LAB 4

DHCP

In this lab, for the first task, we will configure the DHCP server and set DHCP assigned network settings. DHCP (Dynamic Host Configuration Protocol) is a client/server network protocol that is used to automatically assign IP addresses and other network configuration parameters to devices (clients) on a network. This eliminates the need for manual IP address configuration for each device, which simplifies network management. With DHCP, this entire process is automated and managed centrally. The DHCP server maintains a pool of IP addresses and leases an address to any DHCP-enabled client when it starts up on the network. Because the IP addresses are dynamic (leased) rather than static (permanently assigned), addresses no longer in use are automatically returned to the pool for reallocation.

How DHCP Works

The client device sends out a **Discover** broadcast message to the network to locate a DHCP server. If the DHCP server is not on the same network as the client, a DHCP relay agent on the network forwards the message to the DHCP server. The DHCP server, which is configured with a DHCP pool, receives the DHCP Discover message. The server selects an available IP address from its DHCP pool and prepares a DHCP **Offer** message that includes the assigned IP address, subnet mask, default gateway, DNS servers, and lease time. The client receives the offer and sends a **Request** to the selected DHCP server to accept the offered IP address. The DHCP server confirms the assignment, and sends **Acknowledgement** to the client with the IP address, lease time, and other configuration details.

What is DHCP pool?

A DHCP pool is a range of IP addresses that a DHCP server can allocate to clients on a network. When a device connects to the network, it requests an IP address from the DHCP server. The server then assigns an IP address from the pool to the device, allowing it to communicate on the network.

What is DHCP relay?

DHCP relay, also known as DHCP forwarding, is a mechanism used to enable DHCP clients and servers to communicate across different networks. This is particularly useful when a DHCP server is not located on the same local network as the DHCP clients.

We can configure a DHCP server on a router using its CLI or a dedicated server.

DHCP Server Configuration and Management using a router

1. **Excluding Addresses**:
    - **Purpose**: Excluding addresses in a DHCP server prevents the server from assigning specific IP addresses to clients, ensuring those addresses are reserved for static devices or

network services. This avoids IP conflicts and ensures reliable assignments for critical devices.
    - **Command**: ***ip dhcp excluded-address [Start IP address] [End IP address]***
2. **Creating a DHCP Pool**:
    - **Command**: ***ip dhcp pool [Pool name]***
3. **Configuring Pool Network Settings**:
    - **Network**: Defines the IP address range and subnet mask.
        - **Command**: ***network [Network address] [Subnet mask]***
    - **DNS Server**: Specifies the DNS server addresses for clients.
        - **Command**: ***dns-server [DNS address]***
    - **Default Router**: Sets the default gateway for clients.
        - **Command**: ***default-router [Default gateway]***
4. **Setting Up a DHCP Relay Agent**:
    - **Enter the Interface**: Access the interface to configure the relay agent.
        - **Command**: ***interface [Interface name]***
    - **Configure Relay Agent**: Specifies the IP address of the DHCP server to forward requests to.
        - **Command**: ***ip helper-address [DHCP server IP address]***
5. **Assigning IP Address via DHCP**:
    - **Command**: ***ip address dhcp***
6. **Viewing DHCP Bindings**:
    - **Purpose**: Provides details about current DHCP leases, including allocated IP addresses, lease expiration times, and associated MAC addresses.
    - **Command**: ***show ip dhcp bindings***

IP Addressing

For the first task of the lab, we'll learn about IP addresses and how it is set in any network.

What is an IP Address?

An IP address is a unique identifier for a device on a network or the internet. There are two types of IP addresses - IPv4 and IPv6 address.

IPv4 Address

This version uses 32-bit addresses. IPv4 addresses are written as four sets of numbers (called octets) separated by periods. For example, 192.168.10.16. Each octet can range from 0-255 and thus gives 2^32 possible addresses. Each IPv4 address has two parts - Network part and Host part.Network part defines the specific network and host part specifies the specific host on that network. Prefix mask/subnet mask is used to define the size of a subnet and to distinguish the network and host part of an IP address. For example, 192.168.10.0/24 means the first 24 bits of the IP address are used for the network part and the

last 8 bits are for the host part. And the subnet mask is written in the same format as the IP address - 255.255.255.0. For example, /8 corresponds to 255.0.0.0.

Routers only find network addresses to direct data packages. Firstly, the router determines the network address based on the IP address and subnet mask by performing bitwise AND operation between them. For example, if the IP address is 192.168.1.1 and subnet mask is 255.255.255.0 -

IP address:	11000000.10101000.00000001.00000001	
Subnet mask:	11111111. 11111111. 11111111 .00000000	
Network address:	11000000.10101000.00000001.00000000	(192.168.1.0)

Here, the last 8 bits are the host part and there are 2^8 possible hosts in that network. But, in this range of 2^8 hosts, the first address (192.168.1.0) is already the network address and the last address (192.168.1.255) is the broadcast address. So, possible hosts of that network can be (2^8-2). Therefore, there are network address, broadcast address and host addresses in a network.

Special Types of IP addresses

Unicast: Unicast is a one-to-one communication method where data is sent from one single sender to one single recipient. Each packet is addressed to a specific IP address. The sender and recipient are uniquely identified by their individual IP addresses.

Broadcast: Broadcast is a one-to-all communication method where data is sent from one sender to all devices within the same network segment or broadcast domain. Packets are sent to a special broadcast address that is recognized by all devices on the local network. There are two types of broadcast IP address - Directed and limited broadcast.

- **Directed Broadcast Address**: This is used to send a broadcast packet to all devices within a specific subnet. Routers generally do not forward directed broadcasts in order to prevent broadcast storms and other security issues.
- **Limited Broadcast Address**: This is used to send a broadcast packet to all devices within the local network segment only, regardless of subnet. The address **255.255.255.255** is used for this purpose. This packet is not routed beyond the local network segment; routers will drop packets addressed to this broadcast address.

Multicast: Multicast is a one-to-many or many-to-many communication method where data is sent from one sender to a specific group of recipients who are interested in receiving the data. Multicast uses specific IP address ranges to target a group of devices. Devices must join a multicast group to receive the data sent to that group. It is efficient for distributing data to multiple recipients without broadcasting to the entire network.

Classful Addressing

Classful addressing is a method of IP address allocation as it divides the IP address space into distinct classes, each with its own range of addresses and default subnet masks.

- **Class A:** The first bit of the first octet determines the class of the IP address. For Class A, this bit is always **0**. So, the range is 0-127. The first 8 bits (one octet) are used for the network part and the remaining 24 bits (three octets) are used for the host part within the network. Therefore, Class A networks can have up to 2^24 addresses per network, which provides a very large number of addresses for each network.
- **Class B:** The first two bits of the first octet is **10**. So, the range of the first octet is from 128-191. The first 16 bits (two octets) are used for the network part. And the remaining 16 bits (two octets) are used for the host part within the network. Class B networks can have up to 2^16 addresses per network, which provides a substantial number of addresses for each network.
- **Class C:** The first three bits of the first octet are **110**. So, the range of the first octet is from 192-223. The first 24 bits (three octets) are used for the network part and the remaining 8 bits (one octet) are used for the host part within the network. Class C networks can have up to 2^8 addresses per network, which provides a relatively smaller number of addresses per network.
- **Multicast:** The first four bits of the first octet are **1110**. So, the range of the first octet is from 224-239. This class is reserved for multicast groups. These addresses are used to send packets to multiple hosts that are part of a multicast group.
- **Experimental:** The first four bits of the first octet are **1111**. Therefore, the range of the first octet is from 240-255. This class is reserved for experimental purposes and future use.

IPv6 Address

This version is designed to provide more addresses. IPv6 addresses use 128 bits and are written as eight groups of four hexadecimal digits separated by colons. For example, 2001:0000:3238:DFE1:0063:0000:0000:FEFB.

IPv6 Representation:

1. Leading zeros in any group can be omitted. However, the number of digits in each group should not be less than one.

   1234:5678:9abc:def0:1234:5678:9abc:0001 => 1234:5678:9abc:def0:1234:5678:9abc:1

2. A contiguous sequence of all-zero groups can be replaced with a double colon (`::`). This can only be done once in an address to avoid ambiguity.

   1234:0000:0000:0000:5678:0000:0000:abcd => 1234::5678:0:0:abcd