PRUEBA DE HABILIDADES PRÁCTICAS CCNA

YULVER ALEXANDER ARIAS GONZALEZ

Director, Juan Carlos Vesga

Universidad Nacional abierta y a distancia

Ingeniería de sistemas

Febrero 2019

RESUMEN

Mediante el presente trabajo, se busca mostrar los conocimientos acerca de redes adquiridos durante el curso, esto se hará realizando dos configuraciones de red, las cuales incluirán protocolos de diferentes capas del modelo OSI, tambíen se plasmarán en este documento los diferentes resultados obtenidos, y las pruebas de conectividad respectivas.

DEDICATORIA

Este trabajo final se la dedico a mi familia y a Dios quien me guio por el camino del bien, por sus grandes principios y cualidades para lograr el éxito en mi carrera, de igual manera a mi hija ya que fue mi mayor motor para conseguir mis metas y objetivos.

AGRADECIMIENTOS

Agradezco a la universidad por brindarme la posibilidad de estudiar a distancia, a tutores que me guiaron y me enseñaron el conocimiento de cada materia, a mis compañeros de estudio y a mi familia.

FUENTES DE FINANCIACIÓN

Se tomaron como guía para la resolución de este trabajo varias fuentes de información, tales como los módulos de CISCO CCNA, el libro de redes de computadoras de Tanenbaum y los conocimientos adquiridos durante el curso.

Glosario

CCNA Cisco Certified Network Associate. 3

NAT Network Address Translation. 3

OSPF Open Shortest Path First. 3

RIP Routing Information Protocol. 3

TABLA DE CONTENIDO

Pag.

ÍNDICE DE FIGURAS

FIGURA Pag.

1. INTRODUCCIÓN

La empresa de redes de telecomunicaciones CISCO, realiza diversos cursos de capacitación, para enseñar a diferentes personas alrededor del mundo, los protocolos y diferentes tópicos acerca de conexión y cinfiguración de dispositivos de red. Posteriormente realiza una evaluación al final de cada curso tomado para verificar si los conocimientos fueron realmente asimilados por la persona que lo tomó.

En este caso puntual se presentaron dos escenarios, cuyas configaciones y conexiones fueron hechas en el programa packet tracer, resolviendo así, las problemáticas planteadas, posteriormente en el presente informe se mostrará la metodología usada.

Para el escenario 1 se planteó una red con cuatro router, tres de ellos proporcionan enlaces redundantes para simular un enrutamiento entre dos redes locales, y el cuarto router simula una conexión con el ISP. La misión es la de configurar los diferentes requerimientos de enrutamiento y conmutación, para permitir una conexión global entre los dispositivos presentes en la topología. Donde se pretende una conexión *DualStack* con la LAN conectada al la interfaz fastEthernet conectada al Router 3. Mostrando así una conexión con el servidor ipv6 e ipv4. Por otra parte, se requiere reforzar los conocimientos en redes locales virtuales Vlan, cuyas utilidades son múltiples, dentro de las cuales están un aislamiento de dominios de difusión.

Para el escenario 2 se requiere simular una conexión entre sucursales remotas a través de enlaces seriales, internet, donde se pretende realizar un aprendizaje acerca de cómo incluir interfaces loopback, enlaces troncales, subinterfaces con router on a stick y el protocolo de enrutamiento OSPF. Por otra parte se necesita implementar el acceso remoto a dispositivos de red, en este caso los switches. En este caso puntual se realizará con SSH, debido a la

inseguridad presente en el protocolo de acceso remoto Telnet, además de la implementación de listas de accesos estandar y extendidas.

1.1 Problema de investigación

Una vez definidas las dos problematicas a desarrollar se procederá a definir los objetivos al realizar éste trabajo:

- Se requiere conocer los diferentes protocolos de red presentes en las diferentes capas del modelo OSI, así como la interconexión de dispositivos de red y dispositivos terminales.

1.2 Objetivo General

- Realizar las configuraciones necesarias para las topologías de red propuestas.

1.3 Objetivos Específicos

- Realizar la configuración de los protocolos de enrutamiento OSPF y RIP
- Implementar NAT
- Crear y aplicar ACL
- Realizar enrutamiento de vlan mediante subinterfaces router on a stick
- Crear y aplicar pool DHCP
- Reconocer el direccionamiento ipv6

2. REVISIÓN

Para la realización de este trabajo se realizaron diversas consultas en el curso de Cisco CCNA.[CISCO,]

2.1 Siglas

Las siglas mas importantes que se muestran en el trabajo son las presentadas a continuación: Cisco Certified Network Associate (CCNA), Open Shortest Path First (OSPF), Routing Information Protocol (RIP), Network Address Translation (NAT).

3. MARCO TEÓRICO

3.1 Capa de red

La capa de red tiene como función llevar los paquetes durante todo el trayecto, desde la fuente de origen a la de destino. Para llegar al destino probablemente sea requerido realizar muchos saltos en el camino mediante router intermediarios. Esta labor en efecto, contrasta ccon la de la capa de enlace de datos, cuyo único objetivo es transmitir tramas de un extremo del cable al otro. Así, la capa de red es la capa más baja que maneja la transmisión de extremo a extremo.[CISCO,]

Para conseguir sus metas, la capa de red debe conocer la topología de red (los diferentes dispositivos de red con sus respectivos enlaces) y elegir las rutas óptimas incluso para redes de mayor tamaño. También tiene que tener cuidado al realizar la elección de rutas para no sobrecargar las líneas de comunicación y los router y dejar inactivos a otros.[CISCO,]

3.2 OSPF

Open Shortest Path First (OSPF), Primer Camino Más Corto, es un protocolo de red para encaminamiento jerárquico de pasarela interior o Interior Gateway Protocol (IGP), que usa el algoritmo Dijkstra, para calcular la ruta más corta entre dos nodos.[CISCO,]

Su medida de métrica se denomina cost, y tiene en cuenta diversos parámetros tales como el ancho de banda y la congestión de los enlaces. OSPF construye además una base de datos enlace-estado (Link-State Database, LSDB) idéntica en todos los routers de la zona.[CISCO,]

OSPF puede operar con seguridad usando MD5 para autenticar sus puntos antes de realizar nuevas rutas y antes de aceptar avisos de enlace-estado.[CISCO,]

OSPF es probablemente el protocolo IGP más utilizado en redes grandes; IS-IS, otro protocolo de encaminamiento dinámico de enlace-estado, es más común en grandes proveedores de servicios. Como sucesor natural de RIP, acepta VLSM y CIDR desde su inicio. A

lo largo del tiempo, se han ido creando nuevas versiones, como OSPFv3 que soporta IPv6 o las extensiones multidifusión para OSPF (MOSPF), aunque no están demasiado extendidas. OSPF puede .etiquetarrutas y propagar esas etiquetas por otras rutas.[CISCO,]

Una red OSPF se puede descomponer en regiones (áreas) más pequeñas. Hay un área especial llamada área backbone que forma la parte central de la red a la que se encuentran conectadas el resto de áreas de la misma. Las rutas entre las diferentes áreas circulan siempre por el backbone, por lo tanto todas las áreas deben conectar con el backbone. Si no es posible hacer una conexión directa con el backbone, se puede hacer un enlace virtual entre redes.[CISCO,]

Los routers (también conocidos como encaminadores) en el mismo dominio de multidifusión o en el extremo de un enlace punto-a-punto forman enlaces cuando se descubren los unos a los otros. En un segmento de red Ethernet los routers eligen a un router designado (Designated Router, DR) y un router designado secundario o de copia (Backup Designated Router, BDR) que actúan como hubs para reducir el tráfico entre los diferentes routers. OSPF puede usar tanto multidifusiones (multicast) como unidifusiones (unicast) para enviar paquetes de bienvenida y actualizaciones de enlace-estado. Las direcciones de multidifusión usadas son 224.0.0.5 y 224.0.0.6. Al contrario que RIP o BGP, OSPF no usa ni TCP ni UDP, sino que se encapsula directamente sobre el protocolo IP poniendo "89.en el campo protocolo.[CISCO,]

3.3 RIP

El Protocolo de Información de Encaminamiento, Routing Information Protocol (RIP), es un protocolo de puerta de enlace interna o interior (Interior Gateway Protocol, IGP) utilizado por los routers o encaminadores para intercambiar información acerca de redes del Internet Protocol (IP) a las que se encuentran conectados. Su algoritmo de encaminamiento está basado en el vector de distancia, ya que calcula la métrica o ruta más corta posible hasta el destino a partir del número de "saltos.o equipos intermedios que los paquetes IP deben atravesar. El límite máximo de saltos en RIP es de 15, de forma que al llegar a 16 se

considera una ruta como inalcanzable o no deseable. A diferencia de otros protocolos, RIP es un protocolo libre, es decir, que puede ser usado por diferentes routers y no únicamente por un solo propietario con uno como es el caso de EIGRP que es de Cisco Systems.[CISCO,]

3.4 Vlan

Una VLAN, acrónimo de virtual LAN (red de área local virtual), es un método para crear redes lógicas independientes dentro de una misma red física. Varias VLAN pueden coexistir en un único conmutador físico o en una única red física. Son útiles para reducir el dominio de difusión y ayudan en la administración de la red, separando segmentos lógicos de una red de área local (los departamentos de una empresa, por ejemplo) que no deberían intercambiar datos usando la red local (aunque podrían hacerlo a través de un enrutador o un conmutador de capa OSI 3 y 4).[CISCO,]

3.5 NAT

La traducción de direcciones de red, también llamado enmascaramiento de IP o NAT (del inglés Network Address Translation), es un mecanismo utilizado por routers IP para intercambiar paquetes entre dos redes que asignan mutuamente direcciones incompatibles. Consiste en convertir, en tiempo real, las direcciones utilizadas en los paquetes transportados. También es necesario editar los paquetes para permitir la operación de protocolos que incluyen información de direcciones dentro de la conversación del protocolo.[CISCO,]

El tipo más simple de NAT proporciona una traducción una-a-una de las direcciones IP. La RFC 2663 se refiere a este tipo de NAT como NAT Básico, también se le conoce como NAT una-a-una. En este tipo de NAT únicamente las direcciones IP, las sumas de comprobación (Checksums) de la cabecera IP y las sumas de comprobación de nivel superior, que se incluyen en la dirección IP, necesitan ser cambiadas. El resto del paquete se puede quedar sin tocar (al menos para la funcionalidad básica del TCP/UDP, algunos protocolos de nivel superior pueden necesitar otra forma de traducción). Es corriente ocultar un espacio completo de direcciones IP, normalmente son direcciones IP privadas, detrás de una única dirección IP

(o pequeño grupo de direcciones IP) en otro espacio de direcciones (normalmente público). [CISCO,]

4. DESARROLLO/SOLUCIÓN

4.1 Escenario 1

Como primera medida se realizó la implementación física de la topología de red, realizando las conexiones entre sus dispositivos de red y los terminales, uniendo los periféricos con los enlaces planteados.

Posteriormente se realizaron las configuraciones para los diferentes dispositivos, teniendo en cuenta las especificaciones planteadas en el documento, como primera medida, para el router 1 (R1), se implementó la lista de acceso para permitir el acceso a través de NAT de la siguiente manera:

4.1.1 R1

R1 ACL

```
enable
configure terminal
hostname R1
ipv6 unicast-routing
ip access-list standard INSIDE-DEVS
permit 10.0.0.0 0.0.0.255
exit
ip nat inside source list INSIDE-DEVS interface Se0/0/0 overload
```

Una vez configurada la access list que será usada por el NAT con sobrecarga, tiene que habilitarse en las interfaces involucradas en el protocolo, tanto en las de entrada como en las de salida, así como la posterior configuración de las direcciones ip para las interfaces y su respectiva activación:

Interfaces R1

```
interface s0/0/0
no shutdown
ipv6 enable
ip nat outside
ip address 200.123.211.2 255.255.255.0
exit
interface s0/1/0
no shutdown
ipv6 enable
ip nat inside
ip address 10.0.0.1 255.255.255.252
exit
interface s0/1/1
no shutdown
ip nat inside
ipv6 enable
ip address 10.0.0.5 255.255.255.252
exit
```

Finalmente para el R1 se realizaron las configuraciones de los protocolos de enrutamiento, en este caso RIPv2 y la ruta por defecto redistribuida dentro de este:

RIP R1

```
router rip
version 2
network 10.0.0.0
network 200.123.211.0
redistribute static
exit
ip route 0.0.0.0 0.0.0.0 serial 0/0/0
```

4.1.2 R2

Una vez configurado el R1 se procedió a realizar la implementación de red para el R2, aunque a comparación con el router configurado previamente, este requiere protocolos diferentes como el DHCP, con las 30 direcciones excluidas tanto para la vlan 40 como para la 30, proceso que se muestra a continuación:

R2: DHCP

```
enable
configure terminal
hostname R2
ipv6 unicast-routing
ip dhcp pool LAPTOPS
default-router 192.168.20.1
network 192.168.20.0 255.255.255.0
dns-server 192.168.30.10
exit
ip dhcp pool DESKTOPS
default-router 192.168.21.1
network 192.168.21.0 255.255.255.0
dns-server 192.168.30.10
exit
ip dhcp excluded-address 192.168.20.1 192.168.20.10
ip dhcp excluded-address 192.168.21.1 192.168.21.10
```

Una vez definidos los pool de DHCP requeridos se procede a configurar las interfaces del router, y en el caso de este enrutador, las subinterfaces mediante router on a stick, esto es requerido debido a la necesidad de enrutar vlan en la topología de red planteada:

R2: Interfaces y subinterfaces

```
interface s0/0/0
no shutdown
ipv6 enable
ip address 10.0.0.2 255.255.255.252
exit
interface s0/0/1
no shutdown
ipv6 enable
ip address 10.0.0.9 255.255.255.252
exit
interface fastEthernet 0/0
no shutdown
exit
interface fastEthernet 0/0.100
no shutdown
ipv6 enable
encapsulation dot1Q 100
ip address 192.168.20.1 255.255.255.0
exit
interface fastEthernet 0/0.200
no shutdown
ipv6 enable
encapsulation dot1Q 200
ip address 192.168.21.1 255.255.255.0
exit
```

Finalmente para el enrutador 2 (R2) se realiza la misma función que para el 1 y es la de implementar RIP:

RIP R2

```
router rip
version 2
network 10.0.0.0
network 192.168.21.0
network 192.168.20.0
exit
```

4.1.3 R3

A diferencia de los dos enrutadores anteiores, para el R3 se requiere realizar la configuración del dual-stack, cuya funcionalidad es la de asignar direcciones tanto de ipv4 como de ipv6 a las diferentes interfaces, por este motivo se usó DHCPv6 sin estado para realizar esta labor, empezando por el pool de DHCPv6:

DHCP y DHCPv6 para el R3

```
enable
configure terminal
hostname R3
ipv6 unicast-routing
ipv6 dhcp pool server
dns-server 2001:DB8:130:0:9C0:80F:301:10
domain-name unad
exit
ip dhcp excluded-address 192.168.30.1 192.168.30.10
ip dhcp pool RED
default-router 192.168.30.1
network 192.168.30.0 255.255.255.0
dns-server 192.168.30.10
exit
```

Para las interfaces, en esta ocasión se añadió el comando ipv6 enable, que genera una ipv6 enrutable, además de su respectiva asociación con el pool de DHCPv6:

Interfaces R3

```
interface s0/0/0
no shutdown
ipv6 enable
ip address 10.0.0.6 255.255.255.252
exit
interface s0/0/1
no shutdown
ipv6 enable
ip address 10.0.0.10 255.255.255.252
exit
interface fastEthernet 0/0
no shutdown
ip address 192.168.30.1 255.255.255.0
ipv6 enable
ipv6 address 2001:db8:130::9c0:80f:301/64
ipv6 dhcp server server
exit
```

Y por ultimo para el R3 se configuró el RIP:

RIP R3

```
router rip
version 2
network 10.0.0.0
network 192.168.30.0
exit
```

4.1.4 ISP

Para el enrutador ISP se tiene:

Router ISP

```
enable
configure terminal
hostname ISP
ipv6 unicast-routing
interface s0/0/0
no shutdown
ipv6 enable
ip address 200.123.211.1 255.255.255.0
exit
router rip
version 2
network 200.123.211.0
exit
```

4.1.5 S2

Para el Switch 2 (S2) se configuraron como primera medida las Vlan requeridas, usando los nombres planteados, luego se configuraron los puertos de acceso y el puerto troncal para intercambiar la información con el enrutador, y finalmente se desactivaron los puertos que no se utilizarán:

S2

```
enable
configure terminal
hostname SW2
vlan 100
name LAPTOPS
exit
vlan 200
name DESKTOPS
exit
interface range fastEthernet 0/2-3
no shutdown
switchport mode access
switchport access vlan 100
exit
interface range fastEthernet 0/4-5
no shutdown
switchport mode access
switchport access vlan 200
exit
interface fastEthernet 0/1
switchport mode trunk
switchport trunk allowed vlan 1,100,200
switchport trunk native vlan 1
exit
interface range fastEthernet 0/6-24
shutdown
exit
```

4.2 Escenario 2

Para esta topología de res se tienen tres enrutadores, otro enrutador que simula internet cuya ubicación es en un cluster, difiere del escenario anterior en el protocolo de enrutamiento, en este caso es ospf.

4.2.1 R1

Para el R1 se usaron los siguientes pool de DHCP, con sus respectivas exclusiones de 30 direcciones dentro de las subredes, además de la asignación del dominio y el servidor dns:

DHCP R1

```
enable
configure terminal
hostname R1
ipv6 unicast-routing
ip dhcp excluded-address 192.168.30.1 192.168.30.30
ip dhcp excluded-address 192.168.40.1 192.168.40.30
ip domain-name ccna-unad.com
ip dhcp pool Administracion
default-router 192.168.30.1
network 192.168.30.0 255.255.255.0
dns-server 10.10.10.11
exit
ip dhcp pool mercadeo
default-router 192.168.40.1
network 192.168.40.0 255.255.255.0
dns-server 10.10.10.11
exit
```

A diferencia del escenario anterior, se requería el enrutamiento de las ip de acceso remoto, incluidas en la vlan 99, por lo tanto, para las interfaces cableadas se tiene:

R1 intefaces

```
interface gigabitEthernet  0/0
no shutdown
ipv6 enable
exit
interface gigabitEthernet  0/0.30
no shutdown
encapsulation dot1Q 30
ip address 192.168.30.1 255.255.255.0
ipv6 enable
exit
interface gigabitEthernet  0/0.40
no shutdown
encapsulation dot1Q 40
ip address 192.168.40.1 255.255.255.0
ipv6 enable
exit
interface gigabitEthernet  0/0.99
no shutdown
encapsulation dot1Q 99
ip address 192.168.99.1 255.255.255.0
ipv6 enable
exit
interface gigabitEthernet  0/0.200
no shutdown
encapsulation dot1Q 200
ip address 192.168.200.1 255.255.255.0
ipv6 enable
exit
```

Para el caso de la interfaz serial del enrutador, se realizó la configuración requerida de ancho de banda de funcionamiento, así como de la variación del costo del enlace:

Enlace serial con BW diferente

```
interface serial 0/0/0
no shutdown
bandwidth 256
ip ospf cost 9600
ip address 172.31.21.1 255.255.255.252
ipv6 enable
exit
```

Finalmente para este enrutador se realizó la configuración del protocolo de enrutamiento OSPFv2, que requiere de un router-id, y de las máscaras wildcard para definir las subredes a enrutar, además de configurar la operación de este dentro de un área específica. Por otra parte, por seguridad en las redes, es recomendable usar interfaces pasivas que generalmente van conectadas a LAN, para que no se envíen actualizaciones de este a dispositivos terminales, y que la infomación de los elementos de red, no pueda ser vista por cualquier persona que acceda a la esta, a continuación la implementación de este algoritmo de enrutamiento:

R1 OSPFv2

```
router ospf 100
router-id 1.1.1.1
passive-interface gigabitEthernet 0/0
network 192.168.30.0 0.0.0.255 area 0
network 192.168.40.0 0.0.0.255 area 0
network 192.168.99.0 0.0.0.255 area 0
network 192.168.200.0 0.0.0.255 area 0
network 172.31.21.1 0.0.0.3 area 0
exit
```

4.2.2 R2

Para el R2, se tiene como primera medida la definición de las listas de acceso, del hostname y el NAT con sobrecarga:

R2 NAT

```
enable
configure terminal
hostname R2
ipv6 unicast-routing
ip access-list standard INSIDE-DEVS
permit 10.10.10.0 0.0.0.255
permit 172.31.0.0 0.0.255.255
exit
ip nat inside source list INSIDE-DEVS interface gigabitEthernet0/0 overload
ip domain-name ccna-unad.com
interface loopback 0
ip address 10.10.10.10 255.255.255.255
ip nat inside
exit
```

En este caso, hay que definir las ACL que se van a utilizar posteriormente en la configuración, dos listas de acceso standar y dos listas de acceso extendidas, cuya funcionalidad bloquea protocolos de red específicos, en este caso se busca permitir el routing entre el R1 y el R2 y denegar el routing entre el R2 y R3:

ACL R2

```
ip access-list standard miami1
permit 172.31.21.0 0.0.0.255
exit
ip access-list standard miami2
deny 172.31.23.0 0.0.0.255
exit
ip access-list extended miami3
permit tcp 172.31.21.1 0.0.0.3 any
exit
ip access-list extended miami4
deny icmp 172.31.23.2 0.0.0.3 any
exit
```

Para el R2 se muestra la aplicación de las ACL definidas previamente para las interfaces involucradas del router, así como la aplicación del costo y el ancho de banda extremo a extremo con otros enrutadores, para que haya convergencia de enlaces:

R2 interfaces

```
interface serial 0/0/1
ip access-group miami1 in
ip access-group miami2 in
ip access-group miami3 in
ip access-group miami4 in
no shutdown
bandwidth 256
ip address 172.31.21.2 255.255.255.252
ipv6 enable
ip nat inside
exit
interface serial 0/0/0
ip access-group miami1 in
ip access-group miami2 in
ip access-group miami3 in
ip access-group miami4 in
no shutdown
bandwidth 256
ip address 172.31.23.1 255.255.255.252
ip ospf cost 9600
ipv6 enable
ip nat inside
ip access-group miami in
exit
```

La interfaz que va conectada a internet se tiene:

Interfaz Internet

```
interface gigabitEthernet  0/0
no shutdown
ipv6 enable
ip address 209.165.200.225 255.255.255.248
ip nat outside
exit
```

Y el protocolo OSPFv2 para este router:

R2 OSPF

```
router ospf 100
router-id 5.5.5.5
network 172.31.21.2 0.0.0.3 area 0
network 172.31.23.1 0.0.0.3 area 0
network 10.10.10.10 0.0.0.0 area 0
network 209.165.200.224 0.0.0.7 area 0
exit
```

4.2.3 R3

A continuación se presenta la configuración del router 3:

Configuración R3

```
enable
configure terminal
hostname R3
ip domain-name ccna-unad.com
interface loopback 4
ip address 192.168.4.0 255.255.255.0
exit
interface loopback 5
ip address 192.168.5.0 255.255.255.0
exit
interface loopback 6
ip address 192.168.6.0 255.255.255.0
exit
interface serial 0/0/1
no shutdown
bandwidth 256
ip address 172.31.21.2 255.255.255.252
ipv6 enable
exit
interface gigabitEthernet  0/0
no shutdown
ip address 209.165.200.225 255.255.255.248
exit
router ospf 100
router-id 8.8.8.8
network 192.168.4.0 0.0.0.255 area 0
network 192.168.5.0 0.0.0.255 area 0
network 192.168.6.0 0.0.0.255 area 0
network 172.31.23.0 0.0.0.3 area 0
exit
```

4.2.4 Internet

Y para el router de internet que va incluido dentro del cluster:

Configuración Internet

```
enable
configure terminal
hostname Internet
ipv6 unicast-routing
interface gigabitEthernet  0/0
no shutdown
ipv6 enable
ip address 209.165.200.226 255.255.255.248
exit
interface gigabitEthernet  0/1
no shutdown
ipv6 enable
ip address 209.165.200.229 255.255.255.248
exit
router ospf 100
router-id 9.9.9.9
network 209.165.200.228 0.0.0.3 area 0
network 209.165.200.224 0.0.0.7 area 0
exit
```

4.2.5 S1

Con respecto a los switch presentados en el escenario anterior, éstos requieren de configuraciones adicionales debido a las especificaciones dadas, dentro de las cuales están la configuración para acceso remoto mediante SSH, que es la forma más adecuada debido a la seguridad que provee, ya que encripta todas las tramas de la sesión de acceso remoto ante analizadores de protocolos, para lograr ésto tienen que realizarse configuraciones de capa 3, a pesar de que los switch trabajan en capa 2. Para esto se asigna un gateway predeterminado como sigue a continuación:

S1 SSH

```
enable
configure terminal
hostname S3
no ip domain-lookup
service password-encryption
ip default-gateway 192.168.99.1
ip ssh version 2
ip domain-name ccna-unad.com
crypto key generate rsa
1024
username yulver secret cisco
enable password cisco
line vty 0 4
login local
transport input ssh
exit
```

Posteriormente se configuraron las Vlan asignandoles nombres y dirección ip para acceso remoto:

S1 Vlan

```
vlan 30
name Administracion
exit
vlan 40
name Mercadeo
exit
vlan 99
name Remota
exit
vlan 200
name Mantenimiento
exit
interface vlan 99
ip address 192.168.99.2 255.255.255.0
exit
```

Luego se configuran los interfaces que serán las troncales y de acceso:

S1 Interfaces

```
interface gigabitEthernet 0/1
switchport mode trunk
switchport trunk allowed vlan 1,30,40,99,200
switchport trunk native vlan 1
exit
interface gigabitEthernet 0/2
switchport mode trunk
switchport trunk allowed vlan 1,30,40,99,200
switchport trunk native vlan 1
exit
interface fastEthernet 0/1
switchport mode access
switchport access vlan 30
exit
```

4.2.6 S3

Por último para el switch 3 se tiene la siguiente configuración:

S3 Configuración

```
enable
configure terminal
hostname S3
no ip domain-lookup
service password-encryption
ip default-gateway 192.168.99.1
ip ssh version 2
ip domain-name ccna-unad.com
crypto key generate rsa
1024
username yulver secret cisco
enable password cisco
line vty 0 4
login local
transport input ssh
exit
vlan 30
name Administracion
exit
vlan 40
name Mercadeo
exit
vlan 99
name Remota
exit
interface vlan 99
ip address 192.168.99.3 255.255.255.0
exit
vlan 200
name Mantenimiento
exit
interface gigabitEthernet 0/2
switchport mode trunk
switchport trunk allowed vlan 1,30,40,99,200
switchport trunk native vlan 1
exit
interface fastEthernet 0/1
switchport mode access
switchport access vlan 40
exit
```

5. PRUEBAS Y RESULTADOS

5.1 Escenario 1

Una vez realizadas las configuraciones de los dispositivos de red, se mostrará el resultado de la conectividad completa para este escenario, empezando por la prueba de conectividad a la interfaz del ISP, desde el PC0 mediante el comando tracert, evidenciando así el correcto funcionamiento de DHCP, además del protocolo de enrutamiento RIP ya que se pueden apreciar los saltos en los gateway:

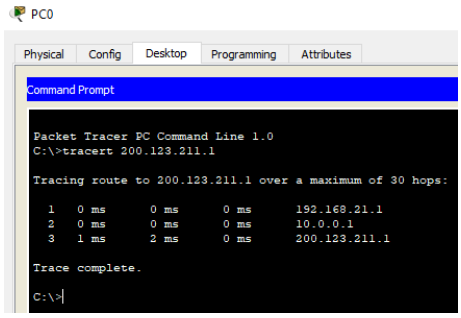

Figura 5.1: Comando tracert PC0 a ISP

Posteriormente se muestra la misma prueba para la VLAN de las Laptops:

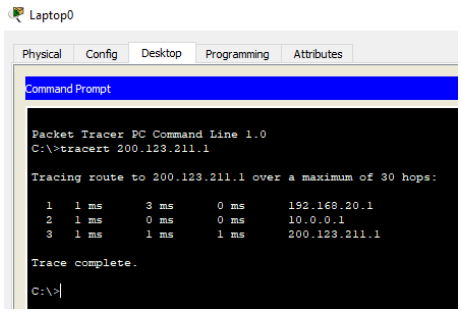

Figura 5.2: Comando tracert laptop0 a ISP

Para la subred que está conectada con el servidor se le hizo la prueba para mostrar la conexión con el ISP:

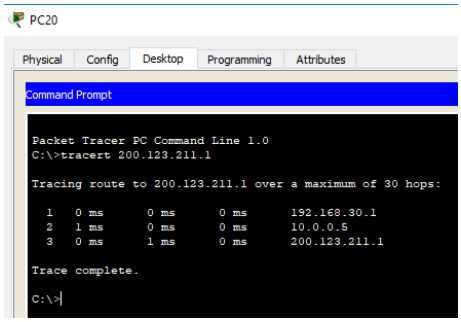

Figura 5.3: Comando tracert PC20 a ISP

Finalmente para evidenciar la operación Dual-Stack en la subred del servidor, se tuvo la siguiente respuesta al ejecutar el comando ping en ipv6 desde la laptop31:

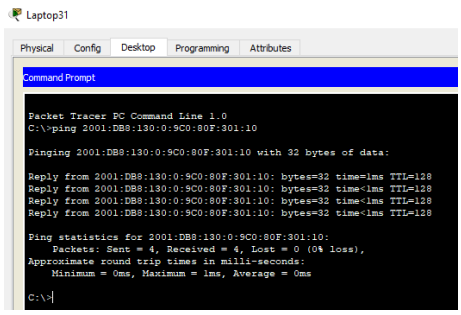

Figura 5.4: Conexión entre la laptop 31 y el servidor

5.2 Escenario 2

Para el escenario 2 se muestra la prueba de conectividad desde el PC1 al PC0 que está detrás de Internet:

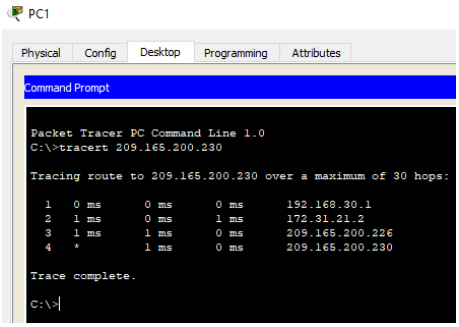

Figura 5.5: Conexión entre PC1 y PC0

A continuación se prueba la conectividad entre el PC2 y el PC0 detrás de internet:

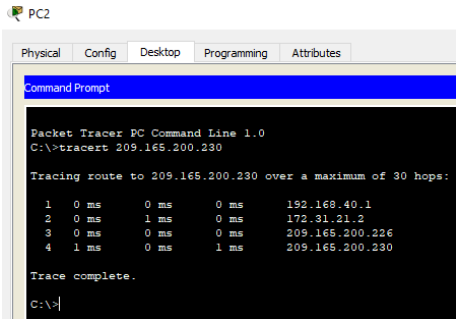

Figura 5.6: Conexión entre PC2 y PC0

Debido a las ACL el tráfico proveniente de R3 se bloquea en R2, por lo tanto, al realizar la prueba de conectividad entre un terminal de la red generada por R3 muestra el siguiente resultado:

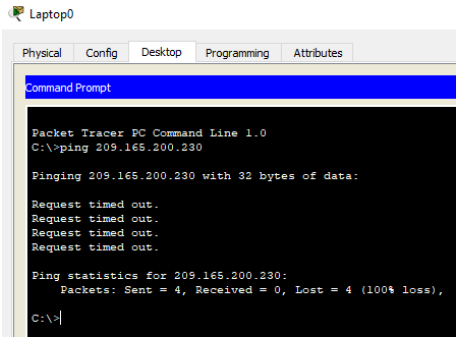

Figura 5.7: Conexión entre Laptop0 y PC0

6. CONCLUSIONES

- Al momento de configurar una red, hay que tener varias normas escenciales para la seguridad de esta, cómo las contraseñas, el envío de tramas con cifrado y ACL, todo esto ayuda a evitar intrusiones, robo de información y sabotaje externo dentro de la red.

- La seguridad de puertos tambien es importante en las redes, evita ataques de reconocimiento por parte de intrusos.

- Uno de los requisitos para que un enlace dentro de un protocolo de enrutamiento como OSPF, es de establecer dentro de este los mismos parámetros de ancho de banda, métrica y costo.

- El protocolo de enrutamiento RIP está hecho para conectar redes de menor tamaño, mientras el OSPF para redes de gran magnitud

7. ACEPTACIÓN

Bogotá, 17 de febrero de 2019

REFERENCIAS

[CISCO,] CISCO. CCNA Switching and Routing.