PRUEBA DE HABILIDADES PRÁCTICAS CCNA

NEIDID MEDINA ATENCIA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA (ECBTI)
INGENIERIA DE SISTEMAS
COROZAL SUCRE
2020

PRUEBA DE HABILIDADES PRÁCTICAS CCNA

NEIDID MEDINA ATENCIA

ASESOR
NILSON ALBEIRO FERREIRA MANZANARES
Docente Ocasional

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA (ECBTI)
INGENIERIA DE SISTEMAS
COROZAL SUCRE
2020

TABLA DE CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

1. RESUMEN

En el siguiente trabajo se realizan dos escenarios, en el primero. Una empresa posee sucursales distribuidas en las ciudades de Bogotá y Medellín en donde se debe 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 y en el escenario dos una red pequeña se debe configurar 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.

1.1 ABSTRACT

In the following work, two scenarios are carried out, in the first. A company has branches distributed in the cities of Bogotá and Medellin where each of the devices that are part of the scenario must be configured and interconnected, in accordance with the guidelines established for IP addressing, routing protocols and other aspects that form Part of the network topology and in Scenario Two a small network must be configured to support IPv4 and IPv6 connectivity, switch security, routing between VLANs, RIPv2 dynamic routing protocol, dynamic host configuration protocol (DHCP) , Static and Dynamic Network Address Translation (NAT), Access Control Lists (ACLs) and Server / Client Network Time Protocol (NTP).

2. INTRODUCCIÓN

El siguiente trabajo hace parte de la actividad final del diplomado de profundización cisco (diseño e implementación de soluciones integradas LAN / WAN, para lo cual se pone en práctica todo lo aprendido durante el curso, donde se le da solución a dos escenarios propuestos y en los cuales se configuran y se interconectan entre sí cada uno de los dispositivos que forman parte del escenario y donde se aplican los comandos como ping, traceroute, show ip route, entre otros

OBJETIVOS

-Realizar las rutinas de diagnóstico y dejar los equipos listos para su configuración.

-Determinar la conexión física de los equipos con base en la topología de red.

-Establecer la autenticación local AAA y cifrado de contraseñas en los Router.

3. DESARROLLO ESCENARIO 1

3.1 ESCENARIO

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.

3.2 TOPOLOGÍA

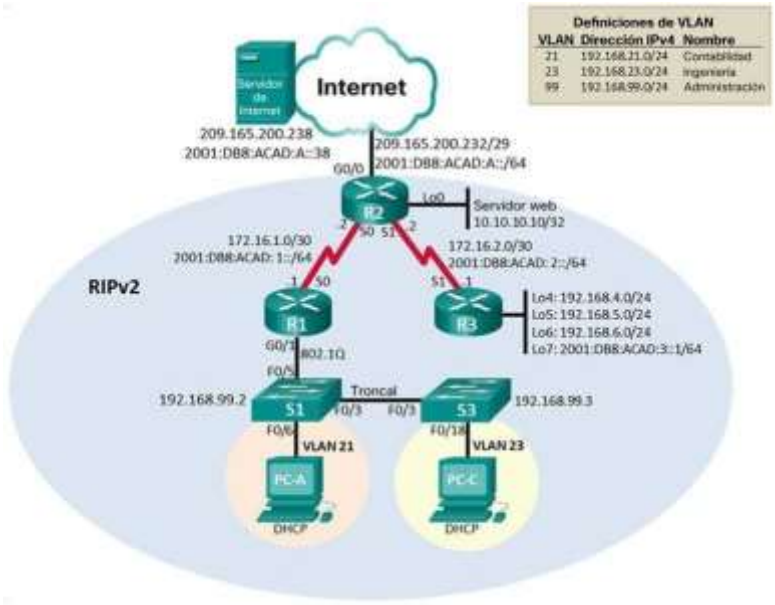


Figura 1. Topología Escenario 1

4.3 PARTE 1: Inicializar dispositivos

4.3.1. Paso 1: Inicializar y volver a cargar los routers y los switches

Tabla 1. Configuración inicial routers y switches.

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	Erase startup-config
Volver a cargar todos los routers	Reload
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Erase startup-config Delete vtp
Volver a cargar ambos switches	Reload
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Show vlan

4.4. PARTE 2: Configurar los parámetros básicos de los dispositivos

4.4.1 Paso 2: Configurar la computadora de Internet

Tabla 2. Configurar la computadora de Internet

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.233
Dirección IPv6/subred	2001:DB8:ACAD:A::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:A::33/64

4.4.2 Paso 3: Configurar R1

Tabla 3. Configuración R1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	no ip domain-lookup
Nombre del router	R1
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	
Mensaje MOTD	Se prohíbe el acceso no autorizado.
Interfaz S0/0/0	Conexión R1 172.16.1.1 255.255.255.252 2001:DB8:ACAD:1::1/64 Establecer la frecuencia de reloj en 128000 Activar la interfaz
Rutas predeterminadas	Configurar una ruta IPv4 predeterminada de S0/0/0 Configurar una ruta IPv6 predeterminada de S0/0/0

```
Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname R1
R1(config)#enable secret class
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#line vty 0 4
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#service password-encryption
```

R1(config)#banner motd "Se prohibe el acceso no autorizado"
R1(config)#ipv6 unicast-routing
R1(config)#interface serial0/0/0
R1(config-if)#clock rate 128000
R1(config-if)#ip address 172.16.1.1 255.255.255.252

R1(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
R1(config-if)#ipv6 address 2001:DB8:ACAD:1::1/64

R1(config-if)#no shutdown

R1(config-if)#ip route 0.0.0.0 0.0.0.0 s0/0/0
%Default route without gateway, if not a point-to-point interface, may impact performance

R1(config)#ipv6 route 2001:DB8:ACAD:1::/64 s0/0/0

Análisis. Se realizan las configuraciones básicas en el R1, se le asigna un nombre, contraseñas, mensaje de acceso no autorizado, se configuran las interfaces, se asigna la frecuencia de reloj, se configuran las rutas predeterminadas, etc.

4.4.3 Paso 4: Configurar R2

Tabla 4. Configuración R2

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	no ip domain-lookup
Nombre del router	R2
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	
Habilitar el servidor HTTP	
Mensaje MOTD	Se prohíbe el acceso no autorizado.
Interfaz S0/0/0	Establezca la descripción 172.16.1.2 255.255.255.252

	2001:DB8:ACAD:1::2/64. Activar la interfaz
Interfaz S0/0/1	Establecer la descripción 172.16.2.2 255.255.255.252 2001:DB8:ACAD:2::2/64. Establecer la frecuencia de reloj en 128000. Activar la interfaz
Interfaz G0/0 (simulación de Internet)	Establecer la descripción. 209.165.200.233 255.255.255.248 2001:DB8:ACAD:A::33/64. Activar la interfaz
Interfaz loopback 0 (servidor web simulado)	Establecer la descripción. Establezca la dirección IPv4.
Ruta predeterminada	Configure una ruta IPv4 predeterminada de G0/0. Configure una ruta IPv6 predeterminada de G0/0.

```
Router(config)#no ip domain-lookup
Router(config)#hostname R2
R2(config)#enable secret class
R2(config)#line console 0
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#line vty 0 4
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#exit
R2(config)#service password-encryption
R2(config)#banner motd;
Enter TEXT message. End with the character ';'.
Se prohibe el acceso no autorizado;
R2(config)#ipv6 unicast-routing
R2(config)#int se0/0/0
R2(config-if)#description Conexion a R1
R2(config-if)#ip address 172.16.1.2 255.255.255.252
R2(config-if)#no sh
R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64
R2(config)#int s0/0/1
R2(config-if)#description Conexion 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)#clock rate 128000
R2(config-if)#no sh
R2(config)#int g0/0
R2(config-if)#description Conexion al Servidor Internet
R2(config-if)#ip address 209.165.200.233 255.255.255.248
R2(config-if)#ipv6 address 2001:DB8:ACAD:A::33/64
R2(config-if)#no sh

R2(config)#int lo0
R2(config-if)#description Conexion Servidor Web Simulado
R2(config-if)#ip address 10.10.10.10 255.255.255.255
R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0
%Default route without gateway, if not a point-to-point interface, may impact
performance
R2(config)#ipv6 route 2001:DB8:ACAD:A::/64 g0/0
R2(config-if)#end
```

Análisis. Se realizan las configuraciones básicas en el R2, se le asigna un nombre, contraseñas, mensaje de acceso no autorizado, se configuran las interfaces, se asigna la frecuencia de reloj, se configuran las rutas predeterminadas, etc.

4.4.4 Paso 5: Configurar R3

Tabla 5. Configuración R3

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	no ip domain-lookup
Nombre del router	R3
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	
Mensaje MOTD	Se prohíbe el acceso no autorizado.

Interfaz S0/0/1	Establecer la descripción 172.16.2.1 255.255.255.252 2001:DB8:ACAD:2::1/64 Activar la interfaz
Interfaz loopback 4	192.168.4.1 255.255.255.0
Interfaz loopback 5	192.168.5.1 255.255.255.0
Interfaz loopback 6	192.168.6.1 255.255.255.0
Interfaz loopback 7	2001:DB8:ACAD:3::1/64
Rutas predeterminadas	

```
Router(config)#no ip domain-lookup
Router(config)#hostname R3
R3(config)#enable secret class
R3(config)#line console 0
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#line vty 0 4
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#exit
R3(config)#service password-encryption
R3(config)#banner motd ;
Enter TEXT message. End with the character ';'.
Se prohibe el acceso no autorizado;
R3(config)#ipv6 unicast-routing
R3(config)#int s0/0/1
R3(config-if)#description Conexion 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)#no sh
R3(config)#int lo4
R3(config-if)#ip address 192.168.4.1 255.255.255.0
R3(config)#int lo5
R3(config-if)#ip address 192.168.5.1 255.255.255.0
R3(config)#int lo6
R3(config-if)#ip address 192.168.6.1 255.255.255.0
R3(config)#int lo7
R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64
```

Análisis. Se realizan las configuraciones básicas en el R3, se le asigna un nombre, contraseñas, mensaje de acceso no autorizado, se configuran las interfaces, se asigna la frecuencia de reloj, se configuran las rutas predeterminadas, etc.

4.4.5. Paso 6: Configurar S1

Tabla 6. Configuración S1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	no ip domain-lookup
Nombre del switch	S1
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	
Mensaje MOTD	Se prohíbe el acceso no autorizado.

```
Switch(config)#no ip domain-lookup
Switch(config)#hostname S1
S1(config)#enable secret class
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#line vty 0 4
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#exit
S1(config)#service password-encryption
S1(config)#banner motd ;
Enter TEXT message. End with the character ';'.
Se prohibe el acceso no autorizado;
```

Análisis. Se realizan las configuraciones básicas en el S1, se le asigna un nombre, contraseñas, mensaje de acceso no autorizado, etc.

4.4.6 Paso 7: Configurar S3

Tabla 7. Configuración S3

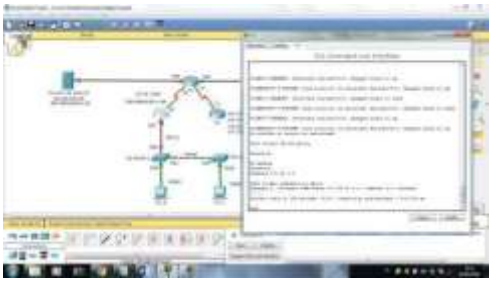
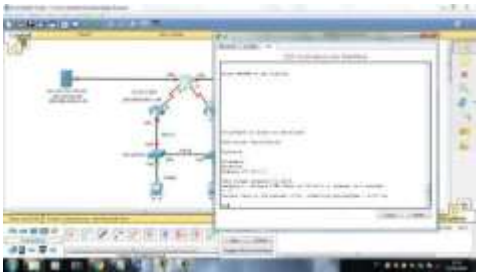
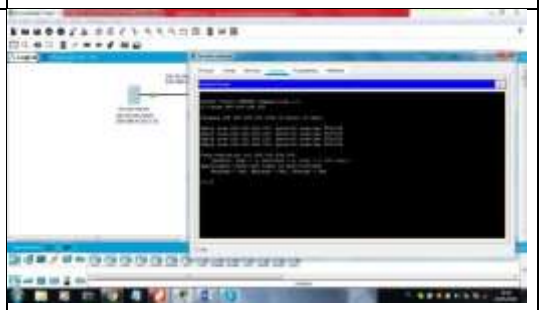
Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	no ip domain-lookup
Nombre del switch	S3
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	
Mensaje MOTD	Se prohíbe el acceso no autorizado.

```
Switch(config)#no ip domain-lookup
Switch(config)#hostname S3
S3(config)#enable secret class
S3(config)#line console 0
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#line vty 0 4
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#exit
S3(config)#
S3(config)#service password-encryption
S3(config)#banner motd ;
Enter TEXT message. End with the character ';'.
Se prohibe el acceso no autorizado;
```

Análisis. Se realizan las configuraciones básicas en el S3, se le asigna un nombre, contraseñas, mensaje de acceso no autorizado, etc.

4.4.7 Paso 8: Verificar la conectividad de la red

Tabla 8. Verificar conectividad

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	 *Figura 2. Ping de R1 a R2*
R2	R3, S0/0/1	172.16.2.1	 *Figura 3. Ping R2 a R3*
PC de Internet	Gateway predeterminado	209.165.200.233	 *Figura 4. Ping Pc Internet a Gateway*

4.5 PARTE 3. Configurar la seguridad del switch, las VLAN y el routing entre VLAN

4.5.1 Paso 1: Configurar S1

Tabla 9. Configuración S1

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para topología para crear y nombrar cada una de las VLAN que se indican.
Asignar la dirección IP de administración.	Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S1 en el diagrama de topología.
Asignar el gateway predeterminado	Asigne la primera dirección IPv4 de la subred como el gateway predeterminado.
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa
Forzar el enlace troncal en la interfaz F0/5	Utilizar la red VLAN 1 como VLAN nativa
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range
Asignar F0/6 a la VLAN 21	
Apagar todos los puertos sin usar	

```
S1(config)#vlan 21
S1(config-vlan)#name CONTABILIDAD
S1(config-vlan)#vlan 23
S1(config-vlan)#name INGENIERIA
S1(config-vlan)#vlan 99
S1(config-vlan)#name ADMINISTRACION
S1(config-vlan)#exit
S1(config)#int vlan 99
S1(config-if)#ip address 192.168.99.2 255.255.255.0
S1(config-if)#no shutdown
S1(config-if)#exit
S1(config)#ip default-gateway 192.168.99.1
S1(config)#int fa0/3
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 1
S1(config-if)#int fa0/5
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 1
```

```
S1(config-if)#int range fa0/1-2, fa0/4, fa0/7-24
S1(config-if-range)#switchport mode access
S1(config-if)#int fa0/6
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 21
S1(config-if)#int range fa0/1-2, fa0/7-23
S1(config-if-range)#shutdown
```

4.5.2 Paso 2: Configurar S3

Tabla 10. Configuración S3

Elemento o tarea de configuración	**Especificación**
Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para topología para crear cada una de las VLAN que se indican Dé nombre a cada VLAN.
Asignar la dirección IP de administración	Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S3 en el diagrama de topología
Asignar el gateway predeterminado.	Asignar la primera dirección IP en la subred como gateway predeterminado.
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range
Asignar F0/18 a la VLAN 21	
Apagar todos los puertos sin usar	

```
S3(config)#vlan 21
S3(config-vlan)#name CONTABILIDAD
S3(config-vlan)#vlan 23
S3(config-vlan)#name INGENIERIA
S3(config-vlan)#vlan 99
S3(config-vlan)#name ADMINISTRACION
S3(config-vlan)#exit
S3(config)#int vlan 99
S3(config-if)#ip address 192.168.99.3 255.255.255.0
S3(config-if)#no shutdown
S3(config-if)#exit
S3(config)#ip default-gateway 192.168.99.1
S3(config)#int fa0/3
```

```
S3(config-if)#switchport mode trunk
S3(config-if)#switchport trunk native vlan 1
S3(config-if)#int range fa0/1-2, fa0/4-24
S3(config-if-range)#switchport mode access
S3(config-if-range)#int fa0/18
S3(config-if)#switchport mode access
S3(config-if)#switchport access vlan 23
```

4.5.3 Paso 3: Configurar R1

Tabla 11. Configuración R1

Elemento o tarea de configuración	**Especificación**
Configurar la subinterfaz 802.1Q .21 en G0/1	Descripción: LAN de Contabilidad Asignar la VLAN 21 Asignar la primera dirección disponible a esta interfaz
Configurar la subinterfaz 802.1Q .23 en G0/1	Descripción: LAN de Ingeniería Asignar la VLAN 23 Asignar la primera dirección disponible a esta interfaz
Configurar la subinterfaz 802.1Q .99 en G0/1	Descripción: LAN de Administración Asignar la VLAN 99 Asignar la primera dirección disponible a esta interfaz
Activar la interfaz G0/1	

```
R1(config)#int g0/1.21
R1(config-subif)#description LAN de CONTABILIDAD
R1(config-subif)#encapsulation dot1Q 21
R1(config-subif)#ip address 192.168.21.1 255.255.255.0
R1(config)#int g0/1.23
R1(config-subif)#description LAN de INGENIERIA
R1(config-subif)#encapsulation dot1Q 23
R1(config-subif)#ip address 192.168.23.1 255.255.255.0
R1(config-subif)#exit
R1(config)#int g0/1.99
R1(config-subif)#description LAN de ADMINISTRACION
R1(config-subif)#encapsulation dot1Q 99
R1(config-subif)#ip address 192.168.99.1 255.255.255.0
R1(config-subif)#exit
```

R1(config)#int g0/1
R1(config-if)#no shutdown

4.5.4 Paso 4: Verificar la conectividad de la red

Tabla 12. Verificación de la conectividad de la red

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	 *Figura 5. Ping de S1 a R1.*
S3	R1, dirección VLAN 99	192.168.99.1	 *Figura 6. Ping de S3 a R1*
S1	R1, dirección VLAN 21	192.168.21.1	 *Figura 7. Ping de S1 a R1*
S3	R1, dirección VLAN 23	192.168.23.1	 *Figura 8. Ping de S3 a R1*

4.6 PARTE 4: Configurar el protocolo de routing dinámico RIPv2

4.6.1 Paso 1: Configurar RIPv2 en el R1

Tabla 13. Configuración RIPv2 en R1

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	
Anunciar las redes conectadas directamente	Asigne todas las redes conectadas directamente.
Establecer todas las interfaces LAN como pasivas	
Desactive la sumarización automática	

```
R1(config)#router rip
R1(config-router)#network 1172.16.1.0
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 g0/1.21
R1(config-router)#passive-interface g0/1.23
R1(config-router)#passive-interface g0/1.99
R1(config-router)#version 2
R1(config-router)#no auto-summary
R1(config-router)#exit
```

4.6.2 Paso 2: Configurar RIPv2 en el R2

Tabla 14. Configurar RIPv2 en R2

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	
Anunciar las redes conectadas directamente	**Nota:** Omitir la red G0/0.
Establecer la interfaz LAN (loopback) como pasiva	
Desactive la sumarización automática.	

```
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 10.10.10.10
R2(config-router)#passive-interface lo0
```

```
R2(config-router)#no auto-summary
R2(config-router)#exit
```

4.6.3 Paso 3: Configurar RIPv2 en el R3

Tabla 15. Configurar RIPv2 en R3

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	
Anunciar redes IPv4 conectadas directamente	
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	
Desactive la sumarización automática.	

```
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 lo4
R3(config-router)#passive-interface lo5
R3(config-router)#passive-interface lo6
R3(config-router)#no auto-summary
R3(config-router)#exit
```

4.6.4 Paso 4: Verificar la información de RIPv2

Tabla 16. Verificación de la información de RIPv2

Pregunta	Respuesta
¿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?	show ip protocols

	 *Figura 9. Comando para visualizar ID del proceso RIP*
¿Qué comando muestra solo las rutas RIP?	show ip route rip  *Figura 10. Comando para visualizar rutas RIP*
¿Qué comando muestra la sección de RIP de la configuración en ejecución?	show ip rip database  *Figura 11. Comando para visualizar sección RIP*

4.7 PARTE 5: Implementar DHCP y NAT para IPv4

4.7.1 Paso 1: Configurar el R1 como servidor de DHCP para las VLAN 21 y 23

Tabla 17. Configuración de R1 como DHCP

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	
Crear un pool de DHCP para la VLAN 21.	Nombre: ACCT Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado
Crear un pool de DHCP para la VLAN 23	Nombre: ENGNR Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado

```
R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20
R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20
R1(config)#ip dhcp pool ACCT
R1(dhcp-config)#dns-server 10.10.10.10
R1(dhcp-config)#domain-name ccna-sa.com
R1(dhcp-config)#default-router 192.168.21.1
R1(dhcp-config)#network 192.168.21.0 255.255.255.0
R1(dhcp-config)#exit
R1(config)#ip dhcp pool ENGNR
R1(dhcp-config)#dns-server 10.10.10.10
R1(dhcp-config)#domain-name ccna-sa.com
R1(dhcp-config)#default-router 192.168.23.1
R1(dhcp-config)#network 192.168.23.0 255.255.255.0
R1(dhcp-config)#exit
```

4.7.2. Paso 2: Configurar la NAT estática y dinámica en el R2

Tabla 18. Configuración NAT en R2

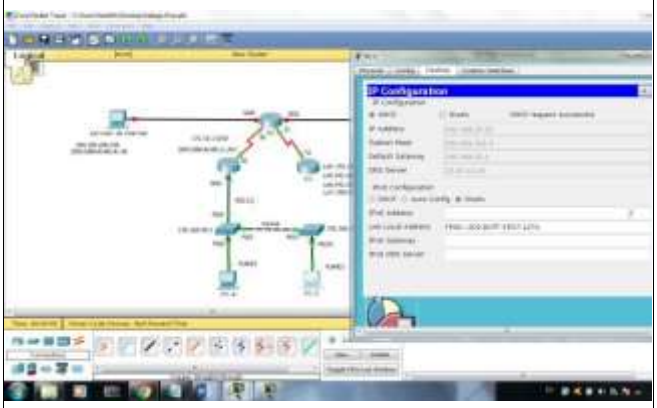
Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	Nombre de usuario: **webuser** Contraseña: **cisco12345** Nivel de privilegio: **15**
Habilitar el servicio del servidor HTTP	
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	
Crear una NAT estática al servidor web.	Dirección global interna: **209.165.200.229**
Asignar la interfaz interna y externa para la NAT estática	
Configurar la NAT dinámica dentro de una ACL privada	Lista de acceso: 1 Permitir la traducción de las redes de Contabilidad y de Ingeniería en el R1 Permitir la traducción de un resumen de las redes LAN (loopback) en el R3
Defina el pool de direcciones IP públicas utilizables.	Nombre del conjunto: **INTERNET** El conjunto de direcciones incluye: **209.165.200.225** – **209.165.200.228**
Definir la traducción de NAT dinámica	

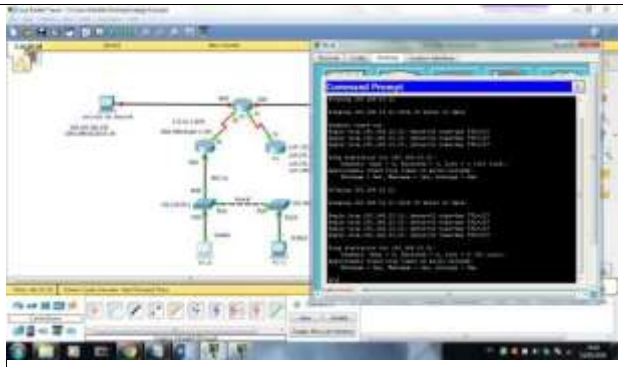
```
R2(config)# username webuser privilege 15 password cisco12345
R2(config)#ip name-server 209.165.200.229
R2(config)#line console 0
R2(config-line)#login local
R2(config-line)#exit
R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255
R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255
R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255
R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask
255.255.255.248
R2(config)#ip nat inside source list 1 pool INTERNET
R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229
```

```
R2(config)#int g0/0
R2(config-if)#ip nat outside
R2(config-if)#int g0/1
R2(config-if)#ip nat inside
R2(config-if)#exit
```

4.7.3 Paso 3: Verificar el protocolo DHCP y la NAT estática

Tabla 19. Verificación DHCP y NAT

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	 *Figura 12. DHCP PC A*
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	 *Figura 13. DHCP PC C*

Verificar que la PC-A pueda hacer ping a la PC-C **Nota:** Quizá sea necesario deshabilitar el firewall de la PC.	 *Figura 14. Ping PC A*
Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.229) Iniciar sesión con el nombre de usuario **webuser** y la contraseña **cisco12345**	Server reset connection

4.8 PARTE 6: Configurar NTP

Tabla 20. Configuración NTP

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	**5 de marzo de 2016, 9 a. m.**
Configure R2 como un maestro NTP.	Nivel de estrato: **5**
Configurar R1 como un cliente NTP.	Servidor: **R2**
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	
Verifique la configuración de NTP en R1.	

R2#clock set 09:00:00 MARCH 5 2016
R2(config)#ntp master 5
R1(config)#ntp server 172.16.1.2

R1#sh ntp associations

R1#sh ntp status

R1#sh clock

4.9 PARTE 7: Configurar y verificar las listas de control de acceso (ACL)

4.9.1 Paso 1: Restringir el acceso a las líneas VTY en el R2

Tabla 21. Restricción de acceso a VTY en R2

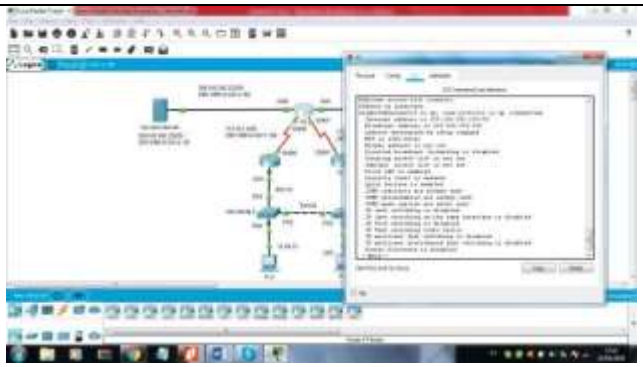
Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	Nombre de la ACL: **ADMIN-MGT**
Aplicar la ACL con nombre a las líneas VTY	
Permitir acceso por Telnet a las líneas de VTY	
Verificar que la ACL funcione como se espera	

```
R2(config)#ip access-list standard ADMIN-MGT
R2(config-std-nacl)#permit host 172.16.1.1
R2(config-std-nacl)#exit
R2(config)#line vty 0 4
R2(config-line)#access-class ADMIN-MGT in
R2(config-line)#exit
```

4.9.1 Paso 2: Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente

Tabla 22. Comando CLI para ACLs

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	 *Figura 15. Comando sh access-list*
Restablecer los contadores de una lista de acceso	clear access-list counters
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	show ip interface

	 *Figura 16. Comando show ip interface*
¿Con qué comando se muestran las traducciones NAT?	sh ip nat translations  *Figura 17. Comando show ip nat translations* **Nota:** Las traducciones para la PC-A y la PC-C se agregaron a la tabla cuando la computadora de Internet intentó hacer ping a esos equipos en el paso 2. Si hace ping a la computadora de Internet desde la PC-A o la PC-C, no se agregarán las traducciones a la tabla debido al modo de simulación de Internet en la red.
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	clear ip nat translation *

5 DESARROLLO ESCENARIO 2

5.1 ESCENARIO

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 red. Este escenario plantea el uso de OSPF como protocolo de enrutamiento, considerando que se tendrán rutas por defecto redistribuidas; así mismo, 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.

5.2 TOPOLOGÍA

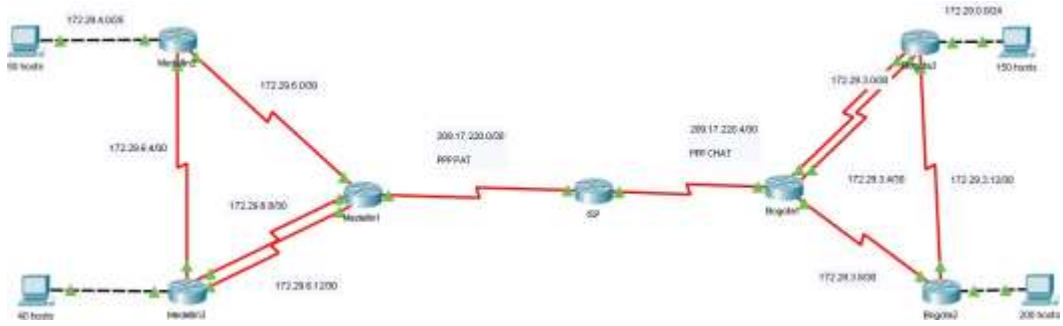


Figura 18. Topología Escenario 2

5.3 PRE-CONFIGURACIÓN

5.3.1 Paso 1: Realizar las rutinas de diagnóstico y dejar los equipos listos para su configuración (asignar nombres de equipos, asignar claves de seguridad, etc).

Router (Config)#: Hostname (nombre del router) Para asignar nombre al router.
Router (Config)#: Hostname ISP
Router (Config)#: Hostname Bogota1
Router (Config)#: Hostname Bogota2
Router (Config)#: Hostname Bogota3
Router (Config)#: Hostname Medellin1
Router (Config)#: Hostname Medellin2
Router (Config)#: Hostname Medellin3

Configuración de contraseñas

Router (Config)# enable secret cisco
Router (Config)# line console 0
Router (Config-line)# password cisco
Router (Config-line)# login
Router (Config)# line vty 0 4 (password para la linea de terminal virtual)
Router (Config-line)# password cisco
Router (Config-line)# login

5.3.2 Paso 2: Realizar la conexión física de los equipos con base en la topología de red

5.4 PARTE 1: Configuración del enrutamiento

5.4.1 Paso 1: Configurar el enrutamiento en la red usando el protocolo OSPF versión 2, declare la red principal, desactive la sumarización automática.

5.4.2 Paso 2: 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.

A continuación, se demuestra el desarrollo de los 2 pasos anteriores:

Medellin1 (config)# router ospf 10
Medellin1 (config-router)# router-id 1.1.1.1
Medellin1 (config-router)# auto-cost reference-bandwidth 1000

```
Medellin1 (config-router)# network 172.29.6.0 0.0.0.3 area 0
Medellin1 (config-router)# network 172.29.6.8 0.0.0.3 area 0
Medellin1 (config-router)# network 172.29.6.12 0.0.0.3 area 0
Medellin1 (config-router)# network 209.17.220.0 0.0.0.3 area 0
Medellin2(config)#router ospf 10
Medellin2(config-router)#router-id 1.1.1.2
Medellin2(config-router)#auto-cost reference-bandwidth 1000
Medellin2(config-router)#network 172.29.6.4 0.0.0.3 area 0
Medellin2(config-router)#network 172.29.6.0 0.0.0.3 area 0
Medellin2(config-router)#network 172.29.4.0 0.0.0.127 area 0
Medellin3(config)#router ospf 10
Medellin3(config-router)#router-id 1.1.1.3
Medellin3(config-router)#network 172.29.6.4 0.0.0.3 area 0
Medellin3(config-router)#network 172.29.6.8 0.0.0.3 area 0
Medellin3(config-router)#network 172.29.6.12 0.0.0.3 area 0
Medellin3(config-router)#network 172.29.4.128 0.0.0.127 area 0
Medellin3(config-router)#auto-cost reference-bandwidth 1000
Bogota1 (config)# router ospf 10
Bogota1 (config-router)# router-id 2.2.2.2
Bogota1 (config-router)# auto-cost reference-bandwidth 1000
Bogota1 (config-router)# network 172.29.3.0 0.0.0.3 area 0
Bogota1 (config-router)# network 172.29.3.4 0.0.0.3 area 0
Bogota1 (config-router)# network 172.29.3.8 0.0.0.3 area 0
Bogota1 (config-router)# exit
Bogota2(config)#router ospf 10
Bogota2(config-router)#router-id 2.2.2.1
Bogota2(config-router)#auto-cost reference-bandwidth 1000
Bogota2(config-router)#network 172.29.3.12 0.0.0.3 area 0
Bogota2(config-router)#network 172.29.3.8 0.0.0.3 area 0
Bogota2(config-router)#network 172.29.1.0 0.0.0.255 area 0
Bogota3(config)#router ospf 10
Bogota3(config-router)#router-id 2.2.2.3
Bogota3(config-router)#network 172.29.3.4 0.0.0.3 area 0
Bogota3(config-router)#network 172.29.3.0 0.0.0.3 area 0
Bogota3(config-router)#network 172.29.3.12 0.0.0.3 area 0
Bogota3(config-router)#network 172.29.0.0 0.0.0.255 area 0
Bogota3(config-router)#auto-cost reference-bandwidth 1000
```

Al implementar el protocolo OSPF v2 para enrutamiento, simplifica bastante el proceso ya que al tener subredes que tienen en común los primeros 16 bits, se puede crear una “super red” que haga la cobertura a todas las demás, esto sucede en ambos routers principales.

Paso 3: 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.

MEDELLIN			1	28	64	32	16	8	4	2	1	128	64	32	16	8	4	2	1
172.29.4.0	172	29	0		0	0	0	0	1	0	0	0	0	0	0	0	0	0	0
172.29.4.128	172	29	0		0	0	0	0	1	0	0	1	0	0	0	0	0	0	0
172.29.6.0	172	29	0		0	0	0	0	1	1	0	0	0	0	0	0	0	0	0
172.29.6.12	172	29	0		0	0	0	0	1	1	0	0	0	0	0	1	1	0	0
172.29.6.8	172	29	0		0	0	0	0	1	1	0	0	0	0	0	1	0	0	0
172.29.6.4	172	29	0		0	0	0	0	1	1	0	0	0	0	0	0	1	0	0
172.29.4.0	**172**	**29**	**0**		**0**	**0**	**0**	**0**	**4**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**

Tabla 24. Sumarización Red Bogotá

BOGOTA			128	64	32	16	8	4	2	1	128	64	32	16	8	4	2	1
172.29.1.0	172	29	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0
172.29.3.0	172	29	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0
172.29.0.0	172	29	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
172.29.3.8	172	29	0	0	0	0	0	0	1	1	0	0	0	0	1	0	0	0
172.29.3.4	172	29	0	0	0	0	0	0	1	1	0	0	0	0	0	1	0	0
172.29.3.12	172	29	0	0	0	0	0	0	1	1	0	0	0	0	1	1	0	0
172.29.0.0	**172**	**29**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**

Tabla 23. Sumarización Red Medellin

Utilizando el comando anterior, determinamos a la tabla de enrutamiento, cuál es la mejor ruta para un paquete de destino.
Se crean las rutas estáticas para ambas subredes desde ISP.

ISP (config)#ip route 172.29.0.0 255.255.252.0 209.17.220.6
ISP (config)#ip route 172.29.0.0 255.255.252.0 209.17.220.1
ISP (config)# router ospf 15
ISP (config-router)# network 209.17.220.2 0.0.0.0 area 0
ISP (config-router)# default-information originate
ISP (config-router)# network 209.17.220.5 0.0.0.0 area 0

5.5 PARTE 2: Tabla de Enrutamiento.

Paso 1: Verificar la tabla de enrutamiento en cada uno de los routers para comprobar las redes y sus rutas

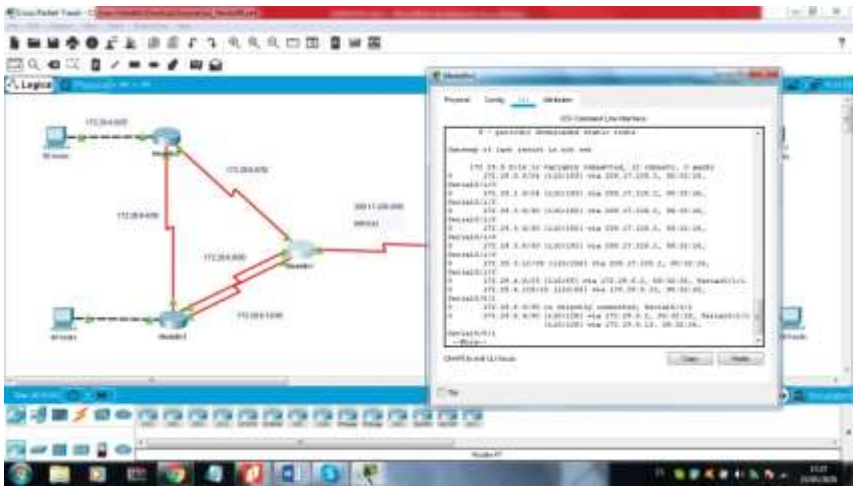


Figura 19. Tabla de enrutamiento- Medellin1

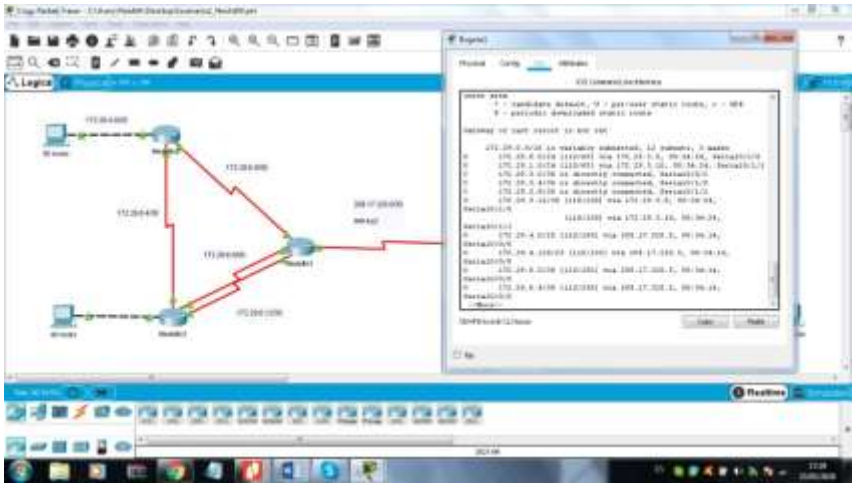


Figura 20. Tabla de enrutamiento-Bogota1

Paso 2: Verificar el balanceo de carga que presentan los routers.

Los routers poseen dos rutas posibles para llegar a las redes lejanas esto se puede observar en las imágenes del punto anterior donde se ven las rutas de los equipos.

Paso 3: 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 con la misma identificación y estructura lógica en la red, se observa tienen la misma distribución, debido a la distribución redundante de las redes Bogotá y Medellín. Para el router Bogota1 y Medellin1 (misma identificación) tienen similitud, lo mismo sucede para Bogota2 - Medellin2 y Bogota3 - Medellin3.

Paso 4: Los routers Medellín2 y Bogotá2 también presentan redes conectadas directamente y recibidas mediante OSPF.

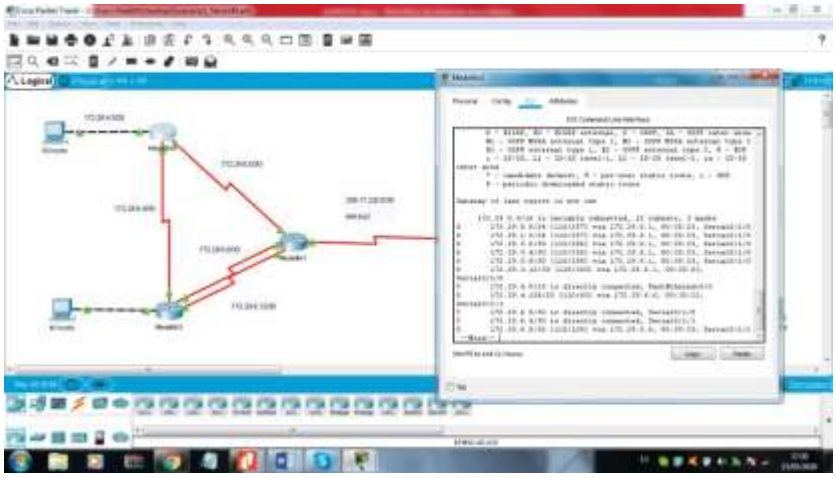


Figura 21. Tabla de enrutamiento- Medellin2

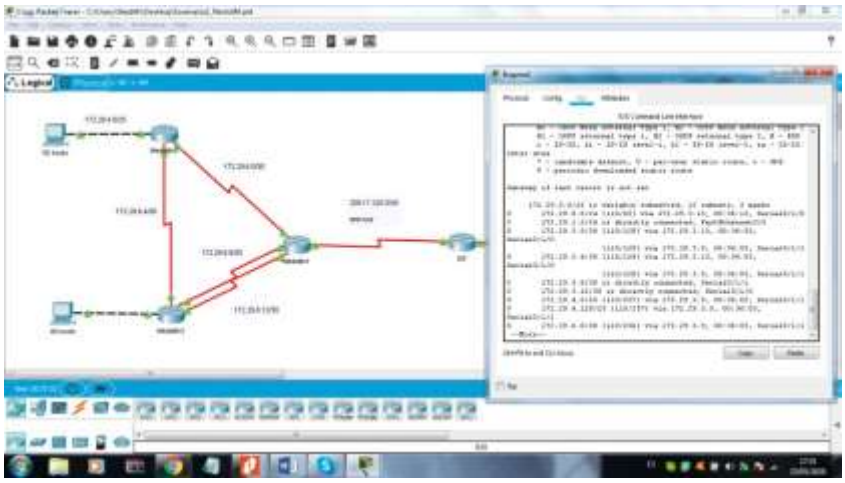


Figura 22. Tabla de enrutamiento-Bogota2

Paso 5: Las tablas de los routers restantes deben permitir visualizar rutas redundantes para el caso de la ruta por defecto.

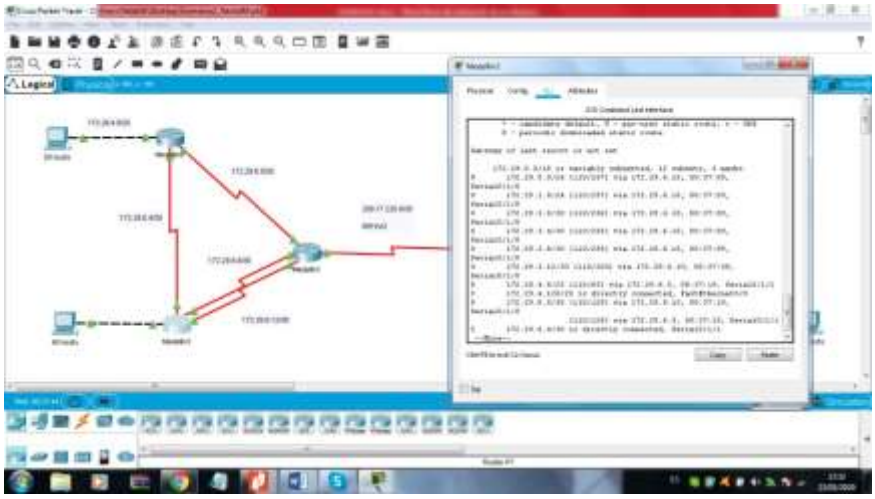


Figura 23. Tabla de enrutamiento- Medellin3

Paso 6: El router ISP solo debe indicar sus rutas estáticas adicionales a las directamente conectadas.

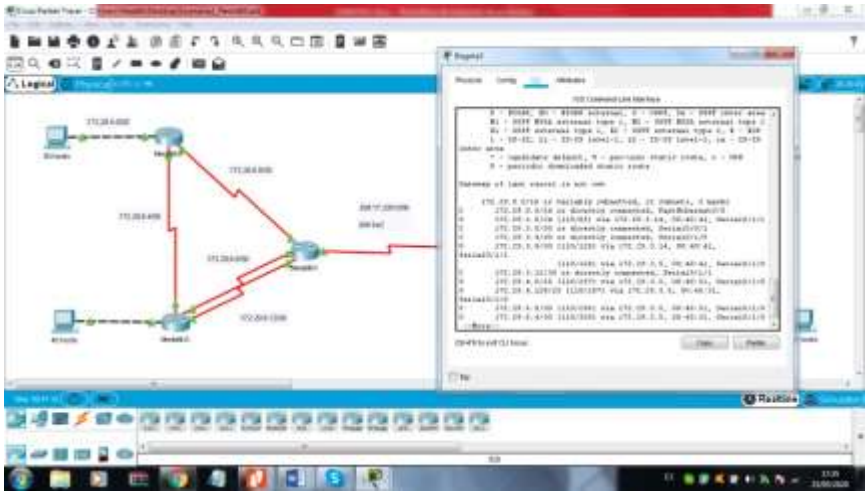


Figura 24. Tabla de enrutamiento- Bogota3

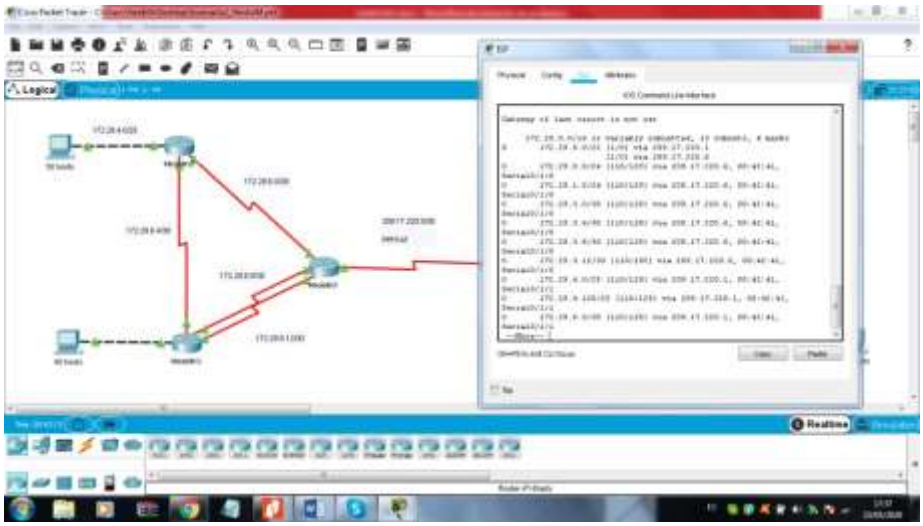


Figura 25. Tabla de enrutamiento- ISP

5.6 PARTE 3: Deshabilitar la propagación del protocolo OSPF.

Paso 1: 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 25. Lista de interfaces deshabilitadas propagación OSPF

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

5.7 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.

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.

En las imágenes anteriores se evidencia de la información que cada router posee frente al protocolo en mención.

5.8 PARTE 5: Configurar encapsulamiento y autenticación PPP.

Paso 1: Según la topología se requiere que el enlace Medellín1 con ISP sea configurado con autenticación PAP.

```
Medellin1(config)# interface se0/1/0
Medellin1(config-if)# encapsulation ppp
ISP(config)#interface s0/1/1
ISP(config-if)#encapsulation ppp

Medellin1(config)#username ISP secret class
Medellin1(config)#interface s0/1/0
Medellin1(config-if)#ppp authentication pap
Medellin1(config-if)#ppp pap sent-username Medellin1 password

ISP(config)#username Medellin1 secret cisco
ISP(config)#interface s0/1/1
ISP(config-if)#ppp authentication pap
ISP(config-if)#ppp pap sent-username ISP password class
```

Paso 2: El enlace Bogotá1 con ISP se debe configurar con autenticación CHAP.

```
ISP(config)#interface s0/1/0
ISP(config-if)#encapsulation ppp

Bogota1(config)#interface s0/0/0
Bogota1(config-if)#encapsulation ppp

ISP(config)#username Bogota1 secret cisco
ISP(config)#interface s0/1/0
ISP(config-if)#ppp authentication chap
```

```
Bogota1(config)#username ISP secret cisco
Bogota1(config)#interface s0/0/0
Bogota1(config-if)#ppp authentication chap
```

5.9 PARTE 6: Configuración de PAT.

Paso 1: 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.

Paso 2: 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, como diferente puerto.

```
Medellin1(config)#access-list 1 permit 172.29.4.0 0.0.3.255
Medellin1(config)#ip nat inside source list 1 interface s0/1/0 overload
Medellin1(config)#interface s0/0/0
Medellin1(config-if)#ip nat inside
Medellin1(config-if)#exit
Medellin1(config)#interface s0/0/1
Medellin1(config-if)#ip nat inside
Medellin1(config-if)#exit
Medellin1(config)#interface s0/1/1
Medellin1(config-if)#ip nat inside
Medellin1(config-if)#exit
Medellin1(config)#interface s0/1/0
Medellin1(config-if)#ip nat outside
Medellin1(config-if)#exit
Medellin1(config)#end
```

Paso 3: 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, como diferente puerto.

```
Bogota1(config)#access-list 2 permit 172.29.0.0 0.0.3.255
Bogota1(config)#ip nat inside source list 2 interface s0/0/0 overload
Bogota1(config)#interface s0/0/1
Bogota1(config-if)#ip nat inside
```

```
Bogota1(config-if)#exit
Bogota1(config)#interface s0/1/0
Bogota1(config-if)#ip nat inside
Bogota1(config-if)#exit
Bogota1(config)#interface s0/1/1
Bogota1(config-if)#ip nat inside
Bogota1(config-if)#exit
Bogota1(config)#interface s0/0/0
Bogota1(config-if)#ip nat outside
Bogota1(config-if)#exit
Bogota1(config)#end
```

5.10 PARTE 7: Configuración del servicio DHCP.

Paso 1: Configurar la red Medellín2 y Medellín3 donde el router Medellín 2 debe ser el servidor DHCP para ambas redes Lan.

```
Medellin2(config)#ip dhcp excluded-address 172.29.4.1
Medellin2(config)#ip dhcp excluded-address 172.29.4.129
Medellin2(config)#ip dhcp excluded-address 172.29.4.127
Medellin2(config)#ip dhcp excluded-address 172.29.4.255

Medellin2(config)#
Medellin2(config)#ip dhcp pool MEDELLIN2
Medellin2(dhcp-config)#network 172.29.4.0 255.255.255.128
Medellin2(dhcp-config)#default-router 172.29.4.1
Medellin2(dhcp-config)#exit
Medellin2(config)#ip dhcp pool MEDELLIN3
Medellin2(dhcp-config)#network 172.29.4.128 255.255.255.128
Medellin2(dhcp-config)#default-router 172.29.4.129
Medellin2(dhcp-config)#exit
```

Paso 2: El router Medellín3 deberá habilitar el paso de los mensajes broadcast hacia la IP del router Medellín2.

```
Medellin3(config)#interface fa0/0
Medellin3(config-if)#ip helper-address 172.29.6.5
Medellin3(config-if)#end
```

Se evidencia que el servicio DHCP está funcionando en la red LAN de Medellin3.

Paso 3: Configurar la red Bogotá2 y Bogotá3 donde el router Bogotá2 debe ser el servidor DHCP para ambas redes Lan.

```
Bogota2(config)#ip dhcp excluded-address 172.29.0.1
Bogota2 (config)#ip dhcp excluded-address 172.29.1.1
Bogota2 (config)#ip dhcp excluded-address 172.29.1.255
Bogota2 (config)#ip dhcp excluded-address 172.29.0.255
Bogota2 (config)#
Bogota2 (config)#ip dhcp pool BOGOTA2
Bogota2 (dhcp-config)#network 172.29.1.0 255.255.255.0
Bogota2 (dhcp-config)#exit
Bogota2 (config)#ip dhcp pool BOGOTA3
Bogota2 (dhcp-config)#network 172.29.0.0 255.255.255.0
Bogota2 (dhcp-config)#default-router 172.29.0.1
Bogota2 (dhcp-config)#exit
```

Paso 4: Configure el router Bogotá3 para que habilite elpaso de los mensajes Broadcast hacia la IP del router Bogotá2.

```
Bogota3(config)#interface fa0/0
Bogota3(config-if)#ip helper-address 172.29.3.14
Bogota3(config-if)#end
```

Se demuestra que el PC de la red LAN Bogotá3 está obteniendo la dirección ip de acuerdo con las reglas establecidas.

Para terminar, se realiza un envío de paquetes mediante un ping entre el PC de Medellín3 hacia el ISP y se hace ping entre el PC de Bogotá3 y el router Medellín1.

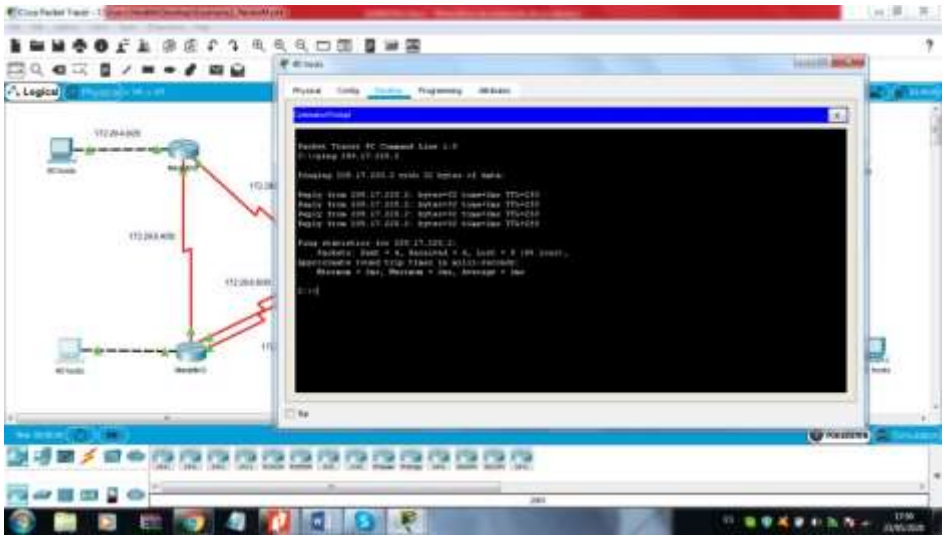


Figura 26. PC Medellin3 hacia ISP

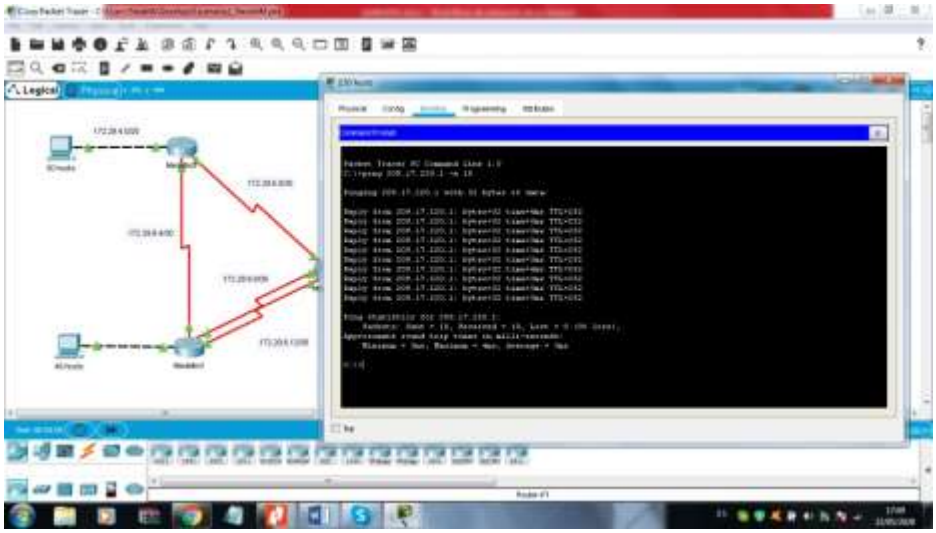


Figura 27. PC Bogotá3 y Router Medellín1

CONCLUSIONES

Del trabajo anterior se puede concluir que: Los escenarios propuestos me permitieron investigar sobre la forma en cómo se podían resolver ya que todo lo que vi durante el curso lo puse en práctica en estos escenario , se me presentaron problemas de configuración como es el caso del código para realizar el diagnostico de vecino ya que no me mostraba cuales eran los equipos que se relacionaban , para poder resolver esto tuve que investigar y darme cuenta que tenía que activar el diagnostico en los equipos para así poder ver los cuándo digitara el código sh cdp neighbors. Por otra parte aplicar los códigos para conocer los enrutamientos, realizar conexiones telnet y entrar a los equipos y digitar el código ping para ver si había conexión entre equipos me pareció muy interesantes porque pude ver cómo funcionaba cada uno de ellos y su función al momento de configurar una red.

Para el escenario 1 se realizaron las siguientes conclusiones:

-Se realizaron las respectivas rutinas de diagnósticos
-Se realizaron los respectivos enrutamientos de la red usando el protocolo RIP.
-Se realizó configuración de enrutamiento de los routers con ruta hacia la ISP.
-Se verifico el balanceo de carga de los routers
-Se deshabilito la propagación del protocolo RIP
-Se verifico la base de datos RIP de cada routers, donde se evidencia todas las rutas hacia cada red
-Se configuro el encapsulamiento y autenticación PPP
-Se configuro las respectivas PAT
-Se configuro el servicio DHCP
-A cada proceso se realizó su respectivo Ping de

verificación Para el escenario 2 se realizó las respectivas:

-Se realizó la configuración IP para cada uno de los dispositivos que hacen parte del escenario.
-Se configuro el protocolo de enrutamiento OSPFv2
-Se realizó la respectiva verificación de OSPF
-Se realize la Visualization Del OSPF Process ID, Router ID, Address summarizations, Routing Networks, and passive interfaces configured en cada router.

-Se configuraron las respectivas VLANs, Puertos troncales, puertos de acceso, encapsulamiento, Inter-VLAN Routing y Seguridad en los Switches acorde a la topología de red establecida.
-Se deshabilito el DNS lookup en el Switch 3
-Se realizó la respectiva asignación de dirección IP a los switches acorde a los lineamientos
-Se desactivaron todas interfaces que no utilizaron en la
red Se Implementó DHCP and NAT for IPv4
-Se configuró R1 como servidor DHCP para las VLANs 30 y 40.
-Se Reservaron las primeras 30 direcciones IP de las VLAN 30 y 40 para configuraciones estáticas.
-Se configuro la NAT en R2 para permitir que los host puedan salir a internet
-Se verifico los procesos de comunicación y re direccionamiento de tráfico en los routers mediante el uso de Ping y Traceroute.

Por ultimo puedo concluir que aprenda mucho y me gusto la metodología aplicada en estos ejercicios ya que pusieron aprueba mi capacidad de análisis de entender cuál era las mejores opciones para resolver los escenarios propuestos.

BIBLIOGRAFÍA

CISCO. Acceso a la red. Fundamentos de Networking. {En línea}. {2017}. Disponible en: (https://static-courseassets.s3.amazonaws.com/ITN50ES/module2/index.html#4.0.1.1)

CISCO. Configuración y conceptos básicos de Switching. Principios de Enrutamiento y Conmutación. {En línea}. {2017}. Disponible en:

(https://static-courseassets.s3.amazonaws.com/RSE50ES/module2/index.html#2.0.1.1)

CISCO. Exploración de la red. Fundamentos de Networking. {En línea}. {2017}. Disponible en:

(https://static- courseassets.s3.amazonaws.com/ITN50ES/module1/index.html#1.0.1.1)

CISCO. OSPF de una sola área. Principios de Enrutamiento y Conmutación. {En línea}. {2017}. Disponible en:

(https://static-courseassets.s3.amazonaws.com/RSE50ES/module8/index.html#8.0.1.1)

CISCO. SubNetting. Fundamentos de Networking. {En línea}. {2017}. Disponible en:

(https://static-courseassets.s3.amazonaws.com/ITN50ES/module9/index.html#9.0.1.1)

UNAD. Diseño y configuración de redes con Packet Tracer. {En línea}. {2017}. Disponible en: (https://1drv.ms/u/s!AmlJYeiNT1IhgCT9VCtl_pLtPD9)