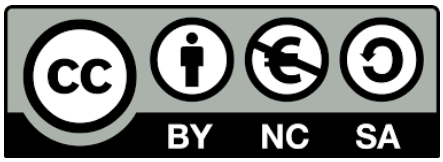
3. Network Services Involved in the Deployment of a Web Application

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.

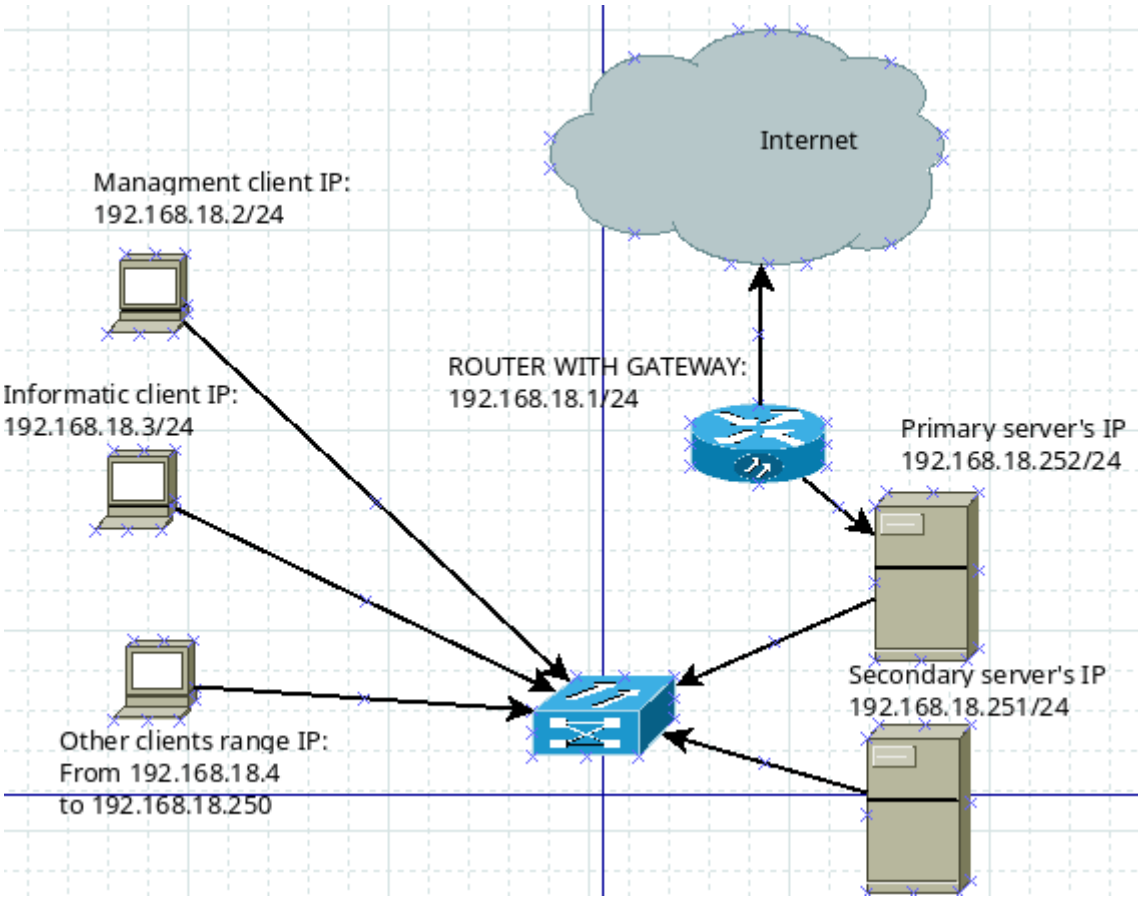
Environment to be simulated:

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.

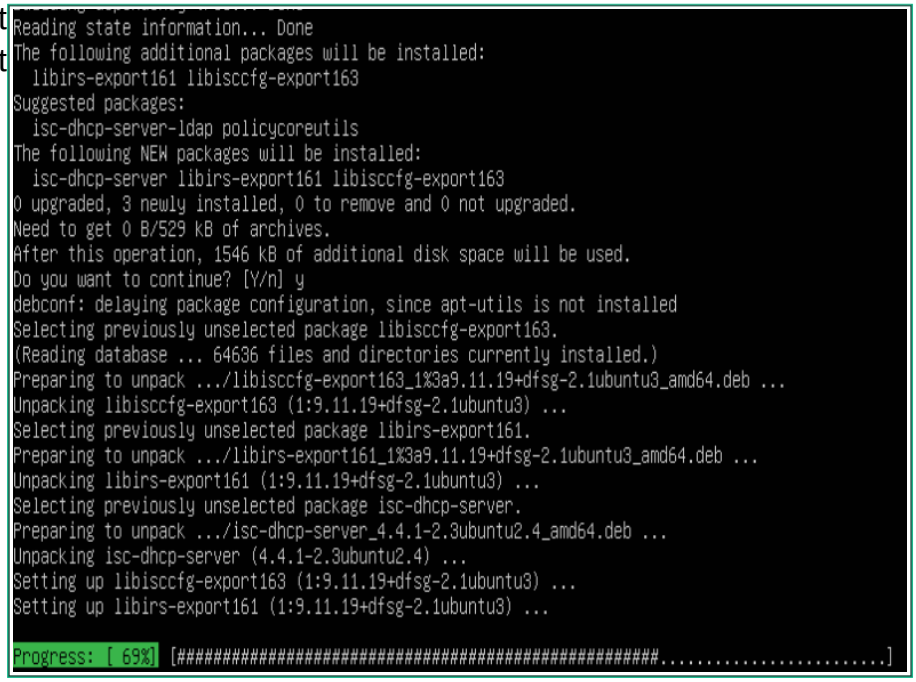
The range of available IP's will consist of 192.168.18.4 to 192.168.18.250 since the client with a static IP, which is the IT department, consists of 192.168.18.3, the maintenance department consists of 192.168.18.2, the link is 192.168.18.1 and 192.168.18.0 is the network address. In the other part of the segment, we end at 192.168.18.250 because the secondary server consists of 192.168.18.251 and the primary server must use 192.168.18.252

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

The default lease time of DHCP configuration its 6000 seconds. In this case, this quantity of time its enough for all the clients that will connect it.

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.

```
network:
    ethernets:
        enp0s3:
            dhcp4: true
        enp0s8:
            addresses: [192.168.18.252/24]
#           gateway4: 192.168.18.1
#           nameservers:
#             search: [eihsa]
#             addresses:
#               - 192.168.18.252
#               - 192.168.18.251
    version: 2
```

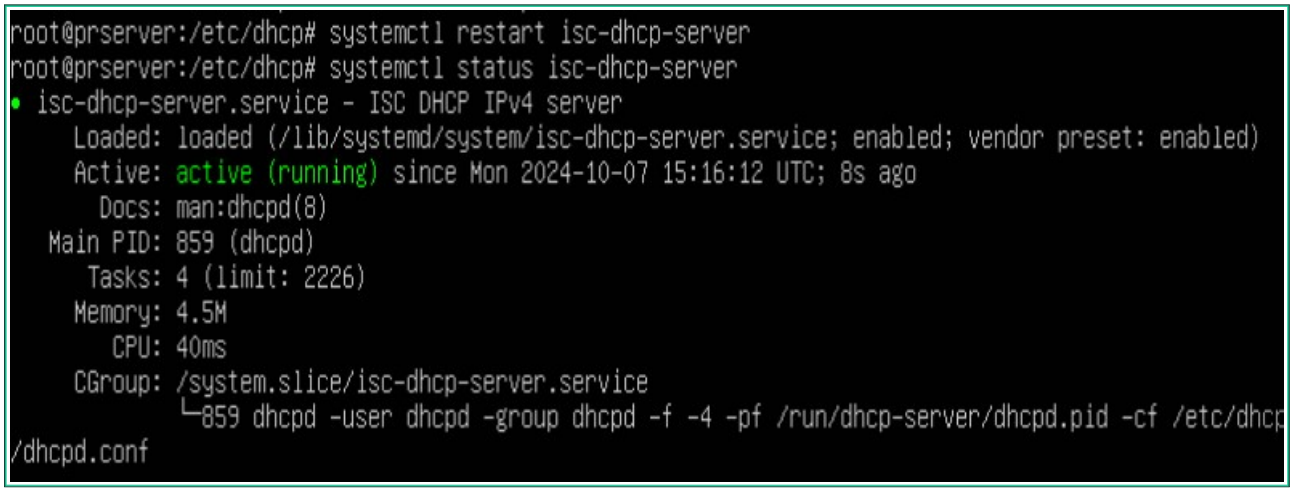
B.2. Check with the help of the `nmap -sU localhost` command if the DHCP server is listening on any port. If yes, indicate the port through which the DHCP server listens. Insert screenshot.

```
root@prserver:/home/prserver# nmap -sU localhost
Starting Nmap 7.80 ( https://nmap.org ) at 2024-10-07 18:33 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000016s latency).
Not shown: 998 closed ports
PORT    STATE         SERVICE
53/udp open          domain

Nmap done: 1 IP address (1 host up) scanned in 1.35 seconds
```

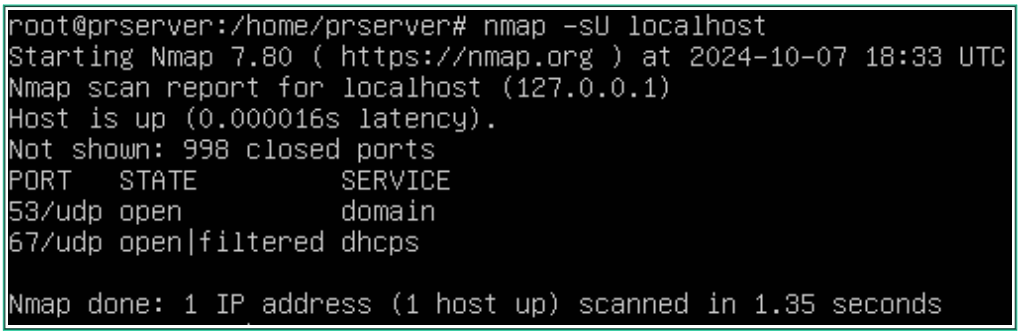
B.3. Access the DHCP server configuration file `/etc/dhcp/dhcpd.conf`. Configure it (creating a new subnet) taking into account the previous requirements. Insert screenshot.

```
  GNU nano 6.2                                    dhcpd.conf
# dhcpd.conf
#
# Sample configuration file for ISC dhcpd
#
# Attention: If /etc/ltsp/dhcpd.conf exists, that will be used as
# configuration file instead of this file.
#

# option definitions common to all supported networks...
option domain-name "example.org";
option domain-name-servers ns1.example.org, ns2.example.org;

default-lease-time 600;
max-lease-time 7200;


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 6000;
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.



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.



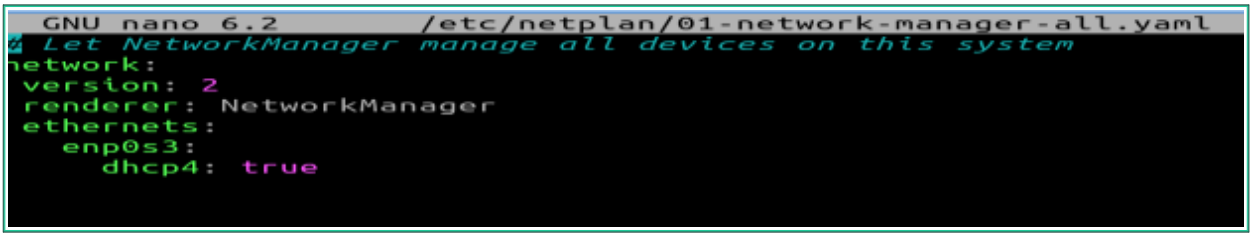
B.6. Why did the DHCP server not appear listening to question B2 on any port and question B5 already appears listening? What is the relationship between the subnet of the configuration file and the NIC of the server? Insert a screenshot and answer, if applicable, the question.

The reason was because in question B2 the server was not configured so it did not receive requests and was not active, with the current configuration it is already active.

It is related to the fact that depending on the IP that is assigned to the network card, it will make requests for it.

C. DHCP Client Configuration

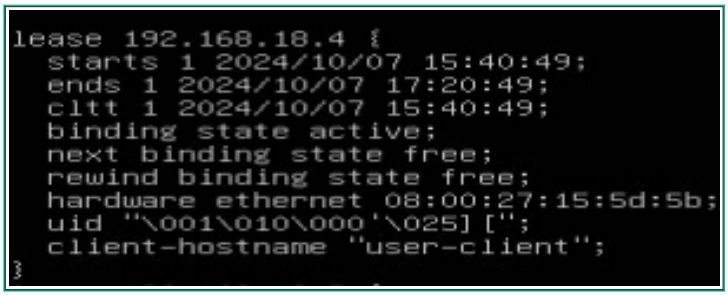
C.1. Assign a dynamic network configuration to the client. Remember that you have to edit the configuration file `/etc/netplan/xx-network-manager-all.yaml`. Insert screenshot.



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.



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

```
root@user-client:/etc/netplan# 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 08:00:27:15:5d:5b brd ff:ff:ff:ff:ff:ff
    inet 192.168.18.4/24 brd 192.168.18.255 scope global dynamic noprefixrout
e enp0s3
       valid_lft 5996sec preferred_lft 5996sec
    inet6 fe80::a00:27ff:fe15:5d5b/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-client{

hardware ethernet 08:00:27:15:5D:5B;
fixed-address 192.168.18.100;
option routers 192.168.18.1;
option domain-name "eihsa.com";
option domain-name-servers 192.168.18.252, 192.168.18.251;
}
```

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

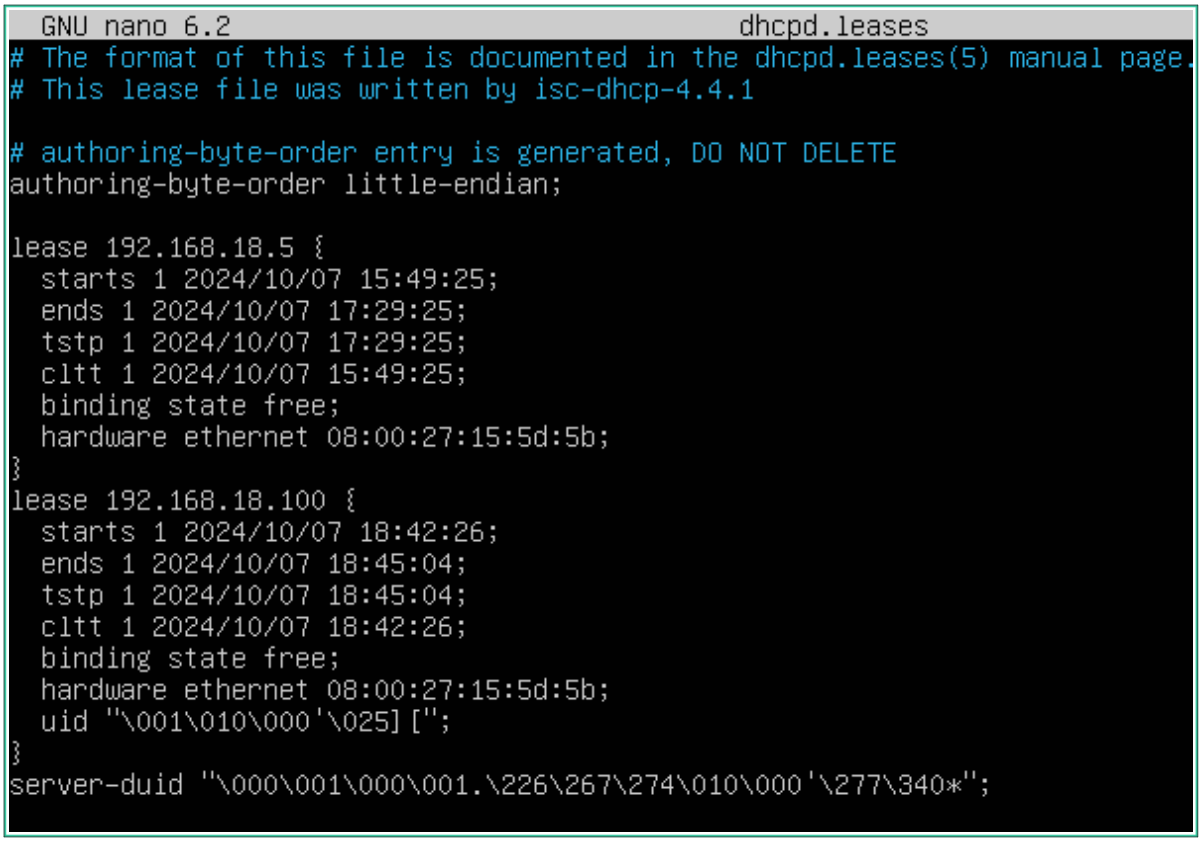
```
user@user-client:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group def
ault qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP
 group default qlen 1000
    link/ether 08:00:27:15:5d:5b 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 5915sec preferred_lft 5915sec
    inet6 fe80::a00:27ff:fe15:5d5b/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.

```
# authoring-byte-order entry is generated, DO NOT DELETE
authoring-byte-order little-endian;

lease 192.168.18.5 {
  starts 1 2024/10/07 15:49:25;
  ends 1 2024/10/07 17:29:25;
  tstp 1 2024/10/07 17:29:25;
  cltt 1 2024/10/07 15:49:25;
  binding state free;
  hardware ethernet 08:00:27:15:5d:5b;
}
lease 192.168.18.4 {
  starts 1 2024/10/07 18:42:26;
  ends 1 2024/10/07 20:22:26;
  tstp 1 2024/10/07 20:22:26;
  cltt 1 2024/10/07 18:42:26;
  binding state active;
  next binding state free;
  rewind binding state free;
  hardware ethernet 08:00:27:15:5d:5b;
  uid "\001\010\000'\025]";
  client-hostname "user-client";
}
server-duid "\000\001\000\001.\226\267\274\010\000'\277\340*";

lease 192.168.18.4 {
  starts 1 2024/10/07 18:42:26;
  ends 1 2024/10/07 18:45:04;
  tstp 1 2024/10/07 18:45:04;
  cltt 1 2024/10/07 18:42:26;
  binding state free;
  hardware ethernet 08:00:27:15:5d:5b;
  uid "\001\010\000'\025]";
}
root@prserver:/var/lib/dhcp# ls
dhcpd.leases  dhcpd.leases~  dhcpd6.leases  dhcpd6.leases~
```

In this file you cand find the concessions of the IP's assigned to the clients were connected to the server

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.



```
  GNU nano 6.2                                    dhcpd.leases
# The format of this file is documented in the dhcpd.leases(5) manual page.
# This lease file was written by isc-dhcp-4.4.1

# authoring-byte-order entry is generated, DO NOT DELETE
authoring-byte-order little-endian;

lease 192.168.18.5 {
  starts 1 2024/10/07 15:49:25;
  ends 1 2024/10/07 17:29:25;
  tstp 1 2024/10/07 17:29:25;
  cltt 1 2024/10/07 15:49:25;
  binding state free;
  hardware ethernet 08:00:27:15:5d:5b;
}
lease 192.168.18.100 {
  starts 1 2024/10/07 18:42:26;
  ends 1 2024/10/07 18:45:04;
  tstp 1 2024/10/07 18:45:04;
  cltt 1 2024/10/07 18:42:26;
  binding state free;
  hardware ethernet 08:00:27:15:5d:5b;
  uid "\001\010\000'\025][";
}
server-duid "\000\001\000\001.\226\267\274\010\000'\277\340*";
```

This client was the first to connect to our server so it received 192.168.18.4. The change made is that from its MAC address we have determined that the private host receives 192.168.18.100 and that is why 192.168.18.4 does not appear in the concessions file but now 192.168.18.100 appears.

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.

```
root@prserver:/var/log# cat dpkg.log| grep dhcp
2024-09-11 14:22:08 install isc-dhcp-client:amd64 <none> 4.4.1-2.3ubuntu2.4
2024-09-11 14:22:08 status half-installed isc-dhcp-client:amd64 4.4.1-2.3ubuntu2.4
2024-09-11 14:22:08 status unpacked isc-dhcp-client:amd64 4.4.1-2.3ubuntu2.4
2024-09-11 14:22:08 install isc-dhcp-common:amd64 <none> 4.4.1-2.3ubuntu2.4
2024-09-11 14:22:08 status half-installed isc-dhcp-common:amd64 4.4.1-2.3ubuntu2.4
2024-09-11 14:22:08 status unpacked isc-dhcp-common:amd64 4.4.1-2.3ubuntu2.4
2024-09-11 14:22:20 configure isc-dhcp-common:amd64 4.4.1-2.3ubuntu2.4 <none>
2024-09-11 14:22:20 status unpacked isc-dhcp-common:amd64 4.4.1-2.3ubuntu2.4
2024-09-11 14:22:20 status half-configured isc-dhcp-common:amd64 4.4.1-2.3ubuntu2.4
2024-09-11 14:22:20 status installed isc-dhcp-common:amd64 4.4.1-2.3ubuntu2.4
2024-09-11 14:22:25 configure isc-dhcp-client:amd64 4.4.1-2.3ubuntu2.4 <none>
2024-09-11 14:22:25 status unpacked isc-dhcp-client:amd64 4.4.1-2.3ubuntu2.4
2024-09-11 14:22:25 status half-configured isc-dhcp-client:amd64 4.4.1-2.3ubuntu2.4
2024-09-11 14:22:25 status installed isc-dhcp-client:amd64 4.4.1-2.3ubuntu2.4
2024-10-07 14:22:12 install isc-dhcp-server:amd64 <none> 4.4.1-2.3ubuntu2.4
2024-10-07 14:22:12 status half-installed isc-dhcp-server:amd64 4.4.1-2.3ubuntu2.4
2024-10-07 14:22:13 status unpacked isc-dhcp-server:amd64 4.4.1-2.3ubuntu2.4
2024-10-07 14:22:15 configure isc-dhcp-server:amd64 4.4.1-2.3ubuntu2.4 <none>
2024-10-07 14:22:15 status unpacked isc-dhcp-server:amd64 4.4.1-2.3ubuntu2.4
2024-10-07 14:22:17 status half-configured isc-dhcp-server:amd64 4.4.1-2.3ubuntu2.4
2024-10-07 14:22:23 status installed isc-dhcp-server:amd64 4.4.1-2.3ubuntu2.4
```

Actually, the syslog file its deprecated, but this logs can find in the same folder but the file is called dpkg.log and using grep | “dhcp” you can find all the changes applied in the server

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.

First we will have to install the tshark package, which is the wireshark prepared for CLI:

```
root@prserver:/var/log# tshark -v
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 1963 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).
```

To capture the operation of DHCP with thsark we must execute tshark -i enp0s8 (name of the interface through which DHCP listens for requests) -f “udp port 67 or udp port 68” (ports where DHCP listens) -w capture.pcap(where you will save the information):

```
root@prserver:/var/log# tshark -i enp0s8 -f "udp port 67 or udp port 68" -w captura.pcap
Running as user "root" and group "root". This could be dangerous.
Capturing on 'enp0s8'
 ** (tshark:1001) 13:59:31.773778 [Main MESSAGE] -- Capture started.
 ** (tshark:1001) 13:59:31.773985 [Main MESSAGE] -- File: "captura.pcap"
```

Finally, to check adding the “bootp” filter, we will execute thsark -r capture.pcap -Y “bootp”:

```
root@prserver:/var/log# tshark -r captura_dhcp.pcap -Y "bootp"
Running as user "root" and group "root". This could be dangerous.
    1 0.000000000       0.0.0.0 → 255.255.255.255 DHCP 337 DHCP Request  - Transaction ID 0xeb2100f1
    2 0.000287092 192.168.18.252 → 192.168.18.100 DHCP 342 DHCP ACK      - Transaction ID 0xeb2100f1
```

The first request is the same since the MAC has value 0000000 and the second request is the configured service where the server IP is 192.168.18.252 and the client is the private host declared previously with the IP 192.168.18.100 and the MAC is the same