MANUAL PRÁCTICO

DAVID SEGURA TRISTANCHO
2º ASIR 2022/23

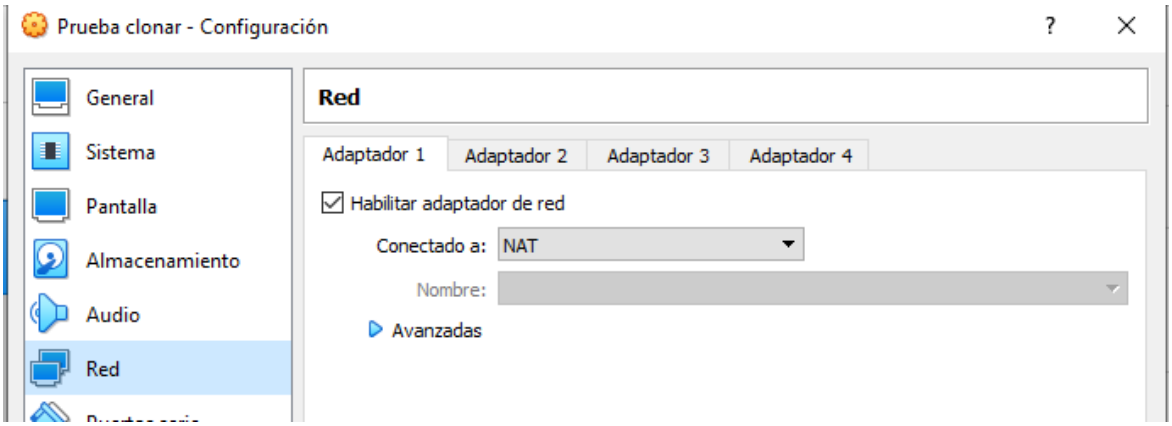
ÍNDICE

1. ¿QUÉ ES DHCP?

El Protocolo de configuración dinámica de host (DHCP) es un protocolo cliente/servidor que proporciona automáticamente un host de Protocolo de Internet (IP) con su dirección IP y otra información de configuración relacionada, como la máscara de subred y la puerta de enlace predeterminada. En este manual vamos a desgranar paso a paso como instalar y configurar un servidor DHCP, y lo haremos acompañándolo de imágenes que nos servirán de soporte ilustrativo. Procedamos pues.

2. INSTALACIÓN

Así que, en primer lugar, nos dirigimos dentro de nuestra máquina virtual a Configuración, accedemos a la red e indicamos que nuestro adaptador de red va a ser de tipo NAT. Una vez hecha esta modificación iniciamos nuestro Ubuntu.



Y dentro de Ubuntu lo primero que se ha de llevar a cabo es actualizar repositorios. Para ello, hacemos uso del comando *sudo apt update*. El siguiente comando en salir al escenario será sudo *apt search dhcp*, que nos servirá para buscar el instalador de dhcp. Ha de aparecernos en una de las líneas y ha de aparecer como isc dhcp server. Una vez dado con él, procedemos a ingresar el siguiente comando para instalar dhcp: *sudo apt install isc-dhcp-server*

3. CONFIGURACIÓN

Antes de nada, es relevante instalar las net tools. Te preguntarás, ¿qué son las net tools? Bien, las net tools son un conjunto de herramientas que se encargan de controlar cada aspecto de la red. Esto incluye arp, ifconfig, netstat, rarp, nameif y route. A nosotros lo que nos interesa en este caso es netstat. Dicho esto, introducimos *sudo apt install net-tools.*

```
usuario@usuario:~$ sudo apt install net-tools
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Se instalarán los siguientes paquetes NUEVOS:
  net-tools
0 actualizados, 1 nuevos se instalarán, 0 para eliminar y 20 no actualizados.
Se necesita descargar 204 kB de archivos.
```

Acto seguido, sudo netstat | more, que nos llevara a la comprobación de los puertos que tenemos. En mi caso, he reducido esa búsqueda mediante una serie de parámetros. Si tecleamos sudo netstat –n –a –p –u –t nos lo mostrará en base a esos parámetros. Por ejemplo, -n, -a y -p significan lo siguiente:

-n: Visualización numérica de direcciones y números de puerto.

-a: Muestra todas las conexiones TCP activas y los puertos TCP y UDP en los que escucha el equipo.

-p: Mostrará las conexiones para el protocolo especificado.

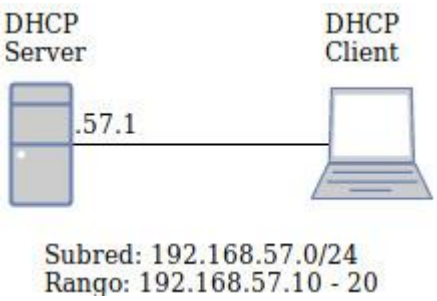
```
usuario@usuario:~$ sudo netstat -n -a -t -u -p
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      657/sshd: /usr/sbin
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      585/systemd-resolve
tcp6       0      0 :::22                   :::*                    LISTEN      657/sshd: /usr/sbin
udp        0      0 127.0.0.53:53           0.0.0.0:*                           585/systemd-resolve
udp        0      0 10.0.2.15:68            0.0.0.0:*                           583/systemd-network
```

Visto el puerto que nos corresponde, es posible que necesitemos cambiar la configuración predeterminada. Para ello, nos dirigimos al archivo /etc/dhcp/dhcpd.conf para adaptarla a sus necesidades y configuración particular. Como recomendación, antes de toquetear nada de lo que posteriormente podamos arrepentirnos, sería aconsejable hacer una copia de seguridad de este archivo. Mediante el comando sudo cp dhcpd.conf dhcpd.confbackup lo he copiado y así me evito tonterías.

4. EJERCICIO 1

Dado el siguiente esquema de red:

- Monta el escenario con máquinas virtuales. Para el DHCP usa un Ubuntu Server 20.04 y para el cliente cualquier sistema operativo.
- Realiza la configuración básica del servidor DHCP, según los datos del esquema y configura el cliente para que tome una dirección dinámica.
- Comprueba cómo afecta la situación de las opciones en el fichero de configuración, según sean opciones de servidor o de ámbito.



Inmersos en el archivo en cuestión (/etc/dhcp/dhcpd.conf), por lo general, lo que se desea hacer es asignar una dirección IP al azar. Esto se puede hacer con la configuración de la siguiente manera:

1º- Primero, borro las líneas que marco en la imagen. En mi caso, las he pegado al final del archivo sin la almohadilla, sin comentario, salvo la de opciones. En la siguiente imagen, queda apreciado al pie de la misma.

```
#shared-network 224-29 {
#  subnet 10.17.224.0 netmask 255.255.255.0 {
#    option routers rtr-224.example.org;
#  }
#  subnet 10.0.29.0 netmask 255.255.255.0 {
#    option routers rtr-29.example.org;
#  }
#  pool {
#    allow members of "foo";
#    range 10.17.224.10 10.17.224.250;
#  }
#  pool {
#    deny members of "foo";
#    range 10.0.29.10 10.0.29.230;
#  }
#}
subnet 192.168.56.0 netmask 255.255.255.0 {
  range 192.168.56.100 192.168.56.200;
#  option routers rtr-239-0-1.example.org, rtr-239-0-2.example.org;
}
```

2º- Después, salimos del archivo guardando lo editado para irnos con sudo nano /etc/netplan/config.yaml a este mencionado archivo, donde modifico la ip según la manera deseada. De nuevo, una imagen vale más que mil palabras.

```
  GNU nano 6.2                          /etc/netplan/config.yaml *
network:
  version: 2
  renderer: networkd
  ethernets:
    enp0s3:
      addresses:
        - 192.168.56.2/24
```

Para aplicar cambios, sudo netplan apply, seguido de sudo service isc-dhcp-server restart para reiniciar y sudo service isc-dhcp-status para comprobar que todo marcha según lo previsto.

```
usuario@usuario:~$ sudo netplan apply
usuario@usuario:~$ sudo service isc-dhcp-server restart
usuario@usuario:~$ sudo service isc-dhcp-server status
• 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 Tue 2022-09-27 08:24:24 UTC; 6s ago
       Docs: man:dhcpd(8)
   Main PID: 1038 (dhcpd)
      Tasks: 4 (limit: 1030)
     Memory: 4.9M
        CPU: 12ms
     CGroup: /system.slice/isc-dhcp-server.service
             └─1038 dhcpd -user dhcpd -group dhcpd -f -4 -pf /run/dhcp-server/dhcpd.pid -cf /etc/dh>
```

3º - Hemos configurado la máquina del servidor, pero hemos de hacer lo mismo con el cliente. Así que procedemos a asignarle la ip adecuada, y como ya sabéis ha de efectuarse en el archivo config.yaml que se encuentra dentro de /etc/netplan.

```
  GNU nano 6.2                          /etc/netplan/config.yaml
network:
  version: 2
  renderer: networkd
  ethernets:
    enp0s3:
      addresses:
        - 192.168.56.3/24
```

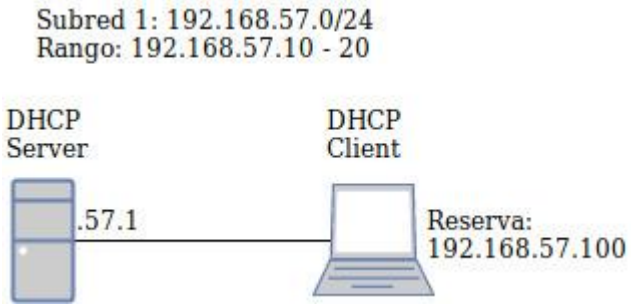
Procedemos a ajustar los cambios con *sudo netplan apply* y *sudo service icp-dhcp-restart*. ¿Y ahora que queda por hacer para establecer la conexión entre servidor y cliente? Es sencillo, solo habremos de dirigirnos al servidor y lanzar un ping a la ip del cliente. En mi caso, aparece en pantalla lo siguiente.

```
--- 192.168.56.2 ping statistics ---
45 packets transmitted, 45 received, 0% packet loss, time 44152ms
rtt min/avg/max/mdev = 0.277/0.702/1.172/0.173 ms
usuario@usuario:~$
```

Esto significa que la conexión se ha efectuado y, por lo tanto, hay comunicación entre servidor y cliente. Para asegurarnos, podemos insertar el siguiente comando *sudo nano /var/lib/dhcp/dhcpd.leases*. Es en este archivo donde podremos verificarlo y, a la misma vez, ver el tiempo de asignación dado al cliente recién creado.

5. EJERCICIO 2

Añade una reserva de dirección a la máquina cliente de la práctica anterior según el siguiente esquema:



Vamos a dar un giro a lo confeccionado, y vamos a asignar una ip diferente al cliente, una ip reservada. ¿Cómo se produce? Para ello, hemos de acceder a un archivo que ya hemos visto anteriormente, /etc/dhcp/dhcpd.conf. Es en él donde podremos configurar los lease time a nivel de servidor, ámbito u host. No solo eso, vamos a crear una segunda subred para otro cliente. Para ello, hago uso del archivo que he mencionado y al final del mismo los edito añadiendo a cada subred un rango de direcciones que podré utilizar para asignar reservas.

```
  GNU nano 6.2                                  /etc/dhcp/dhcpd.conf *
# other clients get addresses on the 10.0.29/24 subnet.

#class "foo" {
#  match if substring (option vendor-class-identifier, 0, 4) = "SUNW"
#}

#shared-network 224-29 {
#  subnet 10.17.224.0 netmask 255.255.255.0 {
#    option routers rtr-224.example.org;
#  }
#  subnet 10.0.29.0 netmask 255.255.255.0 {
#    option routers rtr-29.example.org;
#  }
#  pool {
#    allow members of "foo";
#    range 10.17.224.10 10.17.224.250;
#  }
#  pool {
#    deny members of "foo";
#    range 10.0.29.10 10.0.29.230;
#  }
subnet 192.168.56.0 netmask 255.255.255.0 {
        default-lease-time 3600;
         range 192.168.56.100 192.168.56.200;
#  option routers rtr-239-0-1.example.org, rtr-239-0-2.example.org;
}
subnet 192.168.57.0 netmask 255.255.255.0 {
        default-lease-time 3600;
         range 192.168.57.100 192.168.57.200;
#  option routers rtr-239-0-1.example.org, rtr-239-0-2.example.org;
}
```

Subred 1

Subred 2

Como puede apreciarse, el lease time es de 3600 segundos, lo cual equivale a una hora de préstamo de la ip por parte del servidor, préstamo que suele renovarse antes de que ese tiempo expire. Y es que el lease time se define como el período de tiempo durante el cual un servidor DHCP asigna una dirección IP a un cliente. Se define en segundos por defecto (default), pero también existe el max time. El parámetro max-lease-time se utiliza para indicar el máximo tiempo de concesión de una IP, si un cliente solicitara una concesión por encima de este tiempo, se le asignaría el máximo. Su sintaxis es la siguiente: ***max-lease-time segundos.***

Volviendo a lo que estábamos, dentro de este archivo (dhcpd.conf), añadimos la ip dinámica de los clientes, una de ellas perteneciente a la subred 1 y otra a la subred 2. El siguiente paso después de aplicar los cambios

en el servidor con *sudo service isc-dhcp-server restart* es dirigirse al primer cliente y añadir lo siguiente dentro del archivo netplan/config.yaml.

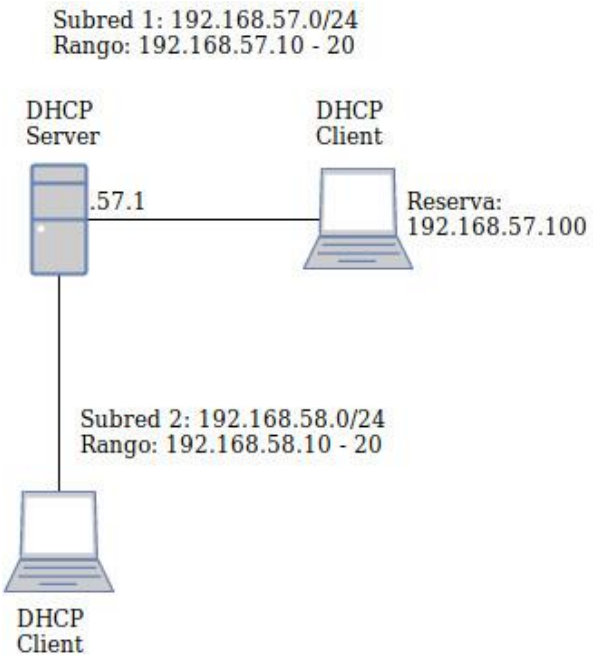
Activamos el dhcp.

```
 GNU nano 6.2                          /etc/netplan/config.yaml
network:
  version: 2
  renderer: networkd
  ethernets:
    enp0s3:
     dhcp4: true
```

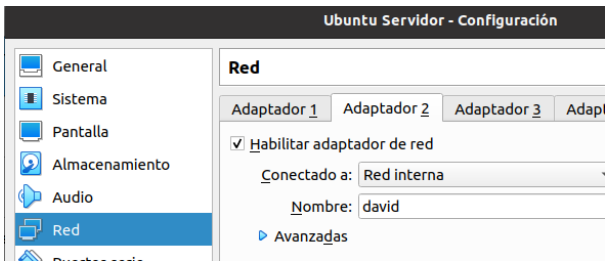
Automáticamente, la ip le ha sido reservada dentro del rango establecido anteriormente. Con el comando *ip a* podremos comprobarlo.

6. EJERCICIO 3

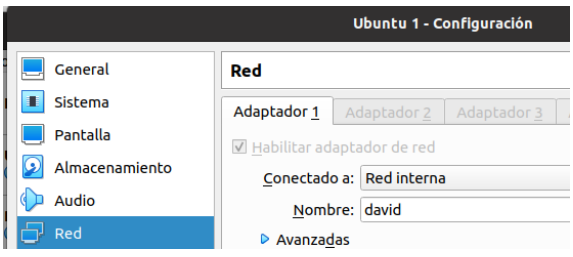
Modifica el esquema anterior para adaptarlo a lo siguiente:



En cuanto al segundo cliente, que tiene que ver con la segunda subred, lo que hemos de hacer es crear en el servidor un segundo adaptador de red interna y nombrarlo de la misma forma que será nombrado el adaptador de red interna del segundo cliente. Aquí queda ilustrado de manera más esclarecedora:



Adaptador de red del servidor



Adaptador de red del cliente 2

Ambos quedarán conectados bajo la misma red, que yo he nombrado david (no me he complicado mucho la vida). Ahora nos encaminamos al archivo /etc/netplan/config.yaml y modificamos la configuración. Por

ejemplo, la interfaz es la enp0s8, la cual se asocia con la segunda subred. Una vez modificado el archivo, y aplicado los cambios con netplan apply, con el comando *ip a* puedo asegurarme si la ip ha sido asignada.

Después lanzamos un ping desde el servidor tanto al cliente 1 como al cliente 2 y verificaremos que la conexión ha quedado establecida correctamente.

```
usuario@usuario:~$ ping 192.168.56.150
PING 192.168.56.150 (192.168.56.150) 56(84) bytes of data.
64 bytes from 192.168.56.150: icmp_seq=1 ttl=64 time=0.625 ms
64 bytes from 192.168.56.150: icmp_seq=2 ttl=64 time=0.566 ms
64 bytes from 192.168.56.150: icmp_seq=3 ttl=64 time=0.684 ms
64 bytes from 192.168.56.150: icmp_seq=4 ttl=64 time=0.595 ms
^C
--- 192.168.56.150 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3066ms
rtt min/avg/max/mdev = 0.566/0.617/0.684/0.043 ms
usuario@usuario:~$ ping 192.168.57.100
PING 192.168.57.100 (192.168.57.100) 56(84) bytes of data.
64 bytes from 192.168.57.100: icmp_seq=1 ttl=64 time=0.482 ms
64 bytes from 192.168.57.100: icmp_seq=2 ttl=64 time=1.04 ms
64 bytes from 192.168.57.100: icmp_seq=3 ttl=64 time=1.11 ms
64 bytes from 192.168.57.100: icmp_seq=4 ttl=64 time=1.11 ms
64 bytes from 192.168.57.100: icmp_seq=5 ttl=64 time=0.422 ms
^C
--- 192.168.57.100 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 0.422/0.831/1.114/0.311 ms
usuario@usuario:~$ _
```

La imagen muestra cómo los paquetes son enviados desde el servidor a cada cliente, alojados en distintas subredes, y como estos, a su vez, los reciben.

7. CONSEJOS ÚTILES

Si hemos llegado a este punto es señal de que todo ha marchado según lo previsto. No obstante, no viene mal recordar ciertos aspectos que son fundamentales y que puede que alguna que otra vez se nos olvide hacer.

1º- Después de cada acción efectuada, de cambiar cualquier aspecto de la configuración de dhcp y aplicar, hemos de comprobar que el proceso está corriendo. Recordad el uso del sudo service isc-dhcp-server status y del restart.

2º- Comprobar que se está ejecutando activamente, sin errores.

```
usuario@usuario:~$ sudo service isc-dhcp-server status
● 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 Thu 2022-09-29 08:24:10 UTC; 1h 34min ago
       Docs: man:dhcpd(8)
   Main PID: 605 (dhcpd)
      Tasks: 4 (limit: 1030)
     Memory: 6.2M
        CPU: 90ms
     CGroup: /system.slice/isc-dhcp-server.service
             └─605 dhcpd -user dhcpd -group dhcpd -f -4 -pf /run/dhcp-server/dhcpd.pid -cf /etc/dhc>

sep 29 09:54:23 usuario dhcpd[605]: ns1.example.org: temporary name server failure
sep 29 09:54:23 usuario dhcpd[605]: ns2.example.org: temporary name server failure
sep 29 09:54:23 usuario dhcpd[605]: DHCPACK on 192.168.57.100 to 08:00:27:5a:9e:0a (usuario) via en>
sep 29 09:55:01 usuario dhcpd[605]: Dynamic and static leases present for 192.168.56.150.
sep 29 09:55:01 usuario dhcpd[605]: Remove host declaration passacaglia or remove 192.168.56.150
sep 29 09:55:01 usuario dhcpd[605]: from the dynamic address pool for 192.168.56.0/24
sep 29 09:55:01 usuario dhcpd[605]: DHCPREQUEST for 192.168.56.150 from 08:00:27:5a:9e:0a via enp0s3
sep 29 09:55:01 usuario dhcpd[605]: DHCPACK on 192.168.56.150 to 08:00:27:5a:9e:0a via enp0s3
sep 29 09:57:05 usuario dhcpd[605]: DHCPREQUEST for 192.168.56.102 from 08:00:27:5a:9e:0a via enp0s>
sep 29 09:57:05 usuario dhcpd[605]: DHCPNAK on 192.168.56.102 to 08:00:27:5a:9e:0a via enp0s3
lines 1-21/21 (END)
```

3º- Asegurarnos de que los puertos están a la escucha, abiertos. Para ello, hacemos uso del sudo netstat –natup.

```
usuario@usuario:~$ sudo netstat -natup
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      586/systemd-resolve
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      676/sshd: /usr/sbin
tcp6       0      0 :::22                   :::*                    LISTEN      676/sshd: /usr/sbin
udp        0      0 127.0.0.53:53           0.0.0.0:*                           586/systemd-resolve
udp        0      0 0.0.0.0:67              0.0.0.0:*                           605/dhcpd
udp        0      0 192.168.56.102:68       0.0.0.0:*                           584/systemd-network
```

Si estos tres pasos son efectuados y todo marcha adecuadamente, no debería haber problemas como tales y nuestros equipos deberían trabajar sin ninguna anomalía.

Por cierto, si queremos ver los últimos procesos que se han ido realizando en el equipo, esto puede hacerse accediendo al fichero /var/log/syslog

```
usuario@usuario:~$ cd /var/log
usuario@usuario:/var/log$ ls
alternatives.log  auth.log              dmesg       faillog     private
apport.log        auth.log.1            dmesg.0     installer   syslog
apport.log.1      bootstrap.log         dmesg.1.gz  journal     syslog.1
apport.log.2.gz   btmp                  dmesg.2.gz  kern.log    ubuntu-advantage.log
apport.log.3.gz   cloud-init.log        dmesg.3.gz  kern.log.1  ubuntu-advantage-timer.log
apport.log.4.gz   cloud-init-output.log dmesg.4.gz  landscape   unattended-upgrades
apt               dist-upgrade          dpkg.log    lastlog     wtmp
usuario@usuario:/var/log$ tail syslog
Sep 29 11:40:05 usuario dhcpd[605]: Dynamic and static leases present for 192.168.56.150.
Sep 29 11:40:05 usuario dhcpd[605]: Remove host declaration passacaglia or remove 192.168.56.150
Sep 29 11:40:05 usuario dhcpd[605]: from the dynamic address pool for 192.168.56.0/24
Sep 29 11:40:05 usuario dhcpd[605]: DHCPREQUEST for 192.168.56.150 from 08:00:27:5a:9e:0a via enp0s3
Sep 29 11:40:05 usuario dhcpd[605]: ns1.example.org: temporary name server failure
Sep 29 11:40:05 usuario dhcpd[605]: ns2.example.org: temporary name server failure
Sep 29 11:40:05 usuario dhcpd[605]: DHCPACK on 192.168.56.150 to 08:00:27:5a:9e:0a via enp0s3
Sep 29 11:42:06 usuario dhcpd[605]: DHCPREQUEST for 192.168.56.102 from 08:00:27:5a:9e:0a via enp0s3
: lease 192.168.56.102 unavailable.
Sep 29 11:42:06 usuario dhcpd[605]: DHCPNAK on 192.168.56.102 to 08:00:27:5a:9e:0a via enp0s3
Sep 29 11:42:06 usuario systemd-timesyncd[422]: Network configuration changed, trying to establish c
onnection.
usuario@usuario:/var/log$
```

También podemos cambiar el dominio de nuestras subredes. Para ello accedemos al archivo ya conocido etc/dhcp/dhcpd.conf y copiamos la línea optain domain-name y option routers en la subred deseada, al final del propio archivo.

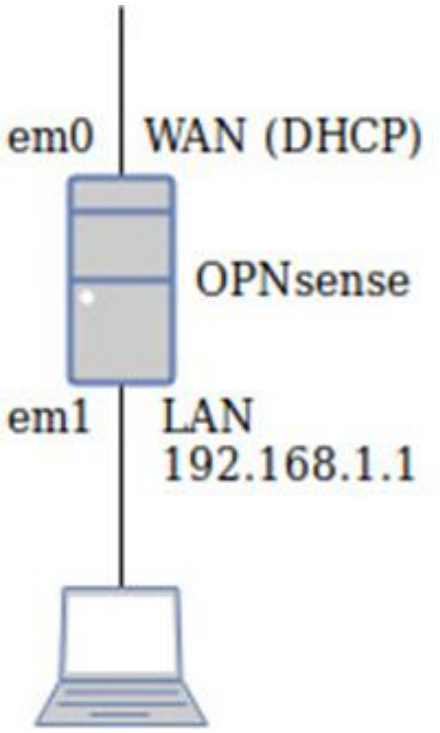
```
# option definitions common to all supported networks...
option domain-name "iespoligonosur.org";
option domain-name-servers 192.168.128.1;
default-lease-time 86400;
max-lease-time 7200;
```

Una vez dado este paso, modificamos el nombre del dominio según convenga.

```
subnet 192.168.56.0 netmask 255.255.255.0 {
        default-lease-time 3600;
         range 192.168.56.100 192.168.56.200;
        option domain-name "aula56.iespoligonosur.org";
        option routers 192.168.56.1;
#  option routers rtr-239-0-1.example.org, rtr-239-0-2.example.org;
}
```

8. EJERCICIO 4

Dado el siguiente esquema de red:



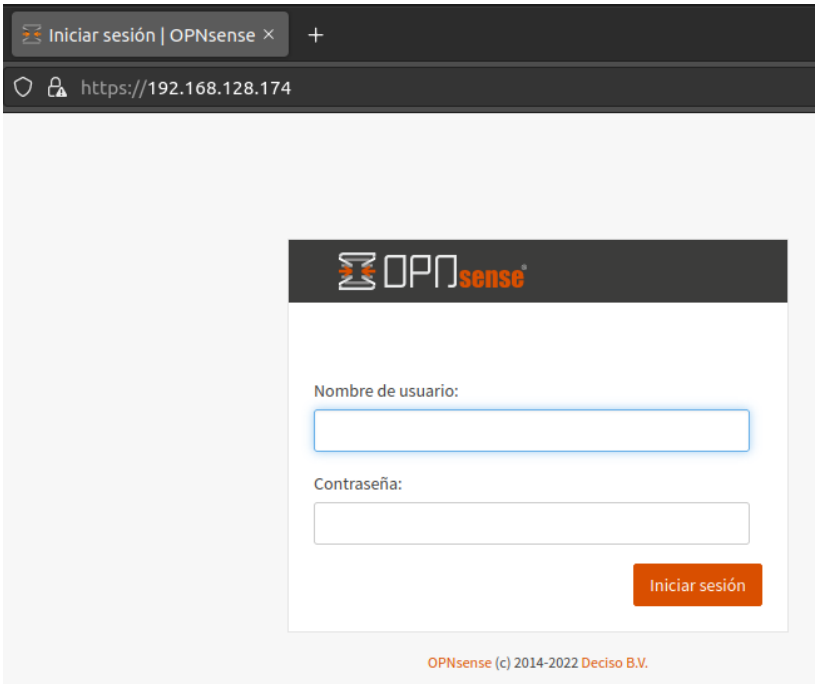
- Realiza la instalación de un OPNsense en una máquina virtual con dos adaptadores, configurados en Adaptador puente (WAN) y Red Interna (LAN). NOTAS:
  - Debes asignar los adaptadores de red a las distintas interfaces (em0 - WAN y em1 - LAN)
  - Para instalar hay que iniciar sesión con el usuario installer y contraseña opnsense.
- Conecta una máquina cliente a la LAN y comprueba que tiene conexión al OPNsense.
- Configura el servidor DHCP para que el cliente obtenga una configuración de red válida.
- Crea una reserva para el cliente.
- Añade un nuevo interfaz a OPNsense y conecta otro cliente, siguiendo un esquema similar al del ejercicio 3. configura el servicio DHCP en ese interfaz y comprueba que el cliente obtiene una configuración de red.

Comencemos por lo elemental. ¿Qué es OpenSense? Pues bien, OpenSense es una distribución personalizada de FreeBSD adaptado para su uso como Firewall y Enrutador. Se caracteriza por ser de código abierto, puede ser instalado en una gran variedad de ordenadores, y además cuenta con una interfaz web sencilla para su configuración.

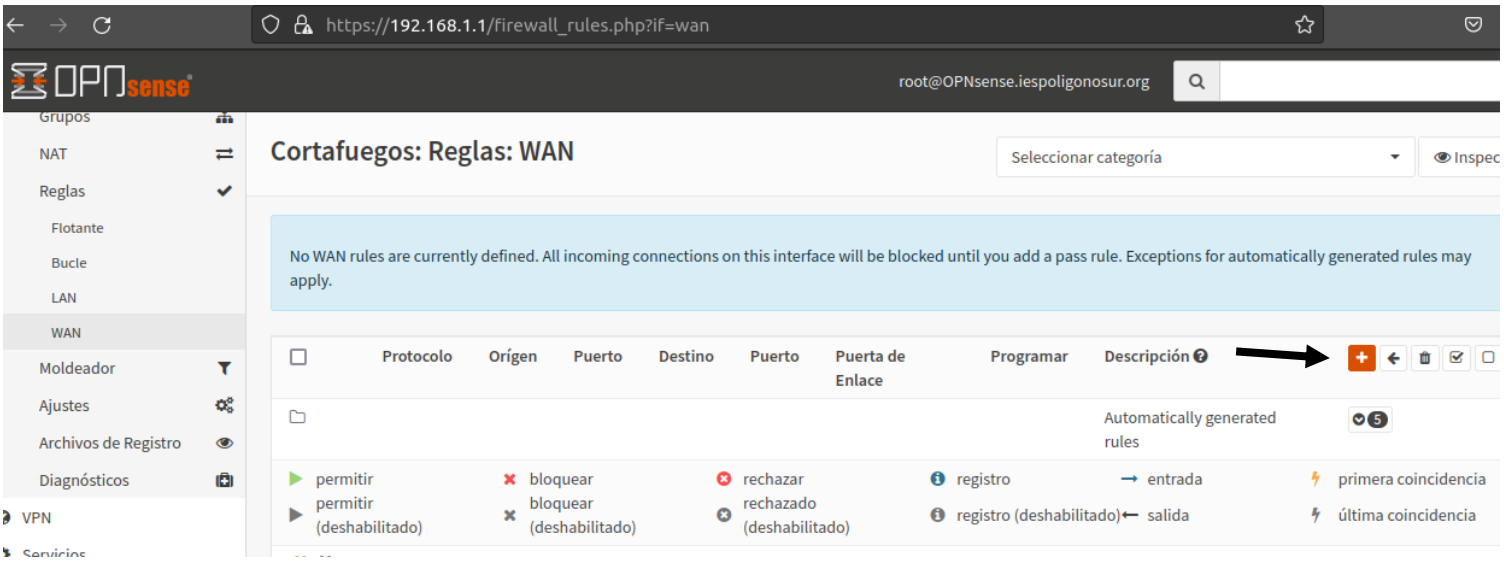
En este apartado, vamos a acceder a su interior para ver cómo funciona tanto a nivel de consola como de entorno gráfico. Y lo vamos a hacer creando una red que va a contar con tres adaptadores, el primero de ellos un adaptador puente y los dos restantes de red interna, llamados lan y dmz. Si inicio la maquina servidora, la de opensense, me aparece lo siguiente:

```
*** OPNsense.localdomain: OPNsense 22.7 (amd64/OpenSSL) ***

LAN (em1)       -> v4: 192.168.1.1/24
WAN (em0)       -> v4/DHCP4: 192.168.128.174/24

HTTPS: SHA256 C8 EC B4 17 11 8A C2 B1 0C BB 94 34 3C 7A BB 54
               52 35 76 85 BA 45 D4 43 EA FB 09 24 7A CE F7 94
```

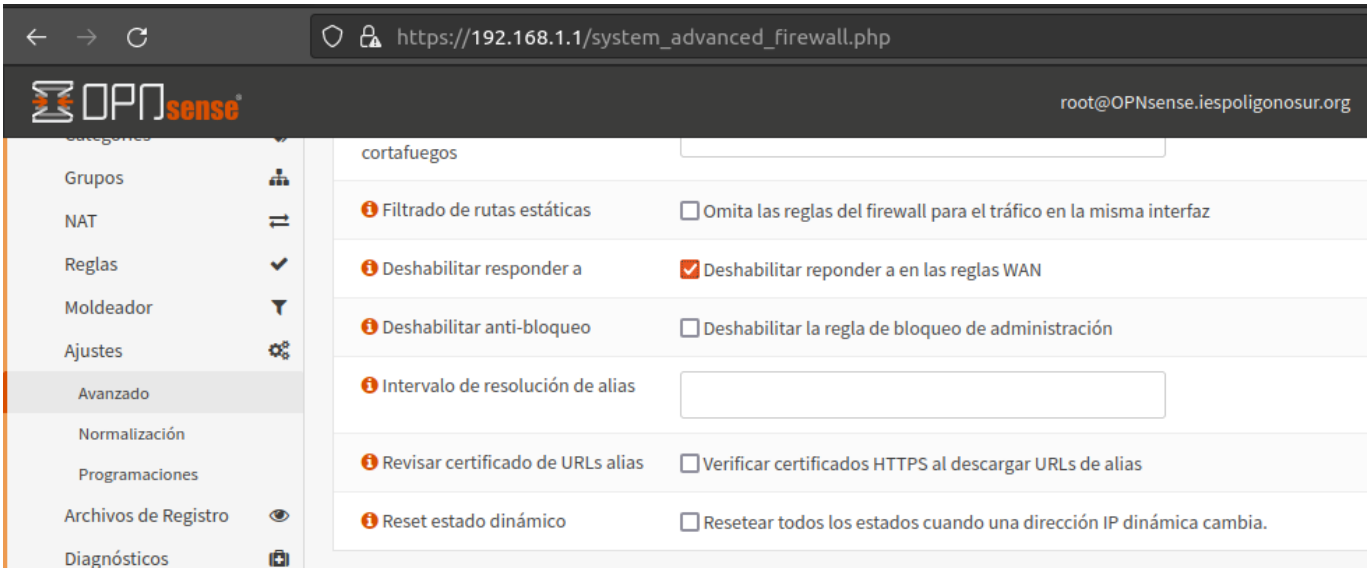
En la imagen adjuntada, puede verse como ya tenemos adjudicada la ip de la red lan y de la red wan junto a sus respectivas interfaces. Si yo ahora me dirijo hacia mi otra máquina, en este caso un Ubuntu Desktop, e inserto en el navegador la ip precedida de https:// nos aparecerá la interfaz gráfica de OpenSense.



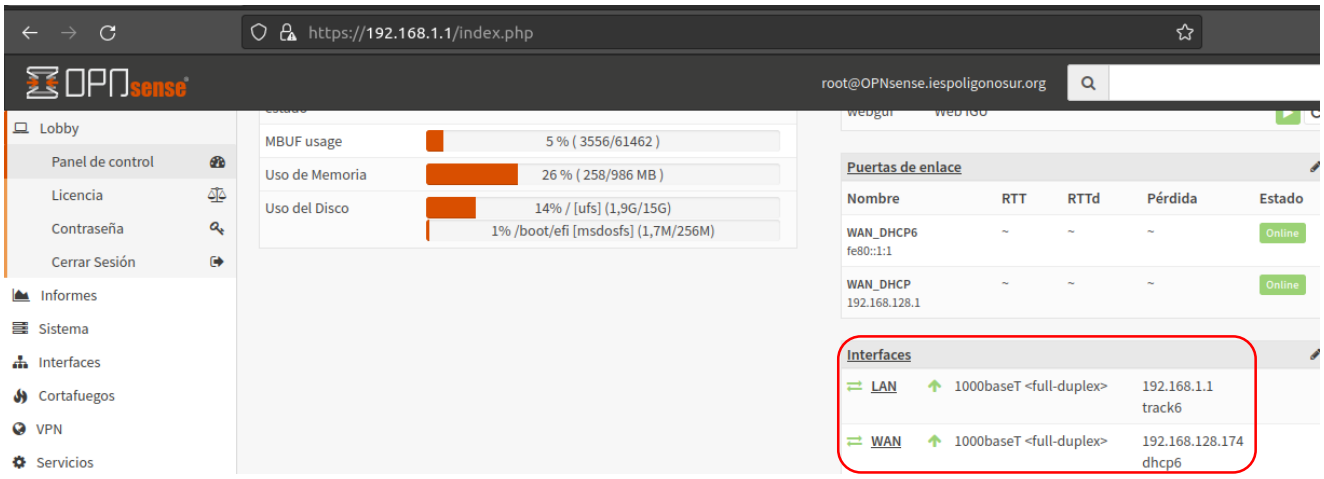
A partir de ahora, y como vais a presenciar, todo va a resultar más sencillo gracias a las utilidades de este software. Así que vamos a ir configurando diferentes parámetros dentro de su asistente para preparar nuestras redes. Al principio, vamos ir a interfaces, dentro del listado de opciones que aparece a la izquierda, y accedemos a Wan, a su asistente, para habilitar la red e insertar el dominio en cuestión, en nuestro caso iespoligonosur.org, así como desbloquear redes privadas y falsas. De ahí pasamos a Firewall, Reglas, Wan.



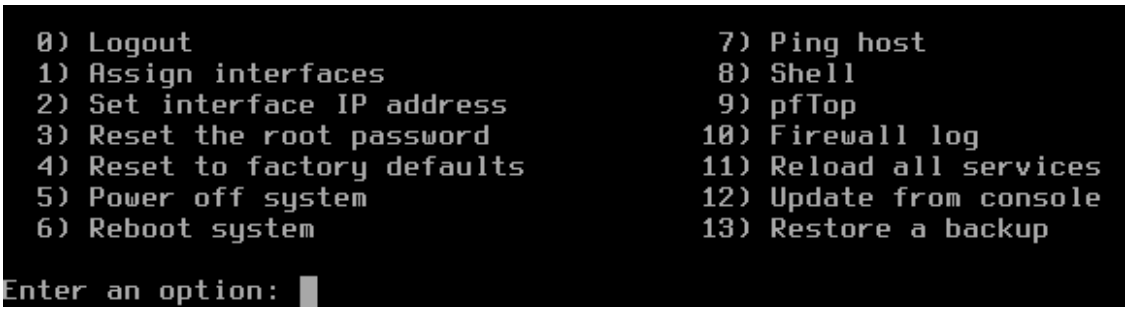
En la cruz de la derecha, puedo asignar las reglas por las cuales se va a regir mi red Wan. Todo aquello que vaya a tocarse ha de añadirse y guardarse. En nuestro caso, no vamos a cambiar nada más allá de irnos a Ajustes, avanzado, donde vamos a deshabilitar responder a en las reglas WAN.



Si echamos un vistazo al panel de control de OpenSense, podremos verificar nuestras interfaces.



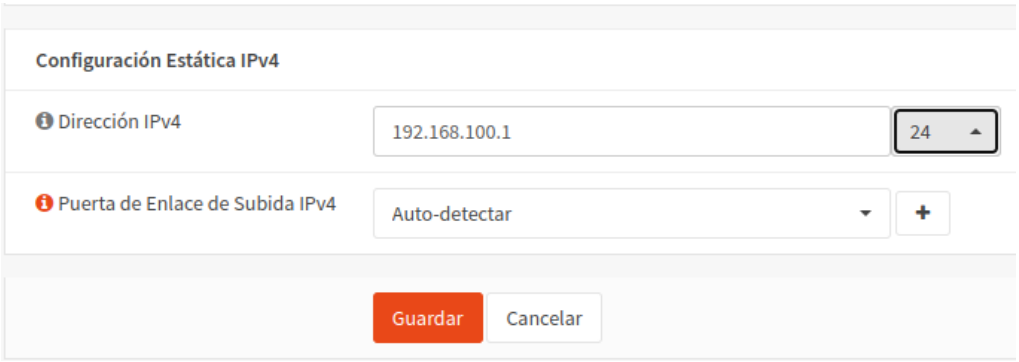
No obstante, me falta por asignar la interfaz de la red interna con el nombre de dmz. Puedo hacerlo de dos maneras. La primera de ellas vía consola, donde no es demasiado difícil.



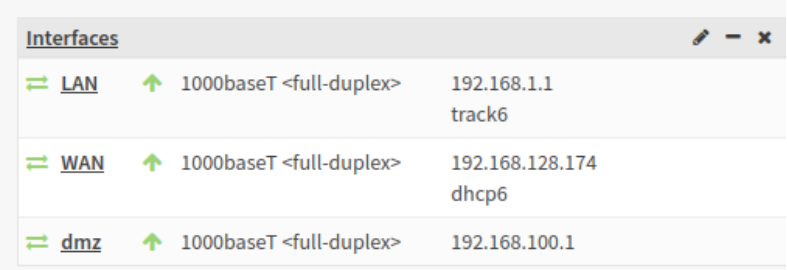
Dentro de esas numeraciones, el 1 y el 2 nos servirán para asignar dicha interfaz, pero aquí estamos hablando de OpenSense y si por algo destaca este software es por su magnífica interfaz gráfica. Dicho esto, vamos de nuevo a su asistente, concretamente a Interfaces, Asignaciones.

Si os fijáis detenidamente, me aparece la interfaz de LAN, de WAN y una tercera, la del centro, llamada OPT1. Si me voy a ella, puedo editarla y darle el nombre convenido. Yo voy a nombrarla dmz.

Incluso voy a configurar su ip, después guardo y los cambios serán efectuados.



Si me voy de nuevo al Panel de control, me aseguro de que la interfaz dmz ya está operativa.



Hasta ahora, estamos viendo las múltiples posibilidades que OpenSense ofrece, y antes de acabar este apartado vamos a conocer algo sobre los arrendamientos, es decir, voy a crear una ip que va a ser reservada para un cliente.

Para ello, solo he de ir a Servicios, DHCPv4, Arrendamientos. Dentro de Arrendamientos, voy a acceder a Lan, y ahí es donde asigno la reserva.

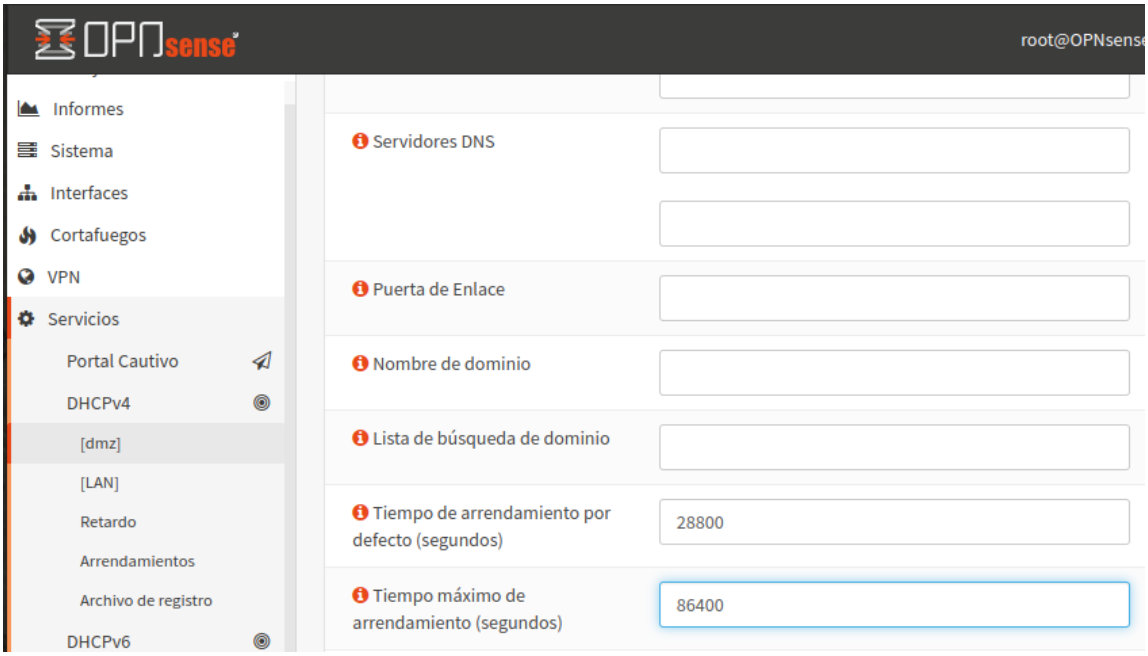
La ip reservada, por cierto, será estática.

Una vez dada la ip y configurado los parámetros deseados, hacemos clic en guardar y los cambios se habrán efectuados. Si observamos en Arrendamientos, nuestra ip reservada ya nos aparece.

¿Y si yo quisiera añadir una reserva para una ip de la red interna dmz, aplicándole un rango y añadiéndole un tiempo de préstamo por defecto de 8 horas y máximo de 1 día?

En mi caso, yo he probado por cambiar el adaptador de mi cliente Ubuntu Desktop, pasando del adaptador de red interna lan a dmz. Esto me ha dado problemas de incompatibilidad en Arrendamientos, algo que he

solucionado eliminando la reserva hecha anteriormente a la red lan. A posteriori, he accedido a Servicios, dentro de OpenSense, y he configurado el rango, entre la 192.168.1.100 y la 200, y he asignado los tiempos de préstamo.

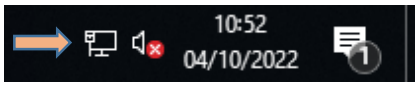


Acto seguido, creo la ip reservada para dmz en Arrendamientos, aplico los cambios, me aseguro de tener la dmz activada en Cortafuegos, Reglas y si observamos en Panel de Control nos aparecerá.

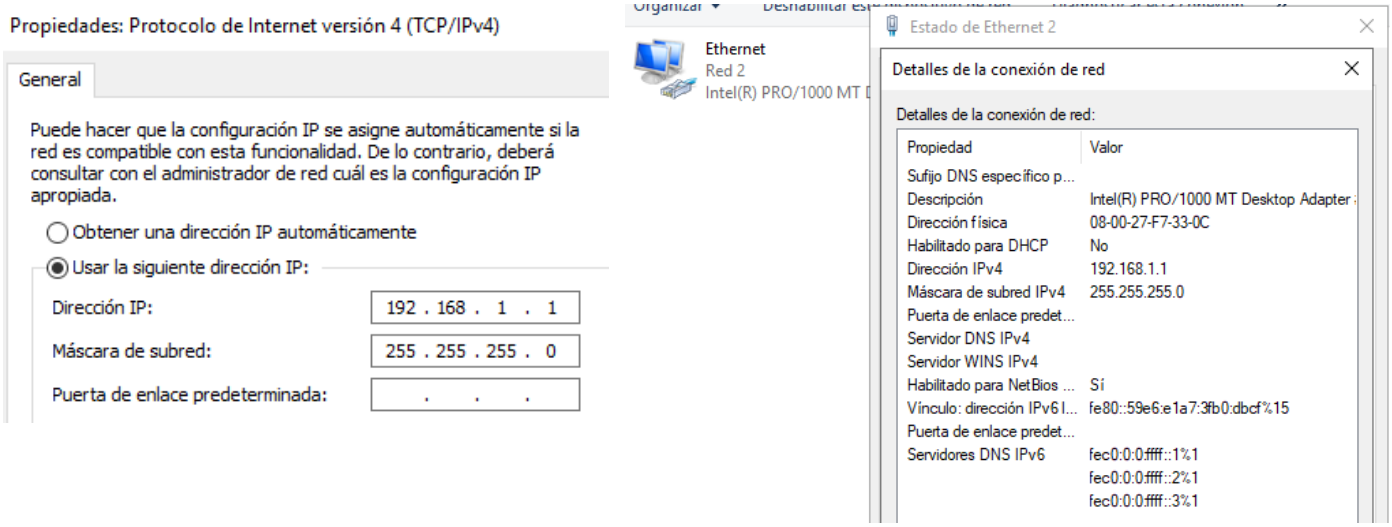
9. EJERCICIO 5

Vuelve a realizar los ejercicios del 1 al 3 pero haciendo uso de un Windows Server.

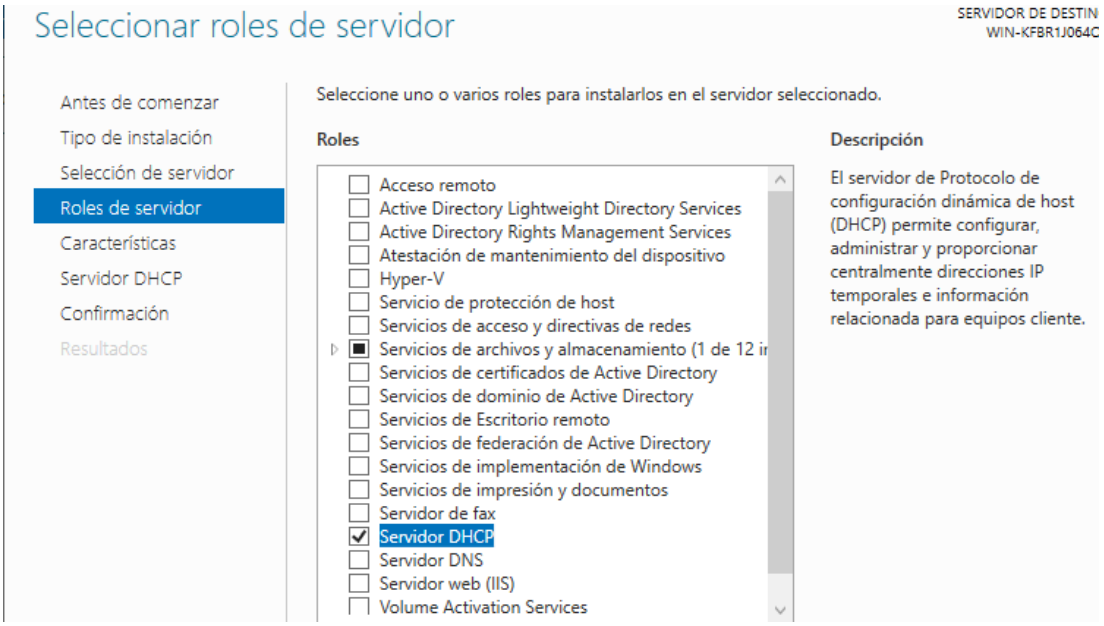
Lo primero que he de decir es que visto cómo funciona el protocolo dhcp en Ubuntu y la funcionalidad de OpenSense, puedo asegurar que en Windows es más sencillo de manejar. Como ejemplo, vamos a crear una red con Windows como servidor al cual vamos a asociar como cliente a un equipo desde red interna y como primer adaptador tendremos un adaptador puente. Lo importante en este caso radica en la configuración de la red lan. Para ello, accedemos a Windows Server y en la zona inferior derecha de la pantalla nos conducimos a Configuración de red.



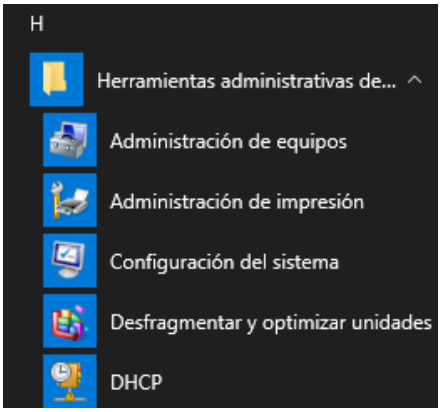
En su interior, cambiamos adaptador, en este caso el segundo de los ethernets que nos surgen, a través de protocolos y reglas, protocolos e ipv4, donde pondremos la ip deseada.



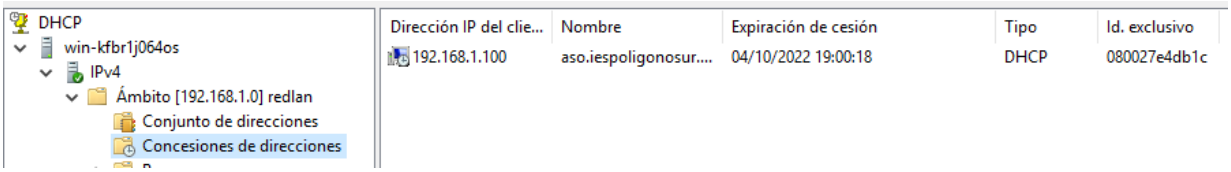
Cuando la tenga asignada, acepto, desactivo y activo. De ahí pasamos, abriendo en la izquierda el menú, a Herramientas Administrativas, Administración de Servidor, Agregar roles y características. Aquí vamos a activar el servidor Dhcp, importante. Aceptar, siguiente e instalar.



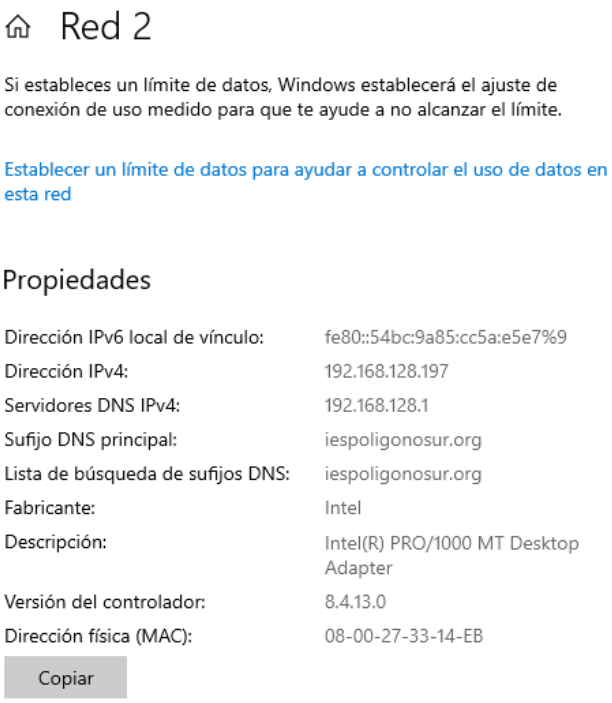
Si echamos un vistazo a Herramientas Administraticas, sale Dhcp.



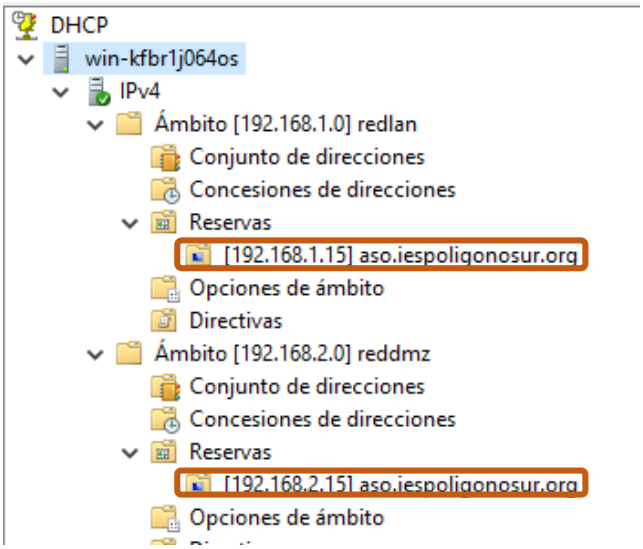
Abro Dhcp, clic derecho en IPv4 y agrego un ámbito de red, que voy a nombrar redlan, avanzo y añado un rango que irá del 192.168.1.100 a la 200 y sigo. En Concesiones de direcciones indico el tiempo de préstamo para la ip y agrego una ip para el enrutador usado para el cliente. Añado el nombre del dominio, como veis en la imagen, activar y finalizar.



Para asegurarme, veo la configuración de la red 2. Y si todo está según lo creado, ya tendremos nuestra configuración dhcp efectuada en Windows Server.



Igualmente, puedo añadir una reserva para cada ámbito dentro de dhcp. Yo, por ejemplo, he hecho sendas reservas, tanto para la red interna lan como para la dmz.



Abro configuración de red, ethernet, cambiar opciones del adaptador y ethernet. Hago clic en propiedades y ahí es donde aparece la ip asignada a cada ámbito.

Hagamos un inciso y vayamos a uno de nuestros clientes para probar una herramienta muy útil como es el WireShark. ¿Qué es Wireshark? Por encima de todo, es un analizador de paquetes de red, una utilidad que captura todo tipo de información que pasa a través de una conexión. Wireshark es gratis y de código abierto, y se puede usar para diagnosticar problemas de red, efectuar auditorías de seguridad y aprender más sobre redes informáticas.

Así que eso vamos a probar, y yo lo voy a hacer en el cliente conectado a través de la red interna lan. Eso sí, yo he cambiado el adaptador a adaptador puente para poder descargar el wireshark. Hecho esto, me dirijo a su terminal e insertamos por línea de comandos sudo apt update y sudo apt install wireshark. Paso a la interfaz gráfica y accedo a Wireshark, marcando la opción dhcp en la barra de búsqueda que nos surgirá en su pantalla inicial. Como veis en la siguiente imagen, me muestra el estado de las transmisiones efectuadas. En este caso en concreto, no me aparecerá ni el offer ni el request, puesto que previamente ya tenía asignada la ip.