**Unit 4 – Network and Transport Layer**

**Network Layer**

**Logical Addressing:** *(Not logical at all yuck.)*

We use the term IP address to mean a logical address in the network layer of the TCP/IP protocol suite.

The Internet addresses are 32 bits in length; this gives us a maximum of 232 addresses. These addresses are referred to as IPv4 (IP version 4) addresses or simply IP addresses.

The need for more addresses, in addition to other concerns about the IP layer, motivated

a new design of the IP layer called the new generation of IP or IPv6 (lP version 6).

In this version, the Internet uses 128-bit addresses that give much greater flexibility in

address allocation. These addresses are referred to as IPv6 (IP version 6) addresses.

***IPv4 ADDRESSES***

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

of a device (for example, a computer or a router) to the Internet. It is 32 bits long.

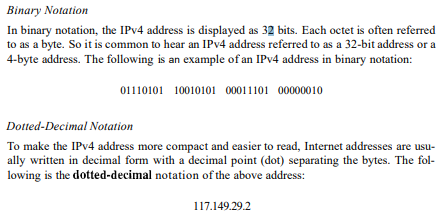
**Unique** in the sense that each address defines one, and only one, connection to the Internet. Two devices on the Internet can never have the same address at the same time.

**Universal** in the sense that the addressing system must be accepted by any host that wants to be connected to the Internet.

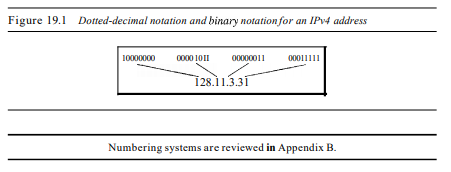
An **address space** is the total number of addresses used by the protocol. If a protocol uses N bits to define an address, the address space is 2N because each bit can have two different values (0 or 1) and N bits can have 2N values.

The address space of IPv4 is 232 or 4,294,967,296

There are 2 kinds of notations:

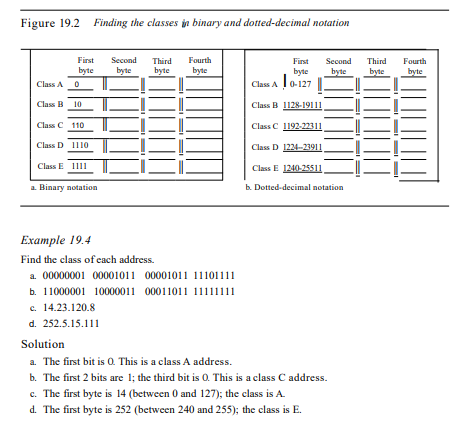


You can change one to another.



IPv4 used classful addressing: the address space is divided into five classes:

A, B, C, D, and E.



In c1assful addressing, a large part of the available addresses was wasted. To overcome this, there were 2 methods:

**Subnetting**: If an organization was granted a large block in class A or B, it could divide the addresses into several contiguous groups and assign each group to smaller networks (called subnets) or, in rare cases, share part of the addresses with neighbours. Subnetting increases the number of Is in the mask, as we will see later when we discuss classless addressing.

**Supernetting:** An organization can combine several class C blocks to create a larger range of addresses. In other words, several networks are combined to create a supernetwork or a supernet. An organization can apply for a set of class C blocks instead of just one**.**

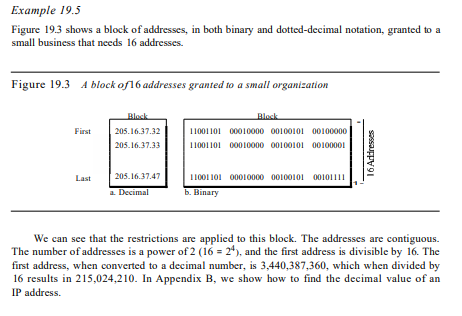
**Classful addressing, which is almost obsolete, is replaced with classless addressing.**

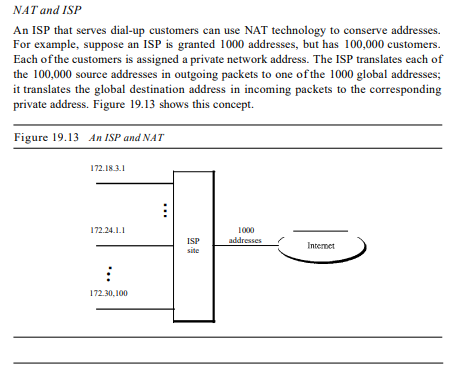
To simplify the handling of addresses, the Internet authorities impose three restrictions on classless address blocks:

1. The addresses in a block must be contiguous, one after another.

2. The number of addresses in a block must be a power of 2 (I, 2, 4, 8, ... ).

3. The first address must be evenly divisible by the number of addresses.

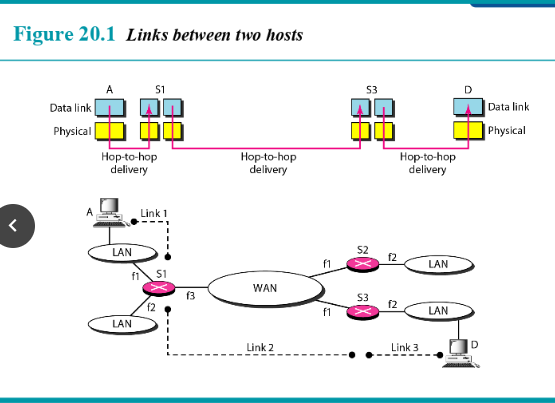




**Internet Protocol:**

In the Internet model, the main network protocol is the Internet Protocol (IP).

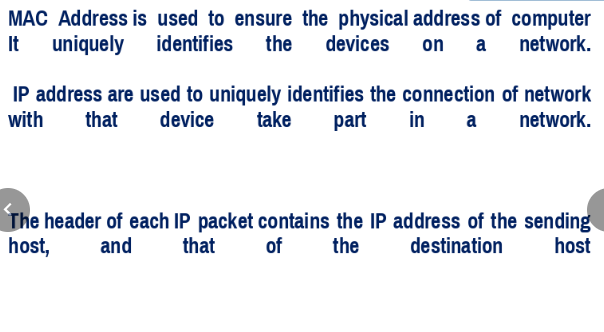
Internetworking: The physical and data link layers of a network operate locally. These two layers are jointly responsible for data delivery on the network from one node to the next, as shown in Figure 20.1.



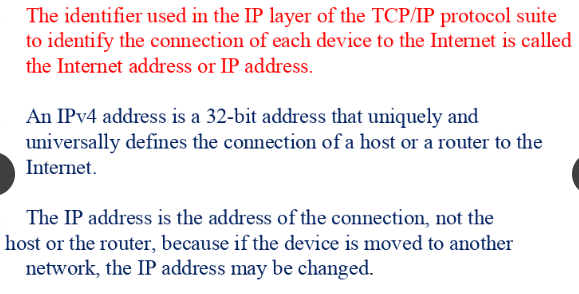
**Need for Network Layer:** To solve the problem of delivery through several links, the network layer (or the internetwork layer, as it is sometimes called) was designed. The network layer is responsible for host-to-host delivery and for routing the packets through the routers or switches.

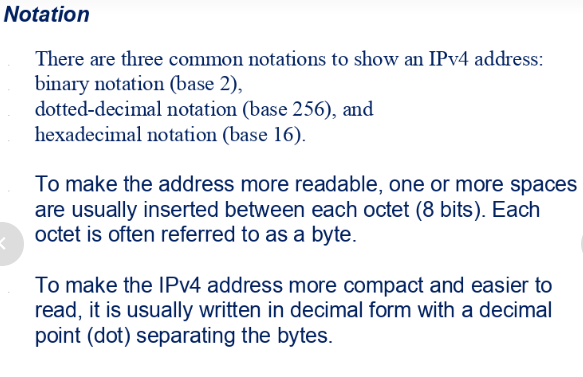
**Switching at the network layer in the Internet uses the datagram approach to packet switching.**

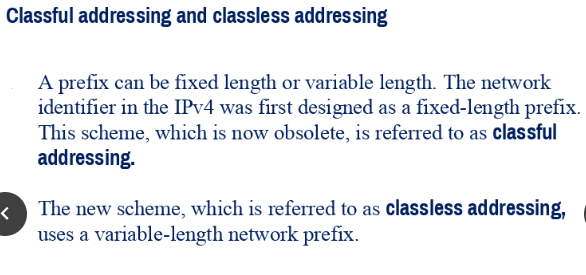
**Communication at the network layer in the Internet is connectionless.**



***IPv4 Address***

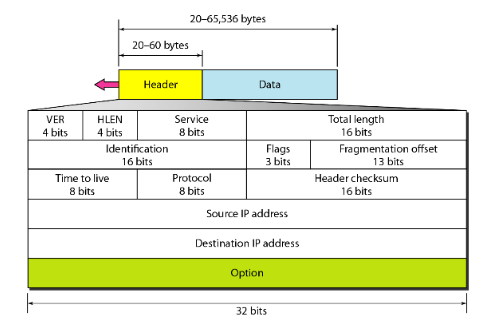




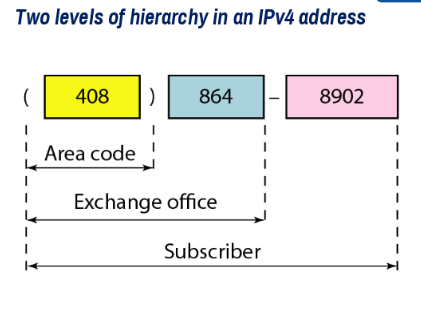


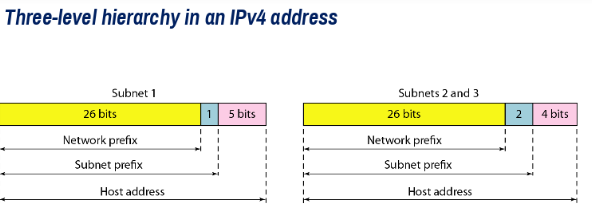
Classless addressing was brought on due to Address Depletion.

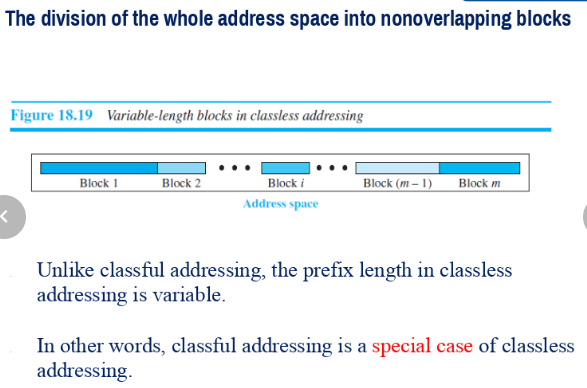
**Datagram:** Packets in the IPv4 layer are called datagrams. Figure 20.5 shows the IPv4 datagram format.

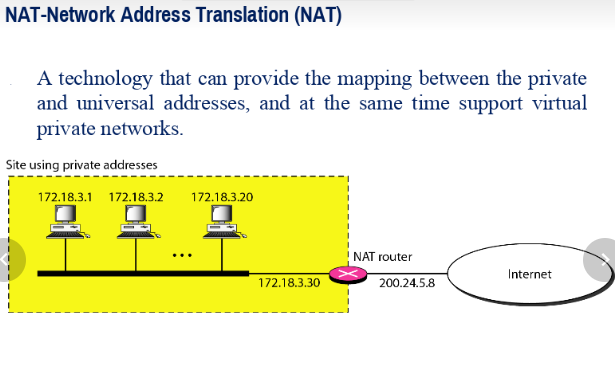


The first address in a block is normally not assigned to any device; it is used as the network address that represents the organization to the rest of the world.









**Fragmentation:** A datagram can travel through different networks. Each router decapsulates the IPv4 datagram from the frame it receives, processes it, and then encapsulates it in another frame. The format and size of the received frame depend on the protocol used by the physical network through which the frame has just traveled. The format and size of the sent frame depend on the protocol used by the physical network through which the frame is going to travel. The fields that are related to fragmentation and reassembly of an IPv4 datagram are the **identification, flags, and fragmentation offset** fields.

**Checksum** : The implementation of the checksum in the IPv4 packet follows the same principles. First, the value of the checksum field is set to O. Then the entire header is divided into 16-bit sections and added together. The result (sum) is complemented and inserted into the checksum field. The checksum in the IPv4 packet covers only the header, not the data. There are two good reasons for this. First, all higher-level protocols that encapsulate data in the IPv4 datagram have a checksum field that covers the whole packet. Therefore, the checksum for the IPv4 datagram does not have to check the encapsulated data. Second, the header of the IPv4 packet changes with each visited router, but the data do not. So the checksum includes only the part that has changed. If the data were included, each router must recalculate the checksum for the whole packet, which means an increase in processing time.

***IPv6 ADDRESSES and Internet Protocol***

IPv4 has some **deficiencies** (listed below) that make it unsuitable for the fast-growing Internet.

o Despite all short-term solutions, such as subnetting, classless addressing, and NAT, address depletion is still a long-term problem in the Internet.

o The Internet must accommodate real-time audio and video transmission. This type of transmission requires minimum delay strategies and reservation ofresources not provided in the IPv4 design.

o The Internet must accommodate encryption and authentication of data for some applications. No encryption or authentication is provided by IPv4

**Advantages of IPv6**

o Larger address space. An IPv6 address is 128 bits long, as we discussed in Chapter 19. Compared with the 32-bit address of IPv4, this is a huge (296) increase in the address space.

o 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 upper-layer data. This simplifies and speeds up the routing process because most of the options do not need to be checked by routers.

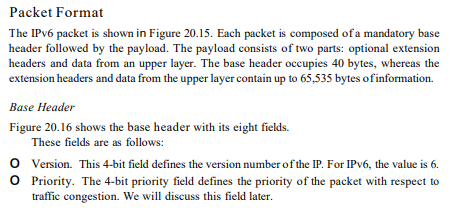
o New options. IPv6 has new options to allow for additional functionalities.

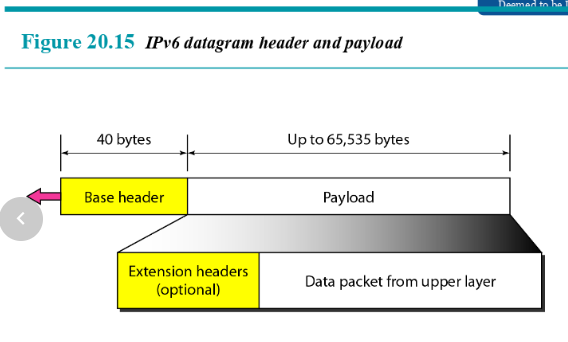
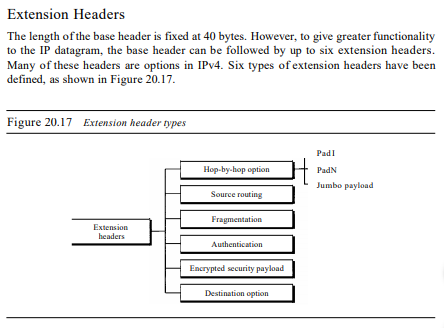
o Allowance for extension. IPv6 is designed to allow the extension of the protocol if required by new technologies or applications.

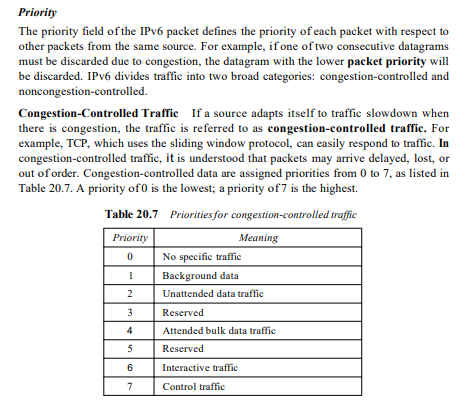
o Support for resource allocation. In IPv6, the type-of-service field has been removed, but a mechanism (called j low label) has been added to enable the source to request special handling of the packet. This mechanism can be used to support traffic such as real-time audio and video.

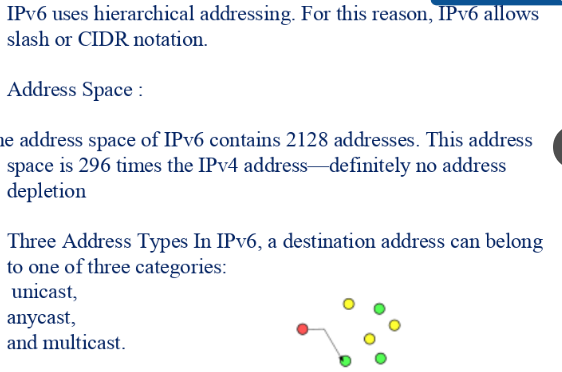
o Support for more security. The encryption and authentication options in IPv6 provide confidentiality and integrity of the packet.

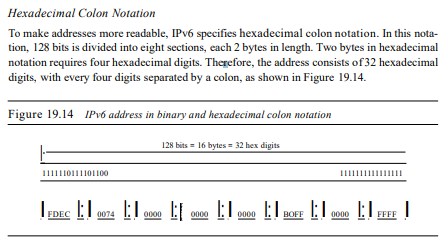
An IPv6 address consists of 16 bytes (octets); it is 128 bits long.

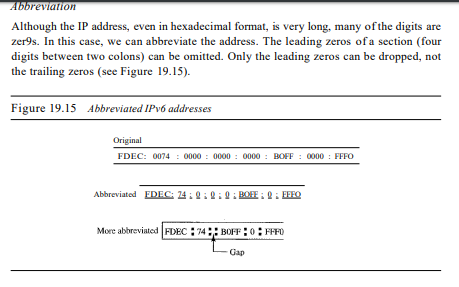




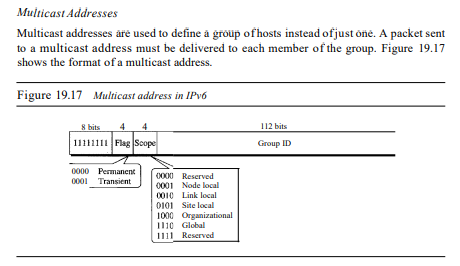




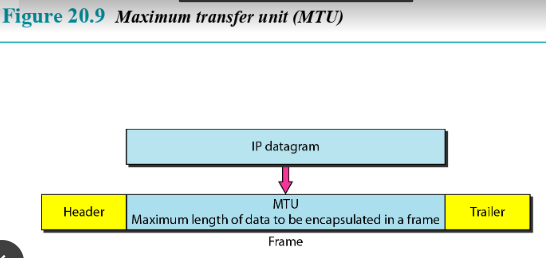


**Address Space:** IPv6 has a much larger address space; 2128 addresses are available.

**Unicast Addresses:** A unicast address defines a single computer. The packet sent to a unicast address must be delivered to that specific computer. IPv6 defines two types of unicast addresses: geographically based and provider-based.

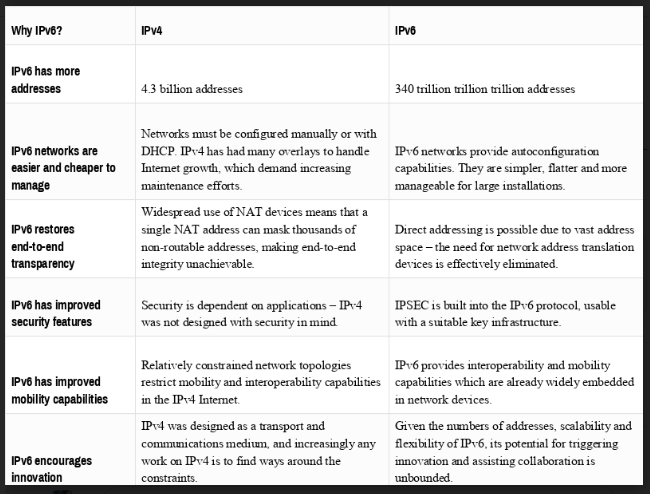


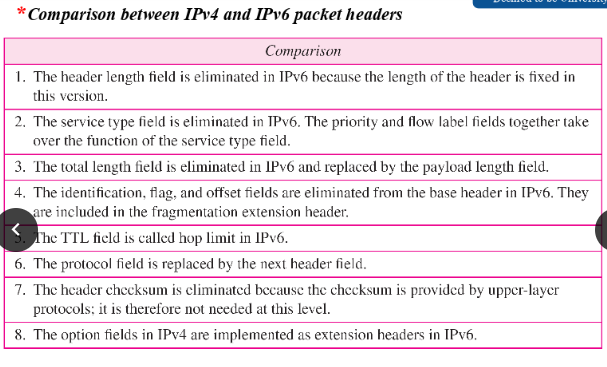
**Maximum Transfer Unit (MTU):** Each data link layer protocol has its own frame format in most protocols. One of the fields defined in the format is the maximum size of the data field. In other words, when a datagram is encapsulated in a frame, the total size of the datagram must be less than this maximum size, which is defined by the restrictions imposed by the hardware and software used in the network (see Figure 20.9). The value of the MTU depends on the physical network protocol. Table 20.5 shows the values for some protocols.



***Comparison between IPv4 and IPv6***





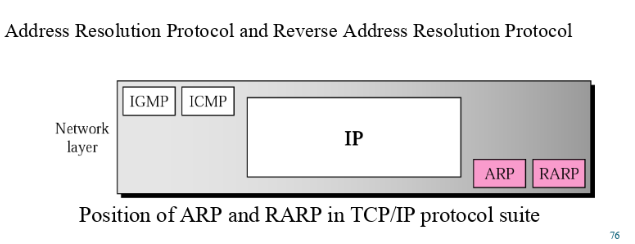


**Address Mapping Protocols**

We need protocols to create a mapping between physical and logical addresses. IP packets use logical (host-to-host) addresses. These packets, however, need to be encapsulated in a frame, which needs physical addresses (node-to-node).

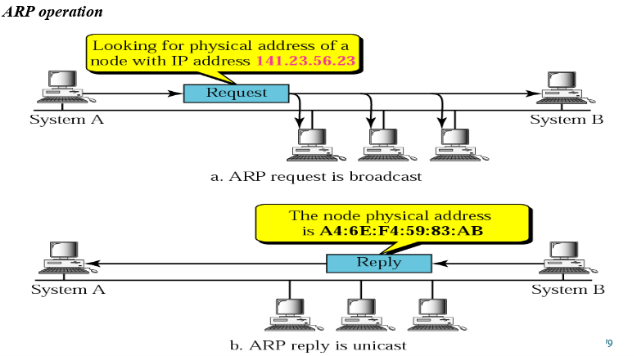
We will see that a protocol called **ARP**, the Address Resolution Protocol, is designed for this purpose.

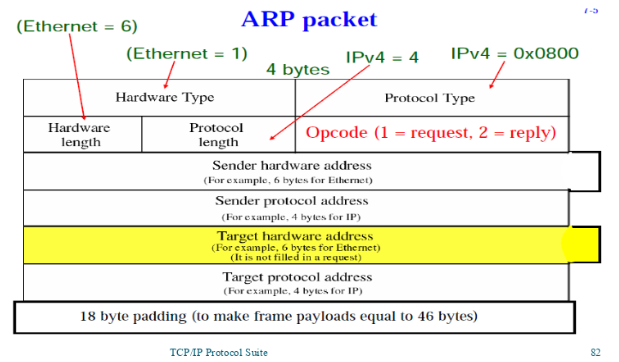
We sometimes need reverse mapping-mapping a physical address to a logical address. For example, when booting a diskless network or leasing an IP address to host such as **RARP**.



***ARP Packet***

ARP associates an IP address with its physical address. On a typical physical network, such as a LAN, each device on a link is identified by a physical or station address that is usually imprinted on the NIC.





o Hardware type. This is a 16-bit field defining the type of the network on which ARP is running. Each LAN has been assigned an integer based on its type. For example, Ethernet is given type 1. ARP can be used on any physical network.

o Protocol type. This is a 16-bit field defining the protocol. For example, the value of this field for the IPv4 protocol is 080016, ARP can be used with any higher-level protocol.

o Hardware length. This is an 8-bit field defining the length of the physical address in bytes. For example, for Ethernet the value is 6.

o Protocol length. This is an 8-bit field defining the length of the logical address in bytes. For example, for the IPv4 protocol the value is 4.

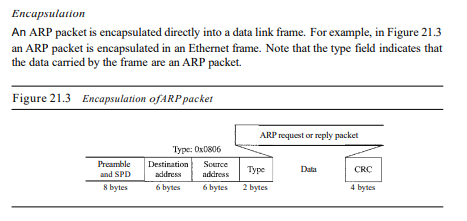
o Operation. This is a 16-bit field defining the type of packet. Two packet types are defined: ARP request (1) and ARP reply (2).

o Sender hardware address. This is a variable-length field defining the physical address of the sender. For example, for Ethernet this field is 6 bytes long.

o Sender protocol address. This is a variable-length field defining the logical (for example, IP) address of the sender. For the IP protocol, this field is 4 bytes long.

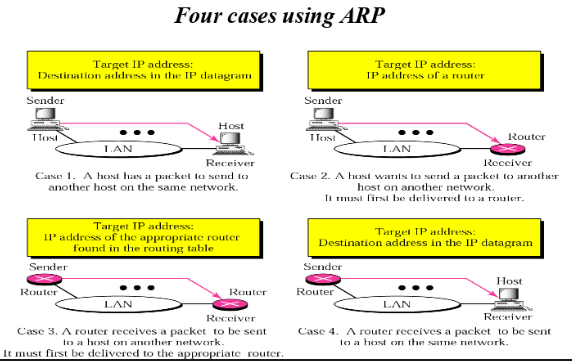
o Target hardware address. This is a variable-length field defining the physical address of the target. For example, for Ethernet this field is 6 bytes long. For an ARP request message, this field is alIOs because the sender does not know the physical address of the target.

o Target protocol address. This is a variable-length field defining the logical (for example, IP) address of the target. For the IPv4 protocol, this field is 4 bytes long.



**An ARP request is broadcast; an ARP reply is unicast.**

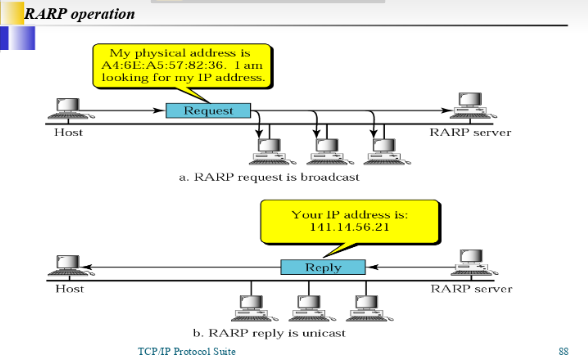
**A proxy ARP is an ARP that acts on behalf of a set of hosts.**

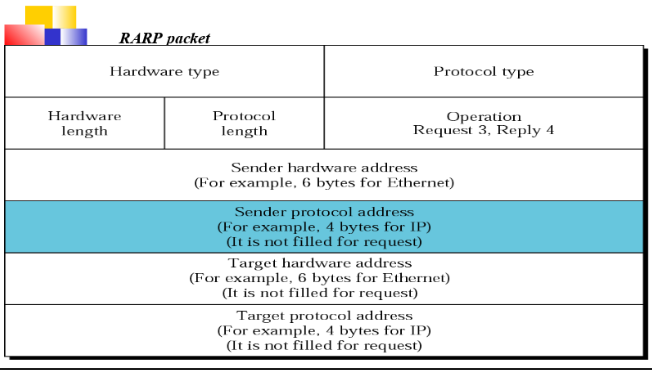


***RARP Packet***

**Reverse Address Resolution Protocol (RARP) finds the logical address for a machine that knows only its physical address.** Each host or router is assigned one or more logical (IP) addresses, which are unique and independent of the physical (hardware) address of the machine.

**The RARP request packets are broadcast; the RARP reply packets are unicast.**





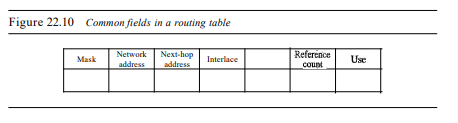
**\*Definitions same as given under ARP\***

**Routing Protocols**

A routing table can be either **static or dynamic**.

A static table is one with manual entries. The administrator enters the route for each destination into the table. When a table is created, it cannot update automatically when there is a change in the Internet. The table must be manually altered by the administrator.

A dynamic table is one that is updated automatically when there is a change somewhere in the Internet. A routing protocol is a combination of rules and procedures that lets routers in the Internet inform each other of changes.



o Mask. This field defines the mask applied for the entry.

o Network address. This field defines the network address to which the packet is finally delivered. In the case of host-specific routing, this field defines the address of the destination host.

o Next-hop address. This field defines the address of the next-hop router to which the packet is delivered.

o Interface. This field shows the name of the interface.

o Flags. This field defines up to five flags. Flags are on/off switches that signify either presence or absence. The five flags are U (up), G (gateway), H (host-specific), D (added by redirection), and M (modified by redirection).

a. U (up). The U flag indicates the router is up and running. If this flag is not present, it means that the router is down. The packet cannot be forwarded and is discarded.

b. G (gateway). The G flag means that the destination is in another network. The packet is delivered to the next-hop router for delivery (indirect delivery). When this flag is missing, it means the destination is in this network (direct delivery).

c. H (host-specific). The H flag indicates that the entry in the network address field is a host-specific address. When it is missing, it means that the address is only the network address of the destination.

d. D (added by redirection). The D flag indicates that routing information for this destination has been added to the host routing table by a redirection message from ICMP.

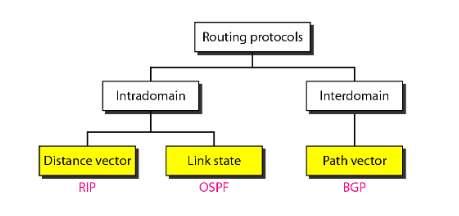
e. M (modified by redirection). The M flag indicates that the routing information for this destination has been modified by a redirection message from ICMP.

o Reference count. This field gives the number of users of this route at the moment. For example, if five people at the same time are connecting to the same host from this router, the value of this column is 5.

o Use. This field shows the number of packets transmitted through this router for the corresponding destination.

***Unicast Routing Protocols***

Unicast routing is the process of forwarding unicasted traffic from a source to a destination on an internetwork. Unicasted traffic is destined for a unique address.



**Distance Vector Routing -** The least-cost route between any two nodes is the route with minimum distance. In this protocol, as the name implies, each node maintains a vector (table) of minimum distances to every node. The table at each node also guides the packets to the desired node by showing the next stop in the route (next-hop routing).

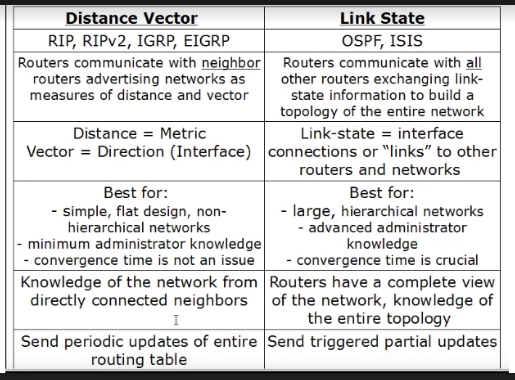
In distance-vector routing, the first thing each node creates is its own least-cost tree with the rudimentary information it has about its immediate neighbours. The incomplete trees are exchanged between immediate neighbours to make the trees more and more complete and to represent the whole internet. In other words, in distance-vector routing, a router continuously tells all of its neighbours what it knows.

**Link State Routing** - It has a different philosophy from that of distance vector routing. In link state routing, if each node in the domain has the entire topology of the domain the list of nodes and links, how they are connected including the type, cost (metric), and condition of the links (up or down)-the node can use Dijkstra's algorithm to build a routing table.

This method uses the term link-state to define the characteristic of a link (an edge) that represents a network in the internet. In this algorithm the cost associated with an edge defines the state of the link. In this algorithm, all routers flood the internet, with information related to their link states. When every router has the complete picture of the states, a link-state database can be created.

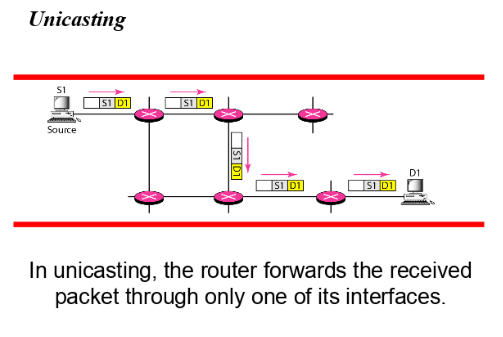
**Path-vector routing -** Both link-state and distance-vector routing are based on theleast-cost goal. However, there are instances where this goal is not the priority. Path-vector routing algorithms have beendesigned for this purpose. We can always insert policies in theforwarding table by preventing a packet from visiting a specificrouter. In path-vector routing, the best route from the source isthe best path, the one that complies with the policy imposed.The protocol that implements path-vector routing is the BorderGateway Protocol (BGP).

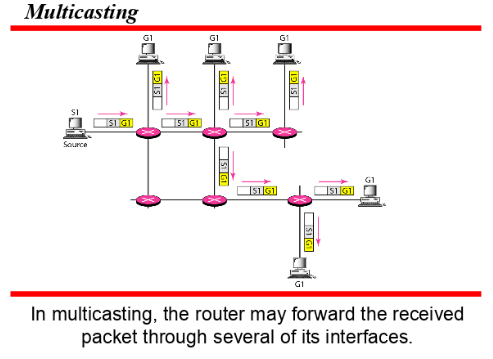
Comparison b/w



***Multicast Routing Protocols***

A message can be unicast, multicast, or broadcast. Let us clarify these terms as they relate to the Internet.

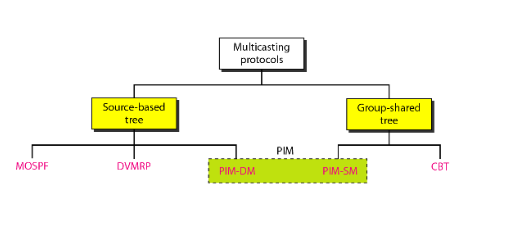




**Broadcasting:** In broadcast communication, the relationship between the source and the destination is one-to-all. There is only one source, but all the other hosts are the destinations.

**Multicast Routing:** When a router receives a multicast packet, the situation is different from when it receives a unicast packet. A multicast packet may have destinations in more than one network. Forwarding of a single packet to members of a group requires a shortest path tree. If we have n groups, we may need n shortest path trees.

**In multicast routing, each involved router needs to construct a shortest path tree for each group.**



**Source-Based Tree Approach**

In the source-based tree approach to multicasting, each router needs to create a separate tree for each source-group combination. In other words, if there are m groups and n sources in the internet, a router needs to create (m × n) routing trees. In each tree, the corresponding source is the root, the members of the group are the leaves, and the router itself is somewhere on the tree. We can compare the situation with unicast routing in which a router needs only one tree with itself as the root and all networks in the internet as the leaves.

**Group-Shared Tree Approach**

In the group-shared tree approach, we designate a router to act as the core source for each group. The designated router, which is called the core router, acts as the representative for the group. Any source that has a packet to send to a member of that group sends it to the core center (unicast communication) and the core center is responsible for multicasting. The core center creates one single routing tree with itself as the root and any routers with active members in the group as the leaves. In this approach, there are m core routers (one for each group) and each core router has a routing tree, for the total of m trees. This means that the number of routing trees is reduced from (m × n) in the source-based tree approach to m in this approach.