***Research Findings***

**Author: Vineeth M**

**Date: 21,10,2025**

***1.IP Addressing (Dynamic IP addressing)­.***

***IP addressing refers to the process of assigning a unique number, called an IP address, to every device connected to a network. When a device connects to a router in a home network or a cellular tower in a mobile network, it initially does not have an IP address. The device then automatically requests an address from the network, and this process of automatically assigning an IP address is known as Dynamic IP addressing. And Dynamic Host Configuration Protocol is a network protocol used to automate the process of assigning IP addresses and other network configuration parameters to devices (such as computers, smartphones and printers) on a network.***

# *****Dynamic Host Configuration Protocol (DHCP)*****

***What Is dhcp***

***Dynamic Host Configuration Protocol (DHCP) is a network protocol that automatically assigns IP addresses to devices when they connect to a network. Instead of manually configuring each device, DHCP allows devices to receive all the necessary network information automatically, including IP address, subnet mask, default gateway, and DNS server addresses, making network setup faster and easier.***

***The IP address identifies the device on the network, while the subnet mask defines the local network range. The default gateway, usually the router’s IP, acts as the exit point for sending data to other networks, including the internet. The DNS server addresses, typically from the ISP, allow the device to translate domain names (like*** *www.google.com****) into IP addresses, enabling it to connect to websites easily.***

### *****Components of DHCP*****

1. ***DHCP Server:*** *Holds IP addresses and other network configuration information.*
2. ***DHCP Client:*** *Any device (mobile, laptop, computer, etc.) that receives IP and configuration from the server.*
3. ***DHCP Relay:*** *Acts as a communication channel between DHCP clients and servers, especially across networks.*
4. ***IP Address Pool:*** *The range of IP addresses available on the DHCP server for allocation.*
5. ***Lease:*** *The time period an assigned IP is valid; after expiration, the IP must be re-assigned.*

*****Attacks Related DHCP*****

*****DHCP Starvation*****

***DHCP starvation is an attack where an attacker floods the DHCP server with fake DHCP requests (using many spoofed MAC addresses) to exhaust the pool of available IP addresses — causing legitimate clients to fail to get an IP and disrupting network access.***

***Rogue DHCP Server Attack***

***In a rogue DHCP server attack, the malicious device pretends to be the router (or the real DHCP server). It gives fake IP addresses, gateway, and DNS info to other devices, so those devices send their traffic through the attacker instead of the real router. This allows the attacker to intercept or manipulate network traffic, like a man-in-the-middle.***

*****DHCP Spoofing*****

***DHCP spoofing (rogue lease injection) is when an attacker sends fake DHCP replies to clients so those clients use wrong IP settings (gateway, DNS). That can break connectivity or let the attacker intercept traffic.***

*****Mitigation Statergies*****

***1. Enable DHCP Snooping (switch)***

***DHCP snooping helps keep the network safe by checking which ports are trusted (for DHCP servers) and which are not (for devices). It only allows real DHCP messages from trusted ports, limits too many requests from untrusted ports, keeps track of assigned IPs, and blocks fake or wrong messages to stop attackers from using up IP addresses.***

*****2.Port Security (switch)*****

***Port security helps stop DHCP starvation attacks by limiting how many devices (MAC addresses) can connect to a single port. This prevents attackers from using fake MAC addresses to flood the DHCP server with requests, working together with DHCP snooping to protect the network.***

*****3.Rate Limiting DHCP Requests*****

***Rate limiting DHCP requests helps protect the network from attacks that try to flood the DHCP server with fake requests. It works by setting a limit on how many DHCP packets a device can send per second. For example, on Cisco switches, you can use the command*** *ip dhcp snooping limit rate <number>* ***to control this. If a device sends too many requests, the switch blocks the extra ones, keeping the DHCP server safe and stable.***

*****4.Monitor and Log DHCP Activity*****

*Monitoring and logging DHCP activity helps detect and prevent network attacks such as DHCP starvation or misuse. By keeping track of DHCP server logs, administrators can notice unusual patterns like too many IP requests from one device or quick depletion of IP leases. Tools like* ***Syslog*** *and* ***SNMP*** *can be used to record these events and send alerts when something suspicious happens. This allows quick action to stop potential attacks and maintain stable network performance.*

***5.Intrusion Detection/Prevention Systems (IDS/IPS)***

*Intrusion Detection and Prevention Systems (IDS/IPS) are security tools that monitor network traffic to detect and stop suspicious activity. In the case of DHCP, IDS/IPS can watch for unusual patterns, like a single device sending a large number of DHCPDISCOVER messages, which could indicate a DHCP starvation attack. When such activity is detected, the system can alert administrators or automatically block the malicious traffic, helping to protect the network and the DHCP server.*

***6.Enable* ***Dynamic ARP Inspection (DAI)*****

***Dynamic ARP Inspection (DAI) works by monitoring ARP messages on the network and allowing only legitimate ones. It first builds a trusted list, called the binding table, using DHCP Snooping to record valid IP-to-MAC pairs for each device. When a device sends an ARP message asking “Who has this IP?”, the switch checks it against the binding table. If the ARP packet matches, it is allowed; if it doesn’t, the switch blocks or drops it to prevent spoofing. DAI also distinguishes between trusted and untrusted ports: ports connected to other switches or routers are trusted, so their ARP messages are not inspected, while ports connected to end devices are untrusted and are fully checked. This ensures that only valid ARP messages are permitted, protecting the network from attacks like ARP spoofing and man-in-the-middle attempts.***

***2.Subnetting***

***Subnetting*** *is the process of dividing a large network into smaller, more manageable subnetworks called subnets. It helps organize IP addresses, improves network performance, and enhances security by controlling which devices can communicate directly. In real-life situations, subnetting is used when a company has multiple departments—like HR, Finance, and IT—so each department can have its own subnet, reducing network congestion and isolating traffic. It’s also used by Internet Service Providers (ISPs) to allocate IP ranges efficiently to different customers, or in home networks when creating separate subnets for devices like computers, smart TVs, and security cameras to improve management and security. By using subnetting, networks become easier to manage, more secure, and more efficient.*

***Fixed Length Subnet Masking (FLSM):*** *is a subnetting method where all subnets are given the same subnet mask and contain the same number of IP addresses. It is simple to design and manage but often leads to wasted IP addresses because every subnet gets an equal size, even if some have only a few devices. For example, if you divide a /24 network into four subnets, each will have 64 IPs, even if one subnet only needs 5 devices.*

***Variable Length Subnet Masking (VLSM):*** *on the other hand, allows subnets of different sizes within the same network. This means network administrators can assign IP addresses based on the actual number of devices needed in each subnet. For instance, a /26 subnet (64 IPs) can be used for a large department, while a /30 subnet (4 IPs) can be used for a point-to-point link. VLSM is more flexible and efficient, helping to reduce IP address waste compared to FLSM.*

***Subnet Mask***

*A* ***subnet mask*** *is a numerical value used in networking to divide an IP address into two parts — the network part and the host part. It helps identify which portion of the IP address belongs to the network and which part is assigned to a specific device within that network. For example, in the IP address* ***192.168.1.10*** *with the subnet mask* ***255.255.255.0****, the first three numbers (192.168.1) represent the network, while the last number (.10) identifies the device. In simple terms, a subnet mask allows computers to determine whether another device is on the same local network or if the data should be sent through a router to reach another network.*

***CIDR notation (Classless Inter-Domain Routing)***

*is a compact way to write an IP address together with its subnet mask. It uses a format like* ***192.168.1.0/24****, where the number after the slash shows how many bits are used for the network part of the address. For example,* ***/24*** *means the first 24 bits identify the network, and the remaining bits are for host devices. This method replaced the old class-based system (Class A, B, and C) and allows more flexibility in creating networks of different sizes. CIDR helps improve routing efficiency and prevents the waste of IP addresses.*

*****3. MAC Addresses (Media Access Control Address)*****

***A MAC (Media Access Control) Address is a unique 48-bit hardware address assigned to a network device’s Network Interface Card (NIC) during manufacturing. It serves as the physical address used for communication within a local network and operates at the Data Link Layer (Layer 2) of the OSI model. The MAC address helps identify devices on the same network so that data can be sent to the correct destination.***

*According to the* ***IEEE 802 standard****, the Data Link Layer is divided into two parts — the* ***Logical Link Control (LLC)*** *and the* ***Media Access Control (MAC)*** *sublayers. The MAC sublayer uses the MAC address to control how devices share access to the network. Each MAC address is globally unique, ensuring that no two devices have the same hardware address.*

## *****Format of MAC Address*****

***The format of a MAC address consists of 12 hexadecimal digits (0–9, A–F), grouped into six pairs. These pairs are usually separated by colons (:), hyphens (-), or dots (.).  
Each pair represents 1 byte, so a full MAC address is 6 bytes (48 bits) long. The first 3 bytes are called the OUI (Organizationally Unique Identifier), which identifies the manufacturer, and the last 3 bytes are called the NIC (Network Interface Controller Identifier), which uniquely identifies the device made by that manufacturer.***

***Example:*** *00:1A:2B:3C:4D:5E* ***or*** *00-1A-2B-3C-4D-5E****.***

## *****Types of MAC Address*****

***MAC addresses are used to identify devices and control how data is delivered on a network. There are three types of MAC addresses:***

*****1. Unicast MAC Address***** *A* ***Unicast MAC address*** *uniquely identifies a single device on a network. It is permanently assigned to the device’s network interface card (NIC) and is used for* ***one-to-one communication*** *between devices.*

*****2. Multicast MAC Address***** *A* ***Multicast MAC address*** *is used to send data to a* ***specific group of devices****. Switches recognize multicast addresses and forward the data only to devices that are part of that group, enabling* ***one-to-many communication****.*

*****3. Broadcast MAC Address***** *A* ***Broadcast MAC address****, written as* ***FF-FF-FF-FF-FF-FF****, is used to send data to* ***all devices*** *on the same local network. The switch forwards the frame to every connected device, making it* ***one-to-all communication****.*

***Characteristics of a MAC Address***

*****1.*** *A MAC (Media Access Control) address is a unique identifier assigned to most network adapters or network interface cards (NICs) by the manufacturer. It is used at the Data Link Layer to identify devices and deliver frames to the correct destination.***

*****2.****An Ethernet MAC address is 48 bits long, expressed as 12 hexadecimal digits (4 bits per digit).***

***3.MAC addresses are in a flat structure, meaning they do not have a network or host portion and are not routable on the Internet.***

*****3.*** *They are burned into the hardware of the NIC and cannot usually be changed, except in rare cases where a manufacturer provides a specific tool.***

*****4.****MAC addresses are used mainly in LAN (Local Area Network) environments to allow communication between devices.***

*****5.****The first 3 bytes of a MAC address represent the manufacturer ID (OUI), while the last 3 bytes are a unique identifier for the device (NIC).***

*****6.****MAC addresses are often used with ARP (Address Resolution Protocol) to map IP addresses to MAC addresses for communication within a LAN.***

***MAC Cloning***

***Some Internet Service Providers (ISPs) assign an IP address to a device based on its MAC address, which is a unique identifier for network devices like routers. When you connect a new router, it has a different MAC address, so the ISP may not recognize it, and the Internet might not work. One solution is MAC cloning, where you copy the old router’s MAC address to the new one, making the ISP think it’s the same device, so the IP is assigned automatically and the connection works seamlessly. Alternatively, for dynamic IPs, you can sometimes request a new IP for the new MAC, but it depends on the ISP — some may require you to wait for the DHCP lease to expire. For static IPs, the IP is tied to a specific MAC, so changing the MAC without cloning usually won’t work; in this case, you must either inform the ISP or use MAC cloning to keep the same IP.***

### *****Advantages of MAC Address*****

1. ***Uniqueness:*** *Each MAC address is unique, so devices on a network can be easily identified and managed.*
2. ***Simplicity:*** *Easy to configure and manage without extra network infrastructure.*
3. ***Compatibility:*** *Supported by most networking technologies and protocols.*
4. ***Security:*** *Can restrict network access by allowing only authorized MAC addresses.*
5. ***Fault-tolerance:*** *Devices can be replaced easily if the new device has the same MAC.*
6. ***Multicasting:*** *Supports sending a single packet to multiple devices at once.*
7. ***Efficiency:*** *Helps devices quickly identify and communicate with each other.*
8. ***Lower network overhead:*** *Direct communication reduces the need for extra routing.*
9. ***Troubleshooting:*** *Useful for identifying the source of network issues.*
10. ***Flexibility:*** *Supports various network setups like peer-to-peer, client-server, and hybrid models.*

### ***Disadvantages of MAC Address***

1. ***Limited address space:*** *Only 48-bit, so conflicts can occur if duplicates exist.*
2. ***Spoofing:*** *Can be easily faked, allowing unauthorized access.*
3. ***Inefficiency for large networks:*** *Not hierarchical, making management harder.*
4. ***Static addressing:*** *Usually fixed by manufacturer, hard to change.*
5. ***Limited scope:*** *Only works within a local network, not across the Internet.*
6. ***Hardware-dependent:*** *Tied to the NIC, so replacing hardware changes the MAC.*
7. ***Lack of encryption:*** *Sent in plain text, vulnerable to interception.*
8. ***No inherent security:*** *Alone, MAC addresses don’t provide security; filtering is needed.*
9. ***MAC collisions:*** *Rarely, two devices may share a MAC, causing network issues.*

***IPv4 and IPv6 addressing schemes***

*****1. IPv4 Addressing Scheme*****

***1.Address Length: 32 bits***

***2.Format: 4 dotted-decimal numbers ex:*** *192.168.1.1*

*3.****Address Classes:***

***Class A:*** *1.0.0.0 – 126.255.255.255*

***Class B:*** *128.0.0.0 – 191.255.255.255*

***Class C:*** *192.0.0.0 – 223.255.255.255*

***Class D:*** *224.0.0.0 – 239.255.255.255 (multicast)*

***Class E:*** *240.0.0.0 – 255.255.255.255 (experimental)*

*4.* ***Subnetting:***

*IPv4 addresses can be divided into subnets using subnet masks (e.g., 255.255.255.0).*

*5.Notation:*

*CIDR notation is common, e.g., 192.168.1.0/24*

## ****2*. IPv6 Addressing Scheme*****

1. ***Address Length:***
   * *128 bits*
2. ***Format:***
   * *8 groups of 4 hexadecimal digits separated by colons*
   * *Example: 2001:0db8:85a3:0000:0000:8a2e:0370:7334*
3. ***Simplification Rules:***
   * *Leading zeros in a group can be omitted*
     + *Example: 2001:db8:85a3::8a2e:370:7334*
   * *Consecutive groups of zeros can be replaced by :: (only once per address)*
4. ***Address Types:***
   * ***Unicast:*** *One-to-one communication*
   * ***Multicast:*** *One-to-many communication*
   * ***Anycast:*** *One-to-nearest communication*
5. ***No NAT Required:***
   * *Every device can have a globally unique IP address*
6. ***Subnetting:***
   * *Uses prefix length notation, e.g., /64*
7. ***Security:***
   * *IPv6 has built-in IPsec for encryption and authentication, providing better security*