EVALUACIÓN – PRUEBA DE HABILIDADES PRÁCTICAS CCNA

ELABORADO POR:

JONATHAN DURAN RINCÓN

GRUPO: 10

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD

PROGRAMA DE INGENIERÍA ELECTRONICA

DIPLOMADO DE PROFUNDIZACIÓN CISCO

2019

TABLA CONTENIDO

LISTA DE FIGURAS

1. RESUMEN

La Universidad Abierta y a Distancia (UNAD), a través de su Diplomado de Profundización CISCO CCNA, permite a los estudiantes generar bases en fundamentos en redes a partir de sus dos módulos, Network Fundamentals (CCNA1 R&S) y Routing and Switching Fundamentals (CCNA2 R&S), a partir de la incursión en la plataforma de CISCO vinculada al diplomado; en donde los estudiantes aprenderán a crear una red empresarial eficaz y escalable; así como a instalar, configurar, supervisar, y solucionar problemas en los equipos pertenecientes a la infraestructura de una red.. A su vez mediante las cuatro unidades establecidas en el entorno del curso se fortalecen dichos conceptos de la siguiente forma jerarquica: Unidad 1 se apropiarán algunos conceptos relacionados con la configuración de sistemas operativos de red, protocolos de comunicación, mecanismos de acceso al medio y características de la capa de red. Unidad 2 se abordarán las temáticas relacionadas con la capa de transporte, asignación de direcciones IP, subnetting y capa de aplicación. En Unidad 3 se presenta la forma adecuada de diseñar y configurar soluciones soportadas en el uso de dispositivos de conmutación acorde con las topologías de red requeridas bajo el uso de protocolos basados en STP y VLANs bajo una arquitectura jerárquica. Unidad 4 se presentan temáticas relacionadas con el enrutamiento estático, enrutamiento dinámico, enrutamiento mediante protocolos de estado enlace, listas de acceso, asignación dinámica de direcciones IP y traducciones de direcciones IP mediante NAT.

2. ABSTRAC

The Open and Distance University (UNAD), through its CISCO CCNA Deepening Diploma, allows students to generate bases in networks based on its two modules, Network Fundamentals (CCNA1 R&S) and Routing and Switching Fundamentals (CCNA2 R&S), from the incursion into the CISCO platform linked to the diploma; where students will learn to create an effective and scalable business network; as well as to install, configure, supervise, and solve problems in the equipment belonging to the infrastructure of a network. In turn, through the four units established in the course environment, these concepts are strengthened in the following hierarchical way: Unit 1 is they will appropriate some concepts related to the configuration of network operating systems, communication protocols, media access mechanisms and characteristics of the network layer. Unit 2 will address the issues related to the transport layer, IP address assignment, subnetting and application layer. Unit 3 presents the appropriate way to design and configure supported solutions in the use of switching devices according to the network topologies required under the use of protocols based on STP and VLANs under a hierarchical architecture. Unit 4 presents topics related to static routing, dynamic routing, routing using link status protocols, access lists, dynamic assignment of IP addresses and translations of IP addresses using NAT.

3. INTRODUCCIÓN

Basándose en los avances tecnológico del presente, las medianas y grandes empresas han hecho uso de arquitecturas que permitan establecer y generar intercomunicación agiles y estables las cuales permiten el manejo de la información de manera práctica, segura y sencilla. Para permitir esto se ha establecido mediante las telecomunicaciones dispositivos que permiten establecer redes que pueden conectar múltiples puntos de trabajo; los cuales patentados por empresas de esta rama presentan una serie de configuraciones esenciales que se pueden ajustar a cada requerimiento.

Dentro de estas empresas se destaca Cisco quien, para garantizar un óptimo funcionamiento, generan certificaciones que son reconocidas a nivel mundial como un estándar de la industria para diseño y soporte de redes, garantizando altos niveles de conocimientos y confiabilidad. Su línea de cursos va desde la tecnología más básica de redes hasta áreas especializadas y tecnología avanzada tales como seguridad, redes inalámbricas y telefonía IP. Con estas certificaciones se validan los conocimientos y habilidades, proporcionando pruebas reales de logros profesionales incrementando las oportunidades de desarrollo y ascenso en la vida profesional.

4. OBJETIVOS

- Describir el propósito, la naturaleza y las operaciones del Protocolo Open Shortest Path First (OSPF).
- Configurar y verificar operaciones básicas de RIPv1, RIPv2, OSPF de área única y EIGRP en una red enrutada pequeña.
- Describir las características y funciones principales del Protocolo Enhanced EIGRP.
- Describir el propósito, la naturaleza y las funciones de un router.
- Explicar el rol crítico que cumple el router para permitir la comunicación a través de varias redes.
- Usar modelos de protocolos de red para explicar las capas de comunicaciones en las redes de datos.

5. DESARROLLO PRACTICA

5.1. Escenario 1

Una empresa posee sucursales distribuidas en las ciudades de Bogotá, Medellín y Cali en donde el estudiante será el administrador de la red, el cual deberá configurar e interconectar entre sí cada uno de los dispositivos que forman parte del escenario, acorde con los lineamientos establecidos para el direccionamiento IP, protocolos de enrutamiento y demás aspectos que forman parte de la topología de red.

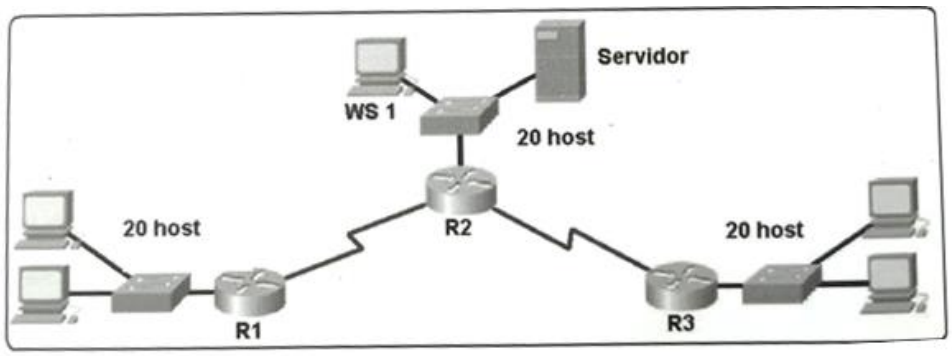


Ilustración 1. Topología Escenario 1

5.1.1. Diseño de Red Packet Tracer

A continuación, se relaciona red realizada en software Packet Tracer referente a escenario1.

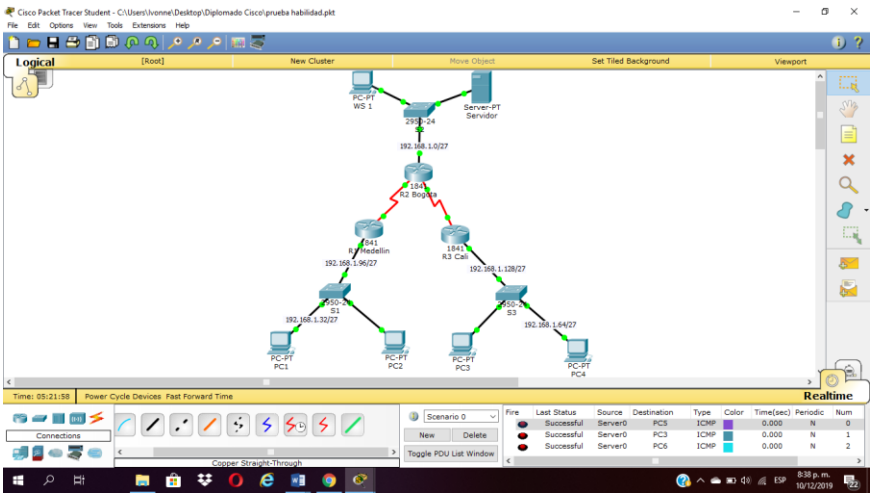


Ilustración 2. Red Packet Tracer

5.1.2. Configuración de hostname y password en routers

Se realiza respectiva configuración de hostname y password para ingresos en modo enable, consola y telnet en cada uno de los routers de la topología. A continuación, se vincula el código fuente con el que se realizó este procedimiento.

R1

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R1
R1(config)#
R1(config)#enable secret class
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#line vty 0 4
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
```

R2

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R2
R2(config)#
R2(config)#enable secret class
R2(config)#line console 0
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#exit
R2(config)#line vty 0 4
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#exit
```

R3

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R3
R3(config)#
R3(config)#enable secret class
R3(config)#line console 0
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#exit
R3(config)#line vty 0 4
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#exit
```

5.1.3. Configuración de hostname y password en Switch

Se realiza respectiva configuración de hostname y password para ingresos en modo enable, consola y telnet en cada uno de los Switch de la topología. A continuación, se vincula el código fuente con el que se realizó este procedimiento.

S1

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#
S1(config)#enable secret class
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#exit
S1(config)#line vty 0 4
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#exit
```

S2

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S2
S2(config)#
S2(config)#enable secret class
S2(config)#line console 0
S2(config-line)#password cisco
S2(config-line)#login
S2(config-line)#exit
S2(config)#line vty 0 4
S2(config-line)#password cisco
S2(config-line)#login
S2(config-line)#exit
```

S3

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S3
S3(config)#
S3(config)#enable secret class
S3(config)#line console 0
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#exit
S3(config)#line vty 0 4
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#exit
```

5.1.4. Configuración banner en cada Router:

Se configura mediante comando “banner” mensaje de inicio al ingresar a modo consola en cada uno de los routers.

R1

User Access Verification

Password:

R1>enable
Password:
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#banner motd #Prueba Habilidades CCNA-UNAD#
R1(config)#
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console
R1#exit
R1 con0 is now available
Press RETURN to get started.
Prueba Habilidades CCNA-UNAD
User Access Verification
Password:

R2

User Access Verification

Password:

R2>enable
Password:
R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#banner motd #Prueba Habilidades CCNA-UNAD#
R2(config)#
R2(config)#exit
R2#
%SYS-5-CONFIG_I: Configured from console by console
R2#exit
R2 con0 is now available
Press RETURN to get started.
Prueba Habilidades CCNA-UNAD
User Access Verification
Password

R3

User Access Verification

Password:

R3>enable
Password:
R3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#banner motd #Prueba Habilidades CCNA-UNAD#
R3(config)#
R3(config)#exit
R3#
%SYS-5-CONFIG_I: Configured from console by console
R3#exit
R3 con0 is now available
Press RETURN to get started.
Prueba Habilidades CCNA-UNAD
User Access Verification
Password

5.1.5. Creación de Subnetting

Se valida la creación de subredes para permitir una segmentación de 8 partes que permitan facilitar la asignación de ip´s a equipos en un crecimiento futuro.

Se relaciona tabla de asignación a continuación:

TABLA SUBNETTING RED				
Subnet	**Dirección**	**Mascara**	**Host**	**Broadcats**
1	192.168.1.0 /27	255.255.255.224	192.168.1.1 /30	192.168.1.31
2	192.168.1.32 /27	255.255.255.224	192.168.1.33 /62	192.168.1.63
3	192.168.1.64 /27	255.255.255.224	192.168.1.65 /94	192.168.1.95
4	192.168.1.96 /27	255.255.255.224	192.168.1.97 /126	192.168.1.127
5	192.168.1.128 /27	255.255.255.224	192.168.1.129/158	192.168.1.159
6	192.168.1.160 /27	255.255.255.224	192.168.1.161/190	192.168.1.191
7	192.168.1.192 /27	255.255.255.224	192.168.1.193/222	192.168.1.223
8	192.168.1.224 /27	255.255.255.224	192.168.1.225/254	192.168.1.255

5.1.6. Asignación de direccionamiento IP

Se vincula tabal donde se completa direccionamiento ip en interfaz serial 1/0 en R1 y R3 según subnetting.

	R1	R2	R3
Nombre de Host	**MEDELLIN**	**BOGOTA**	**CALI**
Dirección de Ip en interfaz Serial 0/0	192.168.1.99	192.168.1.98	192.168.1.131
Dirección de Ip en interfaz Serial 0/1	192.168.1.162	192.168.1.130	192.168.1.194
Dirección de Ip en interfaz FA 0/0	192.168.1.33	192.168.1.1	192.168.1.65
Protocolo de enrutamiento	EIGRP	EIGRP	EIGRP
Sistema Autónomo	200	200	200
Afirmaciones de red	192.168.1.0	192.168.1.0	192.168.1.0

5.1.7. Configuración Puerto serial Routers

Se realiza configuración en router R1, R2 y R3 en puertos serial 0/0 y 0/1

R1

```
R1>enable
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#interface serial 0/0/0
R1(config-if)#ip address 192.168.1.99 255.255.255.224
R1(config-if)#no shutdown
```

```
R1>enable
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#interface serial 0/0/1
R1(config-if)#ip address 192.168.1.162 255.255.255.224
R1(config-if)#no shutdown
```

R2

```
R2>enable
R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#interface serial 0/0/0
R2(config-if)#ip address 192.168.1.98 255.255.255.224
R2(config-if)#no shutdown
```

```
R2>enable
R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#interface serial 0/0/1
R2(config-if)#ip address 192.168.1.130 255.255.255.224
R2(config-if)#no shutdown
```

R3

```
R3>enable
R3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#interface serial 0/0/0
R3(config-if)#ip address 192.168.1.131 255.255.255.224
R3(config-if)#no shutdown
```

```
R3>enable
R3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#interface serial 0/0/1
R3(config-if)#ip address 192.168.1.194 255.255.255.224
R3(config-if)#no shutdown
```

5.1.8. Configuración puertos FastEthernet Routers

Se realiza configuración en router R1, R2 y R3 en puertos fastethernet 0/0

R1

```
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#interface fastEthernet 0/0
R1(config-if)#ip address 192.168.1.33 255.255.255.224
R1(config-if)#no shutdown
```

R2

```
R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#interface fastethernet 0/0
R2(config-if)#ip address 192.168.1.1 255.255.255.240
R2(config-if)#no shutdown
R2(config-if)#exit
```

R3

```
R3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#interface fastethernet 0/0
R3(config-if)#ip address 192.168.1.65 255.255.255.224
R3(config-if)#no shutdown
R3(config-if)#exit
```

5.1.9. Asignación parámetro de red a periféricos

A continuación, se relacionan imágenes de configuración de red a periféricos de salida tales como servidores y laptops

WS1:

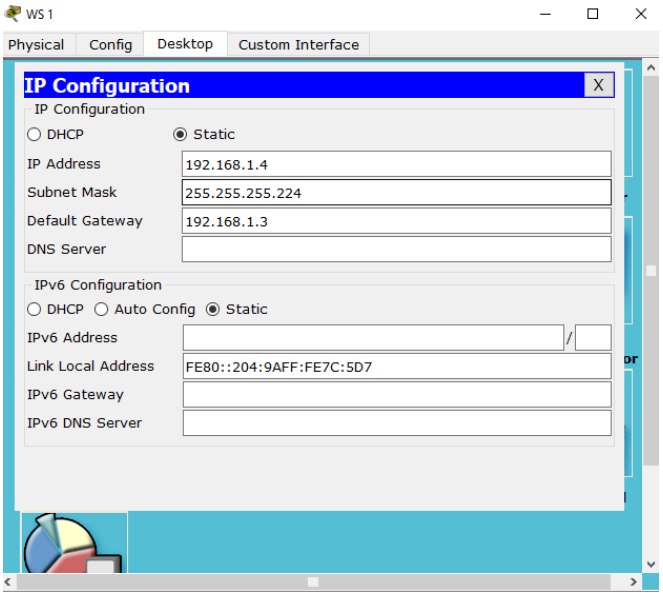


Ilustración 3. Configuración red WS1

Servidor

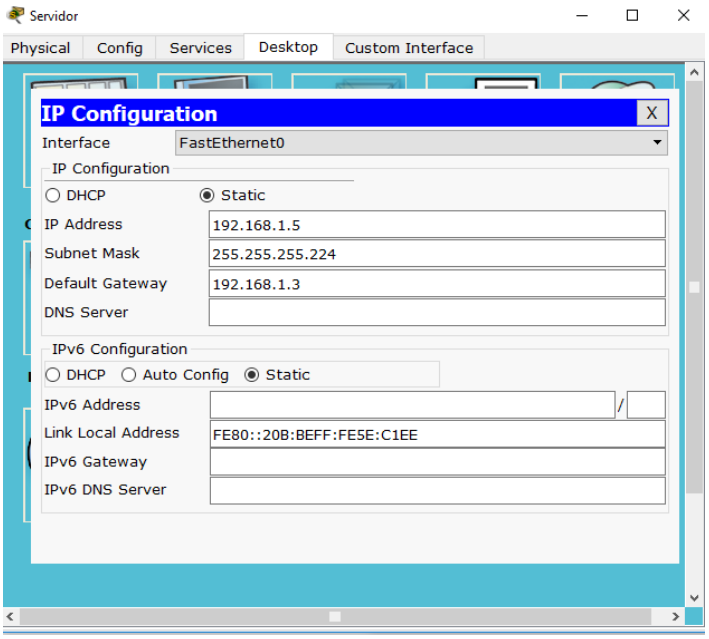


Ilustración 4. Configuración red Servidor

PC1

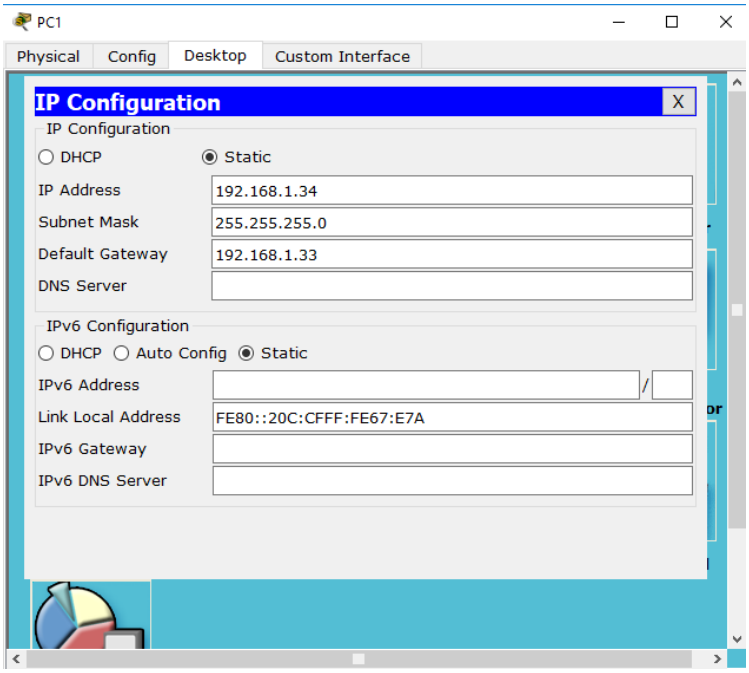


Ilustración 5. Configuración red PC1

PC2

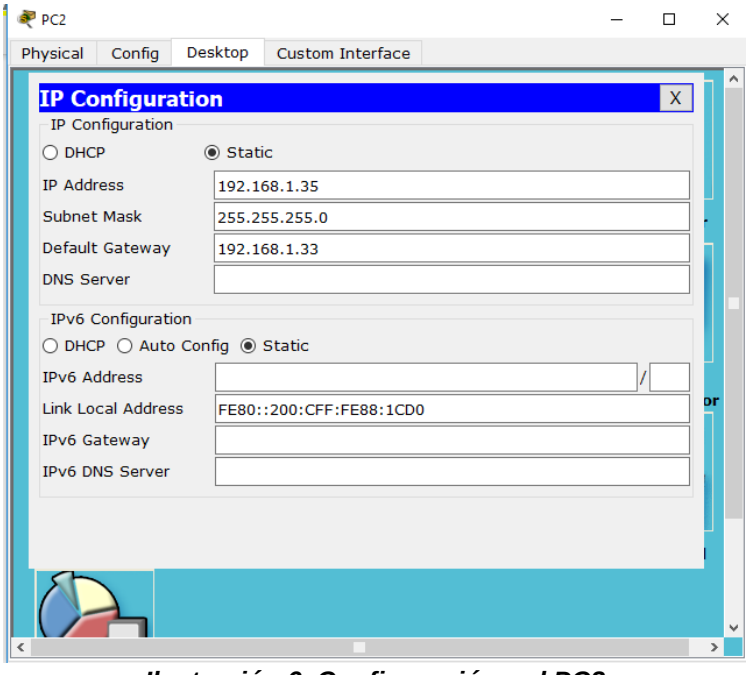


Ilustración 6. Configuración red PC2

PC3

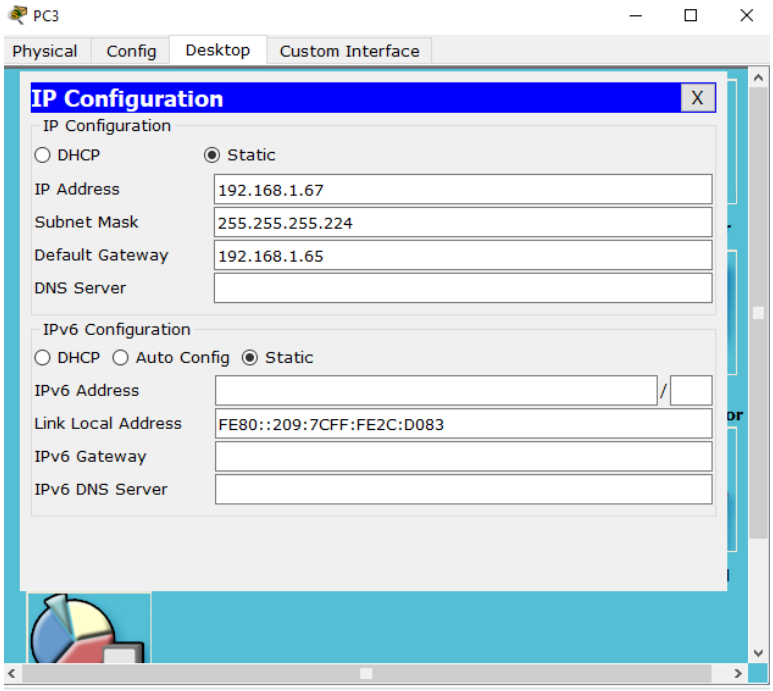


Ilustración 7. Configuración red PC3

PC4

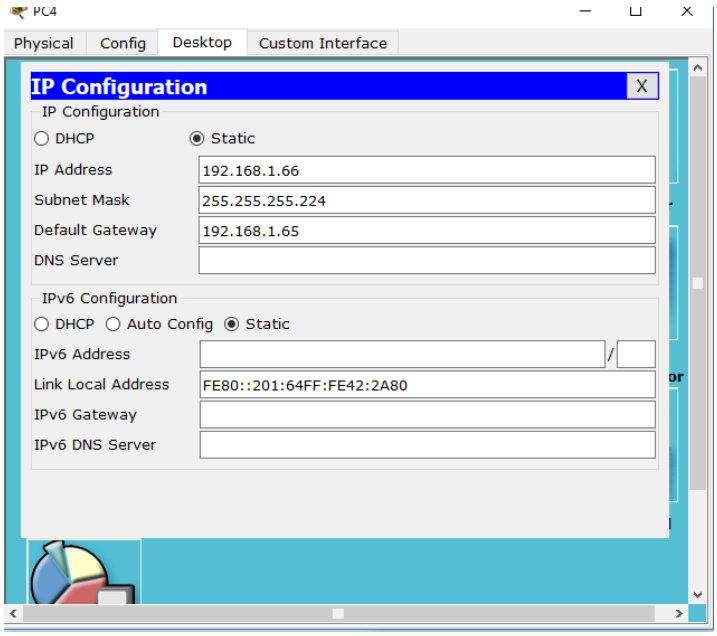


Ilustración 8. Configuración red PC4.

5.1.10. Verificación enrutamiento routers

Se procede a validar tabla de enrutamiento de routers R1, R2 y R3 a partir del comando "***show ip router"***

R1

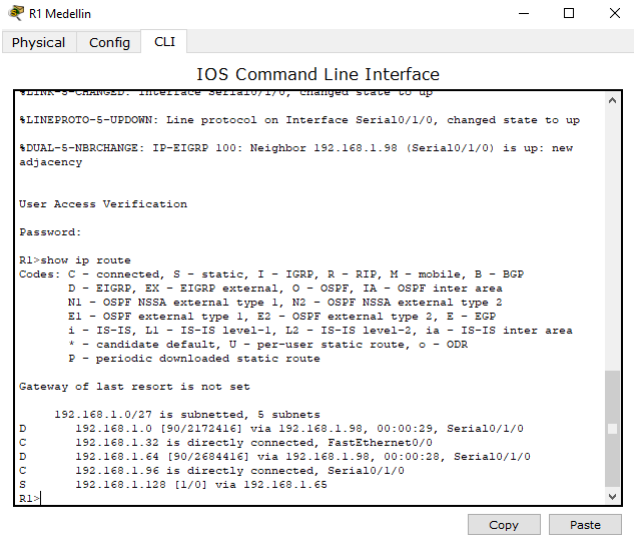


Ilustración 9. Enrutamiento R1

R2

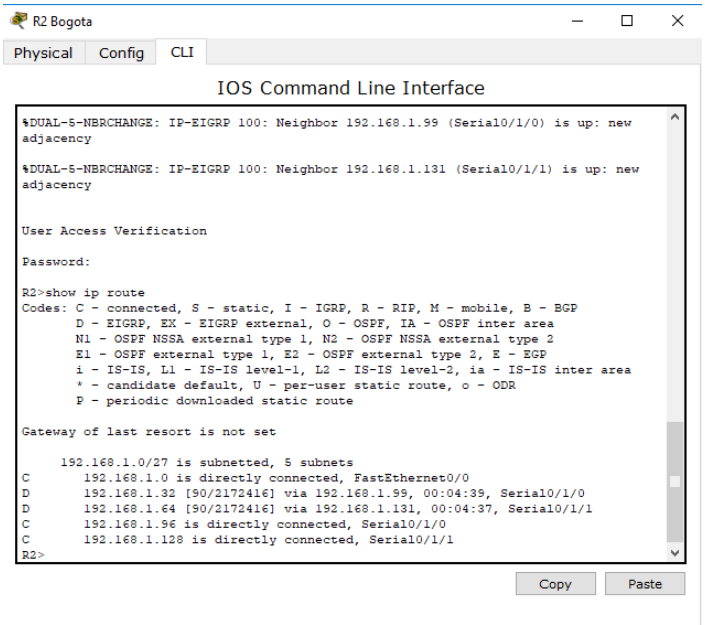


Ilustración 10. Enrutamiento R2

R3

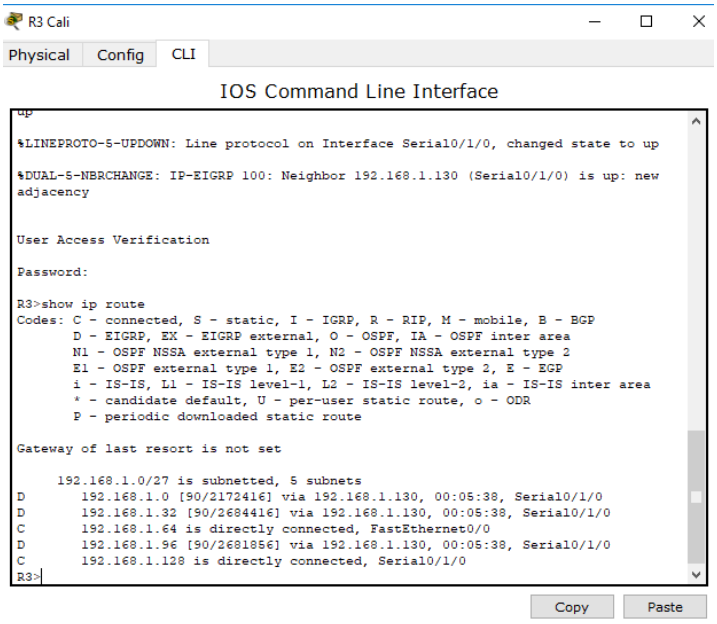


Ilustración 11. Enrutamiento R3

5.1.11. Diagnostico vecindad Routers

Mediante el comando "***show cdp neigborn"*** se puede validar información relacionada a conexiones locales de este equipo.

A continuación, se anexa código fuente de ejecución y tabla vinculada a esta vista.

R1

User Access Verification
Password:
R1>enable
Password:
R1#sh cdp nei

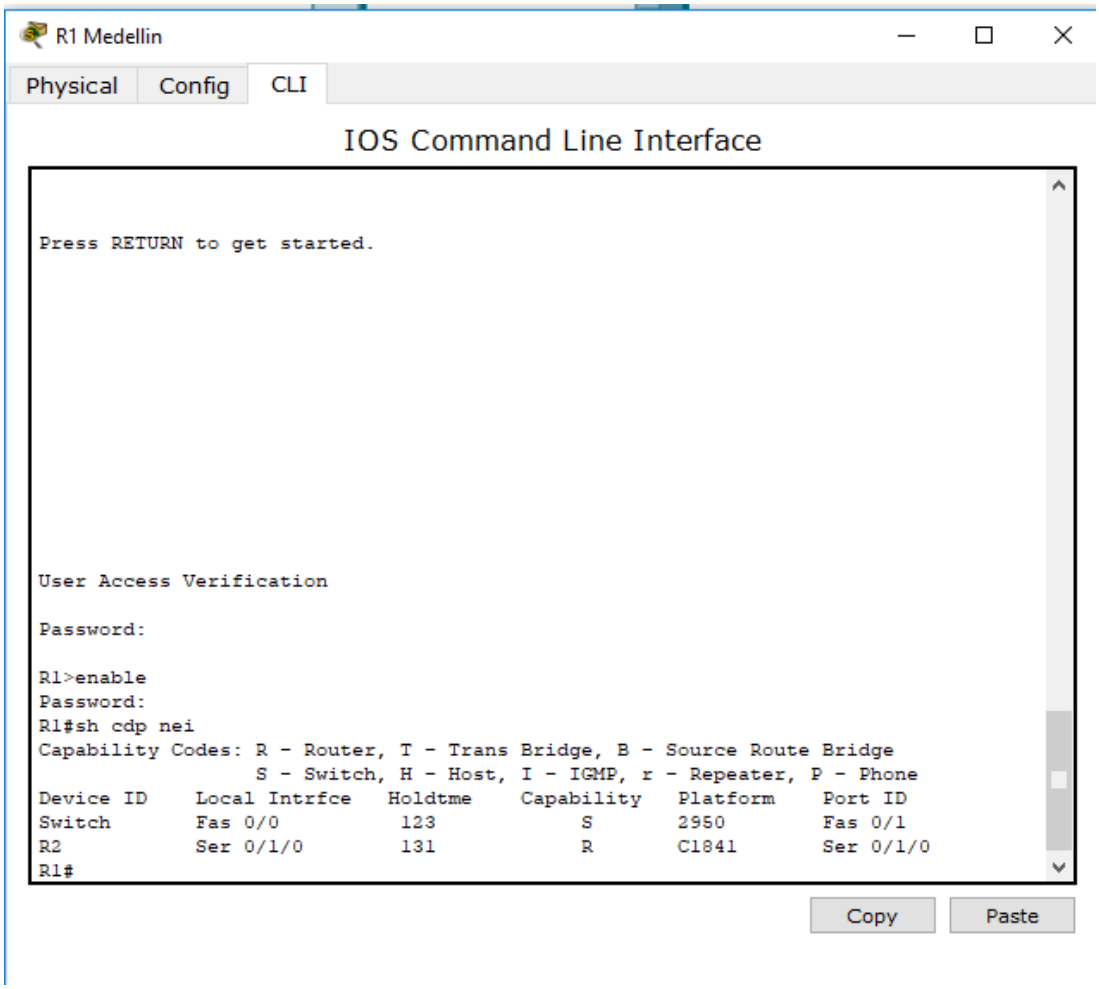


Ilustración 12. Vecindad R1

R2

User Access Verification
Password:
R2>enable
Password:
R2#sh cdp nei

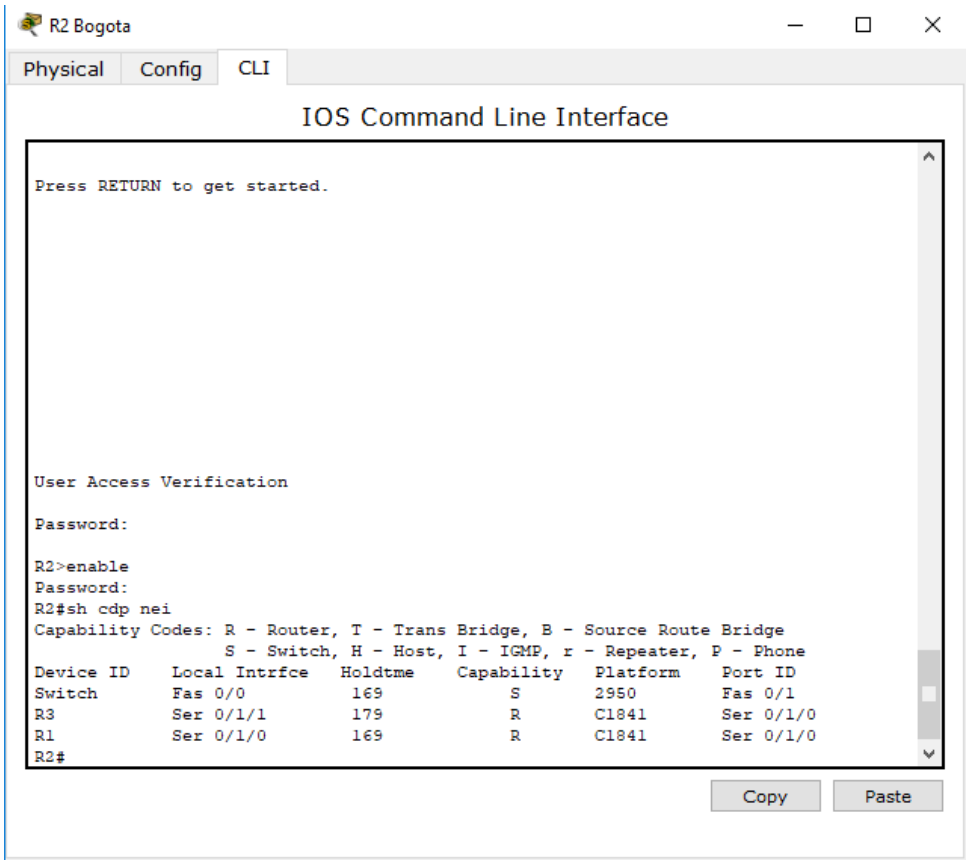


Ilustración 13. Vecindad R2

R3

User Access Verification
Password:
R3>enable
Password:
R3#sh cdp nei

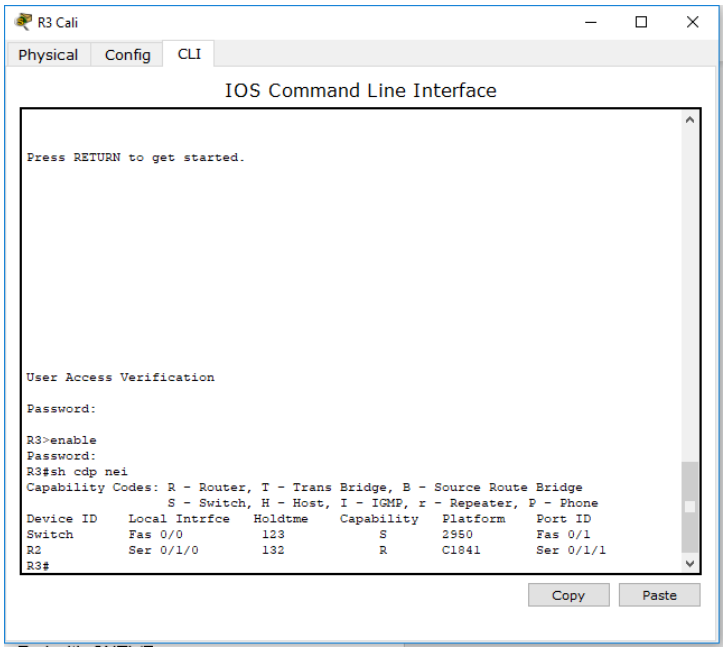


Ilustración 14. Vecindad R3

Reloj

R1>enable
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#interface serial 0/1/0
R1(config-if)#clock rate 64000

R2>enable
R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#interface serial 0/1/1
R2(config-if)#clock rate

5.1.12. EIGRP routers con Wirdcard

Por medio del enrutamiento EIGRP (Enhanced Interior Gateway Routing Protocol) el cual es una versión mejorada de IGRP, permite el manejo de tecnología de vector distancia para que la información de la distancia subyacente no presenta cambios.

A continuación, se relaciona código fuente donde se configura este enrutamiento en cada router de la topología.

R1

R1>enable
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#router eigrp 200

```
R1(config-router)#network 192.168.1.32 0.0.0.31
R1(config-router)#network 192.168.1.96 0.0.0.31
R1(config-router)#network 192.168.1.0 0.0.0.31
R1(config-router)#network 192.168.1.128 0.0.0.31
R1(config-router)#network 192.168.1.64 0.0.0.31
R1(config-router)#exit
R1(config)#
```

R2

```
R2>enable
R2#
R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#router eigrp 200
R2(config-router)#network 192.168.1.32 0.0.0.31
R2(config-router)#network 192.168.1.96 0.0.0.31
R2(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 100: Neighbor 192.168.1.99 (Serial0/1/0) is up: new adjacency
R2(config-router)#network 192.168.1.0 0.0.0.31
R2(config-router)#network 192.168.1.1 0.0.0.31
R2(config-router)#network 192.168.1.64 0.0.0.31
R2(config-router)#exit
```

R3

```
R3>enable
R3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#router eigrp 200
R3(config-router)#network 192.168.1.32 0.0.0.31
R3(config-router)#network 192.168.1.96 0.0.0.31
R3(config-router)#network 192.168.1.0 0.0.0.31
R3(config-router)#network 192.168.1.128 0.0.0.31
R3(config-router)#network 192.168.1.64 0.0.0.31
R3(config-router)#exit
R3(config)#
```

5.1.13. Prueba de ping entre periféricos de salida.

A partir de las configuraciones anteriores, se procede a ejecutar prueba de ping para establecer comunicación entre todos los periféricos de salida de todas las ciudades

Tabla direccionamiento IP equipos de salida				
ítem	**Equipo**	**Ip**	**Mascara**	**Puerta de enlace**
1	WS1	192.168.1.4	255.255.255.224	192.168.1.3
2	Servidor	192.168.1.5	255.255.255.224	192.168.1.3
3	PC1	192.168.1.34	255.255.255.224	192.168.1.33

4	PC2	192.168.1.35	255.255.255.224	192.168.1.33
5	PC3	192.168.1.67	255.255.255.224	192.168.1.65
6	PC4	192.168.1.66	255.255.255.224	192.168.1.65

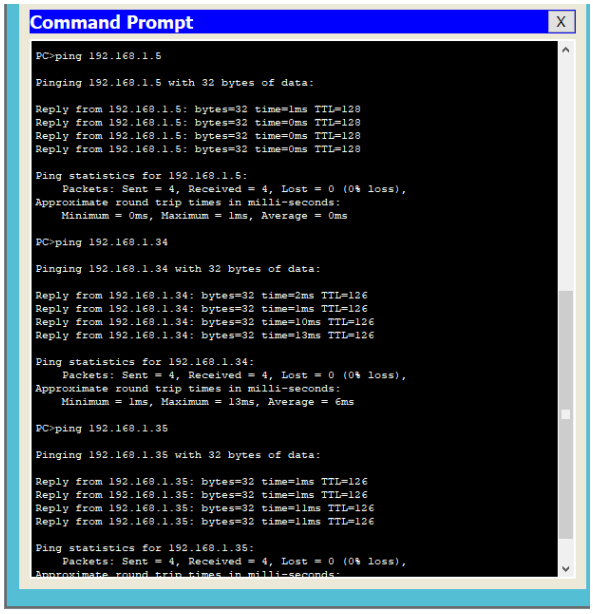


Ilustración 15. Ping WS1 a Servidor, PC1 y PC2

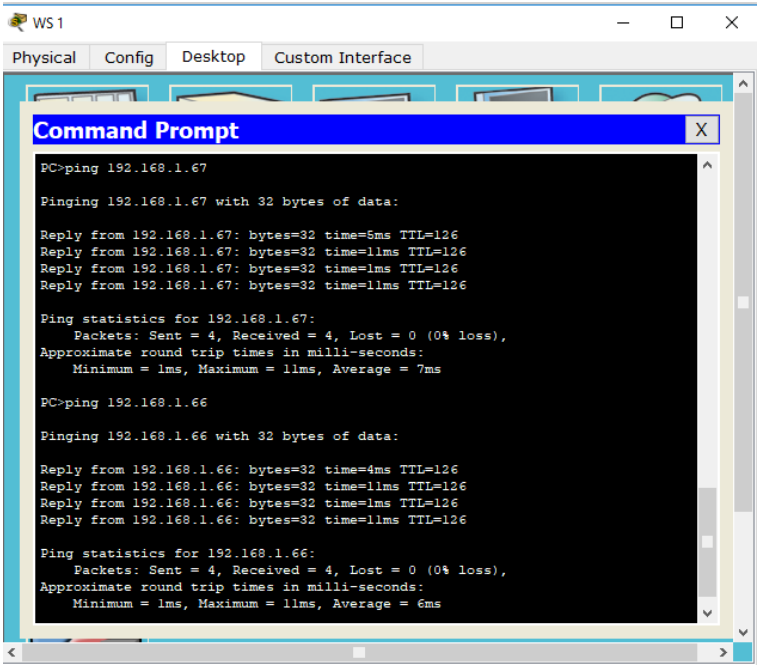


Ilustración 16. Ping WS1 a PC3 y PC4

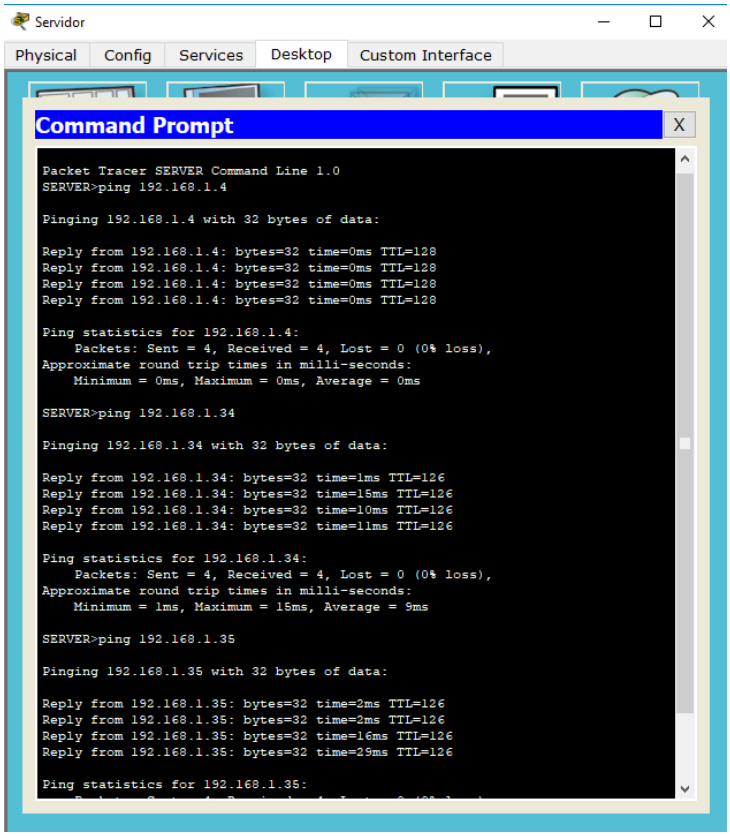


Ilustración 17. Ping Servidor a WS1, Pc1 y PC2

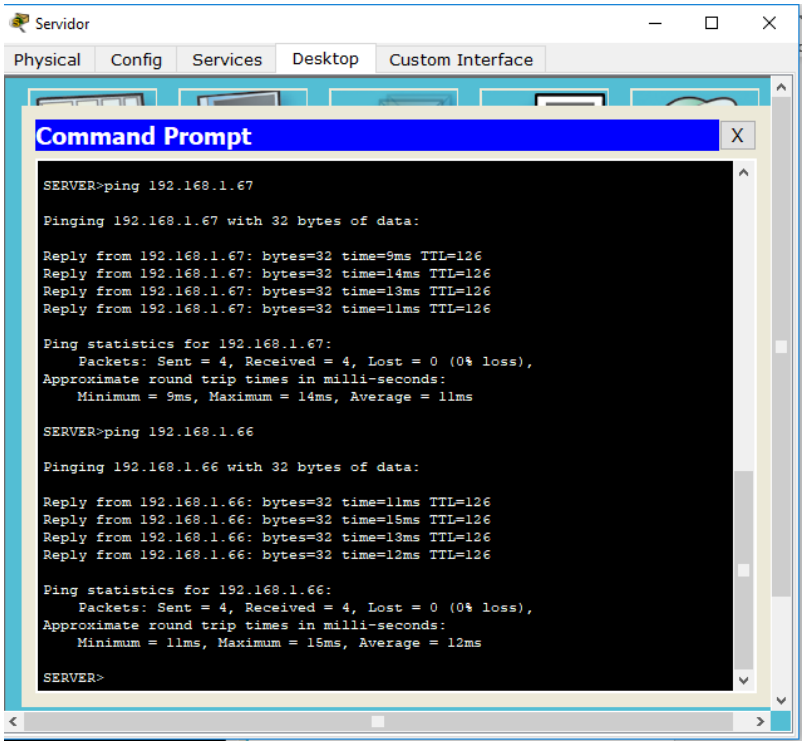


Ilustración 18. Ping Servidor a PC3 y PC4

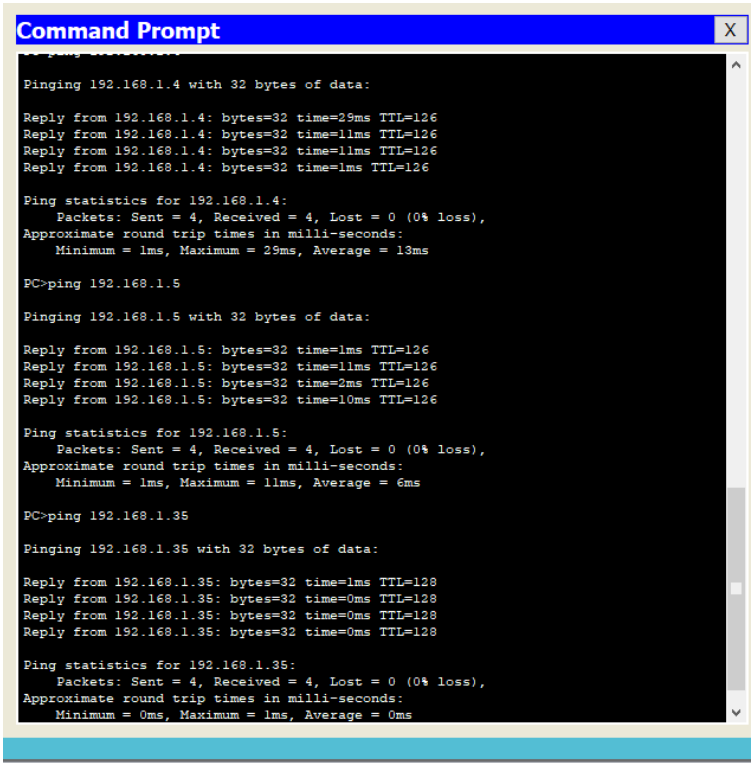


Ilustración 19. Ping PC1 a WS1, Servidor y PC2.

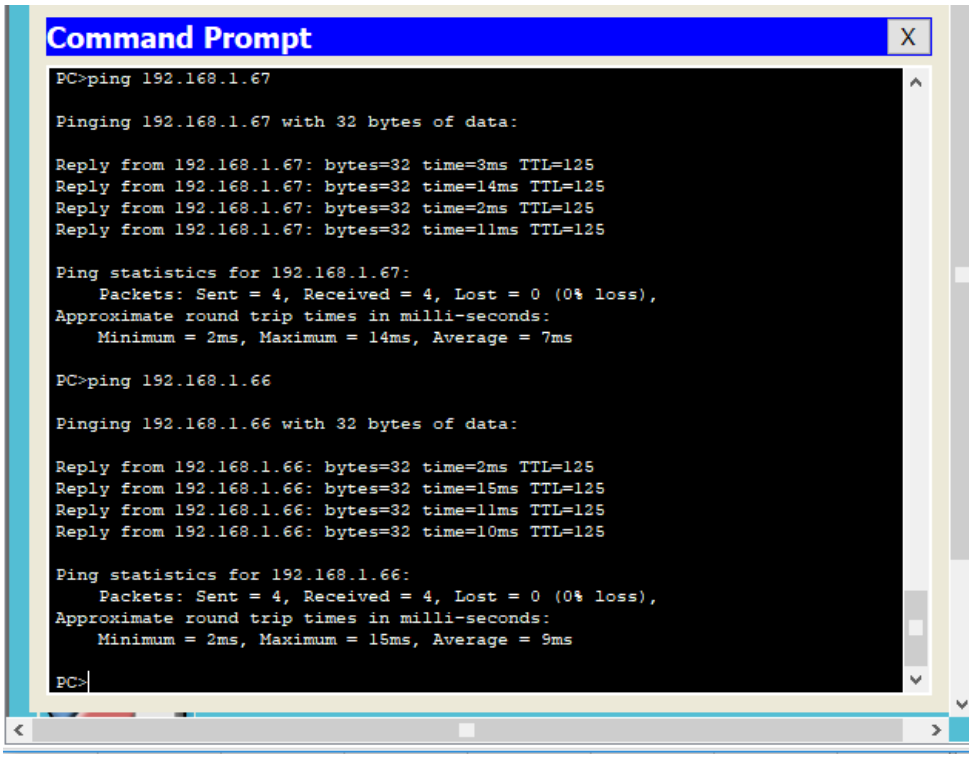


Ilustración 20. Ping PC1 a PC3 y PC4.

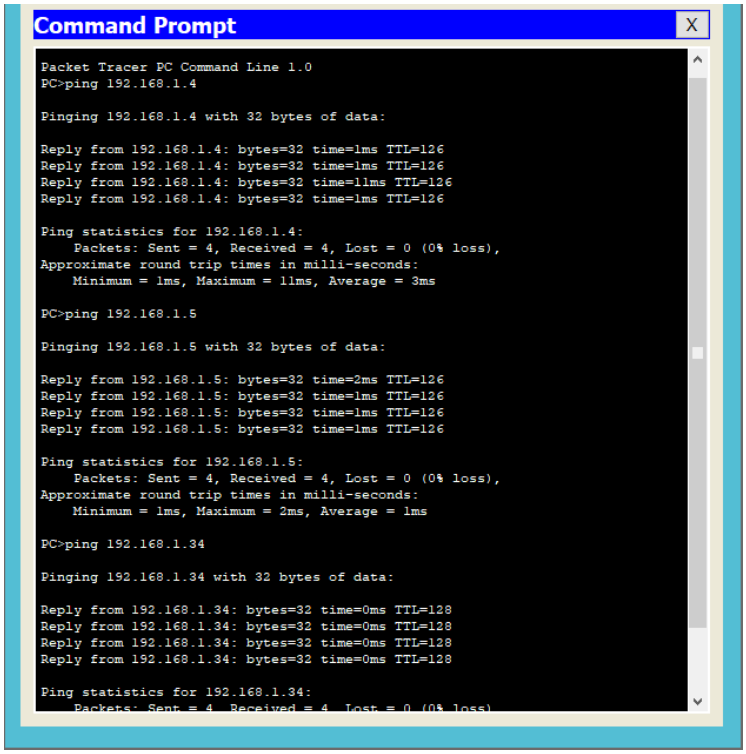


Ilustración 21. Ping PC2 a WS1, Servidor y PC1.

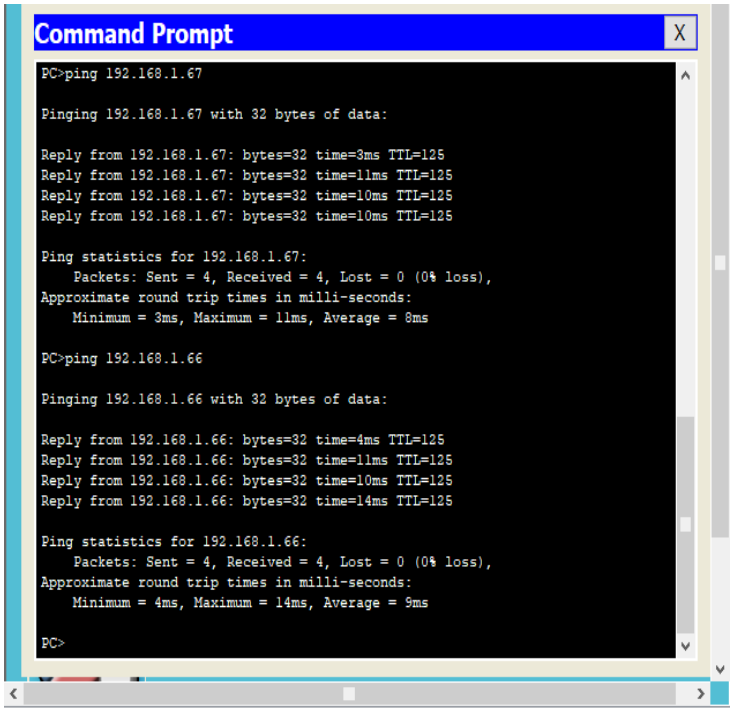


Ilustración 22. Ping PC2 a PC3 y PC4.

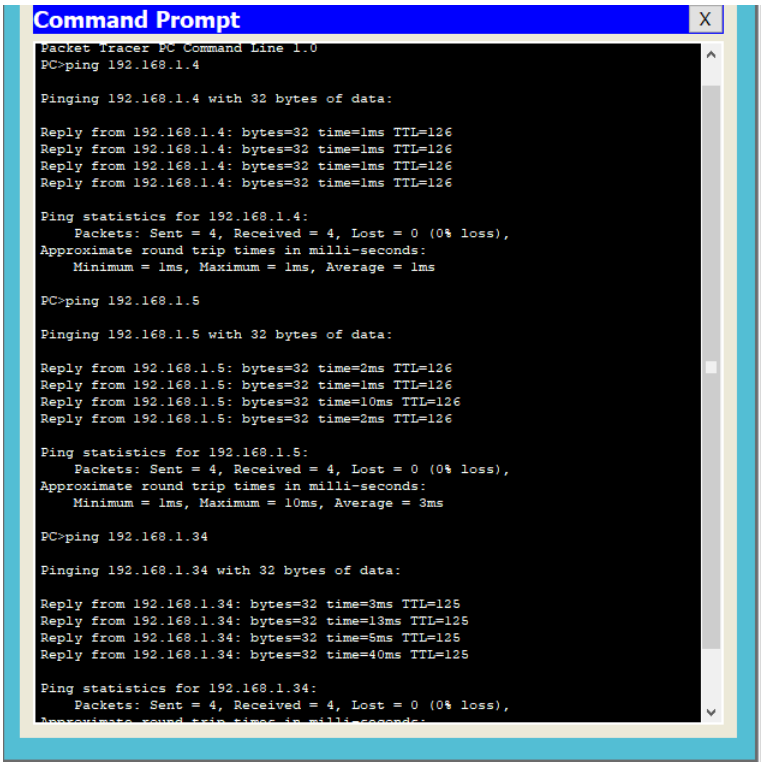


Ilustración 23. Ping PC3 a WS1, Servidor y PC1

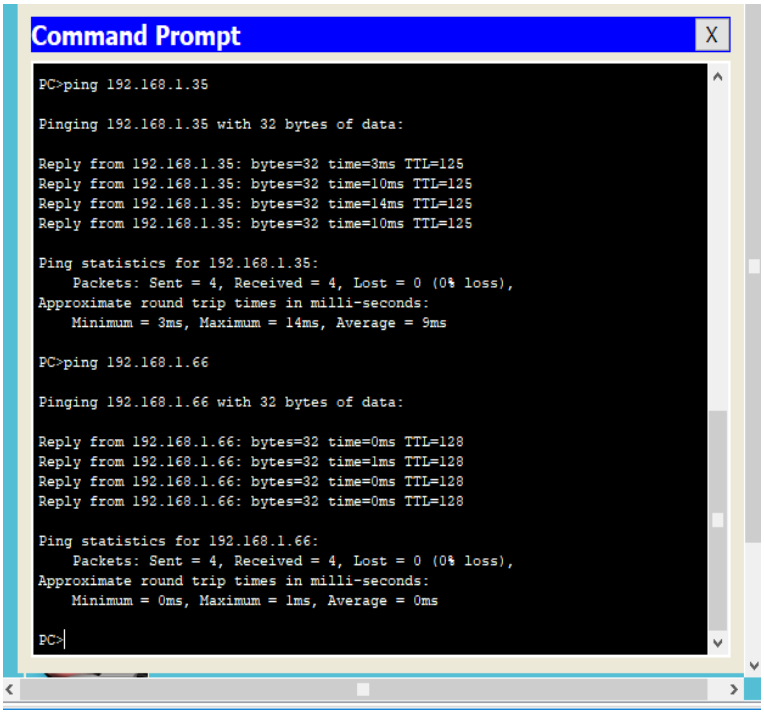


Ilustración 24. Ping PC3 a PC2 y PC4

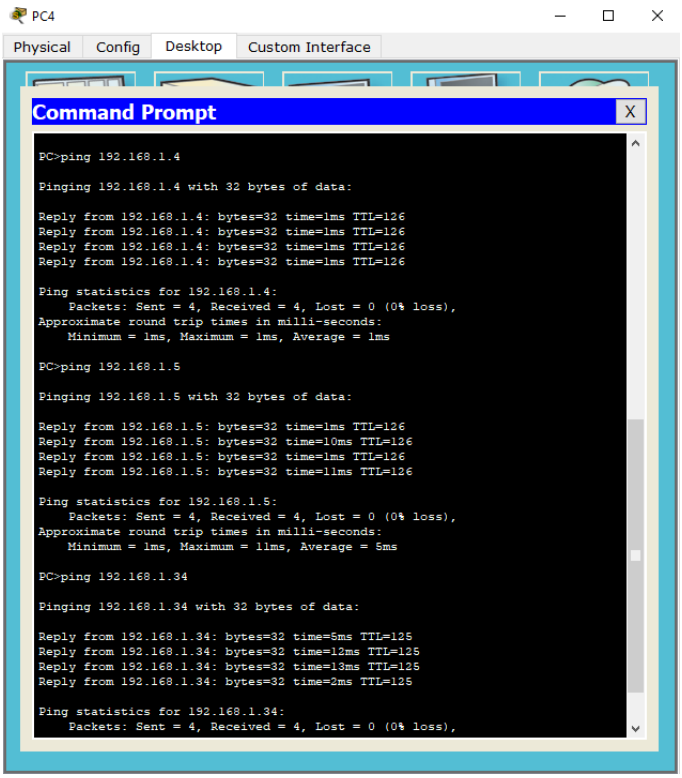


Ilustración 25. Ping PC4 a WS1, Servidor y PC1.

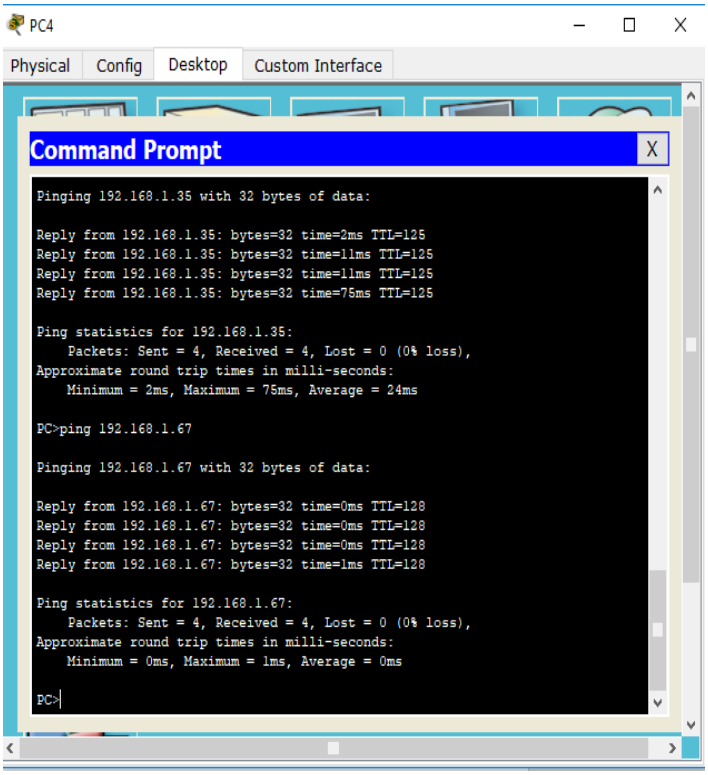


Ilustración 26. Ping PC4 a PC2 y PC3

5.1.14. Configuración control de accesos.

Teniendo en cuenta el paso 5.1.2. donde se habilito en lo routers acceso de telnet, a este acceso se le concede un nivel de privilegio de 15 y posteriormente se vincula acces- list

A continuación, se relaciona código fuente ejecutado en cada router.

R1

```
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#line vty 0 4
R1(config-line)#privilege level 15
R1(config-line)#login local
R1(config-line)#transport input telnet
R1(config-line)#exit
R1(config)#access-list 105 permit tcp host 192.168.1.99 host 192.168.1.98 eq telnet
R1(config)#access-list 105 permit tcp host 192.168.1.99 host 192.168.1.131 eq telnet
R1(config)#do wr Building configuration... [OK]
R1(config)#end
R1#%SYS-5-CONFIG_I: Configured from console by console
R1#
```

R2

```
R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#line vty 0 4
R2(config-line)#privilege level 15
R2(config-line)#login local
R2(config-line)#transport input telnet
R2(config-line)#exit
R2(config)#access-list 106 permit tcp host 192.168.1.98 host 192.168.1.131 eq telnet
R2(config)#access-list 106 permit tcp host 192.168.1.130 host 192.168.1.131 eq telnet
R2(config)#do wr Building configuration... [OK]
R2(config)#end
R2#%SYS-5-CONFIG_I: Configured from console by console
R2#
```

R3

```
R3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#line vty 0 4
R3(config-line)#privilege level 15
R3(config-line)#login local
R3(config-line)#transport input telnet CALI(config-line)#do wr
R3(config)#access-list 107 permit tcp host 192.168.1.131 host 192.168.1.99 eq telnet
R3#(config)#access-list 107 permit tcp host 192.168.1.131 host 192.168.1.98 eq telnet
R3(config)#do wr Building configuration... [OK]
```

R3(config)#end
R3#%SYS-5-CONFIG_I: Configured from console by console
R3#

5.1.15. Acceso Únicamente de servidor a cualquier equipo de la red.

R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#access-list 104 deny tcp host 192.168.1.2 host 192.168.1.66
R2(config)#access-list 104 deny tcp host 192.168.1.2 host 192.168.1.67
R2(config)#access-list 104 permit tcp host 192.168.1.3 host 192.168.1.66
R2(config)#access-list 104 permit tcp host 192.168.1.3 host 192.168.1.67 R2(config)#interface se0/0/0
R2(config-if)#ip access-group 104 out
R2(config-if)#interface se0/0/1
R2(config-if)#ip access-group 104 out
R2(config-if)#
R2(config-if)#do wr Building configuration... [OK]
R2(config-if)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console

5.1.16. Restricción total de LAN Medellin y Cali

R1

R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#access-list 101 permit tcp host 192.168.1.34 host 192.168.1.3 eq www
R1(config)#access-list 101 permit tcp host 192.168.1.36 host 192.168.1.3 eq www
R1(config)#access-list 101 permit icmp host 192.168.1.34 host 192.168.1.3
R1(config)#access-list 101 permit icmp host 192.168.1.36 host 192.168.1.3 R1(config)#access-list 101 deny tcp any any
R1(config)#interface serial 0/0/0
R1(config-if)#ip access-group 101 out
R1(config-if)#do wr
Building configuration... [OK]
R1(config-if)#end
R1#

R2

R3 CALI# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#access-list 103 permit tcp host 192.168.1.66 host 192.168.1.3
R3(config-if)#access-list 103 permit tcp host 192.168.1.67 host 192.168.1.3
R3(config)#access-list 103 permit icmp host 192.168.1.66 host 192.168.1.3

R3(config)#access-list 103 permit icmp host 192.168.1.67 host 192.168.1.3 R3(config)#access-list 103 deny tcp any an
R3(config)#interface serial0/0/0

R3(config-if)#ip access-group 103 out	**ORIGEN**	**DESTINO**	**RESULTADO**
TELNET	Router MEDELLIN	Router CALI	Sin acceso
	WS_1	Router BOGOTA	Con acceso
	Servidor	Router CALI	Con acceso
	Servidor	Router MEDELLIN	Con acceso
TELNET	LAN del Router MEDELLIN	Router CALI	Sin acceso
	LAN del Router CALI	Router CALI	Con acceso
	LAN del Router MEDELLIN	Router MEDELLIN	Con acceso
	LAN del Router CALI	Router MEDELLIN	Sin acceso
PING	LAN del Router CALI	WS_1	Sin respuesta
	LAN del Router MEDELLIN	WS_1	Sin respuesta
	LAN del Router MEDELLIN	LAN del Router CALI	Sin respuesta
PING	LAN del Router CALI	Servidor	Con respuesta
	LAN del Router MEDELLIN	Servidor	Con respuesta
	Servidor	LAN del Router MEDELLIN	Con respuesta
	Servidor	LAN del Router CALI	Con respuesta
	Router CALI	LAN del Router MEDELLIN	Sin respuesta
	Router MEDELLIN	LAN del Router CALI	Sin respuesta

5.2. Escenario 2

Una empresa tiene la conexión a internet en una red Ethernet, lo cual deben adaptarlo para facilitar que sus routers y las redes que incluyen puedan, por esa vía, conectarse a internet, pero empleando las direcciones de la red LAN original.

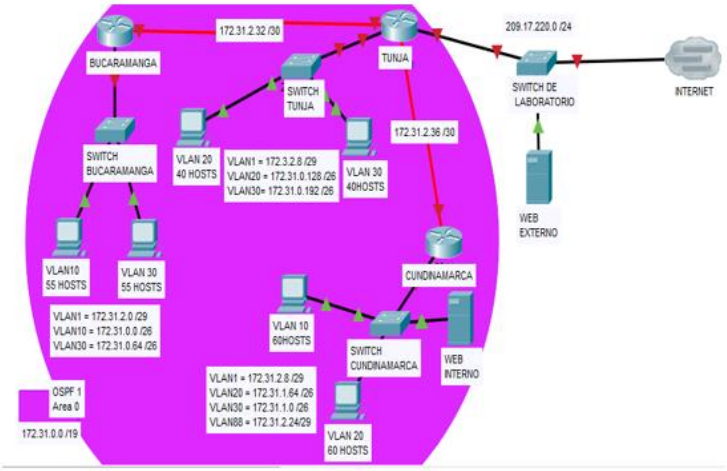


Ilustración 27. Topología Escenario 2

5.2.1. Diseño de Red Packet Tracer

A continuación, se relaciona red realizada en software Packet Tracer referente a escenario 2.

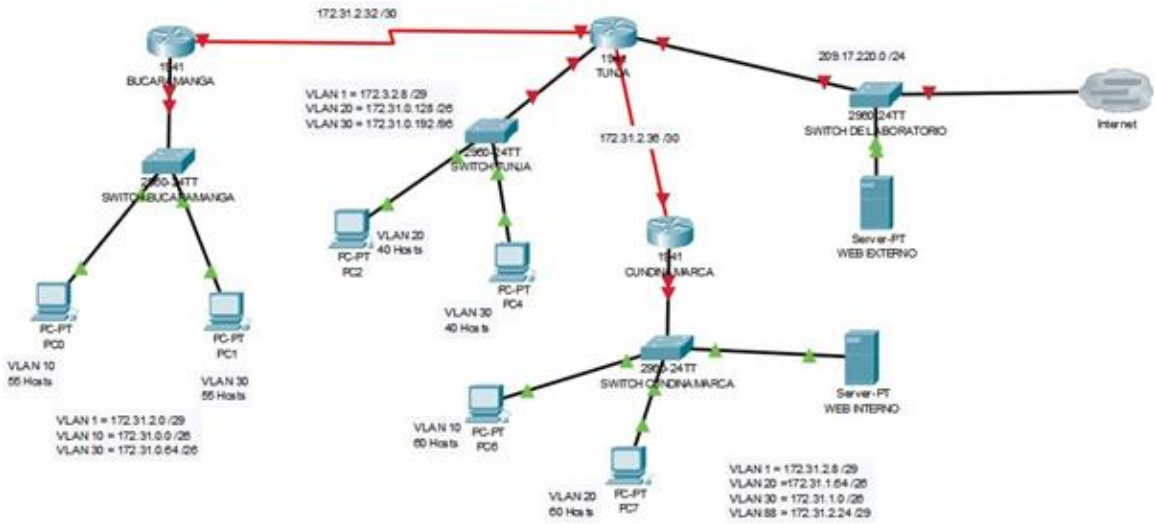


Ilustración 28. Diseño red Packet Tracer

5.2.2. Configuración de hostname en routers

Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R-R-Bucaramanga
R-R-Bucaramanga (config)#exit

Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R-R-Tunja
R-R-Tunja(config)#exit

Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R-Cundinamarca
R-Cundinamarca (config-)#exit

5.2.3. Ip Serial Routers
R-Bucaramanga (0/1/0)

R-Bucaramanga#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R-Bucaramanga(config)#interface serial 0/1/0
R-Bucaramanga(config-if)#ip address 172.31.2.34 255.255.255.252
R-Bucaramanga(config-if)#no shutdown

R-Tunja (0/1/0)

R-Tunjar#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R-Tunja(config)#interface serial 0/1/0
R-Tunja(config-if)#ip address 172.31.2.34 255.255.255.252
R-Tunja(config-if)#no shutdown

R-Tunja (0/1/1)

R-Tunja(config)#interface serial 0/1/1
R-Tunja(config-if)#ip address 172.31.2.37 255.255.255.252
R-Tunja(config-if)#no shutdown

Cundinamarca (0/1/0)

R-Cundinamarca>enable
R-Cundinamarca#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R-Cundinamarca(config)#interface serial 0/1/0
R-Cundinamarca(config-if)#ip address 172.31.2.38 255.255.255.252
R-Cundinamarca(config-if)#no shutdown

5.2.4. AAA (Authentication, Authorization y Acconting)

R-Cundinamarca

```
R-Cundinamarca>enable
R-Cundinamarca #configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R-Cundinamarca (config)#username admin secret 1234
R-Cundinamarca (config)#aaa new-mode
R-Cundinamarca (config)#aaa authentication login default local
R-Cundinamarca (config)#
R-Cundinamarca (config)#line console 0
R-Cundinamarca (config-line)#login authentication default
R-Cundinamarca (config-line)#exit
R-Cundinamarca (config)#aaa authentication login telnet-login local
R-Cundinamarca (config)#line console 0
R-Cundinamarca (config-line)#login authentication default
R-Cundinamarca (config-line)#exit
R-Cundinamarca (config)#line vty 0 4
R-Cundinamarca (config-line)#login authentication telnet-login
R-Cundinamarca (config-line)#exit
R-Cundinamarca (config)#do wr
Building configuration...
[OK]
R-Cundinamarca (config)#
```

R-Bucaramanga

```
R-Bucaramanga>enable
R-Bucaramanga#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R-Bucaramanga(config)#username admin secret 1234
R-Bucaramanga(config)#aaa new-mode
R-Bucaramanga(config)#aaa authentication login default local
R-Bucaramanga(config)#
R-Bucaramanga(config)#line console 0
R-Bucaramanga(config-line)#login authentication default
R-Bucaramanga(config-line)#exit
R-Bucaramanga(config)#aaa authentication login telnet-login local
R-Bucaramanga(config)#line console 0
R-Bucaramanga(config-line)#login authentication default
R-Bucaramanga(config-line)#exit
R-Bucaramanga(config)#line vty 0 4
R-Bucaramanga(config-line)#login authentication telnet-login
R-Bucaramanga(config-line)#exit
R-Bucaramanga(config)#do wr
Building configuration...
[OK]
R-Bucaramanga(config)#
```

R-Tunja

```
R-Tunja>enable
R-Tunja#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R-Tunja(config)#username admin secret 1234
R-Tunja(config)#aaa new-mode
R-Tunja(config)#aaa authentication login default local
R-Tunja(config)#line console 0
R-Tunja(config-line)#login authentication default
R-Tunja(config-line)#exit
R-Tunja(config)#aaa authentication login telnet-login local
R-Tunja(config)#line console 0
R-Tunja(config-line)#login authentication default
R-Tunja(config-line)#exit
R-Tunja(config)#line vty 0 4
R-Tunja(config-line)#login authentication telnet-login
R-Tunja(config-line)#exit
R-Tunja(config)#do wr
Building configuration...
[OK]
R-Tunja(config)#
```

5.2.5. Asignación Ip terminal FastEthernet

R-Bucaramanga

```
R-Bucaramanga>enable
R-Bucaramanga#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R-Bucaramanga(config)#interface fastethernet 0/0
R-Bucaramanga(config-if)#ip address 172.31.2.1 255.255.255.252
R-Bucaramanga(config-if)#no shutdown
```

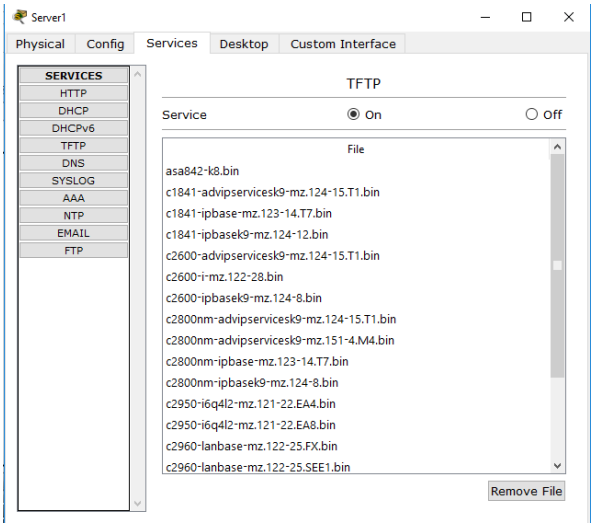
R-Tunja

```
R-Tunja#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R-Tunja(config)#interface fastethernet 0/0
R-Tunja(config-if)#ip address 171.31.2.2 255.255.255.252
R-Tunja(config-if)#no shutdown
```

R-Cundinamarca

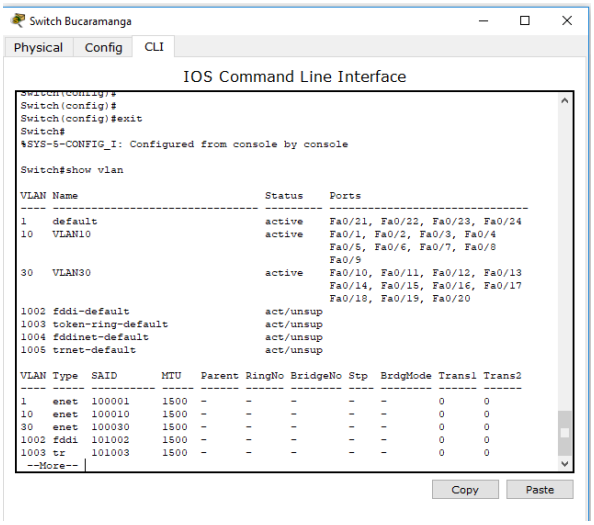
```
R-Cundinamarca#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R- Cundinamarca (config)#interface fastethernet 0/0
R- Cundinamarca (config-if)#ip address 171.31.2.1 255.255.255.252
R- Cundinamarca (config-if)#no shutdown
```

5.2.6. Servidor TFTP



5.2.7. Configuración Vlan en Switch

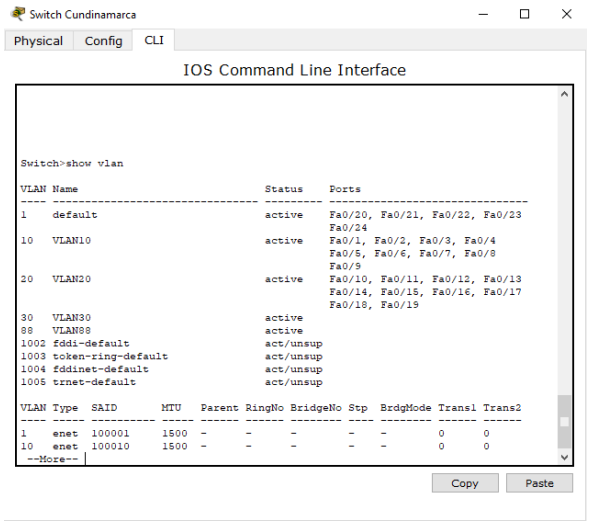
Switch R-Bucaramanga



Switch Cundinamarca

S-Cundinamarca>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S-Cundinamarca (config)#vlan 10
S-Cundinamarca (config-vlan)#NAME VLAN10
S-Cundinamarca (config-vlan)#exit
S-Cundinamarca (config)#vlan 30
S-Cundinamarca (config-vlan)#NAME VLAN20

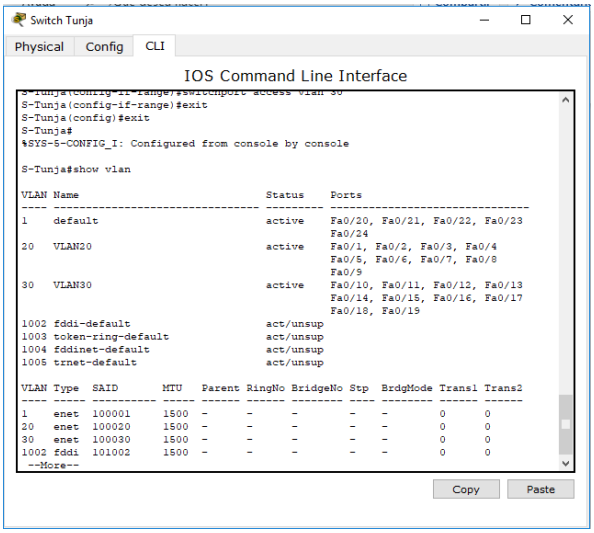
S-Cundinamarca (config-vlan)#exit
S-Cundinamarca (config)#vlan 88
S-Cundinamarca (config-vlan)#NAME VLAN88
S-Cundinamarca (config-vlan)#exit
S-Cundinamarca (config)#
S-Cundinamarca (config)#interface range f0/1-9
S-Cundinamarca (config-if-range)#switchport mode access
S-Cundinamarca (config-if-range)#switchport access vlan 10
S-Cundinamarca (config-if-range)#exit
S-Cundinamarca (config)#interface range f0/10-19
S-Cundinamarca (config-if-range)#switchport mode access
S-Cundinamarca (config-if-range)#switchport access vlan 20
S-Cundinamarca (config-if-range)#exit
S-Cundinamarca (config)#



Switch R-Tunja

S-Tunja>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S-Tunja (config)#vlan 10
S-Tunja (config-vlan)#NAME VLAN10
S-Tunja (config-vlan)#exit
S-Tunja (config)#vlan 30
S-Tunja (config-vlan)#NAME VLAN20
S-Tunja (config-vlan)#exit
S-Tunja (config)#vlan 88
S-Tunja (config-vlan)#NAME VLAN88
S-Tunja (config-vlan)#exit
S-Tunja (config)#
S-Tunja (config)#interface range f0/1-9
S-Tunja (config-if-range)#switchport mode access
S-Tunja (config-if-range)#switchport access vlan 10
S-Tunja (config-if-range)#exit
S-Tunja (config)#interface range f0/10-19
S-Tunja (config-if-range)#switchport mode access

S-Tunja (config-if-range)#switchport access vlan 20
S-Tunja (config-if-range)#exit
S-Tunja (config)#



5.2.8. Máximo de intentos para acceder a router

Se configura router teniendo en cuenta los siguiente:

- Máximo 3 intentos de loggin
- Tiempo 60 segundos.

R-Bucaramanga

R-Bucaramanga#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
R-Bucaramanga(config)#ip ssh time-out 60
R-Bucaramanga(config)#ip ssh authentication-retries 3
R-Bucaramanga(config)#do wr
Building configuration... [OK]
R-Bucaramanga(config)#end
R-Bucaramanga#
*mar. 01, 02:52:35.5252: SYS-5-CONFIG_I: Configured from console by console

R-Cundinamarca

R-Cundinamarca#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
R-Cundinamarca(config)#ip ssh time-out 60
R-Cundinamarca(config)#ip ssh authentication-retries 3
R-Cundinamarca(config)#do wr
Building configuration... [OK]
R-Cundinamarca(config)#end

R-Cundinamarca#
*mar. 01, 02:52:35.5252: SYS-5-CONFIG_I: Configured from console by console

R-Tunja

R-Tunja#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
R-Tunja (config)#ip ssh time-out 60
R-Tunja (config)#ip ssh authentication-retries 3
R-Tunja (config)#do wr
Building configuration... [OK]
R-Tunja (config)#end
R-Tunja #
*mar. 01, 02:52:35.5252: SYS-5-CONFIG_I: Configured from console by console

5.2.9. CONFIGURACIÓN DE SERVIDOR TFTP

Por medio de este código fuente se puede establecer un servidor TFTP que permita almacenar un backup de configuración de cada router de la red. A continuación, se vincula estos paramentros en cada router

R-Cundinamarca

R-Cundinamarca#copy run tftp
Address or name of remote host []? 172.31.2.227
Destination filename [CUNDINAMARCA-confg]?
running-config...!!
[OK - 2044 bytes]
2044 bytes copied in 0.011 secs (185818 bytes/sec)
R-Cundinamarca#

R-Tunja

R-Tunja#copy run tftp
Address or name of remote host []? 209.17.220.2
Destination filename [R-TUNJA-confg]?
Writing running-config !!
[OK - 1771 bytes]
1771 bytes copied in 3.010 secs (587 bytes/sec)
R-Tunja#

R-Bucaramanga

R-Bucaramanga#copy run tftp
Address or name of remote host []? 172.31.2.227
Destination filename [R-BUCARAMANGA-confg]?
Writing running-config !!
[OK - 1968 bytes]
1968 bytes copied in 3.082 secs (639 bytes/sec)

R-Bucaramanga#

5.2.10. Configuración de DHCP para R-Bucaramanga y Cundinamarca

Se ejecutará configuración DHCP para las sedes de R-Bucaramanga y Cundinamarca a cada router, teniendo en cuenta la interfaz del router de R-Tunja, el cual realizará la labor de entrega de direccionamiento IP.

R-Tunja – Cundinamarca DHCP

```
R-Tunja#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R-Tunja(config)#ip dhcp excluded-address 172.31.1.65 172.31.1.94
R-Tunja(config)#ip dhcp pool VLAN_20
R-Tunja(dhcp-config)#network 172.31.1.64 255.255.255.192
R-Tunja(dhcp-config)#default-router 172.31.1.65
R-Tunja(dhcp-config)#exit
R-Tunja(config)#ip dhcp excluded-address 172.31.1.1 172.31.1.30
R-Tunja(config)#ip dhcp pool VLAN_30
R-Tunja(dhcp-config)#network 172.31.1.0 255.255.255.192
R-Tunja(dhcp-config)#default-router 172.31.1.1
R-Tunja(dhcp-config)#exit
R-Tunja(config)#ip dhcp pool VLAN_20
R-Tunja(dhcp-config)#no network 172.31.1.34 255.255.255.192
R-Tunja(dhcp-config)#network 172.31.1.64 255.255.255.192
R-Tunja(dhcp-config)#exit
R-Tunja(config)#ip dhcp exc
R-Tunja(config)#ip dhcp excluded-address 172.31.2.25 172.31.2.30
R-Tunja(config)#ip dhcp pool VLAN_88
R-Tunja(dhcp-config)#network 172.31.2.24 255.255.255.248
R-Tunja(dhcp-config)#default-router 172.31.2.25 R-TUNJA(dhcp-config)#do wr
R-Tunja(dhcp-config)#end
R-Tunja#
```

R-Cundinamarca

```
R-Cundinamarca#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R-Cundinamarca(config)#interface giga0/0.30
R-Cundinamarca(config-subif)#ip helper-address 172.31.2.37
R-Cundinamarca(config-subif)#interface giga0/0.20
R-Cundinamarca(config-subif)#ip helper-address 172.31.2.37
R-Cundinamarca(config-subif)#end
R-Cundinamarca#
%SYS-5-CONFIG_I: Configured from console by console
```

R-Tunja – R-Bucaramanga DHCP

```
R-Tunja#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

```
R-Tunja(config)#
R-Tunja(config)#ip dhcp excluded-address 172.31.0.1 172.31.0.30
R-Tunja(config)#ip dhcp pool VLAN_10
R-Tunja(dhcp-config)#network 172.31.0.0 255.255.255.192
R-Tunja(dhcp-config)#default-router 172.31.0.1
R-Tunja(dhcp-config)#exit
R-Tunja(config)#ip dhcp excluded-address 172.31.0.65 172.31.0.94
R-Tunja(config)#ip dhcp pool VLAN-30
R-Tunja(dhcp-config)#network 172.31.0.64 255.255.255.192
R-Tunja(dhcp-config)#default-router 172.31.0.65
R-Tunja(dhcp-config)#exit
R-Tunja(config)#do wr Building configuration... [OK]
R-Tunja(config)#end
R-Tunja#
```

R-Bucaramanga

```
R-Bucaramanga#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R-Bucaramanga(config)#interface giga0/0.10
R-Bucaramanga(config-subif)#ip helper
R-Bucaramanga(config-subif)#ip helper-address 172.31.2.34
R-Bucaramanga(config-subif)#exit
R-Bucaramanga(config)#interface giga0/0.30
R-Bucaramanga(config-subif)#ip helper-address 172.31.2.34
R-Bucaramanga(config-subif)#do wr
Building configuration... [OK]
R-Bucaramanga(config-subif)#end
R-Bucaramanga#
```

5.2.11. Opciones puerto de consola y terminal virtual

Se configura accesibilidad a puerto de consola en un tiempo de 0 a 60 segundos en cada router.

R-Bucaramanga

```
R-Bucaramanga(config)#enable password cisco
R-Bucaramanga(config)#service password-encryption
R-Bucaramanga(config)#line vty 0 4
R-Bucaramanga(config-line)#password cisco
R-Bucaramanga(config-line)#exec-t
R-Bucaramanga(config-line)#exec-timeout 0 60
R-Bucaramanga(config-line)#login
R-Bucaramanga(config-line)#logging synchronous
R-Bucaramanga(config-line)#exit
R-Bucaramanga(config)#service password-encryption
R-Bucaramanga(config)#
R-Bucaramanga(config)#do wr
Building configuration... [OK]
R-Bucaramanga(config)#end
R-Bucaramanga#
```

```
R-Bucaramanga(config)#username whitney password cisco
R-Bucaramanga(config)#line console 0
R-Bucaramanga(config-line)#login local
R-Bucaramanga(config-line)#password cisco
R-Bucaramanga(config-line)#exit
R-Bucaramanga(config)#
R-Bucaramanga(config)#do wr
Building configuration...[OK]
R-Bucaramanga(config)#end
R-Bucaramanga#
```

Router R-Tunja

```
R-Tunja#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R-Tunja(config)#username whitney password cisco
R-Tunja(config)#line console 0
R-Tunja(config-line)#login local
R-Tunja(config-line)#password cisco
R-Tunja(config-line)#exit
R-Tunja(config)#service password-encryption
R-Tunja(config)#enable password cisco
R-Tunja(config)#service password-encryption
R-Tunja(config)#line vty 0 4
R-Tunja(config-line)#password cisco
R-Tunja(config-line)#exec-timeout 0 60
R-Tunja(config-line)#login
R-Tunja(config-line)#logging synchronous
R-Tunja(config-line)#exit
R-Tunja(config)#service password-encryption
R-Tunja(config)#
R-Tunja(config)#do wr
Building configuration... [OK]
R-Tunja(config)#end
R-Tunja#
```

R-Cundinamarca

```
R-Cundinamarca#configure termina
Enter configuration commands, one per line. End with CNTL/Z.
R-Cundinamarca(config)#username whitney password cisco
R-Cundinamarca(config)#line console 0
R-Cundinamarca(config-line)#login local
R-Cundinamarca(config-line)#password cisco
R-Cundinamarca(config-line)#exit
R-Cundinamarca(config)#service password-encryption
R-Cundinamarca(config)#line vty 0 4
R-Cundinamarca(config-line)#password cisco
R-Cundinamarca(config-line)#exec-timeout 0 60
R-Cundinamarca(config-line)#login
R-Cundinamarca(config-line)#loggin synchronous
R-Cundinamarca(config-line)#exit
```

R-Cundinamarca(config)#service password-encryption
R-Cundinamarca(config)#do wr
Building configuration... [OK]
R-Cundinamarca(config)#end
R-Cundinamarca#

5.2.12. Configuración de NAT estático

Se procede a configurar NAT estático para web servers.

R-Tunja

R-Tunja#configureterminal
Enter configuration commands, one per line. End with CNTL/Z.
R-Tunja(config)#ip nat inside source static 172.31.2.227 209.17.220.0
R-Tunja(config)#interface serial 0/0/1
R-Tunja(config-if)#ip nat inside
R-Tunja(config-if)#interface serial 0/0/0
R-Tunja(config-if)#ip nat outside
R-Tunja(config-if)#interface giga0/0
R-Tunja(config-if)#ip nat outside
R-Tunja(config-if)#
R-Tunja(config-if)#do wr
Building configuration... [OK]
R-Tunja(config-if)#end
R-Tunja#

```
TUNJA#sh ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 209.17.220.0:16   172.31.2.227:16    172.31.0.31:16     172.31.0.31:16
icmp 209.17.220.0:17   172.31.2.227:17    172.31.0.31:17     172.31.0.31:17
icmp 209.17.220.0:18   172.31.2.227:18    172.31.0.31:18     172.31.0.31:18
icmp 209.17.220.0:19   172.31.2.227:19    172.31.0.31:19     172.31.0.31:19
```

Ilustración 28. Configuración NAT estático para Web Server Interno

R-Tunja –
R-Tunja#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R-Tunja(config)#ip nat inside source static 209.17.220.2 200.200.200.7
R-Tunja(config)#interface giga0/1
R-Tunja(config-if)#ip nat inside
R-Tunja(config-if)#interface serial 0/0/0
R-Tunja(config-if)#ip nat outside
R-Tunja(config-if)#interface giga0/0
R-Tunja(config-if)#ip nat outside

R-Tunja(config-if)#

```
TUNJA#sh ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 200.200.200.7:5   209.17.220.2:5     172.31.0.95:5      172.31.0.95:5
icmp 200.200.200.7:6   209.17.220.2:6     172.31.0.95:6      172.31.0.95:6
icmp 200.200.200.7:7   209.17.220.2:7     172.31.0.95:7      172.31.0.95:7
icmp 200.200.200.7:8   209.17.220.2:8     172.31.0.95:8      172.31.0.95:8
```

Ilustración 29. Configuración NAT estático para Web Server Externo

5.2.13. Sobrecarga PAT para los demás equipos

R-Tunja#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R-Tunja(config)#ip nat inside source static tcp 209.17.220.2 80 200.200.200.7 80
R-Tunja(config)#ip nat inside source static tcp 209.17.220.2 80 200.200.200.7 80
R-Tunja(config)#do wr
Building configuration... [OK]
R-Tunja(config)#end
R-Tunja#

Ilustración 30.Configuración PAT de sobrecarga

5.2.14. Restricciones hosts de VLAN 20 Cundinamarca

Desarrollo de configuración de lista de acceso extendida 101, para el router de Cundinamarca para permitir tráfico del host con red 172.31.1.64/26 (VLAN20), hacia la red interna de R-Tunja 172.31.0.129 /26 y 172.31.0.193 /26.

R-Cundinamarca
R-Cundinamarca#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R-Cundinamarca(config)#access-list 110 permit ip 172.31.1.64 0.0.0.63 172.31.0.193 0.0.0.63
R-Cundinamarca(config)#access-list 110 permit ip 172.31.1.29 0.0.0.63 172.31.0.129 0.0.0.63

Se utiliza command “***any any***” para bloquear tráfico de cualquier host

R-Cundinamarca(config)#access-list 110 deny ip any any.
R-Cundinamarca(config)#interface serial 0/0/0
R-Cundinamarca(config-if)#ip access-group 110 out
R-Cundinamarca(config-if)#do wr
Building configuration...

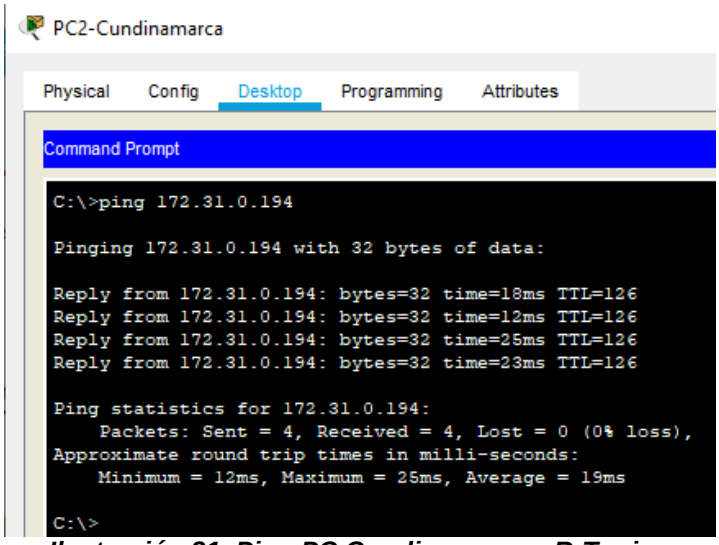


Ilustración 31. Ping PC Cundinamarca - R-Tunja

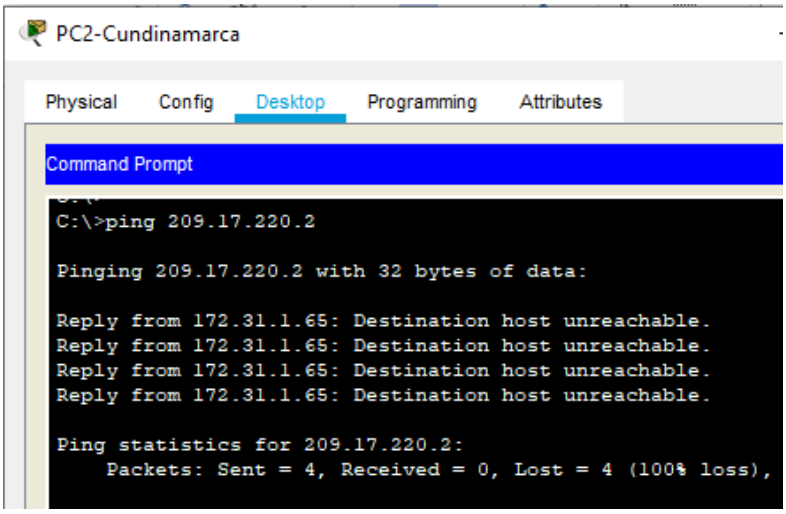


Ilustración 32. Ping PC Cundinamarca-internet

5.2.15. Restricción hosts de VLAN 20 R-Tunja

Se realiza configuración de lista de acceso extendida 120, en el router de R-Tunja teniendo en cuenta que solo acceden a la VLAN 20 de Cundinamarca y VLAN 10 de R-Bucaramanga.

Adicionalmente se crea una lista de acceso 120 para denegar tráfico hacia cualquier host. A través de comandos "***any any***".

```
R-Tunja VLAN 20
R-Tunja# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R-Tunja(config)#access-list 120 permit ip 172.31.0.128 0.0.0.30 172.31.1.64 0.0.0.63
R-Tunja(config)#access-list 120 permit ip 172.31.0.128 0.0.0.63 172.31.0.0 0.0.0.63
R-Tunja(config)#access-list 120 deny ip any
R-Tunja(config)#interface serial 0/0/1
R-Tunja(config-if)#ip access-group 120 out
R-Tunja(config-if)#interface serial 0/0/0
R-Tunja(config-if)#ip access-group 120 out
R-Tunja(config-if)#
R-Tunja(config-if)#
R-Tunja(config-if)#do wr
```

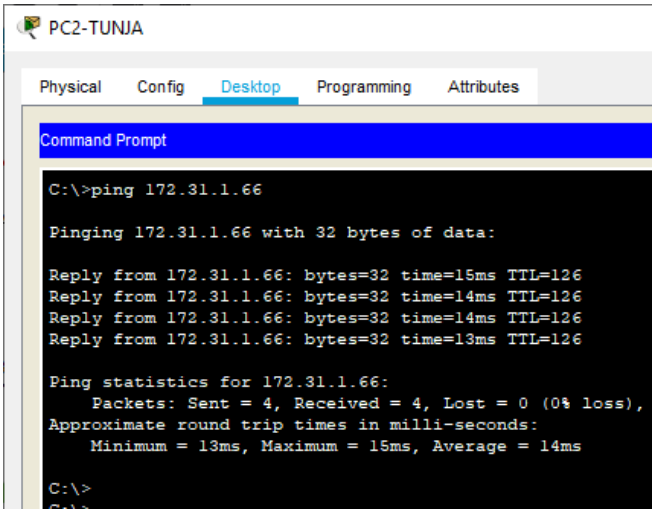


Ilustración 33. Ping PC R-Tunja a PC Cundinamarca VLAN 2

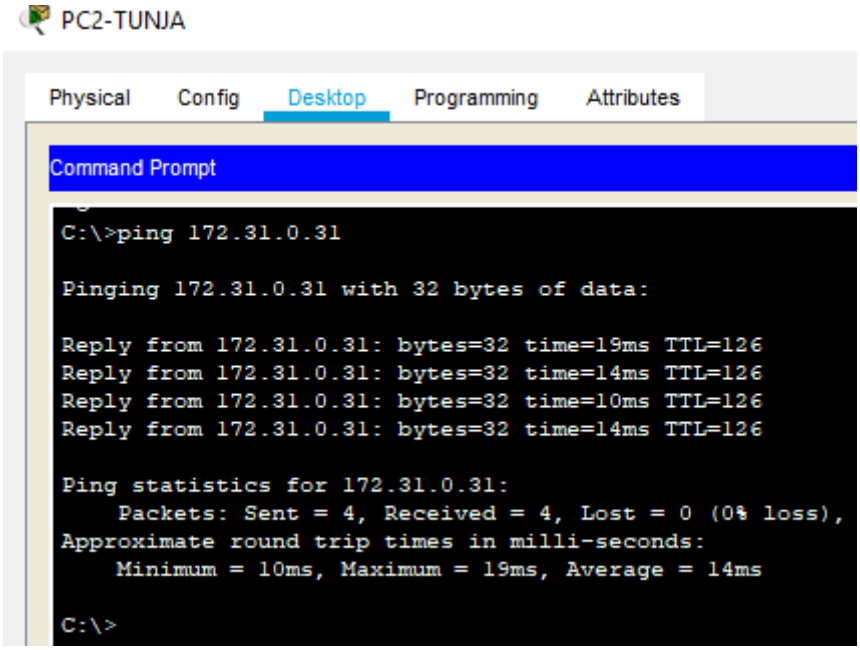


Ilustración 34. Ping PC R-Tunja VLAN 20 a PC R-Bucaramanga VLAN 10

5.2.16. Permisos hosts de VLAN 30 de R-Bucaramanga

Se realiza configuración de lista de acceso extendida 101, en el router de R-Bucaramanga Ping desde PC R-Tunja VLAN 20 a PC R-Bucaramanga VLAN 10 sobre la (VLAN30) con red 172.31.0.64 /26 para permitir tráfico hacia Internet y a cualquier equipo de la (VLAN10) con red 172.31.0.0 /26

R-Bucaramanga
R-Bucaramanga#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R-Bucaramanga(config)#access-list 101 permit ip 172.31.0.64 0.0.0.63 172.31.0.0 0.0.0.63
R-Bucaramanga(config)#access-list 101 permit ip 172.31.0.64 0.0.0.63
209.17.220.0 0.0.0.255
R-Bucaramanga(config)#interface giga0/0
R-Bucaramanga(config-if)#ip access-group 101 out
R-Bucaramanga(config-if)#

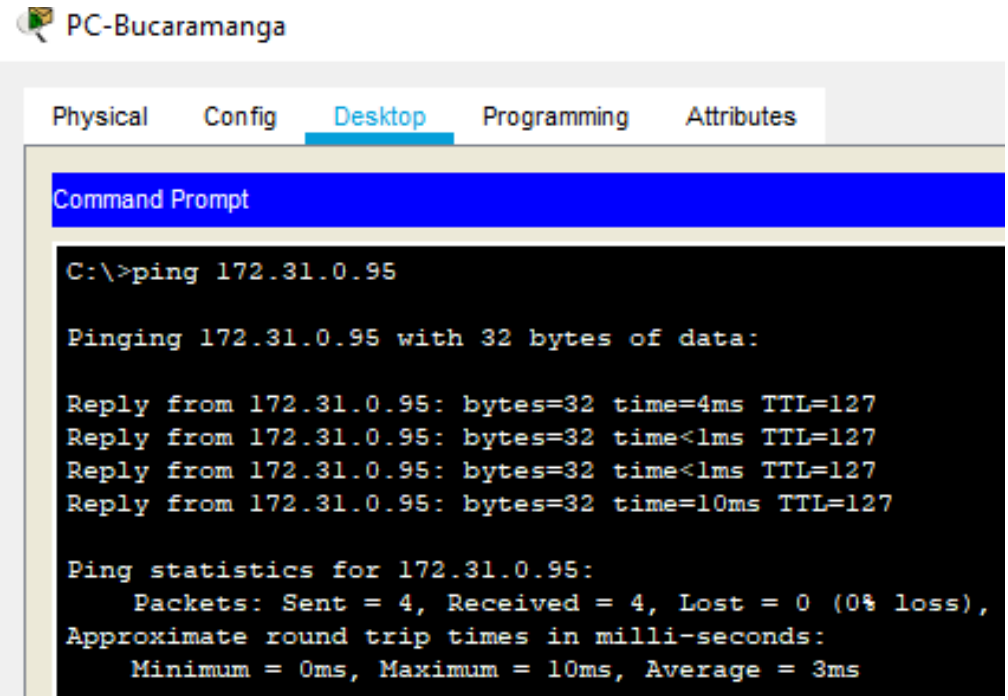


Ilustración 35. Ping PC-Bucaramanga Vlan 30 a Vlan 10

5.2.17. Permisos Hosts de VLAN 10 en R-Bucaramanga

Se realiza configuración de lista de acceso extendida 103, en el router de R-Bucaramanga sobre la (VLAN10) acceden a la red de Cundinamarca (VLAN 20) y R-Tunja (VLAN 20), no internet.

R-Bucaramanga

```
R-Bucaramanga#configure terminal
R-Bucaramanga(config)#access-list 103 permit ip 172.31.0.0 0.0.0.63 172.31.1.64 0.0.0.63
R-Bucaramanga(config)#access-list 103 permit ip 172.31.0.0 0.0.0.63 172.31.0.128 0.0.0.63
R-Bucaramanga(config)#access-list 103 deny ip 172.31.0.0 0.0.0.63 209.17.220.2 0.0.0.255
R-Bucaramanga(config)#
R-Bucaramanga(config)#interface serial 0/0/0
R-Bucaramanga(config-if)#ip access-group 103 out
R-Bucaramanga(config-if)#
R-Bucaramanga(config-if)#end
R-Bucaramanga#
```

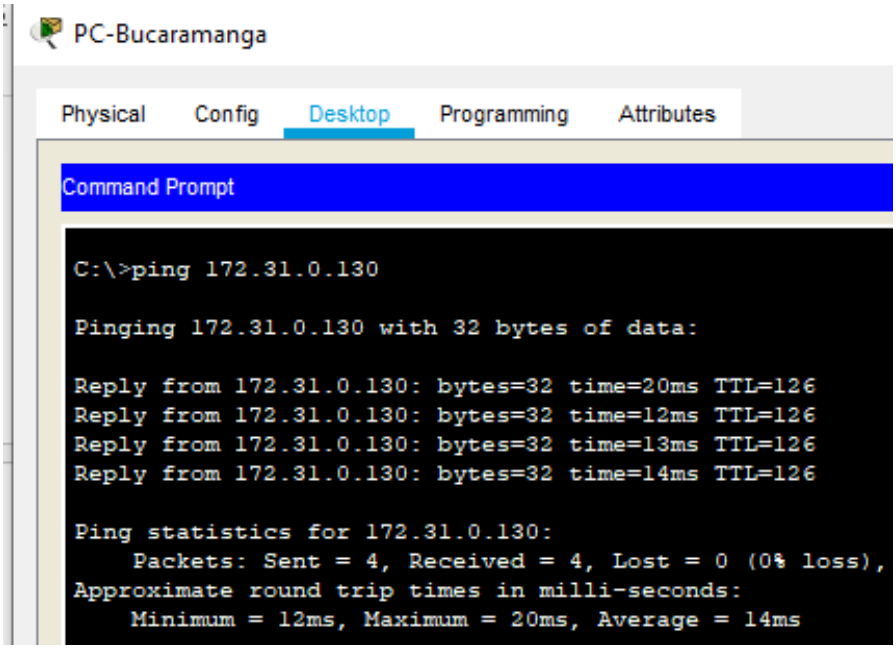


Ilustración 36. Ping PC R-Bucaramanga VLAN 10-VLAN 20 PC R-Tunja

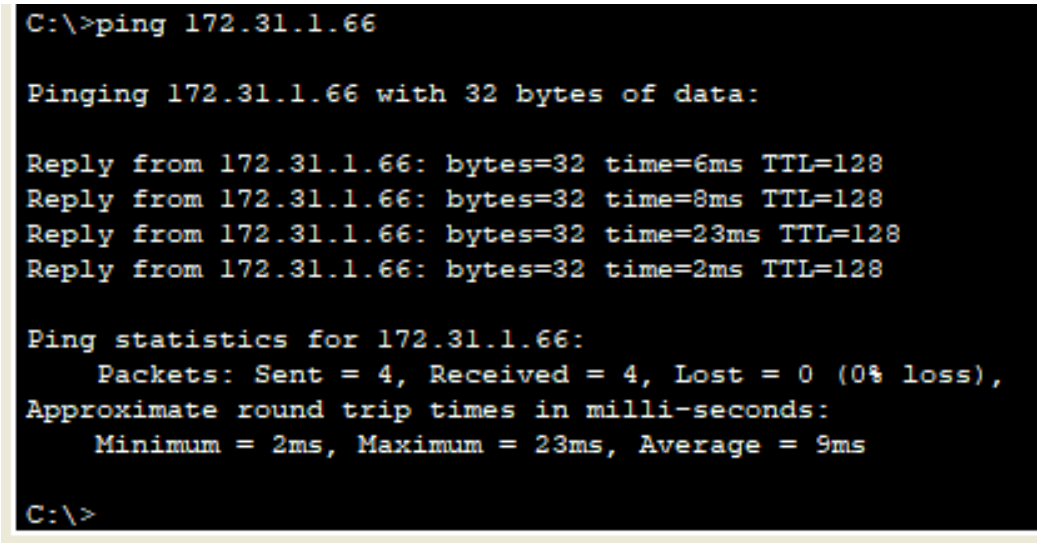


Ilustración 37. Ping PC R-Bucaramanga VLAN 10- VLAN 20 PC Cundinamarca

6. CONCLUSIONES

- El protocolo DHCP está diseñado fundamentalmente para ahorrar tiempo gestionando direcciones IP en una red grande. El servicio DHCP se encuentra activo en un servidor donde se centraliza la administración de las direcciones IP de la red.

- OSPF es un protocolo que gestiona un sistema autónomo (AS) en áreas. Dichas áreas son grupos lógicos de routers cuya información se puede resumir para el resto de la red. Un área es una unidad de encaminamiento, es decir, todos los routers de la misma área mantienen la misma información topológica en su base de datos de estado-enlace (Link State Database): de esta forma, los cambios en una parte de la red no tienen por qué afectar a toda ella, y buena parte del tráfico puede ser "parcelado" en su área.

- El desarrollo de prácticas en CISCO genera la facilidad de implementar protocolos prácticos, los cuales permiten gestionar acciones básicas como la asignación de direcciones ip a periféricos hasta la configuración de routers en sus parámetros de seguridad.

- EIGRP es utilizado en redes TCP/IP y de Interconexión de Sistemas Abierto (OSI) como un protocolo de enrutamiento del tipo vector distancia avanzado, propiedad de Cisco, que ofrece las mejores características de los algoritmos vector distancia y de estado de enlace.

7. BIBLIOGRAFIA

- Temática: Exploración de la red
  CISCO. (2014). Exploración de la red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module1/index.html#1.0.1.1
- Temática: Configuración de un sistema operativo de red
  CISCO. (2014). Configuración de un sistema operativo de red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#2.0.1.1
- Temática: Protocolos y comunicaciones de red
  CISCO. (2014). Protocolos y comunicaciones de red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#3.0.1.1
- Temática: Acceso a la red
  CISCO. (2014). Acceso a la red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#4.0.1.1
- Temática: Ethernet
  CISCO. (2014). Ethernet. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#5.0.1.1
- Temática: Capa de red
  CISCO. (2014). Capa de red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#6.0.1.1
- Vesga, J. (2014). Diseño y configuración de redes con Packet Tracer [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgCT9VCtl_pLtPD9
- Vesga, J. (2019). Introducción al Laboratorio Remoto SmartLab [OVI]. Recuperado de http://hdl.handle.net/10596/24167
- Macfarlane, J. (2014). Network Routing Basics : Understanding IP Routing in Cisco Systems. Recuperado de http://bibliotecavirtual.unad.edu.co:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=e000xww&AN=158227&lang=es&site=ehost-live
- Lucas, M. (2009). Cisco Routers for the Desperate : Router and Switch Management, the Easy Way. San Francisco: No Starch Press. Recuperado de https://1drv.ms/b/s!AmIJYei-NT1Im3L74BZ3bpMiXRx0

- Odom, W. (2013). CISCO Press (Ed). CCNA ICND1 Official Exam Certification Guide. Recuperado de http://ptgmedia.pearsoncmg.com/images/9781587205804/samplepages/9781587205804.pdf

- Odom, W. (2013). CISCO Press (Ed). CCNA ICND2 Official Exam Certification Guide. Recuperado de http://mr-telecomunicaciones.com/wp-content/uploads/2018/09/wendellodom.pdf
- Lammle, T. (2010). CISCO Press (Ed). Cisco Certified Network Associate Study Guide. Recuperado de https://1drv.ms/b/s!AmIJYei-NT1Im3GQVfFFrjnEGFFU
- CISCO. (2014). Capa de Transporte. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module7/index.html#7.0.1.1
- CISCO. (2014). Asignación de direcciones IP. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module8/index.html#8.0.1.1
- CISCO. (2014). SubNetting. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module9/index.html#9.0.1.1
- CISCO. (2014). Capa de Aplicación. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module10/index.html#10.0.1.1
- CISCO. (2014). Soluciones de Red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module11/index.html#11.0.1.1
- Vesga, J. (2014). PING y TRACER como estrategia en procesos de Networking [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgTCtKY-7F5KIRC3
- Macfarlane, J. (2014). etwork Routing Basics : Understanding IP Routing in Cisco Systems. Recuperado de http://bibliotecavirtual.unad.edu.co:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=e000xww&AN=158227&lang=es&site=ehost-live
- Lucas, M. (2009). Cisco Routers for the Desperate : Router and Switch Management, the Easy Way. San Francisco: No Starch Press. Recuperado de https://1drv.ms/b/s!AmIJYei-NT1Im3L74BZ3bpMiXRx0
- Odom, W. (2013). CISCO Press (Ed). CCNA ICND1 Official Exam Certification Guide. Recuperado de http://ptgmedia.pearsoncmg.com/images/9781587205804/samplepages/9781587205804.pdf
- Odom, W. (2013). CISCO Press (Ed). CCNA ICND2 Official Exam Certification Guide. Recuperado de http://mr-telecomunicaciones.com/wp-content/uploads/2018/09/wendellodom.pdf
- Lammle, T. (2010). CISCO Press (Ed). Cisco Certified Network Associate Study Guide. Recuperado de https://1drv.ms/b/s!AmIJYei-NT1Im3GQVfFFrjnEGFFU
- CISCO. (2014). Introducción a redes conmutadas. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module1/index.html#1.0.1.1

- CISCO. (2014). Configuración y conceptos básicos de Switching. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module2/index.html#2.0.1.1
- CISCO. (2014). VLANs. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module3/index.html#3.0.1.1
- CISCO. (2014). Conceptos de Routing. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module4/index.html#4.0.1.1
- CISCO. (2014). Enrutamiento entre VLANs. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module5/index.html#5.0.1.1
- CISCO. (2014). Enrutamiento Estático. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module6/index.html#6.0.1.1
- Vesga, J. (2014). Configuración de Switches y Routers [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgL9QChD1m9EuGqC
- Macfarlane, J. (2014). Network Routing Basics : Understanding IP Routing in Cisco Systems. Recuperado de http://bibliotecavirtual.unad.edu.co:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=e000xww&AN=158227&lang=es&site=ehost-live
- Lucas, M. (2009). Cisco Routers for the Desperate : Router and Switch Management, the Easy Way. San Francisco: No Starch Press. Recuperado de https://1drv.ms/b/s!AmIJYei-NT1Im3L74BZ3bpMiXRx0
- Odom, W. (2013). CISCO Press (Ed). CCNA ICND1 Official Exam Certification Guide. Recuperado de http://ptgmedia.pearsoncmg.com/images/9781587205804/samplepages/9781587205804.pdf
- Odom, W. (2013). CISCO Press (Ed). CCNA ICND2 Official Exam Certification Guide. Recuperado de http://mr-telecomunicaciones.com/wp-content/uploads/2018/09/wendellodom.pdf
- Lammle, T. (2010). CISCO Press (Ed). Cisco Certified Network Associate Study Guide. Recuperado de https://1drv.ms/b/s!AmIJYei-NT1Im3GQVfFFrjnEGFFU
- CISCO. (2014). Enrutamiento Dinámico. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module7/index.html#7.0.1.1
- CISCO. (2014). OSPF de una sola área. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module8/index.html#8.0.1.1
- CISCO. (2014). Listas de control de acceso. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module9/index.html#9.0.1.1

- CISCO. (2014). DHCP. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module10/index.html#10.0.1.1
- CISCO. (2014). Traducción de direcciones IP para IPv4. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module11/index.html#11.0.1.1
- Vesga, J. (2014). Principios de Enrutamiento [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgOyjWeh6timi_Tm
- Macfarlane, J. (2014). Network Routing Basics : Understanding IP Routing in Cisco Systems. Recuperado de http://bibliotecavirtual.unad.edu.co:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=e000xww&AN=158227&lang=es&site=ehost-live
- Lucas, M. (2009). Cisco Routers for the Desperate : Router and Switch Management, the Easy Way. San Francisco: No Starch Press. Recuperado de https://1drv.ms/b/s!AmIJYei-NT1Im3L74BZ3bpMiXRx0
- Odom, W. (2013). CISCO Press (Ed). CCNA ICND1 Official Exam Certification Guide. Recuperado de http://ptgmedia.pearsoncmg.com/images/9781587205804/samplepages/9781587205804.pdf
- Odom, W. (2013). CISCO Press (Ed). CCNA ICND2 Official Exam Certification Guide. Recuperado de http://mr-telecomunicaciones.com/wp-content/uploads/2018/09/wendellodom.pdf
- Lammle, T. (2010). CISCO Press (Ed). Cisco Certified Network Associate Study Guide. Recuperado de https://1drv.ms/b/s!AmIJYei-NT1Im3GQVfFFrjnEGFFU