DHCP (D-IETF, 1990s, Stand- 1993-RFC-1531, 2131)

virtual machine: It is a software-based computer that runs inside your real computer
It runs inside software like:
vmware, virtual Box, Hyper-V
└ These supports installation of windows, Linux or any OS in a vm
- It is work similar to a real PC.

DC-1, DC-2, DC-3 (Domain Controllers):
→ DC stands for Domain controller.
→ These are special servers that manage the domain.
→ A Domain is a group of computers and users managed under one central system (like in schools, offices, or companies).
→ DCs run Active Directory (AD), which stores:
• usernames and passwords • Security rules
→ Multiple DCs are used for:
• Backup (if DC-1 fails, DC2 still works)
• Split the work between DCs (Load Sharing)
→ IP Address: usually static (manual), dynamic (DHCP), so clients always find them.

Client-1, client-2 (client computers):
→ These are normal user computers (like windows 10 or 11).
→ They are joined to the domain, which means they log in using account created on the DC.
→ They can perform/Access:
• Access Shared Folder
• Get security setting from the domain
• use shared printers or internet safely

__/__/____

Member-1, Member-2 (Member Servers):

→ These are servers that are part of the domain, but not domain controllers. (member — belong to the domain)

→ They do other important tasks like:

- Hosting websites (IIS, Apache)
- Runnig databases (SQL)
- File Sharing
- Printing Services
- Acting as a DHCP Server

=> Member-1: File Server Member-2: DHCP + DNS Server

DHCP: (Dynamic Host configuration protocol)

→ It is a network Service that automatically gives IP address to computers, PC, and any device connected to it.

→ Usually, one of the Devices (like Member-1 or DC-1) has the DHCP role installed.

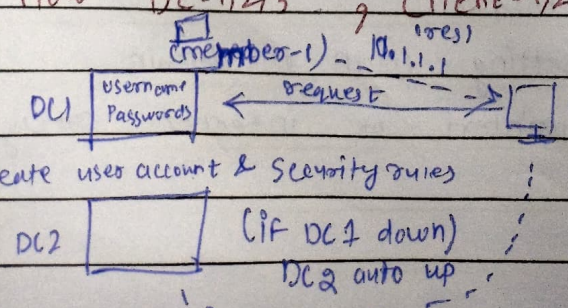
→ what happens if a client tries to connect?

- it sends a request: say "can i have a IP address please"
- The DHCP server replies: " Here is your IP, gateway, and DNS info."

→ why dhcp is important:

- Saves time
- Reduces mistakes (no Human error)
- Easy to manage large networks

Q- How DC-1,2,3 & Client-1,2 all work together ??



__/__/____

DHCP Lease Generation

Def: It means the DHCP server gives a device An ip address for a limited amount of time, called a lease. This process is part of how IP addresses are managed efficiently in a network.

→ what is a lease ?? (duration: Fixed time like 8hours, 1day etc.)

- A lease is a temporary agreement between the DHCP server and DHCP Client.
- what clients get ?

  The client gets: (An ip Address, A subnet mask, default gateway etc.)

→ It includes 4 steps. They are called DORA.

i) Discover:

A client who needs an ip address, and it's been configured to get it automatically from a DHCP server, it needs to discover presence of any DHCP servers on the Network. So it will do a broadcast.

Q. broadcast:

client says: I'm a client, I need an IP address, is there any dhcp server?? (It goes to next step)

ii) Offer:

Any dhcp servers on the network which hear that broadcast, they will go ahead and make an offer back to the client.

Servers says: Yes, I am dhcp server, and i have an IP address for you. (It goes to step 3)

iii) Request:

when a client receives an offer packet, it decapsulate it check the ip address.

client says: client request back to the dhcp and says, yes, i would indeed like that IP address. I am gonna take that ip address. If more than one messages receives it,

it chooses the first one.

(iv) Acknowledge:

DHCP Server responses back to client with an acknowledgment

Server says: okay it's yours, i logged in my database (DC, member) and you can use it until expiration time period.

DHCP Lease Renewal:

when a computer gets an IP address from DHCP Server, it's like renting it for a set time (this is called lease).

Q. what is Lease renewal?

Your computer is asking the DHCP Server: Can i keep this same IP address for longer?"

Q. When it does happen? (at least of 50% lease duration expires)

Let's say your lease time is 2 hours.

Your pc will try to renew the lease when half the time is over.

If successful, it can keep the same IP and the lease starts fresh again.

Q. why client doesn't go with fully dora process?

Because the client has already discovered the server in the previous DORA Process.

-> client sends a request to the DHCP Server

-> Server replies with an acknowledge packet says: you got it, you can use that IP address

NOTE:
- A client will attempt to renew its lease after 50% of the lease duration has expired.
- If the client fails to renew its lease after 87.5% of the lease has expired, then the full DHCP lease generation process starts over again.

Extra Four DHCP Messages:

__/__/__

iv) DHCP NACK:

It is a message sent by the DHCP Server to tell a device: "X The ip address you asked for is not valid".

Q. When does it happen?

when the client tries to use an invalid or wrong IP, often from a different network.

- You move your laptop from your home network to office network
- The laptop tries to use its old home IP.
- The office DHCP Server says: "That IP doesn't belong here!" Sends DHCP NAK

→ Force device to start the IP request process again and get a correct IP.

vi) DHCP Decline:

It is a message send by the client to the DHCP Server to say: "The IP address you gave me is already in use."

→ To avoid IP address conflict (uses garp for duplicacy check)

vii) DHCP Release:

A DHCP release is a message sent by the client to the DHCP Server to say:

"I am done using this IP. You can give it to someone else."

→ happens: device shutdown, disconnects, or change networks

→ used: To help the server reuse the IP address quickly

viii) DHCP Inform:

A DHCP Inform is a message sent by the client to the DHCP Server saying:

"I already have an ip address, just give me extra info like DNS, gateway, etc."

→ happens: when a device has a static IP but still wants DHCP options like: Default gateway, DNS Server, Domain Name

→ used: with manual IPs to still get network setting automatically

__/__/____

DHCP Reservation:

Def: DHCP server remembers the device's MAC address and always gives it the same IP every time it connects.

→ used / Required:

- Consistency - Devices like printers, servers or CCTV system need same IP always so others can find them easily.

DHCP Relay Agent (IP Helper Address):

Def: A DHCP Relay Agent is a device (usually router or L3 switch) that forwards DHCP Requests from client in one subnet to DHCP server in another subnet.

→ Required: DHCP discover messages are broadcasts don't cross routers by default.

If the DHCP server is on a different network (subnet), clients can't reach it.

DHCP Options: (Q. why Request is broadcast)

Def: DHCP Options are extra setting sent by the DHCP Server to the client along with the IP address.

→ Option 3 - default Gateway
→ Option 6 - DNS Server
→ option 15 - Domain Name
→ 53 - DHCP Message Type (Request / Res)
→ 54 - Server identifier
→ 61 - Client identifier
→ 50 - Requested IP address
→ 255 - end

DHCP Snooping: (DHCP Inspection)

It is a security feature on switches that helps stop fake (unauthorized) DHCP servers from giving out IP addresses in your network.

__/__/____

→ ~~Used~~ ~~when~~ (~~required~~): Why it is impotant?

In a LAN, anyone can plug in a laptop and run a rogue DHCP server, which could:

- Give wrong IP addresses
- Redirect traffic
- Launch Man-in-the-Middle (MITM) attacks
- Break network access

→ used: DHCP Snooping prevents this by letting the switch decide who is allowed to send DHCP offers.

→ How it works:

- Switch learns and trust which port the real DHCP server is on.
- Other ports are marked untrusted.
- when an untrusted port tries to send a DHCP offer, ACK etc, It is blocked.

DHCP in virtual Machines:

Def: when you connect or run a virtual machine (VM) (like in Vmware, Virtual Box, or Hyper-v), it needs an IP address to connect to the internet or local network.

Just like physical computers, VMs also use DHCP to automatically get IPs.

→ How does your VM get IP using DHCP?

It depends on how the VM is connected to the network.

Your VM software gives you 3 options:

i) NAT

- Think of NAT like sharing your interface from your main pc to your VM.
- It gets IP from virtual DHCP (inside your VM software)

ii) Bridge Network (used for Testing, servers, pinging other devices)

- VM gets IP from your real network's DHCP server
- VM acts like a real PC on the network

__/__/____

iii) Host only network:

- VM gets IP from virtual DHCP
- VM can only talk to the host PC, not to the internet or LAN
- Good for: Safe labs, local testing, offline environments.

Q. Why client send broadcast in request message after getting ~~the~~ ~~IP~~ knowing the server ip in offer message??

A: Choose and confirm the DHCP offer

→ multiple DHCP servers might send offers.

→ The client picks one offer and sends a DHCP request broadcast to tell all DHCP servers:

"I am ~~saying~~ accepting this offer from Server X."

"The other should withdraw their offers."