Practice Lab 3: DHCP, Operation and Trace Analysis

1. Preliminary Work

Pre-reading: Kurose 7th Edition, Section 4.3.3, subsection **"Obtaining a Host Address: Dynamic Host Configuration Protocol"** (pages 284-286).

Tasks to be completed before the lab session:

- Read the **Introduction** section.
- Study the **DHCP Protocol Operation** section.

The lab will be conducted on **Windows**, as it allows the **DHCP client** to run without requiring **administrator privileges**, unlike Linux. **Exercises 1 and 2** include alternatives for performing them on Linux if you have the necessary permissions. From **Exercise 3** onward, we will work with **pre-recorded captures** available in **PoliformaT**, making it possible to complete them on Linux as well.

2. Objectives

At the end of this lab, you should understand DHCP well enough to:

- Explain the **purpose** of the **DHCP protocol**.
- Describe its **basic messages** and their names.
- Interpret the **main fields** of a **DHCP message** captured using **Wireshark**.
- Explain the role of a **DHCP relay agent**.
- Analyse a **Wireshark capture** to determine if a **relay agent** is being used and, if so, identify its **IP address**.

3. Introduction

In this lab, we will study the most common method a node uses to obtain an **IP address**: the **Dynamic Host Configuration Protocol (DHCP)**.

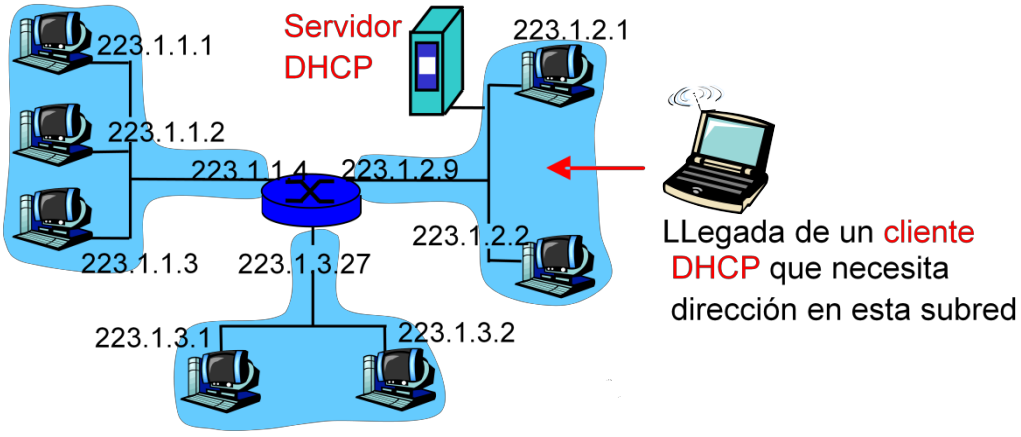
As discussed in class, a device needs at least **one IP address** to communicate its **applications** over a **TCP/IP network**. This assignment can be done **manually**, where an **administrator** configures the device with a **static IP address** (commonly used in **routers**). However, in most cases, it is more convenient for the assignment to be **dynamic**, occurring during **system startup**. This is particularly useful for **laptops**, which often connect to **different networks**.

DHCP enables the **automatic assignment of IP addresses** to nodes. In addition to **IP addresses**, DHCP allows a node to obtain **additional configuration information**, such as the **subnet mask**, **default gateway (router)**, and **local DNS server address**.

Although we study DHCP alongside the **network layer** of the **TCP/IP stack**, DHCP is actually an **application-layer protocol** that operates over **UDP**:

- **DHCP Client**: A node that connects to a **subnet** and requests an **IP address**.
- **DHCP Server**: A node responsible for **managing** an organization's **IP address pool**. The **DHCP server** listens on **UDP port 67**.

In the **simplest case**, each **subnet** has its **own DHCP server**. If **no DHCP server** is present in a subnet, a **DHCP relay agent** (usually a **router**) is required to **forward DHCP requests** to a **DHCP server**. The following figure illustrates a **DHCP server** located on the **same network** as the **client**.



4. DHCP Protocol Operation

When a **node boots up** without **IP configuration**, it must go through **four stages** to obtain one:

1. **Discovery Stage:** The device has just **started up** and does not know:

   - The **network address** it is connecting to.
   - The **DHCP server's IP address**.

   To locate a **DHCP server**, the **node broadcasts a DHCPDiscover message** on **port 67** to the **entire network**. Since it does not know its own IP or the server's IP, the IP datagram containing the discovery message will use the following addresses:

   - **Source IP Address**: 0.0.0.0 (since the node has no assigned IP).
   - **Destination IP Address**: 255.255.255.255 (broadcast to the entire network).

   This **DHCPDiscover message** contains a **Transaction Identifier**, which **associates responses** with the **original request**.

2. **Offer Stage:** The **DHCPDiscover message** is received by **all network elements**, including **DHCP servers**. However, only **servers configured to respond** to a particular **client** will send a **DHCPOffer message**.

   A client may receive **zero or more responses**. Each **DHCPOffer message** includes:

   - The **Transaction Identifier** from the **DHCPDiscover message**.
   - The **IP address** the server offers.
   - The **subnet mask**.
   - The **lease time** (validity period of the IP address).

   DHCPOffer messages are usually sent as **unicast**, unless the **client requests** a **broadcast response**.

The DHCPOffer message will carry the following IP addresses:

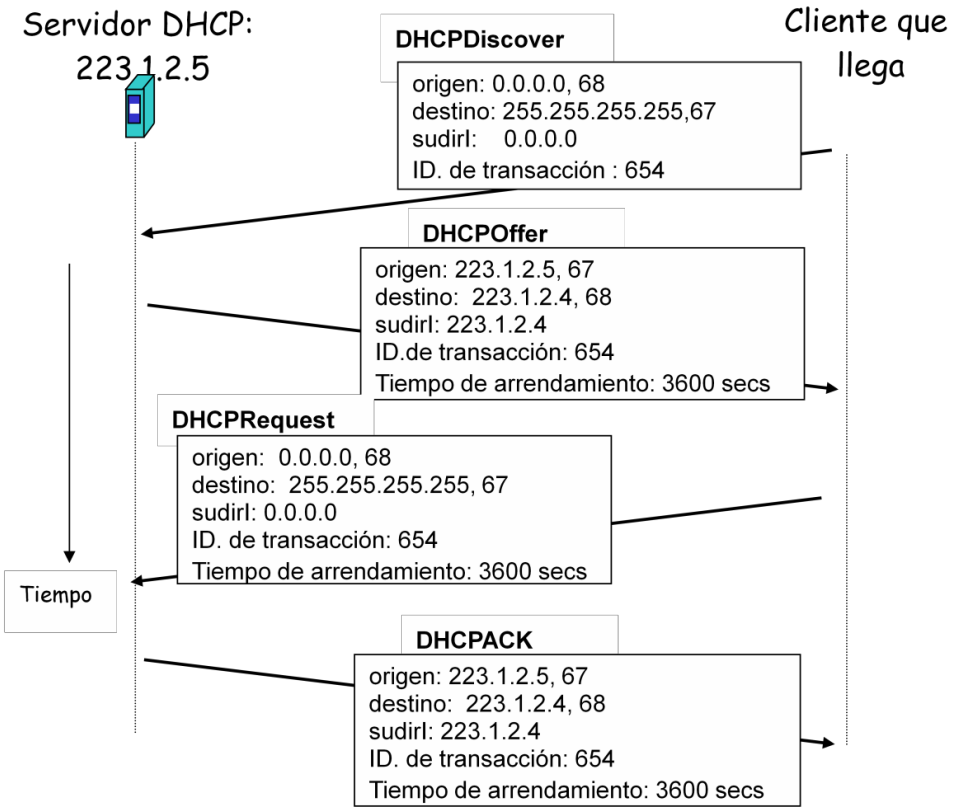
- **Source address:** IP address of the DHCP server.
- **Destination address:** IP address that the server offers to the client or 255.255.255.255 if the client has requested it.

3. **DHCP Request Stage:** The **DHCP client** selects a **DHCPOffer** based on criteria such as **earliest response** or **longest lease time**. It then sends a **DHCPRequest message** to confirm its choice, repeating the **configuration parameters** the **server proposed**.

4. **Acknowledgment Stage:** After the **DHCPRequest message**, the **client waits** for a **server confirmation** through a **DHCPAcknowledge (DHCPACK) message**.

5. At this point, the **client enters a stable state**, using the **assigned IP address** until the **lease expires**.

The following figure shows the previous stages:



Once the client has obtained its IP address, it can stop needing it at any time. To end the IP address lease before the allotted time, the client must send a **DHCPRELEASE** message to the server. From that moment on, the client can no longer use that IP address and the DHCP server can assign it to any other node that requests it.

On the other hand, if a node exhausts the lease time that it was granted when assigning the IP address and wants to continue using it, it can renew its lease time by means of a **DHCPREQUEST** message.

The server can respond affirmatively by means of a **DHCPACK**, or deny the time

extension by means of a **DHCPNACK** message (DHCP negative acknowledgement message). In this last case, the client will give up the IP address immediately.

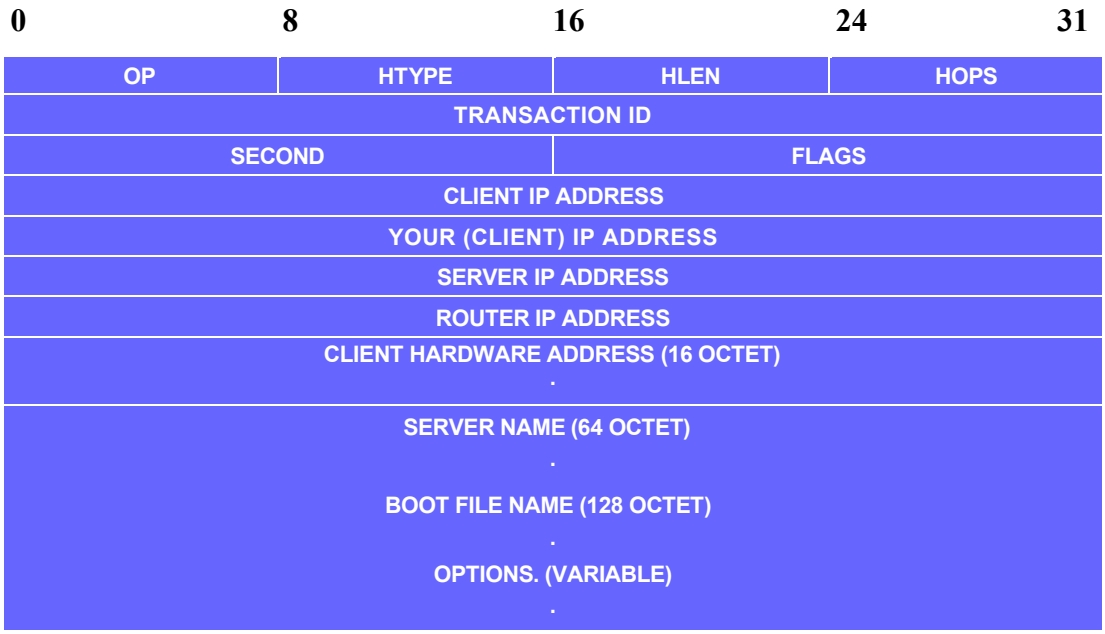
DHCP Relay Agent

Some **DHCP messages** are sent to the **broadcast address** (255.255.255.255). Since **routers filter broadcast traffic**, DHCP messages cannot reach **external networks,** this means that, in principle, a DHCP server would be required on each network that wanted to use the service unless a **DHCP relay agent** is used. Relay agents can be used to avoid this requirement.

A **DHCP relay agent** is a **device (router or host)** that receives **broadcast DHCP requests** and forwards them as **unicast messages** to a **DHCP server**.

DHCP Message Format

Both **DHCP request** and **response messages** share the following format:



Explanation of Each Field:

- **OP**: (1) Request, (2) Reply.
- **HTYPE**: Network Hardware Type. Example: (1) Ethernet.
- **HLEN**: Hardware Address Length. Example: (6) Ethernet.
- **HOPS**: Number of hops. The client sets this to **zero**. If a server receives the request and forwards, it to another machine, it increments this value.
- **TRANSACTION ID**: A unique **integer number** used by the machine to match **responses** with **requests**.
- **SECONDS**: The client records the **number of seconds** since the boot process started.
- **FLAGS**: Only the **most significant bit** has an assigned meaning; the rest are set to **zero**.

- A **1** in the most significant bit means the **server must respond** using the **broadcast IP address**, which will also imply **hardware broadcast**.
- A **0** requests a **unicast response**.

- **CLIENT IP ADDRESS:** If the client **already has an assigned IP address**, it will use this field to specify it. Otherwise, it will be set to **zero**.
- **YOUR (CLIENT) IP ADDRESS:** If the client **does not have an assigned address**, this field is used to indicate the **offered IP address**.
- **NEXT SERVER IP ADDRESS:** Used by the server in **DHCPOFFER** and **DHCPACK** responses to inform the client of the next DHCP server it should use during the boot process.
- **RELAY AGENT IP ADDRESS:** Used when a **relay agent** is present.
- **SERVER NAME:** Works the same way as the server IP address field.
- **BOOT FILE NAME:** An administrator may want to configure **different boot types** (e.g., UNIX, Windows, etc.). This field allows specifying the boot file.
- **OPTIONS**: The **DHCP options field** encodes a **wide variety of settings**, including **lease duration, message type, subnet mask**, and more.

  Each **option** consists of three subfields:

  1. **Code**: Indicates the **type of option** (1 byte).
  2. **Length**: Specifies the **number of bytes** in the **data field** (1 byte).
  3. **Data**: The **actual information** associated with the option (variable length).

Example of a DHCP Option: Message Type (Option 53):

An option that appears in all DHCP messages is number 53, which indicates the type of DHCP message. This is a 3-octet option that has the following meaning and value:

CODE (53)	LENGTH (1)	TYPE (1-7)

Where the basic message types are:

TYPE	MESSAGE
1	DHCPDISCOVER
2	DHCPOFFER
3	DHCPREQUEST
4	DHCPDECLINE
5	DHCPACK
6	DHCPNACK
7	DHCPRELEASE

The **DHCPDECLINE** message is used by the **client** to inform the **server** that the **offered IP address is already in use**.

4. Traffic Analysis

In this lab, we will use the **protocol analyser** we are already familiar with, **Wireshark**, to examine the traffic exchanged between a **DHCP client and server** when the **client requests an IP address** from the server and when it **releases** it.

Before working with the **protocol analyser**, it is useful to recall from **Lab 1** how our computer determines its **IP configuration**, that is, how it obtains an **IP address**. As we saw in **Lab 1**, our workstations **automatically obtain IP configuration** through communication with a **DHCP server**.

This **DHCP server** may be located **within the local network** (as is usually the case in **home networks**) or **outside the network**, as in the **Network Laboratory workstations**. In the latter case, a **DHCP relay agent** will mediate the **DHCP communication** between our machine (**DHCP client**) and the **DHCP server** providing the IP configuration.

Exercise 1

Open a **Command Prompt (cmd.exe)** window and run the command: ***ipconfig /all***

From the displayed information, **which parameters** are related to the **initial DHCP exchange** that occurred **during system startup**? Answered below

- When was the **IP address lease obtained**? miércoles, 26 de febrero de 2025, 6:51:06
- When does it **expire**? viernes, 28 de febrero de 2025, 7:51:05

(**Note:** The equivalent command in Linux is: **ip address**.)

A particular feature of the **DHCP protocol** is that **DHCP traffic is mainly generated during system startup**. Once the node is ready to **capture traffic** with **Wireshark**, the **DHCP exchange** has likely **already concluded**. A **new DHCP exchange** may occur when the **IP address lease time expires** and needs renewal, but waiting for this to happen naturally is not practical.

To force a **new DHCP exchange**, we can use the **ipconfig** command, which we studied in **Lab 1**. This command allows us to **release the current IP address** and then **request a new assignment** through a **DHCP exchange**.

- ***ipconfig /all**:* Displays complete **network and link-layer configuration** details, including the **IP addresses of DNS and DHCP servers**.

- ***ipconfig /release***: Releases the **IPv4 address assigned by DHCP**, notifying the **DHCP server**. The associated **network interface** is left **unconfigured**.

- ***ipconfig /renew**:* Requests the **DHCP server** to **renew the IPv4 address**.

E1, 1)
Sufico DNS específico para la conexión
Dirección IPv6 local
Dirección IPv4
Máscara de subred
Concesión obtenida
La concesión expira
Puerta de enlace predeterminada
Servidor DHCP
IAID DHCPv6
DUID de cliente DHCPv6
Servidores DNS

Exercise 2
Start the **Wireshark protocol analyser** and begin a **capture**, filtering **UDP traffic on port 67**.

Next, use the command: ***ipconfig /release*** to **release** the **IP configuration** assigned to your computer.

Important: After executing this command, your computer will **lose network access**, including access to the **W drive**. If you are in **W**, switch to **C** using command: ***C:*** to continue working.

Now, request a new IP address by running: ***ipconfig /renew*** while **Wireshark is still capturing traffic**. Once completed, **stop the capture**.
Equivalent **Linux commands**:

- ***sudo dhclient –r*** to release the IP address.
- ***sudo dhclient*** to request a new IP address.

Through this process, we have obtained the **entire DHCP exchange** between a **DHCP client and server** for acquiring an **IP address**. In our case, this exchange is **preceded by the process in which the client relinquishes the IP configuration** it had obtained during **system startup**.

Observe whether the **captured messages** correspond to those explained in the **previous sections**.

To ensure that **everyone works with the same captures**, we have made **two pre-recorded captures** available in **PoliformaT**:

- **Captura1Practica3.pcap**: Records the process of **obtaining IP configuration**.
- **Captura2Practica3.pcap**: Records the process of **releasing IP configuration**.

These captures were taken on a **computer in the Network Laboratory**, allowing us to gain a **better understanding** of the **network's IP configuration**.

Both captures are **ready for analysis**, and we can now begin working with them.

Exercise 3

Download the **Captura1Practica3.pcap** file from **PoliformaT** and open it in **Wireshark**.

a) Focus on the **first DHCP message** in the **IP address acquisition process**: **DHCPDISCOVER**.

- Based on the captured information, **does DHCP use TCP or UDP**? UDP
- Looking at the **source and destination IP addresses** in this first message, **can you justify why DHCP uses a connectionless service?**

Because the host doesn't have an IP yet, and it doesn't know the IP of the DHCP server, so it has to broadcast the discover message to the entire network.

b) Select the **DHCPDiscover** message and find the relevant information to fill in the following fields (data is found across different layers in the packet headers):

Message Type (DHCP options field)	Discover
Datagram Source IP (IP header)	0.0.0.0
Datagram Destination IP (IP header)	255.255.255.255
Source and Destination Ports (UDP header)	Source: 68 Destination: 67
Transaction ID (DHCP header)	0xa4e6fddd
Client IP Address Field (DHCP header)	0.0.0.0
Your IP Address Field (DHCP header)	0.0.0.0
Relay Agent IP Address Field (DHCP header)	0.0.0.0

a) In this message, the **client does not request just any IP address**, but instead asks for a **specific address associated with its MAC address**. **Which field contains this request?** Option 50: Requested IP Address

b) Among the **DHCP options**, there is a **list of parameters** requested by the **client**. List the **first four**. Option 53: DHCP Message Type
Option 61: Client identifier
Option 50: Requested IP Address
Option 12: Host Name

Exercise 4

Next, we analyse the **server response messages**: **DHCPOFFER**.

a) **How many DHCPOFFER messages are there?** What conclusions can be drawn about the **number of DHCP servers available** in the **UPV network**?
There are 2 offers, so at least 2 DHCP servers are available in the UPV network

b) Find the relevant information in the **first DHCPOffer** message to fill in the following fields:

Message Type (DHCP options field)	Offer
Datagram Source IP (IP header)	158.42.1.81
Datagram Destination IP (IP header)	158.42.180.23
Source and Destination Ports (UDP header)	Source: 67 Destination: 68
Transaction ID (DHCP header)	0xa4e6fddd
Client IP Address Field (DHCP header)	0.0.0.0
Your IP Address Field (DHCP header)	158.42.180.23
Relay Agent IP Address Field (DHCP header)	158.42.181.250

c) **Which field in the DHCPOFFER message contains most of the IP configuration settings that the server offers to the client?** The options field (it contains all the additional options)

- Check all the settings provided by the **DHCP servers**.
- Pay special attention to the **"DHCP Server Identifier"** field.
- **Does it match** any of the IPs noted in your table? Yes, the datagram source IP

d) Look for and **record** the following **IP configuration details** provided by the **DHCP servers**:

- **Offered IP Address** 158.42.180.23
- **Subnet Mask** 255.255.254.0
- **Assigned Router (Gateway)** 158.42.181.250
- **Domain Name** upv.es

e) **Who owns the source IP address of these DHCPOFFER datagrams?** A DHCP server

f) Compare the **"DHCP Server Identifier"** field values in all **DHCPOffer messages** from the capture. **How many different DHCP servers responded?**
As the server identifier is different in both packets, 2 servers responded

Exercise 5

Now, we analyse the **DHCPREQUEST** message, which the client sends to accept one of the server's offers.

a) Fill in the following table with information from this message:

Message Type (DHCP options field)	Request
Datagram Source IP (IP header)	0.0.0.0
Datagram Destination IP (IP header)	255.255.255.255
Source and Destination Ports (UDP header)	Source: 68 Destination: 67
Transaction ID (DHCP header)	0xa4e6fddd
Client IP Address Field (DHCP header)	0.0.0.0
Your IP Address Field (DHCP header)	0.0.0.0
Relay Agent IP Address Field (DHCP header)	0.0.0.0

b) Find the **DHCP server's IP address** that the **client is responding to**.

158.42.1.81 (can be seein in Option 54: DHCP Server Identifier)

Exercise 6

Finally, we analyse the **DHCPACK** message sent by the **UPV server**, confirming that the **client has obtained an IP address**.

- Find the **IP address of the UPV DHCP server** that issued the confirmation.

158.42.1.81

Exercise 7

For the final task, we will analyse a new **Wireshark capture** to study the **DHCP traffic generated when a node releases its IP address**.

- Open the capture file **Captura2Practica3.pcap**, which was obtained using: ***ipconfig /release***

What type of DHCP message is involved in this process? Release

What are the source and destination of this message? Source: 158.42.180.23
Destination: 158.42.1.81

Is there any response to this message? No