DIPLOMADO DE PROFUNDIZACIÓN CISCO - PRUEBA DE HABILIDADES PRÁCTICAS

PRESENTADO POR:
YENIS PAOLA BOLAÑO PASSO

PRESENTADO A:
GIOVANNI ALBERTO BRACHO

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
DICIEMBRE 2019

Tabla de contenido

1. Resumen

En el siguiente informa describe la importancia es se ha vuelto las TIC en nuestro diario vivir, que nos permite Sumergirnos en el funcionamiento de las redes de la información, también se describe las actividades realizadas acerca de la configuración de la Topología de Red que colocamos en práctica durante todo el proceso del desarrollo del Diplomado, en este informe se desarrollaran las pruebas de habilidades Prácticas para la aprobación de este, mediante la Universidad en convenio con Networking Academy CISCO, propone dos escenarios uno es respecto a una empresa que cuenta con tres sucursales distribuidas en las ciudades de Bogotá, Medellín y Cali, que se encuentras en lugares diferentes y la otra respecto a una empresa que tiene conexión a internet en una red Ethernet, la cual esta se debe adaptar para facilitar la conectividad entre estos a internet, esta activada de habilidades practicas se desarrolla mediante la herramienta Packet Tracer que nos permite realizar las configuraciones de los dispositivos basados en la topología propuesta en esta actividad, como lo es la configuración de enrutamiento con el protocolo EIGRP

2. Abstract

In the following report describes the importance of ICTs in our daily lives, which allows us to immerse ourselves in the operation of information networks, it also describes the activities carried out about the configuration of the Network Topology that we place in practice throughout the development process of the Diploma, in this report the skills tests will be developed Practices for the approval of this, through the University in agreement with Networking Academy CISCO, proposes two scenarios one is regarding a company that has three branches distributed in the cities of Bogotá, Medellin and Cali, which are located in different places and the other with respect to a company that has internet connection in an Ethernet network, which must be adapted to facilitate connectivity between them to the internet, this activated practical skills is developed using the Packet Tracer tool that allows us to perform the c Device configurations based on the topology proposed in this activity, such as the routing configuration with the EIGRP protocol

3. Introducción

En el desarrollo de la siguiente activada tiene como funcionalidad presentar y demostrar el aprendizaje adquirido durante el transcurso del Diplomado en Profundización CISCO CCNA, los escenarios resueltos corresponde a los conocimientos que adquirimos en el los capítulos del 1 al 11 del CCNA1 Y CCNA2, donde obtuvimos conocimientos respecto a Routing, VLAN, enrutamientos dinámicos DHCP, NAT, desarrollado estos en el simulador Packet Tracer ya que esta herramienta nos permitió desarrollar todas las actividades con facilidad que nos permitió aprender cómo usar y configurar desde redes pequeñas hasta grandes Internet Works.

Como finalización del diplomado se realiza esta actividad anexando como evidencia las líneas de códigos de configuración y pantallazos de los comandos SHOW utilizados para la funcionalidad y solución de las Topologías propuestas en los dos escenarios

4. Objetivos

4.1 Objetivo General

Este informe tiene como objetivo general realizar la implementación de las habilidades Teóricas, Prácticas adquiridas durante todo el proceso de este Diplomado, como futuros Ingenieros debemos afrontar y solucionar cualquier problemática que se nos presenten en nuestro ámbito laboral.

4.2 Objetivos Específicos

- Identificar y Realizar Topologías en las diferentes Herramientas como Packet Tracer
- Verificar que allá conectividad entre diferentes dispositivos de una topología
- Configuraciones de dispositivos como: Switch, Router, Pc, Servidores entre otros
- Configuraciones de contraseñas para la seguridad de la información o seguridad de la entidad
- Implementar DHCP Y NAT en dispositivos de comunicación
- Verificar y configurar las listas de control de acceso a los ACL

5. Desarrollo de los dos escenarios

Evaluación –Prueba de habilidades prácticas CCNA

Descripción general de la prueba de habilidades

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.

Para esta actividad, el estudiante dispone de cerca de dos semanas para realizar las tareas asignadas en cada uno de los **dos (2) escenarios propuestos**, acompañado de los respectivos procesos de documentación de la solución, correspondientes al registro de la configuración de cada uno de los dispositivos, la descripción detallada del paso a paso de cada una de las etapas realizadas durante su desarrollo, el registro de los procesos de verificación de conectividad mediante el uso de comandos **ping, traceroute, show ip route, entre otros.**

Teniendo en cuenta que la Prueba de habilidades está conformada por dos (2) escenarios, el estudiante deberá realizar el proceso de configuración de usando cualquiera de las siguientes herramientas: **Packet Tracer** o **GNS3**.

- Es muy importante mencionar que esta actividad es de carácter **INDIVIDUAL y OBLIGATORIA.**
- Toda evidencia de **copy-paste o plagio (de la web o de otros informes)** será penalizada con severidad.

Lineamientos para la elaboración del Informe

Finalmente, el informe a presentar deberá cumplir con las normas **ICONTEC 1486** para la presentación de trabajos escritos e incluir los siguientes elementos en su

- **Portada (**no registre su número de identificación**)**
- **Tabla de contenido**
- **Resumen**
- **Abstract**
- **Introducción**
- **Objetivos**
- **Desarrollo de los dos escenarios**
  IMPORTANTE: Para cada uno de los escenarios se debe describir el paso a paso de cada punto realizado y deben digitar el código de configuración aplicado (no incluir imágenes ni capturas de pantalla). Las imágenes o capturas de pantalla sólo serán usadas para evidenciar los resultados de comandos como **ping, traceroute, show ip route, entre otros.**
- **Conclusiones**
- **Bibliografía**

El informe deberá estar acompañado de las respectivas evidencias de configuración de los dispositivos (Packet Tracer ó GNS3), las cuales generarán veracidad al trabajo realizado. **El informe deberá ser entregado en el espacio creado para tal fin en el Campus**.

IMPORTANTE: Teniendo en cuenta que este documento deberá ser entregado al final del curso en el **Repositorio Institucional**, acorde con los lineamientos institucionales para grado. El procedimiento será socializado al finalizar el curso, pero puede ir revisando este link. (Lineamientos para el estudiante que carga trabajo de grado)

6. Escenario 1

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

Topología de red

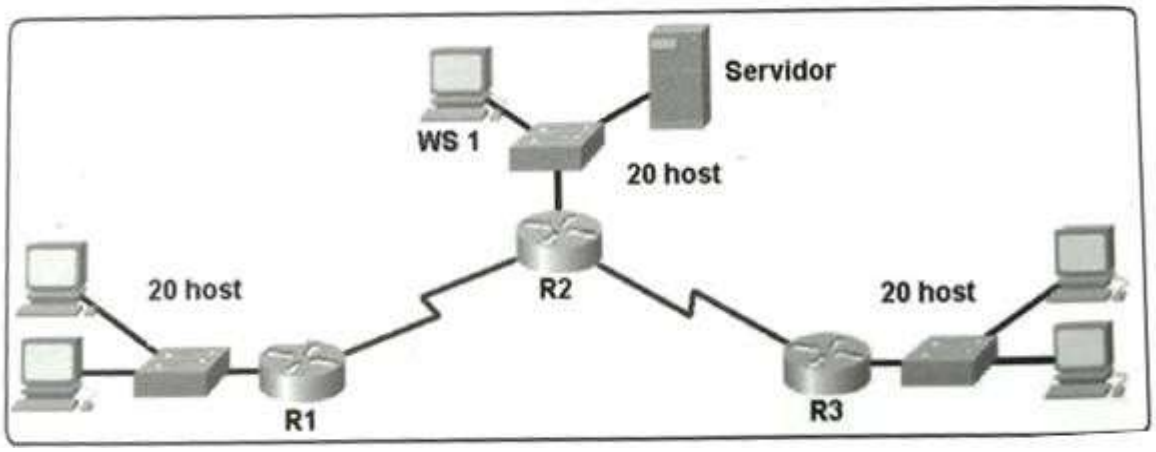
Los requerimientos solicitados son los siguientes:

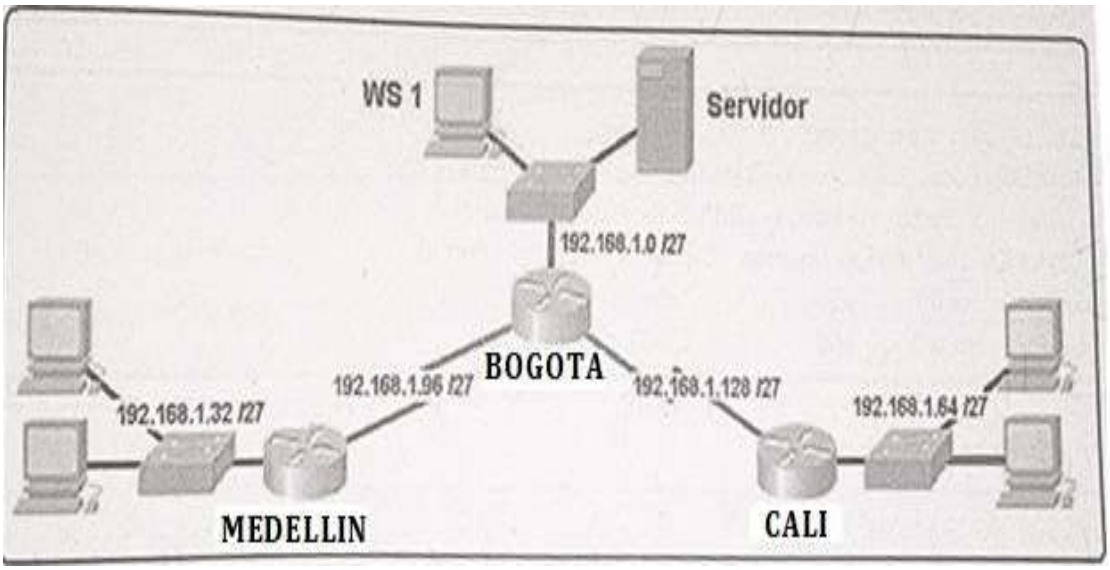
Parte 1: Para el direccionamiento IP debe definirse una dirección de acuerdo con el número de hosts requeridos.

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

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

Parte 4: Implementar la seguridad en la red, se debe restringir el acceso y comunicación entre hosts de acuerdo con los requerimientos del administrador de red.
Parte 5: Comprobación total de los dispositivos y su funcionamiento en la red. Parte 6: Configuración final.





Desarrollo

Como trabajo inicial se debe realizar lo siguiente.

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

7. 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.

RED	192.168.1.0	/27	RED	192.168.1.32	/27
PRIMERA IP	192.168.1.1	/27	PRIMERA IP	192.168.1.33	/27
ULTIMA IP	192.168.1.30	/27	ULTIMA IP	192.168.1.62	/27
BROADCAST	192.168.1.31	/27	BROADCAST	192.168.1.63	/27
RED	192.168.1.64	/27	RED	192.168.1.96	/27
PRIMERA IP	192.168.1.65	/27	PRIMERA IP	192.168.1.97	/27
ULTIMA IP	192.168.1.94	/27	ULTIMA IP	192.168.1.126	/27
BROADCAST	192.168.1.95	/27	BROADCAST	192.168.1.127	/27
RED	192.168.1.128	/27	RED	192.168.1.160	/27
PRIMERA IP	192.168.1.129	/27	PRIMERA IP	192.168.1.161	/27
ULTIMA IP	192.168.1.158	/27	ULTIMA IP	192.168.1.190	/27
BROADCAST	192.168.1.159	/27	BROADCAST	192.168.1.191	/27
RED	192.168.1.192	/27	RED	192.168.1.224	/27
PRIMERA IP	192.168.1.193	/27	PRIMERA IP	192.168.1.225	/27
ULTIMA IP	192.168.1.222	/27	ULTIMA IP	192.168.1.254	/27
BROADCAST	192.168.1.223	/27	BROADCAST	192.168.1.255	/27

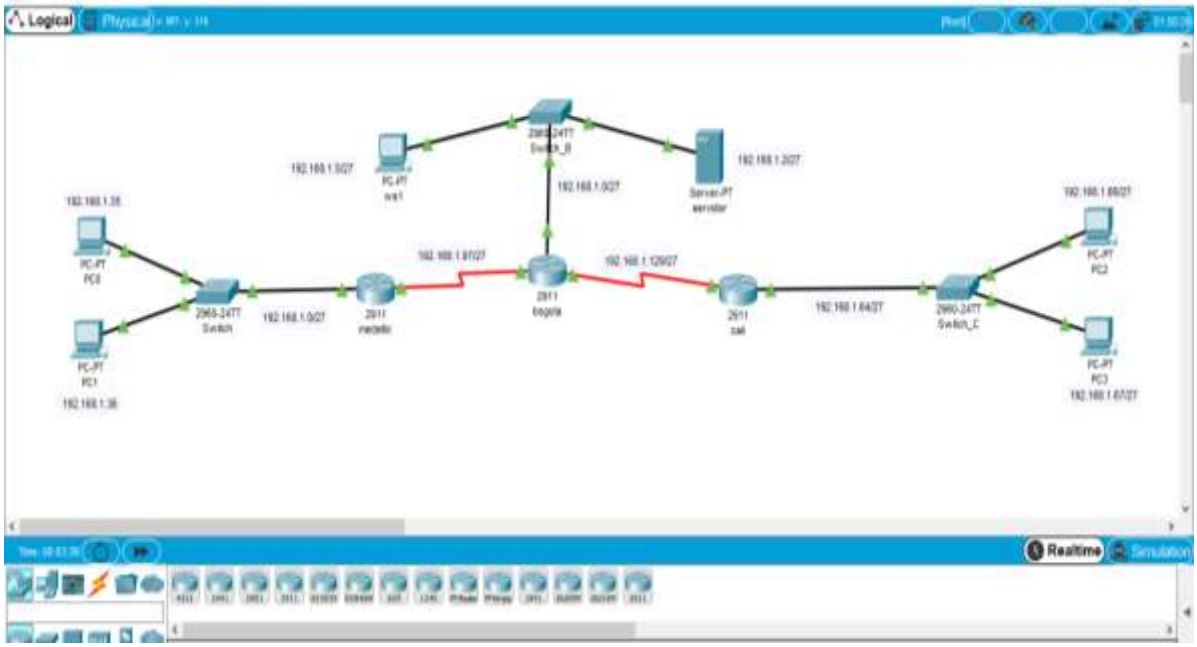
b. Asignar una dirección IP a la red.

192.168.1.0

8. Parte 2: Configuración Básica.

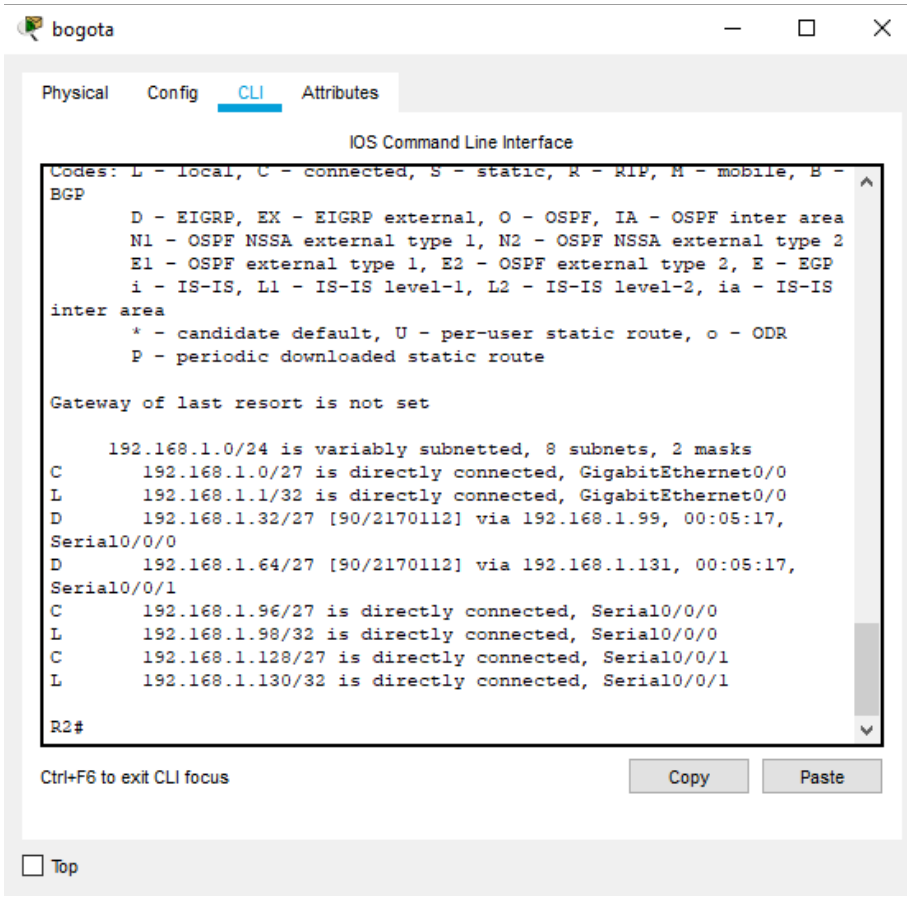
a. Completar la siguiente tabla con la configuración básica de los routers, teniendo en cuenta las subredes diseñadas.

	R1	R2	R3
Nombre de Host	**MEDELLIN**	**BOGOTA**	**CALI**
Dirección de Ip en interfaz Serial 0/0	192.168.1.99	192.168.1.98	192.168.1.131
Dirección de Ip en interfaz Serial 0/1		192.168.1.130	
Dirección de Ip en interfaz FA 0/0	192.168.1.33	192.168.1.1	192.168.1.65
Protocolo de enrutamiento	**Eigrp**	**Eigrp**	**Eigrp**
Sistema Autónomo	200	200	200
Afirmaciones de red	192.168.1.0	192.168.1.0	192.168.1.0



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

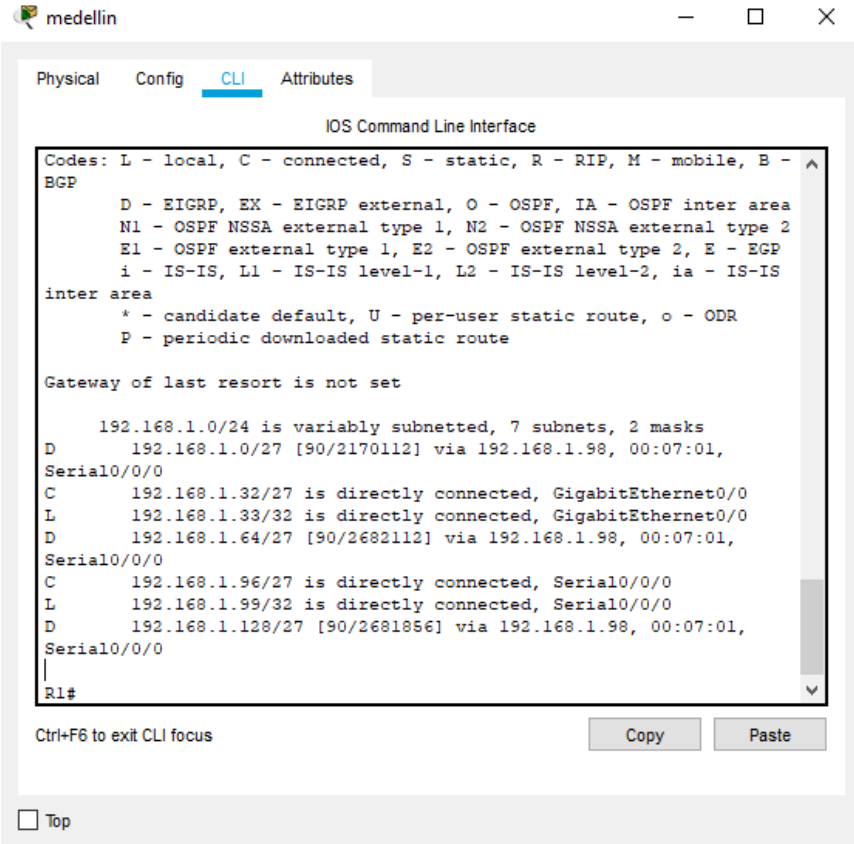


Gateway of last resort is not set

192.168.1.0/24 is variably subnetted, 8 subnets, 2 masks
C 192.168.1.0/27 is directly connected, GigabitEthernet0/0
L 192.168.1.1/32 is directly connected, GigabitEthernet0/0
D 192.168.1.32/27 [90/2170112] via 192.168.1.99, 00:05:17, Serial0/0/0
D 192.168.1.64/27 [90/2170112] via 192.168.1.131, 00:05:17, Serial0/0/1
C 192.168.1.96/27 is directly connected, Serial0/0/0
L 192.168.1.98/32 is directly connected, Serial0/0/0
C 192.168.1.128/27 is directly connected, Serial0/0/1

L 192.168.1.130/32 is directly connected, Serial0/0/1

MEDELLIN

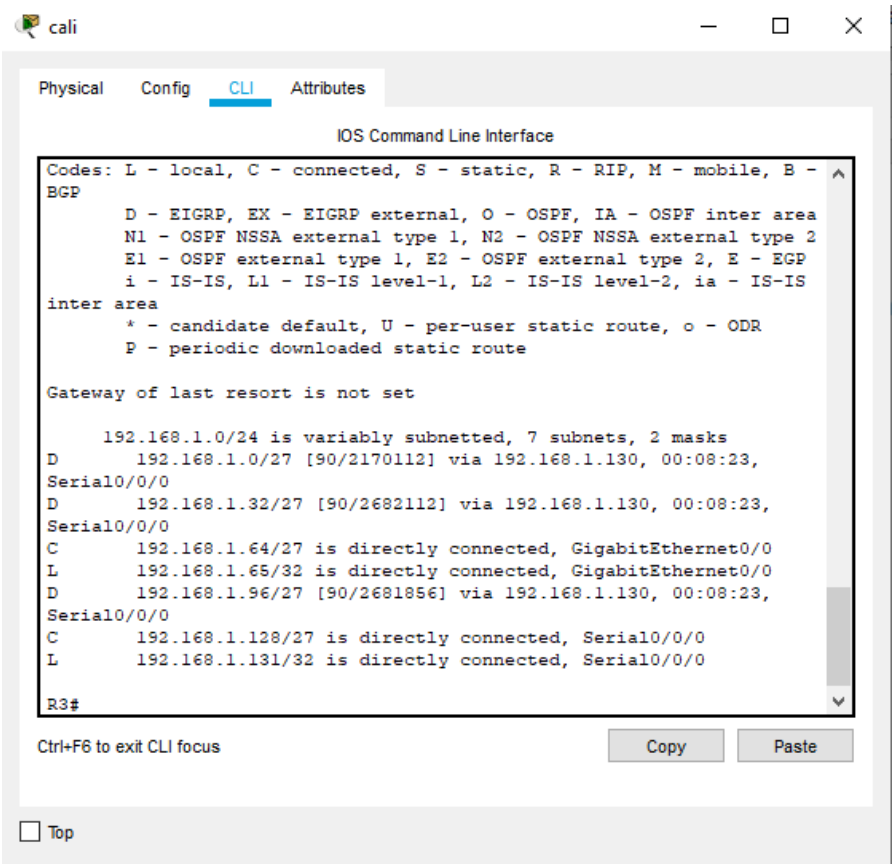


Gateway of last resort is not set

192.168.1.0/24 is variably subnetted, 7 subnets, 2 masks
D 192.168.1.0/27 [90/2170112] via 192.168.1.98, 00:07:01, Serial0/0/0
C 192.168.1.32/27 is directly connected, GigabitEthernet0/0
L 192.168.1.33/32 is directly connected, GigabitEthernet0/0
D 192.168.1.64/27 [90/2682112] via 192.168.1.98, 00:07:01, Serial0/0/0
C 192.168.1.96/27 is directly connected, Serial0/0/0
L 192.168.1.99/32 is directly connected, Serial0/0/0

D 192.168.1.128/27 [90/2681856] via 192.168.1.98, 00:07:01, Serial0/0/0

CALI



Gateway of last resort is not set

192.168.1.0/24 is variably subnetted, 7 subnets, 2 masks
D 192.168.1.0/27 [90/2170112] via 192.168.1.130, 00:08:23, Serial0/0/0
D 192.168.1.32/27 [90/2682112] via 192.168.1.130, 00:08:23, Serial0/0/0
C 192.168.1.64/27 is directly connected, GigabitEthernet0/0
L 192.168.1.65/32 is directly connected, GigabitEthernet0/0
D 192.168.1.96/27 [90/2681856] via 192.168.1.130, 00:08:23, Serial0/0/0
C 192.168.1.128/27 is directly connected, Serial0/0/0

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

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

BOGOTA

show ip eigrp traffic 200
IP-EIGRP Traffic Statistics for process 200
Hellos sent/received: 18871/12575
Updates sent/received: 22/30
Queries sent/received: 4/0
Replies sent/received: 0/2
Acks sent/received: 30/19
Input queue high water mark 1, 0 drops
SIA-Queries sent/received: 0/0
SIA-Replies sent/received: 0/0

MEDELLIN

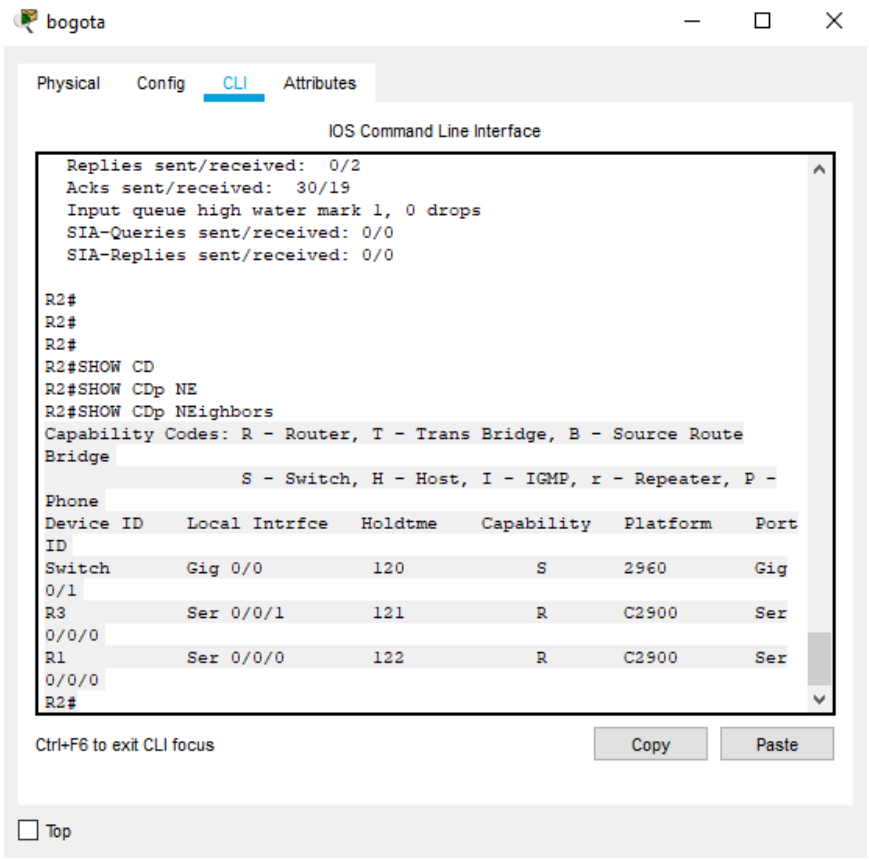
IP-EIGRP Traffic Statistics for process 200
Hellos sent/received: 12624/6305
Updates sent/received: 16/10
Queries sent/received: 0/0
Replies sent/received: 0/0
Acks sent/received: 10/16
Input queue high water mark 1, 0 drops
SIA-Queries sent/received: 0/0
SIA-Replies sent/received: 0/0

CALI

IP-EIGRP Traffic Statistics for process 200
Hellos sent/received: 445/220
Updates sent/received: 4/4
Queries sent/received: 0/0
Replies sent/received: 0/0
Acks sent/received: 4/4
Input queue high water mark 1, 0 drops
SIA-Queries sent/received: 0/0
SIA-Replies sent/received: 0/0

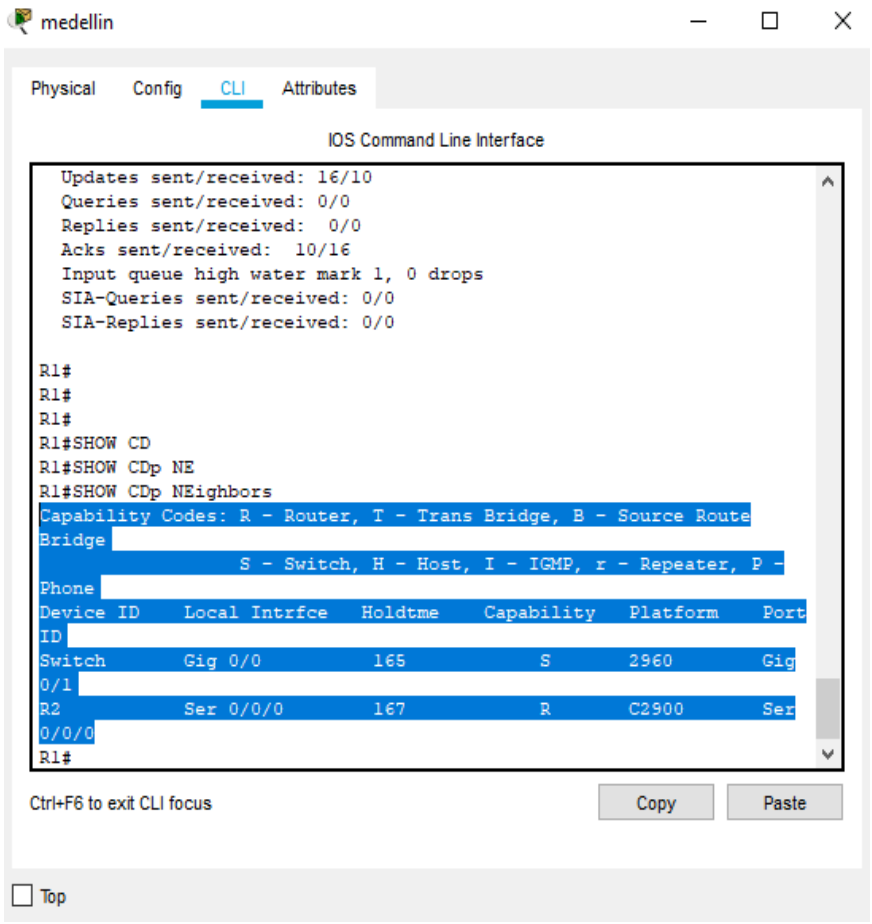
d. Realizar un diagnóstico de vecinos usando el comando cdp.

BOGOTA



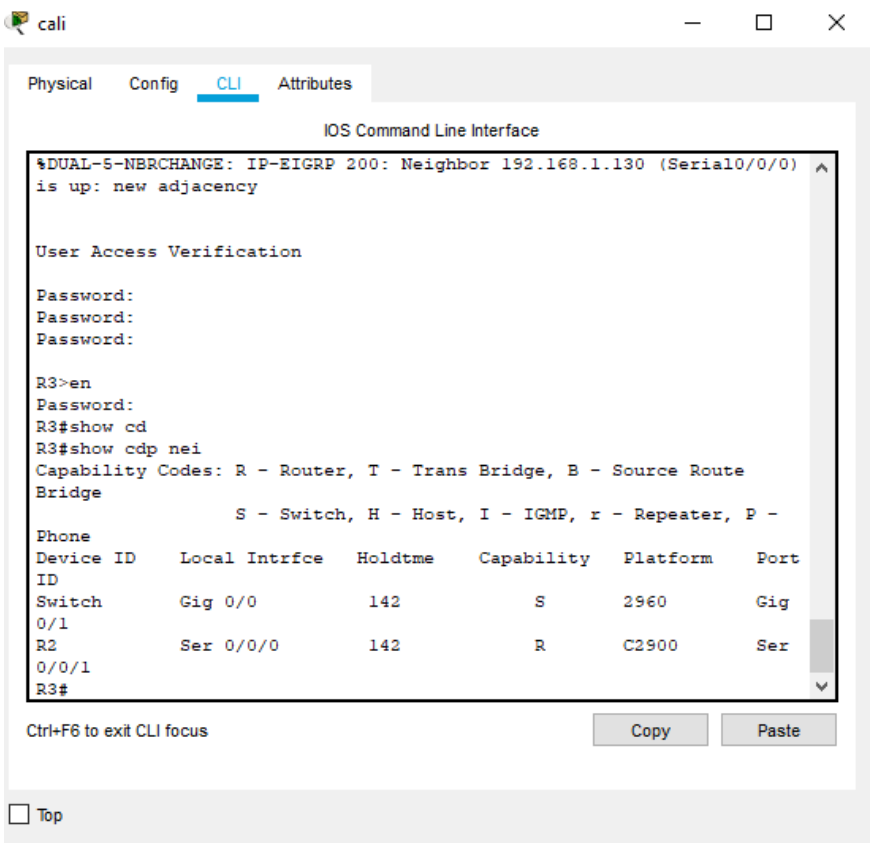
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID Local Intrfce Holdtme Capability Platform Port ID
Switch Gig 0/0 120 S 2960 Gig 0/1
R3 Ser 0/0/1 121 R C2900 Ser 0/0/0
R1 Ser 0/0/0 122 R C2900 Ser 0/0/0

MEDELLIN



Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID Local Intrfce Holdtme Capability Platform Port ID
Switch Gig 0/0 165 S 2960 Gig 0/1
R2 Ser 0/0/0 167 R C2900 Ser 0/0/0

CALI



Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID Local Intrfce Holdtme Capability Platform Port ID
Switch Gig 0/0 142 S 2960 Gig 0/1
R2 Ser 0/0/0 142 R C2900 Ser 0/0/1

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

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
	Successful	medellin	cali	ICMP		0.000	N	0	(edi
	Successful	medellin	bogota	ICMP		0.000	N	1	(edi

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
	Successful	cali	medellin	ICMP		0.000	N	0	(edi
	Successful	cali	bogota	ICMP		0.000	N	1	(edi

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
	Successful	bogota	cali	ICMP		0.000	N	0	(edi
	Successful	bogota	medellin	ICMP		0.000	N	1	(edi

9. Parte 3: Configuración de Enrutamiento.

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

Para asignarle el protocolo a cada router es necesario ejecutar los siguientes comandos:

BOGOTA

```
bogota>enable
Password:
bogota#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
bogota(config)#ROUTER EIGRP 200
bogota(config-router)#network 192.168.1.0 0.0.0.255
```

MEDELLIN

```
medellin>enable
Password:
medellin#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
medellin(config)#ROUTER EIGRP 200
medellin(config-router)#network 192.168.1.0 0.0.0.255
```

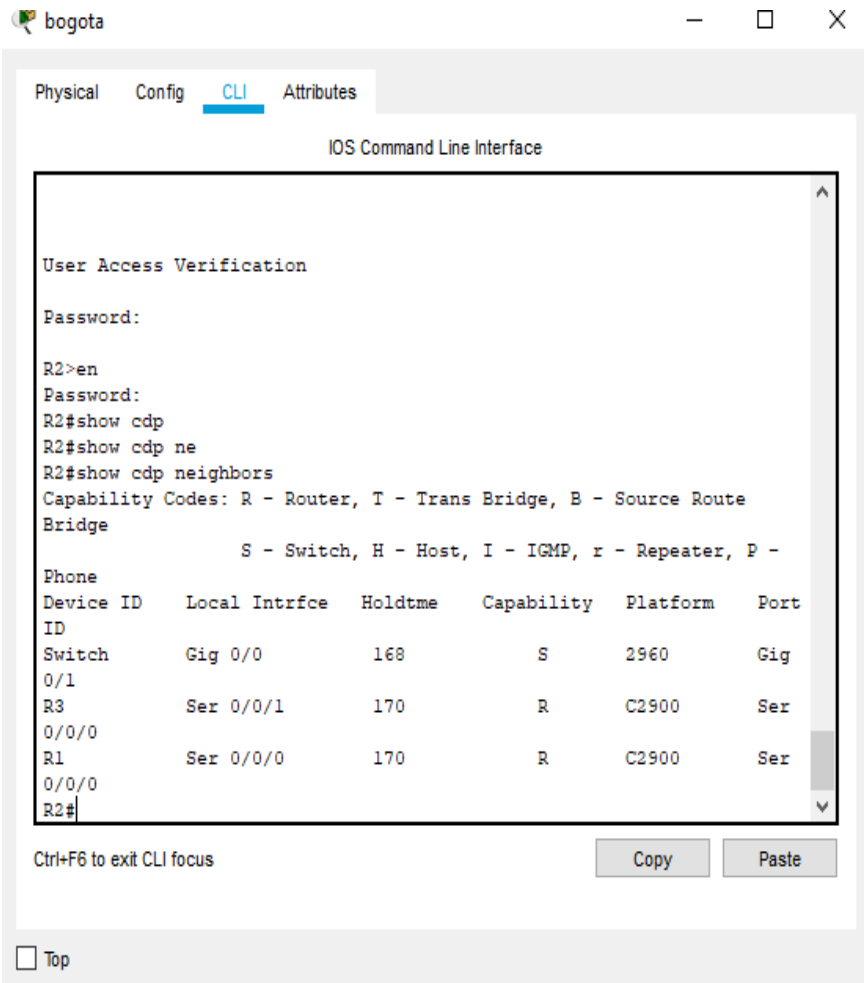
CALI

```
cali>enable
Password:
cali#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
cali(config)#ROUTER EIGRP 200
cali(config-router)#network 192.168.1.0 0.0.0.255
```

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

BOGOTA

bogota#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID Local Intrfce Holdtme Capability Platform Port ID
R3 Ser 0/0/1 156 R C2900 Ser 0/0/0
R1 Ser 0/0/0 158 R C2900 Ser 0/0/0



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

BOGOTA

Gateway of last resort is not set
192.168.1.0/24 is variably subnetted, 8 subnets, 2 masks
C 192.168.1.0/27 is directly connected, GigabitEthernet0/0
L 192.168.1.1/32 is directly connected, GigabitEthernet0/0
D 192.168.1.32/27 [90/2170112] via 192.168.1.99, 05:53:11, Serial0/0/0
D 192.168.1.64/27 [90/2170112] via 192.168.1.131, 05:53:11, Serial0/0/1
C 192.168.1.96/27 is directly connected, Serial0/0/0
L 192.168.1.98/32 is directly connected, Serial0/0/0
C 192.168.1.128/27 is directly connected, Serial0/0/1
L 192.168.1.130/32 is directly connected, Serial0/0/1

MEDELLIN

Gateway of last resort is not set

192.168.1.0/24 is variably subnetted, 7 subnets, 2 masks
D 192.168.1.0/27 [90/2170112] via 192.168.1.98, 05:53:33, Serial0/0/0
C 192.168.1.32/27 is directly connected, GigabitEthernet0/0
L 192.168.1.33/32 is directly connected, GigabitEthernet0/0
D 192.168.1.64/27 [90/2682112] via 192.168.1.98, 05:53:33, Serial0/0/0
C 192.168.1.96/27 is directly connected, Serial0/0/0
L 192.168.1.99/32 is directly connected, Serial0/0/0
D 192.168.1.128/27 [90/2681856] via 192.168.1.98, 05:53:33, Serial0/0/0

CALI

Gateway of last resort is not set
192.168.1.0/24 is variably subnetted, 7 subnets, 2 masks
D 192.168.1.0/27 [90/2170112] via 192.168.1.130, 05:53:50, Serial0/0/0
D 192.168.1.32/27 [90/2682112] via 192.168.1.130, 05:53:50, Serial0/0/0
C 192.168.1.64/27 is directly connected, GigabitEthernet0/0
L 192.168.1.65/32 is directly connected, GigabitEthernet0/0
D 192.168.1.96/27 [90/2681856] via 192.168.1.130, 05:53:50, Serial0/0/0
C 192.168.1.128/27 is directly connected, Serial0/0/0
L 192.168.1.131/32 is directly connected, Serial0/0/0

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

De cali a medellin si se tiene respuestas entre lanes:

C:\>ping 192.168.1.35
Pinging 192.168.1.35 with 32 bytes of data:

Reply from 192.168.1.35: bytes=32 time=2ms TTL=125
Reply from 192.168.1.35: bytes=32 time=2ms TTL=125
Reply from 192.168.1.35: bytes=32 time=2ms TTL=125
Reply from 192.168.1.35: bytes=32 time=2ms TTL=125

Ping statistics for 192.168.1.35:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 2ms, Maximum = 2ms, Average = 2ms

```
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Link-local IPv6 Address.....: FE80::200:CFF:FE97:BED3
   IP Address.....: 192.168.1.66
   Subnet Mask.....: 255.255.255.224
   Default Gateway.....: 192.168.1.65

Bluetooth Connection:

   Link-local IPv6 Address.....: ::
   IP Address.....: 0.0.0.0
   Subnet Mask.....: 0.0.0.0
   Default Gateway.....: 0.0.0.0

C:\>ping 192.168.1.35

Pinging 192.168.1.35 with 32 bytes of data:

Reply from 192.168.1.35: bytes=32 time=2ms TTL=125
Reply from 192.168.1.35: bytes=32 time=2ms TTL=125
Reply from 192.168.1.35: bytes=32 time=2ms TTL=125
Reply from 192.168.1.35: bytes=32 time=2ms TTL=125

Ping statistics for 192.168.1.35:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 2ms, Average = 2ms
```

10. Parte 4: Configuración de las listas de Control de Acceso.

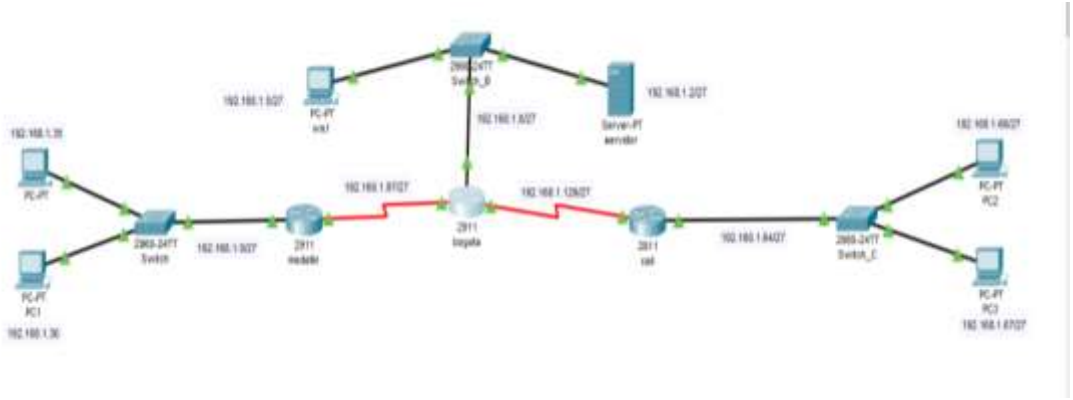
En este momento cualquier usuario de la red tiene acceso a todos sus dispositivos y estaciones de trabajo. El jefe de redes le solicita implementar seguridad en la red. Para esta labor se decide configurar listas de control de acceso (ACL) a los routers.
Las condiciones para crear las ACL son las siguientes:

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

Enter configuration commands, one per line. End with CNTL/Z.
(config)#access-list 90 deny 192.168.1.32 0.0.0.31
(config)#access-list 91 permit host 192.168.1.2
(config)#inter g0/0
(config-if)#ip access-group 90 out
(config-if)#ip access-group 91 out
(config-if)#exit
(config)#

El Access list no permite tráfico hacia cualquier equipo que no esté dentro de su red, la 91 permite que solo tenga acceso al servidor ubicado en Bogotá.

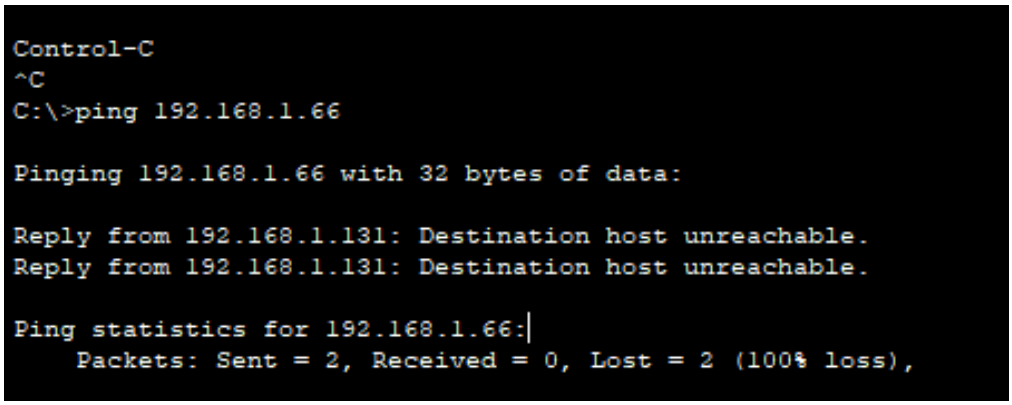
b. El equipo WS1 y el servidor se encuentran en la subred de administración. Solo el servidor de la subred de administración debe tener acceso a cualquier otro dispositivo en cualquier parte de la red.



No se tiene respuesta hacia el ws1como se pide en la guía.

C:\>ping 192.168.1.66
Pinging 192.168.1.66 with 32 bytes of data:
Reply from 192.168.1.131: Destination host unreachable.
Reply from 192.168.1.131: Destination host unreachable.

Ping statistics for 192.168.1.66:
Packets: Sent = 2, Received = 0, Lost = 2 (100% loss),
Control-C



Desde el servidor si se tiene respuesta

C:\>ping 192.168.1.35
Pinging 192.168.1.35 with 32 bytes of data:
Reply from 192.168.1.35: bytes=32 time=3ms TTL=126
Reply from 192.168.1.35: bytes=32 time=0ms TTL=126
Reply from 192.168.1.35: bytes=32 time=1ms TTL=126
Ping statistics for 192.168.1.35:
Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 5ms, Average = 2ms

C:\>ping 192.168.1.66
Pinging 192.168.1.66 with 32 bytes of data:
Reply from 192.168.1.66: bytes=32 time=0ms TTL=126
Reply from 192.168.1.66: bytes=32 time=0ms TTL=126
Reply from 192.168.1.66: bytes=32 time=0ms TTL=126
Ping statistics for 192.168.1.66:
Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 1ms, Average = 1msControl-C

```
C:\>ping 192.168.1.35

Pinging 192.168.1.35 with 32 bytes of data:

Reply from 192.168.1.35: bytes=32 time=2ms TTL=126
Reply from 192.168.1.35: bytes=32 time=5ms TTL=126
Reply from 192.168.1.35: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.1.35:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 5ms, Average = 2ms

Control-C
^C
C:\>ping 192.168.1.66

Pinging 192.168.1.66 with 32 bytes of data:

Reply from 192.168.1.66: bytes=32 time=1ms TTL=126
Reply from 192.168.1.66: bytes=32 time=1ms TTL=126
Reply from 192.168.1.66: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.1.66:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

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.

LAN MEDELLIN A LAN CALI

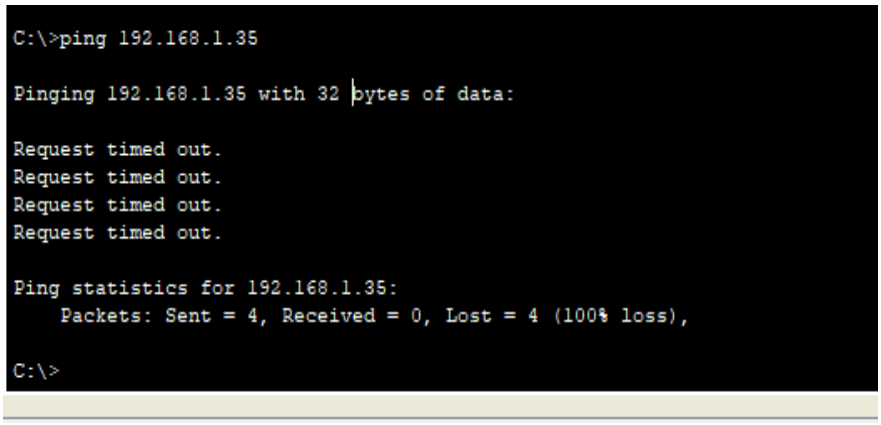
C:\>ping 192.168.1.66
Pinging 192.168.1.66 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 192.168.1.66:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\

```
C:\>ping 192.168.1.66

Pinging 192.168.1.66 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.66:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

LAN CALI A MEDELLIN LAN

C:\>ping 192.168.1.35
Pinging 192.168.1.35 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.35:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>



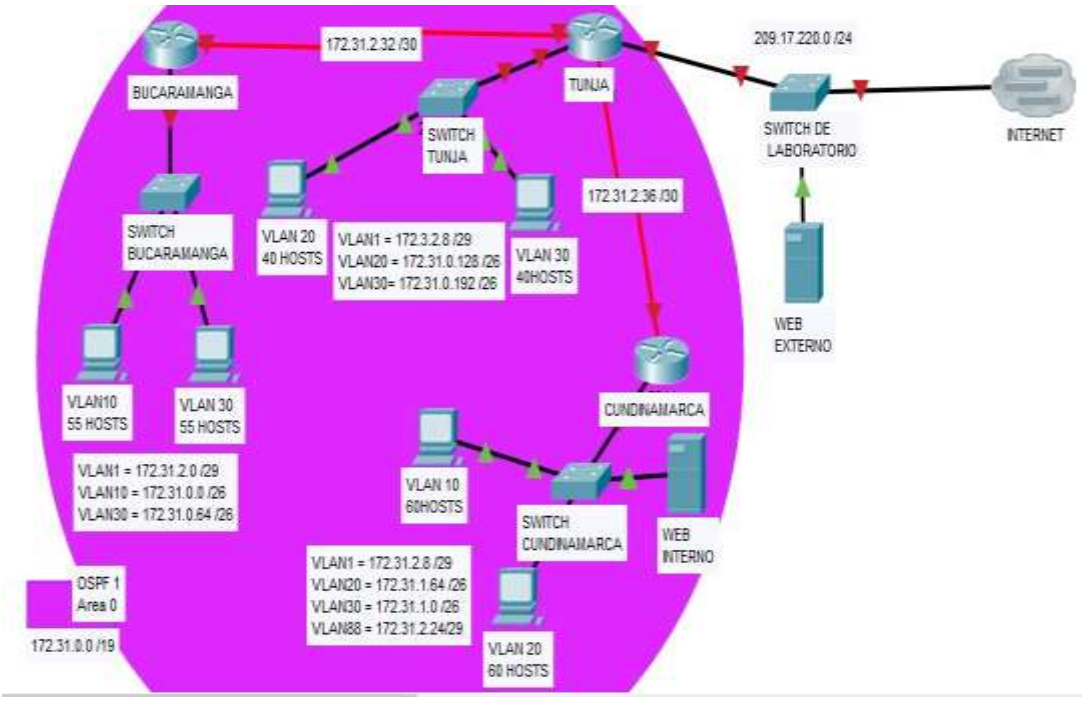
11. Parte 5: Comprobación de la red instalada.

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.

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

12. Escenario 2

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



Desarrollo

Los siguientes son los requerimientos necesarios:

1. Todos los routers deberán tener los siguiente:

- **Configuración básica.**

  Se realiza la configuración básica, configurando las ip y realizando las conexiones físicas entre router y switches y lan.

- **Configuración AAA**

  TUNJA(config)#aaa new-model
  TUNJA(config)#username cisco password 123456789
  TUNJA(config)#

TUNJA#

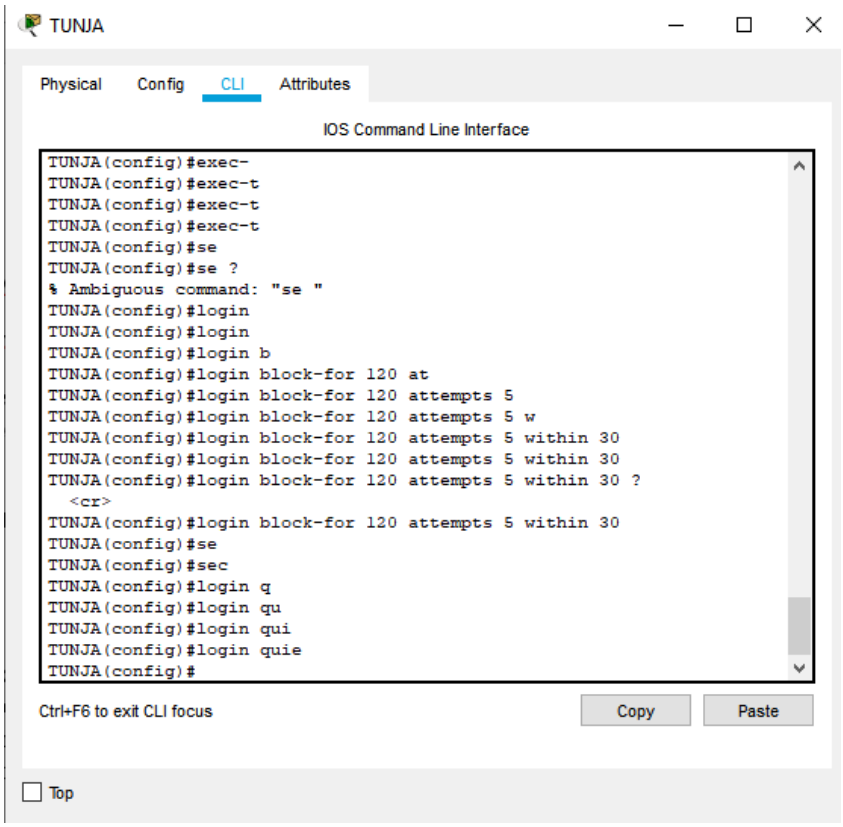
BUCARAMANGA(config)#aaa new-model
BUCARAMANGA(config)#username cisco password 123456789
BUCARAMANGA(config)#
CUNDINAMARCA(config)#aaa new-model
CUNDINAMARCA(config)#username cisco password 123456789
CUNDINAMARCA(config)#

- **Cifrado de contraseñas.**

TUNJA(config)#service password-encryption
BUCARAMANGA(config)#SERVICE PAssword-encryption
CUNDINAMARCA(config)#service password-encryption

- **Un máximo de internos para acceder al router.**

TUNJA(config)#login block-for 120 attempts 5 within 30



```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#login block-for 120 attempts 5 within 30
Router(config)#hostna
Router(config)#hostname BUCARAMANGA
BUCARAMANGA(config)#
```

- **Máximo tiempo de acceso al detectar ataques.**

```
TUNJA# configure terminal
TUNJA(config)# line vty
TUNJA(config-line)# no exec-timeout

CUNDINAMARCA# configure terminal
CUNDINAMARCA(config)# line vty
CUNDINAMARCA(config-line)# no exec-timeout

BUCARAMANGA# configure terminal
BUCARAMANGA(config)# line vty
BUCARAMANGA(config-line)# no exec-timeout
```

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

GUARDO LA CONFIGURACION DEL ROUTER EN EL SERVIDOR

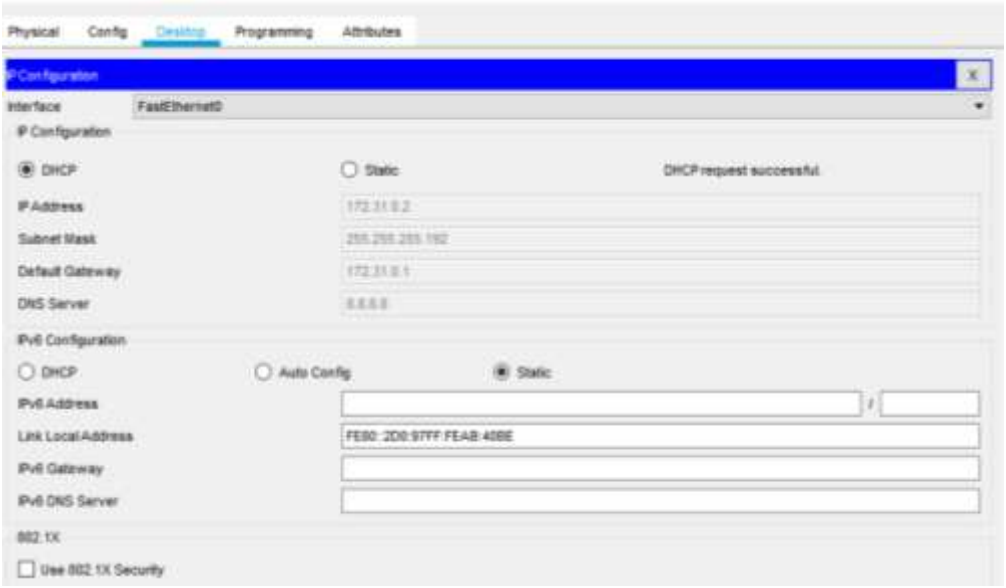
2. El DHCP deberá proporcionar solo direcciones a los hosts de Bucaramanga y

Cundinamarca

VLAN10

Switch_BUCARAMANGA (dhcp-config)#NETWORK 172.31.0.0 255.255.255.192
Switch_BUCARAMANGA (dhcp-config)#DEFAULT-ROUTER 172.31.0.1
Switch_BUCARAMANGA (dhcp-config)#DNS-SERVER 8.8.8.8
Switch_BUCARAMANGA (dhcp-config)#EXIT

Dhcp de la vlan 10



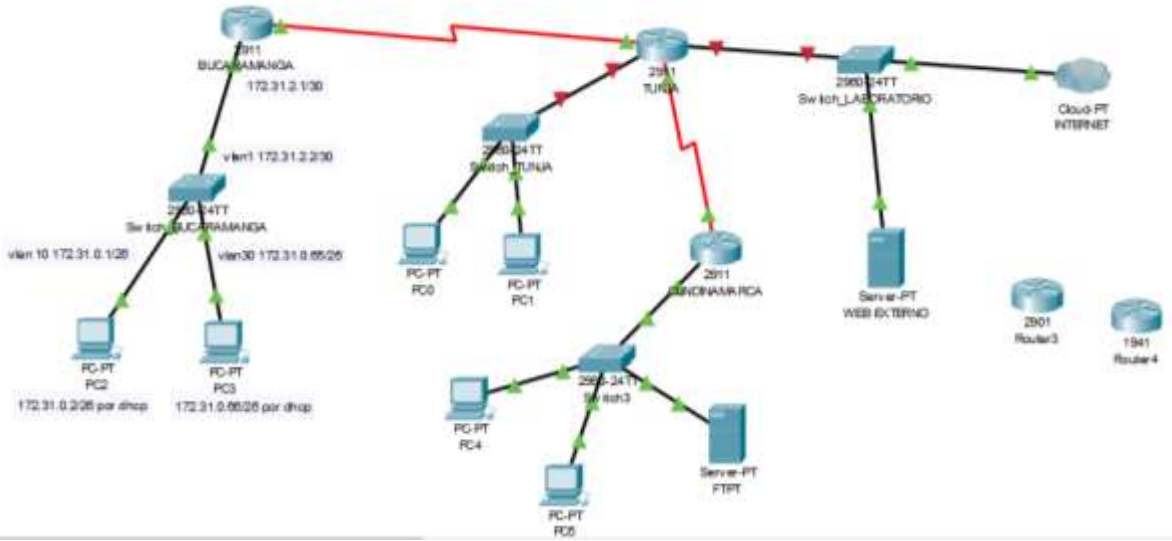
Prueba de conectividad dhcp Bucaramanga

```
Packet Tracer PC Command Line 1.0
C:\>ping 172.31.0.1

Pinging 172.31.0.1 with 32 bytes of data:

Reply from 172.31.0.1: bytes=32 time<1ms TTL=255
Reply from 172.31.0.1: bytes=32 time<1ms TTL=255
Reply from 172.31.0.1: bytes=32 time<1ms TTL=255
Reply from 172.31.0.1: bytes=32 time<1ms TTL=255

Ping statistics for 172.31.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Router de bucarmanga asociando la vlan 1 del switch

BUCARAMANGA#ping 172.31.2.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.31.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
BUCARAMANGA#

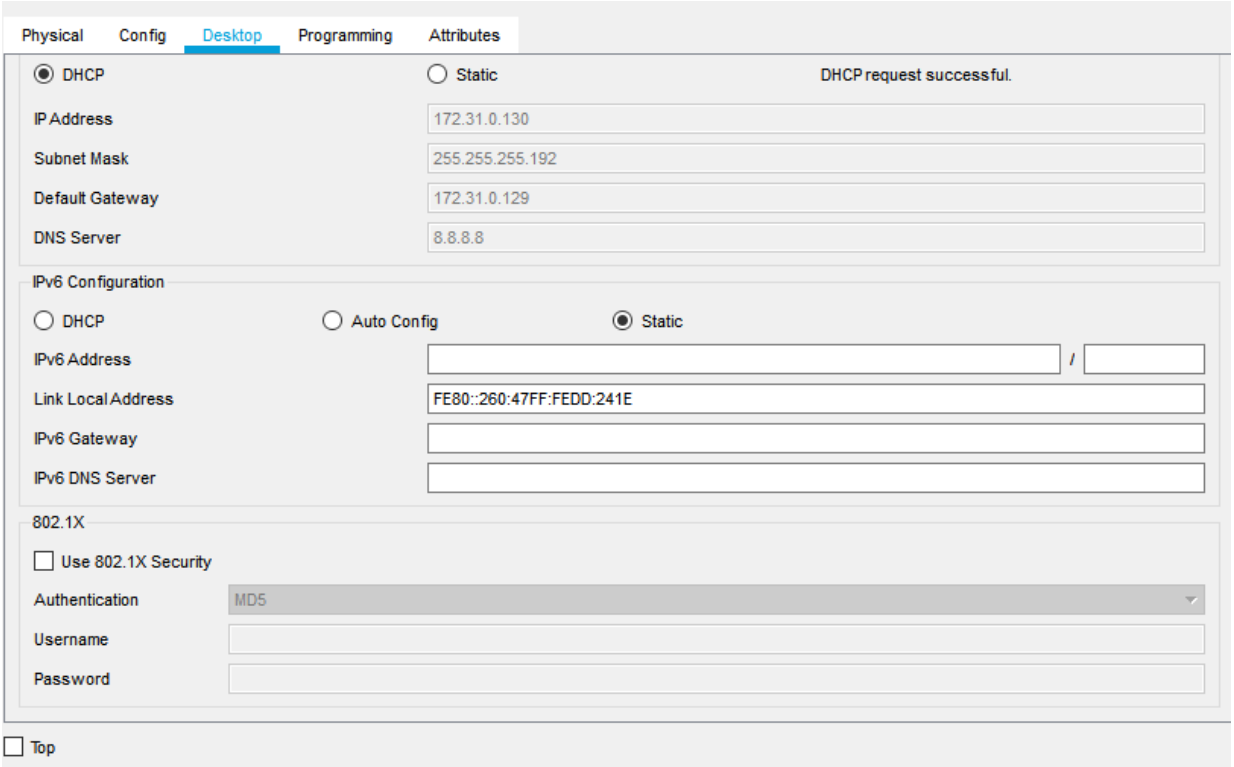


Configuración vlan 20

Switch(config-if)#ip add
Switch(config-if)#ip address 172.31.0.128 255.255.255.192
Bad mask /26 for address 172.31.0.128
Switch(config-if)#ip address 172.31.0.129 255.255.255.192
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#exit
Switch(config)#dhc
Switch(config)#ip dh
Switch(config)#ip dhcp pool
Switch(config)#ip dhcp pool ?
WORD Pool name
Switch(config)#ip dhcp pool vlan
Switch(config)#ip dhcp pool vlan20
Switch(dhcp-config)#?
address Configure a reserved address
default-router Default routers

dns-server Set name server
domain-name Domain name
exit Exit from DHCP pool configuration mode
network Network number and mask
no Negate a command or set its defaults
option Raw DHCP options
Switch(dhcp-config)#net
Switch(dhcp-config)#network 172.31.0.128
Switch(dhcp-config)#network 172.31.0.128 255.255.255.192
Switch(dhcp-config)#network 172.31.0.128 255.255.255.192
Switch(dhcp-config)#de
Switch(dhcp-config)#default-router 172.31.0.129
Switch(dhcp-config)#dn
Switch(dhcp-config)#dns-server 8.8.8.8
Switch(dhcp-config)#exit
Switch(config)#

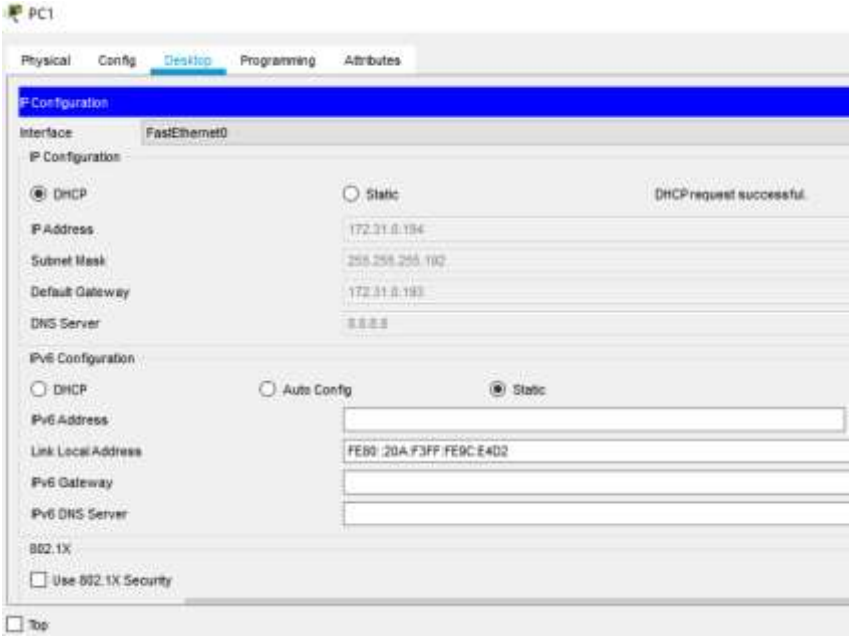
Vlan 20 pc aprende dhcp



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

```
TUNJA(config)#ip nat inside source static 209.17.22.2 5.5.5.5
TUNJA(config)#inter
TUNJA(config)#interface g
TUNJA(config)#interface gigabitEthernet 0/0
TUNJA(config)#interface gigabitEthernet 0/0
TUNJA(config-if)#nat
TUNJA(config-if)#ip nat
TUNJA(config-if)#ip nat ou
TUNJA(config-if)#ip nat outside
TUNJA(config-if)#ip nat outside

Switch(config)#interface fastEthernet 0/2
Switch(config-if)#switchport access vlan 30
Switch(config-if)#exit
Switch(config)#interface vlan 30
%LINK-5-CHANGED: Interface Vlan30, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan30, changed state to
up

Switch(config-if)#ip address 172.31.0.193 255.255.255.192
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#ip dhcp pool ?
WORD Pool name
Switch(config)#ip dhcp pool vlan30
Switch(dhcp-config)#network 172.31.0.192
Switch(dhcp-config)#network 172.31.0.192 255.255.255.192
Switch(dhcp-config)#default-router 172.31.0.193
Switch(dhcp-config)#dn
Switch(dhcp-config)#dns-server 8.8.8.8
Switch(dhcp-config)#exit
Switch(config)#
```

Vlan 30 equipos aprendido dhcp-



4. El enrutamiento deberá tener autenticación.

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
Gateway of last resort is not set
172.3.0.0/16 is variably subnetted, 2 subnets, 2 masks
C 172.3.2.8/29 is directly connected, GigabitEthernet0/1
L 172.3.2.9/32 is directly connected, GigabitEthernet0/1
172.31.0.0/16 is variably subnetted, 4 subnets, 2 masks
C 172.31.2.32/30 is directly connected, Serial0/0/1
L 172.31.2.33/32 is directly connected, Serial0/0/1
C 172.31.2.36/30 is directly connected, Serial0/0/0
L 172.31.2.37/32 is directly connected, Serial0/0/0
209.17.220.0/24 is variably subnetted, 2 subnets, 2 masks
C 209.17.220.0/24 is directly connected, GigabitEthernet0/0
L 209.17.220.2/32 is directly connected, GigabitEthernet0/0

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 10 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 accedo a los routers e internet.

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

```
Reply from 172.31.0.1: bytes=32 time<1ms TTL=255
Reply from 172.31.0.1: bytes=32 time<1ms TTL=255

Ping statistics for 172.31.0.1:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

Control-C
^C
C:\>ping 172.31.0.130

Pinging 172.31.0.130 with 32 bytes of data:

Request timed out.
Request timed out.

Ping statistics for 172.31.0.130:
    Packets: Sent = 3, Received = 0, Lost = 3 (100% loss),
```

13. Aspectos a tener en cuenta

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

14. Conclusión

En el desarrollo anterior del informe se realizaron diferentes ámbitos de tareas para dar solución a los dos Escenarios propuestos de manera que se pudo realizar a satisfacción de estas Topologías, de esta forma se demostró todo el aprendizaje adquirido durante el transcurso del diplomado, aplicando configuraciones básicas de enrutamiento VLAN, Enrutamientos dinámicos, lista de accesos NAT y DHCP, configuración de ACL de los Router.

15. Bibliografía

CISCO. (s.f.). Cisco Networking Academy. Obtenido de: https://repository.unad.edu.co/bitstream/handle/10596/18652/1017191659.pdf?sequence=1&isAllowed=y

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

Eugenio Duarte, E. D. (2016, 13 abril). Cisco CCNA – Cómo Configurar DHCP En Cisco Router. Recuperado 5 junio, 2019, de

Rosbarbosa, R. B. (2017, 25 septiembre). IP Helper y Relay Agent – Manteniendo un servidor DHCP en otra red. Obtenido 5 junio, 2019, de: https://www.seaccna.com/ip-helper-relay-agent/

Victor E. Martinez G, V. E. (2018, 16 agosto). Configuración de rutas estáticas (static route) Router Cisco. Recuperado 5 junio, 2019, de: http://theosnews.com/2013/02/configuracion-de-rutas-estaticas-static-route-router-cisco/

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

Configurar las Listas de acceso IP, 27 de diciembre de 2007, Obtenido de: https://www.cisco.com/c/es_mx/support/docs/security/ios-firewall/23602-confaccesslists.html

Understanding and Configuring PPP CHAP Authentication, eptiembre 29 2014, Obtenido de: https://www.cisco.com/c/en/us/support/docs/wan/point-to-point-protocol-ppp/25647-understanding-ppp-chap.html

Configuración de conexión troncal ISL y 802.1, Actualizado 1 de septiembre de 2005, Obtenido de: https://www.cisco.com/c/es_mx/support/docs/switches/catalyst-4000-series-switches/24064-171.html