DIPLOMADO DE PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN)

PRUEBA DE HABILIDADES PRACTICAS CCNA

GERMAN ANDRÉS RODRIGUEZ MORENO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
INGENIERIA DE SISTEMAS
CISCO CCNA I-II
2019

DIPLOMADO DE PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN)

PRUEBA DE HABILIDADES PRACTICAS CCNA

GERMAN ANDRÉS RODRIGUEZ MORENO

DIPLOMADO DE PROFUNDIZACION CISCO

JUAN CARLOS VESGA
INGENIERO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
INGENIERIA DE SISTEMAS
CISCO CCNA I-II
2019

Nota de Aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Facatativá, 12 diciembre 2019

Este trabajo está dedicado en primera instancia a Dios por brindarme salud para poder cumplir este proceso.

Como segunda instancia a mi hijo la cual fue la persona que me inspiro, apoyo, me guio en todo momento, es un gran pilar para este proyecto.

AGRADECIMIENTOS

Quiero expresar mi agradecimiento a los tutores del curso en especial al Ingeniero Giovani Bracho el cual nos acompañó mediante su orientación y recomendaciones de las actividades durante el transcurso del diplomado Cisco CNNA.

Gracias a la planta de formadores del CEAD de Facatativá, los cuales me brindaron herramientas y orientación en cada una de las actividades realizadas, contribuyendo con este proceso en formación de la carrera profesional; y a cada una de las personas que formaron parte de esta gran experiencia.

TABLA DE CONTENIDO

1 INDICE FIGURAS

2 RESUMEN

Cabe señalar que el desarrollo de las herramientas frente a las tecnologías de la información para realizar integración de las redes a nivel mundial, se muestra a través de estos escenarios propuestos en el desarrollo de habilidades POCKET TRACER, en el cual se aplicaran diferentes comandos para la generación de conectividad entre los distintos dispositivos.

Es así como en el siguiente documento se presentará solución a los dos escenarios propuestos, los cuales constará desde aplicar los diferentes equipos, hasta la conexión entre ellos, generando la mayor eficacia que se pueda presentar a las posibles situaciones que se nos puedan presentar en la vida cotidiana.

3 ABSTRAC

It should be noted that the development of tools against information technologies to perform global network integration is shown through these scenarios proposed in the development of POCKET TRACER skills, in which different commands will be applied to the connectivity generation between different devices.

This is how the following document will present a solution to the two proposed scenarios, which will consist of applying the different equipment, to the connection between them, generating the greatest efficiency that can be presented to the possible situations that may arise in the daily life.

4 INTRODUCCION

A partir de las temáticas realizadas anteriormente, en este documento colocaremos nuestras habilidades practicas a partir de dos escenarios los cuales fueron diseñados con el fin de emplear los distintos comandos y poder generar las conexiones pertinentes en las diferentes estaciones logrando llevar a cabo la topología de la red.

A este propósito se podrá realizar el direccionamiento IP de acuerdo a la cantidad de host solicitados, luego la detección de vecinos directamente conectados, poder implementar la seguridad en la red al llegar a este punto se debe restringir el acceso y comunicación de acuerdo a los requerimientos exigidos.

Avanzando en la actividad los router deberán tener configuraciones básicas, autenticación AAA, cifrado de contraseñas, adicional a eso se deberá trabajar con NAT estático, se deberá configurar diferentes VLAN para permitir los distintos enrutamientos, de esta manera se utilizará enrutamientos OSPF, DHCP, para poder establecer los accesos con los criterios señalados.

5 OBJETIVOS

5.1 Objetivo General

Desarrollar los escenarios de habilidades prácticas de Pocket tracer del diplomado profundización Cisco CCNA.

5.2 Objetivos específicos

- Cumplir con los requisitos exigidos para la actividad.
- Desarrollar las habilidades adquiridas durante el transcurso del curso a través de los escenarios propuestos de la guía.
- Generar informe detallado con su respectivo paso a paso.

6 DESARROLLO 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.

Topología de red

Los requerimientos solicitados son los siguientes:

Parte 1: Para el direccionamiento IP debe definirse una dirección de acuerdo con el número de hosts requeridos.

Parte 2: Considerar la asignación de los parámetros básicos y la detección de vecinos directamente conectados.

Parte 3: La red y subred establecidas deberán tener una interconexión total, todos los hosts deberán ser visibles y poder comunicarse entre ellos sin restricciones.

Parte 4: Implementar la seguridad en la red, se debe restringir el acceso y comunicación entre hosts de acuerdo con los requerimientos del administrador de red.

Parte 5: Comprobación total de los dispositivos y su funcionamiento en la red.

Parte 6: Configuración final.

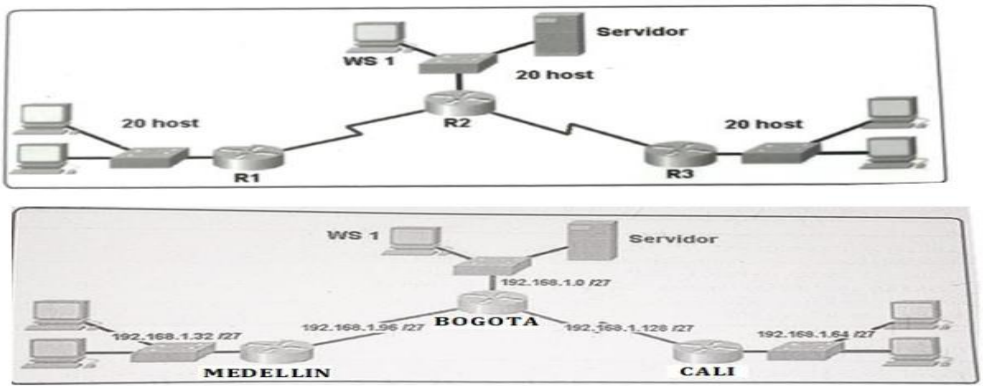


Ilustración 1Topologia Escenario 1

Desarrollo

Como trabajo inicial se debe realizar lo siguiente.

• Realizar las rutinas de diagnóstico y dejar los equipos listos para su configuración (asignar nombres de equipos, asignar claves de seguridad, etc.).

• Realizar la conexión fisica de los equipos con base en la topología de red

Configurar la topología de red, de acuerdo con las siguientes especificaciones.

6.1 Parte 1: Asignación de direcciones IP

a. Sé debe dividir (subnetear) la red creando una segmentación en ocho partes, para permitir crecimiento futuro de la red corporativa.

La mejor forma de poder dividir la red, es tomando del último octeto ciertos bits más significativos prestados, y le número de bits prestados está dado por la siguiente formula:

$$\#\ bits\ prestados = 2^n,\ \ donde\ n\ es\ el\ numero\ de\ bits$$

Por ejemplo, si deseamos tener un subneteo de red en ocho partes, se toman 3 bits:

$$2^n = 2^3 = 8$$

La forma de poder conocer el número de host que cada sub red puede tener como máximo está dado por:

$$2^n - 2 = 2^5 - 2 = 32 - 2 = 30$$

Así las cosas, el siguiente paso es poder crear las ocho tablas respectivas que nos darán las direcciones de cada red para obtener:

SUBRED	Dirección de red	Rango de Host	Dirección de difusión
0	192.168.1.0/27	192.168.1.1 – 192.168.1.30	192.168.1.31
1	192.168.1.32/27	192.168.1.33 – 192.168.1.62	192.168.1.63
2	192.168.1.64/27	192.168.1.65 – 192.168.1.94	192.168.1.95
3	192.168.1.96/27	192.168.1.97 – 192.168.1.126	192.168.1.127
4	192.168.1.128/27	192.168.1.129 – 192.168.1.158	192.168.1.159
5	192.168.1.160/27	192.168.1.161 – 192.168.1.190	192.168.1.191
6	192.168.1.192/27	192.168.1.193 – 192.168.1.222	192.168.1.223
7	192.168.1.224/27	192.168.1.225 – 192.168.1.254	192.168.1.255

Con las imágenes de la topología dada, se puede evidenciar que las redes obtenidas mediante el Excel corresponden en su mayoría y de las 8 obtenidas usaremos las primeras 5 (se reservan 3 redes más para un posible crecimiento de la red)

a. Asignar una dirección IP a la red.

- Configuración realizada para Serial 0/0/0, aplicado al router de medellin

```
MEDELLIN(config)#int 50/0/0
MEDELLIN(config-if)#ip add
MEDELLIN(config-if)#ip address 192.168.1.99 255.255.255.224
MEDELLIN(config-if)#no shu
MEDELLIN(config-if)#no shutdown
```

- Configuración realizada para gigabit 0/0

MEDELLIN(config-if)#exit
MEDELLIN(config)#int g0/0
MEDELLIN(config-if)#ip add
MEDELLIN(config-if)#ip address 192.168.1.33 255.255.255.224 MEDELLIN(config-if)#no shut MEDELLIN(config-if)#no shutdown

- Configuración para el Router de Bogotá puertos serial 0/0 y 0/1

BOGOTA>enable
BOGOTA#config t Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA(config)#int s0/0/1
BOGOTA(config-if)#ip add
BOGOTA(config-if)#ip address 192.168.1.130 225.225.225.224 Bad mask OxE1E1E1E0 for address 192.168.1.130
BOGOTA(config-if)#ip address 192.168.1.130 225.225.225.0 Bad mask OxE1E1E100 for address 192.168.1.130
BOGOTA(config-if)#ip address 192.168.1.130 255.255.255.224
BOGOTA(config-if)#no shu

BOGOTA(config-if)#no shutdown

%LINK-5-CHANGED: Interface Seria10/0/1, changed state to down BOGOTA(config-if)#exit

BOGOTA(config)#int s0/0/0

BOGOTA(config-if)#ip add

BOGOTA(config-if)#ip address 192.168.1.98 255.255.255.224 BOGOTA(config-if)tno shut

BOGOTA(config-if)#no shutdown

BOGOTA(config-if)* %LINK-5-CHANGED: Interface Seria10/0/0, changed state to up

- Puerto gigabit 0/0 en el router BOGOTA

BOGOTA(config-if)#exit

BOGOTA(config)#int g0/0 BOGOTA(config-ifltip add

BOGOIA(config-if)#ip address 192.168.1.1 255.255.255.224

BOGOTA(config-if)#no shu

BOGOTA(config-if)#no shutdown

BOGOTA(config-if)#exit

- Router cali, configuración puertos s0/0/0 y gigabit 0/0

CALI>enable

CALIftonfig t

Enter configuration commands, one per line. End with CNTL/Z.

CALI(config)#int 50/0/0

CALI(config-if)#ip add CALI(COnfig-if)#ip address 192.168.1.131 255.255.255.224

CALI(config-if)#no shut CALI(Config-iflino shutdown

CALI(COnfig-if)# %LINK-5 -CHANGED: Interface Seria10/0/0, changed state to up

CALI(config-if)# 4LINEPROTO-5-UPDOWN: Line protocol on Interface Seria10/0/0, changed state to up

CALI(config-if)#exit

CALI(confio)aint g0/0

CALI(config-if)#ip add

CALI(config-if)#ip address 192.168.1.65 255.255.255.224

CALI(config-if)#no shut

CALI(config-if)#no shutdown

- Configuración Ip Pc 0/1 Medellín, proceso donde realizamos la configuración básica de los PC de Medellin

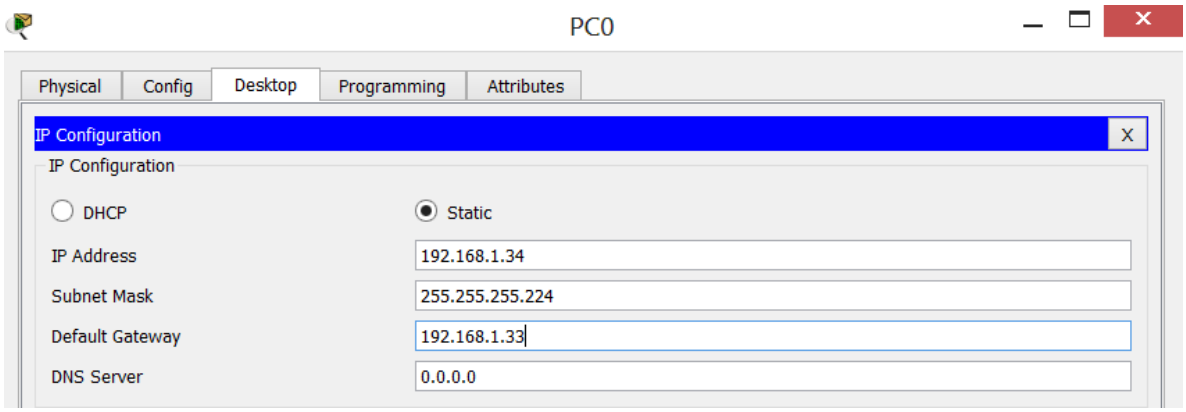
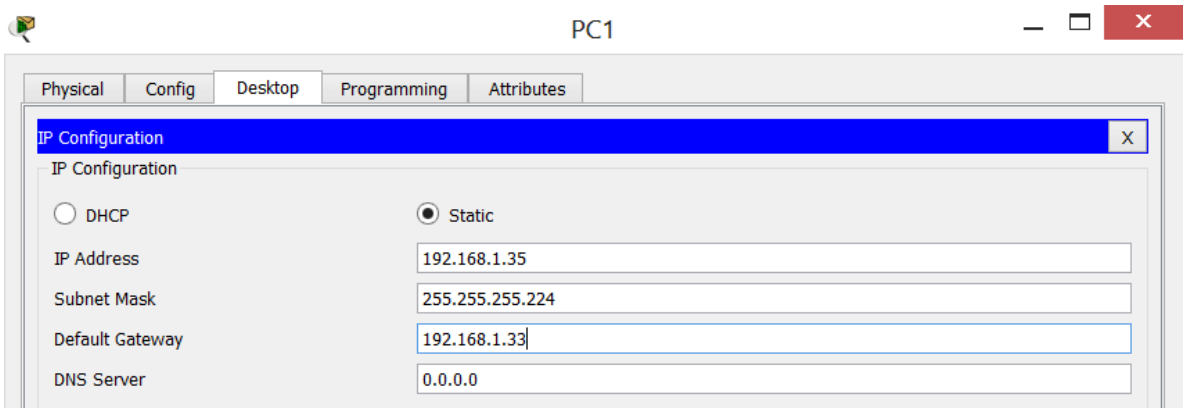


Ilustración 2 Configuración Pc Medellín

IP PC 0 MEDELLIN



IP PC 1 MEDELLIN

6.2 Parte 2: Configuración Básica.

a. Completar la siguiente tabla con la configuración básica de los routers, teniendo en cuenta las subredes diseñadas.

	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		192.168.1.130	
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

tabla de direccionamiento con protocolo EIGRP

b. Después de cargada la configuración en los dispositivos, verificar la tabla de enrutamiento en cada uno de los routers para comprobar las redes y sus rutas.

La mejor forma para comprobar que se logró configurar apropiadamente cada uno de los router con respecto a la tabla con el comando **show ip interface brief**:

Show ip interface brief – router Medellín

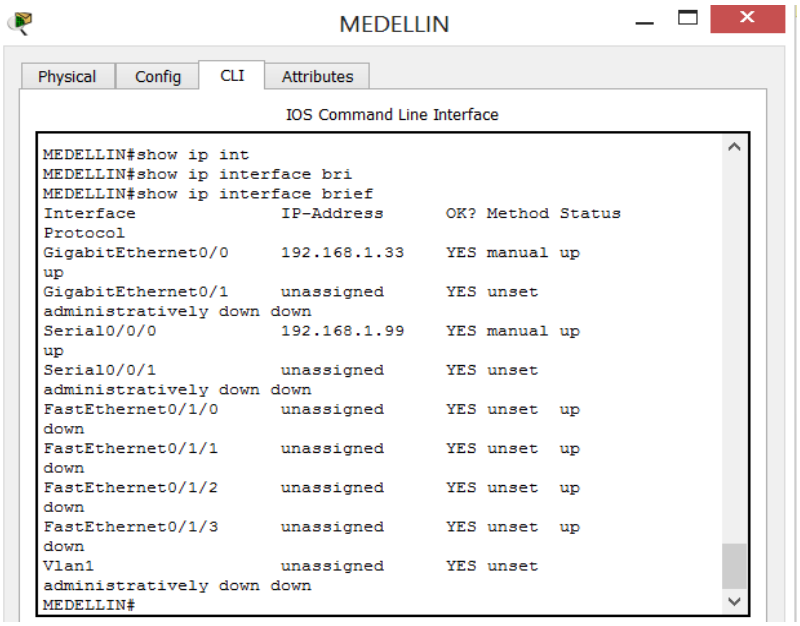


Ilustración 3 Configuración Router Medellín

Show ip interface brief – router Bogotá

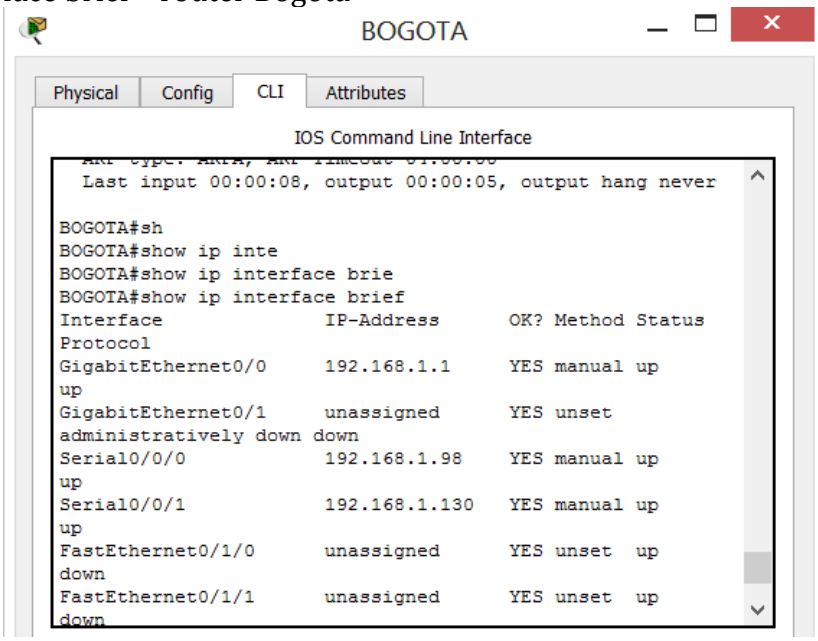


Ilustración 4 Configuración Router Bogotá

Show ip interface brief – router Cali

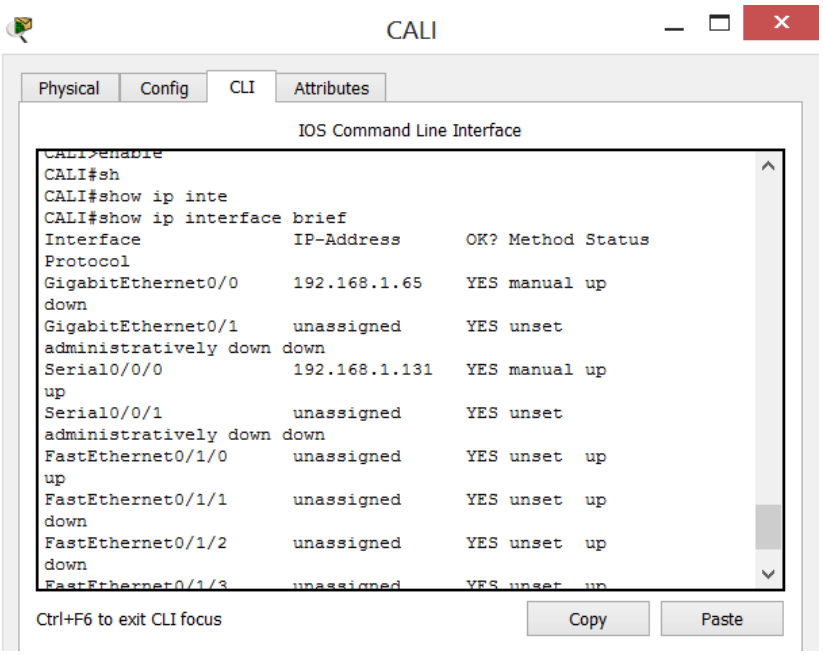


Ilustración 5 Configuración Router Cali

c. Verificar el balanceo de carga que presentan los router.

El balanceo de cargas de los router se realiza con el comando **show ip route:**

Show IP router – Medellín

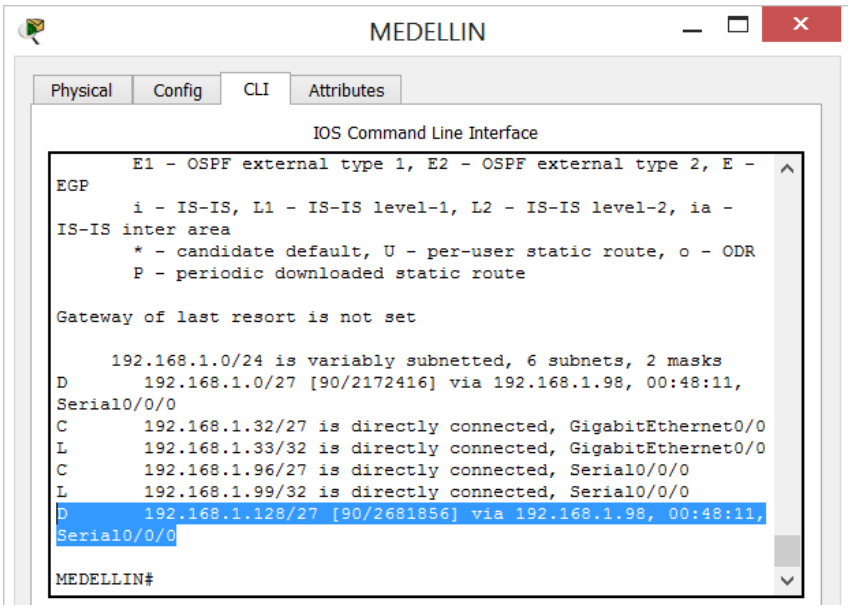


Ilustración 6 Configuración Show IP Router Bogotá

Show IP router – Bogotá

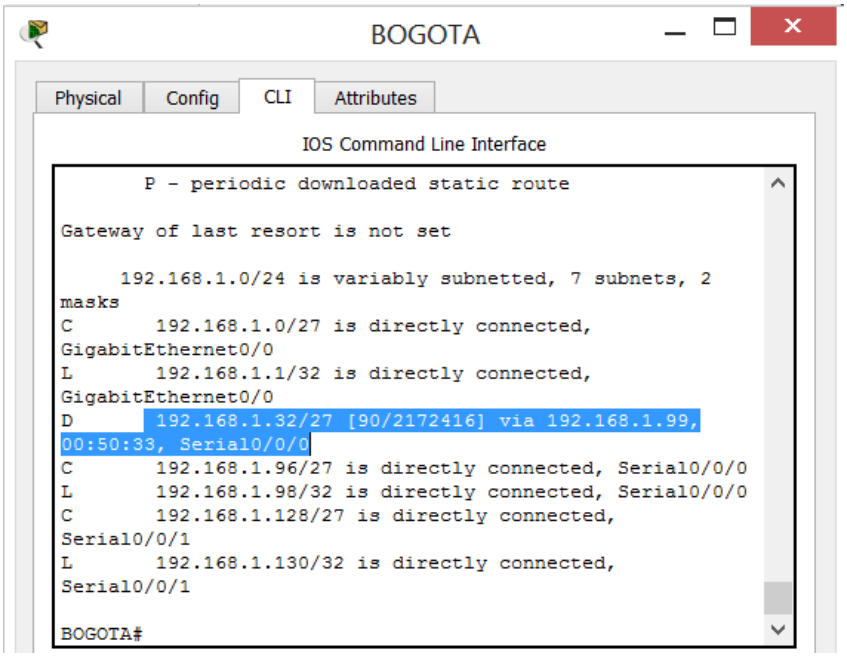


Ilustración 7 Configuración Show IP Router Bogotá

Show IP router – Cali

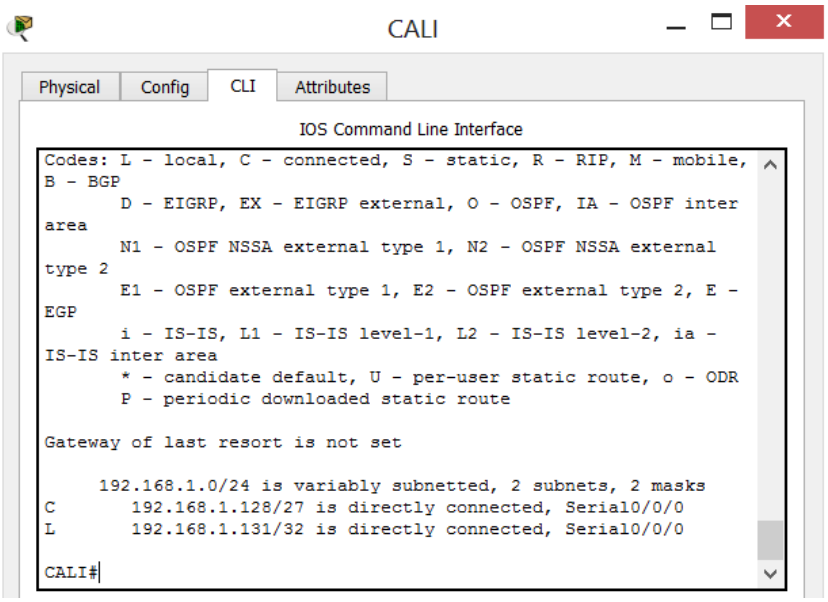


Ilustración 8 Configuración Show IP Router Cali

d. Realizar un diagnóstico de vecinos usando el comando cdp.

Es probable que debido a que en ningún momento se usó el comando **cdp run** en ninguna interfaz la salida es negativa:

Salida del comando **show cdp** interface

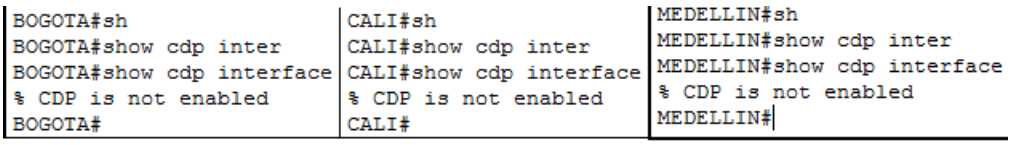


Ilustración 9 comando show cdp interface

e. Realizar una prueba de conectividad en cada tramo de la ruta usando Ping.

Ping fallido entre el pc 1, red Medellín y router Cali

```
C:\>ping 192.168.1.65

Pinging 192.168.1.65 with 32 bytes of data:

Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.

Ping statistics for 192.168.1.65:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Ilustración 10 Ping Medellín-Cali

Ping correcto entre la red Medellín

```
C:\>ping 192.168.1.34

Pinging 192.168.1.34 with 32 bytes of data:

Reply from 192.168.1.34: bytes=32 time<1ms TTL=128
Reply from 192.168.1.34: bytes=32 time<1ms TTL=128
Reply from 192.168.1.34: bytes=32 time<1ms TTL=128
Reply from 192.168.1.34: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.34:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

```
C:\>ping 192.168.1.33

Pinging 192.168.1.33 with 32 bytes of data:

Reply from 192.168.1.33: bytes=32 time<1ms TTL=255
Reply from 192.168.1.33: bytes=32 time<1ms TTL=255
Reply from 192.168.1.33: bytes=32 time<1ms TTL=255
Reply from 192.168.1.33: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.33:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Ilustración 11 Ping entre la red de Medellín

Ping correcto entre PC WS 1 y servidor red Bogotá

```
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

```
C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time=4ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 4ms, Average = 1ms
```

Ilustración 12 Ping red Bogotá

Ping correcto entre la red de Cali

```
C:\>ping 192.168.1.66

Pinging 192.168.1.66 with 32 bytes of data:

Reply from 192.168.1.66: bytes=32 time<1ms TTL=128
Reply from 192.168.1.66: bytes=32 time<1ms TTL=128
Reply from 192.168.1.66: bytes=32 time<1ms TTL=128
Reply from 192.168.1.66: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.66:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Ilustración 13 Ping red Cali

6.3 Parte 3: Configuración de Enrutamiento.

a. Asignar el protocolo de enrutamiento EIGRP a los router considerando el direccionamiento diseñado.

Aunque los dispositivos cuentan con las direcciones IP de la tabla anterior, se debe iniciar el protocolo de comunicación **EIGRP** en cada uno de los router:

- Protocolo **EIGRP** router Medellín,

MEDELLIN(config)#int s0/0/0
MEDELLIN(config-if)#clock rate 64000
MEDELLIN(config -if)frouter eigrp 200
MEDELLIN(config-router)#192.168.1.33 0.0.0.31
Invalid input detected at "" marker.
MEDELLIN(config-router)#network 192.168.1.33 0.0.0.31
MEDELLIN(config-router)#network 192.168.1.99 0.0.0.31
MEDELLIN(config-router)#no auto
MEDELLIN(config-router)#no auto-summary

En la configuración anterior se evidencia como al puerto serial 0/0/0 se le configura (únicamente en el extremo de Medellín) el reloj de 64.000, para verificar en cuál de los dos extremos se debe configurar el reloj se puede en packet tracer ubicar el puntero del cursor y únicamente en uno de ellos se verá reflejado un pequeño reloj:

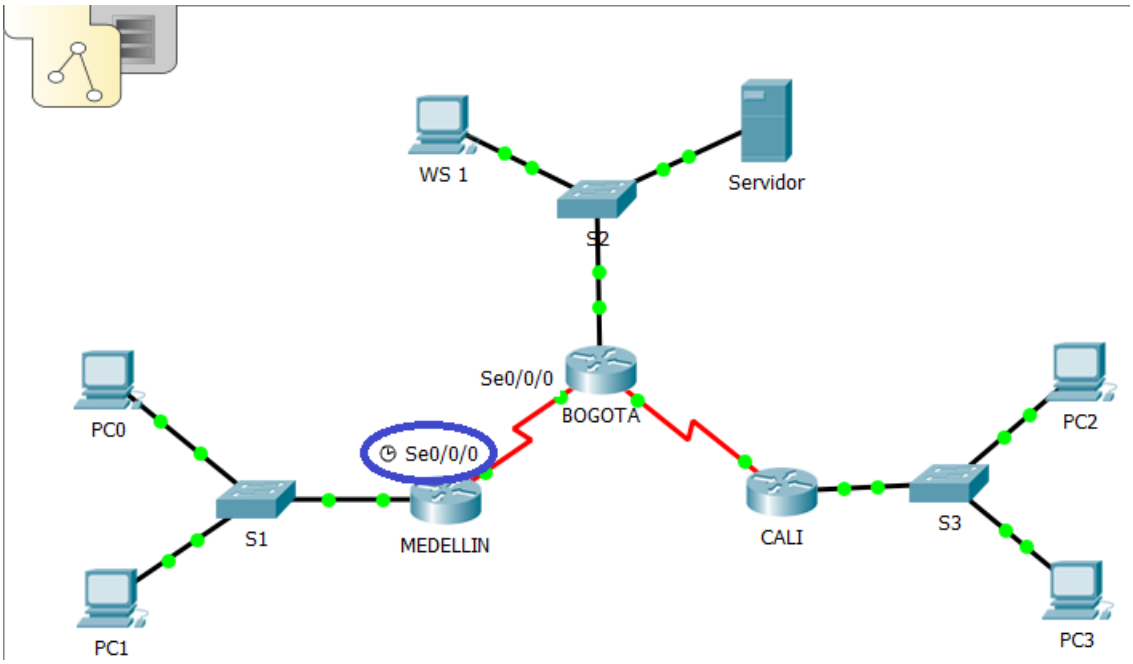


Ilustración 14 Topologia Protocolo EIGRP

Imagen, Topología que evidencia el pin al que se debe configurar el reloj

Para la configuración del protocolo EIGRP del router Bogotá y Cali tenemos:

- Protocolo EIGRP router Bogotá

BOGOTA(config)frouter eigrp 200

BOGOTA(config-router)#net

BOGOTA(config-router)#network 192.168.1.1 0.0.0.224 EIGRP: Invalid address/mask combination (discontiguous mask)

BOGOTA(config-router)#network 192.168.1.130 0.0.0.31

BOGOTA(config-router)#network 192.168.1.1 0.0.0.31

BOGOTA(config-router)#network 192.168.1.98 0.0.0.31

BOGOTA(config-router)#no auto

BOGOTA(config-router)#no auto-summary

- Protocolo EIGRP router Cali

CAL/>enable CALI#config t Enter configuration commands, one per line. End with CNTL/Z. CAL/(config)#router eigrp 200

CALI(config-router)#net

CALI(config-router)#network 192.168.1.65 0.0.0.31

CALI(config-router)inetwork 192.168.1.131 0.0.0.31

CALI(config-router)# %DDAL-5-NBRCHANGE: IP-EIGRP 200: Neighbor 192.168.1.130 (Seria10/0/0) is up: new adjacency

b. Verificar si existe vecindad con los routers configurados con EIGRP.

Para la verificación se hace uso del comando **show ip eigrp neighbors [número del sistema autónomo]** donde el número del sistema autónomo es **200** según la tabla dada:

- Vecindad de router con protocolo EIGRP en los tres router como se muestra en la imagen siguiente.

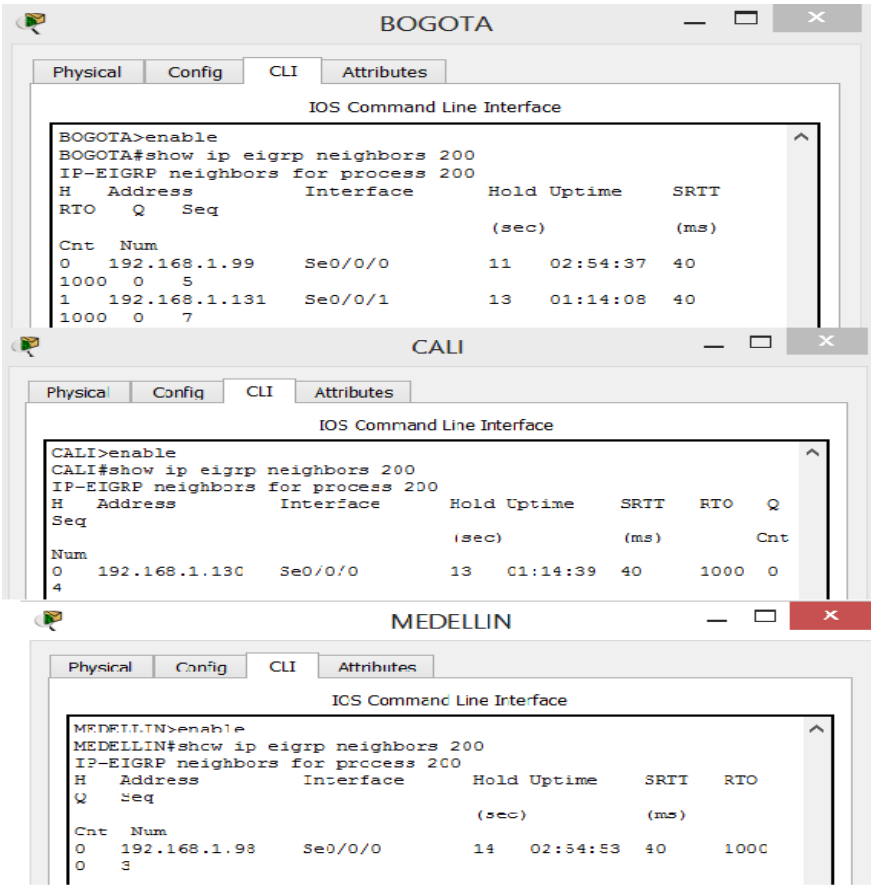


Ilustración 15 show ip eigrp neighbors Bogotá, Cali, Medellín

c. Realizar la comprobación de las tablas de enrutamiento en cada uno de los routers para verificar cada una de las rutas establecidas.

Se realiza mediante el comando **show ip eigrp topology 200:**

- Verificación tablas de enrutamiento de los tres router.

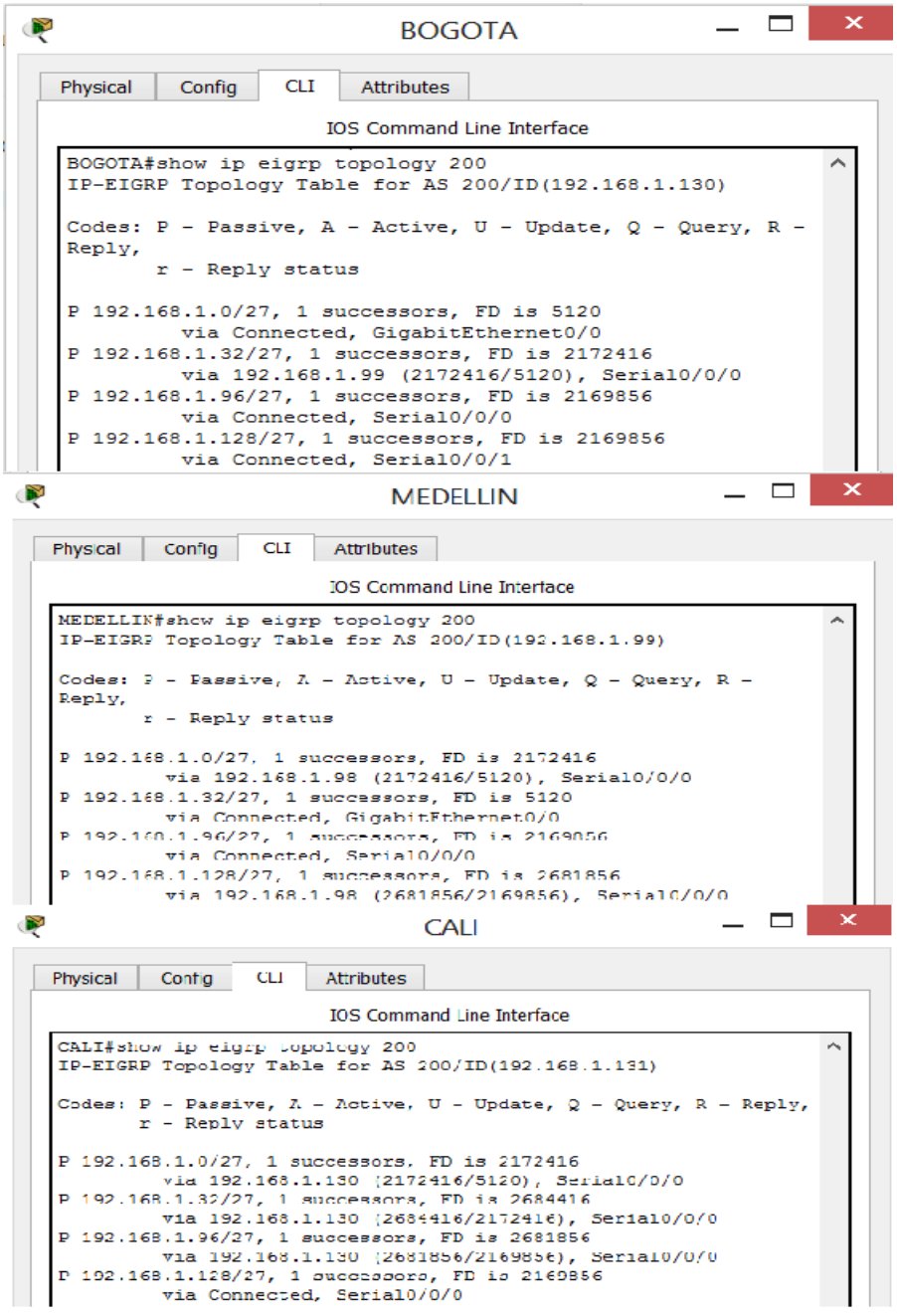


Ilustración 16 verificación show ip eigrp topology 200

d. Realizar un diagnóstico para comprobar que cada uno de los puntos de la red se puedan ver y tengan conectividad entre sí. Realizar esta prueba desde un host de la red LAN del router CALI, primero a la red de MEDELLIN y luego al servidor.

La forma más adecuada para poder lograr la verificación es por medio de **ping** en cualquier host de la red de CALI, para estos efectos desde el PC2 a la PC0 que pertenece a la red de MEDELLIN. Para ello se muestra la dirección IP asignada en el PC0 dada por:

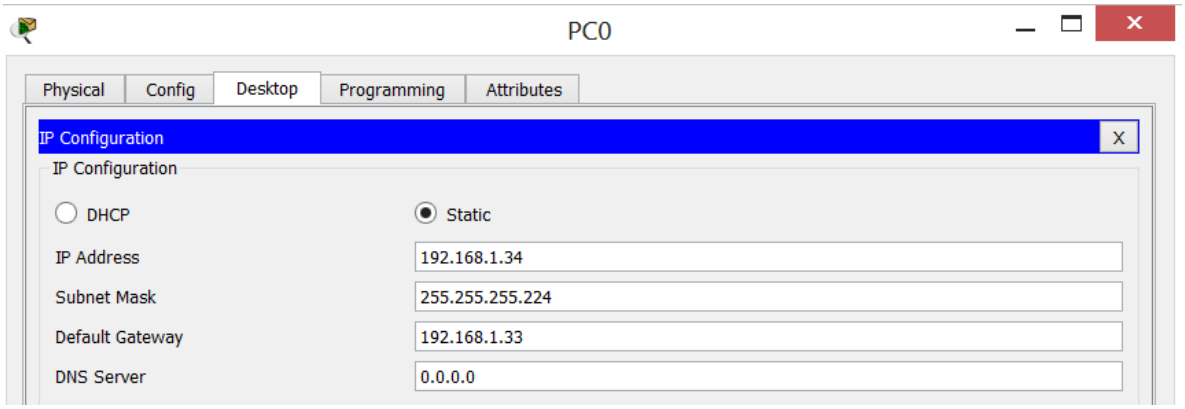


Ilustración 17 Dirección IP pc0

Dirección IP del PC0 en la red de MEDELLIN

El siguiente paso es acceder a la consola del PC2 (perteneciente a la red CALI) y hacer ping:

Ping que se realiza exitoso entre PC2 RED Cali y PC0 red MEDELLIN

De la misma forma se toma la dirección IP del servidor de la red BOGOTA para hacer desde el mismo PC2 ping:

```
C:\>ping 192.168.1.34

Pinging 192.168.1.34 with 32 bytes of data:

Reply from 192.168.1.34: bytes=32 time=2ms TTL=125
Reply from 192.168.1.34: bytes=32 time=2ms TTL=125
Reply from 192.168.1.34: bytes=32 time=2ms TTL=125
Reply from 192.168.1.34: bytes=32 time=5ms TTL=125

Ping statistics for 192.168.1.34:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 5ms, Average = 2ms
```

Ilustración 18 Ping Cali-Medellín

Ping que se realiza exitoso entre PC2 RED Cali y Servidor red BOGOTA

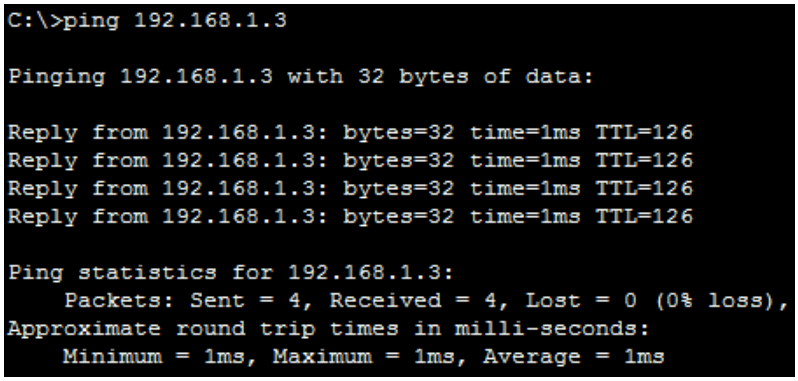


Ilustración 19 Ping Cali-Bogotá

6.4 Parte 4: Configuración de las listas de Control de Acceso.

En este momento cualquier usuario de la red tiene acceso a todos sus dispositivos y estaciones de trabajo.

El jefe de redes le solicita implementar seguridad en la red. Para esta labor se decide configurar listas de control de acceso (ACL) a los routers.

Las condiciones para crear las ACL son las siguientes:

a. Cada router debe estar habilitado para establecer conexiones Telnet con los demás routers y tener acceso a cualquier dispositivo en la red.

Para las conexiones telnet se hace uso de la VLAN 1 y se configura la clave como

MEDELLIN para el primer router:

MEDELLIN4config t

Enter configuration commands, one per line. End with CNTL/Z.

MEDELLIN(config)#int

MEDELLIN(config)#interface vlan 1

MEDELLIN(config-if)#ip add

MEDELLIN(config-if)#ip address 192.168.1.99 255.255.255.224 % 192.168.1.96 overlaps with Seria10/0/0
MEDELLIN(config-if)#no shu
MEDELLIN(config-if)#no shutdown
MEDELLIN(config-if)# IMINK-5-CHANGED: Interface Vlanl, changed state to up
11I.INEPROTO-S-UPDOWN: Line protocol on Interface Vlanl, changed state to up
MEDELLIN(config-if)#exit
MEDELLIN(config)#1ine vty 0 15
MEDELLIN(config-line)#trans
MEDELLIN(config-line)#transport input tel
MEDELLIN(config-line)#transport input telnet
MEDELLIN(config-line)#pass
MEDELLIN(config-line)#password MEDELLIN 1MEDELLIN(config -line)Slogin IIEDELLIN(config-line)#exit
MEDELLIN(config)#

Después de la configuración, se puede desde cualquier computador de otra red acceder mediante telnet, lo primero es realizar ping al puerto y de ser exitoso desde la consola escribir **ping [dirección IP del router configurado para telnet]:**

Conexión Telnet correcta entre PC2 (red CALI) y router MEDELLIN

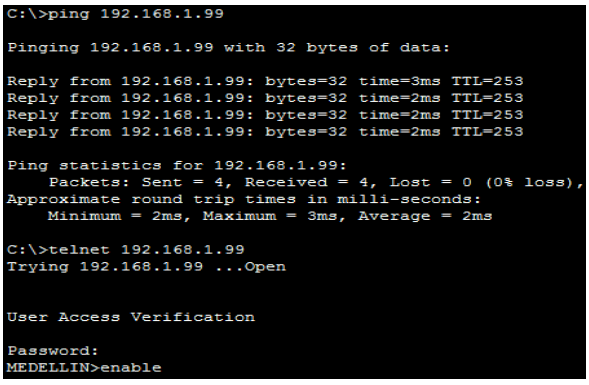


Ilustración 20 Conexión Telnet

En la anterior configuración se tiene la configuración para Bogotá.

BOGOTA#config t
Enter configuration commands, one per line. End with CRTL/Z.
BOGOTA(config)#int elan 1
BOGOTA(config-if)#ip add
BOGOTAiconfig-21)#ip address 192.168.1.98 266.266.266.229 I 192.168.1.96 overlaps with Serla10/0/0
BOGOTA(config-if)#no shut
BOGOTA(config-if)#no shutdown
BOGOTAlconfig-if)# ILINX-S-CHANGED: Interface Vlanl, changed state to up
SLINEPROTO-S-OPDOWN: Line protocol on Interface Vlani, changed state to up
BOGOTA(config-If)#exit
BOGOTA(config)#line vty 0 I5
BOGOTA(eonfig-line)#tran
BOGOTA(config-line)#transport input telnet
BOGOTAIconflg-line)#paas BOGOTA4config-line)dpassword BOGOTA
BOGOTA(config-11ne)#login
BCGOTAIcontig-line)#exit

como prueba se toma un PC de la red de Cali o Medellín:

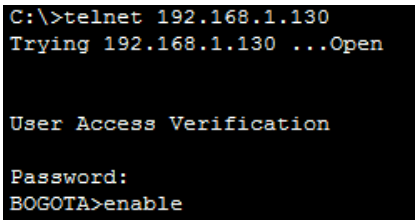


Ilustración 21 Acceso de verificación Bogotá

Es válido aclarar que debido a que en el router BOGOTA se tiene dos redes que conectan entre Medellín y Cali, se puede configurar las líneas vty para ambas direcciones IP. Para el tercer router, la configuración de la ip 192.168.1.131:

Configuración router CALI – telnet

CALI>enable

CALI#contig t

Ent*: configuration commands, one per line. End with 61/TL/2.

CALI(config)#int vlan 1

CALI(config-If)#ip add

CALl(config-ip)#ip address 192.268.1.131 255.255.255.224 % 192.160.1.128 overlaps with Serial10/0/0

CALI(config -If)#no shut

CALI(config-if)#no shutdown

CALI1conftg-Ifla %LINK -a-CHANCED: Interface Vital, changed state to up

%LINEPROTO-S-UPDOMM: Line protocol on Interface Vlanl, changed state to up

CALI(config-if)#exit

CALI(config)#

CALI(config)#line vty 0 I5

CALl(config-line)#trans

CaLl(config-line)#transport input telnet

CALI(config-line)#pass

CALl(config-line)#password CALI

CALI(config-line)#login

CALI(config-line)#exit

Conexión por Telnet

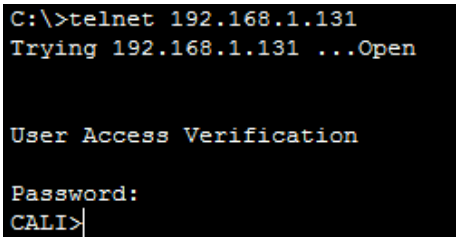


Ilustración 22 Configuración Telnet Cali

b. El equipo WS1 y el servidor se encuentran en la subred de administración. Solo el servidor de la subred de administración debe tener acceso a cualquier otro dispositivo en cualquier parte de la red.

Configuración SW

BOGOTA>enable

BOGOTA#config t

Enter configuration commands, one per line. End with CNTL/Z.

BOGOTA(config)#int g0/0 BOGOTA(config-if)#no ip acc

BOGOTA(config-if)#no ip access-group ListaDeAcceso out

BOGOTA(config-if)#ipacc

BOGOTA(config-if)#ip acc

BOGOTA(config-if)#ip access-group ListaDeAcceso in

BOGOTA(config-if)#no ip access-group ListaDeAcceso in

BOGOTA(config-if)#ip access-group ListaDeAcceso out

BOGOTA(config-if)#no ip access-group ListaDeAcceso out

BOGOTA(config-if)#ip access-group ListaDeAcceso out

BOGOTA(config-ifltno ip access-group ListaDeAcceso out

BOGOTA(config-if)#ip access-group ListaDeAcceso out

BOGOTA(config-if)#exit

BOGOTA(config)#ip acc

BOGOTA(config)#ip access-list scan

BOGOTA(config)#ip access-list standard Lista

BOGOTA(config-std-nac1)#permit host 192.167.1.2

BOGOTA(config-std-nac1)#permit host 192.167.1.3

BOGOTA(config-std-nac1)#exit

BOGOTA(config)#int g0/0

c. Las estaciones de trabajo en las LAN de MEDELLIN y CALI no deben tener acceso a ningún dispositivo fuera de su subred, excepto para interconectar con el servidor.

CALI#config t

Enter configuration commands, one per line. End with CNTL/Z.

CALI(config)#ip acc

CALI(config)#ip access-list stan

CALI(config)#ip access-list standard ListaCali

CALI(config-std-nac1)#permit host 192.168.1.66

CALI(config-std-nac1)#permit host 192.168.1.67

CALI(config-std-nac1)#deny any

CALI(config-std-nac1)#exit

CALI(config)#int g0/0

CALI(config-if)#ip acc

CALI(config-if)#ip access-group ListaCali out

CALI(config-if)#

6.5 Parte 5: Comprobación de la red instalada.

a. Se debe probar que la configuración de las listas de acceso fue exitosa.

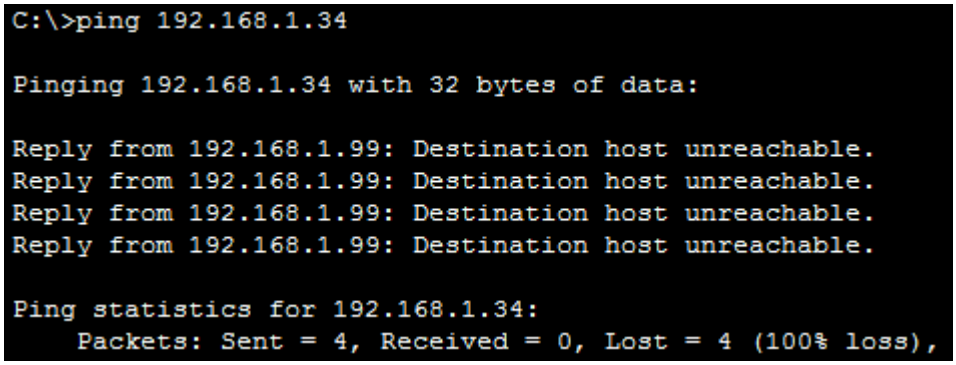


Ilustración 23 Ping Pc2-Pc0

Resultado de ping Entre PC2 y PC0

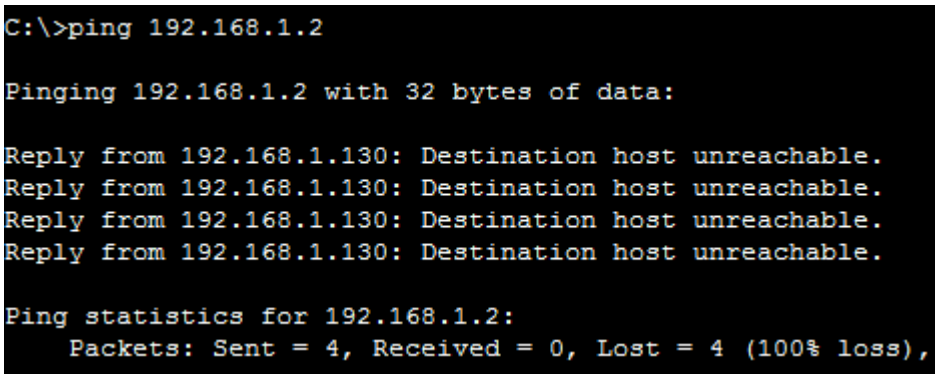


Ilustración 24 Ping Pc2-Servidor

Ping entre PC2 y servidor

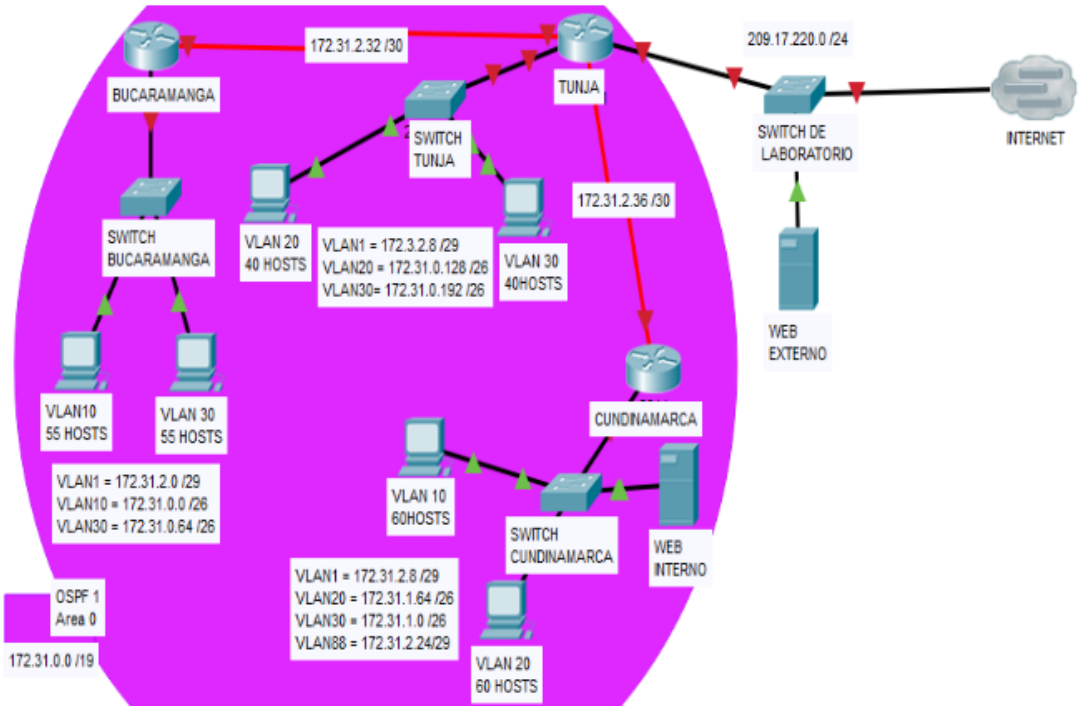
b. Comprobar y Completar la siguiente tabla de condiciones de prueba para confirmar el óptimo funcionamiento de la red e.

	ORIGEN	DESTINO	RESULTADO
TELNET	Router MEDELLIN	Router CALI	CORRECTO
	WS_1	Router BOGOTA	CORRECTO
	Servidor	Router CALI	CORRECTO
	Servidor	Router Medellin	CORRECTO
TELNET	Lan del Router MEDELLIN	Router CALI	CORRECTO
	LAN del Router CALI	Router CALI	INCORRECTO
	LAN del Router MEDELLIN	Router Medellin	INCORRECTO
	LAN del Router CALI	Router Medellin	CORRECTO
PING	LAN del Router CALI	WS_1	INCORRECTO
	LAN del Router MEDELLIN	WS_1	INCORRECTO
	LAN del Router MEDELLIN	LAN del Router CALI	INCORRECTO
PING	LAN del Router CALI	Servidor	INCORRECTO
	LAN del Router MEDELLIN	Servidor	INCORRECTO
	Servidor	LAN del Router MEDELLIN	CORRECTO

	Servidor	LAN del Router CALI	CORRECTO
	Router CALI	LAN del Router MEDELLIN	INCORRECTO
	Router Medellín	LAN del Router CALI	INCORRECTO

7 DESARROLLO ESCENARIO 2

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



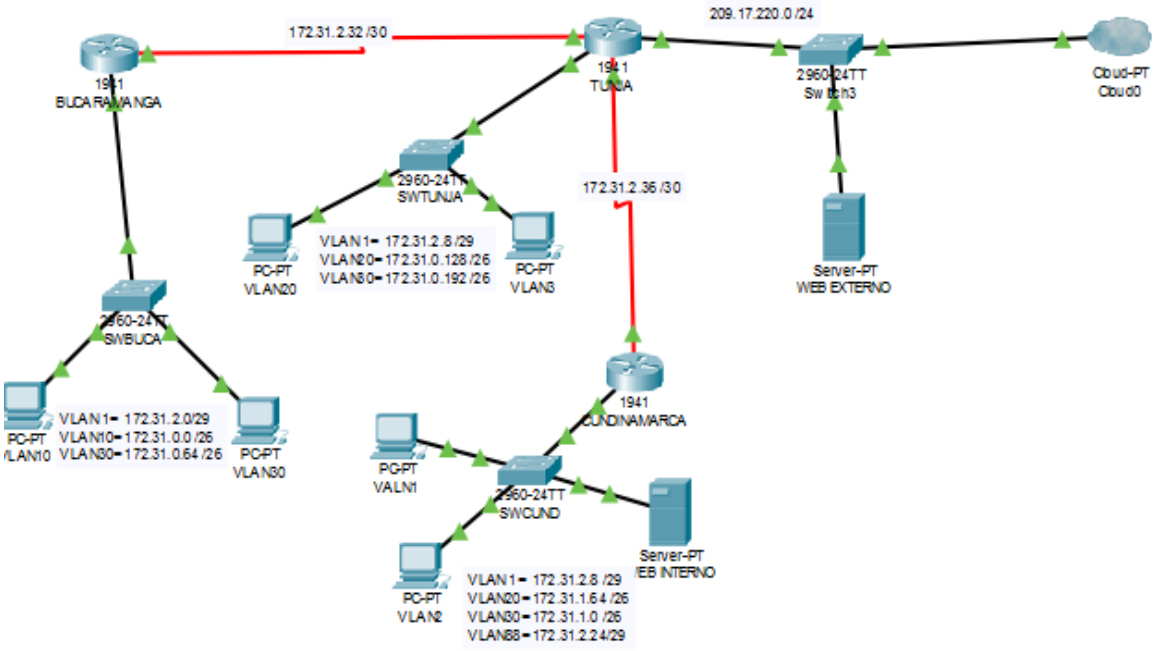


Ilustración 25 Escenario 2

7.1 Desarrollo

Los siguientes son los requerimientos necesarios:

1. Todos los router deberán tener los siguiente:

• Configuración básica.
• Autenticación local con AAA.
• Cifrado de contraseñas.
• Un máximo de internos para acceder al router.
• Máximo tiempo de acceso al detectar ataques.
• Establezca un servidor TFTP y almacene todos los archivos necesarios de los router.

7.1.1 Configuración Básica

Configuración básica Tunja.

Router>enable
RouterSconfig t
Enter configuration commands, one per line. End with CNTL/2.
Router(config)#no ip domain-loo
Router(config)#no ip domain-lookup
Router(config)#enable pass

Router(config)#enable password AAA
Router(config)#line console 0
Router(config-line)#pass
Roucer(confic-line)#password AAA
Router(coneia-line)#loggin
Roucer(conflo-line)#loggin sybch
Roucer(contlg-line)#logging synch
Roucer(coneig-line)#logging synchronous
Roucer(config-line)#exit
Router(config)#hossname TUNJA
TUNJA(config)#exit
TUNJA#
%SYS -S -CONFIG_I: Configured from console by console
TUNJA#copy run
TUNJA#copy running -config star
TUNJA#copy running-config startup-config
Destination filename (startup-config)?

Configuración básica Bucaramanga

Router#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip dome
Router(config)#no ip domain-loo
Router(config)#no Sp domain-lookup
Router(config)#enable pass
Router(config)#enable password AAA
Router (config)#line consol
Router(config)#line console 0
Router(config-line)#pass
Router(config-line)#password cisco
Router(config-line)#logg
Router(config-line)#logging asy
Router(config-line)#logging syncr
Router(config-line)#logging synchronous
Router(config-line)#exit
Router(config)#ser
Router(config)#service pass
Router(config)#service password-encryption
Router(config)#copy run

Router(config)#copy runn
Router (config)#exit
Router#
%SES-5-CONFIG_I: Configured from console by console

Configuración básica Cundinamarca

Router>enable
Router#config t
Enter configuration commands, one per line. End with CNTL/2.
Router(config)#no ip domain-loo
Router(config)#no ip domain-lookup
Router(config)#enable pass
Router(config)#enable password AAA
Router(config)#line console 0
Router(config-line)#pass
Router(config-line)#password AAA
Router(config-line)#loggin
Router(config-line)#loggin sybch
Router(config-line)#logging synch
Router(config-line)#logging synchronous
Router(config-line)#exit
Router(config)#hossname CUNDINAMARCA
CUNDINAMARCA(config)#exit
CUNDINAMARCA #

7.1.2 Autenticación local con AAA.

TUNJA(config)#aaa new-model
TUNJA(config)#username Admin1 secret ozkr636
TUNJA(config)#aaa authentication login default group tacacs+ local
TUNJA(config)#tacacs-server host 192.168.2.2
TUNJA(config)#tacacs-server key tacacspa55
TUNJA(config)#exit
TUNJA#

BUCARAMANGA(config)#aaa new-model
BUCARAMANGA(config)#username Admin1 secret ozkr636

```
BUCARAMANGA(config)#aaa authentication login default group tacacs+ local
BUCARAMANGA(config)#tacacs-server host 192.168.2.2
BUCARAMANGA(config)#tacacs-server key tacacspa55
BUCARAMANGA(config)#exit
BUCARAMANGA#


CUNDINAMARCA(config)#aaa new-model
CUNDINAMARCA(config)#username Admin1 secret ozkr636
CUNDINAMARCA(config)#aaa authentication login default group tacacs+ local
CUNDINAMARCA(config)#tacacs-server host 192.168.2.2
CUNDINAMARCA(config)#tacacs-server key tacacspa55
CUNDINAMARCA(config)#exit
CUNDINAMARCA#
```

7.1.3 Cifrado de contraseñas.

```
TUNJA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
TUNJA(config)#service password-encryption
TUNJA(config)#end
TUNJA#show running-config
%SYS-5-CONFIG_I: Configured from console by console

BUCARAMANGA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
BUCARAMANGA(config)#service password-encryption
BUCARAMANGA(config)#end
BUCARAMANGA#show running-config
%SYS-5-CONFIG_I: Configured from console by console

CUNDINAMARCA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
CUNDINAMARCA(config)#service password-encryption
CUNDINAMARCA(config)#end
CUNDINAMARCA#show running-config
%SYS-5-CONFIG_I: Configured from console by console
```

Antes de continuar con las configuraciones básicas se debe crear en cada switch las diversas VLAN solicitadas, por ejemplo, el **switch Bucaramanga** tiene tres vlan las cuales asignaremos a los puertos físicos.

7.2 Configuración VLAN

7.2.1 switch Bucaramanga

Switch#config t
Enter configuration commands, one per line. End with OffL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#name VLAN10
Switch(config-vlan)#exit
Switch(config)#int f0/1
Switch(config-if)#switch
Switch(config-if)#switchport mode acc
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#exit
Switch(confiq)#vlan 1
Switch(config-vlan)#name VLAN1
Default VLAN 1 may not have its name changed.
Switch(config-vlan)#exit
Switch(config)#vlan 30
Switch(config-vlan)#name VLAN30
Switch(config-vlan)#exit
Switch(config)#int f0/2
Switch(config-if)switch
Switch(config-if)#switchport mode acc
Switch(config-If)#switchport mode access
switch(config-if)#switchport access vlan 30
Switch(config-lf)#exit

7.2.2 Switch Tunja

Switch#config te
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 1
switch(config-vlan)#name VLAN1
Default VIAN 1 may not have its name changed.
Switch(config-vlan)#exit
switch(config)#vlan 20
switch(config-vlan)#name VLAN20
switch(config-vlan)#exit
Switch(config)#int f0/2

switch(config-if)#switch
switch(config-if)#switchport mode acc
switch(config-if)#witchport mode access
switch(config-if)#switchport access vlan 20
Switch(config-if)#exit
switch(config)#vlan 30
switch(config-vlan)#nameVLAN30
switch(config-vlan)#exit
switch(config)#int f0/3
switch(config-if)#switch
Switch(config-if)#switchport mode acc
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 90
Switch(config-if)#exit

7.2.3 Switch Cundinamarca

Switch(config)#vlan 1
Switch(config-vlan)#name VLAN1
Default VLAN 1 may not have its name changed.
switch(config-vlan)#exit
Switch(config)#vlan 20
Switch(config-vlan)#name VLAN20
Switch(config-vlan)#exit
Switch(config)#vlan 30
Switch(config-vlan)#name VLAN30
Switch(config-vlan)#exit
Switch(config)#vlan 88
Switch(config-vlan)#name VLAN88
Switch(config-vlan)#exit
Switch(Config)#int f0/2
Switch(config-if)#swit
Switch(config-if)#switchport mode acce
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
% Access VLAN does not exist. Creating flan 10

7.3 Habilitar VLAN en cada switch y permitir su enrutamiento

7.3.1 Router Bucaramanga

G0/0

BUCARAMANGA(config)#int g0/0
BUCARAMANGA(config-if)#ip add
BUCARAMANGA(config-if)#ip address 172.31.0.1 255.255.225.192 Bad mask OxFFFFE1C0 for address 172.31.0.1
BUCARAMANGA(config-if)#ip address 172.31.0.1 255.255.255.192
BUCARAMANGA(config-if)#no shu
BUCARAMANGA(config-if)#no shutdown
BUCARAHANGA(config-if)# %LINK -5 -CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
BUCARAMANGA (conf ig-if)#1

Router Bucaramanga SO/0/0

BUCARAMANGA>enable
Password:
BUCARAMANGA#config t
Enter configuration commands, one per line. End with CNTL/Z.
BUCARAMANGA(config)#int s0/0/0
BUCARAMANGA(config-if)#descri
BUCARAMANGA(config-if)#description conn
BUCARAMANGA(config-if)#description connectio
BUCARAMANGA(config-if)#ip add
BUCARAMANGA(config-if)#ip address 172.31.2.33 255.255.255.252
BUCARAMANGA(config-if)#no shut
BUCARAMANGA(config-if)#clock rate 128000
BUCARAMANGA(config-if)#no shut
BUCARAMANGA(config-if)#no shutdown
%LINK -5 -CHANGED: Interface Seria10/0/0, changed state to down B
UCARAMANGA(config -if)#

7.3.2 Router Tunja

s0/0/0

TUNJA>enable
Password:
TUNJA#config t Enter configuration commands, one per line. End with CNTL/Z.
TUNJA(config)#int s0/0/0
TUNJA(config-if)#ip add
TUNJA(config-if)#ip address 172.31.2.34 255.255.255.252
TUNJA(config-if)#no shut

TUNJA(config-if)#no shutdown
TUNJA(config-if)# %LINK-5-CHANGED: Interface Seria10/0/0, changed state to up
TUNJA(config-if)# %LINEPROTO-5-UPDOWN: Line protocol on Interface Seria10/0/0, changed state to up
TUNJA#(config-if)#

Router Tunja puerto S0/0/1

TUNJA(config)#int s0/0/1
TUNJA(config-if)flp add
TUNJA(config-if)flp address 172.31.2.36 255.255.255.252
Bad mask /30 for address 172.31.2.36
TUNJA(config-if)flp address 172.31.2.37 255.255.255.252
TUNJA(config-if)#clock rate 128000
TUNJA(config-if)#no shut
TUNJA(config-if)#no shutdown
%LINK-5-CHANGED: Interface Seria10/0/1, changed state to down
TUNJA(config-if)#exit
TUNJA(config)#

Router Tunja puerto G0/0

TUNJA(config)#int s0/0/1
TUNJA(config-if)flp add
TUNJA(config-if)flp address 172.31.2.36 255.255.255.252
Bad mask /30 for address 172.31.2.36
TUNJA(config-if)flp address 172.31.2.37 255.255.255.252
TUNJA(config-if)#clock rate 128000
TUNJA(config-if)#no shut
TUNJA(config-if)#no shutdown
%LINK-5-CHANGED: Interface Seria10/0/1, changed state to down
TUNJA(config-if)#exit
TUNJA(config)#

Router Tunja Puerto G0/1

TUNJA(config)#int g0/1
TUNJA(config-if)#209.17.220.1 255.255.255.0
% Invalid input detected at 1^1 marker.
TUNJA(config-if)#ip add209.17.220.1 255.255.255.0
TUNJA(config-if)#ip address 209.17.220.1 255.255.255.0
TUNJA(config-if)#no shut TUNJA(config-if)#no shutdown
TUNJA(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
TUNJA (config-if)#exit

TUNJA (config)#

7.3.3 Router Cundinamarca

S0/0/0

CUNDINAMARCA>enable
Password:
CUNDINAMARCA#config t Enter configuration commands, one per line. End with CNTL/Z.
CUNDINAMARCA(config)#int s0/0/0
CUNDINAMARCA(config-if)#ip add
CUNDINAMARCA(config-if)#ip address 172.31.2.38 255.255.255.252
CUNDINAMARCA(config-if)#no shut
CUNDINAMARCA(config-if)#no shutdown
CUNDINAMARCA(config-ifl# %LINK-5-CHANGED: Interface Seria10/0/0, changed state to up
CUNDINAMARCA(config-if)#1

Router Cundinamarca – interfaz G0/0

CUNDINAMARCA(config)#int g0/0
CUNDINAMARCA(config-if)tip add
CUNDINAMARCA(config-if)#ip address 172.31.1.1 255.255.255.192
CUNDINAMARCA(config-if)#no shut
CUNDINAMARCA(config-if)#no shutdown
CUNDINAMARCA(config-if)#
%I.INK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
CUNDINAMARCA(config -if)#

Switch Red Bucaramanga – config VLAN 10

Switch(config)#int vlan 10
Switch(config-if)# %LINK-5-CHANGED: Interface Vlan10, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to up
Switch(config-if)#ip add
Switch(config-if)#ip address 172.31.0.2 255.255.255.192
Switch(config-if)#exit
Switch(config)#ip defa
Switch(config)#ip default-gateway 172.31.0.1 255.255.255.192
% Invalid input detected at "" marker.
Switch(config)#ip default-gateway 172.31.0.1
Switch(config)#

Switch Red CUNDINAMARCA – config VLAN 20

Switch(config)#int vlan 20
Switch(config-if)# %LINK-5-CHANGED: Interface Vlan20, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan20, changed state to up
Switch(config-if)#ip address 172.31.1.66 255.255.255.192
Switch(config-if)#exit
Switch(config)#1

Switch Red CUNDINAMARCA – config VLAN 10 y 88

Switch(config-if)#ip address 172.31.1.66 255.255.255.192
Switch(config-if)#exit
Switch(config)#int vlan 10
Switch(config-if)#ip address 172.31.1.2 255.255.255.192
Switch(config-if)#exit
Switch(config)#int vlan 1
Switch(config-if)#ip address 172.31.2.9 255.255.255.248
Switch(config-if)#exit
Switch(config)#vlan 88
Switch(config-vlan)#name VLAN88
Switch(config-vlan)#exit
Switch(config)#int vlan 88
Switch(config-if)# %LINK-5-CHANGED: Interface V1an88,
changed state to up
Switch(config-if)#ip address 172.31.2.25 255.255.255.248
Switch(config-if)#exit
Switch(config)#1

Switch Red CUNDINAMARCA – config VLAN 20 y 30

Switch(config)#int vlan 20
Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan20, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan20, changed state to up
Switch(config-if)#ip address 172.31.0.129 255.255.255.192
Switch(config-if)#exit
Switch(config)#vlan 30
Switch(config-vlan)#name VLAN30
Switch(config-vlan)#exit
Switch(config)#int vlan 30
Switch(config-if)# %LINK-5-CHANGED: Interface Vlan30, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan30, changed state to up
Switch(config-if)#172.31.0.193 255.255.255.192 % Invalid input detected at 1^1 marker.
Switch(config-if)#ip address 172.31.0.193 255.255.255.192

Creación VLAN 1, 20, 30, 88 en Switch Cundinamarca
Como se evidencia en la configuración anterior, al intentar asignar la **VLAN 10** al puerto f0/2 genera error por no existir dicha VLAN, esto debido a un posible error en la gráfica dada por la segunda topología, por lo tanto, se crea otra VLAN y se asigna según corresponde:

Asignación VLAN switch Cundinamarca a los puertos

```
Switch(config)#int f0/2
Switch(config-if)#swit
Switch(config-if)#switchport mode acce
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
I Access wax does not exist. Creating vlan 10
Switch(config-if)#exit
Switch(config)#vlan 10
Switch(config-vlan)#name VLAN10
Switch(config-vlan)#exit
Switch(config)#Int 10/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#exit
Switch(config)#int f0/3
Switch(config-if)#
Switch#
SYS-5-CONFIG_I: Configured from console by console
Switcht#config t
Enter configuration conmands, one per line. End with CNTL/Z.
Switch(config)#int f0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
```

Como paso seguido, se debe configurar el área 0 mediante le protocolo **OSPF** en cada router como:

7.4 Configuración OSPF con autenticación

7.4.1 Router Cundinamarca

```
CUNDINANARCA>enable
Password:
Password:
```

CUNDINAMARCA#config t
Enter configuration commands, one per line. End with CNTL/Z.
CUNDINANARCA(config)#router ospf 20
OSPF process 20 cannot start. There must be at least one "up" IP interface
CUNDINAMARCA(config-router)#networ
CUNDINANARCA(config-router)#network 172.31.0.0 0.0.31.255 area 0
CUNDINAMARCA(config-router)#

7.4.2 Router Bucaramanga

BUCARAMANGA>enable
Password:
BUCARAMANGA#config t
Enter configuration commands, one per line. End with CNTL/Z.
BUCARANANGA(config)#router ospf 1
OSPF process 1 cannot start. There must be at least one "up" IP interface
BUCARAMANGA(config-router)#exit
BUCARAMANGA(config)#router ospf 20
OSPF process 20 cannot start. There must be at least one "up" IP interface
BUCARAMANGA(config-router)#netw
BUCARAMANGA(config-router)#network 172.31.0.0 0.0.31.255 I Incomplete command.
BUCARAMANGA(config-rOuter)#network 172.31.0.0 0.0.31.255 area 0
BUCARAMANGA(Config-router)#

7.4.3 Router Tunja

TUNJA>enable
Password:
TUNJA#config t
Enter Configuration commands, one per line. End with CNTL/Z.
TUNJA(config)frouter ospf 20
OSPF process 20 cannot start. There must be at least one "up" IP interface
TUNJA(config-router).192.31.0.0 0.0.31.255 area 0
% Invalid input detected at 1" marker.
TUNJA(config-router)#network 192.31.0.0 0.0.31.255 area 0
TUNJA(config-router)#

2. El DHCP deberá proporcionar solo direcciones a los hosts de Bucaramanga y Cundinamarca.

7.5 Configuración DHCP

Para poder tener una óptima conectividad con el protocolo DHCP se debe tomar cada host de las redes y que cada uno solicite de manera dinámica las direcciones IP

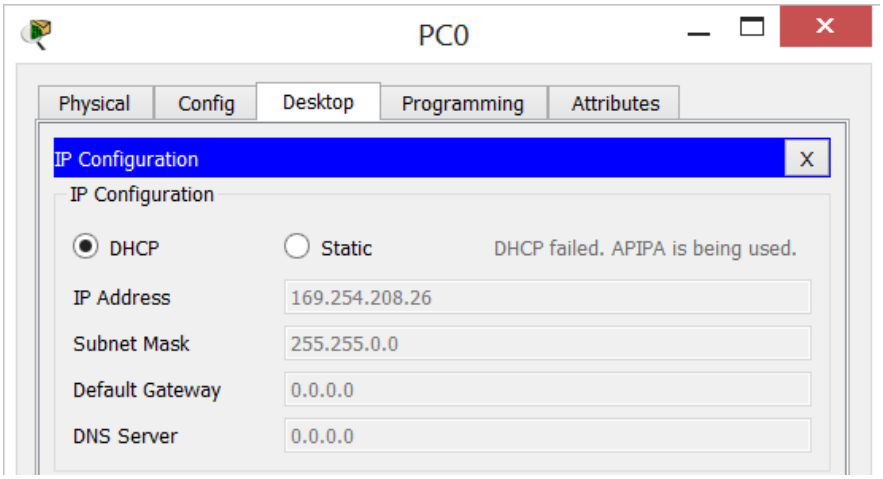


Ilustración 26 Configuración DHCP

Router de Bucaramanga se tiene:

BUCARAMANGA>enable
Password:
BUCARAMANGA#config t
Enter configuration commands, one per line. End with CNTL/2.
BUCARANANGA(config)#ip dhcp exclu
BUCARAMANGA(config)#ip dhcp excluded-address 172.31.0.129 172.31.0.2551
BUCARAMANGA(config)#ip dhcp pool DHCP_BUCARA
BUCARAMANGA(dhcp-config),172.31.0.0 255.255.255.192
t Invalid input detected at '^' marker.
BUCARAMANGA(dhcp-config)#network 172.31.0.0 255.255.255.192
BUCARAMANGA(dhcp-config)#defaul
BUCARAMANGA(dhcp-config)#default-router 172.31.0.1
BUCARAMANGA(dhcp-config)#dns-ser
BUCARAMANGA(dhcp-config)#dns-server 8.8.8.8
BUCARAMANGA(dlicp-config),

- Comando **Show ip dhcp pool**

```
BUCARAMANGA#show ip dhcp pool

Pool DHCP_BUCARA :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 62
 Leased addresses               : 0
 Excluded addresses             : 1
 Pending event                  : none

 1 subnet is currently in the pool
 Current index        IP address range                    Leased/
Excluded/Total
 172.31.0.1           172.31.0.1       - 172.31.0.62       0    / 1
/ 62

Pool bucaramanga :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 511
 Leased addresses               : 0
 Excluded addresses             : 1
 Pending event                  : none
```

Ilustración 27 Comando Show ip DHCP pool

Router de Cundinamarca se tiene

CUNDINAMARCA>enable
Password:
CUNDINAMARCA#config t
Enter configuration commands, one per line. End with CNTL/Z.
CUNDINAMARCA(config)#ip dhcp exclu
CUNDINAMARCA(config)#ip dhcp excluded-address 172.31.1.129 172.31.1.255
CUNDINAMARCA(config)#ip dhcp exclude
CUNDINAMARCA(config)#ip dhcp pool DHCP_CUNDI
CUNDINAMARCA(dhcp-config)#network 172.31.1.0 255.255.255.192
CUNDINAMARCA(dhcp-config)#defau
CUNDINAMARCA(dhcp-config)#default-router 172.31.1.1
CUNDINAMARCA(dhcp-config)#dns-s
CUNDINAMARCA(dhcp-config)#dns-server 8.8.8.8
CUNDINAMARCA(dhcp-config)#

3. El web server deberá tener NAT estático y el resto de los equipos de la topología emplearan NAT de sobrecarga (PAT).

7.6 Configuración NAT

- Configuración estática web server externo

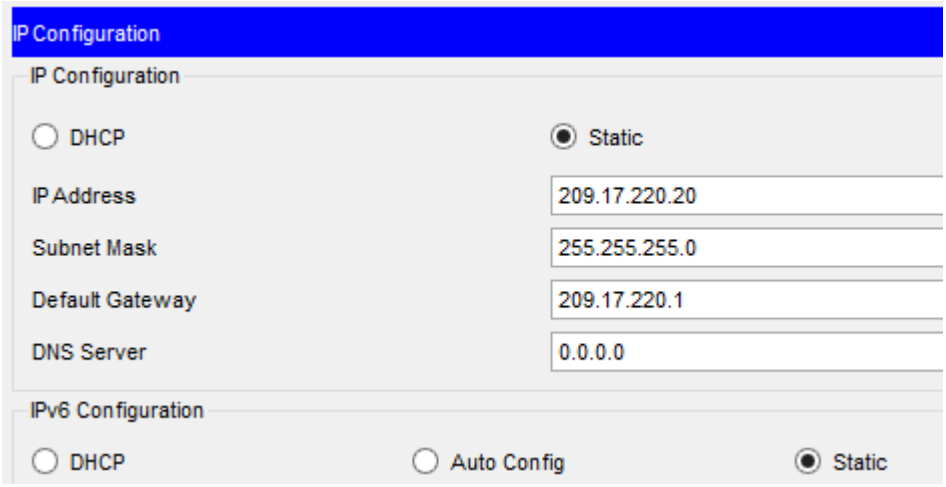


Ilustración 28 Configuración Web externo

NAT router Tunja

TUNJA>enable
Password:
TUNJA#configur t
TUNJA#configur terminal
Enter configuration commands, one per line. End with CNTL/Z.
TUNJA(config)#access
TUNJA(config)#access-list 1 permit 172.31.0.0 255.255.192
TUNJA(config)#ip nat inside source list 1 interface serial 0/0/0 overload
TUNJA(config)#interface g0/0
TUNJA(config-if)#ip nat inside
TUNJA(config-if)#exit
TUNJA(config)#interface serial 0/0
TUNJA(config-if)#ip nat outside
TUNJA(config-if)#exit
TUNJA(config)#
TUNJA#

NAT Bucaramanga

BUCARAMANGA>en
Password:
BUCARAMANGA#config t
Enter configuration commands, one per line. End with CNTL/Z.
BUCARAMANGA(config)#access-list 1 permit 172.31.0.0 255.255.255.192
BUCARAMANGA(config)#access-list 1 permit 172.31.0.0 0.0.0.192

BUCARAMANGA(config)#ip nat inside source list 1 interface g0/0 overload
BUCARAMANGA(config)#interface g0/0
BUCARAMANGA(config-if)#ip nat inside
BUCARAMANGA(config-if)#exit
BUCARAMANGA(config)#interface s0/0
BUCARAMANGA(config)#interface serial 0/0
BUCARAMANGA(config-if)#ip nat outside
BUCARAMANGA(config-if)#exit
BUCARAMANGA(config)#exit
BUCARAMANGA#
%SYS-5-CONFIG_I: Configured from console by console
BUCARAMANGA#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]

NAT Cundinamarca
CUNDINAMARCA>enable
Password:
CUNDINAMARCA#configu t
Enter configuration commands, one per line. End with CNTL/Z.
CUNDINAMARCA(config)#access-list 1 permit 172.31.1.0 0.0.0.192
CUNDINAMARCA(config)#ip nat inside source list 1 in
CUNDINAMARCA(config)#ip nat inside source list 1 interface g0/0 overload
CUNDINAMARCA(config)#interfac g0/0
CUNDINAMARCA(config-if)#ip nat inside
CUNDINAMARCA(config-if)#exit
CUNDINAMARCA(config)#interface se
CUNDINAMARCA(config)#interface s0/1/0
CUNDINAMARCA(config-if)#ip nat outside
CUNDINAMARCA(config-if)#exit
CUNDINAMARCA(config)#exit
CUNDINAMARCA#

4. El enrutamiento deberá tener autenticación.

Autenticación Cundinamarca
CUNDINAMARCA#ena
CUNDINAMARCA#conf t

```
Enter configuration commands, one per line.  End with CNTL/Z.
CUNDINAMARCA(config)#key chain cisco
CUNDINAMARCA(config-keychain)#key 1
CUNDINAMARCA(config-keychain-key)#key-string aula
CUNDINAMARCA(config-keychain-key)#no shut
                          ^
% Invalid input detected at '^' marker.
CUNDINAMARCA(config-keychain-key)#key-string cisco
CUNDINAMARCA(config-keychain-key)#int f0/0
CUNDINAMARCA(config-if)#ip authentication mode eigrp 100 md5
CUNDINAMARCA(config-if)#ip authentication key-chain eigrp 100 cisco
CUNDINAMARCA(config-if)#end
CUNDINAMARCA#
%SYS-5-CONFIG_I: Configured from console by console
Enable
```

Autenticación Tunja

```
Password:
TUNJA>ena
Password:
TUNJA#conf ter
Enter configuration commands, one per line.  End with CNTL/Z.
TUNJA(config)#key chain cisco
TUNJA(config-keychain)#key 1
TUNJA(config-keychain-key)#key string cisco
TUNJA(config-keychain-key)#int f0/0
TUNJA(config-if)#ip authentication mode eigrp 100 md5
TUNJA(config-if)#ip authentication key-chain eigrp 100 cisco
TUNJA(config-if)#end
TUNJA#
%SYS-5-CONFIG_I: Configured from console by console
```

Autenticación Bucaramanga

```
Password:
BUCARAMANGA>ena
Password:
BUCARAMANGA#conf te
Enter configuration commands, one per line.  End with CNTL/Z.
BUCARAMANGA(config)#key chain cisco
```

BUCARAMANGA(config-keychain)#key 1
BUCARAMANGA(config-keychain-key)#key string cisco
BUCARAMANGA(config-keychain-key)#int s0/1/0
BUCARAMANGA(config-if)#ip authentication mode eigrp 100 md5
BUCARAMANGA(config-if)#ip authentication key-chain eigrp 100 cisco
BUCARAMANGA(config-if)#end
BUCARAMANGA#
%SYS-5-CONFIG_I: Configured from console by console

7.7 5. Listas de control de acceso:

• Los hosts de VLAN 20 en Cundinamarca no acceden a internet, solo a la red interna de Tunja.
• Los hosts de VLAN 10 en Cundinamarca si acceden a internet y no a la red interna de Tunja.
• Los hosts de VLAN 30 en Tunja solo acceden a servidores web y ftp de internet.
• Los hosts de VLAN 20 en Tunja solo acceden a la VLAN 20 de Cundinamarca y VLAN 10 de
Bucaramanga.
• Los hosts de VLAN 30 de Bucaramanga acceden a internet y a cualquier equipo de VLAN 10.
• Los hosts de VLAN 10 en Bucaramanga acceden a la red de Cundinamarca (VLAN 20) y Tunja (VLAN20), no internet.
• Los hosts de una VLAN no pueden acceder a los de otra VLAN en una ciudad.
• Solo los hosts de las VLAN administrativas y de la VLAN de servidores tienen accedo a los routers e internet.

6. VLSM: utilizar la dirección 172.31.0.0 /18 para el direccionamiento.

Aspectos a tener en cuenta
• Habilitar VLAN en cada switch y permitir su enrutamiento.
• Enrutamiento OSPF con autenticación en cada router.
• Servicio DHCP en el router Tunja, mediante el helper address, para los routers Bucaramanga y
Cundinamarca.
• Configuración de NAT estático y de sobrecarga.
• Establecer una lista de control de acceso de acuerdo con los criterios señalados.
• Habilitar las opciones en puerto consola y terminal virtual

8 CONCLUISONES

Teniendo en cuenta el desarrollo de la actividad de los escenarios se logra dar cumplimiento con el objetivo general, donde se encuentra dificultades al aplicar comandos EIGRP que a la vez se debía configurar el reloj, para poder generar los protocolos del mismo.

Sin embargo, a través de las practicas realizadas en las actividades colaborativas se logra resolver las dudas presentadas al momento de ejecutar los comandos, EIGRP, DHCP, NAT, PAT, entre otros que se aprendieron a lo largo de estos meses.

Lo que es más importante al resolver los dos escenarios propuestos por la guía a desarrollar, conviene distinguir que todo lo que se realizó en las actividades grupales, se asemeja en estos ejercicios resueltos, los cuales tienen cierto grado de dificultad y al momento de aplicar en este campo se genera confusión ya que se aplica de forma grupal los comandos explicados anteriormente.

De lo que llevo dicho concluyo que la herramienta Pocket tracert nos facilita el manejo al montar una topología de red, poder generar los cambios al momento de efectuar los comandos para cambiar alguna interfaz, direccionamiento y demás.

9 REFERENCIAS BIBLIOGRAFICAS

IP Addressing and Subnetting for New Users, tomado de: https://www.cisco.com/c/es_mx/support/docs/ip/routing-information-protocol-rip/13788-3.html

CISCO NETWORKING ACADEMY – CCNA 1 tomado de: https://static-course-assets.s3.amazonaws.com/ITN503/es/index.html

CISCO NETWORKING ACADEMY – CCNA 2, tomado de: https://static-course-assets.s3.amazonaws.com/RSE503/es/index.html

Calculadora de IP https://www.aprendaredes.com/cgi-bin/ipcalc/ipcalc_cgi?host=172.31.0.64&mask1=29&mask2=

Capítulo 9, división de redes IP en subredes – CISCO, tomado de: https://www.minagricultura.gov.co/ministerio/recursos-humanos/Actos_Administrativos/Informe_2.pdf

EIGRP Mode Nombrado de la configuración, tomado de: https://www.cisco.com/c/es_mx/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/200156-Configure-EIGRP-Named-Mode.html

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). 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). Acceso a la red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#4.0.1.1

Vesga, J. (2014). Diseño y configuración de redes con Packet Tracer [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgCT9VCtl_pLtPD9

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