ARP, RARP
DHCP

ARP - Address Resolution Protocol

- ARP (Address Resolution Protocol) is a network protocol used to determine the MAC address (hardware address) corresponding to an IP address.
- When one device in a LAN (Local Area Network) wants to communicate with another, it must know the destination's MAC address.
- Since users and applications work with IP addresses, ARP acts as the translator, converting IP addresses into MAC addresses.
- ***Note:*** *ARP works at the Network Layer (Layer 3) but interacts closely with the Data Link Layer (Layer 2).*

Important ARP Terms

- **ARP Cache**: A table where resolved MAC addresses are stored for quick future use.
- **ARP Cache Timeout**: The duration for which an entry remains valid in the ARP cache.
- **ARP Request**: A broadcast message asking, "Who has this IP address?”
- **ARP Reply/Response**: A unicast message containing the MAC address of the requested IP.

Types of ARP

1. Proxy ARP - allows a proxy device (like a router) to respond to ARP requests on behalf of another device. Useful for hiding network complexity or connecting different subnets.

2. Gratuitous ARP - A host sends an ARP request for its own IP address. Used to detect duplicate IP addresses and update ARP tables on other devices.

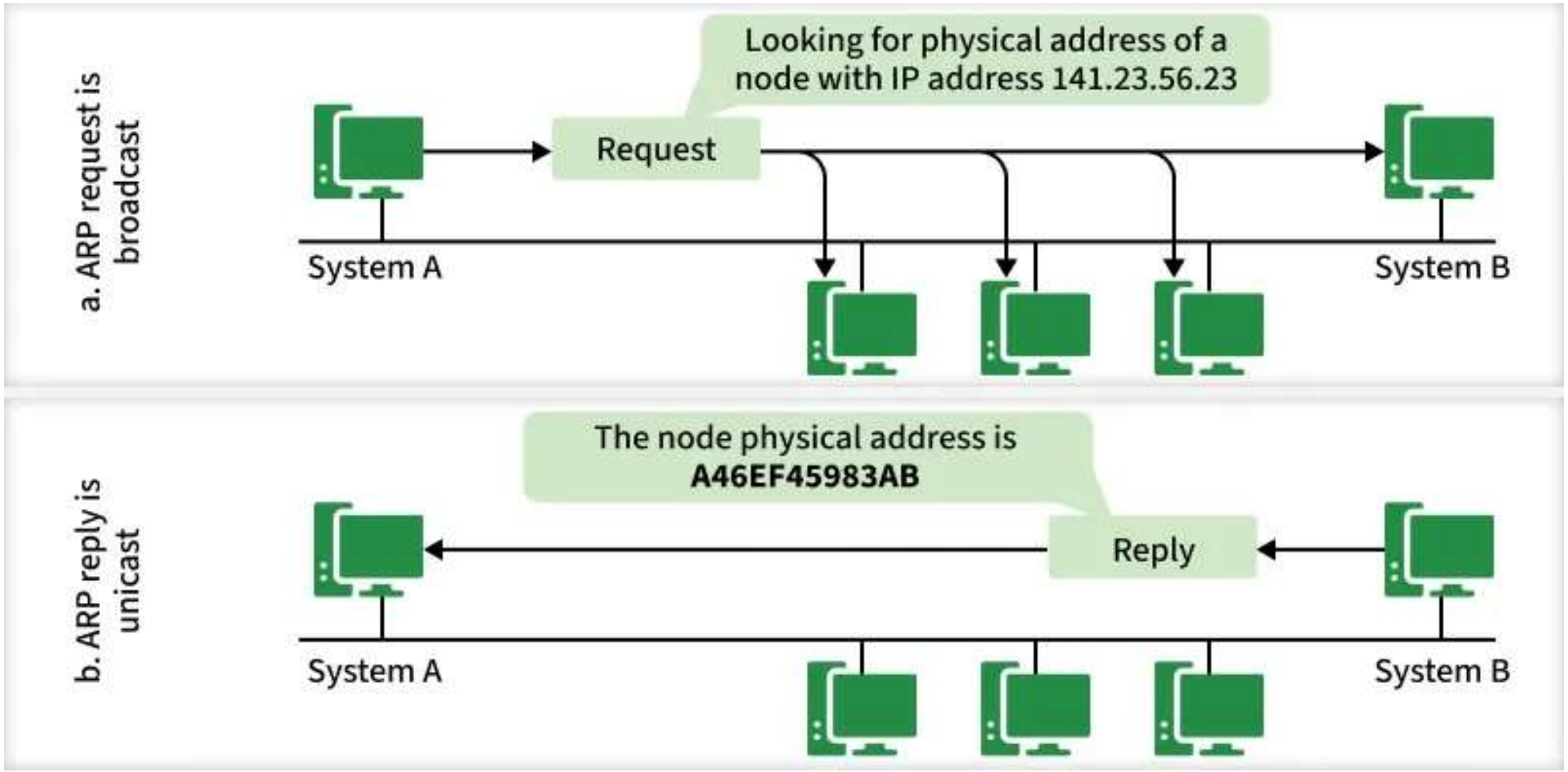
3. Reverse ARP (RARP) - Used by a device to discover its own IP address when it only knows its MAC address. Example: Diskless computers at boot time request their IP from a server.

4. Inverse ARP (InARP) - Opposite of ARP - used to discover the IP address from a known MAC address. Common in technologies like Frame Relay and ATM networks.

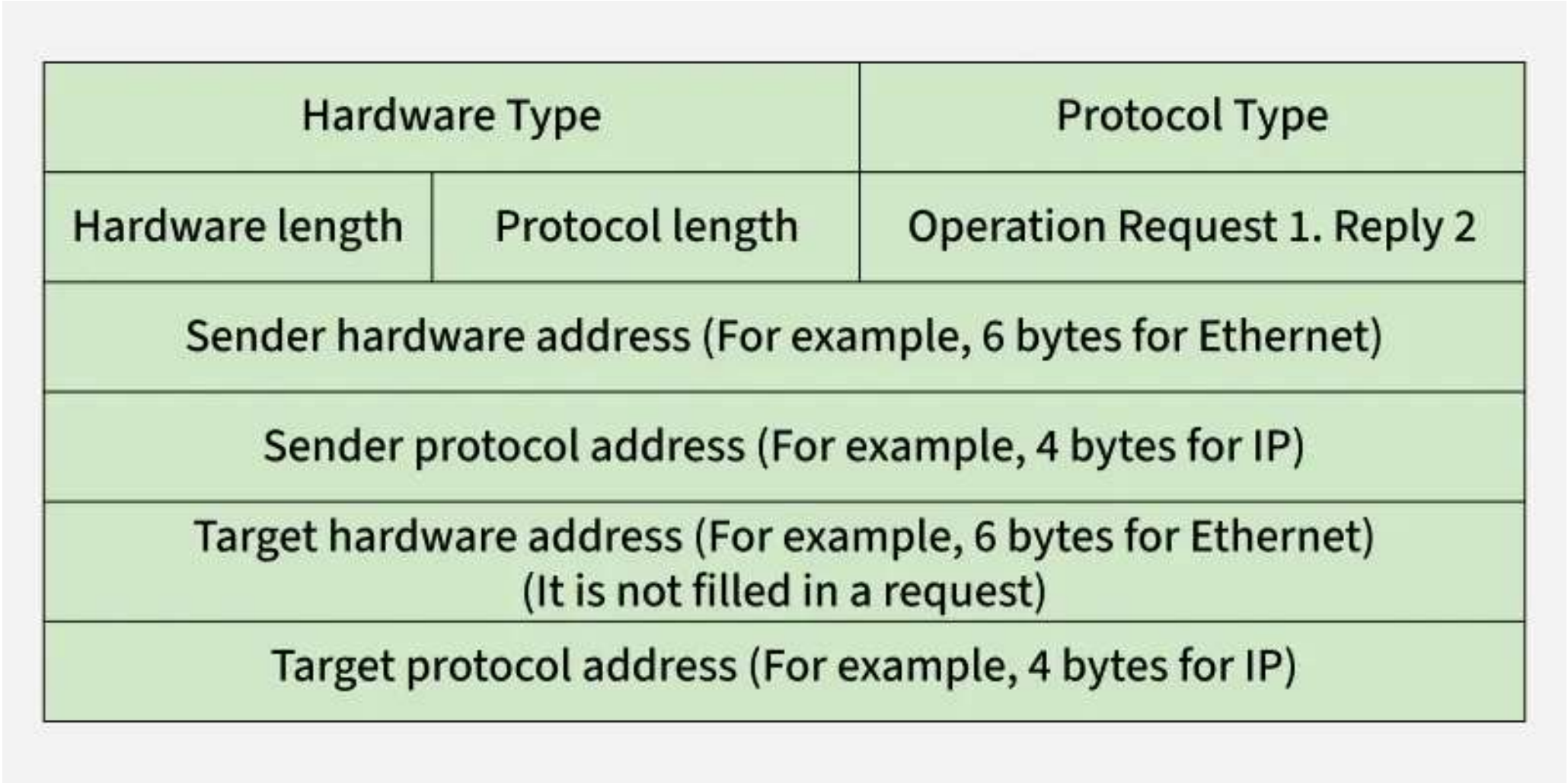
How ARP Works

- The following steps are involved
- **Sender checks ARP Cache:** If the MAC address for the destination IP is already cached, communication starts immediately.
- **ARP Request Broadcast**: If not cached, the sender broadcasts an ARP request on the LAN.
- **All Devices Receive Request**: Each device checks whether the requested IP matches its own.
- **Destination Replies**: The device with the matching IP sends an ARP reply (unicast) containing its MAC address.
- **Cache Update**: The sender updates its ARP cache with the new MAC address for future use.

How ARP Works (cont.)



ARP Message Format



ARP Message Format

- An ARP message consists of several fields:
- **Hardware Type (2 bytes):** Defines hardware (Ethernet = 1).
- **Protocol Type (2 bytes):** Defines protocol (IPv4 = 0x0800).
- **Hardware Address Length (1 byte):** Length of MAC address (6 for Ethernet).
- **Protocol Address Length (1 byte):** Length of IP address (4 for IPv4).
- **Operation Code (2 bytes):** 1 for request, 2 for reply.
- **Sender Hardware Address:** MAC of the sender.
- **Sender Protocol Address:** IP of the sender.
- **Target Hardware Address:** Empty in request; receiver's MAC in reply.
- **Target Protocol Address:** Receiver's IP.

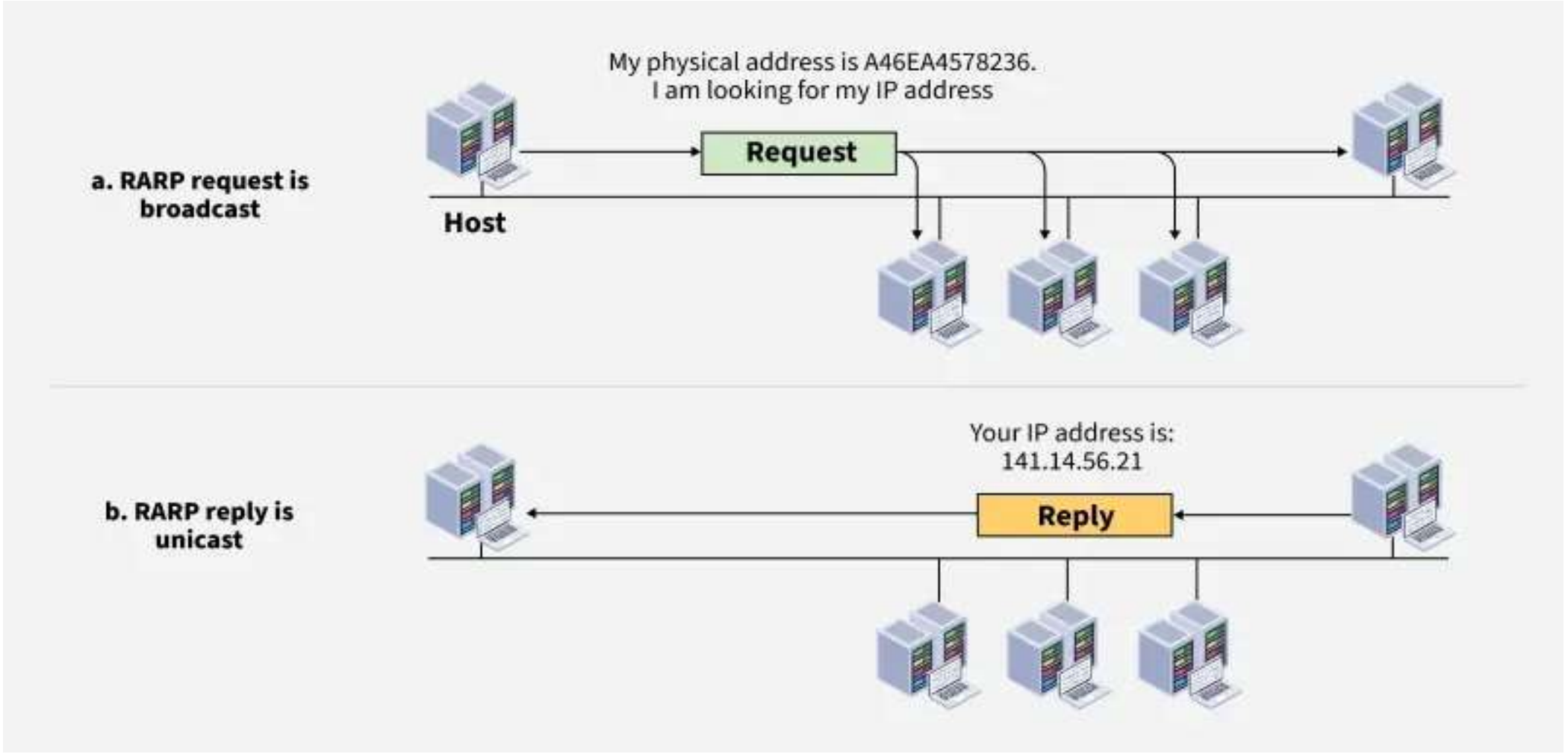
Advantages of ARP Protocol

- **Automatic Mapping:** No need for manual configuration to resolve MAC addresses.
- **Efficiency:** Ensures smooth communication within LANs.
- **Transparency:** Works in the background without user intervention.
- **Flexibility:** Supports different types (Proxy, Gratuitous, Reverse, Inverse) for varied networking needs.

RARP-Reverse Address Resolution Protocol

- Reverse Address Resolution Protocol (RARP) is a network protocol that allows a device to discover its IP address when only its MAC (Media Access Control) address is known. Components are-
- **IP Address Assignment:** Normally, a machine stores its IP address in a configuration file. Diskless systems cannot do this and rely on RARP for IP assignment.
- **Physical Address:** Every network device has a unique MAC address, stored in its Network Interface Card (NIC).
- **RARP Request**: A device broadcasts a request containing its MAC address to ask for the corresponding IP address.
- **RARP Server:** The server maintains a mapping of MAC addresses to IP addresses. On receiving a request, it replies with the correct IP address.

RARP


My physical address is A46EA4578236.
I am looking for my IP address
Request
Host
a. RARP request is broadcast
Your IP address is:
141.14.56.21
Reply
b. RARP reply is unicast

How it works

- When a machine doesn't have the memory to store its IP address, such as diskless machines or newly configured systems, it uses RARP to request an IP address.
- **RARP Request**: A client broadcasts a RARP request containing its MAC address.
- **Server Lookup**: A RARP server (or gateway router with ARP table) checks its mapping of MAC -> IP.
- **RARP Reply**: If a match is found, the server responds with the client’s IP address.
- **Client Configuration**: The client configures itself with the provided IP and can now communicate on the network.

RARP Packet Format & Encapsulation

RARP Packet Format

Hardware Type		Protocol Type
Hardware length	Protocol length	Operation Request 3. Reply 4
Sender hardware address	(For example, 6 bytes for Ethernet)	
Sender protocol address	(For example, 4 bytes for IP) (It is not filled for request)	
Target hardware address	(For example, 6 bytes for Ethernet) (It is not filled for request)	
Target protocol address	(For example, 4 bytes for IP) (It is not filled for request)	

Exactly the same as ARP

Encapsulation: RARP packets are encapsulated directly into data-link layer frames (e.g., Ethernet frames) so they can be transmitted over the LAN.

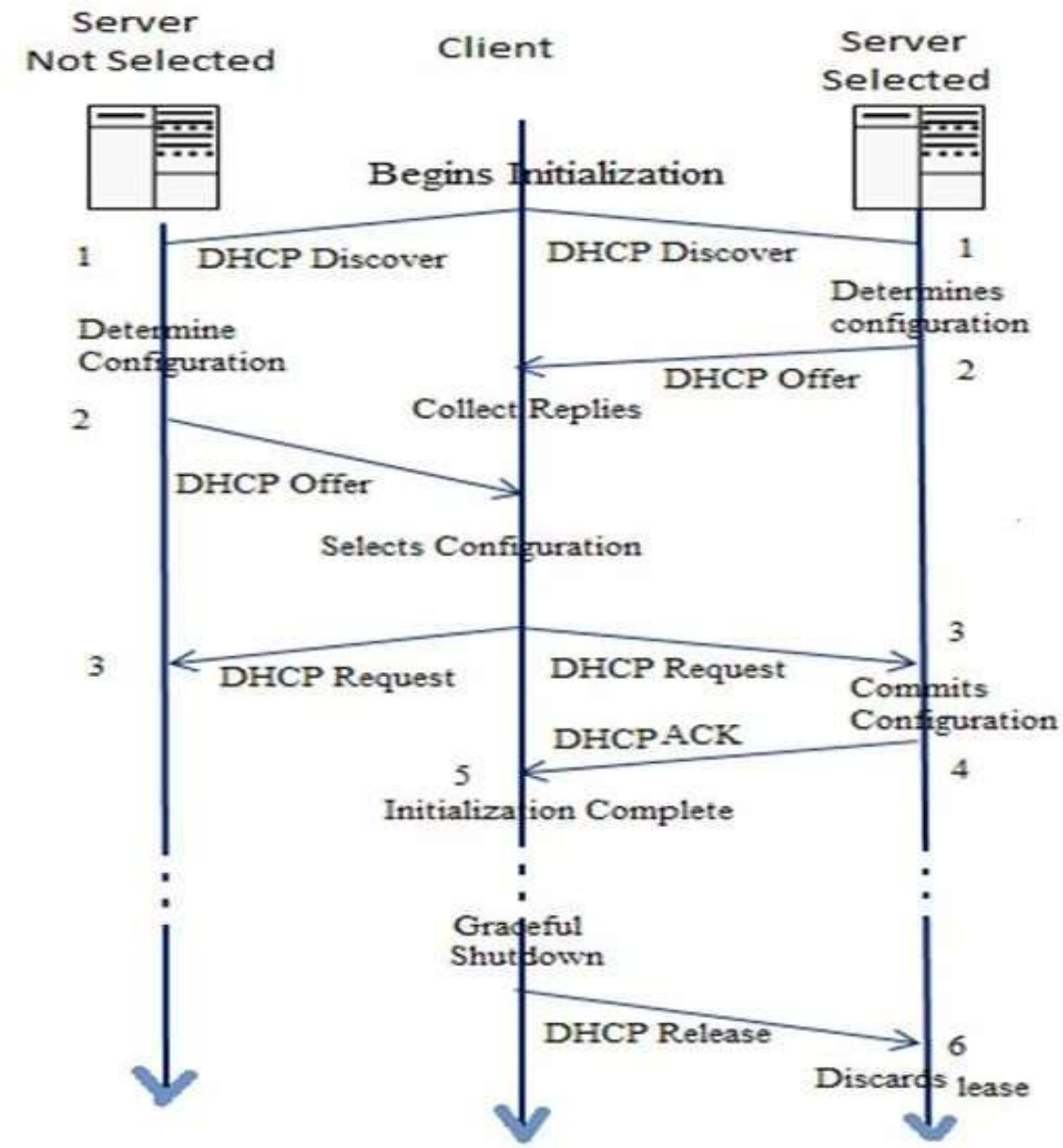
Dynamic Host Configuration Protocol (DHCP)

- Dynamic Host Configuration Protocol (DHCP) is a network protocol used to automate the process of assigning IP addresses and other network configuration parameters to devices such as computers, smartphones and printers. Instead of manually configuring each device, DHCP enables devices to join a network and automatically receive:
- IP Address
- Subnet Mask
- Default Gateway
- DNS Server addresses
- Other TCP/IP configuration options

Components of DHCP

- **DHCP Server:** Stores IP addresses and configuration details. Allocates addresses dynamically to clients.
- **DHCP Relay**: Acts as a bridge between clients and servers when they are not on the same subnet.
- **DHCP Client**: A device (PC, phone, printer, etc.) that requests and receives network configuration from the DHCP server.
- **IP Address Pool**: A predefined range of IP addresses that the DHCP server can lease to devices.
- **Subnets**: Logical partitions of an IP network to organize and manage IP allocation.
- **Lease**: The time period for which an IP address is assigned to a client. After expiry, the client must renew or request a new lease.
- **DNS Servers**: DHCP can provide DNS server information to clients for resolving domain names.
- **Default Gateway**: The gateway router information is provided to clients so they can communicate outside their subnet.
- **Options**: Additional parameters like subnet mask, domain name and time servers.

Working of DHCP



DHCP (cont.)

- DHCP operates on the Application Layer using UDP ports 67 (server) and 68 (client). It follows a client-server model. The client and server primarily exchange four key messages—a process called DORA (Discover, Offer, Request, Acknowledge). In DHCP, the client and the server exchange DHCP messages to establish a connection. However, DHCP defines following messages:

1. **DHCP Discover Message:**

- It is the first message produced by a client in the communication process between the client and server with the target address 255.255.255.255 and the source address 0.0.0.0.
- This message is produced by the client host to discover if there are any DHCP servers present in a network or not.
- The message might contain other requests like subnet mask, domain name server, and domain name, etc.
- The message is broadcast to all the devices in a network to find the DHCP server.

2. DHCP Offers A Message

- The DHCP server will reply/respond to the host in this message, specifying the unleashed IP address and other TCP configuration information.
- This message is broadcasted by the server.
- If there are more than one DHCP servers present in the network, then the client host accepts the first DHCP OFFER message it receives.
- Also, a server ID is specified in the packet to identify the server.

3. DHCP Request Message – Client Accepts DHCP Server Offer

- The Client receives the DHCP offer message from the DHCP server that replied/responded to the DHCP discover message.
- After receiving the offer message, the client will compare the offer that is requested, and then select the server it wants to use.
- The client sends the DHCP Request message to accept the offer, showing which server is selected.
- Then this message is broadcast to the entire network to let all the DHCP servers know which server was selected.

4. DHCP Acknowledgment Message – DHCP server acknowledges the client and leases the IP address.

- If a server receives a DHCP Request message, the server marks the address as leased.
- Servers that are not selected will return the offered addresses to their available pool.
- Now, the selected server sends the client an acknowledgment (DHCP ASK), which contains additional configuration information.
- The client may use the IP address and configuration parameters. It will use these settings till its lease expires or till the client sends a DHCP Release message to the server to end the lease.

5. DHCP Request, DHCP ACK Message – Client attempts to renew the lease

- The client starts to renew a lease when half of the lease time has passed.
- The client requests the renewal by sending a DHCP Request message to the server.
- If the server accepts the request, it will send a DHC ACK message back to the client.
- If the server does not respond to the request, the client might continue to use the IP address and configuration information until the lease expires.
- As long as the lease is still active, the client and server do not need to go through the DHCP Discover and DHCP Request process.
- When the lease has expired, the client must start over with the DHCP Discover process.

6. The client ends the lease – DHCPRELEASE

- The client ends the lease by sending a DHCP Release message to the DHCP server.
- The server will then return the client's IP address to the available address pool and cancel any remaining lease time.