

Reminder of the previous session


Reminder of the previous session

- Introduction to Linux
- Linux Directory Structure and File Management
- Linux Shell and Shell Scripting
- Linux Package Management
- Comparison of Popular Distributions
- Introduction to Virtualization
- Setting up Fedora Server on a Virtual Machine



DHCP – Dynamic Host Configuration Protocol

Prof. Dr. Soufiane Hourri



PLAN – DHCP



PLAN – DHCP

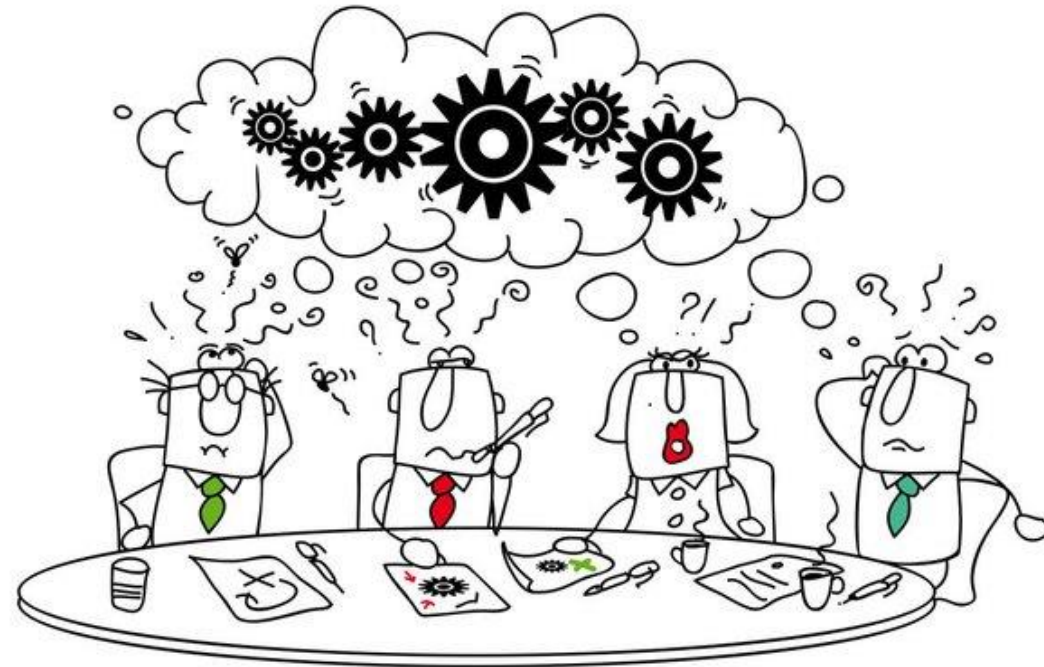
- I. Overview of DHCP
- II. How DHCP Works?
- III. DHCP Packet Structure
- IV. Setting up a Network on Fedora Server
- V. Setting up DHCP
- VI. Setting up Relay Agent
- VII. Practice
- VIII. Q&A



Overview of DHCP

Problematic

- Imagine you have a **large network** with hundreds of devices, including computers, printers, and other devices.
- Each device needs to have a **unique IP** address in order to communicate with other devices on the network.
- The problem is that configuring each device with a unique IP address, subnet mask, default gateway, and other network configurations can be **time-consuming and prone to errors**.
- This becomes even more challenging as the network grows and new devices are added.



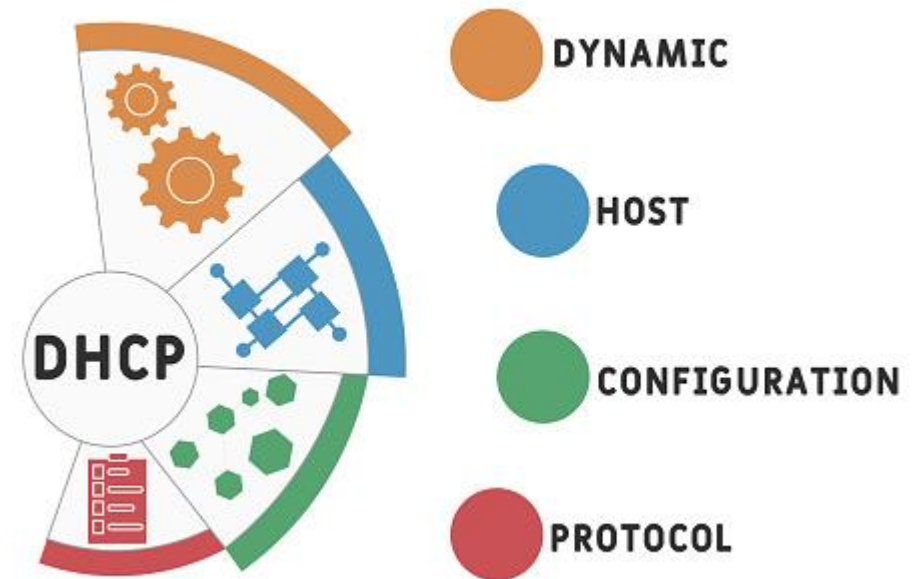
Solution

- To address this problem, network administrators have turned to DHCP as a solution.
- By using DHCP, they can automate the process of assigning IP addresses and other network configurations to devices, making it easier to manage and maintain large networks.



Definition

- DHCP is Dynamic Host Configuration Protocol.
- DHCP is a **network protocol** used to **dynamically** assign IP addresses to **devices** on a network.
- DHCP **automates** the process of **assigning** IP addresses, subnet masks, default gateways, and other network **configurations** to **devices** that connect to a network.
 - DHCP helps eliminate the need for manual configuration of network settings and makes it easier to manage and maintain large networks.
- With DHCP, network administrators can **centrally manage and configure** network settings, which helps to reduce errors and improve network security.



Purpose

Automation

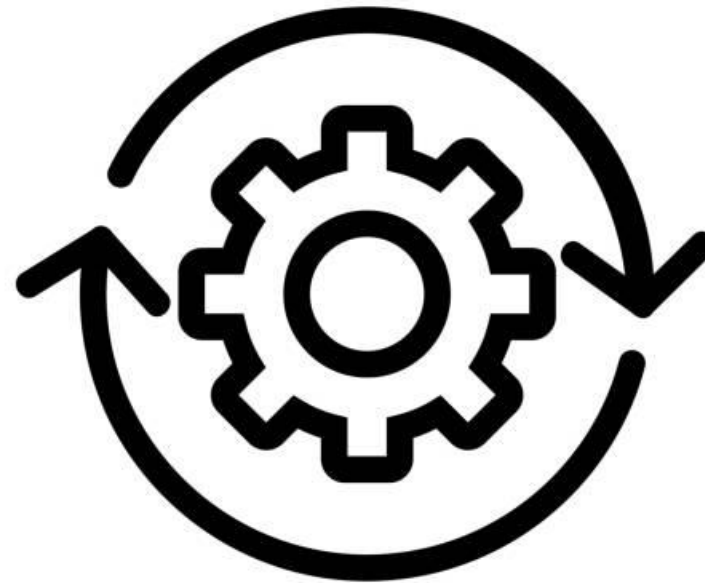
Centralized Management

Scalability

Ease of Use

Purpose – Automation

- Automation refers to the process of using technology to perform tasks without human intervention.
- In the context of DHCP, automation means that the process of assigning IP addresses and other network configurations to devices on a network is performed automatically by the DHCP server, rather than having to be manually configured on each device.
- With DHCP, when a device connects to a network, it sends a broadcast message requesting IP address information.
- The DHCP server receives this message and assigns the device an IP address, along with other network configurations such as the subnet mask, default gateway, and DNS servers.
- This process happens automatically and eliminates the need for manual configuration of network settings on each device.



Purpose – Centralized Management

- Centralized management refers to the practice of managing and configuring network settings from a central location, rather than on each individual device.
- DHCP centralized management means that network administrators can manage and configure network settings for all devices on a network from a single location, typically a DHCP server.
- With centralized management, network administrators can:
 - Easily update network configurations
 - Improve network security
 - Reduce errors
 - Simplify network maintenance



Purpose – Scalability

- Scalability refers to the ability of a system or technology to grow and adapt to meet increasing demands.
- In the context of DHCP, scalability means that the DHCP system can accommodate growth in the number of devices on a network, and can dynamically assign IP addresses and other network configurations to new devices as they are added.
- The scalability of DHCP provides several benefits, including:
 - Ease of growth
 - Improved efficiency
 - Reduced errors
 - Improved network security



Purpose – Ease of Use

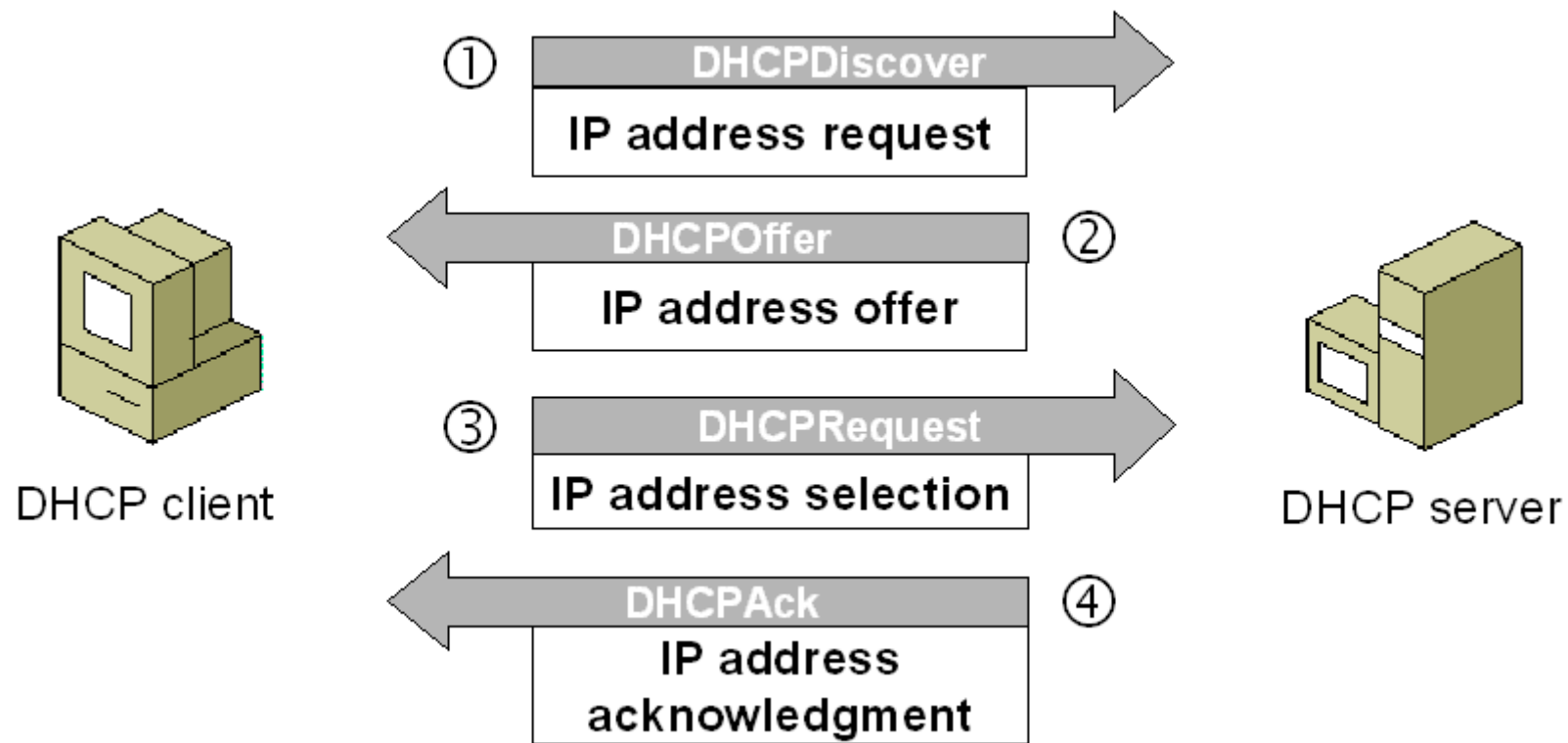
- Ease of use refers to the simplicity and user-friendliness of a system or technology.
- In the context of DHCP, ease of use means that the DHCP system is designed to be straightforward and easy to use, allowing network administrators to quickly and easily manage and configure network settings.





How DHCP works ?

How it works?





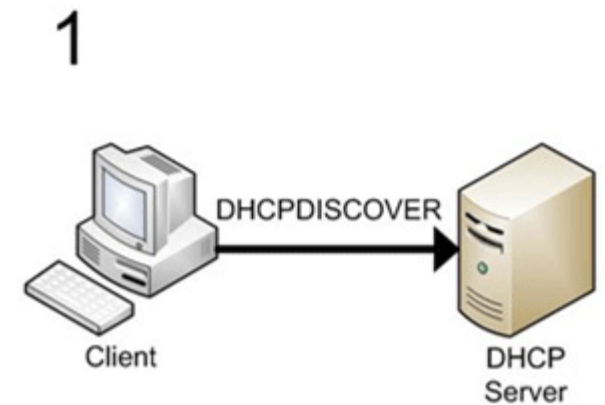
How it works?

The basic operation of DHCP can be described as follows:

- **DHCP Client Discovery:** When a device is connected to a network, it sends a broadcast message called a DHCP Discover message to request an IP address and other network configurations.
- **DHCP Server Offer:** The DHCP server receives the DHCP Discover message and sends a DHCP Offer message to the device, offering an IP address and other configurations.
- **DHCP Client Request:** The device receives the DHCP Offer message and sends a DHCP Request message to the DHCP server, accepting the IP address and other configurations offered.
- **DHCP Server Acknowledgment:** The DHCP server receives the DHCP Request message and sends a DHCP Acknowledgment message to the device, confirming the assignment of the IP address and other configurations.

(1) DHCP Client Discovery

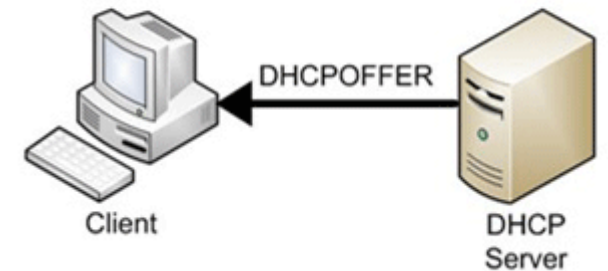
- When we start a device, it checks whether a valid IP configuration is available or not.
- If the valid IP configuration is not available, the device generates a special message known as the **DHCPDISCOVER** message and broadcasts this message on the local LAN segment.
- To broadcast **DHCPDISCOVER** messages, the device uses the **0.0.0.0** and **255.255.255.255** as the source address and destination address, respectively.
- The **0.0.0.0** and **255.255.255.255** are two special addresses. Any device, whether it has a valid IP configuration or not, can use these addresses to send local broadcast messages.
- From these addresses,
 - The **0.0.0.0** is used as the source address. If a device does not have the source address, it can use this address to send broadcast messages.
 - **255.255.255.255** is the local broadcast address. Any message sent on this address is received by all hosts of the local network.



➤ (2) DHCP Server Offer

- Since the client sends the **DHCPDISCOVER** message to the local broadcast address, if a DHCP server is configured on the local network, it will also receive the message.
- If multiple DHCP servers are configured on the local network, they all will receive the **DHCPDISCOVER** message.
- If multiple DHCP servers are available, based on their configuration, one of them or all of them can reply to the **DHCPDISCOVER** message.
- In reply to the **DHCPDISCOVER** message, a DHCP server sends a **DHCPOFFER** message to the client.

2



➤ (2) DHCP Server Offer

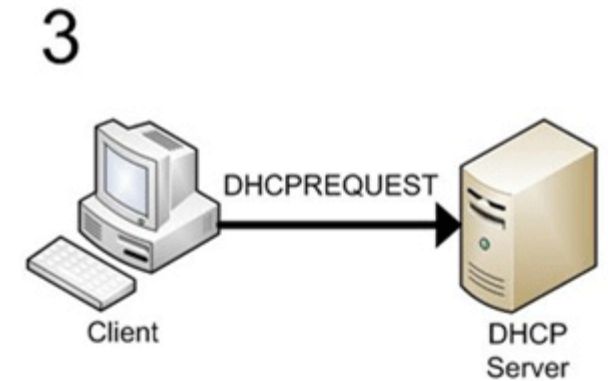
- Since the client does not have an IP address, the DHCP server cannot send the **DHCPOFFER** message directly to the client.
- Because of this, the server sets the destination address to **255.255.255.255**. In other words, the server also broadcasts the **DHCPOFFER** message to the local network.
- The **DHCPOFFER** message contains protocol specific information and an IP configuration.
- An IP configuration typically includes the following important information:
 - the IP address for the client,
 - the subnet mask of the proposed IP address,
 - the IP address of the default gateway,
 - the DNS domain name,
 - the DNS server address or addresses.

2



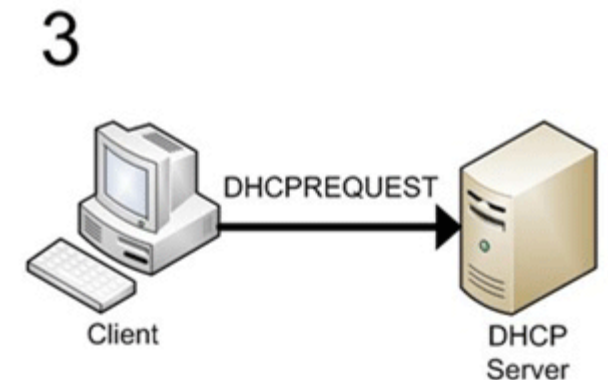
(3) DHCP Client Request

- All hosts in the local network receive the **DHCPOFFER** message.
 - The host that sent the **DHCPDISCOVER** message accepts the **DHCPOFFER** message.
 - Except the original host, all other hosts ignore the **DHCPOFFER**.
-
- *How does a host know whether the broadcasted DHCPOFFER message is for it or not?*



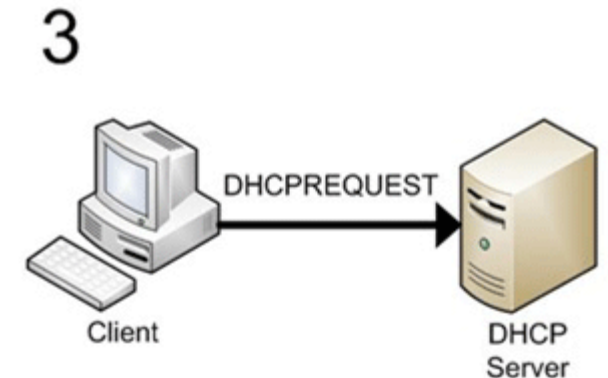
(3) DHCP Client Request

- The **DHCPDISCOVER** message contains the host's **MAC address**.
- When a DHCP server broadcasts a **DHCPOFFER** message, it also includes the host's **MAC address** in a parameter known as the **client ID**.
- When hosts receive the **DHCPOFFER** message, they check the **client ID** field in the message.
 - If a host sees its **MAC address** in the **client ID** field, the host knows that the message is meant for it.
 - If a host sees the **MAC address** of another host in the **client ID** field, the host knows that the message is not intended for it.



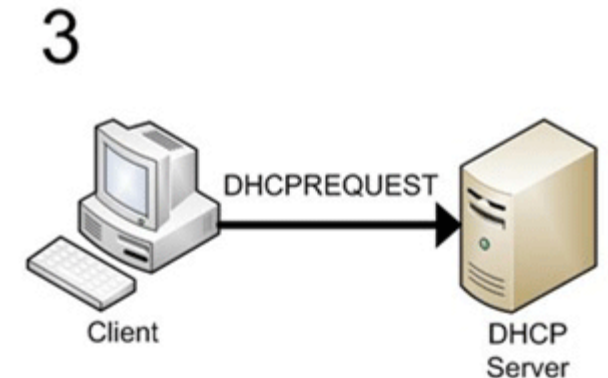
(3) DHCP Client Request

- Depending on the number of DHCP servers, a host may receive multiple **DHCPOFFER** messages.
- If a host receives multiple **DHCPOFFER** messages, it accepts only one message and tells the corresponding server with a **DHCPREQUEST** message that it wants to use the offered IP configuration.
- If only one DHCP server is available and the provided IP configuration conflicts with the client's configuration, the client can respond with a **DHCPDECLINE** message.
 - In this situation, the DHCP server offers another IP configuration.



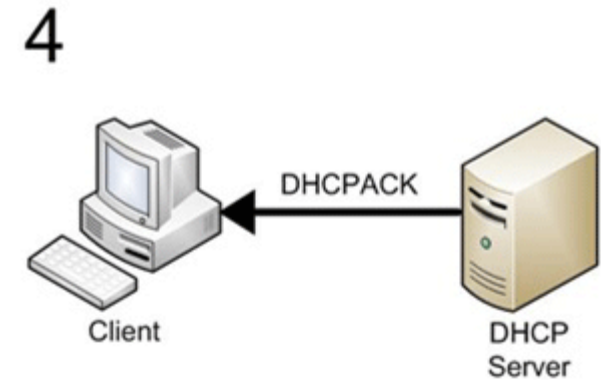
(3) DHCP Client Request

- When DHCP servers receive the **DHCPREQUEST** message, besides the server whose offer has been accepted, all other servers withdraw any offers that they might have made to the client and return the offered address to the pool of available addresses.
- The **DHCPREQUEST** message contains a Transaction ID field. Just like hosts use the client ID field of the **DHCPOFFER** message to know whether the message is intended for them or not, DHCP servers use the Transaction ID field of the **DHCPREQUEST** message to know whether their offer has been accepted or not.



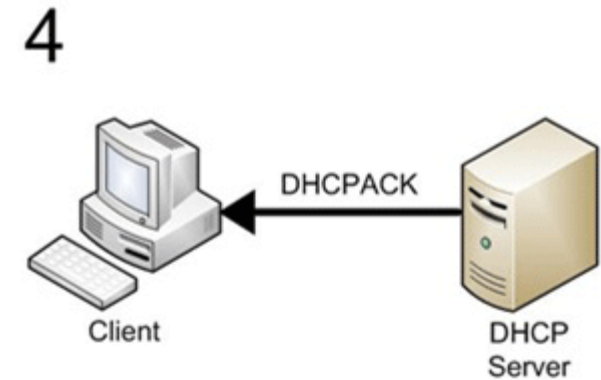
(4) DHCP Client Acknowledgment

- When the DHCP server receives a **DHCPREQUEST** message from the client, the configuration process enters its final stage.
- In this stage, the server sends a **DHCPACK** message to the client.
- The **DHCPACK** message is an acknowledgment to the client indicating that the DHCP server has received the **DHCPREQUEST** message of the client, and the client can use the offered IP configuration.



➤ (4) DHCP Client Acknowledgment

- In some cases, the server may also respond with a **DHCPNACK** message.
- The **DHCPNACK** message tells the client that the offer is no longer valid and the client needs to request an IP configuration again.
- This occurs when the client takes too long to respond with a **DHCPREQUEST** message after receiving a **DHCOFFER** message from the server.
- In such a case, the client can make a new request for another IP configuration.





Other DHCP Messages

- **DHCPRelease**

- A DHCP client sends a **DHCPRelease** packet to the server to release the IP address and cancel any remaining lease.

- **DHCPInform**

- **DHCPInform** is a new DHCP message type, defined in RFC 2131, used by computers on the network to request and obtain information from a DHCP server for use in their local configuration.
- When this message type is used, the sender is already externally configured for its IP address on the network, which may or may not have been obtained using DHCP.
- This message type is not currently supported by the DHCP service provided in earlier versions of Windows NT Server and may not be recognized by third-party implementations of DHCP software.

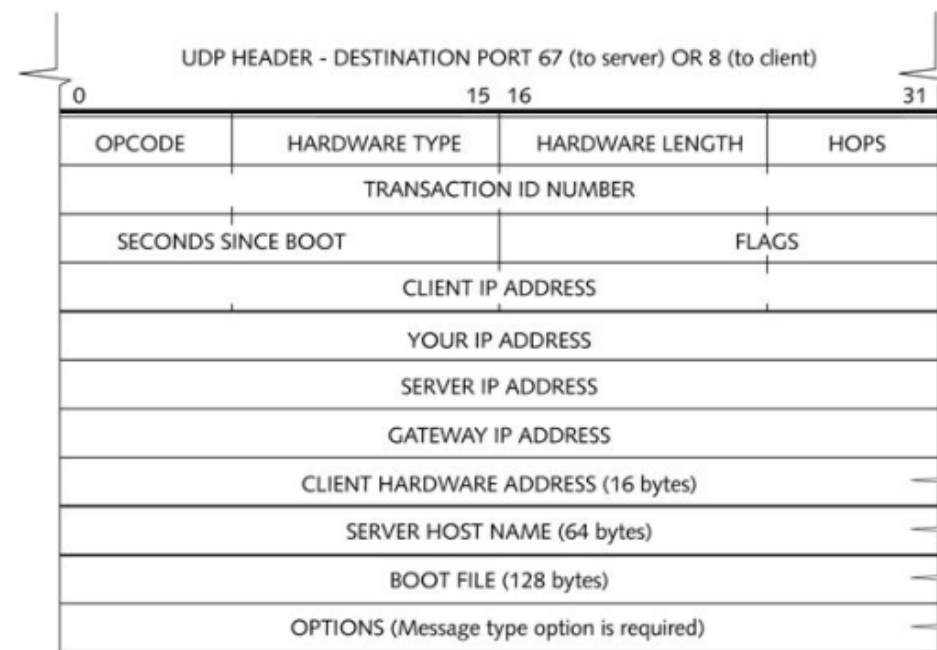


DHCP Packet Structure

DHCP Packet Structure

The basic structure of a DHCP packet consists of the following fields:

- **Operation Code:** Specifies the type of DHCP message, such as request, reply, or decline.
- **Hardware Type:** Specifies the type of hardware used by the client device, such as Ethernet.
- **Hardware Address Length:** Specifies the length of the hardware address of the client device.
- **Hops:** Specifies the number of relay agents that have forwarded the DHCP message.
- **Transaction ID:** A unique identifier for the DHCP transaction, used to match requests and replies.
- **Seconds:** Specifies the number of seconds elapsed since the client device began the DHCP process.
- **Flags:** Specifies various options for the DHCP message, such as whether the client device is capable of broadcasting.
- **Client IP Address:** Specifies the current IP address of the client device, if any.
- **Your IP Address:** Specifies the assigned IP address for the client device.
- **Server IP Address:** Specifies the IP address of the DHCP server.
- **Gateway IP Address:** Specifies the IP address of the default gateway for the client device.
- **Client Hardware Address:** Specifies the hardware address of the client device.
- **Server Name:** Specifies the host name of the DHCP server, if any.
- **Boot File Name:** Specifies the name of the boot file for the client device, if any.
- **Options:** Contains various optional configuration information for the client device, such as the subnet mask, DNS server addresses, and lease time.





Setting up a network on Fedora

Setting up a network on Fedora

- **Installing Network Manager:** Fedora 37 uses Network Manager as the default network management tool. You can install Network Manager using the following command: "dnf install NetworkManager"
- **Configuring a network interface:** You can configure a network interface using the Network Manager graphical user interface (GUI) or the command-line interface (CLI). In the GUI, you can access the Network settings through the System Settings menu. In the CLI, you can use the "nmtui" command to configure the network interface.
- **Testing the network connection:** You can use the "ping" command to test the network connection to another device on the network.

Setting up a network on Fedora

```
# display devices
[root@localhost ~]# nmcli device
DEVICE  TYPE      STATE      CONNECTION
enp1s0  ethernet  connected  enp1s0
lo      loopback  unmanaged  --

# set IPv4 address
[root@localhost ~]# nmcli connection modify enp1s0 ipv4.addresses 10.0.0.30/24

# set gateway
[root@localhost ~]# nmcli connection modify enp1s0 ipv4.gateway 10.0.0.1
```




Setting up DHCP



Setting up DHCP

- **Installing the DHCP server:** You can install the DHCP server on Fedora 37 by using the following command: `dnf install dhcp`
- **Configuring the DHCP server:** The DHCP server configuration file is located at `/etc/dhcp/dhcpd.conf`. In this file, you can specify the range of IP addresses that the DHCP server will assign to clients, as well as other parameters such as the subnet mask, default gateway, and DNS server information.
- **Starting the DHCP server:** You can start the DHCP server by using the following command: `systemctl start dhcpd`

Setting up DHCP

```
# default lease time
default-lease-time 600;

# max lease time
max-lease-time 7200;

# this DHCP server to be declared valid
authoritative;

# specify network address and subnetmask
subnet 10.0.0.0 netmask 255.255.255.0 {
    # specify the range of lease IP address
    range dynamic-bootp 10.0.0.200 10.0.0.254;
    # specify broadcast address
    option broadcast-address 10.0.0.255;
    # specify gateway
    option routers 10.0.0.1;
}
```



Setting up a relay agent



Setting up a relay agent

- A DHCP relay agent is used to forward DHCP requests from clients on one network segment to a DHCP server on another network segment.
- **Installing the DHCP relay agent:** You can install the DHCP relay agent on Fedora 37 by using the following command: `dnf install dhcrelay`
- **Configuring the DHCP relay agent:** The DHCP relay agent configuration file is located at `/etc/sysconfig/dhcrelay`. In this file, you can specify the IP address of the DHCP server that the relay agent will forward requests to.
- **Starting the DHCP relay agent:** You can start the DHCP relay agent by using the following command: `systemctl start dhcrelay`

Setting up a relay agent

```
# Options for dhcrelay
# The DHCP relay agent.
#
# If you want to run dhcrelay on all interfaces, use -i all
#
OPTIONS="-i eth0 -s 192.168.0.1"
```

```
dhcrelay -i eth0 -s 192.168.0.1
```



Q&A



Q&A

- What are the benefits of using DHCP?
→ The benefits of using DHCP include reduced network administration overhead, ease of network configuration, and automatic IP address assignment. With DHCP, you don't have to manually configure IP addresses and other network information on each client, which can save time and reduce the risk of errors.



Q&A

- What happens if multiple DHCP servers are on the same network?
→ If multiple DHCP servers are on the same network, it can cause IP address conflicts and other network issues. To avoid these problems, you should have only one DHCP server on the network, or use a DHCP relay agent to forward client requests to a single DHCP server.



Q&A

- What is a DHCP lease?
→ A DHCP lease is the amount of time that a client can use a dynamically assigned IP address. After the lease time expires, the client must request a new IP address assignment from the DHCP server.



Q&A

- How does DHCP handle IP address conflicts?
 - ➔ When a client requests an IP address from the DHCP server, the DHCP server checks its pool of available IP addresses to ensure that the requested address is not already in use. If the address is in use, the DHCP server sends a negative response to the client. The client must then wait a short period of time before sending another request for an IP address.

.



Q&A

- What is a DHCP relay agent and when is it used?
→ A DHCP relay agent is a device that forwards DHCP requests from clients on one network segment to a DHCP server on another network segment. DHCP relay agents are used when there is a need to separate the DHCP server and clients on different network segments, such as when the DHCP server is located on a different subnet than the clients.

.



Practice



Text Editors

There are many text editors available for Fedora, but some of the most well-known and widely used include:

- **nano** - a small and simple text editor with an intuitive interface
- **vim** - a highly configurable and powerful text editor that is well-suited for advanced users
- **gedit** - a simple and easy-to-use text editor with a modern interface
- **emacs** - a highly customizable text editor with a large user community and extensive plugin library
- **Visual Studio Code** - a popular, open-source text editor developed by Microsoft that offers a range of features for developers



Text Editors

"**nano**" and "**vim**" are two popular text editors in Fedora with differences in:

- **User interface:** nano is simple, while vim is complex and mode-based.
- **Customizability:** vim is highly configurable, while nano is basic.
- **Speed:** vim is faster, with keyboard shortcuts for common actions.
- **Plugins/Extensions:** vim has many plugins and extensions, while nano has limited options.



Practice outline

1. Clone the Fedora server, and name the new clone as “DHCP Server”
2. Install nano text editor
3. Install Wireshark
4. Configure the network for your DHCP Server using **nmcli**
 - Attribute the following IP address to the DHCP server : 192.168.1.1
5. Configure DHCP for the LAN: 192.168.1.0/24
6. Verify if a client within the 192.168.1.0/24 network can obtain an IP address automatically.
7. Capture the DHCP messages using Wireshark from the Server part.
8. Configure DHCP for the LAN: 192.168.2.0/24
9. Configure the Relay Agent
10. Verify if a client within the 192.168.1.0/24 network can obtain an IP address automatically.
11. Capture the DHCP messages using Wireshark from the Server part.
12. Write your report.