3. Network Services Involved in the Deployment of a Web Application

Miquel Àngel París i Peñaranda

Web Application Deployment

2nd C-VET Web Application Development

Index

DHCP Service Activity

Preliminary considerations:

For the development of this activity you need the two previously created virtual machines.

You have to foresee that if the environment where the activity takes place has some other equipment (such as a router) with DHCP server functions, it can interfere with the DHCP server that you will configure and so you have to take this into account.

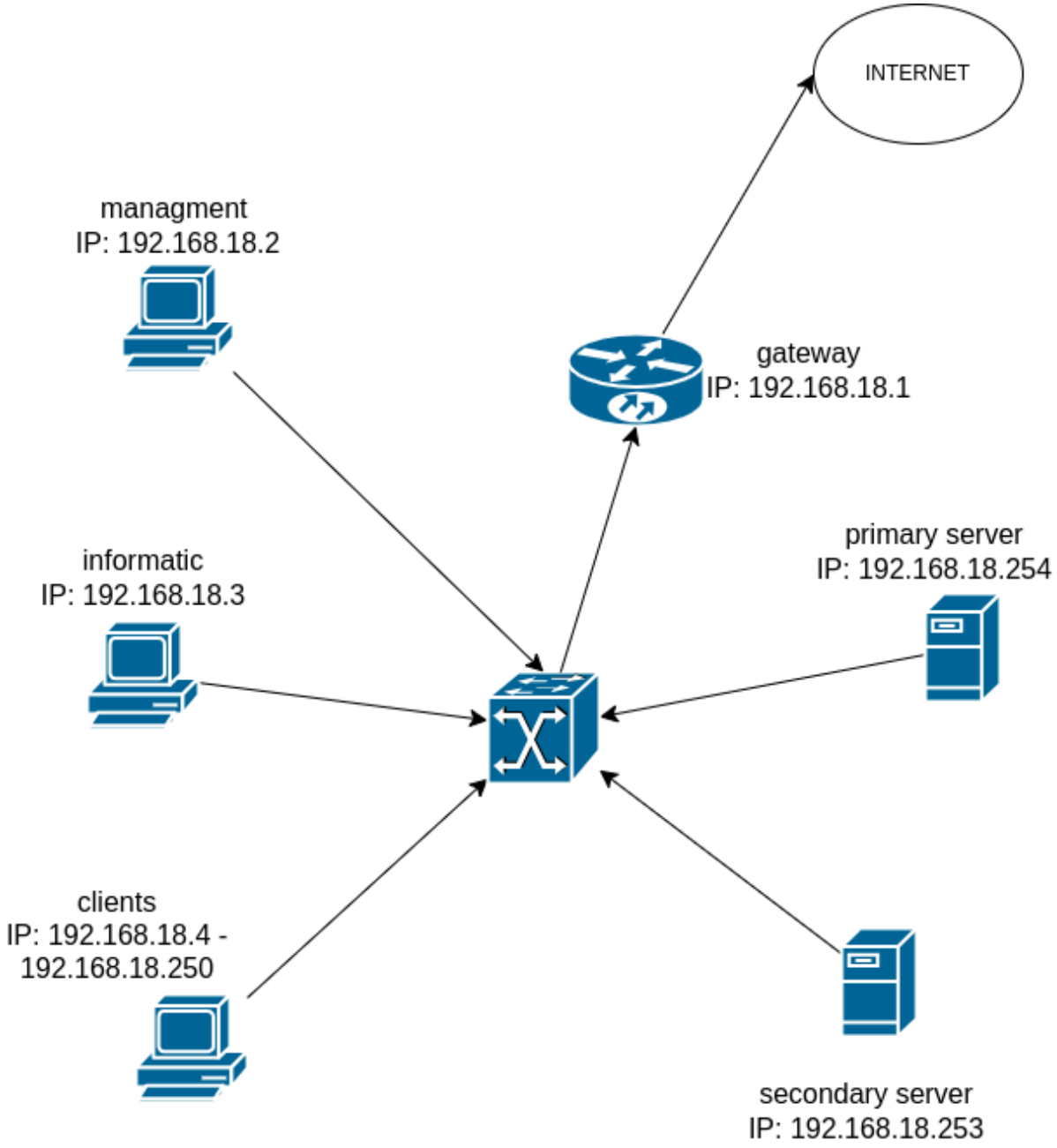
Environment to be simulated:

It is intended to implement a dynamic network configuration assignment service within a public library. The network where the equipment will be located will be 192.168.18.0/24 and it should be taken into account that the router has 192.168.18.1/24 as its IP address and the DHCP server to be implemented is 192.168.18.252/24.

The DNS server addresses will be provided as 192.168.18.252 and 8.8.8.8

A. Installation planning

A.1. With the DÍA software or similar, you make a physical and logical diagram of the network where the different computers and devices are shown, as well as their IPs. Insert the physical/logical schematic of the network.



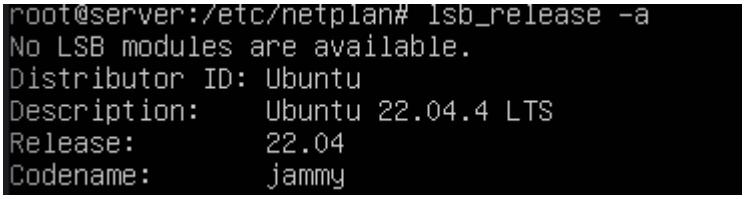
A.2. Define what the range of available addresses will be, if you want the DHCP server to handle as many addresses as possible. Indicates the range of available addresses.

- The range of available IPs for clients is from 192.168.18.4 to 192.168.18.250, since there are reserved IPs. These reserved IPs are: the gateway, which is 192.168.18.1, the management department, which is 192.168.18.2, the IT department, which is 192.168.18.3, the primary server, which is 192.168.18.254, the secondary server, which is 192.168.18.253, the web and FTP service, which is 192.168.18.252, and the mail service, which is 192.168.18.251.

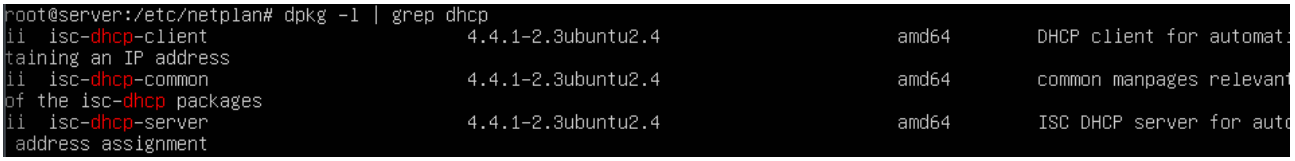
A.3. Propose a lease time appropriate to the scenario. Justify your answer. Indicate the lease time in seconds. Justify your choice.

- We will set the default that comes in the DHCP configuration, which is 6000 seconds, because the clients will have enough time.

A.4. With the `lsb_release -a` command you get the distribution and version of the server. Insert screenshot.



A.5. Install the `isc-dhcp-server`, `nmap` and `wireshark` packages that you will use during the development of the activity. Insert screenshot.



B. DHCP Server Configuration

If you experience errors during the configuration of the service or the service does not start up correctly, go to section D.7.

B.1. Assign a static network configuration to the server. Insert screenshot.

```
  GNU nano 6.2                                    00-installer-config.yaml
# This is the network config written by 'subiquity'
network:
  ethernets:
    enp0s3:
      dhcp4: true
    enp0s8:
      addresses: [192.168.18.254/24]
#       gateway4: 192.168.18.1
#       nameservers:
#         search: [eihsa]
#         addresses: [192.168.18.254]
  version: 2
```

B.2. Check with the help of the `nmap -sU localhost` command if the DHCP server is listening on any port. If yes, indicate the port through which the DHCP server listens. Insert screenshot.

```
root@server:/home/user# nmap -sU localhost
Starting Nmap 7.80 ( https://nmap.org ) at 2024-10-08 17:58 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000010s latency).
Not shown: 998 closed ports
PORT   STATE         SERVICE
53/udp open          domain


Nmap done: 1 IP address (1 host up) scanned in 1.38 seconds
root@server:/home/user# _
```

B.3. Access the DHCP server configuration file `/etc/dhcp/dhcpd.conf`. Configure it (creating a new subnet) taking into account the previous requirements. Insert screenshot.

```
subnet 192.168.18.0 netmask 255.255.255.0 {
        range 192.168.18.4 192.168.18.250;
        option routers 192.168.18.1;
        option domain-name-servers ns1.eihsa, ns2.eihsa;
        option domain-name "eihsa.com";
        default-lease-time 600;
        max-lease-time 7200;
}
```

B.4. Remember that when a configuration file is modified, in order for the changes to take effect, the service has to be started/restarted. Start the DHCP server with the command: `sudo systemctl start isc-dhcp-server` Insert screenshot.

```
root@server:/etc/dhcp# systemctl restart isc-dhcp-server
root@server:/etc/dhcp# systemctl status isc-dhcp-server
● isc-dhcp-server.service - ISC DHCP IPv4 server
     Loaded: loaded (/lib/systemd/system/isc-dhcp-server.service; enabled; vendor preset: enabled)
     Active: active (running) since Mon 2024-10-07 15:16:16 UTC; 5s ago
       Docs: man:dhcpd(8)
   Main PID: 1661 (dhcpd)
      Tasks: 4 (limit: 5969)
     Memory: 4.7M
        CPU: 37ms
     CGroup: /system.slice/isc-dhcp-server.service
             └─1661 dhcpd -user dhcpd -group dhcpd -f -4 -pf /run/dhcp-server/dhcpd.pid -cf /etc/dhcp/dhcpd.conf

Oct 07 15:16:16 server dhcpd[1661]: Sending on   LPF/enp0s8/08:00:27:1a:6c:50/192.168.18.0/24
Oct 07 15:16:16 server dhcpd[1661]:
Oct 07 15:16:16 server dhcpd[1661]: No subnet declaration for enp0s3 (10.2.18.152).
Oct 07 15:16:16 server dhcpd[1661]: ** Ignoring requests on enp0s3.  If this is not what
Oct 07 15:16:16 server dhcpd[1661]:    you want, please write a subnet declaration
Oct 07 15:16:16 server dhcpd[1661]:    in your dhcpd.conf file for the network segment
Oct 07 15:16:16 server dhcpd[1661]:    to which interface enp0s3 is attached. **
Oct 07 15:16:16 server dhcpd[1661]:
Oct 07 15:16:16 server dhcpd[1661]: Sending on   Socket/fallback/fallback-net
Oct 07 15:16:16 server dhcpd[1661]: Server starting service.
root@server:/etc/dhcp#
```

B.5. Double-check, with the help of the `nmap -sU` command, if the DHCP server is listening on any port. If yes, indicate the port through which the DHCP server listens. Insert screenshot.

```
root@server:/home/user# nmap -sU localhost
Starting Nmap 7.80 ( https://nmap.org ) at 2024-10-08 17:58 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000010s latency).
Not shown: 998 closed ports
PORT   STATE         SERVICE
53/udp open          domain
67/udp open|filtered dhcps

Nmap done: 1 IP address (1 host up) scanned in 1.38 seconds
```

B.6. Why did the DHCP server not appear listening to question B2 on any port and question B5 already appears listening?

- The reason why B2 wasn't configured is because it wasn't receiving requests.

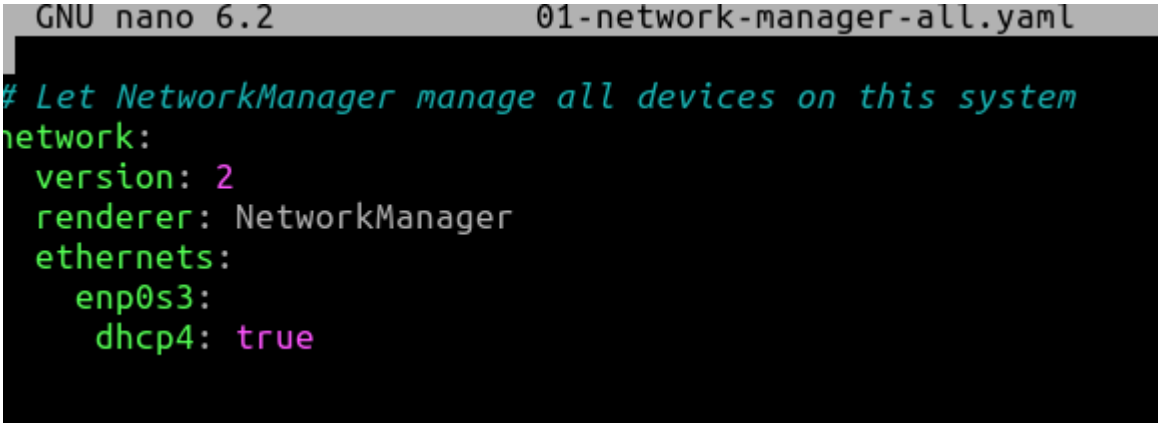
What is the relationship between the subnet of the configuration file and the NIC of the server?

- This relationship depends on the IP address assigned to the network card through which it will receive the requests.

Insert a screenshot and answer, if applicable, the question.

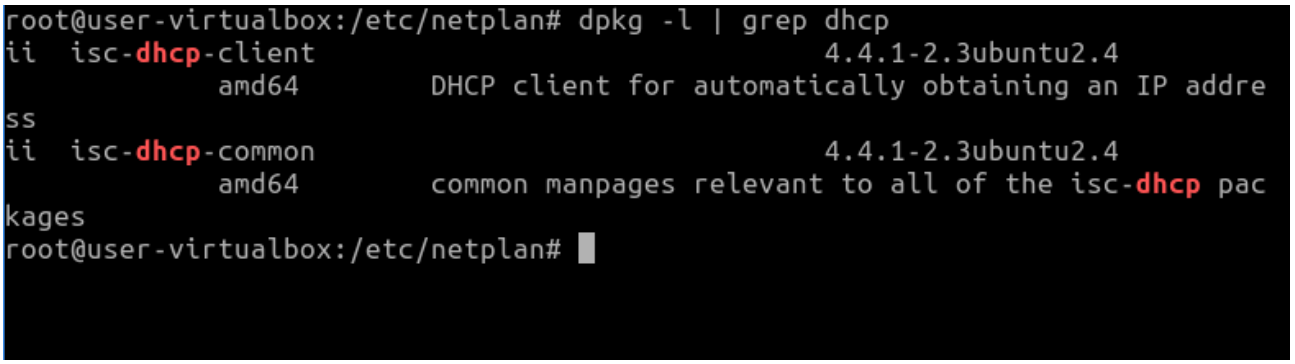
C. DHCP Client Configuration

C.1. Assign a dynamic network configuration to the client. Remember that you have to edit the configuration file `/etc/netplan/xx-network-manager-all.yaml`. Insert screenshot.



C.2. If not IP address is allocated you can start the dynamic allocation process using the `sudo dhclient [interface]` command. Insert screenshot of network interface IP address.

C.3. Why didn't I have to install the DHCP client package? You can use the command `dpkg -L package` or `dpkg -l | grep search-string` to get the packages installed on the system. Insert a screenshot and answer the question.



C.4. In the client's `/var/lib/dhcp/` folder you can check the granting times and the renews of these loans. Insert a screenshot showing this data and indicate the file consulted.

```
  GNU nano 6.2                          dhclient.leases
lease {
  interface "enp0s3";
  fixed-address 192.168.18.5;
  option subnet-mask 255.255.255.0;
  option dhcp-lease-time 584;
  option routers 192.168.18.1;
  option dhcp-message-type 5;
  option dhcp-server-identifier 192.168.18.254;
  option domain-name "eihsa.com";
  renew 2 2024/10/08 18:23:08;
  rebind 2 2024/10/08 18:27:55;
  expire 2 2024/10/08 18:29:08;
}
```

C.5. Using the `ifconfig` command you display the client's network configuration. Insert screenshot.

```
root@ubuntucliente:/var/lib/dhcp# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 100
0
    link/ether 08:00:27:70:ee:c3 brd ff:ff:ff:ff:ff:ff
    inet 192.168.18.4/24 metric 100 brd 192.168.18.255 scope global dynamic enp0s3
       valid_lft 320sec preferred_lft 320sec
    inet 192.168.18.5/24 brd 192.168.18.255 scope global secondary dynamic enp0s3
       valid_lft 461sec preferred_lft 461sec
    inet6 fe80::a00:27ff:fe70:eec3/64 scope link
       valid_lft forever preferred_lft forever
```

D. Advanced management

D.1. Suppose that your client computer is the computer used by the librarian and therefore we want to always have it identified with the same IP address. Configure the server (file `/etc/dhcp/dhcpd.conf`) so that this client has the address 192.168.18.100 reserved. Insert a screenshot showing the client's MAC address.

Insert a screenshot showing the configuration made on the server.

```
host user{
        hardware ethernet 08:00:27:C3:28:47;
        fixed-address 192.168.18.100;
        option routers 192.168.18.1;
        option domain-name "eihsa.com";
        option domain-name-servers 192.168.18.254, 192.168.18.253;
}
```

D.2. Make a request from the client and verify that the IP address assigned is the 192.168.18.100. Insert screenshot.

```
user@user-virtualbox:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group def
ault qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP
 group default qlen 1000
    link/ether 08:00:27:c3:28:47 brd ff:ff:ff:ff:ff:ff
    inet 192.168.18.100/24 brd 192.168.18.255 scope global dynamic noprefixro
ute enp0s3
       valid_lft 520sec preferred_lft 520sec
    inet6 fe80::a00:27ff:fec3:2847/64 scope link
       valid_lft forever preferred_lft forever
```

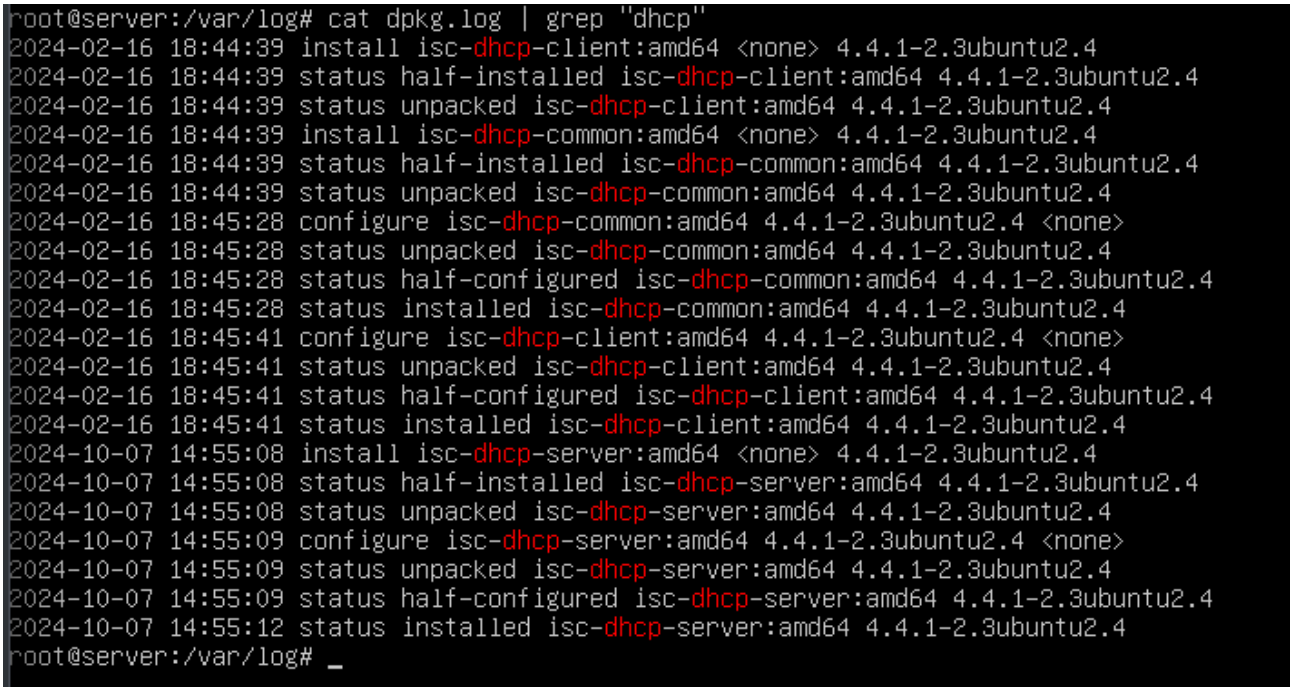
D.3. Check the server's concessions database (`/var/lib/dhcp/dhcpd` file). What can you find in this file? Relate the content of the file to the practice you are developing. Insert a screenshot and answer the question.

```
lease 192.168.18.100 {
  starts 2 2024/10/08 18:30:06;
  ends 2 2024/10/08 18:32:01;
  tstp 2 2024/10/08 18:32:01;
  cltt 2 2024/10/08 18:30:06;
  binding state free;
  hardware ethernet 08:00:27:c3:28:47;
  uid "\001\010\000'\303(G";
}
```

D.4. Go to the `/var/lib/dhcp` folder. Can you find the file for question C.4.? Why do you think this file is not on the server? Insert a screenshot and answer the question.

- We couldn't find the IP that appeared in exercise C4 because the lease for that IP expired, and the client was assigned 100 as a private host. That's why we see the IP 192.168.18.100.

D.5. The log of actions/errors is monitored to the `/var/log/syslog` file. This file is usually very large since it monitors a large number of system services/actions, so you can look for incidents related to the `sudo cat /var/log/syslog | grep dhcp` command. Can you identify any issues related to a configuration error? If so, how did you solve it? Insert a screenshot and answer the question.



Note: Screenshots must incorporate a timestamp (i.e. in a corner you must put a small console and execute the date command, so that the user is seen in the screenshot as well as the day and time of its completion).

E. Extension

E.1. With the help of the Wireshark software (which you will have to run with administrator privileges) analyze the operation of the DHCP service. Run this software, monitor the network card that the DHCP server is listening on, and filter by the BOOTP protocol (predecessor to dhcp). With the results, analyze the operation of the DHCP (type of messages that are sent and addresses) relating it to the protocol studied in class. Insert screenshot and analyze the protocol.

- We have installed the 'tshark' package, which is like Wireshark but designed for the command line.

```
root@server:/var/log# tshark --version
Running as user "root" and group "root". This could be dangerous.
TShark (Wireshark) 3.6.2 (Git v3.6.2 packaged as 3.6.2-2)

Copyright 1998-2022 Gerald Combs <gerald@wireshark.org> and contributors.
License GPLv2+: GNU GPL version 2 or later <https://www.gnu.org/licenses/gpl-2.0.html>
This is free software; see the source for copying conditions. There is NO
warranty; not even for MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.

Compiled (64-bit) using GCC 11.2.0, with libpcap, with POSIX capabilities
(Linux), with libnl 3, with GLib 2.71.2, with zlib 1.2.11, with Lua 5.2.4, with
GnuTLS 3.7.3 and PKCS #11 support, with Gcrypt 1.9.4, with MIT Kerberos, with
MaxMind DB resolver, with nghttp2 1.43.0, with brotli, with LZ4, with Zstandard,
with Snappy, with libxml2 2.9.12, with libsmi 0.4.8.

Running on Linux 5.15.0-122-generic, with Intel(R) Core(TM) i3-4160 CPU @
3.60GHz (with SSE4.2), with 1951 MB of physical memory, with GLib 2.72.4, with
zlib 1.2.11, with libpcap 1.10.1 (with TPACKET_V3), with c-ares 1.18.1, with
GnuTLS 3.7.3, with Gcrypt 1.9.4, with nghttp2 1.43.0, with brotli 1.0.9, with
LZ4 1.9.3, with Zstandard 1.4.8, with libsmi 0.4.8, with LC_TYPE=C.UTF-8, binary
plugins supported (0 loaded).
root@server:/var/log#
```

- Packet capture.

```
root@server:/var/log# tshark -i enp0s8 -f "udp port 67 or udp port 68" -w ejercicio_E1.pcap
Running as user "root" and group "root". This could be dangerous.
Capturing on 'enp0s8'
 ** (tshark:1134) 14:17:58.108784 [Main MESSAGE] -- Capture started.
 ** (tshark:1134) 14:17:58.109435 [Main MESSAGE] -- File: "ejercicio_E1.pcap"
```

- Inspecting the previous capture with the 'bootp' filter, which is the predecessor of DHCP.

```
root@server:/var/log# tshark -r ejercicio_E1.pcap -Y "bootp"
Running as user "root" and group "root". This could be dangerous.
    1 0.000000000 192.168.18.6 → 255.255.255.255 DHCP 342 DHCP Request  - Transaction ID 0xdc898725
```