



UNIVERSITAT
POLITÈCNICA
DE VALÈNCIA



Escola Tècnica
Superior d'Enginyeria
Informàtica

Escola Tècnica Superior d'Enginyeria Informàtica
Universitat Politècnica de València

Práctica/Trabajo 1: Túnel EoIP con routers dd-wrt

PRÁCTICA RCO

Grado en Ingeniería Informática

Autor: Julio Pons Terol

Grupo: 1

Curso 2024-2025

Resumen

En este documento se presenta la práctica 1, donde se debe configura un tunel EoIP entre los dos routers DD-WRT.

Se muestra como tiene que ser la red del trabajo y se indican los pasos para hacer todas las configuraciones tanto desde el entorno virtual como desde los archivos de configuración de las máquinas en ejecución.

Se plantean unas pruebas de funcionamiento y se explica como debe presentarse la documentación del trabajo.

Palabras clave: EoIP, ...

Abstract

This document presents practice 1, where an EoIP tunnel must be configured between the two DD-WRT routers.

It shows how the work network should be and indicates the steps to make all the configurations both from the virtual environment and from the configuration files of the running machines.

Some performance tests are proposed and it is explained how the documentation of the work should be presented.

Key words: EoIP, ...

Índice general

Índice general	V
Índice de figuras	VII
Índice de tablas	VII

1	Introducción	1
1.1	Objetivos	2
2	Recomendaciones generales para trabajar con DD-WRT	3
3	Configuración del servicio túnel EoIP (en modo Bridging).	7
4	Pruebas de funcionamiento	13
5	Documentación	17

Índice de figuras

1.1	Ejemplo de dos intranets con EoIP	1
1.2	Formato del encapsulado EoIP	2
2.1	Ajustes de fecha y hora	4
3.1	Esquema de red genérico	7
3.2	Esquema de red personalizado para el grupo 1	8
3.3	Conexión de red de ddwrt-noX (izquierda) y ddwrt-X (derecha)	9
3.4	Configuración de las IPs de LAN en ddwrt-noX (izquierda) y ddwrt-X (derecha)	9
3.5	IPs de RCO-noX	9
3.6	Archivos de configuración de RCO-noX, cambios sugeridos para el grupo 1	10
3.7	Configuración del EoIP en los ddwrt	10
4.1	Acceso al servidor web de rco-noX desde rco-X	13
4.2	Últimas líneas del archivo de registro de accesos del servidor web	14
4.3	Accediendo a ajustes VMWare en una máquina encendida	14
4.4	Desconectando la LAN en el ddwrt-noX	14

Índice de tablas

3.1	Valores para la configuración según esquema	8
3.2	Valores para la configuración reales	8

CAPÍTULO 1

Introducción

EoIP es un diseño de la empresa de dispositivos de red MikroTik. Aunque la implementación DD-WRT de EoIP tiene fallos conocidos documentados que dependen de la versión de DD-WRT que tenga instalada, todos los aspectos utilizados en esta práctica han sido verificados y funcionan correctamente con la versión de DD-WRT de los routers virtuales.

Ethernet over IP (EoIP) Tunneling permite crear un túnel Ethernet entre dos routers a través de Internet. El túnel funciona como si fuera una interface Ethernet y todo el tráfico Ethernet de un router es visto por el otro (y viceversa) como si hubiera un cable Ethernet uniendo los dos routers.

Existe dos posibilidades de configuración de EoIP: (1) Bridging (simulando un puente) y (2) Routing (haciendo routing). El aspecto diferencial de encapsular Ethernet en lugar de IP para hacer un túnel solo se aprovecha correctamente en modo bridge por tanto solo vamos a trabajar con esta configuración.

EoIP con Bridging hace que las dos intranets funcionan como si fuera una única red local Ethernet.

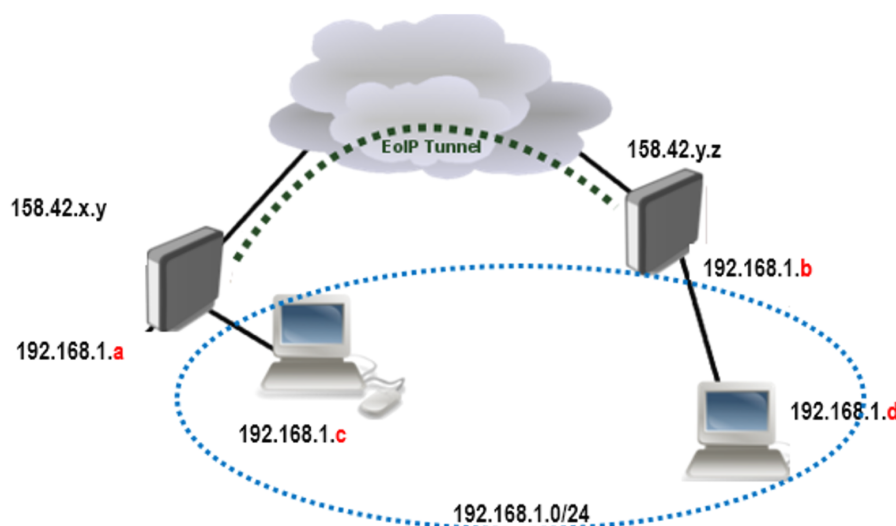


Figura 1.1: Ejemplo de dos intranets con EoIP

Para que funcione, las dos intranets deben tener la MISMA dirección de red. En la figura 1.1 puede observarse que ambas intranets tienen dirección 192.168.1.0/24.

Obviamente, el administrador debe tener cuidado de no asignar una misma IP en ambas intranets, porque cuando se active el túnel nos encontraríamos con máquinas distintas con la misma IP.

Vamos a configurar el túnel EoIP en modo BRIDGE. Esto implica que el túnel va a funcionar como si hubiera un puente-switch que conectara las dos intranets. Entonces todo el tráfico Ethernet (ARPs, broadcast... todo) de la intranet es visto por la otra intranet (y viceversa). Esto puede ser una opción (muy cómoda de configurar) para oficinas separadas físicamente que quieren compartir recursos locales (impresoras, fax, servidores...).

EoIP en modo bridge encapsula las tramas Ethernet en un datagrama IP. El formato utilizado es el mostrado en la figura 1.2. La cabecera IP lleva, en el campo "protocol", el identificador 0x61(en decimal 97) indicando que el campo de datos del datagrama contiene una trama Ethernet precedida por una cabecera EoIP.

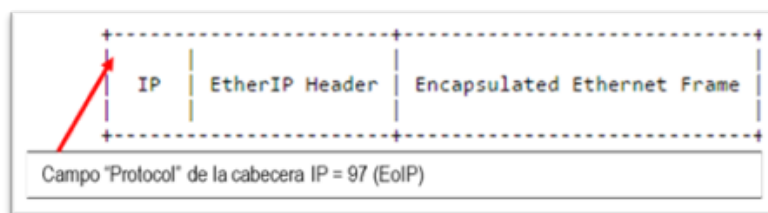


Figura 1.2: Formato del encapsulado EoIP

1.1 Objetivos

El objetivo principal de este documento es presentar la práctica/trabajo 1, explicando EoIP y proponiendo un esquema de red para probar un túnel EoIP.

Además se darán las directrices para la redacción de la memoria del trabajo.

CAPÍTULO 2

Recomendaciones generales para trabajar con DD-WRT

Aquí le damos algunos consejos útiles que son válidos para esta y futuras prácticas.

1. Usar el navegador adecuado.

DD-WRT se administra principalmente vía Web. En principio cualquier navegador debería valer, pero nos vamos encontrando con versiones DD-WRT que no funcionan bien con algunos navegadores. Mozilla Firefox es el navegador que parece que da menos problemas. En cualquier caso, para trabajar en la UPV, le recomendamos que configure el navegador para que no utilice el Proxy de la UPV.

A veces al acceder al interfaz web, puede quedar en cache información de una sesión anterior que hace que no se cargue correctamente la página, en este caso es recomendable borrar la cache del navegador o probar con otro navegador.

2. NO Borrar la NVRAM en los routers virtuales.

Con routers físicos, después de hacer una práctica, puede ser recomendable devolver el router a los ajustes de fábrica, puesto que una configuración anterior podría ser incompatible con la nueva.

Con las máquinas virtuales esto NO es recomendable ya que la máquina virtual original tiene configuraciones manuales realizadas después del ajuste de fábrica.

Si vamos a hacer una práctica que empezamos prácticamente de cero, es una buena costumbre utilizar la máquina original, es decir, volverla a extraer del archivo comprimido.

3. Sobre el SAVE y el APPLY SETTINGS

Cuando en una página de la interface web del router hacemos un cambio en la configuración, SAVE lo registra en la memoria NVRAM, pero no se produce ningún cambio en el funcionamiento del router. Cuando pulsamos APPLY SETTINGS se ejecuta un script, se paran/arrancan servicios (a veces conocidos como demonios), se escribe los valores de la RAM a la NVRAM (nvram commit), etc. Se puede observar que el APPLY SETTINGS no hace un reboot, sólo re-arrancan los servicios afectados. Lo cual es más rápido que un reboot completo.

¡Ojo! No queda muy claro que todos los APPLY SETTINGS de cualquier página hagan lo mismo. Concretamente, referente a los scripts, si la interfaz web estuviera perfectamente programada DEBERÍA ser lo mismo, PERO los numerosos errores de la interfaz web dan que pensar. Entonces, hacer todos los cambios en las páginas afectadas, con los correspondientes SAVE, y finalmente hacer un único APPLY... es

lo que debería ser, PERO puede ser mejor idea hacer APPLYS antes de cambiar de página.

4. El reloj del router

Esto es más importante de lo que parece. Sobre todo, cuando se usan certificados. Los certificados tienen un periodo de validez. Un reloj mal configurado es más que probable que haga que el certificado se interprete como revocado y sea imposible la conexión VPN que lo utiliza. Así que toca configurar el cliente NTP que lleva el router (figura 2.1).

Puede poner cualquier servidor NTP. Por ejemplo “es.pool.ntp.org”.

Compruebe que la hora es correcta en la parte superior derecha de la página.

Figura 2.1: Ajustes de fecha y hora

NOTA: si el router no tiene conectividad a internet, lógicamente no podrá acceder al servidor de tiempo. En caso de que se quede bloqueado (por timeouts en el acceso a este servidor) se puede optar por desactivar temporalmente este cliente NTP.

5. Comprobamos si tenemos activo el servidor Telnet o el SSH Por defecto, el servidor Telnet debería estar activo (si no es así, habilítelo). O mejor, puede también hacerlo con un cliente ssh, en cuyo caso debe habilitar el demonio SSHd. (Como se vio en la práctica 0 ambos servicios están activos en nuestros routers virtuales).

Para abordar las prácticas puede hacerlo con Telnet, pero es buena práctica que se acostumbre a usar SSH. Compruebe si el PC dispone de un cliente SSH como MobaXterm. Verifique que accede desde el PC con un cliente Telnet o SSH. Login/-password root/root

Ojo, telnet solo son accesibles desde la LAN. Además, el servidor SSH del dd-wrt tiene una versión de algoritmos de intercambio de claves bastante antigua y los clientes modernos no la suelen incluir por defecto, lo que hace que no podamos conectar, por ejemplo, si desde el mobaxterm intentamos conectar a un dd-wrt en la dirección 10.24.1.1:

```
1 ssh root@10.24.1.1
2 Unable to negotiate with 10.24.1.1 port 22: no matching key exchange
  method found.
3 Their offer: diffie-hellman-group1-sha1
```

La forma de resolverlo (con la última versión de mobaxterm) es con la siguiente opción:

```
1 ssh -legacy root@10.24.1.1
2 Warning: Permanently added '10.24.1.1' (RSA) to the list of known hosts.
3 DD-WRT v24-sp2 std (c) 2010 NewMedia-NET GmbH
```

```
4 Release: 08/07/10 (SVN revision: 14896)
5 root@10.24.1.1 's password:
```

También podemos conectar con telnet:

```
1 telnet 10.24.1.1
2 Trying 10.24.1.1...
3 Connected to 10.24.1.1.
4 Escape character is '^]'.
5 DD-WRT v24-sp2 std (c) 2010 NewMedia-NET GmbH
6 Release: 08/07/10 (SVN revision: 14896)
7 DD-WRT login:
```

En un entorno de producción se recomienda no usar nunca telnet ya que todos los datos se transmiten sin cifrar.

CAPÍTULO 3

Configuración del servicio túnel EoIP (en modo Bridging).

Para hacer esta práctica se requieren 2 PCs y 2 routers, en la figura 3.1 se muestra el esquema de conexión.

El campo “nº grupo” debe ser sustituido por el número asignado al grupo de prácticas, por ejemplo, si el número de grupo fuese el 1 las redes VNnet1 y VMnet2 serían 10.24.1.0/24. El esquema personalizado se muestra en la figura 3.2.

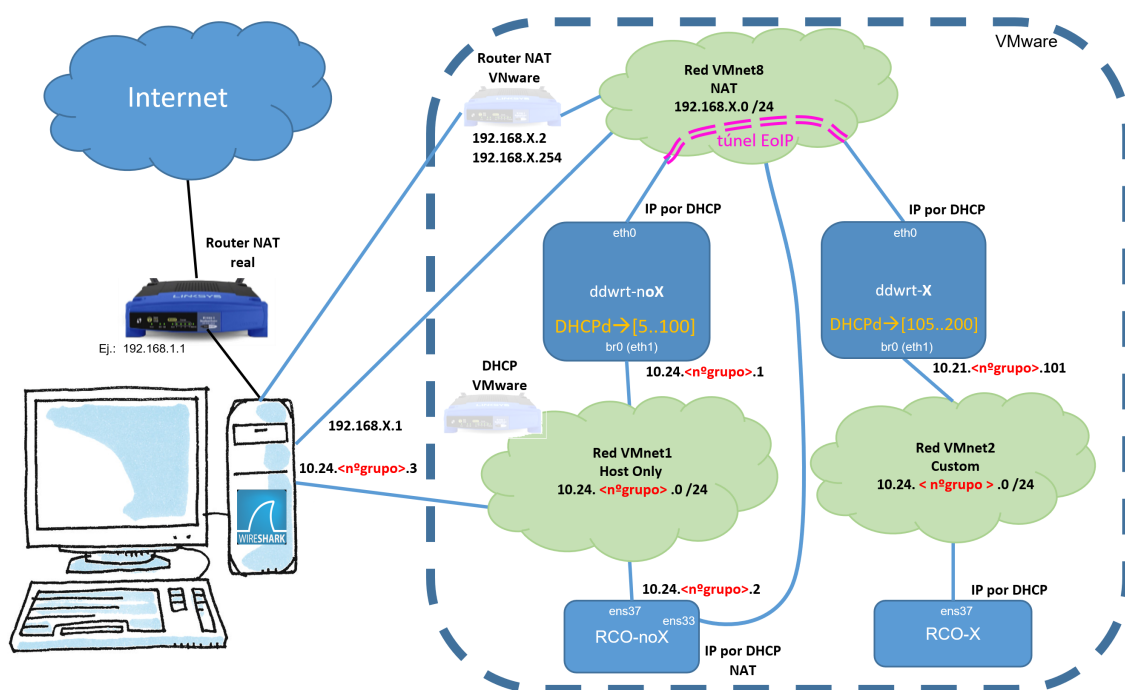


Figura 3.1: Esquema de red genérico

La red NAT (VMnet8) (“compartir con mi mac” en vm-fusion) es de similares características a la red Host Only con la diferencia de que VMWare incluye un router NAT virtual que permite la conexión a internet. En la configuración del VMWare Player 16 para Windows, dicho router tiene asignada la IP 192.168.X.2 y la tarjeta de red del ordenador anfitrión la IP: 192.168.X.1. El valor de X se asigna de forma aleatoria al hacer la instalación del VMWare, en nuestros ejemplos vamos a usar X=239 tal y como se puede ver en la figura 3.2.

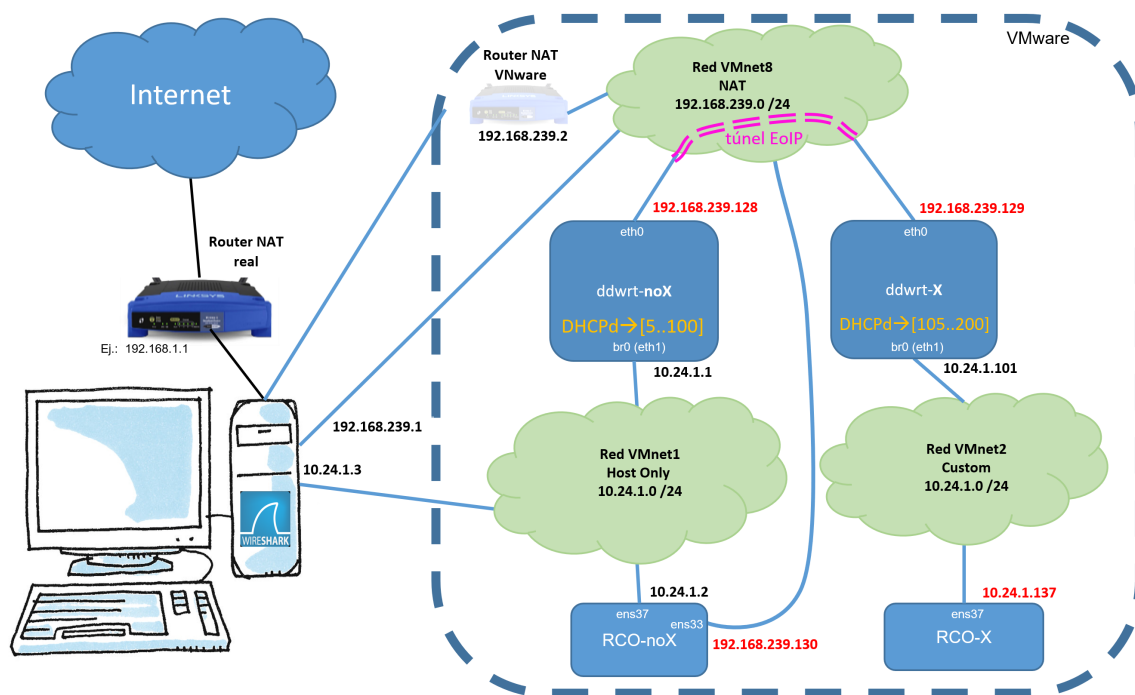


Figura 3.2: Esquema de red personalizado para el grupo 1

Una de las ventajas de utilizar la red NAT en lugar de bridge, es que reducimos el tráfico ya que todo el tráfico que el pc anfitrión con su red local e internet no es visible desde esta red NAT. Configuración Supongamos que Vd. está en el grupo n° 1. Con los datos que podemos obtener del esquema de la figura 3.2 podemos hacer la tabla 3.1.

	PC	dd-wrt NoX	dd-wrt X	RCO-noX	RCO-X
VMnet8	192.168.239.1	dhcp-1	dhcp-2	dhcp-3	-
VMnet1	10.24.1.3	10.24.1.1	-	10.24.1.2	-
VMnet2	-		10.24.1.101	-	dhcp-4
EoIP Tunel	-	Tunnel 1	Tunnel 1	-	-
EoiP Remote IP	-	dhcp-2	dhcp-1	-	-

Tabla 3.1: Valores para la configuración según esquema

Una vez tengamos todo funcionando, anotaremos las IPs asignadas por DHCP, como se muestra en la tabla 3.1.

	PC	dd-wrt NoX	dd-wrt X	RCO-noX	RCO-X
VMnet8	192.168.239.1	192.168.1.128	192.168.1.129	192.168.1.130	-
VMnet1	10.24.1.3	10.24.1.1	-	10.24.1.2	-
VMnet2	-		10.24.1.101	-	10.24.1.137
EoIP Tunel	-	Tunnel 1	Tunnel 1	-	-
EoiP Remote IP	-	192.168.1.129	192.168.1.128	-	-

Tabla 3.2: Valores para la configuración reales

El orden en que tenemos que hacer la configuración es el siguiente:

1. Comprobamos (ver figura 3.3) que la configuración de las dos tarjetas de red de los dos routers es la misma que en la práctica 0.



Figura 3.3: Conexión de red de ddwrt-noX (izquierda) y ddwrt-X (derecha)

2. Como la IP de la WAN de los routers se obtiene con DHCP vamos a averiguar la que nos han asignado, lo haremos desde la consola con la orden "ifconfig eth0". Utilizaremos esa IP para conectarnos a la web por ejemplo <http://192.168.239.128>
3. Cambiamos las IPs de las redes locales en los dos routers (figura 3.4). La configuración de DHCP no es necesaria modificarla pues coincide con la de la práctica 0.

Router IP					Router IP				
Local IP Address	10	24	1	1	Local IP Address	10	24	1	101
Subnet Mask	255	255	255	0	Subnet Mask	255	255	255	0
Gateway	0	0	0	0	Gateway	0	0	0	0
Local DNS	0	0	0	0	Local DNS	0	0	0	0

Figura 3.4: Configuración de las IPs de LAN en ddwrt-noX (izquierda) y ddwrt-X (derecha)

4. Ahora, en el pc, cambiamos en la tarjeta VMnet1 la IP estática a la que corresponda, en este ejemplo 10.24.1.3. Si todo está bien configurado, podremos acceder al router ddwrt-noX con su IP local, <http://10.24.1.1> y vía telnet o SSH con esa misma IP.
5. En RCO-noX cambiamos la configuración de la tarjeta "Network Adapter" de bridge a NAT (ver figura 3.5), mantenemos "Network Adapter 2" pues es la misma que en la práctica 0. Nos aseguramos de que está marcada la opción "Connect at power on". En RCO-X no es necesario cambiar nada.

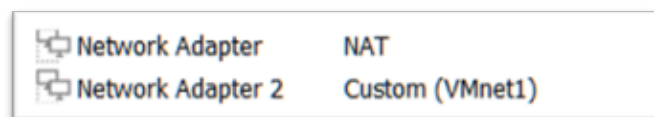


Figura 3.5: IPs de RCO-noX

6. En RCO-noX debemos hacer varios cambios. Primero en la interfaz ens33 que es la que tenemos conectada a la red NAT, debemos desactivar el gateway ya que queremos salir por la LAN y el ddwrt-noX. Este interfaz ya está configurado por DHCP por lo que el único cambio a realizar es en la línea DEFROUTE cambiando yes por no.

En el archivo de configuración de ens37 hay que cambiar la IP y el gateway tal y como se hizo en la práctica 0 pero con los nuevos valores.

En la figura 3.6 se muestran las rutas y los contenidos de los dos archivos de configuración. Además se muestran las tablas de routing que debemos tener una vez esté todo correctamente configurado.

Recordar que hay que hacer la secuencia ifup interfaz; ifdown interfaz después de editar el archivo de configuración de cada interfaz.

```
[root@rco-nox ~]# cd /etc/sysconfig/network-scripts/
[root@rco-nox network-scripts]# cat ifcfg-ens33
TYPE="Ethernet"
PROXY_METHOD="none"
BROWSER_ONLY="no"
BOOTPROTO="dhcp"
DEFROUTE="no"
IPV4_FAILURE_FATAL="no"
IPV6INIT="yes"
IPV6_AUTOCONF="yes"
IPV6_DEFROUTE="yes"
IPV6_FAILURE_FATAL="no"
IPV6_ADDR_GEN_MODE="stable-privacy"
NAME="ens33"
UUID="3b0c93eb-7c90-4170-8514-e1ac53069254"
DEVICE="ens33"
ONBOOT="yes"
[root@rco-nox network-scripts]# cat ifcfg-ens37
TYPE="Ethernet"
PROXY_METHOD="none"
BROWSER_ONLY="no"
BOOTPROTO="none"
IPV4_FAILURE_FATAL="no"
IPV6INIT="no"
NAME="ens37"
DEVICE="ens37"
ONBOOT="yes"
IPADDR=10.24.1.2
GATEWAY=10.24.1.1
PREFIX=24
UUID="c5b60d3c-f3f5-4e8d-8267-da3c24dfec47"
[root@rco-nox network-scripts]# ip route
default via 10.24.1.1 dev ens37 proto static metric 103
10.24.1.0/24 dev ens37 proto kernel scope link src 10.24.1.2 metric 103
192.168.239.0/24 dev ens33 proto kernel scope link src 192.168.239.130 metric 102
```

Figura 3.6: Archivos de configuración de RCO-noX, cambios sugeridos para el grupo 1

- Después de verificar vía ping que tenemos conectividad entre todos los componentes de cada red (VMnet8, VMnet1 y VMnet2) pasamos a configurar el túnel EoIP. Es importante sobre todo verificar que rco-X tiene la IP correcta que ha obtenido por DHCP del ddwrt-X ya que en el momento que activemos el túnel EoIP el servidor DHCP que VMWare aporta a la VMnet1 será visible desde la red VMnet2.

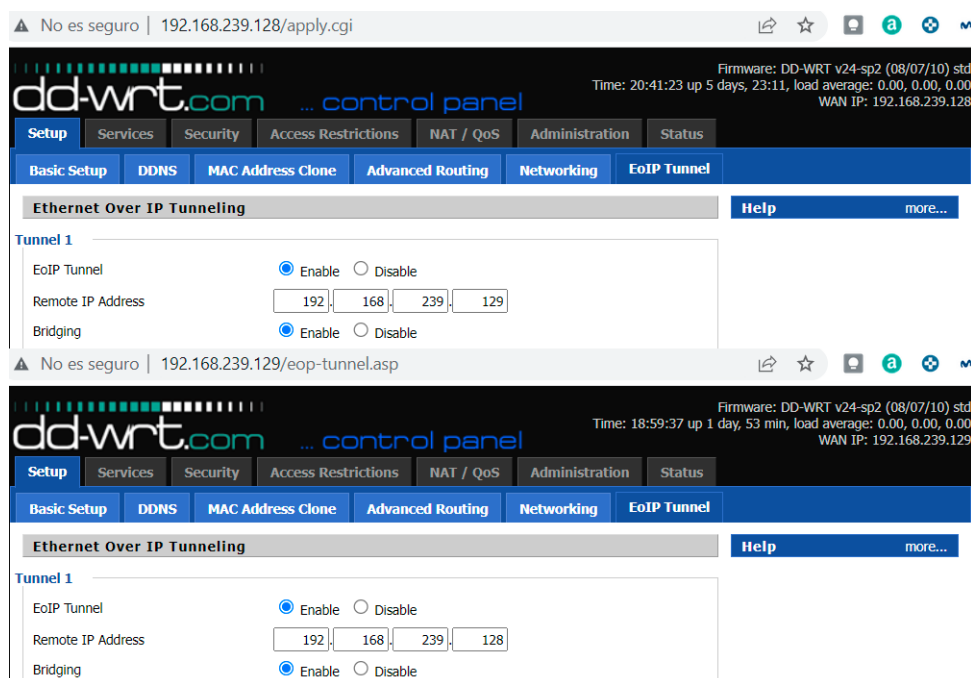


Figura 3.7: Configuración del EOIP en los ddwrt

Para configurar el túnel EoIP accederemos a la interfaz web de los dos routers e indicaremos a cada uno la IP de la WAN del otro (figura 3.7). Después de aplicar la configuración a ambos routers, el túnel EoIP debe establecerse.

CAPÍTULO 4

Pruebas de funcionamiento

En este capítulo se van a enumerar algunas pruebas que nos permitan verificar el funcionamiento del túnel, y además se propondrán modificaciones para analizar posibilidades de la conexión. Además se plantearán algunas cuestiones.

Antes de proceder a realizar las pruebas, es muy recomendable leer todo este documento, en especial el capítulo de documentación ya que nos va a dar pistas de que deberíamos capturar para a presentar posteriormente el trabajo.

1. Pruebe a hacer un ping desde el PC a la dirección local del rco-X (por ejemplo 10.24.1.137). Si funciona es gracias al túnel EoIP y todo ha ido bien. Si no funciona, verifique si llega un ping entre routers (por ejemplo 10.24.1.1 y 10.24.1.101), si no revise la configuración y vuelva a hacer “Apply Settings” en ambos routers. Si es necesario reinicie ambos routers.
2. Hacemos un “ifconfig” en los routers ddwrt-noX y ddwrt-X. Se puede observar que hay un nuevo adaptador “oet1”. Esta interfaz se crea al configurar el túnel EoIP. Obsérvese que está operando en modo promiscuo. Revise todos los interfaces de los routers a ver si hay alguno más que esté en modo promiscuo.

Intentar imaginar como funcionaría desde el punto de vista software le túnel en el ddwrt.

3. Utilice el servidor web de RCO-noX para ver la dirección NAT asignada a RCO-X.

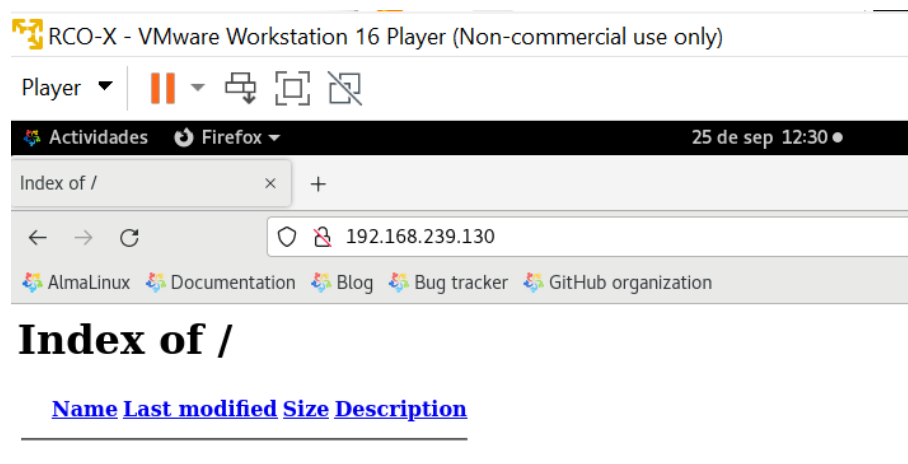


Figura 4.1: Acceso al servidor web de rco-noX desde rco-X

RCO-noX tiene un servidor web en marcha que escucha en todas sus direcciones IPs. Vamos a acceder desde el navegador de rco-X poniendo la IP del rco-noX de la red VMnet8, en nuestro ejemplo es 192.168.239.130 (ver figura 4.1).

Cómo no hay ninguna página definida en el servidor web nos sale un listado de un directorio vacío, pero el acceso queda registrado en el archivo de log del servidor web de RCO-noX que podemos consultar con la orden “tail /var/log/httpd/access_log” (tail nos saca las últimas líneas de un archivo, podemos usar otras órdenes como cat, less o cualquier editor para ver todo el archivo). En nuestro caso el resultado se muestra en la figura 4.2. Vemos como la IP que ha accedido es la IP de la WAN del router ddwrt-X (192.168.1.129 en nuestra configuración) que es lo que cabía esperar ya que este hace NAT y cambia la IP local de RCO-X por la suya de la WAN.

```
[root@rco-nox ~]# tail /var/log/httpd/access_log
192.168.239.129 - - [22/Sep/2024:18:34:11 +0200] "GET / HTTP/1.1" 200 481 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
192.168.239.129 - - [22/Sep/2024:18:34:11 +0200] "GET /icons/blank.gif HTTP/1.1" 200 148 "http://192.168.239.130/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
192.168.239.129 - - [22/Sep/2024:18:34:11 +0200] "GET /favicon.ico HTTP/1.1" 404 196 "http://192.168.239.130/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
```

Figura 4.2: Últimas líneas del archivo de registro de accesos del servidor web

4. Vamos a hacer que el servidor DHCP de la red VMnet2 sea ahora el de ddwrt-noX.

Primero desactive el servidor de DHCP de ddwrt-X (desde su interfaz web). Asegúrese de que el túnel se mantiene operativo (es posible que al cambiar configuraciones el túnel se desconecte).

A continuación, desconecte la red local de ddwrt-noX (desde ajustes de VMWare casilla Connected) como se muestra en las figuras 4.3 y 4.4.

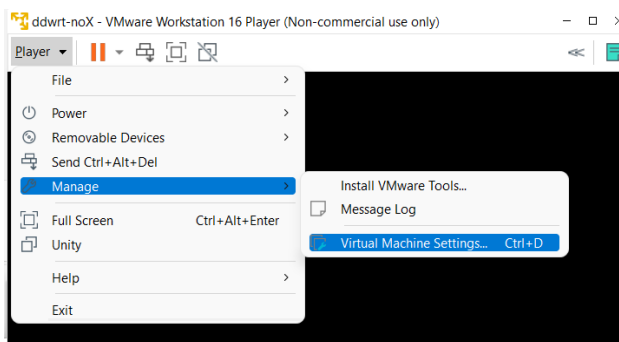


Figura 4.3: Accediendo a ajustes VMWare en una máquina encendida

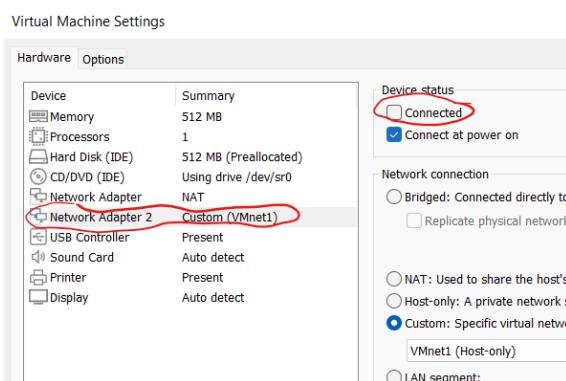


Figura 4.4: Desconectando la LAN en el ddwrt-noX

Esto aislará este router de la red VMnet1. Reinicie la interfaz de red de RCO-X para que vuelva a pedir una dirección IP.

Como se ha indicado anteriormente, el objetivo de este apartado es que rco-X contacte (vía el túnel EoIP) con el servidor DHCP de ddwrt-noX.

Hemos tenido que desconectarlo de la red VMnet1 porque VMWare incluye un servidor DHCP en la red VMnet1 y podría entrar en conflicto con el de nuestro router. Si lo hemos hecho bien, veremos que el rango de la IP asignada corresponde a la del primer router, en nuestro ejemplo nos ha asignado la 10.24.1.37.

Ahora vamos a volver a acceder a la página web de RCO-noX y ver lo que nos dice el registro de accesos. La IP con la que accedemos es la del router ddwrt-noX (en nuestro ejemplo 192.168.1.128).

Explique porqué sucede esto.

Después de esta prueba vuelva a dejar la configuración inicial (active el DHCP de ddwrt-X, reconecte ddwrt-noX a la red VMnet1 y reinicie la interfaz de RCO-X)

5. Desactive el servidor DHCP del ddwrt-noX y vuelva a activar el DHCP de ddwrt-X. Una vez hecho esto, fuerce a que rco-X vuelva a solicitar una IP. Si todo es correcto debería volver a tener la IP inicial (en nuestro ejemplo 10.24.1.137).

Configure el router ddwrt-X para salir a la WAN por el router ddwrt-noX. Indique que ha tenido que hacer.

Pistas: Tendrá que cambiar la tabla de routing. Hágalo por SSH. Utilice el comando: "ip route [add | del] x.x.x.x/m via x.x.x.x". Para ver las rutas actuales puede usar la orden "ip route list"

Los cambios deben conseguir lo siguiente: en ddwrt-X debe eliminar la regla default y luego añadir una regla default que encamine via la IP 10.24... del ddwrt-noX.

Además si queremos probar el NAT con la página web de rco-noX deberíamos añadir una regla adicional con la IP de rco-noX de la red NAT, con /32 para forzar que el acceso a esta IP se haga via la 10.24... del ddwrt-noX.

¿Por qué es necesaria esta regla adicional?

¿Qué ventaja ofrece este método frente al anterior (4)? (Piense en una oficina con varios PCs)

6. Realice medidas de prestaciones comparativas entre acceso directos y accesos a través del túnel EoIP.

Para esto utilizaremos el hecho de que RCO-noX tiene doble conexión con VMnet1 y VMnet8. Podemos transferir ficheros entre RCO-noX y RCO-X utilizando las IPs de RCO-noX 10.23... (usaría túnel) y 192.168... (usaría NAT). También podemos usar el PC para transferir archivos con RCO-noX a la dirección 10.23... (directa) y a RCO-X a la dirección 10.23... (usaría túnel).

Tanto RCO-noX como RCO-X tiene servidor SSH instalado que admite transferencias de archivos.

Además se pueden evaluar distintos tiempos de pings entre los distintos componentes de la red.

CAPÍTULO 5

Documentación

El trabajo se redactará en la plataforma online overleaf.com cargando una plantilla que se facilitará en la sección de recursos del poliformat.

Para que podáis tener ejemplos de uso del latex os facilitaré el acceso al código fuente de los enunciados de las prácticas 0 y 1.

La plantilla que se os facilita incluye los siguientes apartados, que son los que deberá tener vuestro trabajo:

- Portada con el título “Túnel EoIP con routers DD-Wrt”, los nombres de los componentes del grupo, el número del grupo y el curso académico.

- Resumen

Debe ser un breve resumen de todo el trabajo realizado, por lógica es la última parte que se rellena en el documento, aunque se presente al principio. Debe servir para que el lector decida si le interesa continuar leyendo.

El resumen se completa con las palabras clave, que se utilizan para indexar el documento en una base de datos bibliográfica, hay que utilizar palabras específicas que se relacionen con el trabajo.

El abstract y las keywords son la traducción al inglés del resumen y las palabras clave.

- Tabla de contenidos. Es el índice del documento se genera automáticamente. Incluirá el índice de figuras y el índice de tablas.

- Introducción

Debe poner al lector en el contexto del trabajo. Explica los objetivos y qué es lo que se va a hacer en el trabajo y debe incluir el esquema de la red virtual con TODAS las direcciones IP utilizadas, personalizadas según lo indicado.

A diferencia del resumen, aquí se indica que es lo que se va a hacer en las siguientes secciones, no pretende ser un resumen del trabajo, es más una planificación.

En la sección de recursos de poliformat se facilita un archivo powerpoint con los dibujos de el esquema para modificarlo y generar la imagen.

- Configuración.

Explicad cómo se ha realizado la configuración de la red virtual (VMWare, y en cada máquina virtual), con capturas de pantalla y TEXTO EXPLICATIVO:

1. ifconfig de los dispositivos ddwrt-noX, ddwrt-X, RCO-noX, RCO-X y PC (en Windows ipconfig), resaltando la IP de los adaptadores involucrados

2. Páginas web de los routers donde se muestre; la configuración de las IP (LAN y WAN), DHCP, EoIP, ...cualquier otra que considere ha sido importante en la configuración.
- **Funcionamiento del túnel.**

Explicar el túnel desde el punto de vista teórico, indicando las cabeceras que deberían transmitirse con ejemplos de comunicación entre vuestras máquinas.

Es importante explicar cómo evolucionan los paquetes (tramas, datagramas, segmentos... al nivel que considere que es el adecuado) desde que se transmiten por la máquina origen hasta que llegan al destino, indicando las máquinas intermedias involucradas y explicando cómo se procesan los paquetes en cada máquina.

Explicad con capturas de pantalla y TEXTO EXPLICATIVO, incluyendo diversas capturas de WireShark, comentando el túnel EoIP.

Recomendable capturar simultáneamente la red VMnet8 y VMnet1. Recomendable ver distintos tipos de tráfico, icmp, arp, etc. e intentar explicar por qué se presenta dicho tráfico.

En este apartado se incluirá igualmente las pruebas realizadas cambiando el servidor DHCP y la puerta de enlace para ver cuál es la IP con la que se accede al servidor web de RCO-noX desde RCO-X.
 - **Conclusiones,** Se indicará lo que se ha conseguido con el trabajo, en qué medida se han cumplido los objetivos, crítica (positiva y/o negativa) de la utilización del túnel EoIP, etc.
 - **Referencias,** las referencias deben tener el mismo formato que se exige en los TFGs (busque la documentación al respecto). Hay que poner un mínimo de 3 o 4 referencias, a ser posible que no sean todas páginas web. Se puede referenciar éste documento pero no contará en el número de referencias totales.

Consideraciones adicionales:

Las 4 máquinas virtuales deberán guardarse por si es necesario hacer alguna comprobación después de entregar el trabajo. El siguiente trabajo se realizará con una copia distinta de las máquinas virtuales.

El trabajo se entregará vía una tarea de poliformat en formato PDF y se incluirá un enlace de acceso de solo lectura al documento en overleaf.

El trabajo deberá entregarse antes de las 23:55 del lunes 14 de octubre.

Entrega fuera de plazo (a partir de las 23:56h) penalizarán en la nota ≥ 1 pto

La mejor nota entre este trabajo y el trabajo 2 aportará una puntuación del 25 % de la nota de la asignatura.