

1.- L'adreça del servidor és 192.168.88.1.

2.- Per començar, el client envia un missatge de descobriment (Discover) per localitzar servidors DHCP disponibles a la xarxa, a continuació els servidors DHCP responen amb un missatge d'oferta (Offer) que inclou una adreça IP disponible i altres paràmetres de configuració de xarxa, el client selecciona una de les ofertes rebudes i respon amb un missatge de sol·licitud (Request) per indicar al servidor que accepta l'adreça IP oferta i per finalitzar el servidor DHCP confirma l'assignació de l'adreça IP enviant un missatge de reconeixement (ACK) al client.

Filter: udp.port		Expression...		Clear	Apply	Desa
No.	Time	Source	Destination	Protocol	Length	Info
8	13.654771000	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xc548ee73
12	14.182934000	192.168.88.1	192.168.88.254	DHCP	342	DHCP Offer - Transaction ID 0xc548ee73
13	14.183431000	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0xc548ee73
14	14.184828000	192.168.88.1	192.168.88.254	DHCP	342	DHCP ACK - Transaction ID 0xc548ee73

3.- DHCP Discover: La seva finalitat és permetre que el client localitzi els servidors DHCP disponibles a la xarxa.

DHCP Offer: La seva finalitat és permetre que els servidors DHCP ofereixin una adreça IP i altres paràmetres de configuració al client.

DHCP Request: La seva finalitat és permetre que el client accepti una de les ofertes rebudes i sol·liciti formalment l'assignació de l'adreça IP.

DHCP ACK: La seva finalitat és confirmar l'assignació de l'adreça IP i proporcionar qualsevol informació addicional necessària per a la configuració de la xarxa.

DHCP Release: La seva finalitat és permetre que el client alliberi l'adreça IP quan ja no en necessita, tornant-la al grup d'adreces disponibles del servidor DHCP.

4.- Els missatges DHCP entre el client i el servidor es vinculen utilitzant l'adreça MAC, que és única per a cada dispositiu de xarxa i permet al servidor DHCP reconèixer el client; l'identificador de transacció, un número únic generat pel client que correlaciona les sol·licituds i les respostes entre el client i el servidor; i l'adreça IP del client, que s'utilitza als missatges següents una vegada assignada.

5.- Els missatges que tenen com a adreça d'origen 0.0.0.0 són perquè el client encara no té assignada una adreça IP vàlida. Això passa principalment quan un client DHCP inicia el procés per obtenir una adreça IP i envia un missatge DHCP Discover amb adreça d'origen 0.0.0.0 perquè encara no té una adreça IP assignada; i després de rebre ofertes de servidors DHCP, el client també envia un DHCP Request amb adreça d'origen 0.0.0.0, ja que encara no ha confirmat ni rebut l'assignació final d'una adreça IP.

6.- L'adreça 255.255.255.255 s'utilitza per enviar missatges a tots els dispositius d'una xarxa local al mateix temps. Això es diu broadcast, i serveix sobretot quan un dispositiu no coneix les adreces IP dels altres o la seva pròpia.

S'utilitza:

-Per demanar una IP: Quan un dispositiu es connecta a la xarxa i no té IP, envia un missatge a 255.255.255.255 per rebre'n una del servidor.

-Per saber quina és l'adreça física (MAC) d'un dispositiu: Si un ordinador sap la IP d'un altre però no la seva MAC, envia un missatge de broadcast per trobar-la.

-Per enviar avisos a tothom de la xarxa: Alguns protocols envien missatges que tothom ha de veure, com alertes o informació important.

Aquests missatges només es queden dins la mateixa xarxa, ja que els routers no els deixen passar més enllà. Es sol utilitzar amb el protocol DHCP Discover i DHCP Request, que hem utilitzat a la sessió de laboratori.

7.- Els principals paràmetres que es reben per DHCP són: L'adreça IP, que determina l'adreça única que tindrà el dispositiu dins la xarxa, la màscara de xarxa, que defineix quina part de l'adreça IP correspon a la xarxa i quina als dispositius, i que ajuda a determinar a quina subxarxa pertany el dispositiu. El Gateway, que és l'adreça IP del router o dispositiu que connecta la xarxa local amb altres xarxes, com internet. Els servidors DNS, que són les adreces IP dels servidors que s'utilitzen per resoldre noms de domini (per exemple convertir google.com en una IP). Per acabar tindríem el lease time (temps de concessió), que és el temps durant el qual el dispositiu pot utilitzar l'adreça IP assignada abans de necessitar-ne una renovació.

8.- No, la configuració que el servidor DHCP assigna no és àlida per sempre, està limitada pel lease time, que és el que hem explicat a la pregunta anterior.

Quan un dispositiu rep una adreça IP, el servidor DHCP li diu quant de temps pot utilitzar-la. Quan arriba a la meitat d'aquest temps, el dispositiu intenta renovar la concessió. Si el servidor ho permet, el dispositiu pot seguir usant la mateixa configuració per un altre període. Si no es pot renovar (per exemple, si el dispositiu s'ha desconnectat o hi ha problemes de xarxa), l'adreça IP caduca quan s'acaba el lease time, i el dispositiu ha de demanar una nova IP. Això assegura que les adreces IP no quedin bloquejades per dispositius que ja no estan connectats.

9.- El servidor DHCP pot identificar els clients encara que no tinguin una adreça IP assignada gràcies a un identificador únic que té cada dispositiu: la adreça MAC (Media Access Control). L'adreça MAC és una adreça única assignada a la targeta de xarxa de cada dispositiu. Quan un dispositiu s'incorpora a la xarxa i demana una IP, envia la seva adreça MAC al servidor DHCP. En el procés de sol·licitar una IP, el dispositiu envia una petició DHCP Discover, incloent-hi la seva adreça MAC. El servidor DHCP utilitza aquesta informació per diferenciar els clients i associar-los una adreça IP. L'adreça MAC és com una empremta digital de cada dispositiu en la xarxa, i és essencial perquè el servidor DHCP pugui reconèixer cada client, fins i tot abans de tenir una IP.

10.- El rang d'IPs va des del 192.168.88.10 fins al 192.168.88.254, la porta d'enllaç predeterminada és 192.168.88.1 i el temps de concessió (lease time) durant el qual una adreça IP assignada és vàlida és de 10 minuts.

11.- Les IPs entre 192.168.99.100 i 192.168.99.110.

12.- Si tot funciona correctament, és poc probable que s'arribi a esgotar la configuració en préstec (adreces IP assignades pel servidor DHCP), però podria passar en determinades circumstàncies. Raons per les quals podria esgotar-se: nombre limitat d'adreces IP disponibles, si el rang d'IP configurat al servidor DHCP (l'anomenat pool d'IP) és molt petit i hi ha molts dispositius connectats al mateix temps, es podrien acabar les adreces disponibles per assignar; lease time massa llarg, si la durada de les concessions DHCP (lease time) és massa llarga, les IP poden quedar bloquejades per dispositius que ja no estan connectats, deixant menys IP disponibles per a nous dispositius; dispositius que no alliberen la IP, alguns dispositius poden desconnectar-se de la xarxa sense alliberar la seva adreça IP, fent que el servidor DHCP no les pugui reutilitzar fins que expiri la concessió; mal ús o configuració inadequada, si el servidor DHCP està mal configurat o hi ha dispositius que sol·liciten múltiples IP, podria causar un esgotament del pool. Per evitar aquest problema, és important configurar un rang d'IP adequat per al nombre de dispositius de la

xarxa i ajustar correctament el lease time per assegurar que les IP s'alliberin quan ja no són necessàries.

13.- Un host renova el préstec de la seva adreça IP quan ha passat la meitat del temps de concessió que li ha assignat el servidor DHCP. Aquest període s'anomena lease time, i és el temps durant el qual el dispositiu pot utilitzar la IP assignada.

Per exemple, si el lease time és de 24 hores, el dispositiu intentarà renovar-lo al cap de 12 hores. Si la renovació és correcta, el dispositiu continuarà utilitzant la mateixa IP per un altre període. Si no es pot renovar, seguirà intentant-ho fins que s'acabi el temps. Si arriba al final sense haver-la pogut renovar, haurà de demanar una nova adreça IP al servidor DHCP.

14.- La principal diferència entre l'intercanvi inicial de missatges entre un client i un servidor DHCP i els posteriors és el context de la connexió i els missatges que s'utilitzen. Quan un client es connecta per primera vegada, envia un missatge DHCP Discover per cercar un servidor DHCP, ja que no té adreça IP. El servidor respon amb un DHCP Offer, oferint una adreça IP i altres paràmetres. Després de l'acceptació mitjançant un DHCP Request, el servidor confirma l'assignació amb un DHCP Acknowledgment. Un cop el client té una IP, els intercanvis posteriors es fan per renovar la concessió. Quan es compleix la meitat del lease time, el client envia un DHCP Request per renovar la seva IP, que pot ser unicast si el servidor reconeix el client. En resum, durant l'intercanvi inicial el client no té IP i ha de descobrir el servidor, mentre que en les renovacions ja té una IP assignada i sol·licita mantenir-la o actualitzar la configuració.

15.- Decidir si configurar un servidor per DHCP depèn de diversos factors, com la mida de la xarxa i els dispositius que hi connectes. Els avantatges del DHCP inclouen: Facilitar la gestió de la xarxa, ja que automatitza l'assignació d'adreces IP, reduint els errors humans. Estalviar temps, perquè els dispositius poden obtenir una IP automàticament, i oferir flexibilitat per adaptar-se als canvis en el nombre de dispositius.

Pel que fa a la configuració, hi ha dues opcions: Dinàmica: És la millor per a xarxes amb dispositius que s'hi connecten i desconnecten sovint, com en oficines. Estàtica (reserves): Aquesta opció és adequada per a dispositius que necessiten una IP fixa, com ara impressores o servidors, per facilitar-ne la identificació.

PLA DE TREBALL:

5.-

Wireshark 1.12.13 (v1.12.13-0-g969649d from master-1.12)

Filter: udp.port

No.	Time	Source	Destination	Protocol	Length	Info
13	0.294800000	192.168.88.254	192.168.88.1	DNS	94	Standard query exceed A ssl.gstatic.com.upc.edu
14	0.296530000	192.168.88.1	192.168.88.254	DNS	83	Standard query response 0xceed Server failure
15	0.296716000	192.168.88.254	192.168.88.1	DNS	83	Standard query 0xceed A ssl.gstatic.com.upc.edu
16	0.298178000	192.168.88.1	192.168.88.254	DNS	83	Standard query response 0xceed Server failure
45	3.165911000	192.168.88.254	192.168.88.1	DNS	95	Standard query 0xa451 A detectportal.firefox.com
46	3.167450000	192.168.88.1	192.168.88.254	DNS	84	Standard query response 0xa451 Server failure
47	3.167635000	192.168.88.254	192.168.88.1	DNS	84	Standard query 0xa451 A detectportal.firefox.com
48	3.168970000	192.168.88.1	192.168.88.254	DNS	84	Standard query response 0xa451 Server failure
72	5.297817000	192.168.88.254	192.168.88.1	DNS	100	Standard query 0x398b A ssl.gstatic.com.upcxi.upc.es
73	5.299217000	192.168.88.1	192.168.88.254	DNS	89	Standard query response 0x398b Server failure
74	5.299338000	192.168.88.254	192.168.88.1	DNS	89	Standard query 0x398b A ssl.gstatic.com.upcxi.upc.es
75	5.300630000	192.168.88.1	192.168.88.254	DNS	89	Standard query response 0x398b Server failure
86	6.406804000	192.168.88.254	192.168.88.1	DNS	90	Standard query 0x79ac A accounts.google.com
87	6.406856000	192.168.88.254	192.168.88.1	DNS	90	Standard query 0xe9e3 AAAA accounts.google.com
88	6.406968000	192.168.88.254	192.168.88.1	DNS	90	Standard query 0xb052 Unknown (65) accounts.google.com
89	6.408026000	192.168.88.1	192.168.88.254	DNS	79	Standard query response 0x79ac Server failure
90	6.408063000	192.168.88.254	192.168.88.1	DNS	79	Standard query 0x79ac A accounts.google.com
91	6.409187000	192.168.88.1	192.168.88.254	DNS	79	Standard query response 0xe9e3 Server failure
92	6.409214000	192.168.88.254	192.168.88.1	DNS	79	Standard query 0xe9e3 AAAA accounts.google.com
93	6.410397000	192.168.88.1	192.168.88.254	DNS	79	Standard query response 0xb052 Server failure
94	6.410430000	192.168.88.254	192.168.88.1	DNS	79	Standard query 0xb052 Unknown (65) accounts.google.com
95	6.411512000	192.168.88.1	192.168.88.254	DNS	79	Standard query response 0x79ac Server failure
96	6.411719000	192.168.88.254	192.168.88.1	DNS	90	Standard query 0xca5c A accounts.google.com
97	6.412711000	192.168.88.1	192.168.88.254	DNS	79	Standard query response 0xe9e3 Server failure
98	6.412916000	192.168.88.254	192.168.88.1	DNS	90	Standard query 0xeb1 AAAA accounts.google.com
99	6.413950000	192.168.88.1	192.168.88.254	DNS	79	Standard query response 0xb052 Server failure
100	6.414132000	192.168.88.254	192.168.88.1	DNS	90	Standard query 0x9568 Unknown (65) accounts.google.com
101	6.415167000	192.168.88.1	192.168.88.254	DNS	79	Standard query response 0xca5c Server failure
102	6.415202000	192.168.88.254	192.168.88.1	DNS	79	Standard query 0xca5c A accounts.google.com
103	6.416380000	192.168.88.1	192.168.88.254	DNS	79	Standard query response 0xeb1 Server failure
104	6.416421000	192.168.88.254	192.168.88.1	DNS	79	Standard query 0xeb1 AAAA accounts.google.com
105	6.417598000	192.168.88.1	192.168.88.254	DNS	79	Standard query response 0x9568 Server failure
106	6.417624000	192.168.88.254	192.168.88.1	DNS	79	Standard query 0x9568 Unknown (65) accounts.google.com
107	6.418792000	192.168.88.1	192.168.88.254	DNS	79	Standard query response 0xca5c Server failure
108	6.419235000	192.168.88.254	192.168.88.1	DNS	90	Standard query 0xbdb5 A accounts.google.com

Frame 13: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface 0

Ethernet II, Src: 6c:4b:90:c1:05:be (6c:4b:90:c1:05:be), Dst: Routerbo c2:22:93 (00:0c:42:c2:22:93)

Internet Protocol Version 4, Src: 192.168.88.254 (192.168.88.254), Dst: 192.168.88.1 (192.168.88.1)

User Datagram Protocol, Src Port: 50722 (50722), Dst Port: 53 (53)

Domain Name System (query)

```
0000 00 0c 42 c2 22 93 6c 4b 90 c1 05 be 00 00 45 00  ..B..LK .....E.
0010 00 50 a1 15 40 00 40 11 67 37 c0 a8 50 fe c0 a8  .P..@. g7..X...
0020 50 01 c6 22 00 35 00 3c 32 9e ce ed 01 00 00 01  X..5.<2.....
0030 00 00 00 00 00 01 03 73 73 6c 07 67 73 74 61 74  ....s slgstat
0040 69 63 03 63 6f 6d 03 75 70 63 03 65 64 75 00 00  .ic.com.u pc.edu..
```

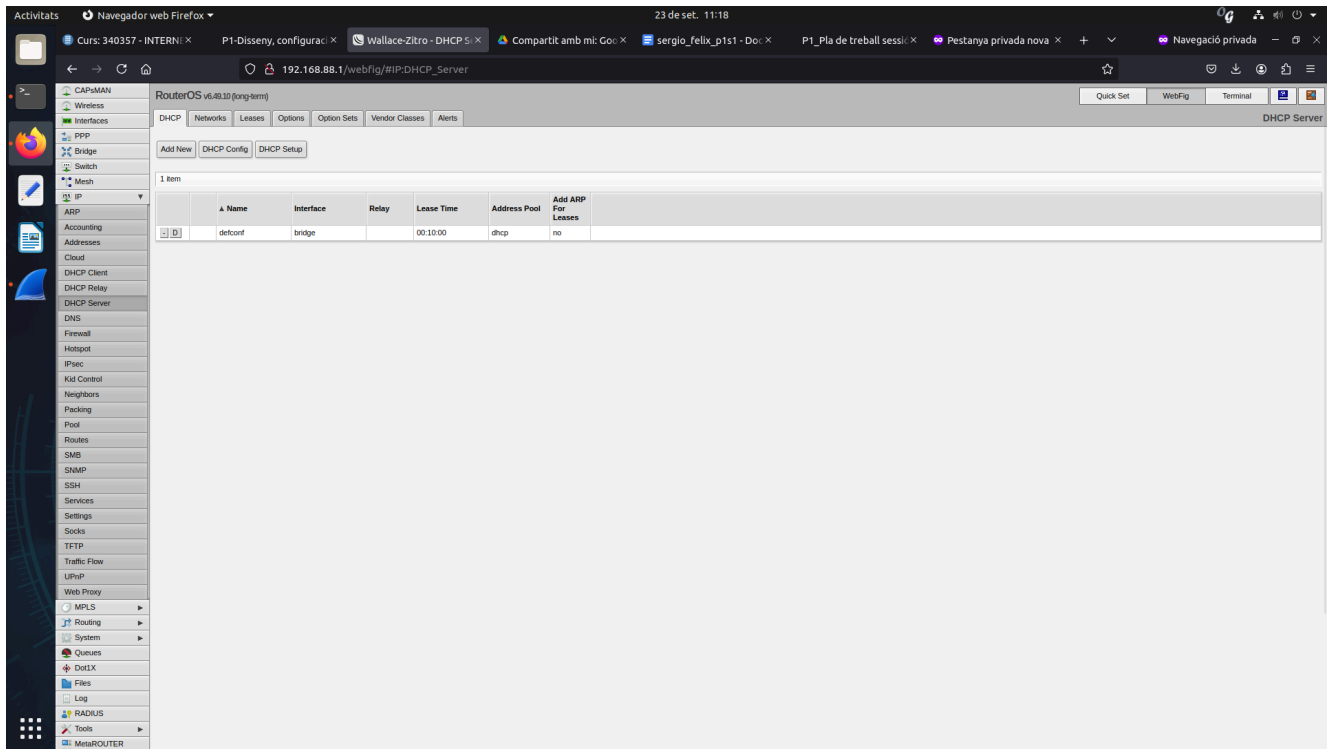
eno1: live capture in progress... Packets: 1702 - Displayed: 671 (39.4%) Profile: Default

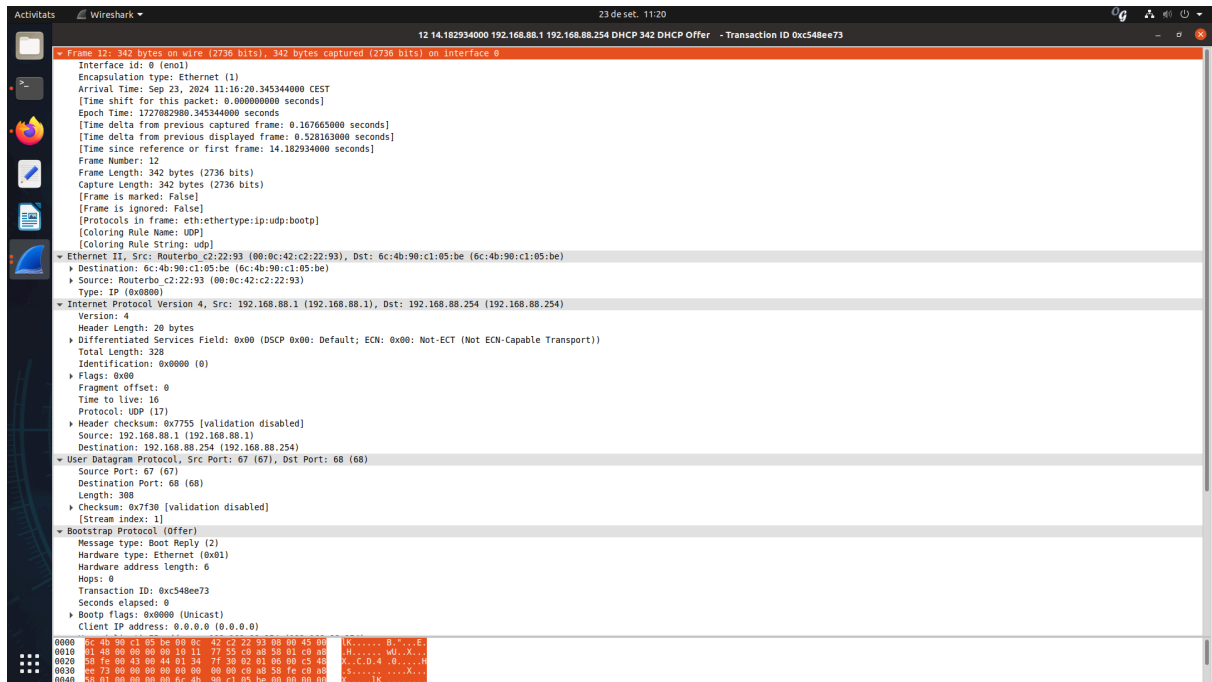
6.-

```
root@AUL-1967:~# sudo dhclient -r
root@AUL-1967:~# sudo dhclient
RTNETLINK answers: File exists
root@AUL-1967:~#
```

7.-

Filter:		udp.port		Expression...	Clear	Apply	Desa
No.	Time	Source	Destination	Protocol	Length	Info	
8	13.654771000	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover	- Transaction ID 0xc548ee73
12	14.182934000	192.168.88.1	192.168.88.254	DHCP	342	DHCP Offer	- Transaction ID 0xc548ee73
13	14.183431000	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request	- Transaction ID 0xc548ee73
14	14.184828000	192.168.88.1	192.168.88.254	DHCP	342	DHCP ACK	- Transaction ID 0xc548ee73





8.-

The screenshot shows the Mikrotik WinBox interface with the DHCP Server Leases page open. The left sidebar contains various configuration menus. The main panel displays a table of active leases.

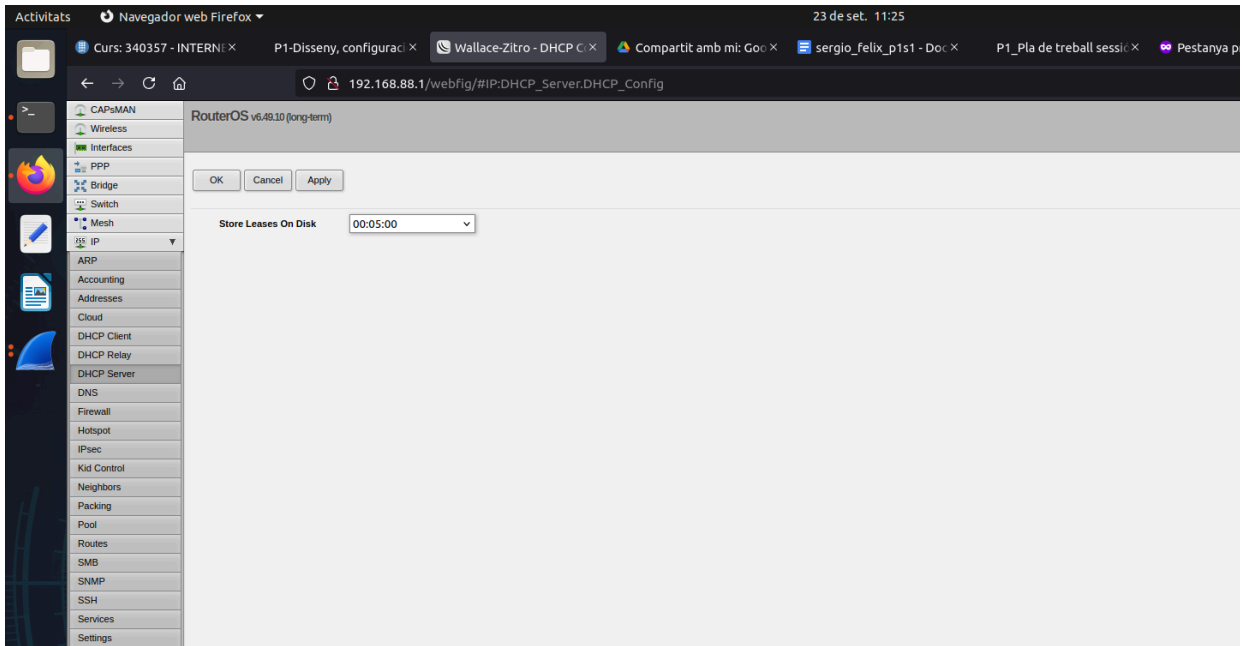
		Address	MAC Address	Client ID	Server	Active Address	Active MAC Address	Active Host Name	Expires After
[D]	D	192.168.88.253	54:E1:AD:37:2D:E6	1-54-e1-ad-37-2d-e6	defconf	192.168.88.253	54:E1:AD:37:2D:E6	DESKTOP-UT	00:06:53
[D]	D	192.168.88.254	6C:4B:90:C1:05:BE		defconf	192.168.88.254	6C:4B:90:C1:05:BE	AUL-1967	00:08:46

9.-

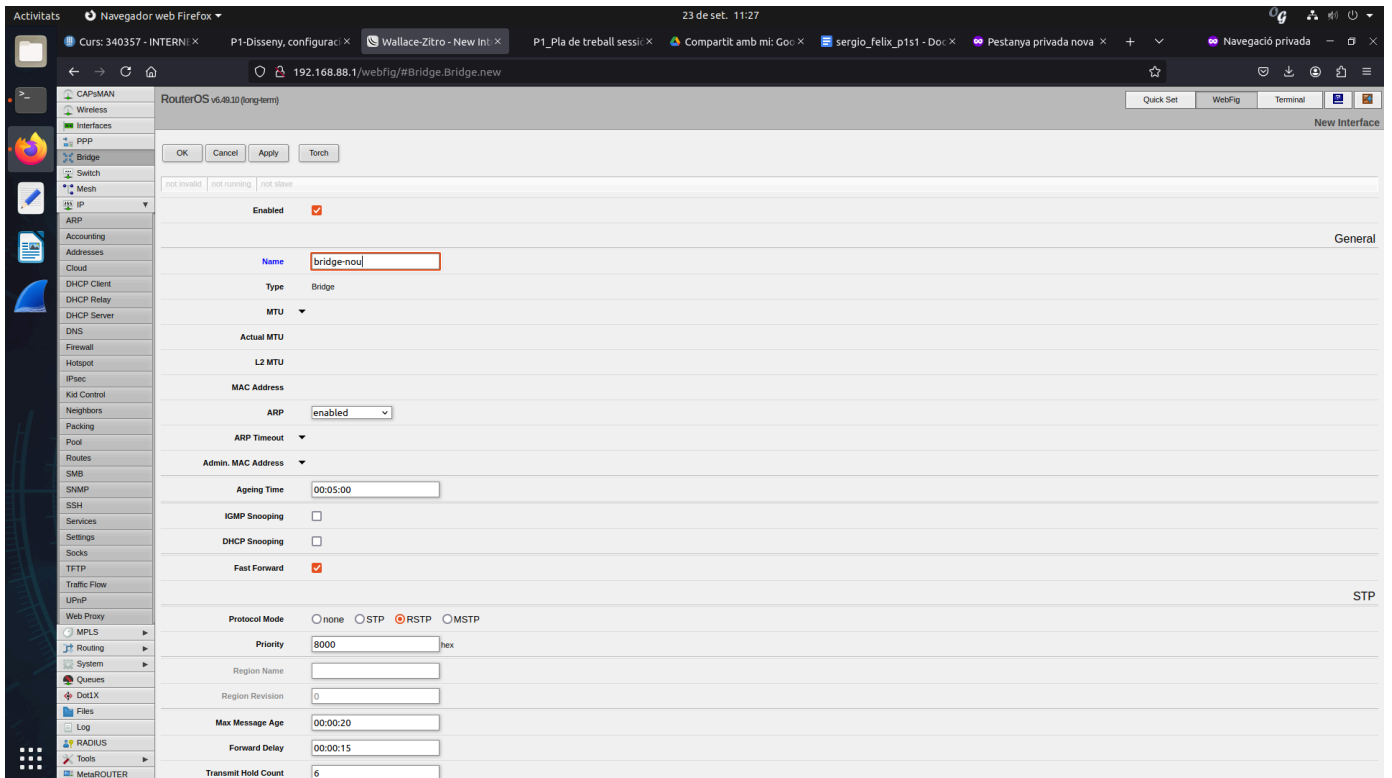
The screenshot shows the Mikrotik WinBox interface with the Interfaces page open. The left sidebar contains various configuration menus. The main panel displays a table of network interfaces.

	Name	Type	Actual MTU	L2 MTU	Tx	Rx	Tx Packet (pps)	Rx Packet (pps)	FP Tx	FP Rx	FP Tx Packet (pps)	FP Rx Packet (pps)
[D]	R	bridge	1500	1598	57.7 kbps	7.8 kbps	6	8	0 bps	7.8 kbps	0	8
[D]	R	ether1	1500	1598	0 bps	0 bps	0	0	0 bps	0 bps	0	0
[D]	RS	ether2	1500	1598	57.9 kbps	8.1 kbps	6	8	57.7 kbps	7.8 kbps	6	8
[D]	RS	ether3	1500	1598	51.2 bps	0 bps	1	0	480 bps	0 bps	1	0
[D]	S	ether4	1500	1598	0 bps	0 bps	0	0	0 bps	0 bps	0	0
[D]	S	ether5	1500	1598	0 bps	0 bps	0	0	0 bps	0 bps	0	0

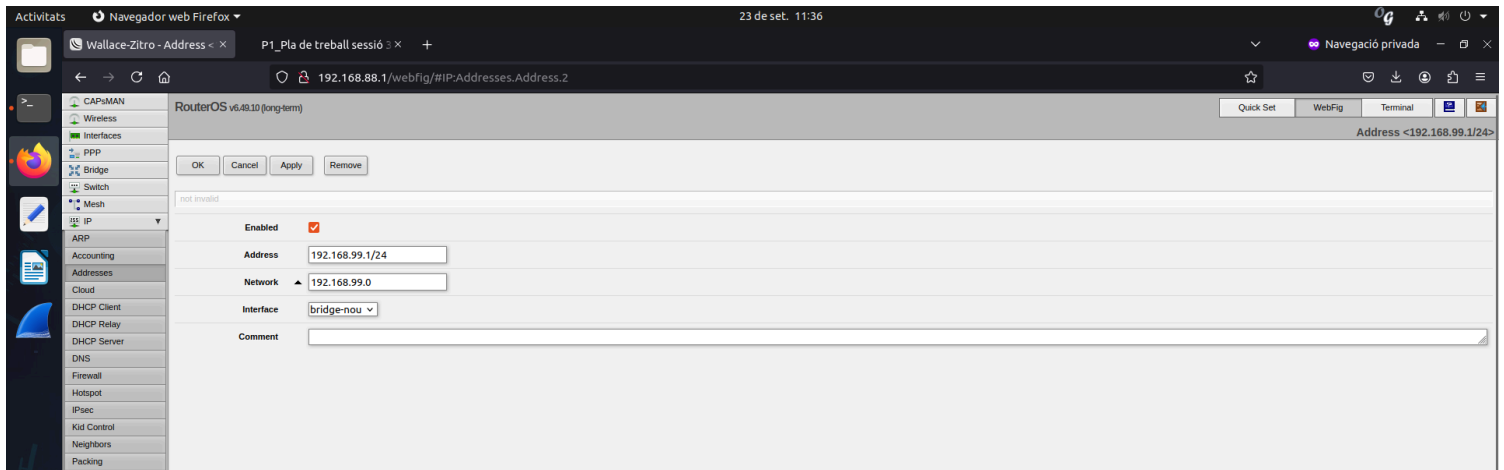
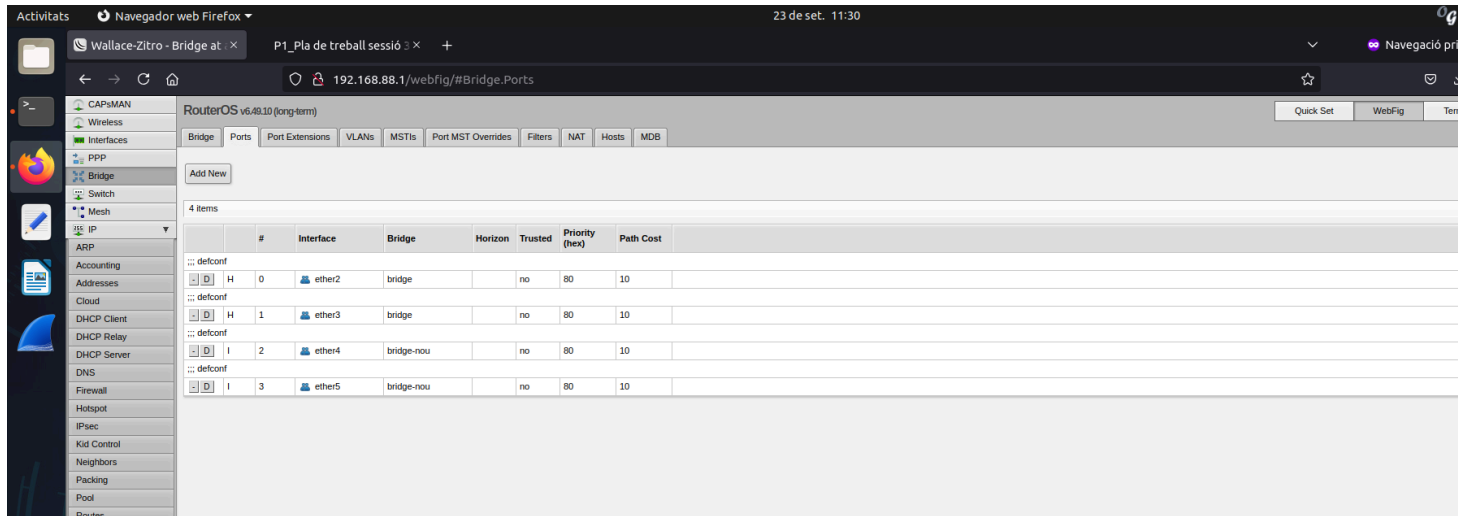
12.-



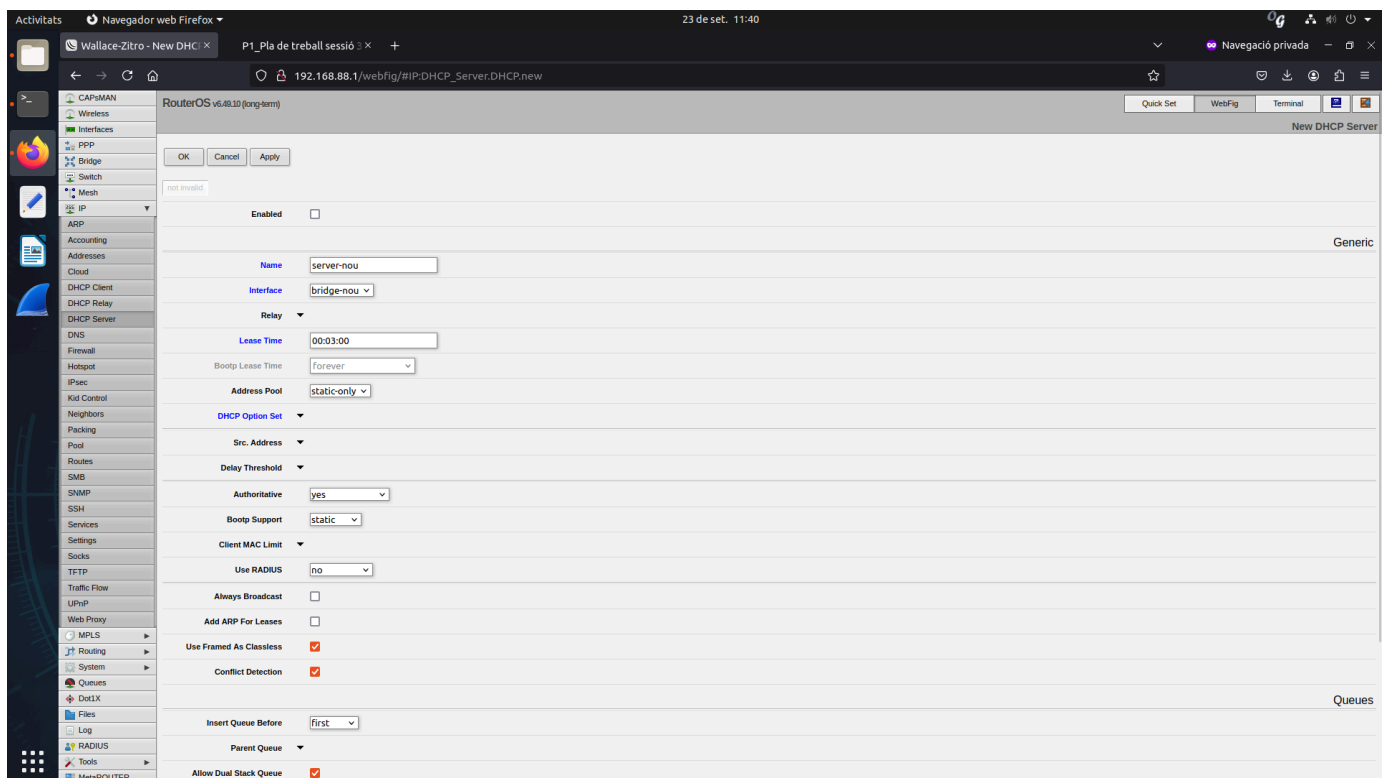
13.-

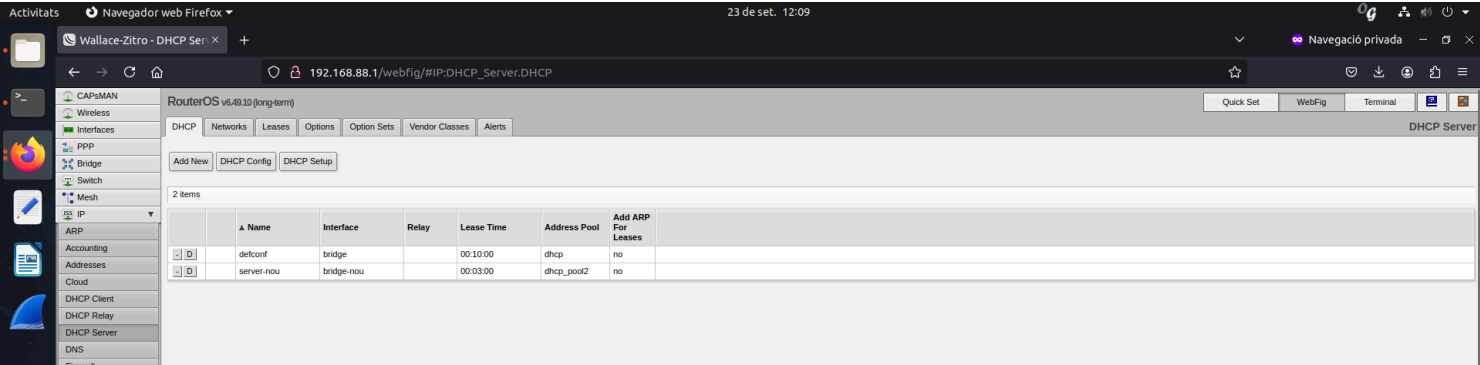
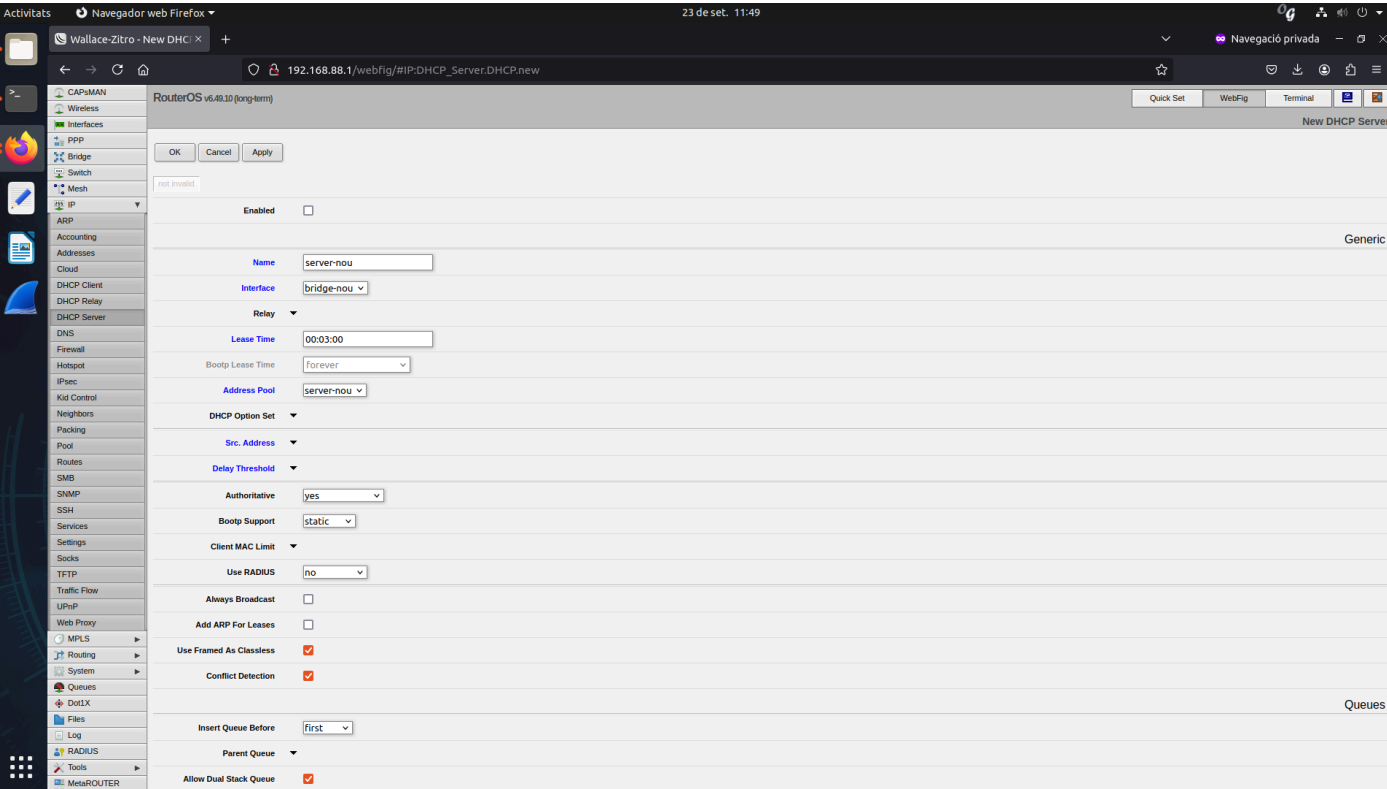
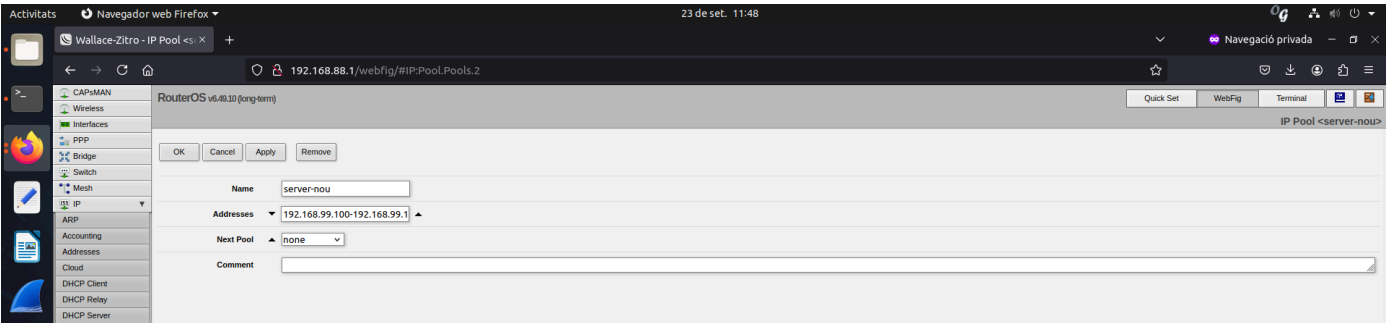


14.-



15.-

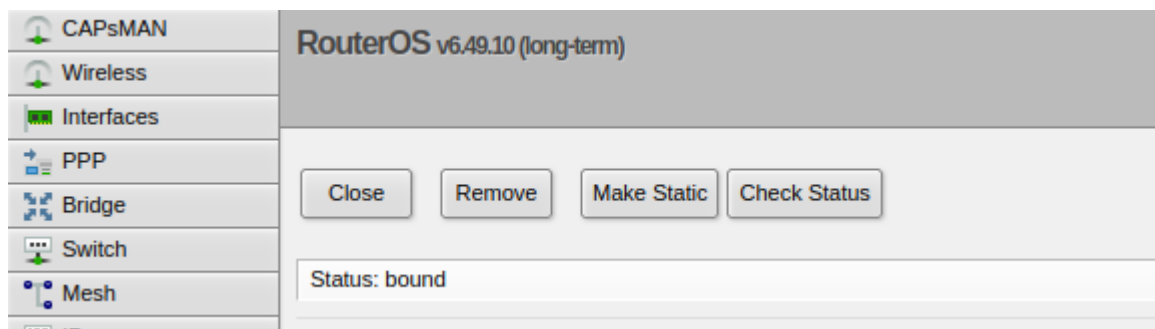




16.-

```
root@AUL-1966:/home/est/f3324858# 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: eno1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 6c:4b:90:c1:68:bc brd ff:ff:ff:ff:ff:ff
    altname enp0s31f6
    inet 192.168.99.110/24 brd 192.168.99.255 scope global dynamic noprefixroute eno1
        valid_lft 168sec preferred_lft 168sec
    inet6 fe80::d6bc:512b:f690:f99b/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
root@AUL-1966:/home/est/f3324858#
```

17.-



Amb "Make Static"

Capturing from eno1 [Wireshark 1.12.13 (v1.12.13-0-g969649d from master-1.12)]

No.	Time	Source	Destination	Protocol	Length	Info
336	48.198966000	192.168.99.110	192.168.99.1	DHCP	328	DHCP Request - Transaction ID 0x79170013
337	48.202196000	192.168.99.1	192.168.99.110	DHCP	342	DHCP ACK - Transaction ID 0x79170013