SERVICIO

DHCP

MARTA GONZÁLEZ ARNAIZ

2º ASIR

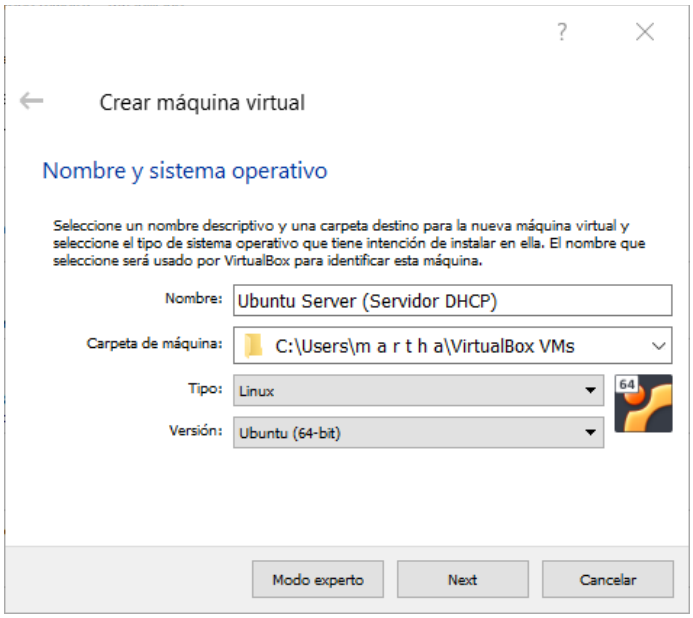
SERVICIOS DE RED E INTERNET

1º EVALUACIÓN

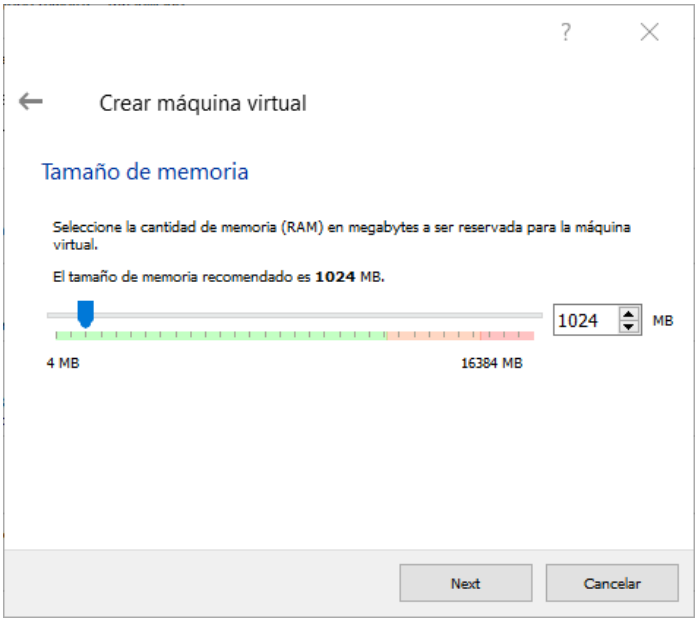
Tabla de contenido

1. CONFIGURA UNA MÁQUINA CON UBUNTU SERVER 20.04.1 TODOS LOS PARÁMETROS NECESARIOS PARA QUE PUEDA REALIZAR LAS FUNCIONES DE SERVIDOR DHCP. SE SABE QUE EN EL SEGMENTO DE RED EN EL QUE ESTARÁ HABRÁ UN MÁXIMO DE 200 HOSTS, UNO DE ELLOS SERÁ EL DE ADMINISTRADOR ("ADMINISTRADOR") AL QUE SIEMPRE LE DARÁ LA MISMA DIRECCIÓN IPV4. ES IMPORTANTE DECIDIR EL TIEMPO DE CONCESIÓN QUE SE DARÁ A CADA UNO DE LOS CLIENTES Y POR QUÉ.

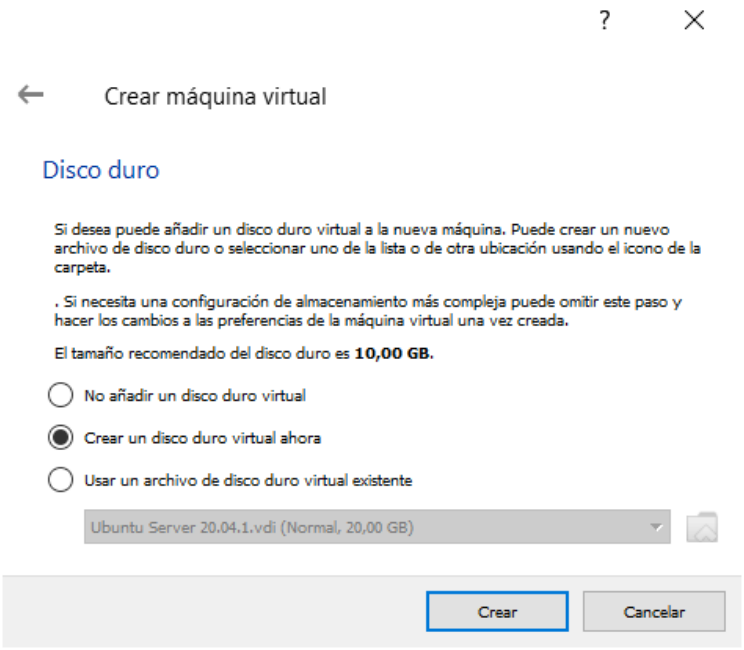
Introducimos el nombre, el tipo y la versión de la máquina virtual. Seleccionamos "Next"



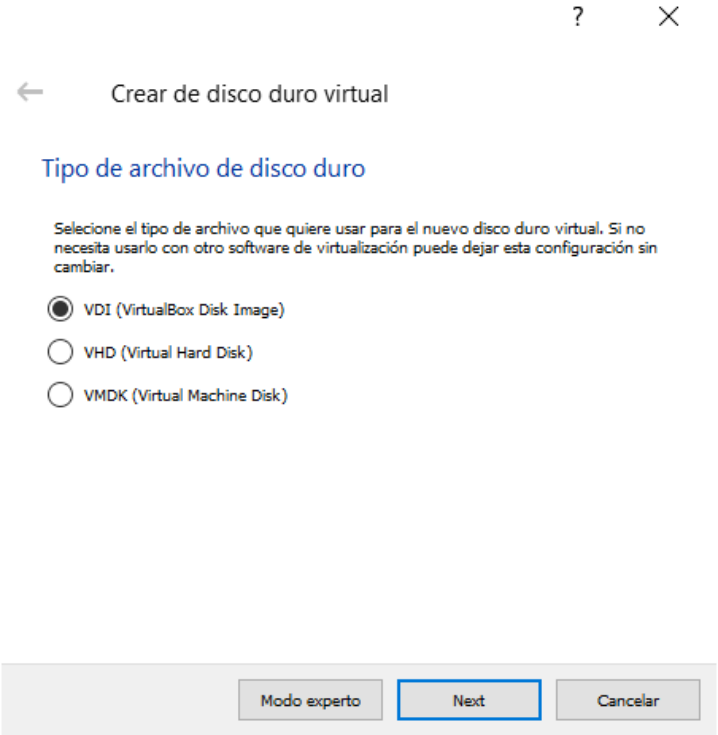
Establecemos el tamaño de la memoria



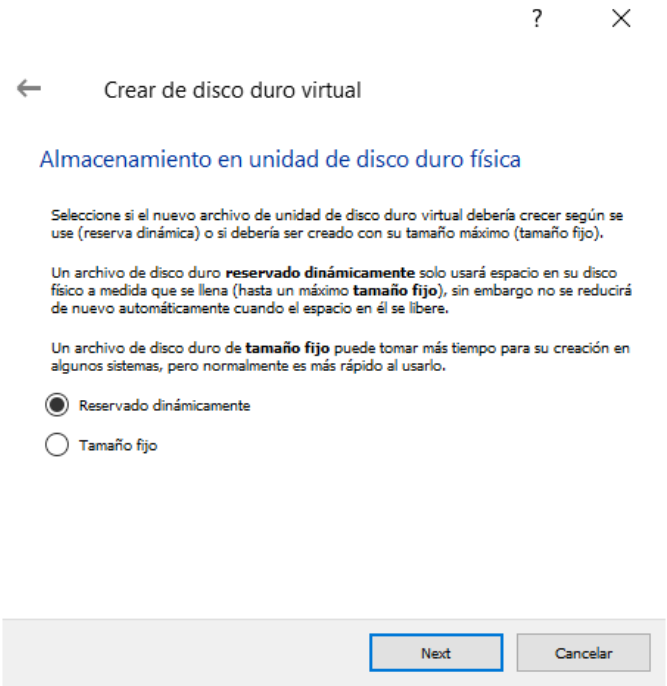
Seleccionamos “Crear un disco duro virtual ahora” y “Crear”



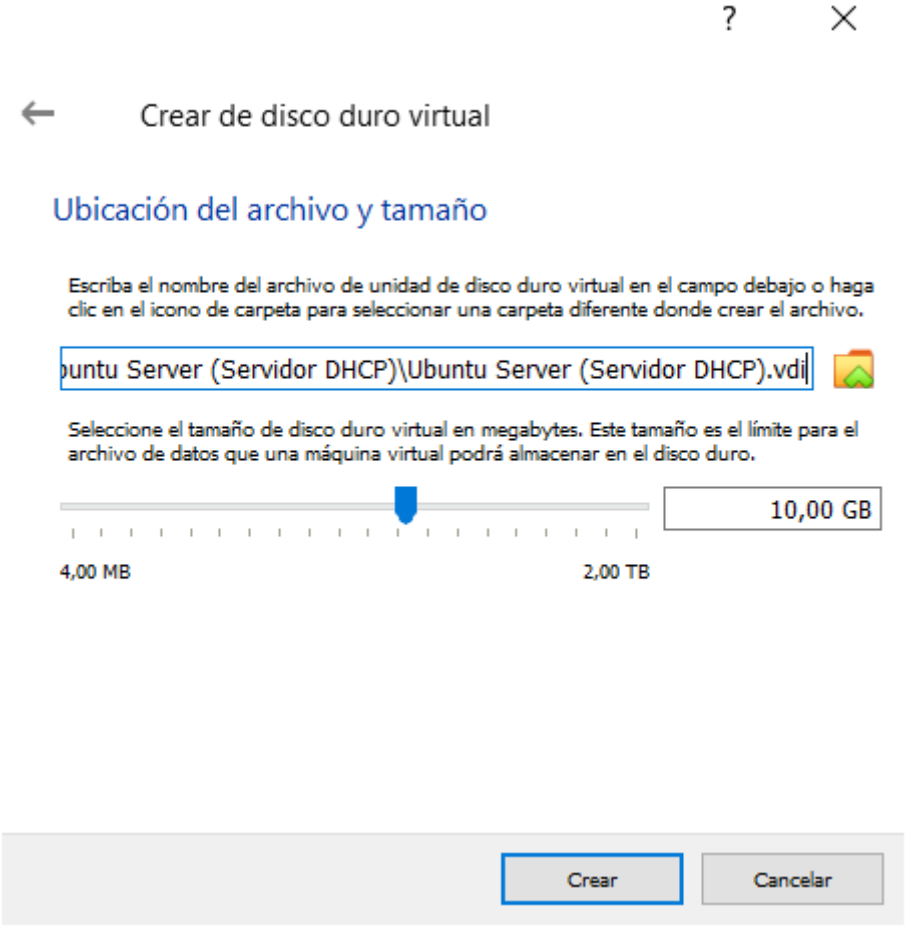
Seleccionamos “VDI” y “Next”



Seleccionamos “Reservado dinámicamente” y “Next”

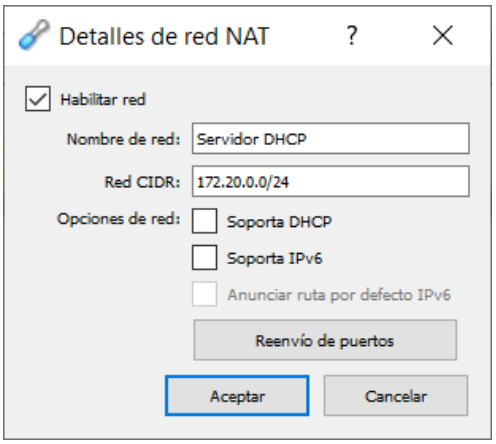


Elegimos la capacidad del disco, en mi caso le asignare 10 GB y seleccionamos “Crear”

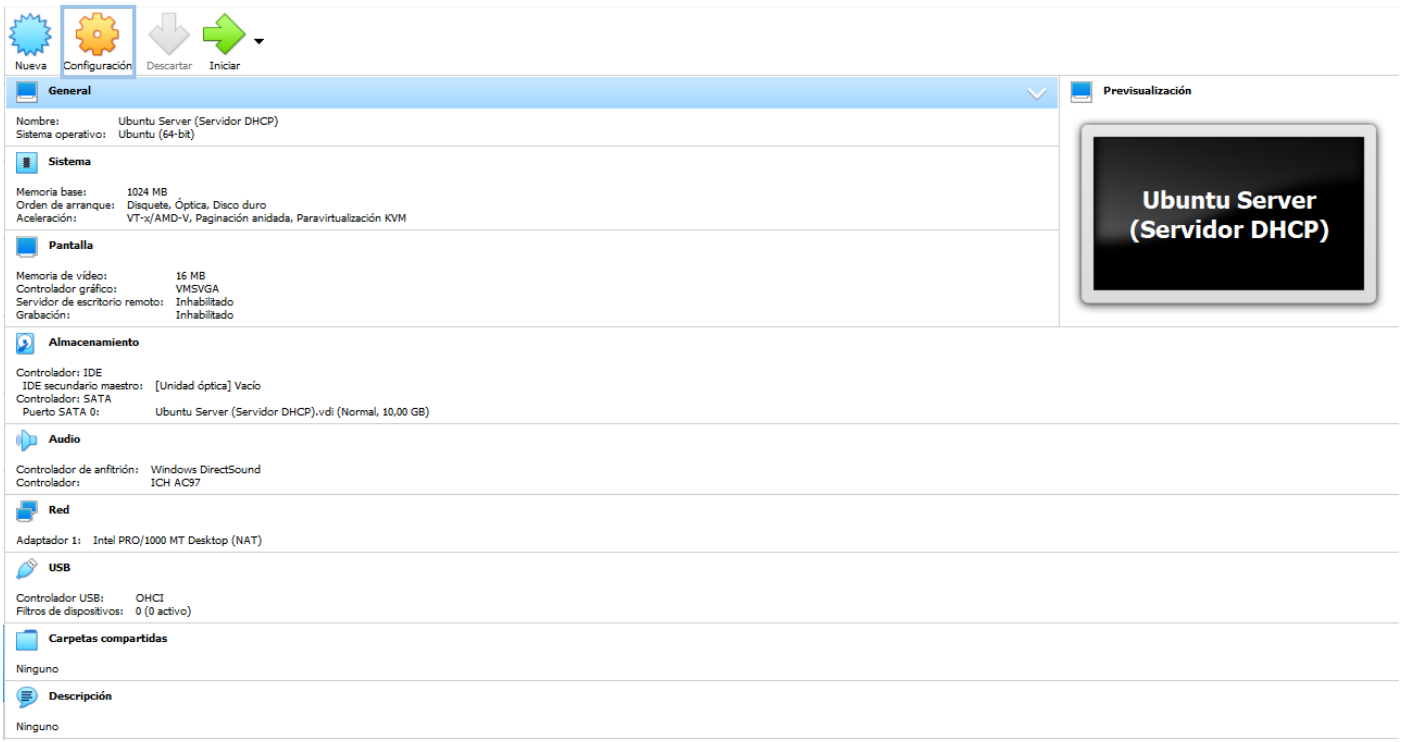


CONFIGURACIÓN DE RED

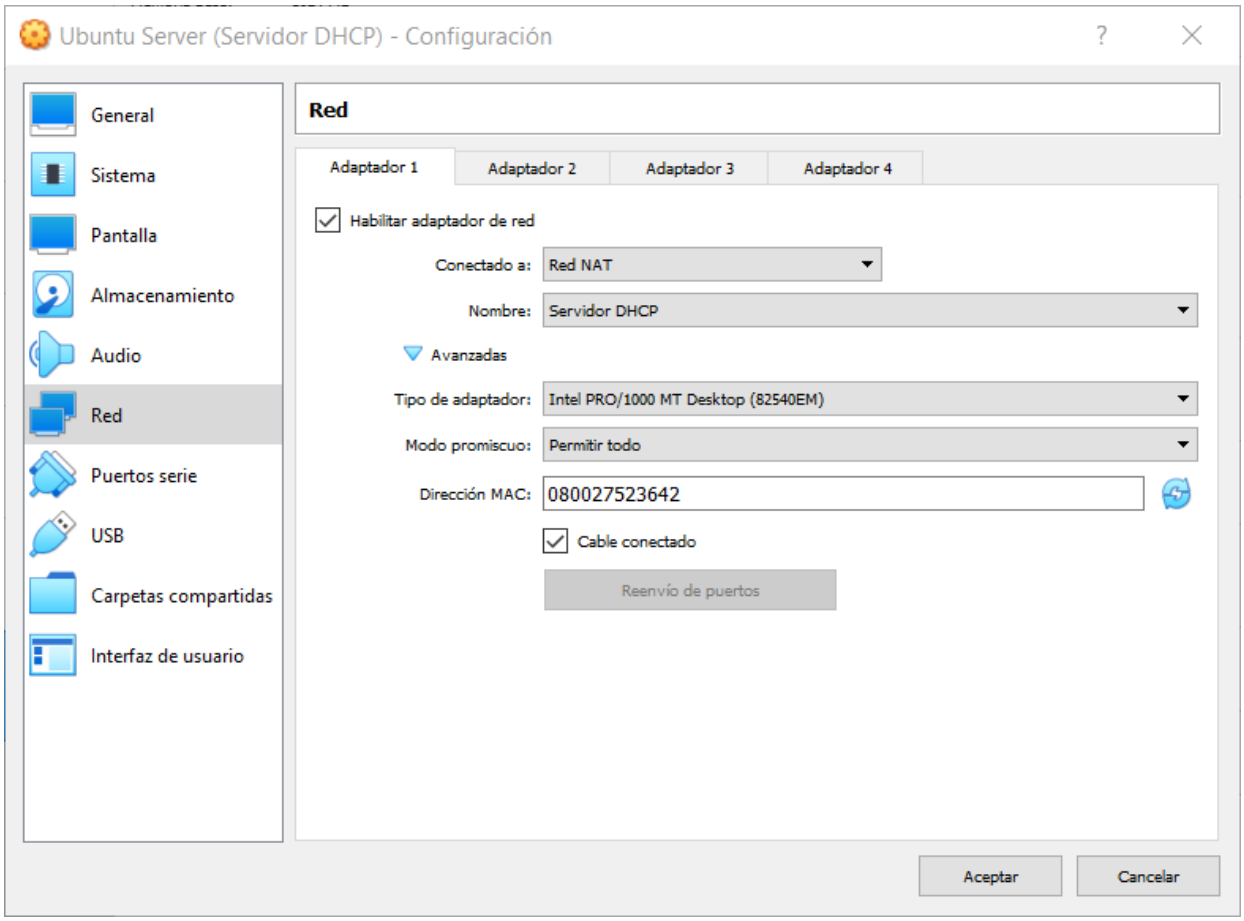
Para esta práctica he creado una red NAT con los siguientes datos:



Seleccionamos la máquina para configurar esa red NAT y "Configuración"

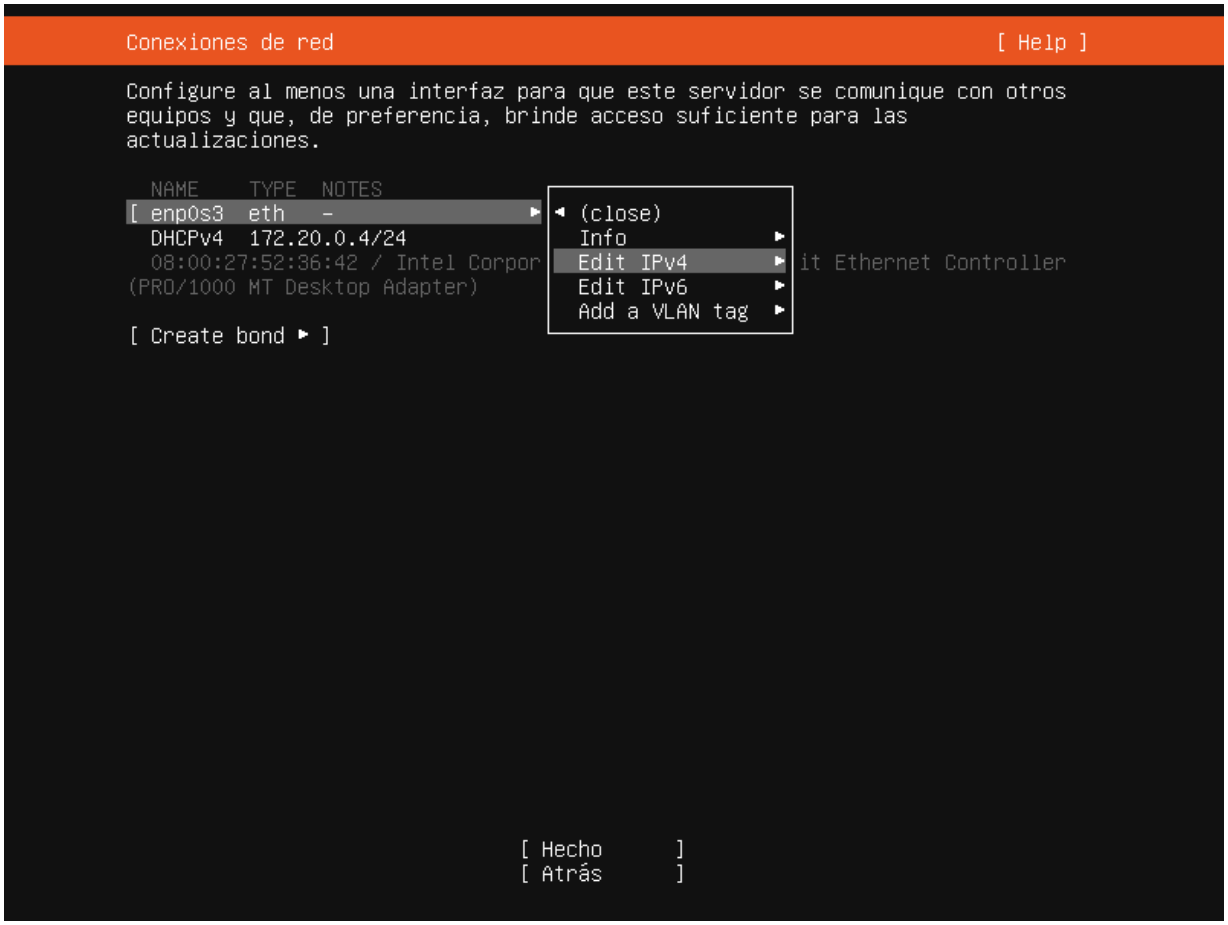


En el apartado de “Red” configuramos las siguientes opciones y seleccionamos “Aceptar”

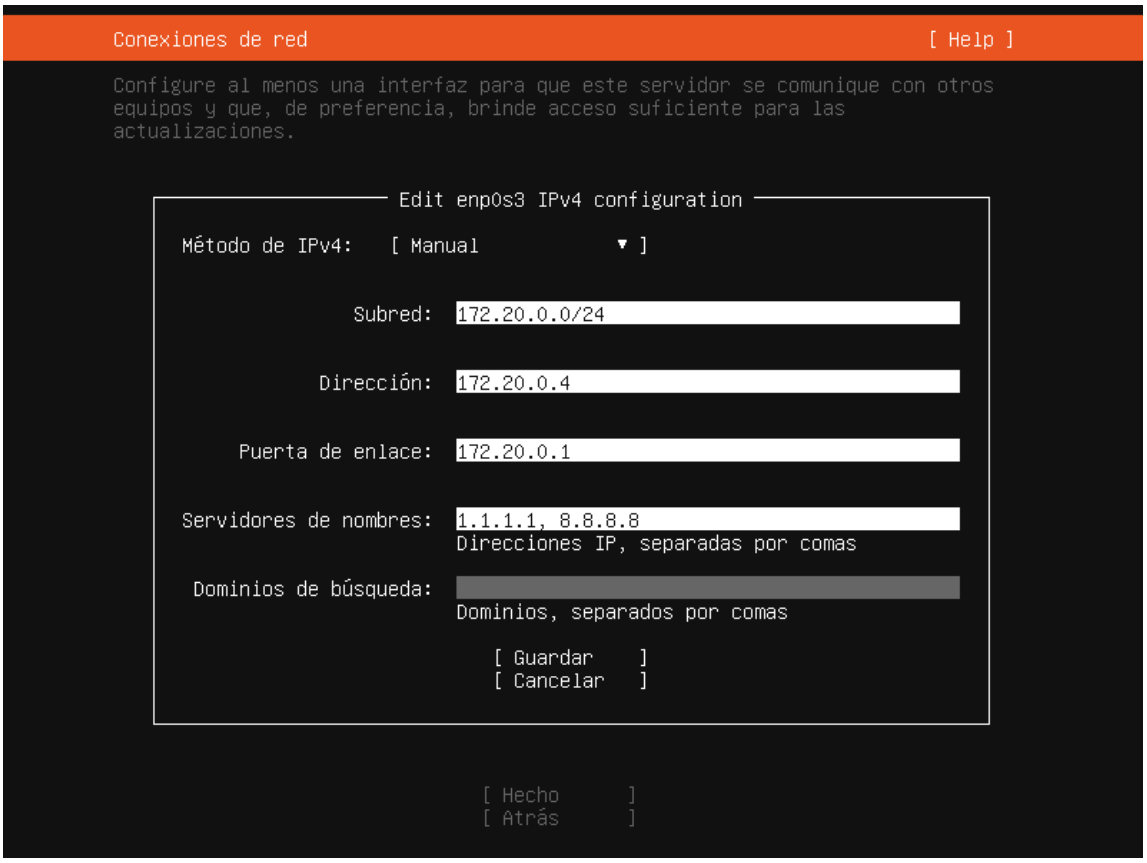


MODIFICACIÓN DE LA CONEXIÓN DE RED EN LA INSTALACIÓN DEL SISTEMA OPERATIVO

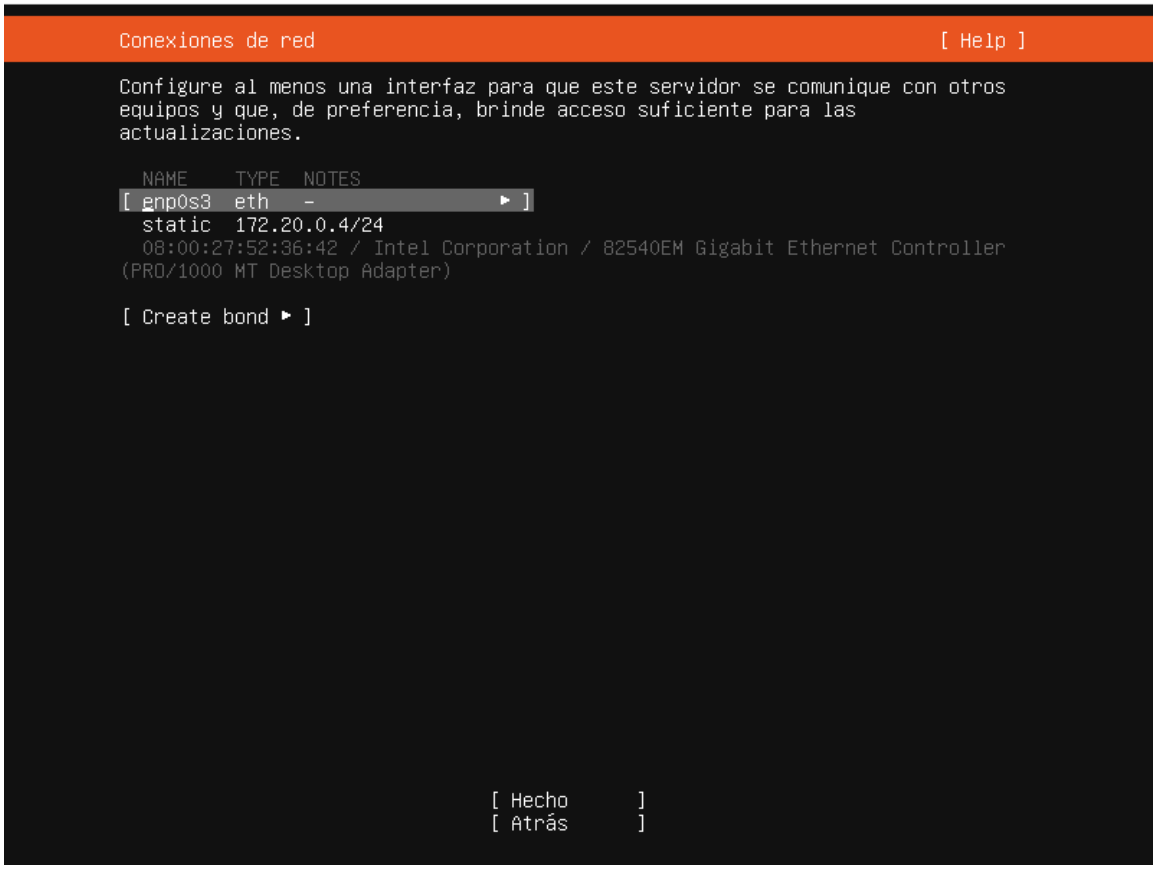
Seleccionamos “enp0s3”>” Edit IPv4”



E introducimos los datos que consideremos, en mi caso los siguientes y seleccionamos “Guardar”



Este sería el aspecto final



CONFIGURACIÓN DEL ARCHIVO DE CONFIGURACION DE RED

Nos dirigimos al siguiente fichero con privilegios root: "/etc/netplan/00-installer-config.yaml"

```
  GNU nano 4.8                    /etc/netplan/00-installer-config.yaml
# This is the network config written by 'subiquity'
network:
  ethernets:
    enp0s3:
      addresses:
      - 172.20.0.4/24
      gateway4: 172.20.0.1
      nameservers:
        addresses:
        - 172.20.0.1
        - 1.1.1.1
        - 8.8.8.8
  version: 2

                                  [ Read 13 lines ]
^G Get Help    ^O Write Out   ^W Where Is    ^K Cut Text    ^J Justify     ^C Cur Pos     M-U Undo
^X Exit        ^R Read File   ^\ Replace     ^U Paste Text  ^T To Spell    ^_ Go To Line  M-E Redo
```

COMPROBACIÓN DEL FUNCIONAMIENTO DEL DNS

```
darlene@allsafe:~$ ping youtube.com
PING youtube.com (172.217.168.174) 56(84) bytes of data.
64 bytes from mad07s10-in-f14.1e100.net (172.217.168.174): icmp_seq=1 ttl=115 time=18.1 ms
64 bytes from mad07s10-in-f14.1e100.net (172.217.168.174): icmp_seq=2 ttl=115 time=18.1 ms
^C
--- youtube.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 18.084/18.109/18.134/0.025 ms
darlene@allsafe:~$ ping google.es
PING google.es (216.58.201.163) 56(84) bytes of data.
64 bytes from mad08s06-in-f3.1e100.net (216.58.201.163): icmp_seq=1 ttl=114 time=20.3 ms
64 bytes from mad08s06-in-f3.1e100.net (216.58.201.163): icmp_seq=2 ttl=114 time=19.8 ms
^C
--- google.es ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 19.778/20.052/20.326/0.274 ms
darlene@allsafe:~$ _
```

INSTALACIÓN DEL PAQUETE

Procedemos a instalar el paquete del servicio DHCP con el comando: “apt-get install isc-dhcp-server”

```
root@allsafe:~# dpkg -l isc-dhcp-server
dpkg-query: no packages found matching isc-dhcp-server
root@allsafe:~# apt install isc-dhcp-server
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libirs-export161 libisccfg-export163
Suggested packages:
  isc-dhcp-server-ldap policycoreutils
The following NEW packages will be installed:
  isc-dhcp-server libirs-export161 libisccfg-export163
0 upgraded, 3 newly installed, 0 to remove and 50 not upgraded.
Need to get 518 kB of archives.
After this operation, 1863 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
```

VERIFICACIÓN DE LA INSTALACIÓN

```
root@allsafe:~# dpkg -s isc-dhcp-server
Package: isc-dhcp-server
Status: install ok installed
Priority: optional
Section: net
Installed-Size: 1501
Maintainer: Ubuntu Developers <ubuntu-devel-discuss@lists.ubuntu.com>
Architecture: amd64
Source: isc-dhcp
Version: 4.4.1-2.1ubuntu5
Replaces: isc-dhcp-common (<= 4.3.3-1)
Depends: debconf (>= 0.5) | debconf-2.0, libc6 (>= 2.15), libdns-export1109, libirs-export161, libis
c-export1105, debianutils (>= 2.8.2), lsb-base, adduser
Recommends: isc-dhcp-common
Suggests: policykit-1, isc-dhcp-server-ldap, policycoreutils
Breaks: isc-dhcp-common (<= 4.3.3-1), logcheck-database (<= 1.3.17~)
Conffiles:
 /etc/apparmor.d/usr.sbin.dhcpd 71899a89baacd8ab357a74b71ce87ce8
 /etc/dhcp/dhcpd.conf 88526c94f8dd06c53d70fcf560304d75
 /etc/dhcp/dhcpd6.conf f35bba2be5960b902190d174dd9f0fb1
 /etc/init.d/isc-dhcp-server 3c7b3c6fa3bcbb7f34e3ec7b657dadf0
 /etc/logcheck/ignore.d.server/isc-dhcp-server 71f490713ed345ec955be8e2a5bc6cf4
Description: ISC DHCP server for automatic IP address assignment
 This is the Internet Software Consortium's DHCP server.
 .
 Dynamic Host Configuration Protocol (DHCP) is a protocol like BOOTP
 (actually dhcpd includes much of the functionality of bootpd). It
 gives client machines "leases" for IP addresses and can
 automatically set their network configuration.
 .
 This server can handle multiple ethernet interfaces.
Homepage: http://www.isc.org
Original-Maintainer: Debian ISC DHCP Maintainers <isc-dhcp@packages.debian.org>
root@allsafe:~#
```

INSTALACIÓN DE NMAP Y COMPROBACION DE LOS PUERTOS

Nmap no viene instalado por lo que ejecutamos el siguiente comando para instalarlo: “apt install nmap”

```
root@allsafe:~# nmap

Command 'nmap' not found, but can be installed with:

snap install nmap  # version 7.80, or
apt  install nmap  # version 7.80+dfsg1-2build1

See 'snap info nmap' for additional versions.

root@allsafe:~# apt install nmap
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libblas3 liblinear4 liblua5.3-0 lua-lpeg nmap-common
Suggested packages:
  liblinear-tools liblinear-dev ncat ndiff zenmap
The following NEW packages will be installed:
  libblas3 liblinear4 liblua5.3-0 lua-lpeg nmap nmap-common
0 upgraded, 6 newly installed, 0 to remove and 50 not upgraded.
Need to get 5669 kB of archives.
After this operation, 26.8 MB of additional disk space will be used.
Do you want to continue? [Y/n] Y
```

Después de la instalación procedemos a verificar el estado de los puertos y en la siguiente captura vemos que los puertos están cerrados ya que el servicio está fallando.

```
root@allsafe:~# nmap 172.20.0.4 -sU -p67-68
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-04 12:23 UTC
Nmap scan report for allsafe (172.20.0.4)
Host is up (0.000016s latency).

PORT   STATE  SERVICE
67/udp closed dhcps
68/udp closed dhcpc

Nmap done: 1 IP address (1 host up) scanned in 0.04 seconds
root@allsafe:~# 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: failed (Result: exit-code) since Sun 2020-10-04 12:17:41 UTC; 6min ago
       Docs: man:dhcpd(8)
   Main PID: 1229 (code=exited, status=1/FAILURE)

Oct 04 12:17:41 allsafe dhcpd[1229]:
Oct 04 12:17:41 allsafe dhcpd[1229]: If you think you have received this message due to a bug rather
Oct 04 12:17:41 allsafe dhcpd[1229]: than a configuration issue please read the section on submitti>
Oct 04 12:17:41 allsafe dhcpd[1229]: bugs on either our web page at www.isc.org or in the README fi>
Oct 04 12:17:41 allsafe dhcpd[1229]: before submitting a bug.  These pages explain the proper
Oct 04 12:17:41 allsafe dhcpd[1229]: process and the information we find helpful for debugging.
Oct 04 12:17:41 allsafe dhcpd[1229]:
Oct 04 12:17:41 allsafe dhcpd[1229]: exiting.
Oct 04 12:17:41 allsafe systemd[1]: isc-dhcp-server.service: Main process exited, code=exited, stat>
Oct 04 12:17:41 allsafe systemd[1]: isc-dhcp-server.service: Failed with result 'exit-code'.
lines 1-16/16 (END)

root@allsafe:~# _
```

CONFIGURACIÓN DEL SERVICIO

Configuración del fichero /etc/default/isc-dhcp-server

Como podemos ver no tenemos puesta ninguna interfaz de escucha

```
  GNU nano 4.8                    /etc/default/isc-dhcp-server
# Defaults for isc-dhcp-server (sourced by /etc/init.d/isc-dhcp-server)

# Path to dhcpd's config file (default: /etc/dhcp/dhcpd.conf).
#DHCPDv4_CONF=/etc/dhcp/dhcpd.conf
#DHCPDv6_CONF=/etc/dhcp/dhcpd6.conf

# Path to dhcpd's PID file (default: /var/run/dhcpd.pid).
#DHCPDv4_PID=/var/run/dhcpd.pid
#DHCPDv6_PID=/var/run/dhcpd6.pid

# Additional options to start dhcpd with.
#       Don't use options -cf or -pf here; use DHCPD_CONF/ DHCPD_PID instead
#OPTIONS=""

# On what interfaces should the DHCP server (dhcpd) serve DHCP requests?
#       Separate multiple interfaces with spaces, e.g. "eth0 eth1".
INTERFACESv4=""
INTERFACESv6=""

                                [ Read 18 lines ]
^G Get Help   ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify    ^C Cur Pos    M-U Undo
^X Exit       ^R Read File  ^\ Replace    ^U Paste Text ^T To Spell   ^_ Go To Line M-E Redo
```

Así que introducimos el alias de nuestra interfaz

```
  GNU nano 4.8                    /etc/default/isc-dhcp-server                    Modified
# Defaults for isc-dhcp-server (sourced by /etc/init.d/isc-dhcp-server)

# Path to dhcpd's config file (default: /etc/dhcp/dhcpd.conf).
#DHCPDv4_CONF=/etc/dhcp/dhcpd.conf
#DHCPDv6_CONF=/etc/dhcp/dhcpd6.conf

# Path to dhcpd's PID file (default: /var/run/dhcpd.pid).
#DHCPDv4_PID=/var/run/dhcpd.pid
#DHCPDv6_PID=/var/run/dhcpd6.pid

# Additional options to start dhcpd with.
#       Don't use options -cf or -pf here; use DHCPD_CONF/ DHCPD_PID instead
#OPTIONS=""

# On what interfaces should the DHCP server (dhcpd) serve DHCP requests?
#       Separate multiple interfaces with spaces, e.g. "eth0 eth1".
INTERFACESv4="enp0s3"
INTERFACESv6=""

^G Get Help   ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify    ^C Cur Pos    M-U Undo
^X Exit       ^R Read File  ^\ Replace    ^U Paste Text ^T To Spell   ^_ Go To Line M-E Redo
```

Configuración del fichero /etc/dhcp/dhcpd.conf

Para agregar la configuración de nuestra red (mascara de red, rango de direcciones o pool, routers …) podemos hacerlo al final del fichero o en esta parte:

```
  GNU nano 4.8                    /etc/dhcp/dhcpd.conf

#subnet 10.152.187.0 netmask 255.255.255.0 {
#}

# This is a very basic subnet declaration.

subnet 172.20.0.0 netmask 255.255.255.0 {
  range 172.20.0.54 172.20.0.254;
  option routers 172.20.0.1;
  option domain-name-servers 1.1.1.1,8.8.8.8,192.168.100.100,192.168.0.61;
  default-lease-time 600;
  max-lease-time 28800;
}_

# This declaration allows BOOTP clients to get dynamic addresses,
# which we don't really recommend.

#subnet 10.254.239.32 netmask 255.255.255.224 {
#  range dynamic-bootp 10.254.239.40 10.254.239.60;
#  option broadcast-address 10.254.239.31;
#  option routers rtr-239-32-1.example.org;
#}

# A slightly different configuration for an internal subnet.
#subnet 10.5.5.0 netmask 255.255.255.224 {
#  range 10.5.5.26 10.5.5.30;
#  option domain-name-servers ns1.internal.example.org;
#  option domain-name "internal.example.org";
#  option subnet-mask 255.255.255.224;
#  option routers 10.5.5.1;
#  option broadcast-address 10.5.5.31;
#  default-lease-time 600;
#  max-lease-time 7200;

^G Get Help   ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify    ^C Cur Pos    M-U Undo
^X Exit       ^R Read File  ^\ Replace    ^U Paste Text ^T To Spell   ^_ Go To Line M-E Redo
```

ASIGNACIÓN DE UNA IP FIJA AL ADMINISTRADOR

Introducimos una máquina Kali al segmento del servidor. Introducimos el siguiente comando para saber su dirección MAC:

```
darlene@MRROBOT: ~
Archivo  Acciones  Editar  Vista  Ayuda

root@MRROBOT:~# ifconfig | grep ether
        ether 08:00:27:70:10:8e  txqueuelen 1000  (Ethernet)
root@MRROBOT:~#
```

En el anterior fichero de configuración nos dirigimos a la siguiente parte:

```
  GNU nano 4.8                          /etc/dhcp/dhcpd.conf
#  option domain-name "internal.example.org";
#  option subnet-mask 255.255.255.224;
#  option routers 10.5.5.1;
#  option broadcast-address 10.5.5.31;
#  default-lease-time 600;
#  max-lease-time 7200;
#}

# Hosts which require special configuration options can be listed in
# host statements.   If no address is specified, the address will be
# allocated dynamically (if possible), but the host-specific information
# will still come from the host declaration.

#host passacaglia {
#  hardware ethernet 0:0:c0:5d:bd:95;
#  filename "vmunix.passacaglia";
#  server-name "toccata.example.com";
#}

# Fixed IP addresses can also be specified for hosts.   These addresses
# should not also be listed as being available for dynamic assignment.
# Hosts for which fixed IP addresses have been specified can boot using
# BOOTP or DHCP.   Hosts for which no fixed address is specified can only
# be booted with DHCP, unless there is an address range on the subnet
# to which a BOOTP client is connected which has the dynamic-bootp flag
# set.
#host fantasia {
#  hardware ethernet 08:00:07:26:c0:a5;
#  fixed-address fantasia.example.com;
#}

# You can declare a class of clients and then do address allocation
# based on that.   The example below shows a case where all clients

^G Get Help   ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify    ^C Cur Pos    M-U Undo
^X Exit       ^R Read File  ^\ Replace    ^U Paste Text ^T To Spell   ^_ Go To Line M-E Redo
```

Se puede incluir la IP fija del administrador en cualquier parte de las dos señaladas

```
  GNU nano 4.8                          /etc/dhcp/dhcpd.conf                    Modified
#  option domain-name "internal.example.org";
#  option subnet-mask 255.255.255.224;
#  option routers 10.5.5.1;
#  option broadcast-address 10.5.5.31;
#  default-lease-time 600;
#  max-lease-time 7200;
#}

# Hosts which require special configuration options can be listed in
# host statements.   If no address is specified, the address will be
# allocated dynamically (if possible), but the host-specific information
# will still come from the host declaration.

host administrador {
  hardware ethernet 08:00:27:70:10:8e;
  fixed-address 172.20.0.7;
}

# Fixed IP addresses can also be specified for hosts.   These addresses
# should not also be listed as being available for dynamic assignment.
# Hosts for which fixed IP addresses have been specified can boot using
# BOOTP or DHCP.   Hosts for which no fixed address is specified can only
# be booted with DHCP, unless there is an address range on the subnet
# to which a BOOTP client is connected which has the dynamic-bootp flag
# set.
#host fantasia {
#  hardware ethernet 08:00:07:26:c0:a5;
#  fixed-address fantasia.example.com;
#}

# You can declare a class of clients and then do address allocation
# based on that.   The example below shows a case where all clients
# in a certain class get addresses on the 10.17.224/24 subnet, and all

^G Get Help   ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify    ^C Cur Pos    M-U Undo
^X Exit       ^R Read File  ^\ Replace    ^U Paste Text ^T To Spell   ^_ Go To Line M-E Redo
```

Y como vemos la configuración se aplica correctamente:

```
root@MRROBOT:~# dhclient -r
root@MRROBOT:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.20.0.54  netmask 255.255.255.0  broadcast 172.20.0.255
        inet6 fe80::a00:27ff:fe70:108e  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:70:10:8e  txqueuelen 1000  (Ethernet)
        RX packets 15  bytes 2068 (2.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 42  bytes 4352 (4.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 12  bytes 556 (556.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 12  bytes 556 (556.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@MRROBOT:~#
```

2. REALIZA Y DOCUMENTA TODAS LAS COMPROBACIONES NECESARIAS PARA COMPROBAR QUE REALMENTE ÉSTA SE ENCUENTRA PREPARADA PARA REALIZAR SU FUNCIÓN Y FUNCIONA DE MANERA CORRECTA.

Aplicamos todos los cambios hecho anteriormente y comprobamos el funcionamiento del servicio:

```
root@allsafe:~# service isc-dhcp-server stop
root@allsafe:~# service isc-dhcp-server start
root@allsafe:~# service isc-dhcp-server restart
root@allsafe:~# 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 Sun 2020-10-04 12:38:23 UTC; 35s ago
       Docs: man:dhcpd(8)
   Main PID: 1913 (dhcpd)
      Tasks: 4 (limit: 1075)
     Memory: 4.5M
     CGroup: /system.slice/isc-dhcp-server.service
             └─1913 dhcpd -user dhcpd -group dhcpd -f -4 -pf /run/dhcp-server/dhcpd.pid -cf /etc/dh>

Oct 04 12:38:23 allsafe sh[1913]: PID file: /run/dhcp-server/dhcpd.pid
Oct 04 12:38:23 allsafe dhcpd[1913]: Wrote 0 leases to leases file.
Oct 04 12:38:23 allsafe sh[1913]: Wrote 0 leases to leases file.
Oct 04 12:38:23 allsafe dhcpd[1913]: Listening on LPF/enp0s3/08:00:27:52:36:42/172.20.0.0/24
Oct 04 12:38:23 allsafe sh[1913]: Listening on LPF/enp0s3/08:00:27:52:36:42/172.20.0.0/24
Oct 04 12:38:23 allsafe sh[1913]: Sending on   LPF/enp0s3/08:00:27:52:36:42/172.20.0.0/24
Oct 04 12:38:23 allsafe sh[1913]: Sending on   Socket/fallback/fallback-net
Oct 04 12:38:23 allsafe dhcpd[1913]: Sending on   LPF/enp0s3/08:00:27:52:36:42/172.20.0.0/24
Oct 04 12:38:23 allsafe dhcpd[1913]: Sending on   Socket/fallback/fallback-net
Oct 04 12:38:23 allsafe dhcpd[1913]: Server starting service.
lines 1-20/20 (END)
```

Hacemos un nmap para comprobar el estado de los puertos:

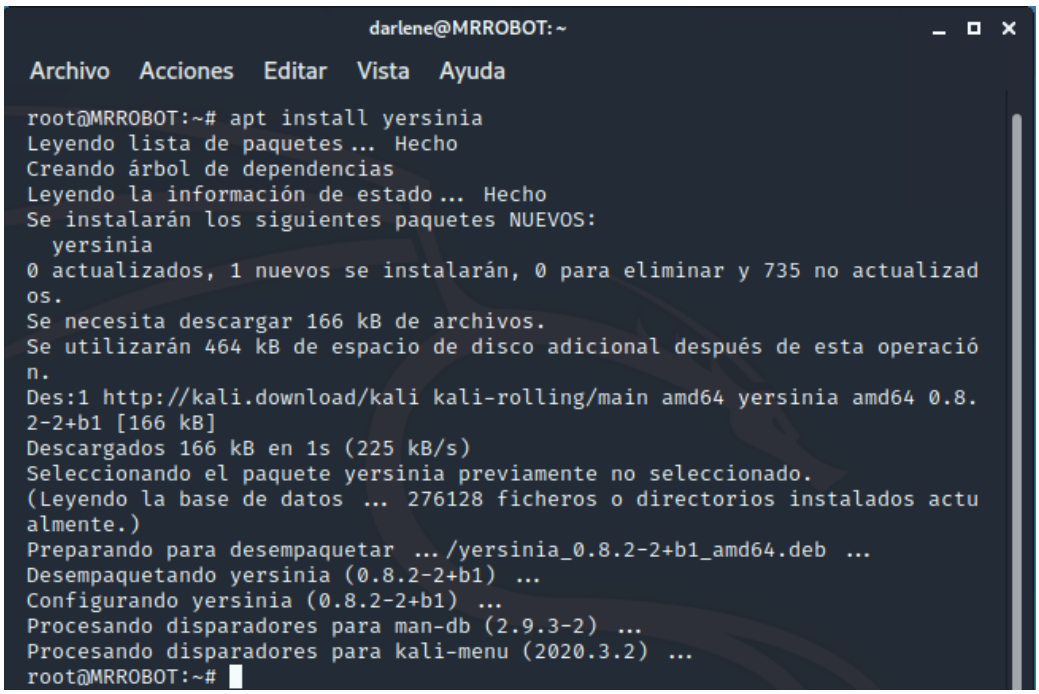
```
root@allsafe:~# nmap 172.20.0.4 -sU -p67-68
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-04 12:39 UTC
Nmap scan report for allsafe (172.20.0.4)
Host is up (0.0000090s latency).

PORT   STATE         SERVICE
67/udp open|filtered dhcps
68/udp closed        dhcpc

Nmap done: 1 IP address (1 host up) scanned in 1.26 seconds
root@allsafe:~#
```

Para comprobar realmente el funcionamiento he introducido una máquina con Windows 10 y podemos ver que funciona perfectamente

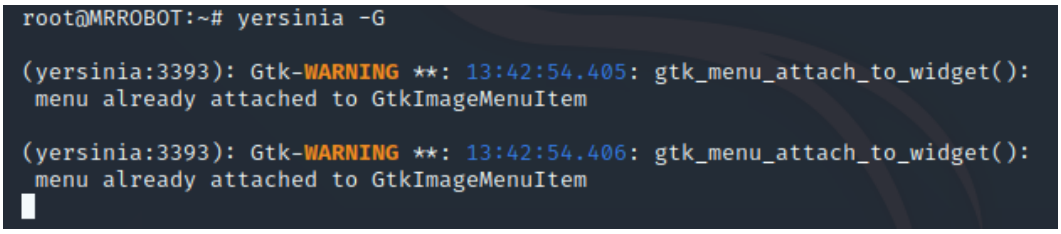
```
Símbolo del sistema
Microsoft Windows [Versión 10.0.19041.508]
(c) 2020 Microsoft Corporation. Todos los derechos reservados.

C:\Users\m a r t h a>ipconfig

Configuración IP de Windows


Adaptador de Ethernet Ethernet:

   Sufijo DNS específico para la conexión. . : home
   Vínculo: dirección IPv6 local. . . : fe80::448b:62f7:757c:fd4%7
   Dirección IPv4. . . . . . . . . . . . . : 172.20.0.5
   Máscara de subred . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . : 172.20.0.1

C:\Users\m a r t h a>_
```

3. AHORA EN EL SEGMENTO DE RED SE CUELA UNA MÁQUINA ATACANTE. ATACA AL SERVIDOR DHCP PARA CONSUMIR TODO SU POOL DE DIRECCIONES DISPONIBLES PARA LOS CLIENTES. PARA ELLO UTILIZA LA HERRAMIENTA YERSINIA (HTTPS://TOOLS.KALI.ORG/VULNERABILITY-ANALYSIS/YERSINIA) PRESENTE EN KALI LINUX.

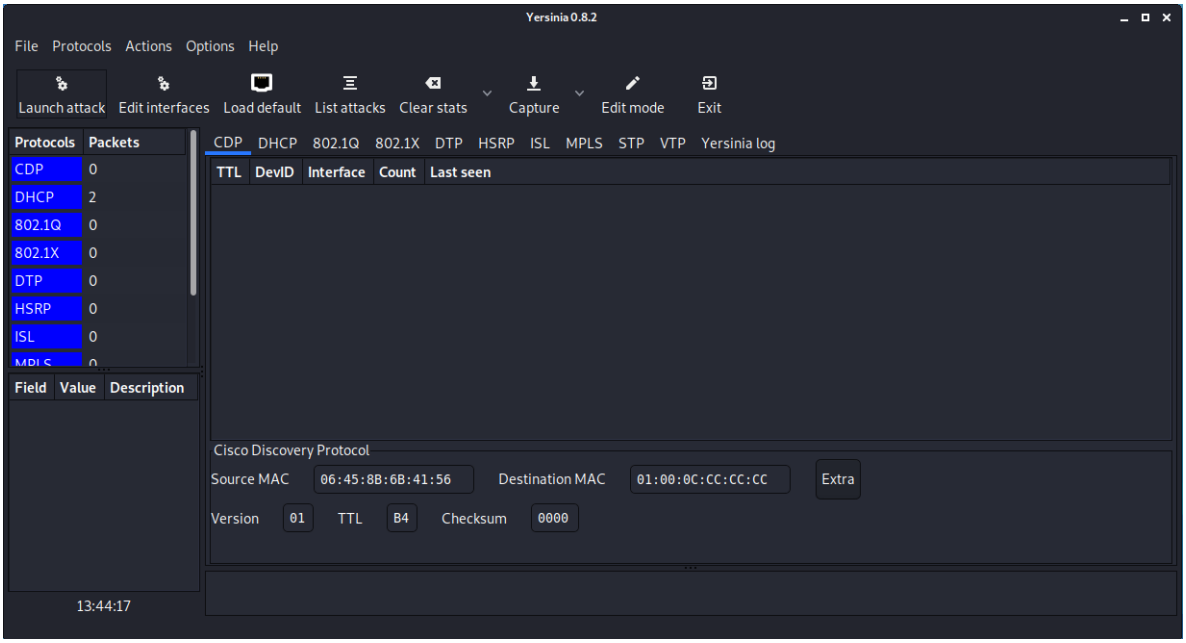
Instalamos la herramienta Yersinia con el siguiente comando: "apt-get install yersinia"



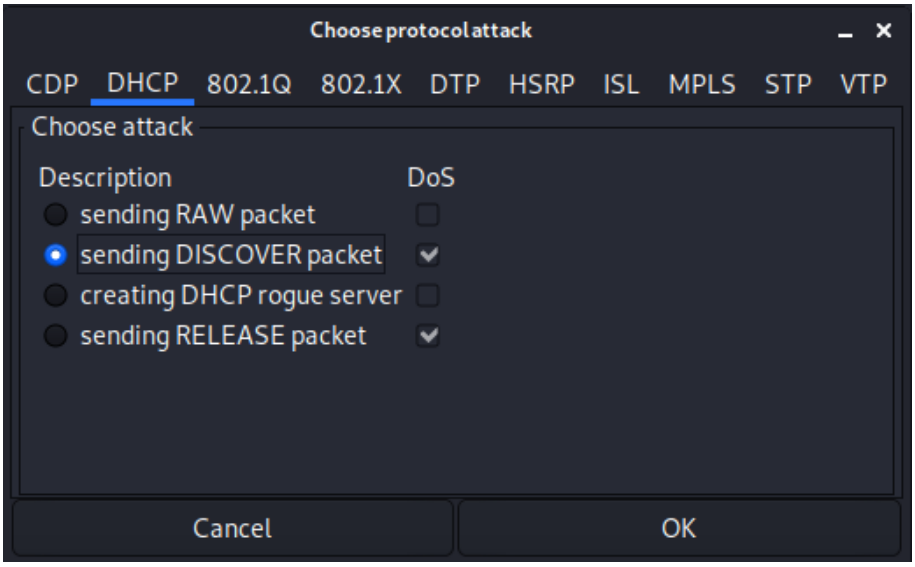
Iniciamos la herramienta con el comando "yersinia -G"



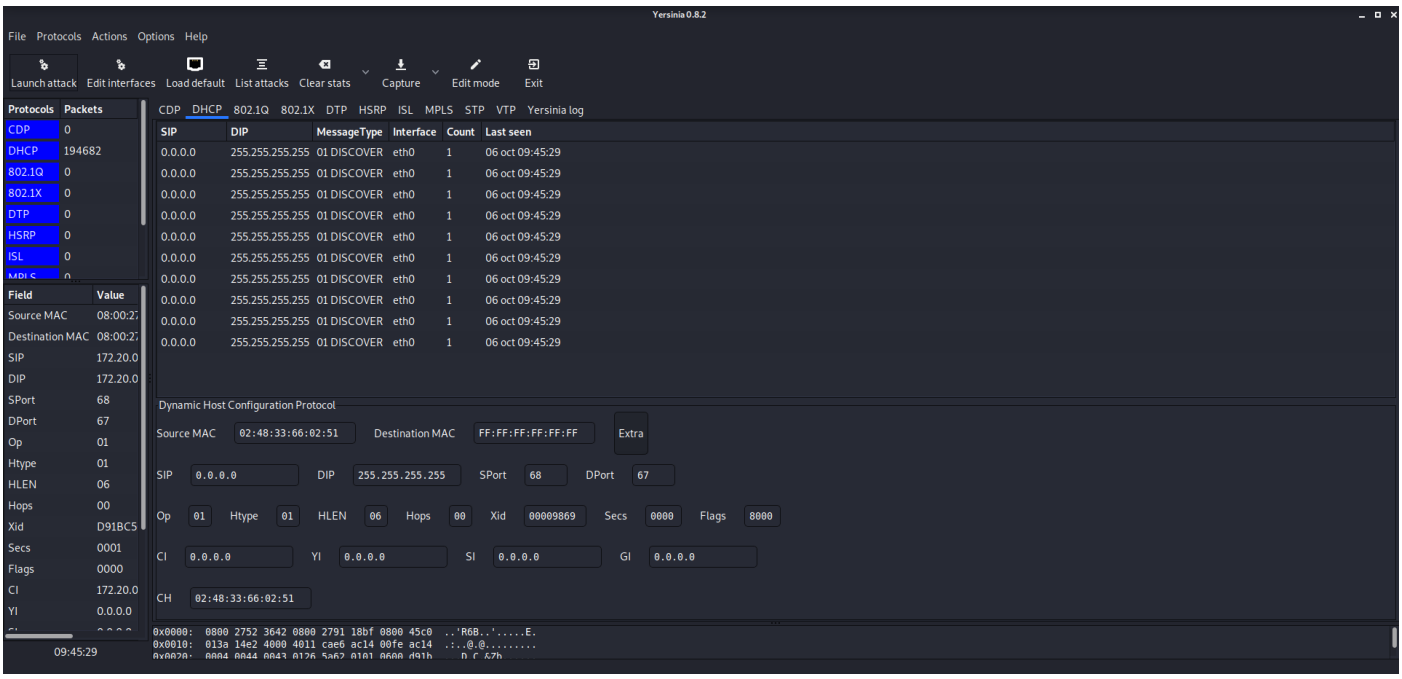
Se iniciará la interfaz de la herramienta y seleccionamos "Launch attack"



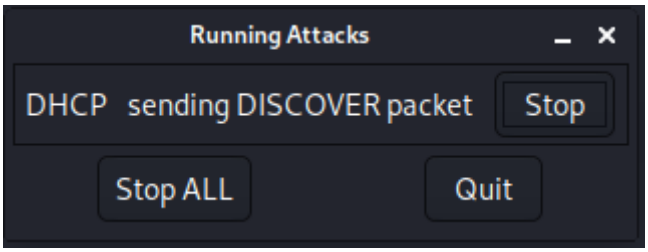
Seleccionamos "DHCP" y el tipo de ataque, en nuestro caso "sending DISCOVER packet" con DoS seleccionado, lo que provocara un ataque de denegación de servicio.



Empieza a mandar peticiones por broadcast con direcciones MAC falsas agotando así el pool de direcciones



Paramos el ataque seleccionando "List attacks" > "Stop"



Si observamos Wireshark, vemos que realmente se están haciendo las peticiones DHCP-DISCOVER consumiendo así todas las direcciones IP que ofrece el servidor.

No.	Time	Source	Destination	Protocol	Length	Info
17422	1.385776136	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
17423	1.385853962	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
17424	1.385870626	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
17425	1.385921515	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
17426	1.386009683	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
17427	1.386027967	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
17428	1.390343060	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
17429	1.390361092	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
17430	1.391653467	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
17431	1.391671547	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
17432	1.391692611	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
17433	1.391705698	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
17434	1.391716217	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
17435	1.391763070	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
17436	1.391776143	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
17437	1.391784667	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
17438	1.391792483	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869

4. DOCUMENTA LOS COMANDOS CON LOS PARÁMETROS UTILIZANDO EN EL PUNTO ANTERIOR EXPLICANDO PARA QUÉ VALEN, ASÍ COMO LOS RESULTADOS OBTENIDOS.

Si nos dirigimos al servidor y observamos el fichero "/var/lib/dhcp/dhcpd.leases" veremos que se han ofrecido la totalidad de las IPs:

```
  GNU nano 4.8                    /var/lib/dhcp/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 172.20.0.57 {
  starts 0 2020/10/04 13:29:09;
  ends 0 2020/10/04 13:31:09;
  tstp 0 2020/10/04 13:31:09;
  cltt 0 2020/10/04 13:29:09;
  binding state free;
  hardware ethernet 40:ef:03:16:16:39;
}
lease 172.20.0.58 {
  starts 0 2020/10/04 13:29:09;
  ends 0 2020/10/04 13:31:09;
  tstp 0 2020/10/04 13:31:09;
  cltt 0 2020/10/04 13:29:09;
  binding state free;
  hardware ethernet fa:06:28:3b:ad:85;
}
lease 172.20.0.59 {
  starts 0 2020/10/04 13:29:09;
  ends 0 2020/10/04 13:31:09;
  tstp 0 2020/10/04 13:31:09;
  cltt 0 2020/10/04 13:29:09;
  binding state free;
  hardware ethernet 2f:f9:66:41:1b:b6;
}
lease 172.20.0.60 {
  starts 0 2020/10/04 13:29:09;
  ends 0 2020/10/04 13:31:09;
                                [ Read 1641 lines ]
^G Get Help   ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify    ^C Cur Pos    M-U Undo
^X Exit       ^R Read File  ^\ Replace    ^U Paste Text ^T To Spell   ^_ Go To Line M-E Redo
```

```
  GNU nano 4.8                    /var/lib/dhcp/dhcpd.leases
  starts 2 2020/10/06 07:32:05;
  ends 2 2020/10/06 07:42:05;
  cltt 2 2020/10/06 07:32:05;
  binding state active;
  next binding state free;
  rewind binding state free;
  hardware ethernet 08:00:27:91:18:bf;
  uid "\001\010\000'\221\030\277";
  client-hostname "yersinia";
}
lease 172.20.0.254 {
  starts 2 2020/10/06 07:37:41;
  ends 2 2020/10/06 07:47:41;
  cltt 2 2020/10/06 07:37:41;
  binding state active;
  next binding state free;
  rewind binding state free;
  hardware ethernet 08:00:27:91:18:bf;
  uid "\001\010\000'\221\030\277";
  client-hostname "yersinia";
}
lease 172.20.0.254 {
  starts 2 2020/10/06 07:42:41;
  ends 2 2020/10/06 07:52:41;
  cltt 2 2020/10/06 07:42:41;
  binding state active;
  next binding state free;
  rewind binding state free;
  hardware ethernet 08:00:27:91:18:bf;
  uid "\001\010\000'\221\030\277";
  client-hostname "yersinia";
}

^G Get Help   ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify    ^C Cur Pos    M-U Undo
^X Exit       ^R Read File  ^\ Replace    ^U Paste Text ^T To Spell   ^_ Go To Line M-E Redo
```

El ataque DHCP DISCOVER o agotamiento DHCP o DHCP Starvation consiste en inundar con peticiones DHCP Discover al servidor simulando diferentes direcciones MAC, consiguiendo una IP nueva por cada dirección MAC con un tiempo indefinido ya que el ataque es continuo.

Se puede decir que es un ataque DoS o denegación de servicio.

Si introducimos el comando "service isc-dhcp-server status" veremos que realmente el servidor ya no tiene IPs disponibles

```
● 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 Fri 2020-10-09 18:07:46 UTC; 19h ago
       Docs: man:dhcpd(8)
   Main PID: 1131 (dhcpd)
      Tasks: 4 (limit: 1075)
     Memory: 5.7M
     CGroup: /system.slice/isc-dhcp-server.service
             └─1131 dhcpd -user dhcpd -group dhcpd -f -4 -pf /run/dhcp-server/dhcpd.pid -cf /etc/dh>

Oct 10 13:26:44 allsafe dhcpd[1131]: DHCPDISCOVER from 46:ea:5f:7e:1b:c9 via enp0s3: network 172.20>
Oct 10 13:26:44 allsafe dhcpd[1131]: DHCPDISCOVER from 30:b0:7e:51:56:2f via enp0s3: network 172.20>
Oct 10 13:26:44 allsafe dhcpd[1131]: DHCPDISCOVER from e0:05:b0:17:17:4a via enp0s3: network 172.20>
Oct 10 13:26:44 allsafe dhcpd[1131]: DHCPDISCOVER from 61:8c:52:01:6f:ac via enp0s3: network 172.20>
Oct 10 13:26:44 allsafe dhcpd[1131]: DHCPDISCOVER from 54:1a:85:7f:37:33 via enp0s3: network 172.20>
Oct 10 13:26:44 allsafe dhcpd[1131]: DHCPDISCOVER from e7:dd:f0:25:a6:b4 via enp0s3: network 172.20>
Oct 10 13:26:44 allsafe dhcpd[1131]: DHCPDISCOVER from 37:4c:9a:22:15:0f via enp0s3: network 172.20>
Oct 10 13:26:44 allsafe dhcpd[1131]: DHCPDISCOVER from 79:ce:59:4a:55:f8 via enp0s3: network 172.20>
Oct 10 13:26:44 allsafe dhcpd[1131]: DHCPDISCOVER from d4:0a:bf:3c:20:f0 via enp0s3: network 172.20>
Oct 10 13:26:44 allsafe dhcpd[1131]: DHCPDISCOVER from 05:31:b0:33:36:be via enp0s3: network 172.20>
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
lines 1-20/20 (END)
```

```
server.service; enabled; vendor preset: enabled)
 18:07:46 UTC; 19h ago




 -f -4 -pf /run/dhcp-server/dhcpd.pid -cf /etc/dhcp/dhcpd.conf

from 46:ea:5f:7e:1b:c9 via enp0s3: network 172.20.0.0/24: no free leases
from 30:b0:7e:51:56:2f via enp0s3: network 172.20.0.0/24: no free leases
from e0:05:b0:17:17:4a via enp0s3: network 172.20.0.0/24: no free leases
from 61:8c:52:01:6f:ac via enp0s3: network 172.20.0.0/24: no free leases
from 54:1a:85:7f:37:33 via enp0s3: network 172.20.0.0/24: no free leases
from e7:dd:f0:25:a6:b4 via enp0s3: network 172.20.0.0/24: no free leases
from 37:4c:9a:22:15:0f via enp0s3: network 172.20.0.0/24: no free leases
from 79:ce:59:4a:55:f8 via enp0s3: network 172.20.0.0/24: no free leases
from d4:0a:bf:3c:20:f0 via enp0s3: network 172.20.0.0/24: no free leases
from 05:31:b0:33:36:be via enp0s3: network 172.20.0.0/24: no free leases
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
lines 1-20/20 (END)
```

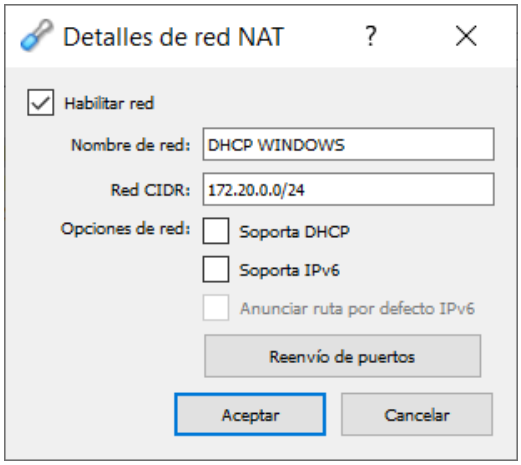
También podemos consultar el fichero /var/log/syslog

```
  [1/1]                                   /var/log/syslog
Oct  4 13:17:01 allsafe CRON[2310]: (root) CMD (   cd / && run-parts --report /etc/cron.hourly)
Oct  4 13:23:09 allsafe dhcpd[2292]: DHCPDISCOVER from 00:da:69:71:29:24 via enp0s3
Oct  4 13:23:09 allsafe dhcpd[2292]: DHCPDISCOVER from 46:62:9f:4b:15:5b via enp0s3
Oct  4 13:23:09 allsafe dhcpd[2292]: DHCPDISCOVER from 30:69:a1:25:88:83 via enp0s3
Oct  4 13:23:09 allsafe dhcpd[2292]: DHCPDISCOVER from f4:fe:f8:37:b7:fb via enp0s3
Oct  4 13:23:09 allsafe dhcpd[2292]: DHCPDISCOVER from 62:a3:d9:11:df:b5 via enp0s3
Oct  4 13:23:09 allsafe dhcpd[2292]: DHCPDISCOVER from 2e:33:6a:0b:01:db via enp0s3
Oct  4 13:23:09 allsafe dhcpd[2292]: DHCPDISCOVER from 80:d8:5c:57:94:df via enp0s3
Oct  4 13:23:09 allsafe dhcpd[2292]: DHCPDISCOVER from 12:07:65:47:98:12 via enp0s3
Oct  4 13:23:09 allsafe dhcpd[2292]: DHCPDISCOVER from 3a:0c:2c:5d:ea:81 via enp0s3
Oct  4 13:23:09 allsafe dhcpd[2292]: DHCPDISCOVER from 25:ce:a7:11:2a:67 via enp0s3
Oct  4 13:23:09 allsafe dhcpd[2292]: DHCPDISCOVER from 61:a8:88:35:11:ce via enp0s3
Oct  4 13:23:09 allsafe dhcpd[2292]: DHCPDISCOVER from 8f:30:dd:2b:6a:e0 via enp0s3
Oct  4 13:23:09 allsafe dhcpd[2292]: DHCPDISCOVER from 84:76:2b:54:85:cc via enp0s3
Oct  4 13:23:09 allsafe dhcpd[2292]: DHCPDISCOVER from 9e:66:a3:44:9c:28 via enp0s3
Oct  4 13:23:09 allsafe dhcpd[2292]: DHCPDISCOVER from 2f:41:6e:78:45:2b via enp0s3
Oct  4 13:23:09 allsafe dhcpd[2292]: DHCPDISCOVER from ec:bb:94:05:07:85 via enp0s3
Oct  4 13:23:09 allsafe dhcpd[2292]: DHCPDISCOVER from 10:1d:5e:32:66:6f via enp0s3
Oct  4 13:23:09 allsafe dhcpd[2292]: DHCPDISCOVER from a3:08:79:57:40:de via enp0s3
Oct  4 13:23:09 allsafe dhcpd[2292]: DHCPDISCOVER from 47:99:a8:59:09:17 via enp0s3
Oct  4 13:23:09 allsafe dhcpd[2292]: DHCPDISCOVER from cd:2e:2b:2b:2b:a8 via enp0s3
Oct  4 13:23:09 allsafe dhcpd[2292]: DHCPDISCOVER from 38:b1:b1:1b:90:98 via enp0s3
Oct  4 13:23:09 allsafe dhcpd[2292]: DHCPDISCOVER from 95:ca:97:38:c6:fc via enp0s3
Oct  4 13:23:09 allsafe dhcpd[2292]: DHCPDISCOVER from 19:04:0c:74:a4:51 via enp0s3
Oct  4 13:23:09 allsafe dhcpd[2292]: DHCPDISCOVER from 8a:64:d4:2a:8b:61 via enp0s3
Oct  4 13:23:09 allsafe dhcpd[2292]: DHCPDISCOVER from 24:0b:6a:48:2c:6f via enp0s3
Oct  4 13:23:09 allsafe dhcpd[2292]: DHCPDISCOVER from 06:17:af:31:78:31 via enp0s3
Oct  4 13:23:09 allsafe dhcpd[2292]: DHCPDISCOVER from c7:ff:76:3d:21:a5 via enp0s3
Oct  4 13:23:09 allsafe dhcpd[2292]: DHCPDISCOVER from 80:75:62:1c:ed:87 via enp0s3
Oct  4 13:23:09 allsafe dhcpd[2292]: DHCPDISCOVER from 4c:9d:5a:54:24:3d via enp0s3
Oct  4 13:23:09 allsafe dhcpd[2292]: DHCPDISCOVER from 60:81:2a:2f:44:2b via enp0s3
Oct  4 13:23:09 allsafe dhcpd[2292]: DHCPDISCOVER from 0b:fd:5d:6b:0b:72 via enp0s3
Oct  4 13:23:09 allsafe dhcpd[2292]: DHCPDISCOVER from aa:f9:a0:36:d8:37 via enp0s3

^G Get Help   ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify    ^C Cur Pos    M-U Undo
^X Exit       ^R Read File  ^\ Replace    ^U Paste Text ^T To Spell   ^_ Go To Line M-E Redo
```

```
Oct  4 13:23:09 allsafe dhcpd[2292]: DHCPDISCOVER from d0:81:19:07:06:95 via enp0s3: network 172.20>
<172.20.0.0/24: no free leases
Oct  4 13:23:09 allsafe dhcpd[2292]: DHCPDISCOVER from 81:70:37:5a:70:e4 via enp0s3: network 172.20>
Oct  4 13:23:09 allsafe dhcpd[2292]: DHCPDISCOVER from 89:40:de:54:e0:a6 via enp0s3: network 172.20>
Oct  4 13:23:09 allsafe dhcpd[2292]: DHCPDISCOVER from 28:74:2c:73:52:1e via enp0s3: network 172.20>
Oct  4 13:23:09 allsafe dhcpd[2292]: DHCPDISCOVER from e2:07:f4:24:14:ba via enp0s3: network 172.20>
Oct  4 13:23:09 allsafe dhcpd[2292]: DHCPDISCOVER from f9:fa:cc:35:9f:6f via enp0s3: network 172.20>
Oct  4 13:23:09 allsafe dhcpd[2292]: DHCPDISCOVER from 8d:37:ba:5c:a2:09 via enp0s3: network 172.20>
Oct  4 13:23:09 allsafe dhcpd[2292]: DHCPDISCOVER from a3:15:30:08:7e:76 via enp0s3: network 172.20>
Oct  4 13:23:09 allsafe dhcpd[2292]: DHCPDISCOVER from a7:52:3f:10:43:9d via enp0s3: network 172.20>
Oct  4 13:23:09 allsafe dhcpd[2292]: DHCPDISCOVER from 52:d2:ce:40:aa:a5 via enp0s3: network 172.20>
Oct  4 13:23:09 allsafe dhcpd[2292]: DHCPDISCOVER from 50:34:da:0f:45:79 via enp0s3: network 172.20>
Oct  4 13:23:09 allsafe dhcpd[2292]: DHCPDISCOVER from a7:af:2b:7b:c9:71 via enp0s3: network 172.20>
Oct  4 13:23:09 allsafe dhcpd[2292]: DHCPDISCOVER from cc:45:06:79:2a:1e via enp0s3: network 172.20>
Oct  4 13:23:09 allsafe dhcpd[2292]: DHCPDISCOVER from 41:99:7b:39:27:fc via enp0s3: network 172.20>
Oct  4 13:23:09 allsafe dhcpd[2292]: DHCPDISCOVER from d9:fa:ff:2b:af:97 via enp0s3: network 172.20>
Oct  4 13:23:09 allsafe dhcpd[2292]: DHCPDISCOVER from d8:80:a1:08:f8:80 via enp0s3: network 172.20>
Oct  4 13:23:09 allsafe dhcpd[2292]: DHCPDISCOVER from 2a:f2:d2:1f:0b:d9 via enp0s3: network 172.20>
Oct  4 13:23:09 allsafe dhcpd[2292]: DHCPDISCOVER from 93:7c:18:45:a5:0c via enp0s3: network 172.20>
Oct  4 13:23:09 allsafe dhcpd[2292]: DHCPDISCOVER from 61:df:7b:23:ee:b7 via enp0s3: network 172.20>
Oct  4 13:23:09 allsafe dhcpd[2292]: DHCPDISCOVER from cf:e6:b3:2a:15:ee via enp0s3: network 172.20>
Oct  4 13:23:09 allsafe dhcpd[2292]: DHCPDISCOVER from 55:29:90:29:be:28 via enp0s3: network 172.20>
Oct  4 13:23:09 allsafe dhcpd[2292]: DHCPDISCOVER from 63:ee:13:2a:36:b1 via enp0s3: network 172.20>
Oct  4 13:23:09 allsafe dhcpd[2292]: DHCPDISCOVER from ab:0d:77:20:e5:27 via enp0s3: network 172.20>
Oct  4 13:23:09 allsafe dhcpd[2292]: DHCPDISCOVER from 6d:8c:cd:2a:be:ca via enp0s3: network 172.20>
Oct  4 13:23:09 allsafe dhcpd[2292]: DHCPDISCOVER from 25:f8:e2:74:ad:03 via enp0s3: network 172.20>
Oct  4 13:23:09 allsafe dhcpd[2292]: DHCPDISCOVER from 29:f0:f4:06:19:b3 via enp0s3: network 172.20>
Oct  4 13:23:09 allsafe dhcpd[2292]: DHCPDISCOVER from 04:90:f8:7c:18:32 via enp0s3: network 172.20>
Oct  4 13:23:09 allsafe dhcpd[2292]: DHCPDISCOVER from 51:7e:a2:6c:44:29 via enp0s3: network 172.20>
Oct  4 13:23:09 allsafe dhcpd[2292]: DHCPDISCOVER from 93:25:3b:6c:3f:28 via enp0s3: network 172.20>
Oct  4 13:23:09 allsafe dhcpd[2292]: DHCPDISCOVER from a2:99:c2:5e:40:ee via enp0s3: network 172.20>
Oct  4 13:23:09 allsafe dhcpd[2292]: DHCPDISCOVER from 4d:2d:1b:53:41:73 via enp0s3: network 172.20>
Oct  4 13:23:09 allsafe dhcpd[2292]: DHCPDISCOVER from fa:c1:af:74:db:39 via enp0s3: network 172.20>

^G Get Help   ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify    ^C Cur Pos    M-U Undo
^X Exit       ^R Read File  ^\ Replace    ^U Paste Text ^T To Spell   ^_ Go To Line M-E Redo
```

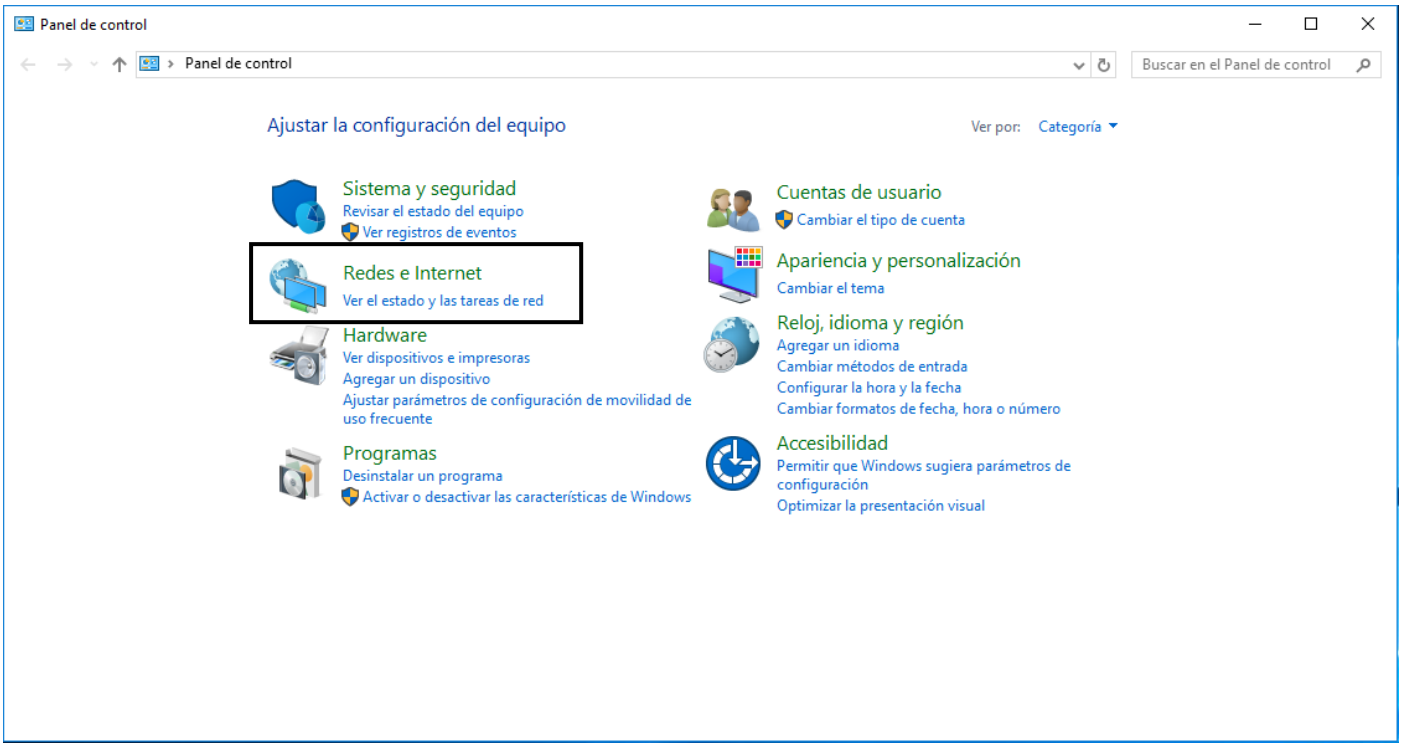
5. REALIZA LO MISMO QUE EN LOS APARTADOS ANTERIORES PERO ESTA VEZ CON UNA MÁQUINA WINDOWS SERVER. DOCUMENTA TODOS LOS PASOS REALIZADOS.

Para este punto he preparado otra red NAT con la siguiente configuración:

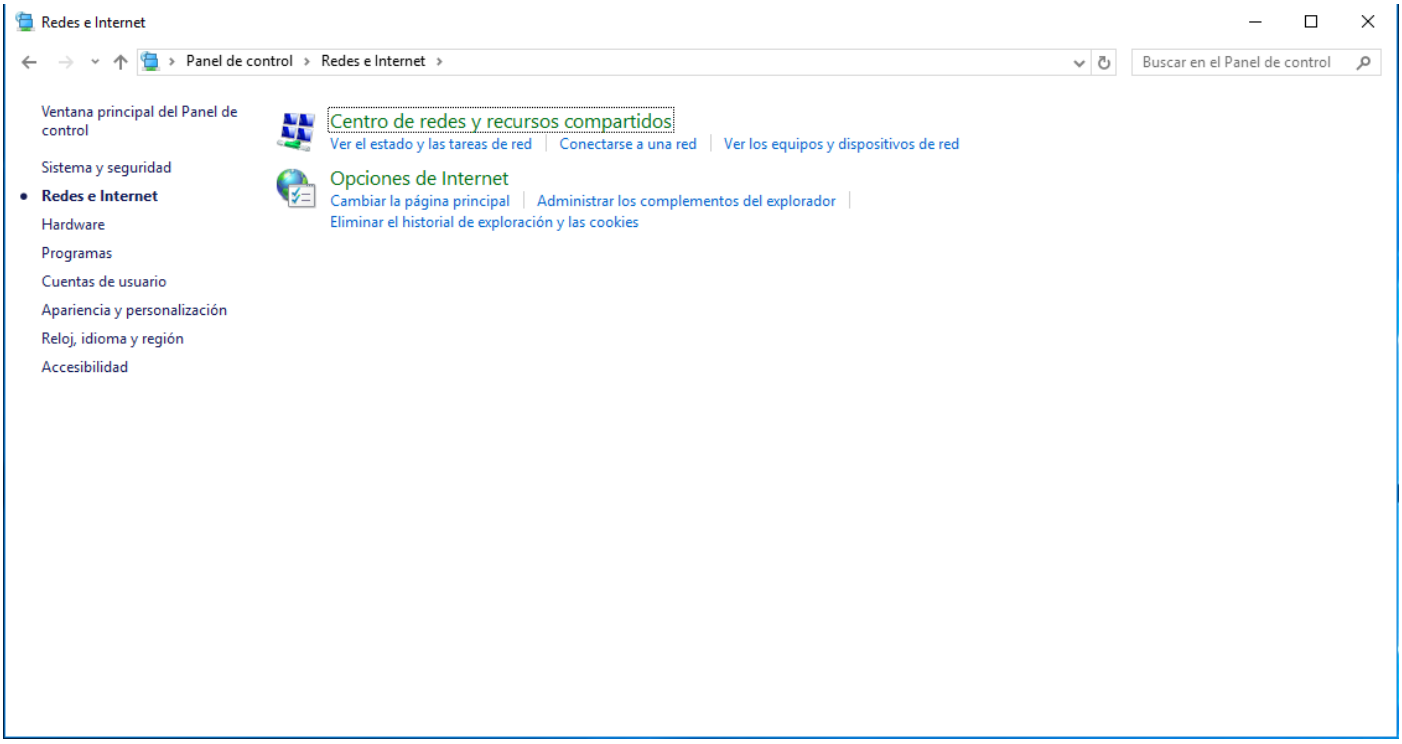


Configuramos primero la IP estática del servidor. Para ello nos dirigimos a Inicio >" Panel de control"

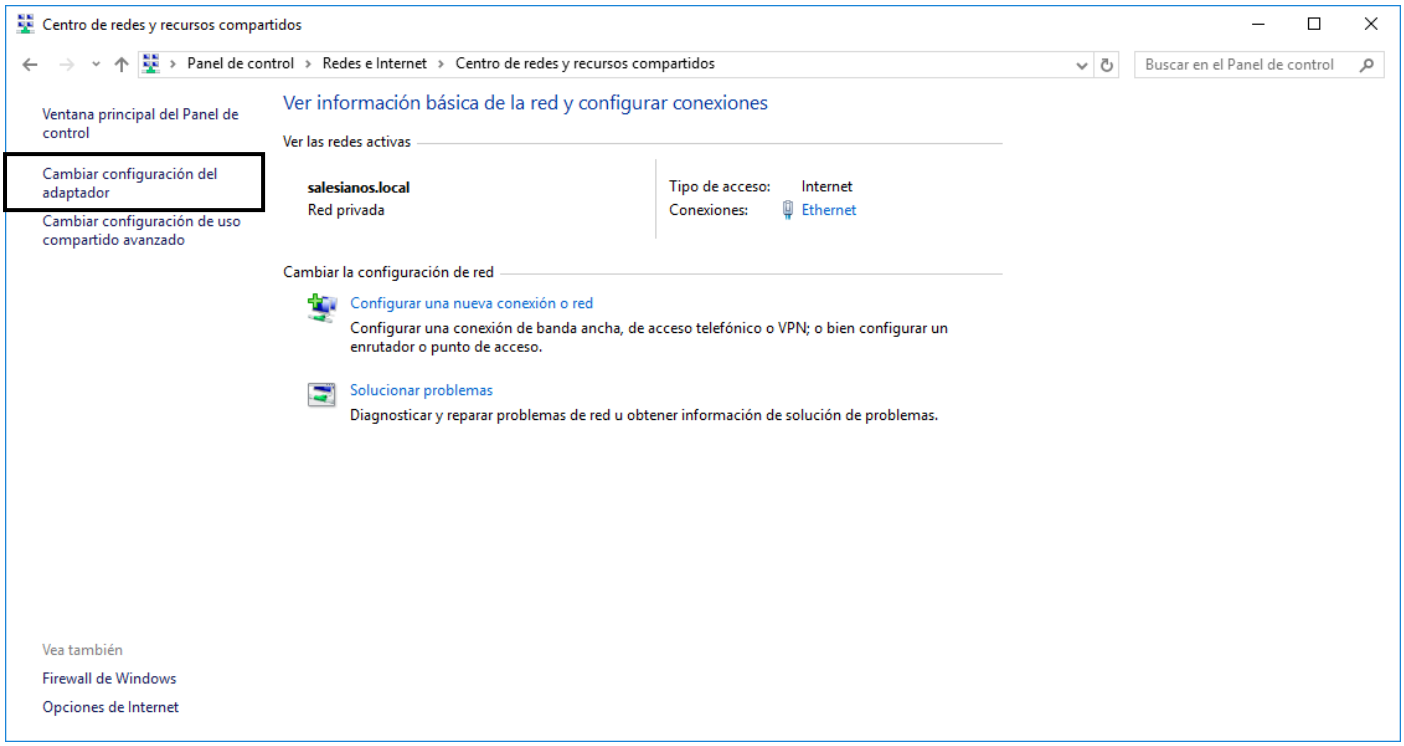
Seleccionamos "Redes e Internet"



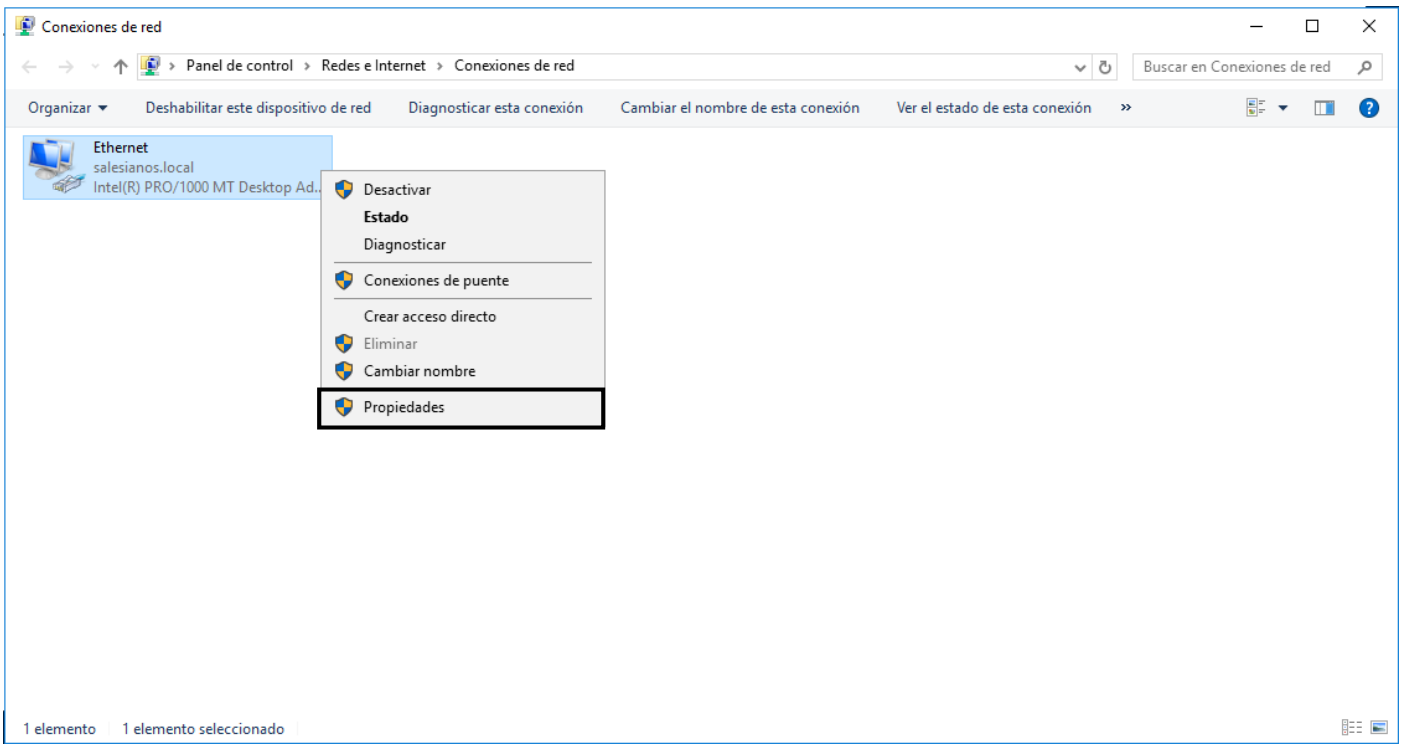
Seleccionamos "Centro de redes y recursos compartidos"



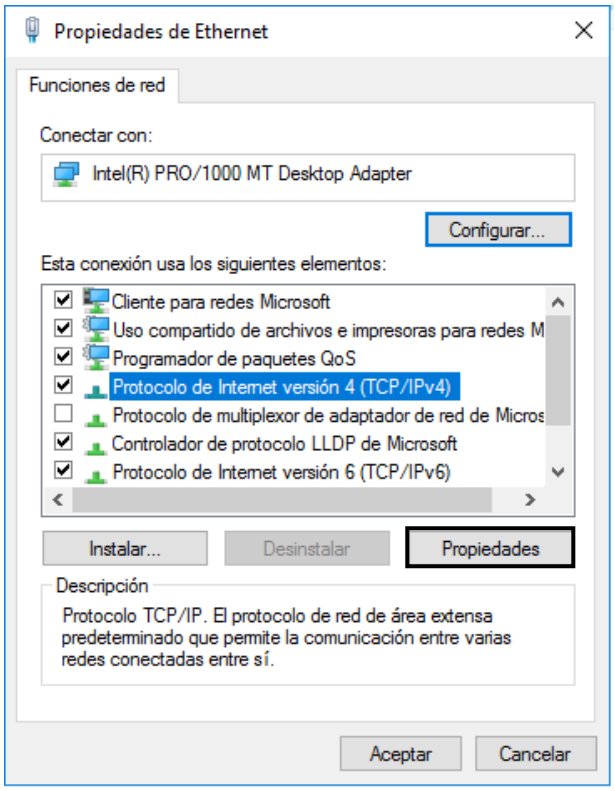
Seleccionamos “Cambiar configuración del adaptador”



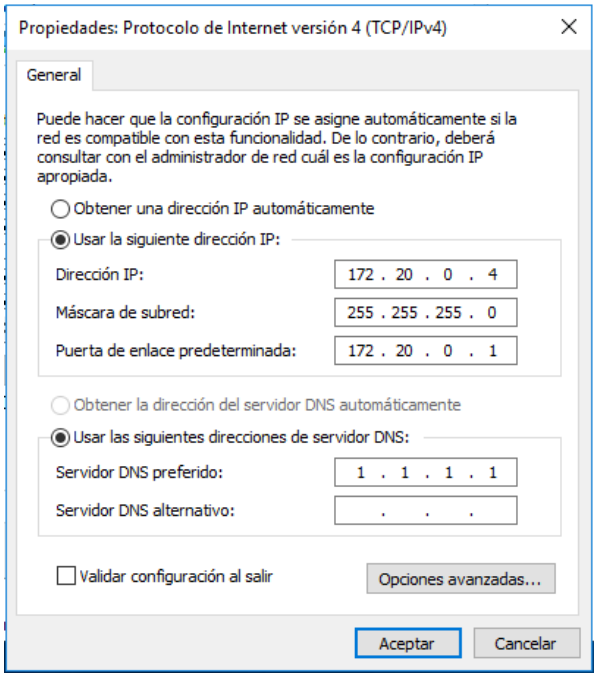
Seleccionamos la interfaz, presionamos el botón secundario del ratón y seleccionamos “Propiedades”



Seleccionamos “Protocolo de Internet version 4 (TCP/IPv4)” y “Propiedades”

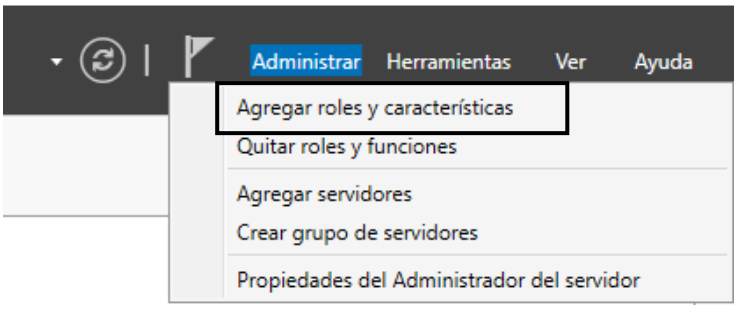


Configuramos las siguientes opciones, yo introducire los mismos parametros que para el servidor Ubuntu ya que estan en redes NAT distintas.

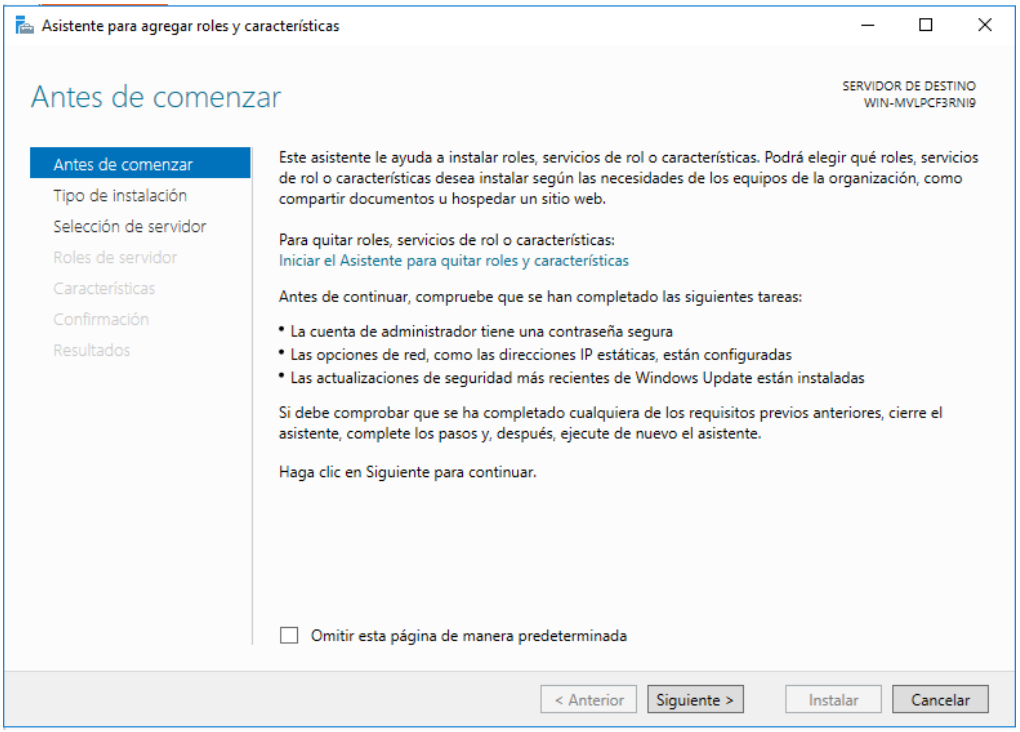


INSTALACIÓN DEL SERVICIO DHCP

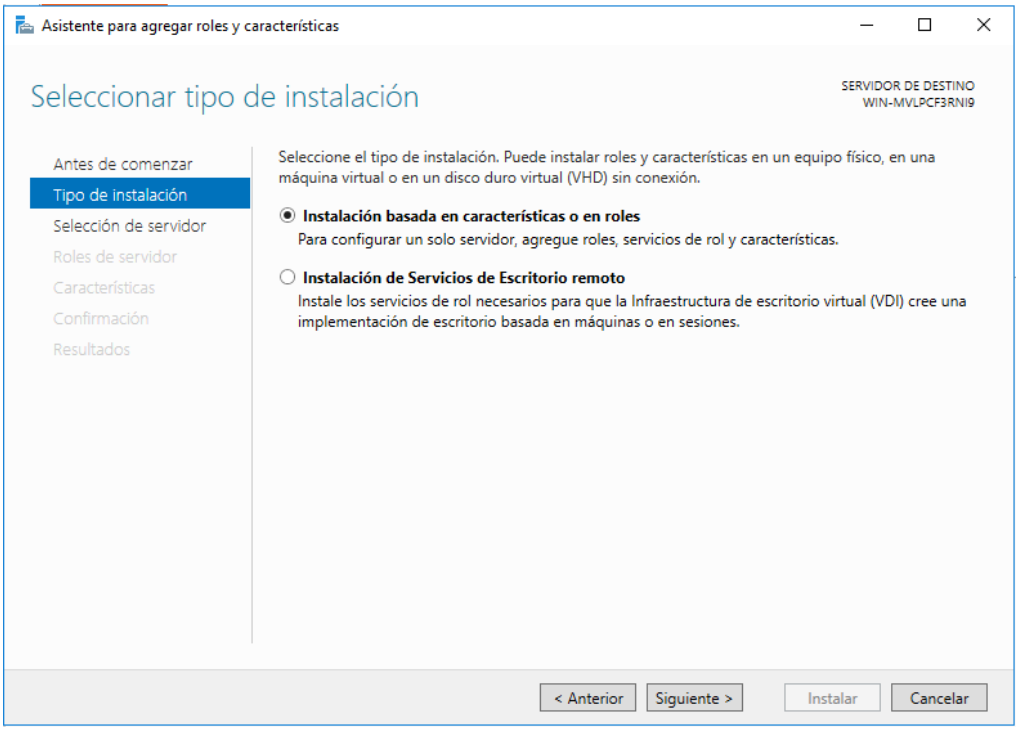
En "Administrador del servidor" seleccionamos "Administrar" y "Agregar roles y características"



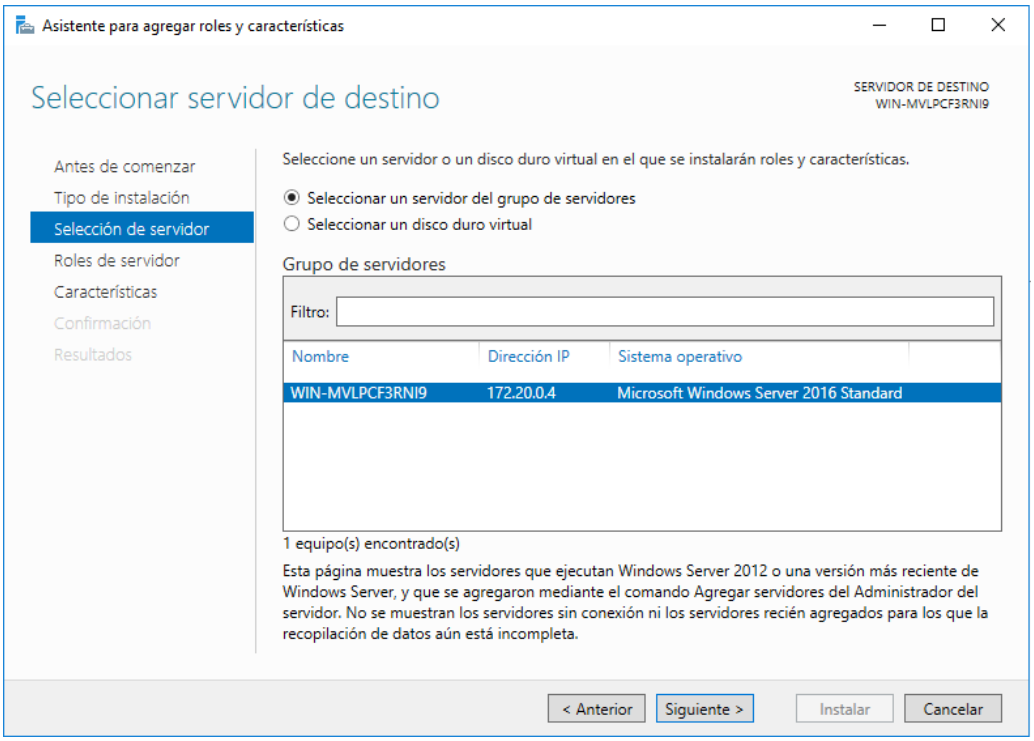
Se iniciará el asistente para agregar roles y características, seleccionamos "Siguiente >"



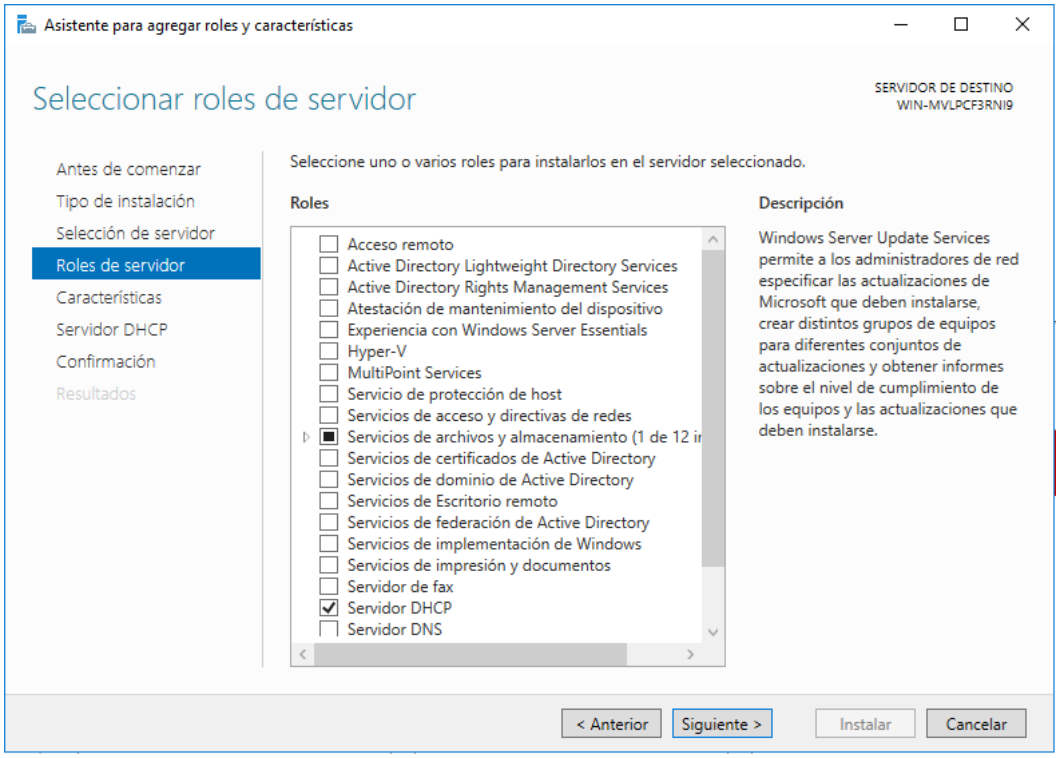
Seleccionamos "Instalación basada en características o en roles" y "Siguiente >"



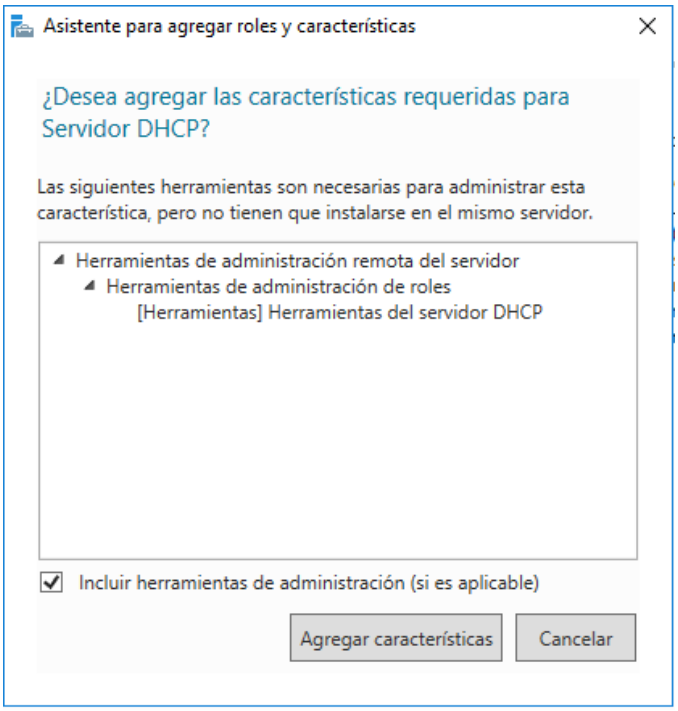
Seleccionamos “Siguiente >” ya que por defecto ya nos escoge nuestro servidor



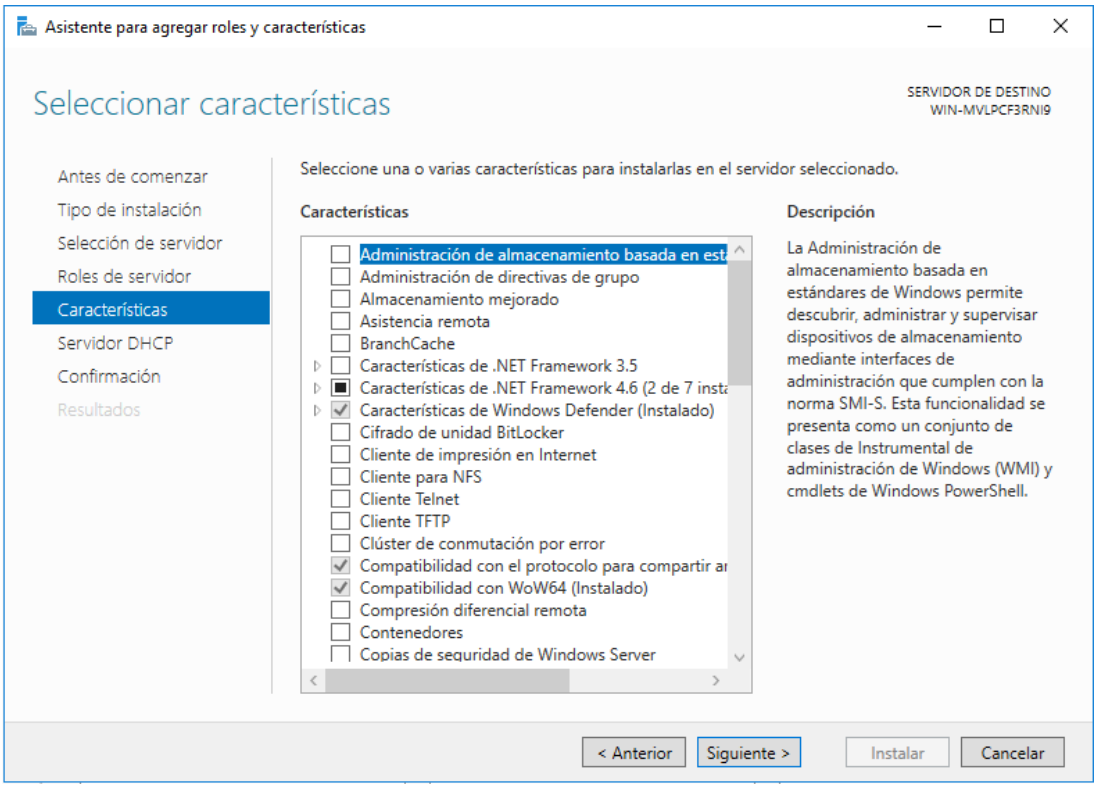
Selecciona “Servidor DHCP” y “Siguiente >”



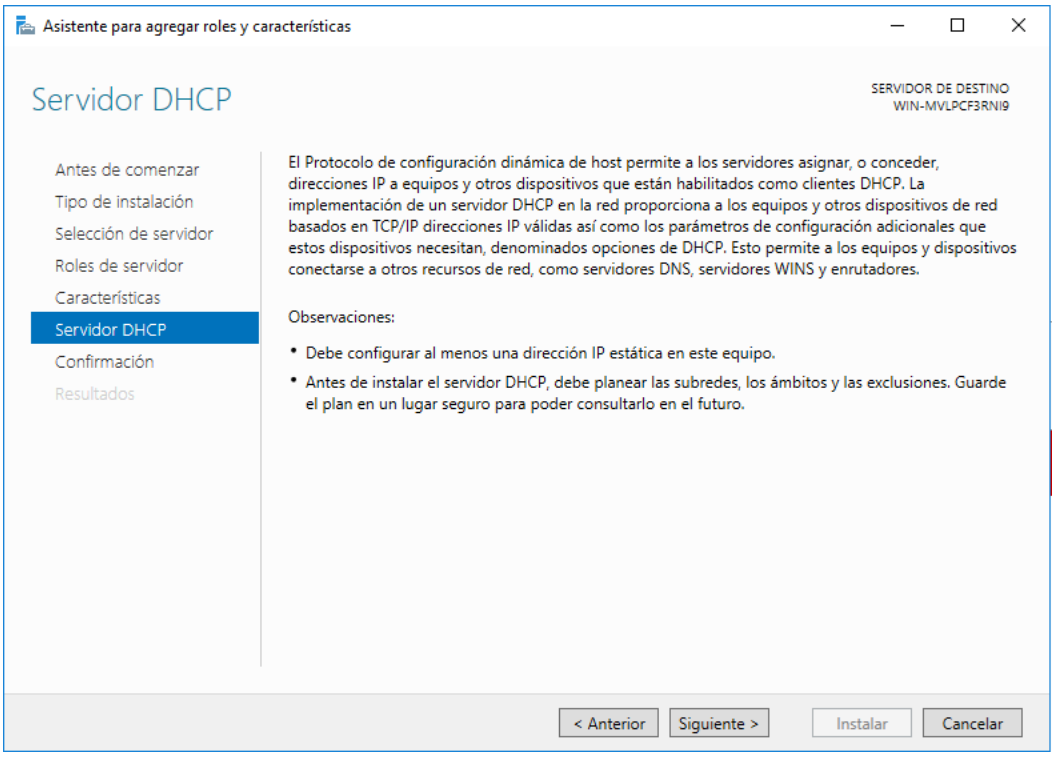
Seleccionamos “Agregar características”



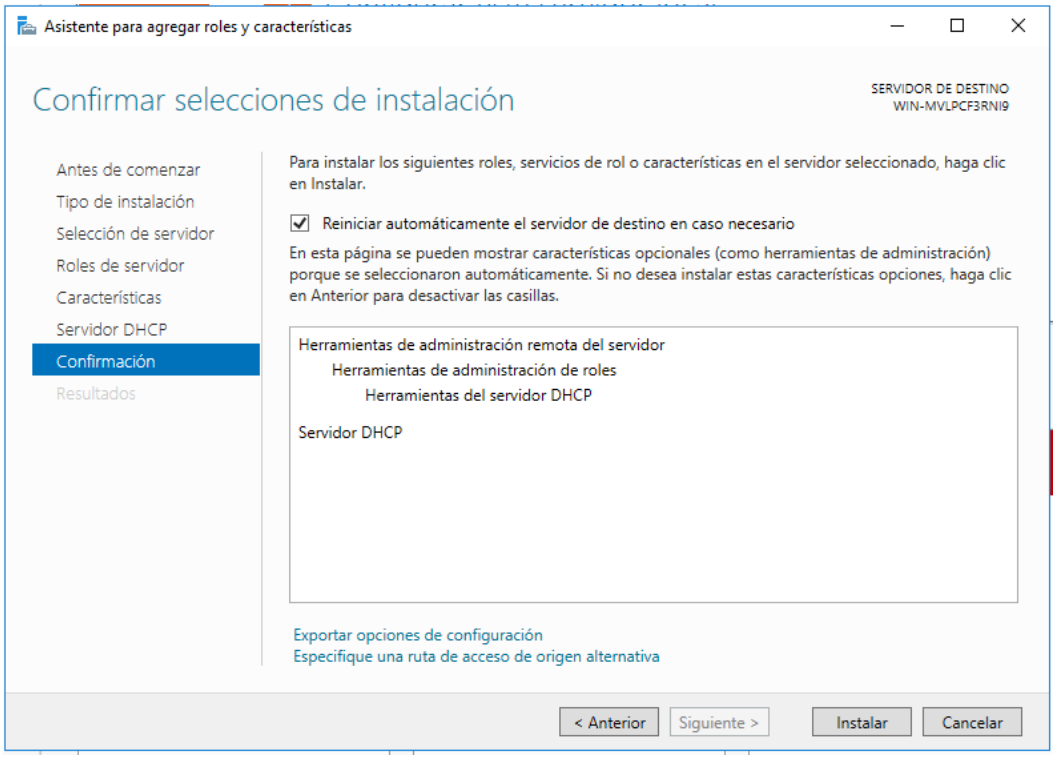
Seleccionamos “Siguiente >”



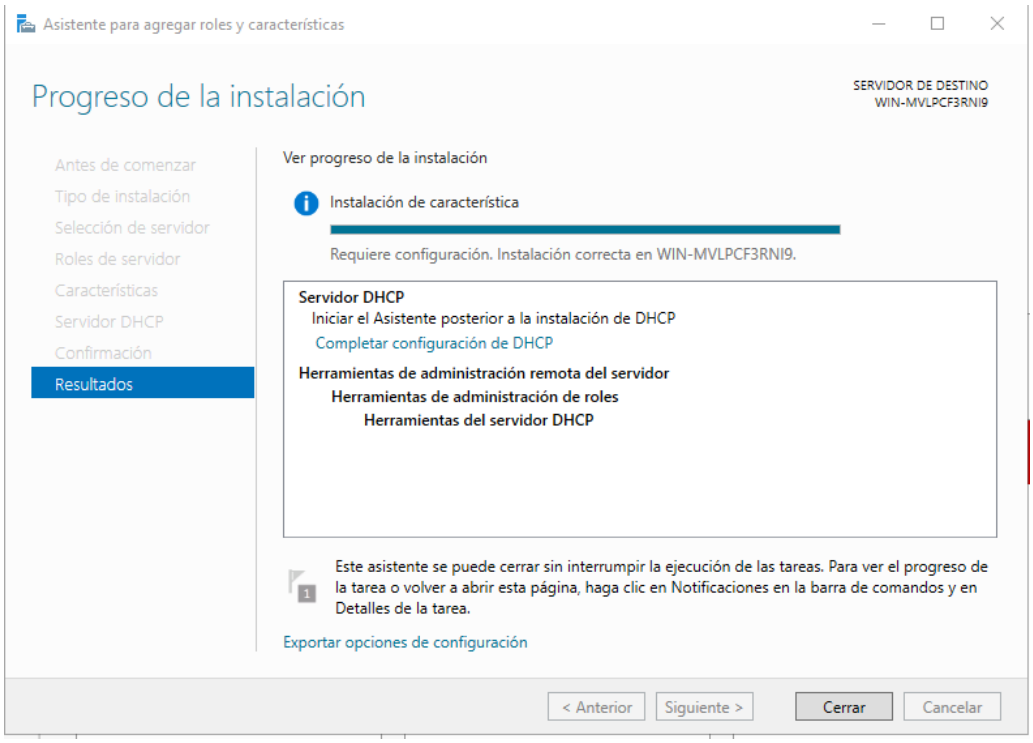
Seleccionamos “Siguiente >”



Seleccionamos “Reiniciar automaticamente el servidor de destino en caso necesario” e “Instalar”

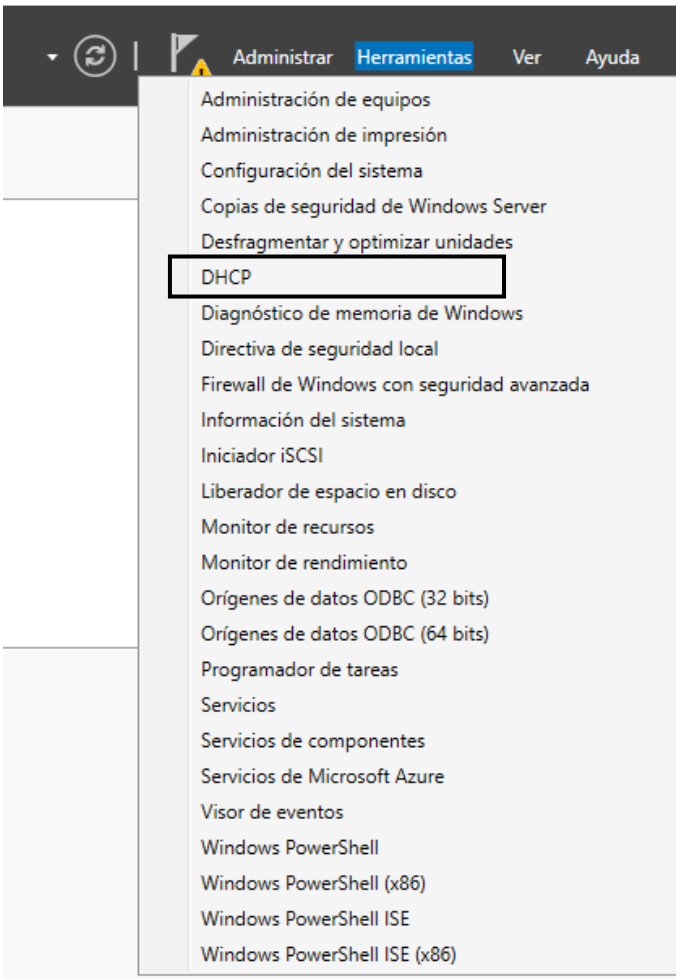


Cuando la instalacion finalice seleccionamos “Cerrar”

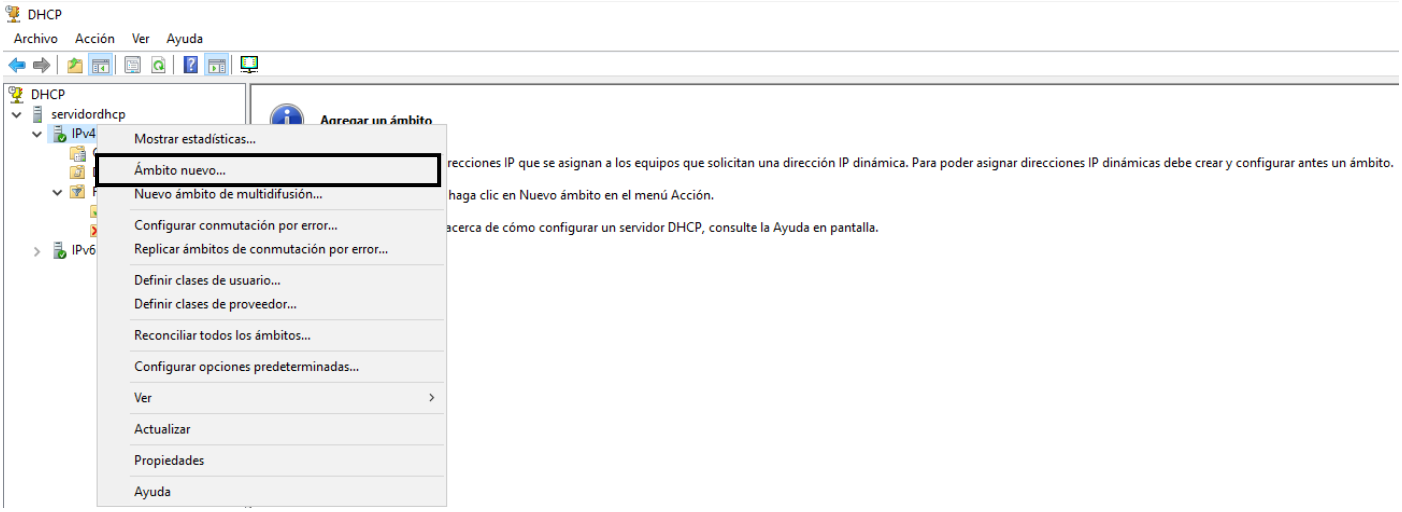


CONFIGURACIÓN DEL SERVICIO DHCP

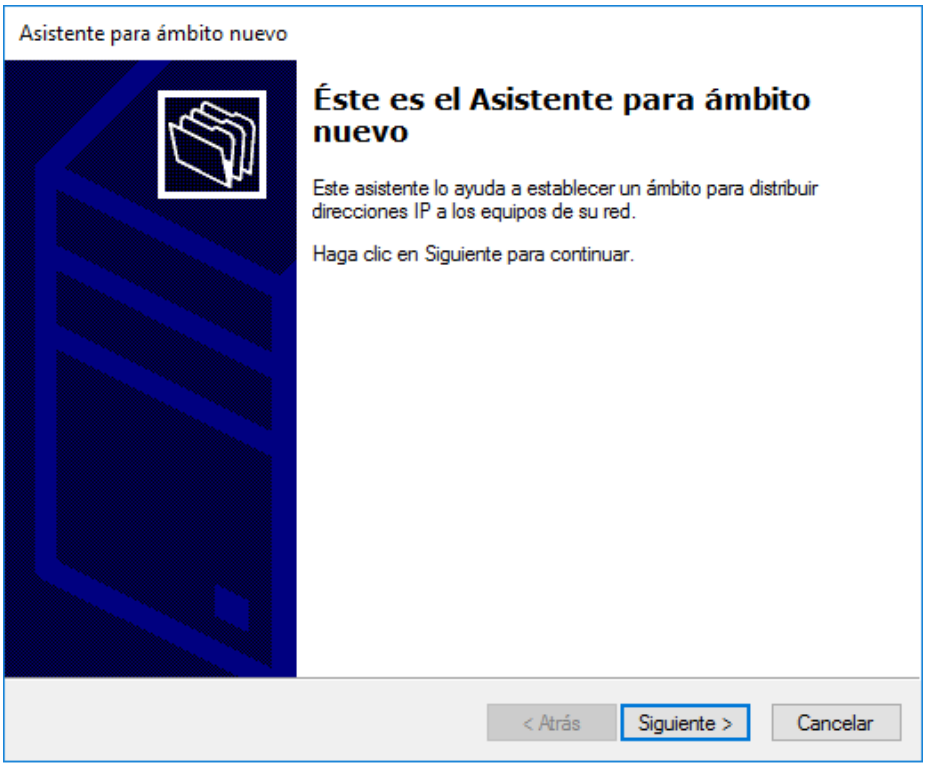
Seleccionamos “Herramientas” > “DHCP”



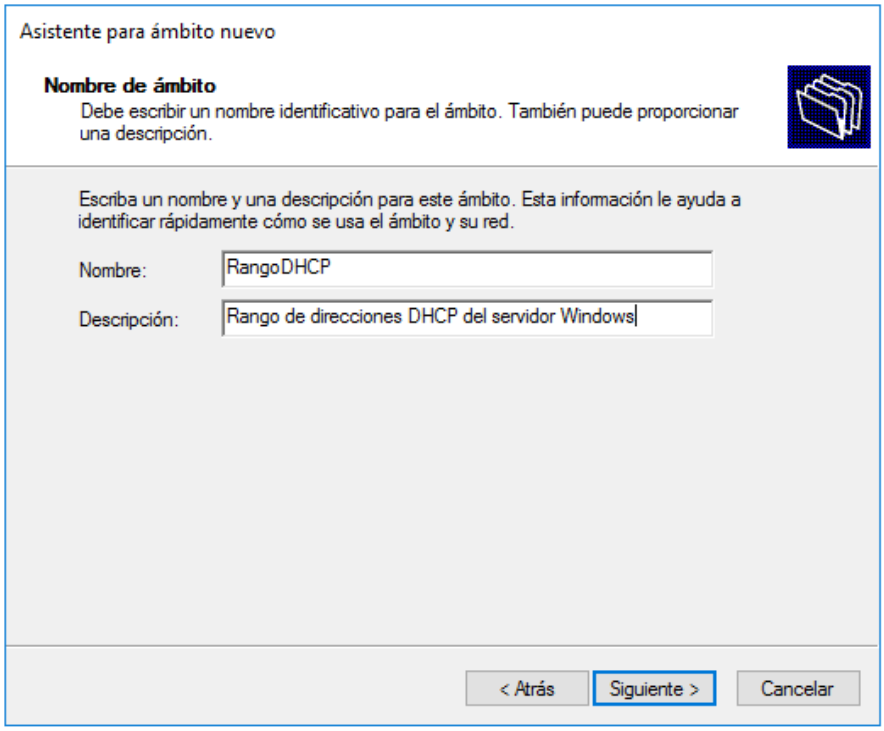
Se abrirá una ventana nueva, en la columna de la izquierda seleccionamos el nombre de nuestro servidor y se desplegará dos opciones, una de ellas "IPv4" presionamos el botón secundario del ratón y seleccionamos "Ámbito nuevo"



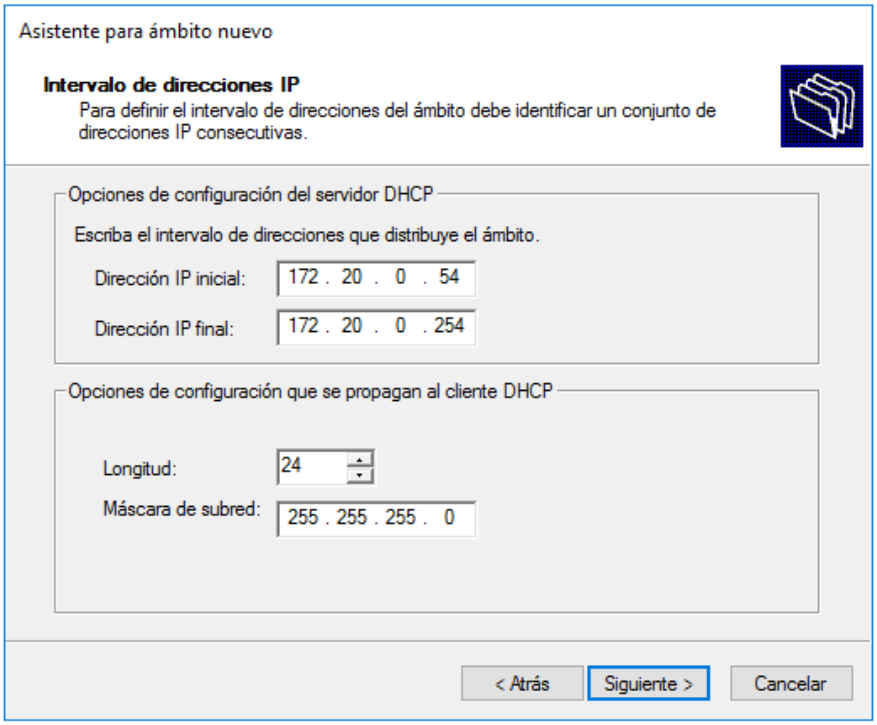
Se iniciara el asistente para ambito nuevo, seleccionamos "Siguiente >"



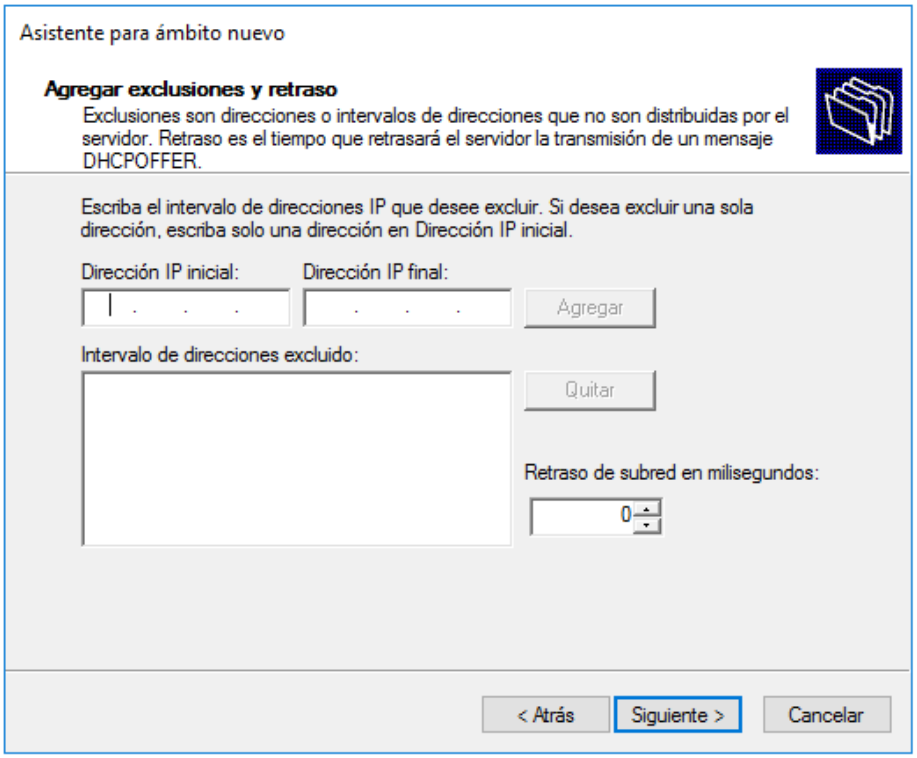
Introducimos los datos deseados y seleccionamos “Siguiente >”



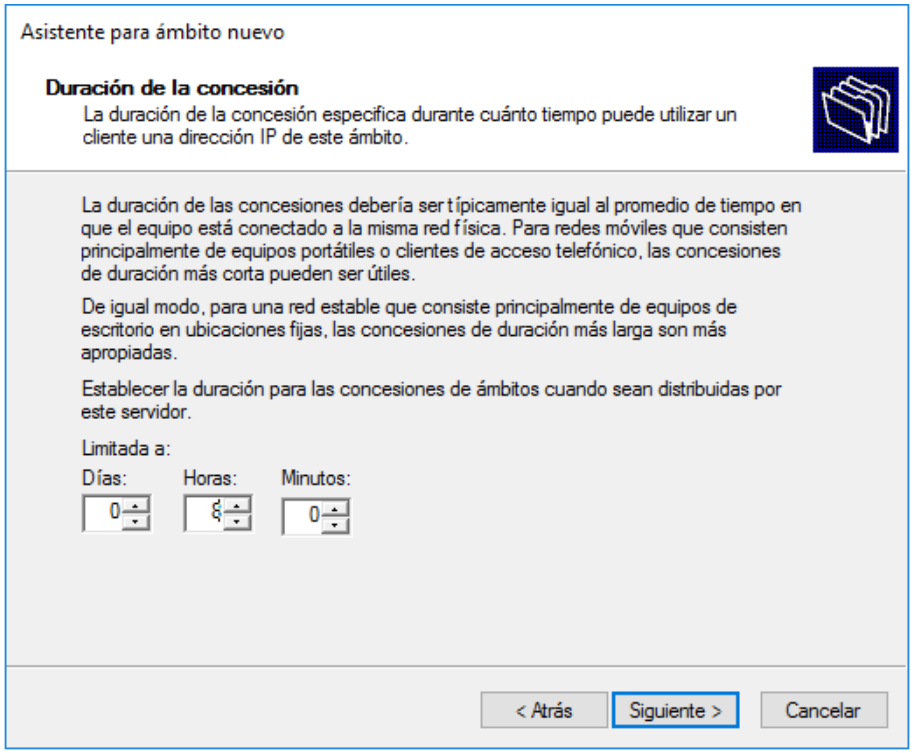
Introducimos el intervalo de direcciones IP que vamos a ofrecer y seleccionamos “Siguiente >”



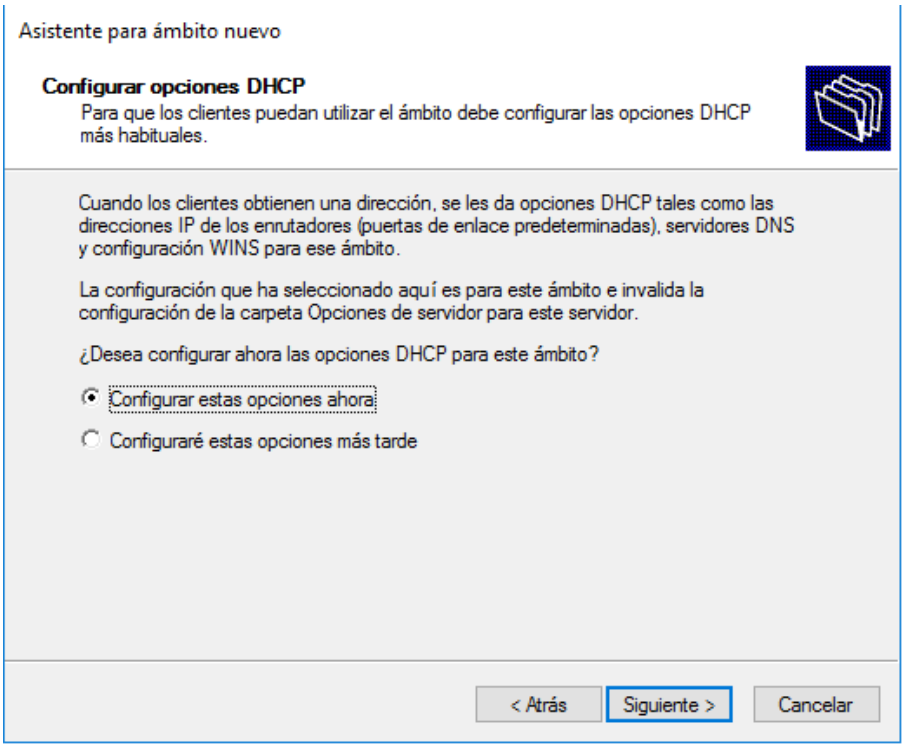
En este paso no introducire ningun dato ya que no quiero excluir direcciones y seleccionamos “Siguiente>”



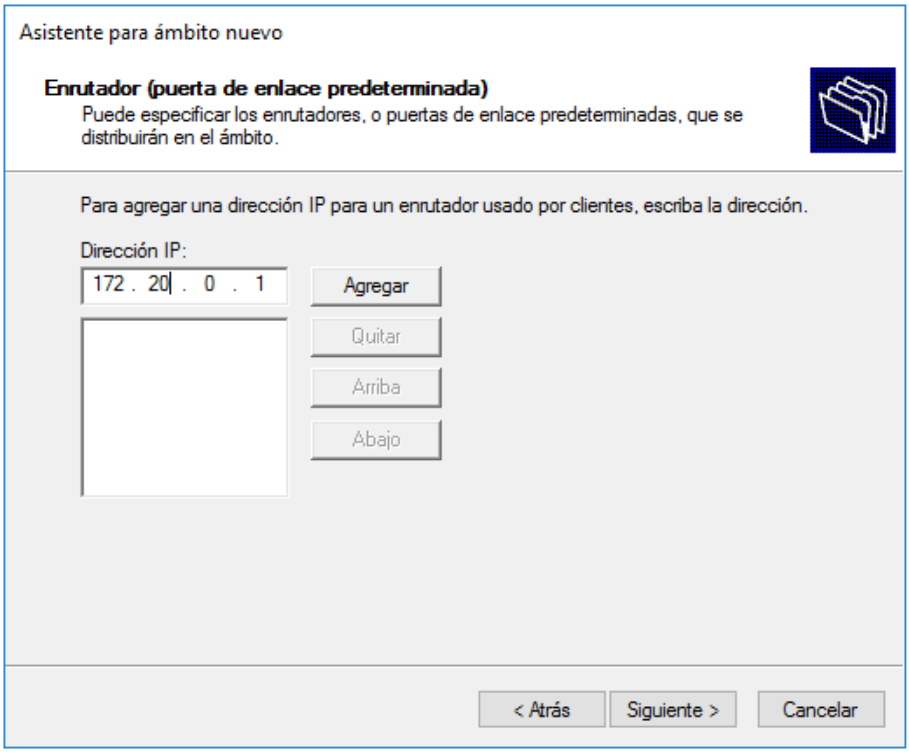
La duracion de la concesion yo la he establecido en 8 horas y seleccionamos “Siguiente >”



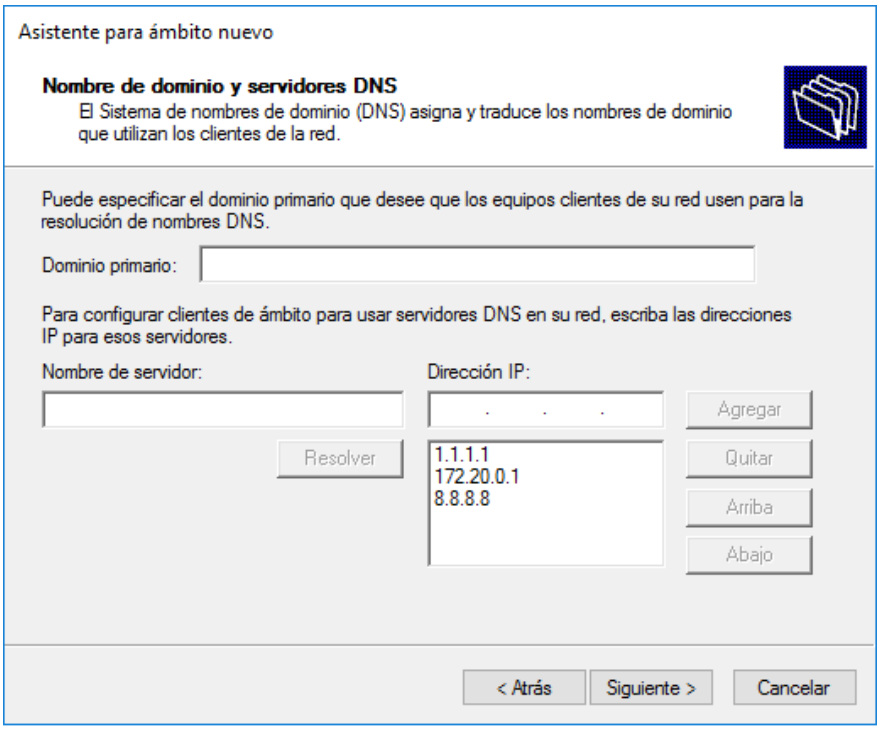
Selecciones "Configurar estas opciones ahora" y "Siguiente >"



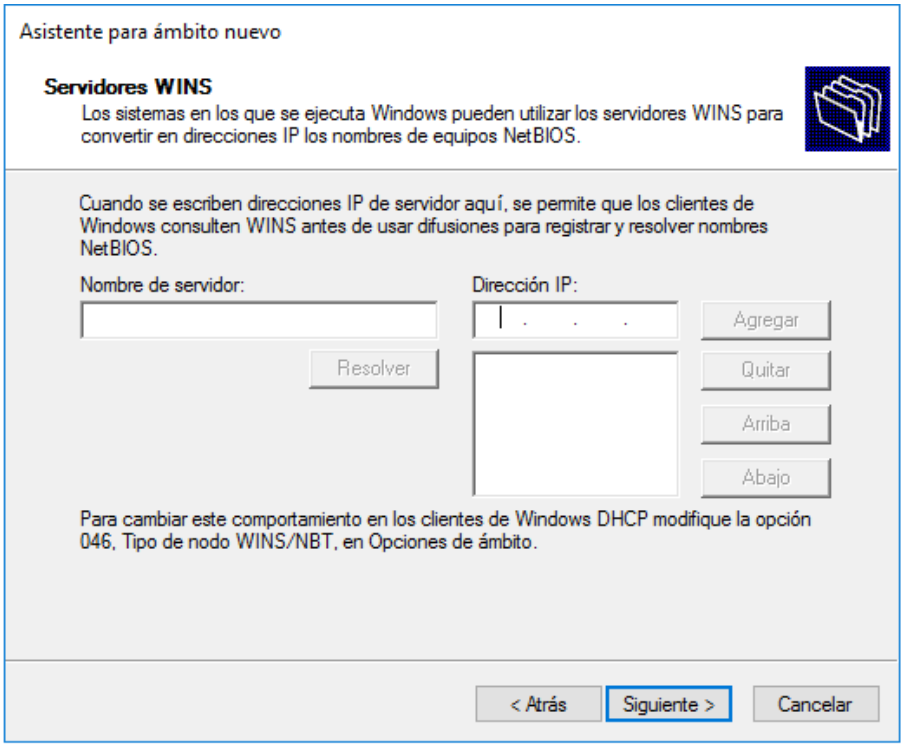
Introducimos nuestra puerta de enlace, en mi caso "172.20.0.1" y seleccionamos "Agregar" y "Siguiente>"



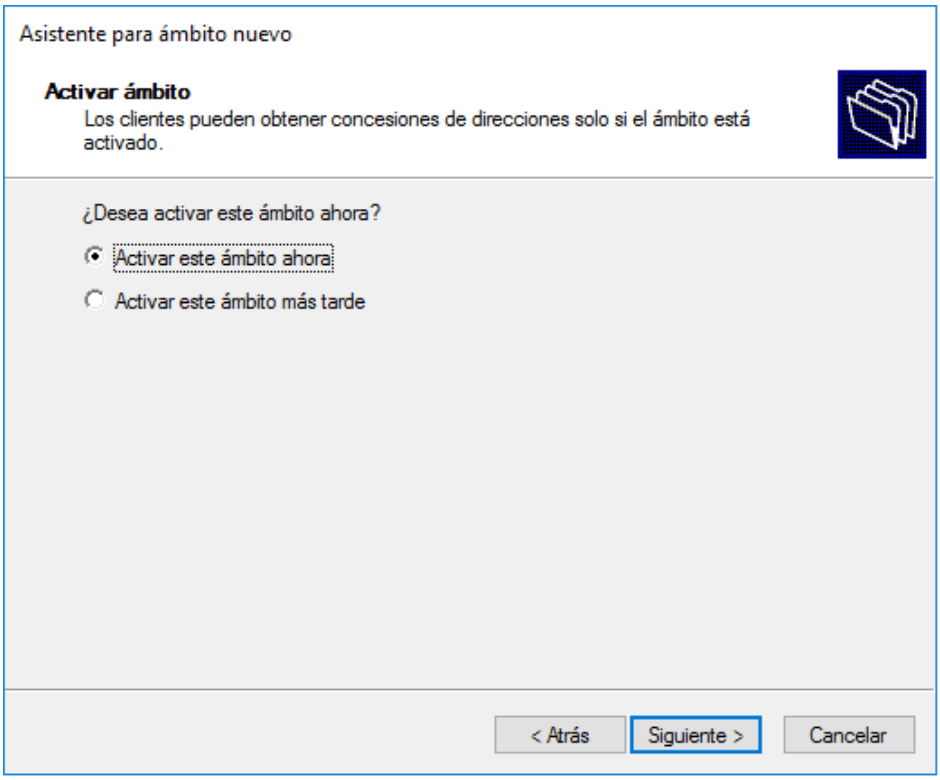
Agregamos los servidores DNS y seleccionamos "Siguiente >"



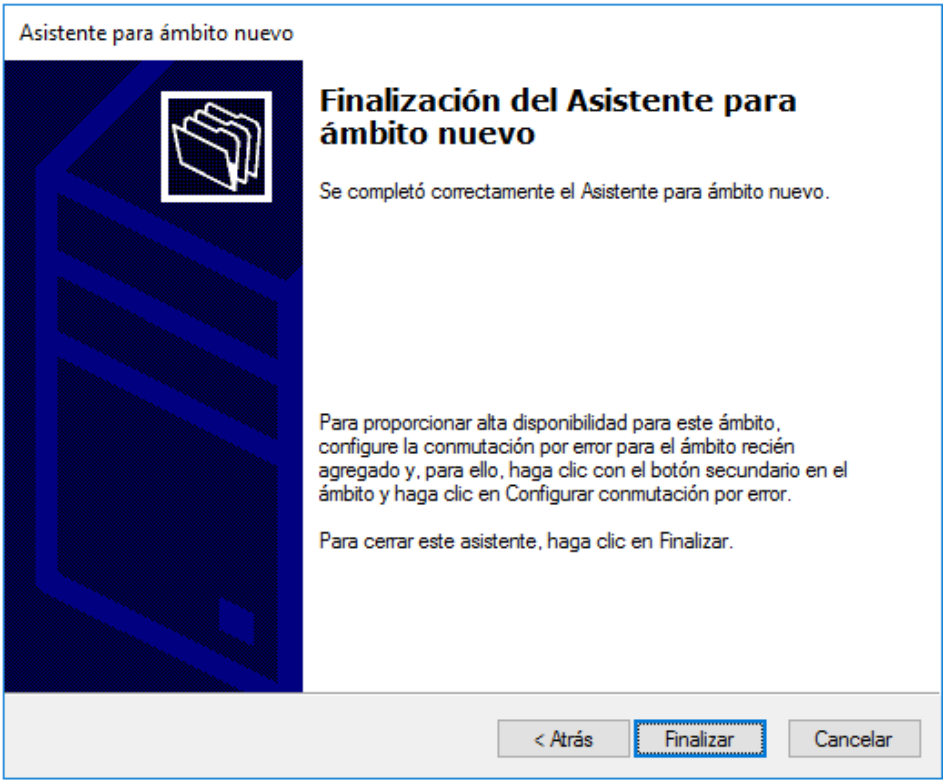
Aquí no introduciré ningún dato por lo que seleccionamos "Siguiente >"



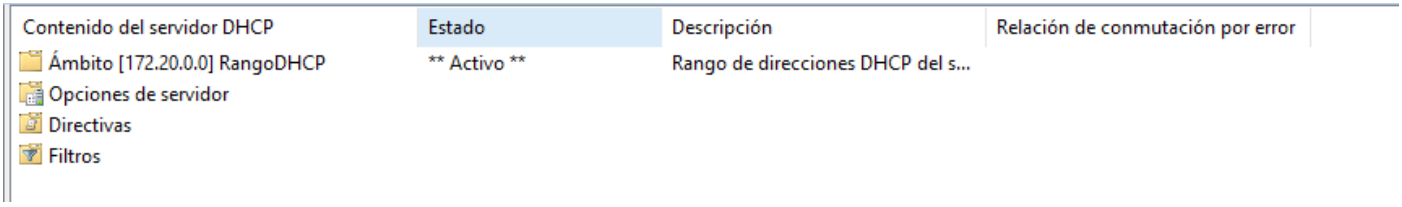
Seleccionamos la opción "Activar este ámbito ahora" y seleccionamos "Siguiente >"



Para terminar, seleccionamos "Finalizar"



Este es el aspecto final:



6. LA EMPRESA 4CK.ES CONTRATA NUESTROS SERVICIOS PARA COMPROBAR LA SEGURIDAD DE LA RED INTERNA DE LA ORGANIZACIÓN. UNA PRUEBA FUNDAMENTAL EN COLOCAR UN DHCP ROGUE DENTRO DE LOS SEGMENTOS DE RED DONDE SE REALIZAN LAS PRUEBAS PARA REALIZAR UN ATAQUE MAN/WOMAN IN THE MIDDLE. CONFIGURA UN SERVIDOR DHCP MALICIOSO QUE CAPTURE LAS CLAVES DE ACCESO CUANDO UN USUARIO DE LA ORGANIZACIÓN QUIERA INGRESAR A LA INTRANET HTTP://WWW.ECO.UVA.ES/RELINT/INDEX.PHP/INTRANET. DOCUMENTA TODAS LAS PRUEBAS Y PASOS NECESARIOS PARA OBTENER LAS CREDENCIALES DE ACCESO DEL USUARIO. EN EL SEGMENTO DE RED DONDE SE COLOQUE EL DHCP ROGUE EXISTIRÁ UN SERVIDOR DHCP LÍCITO PERTENECIENTE A LA ORGANIZACIÓN A AUDITAR.

Clonamos el servidor Ubuntu DHCP y modificamos el fichero "/etc/netplan/00-installer-config.yaml" cambiando la dirección IP:

```
  GNU nano 4.8                    /etc/netplan/00-installer-config.yaml                    Modified
# This is the network config written by 'subiquity'
network:
  ethernets:
    enp0s3:
      addresses:
      - 172.20.0.5/24
      gateway4: 172.20.0.1
      nameservers:
        addresses:
        - 172.20.0.1
        - 1.1.1.1
        - 8.8.8.8
  version: 2

                                    [ Read 13 lines ]
^G Get Help    ^O Write Out   ^W Where Is    ^K Cut Text    ^J Justify     ^C Cur Pos     M-U Undo
^X Exit        ^R Read File   ^\ Replace     ^U Paste Text  ^T To Spell    ^_ Go To Line  M-E Redo
```

Modificamos el fichero "/etc/dhcp/dhcpd.conf" cambiando el pool de direcciones IPs

```
  GNU nano 4.8                    /etc/dhcp/dhcpd.conf

# The ddns-updates-style parameter controls whether or not the server will
# attempt to do a DNS update when a lease is confirmed. We default to the
# behavior of the version 2 packages ('none', since DHCP v2 didn't
# have support for DDNS.)
ddns-update-style none;

# If this DHCP server is the official DHCP server for the local
# network, the authoritative directive should be uncommented.
#authoritative;

# Use this to send dhcp log messages to a different log file (you also
# have to hack syslog.conf to complete the redirection).
#log-facility local7;

# No service will be given on this subnet, but declaring it helps the
# DHCP server to understand the network topology.

#subnet 10.152.187.0 netmask 255.255.255.0 {
#}

# This is a very basic subnet declaration.

subnet 172.20.0.0 netmask 255.255.255.0 {
  range 172.20.0.10 172.20.0.53;
  option routers 172.20.0.1;
  option domain-name-servers 1.1.1.1,8.8.8.8,192.168.100.100,192.168.0.61;
  default-lease-time 600;
  max-lease-time 28800;
}

# This declaration allows BOOTP clients to get dynamic addresses,
# which we don't really recommend.

^G Get Help   ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify    ^C Cur Pos    M-U Undo
^X Exit       ^R Read File  ^\ Replace    ^U Paste Text ^T To Spell   ^_ Go To Line M-E Redo
```

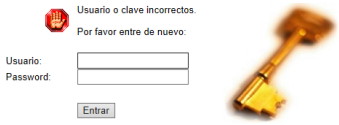
COMPROBACIÓN DEL FUNCIONAMIENTO

He introducido una maquina Windows 10 con una configuración DHCP y el servidor funciona correctamente:

```
C:\Users\m a r t h a>ipconfig

Configuración IP de Windows


Adaptador de Ethernet Ethernet:

   Sufijo DNS específico para la conexión. . : example.org
   Vínculo: dirección IPv6 local. . . : fe80::448b:62f7:757c:fd4%7
   Dirección IPv4. . . . . . . . . . . . . . : 172.20.0.10
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . : 172.20.0.1

C:\Users\m a r t h a>ipconfig /all

Configuración IP de Windows

   Nombre de host. . . . . . . . . : DESKTOP-L40J8CM
   Sufijo DNS principal  . . . . . :
   Tipo de nodo. . . . . . . . . . : híbrido
   Enrutamiento IP habilitado. . . : no
   Proxy WINS habilitado . . . . . : no
   Lista de búsqueda de sufijos DNS: example.org

Adaptador de Ethernet Ethernet:

   Sufijo DNS específico para la conexión. . : example.org
   Descripción . . . . . . . . . . . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
   Dirección física. . . . . . . . . . . . . : 08-00-27-75-4F-7C
   DHCP habilitado . . . . . . . . . . . . . : sí
   Configuración automática habilitada . . . : sí
   Vínculo: dirección IPv6 local. . . : fe80::448b:62f7:757c:fd4%7(Preferido)
   Dirección IPv4. . . . . . . . . . . . . . : 172.20.0.10(Preferido)
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Concesión obtenida. . . . . . . . . . . . : jueves, 8 de octubre de 2020 9:04:12
   La concesión expira . . . . . . . . . . . : jueves, 8 de octubre de 2020 9:14:11
   Puerta de enlace predeterminada . . . . . : 172.20.0.1
   Servidor DHCP . . . . . . . . . . . . . . : 172.20.0.5
   IAID DHCPv6 . . . . . . . . . . . . . . . : 101187623
   DUID de cliente DHCPv6. . . . . . . . . . : 00-01-00-01-27-01-3E-38-08-00-27-75-4F-7C
   Servidores DNS. . . . . . . . . . . . . . : 192.168.100.100
                                               192.168.0.61
   NetBIOS sobre TCP/IP. . . . . . . . . . . : habilitado

C:\Users\m a r t h a>
```

ATAQUE MAN/WOMAN IN THE MIDDLE

Con el servidor rogue en funcionamiento, la victima accede a la página web http://www.eco.uva.es/relint/index.php/intranet



Con una máquina Kali, introducida en el servidor rogue, ponemos en funcionamiento un analizador de tráfico para poder así capturar los datos de sesión de la víctima.

Aplicamos el siguiente filtro: "ipdr 172.20.0.10" (también podríamos haber usado un filtro especificando HTTP), analizamos las peticiones que se ha realizado por HTTP y cómo podemos ver ya tenemos los datos de sesión de la víctima.