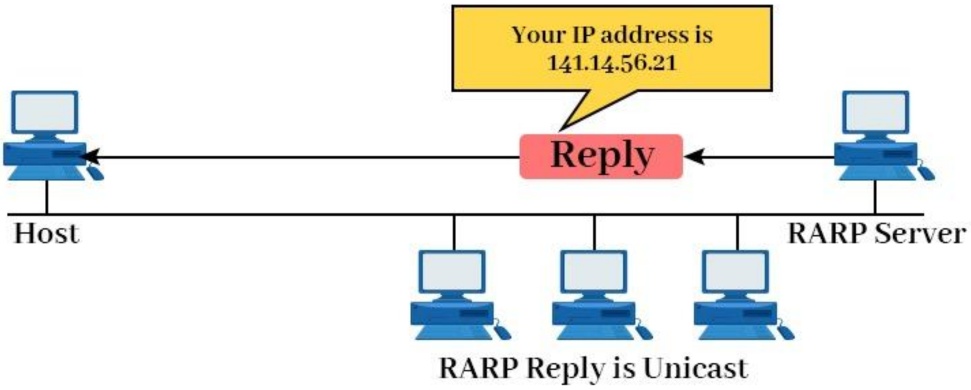
RARP enables these devices to dynamically acquire an IP address from an RARP server. The RARP server maintains a table associating MAC addresses with corresponding IP addresses. Once obtained, the device can utilize this IP address for communication with network devices or for accessing network resources.

Additionally, the RARP protocol plays a role in preventing conflicts related to IP addresses. By ensuring that each MAC address is assigned an IP address, the RARP server prevents instances where two devices share the IP address within the network. Such conflicts can lead to communication errors and disruptions in network connectivity.

How does Reverse Address Resolution Protocol work?

The functioning of RARP can be summarized as follows:


My physical address is A46EA4578236, I am looking for my IP address.
Request
Host
RARP Server
RARP Request is Broadcast



- When a device needs an IP address, it broadcasts a RARP request packet containing its MAC address in both the sender and receiver hardware address fields.
- A special host known as a RARP server configured on the network receives the RARP request packet. After that, it checks its table of MAC addresses and IP addresses.
- If the RARP server finds a matching entry for the MAC address, it sends back an RARP reply packet that includes both the MAC address and the corresponding IP address.
- The device that initiated the RARP request packet receives the RARP reply packet. After getting the reply, it then extracts the IP address from it. This IP address is then used for communication on the network.

RARP Structure

The RARP packet structure is similar to ARP's but has minor differences. The packet contains:

- **Hardware Type**: Specifies the network technology (e.g., Ethernet).
- **Protocol Type**: Identifies the protocol being used (usually IP).
- **Hardware Address Length**: The length of the MAC address.
- **Protocol Address Length**: The length of the IP address.
- **Operation Code**: Specifies if it's a request or a response.
- **Sender/Receiver Hardware Address**: The MAC addresses of the sender and receiver.
- **Sender/Receiver Protocol Address**: The IP addresses (if available).

Each field in the RARP packet helps the server determine which machine requests an IP and ensures the correct IP is returned.

Components of RARP

- **IP Address Assignment:** RARP assists a device in learning its IP address on startup. RARP server associates the MAC address of the device to an IP and replies with it.

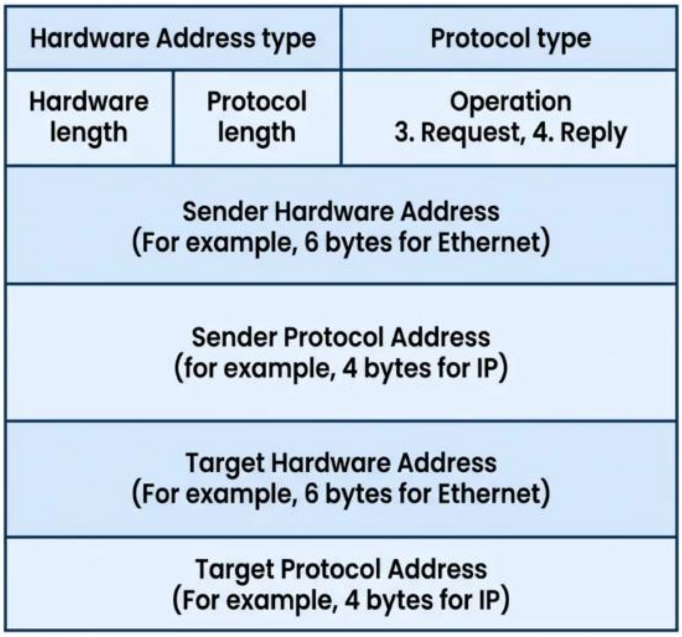
- **RARP Server:** RARP server gets the request and then checks a table which maps MAC address to IP. If it discovers a match, it will prepare the appropriate IP.

- **RARP Reply:** A server will send a RARP reply back to the client. Usually, it's on the local network. This reply includes the IP address associated with the client's MAC address.

- **Physical Address**: The physical address refers to the device' Mac address. RARP relies on this MAC as the key identifier on the local network to request and receive the appropriate IP address.

RARP Packet Format

RARP uses almost the same header layout as ARP. The main difference is the purpose: RARP helps a device learn its IP using its MAC address.



<table>
<tr><td colspan="2">Hardware Address type</td><td>Protocol type</td></tr>
<tr><td>Hardware length</td><td>Protocol length</td><td>Operation
3. Request, 4. Reply</td></tr>
<tr><td colspan="3">Sender Hardware Address
(For example, 6 bytes for Ethernet)</td></tr>
<tr><td colspan="3">Sender Protocol Address
(for example, 4 bytes for IP)</td></tr>
<tr><td colspan="3">Target Hardware Address
(For example, 6 bytes for Ethernet)</td></tr>
<tr><td colspan="3">Target Protocol Address
(For example, 4 bytes for IP)</td></tr>
</table>

- **Hardware Address Type:** Tells what kind of hardware address is used, like Ethernet. This helps both sides interpret the MAC address field in a standard, correct way.

- **Protocol Address Type (PTYPE):** Identifies the network protocol for the logical address, commonly IPv4. It tells the receiver what type of "protocol address" is being carried out.

- **Hardware length (HLEN):** The size of the hardware address in bytes. For Ethernet MAC addresses, this value is usually 6, so devices know the exact address length.

- **Protocol length (PLEN):** The length of the protocol's address in bytes. For IPv4, the most common is 4. This ensures that that the IP address is read in the correct size.

- **Operation:** Determines if it is either a request, or a reply. In RARP, one value signifies "request IP for this MAC," while the other is "here is the IP."

- **Sender Hardware Address:** It is the MAC address of the person who is the sender of the packet. In a request, this will be your client's MAC. In a reply, it's usually that server's MAC.

- **Sender Protocol Address:** The protocol address of the sender (like the IP). In a request, the user might not know its own IP; therefore, it could be blank and set at zero.

- **Target Hardware Address:** The MAC address being asked about. In a request, it is usually the client's MAC again. In a reply, it confirms which device the IP belongs to.

- **Target Protocol Address:** The protocol address for the target. In reply, this is the IP address the client needs. In a request, it is usually unknown and left blank.

Why Reverse Address Resolution Protocol Became Obsolete?

With the advancement in protocols like DHCP and BOOTP, RARP became useless. These protocols offered **more features, dynamic IP allocation**, and better scalability, which made RARP unnecessary in most modern networks.

As RARP became obsolete, modern networks moved to protocols like DHCP for automatic IP address assignment. These concepts are explored in more detail during practical network configuration labs in our Network Engineer Course.

Alternatives to RARP

Today, **DHCP** has almost entirely replaced RARP, offering a **more efficient and secure** way to assign IP addresses dynamically across networks.

Advantages of RARP Protocol

Some advantages of utilizing RARP include:

- Simplification of device configuration and management for those lacking storage or configuration files for storing their IP addresses.
- Reduction of overhead and complexity by eliminating manual assignment of individual IP addresses to each device.
- Prevention of potential conflicts by guaranteeing that every MAC address receives a distinct IP address assigned by the RARP server.
- Support for legacy devices that do not support newer protocols, like DHCP or BOOTP.

Disadvantages of RARP Protocol

Apart from all the advantages, RARP also has some disadvantages. Some disadvantages of using RARP are:

- It requires a RARP server on each network segment, which increases both cost and maintenance overhead for network infrastructure.
- Broadcasting is relied upon by RARP, causing consumption and potential network congestion.
- There is no provision for security or authentication mechanisms to verify the identity or validity of devices requesting or receiving IP addresses.
- It lacks support for any functionalities or choices like subnet mask, default gateway, DNS server, or lease time. These features are typically offered by protocols such as DHCP or BOOTP.