



UNIVERSITAT
POLITÈCNICA
DE VALÈNCIA



Escola Tècnica
Superior d'Enginyeria
Informàtica

Escola Tècnica Superior d'Enginyeria Informàtica
Universitat Politècnica de València

Trabajo 2: PPTP

TRABAJO RCO

Grado en Ingeniería Informática

Autor: Diego Córdoba Serra
Javier García Bartolomé
Maria Carmen Rea Mejia
Grupo: 181

Curso 2024-2025

Resumen

Este trabajo analiza en profundidad el funcionamiento del túnel PPTP en dos modos: site-to-site y remote-access. En el modo site-to-site, se configura una conexión VPN entre dos routers (ddwrt-noX y ddwrt-X), conectando así un cliente PPTP (ddwrt-noX) a un servidor PPTP (ddwrt-X). Mientras que en el modo remote-access, el cliente se ejecuta en un nuestro PC, sólo él podrá acceder a la intranet del servidor, y se mantiene el mismo servidor PPTP (ddwrt-X).

Palabras clave: PPTP, túnel, VPN, site-to-site, remote-access

Abstract

This paper provides an in-depth analysis of the PPTP tunnel functionality in two modes: site-to-site and remote-access. In the site-to-site mode, a VPN connection is configured between two routers (ddwrt-noX and ddwrt-X), connecting a PPTP client (ddwrt-noX) to a PPTP server (ddwrt-X). Meanwhile, in remote-access mode, the client runs on our PC, only it will be able to access the server's intranet, and the same PPTP server (ddwrt-X) is maintained.

Key words: PPTP, tunnel, VPN, site-to-site, remote-access

Índice general

Índice general	V
Índice de figuras	VII
<hr/>	
1 Introducción	1
1.1 Objetivos	2
2 Configuración de las máquinas	3
2.1 Desactivación del túnel EoIP	3
2.2 Reajustar la IP de red local de ddwrt-X	3
2.3 Configuración de la máquina virtual RCO-noX	4
3 Funcionamiento del túnel PPTP site-to-site	7
3.1 Configuración del túnel PPTP site-to-site	7
3.1.1 Configuración del servidor PPTP (ddwrt-X)	7
3.1.2 Configuración de cliente PPTP (ddwrt-noX)	9
3.2 Pruebas de funcionamiento	12
4 Funcionamiento del túnel PPTP remote-access	21
4.1 Configuración y verificación	21
4.2 Pruebas de funcionamiento	27
5 Conclusiones	33
Bibliografía	35

Índice de figuras

1.1	Esquema con túnel PPTP site-to-site	1
1.2	Esquema con túnel PPTP site-to-site	2
2.1	EoIP deshabilitado tanto en ddwrt-noX como en ddwrt-X	3
2.2	Modificación de la IP del ddwrt-X	3
2.3	Configuración de la red en RCO-noX	4
2.4	Configuración de la interfaz ens33 de RCO-noX	4
2.5	ifconfig de ens33 de RCO-noX	4
2.6	ip route show de ens33 de RCO-noX	5
2.7	Ping a google.es	5
3.1	Configuración PPTP Server	8
3.2	Redirección en ddwrt-x	8
3.3	Nueva regla de enrutamiento en ddwrt-X	9
3.4	Configuración del cliente PPTP en ddwrt-noX	10
3.5	Verificación de la opción PPTP Passthrough	10
3.6	Opcion Reboot Router	11
3.7	Comprobación de interfaces y tabla de rout ddwrt-X	11
3.8	Comprobación de interfaces y tabla de rout ddwrt-noX	11
3.9	ping de RCO-noX a RCO-X	12
3.10	Captura de paquetes de RCO-noX a RCO-X en VMnet1	12
3.11	Captura de paquetes de RCO-noX a RCO-X en VMnet8	13
3.12	ping anfitrion a RCO-x no funciona	14
3.13	Regla de routing RCO-x y tabla de enrutamento desde anfitrion	15
3.14	ping anfitrion a RCO-x funciona	15
3.15	tracert desde anfitrión a RCO-x	16
3.16	Instalacion traceroute	16
3.17	Orden traceroute desde RCO-noX a RCO-X	17
3.18	Orden traceroute desde RCO-X a RCO-noX	17
3.19	ip route de RCO-X	18
3.20	ip route de RCO-noX	18
3.21	ip route de ddwrt-X	19
3.22	ip route de ddwrt-noX	19
4.1	ping de RCO-noX a RCO-X no funciona	21
4.2	ifconfig de ddwrt-noX pp0 no aparece	22
4.3	Creacion de conexion a ddwrt-noX	23
4.4	Tracert en anfitrion, bucle infinito	23
4.5	vpn config3	24
4.6	vpn config1	24
4.7	vpn config2	25
4.8	Tracert en anfitrion correcto funcionamiento	25
4.9	ip route y ifconfig ppp0 de ddwrt-X tras configurar vpn	26
4.10	route print de anfitrion tras configurar la vpn	27

4.11	ping desde anfitrión a RCO-X	27
4.12	tráfico PPTP de la VMnet8 con pings entre el PC y RCO-X	28
4.13	ipconfig del cliente pptp	29
4.14	Tabla de enrutamiento del PC anfitrión	30
4.15	Tabla de forwarding de ddwrt-X	30
4.16	Tabla de forwarding de RCO-X	30
4.17	tracert desde anfitrión a RCO-x completado	31

CAPÍTULO 1

Introducción

En este trabajo se va a explicar de forma detallada la configuración y el funcionamiento de un túnel PPTP. Para ello se ha hecho uso de una red virtual creada con VMWare, la cual está compuesta por dos routers, llamados ddwrt-noX y ddwrt-X, y dos hosts, llamados RCO-noX y RCO-X.

En concreto se procederá a configurar un túnel PPTP en dos modos distintos: site-to-site y remote access. En el modo site-to-site, estableceremos un túnel PPTP de tipo site-to-site, donde tenemos a un cliente PPTP (ddwrt-noX) y un servidor (ddwrt-X), permitiendo así la conexión entre dispositivos de ambas redes que quedan unidas por el túnel PPTP. Todo esto queda reflejado en la figura 1.1

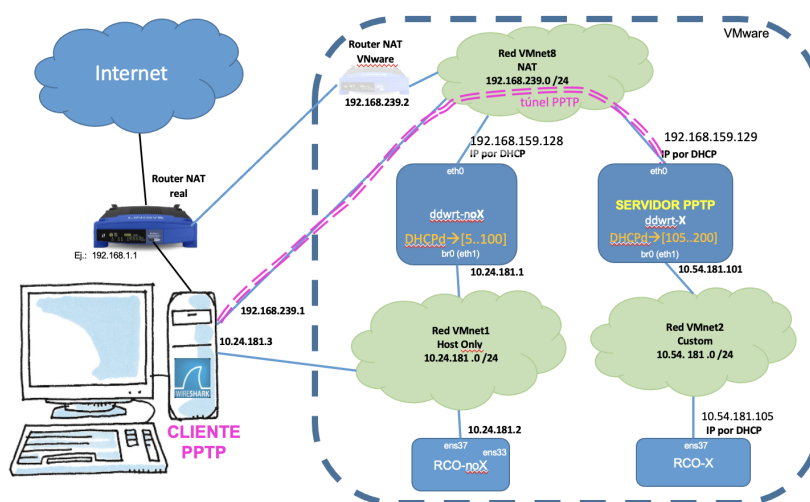


Figura 1.1: Esquema con túnel PPTP site-to-site

En contraste, en el modo remote-access, el cliente PPTP se ejecutará en un PC y sólo él podrá acceder a la intranet del servidor PPTP. En este caso, el servidor PPTP sirve como facilitador de la conexión para los clientes remotos.

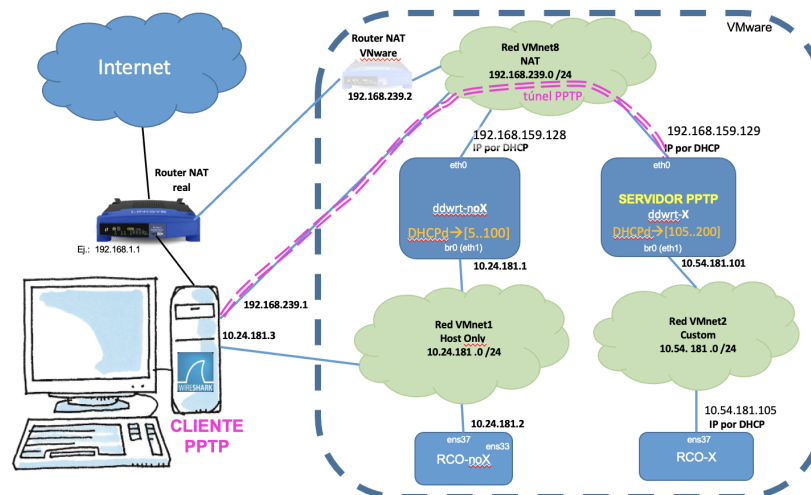


Figura 1.2: Esquema con túnel PPTP site-to-site

Por último se detallará las pruebas de funcionamiento realizadas sobre la red virtual con el túnel PPTP funcionando en site-to-site o en remote access para comprobar que el comportamiento de la misma es, en efecto, el apropiado.

1.1 Objetivos

Los objetivos de este trabajo se detallan a continuación:

- Analizar y entender el funcionamiento del túnel PPTP en los modos site-to-site y remote-access.
- Realizar pruebas de desempeño y análisis de los paquetes para verificar la correcta configuración del túnel.
- Examinar las tablas de enrutamiento de los dispositivos involucrados.
- Ofrecer un análisis de las ventajas y desventajas del PPTP, así como su relevancia en el contexto actual.

CAPÍTULO 2

Configuración de las máquinas

2.1 Desactivación del túnel EoIP

Primeramente, deshabilitaremos el túnel EoIP. Para ello, accedemos a las IP de los routers ddwrt-noX (192.168.159.128) y ddwrt-X (192.168.14.129). Luego, ingresamos a Setup > EoIP Tunnel, seleccionamos la opción disable y guardamos los cambios haciendo clic en Save y Apply Settings. Este procedimiento se ilustra en la figura 2.1

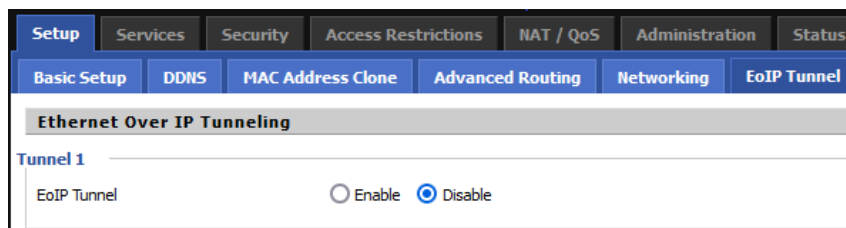


Figura 2.1: EoIP deshabilitado tanto en ddwrt-noX como en ddwrt-X

2.2 Reajustar la IP de red local de ddwrt-X

Como podemos observar en la figura la red Vmnet2 es “10.54”, por tanto en ddwrt-X habrá que reajustar la IP de la red local. Para ello, accedemos a su portal de configuración desde el navegador y en Setup > Basic Setup > Network Setup > Local IP Address cambiamos el tercer octeto por el número asignado a nuestro grupo (181). Esto se muestra en la figura 2.2

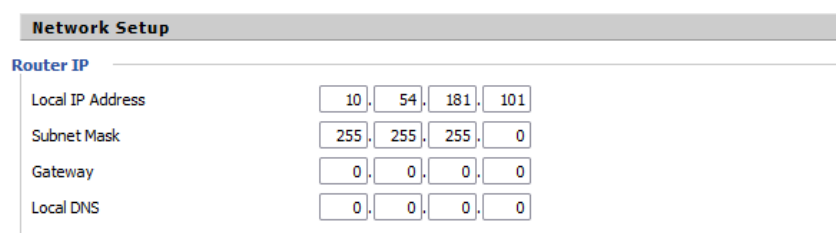


Figura 2.2: Modificación de la IP del ddwrt-X

2.3 Configuración de la máquina virtual RCO-noX

Seleccionamos la máquina RCO-noX y ajustamos las opciones del Adaptador de Red 1 (Network Adapter) para desconectarlo, desmarcando la opción 'Connect at power on' y quedarnos solo con la red VMnet1 (Figura 2.3)

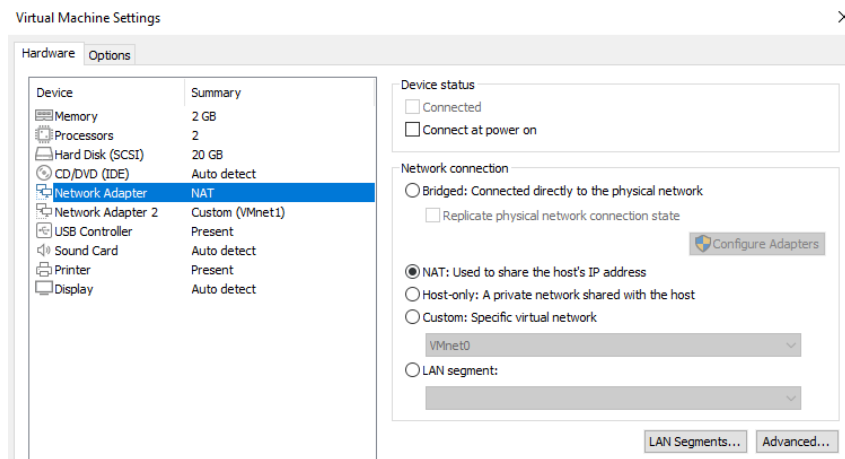


Figura 2.3: Configuración de la red en RCO-noX

Asimismo, para evitar que el sistema operativo active automáticamente la interfaz ens33, editaremos el archivo `/etc/sysconfig/network-scripts/ifcfg-ens33`, modificando la línea `ONBOOT=yes` por `ONBOOT=no`. Esto se muestra en la figura 2.4

```
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="no"
```

Figura 2.4: Configuración de la interfaz ens33 de RCO-noX

Después de aplicar estos cambios, reiniciamos la máquina y al ejecutar los comandos 'ifconfig' e 'ip route' deberíamos ver un resultado similar como en las siguientes imágenes, donde se observa que ens33 no tiene asignada una IP y que la ruta 'default' corresponde a nuestro router. La comprobación la podemos observar en la figura 2.5 y 2.6

```
[root@rc0-nox ~]# ifconfig
ens33: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    ether 00:0c:29:07:0f:61 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

ens37: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.24.181.2 netmask 255.255.255.0 broadcast 10.24.181.255
    inet6 fe80::20c:29ff:fe07:f6b prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:07:0f:6b txqueuelen 1000 (Ethernet)
```

Figura 2.5: ifconfig de ens33 de RCO-noX

```
[root@rco-nox ~]# ip route show
default via 10.24.181.1 dev ens37 proto static metric 100
10.24.181.0/24 dev ens37 proto kernel scope link src 10.24.181.2 metric 100
```

Figura 2.6: ip route show de ens33 de RCO-noX

Además, verificamos que tenemos acceso a Internet haciendo un ping a google.es y como podemos observar en la figura 2.7 muestra que la respuesta es satisfactoria.

```
[root@rco-nox ~]# ping google.es
PING google.es (142.250.185.3) 56(84) bytes of data.
64 bytes from mad41s11-in-f3.1e100.net (142.250.185.3): icmp_seq=1 ttl=127 time=14.10 ms
64 bytes from mad41s11-in-f3.1e100.net (142.250.185.3): icmp_seq=2 ttl=127 time=17.6 ms
64 bytes from mad41s11-in-f3.1e100.net (142.250.185.3): icmp_seq=3 ttl=127 time=17.10 ms
64 bytes from mad41s11-in-f3.1e100.net (142.250.185.3): icmp_seq=4 ttl=127 time=15.9 ms
```

Figura 2.7: Ping a google.es

CAPÍTULO 3

Funcionamiento del túnel PPTP site-to-site

3.1 Configuración del túnel PPTP site-to-site

3.1.1. Configuración del servidor PPTP (ddwrt-X)

Para que el túnel PPTP de tipo site-to-site funcione correctamente, comenzaremos configurando el servidor (ddwrt-X) y luego el cliente (ddwrt-noX). Abrimos un navegador e ingresamos la dirección IP del servidor. Nos conectamos con las credenciales de acceso <Usuario, Contraseña>= <root, root>y navegamos a Services >VPN ->PPTP Server.

Para habilitar el Servidor, seleccionamos la opción 'Enable' en PPTP Server. También activamos 'Broadcast Support' y desactivamos tanto 'Force MPPE Encryption', de forma que permitiremos que el cliente decida si activa o no el cifrado.

Finalmente, en el campo de 'Server IP' ingresamos 10.54.181.101 (que corresponde a la IP del router en VMnet2), establecemos el rango de direcciones 'Client IP(s)' como 10.54.181.201-209 (permitiendo hasta 9 clientes simultáneos), y en 'CHAP-Secrets' ingresamos 'admin * admin *'. Estos datos representan usuario y contraseña, separados por asteriscos y con espacios en blanco específicos que deben mantenerse.

The screenshot shows the 'PPTP Server' configuration page. The 'Services' tab is selected, and the 'PPTP Server' sub-tab is active. The configuration includes:

- PPTP Server:** ☒ Enable ☐ Disable
- Broadcast support:** ☒ Enable ☐ Disable
- Force MPPE Encryption:** ☐ Enable ☒ Disable
- DNS1:** [Empty text box]
- DNS2:** [Empty text box]
- WINS1:** [Empty text box]
- WINS2:** [Empty text box]
- Server IP:** 10.54.181.101
- Client IP(s):** 10.54.181.201-209
- CHAP-Secrets:** admin * admin *
- Radius:** ☐ Enable ☒ Disable

Figura 3.1: Configuración PPTP Server

Tras realizar dicha configuración, puesto que el PPTP usa el puerto TCP 1723, crearemos una redirección del puerto público al servidor PPTP. Aunque podría no ser necesario porque el servidor PPTP está configurado para usar la IP local, ya que es el propio router. Pero para evitar inconvenientes, realizaremos la redirección de puertos. Esto lo haremos desde la pestaña NAT/QoS >Port Forwarding (ver figura 3.2)

The screenshot shows the 'Port Forwarding' configuration page. The 'NAT / QoS' tab is selected, and the 'Port Forwarding' sub-tab is active. The configuration includes:

Application	Port from	Protocol	IP Address	Port to	Enable
pptp	1723	TCP	10.54.181.101	1723	<input checked="" type="checkbox"/>

Buttons: Add, Remove, Save, Apply Settings, Cancel Changes

Figura 3.2: Redirección en ddwrt-x

Además, añadiremos una nueva regla de routing para así indicarle al servidor que debe de hacer con los datagramas cuyo destino sea la red del cliente (10.24.181.0/24). Esto lo haremos desde la Setup >Advanced Routing >Operating Mode seleccionamos 'Gateway', le asignamos un nombre a nuestro router, en 'Metric' la dejamos a 0, en 'Destination LAN NET' colocamos 10.24.181.0 con máscara de red 255.255.255.0 y en 'Gateway' 10.24.181.1. Por último, es importante que coloquemos como interfaz 'ANY'. Todo esta configuración se muestra en la figura 3.3

The screenshot shows the configuration interface for ddwrt-X. The top navigation bar includes tabs for Setup, Services, Security, Access Restrictions, NAT / QoS, Administration, and Status. Below this, there are sub-tabs for Basic Setup, DDNS, MAC Address Clone, Advanced Routing, Networking, and EoIP Tunnel. The 'Advanced Routing' tab is selected, and the 'Operating Mode' is set to 'Gateway'. Under the 'Static Routing' section, a new rule is being configured with the following details:

- Select set number: 1 (a-ddwr-noX-via-PPTP) [Delete]
- Route Name: a-ddwr-noX-via-PPTP
- Metric: 0
- Destination LAN NET: 10.24.181.0
- Subnet Mask: 255.255.255.0
- Gateway: 10.24.181.1
- Interface: ANY

At the bottom of the configuration area, there are buttons for 'Save', 'Apply Settings', and 'Cancel Changes'.

Figura 3.3: Nueva regla de enrutamiento en ddwrt-X

3.1.2. Configuración de cliente PPTP (ddwrt-noX)

Una vez tenemos la configuración del servidor PPTP, procedemos al cliente PPTP. En primer lugar, hay que indicar la IP pública del servidor PPTP en el campo 'Sever IP or DNS Name', en nuestro caso escribimos la IP de ddwrt-X, es decir, 192.168.159.129, que es el que acabamos de configurar como servidor PPTP en los pasos anteriores. Luego indicamos en 'Remote Subnet' la 10.54.181.0 y en 'Remote Subnet Mask' la máscara 255.255.255.0, el cifrado, en este cliente vamos a optar por activarlo, por lo que en 'MPPE Encryption' le colocamos 'mppe required', ya que los paquetes del cliente estarán comprimidos dentro del túnel, lo que dificultará la lectura del datagrama. Por lo tanto, es conveniente activarlo.

En cambio, debemos de desactivar la NAT porque los mensajes ya están viajando a través del túnel, y por último, rellenaremos los campos 'User Name' y 'Password' como admin, admin respectivamente. Todos estos cambios podemos observarlo en la figura 3.4

The screenshot shows the 'Services' tab in the dd-wrt configuration interface. Under the 'VPN' sub-tab, the 'PPTP Client' section is expanded. The 'PPTP Server' is set to 'Disable'. The 'PPTP Client Options' are set to 'Enable'. The 'Server IP or DNS Name' is '192.168.159.129'. The 'Remote Subnet' is '10.54.181.0' and the 'Remote Subnet Mask' is '255.255.255.0'. The 'MPPE Encryption' is set to 'mppe required'. The 'MTU' and 'MRU' are both set to '1450', with '(Default: 1450)' noted next to each. The 'NAT' option is set to 'Disable'. The 'User Name' is 'admin' and the 'Password' is masked with dots. There is an 'Unmask' checkbox next to the password field.

Figura 3.4: Configuración del cliente PPTP en ddwrt-noX

Cabe destacar que los valores de los campos de MTU y MRU los dejamos con sus valores por defecto: 1450. Por varias razones clave.

- **Sobrecarga por cabeceras:** Al usar PPTP, se agregan cabeceras de los protocolos GRE (24 Bytes) e IP (20-24 Bytes). Esto reduce el espacio disponible para los datos transmitidos. El tamaño máximo de MTU para redes Ethernet es 1500 Bytes, por lo que el valor más grande que se puede configurar para los datos es 1456 Bytes. Dejando 1450, se evita exceder el límite de 1500 Bytes cuando se suman las cabeceras.
- **Compatibilidad y rendimiento:** El valor 1450 es estándar y adecuado para la mayoría de redes que usan PPTP, evitando fragmentación de los paquetes, lo que podría afectar el rendimiento y la estabilidad.
- **Prevención de problemas:** Si se usan valores mayores, los paquetes podrían exceder el tamaño máximo permitido, lo que causaría fragmentación y posibles pérdidas de datos. Usar 1450 minimiza este riesgo.

Una vez configurado el cliente, tenemos que asegurarnos que el NAT es compatible con clientes PPTP de la red local, verificaremos que está habilitada la opción 'PPTP Passthrough' como en la figura 3.5, para ello nos dirigimos a Security > VPN Passthrough.

The screenshot shows the 'Security' tab in the dd-wrt configuration interface. Under the 'VPN Passthrough' sub-tab, the 'Virtual Private Network (VPN)' section is expanded. The 'VPN Passthrough' section shows three options: 'IPSec Passthrough', 'PPTP Passthrough', and 'L2TP Passthrough', all of which are set to 'Enable'. A 'Help' link is available. A note on the right states: 'You may choose to enable IPSec, PPTP and/or L2TP passthrough to allow your network devices to communicate via VPN.' At the bottom, there are buttons for 'Save', 'Apply Settings', and 'Cancel Changes'.

Figura 3.5: Verificación de la opción PPTP Passthrough

Una vez que todo esté configurado, es necesario reiniciar los routers para que el túnel PPTP entre en funcionamiento. Esto se realiza accediendo a ambos routers ddwrt, primero al servidor y luego al cliente, y seleccionando Administration >Management >Reboot Router (ver figura 3.6)

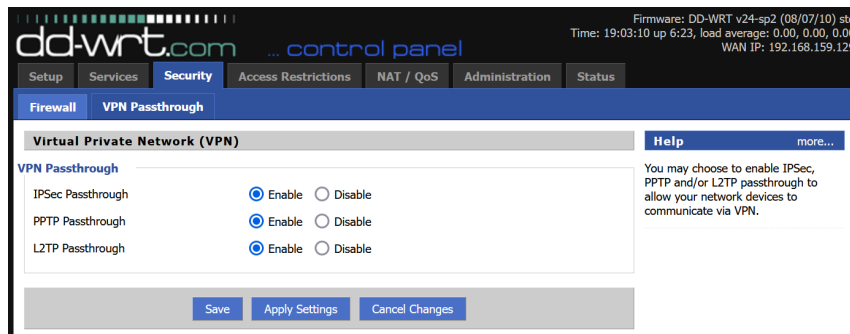


Figura 3.6: Opcion Reboot Router

Una vez finalizados ambos reinicios, volvemos a iniciar sesión. Como podemos observar en las siguientes imágenes hay una nueva interfaz llamada ppp0 y nuevas entradas en las tablas de routing vinculadas a dichas interfaces, tal y como se aprecia en la figura 3.7 y 3.8.

```
ppp0      Link encap:Point-to-Point Protocol
          inet addr:10.54.181.101  P-t-P:10.24.181.1  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1442  Metric:1
          RX packets:10  errors:0  dropped:0  overruns:0  frame:0
          TX packets:10  errors:0  dropped:0  overruns:0  carrier:0
          collisions:0 txqueuelen:3
          RX bytes:151 (151.0 B)  TX bytes:157 (157.0 B)

root@DD-WRT:~# ip route
10.24.181.1 dev ppp0 proto kernel scope link src 10.54.181.101
192.168.159.2 dev eth0 scope link
10.24.181.0/24 via 10.24.181.1 dev ppp0
10.54.181.0/24 dev br0 proto kernel scope link src 10.54.181.101
192.168.159.0/24 dev eth0 proto kernel scope link src 192.168.159.129
169.254.0.0/16 dev br0 proto kernel scope link src 169.254.255.1
127.0.0.0/8 dev lo scope link
default via 192.168.159.2 dev eth0
root@DD-WRT:~#
```

Figura 3.7: Comprobación de interfaces y tabla de rout ddwrt-X

```
ppp0      Link encap:Point-to-Point Protocol
          inet addr:10.24.181.1  P-t-P:10.54.181.101  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1438  Metric:1
          RX packets:10  errors:0  dropped:0  overruns:0  frame:0
          TX packets:10  errors:0  dropped:0  overruns:0  carrier:0
          collisions:0 txqueuelen:3
          RX bytes:157 (157.0 B)  TX bytes:151 (151.0 B)

root@DD-WRT:~# ip route
192.168.159.2 dev eth0 scope link
10.54.181.101 dev ppp0 proto kernel scope link src 10.24.181.1
10.24.181.0/24 dev br0 proto kernel scope link src 10.24.181.1
10.54.181.0/24 dev ppp0 scope link
192.168.159.0/24 dev eth0 proto kernel scope link src 192.168.159.128
169.254.0.0/16 dev br0 proto kernel scope link src 169.254.255.1
127.0.0.0/8 dev lo scope link
default via 192.168.159.2 dev eth0
root@DD-WRT:~#
```

Figura 3.8: Comprobación de interfaces y tabla de rout ddwrt-noX

3.2 Pruebas de funcionamiento

El túnel PPTP en modo site-to-site nos permitirá la comunicación entre dispositivos ubicados en la Vnet1 y aquellos ubicados en la Vnet2. Para verificar que esto es cierto se realizará una prueba de conectividad mediante un ping entre los routers RCO-noX y RCO-X. El comportamiento esperado será que el ping de RCO-noX llegue sin problemas a RCO-X.

```
[root@rco-nox ~]# ping 10.54.181.105
PING 10.54.181.105 (10.54.181.105) 56(84) bytes of data.
64 bytes from 10.54.181.105: icmp_seq=1 ttl=62 time=1.32 ms
64 bytes from 10.54.181.105: icmp_seq=2 ttl=62 time=1.47 ms
64 bytes from 10.54.181.105: icmp_seq=3 ttl=62 time=1.13 ms
64 bytes from 10.54.181.105: icmp_seq=4 ttl=62 time=1.14 ms
64 bytes from 10.54.181.105: icmp_seq=5 ttl=62 time=1.30 ms

--- 10.54.181.105 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 1.125/1.270/1.468/0.126 ms
[root@rco-nox ~]#
```

Figura 3.9: ping de RCO-noX a RCO-X

De acuerdo con lo esperado, la prueba de conectividad mediante ping se llevó a cabo con éxito. Durante la ejecución del ping, se realizó un análisis del tráfico de red utilizando Wireshark en las interfaces correspondientes a las redes VMnet1 y VMnet8, con el objetivo de examinar el flujo de paquetes y evaluar el comportamiento del tráfico a través del túnel configurado.

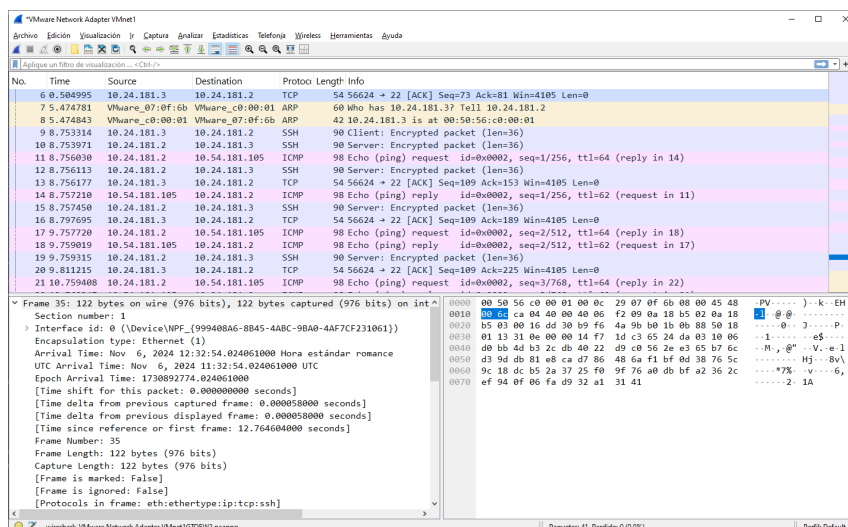


Figura 3.10: Captura de paquetes de RCO-noX a RCO-X en VMnet1

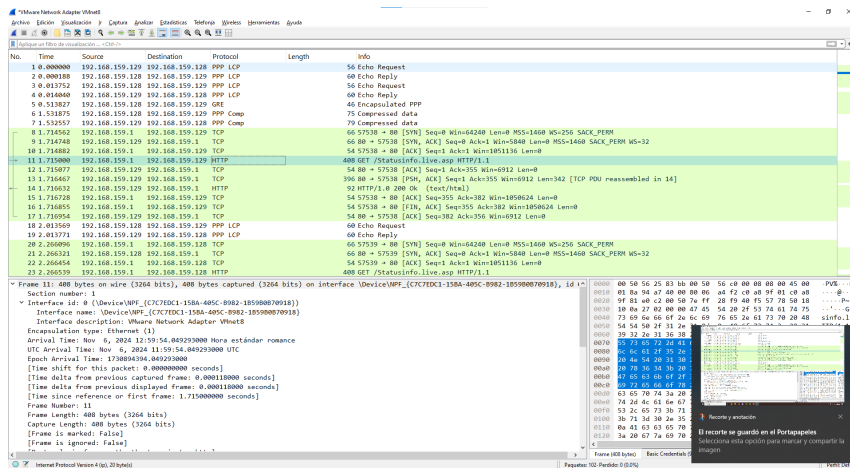


Figura 3.11: Captura de paquetes de RCO-noX a RCO-X en Vmnet8

En las capturas de tráfico realizadas tanto en la red Vmnet1 como en la Vmnet8, se pueden identificar varios paquetes correspondientes a distintos protocolos, los cuales serán analizados a continuación.

El primer tipo de paquete observado corresponde al protocolo ARP (Address Resolution Protocol). Este protocolo se emplea para mapear direcciones IP a direcciones MAC dentro de una red local. Cuando un dispositivo necesita comunicarse con otro en la misma red y solo dispone de la dirección IP de destino, ARP permite obtener la dirección MAC correspondiente mediante una solicitud de tipo broadcast. En respuesta, el dispositivo de destino proporciona su dirección MAC, lo que facilita la comunicación a nivel de enlace de datos.

A continuación, se identifican paquetes de tipo PPP LCP (Link Control Protocol) y PPP Comp (compresión). Los paquetes PPP LCP tienen como función negociar y gestionar la conexión entre los dos extremos de la comunicación, garantizando que ambos dispositivos estén configurados adecuadamente para el intercambio de datos. Por otro lado, los paquetes PPP Comp se utilizan para comprimir los datos antes de ser transmitidos a través del túnel, optimizando así el uso del ancho de banda y mejorando la eficiencia de la transmisión de información.

Seguidamente podemos observar paquetes de tipo GRE (Generic Routing Encapsulation). El protocolo GRE se usa para transportar los paquetes de datos del túnel. Por lo tanto, los paquetes enviados a través del túnel se encapsulan en un encabezado GRE. En este contexto, GRE encapsula el protocolo PPP.

Finalmente, en la captura realizada en Vmnet1, se pueden distinguir paquetes de tipo ICMP. El protocolo ICMP (Internet Control Message Protocol) es un protocolo de control que se utiliza para enviar mensajes de error o para proporcionar información de diagnóstico, como es el caso de los paquetes generados por un comando ping.

Cuando se realiza un ping entre dispositivos conectados a través del túnel, los paquetes ICMP se encapsulan dentro del túnel para ser transmitidos entre los extremos. En las capturas de red, los datos ICMP correspondientes al ping no se visualizarán de manera directa, a menos que el túnel no esté cifrado. En el caso de que el túnel estuviera cifrado, únicamente se observarían los paquetes GRE (Generic Routing Encapsulation) que contienen los datos ICMP cifrados, sin poder acceder a los detalles específicos del ping o su contenido. Dado que nuestro túnel está cifrado, debemos suponer que los paquetes ICMP no fueron ocasionados por el ping realizado.

Finalmente, cabe destacar que en Vmnet8 no se pueden visualizar paquetes de tipo ARP ni de tipo ICMP. La razón de ello es la manera en la que está configurada el túnel, puesto que es en Vmnet8 donde está situado el túnel y por donde viaja el tráfico de nivel 2.

A continuación, se llevará a cabo una prueba de conectividad mediante ping entre el PC anfitrión y el router RCO-X. A diferencia del ping realizado en el apartado anterior, este no debería ser exitoso.

```
[root@rco-nox ~]# ip route
default via 10.24.181.1 dev ens37 proto static metric 100
10.24.181.0/24 dev ens37 proto kernel scope link src 10.24.181.2 metric 100
[root@rco-nox ~]# ping 10.54.181.105
PING 10.54.181.105 (10.54.181.105) 56(84) bytes of data.

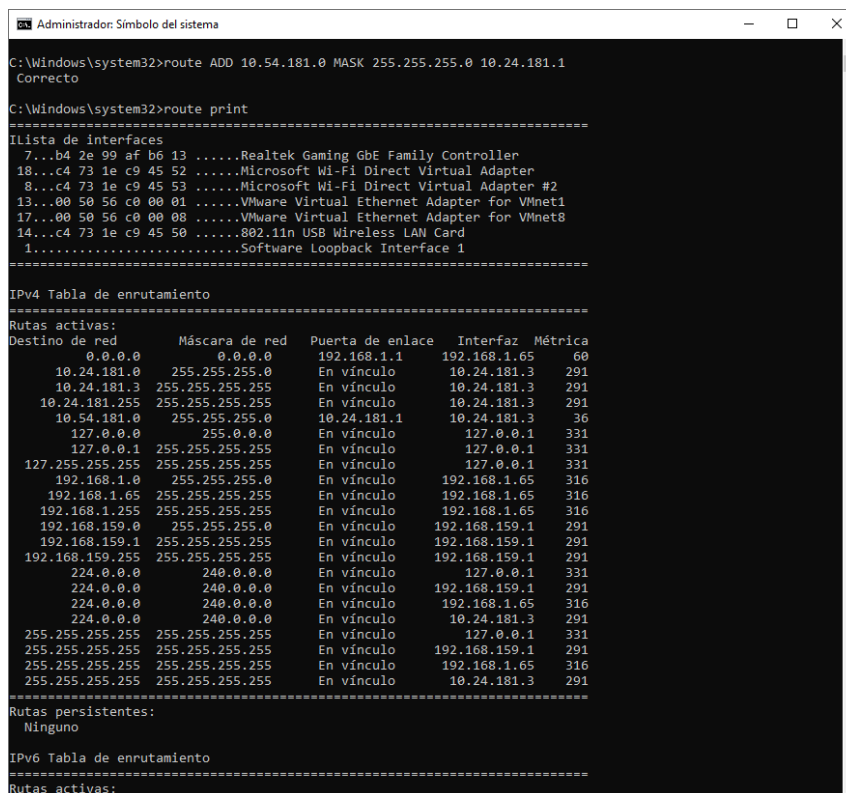
--- 10.54.181.105 ping statistics ---
109 packets transmitted, 0 received, 100% packet loss, time 110622ms

[root@rco-nox ~]# █
```

Figura 3.12: ping anfitrión a RCO-x no funciona

Efectivamente, a diferencia del ping realizado entre los routers RCO-noX y RCO-X, el PC anfitrión no puede realizar un ping exitoso hacia RCO-X, a pesar de que ambas máquinas se encuentran en la misma red VMnet1. La razón de este comportamiento radica en que en la tabla de encaminamiento del PC anfitrión no figura una ruta hacia la red VMnet2.

Para habilitar la conectividad entre el PC anfitrión y RCO-X, será necesario agregar una entrada en la tabla de encaminamiento del PC anfitrión que apunte hacia la red 10.54.181.0, correspondiente a VMnet2. Esto permitirá que el PC anfitrión pueda enrutar correctamente los paquetes hacia dicha red y, por ende, lograr la comunicación con RCO-X. Esta modificación la realizaremos mediante el comando `route add <ip>mask <máscara><puerta de enlace>`.



```

C:\Windows\system32>route ADD 10.54.181.0 MASK 255.255.255.0 10.24.181.1
Correcto

C:\Windows\system32>route print

=====
Lista de interfaces
=====
7...b4 2e 99 af b6 13 .....Realtek Gaming GbE Family Controller
18...c4 73 1e c9 45 52 .....Microsoft Wi-Fi Direct Virtual Adapter
8...c4 73 1e c9 45 53 .....Microsoft Wi-Fi Direct Virtual Adapter #2
13...00 50 56 c0 00 01 .....VMware Virtual Ethernet Adapter for VMnet1
17...00 50 56 c0 00 08 .....VMware Virtual Ethernet Adapter for VMnet8
14...c4 73 1e c9 45 50 .....802.11n USB Wireless LAN Card
1.....Software Loopback Interface 1
=====

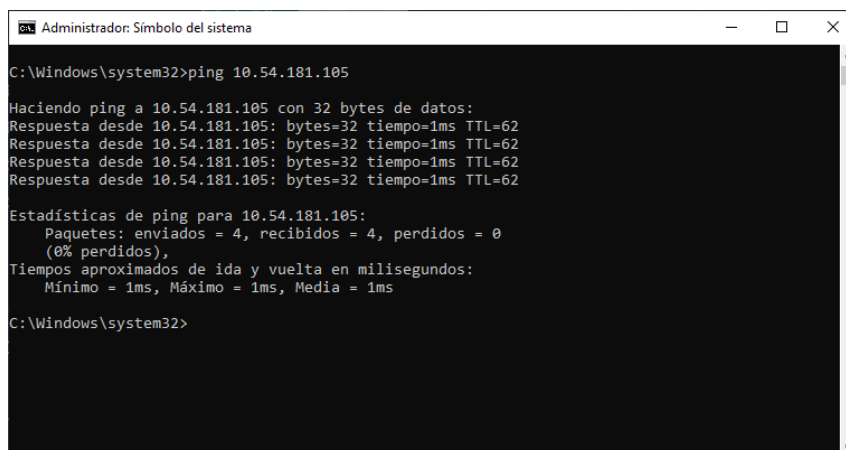
IPv4 Tabla de enrutamiento
=====
Rutas activas:
Destino de red      Máscara de red      Puerta de enlace    Interfaz  Métrica
0.0.0.0             0.0.0.0             192.168.1.1         192.168.1.65 60
10.24.181.0         255.255.255.0       En vínculo          10.24.181.3 291
10.24.181.3         255.255.255.255     En vínculo          10.24.181.3 291
10.24.181.255       255.255.255.255     En vínculo          10.24.181.3 291
10.54.181.0         255.255.255.0       10.24.181.1         10.24.181.3 36
127.0.0.0           255.0.0.0           En vínculo          127.0.0.1 331
127.0.0.1           255.255.255.255     En vínculo          127.0.0.1 331
127.255.255.255     255.255.255.255     En vínculo          127.0.0.1 331
192.168.1.0         255.255.255.0       En vínculo          192.168.1.65 316
192.168.1.65        255.255.255.255     En vínculo          192.168.1.65 316
192.168.1.255       255.255.255.255     En vínculo          192.168.1.65 316
192.168.150.0       255.255.255.0       En vínculo          192.168.150.1 291
192.168.150.1       255.255.255.255     En vínculo          192.168.150.1 291
192.168.150.255     255.255.255.255     En vínculo          192.168.150.1 291
224.0.0.0           240.0.0.0           En vínculo          127.0.0.1 331
224.0.0.0           240.0.0.0           En vínculo          192.168.150.1 291
224.0.0.0           240.0.0.0           En vínculo          192.168.1.65 316
224.0.0.0           240.0.0.0           En vínculo          10.24.181.3 291
255.255.255.255     255.255.255.255     En vínculo          127.0.0.1 331
255.255.255.255     255.255.255.255     En vínculo          192.168.150.1 291
255.255.255.255     255.255.255.255     En vínculo          192.168.1.65 316
255.255.255.255     255.255.255.255     En vínculo          10.24.181.3 291
=====
Rutas persistentes:
Ninguna

IPv6 Tabla de enrutamiento
=====
Rutas activas:

```

Figura 3.13: Regla de routing RCO-x y tabla de enrutamiento desde anfitrion

Una vez realizada la modificación en la tabla de encaminamiento del PC anfitrión, será posible ejecutar el ping entre el PC y RCO-X de manera exitosa.



```

C:\Windows\system32>ping 10.54.181.105

Haciendo ping a 10.54.181.105 con 32 bytes de datos:
Respuesta desde 10.54.181.105: bytes=32 tiempo=1ms TTL=62
Respuesta desde 10.54.181.105: bytes=32 tiempo=1ms TTL=62
Respuesta desde 10.54.181.105: bytes=32 tiempo=1ms TTL=62
Respuesta desde 10.54.181.105: bytes=32 tiempo=1ms TTL=62

Estadísticas de ping para 10.54.181.105:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
            (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
            Mínimo = 1ms, Máximo = 1ms, Media = 1ms

C:\Windows\system32>

```

Figura 3.14: ping anfitrión a RCO-x funciona

Como se puede observar, el PC anfitrión ya puede conectar con RCO-X.

A continuación, se utilizará el comando tracert en el PC anfitrión para analizar la ruta que toma un paquete de datos desde el PC hasta RCO-X. El comando tracert es una herramienta de diagnóstico de red en Windows que permite rastrear el camino que recorren los paquetes de datos a través de los dispositivos de la red hasta llegar al destino deseado. Cada línea de salida de tracert representa un nodo de red (normalmente un router) por el cual el paquete debe pasar para alcanzar el destino final.


```

Administrador: Símbolo del sistema
Microsoft Windows [Versión 10.0.19045.5011]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Windows\system32>tracert 10.54.181.105

Traza a 10.54.181.105 sobre caminos de 30 saltos como máximo.

 1  <1 ms  <1 ms  <1 ms  10.24.181.1
 2  <1 ms  <1 ms  <1 ms  10.54.181.101
 3   1 ms  <1 ms  <1 ms  10.54.181.105

Traza completa.

C:\Windows\system32>

```

Figura 3.15: tracert desde anfitrión a RCO-x

Al ejecutar el comando correspondiente, se observa que la ruta empleada por el PC anfitrión para llegar a RCO-X es la siguiente: 10.24.181.1 ->10.54.181.101 ->10.54.181.105. A partir de esta información, se puede deducir que el trayecto recorrido por el paquete se distribuye en tres segmentos: en primer lugar, el paquete se dirige desde el PC anfitrión a ddwrt-noX a través de la red Vmnet1; en segundo lugar, el paquete es transmitido desde ddwrt-noX a ddwrt-X utilizando un túnel PPTP; finalmente, el paquete llega a su destino, RCO-X, a través de la red VMnet2 desde ddwrt-X.

Para llevar a cabo el análisis de las trazas de red entre los nodos RCO-noX y RCO-X (y viceversa), se empleará la herramienta traceroute, que es el equivalente a la orden tracert en sistemas Linux. El primer paso para utilizar traceroute en ambas máquinas, RCO-noX y RCO-X, consiste en instalar la herramienta en dichos sistemas. Para ello, es necesario ejecutar el comando `sudo yum install traceroute` en ambas máquinas. Este comando descargará e instalará el paquete traceroute desde los repositorios del sistema, permitiendo así la ejecución de la herramienta en ambas máquinas.

```

[root@rc0-x ~]# sudo yum install traceroute
Última comprobación de caducidad de metadatos hecha hace 0:03:41, el lun 11 nov 2024 11:56:52 CET.
Dependencias resueltas.
=====
Paquete      Arquitectura  Versión      Repositorio  Tam.
=====
Instalando:
traceroute   x86_64        3:2.1.0-8.el8  baseos       66 k
=====
Resumen de la transacción
=====
Instalar 1 Paquete

Tamaño total de la descarga: 66 k
Tamaño instalado: 101 k
¿Está de acuerdo [s/N]? s
Descargando paquetes:
traceroute-2.1.0-8.el8.x86_64.rpm                503 kB/s | 66 kB    00:00
-----
Total                                           99 kB/s | 66 kB    00:00
Ejecutando verificación de operación
Verificación de operación exitosa.
Ejecutando prueba de operaciones
Prueba de operación exitosa.
Ejecutando operación
Preparando :
Instalando : traceroute-3:2.1.0-8.el8.x86_64          1/1
Ejecutando scriptlet: traceroute-3:2.1.0-8.el8.x86_64 1/1
Verificando : traceroute-3:2.1.0-8.el8.x86_64          1/1
Productos instalados actualizados.

Instalado:
traceroute-3:2.1.0-8.el8.x86_64

¡Listo!
[root@rc0-x ~]#

```

Figura 3.16: Instalacion traceroute

Una vez completada la instalación en ambos equipos, comenzaremos ejecutando traceroute desde RCO-noX a RCO-X mediante el comando `traceroute 10.54.181.105`


```
[root@rco-nox ~]# traceroute 10.54.181.105
traceroute to 10.54.181.105 (10.54.181.105), 30 hops max, 60 byte packets
 1 DD-WRT (10.24.181.1)  0.567 ms  0.403 ms  0.381 ms
 2 10.54.181.101 (10.54.181.101)  2.449 ms  2.421 ms  2.543 ms
 3 10.54.181.105 (10.54.181.105)  5.069 ms !X  5.023 ms !X  5.103 ms !X
[root@rco-nox ~]#
```

Figura 3.17: Orden traceroute desde RCO-noX a RCO-X

Tras ejecutar la herramienta traceroute, se observa que la ruta seguida por el paquete de datos es 10.42.181.1 ->10.54.181.101 ->10.54.181.105 A partir de este recorrido, se puede deducir que el trayecto de un paquete con origen en RCO-noX y destino en RCO-X sigue los siguientes pasos:

1. El paquete se traslada desde RCO-noX hacia el dispositivo ddwrt-noX a través de la red VMnet1.
2. Desde ddwrt-noX, el paquete continúa su trayecto hacia el dispositivo ddwrt-X mediante el túnel PPTP.
3. Finalmente, el paquete llega a RCO-X a través de la red VMnet2.

Ahora volveremos a ejecutar el traceroute pero esta vez en sentido contrario, desde RCO-X a RCO-noX.

```
[root@rco-x ~]# traceroute 10.24.181.2
traceroute to 10.24.181.2 (10.24.181.2), 30 hops max, 60 byte packets
 1 gateway (10.54.181.101)  0.301 ms  0.208 ms  0.170 ms
 2 10.24.181.1 (10.24.181.1)  2.234 ms  2.218 ms  2.132 ms
 3 10.24.181.2 (10.24.181.2)  2.329 ms !X  2.896 ms !X  2.857 ms !X
[root@rco-x ~]#
```

Figura 3.18: Orden traceroute desde RCO-X a RCO-noX

AL ejecutar traceroute esta vez en RCO-X, se observa que la ruta seguida por el paquete de datos esta vez es 10.54.181.101 ->10.24.181.1 ->10.24.181.2 A partir de este recorrido, se puede deducir que el trayecto de un paquete con origen en RCO-X y destino en RCO-noX sigue los siguientes pasos:

1. El paquete se traslada desde RCO-X hacia ddwrt-X a través de la red VMnet2.
2. Desde ddwrt-X, el paquete continúa su trayecto hacia ddwrt-noX mediante el túnel PPTP.
3. Finalmente, el paquete llega a RCO-noX a través de la red VMnet1.

Finalmente, procederemos a mostrar las tablas de enrutamiento de ddwrt-noX, ddwrt-X, RCO-x y RCO-noX, utilizando el comando ip route. Este comando permite consultar las rutas configuradas en cada dispositivo, proporcionando información sobre el encaminamiento de los paquetes de datos a través de la red.

El análisis comenzará con la visualización de la tabla de enrutamiento de RCO-X.

```
[root@rco-x ~]# ip route
default via 10.54.181.101 dev ens37 proto dhcp src 10.54.181.105 metric 100
10.54.181.0/24 dev ens37 proto kernel scope link src 10.54.181.105 metric 100
[root@rco-x ~]#
```

Figura 3.19: ip route de RCO-X

La línea correspondiente a default en la tabla de enrutamiento indica la puerta de enlace predeterminada para el tráfico de red que no coincide con otras rutas más específicas. En este caso, todo el tráfico que no se ajusta a una ruta definida previamente será dirigido hacia la dirección IP 10.54.181.101, que actúa como la puerta de enlace predeterminada, y por lo tanto, serán enviados a ddwrt-x.

Este tráfico se enviará a través de la interfaz de red ens37, que es la interfaz configurada para gestionar este tipo de tráfico. Además, el protocolo DHCP (Dynamic Host Configuration Protocol) ha sido utilizado para establecer esta ruta, lo que significa que la configuración de la puerta de enlace y otros parámetros de red fueron obtenidos automáticamente desde un servidor DHCP.

En cuanto al parámetro SRC (source), se observa que la dirección IP de origen es 10.54.181.105, que corresponde a la dirección IP del propio dispositivo RCO-X. Finalmente, el parámetro metric indica la prioridad de la ruta en caso de existir múltiples rutas disponibles para un destino. En este caso, el valor de la métrica es 100.

La segunda línea en la tabla de enrutamiento corresponde a una ruta específica, que abarca la subred 10.54.181.0/24. Esta subred incluye todas las direcciones IP comprendidas entre 10.54.181.0 y 10.54.181.255. La ruta está asociada a la interfaz de red ens37, lo que significa que el tráfico destinado a esta subred será encaminado a través de dicha interfaz. Como se puede observar, independientemente de que sea default o una ruta específica, siempre se va a usar la misma interfaz de red, ens37.

El protocolo kernel indica que esta ruta fue agregada de manera automática por el núcleo del sistema operativo, como parte de la configuración de la interfaz de red.

En cuanto al parámetro scope, se especifica que el alcance de la ruta es de tipo link, lo que implica que la ruta solo es válida para dispositivos que están directamente conectados dentro de la misma subred.

Finalmente, los valores de la IP de origen y la métrica son los mismos que en la ruta default. Continuamos ejecutando ip route en RCO-noX

```
[root@rco-nox ~]# ip route
default via 10.24.181.1 dev ens37 proto static metric 100
10.24.181.0/24 dev ens37 proto kernel scope link src 10.24.181.2 metric 100
[root@rco-nox ~]#
```

Figura 3.20: ip route de RCO-noX

Como en RCO-X, RCO-noX solamente tiene definida una ruta específica además de la default. Como en el caso anterior, siempre se va a usar la interfaz de red ens 37. Continuando, ahora ejecutaremos ip route sobre ddwrt-X.

```
root@DD-WRT:~# ip route
10.24.181.1 dev ppp0 proto kernel scope link src 10.54.181.101
192.168.159.2 dev eth0 scope link
10.24.181.0/24 via 10.24.181.1 dev ppp0
10.54.181.0/24 dev br0 proto kernel scope link src 10.54.181.101
192.168.159.0/24 dev eth0 proto kernel scope link src 192.168.159.129
169.254.0.0/16 dev br0 proto kernel scope link src 169.254.255.1
127.0.0.0/8 dev lo scope link
default via 192.168.159.2 dev eth0
root@DD-WRT:~#
```

Figura 3.21: ip route de ddwrt-X

A diferencia de los casos anteriores, este escenario presenta una estructura de enrutamiento más compleja, que involucra el uso de distintas interfaces de red. En este caso, se observan varias rutas asociadas a direcciones IP y subredes específicas, cada una con su propia interfaz de salida.

Para la dirección IP 192.168.159.2, que pertenece a la subred 192.168.159.0/24 y que se encuentra dentro de la ruta default, se utilizará la interfaz de red eth0. Esto implica que los paquetes destinados a esta subred serán encaminados hacia el dispositivo ddwrt-noX a través de esta interfaz.

En la dirección IP 10.24.181.1 y en la subred 169.254.0.0/16, la ruta se asociará con la interfaz ppp0, lo que indica que se está utilizando una conexión de Protocolo Punto a Punto (PPP). Esta conexión es utilizada para el túnel PPTP.

Finalmente, en las subredes 10.54.181.0/24 y 169.254.0.0/16, se utilizará la interfaz br0. Esto significa que los paquetes destinados a estas subredes serán enviados a través de esta interfaz, encaminándolos hacia el dispositivo RCO-X. Por último, analizaremos el ip route en ddwrt-noX.

```
root@DD-WRT:~# ip route
192.168.159.2 dev eth0 scope link
10.54.181.101 dev ppp0 proto kernel scope link src 10.24.181.1
10.24.181.0/24 dev br0 proto kernel scope link src 10.24.181.1
10.54.181.0/24 dev ppp0 scope link
192.168.159.0/24 dev eth0 proto kernel scope link src 192.168.159.128
169.254.0.0/16 dev br0 proto kernel scope link src 169.254.255.1
127.0.0.0/8 dev lo scope link
default via 192.168.159.2 dev eth0
root@DD-WRT:~#
```

Figura 3.22: ip route de ddwrt-noX

Muy similar al ip route en ddwrt-X, únicamente cambia, como es lógico al tratarse de máquinas distintas, las salidas de las interfaces de red.

CAPÍTULO 4

Funcionamiento del túnel PPTP remote-access

El túnel PPTP de acceso remoto hace posible la conexión remota de los usuarios a una red a través de Internet u otras redes, utilizando una infraestructura de túnel cifrado. Este protocolo se basa en encapsular paquetes de datos dentro de otros paquetes, de manera que se transportan a través de redes públicas de forma segura. Para ello, un cliente PPTP establece una conexión con un servidor PPTP en la red, creando un "túnel" seguro sobre la red pública. Este túnel asegura que los datos transmitidos estén cifrados y protegidos mientras viajan entre el cliente remoto y la red interna.

El tráfico de datos del usuario se encapsula en paquetes que son enviados de manera segura por el túnel hasta el servidor remoto, donde se desenscriptan y se dirigen a la red interna. Esto garantiza la privacidad e integridad de la información.

Para proceder con la configuración de una nueva conexión remota desde el anfitrión a ddwrt-noX, desactivaremos el cliente PPTP que ha sido previamente creado desde la configuración del router ddwrt-noX. Una vez desactivado el cliente PPTP en el router ddwrt-noX, procederemos a crear una nueva conexión VPN por PPTP desde el PC anfitrión.

4.1 Configuración y verificación

En primer lugar, desde la configuración del router ddwrt-noX, se procede con al desactivación del cliente PPTP. Esto se puede verificar, realizando un ping desde RCO-noX a RCO-X, y viendo que no funciona, como se muestra en la Figura 4.1.

```
[root@rco-nox ~]# ip route
default via 10.24.181.1 dev ens37 proto static metric 100
10.24.181.0/24 dev ens37 proto kernel scope link src 10.24.181.2 metric 100
[root@rco-nox ~]# ping 10.54.181.105
PING 10.54.181.105 (10.54.181.105) 56(84) bytes of data.
--- 10.54.181.105 ping statistics ---
109 packets transmitted, 0 received, 100% packet loss, time 110622ms
[root@rco-nox ~]#
```

Figura 4.1: ping de RCO-noX a RCO-X no funciona

También, se puede observar en la Figura 4.2, como al ejecutar el comando `ifconfig` en la máquina `ddwrt-noX`, la interfaz `pp0` ya no aparece.

```
root@DD-WRT:~# ifconfig
br0      Link encap:Ethernet  HWaddr 00:50:56:2C:2A:18
         inet addr:10.24.181.1  Bcast:10.24.181.255  Mask:255.255.255.0
         UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
         RX packets:207 errors:0 dropped:0 overruns:0 frame:0
         TX packets:5 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:0
         RX bytes:15953 (15.5 KiB)  TX bytes:210 (210.0 B)

br0:0    Link encap:Ethernet  HWaddr 00:50:56:2C:2A:18
         inet addr:169.254.255.1  Bcast:169.254.255.255  Mask:255.255.0.0
         UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1

eth0     Link encap:Ethernet  HWaddr 00:50:56:21:35:CA
         inet addr:192.168.159.128  Bcast:192.168.159.255  Mask:255.255.255.0
         UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
         RX packets:1160 errors:0 dropped:0 overruns:0 frame:0
         TX packets:2116 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:1000
         RX bytes:128947 (125.9 KiB)  TX bytes:1993953 (1.9 MiB)
         Interrupt:5 Base address:0x2000

eth1     Link encap:Ethernet  HWaddr 00:50:56:2C:2A:18
         UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
         RX packets:211 errors:0 dropped:0 overruns:0 frame:0
         TX packets:5 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:1000
         RX bytes:19187 (18.7 KiB)  TX bytes:210 (210.0 B)
         Interrupt:9 Base address:0x2080

lo       Link encap:Local Loopback
         inet addr:127.0.0.1  Mask:255.0.0.0
         UP LOOPBACK RUNNING MULTICAST  MTU:16436  Metric:1
         RX packets:20 errors:0 dropped:0 overruns:0 frame:0
         TX packets:20 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:0
         RX bytes:1260 (1.2 KiB)  TX bytes:1260 (1.2 KiB)

root@DD-WRT:~#
```

Figura 4.2: `ifconfig` de `ddwrt-noX` `pp0` no aparece

El objetivo de crear una conexión VPN de acceso remoto (`remote-access`) en la máquina anfitrión hasta `ddwrt-noX`, es permitir que un usuario individual se conecte a la red local del router a través de la red. A diferencia de una VPN `site-to-site`, que conecta redes completas entre sí, una conexión de acceso remoto está diseñada para que un solo cliente tenga acceso directo a los recursos de la red, como si estuviera conectado físicamente a esta.

En este tipo de configuración, el PC Windows actúa como el cliente VPN que inicia la conexión, mientras que el router se configura como el servidor VPN. Para ello, es necesario crear una conexión VPN al router, como podemos ver en la Figura 4.3

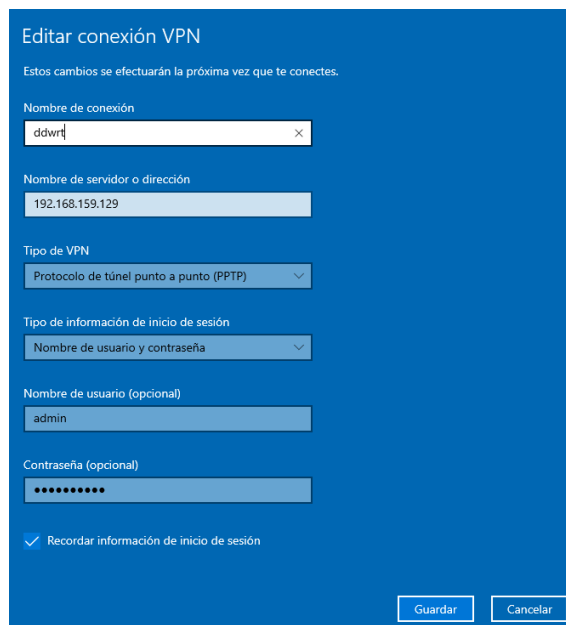


Figura 4.3: Creacion de conexion a ddwrt-noX

Al conectar el pc anfitrión a la VPN, todo el tráfico va dirigido al router ddwrt-noX, esto incluye también el tráfico de internet que se redirige a través del túnel PPTP hacia el router remoto.

Se puede observar en la Figura 4.4 como al ejecutar un tracert a 8.8.8.8, el pc anfitrión envía un paquete a dns.google y este paquete se envía al router ddwrt-noX. Como la red NAT usa nuestro ordenador para salir Internet, esta envía el paquete al router de nuevo, lo que genera un bucle infinito.

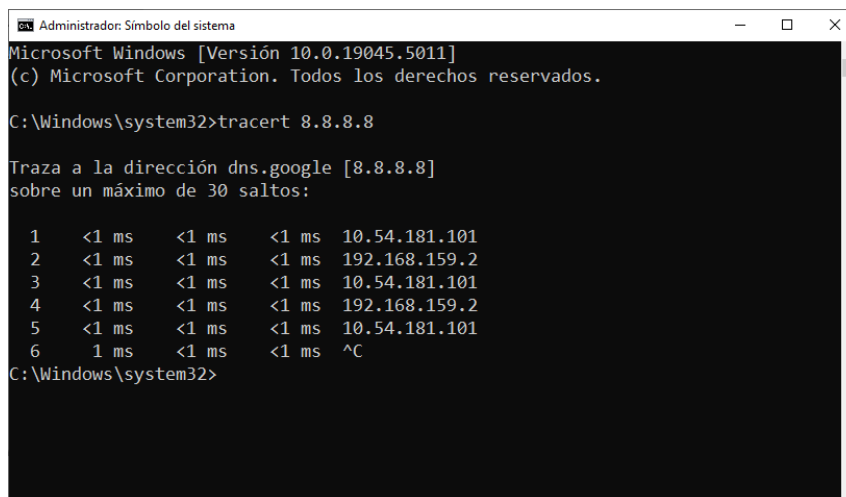


Figura 4.4: Tracert en anfitrion, bucle infinito

Para solucionar este problema, simplemente deshabilitamos la opción usar la puerta de enlace predeterminada en la red remota, Figura 4.5.

Al desactivar esta opción, se evita que todo el tráfico se envíe por el túnel VPN. Solo el tráfico dirigido a la red remota se enviará a través de la VPN, mientras que el tráfico de Internet o de otras redes, continuará usando la puerta de enlace predeterminada local, como el router de casa.

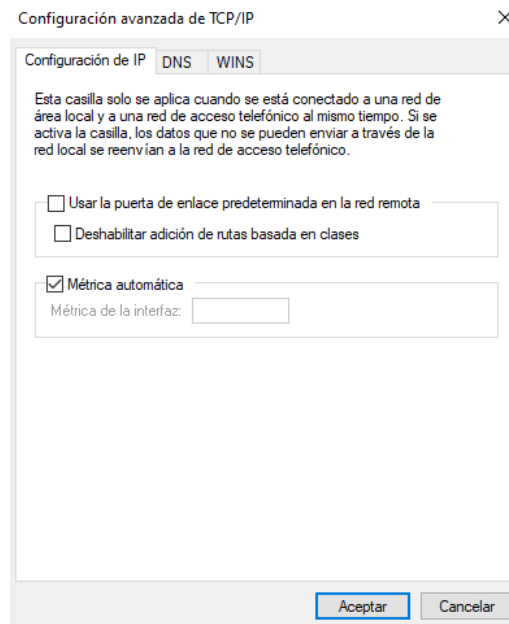


Figura 4.5: vpn config3

Además, para poder identificar correctamente las tramas enviadas a través del túnel PPTP, desactivaremos la opción Habilitar la compresión por software Figura 4.6 y en Seguridad, quitamos el cifrado Figura 4.7.

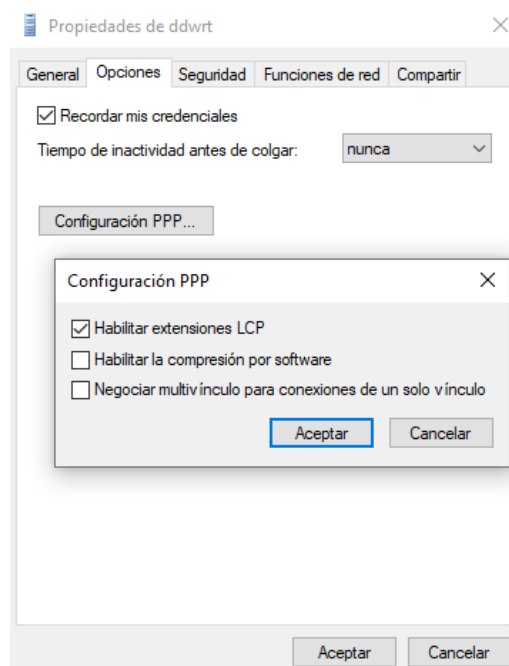


Figura 4.6: vpn config1

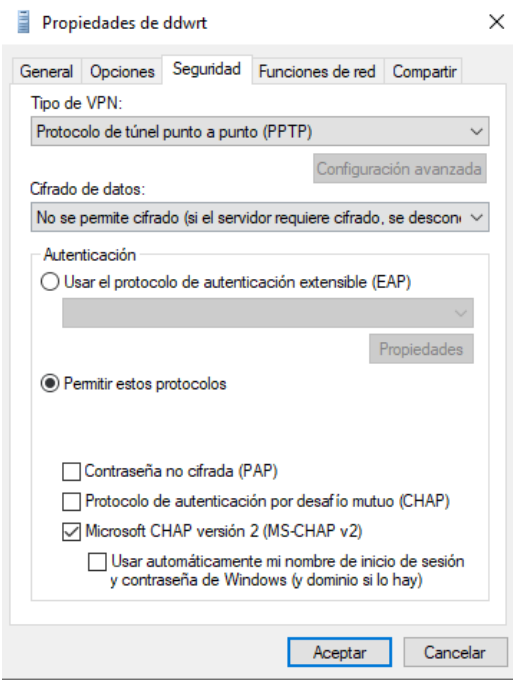


Figura 4.7: vpn config2

Para verificar el correcto funcionamiento de la conexión remota, ejecutamos nuevamente la orden `tracert 8.8.8.8` y observamos que el primer salto en la traza es hacia liveboxfibra, el router de casa.

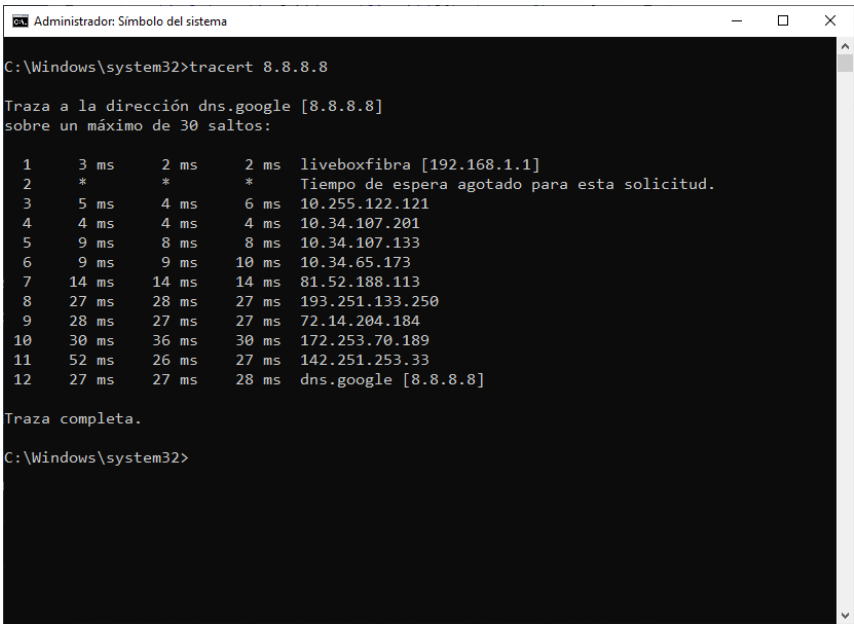


Figura 4.8: Tracert en anfitrion correcto funcionamiento

La primera línea de la Figura 4.9 es la configuración de la interfaz `ppp0`. Muestra que el router está utilizando el protocolo PPTP para crear un túnel de acceso remoto y la dirección `10.54.181.201` está asignada a esta interfaz.

La línea src 10.54.181.101 indica lo que será la IP origen del router cuando el tráfico sea enviado a través del túnel.

En la conexión site-to-site, el túnel VPN conecta dos redes completas. Todo el tráfico de la red de un sitio es enrutado hacia la red del otro sitio a través del túnel VPN.

En las conexiones remote-access, el túnel VPN conecta un solo dispositivo a la red. Esto significa que solo el tráfico de ese dispositivo pasa por el túnel, y no toda la red.

Comparando la tabla de routing de site-to-site con remote-access, en site-to-site se añade 10.24.181.0/24 via 10.24.181.1 dev ppp0, lo que indica que toda la subred 10.24.181.0/24 encamina a través del túnel VPN, ampliando la red. De lo contrario, en remote-access, la ruta se configura de manera que solo la ruta de un cliente individual concreto, pase por el túnel.

```
root@DD-WRT:~# ip route
10.54.181.201 dev ppp0 proto kernel scope link src 10.54.181.101
192.168.159.2 dev eth0 scope link
10.54.181.0/24 dev br0 proto kernel scope link src 10.54.181.101
192.168.159.0/24 dev eth0 proto kernel scope link src 192.168.159.129
169.254.0.0/16 dev br0 proto kernel scope link src 169.254.255.1
127.0.0.0/8 dev lo scope link
default via 192.168.159.2 dev eth0
root@DD-WRT:~# ifconfig ppp0
ppp0      Link encap:Point-to-Point Protocol
          inet addr:10.54.181.101 P-t-P:10.54.181.201 Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST MTU:1400 Metric:1
          RX packets:10111 errors:0 dropped:0 overruns:0 frame:0
          TX packets:264 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:3
          RX bytes:700627 (684.2 KiB) TX bytes:36639 (35.7 KiB)

root@DD-WRT:~#
```

Figura 4.9: ip route y ifconfig ppp0 de ddwrt-X tras configurar vpn

```

C:\Users\Diego>route print

=====
Lista de interfaces
7...b4 2e 99 af b6 13 .....Realtek Gaming GbE Family Controller
18...c4 73 1e c9 45 52 .....Microsoft Wi-Fi Direct Virtual Adapter
8...c4 73 1e c9 45 53 .....Microsoft Wi-Fi Direct Virtual Adapter #2
13...00 50 56 c0 00 01 .....VMware Virtual Ethernet Adapter for VMnet1
17...00 50 56 c0 00 08 .....VMware Virtual Ethernet Adapter for VMnet8
52.....ddwrt
14...c4 73 1e c9 45 50 .....802.11n USB Wireless LAN Card
1.....Software Loopback Interface 1
=====

IPv4 Tabla de enrutamiento
=====
Rutas activas:
Destino de red      Máscara de red      Puerta de enlace    Interfaz  Métrica
0.0.0.0             0.0.0.0             192.168.1.1         192.168.1.65  60
10.0.0.0            255.0.0.0           10.54.181.101       10.54.181.201  36
10.24.181.0         255.255.255.0       En vínculo          10.24.181.3    291
10.24.181.3         255.255.255.255     En vínculo          10.24.181.3    291
10.24.181.255       255.255.255.255     En vínculo          10.24.181.3    291
10.54.181.201       255.255.255.255     En vínculo          10.54.181.201  291
127.0.0.0           255.0.0.0           En vínculo          127.0.0.1      331
127.0.0.1           255.255.255.255     En vínculo          127.0.0.1      331
127.255.255.255     255.255.255.255     En vínculo          127.0.0.1      331
192.168.1.0         255.255.255.0       En vínculo          192.168.1.65   316
192.168.1.65       255.255.255.255     En vínculo          192.168.1.65   316
192.168.1.255      255.255.255.255     En vínculo          192.168.1.65   316
192.168.159.0       255.255.255.0       En vínculo          192.168.159.1  291
192.168.159.1       255.255.255.255     En vínculo          192.168.159.1  291
192.168.159.129     255.255.255.255     En vínculo          192.168.159.1  36
192.168.159.255     255.255.255.255     En vínculo          192.168.159.1  291
224.0.0.0           240.0.0.0           En vínculo          127.0.0.1      331
224.0.0.0           240.0.0.0           En vínculo          192.168.1.65   316
224.0.0.0           240.0.0.0           En vínculo          10.24.181.3    291
224.0.0.0           240.0.0.0           En vínculo          192.168.159.1  291
224.0.0.0           240.0.0.0           En vínculo          10.54.181.201  291
255.255.255.255     255.255.255.255     En vínculo          127.0.0.1      331
255.255.255.255     255.255.255.255     En vínculo          192.168.1.65   316
255.255.255.255     255.255.255.255     En vínculo          10.24.181.3    291
255.255.255.255     255.255.255.255     En vínculo          192.168.159.1  291
255.255.255.255     255.255.255.255     En vínculo          10.54.181.201  291
=====
Rutas persistentes:
Ninguno

```

Figura 4.10: route print de anfitrión tras configurar la vpn

```

C:\Users\Diego>ping 10.54.181.105

Haciendo ping a 10.54.181.105 con 32 bytes de datos:
Respuesta desde 10.54.181.105: bytes=32 tiempo<1m TTL=63
Respuesta desde 10.54.181.105: bytes=32 tiempo<1m TTL=63
Respuesta desde 10.54.181.105: bytes=32 tiempo<1m TTL=63
Respuesta desde 10.54.181.105: bytes=32 tiempo<1m TTL=63

Estadísticas de ping para 10.54.181.105:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
              (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 0ms, Media = 0ms

C:\Users\Diego>

```

Figura 4.11: ping desde anfitrión a RCO-X

4.2 Pruebas de funcionamiento

Podemos observar en la Figura 4.12, como el PC anfitrión y el router establecen la comunicación PPP.

El paquete GRE muestra la encapsulación de los paquetes PPP. Es un protocolo utilizado para encapsular paquetes dentro de otro paquete con el fin de transportar datos de manera segura a través de la VPN.

LCP es parte del protocolo PPP que se usa para establecer, configurar y probar la conexión entre los dispositivos conectados. El paquete de Echo Request indica que el dispositivo local está enviando una solicitud para verificar que la conexión PPP esté preparada. El router local responde al PC anfitrión confirmando que el enlace PPP está activo y funcionando correctamente mediante un Echo Reply.

El router remoto envía un ping ICMP Echo Request al PC anfitrión como parte de la comunicación a través de la VPN. Esto es necesario para comprobar la correcta conectividad, verificando si el PC anfitrión puede recibir y responder a los paquetes a través del túnel. Por otro lado el PC anfitrión responde al router remoto con un ping de respuesta ICMP Echo Reply, confirmando que la solicitud de ping fue recibida correctamente. Este paquete completa la solicitud y respuesta del ping, verificando la conexión de la VPN.

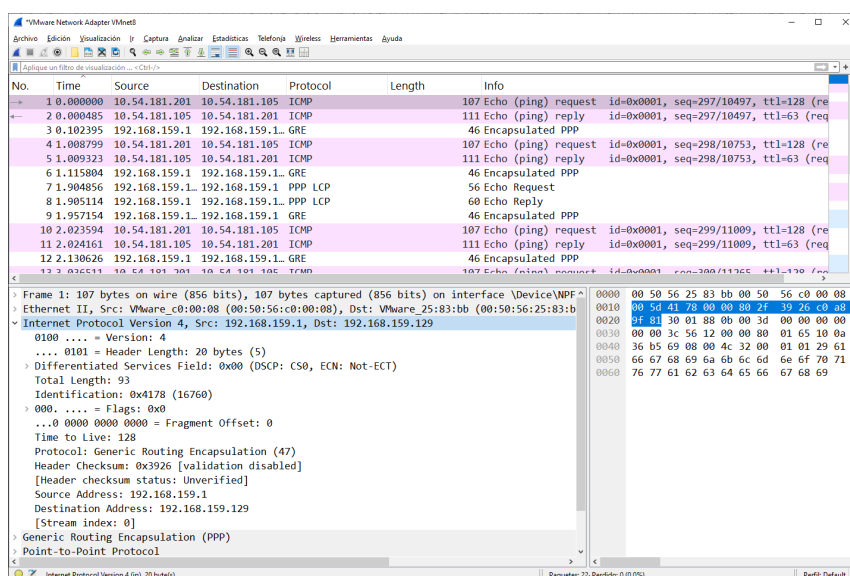


Figura 4.12: tráfico PPTP de la VMnet8 con pings entre el PC y RCO-X

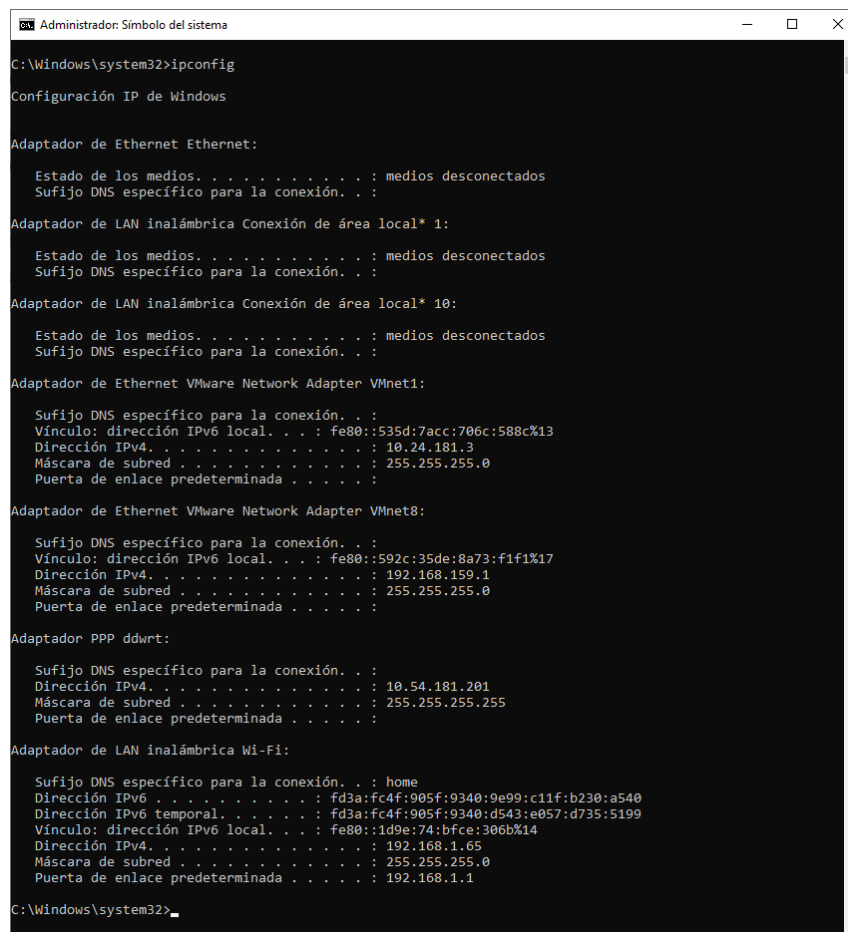
¿Puede ver el datagrama original?

Los ICMP son los paquetes que se utiliza para enviar un ping desde el router remoto al PC anfitrión. Sin embargo, debido a que el tráfico viaja a través de la VPN, el paquete ICMP está encapsulado en otros protocolos antes de llegar a destino. Primero el paquete enviado se encapsula en GRE, luego el ping pasa por el protocolo PPP y la respuesta se encapsula en GRE de nuevo.

El ping ICMP va a través del túnel VPN de forma segura. Sin embargo, el datagrama ICMP original no se ve directamente ya que está encapsulado en estos otros protocolos.

¿Ve más "echo requests" que los que Vd. manda?

No, cada Echo Request enviado desde el PC anfitrión tiene su correspondiente Echo Reply del router remoto.



```
C:\Windows\system32>ipconfig

Configuración IP de Windows

Adaptador de Ethernet Ethernet:

    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión. . . :

Adaptador de LAN inalámbrica Conexión de área local* 1:

    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión. . . :

Adaptador de LAN inalámbrica Conexión de área local* 10:

    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión. . . :

Adaptador de Ethernet VMware Network Adapter VMnet1:

    Sufijo DNS específico para la conexión. . . :
    Vínculo: dirección IPv6 local. . . : fe80::535d:7acc:706c:588c%13
    Dirección IPv4. . . . . : 10.24.181.3
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . . :

Adaptador de Ethernet VMware Network Adapter VMnet8:

    Sufijo DNS específico para la conexión. . . :
    Vínculo: dirección IPv6 local. . . : fe80::502c:35de:8a73:f1f1%17
    Dirección IPv4. . . . . : 192.168.150.1
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . . :

Adaptador PPP ddwrt:

    Sufijo DNS específico para la conexión. . . :
    Dirección IPv4. . . . . : 10.54.181.201
    Máscara de subred . . . . . : 255.255.255.255
    Puerta de enlace predeterminada . . . . . :

Adaptador de LAN inalámbrica Wi-Fi:

    Sufijo DNS específico para la conexión. . . : home
    Dirección IPv6 . . . . . : fd3a:fc4f:905f:9340:9e99:c11f:b230:a540
    Dirección IPv6 temporal. . . . . : fd3a:fc4f:905f:9340:d543:e057:d735:5199
    Vínculo: dirección IPv6 local. . . : fe80::1d9e:74bfce:306b%14
    Dirección IPv4. . . . . : 192.168.1.65
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . . : 192.168.1.1

C:\Windows\system32>
```

Figura 4.13: ipconfig del cliente pptp

Procedemos a explicar los dispositivos creados para el túnel en el anfitrión. Si nos fijamos en la Figura 4.13, observaremos un Adaptador PPP ddwrt. El cliente tiene asignada la dirección IP 10.54.181.201 dentro del túnel VPN. La máscara de subred 255.255.255.255 indica que este adaptador solo está interesado en comunicarse directamente con el servidor PPTP y no tiene una red local compartida.

Procedemos al analizar las tablas de enrutamiento de las siguientes máquinas implicadas:

IPv4 Tabla de enrutamiento

```
=====
```

Rutas activas:

Destino de red	Máscara de red	Puerta de enlace	Interfaz	Métrica
0.0.0.0	0.0.0.0	192.168.1.1	192.168.1.65	55
10.0.0.0	255.0.0.0	10.54.181.101	10.54.181.201	36
10.24.181.0	255.255.255.0	En vínculo	10.24.181.3	291
10.24.181.3	255.255.255.255	En vínculo	10.24.181.3	291
10.24.181.255	255.255.255.255	En vínculo	10.24.181.3	291
10.54.181.201	255.255.255.255	En vínculo	10.54.181.201	291
127.0.0.0	255.0.0.0	En vínculo	127.0.0.1	331
127.0.0.1	255.255.255.255	En vínculo	127.0.0.1	331
127.255.255.255	255.255.255.255	En vínculo	127.0.0.1	331
192.168.1.0	255.255.255.0	En vínculo	192.168.1.65	311
192.168.1.65	255.255.255.255	En vínculo	192.168.1.65	311
192.168.1.255	255.255.255.255	En vínculo	192.168.1.65	311
192.168.159.0	255.255.255.0	En vínculo	192.168.159.1	291
192.168.159.1	255.255.255.255	En vínculo	192.168.159.1	291
192.168.159.129	255.255.255.255	En vínculo	192.168.159.1	36
192.168.159.255	255.255.255.255	En vínculo	192.168.159.1	291
224.0.0.0	240.0.0.0	En vínculo	127.0.0.1	331
224.0.0.0	240.0.0.0	En vínculo	192.168.1.65	311
224.0.0.0	240.0.0.0	En vínculo	10.24.181.3	291
224.0.0.0	240.0.0.0	En vínculo	192.168.159.1	291
224.0.0.0	240.0.0.0	En vínculo	10.54.181.201	291
255.255.255.255	255.255.255.255	En vínculo	127.0.0.1	331
255.255.255.255	255.255.255.255	En vínculo	192.168.1.65	311
255.255.255.255	255.255.255.255	En vínculo	10.24.181.3	291
255.255.255.255	255.255.255.255	En vínculo	192.168.159.1	291
255.255.255.255	255.255.255.255	En vínculo	10.54.181.201	291

```
=====
```

Figura 4.14: Tabla de enrutamiento del PC anfitrión

```
root@DD-WRT:~# ip route
10.54.181.201 dev ppp0 proto kernel scope link src 10.54.181.101
192.168.159.2 dev eth0 scope link
10.54.181.0/24 dev br0 proto kernel scope link src 10.54.181.101
192.168.159.0/24 dev eth0 proto kernel scope link src 192.168.159.129
169.254.0.0/16 dev br0 proto kernel scope link src 169.254.255.1
127.0.0.0/8 dev lo scope link
default via 192.168.159.2 dev eth0
root@DD-WRT:~#
```

Figura 4.15: Tabla de forwarding de ddwrt-X

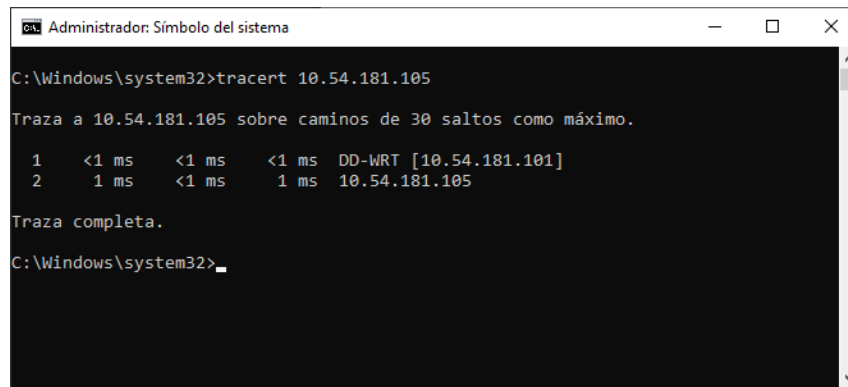
```
[root@rco-x ~]# ip route
default via 10.54.181.101 dev ens37 proto dhcp src 10.54.181.105 metric 100
10.54.181.0/24 dev ens37 proto kernel scope link src 10.54.181.105 metric 100
[root@rco-x ~]#
```

Figura 4.16: Tabla de forwarding de RCO-X

Como se puede observar en la tabla de enrutamiento, el ping saldría hacia la red 10.54.181.0, utilizando la interfaz 10.54.181.201, que es la dirección asignada al cliente PPTP por ddwrt-X.

Cuando el paquete llega al router, este consultará su tabla de enrutamiento y verá que la salida para la red 10.54.181.0 (indicada en el tercer registro) está asignada a la interfaz br0 (broadcast). El router entonces enviará el paquete hacia esa red, permitiendo que RCO-X lo reciba mediante una entrega local, dado que su Gateway es 0.0.0.0 (es decir, sin necesidad de pasar por otro punto de acceso).

A continuación, hemos ejecutado la orden `tracert 10.54.181.105` para observar cuál es la ruta que sigue para alcanzar a RCO-X, la ruta seguida se puede observar en la figura 4.17.



```

C:\Windows\system32>tracert 10.54.181.105

Traza a 10.54.181.105 sobre caminos de 30 saltos como máximo.

 1    <1 ms    <1 ms    <1 ms    DD-WRT [10.54.181.101]
 2     1 ms     <1 ms     1 ms     10.54.181.105

Traza completa.

C:\Windows\system32>

```

Figura 4.17: tracert desde anfitrión a RCO-x completado

PRUEBAS DE FUNCIONAMIENTO

1. Realice pings entre RCO-noX y RCO-X. Ejecute el analizador de protocolos Wireshark en el pc anfitrión y observe el tráfico PPTP de la VMnet1 y la VMnet8, explique lo que sucede. Tenga en cuenta que, al estar cifrado el contenido del túnel, wireshark no puede saber que se transporta. 2.3 Pruebas de funcionamiento 9 Si ve tráfico ICMP, no puede ser el ocasionado por nuestros pings. Le recomendamos que acceda a este enlace:

<http://www.tcpipguide.com/free/tpPPLinkControlProtocolLCP.htm> Donde encontrar un gráfico muy ilustrativo de cómo funcionan. Explique por qué cuando el PC anfitrión y el RCO - noX están en la misma red VMnet1, el primer no funciona y el segundo sí. Proponga una solución (añada una regla de routing en el PC). 3. Usando la orden tracert en el PC anfitrión, pruebe las rutas desde el PC anfitrión al RCO - X, 4. Instale la orden traceroute en los dos RCOs (y use el comando yum install traceroute), y pruebe las rutas desde el RCO - noX al RCO - X y viceversa, 5. Muestre las tablas de routing (orden ip route) en ddwrt - noX, ddwrt - X, RCO - xy y RCO - noX. Comente los resultados.

CAPÍTULO 5

Conclusiones

El protocolo PPTP es un protocolo obsoleto en la actualidad debido a múltiples vulnerabilidades de seguridad conocidas, como la debilidad en el cifrado y los métodos de autenticación. Actualmente, se recomienda utilizar protocolos más seguros, como L2TP/IPsec o OpenVPN. Pese a ello, al realizar el trabajo nos hemos dado cuenta de que PPTP es un protocolo sencillo de configurar y que viene bien para realizar prácticas con fines didácticos.

En este trabajo, se ha implementado un túnel PPTP sobre un entorno virtual, configurando el protocolo en dos modalidades distintas. La primera modalidad corresponde a un Site-to-Site, en la que el cliente PPTP se ejecuta en un router, lo que permite la interconexión de dos intranets a través del túnel PPTP. La segunda modalidad es Remote Access, en la cual el cliente PPTP se ejecuta en un ordenador personal (PC), permitiendo que únicamente dicho dispositivo acceda a la intranet del servidor PPTP. Estas configuraciones han permitido analizar las diferencias en la implementación y el funcionamiento del túnel PPTP en ambos contextos.

Bibliografía

- [1] Scott Hogg Josh Fruhlinger. Mtu size issues, fragmentation, and jumbo frames. Technical report, 2021. Disponible en <https://www.rfc-editor.org/rfc/rfc2766>.
- [2] Jon C Snader. *VPNs Illustrated: Tunnels, VPNs, and IPsec: Tunnels, VPNs, and IPsec*. Addison-Wesley Professional, 2015.
- [3] Wayne Lawson. *Building Cisco Remote Access Networks*. Syngress, 2000.
- [4] Ph.D. Plamen Nedeltchev. *Troubleshooting Remote Access Networks*. Cisco Press, 2002.
- [5] Gilbert Held. *Virtual private networking : a construction, operation and utilization guide*. Chichester : John Wiley, 2004.