PRUEBA DE HABILIDADES PRÁCTICAS CCNA

Nicolás Simón Ruiz Gamba

Universidad Nacional Abierta y a Distancia CCVA-FACATATIVA

ECBTI Ingeniería de Telecomunicaciones

Facatativá

2019

PRUEBA DE HABILIDADES PRÁCTICAS CCNA

Nicolás Simón Ruiz Gamba

Trabajo Final Diplomado de profundización Cisco (Diseño e implementación de soluciones integradas LAN / WAN) – Grupo 203092_1

Director de curso Ingeniero Juan Carlos Vesga

Universidad Nacional Abierta y a Distancia CCVA-FACATATIVA

ECBTI Facultad de Ingeniería de Telecomunicaciones

Febrero 2019

Facatativá, (Febrero de 2019)

NOTA DE ACEPTACIÓN

_____
_____
_____
_____
_____
_____
_____

_____
Presidente del jurado

_____
Jurado

Tabla de contenido

Tabla de imágenes

Glosario

LAN: son las siglas de Local Area Network, Red de área local. Una LAN es una red que conecta los ordenadores en un área relativamente pequeña y predeterminada.

OSPF: (Open Shortest Path First) 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

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

CCNA: (Cisco Certified Network Associate) es una certificación entregada por la compañía Cisco Systems a las personas que hayan rendido satisfactoriamente el examen correspondiente sobre infraestructuras de red e Internet.

Cisco IOS: (originalmente Internetwork Operating System) es el software utilizado en la gran mayoría de routers (encaminadores) y switches (conmutadores) de Cisco Systems (algunos conmutadores obsoletos ejecutaban CatOS).

IPv4: es la versión actual del protocolo de Internet, el sistema de identificación que utiliza Internet para enviar información entre dispositivos.

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

Resumen

Este trabajo se realizó con el objetivo poner en práctica el trabajo asimilado y las habilidades prácticas adquiridas durante el desarrollo del diplomado de profundización CCNA, la práctica se lleva a cabo bajo la modalidad de escenarios aplicados, facilitando de una manera práctica y real, problemas o implementaciones a las que se puede ver enfrentado un ingeniero en la rama de las Telecomunicaciones se pone a prueba toda la comprensión de los conceptos y adicionalmente se fortalece la resolución de problemas del mundo real.

1. Introducción

Durante el tiempo de preparación, donde se desarrollaron las diversas actividades del diplomado de profundización CCNA, se adquirieron conocimientos relacionados con diversos aspectos de Networking, los cuales se colocaron en práctica en el desarrollo de las dos actividades propuestas, donde se configuro cada uno de los dispositivos de red de una empresa para interconectarlos entre sí, esto acorde con los lineamientos establecidos para aplicar hitos importantes, dentro de estos encontramos el direccionamiento IP, protocolos de enrutamiento, parámetros de seguridad, buenas practicas de endurecimiento de la infraestructura de comunicaciones y demás aspectos que forman parte de la topología de red. Adicionalmente, todos los procedimientos desarrollados en los escenarios planteados se realizaron con el apoyo de la herramienta Packet Tracert, logrando de esta manera poner en práctica las habilidades adquiridas en el desarrollo del diplomado, dentro de estas se cumple con el objetivo de fortalecer el manejo del sistema operativo de los dispositivos, manipulación eficiente de software especializado y tener un contacto preliminar con equipos de red de manera virtual.

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

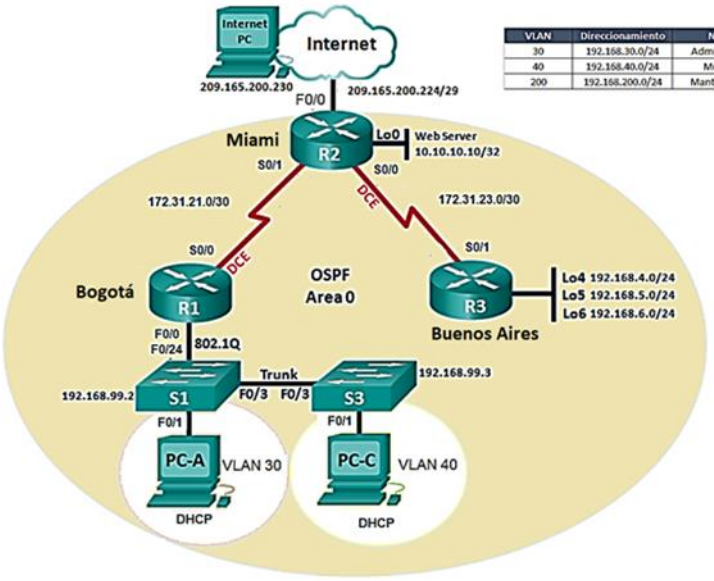
2. Desarrollo de los escenarios propuestos

2.1Escenario 1

2.2Descripción del escenario

Una empresa de Tecnología posee tres sucursales distribuidas en las ciudades de Miami, Bogotá y Buenos Aires, 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. A continuación en la ilustración se evidencia la disposición de los equipos de red, los servicios prestados y el respectivo direccionamiento asignado.

Imagen 1. Topología Escenario 1



VLAN	Direccionamiento	Nombre
30	192.168.30.0/24	Administración
40	192.168.40.0/24	Mercadeo
200	192.168.200.0/24	Mantenimiento

Fuente: Guía Packet Tracert Academy

Dentro de las actividades llevadas a cabo para la solución del escenario, de acuerdo a los parámetros dados por la ilustración 1, se realizó actividades como: configuración de protocolos de enrutamiento dinámico OSPF V2 para interconectar los routers.

En el R2 se llevó a cabo la configuración de NAT para permitir la salida de internet de los equipos

En el router de Bogotá también se realiza una configuración especial con el fin de tener conexiones entre VLAN, se realizó configuración DHCP para los segmentos de administración y Mercadeo. Se procedió a realizar el aseguramiento de acceso por medio de listas de ip permitidas

Adicionalmente dentro de los requerimientos establecidos y las practicas anteriormente realizadas, se implementan configuraciones como la protección de acceso a la línea de comandos, aseguramientos de las líneas de acceso VTY, cifrar Password, crear banners previniendo el acceso no autorizado y cambar nombre de las host.

2.3Direccionamiento asignado

En la ilustración que se relaciona a continuación se relacionan, los dispositivos a utilizar, las interfaces que se deben configurar y el direccionamiento IP que se debe asignar a cada una.

Imagen 2. Dispositivos, Interfaces y Direcciones IP

DISPOSITIVO	INTERFACE	DIRECCION IP	MASCARA DE RED
ROUTER ISP	GI 0/0	209.165.200.230	255.255.255.248
R2	FA 0/0	209.165.200.225	255.255.255.248
R2	S0/0/0	172.31.23.1	255.255.255.252
R2	S0/0/1	172.31.21.2	255.255.255.252
R2	Lo0	10.10.10.10	255.255.255.255
R1	S 0/0/0	172.31.21.1	255.255.255.252
R1	FA 0/0.30	192.168.30.1	255.255.255.0
R1	FA 0/0.40	192.168.40.1	255.255.255.0
R1	FA 0/0.200	192.168.200.1	255.255.255.0
R1	FA 0/0.99	192.168.99.1	255.255.255.0
R3	S0/0/1	172.31.23.2	255.255.255.252
R3	Lo4	192.168.4.1	255.255.255.0
R3	Lo5	192.168.5.1	255.255.255.0
R3	Lo6	192.168.6.1	255.255.255.0
SW1	Vlan 99	192.168.99.2	255.255.255.0
SW3	Vlan 99	192.168.99.3	255.255.255.0
PC-A	Vlan 30	Dinámica	Dinámica
PC-C	Vlan 40	Dinámica	Dinámica

Fuente: Guía Packet Tracert Academy

2.4Configuración y verificación del protocolo OSPF V2

A continuación a través de las ilustraciones, se evidencia los comandos que se usan en los equipos de enrutamiento, para llevar a cabo la tarea de configuración del protocolo OSPF, se muestra la asignación de direcciones ip y áreas, cumpliendo con los parámetros necesarios, garantizando una correcta configuración. Dicha información se ejecuta de acuerdo a la información suministrada por la guía de actividades de CISCO.

Imagen 3 configuración OSPF V2 Router 1

```
R1>ena
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#router ospf 1
R1(config-router)#router-id 1.1.1.1
R1(config-router)#network  172.31.21.0 0.0.3 area 0
                                       ^
% Invalid input detected at '^' marker.

R1(config-router)#network  172.31.21.0 0.0.0.3 area 0
R1(config-router)#network  192.168.30.0 0.0.0.255 area 0
R1(config-router)#network  192.168.40.0 0.0.0.255 area 0
R1(config-router)#network  192.168.200.0 0.0.0.255 area 0
R1(config-router)#passive-interfa g0/0.30
R1(config-router)#passive-interfa g0/0.40
R1(config-router)#passive-interfa g0/0.200
R1(config-router)#exit
R1(config)#inter s0/0/0
R1(config-if)#bandwi 256
R1(config-if)# ip ospf cost 9500
R1(config-if)#
```

Fuente Packet Tracert

En la ilustración se evidencia que una vez se ingresa en modo configuración en el Router 1, se ejecuta el comando ROUTER OSPF 1, con el fin de empezar a asignar los parámetros necesarios para una correcta configuración. Dentro de estos encontramos el ID, la red que se asigna, el área de trabajo, la interfaz de red, a la que se le asigna el protocolo, el ancho de banda a utilizar y el costo.

De igual manera, se ejecuta el procedimiento anteriormente detallado, con el Router 2 y el Router 3, con la variante, que se detalla en las respectivas ilustraciones, en estas cambia el ID asociado, la red que se propaga y la interfaz a la que se le asigna. El costo y ancho de banda permanecen iguales.

Imagen 4 configuración OSPF V2 Router 2

```
R2>ena
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#router ospf 1
R2(config-router)#router-id 5.5.5.5
R2(config-router)#networ 172.31.21.0 0.0.0.3 area 0
R2(config-router)#
01:23:14: %OSPF-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/1
from LOADING to FULL, Loading Done

R2(config-router)#networ 172.31.23.0 0.0.0.3 area 0
R2(config-router)#networ 10.10.10.0 0.0.0.255 area 0
R2(config-router)#passive-inter g0/0
R2(config-router)#inte s0/0/0
R2(config-if)#bandwi 256
R2(config-if)#inte s0/0/1
R2(config-if)#bandwi 256
R2(config-if)#inte s0/0/0
R2(config-if)#ip ospf cost 9500
R2(config-if)#
```

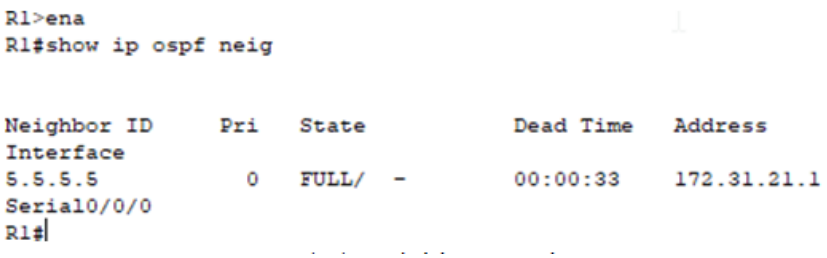
Imagen 5 configuración OSPF V2 Router 3

```
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1,
changed state to up


R3>en
R3#conf
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#router ospf 1
R3(config-router)#router-id 8.8.8.8
R3(config-router)#network 172.31.23.0 0.0.0.3 area 0
R3(config-router)#
01:38:41: %OSPF-5-ADJCHG: Process 1, Nbr 5.5.5.5 on Serial0/0/1
from LOADING to FULL, Loading Done

R3(config-router)#network 192.168.4.0 0.0.0.255 area 0
R3(config-router)#passive-interf lo4
R3(config-router)#passive-interf lo5
R3(config-router)#passive-interf lo6
R3(config-router)#exit
R3(config)#inte s0/0/1
R3(config-if)#bandwi 256
R3(config-if)#
```

Fuente Packet Tracer

Como se indicó en el inicio de esta sección, una vez realizado el proceso de configuración, es necesario validar que dichos pasos se hallan ejecutado de una manera correcta, para esto a continuación se relacionan las respectivas ilustraciones de los equipos R1,R2,R3, en donde al ejecutar el comando SHOW IP NEIGHBOR, nos permite de manera gráfica sobre el equipo, visualizar el status de la configuración. Una vez ejecutado observamos datos como, tiempo de conexión, ID, red propagada y estado.

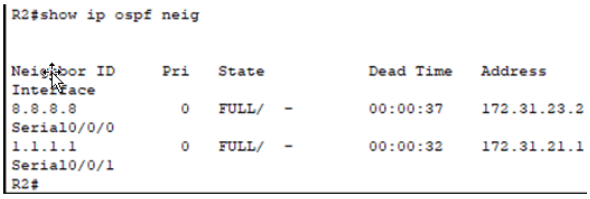
Imagen 6 Estatus OSPF R1



Fuente Packet Tracert

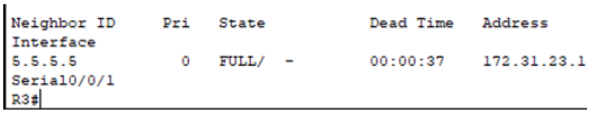
De igual manera, se realiza la ejecución del comando relacionado en los dos router restantes. En estos se tiene como resultado las redes, el Id de conexión, el estado de conexión.

Imagen 7 Estatus OSPF R2



Fuente Packet Tracert

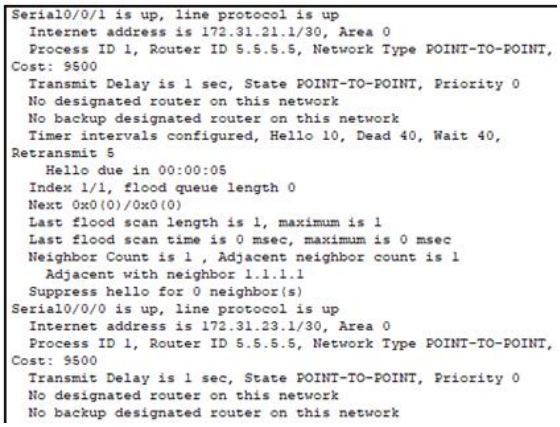
Imagen 8 Estado OSPF R3



Fuente Packet Tracert

Para una visualización más detallada se ejecuta el comando SHOW IP PROTOCOLS, el cual permite verificar los parámetros y otra información del estado actual de cualquier proceso activo de enrutamiento. Se relacionan los resultados obtenidos de la ejecución del comando en los dispositivos router del ejercicio practico.

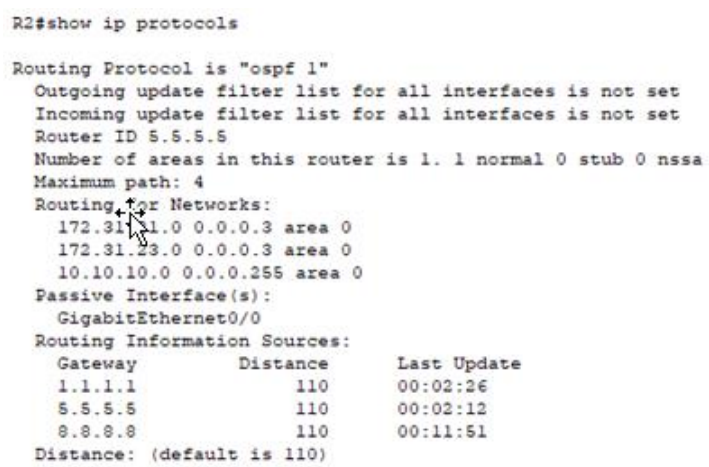
Imagen 9 Show ip protocols R3



```
Serial0/0/1 is up, line protocol is up
  Internet address is 172.31.21.1/30, Area 0
  Process ID 1, Router ID 5.5.5.5, Network Type POINT-TO-POINT,
Cost: 9500
  Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40,
Retransmit 5
    Hello due in 00:00:05
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1 , Adjacent neighbor count is 1
    Adjacent with neighbor 1.1.1.1
  Suppress hello for 0 neighbor(s)
Serial0/0/0 is up, line protocol is up
  Internet address is 172.31.23.1/30, Area 0
  Process ID 1, Router ID 5.5.5.5, Network Type POINT-TO-POINT,
Cost: 9500
  Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
  No designated router on this network
  No backup designated router on this network
```

Fuente Packet Tracert

Imagen 10 Ip Protocols R2



```
R2#show ip protocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 5.5.5.5
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.31.21.0 0.0.0.3 area 0
    172.31.23.0 0.0.0.3 area 0
    10.10.10.0 0.0.0.255 area 0
  Passive Interface(s):
    GigabitEthernet0/0
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1              110      00:02:26
    5.5.5.5              110      00:02:12
    8.8.8.8              110      00:11:51
  Distance: (default is 110)
```

Fuente Packet Tracert

2.5Tabla de enrutamiento y conexiones por OSPF

Una vez realizado el proceso de configuración, se hace la verificación de las tablas de enrutamiento con el fin de garantizar las conexiones con los equipos próximos. Esta validación se realiza con el comando SHOW IP ROUTE OSPF, al ejecutarlo en los router R1, R2, R3, se obtuvieron los resultados relacionados en las imágenes a continuación.

Imagen 11 Show ip route ospf R1

```
R1#show ip route ospf
     10.0.0.0/24 is subnetted, 1 subnets
O       10.10.10.0 [110/9501] via 172.31.21.1, 00:34:04,
Serial0/0/0
     172.31.0.0/16 is variably subnetted, 3 subnets, 2 masks
O       172.31.23.0 [110/19000] via 172.31.21.1, 00:24:32,
Serial0/0/0
     192.168.4.0/32 is subnetted, 1 subnets
O       192.168.4.1 [110/19001] via 172.31.21.1, 00:17:56,
Serial0/0/0
```

Fuente Packet Tracert

Imagen 12 Show ip route ospf R2

```
R2>ena
R2#sh
R2#show ip ro
R2#show ip route os
R2#show ip route ospf
     192.168.4.0/32 is subnetted, 1 subnets
O       192.168.4.1 [110/9501] via 172.31.23.2, 02:19:55,
Serial0/0/0
O    192.168.30.0 [110/9501] via 172.31.21.1, 02:08:02,
Serial0/0/1
O    192.168.40.0 [110/9501] via 172.31.21.1, 02:08:02,
Serial0/0/1
O    192.168.200.0 [110/9501] via 172.31.21.1, 02:08:02,
Serial0/0/1
```

Fuente Packet Tracert

Imagen 13 Show ip route ospf R3

```
R3#show ip route ospf
     10.0.0.0/24 is subnetted, 1 subnets
O       10.10.10.0 [110/391] via 172.31.23.1, 00:16:33,
Serial0/0/1
     172.31.0.0/16 is variably subnetted, 3 subnets, 2 masks
O       172.31.21.0 [110/9890] via 172.31.23.1, 00:06:50,
Serial0/0/1
O    192.168.30.0 [110/9891] via 172.31.23.1, 00:06:50,
Serial0/0/1
O    192.168.40.0 [110/9891] via 172.31.23.1, 00:06:50,
Serial0/0/1
O    192.168.200.0 [110/9891] via 172.31.23.1, 00:06:50,
Serial0/0/1
```

Fuente Packet Tracert

2.6 Configuración de VLAN, puertos troncales, puertos de acceso, encapsulamiento y enrutamiento entre VLAN

De acuerdo al escenario planteado, se deben realizar configuraciones sobre los equipos, dichos parámetros tienen como propósito crear las redes virtuales segmentando el tráfico, troncalizar y encapsular puertos con el fin de realizar conexiones entre los mismos, adicionalmente se establecen rutas que permitan enviar el trafico de una sede a otra de acuerdo a como se den las comunicaciones. Para evidenciar el proceso en las imágenes (14 - a continuación se relacionan los comandos ejecutados sobre los diferentes equipos de red.

Imagen 14 Configuración R1

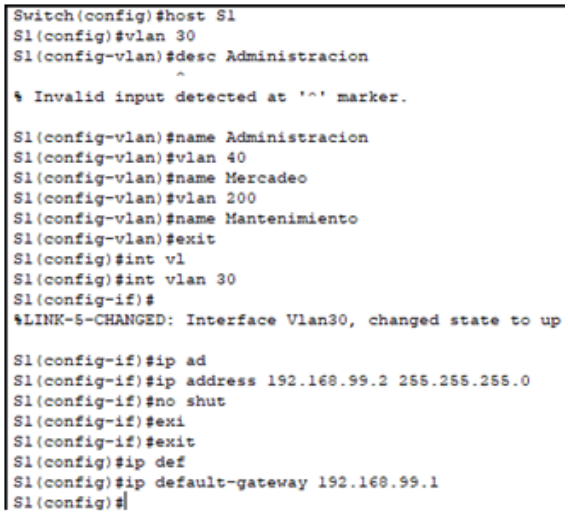
```
R1(config-subif)#en
R1(config-subif)#encapsulation do
R1(config-subif)#encapsulation dot1Q 30
R1(config-subif)#ip add 192.168.30.1 255.255.255.0
R1(config-subif)#no ip add
R1(config-subif)#no encapsulation dot1Q 30
R1(config-subif)#no descri Mantenimiento
R1(config-subif)#no int g0/0.40
R1(config)#int g0/0.30
R1(config-subif)# descri Administracion
R1(config-subif)#encapsulation dot1Q 30
R1(config-subif)#ip add 192.168.30.1 255.255.255.0
R1(config-subif)#exit
R1(config)#int g0/0.40
R1(config-subif)# descri Mercadeo
R1(config-subif)#encapsulation dot1Q 40
R1(config-subif)#ip add 192.168.40.1 255.255.255.0
R1(config-subif)#int g0/0.200
R1(config-subif)#descr Mantenimiento
R1(config-subif)#encapsulation dot1Q 200
R1(config-subif)#ip add 192.168.200.1 255.255.255.0
R1(config-subif)#exit
R1(config)#int g0/0
R1(config-if)#no shut
```

Fuente Packet Tracert

En la imagen 14 se realiza creación de vlan, troncalización y encapsulamiento, así como se agrega la respectiva descripción a cada una de las Vlan, con el fin de organización, seguridad y una buena administración.

Sobre la imagen 15, se relaciona la configuración del SW1 con sus respectivos comandos

Imagen 15 Configuración SW1

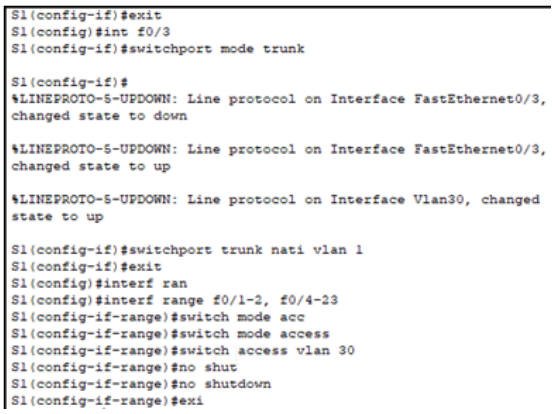


```
Switch(config)#host S1
S1(config)#vlan 30
S1(config-vlan)#desc Administracion
                 ^
% Invalid input detected at '^' marker.

S1(config-vlan)#name Administracion
S1(config-vlan)#vlan 40
S1(config-vlan)#name Mercadeo
S1(config-vlan)#vlan 200
S1(config-vlan)#name Mantenimiento
S1(config-vlan)#exit
S1(config)#int vl
S1(config)#int vlan 30
S1(config-if)#
%LINK-5-CHANGED: Interface Vlan30, changed state to up

S1(config-if)#ip ad
S1(config-if)#ip address 192.168.99.2 255.255.255.0
S1(config-if)#no shut
S1(config-if)#exi
S1(config-if)#exit
S1(config)#ip def
S1(config)#ip default-gateway 192.168.99.1
S1(config)#
```

Fuente Packet Tracert

La anterior imagen evidencia la creación de Vlan sobre el Sw, esto para realizar una segmentación del tráfico, adicionalmente muestra la asignación de la red y la puerta de enlace.

Imagen 16 configuración SW puertos

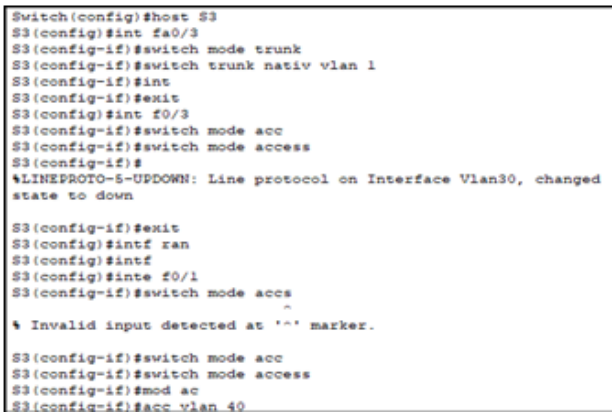


```
S1(config-if)#exit
S1(config)#int f0/3
S1(config-if)#switchport mode trunk

S1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3,
changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3,
changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan30, changed
state to up

S1(config-if)#switchport trunk nati vlan 1
S1(config-if)#exit
S1(config)#interf ran
S1(config)#interf range f0/1-2, f0/4-23
S1(config-if-range)#switch mode acc
S1(config-if-range)#switch mode access
S1(config-if-range)#switch access vlan 30
S1(config-if-range)#no shut
S1(config-if-range)#no shutdown
S1(config-if-range)#exi
```

Fuente Packet Tracert

La imagen 16 nos muestra como en el switch 1 se llevó a cabo una configuración de puertos troncales (conexión para router 1 y conexión a SW3), puerto de acceso, conexión a PC-A.

Imagen 17 Configuración SW3



Fuente Packet Tracer

En el SW3 de configuró como nos muestra la imagen 17, el puerto de acceso para la conexión a PC – C y un puerto troncal que conecta a SW1.

Para evitar búsquedas por DNS sobre los equipos de red en el momento en que se cometa un error de transcripción se procede a deshabilitar la búsqueda a través del DNS por defecto. A continuación en la imagen se evidencia este procedimiento.

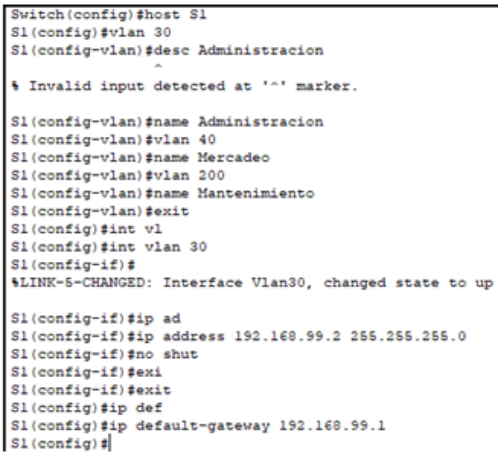
Imagen 18 Deshabilitar DNS Lookup

Fuente Packet Tracert

2.7 Asignación de ip a los Switches

Para la administración de los switches se llevó a cabo la configuración de una vlan para gestionar los equipos, esta se relaciona en la imagen 2 (Dispositivos, Interfaces y Direcciones IP) se resumen el direccionamiento IP asignado a los dispositivos.

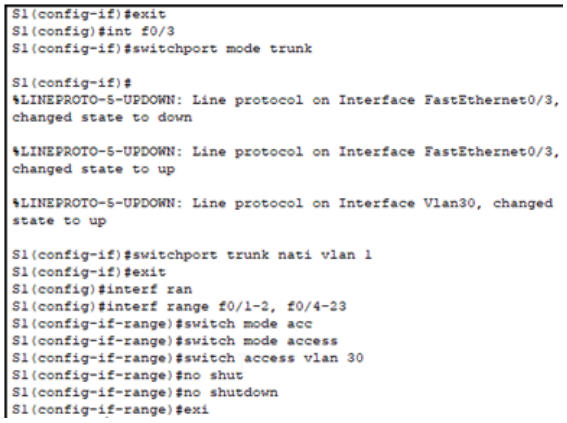
Imagen 19 Configuración Vlan Administración



Fuente Packet Tracert

Adicionalmente también se muestra la creación de las Vlan para las áreas de Mantenimiento y mercadeo, a etas se les asigna su respectivo ID de red, se configura Gateway al equipo el cual envía el trafico desconocido hacia el router para encontrar el destino que se desee consultar.

Imagen 20 continuación configuración SW 1



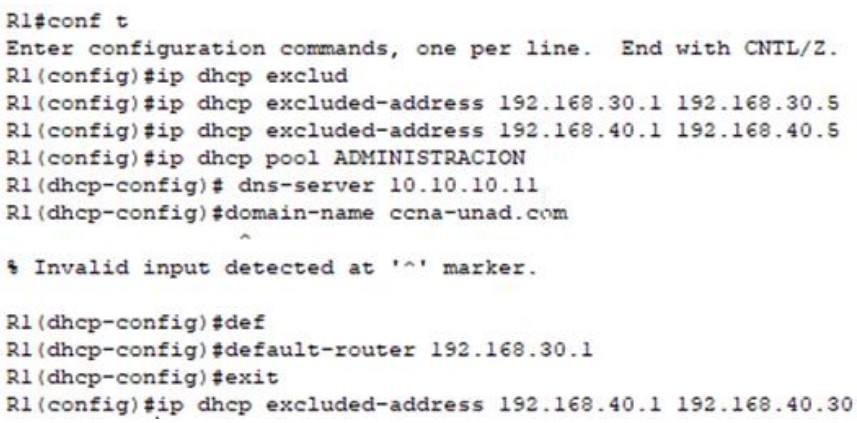
Fuente Packet Tracert

En esta continuación se relaciona los puertos que se encuentran configurados como acceso, las Vlan a las que pertenecen, así como también se configura el puerto fa0/3 como troncal.

2.8Configuración DHCP

La configuración de este protocolo (DHCP), para las VLAN 30 y 40 se llevó a cabo en el R1, inicialmente se configuró en el dispositivo los rangos de IP que debían excluirse y posteriormente se asignaron los parámetros propuestos en el escenario número 1.

Imagen 21 Configuración DHCP R1



Fuente Packet Tracert

En la anterior imagen se establece desde que ip se realizaran la asignaciones de direcciones ip de manera dinámica, así como también se detalla los rangos ip excluidos.

Imagen 22 Creación de pool DHCP

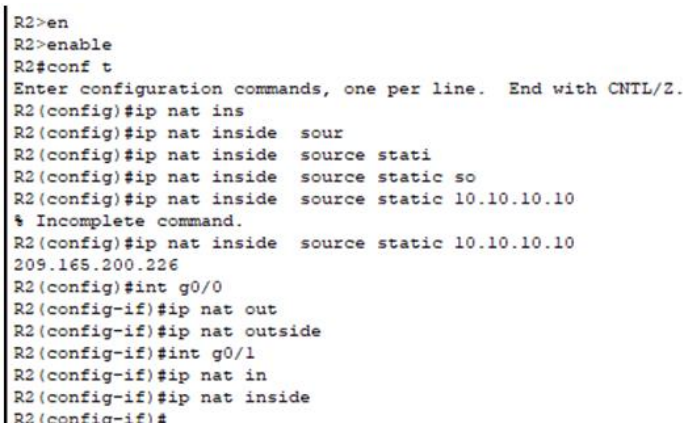
Fuente Packet Tracert

En la anterior imagen podemos ver las exclusiones realizadas, esto posteriormente para crear los pool asignarlos a las áreas específicas, así como también relacionar el dominio que usaran (ccna-unad.com).

2.9 Configuración Network Address Translation (NAT)

Basado en la topología de red suministrada inicial mente para este escenario, se muestra que las estaciones tienen una salida hacia internet, a través del R2, en la siguiente imagen se puede visualizar la configuración realizada.

Imagen 23 Configuración NAT



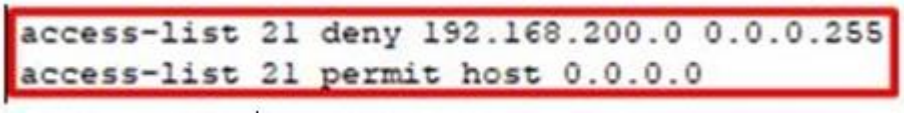
Fuente Packet Tracert

En esta imagen se evidencia el NAT estatico creado, las ip de la red LAN y la ip Publica, así como también se detallan las interfaces de entrada y salida de tráfico

2.10 Configuración ACL estándar

La seguridad a través de ACL, configurada para este caso, nos permite filtrar tráfico con base en la dirección ip de origen.

Imagen 24 Configuración Listas de Acceso



Fuente Packet Tracert

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

Imagen 25 ACL VLAN 30 Y 40

```
R2(config-if)#exit
R2(config)#acc
R2(config)#access-list 1 perm
R2(config)#access-list 1 permit 192.168.30.0 0.0.0.255
R2(config)#access-list 1 permit 192.168.40.0 0.0.0.255
```

Fuente Packet Tracert

En la imagen anterior se crearon dos listas de acceso extendidas en R2: La ACL 1 permite el tráfico de la red 192.168.30.0/24 hacia la red de internet, si mismo como la red192.168.40.0/24.

2.11 Pruebas de conectividad escenario 1

A continuación se relaciona las imanes que nos permiten garantizar que la configuración realizada a nivel de los dispositivos de red, esta correcta y que la distribución de los paquetes se realiza de acuerdo a lo establecido en la topología suministrada inicialmente.

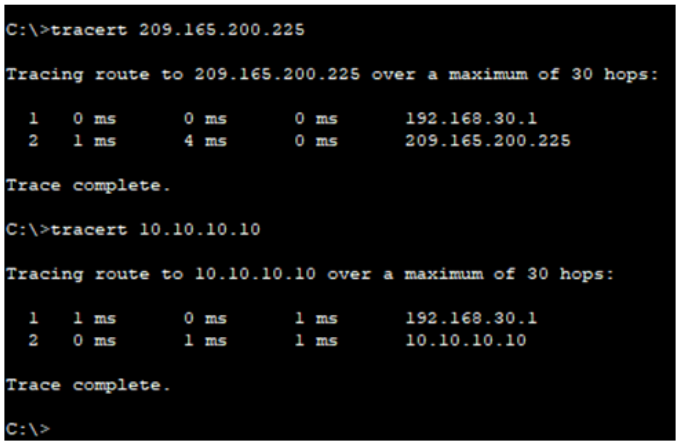
Imagen 26 Trazas desde la PC-A hacia las redes de R3

```
Packet Tracer PC Command Line 1.0
C:\>tracert 192.168.5.1

Tracing route to 192.168.5.1 over a maximum of 30 hops:

  1   1 ms      0 ms      0 ms      192.168.30.1
  2   1 ms      0 ms      1 ms      172.31.21.2
  3   47 ms     2 ms      1 ms      192.168.5.1

Trace complete.

C:\>tracert 192.168.4.1

Tracing route to 192.168.4.1 over a maximum of 30 hops:

  1   0 ms      0 ms      0 ms      192.168.30.1
  2   1 ms      0 ms      6 ms      172.31.21.2
  3   0 ms      3 ms      2 ms      192.168.4.1

Trace complete.

C:\>tracert 192.168.6.1

Tracing route to 192.168.6.1 over a maximum of 30 hops:

  1   0 ms      1 ms      0 ms      192.168.30.1
  2   1 ms      1 ms      0 ms      172.31.21.2
  3   1 ms      2 ms      0 ms      192.168.6.1

Trace complete.
```

Fuente Packet Tracert

En la imagen 26, vemos que los saltos que se realizan desde la PC A, hacia las redes configuradas en el R3, se ejecutan de manera exitosa.

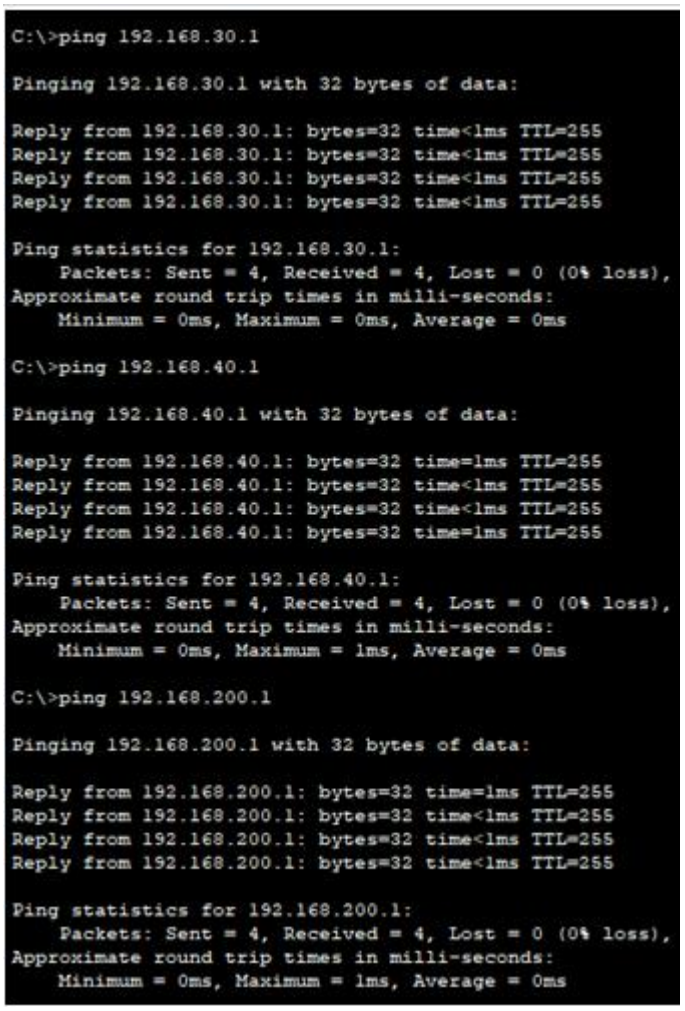
Imagen 27 Trazas desde PC – A hacia redes de R2



Fuente Packet Tracert

De igual manera, se evidencia en la imagen anterior, que las pruebas de conectividad realizadas desde la misma PC A, hacia las redes de R2, se están completando de manera exitosa, garantizando que este segmento tiene la salida hacia internet y que el NAT esta bien configurado.

Imagen 28 Conectividad desde PC – A hacia redes de R1

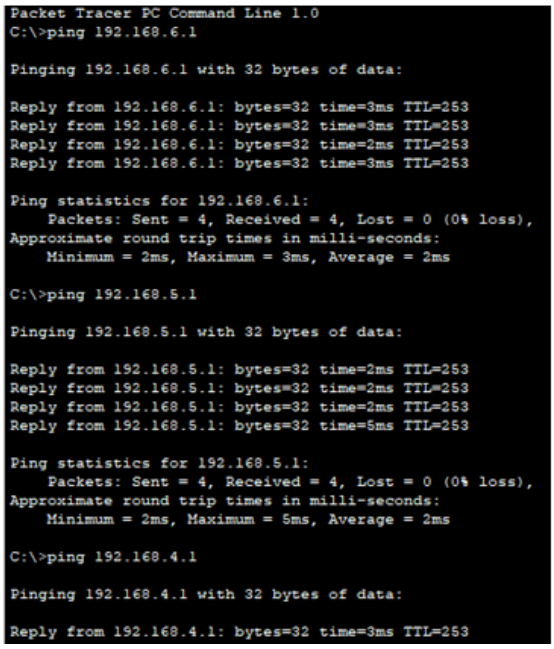


Fuente Packet Tracert

La imagen 28 permite validar las conexiones exitosas desde uno de los extremos (PC-A) hacia las redes configuradas dentro de R1

De la misma manera, se realizan pruebas de conexión desde los otros PC, relacionados en la topología propuesta para este escenario, esto con el fin de validar las configuraciones realizadas a nivel de equipos de red.

Imagen 29 Conectividad desde PC-C hacia R3

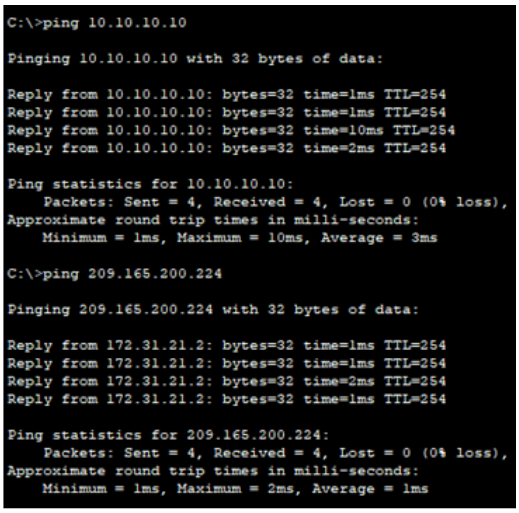


Fuente 1 Packet Tracert

Desde el extremo donde se encuentra ubicada la PC C, se hacen pruebas de conexión hacia las redes configuradas en R3, estas muestran respuesta exitosa.

Ahora se relaciona la prueba desde el mismo extremo hacia R2

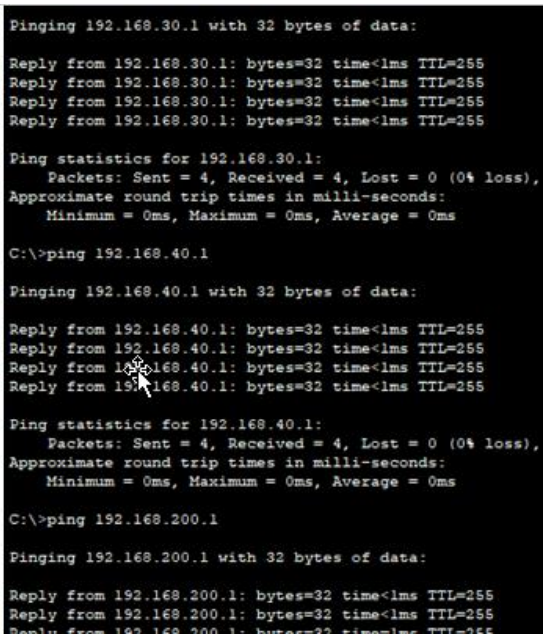
Imagen 30 Conectividad desde PC-C hacia R2



En la imagen 30 vemos la conexión que existe desde el PC C hacia las redes configuradas en R2.

Para finalizar las pruebas se realizan desde la PC C hacia las redes configuradas de tras de R1

Imagen 31 Conectividad desde PC-C hacia R1



Fuente Packet Tracert

2.12 Archivos de configuración

A continuación se relaciona la configuración de todos los dispositivos de red, que intervinieron y se configuraron en las comunicaciones, respecto a la topología establecida en la guía de actividades.

ROUTER 1

R1#sh run

Building configuration...

Current configuration : 2609
bytes version 12.4
no service timestamps log datetime msec

no service timestamps debug datetime msec service password-
encryption hostname R1
enable secret 5 $12Wlk.mert567uHSWQ.&%FUY enable password 7
0822455D0A16 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 dhcp pool ADMINISTRACION network 192.168.30.0
255.255.255.0 default-router 192.168.30.1
dns-server
10.10.10.11 ip dhcp
pool MERCADEO
network 192.168.40.0 255.255.255.0

default-router 192.168.40.1

dns-server
10.10.10.11 no ip
cef no ipv6 cef
username admin secret 5
1mERr$9cTjUIEqNGurQiFU.ZeCi1 ip ssh version 2
ip domain-name ccna-
unad.com spanning-tree

mode pvst
interface FastEthernet0/0 description
LAN no ip address duplex auto speed
auto
interface FastEthernet0/0.30 description VLAN Administracion encapsulation dot1Q
30 ip address 192.168.30.1 255.255.255.0
ip access-group 102 out

interface FastEthernet0/0.40 description VLAN Mercadeo
encapsulation dot1Q 40
ip address 192.168.40.1 255.255.255.0
ip access-group 101 out
interface FastEthernet0/0.99 description VLAN Management encapsulation dot1Q
99 ip address 192.168.99.1 255.255.255.0
interface FastEthernet0/0.200 description VLAN Mantenimiento encapsulation dot1Q
200 ip address 192.168.200.1 255.255.255.0
ip access-group 21 out
interface FastEthernet0/1 no ip
address duplex auto speed auto
shutdown
interface Serial0/0/0 description Enlace a R2 bandwidth
128 ip address 172.31.21.1 255.255.255.252
ip ospf cost 7500 clock rate
64000 interface Serial0/0/1 no
ip address clock rate 2000000
shutdown
interface Vlan1 no ip address
shutdown router ospf 1
router-id 1.1.1.1
log-adjacency-changes
passive-interface FastEthernet0/0 network 172.31.21.0 0.0.0.3 area 0 network 192.168.30.0
0.0.0.255 area 0
network 192.168.40.0 0.0.0.255 area 0
network 192.168.200.0 0.0.0.255 area 0
network 192.168.99.0 0.0.0.255
area 0 ip classless
ip flow-export version 9
access-list 21 deny 192.168.200.0 0.0.0.255
access-list 21 permit host 0.0.0.0
access-list 101 deny ip 192.168.40.0 0.0.0.255 209.165.200.224 0.0.0.7
access-list 101 permit ip any any
access-list 102 deny ip 192.168.30.0 0.0.0.255 host 10.10.10.10 access-list 102 permit ip any
any no cdp run
banner motd ^C Acceso solo a personal autorizado
^C line con 0
exec-timeout 5 0

password 7 0822455D0A16
login line aux 0
line vty 0 4 login local
transport input ssh line vty 5
15 login local transport input
ssh end R1#

ROUTER 2

R2#sh run

Building configuration...
Current configuration : 2077
bytes version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec service password-
encryption hostname R2
enable secret 5 1mERr$9cTjUIEqNGurQiFU.ZeCi1 enable password 7
0822455D0A16 no ip cef no ipv6 cef
username admin secret 5
1mERr$9cTjUIEqNGurQiFU.ZeCi1 ip ssh version 2
ip domain-name unad-
ccna.com spanning-tree
mode pvst
interface Loopback0 description Web
Server ip address 10.10.10.10
255.255.255.255
interface FastEthernet0/0 description
Enlace_ISP ip address 209.165.200.225
255.255.255.248
ip nat outside duplex auto speed
auto interface FastEthernet0/1 no ip
address duplex auto speed auto
shutdown interface Serial0/0/0 description Enlace a R3 bandwidth 128 ip address 172.31.23.1
255.255.255.252
ip ospf cost 7500 ip nat inside clock rate 64000
interface Serial0/0/1 description Enlace a R1 bandwidth
128 ip address 172.31.21.2 255.255.255.252
ip nat inside
interface Vlan1 no ip address
shutdown router ospf 1
router-id 2.2.2.2
log-adjacency-changes
passive-interface FastEthernet0/0 network 172.31.21.0 0.0.0.3 area 0
network 10.10.10.10 0.0.0.0 area 0
network 172.31.23.0 0.0.0.255 area 0

network 209.165.200.224 0.0.0.7 area 0
ip nat inside source list 10 interface FastEthernet0/0
overload ip classless
ip route 0.0.0.0 0.0.0.0 209.165.200.230
ip flow-export version 9
access-list 10 permit 172.31.21.0 0.0.0.3
access-list 10 permit 172.31.23.0 0.0.0.3
access-list 10 permit host 10.10.10.10
access-list 10 permit 192.168.30.0 0.0.0.255
access-list 10 permit 192.168.40.0 0.0.0.255
access-list 10 permit 192.168.200.0 0.0.0.255
access-list 10 permit 192.168.4.0 0.0.0.255
access-list 10 permit 192.168.5.0 0.0.0.255
access-list 10 permit 192.168.6.0
0.0.0.255 no cdp run
banner motd ^C Acceso solo a peronal aoturizado
^C line con 0
exec-timeout 5 0
password 7 0822455D0A16
login line aux 0
line vty 0 4 login local
transport input ssh line vty 5 15
login local transport input ssh end
ROUTER 3

R3#sh run

Building configuration...

Current configuration : 1615
bytes version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec service password-
encryption hostname R3
enable secret 5 1mERr$9cTjUIEqNGurQiFU.ZeCi1 enable password 7
0822455D0A16 no ip cef no ipv6 cef
username admin secret 5
1mERr$9cTjUIEqNGurQiFU.ZeCi1 ip ssh version 2
ip domain-name unad-
ccna.com spanning-tree
mode pvst interface
Loopback4
ip address 192.168.4.1 255.255.255.0
interface Loopback5
ip address 192.168.5.1 255.255.255.0
interface Loopback6

ip address 192.168.6.1 255.255.255.0
interface FastEthernet0/0 no ip
address duplex auto speed auto
shutdown interface FastEthernet0/1
no ip address duplex auto speed
auto shutdown interface Serial0/0/0
no ip address clock rate 2000000
shutdown
interface Serial0/0/1 description Enlace a R2 bandwidth
128 ip address 172.31.23.2 255.255.255.252
ip access-group 20 out
interface Vlan1 no ip address
shutdown router ospf 1
router-id 3.3.3.3
log-adjacency-changes
passive-interface FastEthernet0/0 network 172.31.23.0 0.0.0.3 area 0
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 ip classless
ip flow-export version 9
access-list 20 deny 192.168.6.0 0.0.0.255
access-list 20 permit host
0.0.0.0 no cdp run
banner motd ^C Acceso solo a personal autorizado
^C line con 0
exec-timeout 5 0
password 7
0822455D0A16 login
line aux 0
line vty 0 4 login local
transport input ssh line vty 5 15
login local transport input ssh end R3#

SWITCH 1

SW1#sh run

Building configuration...

Current configuration : 2521
bytes version 12.1
no service timestamps log datetime msec
no service timestamps debug datetime msec service password-
encryption hostname SW1
enable secret 5 1mERr$9cTjUIEqNGurQiFU.ZeCi1 enable password 7

0822455D0A16 ip ssh version 2
ip domain-name unad-ccna.com
username admin secret 5
1mERr$9cTjUIEqNGurQiFU.ZeCi1 spanning-tree mode
pvst
interface FastEthernet0/1 description PC VLAN 30 switchport access vlan 30 switchport mode access spanning-tree portfast
interface FastEthernet0/2 description Sin uso shutdown
interface FastEthernet0/3 description Enlace a SW3 switchport mode
trunk interface FastEthernet0/4 description Interfaces sin uso shutdown
interface FastEthernet0/5 description Interfaces sin uso shutdown
interface FastEthernet0/6
description Interfaces sin uso shutdown
interface FastEthernet0/7 description Interfaces sin uso shutdown interface FastEthernet0/8 description Interfaces sin uso shutdown interface FastEthernet0/9 description Interfaces sin uso shutdown
interface FastEthernet0/10 description Interfaces sin uso shutdown interface FastEthernet0/11 description Interfaces sin uso shutdown interface FastEthernet0/12 description Interfaces sin uso shutdown interface FastEthernet0/13 description Interfaces sin uso shutdown interface FastEthernet0/14 description Interfaces sin uso shutdown interface FastEthernet0/15 description Interfaces sin uso shutdown interface FastEthernet0/16 description Interfaces sin uso shutdown interface FastEthernet0/17 description Interfaces sin uso shutdown interface FastEthernet0/18 description Interfaces sin uso shutdown interface FastEthernet0/19 description Interfaces sin uso shutdown interface FastEthernet0/20 description Interfaces sin uso shutdown interface FastEthernet0/21
description Interfaces sin uso shutdown
interface FastEthernet0/22 description Interfaces sin uso shutdown
interface FastEthernet0/23 description Interfaces sin uso shutdown
interface FastEthernet0/24 description Enlace a R1 switchport mode
trunk interface Vlan1 no ip address shutdown
interface Vlan99 description
Management mac-address
00d0.5840.3901
ip address 192.168.99.2 255.255.255.0
ip default-gateway 192.168.99.1
banner motd ^C Acceso solo a personal autorizado
^C line con 0
password 7
0822455D0A16 login
exec-timeout 5 0

line vty 0 4 login local
transport input ssh line vty 5
15 login local transport input
ssh end
SW1#
SWITC
H 3
SW3#sh run

Building configuration...
Current configuration : 2458
bytes version 12.1
no service timestamps log datetime msec
no service timestamps debug datetime msec service password-
encryption hostname SW3
enable secret 5 1mERr$9cTjUIEqNGurQiFU.ZeCi1 enable password 7
0822455D0A16 ip ssh version 2
no ip domain-lookup
ip domain-name unad-ccna.com
username admin secret 5
1mERr$9cTjUIEqNGurQiFU.ZeCi1 spanning-tree mode
pvst
interface FastEthernet0/1 description PC VLAN 40 switchport access vlan 40 switchport
mode access spanning-tree portfast
interface FastEthernet0/2 description Puerto sin uso shutdown
interface FastEthernet0/3 description Enlace a SW1 switchport mode
trunk interface FastEthernet0/4 description Puerto Sin uso shutdown
interface FastEthernet0/5 description Puerto Sin uso
shutdown interface FastEthernet0/6 description Puerto Sin
uso shutdown
interface FastEthernet0/7 description Puerto Sin uso
shutdown interface FastEthernet0/8 description Puerto Sin
uso shutdown interface FastEthernet0/9 description Puerto
Sin uso shutdown interface FastEthernet0/10 description
Puerto Sin uso shutdown interface FastEthernet0/11
description Puerto Sin uso shutdown interface
FastEthernet0/12 description Puerto Sin uso shutdown
interface FastEthernet0/13
description Puerto Sin uso shutdown
interface FastEthernet0/14 description Puerto Sin uso
shutdown interface FastEthernet0/15 description Puerto Sin
uso shutdown interface FastEthernet0/16 description Puerto
Sin uso shutdown interface FastEthernet0/17 description
Puerto Sin uso shutdown interface FastEthernet0/18
description Puerto Sin uso shutdown interface
FastEthernet0/19 description Puerto Sin uso shutdown

interface FastEthernet0/20 description Puerto Sin uso shutdown interface FastEthernet0/21 description Puerto Sin uso shutdown interface FastEthernet0/22 description Puerto Sin uso shutdown interface FastEthernet0/23 description Puerto Sin uso shutdown interface FastEthernet0/24 description Puerto Sin uso shutdown interface Vlan1 no ip address shutdown
interface Vlan99 description
Management mac-address
0090.2b35.9401
ip address 192.168.99.3 255.255.255.0
ip default-gateway 192.168.99.1
banner motd ^C Acceso solo a personal autorizado
C line con 0 password 7 0822455D0A16 login exec-timeout 5 0
line vty 0 4 login local
transport input ssh line vty 5
15 login local transport input
ssh end

3. Escenario 2

3.1Descripción del escenario

En esta actividad, demostrará y reforzará su capacidad para implementar NAT, servidor de DHCP, RIPV2 y el routing entre VLAN, incluida la configuración de direcciones IP, las VLAN, los enlaces troncales y las subinterfaces. Todas las pruebas de alcance deben realizarse a través de ping únicamente

3.2 Direccionamiento asignado puertos y VLAN

A continuación, se relacionan los elementos mínimos de configuración que se deben tener en cuenta para el desarrollo de esta actividad.

Imagen32 Direccionamiento asignado escenario 2

El administrador	Interfaces	Dirección IP	Máscara de subred	Gateway predeterminado
ISP	S0/0/0	200.123.211.1	255.255.255.0	N/D
R1	Se0/0/0	200.123.211.2	255.255.255.0	N/D
	Se0/1/0	10.0.0.1	255.255.255.252	N/D
	Se0/1/1	10.0.0.5	255.255.255.252	N/D
R2	Fa0/0,100	192.168.20.1	255.255.255.0	N/D
	Fa0/0,200	192.168.21.1	255.255.255.0	N/D
	Se0/0/0	10.0.0.2	255.255.255.252	N/D
	Se0/0/1	10.0.0.9	255.255.255.252	N/D
R3	Fa0/0	192.168.30.1	255.255.255.0	N/D
		2001:db8:130::9C0:80F:301	/64	N/D
	Se0/0/0	10.0.0.6	255.255.255.252	N/D
	Se0/0/1	10.0.0.10	255.255.255.252	N/D
SW2	VLAN 100	N/D	N/D	N/D
	VLAN 200	N/D	N/D	N/D
SW3	VLAN1	N/D	N/D	N/D

PC20	NIC	DHCP	DHCP	DHCP
PC21	NIC	DHCP	DHCP	DHCP
PC30	NIC	DHCP	DHCP	DHCP
PC31	NIC	DHCP	DHCP	DHCP
Laptop20	NIC	DHCP	DHCP	DHCP
Laptop21	NIC	DHCP	DHCP	DHCP
Laptop30	NIC	DHCP	DHCP	DHCP
Laptop31	NIC	DHCP	DHCP	DHCP

Fuente Guía Packet Tracert Academy

Tabla 1 Asignación VLAN y Puertos fisicos

Dispositivo	VLAN	Nombre	Interfaz
SW2	100	LAPTOPS	Fa0/2-3
SW2	200	DESTOPS	Fa0/4-5
SW3	1	-	Todas las interfaces

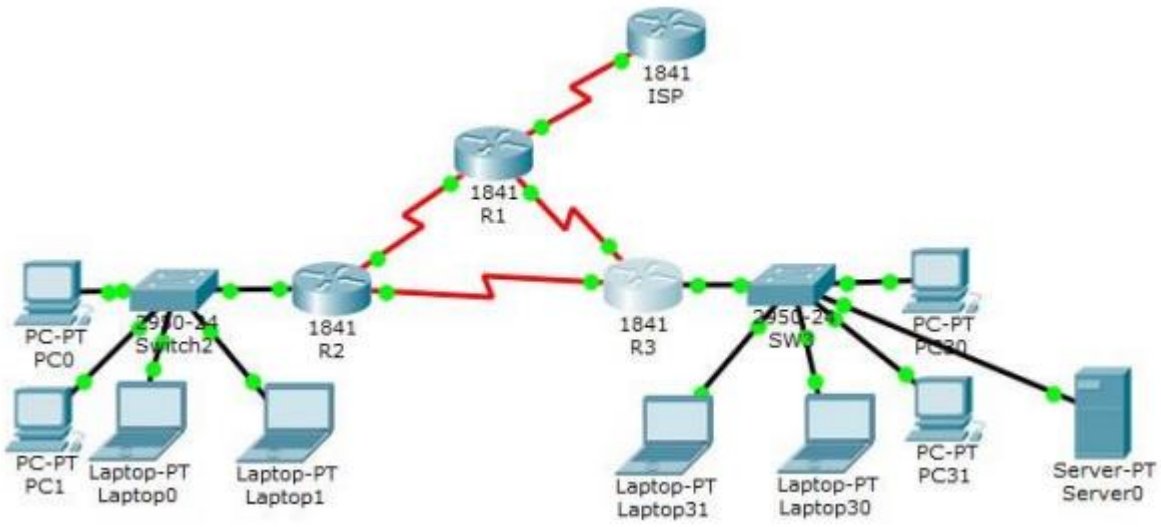
Fuente Guía Packet Tracert Academy

3.3Desarrollo de la Actividad Escenario 2

En este planteamiento se debe tener en cuenta la topología planteada por la guía de actividades, ya que en este se resalta el uso de un router de ISP, adicionalmente también se integran tres router adicionales, los cuales cuentan con una interconexión. En el siguiente nivel se configuraron dos Switch, los cuales se conectan a R2 y R3, a su vez dos equipos de cómputo (escritorio) y dos equipos portátiles. Esto como requerimiento mínimo para ahondar e identificar cada uno de los elementos que componen el sistema. El objetivo primordial es realizar el NAT (Network Address Traslation), partiendo de paramentros de seguridad como lo son las listas de acceso ACL, para tener las respectivas políticas a la hora de realizar las traducciones, es necesario para el buen funcionamiento aplicar el respectivo enrutamiento para alcanzar la salida a través del router de ISP.

3.4Topología

Imagen33 Topología Escenario 2



Fuente Guía Packet Tracert Academy

De acuerdo con los hitos establecidos en la guía de actividades, se realiza la asignación de puertos y configuración de VLAN, esto dando alcance a lo establecido en direccionamiento asignado para cada dispositivo. Adicionalmente, se procede a deshabilitar los puertos de red que no se están usando para el ejercicio.

Con la configuración que se relaciona a continuación, se procede a modificar el nombre de host, para cada uno de los equipos de red, se habilitan las interfaces de los Router, configuramos el direccionamiento y se deshabilitan las interfaces en los Sw que no se están utilizando, este último proceso por parte del endurecimiento de la red (Seguridad).

3.5Proceso de configuración

enable
configure terminal
host SW2
inter f0/1

```
switchport mode trunk
vlan 100
vlan 200
interface f0/2
switchport access vlan 100
switchport mode access
interface f0/3
switchport access vlan 100
switchport mode access
interface f0/4
switchport access vlan 200
switchport mode access
interfac f0/5
switchport access vlan 200
switchport mode access
inter range f0/6-24
shutdown
end
```

3.5.1 Configuración Router ISP

De acuerdo con los requerimientos establecidos para la configuración de este equipo, se procede a habilitar las interfaces y asignar el direccionamiento publico descrito

```
enable
configure terminal
hostname ISP
interface s0/0/0
ip addr 200.123.211.1 255.255.255.0
end
```

3.5.2 Configuración Routers R1, R2, R3

A continuación se relaciona la configuración realizada en el simulador para los equipo enrutadores, con el fin de garantizar las conexiones.

```
enable
configure terminal
host R1
```

```
interface s0/0/0
ip addr 200.123.211.2 255.255.255.0
no shut
inter s0/1/0
ip addr 10.0.0.1 255.255.255.252
no shut
inter s0/1/1
ip addr 10.0.0.5 255.255.255.252
no shut
end
```

R2

```
enable
configure terminal
host R2
interface f0/0
no shutdown
inter f0/0.100
encapsulation dot1Q 100
ip addr 192.168.20.1 255.255.255.0
interface f0/0.200
encapsulation dot1Q 200
ip address 192.168.21.1 255.255.255.0
inter s0/0/0
ip addr 10.0.0.2 255.255.255.252
no shutdown
inter Serial0/0/1
ip address 10.0.0.9 255.255.255.252
no shutdown
end
```

R3

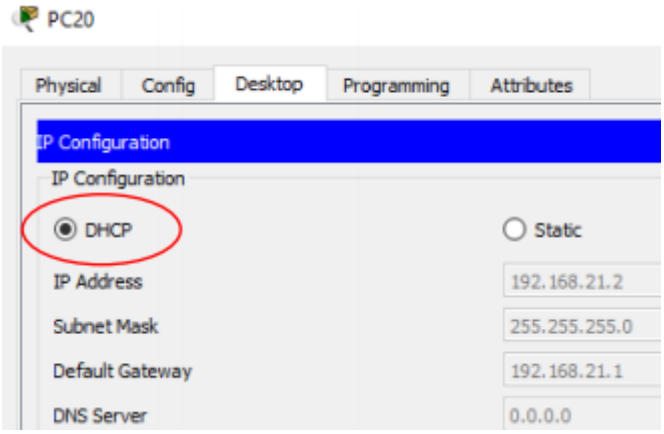
```
enable
configure terminal
host R3
inter f0/0
ip addr 192.168.30.1 255.255.255.0
ipv6 address 2001:DB8:130::9C0:80F:301/64
ipv6 enable
no shutdown
inter s0/0/0
ip addr 10.0.0.6 255.255.255.252
inter s0/0/1
```

ip addr 10.0.0.10 255.255.255.252
no shutdown
end

3.6Configuración DHCP en los HOST

De acuerdo a la descripción de las actividades, para este ítem se debe realizar la configuración DHCP en los equipos host, esto con el fin de que tomen el respectivo direccionamiento de router que se configuró para este fin.

Imagen34 Configuración DHCP



Fuente 2 Guía de trabajo Packet Tracert

Realizando el procedimiento sobre los equipos, se logra la conexión para el servicio DHCP, en la anterior imagen se observa la ip asignada por el router, garantizando la funcionalidad. Del mismo modo se realizó la activación del servicio en los demás equipos asociados a la topología.

3.7Configuración NAT

De acuerdo con la descripción este NAT, debe ser configurado bajo los siguientes lineamientos; NAT con sobrecarga sobre una dirección IPv4 pública. Asegúrese de

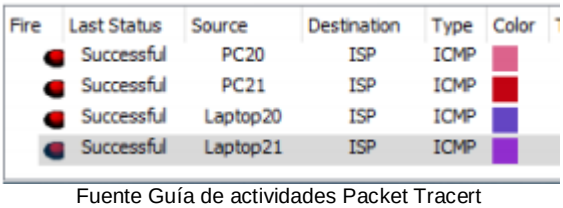
que todos los terminales pueden comunicarse con Internet pública (haga ping a la dirección ISP) y la lista de acceso estándar se llama INSIDE-DEVS

Configuración

```
enable
configure terminal
ip access-list standard INSIDE-DEVS
permit 192.168.0.0 0.0.255.255
ip nat inside source list INSIDE-DEVS inter s0/0/0 overload
inter s0/0/0
ip nat outside
inter s0/1/0
ip nat inside
inter s0/1/1
ip nat inside
end
```

Una vez culminada la ejecución de la configuración, se realizaron pruebas de conexión las cuales fueron exitosas, para esto se relaciona la imagen a continuación

Imagen35 Pruebas de conexión



Fuente Guía de actividades Packet Tracert

3.8 Configuración rutas estaticas en R1

Con base a la topología presentada, se debe configurar en R1 una ruta estatica predeterminada que envíe el trafico hacia R ISP, este ultimo incluye la ruta en el dominio RIPv2.

A continuación, observamos los comandos que se ejecutaron dentro del equipo virtual para configurar este enrutamiento.

```
enable
configure terminal
ip route 0.0.0.0 0.0.0.0 Serial0/0/0
end
```

En la anterior configuración se evidencia que el trafico desconocido es enviado por la interfaz serial, lo que garantiza que el trafico es entregado al R ISP

3.9 Configuración DHCP en R2

El equipo router 2 funciona en este escenario como un servidor DHCP para los dispositivos que se encuentran conectados a la interfaz Fasehternet0/0, a continuación se relaciona la configuración que se ejecutó en el equipo para que los pc, tomaran el direccionamiento de manera automática.

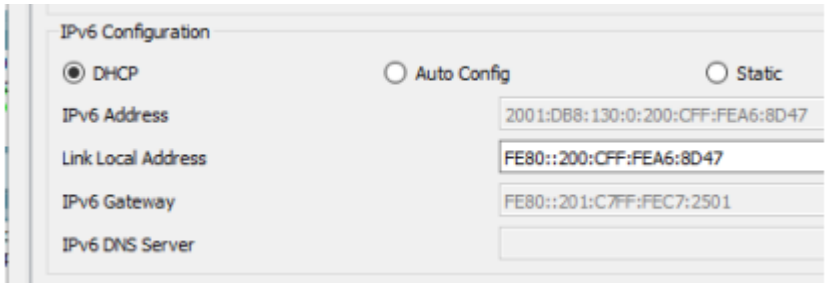
```
enable
configure terminal
ip dhcp pool vlan_100
network 192.168.20.0 255.255.255.0
default-router 192.168.20.1
ip dhcp pool vlan_200
network 192.168.21.0 255.255.255.0
default-router 192.168.21.1
end
```

3.10 Pruebas funcionales de conectividad

Basados en la descripción de las actividades, se establece que el servidor 0 es un servidor que solo maneja direccionamiento IPv6, por lo que solo debe estar accesible para los dispositivos que se encuentran configurados en R3.

En este ítem, se realiza un procedimiento similar al anterior, esto con el fin de habilitar el protocolo DHCP sobre el servidor.

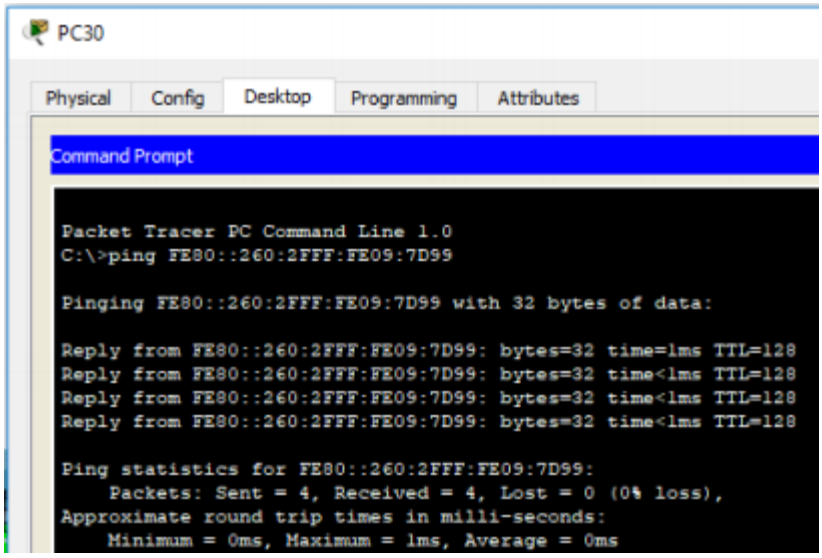
Imagen36 configuración DHCP V6



Fuente Packet Tracert

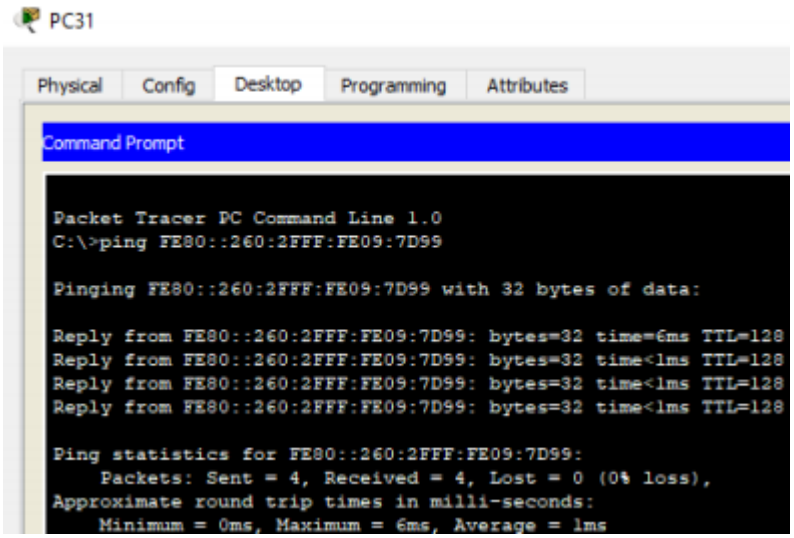
Una vez realizada la configuración anterior, se realizan pruebas de conexión para garantizar las configuraciones.

Imagen37 Conexión PC 30 a servidor 0



Fuente Packet Tracert

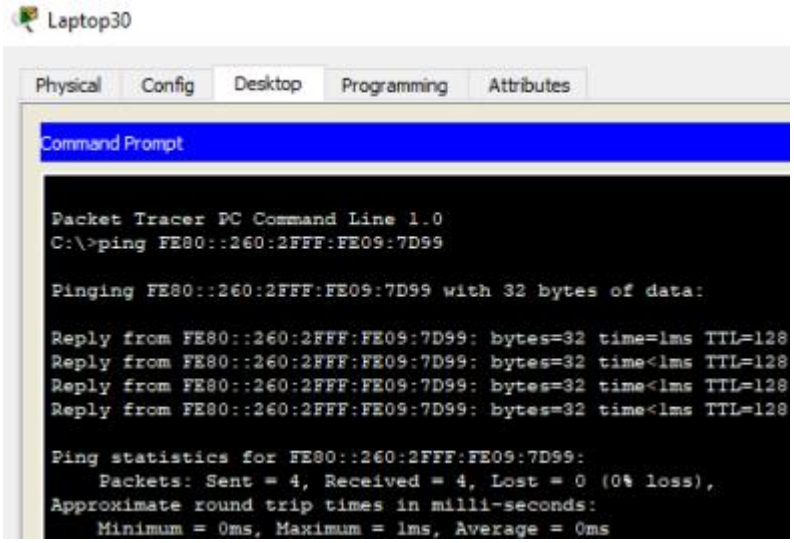
Imagen38 Conexión PC 31 a servidor 0



Fuente Packet Tracert

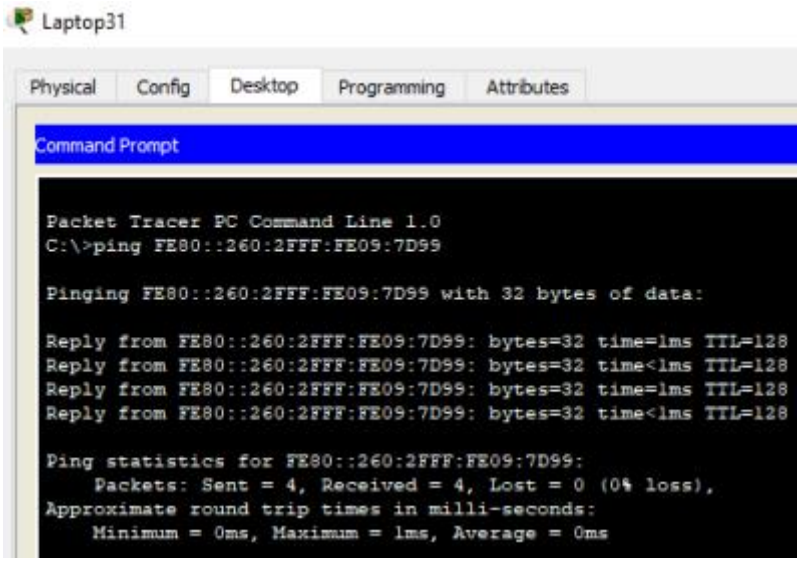
Ahora se relaciona las pruebas de conexión realizadas desde los equipos portátiles.

Imagen39 Conexión portátil 30 a servidor 0



Fuente Packet Tracert

Imagen40 Conexión portátil 31 a servidor 0

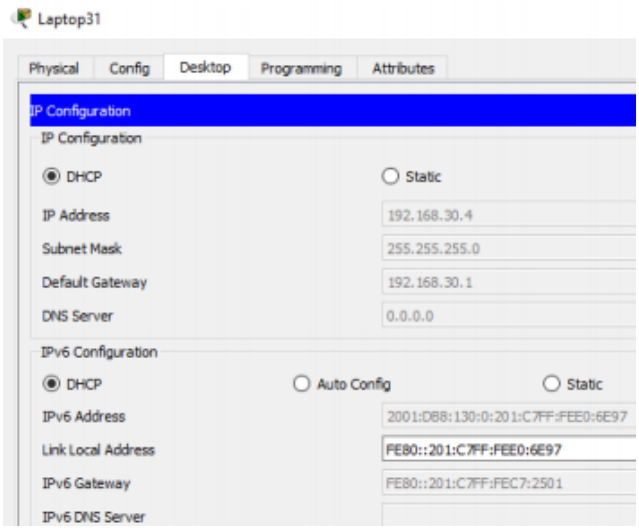


Fuente Packet Tracert

4. Configuración Laptop30, de Laptop31, de PC30 y PC31 (dual-stack)

En este caso, es necesario configurar las tarjetas de red, de los pc y los equipos portátiles, en doble pila, esto con el fin de que las estaciones soporten de manera simultanea la asignación de direcciones ip en V4 y en V6, esto como estrategia a usar en un manejo de migración de protocolo.

Imagen41 Configuración IPv6 portátil 31



Fuente 3 Packet Tracert

4.1Configuración FastEthernet 0/0 del R3 (dual- stack).

La descripción del escenario, solicita la configuración de una interfaz de R3, con el fin de que esta también cuente con una doble pila (ip en v4 e ip en v6), a continuación se relaciona el procedimiento que se llevo a cabo para lograr ese objetivo.

```
enable
configure terminal
ipv6 unicast-routing
ipv6 dhcp pool dhcpv6
prefix-delegation pool dhcpv6-pool1 lifetime 1800 600
exit
ipv6 local pool dhcpv6-pool1 2001:DB8:130::9C0:80F:301/40 48
inter f0/0
18
ip addr 192.168.30.1 255.255.255.0
ipv6 address 2001:DB8:130::9C0:80F:301/64
ipv6 enable
ipv6 dhcp server dhcpv6
end
```

4.2 Configuración RIPv2 R1, R2, R3

Los equipos activos R1, R2, R3, realizan intercambio de paquetes de enrutamiento a través de RIP en su versión 2, la manera mas eficiente de realizar este procesamiento entre los equipos es habilitando este protocolo con el fin de que la negociación se realice de manera automática y entre ellos se aprendan las rutas que deben intercambiar, tan solo declarando las redes que se publican a través de las diferentes interfaces.

R1:
enable
configure terminal
router rip
version 2
network 10.0.0.0
network 200.123.211.0
end

R2:
enable
configure terminal
router rip
version 2
network 10.0.0.0
network 192.168.20.0
network 192.168.21.0
network 200.123.211.0
end

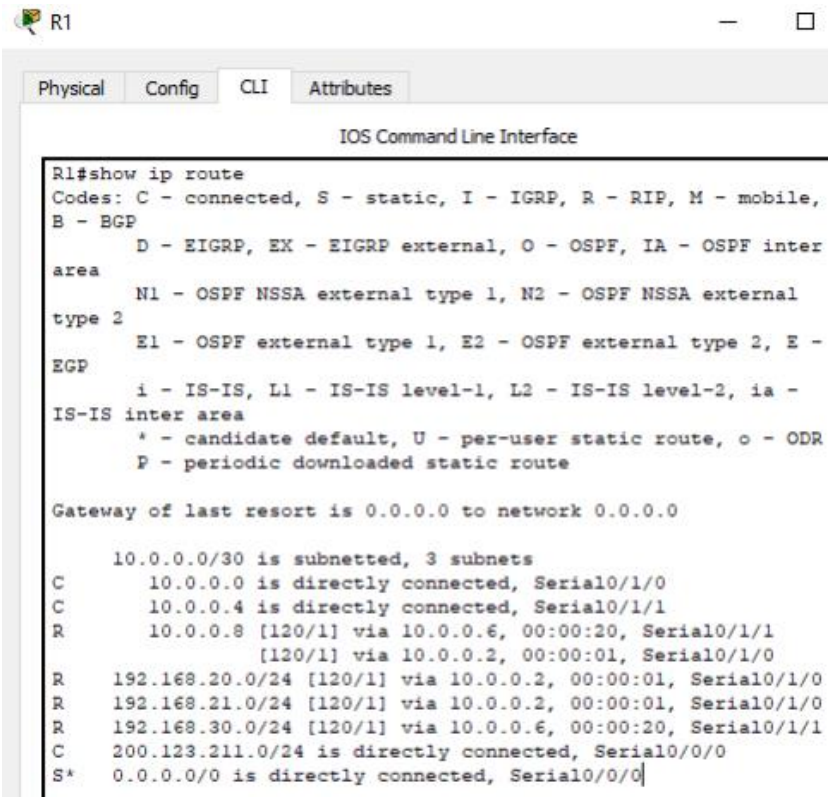
R3
enable
configure terminal
router rip
version 2
network 10.0.0.0
network 192.168.30.0
network 200.123.211.0
end

4.3Tablas de enrutamiento

R1, R2 y R3 deben saber sobre las rutas de cada uno y la ruta predeterminada desde R1.

Debido a que ya se realizó la configuración del protocolo en lo equipos, con el fin de que todo el enrutamiento se realizara a través del protocolo RIP versión 2, se procede a validar la configuración de las tablas de enrutamiento desde el Router 1, a continuación, se relaciona en la imagen, el resultado de consultar la tabla de enrutamiento sobre el equipo.

Imagen42 Tabla de enrutamiento

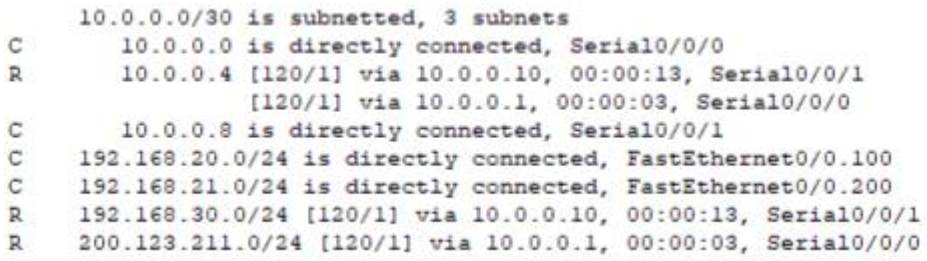


Fuente Packet Tracert

Analizando los resultados de la imagen, se evidencia la existencia de rutas con un carácter asociado, en estas encontramos el carácter C, lo que resulta de conectar una ruta directamente, si en cambio el carácter es R, podemos determinar que se

trata de una ruta obtenida por medio del protocolo RIP, y S es una ruta estática que se configuró de manera manual.

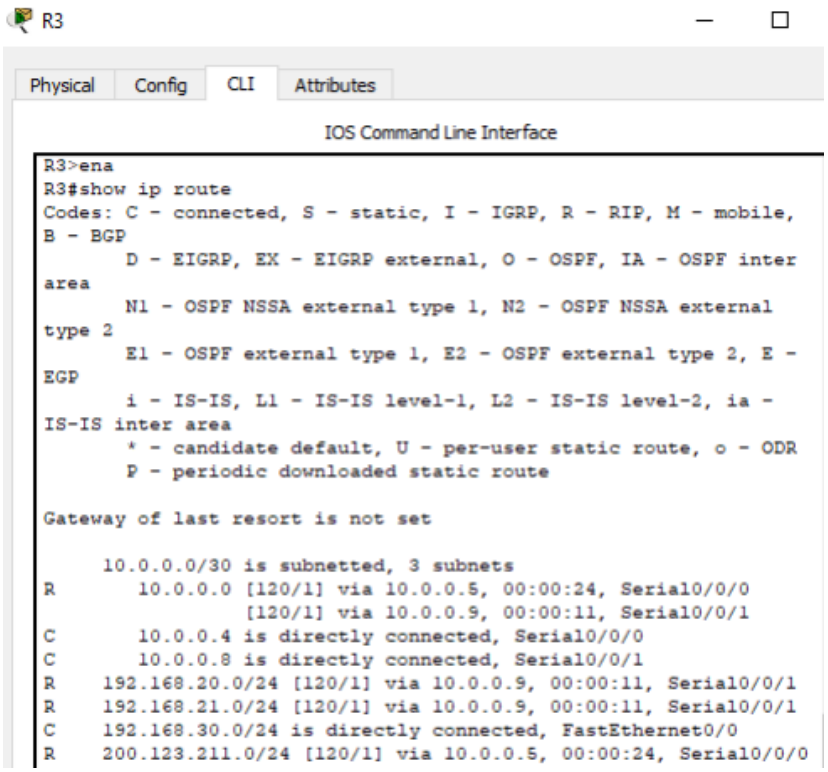
Imagen43 Enrutamiento R2



Fuente Packet Tracert

En el router 2 se ven las respectivas redes compartidas por protocolo o conectadas directamente, adicionalmente, se evidencia la sumarización que se realiza de las mismas 10.0.0.0/30.

Imagen44 Tabla de enrutamiento R3



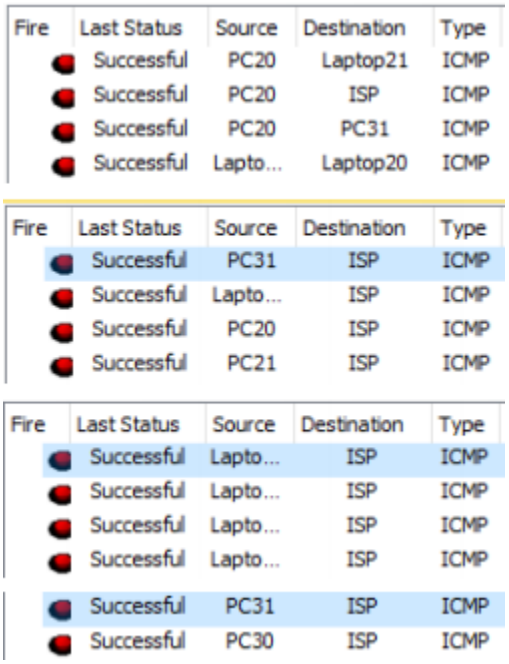
Fuente 4Packet Tracert

En la imagen anterior se evidencia la configuración de la tabla de enrutamiento con la que cuenta el Router 3, también se logra identificar la sumarización de las redes, así como las rutas que se aprenden por protocolo RIP y las que se encuentran conectadas directamente.

5. Pruebas de conexión

En este ítem se relaciona la evidencia de las pruebas de conexión entre todos los dispositivos de red, garantizando la conectividad con el router de ISP y las pruebas mediante ping, que se realizan tanto a ipv4, como a las ipv6.

Imagen45 Prueba conexión topología



Fire	Last Status	Source	Destination	Type
	Successful	PC20	Laptop21	ICMP
	Successful	PC20	ISP	ICMP
	Successful	PC20	PC31	ICMP
	Successful	Lapto...	Laptop20	ICMP

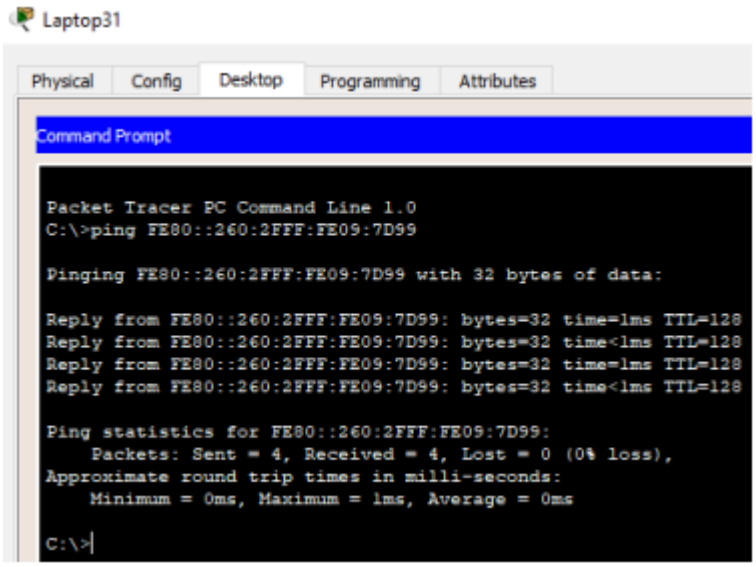
Fire	Last Status	Source	Destination	Type
	Successful	PC31	ISP	ICMP
	Successful	Lapto...	ISP	ICMP
	Successful	PC20	ISP	ICMP
	Successful	PC21	ISP	ICMP

Fire	Last Status	Source	Destination	Type
	Successful	Lapto...	ISP	ICMP
	Successful	Lapto...	ISP	ICMP
	Successful	Lapto...	ISP	ICMP
	Successful	Lapto...	ISP	ICMP
	Successful	PC31	ISP	ICMP
	Successful	PC30	ISP	ICMP

Fuente Packet Tracert

A través de la interfaz grafica de packet tracert se realizan las pruebas de conexión, estas evidentemente demuestran el éxito de la configuración. A continuación, se relacionan las pruebas relacionadas con Ipv6

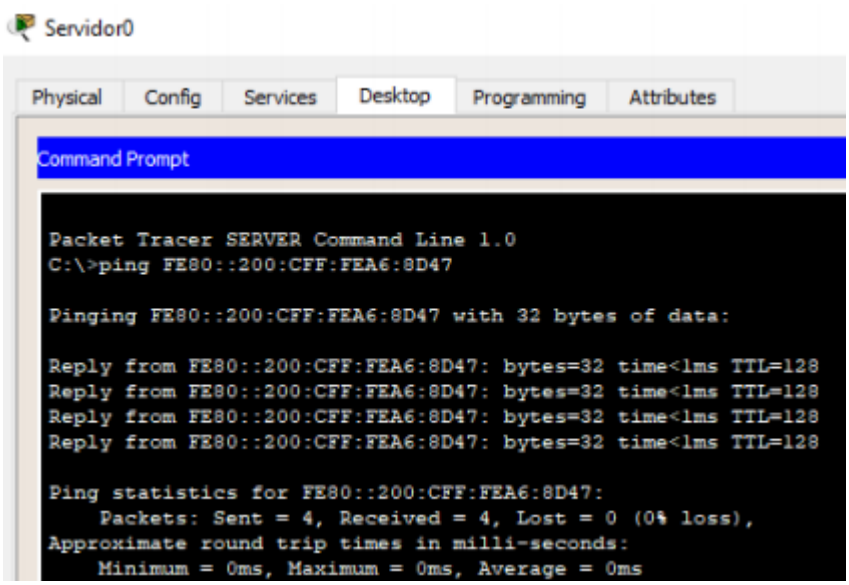
Imagen46Prueba portátil 31 a servido 0



Fuente Packet Tracert

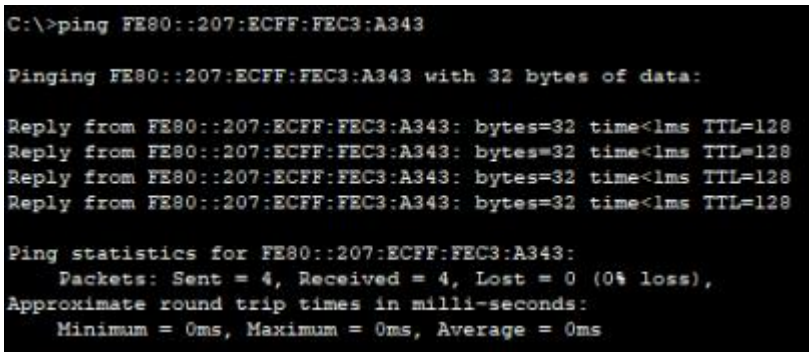
Ahora se relaciona las pruebas de conexión realizadas desde el servidor 0 hacia las estaciones.

Imagen47 Conexión desde servidor 0 a PC



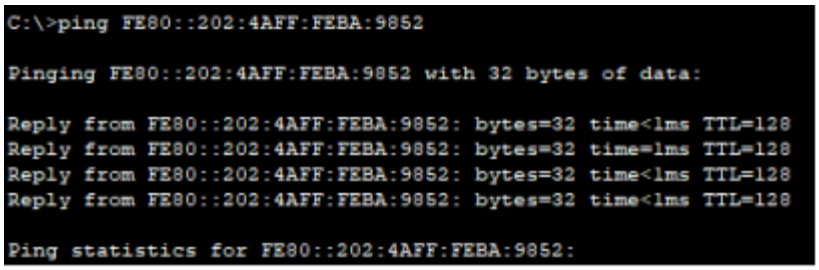
Fuente Packet Tracert

Imagen48 Desde servidor 0 a Pc



Fuente Packet Tracert

Imagen49 Desde servidor 0 a Pc



Fuente Packet Tracert

6. Conclusiones

Con la realización de la prueba de habilidades prácticas, se puso a prueba los conocimientos adquiridos durante el desarrollo del diplomado Cisco, adicionalmente se realizan estas con base a escenarios de la vida real, lo que permite tener la manera de plantear soluciones eficientes de acuerdo con los objetivos propuestos.

Se entendió los pasos básicos para la configuración de un dispositivo de red, en estos se debe hacer un aseguramiento del equipo con el fin de garantizar un mínimo de seguridad sobre el acceso a la red.

Se comprendió la importancia y la eficiencia que presta los protocolos de enrutamineto para la interacción entre redes remotas, esto permitió que se realice una conexión de manera más sencilla y que de manera practica se entienda los diversos factores que intervienen dentro de la negociación e intercambio de paquetes.

Con las practicas realizadas se refuerza y se logra adquirir nuevos conocimientos en el manejo de software de simulación, se logra crear, entender y configurar, tanto las topologías planteadas, así como los diversos equipos en los escenarios propuestos.

Se entendió el funcionamiento, el manejo y la configuración que se realiza entre el saliente protocolo IPv4 y el creciente protocolo IPv6. Se logro el objetivo de entender el funcionamiento del modelo de migración de estos protocolos, haciendo uso de la doble pila o doble stack.

7. Bibliografía

CISCO. (2014). Conceptos de Routing. Principios de Enrutamiento y Conmutación.

Recuperado de: https://static-courseassets.s3.amazonaws.com/RSE50ES/module4/index.html#4.0.1.1. (s.f.).

CISCO. (2014). Enrutamiento entre VLANs. Principios de Enrutamiento y

Conmutación. Recuperado de: https://static-courseassets.s3.amazonaws.com/RSE50ES/module5/index.html#5.0.1.1. (s.f.).

CISCO. (2014). Enrutamiento Estático. Principios de Enrutamiento y Conmutación.

Recuperado de: https://static-courseassets.s3.amazonaws.com/RSE50ES/module6/index.html#6.0.1.1. (s.f.).

CISCO. (2014). Introducción a redes conmutadas. Principios de Enrutamiento y

Conmutación. recuperado de https://static-course

assets.s3.amazonaws.com/RSE50ES/module1/index.html#1.0.1.1. (s.f.)