P5: DHCP

Exercise 1.1– In this exercise we analize the DHCP service using the scenario dns-basic. After the scenario has been started, execute the labels initial and dhcp:

//from terminal
simctl dns-basic sh
exec initial
exec dhcp

1. In joker, check if a DHCP server is running and analyze the DHCP configuration file (/etc/dhcp3/dhcpd.conf).

//from joker
/etc/init.d/dhcp3-server status
netstat -np | grep dhcp

```
joker:~# /etc/init.d/dhcp3-server status
Status of DHCP server: dhcpd3 is running.
joker:~# netstat -np | grep dhcp
unix  2      [ ]         DGRAM                    1634     1182/dhcpd3
```

the dhcpd3 is running in PID 1182

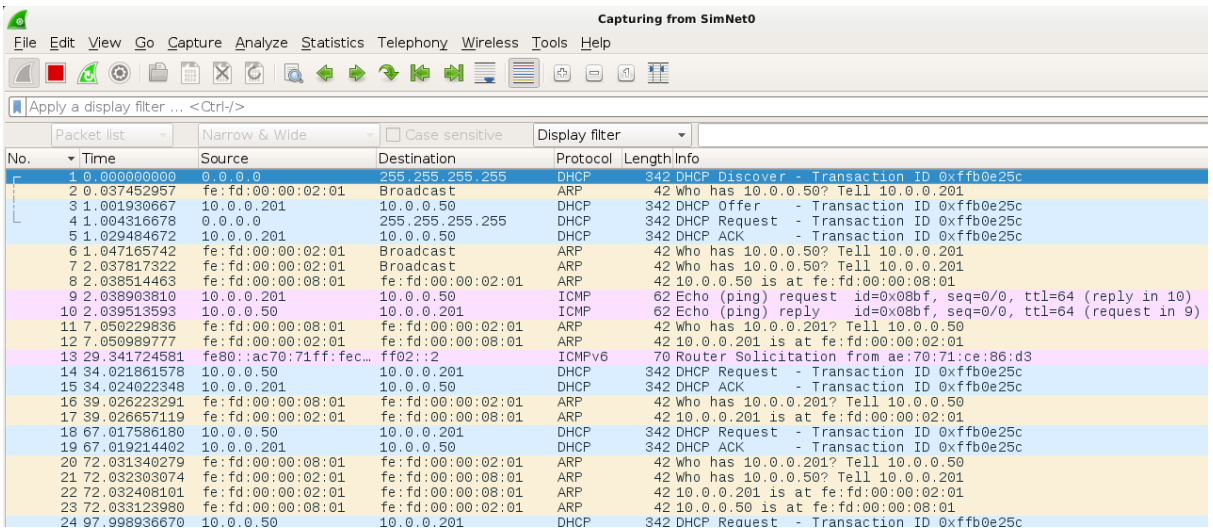
2. Capture with wireshark tap0 and explain the flow of DHCP messages captured when executing the following command line:

//from alice
dhclient3 eth1

```
alice:~# dhclient3 eth1
Internet Systems Consortium DHCP Client V3.1.1
Copyright 2004-2008 Internet Systems Consortium.
All rights reserved.
For info, please visit http://www.isc.org/sw/dhcp/

Listening on LPF/eth1/fe:fd:00:00:08:01
Sending on   LPF/eth1/fe:fd:00:00:08:01
Sending on   Socket/fallback
DHCPDISCOVER on eth1 to 255.255.255.255 port 67 interval 8
DHCPOFFER from 10.0.0.201
DHCPREQUEST on eth1 to 255.255.255.255 port 67
DHCPACK from 10.0.0.201
bound to 10.0.0.51 -- renewal in 31 seconds.
```

Capture at least 2 minutes. Which is the assigned IP? Which is the content of the file /etc/resolv.conf of alice. Take a look at the file /var/lib/dhcp3/dhclient.leases and explain the content of this file. Explain the renew, rebind and expire fields. To do so, you can use the manual page of dhclient.conf. Can you now access Alice by her name? why?



The alice ip is 10.0.0.50 (client). The server ip is 10.0.0.201.

//from alice
cat /etc/resolv.conf

```
alice:~# cat /etc/resolv.conf
domain example.com
search example.com
nameserver 10.0.0.21
```

cat /var/lib/dhcp3/dhclient.leases

```
alice:~# cat /var/lib/dhcp3/dhclient.leases | more
lease {
  interface "eth1";
  fixed-address 10.0.0.50;
  option subnet-mask 255.255.255.0;
  option dhcp-lease-time 70;
  option dhcp-message-type 5;
  option domain-name-servers 10.0.0.21;
  option dhcp-server-identifier 10.0.0.201;
  option domain-name "example.com";
  renew 5 2022/10/14 17:25:09;
  rebind 5 2022/10/14 17:25:39;
  expire 5 2022/10/14 17:25:48;
}
lease {
  interface "eth1";
  fixed-address 10.0.0.50;
  option subnet-mask 255.255.255.0;
  option dhcp-lease-time 70;
  option dhcp-message-type 5;
  option domain-name-servers 10.0.0.21;
  option dhcp-server-identifier 10.0.0.201;
  option domain-name "example.com";
  renew 5 2022/10/14 17:25:45;
  rebind 5 2022/10/14 17:26:10;
  expire 5 2022/10/14 17:26:19;
}
lease {
--More--
```

This is a register of all the leases including the time which they are renewed, when they are rebinded and when they expire.

Renew: last lease renew time.
Rebind: time on wich we should renew.
Expire: ip expire time if it's not renewed.

Falta acceder a alice por su nombre

No es pot accedir per nom a la alice pk s'ha activat el dhcp dinamic i la adreça ip donada no es la mateixa que la que te el servidor de dns, per tant si fas ping a alice.example.com. o a alice, et redirigira a la adreça del servidor de dns.

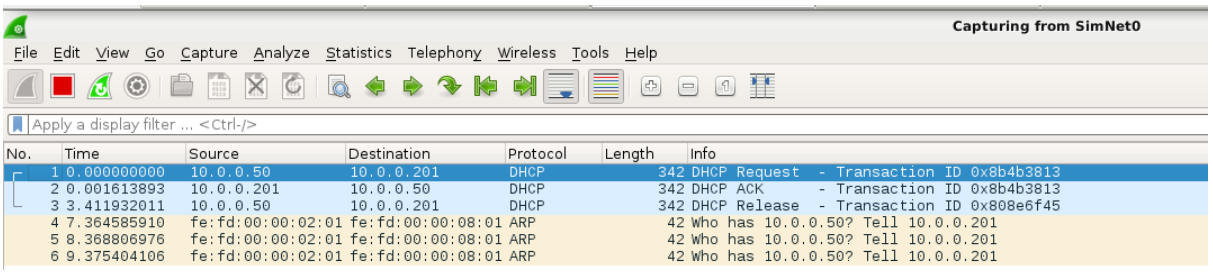
podriem activar dhcp manual?, SI apartat 4.

3. Capture with wireshark tap0 and explain the flow of DHCP messages captured when executing the following command line:

//from alice
dhclient3 -r eth1

```
alice:~# dhclient3 -r eth1
There is already a pid file /var/run/dhclient.pid with pid 1181
killed old client process, removed PID file
Internet Systems Consortium DHCP Client V3.1.1
Copyright 2004-2008 Internet Systems Consortium.
All rights reserved.
For info, please visit http://www.isc.org/sw/dhcp/

Listening on LPF/eth1/fe:fd:00:00:08:01
Sending on   LPF/eth1/fe:fd:00:00:08:01
Sending on   Socket/fallback
DHCPRELEASE on eth1 to 10.0.0.201 port 67
```



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.0.50	10.0.0.201	DHCP	342	DHCP Request - Transaction ID 0x8b4b3813
2	0.001613893	10.0.0.201	10.0.0.50	DHCP	342	DHCP ACK - Transaction ID 0x8b4b3813
3	3.411932011	10.0.0.50	10.0.0.201	DHCP	342	DHCP Release - Transaction ID 0x808e6f45
4	7.364585910	fe:fd:00:00:02:01	fe:fd:00:00:08:01	ARP	42	Who has 10.0.0.50? Tell 10.0.0.201
5	8.368806976	fe:fd:00:00:02:01	fe:fd:00:00:08:01	ARP	42	Who has 10.0.0.50? Tell 10.0.0.201
6	9.375404106	fe:fd:00:00:02:01	fe:fd:00:00:08:01	ARP	42	Who has 10.0.0.50? Tell 10.0.0.201

cat /var/lib/dhcp3/dhclient.leases

```
alice:~# cat /var/lib/dhcp3/dhclient.leases
lease {
  interface "eth1";
  fixed-address 10.0.0.50;
  option subnet-mask 255.255.255.0;
  option dhcp-lease-time 70;
  option dhcp-message-type 5;
  option dhcp-server-identifier 10.0.0.201;
  option domain-name-servers 10.0.0.21;
  option domain-name "example.com";
  renew 3 2022/10/19 15:52:43;
  rebind 3 2022/10/19 15:53:16;
  expire 3 2022/10/19 15:53:25;
}
lease {
  interface "eth1";
  fixed-address 10.0.0.50;
  option subnet-mask 255.255.255.0;
  option dhcp-lease-time 70;
  option dhcp-message-type 5;
  option dhcp-server-identifier 10.0.0.201;
  option domain-name-servers 10.0.0.21;
  option domain-name "example.com";
  renew 3 2022/10/19 15:52:18;
  rebind 3 2022/10/19 15:52:18;
  expire 3 2022/10/19 15:52:18;
}
```

We can observe that the 3 lease times are the same.

4. Capture with wireshark tap0 and explain the flow of DHCP and DNS messages captured when you modify the configuration of the DHCP server in the joker to activate the manual allocation for alice.example.com. Restart the DHCP server of joker and try the configuration.

//from joker

nano /etc/dhcp3/dhcpd.conf

```
  GNU nano 2.0.7          File: /etc/dhcp3/dhcpd.conf

# This is a very basic subnet declaration.

subnet 10.0.0.0 netmask 255.255.255.0 {
  range 10.0.0.50 10.0.0.60;
}

host alice {
  hardware ethernet  fe:fd:00:00:08:01;
  fixed-address alice.example.com;
}
```

//from joker

/etc/init.d/dhcp3-server restart

```
joker:~# /etc/init.d/dhcp3-server restart
Stopping DHCP server: dhcpd3.
Starting DHCP server: dhcpd3.
```

//from alice

dhclient3 eth1

```
alice:~#  dhclient3 eth1
Internet Systems Consortium DHCP Client V3.1.1
Copyright 2004-2008 Internet Systems Consortium.
All rights reserved.
For info, please visit http://www.isc.org/sw/dhcp/

Listening on LPF/eth1/fe:fd:00:00:08:01
Sending on   LPF/eth1/fe:fd:00:00:08:01
Sending on   Socket/fallback
DHCPDISCOVER on eth1 to 255.255.255.255 port 67 interval 8
DHCPOFFER from 10.0.0.201
DHCPREQUEST on eth1 to 255.255.255.255 port 67
DHCPACK from 10.0.0.201
bound to 10.0.0.22 -- renewal in 31 seconds.
```

Capturing from SimNet0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xb9d9080f
2	0.037567833	fe:fd:00:00:02:01	Broadcast	ARP	42	Who has 10.0.0.1? Tell 10.0.0.201
3	0.037798057	fe:fd:00:00:01:01	fe:fd:00:00:02:01	ARP	42	10.0.0.1 is at fe:fd:00:00:01:01
4	0.037985914	10.0.0.201	10.0.0.1	DNS	88	Standard query 0x1f75 A alice.example.com OPT
5	0.039294437	10.0.0.1	10.0.0.201	DNS	122	Standard query response 0x1f75 A alice.example.com NS nsc.com A 10.0.0.11 OPT
6	0.039523521	10.0.0.201	10.0.0.1	DNS	70	Standard query 0x4038 NS <Root> OPT
7	0.039816612	10.0.0.1	10.0.0.201	DNS	110	Standard query response 0x4038 NS <Root> NS ROOT-SERVER A 10.0.0.1 OPT
8	0.062430553	fe:fd:00:00:02:01	Broadcast	ARP	42	Who has 10.0.0.11? Tell 10.0.0.201
9	0.062651627	fe:fd:00:00:03:01	fe:fd:00:00:02:01	ARP	42	10.0.0.11 is at fe:fd:00:00:03:01
10	0.062823426	10.0.0.201	10.0.0.11	DNS	88	Standard query 0x3b92 A alice.example.com OPT
11	0.064056759	10.0.0.11	10.0.0.201	DNS	123	Standard query response 0x3b92 A alice.example.com NS nsce.example.com A 10.0.0.21 OPT
12	0.086198150	fe:fd:00:00:02:01	Broadcast	ARP	42	Who has 10.0.0.21? Tell 10.0.0.201
13	0.086453884	fe:fd:00:00:04:01	fe:fd:00:00:02:01	ARP	42	10.0.0.21 is at fe:fd:00:00:04:01
14	0.086607245	10.0.0.201	10.0.0.21	DNS	88	Standard query 0x5fe2 A alice.example.com OPT
15	0.087784651	10.0.0.21	10.0.0.201	DNS	139	Standard query response 0x5fe2 A alice.example.com A 10.0.0.22 NS nsce.example.com A 10.0.0.21 OPT
16	0.091150009	10.0.0.201	10.0.0.22	DHCP	342	DHCP Offer - Transaction ID 0xb9d9080f
17	0.091736848	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0xb9d9080f
18	0.092569700	10.0.0.201	10.0.0.22	DHCP	342	DHCP ACK - Transaction ID 0xb9d9080f
19	5.093474125	fe:fd:00:00:04:01	fe:fd:00:00:02:01	ARP	42	Who has 10.0.0.201? Tell 10.0.0.21
20	5.093755850	fe:fd:00:00:02:01	fe:fd:00:00:04:01	ARP	42	10.0.0.201 is at fe:fd:00:00:02:01
21	30.790696045	fe:fd:00:00:08:01	Broadcast	ARP	42	Who has 10.0.0.201? Tell 10.0.0.22
22	30.790889758	fe:fd:00:00:02:01	fe:fd:00:00:08:01	ARP	42	10.0.0.201 is at fe:fd:00:00:02:01
23	30.791059961	10.0.0.22	10.0.0.201	DHCP	342	DHCP Request - Transaction ID 0xb9d9080f
24	30.791449416	10.0.0.201	10.0.0.22	DHCP	342	DHCP ACK - Transaction ID 0xb9d9080f
25	35.808264871	fe:fd:00:00:02:01	fe:fd:00:00:08:01	ARP	42	Who has 10.0.0.22? Tell 10.0.0.201
26	35.808503482	fe:fd:00:00:08:01	fe:fd:00:00:02:01	ARP	42	10.0.0.22 is at fe:fd:00:00:08:01

Now Alice ip is 10.0.0.22 the initial ip.

And the connection is done, by sending the first DHCP broadcast and after establishing a connection with servers with DNS frames (funciona como el lab 4), because Alice is in @example.com and this zone is controlled by DNS. After that, there is an exchange of DHCP frames, DHCP offer and DHCP Request and finally DHCP ACK.