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

Prueba De Habilidades CCNA

Autor

Edilberto Laverde Bernal

TUTOR

Jose Ignacio Cardona

Universidad nacional abierta y a distancia - UNAD

Escuela de ciencias básicas, tecnología e ingeniería - ECBTI

Ingeniería de sistemas

Palmira - valle

Diciembre 12 de 2019

Tabla De Contenido

Resumen

Con la evolución y crecimiento de las telecomunicaciones y tecnologías de la información y como el hombre en su afán de buscar una comunicación más asertiva y de manera más rápida aplicada en su diario vivir a desarrollado herramientas de aprendizaje que permiten lograr todo esto.

Es por eso por lo que Packet Tracer es una herramienta de simulación de redes que a través de su entorno interactivo permite desarrollar diferentes tipos de redes que permiten grandemente mejorar esa comunicación a través de la unión de varios dispositivos en una sola red de comunicación. Esta herramienta nos ayuda a simular redes de empresas basándose en sus necesidades, con esta herramienta se pueden configurar la manera como se comunicarán cada equipo, que seguridad será utilizada y los permisos de accesos que cada dispositivo debe tener para garantizar una buena comunicación.

A atreves del curso de cisco CCNA 1 y CCNA2, en sus diferentes actividades presentes durante el diplomado, nos enfocaron en la importancia de definir varios aspectos a tener en cuenta para diseñar una topología, esta herramienta diseñada para que tanto estudiantes como instructores utilicen Packet Tracer como una herramienta educativa donde se pueden desarrollar simulaciones de redes, utilizando una interfaz de comandos en cada uno de los dispositivos ejerciendo con ello un aprendizaje autónomo en cada una de las practicas creando topologías de redes, insertando paquetes gracias a su interfaz visual e intuitiva.

La forma de operar de Packet Tracer es muy amigable ya que podemos configurar la red que deseamos con solo arrastrar cada uno de los dispositivos que necesitamos de acuerdo con la topología de la red, luego dando clic en cada uno de ellos podemos ingresar y configurar usando los comandos que ofrece cisco, después de terminada la red podemos simular la conectividad de la red y las posibles mejoras u oportunidades presentes.

Es así como la UNAD complementa el diplomado de profundización cisco con esta herramienta interactiva que permite tanto a los instructores como a estudiantes profundizar en el aprendizaje autónomo y forjarse como ingenieros en telecomunicaciones con habilidades de diseñar ya administrar redes .

Absctrac

With the evolution and growth of telecommunications and information technologies and as the man in his eagerness to seek more assertive communication and more quickly applied in his diary, live to develop learning tools that allow to achieve all this.

That is why Packet Tracer is a network simulation tool that through its interactive environment allows to develop different types of networks that greatly improve that communication through the union of several devices in a single communication network. This tool helps us to simulate networks of companies based on their needs, with this tool you can configure the way each team will communicate, what security will be used and the access permissions that each device must have to ensure good communication.

Through the cisco course CCNA 1 and CCNA2, in their different activities present during the diploma, we focused on the importance of defining several aspects to consider to design a topology, this tool designed for both students and instructors to use Packet Tracer as an educational tool where network simulations can be developed, using a command interface on each of the devices, thereby exercising autonomous learning in each of the practices creating network topologies, inserting packages thanks to its visual and intuitive interface.

The way Packet Tracer operates is very friendly since we can configure the network we want by simply dragging each of the devices we need according to the topology of the network, then clicking on each of them we can enter and configure using The commands offered by Cisco, after the end of the network, we can simulate the network connectivity and the possible improvements or opportunities present.

This is how UNAD complements the cisco deepening diploma with this interactive tool that allows both instructors and students to deepen autonomous learning and forge as telecommunications engineers with skills in designing and managing networks.

Introducción

Extender y potenciar nuestra capacidad de comunicarnos en un mundo que avanza tecnológicamente a pasos agigantados y partiendo que el uso de internet es la base para nuevas creaciones y desarrollo innovador para esta generación que estamos viviendo y que seguirá creciendo a través del tiempo, nos asegurara estar a la vanguardia de las comunicaciones, de aquí la importancia del correcto desarrollo del presente curso que mediante diferentes herramientas tecnológicas como Cisco Packet Tracer, las cuales nos permite adquirir destreza de una forma práctica y de fácil comprensión llevándonos paso a paso a la consecución del conocimiento suficiente para afrontar cualquier tipo de situación se nos presente en el desarrollo en el ámbito profesional.

Por tal motivo el presente trabajo se realiza con el fin de demostrar y aplicar los conocimientos adquiridos al cursar los módulos de CCNA 1 y CCNA 2 en el cual encontramos temas como la configuración de protocolos como listas de control de acceso, DHCP, NAT y el tema que profundiza el conocimiento de los temas anteriores y le permite al administrador de la red adquirir habilidades para detectar, administrar y realizar mantenimiento a los dispositivos de comunicación como son los Switch y routers principalmente.

En el presente trabajo se evidenciará el desarrollo de diferentes ejercicios prácticos donde se diseñarán topologías de red las cuales se configuran utilizando diferentes comandos para la configuración de un Switch, Router, PC y de igual forma presentamos las pruebas de comunicación entre los dispositivos usados para tal fin, lo que nos permite adquirir destrezas y conocimiento en los temas

Objetivos

Objetivo General

Realizar configuraciones avanzadas en Reuters, Switch y dispositivos con el propósito de unificar los conocimientos adquiridos en los casos de estudio de los módulos CCNA 1 y CCNA 2 implementando RIP, OSPF y enrutamiento estático; bajo un esquema de direccionamiento IP sin clase, para dar soluciones de red y conectividad escalables, mediante el uso de los principios de enrutamiento y conmutación de paquetes en ambientes LAN y WAN

Objetivos Específicos

- ✓ Instalar y conocer el funcionamiento de la herramienta Cisco Packet Tracer.
- ✓ Diseñar las topologías en los escenarios 1 y 2, teniendo en cuenta la cantidad de Host y subredes presentes en los escenarios 1 y 2
- ✓ Conectar dispositivos y desarrollar un esquema de direccionamiento y prueba.
- ✓ Adquirir el conocimiento sobre las listas de control de acceso.
- ✓ Configurar un servidor de protocolo de configuración dinámica de host (DHCP).
- ✓ Conocer las herramientas que pueden usar los administradores de redes para la detección, la administración y el mantenimiento de dispositivos.
- ✓ Utilizar funciones comunes de las redes para verificar pequeñas operaciones de red y analizar el tráfico de datos.

Descripción de escenarios propuestos para la prueba de habilidades

Escenario 1

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

Topología de red

Los requerimientos solicitados son los siguientes:

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

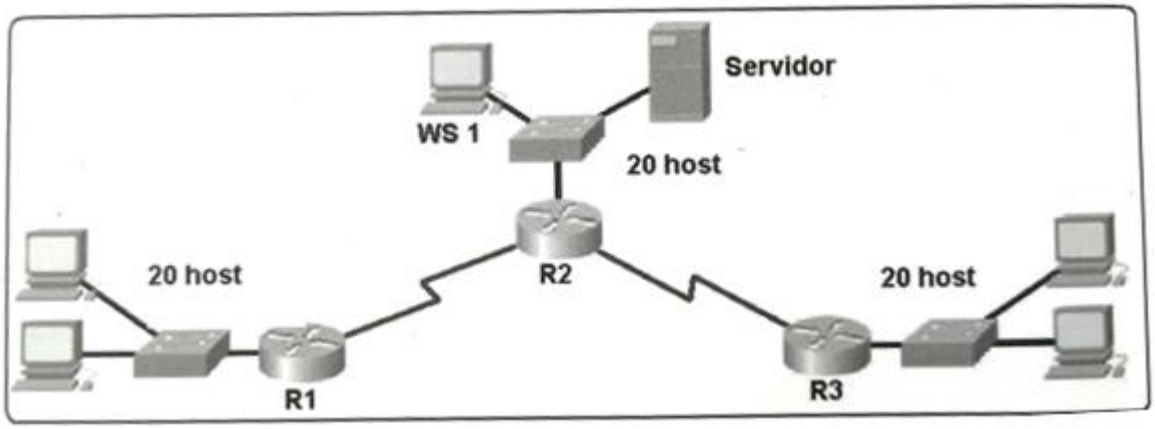
Parte 2: Considerar la asignación de los parámetros básicos y la detección de vecinos directamente conectados.

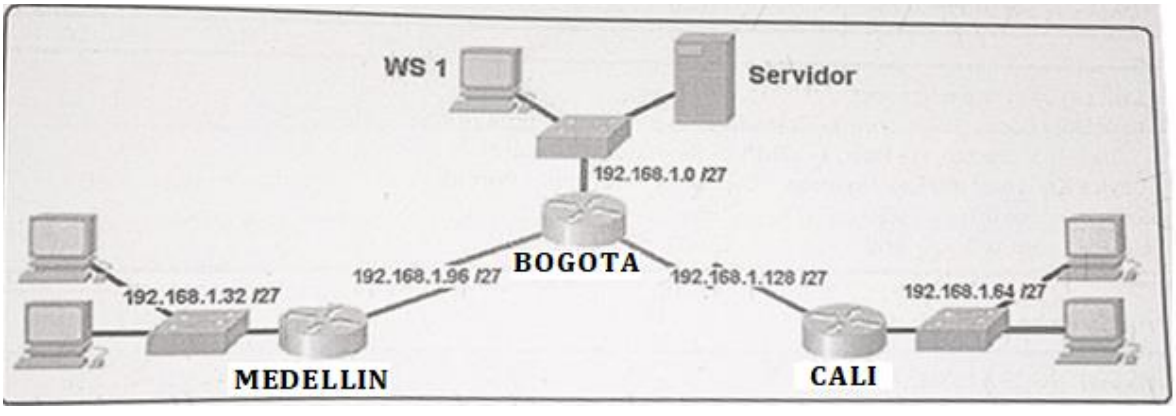
Parte 3: La red y subred establecidas deberán tener una interconexión total, todos los hosts deberán ser visibles y poder comunicarse entre ellos sin restricciones.

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

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

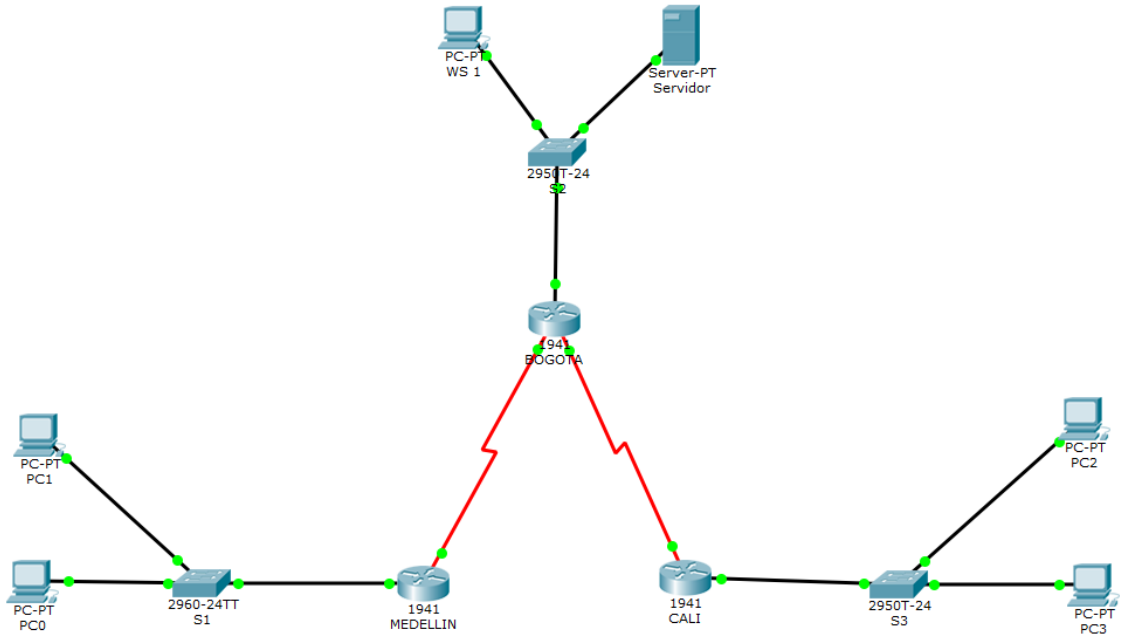
Parte 6: Configuración final.





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.



Recursos necesarios

- 3 Reuters (Cisco 1941 con IOS de Cisco versión 15.2(4)M3).
- 3 Switch (Cisco 2960 con IOS de Cisco versión 15.0(2).
- 5 pc con Windows
- 1 servidor computadoras (Windows 7, Vista o XP con un programa de emulación de terminal)
- Cables Ethernet y seriales, como se muestra en la topología

Parte 1: Asignación de direcciones IP:

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

Para realizar el proceso de dividir la red es tomar los valores de cada direccion IP y su mascara de red y calcula la dirección broadcast, red, Cisco wildcard mask y el número de IPs en la red. Este proceso lo podemos realizar con calculadoras IP

1.

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

2.

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

3.

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

4.

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

5.

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

6.

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

7.

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

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

Como resultado final tenemoas las 8 subredes en caso de un crecimientos en la red

Para realizar el proceso de asignación de las IP en cada uno de los router, ingresamos a cada router dando clic en cada uno de ellos, a modo excec privilegiado con el comando **enable**, luego digitamos el **comando config** terminal es decir el modo de configuración.

Posteriormente procedemos a crear cada una de las interfaces con sus respectivas direcciones IP, para ello utilizamos el comando **interface** ejemplo (interface g0/0) y con el comado **ip address** asignamos las IP (ip address 192.168.1.64 255.255.255.224) y despues de crear la interface, con el comando **no shutdown** activamos la interfaz del Router

Configuracion de la IP en R1 Medellin

```
Medellin(config)# interface s0/0/0
Medellin(config-if)#clock rate 128000
Medellin(config-if)#ip address 192.168.1.99 255.255.255.224
Medellin(config-if)#no shutdown

Medellin(config)#interface g0/0
Medellin(config-if)#ip address 192.168.1.33 255.255.255.224
Medellin(config-if)#no shutdown
```

Configuracion de la IP en R2 Bogota

```
Bogota(config-if)#interface s0/0/0
Bogota(config-if)#clock rate 128000
Bogota(config-if)#ip address 192.168.1.98 255.255.255.224
Bogota(config-if)#no shutdown

Bogota(config)#interface s0/0/1
Bogota(config-if)#clock rate 128000
Bogota(config-if)#ip address 192.168.1.130 255.255.255.224
Bogota(config-if)#no shutdown

Bogota(config)#interface g0/0
Bogota(config-if)#ip address 192.168.1.1 255.255.255.224
Bogota(config-if)#no shutdown
```

Configuracion de la IP en R3 Cali

```
Cali(config)#interface s0/0/0
Cali(config-if)#clock rate 128000
Cali(config-if)#ip address 192.168.1.131 255.255.255.224
Cali(config-if)#no shutdown

Cali(config-if)#interface g0/0
Cali(config-if)#ip address 192.168.1.65 255.255.255.224
Cali(config-if)#no shutdown

Cali(config)#interface s0/0/1
Cali(config-if)#clock rate 128000
Cali(config-if)#ip address 192.168.1.193 255.255.255.224
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.

	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

Configuración del Router R1 Medellin

Para la configuración básica de cada Router y Switch, presentes en la topología Ingresamos a cada uno de ellos en modo exec configurado con el comando **enable** y luego con el comando **configure terminal,** posteriormente a cada dispositivo asignamos el nombre con el comando **hostname**, desactivamos la búsqueda de DNS con el comando **no ip domain lookup,** creamos la contraseña cifrada con el comando **line vty,** encriptamos las contraseñas con el comando **service password-encryption** por ultimo a cada Router y Switch asignamos el mensaje que está prohibido el acceso no autorizado a cada dispositivo esto lo hacemos con el comando **banner motd** #Esta prohibido el acceso no autorizado# autorizado#

Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.

Con el comando Hostname, damos el nombre del host
Router(config)#hostname Medellin
Medellin(config)#

Con el comando no ip domain lookup, desactivamos la búsqueda DNS.

Medellin(config)#no ip domain lookup
Medellin(config)#

Asigno class como la contraseña cifrada del modo EXEC privilegiado. Con el comando enable secret

Medellin(config)#enable secret class
Medellin(config)#

Asigno cisco como la contraseña de consola y la contraseña de vty. Con el comando line vty 0 4 y el comando password

Medellin(config-line)#line con 0
Medellin(config-line)#password cisco
Medellin(config-line)#login
Medellin(config-line)#line vty 0 4
Medellin(config-line)#password cisco

Comando para encriptar las contraseñas
Medellin(config)#service password-encryption

Mensaje en e l Router
Medellin(config)#banner motd #Esta prohibido el acceso no autorizado#

autorizado#

Configuración del Router R2 Bogota

Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.

Con el comando Hostname, damos el nombre del host

Router(config)#hostname Bogota
Bogota(config)#

Con el comando no ip domain lookup, desactivamos la búsqueda DNS.

Bogota(config)#no ip domain lookup
Bogota(config)#

Asigno class como la contraseña cifrada del modo EXEC privilegiado. Con el comando enable secret

Bogota(config)#enable secret class
Bogota(config)#

Asigno cisco como la contraseña de consola y la contraseña de vty. Con el comando line vty 0 4 y el comando password

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)#

Comando para encriptar las contraseñas
Bogota (config)#service password-encryption

Mensaje en e l Router
Bogota (config)#banner motd #Esta prohibido el acceso no autorizado#

Configuración del Router R3 Cali

Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Con el comando Hostname, damos el nombre del host
Router(config)#hostname Cali
Cali(config)#

Con el comando no ip domain lookup, desactivamos la búsqueda DNS.

Cali(config)#no ip domain lookup
Cali(config)#

Asigno class como la contraseña cifrada del modo EXEC privilegiado. Con el comando enable secret

Cali(config)#enable secret class
Cali(config)#

Asigno cisco como la contraseña de consola y la contraseña de vty. Con el comando line vty 0 4 y el comando password

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

Comando para encriptar las contraseñas
Cali (config)#service password-encryption

Mensaje en e l Router
Cali (config)#banner motd #Esta prohibido el acceso no autorizado

Configuración del Switch 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)#line vty 0 4
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#exit
S1(config)#service password-encryption

S1(config)#banner motd #Esta prohibido el acceso no autorizado#

S1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]

S1(config)#interface vlan 1
S1(config-if)#ip address 192.168.1.97 255.255.255.224
S1(config-if)#no shutdown
```

Configuración del Switch 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)#line vty 0 4
S2(config-line)#password cisco
S2(config-line)#login
S2(config-line)#exit
S2(config)#service password-encryption
S2(config)#banner motd #Esta prohibido el acceso no autorizado#
S2(config)#exit
```

S2#
%SYS-5-CONFIG_I: Configured from console by console
S2#copy running-config st
S2#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]

Configuración del Switch S3

Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S3
S3(config)#no ip domain-lookup
S3(config)#enable secret class
S3(config)#line con 0
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#line vty 0 4
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#exit
S3(config)#service password-encryption
S3(config)#banner motd #Esta prohibido el acceso no autorizado#
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]

Configuración de los equipos PC

Después de asignar las IP de los Router y configurar los Switch, asignamos cada una de las IP de los 5 computadores y el servidor, esto lo asignamos de acuerdo como se quedó las 8 subredes

PC0	192.168.1.34	255.255.255.224	192.168.1.33
PC1	192.168.1.36	255.255.255.224	192.168.1.33
PC2	192.168.1.68	255.255.255.224	192.168.1.65
PC3	192.168.1.69	255.255.255.224	192.168.1.65
WS1	192.168.1.11	255.255.255.224	192.168.1.1
Servidor	192.168.1.10	255.255.255.224	192.168.1.1

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.

Con el comando **show ip route** verificamos la tabla de enrutamiento para cada Roter

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

Gateway of last resort is not set

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

Bogota#show ip route

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

Gateway of last resort is not set

192.168.1.0/24 is variably subnetted, 6 subnets, 2 masks
C 192.168.1.0/27 is directly connected, GigabitEthernet0/0
L 192.168.1.1/32 is directly connected, GigabitEthernet0/0
C 192.168.1.96/27 is directly connected, Serial0/0/0
L 192.168.1.98/32 is directly connected, Serial0/0/0
C 192.168.1.128/27 is directly connected, Serial0/0/1
L 192.168.1.130/32 is directly connected, Serial0/0/1
Bogota#
```

Cali#show ip route

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

Gateway of last resort is not set

192.168.1.0/24 is variably subnetted, 4 subnets, 2 masks
C 192.168.1.64/27 is directly connected, GigabitEthernet0/0
L 192.168.1.65/32 is directly connected, GigabitEthernet0/0
C 192.168.1.192/27 is directly connected, Serial0/0/1
L 192.168.1.193/32 is directly connected, Serial0/0/1
Cali#
```

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

Al igual que otros IGP, EIGRP permite el balanceo de carga cuando conoce la misma red por varios vecinos, y esta posee el mismo costo en todas estas. Esto es conocido como enrutamiento *equal-cost multipath* (ECMP, o enrutamiento de múltiples rutas del mismo costo).

Por defecto, en plataformas IOS vienen habilitadas un máximo de 4 rutas para hacer balanceo de carga (se permiten tener 4 rutas del mismo costo), la cual puede aumentar hasta un máximo de 32 ECMP por prefijos (redes).

Con el comando show ip route aplicado anteriormente, podemos observar el comportamiento de cada router y las interfaces presentes en cada uno

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

El comando **show cdp neighbors detail** muestra la direccion IP de un dispoditivo vecino.

Router Medellin
Medellin#show cdp neighbors detail

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: 134

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: S1

Entry address(es):
Platform: cisco 2950, Capabilities: Switch
Interface: GigabitEthernet0/0, Port ID (outgoing port): FastEthernet0/1
Holdtime: 170

Version:
Cisco Internetwork Operating System Software
IOS (tm) C2950 Software (C2950-I6Q4L2-M), Version 12.1(22)EA4, RELEASE SOFTWARE(fc1)
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Wed 18-May-05 22:31 by jharirba

advertisement version: 2
Duplex: full

Medellin#
Router Medellin

Medellin #show cdp neighbors detail

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: 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

Device ID: Cali
Entry address(es):
IP address : 192.168.1.193
Platform: cisco C1900, Capabilities: Router
Interface: Serial0/0/1, Port ID (outgoing port): Serial0/0/1
Holdtime: 144

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: S1
Entry address(es):
Platform: cisco 2960, Capabilities: Switch
Interface: GigabitEthernet0/0, Port ID (outgoing port): FastEthernet0/1
Holdtime: 143
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#

Router Cali
Cali#show cdp neighbors detail

Device ID: S3
Entry address(es):
Platform: cisco 2950, Capabilities: Switch
Interface: GigabitEthernet0/0, Port ID (outgoing port): FastEthernet0/1
Holdtime: 144
Version :
Cisco Internetwork Operating System Software
IOS (tm) C2950 Software (C2950-I6Q4L2-M), Version 12.1(22)EA4, RELEASE SOFTWARE(fc1)
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Wed 18-May-05 22:31 by jharirba

advertisement version: 2
Duplex: full

Device ID: Bogota

Entry address(es):
IP address : 192.168.1.130
Platform: cisco C1900, Capabilities: Router
Interface: Serial0/0/1, Port ID (outgoing port): Serial0/0/1
Holdtime: 144

Version :
Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version 15.1(4)M4, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Thurs 5-Jan-12 15:41 by pt_team
advertisement version: 2
Duplex: full

Cali#

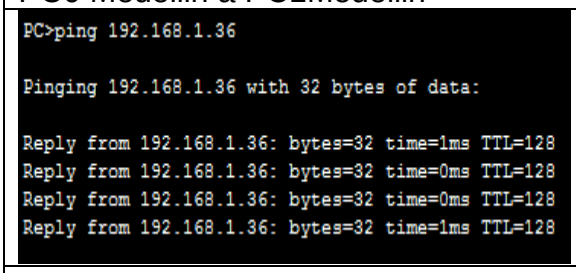
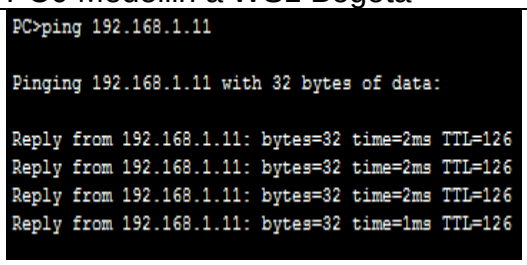
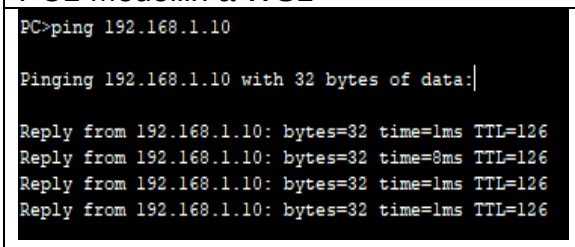
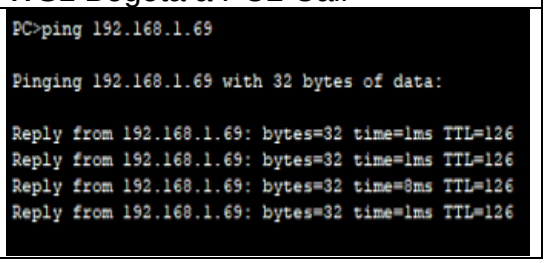
Configuración IP Route

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#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
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#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Cali(config)#ip route 192.168.1.0 255.255.255.224 192.168.1.130
Cali(config)#ip route 192.168.1.96 255.255.255.224 192.168.1.130
Cali(config)#ip route 192.168.1.96 255.255.255.224 192.168.1.130
Cali(config)#

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

PC0 Medellin a PC1Medellin	PC0 Medellin a WS1 Bogota
	
PC1 Medellin a WS1	**WS1 Bogota a PC2 Cali**
	

Parte 3: Configuración de Enrutamiento.

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

Configuración 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)#no auto
Medellin(config-router)#no auto-summary
Medellin(config-router)#
```

Configuración enrutamiento Bogota

```
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)#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)#
```

Configuración enrutamiento 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)#network 192.168.1.64 0.0.0.31
Cali(config-router)#no auto
Cali(config-router)#no auto-summary
Cali(config-router)#
```

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

```
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 Se0/0/0 14 00:37:38 40 1000 0 8

Medellin#
```

```
Bogota#show ip eigrp neighbors
IP-EIGRP neighbors for process 200
H Address Interface Hold Uptime SRTT RTO Q Seq
(sec) (ms) Cnt Num
0 192.168.1.99 Se0/0/0 13 00:39:08 40 1000 0 11

Bogota#
```

Cali#show ip eigrp neighbors
IP-EIGRP neighbors for process 200

Cali#

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

Con el comando **show ip interface brief**, verificamos las tablas de enrutamiento

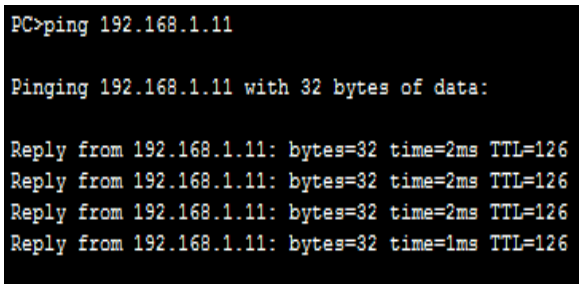
Medellin#show ip interface brief
Interface IP-Address OK? Method Status Protocol
GigabitEthernet0/0 192.168.1.33 YES manual up up
GigabitEthernet0/1 unassigned YES unset administratively down down
Serial0/0/0 192.168.1.99 YES manual up up
Serial0/0/1 192.168.1.131 YES manual down down
Vlan1 unassigned YES unset administratively down down
Medellin#

Bogota#show ip interface brief
Interface IP-Address OK? Method Status Protocol
GigabitEthernet0/0 192.168.1.1 YES manual up up
GigabitEthernet0/1 unassigned YES unset administratively down down
Serial0/0/0 192.168.1.98 YES manual up up
Serial0/0/1 192.168.1.130 YES manual up up
Vlan1 unassigned YES unset administratively down down
Bogota#

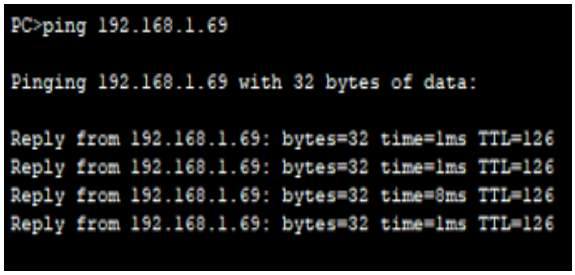
Cali#sho ip interface brief
Interface IP-Address OK? Method Status Protocol
GigabitEthernet0/0 192.168.1.65 YES manual up up
GigabitEthernet0/1 unassigned YES unset administratively down down
Serial0/0/0 192.168.1.131 YES manual down down
Serial0/0/1 192.168.1.193 YES manual up up
Vlan1 unassigned YES unset administratively down down
Cali#

a. 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.

PC0 Medellin a Servidor Bogota



WS1 Bogota a PC2 Cali



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.

Con el comando "**line vty"** se habilita el telnet y el "0 " simplemente deja una sola línea o sesión al enrutador. Si necesita más sesiones simultáneamente, debe escribir "line vty 0 4"

Medellin(config)#line vty 0
Medellin(config-line)#exec-timeout 40
Medellin(config-line)#

Bogota(config)#line vty 0
Bogota(config-line)#exec-timeout 40
Bogota(config-line)#

Cali(config)#line vty 0
Cali(config-line)#exec-timeout 40
Cali(config-line)#

Prueba funcionando desde el Reuter de Medellin a Bogota con el comando telnet

Medellin#telnet 192.168.1.1
Trying 192.168.1.1 ...OpenEsta prohibido el acceso no autorizado

User Access Verification

Password:
Bogota>enable
Password:
Password:
Bogota#

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.

Denegar el acceso de WS1 a cualquier dispositivo de la red

Bogota#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Bogota(config)#access
Bogota(config)#access-list 1 deny 192.168.1.11 0.0.0.31
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)#interface serial 0/0/1
Bogota(config-if)#ip access-group 1 out
Bogota(config-if)#

Ping WS1 a PC3 Cali

```
PC>ping 192.168.1.69

Pinging 192.168.1.69 with 32 bytes of data:

Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.

Ping statistics for 192.168.1.69:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Permitir que el servidor tenga acceso a cualquier dispositivo de la red

Bogota#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Bogota(config)#access-list 2 permit 192.168.1.10 0.0.0.31
Bogota(config)#access-list 2 permit any
Bogota(config)#interface g
Bogota(config)#interface gigabitEthernet 0/0
Bogota(config-if)#ip access
Bogota(config-if)#ip access-group 2 in
Bogota(config-if)#

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.

```
Cali(config)#access
Cali(config)#access-list 102 deny ip 192.168.1.64 0.0.0.31 192.168.1.128 0.0.0.31
Cali(config)#interface g
Cali(config)#interface gigabitEthernet 0/0
Cali(config-if)#ip access-group 102 in
Cali(config-if)#
```

Ping de PC2 Cali a WS1 de Bogota

```
PC>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.65: Destination host unreachable.
Reply from 192.168.1.65: Destination host unreachable.
Reply from 192.168.1.65: Destination host unreachable.
Reply from 192.168.1.65: Destination host unreachable.

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Parte 5: Comprobación de la red instalada.

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

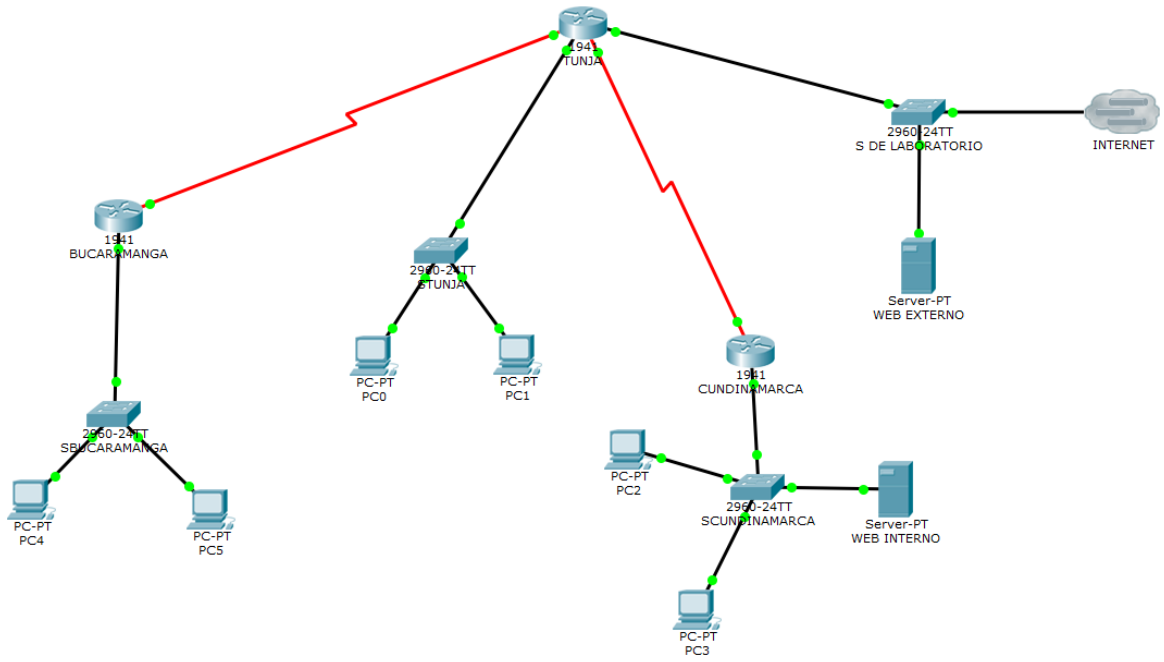
Las listas de acceso realizadas anteriormente fueron exitosas ya que al realizar ping entre los hosts de los router los pings eran fallidos

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	unreachable
	Servidor	Router MEDELLIN	unreachable
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	Fallido
	LAN del Router MEDELLIN	WS_1	Fallido
	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

Escenario 2

Una empresa tiene la conexión a internet en una red Ethernet, lo cual deben adaptarlo para facilitar que sus routers y las redes que incluyen puedan, por esa vía, conectarse a internet, pero empleando las direcciones de la red LAN original.



Desarrollo

Los siguientes son los requerimientos necesarios:

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

Configuración básica.

Así mismo como se realizó en el escenario 1, para e escenario 2 la configuración básica de cada Router y Switch, presentes en la topología Ingresamos a cada uno de ellos en modo exec configurado con el comando **enable** y luego con el comando **configure terminal,** posteriormente a cada dispositivo asignamos el nombre con el comando **hostname**, desactivamos la búsqueda de DNS con el comando **no ip domain lookup,** creamos la contraseña cifrada con el comando **line vty,** encriptamos las contraseñas con el comando **service password-encryption** por ultimo a cada Router y Switch asignamos el mensaje que está prohibido el acceso no autorizado a cada dispositivo esto lo hacemos con el comando **banner motd** #Esta prohibido el acceso no autorizado# autorizado#

Configuración router TUNJA

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname TUNJA
TUNJA(config)#no ip domain-lookup
TUNJA(config)#enable secret AAA
TUNJA(config)#line con 0
TUNJA(config-line)#password cisco
TUNJA(config-line)#login
TUNJA(config-line)#line vty 0 4
TUNJA(config-line)#password cisco
TUNJA(config-line)#login
TUNJA(config-line)#exit
TUNJA(config)#service password-encryption
TUNJA(config)#banner motd #Esta prohibido el acceso no autorizado#
TUNJA(config)#interface g0/0
TUNJA(config-if)#ip address 172.3.2.9 255.255.255.248
TUNJA(config-if)#no shutdown

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

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

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

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname STUNJA
STUNJA(config)#no ip domain-lookup
STUNJA(config)#enable secret AAA
STUNJA(config)#line con 0
STUNJA(config-line)#password cisco
STUNJA(config-line)#line vty 0 4
STUNJA(config-line)#password cisco
STUNJA(config-line)#login
STUNJA(config-line)#exit
STUNJA(config)#service password-encryption
STUNJA(config)#banner motd #Esta prohibido el acceso no autorizado#
STUNJA(config)#interface vlan 1
STUNJA(config-if)#ip address 172.3.2.10 255.255.255.248
STUNJA(config-if)#no shutdown
TUNJA(config)#interface s0/0/1
TUNJA(config-if)#ip address 172.31.2.33 255.255.255.252
TUNJA(config-if)#no shutdown
TUNJA(config-if)#interface s0/0/0
TUNJA(config-if)#ip address 172.31.2.37 255.255.255.252
TUNJA(config-if)#no shutdown
TUNJA(config)#interface g0/1
TUNJA(config-if)#ip address 209.17.220.2 255.255.255.0
TUNJA(config-if)#no shutdown
STUNJA(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

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

STUNJA#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
STUNJA#
STUNJA(config-if)#interface vlan 20
STUNJA(config-if)#ip address 172.31.0.130 255.255.255.192
STUNJA(config-if)#no shutdown
STUNJA(config-if)#interface vlan 30
STUNJA(config-if)#ip address 172.31.0.193 255.255.255.192
STUNJA(config-if)#no shutdown
```

Configuración router CUNDINAMARCA

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname CUNDINAMARCA
CUNDINAMARCA(config)#enable secret AAA
CUNDINAMARCA(config)#line con 0
CUNDINAMARCA(config-line)#password cisco
CUNDINAMARCA(config-line)#login
CUNDINAMARCA(config-line)#line vty 0 4
CUNDINAMARCA(config-line)#password cisco
CUNDINAMARCA(config-line)#login
CUNDINAMARCA(config-line)#exit
CUNDINAMARCA(config)#no ip domain-lookup
CUNDINAMARCA(config)#service password-encryption
CUNDINAMARCA(config)#banner motd #Esta prohibido el acceso no autorizado#
CUNDINAMARCA(config)#exit
CUNDINAMARCA#
%SYS-5-CONFIG_I: Configured from console by console

CUNDINAMARCA#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
CUNDINAMARCA#
CUNDINAMARCA(config)#interface g0/0
CUNDINAMARCA(config-if)#ip address 172.31.2.9 255.255.255.248
CUNDINAMARCA(config-if)#no shutdown
CUNDINAMARCA(config)#interface s0/0/0
CUNDINAMARCA(config-if)#ip address 172.31.2.38 255.255.255.252
CUNDINAMARCA(config-if)#no shutdown


Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SCUNDINAMARCA
SCUNDINAMARCA(config)#no ip domain-lookup
SCUNDINAMARCA(config)#enable secret AAA
SCUNDINAMARCA(config)#line con 0
SCUNDINAMARCA(config-line)#password cisco
SCUNDINAMARCA(config-line)#login
SCUNDINAMARCA(config-line)#line vty 0 4
```

SCUNDINAMARCA(config-line)#password cisco
SCUNDINAMARCA(config-line)#login
SCUNDINAMARCA(config-line)#exit
SCUNDINAMARCA(config)#service password-encryption
SCUNDINAMARCA(config)#banner motd #Esta prohibido el acceso no autorizado#
SCUNDINAMARCA(config)#interface vlan 1
SCUNDINAMARCA(config-if)#ip address 172.31.2.10 255.255.255.248
SCUNDINAMARCA(config-if)#no shutdown
SCUNDINAMARCA#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]

SCUNDINAMARCA(config)#interface vlan 20
SCUNDINAMARCA(config-if)#ip address 172.31.1.65 255.255.255.192
SCUNDINAMARCA(config-if)#no shutdown
SCUNDINAMARCA(config-if)#interface vlan 30
SCUNDINAMARCA(config-if)#ip address 172.31.1.1 255.255.255.192
SCUNDINAMARCA(config-if)#no shutdown
SCUNDINAMARCA(config-if)#interface vlan 88
SCUNDINAMARCA(config-if)#ip address 172.31.2.1 255.255.255.192
SCUNDINAMARCA(config-if)#no shutdown

Configuración router BUCARAMANGA

Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname BUCARAMANGA
BUCARAMANGA(config)#enable secret AAA
BUCARAMANGA(config)#line con 0
BUCARAMANGA(config-line)#password cisco
BUCARAMANGA(config-line)#line vty 0 4
BUCARAMANGA(config-line)#password cisco
BUCARAMANGA(config-line)#login
BUCARAMANGA(config-line)#exit
BUCARAMANGA(config)#no ip domain-lookup
BUCARAMANGA(config)#service password-encryption
BUCARAMANGA(config)#banner motd #Esta prohibido el acceso no autorizado#
BUCARAMANGA(config)#exit

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

BUCARAMANGA#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
BUCARAMANGA#
BUCARAMANGA(config)#interface g0/0
BUCARAMANGA(config-if)#ip address 172.31.2.1 255.255.255.248
BUCARAMANGA(config-if)#no shutdown
BUCARAMANGA(config)#interface s0/0/1
BUCARAMANGA(config-if)#ip address 172.31.2.34 255.255.255.252
BUCARAMANGA(config-if)#no shutdown
BUCARAMANGA(config)#interface Serial0/0/0
BUCARAMANGA(config-if)#clock rate 128000
BUCARAMANGA(config)#interface Serial0/0/1
BUCARAMANGA(config-if)#clock rate 128000

Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SBUCARAMANGA
SBUCARAMANGA(config)#no ip domain-lookup
SBUCARAMANGA(config)#enable secret AAA
SBUCARAMANGA(config)#line con 0
SBUCARAMANGA(config-line)#password cisco
SBUCARAMANGA(config-line)#login
SBUCARAMANGA(config-line)#line vty 0 4
SBUCARAMANGA(config-line)#password cisco
SBUCARAMANGA(config-line)#login
SBUCARAMANGA(config-line)#exit
SBUCARAMANGA(config)#service password-encryption
SBUCARAMANGA(config)#banner motd #Esta prohibido el acceso no autorizado#
SBUCARAMANGA(config)#interface vlan 1
SBUCARAMANGA(config-if)#ip address 172.31.2.2 255.255.255.248
SBUCARAMANGA(config-if)#no shutdown
SBUCARAMANGA(config-if)#interface vlan 10
SBUCARAMANGA(config-if)#ip address 172.31.0.1 255.255.255.192
SBUCARAMANGA(config-if)#no shutdown
SBUCARAMANGA(config-if)#interface vlan 30
SBUCARAMANGA(config-if)#ip address 172.31.0.68 255.255.255.192
SBUCARAMANGA(config-if)#no shutdown
SBUCARAMANGA(config-if)#
```

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

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

SBUCARAMANGA(config-if)#exit
SBUCARAMANGA(config)#exit
SBUCARAMANGA#
%SYS-5-CONFIG_I: Configured from console by console

SBUCARAMANGA#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
SBUCARAMANGA#

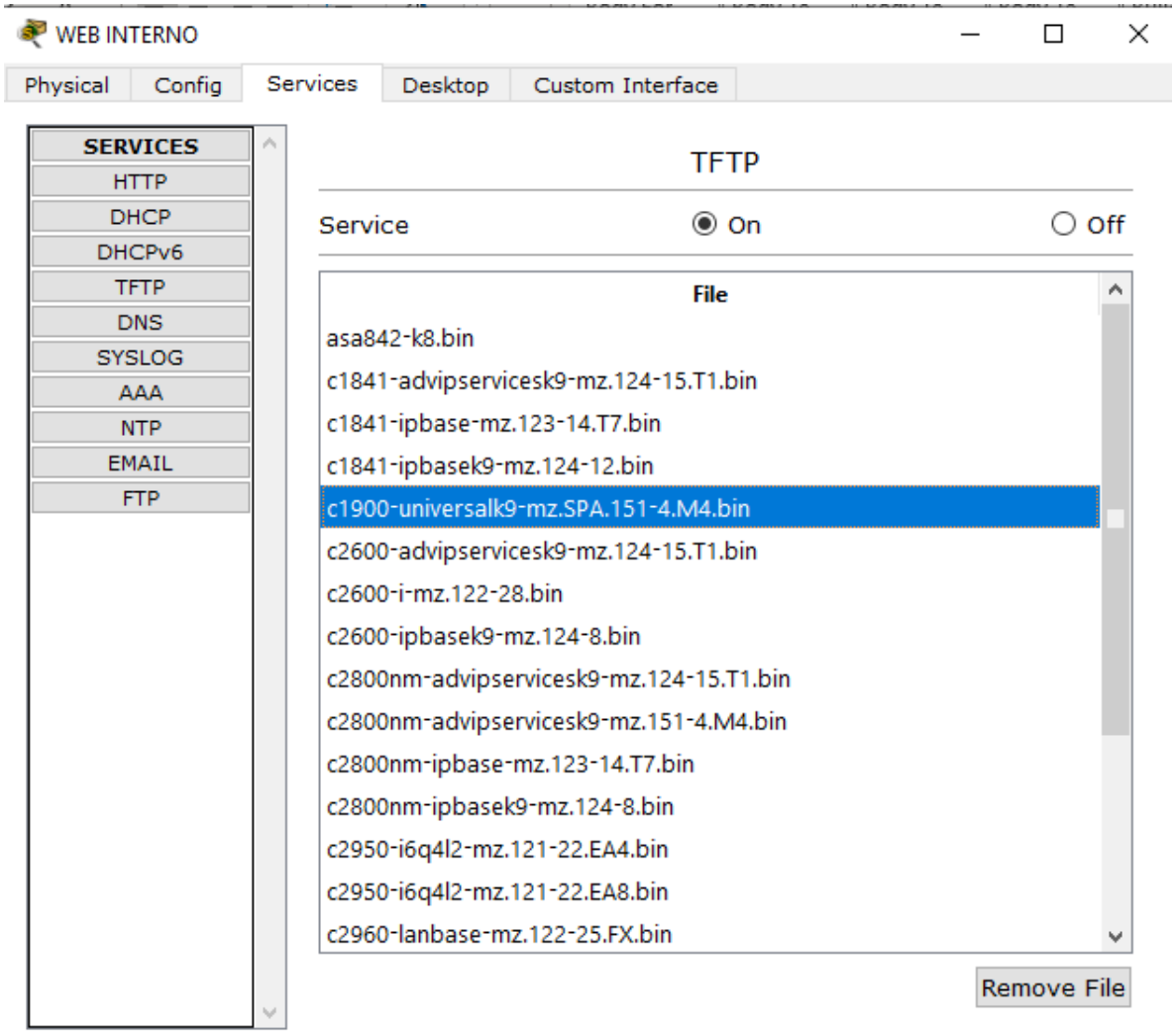
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S DE LABORATORIO
^
% Invalid input detected at '^' marker.
Switch(config)#hostname SDELABORATORIO
SDELABORATORIO(config)#no ip domain-lookup
SDELABORATORIO(config)#enable secret AAA
SDELABORATORIO(config)#line con 0
SDELABORATORIO(config-line)#password cisco
SDELABORATORIO(config-line)#login
SDELABORATORIO(config-line)#line vty 0 4
SDELABORATORIO(config-line)#password cisco
SDELABORATORIO(config-line)#login
SDELABORATORIO(config-line)#exit
SDELABORATORIO(config)#service password-encryption
SDELABORATORIO(config)#banner motd #Esta prohibido el acceso no autorizado#
SDELABORATORIO(config)#interface vlan 1
SDELABORATORIO(config-if)#ip address 209.17.220.3 255.255.255.0
SDELABORATORIO(config-if)#no shutdown
SDELABORATORIO#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]

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

La copia de respaldo del IOS se puede hacer desde el modo privilegiado, mediante el comando copy flash tftp.

router# **copy flash tftp**

En este caso se crea para nuestro servidor WEB INTERNO y se crea desde cada router



BUCARAMANGA#copy flash: tftp:
Source filename []? c1900-universalk9-mz.SPA.151-4.M4.bin
Address or name of remote host []? 172.31.2.11
Destination filename [c1900-universalk9-mz.SPA.151-4.M4.bin]?

Writing c1900-universalk9-mz.SPA.151-
4.M4.bin...!!
!!!
!!!
!!!
!!!
!!!!!!!!!!!!!!!!
[OK - 33591768 bytes]

33591768 bytes copied in 3.908 secs (902506 bytes/sec)
BUCARAMANGA#

CUNDINAMARCA#dir flash
Directory of flash0:/

3 -rw- 33591768 <no date> c1900-universalk9-mz.SPA.151-4.M4.bin
2 -rw- 28282 <no date> sigdef-category.xml
1 -rw- 227537 <no date> sigdef-default.xml

255744000 bytes total (221896413 bytes free)
CUNDINAMARCA#copy fl
CUNDINAMARCA#copy flash:
CUNDINAMARCA#copy flash: tf
CUNDINAMARCA#copy flash: tftp:
Source filename []? c1900-universalk9-mz.SPA.151-4.M4.bin
Address or name of remote host []? 172.31.2.11
Destination filename [c1900-universalk9-mz.SPA.151-4.M4.bin]?

Writing c1900-universalk9-mz.SPA.151-
4.M4.bin....!!!
!!!
!!!
!!!
!!!
!!!!!!!!!!!!!!!!!
[OK - 33591768 bytes]

33591768 bytes copied in 3.799 secs (928401 bytes/sec)
CUNDINAMARCA#

TUNJA#copy flash: tftp:
Source filename []? c1900-universalk9-mz.SPA.151-4.M4.bin
Address or name of remote host []? 172.31.2.11
Destination filename [c1900-universalk9-mz.SPA.151-4.M4.bin]?

Writing c1900-universalk9-mz.SPA.151-
4.M4.bin...!!
!!!
!!!
!!!
!!!
!!!!!!!!!!!!!!!!!!
[OK - 33591768 bytes]

33591768 bytes copied in 2.673 secs (1319490 bytes/sec)
TUNJA#

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

DHCP permite que un equipo se configura de forma automática, eliminando la necesidad de la intervención de un administrador de red, es decir la IP de configuración del equipo se realiza de forma automática

DHCP Bucaramanga
BUCARAMANGA(config)#ip dhcp pool vlan1
BUCARAMANGA(dhcp-config)#network 172.31.2.0 255.255.255.248
BUCARAMANGA(dhcp-config)#dns-server 0.0.0.0
BUCARAMANGA(dhcp-config)#default-router 172.31.2.1

BUCARAMANGA(config)#ip dhcp pool vlan10
BUCARAMANGA(dhcp-config)#network 172.31.0.0 255.255.255.192
BUCARAMANGA(dhcp-config)#dns-server 0.0.0.0
BUCARAMANGA(dhcp-config)#default-router 172.31.2.1

BUCARAMANGA(config)#ip dhcp pool vlan30
BUCARAMANGA(dhcp-config)#network 172.31.0.0 255.255.255.192
BUCARAMANGA(dhcp-config)#dns-server 0.0.0.0
BUCARAMANGA(dhcp-config)#default-router 172.31.2.1

DHCP Cundinamarca

```
CUNDINAMARCA(config)#ip dhcp pool vlan1
CUNDINAMARCA(dhcp-config)#network 172.31.2.8 255.255.255.248
CUNDINAMARCA(dhcp-config)#dns-server 0.0.0.0
CUNDINAMARCA(dhcp-config)#default-router 172.31.2.9
CUNDINAMARCA(dhcp-config)#ip dhcp pool vlan20
CUNDINAMARCA(dhcp-config)#network 172.31.1.64 255.255.255.192
CUNDINAMARCA(dhcp-config)#dns-server 0.0.0.0
CUNDINAMARCA(dhcp-config)#default-router 172.31.2.9
CUNDINAMARCA(dhcp-config)#ip dhcp pool vlan30
CUNDINAMARCA(dhcp-config)#network 172.31.1.0 255.255.255.192
CUNDINAMARCA(dhcp-config)#dns-server 0.0.0.0
CUNDINAMARCA(dhcp-config)#default-router 172.31.2.9
CUNDINAMARCA(dhcp-config)#ip dhcp pool vlan88
CUNDINAMARCA(dhcp-config)#network 172.31.2.24 255.255.255.248
CUNDINAMARCA(dhcp-config)#dns-server 0.0.0.0
CUNDINAMARCA(dhcp-config)#default-router 172.31.2.9
```

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

```
CUNDINAMARCA(config)#router rip
CUNDINAMARCA(config-router)#network 172.31.0.0
CUNDINAMARCA(config-router)#
```

4. Listas de control de acceso:

Para configurar las listas de control utilizaremos los comandos access-list (100) con el número de lista, con el comando **deny** (denegar), se niega el acceso, o con el comando **permit** (permitir) dependiendo el caso, esto seguido de la ip y de la máscara para que surja el efecto deseado

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

```
CUNDINAMARCA(config)#access-list
CUNDINAMARCA(config)#access-list 102 deny tcp 172.31.1.64 0.0.0.63
host 209.17.220.6 eq 80
CUNDINAMARCA(config)#access
CUNDINAMARCA(config)#access-list 102 permit ip any any
CUNDINAMARCA(config)#interface
CUNDINAMARCA(config)#interface gi
CUNDINAMARCA(config)#interface gigabit Ethernet 0/0
CUNDINAMARCA(config-if)#ip access
CUNDINAMARCA(config-if)#ip access-group 102 in
```

CUNDINAMARCA(config-if)#

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

  En el Switch de Cundinamarca no existe la VLAN 10

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

```
TUNJA(config)#access
TUNJA(config)#access-list 101 permit tcp 172.31.0.192 0.0.0.63 host
209.17.220.3 eq 80
TUNJA(config)#access-list 102 permit tcp 172.31.0.192 0.0.0.63 host
209.17.220.3 eq  21
TUNJA(config)#access-list 101 deny ip any any
TUNJA(config)#access-list 102 deny ip any any
TUNJA(config)#interface gi
TUNJA(config)#interface gigabitEthernet 0/0
TUNJA(config-if)#ip acc
TUNJA(config-if)#ip access-group 101 in
TUNJA(config-if)#ip access-group 102 in
TUNJA(config-if)#
```

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

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

  BUCARAMANGA (config)#access
  BUCARAMANGA(config)#access-list 103 permit tcp 172.31.0.64 0.0.0.63 host 209.17.220.3
  BUCARAMANGA (config)#access
  BUCARAMANGA(config)#access-list 104 permit tcp 172.31.0.0 0.0.0.63 any

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

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

BUCARAMANGA(config)#access-list 101 deny ip 172.31.2.0 0.0.0.7 172.31.0.0 0.0.0.63

BUCARAMANGA(config-if)#interface G0/0
BUCARAMANGA(config-if)#ip access-group 102 in

BUCARAMANGA(config-if)#access-list 101 deny ip 172.31.2.0 0.0.0.7 172.31.0.64 0.0.0.63
BUCARAMANGA(config)#access-list 102 deny ip 172.31.2.0 0.0.0.7 172.31.0.64 0.0.0.63

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

Aspectos a tener en cuenta

Habilitar VLAN en cada switch y permitir su enrutamiento.

Con el comando vlan y el numero de la vlan lo que hacemos es habilitar la vlan y cambiar el estado de la vlan de down a up

VLAN SBUCARAMANGA

SBUCARAMANGA (config)#vlan 10
SBUCARAMANGA (config-vlan)#
%LINK-5-CHANGED: Interface Vlan10, changed state to up
SBUCARAMANGA (config)#vlan 30
SBUCARAMANGA (config-vlan)#
%LINK-5-CHANGED: Interface Vlan30, changed state to up

VLAN STUNJA

STUNJA(config)#vlan 20
STUNJA(config-vlan)#
%LINK-5-CHANGED: Interface Vlan20, changed state to up
STUNJA(config-vlan)#vlan 30
STUNJA(config-vlan)#
%LINK-5-CHANGED: Interface Vlan30, changed state to up

VLAN SCUNDINAMARCA

SCUNDINAMARCA(config-if)#vlan 20
SCUNDINAMARCA(config-vlan)#
%LINK-5-CHANGED: Interface Vlan20, changed state to up

SCUNDINAMARCA(config-vlan)#vlan 30
SCUNDINAMARCA(config-vlan)#
%LINK-5-CHANGED: Interface Vlan30, changed state to up

SCUNDINAMARCA(config-vlan)#vlan 88
SCUNDINAMARCA(config-vlan)#
%LINK-5-CHANGED: Interface Vlan88, changed state to up

Enrutamiento OSPF con autenticación en cada router.

Los procesos de enrutamiento buscan la mejor ruta para enviar paquetes entre las redes

Enrutamiento OSPF BUCARAMANGA

BUCARAMANGA (config)#router ospf 1
BUCARAMANGA (config-router) #network 172.31.2.32 0.0.0.3 area 0
BUCARAMANGA (config-router) #network 172.31.2.0 0.0.0.7 area 0
BUCARAMANGA (config-router) #network 172.31.0.0 0.0.0.63 area 0
BUCARAMANGA (config-router) #network 172.31.0.64 0.0.0.63 area 0

BUCARAMANGA#show run
router ospf 1
log-adjacency-changes
network 172.31.2.32 0.0.0.3 area 0
network 172.31.2.0 0.0.0.7 area 0
network 172.31.0.0 0.0.0.63 area 0
network 172.31.0.64 0.0.0.63 area 0

Enrutamiento OSPF TUNJA

TUNJA (config)#router ospf 1
TUNJA(config-router) #network 172.31.2.32 0.0.0.3 area 0
TUNJA(config-router)#
01:48:16: %OSPF-5-ADJCHG: Process 1, Nbr 172.31.2.34 on Serial0/0/1 from LOADING to FULL, Loading Done

TUNJA(config-router)#network 172.31.2.36 0.0.0.3 area 0
TUNJA(config-router)#network 209.17.220.0 0.0.0.255 area 0
TUNJA(config-router)#network 172.3.2.8 0.0.0.7 area 0
TUNJA(config-router)#network 172.31.0.128 0.0.0.63 area 0

TUNJA (config-router) #network 172.31.0.192 0.0.0.63 area 0

TUNJA#show run

router ospf 1
log-adjacency-changes
network 172.31.2.32 0.0.0.3 area 0
network 172.31.2.36 0.0.0.3 area 0
network 209.17.220.0 0.0.0.255 area 0
network 172.3.2.8 0.0.0.7 area 0
network 172.31.0.128 0.0.0.63 area 0
network 172.31.0.192 0.0.0.63 area 0

Enrutamiento OSPF CUNDINAMARCA

CUNDINAMARCA(config)#router ospf 1
CUNDINAMARCA(config-router)#network 172.31.2.36 0.0.0.3 area 0
CUNDINAMARCA(config-router)#
01:59:33: %OSPF-5-ADJCHG: Process 1, Nbr 209.17.220.2 on Serial0/0/0 from LOADING to FULL, Loading Done

CUNDINAMARCA(config-router)#network 172.31.2.8 0.0.0.7 area 0
CUNDINAMARCA(config-router)#network 172.31.1.64 0.0.0.63 area 0
CUNDINAMARCA(config-router)#network 172.31.1.0 0.0.0.63 area 0
CUNDINAMARCA(config-router)#network 172.31.2.24 0.0.0.7 area 0

CUNDINAMARCA #show run

router ospf 1
log-adjacency-changes
network 172.31.2.36 0.0.0.3 area 0
network 172.31.2.8 0.0.0.7 area 0
network 172.31.1.64 0.0.0.63 area 0
network 172.31.1.0 0.0.0.63 area 0
network 172.31.2.24 0.0.0.7 area 0

- Servicio DHCP en el router Tunja, mediante el helper address, para los routers Bucaramanga y Cundinamarca.

```
CUNDINAMARCA(config)#router rip
CUNDINAMARCA(config-router)#network 172.31.0.0
CUNDINAMARCA(config-router)#
```

- Establecer una lista de control de acceso de acuerdo con los criterios señalados.
- Habilitar las opciones en puerto consola y terminal virtual

Conclusiones

Durante el desarrollo de las pruebas de habilidades en la plataforma de cisco, se abordó ambientes de simulación Packet Tracer donde se realizó configuraciones e implementaciones en dos topologías de redes.

Utilizando el ambiente virtual para la resolución de las practicas, se identificaron los componentes que integran una red así como los posibles errores o inconvenientes durante el diseño e interconexión de los componentes en un ambiente controlado, de esta forma poder evidenciar claramente aquellos factores con los que nos podemos encontrar en nuestro desarrollo profesional

Los dos escenarios propuestos para desarrollar el trabajo y diseñar las topologías pertinentes, las cuales se realizaron utilizando la herramienta de Packet Tracer me permitió adquirir el conocimiento suficiente para detectar, administrar y mantener el buen funcionamiento de los dispositivos que conforma una red LAN y WAN, adicionalmente se expandió el conocimiento sobre conceptos de vital importancia para un administrador de red como son las listas de control de acceso, DHCP y la configuración del NAT.

Como conclusión en el aspecto personal me deja un gran aporte para mi perfil profesional como ingeniero en sistemas ya que al desarrollar cada uno de los puntos presentes en la prueba de habilidades, incremento enormemente acerca de las topologías de red, su funcionamiento, configuración e importancia a la hora de implementar una red en una empresa, estos conocimientos para mi eran desconocidos y gracias a la UNAD con este tipo de laboratorios realizados me preparan para asumir roles en administración y configuración de redes

CISCO. (2014). *Acceso a la red. Fundamentos de Networking*. Obtenido de https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#4.0.1.1

CISCO. (2014). *Capa de red. Fundamentos de Networking*. Obtenido de https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#5.0.1.1

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

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

CISCO. (2014). *Protocolos y comunicaciones de red. Fundamentos de Networking*. Obtenido de https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#3.0.1.1

Vesga, J. (2014). *Diseño y configuración de redes con Packet Tracer [OVA]*. Obtenido de https://1drv.ms/u/s!AmIJYei-NT1IhgCT9VCtl_pLtPD9

Vesga, J. (2019). *Introducción al Laboratorio Remoto SmartLab [OVI]*. Obtenido de http://hdl.handle.net/10596/24167

Canosa Ferreiro Alejandro. (2017). Reforzando la seguridad en los router cisco. Obtenido de https://backtrackacademy.com/articulo/reforzando-la-seguridad-en-los-router-cisco

Cisco. (2015). Problemas comunes del EIGRP del Troubleshooting. Obtenido de https://www.cisco.com/c/es_mx/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/118974-technote-eigrp-00.html

Jramon208. (s.f) Configurar telnet en router Cisco. Obtenido de https://sites.google.com/site/jramon208/inicio/redes/ejerciciospackettracer/configurar-telnet-en-router-cisco

Cisco. (2007). Configuración de listas de acceso IP. Obtenido de https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/23602-confaccesslists.html.

Vesga, J. (2019). *Introducción al Laboratorio Remoto SmartLab [OVI]*. Obtenido de http://hdl.handle.net/10596/24167

Vesga, J. (2014). *Diseño y configuración de redes con Packet Tracer [OVA]*. Obtenido de https://1drv.ms/u/s!AmIJYei-NT1IhgCT9VCtl_pLtPD9

Redes locales y globales. Copias de respaldo de una imagen del IOS. Obtenido de https://sites.google.com/site/redeslocalesyglobales/4-configuracion-de-red/2-configuracion-de-routers/8-tareas-de-administracion-en-los-routers-cisco/1-copias-de-respaldo-de-una-imagen-del-ios

Rivas Andres. (2019). Normas ICONTEC para trabajos escritos. Obtenido de https://www.colconectada.com/normas-icontec/