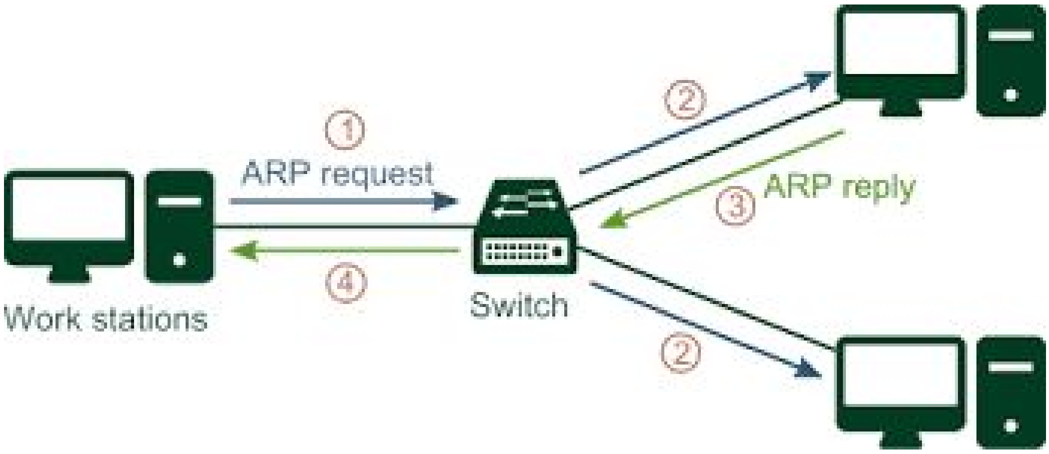
CN LAB 7

U18CO021: SAHIL BONDRE

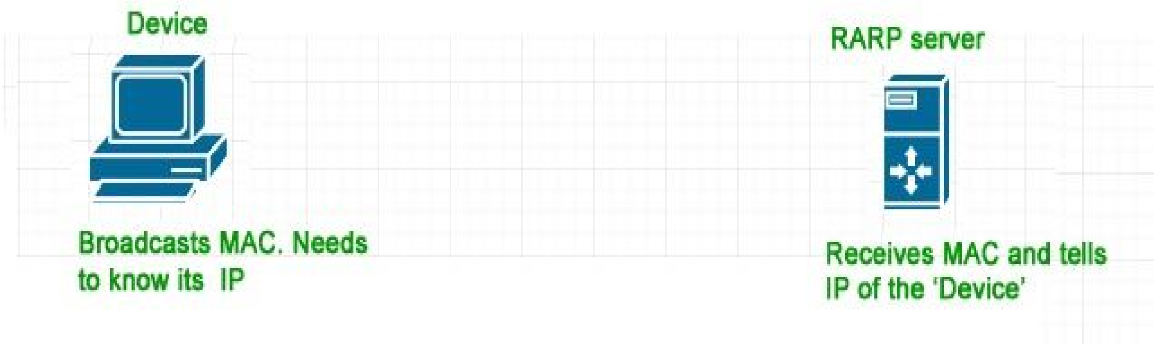
ARP (Address Resolution Protocol)



Address Resolution Protocol is a communication protocol adopted to identify the physical address linked with a given network address. It is a network-layer to the data-link-layer mapping process. It is used to find the MAC address for a given IP Address. In order to transfer the data to the destination, having an IP address is necessary but not sufficient; we also require the physical address of the destination machine. ARP gets the physical address (MAC address) of the destination machine.

Before transferring the IP packet, the MAC address of the destination must be known. If not so, then the sender broadcasts the ARP-discovery packet requesting the MAC address of the proposed destination. Since ARP-discovery is a broadcast, every host inside that network will get this message. However, the packet will be rejected by everyone except that intended receiver host whose IP is associated. Now, this receiver will send a unicast packet with its MAC address (ARP-reply) to the sender of ARP-discovery packet. After the initial sender receives the ARP-reply, it updates ARP-cache and starts sending a unicast message to the destination.

RARP (Reverse Address Resolution Protocol)

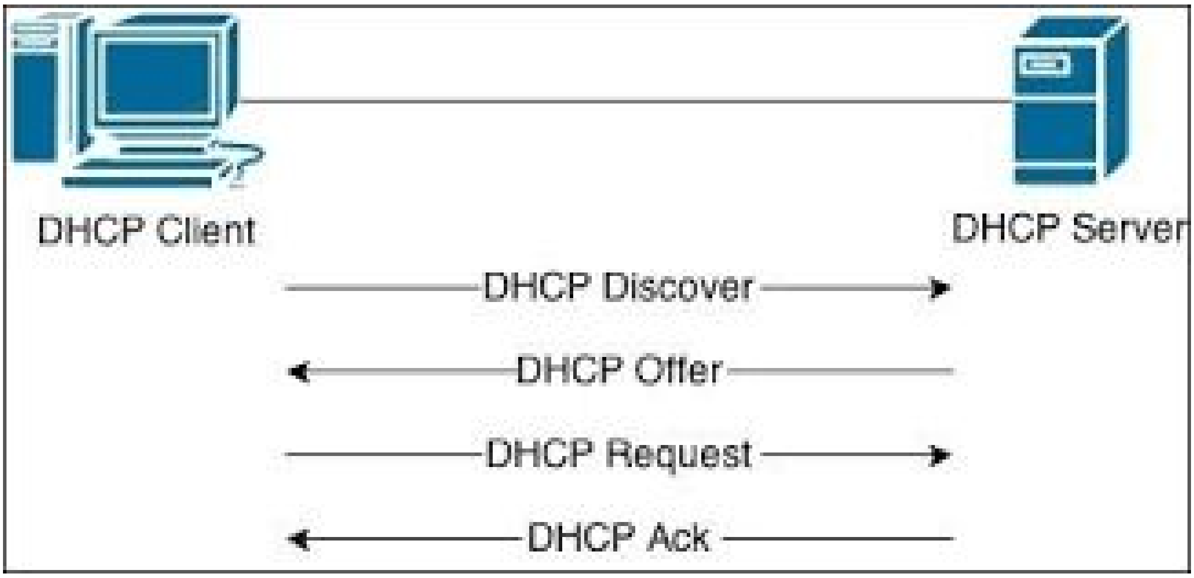

Device
Broadcasts MAC. Needs to know its IP
RARP server
Receives MAC and tells IP of the 'Device'

Reverse ARP is a networking protocol utilised by the client in a LAN to request its IPv4 address from the gateway router's ARP table. The network administrator generates a table in the gateway-router, which is used to map the MAC address to the corresponding IP address.

When a new device is set up or any machine which does not have the memory to store the IP address, needs an IP address for its use. So the device sends a RARP broadcast packet which contains its own MAC address in both sender and receiver hardware address field.

A particular host configured inside the local area network, called as RARP-server is responsible for replying for these kinds of broadcast packets. The RARP server attempts to find out the entry in IP to MAC address mapping table. If any entry matches in the table, the RARP server sends the response packet to the requesting device along with the IP address.

DHCP (Dynamic Host Configuration Protocol)



It is a network protocol used on IP networks where a DHCP server automatically assigns an IP address and other information to each host on the network so they can communicate efficiently with other endpoints - In addition to the IP address, DHCP also assigns the subnet mask, default gateway address, the domain name server (DNS) address and other pertinent configuration parameters.

Components:

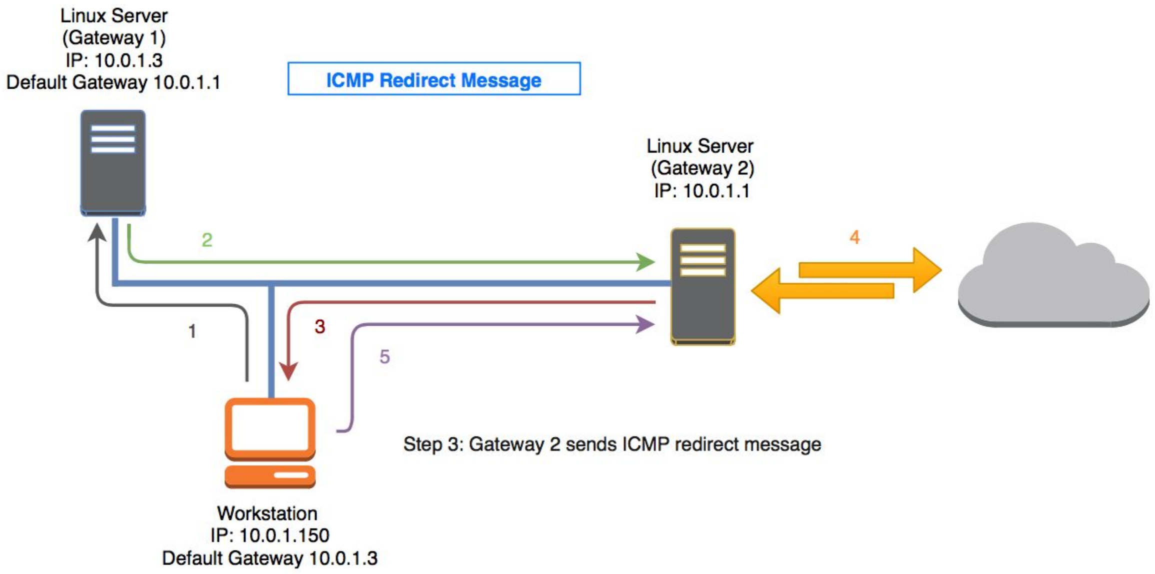
1. **DHCP Server** A networked device is running the DHCP service that holds IP addresses and related configuration information.
2. **DHCP Client** The endpoint that receives configuration information from a DHCP server.
3. **IP Address Pool** The range of addresses that are available to DHCP clients.
4. **Subnet** IP networks can be partitioned into segments known as subnets. Subnets help keep networks manageable.
5. **Lease** The length of time for which a DHCP client holds the IP address information. When a lease expires, the client must renew it.
6. **DHCP relay** A router or host that listens for client messages being broadcast on that network and then forwards them to a configured server. The server then sends responses back to the relay agent that passes them along to the client.

This can be used to centralize DHCP servers instead of having a server on each subnet.

Benefits

1. Accurate IP configuration
2. Reduced IP address conflicts
3. Automation of IP address administration
4. Efficient change management

ICMP (Internet Control Message Protocol)



It is a network layer protocol used by network devices to diagnose network communication issues. ICMP is mainly used to determine whether or not data is reaching its intended destination in a timely manner. ICMP is crucial for error reporting and testing

How does it work?

- ICMP is not associated with a transport layer protocol such as TCP or UDP. This makes.
- ICMP a connectionless protocol: one device does not need to open a connection with another device before sending an ICMP message
- ICMP does not open a connection in this way. The ICMP protocol also does not allow for targeting a specific port on a device

How is it used in DDoS attacks?

1. ICMP Flood Attack

- A ping flood or ICMP flood is when the attacker attempts to overwhelm a targeted device with ICMP echo-request packets
- The target has to process and respond to each packet, consuming its computing resources until legitimate users cannot receive service

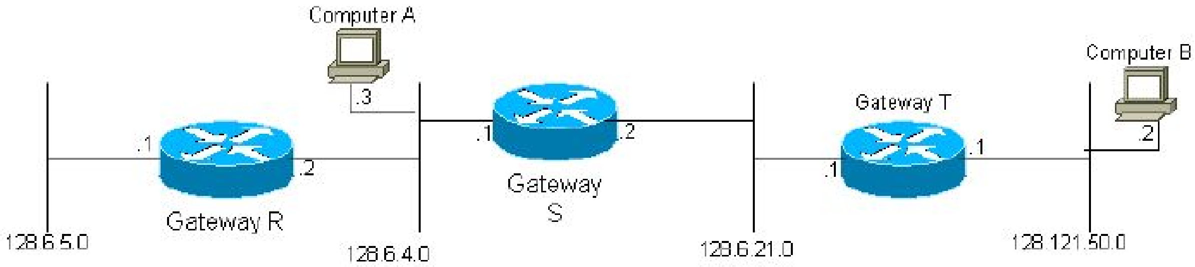
2. Ping of death Attack

- A ping of death attack is when the attacker sends a ping larger than the maximum allowable size for a packet to a targeted machine, causing the machine to freeze or crash
- The packet gets fragmented on the way to its target, but when the target reassembles the packet into its original maximum-exceeding size, the size of the packet causes a buffer overflow

3. Smurf Attack

- The attacker sends an ICMP packet with a spoofed source IP address
- Networking equipment replies to the packet, sending the replies to the spoofed IP and flooding the victim with unwanted ICMP packets

IGRP (Internet Group Management Protocol)



IGMP is used by IP hosts to register their dynamic multicast group membership. It is also used by connected routers to discover these group members.

Membership report

- Host or a router can join a group
- A host maintains a list of processes that have membership in a group
- When a process wants to join a new group, it sends its request to the host The host then adds the name of the process and the name of the requested group to its list, and sends the membership report to the router.

Leave report

- When a host sees that no process is interested in a specific group G, it sends a leave report. If router receives a leave report it won't purge the list if there are still other hosts interested in that group
- For that purpose the router sends a special query message with a specified response time for the group in question to see if there is anyone interested in that group. If there is no response to a membership report, it purges the list.

General Query Message

- Membership report and leave report are not enough to maintain the membership information.
- **Example:** a host that is a member of a group can shut down and the m/c router would never receive the leave report. Therefore the m/c router monitors the hosts and routers in LAN by periodically sending (by default every 125 sec)

general query message. Hosts/routers respond by membership report if there is still interest in groups

Delayed Response

- In order to keep the traffic low the response to general query message must be done by only one host for a given group.
- How can be made sure that only one host answers the query, while the others which have to report the same group, or groups are not? This is achieved with delayed response: When a host receives general query message it delays the response: it sets a timer for each group to a different random value between 0 and 10 seconds, then broadcasts the response(s) according to the timers.
- If the host receives a response from another host, whose timer for that group has expired earlier, the host cancels the corresponding timer and doesn’t send the duplicate response for the group.
- Only one router on the LAN is designated for sending the query messages – the query router. This further reduces the traffic.