

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

EVALUACIÓN – PRUEBA DE HABILIDADES PRÁCTICAS CCNA

Elaborador Por:
JOHN FREDY PLAZAS MACIAS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
Enero / 2020
Sogamoso (BOYACA)

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

EVALUACIÓN – PRUEBA DE HABILIDADES PRÁCTICAS CCNA

Elaborador Por:
JOHN FREDY PLAZAS MACIAS

Presentado A:
DIEGO EDISON RAMIREZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnologías e Ingeniería
Enero / 2020
Sogamoso (BOYACA)

NOTA DE ACEPTACION

Presidente del jurado

Jurado

Jurado

Tabla de Contenido

Resumen	6
Abstract	6
Introducción	7
Objetivos	8
ACTIVIDADES PARA DESARROLLAR:	9
Escenario 1	9
Topología de red	9
Parte 1: Asignación de direcciones IP:	14
Parte 2: Configuración Básica.	15
Parte 4: Configuración de las listas de Control de Acceso.	25
a. Cada router debe estar habilitado para establecer conexiones Telnet con los demás routers y tener acceso a cualquier dispositivo en la red.	25
b. 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.	26
Parte 5: Comprobación de la red instalada.	27
a. Se debe probar que la configuración de las listas de acceso fue exitosa.	27
b. Comprobar y Completar la siguiente tabla de condiciones de prueba para confirmar el óptimo funcionamiento de la red e.	31
Escenario 2	32
1. Todos los routers deberán tener los siguiente:	32
<i>Configuración básica</i>	32
• Autenticación local con AAA.	42
• Cifrado de contraseñas.....	45
• Establezca un servidor TFTP y almacene todos los archivos necesarios de los routers.	48
2. El DHCP deberá proporcionar solo direcciones a los hosts de Bucaramanga y Cundinamarca	49
3. El web server deberá tener NAT estático y el resto de los equipos de la topología emplearan NAT de sobrecarga (PAT).	51
4. El enrutamiento deberá tener autenticación.	51

5. Listas de control de acceso	53
• Los hosts de VLAN 20 en Cundinamarca no acceden a internet, solo a la red interna de Tunja.....	53
• Los hosts de VLAN 30 en Cundinamarca si acceden a internet y no a la red interna de Tunja.....	54
Conclusiones	56
Bibliografía	58

Resumen

La evaluación denominada “Prueba de habilidades prácticas”, es de carácter obligatorio porque forma parte de las actividades evaluativas del Diplomado de Profundización CCNA, porque busca identificar el grado de desarrollo de competencias y habilidades que fueron adquiridas a lo largo del diplomado. Lo esencial es poner a prueba los niveles de comprensión y solución de problemas relacionados con diversos aspectos diarios profesionalmente en cuanto a Networking.

En este proyecto se presenta la solución de dos escenarios propuestos, los cuales describen los conceptos teóricos y prácticos adquiridos en los dos módulos desarrollados CCNA1 y CCNA2, estos cursos comprenden Introducción a redes y Principios básicos de routing y switching, es indispensable el uso de la herramienta de simulación Cisco Packet Tracer o GNS3 para logra el desarrollo y comprensión de la prueba en su totalidad

Abstract

The evaluation called "Practical skills test" is mandatory because it is part of the evaluation activities of the CCNA Deepening Diploma, because it seeks to identify the degree of development of skills and abilities that were acquired throughout the diploma. The essential thing is to test the levels of understanding and solution of problems related to various daily aspects professionally in terms of Networking

This project presents the solution of two proposed scenarios, which describe the theoretical and practical concepts acquired in the two modules developed CCNA1 and CCNA2, these courses include Introduction to networks and basic principles of routing and switching, it is essential to use the Cisco Packet Tracer or GNS3 simulation tool to achieve the development and understanding of the test in its entirety

Introducción

El siguiente trabajo tiene como fin proporcionar al estudiante una visión del curso CCNA de cisco, en este curso encontramos 4 unidades las cuales nos enseñan la forma y las herramientas de cómo utilizarlo de forma que nos oriente para abordar las necesidades de redes simples y compuestas, para lograr el desarrollo de las actividades requeridas en nuestro habito laboral y profesional.

En el siguiente desarrollo sobre la guía de actividades para esta fase se verá entre otros aspectos la importancia y características de estos protocolos y su implementación en redes, para él envío de paquetes así como su configuración entre otras cualidades y prestaciones como las observadas por los protocolos de enrutamiento "Eigrp", la diferencia entre el enrutamiento por vector de distancia y de estado de enlace así como la manera en que los routers utilizan dichos protocolos para determinar la ruta más corta hacia cada red y la forma en que ellos ejecutan un protocolo de enrutamiento de estado de enlace envían información acerca del estado de sus enlaces a otros routers en el dominio de enrutamiento, es decir, a sus redes conectadas directamente incluyendo información acerca del tipo de red y los routers vecinos en dichas redes.

Objetivos

- ✓ Fomentar la capacidad de configurar y administrar dispositivos de Networking orientados al diseño de redes escalables y de conmutación.
- ✓ Fortalecer los conocimientos necesarios para el diseño de redes mediante el uso del modelo jerárquico de tres niveles, con el fin de optimizar el rendimiento de la red e incorporar de manera adecuada el uso de tecnologías y protocolos de conmutación y enrutamiento.

ACTIVIDADES PARA DESARROLLAR:

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.

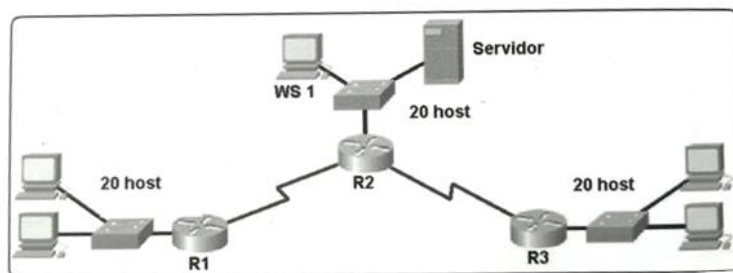
Parte 2: Considerar la asignación de los parámetros básicos y la detección de vecinos directamente conectados.

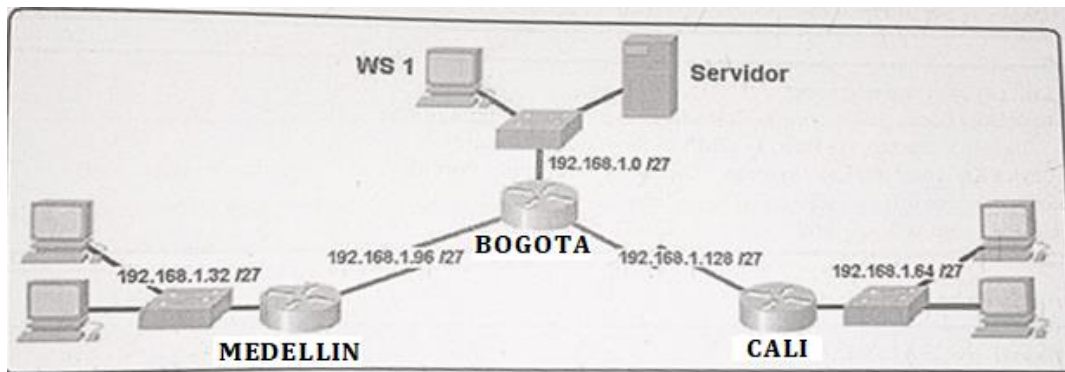
Parte 3: La red y subred establecidas deberán tener una interconexión total, todos los hosts deberán ser visibles y poder comunicarse entre ellos sin restricciones.

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.





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).

Asignar Nombres y claves

RTA:

Clave de Ingreso A todos los router **cisco**

- **Configuro Router1 Medellin Nombre, Clave consola y Vty**

```
Router>EN
Router#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname MEDELLIN
MEDELLIN(config)#no ip domain-lookup
MEDELLIN(config)#service pass
MEDELLIN(config)#service password-encryption
MEDELLIN(config)#line console 0
MEDELLIN(config-line)#password cisco
MEDELLIN(config-line)#login
MEDELLIN(config-line)#line vty 0 4
MEDELLIN(config-line)#password cisco
MEDELLIN(config-line)#login
MEDELLIN(config-line)#exit
MEDELLIN(config)#enable secret cisco
MEDELLIN(config)#do write
MEDELLIN(config)#do write
```

- **Configuración Switch Medellin Nombre, Clave Consola, Vty y Hora**

```
Switch>en
Switch#config ter
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SW1-Med
SW1-Med(config)#no ip domain-lookup
SW1-Med(config)#line console 0
SW1-Med(config-line)#password cisco
SW1-Med(config-line)#login
SW1-Med(config-line)#line vty 0 4
SW1-Med(config-line)#password cisco
SW1-Med(config-line)#login
SW1-Med(config-line)#exit
SW1-Med(config)#service password-encryption
SW1-Med(config)#enable secret cisco
SW1-Med(config)#do write
Building configuration..
SW1-Med(config)#
```

- **Configuro Router Bogota Nombre, Clave consola y Vty**

```
Router>EN
Router#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname Bogota
Bogota(config)#no ip domain-lookup
Bogota(config)#service pass
Bogota(config)#service password-encryption
Bogota(config)#line console 0
Bogota(config-line)#password cisco
Bogota(config-line)#login
Bogota(config-line)#line vty 0 4
Bogota(config-line)#password cisco
Bogota(config-line)#login
Bogota(config-line)#exit
Bogota(config)#enable secret cisco
Bogota(config)#do write
```

Configuro Switch Bogota Nombre, Clave consola y Vty

```
Switch>en
Switch#config ter
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SW_BOG
SW_BOG(config)#no ip domain-lookup
SW_BOG(config)#line console 0
```

```
SW_BOG(config-line)#password cisco
SW_BOG(config-line)#login
SW_BOG(config-line)#line vty 0 4
SW_BOG(config-line)#password cisco
SW_BOG(config-line)#login
SW_BOG(config-line)#exit
SW_BOG(config)#service password-encryption
SW_BOG(config)#enable secret cisco
SW_BOG(config)#do write
Building configuration..
```

- Configuro Router Cali Nombre, Clave consola y Vty

```
Router>en
Router#config ter
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#Hostname CALI
CALI(config)#no ip domain-lookup
CALI(config)#line console 0
CALI(config-line)#password cisco
CALI(config-line)#login
CALI(config-line)#line vty 0 4
CALI(config-line)#password cisco
CALI(config-line)#login
CALI(config-line)#exit
CALI(config)#enable secret cisco
CALI(config)#service password-encryption
CALI(config)#do wr
Building configuration...
[OK]
CALI(config)#
CALI#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
CALI#
```

- Configuro Switch Cali Nombre, Clave consola y Vty

```
Switch>en
Switch#SW_Cali
Translating "SW_Cali"...domain server (255.255.255.255)
% Unknown command or computer name, or unable to find computer address
```

```
Switch#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
```

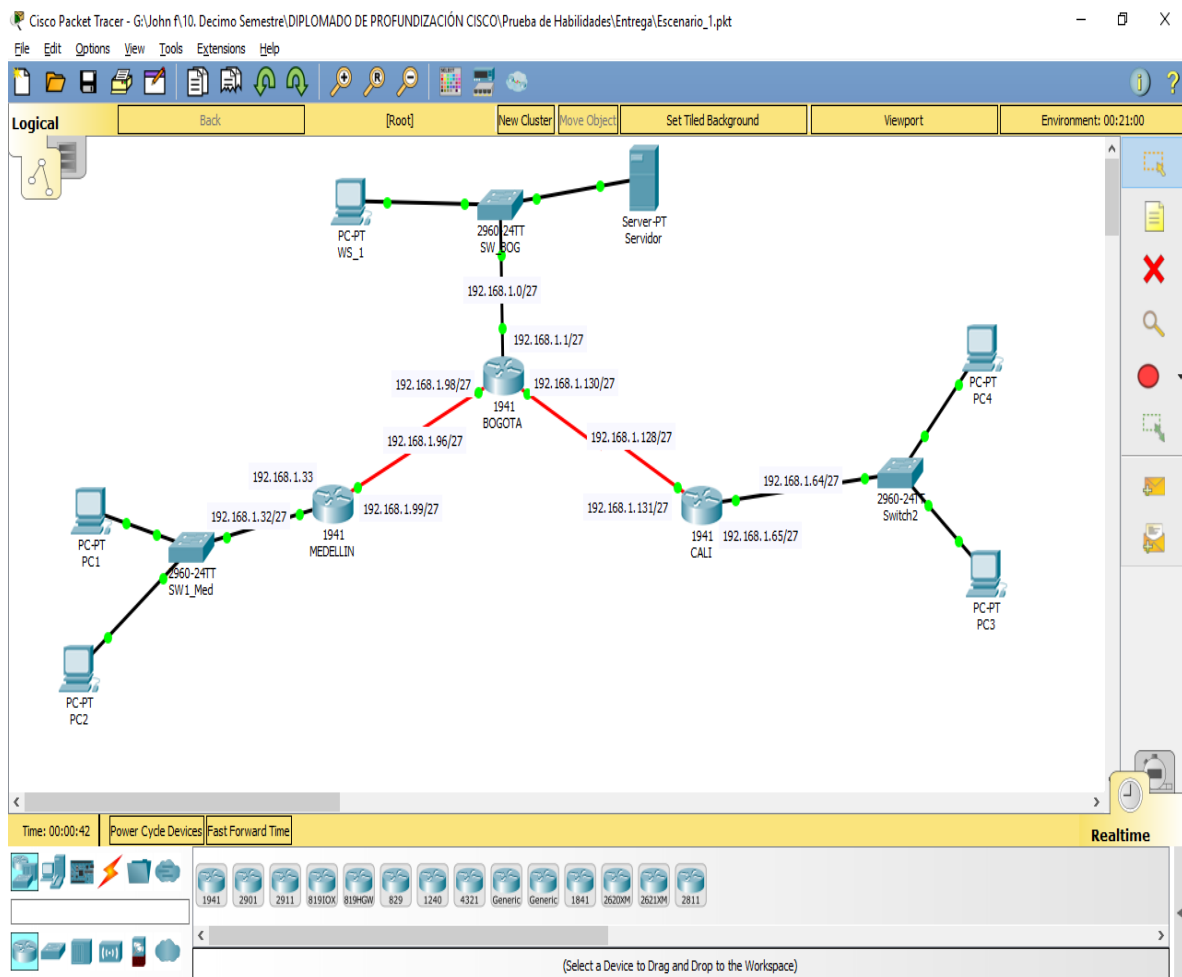
```

Switch(config)#hostname SW_Cali
SW_Cali(config-line)#line vty 0 4
SW_Cali(config-line)#password cisco
SW_Cali(config-line)#login
SW_Cali(config-line)#line console 0
SW_Cali(config-line)#password cisco
SW_Cali(config-line)#login
SW_Cali(config-line)#exit
SW_Cali(config)#enable secret cisco
SW_Cali(config)#service pass
SW_Cali(config)#service password-encryption
SW_Cali(config)#do write
Building configuration...
[OK]
SW_Cali(config)#

```

- Realizar la conexión física de los equipos con base en la topología de red

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



Parte 1: Asignación de direcciones IP:

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

RTA:

Red Clase C: 192.168.1.0

Crear una segmentación en ocho partes

Mascara Por default	255	255	255	0
Mascara Por default Binario	11111111	11111111	11111111	00000000

Entonces:

Uso formula

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

Mascara Adaptada - Binario	11111111	11111111	11111111	11100000
Mascara Adaptada	255	255	255	224 o /27

Host Utiles: 30

Uso formula

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

b. Asignar una dirección IP a la red.

192.168.1.0

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

Dispositivo	Interface	Direccion IP	Masdca de Subred	Puerta de enlace predeterminada
R1	S0/0	192.168.1.99	255.255.255.242	
	G0/0	192.168.1.33	255.255.255.242	
R2	S0/0	192.168.1.98	255.255.255.242	
	S0/1	192.168.1.130	255.255.255.242	
	G0/0	192.168.1.1	255.255.255.242	
R3	S0/0	192.168.1.131	255.255.255.242	
	G0/0	192.168.1.65	255.255.255.242	
SERVIDOR	F0	192.168.1.12	255.255.255.224	192.168.1.31
WS	NIC	192.168.1.14	255.255.255.224	192.168.1.31
PC-1	NIC	192.168.1.35	255.255.255.224	192.168.1.63
PC-2	NIC	192.168.1.36	255.255.255.224	192.168.1.63
PC-3	NIC	192.168.1.67	255.255.255.224	192.168.1.95
PC-4	NIC	192.168.1.68	255.255.255.224	192.168.1.95

- Interface Router Medellin

```
MEDELLIN>en
```

```
Password:
```

```
MEDELLIN#conf ter
```

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

```
MEDELLIN(config)#inter s0/0/0
```

```
%Invalid interface type and number
MEDELLIN(config)#inter s0
MEDELLIN(config)#inter
MEDELLIN(config)#interface s0/1/0
MEDELLIN(config-if)#ip add 192.168.1.99 255.255.255.224
MEDELLIN(config-if)#no shut
```

```
%LINK-5-CHANGED: Interface Serial0/1/0, changed state to down
MEDELLIN(config-if)#exit
MEDELLIN(config)#exit
MEDELLIN#
MEDELLIN#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN(config)#inter GIGA0/0
MEDELLIN(config-if)#ip add 192.168.1.33 255.255.255.224
MEDELLIN(config-if)#no shut
```

```
MEDELLIN(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
```

```
MEDELLIN#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
MEDELLIN#
```

- Interface Router Bogota

```
Bogota#config ter
Enter configuration commands, one per line. End with CNTL/Z.
Bogota(config)#inter s0/1/0
Bogota(config-if)#ip add 192.168.1.98 255.255.255.224
Bogota(config-if)#no shut
```

```
Bogota(config-if)#
%LINK-5-CHANGED: Interface Serial0/1/0, changed state to up
```

```
Bogota(config-if)#exit
Bogota(config)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed state to up
```

```
Bogota(config)#inter s0/1/1
Bogota(config-if)#ip add 192.168.1.130 255.255.255.224
```

```
Bogota(config-if)#no shut
```

```
%LINK-5-CHANGED: Interface Serial0/1/1, changed state to down
```

```
Bogota(config-if)#exit
```

```
Bogota(config)#inter giga0/0
```

```
Bogota(config-if)#ip add 192.168.1.1 255.255.255.224
```

```
Bogota(config-if)#no shut
```

```
Bogota(config-if)#
```

- Interface Router Cali

```
CALI>en
```

```
Password:
```

```
CALI#conf ter
```

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

```
CALI(config)#inter s0/1/0
```

```
CALI(config-if)#ip add 192.168.1.131 255.255.255.224
```

```
CALI(config-if)#no shut
```

```
CALI(config-if)#
```

```
%LINK-5-CHANGED: Interface Serial0/1/0, changed state to up
```

```
CALI(config-if)#ext
```

```
^
```

```
% Invalid input detected at '^' marker.
```

```
CALI(config-if)#
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed state to up
```

```
CALI(config-if)#exit
```

```
CALI(config)#inter G0/0
```

```
CALI(config-if)#ip add 192.168.1.55 255.255.255.224
```

```
CALI(config-if)#no shut
```

```
CALI(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
```

```
CALI(config-if)#
```

```
CALI#
```

```
%SYS-5-CONFIG_I: Configured from console by console
```

```
wr
```

```
Building configuration...
```

```
[OK]
```

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.

- **Router Medellin**

```
MEDELLIN>en
```

```
Password:
```

```
MEDELLIN#sh ip route
```

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
```

```
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
```

```
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
```

```
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
```

```
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
```

```
* - candidate default, U - per-user static route, o - ODR
```

```
P - periodic downloaded static route
```

```
Gateway of last resort is not set
```

```
192.168.1.0/24 is variably subnetted, 4 subnets, 2 masks
```

```
C 192.168.1.32/27 is directly connected, GigabitEthernet0/0
```

```
L 192.168.1.33/32 is directly connected, GigabitEthernet0/0
```

```
C 192.168.1.96/27 is directly connected, Serial0/1/0
```

```
L 192.168.1.99/32 is directly connected, Serial0/1/0
```

```
MEDELLIN#
```

- **Router BOGOTA**

```
Bogota#sh ip route
```

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
```

```
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
```

```
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
```

```
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
```

```
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
```

```
* - candidate default, U - per-user static route, o - ODR
```

```
P - periodic downloaded static route
```

```
Gateway of last resort is not set
```

```
192.168.1.0/24 is variably subnetted, 6 subnets, 2 masks
```

```
C 192.168.1.0/27 is directly connected, GigabitEthernet0/0
```

```
L 192.168.1.1/32 is directly connected, GigabitEthernet0/0
```

```
C 192.168.1.96/27 is directly connected, Serial0/1/0
```

```
L 192.168.1.98/32 is directly connected, Serial0/1/0
```

```
C 192.168.1.128/27 is directly connected, Serial0/1/1
```

```
L 192.168.1.130/32 is directly connected, Serial0/1/1
```

Bogota#

- **Router CALI**

CALI>en

Password:

CALI#sh ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area

* - candidate default, U - per-user static route, o - ODR

P - periodic downloaded static route

Gateway of last resort is not set

192.168.1.0/24 is variably subnetted, 4 subnets, 2 masks

C 192.168.1.32/27 is directly connected, GigabitEthernet0/0

L 192.168.1.55/32 is directly connected, GigabitEthernet0/0

C 192.168.1.128/27 is directly connected, Serial0/1/0

L 192.168.1.131/32 is directly connected, Serial0/1/0

CALI#

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

- **Router Bogota**

Bogota#sh cdp neig

Bogota#sh cdp neighbors

Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge

S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone

Device ID Local Intrfce Holdtme Capability Platform Port ID

MEDELLIN Ser 0/1/0 142 R C1900 Ser 0/1/0

SW_BOG Gig 0/0 161 S 2960 Gig 0/1

CALI Ser 0/1/1 123 R C1900 Ser 0/1/0

Bogota#

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

- **Se realiza ping desde el PC1 Al Servidor**

C:\>ping 192.168.1.12

Pinging 192.168.1.12 with 32 bytes of data:

Reply from 192.168.1.12: bytes=32 time=1ms TTL=128

Reply from 192.168.1.12: bytes=32 time<1ms TTL=128

Reply from 192.168.1.12: bytes=32 time<1ms TTL=128
Reply from 192.168.1.12: bytes=32 time=3ms TTL=128

Ping statistics for 192.168.1.12:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 3ms, Average = 1ms

C:\>

- **Se realiza ping desde el PC 2 Al PC1 de la lan 2**

C:\>ping 192.168.1.35

Pinging 192.168.1.35 with 32 bytes of data:

Reply from 192.168.1.35: bytes=32 time<1ms TTL=128
Reply from 192.168.1.35: bytes=32 time<1ms TTL=128
Reply from 192.168.1.35: bytes=32 time<1ms TTL=128
Reply from 192.168.1.35: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.35:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>

- **Se realiza ping desde el PC3 al PC4**

C:\>ping 192.168.1.57

Pinging 192.168.1.57 with 32 bytes of data:

Reply from 192.168.1.57: bytes=32 time=9ms TTL=128
Reply from 192.168.1.57: bytes=32 time=1ms TTL=128
Reply from 192.168.1.57: bytes=32 time=6ms TTL=128
Reply from 192.168.1.57: bytes=32 time=14ms TTL=128

Ping statistics for 192.168.1.57:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 14ms, Average = 7ms

C:\>

Parte 3: Configuración de Enrutamiento.

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

- Router MEDELLIN

```
MEDELLIN>en
Password:
MEDELLIN#conf termi
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN(config)#router eigrp 10
MEDELLIN(config-router)#network 192.168.1.32 0.0.0.31
MEDELLIN(config-router)#network 192.168.1.96 0.0.0.31
MEDELLIN(config-router)#no auto
MEDELLIN(config-router)#no auto-summary
MEDELLIN(config-router)#exit
MEDELLIN(config)#do write
Building configuration...
[OK]
MEDELLIN(config)#
MEDELLIN#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
MEDELLIN#
```

- Router BOGOTA

```
Bogota>en
Password:
Bogota#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
Bogota(config)#router eigrp 10
Bogota(config-router)#network 192.168.1.0 0.0.0.31
Bogota(config-router)#network 192.168.1.96 0.0.0.31
Bogota(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 10: Neighbor 192.168.1.99 (Serial0/1/0) is up: new
adjacency

Bogota(config-router)#network 192.168.1.97 0.0.0.31
Bogota(config-router)#network 192.168.1.128 0.0.0.31
Bogota(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 10: Neighbor 192.168.1.131 (Serial0/1/1) is up:
new adjacency
```

```
Bogota(config-router)#network 192.168.1.129 0.0.0.31
Bogota(config-router)#auto sum
Bogota(config-router)#no auto
Bogota(config-router)#no auto-summary
Bogota(config-router)#exit
Bogota(config)#do wr
Building configuration...
[OK]
Bogota(config)#
Bogota#
```

- Router CALI

```
CALI>en
Password:
CALI#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
CALI(config)#router eigrp 10
CALI(config-router)#network 192.168.1.32 0.0.0.31
CALI(config-router)#network 192.168.1.128 0.0.0.31
CALI(config-router)#no aut
CALI(config-router)#no auto-summary
CALI(config-router)#exit
CALI(config)#do wr
Building configuration...
[OK]
CALI(config)#
CALI#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
CALI#
```

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

- Router MEDELLIN

```
MEDELLIN>en
Password:
MEDELLIN#sh ip eigrp nei
MEDELLIN#sh ip eigrp neighbors
IP-EIGRP neighbors for process 10
H Address Interface Hold Uptime SRTT RTO Q Seq
(sec) (ms) Cnt Num
0 192.168.1.98 Se0/1/0 12 00:07:30 40 1000 0 4

MEDELLIN#
```

- **Router BOGOTA**

```
Bogota#sh ip eigrp nei
Bogota#sh ip eigrp neighbors
IP-EIGRP neighbors for process 10
H Address Interface Hold Uptime SRTT RTO Q Seq
(sec) (ms) Cnt Num
0 192.168.1.99 Se0/1/0 12 00:05:11 40 1000 0 5
1 192.168.1.131 Se0/1/1 10 00:03:50 40 1000 0 5
```

Bogota#

- **Router Cali**

```
CALI>en
Password:
CALI#sh ip eigrp neig
CALI#sh ip eigrp neighbors
IP-EIGRP neighbors for process 10
H Address Interface Hold Uptime SRTT RTO Q Seq
(sec) (ms) Cnt Num
0 192.168.1.130 Se0/1/0 11 00:07:45 40 1000 0 6
```

CALI#

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

- **Router Medellin:**

```
MEDELLIN#sh ip route eigrp
192.168.1.0/24 is variably subnetted, 6 subnets, 2 masks
D 192.168.1.0/27 [90/2170112] via 192.168.1.98, 00:15:03, Serial0/1/0
D 192.168.1.128/27 [90/2681856] via 192.168.1.98, 00:13:41, Serial0/1/0
```

MEDELLIN#

- **Router Bogota:**

```
Bogota>en
Password:
Bogota#sh ip route eigrp
192.168.1.0/24 is variably subnetted, 7 subnets, 2 masks
D 192.168.1.32/27 [90/2170112] via 192.168.1.99, 00:13:16, Serial0/1/0
[90/2170112] via 192.168.1.131, 00:11:54, Serial0/1/1
```

Bogota#

- **Router Cali**

```
CALI#sh ip route eigrp
```

192.168.1.0/24 is variably subnetted, 6 subnets, 2 masks
D 192.168.1.0/27 [90/2170112] via 192.168.1.130, 00:10:53, Serial0/1/0
D 192.168.1.96/27 [90/2681856] via 192.168.1.130, 00:10:53, Serial0/1/0

CALI#

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.

- **Ping de la LAN Cali (PC4) A LAN Medellin (PC1)**

C:\>ping 192.168.1.35

Pinging 192.168.1.35 with 32 bytes of data:

Reply from 192.168.1.35: bytes=32 time=10ms TTL=125
Reply from 192.168.1.35: bytes=32 time=11ms TTL=125
Reply from 192.168.1.35: bytes=32 time=15ms TTL=125
Reply from 192.168.1.35: bytes=32 time=19ms TTL=125

Ping statistics for 192.168.1.35:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 10ms, Maximum = 19ms, Average = 13ms

C:\>

- **Ping de la LAN Cali (PC4) A LAN Bogotá (Servidor)**

C:\>ping 192.168.1.12

Pinging 192.168.1.12 with 32 bytes of data:

Reply from 192.168.1.12: bytes=32 time=2ms TTL=126
Reply from 192.168.1.12: bytes=32 time=14ms TTL=126
Reply from 192.168.1.12: bytes=32 time=1ms TTL=126
Reply from 192.168.1.12: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.1.12:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 14ms, Average = 4ms

C:\>

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.

- CONFIGURACION ROUTER LAN MEDELLIN

```
MEDELLIN >en
MEDELLIN#config ter
MEDELLIN(config)#no ip domain-lookup
MEDELLIN(config-line)#line vty 0 4
MEDELLIN(config-line)#password cisco
MEDELLIN(config-line)#login
MEDELLIN(config-line)#exit
MEDELLIN(config)#enable secret cisco
MEDELLIN(config)#service password-encryption
MEDELLIN(config)#do wr
Building configuration...
[OK]
Bogota(config)#
```

- CONFIGURO ROUTER LAN BOGOTA

```
Bogota>en
Bogota#config ter
Bogota(config)#no ip domain-lookup
Bogota(config-line)#line vty 0 4
Bogota(config-line)#password cisco
Bogota(config-line)#login
Bogota(config-line)#exit
Bogota(config)#enable secret cisco
Bogota(config)#service password-encryption
Bogota(config)#do wr
Building configuration...
[OK]
Bogota(config)#
```

- CONFIGURO ROUTER LAN CALI

```
CALIr>en
CALI#config ter
CALI(config)#no ip domain-lookup
```

```
CALI(config-line)#line vty 0 4
CALI(config-line)#password cisco
CALI(config-line)#login
CALI(config-line)#exit
CALI(config)#enable secret cisco
CALI(config)#service password-encryption
CALI(config)#do wr
Building configuration...
[OK]
CALI(config)#
```

- b. 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.

- **LAN Medellin**

```
MEDELLIN>en
Password:
MEDELLIN#conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN(config)#acc
MEDELLIN(config)#access-list 1 deny 192.168.1.64 0.0.0.31
MEDELLIN(config)#access-list 1 permit any
MEDELLIN(config)#
MEDELLIN#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN(config)#inter G0/0
MEDELLIN(config-if)#ip acc
MEDELLIN(config-if)#ip access-group 1 out
MEDELLIN(config-if)#
MEDELLIN #
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
MEDELLIN#sh run
```

```
Building configuration...
[OK]
MEDELLIN#
```

- **LAN Cali**

```
CALI>en
Password:
CALI#conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

```
CALI(config)#acc
CALI(config)#access-list 1 deny 192.168.1.32 0.0.0.31
CALI(config)#access-list 1 permit any
CALI(config)#
CALI#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
CALI(config)#inter G0/0
CALI(config-if)#ip acc
CALI(config-if)#ip access-group 1 out
CALI(config-if)#
CALI#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
CALI#sh run

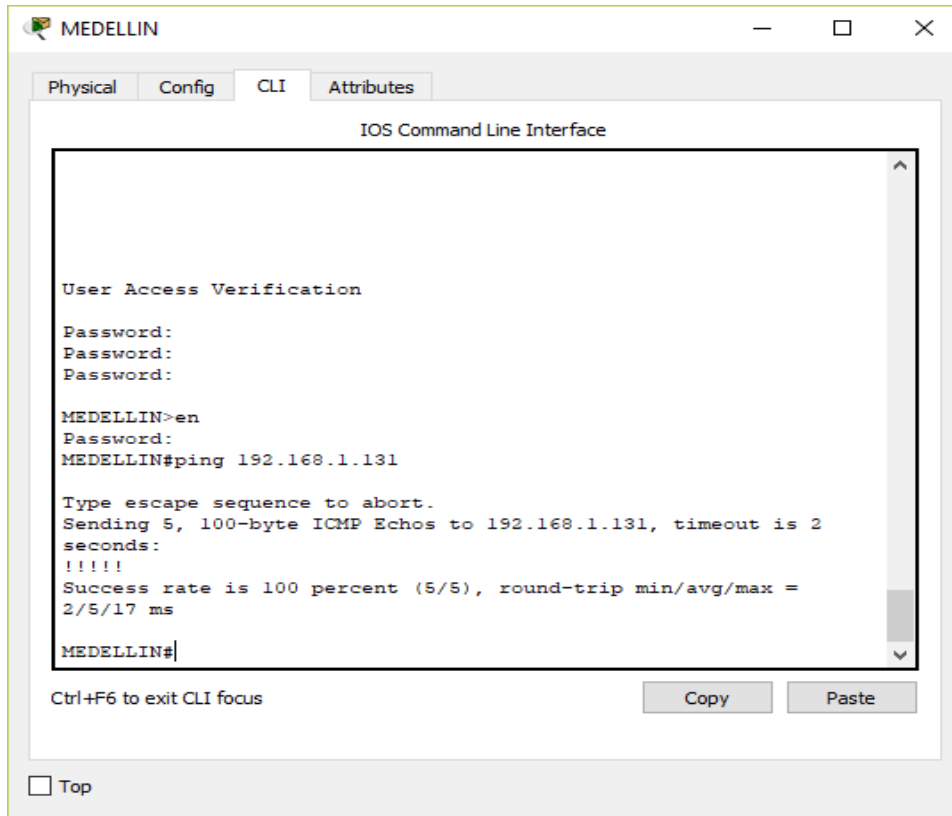
Building configuration...
[OK]
CALI#
- Valido
```

```
Bogota#sh access-lists
Standard IP access list 1
10 deny 192.168.1.32 0.0.0.31 (182 match(es))
20 permit any (8 match(es))
Standard IP access list 2
10 deny 192.168.1.64 0.0.0.31 (153 match(es))
20 permit any
```

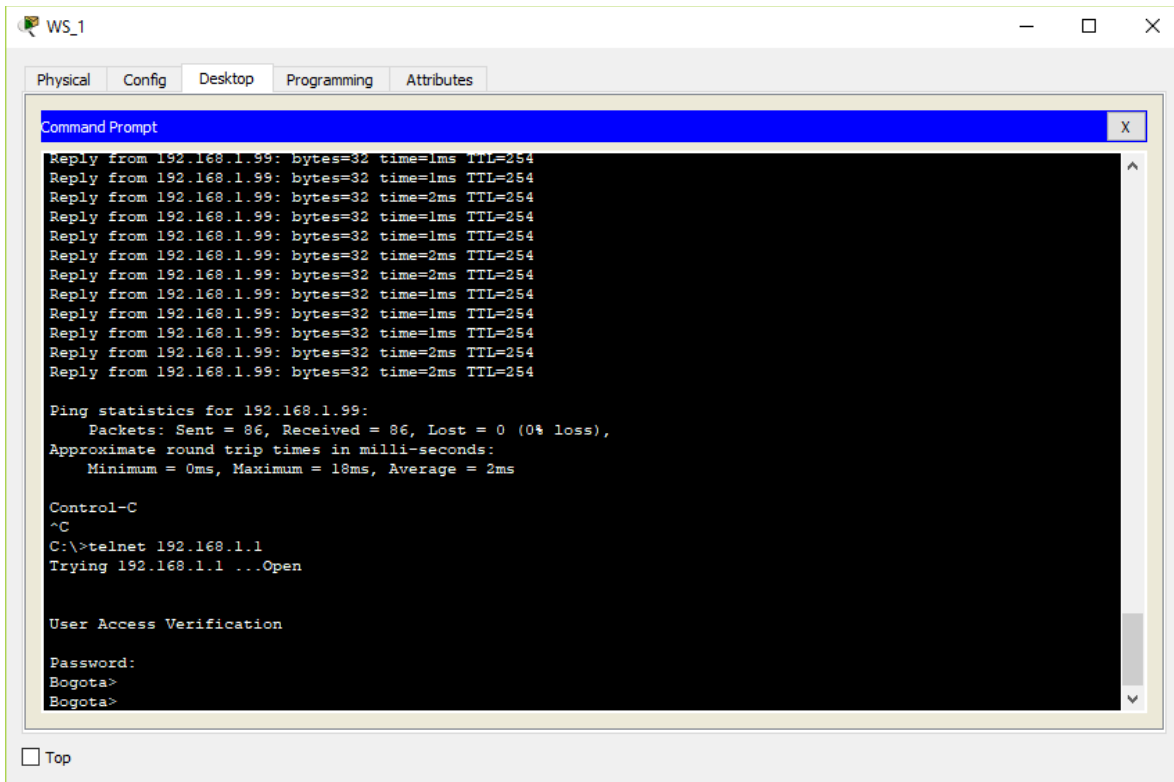
```
Bogota#
```

Parte 5: Comprobación de la red instalada.

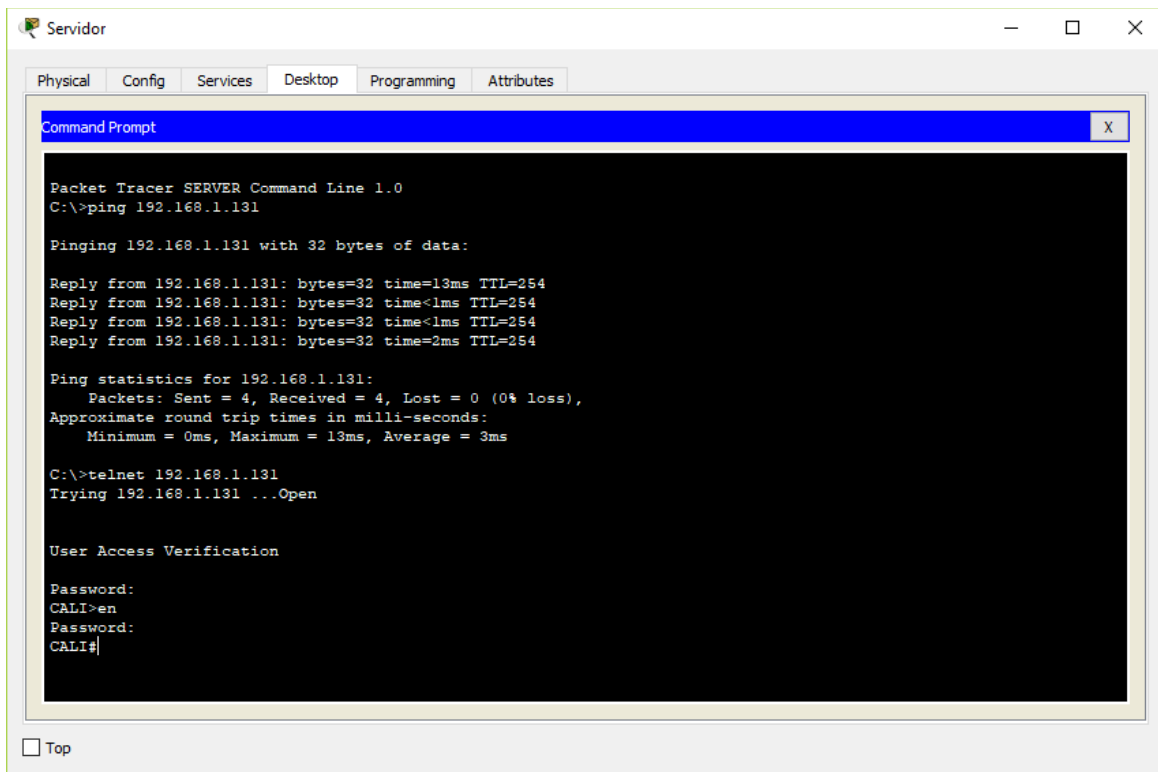
- a. Se debe probar que la configuración de las listas de acceso fue exitosa.
 - **Ping de router de medellin a router de cali**



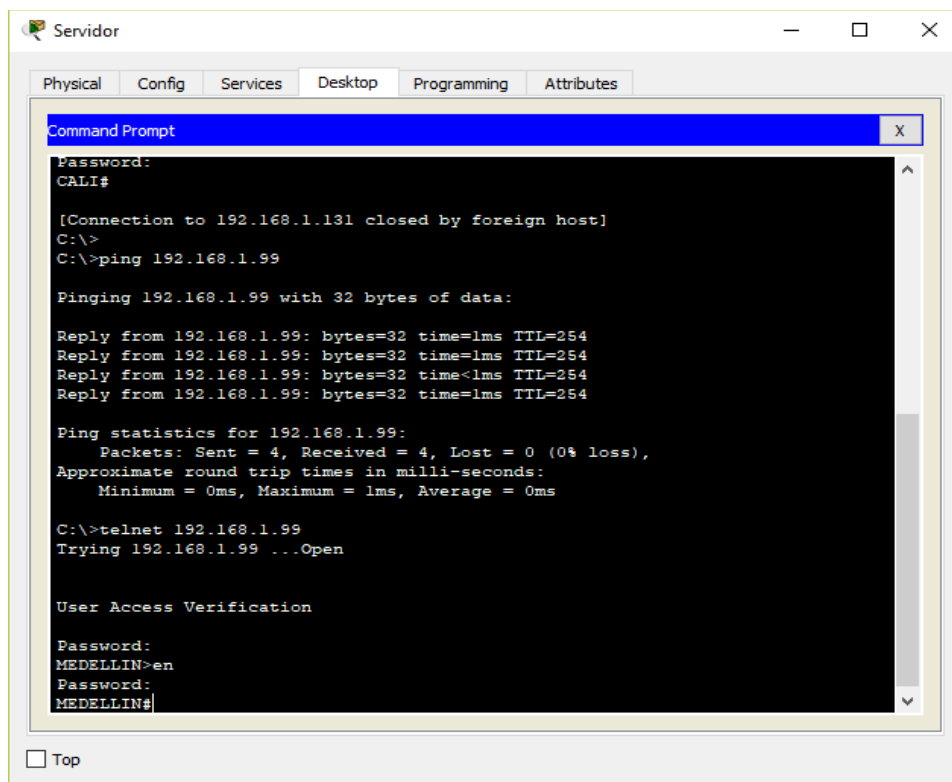
- Ping y telnet de WS_1 a Router Bogota



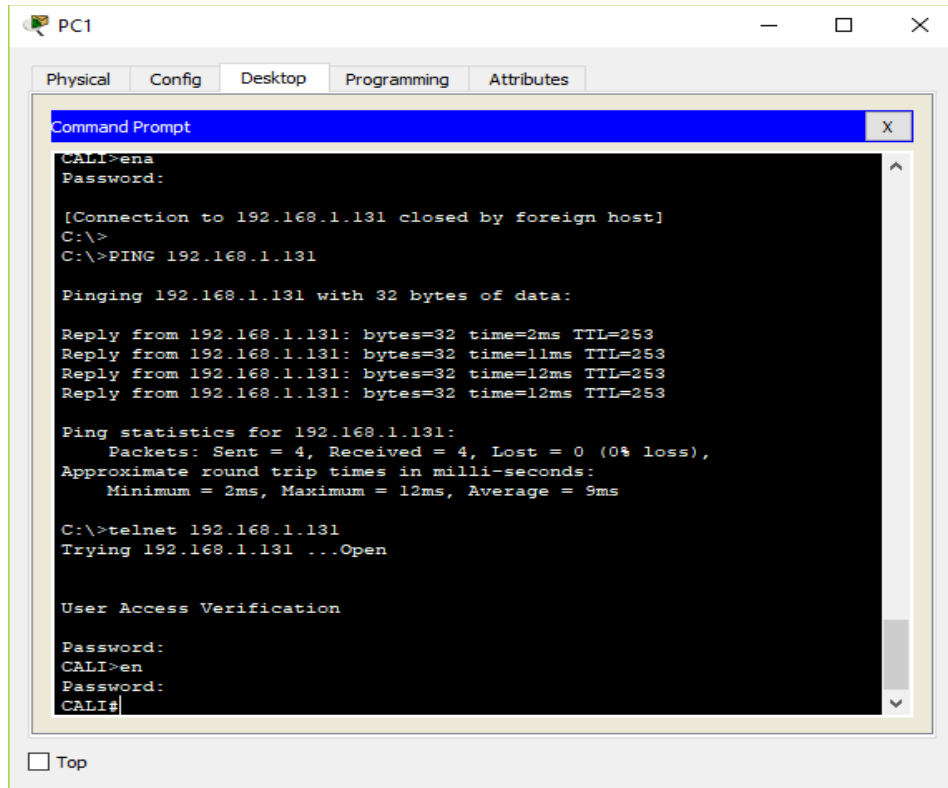
- Ping y telnet de servidor a router cali



- Ping y telnet de servidor a router medellin



- Ping y telnet de LAN Medellin A cali



```
PC1
Physical Config Desktop Programming Attributes
Command Prompt
CALI>ena
Password:
[Connection to 192.168.1.131 closed by foreign host]
C:\>
C:\>PING 192.168.1.131

Pinging 192.168.1.131 with 32 bytes of data:

Reply from 192.168.1.131: bytes=32 time=2ms TTL=253
Reply from 192.168.1.131: bytes=32 time=11ms TTL=253
Reply from 192.168.1.131: bytes=32 time=12ms TTL=253
Reply from 192.168.1.131: bytes=32 time=12ms TTL=253

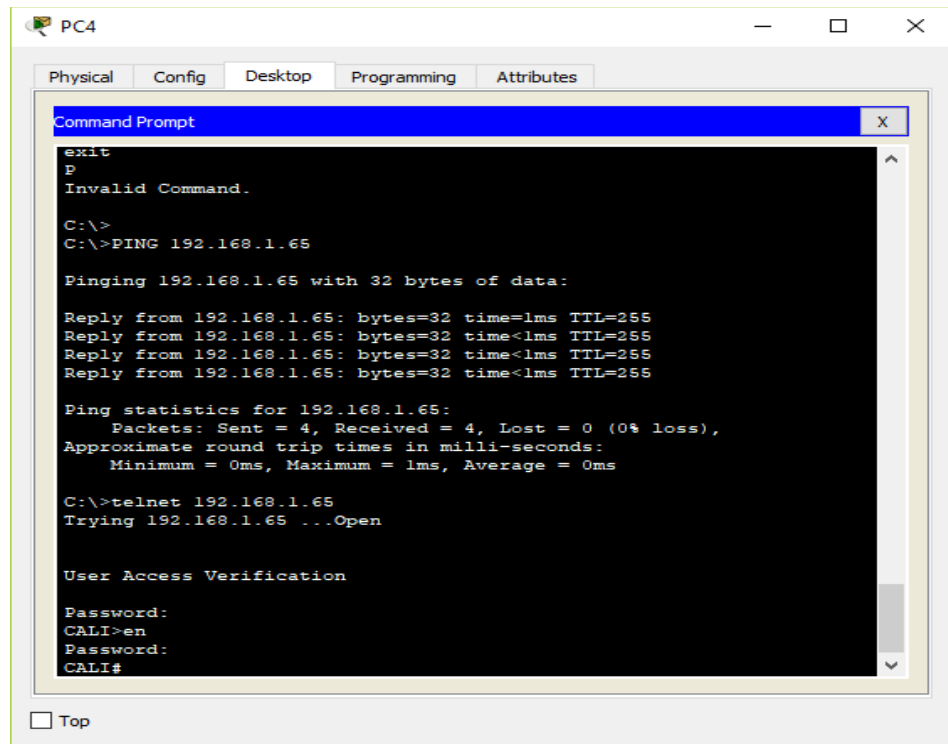
Ping statistics for 192.168.1.131:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 12ms, Average = 9ms

C:\>telnet 192.168.1.131
Trying 192.168.1.131 ...Open

User Access Verification

Password:
CALI>en
Password:
CALI#
```

- Ping y telnet de LAN cali A Router cali



```
PC4
Physical Config Desktop Programming Attributes
Command Prompt
exit
P
Invalid Command.
C:\>
C:\>PING 192.168.1.65

Pinging 192.168.1.65 with 32 bytes of data:

Reply from 192.168.1.65: bytes=32 time<1ms TTL=255
Reply from 192.168.1.65: bytes=32 time<1ms TTL=255
Reply from 192.168.1.65: bytes=32 time<1ms TTL=255
Reply from 192.168.1.65: bytes=32 time<1ms TTL=255

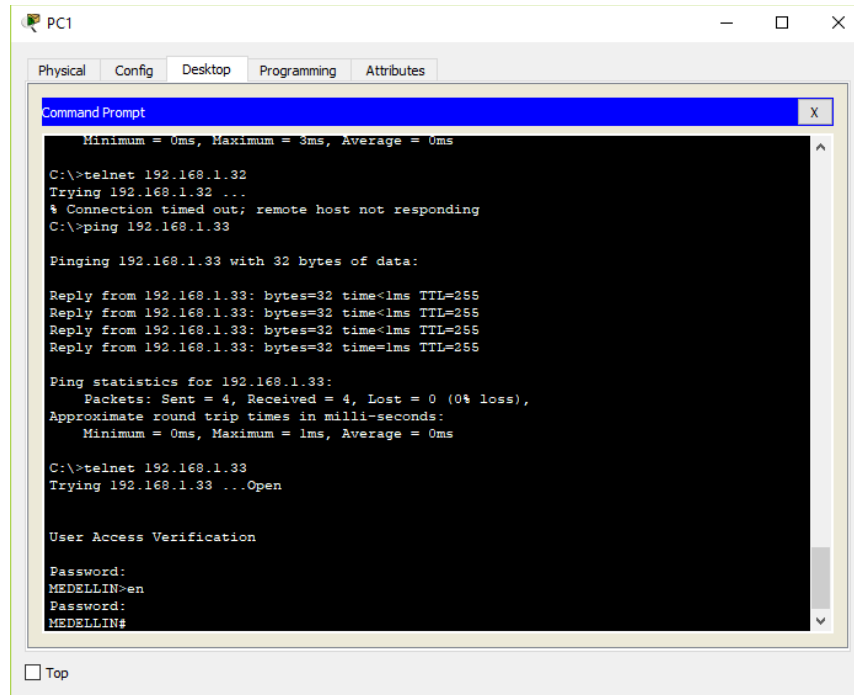
Ping statistics for 192.168.1.65:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>telnet 192.168.1.65
Trying 192.168.1.65 ...Open

User Access Verification

Password:
CALI>en
Password:
CALI#
```

- Ping y telnet de LAN Medellin A router medellin



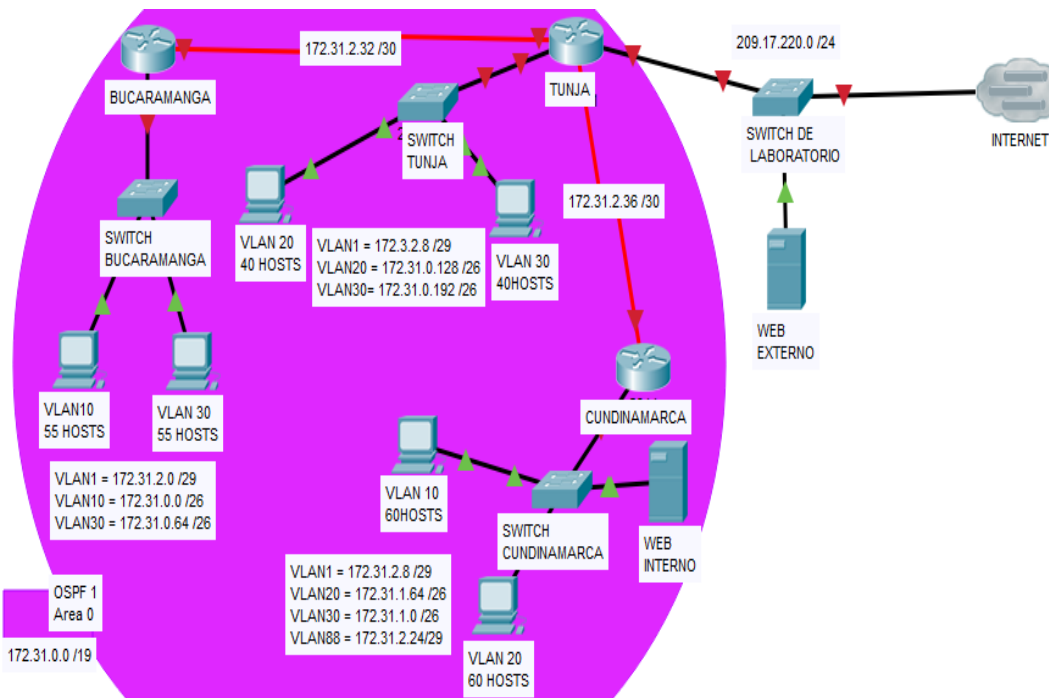
b. Comprobar y Completar la siguiente tabla de condiciones de prueba para confirmar el óptimo funcionamiento de la red e.

	ORIGEN	DESTINO	RESULTADO
TELNET	Router MEDELLIN	Router CALI	EXITOSO
	WS_1	Router BOGOTA	EXITOSO
	Servidor	Router CALI	EXITOSO
	Servidor	Router MEDELLIN	EXITOSO
TELNET	LAN del Router MEDELLIN	Router CALI	EXITOSO
	LAN del Router CALI	Router CALI	EXITOSO
	LAN del Router MEDELLIN	Router MEDELLIN	EXITOSO
	LAN del Router CALI	Router MEDELLIN	EXITOSO
PING	LAN del Router CALI	WS_1	EXITOSO
	LAN del Router MEDELLIN	WS_1	EXITOSO
	LAN del Router MEDELLIN	LAN del Router CALI	EXITOSO
PING	LAN del Router CALI	Servidor	EXITOSO
	LAN del Router MEDELLIN	Servidor	EXITOSO

	Servidor	LAN del Router MEDELLIN	EXITOSO
	Servidor	LAN del Router CALI	EXITOSO
	Router CALI	LAN del Router MEDELLIN	EXITOSO
	Router MEDELLIN	LAN del Router CALI	EXITOSO

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.



Desarrollo

Los siguientes son los requerimientos necesarios:

1. Todos los routers deberán tener los siguiente:

Configuración básica.

- **Configuro ip y hostname router Bucaramanga**

```
Router>EN
```

```
Router#CONF TER
```

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

```
Router(config)#hostname BUCARA
```

```
BUCARA(config)#inter s0/1/0
```

```
BUCARA(config-if)#ip add 172.31.2.34 255.255.255.252
BUCARA(config-if)#no shut
```

```
%LINK-5-CHANGED: Interface Serial0/1/0, changed state to down
BUCARA(config-if)#exit
BUCARA(config)#inter g0/0
BUCARA(config-if)#no shu
```

```
BUCARA(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
```

```
BUCARA(config-if)#exit
BUCARA(config)#end
BUCARA#
%SYS-5-CONFIG_I: Configured from console by console
```

```
BUCARA#wr
Building configuration...
[OK]
BUCARA#
```

- **Configuro Hostname y IPs Router TUNJA**

```
Router>en
Router#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R_TUNJA
R_TUNJA(config)#inter s0/1/0
R_TUNJA(config-if)#ip add 172.31.2.33 255.255.255.252
R_TUNJA(config-if)#no shut

R_TUNJA(config-if)#
%LINK-5-CHANGED: Interface Serial0/1/0, changed state to up

R_TUNJA(config-if)#exit
R_TUNJA(config)#inter s0/1/1
R_TUNJA(config-if)#ip add 172.31.2.37 255.255.255.252
% 172.31.2.36 overlaps with Serial0/1/0
R_TUNJA(config-if)#clock rate 128000
R_TUNJA(config-if)#no shut
R_TUNJA(config-if)#
R_TUNJA#
%SYS-5-CONFIG_I: Configured from console by console
```

```

wr
Building configuration...
[OK]
R_TUNJA#
R_TUNJA>EN
R_TUNJA#CONF TER
Enter configuration commands, one per line. End with CNTL/Z.
R_TUNJA(config)#inter g0/0
R_TUNJA(config-if)#ip add 209.17.220.5 255.255.255.0
R_TUNJA(config-if)#no shut

R_TUNJA(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

R_TUNJA(config-if)#exit
R_TUNJA(config)#inter g0/1
R_TUNJA(config-if)#no shu

R_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

R_TUNJA(config-if)#

R_TUNJA#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
R_TUNJA#

```

- Configuro Hostname y IPs Router CUNDINAMARCA

```

Router>en
Router#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#Hostname R_Cund
R_Cund(config)#inter s0/1/0
R_Cund(config-if)#ip add 172.31.2.38 255.255.255.252
R_Cund(config-if)#no shut

```

```
%LINK-5-CHANGED: Interface Serial0/1/0, changed state to down
R_Cund(config-if)#
R_Cund#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
R_Cund#
R_Cund(config)#inter G0/0
R_Cund(config-if)#no shut
R_Cund(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
```

```
R_Cund(config-if)#
R_Cund#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
R_Cund#
```

- **Activo SSH**

Activo SSH y consola Router Tunja

```
R_TUNJA>en
R_TUNJA#conf termin
Enter configuration commands, one per line. End with CNTL/Z.
R_TUNJA(config)#ip domain name escenario.org
R_TUNJA(config)#ip ssh version 2
Please create RSA keys (of at least 768 bits size) to enable SSH v2.
R_TUNJA(config)#crypto key generate rsa
The name for the keys will be: R_TUNJA.escenario.org
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.
How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
R_TUNJA(config)#do write
*mar. 1 0:16:59.835: %SSH-5-ENABLED: SSH 2 has been enabled
Building configuration...
[OK]
R_TUNJA(config)#line console 0
R_TUNJA(config-line)#password cisco
```

```
R_TUNJA(config-line)#exit
R_TUNJA(config)#service password-encryption
R_TUNJA(config)#enable secret cisco
R_TUNJA(config)#
R_TUNJA#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration.
[OK]
R_TUNJA#
```

- **Activo SSH Router Bucaramanga**

```
BUCARA>en
BUCARA#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
BUCARA(config)#ip domain name escenario.org
BUCARA(config)#ip ssh version 2
Please create RSA keys (of at least 768 bits size) to enable SSH v2.
BUCARA(config)#crypto key generate rsa
The name for the keys will be: BUCARA.escenario.org
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.
```

```
How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
```

```
BUCARA(config)#do wr
*mar. 1 0:27:53.40: %SSH-5-ENABLED: SSH 2 has been enabled
Building configuration...
[OK]
BUCARA(config)#
```

• **Configuro Vlan en Switch y Router**

- **Router Cundinamarca vlan 20, 30 y 1**

```
R_Cund>en
Password:
R_Cund#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
R_Cund(config)#inter g0/0
R_Cund(config-if)#exit
R_Cund(config)#inter g0/0.20
R_Cund(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.20, changed state to up
```

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.20, changed state to up

```
R_Cund(config-subif)#encas
R_Cund(config-subif)#enc
R_Cund(config-subif)#enc
R_Cund(config-subif)#encapsulation dot1Q 20
R_Cund(config-subif)#ip add 172.31.1.65 255.255.255.192
R_Cund(config-subif)#exit
R_Cund(config)#inter g0/0.30
R_Cund(config-subif)#
```

%LINK-5-CHANGED: Interface GigabitEthernet0/0.30, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.30, changed state to up

```
R_Cund(config-subif)#encapsulation dot1Q 30
R_Cund(config-subif)#ip add 172.31.1.1 255.255.255.192
R_Cund(config-subif)#exit
R_Cund(config)#inter g0/0.88
R_Cund(config-subif)#
```

%LINK-5-CHANGED: Interface GigabitEthernet0/0.88, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.88, changed state to up

```
R_Cund(config-subif)#encapsulation dot1Q 88
R_Cund(config-subif)#ip add 172.31.2.25 255.255.255.248
R_Cund(config-subif)#exit
R_Cund(config)#inter g0/0.1
R_Cund(config-subif)#
```

%LINK-5-CHANGED: Interface GigabitEthernet0/0.1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.1, changed state to up

```
R_Cund(config-subif)#encapsulation dot1Q 1
R_Cund(config-subif)#ip add 172.31.2.9 255.255.255.248
R_Cund(config-subif)#exit
R_Cund(config)#
```

R_Cund#

%SYS-5-CONFIG_I: Configured from console by console

wr

Building configuration...

[OK]

R_Cund#

- **Router Tunja vlan 20, 30 y 1**

```
R_TUNJA>en
Password:
R_TUNJA#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
R_TUNJA(config)#inter g0/1.20
R_TUNJA(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1.20, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.20, changed
state to up

R_TUNJA(config-subif)#enca
R_TUNJA(config-subif)#encapsulation dot1Q 20
R_TUNJA(config-subif)#ip add 172.31.0.129 255.255.255.192
R_TUNJA(config-subif)#exit
R_TUNJA(config)#inter g0/1.30
R_TUNJA(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1.30, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.30, changed
state to up

R_TUNJA(config-subif)#encapsulation dot1Q 30
R_TUNJA(config-subif)#ip add 172.31.0.193 255.255.255.192
R_TUNJA(config-subif)#exit
R_TUNJA(config)#inter g0/1.1
R_TUNJA(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1.1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.1, changed
state to up

R_TUNJA(config-subif)#encapsulation dot1Q 1
R_TUNJA(config-subif)#ip add 172.31.2.9 255.255.255.248
R_TUNJA(config-subif)#exit
R_TUNJA(config)#
R_TUNJA#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
R_TUNJA#
```

```
R_TUNJA#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
R_TUNJA(config)#inter g0/1
R_TUNJA(config-if)#ip add 172.3.2.9 255.255.255.248
R_TUNJA(config-if)#no shut
R_TUNJA(config-if)#exit
R_TUNJA(config)#
R_TUNJA#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
```

- Router Bucaramanga vlan 10, 30 y 1

```
BUCARA>en
Password:
BUCARA#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
BUCARA(config)#inter g0/0
BUCARA(config-if)#no shut
BUCARA(config-if)#exit
BUCARA(config)#inter g0/0.10
BUCARA(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.10, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.10, changed
state to up

BUCARA(config-subif)#enca
BUCARA(config-subif)#encapsulation dot1Q 10
BUCARA(config-subif)#ip add 172.31.0.1 255.255.255.192
BUCARA(config-subif)#exit
BUCARA(config)#inter g0/0.30
BUCARA(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.30, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.30, changed
state to up

BUCARA(config-subif)#encapsulation dot1Q 30
BUCARA(config-subif)#ip add 172.31.0.65 255.255.255.192
BUCARA(config-subif)#exit
BUCARA(config)#inter g0/0.1
```

```

BUCARA(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.1, changed
state to up

BUCARA(config-subif)#encapsulation dot1Q 1
BUCARA(config-subif)#ip add 172.31.2.1 255.255.255.248
BUCARA(config-subif)#exit
BUCARA(config)#
BUCARA#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
BUCARA#

```

- SWITCH CUNDINAMARCA Activo VLAN's y asigno puertos Vlan 10, 20 y 88

```

SW-Cund#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
SW-Cund(config)#vlan 88
SW-Cund(config-vlan)#name vlan88
SW-Cund(config-vlan)#exit
SW-Cund(config)#inter f0/1
SW-Cund(config-if)#switchport mode access
SW-Cund(config-if)#switchport access vlan 88
SW-Cund(config-if)#exit
SW-Cund(config)#vlan 10
SW-Cund(config-vlan)#name vlan10
SW-Cund(config-vlan)#exit
SW-Cund(config)#vlan 20
SW-Cund (config-vlan)#name vlan20
SW-Cund(config-vlan)#exit
SW-Cund(config)#interface range f0/2 - 15
SW-Cund(config-if-range)#switchport mode access
SW-Cund(config-if-range)#switchport access vlan 10
SW-Cund(config-if-range)#no shutdown
SW-Cund(config-if-range)#exit
SW-Cund(config)#interface range f0/16 - 22
SW-Cund(config-if-range)#switchport mode access
SW-Cund(config-if-range)#switchport access vlan 20
SW-Cund(config-if-range)#no shutdown
SW-Cund(config-if-range)#exit
SW-Cund(config)#inter g0/1
SW-Cund(config-if)#switchport mode trunk

```

```
SW-Cund(config-if)#no shutdown
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state
to down
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state
to up
```

```
SW-Cund(config-if)#exit
```

```
SW-Cund(config)#
```

```
SW-Cund#
```

```
%SYS-5-CONFIG_I: Configured from console by console
```

```
wr
```

```
Building configuration...
```

```
[OK]
```

```
Switch#
```

- SWITCH TUNJA Activo VLAN's y asigno puertos Vlan 20, 30

```
SW-Tunja>en
```

```
Password:
```

```
SW-Tunja#conf ter
```

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

```
SW-Tunja(config)#vlan 20
```

```
SW-Tunja(config-vlan)#name vlan20
```

```
SW-Tunja(config-vlan)#exit
```

```
SW-Tunja(config)#vlan 30
```

```
SW-Tunja(config-vlan)#name vlan30
```

```
SW-Tunja(config-vlan)#exit
```

```
SW-Tunja(config)#inter range f0/1 -12
```

```
SW-Tunja(config-if-range)#swit
```

```
SW-Tunja(config-if-range)#switchport mode access
```

```
SW-Tunja(config-if-range)#switchport access vlan 20
```

```
SW-Tunja(config-if-range)#no shutdown
```

```
SW-Tunja(config-if-range)#exit
```

```
SW-Tunja(config)#inter range f0/13 - 24
```

```
SW-Tunja(config-if-range)#switchport mode access
```

```
SW-Tunja(config-if-range)#switchport access vlan 30
```

```
SW-Tunja(config-if-range)#no shutdown
```

```
SW-Tunja(config-if-range)#exit
```

```
SW-Tunja(config)#inter g0/1
```

```
SW-Tunja(config-if)#switchport mode trunk
```

```
SW-Tunja(config-if)#
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state
to down
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state
to up
```

```
SW-Tunja(config-if)#exit
```

```

SW-Tunja(config)#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
SW-Tunja#

```

- **SWITCH Bucaramanga Activo VLAN's y asigno puertos Vlan 10, 30**

```

Switch>en
Switch#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SW_Buca
SW_Buca(config)#vlan 10
SW_Buca(config-vlan)#name vlan10
SW_Buca(config-vlan)#exit
SW_Buca(config)#vlan 30
SW_Buca(config-vlan)#name vlan30
SW_Buca(config-vlan)#exit
SW_Buca(config)#inter range f0/1 - 12
SW_Buca(config-if-range)#switchport mode access
SW_Buca(config-if-range)#switchport access vlan 10
SW_Buca(config-if-range)#no shutdown
SW_Buca(config-if-range)#exit
SW_Buca(config)#inter range f0/13 - 24
SW_Buca(config-if-range)#switchport mode access
SW_Buca(config-if-range)#switchport access vlan 30
SW_Buca(config-if-range)#no shutdown
SW_Buca(config-if-range)#exit
SW_Buca(config)#inter g0/1
SW_Buca(config-if)#switchport mode trunk
SW_Buca(config-if)#exit
SW_Buca#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
SW_Buca#

```

- Autenticación local con AAA.

Autenticación usuarios	
Usuario	Clave
cisco	cisco
Cisco1	Cisco1

- **Configuro Router Cundinamarca**

```
R_Cund>en
R_Cund#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
R_Cund(config)#ip domain name escenario.org
R_Cund(config)#ip ssh version 2
Please create RSA keys (of at least 768 bits size) to enable SSH v2.
R_Cund(config)#crypto key generate rsa
The name for the keys will be: R_Cund.escenario.org
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.
```

```
How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
```

```
R_Cund(config)#do wr
*mar. 1 0:23:36.211: %SSH-5-ENABLED: SSH 2 has been enabled
Building configuration...
[OK]
R_Cund(config)#aaa new-model
R_Cund(config)#aaa authentication login Cisco group radius local enable
R_Cund(config)#radius-server host 172.31.2.2 key 0123456789
R_Cund(config)#line vty 0 4
R_Cund(config-line)#transport input ssh
R_Cund(config-line)#login authentication cisco
R_Cund(config)#username cisco secret cisco
R_Cund(config)#username cisco1 secret cisco1
R_Cund(config)#line console 0
R_Cund(config-line)#password cisco
R_Cund(config-line)#exit
R_Cund(config)#service password-encryption
R_Cund(config)#enable secret cisco
R_Cund(config)#do wr
R_Cund(config)#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration.
[OK]
R_Cund#
```

- **Configuro Router TUNJA**

```
R_TUNJA#CONF TERMINAL
Enter configuration commands, one per line. End with CNTL/Z.
R_TUNJA(config)#ip domain name escenario.org
```

```
R_TUNJA(config)#ip ssh version 2
R_TUNJA(config)#crypto key generate rsa
% You already have RSA keys defined named R_TUNJA.escenario.org .
% Do you really want to replace them? [yes/no]: y
The name for the keys will be: R_TUNJA.escenario.org
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.
```

```
How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
```

```
R_TUNJA(config)#
*mar. 1 0:28:57.336: %SSH-5-ENABLED: SSH 2 has been enabled
R_TUNJA(config)#aaa new-model
R_TUNJA(config)#aaa authentication login Cisco group radius local enable
R_TUNJA(config)#radius-server host 172.31.2.26 key 0123456789
R_TUNJA(config)#line vty 0 4
R_TUNJA(config-line)#tra
R_TUNJA(config-line)#transport input ssh
R_TUNJA(config-line)#login authentication Cisco
R_TUNJA(config-line)#exit
R_TUNJA(config)#username Cisco1 secret Cisco1
R_TUNJA(config)#username cisco secret cisco
R_TUNJA(config)#do wr
Building configuration...
[OK]
R_TUNJA(config)#
```

- **Configuro Router Bucaramanga**

```
BUCARA>en
Password:
BUCARA#conf term
Enter configuration commands, one per line. End with CNTL/Z.
BUCARA(config)#ip domain name escenario.org
BUCARA(config)#ip ssh version 2
BUCARA(config)#crypto key generate rsa
% You already have RSA keys defined named BUCARA.escenario.org .
% Do you really want to replace them? [yes/no]: y
The name for the keys will be: BUCARA.escenario.org
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.
```

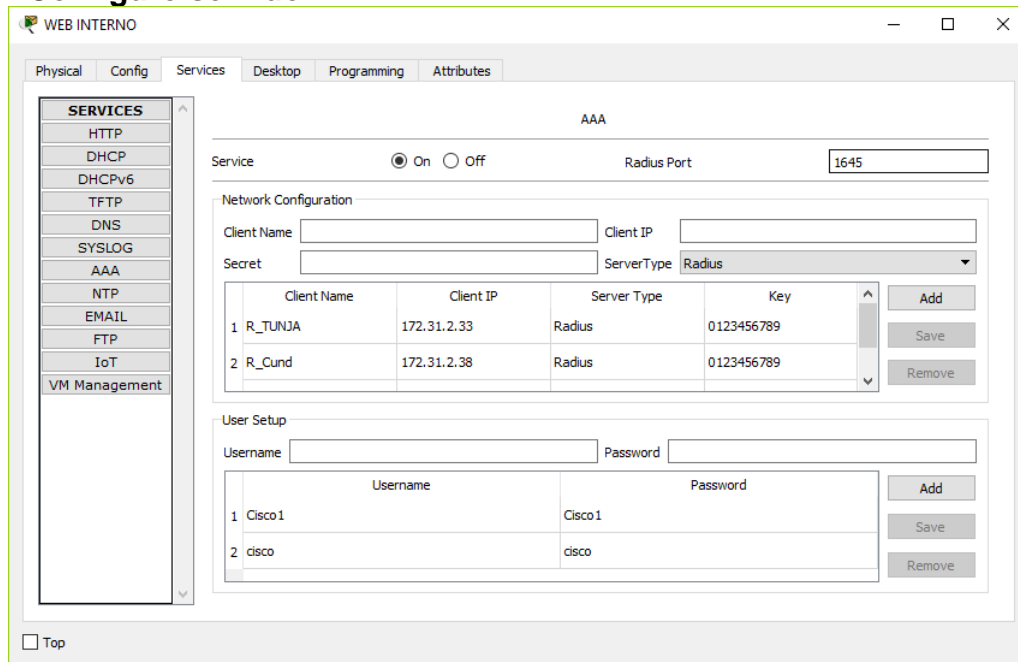
```
How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
```

```

BUCARA(config)#aaa new-model
*mar. 1 0:47:17.507: %SSH-5-ENABLED: SSH 2 has been enabled
BUCARA(config)#aaa authentication login Cisco group radius local enable
BUCARA(config)#radius-server host 172.31.2.26 key 0123456789
BUCARA(config)#line vty 0 4
BUCARA(config-line)#transport input ssh
BUCARA(config-line)#login authentication Cisco
BUCARA(config-line)#exit
BUCARA(config)#username Cisco1 secret Cisco1
BUCARA(config)#username cisco secret cisco
BUCARA(config)#do wr
Building configuration...
[OK]
BUCARA(config)#

```

- Configuro servidor AAA



- Cifrado de contraseñas.

Configuro todos los dispositivos

- Router de Cundinamarca

```

R_Cund#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
R_Cund(config)#service password-encryption
R_Cund(config)#enable secret cisco
R_Cund(config)#exit
R_Cund#

```

- **Router de TUNJA**

```
R_TUNJA#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
R_TUNJA(config)#service password-encryption
R_TUNJA(config)#enable secret cisco
R_TUNJA(config)#exit
R_TUNJA#
```

- **Router de BUCARAMANGA**

```
BUCARA#conf termi
Enter configuration commands, one per line. End with CNTL/Z.
BUCARA(config)#service password-encryption
BUCARA(config)#enable secret cisco
BUCARA(config)#exit
BUCARA#
```

- **Switch de Cundinamarca**

```
SW_Cund (config)#line console 0
SW_Cund(config-line)#password cisco
SW_Cund(config-line)#exit
SW_Cund(config)#service password-encryption
SW_Cund(config)#ena secret cisco
SW_Cund (config)#
SW_Cund#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
SW_Cund#
```

- **Switch de Tunja**

```
SW-Tunja(config)#line console 0
SW-Tunja(config-line)#password cisco
SW-Tunja(config-line)#exit
SW-Tunja(config)#service password-encryption
SW-Tunja(config)#ena secret cisco
SW-Tunja(config)#
SW-Tunja#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
SW-Tunja#
```

- **Switch de Cundinamarca**

```
SW_Buca(config)#line console 0
SW_Buca(config-line)#password cisco
SW_Buca(config-line)#login
SW_Buca(config-line)#exit
SW_Buca(config)#service password-encryption
SW_Buca(config)#enable secret cisco
SW_Buca(config)#
SW_Buca#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
```

• **Router Cundinamarca**

```
R_Cund(config)#ip ssh authentication-retries 3
R_Cund(config)#ip ssh time-out 60
R_Cund(config)#
R_Cund#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
R_Cund#
```

• **Router Tunja**

```
R_TUNJA(config)#ip ssh authentication-retries 3
R_TUNJA(config)#ip ssh time-out 60
R_TUNJA(config)#
R_TUNJA#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
R_TUNJA#
```

• **Router Bucaramanga**

```
BUCARA(config)#ip ssh authentication-retries 3
BUCARA(config)#ip ssh time-out 60
BUCARA(config)#
BUCARA#
%SYS-5-CONFIG_I: Configured from console by console
```

wr
Building configuration...
[OK]
BUCARA#

- Establezca un servidor TFTP y almacene todos los archivos necesarios de los routers.
- **Configuro router de Cundinamarca**

```
R_Cund>enable
Password:
R_Cund#copy running-config tftp
Address or name of remote host []? 172.31.2.26
Destination filename [R_Cund-config]? Backup_R_Cund
```

Writing running-config.....

```
R_Cund#copy flas tftp
Source filename []? c1900-universalk9-mz.SPA.151-1.M4.bin
Address or name of remote host []? 172.31.2.26
Destination filename [c1900-universalk9-mz.SPA.151-1.M4.bin]? Backup_c1900-
universalk9-mz.SPA.151-1.M4.bin
```

R_Cund#

- **Configuro router de TUNJA**

```
R_TUNJA#copy run
R_TUNJA#copy running-config tftp
Address or name of remote host []? 172.31.2.26
Destination filename [R_TUNJA-config]? Backup_R_Tunja
```

Writing running-config.....

```
R_TUNJA#copy flas tftp
Source filename []? c1900-universalk9-mz.SPA
Address or name of remote host []? 172.31.2.26
Destination filename [c1900-universalk9-mz.SPA]? Bakup_c1900-universalk9-mz.SPA
```

- **Configuro router de BUCARAMANGA**

```
BUCARA#copy run
BUCARA#copy running-config tftp
```

Address or name of remote host []? 172.31.2.26
Destination filename [BUCARA-config]? Backup_R_Bucar

Writing running-config....

R_TUNJA#copy flas tftp
Source filename []? c1900-universalk9-mz.SPA
Address or name of remote host []? 172.31.2.26
Destination filename [c1900-universalk9-mz.SPA]? Bakup_c1900-universalk9-mz.SPA

2. El DHCP deberá proporcionar solo direcciones a los hosts de Bucaramanga y Cundinamarca
- **Configuro router de Cundinamarca para DHCP**

```
R_Cund#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
R_Cund(config)#ip dhcp pool vlan20
R_Cund(dhcp-config)#network 172.31.1.64 255.255.255.192
R_Cund(dhcp-config)#dns-server 8.8.8.8
R_Cund(dhcp-config)#default-router 172.31.1.65
R_Cund(dhcp-config)#exit
R_Cund(config)#ip dhcp excluded-address 172.31.1.65
R_Cund(config)#ip dhcp pool vlan30
R_Cund(dhcp-config)#network 172.31.0.192 255.255.255.192
R_Cund(dhcp-config)#dns-server 172.31.0.193
R_Cund(dhcp-config)#exit
R_Cund(config)#ip dhcp excluded-address 172.31.0.193
R_Cund(config)#ip dhcp pool vlan30
R_Cund(dhcp-config)#netwok 172.31.1.0 255.255.255.192
R_Cund(dhcp-config)#dns-server 8.8.8.8
R_Cund(dhcp-config)#default-router 172.31.1.1
R_Cund(dhcp-config)#exit
R_Cund(config)#ip dhcp excluded-address 172.31.1.1
R_Cund(config)#
R_Cund#
%SYS-5-CONFIG_I: Configured from console by console

R_Cund#wr
Building configuration...
[OK]
R_Cund#%DHCPD-4-PING_CONFLICT: DHCP address conflict: server pinged
172.31.1.65.
%DHCPD-4-PING_CONFLICT: DHCP address conflict: server pinged 172.31.1.65.

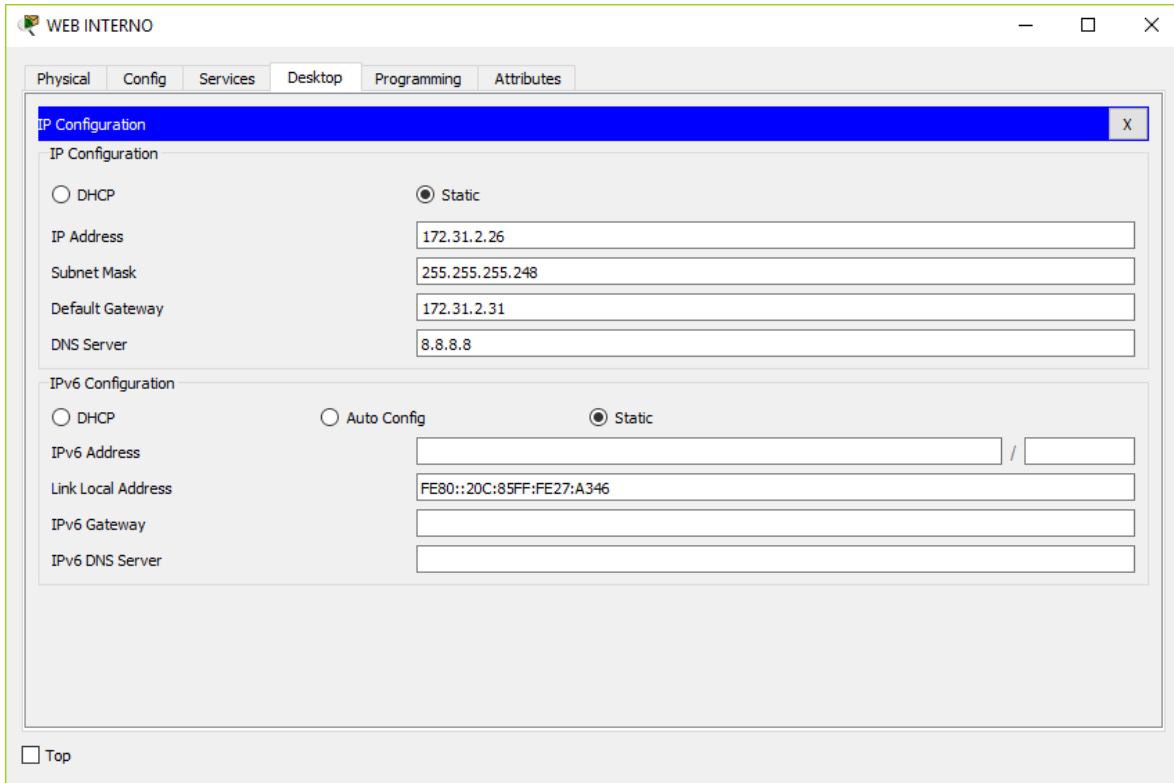
R_Cund#
%SYS-5-CONFIG_I: Configured from console by console
```

R_Cund#

- **Configuro router de Bucaranamaga para DHCP**

```
BUCARA#conf termina
Enter configuration commands, one per line. End with CNTL/Z.
BUCARA(config)#ip dhcp pool vlan10
BUCARA(dhcp-config)#network 172.31.0.0 255.255.255.192
BUCARA(dhcp-config)#dns-server 8.8.8.8
BUCARA(dhcp-config)#default-router 172.31.0.1
BUCARA(dhcp-config)#exit
BUCARA(config)#ip dhcp excluded-address 172.31.0.1
BUCARA(config)#ip dhcp pool vlan30
BUCARA(dhcp-config)#network 172.31.0.64 255.255.255.192
BUCARA(dhcp-config)#dns-server 8.8.8.8
BUCARA(dhcp-config)#default-router 172.31.0.65
BUCARA(dhcp-config)#exit
BUCARA(config)#ip dhcp excluded-address 172.31.0.65
BUCARA(config)#
BUCARA#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
BUCARA#
```

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



4. El enrutamiento deberá tener autenticación.

- **Configuro OSPF de Cundinamarca**

R_Cund#conf ter

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

R_Cund(config)#router ospf 1

R_Cund(config-router)#network 172.31.2.36 0.0.0.3 area 0

R_Cund(config-router)#network 172.31.2.0 0.0.0.3 area 0

R_Cund(config-router)#network 172.31.2.24 0.0.0.7 area 0

R_Cund(config-router)#network 172.31.1.0 0.0.0.63 area 0

R_Cund(config-router)#network 172.31.1.64 0.0.0.63 area 0

R_Cund(config-router)#network 172.3.2.8 0.0.0.7 area 0

R_Cund(config-router)#

03:38:00: %OSPF-5-ADJCHG: Process 1, Nbr 209.17.220.5 on Serial0/1/0 from LOADING to FULL, Loading Done

R_Cund(config-router)#network 172.31.2.8 0.0.0.3 area 0

R_Cund(config-router)#exit

R_Cund(config)#inter s0/1/0

R_Cund(config-if)#ip ospf message-digest-key 1 md5 cisco

R_Cund(config-if)#ip ospf authentication message-digest

```
R_Cund(config-if)#exit
R_Cund(config)#exit
R_Cund#wr
```

```
R_Cund#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
R_Cund#
```

- **Configuro OSPF de TUNJA**

```
R_TUNJA#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
R_TUNJA(config)#router ospf 1
R_TUNJA(config-router)#network 172.31.0.0 0.0.0.3 area 0
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/1, changed state to
down

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed state to
down

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface router ospf 1
R_TUNJA(config-router)#network 172.31.2.0 0.0.0.3 area 0
R_TUNJA(config-router)#network 172.31.2.32 0.0.0.3 area 0
R_TUNJA(config-router)#network 172.31.2.36 0.0.0.3 area 0
R_TUNJA(config-router)#network 209.17.220.5 0.0.0.255 area 0
R_TUNJA(config-router)#network 172.31.0.128 0.0.0.63 area 0
R_TUNJA(config-router)#network 172.31.0.192 0.0.0.63 area 0
R_TUNJA(config-router)#network 172.3.2.8 0.0.0.7 area 0
R_TUNJA(config-router)#
03:36:36: %OSPF-5-ADJCHG: Process 1, Nbr 172.31.2.34 on Serial0/1/0 from LOADING
to FULL, Loading Done

R_TUNJA(config-router)#exit
R_TUNJA(config)#inter s0/1/0
R_TUNJA(config-if)#ip ospf message-digest-key 1 md5 cisco
R_TUNJA(config-if)#ip ospf authentication message-digest
R_TUNJA(config-if)#exit
R_TUNJA(config)#inter s0/1/1
R_TUNJA(config-if)#ip ospf message-digest-key 1 md5 cisco
R_TUNJA(config-if)#ip ospf authentication message-digest
R_TUNJA(config-if)#do write
R_TUNJA#wr
```

Building configuration...
[OK]

- **Configuro OSPF de Bucaramanga**

```
BUCARA#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
BUCARA(config)#router ospf 1
BUCARA(config-router)#network 172.31.0.0 0.0.0.3 area 0
BUCARA(config-router)#network 172.31.2.0 0.0.0.3 area 0
BUCARA(config-router)#network 172.31.2.32 0.0.0.3 area 0
BUCARA(config-router)#network 172.31.2.0 0.0.0.7 area 0
BUCARA(config-router)#network 172.31.0.0 0.0.0.63 area 0
BUCARA(config-router)#network 172.31.0.64 0.0.0.63 area 0
BUCARA(config-router)#exit
BUCARA(config)#inter s0/1/0
BUCARA(config-if)#ip ospf message-digest-key 1 md5 cisco
BUCARA(config-if)#ip ospf authentication message-digest
BUCARA(config-if)#exit
BUCARA(config)#
BUCARA#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
BUCARA#
```

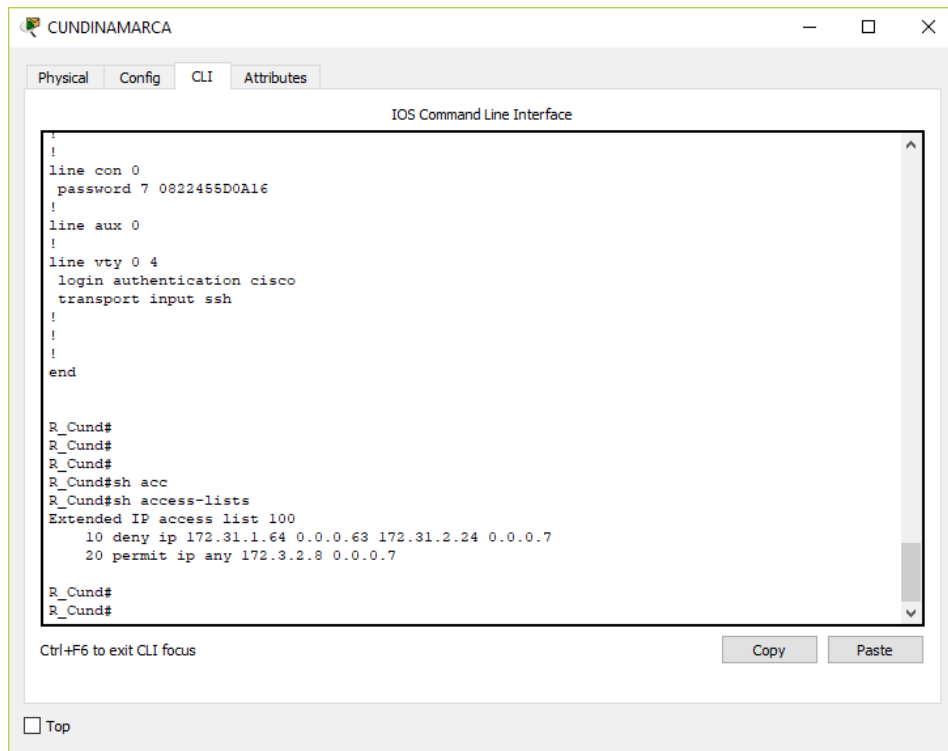
5. **Listas de control de acceso:**

- Los hosts de VLAN 20 en Cundinamarca no acceden a internet, solo a la red interna de Tunja.

- **Configuro Router Cundinamarca**

```
R_Cund(config)#access-list 100 deny ip 172.31.1.64 0.0.0.63 172.31.2.24 0.0.0.7
R_Cund(config)#access-list 100 permit ip any 172.31.2.8 0.0.0.7
R_Cund(config)#
R_Cund#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
R_Cund(config)#inter g0/0.20
R_Cund(config-subif)#
% Unknown command or computer name, or unable to find computer address

R_Cund(config-subif)#ip access-group 100 in
R_Cund(config-subif)#
```



- Los hosts de VLAN 30 en Cundinamarca si acceden a internet y no a la red interna de Tunja.
- **Configuro Router Cundinamarca**

```

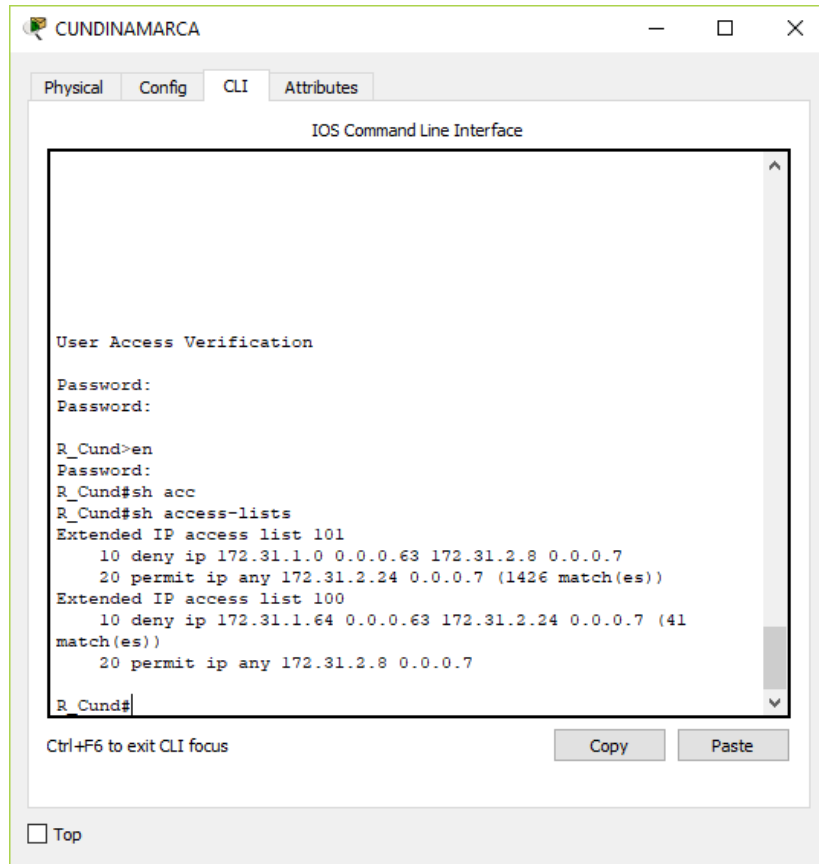
R_Cund(config)#access-list 101 deny ip 172.31.1.0 0.0.0.63 172.31.2.8 0.0.0.7
R_Cund(config)#access-list 101 permit ip any 172.31.2.24 0.0.0.7
R_Cund(config)#inter g0/0.30
R_Cund(config-subif)#ip access-group 101 in
R_Cund(config-subif)#

```

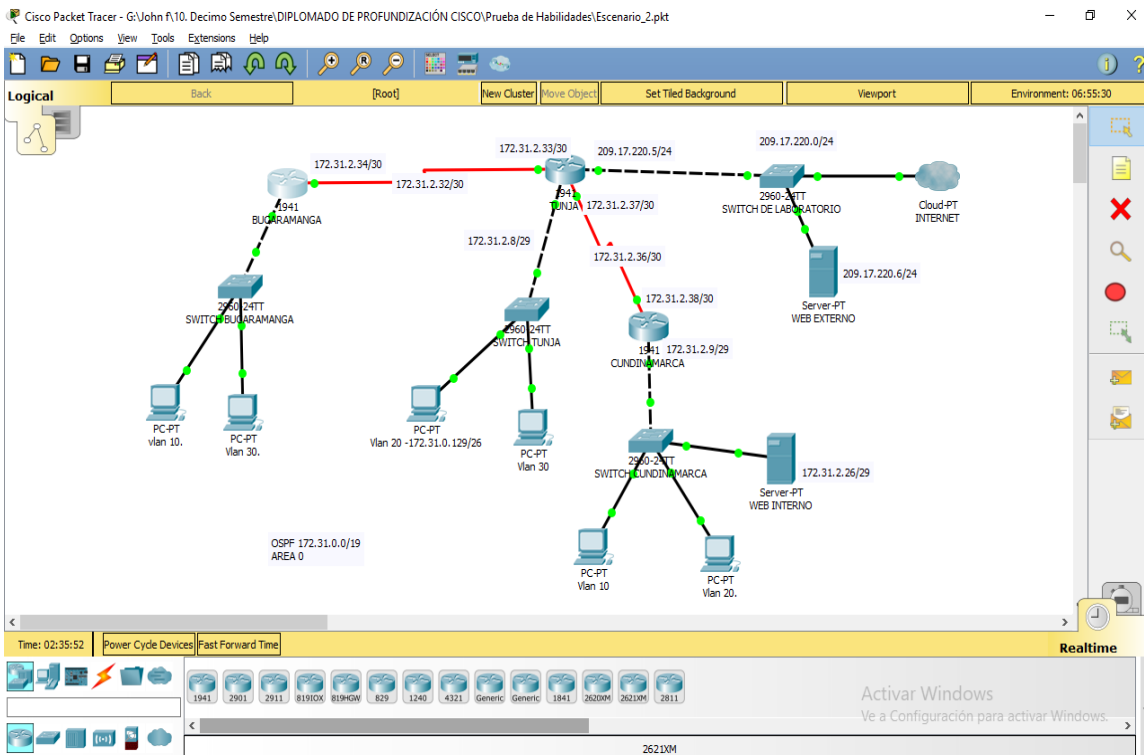
```

access-list 101 deny ip 172.31.1.0 0.0.0.63 172.31.2.8 0.0.0.7
access-list 101 permit ip any 172.31.2.24 0.0.0.7
access-list 100 deny ip 172.31.1.64 0.0.0.63 172.31.2.24 0.0.0.7
access-list 100 permit ip 172.31.2.24 0.0.0.7 any

```



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



Conclusiones

- Este proyecto de simulación con Packet Tracer nos ayudo con la seguridad, controlar el tráfico, permitir y bloquear al usar ACL, creo que es una herramienta de mucha ayuda para realizar cada uno de los procesos anteriormente mencionados, pues esta es fácil de configurar, se presta para analizar las rutas de una topología y optimizar el debido funcionamiento de cualquier red
- Al desarrollar las listas de acceso (ALC), puedo concluir que la seguridad dentro de una red es indispensable para la protección de los dispositivos y la información que se transporta por medio de esos dispositivos que administran nuestra red.
- Puedo concluir que el protocolo EIGRP es un protocolo sencillo que ayuda a muchos procesos dentro de la implementación de red, ayuda a saber cuándo se presentan daños, permite conocer dispositivos que son vecinos o están conectados adyacentemente, enruta de manera ordenada las direcciones de las interfaces.
- Packet Tracer destinado a la simulación de conexión de computadores, tables, celulares en una red, permite conocer más a fondo las configuraciones de red que se realiza para una posterior aplicación.
- Para la configuración del protocolo de enrutamiento del OSPFv2 se debe crear el proceso de OSPF desde la configuración global con el comando "router ospf", después se deben configurar los rangos de red mediante "network área", todas las interfaces que se incluyan mediante ese comando estarán participando en esa área de OSPF.
- Las herramientas de simulación permiten establecer escenarios LAN/WAN para realizar un análisis sobre el comportamiento de diversos protocolos y métricas de enrutamiento.

- El protocolo OSPF (Open Shortest Path First) es un protocolo de routing de estado de enlace desarrollado como reemplazo del protocolo de routing vector distancia RIP.
- OSPF es un protocolo de enrutamiento sin clase que utiliza el concepto de áreas para realizar la escalabilidad.

Bibliografía

- **Temática: Listas de control de acceso**

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>

- **Temática: Traducción de direcciones IP para IPv4**

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>

- **OVA Unidad 4 - Video - Principios de Enrutamiento**

Este Objeto Virtual de Aprendizaje, titulado Video - Principios de Enrutamiento, tiene como objetivo, orientar al estudiante sobre la configuración básica de Switches y Routers. Vesga, J. (2014). Principios de Enrutamiento [OVA]. Recuperado de https://1drv.ms/u/s!AmlJYei-NT1lhgOyjWeh6timi_Tm

- **Temática: Enrutamiento entre VLANs**

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>

- **OVA Unidad 3 - Configuración de Switches y Routers**

Este Objeto Virtual de Aprendizaje, titulado • Video - Configuración de Switches y Routers, tiene como objetivo, orientar al estudiante sobre la configuración básica de Switches y Routers.

Vesga, J. (2014). Configuración de Switches y Routers [OVA]. Recuperado de <https://1drv.ms/u/s!AmlJYei-NT1lhgL9QChD1m9EuGqC>