

Comunicación de Datos I

Trabajo Práctico Especial 2020



N.º de grupo: 26

Autores: Ardito Lautaro - lautaroardito88@gmail.com

Huarte Franco - Franconicolashuarte@hotmail.com

Mazzoni Lucas - lucas.mazzoni@hotmail.com

Ayudante: Leonardo Dominguez

Fecha: 22/10/2020

Índice

Introducción	3
Análisis previo a implementación	4
Ejercicio 1	7
Ejercicio 2	7
VLSM Parque Industrial:	8
VLSM Fabrica A:	9
VLSM Fabrica B:	10
Ejercicio 3	11
Ejercicio 4	12
Tablas de ruteo	13
Ejercicio 5	15
Ejercicio 6	16
Ejercicio 7	17
Ejercicio 8	17
Ejercicio 9	18
Ejercicio 10	21
Ejercicio 11	21
Ejercicio 12	22
Ejercicio 13	24
Ejercicio 14	27
Comandos	30
Conclusión	32
Bibliografía	33

Introducción

En este informe se encontrarán las resoluciones a diferentes consignas planteadas por la cátedra de Comunicación de datos I, donde se mostrarán los pasos para poder desarrollar la comunicación entre tres infraestructuras (siendo el parque industrial, ISP y la casa) con sus respectivas subredes. Para poder resolverlo se utilizó distintos softwares como Core (Herramienta para emular redes) y Wireshark (Analizador de paquetes/protocolos de red).

El objetivo es implementar la siguiente estructura de red (Figura 1) en el Core y a través de diferentes análisis teóricos/prácticos construir una comunicación estable sin conflictos, el desafío planteado en este trabajo es superar los distintos problemas que se nos interpongan en el camino a la hora de construir la red y hacer un análisis completo para lograr responder las consignas del trabajo.

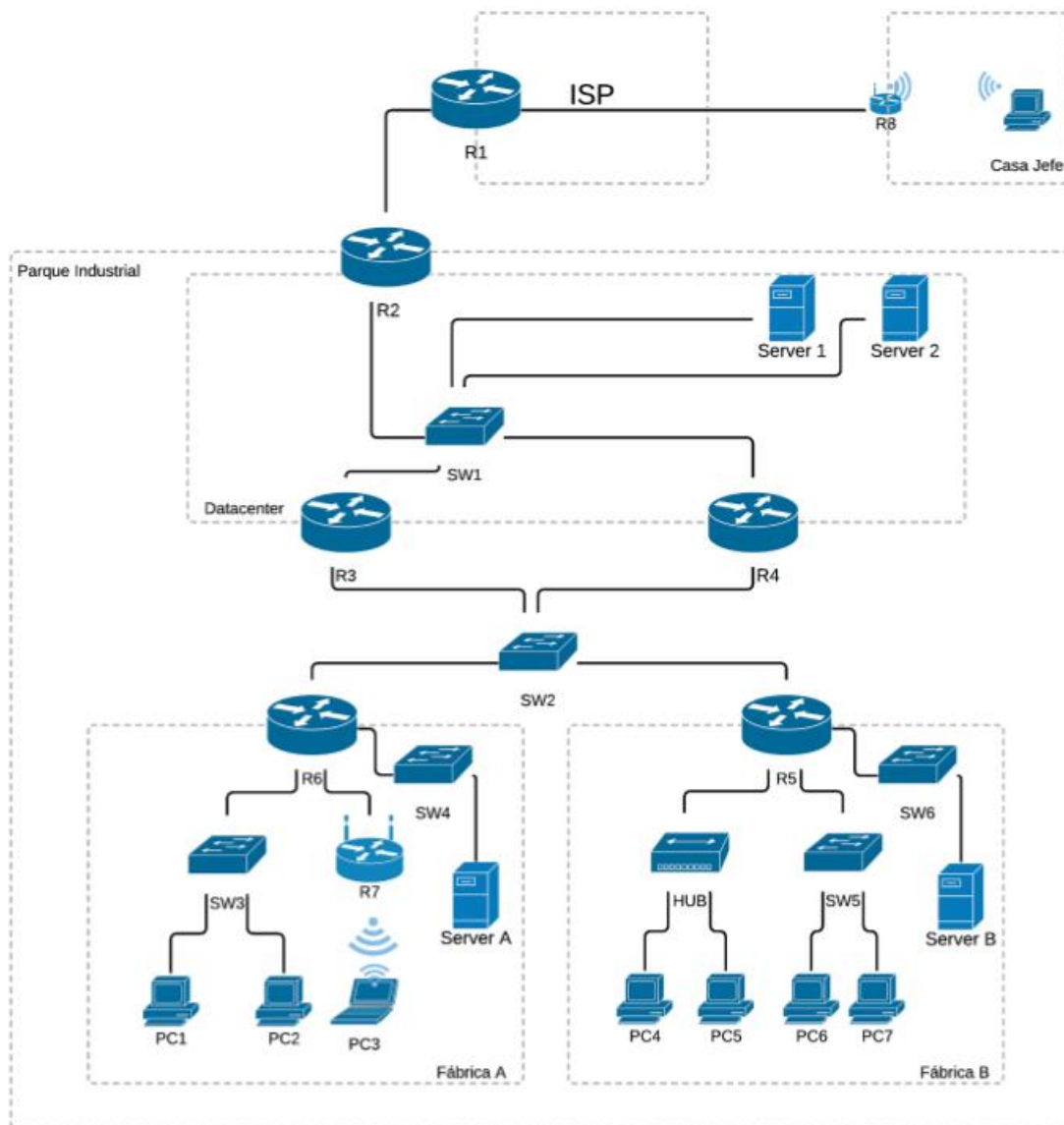


Figura 1 - Topología de red

Análisis previo a implementación

Antes de comenzar a resolver los enunciados se hizo un breve análisis donde se concretó como se iban a dividir las subredes dentro del parque industrial (Figura 2).

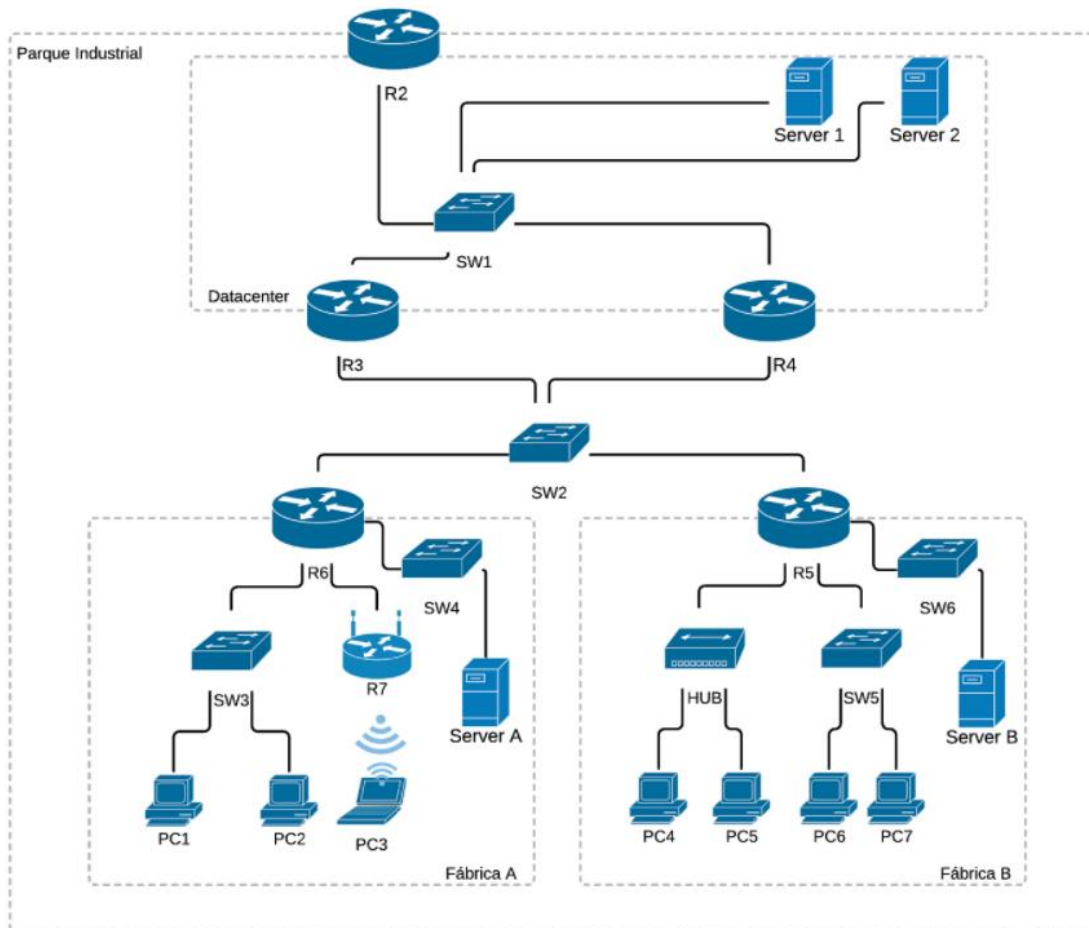


Figura 2 - Topología Parque Industrial

El parque industrial se divide en 4 subredes:

- Red Troncal: En la red troncal reservamos un lugar para conectar como máximo 300 fábricas interconectadas a través del SW2, con actualmente 2 fábricas (como se muestra en la Figura 2) con un bloque de 304 direcciones ip posibles para las fábricas, a su vez también para conectar con el datacenter para un mejor uso a futuro.
- Datacenter: El datacenter cuenta con los equipos frontera DMZ (R2, R3 y R4) necesarios para dar acceso controlado y un espacio en donde se pueden alojar hasta 120 servidores con un bloque de 125 direcciones ip para cada servidor, aunque actualmente tenga 2.

- Fabrica A: La fábrica A se divide internamente en 4 subredes (Figura 3).
 - Red 1 (Wifi): La red 1 cuenta un router Wifi (R7), el cual debe soportar como mínimo 80 equipos, se decidió asignarle un bloque de 83 direcciones ip.
 - Red 2 (SW3): En el SW3 hay actualmente 2 PC conectadas y la cantidad de conexiones que soporta el Switch es 45 dispositivos, se le asigno un bloque de 48 direcciones ip.
 - Red 3 (SW4): En el SW4 se prevé tener hasta 10 servidores, pero actualmente hay solo 1 conectado (Server A), se le asigno un bloque de 13 direcciones ip.
 - Red 4 (R7): Debido a que existe una pequeña subred entre el router R6 y el router R7 decidimos agregarle un pequeño bloque de 4 direcciones ip.

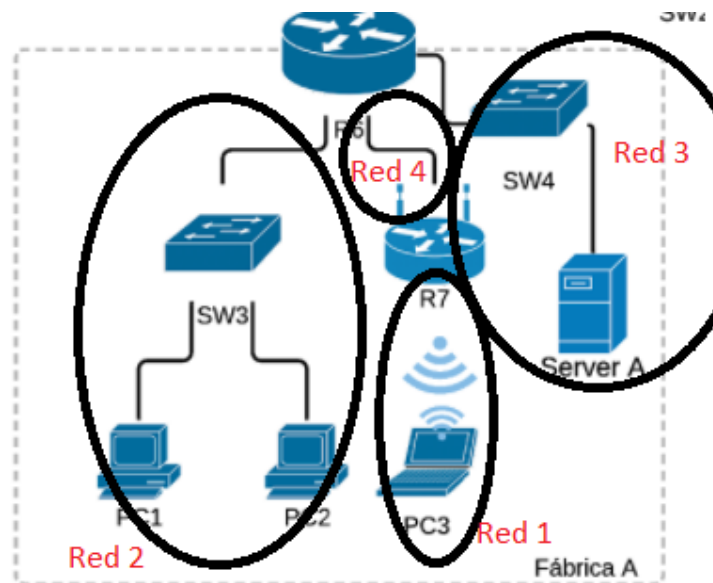


Figura 3 - Subredes Fabrica A

- Fabrica B: La fabrica B consta de 3 subredes (Figura 4).
 - Red 1 (SW5): En el SW5 hay actualmente 2 PC conectadas y la cantidad de conexiones que soporta el Switch es de 65 dispositivos, se le asigno un bloque de 68 direcciones ip.

- Red 2 (SW6): En el SW6 se prevé tener hasta 24 equipos, pero actualmente hay solo 1 conectado (Server B), se le asignó un bloque de 27 direcciones ip.
- Red 3 (HUB): En el HUB hay actualmente 2 PC conectadas y la cantidad de interfaces con las que cuenta el HUB es de 8, se decidió asignarle un bloque de 11 direcciones ip.

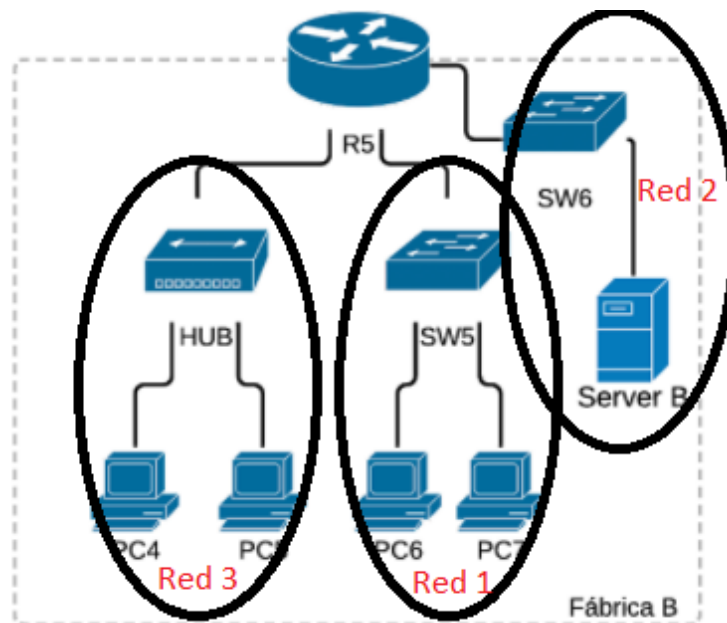


Figura 4 - Subredes Fábrica B

Ejercicio 1

Enunciado: Para la cantidad de conexiones proyectadas para cada una de las redes, realice una asignación de direcciones IP, creando un VLSM general para el parque industrial, y uno particular para cada una de las fábricas. Considere que las direcciones privadas se encuentren en la red 172.26.0.0/20.

Ejercicio 2

Enunciado: 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 de ip asignables que incluye cada bloque.

En este ejercicio se plantearon tres tablas VLSM (Parque industrial, Fábrica A, Fábrica B) donde se deciden varias cuestiones a tener en cuenta, **primero se ordenan las subredes** de mayor requerimiento de host a la de menor requerimiento, de cada subred, luego se calcula el VLSM de cada red a partir de las siguientes definiciones.

Cantidad de direcciones: Las cantidades de direcciones se calcularon dependiendo la cantidad de equipos y/o interfaces que se encuentran en las redes y a su vez se le sumó una dirección base y una dirección broadcast (Ver pág. 4).

N.º bits: Para cada subred, los números de bits se calculan dependiendo de la cantidad de equipos que tendrán que reservarse para hosts a través de la siguiente formula:

$$nbits = \lceil \log_2 (cantidad\ de\ direcciones) \rceil \quad (1)$$

Dirección base: La dirección base se utiliza para identificar donde comienza esa red, casi siempre es una dirección ip par y es la primera del rango que se le asignó a esa red.

Rango asignable: El rango asignable es el conjunto de direcciones ip que puede tomar una subred

Dirección Broadcast: La dirección broadcast sirve para comunicarse con todos los equipos de la red, casi siempre es una dirección ip impar y es la última del rango que se le asigno a la red.

Prefijo: El prefijo se conoce también como la mascara de una subred de longitud variable ya que puede variar de subred en subred. Se puede calcular haciendo la diferencia entre la longitud de la dirección ip (32 bits) y los nbits calculados anteriormente de la siguiente manera:

$$prefixLen = addrLen - nbits \quad (2)$$

VLSM Parque Industrial:

Dada la introducción de la pagina anterior se pasará a conocer como se calculó el VLSM del Parque industrial partiendo de la dirección privada 172.26.0.0 dada por el ejercicio 1.

Se decidió dividir la red en 4 subredes (Red 1, Red 2, Red 3 y Red 4), luego se ordenaron de mayor a menor dependiendo las cantidades de direcciones a tratar (Figura 5).

- **Red 1:** Red troncal
 - Cantidad de direcciones: 302 equipos/interfaces + dirección base + dirección broadcast
 - N.º de bits: Usando la formula (1) dio un resultado de 9
 - Dirección base: 172.26.0.0
 - Dirección Broadcast: 172.26.1.255
 - Prefijo: Usando la formula (2) dio un resultado de 23 y se denota /23

- **Red 2:** Fabrica A
 - Cantidad de direcciones: 210 equipos/interfaces + dirección base + dirección broadcast
 - N.º de bits: Usando la formula (1) dio un resultado de 8
 - Dirección base: 172.26.2.0
 - Dirección Broadcast: 172.26.2.255
 - Prefijo: Usando la formula (2) dio un resultado de 24 y se denota /24

- **Red 3:** Fabrica B
 - Cantidad de direcciones: 174 equipos/interfaces + dirección base + dirección broadcast
 - N.º de bits: Usando la formula (1) dio un resultado de 8
 - Dirección base: 172.26.3.0
 - Dirección Broadcast: 172.26.3.255
 - Prefijo: Usando la formula (2) dio un resultado de 24 y se denota /24

- **Red 4:** Data center
 - Cantidad de direcciones: 123 equipos/interfaces + dirección base + dirección broadcast
 - N.º de bits: Usando la formula (1) dio un resultado de 7
 - Dirección base: 172.26.4.0
 - Dirección Broadcast: 172.26.4.127
 - Prefijo: Usando la formula (2) dio un resultado de 25 y se denota /25

Quedando así 129 direcciones ip libres en un rango de [172.26.4.128 a 172.26.4.255] como se muestra en la Figura 6.

Parque industrial:						
Nombre de subred	Cantidad de direcciones	nº bits	Dirección base	Rango asignable	Dirección broadcast	Prefijo
Red 1 (Red troncal)	304	9	172.26.0.0	[172.26.0.1 a 172.26.1.254]	172.26.1.255	/23
Red 2 (Fabrica A)	212	8	172.26.2.0	[172.26.2.1 a 172.26.2.254]	172.26.2.255	/24
Red 3 (Fabrica B)	176	8	172.26.3.0	[172.26.3.1 a 172.26.3.254]	172.26.3.255	/24
Red 4 (Data center)	125	7	172.26.4.0	[172.26.4.1 a 172.26.4.126]	172.26.4.127	/25

Figura 5 - VLSM Parque Industrial

Forma gráfica de representar en bloques de direcciones de ip asignadas al VLSM del Parque Industrial:

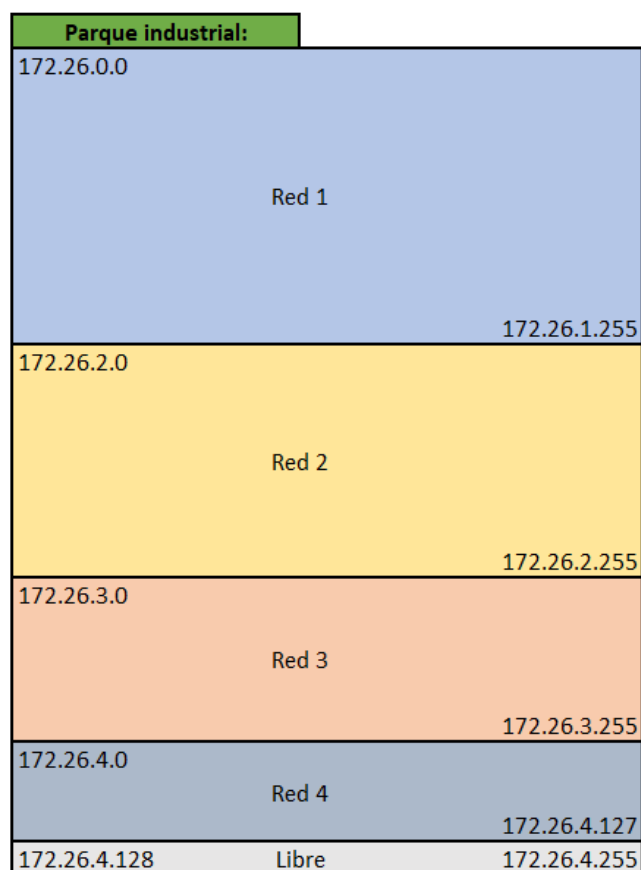


Figura 6 - Representación de VLSM Parque Industrial

VLSM Fabrica A:

La fábrica A cuenta (según con el VLSM del Parque Industrial) con 212 direcciones ip privadas para dividir las en 4 subredes (Red 1, Red 2, Red 3, Red 4).

La forma de calcular los datos de la tabla fueron los mismos pasos que se encuentran en la página 7.

Fabrica A:						
Nombre de subred	Cantidad de direcciones	nº bits	Dirección base	Rango asignable	Dirección broadcast	Prefijo
Red 1 (Wifi)	83	7	172.26.2.0	[172.26.2.1 a 172.26.2.126]	172.26.2.127	/25
Red 2 (SW3)	48	6	172.26.2.128	[172.26.2.129 a 172.26.2.190]	172.26.2.191	/26
Red 3 (SW4)	13	4	172.26.2.192	[172.26.2.193 a 172.26.2.206]	172.26.2.207	/28
Red 4 (R7)	4	2	172.26.2.208	[172.26.2.209 a 172.26.2.210]	172.26.2.211	/30

Figura 7 - VLSM Fabrica A

La fábrica A además cuenta con 45 direcciones ip Libres en un rango de [172.26.2.212 a 172.26.2.255] como se muestra en la Figura 8.

Forma gráfica de representar en bloques de direcciones de ip asignadas al VLSM de la Fabrica A:

Fabrica A:		
172.26.2.0	Red 1 (Wifi)	172.26.2.127
172.26.2.128	Red 2 (SW3)	172.26.2.191
172.26.2.192	Red 3 (SW4)	172.26.2.207
172.26.2.208	Red 4 (R7)	172.26.2.211
172.26.2.212	Libre	172.26.2.255

Figura 8 - Representación de VLSM Fabrica A

VLSM Fabrica B:

La fábrica B cuenta con 176 direcciones ip privadas para dividir las en 3 subredes (Red 1, Red 2, Red 3).

La forma de calcular los datos de la tabla fueron los mismos pasos que se encuentran en la página 7.

Fabrica B:						
Nombre de subred	Cantidad de direcciones	nº bits	Dirección base	Rango asignable	Dirección broadcast	Prefijo
Red 1 (SW5)	68	7	172.26.3.0	[172.26.3.1 a 172.26.3.126]	172.26.3.127	/25
Red 2 (SW6)	27	5	172.26.3.128	[172.26.3.129 a 172.26.3.158]	172.26.3.159	/27
Red 3 (HUB)	11	4	172.26.3.160	[172.26.3.161 a 172.26.3.174]	172.26.3.175	/28

Figura 9 - VLSM Fabrica B

La fábrica B además cuenta con 81 direcciones ip Libres en un rango de [172.26.3.176 a 172.26.3.255] como se muestra en la Figura 10.

Forma gráfica de representar en bloques de direcciones de ip asignadas al VLSM de la Fabrica B:

Fabrica B:		
172.26.3.0	Red 1 (SW5)	172.26.3.127
172.26.3.128	Red 2 (SW6)	172.26.3.159
172.26.3.160	Red 3 (HUB)	172.26.3.175
172.26.4.176	Libre	172.26.4.255

Figura 10 - Representación de VLSM Fabrica B

Ejercicio 3

Enunciado: 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.

Este ejercicio se podrá observar mejor en el archivo. inm adjuntado junto con este informe, pero en la figura 11 se observa un breve pantallazo de lo simulado en el emulador Core.

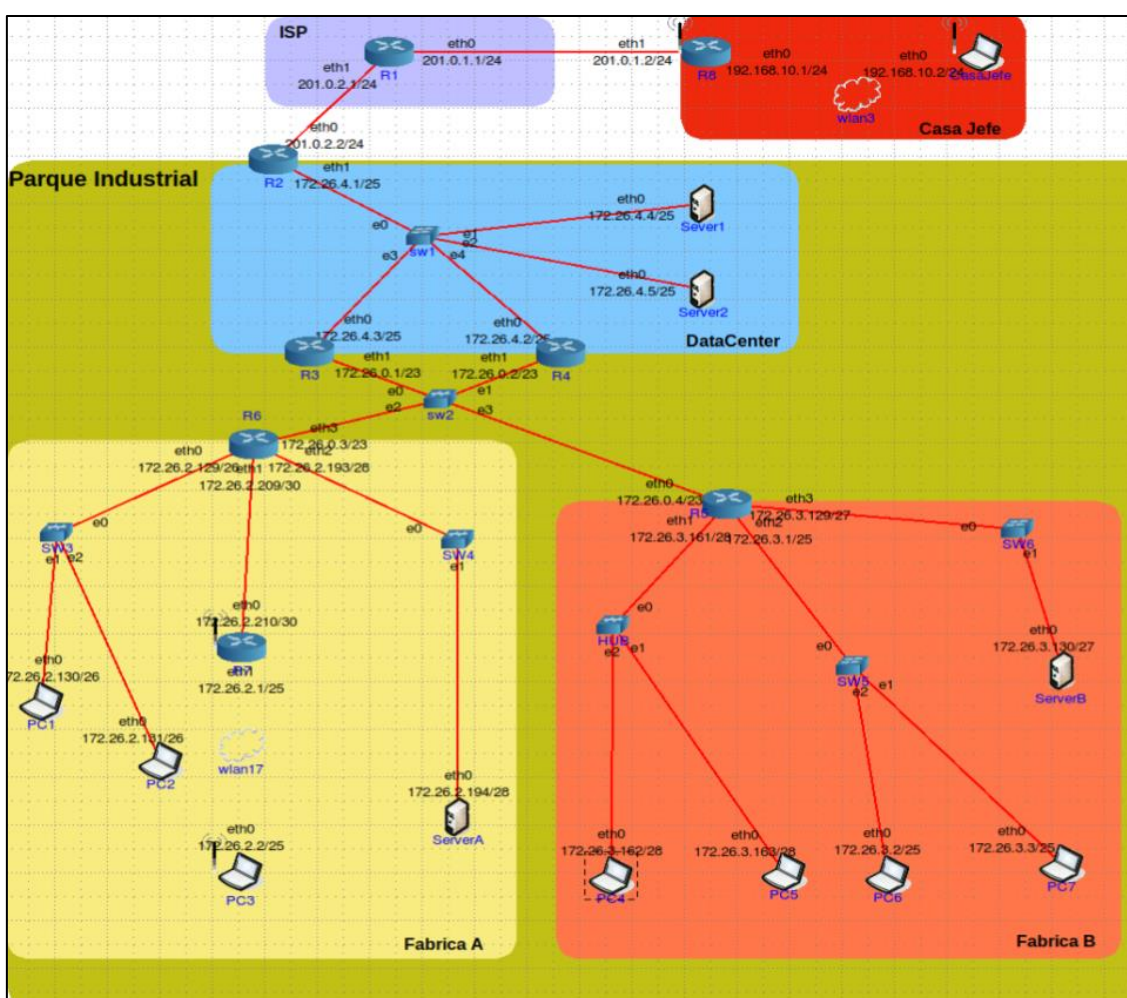


Figura 11- Implementación en emulador Core

Ejercicio 4

Enunciado: Configurar todas las interfaces y rutas de los routers y hosts, **minimizando** la cantidad de entradas en las tablas de ruteo (considere el uso de rutas por defecto) para que todas las redes del parque industrial estén interconectadas.

Cabe destacar que los comandos correspondientes deben estar cargados en la opción “User Defined” -> “Startup Commands” de cada dispositivo, y que dentro de los servicios sólo deben quedar habilitados el “IP FORWARD” y “User Defined”.

Tenga en cuenta que el router del ISP no lleva ruta por defecto.

En este ejercicio lo que se hizo fue una tabla para cada router del parque industrial donde contiene las diferentes redes asignadas en los incisos anteriores, donde se le indicó por medio de cada router hacia donde debería reenviar el paquete que le llega al mismo por un determinado destino.

En primera instancia lo que se hizo es hacer las tablas sin minimizar de tal forma que:

- D/I: Indica de qué forma esta comunicada la red, siendo “D” red conectada de forma directa e “I” red conectada de forma indirecta.
- Int: En este campo indica el medio por el que se mandan los paquetes.
- Próximo router: Medio por donde tiene que pasar el paquete para llegar a la red (Se les asigna a las redes que no están conectadas de forma directa).

En las redes indirectas se analizó la posibilidad de una minimización ya que una gran parte de la red están en bloques contiguos y pasan por un mismo router como bien se muestra en la figura 13. Lo que aparece marcado en **rojo** son las direcciones sin minimizar y lo que aparece marcado en **verde** son las redes minimizadas.

Tabla de reenvio R3			
Red	D/I	Int	Proximo Router
172.26.3.5/25	D	eth0	-
172.26.0.2/23	D	eth1	-
172.26.2.0/25	I	eth1	172.26.0.3
172.26.2.128/26	I	eth1	172.26.0.3
172.26.2.192/28	I	eth1	172.26.0.3
172.26.2.208/30	I	eth1	172.26.0.3
172.26.2.0/24	I	eth1	172.26.0.3
172.26.3.0/25	I	eth1	172.26.0.4
172.26.3.128/27	I	eth1	172.26.0.4
172.26.3.160/28	I	eth1	172.26.0.4
172.26.3.0/24	I	eth1	172.26.0.4

Figura 12 - Tabla de ruteo R3

Ejemplo Router 3

172.26.2.0/25 = 172.26.2.00000000
 172.26.2.128/26 = 172.26.2.10000000
 172.26.2.192/28 = 172.26.2.11000000
 172.26.2.208/30 = 172.26.2.11011000

Aumentamos el prefijo para que pueda contemplar todas las variaciones de host necesarias.

172.26.2.0/24 = 172.26.2.00000000 \Rightarrow Red minimizada con prefijo /24

172.26.3.0/25 = 172.26.3.00000000
 172.26.3.128/27 = 172.26.3.10000000
 172.26.3.160/28 = 172.26.3.10100000

172.26.3.0/24 = 172.26.3.00000000 \Rightarrow Red minimizada con prefijo /24

Figura 13 - Ejemplo: Minimización R3

Tablas de ruteo

Teniendo en cuenta lo que se planteó en el ejemplo anterior, se hizo lo mismo para los siguientes routers.

Tabla de reenvío R2			
Red	D/I	Int	Proximo Router
201.0.1.2/24	D	eth0	-
172.26.4.1/25	D	eth1	-
172.26.3.0/24	I	eth1	172.26.4.3
172.26.2.0/24	I	eth1	172.26.4.3
172.26.0.0/23	I	eth1	172.26.4.3
172.26.0.0/22			172.2.4.3
Default(0.0.0.0/0)	I	eth0	201.0.1.1

Figura 14 - Tabla de ruteo R2

Tabla de reenvio R4			
Red	D/I	Int	Proximo Router
172.26.3.4/25	D	eth0	-
172.26.0.1/23	D	eth1	-
172.26.2.0/25	I	eth1	172.26.0.3
172.26.2.128/26	I	eth1	172.26.0.3
172.26.2.192/28	I	eth1	172.26.0.3
172.26.2.208/30	I	eth1	172.26.0.3
172.26.2.0/24	I	eth1	172.26.0.3
172.26.3.0/25	I	eth1	172.26.0.4
172.26.3.128/27	I	eth1	172.26.0.4
172.26.3.160/28	I	eth1	172.26.0.4
172.26.3.0/24	I	eth1	172.26.0.4
Default(0.0.0.0/0)	I	eth1	172.26.4.1

Figura 15 - Tabla de ruteo R4

Tabla de reenvio R5			
Red	D/I	Int	Proximo Router
172.26.3.0/25	D	eth2	-
172.26.3.128/27	D	eth3	-
172.26.3.160/28	D	eth1	-
172.26.2.0/25	I	eth0	172.26.0.3
172.26.2.128/26	I	eth0	172.26.0.3
172.26.2.192/28	I	eth0	172.26.0.3
172.26.2.208/30	I	eth0	172.26.0.3
172.26.2.0/24	I	eth0	172.26.0.3
172.26.4.0/25	I	eth0	172.26.0.1
Default(0.0.0.0/0)	I	eth0	172.26.0.2

Figura 16 - Tabla de ruteo R5

Tabla de reenvio R6			
Red	D/I	Int	Proximo Router
172.26.2.128/26	D	eth1	-
172.26.2.192/28	D	eth2	-
172.26.2.208/30	D	eth3	-
172.26.3.0/25	I	eth3	172.26.0.4
172.26.3.128/27	I	eth3	172.26.0.4
172.26.3.160/28	I	eth3	172.26.0.4
172.26.3.0/24	I	eth3	172.26.0.4
172.26.2.0/25	I	eth0	172.26.2.210
172.26.4.0/25	I	eth0	172.26.0.1
Default(0.0.0.0/0)	I	eth0	172.26.0.2

Figura 17 - Tabla de ruteo R6

Tabla de reenvio R7			
Red	D/I	Int	Proximo Router
172.26.2.208/30	D	eth0	-
172.26.2.0/25	D	eth1	-
172.26.3.0/25	I	eth0	172.26.2.209
172.26.3.128/27	I	eth0	172.26.2.209
172.26.3.160/28	I	eth0	172.26.2.209
172.26.4.0	I	eth0	172.26.2.209
Default(0.0.0.0/0)	I	eth0	172.26.2.209

Figura 18 - Tabla de ruteo R7

Ejercicio 5

Enunciado: Configurar el R2 para que solo tengan acceso a internet los equipos conectados a la red Datacenter, Fábrica A y Fabrica B.

En este inciso se logró comunicar los equipos conectados del Datacenter, Fabrica A y Fabrica B con internet atreves de los siguientes comandos mostrados en la figura 19 (señalizados con ←).

Los comandos:

- I. `iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE`
- II. `iptables -t filter -A FORWARD -s 172.26.3.0/24 -j ACCEPT`
- III. `iptables -t filter -A FORWARD -s 172.26.4.0/25 -j ACCEPT`
- IV. `iptables -t filter -A FORWARD -s 172.26.2.0/24 -j ACCEPT`
- V. `iptables -t filter -A FORWARD -o eth0 -j REJECT`

El comando I se utilizó para convertir de IPs privadas a IPs públicas.

Los comandos II, III y IV son condiciones donde se verifica si el paquete viene de las redes 172.26.3.0/24 (Fabrica B) o de la red 172.26.4.0/25 (Datacenter) o de la red 172.26.2.0/24 (Fabrica A) este acepta los paquetes de los equipos de las redes mencionadas anteriormente.

El comando V rechaza todos los paquetes que no acepta o no están aclarados dentro de la configuración de R2.

```

ifconfig eth1 172.26.4.1/25 up
ifconfig eth0 201.0.2.2/24 up
ip route add default via 201.0.2.1 dev eth0
ip route add 172.26.0.0/22 via 172.26.4.3 dev eth1
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
iptables -t filter -A FORWARD -s 172.26.3.0/24 -j ACCEPT
iptables -t filter -A FORWARD -s 172.26.4.0/25 -j ACCEPT
iptables -t filter -A FORWARD -s 172.26.2.0/24 -j ACCEPT
iptables -t nat -A PREROUTING -p tcp --dport 80 -j DNAT --to 172.26.4.4:8080
iptables -t filter -A FORWARD -o eth0 -j REJECT

```

Figura 19 - Configuración R2

Ejercicio 6

Enunciado: Configurar el R5 para que todos los dispositivos del área de servicio conectados a través del HUB solo se puedan conectar al resto de los equipos de la Fábrica B y también a los equipos del centro de cómputo conectados en el Datacenter.

En este inciso se usaron los comandos que se muestran en la figura 20 donde a través de estos se logra configurar R5 para que los dispositivos del HUB solo se puedan comunicar con la Fabrica B y el Datacenter.

Los primeros tres comandos señalados (←) en la figura 20 son condiciones donde si el paquete proviene de la red correspondiente utilizando como intermediario el router 5 entonces este comando los acepta.

El ultimo comando de la figura 20 (también señalado con ←) rechaza todos los paquetes que no acepta o no están aclarados dentro de la configuración de R5.

```

ifconfig eth1 172.26.3.161/28 up
ifconfig eth2 172.26.3.1/25 up
ifconfig eth3 172.26.3.129/27 up
ifconfig eth0 172.26.0.4/23 up
ip route add default via 172.26.0.2 dev eth0
ip route add 172.26.2.0/24 via 172.26.0.3 dev eth0
iptables -t filter -A FORWARD -i eth1 -d 172.26.4.0/25 -o eth0 -j ACCEPT
iptables -t filter -A FORWARD -i eth1 -d 172.26.3.0/24 -o eth2 -j ACCEPT
iptables -t filter -A FORWARD -i eth1 -d 172.26.3.0/24 -o eth3 -j ACCEPT
iptables -t filter -A FORWARD -i eth1 -j REJECT

```

Figura 20 - Configuración R5

Ejercicio 7

Enunciado: Configurar el R8 para que la PC-Casa pueda acceder a internet.

En este inciso se utilizó el comando de la figura 21 (←) para convertir la ip privada de la red donde se encuentra la casa jefe a una ip pública.

```
ifconfig eth0 192.168.10.1/24 up
ifconfig eth1 201.0.1.2/24 up
ip route add default via 201.0.1.1 dev eth1
iptables -t nat -A POSTROUTING -o eth1 -j MASQUERADE ←
```

Figura 21 - Configuración R8

Ejercicio 8

Enunciado: Por cuestiones de seguridad, todo el tráfico proveniente de las fábricas y dirigido al datacenter debe pasar por el router R3, y el tráfico dirigido a Internet, debe pasar por el router R4.

En este inciso se modificaron las configuraciones del router R5 y R6 para así lograr dividir los paquetes dirigidos a internet y los paquetes dirigidos al Datacenter.

Como bien muestra en ambas figuras (22 y 23) la flecha de color rojo indica la ruta por defecto que circula todo el trafico de internet por la dirección ip 172.26.0.2 (R4) por su respectivo puerto. Mientras que la flecha de color azul indica que todo el tráfico dirigido a la red 172.26.4.0/25 (red troncal) tiene que transitar por la dirección ip 172.26.0.1 (R3) por su respectivo puerto.

```
ifconfig eth1 172.26.3.161/28 up
ifconfig eth2 172.26.3.1/25 up
ifconfig eth3 172.26.3.129/27 up
ifconfig eth0 172.26.0.4/23 up
ip route add default via 172.26.0.2 dev eth0 ←
ip route add 172.26.4.0/25 via 172.26.0.1 dev eth0 ←
ip route add 172.26.2.0/24 via 172.26.0.3 dev eth0
iptables -t filter -A FORWARD -i eth1 -d 172.26.4.0/25 -o eth0 -j ACCEPT
iptables -t filter -A FORWARD -i eth1 -d 172.26.3.0/24 -o eth2 -j ACCEPT
iptables -t filter -A FORWARD -i eth1 -d 172.26.3.0/24 -o eth3 -j ACCEPT
iptables -t filter -A FORWARD -i eth1 -j REJECT
```

Figura 22 - Configuración R5

```

ifconfig eth2 172.26.2.193/28 up
ifconfig eth0 172.26.2.129/26 up
ifconfig eth1 172.26.2.209/30 up
ifconfig eth3 172.26.0.3/23 up
ip route add default via 172.26.0.2 dev eth3
ip route add 172.26.4.0/25 via 172.26.0.1 dev eth3
ip route add 172.26.2.0/25 via 172.26.2.210 dev eth1
ip route add 172.26.3.0/24 via 172.26.0.4 dev eth3

```

Figura 23 - Configuración R6

Ejercicio 9

Enunciado: Configure la red de manera de poder enviar el mensaje “Hola Data Center” desde PC-Casa hasta Server 1, utilizando Netcat. Tenga en cuenta configurar el reenvío de paquetes en Router 2. Considere que el puerto que está abierto en el Router 2 es el 80, mientras que el servicio en el Server 1 está corriendo en el puerto 8080. Luego, replique la conexión desde la Pc1.

Indique para ambos casos, ¿qué dirección IP y qué puertos se deben utilizar?

Para poder lograr esta comunicación entre la casa jefe y el server 1 se tuvo que tener en cuenta primero el router por donde atraviesa el mensaje antes de llegar al receptor que sería en el router 2 (R2), el comando especificado en la figura 24 (←) indica que antes de empezar con el enrutamiento a todo paquete que atravesase la interfaz se cambia su dirección destino por 172.26.4.4 con el puerto 8080.

```

ifconfig eth1 172.26.4.1/25 up
ifconfig eth0 201.0.2.2/24 up
ip route add default via 201.0.2.1 dev eth0
ip route add 172.26.0.0/22 via 172.26.4.3 dev eth1
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
iptables -t filter -A FORWARD -s 172.26.3.0/24 -j ACCEPT
iptables -t filter -A FORWARD -s 172.26.4.0/25 -j ACCEPT
iptables -t filter -A FORWARD -s 172.26.2.0/24 -j ACCEPT
iptables -t nat -A PREROUTING -p tcp --dport 80 -j DNAT --to 172.26.4.4:8080
iptables -t filter -A FORWARD -o eth0 -j REJECT

```

Figura 24 - Configuración R2

Luego para enviar el mensaje sugerido por la consigna desde la casa jefe hasta el server 1 primero se colocó el comando `nc -4 -l 8080` en la terminal del server donde se pone a la espera de un mensaje por el puerto 8080 (Figura 25). Luego una vez realizado el anterior paso se continúa abriendo la terminal de la casa jefe colocando el comando `nc -4 201.0.2.2 80` donde en este comando se busca la dirección pública del router (Figura 26), una vez realizado esto se pasa a mandar el mensaje “Hola data center” y observar en la terminal del servidor que halla llegado correctamente.



Figura 25 - Terminal Server 1



Figura 26 - Terminal Casa jefe

Para mandar un mensaje desde la PC1 hasta el server 1 se hace de la misma manera en el server 1 (figura 27) pero en la consola de PC1 se la cambia la dirección ip ya que al tratarse de una red privada del Parque Industrial se le asigna la dirección ip correspondiente al server 1, siendo así la comunicación se continúa mandando el mensaje “*Hola data center*” (Figura 28).

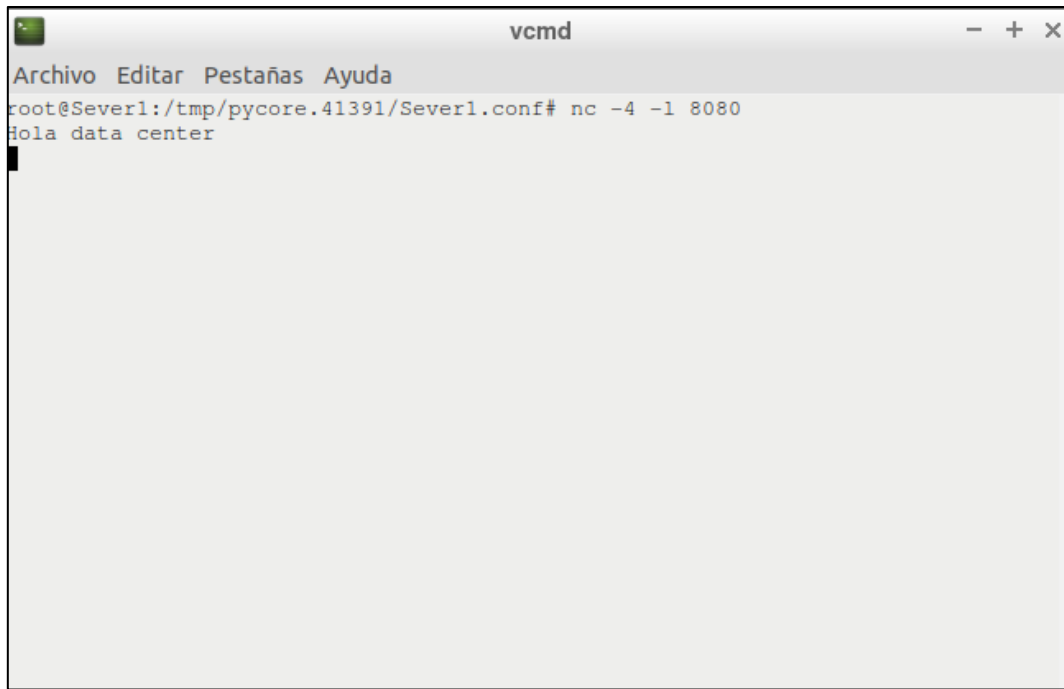


Figura 27 - Terminal Server 1



Figura 28 - Terminal Pc1

Para los ejercicios 5,6,7 y 9 los comandos se encuentran detallados en la página 26.

Ejercicio 10

Enunciado: Realice un Ping desde la PC4 a la PC6. Analice las diferencias en el funcionamiento entre el dispositivo de Hub y el Switch. Justificar con la captura de las pantallas de Wireshark correspondientes.

Las diferencias que se pueden observar a la hora de transmitir los paquetes, son de qué manera lo hacen, como bien se observan en la figura 29 cuando se habla de un dispositivo HUB es visto como un repetidor multipuerto, donde regenera los datos y transmite a todos los puertos. A su vez, trabaja en la capa física (en un bajo nivel) para regenerar la señal de la red y reenviarlos a demás segmentos.

Mientras que por otro lado tenemos el Switch que como se puede observar en la figura 30 en un comienzo envía los datos al broadcast y luego cuando obtiene una dirección física (Mac) de la Pc la preserva internamente en una tabla para una futura comunicación de datos. Este dispositivo divide una red en varios canales aislados, cada canal tiene su propia capacidad y no tiene por qué ser compartida con otros canales.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000000	fe80::4c7f:9249:fe0c::1	ff02::1	ICMPv6	70	Router Solicitation from 4c7f:9249:fe0c::1
2	13.22111590	fe80::b8ac:35ff:fe5f::f2	ff02::1	MDNS	180	Standard query 0x0000 PTR nfs.tcp.local, "QM" question PTR ftp.tcp.local, "QM" question PTR
3	20.23115688	fe80::4c7f:9249:fe0c::1	ff02::1	MDNS	180	Standard query 0x0000 PTR nfs.tcp.local, "QM" question PTR ftp.tcp.local, "QM" question PTR
4	24.575512238	fe80::b8ac:35ff:fe5f::f2	ff02::1	ICMPv6	70	Router Solicitation from 06:56:45:f9:44:9d
5	38.264914324	00:00:00:aa:00:14	Broadcast	ARP	42	Who has 172.26.3.161? Tell 172.26.3.162
6	38.264914324	00:00:00:aa:00:12	00:00:00:aa:00:14	ARP	42	172.26.3.161 is at 00:00:00:aa:00:12
7	38.264914324	172.26.3.162	172.26.3.2	ICMP	98	Echo (ping) request id=0x0027, seq=1/256, ttl=64 (reply in 8)
8	38.264914324	172.26.3.2	172.26.3.162	ICMP	98	Echo (ping) reply id=0x0027, seq=1/256, ttl=63 (request in 7)
9	43.520144853	00:00:00:aa:00:12	00:00:00:aa:00:14	ARP	42	Who has 172.26.3.162? Tell 172.26.3.161
10	43.520144853	00:00:00:aa:00:14	00:00:00:aa:00:12	ARP	42	172.26.3.162 is at 00:00:00:aa:00:14

Figura 29 – HUB

No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000000	fe80::2c18:10ff:fe4f::f2	ff02::1	MDNS	180	Standard query 0x0000 PTR nfs.tcp.local, "QM" question PTR ftp.tcp.local, "QM" question PTR
2	2.209366054	fe80::2c18:10ff:fe4f::f2	ff02::1	ICMPv6	70	Router Solicitation from 42:db:ef:42:06:c2
3	7.197677124	fe80::40db:efff:fe4f::f2	ff02::1	MDNS	180	Standard query 0x0000 PTR nfs.tcp.local, "QM" question PTR ftp.tcp.local, "QM" question PTR
4	14.488248496	fe80::40db:efff:fe4f::f2	ff02::1	ICMPv6	70	Router Solicitation from 42:db:ef:42:06:c2
5	24.08105519	00:00:00:aa:00:15	Broadcast	ARP	42	Who has 172.26.3.2? Tell 172.26.3.1
6	24.08105519	00:00:00:aa:00:17	00:00:00:aa:00:15	ARP	42	172.26.3.2 is at 00:00:00:aa:00:17
7	24.08105519	172.26.3.162	172.26.3.2	ICMP	98	Echo (ping) request id=0x0027, seq=1/256, ttl=63 (reply in 8)
8	24.08105519	172.26.3.2	172.26.3.162	ICMP	98	Echo (ping) reply id=0x0027, seq=1/256, ttl=64 (request in 7)
9	29.337086677	00:00:00:aa:00:17	00:00:00:aa:00:15	ARP	42	Who has 172.26.3.1? Tell 172.26.3.2
10	29.337086677	00:00:00:aa:00:15	00:00:00:aa:00:17	ARP	42	172.26.3.1 is at 00:00:00:aa:00:15

Figura 30 – Switch

Ejercicio 11

Enunciado: Realice un ping desde la PC4 a una dirección que pertenezca a la misma red pero que no esté conectada. Luego realice un ping desde la PC4 a una dirección que pertenezca a la red Datacenter pero que no esté conectada. Analice en ambos casos los paquetes que se generan (mensajes ICMP y ARP). Utilice la opción -c 1 en ambos pings.

En la primera figura (Figura 31) se puede llegar a observar cómo desde la Pc 4 intenta mandar un paquete a una dirección que no está conectada e intentar conocer la MAC

a través del protocolo ARP pero al no obtener ninguna respuesta, ya que la dirección ip no está conectada en la red, termina intentándolo dos veces más sin respuestas.

En figura siguiente (Figura 32) se logra observar que se puede enviar un paquete a una dirección ip (172.26.4.6) de la red Datacenter pero como esta no está conectada no retorna nada ya que al no existir no puede retornar un echo reply dando lugar a un error ICMP de “Destination Unreachable (Host unreachable)”.

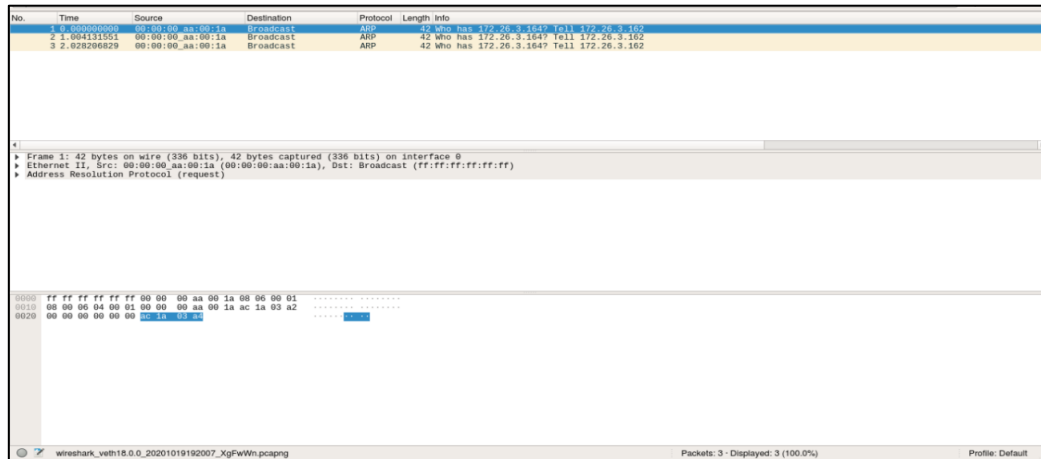


Figura 31 – Ping desde Pc4 a la misma red

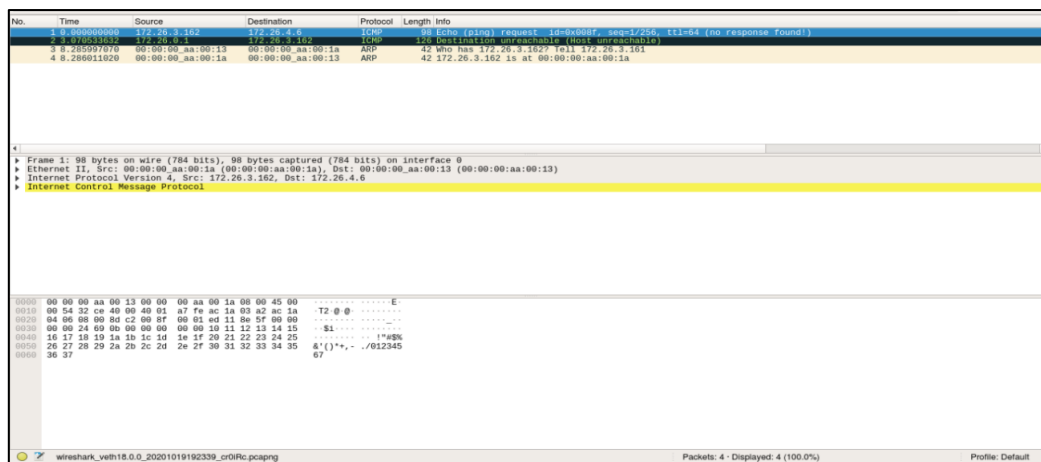


Figura 32- Ping desde Pc4 a la red Datacenter

Ejercicio 12

Enunciado: Realizar pruebas utilizando el comando ping entre los siguientes puntos y mediante la utilización de Wireshark, analice el camino seguido por los paquetes generados, adjuntando al informe las capturas de pantalla correspondientes:

- Desde un equipo conectado a la Fábrica A hasta la dirección **privada** del R2
- Desde un equipo conectado a la Fábrica A hasta la dirección **pública** del R2
- Desde Pc4 a la interfaz pública del R8

En el ejercicio **A** podemos observar la Figura 33 donde se hace un ping de la PC1 de la Fabrica A hacia la dirección privada de R2 lo que se pudo analizar es que cuando el ping se encuentra en el R6 el mismo intenta obtener la dirección de R2, una vez encontrada devuelve un *“Echo request”* (Como se observa en la figura 33 línea 6) proveniente de la PC1 con destino a la PC2. Si se observa detalladamente el paquete ha tenido dos saltos entre router para poder llegar a su destino (se puede apreciar con el ttl disminuido en 2 unidades). En el retorno de los datos se envía un *“echo reply”* (Como se observa en la figura 33 línea 7) y el tiempo de vida del mismo es de 64 ya que no ha realizado ningún salto (ttl).

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	00:00:00 aa:00:0b	Broadcast	ARP	42	Who has 172.26.2.129? Tell 172.26.2.130
2	0.000038352	00:00:00 aa:00:0d	00:00:00 aa:00:0b	ARP	42	172.26.2.129 is at 00:00:00 aa:00:0d
3	0.000049907	172.26.2.130	172.26.4.1	ICMP	98	Echo (ping) request id=0x0027, seq=1/256, ttl=64 (reply in 4)
4	0.000134665	172.26.4.1	172.26.2.130	ICMP	98	Echo (ping) reply id=0x0027, seq=1/256, ttl=62 (request in 4)
5	5.106293561	00:00:00 aa:00:0d	00:00:00 aa:00:0b	ARP	42	Who has 172.26.2.130? Tell 172.26.2.129
6	5.106311605	00:00:00 aa:00:0b	00:00:00 aa:00:0d	ARP	42	172.26.2.130 is at 00:00:00 aa:00:0b

Figura 33 - Captura de Wireshark de R6

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	00:00:00:aa:00:05	Broadcast	ARP	42	Who has 172.26.4.1? Tell 172.26.4.3
2	0.000015930	00:00:00:aa:00:02	00:00:00:aa:00:05	ARP	42	172.26.4.1 is at 00:00:00:aa:00:02
3	0.000019460	172.26.4.139	172.26.4.1	ICMP	98	Echo (ping) request id=0x002 seq=1/256, ttl=62 (reply in 4)
4	0.000040695	172.26.4.1	172.26.4.139	ICMP	98	Echo (ping) reply id=0x0027, seq=1/256, ttl=64 (request in 3)
5	0.000171830	00:00:00:aa:00:02	00:00:00:aa:00:05	ARP	42	Who has 172.26.4.3? Tell 172.26.4.1
6	5.106233267	00:00:00:aa:00:05	00:00:00:aa:00:02	ARP	42	172.26.4.3 is at 00:00:00:aa:00:05
7	26.609665783	fe80::8095:51ff:fe6::ff02::2	ff02::2	ICMPv6	70	Router Solicitation from 36:7e:4c:f0:5b:05

Figura 34 - Captura de Wireshark de R2

En el ejercicio **B** se analizó el comando ping desde la PC1 de la Fabrica A hacia la dirección de la IP pública del R2. En la figura 35 se observa como el ping al salir de la PC1 pregunta por el método de direccionamiento más cercano (En este caso R6). Una vez que identifica el camino devuelve un “*echo request*” logrando así el mismo camino que el ping desde la PC1 a la IP privada del R2. La diferencia que se notó es en la Figura 36 es al no haber flujo de datos en la interfaz de la ip pública (eth0) la misma no presenta trafico de datos.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	080800450b1f1c2c	0a02112	ICMPv6	70	Router Solicitation from 26:08:02:17:2c:11:02
2	0.000016531	0a02:11:02:17:2c:11:02	080800450b1f1c2c	ICMPv6	102	Router Advertisement
3	0.026614348	172.26.2.130	201.0.2.2	ICMP	90	Echo (ping) request id=0x0032, seq=1256, ttl=64 (reply in 4)
4	0.026745375	201.0.2.2	172.26.2.130	ICMP	90	Echo (ping) reply id=0x0032, seq=1256, ttl=62 (request in 3)
5	0.041414383	00:00:00:aa:00:00	00:00:00:aa:00:00	ARP	42	Who has 172.26.2.129? Tell 172.26.2.129
6	0.041605511	00:00:00:aa:00:00	00:00:00:aa:00:00	ARP	42	Who has 172.26.2.129? Tell 172.26.2.130
7	0.134164937	00:00:00:aa:00:00	00:00:00:aa:00:00	ARP	42	172.26.2.130 is at 00:00:00:aa:00:00
8	0.134178463	00:00:00:aa:00:00	00:00:00:aa:00:00	ARP	42	172.26.2.129 is at 00:00:00:aa:00:00

Figura 35 - Captura de Wireshark de R2

No.	Time	Source	Destination	Protocol	Length	Info

Figura 36 - Captura de Wireshark de R6

En el ejercicio **C** se realizó un ping desde la PC4 a la IP pública del R8. En la figura 37 se puede observar que, al mandar el dicho ping, este no logra encontrar destino. Esto se debe al filtrado hecho en el ejercicio 6, el cual a través del comando *iptables -t filter -A FORWARD -j REJECT* dejan así a las PC's conectadas al HUB con el poder de conectarse solo a los equipos de la Fabrica B y Datacenter.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	00:00:00_00:00:00	00:00:00_00:00:00	ARP	42	who has 172.26.3.161? tell 172.26.3.162
2	0.00001550	00:00:00_00:00:00	00:00:00_00:00:00	ARP	42	172.26.3.161 is at 00:00:00:aa:00:11
3	0.00003470	172.26.3.162	201-0-1-2.dial-up.t	ICMP	98	Echo (ping) request id=0x0027, seq=1/256, ttl=64 (no response found!)
4	0.00004890	172.26.3.161	172.26.3.162	ICMP	126	destination unreachable (Port unreachable)
5	1.01741920	172.26.3.162	201-0-1-2.dial-up.t	ICMP	98	Echo (ping) request id=0x0027, seq=2/256, ttl=64 (no response found!)
6	1.01748428	172.26.3.161	172.26.3.162	ICMP	126	Destination unreachable (Port unreachable)
7	2.040920253	172.26.3.162	201-0-1-2.dial-up.t	ICMP	98	Echo (ping) request id=0x0027, seq=3/256, ttl=64 (no response found!)
8	2.041092021	172.26.3.161	172.26.3.162	ICMP	126	destination unreachable (Port unreachable)
9	5.145599995	00:00:00_00:00:00	00:00:00_00:00:00	ARP	42	who has 172.26.3.162? tell 172.26.3.161
10	5.145614954	00:00:00_00:00:00	00:00:00_00:00:00	ARP	42	172.26.3.162 is at 00:00:00:aa:00:18

Figura 37 - Captura de Wireshark de PC4

Ejercicio 13

Enunciado: Modifique las tablas de ruteo de manera que se generen paquetes ICMP con los siguientes códigos de error:

- Destination network unreachable.
- Time Exceeded.

Importante: No se podrán utilizar las opciones del comando ping para generar los errores.

En el ejercicio **13-a**, se logró generar el error Destination network unreachable, eliminando el ip route del R7 hacia el Datacenter (Figura 38). Una vez eliminado se procedió a desarrollar un ping desde la PC3 de la Fabrica A al Server 1 del datacenter (Figura 39). Este al no encontrar la ruta hacia esa dirección establece error de conexión.

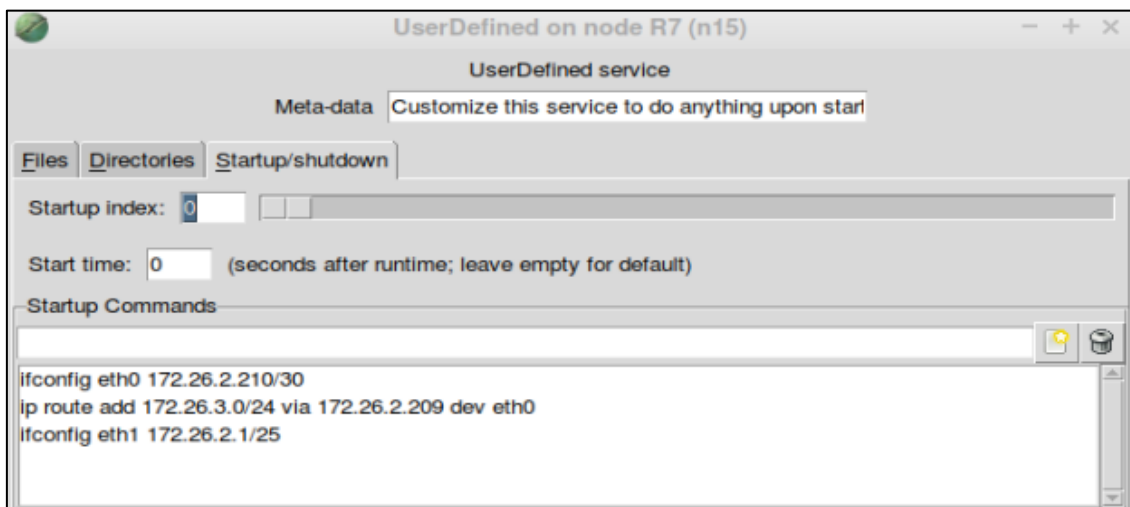
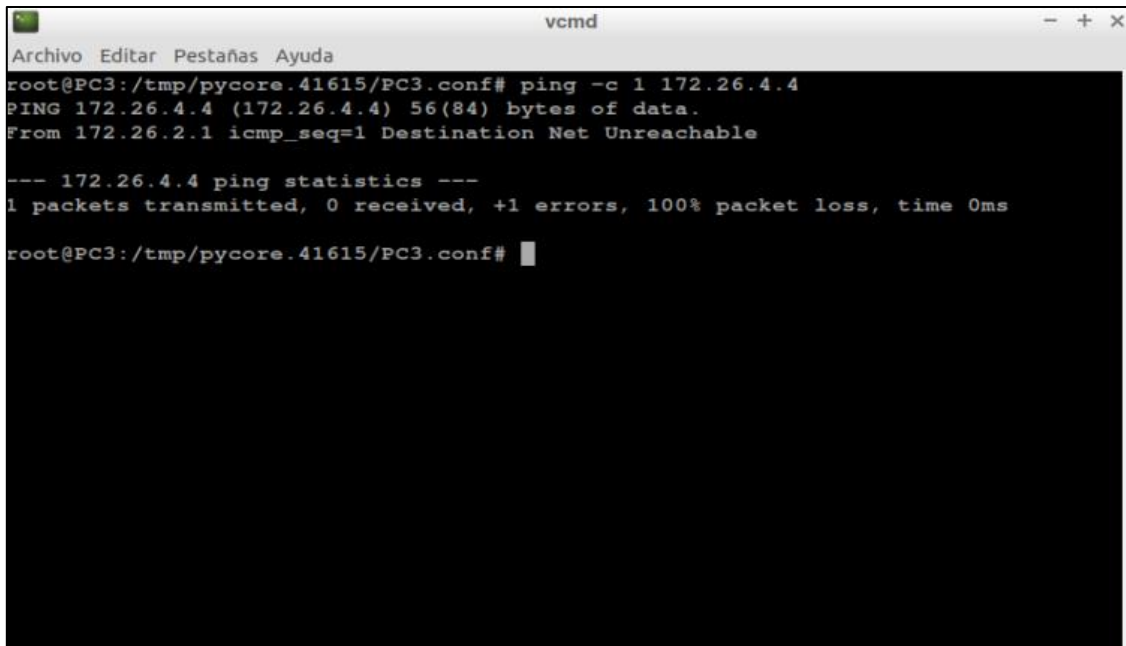


Figura 38 - Configuración de R7



```

vcmd
Archivo Editar Pestañas Ayuda
root@PC3:/tmp/pycore.41615/PC3.conf# ping -c 1 172.26.4.4
PING 172.26.4.4 (172.26.4.4) 56(84) bytes of data.
From 172.26.2.1 icmp_seq=1 Destination Net Unreachable

--- 172.26.4.4 ping statistics ---
1 packets transmitted, 0 received, +1 errors, 100% packet loss, time 0ms

root@PC3:/tmp/pycore.41615/PC3.conf#

```

Figura 39 - Resultado de comando ping a Server1

En el ejercicio **13-b**, se logró el error *Time to live Exceeded* configurando los router R3 y R4 para que se genere un bucle del cual el ping no pueda llegar a destino y así se termine su tiempo de vida. El bucle se generó realizando un *ip route add default* que tenga como vía la dirección de IP del R4 (Figura 40). Luego se realizó el mismo procedimiento con el R4, configurándolo para que su vía por defecto se la dirección de IP del R3 (Figura 41). El resultado de este bucle se puede observar en la figura 42, logrando que este pierda su tiempo de vida y no llegue a destino.

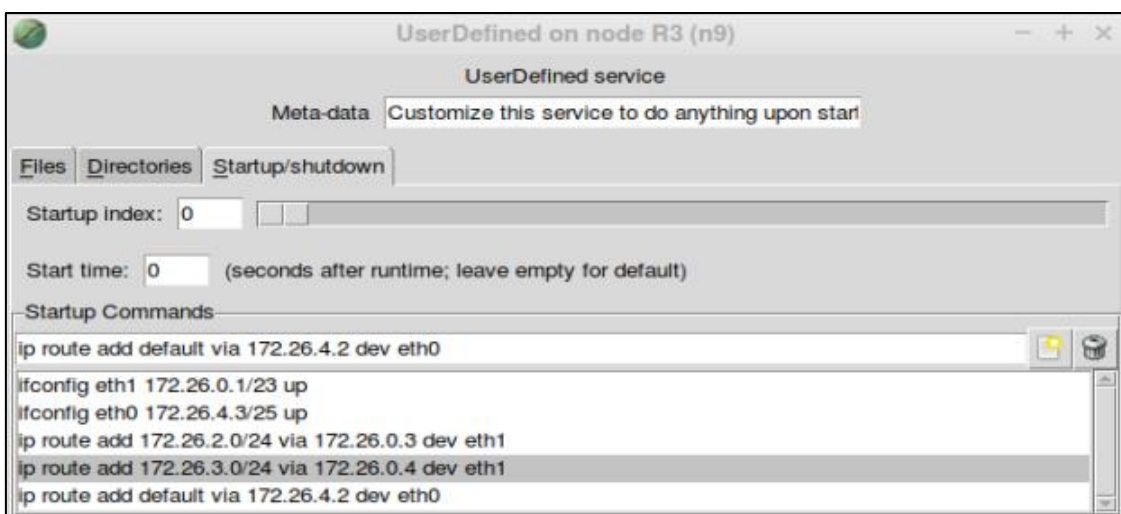


Figura 40 - Configuración de R3

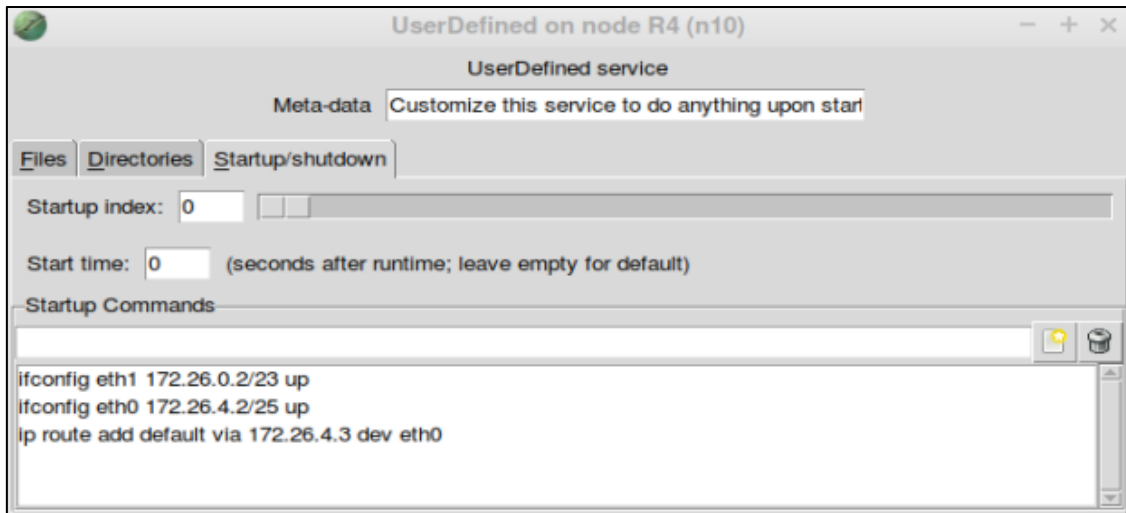


Figura 41 - Configuración de R4

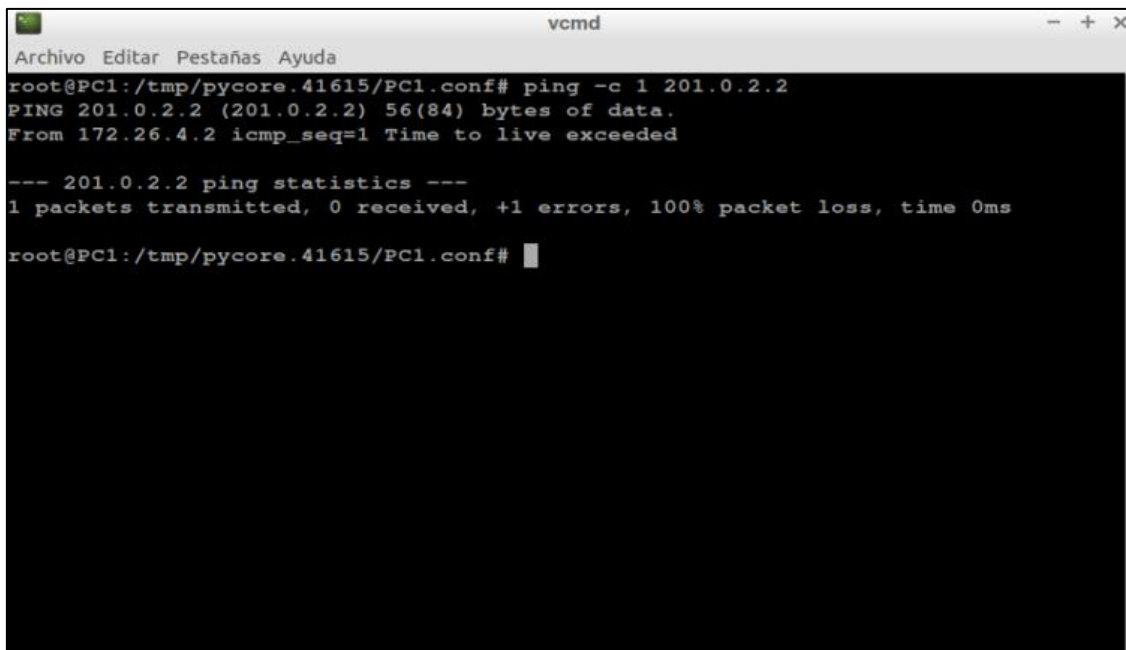


Figura 42 - Resultado de comando ping a red publica

Ejercicio 14

Enunciado: Realice los siguientes traceroute y explique lo observado:

- Desde la Pc6 a la ip pública de R8.
- Desde la Pc4 a la ip pública de R8.
- Desde la Pc1 a la ip del Server 1.

Indique los saltos de routers generados para cada punto.

Para los casos en que interviene el Router 2, describa apoyándose en capturas de Wireshark, los paquetes y protocolos que intervienen en ambas interfaces y que implican estos.

El comando *traceroute* le permite determinar la ruta que toma un paquete para llegar a un destino desde una fuente determinada al devolver la secuencia de saltos que ha atravesado el paquete.

Operación general

Si se ejecuta el comando *traceroute ip-address* en un dispositivo de origen (como un host o un enrutador que actúa como host), envía paquetes IP hacia el destino con valores de tiempo de vida (TTL) que aumentan hasta el máximo especificado número de saltos. Este es 30 por defecto. Por lo general, cada enrutador en la ruta hacia el destino disminuye el campo TTL en una unidad mientras reenvía estos paquetes. Cuando un enrutador en el medio de la ruta encuentra un paquete con TTL = 1, responde con un mensaje de "tiempo excedido" del Protocolo de mensajes de control de Internet (ICMP) a la fuente. Este mensaje le permite a la fuente saber que el paquete atraviesa ese enrutador en particular como un salto.

En el ejercicio **14-a**, se analizó a través del comando *Traceroute*, el camino que realizaría el ping desde la PC4 hacia la IP pública del R8 (Figura 43). Una vez que se ejecutó el comando por medio del wireshark (Figura 44) se observó como este mandaba ping y no llegaban a destino, esto se origina ya que en el ejercicio 6, se logró poner en funcionamiento un filtrado el cual no permite que las PC's conectadas al HUB logren comunicarse con internet.

```

vcmid
Archivo Editar Pestañas Ayuda
root@PC4:/tmp/pycore.41615/PC4.conf# traceroute 201.0.1.2
traceroute to 201.0.1.2 (201.0.1.2), 30 hops max, 60 byte packets
 1 172.26.3.161 (172.26.3.161) 0.037 ms 0.005 ms 0.004 ms
 2 172.26.3.161 (172.26.3.161) 0.006 ms 0.005 ms 0.004 ms
root@PC4:/tmp/pycore.41615/PC4.conf#

```

Figura 43 - Resultado de traceroute PC4

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	172.26.3.162	201.0.1.2.dial-up.t	ICMP	74	43848 - traceroute(33434) len=32
2	0.000017770	172.26.3.161	172.26.3.162	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
3	0.000032960	172.26.3.162	201.0.1.2.dial-up.t	UDP	74	38978 - ntrace(33435) len=32
4	0.000034510	172.26.3.161	172.26.3.162	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
5	0.000042610	172.26.3.162	201.0.1.2.dial-up.t	UDP	74	33966 - 33436 len=32
6	0.000044750	172.26.3.161	172.26.3.162	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
7	0.000052370	172.26.3.162	201.0.1.2.dial-up.t	UDP	74	43310 - 33437 len=32
8	0.000052750	172.26.3.161	172.26.3.162	ICMP	102	Destination unreachable (Port unreachable)
9	0.000064110	172.26.3.162	201.0.1.2.dial-up.t	UDP	74	41323 - 33438 len=32
10	0.000066330	172.26.3.161	172.26.3.162	ICMP	102	Destination unreachable (Port unreachable)
11	0.000072700	172.26.3.162	201.0.1.2.dial-up.t	UDP	74	80484 - 33439 len=32
12	0.000075750	172.26.3.161	172.26.3.162	ICMP	102	Destination unreachable (Port unreachable)
13	0.000083340	172.26.3.162	201.0.1.2.dial-up.t	UDP	74	48814 - 33440 len=32
14	0.000090720	172.26.3.162	201.0.1.2.dial-up.t	UDP	74	41842 - 33441 len=32
15	0.000097330	172.26.3.162	201.0.1.2.dial-up.t	UDP	74	34684 - 33442 len=32
16	0.000104370	172.26.3.162	201.0.1.2.dial-up.t	UDP	74	32852 - 33443 len=32
17	0.000110960	172.26.3.162	201.0.1.2.dial-up.t	UDP	74	49336 - 33444 len=32
18	0.000117190	172.26.3.162	201.0.1.2.dial-up.t	UDP	74	47414 - 33445 len=32

Figura 44 - Captura de Wireshark PC4

En el ejercicio **14-b**, Se realizó el mismo procedimiento que en el ejercicio anterior, pero esta vez ejecutando los comandos desde la PC6 (Figura 45), a diferencia del análisis anterior en este podemos observar como el comando traceroute comienza mandando ping's con ttl 1 (y luego incrementando de a 1 cuando el anterior haya excedido su tiempo de vida) repetitivamente logrando así los dichos saltos hasta lograr llegar al destino (Figura 46), esto se debe a que la PC6 no tiene ningún tipo de filtrado que le impida comunicarse con la dirección IP del router 8 (R8).

```

vcmid
Archivo Editar Pestañas Ayuda
root@PC6:/tmp/pycore.41615/PC6.conf# traceroute 201.0.1.2
traceroute to 201.0.1.2 (201.0.1.2), 30 hops max, 60 byte packets
 1 172.26.3.1 (172.26.3.1) 0.061 ms 0.004 ms 0.004 ms
 2 172.26.4.2 (172.26.4.2) 0.074 ms 0.011 ms 0.010 ms
 3 172.26.4.1 (172.26.4.1) 0.018 ms 0.011 ms 0.011 ms
 4 201.0.2.1 (201.0.2.1) 0.033 ms 0.014 ms 0.014 ms
 5 201.0.1.2 (201.0.1.2) 0.037 ms 0.018 ms 0.018 ms
root@PC6:/tmp/pycore.41615/PC6.conf#

```

Figura 45 - Resultado de traceroute PC6

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	172.26.3.2	201-0-1-2.dial-up.t...	UDP	74	42069 - traceroute(33434) Lens32
2	0.000024870	172.26.3.1	172.26.3.2	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
3	0.000035008	172.26.3.2	201-0-1-2.dial-up.t...	UDP	74	36482 - ntrace(33435) Lens32
4	0.000038748	172.26.3.1	172.26.3.2	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
5	0.000045368	172.26.3.2	201-0-1-2.dial-up.t...	UDP	74	47926 - 33436 Lens32
6	0.000048486	172.26.3.1	172.26.3.2	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
7	0.000054267	172.26.3.2	201-0-1-2.dial-up.t...	UDP	74	57729 - 33437 Lens32
8	0.000087676	172.26.4.2	172.26.3.2	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
9	0.000094885	172.26.3.2	201-0-1-2.dial-up.t...	UDP	74	45407 - 33438 Lens32
10	0.000104225	172.26.4.2	172.26.3.2	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
11	0.000111255	172.26.3.2	201-0-1-2.dial-up.t...	UDP	74	37344 - 33439 Lens32
12	0.000120324	172.26.4.2	172.26.3.2	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
13	0.000126524	172.26.3.2	201-0-1-2.dial-up.t...	UDP	74	41071 - 33440 Lens32
14	0.000144993	172.26.4.1	172.26.3.2	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
15	0.000151353	172.26.3.2	201-0-1-2.dial-up.t...	UDP	74	42088 - 33441 Lens32
16	0.000157382	172.26.4.1	172.26.3.2	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
17	0.000168352	172.26.3.2	201-0-1-2.dial-up.t...	UDP	74	36169 - 33442 Lens32
18	0.000178671	172.26.4.1	172.26.3.2	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
19	0.000184761	172.26.3.2	201-0-1-2.dial-up.t...	UDP	74	53422 - 33443 Lens32
20	0.000208080	201-0-2-1.dsl.teles...	172.26.3.2	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
21	0.000215479	172.26.3.2	201-0-1-2.dial-up.t...	UDP	74	37567 - 33444 Lens32
22	0.000226138	201-0-2-1.dsl.teles...	172.26.3.2	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
23	0.000236588	172.26.3.2	201-0-1-2.dial-up.t...	UDP	74	33408 - 33445 Lens32
24	0.000249927	201-0-2-1.dsl.teles...	172.26.3.2	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
25	0.000259307	172.26.3.2	201-0-1-2.dial-up.t...	UDP	74	43091 - 33446 Lens32
26	0.000261486	201-0-1-2.dial-up.t...	172.26.3.2	ICMP	102	Destination unreachable (Port unreachable)
27	0.000268895	172.26.3.2	201-0-1-2.dial-up.t...	UDP	74	49378 - 33447 Lens32
28	0.000280415	201-0-1-2.dial-up.t...	172.26.3.2	ICMP	102	Destination unreachable (Port unreachable)
29	0.000311604	172.26.3.2	201-0-1-2.dial-up.t...	UDP	74	43977 - 33448 Lens32
30	0.000328593	201-0-1-2.dial-up.t...	172.26.3.2	ICMP	102	Destination unreachable (Port unreachable)
31	0.000335093	172.26.3.2	201-0-1-2.dial-up.t...	UDP	74	37023 - 33449 Lens32
32	0.000350622	201-0-1-2.dial-up.t...	172.26.3.2	ICMP	102	Destination unreachable (Port unreachable)
33	61.792132679	core.local	ip6-allrouters	ICMPv6	70	Router Solicitation from 3210f:56:d1:98:5d
34	87.176227066	core.local	ff02::fb	MDNS	180	Standard query 0x0000 PTR _nfs._tcp.local, "QM" question PTR _ftp._tcp.local, "QM" question PTR
35	91.302902998	core.local	ff02::fb	MDNS	180	Standard query 0x0000 PTR _nfs._tcp.local, "QM" question PTR _ftp._tcp.local, "QM" question PTR

Figura 46 - Captura Wireshark PC6

En el ejercicio 14-c, se realizó el análisis del traceroute de un ping enviado desde la PC1 al Server 1 (Figura 47), logrando identificar que primero debe pasar por el R6 el cual tiene el camino hacia la red del Datacenter, logrando así desarrollar una correcta comunicación con su IP de destino.

```

Archivo Editar Pestañas Ayuda
root@PC1:/tmp/pycore.39665/PC1.conf# traceroute 172.26.4.4
traceroute to 172.26.4.4 (172.26.4.4), 30 hops max, 60 byte packets
 1 172.26.2.129 (172.26.2.129) 0.060 ms 0.005 ms 0.005 ms
 2 172.26.0.1 (172.26.0.1) 0.038 ms 0.009 ms 0.008 ms
 3 172.26.4.4 (172.26.4.4) 0.037 ms 0.011 ms 0.010 ms
root@PC1:/tmp/pycore.39665/PC1.conf#

```

Figura 47 - Resultado de traceroute PC1

Comandos

En esta sección se encuentran todos los comandos utilizados a lo largo del informe.

- ***ifconfig***: El comando *ifconfig* se utilizó para consultar o cambiar la configuración de una interfaz de red. Como se logra observar en la figura 48 esta muestra la asignación de la dirección ip *172.26.2.131/26* por un canal *eth0* con el comando *ifconfig*. Este comando fue usado en el ejercicio 3.
- ***ip route add***: Este comando fue utilizado para configurar la tabla de ruteo en cada equipo, luego de analizar las rutas en algunos casos precisamente las que son dirigidas a internet se logró minimizar con el comando *ip route add default via <dir-ip-dest> dev <output-interface>* el cual asigna una vía por defecto hacia la red ISP como bien se muestra en la figura 48. Este comando fue usado en el ejercicio 4 y 8.

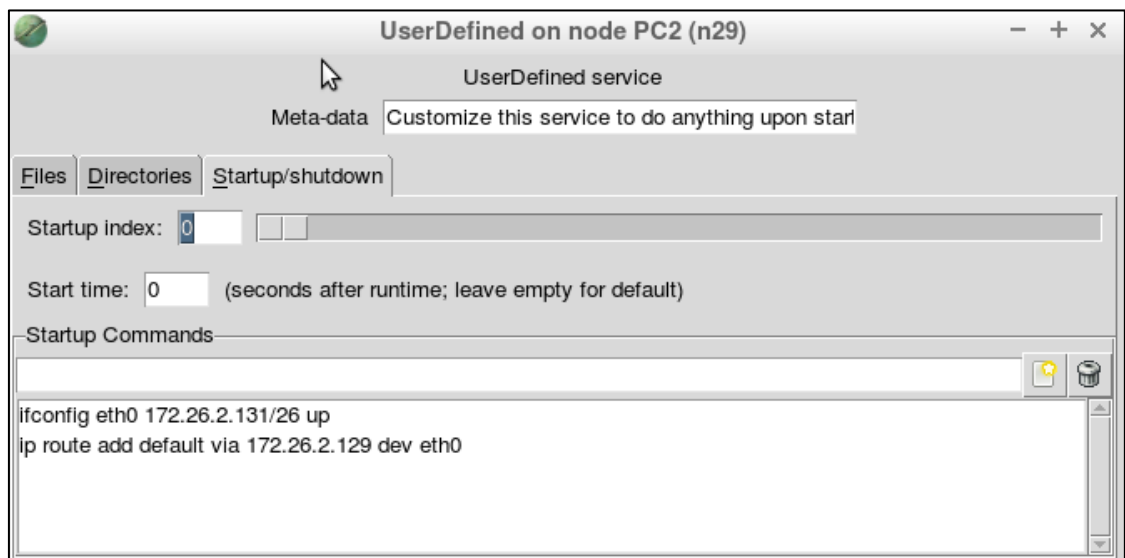


Figura 48 - Ejemplo de *ifconfig* e *ip route* en PC2

- ***Ping <dirección ip destino>***: Este comando se utiliza más bien en la consola y comprueba que un paquete llegue a destino mandando así un ping de 64 bytes.
- ***Ping -C <cantidad paquetes> <dirección ip destino>***: Este comando es similar al comando anterior *Ping* donde también es ejecutado por consola y comprueba que un paquete llegue a destino.
- ***iptables [-t <tabla>] <comando> [<cadena>] [<condición>][<acción>]***: El comando *ip tables* fue utilizado para configurar las reglas de filtrado de netfilter.

- *iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE*

-t nat: Tabla para la traducción de direcciones de red.

-A: Comando que añade una regla.

POSTROUTING: Cadena que denota a los paquetes que salen de la máquina.

-o: Interfaz de salida.

-j: Ejecuta la acción siguiente.

-MASQUERADE: Permite realizar enmascaramiento IP, para realizar la conversión de ip privada a publica.

- *iptables -t filter -A FORWARD -s 172.26.3.0/24 -j ACCEPT*

-t filter: Tabla encargada del filtrado de paquetes.

FORWARD: Se aplican a los paquetes que han llegado a la máquina, pero van destinados a otra.

-s: Indica que el próximo campo será la red de origen del paquete.

ACCEPT: Condición que acepta los paquetes.

- *iptables -t filter -A FORWARD -o eth0 -j REJECT*

REJECT: Elimina los paquetes que no cumplen la condición.

- *iptables -t filter -A FORWARD -i eth1 -d 172.26.4.0/25 -o eth0 -j ACCEPT*

-i: Interfaz de entrada.

-d: Dirección destino.

- *iptables -t nat -A PREROUTING -p tcp -dport 80 -j DNAT --to*

PREROUTING: Se aplican a los paquetes que han llegado a la máquina, pero van destinados a otra, antes del enrutamiento.

-p: Protocolo.

-dport: Puerto destino.

-DNAT: Utilizado cuando la red de destino puede variar.

--to: Antecede a la dirección de origen por la cual se intercambiará.

Conclusión

En el presente informe, se realizó una topología de redes presentado por la catedra asignando mediante VLSM las diferentes direcciones IP a cada una de las redes.

Para poder lograr esto, no solo se aprendió a utilizar los comandos y el entorno del emulador Core, sino que además se pudo lograr entender como utilizar consolas virtuales para diferentes tipos de tareas.

Luego, se hicieron configuraciones de routers para poder así , realizar un test de *ping* y *traceroute* sobre ciertos Host requeridos, analizando los datos enviados y recibidos mediante herramientas de software como Wireshark.

Gracias a esto, se ha aprendido a interpretar la información que se transmite entre redes por distintos tipos de interfaces permitiéndonos comenzar a relacionarnos con este tipo de tareas de comunicación.

Bibliografía

- Traceroute <https://www.cisco.com/c/en/us/support/docs/ip/ip-routed-protocols/22826-traceroute.html>.