DIPLOMADO DE PROFUNDIZACION CISCO

LUIS HUMBERTO VILLAMIL MAHECHA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA –

UNAD PROGRAMA DE INGENIERIA TELECOMUNICACIONES

CEAD JAG 2020

DIPLOMADO DE PROFUNDIZACION CISCO

Luis Humberto Villamil Mahecha

Diplomado de opción de grado presentado para optar el titulo
de INGENIERO DE TELECOMUNICACIONES

TUTOR:

GIOVANNI ALBERTO BRACHO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA –

UNAD PROGRAMA DE INGENIERIA TELECOMUNICACIONES

CEAD JAG 2020

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Bogotá, 12 de diciembre de 2019

DEDICATORIA

CONTENIDO

Tabla de contenido

RESUMEN

Para la prueba de habilidades requeridas en el diplomado de CCNA se requiere haber obtenido previamente los conocimientos necesarios a través de las diferentes actividades, proponiendo así una solución efectiva aplicando los diferentes conocimientos, los cuales serán aplicados por las personas que decidan aplicar sus conocimientos en esta área tan importante de las telecomunicaciones, pudiendo así aprovechar al máximo y engrosar los conocimientos adquiridos.

Siendo así buscamos mostrar en este documento la solución de los escenarios propuestos para ser resueltos, evidenciando que esto es aplicado a un ejercicio que puede ser aplicado en una compañía, teniendo en cuenta las configuraciones que se realizaron en los diferentes equipos de la red y validando el funcionamiento se debe proceder con la solución.

ABSTRACT

For the test of skills required in the CCNA diploma it is required to have previously obtained the necessary knowledge through the different activities, thus proposing an effective solution applying the different knowledge, which will be applied by the people who decide to apply their knowledge in this such an important area of telecommunications, thus being able to make the most of and increase the knowledge acquired.

Thus, we seek to show in this document the solution of the scenarios proposed to be solved, evidencing that this is applied to an exercise that can be applied in a company, taking into account the configurations that were made in the different network equipment and validating The operation must proceed with the solution.

GLOSARIO

GNS3: Es un simulador gráfico de red que te permite diseñar topologías de red complejas y poner en marcha simulaciones sobre ellos. Para permitir completar simulaciones, GNS3 está estrechamente vinculada con: Dynamips, un emulador de IOS que permite a los usuarios ejecutar binarios e imágenes IOS de Cisco Systems.

Networking: Es una red de computadoras, también llamada red de ordenadores, red de comunicaciones de datos o red informática conjunto de equipos informáticos y software reconectados entre sí por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de compartir información, recursos y ofrecer servicios.

Protocolos de red: Conjunto de normas standard que especifican el método para enviar y recibir datos entre varios ordenadores. Es una convención que controla o permite la conexión, comunicación, y transferencia de datos entre dos puntos finales.

VLAN: Es un método para crear redes lógicas independientes dentro de una misma red física. Varias VLAN pueden coexistir en un único conmutador físico o en una única red física. Son útiles para reducir el dominio de difusión y ayudan en la administración de la red, separando segmentos lógicos de una red de área local.

OBJETIVOS

General

Se requiere aplicar los conocimientos y habilidades adquiridas en el transcurso del curso, brindando solución a los escenarios propuestos en la guía, por medio del software Packet tracer, complementando así la práctica.

Específicos

- Validar las configuraciones básicas de los equipos de red, incluyendo routers, switchs y computadores.
- Aplicar las configuraciones correspondientes a los protocolos de enrutamiento.
- Configurar las rutas de acceso para comprender su funcionamiento en la protección y restricción de los dispositivos

INTRODUCCIÓN

La certificación CCNA permite aumentar la capacidad de planificar, implementar, verificar y solucionar problemas en redes empresariales LAN y WAN, también de integrar soluciones de: seguridad, voz, inalámbricas y video, el desarrollo de habilidades practicas permite que se implementen las temáticas en los escenarios propuestos.

El Diplomado como opción de grado está constituido por dos módulos: CCNA ROUTE y CCNA SWITCH, los cuales forman parte del currículo CCNA de la Academia CISCO.

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.

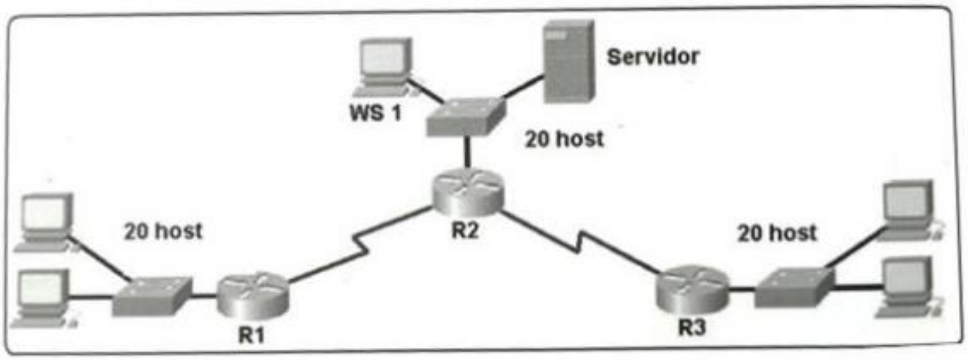
Parte 2: Considerar la asignación de los parámetros básicos y la detección de vecinos directamente conectados.

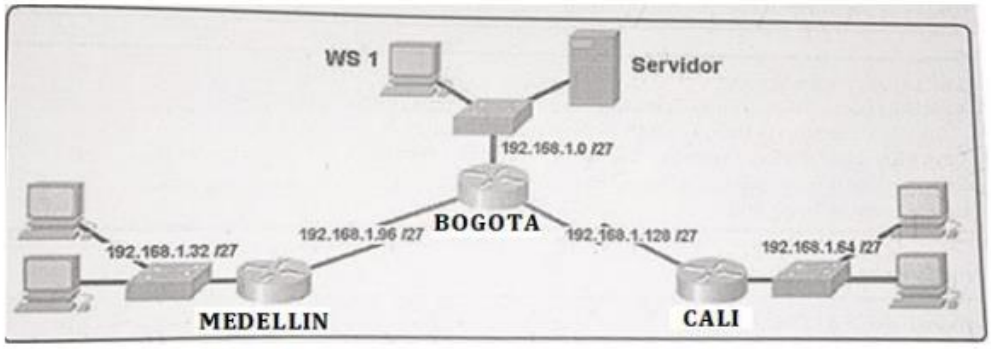
Parte 3: La red y subred establecidas deberán tener una interconexión total, todos los hosts deberán ser visibles y poder comunicarse entre ellos sin restricciones.

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: Configuration final.






```
Router#conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname BOGOTA
BOGOTA(config)#service encry
BOGOTA(config)#service pass
BOGOTA(config)#service password-encryption
BOGOTA(config)#banner motd &###Solo personal autorizado###&
BOGOTA(config)#enable secret class
BOGOTA(config)#line cons
BOGOTA(config)#line console 0
BOGOTA(config-line)#pass
BOGOTA(config-line)#password cisco
BOGOTA(config-line)#login
BOGOTA(config-line)#logging syn
BOGOTA(config-line)#logging synchronous
```

```
BOGOTA(config-line)#line vty 0 15
BOGOTA(config-line)#pass
BOGOTA(config-line)#password cisco
BOGOTA(config-line)#login
BOGOTA(config-line)#logging synchronous
BOGOTA(config-line)#no ip domain-lookup
ROUTER 2 MEDELLIN
Router>enable
Router#config t
Router(config)#hostname MEDELLN
MEDELLN(config)#no ip domain-lookup
MEDELLN(config)#service pass
MEDELLN(config)#service password-encryption
MEDELLN(config)#enable secret class
MEDELLN(config)#banner motd &###solo personal autorizado###&
MEDELLN(config)#line console 0
MEDELLN(config-line)#password cisco
MEDELLN(config-line)#login
MEDELLN(config-line)#logging syn
MEDELLN(config-line)#logging synchronous
MEDELLN(config-line)#line vty 0 15
MEDELLN(config-line)#password cisco
MEDELLN(config-line)#login
MEDELLN(config-line)#logg
MEDELLN(config-line)#logging syn
MEDELLN(config-line)#logging synchronous
MEDELLN(config-line)#copy run
MEDELLN(config-line)#end
ROUTER 3 CALI
Router>enable
Router#conf terminal
```

```
Router(config)#hostname CALI
CALI(config)#no ip domain-lookup
CALI(config)#service password-encryption
CALI(config)#enable secret class
CALI(config)#banner motd &###solo personal autorizado###&
CALI(config)#line console 0
CALI(config-line)#password cisco
CALI(config-line)#login
CALI(config-line)#logging synchronous
CALI(config-line)#line vty 0 15
CALI(config-line)#password cisco
CALI(config-line)#login
CALI(config-line)#logging synchronous
```

SWITCH DE BOGOTA

```
Switch>enable
Switch#CONF Terminal
Switch(config)#hostname SW-BOGOTA
SW-BOGOTA(config)#no ip domain-lookup
SW-BOGOTA(config)#service password-encryption
SW-BOGOTA(config)#enable secret class
SW-BOGOTA(config)#banner motd &###solo personal autorizado###&
SW-BOGOTA(config)#line console 0
SW-BOGOTA(config-line)#password cisco
SW-BOGOTA(config-line)#login
SW-BOGOTA(config-line)#logging synchronous
SW-BOGOTA(config-line)#line vty 0 15
SW-BOGOTA(config-line)#password cisco
SW-BOGOTA(config-line)#login
SW-BOGOTA(config-line)#logging synchronous
```

SWITCH DE MEDELLÍN

```
Switch>enable
Switch#configure Terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SW-MEDELLIN
SW-MEDELLIN(config)#no ip domain-lookup
SW-MEDELLIN(config)#service password-encryption
SW-MEDELLIN(config)#enable secret class
SW-MEDELLIN(config)#banner motd &###solo personal autorizado###&
SW-MEDELLIN(config)#line console 0
SW-MEDELLIN(config-line)#password cisco
SW-MEDELLIN(config-line)#login
SW-MEDELLIN(config-line)#logging synchronous
SW-MEDELLIN(config-line)#line vty 0 15
SW-MEDELLIN(config-line)#password cisco
SW-MEDELLIN(config-line)#login
SW-MEDELLIN(config-line)#logging synchronous
SW-MEDELLIN(config-line)#
```

```
SWITCH DE CALI
Switch>enable
Switch#conf t
Switch#conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SW-CALI
SW-CALI(config)#no ip domain-lookup
SW-CALI(config)#service password-encryption
SW-CALI(config)#enable secret class
SW-CALI(config)#banner motd &SOLO PERSONAL AUTORIZADO&
SW-CALI(config)#line console 0
SW-CALI(config-line)#password cisco
```

```
SW-CALI(config-line)#login
SW-CALI(config-line)#logging synchronous
SW-CALI(config-line)#line vty 0 15
SW-CALI(config-line)#password cisco
SW-CALI(config-line)#login
SW-CALI(config-line)#logging synchronous
```

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.

Tabla 1: tabla para el subneting

SUBNETING			
RED	**SUBRED**	**DIRECCION IP**	**MASCARA DE SUBRED**
1	**BOGOTA**	**192.168.1.0**	**255.255.255.224**
2	**MEDELLIN**	**192.168.1.32**	**255.255.255.224**
3	**CALI**	**192.168.1.64**	**255.255.255.224**
4	**BOGOTA-MEDELLIN**	**192.168.1.96**	**255.255.255.224**
5	**BOGOTA-CALI**	**192.168.1.128**	**255.255.255.224**
6	**RED 6**	**192.168.1.160**	**255.255.255.224**
7	**RED 7**	**192.168.1.192**	**255.255.255.224**
8	**RED 8**	**192.168.1.224**	**255.255.255.224**

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.

Se realiza la revisión de las rutas mediante el comando show ip route, no se tiene protocolo de enrutamiento ni rutas estáticas, por lo que se conoce las redes configuradas localmente en cada interfaces.

A continuación, la evidencia de las rutas que se aprenden en cada uno de los Equipos:

MEDELLIN:

```
MEDELLIN#show ip 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, Serial0/3/0
L 192.168.1.99/32 is directly connected, Serial0/3/0
```

BOGOTA:

```
BOGOTA#show ip 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, Serial0/3/0
L 192.168.1.98/32 is directly connected, Serial0/3/0
C 192.168.1.128/27 is directly connected, Serial0/3/1
L 192.168.1.130/32 is directly connected, Serial0/3/1
```

CALI

```
CALI#show ip route
Gateway of last resort is not set
192.168.1.0/24 is variably subnetted, 4 subnets, 2 masks
C 192.168.1.64/27 is directly connected, GigabitEthernet0/0
L 192.168.1.65/32 is directly connected, GigabitEthernet0/0
C 192.168.1.128/27 is directly connected, Serial0/3/0
L 192.168.1.131/32 is directly connected, Serial0/3/0
```

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

No se observa balanceo puesto que no se han configurado los protocolos de enrutamiento.

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

Se valida con el comnado show cdp neighbors y se conocen los vecinos que están conectados a cada dispositivo

```
BOGOTA#show 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
Switch Gig 0/0 149 S 2960 Fas 0/1
MEDELLIN Ser 0/3/0 149 R C2900 Ser 0/3/0
CALI Ser 0/3/1 149 R C2900 Ser 0/3/0
```

CALI#show 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
Switch Gig 0/0 137 S 2960 Fas 0/1
BOGOTA Ser 0/3/0 137 R C2900 Ser 0/3/1
```

MEDELLIN#show 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
Switch Gig 0/0 120 S 2960 Fas 0/1
BOGOTA Ser 0/3/0 179 R C2900 Ser 0/3/0
```

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

Se procede a ejecutar comando ping validando conectividad desde Bogotá hacia Cali y Medellín, pero desde Cali hacia Medellín no se alcanza y viceversa.

Prueba desde Bogota

```
BOGOTA#ping 192.168.1.99
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.99, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/12 ms
BOGOTA#ping 192.168.1.131
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.131, timeout is 2 seconds:
```

```
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/8 ms
```

Prueba desde Cali

```
CALI#ping 192.168.1.130
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.130, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/9 ms
CALI#ping 192.168.1.98
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.98, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

Prueba desde Medellin

```
MEDELLIN#ping 192.168.1.98
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.98, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
MEDELLIN#ping 192.168.1.131
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.131, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

Parte 3: Configuración de Enrutamiento.

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

Se configura el protocolo de enrutamiento dinámico EIGRP con las redes que están

directamente conectadas a las interfaces de cada router para su respectiva

propagación en la red, en las siguientes líneas se observa como se aplicaron en

cada dispositivo:

```
BOGOTA(config)#router eigrp 200
BOGOTA(config-router)#network 192.168.1.96 0.0.0.31
BOGOTA(config-router)#network 192.168.1.128 0.0.0.31
BOGOTA(config-router)#network 192.168.1.1 0.0.0.31
CALI(config)#router eigrp 200
CALI(config-router)#network 192.168.1.64 0.0.0.31
CALI(config-router)#network 192.168.1.128 0.0.0.31
CALI(config-router)#end
MEDELLIN(config)#router eigrp 200
MEDELLIN(config-router)#network 192.168.1.98 0.0.0.31
MEDELLIN(config-router)#network 192.168.1.32 0.0.0.31
MEDELLIN(config-router)#end
```

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

Mediante el comando show ip eigrp neigbors se identifica los vecinos que se están conociendo mediante el protocolo EIGRP en cada router, en las siguientes líneas se evidencian cada una de las salidas de los routers:

```
BOGOTA#show ip eigrp neighbors
IP-EIGRP neighbors for process 200
H Address Interface Hold Uptime SRTT RTO Q Seq
(sec) (ms) Cnt Num
0 192.168.1.99 Se0/3/0 13 00:06:24 40 1000 0 9
1 192.168.1.131 Se0/3/1 14 00:04:28 40 1000 0 7
CALI#show ip eigrp neighbors
IP-EIGRP neighbors for process 200
H Address Interface Hold Uptime SRTT RTO Q Seq
```

```
(sec) (ms) Cnt Num
0 192.168.1.130 Se0/3/0 11 00:05:03 40 1000 0 6
MEDELLIN#show ip eigrp neighbors
IP-EIGRP neighbors for process 200
H Address Interface Hold Uptime SRTT RTO Q Seq
(sec) (ms) Cnt Num
0 192.168.1.98 Se0/3/0 13 00:07:28 40 1000 0 5
```

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

Se lanza de nuevo en todos los routers el comando show ip route con el cual ya se observan todas las redes que se configuraron y que se están recibiendo mediante el protocolo EIGRP.

```
BOGOTA#show ip route
Gateway of last resort is not set
192.168.1.0/24 is variably subnetted, 8 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
D 192.168.1.32/27 [90/2172416] via 192.168.1.99, 00:09:00, Serial0/3/0
D 192.168.1.64/27 [90/2172416] via 192.168.1.131, 00:07:23, Serial0/3/1
C 192.168.1.96/27 is directly connected, Serial0/3/0
L 192.168.1.98/32 is directly connected, Serial0/3/0
C 192.168.1.128/27 is directly connected, Serial0/3/1
L 192.168.1.130/32 is directly connected, Serial0/3/1
CALI#sh ip route
Gateway of last resort is not set
192.168.1.0/24 is variably subnetted, 7 subnets, 2 masks
D 192.168.1.0/27 [90/2172416] via 192.168.1.130, 00:08:22, Serial0/3/0
D 192.168.1.32/27 [90/2684416] via 192.168.1.130, 00:08:22, Serial0/3/0
C 192.168.1.64/27 is directly connected, GigabitEthernet0/0
L 192.168.1.65/32 is directly connected, GigabitEthernet0/0
```

```
D 192.168.1.96/27 [90/2681856] via 192.168.1.130, 00:08:22, Serial0/3/0
C 192.168.1.128/27 is directly connected, Serial0/3/0
L 192.168.1.131/32 is directly connected, Serial0/3/0
MEDELLIN#sh ip route
Gateway of last resort is not set
192.168.1.0/24 is variably subnetted, 7 subnets, 2 masks
D 192.168.1.0/27 [90/2172416] via 192.168.1.98, 00:11:01, Serial0/3/0
C 192.168.1.32/27 is directly connected, GigabitEthernet0/0
L 192.168.1.33/32 is directly connected, GigabitEthernet0/0
D 192.168.1.64/27 [90/2684416] via 192.168.1.98, 00:09:06, Serial0/3/0
C 192.168.1.96/27 is directly connected, Serial0/3/0
L 192.168.1.99/32 is directly connected, Serial0/3/0
D 192.168.1.128/27 [90/2681856] via 192.168.1.98, 00:11:01, Serial0/3/0
```

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.

Mediante el comando ping se ejecutan las pruebas de conectividad entre los diferentes dispositivos, confirmando que responden correctamente entre todos, a continuación, las evidencias de las pruebas ejecutadas:

```
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=1ms TTL=126

Reply from 192.168.1.3: bytes=32 time=1ms TTL=126

Reply from 192.168.1.3: bytes=32 time=4ms TTL=126

Reply from 192.168.1.3: bytes=32 time=13ms TTL=126

Ping statistics for 192.168.1.3:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round
trip times

in milli-seconds:Minimum = 1ms, Maximum = 13ms, Average = 4ms

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 = 1ms, Average = 0ms
```

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.

ROUTER BOGOTÁ

```
SW-BOGOTA(config)#line console 0
SW-BOGOTA(config-line)#password cisco
SW-BOGOTA(config-line)#login
SW-BOGOTA(config-line)#logging synchronous
SW-BOGOTA(config-line)#line vty 0 15
SW-BOGOTA(config-line)#password cisco
SW-BOGOTA(config-line)#login
SW-BOGOTA(config-line)#logging synchronous
```

ROUTER MEDELLÍN

```
SW-MEDELLIN(config)#line console 0
SW-MEDELLIN(config-line)#password cisco
SW-MEDELLIN(config-line)#login
SW-MEDELLIN(config-line)#logging synchronous
SW-MEDELLIN(config-line)#line vty 0 15
SW-MEDELLIN(config-line)#password cisco
SW-MEDELLIN(config-line)#login
SW-MEDELLIN(config-line)#logging synchronous
```

ROUTER CALI

```
SW-CALI(config)#line console 0
SW-CALI(config-line)#password cisco
SW-CALI(config-line)#login
```

```
SW-CALI(config-line)#logging synchronous
SW-CALI(config-line)#line vty 0 15
SW-CALI(config-line)#password cisco
SW-CALI(config-line)#login
SW-CALI(config-line)#logging synchronous
```

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.

ACL MEDELLÍN

```
MEDELLIN>en
Password:
MEDELLIN#conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN(config)#acc
MEDELLIN(config)#access-list 101 per
MEDELLIN(config)#access-list 101 permit ip 192.168.1.32 0.0.0.31 host
192.168.1.6
MEDELLIN(config)#int g
MEDELLIN(config)#int gigabitEthernet 0/0
MEDELLIN(config-if)#ip access-group 101 in
MEDELLIN(config-if)#
```

ACL CALI

```
CALI#
CALI#conf t
CALI#conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
CALI(config)#acc
CALI(config)#access-list 101 per
CALI(config)#access-list 101 permit ip 192.168.1.64 0.0.0.31 host
192.168.1.6
```

```
CALI(config)#int g
CALI(config)#int gigabitEthernet 0/0
CALI(config-if)#ip access-group 101 in
CALI(config-if)#
```

COMPROBACION DE LA LISTA DE CONTROL DE ACCESO

```
Pinging 192.168.1.6 with 32 bytes of data:
Reply from 192.168.1.6: bytes=32 time=13ms TTL=126
Reply from 192.168.1.6: bytes=32 time=11ms TTL=126
Reply from 192.168.1.6: bytes=32 time=12ms TTL=126
Reply from 192.168.1.6: bytes=32 time=15ms TTL=126
Ping statistics for 192.168.1.6:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 11ms, Maximum = 15ms, Average = 12ms
C:\>ping 192.168.1.5
Pinging 192.168.1.5 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 192.168.1.5:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
Pinging 192.168.1.3 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 192.168.1.3:
 Packets: Sent = 4, Received = 0, Lost = 4 (100% loss)
```

Se configuran las listas de acceso permitiendo solo la conexión desde redes específicas para cumplir con lo requerido y aumentar la seguridad sobre los dispositivos, las listas fueron llamadas sobre la línea de acceso vty 0 4 que es la que permite la conexión mediante el protocolo telnet.

A continuación, cada una de las líneas de comando aplicada para cada router:

Medellin

```
access-list 110 permit ip 192.168.1.96 0.0.0.31 any
access-list 110 permit ip 192.168.1.130 0.0.0.31 any
access-list 110 permit ip 192.168.1.3 0.0.0.0 any
access-list 110 deny ip any any
```

Bogota

```
access-list 110 permit ip 192.168.1.96 0.0.0.31 any
access-list 110 permit ip 192.168.1.130 0.0.0.31 any
access-list 110 permit ip 192.168.1.3 0.0.0.0 any
access-list 110 deny ip any any
```

Cali

```
access-list 110 permit ip 192.168.1.96 0.0.0.31 any
access-list 110 permit ip 192.168.1.130 0.0.0.31 any
access-list 110 permit ip 192.168.1.3 0.0.0.0 any
access-list 110 deny ip any any

line vty 0 4
access-class 110 in
```

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.

Se configuran las listas de acceso permitiendo solo la conexión a redes específicas para cumplir con lo requerido, las listas fueron llamadas sobre la interfaz gi0/0 que es la que permite la conexión WAN en cada router.

A continuación, cada una de las líneas de comando aplicada para cada router, para cumplir con la necesidad planteada:

Medellin

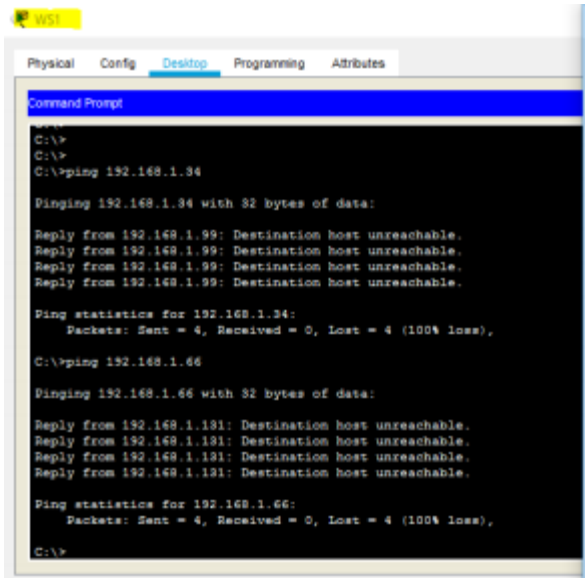
```
access-list 120 permit ip 192.168.1.3 0.0.0.0 any

access-list 120 deny ip any any

interfasce gi0/0

ip access-group 120 out
```

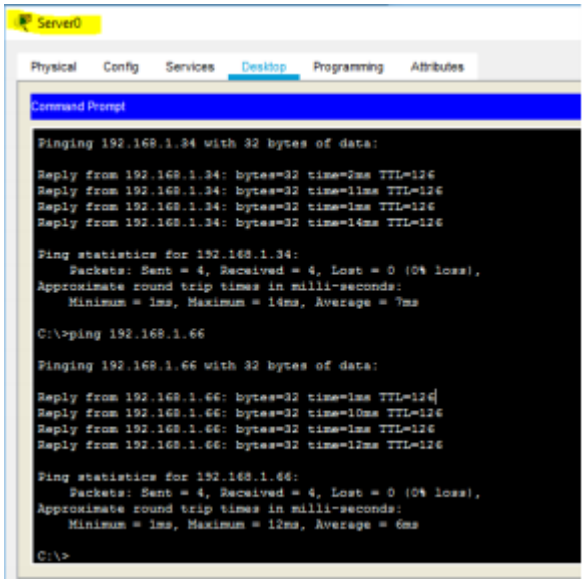
Cali

```
access-list 120 permit ip 192.168.1.3 0.0.0.0 any

access-list 120 deny ip any any

interface gi0/0

ip access-group 120 out
```

Parte 5: Comprobación de la red instalada.

a. Se debe probar que la configuración de las listas de acceso fue exitosa Se valida por medio de ping desde WS1



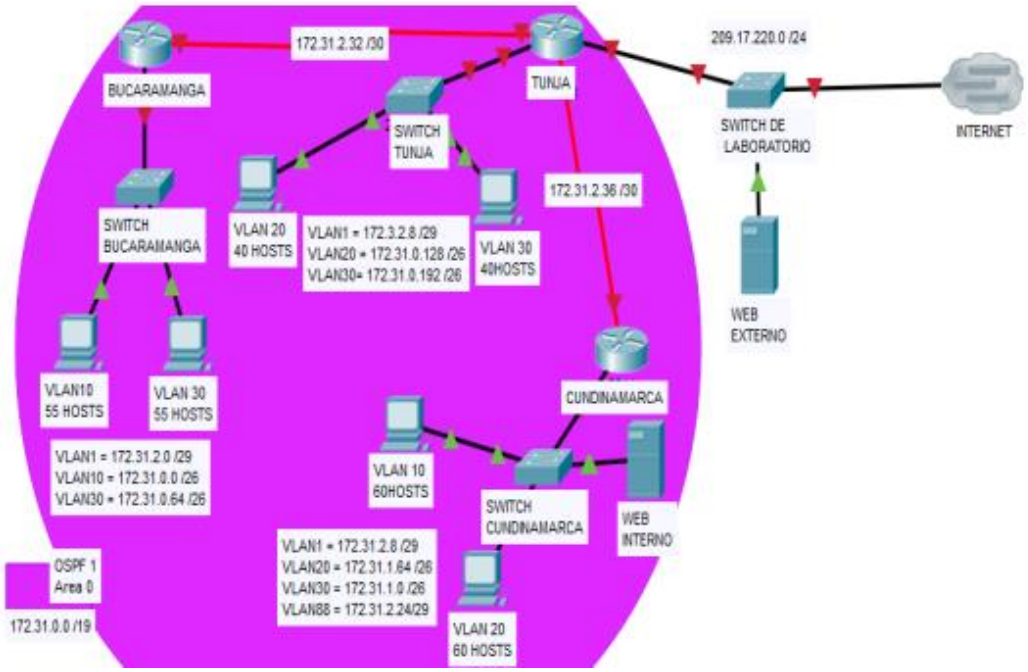


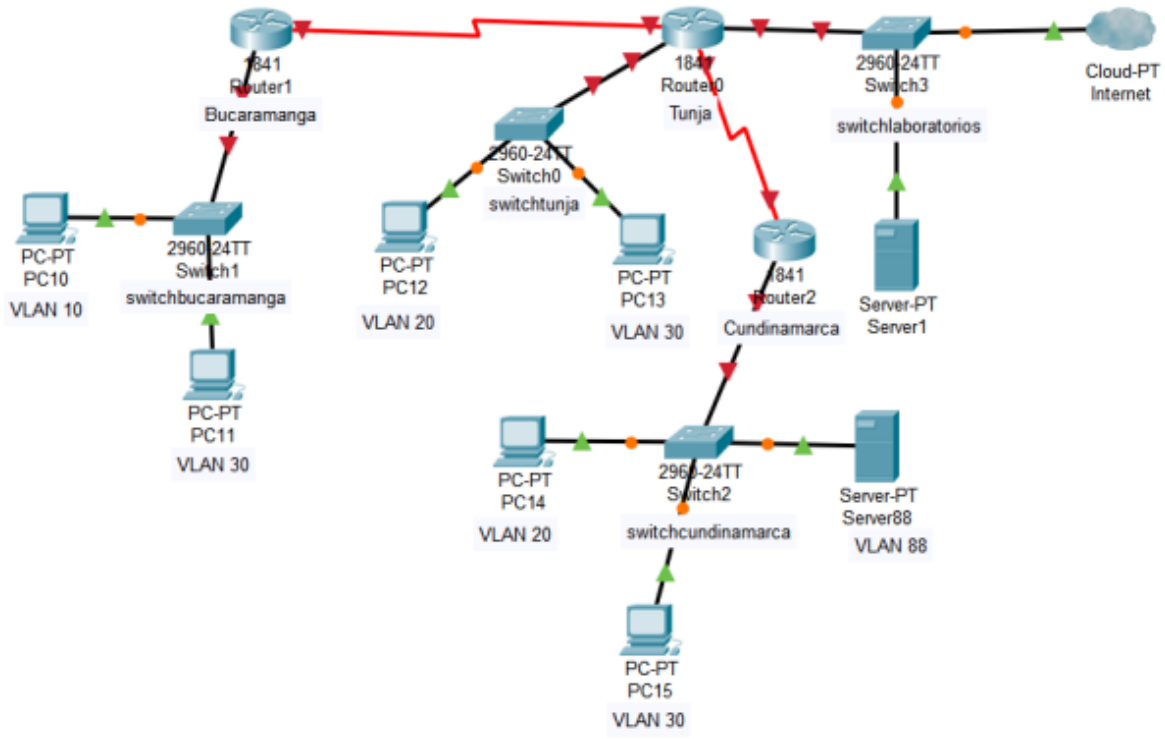
b. Comprobar y Completar la siguiente tabla de condiciones de prueba para confirmar el óptimo funcionamiento de la red e.

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

ESCENARIO 2

Escenario 2
Una empresa tiene la conexión a internet en una red Ethernet, lo cual deben adaptarlo para facilitar que sus routers y las redes que incluyen Puedan, por esa vía, conectarse a internet, pero empleando las direcciones de la red LAN original.





Desarrollo

Los siguientes son los requerimientos necesarios:

1. Todos los routers deberán tener los siguiente:

• Configuración básica.

- Procedo en esta parte a realizar la configuración de cada uno de los routers que hacen parte de nuestra red, nombres, contraseñas, mensajes, direcciones IP según tablas de direccionamiento, etc.

Router(config)#hostname bucaramanga
Bucaramanga(config)#no ip domain-lookup
Bucaramanga (config)#banner motd $El Acceso no autorizado est prohibido$
Bucaramanga bucaramanga(config)#line console 0
Bucaramanga (config-line)#password cisco123
Bucaramanga (config-line)#login
Bucaramanga (config-line)#line vty 0 15
Bucaramanga (config-line)#password cisco123
Bucaramanga (config-line)#login
Bucaramanga (config)#int f0/0.1
Bucaramanga (config-subif)#encapsulation dot1q 1
Bucaramanga (config-subif)#ip address 172.31.2.1 255.255.255.248

```
Bucaramanga (config-subif)#int f0/0.10
Bucaramanga (config-subif)#encapsulation dot1q 10
Bucaramanga (config-subif)#ip address 172.31.0.1 255.255.255.192
Bucaramanga (config-subif)#int f0/0.30
Bucaramanga (config-subif)#encapsulation dot1q 30
Bucaramanga (config-subif)#ip address 172.31.0.65 255.255.255.192
Bucaramanga (config-subif)#int f0/0
Bucaramanga (config-if)#no shutdown
Bucaramanga (config-if)#int s0/0/0
Bucaramanga (config-if)#ip address 172.31.2.34 255.255.255.252
Bucaramanga (config-if)#no shutdown
Bucaramanga (config-if)#router ospf 1
Bucaramanga (config-router)#network 172.31.0.0 0.0.0.63 area 0
Bucaramanga (config-router)#network 172.31.0.64 0.0.0.63 area 0
Bucaramanga (config-router)#network 172.31.2.0 0.0.0.7 area 0
Bucaramanga (config-router)#network 172.31.2.32 0.0.0.3 area 0
Bucaramanga (config-router)#end
Bucaramanga #
Router(config)#hostname tunja
tunja(config)#no ip domain-lookup
tunja(config)#banner motd $El Acceso no autorizado est prohibido$
tunja(config)#enable secret class123
tunja(config)#line console 0
tunja(config-line)#password cisco123
tunja(config-line)#login
tunja(config-line)#line vty 0 15
tunja(config-line)#password cisco123
tunja(config-line)#login
tunja(config)#int f0/0.1
tunja(config-subif)#encapsulation dot1q 1
tunja(config-subif)#ip address 172.3.2.9 255.255.255.248
tunja(config-subif)#int f0/0.20
tunja(config-subif)#encapsulation dot1q 20
tunja(config-subif)#ip address 172.31.0.129 255.255.255.192
tunja(config-subif)#int f0/0.30
tunja(config-subif)#encapsulation dot1q 30
tunja(config-subif)#ip address 172.31.0.193 255.255.255.192
tunja(config-subif)#int f0/0
tunja(config-if)#no shutdown
tunja(config-if)#int s0/0/0
tunja(config-if)#ip address 172.31.2.33 255.255.255.252
```

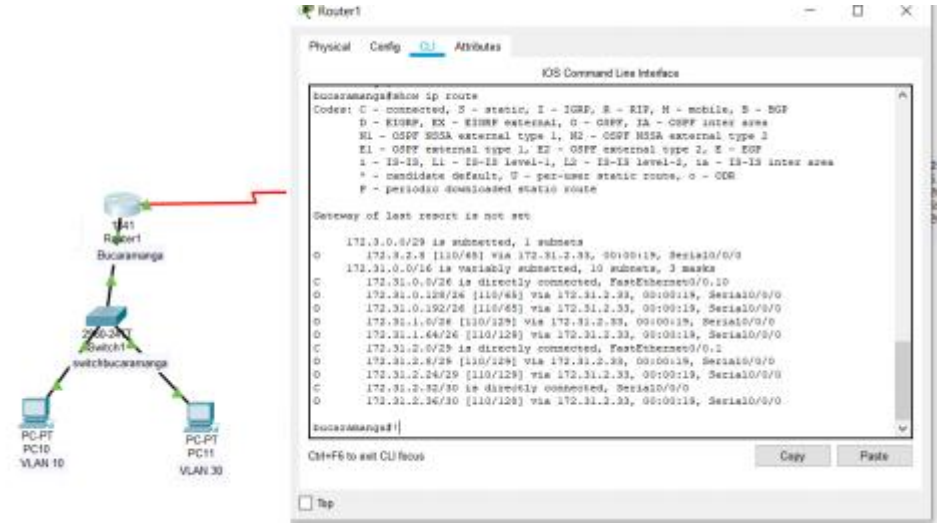
```
tunja(config-if)#no shutdown
tunja(config-if)#int s0/0/1
tunja(config-if)#ip address 172.31.2.37 255.255.255.252
tunja(config-if)#no shutdown
tunja(config-if)#int f0/1
tunja(config-if)#ip address 209.165.220.1 255.255.255.0
tunja(config-if)#no shutdown
tunja(config-if)#router ospf 1
tunja(config-router)#network 172.3.2.8 0.0.0.7 area 0
tunja(config-router)#network 172.31.0.128 0.0.0.63 area 0
tunja(config-router)#network 172.31.0.192 0.0.0.63 area 0
tunja(config-router)#network 172.31.2.32 0.0.0.3 area 0
tunja(config-router)#network 172.31.2.36 0.0.0.3 area 0
tunja(config-router)#end
tunja#
Router(config)#hostname CUNDINAMARCA
CUNDINAMARCA(config)#no ip domain-lookup
cundinamarca(config)#banner motd $El Acceso no autorizado est
prohibido$
CUNDINAMARCA (config)#enable secret class123
CUNDINAMARCA (config)#line console 0
CUNDINAMARCA (config-line)#password cisco123
CUNDINAMARCA (config-line)#login
CUNDINAMARCA (config-line)#line vty 0 15
CUNDINAMARCA (config-line)#password cisco123
CUNDINAMARCA (config-line)#login
CUNDINAMARCA (config)#int f0/0.1
CUNDINAMARCA (config-subif)#encapsulation dot1q 1
CUNDINAMARCA (config-subif)#ip address 172.31.2.9 255.255.255.248
CUNDINAMARCA (config-subif)#int f0/0.20
CUNDINAMARCA (config-subif)#encapsulation dot1q 20
CUNDINAMARCA (config-subif)#ip address 172.31.1.65 255.255.255.192
CUNDINAMARCA (config-subif)#int f0/0.30
CUNDINAMARCA (config-subif)#encapsulation dot1q 30
CUNDINAMARCA (config-subif)#ip address 172.31.1.1 255.255.255.192
CUNDINAMARCA (config-subif)#int f0/0.88
CUNDINAMARCA (config-subif)#encapsulation dot1q 88
CUNDINAMARCA (config-subif)#ip address 172.31.2.25 255.255.255.248
CUNDINAMARCA (config-subif)#int f0/0
CUNDINAMARCA (config-if)#no shutdown
CUNDINAMARCA (config-if)#
```

```
CUNDINAMARCA (config-if)#int s0/0/0
CUNDINAMARCA (config-if)#ip address 172.31.2.38 255.255.255.252
CUNDINAMARCA (config-if)#no shutdown
CUNDINAMARCA (config-if)#router ospf 1
CUNDINAMARCA (config-router)#network 172.31.1.0 0.0.0.63 area 0
CUNDINAMARCA (config-router)#network 172.31.1.64 0.0.0.63 area 0
CUNDINAMARCA (config-router)#network 172.31.2.8 0.0.0.7 area 0
CUNDINAMARCA (config-router)#network 172.31.2.24 0.0.0.7 area 0
CUNDINAMARCA (config-router)#network 172.31.2.36 0.0.0.3 area 0
CUNDINAMARCA (config-router)#end
```

Se realizan las configuraciones en cada switch validando, nombres, contraseñas direcciones IP¨todo esto según las tablas de direccionamiento.

```
Switch(config)#hostname Bucaramanga
Bucaramanga (config)#vlan 1
Bucaramanga (config-vlan)#vlan 10
Bucaramanga (config-vlan)#vlan 30
Bucaramanga (config-vlan)#int f0/10
Bucaramanga (config-if)#switchport mode access
Bucaramanga (config-if)#switchport access vlan 10
Bucaramanga (config-if)#int f0/14
Bucaramanga (config-if)#switchport mode access
Bucaramanga (config-if)#switchport access vlan 30
Bucaramanga (config-if)#int f0/1
Bucaramanga (config-if)#switchport mode trunk
Bucaramanga (config-if)#int vlan 1
- configuramos ahora las direcciones IP
Bucaramanga (config-if)#ip address 172.31.2.3 255.255.255.248
Bucaramanga (config-if)#no shutdown
Bucaramanga (config-if)#ip default-gateway 172.31.2.1
Bucaramanga (config)#
Switch(config)#hostname tunja
tunja (config)#vlan 1
tunja (config-vlan)#vlan 20
tunja (config-vlan)#vlan 30
tunja (config-vlan)#int f0/10
tunja (config-if)#switchport mode access
tunja (config-if)#switchport access vlan 20
tunja (config-if)#int f0/14
tunja (config-if)#switchport mode access
```

tunja (config-if)#switchport access vlan 30
tunja (config-if)#int f0/1
tunja (config-if)#switchport mode trunk
tunja (config-if)#
- configuramos ahora las direcciones IP
tunja (config-if)#int vlan 1
tunja swtichtunja(config-if)#no shutdown
tunja(config-if)#
tunja (config-if)#ip default-gateway 172.3.2.9
tunja (config)#
tunja (config)#
Switch(config)#hostname CUNDINAMARCA
CUNDINAMARCA (config)#vlan 1
CUNDINAMARCA (config-vlan)#vlan 20
CUNDINAMARCA (config-vlan)#vlan 30
CUNDINAMARCA (config-vlan)#vlan 88
CUNDINAMARCA (config-vlan)#exit
CUNDINAMARCA (config)#int f0/10
CUNDINAMARCA (config-if)#switchport mode access
CUNDINAMARCA (config-if)#switchport access vlan 20
CUNDINAMARCA (config-if)#int f0/14
CUNDINAMARCA (config-if)#switchport mode access
CUNDINAMARCA (config-if)#switchport access vlan 30
CUNDINAMARCA (config-if)#int f0/20
CUNDINAMARCA (config-if)#switchport mode access
CUNDINAMARCA (config-if)#switchport access vlan 88
CUNDINAMARCA (config-if)#int f0/1
CUNDINAMARCA (config-if)#switchport mode trunk
CUNDINAMARCA (config-if)#
- configuramos ahora las direcciones IP
CUNDINAMARCA (config-if)#int vlan 1
CUNDINAMARCA (config-if)#ip address 172.31.2.11 255.255.255.248
CUNDINAMARCA (config-if)#no shutdown
CUNDINAMARCA (config-if)#
CUNDINAMARCA (config-if)#ip default-gateway 172.31.2.9



Router0

Physical Config CLI Attributes

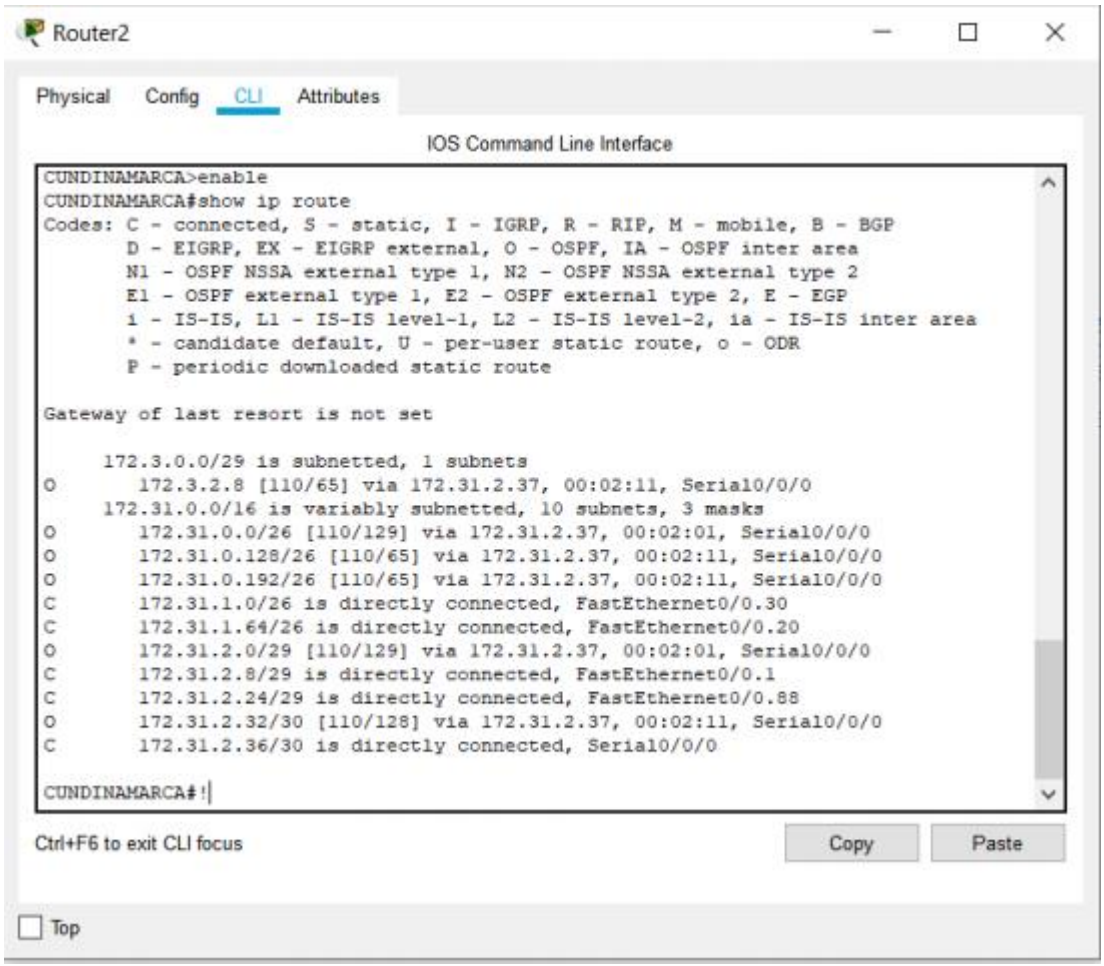
IOS Command Line Interface

```
tunja#show ip route
Codes: C - connected, S - static, I - IGRP, 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

     172.3.0.0/29 is subnetted, 1 subnets
C       172.3.2.8 is directly connected, FastEthernet0/0.1
     172.31.0.0/16 is variably subnetted, 10 subnets, 3 masks
O       172.31.0.0/26 [110/65] via 172.31.2.34, 00:01:36, Serial0/0/0
C       172.31.0.128/26 is directly connected, FastEthernet0/0.20
C       172.31.0.192/26 is directly connected, FastEthernet0/0.30
O       172.31.1.0/26 [110/65] via 172.31.2.38, 00:01:36, Serial0/0/1
O       172.31.1.64/26 [110/65] via 172.31.2.38, 00:01:36, Serial0/0/1
O       172.31.2.0/29 [110/65] via 172.31.2.34, 00:01:36, Serial0/0/0
O       172.31.2.8/29 [110/65] via 172.31.2.38, 00:01:36, Serial0/0/1
O       172.31.2.24/29 [110/65] via 172.31.2.38, 00:01:36, Serial0/0/1
C       172.31.2.32/30 is directly connected, Serial0/0/0
C       172.31.2.36/30 is directly connected, Serial0/0/1
C    209.165.220.0/24 is directly connected, FastEthernet0/1

tunja#!
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

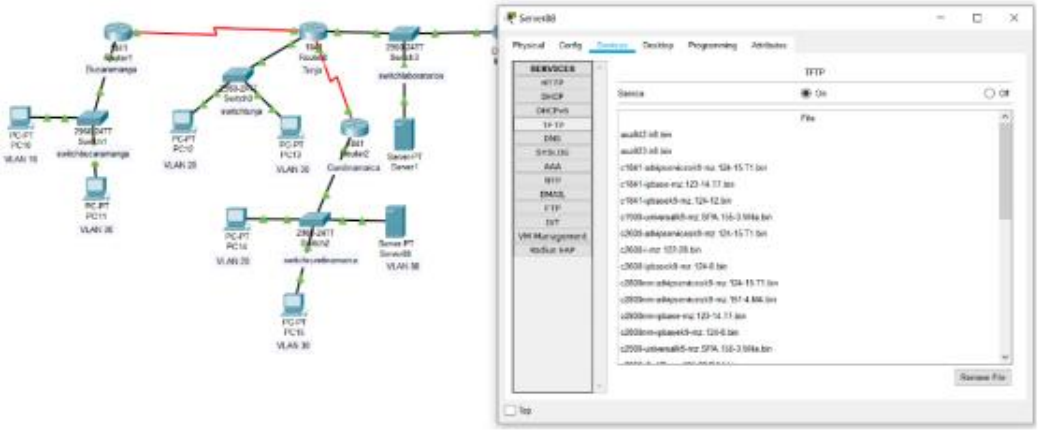


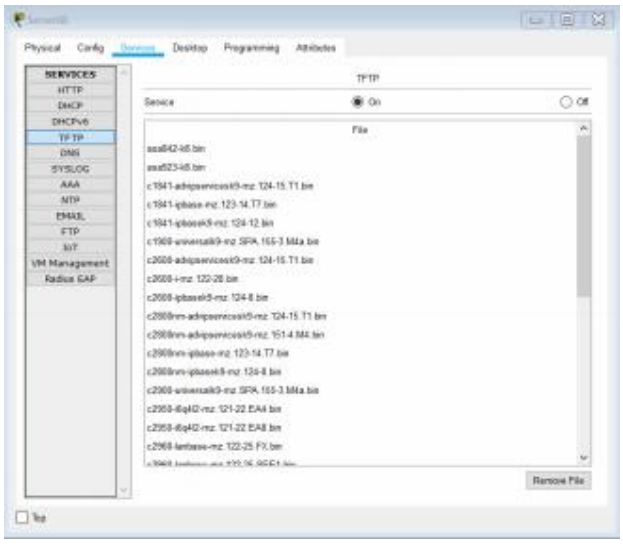
Autenticación local con AAA.

```
Bucaramanga(config-line)#username admin01 secret admin01pass
Bucaramanga(config)#aaa new-model
Bucaramanga(config)#aaa authentication login aaalocal local
Bucaramanga(config)#line console 0
Bucaramanga(config-line)#login authentication aaalocal
Bucaramanga(config-line)#line vty 0 15
Bucaramanga(config-line)#login authentication aaalocal
tunja(config-line)#username admin01 secret admin01pass
tunja(config)#aaa new-model
tunja(config)#aaa authentication login aaalocal local
tunja(config)#line console 0
tunja(config-line)#login authentication aaalocal
tunja(config-line)#line vty 0 15
tunja(config-line)#login authentication aaalocal
CUNDINAMARCA(config-line)#username admin01 secret admin01pass
```

CUNDINAMARCA (config)#aaa new-model
CUNDINAMARCA (config)#aaa authentication login aaalocal local
CUNDINAMARCA (config)#line console 0
CUNDINAMARCA (config-line)#login authentication aaalocal
CUNDINAMARCA (config-line)#line vty 0 15
CUNDINAMARCA (config-line)#login authentication aaalocal

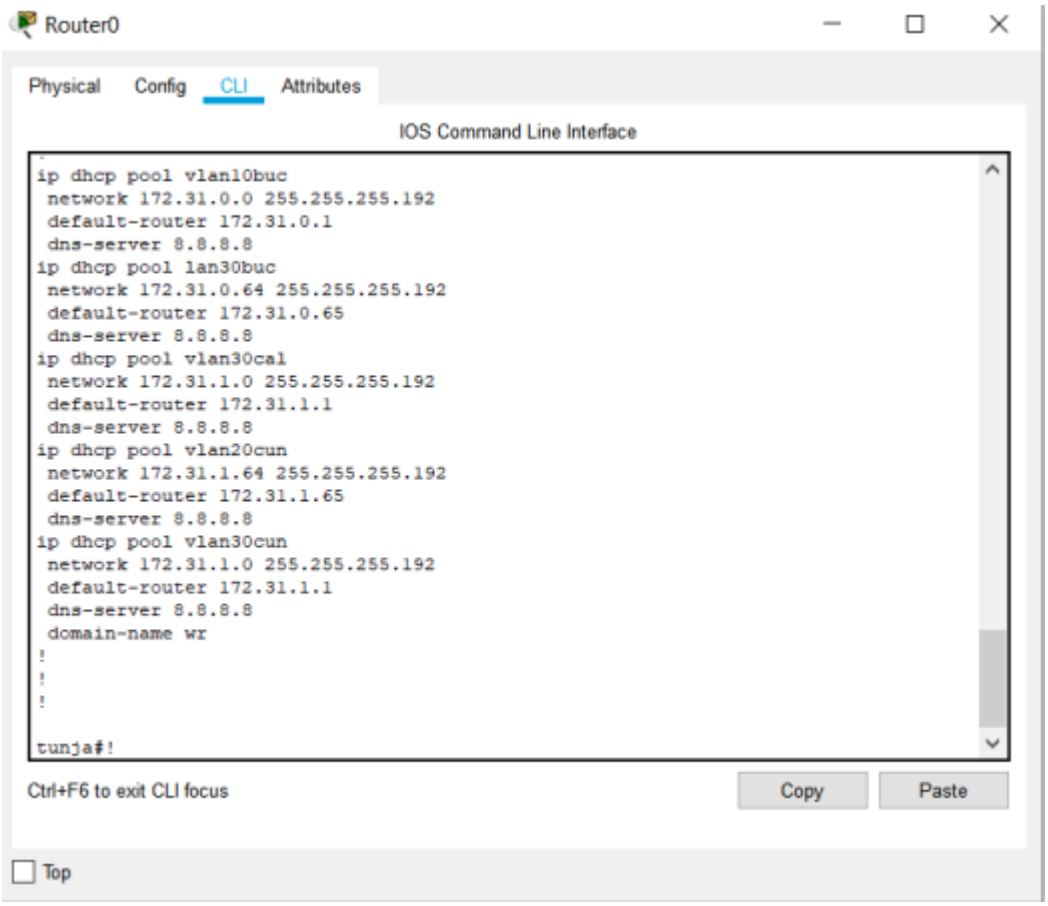
• Cifrado de contraseñas.
Bucaramanga(config)#service password-encryption
tunja(config)#service password-encryption
cundinamarca(config)#service password-encryption
• Un máximo de internos para acceder al router.
Bucaramanga(config-line)#login block-for 20 attempts 10 within 60
tunja(config-line)#login block-for 20 attempts 10 within 60
CUNDINAMARCA (config-line)#login block-for 20 attempts 10 within 60
• Máximo tiempo de acceso al detectar ataques.
Bucaramanga(config-line)#login block-for 20 attempts 10 within 60
tunja(config-line)#login block-for 20 attempts 10 within 60
CUNDINAMARCA (config-line)#login block-for 20 attempts 10 within 60





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

```
tunja(config)#ip dhcp excluded-address 172.31.0.1 172.31.0.3
tunja(config)#ip dhcp excluded-address 172.31.0.65 172.31.0.67
tunja(config)#ip dhcp excluded-address 172.31.1.65 172.31.1.67
tunja(config)#ip dhcp excluded-address 172.31.1.1 172.31.1.3
tunja(config)#ip dhcp pool vlan10buc
tunja(dhcp-config)#network 172.31.0.0 255.255.255.192
tunja(dhcp-config)#default-router 172.31.0.1
tunja(dhcp-config)#dns-server 8.8.8.8
tunja(dhcp-config)#ip dhcp pool lan30buc
tunja(dhcp-config)#network 172.31.0.64 255.255.255.192
tunja(dhcp-config)#default-router 172.31.0.65
tunja(dhcp-config)#dns-server 8.8.8.8
tunja(dhcp-config)#ip dhcp pool vlan20cun
tunja(dhcp-config)#network 172.31.1.64 255.255.255.192
tunja(dhcp-config)#default-router 172.31.1.65
tunja(dhcp-config)#dns-server 8.8.8.8
tunja(dhcp-config)#ip dhcp pool vlan30cun
tunja(dhcp-config)#network 172.31.1.0 255.255.255.192
tunja(dhcp-config)#default-router 172.31.1.1
tunja(dhcp-config)#dns-server 8.8.8.8
```



3. El web server deberá tener NAT estático y el resto de los equipos de la topología
emplearan NAT de sobrecarga (PAT).
Username: admin
Password:
tunja >en
Password:
tunja #conf t
tunja #conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
tunja (config)#ip nat inside sourse static?
% Unrecognized command
tunja (config)#ip nat inside sourse static 172.31.2.27?
% Unrecognized command
tunja (config)#ip nat inside source static 172.31.2.27 209.165.220.3

3. El enrutamiento deberá tener autenticación.
Bucaramanga(config)#int s0/0/0
Bucaramanga (config-if)#ip ospf authentication message-digest
Bucaramanga (config-if)#ip ospf message-digest-key 1 md5 cisco123
Bucaramanga #
04:55:49: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.220.1 on Serial0/0/0 from
LOADING to FULL, Loading Done
Bucaramanga #
CUNDINAMARCA(config)#int s0/0/0
CUNDINAMARCA(config-if)#ip ospf authentication message-digest
CUNDINAMARCA(config-if)#ip ospf message-digest-key 1 md5 cisco123
CUNDINAMARCA(config-if)#
04:57:08: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.220.1 on Serial0/0/0 from
FULL to DOWN, Neighbor Down: Dead timer expired
04:57:08: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.220.1 on Serial0/0/0 from
FULL to DOWN, Neighbor Down: Interface down or detached
CUNDINAMARCA(config-if)#
tunja (config)#int s0/0/0
tunja (config-if)#ip ospf authentication message-digest
tunja (config-if)#ip ospf message-digest-key 1 md5 cisco123
tunja (config-if)#
04:59:04: %OSPF-5-ADJCHG: Process 1, Nbr 172.31.2.34 on Serial0/0/0 from
LOADING to FULL, Loading Done
tunja (config-if)#
tunja (config-if)#int s0/0/1
tunja (config-if)#ip ospf authentication message-digest
tunja (config-if)#ip ospf message-digest-key 1 md5 cisco123
tunja (config-if)#
05:00:48: %OSPF-5-ADJCHG: Process 1, Nbr 172.31.2.38 on Serial0/0/1 from
LOADING to FULL, Loading Done
TUNJA(config-if)#
Comprobación de conectividad entre terminales
C:\>ping 172.31.0.67
Pinging 172.31.0.67 with 32 bytes of data:

Reply from 172.31.0.67: bytes=32 time=12ms TTL=127
Reply from 172.31.0.67: bytes=32 time<1ms TTL=127
Reply from 172.31.0.67: bytes=32 time<1ms TTL=127
Reply from 172.31.0.67: bytes=32 time<1ms TTL=127
Ping statistics for 172.31.0.67:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 12ms, Average = 3ms
C:\>ping 172.31.0.135
Pinging 172.31.0.135 with 32 bytes of data:
Request timed out.
Reply from 172.31.0.135: bytes=32 time=15ms TTL=126
Reply from 172.31.0.135: bytes=32 time=14ms TTL=126
Reply from 172.31.0.135: bytes=32 time=14ms TTL=126
Ping statistics for 172.31.0.135:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 14ms, Maximum = 15ms, Average = 14ms
C:\>ping 172.31.0.196
Pinging 172.31.0.196 with 32 bytes of data:
Request timed out.
Reply from 172.31.0.196: bytes=32 time=14ms TTL=126
Reply from 172.31.0.196: bytes=32 time=12ms TTL=126
Reply from 172.31.0.196: bytes=32 time=14ms TTL=126
Ping statistics for 172.31.0.196:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 12ms, Maximum = 14ms, Average = 13ms

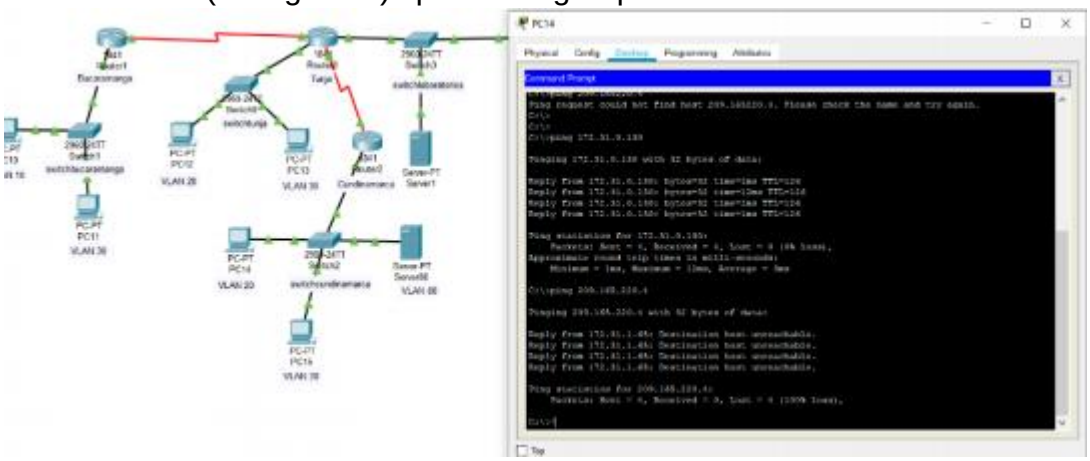
4. El enrutamiento deberá tener autenticación.
Bucaramanga#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Bucaramanga (config)#int s0/0/0
Bucaramanga (config-if)#ip ospf authentication message-digest
Bucaramanga (config-if)#ip ospf message-digest-key 1 md5 ospfpass
Bucaramanga (config-if)#
tunja(config)#int s0/0/0
tunja(config-if)#ip ospf authentication message-digest
tunja(config-if)#ip ospf message-digest-key 1 md5 ospfpass
tunja(config-if)#int s0/0/1
tunja(config-if)#ip ospf authentication message-digest

tunja(config-if)#ip ospf message-digest-key 1 md5 ospfpass
tunja(config-if)#
CUNDINAMARCA(config)#int s0/0/0
CUNDINAMARCA (config-if)#ip ospf authentication message-digest
CUNDINAMARCA (config-if)#ip ospf message-digest-key 1 md5 ospfpass

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

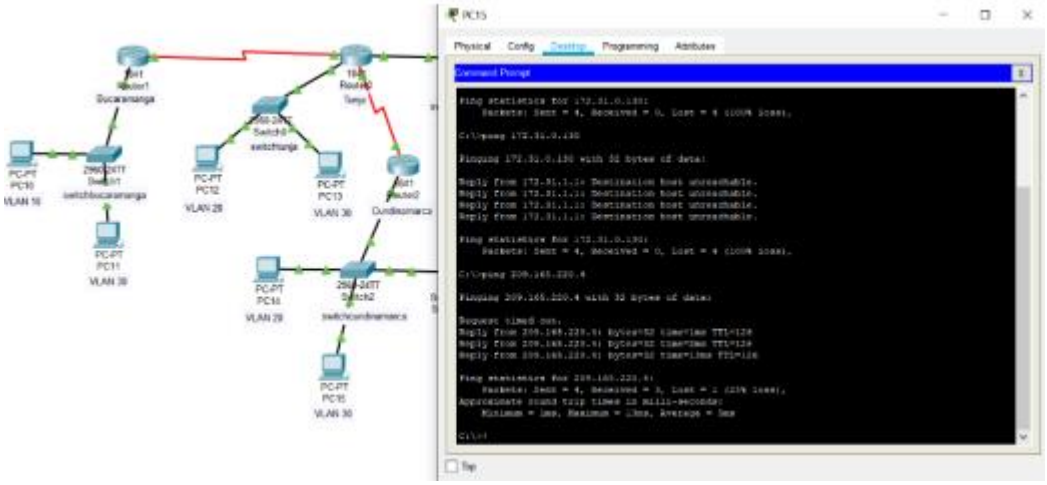
Los hosts de VLAN 20 en Cundinamarca no acceden a internet, solo a la red interna de Tunja.

cundinamarca(config-if)#access-list 121 deny ip 172.31.1.64 0.0.0.63 209.165.220.0 0.0.0.255
cundinamarca(config)#access-list 121 permit ip any any
cundinamarca(config)#int f0/0.20
cundinamarca(config-subif)#ip access-group 121 in



Los hosts de VLAN 10 en Cundinamarca si acceden a internet y no a la red interna de Tunja.

cundinamarca(config-subif)#access-list 122 permit ip 172.31.1.0 0.0.0.63 209.165.220.0 0.0.0.255
cundinamarca(config)#access-list 122 deny ip any any
cundinamarca(config)#int f0/0.30
cundinamarca(config-subif)#ip access-group 122 in



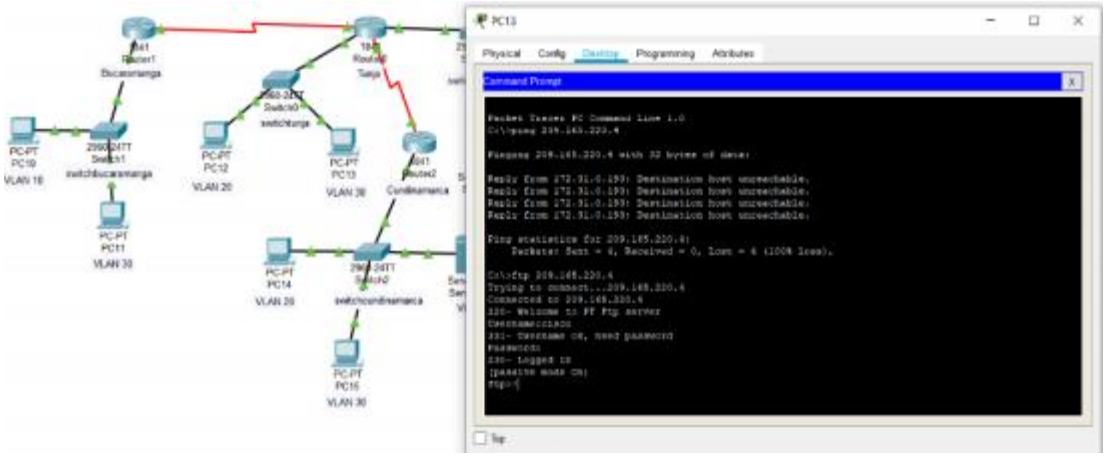
Los hosts de VLAN 30 en Tunja solo acceden a servidores web y ftp de internet.

tunja(config)#access-list 121 permit tcp 172.31.0.192 0.0.0.63 209.165.220.0.0.0.0.255 eq www

tunja(config)#access-list 121 permit tcp 172.31.0.192 0.0.0.63 209.165.220.00.0.0.255 eq ftp

tunja(config)#int f0/0.30

tunja(config-subif)#ip access-group 121 in



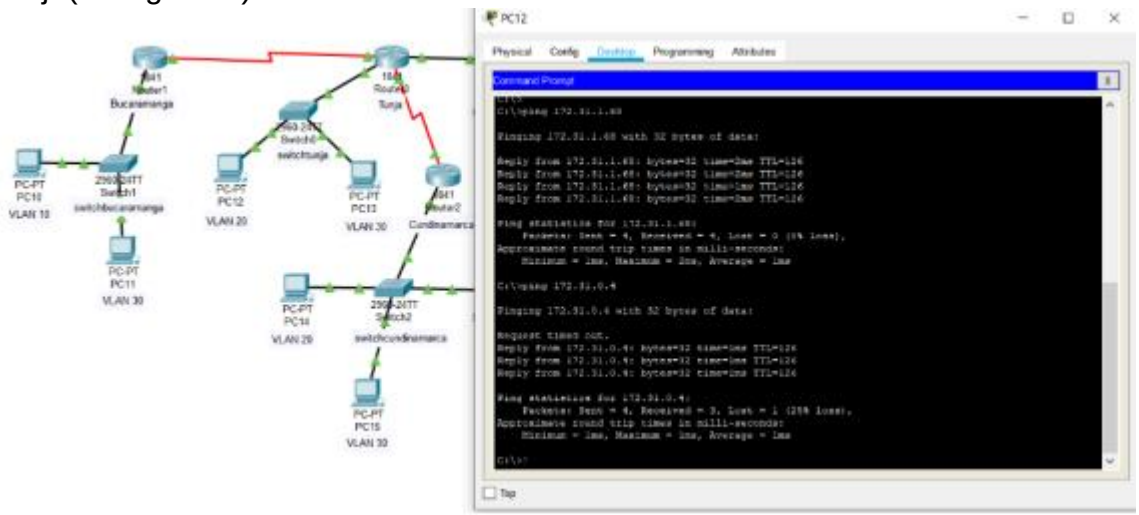
Los hosts de VLAN 20 en Tunja solo acceden a la VLAN 20 de Cundinamarca y VLAN 10 de Bucaramanga.

tunja(config-subif)#access-list 122 permit ip 172.31.0.128 0.0.0.63 172.31.1.64
0.0.0.63

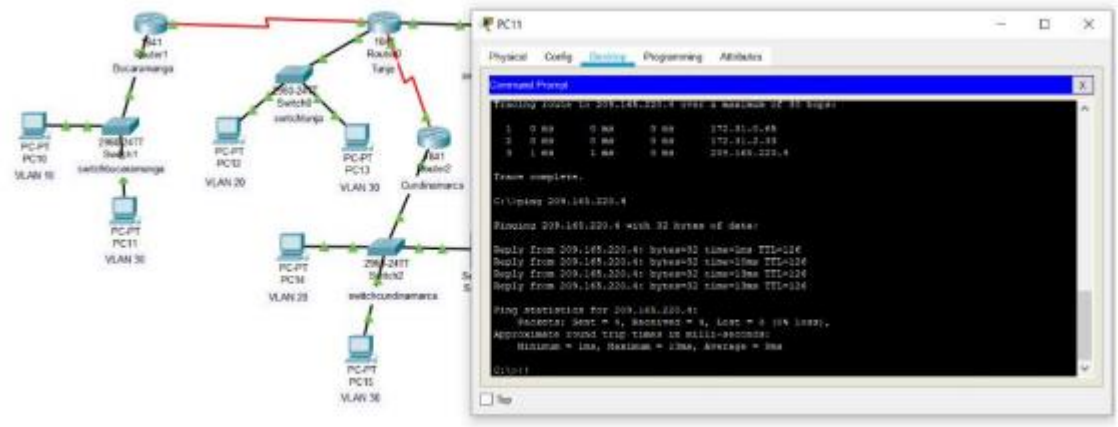
tunja(config)#access-list 122 permit ip 172.31.0.128 0.0.0.63 172.31.0.0 0.0.0.63

tunja(config)#int f0/0.20

tunja(config-subif)#ip access-group 122 in
tunja(config-subif)#

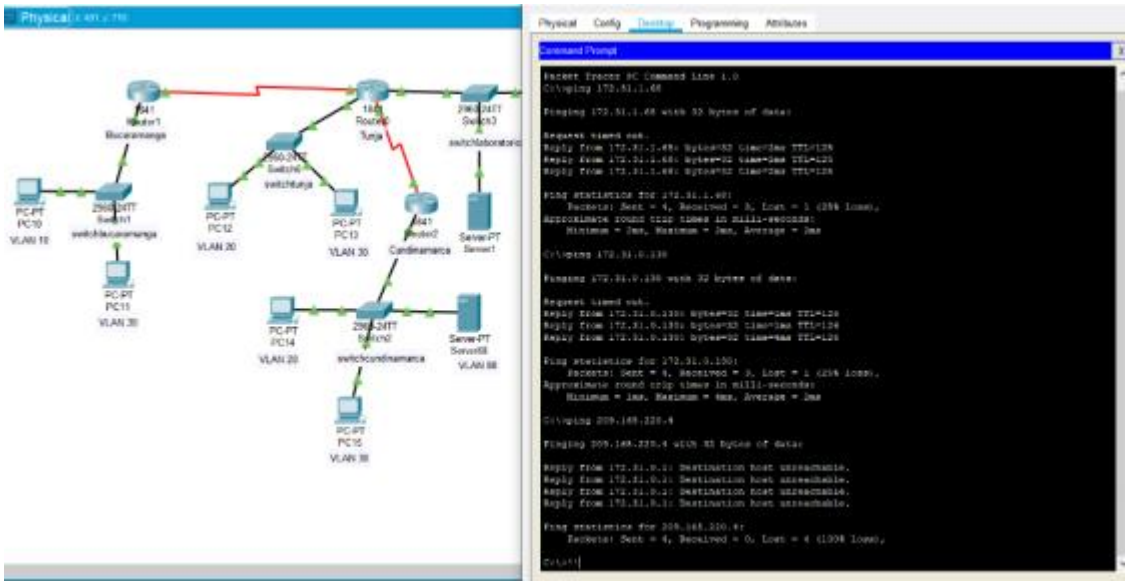


Los hosts de VLAN 30 de Bucaramanga acceden a internet y a cualquier equipo de VLAN 10.
bucaramanga(config)#access-list 121 permit ip 172.31.0.64 0.0.0.63 209.165.220.0 0.0.0.255
bucaramanga(config)#int f0/0.30
bucaramanga(config-subif)#ip access-group 121 in



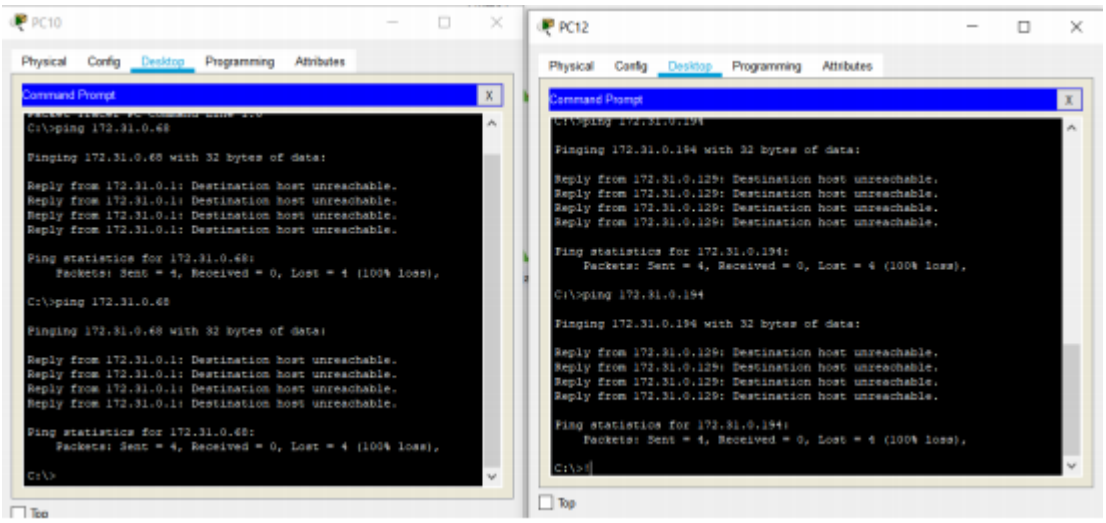
Los hosts de VLAN 10 en Bucaramanga acceden a la red de Cundinamarca (VLAN 20) y Tunja (VLAN 20), no internet.
bucaramanga(config-subif)#access-list 122 permit ip 172.31.0.0 0.0.0.63 172.31.1.64 0.0.0.63
bucaramanga(config)#access-list 122 permit ip 172.31.0.0 0.0.0.63 172.31.0.128 0.0.0.63
bucaramanga(config)#int f0/0.10

bucaramanga(config-subif)#ip access-group 122 in



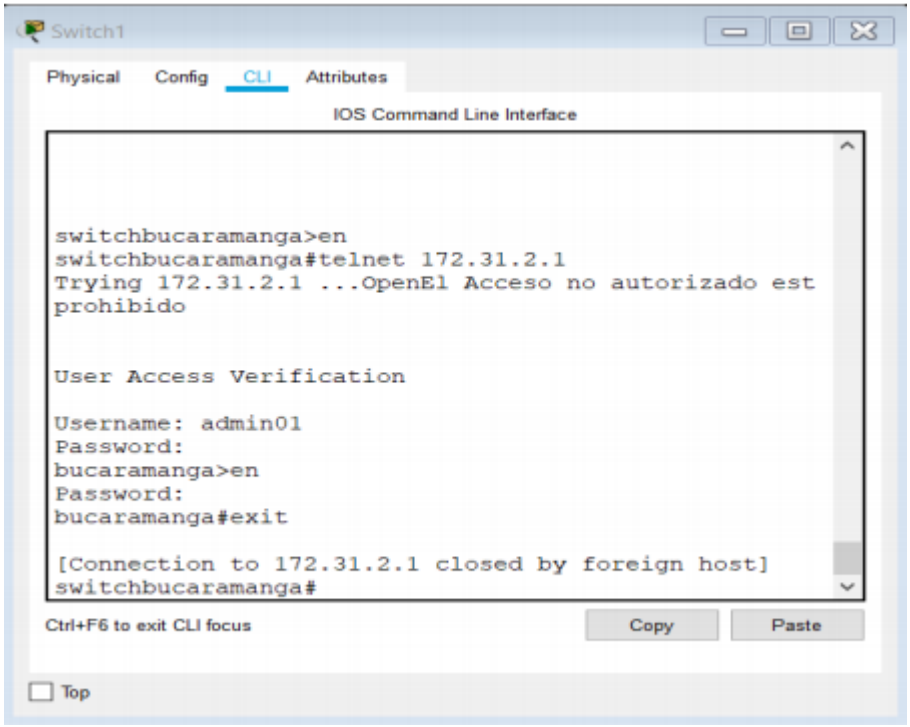
Los hosts de una VLAN no pueden acceder a los de otra VLAN en una ciudad.
bucaramanga(config-subif)#access-list 123 deny ip 172.31.2.0 0.0.0.7 172.31.0.0 0.0.0.63
bucaramanga(config)#access-list 123 deny ip 172.31.0.64 0.0.0.63 172.31.0.0
0.0.0.63
bucaramanga(config)#access-list 123 permit ip any any
bucaramanga(config)#int f0/0.10
bucaramanga(config-subif)#ip access-group 123 out
bucaramanga(config-subif)#
tunja(config)#access-list 123 deny ip 172.3.2.8 0.0.0.7 172.31.0.128 0.0.0.63
tunja(config)#access-list 123 deny ip 172.3.0.192 0.0.0.63 172.31.0.128 0.0.0.63
tunja(config)#access-list 123 permit ip any any
tunja(config)#int f0/0.20
tunja(config-subif)#ip access-group 123 out
tunja(config-subif)#
cundinamarca(config)#access-list 123 deny ip 172.31.2.8 0.0.0.7 172.31.1.64

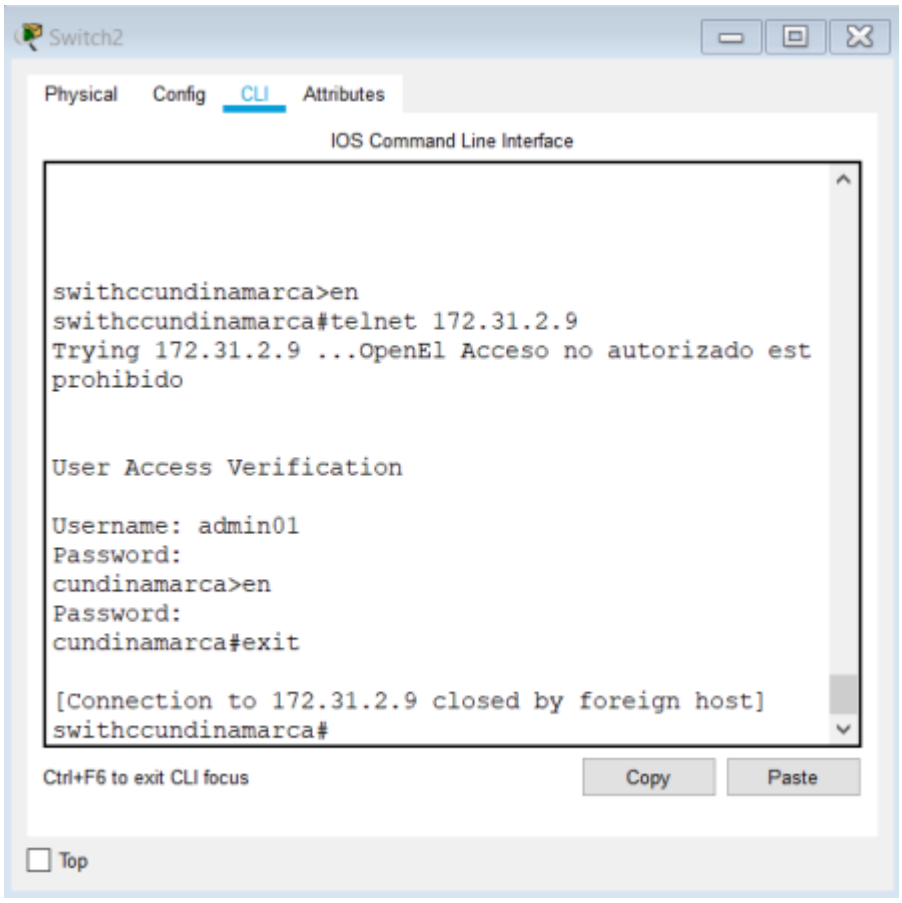
0.0.0.63
cundinamarca(config)#access-list 123 deny ip 172.31.1.0 0.0.0.63
172.31.1.64
0.0.0.63
cundinamarca(config)#access-list 123 deny ip 172.31.2.24 0.0.0.7
172.31.1.64
0.0.0.63
cundinamarca(config)#access-list 123 permit ip any any
cundinamarca(config)#int f0/0.20
cundinamarca(config-subif)#ip access-group 123 out



Solo los hosts de las VLAN administrativas y de la VLAN de servidores tienen accedo a los routers e internet.
bucaramanga(config-subif)#access-list 10 permit 172.31.2.0 0.0.0.7
bucaramanga(config)#access-list 10 permit 172.3.2.8 0.0.0.7
bucaramanga(config)#access-list 10 permit 172.31.2.8 0.0.0.7
bucaramanga(config)#line vty 0 15
bucaramanga(config-line)#access-class 10 in
bucaramanga(config-line)#
tunja(config-subif)#access-list 10 permit 172.31.2.0 0.0.0.7
tunja(config)#access-list 10 permit 172.3.2.8 0.0.0.7
tunja(config)#access-list 10 permit 172.31.2.8 0.0.0.7
tunja(config)#line vty 0 15
tunja(config-line)#access-class 10 in
tunja(config-line)#
cundinamarca(config-subif)#access-list 10 permit 172.31.2.0 0.0.0.7
cundinamarca(config)#access-list 10 permit 172.3.2.8 0.0.0.7

cundinamarca(config)#access-list 10 permit 172.31.2.8 0.0.0.7
cundinamarca(config)#line vty 0 15
cundinamarca(config-line)#access-class 10 in




Switch2
Physical
Config
CLI
Attributes
IOS Command Line Interface
switchccundinamarca>en
switchccundinamarca#telnet 172.31.2.9
Trying 172.31.2.9 ...OpenEl Acceso no autorizado est
prohibido
User Access Verification
Username: admin01
Password:
cundinamarca>en
Password:
cundinamarca#exit
[Connection to 172.31.2.9 closed by foreign host]
switchccundinamarca#
Ctrl+F6 to exit CLI focus
Copy
Paste
Top

CONCLUSIONES

Las listas de acceso estándar permiten la restricción de redes o host, pero son genéricas, cabe anotar que son más simples en situaciones que no ameriten una restricción estricta, en el escenario uno, se implementa una lista de acceso simple para permitir el acceso por protocolo remoto telnet.
Las listas de acceso extendidas, son más complejas, pero requieren una habilidad en el manejo de protocolos y puertos, ya que principalmente se estructuran bajo dichas métricas, de igual manera estas permiten diseñar redes y subredes más seguras, la correcta implementación de las misma optimiza el tráfico de la red, ya que no todos los hosts de una red requieren los mismos servicios, ni se le pueden conceder a todos, acceso libre.

Después del anterior orden de ideas se puede verificar que los conocimientos adquiridos en este diplomados nos sirven como una base para desenvolvernos en el mundo de las redes futuramente como profesionales de la materia

REFERENCIAS BIBLIOGRAFICAS

CISCO. (2014). VLANs. Principios de Enrutamiento y Conmutación. Disponible en: https://static-courseassets.s3.amazonaws.com/RSE50ES/module3/index.html#3.0.1.1

CISCO. (2014). OSPF de una sola área. Principios de Enrutamiento y Conmutación. Recuperado de https://static-courseassets.s3.amazonaws.com/RSE50ES/module8/index.html#8.0.1.1

CISCO. (2014). DHCP. Principios de Enrutamiento y Conmutación. Recuperado de https://static-courseassets.s3.amazonaws.com/RSE50ES/module10/index.html#10.0.1.1

Academia Cisco. (2019). Retrieved 12 December 2019, from https://www.netacad.com/portal/learning