DIPLOMADO DE PROFUNDIZACIÓN CISCO LAN / WAN
PRUEBA DE HABILIDADES PRACTICAS

HEIMER JOSE JARABA CAMARGO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA
INGENIERIA ELECTRONICA
SANTA MARTA
2020

DIPLOMADO DE PROFUNDIZACIÓN CISCO LAN / WAN
PRUEBA DE HABILIDADES PRACTICAS

HEIMER JOSE JARABA CAMARGO

Diplomado de opción de grado
presentado para optar el título de
INGENIERO ELECTRONICO

DIRECTOR:
MSc. JUAN CARLOS VESGA FERREIRA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA
INGENIERIA ELECTRONICA
SANTA MARTA
2020

NOTA DE ACEPTACIÓN

Presidente del Jurado

Jurado

Jurado

Santa Marta, 26 de enero de 2020

DEDICATORIA

Esta es una etapa en la cual me siento agradecido con Dios por darme la fortaleza diaria para poder finalizar unos de mis sueños la de terminar mi carrera la de ser un profesional integro, agradecido con mis padres que colocaron sus esfuerzos encaminándome al estudio y persistencia.

Dedico este logro académico a mi esposa y mis hijas las cuales sacrificaron tiempo y espacio para apoyarme día a día, alentándome a seguir adelante, ya que muchas veces me sentí agotado a los tutores de la UNAD que estuvieron siempre con la disponibilidad y dedicación a cada etapa de formación.

TABLA DE CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

Smart Lab: es un centro especializado en difusión de conocimiento, intercambio de experiencias y espacios compartidos de trabajo vinculado a las ciudades inteligentes. El objetivo es crear un entorno compartido que estimule el intercambio de ideas y la generación de proyectos innovadores.

OSPFv2: es la versión del protocolo OSPF que actualmente utilizamos en redes IPv4. En este caso, el formato del router ID coincide con el formato de las direcciones IP utilizadas en las interfaces por lo que es posible utilizar la dirección IP de una interfaz como router ID, de manera tal que no es obligatorio configurar un router-id y el sistema operativo puede tomar la dirección IP de una interfaz para ser utilizada en esta función.

VLAN: es un método para crear redes lógicas independientes dentro de una misma red física.1 Varias VLAN pueden coexistir en un único conmutador físico o en una única red física.

DHCP: es un servidor que usa protocolo de red de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme éstas van quedando libres, sabiendo en todo momento quién ha estado en posesión de esa IP, cuánto tiempo la ha tenido y a quién se la ha asignado después.

EIGRP: protocolo de Enrutamiento de Puerta de enlace Interior Mejorado, es un protocolo de encaminamiento de vector distancia, propiedad de Cisco Systems, que ofrece lo mejor de los algoritmos de vector de distancia. Se considera un protocolo avanzado que se basa en las características normalmente asociadas con los protocolos del estado de enlace.

RESUMEN

La finalidad de desarrollo de este trabajo fue la implementación de los conocimientos y habilidades aprendidas durante el curso de cisco. En el cual implementamos diferentes estudios para generar la conectividad entre varias ciudades.

Para el logro de este objetivo o problemática planteada al inicio se desarrolló un archivo de simulación en el programa CISCO Packet Tracer. El cual nos permite realizar cada una de las configuraciones solicitadas y posteriormente cumplir con el objetivo. El propósito de ello se basó principalmente en interconectar tres ciudades donde se localizan sucursales de una empresa y de esta manera tener una comunicación directa acorde con los lineamientos establecidos para el direccionamiento IP, protocolos de enrutamiento y demás aspectos que forman parte de la topología de red.

Palabras Clave: Electrónica, Redes, Telecomunicaciones, CISCO

ABSTRACT

The purpose of this work was the implementation of the knowledge and skills learned during the course of Cisco. In which we implement different studies to generate connectivity between several cities.

To achieve this objective or problem raised at the beginning, a simulation file was developed in the CISCO Packet Tracer program. Which allows us to make each of the requested configurations and subsequently meet the objective. The purpose of this was mainly based on interconnecting three cities where branches of a company are located and thus having direct communication in accordance with the guidelines established for IP addressing, routing protocols and other aspects that are part of the network topology.

Keywords: Electronics, Networking, Telecommunications, CISCO.

INTRODUCCIÓN

La tecnología ha influido hoy en día en cada una de las carreras o actividades del ser humano. Entre tastas novedades, el internet se ha convertido en el medio de comunicación más grande del mundo y el más importante. En la actualidad cada una de las actividades o tareas del ser humano están sujetas a la implementación de la tecnología o de la red más grande de información como el internet.

Esta herramienta ha cambiado el mundo, su avance ha revolucionado nuestra vida diaria, transformando la forma de comunicación en segundos puedes realizar mensajerías de texto, transmitir videos e imágenes, realizar una videoconferencia y hasta realizar compras y ventas de servicio; ni la invención del telégrafo, el teléfono o la radio lograron con el pasar de los años lo que sí generó la red, el internet ha generado un conjunto de connotaciones nuevas, que crean oportunidades para las comunidades de todo el mundo.

Ciscó Networking Academy es una herramienta o sistema que ayuda a mejorar la demanda al ofrecer formas de aprendizaje innovadoras y prácticas para preparar a los profesionales dispuestos a triunfar en todos campos relacionados directamente con las TIC.

Las prácticas de las pruebas de habilidades son una herramienta de evaluación del Diplomado de Profundización CISCO LAN / WAN, con la cual se busca medir las habilidades y competencias que el estudiante logró alcanzar mediante el desarrollo del diplomado y cada una de sus actividades. Esta evaluación pondrá a prueba al estudiante mediante la solución de problemas relacionados con redes.

Esta actividad final contará con dos escenarios en la cual cada estudiante realizará cada una de las configuraciones necesarias para solventar el problema propuesto, anexando cada una de las evidencias que muestran la solución del problema.

Los conocimientos adquiridos en el desarrollo de este diplomado son fundamentales en la aplicación del aprendizaje obtenido en la carrera como Ingeniero Electrónico, teniendo en cuenta que el sistema CISCO, tiene a nivel internacional una utilización generalizada, gracias a que sus redes poseen grandes índices de capacidad y seguridad, situación que permite enfrentarse con este tipo sistemas en el ámbito laboral.

Escenarios propuestos para la Prueba de Habilidades

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.

Figura 1. Topología Escenario 1

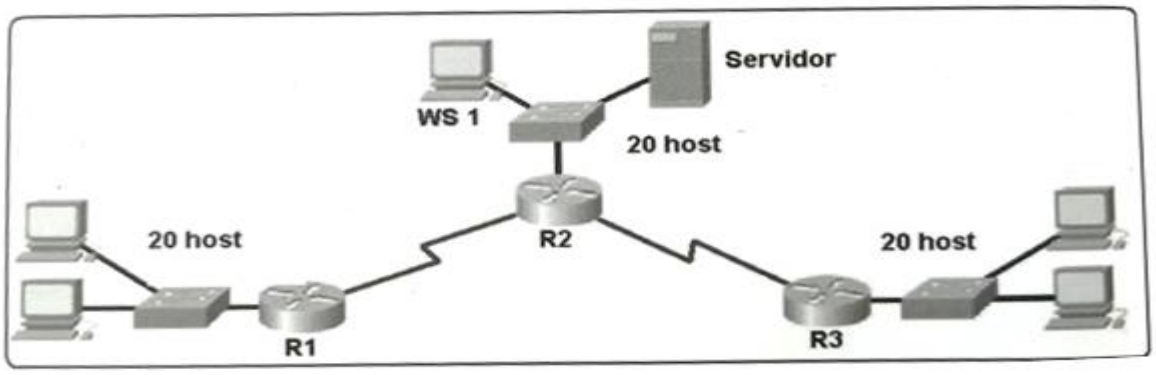
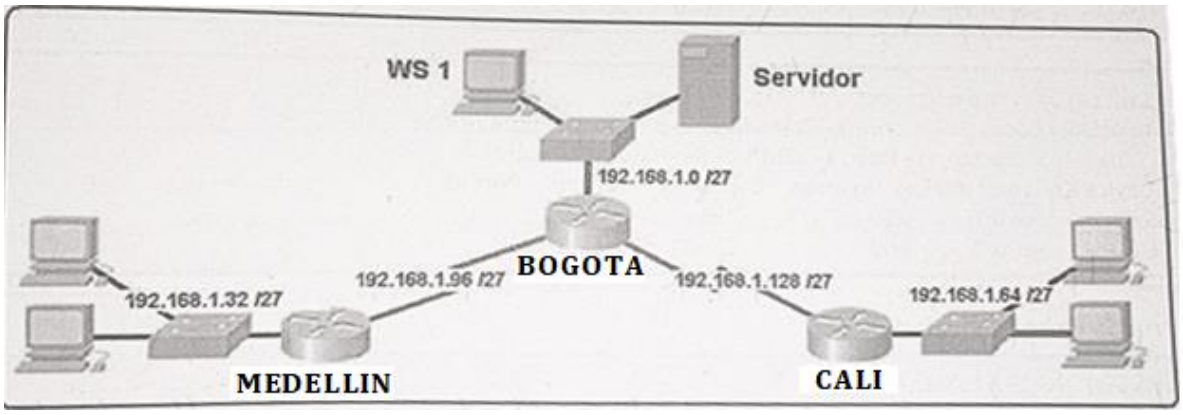


Figura 2. Topología Escenario 1 # 2



Desarrollo de la actividad en el escenario 1

Para el desarrollo del problema se debe comenzar con la configuración de cada router asignándole nombre y los niveles de seguridad.

Código fuente de la configuración de los Routers

Configuración Router sede Medellín

```
Router 2>en
Router 2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Medellin(config)#hostname Medellin
Medelin(config)#no ip domain-lookup
Medelin(config)#service password-encryption
Medelin(config)#banner motd $El Acceso no autorizado est prohibido$
Medelin(config)#enable secret class1
Medelin(config)#line console 0
Medelin(config-line)#password cisco1
Medelin(config-line)#login
Medelin(config-line)#line vty 0 15
Medelin(config-line)#password cisco1
Medelin(config-line)#login
Medelin(config-line)#
```

Configuración Router sede Bogotá

```
Router 1>en
Router 1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname Bogota
```

```
Bogota(config)#no ip domain-lookup
Bogota(config)#service password-encryption
Bogota(config)#banner motd $El Acceso no autorizado est prohibido$
Bogota(config)#enable secret class1
Bogota(config)#line console 0
Bogota(config-line)#password cisco1
Bogota(config-line)#login
Bogota(config-line)#line vty 0 15
Bogota(config-line)#password cisco1
Bogota(config-line)#login
Bogota(config-line)#
```

Configuración Router sede Cali

```
Router 3>en
Router 3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Cali(config)#hostname cali
Cali(config)#no ip domain-lookup
Cali(config)#service password-encryption
Cali(config)#banner motd $El Acceso no autorizado est prohibido$
Cali(config)#enable secret class1
Cali(config)#line console 0
Cali(config-line)#password cisco1
Cali(config-line)#login
Cali(config-line)#line vty 0 15
Cali(config-line)#password cisco1
Cali(config-line)#login
Cali(config-line)#
```

Se procede a realizar la configuración de los Switch asignándoles nombre y los niveles de seguridad.

Configuración Switch sede Medellín

```
Switch0>en
Switch0#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch0 (config)#hostname switchMedellin
switchMedellin(config)#no ip domain-lookup
switchMedellin(config)#service password-encryption
switchMedellin(config)#banner motd $El Acceso no autorizado est prohibido$
switchMedellin(config)#enable secret class1
switchMedellin(config)#line console 0
```

```
switchMedellin(config-line)#password cisco1
switchMedellin(config-line)#login
switchMedellin(config-line)#line vty 0 15
switchMedellin(config-line)#password cisco1
switchMedellin(config-line)#login
```

Configuración Switch sede Bogotá

```
Switch5>en
Switch5#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch5 (config)#hostname switchBogota
switchBogota(config)#no ip domain-lookup
switchBogota(config)#service password-encryption
switchBogota(config)#banner motd $El Acceso no autorizado est prohibido$
switchBogota(config)#enable secret class1
switchBogota(config)#line console 0
switchBogota(config-line)#password cisco1
switchBogota(config-line)#login
switchBogota(config-line)#line vty 0 15
switchBogota(config-line)#password cisco1
switchBogota(config-line)#login
switchBogota(config-line)#
```

Configuración Switch sede Cali

```
Switch6>en
Switch6#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch6 (config)#hostname switchcali
switchCali(config)#no ip domain-lookup
switchCali(config)#service password-encryption
switchCali(config)#banner motd $El Acceso no autorizado est prohibido$
switchCali(config)#enable secret class1
switchCali(config)#line console 0
switchCali(config-line)#password cisco1
switchCali(config-line)#login
switchCali(config-line)#line vty 0 15
switchCali(config-line)#password cisco1
switchCali(config-line)#login
switchCali(config-line)#
```

- 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.

b. Asignar una dirección IP a la red.

Para este paso de la asignación de la IP se debe realizar una división tomando la red física existente y fragmentándola en ocho partes lógicas las cuales enviaran paquetes de datos y mensajes de forma individuales. Estas divisiones se realizan en el último octeto de la dirección IP física llevando la paridad de 32 bits.

Tabla 1. Direcciones IP para asignación

Bogota-LAN	192.168.1.0/27
Medellín-LAN	192.168.1.32/27
Cali-LAN	192.168.1.64/27
Bogota-Medellín	192.168.1.96/27
Bogota-Cali	192.168.1.128/27
Disponible	192.168.1.160/27
Disponible	192.168.1.192/27
Disponible	192.168.1.224/27

Parte 2: Configuración Básica

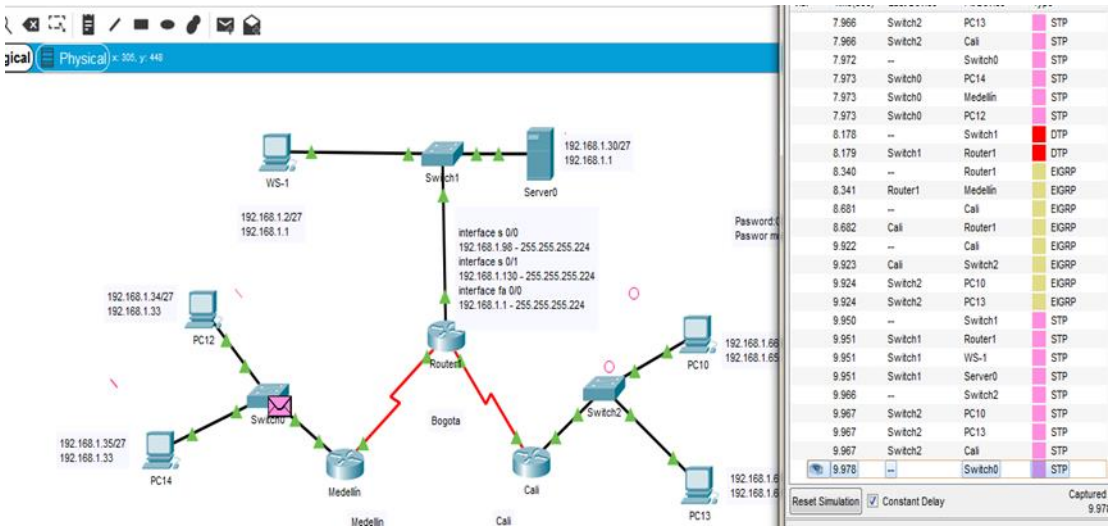
a. Completar la siguiente tabla con la configuración básica de los routers, teniendo en cuenta las subredes diseñadas.

Tabla 2. Configuración básica de los routers

	R1	**R2**	**R3**
Nombre de Host	**MEDELLIN**	**BOGOTA**	**CALI**
Dirección Ip en interfaz Serial 0/0	192.168.1.99	192.168.1.98	192.168.1.131
Dirección Ip en interfaz Serial 0/1		192.168.1.130	
Dirección 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

- Conexión física de los dispositivos

Figura 3. Conexión física de los dispositivos



Configuración de las interfaces direcciones IP con el protocolo de enrutamiento

Configuración Interfaces Router Bogotá.

```
bogota(config)#int s0/0/0
bogota(config-if)#ip address 192.168.1.98 255.255.255.224
bogota(config-if)#no shutdown
bogota(config-if)#int s0/0/1
bogota(config-if)#ip address 192.168.1.130 255.255.255.224
bogota(config-if)#no shutdown
bogota(config-if)#int f0/0
bogota(config-if)#ip address 192.168.1.1 255.255.255.224
bogota(config-if)#no shutdown
bogota(config-if)#router eigrp 200
bogota(config-router)#no auto-summary
bogota(config-router)#network 192.168.1.0
bogota(config-router)#end
```

Configuración Interfaces Router Medellín.

```
medellin(config)#int s0/0/0
medellin(config-if)#ip address 192.168.1.99 255.255.255.224
medellin(config-if)#no shutdown
medellin(config-if)#
medellin(config-if)#int f0/0
medellin(config-if)#ip address 192.168.1.33 255.255.255.224
medellin(config-if)#no shutdown
```

```
medellin(config-if)#
medellin(config-if)#router eigrp 200
medellin(config-router)#no auto-summary
medellin(config-router)#network 192.168.1.0
medellin(config-router)#end
```

Configuración Interfaces Router Cali.

```
cali(config)#int s0/0/0
cali(config-if)#ip address 192.168.1.231 255.255.255.224
cali(config-if)#no shutdown
cali(config-if)#int f0/0
cali(config-if)#ip address 192.168.1.65 255.255.255.224
cali(config-if)#no shutdown
cali(config-if)#router eigrp 200
cali(config-router)#no auto-summary
cali(config-router)#network 192.168.1.0
cali(config-router)#end
cali#
```

b. Después de cargada la configuración en los dispositivos, verificar la tabla de enrutamiento en cada uno

Para realizar esta verificación utilizaremos el comando show ip route nos mostrara una tabla completa de los enrutamientos hecho en la red.

Tabla 3. Verificación tabla de enrutamiento en Bogota con show ip route

```
bogota#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

192.168.1.0/27 is subnetted, 5 subnets
C 192.168.1.0 is directly connected, FastEthernet0/0
D 192.168.1.32 [90/2172416] via 192.168.1.99, 00:04:34, Serial0/0/0
D 192.168.1.64 [90/2172416] via 192.168.1.231, 00:03:31, Serial0/0/1
C 192.168.1.96 is directly connected, Serial0/0/0
C 192.168.1.128 is directly connected, Serial0/0/
```

Figura 4. Verificación tabla de enrutamiento en Bogota con show ip route

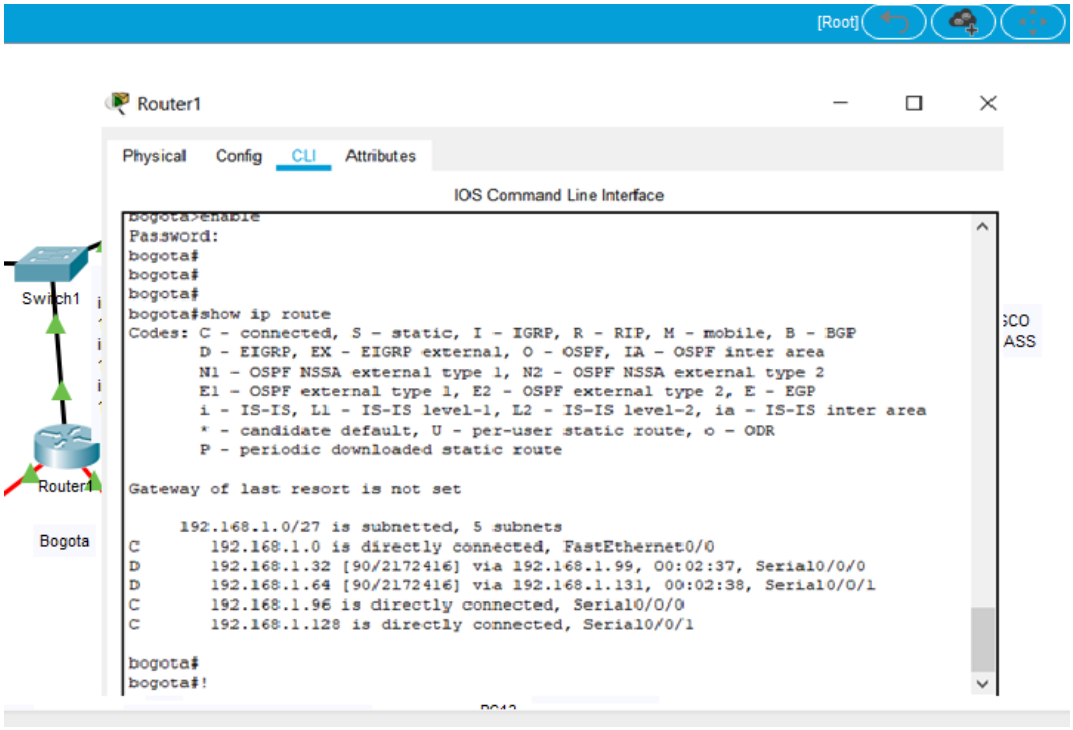


Tabla 4. Verificación tabla de enrutamiento en Medellin con show ip route

medellin#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 192.168.1.0/27 is subnetted, 5 subnets D 192.168.1.0 [90/2172416] via 192.168.1.98, 00:04:41, Serial0/0/0 C 192.168.1.32 is directly connected, FastEthernet0/0 D 192.168.1.64 [90/2684416] via 192.168.1.98, 00:03:38, Serial0/0/0 C 192.168.1.96 is directly connected, Serial0/0/0 D 192.168.1.128 [90/2681856] via 192.168.1.98, 00:03:44, Serial0/0/0

Figura 5. Verificación tabla de enrutamiento en Medellin con show ip route

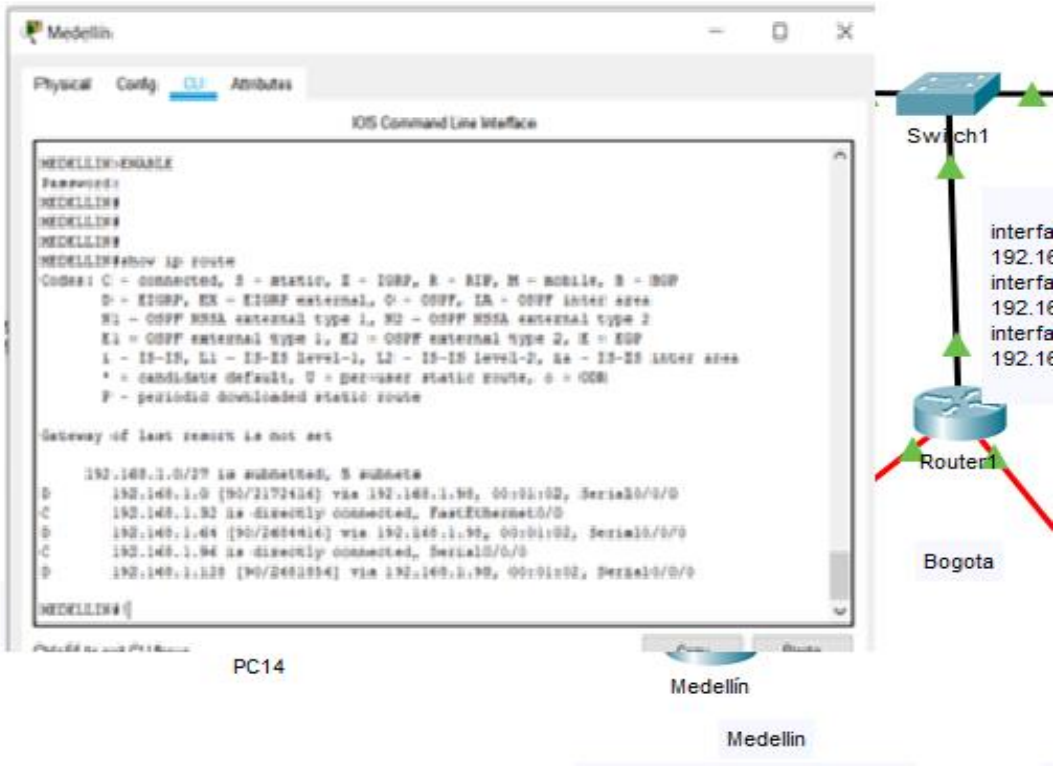
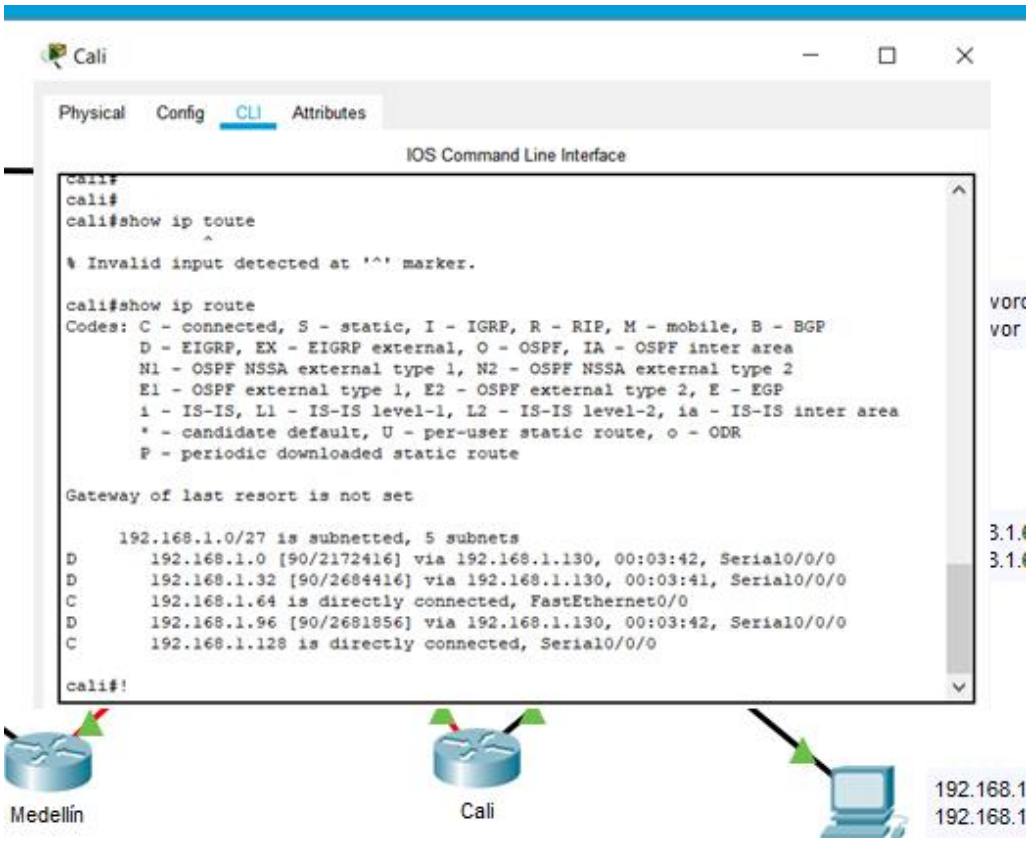


Tabla 5. Verificación tabla de enrutamiento en Cali con show ip route

cali#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 192.168.1.0/27 is subnetted, 5 subnets D 192.168.1.0 [90/2172416] via 192.168.1.130, 00:03:47, Serial0/0/0 D 192.168.1.32 [90/2684416] via 192.168.1.130, 00:03:47, Serial0/0/0 C 192.168.1.64 is directly connected, FastEthernet0/0 D 192.168.1.96 [90/2681856] via 192.168.1.130, 00:03:47, Serial0/0/0 C 192.168.1.128 is directly connected, Serial0/0/0

Figura 6. Verificación tabla de enrutamiento en Cali con show ip route



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

El balanceo de carga se utiliza para equilibrar los datos en una red utilizada por varias terminales conocidas como vecinos y esta posee el mismo costo esto es conocido ECMP (enrutamiento de múltiples rutas del mismo costo).
Por defecto, en plataformas IOS vienen habilitadas un máximo de 4 rutas para hacer balanceo de carga (se permiten tener 4 rutas del mismo costo), la cual puede aumentar hasta un máximo de 32 ECMP por prefijos (redes).

El comando **show ip eigrp topology** muestra la informacion almacenada por el protocolo en la tipologia de la red, permite revisar las rutas factibles y no factibles

Tabla 6. Verificación balanceo de carga en Bogota con show ip eigrp topology

```
bogota#show ip eigrp topology
IP-EIGRP Topology Table for AS 200/ID(192.168.1.130)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
r - Reply status

P 192.168.1.0/27, 1 successors, FD is 28160
via Connected, FastEthernet0/0
P 192.168.1.32/27, 1 successors, FD is 2172416
via 192.168.1.99 (2172416/28160), Serial0/0/0
P 192.168.1.64/27, 1 successors, FD is 2172416
via 192.168.1.231 (2172416/28160), Serial0/0/1
P 192.168.1.96/27, 1 successors, FD is 2169856
via Connected, Serial0/0/0
P 192.168.1.128/27, 1 successors, FD is 2169856
via Connected, Serial0/0/1
```

Tabla 7. Verificación balanceo de carga en Medellin con show ip eigrp topology

```
medellin#show ip eigrp topology
IP-EIGRP Topology Table for AS 200/ID(192.168.1.99)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
r - Reply status

P 192.168.1.0/27, 1 successors, FD is 2172416
via 192.168.1.98 (2172416/28160), Serial0/0/0
P 192.168.1.32/27, 1 successors, FD is 28160
via Connected, FastEthernet0/0
P 192.168.1.64/27, 1 successors, FD is 2684416
via 192.168.1.98 (2684416/2172416), Serial0/0/0
P 192.168.1.96/27, 1 successors, FD is 2169856
via Connected, Serial0/0/0
P 192.168.1.128/27, 1 successors, FD is 2681856
via 192.168.1.98 (2681856/2169856), Serial0/0/0
```

Tabla 8. Verificación balanceo de carga en Cali con show ip eigrp topology

cali#show ip eigrp topology
IP-EIGRP Topology Table for AS 200/ID(192.168.1.231)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
r - Reply status

P 192.168.1.0/27, 1 successors, FD is 2172416
via 192.168.1.130 (2172416/28160), Serial0/0/0
P 192.168.1.32/27, 1 successors, FD is 2684416
via 192.168.1.130 (2684416/2172416), Serial0/0/0
P 192.168.1.64/27, 1 successors, FD is 28160
via Connected, FastEthernet0/0
P 192.168.1.96/27, 1 successors, FD is 2681856
via 192.168.1.130 (2681856/2169856), Serial0/0/0
P 192.168.1.128/27, 1 successors, FD is 2169856
via Connected, Serial0/0/0

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

Este comando ayuda a determinar si alguno de los vecinos con cdp tiene algun error de configuracion.
El CDP brinda la siguiente información acerca de cada dispositivo vecino de CDP:
Identificadores de dispositivos: por ejemplo, el nombre host configurado de un switch.
Lista de direcciones: hasta una dirección de capa de red para cada protocolo admitido.
Identificador de puerto: el nombre del puerto local y remoto en forma de una cadena de caracteres ASCII, como por ejemplo, ethernet0
Lista de capacidades: por ejemplo, si el dispositivo es un router o un switch
Plataforma: plataforma de hardware del dispositivo

Tabla 9. Verificación de vecinos en Bogota con show cdp neighbor

bogota#show cdp neighbor
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
switchbogota
Fas 0/0 176 S 2960 Fas 0/1
medellin Ser 0/0/0 145 R C1841 Ser 0/0/0
cali Ser 0/0/1 148 R C1841 Ser 0/0/0

Figura 7. Verificación de vecinos en Bogota con show cdp neighbor

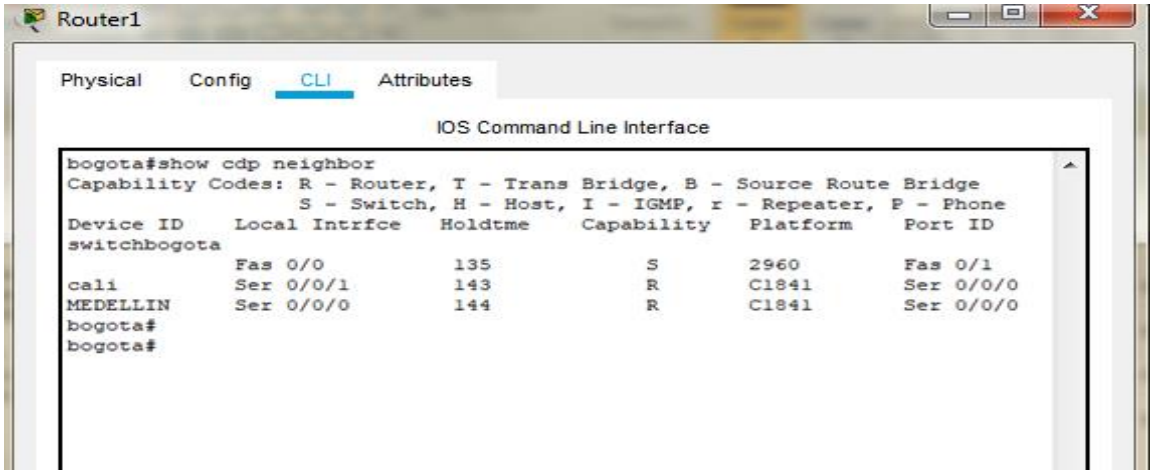


Tabla 10. Verificación de vecinos en Medellin con show cdp neighbor

medellin#show cdp neighbor 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 switchmedellin Fas 0/0 231 S 2960 Fas 0/1 bogota Ser 0/0/0 136 R C1841 Ser 0/0/0

Figura 8. Verificación de vecinos en Medellin con show cdp neighbor

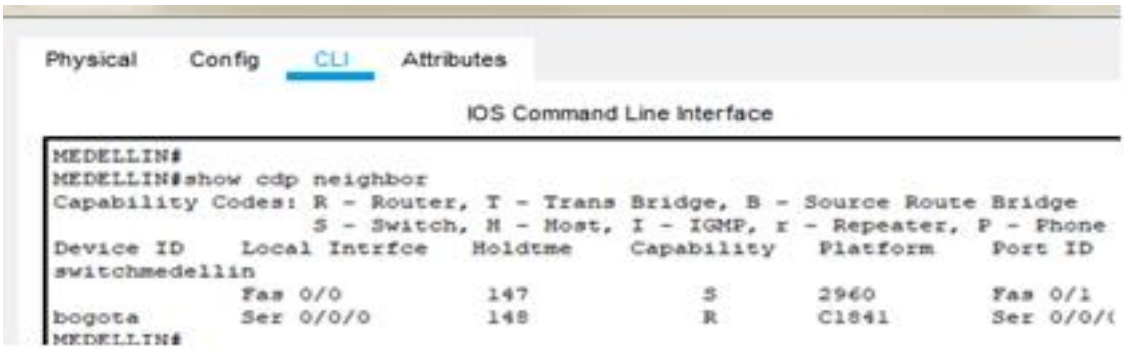
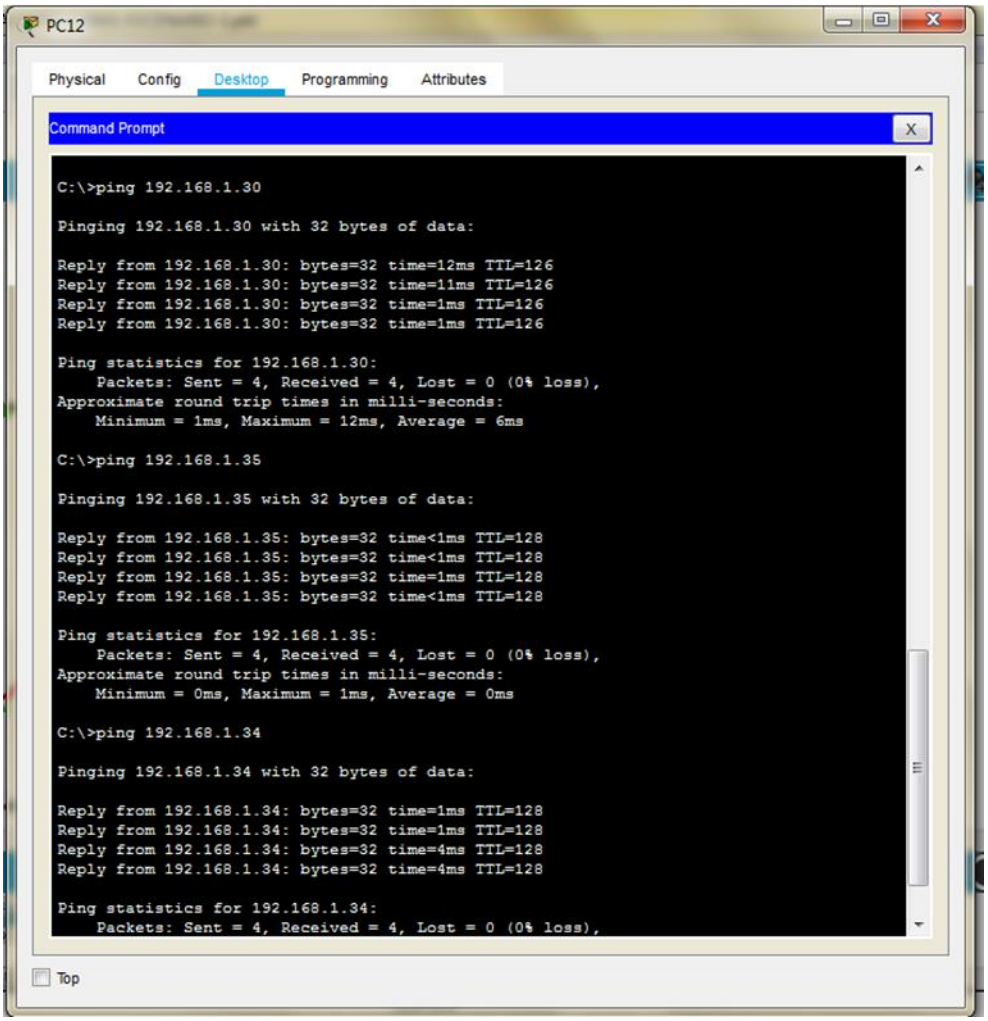


Tabla 11. Verificación de vecinos en Cali con show cdp neighbor

cali#show cdp neighbor 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 switchcali Fas 0/0 126 S 2960 Fas 0/1 bogota Ser 0/0/0 126 R C1841 Ser 0/0/1

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

Figura 9. Verificación prueba de conectividad usando Ping



Parte 3: Configuración de Enrutamiento.

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

Este procedimiento se realizó en el primer punto de la configuración básica se confirma el código de configuración

Configuración Interfaces Router Bogotá.

```
bogota(config-if)#
bogota(config-if)#router eigrp 200
bogota(config-router)#no auto-summary
bogota(config-router)#network 192.168.1.0
bogota(config-router)#end
bogota#
```

Configuración Interfaces Router Medellín.

```
medellin(config-if)#
medellin(config-if)#router eigrp 200
medellin(config-router)#no auto-summary
medellin(config-router)#network 192.168.1.0
medellin(config-router)#end
medellin#
```

Configuración Interfaces Router Cali.

```
cali(config-if)#router eigrp 200
cali(config-router)#no auto-summary
cali(config-router)#network 192.168.1.0
cali(config-router)#end
cali#
```

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

Para verificar la vecindad existente con los router configurado con EIGRP utilizaremos el comando **show ip eigrp neighbor** el cual nos permite ver por medio de una tabla los vecinos descubierto configurados dinámicamente o estáticamente, mostrando el orden, la dirección EGRP, la interface

Tabla 12. Verificación vecindad con Bogota (EIGRP) con show ip eigrp neighbor

bogota#show ip eigrp neighbor
IP-EIGRP neighbors for process 200
H Address Interface Hold Uptime SRTT RTO Q Seq
(sec) (ms) Cnt Num
0 192.168.1.99 Se0/0/0 13 00:04:34 40 1000 0 7
1 192.168.1.231 Se0/0/1 12 00:03:31 40 1000 0 7

Figura 10. Verificación vecindad con Bogota (EIGRP) con show ip eigrp neighbor

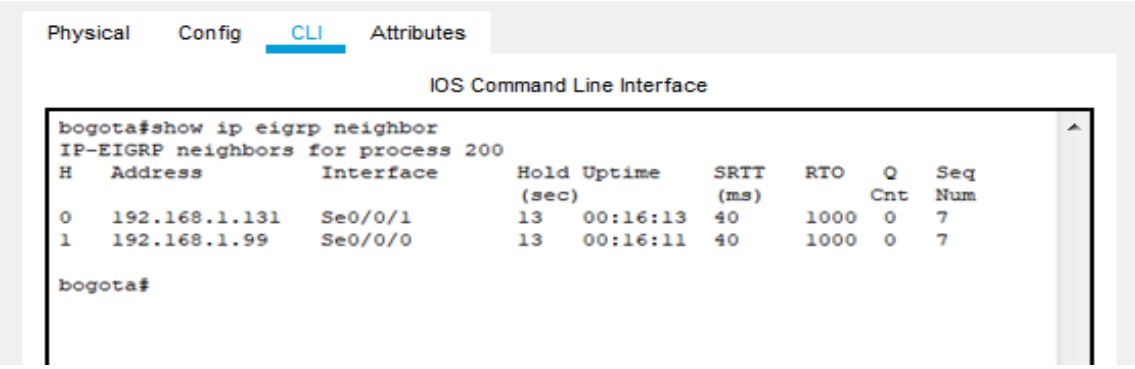


Tabla 13. Verificación vecindad con Medellin (EIGRP) con show ip eigrp neighbor

medellin#show ip eigrp neighbor
IP-EIGRP neighbors for process 200
H Address Interface Hold Uptime SRTT RTO Q Seq
(sec) (ms) Cnt Num
0 192.168.1.98 Se0/0/0 11 00:04:40 40 1000 0 7

Tabla 14. Verificación vecindad con Cali (EIGRP) con show ip eigrp neighbor

cali#show ip eigrp neighbor
IP-EIGRP neighbors for process 200
H Address Interface Hold Uptime SRTT RTO Q Seq
(sec) (ms) Cnt Num
0 192.168.1.130 Se0/0/0 12 00:03:47 40 1000 0 8

SHOW IP EIGRP TOPOLOGY

Tabla 15. Verificación Bogota (EIGRP) con show ip eigrp topology

```
bogota#show ip eigrp topology
IP-EIGRP Topology Table for AS 200/ID(192.168.1.130)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
r - Reply status

P 192.168.1.0/27, 1 successors, FD is 28160
via Connected, FastEthernet0/0
P 192.168.1.32/27, 1 successors, FD is 2172416
via 192.168.1.99 (2172416/28160), Serial0/0/0
P 192.168.1.64/27, 1 successors, FD is 2172416
via 192.168.1.231 (2172416/28160), Serial0/0/1
P 192.168.1.96/27, 1 successors, FD is 2169856
via Connected, Serial0/0/0
P 192.168.1.128/27, 1 successors, FD is 2169856
via Connected, Serial0/0/1
```

Tabla 16. Verificación Medellin (EIGRP) con show ip eigrp topology

```
medellin#show ip eigrp topology
IP-EIGRP Topology Table for AS 200/ID(192.168.1.99)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
r - Reply status

P 192.168.1.0/27, 1 successors, FD is 2172416
via 192.168.1.98 (2172416/28160), Serial0/0/0
P 192.168.1.32/27, 1 successors, FD is 28160
via Connected, FastEthernet0/0
P 192.168.1.64/27, 1 successors, FD is 2684416
via 192.168.1.98 (2684416/2172416), Serial0/0/0
P 192.168.1.96/27, 1 successors, FD is 2169856
via Connected, Serial0/0/0
P 192.168.1.128/27, 1 successors, FD is 2681856
via 192.168.1.98 (2681856/2169856), Serial0/0/0
```

Tabla 17. Verificación Cali (EIGRP) con show ip eigrp topology

```
cali#show ip eigrp topology
IP-EIGRP Topology Table for AS 200/ID(192.168.1.231)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
r - Reply status

P 192.168.1.0/27, 1 successors, FD is 2172416
via 192.168.1.130 (2172416/28160), Serial0/0/0
P 192.168.1.32/27, 1 successors, FD is 2684416
via 192.168.1.130 (2684416/2172416), Serial0/0/0
P 192.168.1.64/27, 1 successors, FD is 28160
via Connected, FastEthernet0/0
P 192.168.1.96/27, 1 successors, FD is 2681856
via 192.168.1.130 (2681856/2169856), Serial0/0/0
P 192.168.1.128/27, 1 successors, FD is 2169856
via Connected, Serial0/0/0
```

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

Para verificar las tablas de enrutamiento utilizaremos el comando **show ip route** el cual nos muestra las direcciones de tráfico de datos.

Tabla 18. Comprobación tabla de enrutamiento en Bogota con show ip route

```
bogota#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

192.168.1.0/27 is subnetted, 5 subnets
C 192.168.1.0 is directly connected, FastEthernet0/0
D 192.168.1.32 [90/2172416] via 192.168.1.99, 00:04:34, Serial0/0/0
D 192.168.1.64 [90/2172416] via 192.168.1.231, 00:03:31, Serial0/0/1
C 192.168.1.96 is directly connected, Serial0/0/0
C 192.168.1.128 is directly connected, Serial0/0/1
```

Figura 11. Comprobación tabla de enrutamiento en Bogota con show ip route

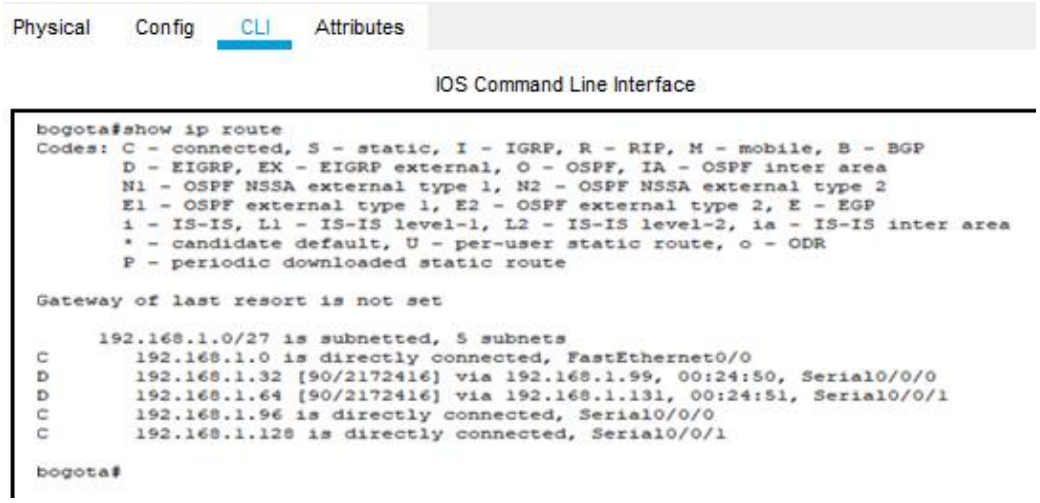


Tabla 19. Comprobación tabla de enrutamiento en Medellin con show ip route

medellin#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

192.168.1.0/27 is subnetted, 5 subnets
D 192.168.1.0 [90/2172416] via 192.168.1.98, 00:04:41, Serial0/0/0
C 192.168.1.32 is directly connected, FastEthernet0/0
D 192.168.1.64 [90/2684416] via 192.168.1.98, 00:03:38, Serial0/0/0
C 192.168.1.96 is directly connected, Serial0/0/0
D 192.168.1.128 [90/2681856] via 192.168.1.98, 00:03:44, Serial0/0/0

Figura 12. Comprobación tabla de enrutamiento en Medellin con show ip route

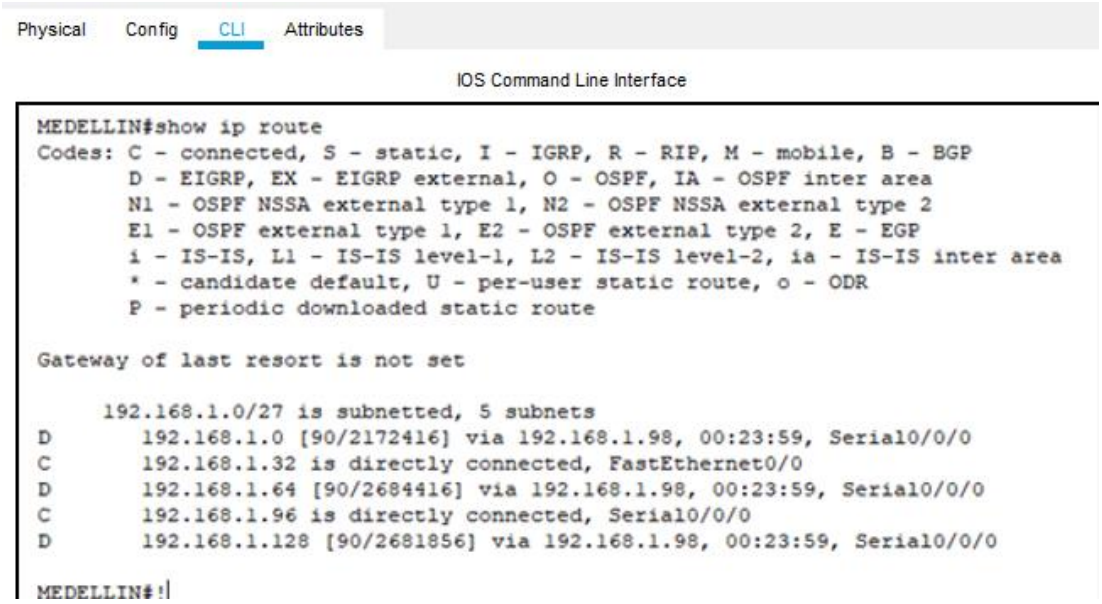


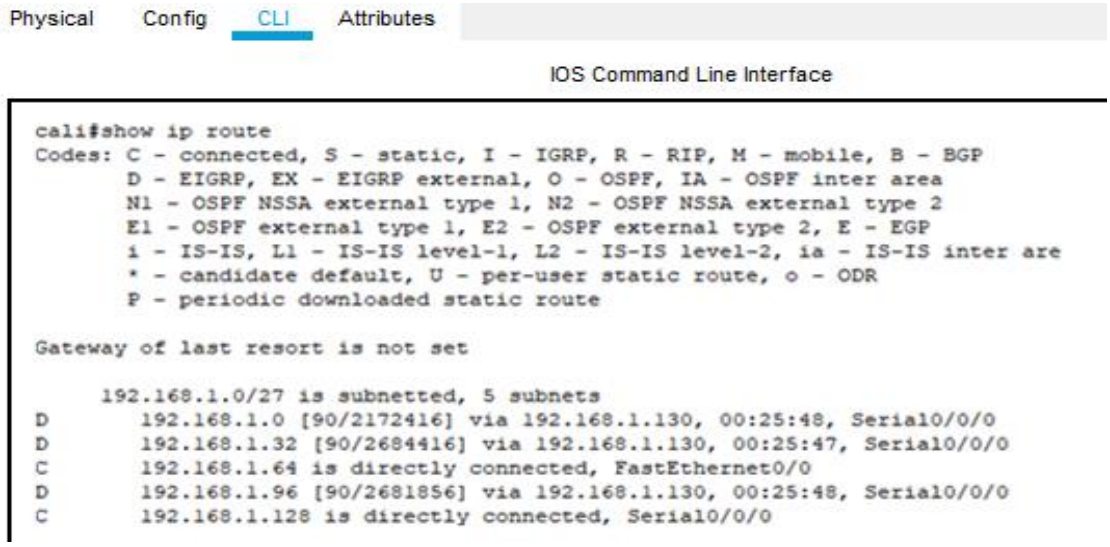
Tabla 20. Comprobación tabla de enrutamiento en Cali con show ip route

cali#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

192.168.1.0/27 is subnetted, 5 subnets
D 192.168.1.0 [90/2172416] via 192.168.1.130, 00:03:47, Serial0/0/0
D 192.168.1.32 [90/2684416] via 192.168.1.130, 00:03:47, Serial0/0/0
C 192.168.1.64 is directly connected, FastEthernet0/0
D 192.168.1.96 [90/2681856] via 192.168.1.130, 00:03:47, Serial0/0/0
C 192.168.1.128 is directly connected, Serial0/0/0

Figura 13. Comprobación tabla de enrutamiento en Cali con show ip route

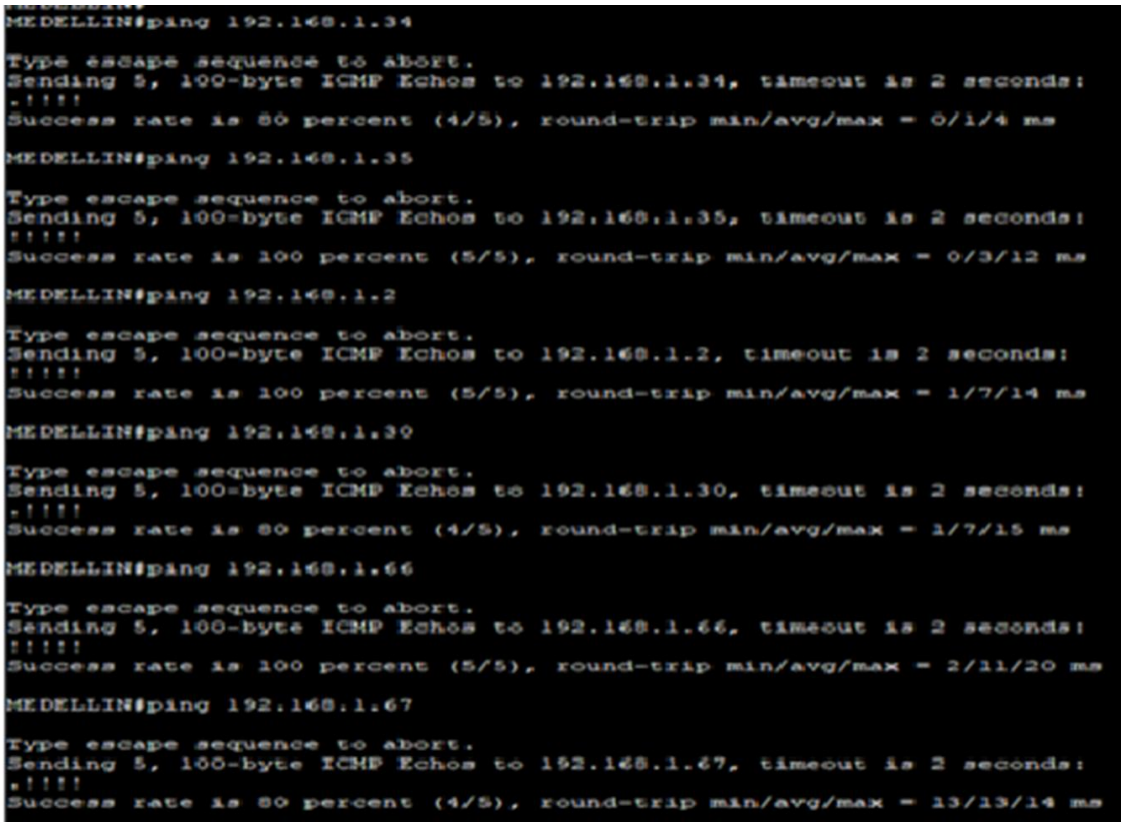


d. Realizar un diagnóstico para comprobar que cada uno de los puntos de la red se puedan ver y tengan conectividad entre sí.

Realizar esta prueba desde un host de la red LAN del router CALI, primero a la red de MEDELLIN y luego al servidor.

Obtenemos respuesta desde cada una de las subredes configuradas

Figura 14. Verificación respuesta subredes configuradas



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:

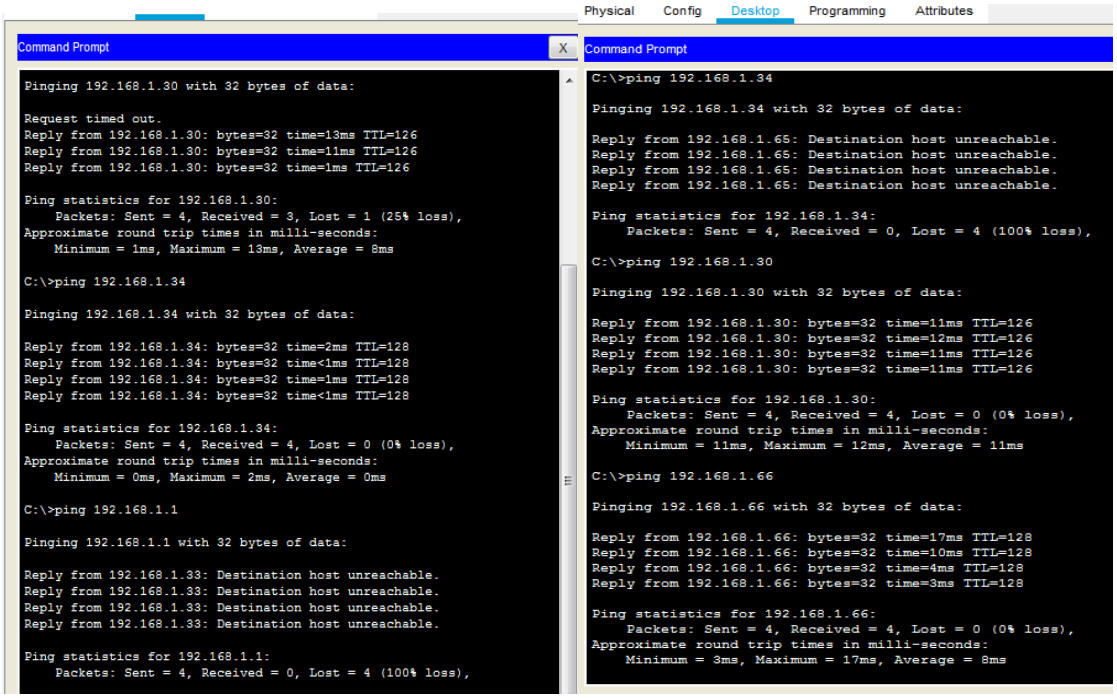
a. Cada router debe estar habilitado para establecer conexiones Telnet con los demás routers y tener acceso a cualquier dispositivo en la red.

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.

Utilizaremos el comando acces-list, el cual permite hacer una lista de control de acceso, para resolver el requisito de la red ejecutaremos el **access-list** estándar donde solo especificaremos una dirección de origen

bogota(config)#access-list 131 permit ip host 192.168.1.30 any
bogota(config)#int f0/0
bogota(config-if)#ip access-group 131 in
bogota(config-if)#

Figura 15. Verificación de listas de Control de Acceso en Bogota

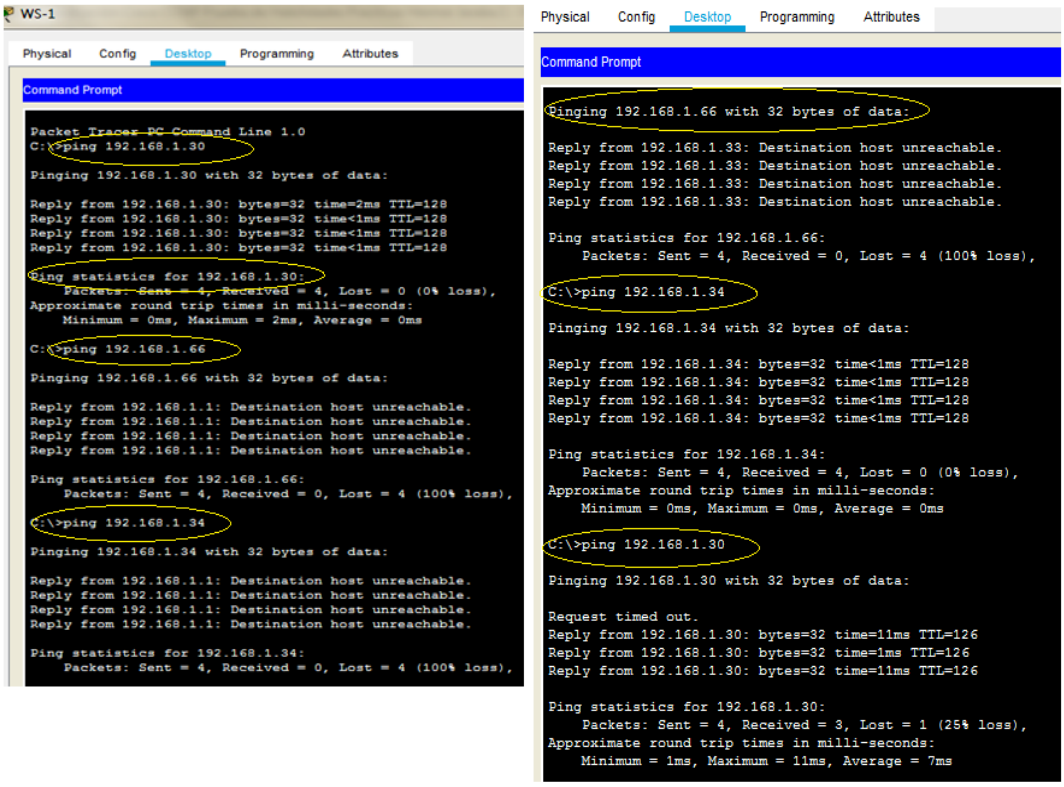


c. Las estaciones de trabajo en las LAN de MEDELLIN y CALI no deben tener acceso a ningún dispositivo fuera de su subred, excepto para interconectar con el servidor.

medellin(config)#access-list **131** permit ip 192.168.1.32 0.0.0.31 host 192.168.1.30
medellin(config)#int f0/0
medellin(config-if)#ip access-group **131** in
medellin(config-if)#

cali(config)#access-list **131** permit ip 192.168.1.64 0.0.0.31 host 192.168.1.30
cali(config)#int f0/0
cali(config-if)#ip access-group 131 in
cali(config-if)#

Figura 16. Verificación de listas de Control de Acceso en Medellin y Cali



Parte 5: Comprobación de la red instalada.

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

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

Tabla 21. Comprobación condiciones de prueba de la Red

	ORIGEN	DESTINO	RESULTADO
TELNET	Router MEDELLIN	Router CALI	exito
	WS_1	Router BOGOTA	Falla
	Servidor	Router CALI	Éxito
	Servidor	Router MEDELLIN	exito
TELNET	LAN del Router MEDELLIN	Router CALI	falla
	LAN del Router CALI	Router CALI	Falle
	LAN del Router MEDELLIN	Router MEDELLIN	Falla
	LAN del Router CALI	Router MEDELLIN	Falla
PING	LAN del Router CALI	WS_1	Falla

	LAN del Router MEDELLIN	**WS_1**	Falla
	LAN del Router MEDELLIN	**LAN del Router CALI**	Falla
PING	**LAN del Router CALI**	**Servidor**	Éxito
	LAN del Router MEDELLIN	**Servidor**	Éxito
	Servidor	**LAN del Router MEDELLIN**	Éxito
	Servidor	**LAN del Router CALI**	Éxito
	Router CALI	**LAN del Router MEDELLIN**	Falla
	Router MEDELLIN	**LAN del Router CALI**	falla

Figura 17. Comprobación condiciones de prueba de la Red 1/9

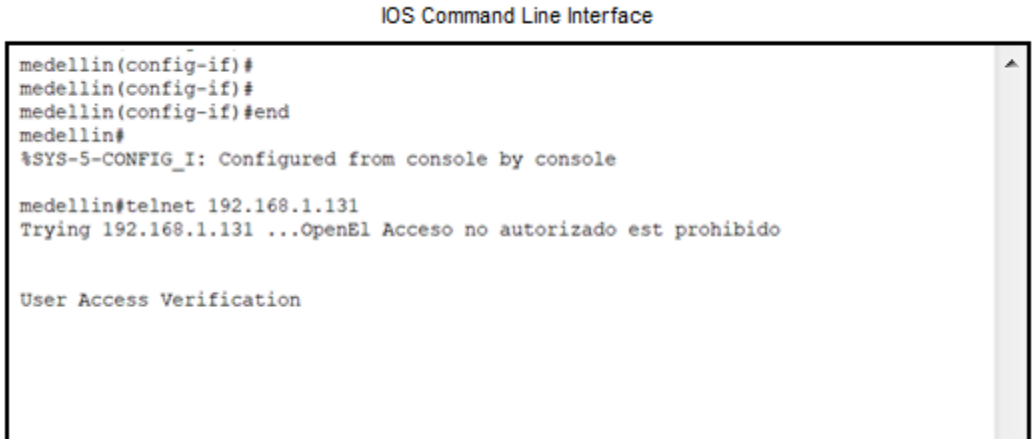


Figura 18. Comprobación condiciones de prueba de la Red 2/9

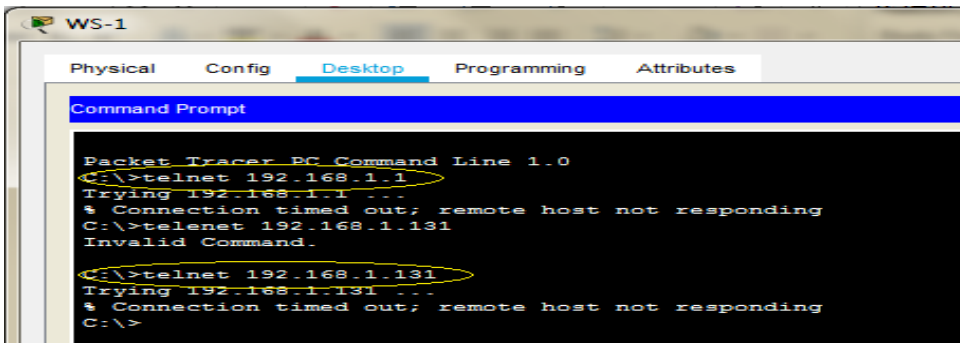


Figura 19. Comprobación condiciones de prueba de la Red 3/9

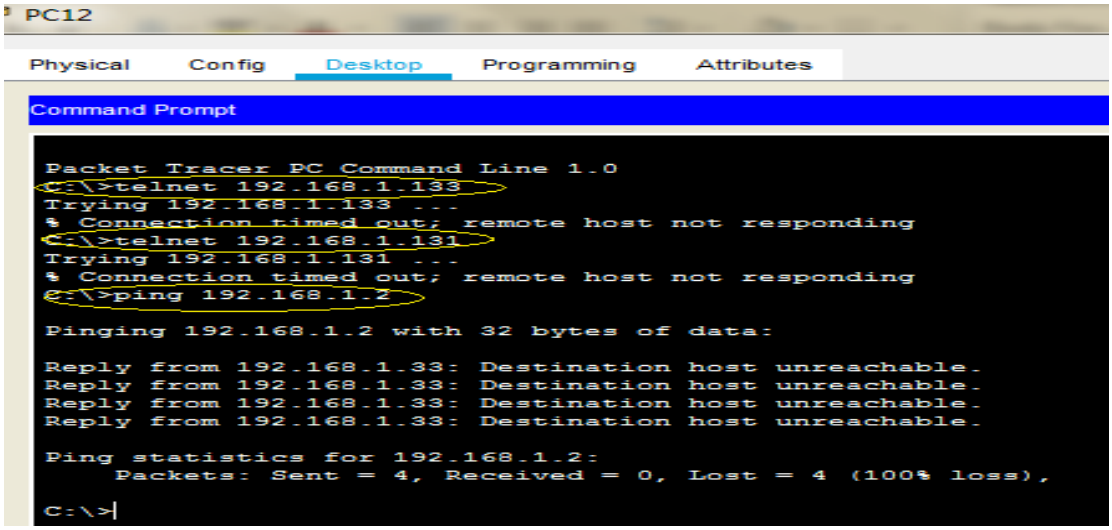


Figura 20. Comprobación condiciones de prueba de la Red 4/9

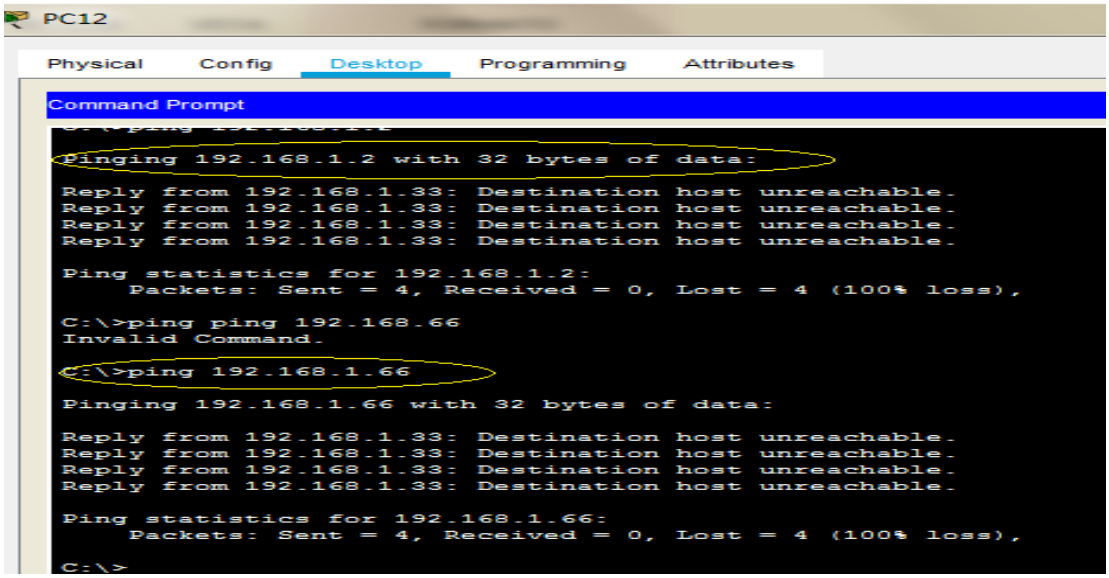


Figura 21. Comprobación condiciones de prueba de la Red 5/9

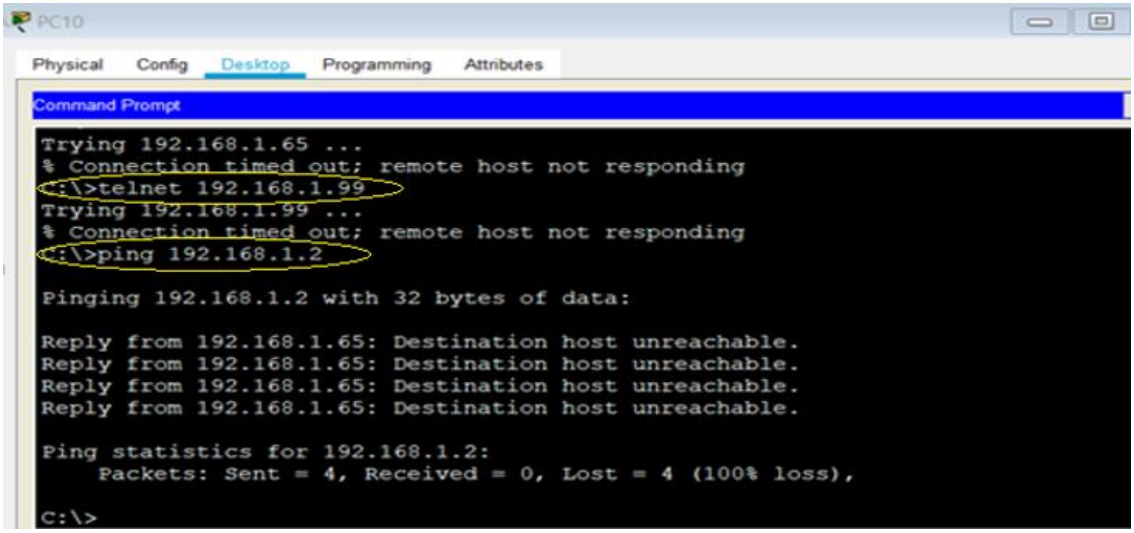


Figura 22. Comprobación condiciones de prueba de la Red 6/9

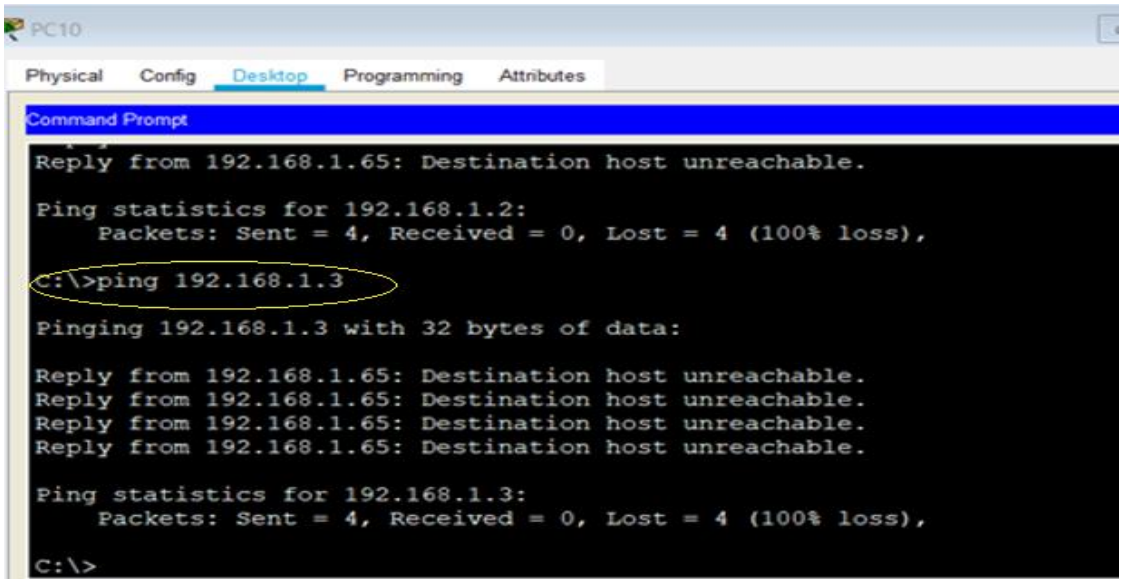


Figura 23. Comprobación condiciones de prueba de la Red 7/9

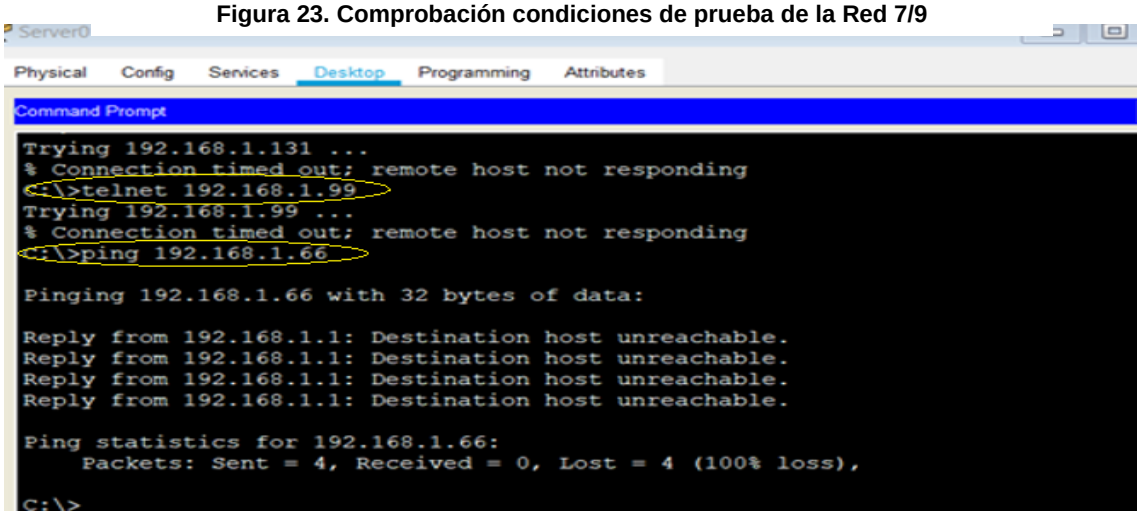


Figura 24. Comprobación condiciones de prueba de la Red 8/9

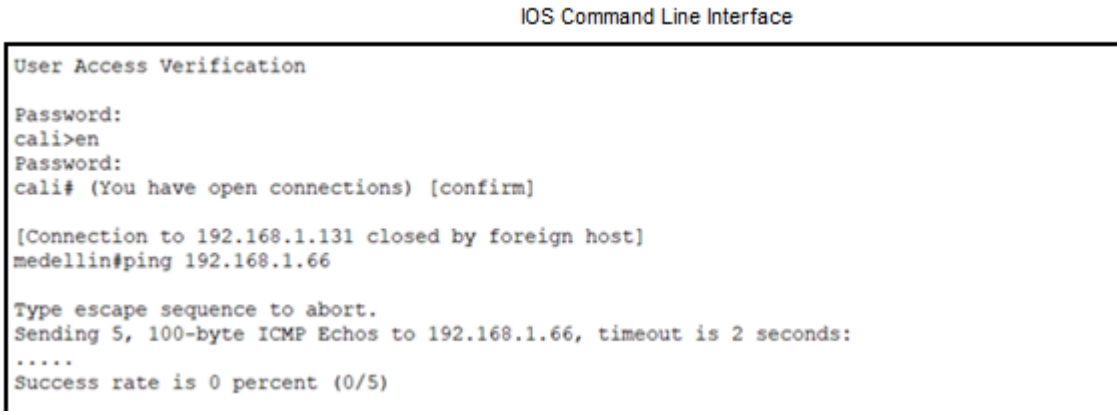
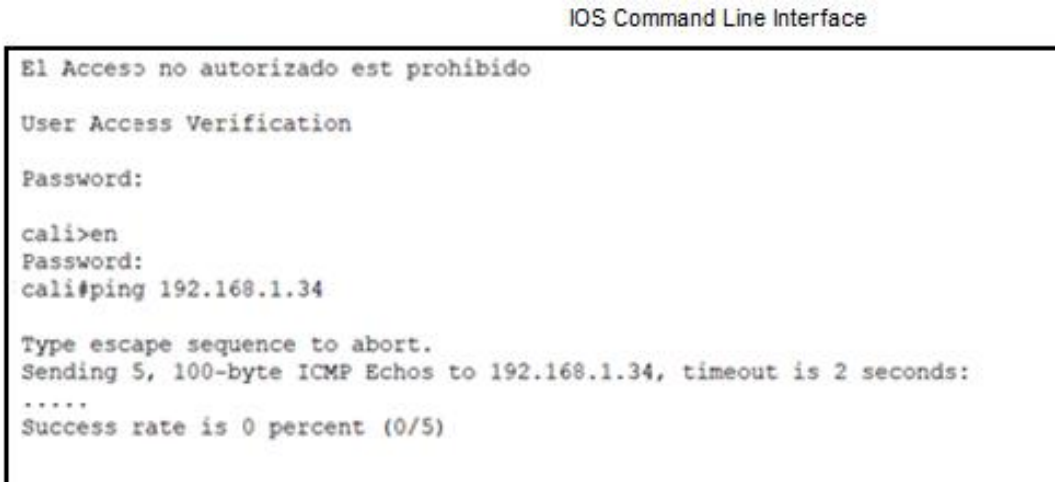


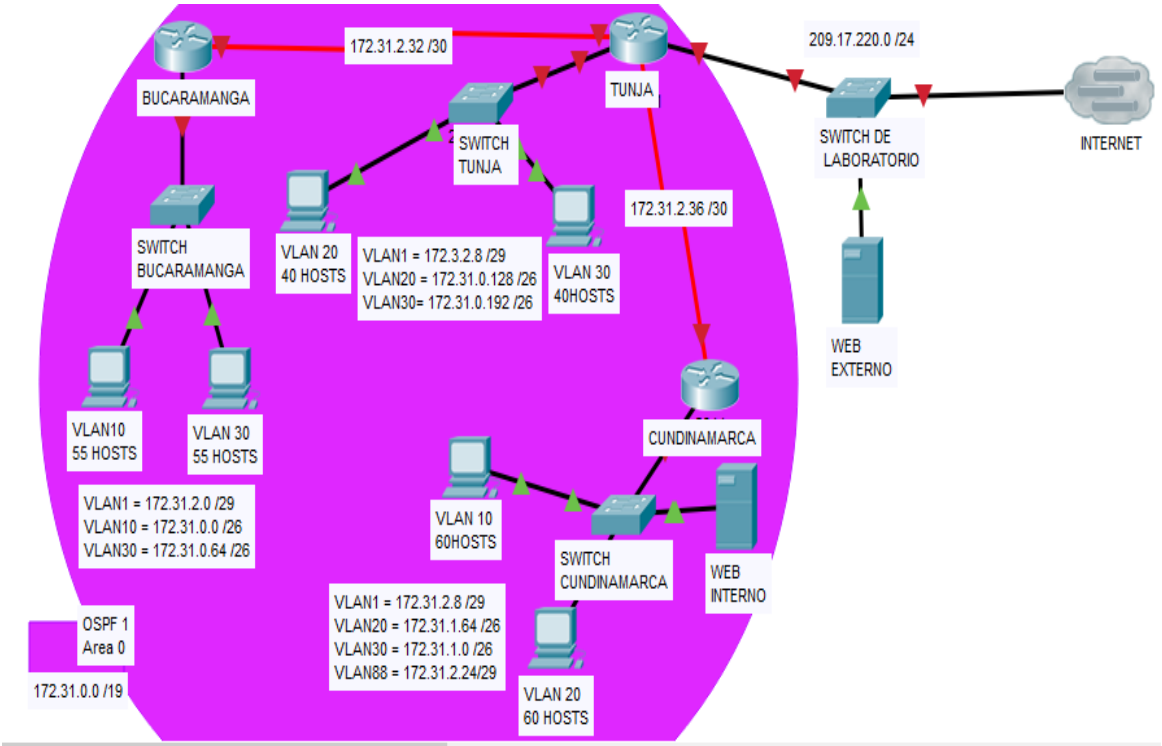
Figura 25. Comprobación condiciones de prueba de la Red 9/9



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

Figura 26. Topología Escenario 2



Desarrollo de la actividad escenario 2

Los siguientes son los requerimientos necesarios:

Parte 1: Todos los routers deberán tener lo siguiente

a. Configuración Básica

- Se realiza el código fuente de los Router para la configuración básica Contraseña, mensaje de alerta, bloqueo del dominio, configuración de interface, asignación de la dirección IP

Configuración router Bucaramanga

```
Router(config)#hostname bucaramanga
bucaramanga(config)#no ip domain-lookup
bucaramanga(config)#banner motd $El Acceso no autorizado está prohibido$
bucaramanga(config)#enable secret class1
bucaramanga(config)#line console 0
bucaramanga(config-line)#password cisco1
bucaramanga(config-line)#login
bucaramanga(config-line)#line vty 0 15
bucaramanga(config-line)#password cisco1
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)#
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#
```

Configuración Router Tunja

```
Router(config)#hostname tunja
tunja(config)#no ip domain-lookup
tunja(config)#banner motd $El Acceso no autorizado est prohibido$
tunja(config)#enable secret class1
tunja(config)#line console 0
tunja(config-line)#password cisco1
tunja(config-line)#login
tunja(config-line)#line vty 0 15
```

```
tunja(config-line)#password cisco1
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#
```

Configuración Router Cundinamarca

```
Router(config)#hostname cundinamarca
cundinamarca(config)#no ip domain-lookup
cundinamarca(config)#banner motd $El Acceso no autorizado est prohibido$
cundinamarca(config)#enable secret class1
cundinamarca(config)#line console 0
cundinamarca(config-line)#password cisco1
cundinamarca(config-line)#login
cundinamarca(config-line)#line vty 0 15
cundinamarca(config-line)#password cisco1
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)#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
cundinamarca#
```

- Se realiza el código fuente de la configuración de los SWITCH, enrutamiento de las interfaces y creación de las VLAN

Configuración del switch Bucaramanga

```
Switch(config)#hostname switchbucaramanga
switchbucaramanga(config)#vlan 1
switchbucaramanga(config-vlan)#vlan 10
switchbucaramanga(config-vlan)#vlan 30
switchbucaramanga(config-vlan)#int f0/10
switchbucaramanga(config-if)#switchport mode access
switchbucaramanga(config-if)#switchport access vlan 10
switchbucaramanga(config-if)#int f0/14
switchbucaramanga(config-if)#switchport mode access
switchbucaramanga(config-if)#switchport access vlan 30
switchbucaramanga(config-if)#int f0/1
switchbucaramanga(config-if)#switchport mode trunk
switchbucaramanga(config-if)#int vlan 1
```

```
switchbucaramanga(config-if)#ip address 172.31.2.3 255.255.255.248
switchbucaramanga(config-if)#no shutdown
switchbucaramanga(config-if)#ip default-gateway 172.31.2.1
switchbucaramanga(config)#
```

Configuración del switch Tunja

```
Switch(config)#hostname swtichtunja
swtichtunja(config)#vlan 1
swtichtunja(config-vlan)#vlan 20
swtichtunja(config-vlan)#vlan 30
swtichtunja(config-vlan)#int f0/10
swtichtunja(config-if)#switchport mode access
swtichtunja(config-if)#switchport access vlan 20
swtichtunja(config-if)#int f0/14
swtichtunja(config-if)#switchport mode access
swtichtunja(config-if)#switchport access vlan 30
swtichtunja(config-if)#int f0/1
swtichtunja(config-if)#switchport mode trunk
swtichtunja(config-if)#int vlan 1
swtichtunja(config-if)#ip address 172.3.2.11 255.255.255.248
swtichtunja(config-if)#no shutdown
swtichtunja(config-if)#ip default-gateway 172.3.2.9
swtichtunja(config)#
swtichtunja(config)#
```

Configuración del switch Cundinamarca

```
Switch(config)#hostname swithccundinamarca
swithccundinamarca(config)#vlan 1
swithccundinamarca(config-vlan)#vlan 20
swithccundinamarca(config-vlan)#vlan 30
swithccundinamarca(config-vlan)#vlan 88
swithccundinamarca(config-vlan)#exit
swithccundinamarca(config)#int f0/10
swithccundinamarca(config-if)#switchport mode access
swithccundinamarca(config-if)#switchport access vlan 20
swithccundinamarca(config-if)#int f0/14
swithccundinamarca(config-if)#switchport mode access
swithccundinamarca(config-if)#switchport access vlan 30
swithccundinamarca(config-if)#int f0/20
swithccundinamarca(config-if)#switchport mode access
swithccundinamarca(config-if)#switchport access vlan 88
```

```
swithccundinamarca(config-if)#int f0/1
swithccundinamarca(config-if)#switchport mode trunk
swithccundinamarca(config-if)#int vlan 1
swithccundinamarca(config-if)#ip address 172.31.2.11 255.255.255.248
swithccundinamarca(config-if)#no shutdown
swithccundinamarca(config-if)#ip default-gateway 172.31.2.9
```

b. Autenticación local con AAA

En esta etapa realizaremos el código para la autenticación AAA en los tres routers

Autenticación triple AAA cumple una función importante en el soporte de seguridad del router ya que comprueban que los usuarios y administradores de la red sean los que dicen ser.
Autorización, después de la autenticación del usuario, decide que recursos puede utilizar en la red.
Registro, crea una base de datos temporalmente

Para la configuración AAA del router la haremos localmente entre el Server por medio de comandos de autenticación y autorización. Para la comunicación entre los routers.

Configuración para el router Bucaramanga

```
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
```

Configuración para el router Tunja

```
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
```

Configuración para el router Cundinamarca

```
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
```

Configuración del cifrado de contraseña, Intentos máximos para acceder al router y tiempo de acceso al detectar el ataque.

c. Cifrado de contraseñas.

El comando **service password-encryption**, aplica un cifrado a las contraseñas en los datos de configuración.

```
bucaramanga(config)#service password-encryption
tunja(config)#service password-encryption
cundinamarca(config)#service password-encryption
```

Con el comando **login block-for** se configura el router para que entre en un periodo de 20 segundos de silencio en 10 intentos fallidos de inicio en un periodo de 60 segundos, con esta configuración no aceptara ninguna conexión adicional en el tiempo establecido.

d. Un máximo de internos para acceder al router.

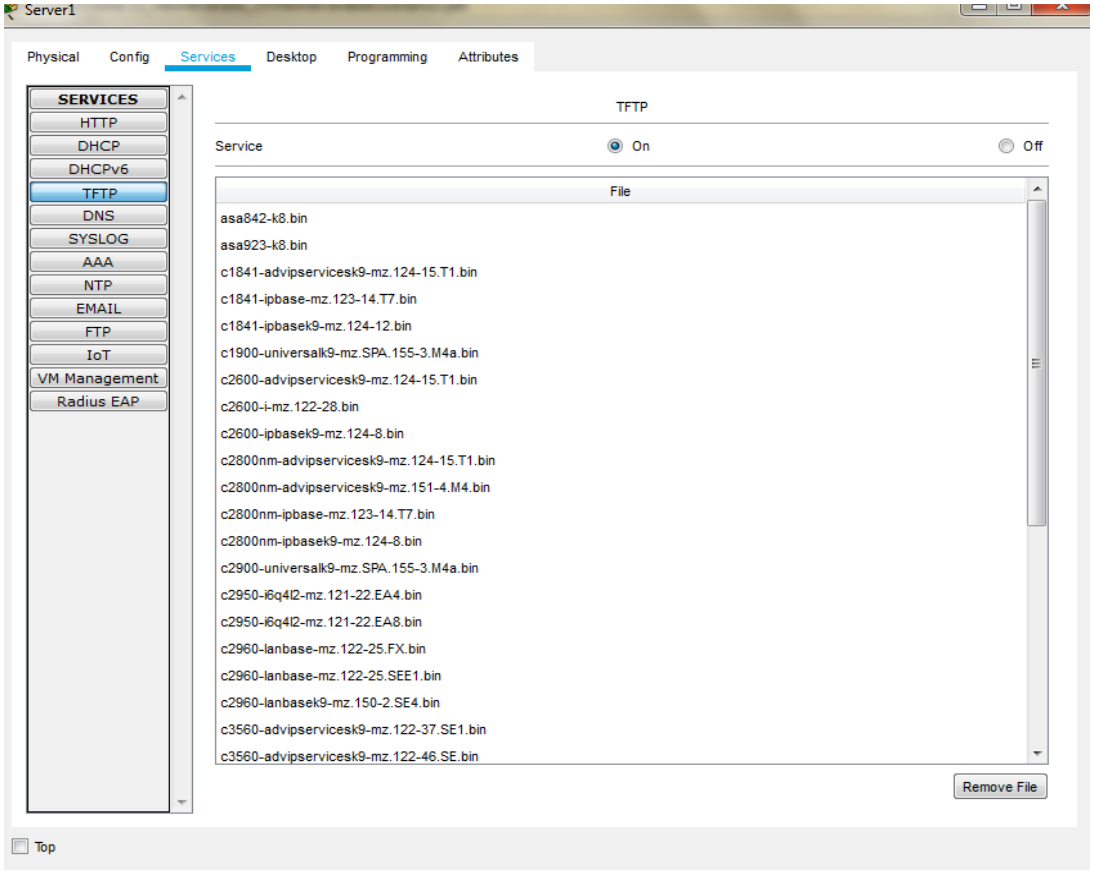
```
bucaramanga(config-line)#login block-for 20 attempts 10 within 60
tunja(config-line)#login block-for 20 attempts 10 within 60
cundinamarca(config-line)#login block-for 20 attempts 10 within 60
```

e. 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

f. Establezca un servidor TFTP y almacene todos los archivos necesarios de los routers.

Figura 27. Verificación almacenamiento en servidor TFTP



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

La configuración DCHP reduce los errores de forma considerable cunado las direcciones IP se asignan manualmente, ya que puede realizar las configuraciones de las terminales y host de forma automática en la red.

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

Se configuran cada uno de los routers para que puedan tener acceso a estos POOL de direcciones.

Se define la agrupación de direcciones IP haciendo el requerimiento al DCHP server con el comando helper-address, para que puede acceder a los nodos móviles de la red, para los host Bucaramanga y Cundinamarca.

Configuración Bucaramanga

bucaramanga(config)#int f0/0.10
bucaramanga(config-subif)#ip helper-address 172.31.2.33
bucaramanga(config-subif)#int f0/0.30
bucaramanga(config-subif)#ip helper-address 172.31.2.33
bucaramanga(config-subif)#end
bucaramanga#

Configuración Cundinamarca

```
cundinamarca(config)#int f0/0.20
cundinamarca(config-subif)#ip helper-address 172.31.2.37
cundinamarca(config-subif)#int f0/0.30
cundinamarca(config-subif)#ip helper-address 172.31.2.37
cundinamarca(config-subif)#end
cundinamarca#
```

Verificamos que cada uno de los PC de las VLAN de los routers de Bucaramanga y Cundinamarca obtenga sus direcciones IP empleando DHCP que es la forma automática que tiene el programa para asignar las IP

Figura 28. Verificación asignación IP por DHCP a los PCS de Bucaramanga y Cundinamarca 1/4

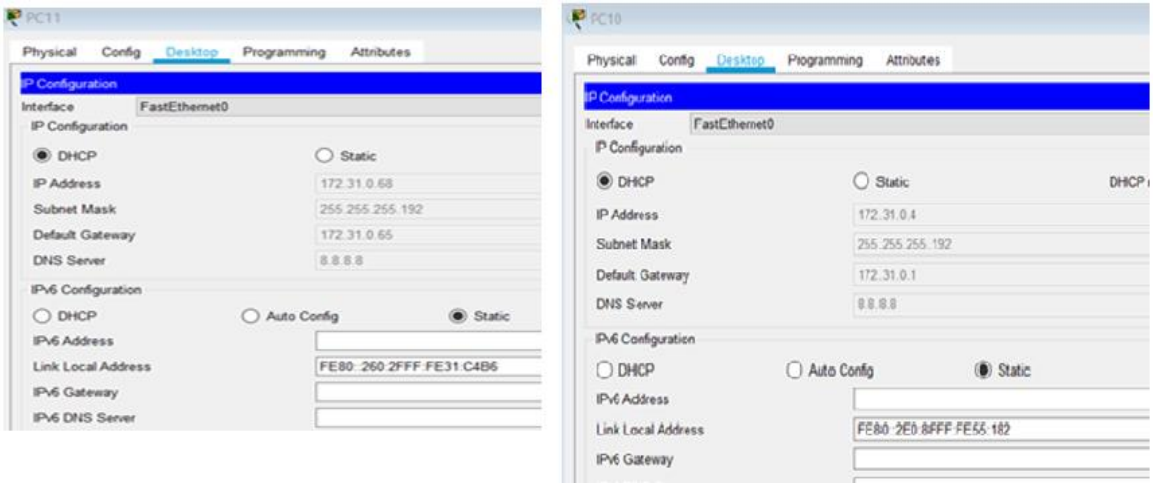


Figura 29. Verificación asignación IP por DHCP a los PCS de Bucaramanga y Cundinamarca 2/4

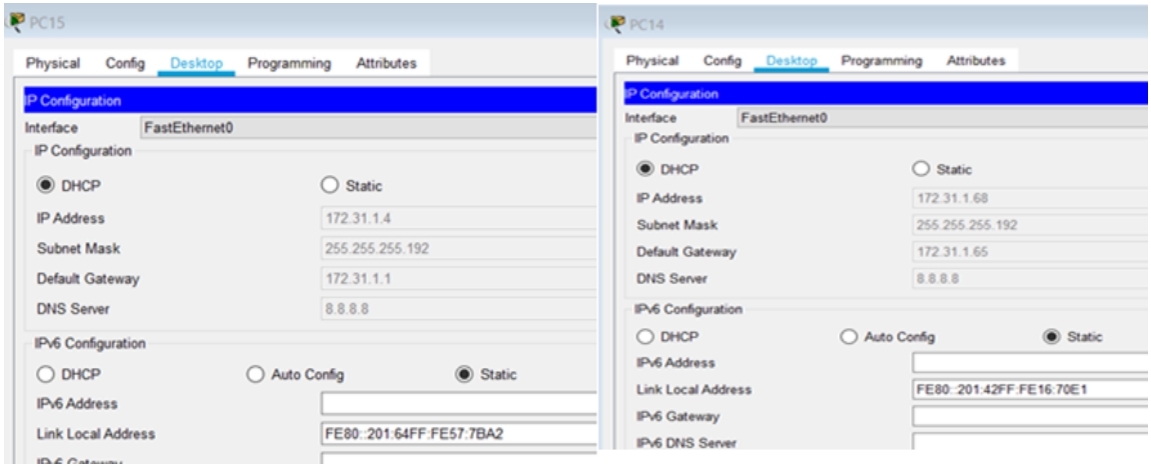


Figura 30. Verificación asignación IP por DHCP a los PCS de Bucaramanga y Cundinamarca 3/4

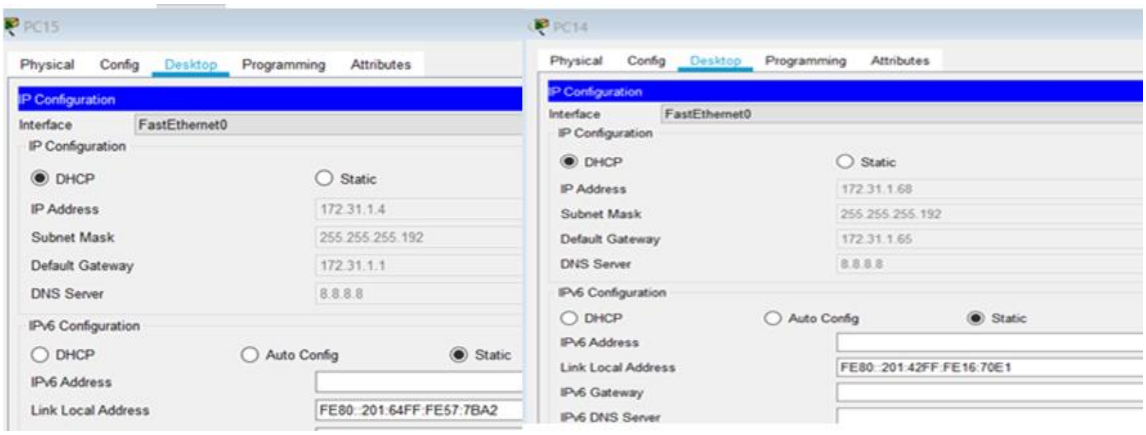
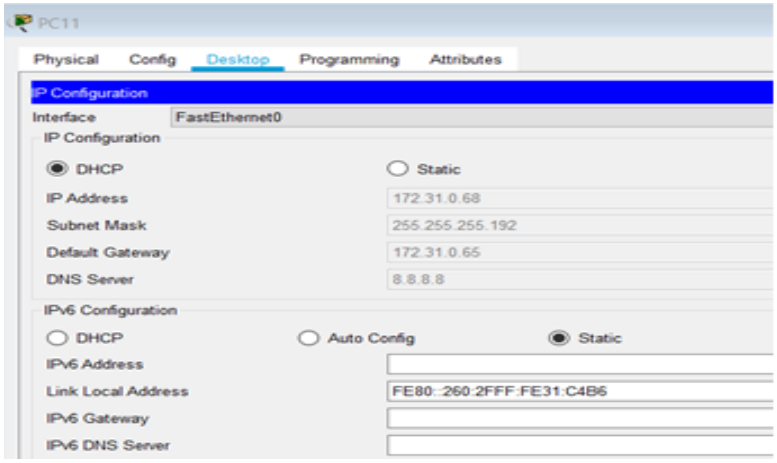


Figura 31. Verificación asignación IP por DHCP a los PCS de Bucaramanga y Cundinamarca 4/4



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

Se configura un Ipv4 pública para el direccionamiento de las Ipv4 privadas internas de esta forma se conserva la dirección del conjunto global interna.

```
tunja(config)#ip nat inside source static 172.31.2.28 209.165.220.10
tunja(config)#access-list 11 permit 172.0.0.0 0.255.255.255
tunja(config)#ip nat inside source list 11 interface f0/1 overload
tunja(config)#int f0/1
tunja(config-if)#ip nat outside
```

```
tunja(config-if)#int f0/0.1
tunja(config-subif)#ip nat inside
tunja(config-subif)#int f0/0.20
tunja(config-subif)#ip nat inside
tunja(config-subif)#int f0/0.30
tunja(config-subif)#ip nat inside
tunja(config-subif)#int s0/0/0
tunja(config-if)#ip nat inside
tunja(config-if)#int s0/0/1
tunja(config-if)#ip nat inside
tunja(config-if)#exit
tunja(config)#ip route 0.0.0.0 0.0.0.0 209.165.220.4
tunja(config)#router ospf 1
tunja(config-router)#default-information originate
tunja(config-router)#end
tunja#
```

Comprobación de las interfaces de los routers con el comando show ip route

Router Tunja

Tabla 22. Comprobación interfaz router Tunja con show ip route

```
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 209.165.220.4 to network 0.0.0.0

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, 11 subnets, 3 masks
O 172.31.0.0/26 [110/65] via 172.31.2.34, 00:10:47, Serial0/0/0
O 172.31.0.64/26 [110/65] via 172.31.2.34, 00:10:47, 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, 00:10:47, Serial0/0/1
O 172.31.1.64/26 [110/65] via 172.31.2.38, 00:10:47, Serial0/0/1
O 172.31.2.0/29 [110/65] via 172.31.2.34, 00:10:47, Serial0/0/0
```

```
O 172.31.2.8/29 [110/65] via 172.31.2.38, 00:10:47, Serial0/0/1
O 172.31.2.24/29 [110/65] via 172.31.2.38, 00:10:47, 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
S* 0.0.0.0/0 [1/0] via 209.165.220.4
```

Router Bucaramanga

Tabla 23. Comprobación interfaz router Bucaramanga con show ip route

```
bucaramanga#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 172.31.2.33 to network 0.0.0.0

172.3.0.0/29 is subnetted, 1 subnets
O 172.3.2.8 [110/65] via 172.31.2.33, 00:11:18, Serial0/0/0
172.31.0.0/16 is variably subnetted, 11 subnets, 3 masks
C 172.31.0.0/26 is directly connected, FastEthernet0/0.10
C 172.31.0.64/26 is directly connected, FastEthernet0/0.30
O 172.31.0.128/26 [110/65] via 172.31.2.33, 00:11:18, Serial0/0/0
O 172.31.0.192/26 [110/65] via 172.31.2.33, 00:11:18, Serial0/0/0
O 172.31.1.0/26 [110/129] via 172.31.2.33, 00:11:18, Serial0/0/0
O 172.31.1.64/26 [110/129] via 172.31.2.33, 00:11:18, Serial0/0/0
C 172.31.2.0/29 is directly connected, FastEthernet0/0.1
O 172.31.2.8/29 [110/129] via 172.31.2.33, 00:11:18, Serial0/0/0
O 172.31.2.24/29 [110/129] via 172.31.2.33, 00:11:18, Serial0/0/0
C 172.31.2.32/30 is directly connected, Serial0/0/0
O 172.31.2.36/30 [110/128] via 172.31.2.33, 00:11:18, Serial0/0/0
O*E2 0.0.0.0/0 [110/1] via 172.31.2.33, 00:00:51, Serial0/0/0
bucaramanga#
```

Router Cundinamarca

Tabla 24. Comprobación interfaz router Cundinamarca con show ip route

```
cundinamarca#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 172.31.2.37 to network 0.0.0.0

172.3.0.0/29 is subnetted, 1 subnets
O 172.3.2.8 [110/65] via 172.31.2.37, 00:12:02, Serial0/0/0
172.31.0.0/16 is variably subnetted, 11 subnets, 3 masks
O 172.31.0.0/26 [110/129] via 172.31.2.37, 00:11:52, Serial0/0/0
O 172.31.0.64/26 [110/129] via 172.31.2.37, 00:11:52, Serial0/0/0
O 172.31.0.128/26 [110/65] via 172.31.2.37, 00:12:02, Serial0/0/0
O 172.31.0.192/26 [110/65] via 172.31.2.37, 00:12:02, Serial0/0/0
C 172.31.1.0/26 is directly connected, FastEthernet0/0.30
C 172.31.1.64/26 is directly connected, FastEthernet0/0.20
O 172.31.2.0/29 [110/129] via 172.31.2.37, 00:11:52, Serial0/0/0
C 172.31.2.8/29 is directly connected, FastEthernet0/0.1
C 172.31.2.24/29 is directly connected, FastEthernet0/0.88
O 172.31.2.32/30 [110/128] via 172.31.2.37, 00:12:02, Serial0/0/0
C 172.31.2.36/30 is directly connected, Serial0/0/0
O*E2 0.0.0.0/0 [110/1] via 172.31.2.37, 00:01:34, Serial0/0/0
cundinamarca#
```

Figura 32. Comprobación interfaz router Tunja con show ip nat tra

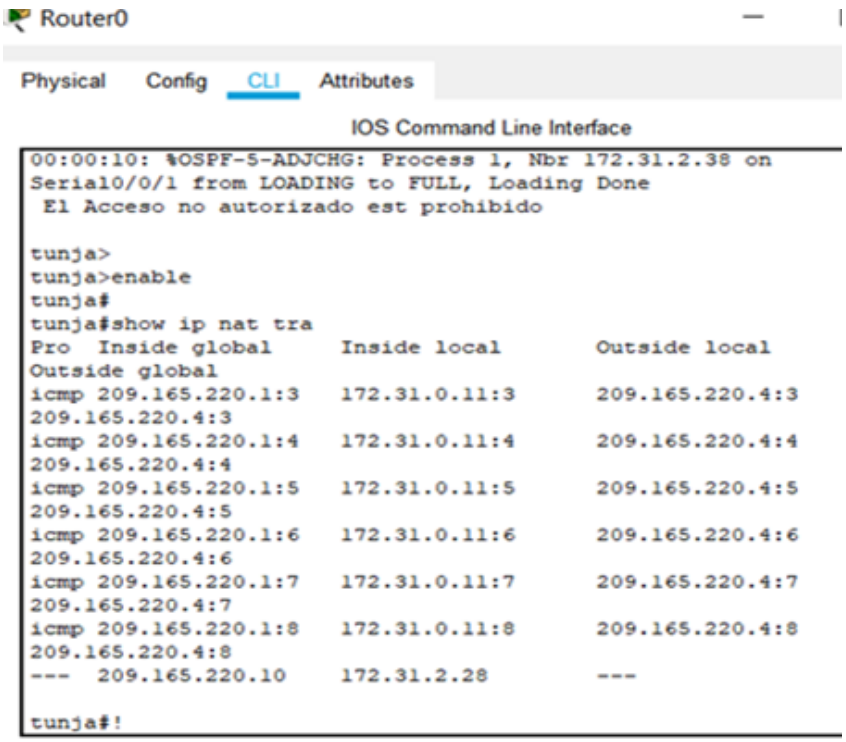
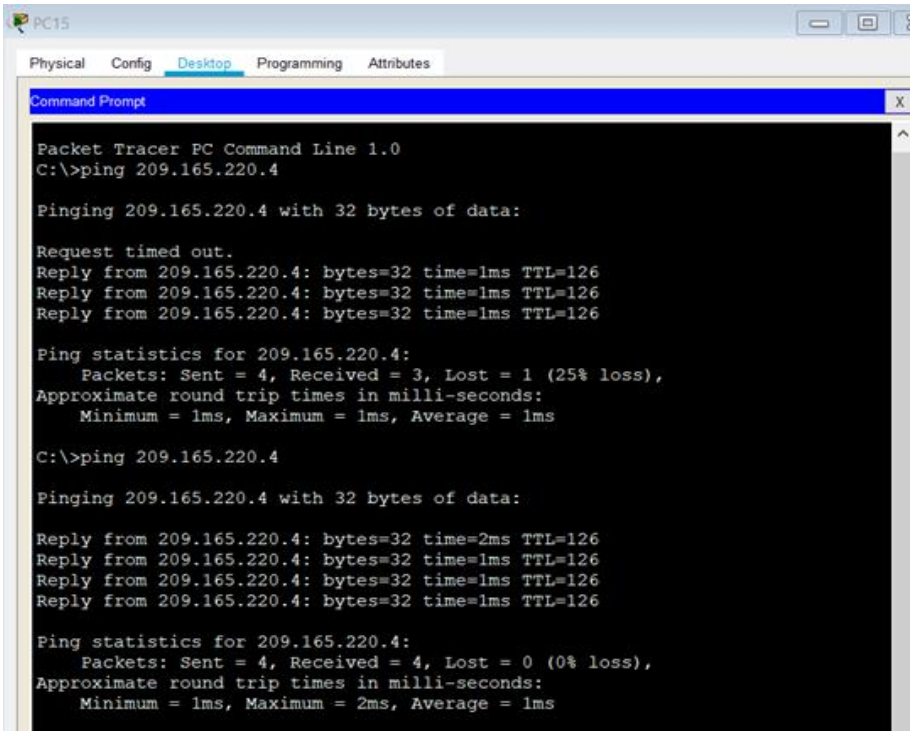


Figura 33. Prueba de Ping a router Tunja



Parte 4: El enrutamiento deberá tener autenticación.

El comando **ip ospf** habilita la autenticación para todas las interfaces del enrutador en un área determinada en nuestro caso autenticaremos el MD5, esto es útil para la autenticación de diferentes interfaces de una misma área y necesitan usar diferentes tipos de autenticación

```
bucaramanga#conf t
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#conf t
Enter configuration commands, one per line. End with CNTL/Z.
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#conf t
Enter configuration commands, one per line. End with CNTL/Z.
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
cundinamarca(config-if)#
```

Parte 5: Listas de control de acceso.

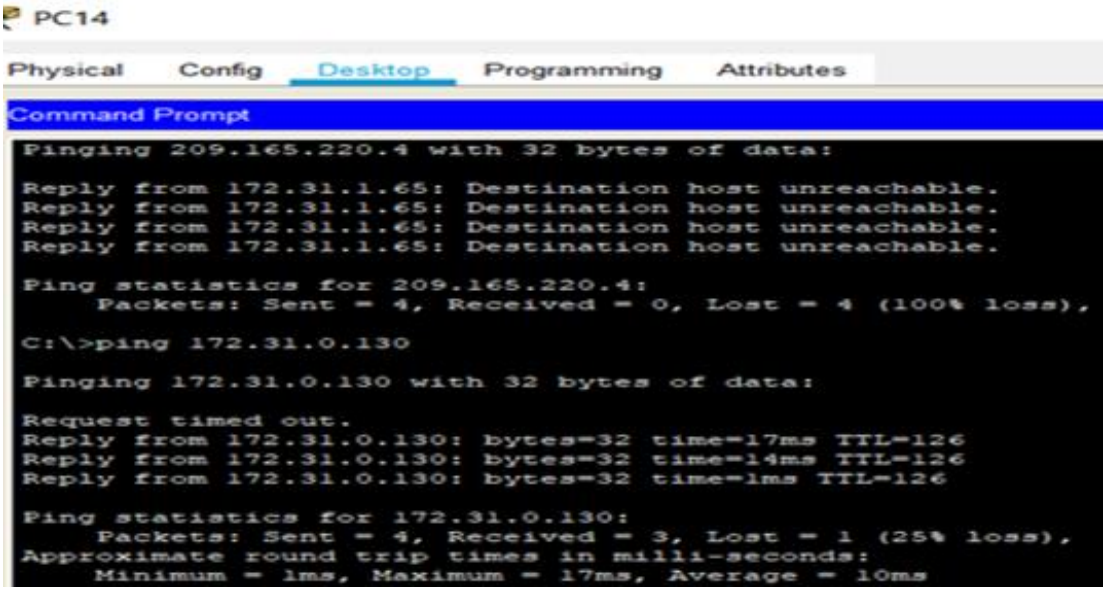
Otorgamos la lista de acceso para los usuarios para la red interna

Por medio de la lista de control de acceso restringimos o filtramos el tráfico de la red y acciones de administración o configuración. De esta forma aumentamos la seguridad, determinan que datos traficar en la interface del switch.

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

cundinamarca(config-if)#access-list **131** deny ip 172.31.1.64 0.0.0.63 209.165.220.0 0.0.0.255
cundinamarca(config)#access-list 131 permit ip any any
cundinamarca(config)#int f0/0.20
cundinamarca(config-subif)#ip access-group **131** in
cundinamarca(config-subif)#

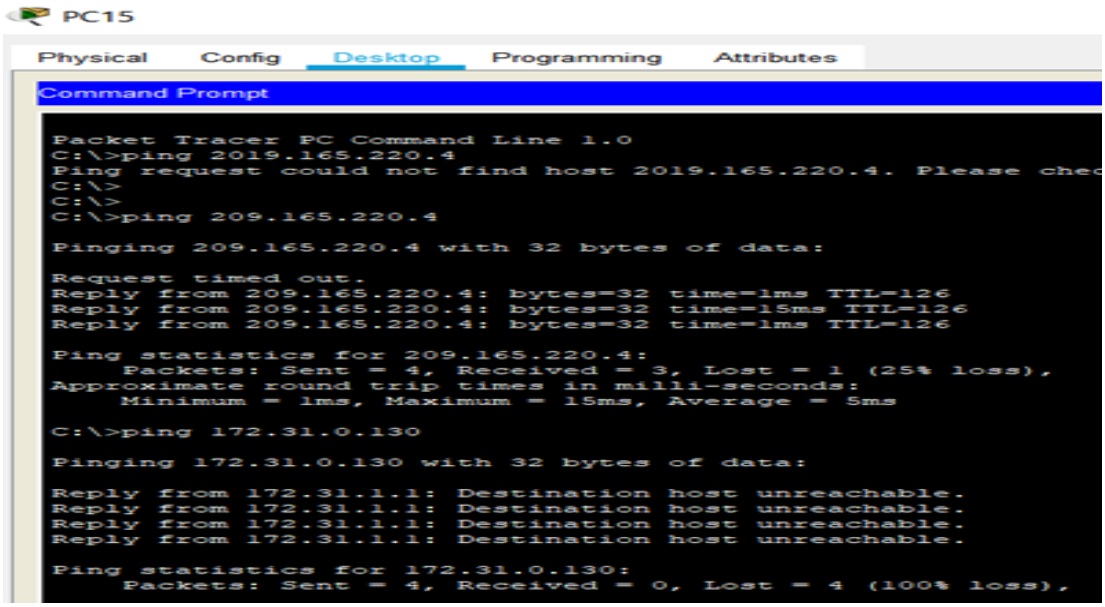
Figura 34. Verificación Parte 5 listas de control de acceso Ítem A



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

cundinamarca(config-subif)#access-list **132** permit ip 172.31.1.0 0.0.0.63 209.165.220.0 0.0.0.255
cundinamarca(config)#access-list **132** deny ip any any
cundinamarca(config)#int f0/0.30
cundinamarca(config-subif)#ip access-group **132** in
cundinamarca(config-subif)#

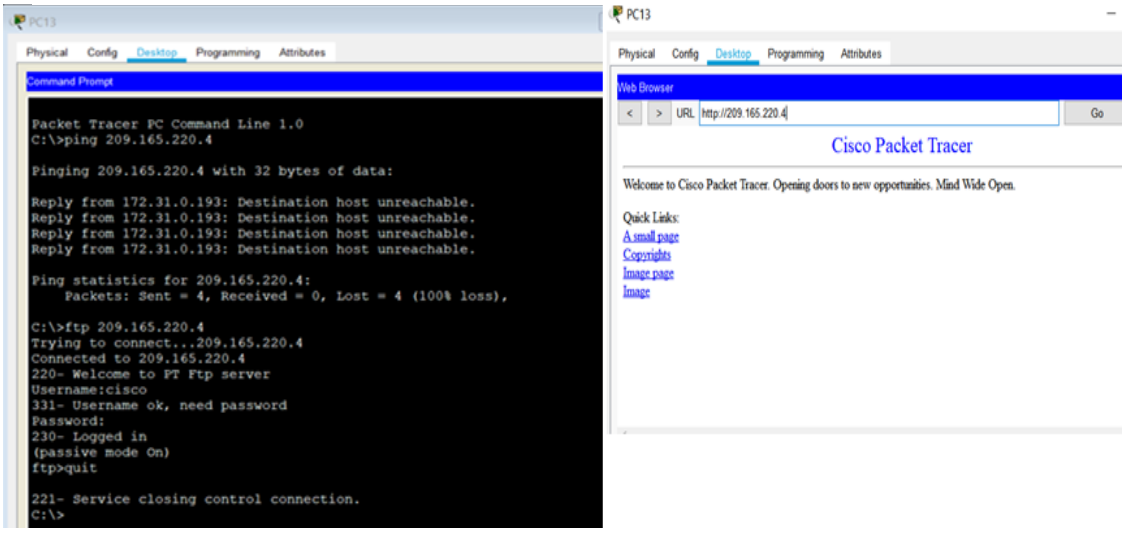
Figura 35. Verificación Parte 5 listas de control de acceso Ítem B



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

tunja(config)#access-list **131** permit tcp 172.31.0.192 0.0.0.63 209.165.220.0 0.0.0.255 eq www
tunja(config)#access-list **131** permit tcp 172.31.0.192 0.0.0.63 209.165.220.0 0.0.0.255 eq ftp
tunja(config)#int f0/0.30
tunja(config-subif)#ip access-group **131** in
tunja(config-subif)#

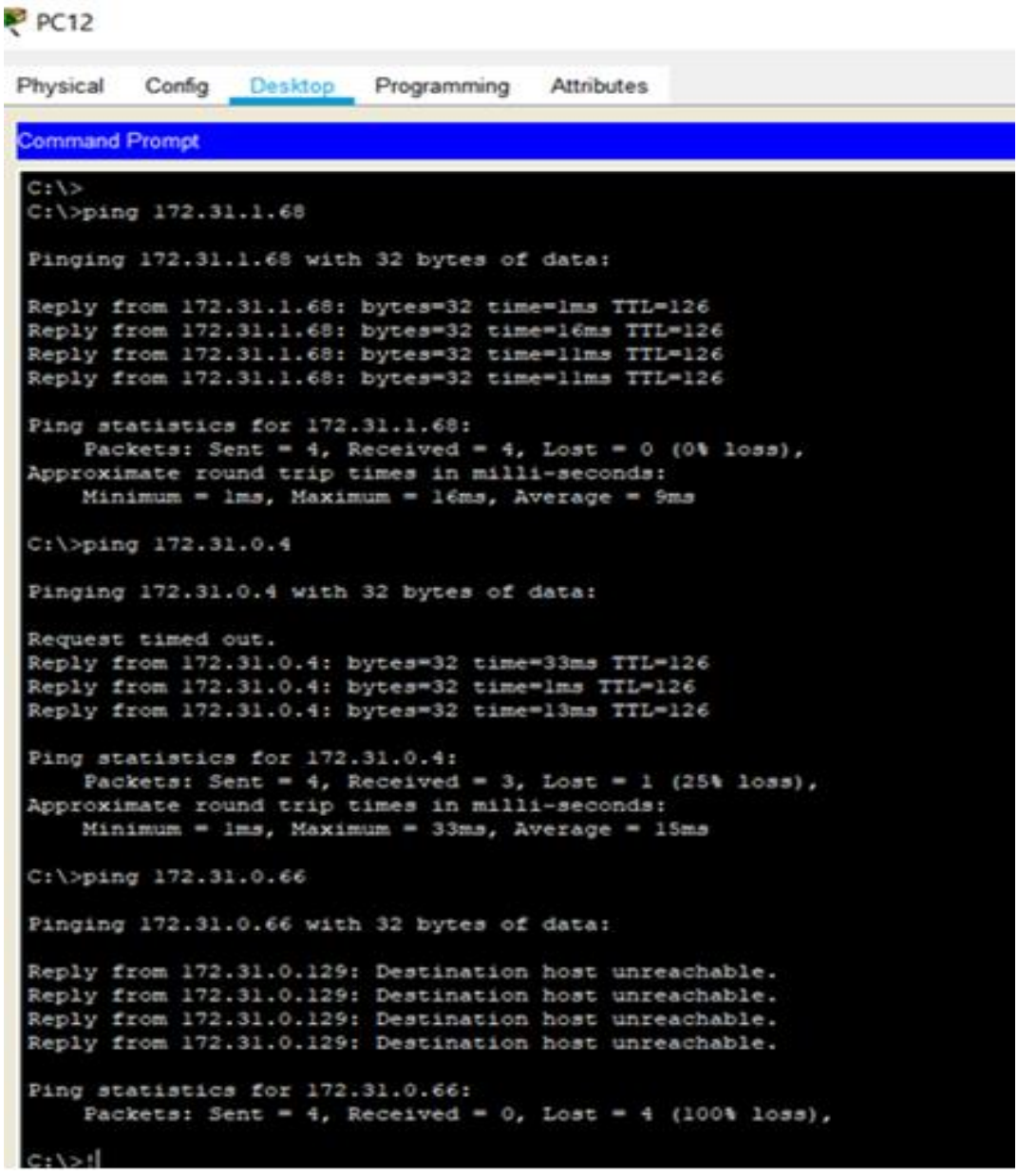
Figura 36. Verificación Parte 5 listas de control de acceso Ítem C



d. 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 **132** permit ip 172.31.0.128 0.0.0.63 172.31.1.64 0.0.0.63
tunja(config)#access-list **132** 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 **132** in
tunja(config-subif)#

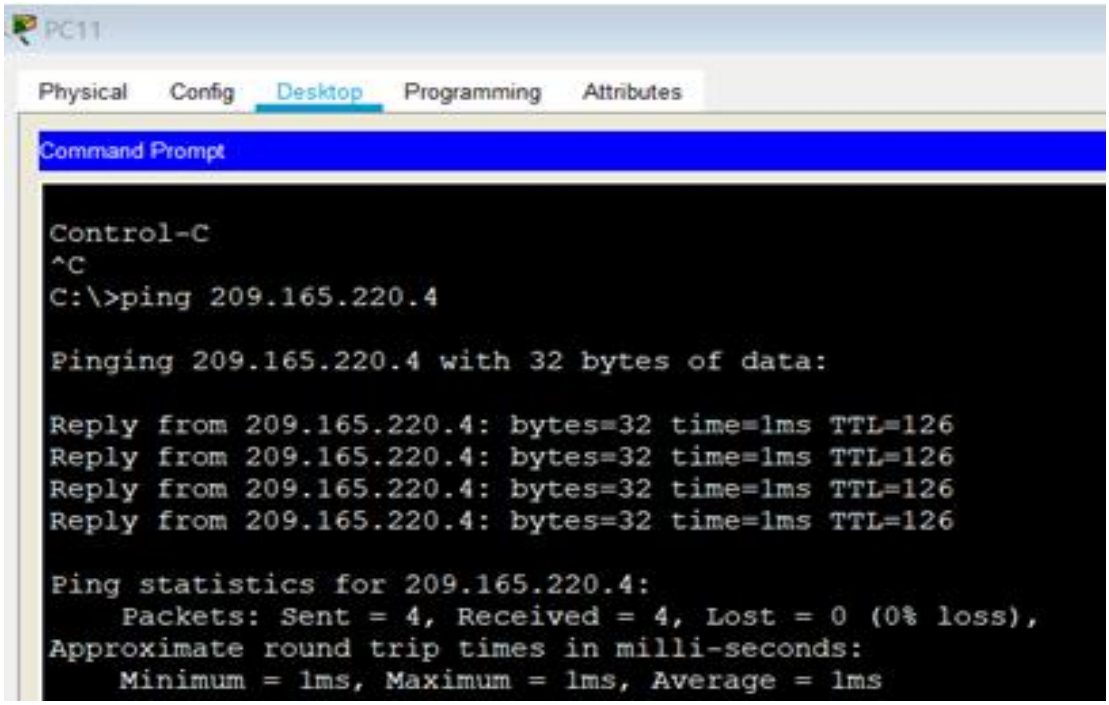
Figura 37. Verificación Parte 5 listas de control de acceso Ítem D



e. Los hosts de VLAN 30 de Bucaramanga acceden a internet y a cualquier equipo de VLAN 10.

bucaramanga(config)#access-list **131** 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 **131** in
bucaramanga(config-subif)#

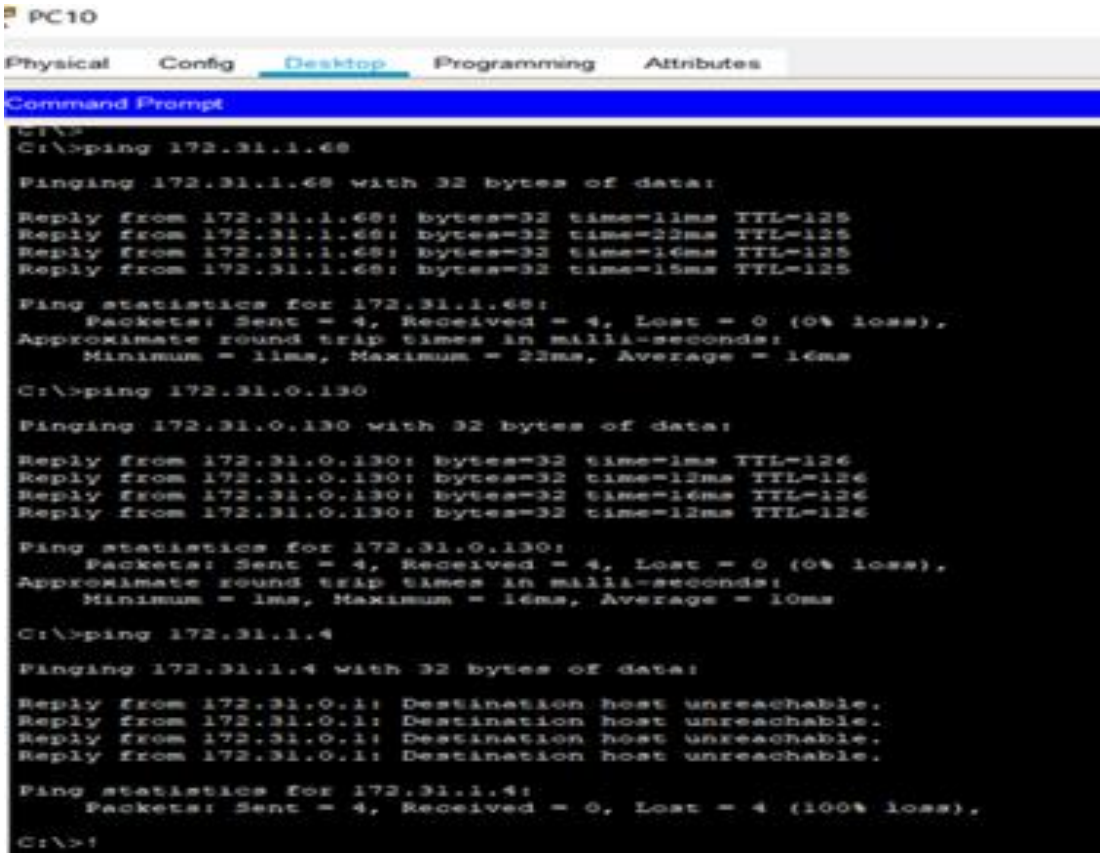
Figura 38. Verificación Parte 5 listas de control de acceso Ítem E



f. 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 **132** permit ip 172.31.0.0 0.0.0.63 172.31.1.64 0.0.0.63
bucaramanga(config)#access-list **132** 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 **132** in
bucaramanga(config-subif)#

Figura 39. Verificación Parte 5 listas de control de acceso Ítem F



g. Los hosts de una VLAN no pueden acceder a los de otra VLAN en una ciudad.
Configuración Bucaramanga

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)#

Configuración Tunja

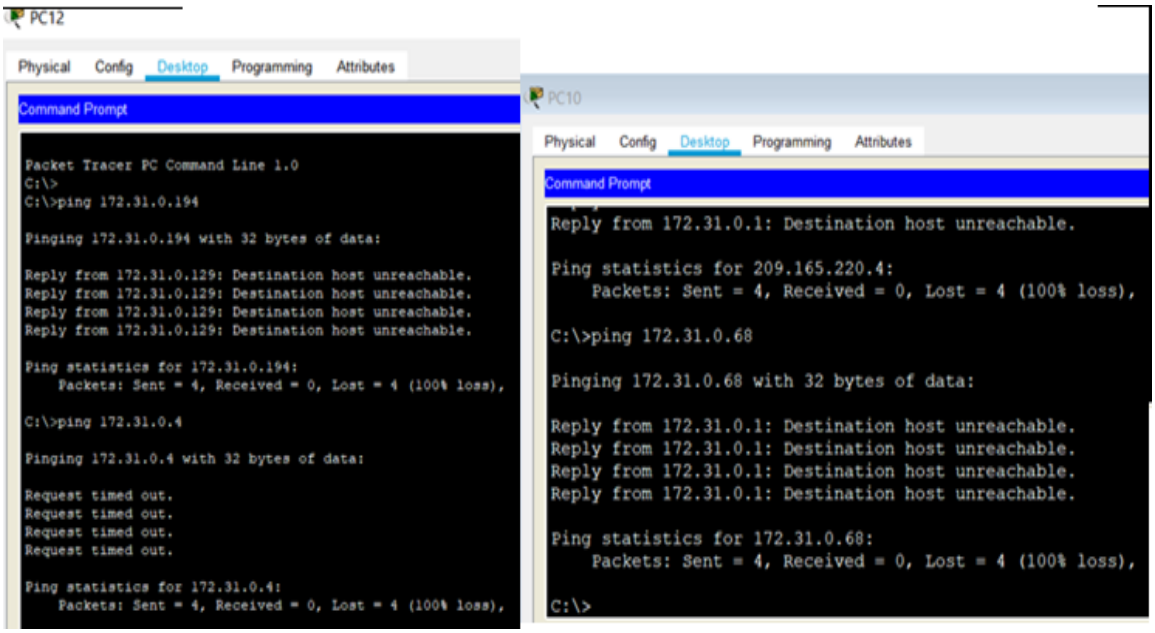
tunja(config)#access-list **123** deny ip 172.3.2.8 0.0.0.7 172.31.0.128 0.0.0.63
tunja(config)#access-list **123** deny ip 172.3.0.192 0.0.0.63 172.31.0.128 0.0.0.63

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)#

Configuración Cundinamarca

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
cundinamarca(config-subif)#

Figura 40. Verificación Parte 5 listas de control de acceso Ítem G



h. Solo los hosts de las VLAN administrativas y de la VLAN de servidores tienen accedo a los routers e internet.

Configuración sede Bucaramanga

```
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)#
```

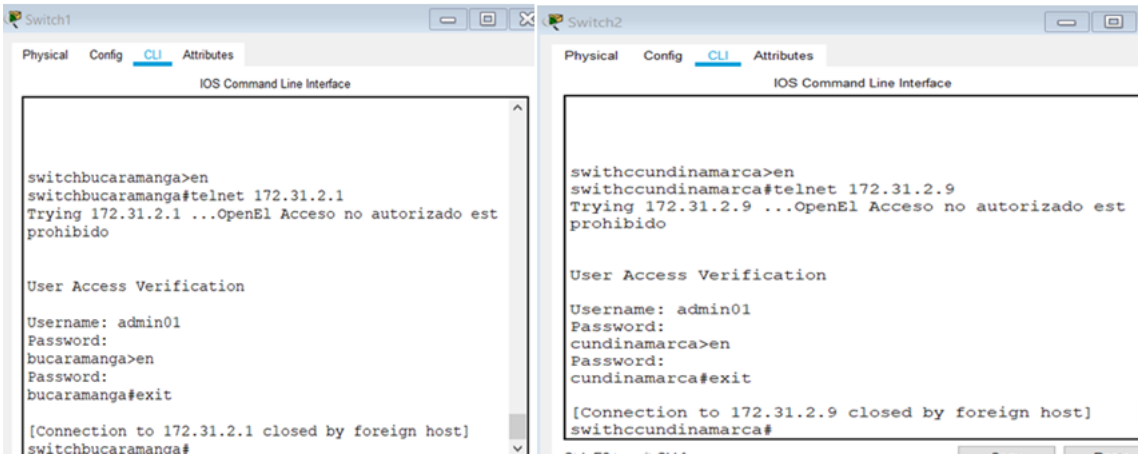
Configuración sede Tunja

```
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)#
```

Configuración sede Cundinamarca

```
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
cundinamarca(config-line)#
```

Figura 41. Verificación Parte 5 listas de control de acceso Ítem H



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

Se utilizo en la configuración de la red el VLSM con la dirección IP base 172.31.0.0 /18 para el direccionamiento, haciendo la máscara subred de diferentes tamaños

CONCLUSIONES

El uso de protocolos de enrutamiento dinámico nos permite el aprendizaje rápido de la topología de red por la cual estemos pasando y la cantidad de saltos posibles para alcanzar un destino.

Como elemento de seguridad el uso de VLAN nos permite la segmentación adecuada de una red limitando el acceso a los recursos que sean absolutamente necesarios y logrando una división basada en departamentos, servicios o localidades.

Se debe poseer especial cuidado al momento de implementar un esquema de red usando el protocolo VTP ya que, al ser el aprendizaje de VLAN dinámico, la introducción de un nuevo Switch con un número de revisión más alto puede afectar el funcionamiento y generar indisponibilidad.

En un ambiente empresarial de alta envergadura donde la disponibilidad de los servicios posee una alta demanda se hace necesaria la implementación de soluciones redundantes donde soluciones como HSRP para los Router y EtherChannel aparecen como alternativas eficientes para dar solución a esta necesidad.

BIBLIOGRAFIA

Configuring a LAN with DHCP and VLANs
Cisco. (2007, 26 septiembre). Configuring a LAN with DHCP and VLANs [Support]. Recuperado 19 julio, 2019, de https://www.cisco.com/en/US/docs/routers/access/800/850/software/configuration/guide/dhcpvlan.html

Lucas, M. (2009). Cisco Routers for the Desperate : Router and Switch Management, the Easy Way. San Francisco: No Starch Press. Recuperado de: http://bibliotecavirtual.unad.edu.co:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=e000xww&AN=440032&lang=es&site=ehost-live

Odom, W. (2013). CISCO Press (Ed). CCNA ICND2 Official Exam Certification Guide. Recuperado de: http://een.iust.ac.ir/profs/Beheshti/Computer%20networking/Auxilary%20materials/Cisco-ICND2.pdf

Packer Tracer
https://www.netacad.com/#/resource/lcms/cnams_site/english/generic_site_areas/library/index_role.htmlCCNA1Exploration

Cisco IOS LAN Switching Command Reference
Cisco. (2013, 7 octubre). Cisco IOS LAN Switching Command Reference - show vlan through spanning-tree vlan [Support]. Recuperado 19 julio, 2019, de https://www.cisco.com/c/en/us/td/docs/ios/lanswitch/command/reference/lsw_book/lsw_s2.html

IP Addressing
Cisco. (2017a, 15 julio). IP Addressing: DHCP Configuration Guide, Cisco IOS Release 12.4 - Configuring the Cisco IOS DHCP Client [Support]. Recuperado 19 julio, 2019, de https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_dhcp/configuration/12-4/dhcp-12-4-book/config-dhcp-client.html

CISCO. (2014). SubNetting. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN50ES/module9/index.html#9.0.1.1