



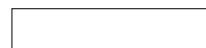
Trabajo Practico Especial 2018- Parte 1

Comunicación de Datos 1

Autores:

Álvarez Maximiliano (maxi25294@gmail.com)
Talú Bernabé(bernitalu234@gmail.com)

Ayudante designado: Mailen Gonzalez



Índice

1.....	<i>Portada.</i>
2.....	<i>Índice.</i>
3.....	<i>Introducción.</i>
3.....	<i>Primera Parte.</i>
11.....	<i>Segunda Parte.</i>
34.....	<i>Conclusión.</i>

Introducción

En esta primer parte del trabajo práctico se pretende crear, desde sus raíces, una red y adentrarse en el mundo de la comunicación de datos mediante la representación VLSM y con la herramienta Core. Desde esta etapa se logró dividir dicha red en sub-redes para distinto uso y con distinta cantidad de usuarios o hosts. Por medio de la máquina virtual y la herramienta Core, se podrá utilizar el comando “ping” entre 2 PCs de la misma sub-red para visualizar su comunicación y luego, con la herramienta Wireshark, poder analizar el envío de paquetes y como se conforma cada uno.

Desarrollo y resolución

Enunciados:

1. *Para la cantidad de conexiones proyectadas para cada una de las redes, realice una asignación de direcciones IP utilizando VLSM. Considere que las direcciones privadas se encuentren en el rango 192.169.X.0 a 192.169.X.255, donde X es el número de grupo que se les asignó.*

La red tiene las siguientes características:

- BR-Admin: Tiene actualmente 2 PC conectadas y la cantidad de conexiones que soporta el Bridge es 4. IP necesarias: 4 para conexión + 1 dirección base + 1 dirección broadcast = 6. Por lo tanto, $2^3 = 8$ direcciones reservadas.
- BR-Ventas: Tiene 3 PC conectadas y la cantidad de conexiones que soporta el Bridge es 64. IP necesarias: 64 para conexión + 1 dirección base + 1 dirección broadcast = 66. Por lo tanto, $2^7 = 128$ direcciones reservadas.
- Hub-Oficinas: Tiene actualmente 2 PC conectadas y la cantidad de conexiones que soporta el Hub es 16. IP necesarias: 16 para conexión + 1 dirección base + 1 dirección broadcast = 18. Por lo tanto, $2^5 = 32$ direcciones reservadas.
- Wifi-Ap: Tiene 2 Laptop conectadas y prevé que se conectarán hasta 60 equipos. IP necesarias: 60 para conexión + 1 dirección base + 1 dirección broadcast = 62. Por lo tanto, $2^6 = 64$ direcciones reservadas.
- Red BR, BR-Datacenter y R1 a R2: Subredes creadas para las conexiones entre Routers:

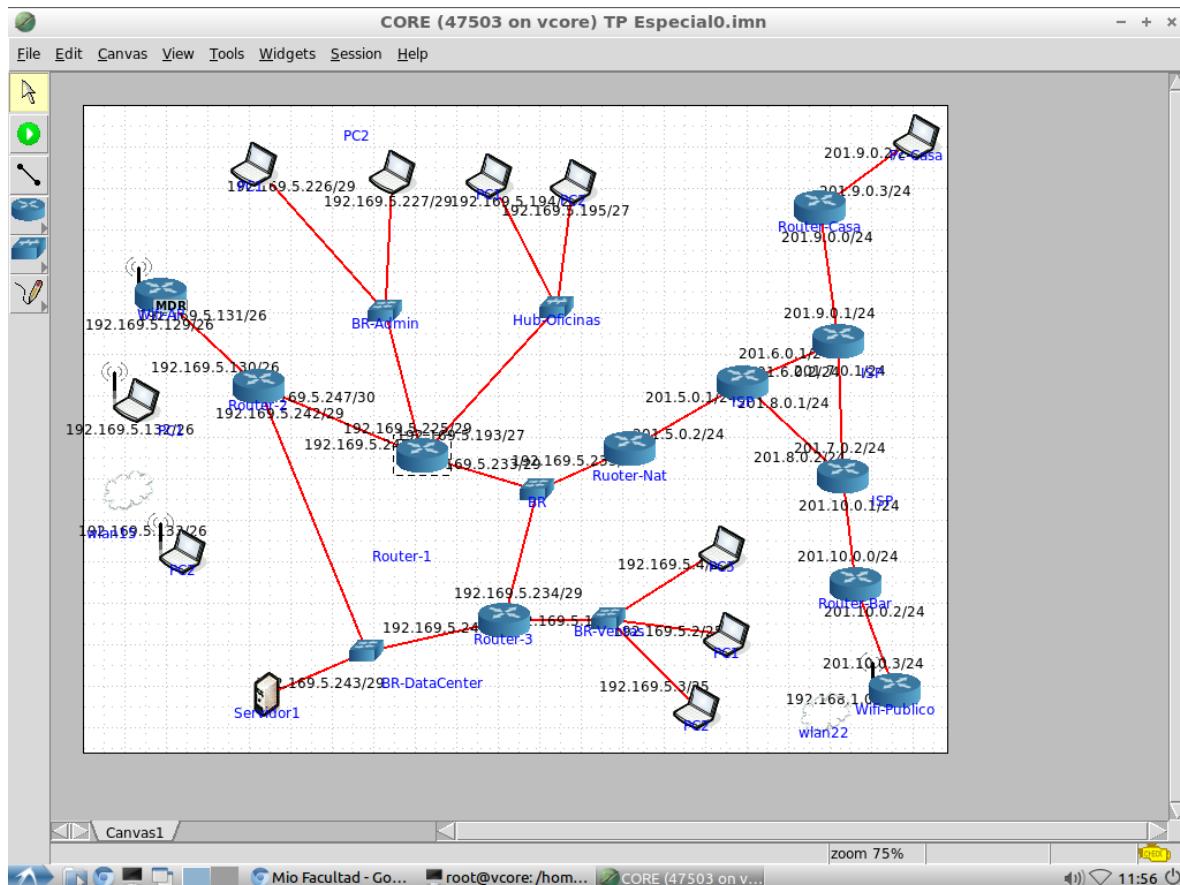
Direcciones, respectivamente:

- 6 direcciones + 1 dirección base + 1 dirección broadcast.
- 6 direcciones + 1 dirección base + 1 dirección broadcast.
- 2 direcciones + 1 dirección base + 1 dirección broadcast.

2. *Realice una tabla en donde se indiquen cada una de las subredes resultantes, indicando el nombre de cada red, su dirección base, la máscara, y el rango que incluye cada bloque.*

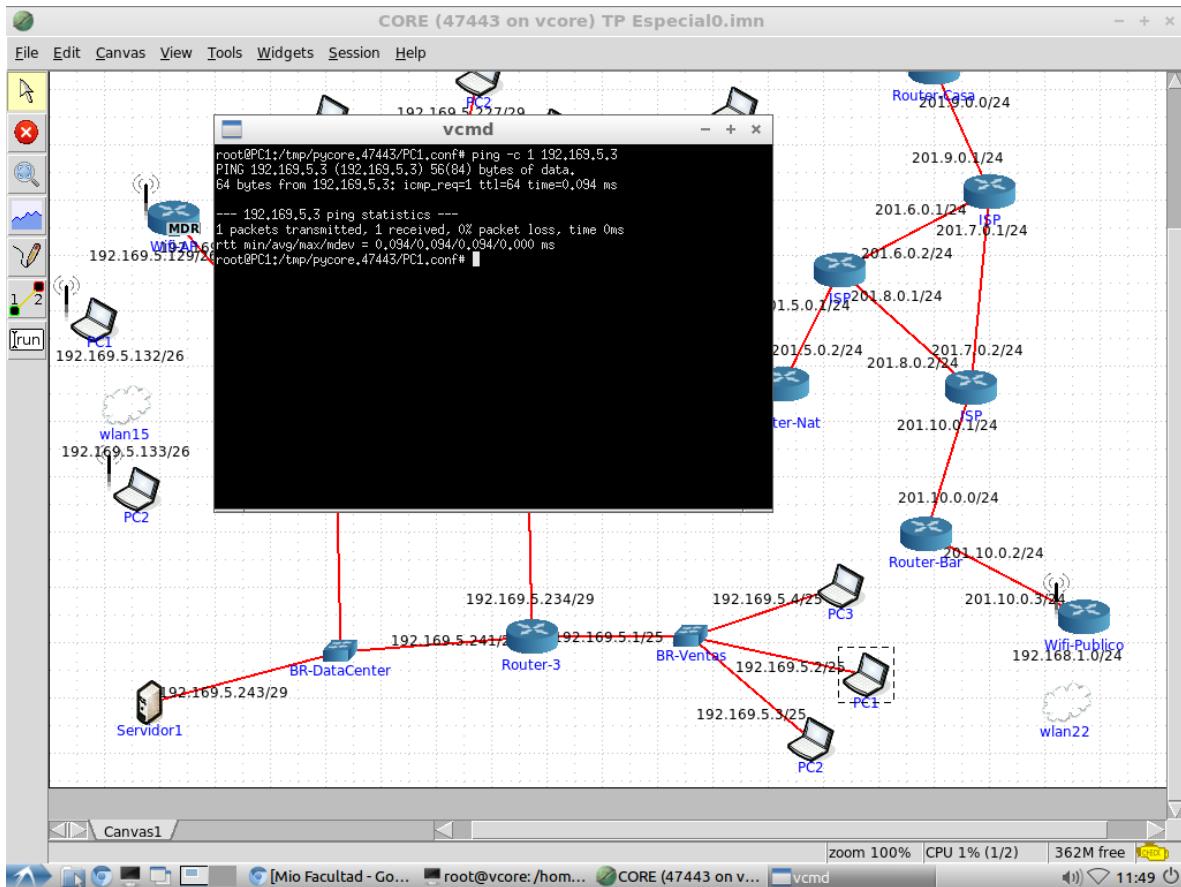
	Sub-red	Dir. Base	Máscara	Rango asignable	Broadcast
1	Ventas	192.169.5.0	/25	192.169.5.1; 192.169.5.126	192.169.5.127
2	Wifi-AP	192.169.5.128	/26	192.169.5.129; 192.169.5.190	192.169.5.191
3	Oficina	192.169.5.192	/27	192.169.5.193; 192.169.5.222	192.169.5.223
4	Admin	192.169.5.224	/29	192.169.5.225; 192.169.5.230	192.169.5.231
5	BR	192.169.5.232	/29	192.169.5.233; 192.169.5.238	192.169.5.239
6	BR-DataC	192.169.5.240	/29	192.169.5.241; 192.169.5.246	192.169.5.247
7	R1 a R2	192.169.5.248	/30	192.169.5.249; 192.169.5.250	192.169.5.251

3. Implemente la red propuesta en el emulador CORE con la disposición de equipos que actualmente se tienen conectados. Considere la asignación IP realizada en el ejercicio 1, y la colocación de direcciones públicas en donde corresponda (considere que se debe utilizar el comando ifconfig para configurar cada una de las interfaces de los routers, mientras que en los host se puede realizar la configuración de la interfaz colocando la Ip que corresponda utilizando la opción IPv4 address de la pantalla de configuración del host).

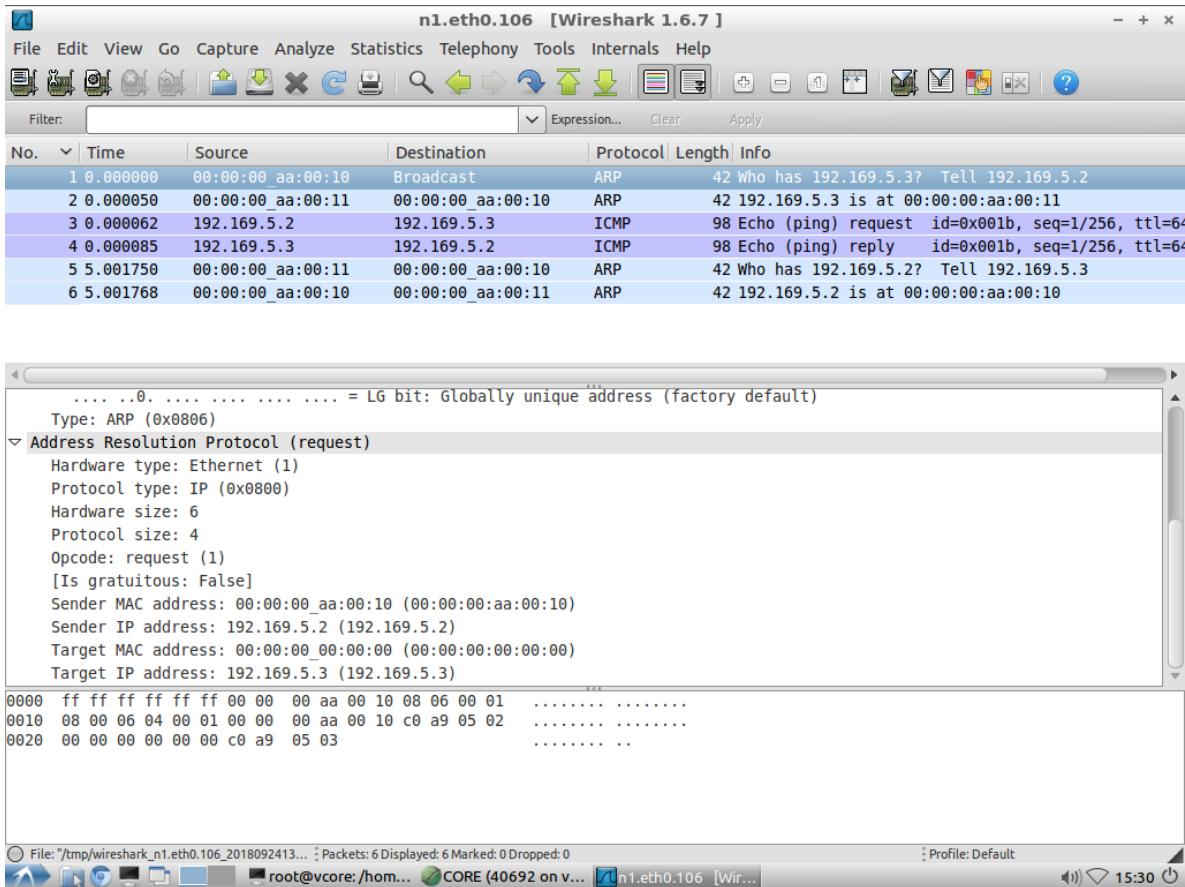


- I. Se configuró los ISP con las direcciones públicas dadas y la privada que ingresa al Router-Nat
- II. Se colocó los routers requeridos con los switchs y hubs correspondientes realizando las respectivas conexiones.
- III. Los routers wifi se conectaron mediante las “Wireless LAN”
- IV. Luego de la asignación de IP correspondientes, en los routers se introdujo el comando ifconfig con sus interfaces en la pestaña de startup. Esto se llevó a cabo con el fin de configurar la interfaz de red de cada uno de ellos, asignándole el comando “up” marca la interfaz como disponible para que se pueda utilizar por la capa IP. Se realiza en cada router, con cada interfaz de estos. Ej. ifconfig eth0 192.169.5.3.

4. Ejecute el comando Ping con la opción `-c 1` entre dos host de la subred ventas. Utilizando la herramienta Wireshark, inspeccione los paquetes que se generan en el origen y destino (captura de la interfaz origen e interfaz destino). Identifique los campos más importantes de cada paquete (dirección origen, dirección destino, protocolo, ttl, tipo de paquete, etc.)



- Se utilizó el comando “ping” entre la PC1 y la PC2 de la subred ventas para verificar la comunicación entre ellos dos. Con el comando `-c 1`, el cual envía sólo un paquete.



- Utilizando la herramienta Wireshark se analiza el envío de paquetes cuando el comando “ping” entre las dos PCs de la subred Ventas ese ejecutado. Esta información está empaquetada en hexadecimal, y en la interfaz gráfica de dicha herramienta lo traduce para que se pueda comprender. Analizamos 3 de los 6 paquetes mostrados, sobre todo por la importancia del número 3 y número 4 que son los que llevan datos.

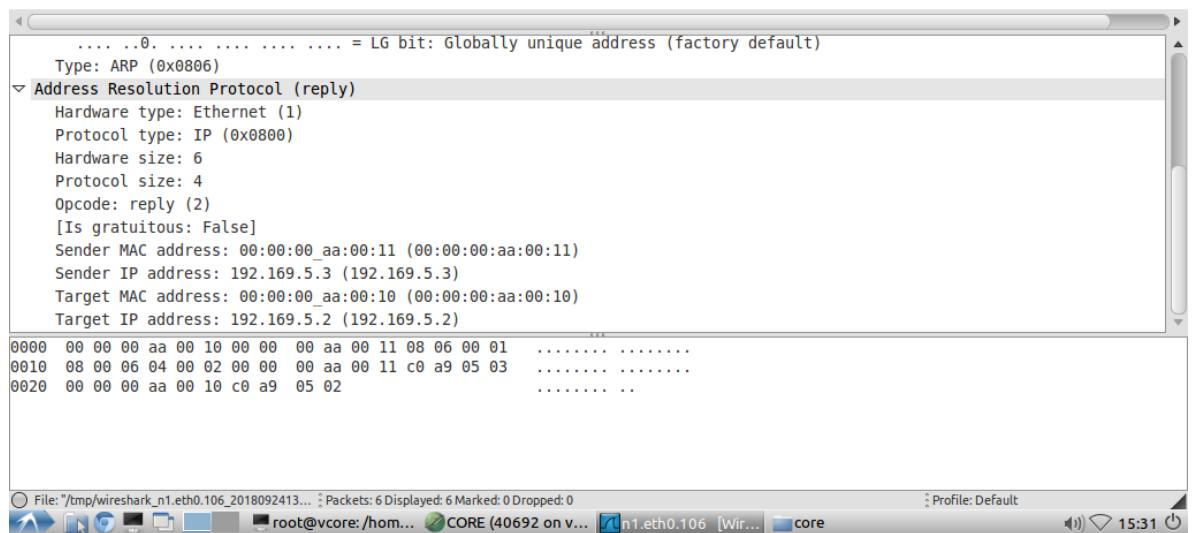
- Si se identificaran las partes de lo enviado y recibido tendríamos como origen la IP 192.169.5.4 de la red Ventas hasta su destino, también de la red Ventas con dirección IP 192.169.5.2. El protocolo es ICMP, con un ttl = 64. Los paquetes que poseen el protocolo ARP, son los encargados de preguntar de donde viene y hacia donde va.
- Si se descompone cada paquete hexadecimal, comprendemos la finalidad de cada conjunto. Por ejemplo, el paquete número 1 (Broadcast):

- ff ff ff ff ff ff: Dirección de destino
- 00 00 00 aa 00 10: Dirección Origen
- 08 06: ARP(0x0806) Type (Protocolo)
- 00 01: Hardware type: Ethernet (1)

- 08 00: Protocol type: IP (0x0800)
- 06: Hardware Size
- 04: Protocol Size
- 00 02: Opcode: request (1)
- 00 00 00 aa 00 10: Sender MAC address
- c0 a9 05 02: Sender IP address
- 00 00 00 00 00 00: Target MAC Address
- c0 a9 05 03: Target IP Address

Wireshark 1.6.7 [n1.eth0.106]

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	00:00:00_aa:00:10	Broadcast	ARP	42	Who has 192.169.5.3? Tell 192.169.5.2
2	0.000050	00:00:00_aa:00:11	00:00:00_aa:00:10	ARP	42	192.169.5.3 is at 00:00:00_aa:00:11
3	0.000062	192.169.5.2	192.169.5.3	ICMP	98	Echo (ping) request id=0x001b, seq=1/256, ttl=64
4	0.000085	192.169.5.3	192.169.5.2	ICMP	98	Echo (ping) reply id=0x001b, seq=1/256, ttl=64
5	5.001750	00:00:00_aa:00:11	00:00:00_aa:00:10	ARP	42	Who has 192.169.5.2? Tell 192.169.5.3
6	5.001768	00:00:00_aa:00:10	00:00:00_aa:00:11	ARP	42	192.169.5.2 is at 00:00:00_aa:00:10



- 00 00 00 aa 00 10: Dirección de destino
- 00 00 00 aa 00 11: Dirección origen
- 08 06: ARP(0x0806) Type (Protocolo)
- 00 01: Hardware type: Ethernet (1)
- 08 00: Protocol type: IP (0x0800)
- 06: Hardware Size
- 04: Protocol Size
- 00 02: Opcode: reply (2)
- 00 00 00 aa 00 11: Sender MAC address

- c0 a9 05 03: Sender IP address
- 00 00 00 aa 00 10: Target MAC Address
- c0 a9 05 02: Target IP Address

Wireshark 1.6.7 [n1.eth0.106]

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	00:00:00_aa:00:10	Broadcast	ARP	42	Who has 192.169.5.3? Tell 192.169.5.2
2	0.000050	00:00:00_aa:00:11	00:00:00_aa:00:10	ARP	42	192.169.5.3 is at 00:00:00_aa:00:11
3	0.000062	192.169.5.2	192.169.5.3	ICMP	98	Echo (ping) request id=0x001b, seq=1/256, ttl=64
4	0.000085	192.169.5.3	192.169.5.2	ICMP	98	Echo (ping) reply id=0x001b, seq=1/256, ttl=64
5	5.0001750	00:00:00_aa:00:11	00:00:00_aa:00:10	ARP	42	Who has 192.169.5.2? Tell 192.169.5.3
6	5.0001768	00:00:00_aa:00:10	00:00:00_aa:00:11	ARP	42	192.169.5.2 is at 00:00:00_aa:00:10

Internet Protocol Version 4, Src: 192.169.5.2 (192.169.5.2), Dst: 192.169.5.3 (192.169.5.3)

Type: IP (0x0800)0. = LG bit: Globally unique address (factory default)
Version: 4	
Header length: 20 bytes	
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))	
0000 00.. = Differentiated Services Codepoint: Default (0x00)	
.... ..00 = Explicit Congestion Notification: Not-ECT (Not ECN-Capable Transport) (0x00)	
Total Length: 84	
Identification: 0x0000 (0)	
Flags: 0x02 (Don't Fragment)	
Fragment offset: 0	
Time to live: 64	

```
0000 00 00 00 aa 00 11 00 00 00 aa 00 10 08 00 45 00 ..... . .... E.
0010 00 54 00 00 40 00 40 01 af 51 c0 a9 05 02 c0 a9 .T..@. @. Q. ....
0020 05 03 08 00 80 5e 00 1b 00 01 6f 4e a9 5b 72 d8 .....^... ..ON.[r.
0030 01 00 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 ..... . .... .
0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 ..... .. !#%$
0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 &'()*, - ./012345
0060 36 37 67
```

File: "/tmp/wireshark_n1.eth0.106_2018092413..." Packets: 6 Displayed: 6 Marked: 0 Dropped: 0 Profile: Default

root@vcore:/home... CORE (40692 on v... n1.eth0.106 [wir... core 15:31

- 00 00 00 aa 00 11: Dirección Destino
- 00 00 00 aa 00 10: dirección origen
- 08 00: type ip(0x0800)
- 45: Header Length: 20 bytes
- 00: Not-ECT (0x00)
- 00 54: Total length: 84
- 00 00: Identification: 0x0000 (0)
- 40 00: Fragment Offset: 0
- 40: time to live: 64
- 01: protocol: icmp (1)
- af 51: header checksum 0xaf51 bad:false

- c0 a9 05 02: header checksum source
- c0 a9 05 03: header checksum destination
- 08: type (echo ping request)
- 00: code
- 80 5e: checksum 0x805e correct
- 00 1b: identifier (le): 6912
- 00 01: sequence number (LE): 256 (0x0100)
- El resto es "Data": 56 bytes

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	00:00:00_aa:00:10	Broadcast	ARP	42	Who has 192.169.5.3? Tell 192.169.5.2
2	0.000050	00:00:00_aa:00:11	00:00:00_aa:00:10	ARP	42	192.169.5.3 is at 00:00:00_aa:00:11
3	0.000062	192.169.5.2	192.169.5.3	ICMP	98	Echo (ping) request id=0x001b, seq=1/256, ttl=64
4	0.000085	192.169.5.3	192.169.5.2	ICMP	98	Echo (ping) reply id=0x001b, seq=1/256, ttl=64
5	0.001750	00:00:00_aa:00:11	00:00:00_aa:00:10	ARP	42	Who has 192.169.5.2? Tell 192.169.5.3
6	0.001768	00:00:00_aa:00:10	00:00:00_aa:00:11	ARP	42	192.169.5.2 is at 00:00:00_aa:00:10

.... ..0. = LG bit: Globally unique address (factory default)
Type: IP (0x0800)
Internet Protocol Version 4, Src: 192.169.5.3 (192.169.5.3), Dst: 192.169.5.2 (192.169.5.2)
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
0000 00.. = Differentiated Services Codepoint: Default (0x00)
.... ..00 = Explicit Congestion Notification: Not-ECT (Not ECN-Capable Transport) (0x00)
Total Length: 84
Identification: 0x9e2b (40491)
Flags: 0x00
Fragment offset: 0
Time to live: 64
0000 00 00 00 aa 00 10 00 00 00 aa 00 11 08 00 45 00E.
0010 00 54 9e 2b 00 00 40 01 51 26 c0 a9 05 03 c0 a9 .T.+..@.Q&.....
0020 05 02 00 00 88 5e 00 1b 00 01 6f 4e a9 5b 72 d8^... .ON.[r.
0030 01 00 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15
0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 !#\$%
0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 &'()*+,- ./012345
0060 36 37 67

- 00 00 00 aa 00 10: Dirección Destino
- 00 00 00 aa 00 11: Dirección Origen
- 08 00: Type IP (0x0800)
- 45: Header Length: 20 bytes
- 00: Not-ECT(0x00)
- 00 54: Total Length: 84
- 9e 2b: Identification
- 00 00: Fragment Offset
- 40: Time to live

- 01: Protocol: ICMP (1)
- 51 26: Header Checksum
- c0 a9 05 03: Header Checksum Source
- c0 a9 05 02: Header Checksum Destination
- 00: Echo “ping” request
- 00: Code
- 88 5e: Checksum
- 00 1b: Identifier (le)
- 00 01: Sequence Number (LE)

Parte 2

1- Configurar todas las rutas de los routers, minimizando la cantidad de entradas en las tablas de ruteo (considere el uso de rutas por defecto). Cabe desatacar que los comandos correspondientes deben estar cargados en la opción UserDefined -> Startup Commands de cada dispositivo, y que dentro de los servicios sólo deben quedar habilitados el IP FORWARD y User Defined.

Consideraciones:

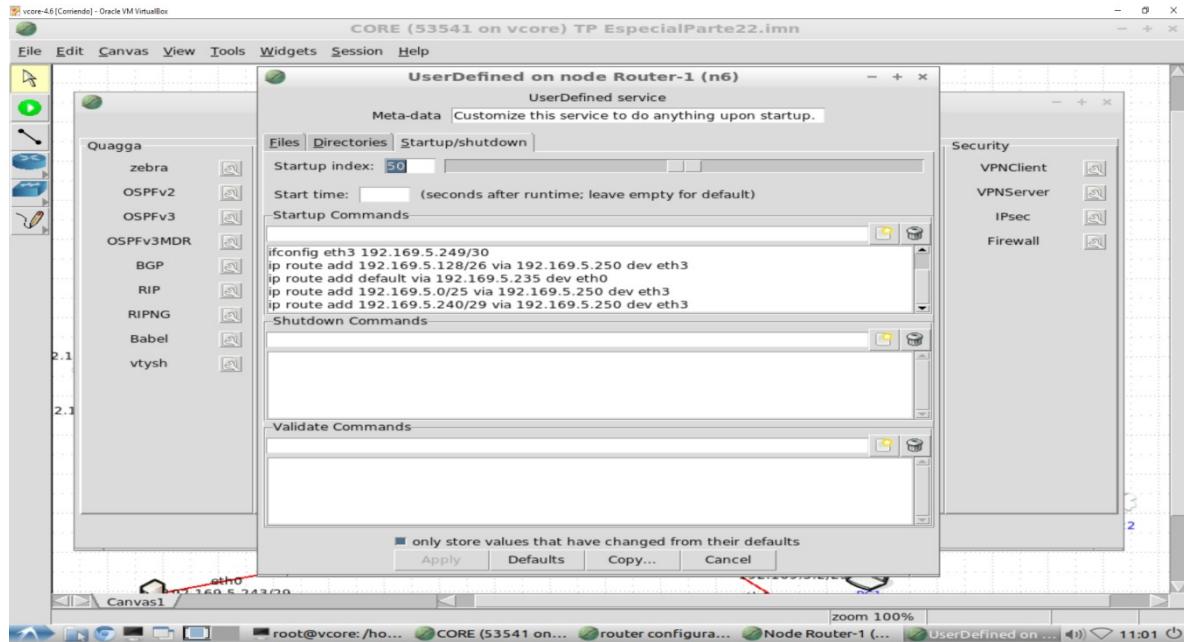
- a. Se considera que pasar por el BR no es seguro, por lo que toda la comunicación interna no debe pasar por dicho bridge.
- b. El tráfico de internet que tenga destino la red Wi-fi debe direccionarse por el Router-1.
- c. Tenga en cuenta que los ISP deben conocer sólo las redes públicas (no deben tener definida la ruta por defecto).

Para configurar las rutas de los routers se utiliza el comando:

- Ip route add <red/mascara> via <dirlPdestino> dev <output-interface>
- Ip route add default via <dirlPdestino> dev <output-interface>

La diferencia es que el primero agrega rutas a redes que se encuentran fuera del alcance del router, mientras que el segundo comando se utiliza en caso de no conocer la red a donde se van a enviar los paquetes para redireccionarlos por defecto.

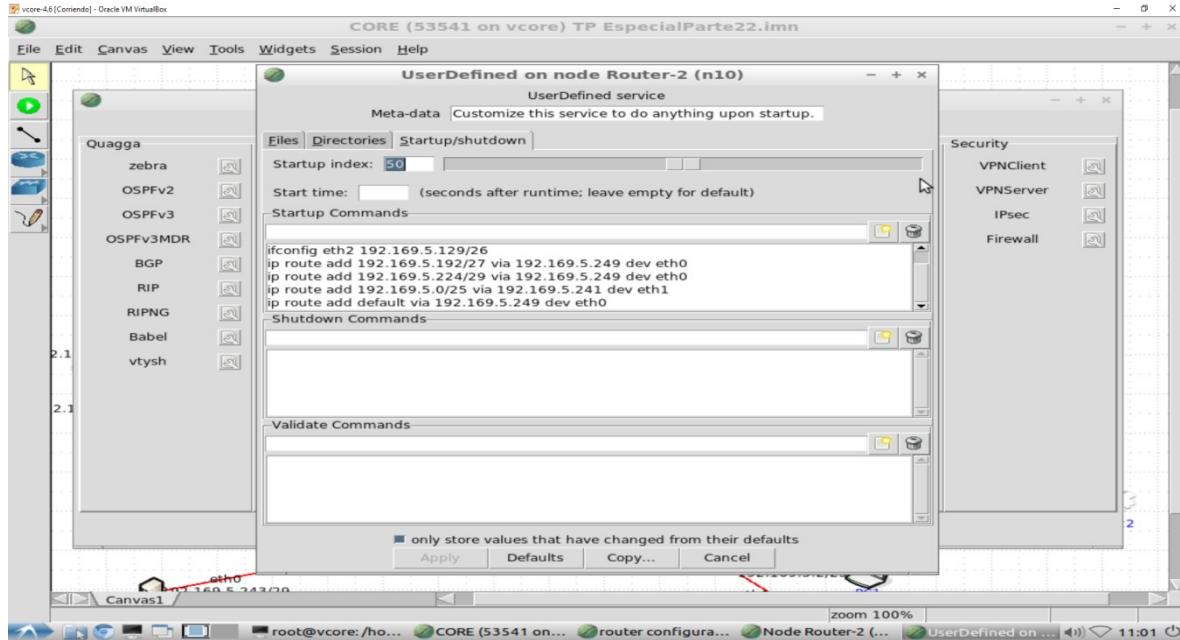
Router 1:



Red	I/D	Interface	Prox. Router
192.169.5.192/27	D	ETH2	-
192.169.5.224/29	D	ETH1	-
192.169.5.248/30	D	ETH3	-
192.169.5.232/29	D	ETH0	-
192.169.5.128/26	I	ETH3	192.169.5.250
192.169.5.240/29	I	ETH3	192.169.5.250
192.169.5.0/25	I	ETH3	192.169.5.250
Default	I	ETH0	192.169.5.235

El motivo de la misma interface ETH3, y el mismo próximo Router es que el BR no es confiable por lo tanto hay que tomar un camino que no pase por él, es decir, Router 2.

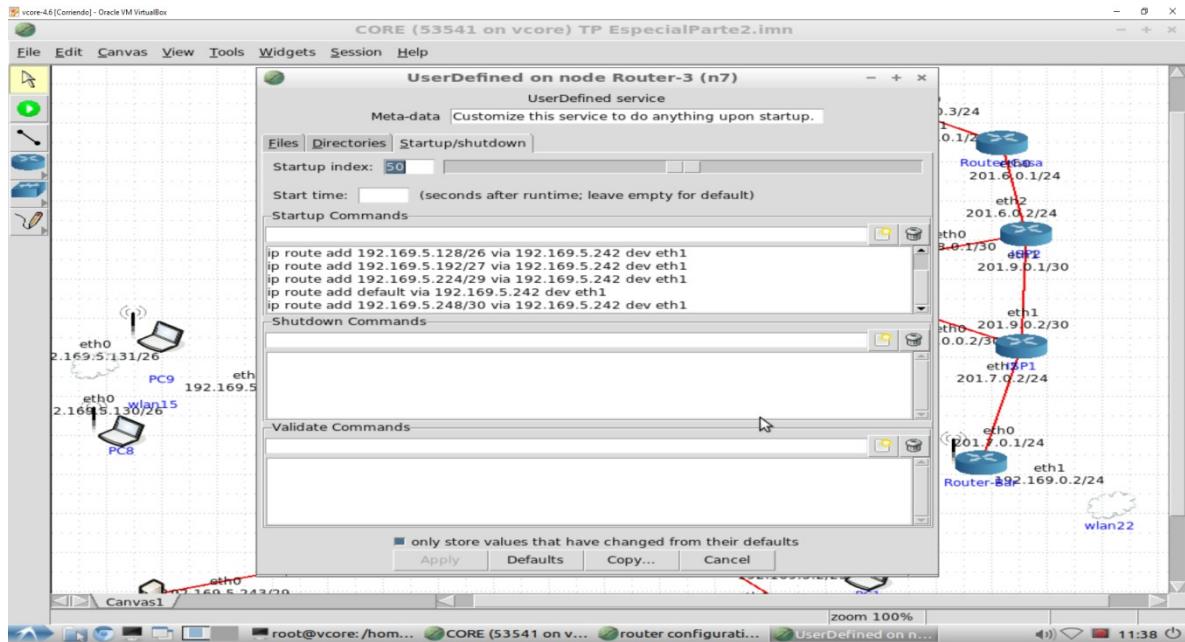
Router 2:



Red	I/D	Interface	Prox. Router
192.169.5.128/26	D	ETH3	-
192.169.5.240/29	D	ETH1	-
192.169.5.248/30	D	ETH0	-
192.169.5.224/29	I	ETH0	192.169.5.249
192.169.5.192/27	I	ETH0	192.169.5.249
192.169.5.232/29	I	ETH0	192.169.5.249
192.169.5.0/25	I	ETH1	192.169.5.241
Default	I	ETH0	192.169.5.249

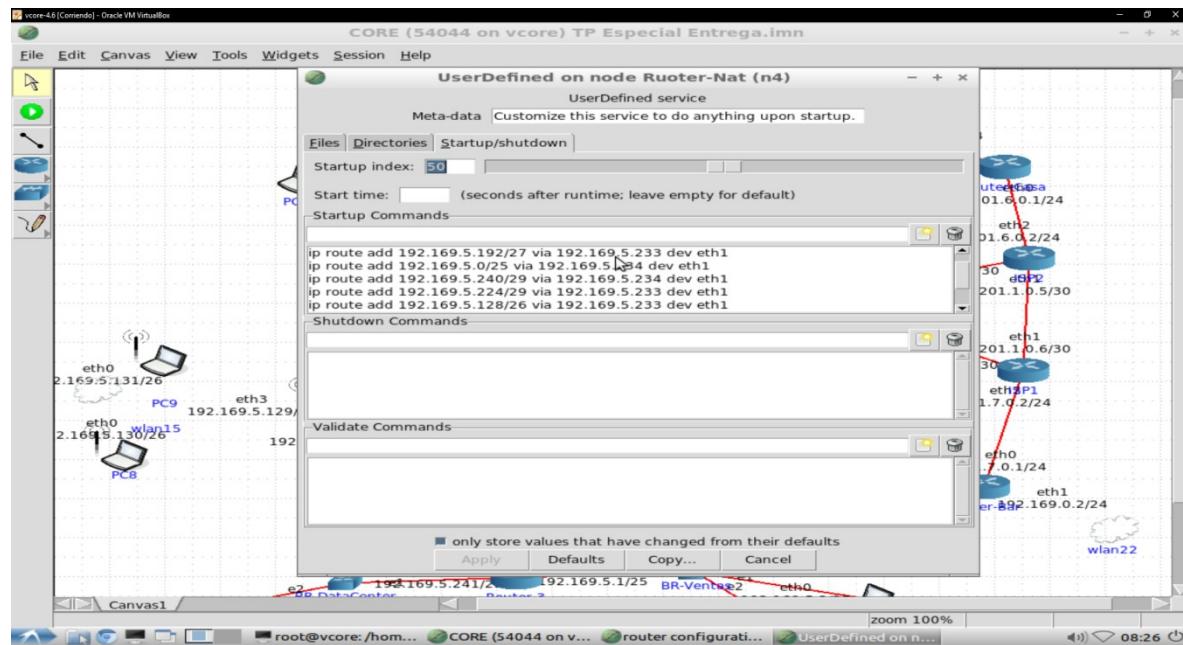
La conexión a Internet Wifi, debe conducirse por el Router 1. El Router 2 hace de nexo entre el Router 1 y el Router 3.

Router 3:



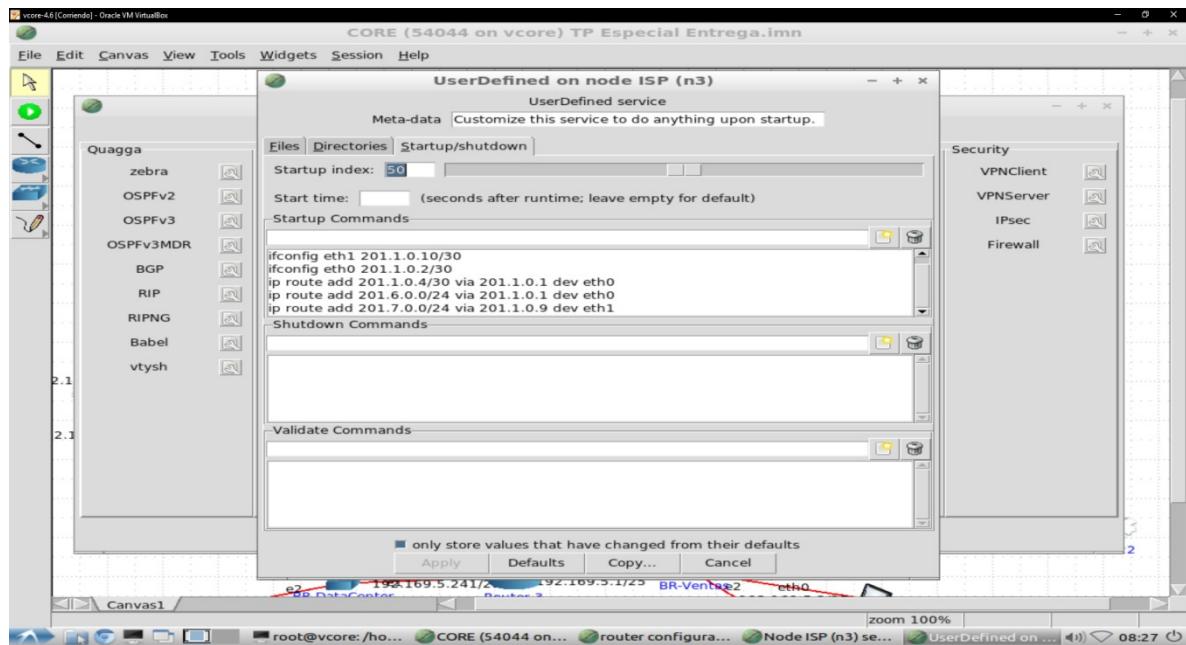
Red	I/D	Interface	Prox. Router
192.169.5.0/25	D	ETH2	-
192.169.5.240/29	D	ETH1	-
192.169.5.232/29	D	ETH0	-
192.169.5.128/26	I	ETH1	192.169.5.242
192.169.5.224/29	I	ETH1	192.169.5.242
192.169.5.192/27	I	ETH1	192.169.5.242
192.169.5.248/30	I	ETH1	192.169.5.242
Default	I	ETH1	192.169.5.242

Router-Nat:



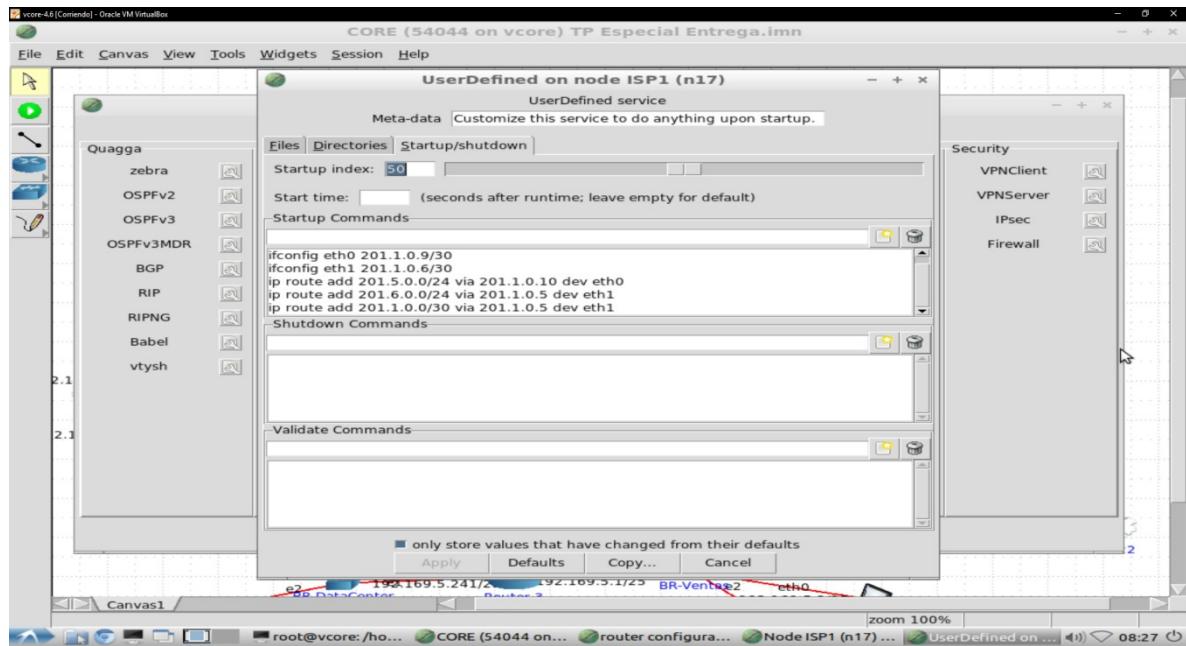
Red	I/D	Interface	Prox. Router
192.169.5.232/29	D	ETH1	-
201.5.0.0/24	D	ETH0	-
192.169.5.192/27	I	ETH1	192.169.5.233
192.169.5.0/25	I	ETH1	192.169.5.234
192.169.5.240/29	I	ETH1	192.169.5.234
192.169.5.224/29	I	ETH1	192.169.5.233
192.169.5.128/26	I	ETH1	192.169.5.233
Default	I	ETH0	201.5.0.1

ISP:



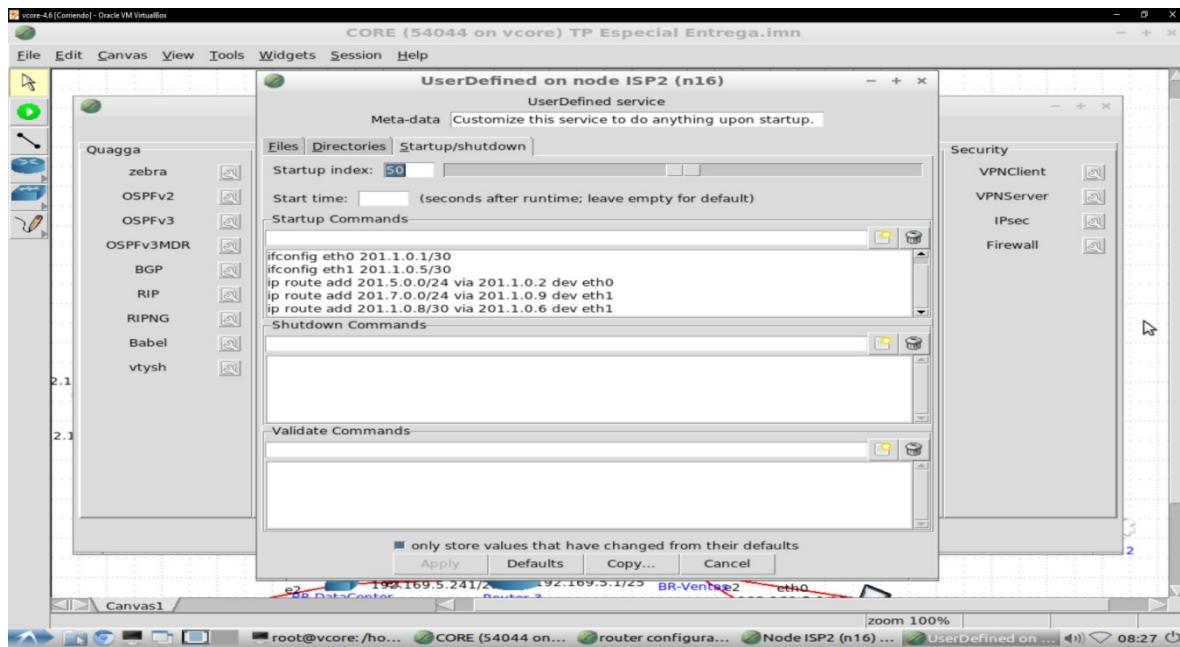
Red	I/D	Interface	Prox. Router
201.5.0.0/24	D	ETH2	-
201.1.0.0/30	D	ETH0	-
201.1.0.8/30	D	ETH1	-
201.1.0.4/30		ETH0	201.1.0.1
201.6.0.0/24		ETH0	201.1.0.1
201.7.0.0/24		ETH1	201.1.0.9

ISP 1:



Red	I/D	Interface	Prox. Router
201.7.0.0/24	D	ETH2	-
201.1.0.4/30	D	ETH1	-
201.1.0.8/30	D	ETH0	-
201.5.0.0/24	I	ETH0	201.1.0.10
201.6.0.0/24	I	ETH0	201.1.0.5
201.1.0.0/30	I	ETH1	201.1.0.5

ISP 2:



Red	I/D	Interface	Prox. Router
201.6.0.0/24	D	ETH2	-
201.1.0.4/30	D	ETH1	-
201.1.0.0/30	D	ETH0	-
201.5.0.0/24	I	ETH0	201.1.0.2
201.7.0.0/24	I	ETH1	201.1.0.9
201.1.0.8/30	I	ETH1	201.1.0.6

2- Configurar el Router-Nat para que los equipos que pertenecen a la Red-Oficina NO puedan conectarse a Internet, mientras que el resto de los equipos SI puedan acceder a internet.

Para lograr que todos los equipos que no pertenecen a Red-Oficina se puedan conectar a Internet, se permitió que las redes lleguen a Router-Nat. Aquí se tiene un escenario en el cual se posee sólo una IP pública asignada a múltiples equipos en una red privada, por lo tanto la solución NAT es que la subred se maneja con un espacio de direcciones privadas, el Router-Nat modifica el número de puerto para el tráfico que se dirige hacia afuera. Esto lo hace mediante el IP masquerading, así como también se le asigna la IP route por defecto del Router-NAT al ISP más cercano.

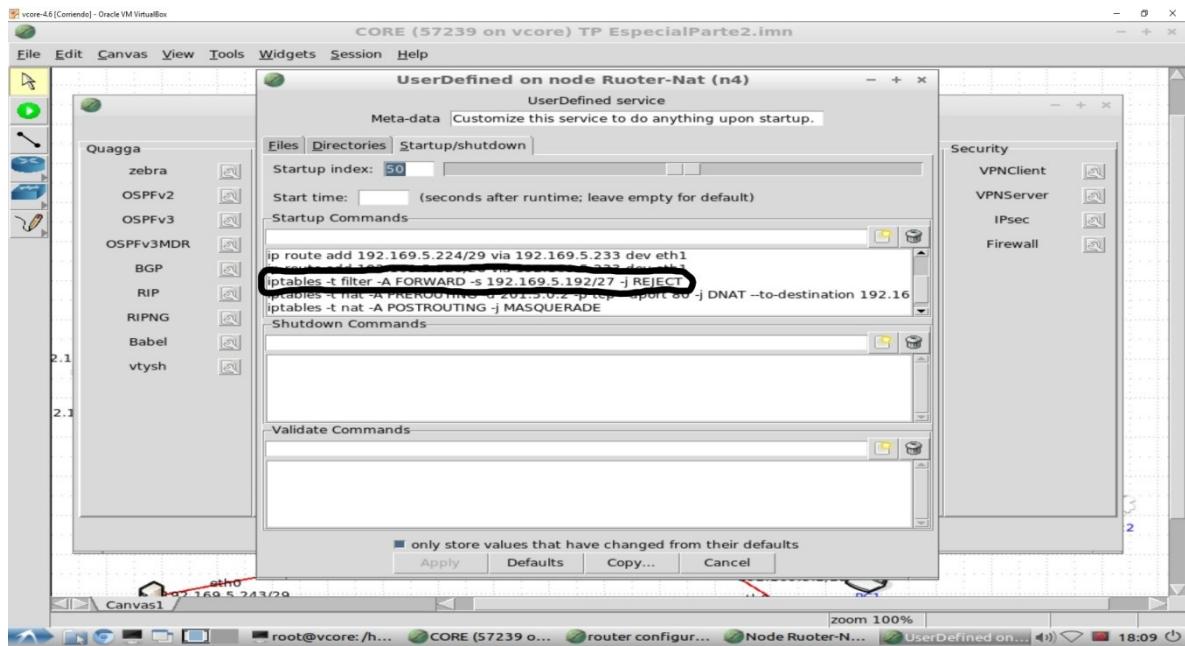
IP Masquerading:

```
-j MASQUERADE --to-source [<dirIP>][:<puerto>]
```

Este comando permite el enmascaramiento IP o NAPT. Esto quiere decir que identifica que un equipo perteneciente a la red quiere conectarse con una dirección externa a esta misma red, por lo tanto, es el mismo servidor quien realiza la petición. De esta manera el servidor toma la dirección IP y el puerto que se le asignó, la envía y cuando el paquete de respuesta llega, lo vuelve a enviar a la máquina y puerto del cual se realizó el pedido.

Para negar la conexión a Internet, en la configuración del Router-Nat, se utilizó un comando de NetFilter llamado iptables con siguientes parámetros, para impedir la conexión de Red-Oficina:

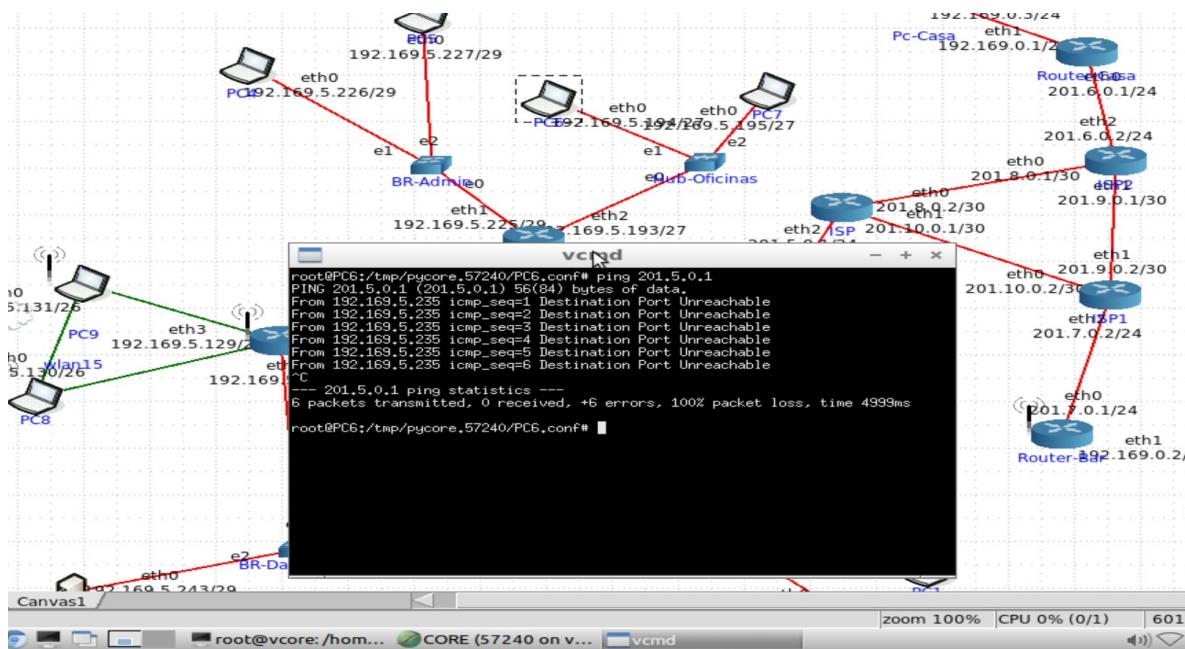
```
Iptables [-t <tabla>] [<cadena>] <comando> [<condición>] [<acción>].
```



Siendo:

- Tabla: FILTER
- Cadena: -A
- Comando: FORWARD
- Condición: -s 192.169.5.192/27 (dirección origen de la cual parten)
- Acción: -j REJECT (que se descarte)

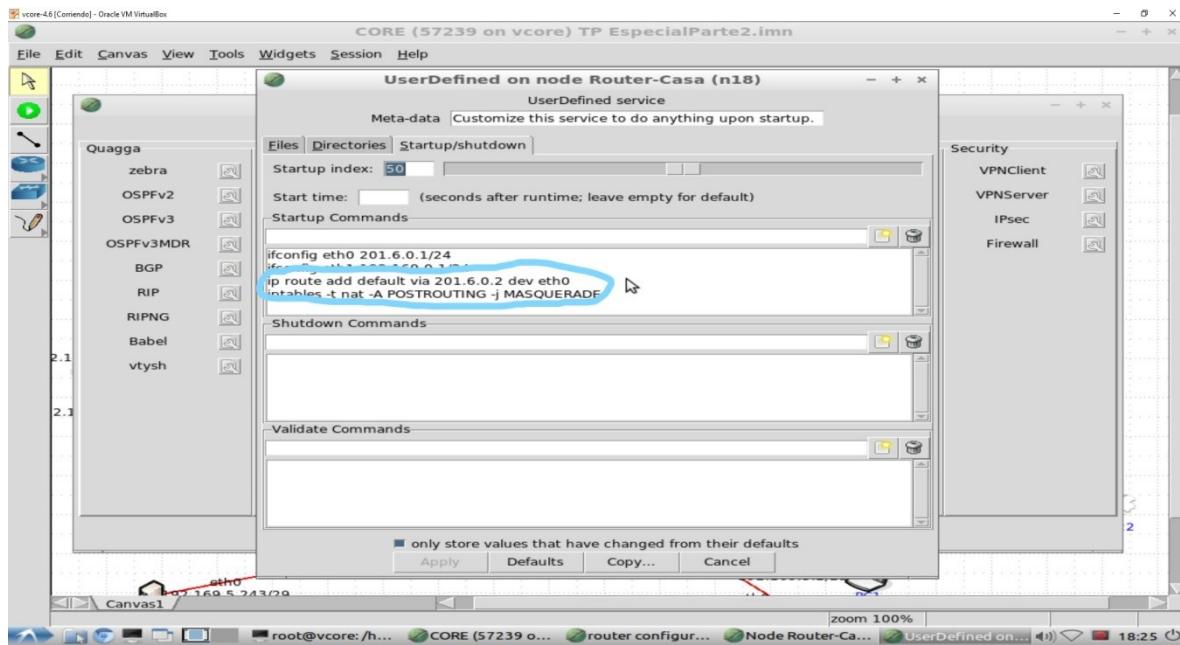
Captura de Red-Oficina sin conexión a Internet:

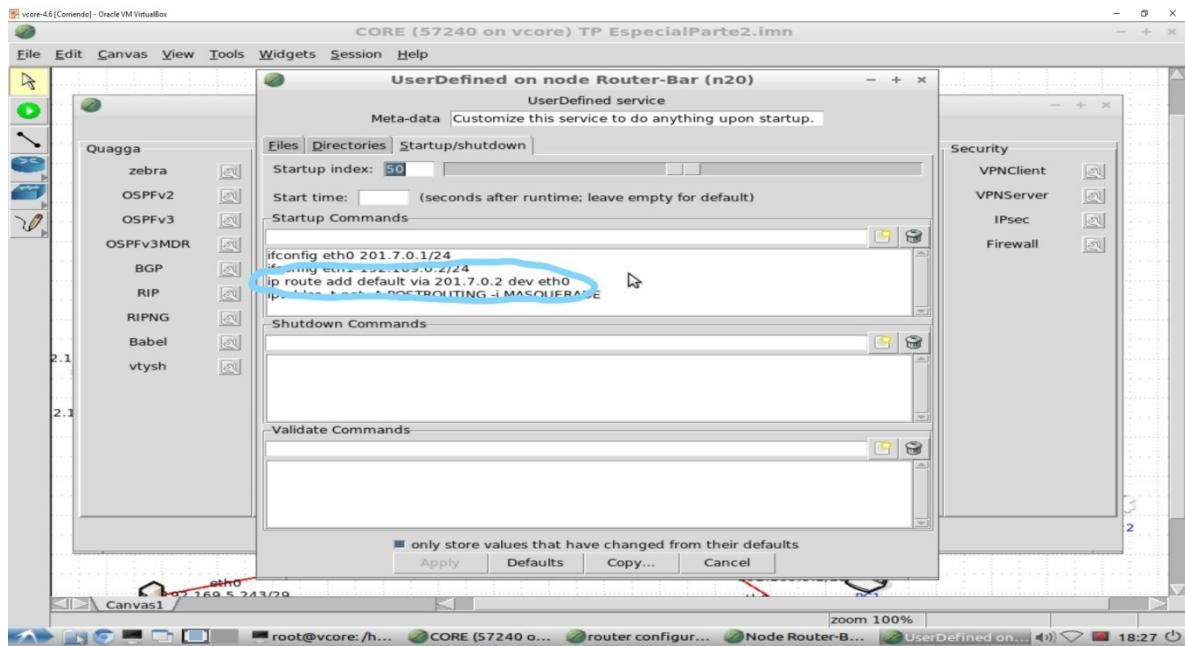


3- Configurar los routers Router-Casa y Router-Bar para que todos los equipos conectados a ellos puedan acceder a internet.

Configurada la tabla de ruteo de ambos Routers para la correcta conexión a Internet de ambos. Esto quiere decir que los usuarios de Router-Casa y de Router-Bar se podrán conectar hacia el ISP, que es lo que habilita la conexión a Internet. Para esto se define por defecto la IP route al ISP más cercano por el cual se enviarán los paquetes, también, haciendo reincidencia sobre el comando MASQUERADE del inciso anterior, se utiliza en combinación con el comando POSTROUTING. Este se utiliza debido a que, si bien ya está claro el destino del paquete y ya pasó por la tabla de ruteo, el paquete hacia internet no puede salir con una IP privada, por eso se “enmascara” y se envía con la dirección pública que posee el Router-NAT.

En esta captura se ven los comandos ejecutados para configurar la tabla de ruteo, Router-Casa y Router-Bar respectivamente:



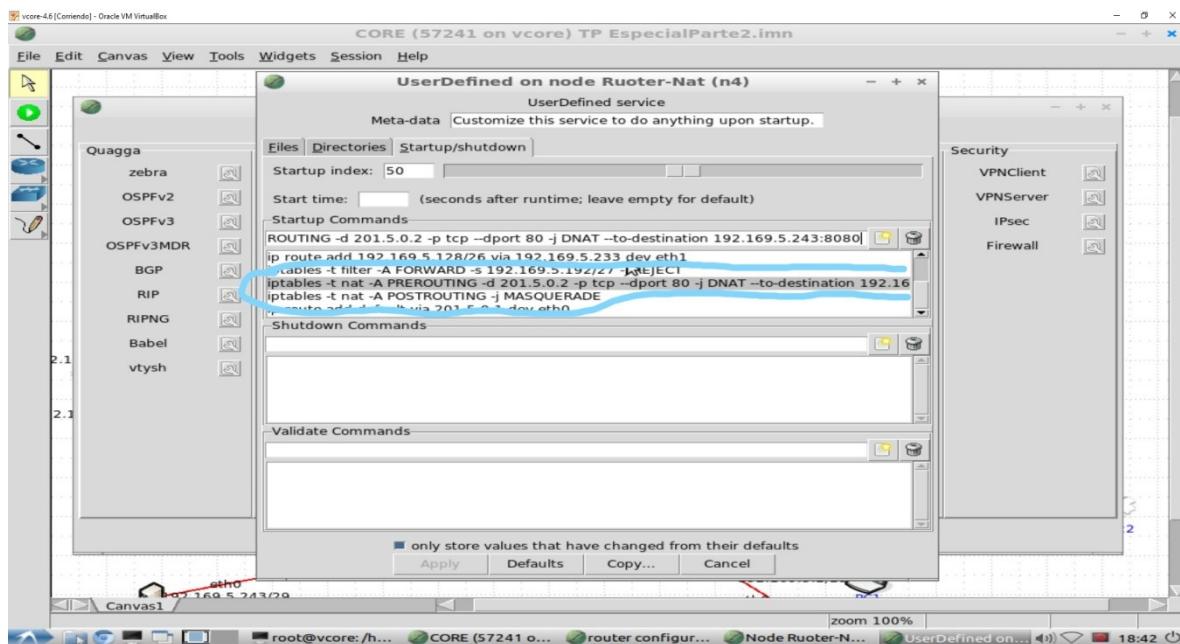


4- Configurar la red de manera de poder enviar un mensaje desde PC-Casa hasta Servidor-1, utilizando Netcat.

Consideraciones:

a. Debe configurar el reenvío de paquetes en Router-Nat

b. El puerto que está abierto en el Router-Nat es el 80, mientras que el servicio en el Servidor-1 está corriendo en el puerto 8080.



En la captura se puede visualizar la configuración del Router-Nat con los comandos ejecutados para el punto en cuestión.

-j DNAT –to-destination [<dirIP>]:<puerto>]

Lo que hace es realizar destination NAT en los paquetes entrantes, es decir que cambia de dirección IP y/o puerto destino. Esto solo puede lograrse en la cadena PREROUTING. Esta regla solo es necesaria para abrir puertos.

Los comandos utilizados para la comunicación son:

- nc -4 -l <puerto>

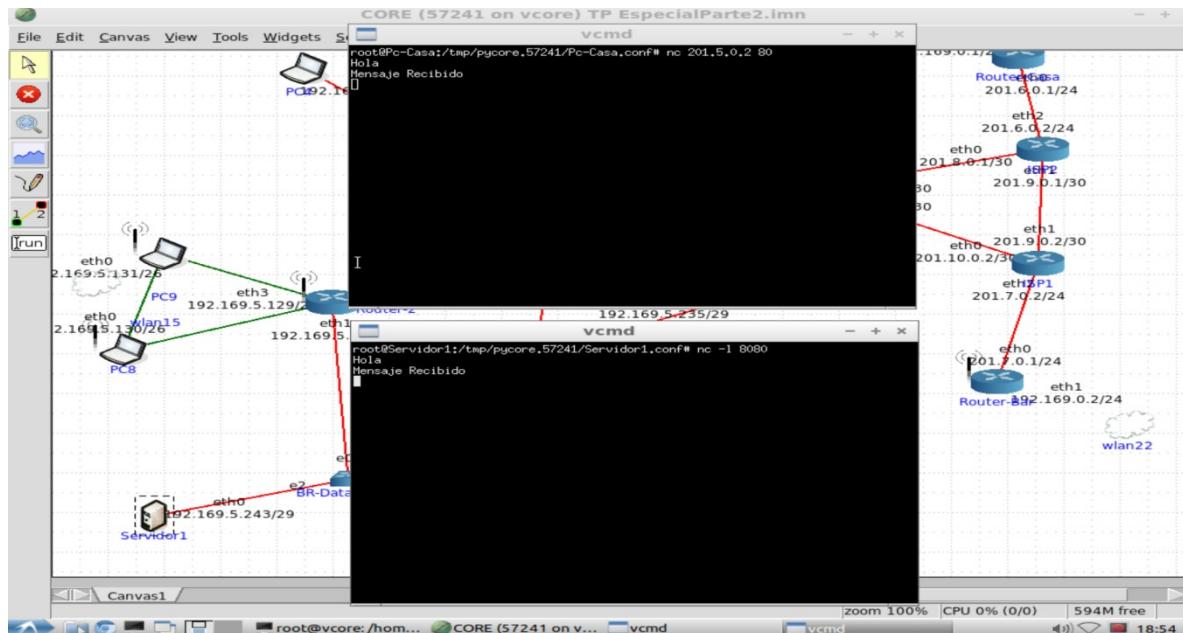
nc proviene de NetCat, -4 de IPV4, -l del modo “listen”, es decir en modo escucha, y el puerto, que en este caso sería el 8080. Este comando se le proporciona al Servidor-1.

En cuanto a PC-Casa, el comando es:

- nc -4 <dirIP> <puerto>

Siendo nc proveniente de NetCat, -4 de IPV4, la dirección IP será la “exterior” del Router-Nat que es el encargado de redireccionar el paquete, y el puerto será el 80, que es el puerto que está abierto.

El -4 se puede obviar debido a que no trabajamos con IPV6.

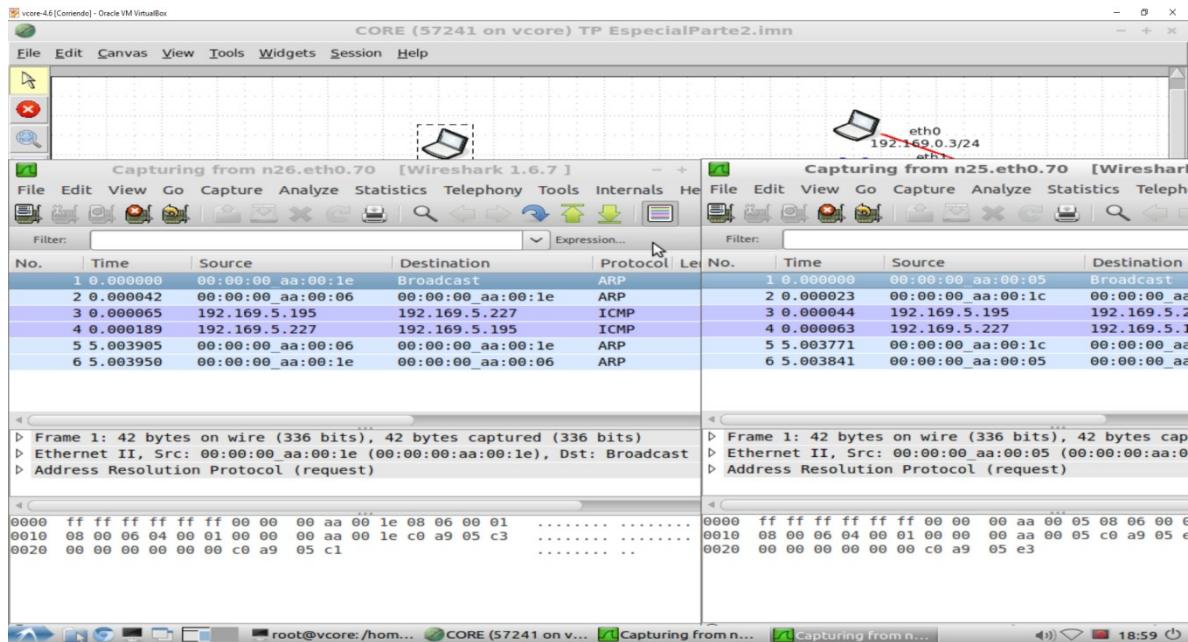


5- Realice un Ping de una PC conectada a Red-Oficina a un equipo conectado a la Red-Admin. Justifique con capturas de Wireshark las diferencias de comportamiento entre el dispositivo Hub y el Bridge. (explique la información de los paquetes capturados)

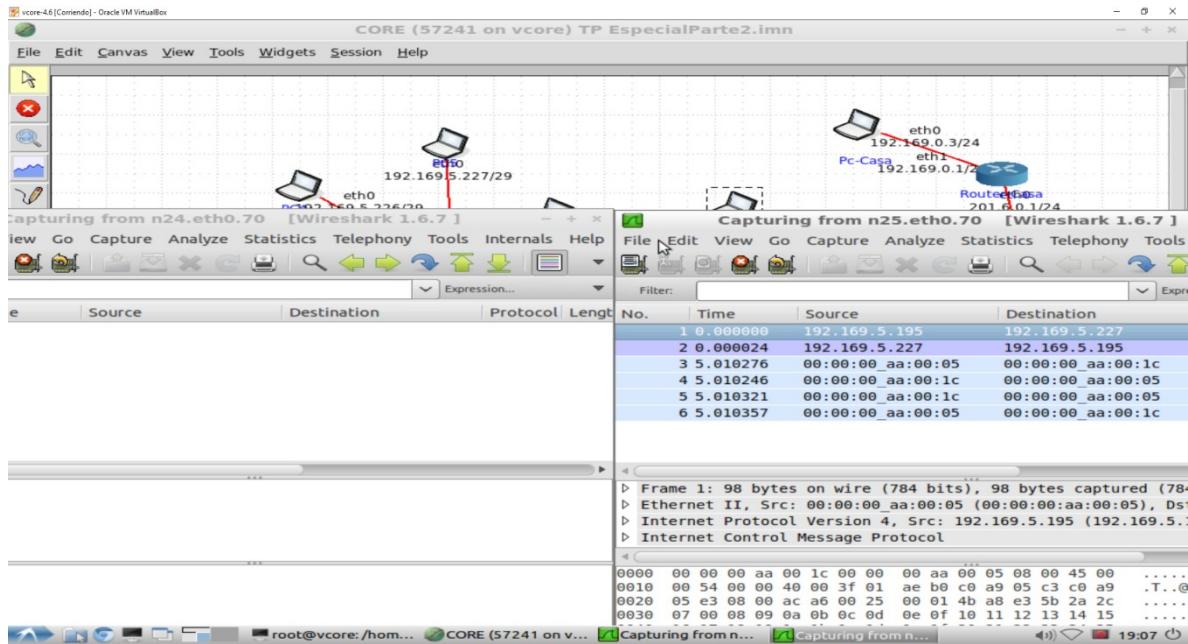
La siguiente captura muestra la realización del comando “ping” desde la PC7, perteneciente a Oficina hacia la PC5 perteneciente a Admin, con la herramienta Wireshark capturando los paquetes de la PC5 y la PC6, perteneciente a Oficina.

Se puede apreciar como el Hub detecta el envío de la PC7 a la PC5, y al pasar por él, también lo envía a la PC6.

N26 corresponde a PC6 y N25 a PC5.



En cambio, en la red Admin, la cual posee un Bridge, se puede observar que los paquetes salientes de PC6, no se envían a PC4, haciendo al Bridge mejor en cuanto a la privacidad.



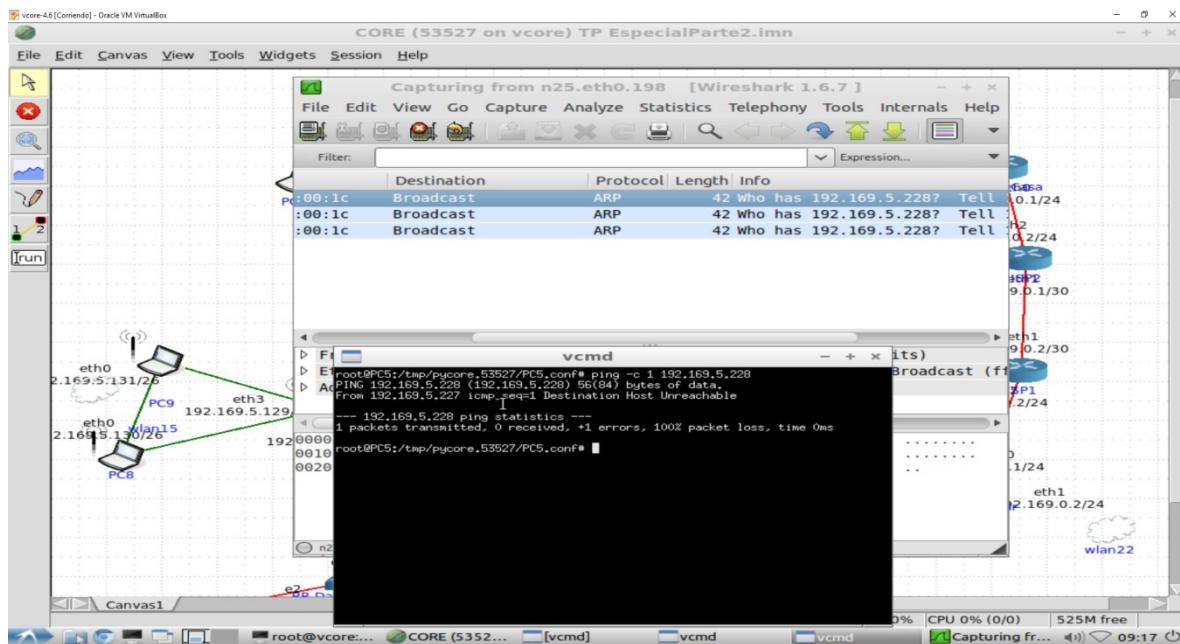
El hub es el dispositivo más sencillo de todos, tiene la función de interconectar los ordenadores de una red local. Se dedica sólo a recibir datos procedentes de un ordenador y transmitirlo a los demás. Es por eso que cuando un paquete es recibido en un puerto, es copiado a todos los demás para que cualquier nodo conectado pueda verlo. Así se ve en la primer captura de pantalla.

El switch es un dispositivo muy semejante al hub, pero envía los datos de manera diferente. A través de un switch aquella información proveniente del ordenador de origen es enviada al ordenador destino, es decir, crean un canal de comunicación exclusivo entre el origen y el destino. Es por eso que en la captura de pantalla n° 2, se ve que en los nodos no incidentes en su comunicación, no reciben nada. El funcionamiento del dispositivo aumenta la respuesta de red ya que la comunicación está siempre disponible, excepto cuando dos o más ordenadores intentan enviar datos simultáneamente a la misma máquina.

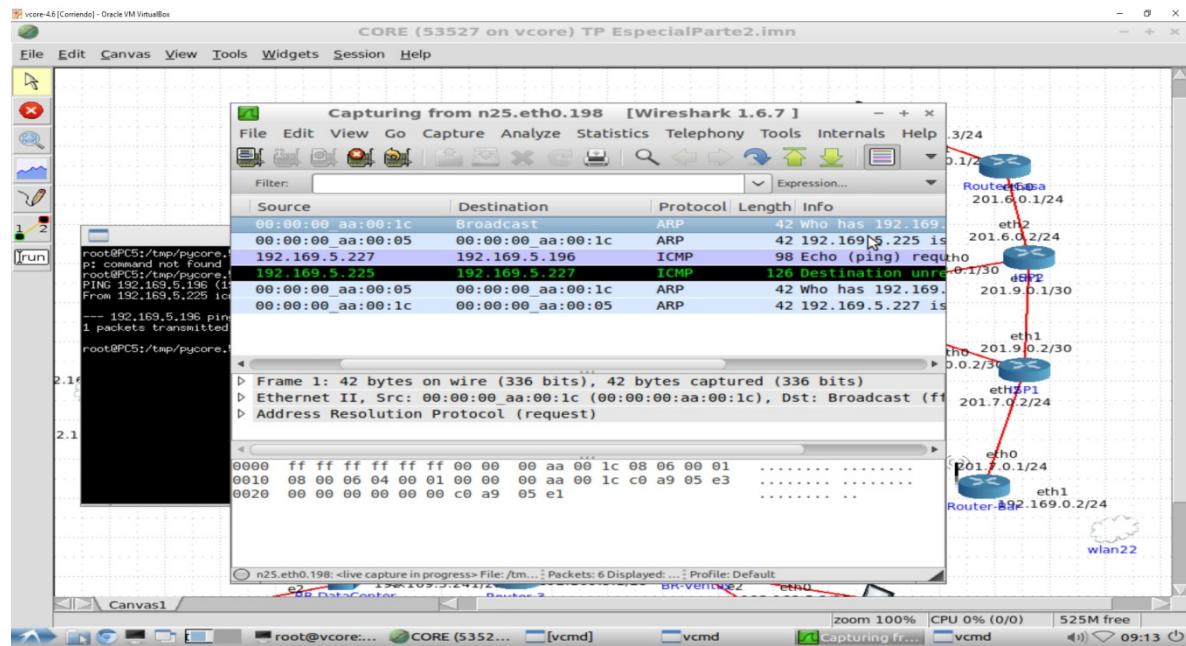
La clara diferencia entre los dos es que el switch distribuye datos a cada máquina destino, mientras que el hub envía todos los datos a todas las máquinas que responden.

6- Realice un Ping (con la opción –c 1) desde una máquina de la Red Admin a una dirección que pertenezca a dicha red pero que no exista el host. Luego realice un Ping (con la opción –c 1) desde la misma máquina de la Red Admin pero a una dirección que pertenezca a la red Oficina y que no exista el host. Desde la máquina origen, analice los paquetes que se generan, explicando las diferencias entre ambas ejecuciones.

Se utiliza el comando “ping” desde la PC5 de la Red Admin, a una dirección de la misma red pero sin que exista el host.



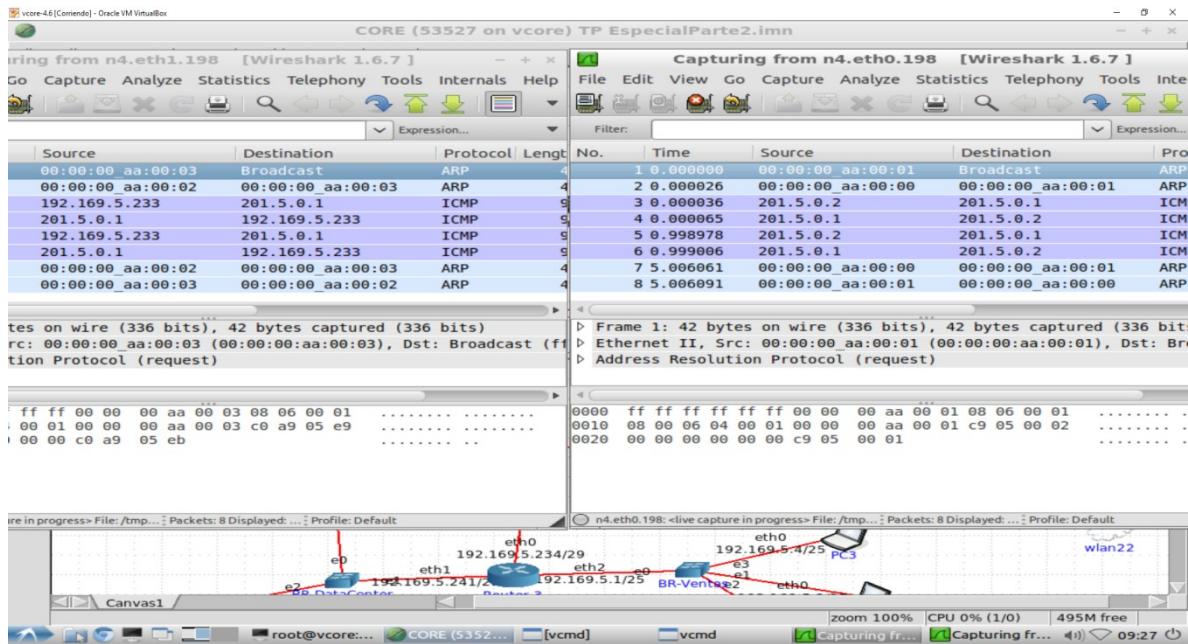
Se observa en la captura la señal enviada desde la PC5, los paquetes ARP que se generaron en el Router 1. Estos preguntan quien tiene la dirección IP 192.169.5.228 (inexistente), para que se lo diga a la dirección IP 192.168.5.227.



En esta captura se observan los paquetes generados en la PC5, donde se genera un paquete ICMP del “ping” y luego se obtiene como respuesta otro paquete ICMP donde avisa que el host es inexistente (destination unreachable), y no puede enviar el paquete. En este caso se está utilizando el comando “ping” con un host inexistente de la Red Oficina.

7- Utilizando capturas de Wireshark y el comando Ping, muestre un ejemplo de intercambio de direcciones IP.

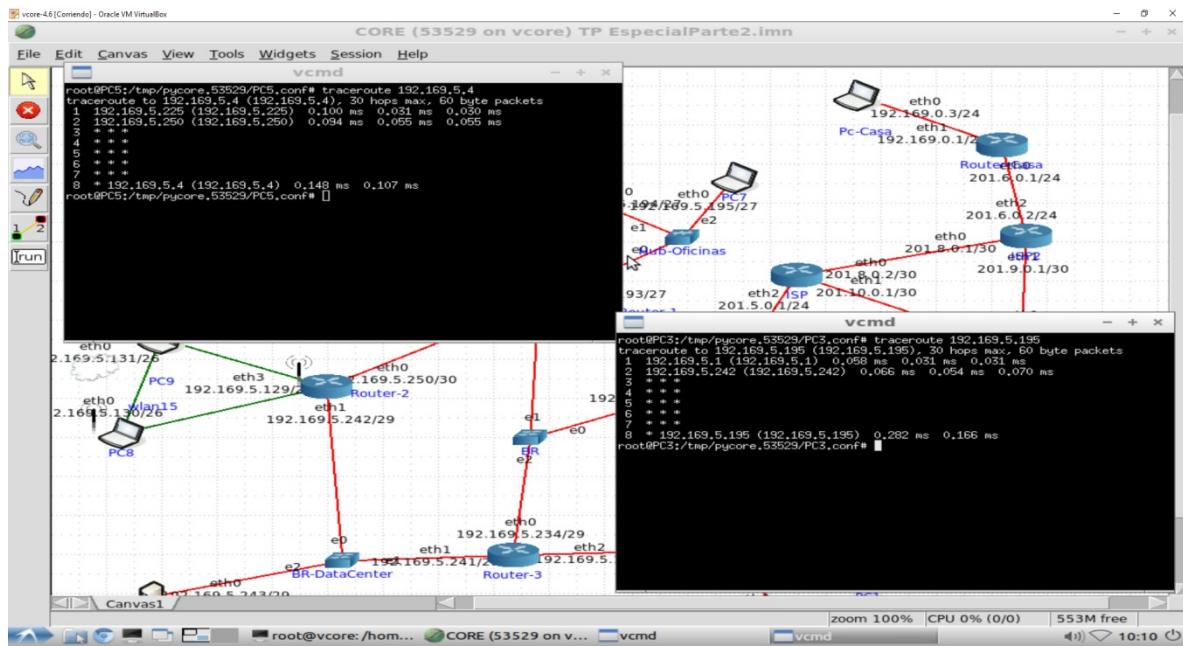
Utilizando el comando “ping” desde el Router-1 hasta el ISP, con la herramienta Wireshark evaluando los paquetes que pasan por el Router-Nat en ambas interfaces, eth1 que es la conexión a la red privada y eth0, conexión a los ISP.



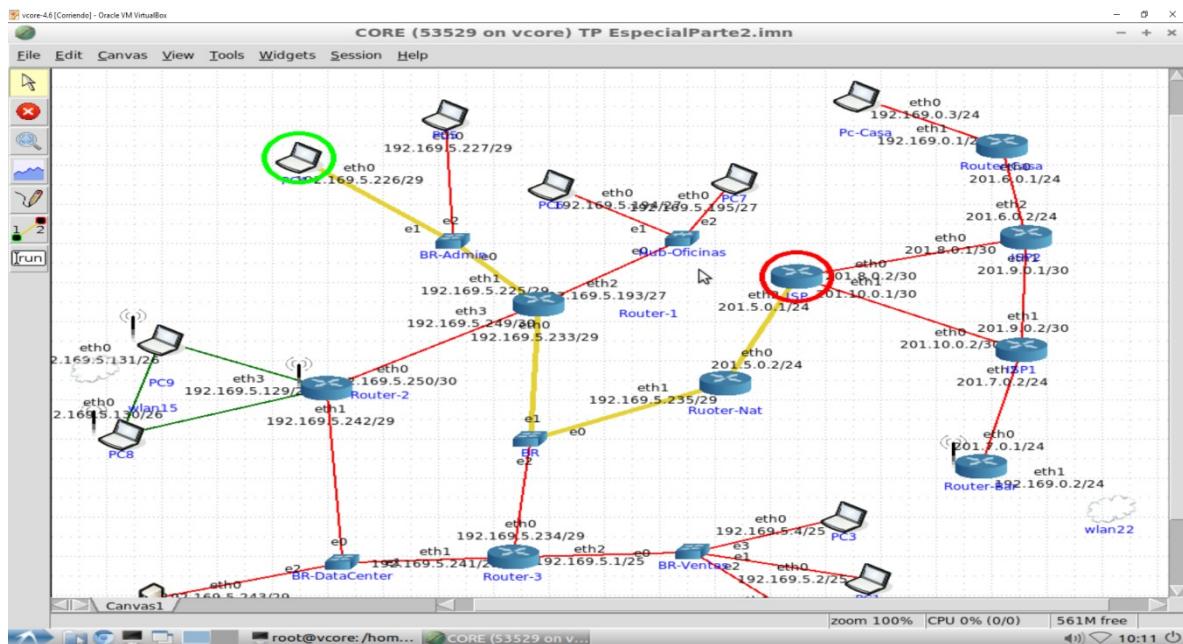
Se puede observar como se genera en el mismo Router-Nat el cambio de IP cuando sale a la Internet, tomando la dirección IP de la red pública.

Esto sucede debido al enmascaramiento de IP, al tener una IP privada no puede conectarse a Internet directamente, por lo que el Router-NAT funciona de “traductor” y “mediador” entre la parte privada y la pública. La función que tiene es recibir los paquetes de alguna dirección privada dentro de la subred, cuando llegan al Router-NAT, modifica la dirección de origen y la cambia con la dirección pública del mismo Router-NAT que es la vía por la cual se llega a Internet, luego, al obtener una respuesta, el paquete de respuesta, llega al Router-NAT y este lo envía con la IP privada, mediante el uso de puertos, a la misma dirección desde la cual se envió el paquete en primera instancia. Es importante remarcar que obligatoriamente ambos paquetes, el primero y el de respuesta, tienen que pasar por el Router-NAT y este tiene que estar configurado con el MASQUERADE, para que esto funcione, sino no habría conexión a Internet de la parte privada y la parte pública no podría comunicarse.

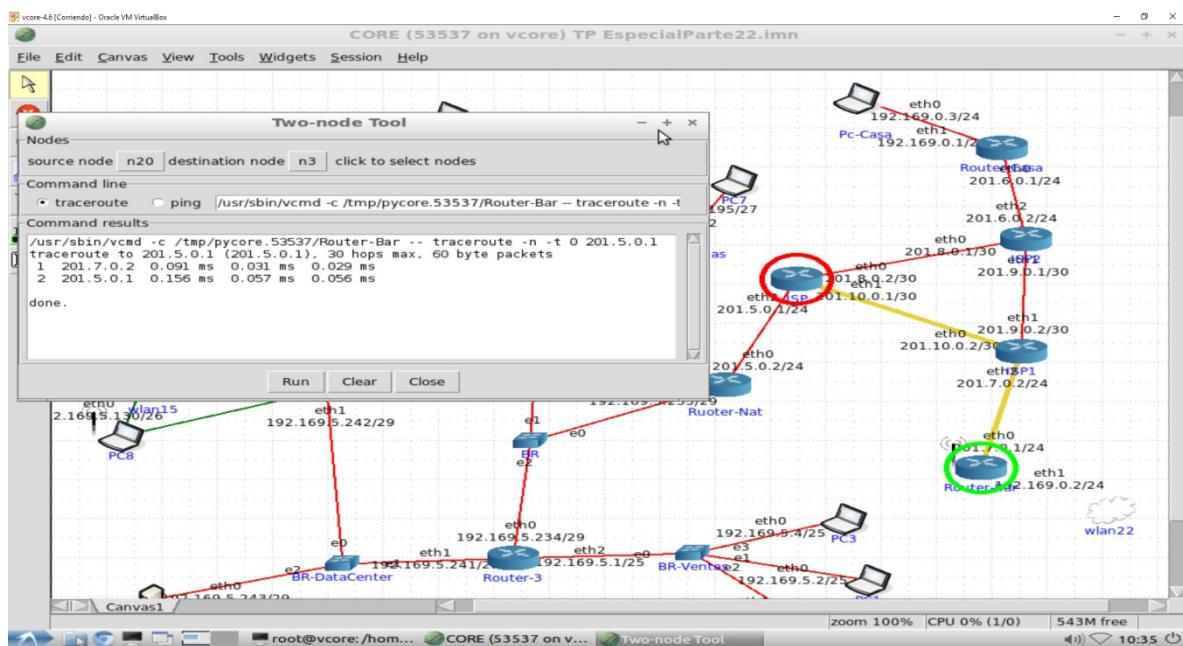
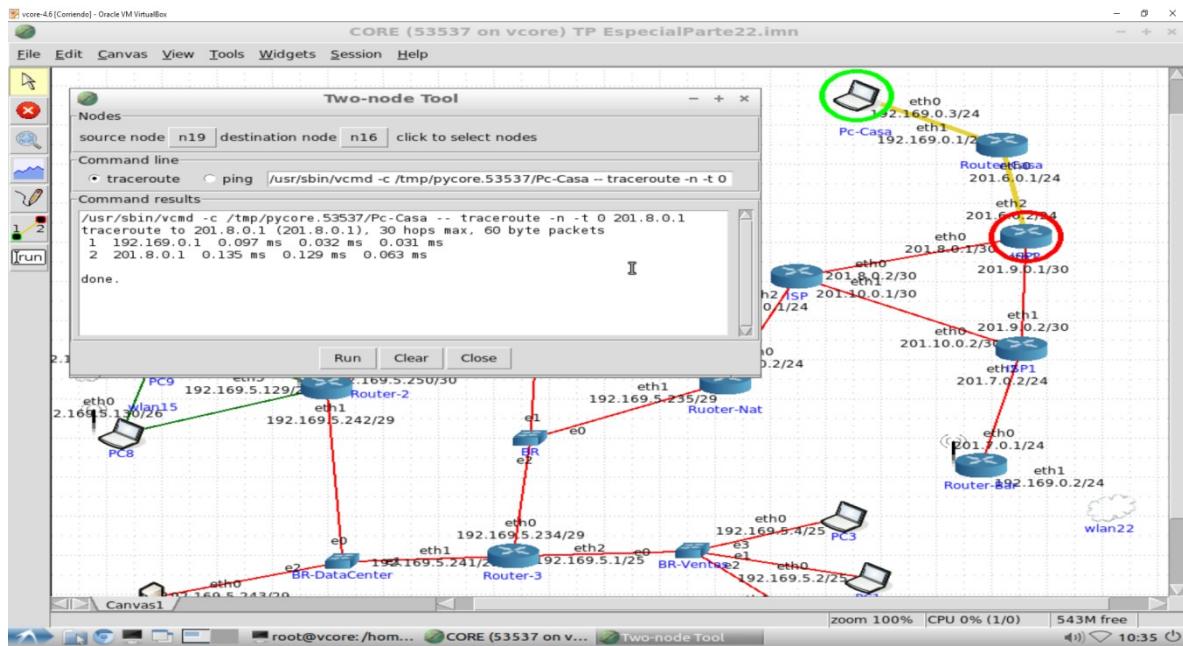
8- Con el comando *TraceRoute*, compruebe que se cumplen las restricciones estipuladas en los incisos anteriores (conectividad dentro de las subredes y con internet).

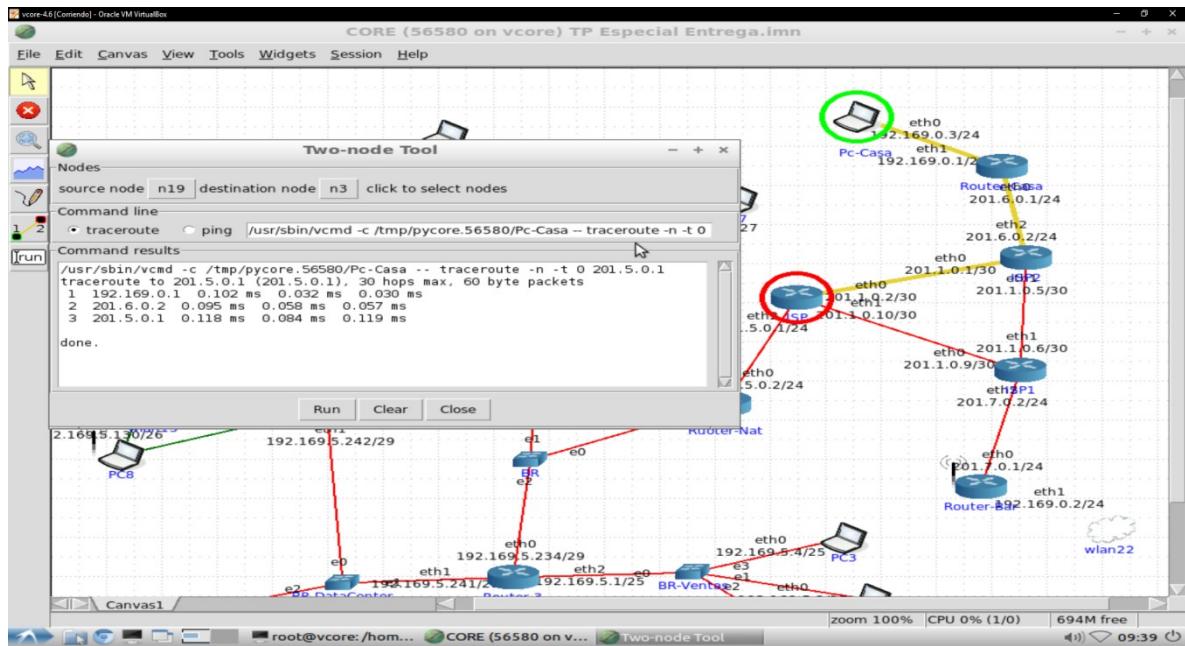


En esta captura se observa dos “traceroute” desde Red Admin a Red Ventas y desde Red Ventas a Red Oficina con el camino que adopta.

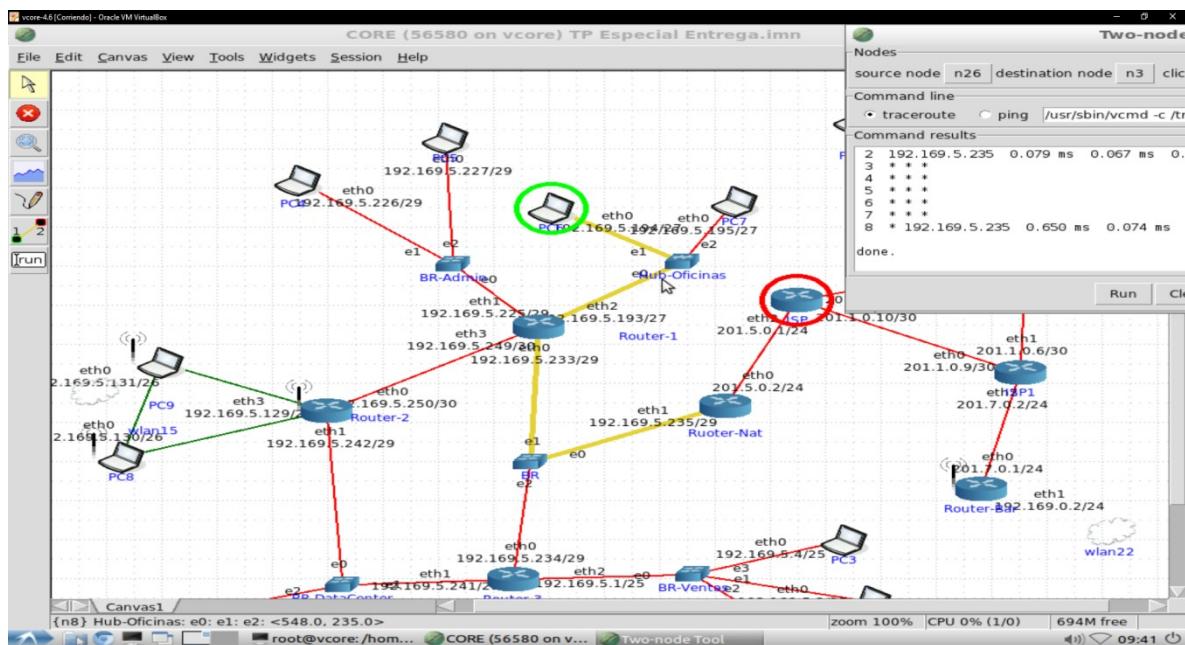


En esta captura se observa la conexión a Internet desde la Red Admin hasta el ISP (condición necesaria para la existencia de la conexión a Internet).



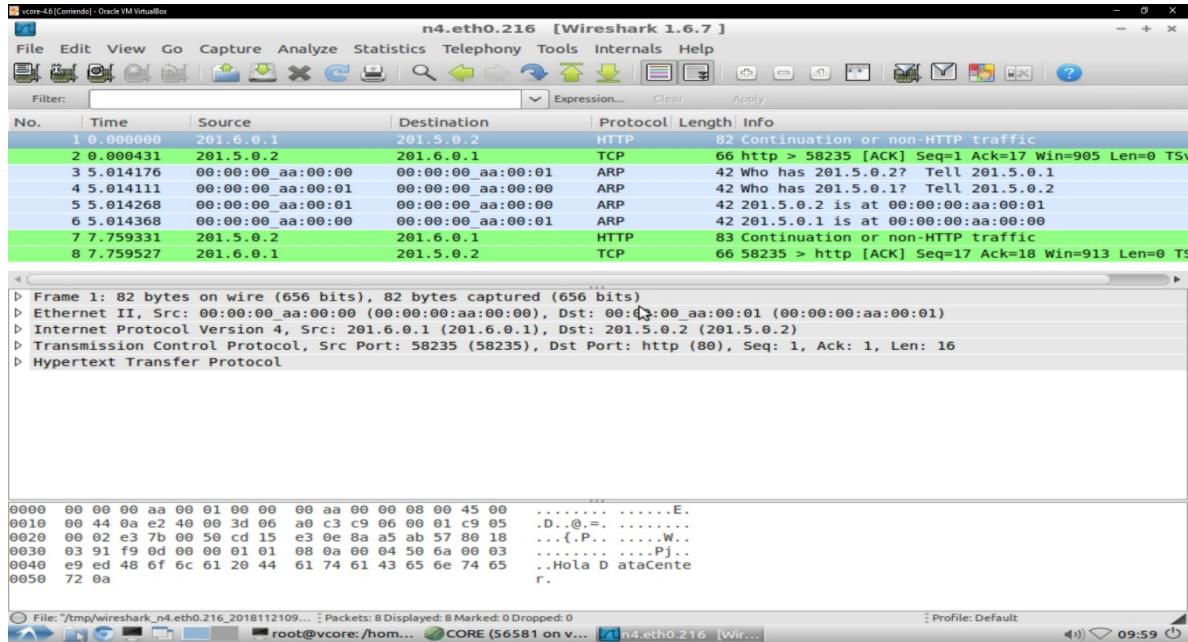


En estas tres capturas se verifican las conexiones a Internet de Router-Casa y de Router-Bar.

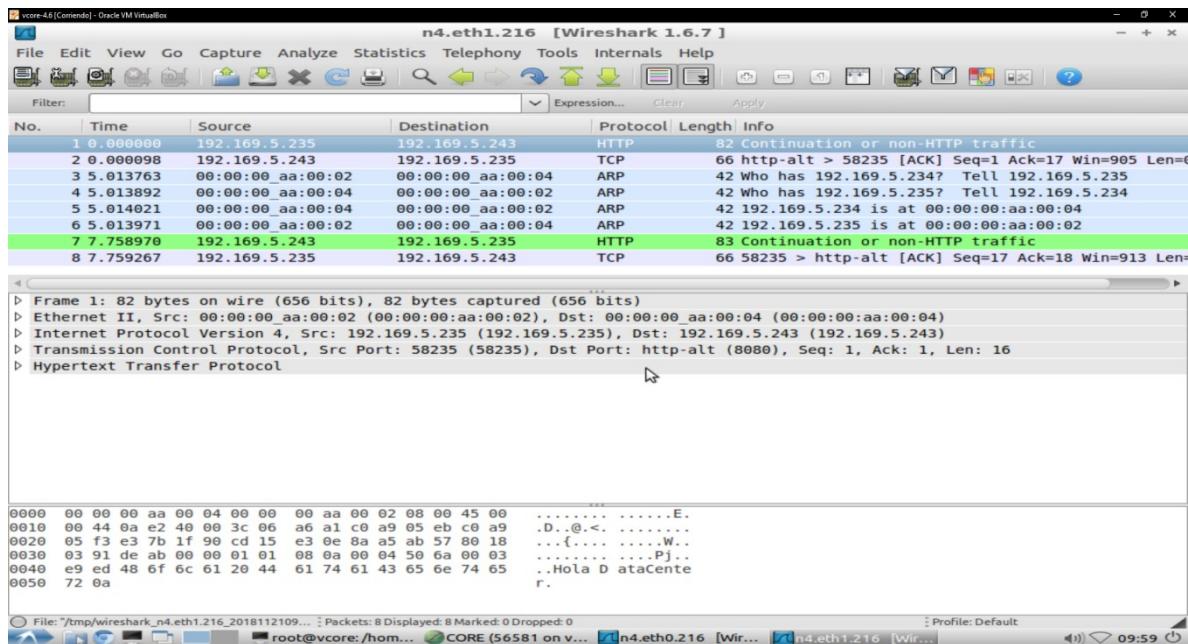


Esta captura indica la incapacidad de conexión a Internet de Oficinas.

9- Utilizando NetCat, enviar el mensaje “Hola Data Center” desde PC-Casa hasta Servidor-1, y luego una confirmación “Mensaje Recibido” desde Servidor-1 hasta PC-Casa. Explique los paquetes que se generan en ambas interfaces del Router-Nat.



Esta captura pertenece a la interfaz eth0, la dirección IP pública del Router-Nat.



Esta captura pertenece a la interfaz eth1, la dirección IP privada del Router-Nat.

En las 2 capturas se ven 3 tipos de Protocolos:

Protocolo ARP: Es el encargado de vincular las direcciones IP con las direcciones de Hardware.

Protocolo TCP: Es el encargado del control de transmisión, es el que asegura que el paquete llegue a destino en orden, sin interrupciones y sin problemas.

Protocolo HTTP: Es el encargado de la conexión entre el cliente y el servidor, que envía un mensaje con la solicitud y si es correcto, se le envía una respuesta con un mensaje similar.

Se ve claramente en la interfaz ETH 0 que primero llega desde la subred 201.6.0.0, hacia el Router-NAT el paquete con el mensaje “Hola DataCenter” y la comprobación de que el paquete haya llegado sin errores por parte del Protocolo TCP. Cuando entra en la subred privada, se envía desde la IP privada del Router-Nat hacia el Servidor1 (ETH1), el mismo paquete con el mensaje “Hola DataCenter”. Una vez que el mensaje llegó, y el Servidor1 responde que el mensaje se recibió correctamente con “Mensaje Recibido”, se envía desde Servidor1 a la IP privada del Router-NAT donde el Protocolo TCP verifica de nuevo que todo se haya conectado correctamente. Nuevamente la dirección pública del Router-NAT (ETH0), luego del MASQUERADE, envía el paquete a la dirección de origen desde donde inicialmente se envió el paquete. El Router-NAT es el encargado de hacer los cambios de puertos y traducciones necesarias, con los comandos explicados previamente, para que llegue desde PC-Casa al Servidor1.

Conclusión

- El método VLSM es un gran avance para la comunicación de datos, aunque cuando se lleva a grandes escalas, no es eficaz. Esto se debe a que las subredes se dividen obligatoriamente en una potencia de 2 y, por ejemplo, si se necesitan exactamente 256 equipos, sin contar con la dirección base y la dirección broadcast , se debería realizar una subred con una disponibilidad de 512 equipos, lo que hace que queden demasiadas direcciones sin ocupar.
- Si se posee una red chica, es improductivo dividirla en muchas subredes debido a que se pierden demasiadas redes en proporción a las obtenidas.
- Por medio de la herramienta Wireshark se observa la composición de cada paquete y al descomponerlo, la disponibilidad de los datos en su envío, las preguntas que se hacen entre receptor y origen para reconocerse, y los movimientos que se realizan para que el paquete con sus datos llegue a destino.
- La importancia del emulador Core para la simulación e implementación de la red, como sus comandos, el sistema operativo que utiliza y sus herramientas.