DIPLOMADO DE PROFUNDIZACIÓN CISCO PRUEBA DE HABILIDADES PRÁCTICAS CCNP

JOSE ANDRÉS MUÑOZ SUANCHA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI

INGENIERÍA DE SISTEMAS

BOGOTÁ D.C.

2020

DIPLOMADO DE PROFUNDIZACIÓN CISCO PRUEBA DE HABILIDADES PRÁCTICAS CCNP

JOSE ANDRÉS MUÑOZ SUANCHA

Diplomado de opción de grado presentado para optar el título de
INGENIERO DE SISTEMAS

DIRECTOR:

MSc. JUAN CARLOS VESGA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI

INGENIERÍA DE SISTEMAS

BOGOTÁ D.C.

2020

NOTA DE ACEPTACIÓN

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

Bogotá D.C. 31 de enero de 2020

AGRADECIMIENTOS

El presente trabajo, es el resultado de mucho esfuerzo y dedicación durante el desarrollo de toda mi carrera de ingeniería de sistemas. No fue fácil, y pude lograr llegar hasta aquí, por el apoyo incondicional de mi familia y de todo el grupo de docente; a ellos dedico este logro y en especial a DIOS, sin el nada es posible.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

ANCHO DE BANDA: el ancho de banda se mide como la cantidad de datos que se pueden transferir entre dos puntos de una red en un tiempo específico. Normalmente, el ancho de banda se mide en bits por segundo (bps) y se expresa como una tasa de bits.

CCNP: la Certificación Cisco es un plan de capacitación en tecnología de redes informáticas que la empresa Cisco ofrece. Se divide en tres niveles, de menor a mayor complejidad: Cisco Certified Network Associate, Cisco Certified Network Professional y Cisco Certified Internetwork Expert, más conocidos por sus siglas: CCNA.

DLS: digital Subscriber Line (Línea Digital de Suscripción) es una forma de conectarse a Internet y transmitir datos a través de líneas telefónicas regulares. Sin embargo, al igual que un módem de cable, un circuito DSL es mucho más rápido que una conexión telefónica normal, a pesar de que los cables que utiliza son de cobre como una línea telefónica. La velocidad DSL se basa en la distancia entre el cliente y la oficina central de teléfono.

DIRECCIÓN IP: es un conjunto de números que identifica, de manera lógica y jerárquica, a una Interfaz en red (elemento de comunicación/conexión) de un dispositivo (computadora, tableta, portátil, teléfono inteligente) que utilice el protocolo o (Internet Protocol), que corresponde al nivel de red del modelo TCP/IP.

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

INTERFAZ: es una conexión entre dos máquinas de cualquier tipo, a las cuales les brinda un soporte para la comunicación a diferentes estratos. Es posible entender la interfaz como un espacio (el lugar donde se desarrolla la interacción y el intercambio), instrumento (a modo de extensión del cuerpo humano.

NETWORKING: el término networking no forma parte del diccionario de la Real Academia Española (RAE). Se trata de un anglicismo que, de todos modos, se utiliza con frecuencia en nuestro idioma para aludir al establecimiento de vínculos profesionales y empresariales con el objetivo de favorecer el desarrollo de negocios y las oportunidades comerciales.

PACKET TRACER: herramienta de aprendizaje y simulación de redes interactiva para los instructores y alumnos de Cisco CCNA. Esta herramienta

les permite a los usuarios crear topologías de red, configurar dispositivos, insertar paquetes y simular una red con múltiples representaciones visuales.

ROUTER: dispositivo de hardware que permite la interconexión de ordenadores en red. El router o enrutador es un dispositivo que opera en capa tres de nivel de 3. Así, permite que varias redes u ordenadores se conecten entre sí.

TOPOLOGÍA DE RED: Arreglo físico o lógico en el cual los dispositivos o nodos de una red (computadoras, impresoras, servidores, hubs, switches, enrutadores, etc.) se interconectan entre sí sobre un medio de comunicación.

VLAN: es un acrónimo que deriva de una expresión inglesa: virtual LAN. Esa expresión, por su parte, alude a una sigla ya que LAN significa Local Área Network. De este modo, podemos afirmar que la idea de VLAN refiere a una red de área local (lo que conocemos como LAN) de carácter virtual.

RESUMEN

Se presenta por medio del siguiente documento las soluciones de dos escenarios de habilidades practicas del Diplomado de Cisco, este diplomado está orientado a profundizar en el currículo oficial de Cisco Networking Academy®, diseñado para ser tomado como opción de grado en el programa de Ingeniería de sistemas ofertado por la universidad nacional abierta y a distancia UNAD.

Esta última actividad brinda el desarrollo y aumento en las habilidades para la aplicación de tecnologías de la información y la comunicación basadas en el protocolo IP. Donde se pretende que como estudiantes demostremos lo aprendido durante todo el curso. Para cada uno de los escenarios se debe describir el paso a paso de cada punto realizado y además digitar el código de configuración aplicado. El informe está acompañado de las respectivas evidencias de configuración de los dispositivos (Packet Tracer ó GNS3), las cuales generarán veracidad al trabajo realizado.

Palabras claves: Cico Networking, Protocolo IP, Tecnologías de la información

ABSTRACT

The following document presents the solutions of two scenarios of practical skills of the Cisco Diploma, this diploma is aimed at deepening the official Cisco Networking Academy® curriculum, designed to be taken as a degree option in the Engineering Program of systems offered by the national university open and distance UNAD.

This last activity provides the development and increase in the skills for the application of information and communication technologies based on the IP protocol. Where it is intended that as students we demonstrate what they have learned throughout the course. For each of the scenarios, you must describe the step by step of each point made and also enter the configuration code applied. The report is accompanied by the respective evidence of configuration of the devices (Packet Tracer or GNS3), which will generate veracity to the work done.

Keywords: Cico Networking, IP Protocol, Information Technology

INTRODUCCIÓN

El presente documento tiene como objetivo solucionar los dos retos de las habilidades prácticas, dados como evaluación final del diplomado de cisco opción de grado del programa de ingeniería de sistemas; se busca poner a prueba las habilidades y capacidades por medio de las prácticas respecto a los aprendido en lo visto en el diplomado.

Se puede por medio de los retos fusionar los cursos de CCNA y CCNP de CISCO, donde se muestra la implementación de redes de datos con la ayuda de dispositivos activos router y switch simulados en herramientas como Packet Tracer y GNS3

Para finalizar mostraremos las conclusiones de lo aprendido y la experiencia que fue el desarrollo de todo el diplomando, enfatizando en la última experiencia de la solución de estos dos retos.

DESARROLLO

1. ESCENARIO 1

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

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. Escenario 1

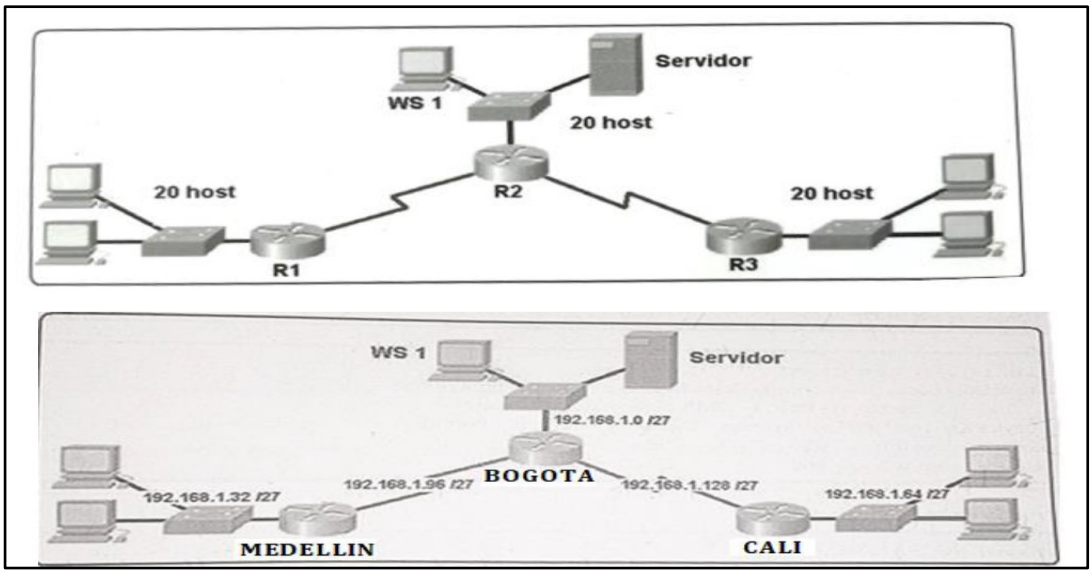
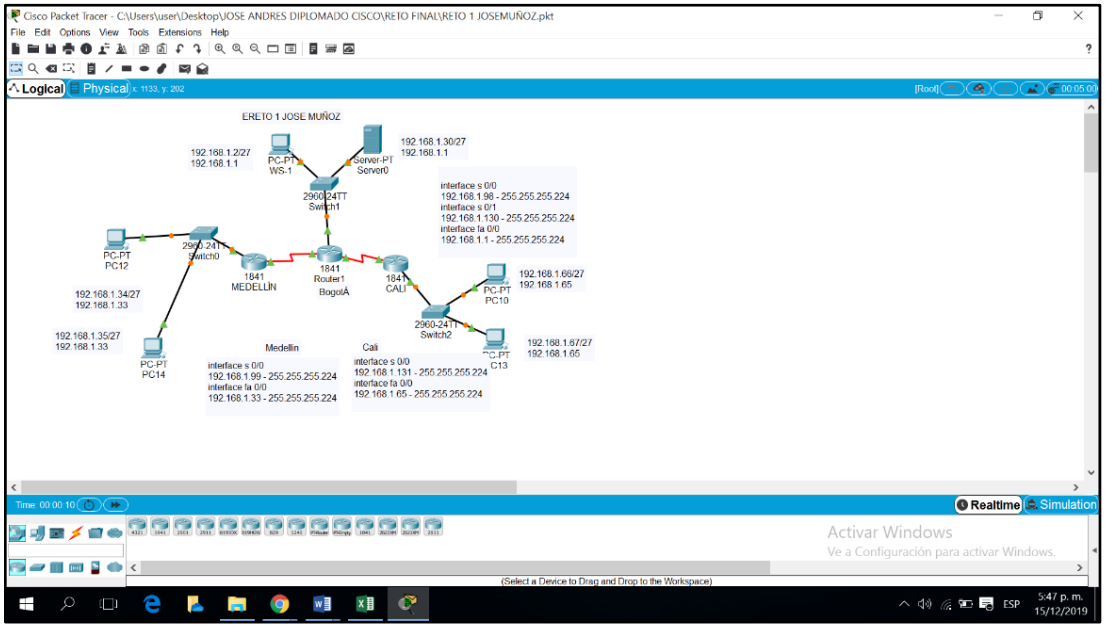


Figura 2. Ilustración Reto 1 solucionado



Se adjunta código y pantallazos con veracidad del código.

Como trabajo inicial se debe realizar lo siguiente.

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

Realizar la conexión 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 creciemiento futuro de la red corporativa.

b. Asignar una dirección IP a la red.

Se debe configurar los parámetros básicos en cada uno de los dispotiviso, entre ellos lo que son el NOMBRE, las contraseñas, tal como lo maestro a continuación.

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

Router(config)#hostname medellin

medellin(config)#no ip domain-lookup

medellin(config)#service password-encryption

medellin(config)#banner motd $El Acceso no autorizado est prohibido$

medellin(config)#enable secret class1

medellin(config)#line console 0

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

Router(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
```

Se hace de igual forma en los switch

```
Switch(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

Switch#conf term
switchmedellin(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

Switch(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)#
Se debe 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.

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.

Tabla 1. Direcciones IP

sucursar	**Dirección ip**
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 de Ip en interfaz Serial 0/0	192.168.1.99	192.168.1.98	192.168.1.231
Dirección de Ip en interfaz Serial 0/1		192.168.1.130	
Dirección de Ip en interfaz FA 0/0	192.168.1.33	192.168.1.1	192.168.1.65
Protocolo de enrutamiento	Eigrp	Eigrp	Eigrp
Sistema Autónomo	200	200	200
Afirmaciones de red	192.168.1.0	192.168.1.0	192.168.1.0

Procedemos a configurar cada una de las interfaces y además configuramos nuestro protocolo de enrutamiento.

Configuration 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 de los routers para comprobar las redes y sus rutas.

```
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

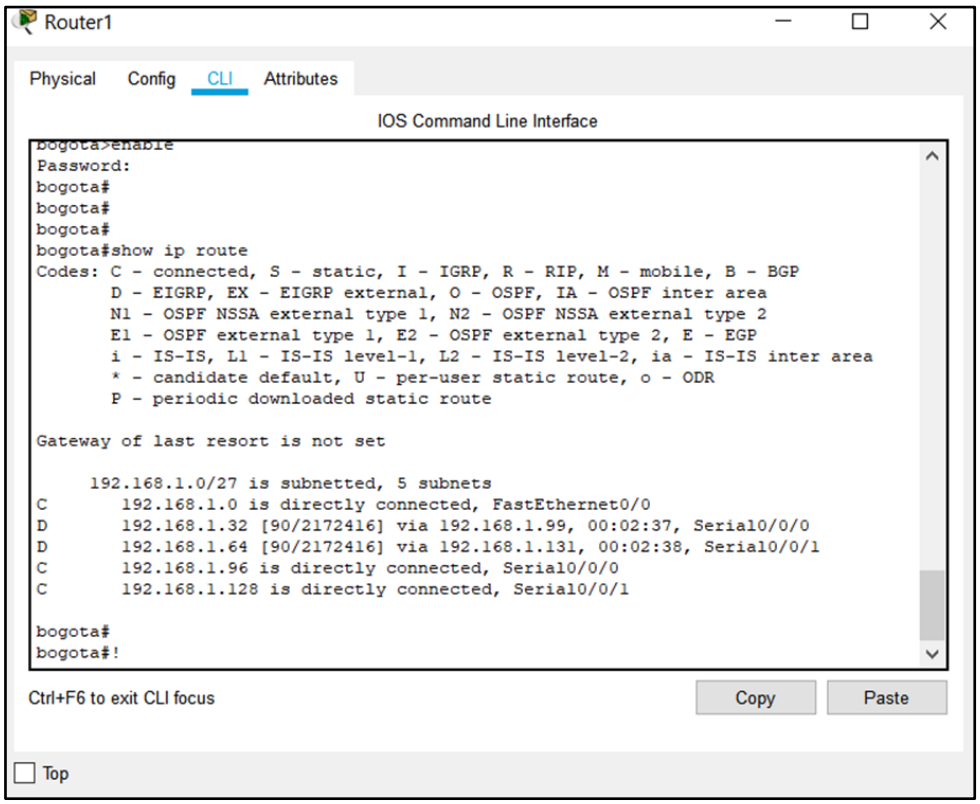
D 192.168.1.32 [90/2172416] via 192.168.1.99, 00:04:34, Serial0/0/0

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 3. Configuración reto 1 R1



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

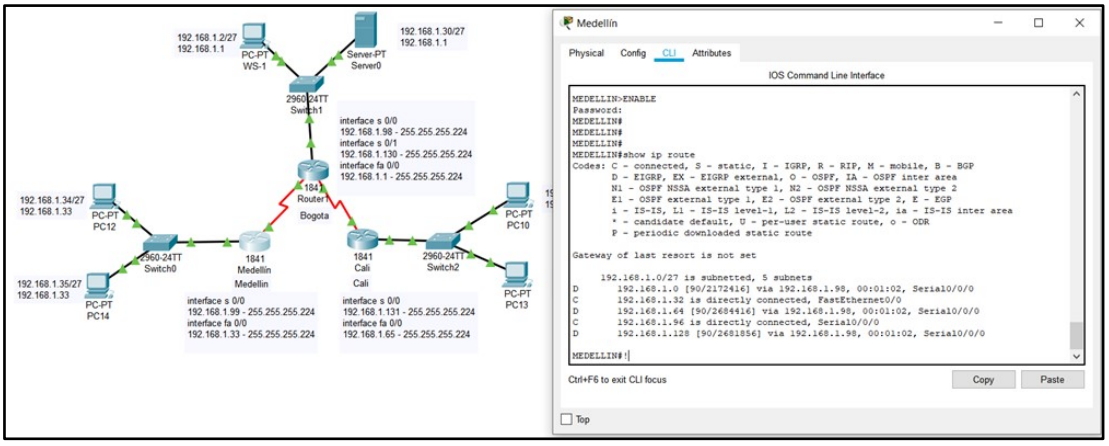
C 192.168.1.32 is directly connected, FastEthernet0/0

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 4. Configuración Sucursal Medellín



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

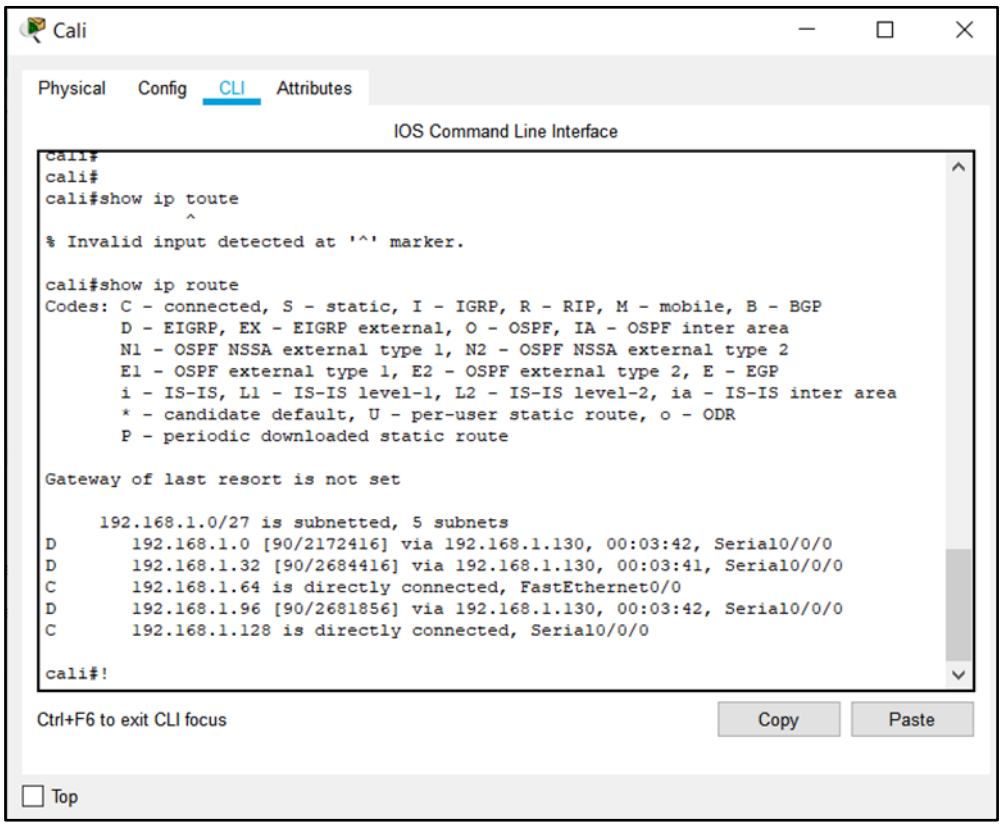
D 192.168.1.32 [90/2684416] via 192.168.1.130, 00:03:47, Serial0/0/0

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 5. Configuración Sucursal Cali



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

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

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

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 cuando el comando cdp.**

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 6. Diagnostico sucursal Bogotá

```
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          135            S       2960        Fas 0/1
cali         Ser 0/0/1        143            R       C1841       Ser 0/0/0
MEDELLIN     Ser 0/0/0        144            R       C1841       Ser 0/0/0
bogota#
bogota#
```

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 7. Diagnostico sucursal Medellín

```
MEDELLIN#
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          147            S       2960        Fas 0/1
bogota       Ser 0/0/0        148            R       C1841       Ser 0/0/0
MEDELLIN#
```

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

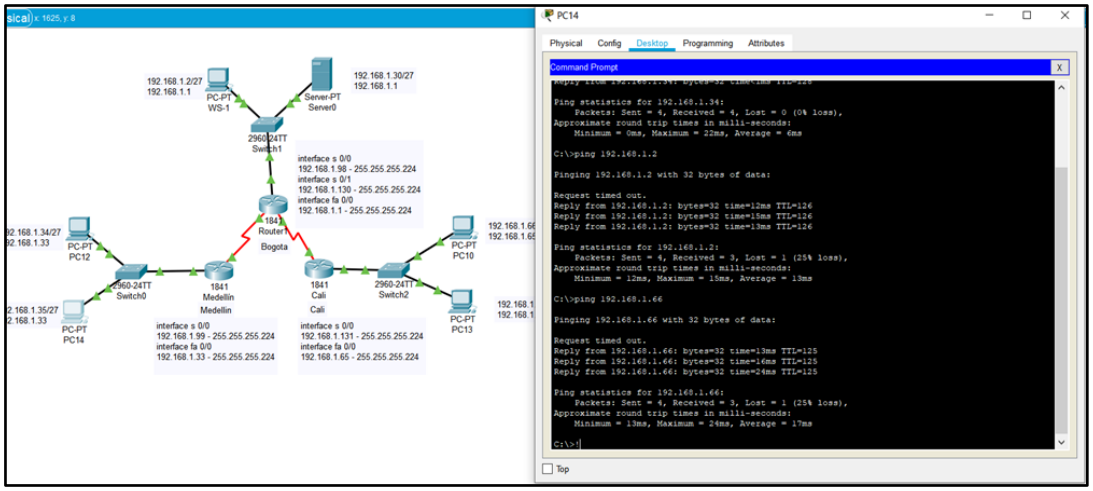
Device ID Local Intrfce Holdtme Capability Platform Port ID

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 8. Prueba de conectividad en cada tramo de la ruta usando Ping



Parte 3: Configuración de Enrutamiento.

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

Este paso ya estaba hecho antes, se realizó junto con la configuración de las interface de los routers, de todas maneras lo indico nuevamente:

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.

SHOW IP EIGRP NEIGHBORS

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 9. Verificación con los routers - Bogotá

```
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   192.168.1.131   Se0/0/1         13   00:16:13  40     1000  0   7
1   192.168.1.99    Se0/0/0         13   00:16:11  40     1000  0   7

bogota#
```

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

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

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

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

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.**

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 10. Comprobación tablas de enrutamientos- Bogotá

```
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, 00:24:50, Serial0/0/0
D       192.168.1.64 [90/2172416] via 192.168.1.131, 00:24:51, 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

bogota#
```

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

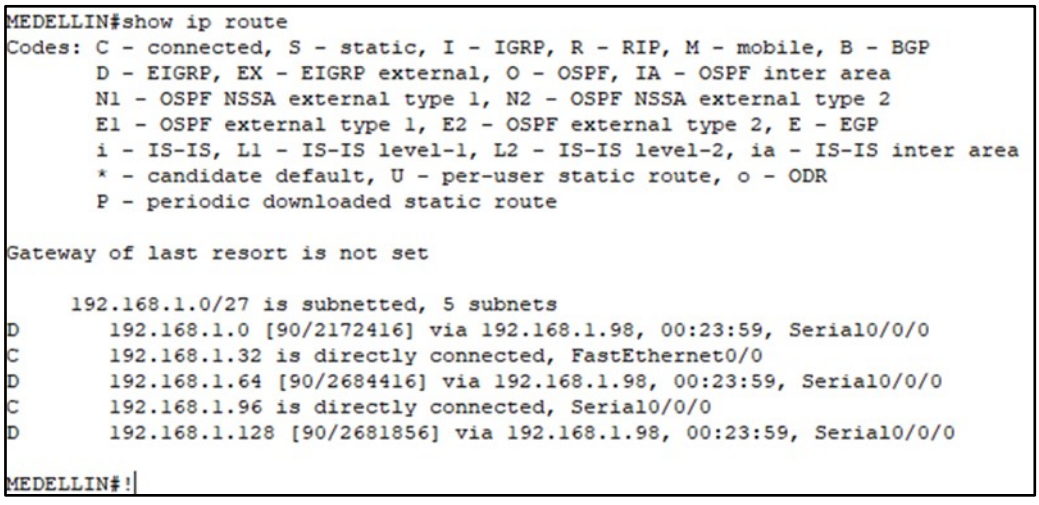
C 192.168.1.32 is directly connected, FastEthernet0/0

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 11. Comprobación tablas de enrutamientos- Medellín



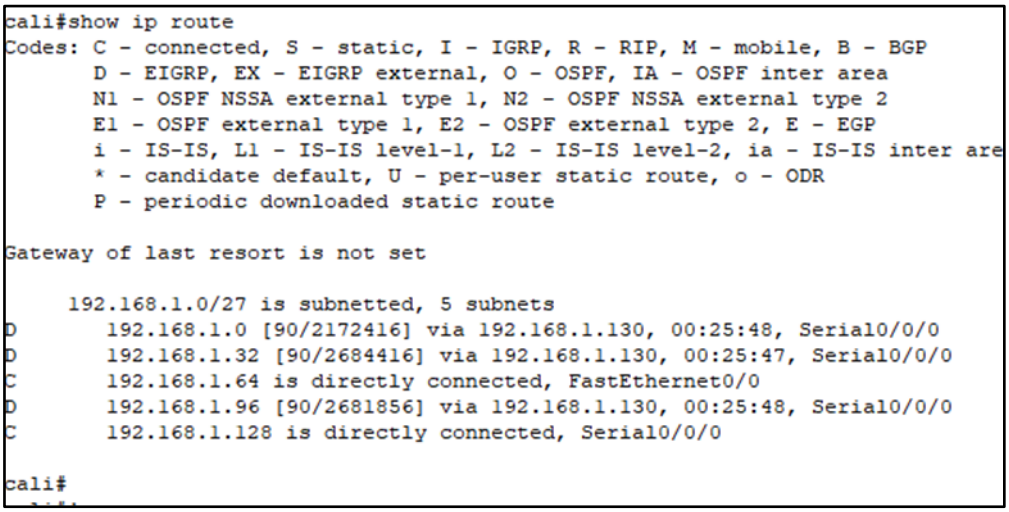
cali#show ip route

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

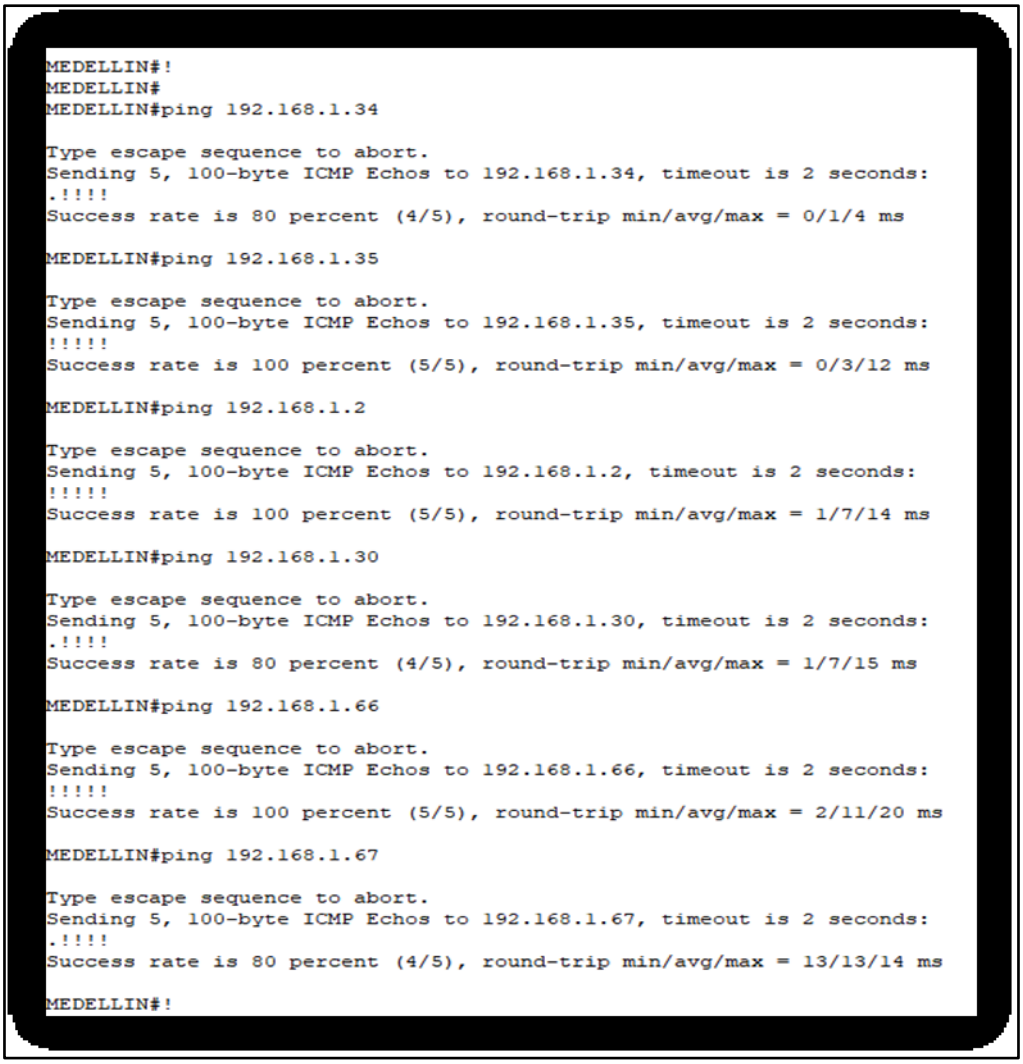
192.168.1.0/27 is subnetted, 5 subnets
D 192.168.1.0 [90/2172416] via 192.168.1.130, 00:03:47, Serial0/0/0
D 192.168.1.32 [90/2684416] via 192.168.1.130, 00:03:47, Serial0/0/0
C 192.168.1.64 is directly connected, FastEthernet0/0
D 192.168.1.96 [90/2681856] via 192.168.1.130, 00:03:47, Serial0/0/0
C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

Figura 12. Comprobación tablas de enrutamientos- Cali



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

Figura 13. Diagnóstico para comprobar que cada uno de los puntos de la red-Medellín



Verificamos que hay respuesta de las configuraciones

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.

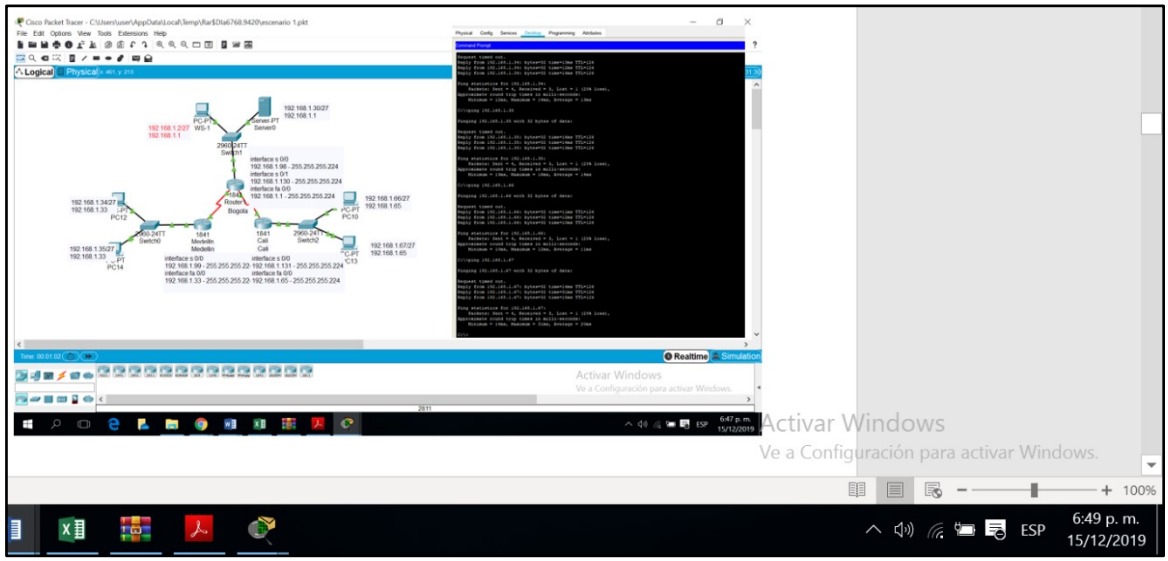
bogota(config)#access-list 131 permit ip host 192.168.1.30 any

bogota(config)#int f0/0

bogota(config-if)#ip access-group 131 in

bogota(config-if)#

Figura 14. Verificación equipo WS1 y el servidor se encuentran en la subred



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)#

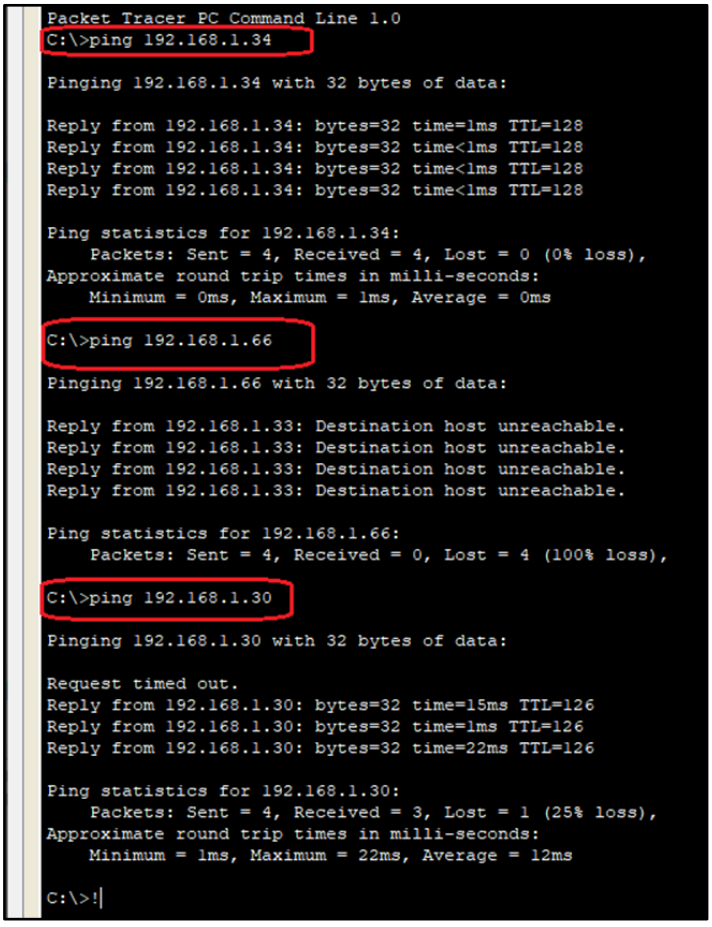
cali(config)#access-list 131 permit ip 192.168.1.64 0.0.0.31 host 192.168.1.30

cali(config)#int f0/0

cali(config-if)#ip access-group 131 in

cali(config-if)#

Figura 15. Verificación LAN de MEDELLÍN 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 e.

Tabla 3. Tabla de condiciones de prueba

	ORIGEN	DESTINO	RESULTADO
TELNET	Router MEDELLÍN	Router CALI	Éxito
	WS_1	Router BOGOTÁ	Falla
	Servidor	Router CALI	Éxito
	Servidor	Router MEDELLÍN	Éxito
TELNET	LAN del Router MEDELLIN	Router CALI	Falla
	LAN del Router CALI	Router CALI	Falla
	LAN del Router MEDELLIN	Router MEDELLÍN	Falla
	LAN del Router CALI	Router MEDELLÍN	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 MEDELLÍN	Éxito
	Servidor	LAN del Router CALI	Éxito
	Router CALI	LAN del Router MEDELLÍN	Falla
	Router MEDELLÍN	LAN del Router CALI	Falla

Figura 16. Comprobación configuración Medellín

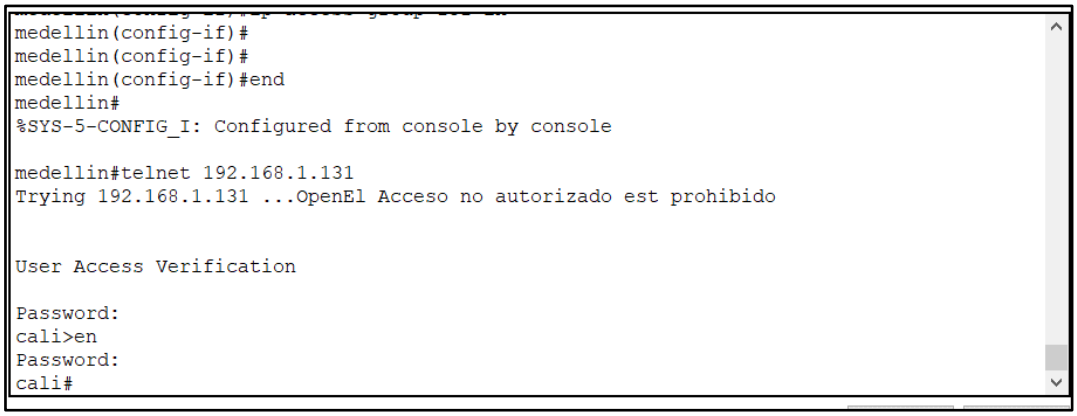


Figura 17. Verificación ws-1

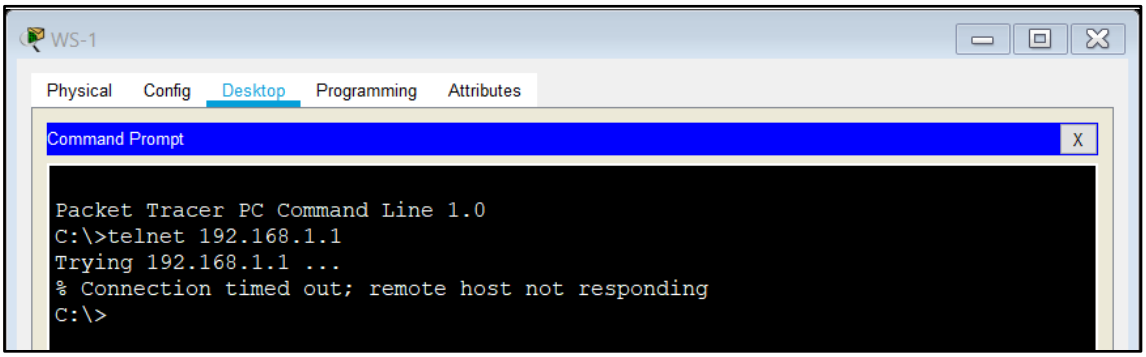


Figura 18. Verificación ip

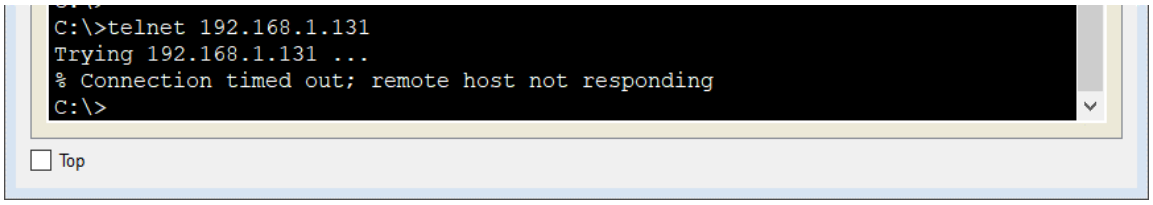


Figura 19. Ping pc 10

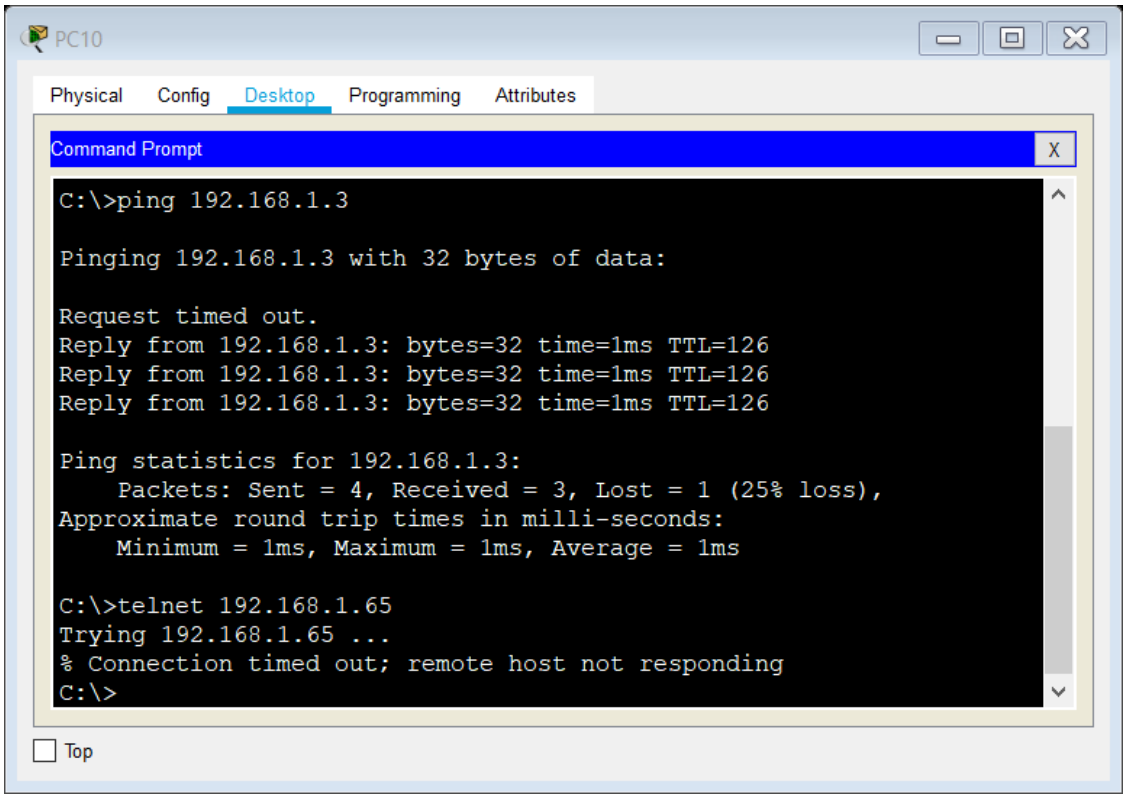


Figura 20. Ping pc 12

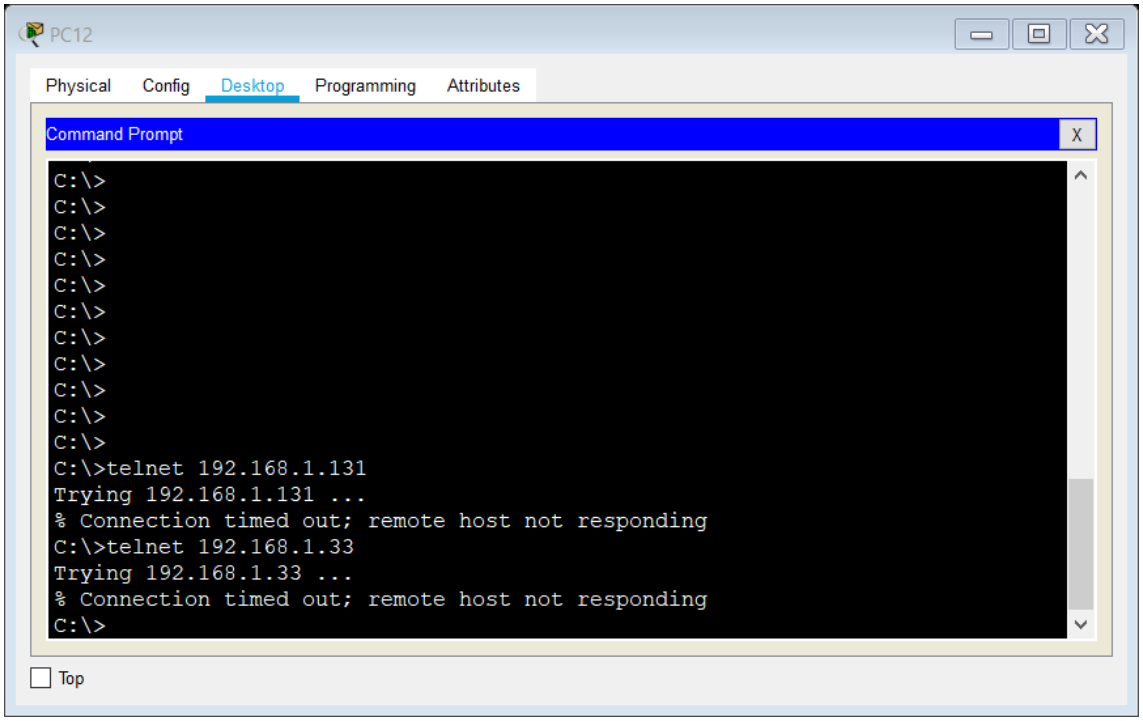


Figura 21 . Respuesta Ping pc 10

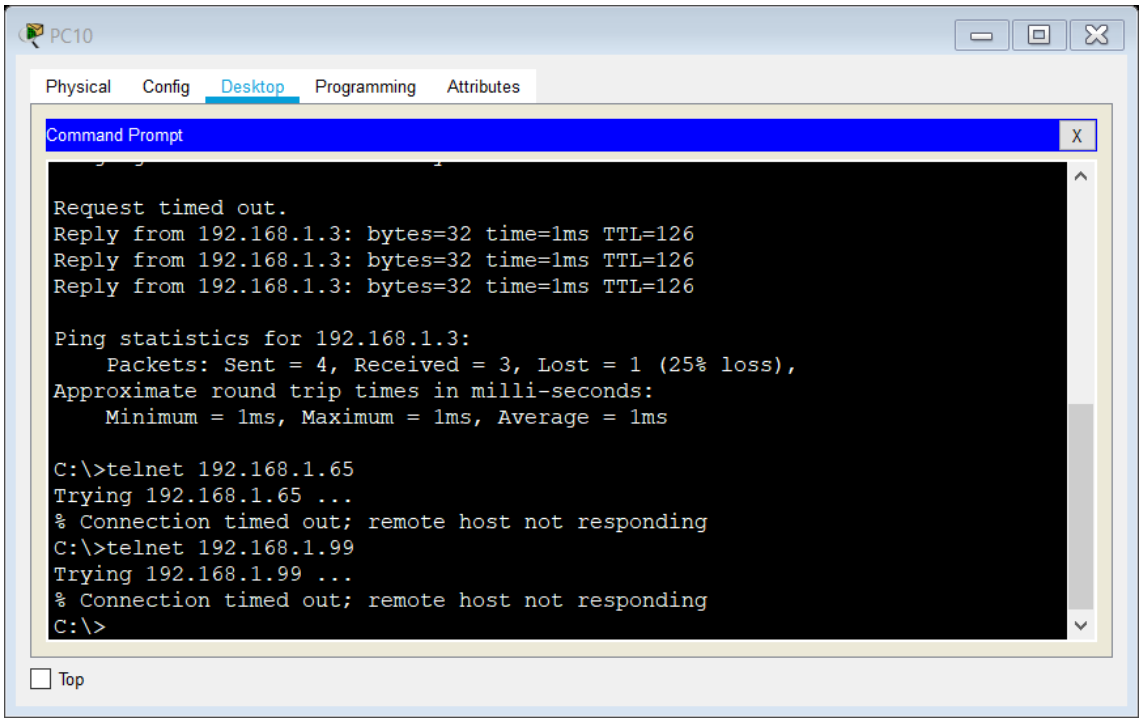


Figura 22. Tiempo de respuesta Ping pc 10

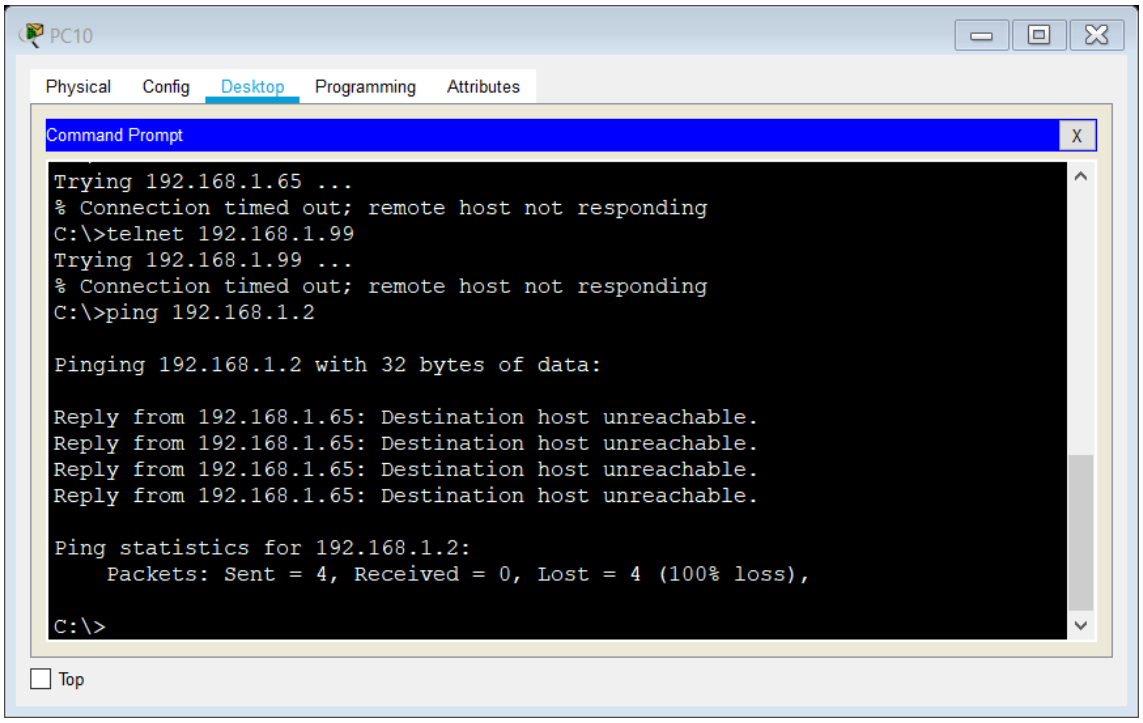


Figura 23. Tiempo de respuesta Ping pc 12

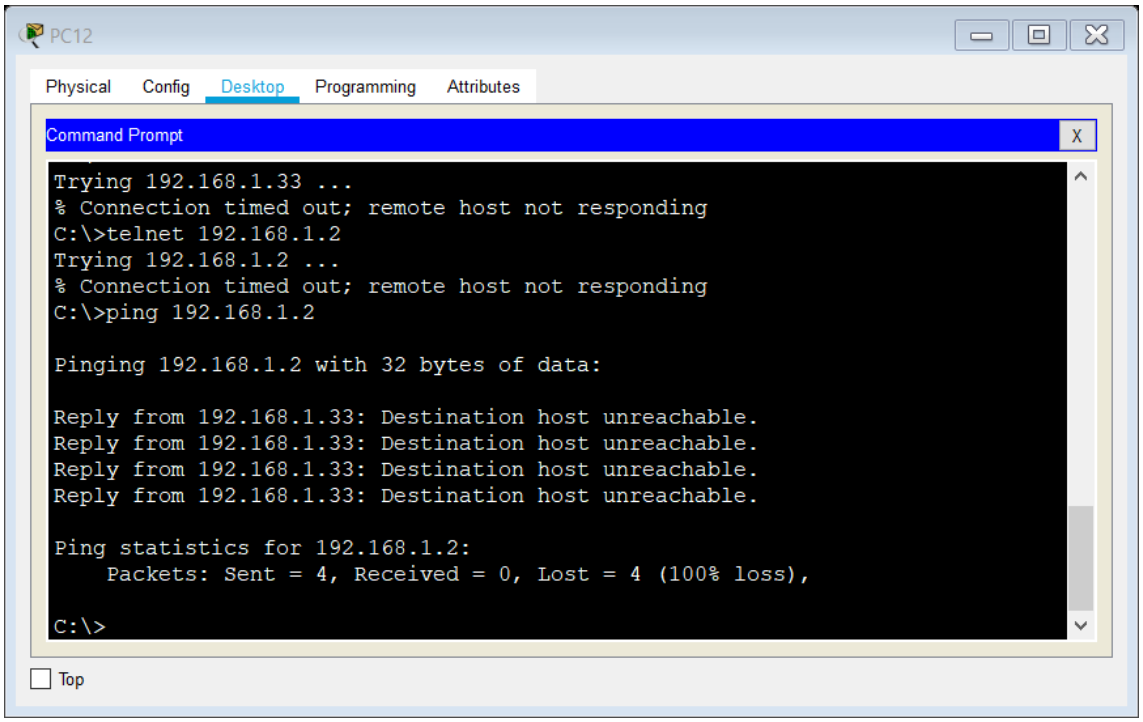


Figura 24. Verificación pc 12

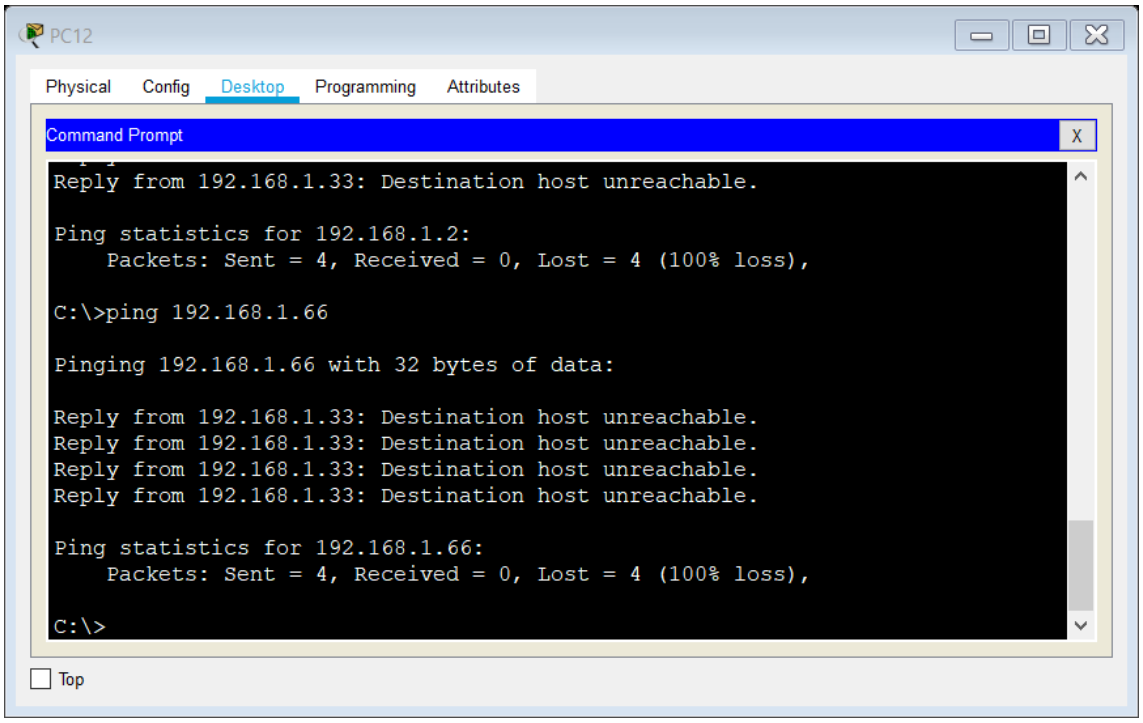


Figura 25. Verificación pc 10

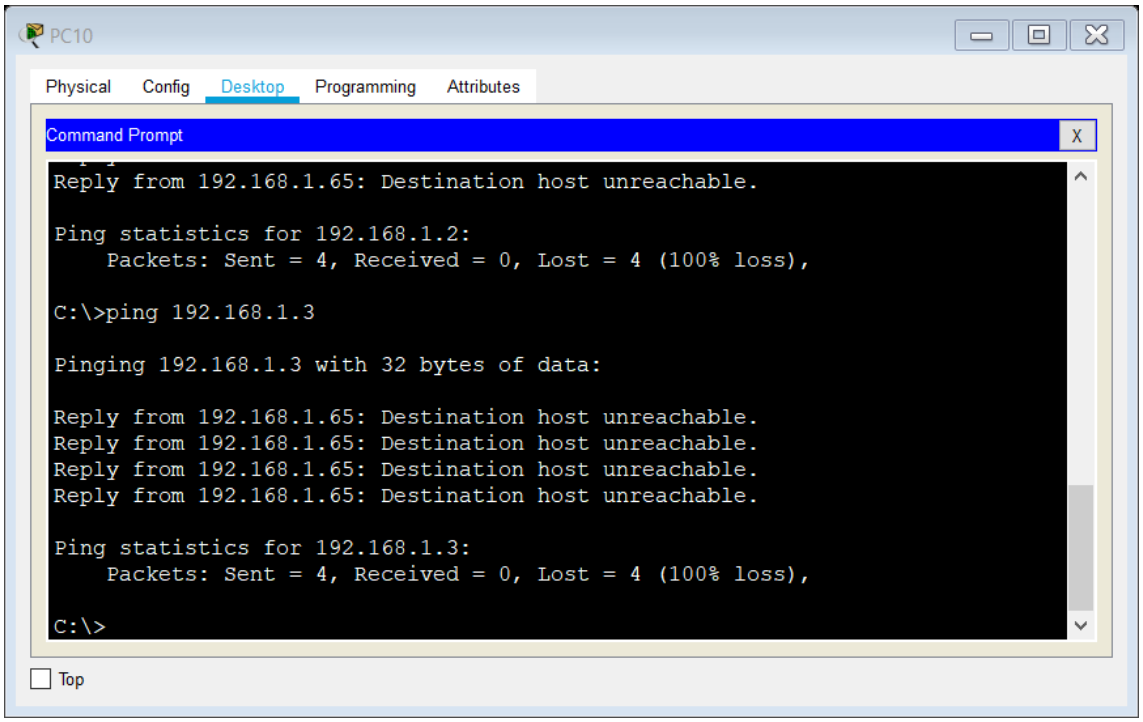


Figura 26 . Verificación destinatarios PC 12

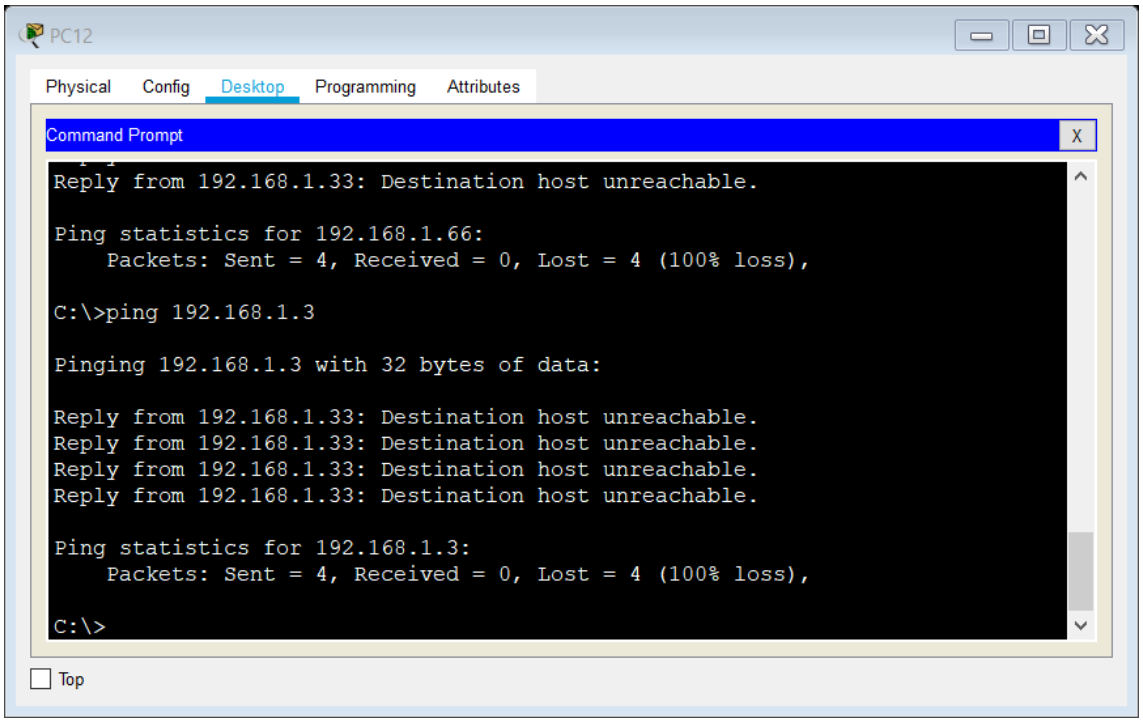


Figura 27. Server 0

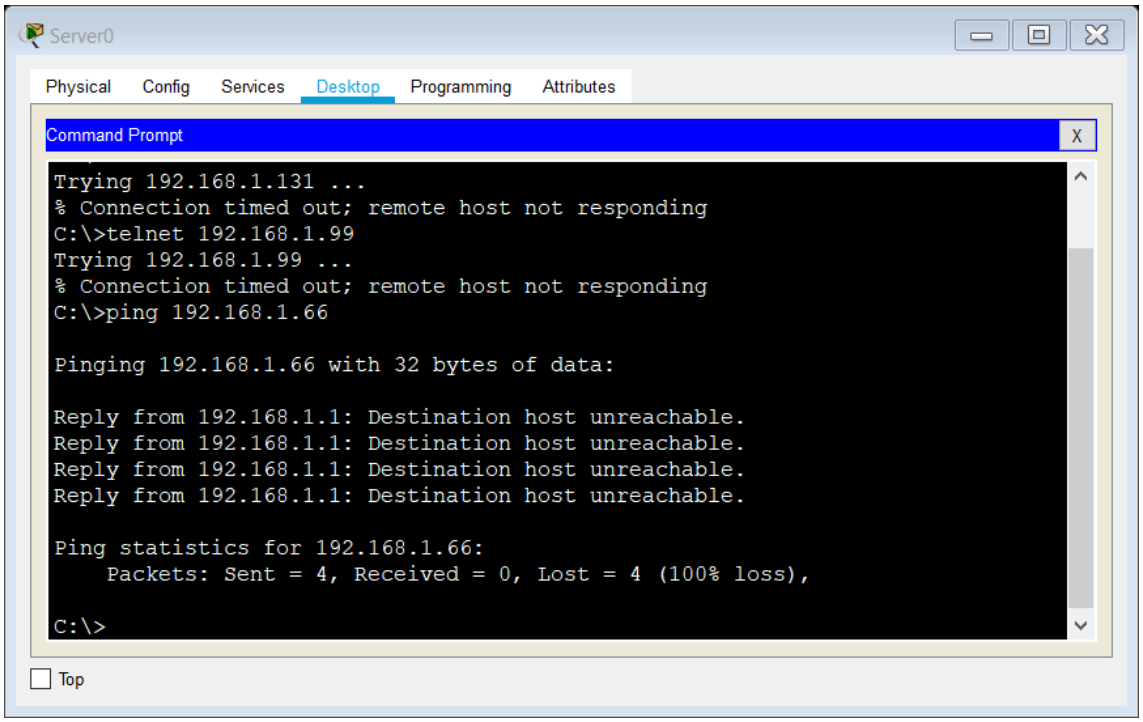


Figura 28. Acceso no autorizado prohibido

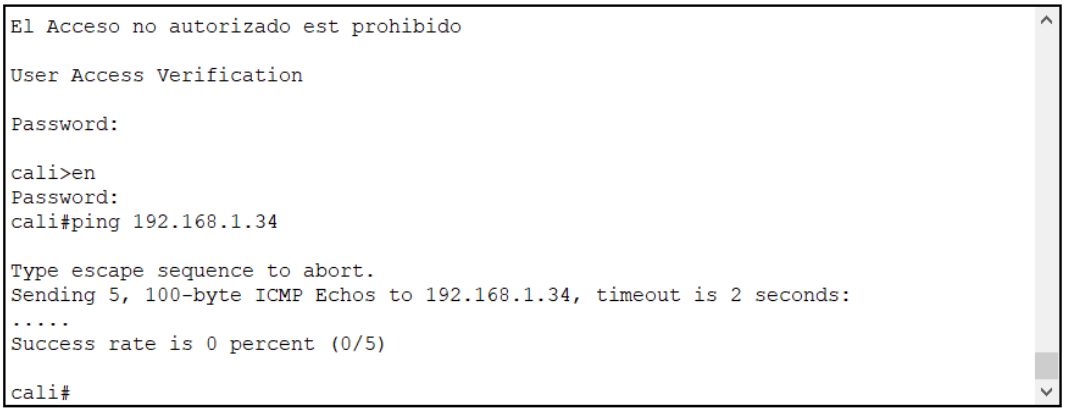
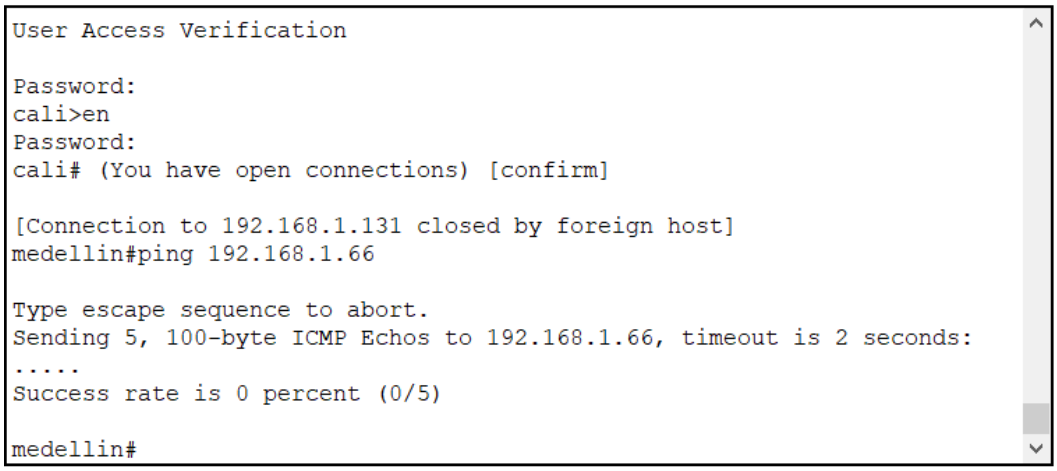


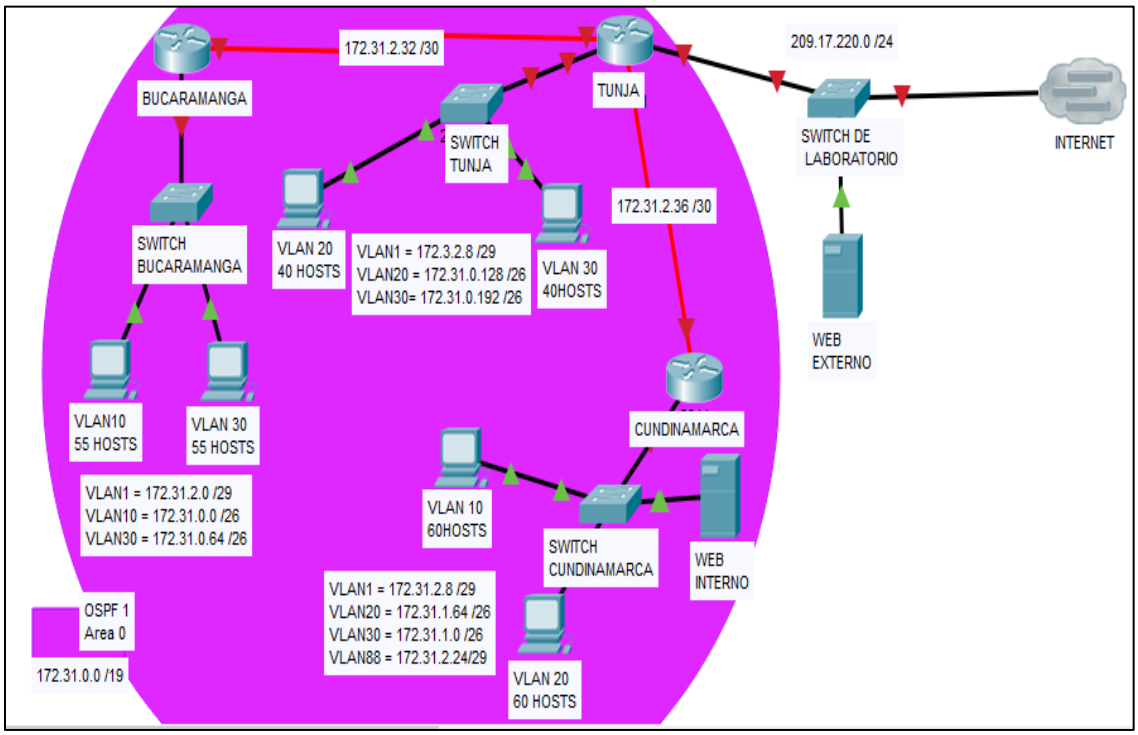
Figura 29. Verificación del acceso



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.

Figura 30. Escenario 2



Los siguientes son los requerimientos necesarios:

Todos los routers deberán tener los siguiente:
Configuración básica.
Realizamos en este paso la configuración básica de cada uno de los routers, no olvidemos que debemos activar cada una de las interfaces de manera manual, de una vez realizamos la configuración del protocolo de enrutamiento

Router(config)#hostname bucaramanga
bucaramanga(config)#no ip domain-lookup

```
bucaramanga(config)#banner motd $El Acceso no autorizado est prohibido$
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#
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 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#
```

```
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#

Pprocedemos a realizar la configuración de los SWITCH, la creación de las VLAN y las respectivas asignaciones de las interfaces a cada una de ellas.

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)#


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)#


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
```

Siguiente paso en nuestro poceso es realizer la configuración de la autenticación AAA, este proceso se describe a continuación, esta tambien debe aplcarse a los 3 reouters

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.

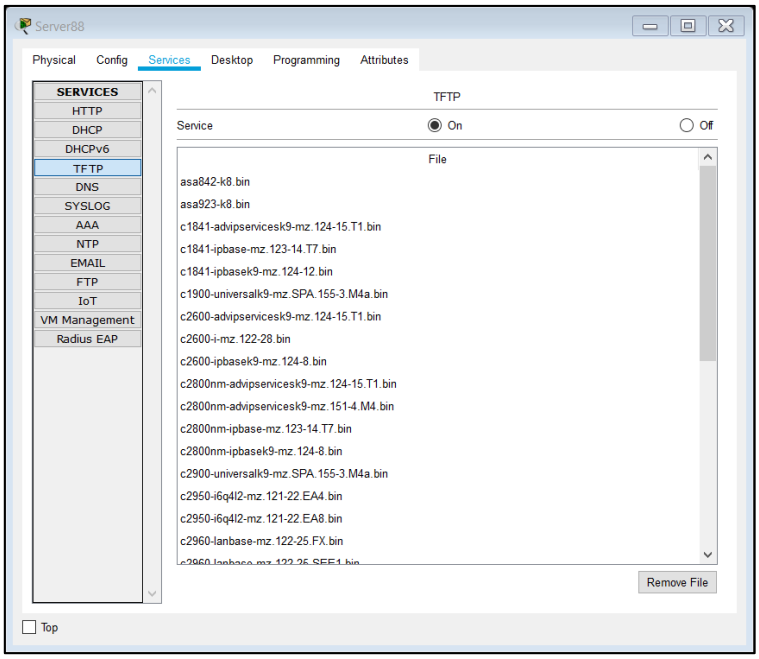
bucaramanga(config-line)#login block-for 20 attempts 10 within 60
tunja(config-line)#login block-for 20 attempts 10 within 60
cundinamarca(config-line)#login block-for 20 attempts 10 within 60

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

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

Figura 31. Server 88



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

El router encargado de realizar la asignación de direcciones IP es el router de TUNJA, debemos excluir las primeras direcciones IP de cada uno de los rangos IP de las 4 vlan indicadas en BUCARAMANGA y en CUNDINAMARCA y posteriormente debemos crear cada uno de los POOL de direcciones, tal como indico a continuación.

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

Procedemos a configurar cada uno de los routers con el fin de que estos puedan tener acceso a estos POOL de direcciones.

```
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#
```

```
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#
```

Siguiente paso es proceder a verificar que cada uno de los PC de las VLAN de los routers de Bucarmanga y Cundinamarca obtengan sus direcciones IP empleando DHCP.

Figura 32. Verificación del PC 10

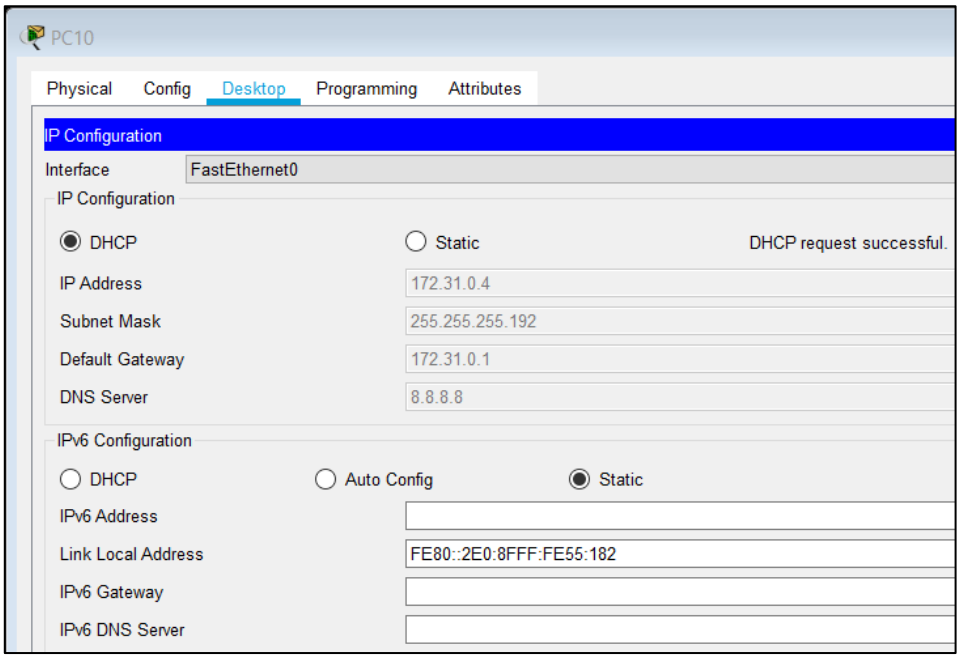


Figura 33. Verificación del PC 11

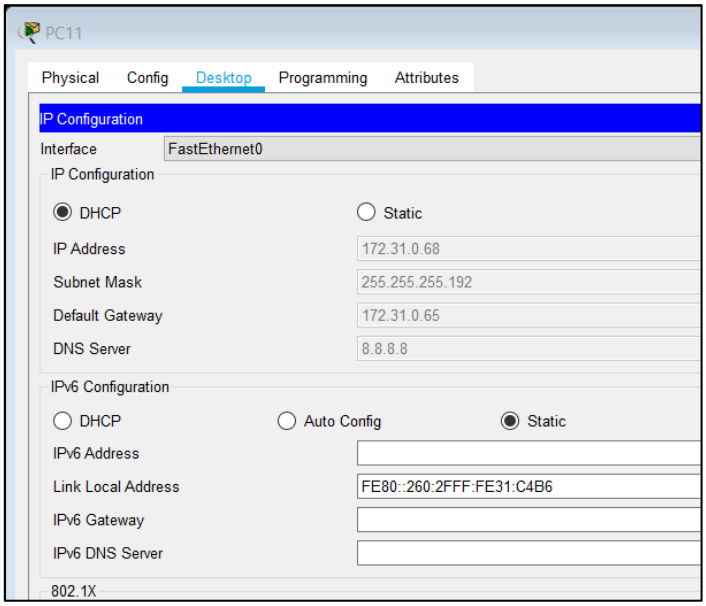


Figura 34. Verificación del PC 14

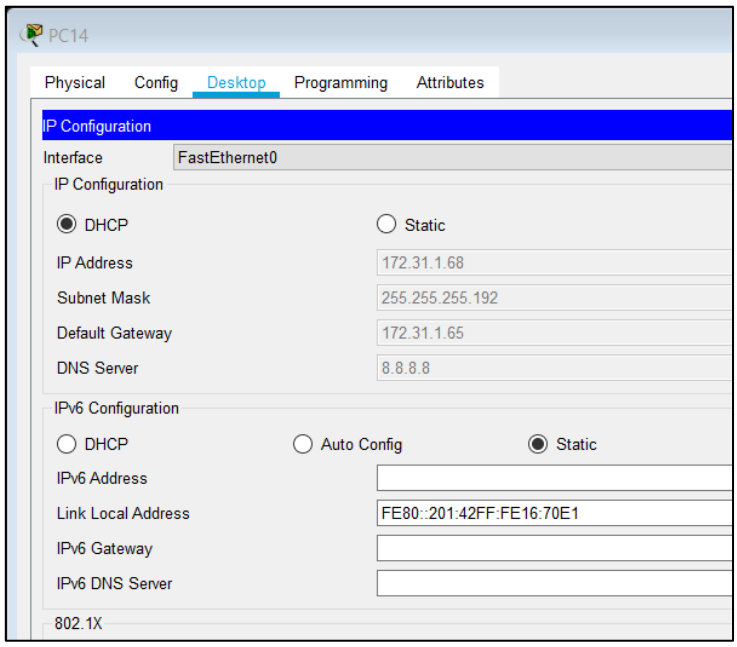
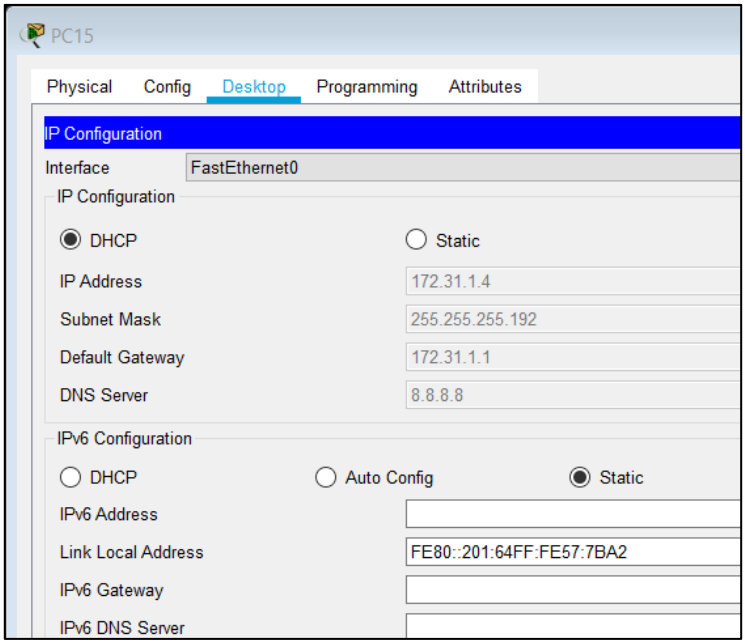


Figura 35. Verificación del PC 15



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

Se nos exige dos tipos de NAT de forma estática para nuestro servidor y con sobrecarga para los demás equipos de nuestra red.

```
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#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

tunja#

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#

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 36. Verificación en PC 15

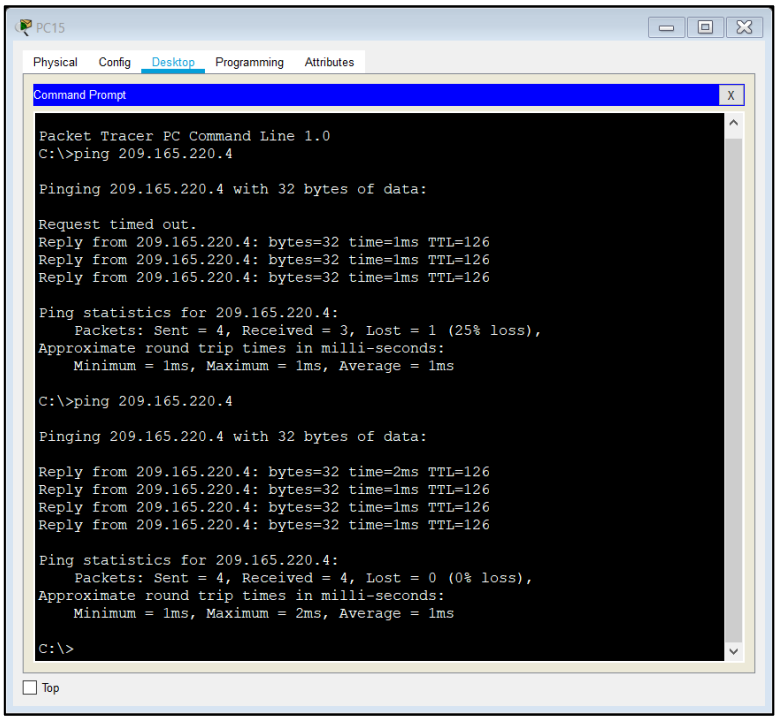
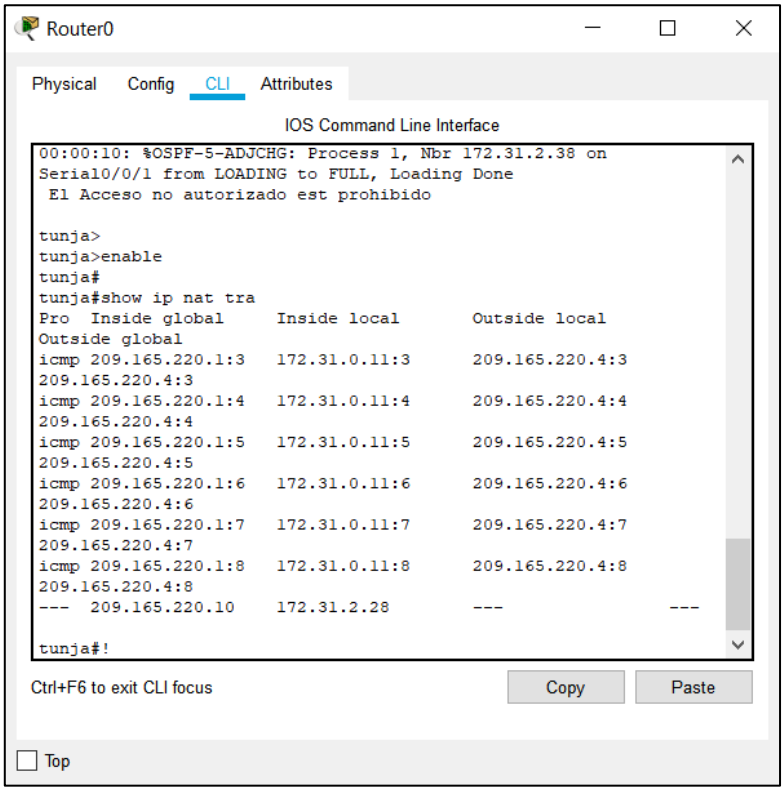


Figura 37. Router 0



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
cundinamarca(config-if)#
```

Listas de control de acceso:

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

Comenzamos creando la primera VLAN, debemos tener en cuenta que la debemos crear y luego asignar a determinada interfaz, indicando si esta es de entrada o de salida.

cundinamarca(config-if)#access-list **131** deny ip 172.31.1.64 0.0.0.63 209.165.220.0 0.0.0.255

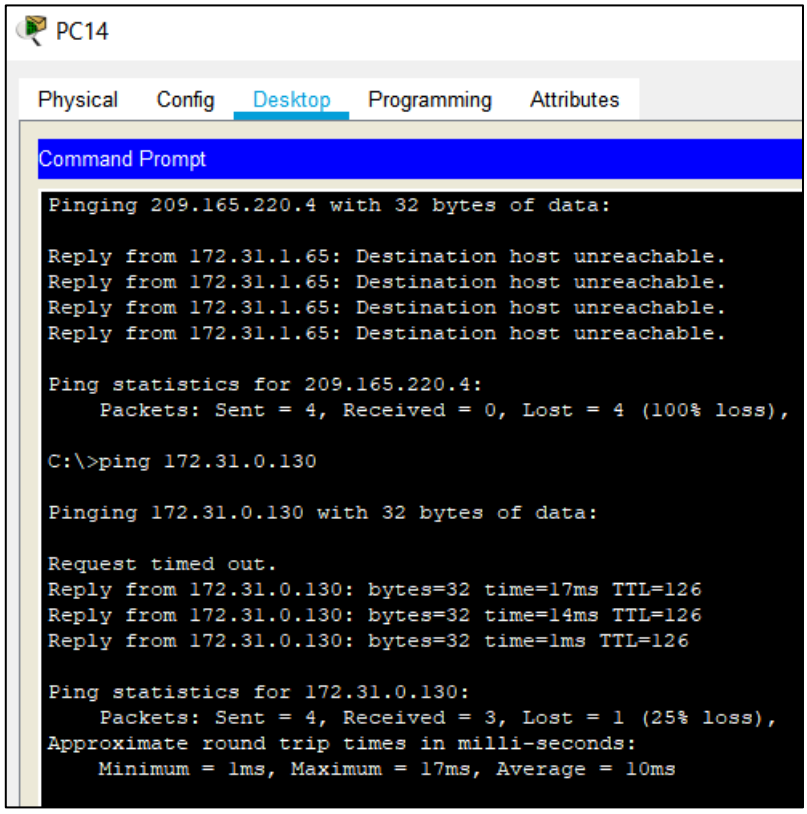
cundinamarca(config)#access-list 131 permit ip any any

cundinamarca(config)#int f0/0.20

cundinamarca(config-subif)#ip access-group 131 in

cundinamarca(config-subif)#

Figura 38, Verificación PC 14



Observamos que no tenemos acceso al servidor, pero si podemos hacer ping a otro dispositivo en la red de Tunja.

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

Nuevamente, debemos crear la ACL y la debemos asignar a determinada interfaz indicando si esta es de entrada o de salida

cundinamarca(config-subif)#access-list **132** permit ip 172.31.1.0 0.0.0.63 209.165.220.0 0.0.0.255

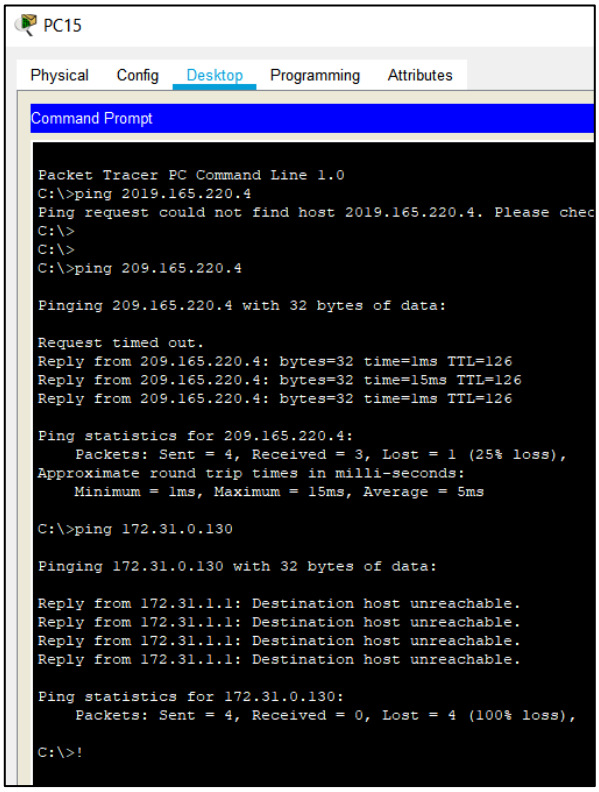
cundinamarca(config)#access-list **132** deny ip any any

cundinamarca(config)#int f0/0.30

cundinamarca(config-subif)#ip access-group **132** in

cundinamarca(config-subif)#

Figura 39. Verificación PC 15



Vemos que la ACL está funcionando, ya que los dispositivos de la VLAN 30 de Cundinamarca en este caso tiene acceso a internet pero no tienen acceso a los dispositivos de TUNJA.

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

Creamos la ACL 131 y la aplicamos a la interfaz correspondiente de la VLAN 30.

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 40. Verificación PC 13

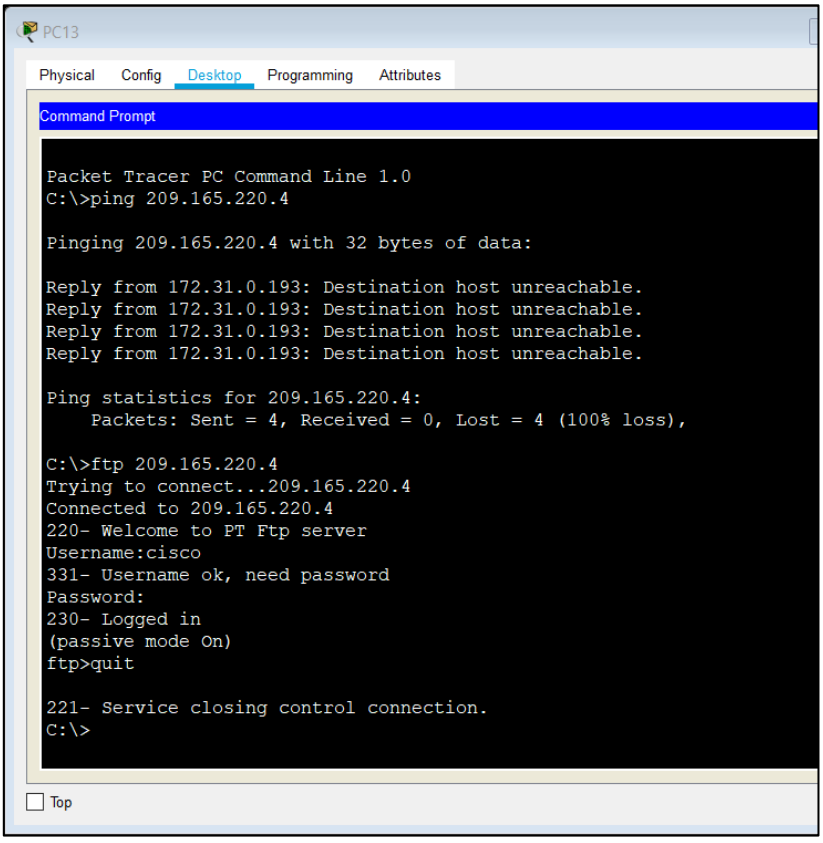
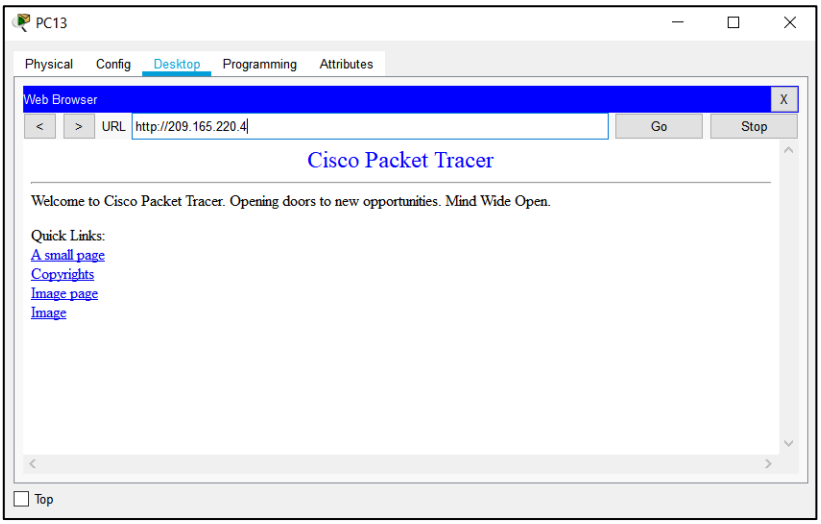


Figura 41 Verificación navegación en PC 13



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

Debemos crear la ACL 132 y asignarla a la interfaz f0/0.20 de Tunja de entrada.

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

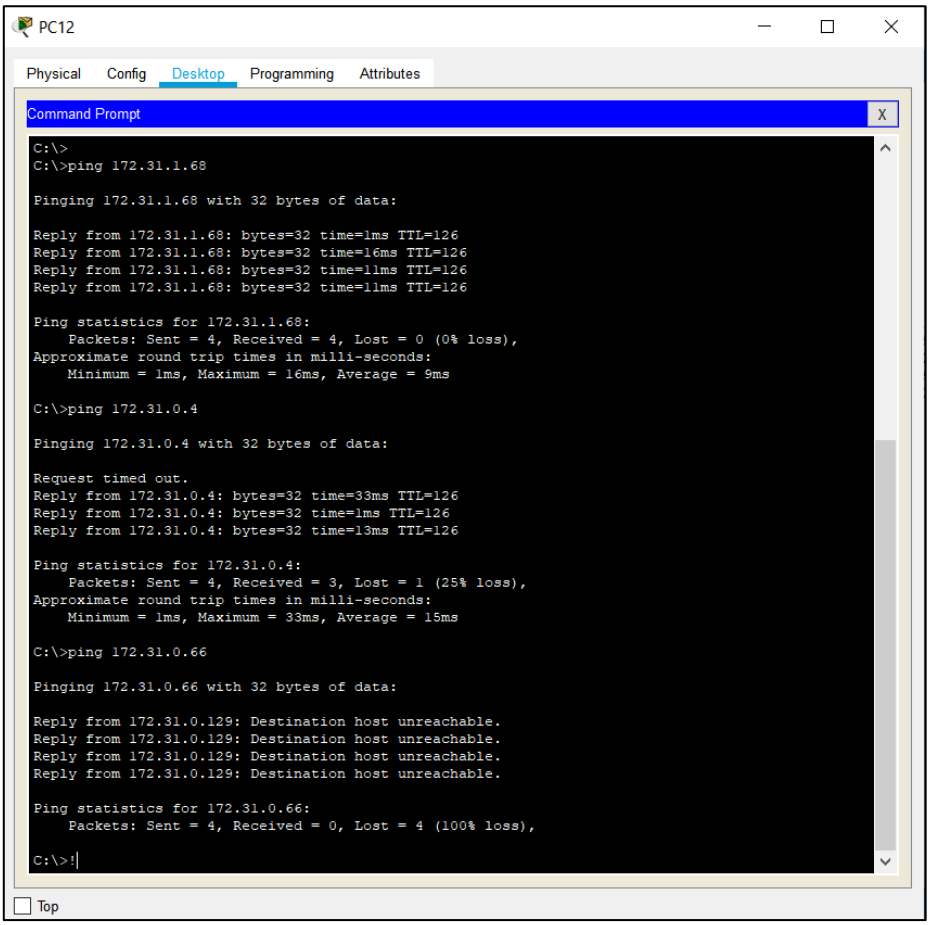
tunja(config)#access-list **132** permit ip 172.31.0.128 0.0.0.63 172.31.0.0 0.0.0.63

tunja(config)#int f0/0.20

tunja(config-subif)#ip access-group **132** in

tunja(config-subif)#

Figura 42. Verificación PC 12



Vemos que si podemos llegar a las VLAN indicadas, pero si le damos PING a una VLAN diferente esta nos aparece destino inalcanzable.

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

Creamos la ACL y la asignamos a la interfaz adecuada indicando en este caso que es de entrada.

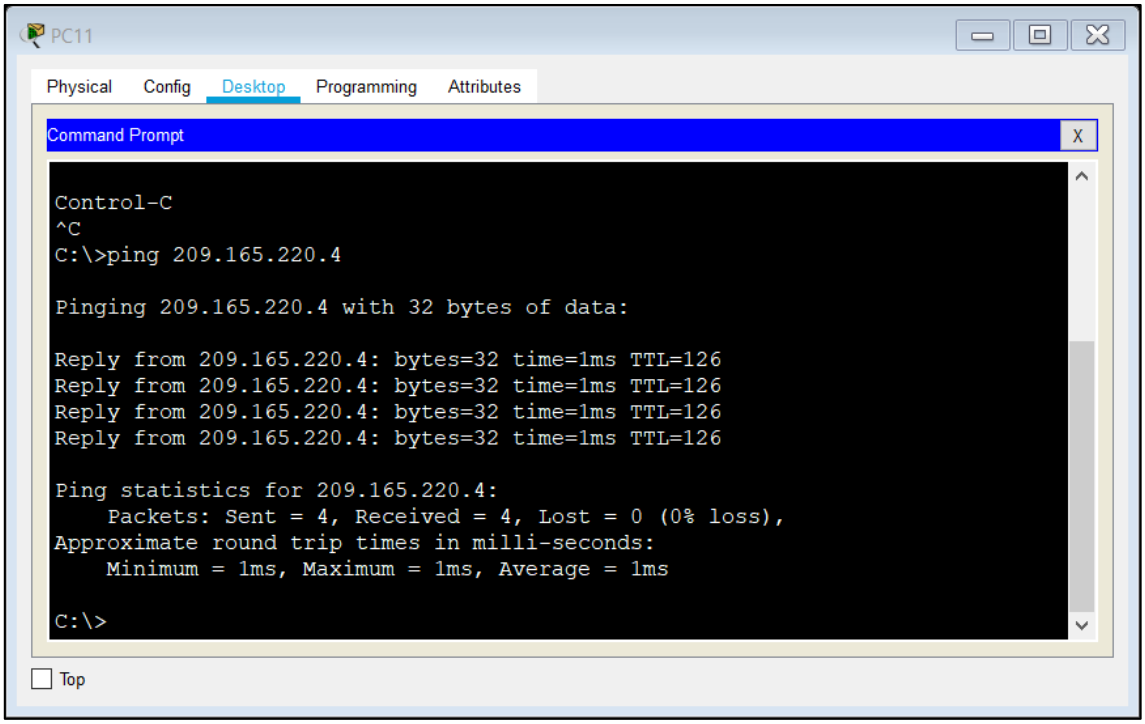
bucaramanga(config)#access-list **131** permit ip 172.31.0.64 0.0.0.63 209.165.220.0 0.0.0.255

bucaramanga(config)#int f0/0.30

bucaramanga(config-subif)#ip access-group **131** in

bucaramanga(config-subif)#

Figura 43. Verificación PC 11



Los hosts de VLAN 10 en Bucaramanga acceden a la red de Cundinamarca (VLAN 20) y Tunja (VLAN 20), no internet.

Creamos nuestras 2 ACL siguiendo las indicaciones y las asignamos a la interfaz adecuada indicando si es de entrada o de salida.

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

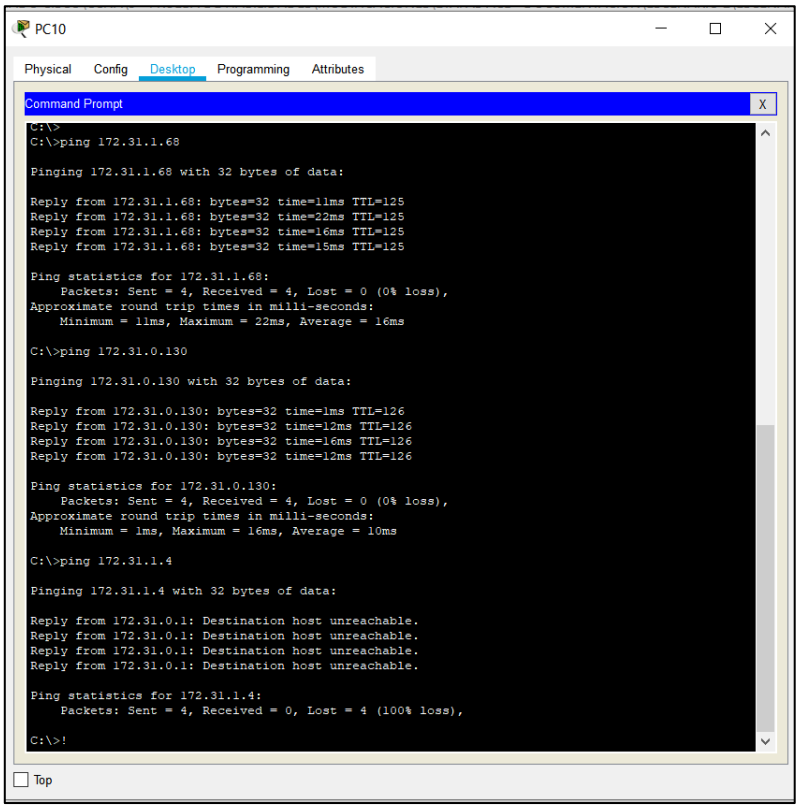
bucaramanga(config)#access-list **132** permit ip 172.31.0.0 0.0.0.63 172.31.0.128 0.0.0.63

bucaramanga(config)#int f0/0.10

bucaramanga(config-subif)#ip access-group **132** in

bucaramanga(config-subif)#

Figura 44. Verificación PC 10



Vemos que nuestras ACL creadas estan fucnoiando muy bien, ya que las 2 vlan nos responden muy bien, pero si hacemos un PING a un dispositivo por fuera de los mismos nos parece INALCANZABLE.

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

En este caso debemos crear ACL de acuerdo al número de VLAN que tengamos en cada router y que no queramos que tenga acceso a otra VLAN. En este caso las asignamos a la interfaz correspondiente pero en este caso serán de salida.

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 1**23** 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

cundinamarca(config-subif)#

En este caso debemos hacer varias pruebas con el fin de verificar el correcto funcionamiento de las ACL configuradas en los 3 routers.

Figura 45. Comando prompt pc 12

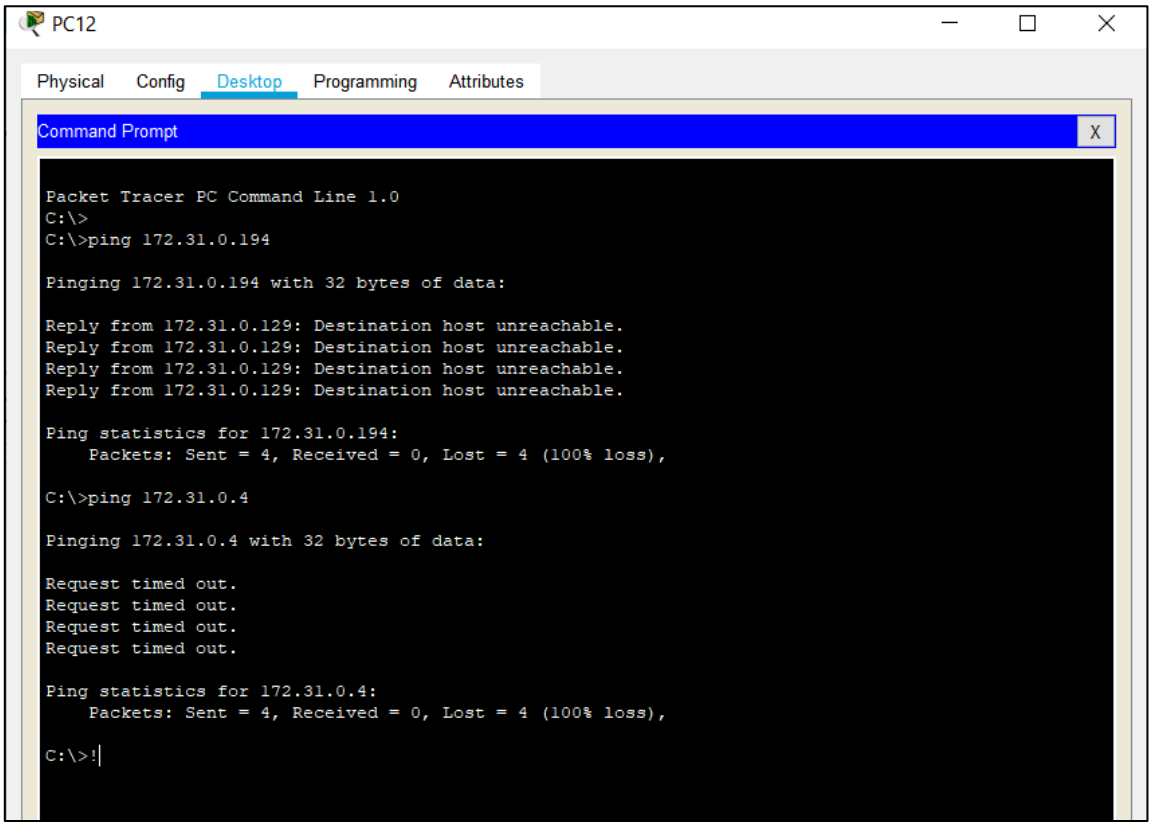
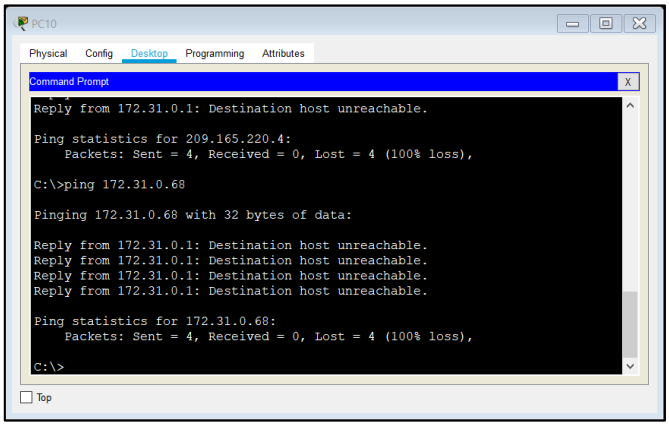


Figura 46 . Destinatario PC 10



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
cundinamarca(config-line)#

Figura 47. Verificación Switch2

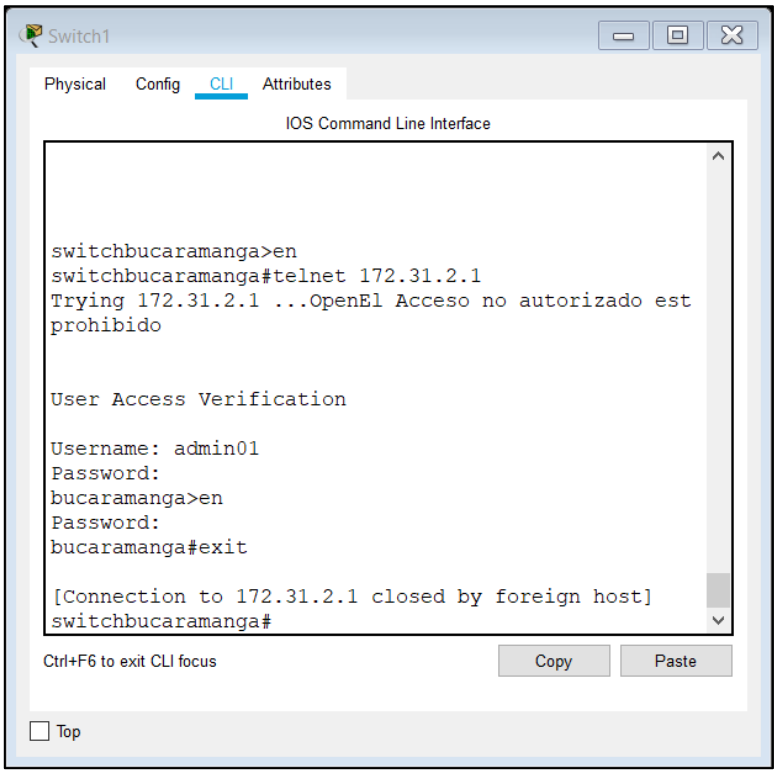
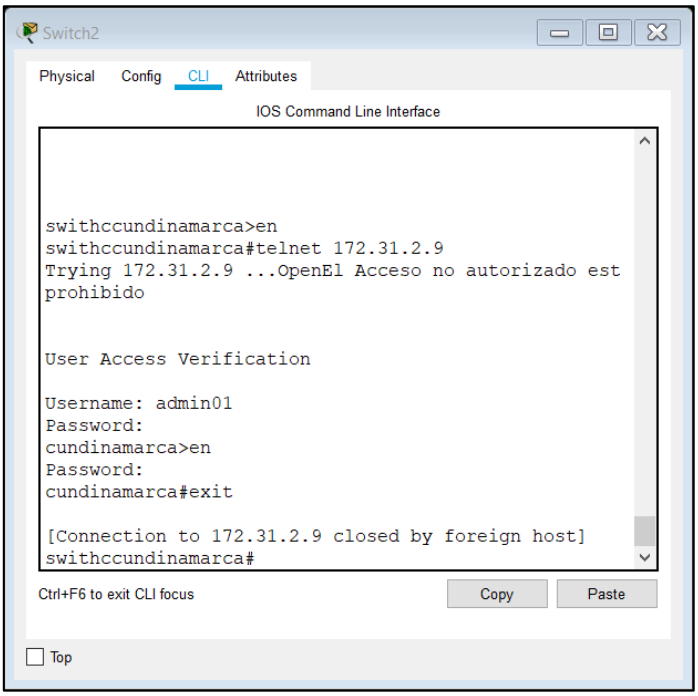
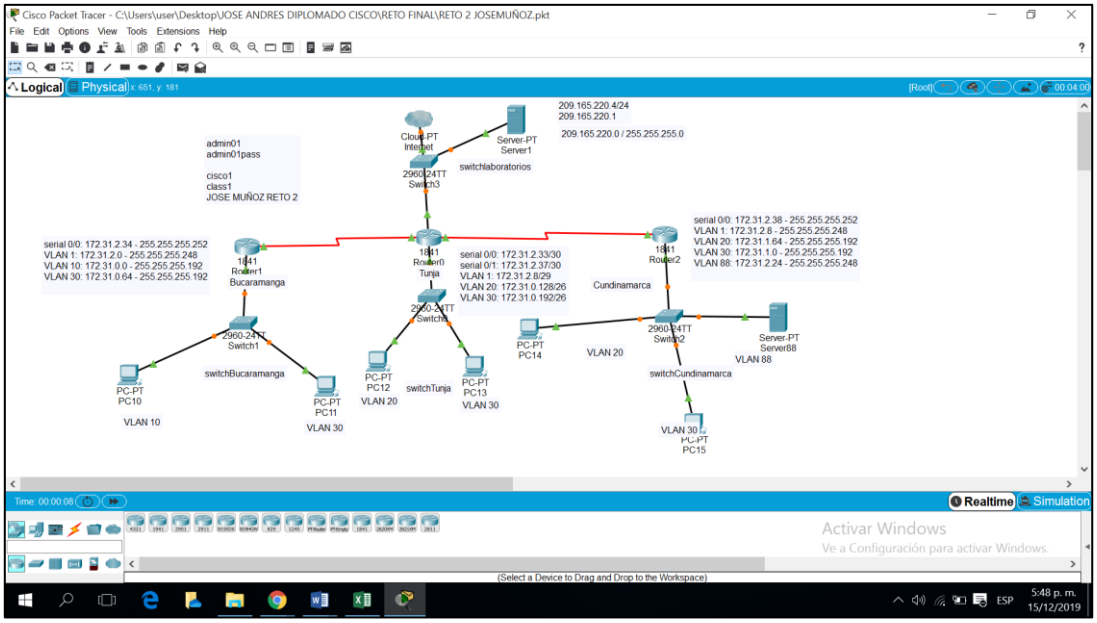


Figura 48. Verificación Switch2



VLSM: utilizar la dirección 172.31

Figura 49. Reto Solucionado



CONCLUSIONES

Los dos últimos retos fueron muy importantes, porque nos ayudó a entender los conceptos y tecnologías básicos de redes. Además, pudimos poner en práctica y desarrollar las aptitudes necesarias para planear y realizar redes pequeñas con una variedad de aplicaciones.

Este curso es muy importante, siendo que las redes permiten que las personas nos comuniquemos, colaboremos e interactuemos de muchas maneras. Las redes se utilizan para acceder a páginas web, hablar mediante teléfonos IP, participar en videoconferencias, competir en juegos interactivos, realizar compras en Internet, completar trabajos de cursos en línea, y más. Me siento con más capacidad para entrar al campo laboral como ingeniero de sistemas.

BIBLIOGRAFÍA

CISCO. (2014). Acceso a la red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#4.0.1.1

CISCO. (2014). Asignación de direcciones IP. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module8/index.html#8.0.1.1

CISCO. (2014). Capa de Aplicación. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module10/index.html#10.0.1.1

CISCO. (2014). Capa de red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#6.0.1.1

CISCO. (2014). Capa de Transporte. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module7/index.html#7.0.1.1

CISCO. (2014). Conceptos de Routing. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module4/index.html#4.0.1.1

CISCO. (2014). Configuración de un sistema operativo de red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#2.0.1.1

CISCO. (2014). Configuración y conceptos básicos de Switching. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module2/index.html#2.0.1.1

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

CISCO. (2014). Enrutamiento Dinámico. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module7/index.html#7.0.1.1

CISCO. (2014). Enrutamiento entre VLANs. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module5/index.html#5.0.1.1

CISCO. (2014). Enrutamiento Estático. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module6/index.html#6.0.1.1

CISCO. (2014). Ethernet. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#5.0.1.1

CISCO. (2014). Exploración de la red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module1/index.html#1.0.1.1

CISCO. (2014). Introducción a redes conmutadas. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module1/index.html#1.0.1.1

CISCO. (2014). Listas de control de acceso. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module9/index.html#9.0.1.1

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

CISCO. (2014). Protocolos y comunicaciones de red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#3.0.1.1

CISCO. (2014). Soluciones de Red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module11/index.html#11.0.1.1

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

CISCO. (2014). Traducción de direcciones IP para IPv4. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module11/index.html#11.0.1.1

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

Lammle, T. (2010). CISCO Press (Ed). Cisco Certified Network Associate Study Guide. Recuperado de https://1drv.ms/b/s!AmIJYei-NT1Im3GQVfFFrjnEGFFU

Lucas, M. (2009). Cisco Routers for the Desperate : Router and Switch Management, the Easy Way. San Francisco: No Starch Press. Recuperado de https://1drv.ms/b/s!AmIJYei-NT1Im3L74BZ3bpMiXRx0

Macfarlane, J. (2014). Network Routing Basics : Understanding IP Routing in Cisco Systems. Recuperado de http://bibliotecavirtual.unad.edu.co:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=e000xww&AN=158227&lang=es&site=ehost-live

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

Odom, W. (2013). CISCO Press (Ed). CCNA ICND2 Official Exam Certification Guide. Recuperado de http://mr-telecomunicaciones.com/wp-content/uploads/2018/09/wendellodom.pdf

Vesga, J. (2014). Configuración de Switches y Routers [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgL9QChD1m9EuGqC

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

Vesga, J. (2014). PING y TRACER como estrategia en procesos de Networking [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgTCtKY-7F5KIRC3

Vesga, J. (2014). Principios de Enrutamiento [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgOyjWeh6timi_Tm