Computer Networks

DHCP and ARP

Fall 25-26, CS 3204

Dr. Nazib Abdun Nasir

Assistant Professor, CS, AIUB

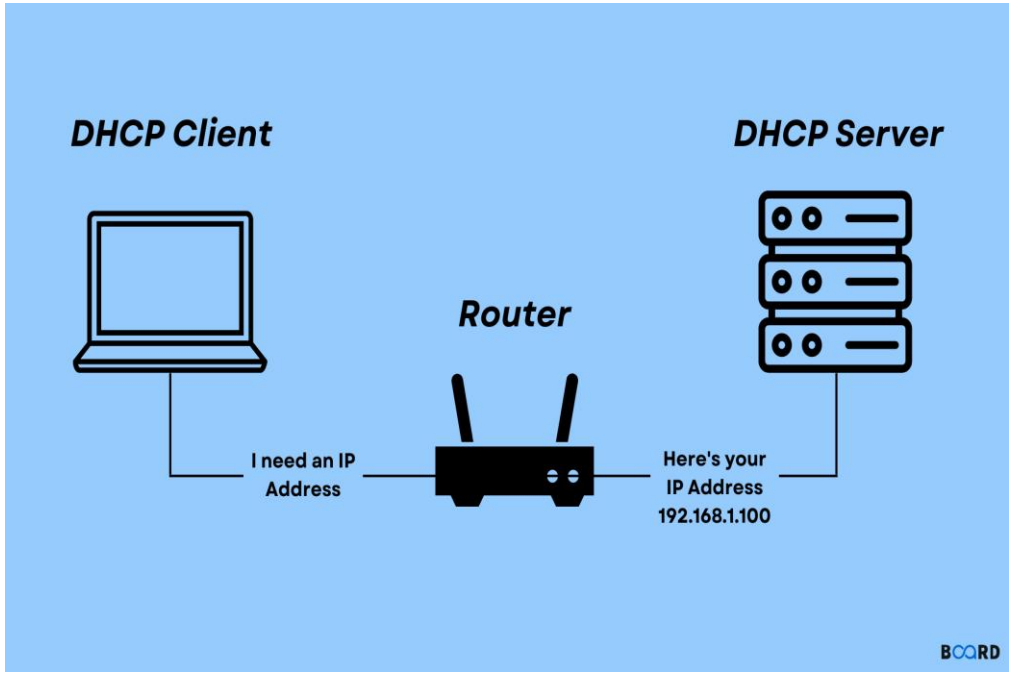
nazib.nasir@aiub.edu

Outline

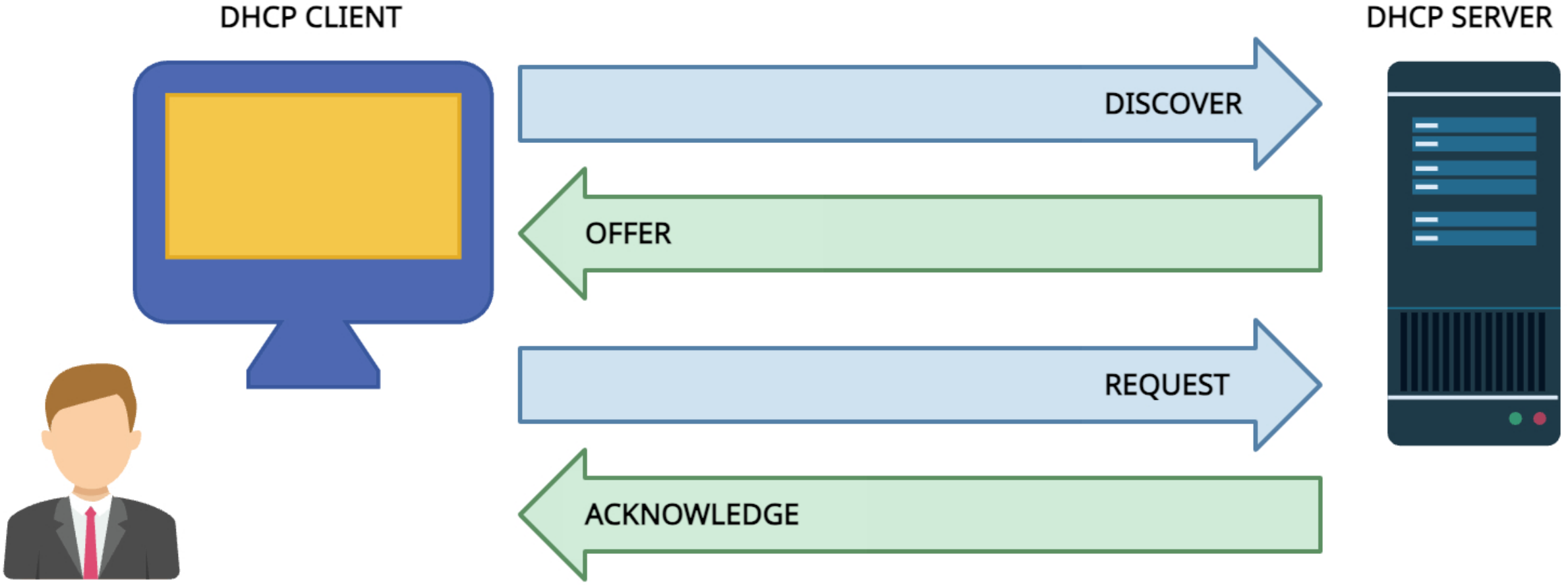
- DHCP
  - → Components, How It Works, Benefits, and Steps.
- BOOTP
- ARP
  - → It’s Functions, How It Works, Types, and Cache Timeout.

DHCP & It's Components

- Dynamic Host Configuration Protocol (DHCP) is a networking protocol that facilitates the automatic allocation of an IP address to a computer by a server, utilizing a specified range of numbers that has been set up for a particular network.
- **DHCP Server:** This server manages a pool of IP addresses and assigns them to clients as they connect to the network. It can also provide additional configuration information, such as subnet masks and DNS server addresses.
- **DHCP Client:** These are the devices (e.g., computers, smartphones, printers) that request IP addresses from the DHCP server when they connect to the network.
- **DHCP Relay Agents:** These agents facilitate communication between clients and servers, especially in larger networks where clients and servers may not be on the same local network.



How DHCP Works



How DHCP Works

- The acquisition of an IP address via DHCP is characterized by a sequence of actions referred to as the DHCP handshake.
- **Discover:** Initially, the client sends out a broadcast message to identify accessible DHCP servers.
- **Offer:** In response, the DHCP server provides an available IP address along with relevant configuration details.
- **Request:** Subsequently, the client chooses one of the offered IP addresses and formally requests it from the server.
- **Acknowledge:** Finally, the server validates the allocation of the IP address and transmits all essential configuration information back to the client.

Benefits of Using DHCP

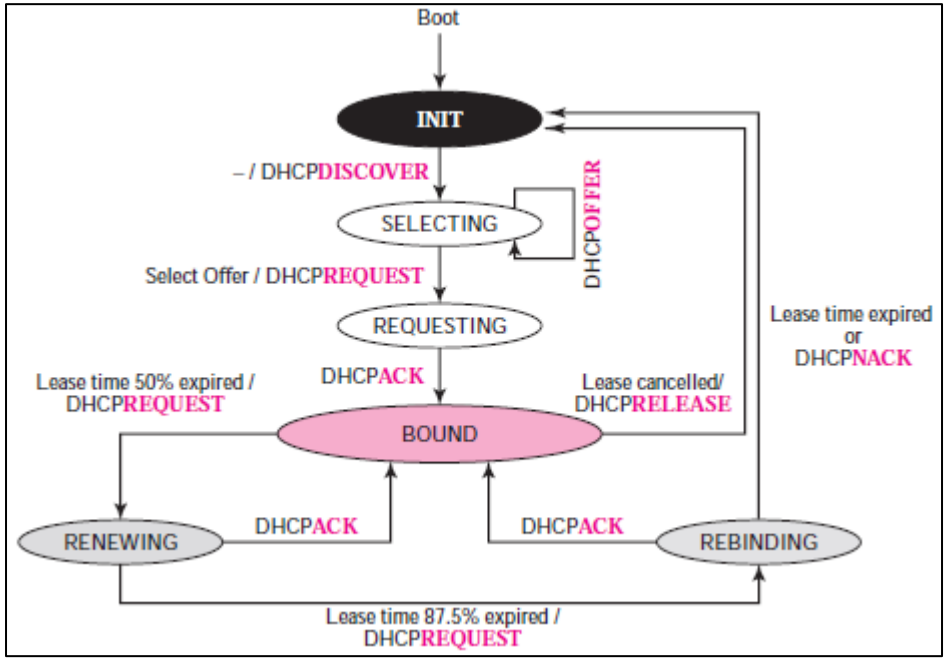
- **Efficiency:** Efficiency is enhanced through the automation of IP address allocation, which minimizes the burden of administrative tasks.

- **Flexibility:** The system offers flexibility by seamlessly adapting to devices that transition between networks, dynamically providing new IP addresses as required.

- **Scalability:** Scalability is a key feature, making it appropriate for both small residential networks and extensive corporate settings, capable of supporting thousands of devices without the need for manual setup.

DHCP Steps: INIT

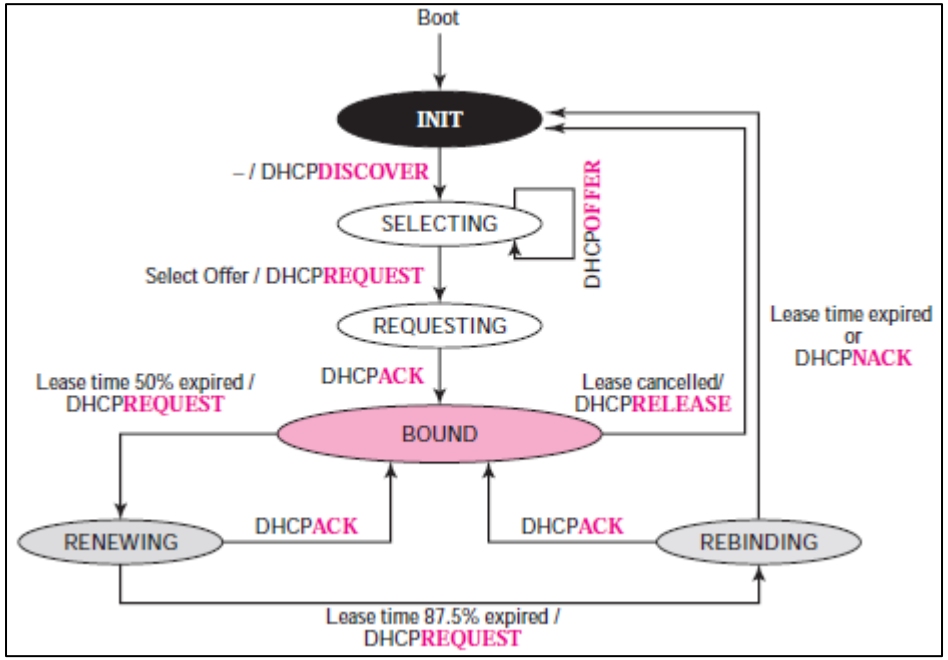
- When the DHCP client first starts, it is in the INIT state (initializing state).
- The client broadcasts a DHCPDISCOVER message **using port 67**.



nazib.nasir@aiub.edu

DHCP Steps: SELECTING

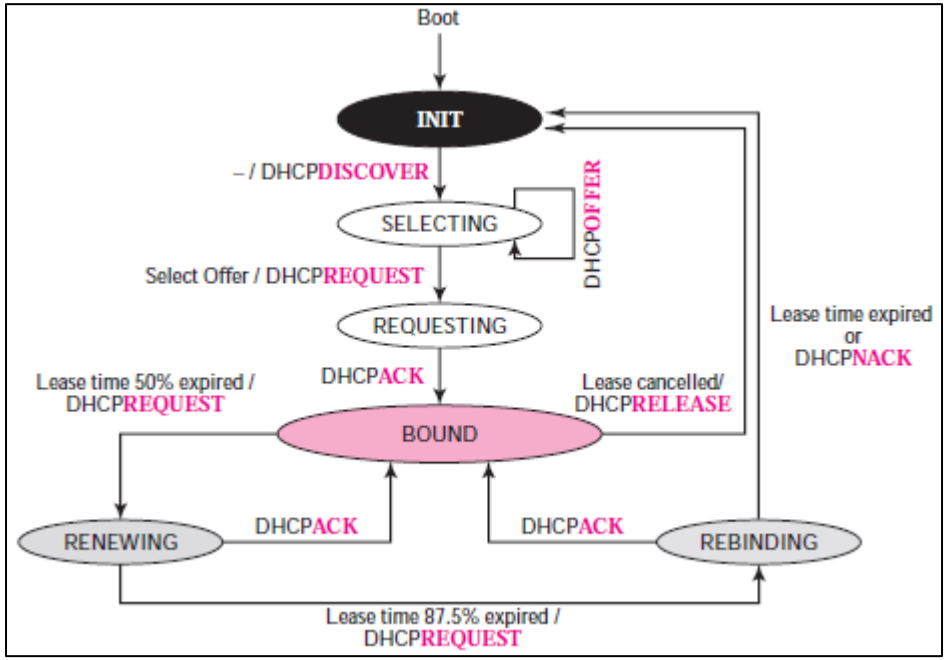
- After sending the DHCPDISCOVER message, the client goes to the SELECTING state.
- The servers respond with a DHCPOFFER message.
- In these messages, the servers offer an IP address.
- They can also offer the lease duration. **The default is 1 hour.**
- The server that sends a DHCPOFFER locks the offered IP address so that it is not available to any other clients.



nazib.nasir@aiub.edu

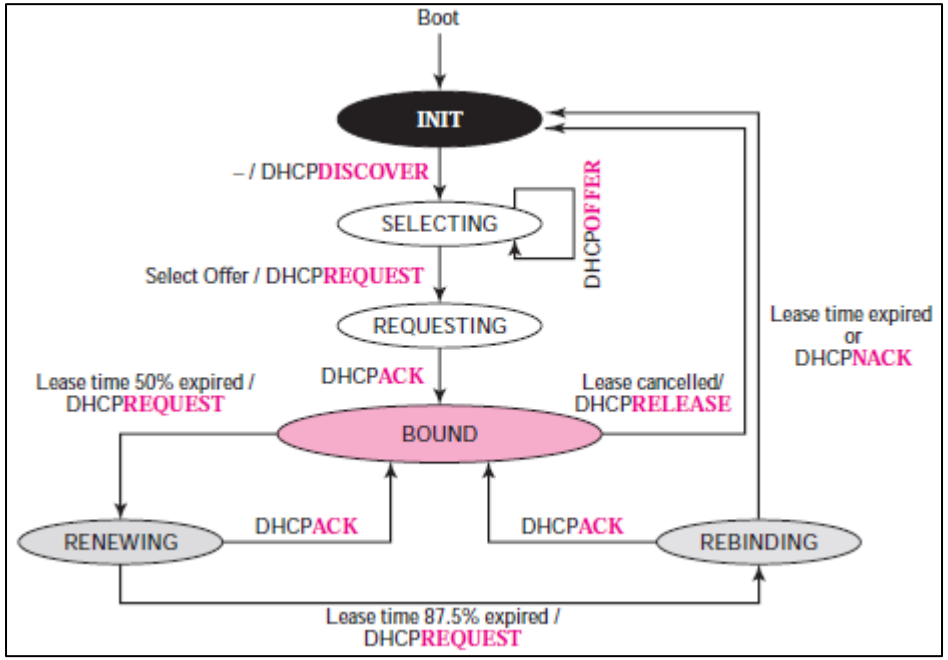
DHCP Steps: SELECTING

- The client chooses one of the offers and sends a DHCPREQUEST message to the server.
- It then goes to the REQUESTING state.
- However, if the client receives no DHCPOFFER message, **it tries four more times, each with a span of 2 seconds.**
- If there is no reply to any of these DHCPDISCOVERs, **the client sleeps for 5 minutes before trying again.**



DHCP Steps: REQUESTING

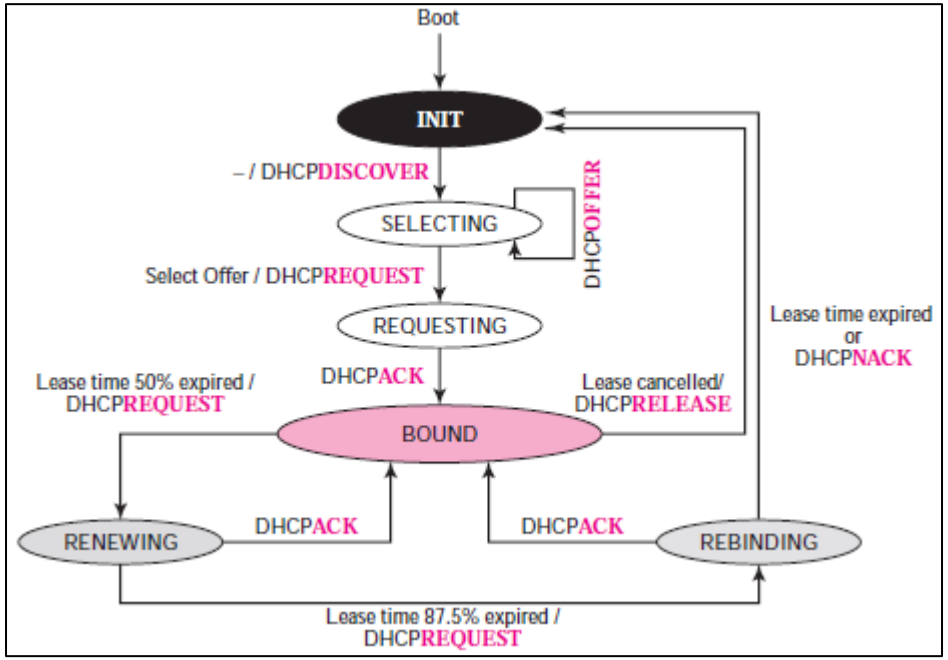
- The client remains in the REQUESTING state until it receives a DHCPACK message from the server that creates the binding between the client physical address and its IP address.
- After receipt of the DHCPACK, the client goes to the BOUND state.



nazib.nasir@aiub.edu

DHCP Steps: BOUND

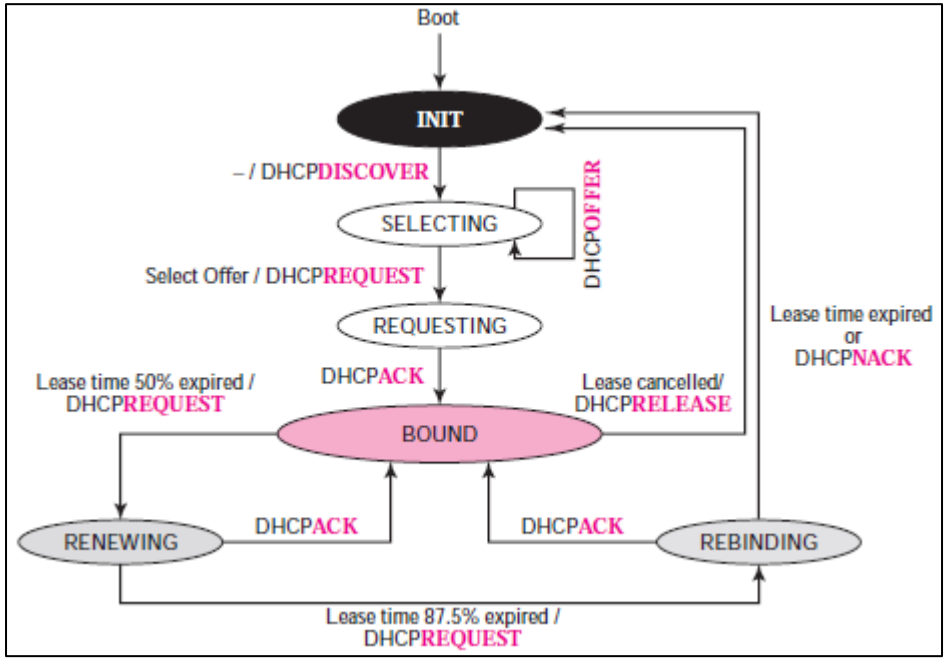
- In this state, the client can use the IP address until the lease time expires.
- When **50 percent** of the lease period is reached, the client sends another DHCPREQUEST to ask for renewal.
- It then goes to the RENEWING state.
- When in the BOUND state, the client can also cancel the lease and go to the INIT state.



nazib.nasir@aiub.edu

DHCP Steps: RENEWING

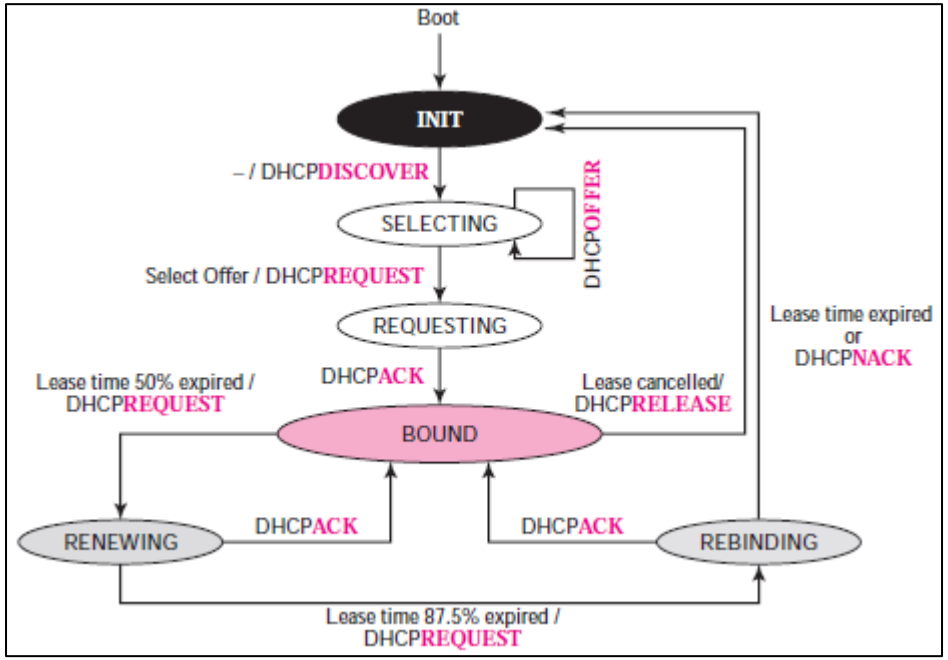
- The client remains in the RENEWING state until one of two events happens.
- It can receive a DHCPACK, which renews the lease agreement.
- In this case, the client resets its timer and goes back to the BOUND state.
- Or, if a DHCPACK is not received, and **87.5 percent** of the lease time expires, the client goes to the REBINDING state.



nazib.nasir@aiub.edu

DHCP Steps: REBINDING

- The client remains in the REBINDING state until either of the following happens.
- If the client receives a DHCPNACK or the lease expires, it goes back to the INIT state and tries to get another IP address.
- If the client receives a DHCPACK, it goes to the BOUND state and resets the timer.



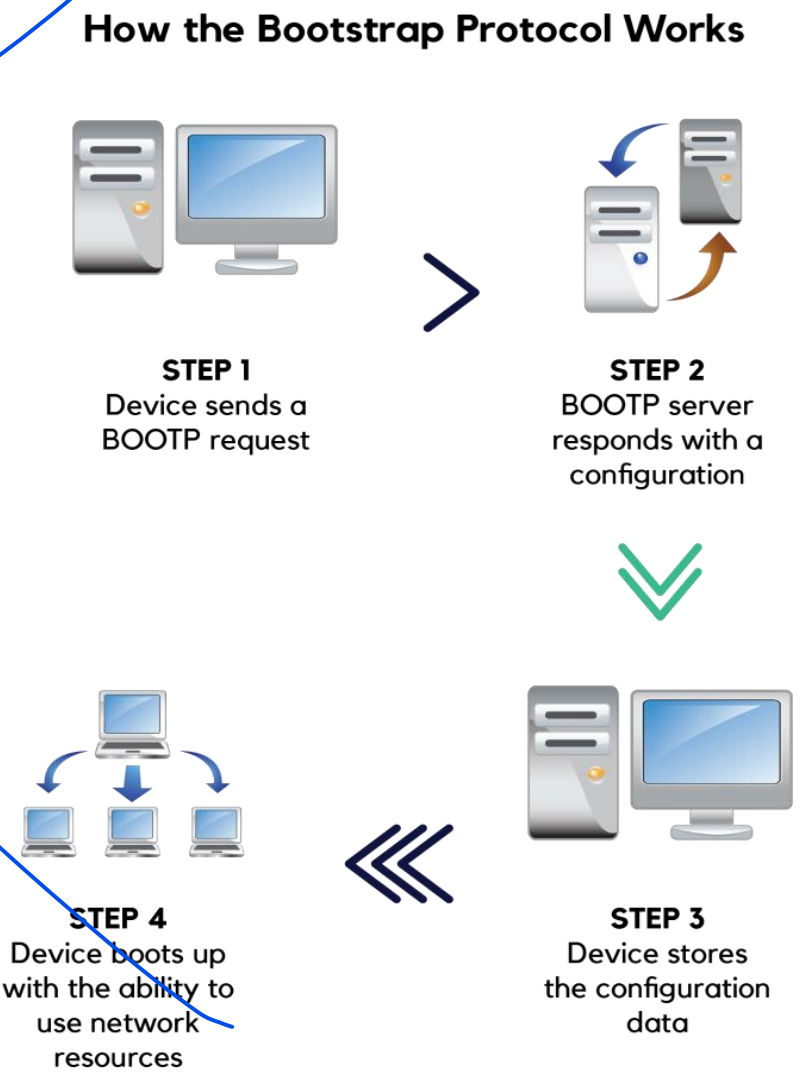
nazib.nasir@aiub.edu

DHCP Math

- A Client PC is looking for an IP address. The DHCP server has offered 3 IP addresses (207.0.0.6/24, Lease Time = 1 hr 14 min), (207.0.0.8/24, Lease Time = 1 hr 28 min), (207.0.0.11/24, Lease Time = 1 hr 32 min).
- Which IP address is best suited if the Client PC estimates a requirement of IP address for 1 hr 20 min?
- The Client has chosen the 2nd IP address. If the client asks for extended Lease Time of 22 minutes, what is the new timer of RENEWING and REBINDING states?

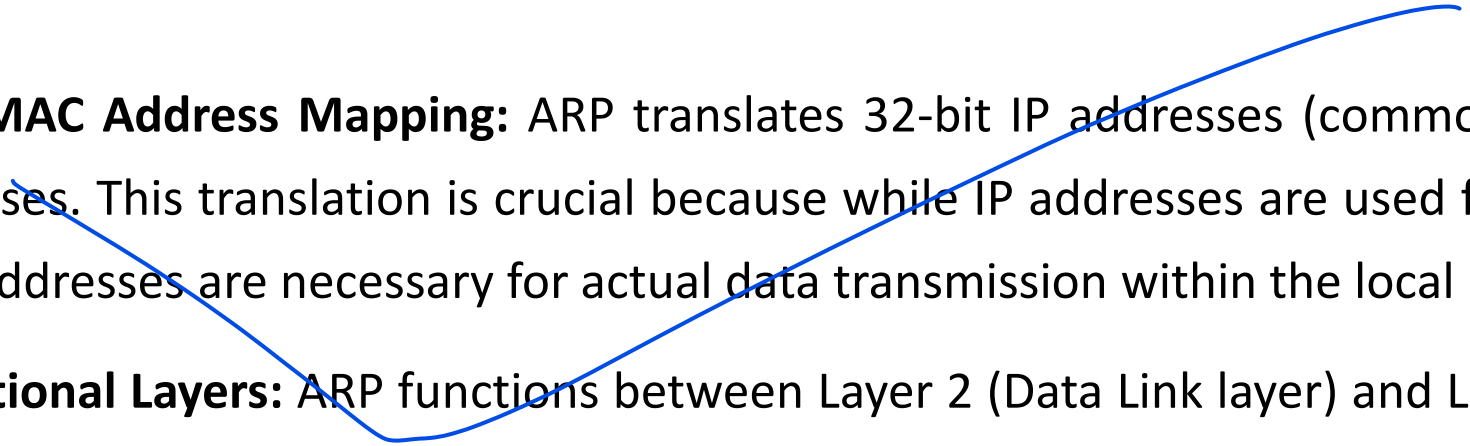
Bootstrap Protocol (BOOTP)

- The Bootstrap Protocol (BOOTP) is a network protocol designed to enable devices on a network to automatically obtain an IP address and other necessary configuration parameters from a server.
- Originating in the 1980s, BOOTP was mainly utilized for the initialization of diskless workstations and is regarded as a forerunner to the more prevalent DHCP.
- **Static Nature:** The protocol does not support dynamic IP address assignment or leasing, which limits its flexibility compared to DHCP.
- **Limited Scalability:** While effective for smaller networks, BOOTP's static nature can create difficulties in larger/dynamic networks.



ARP & It's Functions

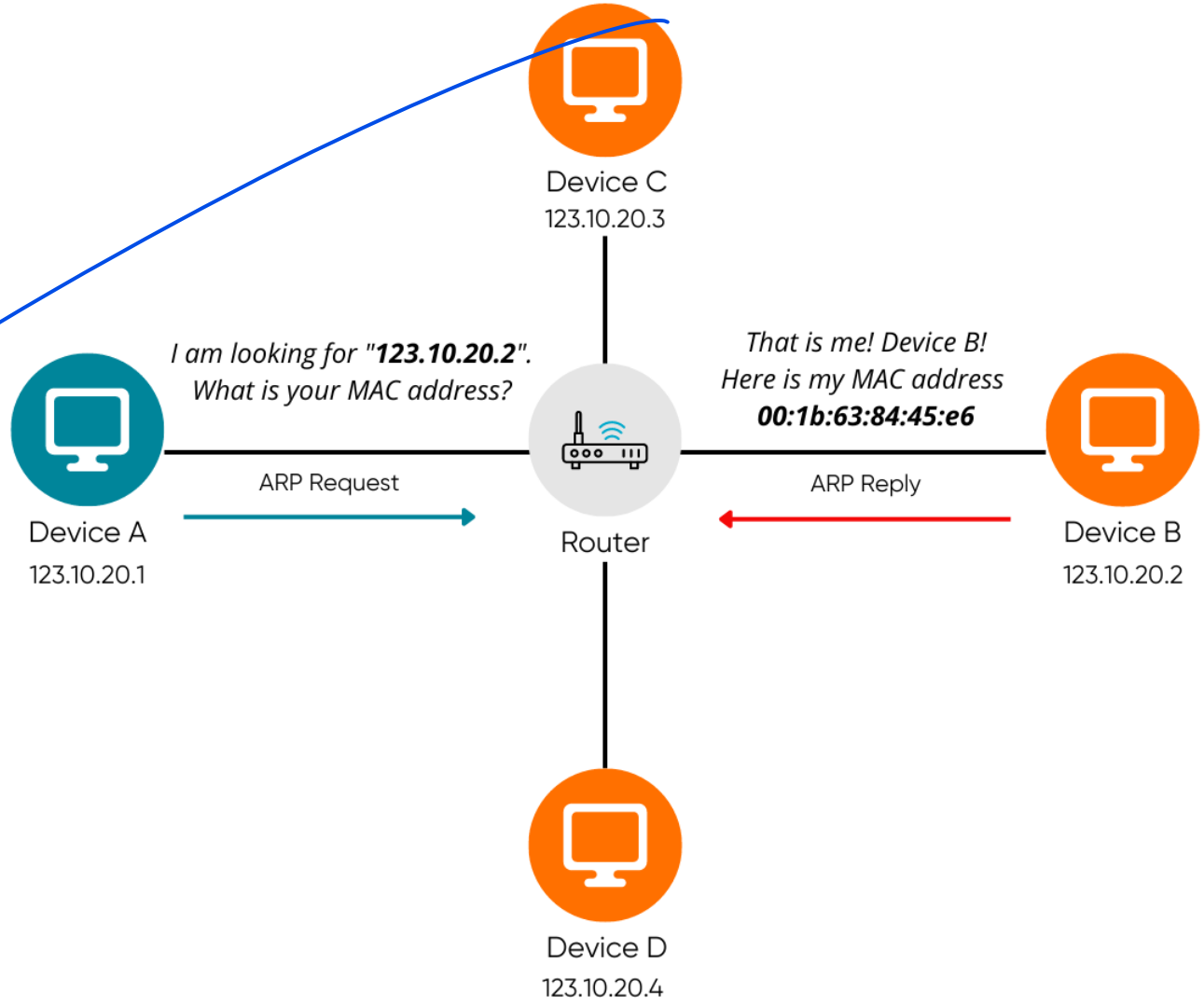
- The Address Resolution Protocol (ARP) is a communication protocol used to map Internet Protocol (IP) addresses to physical machine addresses, known as Media Access Control (MAC) addresses, within a Local Area Network (LAN).
- This mapping is essential for enabling devices to communicate effectively over the network.



- **IP to MAC Address Mapping:** ARP translates 32-bit IP addresses (commonly used in IPv4) to 48-bit MAC addresses. This translation is crucial because while IP addresses are used for routing data across networks, MAC addresses are necessary for actual data transmission within the local network segment.
- **Operational Layers:** ARP functions between Layer 2 (Data Link layer) and Layer 3 (Network layer) of the OSI model, facilitating communication between devices that use different addressing schemes.

How ARP Works

- **ARP Request:** When a device wants to communicate with another device but only knows its IP address, it sends an ARP request as a broadcast message on the network. This request asks, "Who has this IP address? Please send me your MAC address".
- **ARP Reply:** The device that owns the specified IP address responds with an ARP reply, providing its MAC address. This reply is sent directly back to the requesting device.
- **Caching:** Once the requesting device receives the MAC address, it stores this information in an ARP cache for future reference, reducing the need for repeated requests.



Types of ARP

- **Proxy ARP:** Allows a router to respond to ARP requests on behalf of devices in different networks, facilitating communication between them.
- **Gratuitous ARP:** A device sends an unsolicited ARP reply to announce its presence on the network or to update its MAC address in other devices' caches.
- **Reverse ARP (RARP):** Used by a device to discover its own IP address when it knows its MAC address.
- **Inverse ARP (InARP):** Determines a device's IP address based on its MAC address, often used in Frame Relay networks.

ARP Cache Timeout

- ARP Cache Timeout refers to the duration that an entry in the ARP cache remains valid before it is considered stale and removed.
- This timeout is crucial for maintaining accurate IP-to-MAC address mappings in a network, ensuring that devices can communicate effectively without relying on outdated information.
- Linux systems typically set the base reachable time for ARP entries to 30 seconds, resulting in a random timeout between 15 and 45 seconds for each entry.
- Cisco routers often have a default ARP cache timeout of 4 hours, which can be configured based on network needs.
- **Advantages:** Independently revalidate, easily determine off nodes, not relying on network hardware.
- **Disadvantage:** Delay – wait until the timer expires.

References

- DHCP and ARP – Provided Material
- Online Website Research