Network Layer Protocols

TCP/IP supports the following protocols:

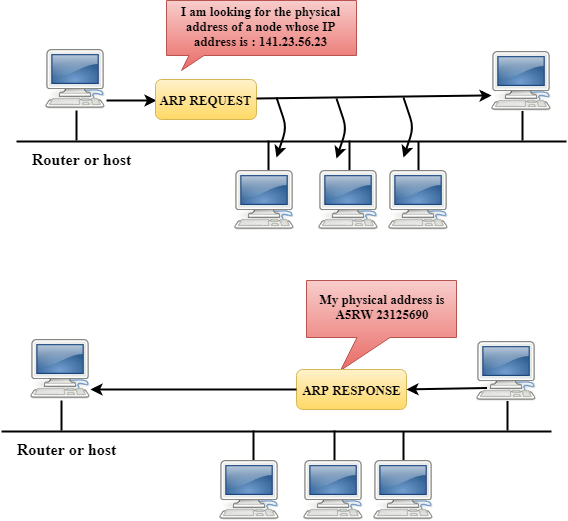
ARP

* ARP stands for Address Resolution Protocol.
* It is used to associate an IP address with the MAC address.
* Each device on the network is recognized by the MAC address imprinted on the NIC. Therefore, we can say that devices need the MAC address for communication on a local area network. MAC address can be changed easily. For example, if the NIC on a particular machine fails, the MAC address changes but IP address does not change. ARP is used to find the MAC address of the node when an internet address is known.

Note: MAC address: The MAC address is used to identify the actual device.  
IP address: It is an address used to locate a device on the network.

How ARP works

If the host wants to know the physical address of another host on its network, then it sends an ARP query packet that includes the IP address and broadcast it over the network. Every host on the network receives and processes the ARP packet, but only the intended recipient recognizes the IP address and sends back the physical address. The host holding the datagram adds the physical address to the cache memory and to the datagram header, then sends back to the sender.



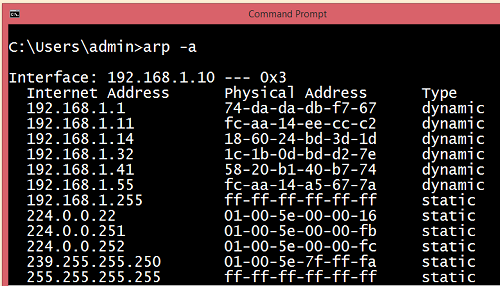
Steps taken by ARP protocol

If a device wants to communicate with another device, the following steps are taken by the device:

* The device will first look at its internet list, called the ARP cache to check whether an IP address contains a matching MAC address or not. It will check the ARP cache in command prompt by using a command **arp-a**.



* If ARP cache is empty, then device broadcast the message to the entire network asking each device for a matching MAC address.
* The device that has the matching IP address will then respond back to the sender with its MAC address
* Once the MAC address is received by the device, then the communication can take place between two devices.
* If the device receives the MAC address, then the MAC address gets stored in the ARP cache. We can check the ARP cache in command prompt by using a command arp -a.



Note: ARP cache is used to make a network more efficient.

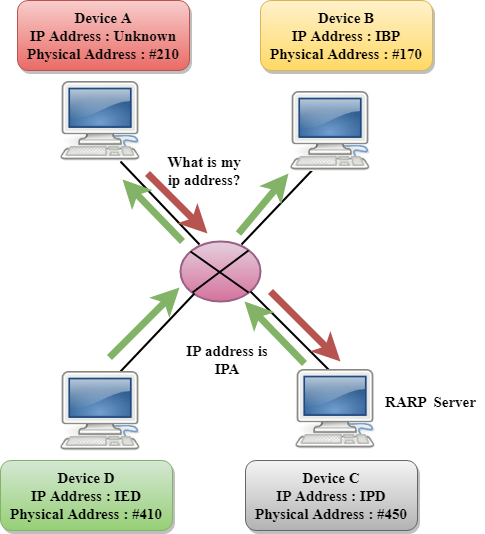
In the above screenshot, we observe the association of IP address to the MAC address.

There are two types of ARP entries:

* **Dynamic entry:** It is an entry which is created automatically when the sender broadcast its message to the entire network. Dynamic entries are not permanent, and they are removed periodically.
* **Static entry:** It is an entry where someone manually enters the IP to MAC address association by using the ARP command utility.

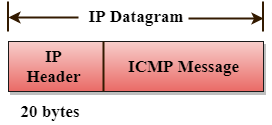
RARP

* RARP stands for **Reverse Address Resolution Protocol**.
* If the host wants to know its IP address, then it broadcast the RARP query packet that contains its physical address to the entire network. A RARP server on the network recognizes the RARP packet and responds back with the host IP address.
* The protocol which is used to obtain the IP address from a server is known as **Reverse Address Resolution Protocol**.
* The message format of the RARP protocol is similar to the ARP protocol.
* Like ARP frame, RARP frame is sent from one machine to another encapsulated in the data portion of a frame.

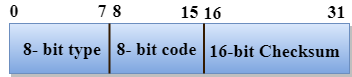


ICMP

* ICMP stands for Internet Control Message Protocol.
* The ICMP is a network layer protocol used by hosts and routers to send the notifications of IP datagram problems back to the sender.
* ICMP uses echo test/reply to check whether the destination is reachable and responding.
* ICMP handles both control and error messages, but its main function is to report the error but not to correct them.
* An IP datagram contains the addresses of both source and destination, but it does not know the address of the previous router through which it has been passed. Due to this reason, ICMP can only send the messages to the source, but not to the immediate routers.
* ICMP protocol communicates the error messages to the sender. ICMP messages cause the errors to be returned back to the user processes.
* ICMP messages are transmitted within IP datagram.



The Format of an ICMP message



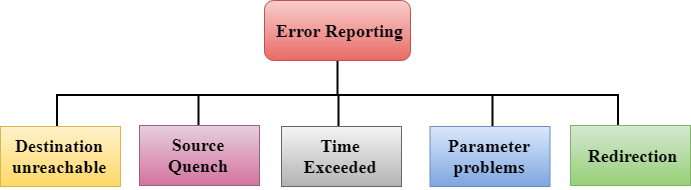
* The first field specifies the type of the message.
* The second field specifies the reason for a particular message type.
* The checksum field covers the entire ICMP message.

Error Reporting

ICMP protocol reports the error messages to the sender.

**Five types of errors are handled by the ICMP protocol:**

* Destination unreachable
* Source Quench
* Time Exceeded
* Parameter problems
* Redirection



* **Destination unreachable:** The message of "Destination Unreachable" is sent from receiver to the sender when destination cannot be reached, or packet is discarded when the destination is not reachable.
* **Source Quench:** The purpose of the source quench message is congestion control. The message sent from the congested router to the source host to reduce the transmission rate. ICMP will take the IP of the discarded packet and then add the source quench message to the IP datagram to inform the source host to reduce its transmission rate. The source host will reduce the transmission rate so that the router will be free from congestion.
* **Time Exceeded:** Time Exceeded is also known as "Time-To-Live". It is a parameter that defines how long a packet should live before it would be discarded.

**There are two ways when Time Exceeded message can be generated:**

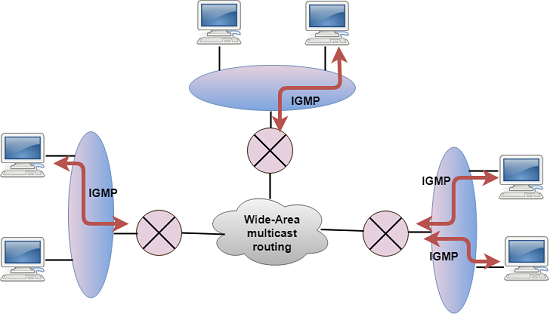
Sometimes packet discarded due to some bad routing implementation, and this causes the looping issue and network congestion. Due to the looping issue, the value of TTL keeps on decrementing, and when it reaches zero, the router discards the datagram. However, when the datagram is discarded by the router, the time exceeded message will be sent by the router to the source host.

When destination host does not receive all the fragments in a certain time limit, then the received fragments are also discarded, and the destination host sends time Exceeded message to the source host.

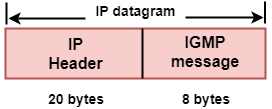
* **Parameter problems:** When a router or host discovers any missing value in the IP datagram, the router discards the datagram, and the "parameter problem" message is sent back to the source host.
* **Redirection:** Redirection message is generated when host consists of a small routing table. When the host consists of a limited number of entries due to which it sends the datagram to a wrong router. The router that receives a datagram will forward a datagram to a correct router and also sends the "Redirection message" to the host to update its routing table.

IGMP

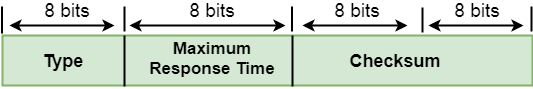
* IGMP stands for **Internet Group Message Protocol**.
* The IP protocol supports two types of communication:
  + **Unicasting:** It is a communication between one sender and one receiver. Therefore, we can say that it is one-to-one communication.
  + **Multicasting:** Sometimes the sender wants to send the same message to a large number of receivers simultaneously. This process is known as multicasting which has one-to-many communication.
* The IGMP protocol is used by the hosts and router to support multicasting.
* The IGMP protocol is used by the hosts and router to identify the hosts in a LAN that are the members of a group.



* IGMP is a part of the IP layer, and IGMP has a fixed-size message.
* The IGMP message is encapsulated within an IP datagram.



The Format of IGMP message



**Where**,

**Type:** It determines the type of IGMP message. There are three types of IGMP message: Membership Query, Membership Report and Leave Report.

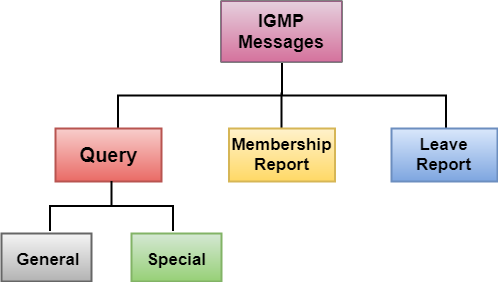
**Maximum Response Time:** This field is used only by the Membership Query message. It determines the maximum time the host can send the Membership Report message in response to the Membership Query message.

**Checksum:** It determines the entire payload of the IP datagram in which IGMP message is encapsulated.

**Group Address:** The behavior of this field depends on the type of the message sent.

* **For Membership Query**, the group address is set to zero for General Query and set to multicast group address for a specific query.
* **For Membership Report**, the group address is set to the multicast group address.
* **For Leave Group**, it is set to the multicast group address.

IGMP Messages



* **Membership Query message**
  + This message is sent by a router to all hosts on a local area network to determine the set of all the multicast groups that have been joined by the host.
  + It also determines whether a specific multicast group has been joined by the hosts on a attached interface.
  + The group address in the query is zero since the router expects one response from a host for every group that contains one or more members on that host.
* **Membership Report message**
  + The host responds to the membership query message with a membership report message.
  + Membership report messages can also be generated by the host when a host wants to join the multicast group without waiting for a membership query message from the router.
  + Membership report messages are received by a router as well as all the hosts on an attached interface.
  + Each membership report message includes the multicast address of a single group that the host wants to join.
  + IGMP protocol does not care which host has joined the group or how many hosts are present in a single group. It only cares whether one or more attached hosts belong to a single multicast group.
  + The membership Query message sent by a router also includes a "**Maximum Response time**". After receiving a membership query message and before sending the membership report message, the host waits for the random amount of time from 0 to the maximum response time. If a host observes that some other attached host has sent the "**Maximum Report message**", then it discards its "**Maximum Report message**" as it knows that the attached router already knows that one or more hosts have joined a single multicast group. This process is known as feedback suppression. It provides the performance optimization, thus avoiding the unnecessary transmission of a "**Membership Report message**".
* **Leave Report**  
  When the host does not send the "Membership Report message", it means that the host has left the group. The host knows that there are no members in the group, so even when it receives the next query, it would not report the group.