PRUEBA DE HABILIDADES PRACTICAS CCNA

ARMANDO JOSE GUERRA CANTILLO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIAS
PROGRAMA INGENIERIA DE SISTEMAS
BARRANQUILLA, ATLANTICO
2019

PRUEBA DE HABILIDADES PRACTICAS CCNA

ARMANDO JOSE GUERRA CANTILLO

TUTOR:

ING. GIOVANNI BRACHO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIAS
PROGRAMA INGENIERIA DE SISTEMAS
BARRANQUILLA, ATLANTICO
2019

Nota de aceptación

_____
_____
_____
_____
_____
_____

_____
Firma del presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

Contenido

Resumen 5
Abstrac 6
Introducción 7
1. Objetivos…….. 8
1.1. Objetivo General 8
1.2. Objetivos Específicos……..8
2. Escenario 1.....9
2.1. Parte 1: Asignación de direcciones IP…….10
2.2. Parte 2: Configuración Básica…….....11
2.3. Parte 3: Configuración de Enrutamiento.....17
2.4. Parte 4: Configuración de las listas de Control de Acceso……22
2.5. Parte 5: comprobación de la red instalada……..28
3. Escenario 2……..... 29
3.1Configuración básica…….....30
3.1.1 Autenticación local con AAA……..39
3.1.2 Cifrado de contraseñas……...39
3.1.3 Un máximo de internos para acceder al router……...40
3.1.4 Máximo tiempo de acceso al detectar ataques……40
3.2. El DHCP proporcionar solo direcciones a los hosts ..... .41
3.3. El enrutamiento deberá tener autenticación…….....46
3.4. Listas de control de acceso…….....48
4. Conclusiones……..60
5. Referencias Bibliografía..……..61

RESUMEN

Entender el papel tan importante que desempeñan las redes y el uso de las tecnologías que aplican al mundo de las redes a nivel mundial y que en nuestro país ha tenido un gran desarrollo durante los últimos 10 años con una amplia cobertura del internet en Colombia, alcanzando coberturas en la mayoría de la población.

EL uso de todo tipo de topologías y redes de ha convertido en una necesidad muy importante en las instituciones educativas como colegios, universidades, empresas, hospitales, empresas públicas y privadas las cuales necesitan optimizar su desempeño y gestiones.

Razón por la cual este curso de CISCO para soluciones integradas LAN/WAN pone a prueba todas las habilidades y conocimientos previos los cuales mediante un estudio y análisis previo se han llevado a una construcción y diseño mediante ayuda del programa PACKET TRACER en cual es una simulación real a casos prácticos y comunes que incluye todas las herramientas necesarias para ejecutar diferentes requerimientos , es así que en el estudio del curso se aplicó los conocimientos de los dos módulos tanto del módulo CCNA 1 R&S y el módulo CCNA 2 R&S en convenio con CISCO Networking Academy el cual mediante un trabajo paralelo y la plataforma de la universidad nacional abierta y a distancia UNAD se logró llevar un trabajo continuo y de mucho apoyo.

Abstract

Understand the important role that networks play and the use of technologies that apply to the world of networks worldwide and that in our country has had a great development during the last 10 years with a wide coverage of the internet in Colombia, reaching coverage in the majority of the population.

The use of all types of topologies and networks has become a very important need in educational institutions such as schools, universities, companies, hospitals, public and private companies which need to optimize their performance and management.

Reason why this course of CISCO for integrated solutions LAN / WAN tests all the previous skills and knowledge which through a previous study and analysis have led to a construction and design by means of the PACKET TRACER program in which is a simulation Real to practical and common cases that includes all the necessary tools to execute different requirements, it is so in the study of the course I applied the knowledge of the two modules of the module CCNA 1 R & S and the module CCNA 2 R & S in agreement with CISCO Networking Academy which through a parallel work and the platform of the national university open and distance UNAD was able to carry a continuous work and a lot of support.

INTRODUCCIÓN

A lo largo de los dos cursos tanto como del CCNA-1 y CCNA-2 se han venido desarrollando una cantidad importante de actividades , así como de evaluaciones de los 21 capítulos que contienen los dos cursos , simultáneamente se han venido trabajando un número significativo de ejercicios prácticos en la plataforma de la UNAD los cuales han sido en su totalidad prácticos y colaborativos , en conjunto con las dos plataformas tanto de CISCO NETCAP como la de la universidad nacional abierta y a distancia se lograron varias metas que son de suprema importancia en el campo profesional en la implementación de soluciones de redes LAN y WAN con un amplio sentido teórico y práctico en participación y apoyo de grupos de trabajo .

Razón por la cual en esta práctica de habilidades se pondrá todo nuestro conocimiento aprendido durante las dos partes del curso y a su vez fortalecerá la versatilidad y desempeño como futuros profesionales.

Objetivos

Objetivo General

Implementar las destrezas, habilidades y conocimientos en el área de redes que permitan evidenciar el desempeño aprendido durante las dos unidades del curso CISCO que conlleven a crear soluciones prácticas y reales a cada uno de los ambientes propuestos.

Objetivos Específicos

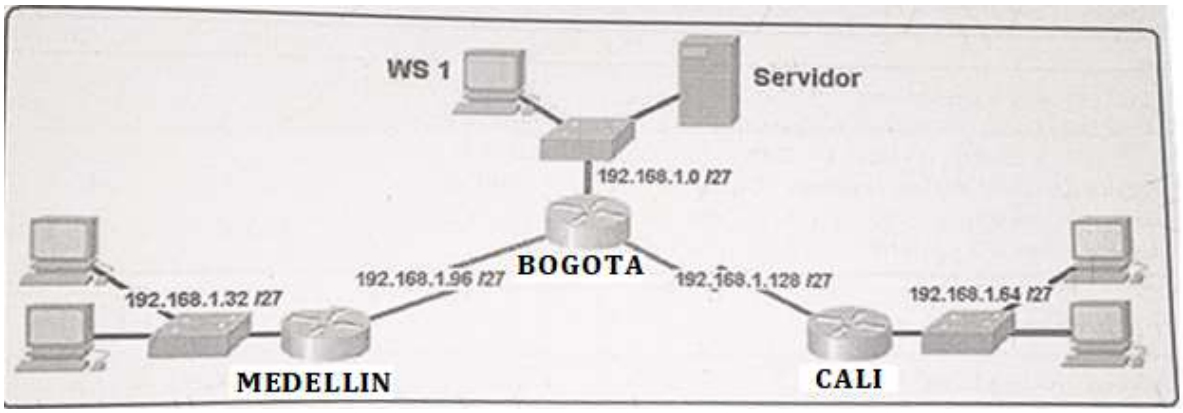
- Identificar la topología mediante un análisis general para luego aplicar los dispositivos más acordes al escenario planteado
- Configurar dispositivos de comunicación como: servidores, Routers y Switch.
- Implementar los protocolos necesarios para que las redes tengan una seguridad confiable
- Aplicar el protocolo DHCP y NAT en dispositivos de comunicación.
- Revisar la conectividad entre los dispositivos realizada a los dos escenarios que fueron propuestos para el desarrollo de la actividad.

DESARROLLO DE LA ACTIVIDAD

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



Desarrollo

Como trabajo inicial se debe realizar lo siguiente.

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

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

Parte 1: Asignación de direcciones IP:

a. Se debe dividir (subnetear) la red creando una segmentación en ocho partes, para permitir creciemiento futuro de la red corporativa.

Para subnetear la red se utilizó la formula 2n donde N será los números de dígitos del ultimo octeto de la macará 255.255.255.0000. Para ello tomamos 3 dígitos de dicho octeto, quedando como resultado: 23 =8, lo correcto sería tomarlo a 24 para tener más de 8 subredes dado que de cada red se deben de dejar de utilizar 2 redes que son la dirección de red y la dirección de Broadcast pero siguiendo el gráfico del escenario donde ya hay unas direcciones definidas con una máscara con prefijo 27 se muestra que se utilizó 23 de esa manera se obtienen 8 redes pero se tiene claro que solo será utilizadas 6 redes en total.

No	Subred	Primera IP utilizable	Ultima IP utilizable	Broadcast
1	192.168.1.0	192.168.1.1	192.168.1.30	192.168.1.31
2	192.168.1.32	192.168.1.33	192.168.1.62	192.168.1.63
3	192.168.1.64	192.168.1.65	192.168.1.94	192.168.1.95
4	192.168.1.96	192.168.1.97	192.168.1.126	192.168.1.127
5	192.168.1.128	192.168.1.129	192.168.1.158	192.168.1.159
6	192.168.1.160	192.168.1.161	192.168.1.190	192.168.1.191
7	192.168.1.192	192.168.1.193	192.168.1.122	192.168.1.123
8	192.168.1.224	192.168.1.225	192.168.1.254	192.168.1.255

b. Asignar una dirección IP a la red.

MEDELLÍN

UserAccess Verification

Password: Medellin>enable

Password:

Hostname>MEDELLIN

MEDELLIN(config)#interface Serial0/1/0

MEDELLIN(config-if)#ip address 192.168.1.99 255.255.255.224

MEDELLIN(config-if)#no shutdown

MEDELLIN(config)#interface GigabitEthernet0/0

MEDELLIN(config-if)#ip address 192.168.1.33 255.255.255.224

BOGOTÁ

Router#config t Router(config)#hostname

BOGOTA BOGOTA(config)#interface

Serial0/1/0

BOGOTA(config-if)#ip address 192.168.1.98 255.255.255.224

BOGOTA(config-if)#no shutdown

BOGOTA(config)#interface Serial0/1/1

BOGOTA(config-if)#ip address 192.168.1.130 255.255.255.224

BOGOTA(config-if)#no shutdown

BOGOTA(config)#interface GigabitEthernet0/0

BOGOTA(config-if)#ip address 192.168.1.1 255.255.255.224

BOGOTA(config-if)#no shutdow

CALI

Router#config t

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

CALI

CALI(config)#interface GigabitEthernet0/0

CALI(config)#interface Serial0/1/0

CALI(config-if)#ip address 192.168.1.131 255.255.255.224

CALI(config-if)#no shutdown

CALI(config)#interface GigabitEthernet0/0

CALI(config-if)#ip address 192.168.1.65 255.255.255.224

CALI(config-if)#no shutdown

Parte 2: Configuración Básica.

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

Se asignan todas las direcciones ip y se agrega el protocolo de enrutamiento para permitir la conexión.

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

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

Se comprueba el direccionamiento ip mediante la tabla de enrutamiento de los routers

BOGOTA>enable Password:
BOGOTA#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type2 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
- candidate default, U - per-user static route, o - ODR P - periodic downloaded static route
Gateway of last resort is not set 192.168.1.0/27 is subnetted, 5 subnets

C 192.168.1.0 is directly connected, FastEthernet0/0
D 192.168.1.32 [90/2172416] via 192.168.1.99, 05:26:26, Serial0/0
D 192.168.1.64 [90/2172416] via 192.168.1.131, 05:26:23, Serial0/1
C 192.168.1.96 is directly connected, Serial0/0 C 192.168.1.128 is directly connected, Serial0/1

MEDELLIN>enable Password:
MEDELLIN#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type2 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
- candidate default, U - per-user static route, o - ODR P - periodic downloaded static route

Gateway of last resort is not set

192.168.1.0/27 is subnetted, 5 subnets
D 192.168.1.0 [90/2172416] via 192.168.1.98, 05:31:25, Serial0/0
C 192.168.1.32 is directly connected, FastEthernet0/0
D 192.168.1.64 [90/2684416] via 192.168.1.98, 05:31:22, Serial0/0
C 192.168.1.96 is directly connected, Serial0/0
D 192.168.1.128 [90/2681856] via 192.168.1.98, 05:31:25, Serial0/0

CALI>enable Password:
CALI#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type2 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
- candidate default, U - per-user static route, o - ODR P - periodic downloaded static route
Gateway of last resort is not set 192.168.1.0/27 is subnetted, 5 subnets
D 192.168.1.0 [90/2172416] via 192.168.1.130, 05:32:24, Serial0/0
D 192.168.1.32 [90/2684416] via 192.168.1.130, 05:32:24, Serial0/0
C 192.168.1.64 is directly connected, FastEthernet0/0
D 192.168.1.96 [90/2681856] via 192.168.1.130, 05:32:24, Serial0/0

C 192.168.1.128 is directly connected, Serial0/0

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

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

Utilizando el comando show ip route se realizó el balanceo de carga de cada router

Medellin>en
Medellin#show ip route 192.168.1.131
Routing entry for 192.168.1.128/27
Known via "eigrp 200", distance 90, metric 2681856, type internal
Redistributing via eigrp 200
Last update from 192.168.1.98 on Serial0/1/0, 00:23:15 ago
Routing Descriptor Blocks:
* 192.168.1.98, from 192.168.1.98, 00:23:15 ago, via Serial0/1/0
Route metric is 2681856, traffic share count is 1
Total delay is 40000 microseconds, minimum bandwidth is 1544 Kbit
Reliability 255/255, minimum MTU 1500 bytes
Loading 1/255, Hops 1

Medellin#show ip route 192.168.1.1
Routing entry for 192.168.1.0/27
Known via "eigrp 200", distance 90, metric 2172416, type internal
Redistributing via eigrp 200
Last update from 192.168.1.98 on Serial0/1/0, 00:25:32 ago
Routing Descriptor Blocks:
* 192.168.1.98, from 192.168.1.98, 00:25:32 ago, via Serial0/1/0
Route metric is 2172416, traffic share count is 1
Total delay is 20100 microseconds, minimum bandwidth is 1544 Kbit
Reliability 255/255, minimum MTU 1500 bytes
Loading 1/255, Hops 1

Cali>en
Cali#show ip route 192.168.1.33
Routing entry for 192.168.1.32/27
Known via "eigrp 200", distance 90, metric 2684416, type internal
Redistributing via eigrp 200
Last update from 192.168.1.130 on Serial0/1/0, 00:26:43 ago
Routing Descriptor Blocks:
* 192.168.1.130, from 192.168.1.130, 00:26:43 ago, via Serial0/1/0
Route metric is 2684416, traffic share count is 1
Total delay is 40100 microseconds, minimum bandwidth is 1544 Kbit

Reliability 255/255, minimum MTU 1500 bytes
Loading 1/255, Hops 2

Bogota>en

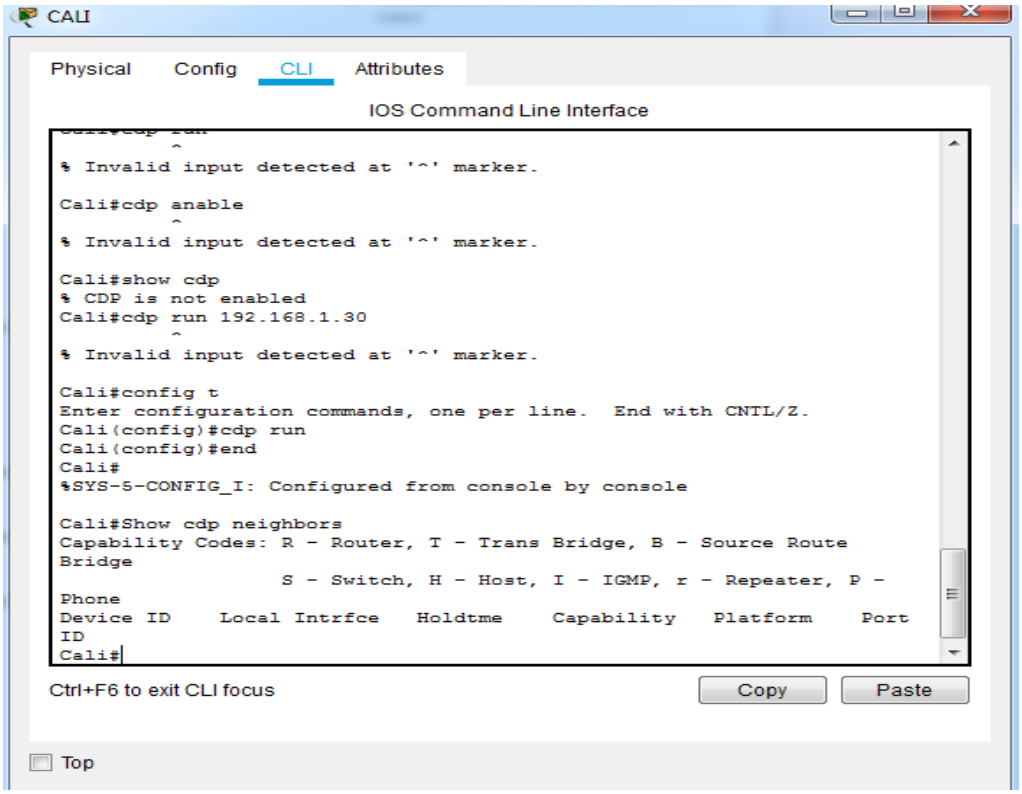
Bogota#show ip route 192.168.1.33 Routing
entry for 192.168.1.32/27
Known via "eigrp 200", distance 90, metric 2172416, type internal
Redistributing via eigrp 200
Last update from 192.168.1.99 on Serial0/1/0, 00:27:29 ago
Routing Descriptor Blocks:
* 192.168.1.99, from 192.168.1.99, 00:27:29 ago, via Serial0/1/0
Route metric is 2172416, traffic share count is 1
Total delay is 20100 microseconds, minimum bandwidth is 1544 Kbit
Reliability 255/255, minimum MTU 1500 bytes
Loading 1/255, Hops 1

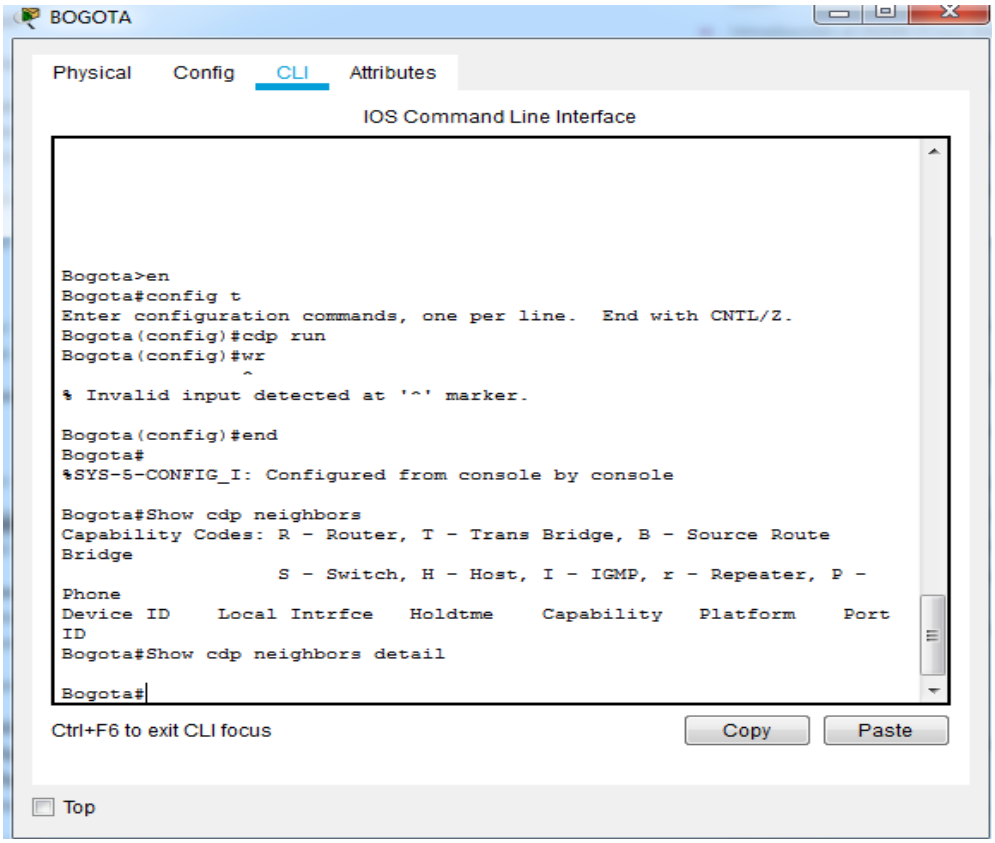
d. Realizar un diagnóstico de vecinos uando el comando cdp.

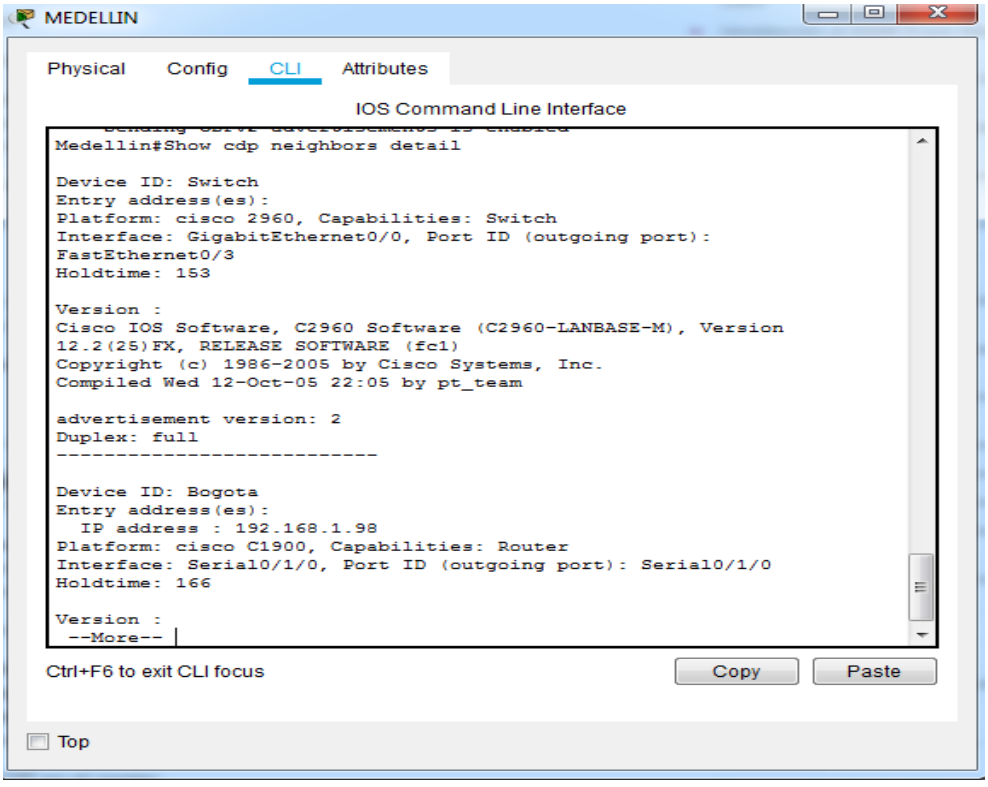
Se activó el comando cdp asi:

Configure terminal cdp run.

Realizo el diagnostico de vecinos utilizando el comando **Show cdp neighbors**



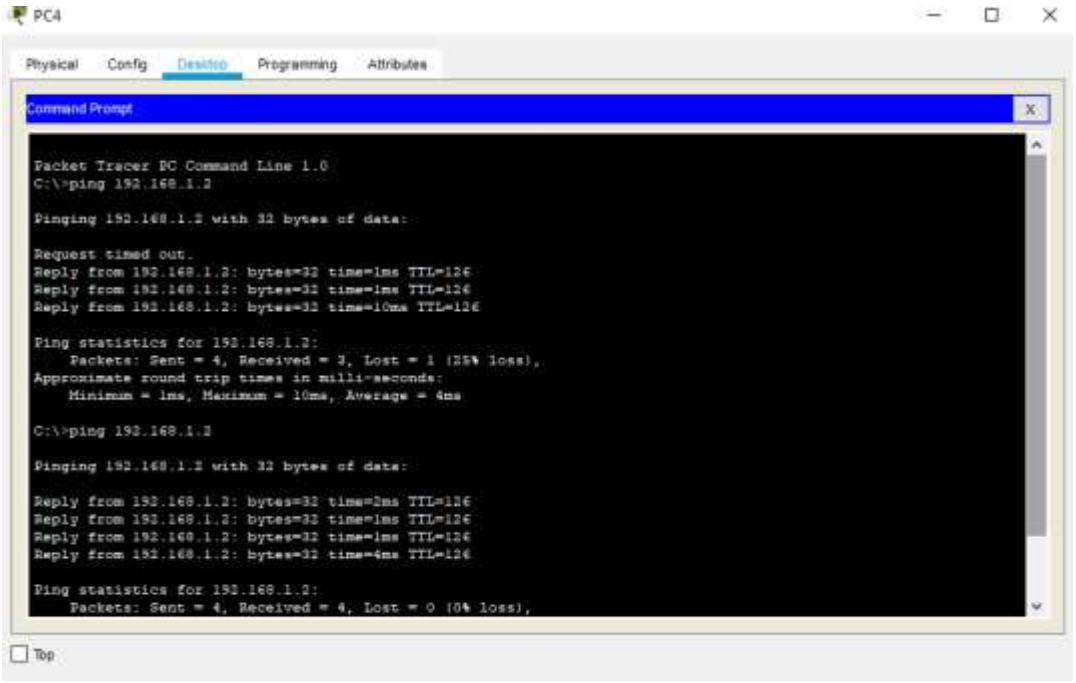

BOGOTA
Physical
Config
CLI
Attributes
IOS Command Line Interface
Bogota>en
Bogota#config t
Enter configuration commands, one per line. End with CNTL/Z.
Bogota(config)#cdp run
Bogota(config)#wr
^
% Invalid input detected at '^' marker.
Bogota(config)#end
Bogota#
%SYS-5-CONFIG_I: Configured from console by console
Bogota#Show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route
Bridge
S - Switch, H - Host, I - IGMP, r - Repeater, P -
Phone
Device ID Local Intrfce Holdtme Capability Platform Port
ID
Bogota#Show cdp neighbors detail
Bogota#
Ctrl+F6 to exit CLI focus
Copy
Paste
Top

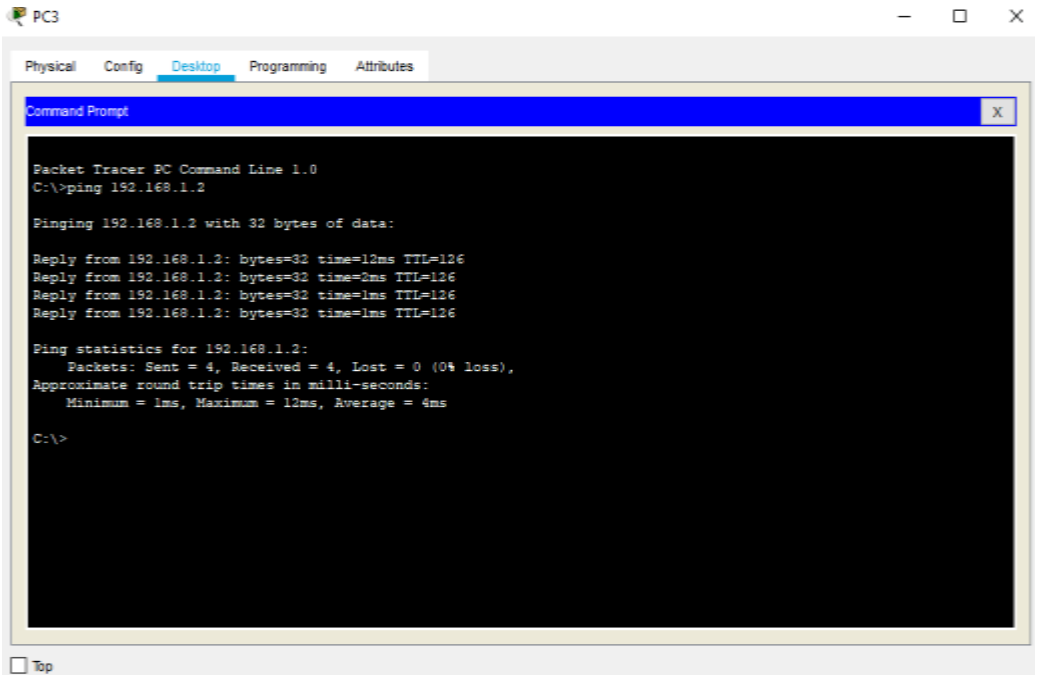

MEDELLIN
Physical
Config
CLI
Attributes
IOS Command Line Interface
Medellin#Show cdp neighbors detail
Device ID: Switch
Entry address(es):
Platform: cisco 2960, Capabilities: Switch
Interface: GigabitEthernet0/0, Port ID (outgoing port):
FastEthernet0/3
Holdtime: 153
Version :
Cisco IOS Software, C2960 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: Serial0/1/0, Port ID (outgoing port): Serial0/1/0
Holdtime: 166
Version :
--More--
Ctrl+F6 to exit CLI focus
Copy
Paste
Top

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

Se envian los respectivos mensajes para verificar la conexión





Parte 3: Configuración de Enrutamiento.

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

BOGOTA>enabl

BOGOTA#config

terminal

Enter configuration commands, one per line. End with

CNTL/Z. BOGOTA(config)#router eigrp 200

BOGOTA(config-router)#no auto-

summary BOGOTA(config-

router)#network 192.168.1.96

BOGOTA(config-router)#network 192.168.1.0

BOGOTA(config-router)#network

192.168.1.128 BOGOTA(config-

router)#end

MEDELLIN>ENABLE

MEDELLIN#config terminal

Enter configuration commands, one per line. End with

CNTL/Z. MEDELLIN(config)#router eigrp 200

MEDELLIN(config-router)#no auto-

summary MEDELLIN(config-

router)#network 192.168.1.32

Router(config-router)#

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

adjacency

MDELLIN(config-router)#network 192.168.1.32

MEDELLIN(config-router)#network

192.168.1.96 MEDELLIN(config-

router)#end

CALI>enabl

e

CALI#config

terminal

Enter configuration commands, one per line. End with

CNTL/Z. CALI(config)#router eigrp 200

CALI(config-router)#no auto-

summary CALI(config-

router)#network 192.168.1.128

Router(config-router)#

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

new adjacency

CALI(config-router)#network 192.168.1.128

CALI(config-router)#network

192.168.1.64 CALI(config-

router)#end

CALI#

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

MEDELLIN>enable Password:
MEDELLIN#show ip eigrp neighbors IP-EIGRP neighbors for process 200
H Address Interface Hold Uptime SRTT RTO Q Seq

(sec) (ms) Cnt Num
0 192.168.1.98 Se0/0 13 00:08:19 40 1000 0 8
CALI>enable Password:
CALI#show ip eigrp neighbors
IP-EIGRP neighbors for process 200
H Address Interface Hold Uptime SRTT RTO Q Seq (sec) (ms) Cnt Num
0 192.168.1.98 Se0/0 13 00:08:19 40 1000 0 8

BOGOTA>enable Password:
BOGOTA#show ip eigrp neighbors IP-EIGRP neighbors for process 200
H Address Interface Hold Uptime SRTT RTO Q Seq (sec) (ms) Cnt Num
0 192.168.1.131 Se0/1 13 00:06:44 40 1000 0 7
1 192.168.1.99 Se0/0 10 00:06:43 40 1000 0 7

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

MEDELLI

N>enable

Password:
MEDELLIN>show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile,
B - BGP D - EIGRP, EX - EIGRP external, O - OSPF, IA -
OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA
external type2 E1 - OSPF external type 1, E2 - OSPF
external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static
route, o - ODR P - periodic downloaded
static route

Gateway of last resort is not set

192.168.1.0/27 is subnetted, 5 subnets
D 192.168.1.0 [90/2172416] via 192.168.1.98, 00:11:32, Serial0/0
C 192.168.1.32 is directly connected, FastEthernet0/0
D 192.168.1.64 [90/2684416] via 192.168.1.98, 00:11:32, Serial0/0
C 192.168.1.96 is directly connected, Serial0/0
D 192.168.1.128 [90/2681856] via 192.168.1.98, 00:11:32, Serial0/0

BOGOTA>enable

BOGOTA#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

192.168.1.0/27 is subnetted, 5 subnets
C 192.168.1.0 is directly connected, FastEthernet0/0
D 192.168.1.32 [90/2172416] via 192.168.1.99, 00:13:26, Serial0/0
D 192.168.1.64 [90/2172416] via 192.168.1.131, 00:13:28, Serial0/1
C 192.168.1.96 is directly connected, Serial0/0 C
192.168.1.128 is directly connected, Serial0/1

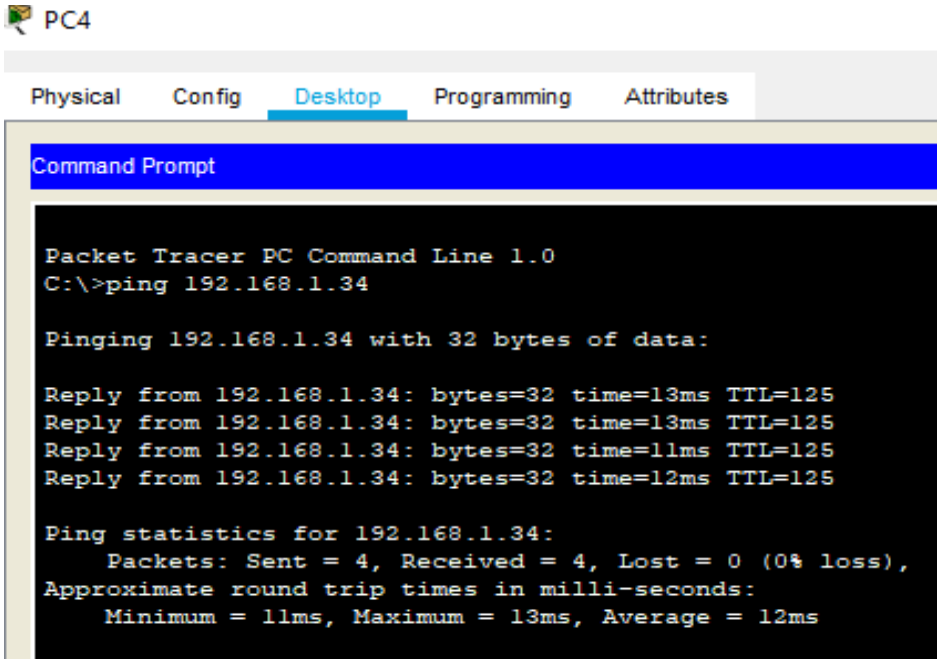
CALI>enable

Password:
CALI#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static
route, o - ODR P - periodic downloaded
static route
Gateway of last resort is not set

192.168.1.0/27 is subnetted, 5 subnets
D 192.168.1.0 [90/2172416] via 192.168.1.130, 00:14:20, Serial0/0
D 192.168.1.32 [90/2684416] via 192.168.1.130, 00:14:18, Serial0/0
C 192.168.1.64 is directly connected, FastEthernet0/0
D 192.168.1.96 [90/2681856] via 192.168.1.130, 00:14:18, Serial0/0
C 192.168.1.128 is directly connected, Serial0/0

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



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.**

Esto es para permitir solo acceso hacia el

servidor MEDELLIN>enable

Password:

MEDELLIN#configure terminal

Enter configuration commands, one per line. End with

CNTL/Z. MEDELLIN(config)#ip access-list extended

ServerPT

MEDELLIN(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.1.3 0.0.0.0

MEDELLIN(config-ext-nacl)#exit

MEDELLIN(config)#interface fa0/0

MEDELLIN(config-if)#ip access-group

ServerPT in MEDELLIN(config-if)#end

CALI>enable

Password: CALI#config terminal

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

CALI(config)#ip access-list extended ServerPT

CALI(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.1.3 0.0.0.0

CALI(config-ext-nacl)#exit

CALI(config)#int fa0/0

CALI(config-if)#ip access-group ServerPT in

CALI(config-if)#end

BOGOTA>enable

Password:

BOGOTA#config terminal

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

BOGOTA(config)#ip access-list extended ServerPT

BOGOTA(config-ext-nacl)#permit ip 192.168.1.3 0.0.0.0 0.0.0.0 255.255.255.255

BOGOTA(config-ext-nacl)#exit

BOGOTA(config)#interface fa0/0 BOGOTA(config-

if)#ip access-group ServerPT in BOGOTA(config-

if)#end

MEDELLIN>enable

Password:

MEDELLIN#config terminal

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

MEDELLIN(config)#ip access-list extended ServerPT

MEDELLIN(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.1.33 0.0.0.0

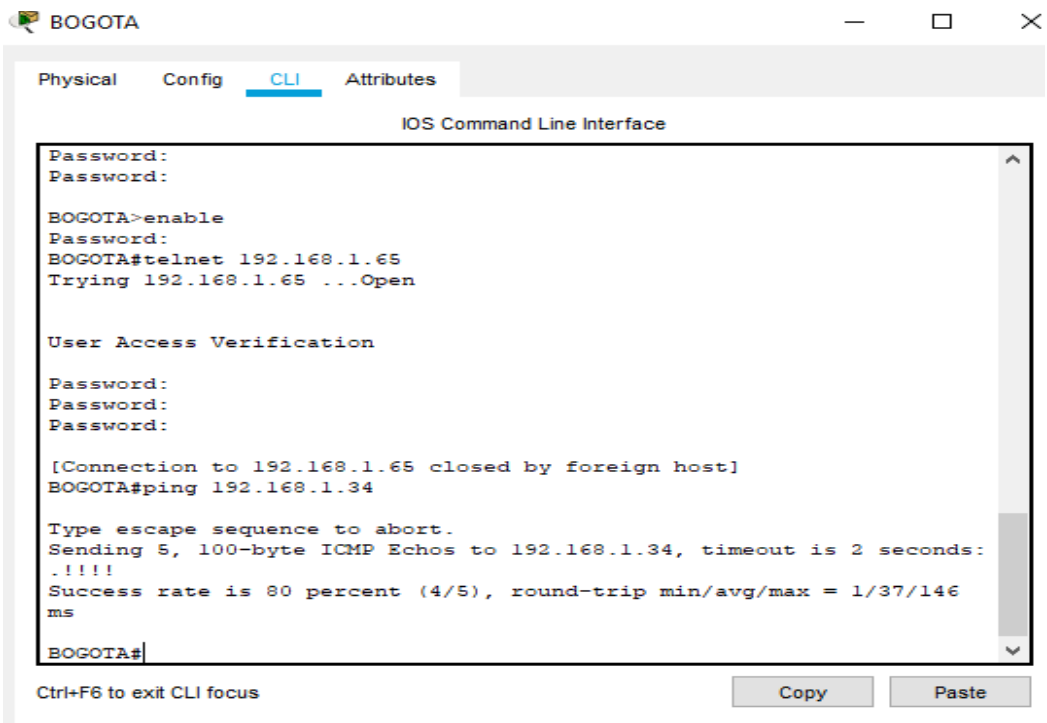
MEDELLIN(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.1.98 0.0.0.0

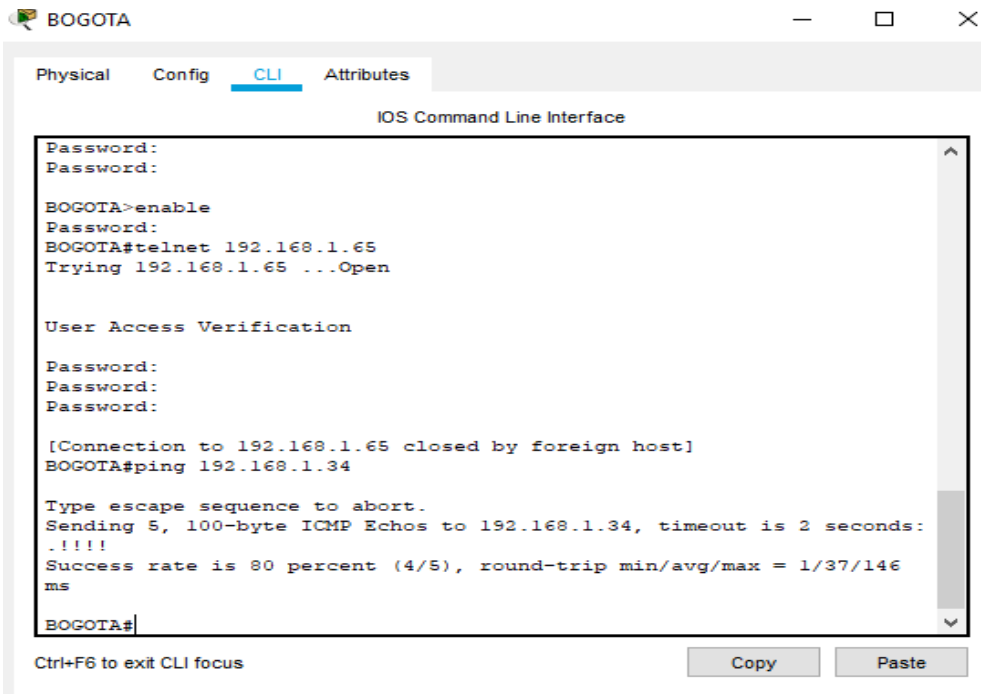
MEDELLIN(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.1.131 0.0.0.0

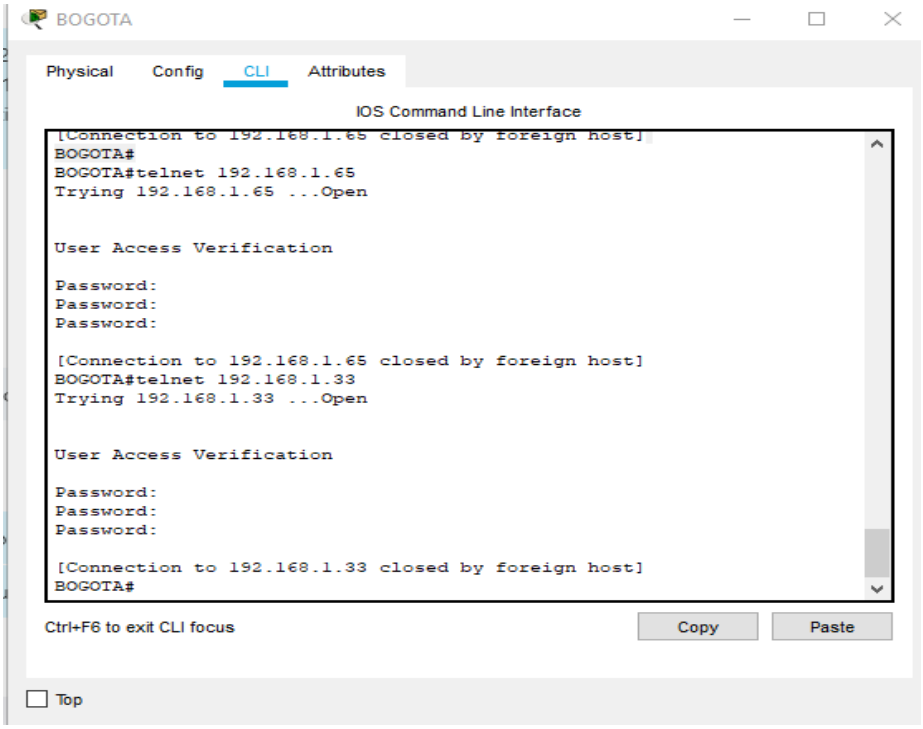
MEDELLIN(config-ext-nacl)#end

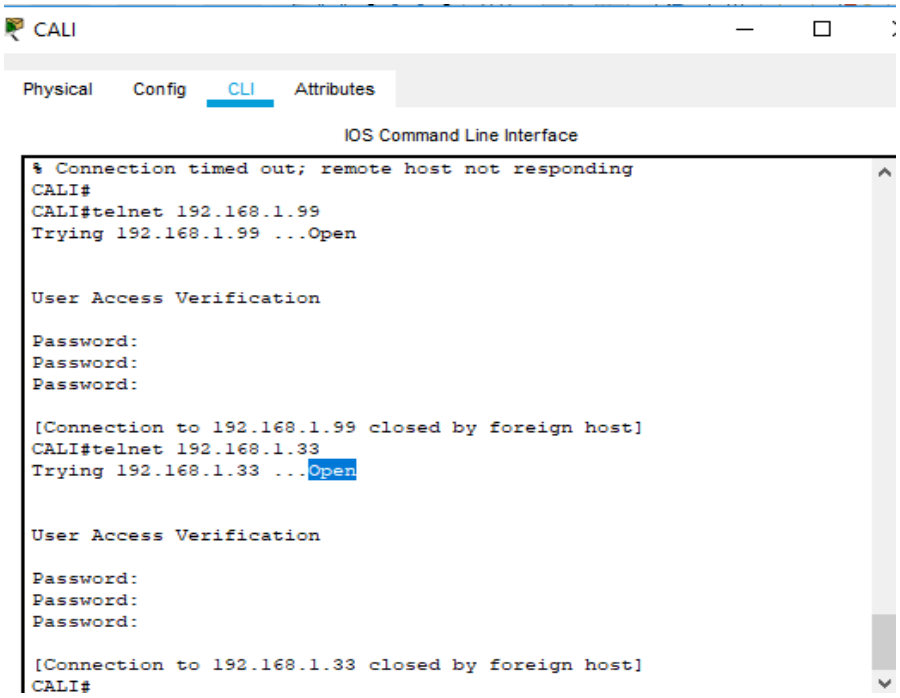
BOGOTA#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA(config)#ip access-list extended ServerPT
BOGOTA(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.1.99 0.0.0.0
BOGOTA(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.1.1 0.0.0.0
BOGOTA(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.1.131 0.0.0.0
BOGOTA(config-ext-nacl)#end

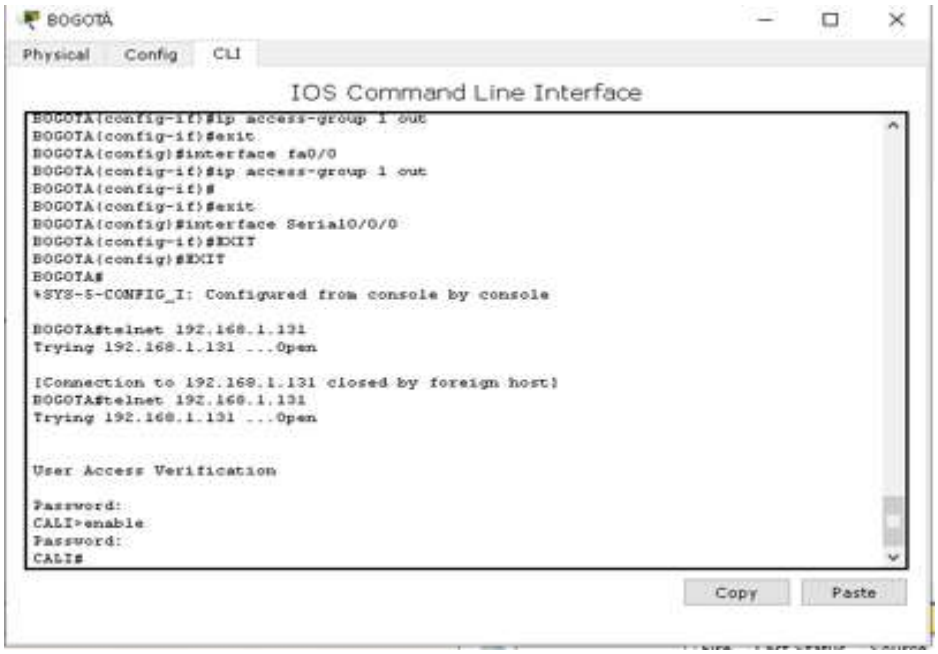
CALI>enable
Password:
Password:
CALI#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
CALI(config)#ip access-list extended ServerPT
CALI(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.1.99 0.0.0.0
CALI(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.1.1 0.0.0.0
CALI(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.1.65 0.0.0.0
CALI(config-ext-nacl)#end Cada router debe estar habilitado para establecer conexiones Telnet con los demás routers y tener acceso a cualquier dispositivo en la red.




BOGOTA
Physical
Config
CLI
Attributes
IOS Command Line Interface
Password:
Password:
BOGOTA>enable
Password:
BOGOTA#telnet 192.168.1.65
Trying 192.168.1.65 ...Open
User Access Verification
Password:
Password:
Password:
[Connection to 192.168.1.65 closed by foreign host]
BOGOTA#ping 192.168.1.34
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.34, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/37/146
ms
BOGOTA#
Ctrl+F6 to exit CLI focus
Copy
Paste


BOGOTA
Physical
Config
CLI
Attributes
IOS Command Line Interface
[Connection to 192.168.1.65 closed by foreign host]
BOGOTA#
BOGOTA#telnet 192.168.1.65
Trying 192.168.1.65 ...Open
User Access Verification
Password:
Password:
Password:
[Connection to 192.168.1.65 closed by foreign host]
BOGOTA#telnet 192.168.1.33
Trying 192.168.1.33 ...Open
User Access Verification
Password:
Password:
Password:
[Connection to 192.168.1.33 closed by foreign host]
BOGOTA#
Ctrl+F6 to exit CLI focus
Copy
Paste
Top





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.

```
MEDELLIN>enable Password:
MEDELLIN#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN(config)#ip access-list extended ServerPT
MEDELLIN(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.1.33
0.0.0.0
MEDELLIN(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.1.98
0.0.0.0
MEDELLIN(config-ext-nacl)#permit    ip        0.0.0.0          255.255.255.255
     192.168.1.131
0.0.0.0
MEDELLIN(config-ext-nacl)#end

BOGOTA#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA(config)#ip access-list extended ServerPT
BOGOTA(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.1.99
0.0.0.0
BOGOTA(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.1.1
0.0.0.0

BOGOTA(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.1.131
0.0.0.0
BOGOTA(config-ext-nacl)#end

CALI>enable Password:
Password:
CALI#config terminal
Enter configuration commands, one per line. End with CNTL/Z. CALI(config)#ip
access-list extended ServerPT
CALI(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.1.99 0.0.0.0
CALI(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.1.1 0.0.0.0
CALI(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.1.65 0.0.0.0
CALI(config-ext-nacl)#end
```

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.

MEDELLIN>enable Password:
MEDELLIN#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN(config)#ip access-list extended ServerPT
MEDELLIN(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.1.3 0.0.0.0
MEDELLIN(config-ext-nacl)#exit MEDELLIN(config)#int f0/0
MEDELLIN(config-if)#ip access-group ServerPT in
MEDELLIN(config-if)#end

CALI>enable Password:
CALI#config t
Enter configuration commands, one per line. End with CNTL/Z.
CALI(config)#ip access-list extended ServerPT
CALI(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.1.3 0.0.0.0
CALI(config-ext-nacl)#exit
CALI(config)#int f0/0
CALI(config-if)#ip access-group ServerPT in CALI(config-if)#end

Parte 5: Comprobación de la red instalada.

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

MEDELLIN#
MEDELLIN#show
Access-list Extended IP
access list ServerPT 10
permit ip any host
192.168.1.3
20 permit ip any host 192.168.1.33
30 permit ip any host 192.168.1.98
40 permit ip any host 192.168.1.131

BOGOTA>enable

Password:
BOGOTA#show
access-list
Extended IP access list
ServerPT 10 permit ip
host 192.168.1.3 any
20 permit ip any host 192.168.1.99
30 permit ip any host 192.168.1.1
40 permit ip any host 192.168.1.131

CALI>enable Password:
CALI#show access-list
Extended IP access list ServerPT
10 permit ip any host 192.168.1.3
20 permit ip any host 192.168.1.99
30 permit ip any host 192.168.1.1
40 permit ip any host 192.168.1.65

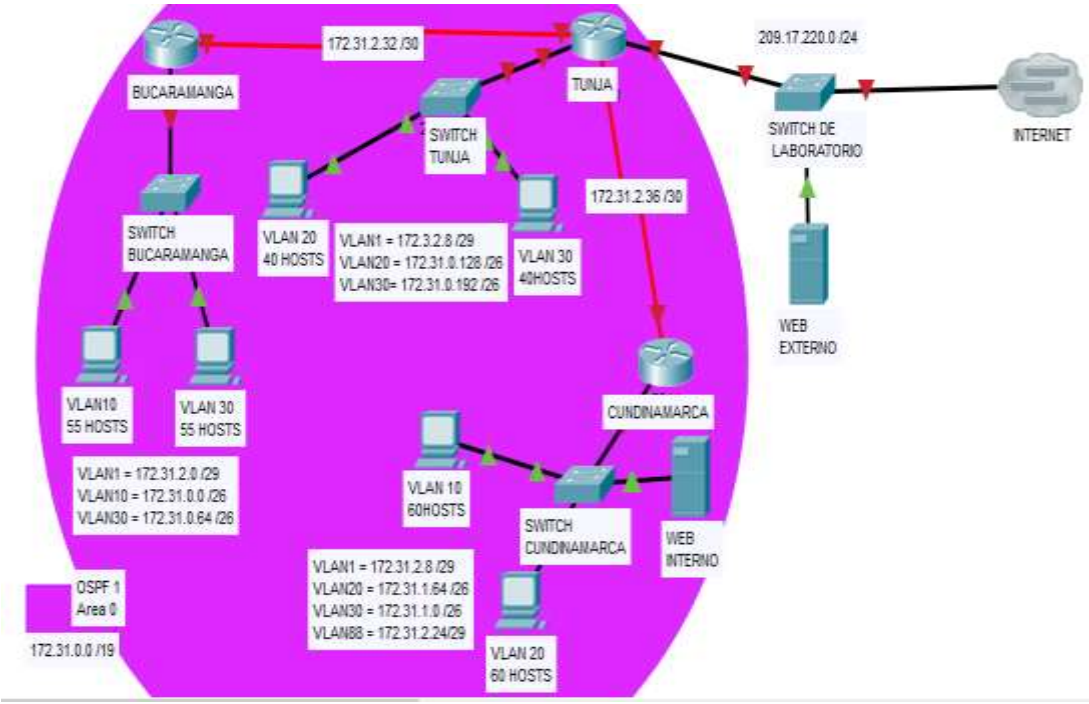
b. Comprobar y Completar la siguiente tabla de condiciones de prueba para confirmar el óptimo funcionamiento de la red.

	ORIGEN	DESTINO	RESULTADO
TELNET	**Router MEDELLIN**	**Router CALI**	SUCCESSFULL
	WS_1	**Router BOGOTA**	SUCCESSFULL
	Servidor	**Router CALI**	SUCCESSFULL
	Servidor	**Router MEDELLIN**	SUCCESSFULL
TELNET	**LAN del Router MEDELLIN**	**Router CALI**	Connection timed out; remote host not responding
	LAN del Router CALI	**Router CALI**	SUCCESSFULL
	LAN del Router MEDELLIN	**Router MEDELLIN**	SUCCESSFULL
	LAN del Router CALI	**Router MEDELLIN**	Connection timed out; remote host not responding

PING	**LAN del Router CALI**	**WS_1**	FAILED
	LAN del Router MEDELLIN	**WS_1**	FAILED
	LAN del Router MEDELLIN	**LAN del Router CALI**	FAILED
PING	**LAN del Router CALI**	**Servidor**	SUCCESSFULL
	LAN del Router MEDELLIN	**Servidor**	SUCCESSFULL
	Servidor	**LAN del Router MEDELLIN**	SUCCESSFULL
	Servidor	**LAN del Router CALI**	SUCCESSFULL
	Router CALI	**LAN del Router MEDELLIN**	FAILED
	Router MEDELLIN	**LAN del Router CALI**	FAILED

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.**

Router>en

Router#conf term

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

Router(config)#hostname BUCARAMANGA

BUCARAMANGA(config)#no ip domain-lookup

BUCARAMANGA(config)#banner motd #Cuidado Acceso Restringido#

BUCARAMANGA(config)#enable secret class123

BUCARAMANGA(config)#line console 0

BUCARAMANGA(config-line)#password cisco123

BUCARAMANGA(config-line)#login
BUCARAMANGA(config-line)#logging
synchronous BUCARAMANGA(config-
line)#line vty 0 15 BUCARAMANGA(config-
line)#password cisco123
BUCARAMANGA(config-line)#login
BUCARAMANGA(config-line)#logging
synchronous 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)#
BUCARAMANGA(config-if)#
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)#
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
```

BUCARAMANGA#

```
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)#banner motd #Cuidado Acceso
Restringido# TUNJA(config)#enable secret
class123
TUNJA(config)#line console 0
TUNJA(config-line)#password
cisco123 TUNJA(config-
line)#login
TUNJA(config-line)#logging
synchronous TUNJA(config-
line)#line vty 0 15
TUNJA(config-line)#password
cisco123 TUNJA(config-
line)#login
TUNJA(config-line)#logging
synchronous 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 shutdown

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 shutdown

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 shutdown

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
TUNJA(config-if)#int f0/1
TUNJA(config-if)#ip address 209.165.220.1255.255.255.0
TUNJA(config-if)#no shutdown

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 area0
TUNJA(config-router)#network 172.31.0.192 0.0.0.63 area0
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#
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

TUNJA#

```
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)#banner motd #Cuidado Acceso Restringido#
CUNDINAMARCA(config)#enable secret class123
CUNDINAMARCA(config)#line console 0
CUNDINAMARCA(config-line)#password cisco123
CUNDINAMARCA(config-line)#login
CUNDINAMARCA(config-line)#logging synchronous
CUNDINAMARCA(config-line)#line vty 0 15
CUNDINAMARCA(config-line)#password cisco123
CUNDINAMARCA(config-line)#login
CUNDINAMARCA(config-line)#logging synchronous
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 shutdown

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 shutdown

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>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SW-BUCARAMANGA
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 shutdown

SW-BUCARAMANGA(config-if)#ip default-gateway 172.31.2.1

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>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SW-TUNJA
```

```
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 shutdown

SW-TUNJA(config-if)#
SW-TUNJA(config-if)#ip default-gateway172.3.2.9
SW-TUNJA(config)#
SW-TUNJA(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

SW-TUNJA(config)#
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname 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)#

%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

SW-CUNDINAMARCA(config)#

Autenticación local con AAA.

BUCARAMANGA(config-line)#username admi secret class14
BUCARAMANGA(config)#aaa new-model
BUCARAMANGA(config)#aaa authentication login LOGIN local
BUCARAMANGA(config)#line console 0
BUCARAMANGA(config-line)#login authentication LOGIN
BUCARAMANGA(config-line)#line vty 0 15
BUCARAMANGA(config-line)#login authentication LOGIN

TUNJA(config-line)#username admi secret class14
TUNJA(config)#aaa new-model
TUNJA(config)#aaa authentication login LOGIN local
TUNJA(config)#line console 0
TUNJA(config-line)#login authentication LOGIN
TUNJA(config-line)#line vty 0 15
TUNJA(config-line)#login authentication LOGIN

CUNDINAMARCA(config-line)#username admi secret class14
CUNDINAMARCA(config)#aaa new-model
CUNDINAMARCA(config)#aaa authentication login LOGIN local
CUNDINAMARCA(config)#line console 0
CUNDINAMARCA(config-line)#login authentication LOGIN
CUNDINAMARCA(config-line)#line vty 0 15
CUNDINAMARCA(config-line)# login authentication LOGIN

Cifrado de contraseñas.

BUCARAMANGA(config)#service password-encryption

TUNJA(config)#service password-encryption

CUNDINAMARCA(config)#service password-encryption

Un máximo de internos para acceder al router.

BUCARAMANGA(config-line)#login block-for 5 attempts 4 within 60

TUNJA(config-line)#login block-for 5 attempts 4 within 60

CUNDINAMARCA(config-line)#login block-for 5 attempts 4 within 60

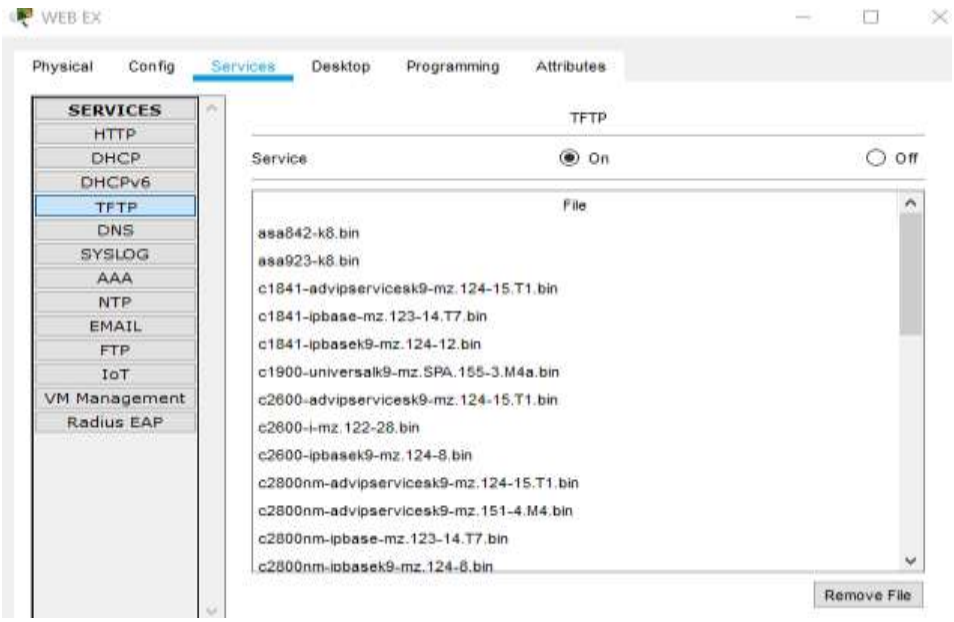
Máximo tiempo de acceso al detectar ataques.

BUCARAMANGA(config-line)#login block-for 5 attempts 4 within 60

TUNJA(config-line)#login block-for 5 attempts 4 within 60

CUNDINAMARCA(config-line)#login block-for 5 attempts 4 within 60

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



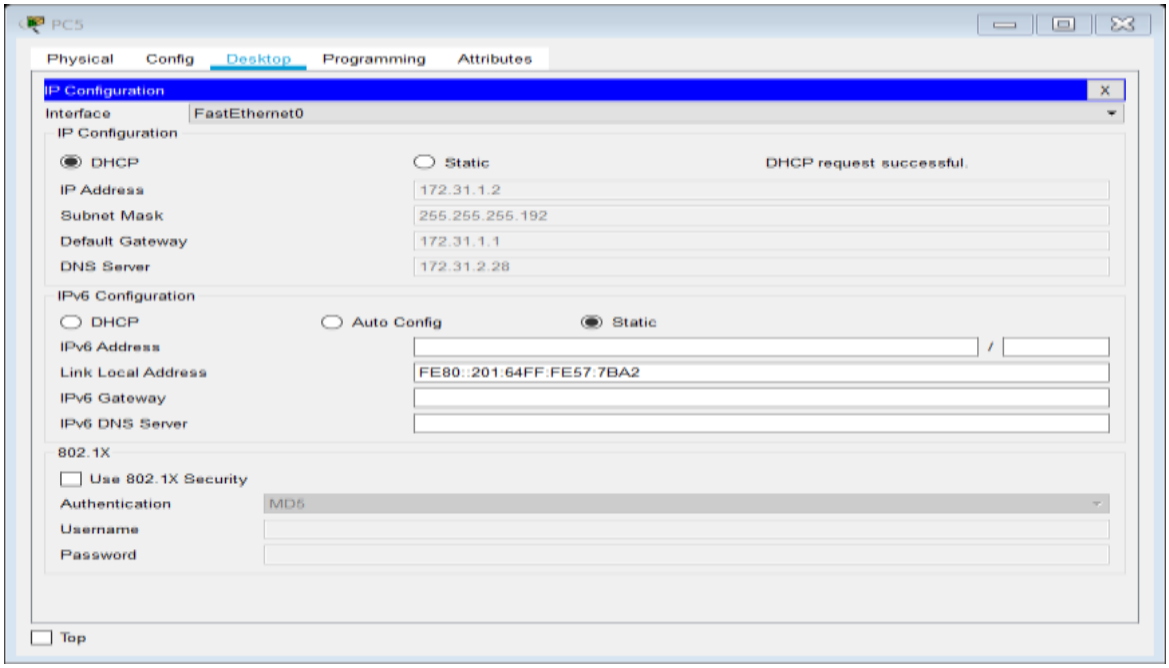
2. El DHCP deberá proporcionar solo direcciones a los hosts de Bucaramanga y Cundinamarca

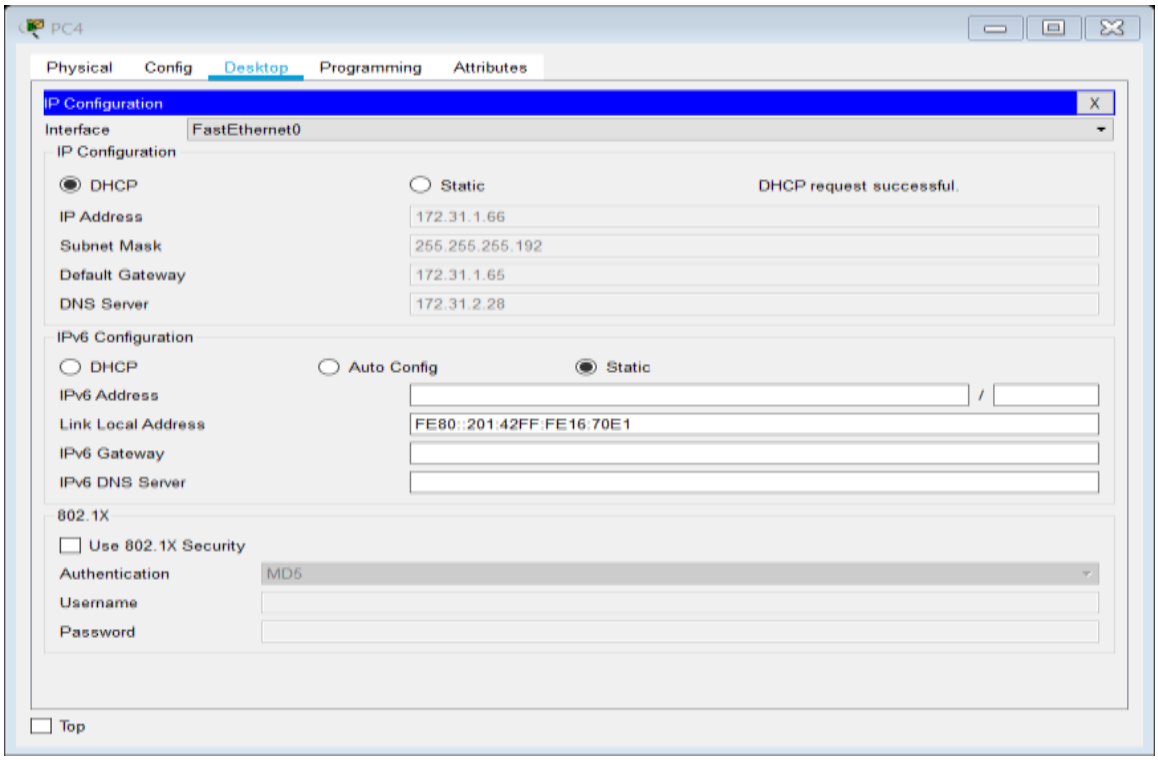
```
TUNJA(config)#ip dhcp excluded-address 172.31.0.1
TUNJA(config)#ip dhcp excluded-address 172.31.0.65
TUNJA(config)#ip dhcp excluded-address 172.31.1.65
TUNJA(config)#ip dhcp excluded-address 172.31.1.1
TUNJA(config)#ip dhcp pool V10B
TUNJA(dhcp-config)#network 172.31.0.0 255.255.255.192
TUNJA(dhcp-config)#default-router 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)#
```

```
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
```

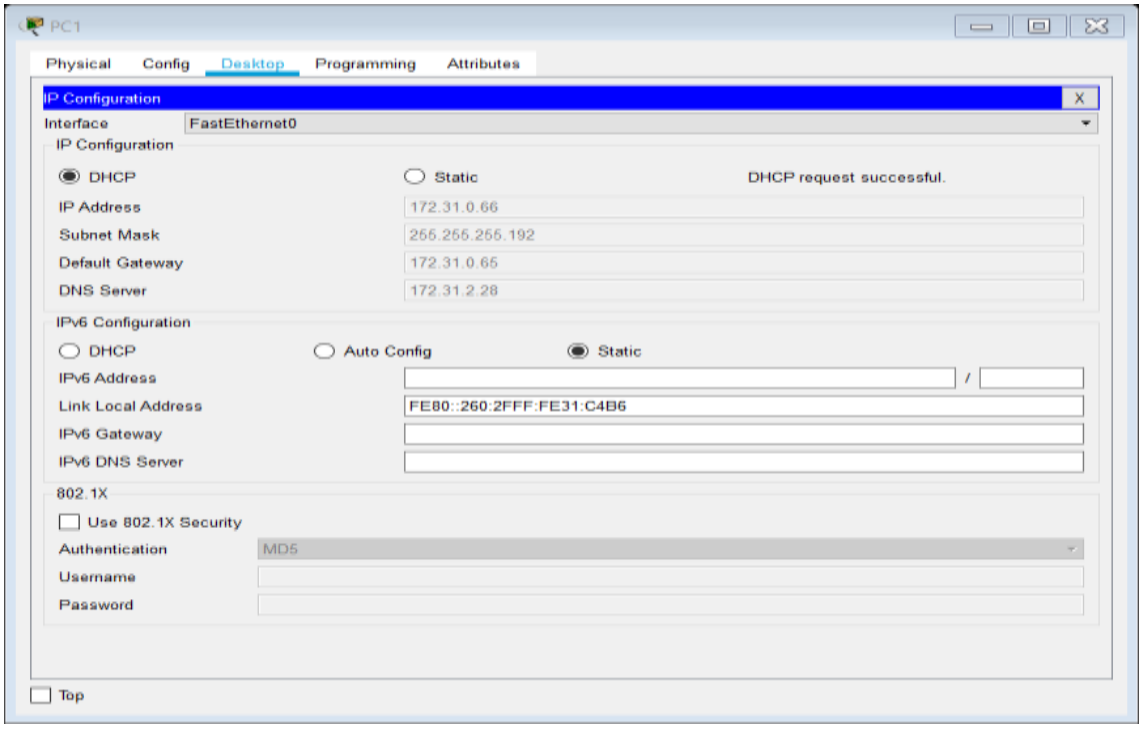
```
CUNDINAMARCA(config)#int f0/0.20 CUNDINAMARCA(config-
subif)#ip helper-address 172.31.2.37 CUNDINAMARCA(config-
subif)#int f0/0.30 CUNDINAMARCA(config-subif)#ip helper-
address 172.31.2.37 CUNDINAMARCA(config-subif)#end
CUNDINAMARCA#
%SYS-5-CONFIG_I: Configured from console by console
```

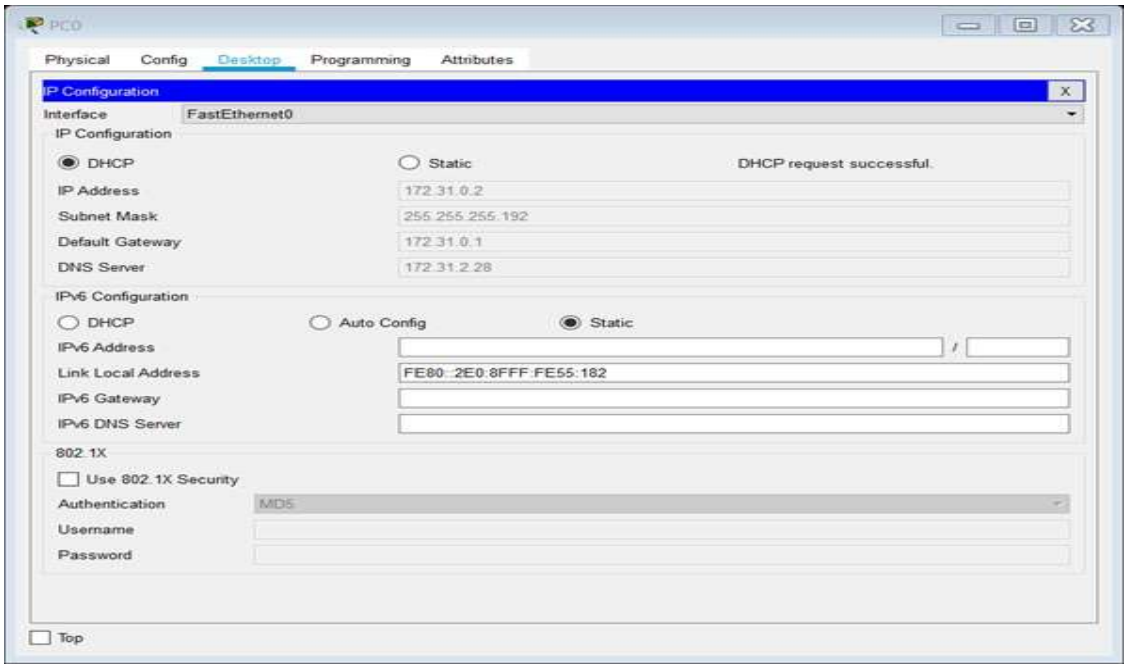
Verificación DHCP Cundinamarca





Verificación DHCP Bucaramanga





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 type2
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#
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 type2
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

BUCARAMANGA#

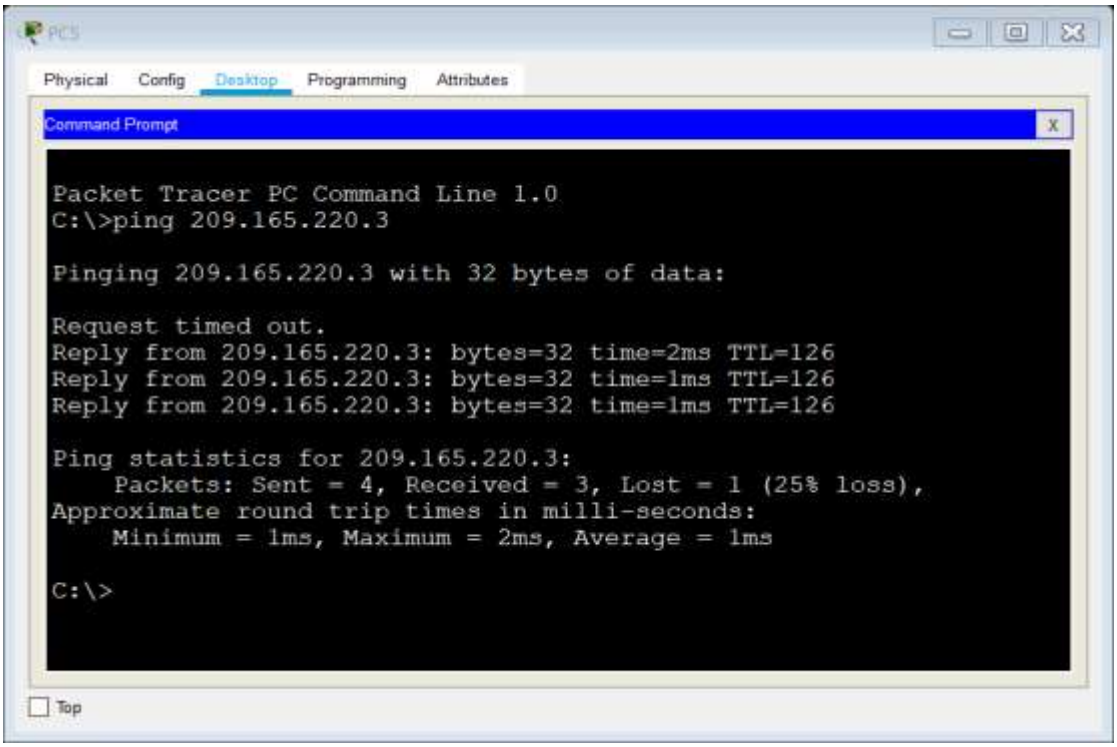
CUNDINAMARCA#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - 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

TUNJA#show ip nat translation
Pro Inside global Inside local Outside local Outside global
icmp 209.165.220.1:1 172.31.1.2:1 209.165.220.3:1209.165.220.3:1
icmp 209.165.220.1:2 172.31.1.2:2 209.165.220.3:2209.165.220.3:2
icmp 209.165.220.1:3 172.31.1.2:3 209.165.220.3:3209.165.220.3:3
icmp 209.165.220.1:4 172.31.1.2:4 209.165.220.3:4209.165.220.3:4
--- 209.165.220.4 172.31.2.28 --- —
```

4. El enrutamiento deberá tener autenticación.

```
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 cisco123
BUCARAMANGA(config-if)#

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)#
```

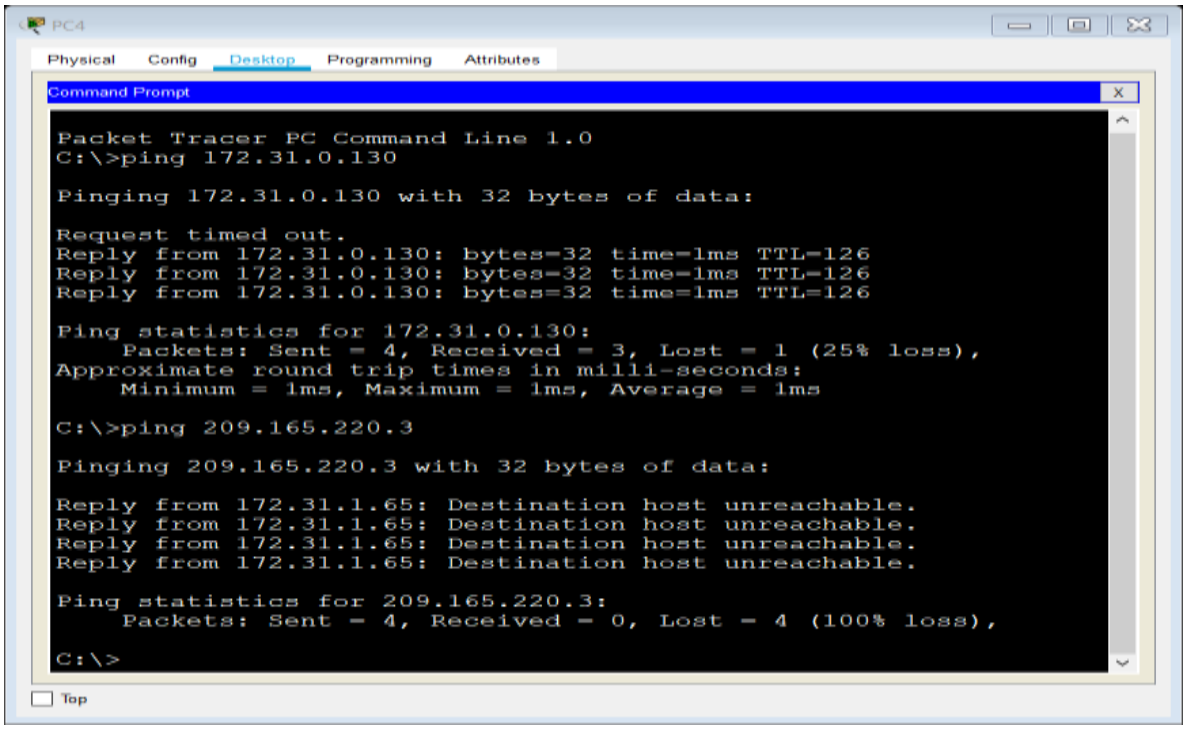
```
TUNJA#
00:30:20: %OSPF-5-ADJCHG: Process 1, Nbr 172.31.2.34 on Serial0/0/0 from
FULL to DOWN, Neighbor Down: Dead timer expired

00:30:20: %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#
00:31:32: %OSPF-5-ADJCHG: Process 1, Nbr 172.31.2.38 on Serial0/0/1 from
FULL to DOWN, Neighbor Down: Dead timer expired

00:31:32: %OSPF-5-ADJCHG: Process 1, Nbr 172.31.2.38 on Serial0/0/1 from
FULL to DOWN, Neighbor Down: Interface down or detached

TUNJA#config 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 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
```



- **Establecer una lista de control de acceso de acuerdo con los criterios señalados.**

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

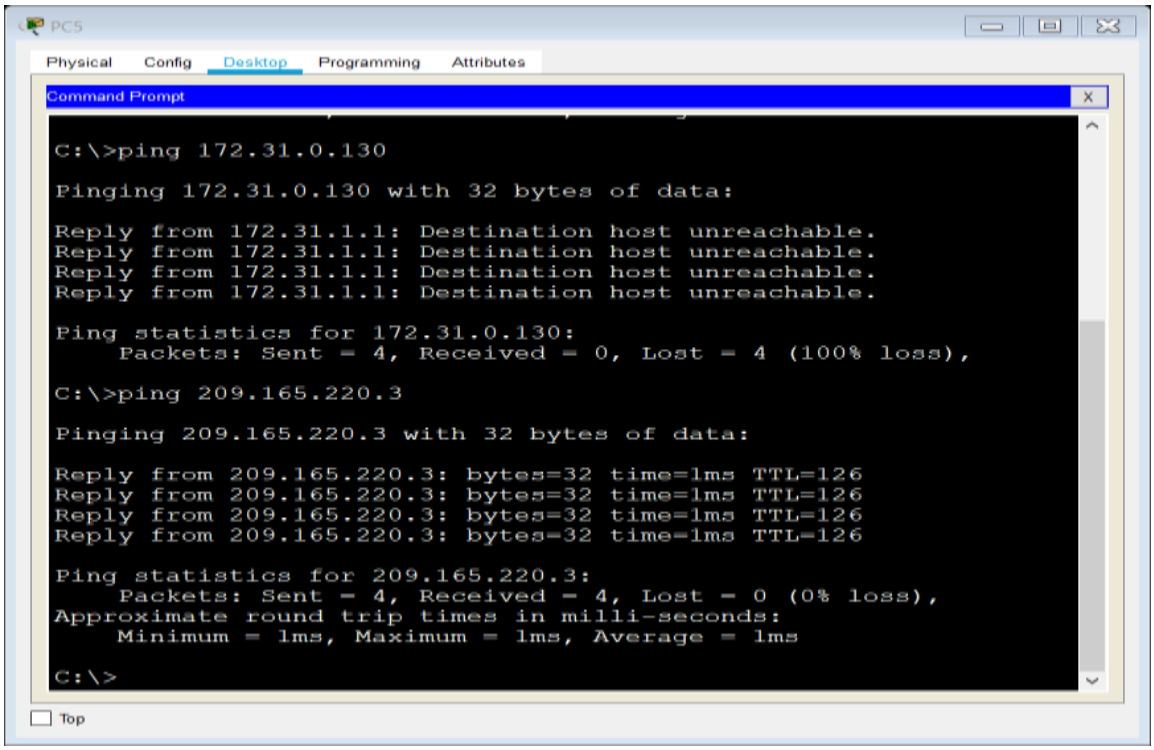
  CUNDINAMARCA(config-if)#access-list 111 deny ip 172.31.1.64 0.0.0.63 209.165.220.0 0.0.0.255
  CUNDINAMARCA(config)#access-list 111 permit ip any any CUNDINAMARCA(config)#int f0/0.20 CUNDINAMARCA(config-subif)#ip access-group 111 in CUNDINAMARCA(config-subif)#



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

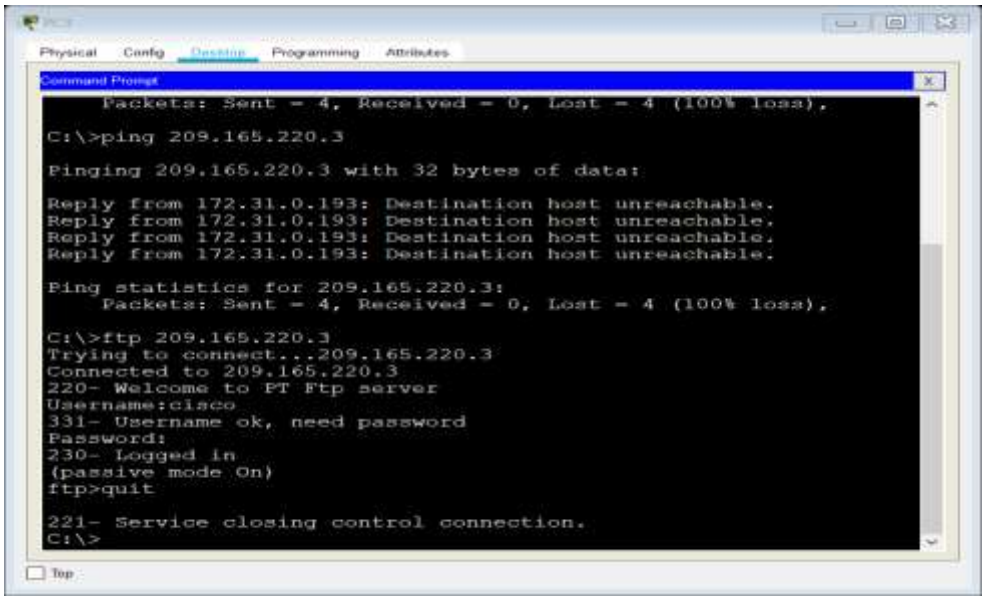
CUNDINAMARCA(config)#access-list 112 deny ip any any CUNDINAMARCA(config)#int f0/0.30 CUNDINAMARCA(config-subif)#ip access-group 112 in CUNDINAMARCA(config-subif)#

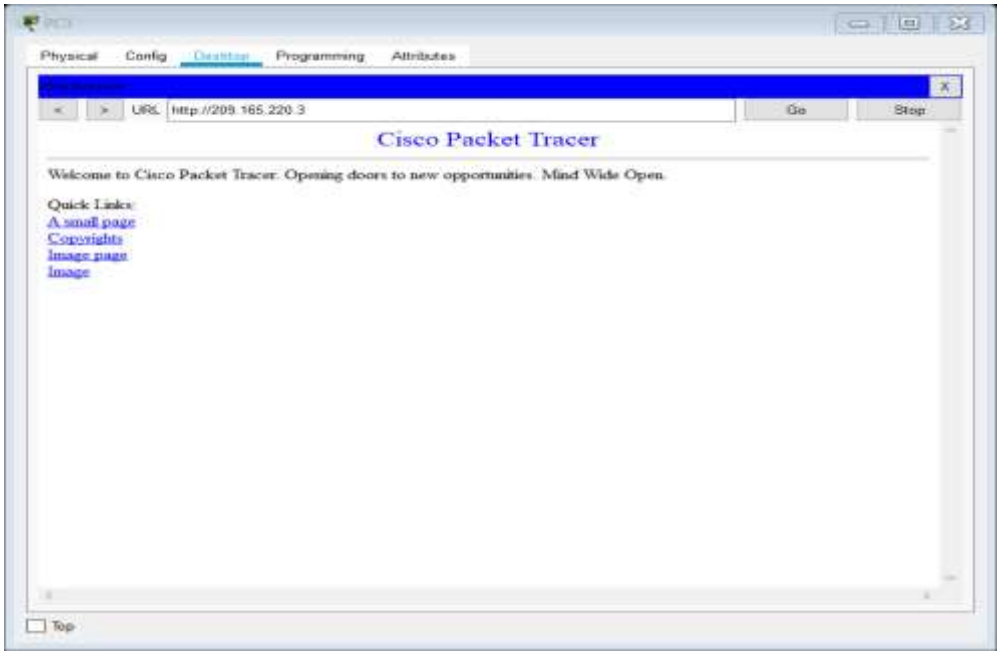


Los hosts de VLAN 30 en Tunja solo acceden a servidores web y ftp de internet.

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



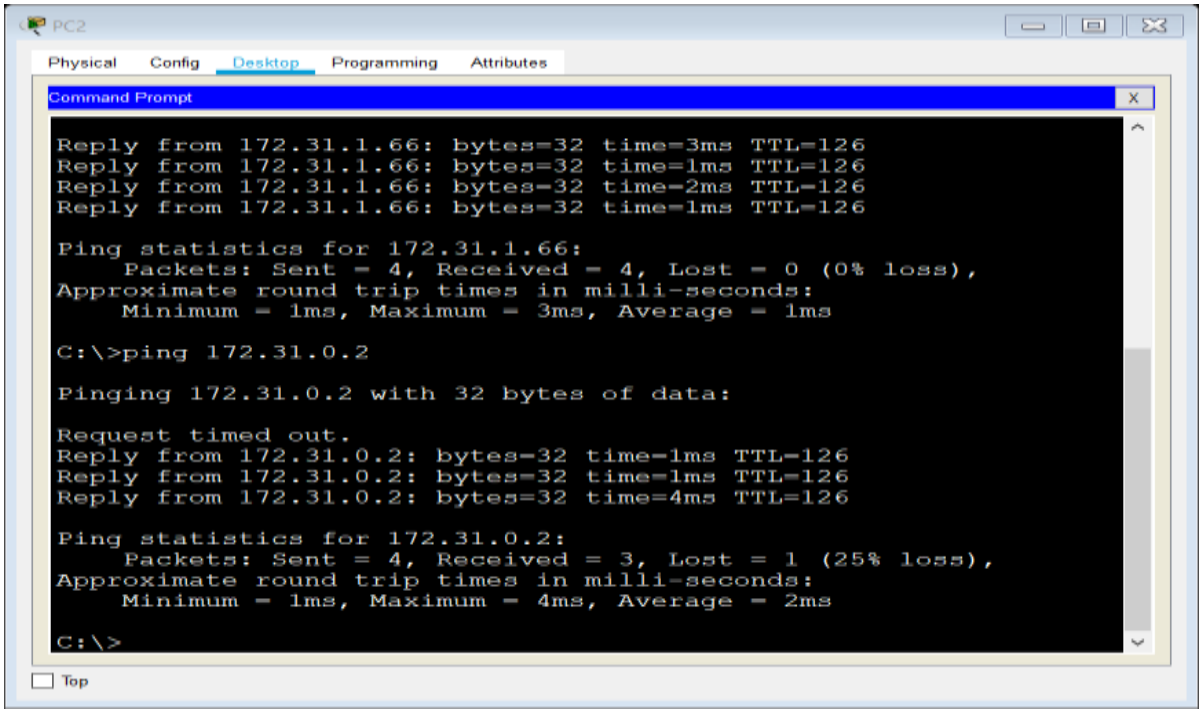


Los hosts de VLAN 20 en Tunja solo acceden a la VLAN 20 de Cundinamarca y VLAN 10 de Bucaramanga.

TUNJA(config-subif)#access-list 112 permit ip 172.31.0.128 0.0.0.63 172.31.1.64

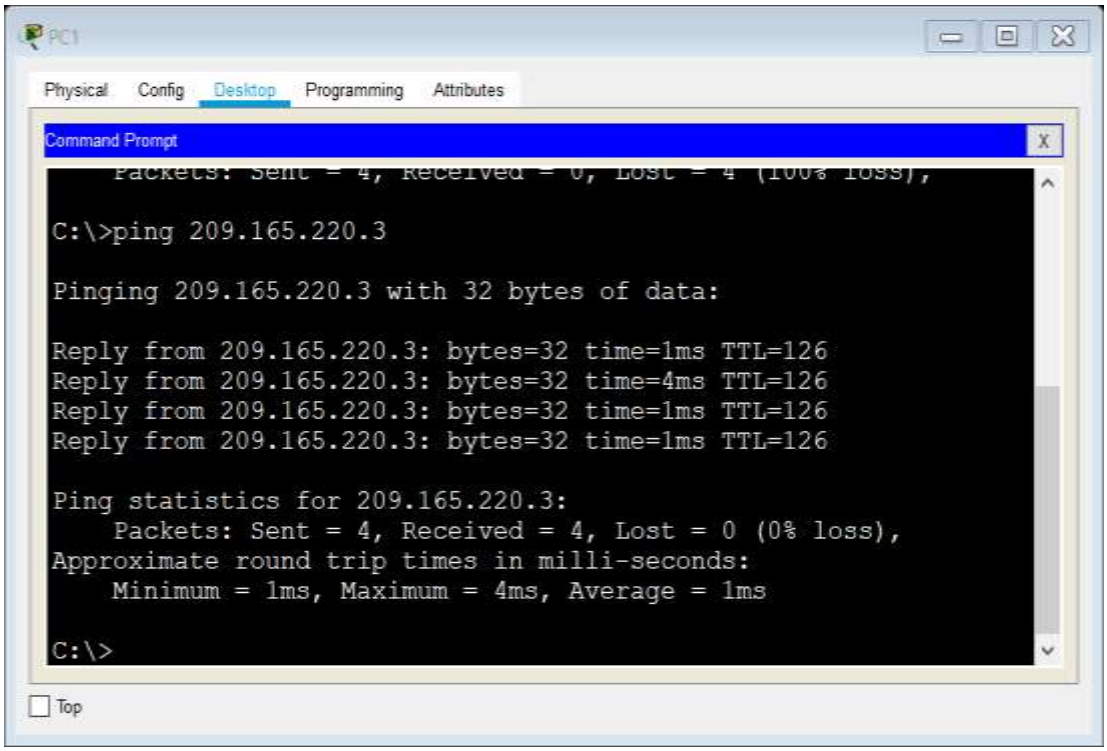
0.0.0.63

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



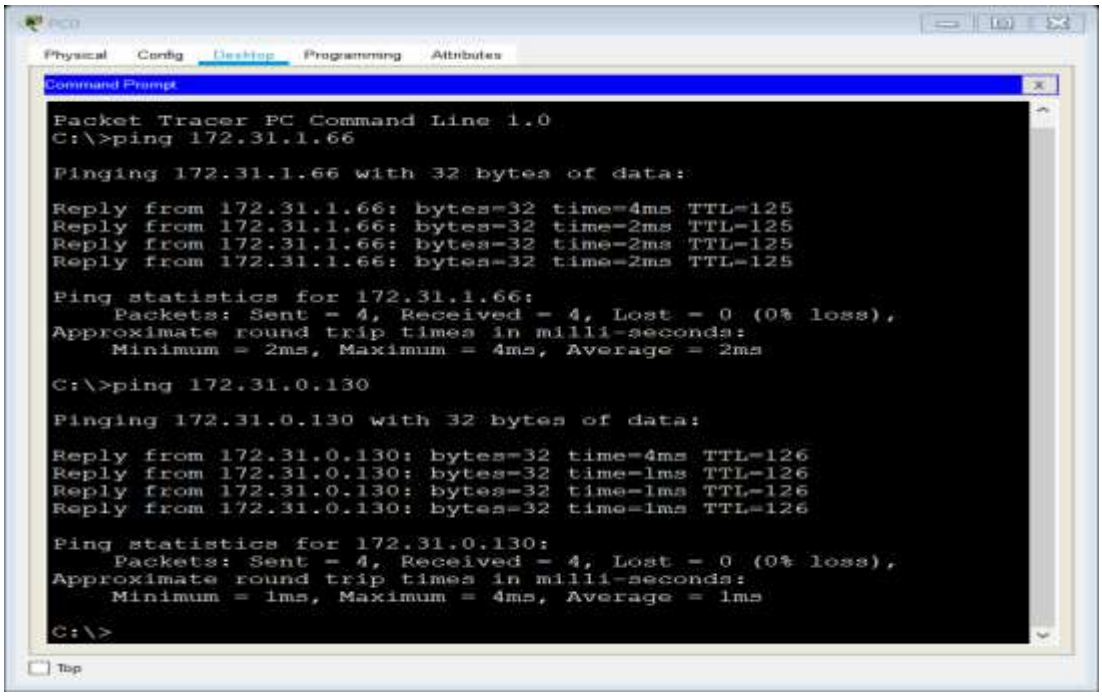
Los hosts de VLAN 30 de Bucaramanga acceden a internet y a cualquier equipo de VLAN 10.

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



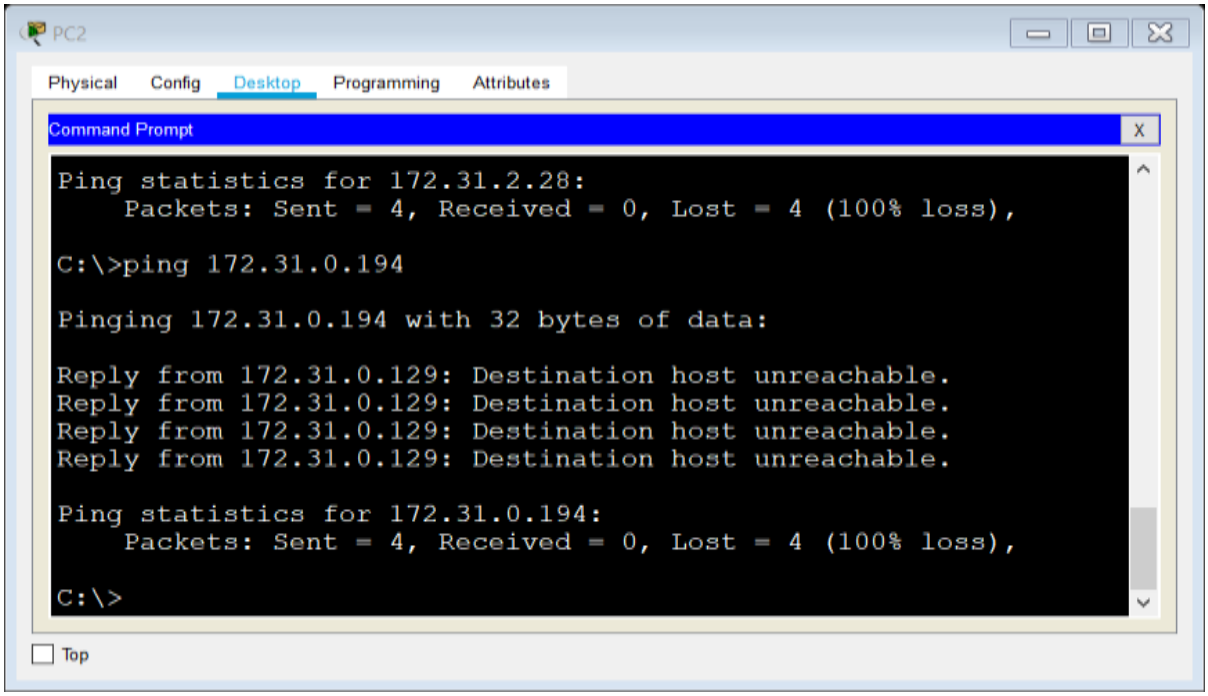
Los hosts de una VLAN no pueden acceder a los de otra VLAN en una ciudad.

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)#

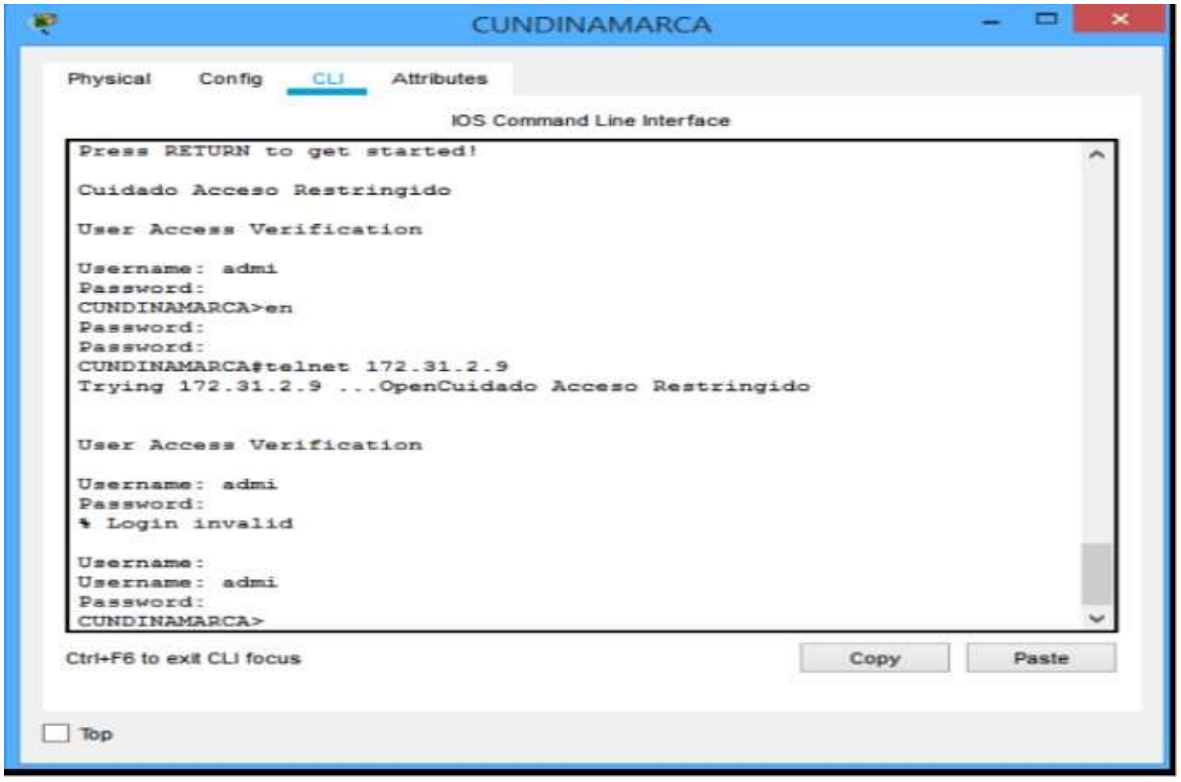
TUNJA(config)#access-list 113 deny ip 172.3.2.8 0.0.0.7 172.31.0.128 0.0.0.63
TUNJA(config)#access-list 113 deny ip 172.3.0.192 0.0.0.63 172.31.0.128 0.0.0.63 TUNJA(config)#access-list 113 permit ip any any
TUNJA(config)#int f0/0.20
TUNJA(config-subif)#ip access-group 113 out TUNJA(config-subif)#

CUNDINAMARCA(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



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

```
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)#

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

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
Physical
Config
CLI
Attributes
IOS Command Line Interface
Press RETURN to get started!
Cuidado Acceso Restringido
User Access Verification
Username: admi
Password:
CUNDINAMARCA>en
Password:
Password:
CUNDINAMARCA#telnet 172.31.2.9
Trying 172.31.2.9 ...OpenCuidado Acceso Restringido
User Access Verification
Username: admi
Password:
% Login invalid
Username:
Username: admi
Password:
CUNDINAMARCA>
Ctrl+F6 to exit CLI focus
Copy
Paste
Top

BUCARAMANGA
Physical
Config
CLI
Attributes
IOS Command Line Interface
BUCARAMANGA>en
Password:
Password:
Password:
% Bad secrets
BUCARAMANGA>en
Password:
Password:
BUCARAMANGA#telnet 172.31.2.1
Trying 172.31.2.1 ...OpenCuidado Acceso Restringido
User Access Verification
Username: admi
Password:
% Login invalid
Username:
Username: admi
Password:
BUCARAMANGA>en
Password:
Ctrl+F6 to exit CLI focus
Copy
Paste
Top

CONCLUSIONES

Por medio de los dos cursos de logro aplicar conocimientos en el área de redes por medio del curso de formación CISCO NETCAP que abordo capítulos para ser aplicados a escenarios reales como los cuales se desarrolló en esta práctica, también con ayuda del programa PACKET TRACER el cual nos fue de mucha ayuda para la creación de varias topologías y variedad de computadoras, servidores, cables de red, routers, switches y demás elementos básicos para la creación de redes y sus configuraciones.

En los dos escenarios se aplicaron la mayoría de protocolos, comandos que fueron vistos a lo largo de los dos módulos del curso CISCO los cuales resultaron útiles para la creación de topologías y configuraciones en cada uno de los pasos planteados para la práctica.

En este trabajo se consolida las actividades prácticas finales en el desarrollo de cada unidad de acuerdo a los casos de estudio dados, se ha aplicado los conocimientos proporcionados en el material de apoyo emanado por la empresa CISCO en el desarrollo del aprendizaje autónomo promovido para este tipo de ambientes virtuales.

Se logró una satisfactoria conexión, configuración y simulación de los dispositivos de las redes en los correspondientes casos de estudio.
Se repasaron todos los conceptos aprendidos en los módulos enfocando todo a los diseños de las redes solicitadas.

Referencias Bibliográficas

García, Jesús “Como configurar: HDCP, DNS, HTTP Y Conexión inalámbrica”. {En línea}. {17 septiembre de 2015}. Disponible en: (https://outlook.office.com/mail/inbox/id/AAQkADgzNDdjZWQ5LWJlOGItNDdkNy1iYTJlLTJiNGMwYzdjZWNhYQAQAGOZUAkpNA1Dnhq4ZTIeNuE%3D)

CISCO “Capa de Transporte. Fundamentos de Networking” {En línea} {2014}. Disponible en: https://static-course-assets.s3.amazonaws.com/ITN50ES/module7/index.html#7.0.1.1

CISCO “Asignación de direcciones IP. Fundamentos de Networking”. {En línea} {2014} Disponible en: https://static-course-assets.s3.amazonaws.com/ITN50ES/module8/index.html#8.0.1.1

CISCO “SubNetting. Fundamentos de Networking”. {En línea} {2014}. Disponible en: https://static-course assets.s3.amazonaws.com/ITN50ES/module9/index.html#9.0.1.1
CISCO “Capa de Aplicación. Fundamentos de Networking”. {En línea} {2014} Disponible en: https://static-course assets.s3.amazonaws.com/ITN50ES/module10/index.html#10.0.1.1

CISCO “Soluciones de Red. Fundamentos de Networking”. {En línea} {2014} Disponible en: https://static-course-assets.s3.amazonaws.com/ITN50ES/module11/index.html#11.0.1.1

Vesga, J. “PING y TRACER Como estrategia en procesos de Networking [OVA]” {En línea} {2014}. Disponible en: (https://1drv.ms/u/s!AmIJYei-NT1IhgTCtKY-7F5KIRC3)