DIPLOMADO DE PROFUNDIZACION CISCO

EVALUACION-PRUEBA DE HABILIDADES PRÁCTICAS CCNA

PRESENTADO POR

LUIS HERNANDO MARTINEZ URUEÑA

GRUPO

203092_10

TUTOR

GIOVANNI ALBERTO BRACHO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA _ UNAD

DICIEMBRE 15 DE 2019

TABLA DE CONTENIDO

Contenido

RESUMEN

El desarrollo a la evaluación final prueba de habilidades CCNA, se requiere implementar los conocimientos obtenidos en todas las pruebas de la plataforma CISCO y en las respectivas actividades desarrolladas por la plataforma de la Unad.

Para esta evaluacion se debe realizar y aplicar los diferentes comandos para una configuracion de routers, switch, tambien implementacion de seguridad en la red, por su puesto confirmar el funcionamiento en la red paa obtener comunicación o interconexion total.

ABSTRACT

The development to the final evaluation test of CCNA skills, it is required to implement the knowledge obtained in all the tests of the CISCO platform and in the respective activities developed by the Unad platform.

For this evaluation the different commands must be carried out and applied for a configuration of routers, switches, also security implementation in the network, of course confirm the operation in the network to obtain communication or total interconnection.

INTRODUCCION

La evaluacion “Prueba de habilidades practicas” desarrolladas en este trabajo, busca conocer el nivel de progreso de las actividades realizadas en el Diplomado CISCO, para esto en el presente trabajo se efectuará la solucion de diferentes ejercicios y configuraciones que se deben realizar en las topologias, el cual se pueden asemejar a las redes de comunicación del entorno real.

OBJETIVOS

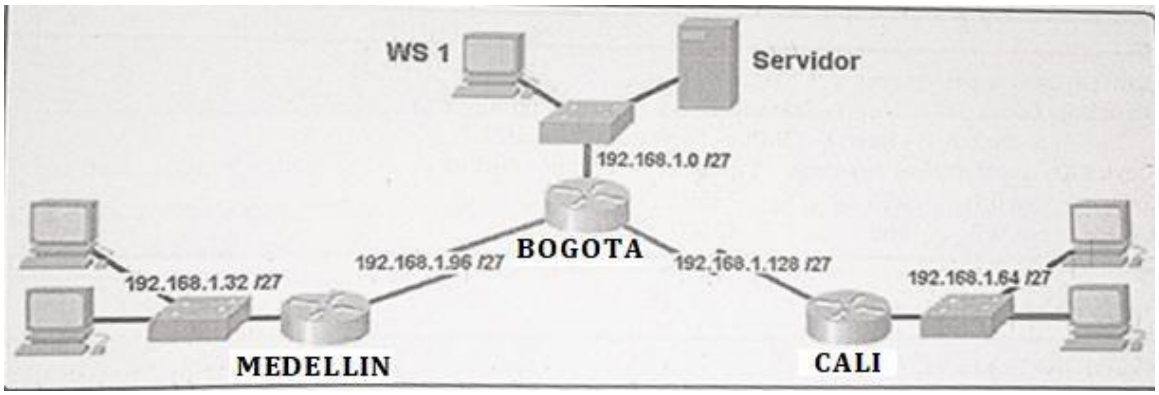
- Definir direcciones de acuerdo al número de hosts solicitados.
- Realizar la asignación de los parámetros básicos.
- Localización de vecinos conectados directamente.
- Hacer interconexión en la red y subred creadas.
- Efectuar la seguridad en la red obteniendo restricciones de acceso.

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.

DIRECCIONES IP	MASCARA
192.168.1.0/27	255.255.255.224
192.168.1.32/27	255.255.255.224
192.168.1.64/27	255.255.255.224
192.168.1.96/27	255.255.255.224
192.168.1.128/27	255.255.255.224
192.168.1.160/27	255.255.255.224
192.168.1.192/27	255.255.255.224
192.168.1.224/27	255.255.255.224

b. Asignar una dirección IP a la red.



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

Para los diferentes comandos especificados en este punto se trabajan los comando hostname para darle un nombre a un router o switch según sea el caso, también se realizo algo muy importante, la clave de acceso al modo privilegiado de los dispositivos, también pues hay la posibilidad de las claves encriptadas.

Esto para tener una seguridad y que cada entrada que se realice pida su nombre y clave.

Comandos para el Router de Medellín:

```
Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname MEDELLIN
MEDELLIN(config)#line con 0
MEDELLIN(config-line)#password luis
MEDELLIN(config-line)#login
MEDELLIN(config-line)#logging synchronous
MEDELLIN(config-line)#line vty 0 15
MEDELLIN(config-line)#password luis1
MEDELLIN(config-line)#login
MEDELLIN(config-line)#logging synchronous
MEDELLIN(config-line)#exit
MEDELLIN(config)#

MEDELLIN(config)#enable password adminluis
MEDELLIN(config)#service password-encryption
MEDELLIN(config)#interface s0/0/0
MEDELLIN(config-if)#ip address 192.168.1.99 255.255.255.224
MEDELLIN(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
MEDELLIN(config-if)#interface g0/0
MEDELLIN(config-if)#ip address 192.168.1.33 255.255.255.224
MEDELLIN(config-if)#no shutdown

MEDELLIN(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0,
changed state to up

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

Comandos para el Router de Bogotá:

```
Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname BOGOTA
BOGOTA(config)#line con 0
BOGOTA(config-line)#password cisco
BOGOTA(config-line)#login
BOGOTA(config-line)#logging synchronous
BOGOTA(config-line)#line vty 0 15
BOGOTA(config-line)#password cisco
BOGOTA(config-line)#login
BOGOTA(config-line)#logging synchronous
BOGOTA(config-line)#exit
BOGOTA(config)#enable password cisco
BOGOTA(config)#service password-encryption
BOGOTA(config)#interface s0/0/0
BOGOTA(config-if)#ip address 192.168.1.98 255.255.255.224
BOGOTA(config-if)#clock rate 1000000
BOGOTA(config-if)#no shutdown

BOGOTA(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

BOGOTA(config-if)#interface
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed
state to up

BOGOTA(config-if)#interface g0/0
BOGOTA(config-if)#ip address


BOGOTA con0 is now available

Press RETURN to get started.

User Access Verification

Password:

BOGOTA>enable
Password:
BOGOTA#enable
BOGOTA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA(config)#interface g0/0
```

```
BOGOTA(config-if)#exit
BOGOTA(config)#interface s0/0/0
BOGOTA(config-if)#ip address 192.168.1.98 255.255.255.224
BOGOTA(config-if)#clock rate 1000000
BOGOTA(config-if)#no shutdown
BOGOTA(config-if)#interface g0/0
BOGOTA(config-if)#ip address 192.168.1.1 255.255.255.224
BOGOTA(config-if)#no shutdown

BOGOTA(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0,
changed state to up

BOGOTA(config-if)#interface s0/0/1
BOGOTA(config-if)#ip address 192.168.1.130 255.255.255.224
BOGOTA(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
BOGOTA(config-if)#end
BOGOTA#
%SYS-5-CONFIG_I: Configured from console by console

BOGOTA#
```

Comandos para el Router de Cali:

```
Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname CALI
CALI(config)#line con 0
CALI(config-line)#password empresa
CALI(config-line)#login
CALI(config-line)#loggins synchronous
^
% Invalid input detected at '^' marker.
CALI(config-line)#loggin synchronous
CALI(config-line)#line vty 0 15
CALI(config-line)#password empresa
CALI(config-line)#login
CALI(config-line)#logging synchronous
CALI(config-line)#exit
CALI(config)#enable password empresa
CALI(config)#service password-encryption

Router>enable
```

```
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname CALI
CALI(config)#line con 0
CALI(config-line)#password empresa
CALI(config-line)#login
CALI(config-line)#loggins synchronous
^
% Invalid input detected at '^' marker.
CALI(config-line)#loggin synchronous
CALI(config-line)#line vty 0 15
CALI(config-line)#password empresa
CALI(config-line)#login
CALI(config-line)#logging synchronous
CALI(config-line)#exit
CALI(config)#enable password empresa
CALI(config)#service password-encryption
```

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.

Se utiliza el comando show ip router para verificar la información de enrutamiento que se maneja para precisar el reenvío de tráfico de Medellín, Bogotá y Cali.

```
MEDELLIN>show ip route
Codes: L - local, C - connected, S - static, 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

     192.168.1.0/24 is variably subnetted, 4 subnets, 2 masks
C       192.168.1.32/27 is directly connected, GigabitEthernet0/0
L       192.168.1.33/32 is directly connected, GigabitEthernet0/0
C       192.168.1.96/27 is directly connected, Serial0/0/0
L       192.168.1.99/32 is directly connected, Serial0/0/0

MEDELLIN>
```

```
BOGOTA>show ip route
Codes: L - local, C - connected, S - static, 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

     192.168.1.0/24 is variably subnetted, 6 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
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

BOGOTA>
```

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

Gateway of last resort is not set

     192.168.1.0/27 is subnetted, 2 subnets
C       192.168.1.64 is directly connected, FastEthernet0/0
C       192.168.1.128 is directly connected, Serial0/0/0

CALI>
```

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

Es este caso solo verifica la información de enrutamiento de la red especificada eje: la red 192.168.1.96

Bogotá:

```
BOGOTA#show ip route 192.168.1.96
Routing entry for 192.168.1.96/27
Known via "connected", distance 0, metric 0 (connected, via
interface)
  Routing Descriptor Blocks:
  * directly connected, via Serial0/0/0
      Route metric is 0, traffic share count is 1

BOGOTA#show ip route 192.168.1.128
Routing entry for 192.168.1.128/27
Known via "connected", distance 0, metric 0 (connected, via
interface)
  Routing Descriptor Blocks:
  * directly connected, via Serial0/0/1
      Route metric is 0, traffic share count is 1

BOGOTA#show ip route 192.168.1.2
Routing entry for 192.168.1.0/27
Known via "connected", distance 0, metric 0 (connected, via
interface)
  Routing Descriptor Blocks:
  * directly connected, via GigabitEthernet0/0
      Route metric is 0, traffic share count is 1
```

Medellín:

```
MEDELLIN#show ip route 192.168.1.32
Routing entry for 192.168.1.32/27
Known via "connected", distance 0, metric 0 (connected, via
interface)
  Routing Descriptor Blocks:
  * directly connected, via GigabitEthernet0/0
      Route metric is 0, traffic share count is 1

MEDELLIN#show ip route 192.168.1.96
Routing entry for 192.168.1.96/27
Known via "connected", distance 0, metric 0 (connected, via
interface)
  Routing Descriptor Blocks:
  * directly connected, via Serial0/0/0
      Route metric is 0, traffic share count is 1

MEDELLIN#
```

Cali:

```
CALI>enable
Password:
CALI#show ip route 192.168.1.128
Routing entry for 192.168.1.128/27
Known via "connected", distance 0, metric 0 (connected, via
interface)
  Routing Descriptor Blocks:
  * directly connected, via Serial0/0/0
      Route metric is 0, traffic share count is 1

CALI#show ip route 192.168.1.64
Routing entry for 192.168.1.64/27
Known via "connected", distance 0, metric 0 (connected, via
interface)
  Routing Descriptor Blocks:
  * directly connected, via FastEthernet0/0
      Route metric is 0, traffic share count is 1
```

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

Por medio de este comando CDP se puede saber que switch se conecta con otros switch.

Lo vemos reflejado en los siguentes pantallazos.

Bogota:

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

Medellín:

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

Cali:

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

Comando show cdp neighbors: se obtienen los nombres y tipos de touters vecinos.

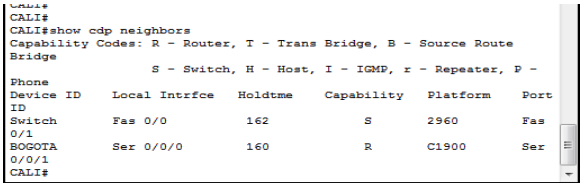
Bogota:

```
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
MEDELLIN     Ser 0/0/0        136            R       C1900       Ser
0/0/0
Switch       Gig 0/0          164            S       2960        Fas
0/3
CALI         Ser 0/0/1        133            R       C1841       Ser
0/0/0
BOGOTA#
```

Medellín:

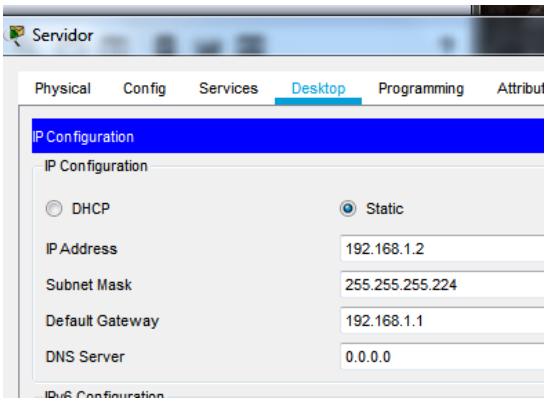
```
MEDELLIN#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route
Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P -
Phone
Device ID    Local Intrfce   Holdtme    Capability   Platform    Port
ID
Switch       Gig 0/0          154            S       2960        Fas
0/1
BOGOTA       Ser 0/0/0        159            R       C1900       Ser
0/0/0
MEDELLIN#
```

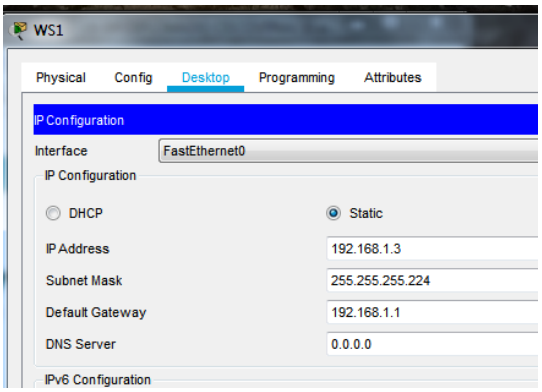
Cali:



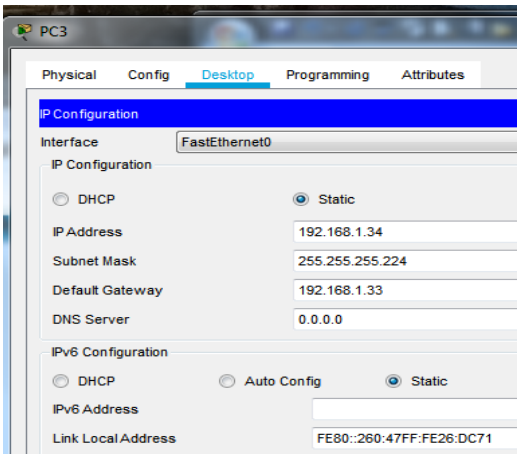
e. Realizar una prueba de conectividad en cada tramo de la ruta usando Ping.

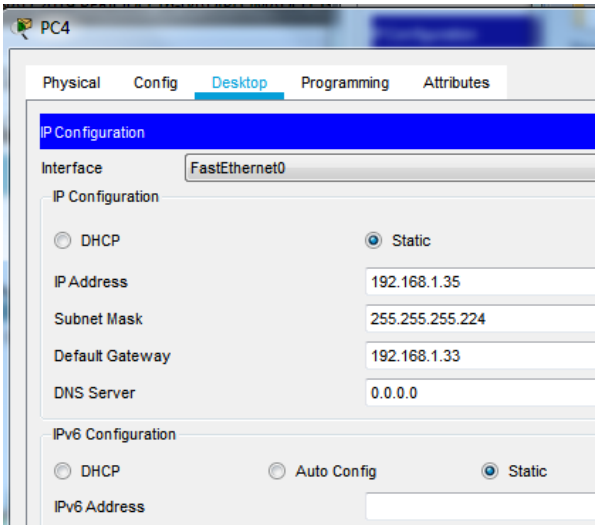
Bogota:



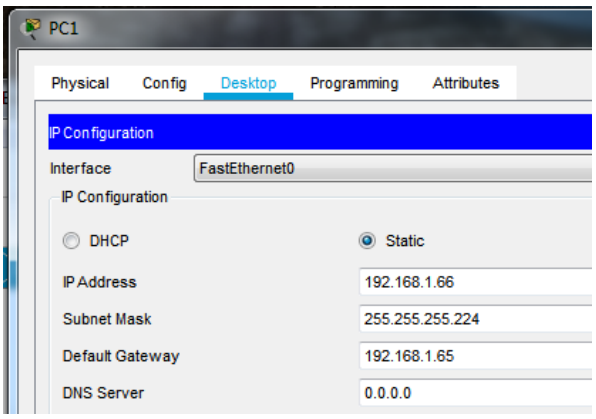


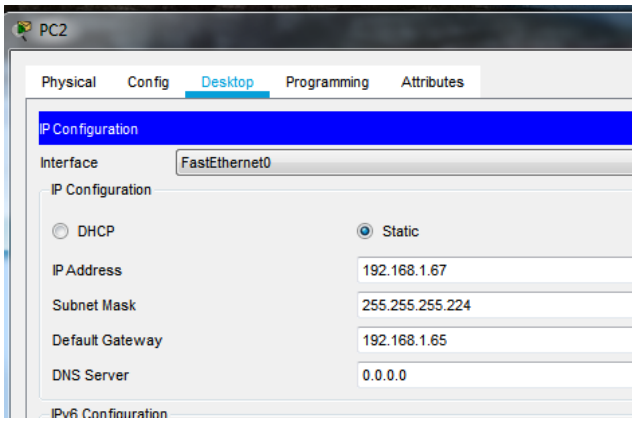
Medellín:


PC3
Physical
Config
Desktop
Programming
Attributes
IP Configuration
Interface
FastEthernet0
IP Configuration
DHCP
Static
IP Address
192.168.1.34
Subnet Mask
255.255.255.224
Default Gateway
192.168.1.33
DNS Server
0.0.0.0
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address
FE80::260:47FF:FE26:DC71


PC4
Physical
Config
Desktop
Programming
Attributes
IP Configuration
Interface
FastEthernet0
IP Configuration
DHCP
Static
IP Address
192.168.1.35
Subnet Mask
255.255.255.224
Default Gateway
192.168.1.33
DNS Server
0.0.0.0
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address

Cali:


PC1
Physical
Config
Desktop
Programming
Attributes
IP Configuration
Interface
FastEthernet0
IP Configuration
DHCP
Static
IP Address
192.168.1.66
Subnet Mask
255.255.255.224
Default Gateway
192.168.1.65
DNS Server
0.0.0.0



Prueba de pings:

```
User Access Verification

Password:

BOGOTA>ping 192.168.1.99

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.99, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/3/11 ms

BOGOTA>
```

```
BOGOTA>ping 192.168.1.131

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.131, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/71/347
ms

BOGOTA>
```

Parte 3: Configuración de Enrutamiento.

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

Se configura los routers con el mondo EIGRP para la detección de vecinos conectados directamente a sus redes.

MEDELLIN>enable
Password:
Password:
MEDELLIN#conf t

```
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN(config)#router eigrp 1
MEDELLIN(config-router)#no auto-summary
MEDELLIN(config-router)#network 192.168.1.32
MEDELLIN(config-router)#network 192.168.1.96
MEDELLIN(config-router)#end
MEDELLIN#
%SYS-5-CONFIG_I: Configured from console by console

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

```
BOGOTA>enable
Password:
BOGOTA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA(config)#router eigrp 1
BOGOTA(config-router)#no auto-summary
BOGOTA(config-router)#network 192.168.1.96
BOGOTA(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 192.168.1.99 (Serial0/0/0) is
up: new adjacency

BOGOTA(config-router)#network 192.168.1.0
BOGOTA(config-router)#network 192.168.1.128
BOGOTA(config-router)#end
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 192.168.1.131 (Serial0/0/1) is
up: new adjacency

BOGOTA(config-router)#end
BOGOTA#
%SYS-5-CONFIG_I: Configured from console by console
```

```
CALI>enable
Password:
CALI#conf t
Enter configuration commands, one per line. End with CNTL/Z.
CALI(config)#router eigrp 1
CALI(config-router)#no auto-summary
CALI(config-router)#network 192.168.1.128
CALI(config-router)#
```

%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 192.168.1.130 (Serial0/0/0) is up: new adjacency

CALI(config-router)#network 192.168.1.64
CALI(config-router)#end
CALI#
%SYS-5-CONFIG_I: Configured from console by console

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

El comando muestra el estado de los vecinos

```
MEDELLIN>enable
Password:
MEDELLIN#show ip eigrp neighbors
IP-EIGRP neighbors for process 1
H   Address         Interface      Hold Uptime    SRTT   RTO   Q   Seq
                                   (sec)          (ms)        Cnt  Num
0   192.168.1.98    Se0/0/0        12   00:35:11  40     1000  0   5

IP-EIGRP neighbors for process 2

MEDELLIN#
```

```
BOGOTA>enable
Password:
BOGOTA#show ip eigrp neighbors
IP-EIGRP neighbors for process 1
H   Address         Interface      Hold Uptime    SRTT   RTO   Q   Se
                                   (sec)          (ms)        Cnt  Nu
0   192.168.1.99    Se0/0/0        11   00:37:10  40     1000  0   7
1   192.168.1.131   Se0/0/1        13   00:33:57  40     1000  0   7

BOGOTA#
```

```
CALI>enable
Password:
CALI#show ip eigrp neighbors
IP-EIGRP neighbors for process 1
H   Address         Interface      Hold Uptime    SRTT   RTO   Q
Seq
                                   (sec)          (ms)        Cnt
Num
0   192.168.1.130   Se0/0/0        13   00:37:08  40     1000  0   6

CALI#
```

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

```
MEDELLIN#
MEDELLIN#show ip route eigrp
     192.168.1.0/24 is variably subnetted, 7 subnets, 2 masks
D       192.168.1.0/27 [90/2172416] via 192.168.1.98, 00:42:09, Serial0/0/0
D       192.168.1.64/27 [90/2684416] via 192.168.1.98, 00:38:56, Serial0/0/0
D       192.168.1.128/27 [90/2681856] via 192.168.1.98, 00:42:09,
Serial0/0/0

MEDELLIN#
```

```
BOGOTA#show ip route eigrp
     192.168.1.0/24 is variably subnetted, 8 subnets, 2 masks
D       192.168.1.32/27 [90/2172416] via 192.168.1.99, 00:42:58, Serial0/0/0
D       192.168.1.64/27 [90/2172416] via 192.168.1.131, 00:39:45, Serial0/0/1

BOGOTA#
```

```
CALI#
CALI#show ip route eigrp
     192.168.1.0/27 is subnetted, 5 subnets
D       192.168.1.0 [90/2172416] via 192.168.1.130, 00:40:18,
Serial0/0/0
D       192.168.1.32 [90/2684416] via 192.168.1.130, 00:40:18,
Serial0/0/0
D       192.168.1.96 [90/2681856] via 192.168.1.130, 00:40:18,
Serial0/0/0

CALI#
```

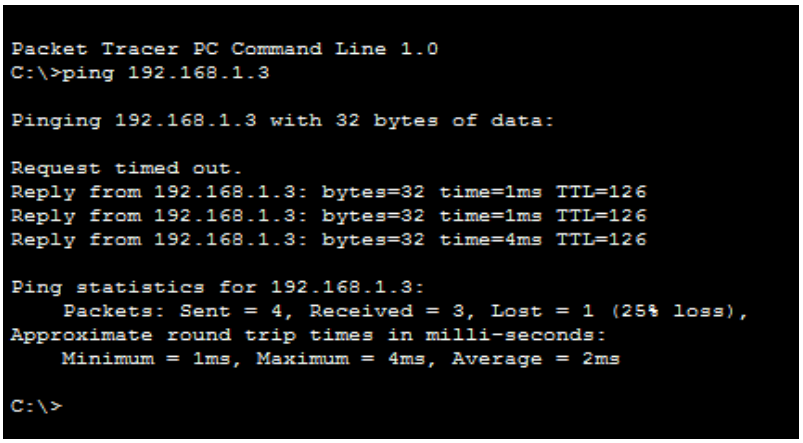
d. Realizar un diagnóstico para comprobar que cada uno de los puntos de la red se puedan ver y tengan conectividad entre sí. Realizar esta prueba desde un host de la red LAN del router CALI, primero a la red de MEDELLIN y luego al servidor.

Se realiza la verificación del estado de una conexión de un host por medio del comando ping y su dirección ip, lo vemos refleja en los diferentes pantallazos.

Conexión de Medellín a Cali:

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.66

Pinging 192.168.1.66 with 32 bytes of data:

Request timed out.
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 = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 3ms, Average = 2ms

C:\>
```

Conexión de Cali a Bogotá:



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

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

Las condiciones para crear las ACL son las siguientes:

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

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

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.

El asunto de creación de una ACL se realiza creando la lista después se relaciona a una interfaz entrante o saliente.

Medellin

MEDELLIN>enable
Password:

Password:
MEDELLIN#conf t
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN(config)#ip access-list extended COMERCIO
MEDELLIN(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.1.2
0.0.0.0
MEDELLIN(config-ext-nacl)#exit
MEDELLIN(config)#int g0/0
MEDELLIN(config-if)#ip access-group COMERCIO
% Incomplete command.
MEDELLIN(config-if)#ip access-group COMERCIO in
MEDELLIN(config-if)#end

Cali:

CALI>enable
Password:
CALI#conf t
Enter configuration commands, one per line. End with CNTL/Z.
CALI(config)#ip access-list extended ADMON
CALI(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.1.2 0.0.0.0
CALI(config-ext-nacl)#exit
CALI(config)#int g0/0
%Invalid interface type and number
CALI(config)#int fa0/0
CALI(config-if)#ip access-group ADMON in
CALI(config-if)#end
CALI#
%SYS-5-CONFIG_I: Configured from console by console

Bogota:

BOGOTA>enable
Password:
BOGOTA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA(config)#ip access-list extended GERENCIA
BOGOTA(config-ext-nacl)#permit ip 192.168.1.2 0.0.0.0 0.0.0.0
255.255.255.255
BOGOTA(config-ext-nacl)#exit
BOGOTA(config)#int g0/0
BOGOTA(config-if)#ip access-group GERENCIA in
BOGOTA(config-if)#end
BOGOTA#
%SYS-5-CONFIG_I: Configured from console by console

Permitir a los routers acceder a los equipos:

```
MEDELLIN>enable
Password:
MEDELLIN#conf t
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN(config)#ip access-list extended COMERCIO
MEDELLIN(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.1.33
0.0.0.0
MEDELLIN(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.1.98
0.0.0.0
MEDELLIN(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.1.131
0.0.0.0
MEDELLIN(config-ext-nacl)#end
MEDELLIN#
%SYS-5-CONFIG_I: Configured from console by console
```

```
BOGOTA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA(config)#ip access-list extended GERENCIA
BOGOTA(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.1.99
0.0.0.0
BOGOTA(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.1.1
0.0.0.0
BOGOTA(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.1.131
0.0.0.0
BOGOTA(config-ext-nacl)#end
BOGOTA#
        %SYS-5-CONFIG_I: Configured from console by console
```

```
CALI>enable
Password:
CALI#conf t
Enter configuration commands, one per line. End with CNTL/Z.
CALI(config)#ip access-list extended ADMON
CALI(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.1.99 0.0.0.0
CALI(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.130.1 0.0.0.0
CALI(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.1.65 0.0.0.0
CALI(config-ext-nacl)#end
CALI#
        %SYS-5-CONFIG_I: Configured from console by console
```

Parte 5: Comprobación de la red instalada.

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

Se realiza la comprobación de acceso individual con el comando *show Access-list*

```
MEDELLIN>enable
Password:
MEDELLIN#show access-list
Extended IP access list COMERCIO
    10 permit ip any host 192.168.1.2
    20 permit ip any host 192.168.1.33
    30 permit ip any host 192.168.1.98
    40 permit ip any host 192.168.1.131

MEDELLIN#
```

```
BOGOTA>enable
Password:
BOGOTA#show access-list
Extended IP access list GERENCIA
    10 permit ip host 192.168.1.2 any
    20 permit ip any host 192.168.1.99
    30 permit ip any host 192.168.1.1
    40 permit ip any host 192.168.1.131

BOGOTA#
```

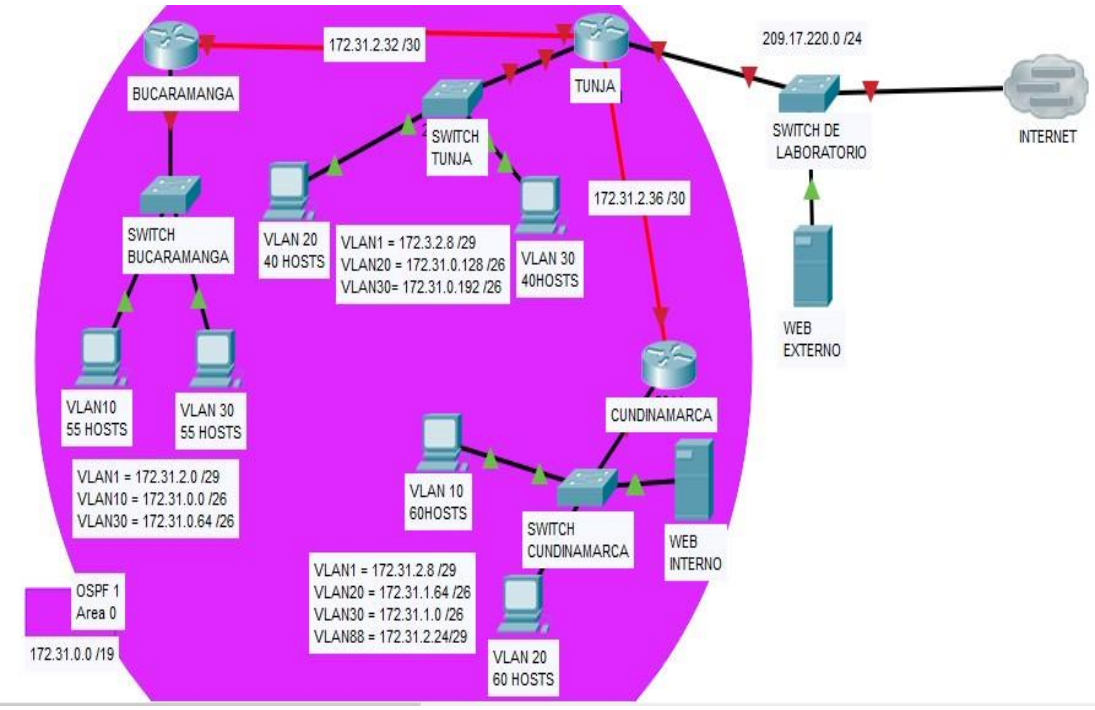
```
User Access Verification

Password:

CALI>enable
Password:
CALI#show access-list
Extended IP access list ADMON
    10 permit ip any host 192.168.1.2
    20 permit ip any host 192.168.1.99
    30 permit ip any host 192.168.130.1
    40 permit ip any host 192.168.1.65

CALI#
```

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	OK
	WS_1	Router BOGOTA	OK
	Servidor	Router CALI	OK
	Servidor	Router MEDELLIN	OK
TELNET	LAN del Router MEDELLIN	Router CALI	OK
	LAN del Router CALI	Router CALI	OK
	LAN del Router MEDELLIN	Router MEDELLIN	OK
	LAN del Router CALI	Router MEDELLIN	OK
PING	LAN del Router CALI	WS_1	FAIL
	LAN del Router MEDELLIN	WS_1	FAIL
	LAN del Router MEDELLIN	LAN del Router CALI	FAIL
PING	LAN del Router CALI	Servidor	OK
	LAN del Router MEDELLIN	Servidor	OK
	Servidor	LAN del Router MEDELLIN	OK
	Servidor	LAN del Router CALI	OK
	Router CALI	LAN del Router MEDELLIN	OK
	Router MEDELLIN	LAN del Router CALI	OK

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.



Los siguientes son los requerimientos necesarios:

Punto 1 Todos los routers deberán tener los siguientes:

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

Se realiza la configuración básica para cada router dándole un nombre a los routers con el comando hostname y sus respectivas contraseñas.

Configuración Inicial Router:

Bucaramanga:

```
Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname BUCARAMANGA
BUCARAMANGA(config)#enable password RED
BUCARAMANGA(config)#enable password RED1
BUCARAMANGA(config)#service password-encryption
BUCARAMANGA(config)#login block-for 150 attempts 3 within 20
BUCARAMANGA(config)#aaa new-model
BUCARAMANGA(config)#aaa authentication login RED1 local enable
BUCARAMANGA(config)#username NOMBRE0 secret REDES2
BUCARAMANGA(config)#line con 0
BUCARAMANGA(config-line)#login authentication RED1
BUCARAMANGA(config-line)#logging synchronous
BUCARAMANGA(config-line)#exe-timeout 11
^
% Invalid input detected at '^' marker.
BUCARAMANGA(config-line)#exec-timeout 11
BUCARAMANGA(config-line)#line vty 0 15
BUCARAMANGA(config-line)#login authentication RED1
BUCARAMANGA(config-line)#logging synchronous
BUCARAMANGA(config-line)#exec-timeout 5
BUCARAMANGA(config-line)#exit
BUCARAMANGA(config)#interface s0/0/0
BUCARAMANGA(config-if)#ip address 172.31.2.33 255.255.255.252
BUCARAMANGA(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
BUCARAMANGA(config-if)#interface g0/1.1
BUCARAMANGA(config-subif)#encapsulation dot1q 1
BUCARAMANGA(config-subif)#ip address 172.31.2.1 255.255.255.248
BUCARAMANGA(config-subif)#interface g0/1.10
BUCARAMANGA(config-subif)#encapsulation dot1q 10
BUCARAMANGA(config-subif)#ip address 172.31.0.1 255.255.255.192
BUCARAMANGA(config-subif)#interface g0/1.30
BUCARAMANGA(config-subif)#encapsulation dot1q 30
```

BUCARAMANGA(config-subif)#ip address 172.31.0.65 255.255.255.192
BUCARAMANGA(config-subif)#interface g0/1
BUCARAMANGA(config-if)#no shutdown

BUCARAMANGA(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/1.1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.1, changed state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/1.10, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.10, changed state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/1.30, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.30, changed state to up

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

Tunja:

Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname TUNJA
TUNJA(config)#enable password SISTEMAS10
TUNJA(config)#service password-encryption
TUNJA(config)#login block-for 150 attempts 3 within 20
TUNJA(config)#aaa new-model
TUNJA(config)#aaa authentication login GERENCIA12 local enable
TUNJA(config)#username NOMBRE13 secret ADMIN23
TUNJA(config)#line con 0

```
TUNJA(config-line)#login authentication GERENCIA12
TUNJA(config-line)#logging synchronous
TUNJA(config-line)#exec-timeout 11
TUNJA(config-line)#line vty 0 15
TUNJA(config-line)#login authentication GERENCIA12
TUNJA(config-line)#logging synchronous
TUNJA(config-line)#exec-timeout 5
TUNJA(config-line)#exit
TUNJA(config)#interface s0/0/0
TUNJA(config-if)#ip address 172.31.2.34 255.255.255.252
TUNJA(config-if)#clock rate 1000000
TUNJA(config-if)#no shutdown

TUNJA(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

TUNJA(config-if)#interface
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed
state to up

TUNJA(config-if)#interface s0/0/1
TUNJA(config-if)#ip address 172.31.2.37 255.255.255.252
TUNJA(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
TUNJA(config-if)#interface g0/0
TUNJA(config-if)#ip address 209.17.220.1 255.255.255.0
TUNJA(config-if)#no shutdown

TUNJA(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0,
changed state to up

TUNJA(config-if)#interface g0/1.1
TUNJA(config-subif)#encapsulation dot1q 20
TUNJA(config-subif)#ip address 172.31.0.129 255.255.255.192
TUNJA(config-subif)#interface g0/1.30
TUNJA(config-subif)#encapsulation dot1q 30
TUNJA(config-subif)#ip address 172.31.0.193 255.255.255.192
TUNJA(config-subif)#interface g0/1
TUNJA(config-if)#no shutdown
```

TUNJA(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/1.1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.1, changed state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/1.30, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.30, changed state to up

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

TUNJA#

Cundinamarca:

Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname CUNDINAMARCA
CUNDINAMARCA(config)#enable password SEGURIDAD40
CUNDINAMARCA(config)#service password-encryption
CUNDINAMARCA(config)#login block-for 150 attempts 3 within 20
CUNDINAMARCA(config)#aaa new-model
CUNDINAMARCA(config)#aaa authentication login CISCO50 local enable
CUNDINAMARCA(config)#username NOMBRE60 secret ANFITRION55
CUNDINAMARCA(config)#line con 0
CUNDINAMARCA(config-line)#login authentication CISCO50
CUNDINAMARCA(config-line)#logging synchronous
CUNDINAMARCA(config-line)#exec-timeout 11
CUNDINAMARCA(config-line)#line vty 0 15
CUNDINAMARCA(config-line)#login authentication CISCO50
CUNDINAMARCA(config-line)#logging synchronous
CUNDINAMARCA(config-line)#exec-timeout 5
CUNDINAMARCA(config-line)#exit
CUNDINAMARCA(config)#interface s0/01
%Invalid interface type and number
CUNDINAMARCA(config)#interface s0/0/1

```
CUNDINAMARCA(config-if)#ip address 172.31.2.38 255.255.255.252
CUNDINAMARCA(config-if)#clock rate 1000000
CUNDINAMARCA(config-if)#no shutdown

CUNDINAMARCA(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up

CUNDINAMARCA(config-if)#interface s0/0/1
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed
state to up

CUNDINAMARCA(config-if)#interface s0/0/1
CUNDINAMARCA(config-if)#interface g0/1.1
CUNDINAMARCA(config-subif)#encapsulation dot1q 1
CUNDINAMARCA(config-subif)#ip address 172..31.2.9 255.255.255.248
^
% Invalid input detected at '^' marker.
CUNDINAMARCA(config-subif)#ip address 172.31.2.9 255.255.255.248
CUNDINAMARCA(config-subif)#interface g0/1.20
CUNDINAMARCA(config-subif)#encapsulation dot1q 20
CUNDINAMARCA(config-subif)#ip address 172.31.1.65 255.255.255.192
CUNDINAMARCA(config-subif)#interface g0/1.30
CUNDINAMARCA(config-subif)#encapsulation dot1q 30
CUNDINAMARCA(config-subif)#ip address 172.31.1.1 255.255.255.192
CUNDINAMARCA(config-subif)#interface g0/1.88
CUNDINAMARCA(config-subif)#encapsulation dot1q 88
CUNDINAMARCA(config-subif)#ip address 172.31.2.25 255.255.255.248
CUNDINAMARCA(config-subif)#interface g0/1
CUNDINAMARCA(config-if)#no shutdown

CUNDINAMARCA(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1,
changed state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/1.1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.1,
changed state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/1.20, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.20,
changed state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/1.30, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.30,
changed state to up
```

%LINK-5-CHANGED: Interface GigabitEthernet0/1.88, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.88, changed state to up

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

CUNDINAMARCA#

Se configuran las VLAN para cada Switch:

Se configuran las VLAN para cada switch con su respectivo número de la VLAN que se desea configurar con el comando config-vlan.
Y también se le da un nombre a la VLAN con el comando name, estos pasos se registraron en los siguientes:

Bucaramanga:

Switch>enable
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan1
^
% Invalid input detected at '^' marker.
Switch(config)#vlan 1
Switch(config-vlan)#name VLAN1
Default VLAN 1 may not have its name changed.
Switch(config-vlan)#vlan 10
Switch(config-vlan)#name VLAN10
Switch(config-vlan)#vlan 30
Switch(config-vlan)#name VLAN30
Switch(config-vlan)#exit
Switch(config)#int VLAN1
Switch(config-if)#ip address 172.31.2.2 255.255.255.248
Switch(config-if)#no shutdown

Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

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

Switch(config-if)#int VLAN10
Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan10, changed state to up

Switch(config-if)#ip address 172.31.0.66 255.255.255.192
Switch(config-if)#no shutdown
Switch(config-if)#int f0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to up

Switch(config-if)#int f0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 30
Switch(config-if)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#copy run start
Destination filename [startup-config]?
Tunja:

Switch>enable
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 1
Switch(config-vlan)#name VLAN1
Default VLAN 1 may not have its name changed.
Switch(config-vlan)#vlan 20
Switch(config-vlan)#name VLAN20
Switch(config-vlan)#vlan 30
Switch(config-vlan)#name VLAN30
Switch(config-vlan)#exit
Switch(config)#int VLAN1
Switch(config-if)#ip address 172.3.2.10 255.255.255.248
Switch(config-if)#no shutdown
Switch(config-if)#int VLAN20
Switch(config-if)#ip address 172.31.0.130 255.255.255.192
Switch(config-if)#no shutdown
Switch(config-if)#int VLAN30
Switch(config-if)#ip address 172.31.0.194 255.255.255.192
Switch(config-if)#no shutdown
Switch(config-if)#int f0/1
Switch(config-if)#switchport mode access

Switch(config-if)#switchport access vlan 20
Switch(config-if)#int f0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 30
Switch(config-if)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#copy run start
Destination filename [startup-config]?

Cundinamarca:

Switch>enable
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 1
Switch(config-vlan)#name VLAN1
Default VLAN 1 may not have its name changed.
Switch(config-vlan)#vlan 20
Switch(config-vlan)#name VLAN20
Switch(config-vlan)#vlan 30
Switch(config-vlan)#name VLAN30
Switch(config-vlan)#vlan 88
Switch(config-vlan)#name VLAN88
Switch(config-vlan)#exit
Switch(config)#int VLAN1
Switch(config-if)#ip address 172.31.2.10 255.255.255.248
Switch(config-if)#no shutdown

Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

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

Switch(config-if)#int VLAN20
Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan20, changed state to up

Switch(config-if)#ip address 172.31.1.66 255.255.255.192
Switch(config-if)#no shutdown
Switch(config-if)#int VLAN30
Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan30, changed state to up

Switch(config-if)#ip address 172.31.1.2 255.255.255.192
Switch(config-if)#no shutdown

```
Switch(config-if)#int VLAN88
Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan88, changed state to up

Switch(config-if)#ip address 172.31.2.26 255.255.255.248
Switch(config-if)#no shutdown
Switch(config-if)#int f0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan20, changed state
to up

Switch(config-if)#int f0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 30
Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan30, changed state
to up

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

Switch#copy run start
    Destination filename [startup-config]?
```

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

Se configuran los routers con el comando DHCP dándole la asignación de direcciones IP.

DHCP en cada router:

Tunja:

```
TUNJA>enable
Password:
Password:
TUNJA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
TUNJA(config)#ip dhcp excluded-address 172.31.2.1 172.31.2.2
TUNJA(config)#ip dhcp excluded-address 172.31.0.1 172.31.0.2
```

```
TUNJA(config)#ip dhcp excluded-address 172.31.0.65 172.31.0.66
TUNJA(config)#ip dhcp excluded-address 172.31.2.9 172.31.2.10
TUNJA(config)#ip dhcp excluded-address 172.31.1.65 172.31.1.66
TUNJA(config)#ip dhcp excluded-address 172.31.1.1 172.31.1.2
TUNJA(config)#ip dhcp excluded-address 172.31.2.25 172.31.2.26
TUNJA(config)#ip dhcp excluded-address 172.31.2.11
TUNJA(config)#ip dhcp pool BucaramangaV1
TUNJA(dhcp-config)#network 172.31.2.0 255.255.255.248
TUNJA(dhcp-config)#default-router 172.31.2.1
TUNJA(dhcp-config)#ip dhcp pool BucaramangaV10
TUNJA(dhcp-config)#network 172.31.0.0 255.255.255.192
TUNJA(dhcp-config)#default-router 172.31.0.1
TUNJA(dhcp-config)#ip dhcp pool BucaramangaV30
TUNJA(dhcp-config)#network 172.31.0.64 255.255.255.192
TUNJA(dhcp-config)#default-router 172.31.0.65
TUNJA(dhcp-config)#ip dhcp pool CundinamarcaV1
TUNJA(dhcp-config)#network 172.31.2.8 255.255.255.248
TUNJA(dhcp-config)#default-router 172.31.2.9
TUNJA(dhcp-config)#ip dhcp pool CundinamarcaV20
TUNJA(dhcp-config)#network 172.31.1.64 255.255.255.192
TUNJA(dhcp-config)#default-router 172.31.1.65
TUNJA(dhcp-config)#ip dhcp pool CundinamarcaV30
TUNJA(dhcp-config)#network 172.31.1.0 255.255.255.192
TUNJA(dhcp-config)#default-router 172.31.1.1
TUNJA(dhcp-config)#ip dhcp pool CundinamarcaV88
TUNJA(dhcp-config)#network 172.31.2.24 255.255.255.248
TUNJA(dhcp-config)#default-router 172.31.2.25
TUNJA(dhcp-config)#end
TUNJA#
%SYS-5-CONFIG_I: Configured from console by console

TUNJA#copy run start
    Destination filename [startup-config]?
```

Bucaramanga:

```
BUCARAMANGA>enable
Password:
Password:
BUCARAMANGA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
BUCARAMANGA(config)#int g0/1.1
BUCARAMANGA(config-subif)#ip helper-address 172.31.2.34
BUCARAMANGA(config-subif)#int g0/1.10
BUCARAMANGA(config-subif)#ip helper-address 172.31.2.34
BUCARAMANGA(config-subif)#int g0/1.30
BUCARAMANGA(config-subif)#ip helper-address 172.31.2.34
```

```
BUCARAMANGA(config-subif)#end
BUCARAMANGA#
%SYS-5-CONFIG_I: Configured from console by console

BUCARAMANGA#copy run start
    Destination filename [startup-config]?
```

Cundinamarca:

```
CUNDINAMARCA>enable
Password:
Password:
CUNDINAMARCA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
CUNDINAMARCA(config)#int g0/1.1
CUNDINAMARCA(config-subif)#ip helper-address 172.31.2.37
CUNDINAMARCA(config-subif)#int g0/1.20
CUNDINAMARCA(config-subif)#ip helper-address 172.31.2.37
CUNDINAMARCA(config-subif)#int g0/1.30
CUNDINAMARCA(config-subif)#ip helper-address 172.31.2.37
CUNDINAMARCA(config-subif)#int g0/1.88
CUNDINAMARCA(config-subif)#ip helper-address 172.31.2.37
CUNDINAMARCA(config-subif)#end
CUNDINAMARCA#
%SYS-5-CONFIG_I: Configured from console by console

CUNDINAMARCA#copy run start
    Destination filename [startup-config]?
```

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

Se realiza la configuración con el comando NAT estático el cual se mapea una dirección IP privada con una publica de forma estática, para esto se realiza con el comando *ip nat inside source static.*

```
TUNJA>enable
Password:
Password:
Password:
TUNJA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
TUNJA(config)#ip nat inside source static 172.31.2.11 209.17.220.7
```

```
TUNJA(config)#ip access-list standart COLOMBIA
^
% Invalid input detected at '^' marker.
TUNJA(config)#ip access-list standard COLOMBIA
TUNJA(config-std-nacl)#permit 172.31.0.0 0.0.255.255
TUNJA(config-std-nacl)#exit
TUNJA(config)#ip nat inside source list COLOMBIA interface g0/0 overload
TUNJA(config)#int g0/0
TUNJA(config-if)#ip nat outside
TUNJA(config-if)#int s0/0/0
TUNJA(config-if)#ip nat inside
TUNJA(config-if)#int s0/0/1
TUNJA(config-if)#ip nat inside
TUNJA(config-if)#int g0/1.1
TUNJA(config-subif)#ip nat inside
TUNJA(config-subif)#int g0/1.20
TUNJA(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1.20, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.20,
changed state to up

TUNJA(config-subif)#ip nat inside
TUNJA(config-subif)#int g0/1.30
TUNJA(config-subif)#ip nat inside
TUNJA(config-subif)#end
TUNJA#
%SYS-5-CONFIG_I: Configured from console by console

TUNJA#copy run start
Destination filename [startup-config]?
```

Configuración de ruta estática predeterminada:

```
TUNJA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
TUNJA(config)#ip route 0.0.0.0 0.0.0.0 g0/0
%Default route without gateway, if not a point-to-point interface, may impact
performance
TUNJA(config)#router ospf 1
TUNJA(config-router)#default-information originate
TUNJA(config-router)#end
TUNJA#
%SYS-5-CONFIG_I: Configured from console by console

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

Punto 4. El enrutamiento deberá tener autenticación.

Se realiza el protocolo de enrutamiento para cada routers.

Se anuncian las redes en cada router:

Bucaramanga:

```
BUCARAMANGA>enable
Password:
Password:
BUCARAMANGA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
BUCARAMANGA(config)#router ospf 100
BUCARAMANGA(config-router)#router-id 1.1.1.1
BUCARAMANGA(config-router)#network 172.31.2.32 0.0.0.3 area 0
BUCARAMANGA(config-router)#network 172.31.2.0 0.0.0.7 area 0
BUCARAMANGA(config-router)#network 172.31.0.1 0.0.0.63 area 0
BUCARAMANGA(config-router)#network 172.31.0.64 0.0.0.63 area 0
BUCARAMANGA(config-router)#passive-interface g0/1
BUCARAMANGA(config-router)#area 0 authentication
BUCARAMANGA(config-router)#exit
BUCARAMANGA(config)#int s0/0/0
BUCARAMANGA(config-if)#ip ospf authentication-key osinterpf
%OSPF: Warning: The password/key will be truncated to 8 characters
BUCARAMANGA(config-if)#copy run start
^
% Invalid input detected at '^' marker.
BUCARAMANGA(config-if)#no ip ospf authentication-key osinterpf
BUCARAMANGA(config-if)#ip ospf authentication-key LuisOSPF
BUCARAMANGA(config-if)#copy run start
^
% Invalid input detected at '^' marker.
BUCARAMANGA(config-if)#end
BUCARAMANGA#
%SYS-5-CONFIG_I: Configured from console by console

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

Tunja:

```
TUNJA>enable
Password:
TUNJA#conf t
```

```
Enter configuration commands, one per line. End with CNTL/Z.
TUNJA(config)#router ospf 100
TUNJA(config-router)#router - id 2.2.2.2
^
% Invalid input detected at '^' marker.
TUNJA(config-router)#router-id 2.2.2.2
TUNJA(config-router)#network 172.31.2.32 0.0.0.3 area 0
TUNJA(config-router)#network 172.31.2.36 0.0.0.3 area 0
TUNJA(config-router)#network 209.17.220.0 0.0.0.255 area 0
TUNJA(config-router)#network 172.3.2.8 0.0.0.7 area 0
TUNJA(config-router)#network 172.31.0.128 0.0.0.63 area 0
TUNJA(config-router)#network 172.31.0.192 0.0.0.63 area 0
TUNJA(config-router)#passive-interface g0/1
TUNJA(config-router)#area 0 authentication
TUNJA(config-router)#exit
TUNJA(config)#int s0/0/0
TUNJA(config-if)#ip ospf authentication-key LuisOSPF
TUNJA(config-if)#
06:53:23: %OSPF-5-ADJCHG: Process 100, Nbr 1.1.1.1 on Serial0/0/0 from
LOADING to FULL, Loading Done

TUNJA(config-if)#int s0/0/1
TUNJA(config-if)#ip ospf authentication-key LuisOSPF
TUNJA(config-if)#copy run start
^
% Invalid input detected at '^' marker.
TUNJA(config-if)#end
TUNJA#
%SYS-5-CONFIG_I: Configured from console by console

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

CUNDINAMARCA:

```
CUNDINAMARCA>enable
Password:
CUNDINAMARCA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
CUNDINAMARCA(config)#router ospf 100
CUNDINAMARCA(config-router)#router-id 3.3.3.3
CUNDINAMARCA(config-router)#network 172.31.2.36 0.0.0.3 area 0
CUNDINAMARCA(config-router)#network 172.31.2.8 0.0.0.7 area 0
CUNDINAMARCA(config-router)#network 172.31.1.64 0.0.0.63 area 0
CUNDINAMARCA(config-router)#network 172.31.1.0 0.0.0.63 area 0
```

```
CUNDINAMARCA(config-router)#network 172.31.2.24 0.0.0.7 area 0
CUNDINAMARCA(config-router)#passive-interface g0/1
CUNDINAMARCA(config-router)#area 0 authentication
CUNDINAMARCA(config-router)#exit
CUNDINAMARCA(config)#int s0/0/0
CUNDINAMARCA(config-if)#ip ospf authentication-key LuisOSPF
CUNDINAMARCA(config-if)#copy run start
^
% Invalid input detected at '^' marker.
CUNDINAMARCA(config-if)#end
CUNDINAMARCA#
%SYS-5-CONFIG_I: Configured from console by console

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

Punto 5. Listas de control de acceso:

En este paso se realiza el control de determinar los permisos de acceso o sea permitiendo o denegando el tráfico de red.
Para esto se realiza con el comando *ip access-list extended.*

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

```
Username: NOMBRE60
Password:
CUNDINAMARCA>enable
Password:
CUNDINAMARCA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
CUNDINAMARCA(config)#ip access-list extended LANCV30
CUNDINAMARCA(config-ext-nacl)#permit ip 172.31.1.0 0.0.0.63 172.31.2.16 0.0.0.7
CUNDINAMARCA(config-ext-nacl)#permit ip 172.31.1.0 0.0.0.63 172.31.0.128
0.0.0.63
CUNDINAMARCA(config-ext-nacl)#permit ip 172.31.1.0 0.0.0.63 172.31.0.192
0.0.0.63
CUNDINAMARCA(config-ext-nacl)#exit
CUNDINAMARCA(config)#int g0/1.30
CUNDINAMARCA(config-subif)#ip access-group LANCV30 in
CUNDINAMARCA(config-subif)#end
```

```
CUNDINAMARCA#
%SYS-5-CONFIG_I: Configured from console by console
```

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

```
CUNDINAMARCA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
CUNDINAMARCA(config)#ip access-list extended LANCV20
CUNDINAMARCA(config-ext-nacl)#deny ip 172.31.1.64 0.0.0.63 172.31.2.16 0.0.0.7
CUNDINAMARCA(config-ext-nacl)#deny ip 172.31.1.64 0.0.0.63 172.31.0.128
0.0.0.63
CUNDINAMARCA(config-ext-nacl)#deny ip 172.31.1.64 0.0.0.63 172.31.0.192
0.0.0.63
CUNDINAMARCA(config-ext-nacl)#permit ip any any
CUNDINAMARCA(config-ext-nacl)#exit
CUNDINAMARCA(config)#int g0/1.20
CUNDINAMARCA(config-subif)#ip access-group LANCV20 in
CUNDINAMARCA(config-subif)#end
CUNDINAMARCA#
%SYS-5-CONFIG_I: Configured from console by console
```

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

```
TUNJA>enable
Password:
TUNJA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
TUNJA(config)#ip access-list extended LANTV30
TUNJA(config-ext-nacl)#permit tcp 172.31.0.192 0.0.0.63 0.0.0.0 255.255.255.255 eq
ftp
TUNJA(config-ext-nacl)#permit tcp 172.31.0.192 0.0.0.63 0.0.0.0 255.255.255.255 eq
www
TUNJA(config-ext-nacl)#exit
TUNJA(config)#int g0/1.30
TUNJA(config-subif)#ip access-group LANTV30 in
TUNJA(config-subif)#end
TUNJA#
%SYS-5-CONFIG_I: Configured from console by console
```

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

```
TUNJA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
TUNJA(config)#ip access-list extended LANTV20
TUNJA(config-ext-nacl)#permit tcp 172.31.0.128 0.0.0.63 172.31.1.0 0.0.0.63
TUNJA(config-ext-nacl)#permit tcp 172.31.0.128 0.0.0.63 172.31.0.0 0.0.0.63
TUNJA(config-ext-nacl)#exit
TUNJA(config)#int g0/1.20
TUNJA(config-subif)#ip access-group LANTV20 in
TUNJA(config-subif)#end
TUNJA#
%SYS-5-CONFIG_I: Configured from console by console
```

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

```
BUCARAMANGA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
BUCARAMANGA(config)#ip access-list extended LANBV30
BUCARAMANGA(config-ext-nacl)#deny ip 172.31.0.64 0.0.0.63 172.31.2.0
0.0.0.7
BUCARAMANGA(config-ext-nacl)#deny ip 172.31.0.64 0.0.0.63 172.31.2.16
0.0.0.7
BUCARAMANGA(config-ext-nacl)#deny ip 172.31.0.64 0.0.0.63 172.31.0.128
0.0.0.63
BUCARAMANGA(config-ext-nacl)#deny ip 172.31.0.64 0.0.0.63 172.31.0.192
0.0.0.63
BUCARAMANGA(config-ext-nacl)#deny ip 172.31.0.64 0.0.0.63 172.31.2.8
0.0.0.7
BUCARAMANGA(config-ext-nacl)#deny ip 172.31.0.64 0.0.0.63 172.31.1.64
0.0.0.63
BUCARAMANGA(config-ext-nacl)#deny ip 172.31.0.64 0.0.0.63 172.31.1.0
0.0.0.63
BUCARAMANGA(config-ext-nacl)#deny ip 172.31.0.64 0.0.0.63 172.31.2.24
0.0.0.7
BUCARAMANGA(config-ext-nacl)#permit ip any any
BUCARAMANGA(config-ext-nacl)#exit
BUCARAMANGA(config)#int g0/1.30
BUCARAMANGA(config-subif)#ip access-group LANBV30
% Incomplete command.
BUCARAMANGA(config-subif)#ip access-group LANBV30 in
BUCARAMANGA(config-subif)#end
BUCARAMANGA#
%SYS-5-CONFIG_I: Configured from console by console
```

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

```
BUCARAMANGA#conf t
```

```
Enter configuration commands, one per line. End with CNTL/Z.
BUCARAMANGA(config)#ip access-list extended LANBV10
BUCARAMANGA(config-ext-nacl)#permit ip 172.31.0.0 0.0.0.63 172.31.1.0
0.0.0.63
BUCARAMANGA(config-ext-nacl)#permit ip 172.31.0.0 0.0.0.63 172.31.0.128
0.0.0.63
BUCARAMANGA(config-ext-nacl)#exit
BUCARAMANGA(config)#int g0/1.10
BUCARAMANGA(config-subif)#ip access-group LANBV10 in
BUCARAMANGA(config-subif)#end
BUCARAMANGA#
%SYS-5-CONFIG_I: Configured from console by console
```

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

```
CUNDINAMARCA>enable
Password:
CUNDINAMARCA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
CUNDINAMARCA(config)#ip access-list extended LANCV20
CUNDINAMARCA(config-ext-nacl)#no permit ip any any
CUNDINAMARCA(config-ext-nacl)#deny ip 172.31.1.64 0.0.0.63 172.31.2.8
0.0.0.7
CUNDINAMARCA(config-ext-nacl)#deny ip 172.31.1.64 0.0.0.63 172.31.1.0
0.0.0.63
CUNDINAMARCA(config-ext-nacl)#deny ip 172.31.1.64 0.0.0.63 172.31.2.24
0.0.0.7
CUNDINAMARCA(config-ext-nacl)#permit ip any any
CUNDINAMARCA(config-ext-nacl)#end
CUNDINAMARCA#
%SYS-5-CONFIG_I: Configured from console by console

CUNDINAMARCA#show access-list
Extended IP access list sl_def_acl
0 deny tcp any any eq telnet
0 deny tcp any any eq www
0 deny tcp any any eq 22
0 permit tcp any any eq 22
Extended IP access list LANCV30
10 permit ip 172.31.1.0 0.0.0.63 172.31.2.16 0.0.0.7
20 permit ip 172.31.1.0 0.0.0.63 172.31.0.128 0.0.0.63
30 permit ip 172.31.1.0 0.0.0.63 172.31.0.192 0.0.0.63
Extended IP access list LANCV20
10 deny ip 172.31.1.64 0.0.0.63 172.31.2.16 0.0.0.7
20 deny ip 172.31.1.64 0.0.0.63 172.31.0.128 0.0.0.63
30 deny ip 172.31.1.64 0.0.0.63 172.31.0.192 0.0.0.63
40 deny ip 172.31.1.64 0.0.0.63 172.31.2.8 0.0.0.7
```

50 deny ip 172.31.1.64 0.0.0.63 172.31.1.0 0.0.0.63
60 deny ip 172.31.1.64 0.0.0.63 172.31.2.24 0.0.0.7
70 permit ip any any

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

Username: NOMBRE0
Password:
BUCARAMANGA>enable
Password:
BUCARAMANGA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
BUCARAMANGA(config)#ip access-list extended LANBV30
BUCARAMANGA(config-ext-nacl)#no permit ip any any
BUCARAMANGA(config-ext-nacl)#deny ip 172.31.0.64 0.0.0.63 172.31.2.0 0.0.0.7
BUCARAMANGA(config-ext-nacl)#permit ip any any
BUCARAMANGA(config-ext-nacl)#end
BUCARAMANGA#
%SYS-5-CONFIG_I: Configured from console by console

BUCARAMANGA#show access-list
Extended IP access list sl_def_acl
0 deny tcp any any eq telnet
0 deny tcp any any eq www
0 deny tcp any any eq 22
0 permit tcp any any eq 22
Extended IP access list LANBV30
10 deny ip 172.31.0.64 0.0.0.63 172.31.2.0 0.0.0.7
20 deny ip 172.31.0.64 0.0.0.63 172.31.2.16 0.0.0.7
30 deny ip 172.31.0.64 0.0.0.63 172.31.0.128 0.0.0.63
40 deny ip 172.31.0.64 0.0.0.63 172.31.0.192 0.0.0.63
50 deny ip 172.31.0.64 0.0.0.63 172.31.2.8 0.0.0.7
60 deny ip 172.31.0.64 0.0.0.63 172.31.1.64 0.0.0.63
70 deny ip 172.31.0.64 0.0.0.63 172.31.1.0 0.0.0.63
80 deny ip 172.31.0.64 0.0.0.63 172.31.2.24 0.0.0.7
90 permit ip any any
Extended IP access list LANBV10
10 permit ip 172.31.0.0 0.0.0.63 172.31.1.0 0.0.0.63
20 permit ip 172.31.0.0 0.0.0.63 172.31.0.128 0.0.0.63

BUCARAMANGA#

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

CONCLUSIONES

- ✓ El diplomado de CISCO se concluye con la prueba de habilidades prácticas CCNA lo cual se pone a prueba lo visto en el desarrollo del curso.
- ✓ Este diplomado de CISCO ayuda para tener un mejor rendimiento en las empresas para un mejor desempeño laboral.
- ✓ EL programa de CISCO favorece a las empresas en beneficios de seguridad, reducción de costos, mejor rendimiento, mayor eficiencia del personal, etc.

BIBLIOGRAFIA

- CISCO. (2014). DHCP. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module10/index.html#10.0.1.1
- CISCO. (2014). 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). Enrutamiento Dinámico. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module7/index.html#7.0.1.1
- El profe García. (Enero 2013). Configuración DHCP con Packet Tracer. Diciembre 2019, de Youtube Sitio web: https://www.youtube.com/watch?v=l8FAx4T7AaA