EVALUACIÓN – PRUEBA DE HABILIDADES PRÁCTICAS CCNA

LUISA FERNANDA PEDRAZA RODRIGUEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
PROGRAMA INGENIERÍA DE SISTEMAS
DIPLOMADO PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN)
LA DORADA, CALDAS
2019

EVALUACIÓN – PRUEBA DE HABILIDADES PRÁCTICAS CCNA

LUISA FERNANDA PEDRAZA RODRIGUEZ

PRUEBA DE HABILIDADES PRÁCTICAS CCNA

TUTOR
NILSON ALBEIRO FERREIRA MANZANARES

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
PROGRAMA INGENIERÍA DE SISTEMAS
DIPLOMADO PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN)
LA DORADA, CALDAS
2019

CONTENIDO

TABLA DE ILUSTRACIONES

RESUMEN

Actualmente las redes de comunicación son necesarias para la humanidad, así mismo, gracias a la competitividad la evolución de esta ha sido inminente. Un ejemplo de lo anterior son las redes informáticas, estas son una de las formas utilizadas para conectar distintos dispositivos informáticos ejecutando un intercambio de comunicación de datos, en donde no solo se utiliza el cableado como infraestructura, sino que también a los enrutadores, servidores y demás dispositivos que intervienen en esta comunicación.

En el presente diplomado denominado Profundización CISCO (Diseño e implementación de soluciones integradas LAN / WAN) se abordaron diferentes temáticas, tales como, exploración de redes, configuración de un sistema operativo de red, protocolos, comunicaciones de red, acceso a la red, ethernet, capa de red, enrutamiento dinámico, OSPF de una sola área, listas de control de acceso, DHCP, traducción de direcciones IP para IPV4, entre otras, conocimientos que enriquecieron el desarrollo profesional de cada uno de los estudiantes y que aporta a la sociedad en esta especialidad.

ABSTRACT

Currently communication networks are necessary for humanity, likewise, thanks to competitiveness the evolution of this has been imminent. An example of the above are computer networks, these are one of the ways used to connect different computing devices by executing an exchange of data communication, where not only wiring is used as infrastructure, but also to routers, servers and other devices involved in this communication.

In this diplomat called Deepening CISCO (Design and implementation of integrated LAN / WAN solutions) different topics were addressed, such as, network exploration, configuration of a network operating system, protocols, network communications, network access, ethernet, network layer, dynamic routing , single area OSPF, access control lists, DHCP, IP address translation for IPV4, among others, knowledges that enriches the professional development of each student and that society provides in this specialty.

INTRODUCCIÓN

El presente documento contiene las evidencias del desarrollo de una serie de pruebas de habilidades ejecutadas por estudiantes de la Universidad Nacional Abierta y a Distancia UNAD, en los cuales se abordaron temáticas tales como direccionamiento IP, seguridad en la red, servidores DHCP, protocolo de enrutamiento EIGRP, conexiones Telnet, listas de control de acceso (ACL), servidores TFTP, enmascaramiento de IP y configuración de VLANS. Lo anterior, con el fin de que cada uno de los estudiantes pusiera a prueba los niveles de comprensión y solución de problemas relacionados con diversos aspectos de Networking, estableciendo escenarios LAN/WAN que permitan realizar un análisis sobre el comportamiento de diversos protocolos y métricas de enrutamiento.

OBJETIVOS

2.1. OBJETIVO GENERAL

Poner a prueba todas las habilidades prácticas y teóricas adquiridas durante el desarrollo del diplomado Profundización CISCO (Diseño e implementación de soluciones integradas LAN / WAN).

2.2 OBJETIVOS ESPECÍFICOS

2.2.1. Determinar los dispositivos requeridos para la construcción de cada topología de red.

2.2.2. Realizar la topología de red de acuerdo con lo solicitado en cada escenario.

2.2.3. Configurar cada uno de los dispositivos (Switch, routers, servidores) de acuerdo con lo solicitado.

2.2.4. Asignar el protocolo de enrutamiento EIGRP de acuerdo con lo solicitado.

2.2.5. Implementar DHCP en los dispositivos de comunicación.

2.2.6. Configurar el NAT estático en el Web Server.

2.2.7. Configurar las listas de control de acceso.

2.2.8. Verificar la conectividad entre los dispositivos de cada topología.

DESARROLLO DE LOS DOS ESCENARIOS

ESCENARIO 1

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

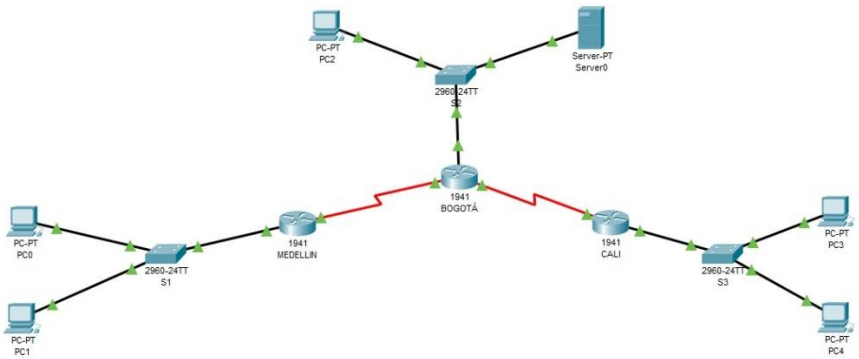
Trabajo inicial

La topología de red se realizó con los siguientes elementos:

- (03) Routers referencia 1941
- (03) Switchs 2960-24TT
- (05) Equipos de computo
- (01) Servidor PT

Se realiza la conexión física de los equipos con base en la topología de red.

Ilustración 1. Conexión física Escenario 1.



Fuente: Propia.

Se procede a realizar la configuración básica de cada uno de los dispositivos de la red:

ROUTERS

MEDELLIN

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname Medellin
Medellin(config)#no ip domain-lookup
Medellin(config)#enable secret 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 pass
Medellin(config)#service password-encryption
Medellin(config)#banner motd $ Unauthorized Access Is Prohibited $
Medellin(config)#
```

BOGOTÁ

```
Router>enable
Router#configure terminal
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 pass
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 runn
Bogota#copy running-config sta
Bogota#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Bogota#
```

CALI

```
Router>enable
Router#config
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname Cali
Cali(config)#no ip domain-lookup
Cali(config)#enable secret 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#
```

CONMUTADORES (SWITCHES)

S1

```
Switch>enable
Switch#configure terminal
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 start
S1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
S1#
```

S2

```
Switch>enable
Switch#configure terminal
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-encr
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#configure terminal
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...
[OK]
S3#
```

Parte 1: Asignación de direcciones IP

Se procede a dividir la red, creando una segmentación de 08 parte, asignando las direcciones IP requeridas.

1.
Network: 192.168.1.0/27
Netmask: 255.255.255.224
HostMin: 192.168.1.1
HostMax: 192.168.1.30
Broadcast: 192.168.1.31

2.
Network: 192.168.1.32/27
Netmask: 255.255.255.224
HostMin: 192.168.1.33
HostMax: 192.168.1.62
Broadcast: 192.168.1.63

3.
Network: 192.168.1.64/27
Netmask: 255.255.255.224
HostMin: 192.168.1.65
HostMax: 192.168.1.94
Broadcast:192.168.1.95

4.
Network: 192.168.1.96/27
Netmask: 255.255.255.224
HostMin: 192.168.1.97
HostMax: 192.168.1.126
Broadcast: 192.168.1.127

5.
Network: 192.168.1.128/27
Netmask: 255.255.255.224
HostMin: 192.168.1.129
HostMax: 192.168.1.158
Broadcast:192.168.1.159

6.
Network: 192.168.1.160/27
Netmask: 255.255.255.224
HostMin: 192.168.1.161
HostMax: 192.168.1.190
Broadcast:192.168.1.191

7.
Network: 192.168.1.192/27
Netmask: 255.255.255.224
HostMin: 192.168.1.193
HostMax: 192.168.1.222
Broadcast:192.168.1.223

8.
Network: 192.168.1.224/27
Netmask: 255.255.255.224
HostMin: 192.168.1.225
HostMax: 192.168.1.254
Broadcast:192.168.1.255

Parte 2: Configuración básica

Teniendo en cuenta las subredes diseñadas, obtenemos:

	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	192.168.1.131	192.168.1.130	192.168.1.193
Dirección de Ip en interfaz G 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

A continuación, se realiza la configuración de la IP Route.

MEDELLÍN

```
User Access Verification
Password:
Medellin>ena
Password:
Medellin#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Medellin(config)#ip    route    192.168.1.0    255.255.255.224
192.168.1.98
Medellin(config)#ip    route    192.168.1.64    255.255.255.224
192.168.1.98
Medellin(config)#ip    route    192.168.1.128    255.255.255.224
192.168.1.98
Medellin(config)#
```

BOGOTÁ

```
User Access Verification
```

```
Password:
Bogota>en
Password:
Bogota #configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Bogota (config)#ip route 192.168.1.32 255.255.255.224
192.168.1.99
Bogota (config)#ip route 192.168.1.64 255.255.255.224
192.168.1.131
Bogota(config)#
```

CALI

```
User Access Verification
Password:
Cali>en
Password:
Password:
Cali #configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Cali (config)#ip route 192.168.1.0 255.255.255.224
192.168.1.130
Cali (config)#ip route 192.168.1.32 255.255.255.224
192.168.1.130
Cali (config)#
```

Luego, se realiza un diagnóstico de vecinos usando el comando cdp.

MEDELLÍN

```
Medellin#show cdp nei
Medellin#show cdp neighbors detail

Device ID: S1
Entry address(es):
Platform: cisco 2960, Capabilities: Switch
Interface: GigabitEthernet0/0, Port ID (outgoing port):
GigabitEthernet0/1
Holdtime: 163

Version :
```

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

advertisement version: 2
Duplex: full
---------------------------
Device ID: Bogota
Entry address(es):
IP address : 192.168.1.98
Platform: cisco C1900, Capabilities: Router
Interface: Serial0/0/0, Port ID (outgoing port): Serial0/0/0
Holdtime: 171

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
```

BOGOTÁ

```
Bogota#show cdp ne
Bogota#show cdp neighbors detail

Device ID: S2
Entry address(es):
Platform: cisco 2960, Capabilities: Switch
Interface: GigabitEthernet0/0, Port ID (outgoing port):
GigabitEthernet0/1
Holdtime: 138

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

advertisement version: 2
```

```
Duplex: full
---------------------------
Device ID: 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: 145

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: 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: 139

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

Bogota#
```

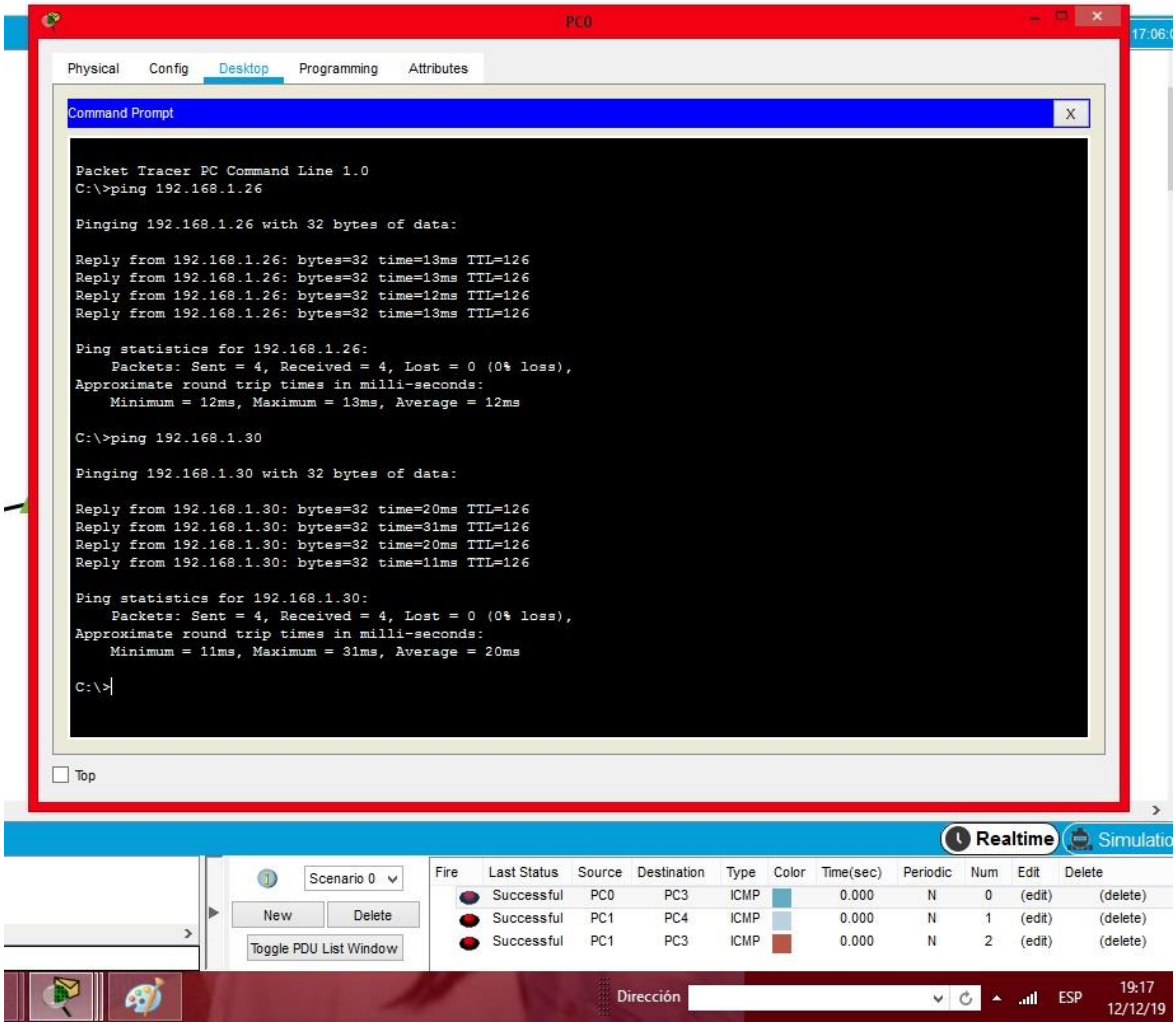
CALI

```
Cali>enable
Password:
Cali#show cdp nei
```

```
Cali#show cdp neighbors det
Cali#show cdp neighbors detail

Device ID: S3
Entry address(es):
Platform: cisco 2960, Capabilities: Switch
Interface:  GigabitEthernet0/0,  Port  ID  (outgoing  port):
GigabitEthernet0/1
Holdtime: 145

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

advertisement version: 2
Duplex: full
---------------------------

Device ID: Bogota
Entry address(es):
IP address : 192.168.1.130
Platform: cisco C1900, Capabilities: Router
Interface: Serial0/0/0, Port ID (outgoing port): Serial0/0/1
Holdtime: 153

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

Cali#
```

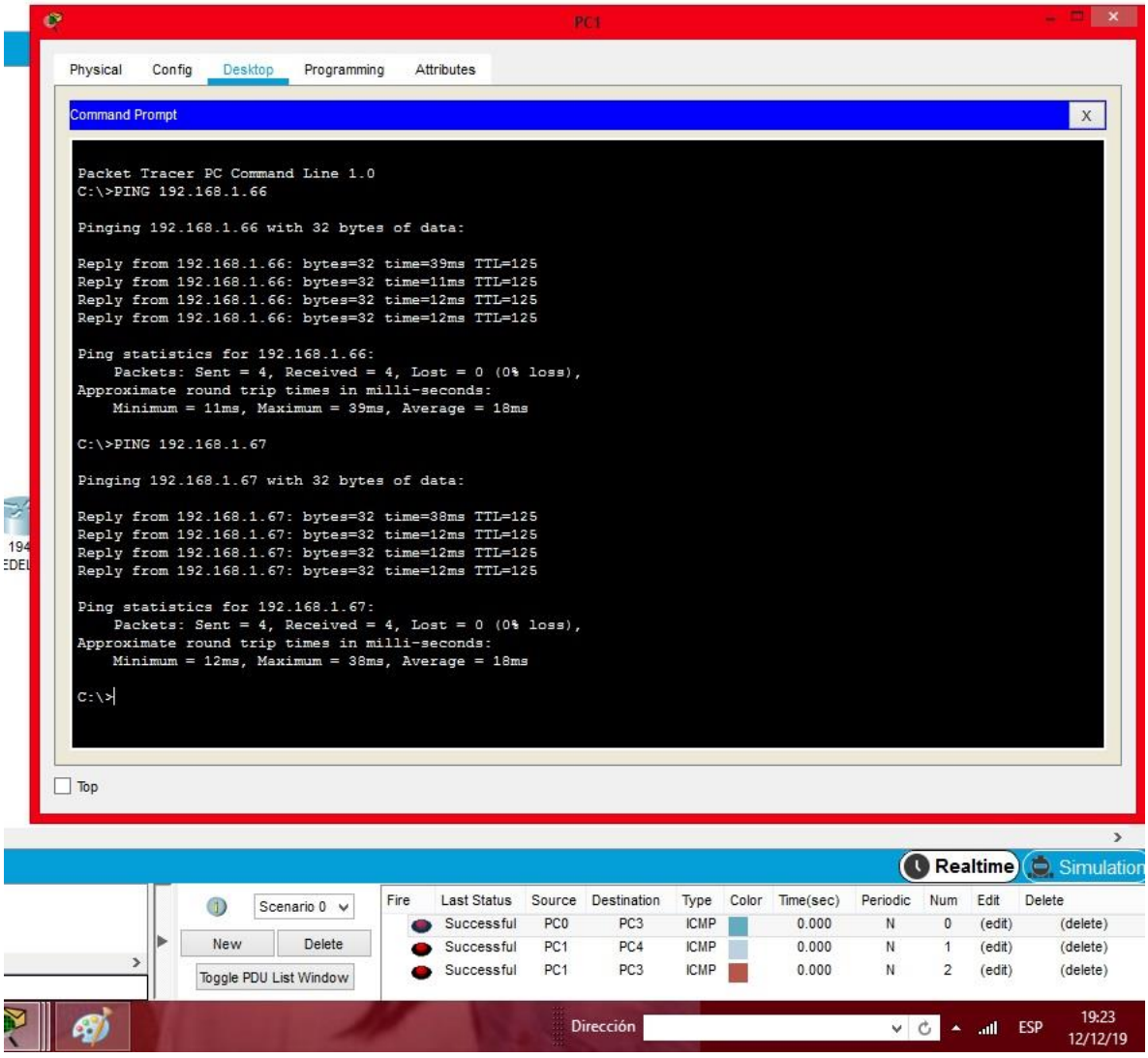
Se realiza una prueba de conectividad en cada tramo de la ruta usando el comando Ping.

Ilustración 2. Ping de PC0 Medellín a Server y PC2 Bogotá.



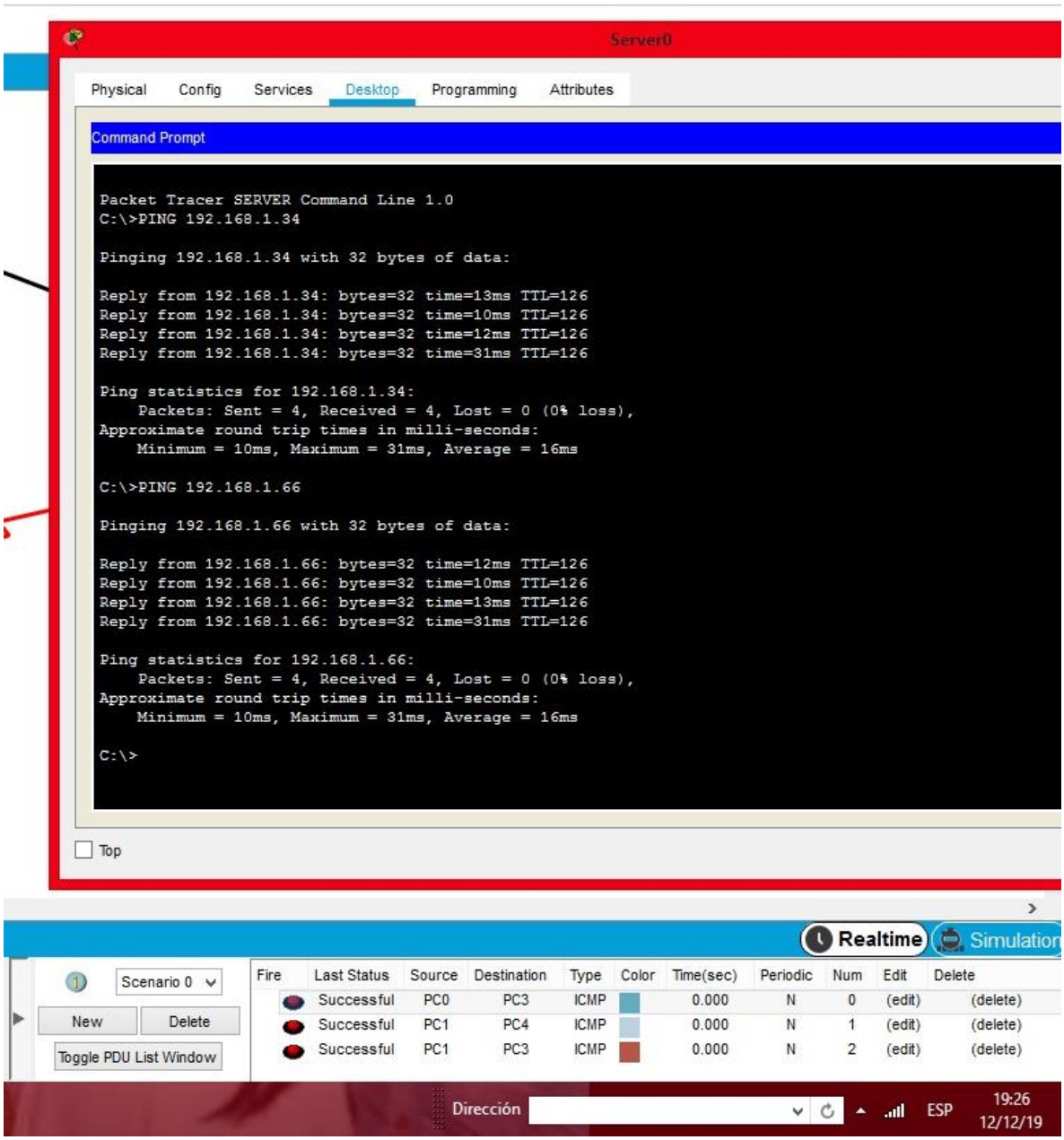
Fuente: Propia

Ilustración 3. Ping PC1 Medellín a PC3 y PC 4 Cali.



Fuente: Propia

Ilustración 4. Ping Server Bogotá a PC0 Medellín y PC 3 Cali.



Fuente: Propia

Parte 3: Configuración de enrutamiento

Se realiza la asignación del protocolo de enrutamiento EIGRP a los routers considerando el direccionamiento diseñado, así mismo se verifica si existe vecindad con los routers configurados.

ROUTER MEDELLIN

```
User Access Verification

Password:
Password:

Medellin>enable
Password:
Medellin#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Medellin(config)#router eig
Medellin(config)#router eigrp 200
Medellin(config-router)#net
Medellin(config-router)#network 192.168.1.32 0.0.0.31
Medellin(config-router)#network 192.168.1.96 0.0.0.31
Medellin(config-router)#no au
Medellin(config-router)#no auto-summary
Medellin(config-router)#end
Medellin#
%SYS-5-CONFIG_I: Configured from console by console

Medellin#
```

ROUTER BOGOTÁ

```
User Access Verification

Password:

Bogota>en
Password:
Bogota#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Bogota(config)#rou
```

```
Bogota(config)#router ei
Bogota(config)#router eigrp 200
Bogota(config-router)#net
Bogota(config-router)#network 192.168.1.0 0.0.0.31
Bogota(config-router)#network 192.168.1.96 0.0.0.31
Bogota(config-router)#
%DUAL-5-NBRCHANGE:   IP-EIGRP   200:   Neighbor   192.168.1.99
(Serial0/0/0) is up: new adjacency

Bogota(config-router)#network 192.168.1.128 0.0.0.31
Bogota(config-router)#network 192.168.1.96 0.0.0.31
Bogota(config-router)#no autosu
Bogota(config-router)#no auto
Bogota(config-router)#no auto-summary
Bogota(config-router)#
```

ROUTER CALI

```
User Access Verification

Password:
Password:

Cali>en
Password:
Cali#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Cali(config)#rou
Cali(config)#router ei
Cali(config)#router eigrp 200
Cali(config-router)#net
Cali(config-router)#network 192.168.1.64 0.0.0.31
Cali(config-router)#network 192.168.1.128 0.0.0.31
Cali(config-router)#
%DUAL-5-NBRCHANGE:   IP-EIGRP   200:   Neighbor   192.168.1.130
(Serial0/0/0) is up: new adjacency

Cali(config-router)#network 192.168.1.128 0.0.0.31
Cali(config-router)#no auto
Cali(config-router)#no auto-summary
Cali(config-router)#
```

A continuación, se realiza la comprobación de las tablas de enrutamiento en cada uno de los routers y se verifica cada una de las rutas establecidas.

ROUTER MEDELLIN

```
Medellin>en
Password:
Medellin#show ip ro
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, 7 subnets, 2 masks
S 192.168.1.0/27 [1/0] via 192.168.1.98
C 192.168.1.32/27 is directly connected, GigabitEthernet0/0
L 192.168.1.33/32 is directly connected, GigabitEthernet0/0
S 192.168.1.64/27 [1/0] via 192.168.1.98
C 192.168.1.96/27 is directly connected, Serial0/0/0
L 192.168.1.99/32 is directly connected, Serial0/0/0
S 192.168.1.128/27 [1/0] via 192.168.1.98

Medellin#
```

ROUTER BOGOTA

```
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, 8 subnets, 2 masks
C 192.168.1.0/27 is directly connected, GigabitEthernet0/0
L 192.168.1.1/32 is directly connected, GigabitEthernet0/0
S 192.168.1.32/27 [1/0] via 192.168.1.97
[1/0] via 192.168.1.99
S 192.168.1.64/27 [1/0] via 192.168.1.131
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#
```

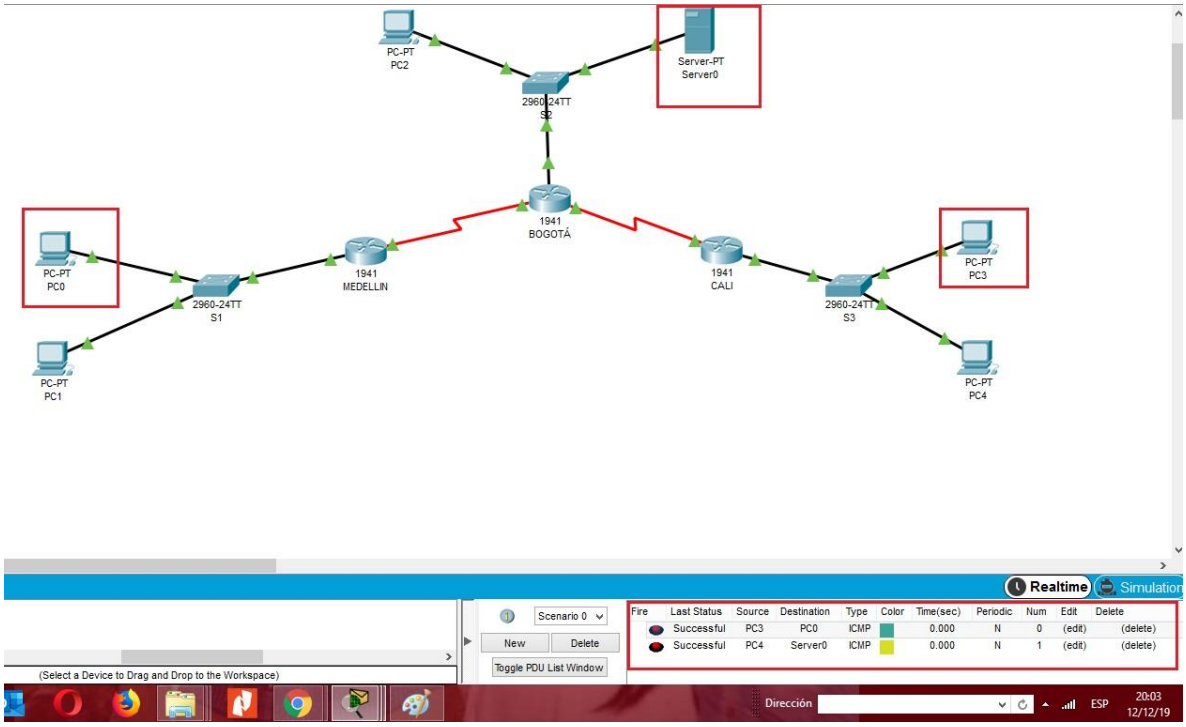
ROUTER CALI

```
Cali#
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, 7 subnets, 2 masks
S 192.168.1.0/27 [1/0] via 192.168.1.130
[1/0] via 192.168.1.98
S 192.168.1.32/27 [1/0] via 192.168.1.130
[1/0] via 192.168.1.98
C 192.168.1.64/27 is directly connected, GigabitEthernet0/0
L 192.168.1.65/32 is directly connected, GigabitEthernet0/0
```

```
S 192.168.1.96/27 [1/0] via 192.168.1.130
C 192.168.1.128/27 is directly connected, Serial0/0/0
L 192.168.1.131/32 is directly connected, Serial0/0/0

Cali#
```

En el presente punto, se realiza un diagnóstico con el fin de comprobar que cada uno de los puntos de la red se puedan ver y tengan conectividad en tre sí. Se realiza la prueba desde un host de la red LAN del router CALI, primero a la red de Medellín y luego al servidor.

Ilustración 5. Diagnóstico conectividad.



Fuente: Propia.

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

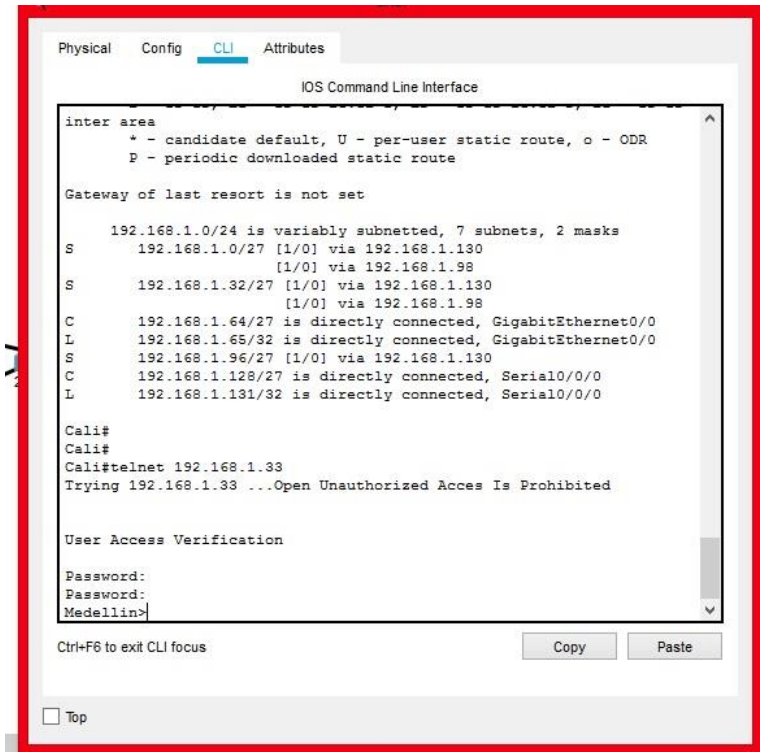
En este momento cualquier usuario de la red tiene acceso a todos sus dispositivos y estaciones de trabajo. El jefe de redes le solicita implementar seguridad en la red. Para esta labor se decide configurar listas de control de acceso (ACL) a los routers.

Las condiciones para crear las ACL fueron:

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

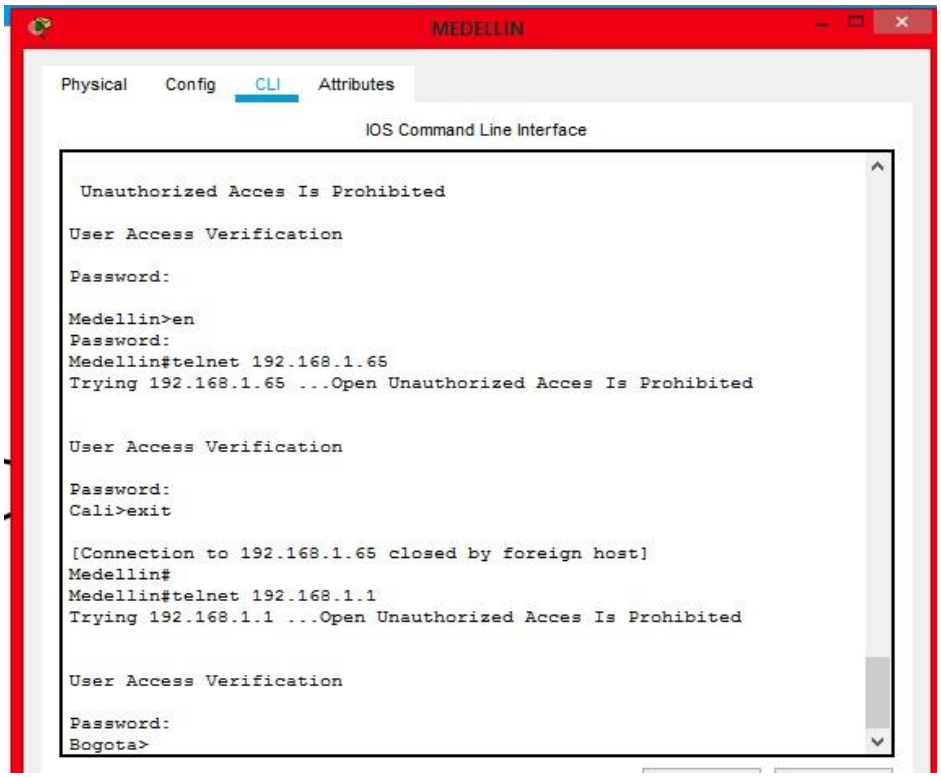
   Pruebas conexión TELNET

   Ilustración 6. Prueba conexión TELNET 1.



   Fuente: Propia.

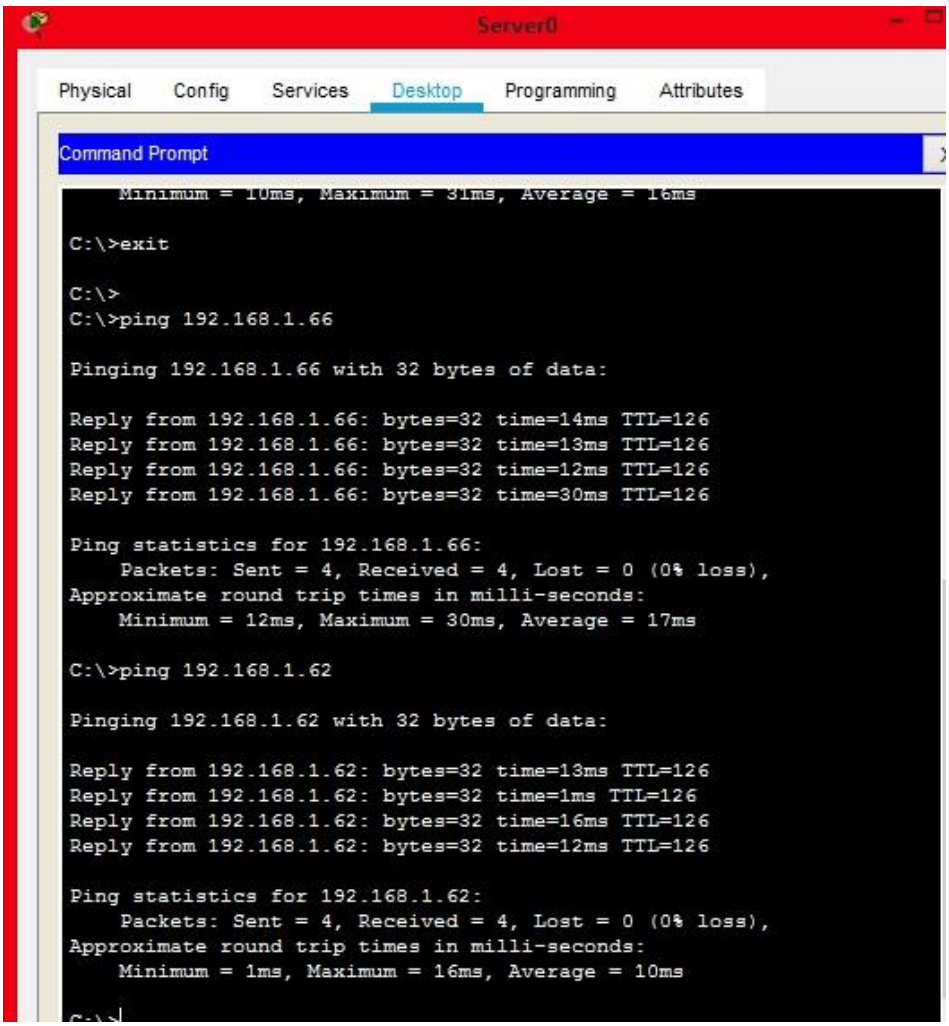
Ilustración 7. Prueba conexión TELNET 2.



Fuente: Propia.

2. 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.

Ilustración 8. Prueba conexión Subred Administración.



Fuente: Propia.

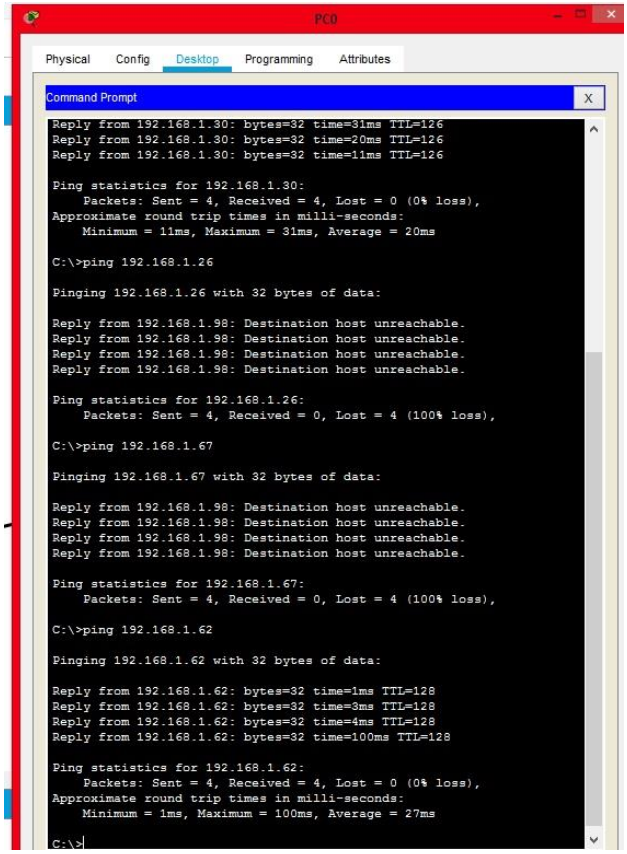
3. Las estaciones de trabajo en las LAN de MEDELLIN y CALI no deben tener acceso a ningún dispositivo fuera de su subred, excepto para interconectar con el servidor.

```
Bogota#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Bogota(config)#
Bogota(config)#
Bogota(config)#
Bogota(config)#acc
Bogota(config)#access-list 1 deny 192.168.1.32 0.0.0.31
Bogota(config)#access-list 1 deny 192.168.1.64 0.0.0.31
```

```
Bogota(config)#acc
Bogota(config)#access-list 1 permit any
Bogota(config)#inter
Bogota(config)#interface giga
Bogota(config)#interface gigabitEthernet 0/0
Bogota(config-if)#ip acc
Bogota(config-if)#ip access-group 1 out
Bogota(config-if)#exit
Bogota(config)#
```

La red de Medellín no tiene acceso a ninguna otra red, excepto la de su misma red.

Ilustración 9. Prueba sin acceso.



Fuente: Propia.

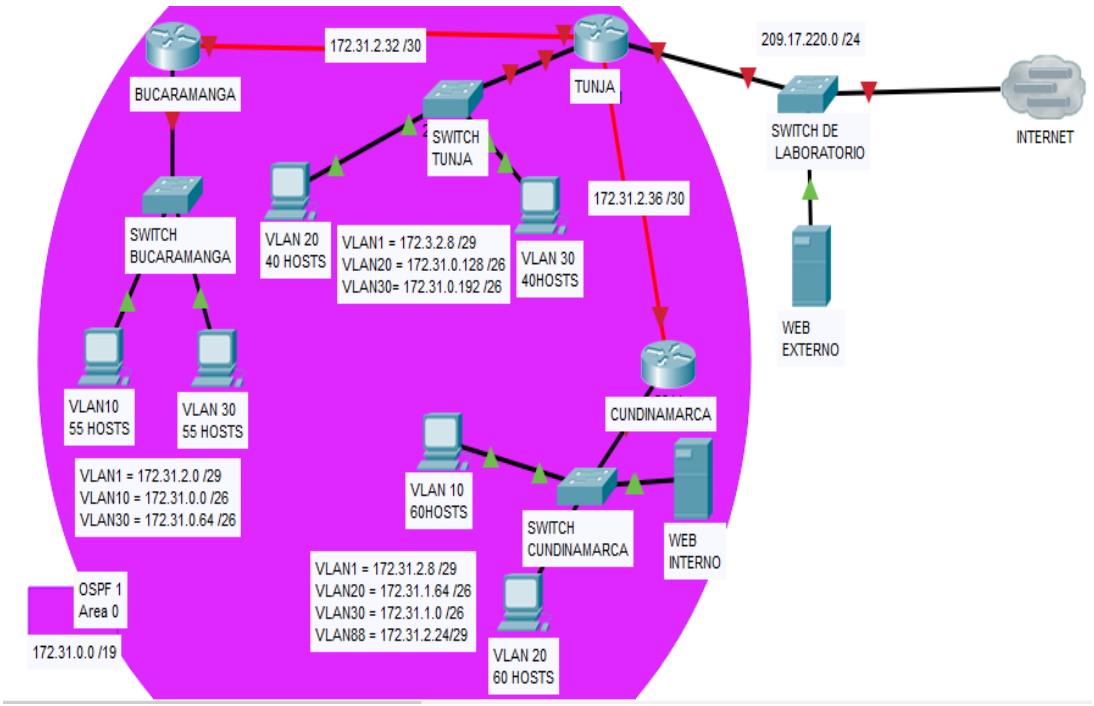
Parte 5: Comprobación de la red instalada.

	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	LOSS
	LAN del Router MEDELLIN	WS_1	LOSS
	LAN del Router MEDELLIN	LAN del Router CALI	LOSS
PING	LAN del Router CALI	Servidor	LOSS
	LAN del Router MEDELLIN	Servidor	LOSS
	Servidor	LAN del Router MEDELLIN	OK
	Servidor	LAN del Router CALI	OK
	Router CALI	LAN del Router MEDELLIN	LOSS
	Router MEDELLIN	LAN del Router CALI	LOSS

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.

Ilustración 10. Topogía de red.



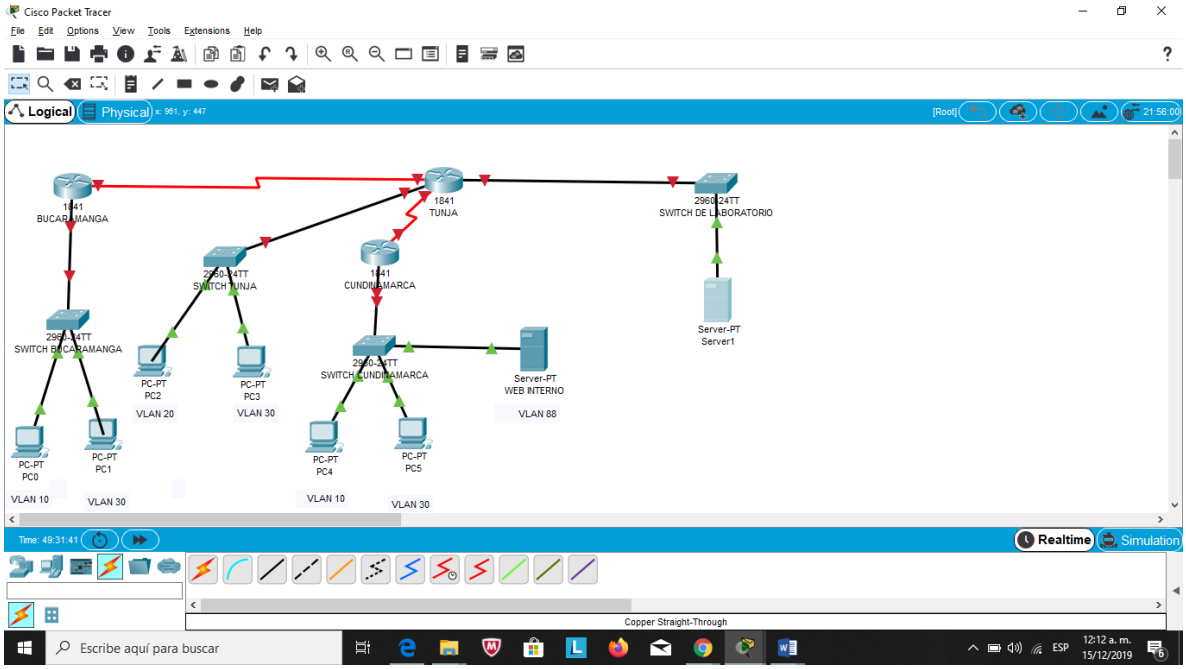
Fuente: (UNAD, 2019)

La topología de red se realizó con los siguientes elementos:

- (03) Routers referencia 1941
- (03) Switchs 2960-24TT
- (06) Equipos de computo
- (02) Servidores PT

Se realiza la conexión física de los equipos con base en la topología de red.

Ilustración 11. Conexión física Escenario 2.



Fuente: Propia.

1. Configuración básica.

BUCARAMANGA

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname BUCARAMANGA
BUCARAMANGA(config)#no ip domain-lookup
BUCARAMANGA(config)#banner motd #Acceso Restringido!#?
LINE
BUCARAMANGA(config)#banner motd #Acceso Restringido!#
BUCARAMANGA(config)#enable secret lufe1995
BUCARAMANGA(config)#line console 0
BUCARAMANGA(config-line)#password lufe1995
BUCARAMANGA(config-line)#login
BUCARAMANGA(config-line)#logging synchronous
BUCARAMANGA(config-line)#line vty 0 15
BUCARAMANGA(config-line)#password lufe1995
```

```
BUCARAMANGA(config-line)#login
BUCARAMANGA(config-line)#logging synchronous
BUCARAMANGA(config-line)#exit
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 shutdown

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

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

%LINK-5-CHANGED: Interface FastEthernet0/0.1, changed state to
up

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

%LINK-5-CHANGED: Interface FastEthernet0/0.10, changed state to
up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/0.10, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/0.30, changed state to
up

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

BUCARAMANGA(config-if)#int s0/0/0
BUCARAMANGA(config-if)#ip address 172.31.2.34 255.255.255.252
BUCARAMANGA(config-if)#no shutdown

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

BUCARAMANGA#
```

TUNJA

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname TUNJA
TUNJA(config)#no ip domain-lookup
TUNJA(config)#banner motd #Acceso Restringido!#
TUNJA(config)#enable secret lufe1995
TUNJA(config)#line console 0
TUNJA(config-line)#password lufe1995
TUNJA(config-line)#login
TUNJA(config-line)#logging synchronous
TUNJA(config-line)#line vty 0 15
TUNJA(config-line)#password lufe1995
TUNJA(config-line)#login
TUNJA(config-line)#logging synchronous
TUNJA(config-line)#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 shutdown

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

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

```
%LINK-5-CHANGED: Interface FastEthernet0/0.1, changed state to up

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

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

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

%LINK-5-CHANGED: Interface FastEthernet0/0.30, changed state to up

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

TUNJA(config-if)#int s0/0/0
TUNJA(config-if)#ip address 172.31.2.33 255.255.255.252
TUNJA(config-if)#no shutdown

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

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

TUNJA(config-if)#int 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)#int f0/1
TUNJA(config-if)#ip address 209.165.220.1 255.255.255.0
TUNJA(config-if)#no shutdown

TUNJA(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

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

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)#
00:51:29: %OSPF-5-ADJCHG: Process 1, Nbr 172.31.2.34 on
Serial0/0/0 from LOADING to FULL, Loading Done

TUNJA(config-router)#network 172.31.2.36 0.0.0.3 area 0
TUNJA(config-router)#end
TUNJA#
%SYS-5-CONFIG_I: Configured from console by console

TUNJA#
```

CUNDINAMARCA

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname CUNDINAMARCA
CUNDINAMARCA(config)#no ip domain-lookup
CUNDINAMARCA(config)#banner motd #Acceso Restringido!#
CUNDINAMARCA(config)#enable secret lufe1995
CUNDINAMARCA(config)#line console 0
CUNDINAMARCA(config-line)#password lufe1995
CUNDINAMARCA(config-line)#login
CUNDINAMARCA(config-line)#logging synchronous
CUNDINAMARCA(config-line)#line vty 0 15
CUNDINAMARCA(config-line)#password lufe1995
CUNDINAMARCA(config-line)#login
CUNDINAMARCA(config-line)#logging synchronous
CUNDINAMARCA(config-line)#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 shutdown

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

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

%LINK-5-CHANGED: Interface FastEthernet0/0.1, changed state to
up

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

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

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

%LINK-5-CHANGED: Interface FastEthernet0/0.30, changed state to
up

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

%LINK-5-CHANGED: Interface FastEthernet0/0.88, changed state to
up

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

CUNDINAMARCA(config-if)#int s0/0/0
CUNDINAMARCA(config-if)#ip address 172.31.2.38 255.255.255.252
CUNDINAMARCA(config-if)#no shutdown

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

CUNDINAMARCA(config-if)#
```

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

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

2. Autenticación local con AAA.

CUNDINAMARCA

```
CUNDINAMARCA(config)#line console 0
CUNDINAMARCA(config-line)#username admin secret lufe1995
CUNDINAMARCA(config)#aaa new-model
CUNDINAMARCA(config)#aaa authentication login AUTH local
CUNDINAMARCA(config)#line console 0
CUNDINAMARCA(config-line)#login authentication AUTH
CUNDINAMARCA(config-line)#line vty 0 15
CUNDINAMARCA(config-line)#login authentication AUTH
CUNDINAMARCA(config-line)#
```

TUNJA

```
User Access Verification

Password:

TUNJA>enable
Password:
TUNJA#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
TUNJA(config)#line console 0
TUNJA(config-line)#username admin secret lufe1995
TUNJA(config)#aaa new-model
TUNJA(config)#aaa authentication login AUTH local
```

```
TUNJA(config)#line console 0
TUNJA(config-line)#login authentication AUTH
TUNJA(config-line)#line vty 0 15
TUNJA(config-line)#login authentication AUTH
TUNJA(config-line)#
```

BUCARAMANGA

```
Acceso Restringido!

User Access Verification

Password:

BUCARAMANGA>enable
Password:
BUCARAMANGA#
BUCARAMANGA#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
BUCARAMANGA(config)#line console 0
BUCARAMANGA(config-line)#username admin secret lufe1995
BUCARAMANGA(config)#aaa new-model
BUCARAMANGA(config)#aaa authentication login AUTH local
BUCARAMANGA(config)#line console 0
BUCARAMANGA(config-line)#login authentication AUTH
BUCARAMANGA(config-line)#line vty 0 15
BUCARAMANGA(config-line)#login authentication AUTH
BUCARAMANGA(config-line)#!
BUCARAMANGA#
%SYS-5-CONFIG_I: Configured from console by console

BUCARAMANGA#
```

3. Cifrado de contraseñas.

CUNDINAMARCA

```
Acceso Restringido!

User Access Verification
```

```
Username: admin
Password:
CUNDINAMARCA>enable
Password:
CUNDINAMARCA#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
CUNDINAMARCA(config)#service password-encryption
CUNDINAMARCA(config)#
```

TUNJA

```
Acceso Restringido!

User Access Verification

Username: admin
Password:
TUNJA>enable
Password:
TUNJA#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
TUNJA(config)#service password-encryption
TUNJA(config)#
```

BUCARAMANGA

```
Acceso Restringido!

User Access Verification

Username: admin
Password:
BUCARAMANGA>enable
Password:
BUCARAMANGA#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
BUCARAMANGA(config)#service password-encryption
BUCARAMANGA(config)#
```

ENRUTADORES – SWITCHES

CUNDINAMARCA

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname SCUNDINAMARCA
SCUNDINAMARCA(config)#vlan 1
SCUNDINAMARCA(config-vlan)#vlan 20
SCUNDINAMARCA(config-vlan)#vlan 30
SCUNDINAMARCA(config-vlan)#vlan 88
SCUNDINAMARCA(config-vlan)#exit
SCUNDINAMARCA(config)#int f0/20
SCUNDINAMARCA(config-if)#switchport mode access
SCUNDINAMARCA(config-if)#switchport access vlan 20
SCUNDINAMARCA(config-if)#int f0/24
SCUNDINAMARCA(config-if)#switchport mode access
SCUNDINAMARCA(config-if)#switchport access vlan 30
SCUNDINAMARCA(config-if)#int f0/10
SCUNDINAMARCA(config-if)#switchport mode access
SCUNDINAMARCA(config-if)#switchport access vlan 88
SCUNDINAMARCA(config-if)#int f0/1
SCUNDINAMARCA(config-if)#switchport mode trunk

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

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

SCUNDINAMARCA(config-if)#int vlan 1
SCUNDINAMARCA(config-if)#ip address 172.31.2.11 255.255.255.248
SCUNDINAMARCA(config-if)#no shutdown

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

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

SCUNDINAMARCA(config-if)#ip default-gateway 172.31.2.9
SCUNDINAMARCA(config)#
```

TUNJA

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname STUNJA
STUNJA(config)#vlan 1
STUNJA(config-vlan)#vlan 20
STUNJA(config-vlan)#vlan 30

STUNJA(config-vlan)#int f0/20
STUNJA(config-if)#switchport mode access
STUNJA(config-if)#switchport access vlan 20
STUNJA(config-if)#int f0/24
STUNJA(config-if)#switchport mode access
STUNJA(config-if)#switchport access vlan 30
STUNJA(config-if)#int f0/1
STUNJA(config-if)#switchport mode trunk

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

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

STUNJA(config-if)#int vlan 1
STUNJA(config-if)#ip address 172.3.2.11 255.255.255.248
STUNJA(config-if)#no shutdown

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

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

STUNJA(config-if)#ip default-gateway 172.3.2.9
STUNJA(config)#
```

BUCARAMANGA

```
Switch>enable
```

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname SBUCARAMANGA
SBUCARAMANGA(config)#vlan 1
SBUCARAMANGA(config-vlan)#vlan 10
SBUCARAMANGA(config-vlan)#vlan 30
SBUCARAMANGA(config-vlan)#int f0/20
SBUCARAMANGA(config-if)#switchport mode access
SBUCARAMANGA(config-if)#switchport access vlan 10
SBUCARAMANGA(config-if)#int f0/24
SBUCARAMANGA(config-if)#switchport mode access
SBUCARAMANGA(config-if)#switchport access vlan 30
SBUCARAMANGA(config-if)#int f0/1
SBUCARAMANGA(config-if)#switchport mode trunk

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

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

SBUCARAMANGA(config-if)#int vlan 1
SBUCARAMANGA(config-if)#ip address 172.31.2.3 255.255.255.248
SBUCARAMANGA(config-if)#no shutdown

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

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

SBUCARAMANGA(config-if)#ip default-gateway 172.31.2.1
SBUCARAMANGA(config)#
```

4. Un máximo de internos para acceder al router.

CUNDINAMARCA

```
CUNDINAMARCA(config)#login block-for 4 attempts 3 within 60
```

TUNJA

```
TUNJA(config)#login block-for 4 attempts 3 within 60
TUNJA(config)#
```

BUCARAMANGA

```
BUCARAMANGA(config)#login block-for 4 attempts 3 within 60
BUCARAMANGA(config)#
```

5. Máximo tiempo de acceso al detectar ataques.

CUNDINAMARCA

```
CUNDINAMARCA(config)#login block-for 4 attempts 3 within 60
```

TUNJA

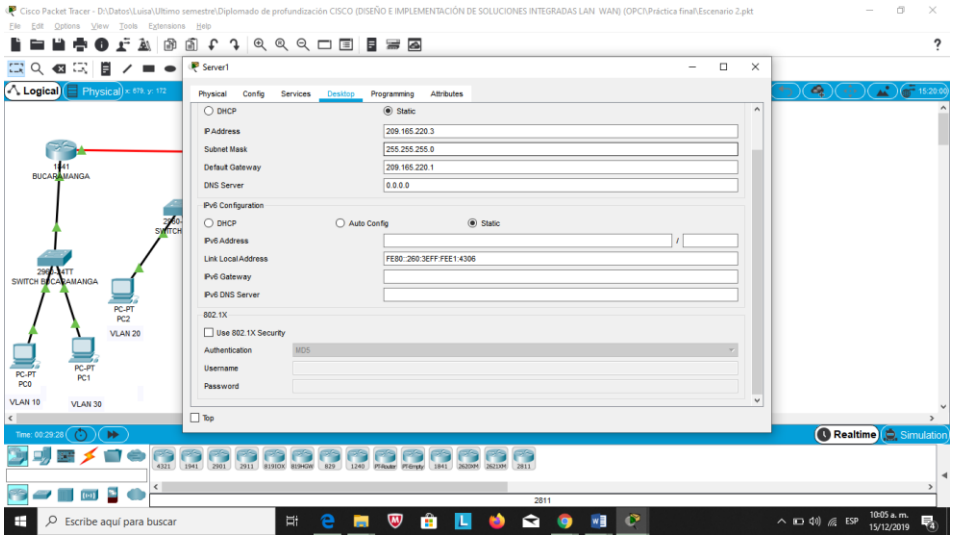
```
TUNJA(config)#login block-for 4 attempts 3 within 60
TUNJA(config)#
```

BUCARAMANGA

```
BUCARAMANGA(config)#login block-for 4 attempts 3 within 60
BUCARAMANGA(config)#
```

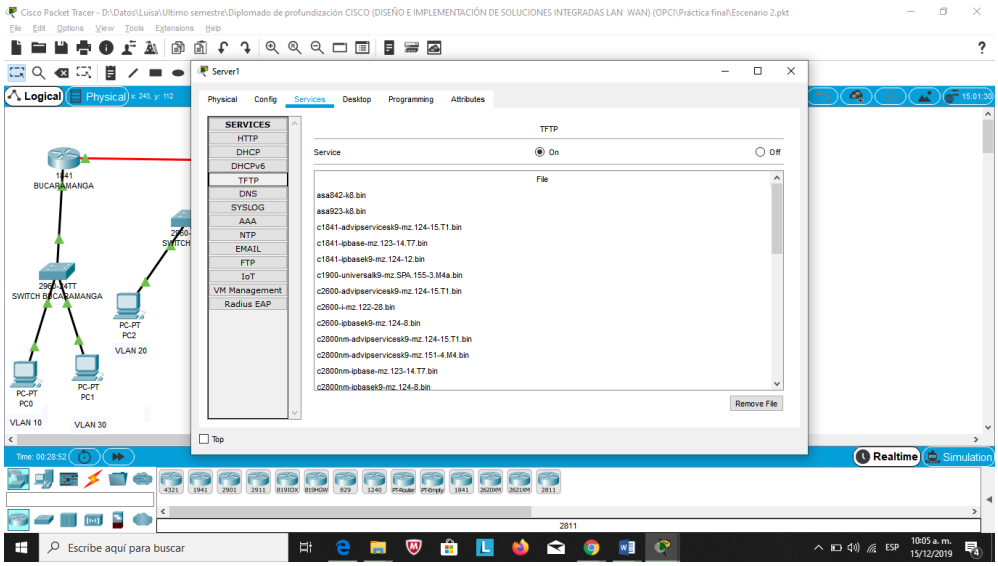
6. Se establece un servidor TFTP y se almacena todos los archivos necesarios de los routers.

Ilustración 12. Configuración servidor TFTP.



Fuente: Propia.

Ilustración 13. Configuración servidor TFTP.



Fuente: Propia.

7. Configuración DHCP.

Se procede a configurar el DHCP para que proporcione solo direcciones a los hosts de Bucaramanga y Cundinamarca.

TUNJA

```
User Access Verification

Username: admin
Password:
TUNJA>enable
Password:
TUNJA#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
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

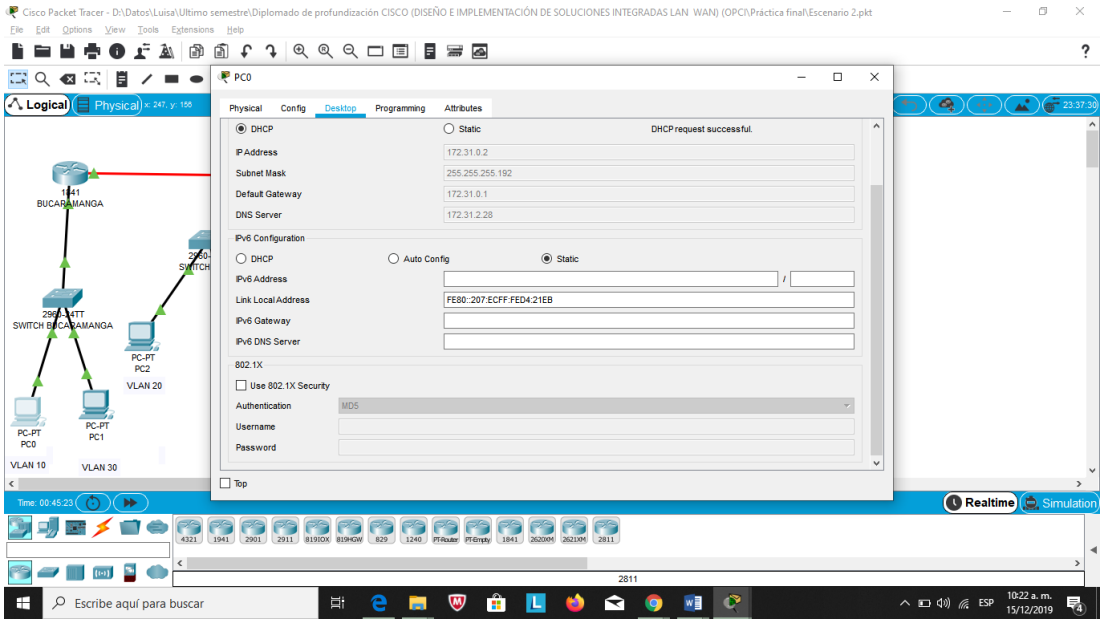
```
Acceso Restringido!

User Access Verification

Username: admin
Password:
CUNDINAMARCA>enable
Password:
CUNDINAMARCA#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
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)#exit
CUNDINAMARCA(config)#
```

BUCARAMANGA

```
Acceso Restringido!

User Access Verification

Username: admin
Password:
BUCARAMANGA>enable
Password:
BUCARAMANGA#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
BUCARAMANGA(config)#int f0/0.10
BUCARAMANGA(config-subif)#ip helper-address 172.31.2.33
BUCARAMANGA(config-subif)#int f0/0.30
BUCARAMANGA(config-subif)#ip helper-address 172.31.2.33
BUCARAMANGA(config-subif)#exit
BUCARAMANGA(config)#
```

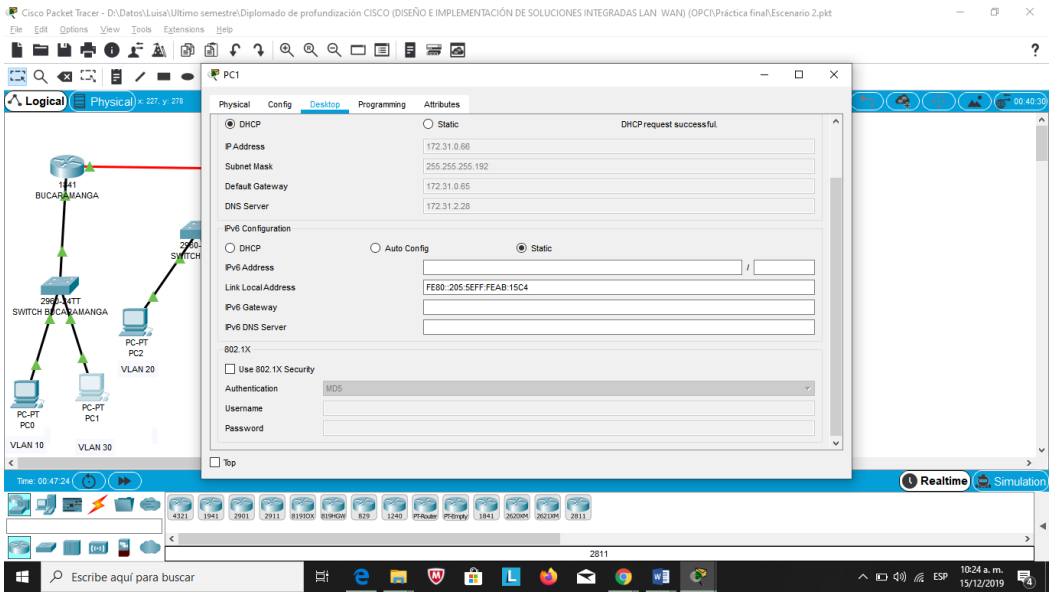
Configuración DHCP en los PC.

Ilustración 14. DHCP PC0.



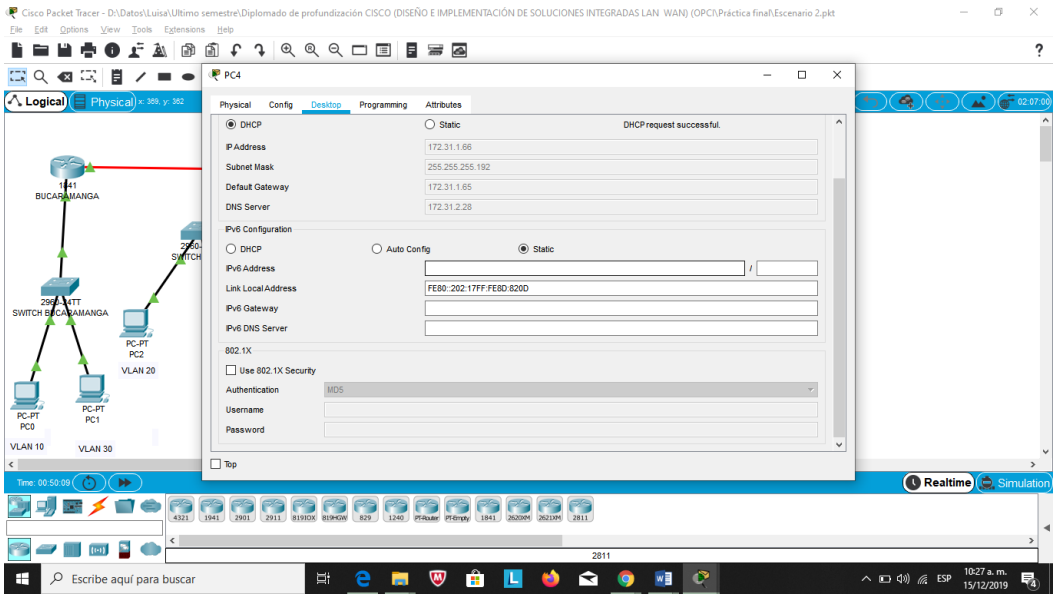
Fuente: Propia.

Ilustración 15. DHCP PC1.



Fuente: Propia.

Ilustración 16. DHCP PC4.

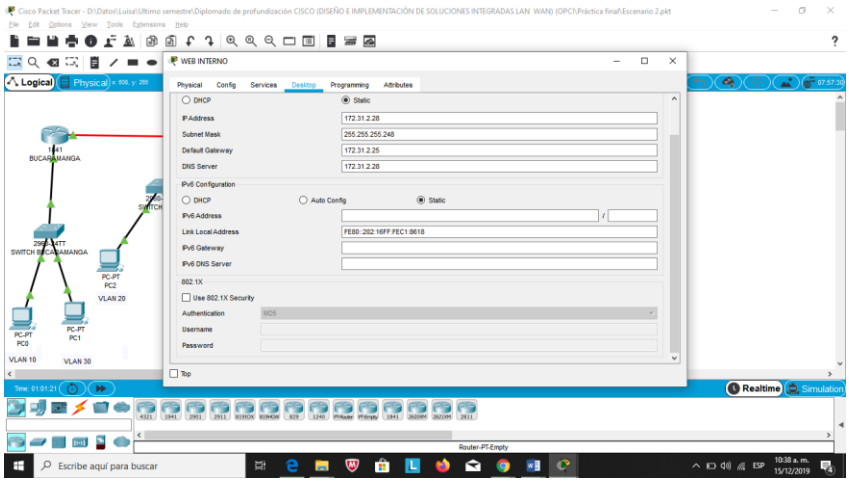


Fuente: Propia.

8. Configuración Web Server con NAT estático.

Se configura el web server con NAT estático y el resto de los equipos de la topología emplean NAT de sobrecarga (PAT).

Ilustración 17. Configuración Web Server.



Fuente: Propia.

TUNJA

```
Acceso Restringido!

User Access Verification

Username: admin
Password:
TUNJA>enable
Password:
TUNJA#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
TUNJA(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)#end
TUNJA#
%SYS-5-CONFIG_I: Configured from console by console

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, 01:07:25,
Serial0/0/0
O          172.31.0.64/26 [110/65] via 172.31.2.34, 01:07:25,
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, 01:07:25,
Serial0/0/1
O          172.31.1.64/26 [110/65] via 172.31.2.38, 01:07:25,
Serial0/0/1
O          172.31.2.0/29 [110/65] via 172.31.2.34, 01:07:25,
Serial0/0/0
O          172.31.2.8/29 [110/65] via 172.31.2.38, 01:07:25,
Serial0/0/1
O          172.31.2.24/29 [110/65] via 172.31.2.38, 01:07:25,
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#
```

BUCARAMANGA

```
Acceso Restringido!

User Access Verification

Username: admin
Password:
BUCARAMANGA>enable
Password:
BUCARAMANGA#configure terminal
```

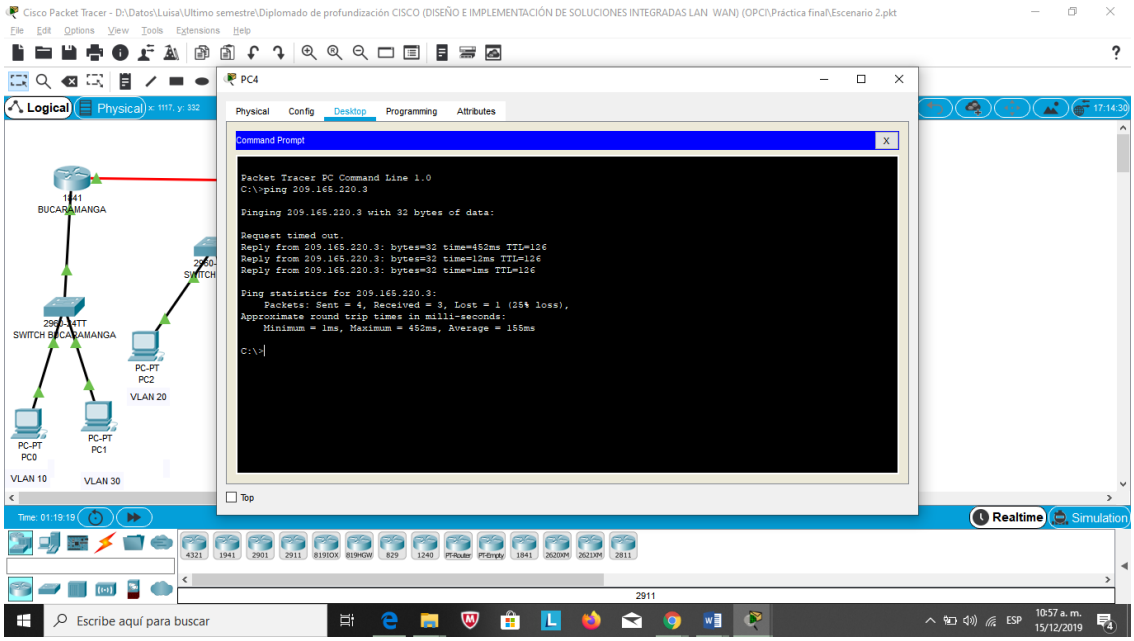
```
Enter configuration commands, one per line.  End with CNTL/Z.
BUCARAMANGA(config)#exit
BUCARAMANGA#
%SYS-5-CONFIG_I: Configured from console by console

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, 01:09:49, 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, 01:09:49,
Serial0/0/0
O         172.31.0.192/26 [110/65] via 172.31.2.33, 01:09:49,
Serial0/0/0
O          172.31.1.0/26 [110/129] via 172.31.2.33, 01:09:49,
Serial0/0/0
O         172.31.1.64/26 [110/129] via 172.31.2.33, 01:09:49,
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, 01:09:49,
Serial0/0/0
O         172.31.2.24/29 [110/129] via 172.31.2.33, 01:09:49,
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, 01:09:49,
Serial0/0/0
O*E2 0.0.0.0/0 [110/1] via 172.31.2.33, 00:02:32, Serial0/0/0

BUCARAMANGA#
```

CUNDINAMARCA

```
Acceso Restringido!

User Access Verification

Username: admin
Password:
CUNDINAMARCA>enable
Password:
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, 01:11:13, 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, 01:11:13,
Serial0/0/0
O         172.31.0.64/26 [110/129] via 172.31.2.37, 01:11:13,
Serial0/0/0
O         172.31.0.128/26 [110/65] via 172.31.2.37, 01:11:13,
Serial0/0/0
O         172.31.0.192/26 [110/65] via 172.31.2.37, 01:11:13,
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, 01:11:13,
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, 01:11:13,
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, 00:04:01, Serial0/0/0
```

CUNDINAMARCA#

Ilustración 18. Prueba de conexión.



Fuente: Propia.

9. Se configura el enrutamiento para que tenga autenticación.

TUNJA

```
TUNJA#configure terminal
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 lufe1995
01:30:42: %OSPF-5-ADJCHG: Process 1, Nbr 172.31.2.34 on Serial0/0/0 from FULL to DOWN, Neighbor Down: Dead timer expired

01:30:42: %OSPF-5-ADJCHG: Process 1, Nbr 172.31.2.34 on Serial0/0/0 from FULL to DOWN, Neighbor Down: Interface down or detached

TUNJA(config-if)#ip ospf message-digest-key 1 md5 lufe1995
```

```
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 lufe1995
TUNJA(config-if)#
```

BUCARAMANGA

```
01:30:40: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.220.1 on Serial0/0/0 from FULL to DOWN, Neighbor Down: Dead timer expired

01:30:40: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.220.1 on Serial0/0/0 from FULL to DOWN, Neighbor Down: Interface down or detached

Acceso Restringido!

User Access Verification

Username: admin
Password:
BUCARAMANGA>enable
Password:
BUCARAMANGA#configure terminal
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 lufe1995
BUCARAMANGA(config-if)#
BUCARAMANGA(config-if)#
01:34:41: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.220.1 on Serial0/0/0 from LOADING to FULL, Loading Done

BUCARAMANGA(config-if)#
```

CUNDINAMARCA

```
01:32:12: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.220.1 on Serial0/0/0 from FULL to DOWN, Neighbor Down: Dead timer expired
```

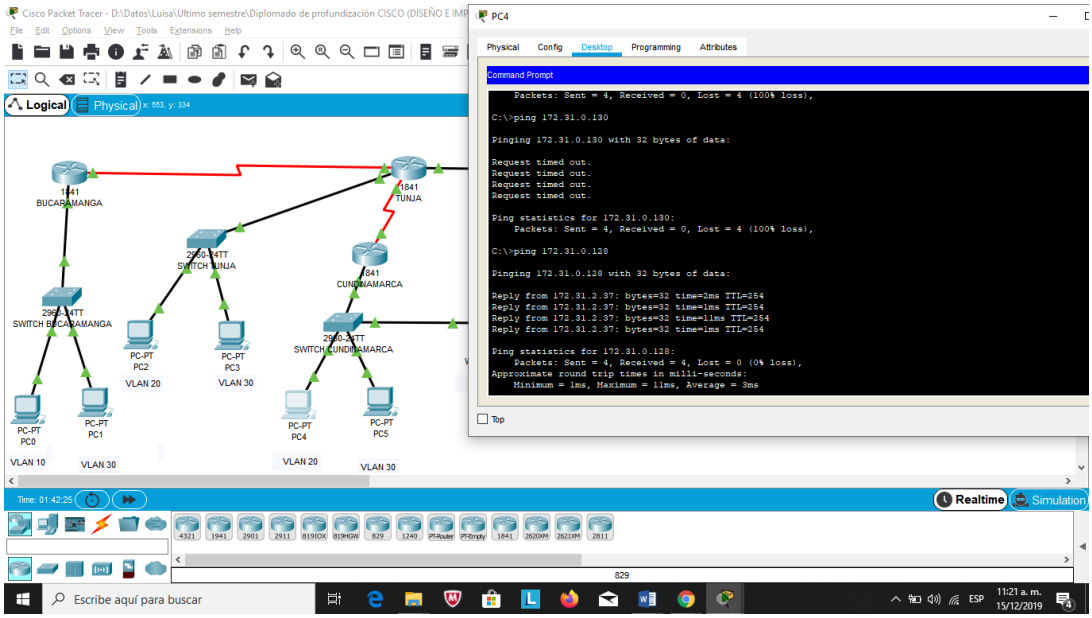
```
01:32:12: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.220.1 on Serial0/0/0 from FULL to DOWN, Neighbor Down: Interface down or detached

Acceso Restringido!

User Access Verification

Username: admin
Password:
CUNDINAMARCA>enable
Password:
CUNDINAMARCA#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
CUNDINAMARCA(config)#int s0/0/0
CUNDINAMARCA(config-if)#ip ospf authentication message-digest
CUNDINAMARCA(config-if)#ip ospf message-digest-key 1 md5 lufe1995
CUNDINAMARCA(config-if)#
01:36:52: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.220.1 on Serial0/0/0 from LOADING to FULL, Loading Done

CUNDINAMARCA(config-if)#
```

10. 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)#
```

Ilustración 19. Prueba.

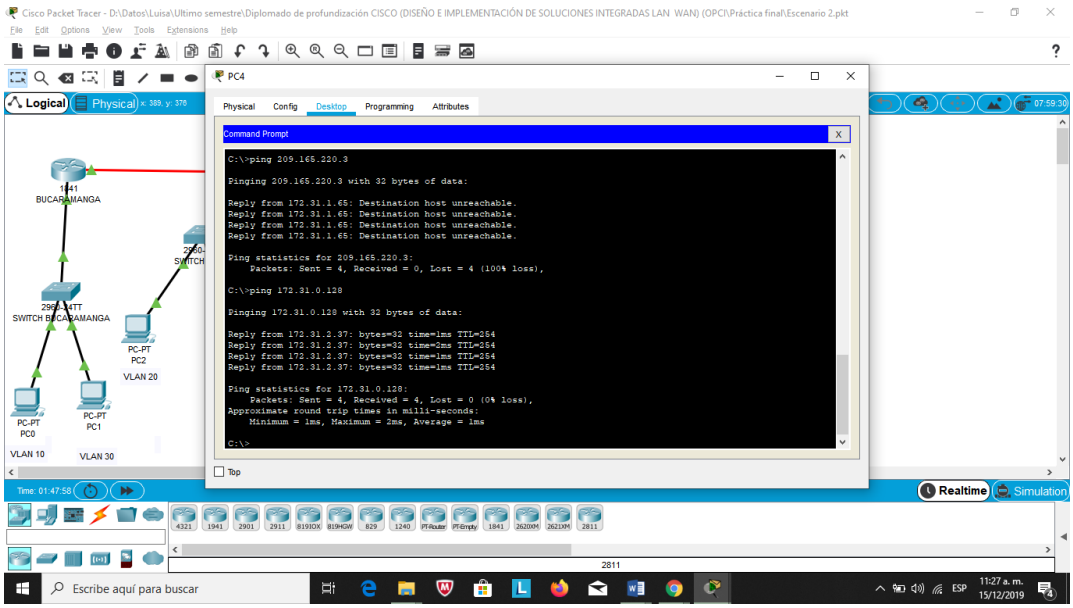


Fuente: Propia.

- 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)#
```

Ilustración 20. Prueba.

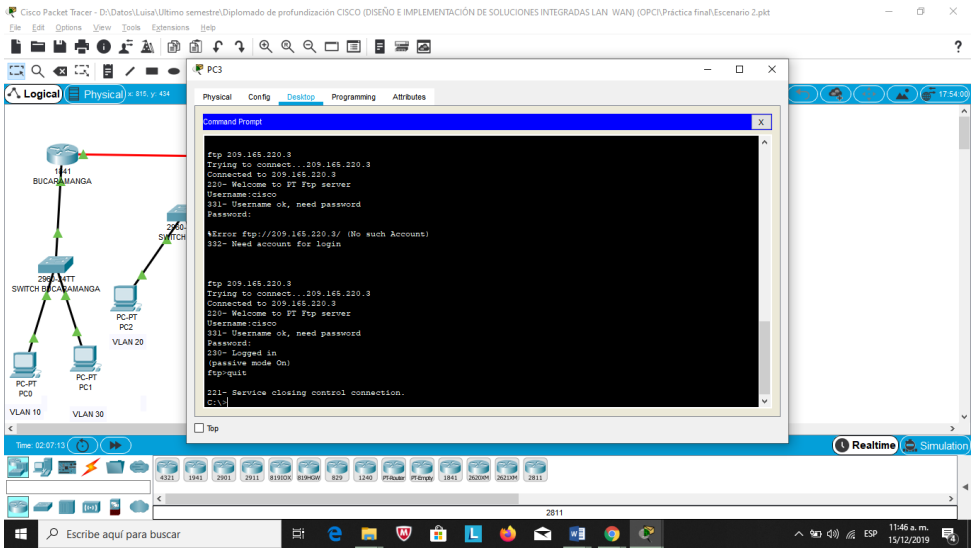


Fuente: Propia.

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

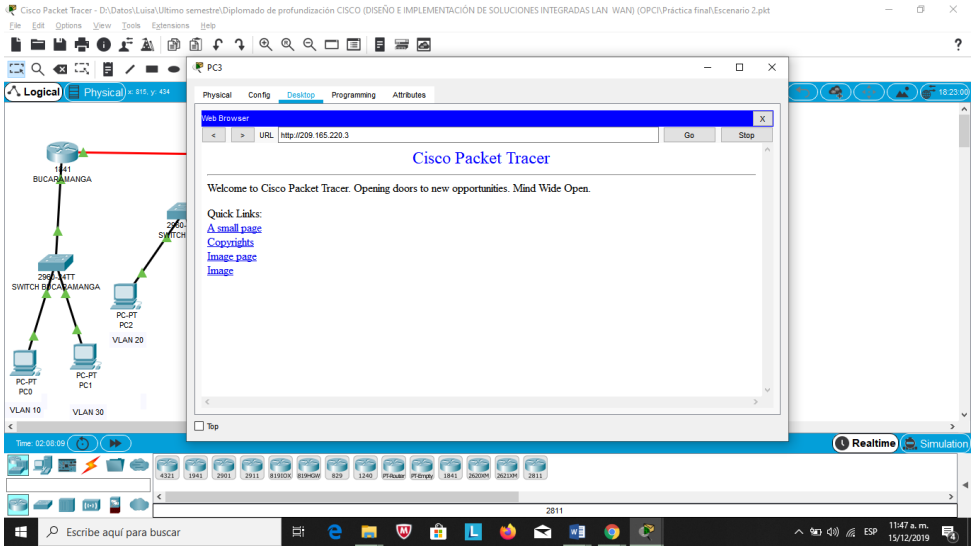
```
Acceso Restringido!

User Access Verification

Username: admin
Password:
TUNJA>enable
Password:
TUNJA#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
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)#
```

Ilustración 21. Prueba 1.



Fuente: Propia.

Ilustración 22. Prueba 2.

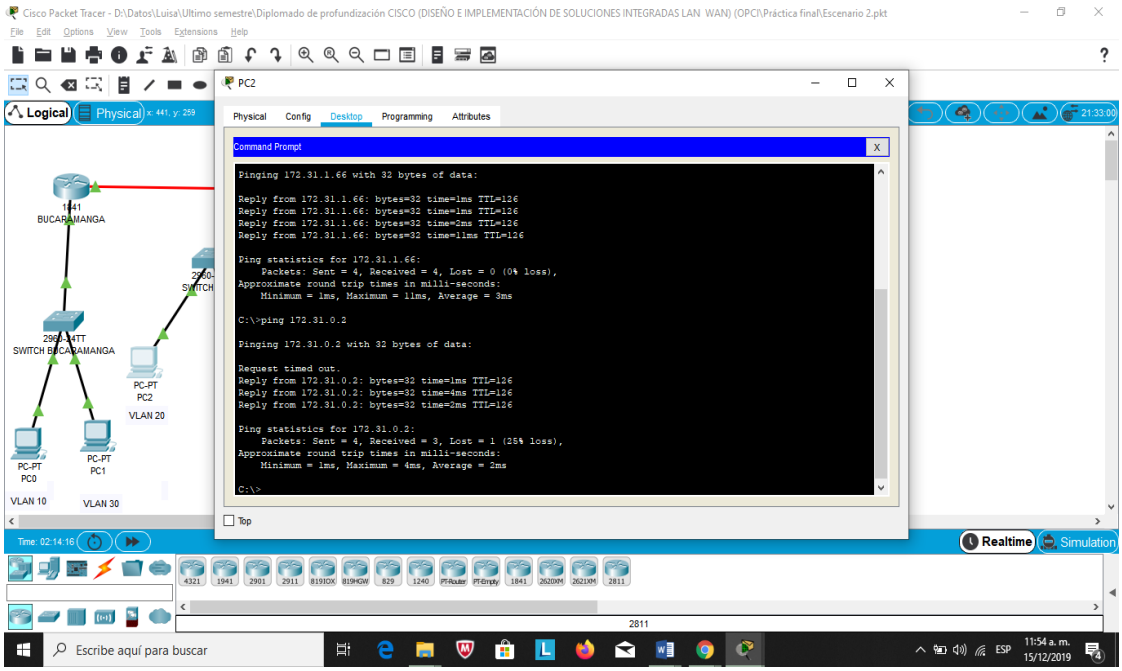


Fuente: Propia.

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

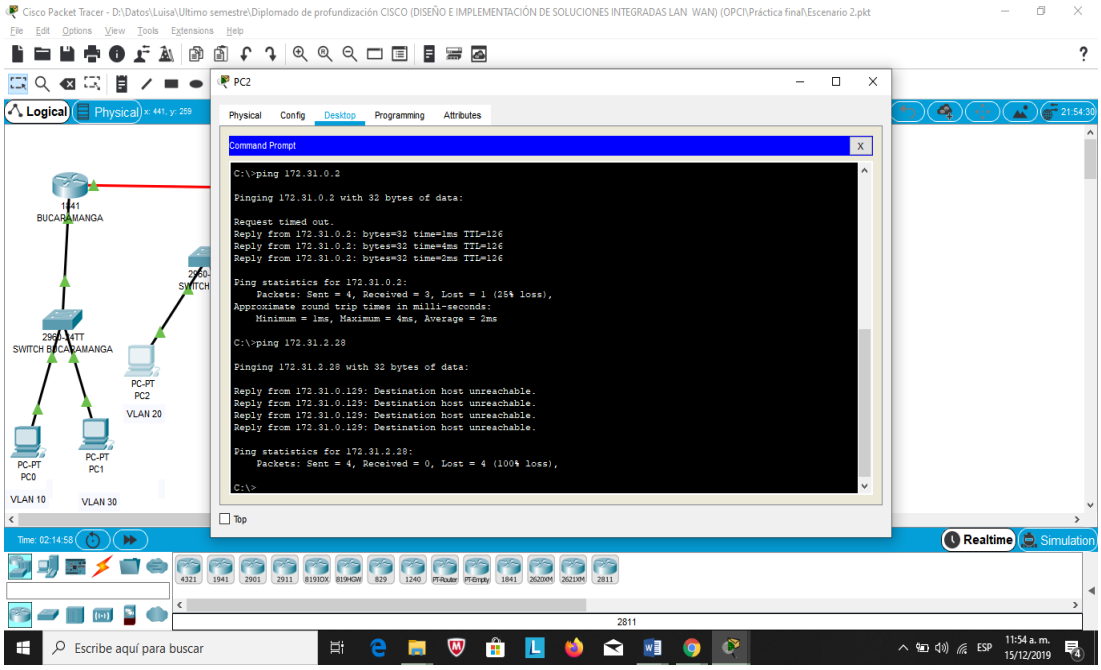
```
User Access Verification

Username: admin
Password:
TUNJA>enable
Password:
TUNJA#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
TUNJA(config)#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
```

Ilustración 23. Prueba 1.



Fuente: Propia.

Ilustración 24. Prueba 2.

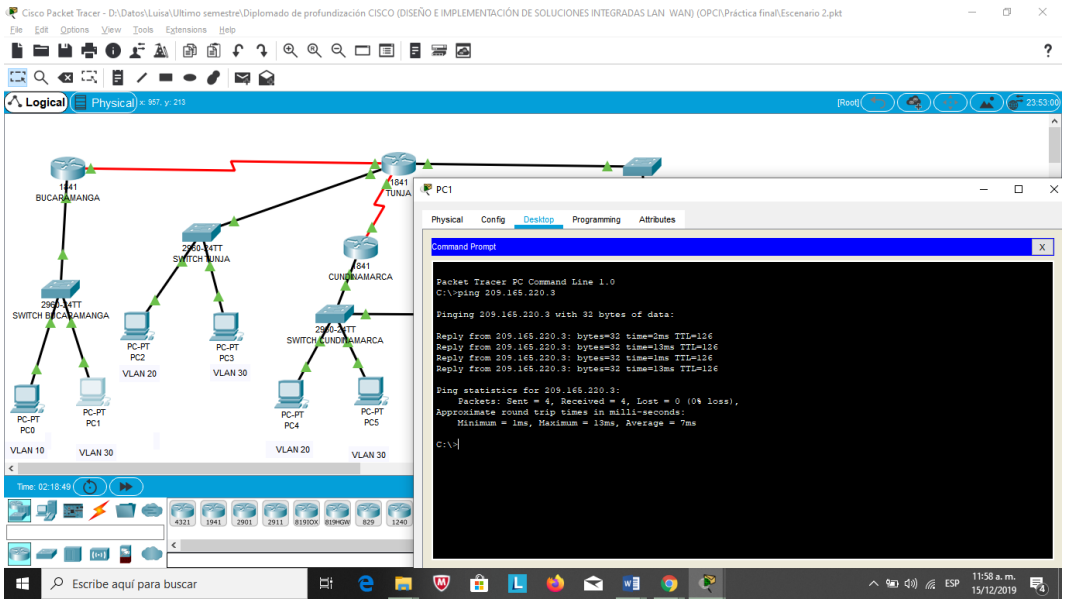


Fuente: Propia.

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

```
Acceso Restringido!

User Access Verification

Username: admin
Password:
BUCARAMANGA>enable
Password:
BUCARAMANGA#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
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)#
BUCARAMANGA(config-subif)#
```

Ilustración 25. Prueba 1.

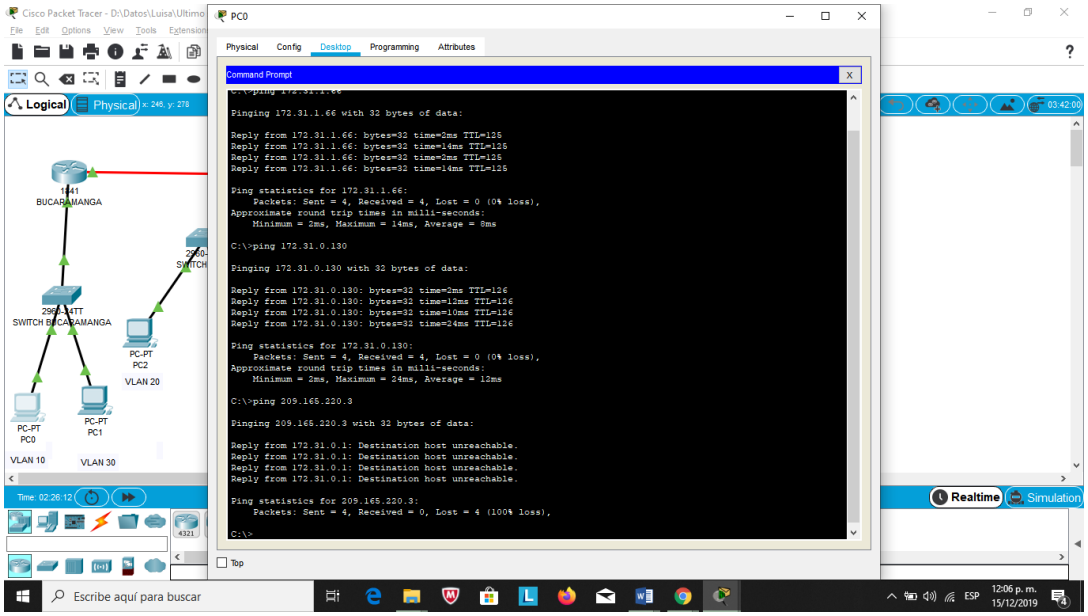


Fuente: Propia.

- 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)#
```

Ilustración 26. Prueba 1.



Fuente: Propia.

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

TUNJA

```
Acceso Restringido!

User Access Verification

Username: admin
Password:
TUNJA>enable
Password:
TUNJA#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
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)#
```

CUNDINAMARCA

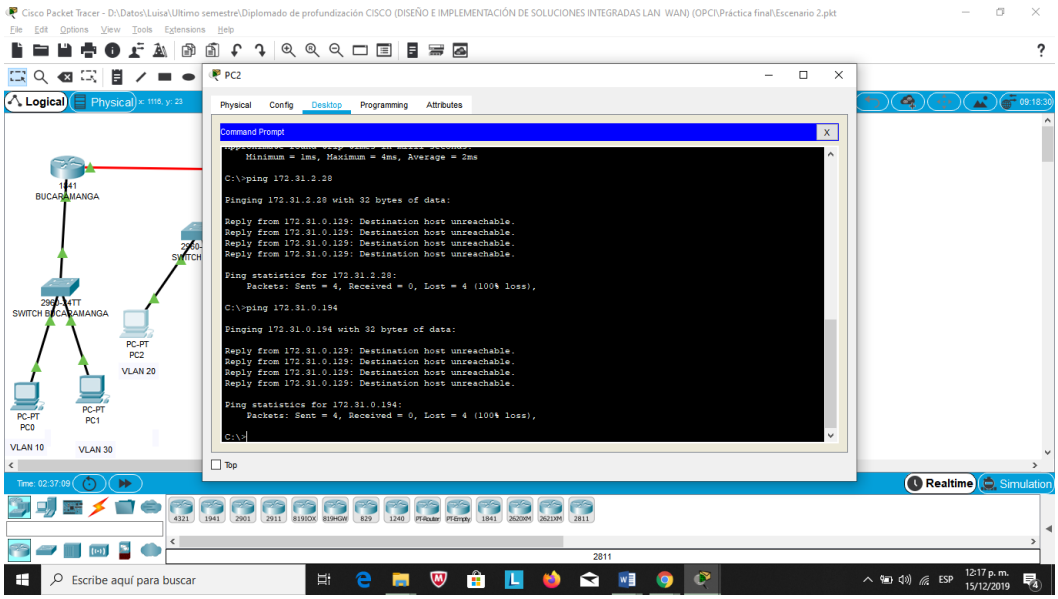
User Access Verification

```
Username: admin
Password:
CUNDINAMARCA>enable
Password:
CUNDINAMARCA#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
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)#
```

BUCARAMANGA

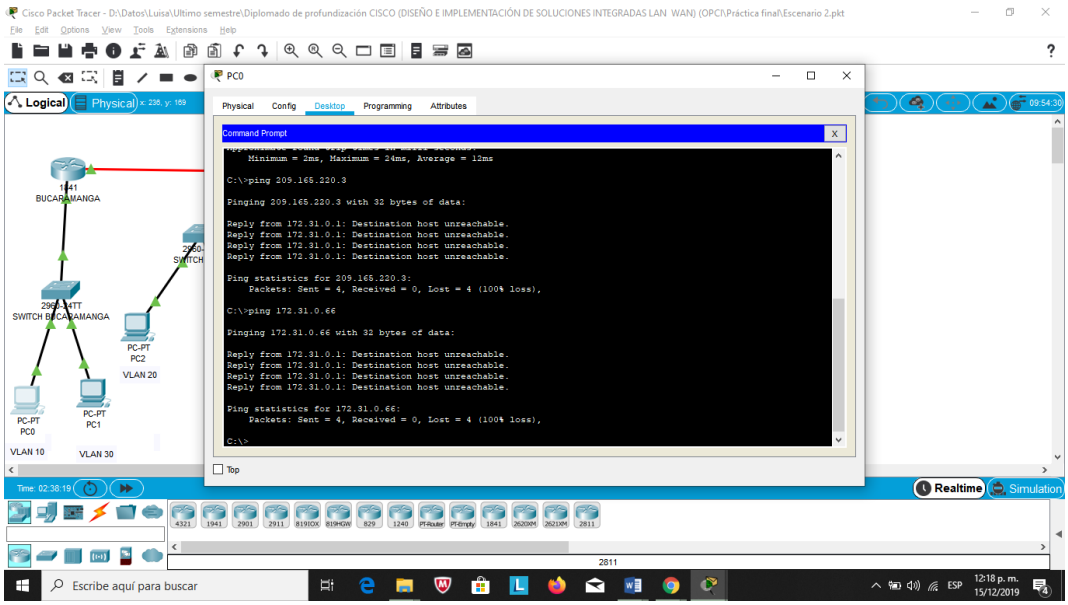
```
BUCARAMANGA(config-subif)#access-list  113  deny  ip  172.31.2.0
0.0.0.7 172.31.0.0 0.0.0.63
BUCARAMANGA(config)#access-list   113   deny   ip   172.31.0.64
0.0.0.63 172.31.0.0 0.0.0.63
BUCARAMANGA(config)#access-list 113 permit ip any any
BUCARAMANGA(config)#int f0/0.10
BUCARAMANGA(config-subif)#ip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

Ilustración 27. Prueba 1.



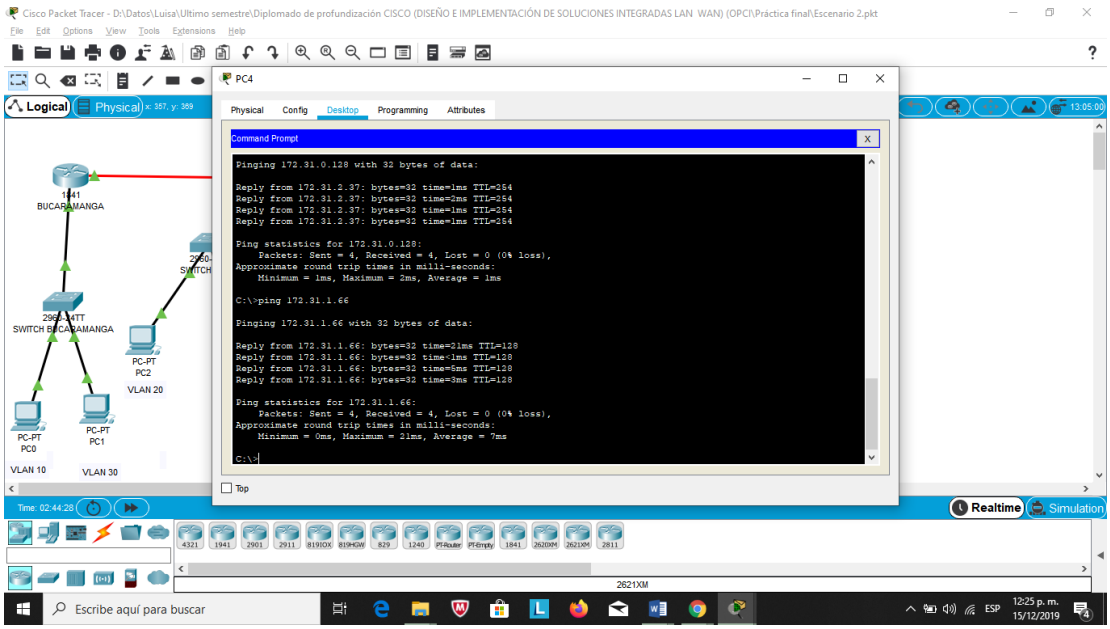
Fuente: Propia.

Ilustración 28. Prueba 2.



Fuente: Propia.

Ilustración 29. Prueba 3.



Fuente: Propia.

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

TUNJA

```
Acceso Restringido!

User Access Verification

Username: admin
Password:
TUNJA>enable
Password:
TUNJA#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
TUNJA(config)#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
```

```
TUNJA(config-line)#
```

CUNDINAMARCA

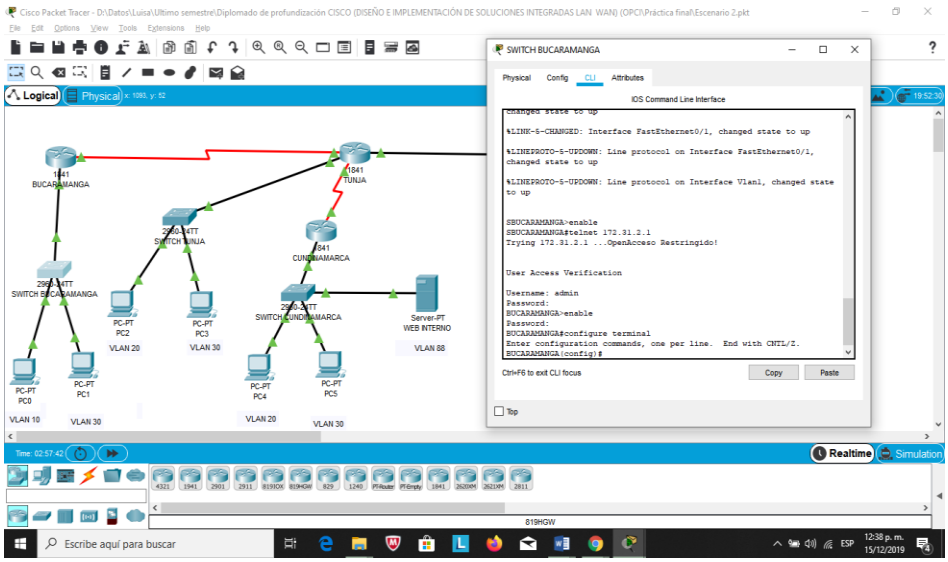
Acceso Restringido!

```
User Access Verification

Username: admin
Password:
CUNDINAMARCA>enable
Password:
CUNDINAMARCA#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
CUNDINAMARCA(config)#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)#
```

BUCARAMANGA

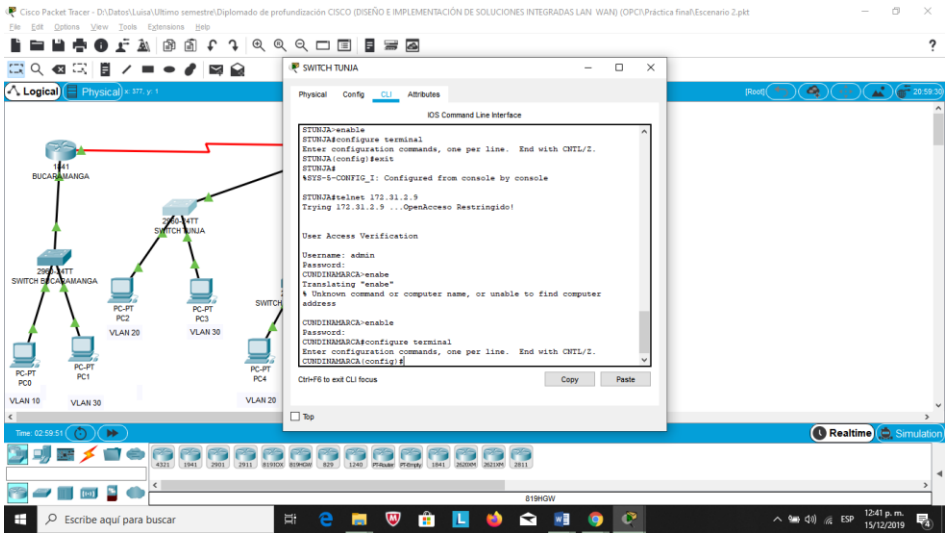
```
Acceso Restringido!

User Access Verification

Username: admin
Password:
BUCARAMANGA>enable
Password:
BUCARAMANGA#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
BUCARAMANGA(config)#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)#
```

Ilustración 30. Prueba 1.



Fuente: Propia.

Ilustración 31. Prueba 2.



Fuente: Propia.

CONCLUSIONES

- Se realizaron las topologías de red propuestas en la presente guía, así como también se configuraron los dispositivos por los cuales están compuestas, haciendo uso de los conocimientos adquiridos durante el desarrollo del presente diplomado.

- El protocolo DHCP permite que un equipo conectado a una red pueda obtener su configuración (principalmente, su configuración de red) en forma dinámica, es decir, sin la intervención del administrador.

- El mecanismo NAT es usado por los routers con el fin de intercambiar paquetes entre dos redes que tienen distintas direcciones.

- En el NAT estático se mapea una dirección IP privada con una dirección IP pública de forma estática. De esta manera, cada equipo en la red privada debe tener su correspondiente IP pública asignada para poder acceder a Internet.

- Las listas de acceso ACL son usadas para determinar los permisos de acceso apropiados a un determinado objeto, dependiendo de la configuración que se realice.

- El principal objetivo de las ACL es filtrar tráfico, permitiendo o denegando el tráfico de red de acuerdo con alguna condición.

BIBLIOGRAFÍA

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

CISCO. (2014). OSPF de una sola área. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module8/index.html#8.0.1.1

CISCO. (2014). Listas de control de acceso. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module9/index.html#9.0.1.1

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

CISCO. (2014). Traducción de direcciones IP para IPv4. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module11/index.html#11.0.1.1

Vesga, J. (2014). Principios de Enrutamiento [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgOyjWeh6timi_Tm