PRUEBA DE HABILIDADES PRÁCTICAS CCNA 16-4 FINAL

YURI GISEL LOPEZ SANTANA

Director de curso: Juan Carlos Vesga

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
PROGRAMA DE INGENIERA DE SISTEMAS
2019

PRUEBA DE HABILIDADES PRÁCTICAS CCNA 16-4 FINAL

YURI GISEL LOPEZ SANTANA

Director de curso: Juan Carlos Vesga

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
PROGRAMA DE INGENIERA DE SISTEMAS
2019

Tabla de Contenido

RESUMEN

La siguiente actividad está planteada para desarrollar por medio de la práctica las habilidades y competencias que fueron adquiridas en el diplomado de profundización CCNA y poder administrar y dar solución a los diferentes problemas que se nos presenten en el ámbito de las redes.

Se presentan dos escenarios para el desarrollo de nuestra práctica, el primero está planteado para tres sucursales donde se deberá configurar e interconectar cada uno de los dispositivos que conforman esta red, se debe generar direccionamientio IP de acuerdo a los hosts que se requieren, permitir comunicación entre las sucursales a traves de una configuración de protocolos de enrutamiento EIGRP entre los routers, se generara un diagnóstico de conectividad entre los hosts vecinos que tiene la red, se implementara seguridad en la red configurando listas de control de acceso (ACL) a los routers para permitir la comunicación de unos hosts entre si y otros no.

El siguiente escenario está planteado para comunicar tres diferentes ciudades y sus subinterfaces por medio del protocolo de enrutamiento OSPF y el protocolo dinámico de host DHCP, este escenario estará enfocado a la seguridad de la red, autenticando el enrutamiento, asignado Cifrado de passwords, aseguramiento de líneas de consola y líneas VTY. En el web server se generará NAT estático y en el resto de los equipos de la topología se emplearán NAT de sobrecarga (PAT), también se configurarán listas de control de acceso (ACL).

Estos escenarios se desarrollarán con ayuda del simulador Packet Tracer el cual nos permitirá la práctica real con cada dispositivo de las redes.

ABSTRACT

The following activity is given to develop, through practice, the skills and competences that were acquired in the CCNA deepening diploma and to manage and solve the different problems that arise in the field of networks.

There are two scenarios for the development of our practice, the first one is planned for three branches where each of the devices that make up this network must be configured and interconnected, IP address must be generated according to the required hosts, allow communication between the branches through an EIGRP routing protocol configuration between the routers, a connectivity diagnosis will be generated between the neighboring hosts that the network has, network security will be implemented by configuring access control lists (ACLs) to the routers to allow the communication of some hosts with each other and not others.

The following scenario is proposed to communicate three different cities and their subinterfaces through the OSPF routing protocol and the dynamic DHCP host protocol, this scenario will be focused on network security, authenticating routing, assigned password encryption, password assurance console lines and VTY lines. In the web server static NAT will be generated and in the rest of the topology equipment, NAT overload (PAT) will be used, access control lists (ACL) will also be configured.

These scenarios will be developed with the help of the Packet Tracer simulator which will allow us to practice with each device in the networks.

INTRODUCCION

El internet a permitido la interconexión de variedad de redes tanto extensas como pequeñas las cuales están interconectadas a través de dispositivos, protocolo de enrutamiento lo que permite la comunicación de las personas de una ciudad a otra, compartir datos, la creación de empresas por medio de internet; esto nos lleva a capacitarnos en conocimiento y en la práctica de las redes en el mundo informático.

La UNAD y CISCO nos proporcionan el conocimiento y la práctica por medio de herramientas como packet Tracer que es una plataforma simulación de redes la cual nos permite a nosotros como estudiantes poder simular redes, configurar dispositivos, generar comunicación en las diferentes capas de la red desde tener el dispositivo, como se conecta, como en rutar cada dispositivo por medio de comandos que nos permitirán comunicación entre una red LAN o una red WAN.

Por lo que este trabajo nos permitirá instalar, configurar y administrar redes empresariales, para poder analizar cada uno del protocolo de enrutamiento propuesto en cada escenario por medio de comandos y poder resolver problemas de configuración, conectividad que se puedan presentar en una red tanto de empresas como una red de hogar.

OBJETIVOS

GENERAL

Analizar y desarrollar los escenarios dados para la actividad, generando soluciones a cada uno de las redes LAN y WAN planteadas mediante la utilización de la herramienta de simulación Packet Tracert.

ESPECÍFICOS

- Diseñar y documentar cada uno de los comandos generados para la solución de los escenarios dados.
- Implementación de seguridad en las redes propuestas.
- Aplicar una configuración básica cada uno de los equipos utilizados en la simulación de las redes implementadas.
- Aplicar los diferentes protocolos de enrutamiento en el desarrollo de los escenarios.
- Utilizar como herramienta de simulación Packet Tracer, para el desarrollo de cada uno de los escenarios.

1. ESCENARIO 1

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

1.1. 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.

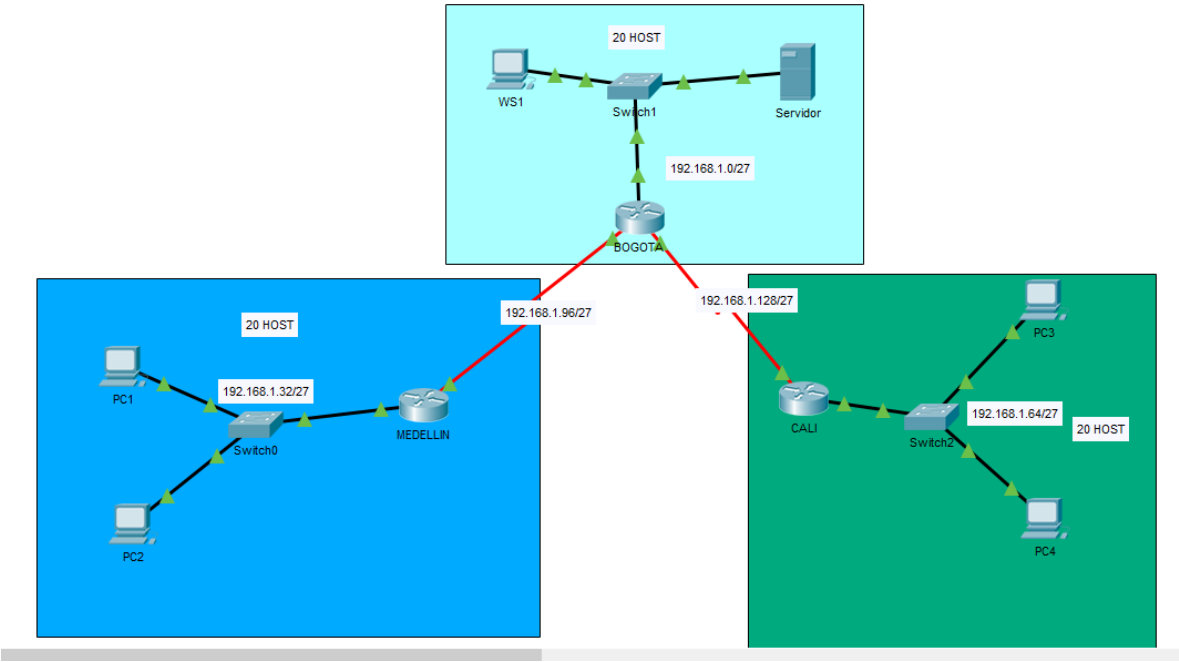
Parte 2: Considerar la asignación de los parámetros básicos y la detección de vecinos directamente conectados.

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 fisica de los equipos con base en la topología de red

Configurar la topología de red, de acuerdo con las siguientes especificaciones.

1.2. 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

11111111.11111111.11111111.11100000
255.255.255.224 MASCARA DE RED

Calcular masara de subre para 20 host.

$$2^n - 2 = host$$
$$2^5 - 2 = 30\ host$$

# redes	Id. red	Rango de direcciones		broadcast	Mascara de sub red
1	192.168.1.0	192.168.1.1	192.168.1.30	192.168.1.31	255.255.255.224
2	192.168.1.32	192.168.1.33	192.168.1.62	192.168.1.63	255.255.255.224
3	192.168.1.64	192.168.1.65	192.168.1.94	192.168.1.95	255.255.255.224
4	192.168.1.96	192.168.1.97	192.168.1.126	192.168.1.127	255.255.255.224
5	192.168.1.128	192.168.1.129	192.168.1.158	192.168.1.159	255.255.255.224

Creación de la topología de red

DISPOSITIVO	INTERFAZ	DIRECCION IP	MASCARA DE SUBRED	GATEWAY
Router Medellín	Fa0/0	192.168.1.33	255.255.255.224	No aplica
	S0/0/1	192.168.1.99	255.255.255.224	
Router Bogotá	Fa0/0	192.168.1.1	255.255.255.224	No aplica
	S0/0/0	192.168.1.98	255.255.255.224	
	S0/0/1	192.168.1.130	255.255.255.224	
Router Cali	Fa0/0	192.168.1.65	255.255.255.224	No aplica
	S0/0/0	192.168.1.131	255.255.255.224	
Sucursal de Medellín				
PC 1 (host 1)	NIC	192.168.1.34	255.255.255.224	192.168.1.33
PC 2 (host 20)	NIC	192.168.1.53	255.255.255.224	192.168.1.33
Sucursal de Bogotá				
PC 0 (host 1)	NIC	192.168.1.2	255.255.255.224	192.168.1.1
Servidor (host 20)	NIC	192.168.1.20	255.255.255.224	192.168.1.1
Sucursal de Cali				
PC 3 (host 1)	NIC	192.168.1.66	255.255.255.224	192.168.1.65
PC 4 (host 20)	NIC	192.168.1.85	255.255.255.224	192.168.1.65

1.3. Configuración Básica dispositivos

1.3.1. Completar la tabla con la configuración básica de los routers.

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

Configuración básica e interfaces de los routers

R1

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname Medellin
Medellin(config)#no ip domain-lookup
Medellin(config)#enable secret cisco
Medellin(config)#line vty 0 4
Medellin(config-line)#password cisco
Medellin(config-line)#login
Medellin(config-line)#exit
Medellin(config)#line console 0
Medellin(config-line)#password cisco
Medellin(config-line)#login
Medellin(config-line)#exit
Medellin(config)#banner motd "Access no authorized"
Medellin(config)#exit
Medellin#
%SYS-5-CONFIG_I: Configured from console by console
Medellin(config)#interface FastEthernet0/0
Medellin(config)#ip address 192.168.1.33 255.255.255.224
Medellin(config)#no shutdown
Medellin(config)#interface Serial0/0/0
Medellin(config)#ip address 192.168.1.99 255.255.255.224
```

```
Medellin(config)#no shutdown
Medellin(config)#clock rate 128000
Medellin#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
```

R2

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname Bogotá
Bogotá(config)#no ip domain-lookup
Bogotá(config)#enable secret cisco
Bogotá(config)#line vty 0 4
Bogotá(config-line)#password cisco
Bogotá(config-line)#login
Bogotá(config-line)#exit
Bogotá(config)#line console 0
Bogotá(config-line)#password cisco
Bogotá(config-line)#login
Bogotá(config-line)#exit
Bogotá(config)#banner motd "Access no authorized"
Bogotá(config)#exit
Bogotá#
%SYS-5-CONFIG_I: Configured from console by console
Bogotá( config)#interface FastEthernet0/0
Bogotá( config-if)#ip address 192.168.1.1 255.255.255.224
Bogotá( config-if)#no shutdown
Bogotá( config)#interface Serial0/0/0
Bogotá( config-if)#ip address 192.168.1.98 255.255.255.224
Bogotá( config-if)#no shutdown
Bogotá( config)#interface Serial0/0/1
Bogotá( config-if)#ip address 192.168.1.130 255.255.255.224
Bogotá( config-if)#no shutdown
Bogotá( config-if)#clock rate 128000
```

R3

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

```
Cali(config)#no ip domain-lookup
Cali(config)#enable secret cisco
Cali(config)#line vty 0 4
Cali(config-line)#password cisco
Cali(config-line)#login
Cali(config-line)#exit
Cali(config)#line console 0
Cali(config-line)#password cisco
Cali(config-line)#login
Cali(config-line)#exit
Cali(config)#banner motd "Access no authorized"
Cali(config)#exit
Cali#
%SYS-5-CONFIG_I: Configured from console by console
Cali(config)#interface FastEthernet0/0
Cali(config-if)#ip address 192.168.1.65 255.255.255.224
Cali(config-if)#no shutdown
Cali(config)#interface Serial0/0/0
Cali(config-if)#ip address 192.168.1.131 255.255.255.224
Cali(config-if)#no shutdown
Cali(config-if)#clock rate 128000

Cali#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
```

1.3.2. 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.

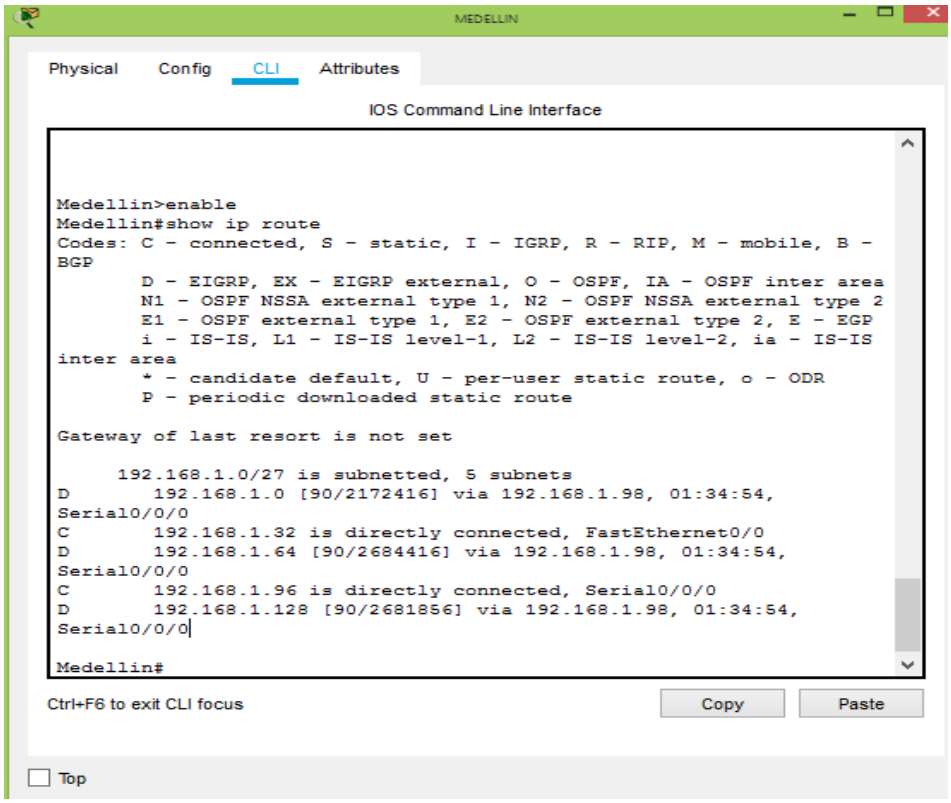
Con el comando **(show ip route**) me permite ver el contenido de la tabla de enrutamiento en cada uno de los routers.

R1 (Medellin)

```
Medellin>enable
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, 01:34:54, 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, 01:34:54, 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, 01:34:54, Serial0/0/0

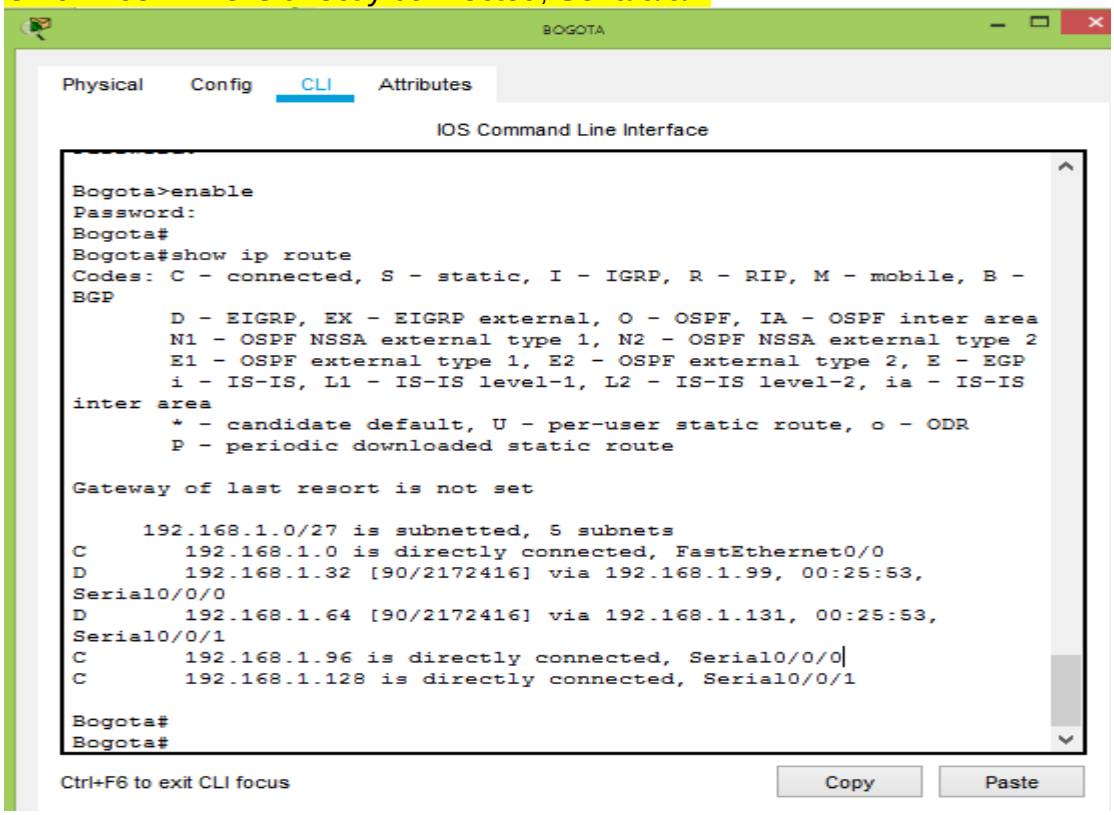


R2 (Bogotá)

Bogota#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

192.168.1.0/27 is subnetted, 5 subnets
C 192.168.1.0 is directly connected, FastEthernet0/0
D 192.168.1.32 [90/2172416] via 192.168.1.99, 00:25:53, Serial0/0/0
D 192.168.1.64 [90/2172416] via 192.168.1.131, 00:25:53, 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



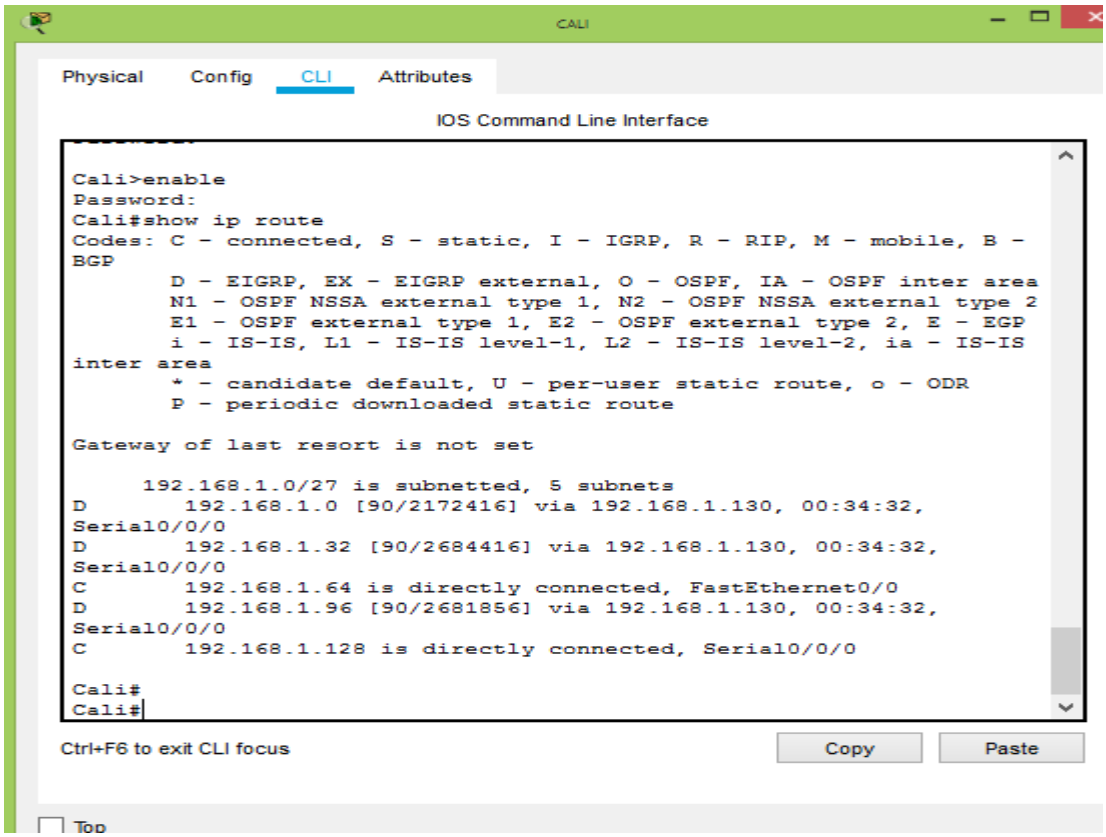
R3 (Cali)

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, 00:34:32, Serial0/0/0
D 192.168.1.32 [90/2684416] via 192.168.1.130, 00:34:32, 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, 00:34:32, Serial0/0/0
C 192.168.1.128 is directly connected, Serial0/0/0



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

Router Medellin

Medellin>enable
Password:
Medellin#sh ip eigrp topology
IP-EIGRP Topology Table for AS 30/ID(192.168.1.99)

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

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

Router Bogotá

Bogotá>enable
Password:
Bogota#sh ip eigrp topology
IP-EIGRP Topology Table for AS 30/ID(192.168.1.130)

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

P 192.168.1.0/27, 1 successors, FD is 28160
via Connected, FastEthernet0/0
P 192.168.1.32/27, 1 successors, FD is 2172416
via 192.168.1.99 (2172416/28160), Serial0/0/0
P 192.168.1.64/27, 1 successors, FD is 2172416
via 192.168.1.131 (2172416/28160), Serial0/0/1
P 192.168.1.96/27, 1 successors, FD is 2169856
via Connected, Serial0/0/0
P 192.168.1.128/27, 1 successors, FD is 2169856
via Connected, Serial0/0/1

Router Cali

Cali>enable
Password:
Cali#sh ip eigrp topology
IP-EIGRP Topology Table for AS 30/ID(192.168.1.131)

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

P 192.168.1.0/27, 1 successors, FD is 2172416
via 192.168.1.130 (2172416/28160), Serial0/0/0

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

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

Con el comando (show cdp neighbors) para verificación de vecinos encontramos:

- Device ID: Hostname del dispositivo vecino.
- Local Intrfce: Interface del dispositivo en el cual se ejecuta el comando, a través de la cual se recibe la información CDP del dispositivo vecino.
- Holdtime: Tiempo remanente en segundos por el cual este dispositivo aguardará una nueva actualización del dispositivo vecino, antes de descartar la entrada.
- Capability: Tipo de dispositivo que ha generado la información CDP que se ha recibido. Puede ser un router (R), switch (S), host (H).
- Platform: Modelo de dispositivo vecino del cual se ha recibido la información.
- Port ID: ID de puerto del dispositivo vecino que generó el paquete de información que se ha recibido.

show cdp: Este comando permite verificar la información global de CDP incluyendo temporizadores.

Router (Medellin)

Medellin>enable
Password:
Medellin#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
S - Switch, H - Host, I - IGMP, r - Repeater, P – Phone

Device ID	Local Intrfce	Holdtme	Capability	Platform	Port ID
Switch	Fas 0/0	156	S	2960	Fas 0/3
Bogotá	Ser 0/0/0	156	R	C2800	Ser 0/0/0

Medellin#show cdp
Global CDP information:
Sending CDP packets every 60 seconds
Sending a holdtime value of 180 seconds
Sending CDPv2 advertisements is enabled

Router (Bogotá)

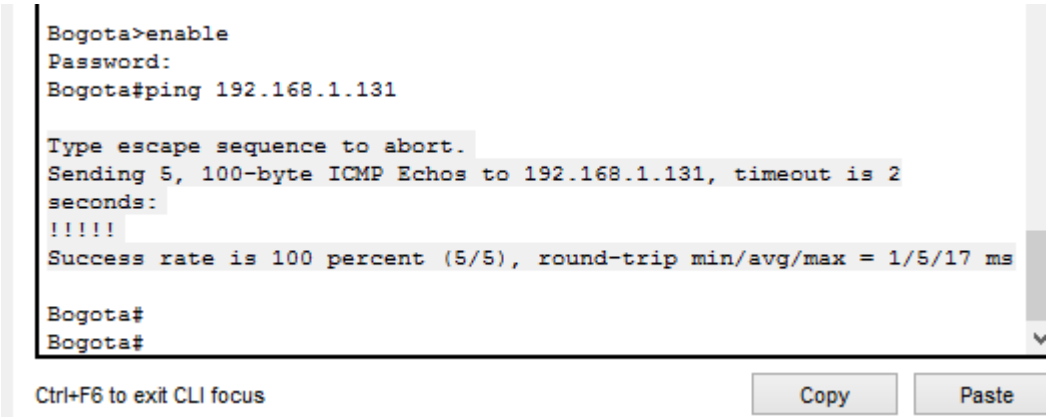
```
Bogotá>enable
Password:
Bogota#show cdp neighbors
Capability Codes:   R - Router, T - Trans Bridge, B - Source Route Bridge
                    S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID        Local Intrfce     Holdtme    Capability  Platform  Port
ID
Switch           Fas 0/0           174           S          2960      Fas
0/3
Cali             Ser 0/0/1         123           R          C2800     Ser
0/0/0
Medellin         Ser 0/0/0         124           R          C2800     Ser
0/0/0

Bogota#show cdp
Global CDP information:
Sending CDP packets every 60 seconds
Sending a holdtime value of 180 seconds
Sending CDPv2 advertisements is enabled
```

Router (Cali)

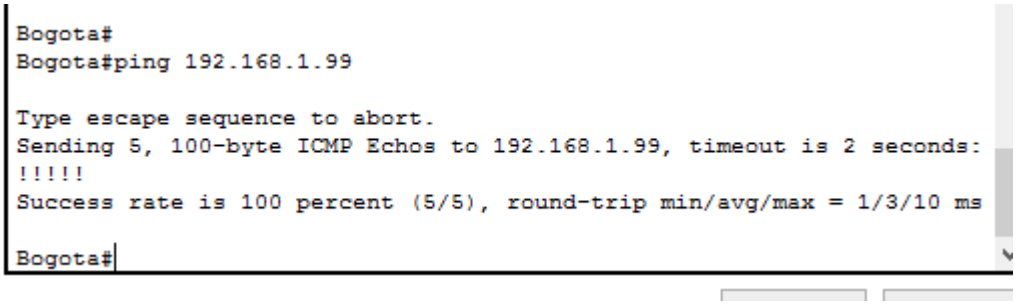
```
Cali>enable
Password:
Cali#show cdp neighbors
Capability Codes:      R - Router, T - Trans Bridge, B - Source Route Bridge
                       S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID        Local Intrfce     Holdtme    Capability  Platform  Port
ID
Switch           Fas 0/0           154           S          2960      Fas
0/3
Bogotá           Ser 0/0/0         154           R          C2800     Ser
0/0/1


Cali#show cdp
Global CDP information:
Sending CDP packets every 60 seconds
Sending a holdtime value of 180 seconds
Sending CDPv2 advertisements is enabled
```

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

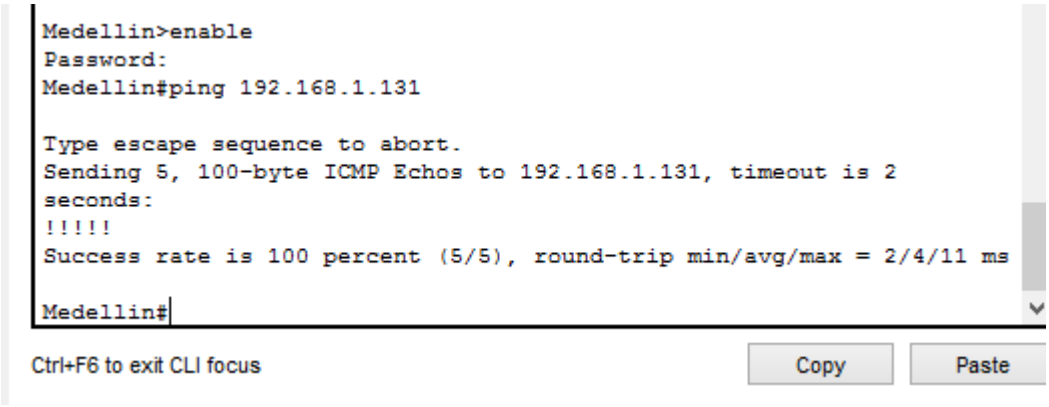
Ping del router de Bogota al router de Cali



Ping del router de Bogota al router de Medellin



Ping del router de Medellin al router de Cali



Ping de la red de Medellin (PC1) a la red de Cali (PC3)

```
    Minimum = 2ms, Maximum = 79ms, Average = 28ms

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=2ms TTL=125
Reply from 192.168.1.66: bytes=32 time=2ms TTL=125
Reply from 192.168.1.66: bytes=32 time=2ms TTL=125
Reply from 192.168.1.66: bytes=32 time=3ms TTL=125

Ping statistics for 192.168.1.66:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 3ms, Average = 2ms

C:\>
```

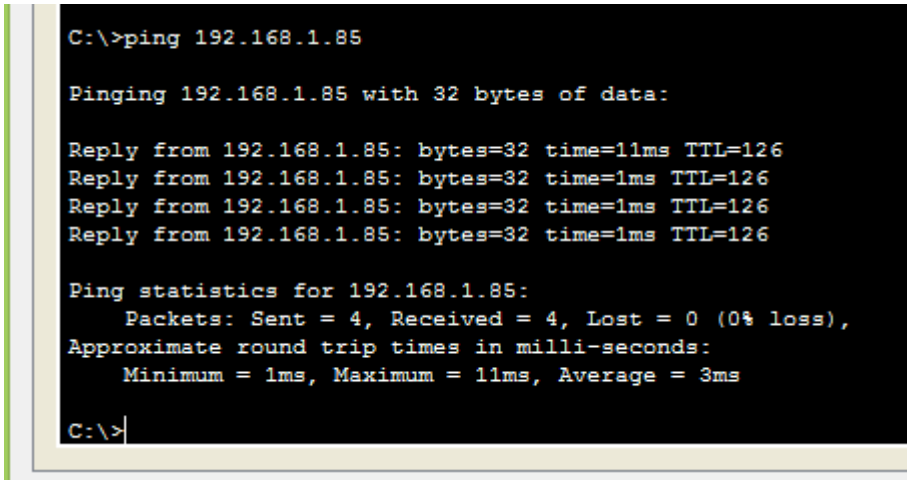
Ping de la red de Medellin (PC1) a la red de Bogotá (WS1)

```
C:\>ping 192.168.1.20

Pinging 192.168.1.20 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.20: bytes=32 time=19ms TTL=126
Reply from 192.168.1.20: bytes=32 time=1ms TTL=126
Reply from 192.168.1.20: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.1.20:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 19ms, Average = 7ms

C:\>
```

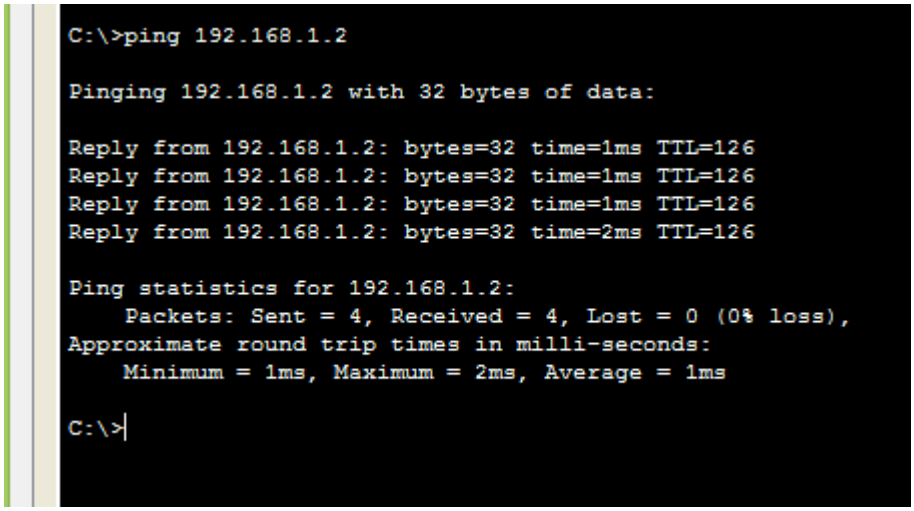
Ping de la red de Bogotá (WS1) a la red de Medellín (PC2)

```
C:\>ping 192.168.1.53

Pinging 192.168.1.53 with 32 bytes of data:

Reply from 192.168.1.53: bytes=32 time=2ms TTL=126
Reply from 192.168.1.53: bytes=32 time=2ms TTL=126
Reply from 192.168.1.53: bytes=32 time=1ms TTL=126
Reply from 192.168.1.53: bytes=32 time=16ms TTL=126

Ping statistics for 192.168.1.53:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 16ms, Average = 5ms

C:\>
```

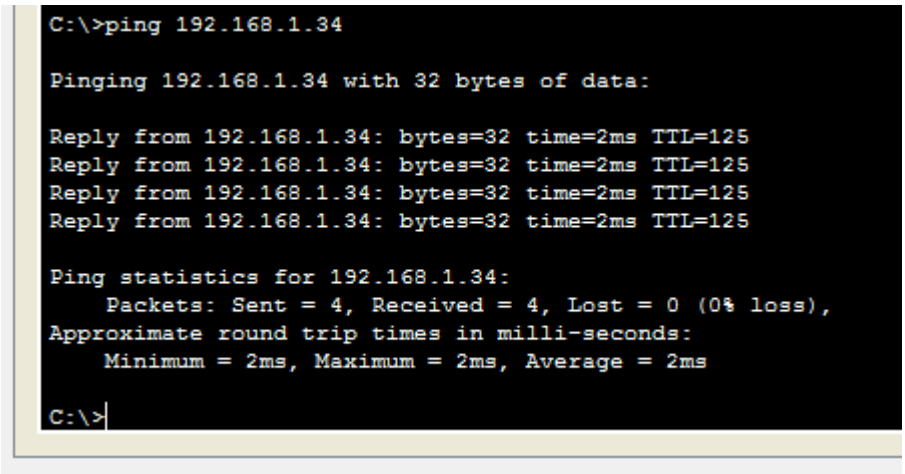
Ping de la red de Bogotá (WS1) a la red de Cali (PC2)



Ping de la red de Cali (PC3) a la red Bogotá (Servidor)



Ping de la red de Cali (PC3) a la red Medellín (PC1)



1.4. Configuración de Enrutamiento.

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

Configuración del protocolo EIGRP

Ingresamos a modo de Usuario, luego a modo privilegiado, luego a modo de configuración donde se aplicará el comando (router EIGRP 30) id para proceso autónomo el cual se debe configurar para los tres routers para que puedan tener comunicación interna entre ellos. Luego se coloca las redes que están conectadas a cada router conectadas con Wildcard, luego el comando (no auto-summary) para que no se haga sumarización

Router Medellin

Medellin>enable
Medellin#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Medellin(config)#router eigrp 30
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)#no auto-summary
Medellin(config-router)#exit

Router Cali

Cali >enable
Cali#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.

```
Cali(config)#router eigrp 30
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)#no auto-summary
Cali(config-router)#exit
```

Router Bogotá

```
Cali>enable
Cali#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Cali(config)#router eigrp 30
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)#no auto-summary
Cali(config-router)#exit
Cali(config)#
%DUAL-5-NBRCHANGE: IP-EIGRP 30: Neighbor 192.168.1.130 (Serial0/0/0) is up:
new adjacency

%DUAL-5-NBRCHANGE: IP-EIGRP 30: Neighbor 192.168.1.130 (Serial0/0/0) is
resync: graceful restart
```

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

Con el comando (show ip eigrp neighbors) verifico la vecindad de cada router.

Router Medellin (solo tiene vecindad con el router de Bogotá)

```
Medellin>enable
Password:
Medellin#show ip eigrp neighbors
IP-EIGRP neighbors for process 30
```

H	Address	Interface	Hold (sec)	Uptime	SRTT (ms)	RTO	Q Cnt	Seq Num
0	192.168.1.98	Se0/0/0	12	02:00:15	40	1000	0	6

Router Bogotá (Tiene vecindad con los routers de Cali y Medellin)

```
Bogotá>enable
Password:
```

```
Bogota#show ip eigrp neighbors
IP-EIGRP neighbors for process 30
H    Address         Interface   Hold  Uptime    SRTT   RTO     Q       Seq
                                 (sec)           (ms)         Cnt     Num
0    192.168.1.131   Se0/0/1     14    01:49:23  40     1000    0       7
1    192.168.1.99    Se0/0/0     13    01:49:22  40     1000    0       7
```

Router Cali (solo tiene vecindad con el route de Bogotá)

```
Cali>enable
Password:
Cali#show ip eigrp neighbors
IP-EIGRP neighbors for process 30
H    Address         Interface   Hold  Uptime    SRTT   RTO     Q       Seq
                                 (sec)           (ms)         Cnt     Num
0    192.168.1.130   Se0/0/0     12    02:02:49  40     1000    0       5
```

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

Para comprobar las tablas de enrutamiento se utilizará el comando (show ip route)

Router de 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, 02:16:46, 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, 02:16:46, 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, 02:16:46, Serial0/0/0
```

```
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, 02:16:46, 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, 02:16:46, 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, 02:16:46, Serial0/0/0

Medellin#
```

Router Bogotá

Bogotá>enable
Password:
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, 02:17:02, Serial0/0/0
D 192.168.1.64 [90/2172416] via 192.168.1.131, 02:17:03, 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

```
Accase no autorizado

User Access Verification

Password:

Bogota>enable
Password:
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, 02:17:02, Serial0/0/0
D       192.168.1.64 [90/2172416] via 192.168.1.131, 02:17:03, 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#
```

Router 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

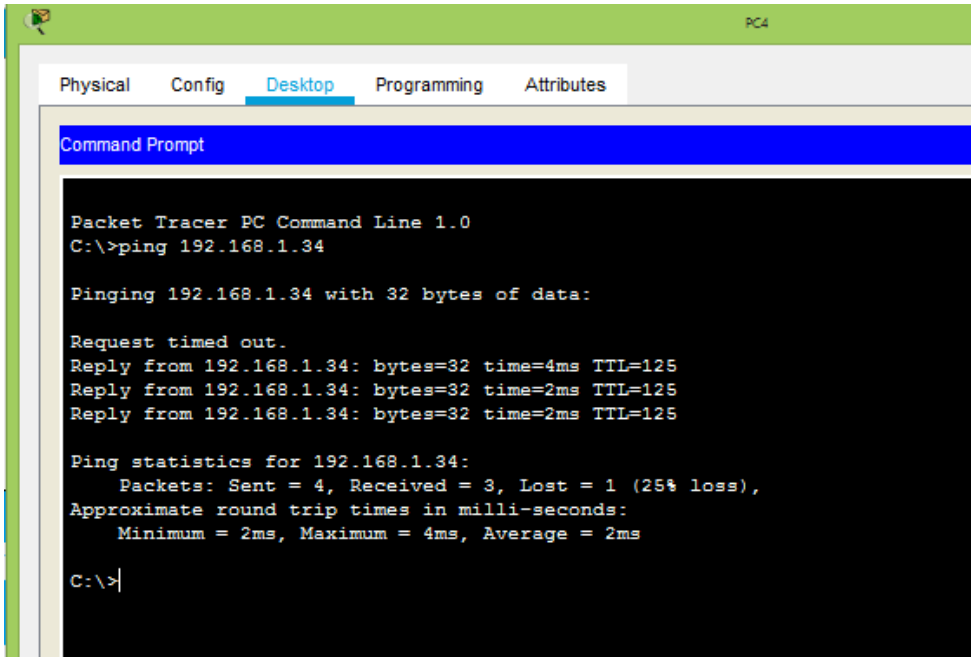
Gateway of last resort is not set

192.168.1.0/27 is subnetted, 5 subnets
D 192.168.1.0 [90/2172416] via 192.168.1.130, 02:17:11, Serial0/0/0
D 192.168.1.32 [90/2684416] via 192.168.1.130, 02:17:10, 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, 02:17:11, Serial0/0/0
C 192.168.1.128 is directly connected, Serial0/0/0

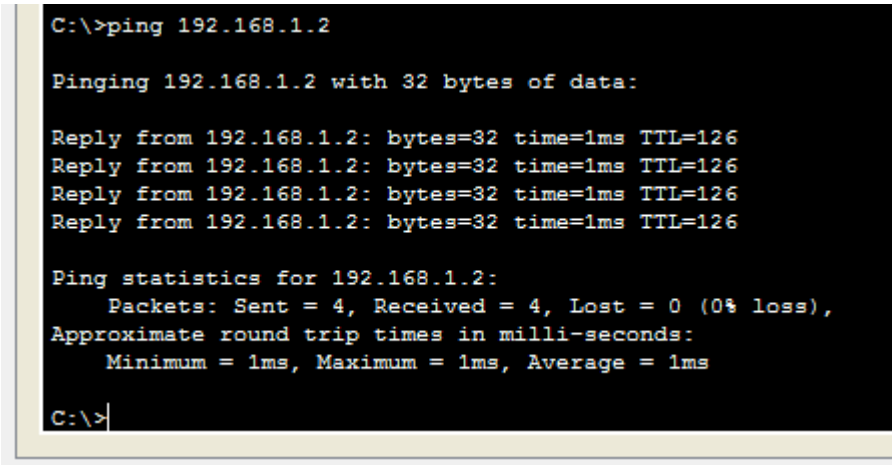
```
Cali#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - 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, 02:17:11, Serial0/0/0
D       192.168.1.32 [90/2684416] via 192.168.1.130, 02:17:10, 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, 02:17:11, Serial0/0/0
C       192.168.1.128 is directly connected, Serial0/0/0

Cali#
Cali#
```

1.4.4. 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.

Red LAN del router CALI a la red de MEDELLIN (PC1): Exitoso



Red LAN del router CALI, al servidor: Exitoso



1.5. Configuración de las listas de Control de Acceso.

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

Las condiciones para crear las ACL son las siguientes:

a. Cada router debe estar habilitado para establecer conexiones Telnet con los demás routers y tener acceso a cualquier dispositivo en la red.
b. El equipo WS1 y el servidor se encuentran en la subred de administración. Solo el servidor de la subred de administración debe tener acceso a cualquier otro dispositivo en cualquier parte de la red.
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.

Configuración de las listas de control de acceso (ACL) a los routers: El proceso de creación de las ACL se configuro por medio de ACL estándar.

LAN de Medellin

Medellin#config t
Enter configuration commands, one per line. End with CNTL/Z.
Medellin(config)#access-list 1 deny host 192.168.1.20
Medellin(config)#access-list 1 deny host 192.168.1.66
Medellin(config)#access-list 1 deny host 192.168.1.85
Medellin(config)#access-list 1 permit host 192.168.1.131

Medellin(config)#access-list 1 permit host 192.168.1.1
Medellin(config)#access-list 1 permit host 192.168.1.2
Medellin(config)#interface fastethernet 0/0
Medellin(config-if)#ip access-group 1 out

```
Medellin#show access-lists
Standard IP access list 1
    10 deny host 192.168.1.20
    20 deny host 192.168.1.66
    30 deny host 192.168.1.85
    40 permit host 192.168.1.131
    50 permit host 192.168.1.1
    60 permit host 192.168.1.2
```

LAN Bogotá

Bogota#config t
Enter configuration commands, one per line. End with CNTL/Z.
Bogotá(config)#no access-list 1
Bogotá(config)#access-list 1 permit 192.168.1.33 0.0.0.31
Bogotá(config)#access-list 1 permit host 192.168.1.99
Bogotá(config)#access-list 1 permit 192.168.1.65 0.0.0.31
Bogotá(config)#access-list 1 permit host 192.168.1.131
Bogotá(config)#access-list 1 deny any
Bogotá(config)#interface fastethernet 0/0
Bogotá(config-if)#ip access-group 1 out

```
Bogota#show access-lists
Standard IP access list 1
    10 permit 192.168.1.32 0.0.0.31
    20 permit host 192.168.1.99
    30 permit 192.168.1.64 0.0.0.31
    40 permit host 192.168.1.131
    50 deny any
```

LAN de Cali

Cali(config)#access-list 1 permit host 192.168.1.2
Cali(config)#access-list 1 permit host 192.168.1.1
Cali(config)#access-list 1 permit host 192.168.1.99
Cali(config)#access-list 1 deny host 192.168.1.20
Cali(config)#access-list 1 deny host 192.168.1.34

Cali(config)#access-list 1 deny host 192.168.1.53
Cali(config)#interface fastethernet 0/0
Cali(config-if)#ip access-group 1 out

```
Cali#show access-lists
Standard IP access list 1
    10 permit host 192.168.1.2
    20 permit host 192.168.1.1
    30 permit host 192.168.1.99
    40 deny host 192.168.1.20
    50 deny host 192.168.1.34
    60 deny host 192.168.1.53

Cali#
```

1.6. Comprobación de la red instalada.

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

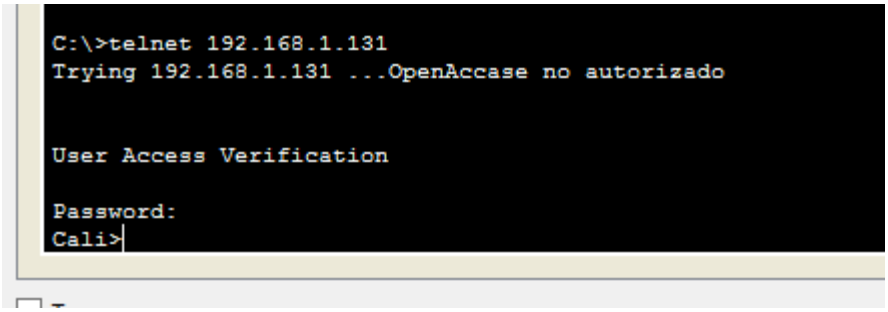
- **Router Medellín a Router Cali**

```
Password:

Medellin>enable
Password:
Medellin#telnet 192.168.1.131
Trying 192.168.1.131 ...OpenAccase no autorizado


User Access Verification

Password:
Cali>enable
Password:
Cali#
```

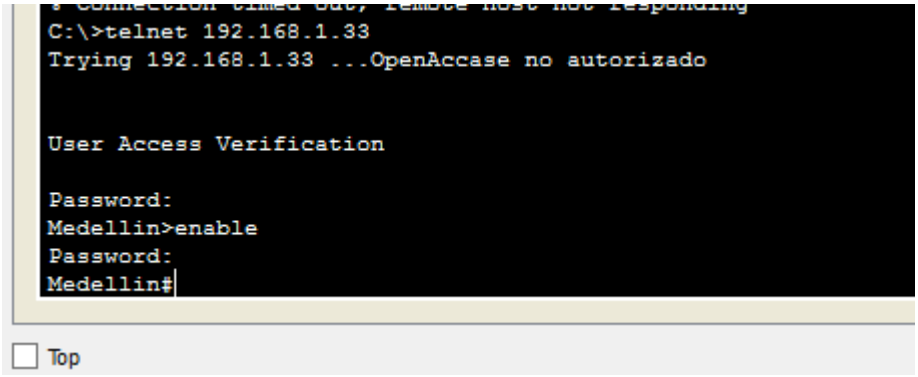
- **WS_1 al Router Bogotá**

```
C:\>telnet 192.168.1.1
Trying 192.168.1.1 ...OpenAccase no autorizado


User Access Verification

Password:
Password:
Bogota>enable
Password:
Bogota#
```

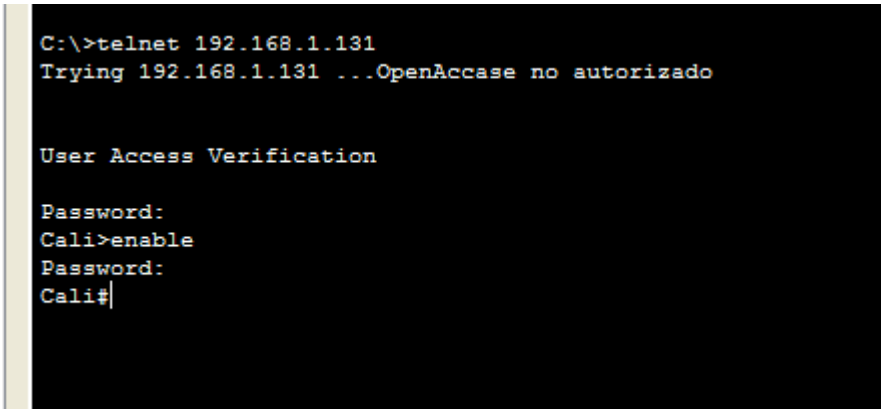
- **Servidor al Router Cali**



- **Servidor a Router Medellín**



- **LAN del Router Medellin a Router Cali**



- **LAN del router Cali al router de Cali**

```
Packet Tracer PC Command Line 1.0
C:\>telnet 192.168.1.131
Trying 192.168.1.131 ...OpenAccase no autorizado


User Access Verification

Password:
Cali>
```

- **LAN del router Medellin al router de Medellin**

```
C:\>telnet 192.168.1.33
Trying 192.168.1.33 ...OpenAccase no autorizado


User Access Verification

Password:
Medellin>enable
Password:
Medellin#
```

- **LAN del router Cali al router de Medellin**

```
[Connection to 192.168.1.131 closed by foreign host]
C:\>telnet 192.168.1.99
Trying 192.168.1.99 ...OpenAccase no autorizado


User Access Verification

Password:
Medellin>
```

- **LAN del router Cali a WS1**

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.20

Pinging 192.168.1.20 with 32 bytes of data:

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

Ping statistics for 192.168.1.20:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

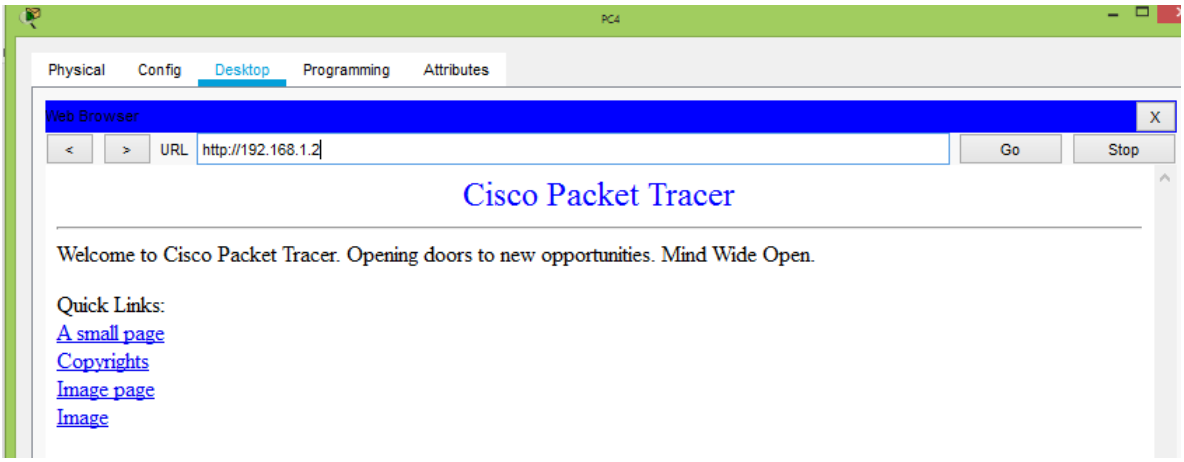
- **LAN del router Medellin a WS1**

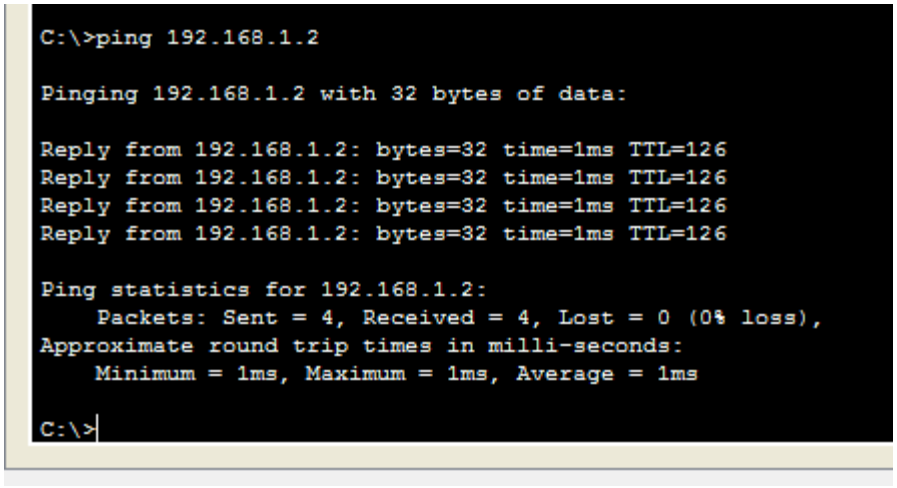
```
C:\>ping 192.168.1.20

Pinging 192.168.1.20 with 32 bytes of data:

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

Ping statistics for 192.168.1.20:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

- **LAN del router Medellin a LAN router de Cali**

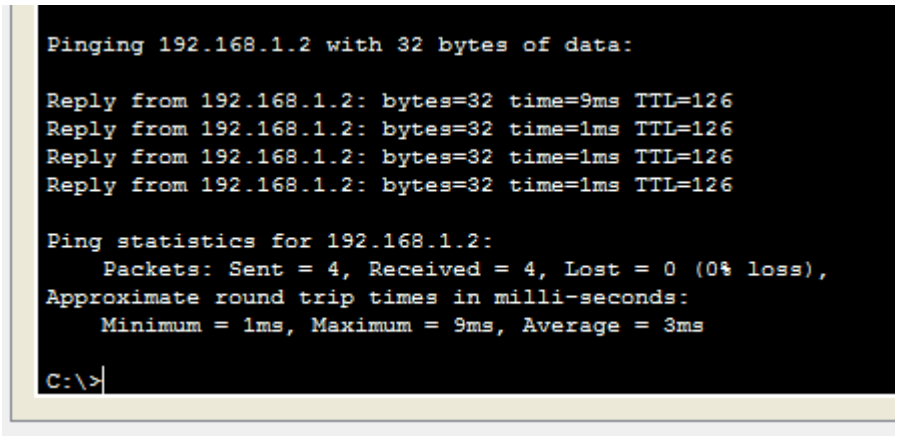
```
C:\>ping 192.168.1.66

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.
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 = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

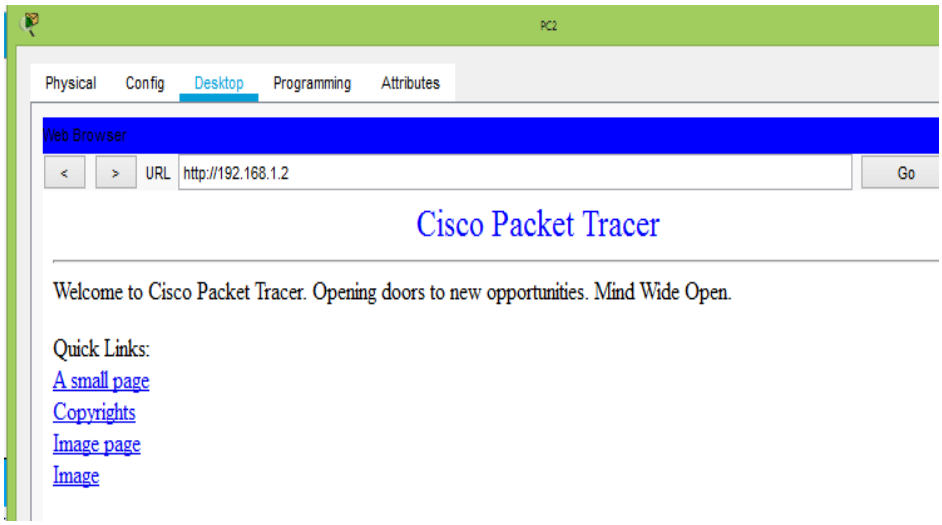
- **LAN del router Cali al servidor**



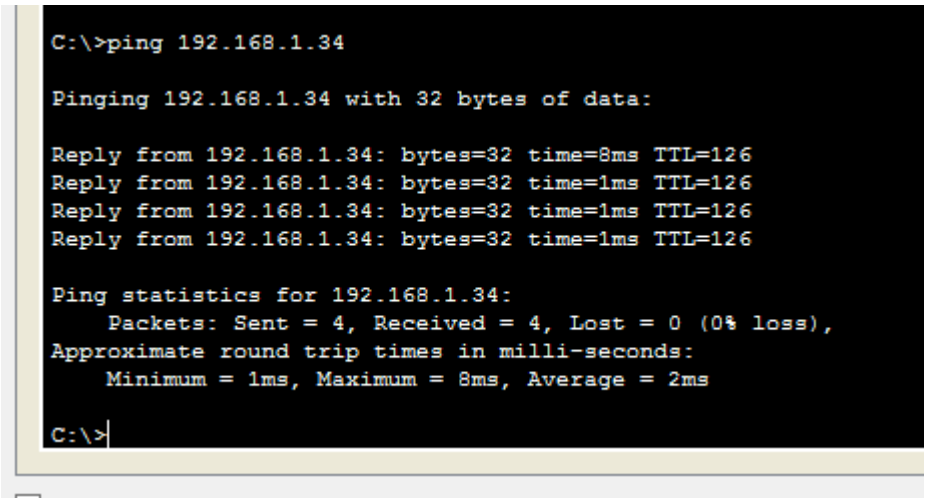


- **LAN del router Medellin al servidor**





- **Servidor a LAN del router Medellin**



- **Servidor a LAN del router Cali**

```
C:\>ping 192.168.1.85

Pinging 192.168.1.85 with 32 bytes of data:

Reply from 192.168.1.85: bytes=32 time=2ms TTL=126
Reply from 192.168.1.85: bytes=32 time=1ms TTL=126
Reply from 192.168.1.85: bytes=32 time=1ms TTL=126
Reply from 192.168.1.85: bytes=32 time=13ms TTL=126

Ping statistics for 192.168.1.85:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 13ms, Average = 4ms

C:\>
```

- **Router Cali a LAN del router Medellin**

```
Password:
Cali#ping 192.168.1.53

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.53, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/6/10 ms

Cali#
```

Ctrl+F6 to exit CLI focus Copy Paste

- **Router Medellin a LAN del router Cali**

```
Medellin>enable
Password:
Medellin#ping 192.168.1.85

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.85, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/9/20 ms

Medellin#
```

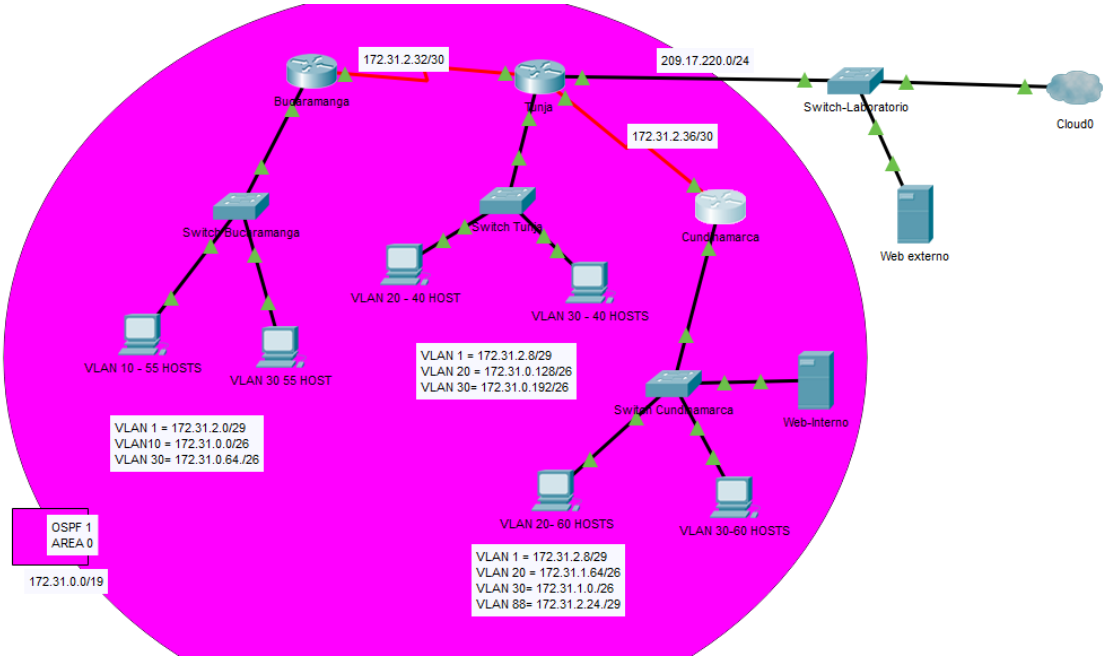
Ctrl+F6 to exit CLI focus Copy Paste

- 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	Exitoso
	LAN del Router CALI	Router CALI	Exitoso
	LAN del Router MEDELLIN	Router MEDELLIN	Exitoso
	LAN del Router CALI	Router MEDELLIN	Exitoso
PING	LAN del Router CALI	WS_1	Fallido
	LAN del Router MEDELLIN	WS_1	Fallido
	LAN del Router MEDELLIN	LAN del Router CALI	Fallido
PING	LAN del Router CALI	Servidor	Exitoso
	LAN del Router MEDELLIN	Servidor	Exitoso
	Servidor	LAN del Router MEDELLIN	Exitoso
	Servidor	LAN del Router CALI	Exitoso
	Router CALI	LAN del Router MEDELLIN	Exitoso
	Router MEDELLIN	LAN del Router CALI	Exitoso

2. ESCENARIO 2

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



Desarrollo

2.1. Configuración básica dispositivos.

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

# hosts	Id. red	Prefijo	Rango de direcciones		broadcast	Mascara de sub red
			Primera IP	Ultima IP		
55	172.31.0.0	26	172.31.0.1	172.31.0.62	172.31.0.63	255.255.255.192
55	172.31.0.64	26	172.31.0.65	172.31.0.126	172.31.0.127	255.255.255.192
40	172.31.0.128	26	172.31.0.129	172.31.0.190	172.31.0.191	255.255.255.192
40	172.31.0.192	26	172.31.0.193	172.31.0.254	172.31.0.255	255.255.255.192
60	172.31.1.0	26	172.31.1.1	172.31.1.62	172.31.1.63	255.255.255.192
60	172.31.1.64	26	172.31.1.2	172.31.1.126	172.31.1.127	255.255.255.192
1	172.31.2.24	29	172.31.2.25	172.31.2.30	172.31.2.31	255.255.255.248

VLAN 1 con la red 172.31.2.0/29 Bucaramanga

Host	Id. red	Prefijo	Rango de direcciones		broadcast	Mascara de sub red
			Primera IP	Ultima IP		
1	172.31.2.0	29	172.31.2.1	172.31.2.2	172.31.2.3	255.255.255.248

VLAN 1 172.31.2.8/29 Tunja

Host	Id. red	Prefijo	Rango de direcciones		broadcast	Mascara de sub red
			Primera IP	Ultima IP		
1	172.31.2.8	29	172.31.2.9	172.31.2.14	172.31.2.15	255.255.255.248

VLAN 1 con la red 172.31.2.8/29 Cundinamarca

Host	Id. red	Prefijo	Rango de direcciones		broadcast	Mascara de sub red
			Primera IP	Ultima IP		
1	172.31.2.8	29	172.31.2.9	172.31.2.14	172.31.2.15	255.255.255.248

Red 209.17.220.0/24

Host	Id. red	Prefijo	Rango de direcciones		broadcast	Mascara de sub red
			Primera IP	Ultima IP		
1	209.17.220.0	24	209.17.220.1	209.17.220.254	209.17.220.255	255.255.255.0

Enlaces de routers con la red 172.31.2.32/30

Enlace	Id. red	Prefijo	Rango de direcciones		broadcast	Mascara de sub red
			Primera IP	Ultima IP		
1	172.31.2.32	30	172.31.2.33	172.31.2.34	172.31.2.35	255.255.255.252
2	172.31.2.36	30	172.31.2.37	172.31.2.38	172.31.2.39	255.255.255.252

Tabla de direccionamiento de la red.

DISPOSITIVO	INTERFAZ	DIRECCION IP	MASCARA DE SUBRED
R-Bucaramanga	Fa0/0	172.31.2.1	255.255.255.192
	S0/1/0	172.31.2.33	255.255.255.252

R-Tunja	Fa0/0	172.31.2.9	255.255.255.248
	Fa0/1	209.17.220.1	255.255.255.0
	S0/1/0	172.31.2.38	255.255.255.252
	S0/1/1	172.31.2.34	255.255.255.252
R-Cundinamarca	Fa0/0		255.255.255.224
	S0/1/0	172.31.2.37	255.255.255.252
Switch Bucaramanga	Vlan 1	172.31.2.1	255.255.255.248
Switch Tunja	Vlan 1	172.31.2.9	255.255.255.248
Switch Cundinamarca	Vlan 1	172.31.2.10	255.255.255.248
Switch Laboratorio	F0/3	209.17.220.254	255.255.255.0
PC-VLAN 10 Bucaramanga	F0/0.10	172.31.0.1	255.255.255.192
PC-VLAN 30 Bucaramanga	F0/0.30	172.31.0.65	255.255.255.192
PC-VLAN 20 Tunja	F0/0.20	172.31.0.129	255.255.255.192
PC-VLAN 30 Tunja	F0/0.30	172.31.0.193	255.255.255.192
PC-VLAN 1 Cundinamarca	F0/0.1	172.31.2.10	255.255.255.248
PC-VLAN 20 Cundinamarca	F0/0.20	172.31.1.65	255.255.255.192
PC-VLAN 30 Cundinamarca	F0/0.30	172.31.1.1	255.255.255192
Web interno – VLAN 88 Cundinamarca	F0/0.80	172.31.2.25	255.255.255.248
Web externo Cundinamarca	F0/1	209.17.220.1	255.255.255.0

2.1.2. Configuración routers

- **Nombrar router Bucaramanga**

```
Router>enable
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname Bucaramanga
Bucaramanga(config)#
```

- **Configurar contraseñas y banner**

```
Bucaramanga(config)#no ip domain-lookup
Bucaramanga(config)#enable secret cisco
Bucaramanga(config)#line vty 0 15
Bucaramanga(config-line)#password cisco
Bucaramanga(config-line)#login
Bucaramanga(config-line)#exit
Bucaramanga(config)#line console 0
Bucaramanga(config-line)#password cisco
Bucaramanga(config-line)#login
Bucaramanga(config-line)#exit
Bucaramanga(config)#banner motd "Access no authorized"
Bucaramanga(config)#
```

- **Autenticación local con AAA.**
- **Cifrado de contraseñas.**
- **Un máximo de internos para acceder al router.**
- **Máximo tiempo de acceso al detectar ataques**

```
Bucaramanga(config)#aaa new-model
Bucaramanga(config)#username Bucaramanga secret cisco
Bucaramanga(config)#aaa authentication login AUTH local
Bucaramanga(config)#line console 0
Bucaramanga(config-line)#login authentication AUTH
Bucaramanga(config-line)#line vty 0 15
Bucaramanga(config-line)#login authentication AUTH
Bucaramanga(config-line)#exit
Bucaramanga(config)#service password-encryption
Bucaramanga(config)#login block-for 30 attempts 5 within 60
```

- **Configurar interfaces y subinterfaces**

```
Bucaramanga#config t
Enter configuration commands, one per line. End with CNTL/Z.
Bucaramanga(config)#interface f0/0
Bucaramanga(config-if)#no ip address
Bucaramanga(config-if)#exit
Bucaramanga(config)#interface f0/0.1
Bucaramanga(config-subif)#encapsulation dot1Q 1
Bucaramanga(config-subif)#ip address 172.31.2.1 255.255.255.248
Bucaramanga(config-subif)#exit
Bucaramanga(config)#interface f0/0.10
Bucaramanga(config-subif)#encapsulation dot1Q 10
```

```
Bucaramanga(config-subif)#ip address 172.31.0.1 255.255.255.192
Bucaramanga(config-subif)#ip helper-address 172.31.2.33
Bucaramanga(config-subif)#exit
Bucaramanga(config)#interface f0/0.30
Bucaramanga(config-subif)#encapsulation dot1Q 30
Bucaramanga(config-subif)#ip address 172.31.0.65 255.255.255.192
Bucaramanga(config-subif)#ip helper-address 172.31.2.33
Bucaramanga(config-subif)#exit
Bucaramanga(config)#interface s0/1/0
Bucaramanga(config-if)#ip address 172.31.2.33 255.255.255.252
Bucaramanga(config-if)#clock rate 128000
Bucaramanga(config-if)#no shutdown
Bucaramanga(config-if)#
%LINK-5-CHANGED: Interface Serial0/1/0, changed state to up
Bucaramanga(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed state
to up
Bucaramanga(config-if)#exit
Bucaramanga(config)#interface FastEthernet0/0
Bucaramanga(config-if)#no shutdown
Bucaramanga(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
%LINK-5-CHANGED: Interface FastEthernet0/0.1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.1, changed
state to up
%LINK-5-CHANGED: Interface FastEthernet0/0.10, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.10,
changed state to up
%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

Bucaramanga(config-if)#end
Bucaramanga#
%SYS-5-CONFIG_I: Configured from console by console

Bucaramanga#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Bucaramanga#
```

- **Nombrar al router Tunja**

```
Router>enable
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname Tunja
Tunja(config)#
```

- **Configurar contraseñas y banner**

```
Tunja(config)#no ip domain-lookup
Tunja(config)#enable secret cisco
Tunja(config)#line vty 0 15
Tunja(config-line)#password cisco
Tunja(config-line)#login
Tunja(config-line)#exit
Tunja(config)#line console 0
Tunja(config-line)#password cisco
Tunja(config-line)#login
Tunja(config-line)#exit
Tunja(config)#banner motd "Access no authorized"
Tunja(config)#
```

- **Autenticación local con AAA.**
- **Cifrado de contraseñas.**
- **Un máximo de internos para acceder al router.**
- **Máximo tiempo de acceso al detectar ataques**

```
Tunja(config)#aaa new-model
Tunja(config)#username Tunja secret cisco
Tunja(config)#aaa authentication login AUTH local
Tunja(config)#line console 0
Tunja(config-line)#login authentication AUTH
Tunja(config-line)#line vty 0 15
Tunja(config-line)#login authentication AUTH
Tunja(config-line)#login block-for 30 attempts 5 within 60
Tunja(config)#service password-encryption
Tunja(config)#exit
```

- **Configurar interfaces y subinterfaces**

```
Tunja(config)#interface f0/1
Tunja(config-if)#ip address 209.17.220.1 255.255.255.0
Tunja(config-if)#exit
Tunja(config)#interface f0/0
Tunja(config-if)#no ip address
```

```
Tunja(config-if)#exit
Tunja(config)#interface f0/0.1
Tunja(config-subif)#encapsulation dot1Q 1
Tunja(config-subif)#ip address 172.31.2.9 255.255.255.248
Tunja(config-subif)#exit
Tunja(config)#interface f0/0.20
Tunja(config-subif)#encapsulation dot1Q 20
Tunja(config-subif)#ip address 172.31.0.129 255.255.255.192
Tunja(config-subif)#exit
Tunja(config)#interface f0/0.30
Tunja(config-subif)#encapsulation dot1Q 30
Tunja(config-subif)#ip address 172.31.0.193 255.255.255.192
Tunja(config-subif)#exit
Tunja(config)#interface s0/1/1
Tunja(config-if)#ip address 172.31.2.34 255.255.255.252
Tunja(config-if)#no shutdown
Tunja(config-if)#exit
Tunja(config)#interface s0/1/0
Tunja(config-if)#ip address 172.31.2.38 255.255.255.252
Tunja(config-if)#clock rate 128000

Tunja(config-if)#no shutdown
Tunja(config-if)#exit
Tunja(config)#interface vlan 1
Tunja(config-if)#shutdown
Tunja(config-if)#exit
Tunja(config)#interface FastEthernet0/0
Tunja(config-if)#no shutdown
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed
state to up
%LINK-5-CHANGED: Interface FastEthernet0/0.1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.1, changed
state to up
%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
%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

Tunja#config t
Tunja(config)#interface FastEthernet0/1
Tunja(config-if)#no shutdown
```

Tunja(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

- **Guardar información**

Tunja#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Tunja#

- **Nombrar al router Cundinamarca**

Router>enable
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname Cundinamarca
Cundinamarca(config)#

- **Configurar contraseñas y banner**

Cundinamarca(config)#no ip domain-lookup
Cundinamarca(config)#enable secret cisco
Cundinamarca(config)#line vty 0 15
Cundinamarca(config-line)#password cisco
Cundinamarca(config-line)#login
Cundinamarca(config-line)#exit
Cundinamarca(config)#line console 0
Cundinamarca(config-line)#password cisco
Cundinamarca(config-line)#login
Cundinamarca(config-line)#exit
Cundinamarca(config)#banner motd "Access no authorized"
Cundinamarca(config)#

- **Autenticación local con AAA.**
- **Cifrado de contraseñas.**
- **Un máximo de internos para acceder al router.**
- **Máximo tiempo de acceso al detectar ataques**

```
Cundinamarca(config)#aaa new-model
Cundinamarca(config)#username Cundinamarca secret cisco
Cundinamarca(config)#aaa authentication login AUTH local
Cundinamarca(config)#line console 0
Cundinamarca(config-line)#login authentication AUTH
Cundinamarca(config-line)#line vty 0 15
Cundinamarca(config-line)#login authentication AUTH
Cundinamarca(config-line)#login block-for 30 attempts 5 within 60
Cundinamarca(config)#service password-encryption
Cundinamarca(config)#exit
```

- **Configurar interfaces y subinterfaces**

```
Cundinamarca(config)#interface f0/0
Cundinamarca(config-if)#no ip address
Cundinamarca(config-if)#exit
Cundinamarca(config)#interface f0/0.1
Cundinamarca(config-subif)#encapsulation dot1Q 1
Cundinamarca(config-subif)#ip address 172.31.2.10 255.255.255.248
Cundinamarca(config-subif)#exit
Cundinamarca(config)#interface f0/0.20
Cundinamarca(config-subif)#encapsulation dot1Q 20
Cundinamarca(config-subif)#ip address 172.31.1.65 255.255.255.192
Cundinamarca(config-subif)#exit
Cundinamarca(config)#interface f0/0.30
Cundinamarca(config-subif)#encapsulation dot1Q 30
Cundinamarca(config-subif)#ip address 172.31.1.1 255.255.255.192
Cundinamarca(config-subif)#exit
Cundinamarca(config)#interface f0/0.88
Cundinamarca(config-subif)#encapsulation dot1Q 88
Cundinamarca(config-subif)#ip address 172.31.2.25 255.255.255.248
Cundinamarca(config-subif)#exit
Cundinamarca(config)#interface s0/1/0
Cundinamarca(config-if)#ip address 172.31.2.38 255.255.255.252
Cundinamarca(config-if)#no shutdown
Cundinamarca(config-if)#exit
Cundinamarca(config)#interface FastEthernet0/0
Cundinamarca(config-if)#no shutdown
Cundinamarca(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
```

%LINK-5-CHANGED: Interface FastEthernet0/0.1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.1, changed state to up
%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
%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
%LINK-5-CHANGED: Interface FastEthernet0/0.88, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.88, changed state to up

- **Guardamos la información**

Cundinamarca#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Cundinamarca#

2.1.3. Configuración VLANS

Creamos las vlans, asignamos puertos, se configura el enlace troncal.

- **Switch Bucaramanga**

Nombramos las vlans.

SB#config t
Enter configuration commands, one per line. End with CNTL/Z.
SB(config)#vlan 10
SB(config-vlan)#name vlan10
SB(config-vlan)#exit
SB(config)#vlan 30
SB(config-vlan)#name vlan30
SB(config-vlan)#exit
SB(config)#int vlan1
SB(config-if)#ip address 172.31.2.2 255.255.255.248
SB(config-if)#ip default-gateway 172.31.2.1
SB(config-if)#no shutdown
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

Truncamiento

SB(config-vlan)#exit
SB(config)#interface f0/3
SB(config-if)#switchport mode trunk

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

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

Asignamos puertos a las vlans.

SB(config-if)#interface f0/2
SB(config-if)#switchport mode access
SB(config-if)#switchport access vlan 30
SB(config-if)#interface f0/1
SB(config-if)#switchport mode access
SB(config-if)#switchport access vlan 10

- **Switch Tunja**

Nombramos las vlans.

Switch>enable
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname ST
ST(config)#vlan 20
ST(config-vlan)#name vlan20
ST(config-vlan)#exit
ST(config)#vlan 30
ST(config-vlan)#name vlan30
ST(config-vlan)#exit
ST(config)#int vlan 1
ST(config-if)#ip address 172.31.2.10 255.255.255.248
ST(config-if)#ip default-gateway 172.31.2.9
ST(config)#int vlan 1
ST(config-if)#no shutdown
ST(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

Truncamiento

ST(config)#interface f0/1
ST(config-if)#switchport mode trunk

ST(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

Asignamos puertos a las interfaces

ST(config-if)#interface f0/2
ST(config-if)#switchport mode access
ST(config-if)#switchport access vlan 30
ST(config-if)#interface f0/1
ST(config-if)#switchport mode access
ST(config-if)#switchport access vlan 20
ST(config-if)#end

- **Switch Cundinamarca**

Nombramos las vlans.

Switch#enable
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SC
SC(config)#vlan 20
SC(config-vlan)#name vlan20
SC(config-vlan)#exit
SC(config)#vlan 30
SC(config-vlan)#name vlan30
SC(config-vlan)#exit
SC(config)#vlan 88
SC(config-vlan)#name vlan88
SC(config-vlan)#exit
SC(config)#int vlan 1
SC(config-if)#ip address 172.31.2.11 255.255.255.248
SC(config-if)#no shutdown

SC(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
SC(config-if)#ip default-gateway 172.31.2.10
SC(config)#

Truncamiento

SC(config)#interface f0/1
SC(config-if)#switchport mode trunk

SC(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

Asignamos puertos a las vlans

SC(config-if)#interface f0/2
SC(config-if)#switchport mode access
SC(config-if)#switchport access vlan 88
SC(config-if)#interface f0/3
SC(config-if)#switchport mode access
SC(config-if)#switchport access vlan 30
SC(config-if)#interface f0/4
SC(config-if)#switchport mode access
SC(config-if)#switchport access vlan 20
SC(config-if)#end

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

Cundinamarca#dir flash:
Directory of flash:/

3 -rw- 50938004 <no date> c2800nm-advipservicesk9-mz.124-15.T1.bin
2 -rw- 28282 <no date> sigdef-category.xml
1 -rw- 227537 <no date> sigdef-default.xml

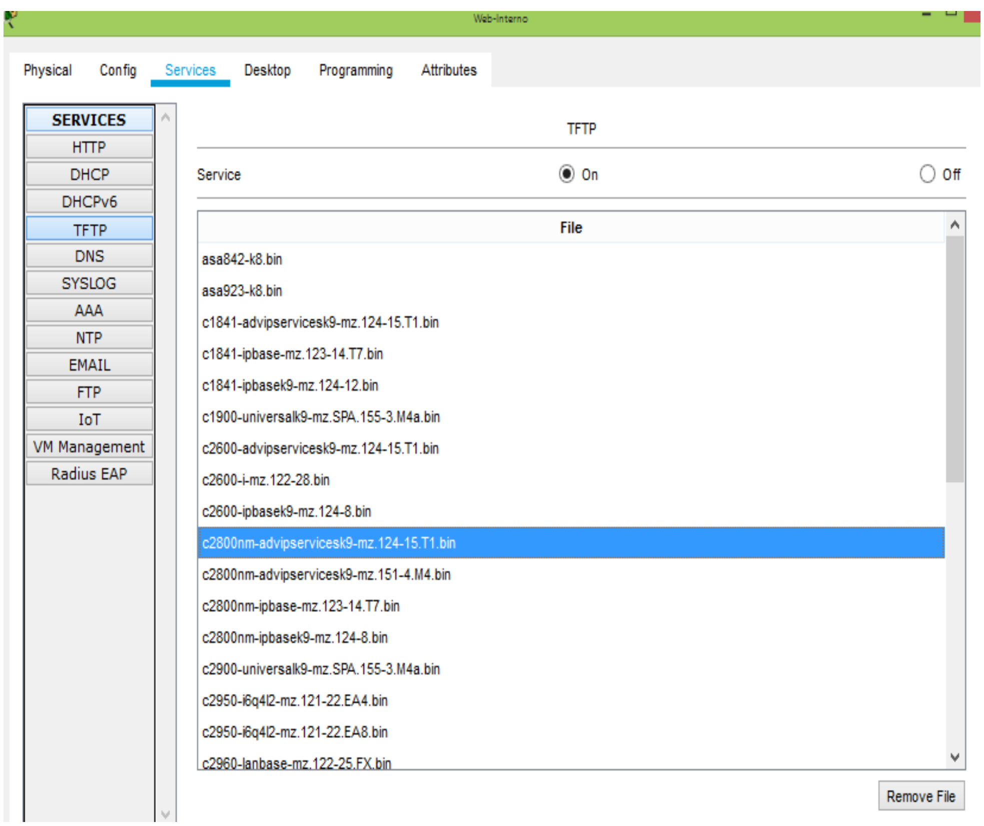
64016384 bytes total (12822561 bytes free)
Cundinamarca#

Con el comando (copy flash: tftp:) copiaremos los archivos del router al servidor TFTP.

Cundinamarca#copy flash: tftp:
Source filename []? c2800nm-advipservicesk9-mz.124-15.T1.bin
Address or name of remote host []? 172.31.2.26
Destination filename [c2800nm-advipservicesk9-mz.124-15.T1.bin]?

Writing c2800nm-advipservicesk9-mz.124-15.T1.bin...!!
!!!
!!
!!
!!
!!
!!
!!!
[OK - 50938004 bytes]

50938004 bytes copied in 1.422 secs (2597302 bytes/sec)
Cundinamarca#



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

- **configuración dhcp router Tunja**

```
Tunja(config)#ip dhcp excluded-address 172.31.2.1 172.31.2.2
Tunja(config)#ip dhcp excluded-address 172.31.0.1
Tunja(config)#ip dhcp excluded-address 172.31.0.65
Tunja(config)#ip dhcp excluded-address 172.31.2.9 172.31.2.11
Tunja(config)#ip dhcp excluded-address 172.31.1.65
Tunja(config)#ip dhcp excluded-address 172.31.1.1
Tunja(config)#ip dhcp excluded-address 172.31.2.25
Tunja(config)#ip dhcp excluded-address 172.31.2.10
Tunja(config)#ip dhcp pool vlan10-Bucaramanga
Tunja(dhcp-config)#network 172.31.0.0 255.255.255.192
Tunja(dhcp-config)#default-router 172.31.0.1
Tunja(dhcp-config)#dns-server 172.31.2.26
Tunja(dhcp-config)#ip dhcp pool vlan30-Bucaramanga
Tunja(dhcp-config)#network 172.31.0.64 255.255.255.192
Tunja(dhcp-config)#default-router 172.31.0.65
Tunja(dhcp-config)#dns-server 172.31.2.26
Tunja(dhcp-config)#ip dhcp pool vlan20-Cundinamarca
Tunja(dhcp-config)#network 172.31.1.64 255.255.255.192
Tunja(dhcp-config)#default-router 172.31.1.65
Tunja(dhcp-config)#dns-server 172.31.2.26
Tunja(dhcp-config)#ip dhcp pool vlan30-Cundinamarca
Tunja(dhcp-config)#network 172.31.1.0 255.255.255.192
Tunja(dhcp-config)#default-router 172.31.1.1
Tunja(dhcp-config)#dns-server 172.31.2.26
```

- **Configuración routers de salida con el comando (helper address)**

```
Bucaramanga#configure t
Enter configuration commands, one per line. End with CNTL/Z.
Bucaramanga(config)#int f0/0.10
Bucaramanga(config-subif)#ip helper-address 172.31.2.33
Bucaramanga(config-subif)#int f0/0.30
Bucaramanga(config-subif)#ip helper-address 172.31.2.33
```

```
Cundinamarca#configure t
Enter configuration commands, one per line. End with CNTL/Z.
```

```
Cundinamarca(config)#interface f0/0.20
Cundinamarca(config-subif)#ip helper-address 172.31.2.37
Cundinamarca(config-subif)#interface f0/0.30
Cundinamarca(config-subif)#ip helper-address 172.31.2.37
```

2.4. 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 172.31.2.26 209.17.220.3
Tunja(config)#access-list 1 permit 172.0.0.0 0.255.255.255
Tunja(config)#ip nat inside source list 1 interface f0/1 overload
Tunja(config)#int f0/1
Tunja(config-if)#ip nat outside
Tunja(config-if)#int f0/0.1
Tunja(config-subif)#ip nat inside
Tunja(config-subif)#int f0/0.20
Tunja(config-subif)#ip nat inside
Tunja(config-subif)#int f0/0.30
Tunja(config-subif)#ip nat inside
Tunja(config-subif)#int s0/1/0
Tunja(config-if)#ip nat inside
Tunja(config-if)#int s0/1/1
Tunja(config-if)#ip nat inside
Tunja(config-if)#exit
Tunja(config)#ip route 0.0.0.0 0.0.0.0 209.165.220.1
Tunja(config)#router ospf 2
Tunja(config-router)#default-information originate
Tunja(config-router)#end
Tunja#
```

2.5. El enrutamiento OSPF y autenticación

- Router Bucaramanga

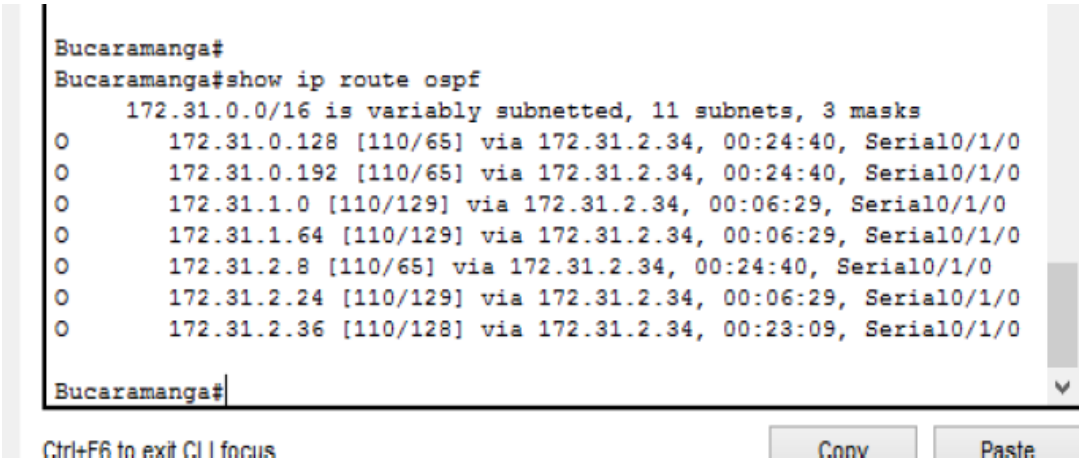
```
Bucaramanga#config t
Enter configuration commands, one per line. End with CNTL/Z.
Bucaramanga(config)#router ospf 1
Bucaramanga(config-router)#network 172.31.0.0 0.0.0.63 area 0
Bucaramanga(config-router)#network 172.31.0.64 0.0.0.63 area 0
Bucaramanga(config-router)#network 172.31.2.0 0.0.0.7 area 0
Bucaramanga(config-router)#network 172.31.2.32 0.0.0.3 area 0
Bucaramanga(config-router)#exit
```

Bucaramanga(config)#

- Autenticación del enrutamiento:

Bucaramanga(config)#int s0/1/0
Bucaramanga(config-if)#ip ospf authentication message-digest
Bucaramanga(config-if)#ip ospf message-digest-key 1 md5 cisco
Bucaramanga(config-if)#
Bucaramanga(config-if)#
03:49:54: %OSPF-5-ADJCHG: Process 1, Nbr 209.17.220.1 on Serial0/1/0 from FULL to DOWN, Neighbor Down: Dead timer expired
03:49:54: %OSPF-5-ADJCHG: Process 1, Nbr 209.17.220.1 on Serial0/1/0 from FULL to DOWN, Neighbor Down: Interface down or detached

- Comprobación del enrutamiento OSPF con el comando show ip route ospf



- Comprobación con el comando show ip ospf interface s0/1/0 se puede verificar la autenticación configurada.

```
Bucaramanga#show ip ospf interface s0/1/0

Serial0/1/0 is up, line protocol is up
  Internet address is 172.31.2.33/30, Area 0
  Process ID 1, Router ID 172.31.2.33, Network Type POINT-TO-POINT,
Cost: 64
  Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit
5
    Hello due in 00:00:07
  Index 4/4, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Suppress hello for 0 neighbor(s)
  Message digest authentication enabled
    Youngest key id is 1
Bucaramanga#
```

- Router Tunja

Tunja#config t
Enter configuration commands, one per line. End with CNTL/Z.
Tunja(config)#route ospf 2
Tunja(config-router)#network 172.31.0.128 0.0.0.63 area 0
Tunja(config-router)#network 172.31.0.192 0.0.0.63 area 0
Tunja(config-router)#network 172.31.2.8 0.0.0.7 area 0
Tunja(config-router)#network 172.31.2.32 0.0.0.3 area 0
Tunja(config-router)#network 172.31.2.36 0.0.0.3 area 0
00:00:10: %OSPF-5-ADJCHG: Process 2, Nbr 172.31.2.37 on Serial0/1/0 from LOADING to FULL, Loading Done
00:00:10: %OSPF-5-ADJCHG: Process 2, Nbr 172.31.2.33 on Serial0/1/1 from LOADING to FULL, Loading Done

- Autenticación del enrutamiento:

Tunja(config)#int s0/1/1
Tunja(config-if)#ip ospf authentication message-digest
Tunja(config-if)#ip ospf message-digest-key 1 md5 cisco
Tunja(config-if)#
04:07:44: %OSPF-5-ADJCHG: Process 2, Nbr 172.31.2.33 on Serial0/1/1 from LOADING to FULL, Loading Done

Tunja(config-if)#int s0/1/0
Tunja(config-if)#ip ospf authentication message-digest
Tunja(config-if)#ip ospf message-digest-key 1 md5 cisco
Tunja(config-if)#

04:10:34: %OSPF-5-ADJCHG: Process 2, Nbr 172.31.2.37 on Serial0/1/0 from FULL to DOWN, Neighbor Down: Dead timer expired

04:10:34: %OSPF-5-ADJCHG: Process 2, Nbr 172.31.2.37 on Serial0/1/0 from FULL to DOWN, Neighbor Down: Interface down or detached

- Comprobación del enrutamiento OSPF con el comando show ip route ospf

```
Tunja>enable
Password:
Tunja#
Tunja#show ip route ospf
     172.31.0.0/16 is variably subnetted, 11 subnets, 3 masks
O       172.31.0.0 [110/65] via 172.31.2.33, 00:22:09, Serial0/1/0
O       172.31.0.64 [110/65] via 172.31.2.33, 00:22:09, Serial0/1/0
O       172.31.1.0 [110/65] via 172.31.2.37, 00:04:08, Serial0/1/1
O       172.31.1.64 [110/65] via 172.31.2.37, 00:04:08, Serial0/1/1
O       172.31.2.0 [110/65] via 172.31.2.33, 00:22:09, Serial0/1/0
O       172.31.2.24 [110/65] via 172.31.2.37, 00:04:08, Serial0/1/1

Tunja#
```

- Comprobación con el comando show ip ospf interface s0/1/0 se puede verificar la autenticación configurada.

```
Tunja#show ip ospf interface s0/1/0

Serial0/1/0 is up, line protocol is up
  Internet address is 172.31.2.38/30, Area 0
  Process ID 2, Router ID 209.17.220.1, Network Type POINT-TO-POINT,
Cost: 64
  Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit
5
    Hello due in 00:00:06
  Index 4/4, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Suppress hello for 0 neighbor(s)
  Message digest authentication enabled
    Youngest key id is 1
Tunja#
```

- Router Cundinamarca

```
Cundinamarca#config t
Enter configuration commands, one per line. End with CNTL/Z.
Cundinamarca(config)#route ospf 3
Cundinamarca(config-router)#network 172.31.1.0 0.0.0.63 area 0
Cundinamarca(config-router)#network 172.31.1.64 0.0.0.63 area 0
Cundinamarca(config-router)#network 172.31.2.8 0.0.0.7 area 0
Cundinamarca(config-router)#network 172.31.2.24 0.0.0.7 area 0
Cundinamarca(config-router)#network 172.31.2.36 0.0.0.3 area 0
Cundinamarca(config-router)#
00:56:24: %OSPF-5-ADJCHG: Process 1, Nbr 209.17.220.1 on Serial0/0/1 from
LOADING to FULL, Loading Done
Cundinamarca(config-router)#end
Cundinamarca#
```

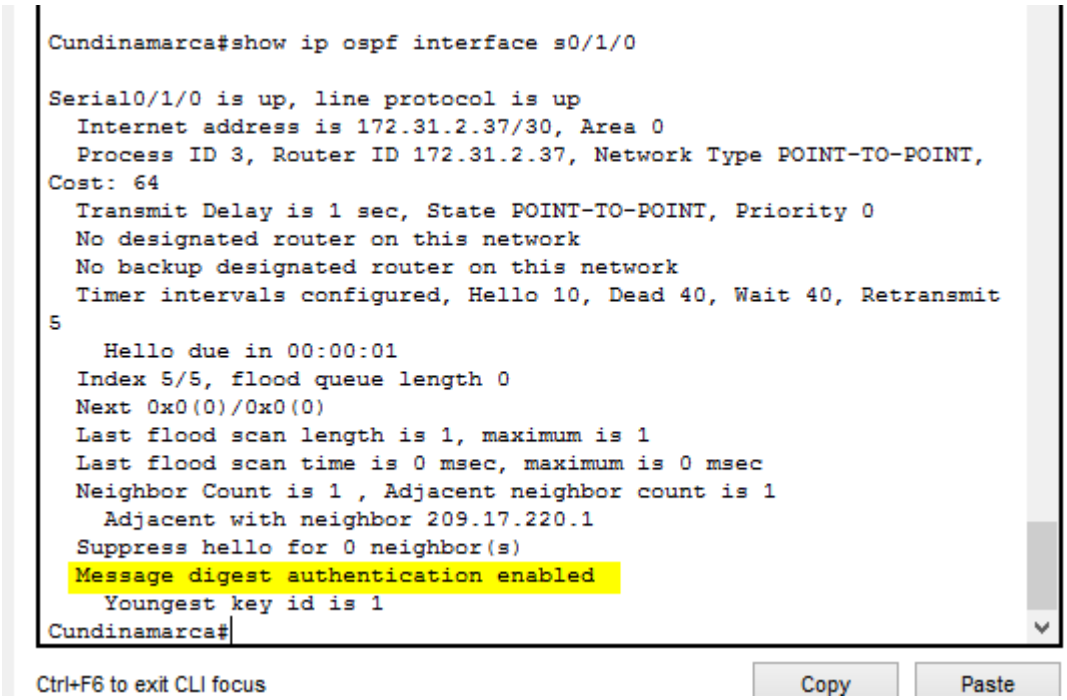
- Autenticación del enrutamiento:

```
Cundinamarca(config)#int s0/1/0
Cundinamarca(config-if)#ip ospf authentication message-digest
Cundinamarca(config-if)#ip ospf message-digest-key 1 md5 cisco
Cundinamarca(config-if)#
04:18:54: %OSPF-5-ADJCHG: Process 3, Nbr 209.17.220.1 on Serial0/1/0 from
LOADING to FULL, Loading Done
Cundinamarca(config-if)#
```

- Comprobación del enrutamiento OSPF con el comando show ip route ospf

```
Cundinamarca#show ip route ospf
     172.31.0.0/16 is variably subnetted, 11 subnets, 3 masks
O       172.31.0.0 [110/129] via 172.31.2.38, 00:03:03, Serial0/1/0
O       172.31.0.64 [110/129] via 172.31.2.38, 00:03:03, Serial0/1/0
O       172.31.0.128 [110/65] via 172.31.2.38, 00:03:03, Serial0/1/0
O       172.31.0.192 [110/65] via 172.31.2.38, 00:03:03, Serial0/1/0
O       172.31.2.0 [110/129] via 172.31.2.38, 00:03:03, Serial0/1/0
O       172.31.2.32 [110/128] via 172.31.2.38, 00:03:03, Serial0/1/0

Cundinamarca#
```

- Comprobación con el comando show ip ospf interface s0/1/0 se puede verificar la autenticación configurada.



2.6. Listas de control de acceso:

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

Cundinamarca(config)#access-list 101 permit ip 172.31.1.0 0.0.0.63 209.17.220.0 0.0.0.255
Cundinamarca(config)#access-list 101 deny ip any
Cundinamarca(config)#int f0/0.30
Cundinamarca(config-subif)#ip access-group 101 in
Cundinamarca(config)#access-list 102 permit ip 172.31.1.64 0.0.0.63 209.17.220.0 0.0.0.255
Cundinamarca(config)#access-list 102 deny ip any any
Cundinamarca(config)#int f0/0.20
Cundinamarca(config-subif)#ip access-group 102 in
Cundinamarca(config-subif)#

- Accede a internet

```
C:\>ping 209.17.220.3

Pinging 209.17.220.3 with 32 bytes of data:

Reply from 209.17.220.3 bytes=32 time=1ms TTL=126
Reply from 209.17.220.3 bytes=32 time=1ms TTL=126
Reply from 209.17.220.3 bytes=32 time=1ms TTL=126
Reply from 209.17.220.3 bytes=32 time=1ms TTL=126

Ping statistics for 209.17.220.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

- No accede a la red interna de Tunja.

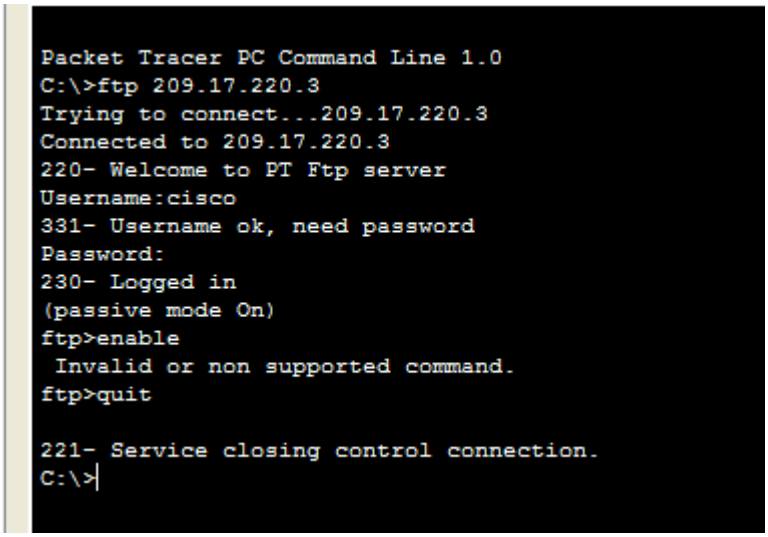
```
C:\>ping 172.31.0.194

Pinging 172.31.0.194 with 32 bytes of data:

Reply from 172.31.1.65: Destination host unreachable.
Reply from 172.31.1.65: Destination host unreachable.
Reply from 172.31.1.65: Destination host unreachable.
Reply from 172.31.1.65: Destination host unreachable.

Ping statistics for 172.31.0.194:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 172.31.0.130

Pinging 172.31.0.130 with 32 bytes of data:

Reply from 172.31.1.65: Destination host unreachable.
Reply from 172.31.1.65: Destination host unreachable.
Reply from 172.31.1.65: Destination host unreachable.
Reply from 172.31.1.65: Destination host unreachable.

Ping statistics for 172.31.0.130:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

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

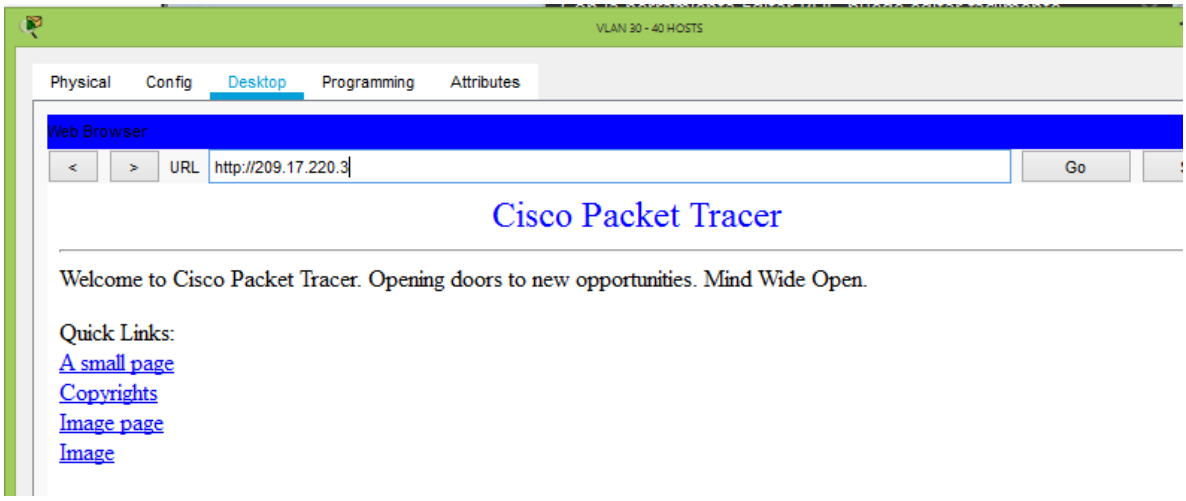
TUNJA(config)#access-list 103 permit tcp 172.31.0.192 0.0.0.63 209.165.220.0 0.0.0.255 eq 80

```
TUNJA(config)#access-list 103 permit tcp 172.31.0.192 0.0.0.63 209.165.220.0
0.0.0.255 eq 21
TUNJA(config)#access-list 103 permit tcp 172.31.0.192 0.0.0.63 209.165.220.0
0.0.0.255 eq 20
TUNJA(config)#int f0/0.30
TUNJA(config-subif)#ip access-group 103 in
TUNJA(config-subif)#
```

- Acceso al servidor ftp



- Acceso al servidor web



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

Tunja(config-subif)#access-list 104 permit ip 172.31.0.128 0.0.0.63 172.31.1.64 0.0.0.63
Tunja(config)#int f0/0.20
Tunja(config-subif)#ip access-group 104 in
Tunja(config-subif)#

```
C:\>ping 172.31.0.2

Pinging 172.31.0.2 with 32 bytes of data:

Reply from 172.31.0.2: bytes=32 time=1ms TTL=126
Reply from 172.31.0.2: bytes=32 time=1ms TTL=126
Reply from 172.31.0.2: bytes=32 time=1ms TTL=126
Reply from 172.31.0.2: bytes=32 time=1ms TTL=126

Ping statistics for 172.31.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

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

Bucaramanga(config)#access-list 3 permit 209.17.220.0
Bucaramanga(config)#access-list 3 permit host 172.31.0.0
Bucaramanga(config)#access-list 3 deny any
Bucaramanga(config)#interface fa0/0
Bucaramanga(config-if)#ip access-group 3 out
Bucaramanga(config-if)#

- Verificación vlan 30 accede a internet

```
C:\>ping 209.17.220.3

Pinging 209.17.220.3 with 32 bytes of data:

Reply from 209.17.220.3 bytes=32 time=1ms TTL=126
Reply from 209.17.220.3 bytes=32 time=1ms TTL=126
Reply from 209.17.220.3 bytes=32 time=1ms TTL=126
Reply from 209.17.220.3 bytes=32 time=1ms TTL=126

Ping statistics for 209.17.220.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

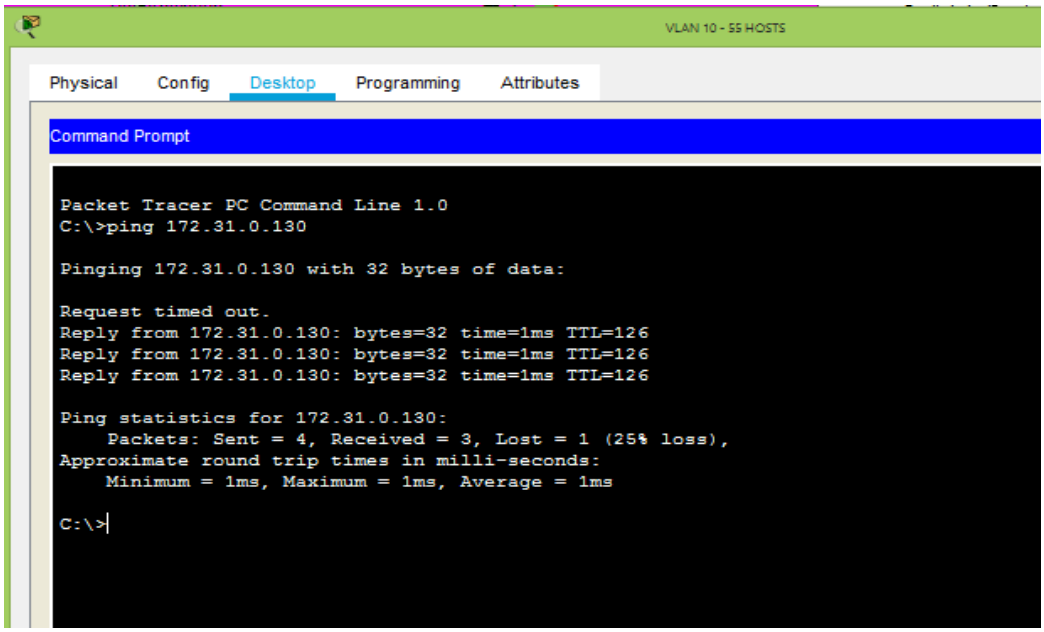
- Verificación vlan 30 accede a vlan 10

```
C:\>ping 172.31.0.2

Pinging 172.31.0.2 with 32 bytes of data:

Reply from 172.31.0.2: bytes=32 time=1ms TTL=126
Reply from 172.31.0.2: bytes=32 time=1ms TTL=126
Reply from 172.31.0.2: bytes=32 time=1ms TTL=126
Reply from 172.31.0.2: bytes=32 time=1ms TTL=126

Ping statistics for 172.31.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

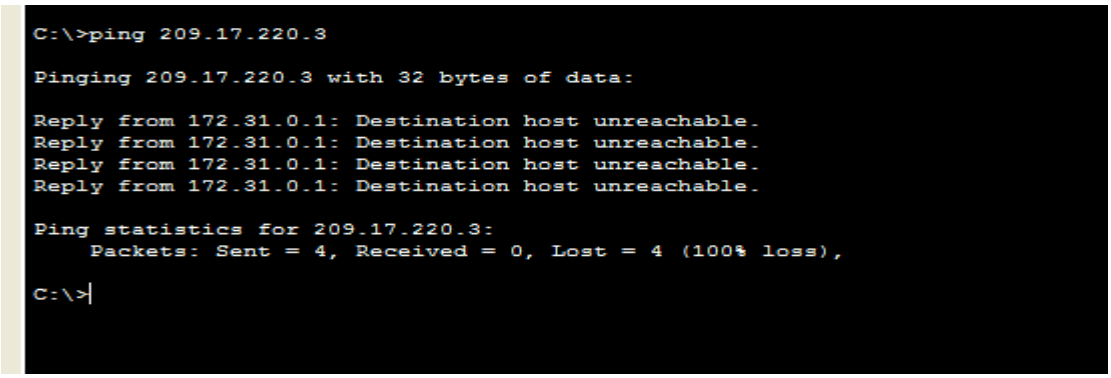
- **Los hosts de VLAN 10 en Bucaramanga acceden a la red de Cundinamarca (VLAN 20) y Tunja (VLAN 20), no internet.**

Bucaramanga(config)#access-list 100 permit ip 172.31.0.0 0.0.0.63 172.31.1.64 0.0.0.63
Bucaramanga(config)#access-list 100 permit ip 172.31.0.0 0.0.0.63 172.31.0.128 0.0.0.63
Bucaramanga(config)#interface f0/0.10
Bucaramanga(config-subif)#ip access-group 100 in
Bucaramanga(config-subif)#

- Comprobación de la red VLAN 10 en Bucaramanga accede a la red Tunja (VLAN 20)



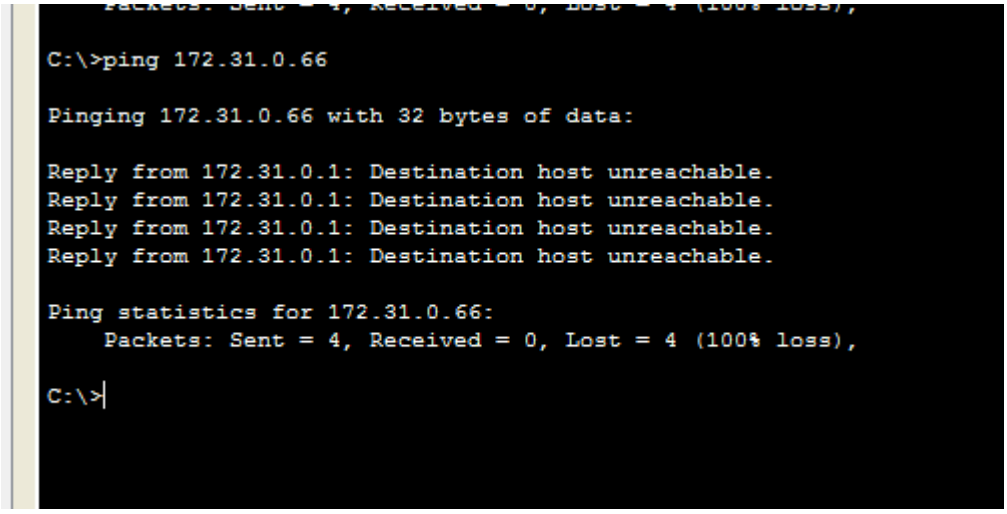
- Comprobación de la red VLAN 10 en Bucaramanga no accede a internet



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

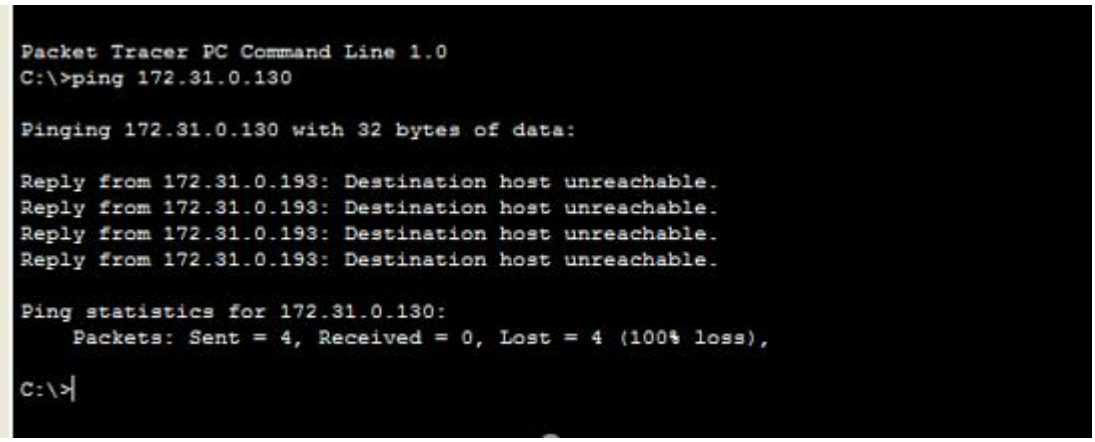
Bucaramanga(config)#access-list 106 deny ip 172.31.2.0 0.0.0.7 172.31.0.0 0.0.0.63
Bucaramanga(config)#access-list 106 deny ip 172.31.2.0 0.0.0.7 172.31.0.64 0.0.0.63
Bucaramanga(config)#access-list 106 permit ip any any
Bucaramanga(config)#interface f0/0.10
Bucaramanga(config-subif)#ip access-group 106 out
Bucaramanga(config-subif)#end
Bucaramanga#

- Verificación Red Bucaramanga vlan 10 no accede a la vlan 30



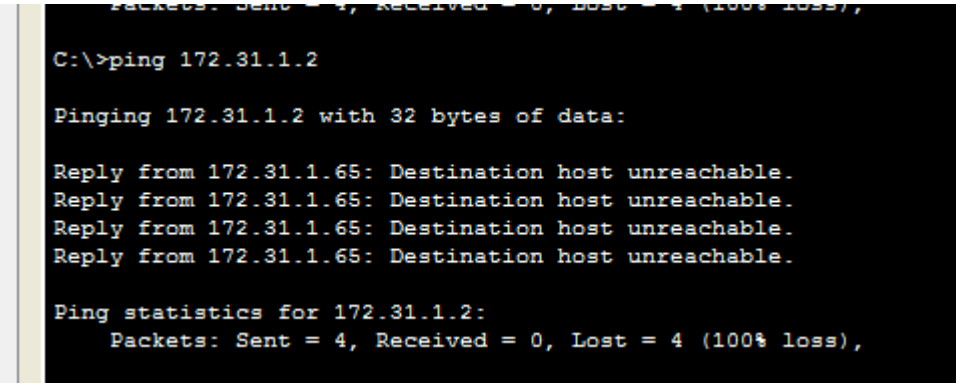
- Verificación Red Tunja vlan 20 no accede a la vlan 30

Tunja(config)#access-list 105 deny ip 172.3.2.8 0.0.0.7 172.31.0.128 0.0.0.63
Tunja(config)#access-list 105 deny ip 172.3.0.192 0.0.0.63 172.31.0.128 0.0.0.63
Tunja(config)#access-list 105 permit ip any any
Tunja(config)#int f0/0.20
Tunja(config-subif)#ip access-group 105 out
Tunja(config-subif)#



- Verificación Red Cundinamarca vlan 20 no accede a la vlan 30

Cundinamarca(config)#access-list 103 deny ip 172.31.1.0 0.0.0.63 172.31.1.64 0.0.0.63
Cundinamarca(config)#access-list 103 deny ip 172.31.1.0 0.0.0.63 172.31.1.64 0.0.0.63
Cundinamarca(config)#access-list 103 permit ip any any
Cundinamarca(config)#int f0/0.20
Cundinamarca(config-subif)#ip access-group 103 out



CONCLUSIONES

- En esta actividad se consolidad los conocimientos de los cursos CCNA1 y CCNA2 para implementar, generar y administrar redes que nos pueden ayudar en nuestros entornos laborales para poder dar solución a los problemas que se nos presenten en una red.

- La actividad fue provechosa porque nos enfatiza en la seguridad de las redes, en los ataques que se pueden tener y que como administradores de una red debemos generar todos los protocolos de seguridad para los dispositivos. En esta parte de seguridad puedo decir que fue un poco difícil y confuso la implementación de comandos como la autenticación AAA y los ACLS ya que no los había implementado en ninguna red por falta de conocimiento o práctica, pero en esta actividad pude ver la importancia de utilizarlos y ver cómo funcionan en una red.

REFERENCIAS BIBLIOGRAFICAS

- CISCO. (2014). SubNetting. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module9/index.html#9.0.1.1
- CISCO. (2014). Ethernet. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#5.0.1.1
- Macfarlane, J. (2014). Network Routing Basics: Understanding IP Routing in Cisco Systems. Recuperado de http://bibliotecavirtual.unad.edu.co:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=e000xww&AN=158227&lang=es&site=ehost-live
- CISCO. (2014). Asignación de direcciones IP. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module8/index.html#8.0.1.1
- CISCO. (2014). Enrutamiento entre VLANs. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module5/index.html#5.0.1.1
- CISCO. (2014). OSPF de una sola área. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module8/index.html#8.0.1.1
- CISCO. (2014). Listas de control de acceso. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module9/index.html#9.0.1.1
- CISCO. (2014). DHCP. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module10/index.html#10.0.1.1