

**PRUEBA DE HABILIDADES PRÁCTICAS
DIPLOMADO DE PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN DE
SOLUCIONES
INTEGRADAS LAN / WAN)**

RAÚL JIMÉNEZ MEDINA

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
FACULTAD DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
CEAD BUCARAMANGA INGENIERÍA DE SISTEMAS
BUCARAMANGA SANTANDER
2019**

**PRUEBA DE HABILIDADES PRÁCTICAS
DIPLOMADO DE PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN DE
SOLUCIONES
INTEGRADAS LAN / WAN)**

RAÚL JIMÉNEZ MEDINA

**Trabajo presentado como requisito para aprobar diplomado de profundización
como opción de grado para obtener el título de ingeniero de sistemas**

**Director
JUAN CARLOS VESGA
Ingeniero Telecomunicaciones**

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
FACULTAD DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
CEAD BUCARAMANGA INGENIERÍA DE SISTEMAS
BUCARAMANGA SANTANDER
2019**

Nota de Aceptación

Presidente del Jurado

Jurado

Jurado

Ciudad, Fecha de sustentación (con Día de Mes de año).

Agradecimiento

Agradezco en primera instancia al ser todo poderoso que nos brinda la vida y la salud para cumplir cada uno de nuestros propósitos y metas. Doy gracias a cada familiar que me brinda un apoyo incondicional para seguir creciendo académica y personalmente, que me acompañan en cada escalón subido y lo celebran junto a mí. Agradezco también a cada persona que fue parte de este proceso de enseñanza de mi ingeniería, compañeros, docentes tutores y directores de los cuales aprendí en cada momento compartido.

Tabla de Contenido

GLOSARIO	9
Resumen	10
ABSTRACT	11
Introducción	12
OBJETIVOS	13
GENERAL	13
ESPECIFICOS	13
DESARROLLO DE LOS ESCENARIOS	14
ESCENARIO 1	14
Topología de red	14
Imagen 1. configuración final	14
Parte 1: Asignación de direcciones IP:	15
a. Se debe dividir (subnetear) la red creando una segmentación en ocho partes, para permitir crecimiento futuro de la red corporativa.....	15
CONVERSIÓN A BINARIO	15
b. Asignar una dirección IP a la red.....	17
Parte 2: Configuración Básica	19
a. Completar la siguiente tabla con la configuración básica de los routers, teniendo en cuenta las subredes diseñadas.	19
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.....	20
c. Verificar el balanceo de carga que presentan los routers.	21
d. Realizar un diagnóstico de vecinos usando el comando cdp.	21
e. Realizar una prueba de conectividad en cada tramo de la ruta usando Ping.	22
Parte 3: Configuración de Enrutamiento.	24
a. Asignar el protocolo de enrutamiento EIGRP a los routers considerando el direccionamiento diseñado.	24
b. Verificar si existe vecindad con los routers configurados con EIGRP.	25

c. Realizar la comprobación de las tablas de enrutamiento en cada uno de los routers para verificar cada una de las rutas establecidas.....	28
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.....	31
Parte 4: Configuración de las listas de Control de Acceso.	32
a. 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. 34	
Parte 5: Comprobación de la red instalada.	35
a. Se debe probar que la configuración de las listas de acceso fue exitosa.	35
b. Comprobar y Completar la siguiente tabla de condiciones de prueba para confirmar el óptimo funcionamiento de la red e.	35
Desarrollo	47
Aspectos en cuenta para el desarrollo del ejercicio 2	49
1. Todos los routers deberán tener los siguiente:	50
2. El DHCP deberá proporcionar solo direcciones a los hosts de Bucaramanga y Cundinamarca	54
3. El web server deberá tener NAT estático y el resto de los equipos de la topología emplearan NAT de sobrecarga (PAT).	54
4. El enrutamiento deberá tener autenticación.	56
5. Listas de control de acceso:	59
6. VLSM: utilizar la dirección 172.31.0.0 /18 para el direccionamiento.	62
Lista de Referencias	65
ANEXOS	66

Lista de Figuras

Imagen 1. configuración final	14
Imagen 3. PC0 – PC1	22
Imagen 4. PC2 – PC3	22
Imagen 5. SERVIDOR – WS 1	23
Imagen 6. prueba a la red de MEDELLIN	31
Imagen 7. prueba al servidor	31
Imagen 8. Router MEDELLIN - Router CALI	36
Imagen 9. WS_1 - Router BOGOTA.....	37
Imagen 10. Servidor - Router CALI	38
Imagen 11. Servidor - Router MEDELLIN.....	38
Imagen 12. LAN del Router MEDELLIN- Router CALI.....	39
Imagen 13. LAN del Router CALI - Router CALI.....	39
Imagen 14. LAN del Router MEDELLIN - Router MEDELLIN.....	40
Imagen 15. LAN del Router CALI - Router MEDELLIN.....	41
Imagen 16. LAN del Router CALI- WS_1	41
Imagen 17. LAN del Router MEDELLIN - WS_1	42
Imagen 18. LAN del Router MEDELLIN - LAN del Router CALI	43
Imagen 19. LAN del Router CALI – Servidor	43
Imagen 20. LAN del Router MEDELLIN – Servidor	44
Imagen 21. Servidor - LAN del Router MEDELLIN	45
Imagen 22. Servidor - LAN del Router CALI.....	46
Imagen 23. Router CALI	LAN - del Router MEDELLIN
	46
Imagen 24.. DESARROLLO ESCENARIO 2.....	49

Lista de Tabla

Tabla 1. CONVERSIÓN A BINARIO	15
Tabla 2. RED.....	15
Tabla 3. BROADCAST	15
Tabla 4. RANGO HOSTS.....	15
Tabla 5. Configuración Básica	19
Tabla 6. Comprobación de la red instalada.....	35

GLOSARIO

Switch: Es un dispositivo para diseñar y resolver errores de rendimiento en la red, maneja el mejoramiento de ancho de banda.

LAN: Red de área local, se conectan múltiples dispositivos, la conexión es por cable o ondas. Los equipos conectados en la red LAN son nodos y se pueden comunicar entre sí.

WAN: Red de área extensa, está distribuida geográficamente para intercomunicar múltiples redes de área local.

IP: Identifica la manera lógica de la interfaz de una red, lo usan los equipos de cómputo, impresoras, tabletas, celulares entre otros.

DSL: Es una línea de abonado digital se usa en servicios de telecomunicaciones distribuidos, mediante el cableado cobre, como la línea telefónica convencional.

Resumen

TITULO: PRUEBA DE HABILIDADES PRÁCTICAS

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

Autor: Raúl Jiménez Medina.

Palabras claves: dsl, wan, lan, switch, ip, packet tracer, GNS3, Networking.

Los escenarios propuestos para la prueba de habilidades muestran las diferentes configuraciones donde se evidencia el código utilizado para lograr completar dichos escenarios, paso a paso se detalla y se cumple con lo solicitado en las actividades, este es el producto del esfuerzo de la adquisición de conocimiento obtenido durante el curso del diplomado.

ABSTRACT

TITLE: PRACTICE SKILLS TEST

CISCO DEPTH DEGREE (DESIGN AND IMPLEMENTATION OF LAN / WAN INTEGRATED SOLUTIONS)

Author: Raúl Jiménez Medina.

Keywords: dsl, wan, lan, switch, ip, **packet tracer**, GNS3, Networking.

The scenarios proposed for the skills test show the different configurations where the code used to complete these scenarios is evidenced, step by step it is detailed and complied with what is requested in the activities, this is the product of the knowledge acquisition effort obtained during the course of the diploma.

Introducción

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

A continuación, se elaboran dos escenarios correspondientes a la temática de implementación de soluciones soportadas en enrutamiento avanzado como etapa final del curso Diplomado de Profundización CCNA.

OBJETIVOS

GENERAL

Realizar el proceso de configuración de 2 escenarios propuestos usando las herramientas GNS3 o Packet Tracer.

ESPECIFICOS

- Describir el paso a paso de cada punto realizado
- Digitar el código de configuración aplicado
- Hacer uso de listas de acceso
- Aplicar el conocimiento adquirido durante el curso del diplomado

DESARROLLO DE LOS ESCENARIOS

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.

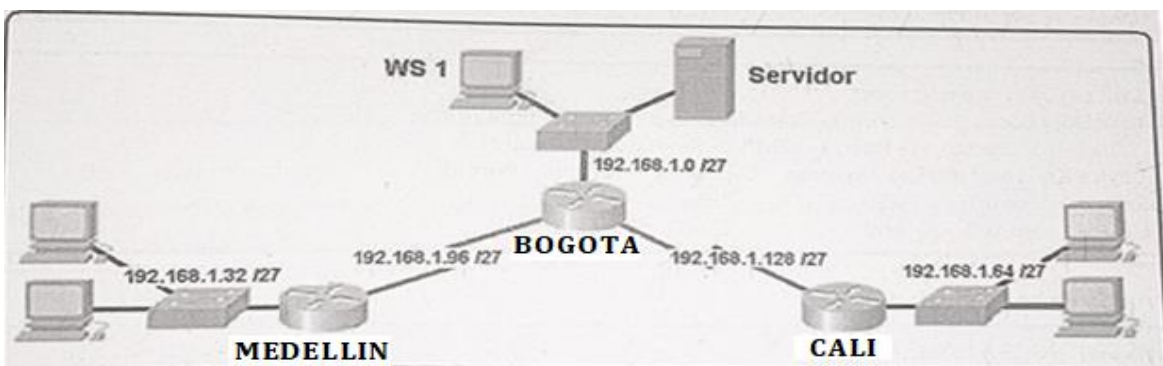
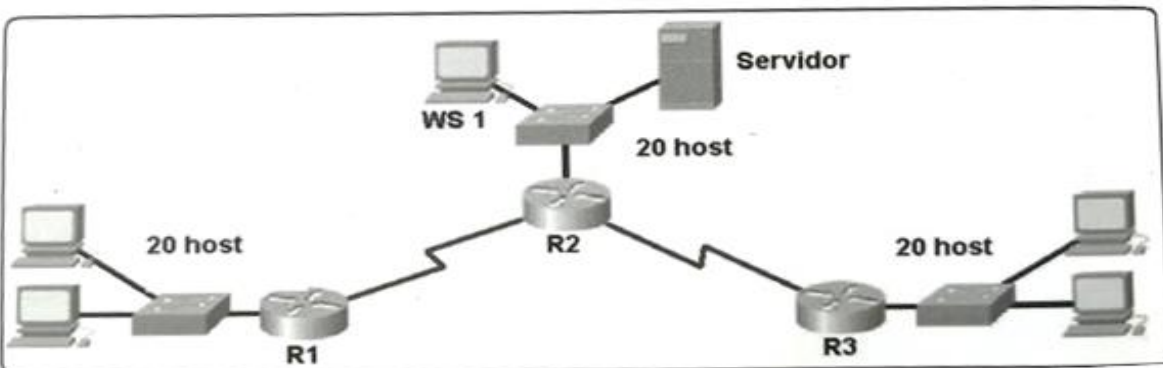
Parte 2: Considerar la asignación de los parámetros básicos y la detección de vecinos directamente conectados.

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.

Imagen 1. configuración final



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.

192.168.1.32 /27

192.168.1.33 – 192.168.1.62

CONVERSIÓN A BINARIO

Tabla 1. CONVERSIÓN A BINARIO

192.168.1.32	>>	1 1 0 0 0 0 0 0 . 1 0 1 0 1 0 0 0 . 0 0 0 0 0 0 0 0 1 . 0 0 1 0 0 0 0 0
255.255.255.224	>>	1 1 1 1 1 1 1 1 . 1 1 1 1 1 1 1 1 . 1 1 1 1 1 1 1 1 . 1 1 1 0 0 0 0 0

La red se obtiene poniendo a cero todos los bits de host. En este caso la red se corresponde con:

RED

Tabla 2. RED

192.168.1.32/27	>>	1 1 0 0 0 0 0 0 . 1 0 1 0 1 0 0 0 . 0 0 0 0 0 0 0 0 1 . 0 0 1 0 0 0 0 0
-----------------	----	---

La dirección broadcast se obtiene poniendo a uno todos los bits de host. En este caso la dirección broadcast se corresponde con:

BROADCAST

Tabla 3. BROADCAST

192.168.1.63	>>	1 1 0 0 0 0 0 0 . 1 0 1 0 1 0 0 0 . 0 0 0 0 0 0 0 0 1 . 0 0 1 1 1 1 1 1
--------------	----	---

El rango de hosts son todos los valores que existen entre la red y la dirección broadcast.

RANGO HOSTS

Tabla 4. RANGO HOSTS

192.168.1.33	>>	1 1 0 0 0 0 0 0 . 1 0 1 0 1 0 0 0 . 0 0 0 0 0 0 0 0 1 . 0 0 1 0 0 0 0 1
--------------	----	---

192.168.1.62	>>	1 1 0 0 0 0 0 0 . 1 0 1 0 1 0 0 0 . 0 0 0 0 0 0 0 0 1 . 0 0 1 1 1 1 1 0
--------------	----	---

192.168.1.64 /27

192.168.1.65 – 192.168.1.95

CONVERSIÓN A BINARIO

192.168.1.64	>>	1 1 0 0 0 0 0 0 . 1 0 1 0 1 0 0 0 . 0 0 0 0 0 0 0 1 . 0 1 0 0 0 0 0 0
255.255.255.224	>>	1 1 1 1 1 1 1 1 . 1 1 1 1 1 1 1 1 . 1 1 1 1 1 1 1 1 . 1 1 1 0 0 0 0 0

La red se obtiene poniendo a cero todos los bits de host. En este caso la red se corresponde con:

RED

192.168.1.64/27	>>	1 1 0 0 0 0 0 0 . 1 0 1 0 1 0 0 0 . 0 0 0 0 0 0 0 1 . 0 1 0 0 0 0 0 0
-----------------	----	---

La dirección broadcast se obtiene poniendo a uno todos los bits de host. En este caso la dirección broadcast se corresponde con:

BROADCAST

192.168.1.95	>>	1 1 0 0 0 0 0 0 . 1 0 1 0 1 0 0 0 . 0 0 0 0 0 0 0 1 . 0 1 0 1 1 1 1 1
--------------	----	---

El rango de hosts son todos los valores que existen entre la red y la dirección broadcast.

RANGO HOSTS

192.168.1.65	>>	1 1 0 0 0 0 0 0 . 1 0 1 0 1 0 0 0 . 0 0 0 0 0 0 0 1 . 0 1 0 0 0 0 0 1
--------------	----	---

192.168.1.94	>>	1 1 0 0 0 0 0 0 . 1 0 1 0 1 0 0 0 . 0 0 0 0 0 0 0 1 . 0 1 0 1 1 1 1 0
--------------	----	---

192.168.1.0 /27

192.168.1.2 – 192.168.1.30

CONVERSIÓN A BINARIO

192.168.1.0	>>	1 1 0 0 0 0 0 0 . 1 0 1 0 1 0 0 0 . 0 0 0 0 0 0 0 1 . 0 0 0 0 0 0 0 0
255.255.255.224	>>	1 1 1 1 1 1 1 1 . 1 1 1 1 1 1 1 1 . 1 1 1 1 1 1 1 1 . 1 1 1 0 0 0 0 0

La red se obtiene poniendo a cero todos los bits de host. En este caso la red se corresponde con:

RED

192.168.1.0/27	>>	1 1 0 0 0 0 0 0 . 1 0 1 0 1 0 0 0 . 0 0 0 0 0 0 0 1 . 0 0 0 0 0 0 0 0
----------------	----	---

La dirección broadcast se obtiene poniendo a uno todos los bits de host. En este caso la dirección broadcast se corresponde con:

BROADCAST

192.168.1.31	>>	1 1 0 0 0 0 0 0 . 1 0 1 0 1 0 0 0 . 0 0 0 0 0 0 0 1 . 0 0 0 1 1 1 1 1
--------------	----	---

El rango de hosts son todos los valores que existen entre la red y la dirección broadcast.

RANGO HOSTS

192.168.1.1	>>	1 1 0 0 0 0 0 0 . 1 0 1 0 1 0 0 0 . 0 0 0 0 0 0 0 1 . 0 0 0 0 0 0 0 1
-------------	----	---


```
192.168.1.30 >> 1 1 0 0 0 0 0 0 . 1 0 1 0 1 0 0 0 . 0 0 0 0 0 0 0 0 1 . 0 0 0 0 1 1 1 1 0
```

b. Asignar una dirección IP a la red.

IP BOGOTA

```
BOGOTA(config)#int s0/0/0
```

```
BOGOTA(config-if)#ip address 192.168.1.98 255.255.255.224
```

```
BOGOTA(config-if)#no shutdown
```

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

```
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
```

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

```
BOGOTA(config-if)#int fa0/0
```

```
BOGOTA(config-if)#ip address 192.168.1.1 255.255.255.224
```

```
BOGOTA(config-if)#no shutdown
```

```
BOGOTA(config-if)#
```

```
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
```

```
BOGOTA(config-if)#
```

IP MEDELLIN

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

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

```
MEDELLIN(config-if)#int fa0/0  
MEDELLIN(config-if)#ip address 192.168.1.33 255.255.255.224  
MEDELLIN(config-if)#no shutdown
```

```
MEDELLIN(config-if)#  
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state  
to up
```

```
MEDELLIN(config-if)#
```

IP CALI

```
CALI(config)#int s0/0/0  
CALI(config-if)#ip address 192.168.1.131 255.255.255.224  
CALI(config-if)#no shutdown  
CALI(config-if)#  
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
```

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

```
CALI(config-if)#int fa0/0  
CALI(config-if)#ip address 192.168.1.65 255.255.255.224  
CALI(config-if)#no shutdown
```

```
CALI(config-if)#  
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
```

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

CALI(config-if)#

PC0

*Ip address 192.168.1.39
Subnet Mask 255.255.255.224*

PC1

*Ip address 192.168.1.40
Subnet Mask 255.255.255.224*

PC2

*Ip address 192.168.1.67
Subnet Mask 255.255.255.224*

PC3

*Ip address 192.168.1.68
Subnet Mask 255.255.255.224*

WS1

*Ip address 192.168.1.4
Subnet Mask 255.255.255.224*

Servidor

*Ip address 192.168.1.3
Subnet Mask 255.255.255.224*

Parte 2: Configuración Básica.

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

Tabla 5. Configuración Básica

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

Dirección de Ip en interfaz Serial 0/1		192.168.1.130	
Dirección de Ip en interfaz FA 0/0	192.168.1.33	192.168.1.1	192.168.1.65
Protocolo de enrutamiento	Eigrp	Eigrp	Eigrp
Sistema Autónomo	200	200	200
Afirmaciones de red	192.168.1.0	192.168.1.0	192.168.1.0

- 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

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, 3 subnets

*C 192.168.1.0 is directly connected, FastEthernet0/0
C 192.168.1.96 is directly connected, Serial0/0/0
C 192.168.1.128 is directly connected, Serial0/0/1*

BOGOTA#

MEDELLIN

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, 2 subnets

C 192.168.1.32 is directly connected, FastEthernet0/0

C 192.168.1.96 is directly connected, Serial0/0/0

MEDELLIN#

CALI

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, 2 subnets

C 192.168.1.64 is directly connected, FastEthernet0/0

C 192.168.1.128 is directly connected, Serial0/0/0

CALI#

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

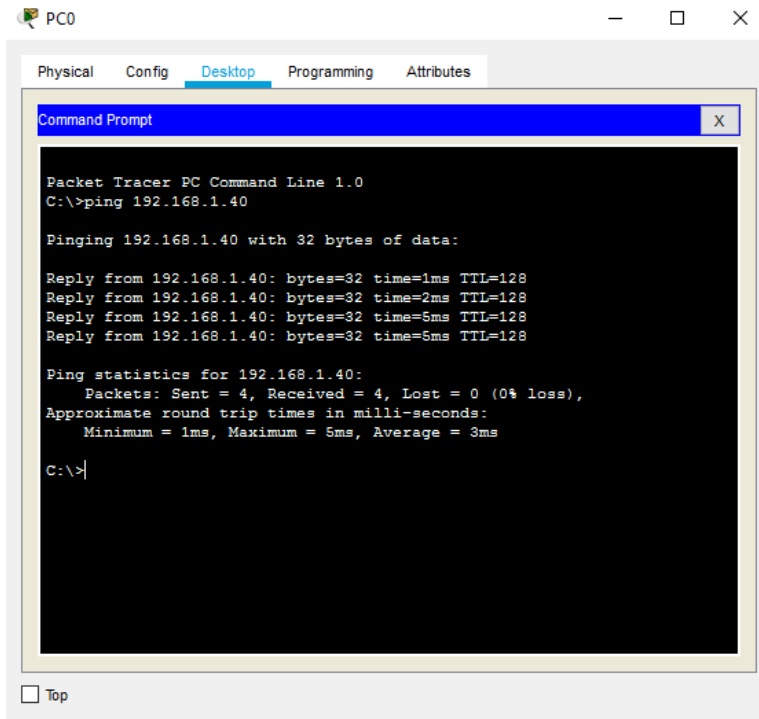
Actualmente no es posible verificar el balanceo puesto que hasta aquí se lleva una configuración básica, por tanto se verificará al final.

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

Actualmente no es posible verificar el balanceo puesto que se lleva una configuración básica, por tanto se verificará al final.

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

Imagen 2. PC0 – PC1



The screenshot shows a Packet Tracer PC Command Line window for PC0. The window title is "Command Prompt" and it has a close button (X). The text inside the window is as follows:

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.40

Pinging 192.168.1.40 with 32 bytes of data:

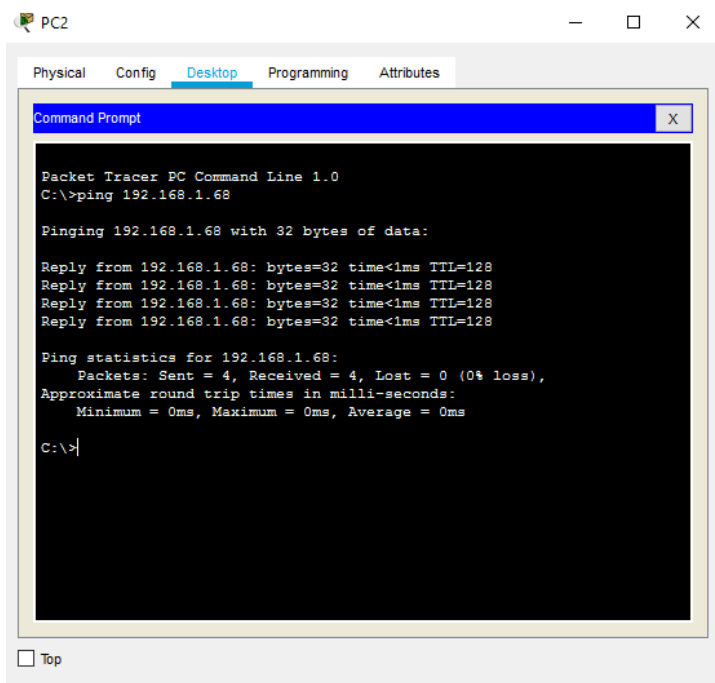
Reply from 192.168.1.40: bytes=32 time=1ms TTL=128
Reply from 192.168.1.40: bytes=32 time=2ms TTL=128
Reply from 192.168.1.40: bytes=32 time=5ms TTL=128
Reply from 192.168.1.40: bytes=32 time=5ms TTL=128

Ping statistics for 192.168.1.40:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 5ms, Average = 3ms

C:\>|
```

At the bottom left of the window, there is a "Top" button.

Imagen 3. PC2 – PC3



The screenshot shows a Packet Tracer PC Command Line window for PC2. The window title is "Command Prompt" and it has a close button (X). The text inside the window is as follows:

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.68

Pinging 192.168.1.68 with 32 bytes of data:

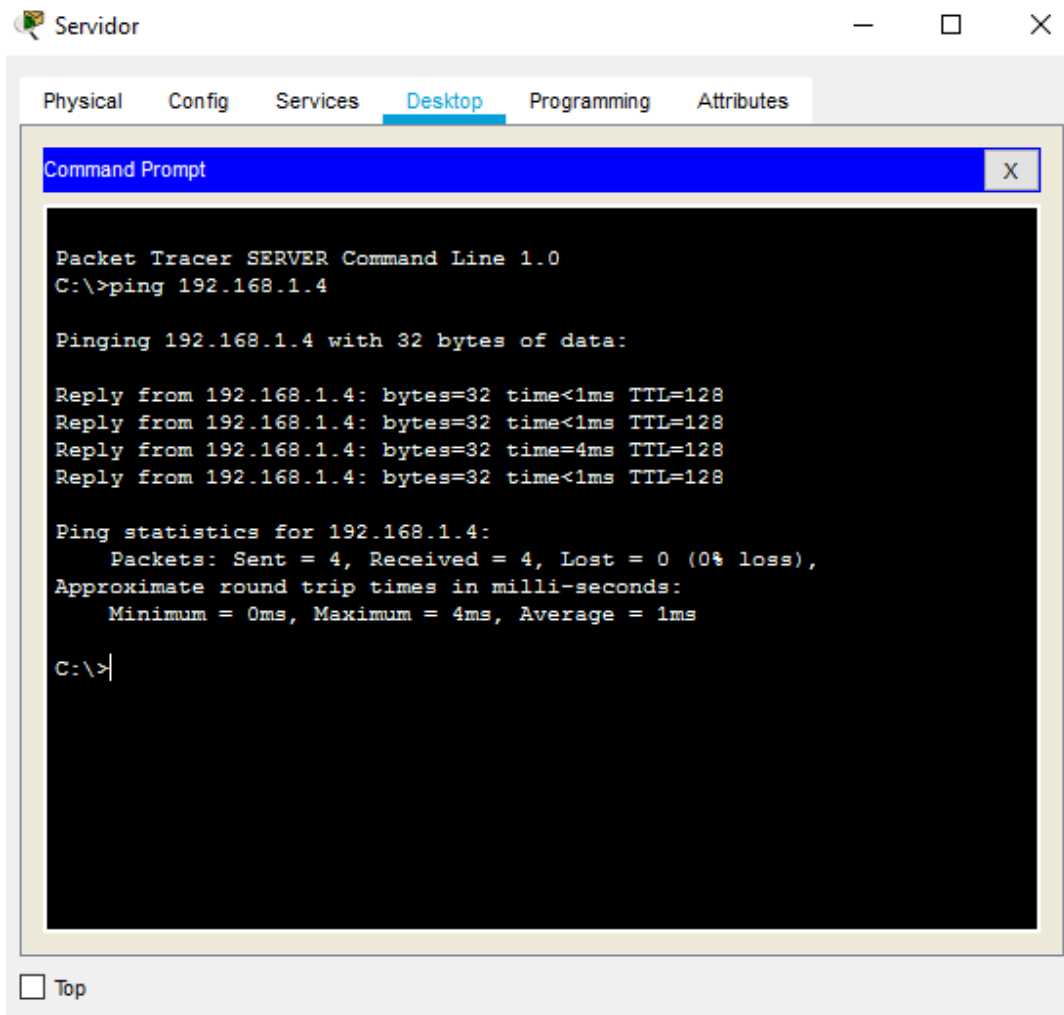
Reply from 192.168.1.68: bytes=32 time<1ms TTL=128
Reply from 192.168.1.68: bytes=32 time<1ms TTL=128
Reply from 192.168.1.68: bytes=32 time<1ms TTL=128
Reply from 192.168.1.68: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.68:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>|
```

At the bottom left of the window, there is a "Top" button.

Imagen 4. SERVIDOR – WS 1



Parte 3: Configuración de Enrutamiento.

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

BOGOTA

```
BOGOTA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA(config)#router eigrp 1
BOGOTA(config-router)#network 192.168.1.0 0.0.0.31
BOGOTA(config-router)#network 192.168.1.96 0.0.0.31
BOGOTA(config-router)#network 192.168.1.128 0.0.0.31
BOGOTA(config-router)#
```

MEDELLIN

```
MEDELLIN(config)#router eigrp 1
MEDELLIN(config-router)#network 192.168.1.32 0.0.0.31
MEDELLIN(config-router)#network 192.168.1.96 0.0.0.31
MEDELLIN(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 192.168.1.98 (Serial0/0/0) is up: new
adjacency

MEDELLIN(config-router)#passive-interface fa0/0
MEDELLIN(config-router)#no auto-summary
MEDELLIN(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 192.168.1.98 (Serial0/0/0) resync:
summary configured

MEDELLIN(config-router)#
```


CALI

```
CALI(config)#router eigrp 1
CALI(config-router)#network 192.168.1.64 0.0.0.31
CALI(config-router)#network 192.168.1.128 0.0.0.31
CALI(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 192.168.1.130 (Serial0/0/0) is up: new adjacency
```

```
CALI(config-router)#passive-interface fa0/0
CALI(config-router)#no auto-summary
CALI(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 192.168.1.130 (Serial0/0/0) resync: summary configured
```

```
CALI(config-router)#
```

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

BOGOTA

```
BOGOTA#show cdp neighbors detail
```

```
Device ID: Switch
```

```
Entry address(es):
```

```
Platform: cisco 2960, Capabilities: Switch
```

```
Interface: FastEthernet0/0, Port ID (outgoing port): FastEthernet0/1
```

```
Holdtime: 159
```

```
Version :
```

```
Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version 12.2(25)FX,
RELEASE SOFTWARE (fc1)
```

```
Copyright (c) 1986-2005 by Cisco Systems, Inc.
```

```
Compiled Wed 12-Oct-05 22:05 by pt_team
```

```
advertisement version: 2
```

```
Duplex: full
```

```
-----
```

```
Device ID: MEDELLIN
```

```
Entry address(es):
```

*IP address : 192.168.1.99
Platform: cisco C1841, Capabilities: Router
Interface: Serial0/0/0, Port ID (outgoing port): Serial0/0/0
Holdtime: 172*

*Version :
Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version
12.4(15)T1, RELEASE SOFTWARE (fc2)
Technical Support: <http://www.cisco.com/techsupport>
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 04:52 by pt_team*

*advertisement version: 2
Duplex: full*

*Device ID: CALI
Entry address(es):
IP address : 192.168.1.131
Platform: cisco C1841, Capabilities: Router
Interface: Serial0/0/1, Port ID (outgoing port): Serial0/0/0
Holdtime: 130*

*Version :
Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version
12.4(15)T1, RELEASE SOFTWARE (fc2)
Technical Support: <http://www.cisco.com/techsupport>
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 04:52 by pt_team*

*advertisement version: 2
Duplex: full*

BOGOTA#

MEDELLIN

MEDELLIN#show cdp neighbors detail

*Device ID: Switch
Entry address(es):*

Platform: cisco 2960, Capabilities: Switch
Interface: FastEthernet0/0, Port ID (outgoing port): FastEthernet0/1
Holdtime: 149

Version :
Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version 12.2(25)FX,
RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Wed 12-Oct-05 22:05 by pt_team

advertisement version: 2
Duplex: full

Device ID: BOGOTA
Entry address(es):
IP address : 192.168.1.98
Platform: cisco C1841, Capabilities: Router
Interface: Serial0/0/0, Port ID (outgoing port): Serial0/0/0
Holdtime: 136

Version :
Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version
12.4(15)T1, RELEASE SOFTWARE (fc2)
Technical Support: <http://www.cisco.com/techsupport>
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 04:52 by pt_team

advertisement version: 2
Duplex: full

MEDELLIN#

CALI

CALI#show cdp neighbors detail

Device ID: Switch
Entry address(es):
Platform: cisco 2960, Capabilities: Switch
Interface: FastEthernet0/0, Port ID (outgoing port): FastEthernet0/1

Holdtime: 167

Version :

Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version 12.2(25)FX, RELEASE SOFTWARE (fc1)

Copyright (c) 1986-2005 by Cisco Systems, Inc.

Compiled Wed 12-Oct-05 22:05 by pt_team

advertisement version: 2

Duplex: full

Device ID: BOGOTA

Entry address(es):

IP address : 192.168.1.130

Platform: cisco C1841, Capabilities: Router

Interface: Serial0/0/0, Port ID (outgoing port): Serial0/0/1

Holdtime: 136

Version :

Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version 12.4(15)T1, RELEASE SOFTWARE (fc2)

Technical Support: <http://www.cisco.com/techsupport>

Copyright (c) 1986-2007 by Cisco Systems, Inc.

Compiled Wed 18-Jul-07 04:52 by pt_team

advertisement version: 2

Duplex: full

CALI#

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

BOGOTA

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, 00:04:35, Serial0/0/0
D 192.168.1.64 [90/2172416] via 192.168.1.131, 00:02:52, 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

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, 00:03:45, 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, 00:04:14, 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, 00:05:57, Serial0/0/0*

MEDELLIN#

*%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 192.168.1.98 (Serial0/0/0) is down:
holding time expired*

MEDELLIN#

%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 192.168.1.98 (Serial0/0/0) is up: new adjacency

MEDELLIN#

%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 192.168.1.98 (Serial0/0/0) is resync: graceful restart

MEDELLIN#

CALI

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, 00:04:55, Serial0/0/0
D 192.168.1.32 [90/2684416] via 192.168.1.130, 00:05:24, 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, 00:05:24, Serial0/0/0
C 192.168.1.128 is directly connected, Serial0/0/0

CALI#

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

Imagen 5. prueba a la red de MEDELLIN

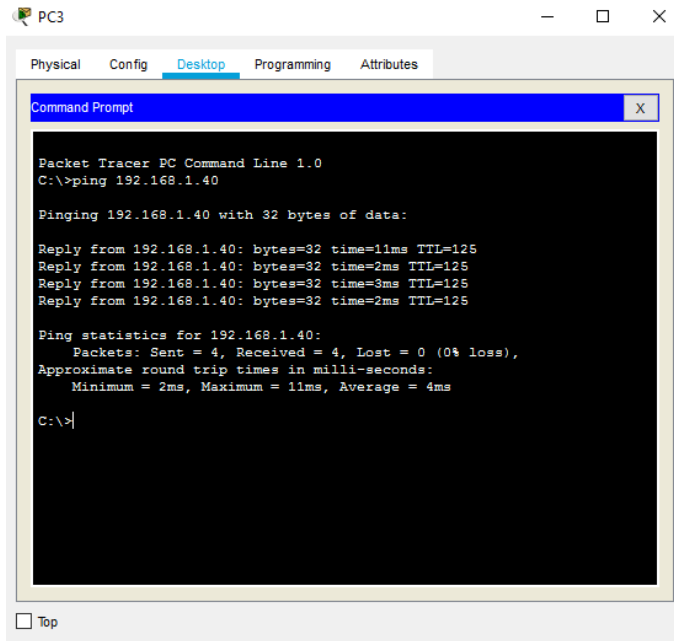
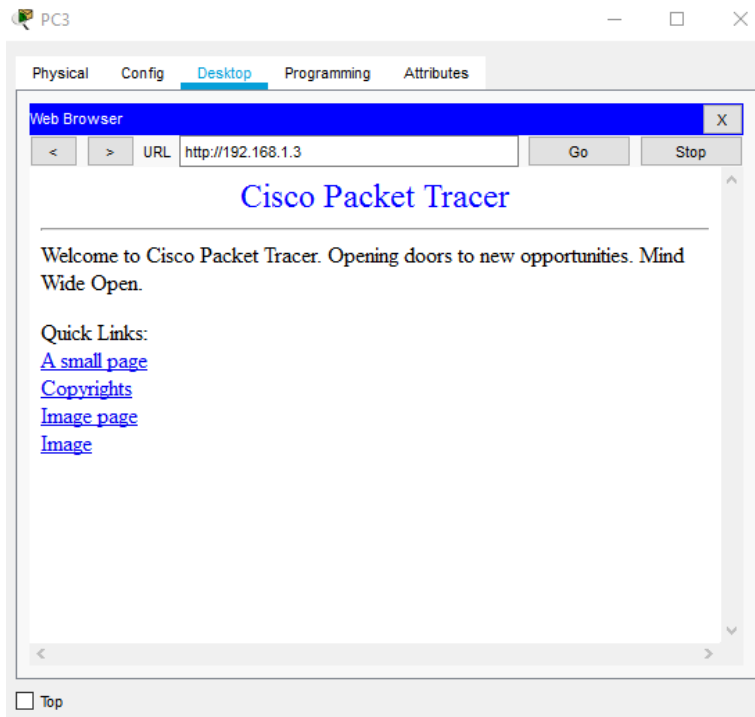


Imagen 6. prueba al servidor



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.

BOGOTA

```
BOGOTA#telnet 192.168.1.33
```

```
Trying 192.168.1.33 ...Open
```

```
-----  
-----
```

```
Prohibido el acceso a personal no autorizado!!!
```

```
-----  
-----
```

User Access Verification

Password:

```
MEDELLIN>exit
```

```
[Connection to 192.168.1.33 closed by foreign host]
```

```
BOGOTA#telnet 192.168.1.65
```

```
Trying 192.168.1.65 ...Open
```

```
-----  
-----
```

```
Prohibido el acceso a personal no autorizado
```

```
-----  
-----
```

User Access Verification

Password:

```
CALI>
```


MEDELLIN

MEDELLIN#telnet 192.168.1.65

Trying 192.168.1.65 ... Open

Prohibido el acceso a personal no autorizado

User Access Verification

Password:

CALI>exit

[Connection to 192.168.1.65 closed by foreign host]

MEDELLIN#telnet 192.168.1.1

Trying 192.168.1.1 ... Open

Prohibido el acceso a personal no autorizado!!!

User Access Verification

Password:

BOGOTA>

CALI

CALI#telnet 192.168.1.33

Trying 192.168.1.33 ... Open

Prohibido el acceso a personal no autorizado!!!

User Access Verification

Password:
MEDELLIN>exit

[Connection to 192.168.1.33 closed by foreign host]
CALI#telnet 192.168.1.1
Trying 192.168.1.1 ... Open

Prohibido el acceso a personal no autorizado!!!

User Access Verification

Password:
BOGOTA>

- a. 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

```
BOGOTA(config)#access-list 1 deny 192.168.1.4
BOGOTA(config)#access-list 1 permit 192.168.1.3
BOGOTA(config)#exit
BOGOTA#
%SYS-5-CONFIG_I: Configured from console by console
```

```
BOGOTA#show access-list
Standard IP access list 1
10 deny host 192.168.1.4
```

20 permit host 192.168.1.3

BOGOTA#conf t

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

BOGOTA(config)#int fa0/0

BOGOTA(config-if)#ip access-group 1 in

BOGOTA(config-if)#

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

MEDELLIN(config)#access-list 104 permit ip host 192.168.1.40 192.168.1.3 0.0.0.31

MEDELLIN(config)#access-list 104 permit ip host 192.168.1.41 192.168.1.3 0.0.0.31

MEDELLIN(config-if)#ip access-group 104 in

MEDELLIN(config)#

CALI

CALI(config)#access-list 105 permit ip host 192.168.1.67 192.168.1.3 0.0.0.31

CALI(config)#access-list 105 permit ip host 192.168.1.68 192.168.1.3 0.0.0.31

CALI(config)#int fa0/0

CALI(config-if)#ip access-group 105 in

CALI(config-if)#

Parte 5: Comprobación de la red instalada.

- Se debe probar que la configuración de las listas de acceso fue exitosa.
- Comprobar y Completar la siguiente tabla de condiciones de prueba para confirmar el óptimo funcionamiento de la red e.

Tabla 6. Comprobación de la red instalada.

	ORIGEN	DESTINO	RESULTADO
TELNET	Router MEDELLIN	Router CALI	CONEXION
	WS_1	Router BOGOTA	DESCONEXION
	Servidor	Router CALI	CONEXIÓN
	Servidor	Router MEDELLIN	CONEXION
TELNET	LAN del Router MEDELLIN	Router CALI	DESCONEXION
	LAN del Router CALI	Router CALI	DESCONEXION

	LAN del Router MEDELLIN	Router MEDELLIN	DESCONEXION
	LAN del Router CALI	Router MEDELLIN	DESCONEXION
PING	LAN del Router CALI	WS_1	DESCONEXION
	LAN del Router MEDELLIN	WS_1	DESCONEXION
	LAN del Router MEDELLIN	LAN del Router CALI	DESCONEXIÓN
PING	LAN del Router CALI	Servidor	CONEXIÓN
	LAN del Router MEDELLIN	Servidor	CONEXIÓN
	Servidor	LAN del Router MEDELLIN	CONEXIÓN
	Servidor	LAN del Router CALI	CONEXIÓN
	Router CALI	LAN del Router MEDELLIN	DESCONEXION

TELNET

Imagen 7. Router MEDELLIN - Router CALI

```

MEDELLIN
Physical Config CLI Attributes
IOS Command Line Interface

User Access Verification
Password:
Password:
Password:
MEDELLIN>en
Password:
MEDELLIN#telnet 192.168.1.131
Trying 192.168.1.131 ...Open
-----
Prohibido el acceso a personal no autorizado
-----

User Access Verification
Password:
CALI#

```

Ctrl+F6 to exit CLI focus Copy Paste

Top

Imagen 8. WS_1 - Router BOGOTA

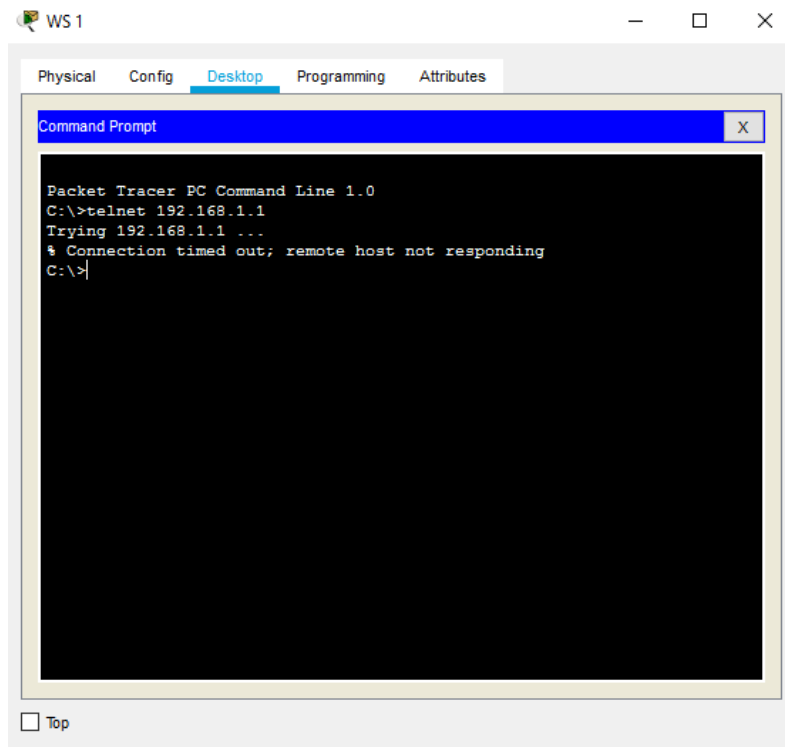


Imagen 9. Servidor - Router CALI

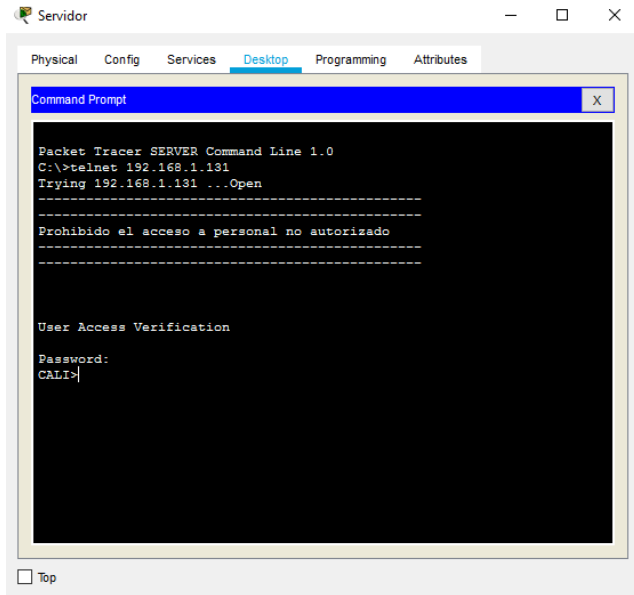


Imagen 10. Servidor - Router MEDELLIN

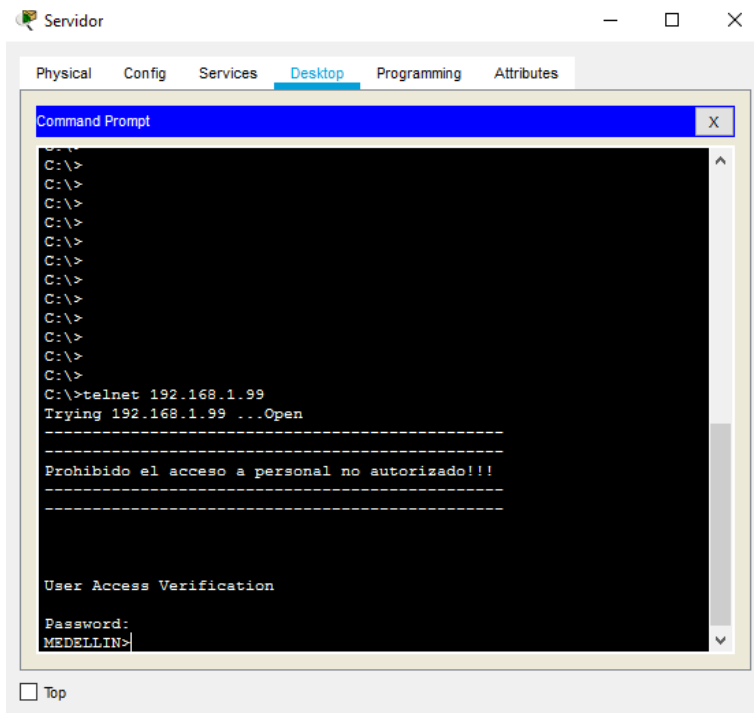


Imagen 11. LAN del Router MEDELLIN- Router CALI

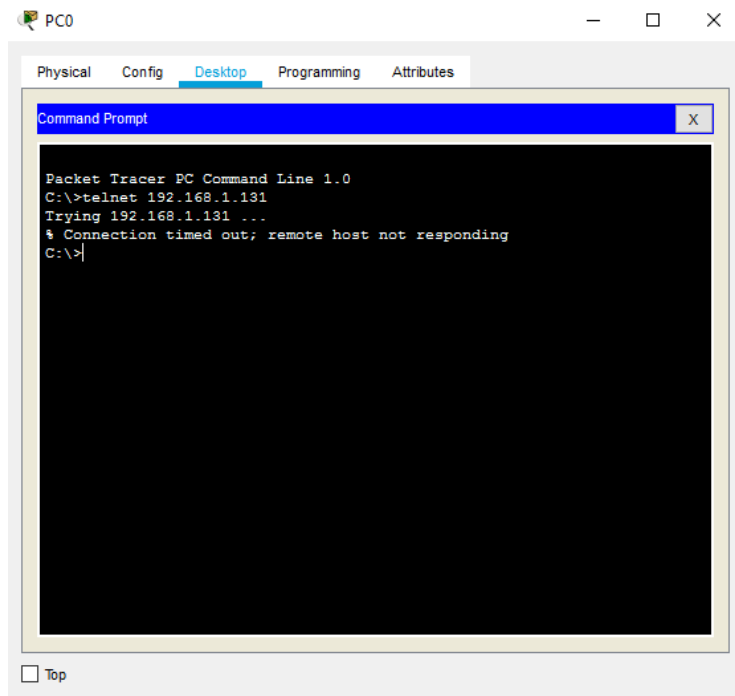


Imagen 12. LAN del Router CALI - Router CALI

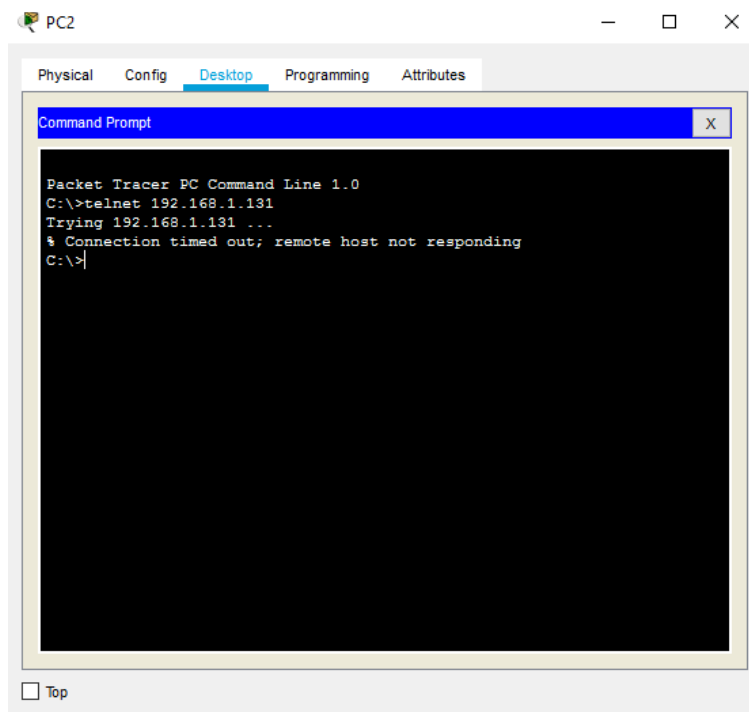


Imagen 13. LAN del Router MEDELLIN - Router MEDELLIN

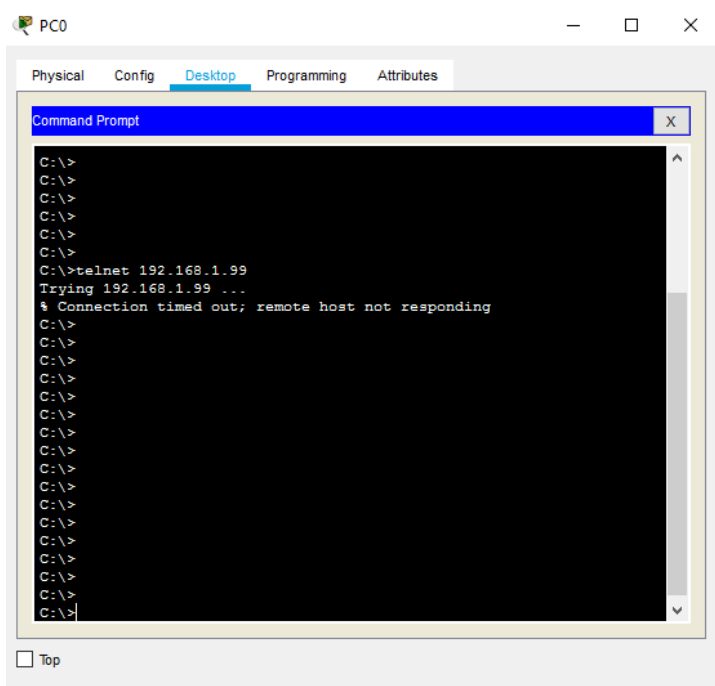
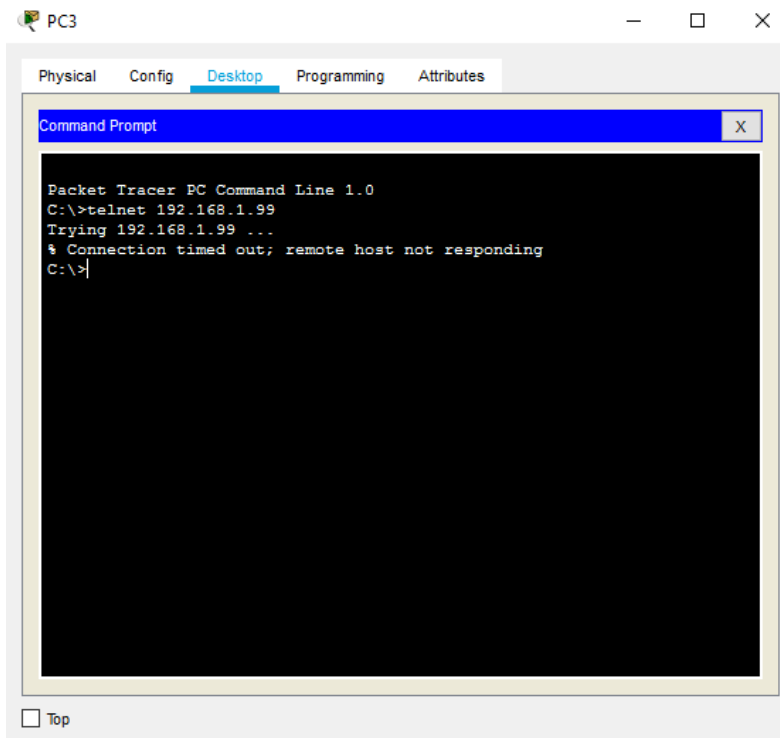


Imagen 14. LAN del Router CALI - Router MEDELLIN



PING

Imagen 15. LAN del Router CALI- WS_1

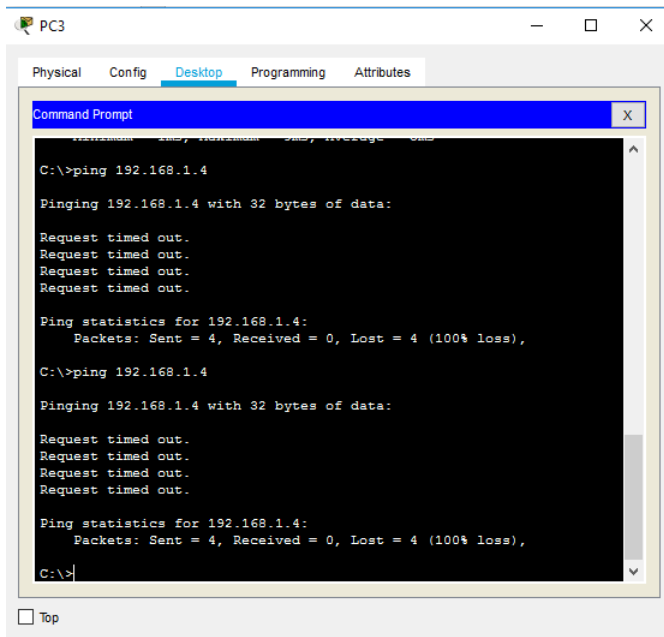


Imagen 16. LAN del Router MEDELLIN - WS_1

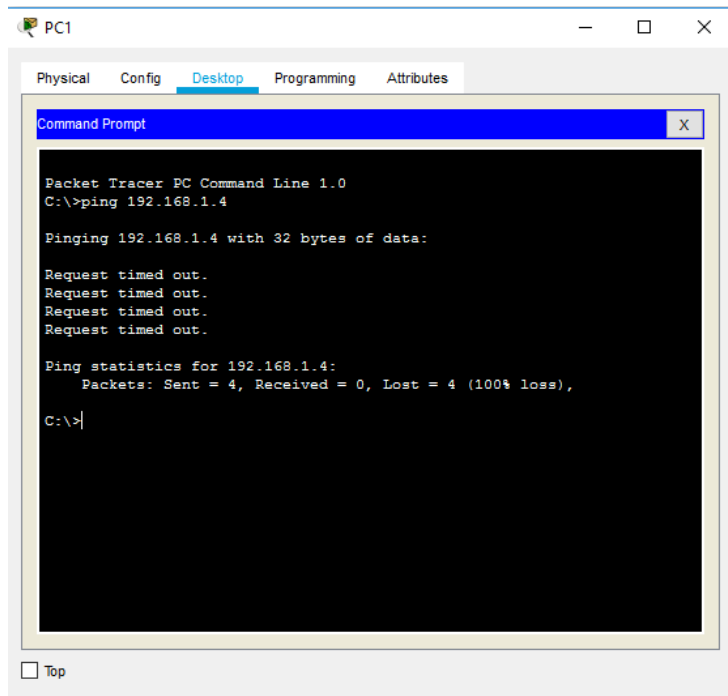


Imagen 17. LAN del Router MEDELLIN - LAN del Router CALI

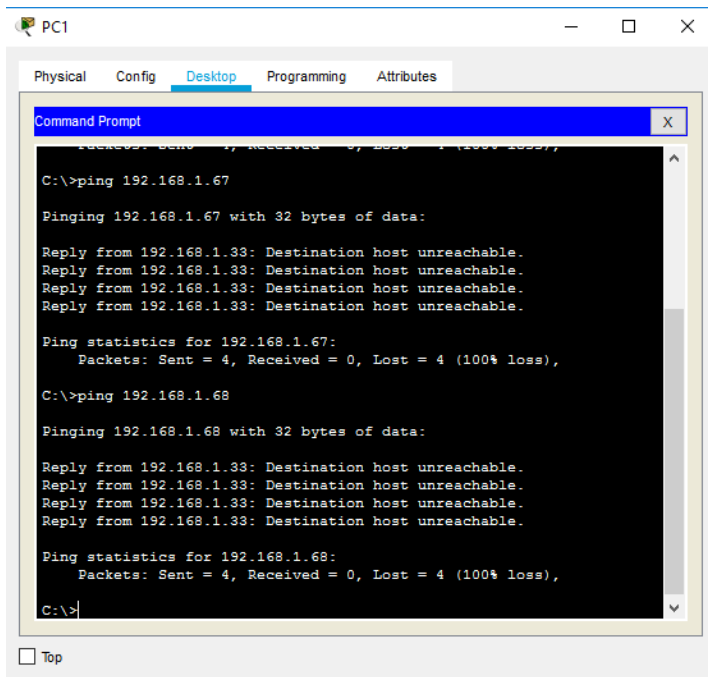


Imagen 18. LAN del Router CALI – Servidor

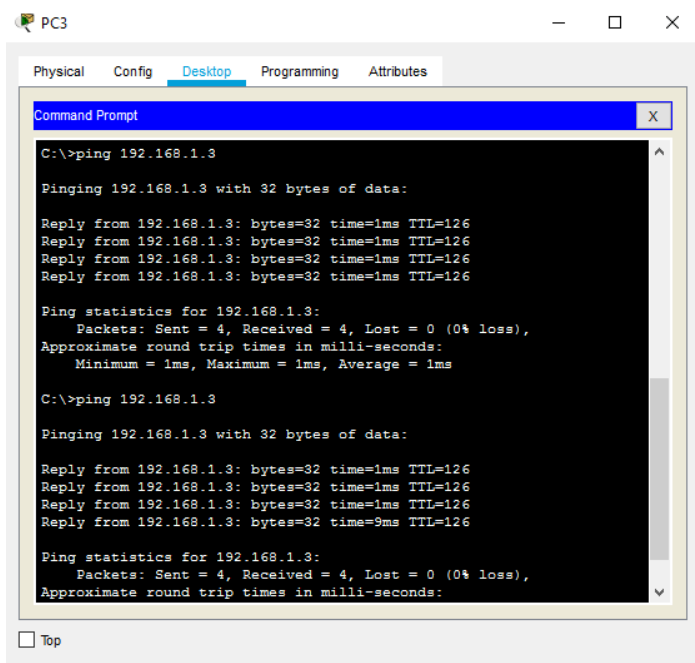
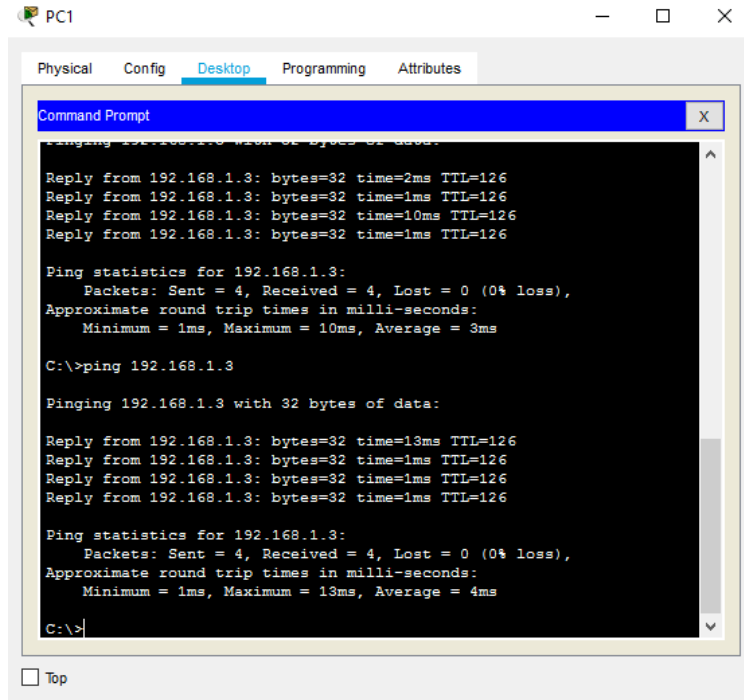


Imagen 19. LAN del Router MEDELLIN – Servidor

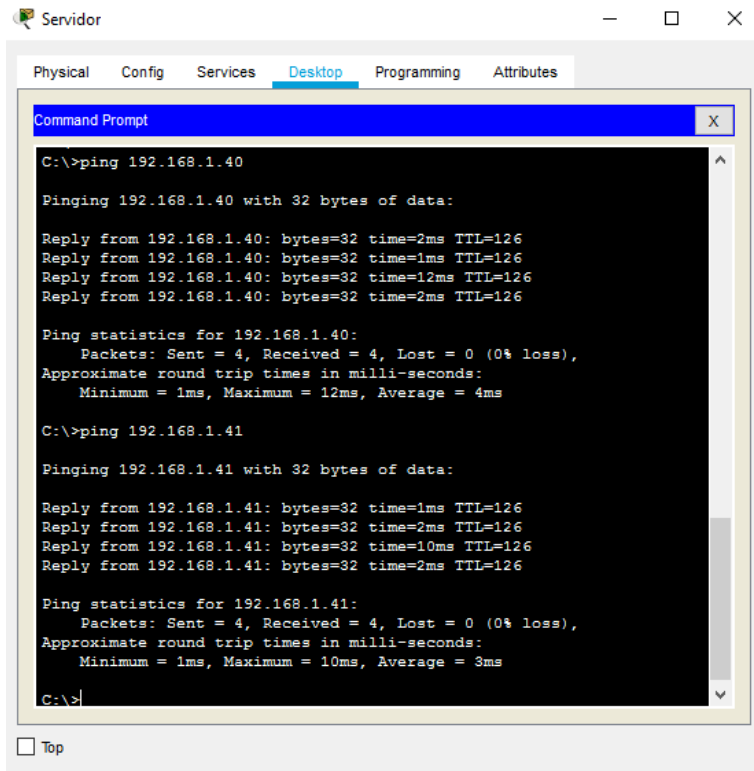


The image shows a screenshot of a PC1 desktop environment. The desktop has a taskbar with icons for PC1 and window controls. A window titled 'Command Prompt' is open, displaying the output of a ping command. The window has tabs for 'Physical', 'Config', 'Desktop', 'Programming', and 'Attributes'. The Command Prompt shows the following text:

```
Pinging 192.168.1.3 with 32 bytes of data:  
Reply from 192.168.1.3: bytes=32 time=2ms TTL=126  
Reply from 192.168.1.3: bytes=32 time=1ms TTL=126  
Reply from 192.168.1.3: bytes=32 time=10ms TTL=126  
Reply from 192.168.1.3: bytes=32 time=1ms TTL=126  
  
Ping statistics for 192.168.1.3:  
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
Minimum = 1ms, Maximum = 10ms, Average = 3ms  
  
C:\>ping 192.168.1.3  
  
Pinging 192.168.1.3 with 32 bytes of data:  
  
Reply from 192.168.1.3: bytes=32 time=13ms TTL=126  
Reply from 192.168.1.3: bytes=32 time=1ms TTL=126  
Reply from 192.168.1.3: bytes=32 time=1ms TTL=126  
Reply from 192.168.1.3: bytes=32 time=1ms TTL=126  
  
Ping statistics for 192.168.1.3:  
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
Minimum = 1ms, Maximum = 13ms, Average = 4ms  
  
C:\>
```

At the bottom left of the window, there is a checkbox labeled 'Top' which is currently unchecked.

Imagen 20. Servidor - LAN del Router MEDELLIN



The image shows a window titled "Servidor" with a menu bar containing "Physical", "Config", "Services", "Desktop", "Programming", and "Attributes". The "Desktop" tab is active, displaying a "Command Prompt" window. The Command Prompt shows the following output:

```
C:\>ping 192.168.1.40

Pinging 192.168.1.40 with 32 bytes of data:

Reply from 192.168.1.40: bytes=32 time=2ms TTL=126
Reply from 192.168.1.40: bytes=32 time=1ms TTL=126
Reply from 192.168.1.40: bytes=32 time=12ms TTL=126
Reply from 192.168.1.40: bytes=32 time=2ms TTL=126

Ping statistics for 192.168.1.40:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 12ms, Average = 4ms

C:\>ping 192.168.1.41

Pinging 192.168.1.41 with 32 bytes of data:

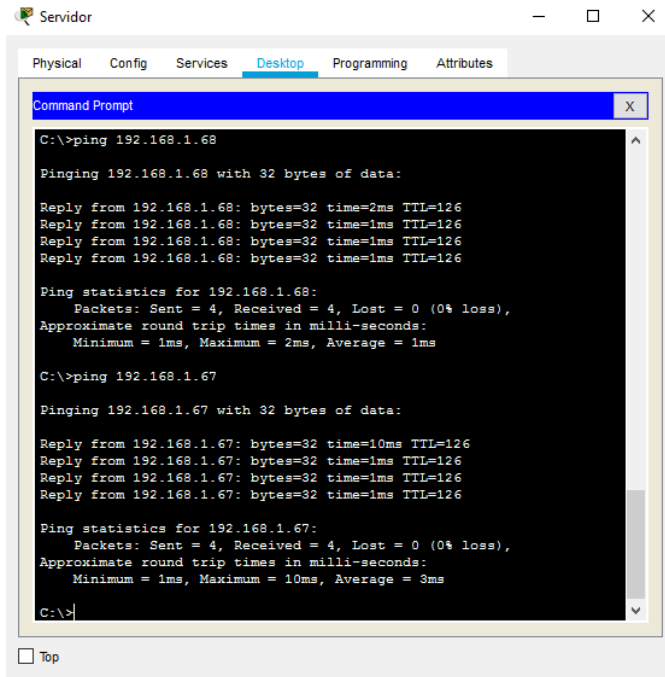
Reply from 192.168.1.41: bytes=32 time=1ms TTL=126
Reply from 192.168.1.41: bytes=32 time=2ms TTL=126
Reply from 192.168.1.41: bytes=32 time=10ms TTL=126
Reply from 192.168.1.41: bytes=32 time=2ms TTL=126

Ping statistics for 192.168.1.41:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 10ms, Average = 3ms

C:\>|
```

At the bottom left of the window, there is a checkbox labeled "Top" which is currently unchecked.

Imagen 21. Servidor - LAN del Router CALI



Servidor

Physical Config Services **Desktop** Programming Attributes

```
Command Prompt
C:\>ping 192.168.1.68

Pinging 192.168.1.68 with 32 bytes of data:

Reply from 192.168.1.68: bytes=32 time=2ms TTL=126
Reply from 192.168.1.68: bytes=32 time=1ms TTL=126
Reply from 192.168.1.68: bytes=32 time=1ms TTL=126
Reply from 192.168.1.68: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.1.68:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\>ping 192.168.1.67

Pinging 192.168.1.67 with 32 bytes of data:

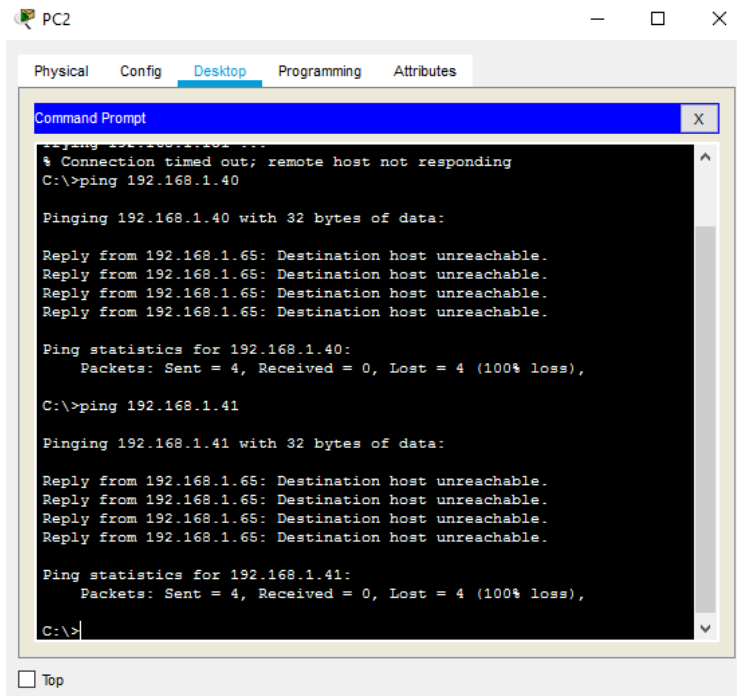
Reply from 192.168.1.67: bytes=32 time=10ms TTL=126
Reply from 192.168.1.67: bytes=32 time=1ms TTL=126
Reply from 192.168.1.67: bytes=32 time=1ms TTL=126
Reply from 192.168.1.67: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.1.67:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 10ms, Average = 3ms

C:\>
```

Top

Imagen 22. Router CALI LAN - del Router MEDELLIN



PC2

Physical Config **Desktop** Programming Attributes

```
Command Prompt
% Connection timed out; remote host not responding
C:\>ping 192.168.1.40

Pinging 192.168.1.40 with 32 bytes of data:

Reply from 192.168.1.65: Destination host unreachable.
Reply from 192.168.1.65: Destination host unreachable.
Reply from 192.168.1.65: Destination host unreachable.
Reply from 192.168.1.65: Destination host unreachable.

Ping statistics for 192.168.1.40:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.1.41

Pinging 192.168.1.41 with 32 bytes of data:

Reply from 192.168.1.65: Destination host unreachable.
Reply from 192.168.1.65: Destination host unreachable.
Reply from 192.168.1.65: Destination host unreachable.
Reply from 192.168.1.65: Destination host unreachable.

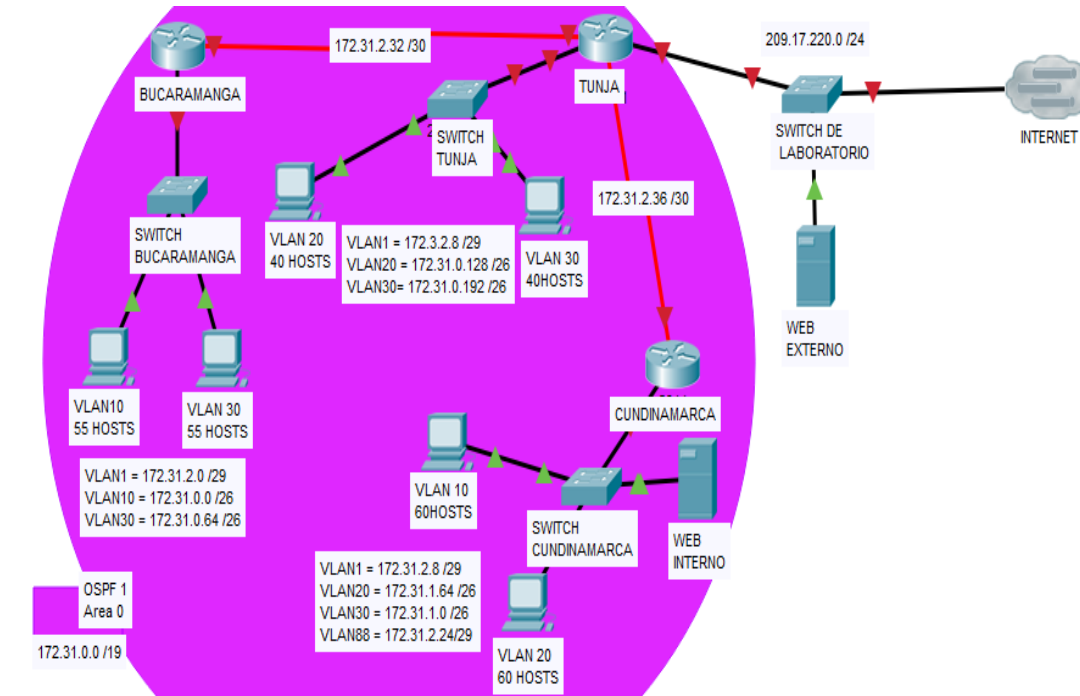
Ping statistics for 192.168.1.41:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Top

ESCENARIO 2

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



Desarrollo

Los siguientes son los requerimientos necesarios:

Todos los routers deberán tener los siguiente:

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

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

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

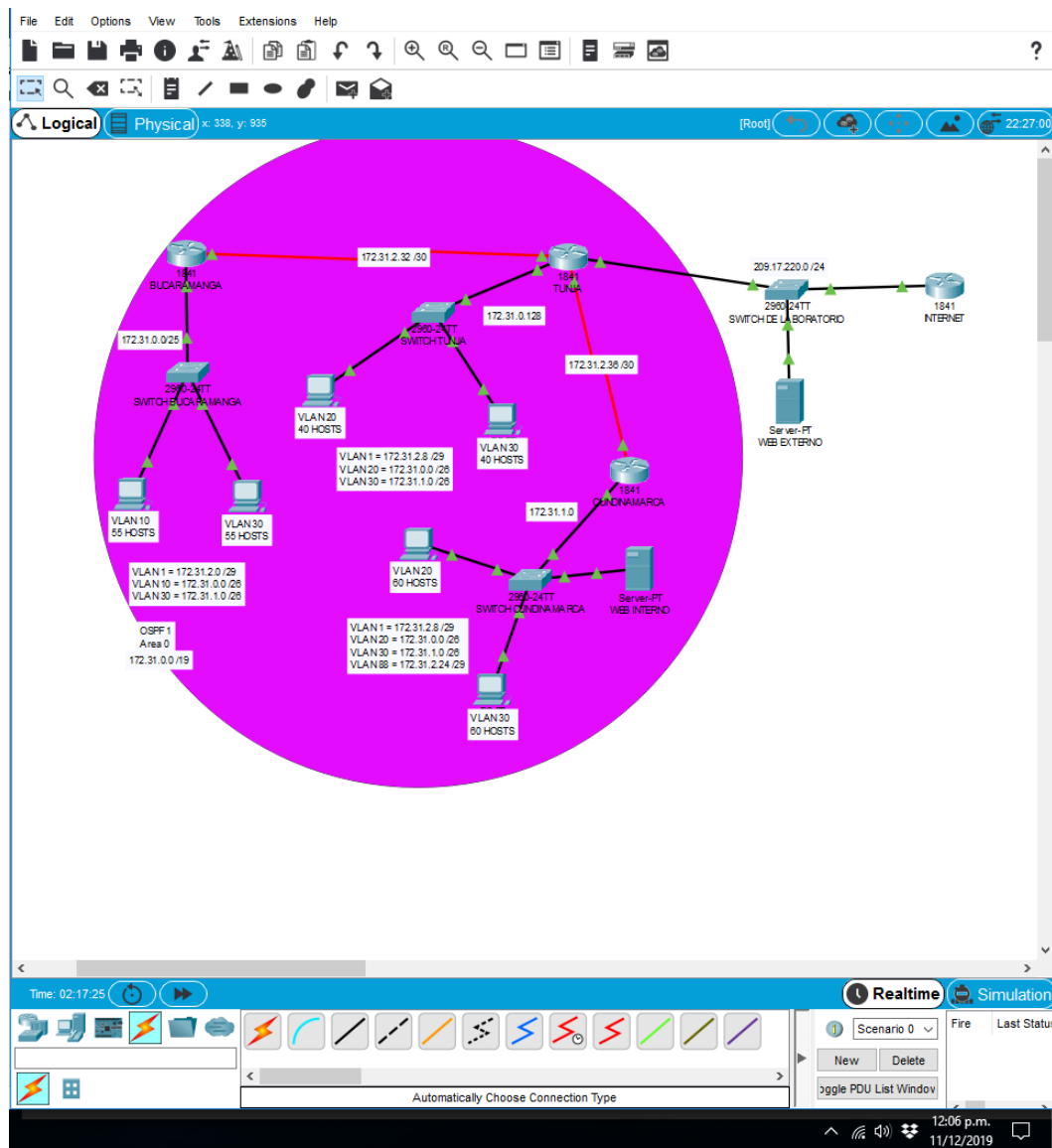
El enrutamiento deberá tener autenticación.

Listas de control de acceso:

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

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

Imagen 23.. DESARROLLO ESCENARIO 2



Aspectos en cuenta para el desarrollo del ejercicio 2

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

1. Todos los routers deberán tener los siguiente:

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

Router TUNJA

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname TUNJA
TUNJA(config)#no ip domain-lookup
TUNJA(config)#enable secret class
TUNJA(config)#username CISCO password CLASS
TUNJA(config)#aaa new-model
TUNJA(config)#aaa authentication login LOCAL local
TUNJA(config)#line console 0
TUNJA(config-line)#password cisco
TUNJA(config-line)#login authentication LOCAL
TUNJA(config-line)#line vty 0 15
TUNJA(config-line)#login authentication LOCAL
TUNJA(config-line)#password cisco
TUNJA(config-line)#exit
TUNJA(config)#banner motd #
Enter TEXT message. End with the character '#'.
-----
-----
Prohibido el acceso a personal no autorizado!!!
-----
-----
#

TUNJA(config)#service password-encryption
TUNJA(config)#line console 0
TUNJA(config-line)#exec-timeout 5 0
TUNJA(config-line)#line vty 0 15
```

```
TUNJA(config-line)#exec-timeout 5 0
TUNJA(config-line)#exit
TUNJA(config)#login block-for 300 attempt 3 within 60
TUNJA(config)#exit
TUNJA#
%SYS-5-CONFIG_1: Configured from console by console
```

```
TUNJA#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
TUNJA(config)#int fa0/0
TUNJA(config-if)#no ip address 209.17.220.3 255.255.255.0
TUNJA(config-if)#ip address 209.17.220.1 255.255.255.0
TUNJA(config-if)#exit
TUNJA(config)#int fa0/0
TUNJA(config-if)#ip address 172.31.0.129 255.255.255.128
TUNJA(config-if)#no shutdown
```

Router CUNDINAMARCA

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname CUNDINAMARCA
CUNDINAMARCA(config)#no ip domain-lookup
CUNDINAMARCA(config)#enable secret class
CUNDINAMARCA(config)#username CISCO password CLASS
CUNDINAMARCA(config)#aaa new-model
CUNDINAMARCA(config)#aaa authentication login LOCAL local
CUNDINAMARCA(config)#line console 0
CUNDINAMARCA(config-line)#password cisco
CUNDINAMARCA(config-line)#login authentication LOCAL
CUNDINAMARCA(config-line)#exec-timeout 5 0
CUNDINAMARCA(config-line)#line vty 0 15
CUNDINAMARCA(config-line)#login authentication LOCAL
CUNDINAMARCA(config-line)#password cisco
CUNDINAMARCA(config-line)#exec-timeout 5 0
CUNDINAMARCA(config-line)#exit
CUNDINAMARCA(config)#banner motd #
```

Enter TEXT message. End with the character '#'.

Prohibido el acceso a personal no autorizado!!!

#

CUNDINAMARCA(config)#service password-encryption
CUNDINAMARCA(config)#login block-for 300 attempt 3 within 60
CUNDINAMARCA(config)#exit
CUNDINAMARCA#
%SYS-5-CONFIG_1: Configured from console by console

CUNDINAMARCA#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
CUNDINAMARCA(config)#int s0/0/0
CUNDINAMARCA(config-if)#ip address 172.31.2.38 255.255.255.252
CUNDINAMARCA(config-if)#no shutdown
TUNJA(config)#int fa0/0
TUNJA(config-if)#ip address 209.17.220.4 255.255.255.0
TUNJA(config-if)#no shutdown
CUNDINAMARCA(config)#int fa0/1
CUNDINAMARCA(config-if)#ip address 172.31.1.1 255.255.255.128
CUNDINAMARCA(config-if)#no shutdown

Router BUCARAMANGA

Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname BUCARAMANGA
BUCARAMANGA(config)#no ip domain-lookup
BUCARAMANGA(config)#enable secret class
BUCARAMANGA(config)#username CISCO password CLASS
BUCARAMANGA(config)#aaa new-model
BUCARAMANGA(config)#aaa authentication login LOCAL local
BUCARAMANGA(config)#line console 0

```
BUCARAMANGA(config-line)#password cisco
BUCARAMANGA(config-line)#login authentication LOCAL
BUCARAMANGA(config-line)#exec-timeout 5 0
BUCARAMANGA(config-line)#line vty 0 15
BUCARAMANGA(config-line)#password cisco
BUCARAMANGA(config-line)#login authentication LOCAL
BUCARAMANGA(config-line)#exec-timeout 5 0
BUCARAMANGA(config-line)#exit
BUCARAMANGA(config)#banner motd #
Enter TEXT message. End with the character '#'.
-----
-----
```

```
Prohibido el acceso a personal no autorizado!!!
-----
-----
```

```
#
```

```
BUCARAMANGA(config)#service password-encryption
BUCARAMANGA(config)#login block-for 300 attempt 3 within 60
BUCARAMANGA(config)#exit
BUCARAMANGA#
%SYS-5-CONFIG_I: Configured from console by console
```

```
BUCARAMANGA#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
BUCARAMANGA(config)#int s0/0/0
BUCARAMANGA(config-if)#ip address 172.31.2.34 255.255.255.252
BUCARAMANGA(config-if)#no shutdown
BUCARAMANGA(config)#int fa0/0
BUCARAMANGA(config-if)#ip address 172.31.0.129 255.255.255.128
BUCARAMANGA(config-if)#no shutdown
```


CUNDINAMARCA

```
CUNDINAMARCA(config)#ip nat pool NATCUND 172.31.2.37 172.31.2.38 netmask
255.255.255.252
CUNDINAMARCA(config)#access-list 1 permit 172.31.1.0 0.0.0.63
CUNDINAMARCA(config)#ip nat inside source list 1 pool NATCUND overload
CUNDINAMARCA(config)#access-list 2 permit 172.31.0.0 0.0.0.63
CUNDINAMARCA(config)#ip nat inside source list 2 pool NATCUND overload
CUNDINAMARCA(config)#int fa0/0
CUNDINAMARCA(config-if)#ip nat inside
CUNDINAMARCA(config-if)#int s0/0/0
CUNDINAMARCA(config-if)#ip nat outside
CUNDINAMARCA(config-if)#
```

BUCARAMANGA

```
BUCARAMANGA(config)#ip nat pool NATBUC 172.31.2.33 172.31.2.34 netmask
255.255.255.252
BUCARAMANGA(config)#access-list 1 permit 172.31.0.0 0.0.0.63
BUCARAMANGA(config)#access-list 2 permit 172.31.1.0 0.0.0.63
BUCARAMANGA(config)#ip nat inside source list 1 pool NATBUC overload
BUCARAMANGA(config)#ip nat inside source list 2 pool NATBUC overload
BUCARAMANGA(config)#int fa0/0
BUCARAMANGA(config-if)#ip nat inside
BUCARAMANGA(config-if)#int s0/0/0
BUCARAMANGA(config-if)#ip nat outside
```

```
CUNDINAMARCA(config)#access-list 100 deny ip host 172.31.0.1 200.17.220.2
0.0.0.255
CUNDINAMARCA(config)#access-list 100 permit ip host 172.31.0.1 172.31.0.20
0.0.0.63
CUNDINAMARCA(config)#access-list 100 permit ip host 172.31.0.1 172.31.1.15
0.0.0.63
CUNDINAMARCA(config)#int fa0/0
CUNDINAMARCA(config-if)#ip access-group 100 out
CUNDINAMARCA(config-if)#no shutdown
CUNDINAMARCA(config-if)#
CUNDINAMARCA(config)#access-list 102 permit ip host 172.31.0.2 200.17.220.2
0.0.0.255
CUNDINAMARCA(config)#access-list 102 deny ip host 172.31.0.2 172.31.0.20 0.0.0.63
CUNDINAMARCA(config)#access-list 102 deny ip host 172.31.0.2 172.31.1.15 0.0.0.63
```

```

CUNDINAMARCA(config)#int fa0/0
CUNDINAMARCA(config-if)#ip access-group 102 out
CUNDINAMARCA(config-if)#no shutdown
CUNDINAMARCA(config-if)#
TUNJA(config)#access-list 100 permit ip host 172.31.1.15 200.17.220.4 0.0.0.255
TUNJA(config)#access-list 100 permit tcp host 172.31.1.15 200.17.220.2 0.0.0.255
TUNJA(config)#int fa0/1
TUNJA(config-if)#ip access-group 100 out
TUNJA(config-if)#no shutdown
TUNJA(config-if)#
TUNJA(config)#access-list 101 permit ip host 172.31.0.20 172.31.0.2 0.0.0.63
TUNJA(config)#access-list 101 permit ip host 172.31.0.20 172.31.0.5 0.0.0.63
TUNJA(config)#int fa0/1
TUNJA(config-if)#ip access-group 101 out
TUNJA(config-if)#no shutdown
TUNJA(config-if)#
BUCARAMANGA(config)#access-list 100 permit ip host 172.31.1.5 200.17.220.2
0.0.0.255
BUCARAMANGA(config)#access-list 100 permit ip host 172.31.1.5 172.31.0.0 0.0.0.63
BUCARAMANGA(config)#int fa0/0
BUCARAMANGA(config-if)#ip access-group 100 out
BUCARAMANGA(config-if)#no shutdown
BUCARAMANGA(config-if)#
BUCARAMANGA(config)#access-list 101 deny ip host 172.31.0.5 200.17.220.2
0.0.0.255
BUCARAMANGA(config)#access-list 101 permit ip host 172.31.0.5 172.31.0.20 0.0.0.63
BUCARAMANGA(config)#access-list 101 permit ip host 172.31.0.5 172.31.0.2 0.0.0.63
BUCARAMANGA(config)#int fa0/0
BUCARAMANGA(config-if)#ip access-group 101 out
BUCARAMANGA(config-if)#no shutdown
BUCARAMANGA(config-if)#

```

CUNDINAMARCA

120 hosts = $2^7 = 128 - 2 = 126$
172.31.0.1/25 – 172.31.0.126/25

BUCARAMANGA

110 hosts = $2^7 = 128 - 2 = 126$
172.31.0.129/25 – 172.31.0.254/25

TUNJA

80 hosts = $2^7 = 128 - 2 = 126$

172.31.1.1/25 – 172.31.1.26/25

5. Listas de control de acceso:

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

TUNJA

```
Switch>en
```

```
Switch#conf t
```

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

```
Switch(config)#vlan 20
```

```
Switch(config-vlan)#exit
```

```
Switch(config)#vlan 30
```

```
Switch(config-vlan)#exit
```

```
Switch(config)#
```

```
Switch(config)#int range fa0/5-10
```

```
Switch(config-if-range)#switchport mode access
```

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

```
Switch(config-if-range)#exit
```

```
Switch(config)#int range fa0/15-20
```

```
Switch(config-if-range)#switchport mode access
```

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

```
Switch(config-if-range)#do wr
```

```
Building configuration...
```

[OK]

Switch(config-if-range)#

TUNJA(config)#int fa0/1.20

TUNJA(config-subif)#encapsulation dot1Q 20

TUNJA(config-subif)#ip address 172.31.0.1 255.255.255.192

TUNJA(config-subif)#no shutdown

TUNJA(config-subif)#int fa0/1.30

TUNJA(config-subif)#encapsulation dot1Q 30

TUNJA(config-subif)#ip address 172.31.1.1 255.255.255.192

TUNJA(config-subif)#no shutdown

TUNJA(config-subif)#

CUNDINAMARCA

Switch>en

Switch#conf t

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

Switch(config)#vlan 10

Switch(config-vlan)#exit

Switch(config)#vlan 20

Switch(config-vlan)#exit

Switch(config)#vlan 30

Switch(config-vlan)#exit

Switch(config)#vlan 88

Switch(config-vlan)#exit

Switch(config)#int range fa0/15-19

Switch(config-if-range)#switchport mode access

Switch(config-if-range)#switchport access vlan 20

Switch(config-if-range)#exit

Switch(config)#int range fa0/20-24

Switch(config-if-range)#switchport mode access

Switch(config-if-range)#switchport access vlan 10

Switch(config-if-range)#exit

Switch(config)#do wr

Building configuration...

[OK]

Switch(config)#

CUNDINAMARCA(config-if)#int fa0/0.20

CUNDINAMARCA(config-subif)#

%LINK-5-CHANGED: Interface FastEthernet0/0.20, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.20, changed state to up

*CUNDINAMARCA(config-subif)#encapsulation dot1Q 20
CUNDINAMARCA(config-subif)#ip address 172.31.0.1 255.255.255.192
CUNDINAMARCA(config-subif)#no shutdown
CUNDINAMARCA(config-subif)#int fa0/0.30
CUNDINAMARCA(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.30, changed state to up*

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.30, changed state to up

*CUNDINAMARCA(config-subif)#encapsulation dot1Q 30
CUNDINAMARCA(config-subif)#ip address 172.31.1.1 255.255.255.192
CUNDINAMARCA(config-subif)#no shutdown
CUNDINAMARCA(config-subif)#*

BUCARAMANGA

*Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#exit
Switch(config)#vlan 30
Switch(config-vlan)#exit
Switch(config)#int range f
%LINK-3-UPDOWN: Interface FastEthernet0/3, changed state to down*

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down

%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/24, changed state to up

% Incomplete command.

```
Switch(config)#int range fa0/2-5
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#do write
Building configuration...
[OK]
Switch(config-if-range)#exit
Switch(config)#int range fa0/20-24
Switch(config-if-range)#switchport access vlan 30
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 30
Switch(config-if-range)#exit
Switch(config)#int range fa0/2-4
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#exit
Switch(config)#
```

```
BUCARAMANGA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
BUCARAMANGA(config)#int fa0/0.10
BUCARAMANGA(config-subif)#encapsulation dot1Q 10
BUCARAMANGA(config-subif)#ip address 172.31.0.1 255.255.255.192
BUCARAMANGA(config-subif)#no shutdown
BUCARAMANGA(config-subif)#int fa0/0.30
BUCARAMANGA(config-subif)#encapsulation dot1Q 30
BUCARAMANGA(config-subif)#ip address 172.31.1.1 255.255.255.192
BUCARAMANGA(config-subif)#no shutdown
BUCARAMANGA(config-subif)#
```

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

TUNJA

```
TUNJA(config)#router ospf 1
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)#network 209.17.220.0 0.0.0.255 area 0
TUNJA(config-router)#exit
TUNJA(config)#int s0/0/0
TUNJA(config-if)#ip ospf authentication-key cisco
TUNJA(config-if)#ip ospf authentication
```

```
03:45:03: %OSPF-5-ADJCHG: Process 1, Nbr 172.31.2.34 on Serial0/0/0 from
LOADING to FULL, Loading Done
TUNJA(config-if)#int s0/0/1
TUNJA(config-if)#ip ospf authentication-key cisco
TUNJA(config-if)#ip ospf authentication
03:45:36: %OSPF-5-ADJCHG: Process 1, Nbr 172.31.2.38 on Serial0/0/1 from
LOADING to FULL, Loading Done
TUNJA(config-if)#exit
TUNJA(config)#
```

CUNDINAMARCA

```
CUNDINAMARCA(config)#router ospf 1
CUNDINAMARCA(config-router)#network 172.31.2.36 0.0.0.3 area 0
CUNDINAMARCA(config-router)#network 172.31.1.0 0.0.0.127 area 0
CUNDINAMARCA(config-router)#exit
CUNDINAMARCA(config)#int s0/0/0
CUNDINAMARCA(config-if)#ip ospf authentication-key cisco
CUNDINAMARCA(config-if)#ip ospf authentication
CUNDINAMARCA(config-if)#
```

BUCARAMANGA

```
BUCARAMANGA(config)#router ospf 1
BUCARAMANGA(config-router)#network 172.31.2.32 0.0.0.3 area 0
BUCARAMANGA(config-router)#network 172.31.0.0 0.0.0.127 area 0
BUCARAMANGA(config-router)#exit
BUCARAMANGA(config)#int s0/0/0
BUCARAMANGA(config-if)#ip ospf authentication-key cisco
BUCARAMANGA(config-if)#ip ospf authentication
BUCARAMANGA(config-if)#
```

CONCLUSIONES

De acuerdo con los contenidos vistos dentro del curso Diplomado de Profundización Cisco CCNA, se logra conceptualizar con claridad el término red, que es un conjunto de dispositivos conectados por medio de cables, ondas, señales, y demás métodos de transporte de datos para compartir información y servicios.

El uso de listas permite limitar el acceso o recibir paquetes desde otras redes.

Lista de Referencias

Acceso. (2017), Tomado de:

<https://staticcourseassets.s3.amazonaws.com/RSE503/es/index.html#9.0.1>

Benchimol, D. (2010). Redes Cisco-Instalacion y administracion de hardware y software. CISCO. (s.f.). Principios básicos de routing y switching: Listas de Control de Chamorro

Serna, L., Montaña Torres, O., Guzmán Pérez, E. H., Daza Navia, M.Y., & Castillo Ortiz, O. F. (2018). Diplomado de Profundización Cisco-Enrutamiento en soluciones de red.

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

Es.wikipedia.org. (2018). Open Shortest Path First. [online] disponible en:

https://es.wikipedia.org/wiki/Open_Shortest_Path_First

Principios básicos de routing y switching: Traducción de direcciones de red para IPv4. (2017), Tomado de:

<https://staticcourseassets.s3.amazonaws.com/RSE503/es/index.html#11.0>

Shaughnessy, T., Velte, T., & Sánchez García, J. I. (2000). Manual de CISCO.

Ariganello, E., & Sevilla, B. (2011). Redes CISCO - guía de estudio para la certificación CCNP (No. 004.6 A73).

Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). Implementing IPv4 in the Enterprise Network. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. Recuperado de

<https://1drv.ms/b/s!AmIJYei-NT1InMfy2rhPZHwEoWx>

Segui, F. B. (2015). Configuración DHCP en routers CISCO.

Se desarrollo en la herramienta de desarrollo PacketTracer-7.2.2-win64-

ANEXOS

Anexo 1

ESCENARIO 1

Link de desarrollo del ejercicio 1 para descargar desde la nube:

<https://drive.google.com/file/d/18-MOkF90mD4wdmqwt5swrRep7P0slaee/view?usp=sharing>

Anexo 2

ESCENARIO 2

Link de desarrollo del ejercicio 2 para descargar desde la nube:

https://drive.google.com/file/d/12B_jHp9EfnxXa9YZPa2Gh1kzoYeQt8Hs/view?usp=sharing