DIPLOMADO DE PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN) (OPCI - (203092A_614)

JORGE ALBERTO CORTES MONTOYA

TUTOR

NILSON ALBEIRO FERREIRA MANZANARES

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA

PROGRAMA DE INGENIERIA DE SISTEMAS

MEDELLÍN

DICIEMBRE, 2019

Tabla de Contenido

Resumen

El presente trabajo se realiza con el propósito de poner en práctica los conocimientos adquiridos durante el desarrollo del Diplomado De Profundización CISCO (Diseño e Implementación de soluciones integradas LAN/WAN), ayudando al estudiante a obtener las habilidades necesarias en el manejo de redes, el trabajo se divide en dos escenarios, donde para cada uno de ellos debe construir su topología.

En el escenario 1 se desarrolla los conocimientos en cuanto a la configuración de los equipos descritos en una topología y en una tabla la cual contiene el direccionamiento de cada uno de ellos, así como el protocolo de enrutamiento EIGRP y las ACL. En el escenario 2, se implementa el servidor TFTP, los DNS, al igual que NAT, PAT, VLAN y DHCP.

Abstract

This work is carried out with the purpose of putting into practice the knowledge acquired during the development of the CISCO Deepening Diploma (Design and Implementation of integrated LAN / WAN solutions), helping the student to obtain the necessary skills in network management, the Work is divided into two scenarios, where for each of them you must build your topology.

In scenario 1, knowledge is developed regarding the configuration of the equipment described in a topology and in a table which contains the address of each of them, as well as the EIGRP routing protocol and the ACLs. In scenario 2, the TFTP server, DNS, as well as NAT, PAT, VLAN and DHCP are implemented.

Introducción

Las características del mundo moderno, con una tendencia creciente hacia el entendimiento entre naciones y personas, se beben en buena medida a la expansión de la aplicación de la tecnología a las comunicaciones en general, pero fundamentalmente a las telecomunicaciones y al aumento de su rapidez y posibilidades. Las telecomunicaciones facilitan la superación de muchas fronteras, permitiendo el nacimiento de nuevos intereses mutuos entre individuos y entre sociedades. Como medio singular con que cuentan las telecomunicaciones modernas. Los sistemas de telecomunicaciones pueden transmitir información de texto, imágenes gráficas, voz o video.

En el mundo actual, la infraestructura de telecomunicaciones es fundamental para el desarrollo económico, humano y social. En las últimas décadas los avances tecnológicos en el área de las telecomunicaciones y la teleinformática han sido sorprendentes y han ampliado considerablemente el espectro de posibilidades y servicios de comunicación. La telefonía inalámbrica ha venido a transformar los paradigmas de comunicación para las comunidades pequeñas y aisladas, reduciendo sustantivamente los costos de la infraestructura necesaria. Los enlaces vía satélite y el desarrollo de las fibras ópticas han permitido incrementar el tráfico de llamadas de manera muy importante.

Objetivos

General

Implementar todas las habilidades teóricas y prácticas, por parte de los estudiantes de la Universidad Nacional Abierta y a Distancia, para identificar y aplicar una solución a un caso o situación estudio de problema de Networking.

Específicos

- Identificar que dispositivos utilizar para la construcción de una topología de red.
- Realizar configuración básica a dispositivos de comunicación como Routers, Switch, Servidores.
- Implementar seguridad en Switch.
- Determinar la configuración necesaria para la implementación de EIGRP.
- Implementar de DHCP y NAT en dispositivos de comunicación.
- Configurar y verificar listas de control de acceso ACL
- Verificar conectividad entre los dispositivos de una topología.

Escenario 1

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

Topología de red

Los requerimientos solicitados son los siguientes:

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

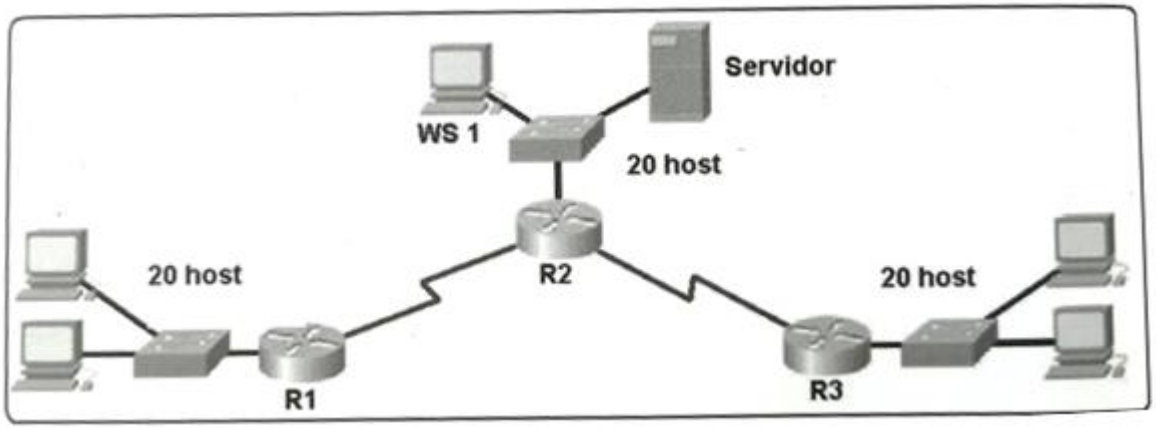
Parte 2: Considerar la asignación de los parámetros básicos y la detección de vecinos directamente conectados.

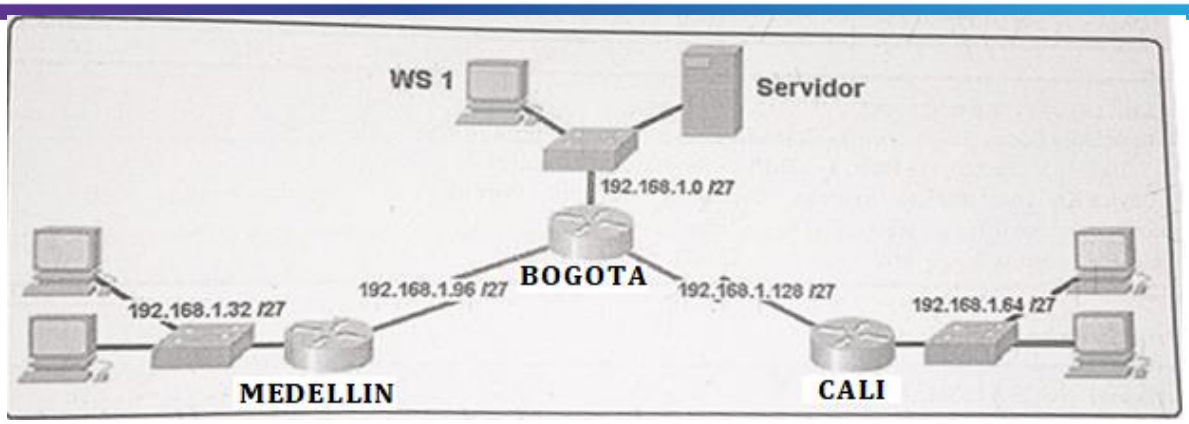
Parte 3: La red y subred establecidas deberán tener una interconexión total, todos los hosts deberán ser visibles y poder comunicarse entre ellos sin restricciones.

Parte 4: Implementar la seguridad en la red, se debe restringir el acceso y comunicación entre hosts de acuerdo con los requerimientos del administrador de red.

Parte 5: Comprobación total de los dispositivos y su funcionamiento en la red.

Parte 6: Configuración final.





Desarrollo

Como trabajo inicial se debe realizar lo siguiente.

- Realizar las rutinas de diagnóstico y dejar los equipos listos para su configuración (asignar nombres de equipos, asignar claves de seguridad, etc).
- Realizar la conexión fisica de los equipos con base en la topología de red

Router Bogota

```
Router>enable
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname BOGOTA
BOGOTA(config)#no ip domain-lookup
BOGOTA(config)#enable secret class
BOGOTA(config)#line con 0
BOGOTA(config-line)#password cisco
BOGOTA(config-line)#login
BOGOTA(config-line)#line vty 0 4
BOGOTA(config-line)#password cisco
BOGOTA(config-line)#login
BOGOTA(config-line)#exit
BOGOTA(config)#service password-encryption
BOGOTA(config)#banner motd # Unauthorized Access Is Prohibited #$
BOGOTA(config)#exit
BOGOTA#
%SYS-5-CONFIG_I: Configured from console by console
BOGOTA#copy running-config startup-config
Destination filename [startup-config]?
```

```
Building configuration...
[OK]
BOGOTA#
```

Router Medellin

```
Router>enable
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname MEDELLIN
MEDELLIN(config)#no ip domain-lookup
MEDELLIN(config)#enable secret class
MEDELLIN(config)#line con 0
MEDELLIN(config-line)#password cisco
MEDELLIN(config-line)#login
MEDELLIN(config-line)#line vty 0 4
MEDELLIN(config-line)#password cisco
MEDELLIN(config-line)#login
MEDELLIN(config-line)#exit
MEDELLIN(config)#service password-encryption
MEDELLIN(config)#banner motd # Unauthorized Access Is Prohibited #
MEDELLIN(config)#exit
MEDELLIN#
%SYS-5-CONFIG_I: Configured from console by console
MEDELLIN #copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
MEDELLIN#
```

Router Cali

```
Router>enable
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname CALI
CALI(config)#no ip domain-lookup
CALI(config)#enable secret class
CALI(config)#line con 0
CALI(config-line)#password cisco
CALI(config-line)#login
CALI(config-line)#line vty 0 4
```

```
CALI(config-line)#password cisco
CALI(config-line)#login
CALI(config-line)#exit
CALI(config)#service password-encryption
CALI(config)#banner motd # Unauthorized Access Is Prohibited #
CALI(config)#exit
CALI#
%SYS-5-CONFIG_I: Configured from console by console
CALI#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
CALI#
```

S1

```
Switch>enable
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#no ip domain-lookup
S1(config)#enable secret class
S1(config)#line con 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#exit
S1(config)#service password-encryption
S1(config)#banner motd # Unauthorized Access Is Prohibited #
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console
S1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
S1#
```

S2

```
Switch>enable
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S2
S2(config)#no ip domain-lookup
S2(config)#enable secret class
S2(config)#line con 0
S2(config-line)#password cisco
S2(config-line)#login
S2(config-line)#exit
S2(config)#service password-encryption
S2(config)#banner motd # Unauthorized Access Is Prohibited #
S2(config)#exit
S2#
%SYS-5-CONFIG_I: Configured from console by console
S2#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
S2#
```

S3

```
Switch>enable
Switch#confi t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S3
S3(config)#no ip domain-lookup
S3(config)#enable secret class
S3(config)#line con 0
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#exit
S3(config)#service password-encryption
S3(config)#banner motd # Unauthorized Access Is Prohibited #
S3(config)#exit
S3#
%SYS-5-CONFIG_I: Configured from console by console
S3#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
```

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

Parte 1: Asignación de direcciones IP:

a. Se debe dividir (subnetear) la red creando una segmentación en ocho partes, para permitir crecimiento futuro de la red corporativa.
b. Asignar una dirección IP a la red.

Network	Netmask	Hostmin	Hostmax	Broadcast
192.168.1.0/27	255.255.255.224	192.168.1.1	192.168.1.30	192.168.1.31
192.168.1.32/27	255.255.255.224	192.168.1.33	192.168.1.62	192.168.1.63
192.168.1.64/27	255.255.255.224	192.168.1.65	192.168.1.94	192.168.1.95
192.168.1.96/27	255.255.255.224	192.168.1.97	192.168.1.126	192.168.1.127
192.168.1.128/27	255.255.255.224	192.168.1.129	192.168.1.158	192.168.1.159
192.168.1.160/27	255.255.255.224	192.168.1.161	192.168.1.190	192.168.1.191
192.168.1.192/27	255.255.255.224	192.168.1.193	192.168.1.222	192.168.1.223
192.168.1.224/27	255.255.255.224	192.168.1.225	192.168.1.254	192.168.1.255

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	192.168.1.132	192.168.1.130	192.168.1.193
Dirección de Ip en interfaz FA 0/0	192.168.1.33	192.168.1.1	192.168.1.65
Protocolo de enrutamiento	**Eigrp**	**Eigrp**	**Eigrp**
Sistema Autónomo	200	200	200
Afirmaciones de red	192.168.1.0	192.168.1.0	192.168.1.0

b. Después de cargada la configuración en los dispositivos, verificar la tabla de enrutamiento en cada uno de los routers para comprobar las redes y sus rutas.

Bogotá

BOGOTA>enable
Password:
BOGOTA #configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA (config)#int s0/0/0
BOGOTA (config-if)#ip address 192.168.1.98 255.255.255.224
BOGOTA (config-if)#clock rate 128000
BOGOTA (config-if)#no shut
BOGOTA (config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
BOGOTA (config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
BOGOTA (config-if)#exit
BOGOTA (config)#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 up
BOGOTA (config-if)#exit
BOGOTA (config)#int g0/0
BOGOTA (config-if)#ip address 192.168.1.1 255.255.255.224
BOGOTA (config-if)#no shut
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)#

Medellín

User Access Verification
Password:
MEDELLIN>enable
Password:
MEDELLIN #configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN (config)#int s0/0/0
MEDELLIN (config-if)#ip address 192.168.1.99 255.255.255.224

```
MEDELLIN (config-if)#clock rate 128000
This command applies only to DCE interfaces
MEDELLIN (config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
MEDELLIN (config-if)#
MEDELLIN #
%SYS-5-CONFIG_I: Configured from console by console
MEDELLIN (config)#int s0/0/1
MEDELLIN (config-if)#ip address 192.168.1.132 255.255.255.224
MEDELLIN (config-if)#no shutdown
MEDELLIN (config-if)#
MEDELLIN (config)#int 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)# exit
MEDELLIN #
```

Cali

```
CALI>enable
Password:
CALI #config t
Enter configuration commands, one per line. End with CNTL/Z.
CALI (config)#int s0/0/0
CALI (config-if)#ip address 192.168.1.131 255.255.255.224
CALI (config-if)#clock rate 128000
CALI (config-if)#no shut
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
CALI (config-if)#
CALI (config-if)#exit
CALI (config)#int s0/0/1
CALI (config-if)#ip address 192.168.1.193 255.255.255.224
CALI (config-if)#clock rate 128000
CALI (config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
CALI (config-if)# exit
CALI (config)#int g0/0
CALI (config-if)#ip address 192.168.1.65 255.255.255.224
CALI (config-if)#no shut
CALI (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
CALI (config-if)#

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

Para ver como esta configurado el balanceo de carga se utiliza le comando
Show ip route

Para configurar el balanceo de cargas se utilizan los comandos
Router eigrp 1
Variance - numero

Router Bogotá

BOGOTA>enable

Password:

BOGOTA#

BOGOTA#config t

Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA(config)#router eigrp 1
BOGOTA(config-router)#variance 10
BOGOTA(config-router)#end
BOGOTA#
%SYS-5-CONFIG_I: Configured from console by console
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, 9 subnets, 2 masks
C 192.168.1.0/27 is directly connected, GigabitEthernet0/0
L 192.168.1.1/32 is directly connected, GigabitEthernet0/0

D 192.168.1.32/27 [90/2172416] via 192.168.1.99, 00:17:30, Serial0/0/0
D 192.168.1.64/27 [90/2172416] via 192.168.1.131, 00:17:31, Serial0/0/1
C 192.168.1.96/27 is directly connected, Serial0/0/0
L 192.168.1.98/32 is directly connected, Serial0/0/0
C 192.168.1.128/27 is directly connected, Serial0/0/1
L 192.168.1.130/32 is directly connected, Serial0/0/1

D 192.168.1.192/27 [90/2681856] via 192.168.1.131, 00:17:31, Serial0/0/1

Router Medellín

MEDELLIN>enable

Password:

MEDELLIN#config t

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

MEDELLIN(config)#router eigrp 1

MEDELLIN(config-router)#variance 10

MEDELLIN(config-router)#end

MEDELLIN#

%SYS-5-CONFIG_I: Configured from console by console

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, 9 subnets, 2 masks

D 192.168.1.0/27 [90/2172416] via 192.168.1.98, 00:23:25, Serial0/0/0

C 192.168.1.32/27 is directly connected, GigabitEthernet0/0

L 192.168.1.33/32 is directly connected, GigabitEthernet0/0

D 192.168.1.64/27 [90/2684416] via 192.168.1.98, 00:23:25, Serial0/0/0
C 192.168.1.96/27 is directly connected, Serial0/0/0
L 192.168.1.99/32 is directly connected, Serial0/0/0
C 192.168.1.128/27 is directly connected, Serial0/0/1
L 192.168.1.132/32 is directly connected, Serial0/0/1
D 192.168.1.192/27 [90/3193856] via 192.168.1.98, 00:23:25, Serial0/0/0

Router Cali

CALI>enable
Password:
CALI#config t
Enter configuration commands, one per line. End with CNTL/Z.
CALI(config)#router eigrp 1
CALI(config-router)#variance 10
CALI(config-router)#end
CALI#
%SYS-5-CONFIG_I: Configured from console by console
CALI#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, 9 subnets, 2 masks
D 192.168.1.0/27 [90/2172416] via 192.168.1.130, 00:26:09, Serial0/0/0
D 192.168.1.32/27 [90/2684416] via 192.168.1.130, 00:26:08, Serial0/0/0

C 192.168.1.64/27 is directly connected, GigabitEthernet0/0

L 192.168.1.65/32 is directly connected, GigabitEthernet0/0

D 192.168.1.96/27 [90/2681856] via 192.168.1.130, 00:26:09, Serial0/0/0

C 192.168.1.128/27 is directly connected, Serial0/0/0

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

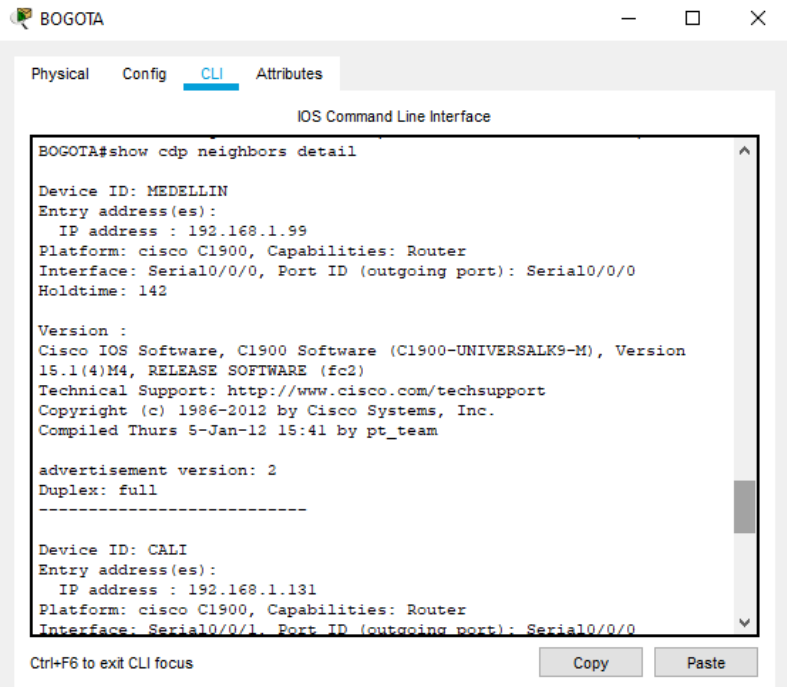
C 192.168.1.192/27 is directly connected, Serial0/0/1

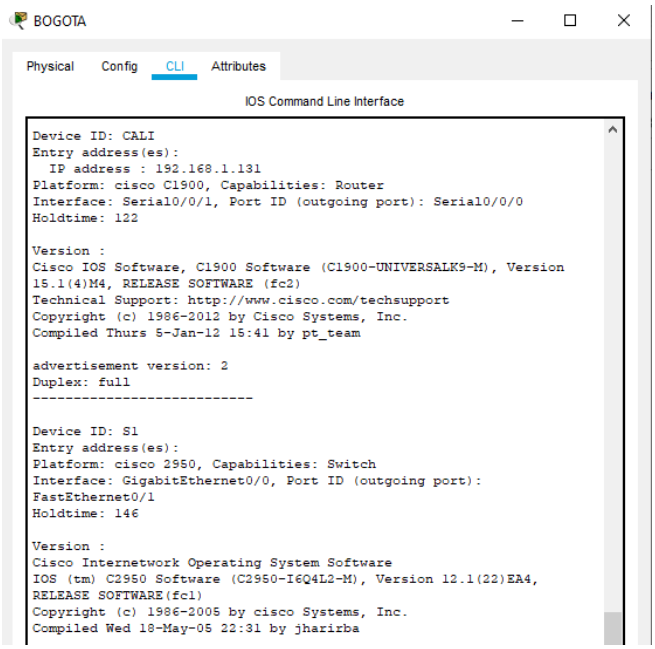
L 192.168.1.193/32 is directly connected, Serial0/0/1

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

Bogota

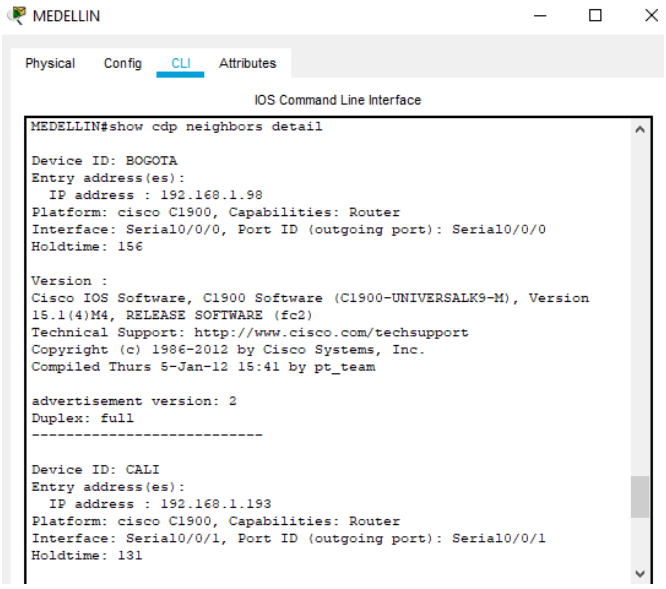
BOGOTA# show cdp neighbors detail

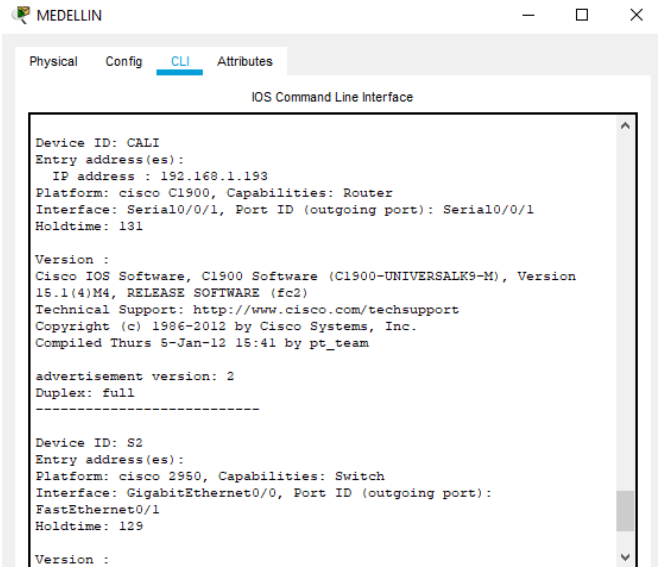




Medellín

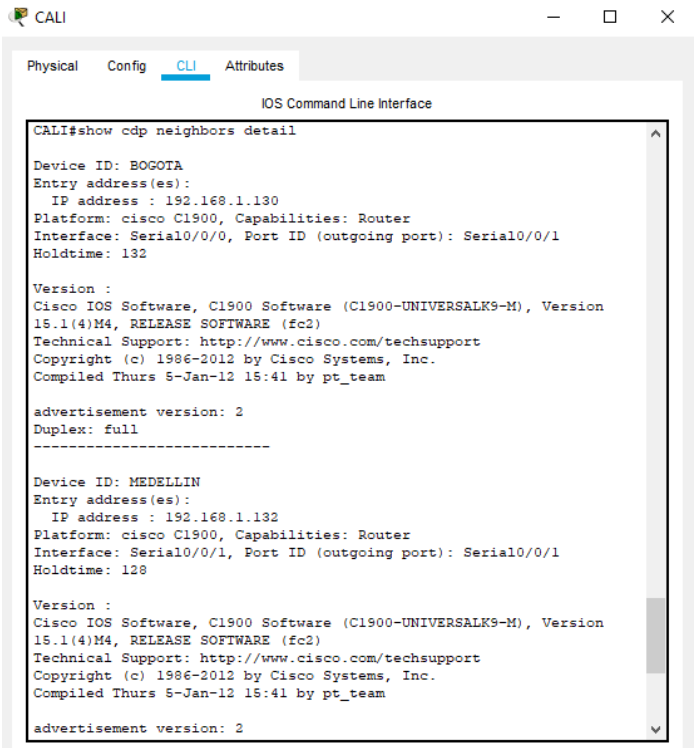
MEDELLIN# show cdp neighbors detail



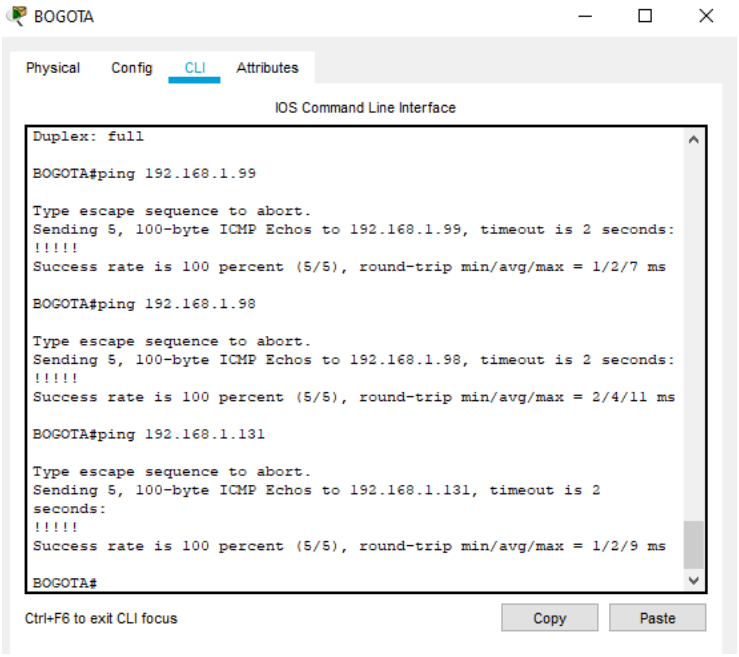


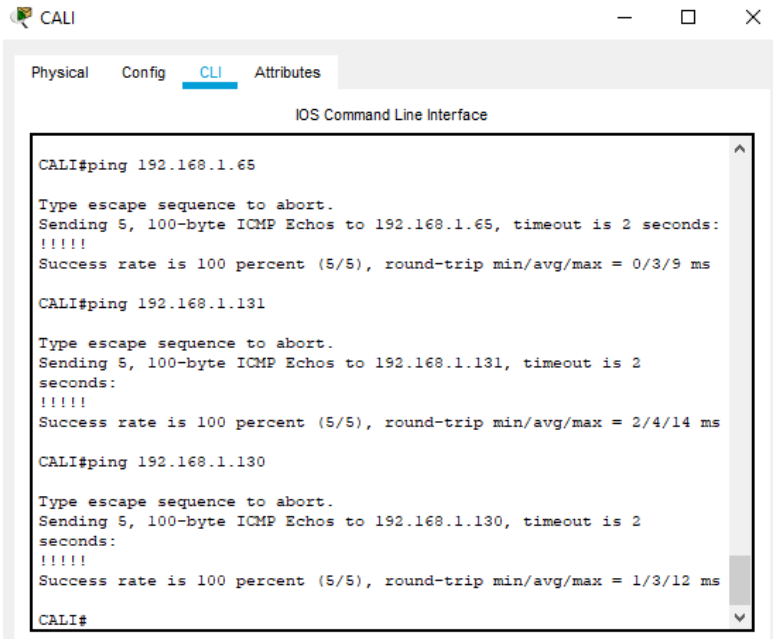
Cali

CALI# show cdp neighbors detail



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





Parte 3: Configuración de Enrutamiento.

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

Bogotá

```
BOGOTA#config t
BOGOTA(config) # router eigrp 200
BOGOTA(config-router) #network 192.168.1.33 0.0.0.0
BOGOTA(config-router) #network 192.168.1.65 0.0.0.0
BOGOTA(config-router) #network 192.168.1.1 0.0.0.0
BOGOTA(config-router) #network 192.168.1.130 0.0.0.0
BOGOTA(config-router) #network 192.168.1.131 0.0.0.0
BOGOTA(config-router) #network 192.168.1.132 0.0.0.0
BOGOTA(config-router) #network 192.168.1.133 0.0.0.0
BOGOTA(config-router) #network 192.168.1.98 0.0.0.0
BOGOTA(config-router) #network 192.168.1.99 0.0.0.0
BOGOTA(config-router) #no auto-summary
BOGOTA(config-router) #end
%SYS-5-CONFIG_I: Configured from console by console
```

Medellín

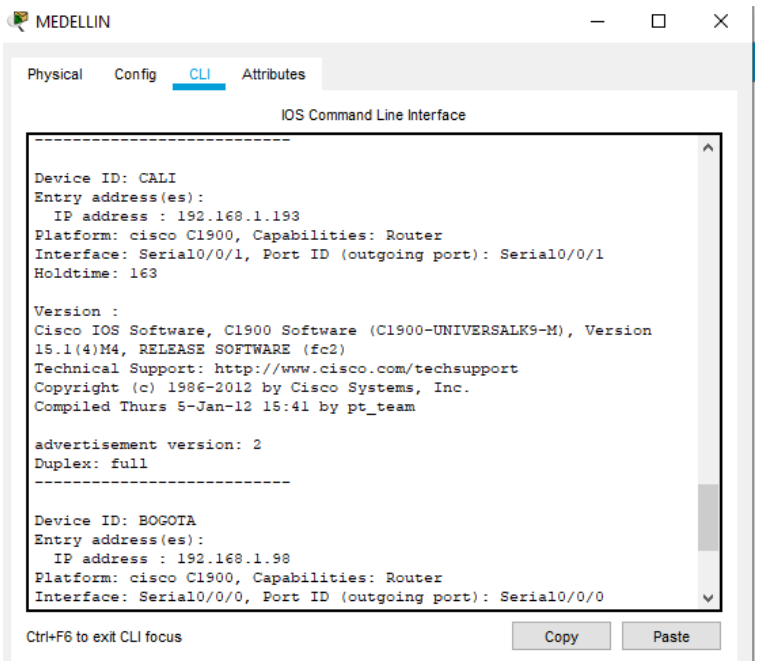
```
MEDELLIN#config t
MEDELLIN(config) # router eigrp 200
MEDELLIN(config-router) #network 192.168.1.1 0.0.0.0
MEDELLIN(config-router) #network 192.168.1.65 0.0.0.0
MEDELLIN(config-router) #network 192.168.1.130 0.0.0.0
MEDELLIN(config-router) #network 192.168.1.131 0.0.0.0
MEDELLIN(config-router) #network 192.168.1.132 0.0.0.0
MEDELLIN(config-router) #network 192.168.1.133 0.0.0.0
MEDELLIN(config-router) #network 192.168.1.193 0.0.0.0
MEDELLIN(config-router) #network 192.168.1.98 0.0.0.0
MEDELLIN(config-router) #network 192.168.1.99 0.0.0.0
MEDELLIN(config-router) #no auto-summary
MEDELLIN(config-router) #end
%SYS-5-CONFIG_I: Configured from console by console
```

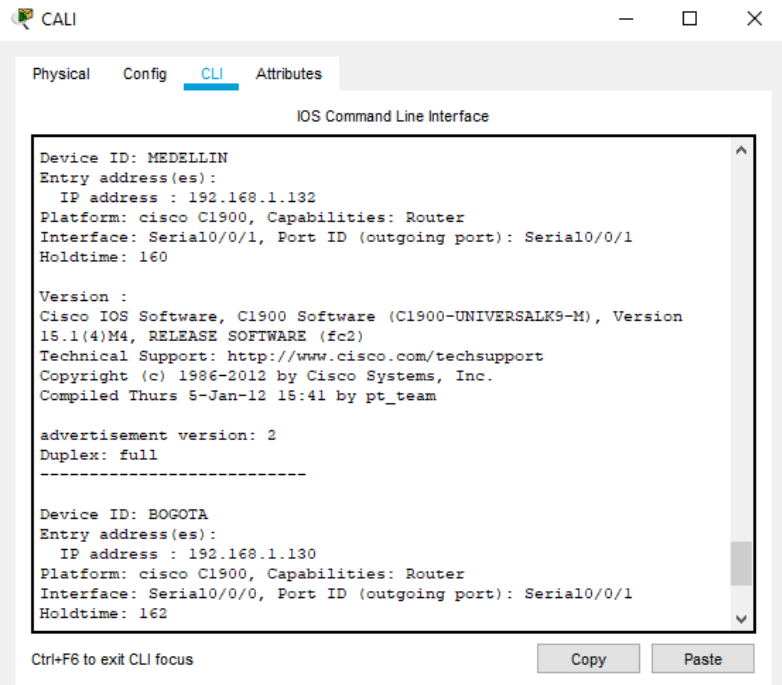
Cali

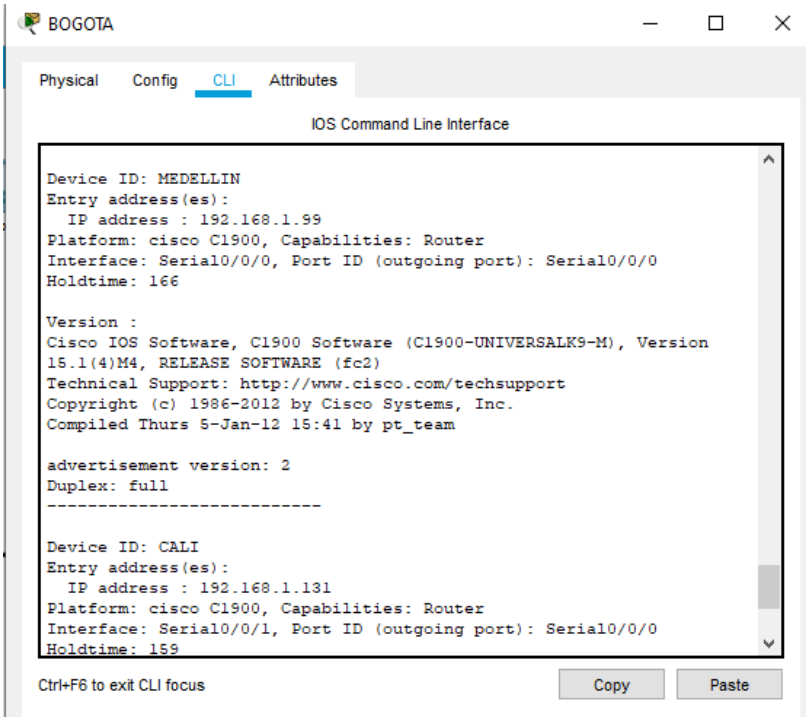
```
CALI#config t
CALI(config) # router eigrp 200
CALI(config-router) #network 192.168.1.130 0.0.0.0
CALI(config-router) #network 192.168.1.131 0.0.0.0
CALI(config-router) #network 192.168.1.132 0.0.0.0
CALI(config-router) #network 192.168.1.133 0.0.0.0
CALI(config-router) #network 192.168.1.1 0.0.0.0
CALI(config-router) #network 192.168.1.65 0.0.0.0
CALI(config-router) #network 192.168.1.193 0.0.0.0
CALI(config-router) #network 192.168.1.98 0.0.0.0
CALI(config-router) #network 192.168.1.99 0.0.0.0
CALI(config-router) #no auto-summary
CALI(config-router) #end
%SYS-5-CONFIG_I: Configured from console by console
```

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

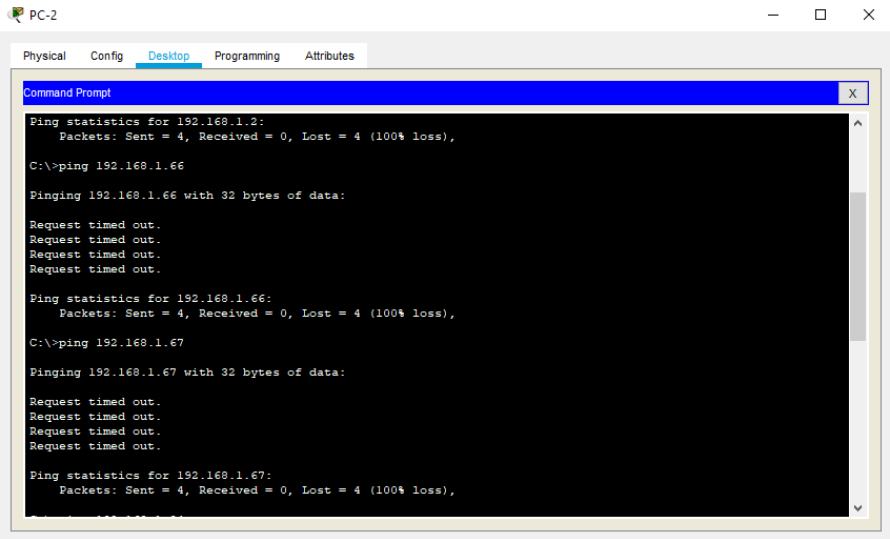
Show cdp neighbors detail

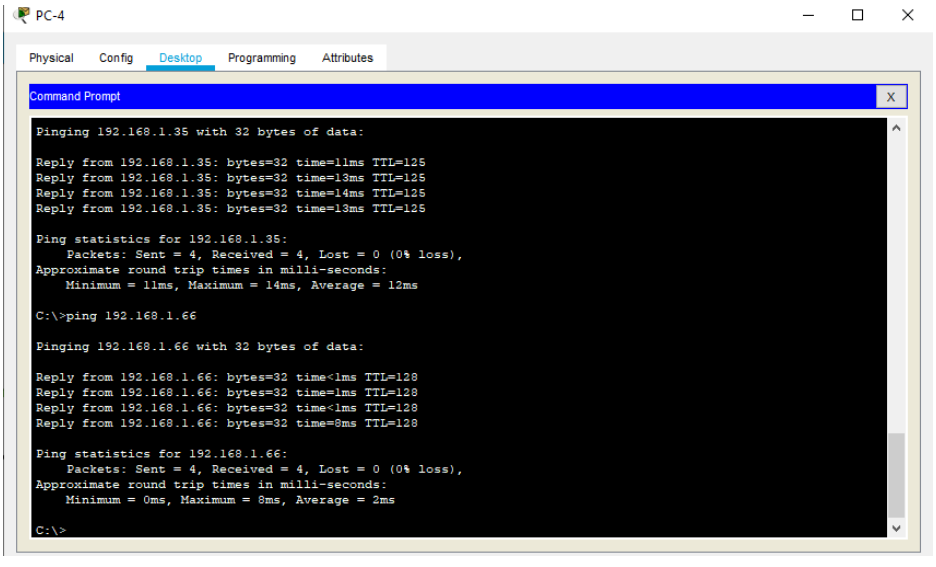


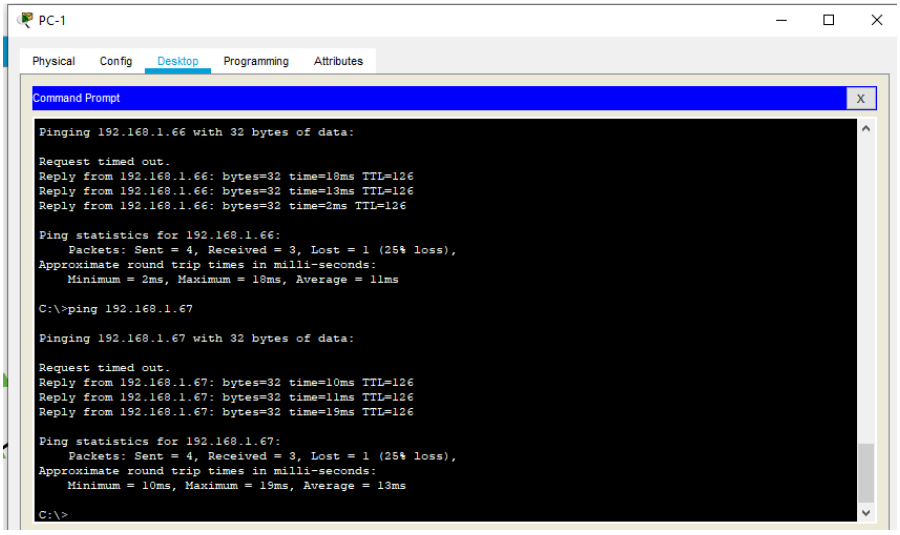

CALI
Physical
Config
CLI
Attributes
IOS Command Line Interface
Device ID: MEDELLIN
Entry address(es):
IP address : 192.168.1.132
Platform: cisco C1900, Capabilities: Router
Interface: Serial0/0/1, Port ID (outgoing port): Serial0/0/1
Holdtime: 160
Version :
Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version
15.1(4)M4, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Thurs 5-Jan-12 15:41 by pt_team
advertisement version: 2
Duplex: full
Device ID: BOGOTA
Entry address(es):
IP address : 192.168.1.130
Platform: cisco C1900, Capabilities: Router
Interface: Serial0/0/0, Port ID (outgoing port): Serial0/0/1
Holdtime: 162
Ctrl+F6 to exit CLI focus
Copy
Paste


BOGOTA
Physical
Config
CLI
Attributes
IOS Command Line Interface
Device ID: MEDELLIN
Entry address(es):
IP address : 192.168.1.99
Platform: cisco C1900, Capabilities: Router
Interface: Serial0/0/0, Port ID (outgoing port): Serial0/0/0
Holdtime: 166
Version :
Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version
15.1(4)M4, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Thurs 5-Jan-12 15:41 by pt_team
advertisement version: 2
Duplex: full
Device ID: CALI
Entry address(es):
IP address : 192.168.1.131
Platform: cisco C1900, Capabilities: Router
Interface: Serial0/0/1, Port ID (outgoing port): Serial0/0/0
Holdtime: 159
Ctrl+F6 to exit CLI focus
Copy
Paste

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







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.

Bogotá a ruoter Medellín

BOGOTA>enable
Password:
BOGOTA# telnet 192.168.1.33
Trying 192.168.1.33 ...Open Unauthorized Access is Prohibited
User Access Verification
Password:
MEDELLIN>

Bogotá a router Cali

BOGOTA#telnet 192.168.1.65
Trying 192.168.1.65 ...Open Unauthorized Access is Prohibited
User Access Verification
Password:
CALI>

Medellín a router Bogotá

MEDELLIN>enable
Password:
MEDELLIN#telnet 192.168.1.1
Trying 192.168.1.1 ...Open Unauthorized Access is Prohibited
User Access Verification
Password:

Medellín a ruoter Cali

MEDELLIN#telnet 192.168.1.65
Trying 192.168.1.65 ...Open Unauthorized Access is Prohibited
User Access Verification
Password:
CALI>
Cali a Ruoter Bogotá

CALI>enable
Password:
CALI#telnet 192.168.1.1
Trying 192.168.1.1 ...Open Unauthorized Access is Prohibited
User Access Verification
Password:
BOGOTA>

Cali a ruoter Medellín

CALI#telnet 192.168.1.33
Trying 192.168.1.33 ...Open Unauthorized Access is Prohibited
User Access Verification
Password:
MEDELLIN>

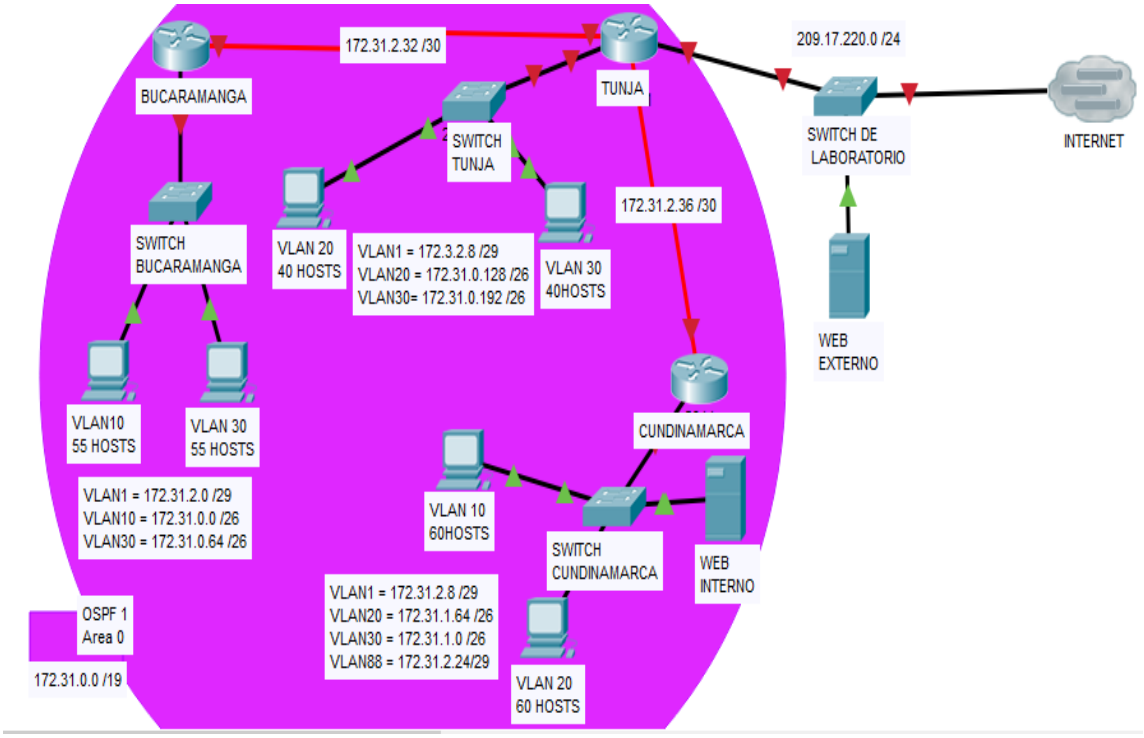
Parte 5: Comprobación de la red instalada.

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

	ORIGEN	DESTINO	RESULTADO
TELNET	Router MEDELLIN	Router CALI	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	OK
	LAN del Router MEDELLIN	WS_1	OK
	LAN del Router MEDELLIN	LAN del Router CALI	OK
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.



Desarrollo

Los siguientes son los requerimientos necesarios:

1. Todos los routers deberán tener los siguiente:
   - Configuración básica.
   - Autenticación local con AAA.
   - Cifrado de contraseñas.
   - Un máximo de internos para acceder al router.
   - Máximo tiempo de acceso al detectar ataques.

Router Tunja

```
Router>en
Router#conf term
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname TUNJA
TUNJA(config)#no ip domain-lookup
TUNJA(config)#enable secret class
TUNJA(config)#line con 0
TUNJA(config-line)#password cisco
TUNJA(config-line)#login
TUNJA(config-line)#logging synchronous
TUNJA(config-line)#line vty 0 15
TUNJA(config-line)#password cisco
TUNJA(config-line)#login
TUNJA(config-line)#logging synchronous
TUNJA(config-line)#username jorge secret cisco
TUNJA(config-line)#login block-for 5 attempts 4 within 60
TUNJA(config)#aaa new-model
TUNJA(config)#aaa authentication login AUTH local
TUNJA(config)#line con 0
TUNJA(config-line)#login authentication AUTH
TUNJA(config-line)#line vty 0 15
TUNJA(config-line)#login authentication AUTH
TUNJA(config)#service password-encryption
TUNJA(config)#banner motd # Unathorized Access is Prohibited #
TUNJA(config)#int f0/0.1
TUNJA(config-subif)#encapsulation dot1q 1
TUNJA(config-subif)#ip address 172.3.2.9 255.255.255.248
TUNJA(config-subif)#int f0/0.20
TUNJA(config-subif)#encapsulation dot1q 20
TUNJA(config-subif)#ip address 172.31.0.129 255.255.255.192
TUNJA(config-subif)#int f0/0.30
TUNJA(config-subif)#encapsulation dot1q 30
TUNJA(config-subif)#ip address 172.31.0.193 255.255.255.192
TUNJA(config-subif)#int f0/0
TUNJA(config-if)#no shut
TUNJA(config-if)#
TUNJA(config-if)#int s0/0/0
TUNJA(config-if)#ip address 172.31.2.33 255.255.255.252
```

```
TUNJA(config-if)#no shut

TUNJA(config-if)#
TUNJA(config-if)#int s0/0/1
TUNJA(config-if)#ip address 172.31.2.37 255.255.255.252
TUNJA(config-if)#no shut
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
TUNJA(config-if)#int f0/1
TUNJA(config-if)#ip address 209.165.220.1 255.255.255.0
TUNJA(config-if)#no shut
TUNJA(config-if)#
TUNJA(config-if)#router ospf 1
TUNJA(config-router)#network 172.3.2.8 0.0.0.7 area 0
TUNJA(config-router)#network 172.31.0.128 0.0.0.63 area 0
TUNJA(config-router)#network 172.31.0.192 0.0.0.63 area 0
TUNJA(config-router)#network 172.31.2.32 0.0.0.3 area 0
TUNJA(config-router)#network 172.31.2.36 0.0.0.3 area 0
TUNJA(config-router)#end
TUNJA#
%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 Serial0/0/0, changed state to up
```

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

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

%SYS-5-CONFIG_I: Configured from console by console

Router Bucaramanga

```
Router>en
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname BUCARAMANGA
BUCARAMANGA(config)#no ip domain-lookup
BUCARAMANGA(config)#enable secret class
BUCARAMANGA(config)#line con 0
BUCARAMANGA(config-line)#password cisco
BUCARAMANGA(config-line)#login
BUCARAMANGA(config-line)#logging synchronous
BUCARAMANGA(config-line)#line vty 0 15
BUCARAMANGA(config-line)#password cisco
BUCARAMANGA(config-line)#login
BUCARAMANGA(config-line)#logging synchronous
BUCARAMANGA(config-line)#username jorge secret cisco
BUCARAMANGA(config-line)#login block-for 5 attempts 4 within 60
BUCARAMANGA(config)#aaa new-model
BUCARAMANGA(config)#aaa authentication login AUTH local
BUCARAMANGA(config)#line con 0
BUCARAMANGA(config-line)#login authentication AUTH
BUCARAMANGA(config-line)#line vty 0 15
BUCARAMANGA(config-line)#login authentication AUTH
BUCARAMANGA(config)#service password-encryption
BUCARAMANGA(config)#banner motd # Unauthorized Access is Prohibited #
BUCARAMANGA(config)#int f0/0.1
BUCARAMANGA(config-subif)#encapsulation dot1q 1
BUCARAMANGA(config-subif)#ip address 172.31.2.1 255.255.255.248
BUCARAMANGA(config-subif)#int f0/0.10
BUCARAMANGA(config-subif)#encapsulation dot1q 10
BUCARAMANGA(config-subif)#ip address 172.31.0.1 255.255.255.192
```

```
BUCARAMANGA(config-subif)#int f0/0.30
BUCARAMANGA(config-subif)#encapsulation dot1q 30
BUCARAMANGA(config-subif)#ip address 172.31.0.65 255.255.255.192
BUCARAMANGA(config-subif)#int f0/0
BUCARAMANGA(config-if)#no shut
BUCARAMANGA(config-if)#int s0/0/0
BUCARAMANGA(config-if)#ip address 172.31.2.34 255.255.255.252
BUCARAMANGA(config-if)#no shut
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
BUCARAMANGA(config-if)#router ospf 1
BUCARAMANGA(config-router)#network 172.31.0.0 0.0.0.63 area 0
BUCARAMANGA(config-router)#network 172.31.0.64 0.0.0.63 area 0
BUCARAMANGA(config-router)#network 172.31.2.0 0.0.0.7 area 0
BUCARAMANGA(config-router)#network 172.31.2.32 0.0.0.3 area 0
BUCARAMANGA(config-router)#end
BUCARAMANGA#
%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

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

Router Cundinamarca

```
Router>en
Router#conf term
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname CUNDINAMARCA
CUNDINAMARCA(config)#no ip domain-lookup
CUNDINAMARCA(config)#enable secret class
CUNDINAMARCA(config)#line con 0
CUNDINAMARCA(config-line)#password cisco
CUNDINAMARCA(config-line)#login
CUNDINAMARCA(config-line)#logging synchronous
CUNDINAMARCA(config-line)#line vty 0 15
CUNDINAMARCA(config-line)#password cisco
CUNDINAMARCA(config-line)#login
CUNDINAMARCA(config-line)#logging synchronous
CUNDINAMARCA(config-line)#username jorge secret cisco
CUNDINAMARCA(config-line)#login block-for 5 attempts 4 within 60
CUNDINAMARCA(config)#aaa new-model
CUNDINAMARCA(config)#aaa authentication login AUTH local
CUNDINAMARCA(config)#line con 0
CUNDINAMARCA(config-line)#login authentication AUTH
CUNDINAMARCA(config-line)#line vty 0 15
CUNDINAMARCA(config-line)#login authentication AUTH
CUNDINAMARCA(config)#service password-encryption
CUNDINAMARCA(config)#banner motd # Unauthorized Access is Prohibited #
CUNDINAMARCA(config)#int f0/0.1
CUNDINAMARCA(config-subif)#encapsulation dot1q 1
CUNDINAMARCA(config-subif)#ip address 172.31.2.9 255.255.255.248
CUNDINAMARCA(config-subif)#int f0/0.20
CUNDINAMARCA(config-subif)#encapsulation dot1q 20
CUNDINAMARCA(config-subif)#ip address 172.31.1.65 255.255.255.192
CUNDINAMARCA(config-subif)#int f0/0.30
CUNDINAMARCA(config-subif)#encapsulation dot1q 30
CUNDINAMARCA(config-subif)#ip address 172.31.1.1 255.255.255.192
CUNDINAMARCA(config-subif)#int f0/0.88
CUNDINAMARCA(config-subif)#encapsulation dot1q 88
CUNDINAMARCA(config-subif)#ip address 172.31.2.25 255.255.255.248
CUNDINAMARCA(config-subif)#int f0/0
CUNDINAMARCA(config-if)#no shut
```

```
CUNDINAMARCA(config-if)#
CUNDINAMARCA(config-if)#int s0/0/0
CUNDINAMARCA(config-if)#ip address 172.31.2.38 255.255.255.252
CUNDINAMARCA(config-if)#no shut
CUNDINAMARCA(config-if)#router ospf 1
CUNDINAMARCA(config-router)#network 172.31.1.0 0.0.0.63 area 0
CUNDINAMARCA(config-router)#network 172.31.1.64 0.0.0.63 area 0
CUNDINAMARCA(config-router)#network 172.31.2.8 0.0.0.7 area 0
CUNDINAMARCA(config-router)#network 172.31.2.24 0.0.0.7 area 0
CUNDINAMARCA(config-router)#network 172.31.2.36 0.0.0.3 area 0
CUNDINAMARCA(config-router)#end
CUNDINAMARCA#
%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

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

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

CUNDINAMARCA#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

CUNDINAMARCA#
00:14:55: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.220.1 on Serial0/0/0 from LOADING to FULL, Loading Done

Switch laboratorio

Switch>enable
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SW-LABORATORIO
SW-LABORATORIO(config)#no ip domain-lookup
SW-LABORATORIO(config)#enable secret class
SW-LABORATORIO(config)#line con 0
SW-LABORATORIO(config-line)#password cisco
SW-LABORATORIO(config-line)#login
SW-LABORATORIO(config-line)#exit
SW-LABORATORIO(config)#service password-encryption
SW-LABORATORIO(config)#banner motd # Unauthorized Access is Prohibited #
SW-LABORATORIO(config)#exit
SW-LABORATORIO#
%SYS-5-CONFIG_I: Configured from console by console
SW-LABORATORIO#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
SW-LABORATORIO#

Switch Tunja

Switch>enable
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SW-TUNJA
SW-TUNJA(config)#no ip domain-lookup
SW-TUNJA(config)#enable secret class
SW-TUNJA(config)#line con 0

```
SW-TUNJA(config-line)#password cisco
SW-TUNJA(config-line)#login
SW-TUNJA(config-line)#exit
SW-TUNJA(config)#service password-encryption
SW-TUNJA(config)#banner motd # Unauthorized Access is prohibited #
SW-TUNJA(config)#exit
SW-TUNJA#
%SYS-5-CONFIG_I: Configured from console by console
SW-TUNJA#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
SW-TUNJA# config t
SW-TUNJA(config)#vlan 1
SW-TUNJA(config-vlan)#vlan 20
SW-TUNJA(config-vlan)#vlan 30
SW-TUNJA(config-vlan)#int f0/20
SW-TUNJA(config-if)#switchport mode access
SW-TUNJA(config-if)#switchport access vlan 20
SW-TUNJA(config-if)#int f0/24
SW-TUNJA(config-if)#switchport mode access
SW-TUNJA(config-if)#switchport access vlan 30
SW-TUNJA(config-if)#int f0/1
SW-TUNJA(config-if)#switchport mode trunk
SW-TUNJA(config-if)#
SW-TUNJA(config-if)#int vlan 1
SW-TUNJA(config-if)#ip address 172.3.2.11 255.255.255.248
SW-TUNJA(config-if)#no shut
SW-TUNJA(config-if)#
SW-TUNJAconfig-if)#ip default-gateway 172.3.2.9
SW-TUNJA(config)#
SW-TUNJA(config)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to
down
```

Switch Bucaramanga

```
Switch>enable
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SW-BUCARAMANGA
SW-BUCARAMANGA(config)#no ip domain-lookup
SW-BUCARAMANGA(config)#enable secret class
SW-BUCARAMANGA(config)#line con 0
SW-BUCARAMANGA(config-line)#password cisco
SW-BUCARAMANGA(config-line)#login
SW-BUCARAMANGA(config-line)#exit
SW-BUCARAMANGA(config)#service password-encryption
SW-BUCARAMANGA(config)#banner motd # Unauthorized Access is Prohibited #
SW-BUCARAMANGA(config)#exit
SW-BUCARAMANGA#
%SYS-5-CONFIG_I: Configured from console by console
SW-BUCARAMANGA#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
SW-BUCARAMANGA#config t
SW-BUCARAMANGA(config)#vlan 1
SW-BUCARAMANGA(config-vlan)#vlan 10
SW-BUCARAMANGA(config-vlan)#vlan 30
SW-BUCARAMANGA(config-vlan)#int f0/20
SW-BUCARAMANGA(config-if)#switchport mode access
SW-BUCARAMANGA(config-if)#switchport access vlan 10
SW-BUCARAMANGA(config-if)#int f0/24
SW-BUCARAMANGA (config-if)#switchport mode access
SW-BUCARAMANGA (config-if)#switchport access vlan 30
SW-BUCARAMANGA(config-if)#int f0/1
SW-BUCARAMANGA(config-if)#switchport mode trunk
SW-BUCARAMANGA(config-if)#int vlan 1
SW-BUCARAMANGA(config-if)#ip address 172.31.2.3 255.255.255.248
SW-BUCARAMANGA(config-if)#no shut
SW-BUCARAMANGA(config-if)#ip default-gateway 172.31.2.1
SW-BUCARAMANGA(config)#
SW-BUCARAMANGA(config)#
%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

%LINK-5-CHANGED: Interface Vlan1, changed state to up

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

Switch Cundinamarca

```
Switch>enable
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SW-CUNDINAMARCA
SW-CUNDINAMARCA(config)#no ip domain-lookup
SW-CUNDINAMARCA(config)#enable secret class
SW-CUNDINAMARCA(config)#line con 0
SW-CUNDINAMARCA(config-line)#password cisco
SW-CUNDINAMARCA(config-line)#login
SW-CUNDINAMARCA(config-line)#exit
SW-CUNDINAMARCA(config)#service password-encryption
SW-CUNDINAMARCA(config)#banner motd # Unauthorized Access is Prohibited #
SW-CUNDINAMARCA(config)#exit
SW-CUNDINAMARCA#
%SYS-5-CONFIG_I: Configured from console by console
SW-CUNDINAMARCA#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
SW-CUNDINAMARCA#
SW-CUNDINAMARCA(config)#vlan 1
SW-CUNDINAMARCA(config-vlan)#vlan 20
SW-CUNDINAMARCA(config-vlan)#vlan 30
SW-CUNDINAMARCA(config-vlan)#vlan 88
SW-CUNDINAMARCA(config-vlan)#exit
SW-CUNDINAMARCA(config)#int f0/20
SW-CUNDINAMARCA(config-if)#switchport mode access
SW-CUNDINAMARCA(config-if)#switchport access vlan 20
SW-CUNDINAMARCA(config-if)#int f0/24
SW-CUNDINAMARCA(config-if)#switchport mode access
```

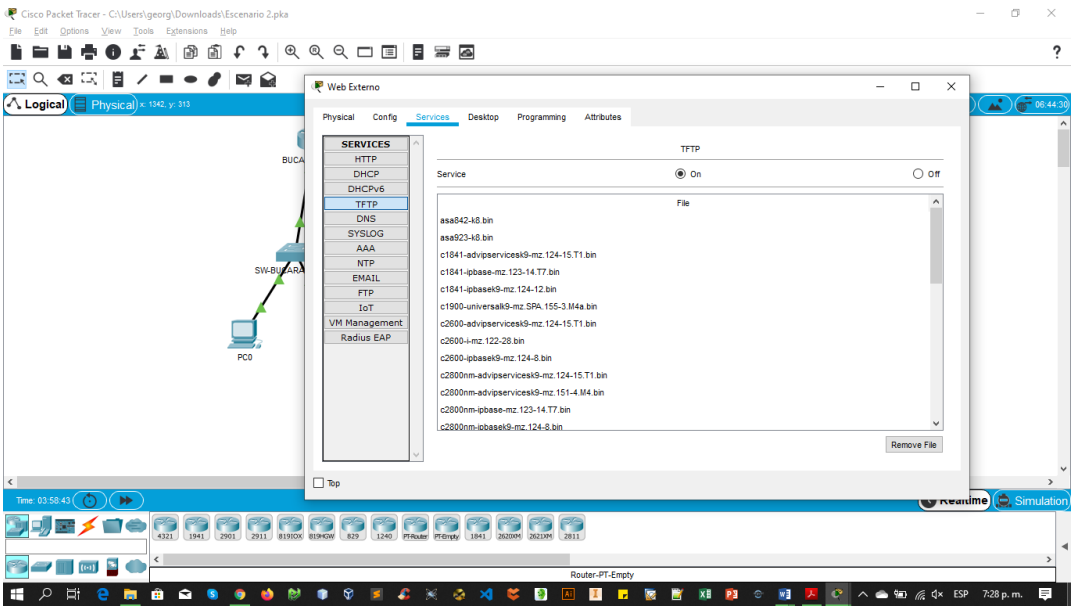
```
SW-CUNDINAMARCA(config-if)#switchport access vlan 30
SW-CUNDINAMARCA(config-if)#int f0/10
SW-CUNDINAMARCA(config-if)#switchport mode access
SW-CUNDINAMARCA(config-if)#switchport access vlan 88
SW-CUNDINAMARCA(config-if)#int f0/1
SW-CUNDINAMARCA(config-if)#switchport mode trunk
SW-CUNDINAMARCA(config-if)#
SW-CUNDINAMARCA(config-if)#int vlan 1
SW-CUNDINAMARCA(config-if)#ip address 172.31.2.11 255.255.255.248
SW-CUNDINAMARCA(config-if)#no shutdown
SW-CUNDINAMARCA(config-if)#
SW-CUNDINAMARCA(config-if)#ip default-gateway 172.31.2.9
SW-CUNDINAMARCA(config)#
SW-CUNDINAMARCA(config)#
%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

%LINK-5-CHANGED: Interface Vlan1, changed state to up

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

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



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

```
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 172.31.1.65
TUNJA(config)#ip dhcp excluded-address 172.31.1.1
TUNJA(config)#ip dhcp pool V10B
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 172.31.2.28
TUNJA(dhcp-config)#ip dhcp pool V30B
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 172.31.2.28
TUNJA(dhcp-config)#ip dhcp pool V20C
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 172.31.2.28
TUNJA(dhcp-config)#ip dhcp pool V30C
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 172.31.2.28
```

```
TUNJA(dhcp-config)#
CUNDINAMARCA(config)#int f0/0.20
CUNDINAMARCA(config-subif)#ip helper-address 172.31.2.37
CUNDINAMARCA(config-subif)#int f0/0.30
CUNDINAMARCA(config-subif)#ip helper-address 172.31.2.37
CUNDINAMARCA(config-subif)#end
CUNDINAMARCA#
%SYS-5-CONFIG_I: Configured from console by console


BUCARAMANGA(config)#int f0/0.10
BUCARAMANGA(config-subif)#ip helper-address 172.31.2.33
BUCARAMANGA(config-subif)#int f0/0.30
BUCARAMANGA(config-subif)#ip helper-address 172.31.2.33
BUCARAMANGA(config-subif)#end
BUCARAMANGA#
BUCARAMANGA#
%SYS-5-CONFIG_I: Configured from console by console
```

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

```
TUNJA(dhcp-config)#ip nat inside source static 172.31.2.28 209.165.220.4
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 s0/0/0
TUNJA(config-if)#ip nat inside
TUNJA(config-if)#int s0/0/1
TUNJA(config-if)#ip nat inside
TUNJA(config-if)#exit
TUNJA(config)#ip route 0.0.0.0 0.0.0.0 209.165.220.3
TUNJA(config)#router ospf 1
TUNJA(config-router)#default-information originate
```

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

Gateway of last resort is 209.165.220.3 to network 0.0.0.0

172.3.0.0/29 is subnetted, 1 subnets
C 172.3.2.8 is directly connected, FastEthernet0/0.1
172.31.0.0/16 is variably subnetted, 11 subnets, 3 masks
O 172.31.0.0/26 [110/65] via 172.31.2.34, 00:24:49, Serial0/0/0
O 172.31.0.64/26 [110/65] via 172.31.2.34, 00:24:49, Serial0/0/0
C 172.31.0.128/26 is directly connected, FastEthernet0/0.20
C 172.31.0.192/26 is directly connected, FastEthernet0/0.30
O 172.31.1.0/26 [110/65] via 172.31.2.38, 00:23:33, Serial0/0/1
O 172.31.1.64/26 [110/65] via 172.31.2.38, 00:23:33, Serial0/0/1
O 172.31.2.0/29 [110/65] via 172.31.2.34, 00:24:49, Serial0/0/0
O 172.31.2.8/29 [110/65] via 172.31.2.38, 00:23:33, Serial0/0/1
O 172.31.2.24/29 [110/65] via 172.31.2.38, 00:23:33, Serial0/0/1
C 172.31.2.32/30 is directly connected, Serial0/0/0
C 172.31.2.36/30 is directly connected, Serial0/0/1
C 209.165.220.0/24 is directly connected, FastEthernet0/1
S* 0.0.0.0/0 [1/0] via 209.165.220.3

TUNJA#show ip nat translation
Pro Inside global Inside local Outside local Outside global
icmp 209.165.220.1:1 172.31.1.2:1 209.165.220.3:1 209.165.220.3:1
icmp 209.165.220.1:2 172.31.1.2:2 209.165.220.3:2 209.165.220.3:2
icmp 209.165.220.1:3 172.31.1.2:3 209.165.220.3:3 209.165.220.3:3
icmp 209.165.220.1:4 172.31.1.2:4 209.165.220.3:4 209.165.220.3:4
--- 209.165.220.4 172.31.2.28 --- ---


BUCARAMANGA#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
```

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is 172.31.2.33 to network 0.0.0.0

172.3.0.0/29 is subnetted, 1 subnets
O 172.3.2.8 [110/65] via 172.31.2.33, 00:25:08, Serial0/0/0
172.31.0.0/16 is variably subnetted, 11 subnets, 3 masks
C 172.31.0.0/26 is directly connected, FastEthernet0/0.10
C 172.31.0.64/26 is directly connected, FastEthernet0/0.30
O 172.31.0.128/26 [110/65] via 172.31.2.33, 00:25:08, Serial0/0/0
O 172.31.0.192/26 [110/65] via 172.31.2.33, 00:25:08, Serial0/0/0
O 172.31.1.0/26 [110/129] via 172.31.2.33, 00:23:42, Serial0/0/0
O 172.31.1.64/26 [110/129] via 172.31.2.33, 00:23:42, Serial0/0/0
C 172.31.2.0/29 is directly connected, FastEthernet0/0.1
O 172.31.2.8/29 [110/129] via 172.31.2.33, 00:23:42, Serial0/0/0
O 172.31.2.24/29 [110/129] via 172.31.2.33, 00:23:42, Serial0/0/0
C 172.31.2.32/30 is directly connected, Serial0/0/0
O 172.31.2.36/30 [110/128] via 172.31.2.33, 00:24:02, Serial0/0/0
O*E2 0.0.0.0/0 [110/1] via 172.31.2.33, 00:02:01, Serial0/0/0

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

Gateway of last resort is 172.31.2.37 to network 0.0.0.0

172.3.0.0/29 is subnetted, 1 subnets
O 172.3.2.8 [110/65] via 172.31.2.37, 00:24:15, Serial0/0/0
172.31.0.0/16 is variably subnetted, 11 subnets, 3 masks
O 172.31.0.0/26 [110/129] via 172.31.2.37, 00:24:15, Serial0/0/0
O 172.31.0.64/26 [110/129] via 172.31.2.37, 00:24:15, Serial0/0/0
O 172.31.0.128/26 [110/65] via 172.31.2.37, 00:24:15, Serial0/0/0
O 172.31.0.192/26 [110/65] via 172.31.2.37, 00:24:15, Serial0/0/0
C 172.31.1.0/26 is directly connected, FastEthernet0/0.30
C 172.31.1.64/26 is directly connected, FastEthernet0/0.20

O 172.31.2.0/29 [110/129] via 172.31.2.37, 00:24:15, Serial0/0/0
C 172.31.2.8/29 is directly connected, FastEthernet0/0.1
C 172.31.2.24/29 is directly connected, FastEthernet0/0.88
O 172.31.2.32/30 [110/128] via 172.31.2.37, 00:24:15, Serial0/0/0
C 172.31.2.36/30 is directly connected, Serial0/0/0
O*E2 0.0.0.0/0 [110/1] via 172.31.2.37, 00:02:24, Serial0/0/0

4. El enrutamiento deberá tener autenticación.

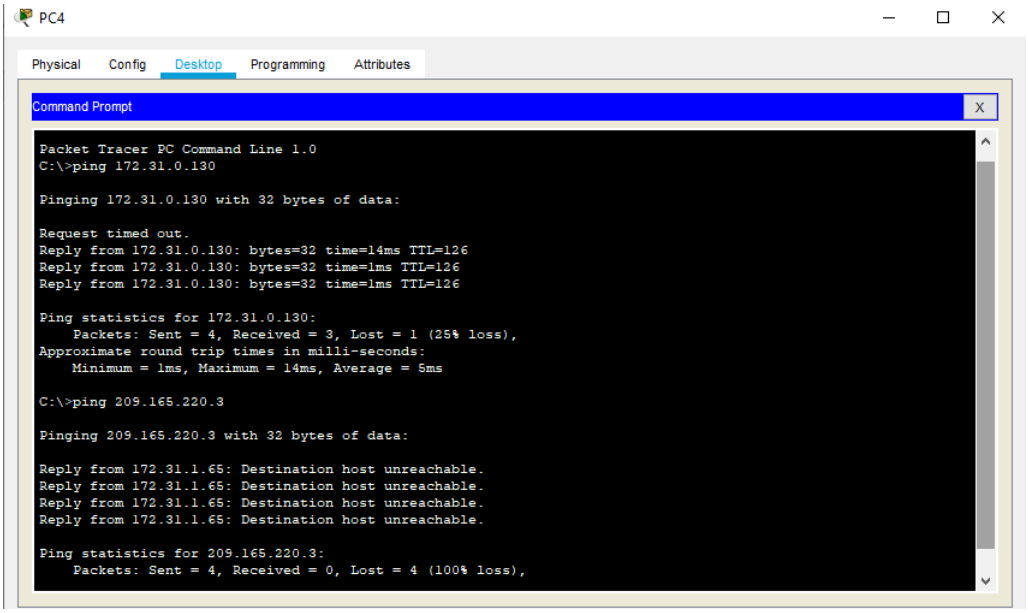
TUNJA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
TUNJA(config)#int s0/0/0
TUNJA(config-if)#ip ospf authentication message-digest
TUNJA(config-if)#ip ospf message-digest-key 1 md5 cisco123
TUNJA(config-if)#int s0/0/1
TUNJA(config-if)#ip ospf authentication message-digest
TUNJA(config-if)#ip ospf message-digest-key 1 md5 cisco123
TUNJA(config-if)#
00:31:40: %OSPF-5-ADJCHG: Process 1, Nbr 172.31.2.34 on Serial0/0/0 from LOADING to FULL, Loading Done
TUNJA(config-if)#
00:31:42: %OSPF-5-ADJCHG: Process 1, Nbr 172.31.2.38 on Serial0/0/1 from LOADING to FULL, Loading Done

BUCARAMANGA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
BUCARAMANGA(config)#int s0/0/0
BUCARAMANGA(config-if)#ip ospf authentication message-digest
BUCARAMANGA(config-if)#ip ospf message-digest-key 1 md5 cisco123
CUNDINAMARCA(config)#int s0/0/0
CUNDINAMARCA(config-if)#ip ospf authentication message-digest
CUNDINAMARCA(config-if)#ip ospf message-digest-key 1 md5 cisco123
CUNDINAMARCA(config-if)#

5. **Listas de control de acceso:**

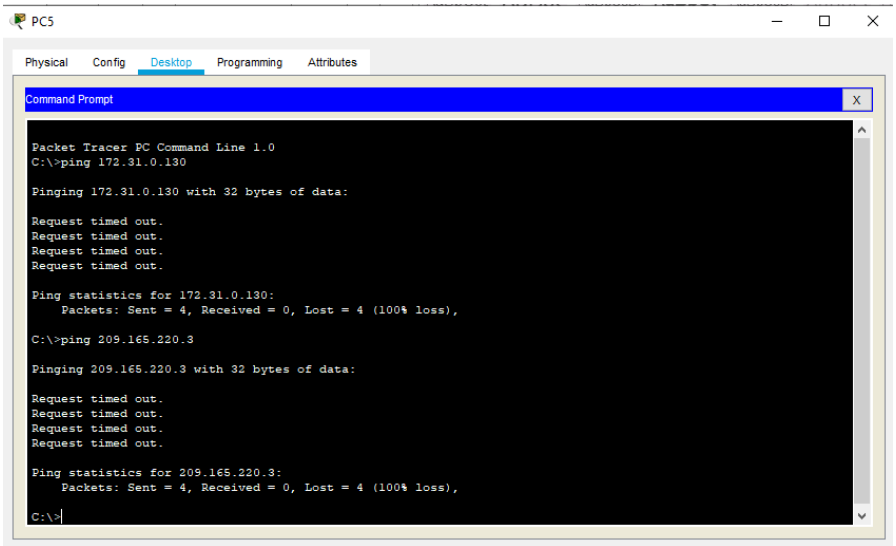
- **Los hosts de VLAN 20 en Cundinamarca no acceden a internet, solo a la red interna de Tunja.**

CUNDINAMARCA(config-if)#access-list 111 deny ip 172.31.1.64 0.0.0.63 209.165.220.0 0.0.0.255
CUNDINAMARCA(config)#access-list 111 permit ip any any
CUNDINAMARCA(config)#int f0/0.20
CUNDINAMARCA(config-subif)#ip access-group 111 in
CUNDINAMARCA(config-subif)#



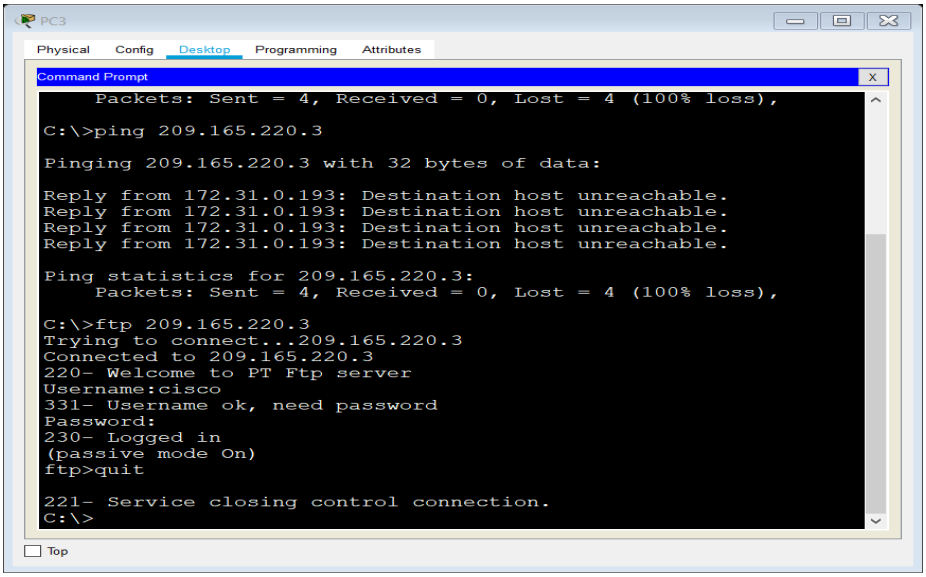
- **Los hosts de VLAN 10 en Cundinamarca si acceden a internet y no a la red interna de Tunja.**

CUNDINAMARCA(config-subif)#access-list 112 permit ip 172.31.1.0 0.0.0.63 209.165.220.0 0.0.0.255
CUNDINAMARCA(config)#access-list 112 deny ip any any
CUNDINAMARCA(config)#int f0/0.30
CUNDINAMARCA(config-subif)#ip access-group 112 in
CUNDINAMARCA(config-subif)#



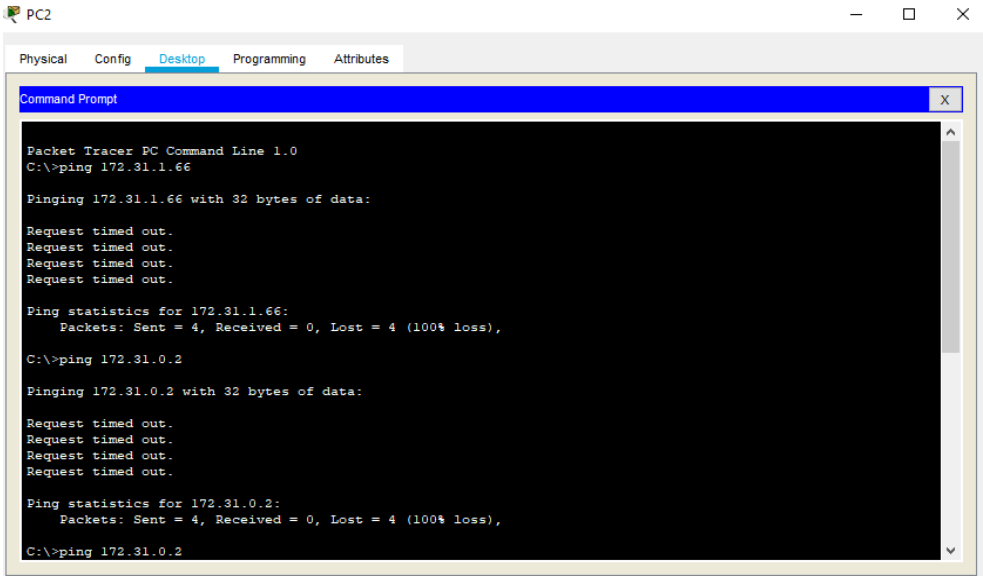
- **Los hosts de VLAN 30 en Tunja solo acceden a servidores web y ftp de internet.**

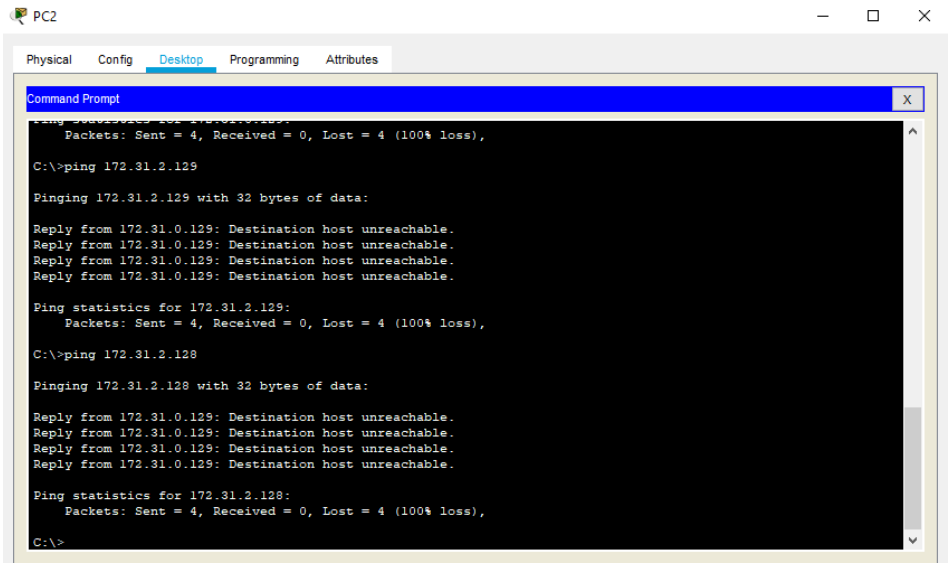
TUNJA(config)#access-list 111 permit tcp 172.31.0.192 0.0.0.63 209.165.220.0 0.0.0.255 eq 80
TUNJA(config)#access-list 111 permit tcp 172.31.0.192 0.0.0.63 209.165.220.0 0.0.0.255 eq 21
TUNJA(config)#access-list 111 permit tcp 172.31.0.192 0.0.0.63 209.165.220.0 0.0.0.255 eq 20
TUNJA(config)#int f0/0.30
TUNJA(config-subif)#ip access-group 111 in
TUNJA(config-subif)#



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

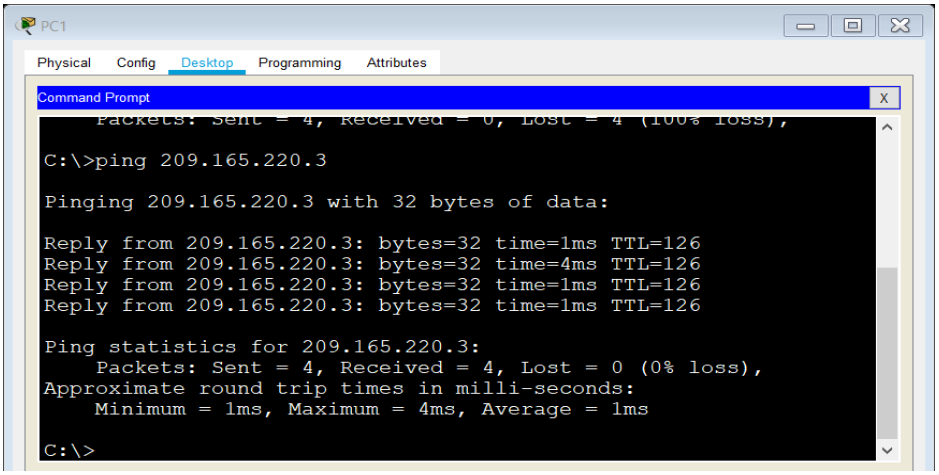
TUNJA(config-subif)#access-list 112 permit ip 172.31.0.128 0.0.0.63 172.31.1.64 0.0.0.63
TUNJA(config)#access-list 112 permit ip 172.31.0.128 0.0.0.63 172.31.0.0 0.0.0.63
TUNJA(config)#int f0/0.20
TUNJA(config-subif)#ip access-group 112 in
TUNJA(config-subif)#





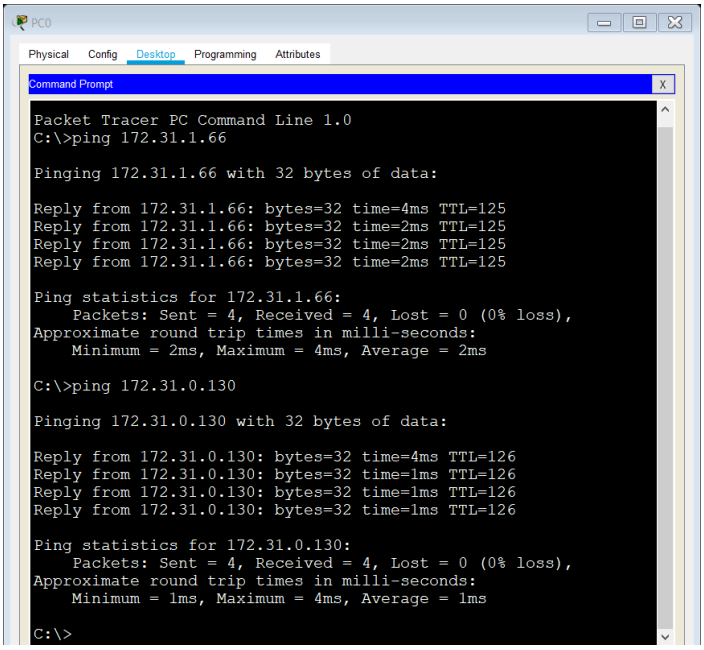
- **Los hosts de VLAN 30 de Bucaramanga acceden a internet y a cualquier equipo de VLAN 10.**

BUCARAMANGA(config)#access-list 111 permit ip 172.31.0.64 0.0.0.63 209.165.220.0 0.0.0.255
BUCARAMANGA(config)#int f0/0.30
BUCARAMANGA(config-subif)
#ip access-group 111 in
BUCARAMANGA(config-subif)#



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

BUCARAMANGA(config-subif)#access-list 112 permit ip 172.31.0.0 0.0.0.63 172.31.1.64 0.0.0.63
BUCARAMANGA(config)#access-list 112 permit ip 172.31.0.0 0.0.0.63 172.31.0.128 0.0.0.63
BUCARAMANGA(config)#int f0/0.10
BUCARAMANGA(config-subif)#ip access-group 112 in
BUCARAMANGA(config-subif)#



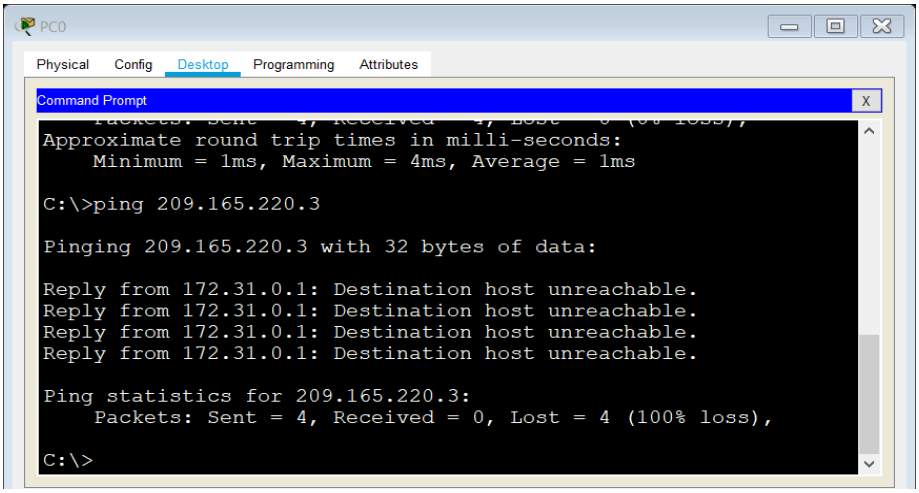
- **Los hosts de una VLAN no pueden acceder a los de otra VLAN en una ciudad.**

  TUNJA(config)#access-list 113 deny ip 172.3.2.8 0.0.0.7 172.31.0.128 0.0.0.63

  TUNJA(config)#access-list 113 deny ip 172.3.0.192 0.0.0.63 172.31.0.128 0.0.0.63
  TUNJA(config)#access-list 113 permit ip any any
  TUNJA(config)#int f0/0.20
  TUNJA(config-subif)#ip access-group 113 out
  TUNJA(config-subif)#

  BUCARAMANGA(config-subif)#access-list 113 deny ip 172.31.2.0 0.0.0.7 172.31.0.0 0.0.0.63
  BUCARAMANGA(config)#access-list 113 deny ip 172.31.0.64 0.0.0.63 172.31.0.0 0.0.0.63
  BUCARAMANGA(config)#access-list 113 permit ip any any
  BUCARAMANGA(config)#int f0/0.10
  BUCARAMANGA(config-subif)#ip access-group 113 out
  BUCARAMANGA(config-subif)#
  CUNDINAMARCA(config)#access-list 113 deny ip 172.31.2.8 0.0.0.7 172.31.1.64 0.0.0.63
  CUNDINAMARCA(config)#access-list 113 deny ip 172.31.1.0 0.0.0.63 172.31.1.64 0.0.0.63
  CUNDINAMARCA(config)#access-list 113 deny ip 172.31.2.24 0.0.0.7 172.31.1.64 0.0.0.63

```
CUNDINAMARCA(config)#access-list 113 permit ip any any
CUNDINAMARCA(config)#int f0/0.20
CUNDINAMARCA(config-subif)#ip access-group 113 out
CUNDINAMARCA(config-subif)#
```

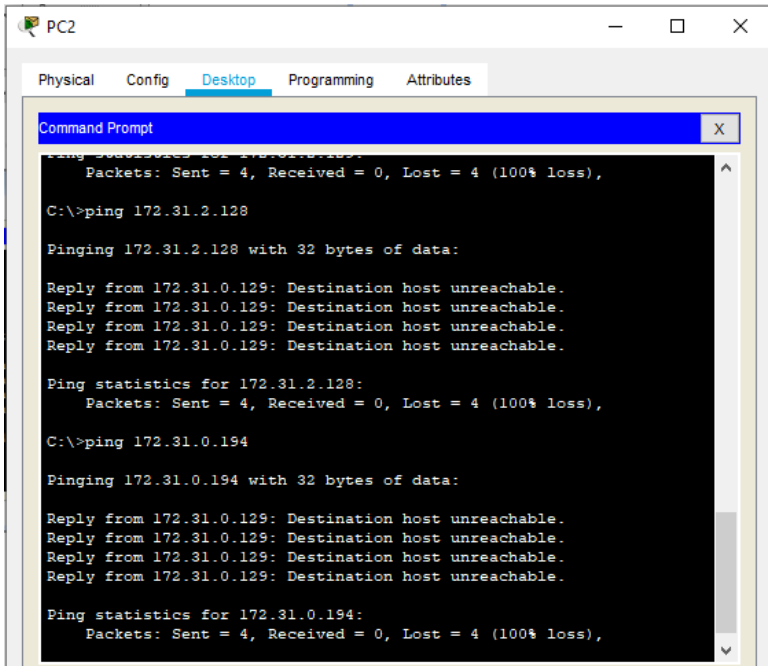


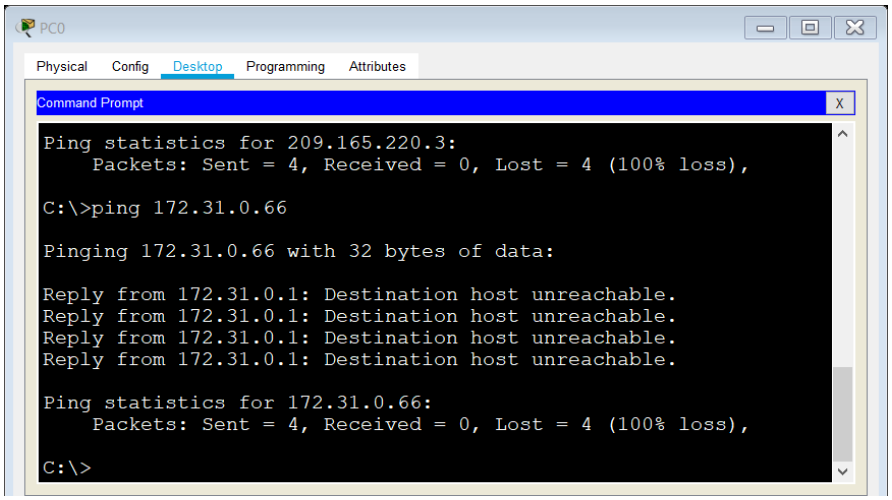
- **Solo los hosts de las VLAN administrativas y de la VLAN de servidores tienen accedo a los routers e internet.**

```
TUNJA(config-subif)#access-list 3 permit 172.31.2.0 0.0.0.7
TUNJA(config)#access-list 3 permit 172.3.2.8 0.0.0.7
TUNJA(config)#access-list 3 permit 172.31.2.8 0.0.0.7
TUNJA(config)#line vty 0 15
TUNJA(config-line)#access-class 3 in

BUCARAMANGA(config-subif)#access-list 3 permit 172.31.2.0 0.0.0.7
BUCARAMANGA(config)#access-list 3 permit 172.3.2.8 0.0.0.7
BUCARAMANGA(config)#access-list 3 permit 172.31.2.8 0.0.0.7
BUCARAMANGA(config)#line vty 0 15
BUCARAMANGA(config-line)#access-class 3 in
BUCARAMANGA(config-line)#

CUNDINAMARCA(config-subif)#access-list 3 permit 172.31.2.0 0.0.0.7
CUNDINAMARCA(config)#access-list 3 permit 172.3.2.8 0.0.0.7
CUNDINAMARCA(config)#access-list 3 permit 172.31.2.8 0.0.0.7
CUNDINAMARCA(config)#line vty 0 15
CUNDINAMARCA(config-line)#access-class 3 in
CUNDINAMARCA(config-line)#
```


PC2
Physical
Config
Desktop
Programming
Attributes
Command Prompt
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 172.31.2.128
Pinging 172.31.2.128 with 32 bytes of data:
Reply from 172.31.0.129: Destination host unreachable.
Reply from 172.31.0.129: Destination host unreachable.
Reply from 172.31.0.129: Destination host unreachable.
Reply from 172.31.0.129: Destination host unreachable.
Ping statistics for 172.31.2.128:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 172.31.0.194
Pinging 172.31.0.194 with 32 bytes of data:
Reply from 172.31.0.129: Destination host unreachable.
Reply from 172.31.0.129: Destination host unreachable.
Reply from 172.31.0.129: Destination host unreachable.
Reply from 172.31.0.129: Destination host unreachable.
Ping statistics for 172.31.0.194:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),


PC0
Physical
Config
Desktop
Programming
Attributes
Command Prompt
Ping statistics for 209.165.220.3:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 172.31.0.66
Pinging 172.31.0.66 with 32 bytes of data:
Reply from 172.31.0.1: Destination host unreachable.
Reply from 172.31.0.1: Destination host unreachable.
Reply from 172.31.0.1: Destination host unreachable.
Reply from 172.31.0.1: Destination host unreachable.
Ping statistics for 172.31.0.66:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>

Conclusiones

Las ACL permiten el acceso de direcciones IP específicas, lo que asegura que solo la computadora del administrador tenga permiso para acceder al Router mediante telnet o SSH.

Con el desarrollo de esta actividad se ejecutan funciones como la de verificar una conexión entre los dispositivos proporcionada en la configuración inicial de la topología.

El servicio DHCP provee a los clientes la configuración de manera automática muy útil para redes grandes.

El desarrollo del trabajo realizado demuestra el aprendizaje obtenido y el manejo de la herramienta de simulación de CISCO, Packet Tracer, donde se inició con actividades para conocer el entorno de trabajo y las herramientas que tiene, posteriormente para la realización de los talleres propuestos a lo largo de la realización del diplomado.

Bibliografía

Capacity. Cisco CCNA – Cómo Configurar VLAN en Cisco Switch. Recuperado de:http://blog.capacityacademy.com/2014/06/06/cisco-ccna-como-configurar-vlanen-switch-cisco/

Cisco Networking Academy. Tomado de: http://ecovi.uagro.mx/ccna1/index.html Introducción a Cisco Packet Tracer. Tomado de: http://simulacionderedeslan.blogspot.com.co/2013/06/introduccion-cisco-packettracer.html

Amberg, E. (2014). CCNA 1 Powertraining: ICND1/CCENT (100-101). Heidleberg: MITP. Recuperado de http://bibliotecavirtual.unad.edu.co:2051/login.aspx?direct=true&db=e000xww&AN=979032&lang=es&site=ehost-live

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

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

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

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

Cisco CCNA – configuración DHCP http://blog.capacityacademy.com/2014/01/09/cisco-ccna-como-configurar-dhcp-encisco-router/

CICO NETWORKING ACADEMY – CCNA 1. https://1314297.netacad.com/courses/882844

CICO NETWORKING ACADEMY – CCNA 2. https://1314297.netacad.com/courses/921962