# DHCP & ARP

Course Title: Computer Networks


**Dr. Nazib Abdun Nasir**
**Assistant Professor**
**CS, AIUB**
**nazib.nasir@aiub.edu**

# Lecture Outline


- DHCP
  - What is DHCP?
  - How DHCP works?
  - Steps of DHCP
- ARP
  - What is ARP?
  - How ARP works?
  - ARP cache timeout
  - Advantage and Disadvantage

# What is DHCP

- Dynamic Host Configuration Protocol (DHCP) is a network protocol that enables a server to automatically assign an IP address to a computer from a defined range of numbers configured for a given network.

# Bootstrap Protocol


- The Bootstrap Protocol (BOOTP) is a computer networking protocol used in Internet Protocol(IP) networks to automatically assign an IP address to network devices from a configuration server.
- When a computer that is connected to a network is powered up and boots its operating system, the system software broadcasts BOOTP messages onto the network to request an IP address assignment.
- A BOOTP configuration server assigns an IP address based on the request from a pool of addresses configured by an administrator.

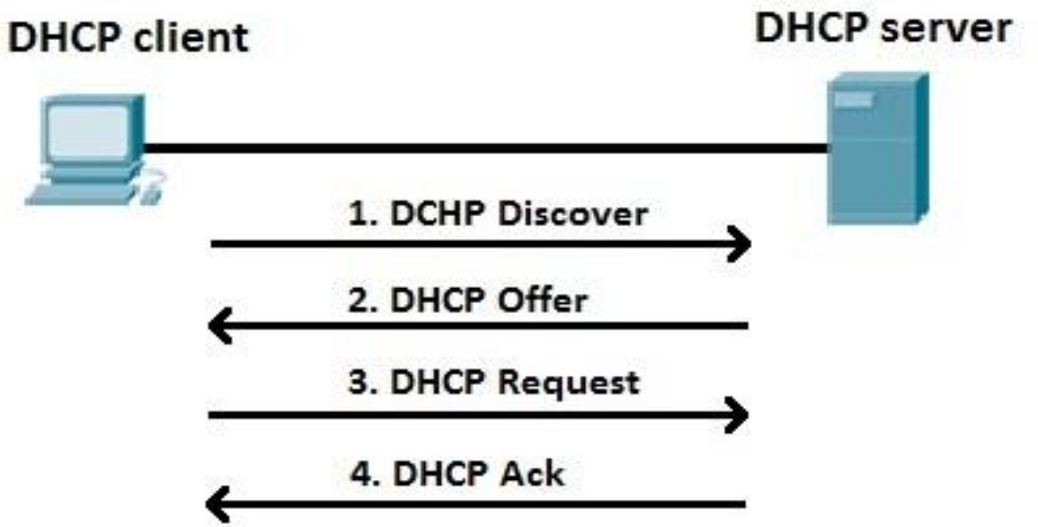
# Bootstrap Protocol


- BOOTP is not a dynamic configuration protocol.
- When a client requests its IP address, the BOOTP server consults a table that matches the physical address of the client with its IP address. This implies that the binding between the physical address and the IP address of the client already exists. The binding is predetermined.
- However, what if a host moves from one physical network to another?
- What if a host wants a temporary IP address?
- BOOTP cannot handle these situations because the binding between the physical and IP addresses is static and fixed in a table until changed by the administrator. BOOTP is a static configuration protocol.

# DHCP

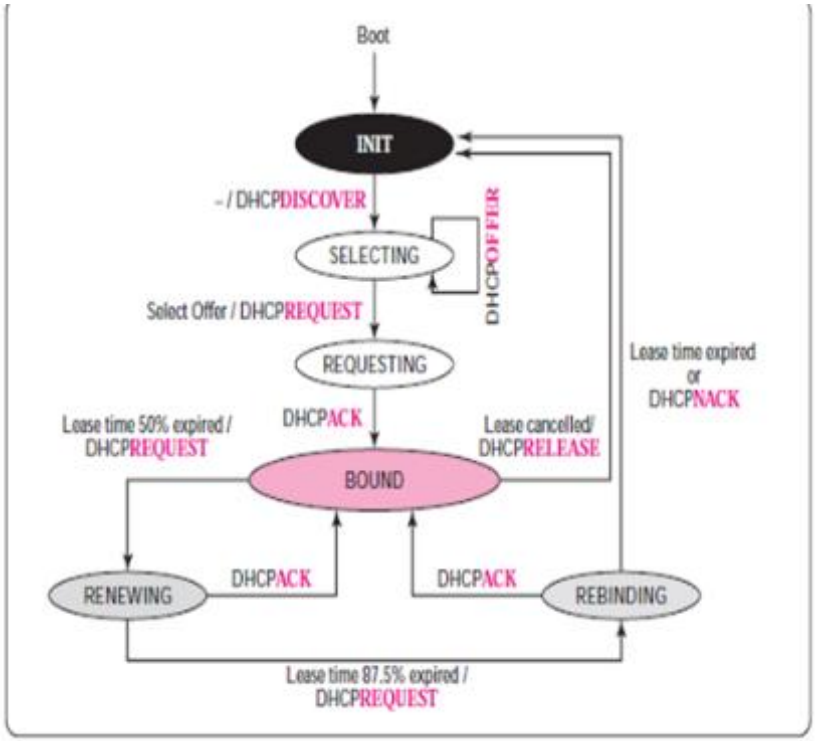

- The Dynamic Host Configuration Protocol (DHCP) has been devised to provide static and dynamic address allocation that can be manual or automatic.
- **Static Address Allocation:** In this capacity DHCP acts as BOOTP does. It is backward compatible with BOOTP, which means a host running the BOOTP client can request a static address from a DHCP server. A DHCP server has a database that statically binds physical addresses to IP addresses.
- **Dynamic Address Allocation:** DHCP has a second database with a pool of available IP addresses. This second database makes DHCP dynamic. When a DHCP client requests a temporary IP address, the DHCP server goes to the pool of available (unused) IP addresses and assigns an IP address for a negotiable period of time.

# DHCP process explained



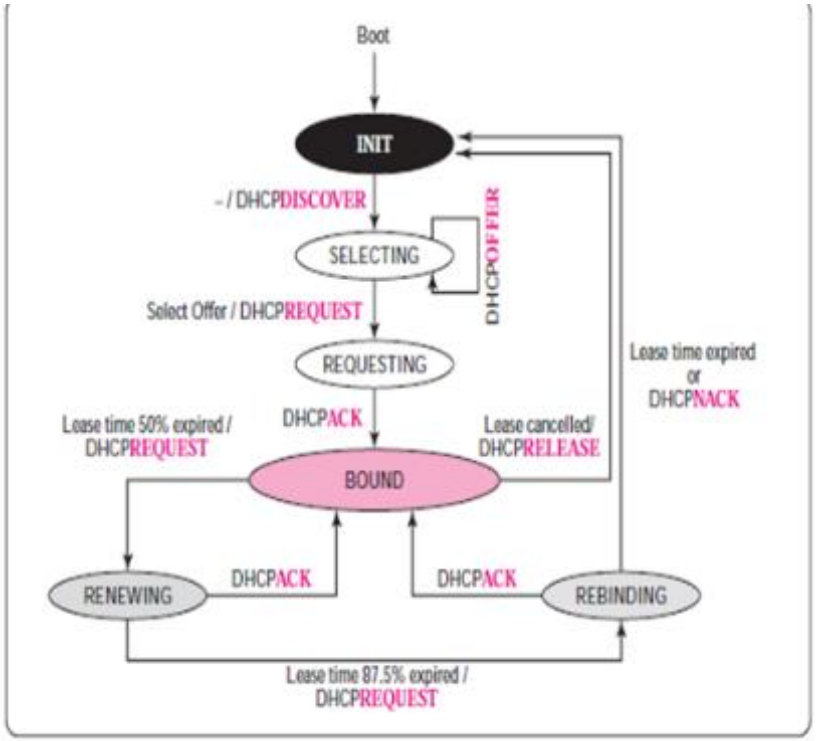
# Steps of DHCP: INIT State

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



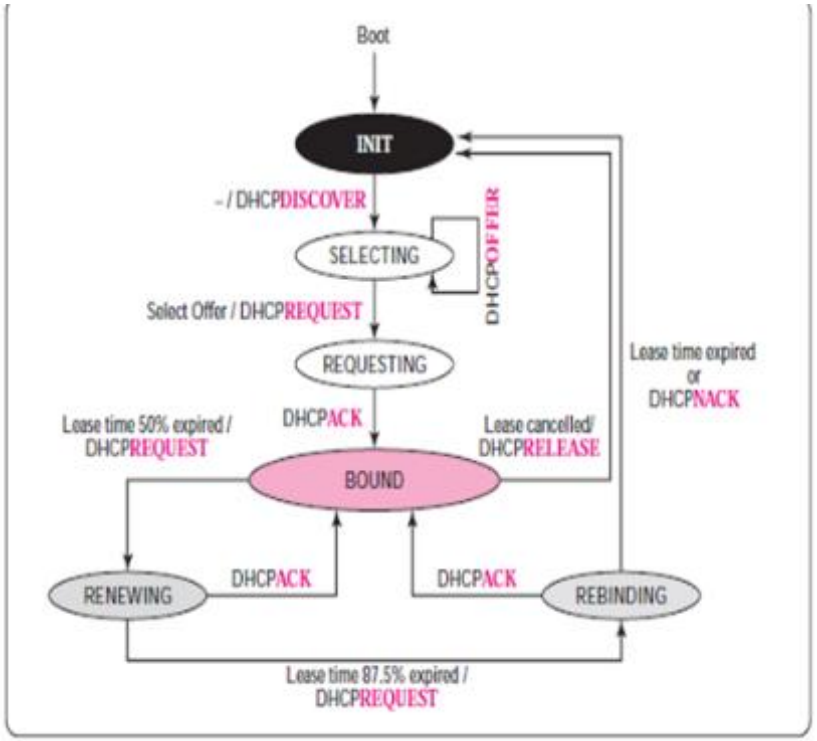
# Steps of DHCP: SELECTING State

- After sending the DHCPDISCOVER message, the client goes to the selecting state.
- Those servers that can provide this type of service 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.



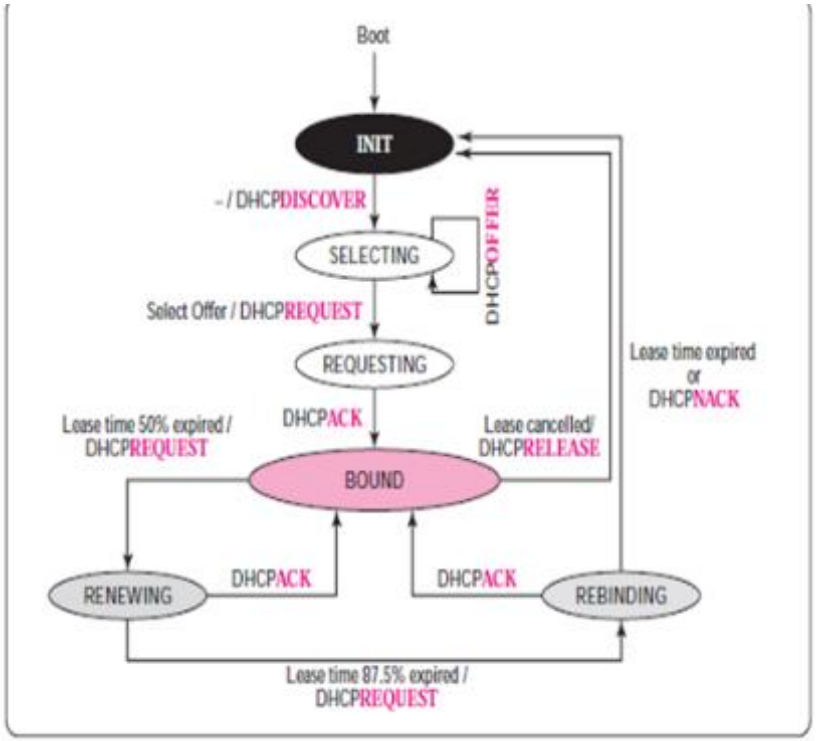
# Steps of DHCP: SELECTING State (cont.)

- The client chooses one of the offers and sends a DHCPREQUEST message to the selected 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.



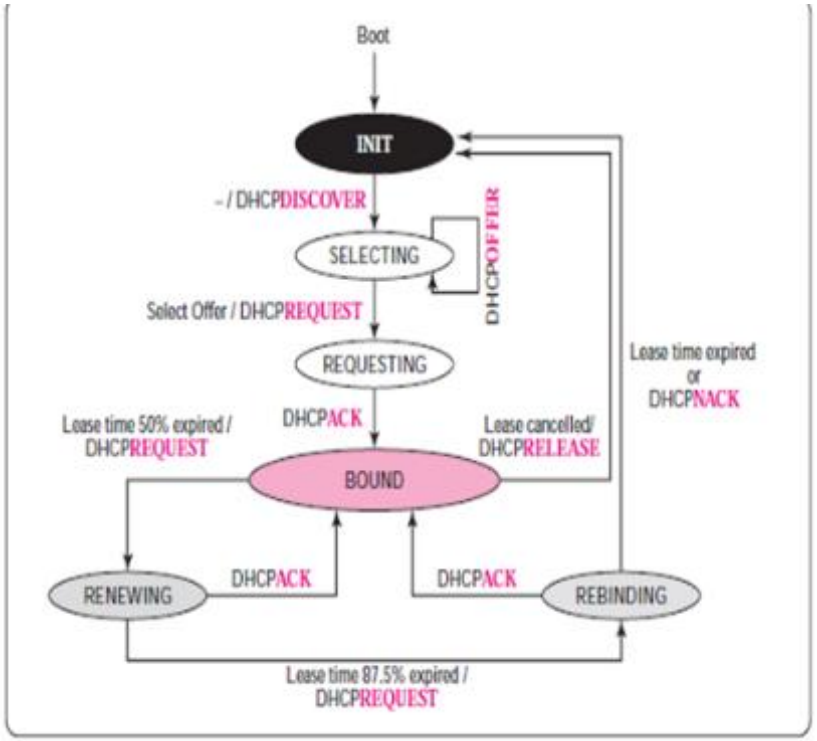
# Steps of DHCP: REQUESTING State

- 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.



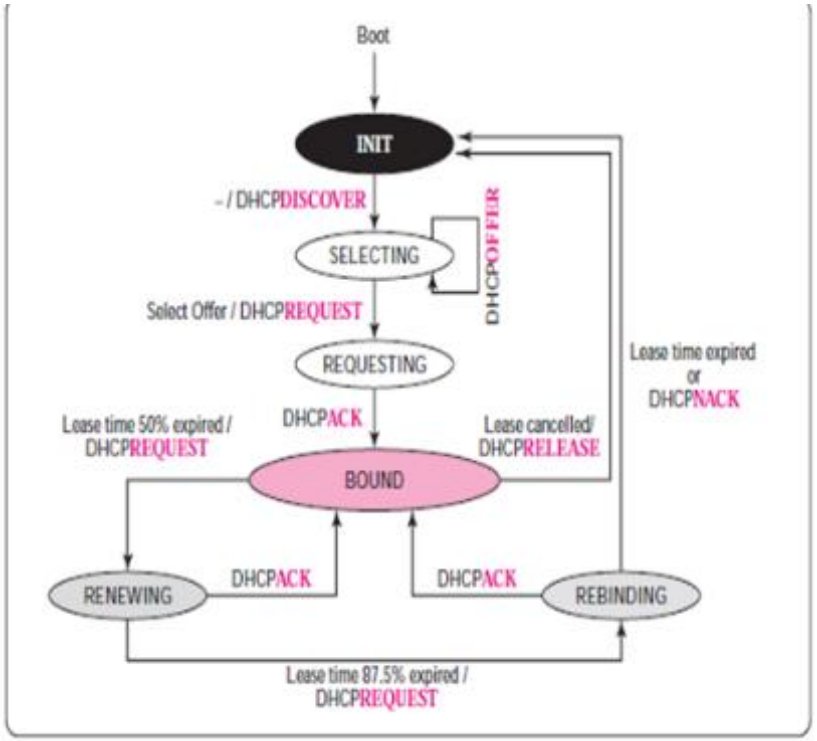
# Steps of DHCP: BOUND State

- In this state, the client can use the IP address until the lease 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 initializing state.



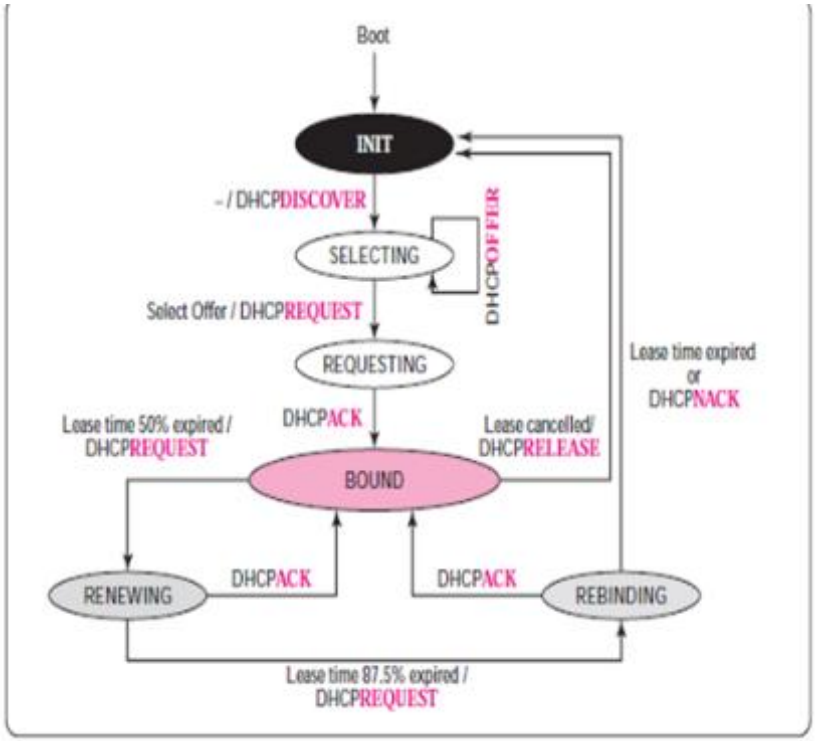
# Steps of DHCP: RENEWING State

- 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.



# Steps of DHCP: REBINDING State

- The client remains in the rebinding state until one of three events happens.
- If the client receives a DHCPNACK or the lease expires, it goes back to the initializing state and tries to get another IP address.
- If the client receives a DHCPACK, it goes to the bound state and resets the timer.



# DHCP Problem

- A Client pc is looking for an ip address. The DHCP server has offered three ip addresses (207.0.0.6/24, LT- 1 hr 14 min), (207.0.0.8/24, LT- 1 hr 28 min), (207.0.0.11/24, LT- 1 hr 32 min). The Client has chosen the 2nd ip address. If the client asks for extended LT of 22 minutes, What is the new timer of RENEWING and REBINDING states? While calculating timer for REBINDING state, consider the lease time was not extended in RENEWING state. [LT means lease time]

# What is ARP?

- In networking it is necessary for the sender to know the IP address and the Physical address of the receiver for successful communication. If the MAC address of the receiver is unknown to the sender; it uses **Address Resolution Protocol (ARP)** protocol to identify the specific MAC address of the receiver.

# ARP Request

PC – A
IP Add. : 10.0.0.5
MAC Add.
:AA:AA:AA:AA:AA

PC – B
IP Add. : 10.0.0.3
MAC Add.
:BB:BB:BB:BB:BB:BB

PC- C
IP Add. : 10.0.0.1
MAC Add.
:CC:CC:CC:CC:CC:CC

- In the above scenario there are three computers in a single network. PC-A wants to communicate with PC-C. But it only knows the IP address of PC-C. So, PC-A will take the help of ARP to get the MAC address of PC-C.

# ARP Request (cont.)

**Packet (Network layer):**


**Frame (Data Link layer):**

# ARP Request (cont.)

- After making the ARP request frame PC-A will broadcast the frame in the network. Assume that PC-B have got the frame it will read the header of the frame and find out the physical address (FFFF:FFFF:FFFF) as destination MAC address. Which means it's a broadcast MAC address and the frame is for everyone in that network. Therefore, PC-B will take the frame to the network layer. In the network layer when the destination IP address is checked. There will be a mismatch as PC-B doesn't hold the ip address 10.0.0.1.

# ARP Reply

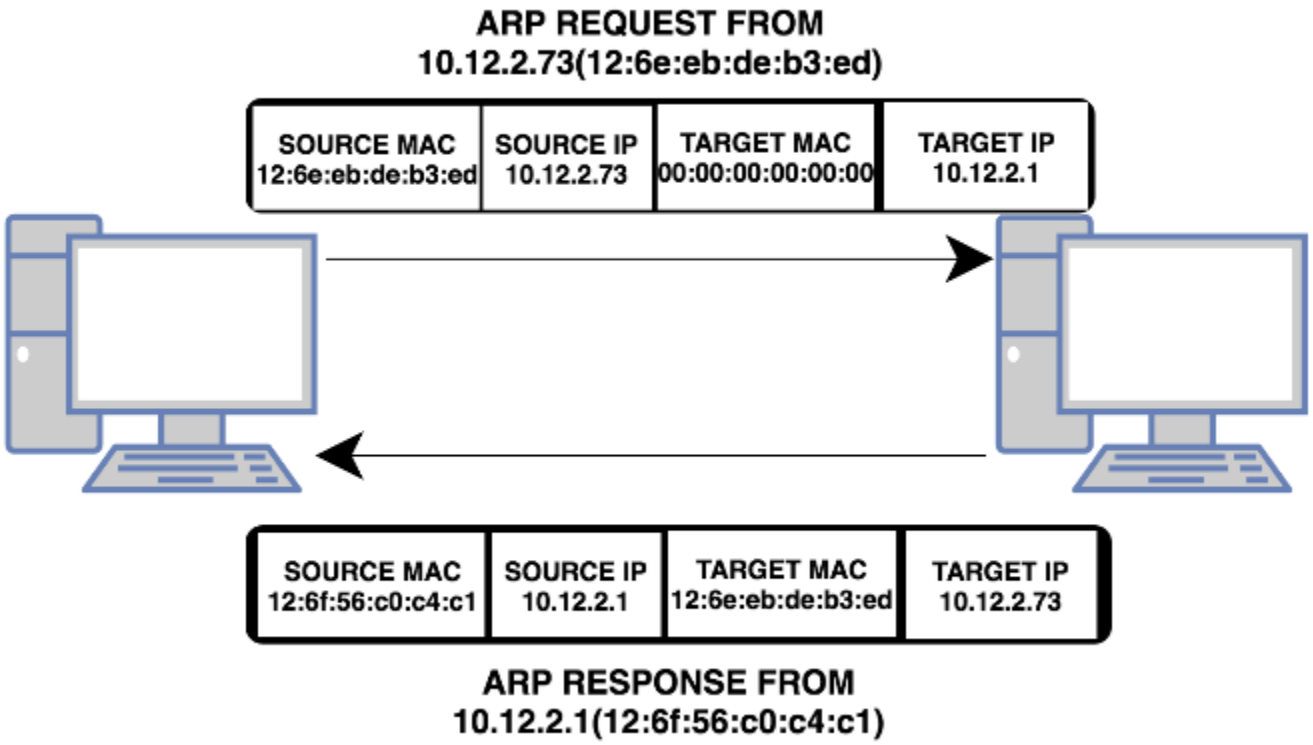
- On the other hand, when PC-C will get the frame it will read the header of the frame and find out the physical address (FFFF:FFFF:FFFF) as destination address. So, PC-C will transfer it to network layer. In network layer the host will check the destination IP and finds out that it matches with its own IP address. Therefore, PC-C will start reading the content of the packet. And it will make an ARP reply frame and send it back to PC- A.

# ARP Reply (cont.)

**Packet (Network layer):**


**Frame (Data Link layer):**

# ARP Example


ARP REQUEST FROM
10.12.2.73(12:6e:eb:de:b3:ed)
SOURCE MAC
12:6e:eb:de:b3:ed
SOURCE IP
10.12.2.73
TARGET MAC
00:00:00:00:00:00
TARGET IP
10.12.2.1
SOURCE MAC
12:6f:56:c0:c4:c1
SOURCE IP
10.12.2.1
TARGET MAC
12:6e:eb:de:b3:ed
TARGET IP
10.12.2.73
ARP RESPONSE FROM
10.12.2.1(12:6f:56:c0:c4:c1)

# ARP Cache Timeout

To reduce communication costs, computers that use ARP maintain a cache of recently acquired IP-to-physical address bindings. That is, whenever a computer sends an ARP request and receives an ARP reply, it saves the IP address and corresponding hardware address information in its cache for successive lookups. When transmitting a packet, a computer always looks in its cache for a binding before sending an ARP request. If it finds the desired binding in its ARP cache, the computer need not broadcast on the network. Thus, when two computers on a network communicate, they begin with an ARP request and response, and then repeatedly transfer packets without using ARP for each one. Experience shows that because most network communication involves more than one packet transfer, even a small cache is worthwhile.

# ARP Cache Timeout (cont.)

The ARP cache provides an example of *soft state*, a technique commonly used in network protocols. The name describes a situation in which information can become "stale" without warning. In the case of ARP, consider two computers, *A* and *B*, both connected to an Ethernet. Assume *A* has sent an ARP request, and *B* has replied. Further assume that after the exchange *B* crashes. Computer *A* will not receive any notification of the crash. Moreover, because it already has address binding information for *B* in its ARP cache, computer *A* will continue to send packets to *B*. The Ethernet hardware provides no indication that *B* is not on-line because Ethernet does not have guaranteed delivery. Thus, *A* has no way of knowing when information in its ARP cache has become incorrect.

# ARP Cache Timeout (cont.)

To accommodate soft state, responsibility for correctness lies with the owner of the information. Typically, protocols that implement soft state use timers, with the state information being deleted when the timer expires. For example, whenever address binding information is placed in an ARP cache, the protocol requires a timer to be set, with a typical timeout being 20 minutes. When the timer expires, the information must be removed. After removal there are two possibilities. If no further packets are sent to the destination, nothing occurs. If a packet must be sent to the destination and there is no binding present in the cache, the computer follows the normal procedure of broadcasting an ARP request and obtaining the binding. If the destination is still reachable, the binding will again be placed in the ARP cache. If not, the sender will discover that the destination is off-line.

# Advantage/Disadvantage

The use of soft state in ARP has advantages and disadvantages. The chief advantage arises from autonomy. First, a computer can determine when information in its ARP cache should be revalidated independent of other computers. Second, a sender does not need successful communication with the receiver or a third party to determine that a binding has become invalid; if a target does not respond to an ARP request, the sender will declare the target to be down. Third, the scheme does not rely on network hardware to provide reliable transfer. The chief disadvantage of soft state arises from delay — if the timer interval is $N$ seconds, a sender may not detect that a receiver has crashed until $N$ seconds elapse.

# References


1. **Data Communications and Networking**, *B. A. Forouzan*, McGraw-Hill, Inc., Fourth Edition, 2007, USA.
2. https://www.geeksforgeeks.org/basics-computer-networking/
3. https://www.tutorialspoint.com/computer_fundamentals/computer_networking.htm

# Books


1. **Data Communications and Networking**, *B. A. Forouzan*, McGraw-Hill, Inc., Fourth Edition, 2007, USA.
2. **Computer Networking: A Top-Down Approach**, *J. F., Kurose, K. W. Ross*, Pearson Education, Inc., Sixth Edition, USA.
3. **Official Cert Guide CCNA 200-301 , vol. 1**, *W. Odom*, Cisco Press, First Edition, 2019, USA.
4. **CCNA Routing and Switching**, *T. Lammle*, John Wily & Sons, Second Edition, 2016, USA.
5. **TCP/IP Protocol Suite**, *B. A. Forouzan*, McGraw-Hill, Inc., Fourth Edition, 2009, USA.
6. **Data and Computer Communication**, *W. Stallings*, Pearson Education, Inc., 10th Education, 2013, USA.