**Configuración y Desarrollo de Aplicaciones en Redes**

***INFORME TPE***

*TUDAI - TANDIL*

*2024*

****

***GRUPO N°: 6***

***INTEGRANTES*:** Arispe Emanuel, Hevia Joaquin, Papaleo Nicolas, Vazquez Francisco

Ayudante de Cátedra: Ing. Oscar Segura [fosegura@gmail.com](mailto:fosegura@gmail.com)

Índice

1. [Introducción](#urdqd77jyfoz): motivación, problemas a abordar,organización del documento 3.
2. [Propuesta red a configurar](#sh4lwzk7rrui): enunciado propuesta requerimientos de topología   
   a abordar 5.
3. [Diseño y configuración de la red](#j50qczmuskng): análisis y desglose de requerimientos para   
   cada red y subred del sistema 7.
4. [Parte 1](#gj3zvhvziut0): desarrollo e implementación de requerimientos en la topología 10.
5. [Punto A](#l5u3yc40cybo): armado de tablas con requerimientos de pabellones 10.
6. [Punto B](#mv2jb1xwuov6): armado de tablas con requerimientos globales pabellones 12.
7. [Punto C](#nljbcfntx6l8): representación esquema VLSM 13.
8. [Punto D](#73icwte2d4i): representación esquema VLSM subredes pabellones 14.
9. [Punto E](#xjol89jpy3tf): representación de tablas con asignación de direcciones IPs 16.
10. [Punto F](#jmi5src7yhpy): implementación de direcciones y asignaciones en simulador 18.
11. [Punto G](#amrp2ix736ea): configuración interfaces en routers y dispositivos 20.
12. [Punto H](#yz61v88yyhmk): demostración de funcionamiento local comando ping 21.
13. [Parte 2:](#p4g66o82rw0a) implementación en simulador 24.
14. [Punto A](#qs00pewnij4e): configuración de tablas de ruteo 24.
15. [Punto B](#98w0j66thclm): configuración primera condición restrictiva 29.
16. [Punto C](#h92biln31qrf):configuración segunda condición restrictiva 31.
17. [Punto D:](#m76w7c9bmzm0)configuración tercera condición restrictiva 33.
18. [Punto E:](#6zdm5r8qz01q)configuración cuarta condición restrictiva 34.
19. [Punto F:](#bhbnsqdgeghn) configuración quinta condición restrictiva 35.
20. [Punto G](#97syt9hv2vfa): configuración sexta condición restrictiva 39.
21. [Conclusión](#3xtt7exd14kh) 40.

Introducción

El presente trabajo práctico especial se desarrolla en el marco de la cátedra de Configuración de Desarrollo de Redes, y tiene como objetivo fundamental aplicar los conocimientos adquiridos a lo largo del curso para diseñar, configurar y simular una red compleja. Para ello, hemos utilizado el simulador CORE, en el cual hemos realizado todas las conexiones necesarias, configurando dispositivos, routers y switches, y segmentando la red en troncales y redes privadas externas a la central.

Problema a abordar

El problema principal que aborda este trabajo es el diseño y la implementación de una red eficiente y funcional que conecta múltiples dispositivos y redes de manera segura y óptima. Esto incluye la correcta configuración de tablas de ruteo, la distribución adecuada de direcciones IP utilizando la técnica de VLSM (Variable Length Subnet Masking), y la implementación de medidas de seguridad para el acceso a recursos internos desde redes externas. Además, se requiere realizar diagnósticos y pruebas de funcionamiento de la red mediante herramientas como ping, traceroute y Wireshark.

Organización del documento

El documento está organizado de la siguiente manera:

Introducción:

Se presenta el objetivo del trabajo y el problema a abordar mostrando los requerimientos de la estructura solicitada y la imagen de la red en cuestión a implementar.

Diseño y configuración de la red:

Se describe detalladamente el proceso de diseño de la red, incluyendo la segmentación en redes privadas, públicas, y la configuración de los dispositivos en el simulador CORE.

Asignación de direcciones IP:

Se detalla el proceso de distribución de direcciones IP utilizando la técnica de VLSM, garantizando una asignación eficiente y sin desperdicio de direcciones.

Tablas de ruteo:

Se explica la creación y configuración de las tablas de ruteo tanto en el informe como en el simulador, utilizando los comandos necesarios para asegurar la conectividad entre todas las redes.

Pruebas y diagnósticos:

Se documentan las simulaciones y pruebas realizadas para verificar el correcto funcionamiento de la red, utilizando herramientas como ping, traceroute y Wireshark, con capturas de pantalla y explicaciones correspondientes.

Acceso a internet y seguridad:

Se describen los ejercicios realizados para proporcionar acceso a internet desde la red privada, abrir puertos para servidores internos y configurar iptables para filtrado y enmascaramiento de direcciones IP.

Conclusiones:

Se presentan las conclusiones finales del trabajo, destacando los aprendizajes y resultados obtenidos.

Cada sección del documento está acompañada de capturas de pantalla y explicaciones breves en el pie de cada imagen, que ilustran el proceso y las técnicas utilizadas, proporcionando una visión clara y detallada del funcionamiento y distribución de la red configurada.

**PARTE1**

**Propuesta de red a configurar:**

En la imagen 1 se observa la topología de red especificada y propuesta para abordar una solución eficiente que en forma distribuida abarque todas las redes que en ella sean requeridas.

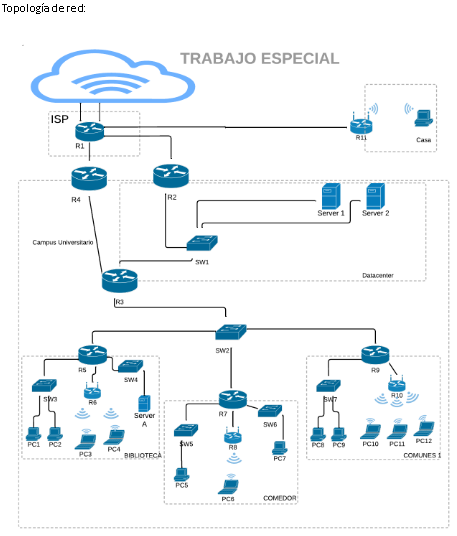


Imagen 1

La red tiene las siguientes características:

* Infraestructura ISP:
  + El ISP utiliza las bandas 201.0.0.0/24, 201.0.1.0/24 y 201.0.2.0/24 para los clientes actuales (casa y campus universitario).
* Infraestructura Casa:
  + La casa dispone de un router wifi que maneja la banda 192.168.10.0/24
* Infraestructura Campus Universitario:
  + El campus dispone de un datacenter que cuenta con los equipos frontera DMZ (R2 y R3) necesarios para dar acceso controlado y un espacio en donde se pueden alojar hasta 500 servidores en un ambiente refrigerado y libre de ruidos, para el uso de las diferentes ÁREAS del CAMPUS. Actualmente solo hay conectados 2 servidores. La salida de Internet del datacenter es a través del router R2.
  + El campus cuenta con la capacidad de albergar 80 pabellones, a los cuales se les puede asignar una única dirección IP en la red troncal para su router (Ej: una ip para el router del pabellón de Biblioteca, otro para el Comedor, etc) como frontera entre los pabellones y el resto del campus universitario. Además la red troncal cuenta con el router R4 el cual es el encargado de dar internet a los pabellones.
  + En el trabajo actual se configurarán 3 pabellones, Biblioteca, Comedor y Aulas Comunes 1 conectadas al SW2.
* Infraestructura Biblioteca:
  + En el SW3 hay actualmente 2 PC conectadas que corresponden a los equipos de secretaría y la cantidad de conexiones que soporta el Switch es 28 dispositivos.
  + Además cuenta con un router WiFi R6, el cual debe soportar dos redes (planta baja y planta alta) de 100 equipos cada una con el fin de brindar conexión para los alumnos.
  + Finalmente, se dispone de un pequeño centro de cómputo conectado a través del SW4. En el mismo se prevé tener hasta 16 servidores, pero actualmente hay solo 1 conectado (Server A).
* Infraestructura Comedor:
  + Cuenta con el SW5 el cual conecta dispositivos del área de cocina. En el mismo hay actualmente una PC conectada y la cantidad de interfaces con las que cuenta el SW es de 8 .
  + En el SW6 que soporta 45 dispositivos, se encuentra conectada actualmente la PC7 que junto al resto corresponden a los equipos de oficina.
  + Además cuenta con un router WiFi (R8), el cual debe soportar 100 equipos con el fin de brindar conexión a los alumnos almorzando.
* Infraestructura Aulas Comunes 1:
  + En este pabellón se cuenta con un router WiFi(R10), el cual provee tres redes, cada una debe soportar 100 equipos con el fin de brindar conexión a los alumnos en cada una de las tres aulas del pabellón (A1, A2, A3).
  + Finalmente, se dispone de un pequeño sector de oficinas en la cual se quiere tener la posibilidad de conectar hasta 32 computadoras conectadas al SW7 y actualmente hay dos PCs conectadas (Pc8 y PC9).

**DISEÑO Y CONFIGURACIÓN DE LA RED**

Análisis de los requerimientos en la red propuesta:

Para analizar los requerimientos de la red general del “Campus Universitario”, es necesario agrupar las redes y sus componentes de manera tal que se establezcan los bloques de direcciones acordes para cada una.

Para esto se genera un recorrido por cada una de las partes de la infraestructura y así asignar lograr las direcciones suficientes para cumplimentar los requisitos.

Para el caso de Las redes “Comedor”, “Biblioteca” y “Comunes” será necesario hacer un recorrido por las subredes que estas contienen para poder conocer los requerimientos generales.

**Data Center:**

Compuesto por 2 routers frontera, 500 servidores, base, broadcast.

504 IPs (2^9=512 direcciones - bloque necesario /23 ).

En total el conjunto de IPs relacionadas a la Red “Data Center” contempla un total de 504 IPs a asignar, los bloques que pueden ser asignados para cumplir con estos requerimientos corresponde a un solo bloque de **512** direcciones IPs(/23).

**Comunes 1:**

*Subred WIFI AULA1*:

Compuesto por 100 host,router, base, broadcast

Son necesarias 103 IPs (2^7=128 direcciones - bloque necesario /25 )

*Subred WIFI AULA2:*

Compuesto por 100 host, router,base, broadcast

Son necesarias 103 IPs (2^7=128 direcciones bloque necesario /25 )

*Subred WIFI AULA 3*:

Compuesto por 100 host,router, base, broadcast

Son necesarias 103 IPs (2^7=128 direcciones - bloque necesario /25 )

*Subred SECRETARIA COMUNES:*

Compuesto por 32 host, router, base, broadcast

Son necesarias 35 IPs (2^6=64 direcciones - bloque necesario /26 )

*Subred R9-R10WF:*

Compuesto por 2 routers t, base, broadcast

Son necesarias 4 IPs (2^2=4 direcciones bloque necesario /30 )

En total el conjunto de IPs relacionadas a la Red “Comunes 1” contempla un total de **348 IPs** a asignar, los bloques que pueden ser asignados para cumplir con estos requerimientos son: tres bloques de 128 IPs(/25), un bloque de 64 direcciones IPs(/26) y un bloque de 4 direcciones IPs(/30/.

El total de direcciones de todos los bloques es de **452** direcciones IPs(/23).

**Biblioteca:**

*Subred BIBLIOTECA WIFI-PB*:

Compuesto por 100 host, router, base, broadcast

Son necesarias 103 IPs (2^7=128 direcciones - bloque necesario /25 )

*Subred BIBLIOTECA WIFI-PA:*

Compuesto por 100 host, router, base, broadcast

Son necesarias 103 IPs (2^7=128 direcciones - bloque necesario /25 )

*Subred RECEPCIÓN BIBLIOTECA:*

Compuesto por 27 host, router, broadcast

Son necesarias 30 IPs (2^5=32 direcciones - bloque necesario /27 )

*Subred OFICINAS BIBLIOTECA:*

Compuesto por 16 host, router, base, broadcast

Son necesarias 19 IPs (2^5=32 direcciones - bloque necesario /27 )

*Subred R5-R6:*

Compuesto por 2 routers, base, broadcast

Son necesarias 4 IPs (2^2=4 direcciones - bloque necesario /30 )

En total el conjunto de IPs relacionadas a la Red “Biblioteca” contempla un total de **259** IPs.

Los bloques que pueden ser asignados para cumplir con estos requerimientos son: dos bloques de 128 IPs(/25), dos de 32 direcciones IPs(/27) y un bloque de 4 direcciones IPs(/30).

El total de direcciones de todos los bloques es de **324** direcciones IPs(/23).

**Comedor:**

*Subred WIFI COMEDOR*:

Compuesto por 100 host, router, base, broadcast

Son necesarias 103 IPs (2^7=128 direcciones - bloque necesario /25 )

*Subred RECEPCIÓN COMEDOR:*

Compuesto por 44 host , router, base, broadcast

Son necesarias 47 IPs (2^6=64 direcciones - bloque necesario /26 )

*Subred ALMACÉN COMEDOR:*

Compuesto por 7 host, router, base, broadcast

Son necesarias 10 IPs (2^4=16 direcciones - bloque necesario /28)

*Subred R7-WFR 8:*

Compuesto por 2 routers, base, broadcast

Son necesarias 4 IPs (2^2=4 direcciones - bloque necesario /30 )

En total el conjunto de IPs relacionadas a la Red “Biblioteca” contempla un total de **164** IPs.Los bloques que pueden ser asignados para cumplir con estos requerimientos son: un bloque de 128 direcciones IPs(/25), un bloque de 64 direcciones IPs(/26), un bloque de 16 direcciones IPs(/28) y un bloque de 4 IPs(/30).  
El total de direcciones de todos los bloques es de **212** direcciones IPs(/24).

**Red Troncal:**

Compuesto con 80 pabellones, router, base, broadcast

Son necesarias 83 IPs (2^7=128 direcciones - bloque necesario /25 )

En total el conjunto de IPs relacionadas a la Red “Troncal” contempla un total de 83 IPs.  
Los bloques que pueden ser asignados para cumplir con estos requerimientos son: un bloque de 128 direcciones IPs(/25).  
El total de direcciones de todos los bloques es de **128** direcciones IPs(/25).

**R4-R3:**

Compuesto por 2 routers, base, broadcast

Son necesarias 4 IPs (2^2=4 direcciones - bloque necesario /30 )

En total el conjunto de IPs relacionadas a la “R4-R3” contempla un total de 4 IPs.  
Los bloques que pueden ser asignados para cumplir con estos requerimientos son: un bloque de 4 direcciones IPs(/30).  
El total de direcciones de todos los bloques es de **4** direcciones IPs(/30).

El total de direcciones para asignar a la red general, es de **1362 IPs** , por lo que la suma de todos los bloques necesarios para poder abastecer este requerimiento es un bloque de ***2048 direcciones IP (/21).***

De esta manera, una vez tomados los requerimientos podemos proceder a plasmar los resultados en tablas que agrupan estos requerimientos y así proseguir con el siguiente paso para aproximar a un organigrama más estructurado de cómo las redes que se deben establecer sean eficientes y bien distribuidas.

**PARTE 1**

**Punto A:**

A continuación se desglosan los pabellones con sus requerimientos finales y el resto de los datos de la infraestructura del Campus Universitario representados en las siguientes tablas, que se componen de las características que identifican a cada red haciendo mención a los pertenecientes pabellones.

| **Comunes** | | | |
| --- | --- | --- | --- |
| **Nombre de la Red** | **Descripción de las IPs necesarias** | **Tamaño del bloque** | **Máscara resultante** |
| WIFI AULA 1 | 100 host + router + base + broadcast = 103 direcciones IPs | 128=2^7 | /25 |
| WIFI AULA 2 | 100 host + router + base + broadcast = 103 direcciones IPs | 128=2^7 | /25 |
| WIFI AULA 3 | 100 host + router + base + broadcast = 103 direcciones IPs | 128=2^7 | /25 |
| SECRETARIA COMUNES | 32 host + router + base + broadcast = 35 direcciones IPs | 64=2^6 | /26 |
| R9-R10WF | 2 routers + base + broadcast = 4 direcciones IPs | 4=2^2 | /30 |

Tabla 1

| **Biblioteca** | | | |
| --- | --- | --- | --- |
| **Nombre de la Red** | **Descripción de las IPs necesarias** | **Tamaño del bloque** | **Máscara resultante** |
| BIBLIOTECA WIFI-PB | 100 host + router + base + broadcast = 103 direcciones IPs | 128=2^7 | /25 |
| BIBLIOTECA WIFI-PA | 100 host + router + base + broadcast = 103 direcciones IPs | 128=2^7 | /25 |
| RECEPCION BIBLIOTECA | 27 host + router + base + broadcast = 30 direcciones IPs | 32=2^5 | /27 |
| OFICINAS BIBLIOTECA | 16 host + router + base + broadcast = 19 direcciones IPs | 32=2^5 | /27 |
| R5-R6 | 2 routers + base + broadcast = 4 direcciones IPs | 4=2^2 | /30 |

Tabla 2

| **Comedor** | | | |
| --- | --- | --- | --- |
| **Nombre de la Red** | **Descripción de las IPs necesarias** | **Tamaño del bloque** | **Máscara resultante** |
| WIFI COMEDOR | 100 host + router + base + broadcast = 103 direcciones IPs | 128=2^7 | /25 |
| RECEPCION COMEDOR | 44 host + router + base + broadcast = 47 direcciones IPs | 64=2^6 | /26 |
| ALMACEN COMEDOR | 7 host + router + base + broadcast = 10 direcciones IPs | 16=2^4 | /28 |
| R7-WFR8 | 2 routers+ base + broadcast = 4 direcciones IPs | 4=2^2 | /30 |

Tabla 3

**Punto B:**

A continuación se desglosan los requerimientos de los pabellones en la siguiente tabla, de la misma manera que en el punto anterior, pero que con la diferencia de que se logra un paneo general del total de direcciones y requerimientos finales necesarios para abastecer toda la red.

| **Nombre de la Red** | **Descripción de las IPs necesarias** | **Tamaño del bloque** | **Máscara resultante** |
| --- | --- | --- | --- |
| Data Center | 2 routers frontera + 500 servidores + base + broadcast=504 direcciones IP | 512=2^9 | /23 |
| Comunes | Subredes WIFI-AULA1 /WIFI-AULA2 / WIFI-AULA3 / SECRETARIA COMUNES/ R9-R10WF + base +broadcast =348 direcciones IPs | 512=2^9 | /23 |
| Biblioteca | Subredes RECEPCIÓN BIBLIOTECA / OFICINAS BIBLIOTECA / WIFI BIBLIOTECA P-B / WIFI BIBLIOTECA P-A / R5-R6 + base + broadcast = 259 direcciones IPs | 512=2^9 | /23 |
| Comedor | Subredes ALMACEN COMEDOR / RECEPCION COMEDOR / WIFI COMEDOR / R7-WFR8 = 164 direcciones IPs | 256=2^8 | /24 |
| Troncal | 80 pabellones + router + base + broadcast = 83 direcciones IPs | 128=2^7 | /25 |
| R4-R3 | 2 router + base + broadcast = 4 direcciones IPs | 4=2^2 | /30 |

Tabla 4

**Punto C:**

En el siguiente gráfico, se observa la puesta en marcha de la técnica VLSM, en la que para los requerimientos generales del Campus Universitario, se agrupan las redes generales de mayor a menor en ámbito de cantidad de direcciones asignadas y las máscaras resultantes.

Como se puede observar, se utiliza un bloque que enmarca la cantidad total de direcciones necesarias. Para este caso, era necesario cumplir con 1362 IPs y para esto es necesario utilizar una máscara /21 para cubrir 2048 IPs.

En la imagen 2 se observa cómo se encuentra configurado el esquema que representa toda la red con sus correspondientes máscaras y direcciones de rango asignadas.

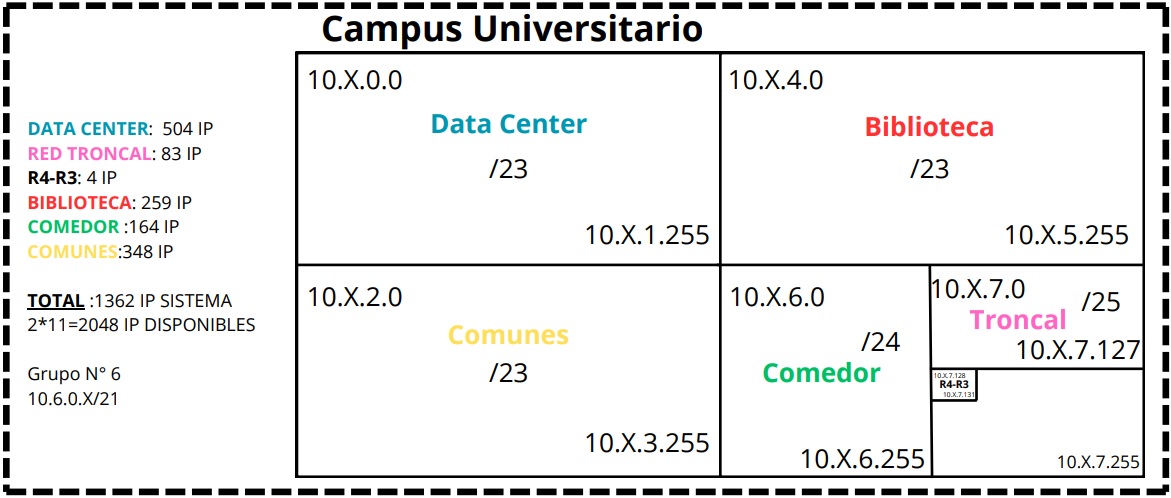


Imagen 2

En la imagen 3 se observa la red R4-R3 en ampliación con sus respectivos valores de máscara y rango como se hizo referencia en la imagen 2.



Imagen 3

**Punto D:**

En las siguientes imágenes , se observan la puesta en marcha de la técnica VLSM, en sintonía con el punto anterior, en la que para los requerimientos específicos de cada pabellón, se agrupan las redes generales de mayor a menor en ámbito de cantidad de direcciones asignadas y las máscaras resultantes.

Como se puede observar, el bloque del pabellón general, ahora vuelve a ser dividido en nuevos bloques que asignan las direcciones de las sub redes.

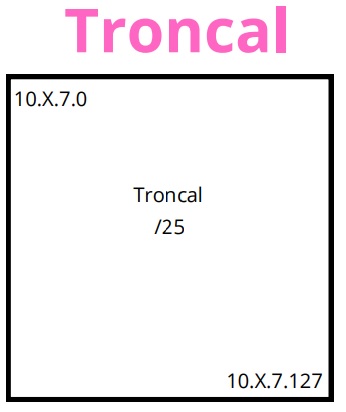
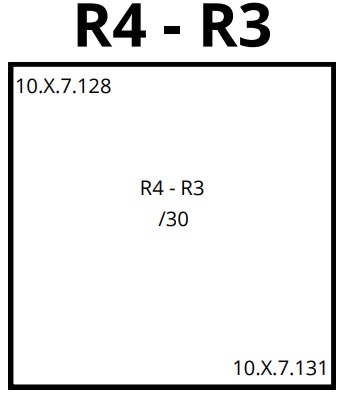
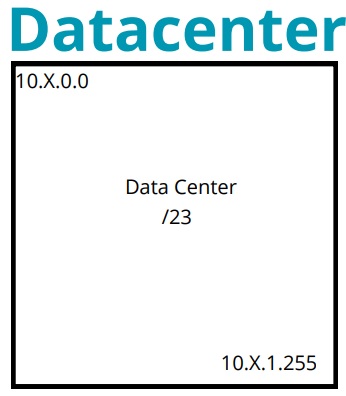


Imagen 4

En la imagen 4, se observan las redes que en su estructura forman un solo bloque para poder abastecer sus requerimientos, mientras que en las siguientes imágenes, podremos observar como las subredes que viven dentro de estos bloques generales son identificadas para una correcta configuración y asignación en los siguientes pasos de este desarrollo.

En la imagen 5, 6 y 7 ya se encuentra nuevamente los bloques subdivididos para las subredes que pertenecen a los pabellones “Comunes”, “Biblioteca” y “Comedor”.

Se puede observar cómo se encuentran distribuidas cada red que fue referenciada en el punto A y que establecen sus bloques contemplando todo el espacio de direcciones disponibles en base a sus requerimientos informados en el enunciado de necesidades para esta red y esta topología.

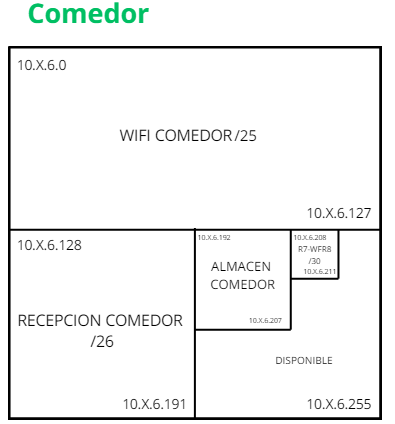


Imagen 5

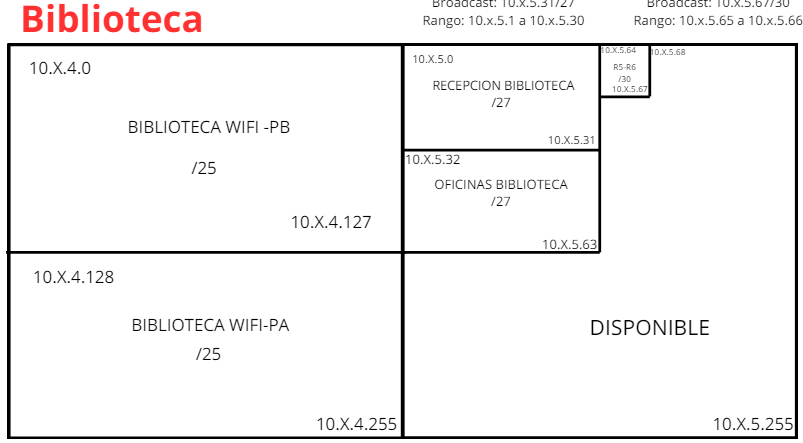


Imagen 6

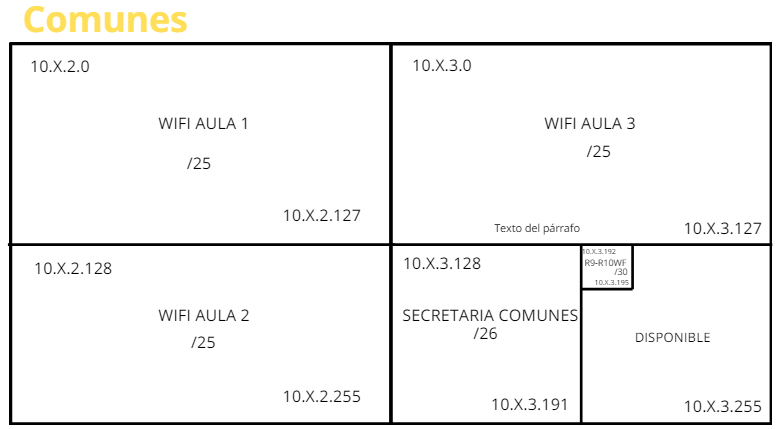


Imagen 7

**Punto E:**

Las siguientes tablas representan la asignación de todas las redes y subredes, con dirección base, broadcast, máscara y rango de IPs asignables. De esta manera ya las distintas redes contemplan información específica necesaria para poder configurar en el simulador dichos atributos y permitir empezar a realizar pruebas de conexión entre las mismas.

| **Redes** | | | | |
| --- | --- | --- | --- | --- |
| **Nombre de la Red** | **Dirección Base** | **Máscara** | **Rango asignable** | **Broadcast** |
| DataCenter | 10.6.0.0 | 255.255.254.0 | 10.6.0.1 a 10.6.1.254 | 10.6.1.255 |
| Comunes | 10.6.2.0 | 255.255.254.0 | 10.6.2.1 a 10.6.2.126 | 10.6.2.127 |
| Biblioteca | 10.6.4.0 | 255.255.254.0 | 10.6.4.1 a 10.6.5.254 | 10.6.5.255 |
| Comedor | 10.6.6.0 | 255.255.255.0 | 10.6.6.1 a 10.6.6.254 | 10.6.6.255 |
| Troncal | 10.6.7.0 | 255.255.254.128 | 10.6.7.1 a 10.6.7.126 | 10.6.7.127 |
| R4-R3 | 10.6.7.128 | 255.255.255.252 | 10.6.7.129 a 10.6.7.130 | 10.6.7.131 |

Tabla 5

| **Comunes 1** | | | | |
| --- | --- | --- | --- | --- |
| **Nombre de la Red** | **Dirección Base** | **Máscara** | **Rango asignable** | **Broadcast** |
| WIFI AULA 1 | 10.6.2.0 | 255.255.255.128 | 10.6.2.1 a 10.6.2.126 | 10.6.2.127 |
| WIFI AULA 2 | 10.6.2.128 | 255.255.255.128 | 10.6.2.129 a 10.6.2.254 | 10.6.2.255 |
| WIFI AULA 3 | 10.6.3.0 | 255.255.255.128 | 10.6.3.1 a 10.6.3.126 | 10.6.3.127 |
| SECRETARIA COMUNES | 10.6.3.128 | 255.255.255.192 | 10.6.3.129 a 10.6.3.190 | 10.6.3.191 |
| R9-R10WF | 10.6.3.192 | 255.255.255.252 | 10.6.3.193 a 10.6.3.194 | 10.6.3.195 |

Tabla 6

| **Biblioteca** | | | | |
| --- | --- | --- | --- | --- |
| **Nombre de la Red** | **Dirección Base** | **Máscara** | **Rango asignable** | **Broadcast** |
| BIBLIOTECA WIFI-PB | 10.6.4.0 | 255.255.255.125 | 10.6.4.1 a 10.6.4.126 | 10.6.4.127 |
| BIBLIOTECA WIFI-PA | 10.6.4.128 | 255.255.255.125 | 10.6.4.129 a 10.6.4.254 | 10.6.4.255 |
| RECEPCIÓN BIBLIOTECA | 10.6.4.5.0 | 255.255.255.224 | 10.6.5.1 a 10.6.5.30 | 10.6.5.31 |
| OFICINAS BIBLIOTECA | 10.6.5.32 | 255.255.255.224 | 10.6.5.33 a 10.6.5.62 | 10.6.5.63 |
| R5-R6 | 10.6.5.64 | 255.255.255.252 | 10.6.5.65 a 10.6.5.66 | 10.6.5.67 |

Tabla 7

| **Comedor** | | | | |
| --- | --- | --- | --- | --- |
| **Nombre de la Red** | **Dirección Base** | **Máscara** | **Rango asignable** | **Broadcast** |
| WIFI COMEDOR | 10.6.6.0 | 255.255.255.128 | 10.6.6.1 a 10.6.6.126 | 10.6.6.127 |
| RECEPCION COMEDOR | 10.6.6.128 | 255.255.255.192 | 10.6.6.129 a 10.6.6.190 | 10.6.6.191 |
| ALMACÉN COMEDOR | 10.6.6.192 | 255.255.255.240 | 10.6.6.193 a 10.6.6.206 | 10.6.6.207 |
| R7-WFR 8 | 10.6.6.208 | 255.255.255.252 | 10.6.6.209 a 10.6.6.210 | 10.6.6.211 |

Tabla 8

**Punto F:**

En la imagen 4,se muestra como quedaron determinadas las redes luego de haber aplicado la técnica VLSM.

Cada red o subred de los pabellones, se encuentra identificada por su número y máscara de red.

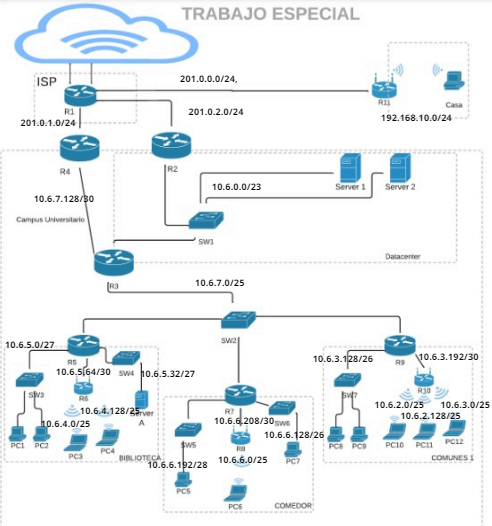


Imagen 4

En la imagen 5, se encuentra profundizado la incorporación de las IPs y las máscaras de red, correspondientes para cada dispositivo que se encuentra en el esquema general.

Se puede observar que además, se encuentran determinadas las interfaces para cada router y cada dispositivo que interviene en el sistema, necesarios para poder establecer la conexión de redes con sus correspondientes puertos físicos que luego serán configurados en las tablas de ruteo.

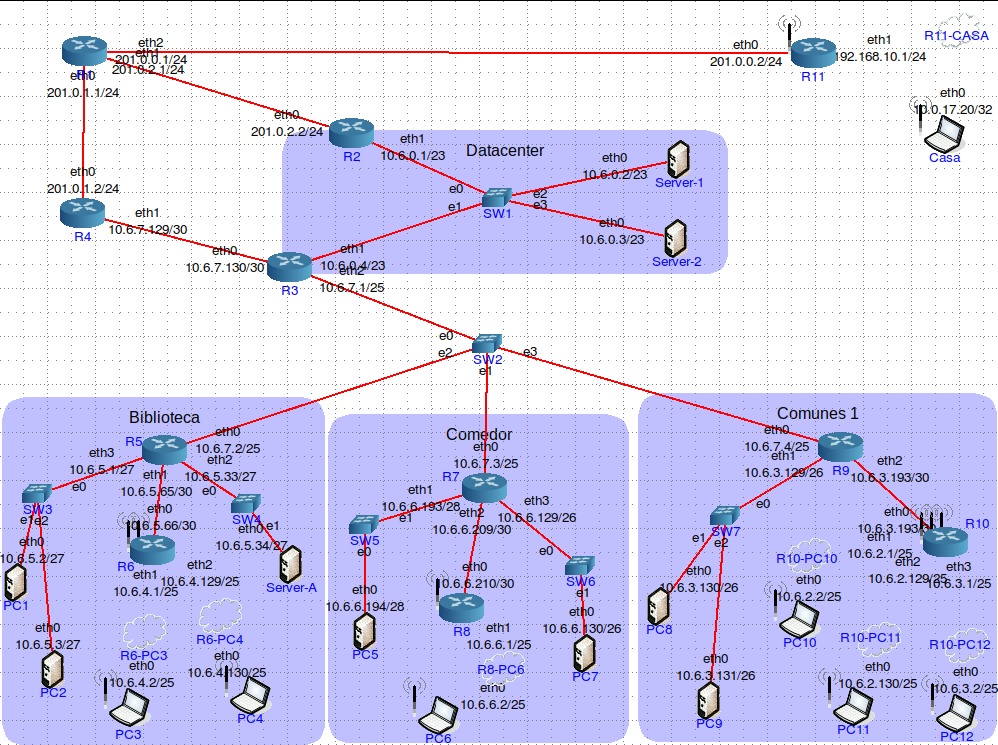
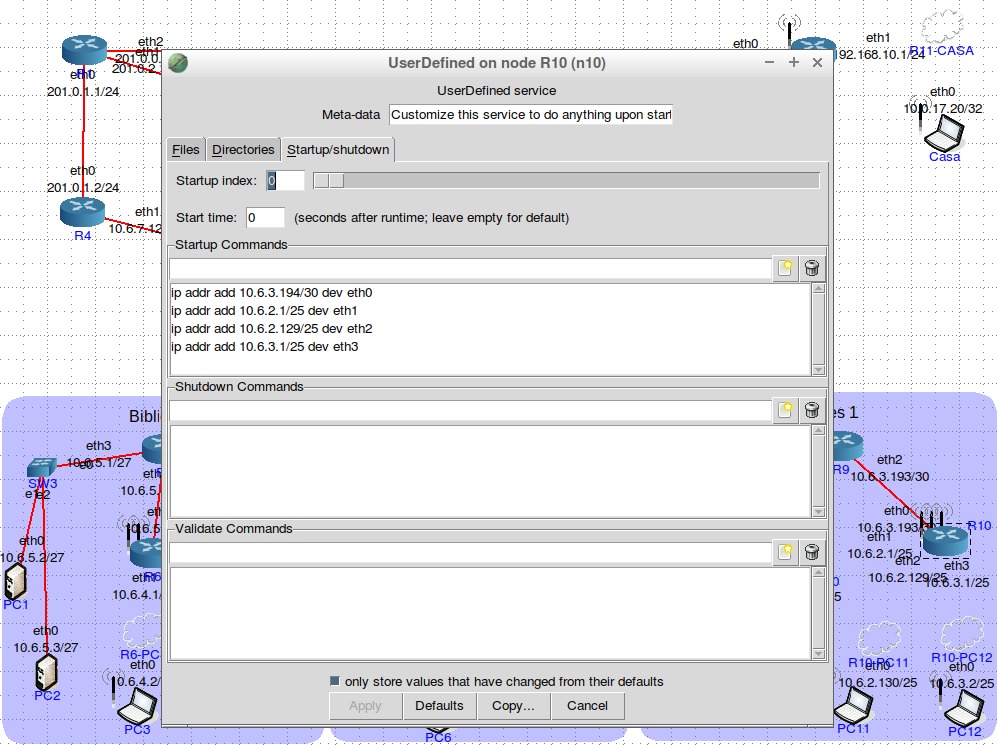


Imagen 5

**Punto G:**

Para esta etapa se adjunta la imagen 6, de la configuración correspondiente de uno de los routers que componen la red. De esta manera, luego de haber en el paso anterior asignado cada red y cada subred, se prosigue implementando la asignación de las interfaces a cada red que los dispositivos tienen a su alcance.

Mediante el comando ***“ip addr add <numero de red y máscara> dev <interfaz de salida>”*** se configura cada dispositivo y así lograr la conexión a dichas redes.

Imagen 6

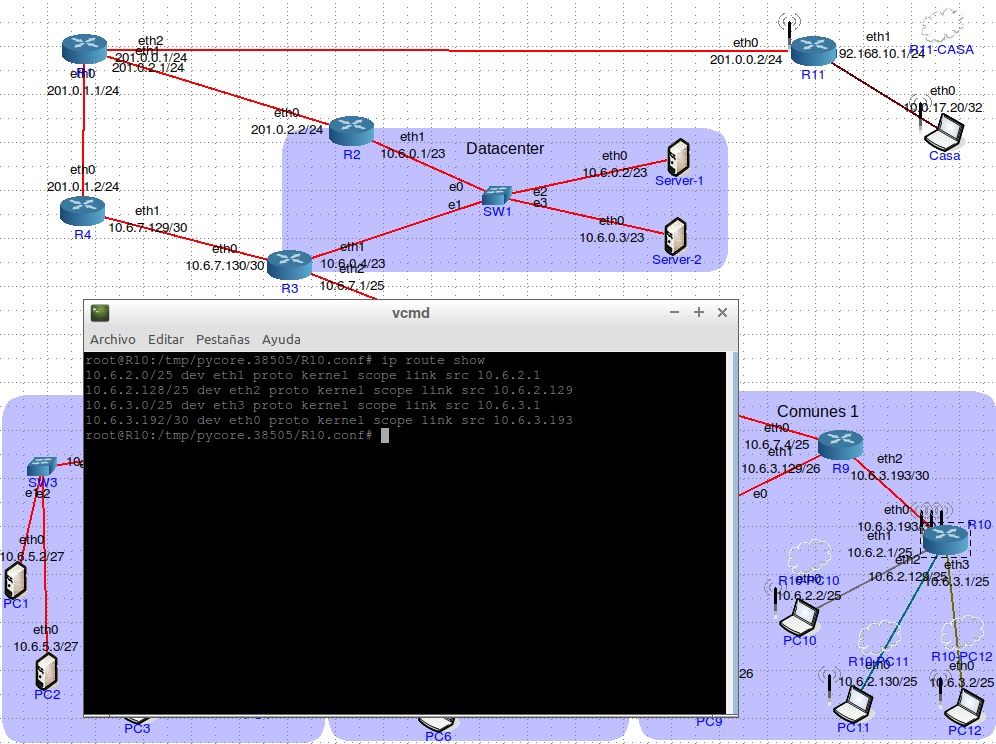
Por medio del comando “ip route show”, en la imagen 7 quedan configuradas las implementaciones en tiempo de ejecución correspondiente a los equipos, a través de la consola CMD.

Imagen 7

**Punto H:**

Las imágenes a continuación demuestran el funcionamiento de una de las redes locales con la configuración establecida en el punto G.

A través del comando ***“ping”***, es posible enviar una cierta cantidad de paquetes si se especifica, donde se comprueba el estado de la comunicación entre un host local hacia otro remoto y chequear que estos sean recibidos por la IP destino por medio del protocolo ICMP.

Como se puede observar en la imagen 8, se encuentra realizado un envío de cuatro paquetes desde PC1 por la interfaz eth0 hacia PC2 con dirección IP 10.6.5.3/27.  
Para este caso, el envío de los paquetes devuelve una respuesta exitosa, pero para el caso en que existan problemas de comunicación, equipo no encontrado o red desconocida las respuestas a estos paquetes pueden ser: “Destination Host Unreachable”, “Destination Net Unreachable” o “Time Exceeded”.

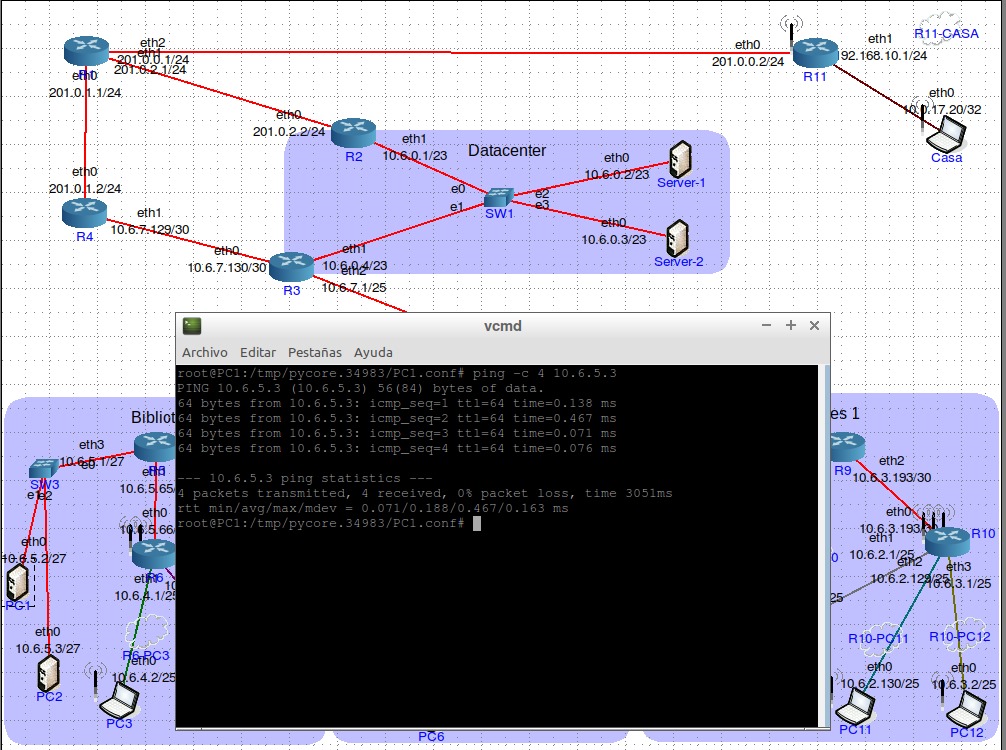


Imagen 8

La imagen 9, expone el comando ejecutado traceroute hacia la dirección IP 10.6.2.130,  
Este comando, corresponde a la herramienta “traceroute”, la cual permite en este caso, conocer la ruta que se recorre hasta llegar a la dirección IP destino.

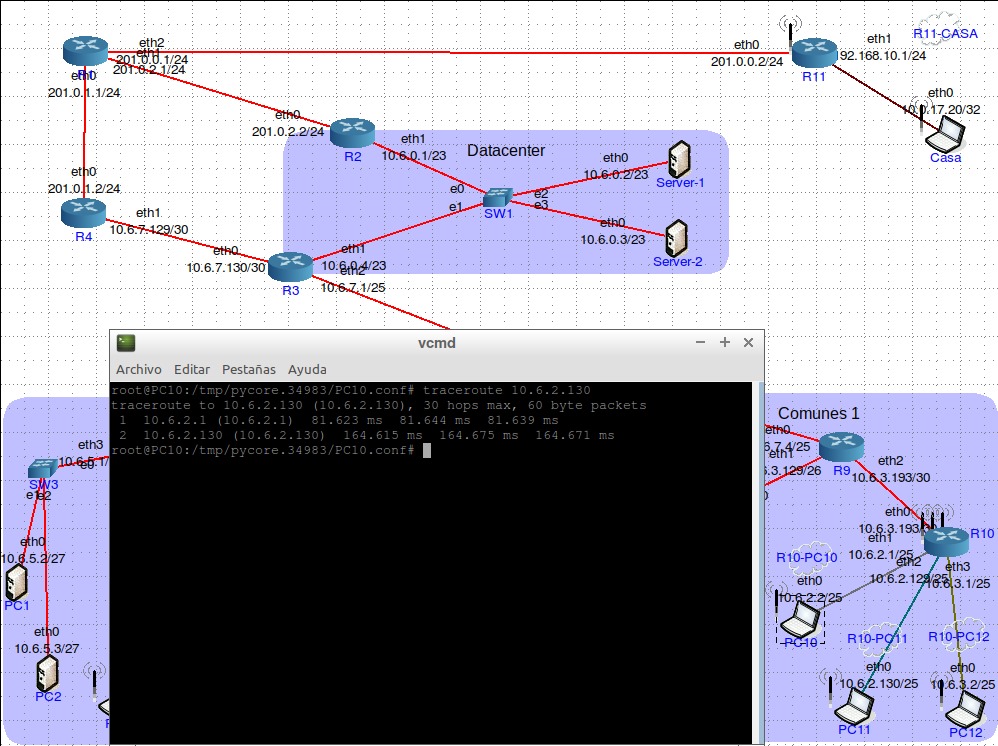


Imagen 9

Por último la imagen 10, demuestra la utilización del SW “WireShark”, el cual permite hacer un diagnóstico personalizado desde una interfaz seleccionada poder observar el tráfico de paquetes que pasan por esta más detallado.

Para esta imagen(imagen 10), se puede observar la captura sobre un conjunto de paquetes enviados a la dirección IP 10.6.2.130, por medio del protocolo ICMP.

En la primera barra de esta interfaz, se puede seleccionar filtros para personalizar las búsquedas según el protocolo seleccionado.

En la barra intermedia, coloreado en lila, se encuentran los paquetes capturados, correspondientemente se muestra el origen y el destino de cada paquete.

También se puede observar el protocolo que utiliza, la información del paquete y el tiempo.

Para la tercera barra, se muestran los detalles específicos que tiene la elección de uno de estos paquetes. En estos detalles, ya está la información correspondiente a las capas de la red por la que estas se encuentran desglosadas, tamaños y tipo de protocolos utilizados.

Por último, en la última barra, se puede observar los datos crudos correspondientes a los paquetes, expresados en notación hexadecimal.

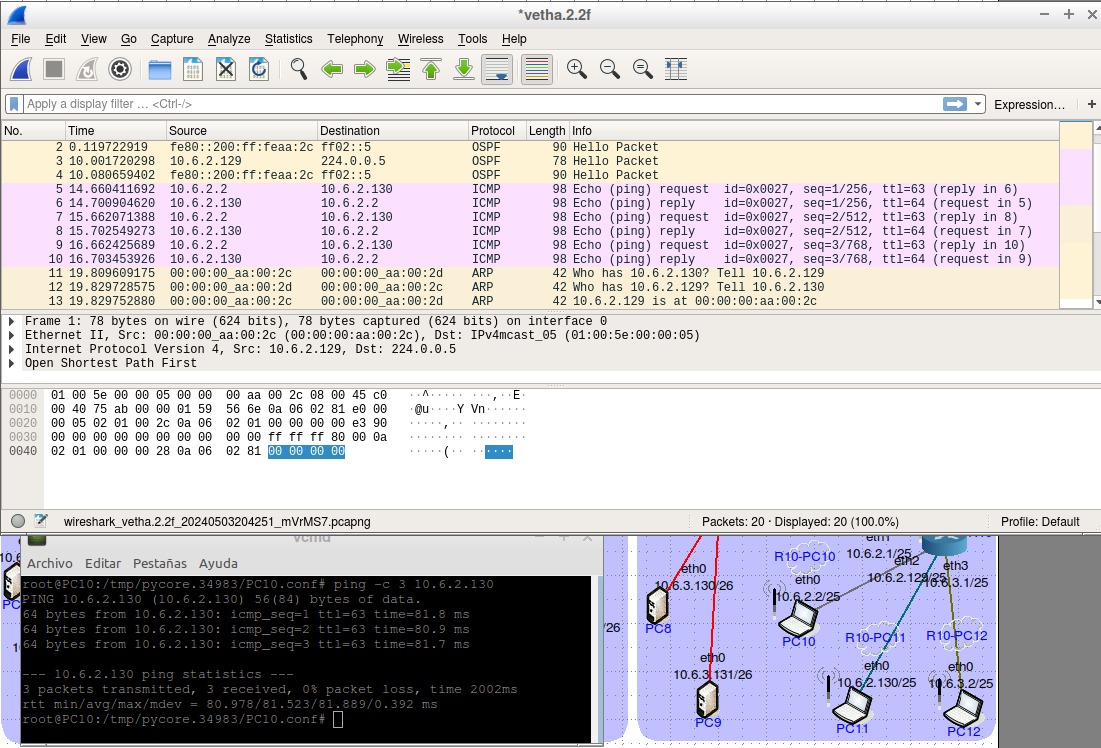


Imagen 10

**PARTE 2**

**Punto A.:**

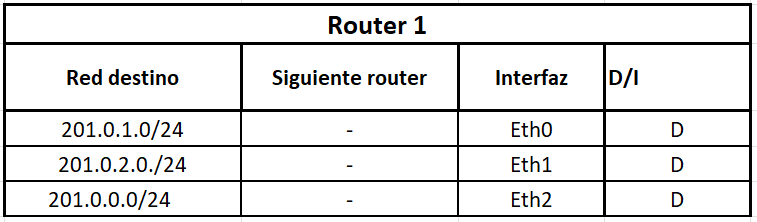
Las tablas expuestas a continuación representan cada dispositivo router en el sistema con sus respectivas redes configuradas en conjunto con las interfaces que permiten este vínculo y los caminos por los cuales deben tomar.  


Tabla 9

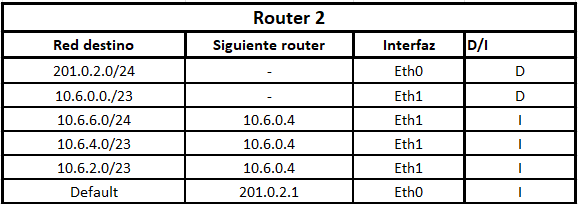


Tabla 10

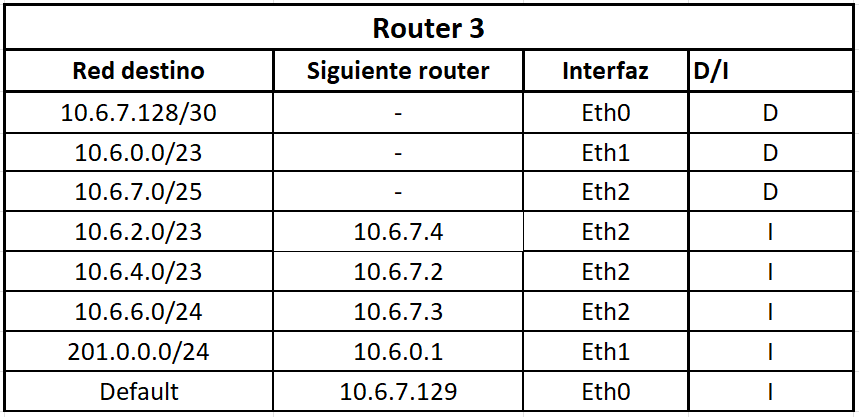


Tabla 11

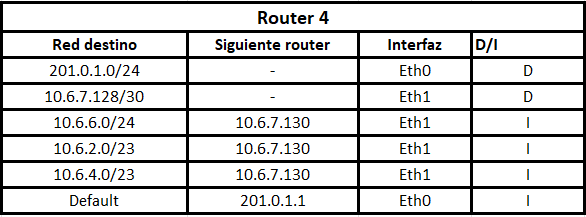


Tabla 12

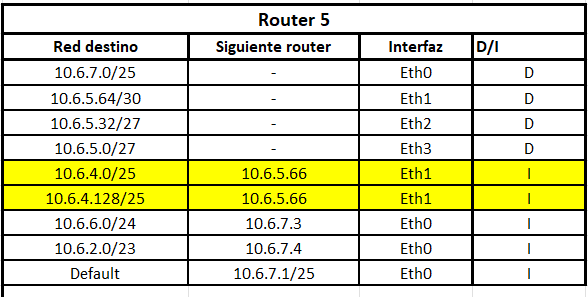


Tabla 13

Como se puede ver en la tabla 13, la ruta desde R5 hacia las redes wifi 10.6.4.0/25 y 10.6.4.128/25 se pueden minimizar por sumarización y queda en una red 10.6.4.0/24, esto es posible ya que comparten bloques contiguos, misma interfaz de salida, misma máscara y mismo siguiente router.  
Para la imagen 11 , se demuestra esta simplificación por medio del comando iproute, correspondiente a este router(R5), en el cual se observa que las rutas cargadas en la tabla 13 ya no se encuentran, sino que han sido simplificadas a la red antes nombrada 10.6.4.0/24.

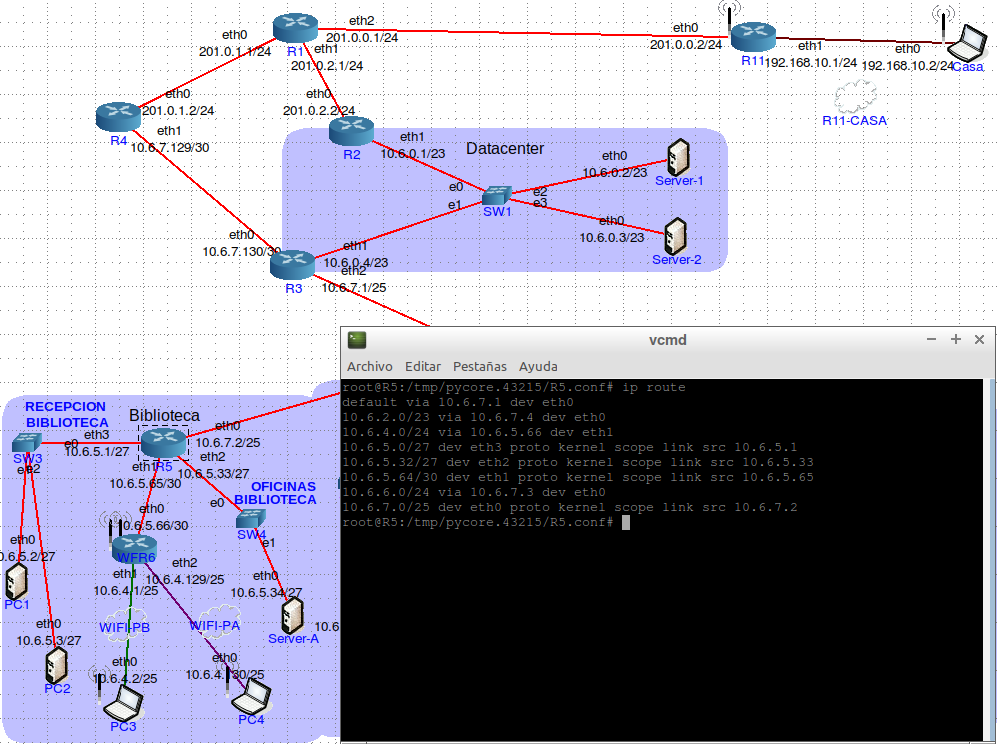


Imagen 11

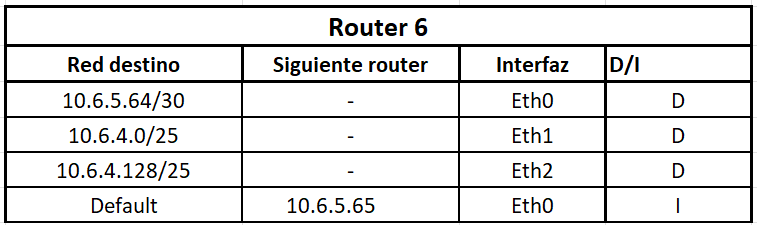


Tabla 14

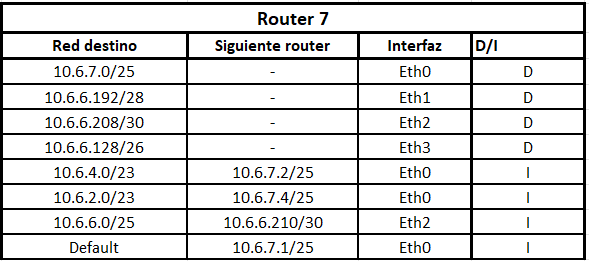


Tabla 15

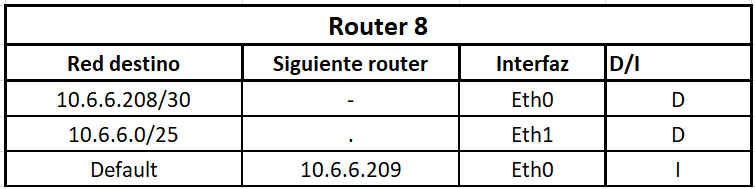


Tabla 16

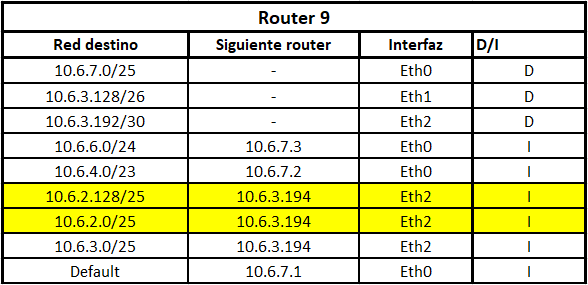


Tabla 17

En la tabla 17 , sucede el mismo ejemplo de sumarización que en la tabla 13.

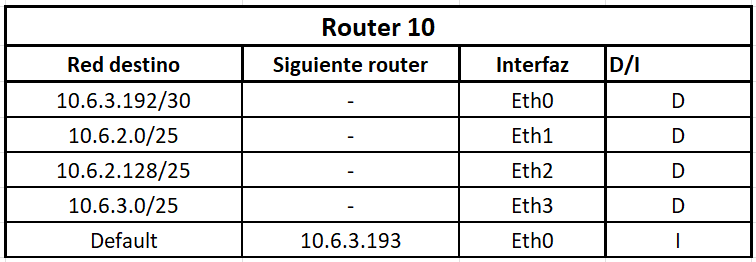


Tabla 18

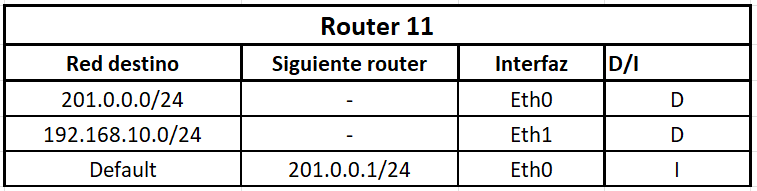


Tabla 19

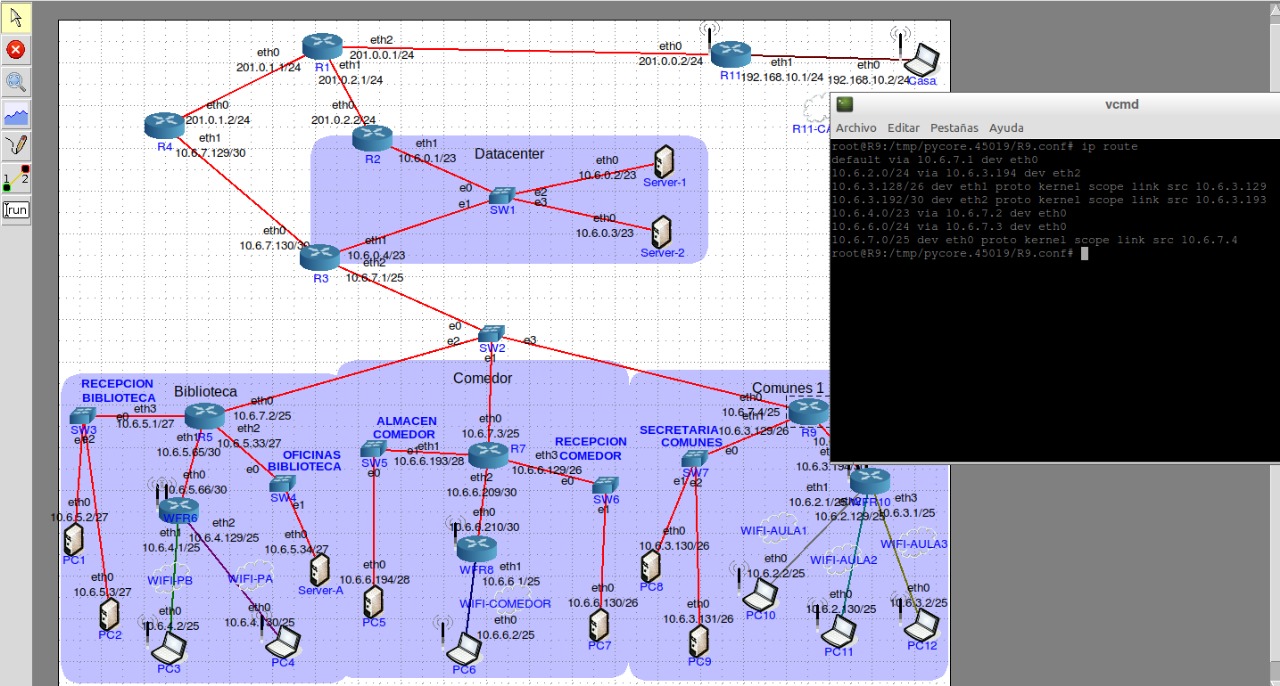


Imagen 12

Para mostrar un ejemplo de como quedan cargadas las rutas estando en tiempo de ejecución, se puede observar la imagen 12, las rutas cargadas en el router R9 y en la imagen 13, las rutas cargadas en el router R8.

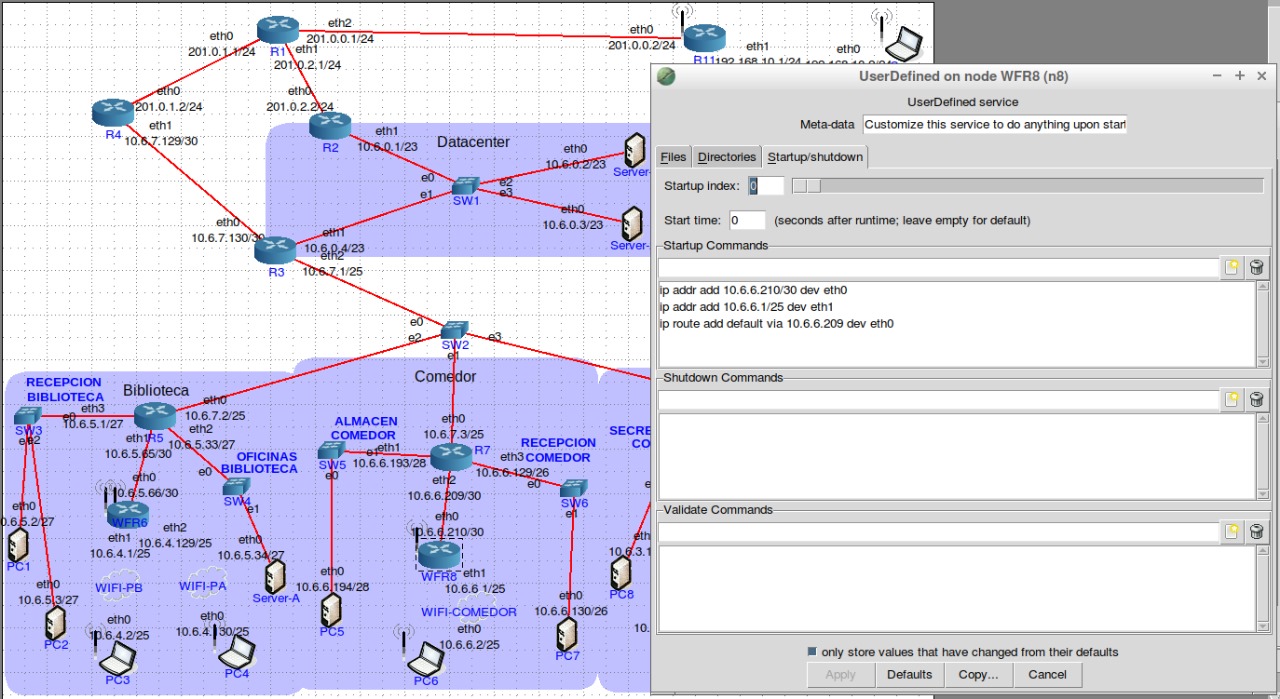


Imagen 13

La diferencia entre las imágenes 12 y 13, son las distintas maneras de ver las rutas por las que se encuentran configurados ambos dispositivos. El simulador permite cargar las rutas previo a ejecutar el programa y simular el funcionamiento.

Con cada dispositivo de la red se implementa de la misma manera que los antes mencionados, para cada uno le corresponde cargar tanto las rutas directas e indirectas, contemplando que se pueden minimizar tanto por sumarización o default siempre que se den las condiciones.

**Punto B.:**

Dentro de los requerimientos solicitados a cumplir, el inciso B solicita configurar el R4 para que solo tengan acceso a internet los equipos conectados a la red Biblioteca y Aulas Comunes 1.

Para lograr configurar la red se establecieron en R4 los siguientes comandos:

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

Esta regla es responsable de configurar la reescritura de direcciones o de puertos de los paquetes permitiendo salir a internet

* ***iptables -t filter -A FORWARD -s <IP red origen> -j ACCEPT***

Esta regla acepta el tráfico con origen Biblioteca y Comunes 1 con destino a internet para el cual deberá pasar por el R3.

* ***iptables -t filter -A FORWARD -i <interfaz de salida> -j REJECT***

Rechaza el tráfico que quiera salir a internet desde la red privada por Eth1 que no sean Biblioteca o Comunes 1, si en algún futuro se agregan redes tampoco puedan acceder, a no ser que se agreguen cadenas que acepten la red (en ambos router frontera).

En la imagen 14 se puede observar por medio del comando ping y un recorrido traceroute, que la PC1 correspondiente a la red Biblioteca, tiene conexión hacia internet, recibiendo la respuesta de los paquetes enviados a la IP del router ISP y el correcto direccionamiento desde el router R3, luego hacia R4 y por último al destino de ISP.



Imagen 14

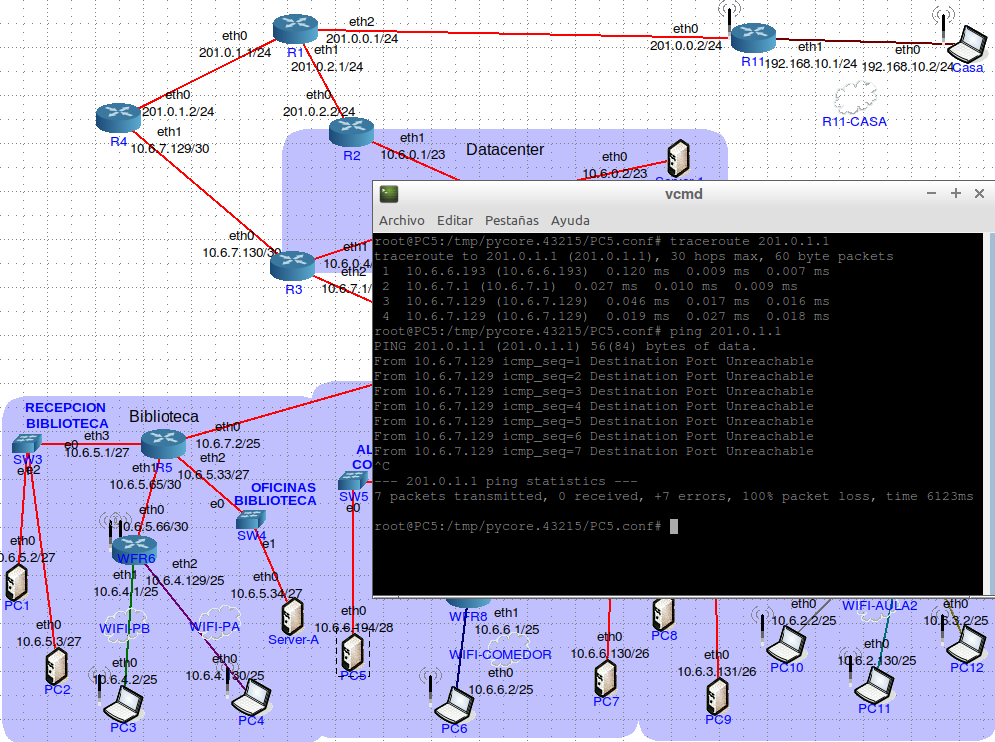


Imagen 15

En cambio en la imagen 15, se puede observar por medio del comando ping y un recorrido traceroute, que la PC5 correspondiente a la red Comedor,no tiene conexión hacia internet, recibiendo la respuesta de los paquetes enviados a la IP del router ISP y el correcto direccionamiento desde el router R3, luego hacia R4 y sin posibilidades de avanzar, gracias a la última regla que se aplica en R4, que rechaza todo flujo que quiera atravesar y que no sea Biblioteca o Comunes.

Para la última imagen correspondiente a esta configuración, la imagen 16 muestra las reglas aplicadas para dar acceso a internet, pero al mismo tiempo restringir solo las redes a las que quiere dar acceso “Biblioteca” y “Comunes”, pero rechaza toda red que no sea las anteriores mencionadas. Permitiendo de esta manera establecer correctamente que ante una nueva red que se agregue, siga teniendo la misma persistencia.



Imagen 16

**Punto C.:**

El siguiente requerimiento solicitado para esta red implementada es configurar el router R2 para que el datacenter salga a Internet por este router.

Para hacer posible este punto es necesario agregar en R2 los comandos:

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

Esta regla es responsable de configurar la reescritura de direcciones o de puertos de los paquetes permitiendo salir a internet.

* ***ip route addr add default via 201.0.2.1 dev Eth0***

Se asigna default para que la red Data Center vaya hacia internet por esta ip.

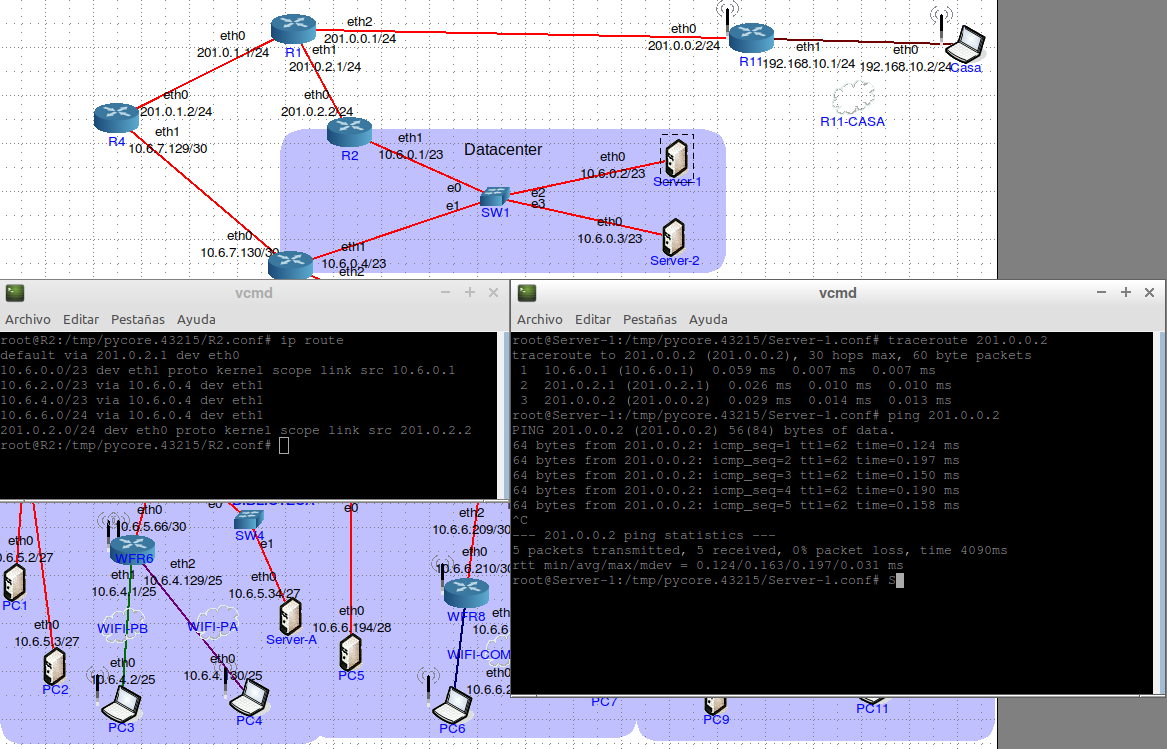


Imagen 17

En la imagen 17, se puede observar que la tabla de ruteo correspondiente al router R2, tiene configurado como ruta default la ip correspondiente al router ISP, permitiendo que todo el tráfico que Data Center quiera establecer con internet, salga por esta ruta.  
Se confirma el correcto funcionamiento, emitiendo paquetes ICMP y capturando por traceroute la dirección de la ruta que toma, como se puede observar en la imagen mencionada.

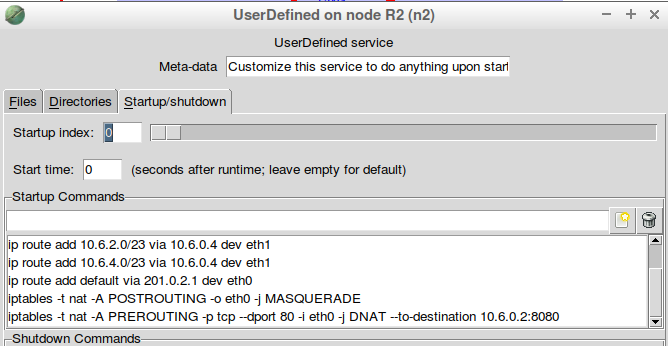


Imagen 18

De la misma manera que se implementó en el inciso anterior, en este caso se puede observar que en la imagen 18, se establecen las políticas en el dispositivo router R2 s ambas reglas que permiten tanto dar internet como que la ruta por defecto sea la salida a internet por la ip pública.

**Punto D.:**

El requerimiento a continuación sigue la misma línea que los requerimientos anteriores y consta de configurar el dispositivo router R11 para que la PC-Casa pueda acceder a internet.

Para hacer posible este punto es necesario agregar a R11 los comandos:

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

Esta regla es responsable de configurar la reescritura de direcciones o de puertos de los paquetes permitiendo salir a internet.

* ***ip route addr add default via 201.0.0.1 dev Eth0***

Asigna default para que la red PC-Casa vaya hacia internet por esta ip.

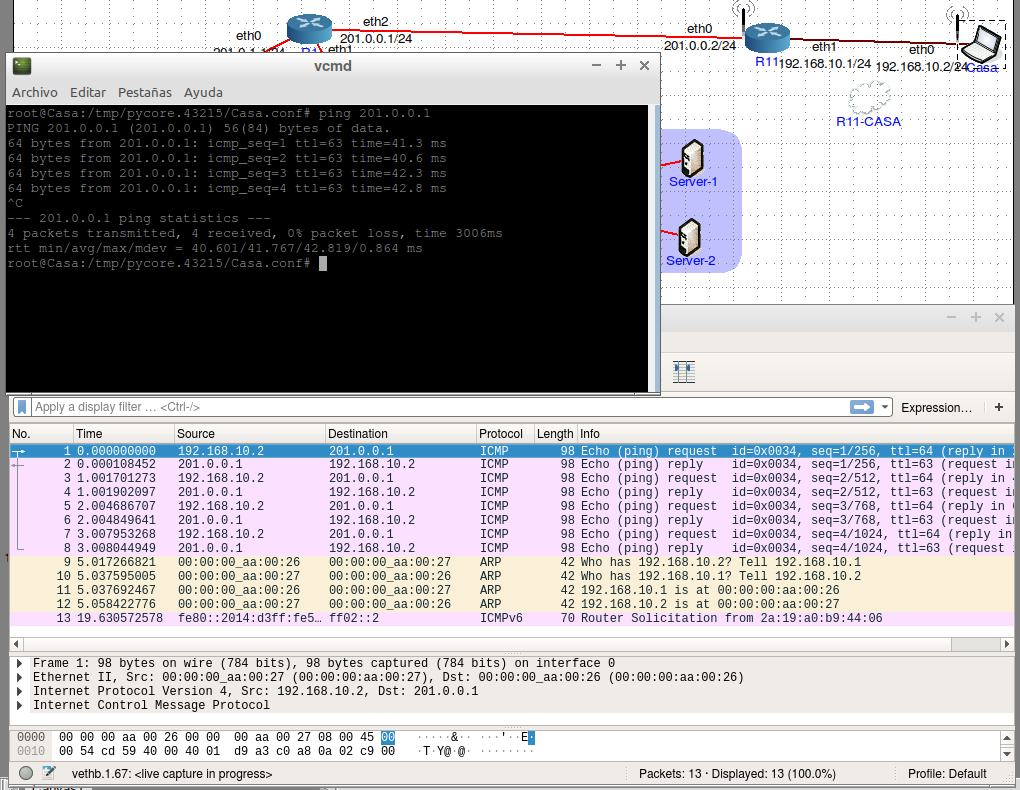


Imagen 19

En la imagen 19 se puede ver cómo por medio de la cadena implementada en R11 es posible salir a internet, permitiendo enmascarar la ip privada de la red R11-CASA a la ip publica 201.0.0.0/24 y demostrando desde el comando ping y traceroute que el flujo de envío de paquetes ICMP y la respuesta es correcta.

**Punto E.:**

Por cuestión de la calidad de los enlaces hacia internet, todo el tráfico del campus dirigido hacia la IP pública del router R11 debe pasar por el router R2, y todos los dispositivos de la red deben poder conectarse a R11. El resto del tráfico hacia internet debe seguir lo especificado en los incisos B y C de esta segunda parte.

Para hacer posible este punto es necesario agregar a R3 los comandos:

* ***ip route addr add 201.0.0.0/24 via 10.6.0.1 dev Eth1***

Agrega la red pública al router, de esta manera cuando el paquete tenga destino a R11 va a ser redirigido por R3 hacia R2.  
Es importante suponer que en “PC-Casa” hay un servicio de internet, de esta manera se conoce la ip pública y de esta forma se puede rutear para que salga exclusivamente por R2. Esto es alvarado ya que una red privada no conoce la red pública, pero para este caso tenemos que interpretar y suponer que existe una red que conecta a PC-Casa.

*Aclaración: este punto fue charlado con la cátedra y nos dieron el “Ok” porque en realidad no es correcto rutear una ip pública, ya que debería salir por default, pero en este caso se la trata de otra manera.*

El resto de los paquetes con otras direcciones públicas distintas a 201.0.0.0/24 salen por default a través del R4.

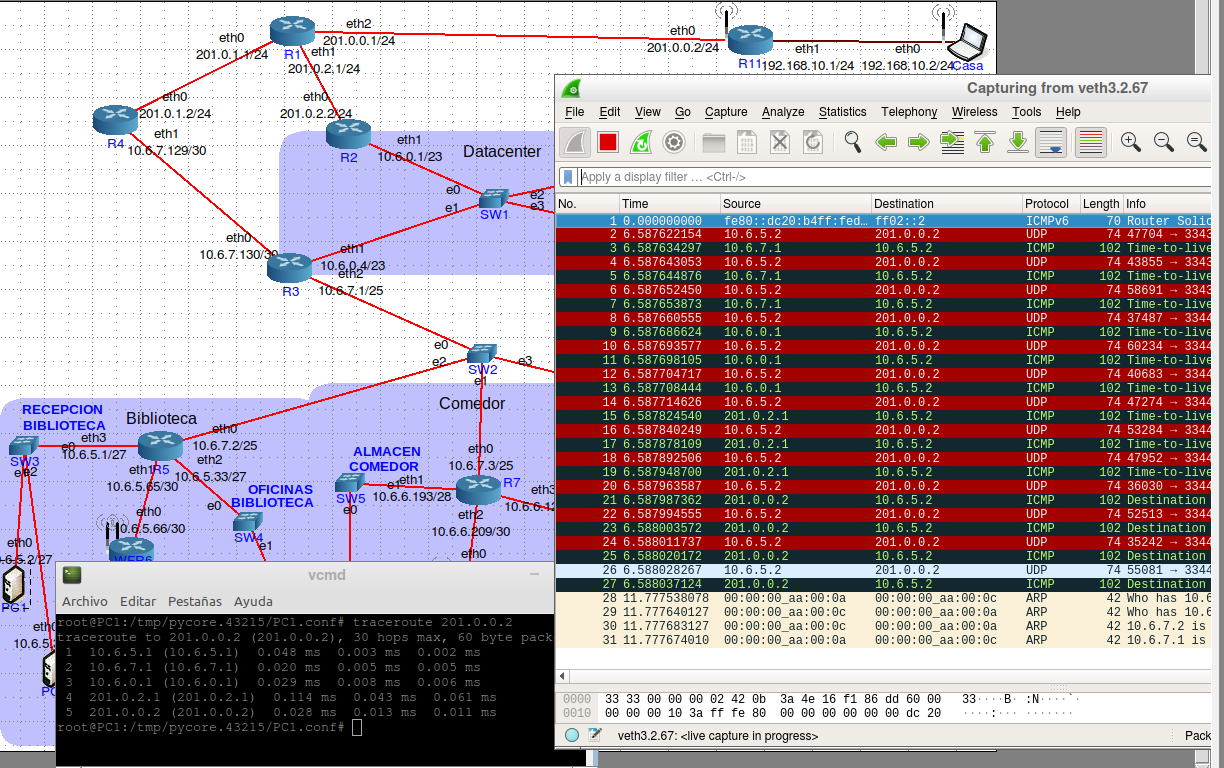


Imagen 20

En la imagen 20,queda demostrado con traceroute y wireshark como funciona el comando mencionado. Que permite que todo los paquetes que se dirijan a la red 201.0.0.0/24 vayan a través del R2 y quedan registrados en la imagen todo su recorrido confirmando la correcta redirección hacia el router mencionado.

De la misma manera hace también referencia a la imagen 21 que en este caso lo demuestra con un comando ping y su correcto funcionamiento al recibir los paquetes que fueron enviados.

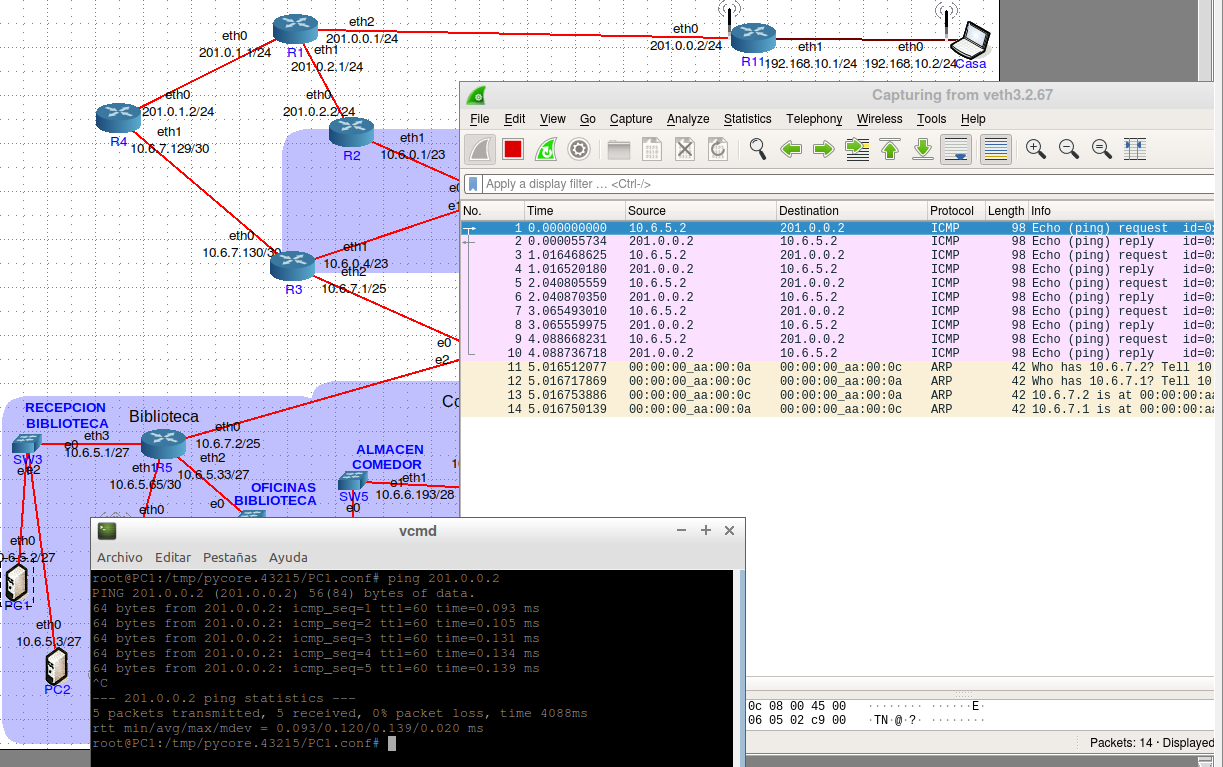


Imagen 21

**Punto F.:**

En este punto se debe configurar la red de manera de poder enviar el mensaje “Hola Data Center” desde PC-Casa hasta el Server 1, utilizando Netcat.

Es imprescindible tener en cuenta configurar el reenvío de paquetes en el router R2 y a fines de la configuración que se intenta implementar en este informe, debe estar estipulado que el puerto que está abierto en el router R2 es el 80.

Es por eso que se establecen los siguientes comandos:

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

Esta regla es responsable de configurar la reescritura de direcciones o de

puertos de los paquetes permitiendo salir a internet.

* ***iptables -t nat -A PREROUTING -p tcp --dport 80 -i eth0 -j DNAT --to- destination 10.6.0.2:8080***

Esta regla toma todos los paquetes TCP que ingresen a la red privada en la interfaz eth0 y tengan destino al puerto 80(HTTP),los redirige a la dirección ip 10.6.0.2 con el puerto 8080. Esta configuración se usa para redirigir el tráfico a un servidor diferente o a un servicio que está escuchando en un puerto diferente.

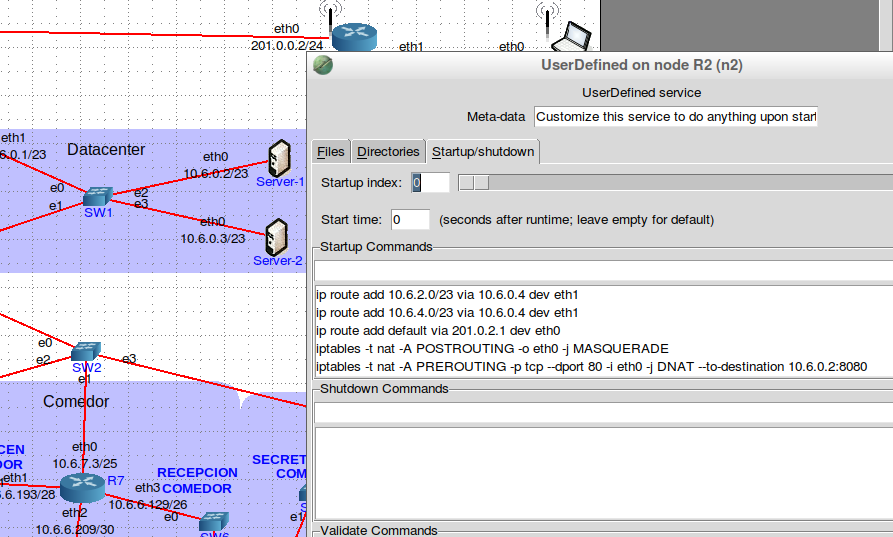


Imagen 22

En la imagen 22 se observan los comandos ya mencionados cargados dentro del R2 que permiten configurar el requerimiento y que a continuación se demuestra el funcionamiento .

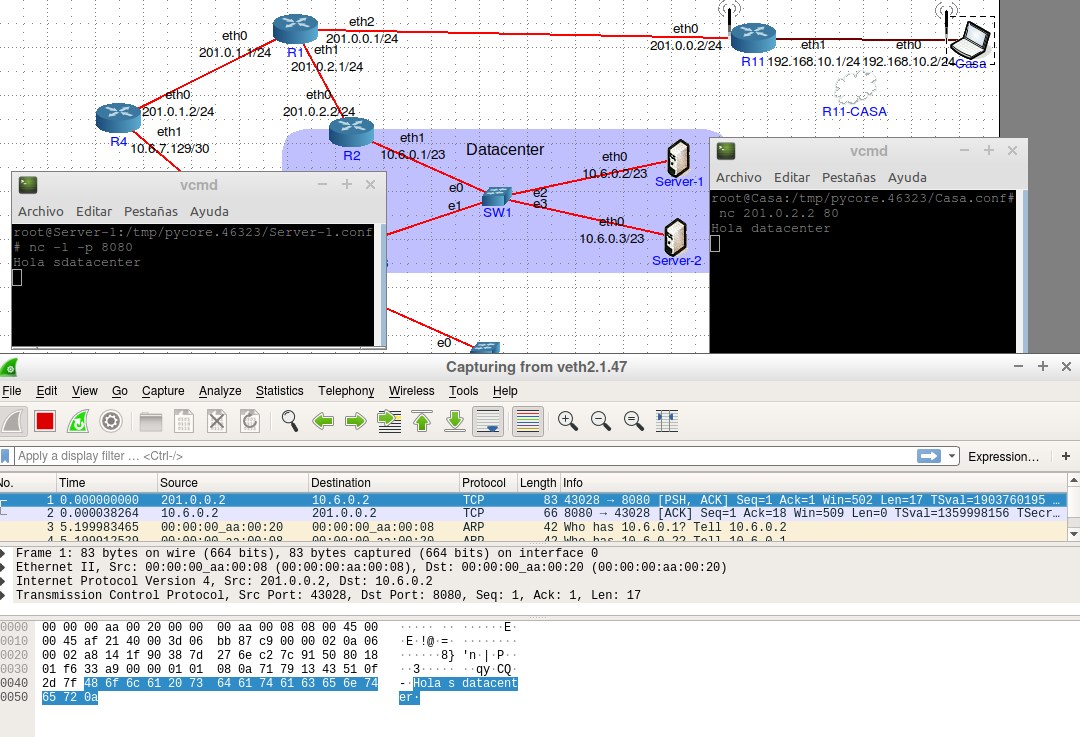


Imagen 23

Para la imagen 23, se observa cómo se hace un llamado al puerto 80 desde PC-Casa (201.0.0.2) con destino al Server (10.6.0.2) y por medio de Wireshark el registro de pasajes por medio del protocolo TCP.

Para lograr configurar que PC-Casa se comunique con el Server 1 situado en DataCenter, se configuró al router R2, que está en la frontera, de forma que aplicando una regla de modificación de IP(por medio de la tabla nat),permite abrir puertos para que desde la red pública se pueda solicitar servicios que pueda ofrecer Server 1.  
En este ejemplo, se indica que toda solicitud que vaya dirigida hacia el puerto 80, debe ser redirigida hacia la ip correspondiente al server con destino de puerto 8080.  
De esta manera y con este tipo de reglas, se permite que las solicitudes que llegan desde una red pública sean macheadas con su correspondiente destino IP y puerto al cual debe responder.

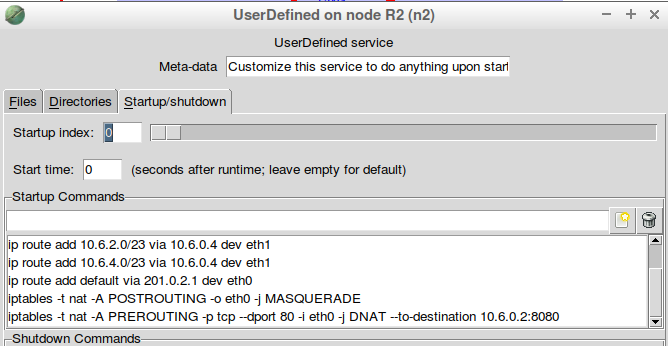


Imagen 24

En la imagen 24 se observa la cadena completa que permite que cada solicitud que sea dirigida al puerto 80 previo a levantar las tablas de ruteo, se modifique la dirección IP y este tráfico sea dirigido hacia la IP 10.6.0.2:8080 correspondiente al Server 1.

Para lograr demostrar la conexión entre estos dos equipos, se utiliza netcat.  
Con el comando **nc -l -p 8080**, se habilita de esta manera que el puerto 8080 ahora esté escuchando correspondiente al Server 1.

Por medio de la regla en la imagen anterior, ahora se puede enviar el mensaje “Hola Data Center” desde PC-Casa, previamente ingresando el comando **nc 201.0.2.2 80**.  
De esta manera se está solicitando entablar comunicación con el puerto 80 perteneciente a la ip pública de R2, que gracias a esta regla, la IP y el puerto destino fueron redirigidos hacia Server 1.

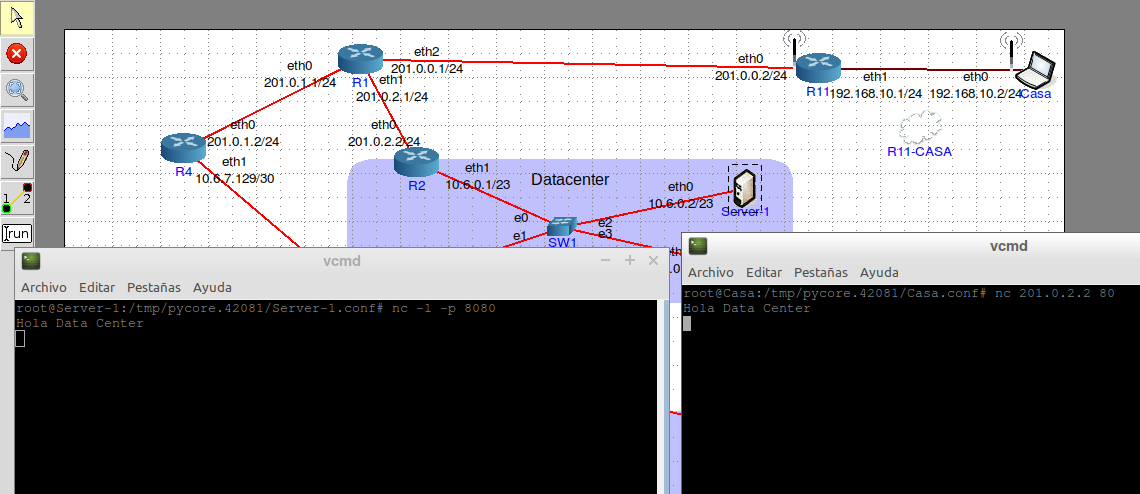


Imagen 25

En la imagen 25 se puede apreciar de una manera más limpia como se establece conexión entre PC Casa y Server 1.

**Punto G.:**

Si se requiere replicar que la conexión del punto anterior se concrete, pero desde la PC1 hacia el Server 1.

Se debe lograr la conexión a través de Netcat, luego de abrir la escucha en el Server-1, en la PC1 se utiliza la dirección IP y puerto específico del servidor nombrado anteriormente (10.6.0.2 8080). Esto es posible, y se diferencia del ejemplo anterior, debido a que ambos equipos pertenecen a la misma red privada.

En la imagen 26 se puede observar la comunicación nombrada.

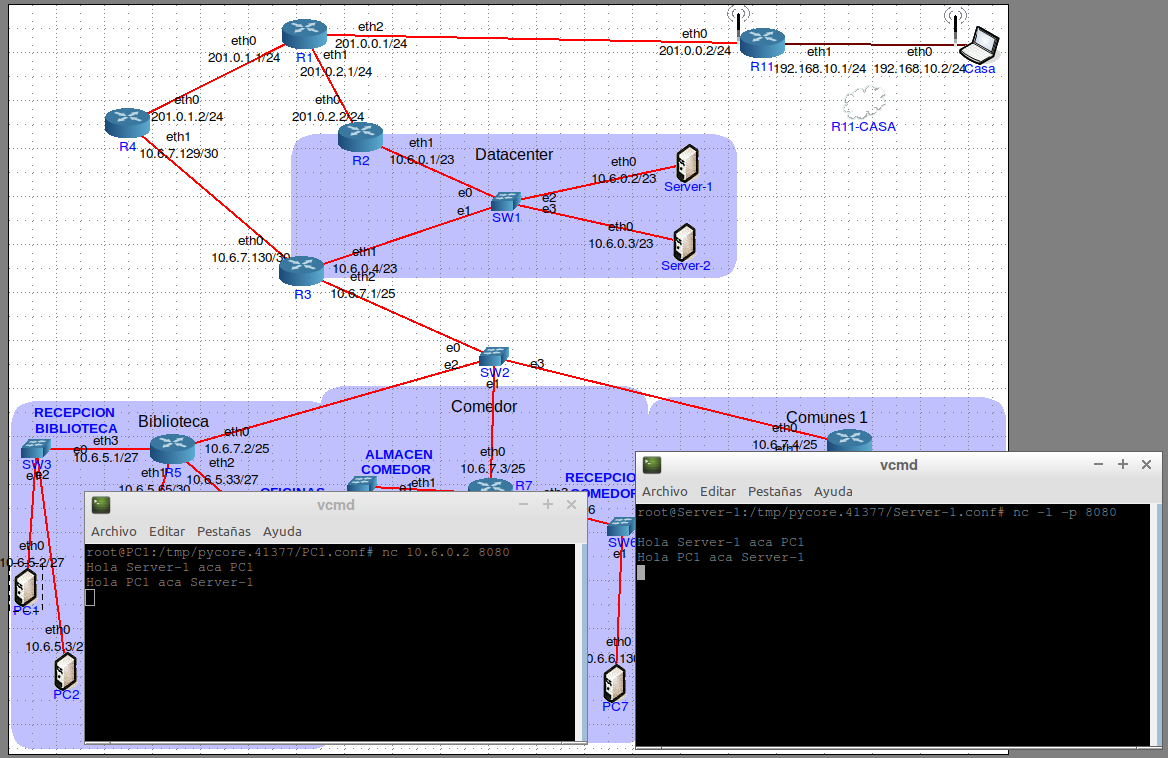


Imagen 26

**Conclusión:**

En el presente trabajo práctico especial, hemos desarrollado y configurado una red compleja para el "Campus Universitario", aplicando los conocimientos adquiridos en la cátedra de Configuración de Desarrollo de Redes. A lo largo del proyecto, se ha diseñado y simulado la red utilizando el simulador CORE, configurando dispositivos, routers y switches, y segmentando la red en troncales y redes privadas.

Resultados Obtenidos

Diseño de Red Eficiente:

Se logró diseñar una red que satisface las necesidades del campus, agrupando las redes y sus componentes de manera coherente y asignando bloques de direcciones IP de manera eficiente utilizando la técnica de VLSM.

Configuración de Tablas de Ruteo:

Se configuraron correctamente las tablas de ruteo, permitiendo la conectividad entre todas las redes y garantizando un ruteo eficiente y seguro.

Distribución de Direcciones IP:

La distribución de direcciones IP se realizó de manera eficiente, asegurando que cada subred disponga de la cantidad de direcciones necesarias sin desperdiciar recursos.

Pruebas y Diagnósticos:

Mediante el uso de herramientas como ping, traceroute y Wireshark, se realizaron pruebas exhaustivas para diagnosticar y asegurar el correcto funcionamiento de la red. Las capturas de pantalla y las explicaciones detalladas corroboran el éxito de estas pruebas.

Acceso a Internet y Seguridad:

Se implementaron configuraciones para proporcionar acceso a internet desde la red privada, abrir puertos para servidores internos y utilizar iptables para filtrado y enmascaramiento de direcciones IP, mejorando así la seguridad de la red.

Posibles Mejoras a Futuro

Optimización del Rendimiento:

Aunque la red está diseñada para ser eficiente, futuras optimizaciones pueden centrarse en mejorar el rendimiento, especialmente en las subredes con mayor tráfico.

En conclusión, el trabajo realizado ha sido exitoso en cuanto a la configuración y simulación de una red compleja y eficiente para el "Campus Universitario". Sin embargo, siempre hay espacio para mejoras y actualizaciones que puedan seguir optimizando el rendimiento, la seguridad y la gestión de la red en el futuro. Este proyecto nos ha proporcionado una base sólida sobre la cual construir y mejorar continuamente.