Computer Networks

Prepared by
Dr. Gaber Hassan

Lect_8

Some Important Protocols "Internet Layer Protocols"

1. Internet Protocol Version 4 (IPv4) (discussed previously)
2. Internet Control Messaging Protocol (ICMP)
3. Dynamic Host Configuration Protocol (DHCP)
4. Address Resolution Protocol (ARP)
5. Domain Name Service (DNS) (Application layer protocol)

Internet Control Messaging Protocol (ICMP)

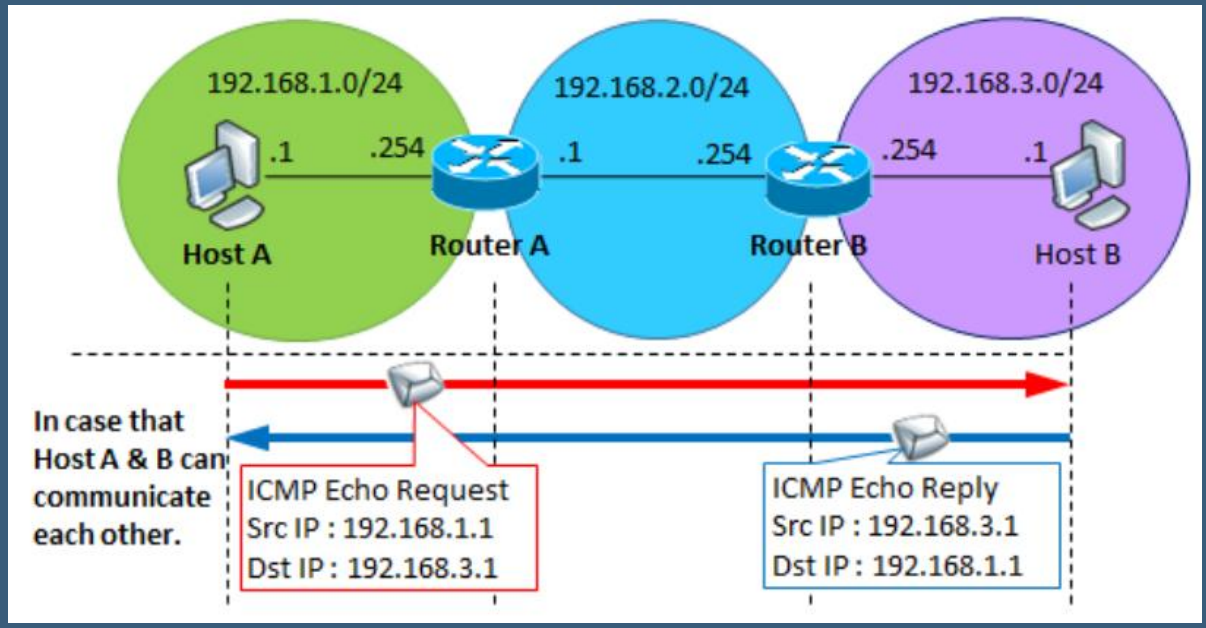
1. Internet Control Messaging Protocol (ICMP)
   - ICMP is an internet layer protocol
   - It used to send error and control information between TCP/IP devices.
   - It used for reporting errors and performing network diagnostics.
   - In the error reporting process, ICMP sends messages from the receiver to the sender where data does not come through as it should.
   - Hence, It responsible for troubleshoot end to end connectivity.

Internet Control Messaging Protocol (ICMP)

- ICMP, defined the RFC 792, includes many different messages, that device can generate or respond to.
- Here is a list of these messages:-
  - Address request
  - Address reply
  - Destination Un reachable
  - Echo (i.e., Echo request)
  - Echo Reply
  - .
  - .
  - .
- Here is the link for the RFC 792 document, https://datatracker.ietf.org/doc/html/rfc792

Internet Control Messaging Protocol (ICMP)

- The most common implementation using ICMP are ping and tracing:-
  1. Ping is used to test whether or not destination is available:-
     - A source generates an ICMP echo packet (echo request), if the destination is available, it will respond back with an echo reply, if not available a router will respond back with destination un reachable message.



Internet Control Messaging Protocol (ICMP)

➢Windows ping command

1. Open a Command Prompt.
2. In the Command Prompt window, type 'ping' followed by the destination, either an IP Address or a Domain Name, and press Enter.
3. The command will begin printing the results of the ping into the Command Prompt.

Command Prompt

```
Microsoft Windows [Version 10.0.18363.1556]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\G_Hassan>ping 192.168.1.5

Pinging 192.168.1.5 with 32 bytes of data:
Reply from 192.168.1.5: bytes=32 time<1ms TTL=128
Reply from 192.168.1.5: bytes=32 time<1ms TTL=128
Reply from 192.168.1.5: bytes=32 time<1ms TTL=128
Reply from 192.168.1.5: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

➢Windows tall ping command

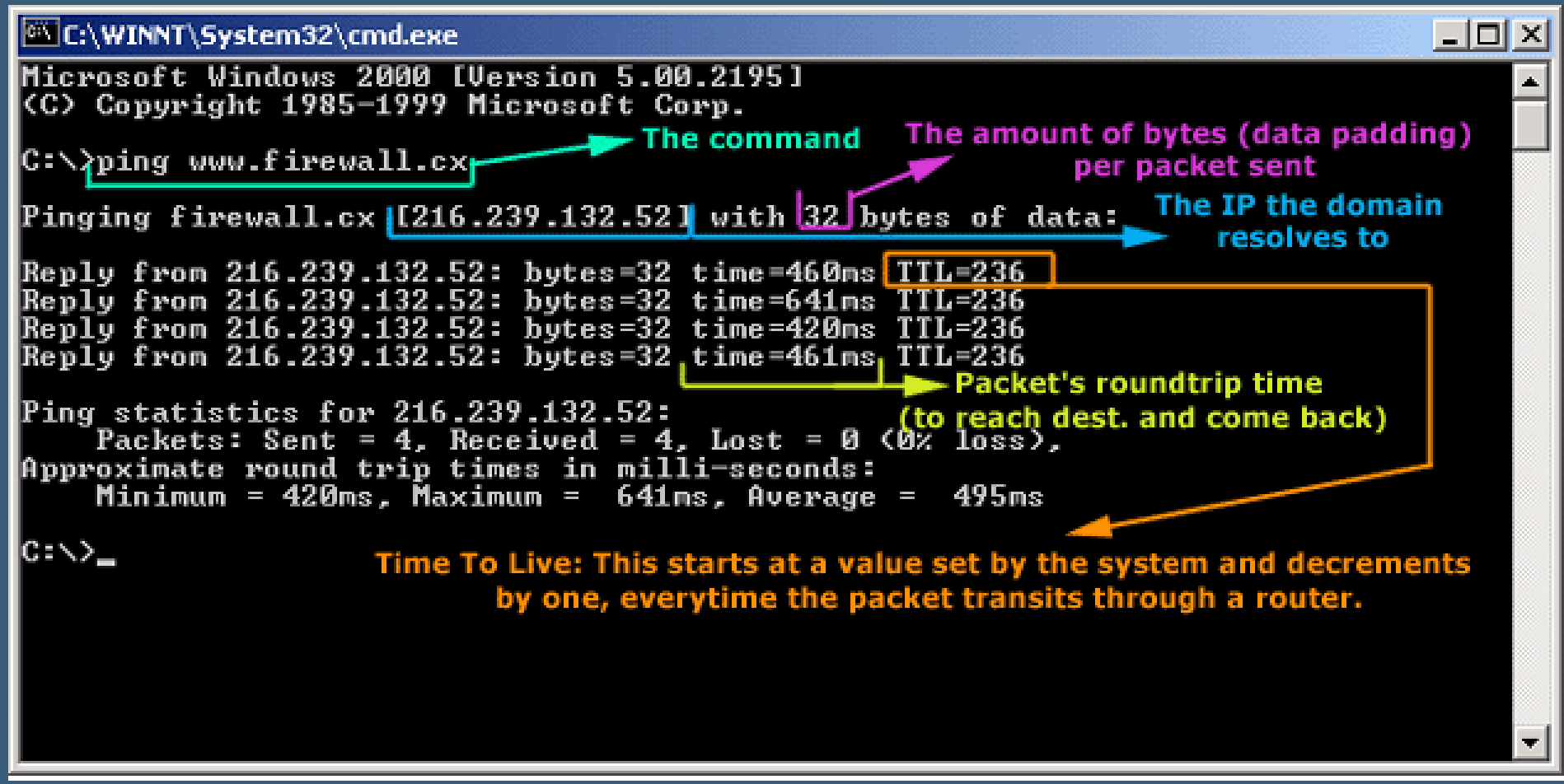
1. Type ping followed by the destination followed by –t.

Command Prompt

```
C:\Users\G_Hassan>ping 192.168.1.5 -t

Pinging 192.168.1.5 with 32 bytes of data:
Reply from 192.168.1.5: bytes=32 time<1ms TTL=128
Reply from 192.168.1.5: bytes=32 time<1ms TTL=128
Reply from 192.168.1.5: bytes=32 time<1ms TTL=128
Reply from 192.168.1.5: bytes=32 time<1ms TTL=128
Reply from 192.168.1.5: bytes=32 time<1ms TTL=128
Reply from 192.168.1.5: bytes=32 time<1ms TTL=128
Reply from 192.168.1.5: bytes=32 time<1ms TTL=128
Reply from 192.168.1.5: bytes=32 time<1ms TTL=128
Reply from 192.168.1.5: bytes=32 time<1ms TTL=128
Reply from 192.168.1.5: bytes=32 time<1ms TTL=128
Reply from 192.168.1.5: bytes=32 time<1ms TTL=128
Reply from 192.168.1.5: bytes=32 time<1ms TTL=128
Reply from 192.168.1.5: bytes=32 time<1ms TTL=128
Reply from 192.168.1.5: bytes=32 time<1ms TTL=128
Reply from 192.168.1.5: bytes=32 time<1ms TTL=128
Reply from 192.168.1.5: bytes=32 time<1ms TTL=128
Reply from 192.168.1.5: bytes=32 time<1ms TTL=128
Reply from 192.168.1.5: bytes=32 time<1ms TTL=128
Reply from 192.168.1.5: bytes=32 time<1ms TTL=128
Reply from 192.168.1.5: bytes=32 time<1ms TTL=128
Reply from 192.168.1.5: bytes=32 time<1ms TTL=128
Reply from 192.168.1.5: bytes=32 time<1ms TTL=128
Reply from 192.168.1.5: bytes=32 time<1ms TTL=128
Reply from 192.168.1.5: bytes=32 time<1ms TTL=128
Reply from 192.168.1.5: bytes=32 time<1ms TTL=128
Reply from 192.168.1.5: bytes=32 time<1ms TTL=128
```

Internet Control Messaging Protocol (ICMP)

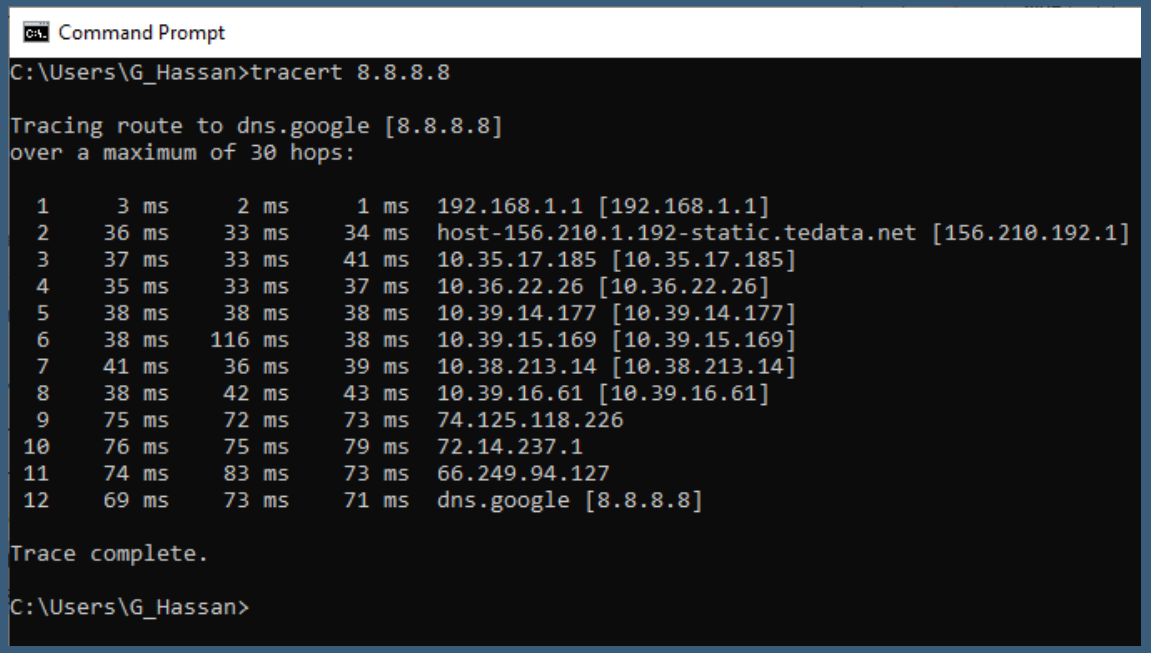


Internet Control Messaging Protocol (ICMP)

2. Tracing or traceroute is used to trace the probable path a packet taken between source and destination

➢Windows tracing command

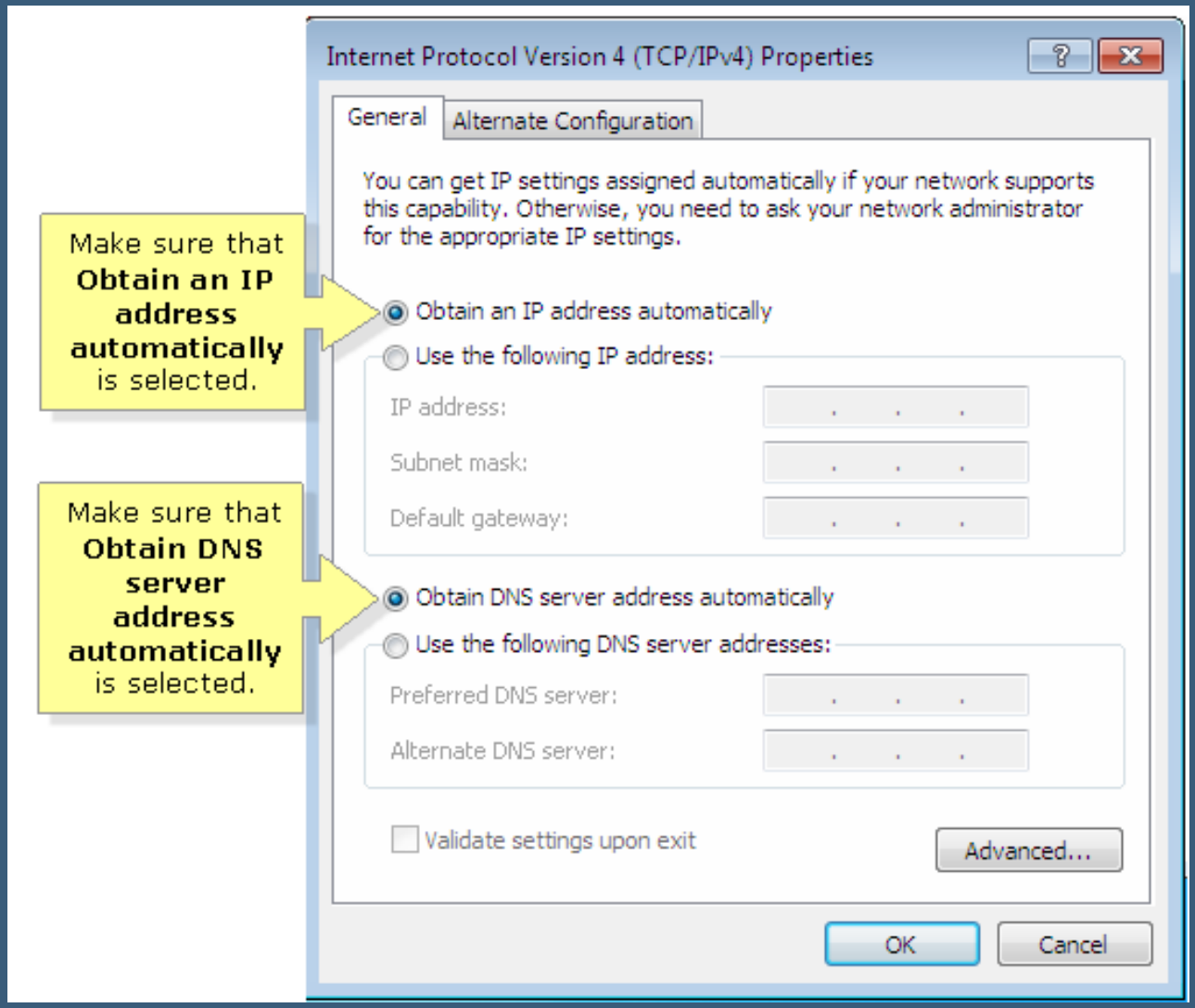
1. Open a Command Prompt.
2. In the Command Prompt window, type ‘tracert' followed by the destination, either an IP Address or a Domain Name, and press Enter.
3. The command will return output indicating the hops discovered and time (in milliseconds) for each hop.



Dynamic Host Configuration Protocol (DHCP)

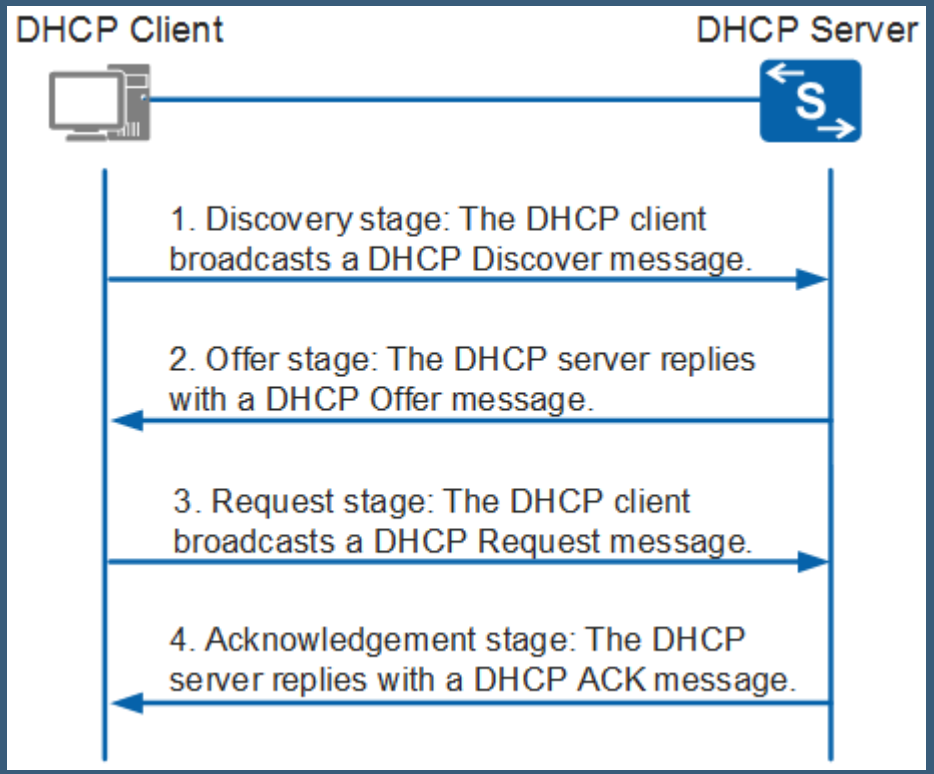
2. Dynamic Host Configuration Protocol (DHCP)
   - DHCP is an application layer protocol, but used in an internet layer for automatically assigning IP address.
   - DHCP allows devices to dynamically acquire their addressing information.
   - This information can include:-
     1. A client IP address.
     2. Subnet mask.
     3. A default gateway.
     4. DNS
   - DHCP Server: It is typically a server or a router that holds the network configuration information.
   - A DHCP server is configured with a pool of available IP addresses and assigns one of them to the DHCP client. A Cisco router can be configured as a DHCP server.

Dynamic Host Configuration Protocol (DHCP)

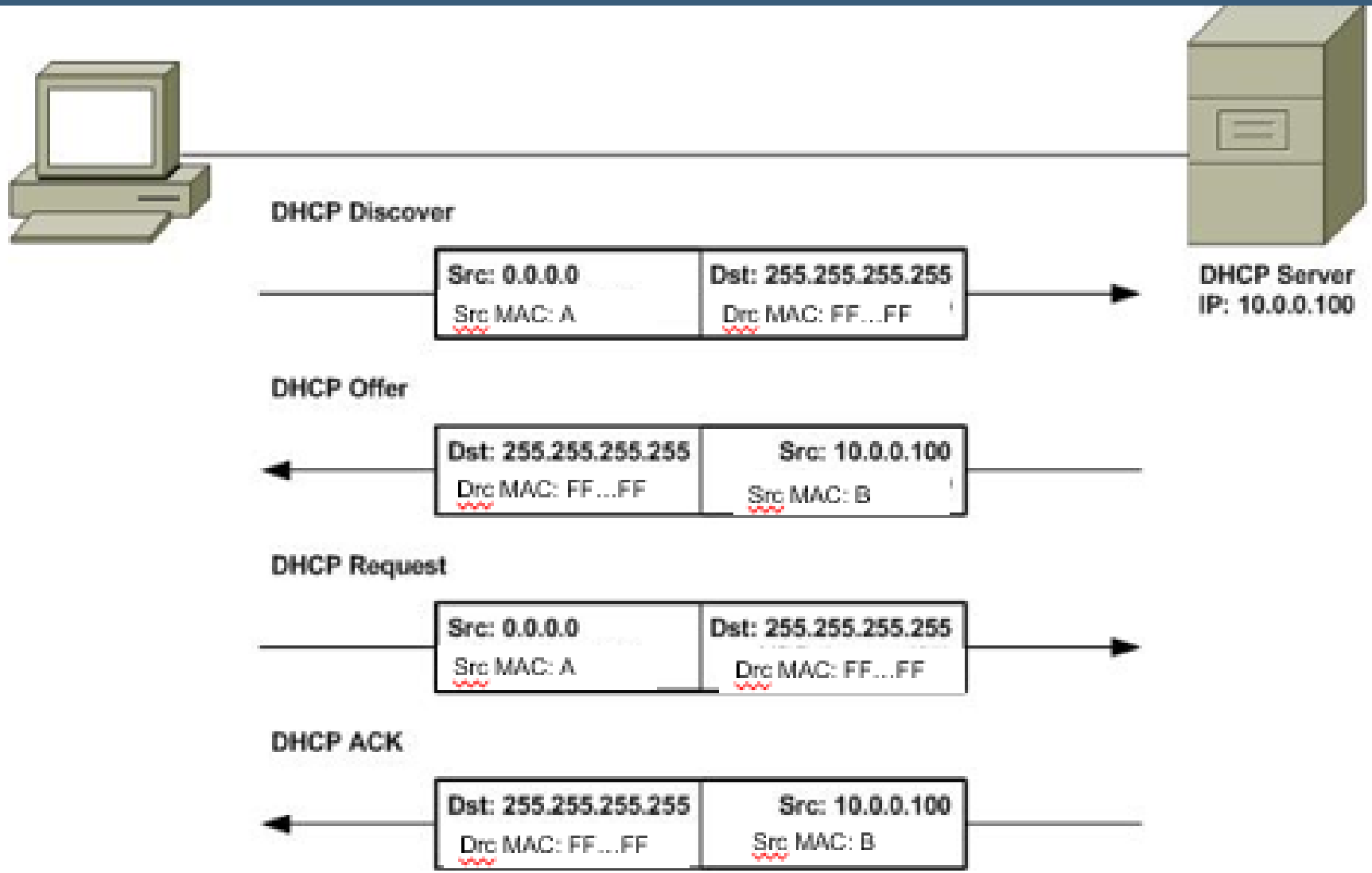


Dynamic Host Configuration Protocol (DHCP)

- By default, home routers set to use DHCP, whereas each connected device will receive the necessary settings from the router. Therefore, on your home network, your router serves as a simple DHCP server that assigns this information to hosts.



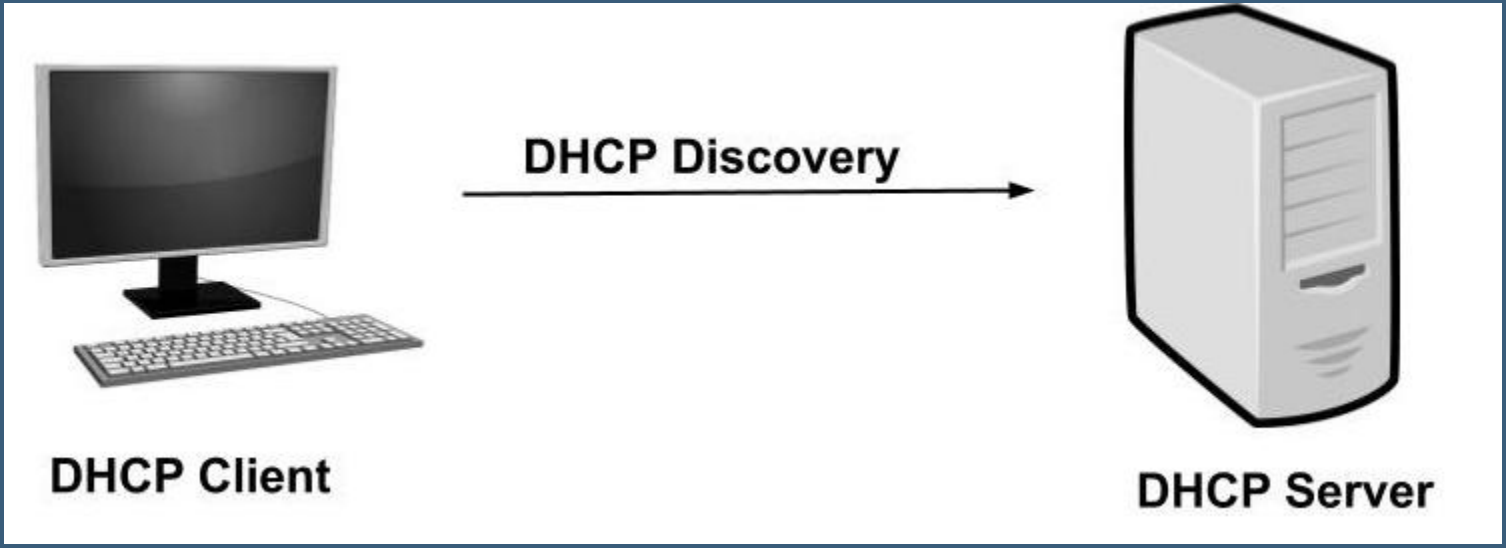
Dynamic Host Configuration Protocol (DHCP)



Dynamic Host Configuration Protocol (DHCP)

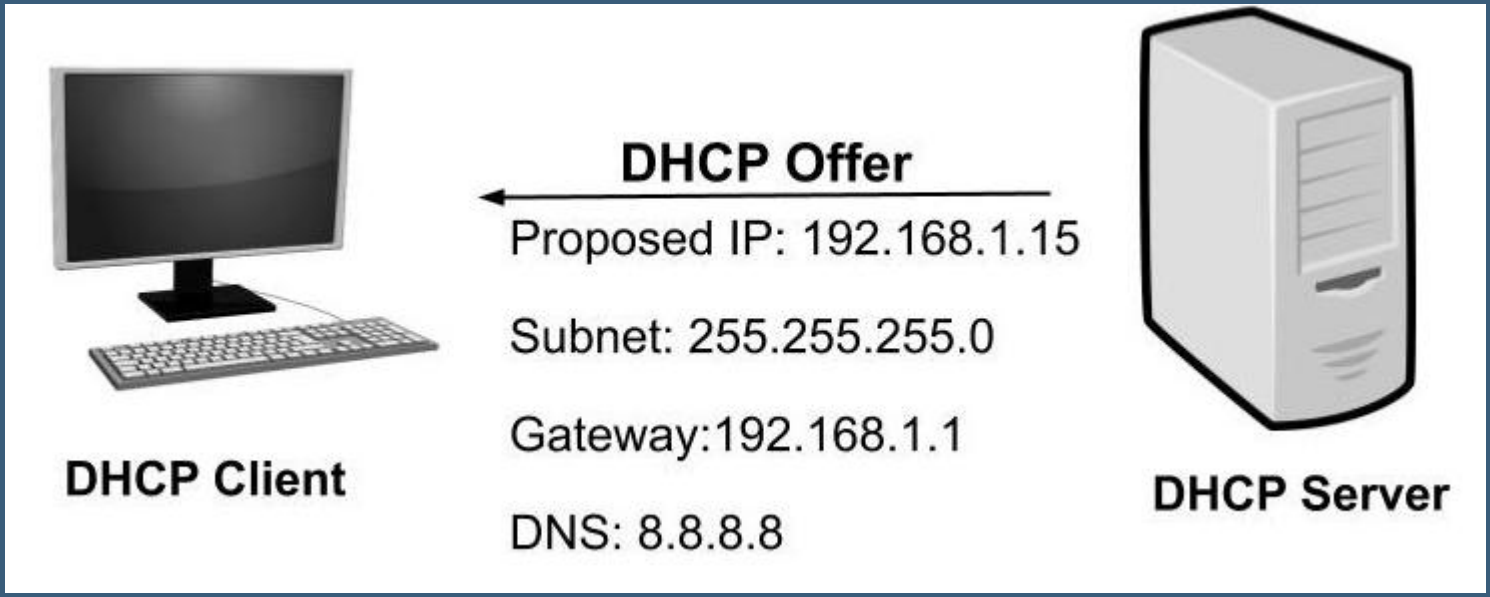
- **How do DHCP works?**

1. **DHCP Discovery:** The DHCP client broadcast messages to discover the DHCP servers. The client computer sends a packet with the default broadcast destination of **255.255.255.255,** it lets you send a broadcast packet to the network you're connected to.



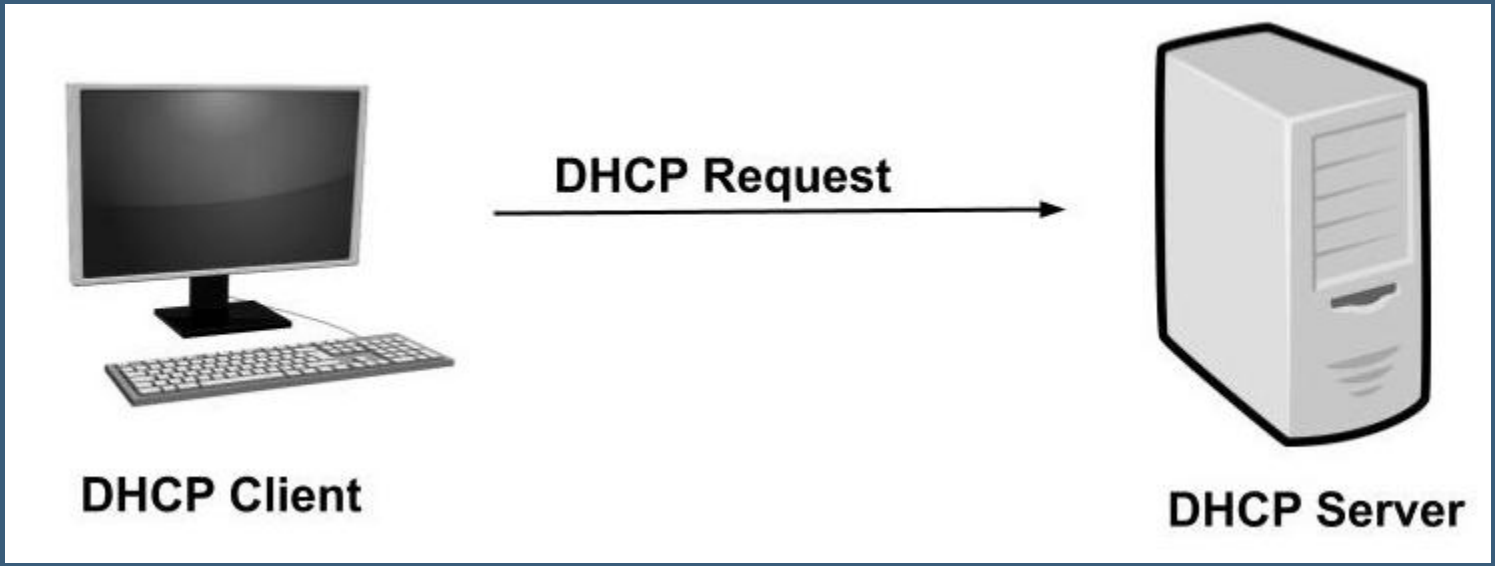
Dynamic Host Configuration Protocol (DHCP)

2. **DHCP Offer:** When the DHCP server receives the DHCP Discover message then it suggests or offers an IP address(form IP address pool) to the client by sending a DHCP offer message to the client. This DHCP offer message contains the proposed IP address for DHCP client, subnet mask, default gateway, and DNS address.



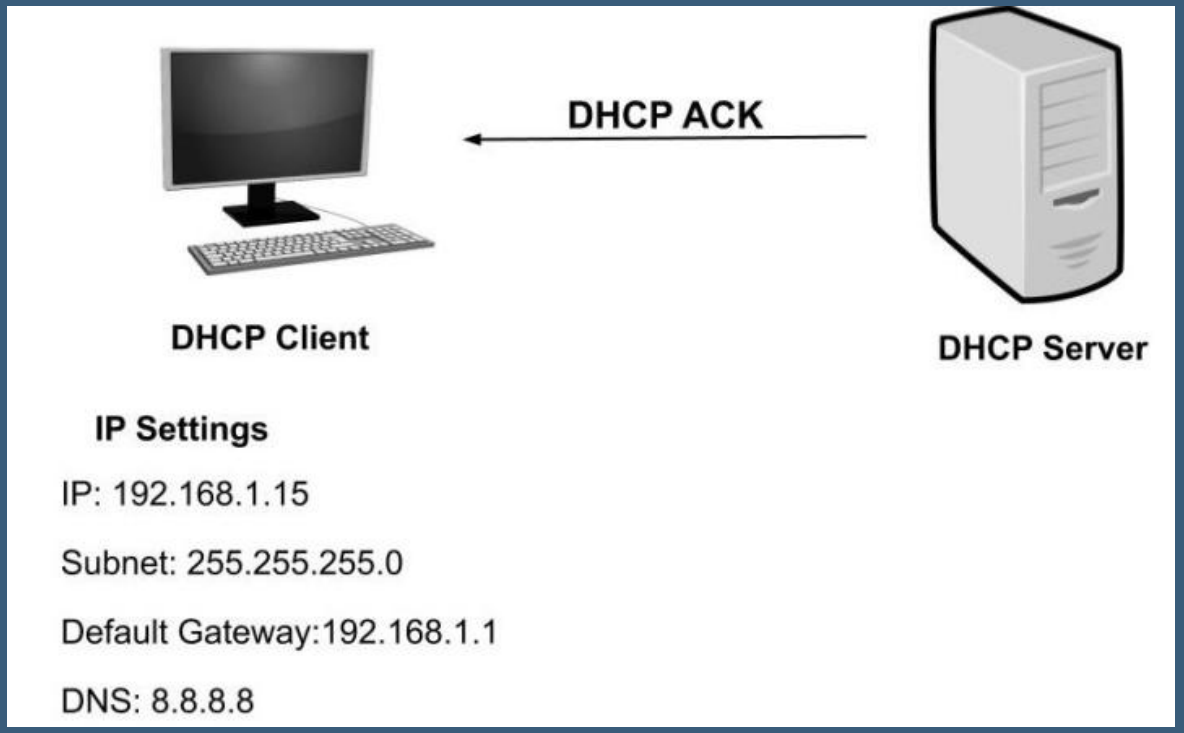
Dynamic Host Configuration Protocol (DHCP)

3. **DHCP Request :** The client sends a DHCP Request requesting the offered address from one of the DHCP servers.



Dynamic Host Configuration Protocol (DHCP)

4. **DHCP Acknowledgment:** The server then sends Acknowledgment to the client confirming the DHCP lease to the client. The server might send any other configuration that the client may have asked. At this step, the IP configuration is completed and the client can use the new IP settings.



Dynamic Host Configuration Protocol (DHCP)

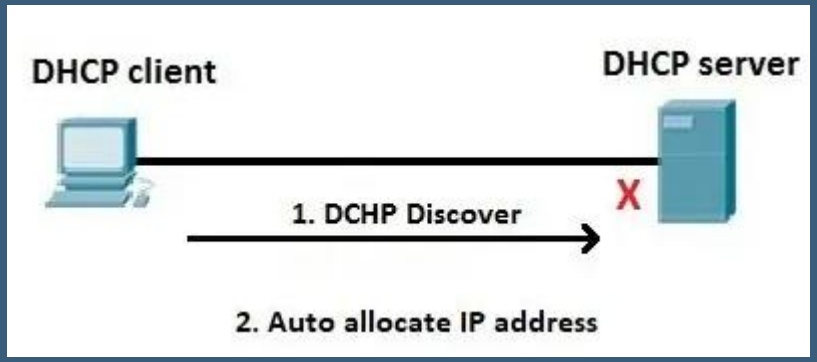
- **Advantages of DHCP**
  1. It is easy to implement and automatic assignment of an IP address means an accurate IP address.
  2. The manual configuration of the IP address is not required. Hence, it saves time and workload for the network administrators.
  3. Duplicate or invalid IP assignments are not there which means there is no IP address conflict.
  4. It is a great benefit for mobile users as the new valid configurations are automatically obtained when they change their network.

Automatic Private IP Addressing (APIPA)

- **Automatic Private IP Addressing (APIPA)**
  1. APIPA is a feature in operating systems (such as Windows) that enables computers to automatically self-configure an IP address and subnet mask when their DHCP server isn't reachable.
  2. The Internet Assigned Numbers Authority (IANA) has reserved 169.254.0.0 to 169.254.255.255 with a subnet mask of 255.255.0.0. for Automatic Private IP Addressing.
  3. If the client can't communicate with the DHCP server, it uses APIPA to configure itself with an IP address from the APIPA range.
  4. Note that the computer cannot communicate with computers on other subnets, or with computers that do not use automatic private IP addressing.
  5. This way, the host will still be able to communicate with other hosts on the local network segment that are also configured for APIPA.

Automatic Private IP Addressing (APIPA)

- Consider the following example:



1. The host on the left is configured as DHCP client (Obtain an IP address automatically) .
2. The host boots up and looks for DHCP servers on the network. However, the DHCP server is down and can't respond to the host.
3. After some time (from a couple of seconds to a couple of minutes, depending on the operating system) the client auto-configures itself with an address from the APIPA range (e.g. 169.254.154.22).
4. The client uses Address Resolution Protocol (ARP) to ensure that the chosen address is not already being used by another network computer.

Automatic Private IP Addressing (APIPA)

- The APIPA service also checks regularly for the presence of a DHCP server (every three minutes). If it detects a DHCP server on the network, the DHCP server replaces the APIPA networking addresses with dynamically assigned addresses.

- **Disadvantages**

1. APIPA is considered non routable approach, where, does not provide network gateway and DNS as DHCP does.
2. Hence it enables client to communicate only inside LAN.

Address Resolution Protocol (ARP)

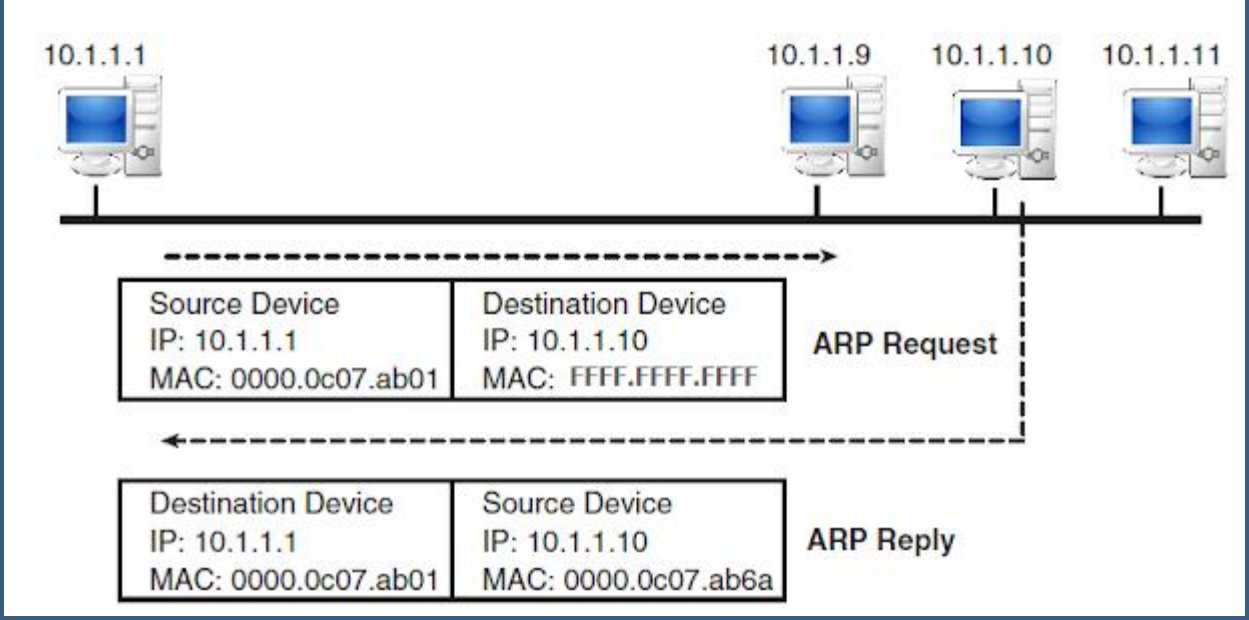
3. Address Resolution Protocol (ARP)
   - It is an internet layer protocol that helps TCP/IP devices find other devices in the same broadcast domain.
   - ARP responsible for determine the next MAC.
   - ARP used to map the logical IP address to the physical MAC address.
   - Both IPs and MACs of network devices stored in ARP table (ARP Cache).
   - The ARP table is used to maintain a correlation between each MAC address and its corresponding IP address.

ARP Table	
IP Address	MAC Address
176.10.16.3	FE:ED:31:22:AA:09
176.10.16.6	FE:ED:31:A2:22:F3
176.10.16.5	FE:ED:31:A2:22:77
176.10.16.2	FE:ED:31:A3:47:14

   - RFC 826 does not give a specific timeout value for ARP cache entries, so each vendor implements this value differently.
   - The typical timeout for ARP Cache is 10 to 20 minutes, but the cache is cleared automatically. The next time the PC or any device requests for that address, a fresh mapping is required.

Address Resolution Protocol (ARP)

- Example 1:-
  - ARP request is broadcast FF-FF-FF-FF-FF-FF.
  - ARP reply is unicast.



Address Resolution Protocol (ARP)

Detailed Example 1:-

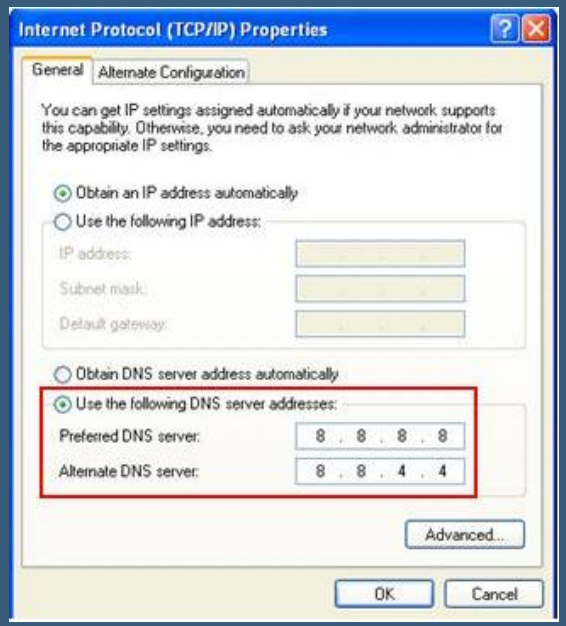
- Two computers in an office (Computer 1 and Computer 2) are connected to each other in a local area network by Ethernet cables and network switches, with no intervening gateways or routers.
- Computer 1 has a packet to send to Computer 2. Through DNS, it determines that Computer 2 has the IP address 10.1.1.10.
- To send the message, it also requires Computer 2's MAC address. First, Computer 1 uses a cached ARP table to look up 10.1.1.10 for any existing records of Computer 2's MAC address (0000:0c07:ab6a).
- If the MAC address is found, it sends an Ethernet frame containing the IP packet onto the link with the destination address 0000:0c07:ab6a.
- If the cache did not produce a result for 192.168.0.55, Computer 1 has to send a broadcast ARP request message (destination FF:FF:FF:FF:FF:FF MAC address), which is accepted by all computers on the local network, requesting an answer for 10.1.1.10.
- Computer 2 responds with an ARP response message containing its MAC and IP addresses.
- As part of fielding the request, Computer 2 may insert an entry for Computer 1 into its ARP table for future use.
- Computer 1 receives and caches the response information in its ARP table and can now send the packet.

Domain Name Service (DNS)

4. Domain Name Service (DNS)
   - DNS is an application layer protocol
   - DNS is the phonebook of the internet.
   - Each device connected to the internet (e.g., google, facebook, youtube…) has a unique IP address which other machines can use to find it. DNS eliminate the need for humans to memorise IP addresses.
   - Human access information online through domain name named, like WWW.youtube.com. DNS translates domain name to IP address so browser can load internet resources.
   - DNS responsible for detect destination IP.

Domain Name Service (DNS)

- Examples of DNS servers:-
  1. Google DNS
     - It has the IP address 8.8.8.8 or 8.8.4.4
  2. WE DNS server
     - It has the IP address 163.121.128.134 or 163.121.128.135
  3. Orange DNS
     - It has the IP address 213.131.65.20 or 213.131.66.246



THANK YOU

For any questions feel free
to contact me by mail

Gh_mcs86@yahoo.com