PRUEBA DE HABILIDADES PRÁCTICAS CCNA
SOLUCIÓN DE DOS ESTUDIOS DE CASO BAJO EL USO DE TECNOLOGÍA CISCO

PRESENTADO POR:
FREDDY EGDAMAR PÁEZ OLIVARES

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
INGENIERÍA DE SISTEMAS
CCAV PAMPLONA
22 DE MAYO DE 2020

PRUEBA DE HABILIDADES PRÁCTICAS CCNA
SOLUCIÓN DE DOS ESTUDIOS DE CASO BAJO EL USO DE TECNOLOGÍA CISCO

PRESENTADO POR:
FREDDY EGDAMAR PÁEZ OLIVARES

Trabajo presentado como opción de grado para obtener el título de INGENIERO DE SISTEMAS

TUTOR
JUAN CARLOS VESGA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
INGENIERÍA DE SISTEMAS
CCAV PAMPLONA
22 DE MAYO DE 2020

TABLA DE CONTENIDO

Pag

LISTA DE TABLAS

LISTA DE FIGURAS

INTRODUCCIÓN

Como ingenieros debemos mejorar nuestras competencias en el manejo de dispositivos que posibilitan la comunicación entre las diferentes redes que hacen parte de las empresas. Por ello en las prácticas propuestas para este diplomado en ccna, se profundizará en este aspecto con el uso de Packet Tracer y en la configuración de routers y swiches al cual podemos acceder de manera gratuita dado que la UNAD tiene convenio con la Academia CISCO que es la dueña de los derechos de este programa. Usted también lo puede descargar desde este link: https://www.itechtics.com/download-cisco-packet-tracer-7-1-free-direct-download-links/ La versión recomendada es la 7.1.

La evaluación denominada “Prueba de habilidades prácticas”, forma parte de las actividades evaluativas del Diplomado de Profundización CNA, y busca identificar el grado de desarrollo de competencias y habilidades que fueron adquiridas a lo largo del diplomado. Lo esencial es poner a prueba los niveles de comprensión y solución de problemas relacionados con diversos aspectos de Networking.

Para esta actividad, el estudiante dispone de cerca de dos semanas para realizar las tareas asignadas en cada uno de los dos (2) escenarios propuestos, acompañado de los respectivos procesos de documentación de la solución, correspondientes al registro de la configuración de cada uno de los dispositivos, la descripción detallada del paso a paso de cada una de las etapas realizadas durante su desarrollo, el registro de los procesos de verificación de conectividad mediante el uso de comandos ping, traceroute, show ip route, entre otros.

Teniendo en cuenta que la Prueba de habilidades está conformada por dos (2) escenarios, el estudiante deberá realizar el proceso de configuración de usando cualquiera de las siguientes herramientas: Packet Tracer o GNS3.

OBJETIVOS

OBJETIVO GENERAL

Examinar los contenidos propuestos en los ejercicios de habilidades prácticas del diplomado de ccna, apropiándose de los elementos más importantes que componen los fundamentos de configuraciones de routers y switches.

OBJETIVOS ESPECÍFICOS

Efectuar de modo individual cada uno de los ejercicios en los dos diferentes escenarios propuestos por el docente.

Demostrar como configurar redes de computadores de forma práctica.

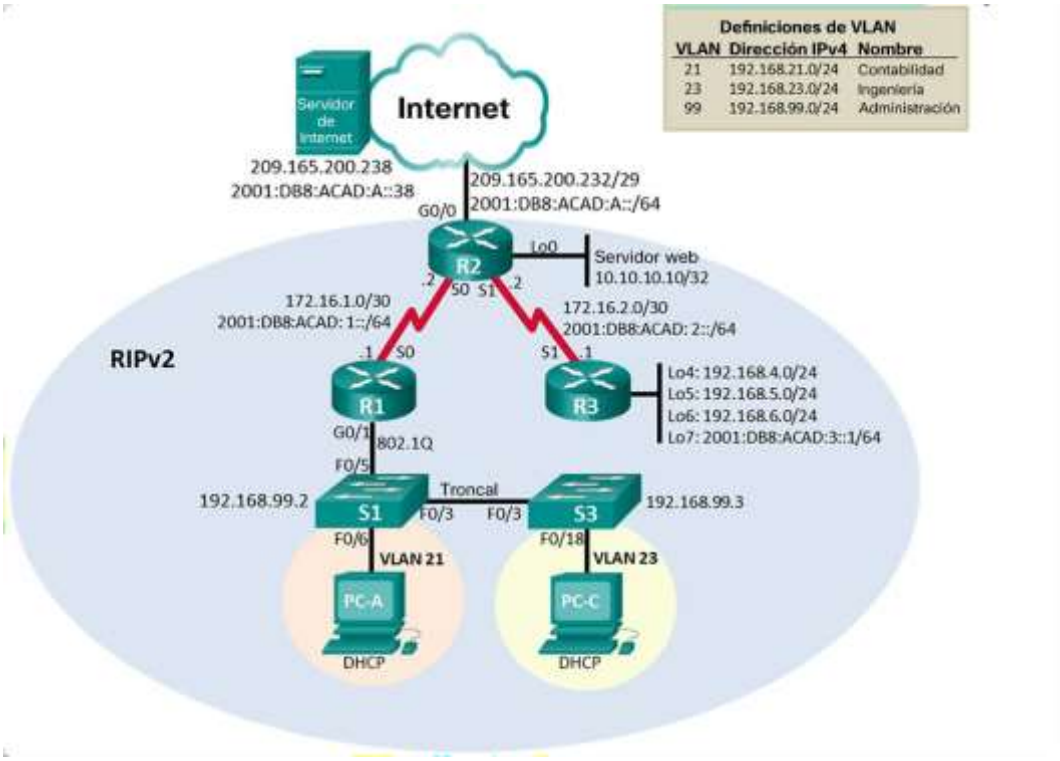
Exponer la herramienta Packet Tracer, para el posterior desarrollo de las experiencias en los escenarios propuestos.

1 ESCENARIO 1

Se debe configurar una red pequeña para que admita conectividad IPv4 e IPv6, seguridad de switches, routing entre VLAN, el protocolo de routing dinámico RIPv2, el protocolo de configuración de hosts dinámicos (DHCP), la traducción de direcciones de red dinámicas y estáticas (NAT), listas de control de acceso (ACL) y el protocolo de tiempo de red (NTP) servidor/cliente. Durante la evaluación, probará y registrará la red mediante los comandos comunes de CLI.

1.1 TOPOLOGÍA

Figura 1. Topología de red-01



Fuente: Suministrada por el ejercicio

2 PARTE 1. INICIALIZAR DISPOSITIVOS

2.1 PASO 1 INICIALIZAR Y VOLVER A CARGAR LOS ROUTERS Y LOS SWITCHES

Excluya las configuraciones de inicio y vuelva a cargar los dispositivos.

Solicitar al instructor que verifique la inicialización de los dispositivos.

Antes de realizar todas las configuraciones, se procede con inicializar todos los equipos.

1. Para eliminar cualquier archivo de configuración de inicio guardado en un router o switch se debe navegar al modo privilegiado y ejecutar el comando erase startup-config Switch#erase startup-config (enter) Router#erase startup-config (enter)

2. Ya en este punto cualquier configuración guardada queda eliminada, pero en el caso del switch, adicional, se debe ejecutar el comando delete vlan.dat desde el modo privilegiado, por si existe alguna información de vlan Switch#delete vlan.dat (enter)

3. Ahora solo queda mandar a cargar los equipos, tantos para los routers como los switches desde el modo privilegiado se ejecuta el comando reload Switch#reload (enter)

3 PARTE 2. CONFIGURAR LOS PARÁMETROS BÁSICOS DE LOS DISPOSITIVOS

3.1 PASO 1. CONFIGURAR LA COMPUTADORA DE INTERNET

a. Para R1, R2, R3, S1 y S3 se ingresa al modo de configuración global con el comando configure terminal desde el modo privilegiado y se ejecutan los siguientes comandos:

- Hostname, no ip domain-lookup, enable secret, service password-encryption, banner motd #mensaje# de la forma:
- Router>enable --para ingresar al modo EXEC privilegiado
- Router#configure terminal --para ingresar al modo de configuración global
- Router(config)#hostname R1 --cambia el nombre de Router a R1
- R1(config)#no ip domain-lookup --desactiva las búsquedas de DNS del IOS
- R1(config)#enable secret class --`protege el modo privilegiado con contraseña encriptada
- R1(config)#service password-encryption -- cifra todas las contraseña configuradas que estén sin cifrar (texto plano, ejemplo: consola, líneas vty, enable password)
- R1(config)#banner motd #Se prohíbe el acceso no autorizado# --muestra un mensaje en la terminal antes de intentar autenticarse al modo usuario de advertencia

b. El proceso anterior se repite de igual forma para R2, R3, S1 y S3 Proteger el modo usuario Routers y switches:

- R1(config)#line console 0 --para ingresar al modo de configuración de la línea de consola
- R1(config-line)#password cisco --configura una contraseña en el modo usuario
- R1 (config-line)#login --hace que el IOS pida una contraseña para autenticarse de forma local y así poder ingresar al modo usuario.
- R1(config-line) #exit –para salir del modo de línea.

c. Este proceso de protección del modo usuario se repite de igual forma solo para R3, S1 y S3. Para R2 será diferente porque en la parte 5 paso 2 se pide que se ingrese a R2 con nombre de usuario.

d. Proteger el modo usuario R2:

- R2(config)#line console 0 --para ingresar al modo de configuración de la línea de consola
- R2(config-line)#password cisco --configura una contraseña en el modo usuario
- R2(config-line)#login local --hace que el IOS pida un usuario y contraseña para autenticarse de forma local y así poder ingresar al modo usuario.
- R2(config-line)#exit

e. En este caso el comando password en la consola no es necesario ya que al ejecutar login local se pedirá un usuario y la contraseña de ese usuario creado en R2, la contraseña cisco configurada no servirá, solo se configuró con fines de precaución si en algún momento se decide cambiar la autenticación con usuario a solo contraseña y se olvide configurar una.
Proteger las líneas VTY R1 y R3s:

- R1(config)#line vty 0 4 --ingresa a las 5 líneas vty del router
- R1(config-line)#password cisco --configura una contraseña en el modo usuario
- R1(config-line)#login --hace que el IOS pida una contraseña para autenticarse de forma local y así poder ingresar de forma remota desde otro dispositivo
- R1(config-line)#exit --salir del modo de linea

f. Este proceso se repite de igual forma para R2 y R3

- Proteger las líneas VTY S1 y S3:
- S1(config)#line vty 0 15 --ingresa a las 16 líneas vty del switch
- S1(config-line)#password cisco --configura una contraseña en el modo usuario
- S1(config-line)#login --hace que el IOS pida una contraseña para autenticarse de forma local y así poder ingresar de forma remota desde otro dispositivo
- S1(config-line)#exit --salir del modo de línea

- Configurar las direcciones IPv4 e IPv6 a los equipos con sus rutas predeterminadas:

3.2 PASO 2. EN R1

Primero se habilita el routing IPv6 con el comando ipv6 unicast-routing en el modo de configuración global, lo que permite que el protocolo IPv6 funcione en el router

- R1(config)#ipv6 unicast-routing
- R1(config)#interface serial 0/0/0
- R1(config-if)#description ENLACE WAN A R2
- R1(config-if)#ip address 172.16.1.1 255.255.255.252
- R1(config-if)#ipv6 address 2001:DB8:ACAD:1::1/64
- R1(config-if)#ipv6 address FE80::1 link-local
- R1(config-if)#clock rate 128000
- R1(config-if)#no shutdown

Configuración de rutas predeterminadas: IPv4 e IPv6 desde el modo de configuración global

- R1(config)#ip route 0.0.0.0 0.0.0.0 serial 0/0/0
- R1(config)#ipv6 route ::/0 serial 0/0/0

3.3 PASO 3. EN R2

- R2(config)#ipv6 unicast-routing
- R2(config)#interface serial 0/0/0
- R2(config-if)#description ENLACE WAN A R1
- R2(config-if)#ip address 172.16.1.2 255.255.255.252
- R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64
- R2(config-if)#ipv6 address FE80::2 link-local
- R2(config-if)#no shutdown
- R2(config-if)#interface serial 0/0/1
- R2(config-if)#description ENLACE WAN A R3

- R2(config-if)#ip address 172.16.2.2 255.255.255.252
- R2(config-if)#ipv6 address 2001:DB8:ACAD:2::2/64
- R2(config-if)#ipv6 address FE80::2 link-local
- R2(config-if)#clock rate 128000
- R2(config-if)#no shutdown
- R2(config-if)#interface gigabitEthernet 0/0
- R2(config-if)#description ENLACE A INTERNET
- R2(config-if)#ip address 209.165.200.233 255.255.255.248
- R2(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64
- R2(config-if)#ipv6 address FE80::2 link-local
- R2(config-if)#no shutdown
- R2(config-if)#interface gigabitEthernet 0/1
- R2(config-if)#description ENLACE A DNS
- R2(config-if)#ip address 10.10.10.9 255.255.255.252
- R2(config-if)#ipv6 address 2001:DB8:ACAD:B::1/64
- R2(config-if)#ipv6 address FE80::2 link-local
- R2(config-if)#no shutdown

Configuración de rutas predeterminadas: IPv4 e IPv6 desde el modo de configuración global

- R2(config)#ip route 0.0.0.0 0.0.0.0 gibabitEthernet 0/0
- R2(config)#ipv6 route ::/0 gigabitEthernet 0/0

3.4 PASO 4. EN R3:

- R3(config-if)#interface serial 0/0/1
- R3(config-if)#description ENLACE WAN A R2
- R3(config-if)#ip address 172.16.2.1 255.255.255.252
- R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64
- R3(config-if)#ipv6 address FE80::3 link-local
- R3(config-if)#no shutdown
- R3(config-if)#interface loopback 4
- R3(config-if)#ip address 192.168.4.1 255.255.255.0
- R3(config-if)#interface loopback 5

- R3(config-if)#ip address 192.168.5.1 255.255.255.0
- R3(config-if)#interface loopback 6
- R3(config-if)#ip address 192.168.6.1 255.255.255.0
- R3(config-if)#interface loopback 7
- R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64

- Configuración de rutas predeterminadas: IPv4 e IPv6 desde el modo de configuración global
- R3(config)#ip route 0.0.0.0 0.0.0.0 serial 0/0/1
- R3(config)#ipv6 route ::/0 serial 0/0/1

3.5 PASO 7. RESULTADOS DE VERIFICACIÓN DE CONECTIVIDAD DE LA RED

Figura 2. Ping 172.16.1.2 de R1 a R2

```
R1#ping 172.16.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/15 ms
```

Fuente: Simulador Packet tracer.7.3.0

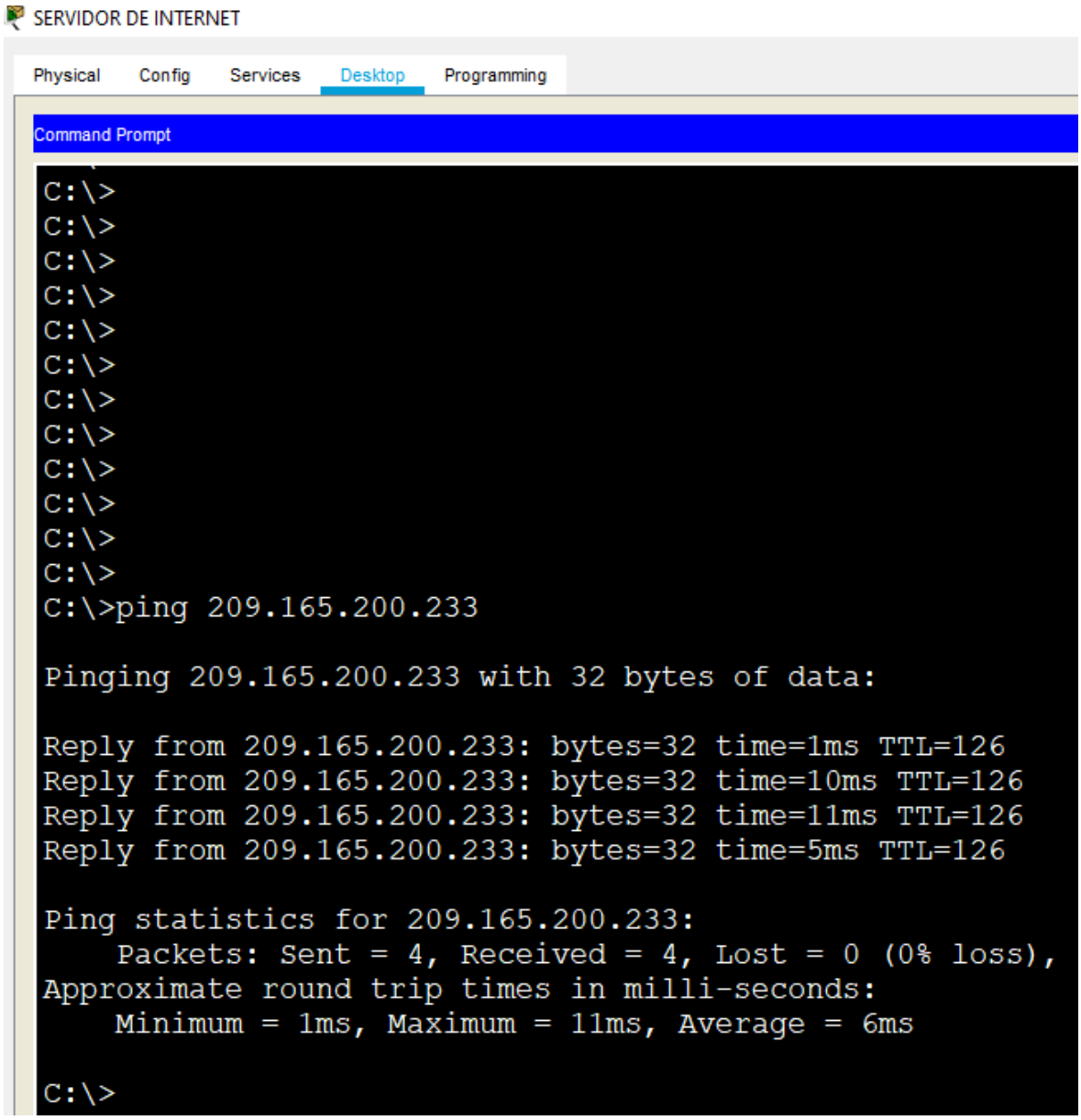
Figura 3. Ping 172.16.1.2 de R2 a R3

```
R2#ping 172.16.2.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/13 ms
```

Fuente: Simulador Packet tracer.7.3.0

Figura 4. PC de Internet a Puerta de Enlace Predeterminada



Fuente: Simulador Packet tracer.7.3.0

1) Para cumplir con este punto (conectividad de la red IPv4-IPv6) se debe evaluar toda la infraestructura y confirmar que todos los dispositivos, servicios… que se manejen en nuestra red soporten ambas versiones del protocolo IP, según sean los resultados se podrá tomar la decisión que mecanismo de transición sea conveniente y óptimo de implementar en la red (doble pila, túneles o traducción)… En esta topología se pudo implementar dual-stock (la recomendada) solo fue necesario la actualización del IOS en

los switches S1 y S2 con el comando show versión se obtiene la información de versión de IOS, S1 y S2 tenían LANBASE-M Version 12.2 (25) FX esta versión no soporta IPv6 y se actualizó a lanbasek9-mz.150-2.SE4.bin en el packet tracer se logra utilizando el servidor TFTP. ¿Cómo?

En ambos switches debemos configurar primero una SVI (interfaz virtual) para que se pueda comunicar con el servidor, en este caso ya el ejercicio pide una SVI 99 de administración, entonces se procede a configurar el paso

4 PARTE 3. LUEGO ACTUALIZAR EL IOS.

Para crear las VLANs se ingresa al modo de configuración global y se ejecuta el comando vlan *(ID de vlan)* y se le configura un nombre, luego se puede ir creando las demás vlan desde el mismo modo de configuración de vlan sin la necesidad de ejecutar el comando exit para regresar al modo de configuración global. Este mismo procedimiento se hace en S2.

- S1(config)#vlan 21
- S1(config-vlan)#name Contabilidad
- S1(config-vlan)#vlan 23
- S1(config-vlan)#name Ingeniería

Nota: este proceso se repite para S3

- S1(config-vlan)#vlan 99
- S1(config-vlan)#name Administración

Ya al tener configuradas las VLANs en ambos switches se procede a configurar la SVI (interfaz virtual) de administración para el acceso remoto de los switches y también permita conectar con el servidor TFTP para actualizar el IOS.

4.1 ASIGNAR LA DIRECCIÓN IP A LA SVI EN S1 Y S3

4.1.1 Para S1

- Desde el modo de configuración global ejecutar el comando interface vlan 99
  S1(config)#interface vlan 99 –se ingresa al modo de configuración de interfaz para la vlan99

  S1(config-if)#ip address 192.168.99.2 255.255.255.0 – se configura una dirección IPv4

4.1.2 Para S3

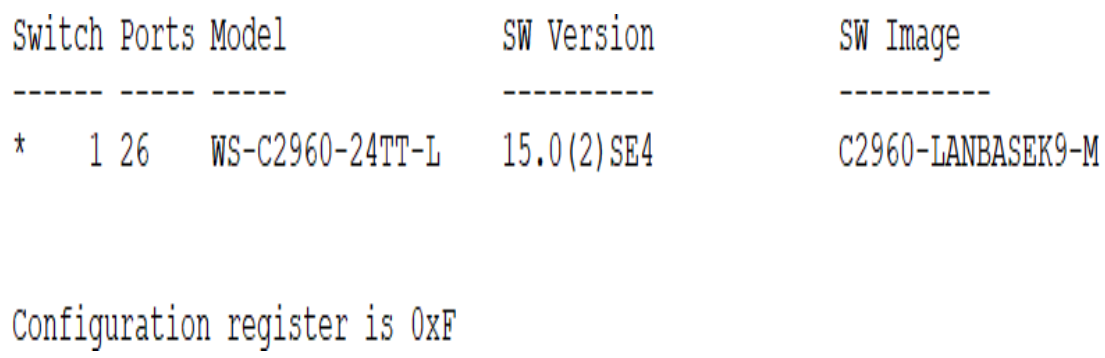
- Desde el modo de configuración global ejecutar el comando interface vlan 99
  S1(config)#interface vlan 99 –se ingresa al modo de configuración de interfaz para la vlan99

S1(config-if)#ip address 192.168.99.3 255.255.255.0 – se configura una dirección IPv4

4.1.3 Actualizar IOS:

- Luego, se conecta directamente a los switches un servidor, se activa el servicio TFTP y se busca en la lista de IOS la versión más actual de IOS para el switch 2960 (c2960-lanbasek9-mz.150-2.SE4.bin) y se copia con CTRL+C
- Seguidamente, se procede a configurar una dirección IPv4 al servidor dentro del rango de direcciones de la red de la VLAN 99 se le configuró la 192.168.99.254 con máscara de 24 bits y para el servidor conectado al S2 la 192.168.99.253 con máscara de 24 bits
- En cada switch desde el modo privilegiado se ejecuta el comando copy tftp: flash: (enter) donde pide colocar la dirección IP del dispositivo que tiene almacenado el IOS en este caso la IPv4 del servidor TFTP 192.168.99.254 se presiona enter y luego pide nombre de archivo de origen pegamos el IOS almacenado en TFTP: c2960-lanbasek9-mz.150-2.SE4.bin con CTRL+V luego (enter) si todo está bien aparece el símbolo de copiando!!!!!!!!!!!!!! Cuando termina el copiado de IOS se verifica que aparezca en la memoria flash con el comando
- dir flash: y aparece dos IOS, la versión antigua que es la que en este momento corre en la RAM y la recién copiada, ahora lo que se necesita es decirle al switch que cargue la versión más reciente y deje de trabajar con la anterior; para lograrlo se debe ir al modo de configuración global y ejecutar comando boot system y pegar la versión más reciente de IOS en S1 como S2 de la forma:
- S1(config)#boot system c2960-lanbasek9-mz.150-2.SE4.bin
- S3(config)#boot system c2960-lanbasek9-mz.150-2.SE4.bin

Figura 5. Configuración S3



Fuente: Simulador Packet tracer.7.3.0

En este punto, debemos activar la plantilla que soporta ambas versiones del protocolo IP ya que de forma predeterminada está activa la plantilla default que no tiene soporte IPv6, primero se debe reiniciar el switch con el comando reload para que cargue la nueva versión IOS y se confirma con el comando show version en el modo privilegiado.

Al momento de confirmar que la versión de IOS es la más reciente activamos la plantilla para soporte IPv4 e IPv6 con el comando sdm prefer dual-ipv4-and-ipv6 en el modo de configuración global (con esto, ya el equipo nos permite configurar una IPv6 en la SVI)

- S1(config)#sdm prefer dual-ipv4-and-ipv6
- S3(config)#sdm prefer dual-ipv4-and-ipv6

Aquí nuevamente el equipo nos pide un reinicio que lo hacemos con el comando reload. Al cargar nuevamente el IOS verificamos que la plantilla si se activó con el comando show sdm prefer

Figura 6. Show Sd en S1

```
S1#show sd
S1#show sdm p
S1#show sdm prefer
 The current template is "dual-ipv4-and-ipv6 default" template.
 The selected template optimizes the resources in
 the switch to support this level of features for
 0 routed interfaces and 1024 VLANs.

  number of unicast mac addresses:                  4K
  number of IPv4 IGMP groups + multicast routes:    0.25K
  number of IPv4 unicast routes:                    0
  number of IPv6 multicast groups:                  0.375k
  number of directly-connected IPv6 addresses:      0
  number of indirect IPv6 unicast routes:           0
  number of IPv4 policy based routing aces:         0
  number of IPv4/MAC qos aces:                      0.125K
  number of IPv4/MAC security aces:                 0.375K
  number of IPv6 policy based routing aces:         0
  number of IPv6 qos aces:                          0.625k
  number of IPv6 security aces:                     0.125K
```

Fuente: Simulador Packet tracer.7.3.0

Ahora se puede eliminar la versión de IOS antigua para liberar espacio del flash desde el modo privilegiado con el comando delete *c2960-lanbase-mz.122-25.FX.bin* y se puede verificar con el comando dir flash:

Figura 7. Dir Flash en S1

```
S1#dir flash:
Directory of flash:/

    1  -rw-     4414921          <no date>  c2960-lanbase-mz.122-25.FX.bin
    2  -rw-     4670455          <no date>  c2960-lanbasek9-mz.150-2.SE4.bin

64016384 bytes total (54931008 bytes free)
```

Fuente: Simulador Packet tracer.7.3.0

- Se elimina la versión más antigua
- S1#delete c2960-lanbase-mz.122-25.FX.bin

Nota: todo este proceso se hizo de igual forma en S3, ya aquí en la SVI de S1 como de S2 se puede configurar una dirección IPv6

4.1.4 Asignar el Gateway predeterminado a S1 y S3:

a. Esto permite acceder al switch desde otras subredes

- S1(config)#ip default-gateway 192.168.99.254
- S3(config)#ip default-gateway 192.168.99.254

b. Forzar los enlaces troncales a S1 y S3

- S3(config)#interface fastEthernet 0/3
- S3(config-if)#description ENLACE TRONCAL A S1
- S3(config-if)#switchport mode trunk
- S3(config-if)#switchport trunk allowed vlan 1,21,23,99
- S3(config-if)#switchport nonegotiate

c. Configurar Puerto de Acceso para la VLAN 23

- S3(config-if)#interface fastEthernet 0/18
- S3(config-if)# switchport mode access
- S3(config-if)#switchport access vlan 23

d. S1:

- S1(config)#interface fastEthernet 0/3
- S1(config-if)#description ENLACE TRONCAL A S3
- S1(config-if)#switchport mode trunk
- S1(config-if)#switchport trunk allowed vlan 1,21,23,99
- S1(config-if)#switchport nonegotiate
- S1(config-if)#interface fastEthernet 0/5
- S1(config-if)#description ENLACE TRONCAL A R1
- S1(config-if)#switchport mode trunk
- S1(config-if)#switchport trunk allowed vlan 1,21,23,99
- S1(config-if)#switchport nonegotiate

e. Configurar Puerto de Acceso para la VLAN 21

- S1(config-if)#interface fastEthernet 0/18
- S1(config-if)# switchport mode access
- S1(config-if)#switchport access vlan 21

4.1.5 Seguridad de switches:

Configurar todos los puertos sin utilizar como acceso y apagarlos

4.2 PASO 1. EN S1

- S1(config)#interface range fastEthernet 0/1-2, fastEthernet 0/4, fastEthernet 0/7-24
- S1(config-if)#switchport modo access
- S1(config-if)#shutdown
- S1(config-if)#interface range gigabitEthernet 0/1-2
- S1(config-if)#switchport modo access
- S1(config-if)#shutdown

4.3 PASO 2. EN S3

- S3(config)#interface range fastEthernet 0/1-2, fastEthernet 0/4-17, fastEthernet 0/19-24
- S3(config-if)#switchport modo access
- S3(config-if)#shutdown
- S3(config-if)#interface range gigabitEthernet 0/1-2
- S3(config-if)#switchport modo access
- S3(config-if)#shutdown

4.3.1 Para el enrutamiento de las VLAN

a. Se va a utilizar la técnica Router-On-A-Stick en R1 donde se van a crear subinterfaces que servirán de puerta de enlace predeterminada para las VLANs

b. Se ingresa al modo de configuración global y se comienza a configurar las subinterfaces para IPv4-IPv6

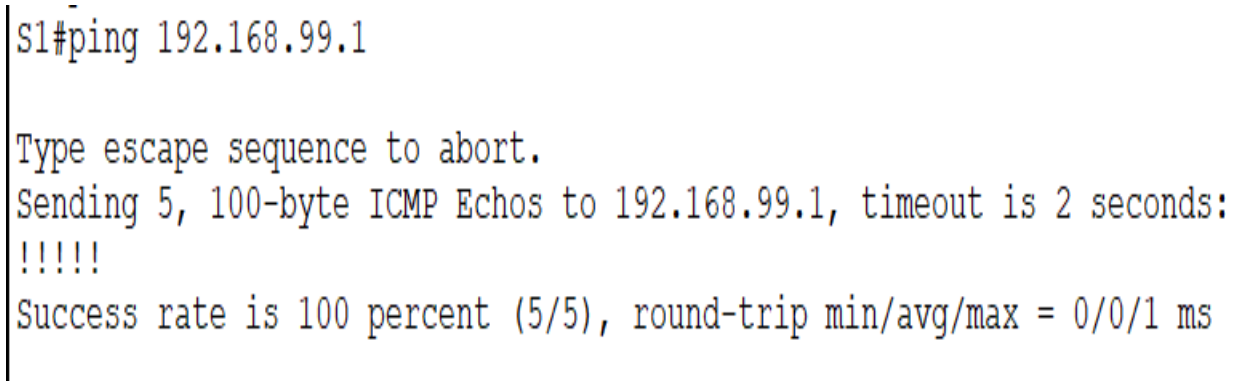
4.3.2 Paso 3. Configuración R1

- R1(config)#interface gigabitEthernet 0/1.21
- R1(config-if)#description LAN de Contabilidad
- R1(config-if)#encapsulation dot1Q 21
- R1(config-if)#ip address 192.168.21.1 255.255.255.0
- R1(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64
- R1(config-if)#ipv6 address FE80::1 link-local
- R1(config-if)#interface gigabitEthernet 0/1.23
- R1(config-if)#description LAN de Ingenieria
- R1(config-if)#encapsulation dot1Q 23
- R1(config-if)#ip address 192.168.23.1 255.255.255.0
- R1(config-if)#ipv6 address 2001:DB8:ACAD:4::1/64
- R1(config-if)#ipv6 address FE80::1 link-local
- R1(config-if)#interface gigabitEthernet 0/1.99
- R1(config-if)#description LAN de Administracion
- R1(config-if)#encapsulation dot1Q 99
- R1(config-if)#ip address 192.168.99.1 255.255.255.0
- R1(config-if)#ipv6 address 2001:DB8:ACAD:5::1/64
- R1(config-if)#ipv6 address FE80::1 link-local
- R1(config-if)#exit
- 4 Activar la interfaz gigabtiEthernet 0/1
- R1(config)#interface gigabitEthernet 0/1
- R1(config-if)#no shutdown

4.4 PASO-4 VERIFICAR LA CONECTIVIDAD DE LA RED

S1 A R1 DIRECCIÓN VLAN 99

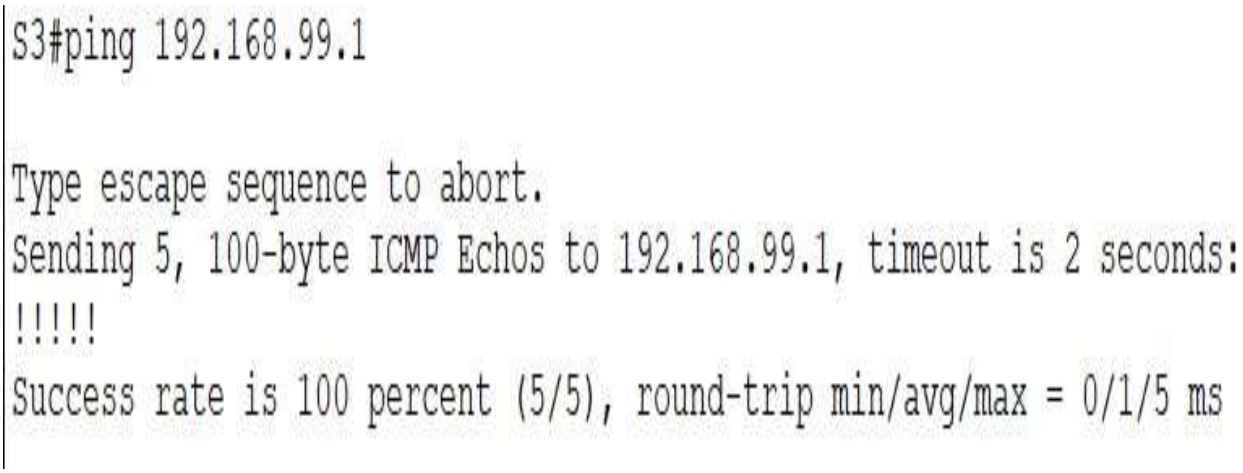
Figura 8. Ping de s1 a 192.168.99.1 en vlan 99



Fuente: Simulador Packet tracer.7.3.0

S3 a R1 dirección VLAN 99

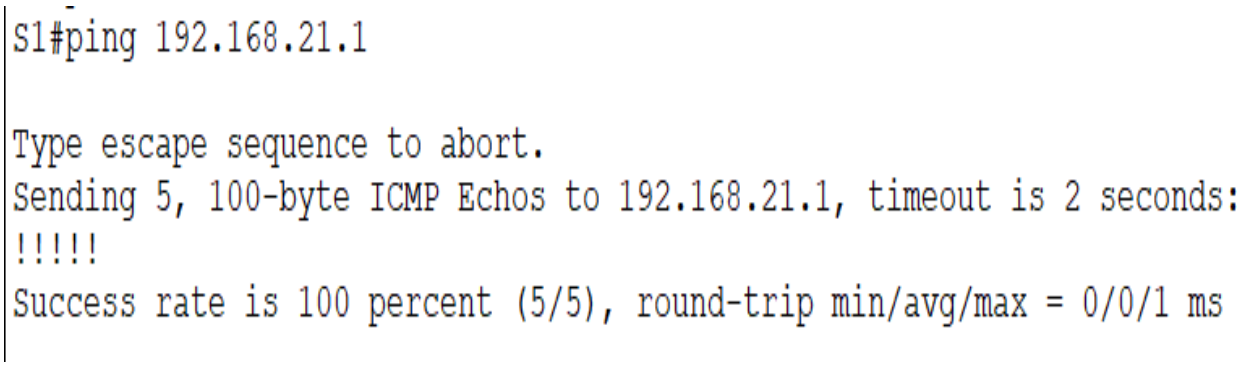
Figura 9. Ping de s3 a 192.168.99.1 en Vlan 99



Fuente: Simulador Packet tracer.7.3.0

S1 a R1 dirección VLAN 21

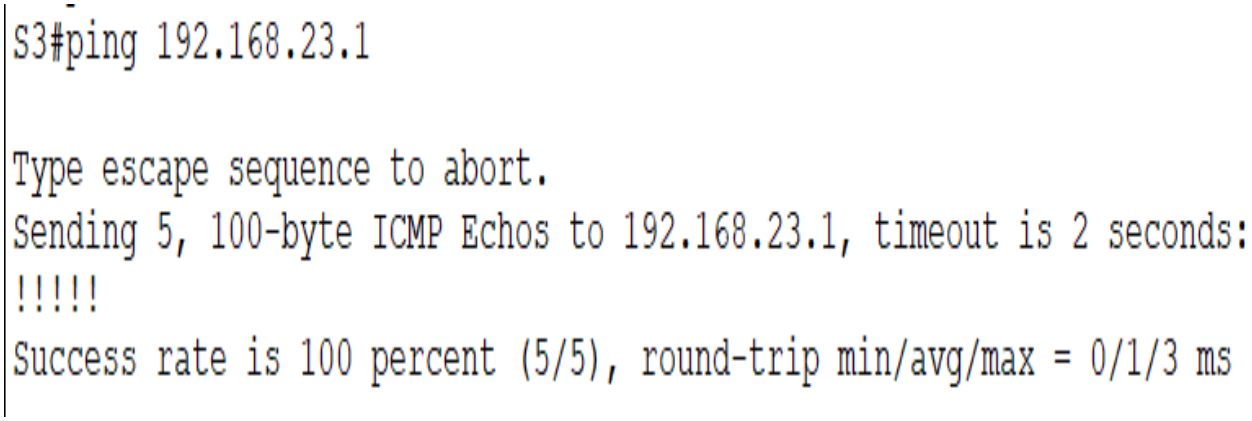
Figura 10. Ping de s1 a r1de dirección Vlan 21



Fuente: Simulador Packet tracer.7.3.0

S3 a R1 dirección VLAN 23

Figura 11. Ping de s3 a r1de dirección Vlan 2



Fuente: Simulador Packet tracer.7.3.0

5 PARTE 4. CONFIGURAR EL PROTOCOLO DE ROUTING DINÁMICO RIPV2

5.1 PASO 1. CONFIGURAR RIPV2

5.1.1 En R1

- R1(config)#router rip
- R1(config-router)#version 2
- R1(config-router)#network 172.16.1.0
- R1(config-router)#network 192.168.21.0
- R1(config-router)#network 192.168.23.0
- R1(config-router)#network 192.168.99.0
- R1(config-router)#passive-interface gigabitEthernet 0/1.21
- R1(config-router)#passive-interface gigabitEthernet 0/1.23
- R1(config-router)#passive-interface gigabitEthernet 0/1.99
- R1(config-router)#no auto-summary

IPv6 RIPng a diferencia de IPv4 en IPv6 se configura RIP para IPv6 (RIPng) en cada interfaz que se quiera publicar con este protocolo, donde se debe configurar un nombre para identificar el proceso de RIPng

- R1(config)#interface gigabitEthernet 0/1.21
- R1(config-if)#ipv6 rip RIPng enable
- R1(config-if)#interface gigabitEthernet 0/1.23
- R1(config-if)#ipv6 rip RIPng enable
- R1(config-if)#interface gigabitEthernet 0/1.99
- R1(config-if)#ipv6 rip RIPng enable
- R1(config-if)#interface serial 0/0/0
- R1(config-if)#ipv6 rip RIPng enable

5.2 PASO 2 EN R2:

- R2(config)#router rip
- R2(config-router)#version 2
- R2(config-router)#network 172.16.1.0
- R2(config-router)#network 172.16.2.0
- R2(config-router)#network 10.10.10.8
- R2(config-router)#passive-interface gigabitEthernet 0/0
- R2(config-router)#passive-interface gigabitEthernet 0/1
- R2(config-router)#no auto-summary

IPv6 RIPng:

- R2(config)#interface serial 0/0/0
- R2(config-if)#ipv6 rip RIPng enable
- R2(config-if)#interface serial 0/0/1
- R2(config-if)#ipv6 rip RIPng enable
- R2(config-if)#interface gigabitEthernet 0/1
- R2(config-if)#ipv6 rip RIPng enable

5.3 PASO 3. EN R3

- R3(config)#router rip
- R3(config-router)#version 2
- R3(config-router)#network 172.16.2.0
- R3(config-router)#network 192.168.4.0
- R3(config-router)#network 192.168.5.0
- R3(config-router)#network 192.168.6.0
- R3(config-router)#passive-interface loopback 4
- R3(config-router)#passive-interface loopback 5
- R3(config-router)#passive-interface loopback 6
- R3(config-router)#passive-interface loopback 7
- R3(config-router)#no auto-summary

5.4 IPV6 RIPNG

R3(config)#interface serial 0/0/1
R3(config-if)#ipv6 rip RIPng enable
R3(config-if)#interface loopback 7
R3(config-if)#ipv6 rip RIPng enable

5.5 PASO 4: VERIFICAR LA INFORMACIÓN DE RIP

a. ¿Con qué comando se muestran la ID del proceso RIP, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router?

Rta= show ip protocols

Nota: el protocol RIP no trabaja con ID de proceso, ni permite configurar un ID al router como otros protocolos como OSPF
R1#show ip protocols

Figura 12. R1#show ip protocols

```
R1#show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 20 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
Default version control: send version 2, receive 2
  Interface              Send  Recv  Triggered RIP  Key-chain
  Serial0/0/0            2     2
Automatic network summarization is not in effect
Maximum path: 4
Routing for Networks:
        172.16.0.0
        192.168.21.0
        192.168.23.0
        192.168.99.0
Passive Interface(s):
        GigabitEthernet0/1.21
        GigabitEthernet0/1.23
        GigabitEthernet0/1.99
Routing Information Sources:
        Gateway         Distance      Last Update
        172.16.1.2           120      00:00:19
Distance: (default is 120)
R1#
```

Fuente: Simulador Packet tracer.7.3.0

Figura 13. R2#show ip protocols

```
R2#show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 26 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
Default version control: send version 2, receive 2
  Interface              Send  Recv  Triggered RIP  Key-chain
  GigabitEthernet0/1     2     2
  Serial0/0/0            2     2
  Serial0/0/1            2     2
Automatic network summarization is not in effect
Maximum path: 4
Routing for Networks:
        10.0.0.0
        172.16.0.0
Passive Interface(s):
        GigabitEthernet0/0
Routing Information Sources:
        Gateway         Distance      Last Update
        172.16.2.1           120      00:00:02
        172.16.1.1           120      00:00:12
Distance: (default is 120)
R2#
```

Fuente: Simulador Packet tracer.7.3.0

Figura 14. r3#show ip protocols

```
R3#show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 1 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
Default version control: send version 2, receive 2
  Interface              Send  Recv  Triggered RIP  Key-chain
  Serial0/0/1            2     2
Automatic network summarization is not in effect
Maximum path: 4
Routing for Networks:
        172.16.0.0
        192.168.4.0
        192.168.5.0
        192.168.6.0
Passive Interface(s):
        Loopback4
        Loopback5
        Loopback6
        Loopback7
Routing Information Sources:
        Gateway         Distance      Last Update
        172.16.2.2           120      00:00:28
Distance: (default is 120)
```

Fuente: Simulador Packet tracer.7.3.0

b. ¿Qué comando muestra solo las rutas RIP?

Rta= show ip route rip

Figura 15. R1#show ip route rip

```
R1#show ip route rip
     10.0.0.0/30 is subnetted, 1 subnets
R       10.10.10.8 [120/1] via 172.16.1.2, 00:00:19, Serial0/0/0
     172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
R       172.16.2.0/30 [120/1] via 172.16.1.2, 00:00:19, Serial0/0/0
R    192.168.4.0/24 [120/2] via 172.16.1.2, 00:00:19, Serial0/0/0
R    192.168.5.0/24 [120/2] via 172.16.1.2, 00:00:19, Serial0/0/0
R    192.168.6.0/24 [120/2] via 172.16.1.2, 00:00:19, Serial0/0/0
     192.168.99.0/24 is variably subnetted, 2 subnets, 2 masks
```

Fuente: Simulador Packet tracer.7.3.0

Figura 16. r2#show ip route rip

```
R2#show ip route rip
     172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
R    192.168.4.0/24 [120/1] via 172.16.2.1, 00:00:25, Serial0/0/1
R    192.168.5.0/24 [120/1] via 172.16.2.1, 00:00:25, Serial0/0/1
R    192.168.6.0/24 [120/1] via 172.16.2.1, 00:00:25, Serial0/0/1
R    192.168.21.0/24 [120/1] via 172.16.1.1, 00:00:06, Serial0/0/0
R    192.168.23.0/24 [120/1] via 172.16.1.1, 00:00:06, Serial0/0/0
R    192.168.99.0/24 [120/1] via 172.16.1.1, 00:00:06, Serial0/0/0
     209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
```

Fuente: Simulador Packet tracer.7.3.0

Figura 17 . R3#show ip route rip

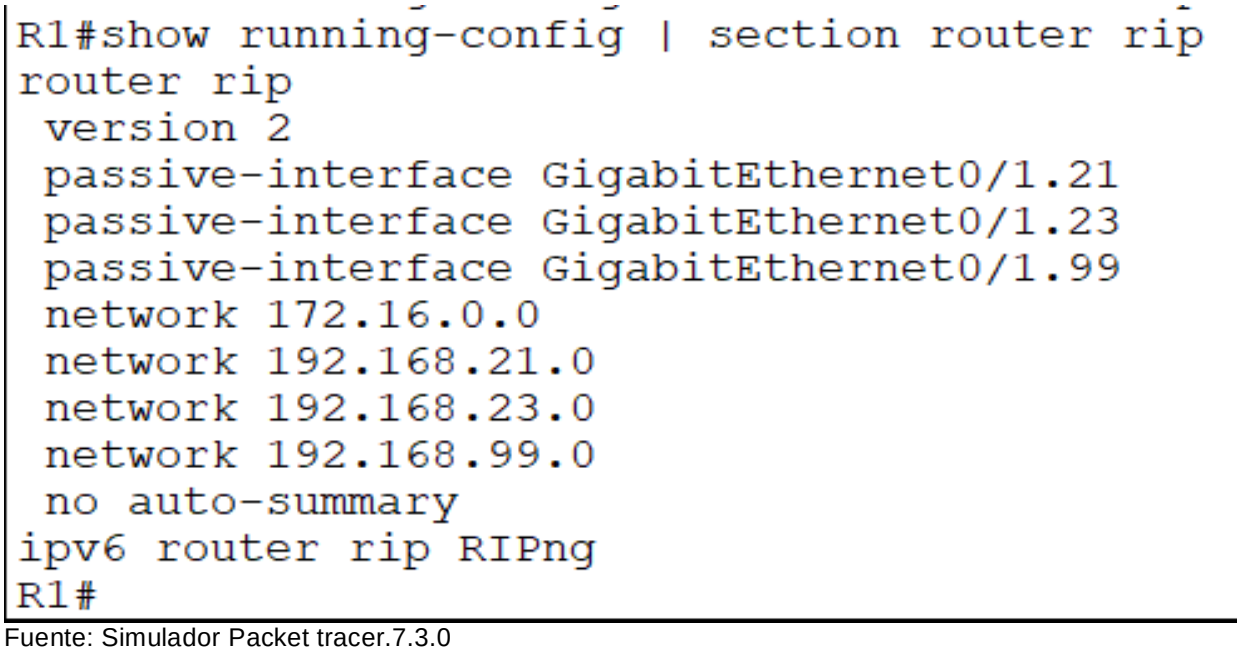
```
R3#show ip route rip
     10.0.0.0/30 is subnetted, 1 subnets
R       10.10.10.8 [120/1] via 172.16.2.2, 00:00:10, Serial0/0/1
     172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
R       172.16.1.0/30 [120/1] via 172.16.2.2, 00:00:10, Serial0/0/1
     192.168.6.0/24 is variably subnetted, 2 subnets, 2 masks
R    192.168.21.0/24 [120/2] via 172.16.2.2, 00:00:10, Serial0/0/1
R    192.168.23.0/24 [120/2] via 172.16.2.2, 00:00:10, Serial0/0/1
R    192.168.99.0/24 [120/2] via 172.16.2.2, 00:00:10, Serial0/0/1
R*   0.0.0.0/0 [120/1] via 172.16.2.2, 00:00:10, Serial0/0/1
```

Fuente: Simulador Packet tracer.7.3.0

c. ¿Qué comando muestra la sección de RIP de la configuración en ejecución?

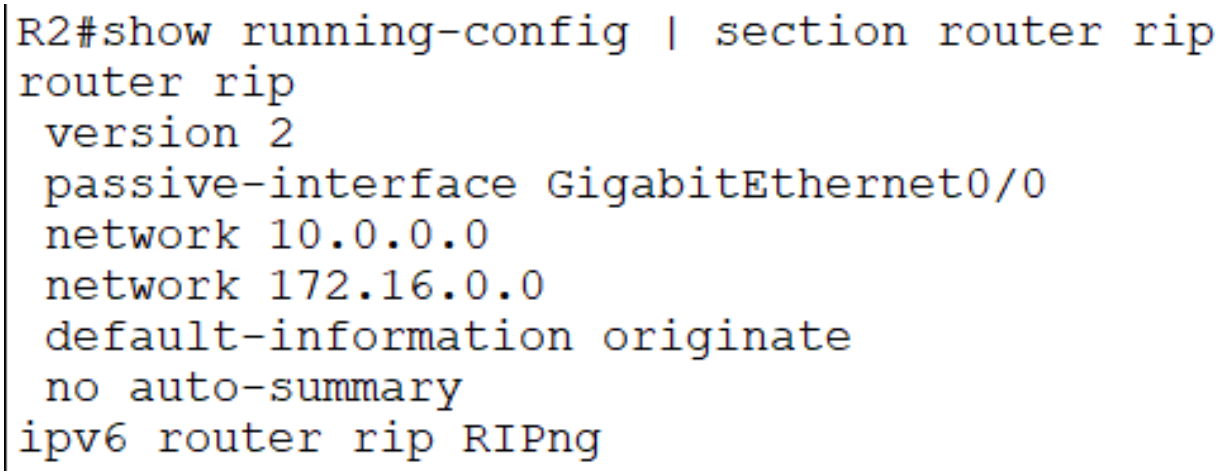
Rta= show running-config | section router rip
R1#show running-config | section router rip

Figura 18. r1#show running-config | section router rip



Fuente: Simulador Packet tracer.7.3.0

Figura 19. R2#show running-config | section router rip



Fuente: Simulador Packet tracer.7.3.0

Figura 20. R3#show running-config | section router rip

```
R3#show running-config | section router rip
router rip
 version 2
 passive-interface Loopback4
 passive-interface Loopback5
 passive-interface Loopback6
 passive-interface Loopback7
 network 172.16.0.0
 network 192.168.4.0
 network 192.168.5.0
 network 192.168.6.0
 no auto-summary
ipv6 router rip RIPng
```

Fuente: Simulador Packet tracer.7.3.0

6 PARTE 5. IMPLEMENTAR DHCP

6.1 PASO 1. CONFIGURAR EL R1 COMO SERVIDOR DE DHCP PARA LAS VLAN 21 Y 23

Se debe configurar un pool para cada VLAN asignándole un nombre al pool, utilizar la dirección de subred asignada a cada VLAN, configurar una dirección de Gateway predeterminado, dirección de DNS y un nombre de dominio. Adicional se pide excluir las primeras 20 direcciones para direccionamiento estático.

6.1.1 Para la VLAN 21

a. Primer paso: excluir las direcciones a reservar

- R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20

b. Segundo paso: crear el pool con un nombre

- R1(config)#ip dhcp pool ACCT

Tercer paso: asignar la dirección de subred con su máscara
R1(dhcp-config)#network 192.168.21.0 255.255.255.0
Cuarto paso: configurar la IP que recibirán los host de la VLAN 21 como gateway predeterminado
R1(dhcp-config)#default-router 192.168.21.1
Quinto paso: configurar la dirección de DNS que recibirán los host de la VLAN 21 para resolver los nombres de dominio.
R1(dhcp-config)#dns-server 10.10.10.10
Sexto paso: configurar un nombre de dominio para los host
R1(dhcp-config)#domain-name ccna-sa.com

6.1.2 Para la VLAN 23

a. Primer paso: excluir las direcciones a reservar

- R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.21.20

b. Segundo paso: crear el pool con un nombre

- R1(config)#ip dhcp pool ENGNR

c. Tercer paso: asignar la dirección de subred con su máscara

- R1(dhcp-config)#network 192.168.23.0 255.255.255.0

d. Cuarto paso: configurar la IP que recibirán los host de la VLAN 23 como gateway predeterminado

- R1(dhcp-config)#default-router 192.168.23.1

e. Quinto paso: configurar la dirección de DNS que recibirán los host de la VLAN 23 para resolver los nombres de dominio.

- R1(dhcp-config)#dns-server 10.10.10.10

f. Sexto paso: configurar un nombre de dominio para los host

- R1(dhcp-config)#domain-name ccna-sa.com

Servidor DHCP para IPv6: Se utilizó sin Estado, ¿Por qué sin estado? Porque el servidor no se encarga de asignar la parte de ID de interfaz a los host, no tiene control sobre el direccionamiento.

a. **Primer paso:** crear un pool con un nombre

- R1(config)#ipv6 dhcp pool DHCPv6_STATELESS
- Segundo paso: configurar una dirección de DNS en IPv6
- R1(config-dhcpv6)#dns-server 2001:DB8:ACAD:B::10
- Tercer paso: configurar un nombre de dominio para los host
- R1(config-dhcpv6)#domain-name ccna-sa.com

Ahora a cada subinterfaz en R1 se debe vincular al servidor DHCPv6 sin estado y cambiar el flag o indicador O del mensaje RA que envía el router a 1

R1(config)#interface gigabitEthernet 0/1.21
R1(config-if)#ipv6 dhcp server DHCPv6_STATELESS --vincula la subinterfaz al pool DHCPv6 sin estado
R1(config-if)#ipv6 nd other-config-flag --cambia el indicador O de cero a uno
R1(config)#interface gigabitEthernet 0/1.23
R1(config-if)#ipv6 dhcp server DHCPv6_STATELESS --vincula la subinterfaz al pool DHCPv6 sin estado
R1(config-if)#ipv6 nd other-config-flag --cambia el indicador O de cero a uno
R1(config)#interface gigabitEthernet 0/1.99
R1(config-if)#ipv6 dhcp server DHCPv6_STATELESS --vincula la subinterfaz al pool DHCPv6 sin estado
R1(config-if)#ipv6 nd other-config-flag --cambia el indicador O de cero a uno

6.2 PASO 2. CONFIGURAR NAT ESTÁTICO Y DINÁMICO

a. Estático: traduce de la forma 1:1, es decir, por cada dirección pública se vincula(mapea) a una privada.

- **Primer paso:** definir el tipo de NAT en este caso estático y vincular las direcciones R2(config)#ip nat inside source static 192.168.21.21 209.165.200.233

- **Segundo paso:** definir en las interfaces del router cuál será NAT de entrada y cuál de salida.

b. Entrada: llegan los paquetes de nuestro host interno (IP privada)
R2(config)#interface serial 0/0/0
R2(config-if)#ip nat inside

Salida: salen los paquetes al Internet (IP pública-la global interna)
R2(config)#interface gigabitEthernet 0/0
R2(config-if)#ipnat outside

c. NAT Dinámico: se debe configurar un pool de direcciones públicas asignadas por el ISP, que serán utilizadas por los host internos, si hay 5 direcciones IP públicas disponibles los primeros 5 host que intenten comunicarse con el exterior se les asignará un de estas IP.

- **Primer paso**: configurar el pool de direcciones públicas asignas por el ISP

  R2(config)#ip nat pool INTERNET 209.165.200.234 209.165.200.237 netmask 255.255.255.248

- **Segundo paso**: crear las ACL que permita la traducción a los hos de las subredes Contabilidad, Administración y la Loopback en R3, en este caso lo más cerca del destino
- (en R2)
- R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255
- R2(config)#access-list 1 remark PERMITE ACCESO A LA RED CONTABILIDAD
- R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255
- R2(config)#access-list 1 remark PERMITE ACCESO A LA RED INGENIERIA
- R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255
- R2(config)#access-list 1 remark PERMITE ACCESO A LA RED SUMARIZADA LOOPBACK

- **Tercer paso:** vincular la ACL con el pool creado

- R2(config)#ip nat inside source list 1 pool INTERNET

- **Cuarto paso:** definir las interfaces de entrada y salida

- R2(config)#interface serial 0/0/1 --para la subred sumarizada Loopback en R3

- R2(config-if)#ip nat inside

Nota: ya la serial 0/0/0 de R2 está definida como NAT inside R2(config)#interface gigabitEthernet 0/0 R2(config-if)#ip nat outside

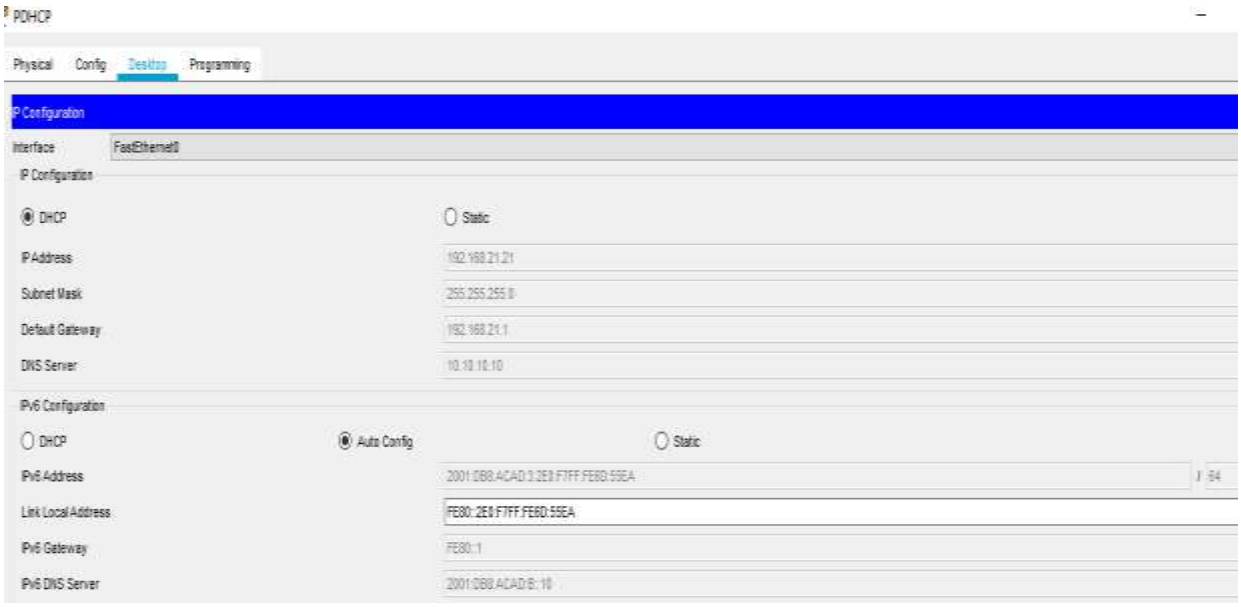
Nota: para calcular la subred sumarizada de las Loopback se deben convertir a sistema binario todas las subredes, comparar bit por bit hasta donde exista mayor coincidencia de izquierda a derecha

Lo4: 192.168.4.0= 11000000.10101000.00000100.00000000
Lo5:192.168.5.0= 11000000.10101000.00000101.00000000
Lo6:192.168.6.0= 11000000.10101000.00000110.00000000
La mayor coincidencia se da hasta los 22 bits, por lo tanto, la red sumarizada será 11000000.10101000.00000100 = 192.168.4.0/22

6.3 PASO 3. VERIFICAR EL PROTOCOLO DHCP

PC-A

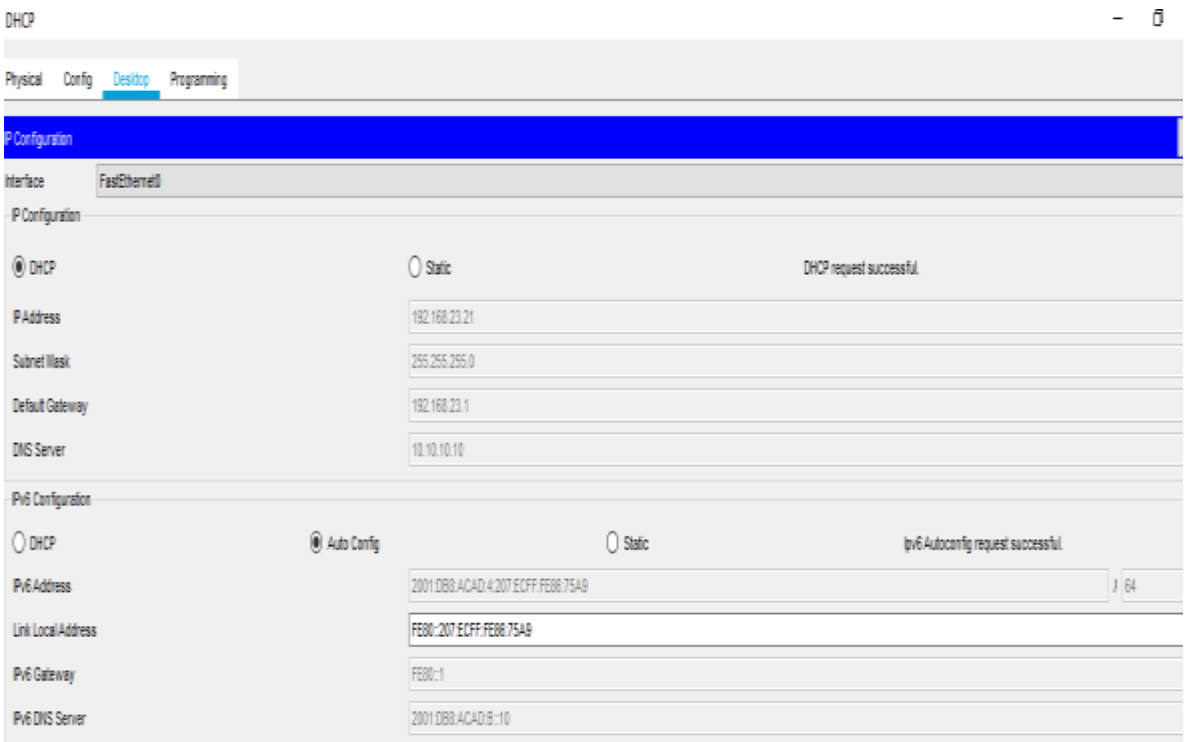
Figura 21. Verificar el protocolo DHCP EN PCA



Fuente: Simulador Packet tracer.7.3.0

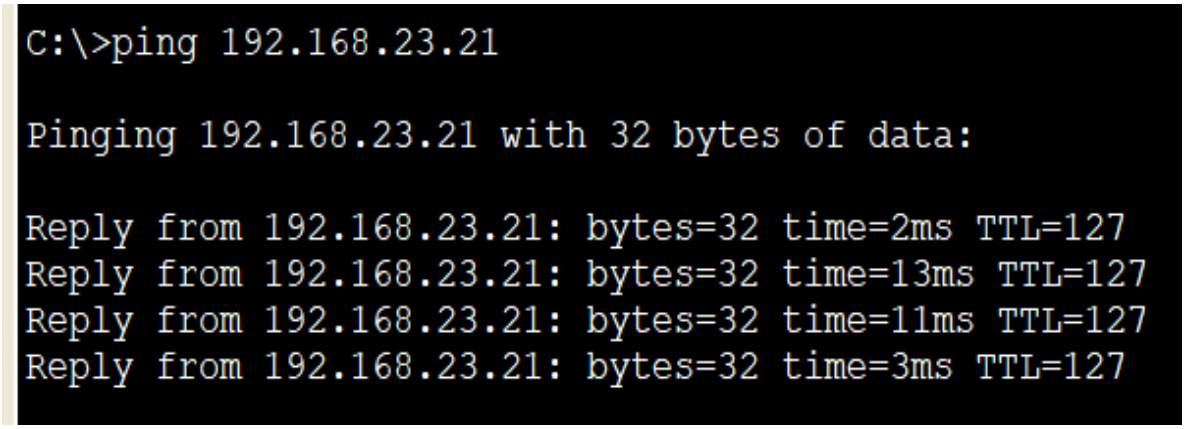
PC-B

Figura 22. Verificar el protocolo dhcp en PC-B



Fuente: Simulador Packet tracer.7.3.0

Figura 23. Ping de PC-A a PC-B



Fuente: Simulador Packet tracer.7.3.0

R2#clock set 09:00:00 5 March 2016

- Configure R2 como un maestro NTP con nivel de estrato: 5

R2(config)#ntp master 5

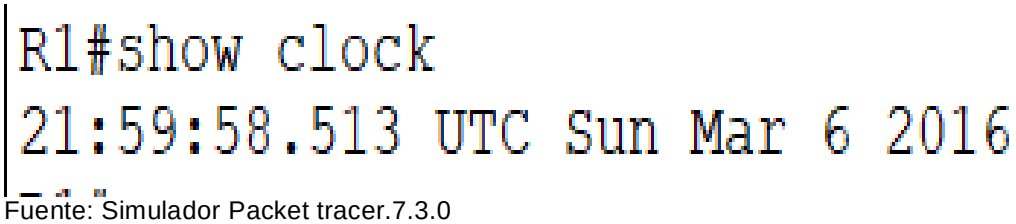
- Configuro una llave de intercambio entre los dispositivos NTP
- R2(config)#ntp trusted-key 20
- Configurar R1 como un cliente NTP.
- R1(config)#ntp server 172.16.1.2 --se coloca la dirección IP del NTP master, en este caso R2
- R1(config)#ntp trusted-key 20
- Configure R1 para actualizaciones de calendario periódicas con hora NTP.
- R1(config)#ntp update-calendar
- Verifique la configuración de NTP en R1.

Figura 24. Configuración en r1# show ntp status

```
R1#show ntp status
Clock is synchronized, stratum 6, reference is 172.16.1.2
nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision is 2**24
reference time is DA623C65.000002EA (21:57:57.746 UTC Sun Mar 6 2016)
clock offset is 3.00 msec, root delay is 28.00 msec
root dispersion is 10.72 msec, peer dispersion is 0.12 msec.
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is - 0.000001193 s/s system poll interval is 4, last
update was 10 sec ago.
```

Fuente: Simulador Packet tracer.7.3.0

Figura 25. Configuración en r1# show clock



Fuente: Simulador Packet tracer.7.3.0

a. Configurar y verificar ACL

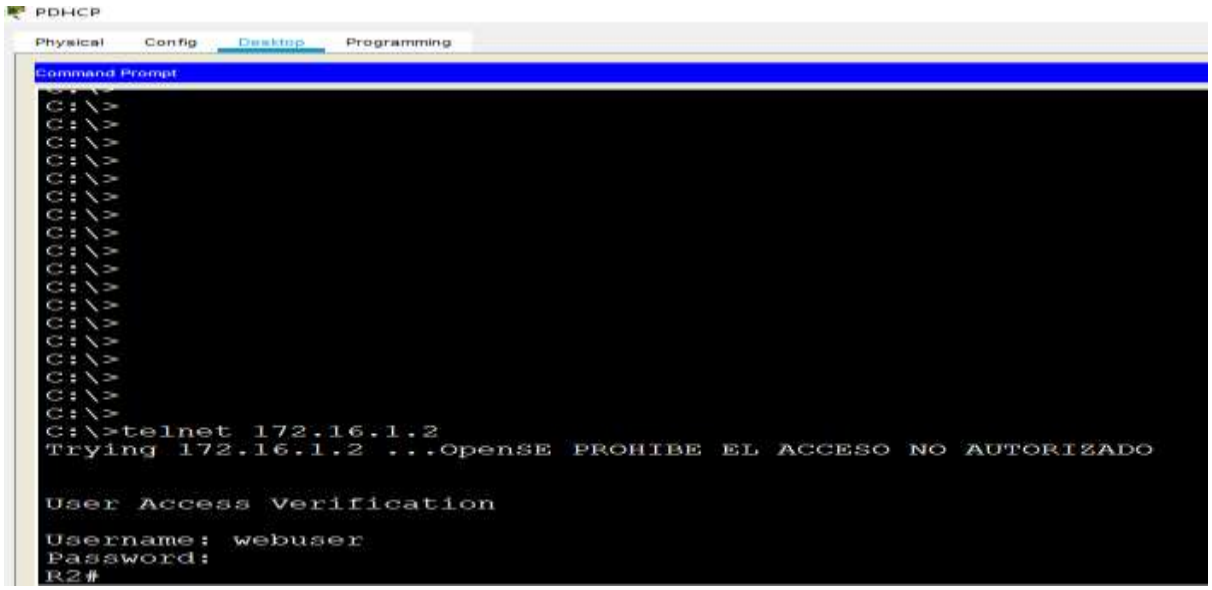
- Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2
- R2(config)#ip access-list standard ADMIN-MGT --Creo la ACL estándar con nombre
- R2(config-std-nacl)#remark PERMITE SOLO ACCESO TELNET A R1 --comentario
- R2(config-std-nacl)#permit 192.168.21.0 0.0.0.255 --permite a la VLAN21
- R2(config-std-nacl)#permit 192.168.23.0 0.0.0.255 --permite a la VLAN23
- R2(config-std-nacl)#permit 192.168.99.0 0.0.0.255 --permite a la VLAN99

b. Aplicar la ACL con nombre a las líneas VTY

- R2(config)#line vty 0 4
- R2(config-line)#access-class ADMIN-MGT in

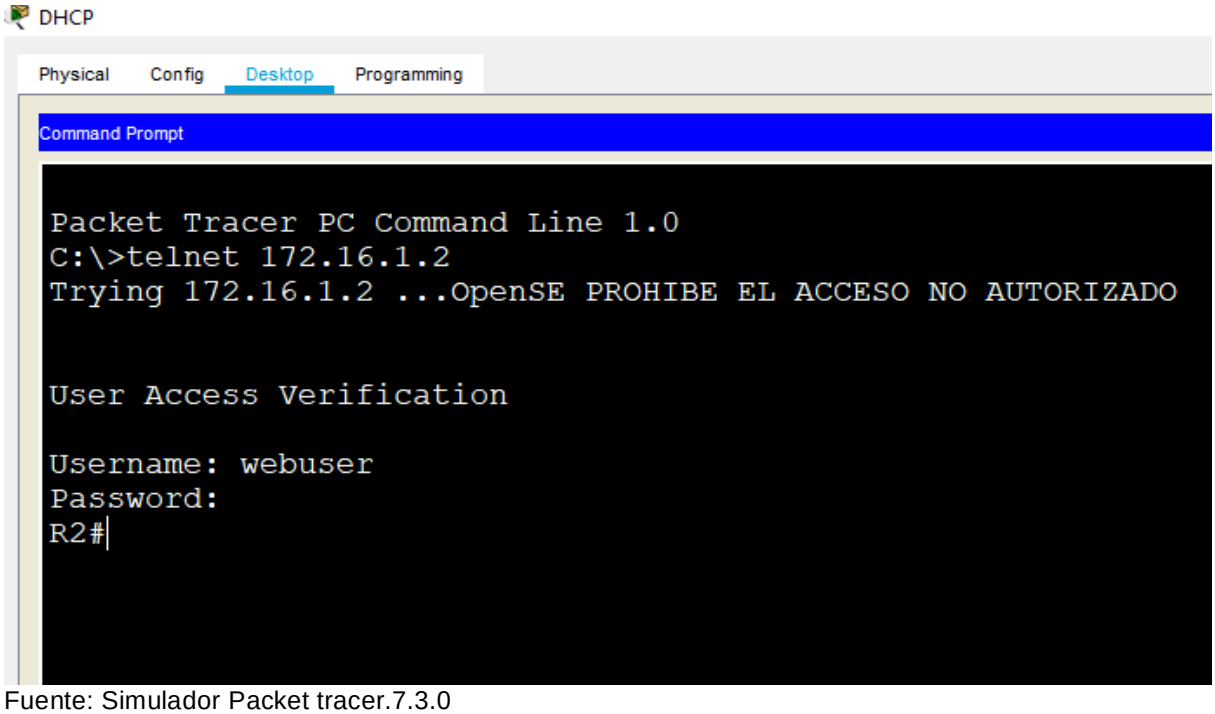
c. Verificar que la ACL funcione como se espera

Figura 26. Probando con una pc de la subred de contabilidad



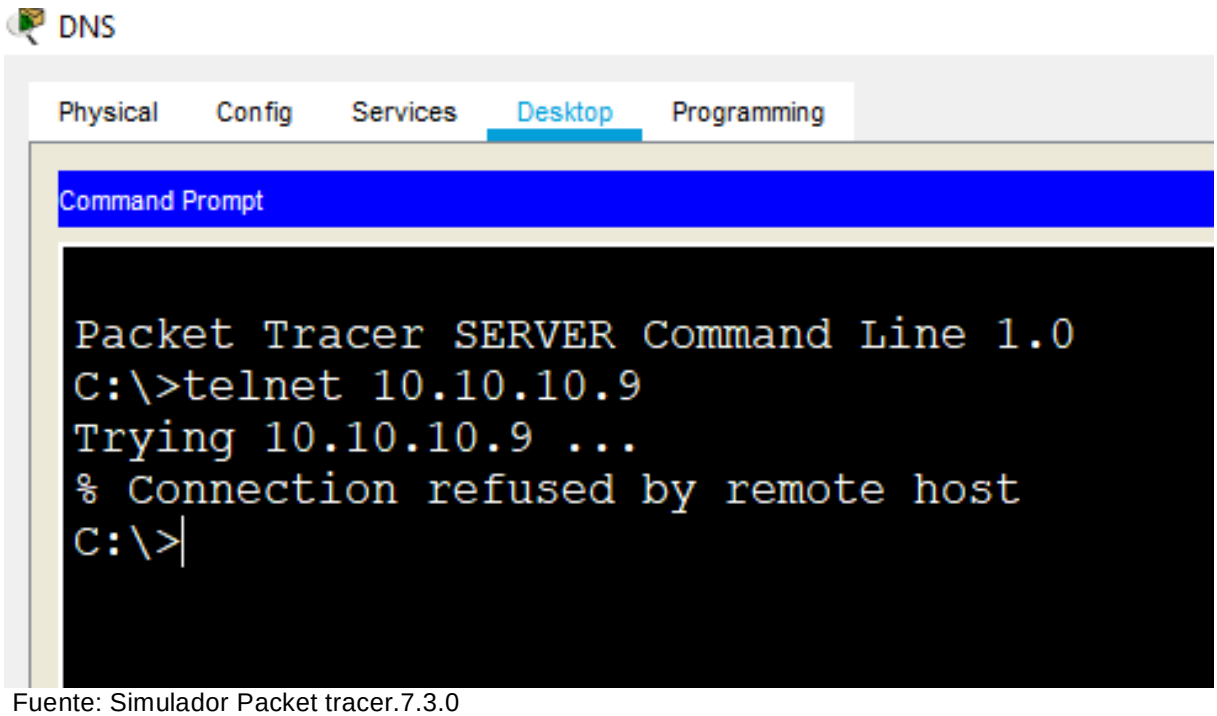
Fuente: Simulador Packet tracer.7.3.0

Figura 27. Probando con la pc de la subred ingeniería



Fuente: Simulador Packet tracer.7.3.0

Figura 28. Probando desde el prompt de el servidor dns (debe ser negado el acceso)



Fuente: Simulador Packet tracer.7.3.0

Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció

Figura 29. r2#show ip access-lists admin-mgt

```
R2#show ip access-lists ADMIN-MGT
Standard IP access list ADMIN-MGT
    permit 192.168.21.0 0.0.0.255 (8 match(es))
    permit 192.168.23.0 0.0.0.255 (2 match(es))
    permit 192.168.99.0 0.0.0.255
```

Fuente: Simulador Packet tracer.7.3.0

Restablecer los contadores de una lista de acceso
R2#clear access-list counters ADMIN-MGT

Figura 30. r2#clear access-list counters admin-mgt

```
R2#
R2#clear access-list counters ADMIN-MGT
R2#show ip access-lists ADMIN-MGT
Standard IP access list ADMIN-MGT
    permit 192.168.21.0 0.0.0.255
    permit 192.168.23.0 0.0.0.255
    permit 192.168.99.0 0.0.0.255

R2#
```

Fuente: Simulador Packet tracer.7.3.0

¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?
R2#show ip interface (tipo) (n°) y show running-config

¿Con qué comando se muestran las traducciones NAT?
R2#show ip nat translations

Figura 31. r2#show ip nat translations

```
R2#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
---  209.165.200.233   192.168.21.21      ---                ---
tcp 209.165.200.233:1030192.168.21.21:1030 209.165.200.238:80 209.165.200.238:80
tcp 209.165.200.233:1031192.168.21.21:1031 209.165.200.238:80 209.165.200.238:80
tcp 209.165.200.233:1032192.168.21.21:1032 209.165.200.238:80 209.165.200.238:80
```

Fuente: Simulador Packet tracer.7.3.0

¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?

R2#clear ip nat translation *

Figura 32. r2# clear ip nat translation *

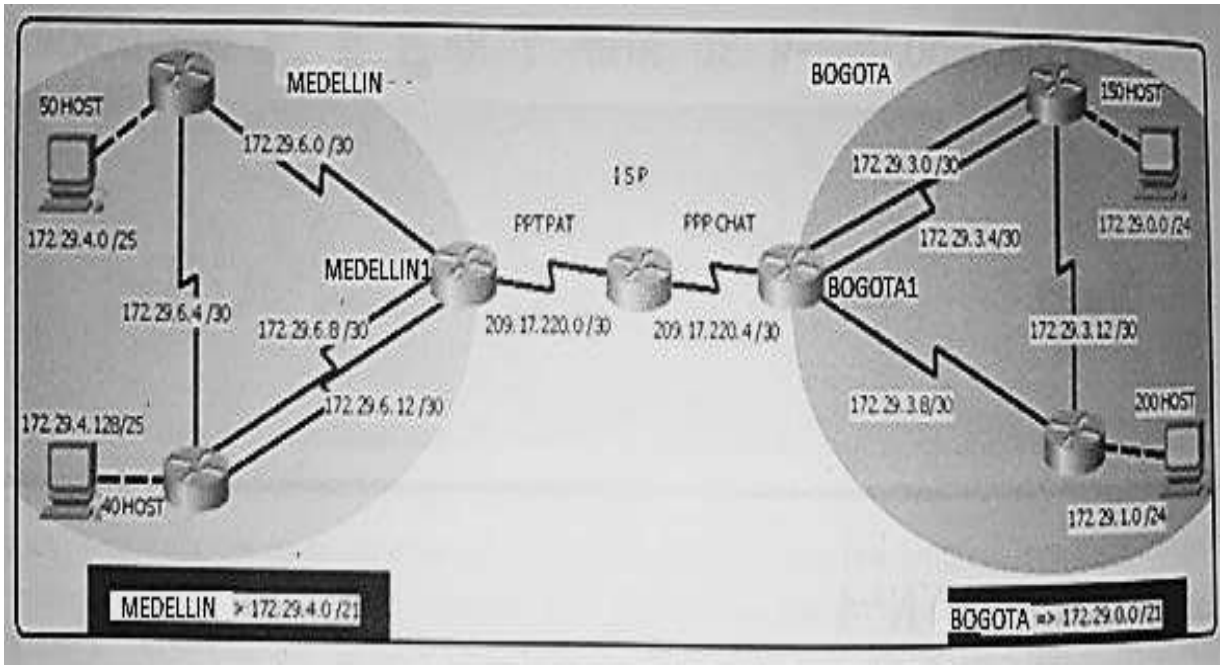
```
R2#clear ip nat translation *
R2#sh
R2#show ip n
R2#show ip na
R2#show ip nat t
R2#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
---  209.165.200.233   192.168.21.21      ---                ---
```

Fuente: Simulador Packet tracer.7.3.0

7 ESCENARIO 2

Una empresa posee sucursales distribuidas en las ciudades de Bogotá y Medellín, 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 re

Figura 33. Topología de red



Fuente: Suministrada por el ejercicio

Este escenario plantea el uso de OSPF como protocolo de enrutamiento, considerando que se tendran rutas por defecto redistribuidas; asimismo, habilitar el encapsulamiento PPP y su autenticación.

Los routers Bogota2 y medellin2 proporcionan el servicio DHCP a su propia red LAN y a los routers 3 de cada ciudad.

Debe configurar PPP en los enlaces hacia el ISP, con autenticación.

Debe habilitar NAT de sobrecarga en los routers Bogota1 y medellin1.

8 PARTE 1: CONFIGURACIÓN DEL ENRUTAMIENTO

a. Configurar el enrutamiento en la red usando el protocolo OSPF versión 2, declare la red principal, desactive la sumarización automática.
b. Los routers Bogota1 y Medellín deberán añadir a su configuración de enrutamiento una ruta por defecto hacia el ISP y, a su vez, redistribuirla dentro de las publicaciones de OSPF.
c. El router ISP deberá tener una ruta estática dirigida hacia cada red interna de Bogotá y Medellín para el caso se sumarizan las subredes de cada uno a /22.

a)
Medellin:

- R5(config)#router ospf 100
- R5(config-router)#router-id 6.6.6.6
- R5(config-router)#log-adjacency-changes
- R5(config-router)#passive-interface Serial0/1/0
- R5(config-router)#network 172.29.6.0 0.0.0.3 area 0
- R5(config-router)#network 172.29.6.8 0.0.0.3 area 0
- R5(config-router)#network 172.29.6.12 0.0.0.3 area 0

- R4(config)#router ospf 100
- R4(config-router)#router router-id 8.8.8.8
- R4(config-router)#router log-adjacency-changes
- R4(config-router)#router passive-interface GigabitEthernet0/1
- R4(config-router)#router network 172.29.4.128 0.0.0.127 area 0
- R4(config-router)#router network 172.29.6.4 0.0.0.3 area 0
- R4(config-router)#router network 172.29.6.8 0.0.0.3 area 0
- R4(config-router)#router network 172.29.6.12 0.0.0.3 area 0
- R3(config)#router ospf 100
- R3(config-router)#router-id 7.7.7.7
- R3(config-router)#log-adjacency-changes
- R3(config-router)#passive-interface GigabitEthernet0/1
- R3(config-router)#network 172.29.6.0 0.0.0.3 area 0
- R3(config-router)#network 172.29.4.0 0.0.0.127 area 0
- R3(config-router)#network 172.29.6.4 0.0.0.3 area 0

Bogotá:

- R7(config)#router ospf 200
- R7(config-router)#router-id 10.10.10.10
- R7(config-router)#log-adjacency-changes
- R7(config-router)#passive-interface Serial0/0/0
- R7(config-router)#network 172.29.3.0 0.0.0.3 area 0
- R7(config-router)#network 172.29.3.4 0.0.0.3 area 0
- R7(config-router)#network 172.29.3.8 0.0.0.3 area 0
- R7(config-router)#default-i nformation originate
- R8(config)#router ospf 200
- R8(config-router)#router-id 7.7.7.7
- R8(config-router)#log-adjacency-changes
- R8(config-router)#network 172.29.3.0 0.0.0.3 area 0
- R8(config-router)#network 172.29.3.4 0.0.0.3 area 0
- R8(config-router)#network 172.29.3.12 0.0.0.3 area 0
- R8(config-router)#network 172.29.0.0 0.0.0.255 area 0
- R9(config)#router ospf 200
- R9(config)#router-id 8.8.8.8
- R9(config)#log-adjacency-changes
- R9(config)#passive-interface GigabitEthernet0/1
- R9(config)#network 172.29.1.0 0.0.0.255 area 0
- R9(config)#network 172.29.3.8 0.0.0.3 area 0
- R9(config)#network 172.29.3.12 0.0.0.3 area 0

b)
Medellín:
Para configurar una ruta estática predeterminada hacia el ISP, se elije en este caso al router conectado directamente a el, que es R5.
R5(config)#ip route 0.0.0.0 0.0.0.0 serial 0/1/0

Ahora, para redistribuirla a los demás routers OSPF, se hace el mismo proceso OSPF creado

R5(config)#router ospf 100
R5(config-router)#default-i nformation originate → este comando redistribulle la ruta predeterminada configurada en R5 a todos los routers OSPF que tenga adyacencia.
Bogotá:

Para configurar una ruta estática predeterminada hacia el ISP, se elije en este caso al router conectado directamente a el, que es R5
R7(config)#ip route 0.0.0.0 0.0.0.0 serial 0/0/0
Ahora, toca redistribuirla a los demás routers OSPF
R5(config)#router ospf 100
R5(config-router)#default-i nformation originate

c)
Ya al tener las 2 subredes sumarizadas se configuran en el router ISP hacia ambas Sucursales
R6(config)#ip route 172.29.4.0 255.255.252.0 serial 0/0/0

Tabla 1. Sumarizacion de redes para Medellin

172.29.4.0	10101100	00011101	00000100	00000000
172.29.4.128	10101100	00011101	00000100	10000000
172.29.6.0	10101100	00011101	00000100	00000000
172.29.6.4	10101100	00011101	00000100	00000100
172.29.6.8	10101100	00011101	00000100	00001000
172.29.6.12	10101100	00011101	00000100	00001100
Resultado	10101100	00011101	00000100	00000000
Direc. De Red	172	29	4	0

Fuente: Simulador Packet tracer.7.3.0

22 bits es la mayor cantidad de bits que coincidencia entre las redes en Medellín por lo tanto la red será **172.29.4.0/22**

9 PARTE 2. TABLA DE ENRUTAMIENTO 172.29.4.0/22

R6(config)#ip route 172.29.4.0 255.255.252.0 serial 0/0/1

Parte 2: Tabla de Enrutamiento.
Verificar la tabla de enrutamiento en cada uno de los routers para comprobar las Tabla redes y sus rutas.

Medellín:

Con el comando show ip route podemos ver las tablas de enrutamiento en cada router

R5#show ip route

Tabla 2. Enrutamiento 172.29.0.0/22

172.29.0.0	10101100	00011101	00000000	00000000
172.29.1.0	10101100	00011101	00000001	00000000
172.29.3.0	10101100	00011101	00000011	00000000
172.29.3.4	10101100	00011101	00000011	00000100
172.29.3.8	10101100	00011101	00000011	00001000
172.29.3.12	10101100	00011101	00000011	00001100
Resultado	10101100	00011101	00000100	00000000
Direc. De Red	172	29	0	0

Fuente: Simulador Packet tracer.7.3.0

22 bits es la mayor cantidad de bits que coincidencia entre las redes en Bogotá por lo tanto la red será **172.29.0.0/22**

De resaltar, las rutas aprendidas por OSPF que aparecen en la tabla con el indicador O y la ruta predeterminada configurada manualmente en este dispositivo.

R4#show ip route

Figura 34. r4#show ip route

```
Gateway of last resort is 172.29.6.9 to network 0.0.0.0

     10.0.0.0/32 is subnetted, 1 subnets
C       10.10.10.10/32 is directly connected, Loopback4
     172.29.0.0/16 is variably subnetted, 10 subnets, 3 masks
O       172.29.4.0/25 [110/138] via 172.29.6.9, 01:06:05, Serial0/0/0
C       172.29.4.128/25 is directly connected, GigabitEthernet0/1
L       172.29.4.129/32 is directly connected, GigabitEthernet0/1
O       172.29.6.0/30 [110/128] via 172.29.6.9, 01:10:32, Serial0/0/0
C       172.29.6.4/30 is directly connected, Serial0/1/0
L       172.29.6.6/32 is directly connected, Serial0/1/0
C       172.29.6.8/30 is directly connected, Serial0/0/0
L       172.29.6.10/32 is directly connected, Serial0/0/0
C       172.29.6.12/30 is directly connected, Serial0/0/1
L       172.29.6.14/32 is directly connected, Serial0/0/1
O*E2 0.0.0.0/0 [110/1] via 172.29.6.9, 01:05:15, Serial0/0/0

R4#
```

Fuente: Simulador Packet tracer.7.3.0

De resaltar, las rutas aprendidas por OSPF que aparecen en la tabla con el indicador O y confirma que se aprendio una ruta predeterminada por medio de OSPF con la redistribución, así lo indica O*E2

Figura 35. R3#show ip route

```
     9.0.0.0/32 is subnetted, 1 subnets
C       9.9.9.9/32 is directly connected, Loopback4
     172.29.0.0/16 is variably subnetted, 9 subnets, 3 masks
C       172.29.4.0/25 is directly connected, GigabitEthernet0/1
L       172.29.4.1/32 is directly connected, GigabitEthernet0/1
O       172.29.4.128/25 [110/138] via 172.29.6.1, 01:09:25, Serial0/0/0
C       172.29.6.0/30 is directly connected, Serial0/0/0
L       172.29.6.2/32 is directly connected, Serial0/0/0
C       172.29.6.4/30 is directly connected, Serial0/0/1
L       172.29.6.5/32 is directly connected, Serial0/0/1
O       172.29.6.8/30 [110/128] via 172.29.6.1, 01:09:25, Serial0/0/0
O       172.29.6.12/30 [110/128] via 172.29.6.1, 01:09:25, Serial0/0/0
O*E2 0.0.0.0/0 [110/1] via 172.29.6.1, 01:07:36, Serial0/0/0
```

Fuente: Simulador Packet tracer.7.3.0

De la misma forma que R4, las rutas aprendidas por OSPF que aparecen en la tabla con el indicador O y confirma que se aprendio una ruta predeterminada por medio de OSPF con la redistribución, así lo indica O*E2

Bogotá

Figura 36. r7#show ip route

```
     4.0.0.0/32 is subnetted, 1 subnets
C       4.4.4.4/32 is directly connected, Loopback0
     172.29.0.0/16 is variably subnetted, 9 subnets, 3 masks
O       172.29.0.0/24 [110/65] via 172.29.3.2, 00:10:13, Serial0/0/1
O       172.29.1.0/24 [110/74] via 172.29.3.10, 00:13:02, Serial0/1/1
C       172.29.3.0/30 is directly connected, Serial0/0/1
L       172.29.3.1/32 is directly connected, Serial0/0/1
C       172.29.3.4/30 is directly connected, Serial0/1/0
L       172.29.3.5/32 is directly connected, Serial0/1/0
C       172.29.3.8/30 is directly connected, Serial0/1/1
L       172.29.3.9/32 is directly connected, Serial0/1/1
O       172.29.3.12/30 [110/128] via 172.29.3.2, 00:10:40, Serial0/0/1
                       [110/128] via 172.29.3.10, 00:10:40, Serial0/1/1
     209.17.220.0/24 is variably subnetted, 2 subnets, 2 masks
C       209.17.220.4/30 is directly connected, Serial0/0/0
L       209.17.220.6/32 is directly connected, Serial0/0/0
S*   0.0.0.0/0 is directly connected, Serial0/0/0
```

Fuente: Simulador Packet tracer.7.3.0

Figura 37. R8#show ip route

```
     172.29.0.0/16 is variably subnetted, 10 subnets, 3 masks
C       172.29.0.0/24 is directly connected, GigabitEthernet0/1
L       172.29.0.1/32 is directly connected, GigabitEthernet0/1
O       172.29.1.0/24 [110/74] via 172.29.3.13, 00:11:28, Serial0/1/0
C       172.29.3.0/30 is directly connected, Serial0/0/0
L       172.29.3.2/32 is directly connected, Serial0/0/0
C       172.29.3.4/30 is directly connected, Serial0/0/1
L       172.29.3.6/32 is directly connected, Serial0/0/1
O       172.29.3.8/30 [110/128] via 172.29.3.1, 00:11:28, Serial0/0/0
                      [110/128] via 172.29.3.13, 00:11:28, Serial0/1/0
C       172.29.3.12/30 is directly connected, Serial0/1/0
L       172.29.3.14/32 is directly connected, Serial0/1/0
O*E2 0.0.0.0/0 [110/1] via 172.29.3.1, 00:11:50, Serial0/0/0
```

Fuente: Simulador Packet tracer.7.3.0

Figura 38. R9#show ip route

```
     172.29.0.0/16 is variably subnetted, 9 subnets, 3 masks
O       172.29.0.0/24 [110/65] via 172.29.3.14, 00:12:25, Serial0/0/1
C       172.29.1.0/24 is directly connected, GigabitEthernet0/1
L       172.29.1.1/32 is directly connected, GigabitEthernet0/1
O       172.29.3.0/30 [110/128] via 172.29.3.9, 00:12:54, Serial0/0/0
                      [110/128] via 172.29.3.14, 00:12:54, Serial0/0/1
O       172.29.3.4/30 [110/128] via 172.29.3.9, 00:12:54, Serial0/0/0
                      [110/128] via 172.29.3.14, 00:12:54, Serial0/0/1
C       172.29.3.8/30 is directly connected, Serial0/0/0
L       172.29.3.10/32 is directly connected, Serial0/0/0
C       172.29.3.12/30 is directly connected, Serial0/0/1
L       172.29.3.13/32 is directly connected, Serial0/0/1
O*E2 0.0.0.0/0 [110/1] via 172.29.3.9, 00:14:04, Serial0/0/0

R9#
```

Fuente: Simulador Packet tracer.7.3.0

Verificar el balanceo de carga que presentan los routers.
Con el comando show ip route se observa los puntos b,c y d

Obsérvese en los routers Bogotá1 y Medellín1 cierta similitud por su ubicación, por tener dos enlaces de conexión hacia otro router y por la ruta por defecto que manejan.

Los routers Medellín2 y Bogotá2 también presentan redes conectadas directamente y recibidas mediante OSPF.

Así como lo muestra las tablas de enrutamiento anteriores, todas las rutas que aparecen con el indicador C son redes conectadas directamente y las que parecen con O son aprendidas por OSPF

Las tablas de los routers restantes deben permitir visualizar rutas redundantes para el caso de la ruta por defecto.
El router ISP solo debe indicar sus rutas estáticas adicionales a las directamente conectadas

10 PARTE 3: DESHABILITAR LA PROPAGACIÓN DEL PROTOCOLO OSPF.

a. Para no propagar las publicaciones por interfaces que no lo requieran se debe deshabilitar la propagación del protocolo OSPF, en la siguiente tabla se indican las interfaces de cada router que no necesitan desactivación.

Tabla 3. Interfaces de cada router

ROUTER	INTERFAZ
Bogota1	SERIAL0/0/1; SERIAL0/1/0; SERIAL0/1/1
Bogota2	SERIAL0/0/0; SERIAL0/0/1
Bogota3	SERIAL0/0/0; SERIAL0/0/1; SERIAL0/1/0
Medellín1	SERIAL0/0/0; SERIAL0/0/1; SERIAL0/1/1
Medellín2	SERIAL0/0/0; SERIAL0/0/1
Medellín3	SERIAL0/0/0; SERIAL0/0/1; SERIAL0/1/0
ISP	No lo requiere

Fuente: Simulador Packet tracer.7.3.0

Para evitar la propagación de rutas por OSPF por interfaces no deseadas como por ejemplo, las interfaces LAN y los enlaces hacia el ISP , eso se logra con el comando passive-interface dentro del proceso OSPF en cada router

R5(config)#router ospf 100
R5(config-router)#passive-interface serial 0/1/0 → aquí le decimos al proceso OSPF que no debe enviar información de las tablas de enrutamiento por esta interfaz, practica recomendada hacer para la seguridad de la red

Nota: este mismo proceso se hace con los demás routers donde puede cambiar en el tipo o número de interfaz, esto se debe hacer para las interfaces LAN.

11 PARTE 4: VERIFICACIÓN DEL PROTOCOLO OSPF

Verificar y documentar las opciones de enrutamiento configuradas en los routers, como el passive interface para la conexión hacia el ISP, la versión de OSPF y las interfaces que participan de la publicación entre otros datos.

Con el comando show ip protocols, permite ver información de los protocolos de routing activos en el equipo, ID de proceso, interfaces pasivas, interfaces y redes que participan en OSPF.

Medellín:

Figura. 39R4#show ip protocols

```
R4#show ip protocols

Routing Protocol is "ospf 100"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 172.29.6.14
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.29.4.128 0.0.0.127 area 0
    172.29.6.4 0.0.0.3 area 0
    172.29.6.8 0.0.0.3 area 0
    172.29.6.12 0.0.0.3 area 0
  Passive Interface(s):
    GigabitEthernet0/1
  Routing Information Sources:
    Gateway         Distance      Last Update
    6.6.6.6              110      00:07:30
    7.7.7.7              110      00:13:12
    172.29.6.14          110      00:12:29
  Distance: (default is 110)
```

Fuente: Simulador Packet tracer.7.3.0

Figura 40. r3#show ip protocols

```
R3#show ip protocols

Routing Protocol is "ospf 100"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 7.7.7.7
  Number of areas in this router is 2. 2 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.29.6.0 0.0.0.3 area 0
    172.29.4.0 0.0.0.127 area 0
  Passive Interface(s):
    GigabitEthernet0/1
  Routing Information Sources:
    Gateway         Distance      Last Update
    6.6.6.6              110      00:14:08
    7.7.7.7              110      00:16:00
    172.29.6.14          110      00:19:06
  Distance: (default is 110)
```

Fuente: Simulador Packet tracer.7.3.0

Figura 41. R5#show ip protocols

```
R5#show ip protocols

Routing Protocol is "ospf 100"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 6.6.6.6
  It is an autonomous system boundary router
  Redistributing External Routes from,
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.29.6.0 0.0.0.3 area 0
    172.29.6.8 0.0.0.3 area 0
    172.29.6.12 0.0.0.3 area 0
  Passive Interface(s):
    Serial0/1/0
  Routing Information Sources:
    Gateway         Distance      Last Update
    6.6.6.6              110      00:14:42
    7.7.7.7              110      00:20:24
    172.29.6.14          110      00:19:41
  Distance: (default is 110)
```

Fuente: Simulador Packet tracer.7.3.0

Bogotá:

Figura 42. r7#show ip protocols

```
R7#show ip protocols

Routing Protocol is "ospf 200"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 10.10.10.10
  It is an autonomous system boundary router
  Redistributing External Routes from,
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.29.3.0 0.0.0.3 area 0
    172.29.3.4 0.0.0.3 area 0
    172.29.3.8 0.0.0.3 area 0
  Passive Interface(s):
    Serial0/0/0
  Routing Information Sources:
    Gateway         Distance      Last Update
    7.7.7.7              110      00:16:25
    8.8.8.8              110      00:16:49
    10.10.10.10          110      00:16:56
  Distance: (default is 110)
```

Fuente: Simulador Packet tracer.7.3.0

Figura 43. r8#show ip protocols

```
R8#show ip protocols

Routing Protocol is "ospf 200"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 7.7.7.7
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.29.3.0 0.0.0.3 area 0
    172.29.3.4 0.0.0.3 area 0
    172.29.3.12 0.0.0.3 area 0
    172.29.0.0 0.0.0.255 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    7.7.7.7              110      00:16:56
    8.8.8.8              110      00:17:20
    10.10.10.10          110      00:17:27
  Distance: (default is 110)
```

Fuente: Simulador Packet tracer.7.3.0

Figura 44. R9#show ip protocols

```
R9#show ip protocols

Routing Protocol is "ospf 200"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 8.8.8.8
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.29.1.0 0.0.0.255 area 0
    172.29.3.8 0.0.0.3 area 0
    172.29.3.12 0.0.0.3 area 0
  Passive Interface(s):
    GigabitEthernet0/1
  Routing Information Sources:
    Gateway         Distance      Last Update
    7.7.7.7              110      00:17:48
    8.8.8.8              110      00:18:11
    10.10.10.10          110      00:18:19
  Distance: (default is 110)
```

Fuente: Simulador Packet tracer.7.3.0

Verificar y documentar la base de datos de OSPF de cada router, donde se informa de manera detallada de todas las rutas hacia cada red.

Con el comando R5#show ip route ospf 100 podemos ver información de las rutas ospf en los routers de Medellín

Figura 45. R5#show ip route ospf 100

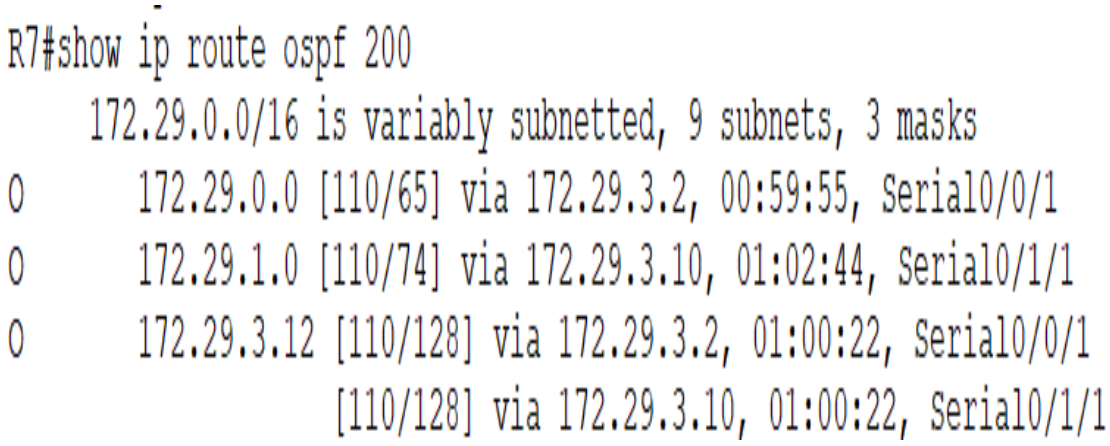
```
R5#show ip route ospf 100
     172.29.0.0/16 is variably subnetted, 9 subnets, 3 masks
O       172.29.4.0 [110/74] via 172.29.6.2, 01:56:48, Serial0/0/0
O       172.29.4.128 [110/74] via 172.29.6.10, 02:01:11, Serial0/0/1
O       172.29.6.4 [110/64841] via 172.29.6.10, 00:30:28, Serial0/0/1

R5#
```

Fuente: Simulador Packet tracer.7.3.0

Para los routers en Bogotá

Figura 46. R7#show ip route ospf 200



Fuente: Simulador Packet tracer.7.3.0

12 PARTE 5. CONFIGURAR ENCAPSULAMIENTO Y AUTENTICACIÓN PPP

Según la topología se requiere que el enlace Medellín1 con ISP sea configurado con autenticación PAT.

El primer paso es configurar un usuario en ambos routers R5 y ISP
R5(config)#username medellin secret 1234
ISP(config)#username ISP secret 4321

Segundo paso, configurar las interfaces seriales de ambos routers con el protocolo PPP con autenticación PAT
R5(config)#interface serial 0/1/0
R5(config-if)#encapsulation ppp → aquí se define el protocolo de capa2 en el enlace
R5(config-if)#ppp authentication ppp → se define la autenticación ppp
R5(config-if)#ppp pap sent-username ISP password 0 4321 →aquí se le dice al dipositivo en este caso R5 los datos de usuario y contraseña que debe enviar a ISP para poder autenticarse(aquí se debe colocar es el usuario y contraseña del otro equipo)

ISP(config)#interface serial 0/0/0
ISP(config-if)#encapsulation ppp → aquí se define el protocolo de capa2 en el enlace
ISP(config-if)#ppp authentication ppp → se define la autenticación ppp
ISP(config-if)#ppp pap sent-username medellin password 0 1234 →aquí se le dice al router ISP los datos de usuario y contraseña que debe enviar a R5 para poder autenticarse(aquí se debe colocar es el usuario y contraseña del otro equipo)

El enlace Bogotá1 con ISP se debe configurar con autenticación CHAT.
Bogotá:
Aquí es importante que el nombre de usuario coincida con el nombre del dispositivo a crear el CHAT y la misma contraseña del usuario de ISP
R7(config)#username R6 secret 4321
R7(config)#interface serial 0/0/0
R7(config-if)#encapsulation ppp → aquí se define el protocolo de capa2 en el enlace
R6(config-if)#ppp authentication chap →se define la autenticación ppp

Ahora del lado del ISP:
R6(config)#username R7 secret 4321
R6(config)#interface serial 0/0/1
R6(config-if)#encapsulation ppp → aquí se define el protocolo de capa2 en el enlace
R6(config-if)#ppp authentication chap →se define la autenticación ppp

13 PARTE 6: CONFIGURACIÓN DEPAT.

a. En la topología, si se activa NAT en cada equipo de salida (Bogotá1 y Medellín1), los routers internos de una ciudad no podrán llegar hasta los routers internos en el otro extremo, sólo existirá comunicación hasta los routers Bogotá1, ISP y Medellín1.
b. Después de verificar lo indicado en el paso anterior proceda a configurar el NAT en el router Medellín1. Compruebe que la traducción de direcciones indique las interfaces de entrada y de salida. Al realizar una prueba de ping, la dirección debe ser traducida automáticamente a la dirección de la interfaz serial 0/1/0 del router Medellín1, cómo diferente puerto.

Medellin:

- R5(config)#ip nat inside source list 1 interface serial 0/1/0 overload
- R5(config)#access-list 1 permit 172.29.4.0 0.0.3.255
- R5(config)#interface serial 0/1/0
- R5(config-if)#ip nat outside
- R5(config-if)#int serial 0/0/1
- R5(config-if)#ip nat inside
- R5(config-if)#int serial 0/1/1
- R5(config-if)#ip nat inside
- R5(config-if)#int serial 0/0/0
- R5(config-if)#ip nat inside

Figuras 47. R5#show ip nat translations

```
R5#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 209.17.220.1:10   172.29.4.130:10    172.29.0.10:10     172.29.0.10:10
icmp 209.17.220.1:11   172.29.4.130:11    172.29.0.10:11     172.29.0.10:11
icmp 209.17.220.1:12   172.29.4.130:12    172.29.0.10:12     172.29.0.10:12
icmp 209.17.220.1:13   172.29.4.130:13    172.29.0.10:13     172.29.0.10:13
icmp 209.17.220.1:14   172.29.4.130:14    172.29.0.10:14     172.29.0.10:14
icmp 209.17.220.1:15   172.29.4.130:15    172.29.0.10:15     172.29.0.10:15
icmp 209.17.220.1:8    172.29.4.130:8     172.29.0.10:8      172.29.0.10:8
icmp 209.17.220.1:9    172.29.4.130:9     172.29.0.10:9      172.29.0.10:9
```

Fuente: Simulador Packet tracer.7.3.0

c. Proceda a configurar el NAT en el router Bogotá1. Compruebe que la traducción de direcciones indique las interfaces de entrada y de salida. Al realizar una prueba de ping, la dirección debe ser traducida automáticamente a la dirección de la interfaz serial 0/1/0 del router Bogotá1, cómo diferente puerto.

Bogotá:

- R7(config)#ip nat inside source list 1 interface serial 0/0/0 overload
- R7(config)#access-list 1 permit 172.29.0.0 0.0.3.255
- R7(config)#interface serial 0/0/0
- R7(config-if)#ip nat outside
- R7(config-if)#int serial 0/1/1
- R7(config-if)#ip nat inside
- R7(config-if)#int serial 0/0/1
- R7(config-if)#ip nat inside
- R7(config-if)#int serial 0/1/0
- R7(config-if)#ip nat inside

Figura 48. R7#show ip nat translation

```
R7#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 209.17.220.6:4    172.29.0.10:4      172.29.4.130:4     172.29.4.130:4
icmp 209.17.220.6:5    172.29.0.10:5      172.29.4.130:5     172.29.4.130:5
icmp 209.17.220.6:6    172.29.0.10:6      172.29.4.130:6     172.29.4.130:6
icmp 209.17.220.6:7    172.29.0.10:7      172.29.4.130:7     172.29.4.130:7

R7#
```

Fuente: Simulador Packet tracer.7.3.0

14 PARTE 7: CONFIGURACIÓN DEL SERVICIO DHCP

a. Configurar la red Medellín2 y Medellín3 donde el router Medellín 2 debe ser el servidor DHCP para ambas redes Lan.
Servidor DHCP Medellín:

- R3(config)#ip dhcp excluded-address 172.29.4.129
- R3(config)#ip dhcp pool LAN-40_HOST
- R3(dhcp-config)#network 172.29.4.128 255.255.255.128
- R3(dhcp-config)#default-router 172.29.4.129
- R3(dhcp-config)#dns-server 8.8.8.8

- R3(config)#ip dhcp excluded-address 172.29.4.1
- R3(config)#ip dhcp pool LAN-50_HOST
- R3(dhcp-config)#network 172.29.4.0 255.255.255.128
- R3(dhcp-config)#default-router 172.29.4.1
- R3(dhcp-config)#dns-server 8.8.8.8

b. El router Medellín3 deberá habilitar el paso de los mensajes broadcast hacia la IP del router Medellín2.

- R4(config)#interface gigabitEthernet 0/1
- R4(config-if)#ip helper-address 172.29.6.5

c. Configurar la red Bogotá2 y Bogotá3 donde el router Medellín2 debe ser el servidor DHCP para ambas redes Lan.

Servidor DHCP Bogotá:

- R8(config)#ip dhcp excluded-address 172.29.0.1
- R8(config)#ip dhcp pool LAN-150_host
- R8(dhcp-config)#network 172.29.0.0 255.255.255.0
- R8(dhcp-config)#default-router 172.29.0.1
- R8(dhcp-config)#dns-server 8.8.8.8

- R8(config)#ip dhcp excluded-address 172.29.1.1
- R8(config)#ip dhcp pool LAN-200_HOST
- R8(dhcp-config)#network 172.29.1.0 255.255.255.0
- R8(dhcp-config)#default-router 172.29.1.1
- R8(dhcp-config)#dns-server 8.8.8.8

d. Configure el router Bogotá1 para que habilite el paso de los mensajes Broadcast hacia la IP del router Bogotá2.

- R9(config)#interface gigabitEthernet 0/1
- R9(config-if)#ip helper-address 172.29.3.14

15 LINK DEL VIDEO

- Https://yuotu.be/LKcLQbua3FQ

CONCLUSIONES

En esta práctica me permitió abordar nuevos conceptos he ideas de una red en un ámbito laborar logrando la segmentación de la red y la comunicación de las mismas gracias a la configuración del router y swithces logre comprender el funcionamiento.

Se usó en este trabajo la aplicación virtual Packet Tracer, que permite la creación de diferentes modelos de redes de una forma más amigable e intuitiva para el usuario que la proporcionada por el propio simulador en un formato ampliamente utilizado en la actualidad.

BIBLIOGRAFIA

ARNEDO, J. (2013). Redes de comunicaciones. Recuperado de http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/reader.action?ppg=30&docID=10853455&tm=1480129103984

GABRIEL BARRETO. (S. f.). Como configurar un Router Cisco como un servidor DHCP en Packet Tracer. Recuperado de https://www.youtube.com/watch?v=yudNmI4p1dU&feature=youtu.be

GALLEGO, P. (2010). E-learning y derecho. Recuperado de http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/reader.action?ppg=33&docID=11046127&tm=1480130515905

IBRAHIM, K. (2008). Elementos básicos de comercio electrónico. Recuperado de http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/reader.action?ppg=16&docID=10219507&tm=1480130867992