NSCOM01

UDP-Based Application Protocols

3rd Term– AY2022 – 2023

Instructor: Dr. Marnel Peradilla

USER DATAGRAM PROTOCOL

- **The User Datagram Protocol (UDP) is a connectionless transport protocol used in TCP/IP networks**
- **Considered as a 'bare-bones' protocol that provides only the essential capabilities needed to transport a data segment between applications**
- **Features:**
  1. Unreliable – datagrams are not acknowledged
  2. No congestion control mechanism- datagrams sent as quickly as possible
  3. Stateless – Server does not keep track of status and session information of a client. Each request-response exchange with a client is treated as an independent transaction
  4. Unordered delivery – datagrams do not contain any sequencing information

WHEN TO USE UDP

- **Connectionless services are commonly used with applications where occasional data loss is tolerable in exchange for reduced protocol overhead:**
  1. Inward Data Collection – periodic sampling of data sources such as sensors or automatic self-test reports from network equipment
  2. Outward Data Dissemination – message broadcasting to nodes or distribution of data to a network
  3. Request – Response – query-based applications that use a transaction service provided by a single server where a single request-response is typical
  4. Real-time applications – applications with a degree of redundancy or real-time requirement e.g. voice, telemetry

APPLICATION PROTOCOLS

- **Several well-known application protocols use UDP as transport protocol to support their operations:**
  - System Logging Protocol
  - Network Time Protocol
  - Domain Name System
  - Dynamic Host Configuration Protocol
  - Trivial File Transfer Protocol
  - Simple Network Management Protocol

DHCP

Dynamic Host Configuration Protocol

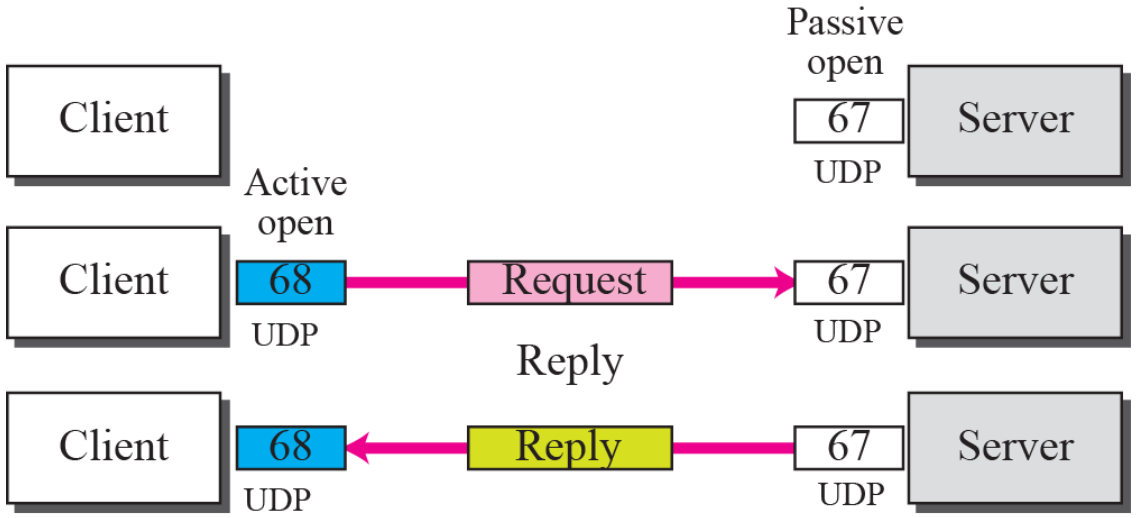
DHCP

- **Every device that connects to a network needs an IP address**

- **Dynamic Host Configuration Protocol allows host addresses to be automatically assigned to network devices.**

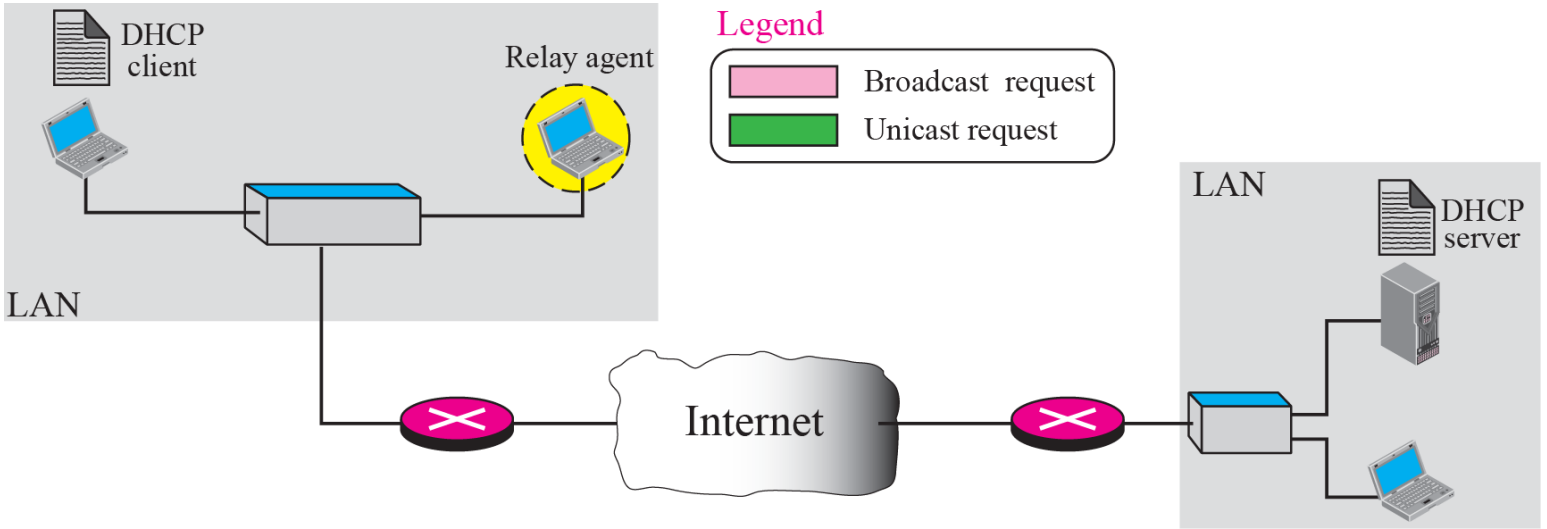
DHCP

- **RFC 2131**
- **Runs over UDP - uses port 68 on the client and port 67 as the server**
- **Designed based on BOOTP, a protocol used by early computers to get IP addresses and boot files from a server**
  - Uses the same client-server architectural model
  - Uses the same packet format
  - Extends BOOTP by adding the capability for dynamic address assignment



DHCP COMPONENTS

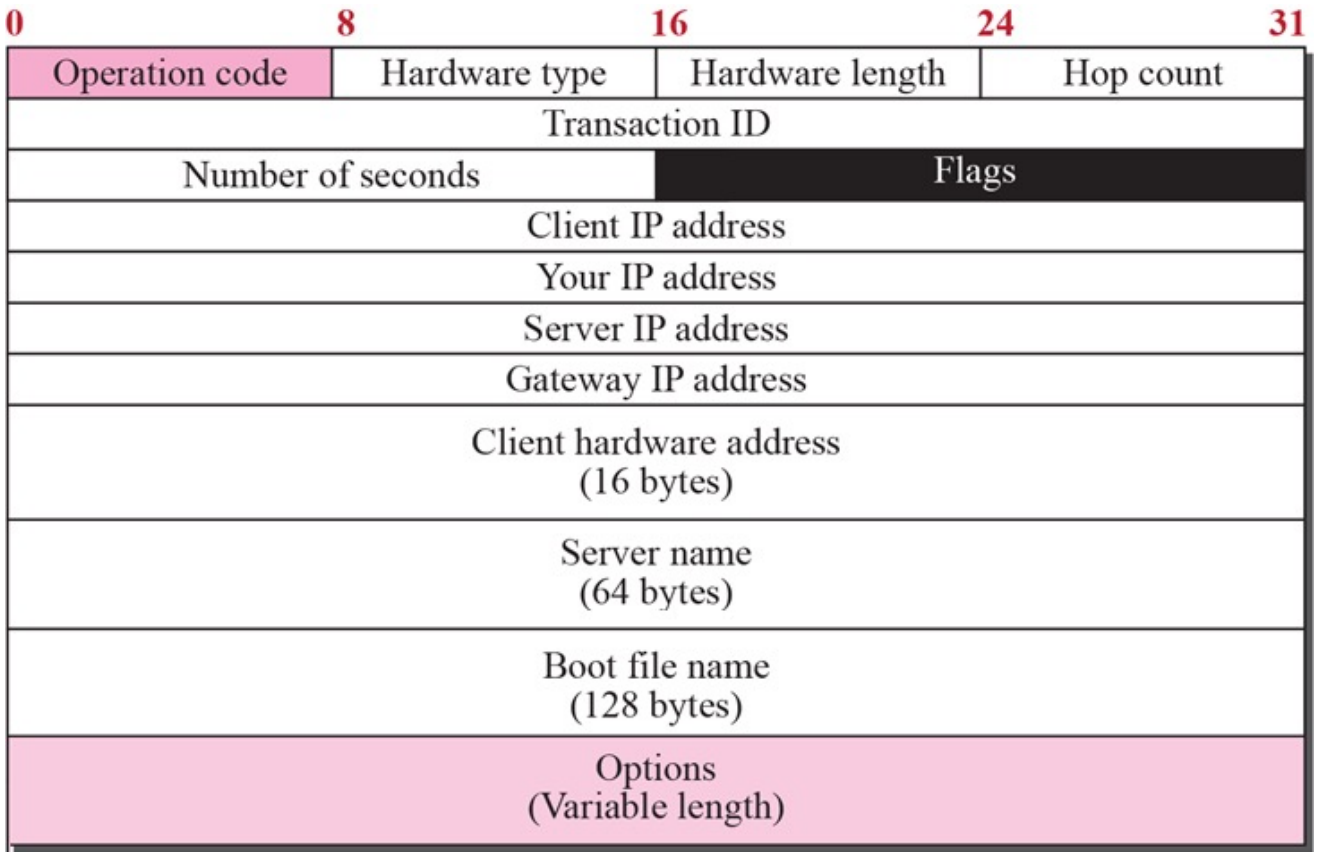
- **DHCP client: a host using DHCP to obtain an IP address and other configuration information**
- **DHCP server: a host that returns IP addresses and other configuration information. Can provide the service as a dedicated server or as part of the operations of a network device (e.g. router, switch, firewall)**
- **BOOTP relay agents: host or router that passes DHCP messages between DHCP clients and DHCP servers**



ADDRESS ALLOCATION METHODS

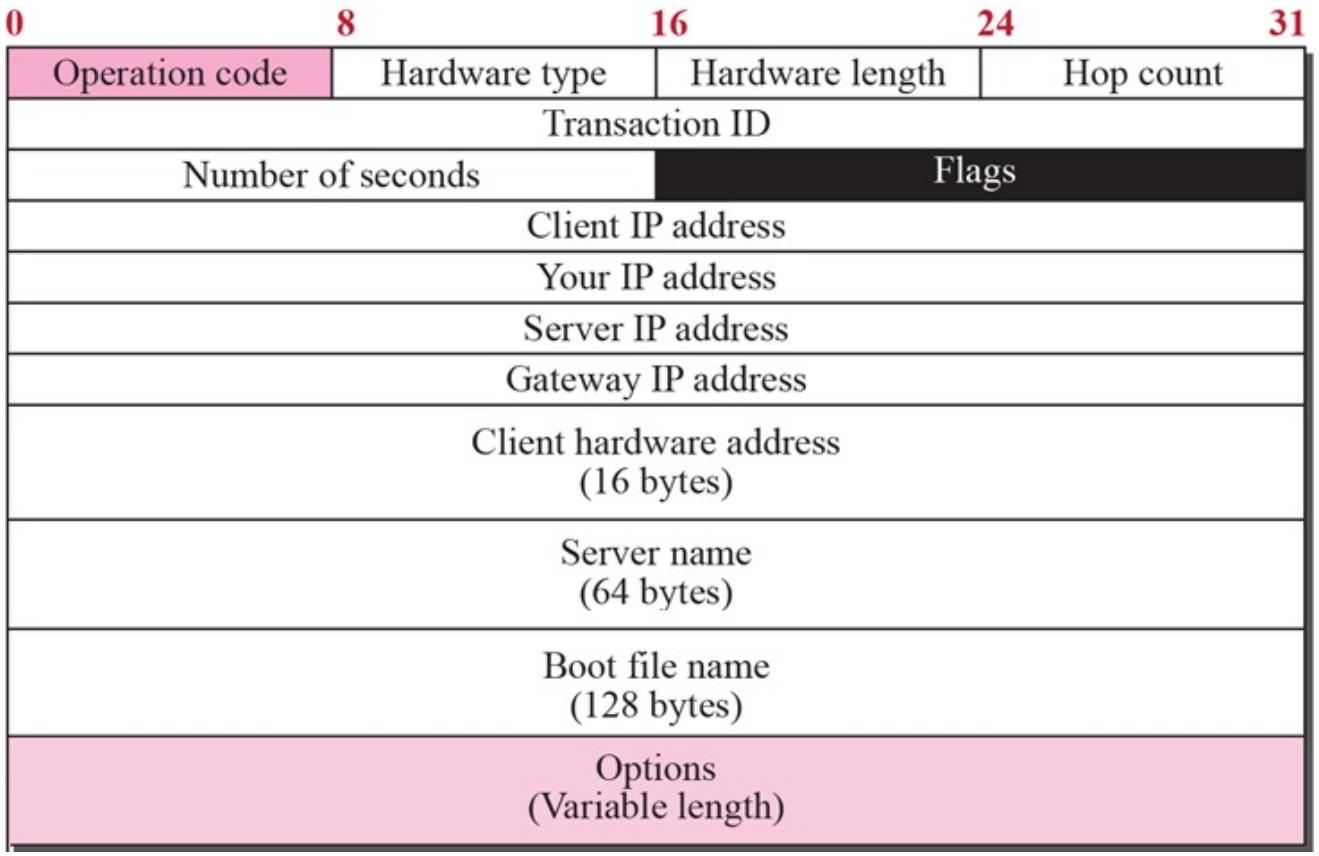
- **Manual:**
  - The IP address for the client is pre-allocated by the administrator and DHCP conveys the address to the client.
- **Automatic:**
  - DHCP automatically assigns a permanent IP address to a client with no lease period.
- **Dynamic:**
  - DHCP assigns, or leases, an IP address to the client for a limited period of time after which the lease may be renewed when the IP address is needed for an extended period, or released when no longer needed.

DHCP MESSAGE FORMAT

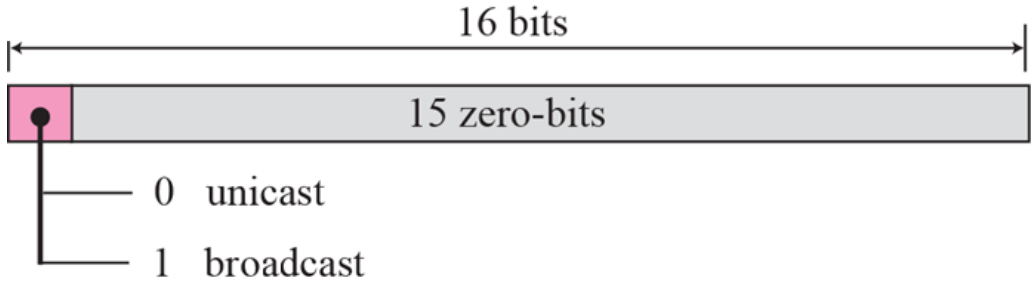


- **Op - message op code / message type**
  - 1 = BootRequest (client → server)
  - 2 = BootReply (server → client)
- **htype - hardware address type**
- **hlen - hardware address length (i.e. '6' for 10mbps Ethernet)**
- **xid - transaction ID, a random number chosen by the client, used to associate messages between a client and a server**

DHCP MESSAGE FORMAT

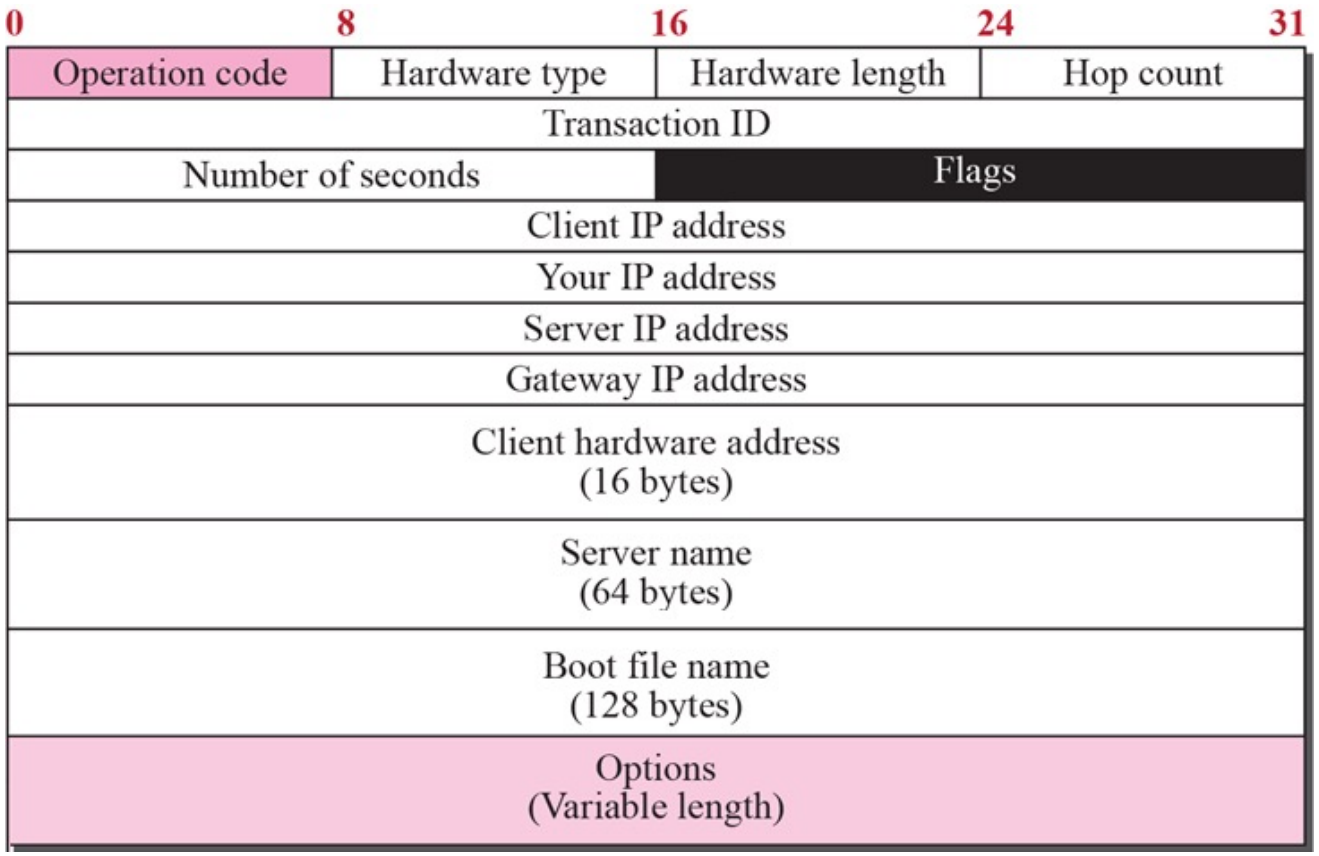


- **flags - "broadcast flag" used if client cannot accept unicast IP packets before IP layer is configured**
  - 1 = BootRequest (client → server)
  - 2 = BootReply (server → client)



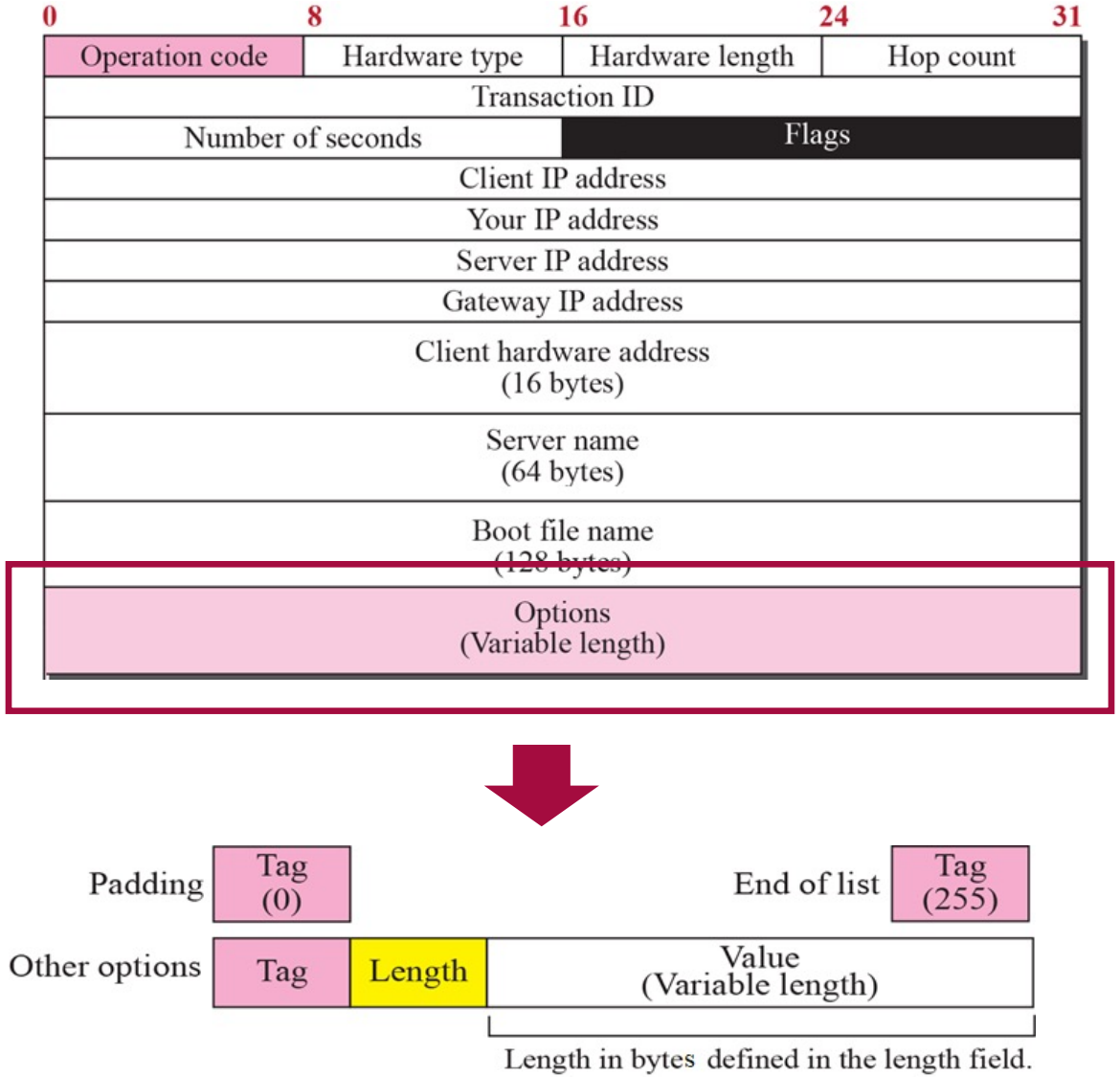
- **ciaddr - client IP address; only filled in if client is in BOUND, RENEW or REBINDING state and can respond to 'ARP' requests**

DHCP MESSAGE FORMAT



- **yiaddr – 'your' (client) IP address (set in DHCPOFFER)**
- **siaddr – IP address of next server to use in bootstrap; returned in DHCPOFFER, DHCPACK by server**
- **giaddr – relay agent IP address, used in booting via a relay agent**
- **chaddr – client hardware addresses**
- **sname – optional server host name**

DHCP MESSAGE FORMAT

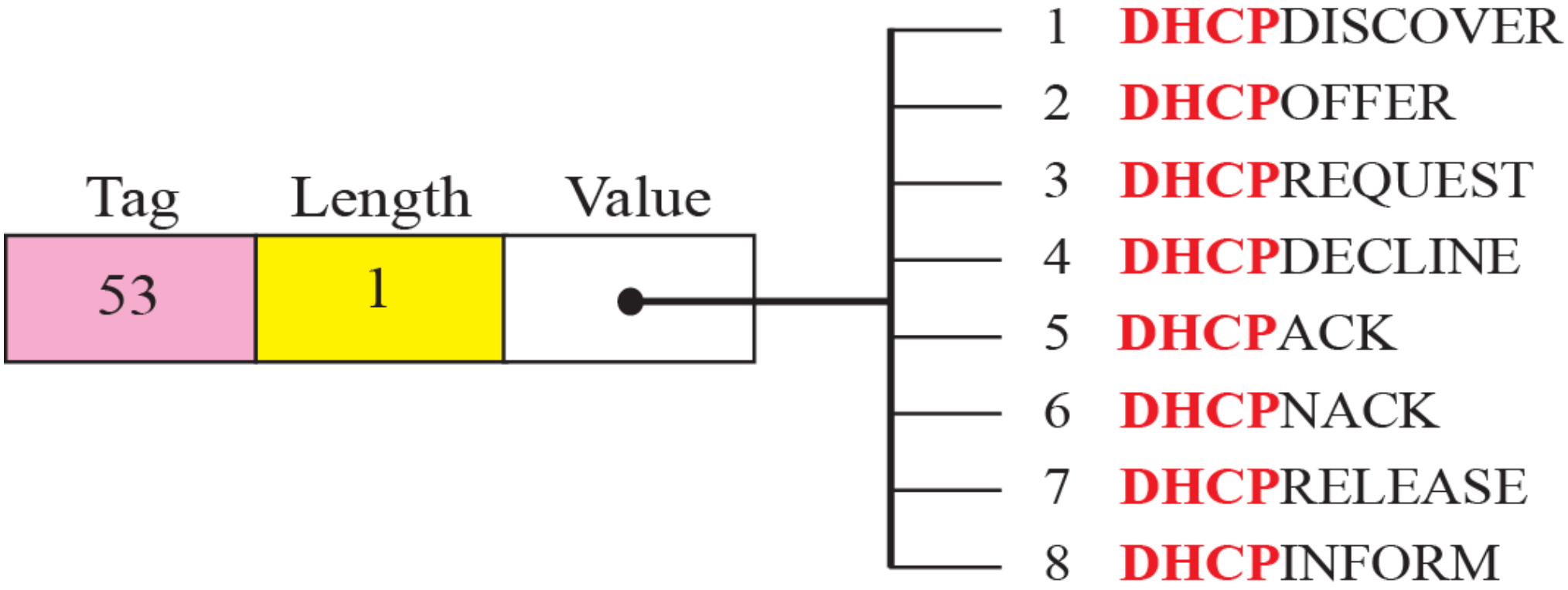


- **The options field is used to include additional optional parameters**
- **Examples:**
  - DHCP Message Type (required in all messages when using dynamic allocation)
  - Requested IP Address
  - Server identifier
  - IP Address Lease Time
  - Renewal Time Value (T1)
  - Rebinding Time Value (T2)
  - DNS (Domain Name Server) option
  - Router (Default gateway) option
  - Subnet Mask
  - Domain name

DHCPDISCOVER - Client broadcast to locate available servers. DHCPOFFER - Server to client in response to DHCPDISCOVER with offer of configuration parameters. DHCPREQUEST - Client message to servers ei

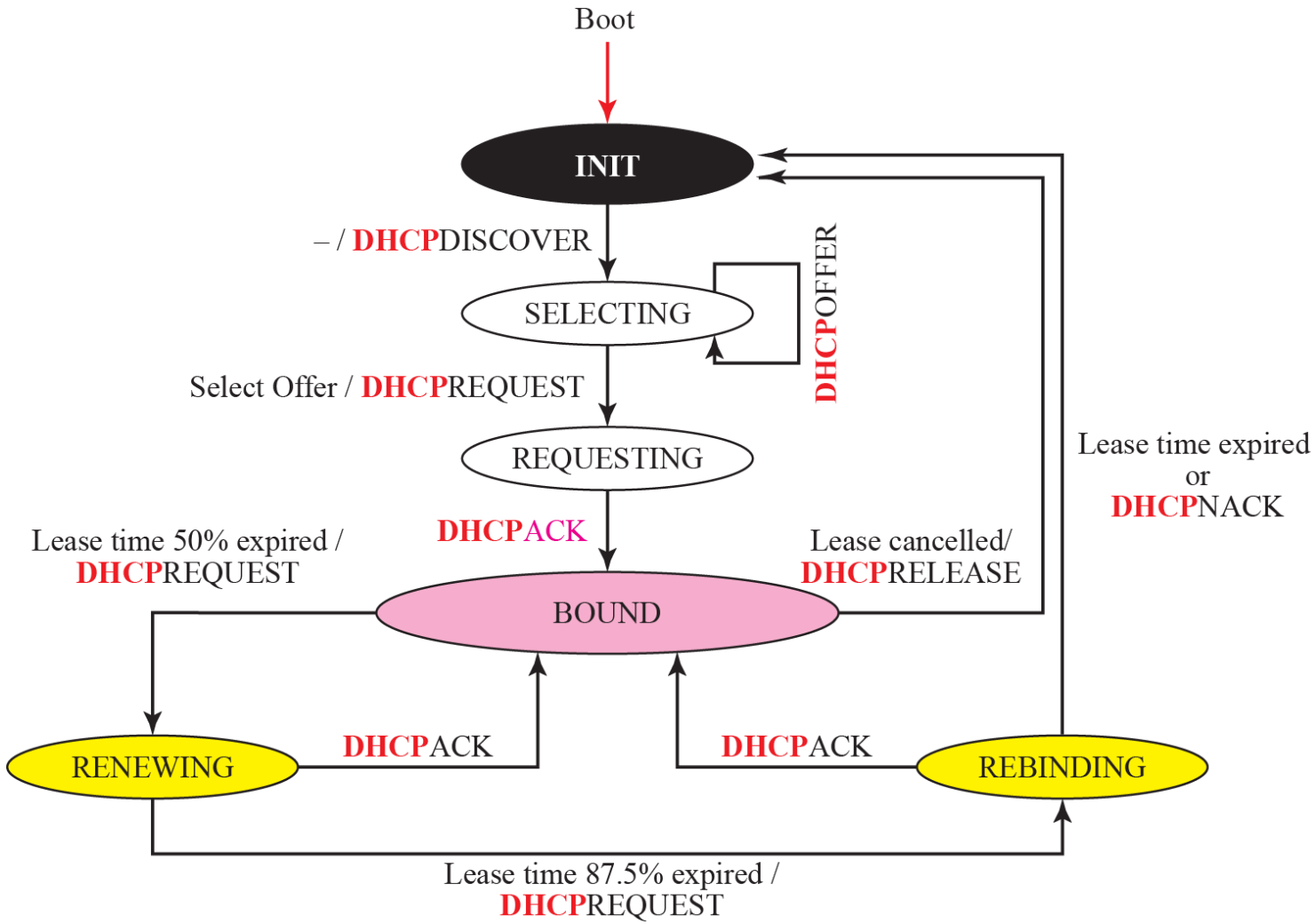
DHCP MESSAGE TYPE

- **When using dynamic address assignment, DHCP uses the message type option (Tag 53) in the message exchange sequence for address leasing**

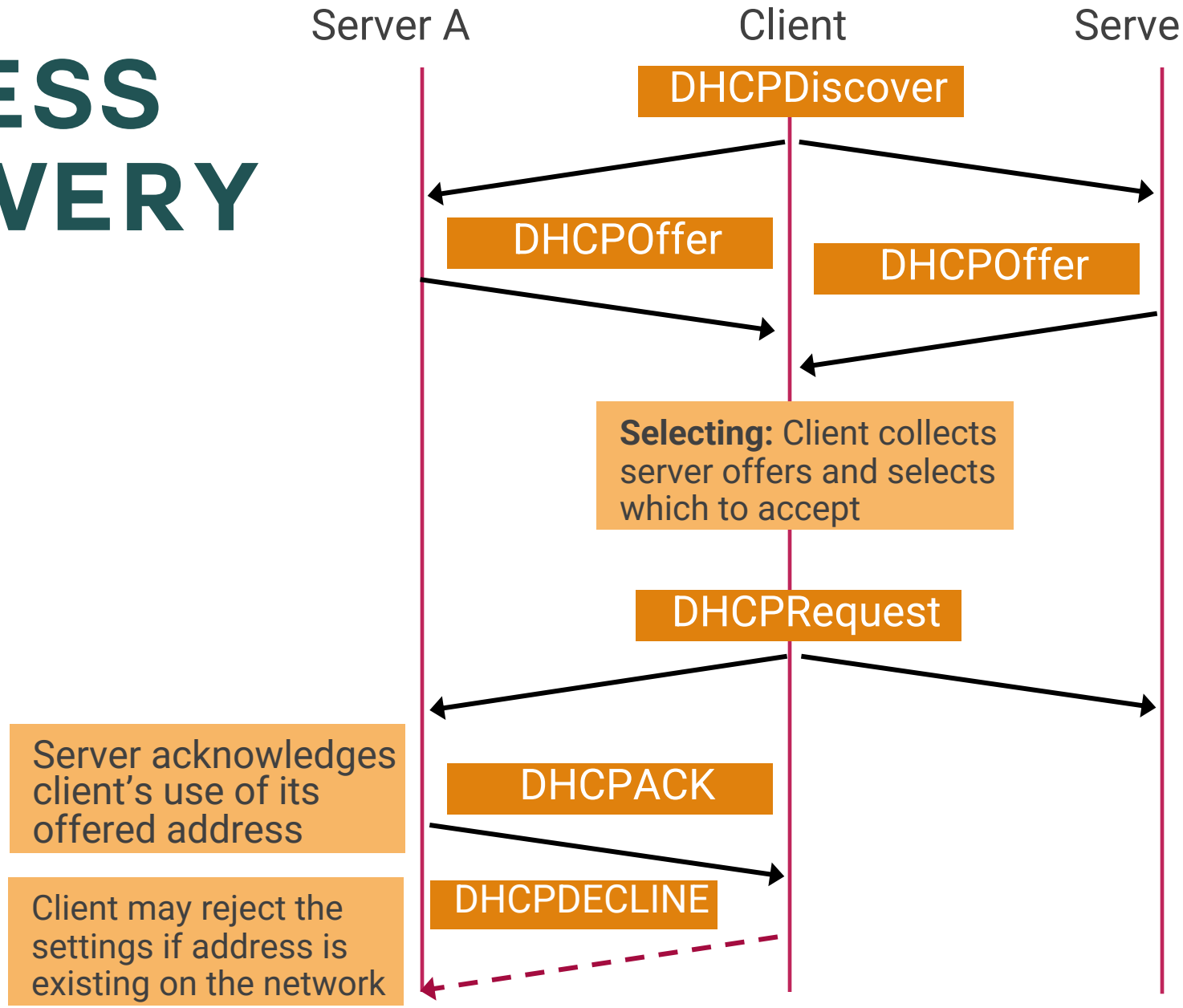


DHCP STATES AND PROCEDURE

- **DHCP clients using dynamic allocation transition between 6 states to perform 3 operations:**
  - Address discovery
  - Address renewal
  - Address release



ADDRESS DISCOVERY



Init: Client attempts to discover DHCP servers on the network

Available DHCP servers offer address settings to the client

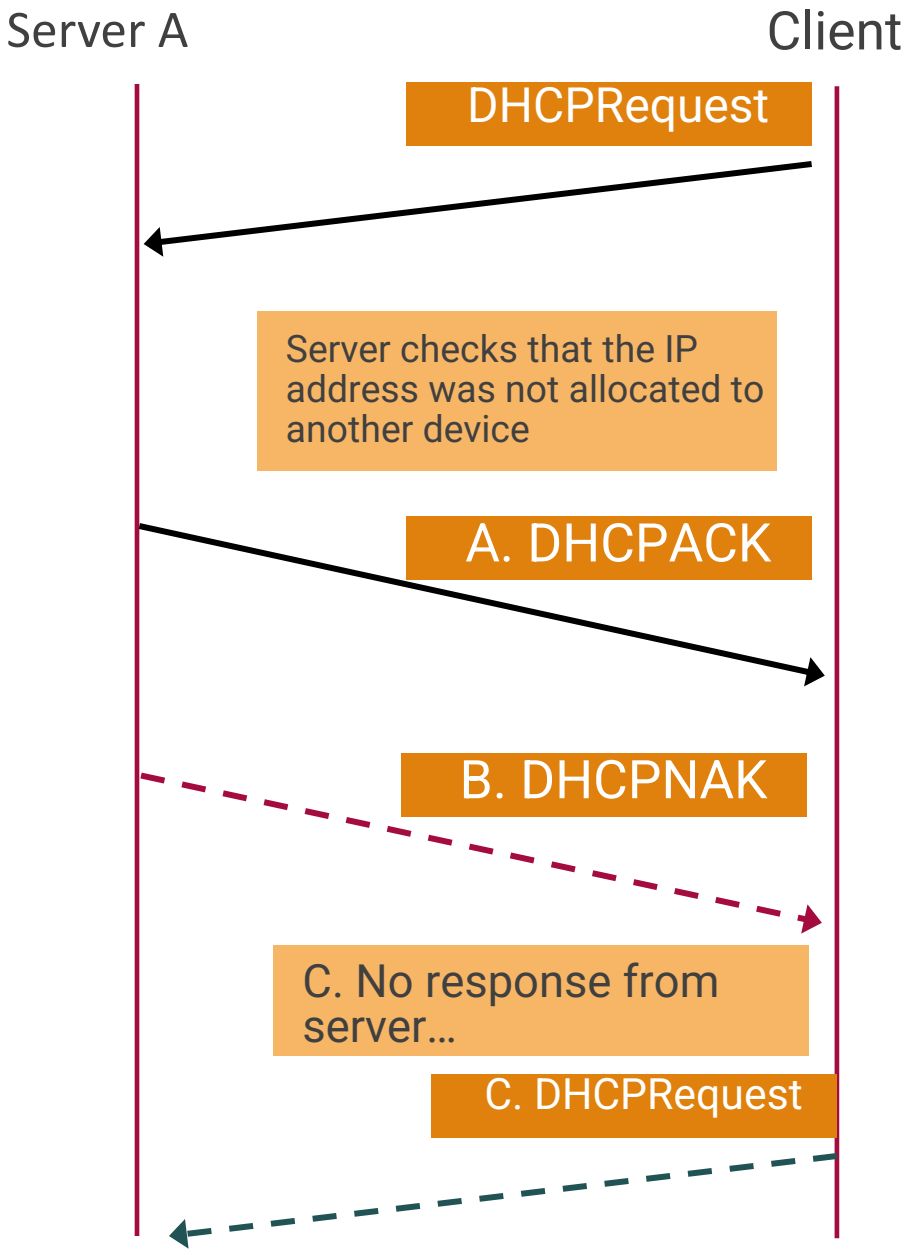
Requesting: Client broadcasts the accepted offer along with additional preferred settings

Bound: Client performs final check that address is not in use. If available, it uses the IP address for communication within the granted lease time by the server

Server acknowledges client's use of its offered address

Client may reject the settings if address is existing on the network

ADDRESS RENEWAL



Renewing: At 50% of its lease timer, client broadcasts a request to renew the lease

Bound: Server confirms address is available and allows client to continue using it

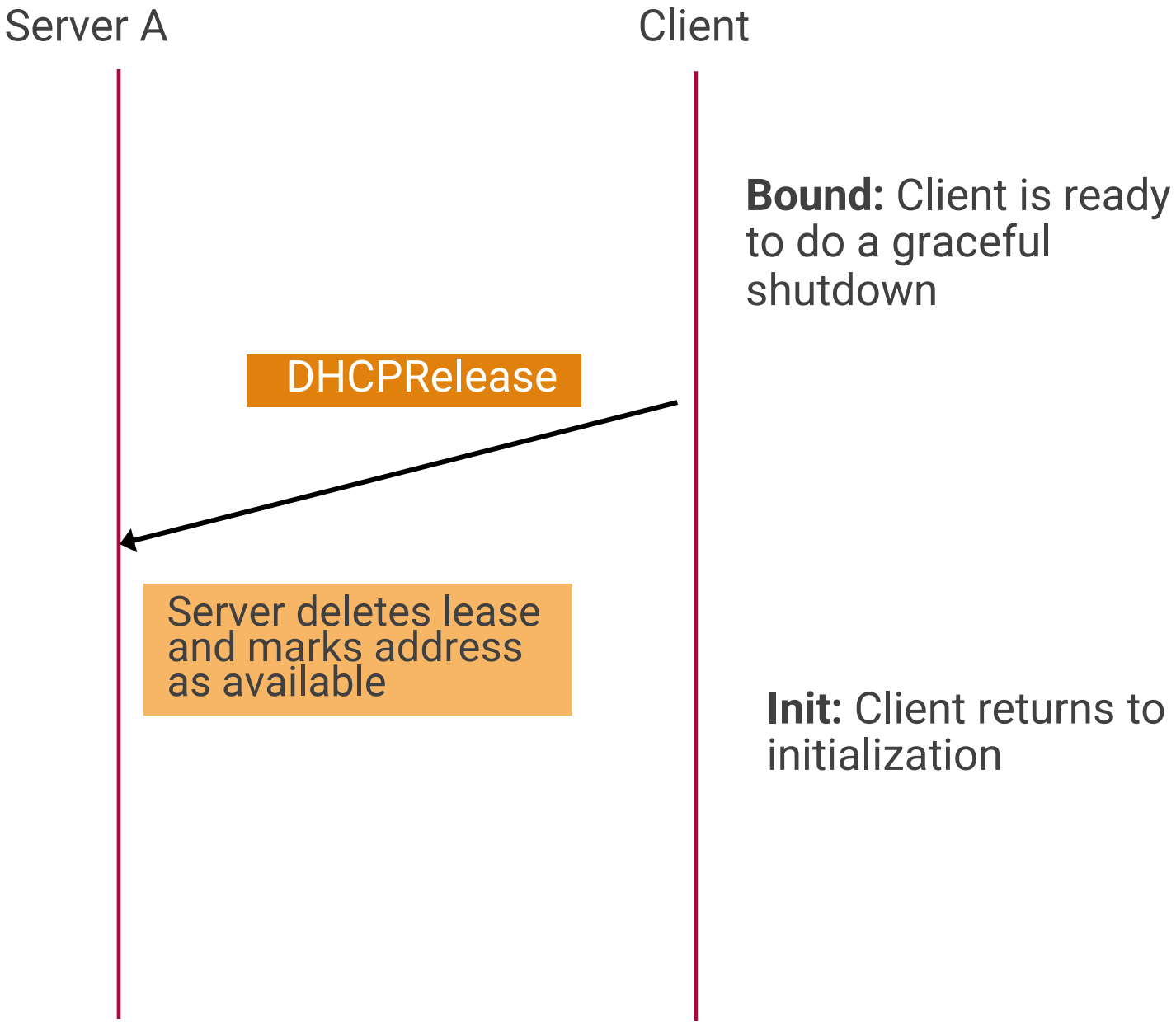
or

Init: Server rejects the renewal request. Client has to redo the address discovery process

or

Rebind: Server does not reply within 87.5% of lease time, client rebroadcasts DHCP request

ADDRESS RELEASE



Bound: Client is ready to do a graceful shutdown

Init: Client returns to initialization

CLIENT-SERVER INTERACTION

1. **DHCP Discover is sent as a broadcast (255.255.255.0) by the client within it's own subnet only to locate servers.**
2. **DHCP servers that receive the discover message each selects an address from their pool, performs a check to ensure it is unused, then sends its proposed address settings in a unicast DHCP Offer message to the client.**
   - YIADDR field contains the proposed IP address
   - All other supplementary settings (e.g. mask, gateway, lease time, etc) are placed in the message options

CLIENT-SERVER INTERACTION

3. **Client collects offers and chooses its preferred settings. DHCP Request containing it's chosen settings is sent as a broadcast to the network**
   - Option will include the address of the server that offered the chosen address, the address that the client will use, and additional settings / options requested by the client
   - Sent as a broadcast to implicitly inform other servers that their offers were not used
4. **DHCP server checks client request**
   - Sends DHCP Ack message containing confirmed settings to commit the address binding for the client if requested settings are acceptable
   - Sends DHCP NAck message if client requested settings that cannot be satisfied

CLIENT-SERVER INTERACTION

5. **Client performs actions based on server response**
   - If Nack, restart process
   - If Ack, perform a final verification that address is unused (e.g. through ARP or ping)
     - Uses the address if verification succeeds
     - Sends a DHCP Decline message to server if address is in use.
   - If no response, resend the DHCP Request
6. **When client reaches 50% of lease time, client renews the lease through a DHCP Request to the server that provide the address. The address it wants to renew is placed in the 'requested IP address' option**

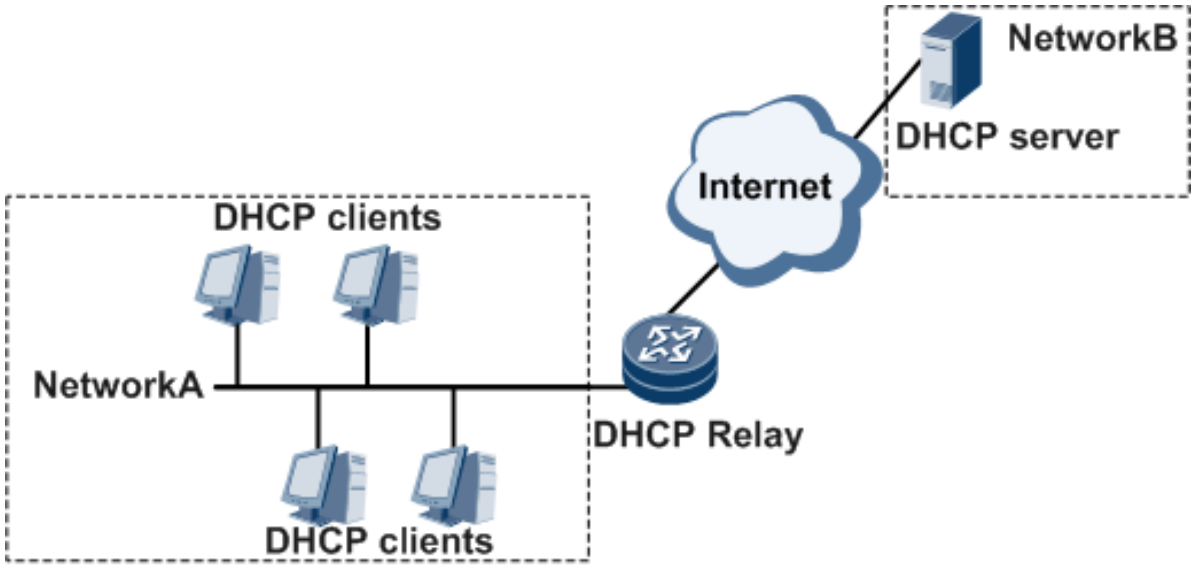
CLIENT-SERVER INTERACTION

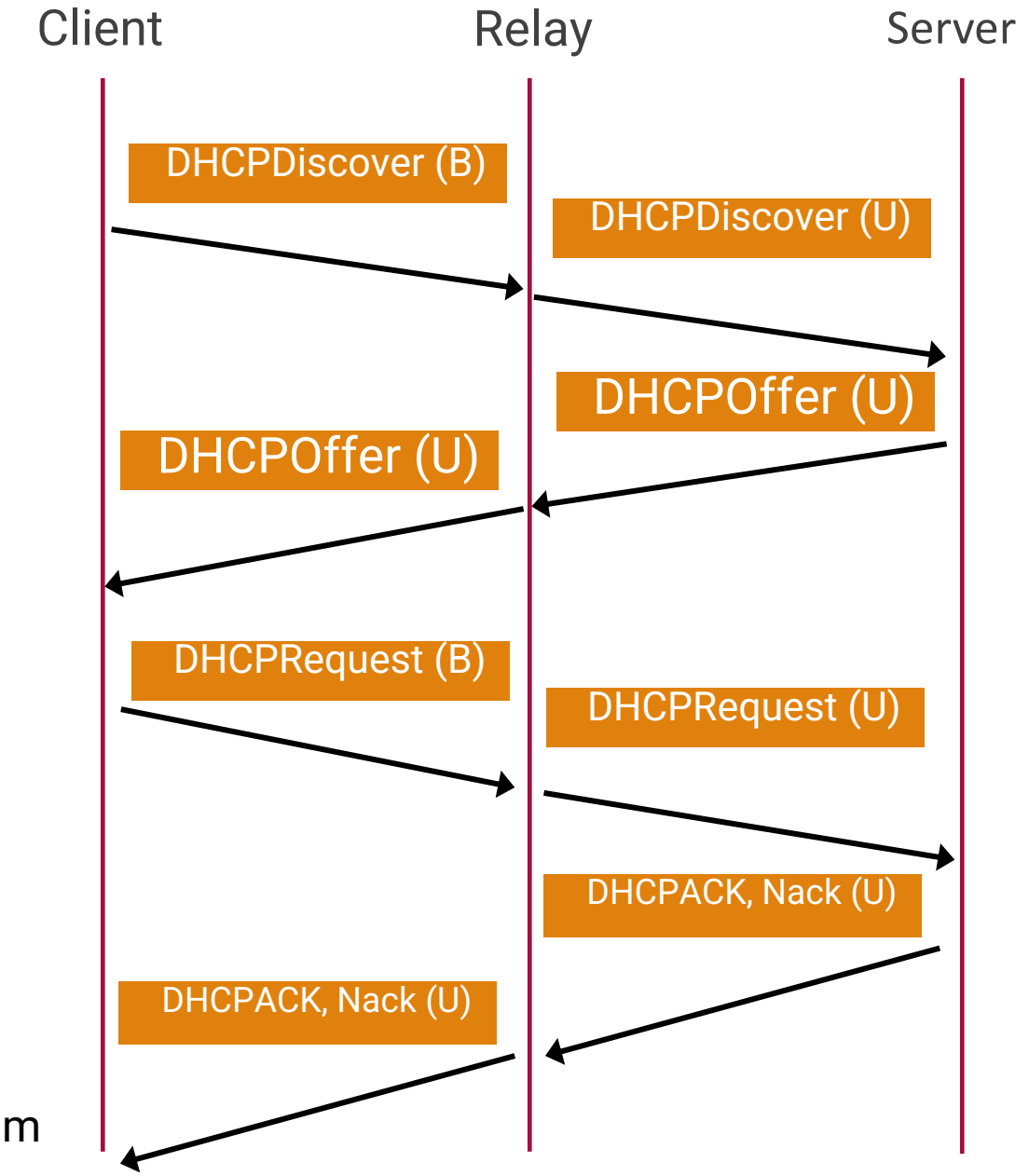
7. **Server that owns the address checks its pool if renewal is possible, no verification**
   - Send DHCP Ack if address is still available
   - Send DHCP NAck if address cannot be renewed
8. **Client that will relinquish its lease sends a DHCP Release to the server**
9. **Server makes the address available for reassignment**
10. **Server will return unreleased addresses to its pool if their leases expire without explicit requests for renewal from the clients**

DHCP RELAYS

- **DHCP Discover and DHCP Request messages are sent as local broadcast only; hence cannot reach servers that may be on a different subnet from the requesting client**
- **Usually, DHCP servers cater to several subnets at the same time from a centralized location on the network.**
- **DHCP relay is a device that is on the same subnet as the client**
  - Listens for broadcast DHCP messages from the client
  - Relays the client message as a unicast to the server on a different network

DHCP RELAYS





support.huawei.com

DHCP LIMITATIONS

- **Uses UDP, an unreliable and insecure protocol. There is not verification method between a client and server. By default:**
  - A server offers and grants addresses to any requesting client as long as the requests can be fulfilled
  - Client will accept any offer from a DHCP server
- **Potentially unauthorized clients requesting addresses from the server and gaining access to the network**
- **Malicious client could exhaust address pool (DHCP Starvation) by requesting for all available addresses of the server leading to a DoS for legitimate clients**
- **Malicious server (Rogue server) can supply incorrect configuration parameters to requesting clients to prevent proper network connectivity or to intercept client transmissions**

MESSAGE FROM DPO

"The information and data contained in the online learning modules, such as the content, audio/visual materials or artwork are considered the intellectual property of the author and shall be treated in accordance with the IP Policies of DLSU. They are considered confidential information and intended only for the person/s or entities to which they are addressed. They are not allowed to be disclosed, distributed, lifted, or in any way reproduced without the written consent of the author/owner of the intellectual property."