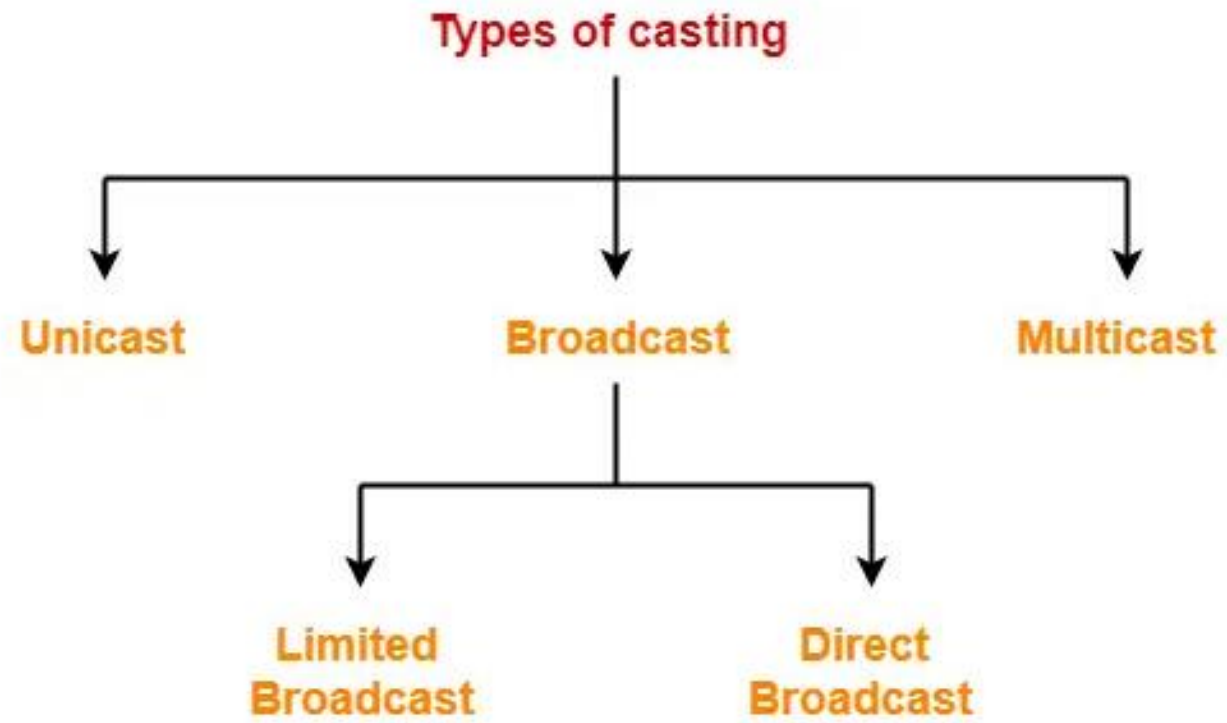
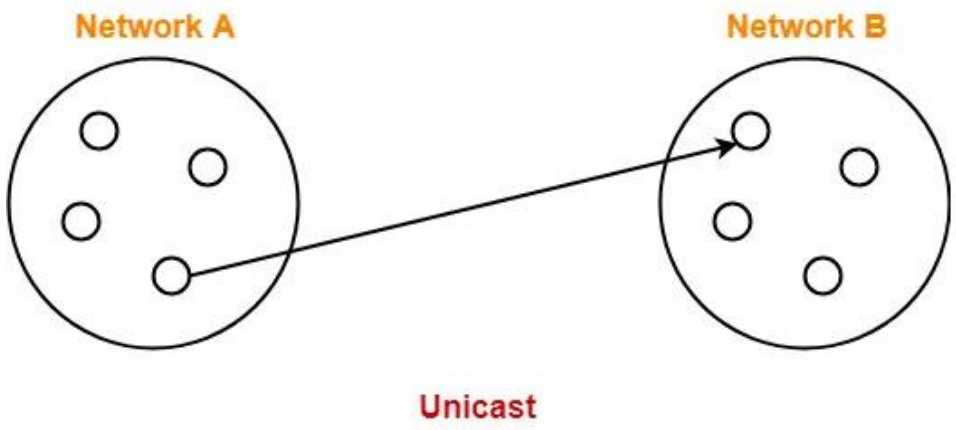
Logical addressing

Casting in Networking-



1. Unicast-

- Transmitting data from one source host to one destination host is called as **unicast**.
- It is a one to one transmission.



- **Example-**
- Host A having IP Address 11.1.2.3 sending data to host B having IP Address 20.12.4.2.
- Here,
- Source Address = IP Address of host A = 11.1.2.3
- Destination Address = IP Address of host B = 20.12.4.2

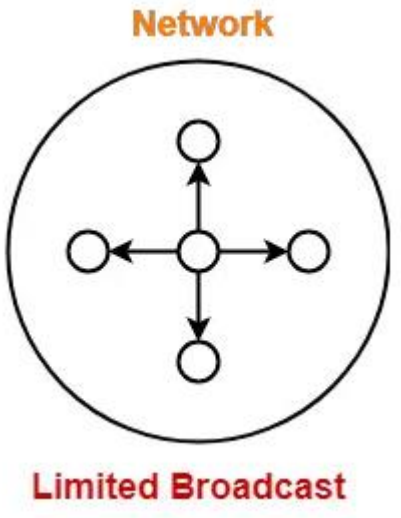
2. Broadcast-

- Transmitting data from one source host to all other hosts residing in the same or other network is called as **broadcast**.
- It is a one to all transmission.

- Based on recipient’s network, it is classified as-
- Limited Broadcast
- Direct Broadcast

A. Limited Broadcast-

- Transmitting data from one source host to all other hosts residing in the same network is called as **limited broadcast**.



NOTE

Limited Broadcast Address for any network

= All 32 bits set to 1

= 11111111.11111111.11111111.11111111

= 255.255.255.255

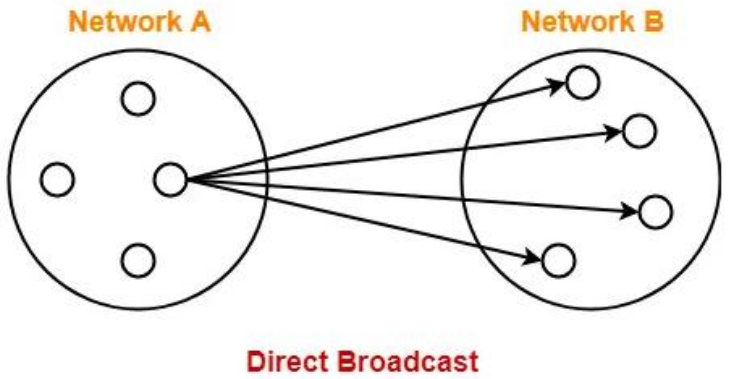
Example-

Host A having IP Address 11.1.2.3 sending data to all other hosts residing in the same network.

Here,
- Source Address = IP Address of host A = 11.1.2.3
- Destination Address = 255.255.255.255

B. Direct Broadcast-

- Transmitting data from one source host to all other hosts residing in some other network is called as **direct broadcast**.



NOTE

Direct Broadcast Address for any network is the IP Address where-

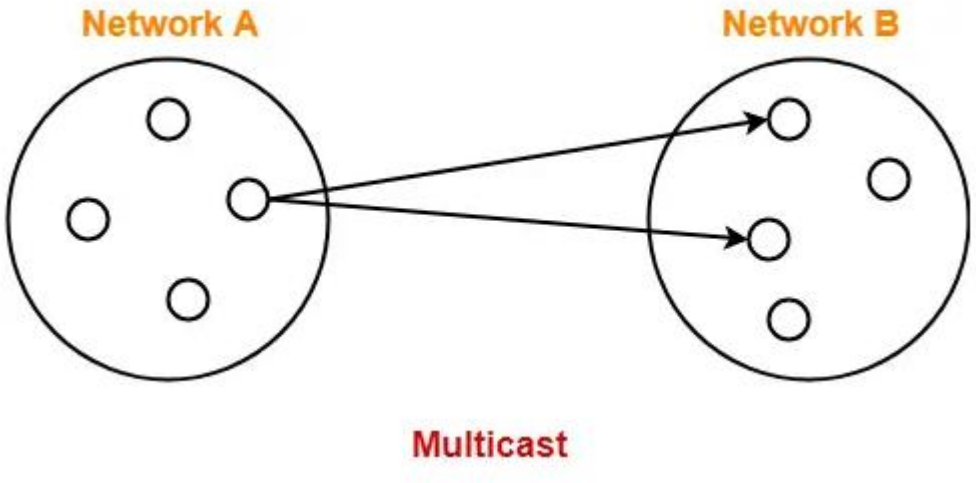
- Network ID is the IP Address of the network where all the destination hosts are present.
- Host ID bits are all set to 1.

Example-

- Host A having IP Address 11.1.2.3 sending data to all other hosts residing in the network having IP Address 20.0.0.0
- Here,
- Source Address = IP Address of host A = 11.1.2.3
- Destination Address = 20.255.255.255

3. Multicast-

- Transmitting data from one source host to a particular group of hosts having interest in receiving the data is called as **multicast**.
- It is a one to many transmission.



Examples-

•Sending a message to a particular group of people on whatsapp
•Sending an email to a particular group of people
•Video conference or teleconference

Basic internetworking (IP, CIDR, ARP, RARP, DHCP, ICMP),

IP Datagram Header Format

Unlike the post office, a router or computer cannot determine the size of a package without additional information.

A person can look at a letter or box and determine how big it is, but a router cannot. Therefore, additional information is required at the IP layer, in addition to the source and destination IP addresses.

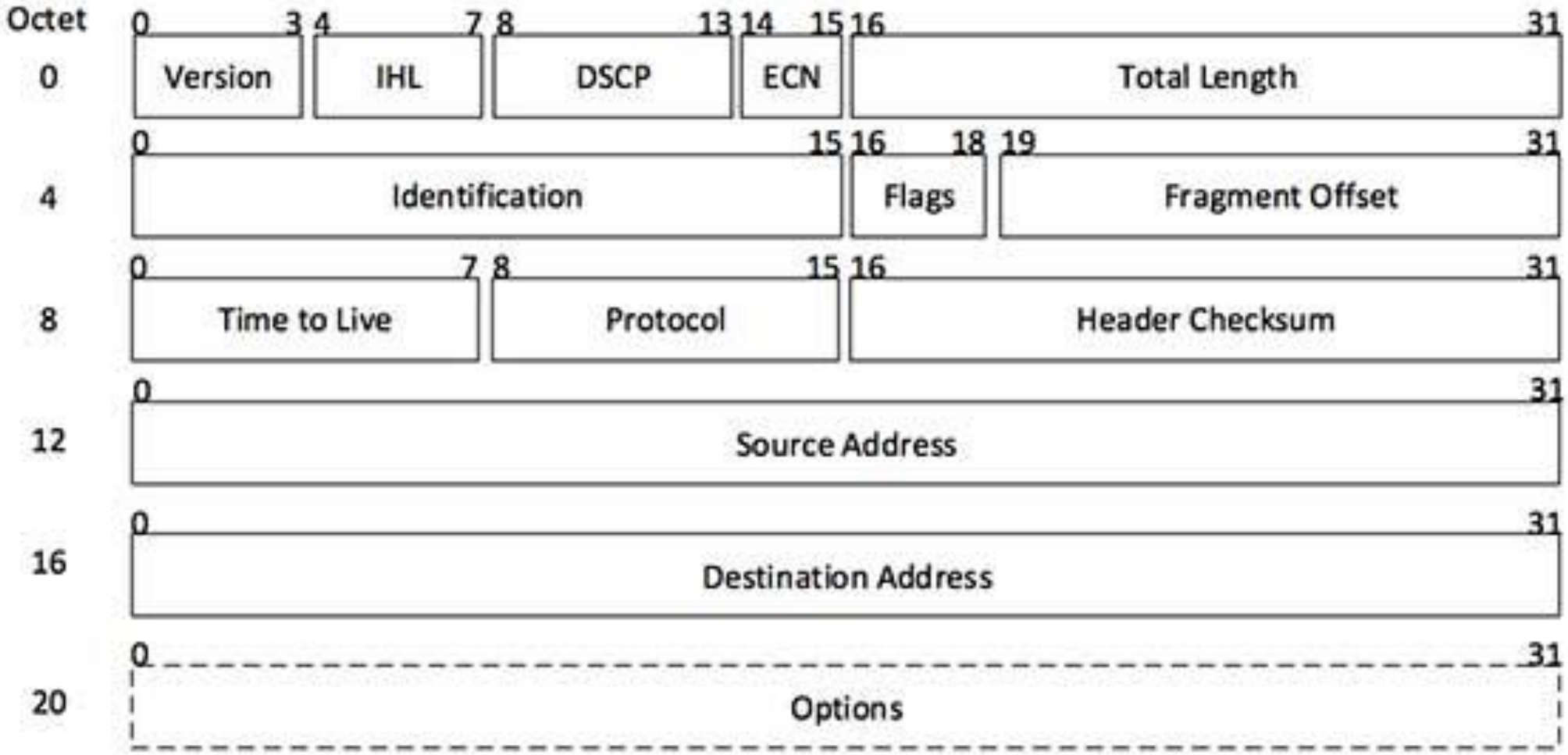
Figure on next slide is a logical representation of the information that is used at the IP layer to enable the delivery of electronic data.

This information is called a header, and is analogous to the addressing information on an envelope.

A header contains the information required to route data on the Internet, and has the same format regardless of the type of data being sent.

This is the same for an envelope where the address format is the same regardless of the type of letter being sent.

IP Datagram Header Format



[Image: IP Header]

IP header includes many relevant information including Version Number, which, in this context, is 4. Other details are as follows −

- **Version** − A 4-bit field that identifies the IP version being used. The current version is 4, and this version is referred to as IPv4.
- **IHL** − Internet Header Length; Length of entire IP header. A 4-bit field containing the length of the IP header in 32-bit increments. The minimum length of an IP header is 20 bytes, or five 32-bit increments. The maximum length of an IP header is 24 bytes, or six 32-bit increments. Therefore, the header length field should contain either 5 or 6.
- **DSCP** − Differentiated Services Code Point; this is Type of Service (ToS). A 6-bit field used to identify the level of service a packet receives in the network. DSCP is a 3-bit expansion of IP precedence with the elimination of the ToS bits.
- **ECN** − Explicit Congestion Notification; It carries information about the congestion seen in the route.
- **Total Length** − Length of entire IP Packet (including IP header and IP Payload). The size of the field is 16 bits.

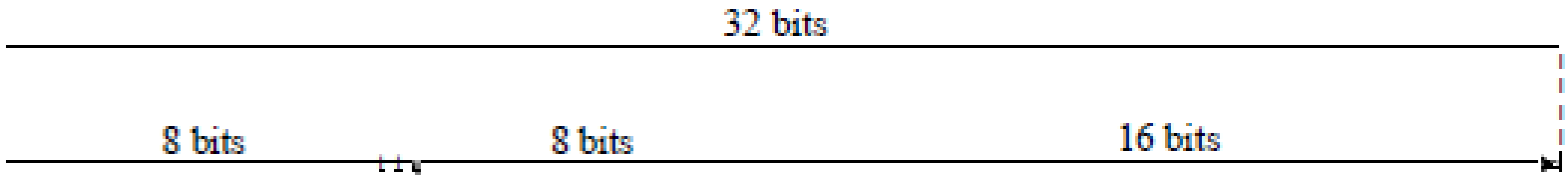
  Total length of the datagram = Length of the header + Length of the data
- **Identification** − If IP packet is fragmented during the transmission, all the fragments contain same identification number to identify original IP packet they belong to.
- **Flags** − As required by the network resources, if IP Packet is too large to handle, these ‘flags’ tells if they can be fragmented or not. In this 3-bit flag, the MSB is always set to ‘0’.
- **Fragment Offset** − This offset tells the exact position of the fragment in the original IP Packet.

- As an IP packet moves through the Internet, it might need to cross a route that cannot handle the size of the packet. The packet will be divided, or fragmented, into smaller packets and reassembled later. These fields are used to fragment and reassemble packets.
- **Time to Live** − To avoid looping in the network, every packet is sent with some TTL value set, which tells the network how many routers (hops) this packet can cross. At each hop, its value is decremented by one and when the value reaches zero, the packet is discarded.
- **Protocol** − Tells the Network layer at the destination host, to which Protocol this packet belongs to, i.e. the next level Protocol. For example protocol number of ICMP is 1, TCP is 6 and UDP is 17.
- **Header Checksum** − This field is used to keep checksum value of entire header which is then used to check if the packet is received error-free.
- **Source Address** − 32-bit address of the Sender (or source) of the packet.
- **Destination Address** − 32-bit address of the Receiver (or destination) of the packet.
- **Options** − This is optional field, which is used if the value of IHL is greater than 5. These options may contain values for options such as Security, Record Route, Time Stamp, etc.

Table 3.2 Values the Protocol Component Can Take

Value (Decimal)	Protocol
1	Internet Control Message Protocol (ICMP)
2	Internet Group Management Protocol (IGMP)
3	Gateway-to-Gateway Protocol (GGP)
4	Internet Protocol (IP)
6	Transmission Control Protocol (TCP)
8	Exterior Gateway Protocol (EGP)
9	Interior Gateway Protocol (IGP)
17	User Datagram Protocol (UDP)
41	Internet Protocol Version 6 (IPv6)
86	Dissimilar Gateway Protocol (DGP)
88	Interior Gateway Routing Protocol (IGRP)
89	Open Shortest Path First (OSPF)

Address Resolution Protocol (ARP)



Hardware Type		Protocol Type
Hardware length	Protocol length	Operation Request 1, Reply 2
Sender hardware address (For example, 6 bytes for Ethernet)		
Sender protocol address (For example, 4 bytes for IP)		
Target hardware address (For example, 6 bytes for Ethernet) (It is not filled in a request)		
Target protocol address (For example, 4 bytes for IP)		

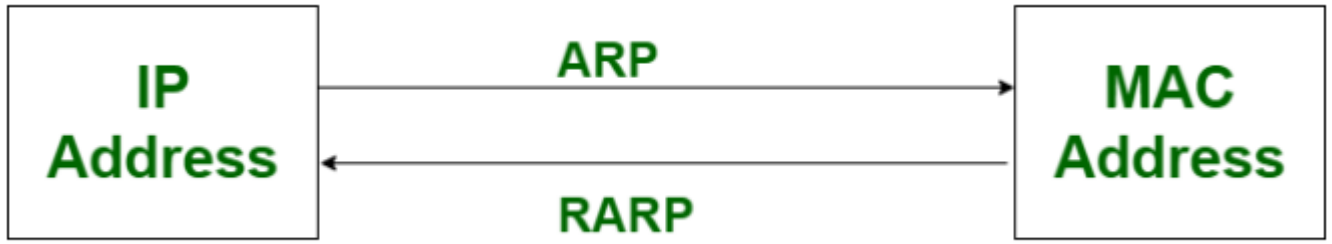
The fields are as follows:

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

- **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.
- **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 all 0s because the sender does not know the physical address of the target.
- **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.

Difference between ARP and RARP

- In **Address Resolution Protocol (ARP)**, Receiver's MAC address is fetched. Through ARP, (32-bit) IP address mapped into (48-bit) MAC address. Whereas, In **Reverse Address Resolution Protocol (RARP)**, IP address is fetched through server. Through RARP, (48-bit) MAC address of 48 bits mapped into (32-bit) IP address.



ARP	RARP
A protocol used to map an IP address to a physical (MAC) address	A protocol used to map a physical (MAC) address to an IP address
To obtain the MAC address of a network device when only its IP address is known	To obtain the IP address of a network device when only its MAC address is known
Client broadcasts its IP address and requests a MAC address, and the server responds with the corresponding MAC address	Client broadcasts its MAC address and requests an IP address, and the server responds with the corresponding IP address
IP addresses	MAC addresses
Widely used in modern networks to resolve IP addresses to MAC addresses	Rarely used in modern networks as most devices have a pre-assigned IP address
ARP stands for Address Resolution Protocol.	Whereas RARP stands for Reverse Address Resolution Protocol.
Through ARP, (32-bit) IP address mapped into (48-bit) MAC address.	Whereas through RARP, (48-bit) MAC address of 48 bits mapped into (32-bit) IP address.
In ARP, broadcast MAC address is used.	While in RARP, broadcast IP address is used.
In ARP, ARP table is managed or maintained by local host.	While in RARP, RARP table is managed or maintained by RARP server.
In Address Resolution Protocol, Receiver's MAC address is fetched.	While in RARP, IP address is fetched.
In ARP, ARP table uses ARP reply for its updation.	While in RARP, RARP table uses RARP reply for configuration of IP addresses .
Hosts and routers uses ARP for knowing the MAC address of other hosts and routers in the networks.	While RARP is used by small users having less facilities.
ARP is used in sender's side to map the receiver's MAC address.	RARP is used in receiver's side to map the sender's IP.