



UNIVERSITAT
POLITÀCNICA
DE VALÈNCIA



Escola Tècnica
Superior d'Enginyeria
Informàtica

Escola Tècnica Superior d'Enginyeria Informàtica
Universitat Politècnica de València

Túnel EoIP

Trabajo Redes Corporativas

Grado en Ingeniería Informática

Autores: Adrián Carrillo y Vicente Arnau

Router: 17

2019-2020

Resumen

En esta práctica de laboratorio vamos a ver el funcionamiento del protocolo EoIP, aprender a configurarlo y comprobar como trabaja. Particularmente nos apoyamos en el firmware DD-WRT para configurar ambos routers y conectarlos aunque estén en distintas redes o localizaciones. Al contrario que usando una VPN, todo el tráfico irá de una red a otra marcando el camino que nosotros queramos y dándole salida a internet por cualquier router.

Palabras clave: protocolo, EoIP, router, VPN, red.

Abstract

In this lab practice we will see the performance of EoIP protocol, know how to configure it and check how it works. Particularly we are supported by DD-WRT firmware to configure both routers and connect them between them although they be in different networks or locations. Unlike using a VPN connection, all the traffic will go from one network to the other one doing the way that we want and giving it an internet output by any of the routers.

Keywords: protocol, EoIP, router, VPN, network.

Tabla de contenidos

1. Introducción	7
2. Configuración de las máquinas.....	9
3. Configuración de los interfaces	13
DD-WRT	13
Clientes	17
4. Configuración de los routers	19
5. Funcionamiento del túnel.....	23
6. Para ampliar.....	25
7. Conclusiones	27
Bibliografía	29

Tabla de ilustraciones

Ilustración 1.....	10
Ilustración 2.....	10
Ilustración 3.....	11
Ilustración 4.....	12
Ilustración 5.....	14
Ilustración 6.....	14
Ilustración 7.....	15
Ilustración 8	16
Ilustración 9.....	16
Ilustración 10.....	17
Ilustración 11	18
Ilustración 12.....	18
Ilustración 13.....	19
Ilustración 14	20
Ilustración 15.....	21
Ilustración 16.....	21
Ilustración 17.....	22
Ilustración 18.....	22
Ilustración 19.....	23
Ilustración 20	23

1. Introducción

Hoy en día se ponen a nuestra disposición multitud de herramientas a la hora de poder configurar redes, desde nuestras preferencias personales, a su modo de funcionamiento, los servicios que queramos utilizar hasta los protocolos en concreto que vamos a emplear. En este caso queremos conectar dos subredes para que puedan trabajar de manera conjunta sin tener que estar conectadas de manera física una al lado de otra. A diario podemos hacer esto en la UPV gracias a la VPN que se ofrece tanto a estudiantes como a personal, permitiendo que el tráfico TCP/IP que generamos desde nuestra máquina vaya a la UPV y desde ahí salga a internet. Pero en este caso queremos que todo el tráfico vaya a una red y luego salga a internet. Esto lo podemos conseguir gracias a un protocolo conocido como Ethernet Over IP.

EoIP es un protocolo creado por Mikrotik hace más de 10 años que crea una interfaz de conexión entre dos routers como si un cable los uniera. Como si de un túnel se tratara, todo el tráfico de una red puede ser redirigido a otra para que desde allí salga a internet. Además de estas funciones podemos compartir servidores DHCP, que por ejemplo permitirían a una empresa con sedes en distintos edificios compartir parte de las direcciones de los equipos de sus trabajadores.

En nuestro caso disponemos de 4 máquinas virtuales dentro de nuestro ordenador de laboratorio. Dos de ellas actúan como ordenadores comunes también llamados clientes, mientras que las otras dos son routers que tenemos que configurar para que se comuniquen entre ellos.

2. Configuración de las máquinas

La estructura de red que se nos solicita en esta práctica necesita salir a internet por dos caminos distintos para atender a dos clientes distintos. Cada uno de estos dos caminos los dirigirá uno de ambos routers, tal como indica la figura.

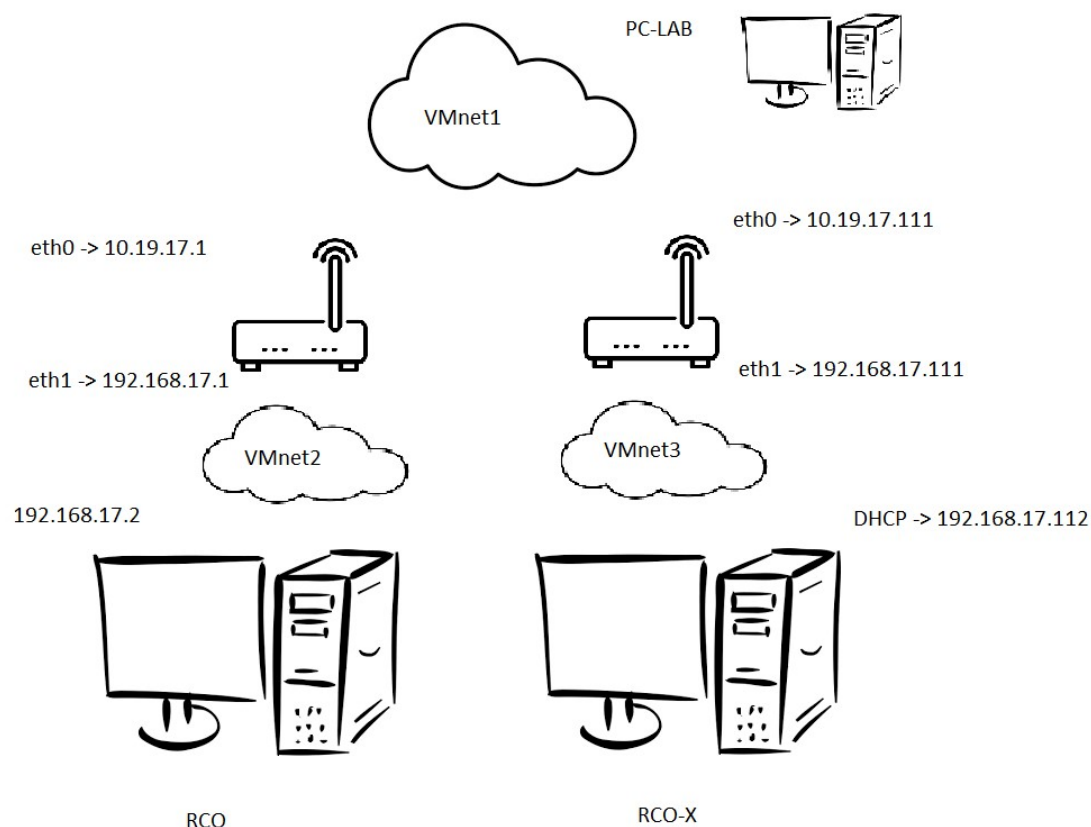


Figura 1

Para ello, y como el tráfico pasará inamoviblemente por el ordenador de laboratorio (de ahora en adelante, *PC*), vamos a configurar el adaptador de red *VMnet 1* del PC para que encaje con la IP de la figura, en nuestro caso 10.19.17.18.

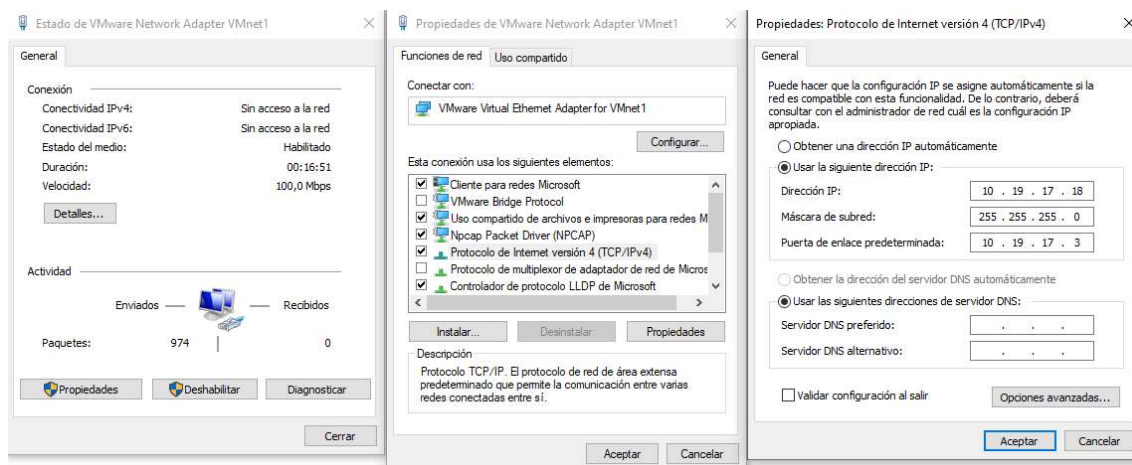


Ilustración 1

En las máquinas virtuales no es necesario configurar direcciones MAC, pues al no estar dentro de la red de la UPV no hay ningún tipo de conflicto, por tanto, las podemos dejar por defecto y que se generen automáticamente. Lo que sí debemos asignar son los respectivos adaptadores de red de cada una de las máquinas y configurar sus interfaces. La configuración para cada máquina la encontraremos en “*Edit virtual machine settings*”:

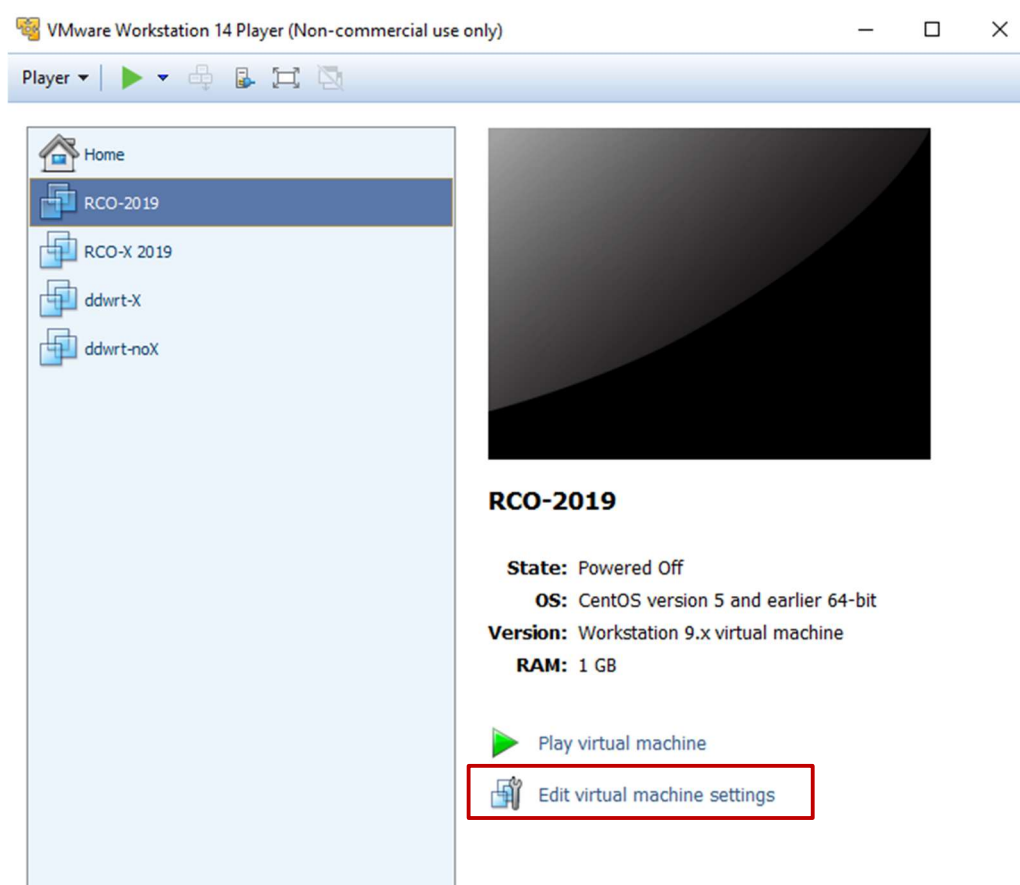


Ilustración 2

En el router `ddwrt-noX` asignaremos al adaptador de red principal la red *VMnet 1*, que estará conectado directamente con el PC. El adaptador secundario acogerá la conexión de la máquina cliente `RCO`, hecho que hará que sea necesaria la asignación de una red distinta. Siguiendo el boletín, esta red será *VMnet 2*. De manera análoga, el router `ddwrt-X` estará conectado al PC mediante *VMnet 1* y a la máquina cliente `RCO-X` por *VMnet 3*, como indica la imagen:

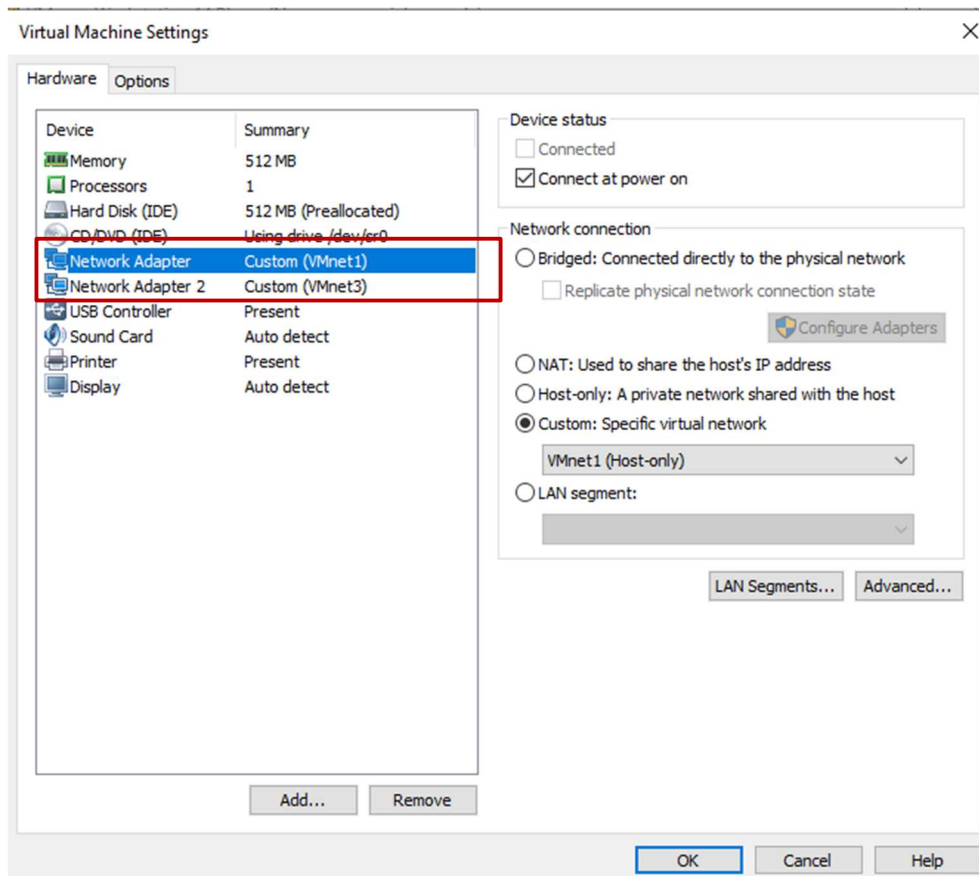


Ilustración 3

Las máquinas clientes **no** necesitan ser configuradas, pues la configuración por defecto es suficiente. Una vez tenemos todas las máquinas configuradas, procedemos a su encendido y comprobación, y nos aseguramos de que la virtualización funciona correctamente.

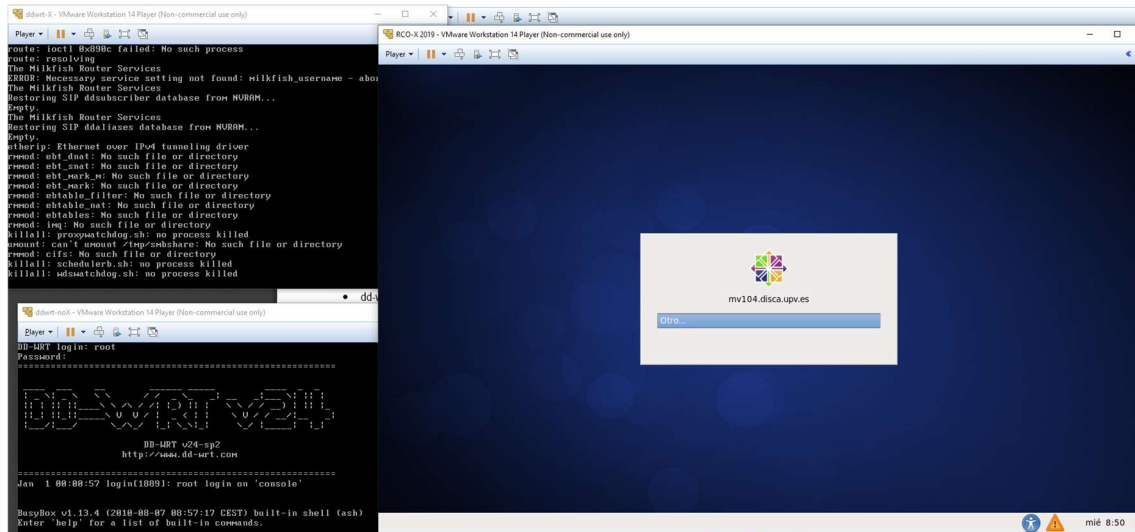


Ilustración 4

3. Configuración de los interfaces

DD-WRT

Para que las máquinas virtuales que emulan routers DD-WRT tengan direcciones IP que puedan alcanzar nuestro PC y salir a internet debemos configurar los adaptadores principales previamente establecidos con las direcciones IP que se nos marcan en el boletín. En este caso lo podemos hacer con las órdenes siguientes para `ddwrt-noX` y `ddwrt-X`, respectivamente:

```
ifconfig eth0 10.19.17.1 netmask 255.255.255.0
```

```
ifconfig eth0 10.19.17.111 netmask 255.255.255.0
```

Vamos a desglosar qué hacen estas órdenes. El comando `ifconfig` permite configurar los distintos interfaces de red disponibles en el sistema. Como nuestra misión es configurar *VMnet 1*, asignado al adaptador de red principal, usaremos como parámetro `eth0`. Tras esto, introduciremos la IP deseada de dicho adaptador, en caso de `ddwrt-noX` será `10.19.17.1` y en el router `ddwrt-X` será `10.19.17.111`. El siguiente parámetro que usaremos será `netmask`. `netmask` permite configurar la máscara de red que usaremos. Ciñéndonos a las instrucciones del boletín, la máscara especificada será `/24`, o sea, `255.255.255.0`.

Las siguientes imágenes muestran cómo quedarían las interfaces de ambos routers tras aplicar las órdenes.

Para `ddwrt-noX`:

```
root@DD-WRT:~# ifconfig eth0 10.19.17.1 netmask 255.255.255.0
root@DD-WRT:~# ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:50:56:1D:11:FF
          inet addr:10.19.17.1  Bcast:10.19.17.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:598 errors:0 dropped:0 overruns:0 frame:0
          TX packets:63 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:54552 (53.2 KiB)  TX bytes:20412 (19.9 KiB)
          Interrupt:5 Base address:0x2000

root@DD-WRT:~#
```

Ilustración 5

Para `ddwrt-X`:

```
root@DD-WRT:~# ifconfig eth0 10.19.17.111 netmask 255.255.255.0
root@DD-WRT:~# ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:50:56:1D:12:FF
          inet addr:10.19.17.111  Bcast:10.19.17.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:573 errors:0 dropped:0 overruns:0 frame:0
          TX packets:57 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:53688 (52.4 KiB)  TX bytes:18468 (18.0 KiB)
          Interrupt:5 Base address:0x2000

root@DD-WRT:~#
```

Ilustración 6

Para que los cambios sean permanentes en los routers, será necesario guardar los cambios que hagamos en la memoria no volátil. Si bien esto se puede hacer mediante comandos, hemos considerado que la opción más factible resulta por hacerlo desde la interfaz gráfica que nos ofrece DD-WRT. Para acceder a dicha interfaz, basta con escribir la dirección IP que acabamos de configurar en el navegador del PC. El hecho de que estas máquinas virtuales sean accesibles mediante el navegador de una máquina física tiene que ver con que ahora están en la misma red y se pueden ver entre ellas.

dd-wrt.com

... control panel

Firmware: DD-WRT v24-sp2 (08/07/10) std

Time: 00:02:57 up 3 min, load average: 0.04, 0.08, 0.03

WAN IP: 10.19.17.1

Setup

Services

Security

Access Restrictions

NAT / QoS

Administration

Status

System Information

Router

Router Name	DD-WRT
Router Model	Generic X86
LAN MAC	00:0C:29:7A:E5:6B
WAN MAC	00:50:56:1D:11:FF
WAN IP	10.19.17.1
LAN IP	192.168.17.1

Services

DHCP Server	Disabled
WRT-radauth	Disabled
WRT-rflow	Disabled
MAC-upd	Disabled
CIFS Automount	Disabled
Sputnik Agent	Disabled

Memory

Total Available	502.8 MB / 512.0 MB
Free	488.8 MB / 502.8 MB
Used	14.0 MB / 502.8 MB
Buffers	1.8 MB / 14.0 MB
Cached	5.2 MB / 14.0 MB
Active	0.9 MB / 14.0 MB
Inactive	1.1 MB / 14.0 MB

Space Usage

CIFS	(Not mounted)
------	---------------

Ilustración 7

Una vez hemos conseguido acceder a la interfaz gráfica del router, será necesario cambiar tanto las direcciones asignadas a LAN y WAN para que sean permanentes. Para configurar la dirección IP asignada a WAN, deberemos acceder a la pestaña “Setup”, y en el desplegable llamado “Connection Type” en “WAN Setup” seleccionaremos “Static IP”.

dd-wrt.com ... control panel

Time: 00:05:50

Setup Services Security Access Restrictions NAT / QoS Administration Status

Basic Setup DDNS MAC Address Clone Advanced Routing Networking **EoIP Tunnel**

WAN Setup

WAN Connection Type

Connection Type Static IP

WAN IP Address 10.19.17.1

Subnet Mask 255.255.255.0

Gateway 0.0.0.0

Static DNS 1 0.0.0.0

Static DNS 2 0.0.0.0

Static DNS 3 0.0.0.0

STP ☐ Enable ☒ Disable

Ilustración 8

La IP que hemos configurado anteriormente la escribiremos en el apartado “WAN IP Address” y escribiremos también la máscara correspondiente.

La configuración de la IP de LAN se hace de manera muy parecida. Dos secciones más abajo de “WAN Setup” encontraremos “Network Setup”. En “Local IP Address” bastará con colocar la IP que corresponderá al router en la red interna de este. Siguiendo el boletín y teniendo en cuenta que el router que estamos configurando actualmente es ddwrt-noX, la IP asignada será 192.168.17.1, como muestra la imagen.

Network Setup

Router IP

Local IP Address 192.168.17.1

Subnet Mask 255.255.255.0

Gateway 0.0.0.0

Local DNS 0.0.0.0

Ilustración 9

En el router ddwrt-X la configuración se realiza de manera análoga, pero con las correspondientes IP asociadas a dicho router.

Para aplicar los cambios, es necesario pulsar “Save” para asegurarnos que los cambios se guardan en la interfaz y “Apply Settings” para escribirlos en la memoria no volátil. Con

esto, y si no ha ocurrido ningún error, debería dejar las IP permanentemente configuradas, hasta un próximo reseteo.

Clientes

El cliente RCO-X va a tomar su dirección IP por DHCP del router ddwrt-X. En este caso y por este hecho, no será necesaria la configuración de su interfaz principal, ya que será el propio router el que le servirá su propia dirección única. La activación del servidor DHCP en el router ddwrt-X la veremos en capítulos posteriores.


La máquina cliente que **sí** necesita configuración es RCO. Para cambiar su dirección IP necesitaremos acceder al archivo `ifcfg-eth1` y editarlo con nuestro editor de ficheros preferido. Este archivo se encuentra en `/etc/sysconfig/network-scripts`. Para acceder allí haremos un `cd` (*change directory*)

```
cd /etc/sysconfig/network-scripts/
```

Y abriremos el archivo con un editor de ficheros. En nuestro caso hemos usado `nano`.

```
sudo nano ifcfg-eth1
```

Una vez abierto el archivo, cambiaremos la entrada `IPADDR` por la requerida en el boletín, en nuestro caso será `192.168.17.2`. El resultado es el siguiente:



```
GNU nano 2.0.9                                Fichero: /etc/sysconfig/network-scripts/ifcfg-eth1
DEVICE=eth1
TYPE=Ethernet
ONBOOT=yes
NM_CONTROLLED=yes
BOOTPROTO=None
DEFROUTE=yes
PEERDNS=yes
PEERROUTES=yes
IPV4_FAILURE_FATAL=yes
IPV6INIT=no
NETWORK=192.168.17.0
NAME="System eth1"
IPADDR=192.168.17.2
GATEWAY=192.168.17.1
```

Ilustración 10

Guardar el archivo **no** nos cambiará la dirección IP en ese momento. Para que esta cambie deberemos tumbar y volver a levantar el interfaz. Esto lo conseguimos con las órdenes `ifdown eth1` y `ifup eth1`.

```
[root@mv203 ~]# ifdown eth1
[root@mv203 ~]# ifup eth1
Determining if ip address 192.168.17.2 is already in use for device eth1...
```

Ilustración 11

La comprobación de que dicha IP ha sido configurada correctamente se puede obtener de manera trivial con `ifconfig`.

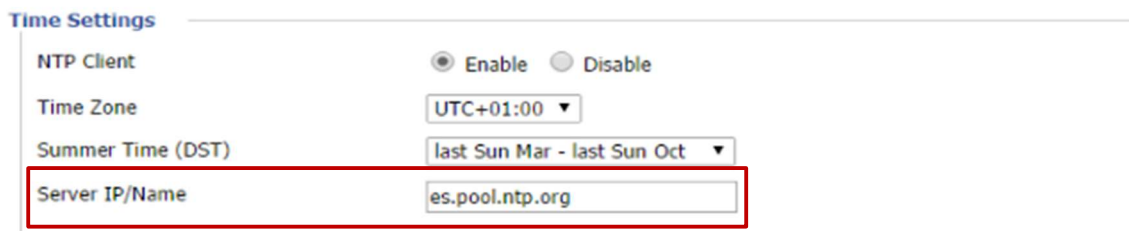
```
[root@mv203 ~]# ifconfig
eth1      Link encap:Ethernet  HWaddr 00:0C:29:B7:CE:11
          inet addr:192.168.17.2  Bcast:192.168.17.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:feb7:ce11/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:204 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:17196 (16.7 KiB)
```

Ilustración 12

4. Configuración de los routers

Una vez hemos hecho las IP permanentes en ambos routers, es momento de modificar la configuración por defecto para evitar que el túnel EoIP cause problemas al conectarnos.

Uno de los principales cambios que realizaremos será la sincronización de los relojes internos de los routers. Este cambio solo es interesante cuando se trabaja con certificados, pues un certificado caducado puede tumbar una conexión a todas luces segura y correcta. Para ello solo tenemos que desplazarnos hasta el apartado “*Time Settings*” y poner cualquier servidor válido. En nuestro caso, hemos tomado el servidor recomendado en una de las prácticas de EoIP, como se muestra en la imagen.



Time Settings

NTP Client ☒ Enable ☐ Disable

Time Zone UTC+01:00 ▼

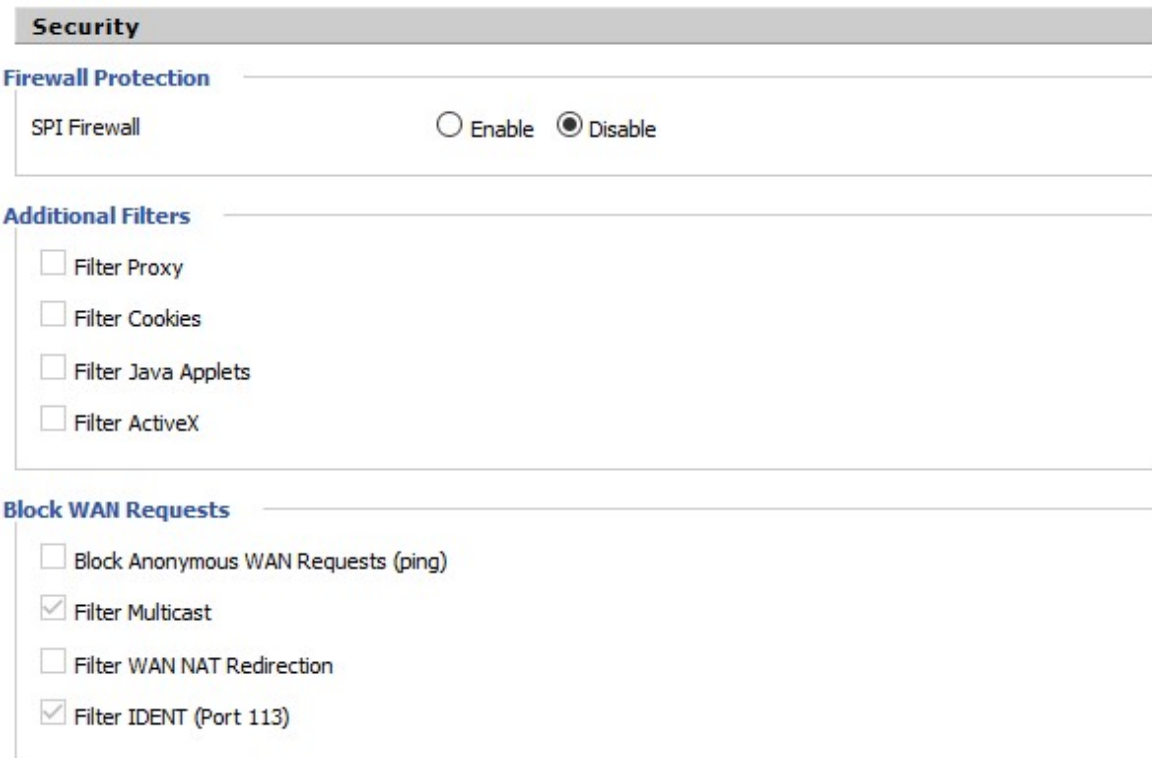
Summer Time (DST) last Sun Mar - last Sun Oct ▼

Server IP/Name es.pool.ntp.org

Ilustración 13

En este caso, dado que los routers y la *VMnet 1* no tendrán salida a internet, nunca podrán sincronizar sus relojes, aunque tampoco será necesario ya que no trabajamos con certificados. Cada router tendrá su reloj conforme al tiempo que lleve encendida la máquina virtual.

Otra de las opciones a modificar será la que habilita recibir pings de fuentes desconocidas, para ello iremos a la pestaña “*Security*” y deshabilitaremos temporalmente el Firewall que implementa DD-WRT. Esto nos dará acceso a desmarcar la opción “*Block anonymous WAN request*”. Una vez hecho esto, también podremos hacer pings entre clientes. Deshabilitar esta opción supone cierto peligro ya que, aunque un ping consume un ancho de banda mínimo, un ataque DDOS centrado en pings podría saturar el túnel que tenemos montado.



Security

Firewall Protection

SPI Firewall ☐ Enable ☒ Disable

Additional Filters

☐ Filter Proxy

☐ Filter Cookies

☐ Filter Java Applets

☐ Filter ActiveX

Block WAN Requests

☐ Block Anonymous WAN Requests (ping)

☒ Filter Multicast

☐ Filter WAN NAT Redirection

☒ Filter IDENT (Port 113)

Ilustración 14

El otro asunto de la configuración es si dejamos el Firewall desactivado o lo ponemos en marcha. A nivel de seguridad es un problema, pero para las pruebas que queremos realizar será mejor dejarlo desactivado para que interfiera lo mínimo posible.

Como hemos visto en el capítulo anterior, las interfaces de los routers están definidas y fijadas para que no creen conflicto. Ahora para que puedan manejar los clientes que se conecten a ellas se nos plantean dos alternativas. Un cliente funcionará con una IP fija que ya se ha configurado en esa máquina y otra obtendrá la dirección IP mediante el servidor DHCP que implementa nuestro router `ddwrt-x`.

En `ddwrt-noX` como no vamos a necesitar que los clientes obtengan direcciones de manera dinámica desactivaremos el servicio DHCP, además nos cubrimos de sufrir problemas, ya que cuando activemos el túnel tendremos una red, y dos servicios DHCP repartiendo direcciones IP. Para desactivar el DHCP solamente hay que pulsar el botón “Disable” en la pestaña principal de la configuración del router como vemos en la siguiente imagen:

Network Address Server Settings (DHCP)

DHCP Type	DHCP Server
DHCP Server	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Start IP Address	192.168.17.5
Maximum DHCP Users	50
Client Lease Time	1440 minutes
WINS	0.0.0.0
Use DNSMasq for DHCP	<input checked="" type="checkbox"/>
Use DNSMasq for DNS	<input checked="" type="checkbox"/>
DHCP-Authoritative	<input checked="" type="checkbox"/>

Ilustración 15

En el caso del otro router se nos pide que dé direcciones en un rango de 112 a 119. Para ello en la configuración del servicio DHCP indicamos como primera dirección a repartir la 112 y un máximo de 7 usuarios DHCP como vemos en la imagen:

Network Address Server Settings (DHCP)

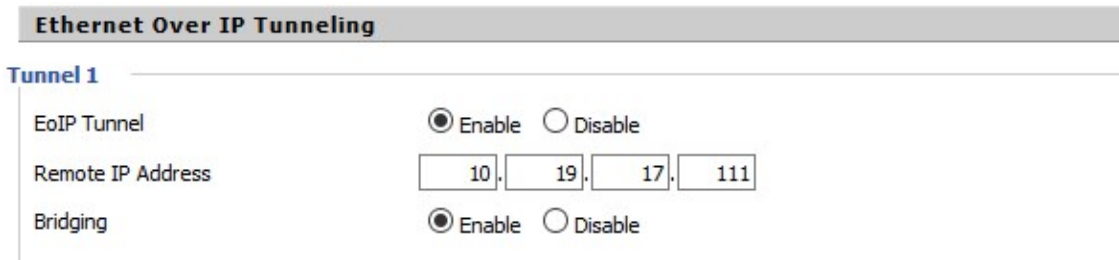
DHCP Type	DHCP Server
DHCP Server	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Start IP Address	192.168.17.112
Maximum DHCP Users	7

Ilustración 16

La configuración del túnel es posiblemente la más sencilla de todas. En DD-WRT hay una pestaña dedicada a ello en la configuración principal del router. En la versión que estamos utilizando cada router deja configurar hasta 10 túneles distintos, aunque a nosotros nos bastará con uno de ellos. Como ambos routers están en una misma red y las direcciones IP WAN que tienen son del mismo rango, hay que activar uno de los 10 túneles que se nos ofrecen (el mismo en ambos routers) y poner la dirección IP del otro router, es decir, un router tiene que saber quien es el otro. Aplicando la configuración a ambos a la vez debe funcionar, cosa que podemos comprobar haciendo un ping al otro

router desde la consola que tenemos en la máquina virtual. En caso de que no obtengamos respuesta al hacer el ping, salvamos la configuración y reiniciamos ambos routers.

En `ddwrt-X` con IP WAN `10.19.17.1`:



Ethernet Over IP Tunneling

Tunnel 1

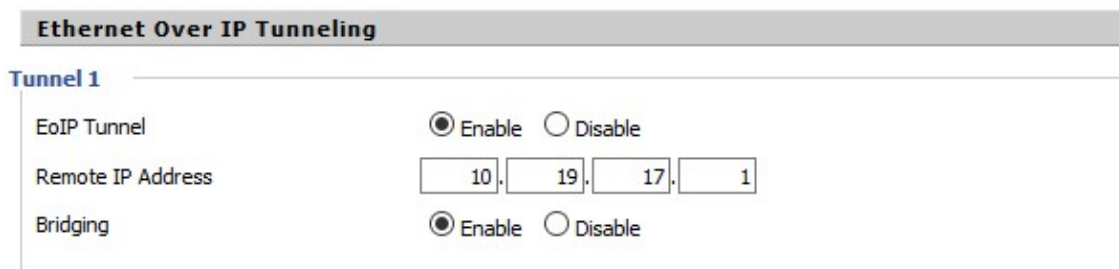
EoIP Tunnel ☒ Enable ☐ Disable

Remote IP Address

Bridging ☒ Enable ☐ Disable

Ilustración 17

En `ddwrt-noX` con IP WAN `10.19.17.111`:



Ethernet Over IP Tunneling

Tunnel 1

EoIP Tunnel ☒ Enable ☐ Disable

Remote IP Address

Bridging ☒ Enable ☐ Disable

Ilustración 18

Como podemos observar en el diagrama, cada router introducirá la dirección del otro y al estar comunicados mediante *VMnet 1*, ambos se conocerán.

5. Funcionamiento del túnel

Para verificar el funcionamiento aparte del funcionamiento teórico arrancamos el Wireshark para capturar todo el tráfico de *VMnet 1* antes de arrancar ambas máquinas virtuales. Una vez arrancadas no vemos ningún tráfico entre ellas pese a que hemos indicado las direcciones de la otra máquina respectivamente. Al hacer un ping de una máquina a otra observamos que la máquina que emite el ping primero hace un *Broadcast* a la red preguntando por la dirección IP que hemos indicado en el ping, en este caso, la del otro router. Éste le responde y a partir de aquí el ping se desarrolla con normalidad.

Time	Source	Destination	Protocol	Length	Info
0.000000	Vmware_1d:12:ff	Broadcast	ARP	42	Who has 10.19.17.1? Tell 10.19.17.111
0.000197	Vmware_1d:11:ff	Vmware_1d:12:ff	ARP	42	10.19.17.1 is at 00:50:56:1d:11:ff
0.000355	10.19.17.111	10.19.17.1	ICMP	98	Echo (ping) request id=0xac08, seq=0/0, ttl=64 (reply in 4)
0.000498	10.19.17.1	10.19.17.111	ICMP	98	Echo (ping) reply id=0xac08, seq=0/0, ttl=64 (request in 3)

Ilustración 19

Cierto es que si observamos los tiempos que se nos dan en la máquina emisora observamos que dada la consulta de “Quién es esta otra máquina” el tiempo de respuesta se demora ligeramente más que en los demás, pero lo vemos totalmente normal y admisible. En caso de hacer ping a la dirección IP de los equipos, el otro router responderá al *Broadcast* indicando que esa dirección está bajo su red, aunque sea por otra interfaz, y por tanto se redirige el tráfico hasta ella.

5.000138	Vmware_1d:11:ff	Vmware_1d:12:ff	ARP	42	Who has 10.19.17.111? Tell 10.19.17.1
5.000589	Vmware_1d:12:ff	Vmware_1d:11:ff	ARP	42	Who has 10.19.17.1? Tell 10.19.17.111
5.000839	Vmware_1d:12:ff	Vmware_1d:11:ff	ARP	42	10.19.17.111 is at 00:50:56:1d:12:ff
5.000914	Vmware_1d:11:ff	Vmware_1d:12:ff	ARP	42	10.19.17.1 is at 00:50:56:1d:11:ff
5.001210	Vmware_81:8e:99	Vmware_b7:ce:11	ARP	96	Who has 192.168.17.2? Tell 192.168.17.112
5.001853	Vmware_b7:ce:11	Vmware_81:8e:99	ARP	96	192.168.17.2 is at 00:0c:29:b7:ce:11

Ilustración 20

6. Para ampliar

Una vez comprobado el correcto funcionamiento de los túneles y tras una pequeña investigación por la red, fuimos conscientes de la cantidad de usos que puede tener esta tecnología. Por poner uno de muchos ejemplos, puede ayudar sobremanera a mejorar la seguridad de una red si ésta tiene una parte especialmente dedicada a invitados. El uso de EoIP permite canalizar el tráfico de la red de invitados directamente hasta el router que sale a internet sin tener que modificar cableado interno de nuestra compañía.

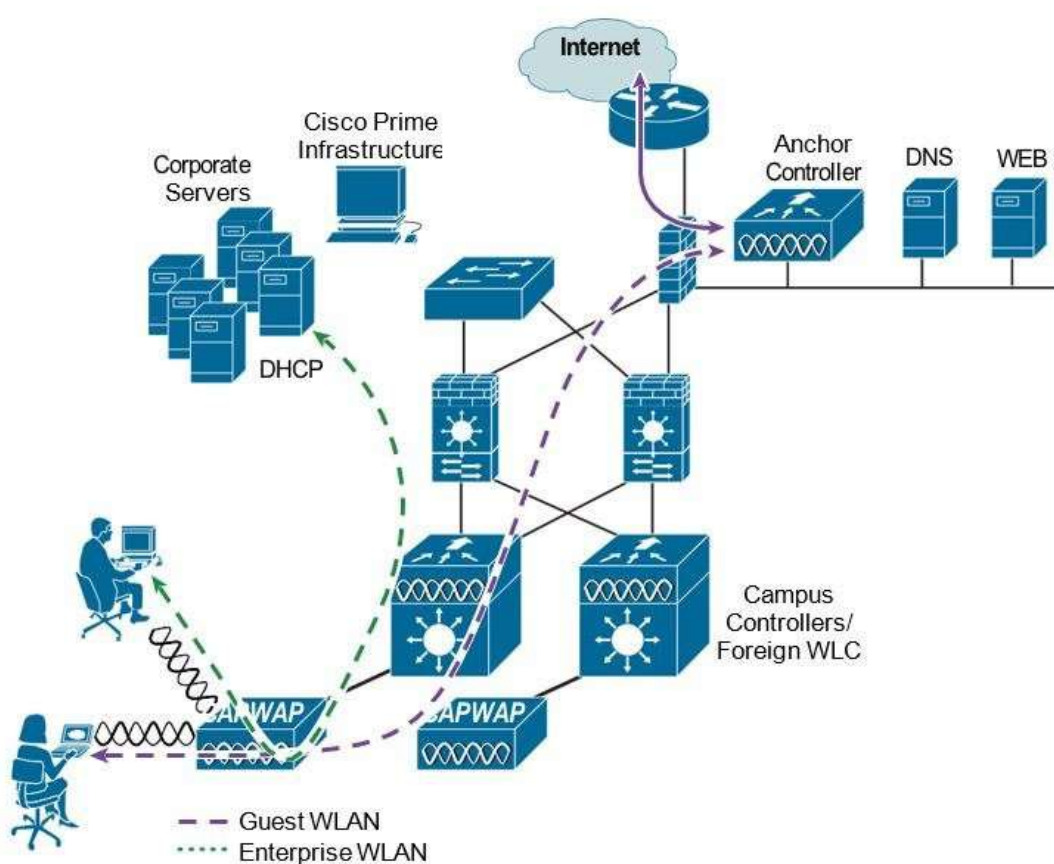


Figura 2

Como muestra esta imagen es posible la tunelización de la información que pase por la red de invitados hasta el router de salida, sin tener acceso directo a la red interna de la organización. Aparte de una mejora sustancial en la escalabilidad, esto también ayuda a mantener la red segura, puesto que las conexiones realizadas desde un ordenador invitado son, en un principio, inocuas a la red interna, ya que sus conexiones permanecen encapsuladas dentro del protocolo de red.

Obviamente este tipo de mecanismo no es inherentemente seguro debido a las limitaciones que puede poseer, pero sí supone una capa más de seguridad al ocultar veladamente la verdadera conexión interna de la red corporativa. Si esto no fuera suficiente, permite tener redes independientes dedicadas a diversos roles de la organización de manera descentralizada y escalable, mejorando así uno de los problemas que muchas redes de hoy en día se pueden encontrar.

7. Conclusiones

Los túneles EoIP son de gran ayuda para simular una red local en un entorno completamente escalable. Su funcionamiento, como hemos explicado en el capítulo 5 nos permite mantenernos conectados a una red a pesar de estar a kilómetros de distancia. Esto aporta a cualquier red unas características que permiten su expansión ilimitada en cualquier entorno, mientras exista una conexión router a router que permita mantener las comunicaciones como si de una LAN se tratara.

Este trabajo nos ha permitido entender de una manera más profunda el funcionamiento de algo tan típico hoy en nuestros días como una VPN. La metodología empleada ha sido muy útil para nuestro aprendizaje y hemos logrado absorber con facilidad toda la información que se esperaba que aprendiésemos. Si bien nos hubiera gustado un trabajo más investigativo, no podemos poner crítica al desarrollo del proyecto que hemos llevado a cabo, pues aprender y saber cómo establecer un sistema de redes como el que hemos creado en el laboratorio es un conocimiento muy importante sobre todo en la rama de tecnologías de la información.

Afirmamos también que se han cumplido con todos los objetivos esperados por el profesor de manera satisfactoria y notable. Además, la propia investigación personal nos ha llevado a descubrir cómo aplicar este tipo de tecnología a ámbitos del mundo real en cuanto a securización de redes se refiere.

No obstante, EoIP también tiene una serie de inconvenientes que no está de más mencionar. Por ejemplo, el hecho de que sea dependiente de un *firmware* específico es un problema real en cuanto a integración se refiere. Si bien usando DD-WRT o usando un router de Mikrotik la configuración es sencilla como hemos visto, otros routers que no dispongan de esta capacidad pueden verse comprometidos a la hora de intentar filtrar, redirigir o manejar este tipo de tráfico que será completamente invisible para ellos. Por tanto, será necesario el uso del *firmware* arriba establecido para poder manejar de verdad este tipo de tráfico.

Bibliografía

CISCO. s.f. *Enterprise Mobility 8.1 Design Guide*. Último acceso: 8 de 10 de 2019.
https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-1/Enterprise-Mobility-8-1-Design-Guide/Enterprise_Mobility_8-1_Deployment_Guide/WirelessNetwork_GuestAccessService.html.

Mikrotik. s.f. *MikroTik Documentation*. Último acceso: 10 de 10 de 2019.
<https://wiki.mikrotik.com/wiki/Manual:Interface/EoIP>.

Pons Terol, Julio. 2019. *Práctica EoIP*. Valencia.

Pons Terol, Julio. 2019. *Seminario EoIP*. Valencia.

