Diplomado De Profundización Cisco (Diseño E Implementación De Soluciones Integradas LAN / WAN) (OPCI - (203092a_614)

Prueba de Habilidades Prácticas CCNA

Tutor

Ing. Giovanni Alberto Bracho

Universidad Nacional Abierta Y A Distancia

Escuela De Ciencias Básicas, Tecnología E Ingeniería

Programa De Ingeniería De Sistemas

Cead - Valledupar

Diciembre - 2019

Prueba De Habilidades Practicas CCNA

Rene Alejandro Quintero Padilla

Trabajo Final Diplomado De Profundización Cisco (Diseño E Implementación De Soluciones Integradas LAN / WAN) (Grupo - (203092 - 23)

Director de curso Ingeniero Juan Carlos Vesga

Universidad Nacional Abierta Y A Distancia
Escuela De Ciencias Básicas, Tecnología E Ingeniería
Programa De Ingeniería De Sistemas
Cead - Valledupar

Diciembre - 2019

Valledupar, (Diciembre de 2019)

NOTA DE ACEPTACIÓN

_____
_____
_____
_____
_____
_____
_____

_____
Presidente del Jurado

_____
Jurado

TABLA DE CONTENIDO

LISTA DE TABLAS

LISTA DE IMÁGENES

GLOSARIO

Router: Originalmente, se identificaba con el término gateway, sobretodo en referencia a la red Internet. En general, debe considerarse como el elemento responsable de discernir cuál es el camino más adecuado para la transmisión de mensajes en una red compleja que está soportando un tráfico intenso de datos

VPN - Red privada virtual: Una conexión IP entre dos sitios sobre una red pública IP que tiene su tráfico de carga útil codificada de manera que sólo los nodos fuente y destino pueden descifrar los paquetes de tráfico. Una VPN permite a una red públicamente accesible será usada para transmisiones de datos altamente confidenciales, dinámicas y seguras.

DHCP: (Dynamic Host Configuration Protocol), protocolo de configuración de host dinámico) es un protocolo que permite que un equipo conectado a una red pueda obtener su configuración (principalmente, su configuración de red) en forma dinámica (es decir, sin una intervención especial).

Packet Tracer: Programa de simulación de redes que permite a los estudiantes experimentar con el comportamiento de la red.

Dirección IP: Una dirección en la red asignada a una in-terfaz de un nodo de la red y usada para identificar (loCALIzar) en forma única el nodo dentro de la Internet. Dos versiones están actualmente implementadas: IPv4 e IPv6.

Dirección IPv4: Una dirección IP con base en el IPv4. Esas direcciones consisten en 32 bits (0 al 31) particionados en cuatro grupos de ocho bits cada uno (llamados octetos) y organizados en cinco clases (A a la E) con base en los valores de bits 0 al 3.

Dirección IPv6: Una dirección IP con base en IPv6. Una dirección IPv6 consiste en 128 bits y tiene 4000 millones X 4000 millones de veces el tamaño del espacio de dirección IPv4 (2128 vs. 232). A diferencia de las direcciones IPv4, las direcciones IPv6 usan dos puntos como delimitador (en vez de una notación “punto”), y ellas son escritas como ocho enteros de 16 bits expresados en forma hexadecimal.

Red de área amplia (WAN): Una red que interconecta recursos de computadoras que están geográficamente ampliamente separadas (usualmente a más de 100 km). Esto incluye pueblos, ciudades, estados y condados. Un WAN cubre generalmente un área mayor que 5 millas (8 km) y puede considerarse que consiste en una colección de LAN.

Red de área local (LAN): Una red que interconecta recursos de computadoras dentro de un área geográfica de tamaño moderado. Esta puede incluir un cuarto, varios cuartos dentro de un edificio, o varios edificios de un campus. El rango de una LAN es usualmente de no más de 10 km de radio.

RESUMEN

Esta prueba de habilidades se realiza con el propósito de aplicar de una forma práctica los conocimientos adquiridos a lo largo del desarrollo del Diplomado De Profundización CCNA (Diseño e Implementación de soluciones integradas LAN/WAN), aportando al estudiante las habilidades necesarias en el manejo de redes, enfrentándolo a dos escenarios, en donde para cada uno de ellos debe construir su topología, configuraciones y codificación.

Escenario 1, se desarrolla los conocimientos en cuanto a la configuración de los equipos relacionados en una topología, realizar las rutinas de diagnóstico, conexión física, según una tabla la cual contiene el direccionamiento de cada uno de ellos, así como enrutamiento EIGRP, enlaces troncales y la implementación de NAT.

Escenario 2, se evalúa las competencias en la implementación del direccionamiento VLSM, al igual que la configuración NAT y VLAN, Autenticación local con AAA, cifrado por contraseñas, Establecer un servidor TFTP

ABSTRACT

This skills test is carried out with the purpose of applying in a practical way the knowledge acquired throughout the development of the CCNA Deepening Certificate (Design and Implementation of integrated LAN / WAN solutions), providing the student with the necessary skills in the management of networks, facing two scenarios, where for each of them you must build your topology, configurations and coding.

Scenario 1, knowledge is developed regarding the configuration of related equipment in a topology, perform diagnostic routines, physical connection, according to a table which contains the address of each of them, as well as EIGRP routing, trunk links and the implementation of NAT.

Scenario 2, the competencies in the implementation of VLSM addressing are evaluated, as well as the NAT and VLAN configuration, Local authentication with AAA, password encryption, Establish a TFTP server

1. INTRODUCCIÓN

Para diseñar redes de ordenadores, es indispensable saber y conocer los componentes que se necesitan para obtener una adecuada comunicación, seguridad, conectividad.

En el transcurso de nuestra preparación como estudiante, donde desarrollamos las distintas actividades propuestas del diplomado de profundización CCNA, se adquirieron conocimientos relacionados con diversos aspectos de NETWORKING, los cuales coloque en práctica, en la prueba de habilidades que incluyeron dos actividades propuestas, donde se configuro cada uno de los dispositivos de red de una empresa para interconectarlos entre sí, siguiendo un paso a paso, dentro de estos encontramos el direccionamiento IP, protocolos de enrutamiento, parámetros de seguridad, buenas prácticas de sostenimiento de la infraestructura de comunicaciones y demás aspectos que forman parte de la topología de red. Adicionalmente, todos los procedimientos desarrollados en los escenarios planteados se realizaron con el apoyo del software Packet Tracert, logrando de esta manera poner en práctica las habilidades adquiridas en el desarrollo del diplomado, dentro de estas se cumple con el objetivo de fortalecer el manejo del sistema operativo de los dispositivos, manipulación eficiente de software especializado y tener un contacto preliminar con equipos de red de manera virtual.

Lo anteriormente expuesto permite tener un apoyo fuerte para empezar a tener un enfrentamiento con el mundo laboral, en el cual el profesional tiene que tener un desempeño eficiente, recursivo, garantizando las respectivas soluciones a las necesidades de las empresas

2. OBJETIVOS

General

- ✓ Aplicar todas las habilidades obtenidas en el desarrollo del curso de forma prácticas, teóricas en el desarrollo de una prueba que incluye dos escenarios, describiendo el paso a paso de cada punto realizado y su respectivo código de configuración aplicado.

Específicos

- ✓ Identificar que dispositivos utilizar para el diseño de una topología de red propuesta.
- ✓ Realizar configuración básica y específica a dispositivos de comunicación como Routers, Switch, Servidores, etc.
- ✓ Implementar seguridad en Switch, elaboración de VLANS e inter VLAN Routing.
- ✓ Determinar la configuración necesaria para la implementación de OPSFv2, protocolo dinámico de Routing.
- ✓ Implementar de DHCP y NAT en dispositivos de comunicación.
- ✓ Verificar conectividad entre los dispositivos de una topología.
- ✓ Configurar y verificar listas de control de acceso ACL

3. DESARROLLO DE ESCENARIO

3.1 Escenario 1

3.2 Descripción Del Escenario.

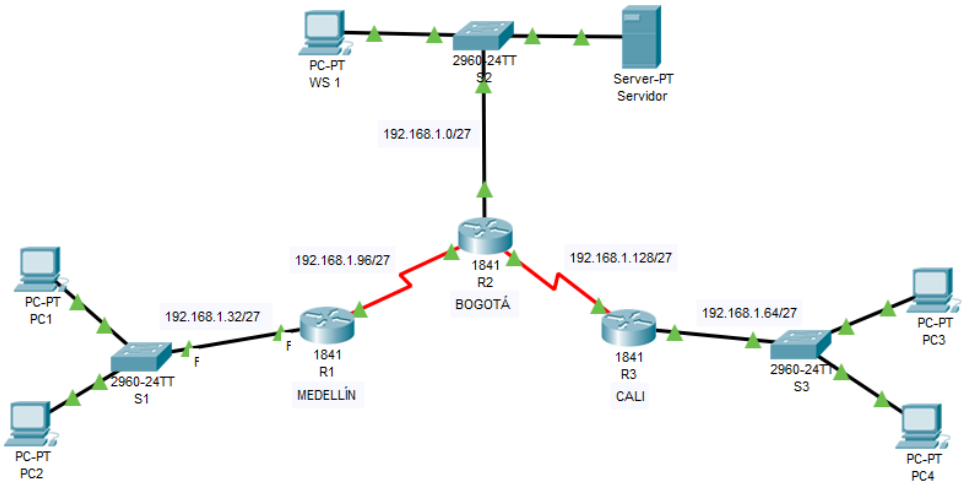
Una empresa posee sucursales distribuidas en las ciudades de Bogotá, Medellín y CALI en donde el estudiante será el administrador de la red, el cual deberá configurar e interconectar entre sí cada uno de los dispositivos que forman parte del escenario, acorde con los lineamientos establecidos para el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

3.3 Topología De La Red

3 ROUTERS 1941
3 SWITCHS 2960 24TT
1 SERVIDOR PT
5 PC WINDOWS 7 GENERICOS

Configuración de la topología de la red propuesta.

Imagen 1 – topología propuesta



Fuente Packet Tracert

3.4 Configuración Básica De Los Dispositivos

Aplicar a cada Router y Switch de la topología, las siguientes configuraciones básicas;

Router 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)#
```

Router BOGOTA

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

Router CALI

Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname CALI
CALI(config)#no ip doma
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 pas
CALI(config)#service password-encryption
CALI(config)#banner motd $ Unauthorized Access Is Prohibited $
CALI(config)#exit
CALI#
%SYS-5-CONFIG_I: Configured from console by console
CALI#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
CALI#

S1
Switch>enable
Switch#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 pass
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 runn
S1#copy running-config st
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-en
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 domai
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#

3.5 Parte 1: Asignación de direcciones IP

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
Subnets: 8

3.6 Part 2: Configuración Básica.

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

	R1	R2	R3
Nombre de Host	**MEDELLIN**	**BOGOTA**	**CALI**
Dirección de Ip en interfaz Serial 0/0	192.168.1.99	192.168.1.98	192.168.1.131
Dirección de Ip en interfaz Serial 0/1	192.168.1.131	192.168.1.130	192.168.1.193
Dirección de Ip en interfaz FA 0/0	192.168.1.33	192.168.1.1	192.168.1.65
Protocolo de enrutamiento	**Eigrp**	**Eigrp**	**Eigrp**
Sistema Autónomo	200	200	200
Afirmaciones de red	192.168.1.0	192.168.1.0	192.168.1.0

MEDELLIN

```
User Access Verification
Password:
MEDELLIN>enable
Password:
MEDELLIN#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN(config)#interface s0/0/0
MEDELLIN(config-if)#ip address 192.168.1.99 255.255.255.224
MEDELLIN(config-if)#clock rate 128000
This command applies only to DCE interfaces
MEDELLIN(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
MEDELLIN(config-if)#
MEDELLIN#
%SYS-5-CONFIG_I: Configured from console by console
MEDELLIN#

MEDELLIN(config)#interface g0/0
MEDELLIN(config-if)#ip address 192.168.1.33 255.255.255.224
MEDELLIN(config-if)#no shutdown
MEDELLIN(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0,
changed state to up
MEDELLIN(config-if)#
MEDELLIN#
```

BOGOTA

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

BOGOTA(config)#interface g0/0
BOGOTA(config-if)#ip address 192.168.1.1 255.255.255.224
BOGOTA(config-if)#no shutdown
BOGOTA(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0,
changed state to up
BOGOTA(config-if)#

BOGOTA(config-if)#
BOGOTA(config-if)#exit
BOGOTA(config)#interface s0/0/1
BOGOTA(config-if)#ip address 192.168.1.130 255.255.255.224
BOGOTA(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up
BOGOTA(config-if)#
```

CALI

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

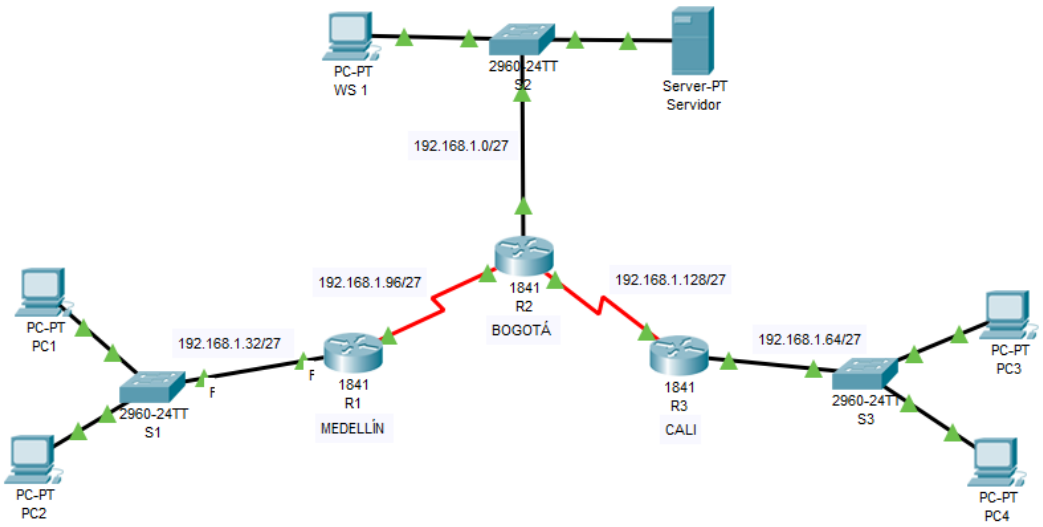
CALI(config-if)#
CALI#

CALI#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
CALI(config)#interface g0/0
CALI(config-if)#ip address 192.168.1.165 255.255.255.224
CALI(config-if)#no shutdown
CALI(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
CALI(config-if)#

CALI(config-if)#exit
CALI(config)#interface s0/0/1
CALI(config-if)#ip address 192.168.1.193 255.255.255.224
CALI(config-if)#clock rate 128000
CALI(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
CALI(config-if)#

Imagen 2 – topología montada



Fuente Packet Tracert

Realizar un diagnóstico de vecinos usando el comando cdp.

MEDELLIN

MEDELLIN#show cdp neighbors detail

Device ID: S1
Entry address(es):
Platform: cisco 2960, Capabilities: Switch
Interface: GigabitEthernet0/0, Port ID (outgoing port): FastEthernet0/1
Holdtime: 121

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: 121

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

MEDELLIN#

BOGOTA

BOGOTA#show cdp neighbors detail
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: 178
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: 178

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: S2
Entry address(es):
Platform: cisco 2960, Capabilities: Switch
Interface: GigabitEthernet0/0, Port ID (outgoing port): FastEthernet0/1
Holdtime: 178
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
BOGOTA#

CALI
CALI#show cdp neighbors detail

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: 127
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: S3
Entry address(es):
Platform: cisco 2960, Capabilities: Switch
Interface: GigabitEthernet0/0, Port ID (outgoing port): FastEthernet0/1
Holdtime: 127

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
CALI#

3.7 Configuración IP Route

MEDELLIN

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 192.168.1.128 255.255.255.224 192.168.1.98
MEDELLIN(config)#ip route 192.168.1.64 255.255.255.224 192.168.1.98
MEDELLIN(config)#

BOGOTA

BOGOTA(config)#ip route 192.168.1.64 255.255.255.224 192.168.1.131
BOGOTA(config)#ip route 192.168.1.32 255.255.255.224 192.168.1.97
BOGOTA(config)#

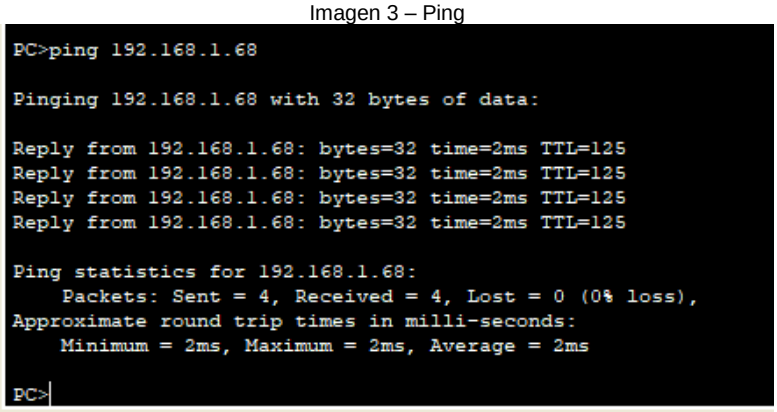
CALI

```
CALI(config)#ip route 192.168.1.0 255.255.255.224 192.168.1.130
CALI(config)#ip route 192.168.1.96 255.255.255.224 192.168.1.130
CALI(config)#ip route 192.168.1.96 255.255.255.224 192.168.1.130
```

3.8 Pruebas de Comunicación

Ping PC1 MEDELLIN a PC2 CALI

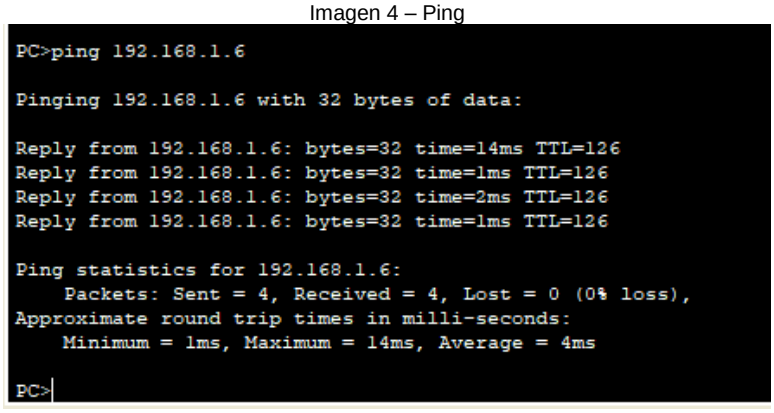
Imagen 3 – Ping



Fuente Packet Tracert

Ping PC1 MEDELLIN a PC4 BOGOTA

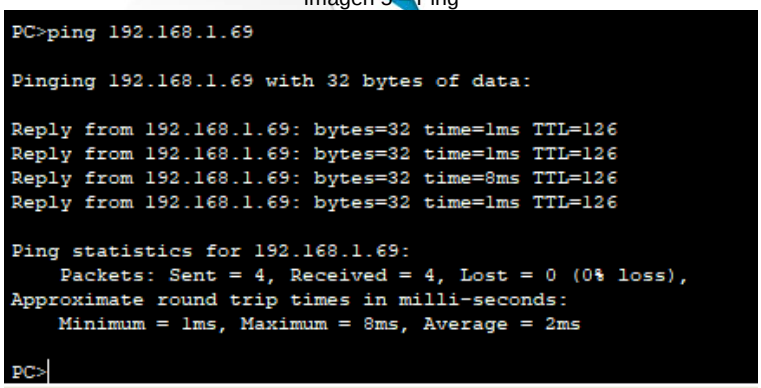
Imagen 4 – Ping



Fuente Packet Tracert

Ping PC4 BOGOTA a PC3 CALI

Imagen 5 – Ping



Fuente Packet Tracert

3.9 Configuración de Enrutamiento

MEDELLIN

MEDELLIN>enable
Password:
MEDELLIN#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN(config)#router eigrp 200
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)#
MEDELLIN(config-router)#no auto-summary

BOGOTÁ

BOGOTA>enable
Password:
BOGOTA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA(config)#router eigrp 200
BOGOTA(config-router)#network 192.168.1.96 0.0.0.31
BOGOTA(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 200: Neighbor 192.168.1.97 (Serial0/0/0) is up: new adjacency
BOGOTA(config-router)#network 192.168.1.0 0.0.0.31
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 auto
BOGOTA(config-router)#no auto-summary
BOGOTA(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 200: Neighbor 192.168.1.97 (Serial0/0/0) resync: summary configured
BOGOTA(config-router)#

CALI

```
CALI>enable
Password:
CALI#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
CALI(config)#router eigrp 200
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 192.168.1.64 0.0.0.31
CALI(config-router)#no auto-summary
CALI(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 200: Neighbor 192.168.1.130 (Serial0/0/0)
resync: summary configured
CALI(config-router)#
```

3.10 Conectividad

Ping PC0 MEDELLÍN a Servidor BOGOTÁ

Imagen 6 – Ping

```
PC>ping 192.168.1.8

Pinging 192.168.1.8 with 32 bytes of data:

Reply from 192.168.1.8: bytes=32 time=1ms TTL=126
Reply from 192.168.1.8: bytes=32 time=3ms TTL=126
Reply from 192.168.1.8: bytes=32 time=1ms TTL=126
Reply from 192.168.1.8: bytes=32 time=3ms TTL=126

Ping statistics for 192.168.1.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 3ms, Average = 2ms

PC>
```

Fuente Packet Tracert

Ping PC4 BOGOTA a PC2 CALI

Imagen 7 – Ping

```
PC>ping 192.168.1.68

Pinging 192.168.1.68 with 32 bytes of data:

Reply from 192.168.1.68: bytes=32 time=1ms TTL=126
Reply from 192.168.1.68: bytes=32 time=2ms TTL=126
Reply from 192.168.1.68: bytes=32 time=1ms TTL=126
Reply from 192.168.1.68: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.1.68:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms

PC>
```

Fuente Packet Tracert

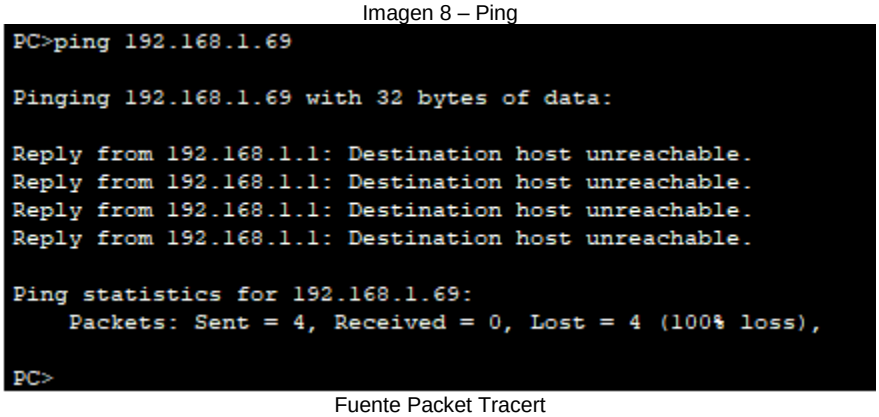
3.11 Configuración de las listas de Control de Acceso

Denegar el acceso de PC4 a cualquier dispositivo de la red.

```
BOGOTA>enable
Password:
BOGOTA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA(config)#acces
BOGOTA(config)#access-list 1 deny 192.168.1.6 0.0.0.31
BOGOTA(config)#acces
BOGOTA(config)#access-list 1 permit any
BOGOTA(config)#interface serial 0/0/0
BOGOTA(config-if)#ip access-group 1 out
BOGOTA(config-if)#exit
BOGOTA(config)#interface serial 0/0/1
BOGOTA(config-if)#ip access-group 1 out
BOGOTA(config-if)#
```

Ping PC4 BOGOTA a PC3 CALI

Imagen 8 – Ping



Fuente Packet Tracert

3.12 Configuración ACL

Permitir Acceso del servidor a cualquier dispositivo de la Red

```
BOGOTA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA(config)#acces
BOGOTA(config)#access-list 2 permit 192.168.1.8 0.0.0.31
BOGOTA(config)#acces
BOGOTA(config)#access-list 2 permit any
BOGOTA(config)#interface g
BOGOTA(config)#interface gigabitEthernet 0/0
BOGOTA(config-if)#ip acces
```

BOGOTA(config-if)#ip access-group 2 in
BOGOTA(config-if)#

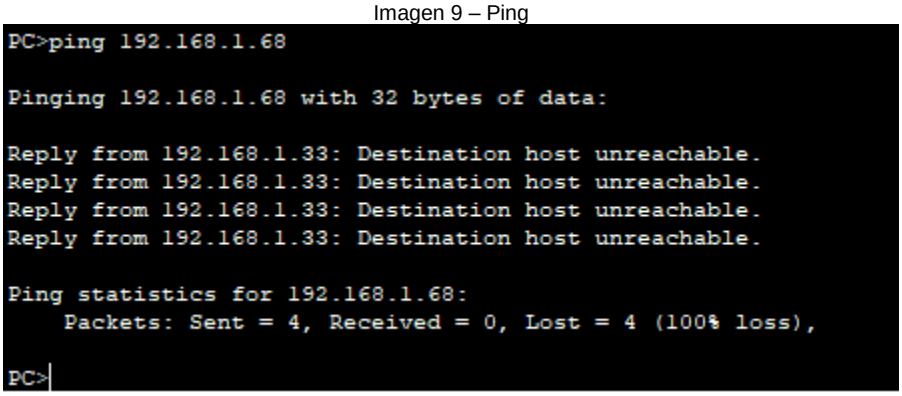
Servidor BOGOTA a PC3 CALI

Denegar el acceso de los equipos de MEDELLIN al resto de la red

MEDELLIN(config)#access-list 100 deny ip 192.168.1.32 0.0.0.31 192.168.1.96 0.0.0.31
MEDELLIN#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN(config)#interface g
MEDELLIN(config)#interface gigabitEthernet 0/0
MEDELLIN(config-if)#ip acces
MEDELLIN(config-if)#ip access-group 100 in
MEDELLIN(config-if)#
MEDELLIN#

PC1 MEDELLIN a PC2 CALI

Imagen 9 – Ping

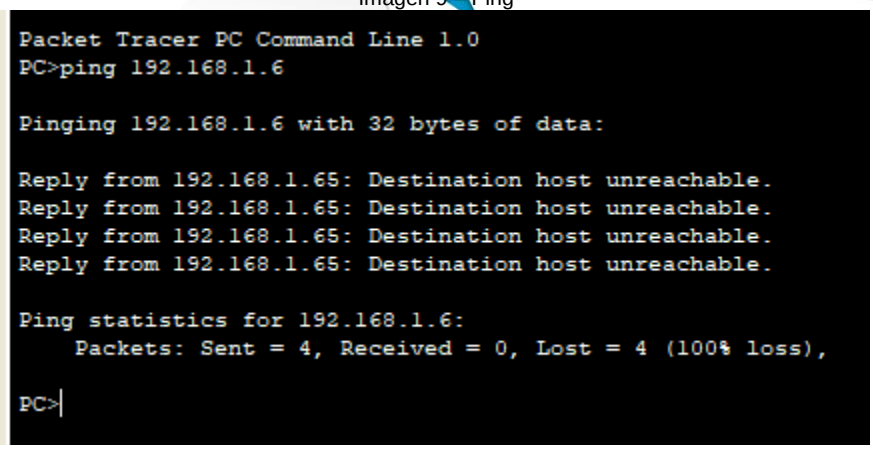


Fuente Packet Tracert

Denegar el acceso de los equipos de CALI al resto de la red

CALI>enable
Password:
CALI#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
CALI(config)#access-list 101 deny ip 192.168.1.64 0.0.0.31 192.168.1.128 0.0.0.31
CALI(config)#inter
CALI(config)#interface g
CALI(config)#interface gigabitEthernet 0/0
CALI(config-if)#ip access-group 101 in
CALI(config-if)#
CALI#

Imagen 9 – Ping



Fuente Packet Tracert

CALI#show access-lists
Extended IP access list 101
10 deny ip 192.168.1.64 0.0.0.31 192.168.1.128 0.0.0.31
CALI#

La seguridad a través de la configuración ACL, en este caso, nos permite filtrar tráfico con base en la dirección IP de Bogotá.

Imagen 11 - Configuración Lista de Acceso

```
(config)#access-list 21 deny 192.168.1.98 255.255.255.224
(config)#access-list 21 permit host 0.0.0.0
```

Fuente Packet Tracert

La configuración de las ACL extendidas se configura cerca de la fuente, de acuerdo a su naturaleza este tipo de seguridad, permite restringir el acceso por puertos, por interfaz o por dirección

Imagen 12 – ACL VLAN 1

```
(config)#access-list 1 permit 192.168.1.98 255.255.255.224
```

Fuente Packet Tracert

En la imagen anterior se creó una lista de acceso extendidas en R2: La ACL 1 permite el tráfico de la red 192.168.1.98/24 hacia la red de internet.

3.13 Comprobación de la red instalada.

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

	ORIGEN	DESTINO	RESULTADO
TELNET	**Router MEDELLIN**	**Router CALI**	OK
	WS_1	**Router BOGOTA**	OK
	Servidor	**Router CALI**	FALLIDO
	Servidor	**Router MEDELLIN**	FALLIDO
TELNET	**LAN del Router MEDELLIN**	**Router CALI**	FALLIDO
	LAN del Router CALI	**Router CALI**	FALLIDO
	LAN del Router MEDELLIN	**Router MEDELLIN**	FALLIDO
	LAN del Router CALI	**Router MEDELLIN**	FALLIDO
PING	**LAN del Router CALI**	**WS_1**	unreachable
	LAN del Router MEDELLIN	**WS_1**	unreachable
	LAN del Router MEDELLIN	**LAN del Router CALI**	unreachable
PING	**LAN del Router CALI**	**Servidor**	unreachable
	LAN del Router MEDELLIN	**Servidor**	unreachable
	Servidor	**LAN del Router MEDELLIN**	unreachable
	Servidor	**LAN del Router CALI**	unreachable
	Router CALI	**LAN del Router MEDELLIN**	unreachable
	Router MEDELLIN	**LAN del Router CALI**	unreachable

4. DESARROLLO DE ESCENARIO

4.1 Escenario 2

4.2 Descripción Del Escenario.

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.

4.3 Topología De La Red

Imagen 13 – topología propuesta de la red – escenario 2

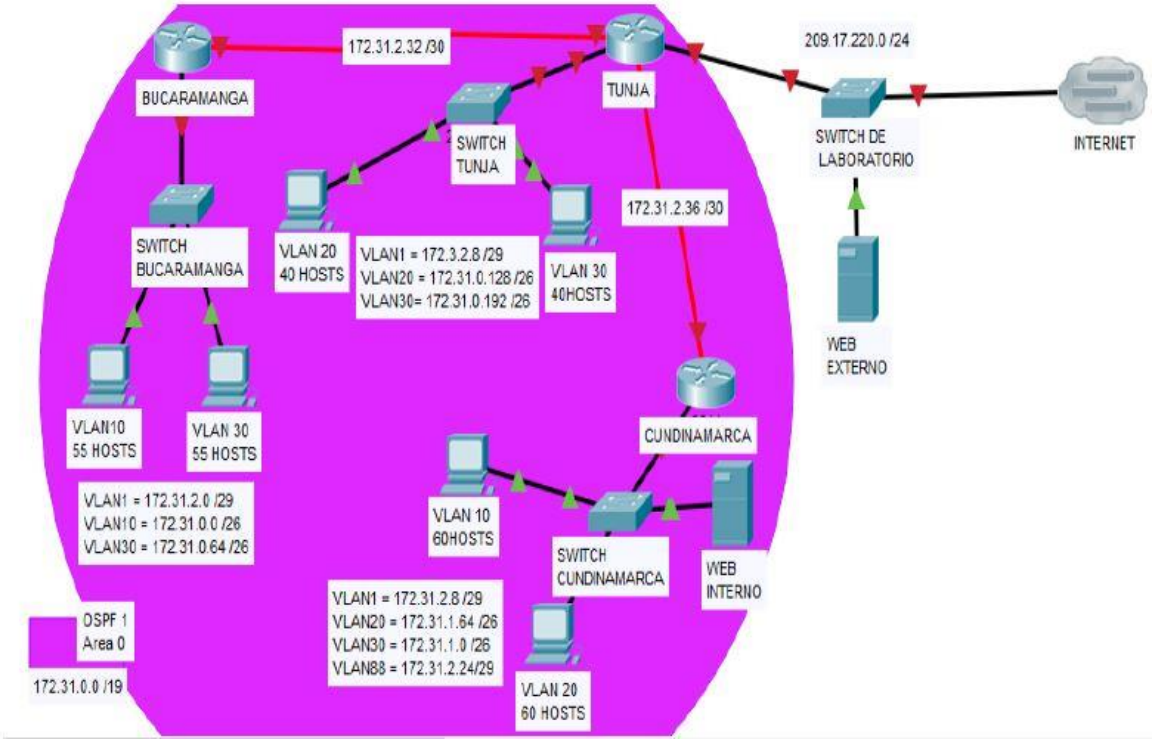
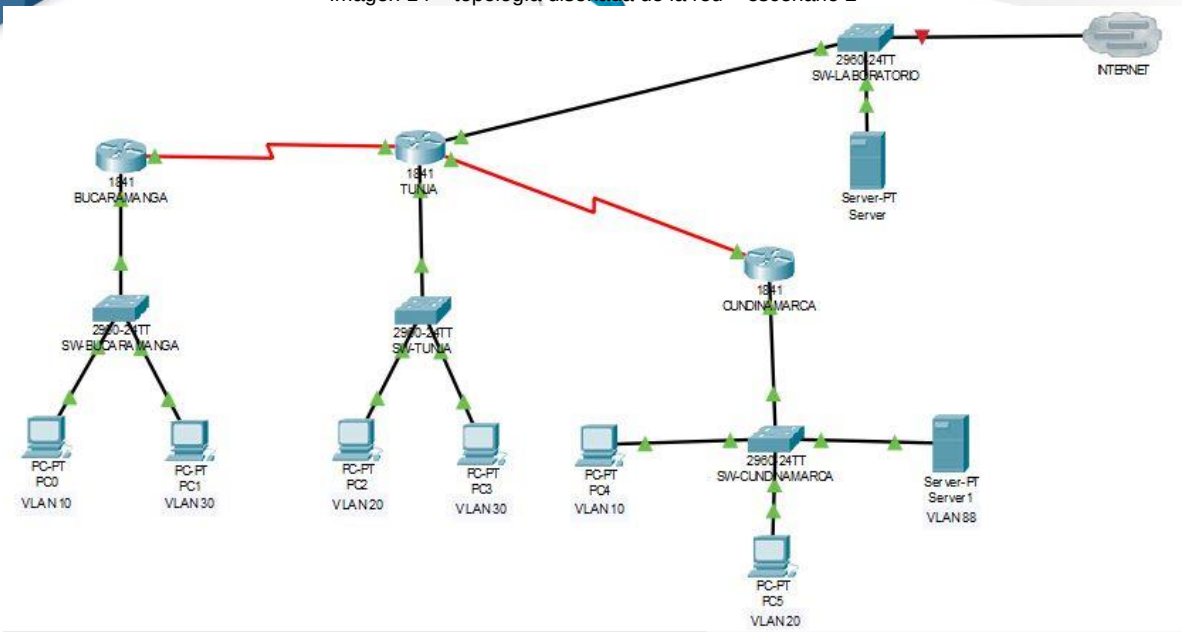


Imagen 14 – topología diseñada de la red – escenario 2



Fuente Packet Tracert

4.4 Configuración Básica Routers

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

```
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 #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 209.165.220.1 255.255.255.0
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 area 0
TUNJA(config-router)#network 172.31.0.192 0.0.0.63 area 0
TUNJA(config-router)#network 172.31.2.32 0.0.0.3 area 0
TUNJA(config-router)#network 172.31.2.36 0.0.0.3 area 0
TUNJA(config-router)#end
TUNJA#
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>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 #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

CUNDINAMARCA#

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)#
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-gateway 172.3.2.9
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)#
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)#

4.5 Autenticación local con AAA.

```
BUCARAMANGA(config-line)#username administrador secret cisco12345
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

TUNJA(config-line)#username administrador secret cisco12345
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

CUNDINAMARCA(config-line)#username administrador secret cisco12345
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
```

4.6 Cifrado de contraseñas.

```
BUCARAMANGA(config)#service password-encryption

TUNJA(config)#service password-encryption

CUNDINAMARCA(config)#service password-encryption
```

4.7 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
```

4.8 Máximo tiempo de acceso al detectar ataques.

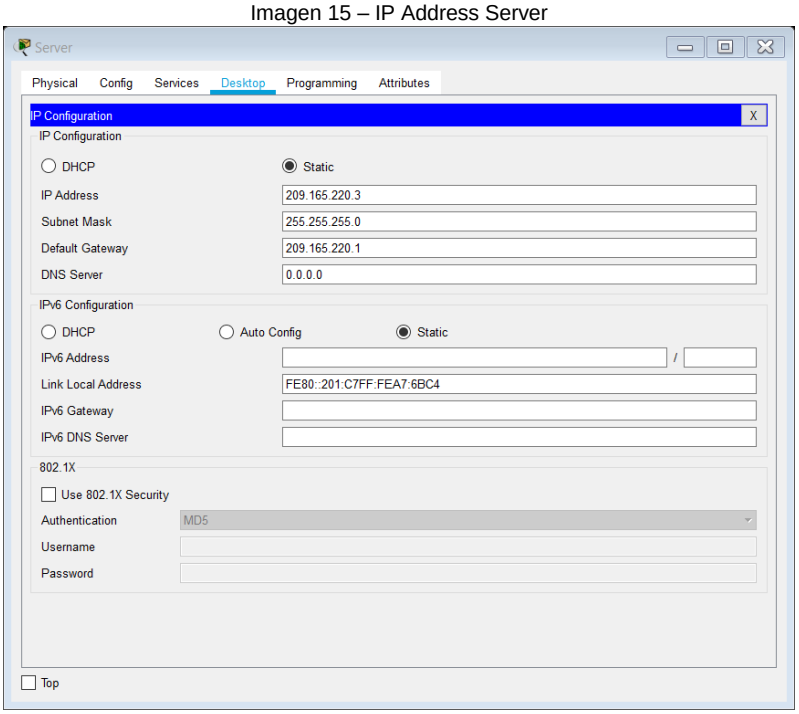
BUCARAMANGA(config-line)#login block-for 5 attempts 4 within 60

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

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

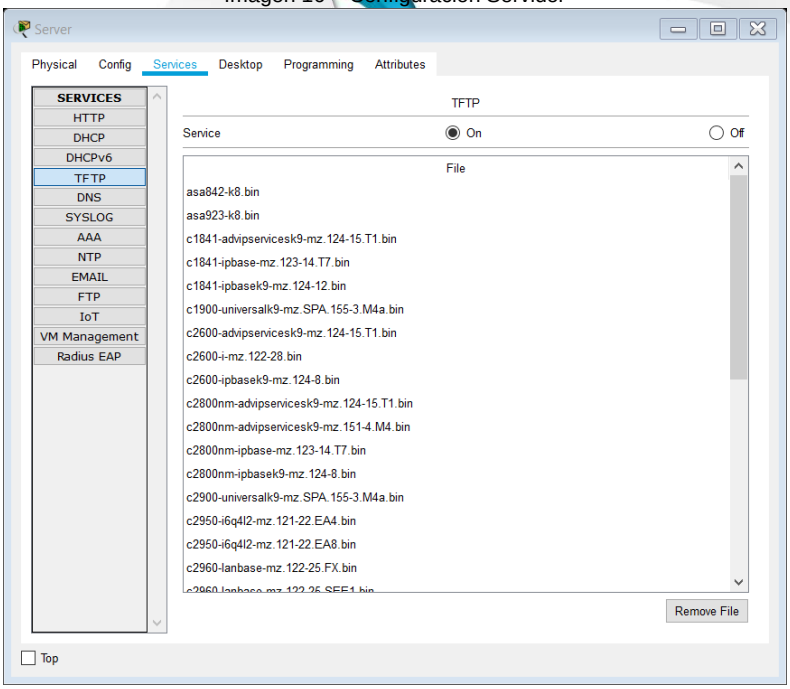
4.9 Establezca un servidor TFTP y almacene todos los archivos necesarios de los routers

Imagen 15 – IP Address Server



Fuente Packet Tracert

Imagen 16 – Configuración Servidor



Fuente Packet Tracert

4.10 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)#

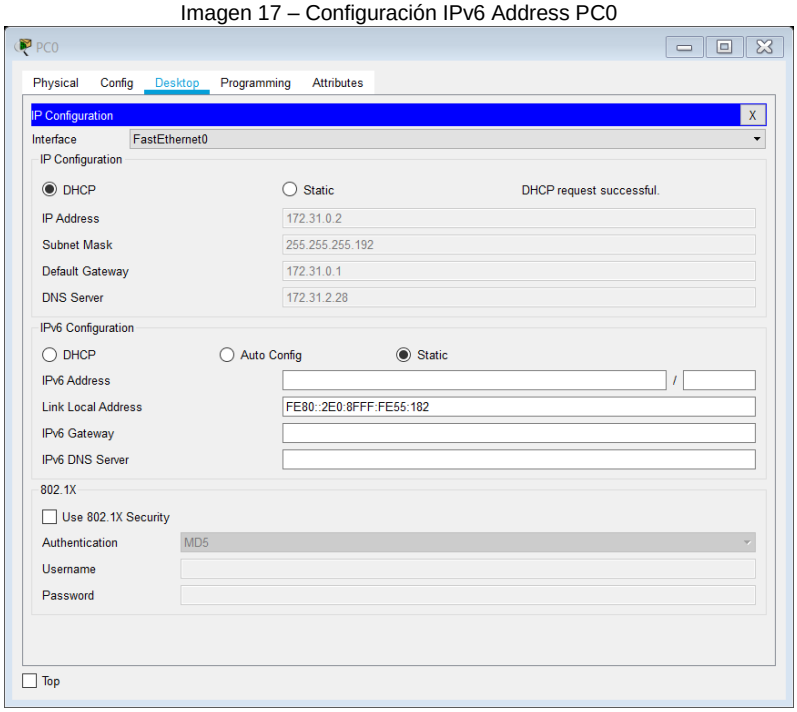
BUCARAMANGA(config)#int f0/0.10
BUCARAMANGA(config-subif)#ip helper-address 172.31.2.33
BUCARAMANGA(config-subif)#int f0/0.30
BUCARAMANGA(config-subif)#ip helper-address 172.31.2.33
BUCARAMANGA(config-subif)#end
BUCARAMANGA#
BUCARAMANGA#
%SYS-5-CONFIG_I: Configured from console by console

BUCARAMANGA#

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

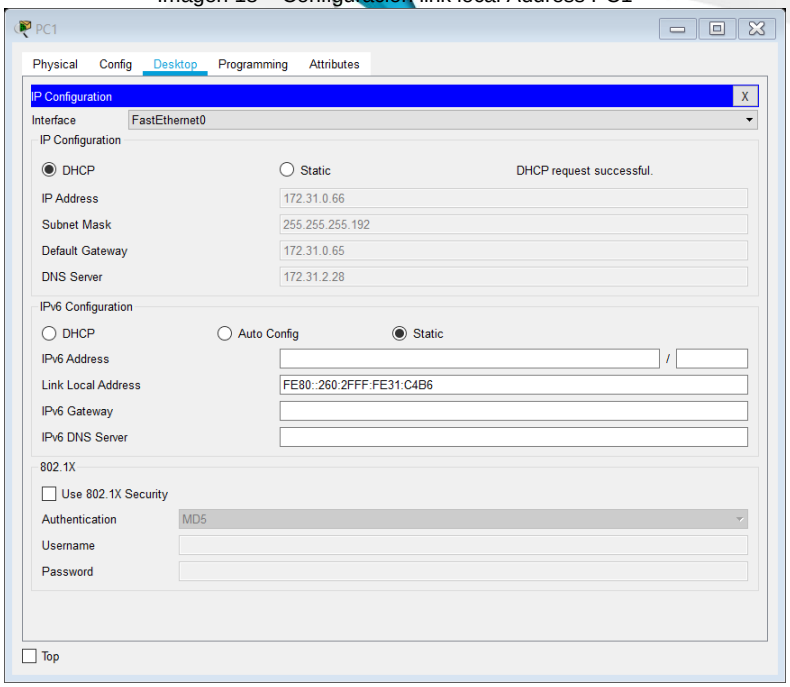
CUNDINAMARCA#

Imagen 17 – Configuración IPv6 Address PC0



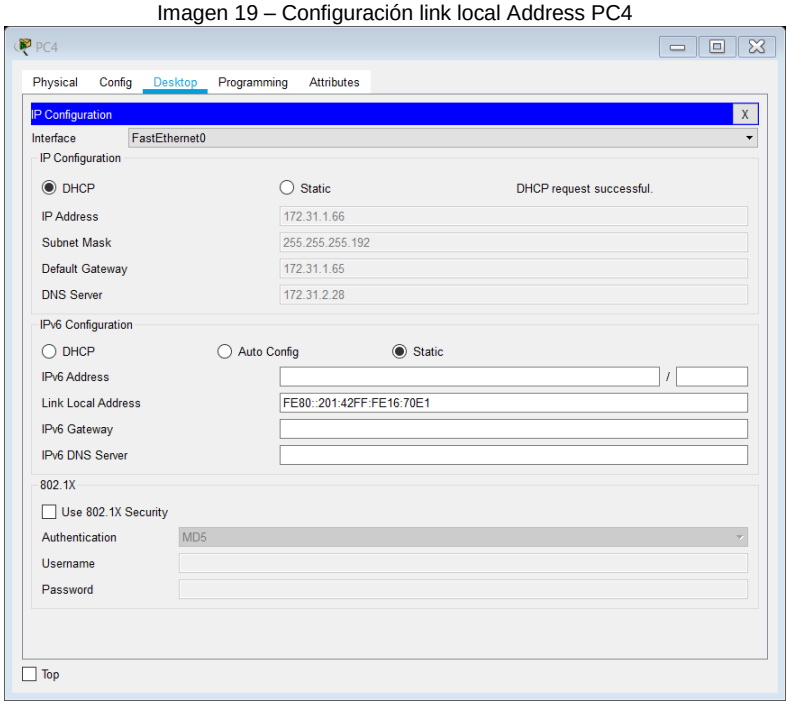
Fuente Packet Tracert

Imagen 18 – Configuración link local Address PC1



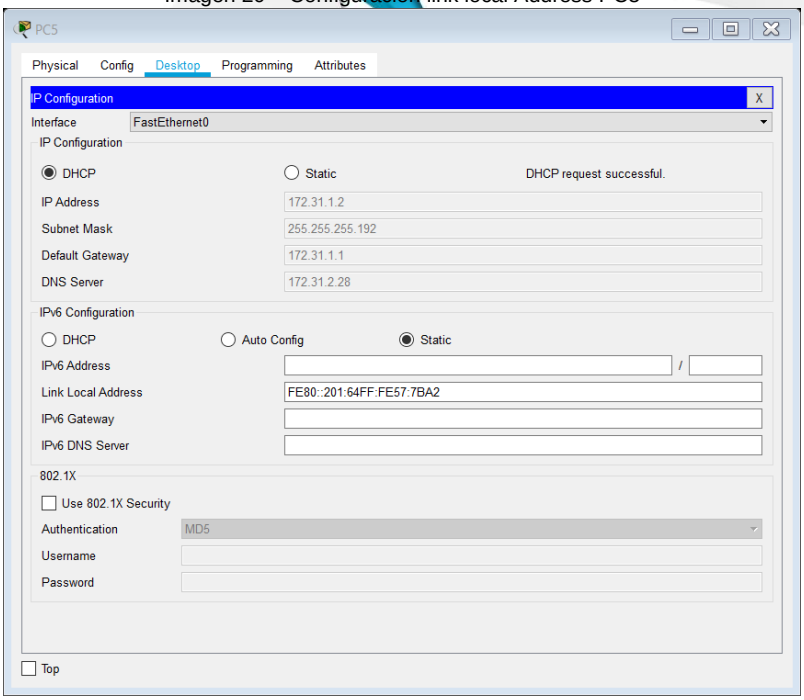
Fuente Packet Tracert

Imagen 19 – Configuración link local Address PC4



Fuente Packet Tracert

Imagen 20 – Configuración link local Address PC5



Fuente Packet Tracert

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

```
TUNJA(dhcp-config)#ip nat inside source static 172.31.2.28 209.165.220.4
TUNJA(config)#access-list 1 permit 172.0.0.0 0.255.255.255
TUNJA(config)#ip nat inside source list 1 interface f0/1 overload
TUNJA(config)#int f0/1
TUNJA(config-if)#ip nat outside
TUNJA(config-if)#int f0/0.1
TUNJA(config-subif)#ip nat inside
TUNJA(config-subif)#int f0/0.20
TUNJA(config-subif)#ip nat inside
TUNJA(config-subif)#int f0/0.30
TUNJA(config-subif)#ip nat inside
TUNJA(config-subif)#int s0/0/0
TUNJA(config-if)#ip nat inside
TUNJA(config-if)#int s0/0/1
TUNJA(config-if)#ip nat inside
TUNJA(config-if)#exit
TUNJA(config)#ip route 0.0.0.0 0.0.0.0 209.165.220.3
TUNJA(config)#router ospf 1
```

```
TUNJA(config-router)#default-information originate
TUNJA(config-router)#

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

Gateway of last resort is 209.165.220.3 to network 0.0.0.0

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

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

Gateway of last resort is 172.31.2.33 to network 0.0.0.0

172.3.0.0/29 is subnetted, 1 subnets
O 172.3.2.8 [110/65] via 172.31.2.33, 00:25:08, Serial0/0/0
172.31.0.0/16 is variably subnetted, 11 subnets, 3 masks
C 172.31.0.0/26 is directly connected, FastEthernet0/0.10
```

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

BUCARAMANGA#

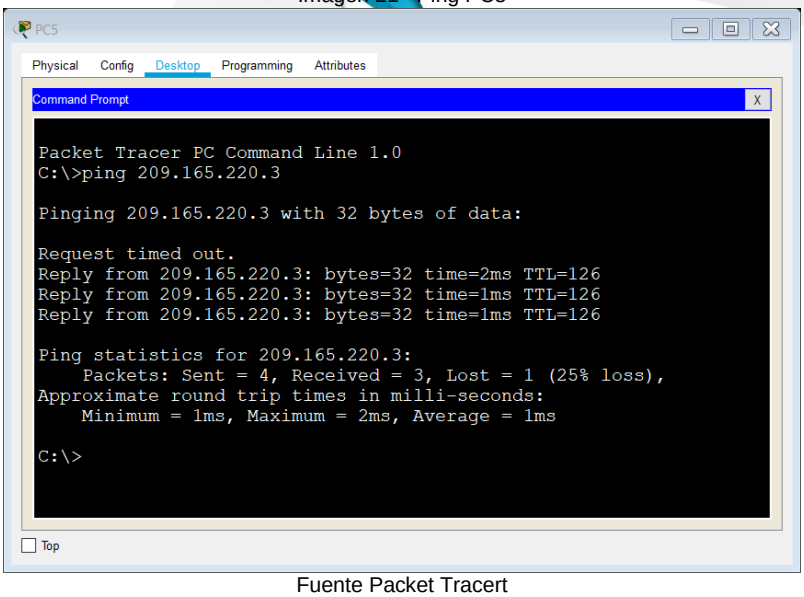
CUNDINAMARCA#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1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

Gateway of last resort is 172.31.2.37 to network 0.0.0.0

172.3.0.0/29 is subnetted, 1 subnets
O 172.3.2.8 [110/65] via 172.31.2.37, 00:24:15, Serial0/0/0
172.31.0.0/16 is variably subnetted, 11 subnets, 3 masks
O 172.31.0.0/26 [110/129] via 172.31.2.37, 00:24:15, Serial0/0/0
O 172.31.0.64/26 [110/129] via 172.31.2.37, 00:24:15, Serial0/0/0
O 172.31.0.128/26 [110/65] via 172.31.2.37, 00:24:15, Serial0/0/0
O 172.31.0.192/26 [110/65] via 172.31.2.37, 00:24:15, Serial0/0/0
C 172.31.1.0/26 is directly connected, FastEthernet0/0.30
C 172.31.1.64/26 is directly connected, FastEthernet0/0.20
O 172.31.2.0/29 [110/129] via 172.31.2.37, 00:24:15, Serial0/0/0
C 172.31.2.8/29 is directly connected, FastEthernet0/0.1
C 172.31.2.24/29 is directly connected, FastEthernet0/0.88
O 172.31.2.32/30 [110/128] via 172.31.2.37, 00:24:15, Serial0/0/0
C 172.31.2.36/30 is directly connected, Serial0/0/0
O*E2 0.0.0.0/0 [110/1] via 172.31.2.37, 00:02:24, Serial0/0/0

CUNDINAMARCA#

Imagen 21 –Ping PC5



Fuente Packet Tracert

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

TUNJA#

4.12 El enrutamiento deberá tener autenticación.

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

TUNJA(config-if)#
00:31:42: %OSPF-5-ADJCHG: Process 1, Nbr 172.31.2.38 on Serial0/0/1 from LOADING to FULL, Loading Done

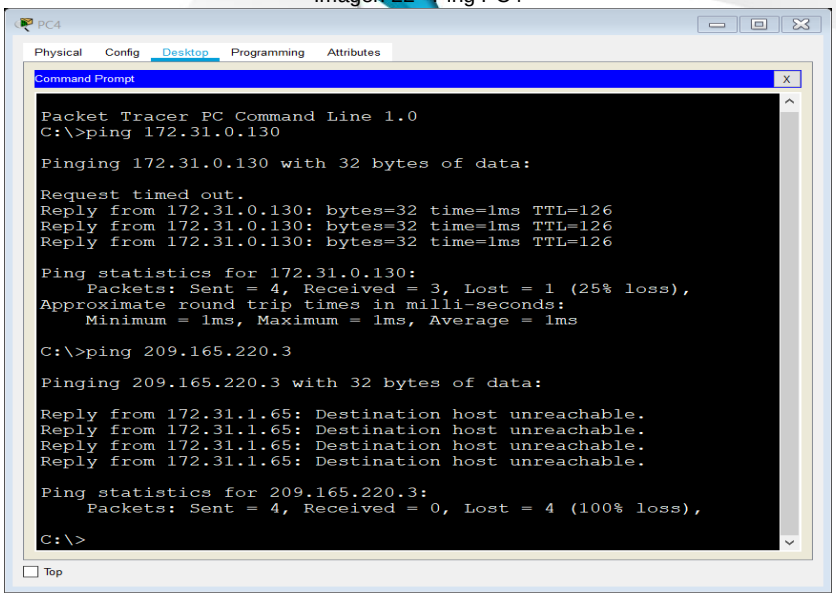
TUNJA(config-if)#

4.13 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)#

Imagen 22 –Ping PC4

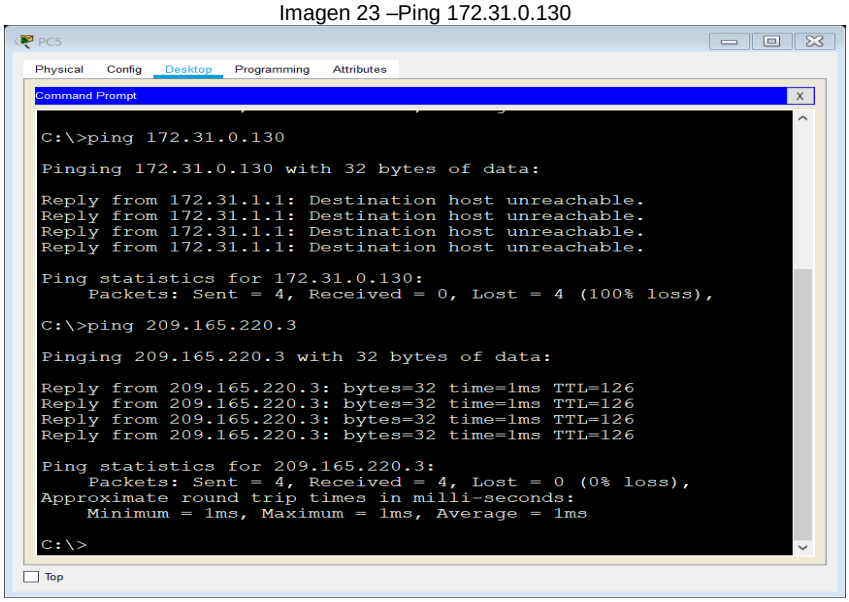


Fuente Packet Tracert

4.14 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)#

Imagen 23 –Ping 172.31.0.130

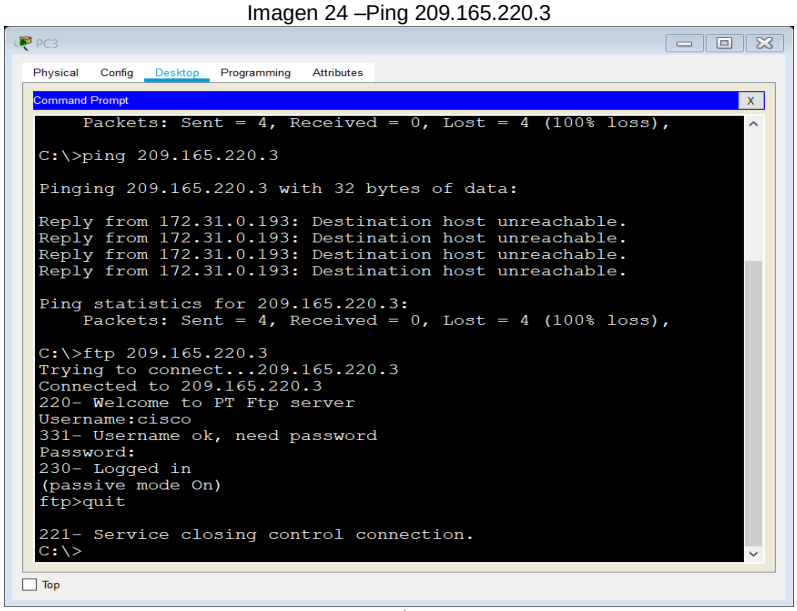


Fuente Packet Tracert

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

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

Imagen 24 –Ping 209.165.220.3



Fuente Packet Tracert

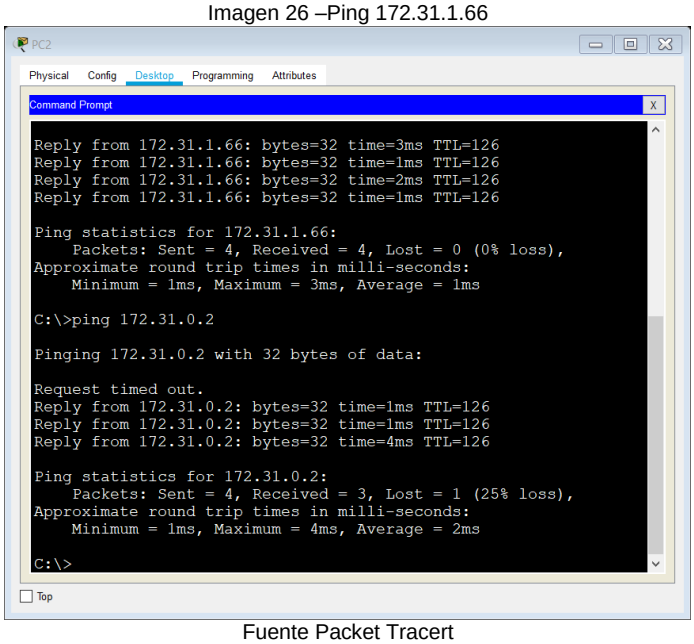
Imagen 25 – Verificación http//209.165.220.3

Fuente Packet Tracert

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

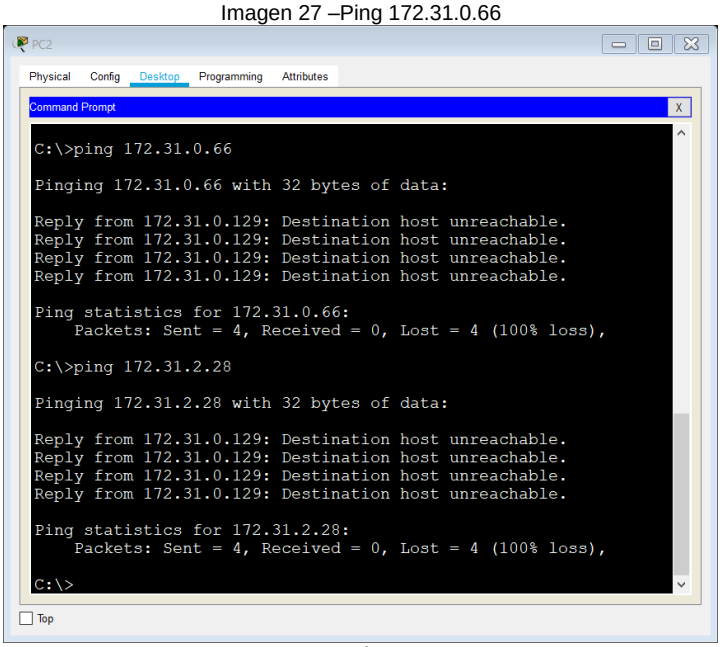
TUNJA(config-subif)#access-list 112 permit ip 172.31.0.128 0.0.0.63 172.31.1.64 0.0.0.63
TUNJA(config)#access-list 112 permit ip 172.31.0.128 0.0.0.63 172.31.0.0 0.0.0.63
TUNJA(config)#int f0/0.20
TUNJA(config-subif)#ip access-group 112 in
TUNJA(config-subif)#

Imagen 26 –Ping 172.31.1.66



Fuente Packet Tracert

Imagen 27 –Ping 172.31.0.66

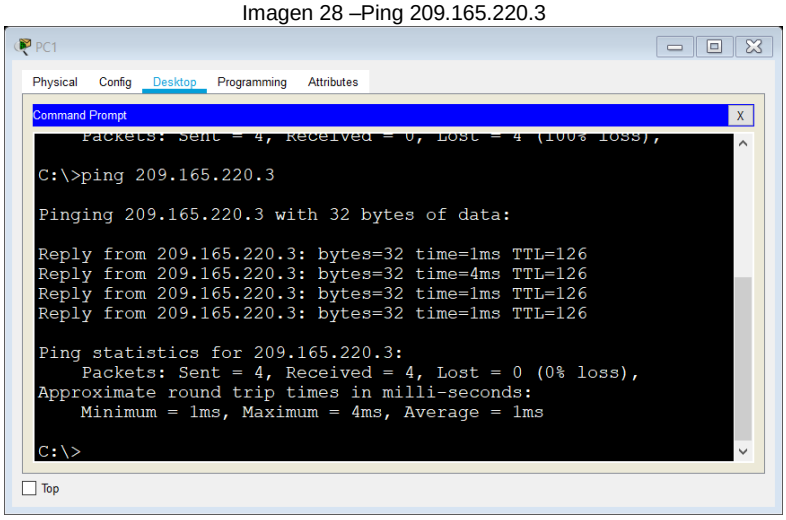


Fuente Packet Tracert

4.17 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)#

Imagen 28 –Ping 209.165.220.3

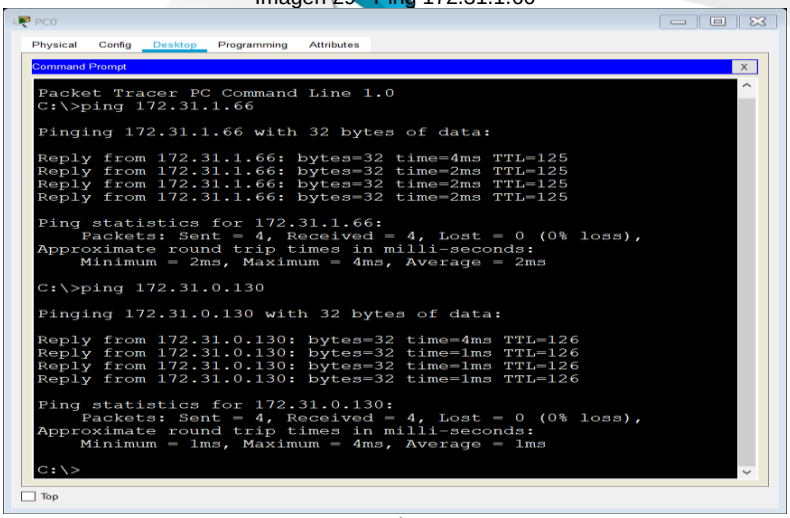


Fuente Packet Tracert

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

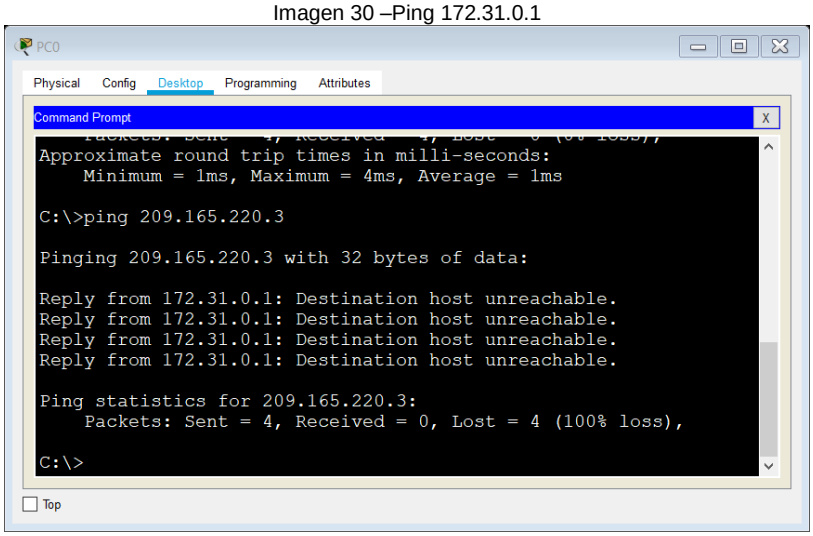
BUCARAMANGA(config-subif)#access-list 112 permit ip 172.31.0.0 0.0.0.63 172.31.1.64 0.0.0.63
BUCARAMANGA(config)#access-list 112 permit ip 172.31.0.0 0.0.0.63 172.31.0.128 0.0.0.63
BUCARAMANGA(config)#int f0/0.10
BUCARAMANGA(config-subif)#ip access-group 112 in
BUCARAMANGA(config-subif)#

Imagen 29 –Ping 172.31.1.66



Fuente Packet Tracert

Imagen 30 –Ping 172.31.0.1



Fuente Packet Tracert

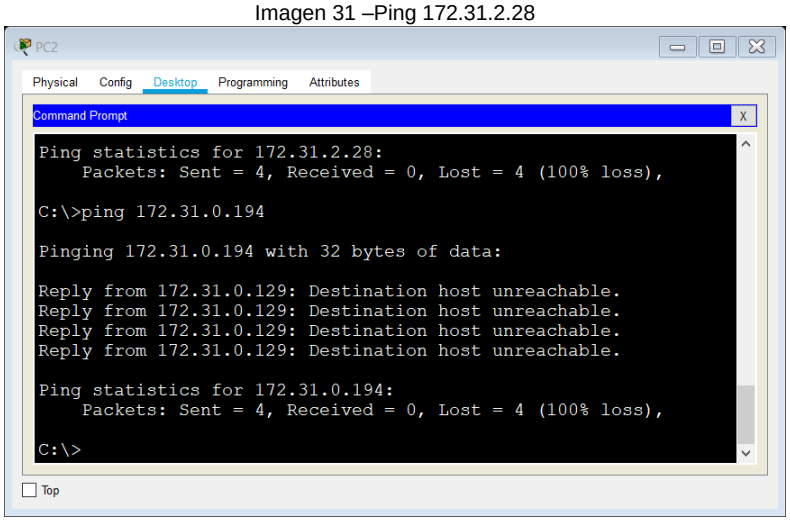
4.19 Los hosts de una VLAN no pueden acceder a los de otra VLAN en una ciudad.

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

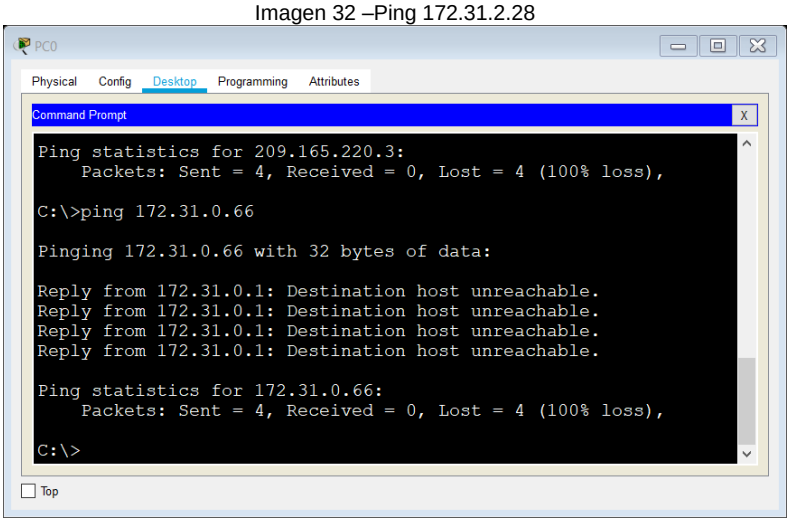
```
TUNJA(config)#access-list 113 deny ip 172.3.0.192 0.0.0.63 172.31.0.128 0.0.0.63
TUNJA(config)#access-list 113 permit ip any any
TUNJA(config)#int f0/0.20
TUNJA(config-subif)#ip access-group 113 out
TUNJA(config-subif)#

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
CUNDINAMARCA(config-subif)#
```

Imagen 31 –Ping 172.31.2.28



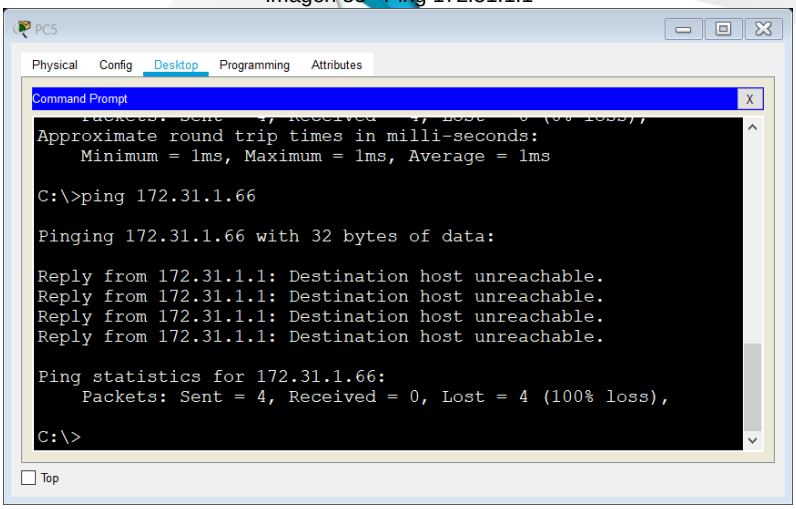
Fuente Packet Tracert

Imagen 32 –Ping 172.31.2.28



Fuente Packet Tracert

Imagen 33 –Ping 172.31.1.1



Fuente Packet Tracert

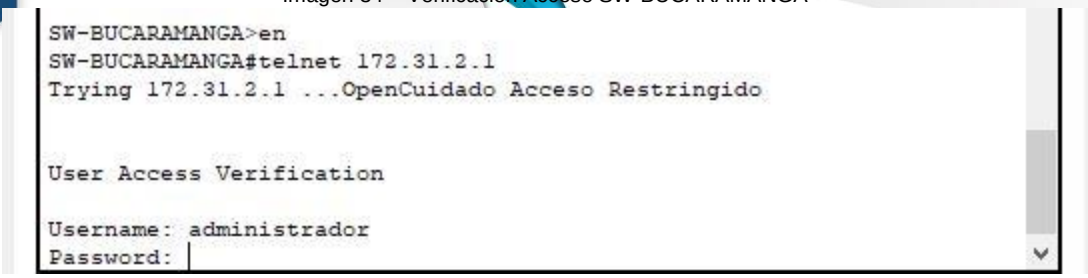
4.20 Solo los hosts de las VLAN administrativas y de la VLAN de servidores tienen accedo a los routers e internet.

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

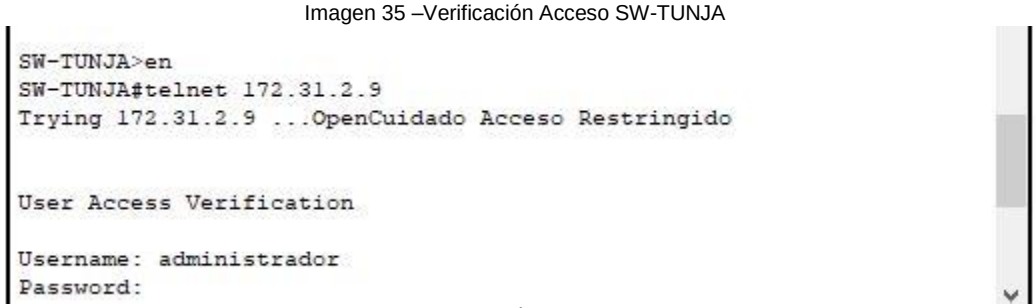
CUNDINAMARCA(config-subif)#access-list 3 permit 172.31.2.0 0.0.0.7
CUNDINAMARCA(config)#access-list 3 permit 172.3.2.8 0.0.0.7
CUNDINAMARCA(config)#access-list 3 permit 172.31.2.8 0.0.0.7
CUNDINAMARCA(config)#line vty 0 15
CUNDINAMARCA(config-line)#access-class 3 in
CUNDINAMARCA(config-line)#

Imagen 34 – Verificación Acceso SW-BUCARAMANGA



Fuente Packet Tracert

Imagen 35 –Verificación Acceso SW-TUNJA



Fuente Packet Tracert

Aspectos a tener en cuenta

- ✓ Habilitar VLAN en cada switch y permitir su enrutamiento.
- ✓ Enrutamiento OSPF con autenticación en cada router.
- ✓ Servicio DHCP en el router Tunja, mediante el helper address, para los routers Bucaramanga y Cundinamarca.
- ✓ Configuración de NAT estático y de sobrecarga.
- ✓ Establecer una lista de control de acceso de acuerdo con los criterios señalados.
- ✓ Habilitar las opciones en puerto consola y terminal virtual

CONCLUSIONES

En esta práctica aprendí a enrutar VLAN por medio de un protocolo y a segmentar redes a través de VLAN para reducir el dominio de broadcast y evitar colisiones.

Aprendí las ventajas de usar un protocolo de enrutamiento con VLAN, que al encapsular se facilita el proceso de enrutamiento en un entorno de múltiples VLAN.

Puedo concluir, la ventaja de utilizar VLAN y un protocolo de enrutamiento como EIGRP en una topología extensa, porque por un lado las VLAN segmentan la red y eso contribuye mucho en el proceso de enrutamiento y ayudan a evitar fallas o colisiones y EIGRP porque es un protocolo que presenta convergencias rápidas para encontrar las mejores rutas para comunicar las ciudades y tiene rutas de respaldo por si las rutas principales llegan fallar.

Al utilizar las interfaces VLAN para implementar una red, me ayudará a economizar, viéndolo desde el punto físico y real.

Finalmente, al usar protocolos de enrutamiento como EIGRP, me ayuda a finalizar la implementación de la red en un rango de tiempo menor al que me llevaría configurar dispositivo por dispositivo o PC por PC utilizando rutas estáticas. debo de decir que al usa VTP en los SWITCHS me hubiera servido de gran ayuda para terminar esta práctica en menor tiempo y con menores las probabilidades de encontrar errores al enrutar las VLAN.

Por otra parte, al desarrollar listas de acceso, puedo concluir que la seguridad dentro de una red es indispensable para la protección de los dispositivos y la información que se transporta por medio de esos dispositivos.

Se mejora y se limita el trafico como su nombre lo indica, por medio de sus restricciones ayudando a que una red sea estable.

Finalmente, aparte de ayudar con la seguridad, controlar el tráfico, permitir y bloquear el usar ACL, creo que es una herramienta de mucha ayuda para realizar cada uno de los procesos anteriormente mencionados, pues esta es fácil de configurar, se presta para analizar las rutas de una topología y optimizar el debido funcionamiento de la red.

BIBLIOGRAFÍA

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

Vesga, J. (2014). Configuración de Switches y Routers [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgL9QChD1m9EuGqC

Macfarlane, J. (2014). Network Routing Basics : Understanding IP Routing in Cisco Systems. Recuperado de http://bibliotecavirtual.unad.edu.co:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=e000xww&AN=158227&lang=es&site=ehost-live

Lucas, M. (2009). Cisco Routers for the Desperate : Router and Switch Management, the Easy Way. San Francisco: No Starch Press. Recuperado de https://1drv.ms/b/s!AmIJYei-NT1Im3L74BZ3bpMiXRx0

Odom, W. (2013). CISCO Press (Ed). CCNA ICND1 Official Exam Certification Guide. Recuperado de http://ptgmedia.pearsoncmg.com/images/9781587205804/samplepages/9781587205804.pdf

Odom, W. (2013). CISCO Press (Ed). CCNA ICND2 Official Exam Certification Guide. Recuperado de http://mr-telecomunicaciones.com/wp-content/uploads/2018/09/wendellodom.pdf