SOLUCIÓN DE DOS ESTUDIOS DE CASO BAJO EL USO DE TECNOLOGÍA CISCO

CCNA1 & CCNA2

RONALD MAURICIO BERMUDEZ GONZALEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA
DIPLOMADO DE PROFUNDIZACION CISCO
Bogotá D.C., Mayo 15 de 2020

SOLUCIÓN DE DOS ESTUDIOS DE CASO BAJO EL USO DE TECNOLOGÍA CISCO

CCNA1 & CCNA2

RONALD MAURICIO BERMUDEZ GONZALEZ

JOSE IGNACIO CARDONA
TUTOR

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA
DIPLOMADO DE PROFUNDIZACION CISCO
Bogotá D.C., Mayo 15 de 2020

Nota de aceptación

_____

_____

_____

_____
Presidente del jurado

_____
Jurado

_____
Jurado

Bogotá D.C., Mayo 15 de 2020

CONTENIDO

LISTADO DE TABLAS

TABLA DE FIGURAS

RESUMEN

La Universidad Nacional Abierta y a Distancia, durante el proceso de aprendizaje del diplomado de profundización CISCO, Nos permite el uso del software de simulación CISCO Packet Tracer, el cual es un programa que nos permite realizar la simulación de las redes, con este se busca experimentar los diferentes parámetros de configuración de una topología de red, que evidenciaremos a lo largo de nuestra profesión.

Palabras clave: CCNA1, CCNA2, CISCO.

INTRODUCCIÓN

A través del presente documento se busca dar solución a las dos pruebas de habilidades relacionadas con el diplomado de profundización CISCO, en tal sentido, se dará respuesta a los interrogantes relacionados con ruteo dinámico RIPv2, protocolo DHCP, traducción de direcciones estáticas y dinámicas (NAT), listas de control de acceso (ACL) y el protocolo de tiempo cliente/servidor (NTP).

En la primera topología se busca implementar direccionamiento DHCP y ruteo dinámico RIPv2, se implementan subredes encapsulamiento dot1q y el uso de conexiones troncales y de acceso entre los swiches y el Router; en el mismo sentido, se implementa en esta topología el uso de 2 servidores, 1 de internet y el otro 1 servidor web.

Para la segunda topología, el ruteo dinámico se realiza a través de OSPF allí se propone una topología de comunicación tipo WAN entre dos ciudades Bogotá y Medellín, la comunicación se efectúa a través de OSPF y entre el ISP y los servidores Bogota1 y Medellín1 la comunicación se realiza con encapsulamiento PPP, uno de los routers de cada ciudad sirve como servidor DHCP para dar direcciones IPv4 a los host de las 4 redes LAN.

DESARROLLO DE LOS DOS ESCENARIOS

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.
Topología

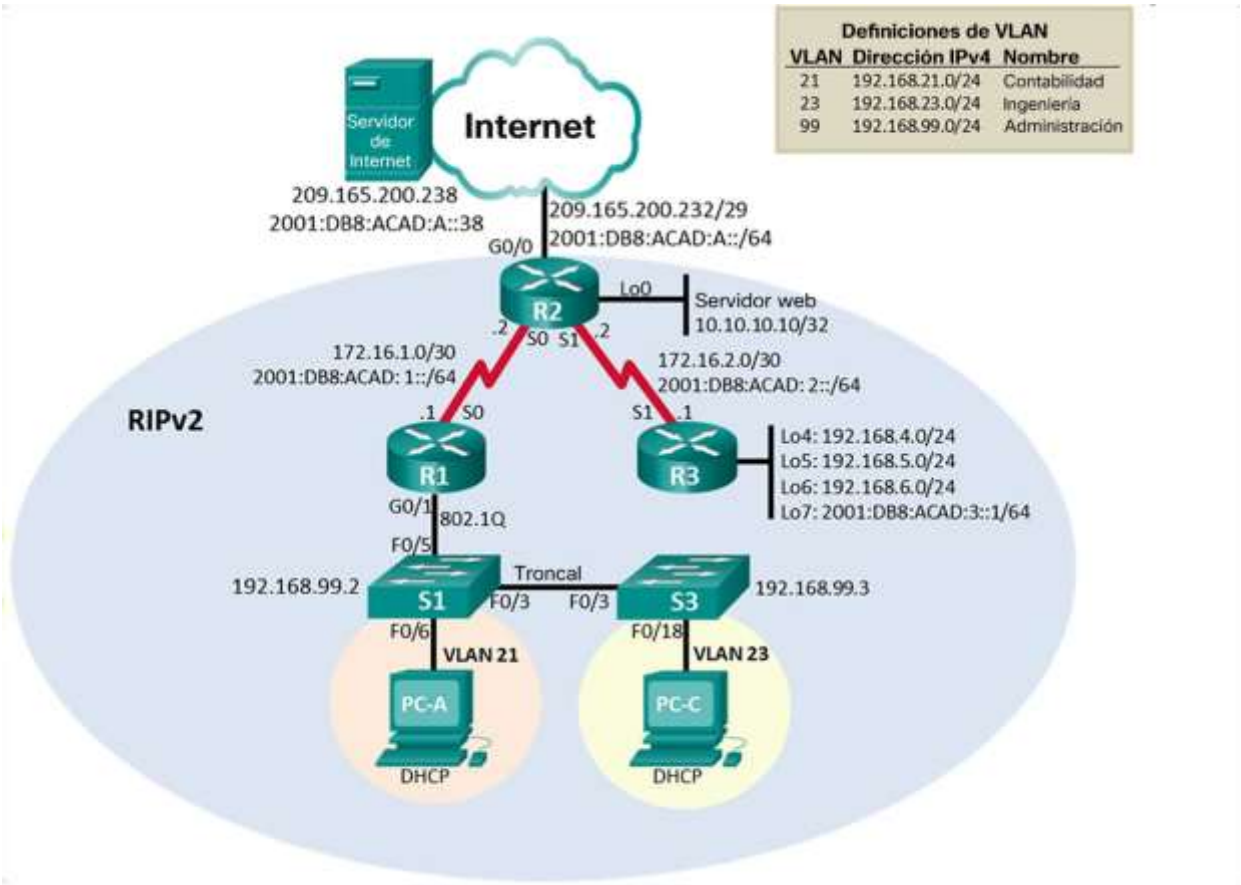


Figura 1. Topología Prueba CCNA 1

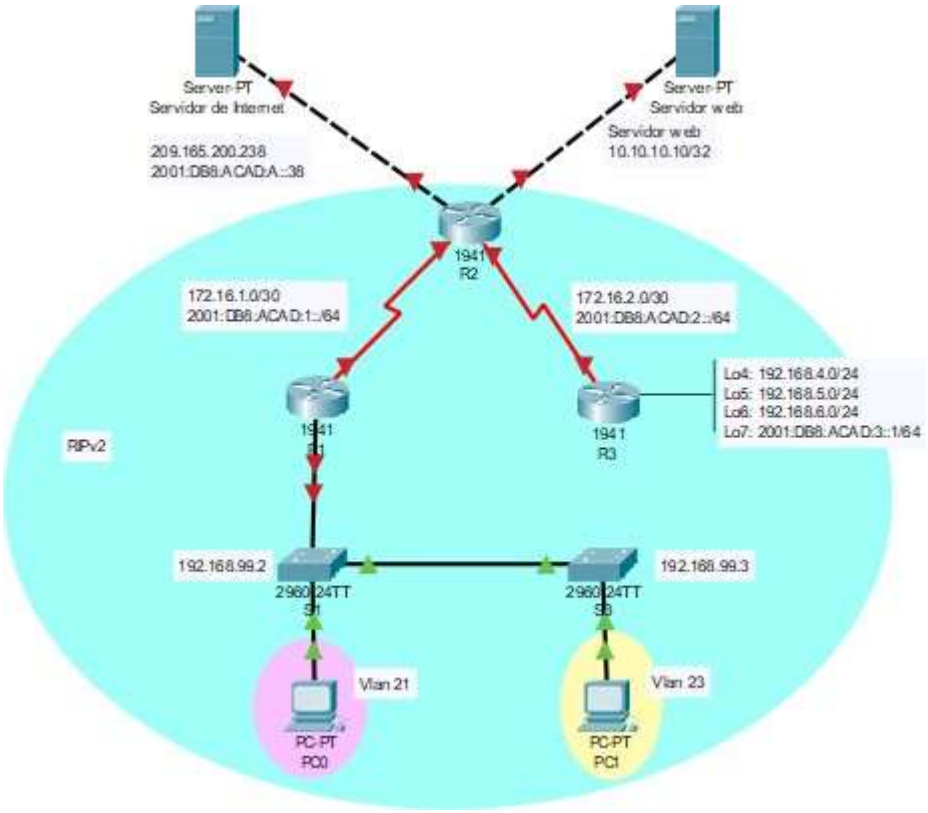


Figura 2. Topología diseñada en Packet Tracer

1.1. Inicializar dispositivos

Para inicializar los dispositivos es necesario borrar las configuraciones existentes en los Router y Switch existentes en la topología, con base a los comandos descritos en la Tabla 1.

Tabla 1. Inicializar dispositivo

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	Erase startup-config Este comando permite realizar el borrado del NVRAM donde está alojada la configuración inicial.
Volver a cargar todos los routers	Reload Este comando reinicializa el dispositivo y aplica el borrado efectuado en el paso anterior.

Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Erase startup-config Delete vlan.date El primer comando elimina la NVRAM del Switch, quitando contraseñas y configuraciones iniciales. El segundo comando elimina las Vlan existentes en el Switch dejando únicamente la Vlan1.
Volver a cargar ambos switches	Reload Este comando reinicializa el Switch aplicando el borrado de NVRAM y de Vlan.
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Show flash Aquí despliega la información contenida en la memoria flash del dispositivo.

1.2. Configurar los parámetros básicos de los dispositivos

1.2.1. Configurar el servidor de Internet

Se realiza la configuración inicial acorde a las direcciones dispuestas en la topología original, se omite el uso de la nube toda vez que se conecta el dispositivo a la interfaz Gigabit0/0.

Tabla 2. Configuración servidor 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	209.165.200.225
Dirección IPv6/subred	2001:DB8:ACAD:A::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:A::1

1.2.2. Configurar R1

Se procede a configurar el Router R1 con la información dispuesta en la topología inicial.

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 La configuración de la contraseña se realiza ingresando el comando Enable secret Class
Contraseña de acceso a la consola	Cisco Se ingresa a Line Console 0 y allí se ingresan los comandos Password Cisco – Contraseña establecida Login – Logueo para que tome el cambio Logging synchronous – Evita el ruido que puede interrumpir algunos comandos
Contraseña de acceso Telnet	Cisco Su configuración se realiza dentro de Line vty 0 4, los puertos 0 al 4 con usados para conexión Telnet, aunque el dispositivo tiene puertos hasta el 15.
Cifrar las contraseñas de texto no cifrado	service password-encryption este comando codifica las contraseñas e impide que con el comando Show running config se pueda detectar las contraseñas ingresadas
Mensaje MOTD	Se prohíbe el acceso no autorizado. Para ingresar el mensaje se incluye el comando Banner motd #Se prohíbe el acceso no autorizado!# Siendo el símbolo # usado para iniciar y terminar el mensaje

Interfaz S0/0/0	Establezca la descripción **Description Acceso a Vlan** Dirección IPv4 **172.16.1.1 255.255.255.252** Dirección IPv6 **2001:db8:acad:1::1/64** **Clock rate 128000** Activar la interfaz **No shutdown**
Rutas predeterminadas	Ruta IPv4 predeterminada de S0/0/0 **Ip route 0.0.0.0 0.0.0.0 172.16.1.2** Ruta IPv6 predeterminada de S0/0/0 **Ipv6 route 2001:db8:acad:1::2/64** Con estos comandos se busca identificar todas las redes que no estén en la tabla de ruteo y enviarlas a través del siguiente salto, aplica para ambos tipos de direccionamiento IPv4 e IPv6.

Nota: Todavía no configure G0/1.

1.2.3. Configurar R2

Se procede a configurar el Router R2 con la información dispuesta en la topología inicial, la configuración aplicada se explica en el Router R1.

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	service password-encryption
Habilitar el servidor HTTP	Se añade un dispositivo tipo “Servidor” y se configura con la ip respectiva, su Gateway y se activan los servicios HTTP y DNS.
Mensaje MOTD	Se prohíbe el acceso no autorizado.

Interfaz S0/0/0	Establezca la descripción **Description Link to R1** Dirección IPv4 **172.16.1.2 255.255.255.252** Dirección IPv6 **2001:db8:acad:1::2/64** Activar la interfaz **No shutdown** El comando No shutdown sirve para activar la interfaz
Interfaz S0/0/1	Establecer la descripción **Description Link to R3** Dirección IPv4 **172.16.2.2 255.255.255.252** Dirección IPv6 **2001:db8:acad:2::2/64** Establecer la frecuencia de reloj en 128000. Activar la interfaz **No shutdown**
Interfaz G0/0 (simulación de Internet)	Establecer la descripción. **Description Link to Internet Server** Dirección IPv4 **209.165.200.225 255.255.255.248** Dirección IPv6 **2001:db8:acad:a::1/64** Activar la interfaz
Interfaz loopback 0 (servidor web simulado) Se configura en la **interfaz G0/1**	Establecer la descripción **Description Link to Web Server** Dirección IPv4 – **10.10.10.1 255.255.255.0**
Ruta predeterminada	Configure una ruta IPv4 predeterminada de G0/0. **Ip route 0.0.0.0 0.0.0.0 g0/0** Configure una ruta IPv6 predeterminada de G0/0. **Ipv6 route ::/0 g0/0**

Se omite el inicio dado que es similar al de R1

1.2.4. Configurar R3

Se procede a configurar el Router R3 con la información dispuesta en la topología inicial.

Tabla 4. 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	Services password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado.
Interfaz S0/0/1	Establecer la descripción **Description Link to R2** Dirección IPv4 **172.16.2.1 255.255.255.252** Dirección IPv6 **2001:DB8:ACAD:2::1/64** Activar la interfaz **No shutdown**
Interfaz loopback 4	Dirección IPv4 **192.168.4.1 255.255.255.0**
Interfaz loopback 5	Dirección IPv4 **192.168.5.1 255.255.255.0**
Interfaz loopback 6	Dirección IPv4 **192.168.6.1 255.255.255.0**
Interfaz loopback 7	Dirección IPv6 **2001:DB8:ACAD:3::1/64**
Rutas predeterminadas	

1.2.5. Configurar S1

Se procede a configurar el Switch S1 con la información dispuesta en la topología inicial.

Tabla 5. Configuracion 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	Service password-encryption

Mensaje MOTD	Se prohíbe el acceso no autorizado.

1.2.6. Configurar el S3

Se procede a configurar el Switch S1 con la información dispuesta en la topología inicial.

Tabla 6. 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	service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado.

1.3. Verificar la conectividad de la red

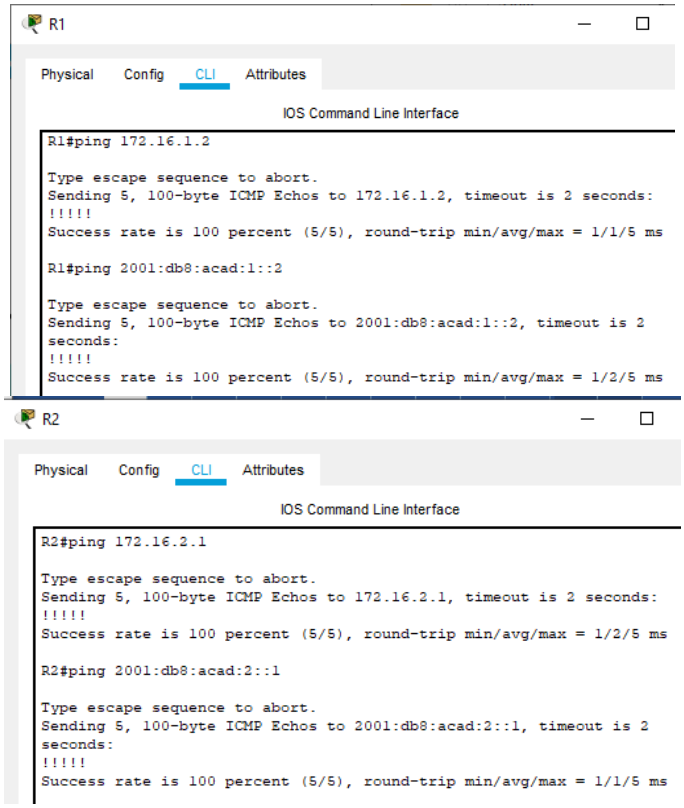
Se hace uso del comando ping para verificar conexión

Se usa la siguiente tabla para incorporar las direcciones IP y dispositivos desde el cual se realiza el ping.

Tabla 7. Información para hacer ping

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2 2001:db8:acad:1::2	Exitosos
R2	R3, S0/0/1	172.16.2.1 2001:db8:acad:2::1	Exitosos
PC de Internet	Gateway predeterminado	209.165.200.225 2001:db8:acad:a::1	Exitosos

Nota: Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.



En estos casos los Router están comunicándose bien con aquellos Router que fungen como vecinos y están conectados directamente en su tabla de ruteo.

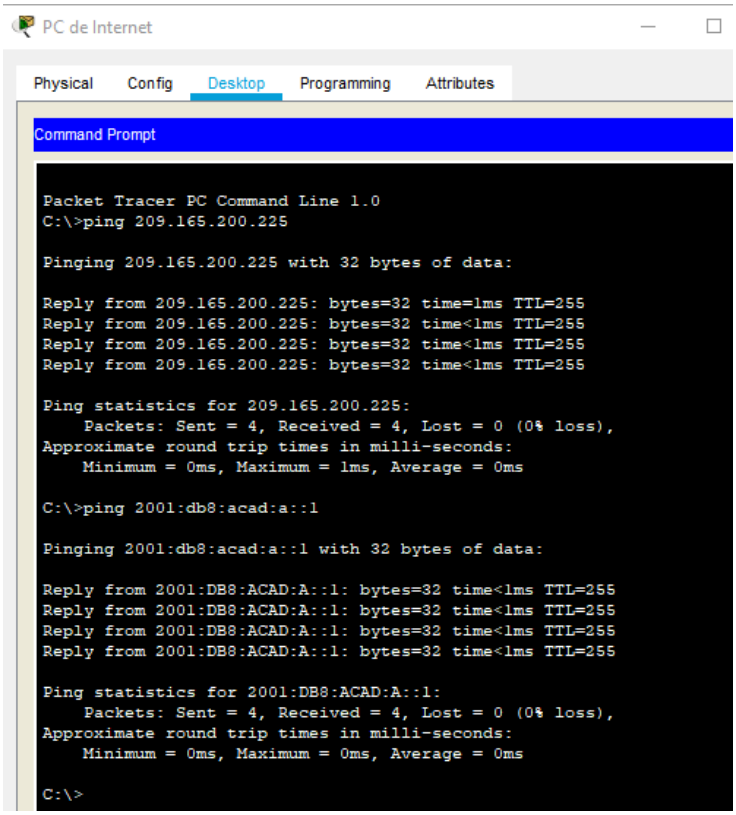


Figura 3. Evidencia ping exitoso

Como se observa la configuración es correcta pues hay comunicación entre los dispositivos y el Router.

2. Configurar la seguridad del switch, las VLAN y el routing entre VLAN

2.1. Configurar S1

Se realiza la configuración con base a la topología y dentro de los parámetros descritos en la siguiente tabla:

Tabla 8. Configuración VLAN S1

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	Config t Vlan 21 Name Contabilidad Vlan 23 Name Ingenieria Vlan 99 Name Administracion Aquí se asignan los nombres y puerto de cada una de las Vlan configuradas
Asignar la dirección IP de administración.	Dirección IPv4 a la VLAN de administración. **192.168.99.2** Como se dijo anteriormente acá se aplica la dirección de la VLAN 99 asignada al dispositivo.
Asignar el gateway predeterminado	Asigne la primera dirección IPv4 de la subred como el gateway predeterminado. **Ip default-gateway 192.168.21.1**
Forzar el enlace troncal en la interfaz F0/3	Int fa0/3 Switchport mode trunk Switchport trunk native vlan 1 Se define conexión troncal entre el Switch y el Router, esta servirá para comunicar también el Switch S3
Forzar el enlace troncal en la interfaz F0/5	Int fa0/5 Switchport mode trunk Switchport trunk native vlan 1 Se asigna a esa conexión troncal la Vlan nativa o Vlan 1
Configurar el resto de los puertos como puertos de acceso	Interface range fa0/1-2, fa0/4, fa0/7-24 Switchport mode Access

Asignar F0/6 a la VLAN 21	Interface fa0/6 Switchport mode Access Switchport access vlan 21 Se da modo de acceso a la interfaz que va hacia el host,
Apagar todos los puertos sin usar	Interface range fa0/1-2, fa0/4, fa0/7-24 Shutdown Se apagan administrativamente los puertos no usados.

2.2. Configurar el S3

Se realiza la configuración con base a la topología y dentro de los parámetros descritos en la siguiente tabla:

Tabla 9. Configuración VLAN S3

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	Config t Vlan 21 Name Contabilidad Vlan 23 Name Ingenieria Vlan 99 Name Administracion
Asignar la dirección IP de administración	Dirección IPv4 a la VLAN de administración. **192.168.99.3**
Asignar el gateway predeterminado.	Asignar la primera dirección IP en la subred como gateway predeterminado. **Ip default-gateway 192.168.23.1**
Forzar el enlace troncal en la interfaz F0/3	Int fa0/3 Switchport mode trunk Switchport trunk native vlan 1

Configurar el resto de los puertos como puertos de acceso	Interface range fa0/1-2, fa0/4-24 Switchport mode Access
Asignar F0/18 a la VLAN 23	Int fa0/18 Switchport Access Vlan 23
Apagar todos los puertos sin usar	Int range fa0/1-3, fa0/4-17, fa0/19-24 Shutdown

2.3. Configurar R1

Se realiza la configuración con base a la topología y dentro de los parámetros descritos en la siguiente tabla:

Tabla 10. Configuración subinterfaces R1

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	Config t Int g0/1.21 Description Lan de Contabilidad Ip add 192.168.21.1 255.255.255.0 Aquí se configura la subinterfaz que sale por la interfaz física Gigabit 0/1 y donde se dará acceso a la VLAN 21.
Configurar la subinterfaz 802.1Q .23 en G0/1	Int g0/1.23 Description Lan de Ingenieria Ip add 192.168.23.1 255.255.255.0 Se da acceso a la VLAN 23 creando su subinterfaz por la misma interfaz física.
Configurar la subinterfaz 802.1Q .99 en G0/1	Int g0/1.99 Description Lan de Administracion Ip add 192.168.99.1 255.255.255.0 Se asigna acceso a VLAN99
Activar la interfaz G0/1	Int g0/0 No shutdown Se activa la interfaz y sus subinterfaces

2.4. Verificar la conectividad de la red

Se hace uso del comando ping para verificar conexión

Se usa la siguiente tabla para incorporar las direcciones IP y dispositivos desde el cual se realiza el ping.

Tabla 11. Información para hacer ping

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	Exitoso
S3	R1, dirección VLAN 99	192.168.99.1	
S1	R1, dirección VLAN 21	192.168.21.1	Exitoso
S3	R1, dirección VLAN 23	192.168.23.1	

```
S1#ping 192.168.99.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
S1#ping 192.168.21.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.21.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
S3#ping 192.168.99.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
S3#ping 192.168.23.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.23.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
```

Figura 4. Evidencia ping exitoso desde Switch S1 y S2 hacia Router R1

Los ping anteriores, evidencian que los Switch fueron bien configurados pues tienen conexión con sus Gateway predeterminados para las VLAN 21, 23 y 99.

3. Configurar el protocolo de routing dinámico RIPv2

3.1. Configurar RIPv2 en el R1

Para configurar realizar la configuración RIPv2 en R1 se tendrá en cuenta la información que brinda la topología y los datos de la siguiente tabla:

Tabla 12. Configuración RIPv2 en R1

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	Config t Router rip version 2
Anunciar las redes conectadas directamente	Network 172.16.1.0 Network 192.168.21.0 Network 192.168.23.0 Network 192.168.99.0 Estas son las redes que están conectadas directamente y se describen para que los otros dispositivos puedan conocerlas a través del protocolo RIP
Establecer todas las interfaces LAN como pasivas	Passive-interface g0/1 La interfaz que conecta la red LAN se establece como pasiva.
Desactive la sumarización automática	No auto-summary Este comando sirve para no sumarizar las redes que tiene, sobre todo cuando son no contiguas

3.2. Configurar RIPv2 en el R2

Para configurar realizar la configuración RIPv2 en R2 se tendrá en cuenta la información que brinda la topología y los datos de la siguiente tabla:

Tabla 13. Configuración RIPv2 en R2

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	Config t Router rip version 2
Anunciar las redes conectadas directamente	Network 172.16.1.0 Network 172.16.2.0 **Se omiten las redes conectadas mediante puertos Gigabit que conectan los servidores**
Establecer todas las interfaces LAN (Gigabit) como pasivas	Passive-interface g0/1 Passive-interface g0/0
Desactive la sumarización automática	No auto-summary

3.3. Configurar RIPv2 en el R3

Para configurar realizar la configuración RIPv2 en R2 se tendrá en cuenta la información que brinda la topología y los datos de la siguiente tabla:

Tabla 14. Configuración RIPv2 en R3

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	Config t Router rip version 2
Anunciar redes IPv4 conectadas directamente	Network 172.16.2.0 Network 192.168.4.0 Network 192.168.5.0 Network 192.168.6.0
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	Passive-interface lo4 Passive-interface lo5 Passive-interface lo6
Desactive la sumarización automática.	No auto-summary

3.4. Verificar la información de RIP

Verifique que RIP esté funcionando como se espera. Introduzca el comando de CLI adecuado para obtener la siguiente información:

Tabla 15. Preguntas de verificación protocolor 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
¿Qué comando muestra solo las rutas RIP?	Show ip route rip
¿Qué comando muestra la sección de RIP de la configuración en ejecución?	Debug ip rip

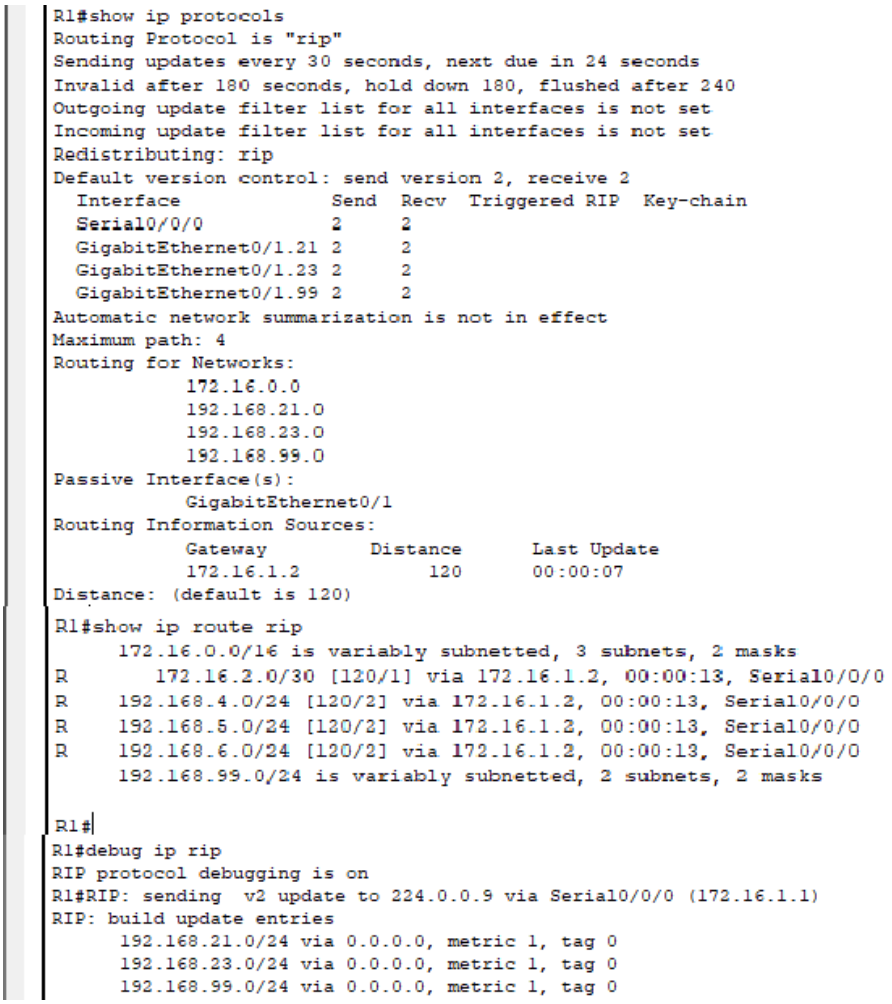


Figura 5. Evidencia ejecución comandos de verificación de configuración RIPv2

Como ser observa el protocolo activado en el Router R1 es RIP, muestra cuales son sus redes conectadas por ruteo y cuales interfaces tiene en modo pasivo, nos brinda información acerca del Gateway o puerta de enlace predeterminada.

El comando show ip rute nos muestra las redes conectadas a través de protocolo RIP, y finalmente el debug ip route nos muestra las conexiones de Gateway de las Vlan.

4. Implementar DHCP y NAT para IPv4

4.1. Configurar el R1 como servidor de DHCP para las VLAN 21 y 23

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 16. Configuración DHCP para R1

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	Config t Ip dhcp excluded-add 192.168.21.1 192.168.21.20 Este comando excluye las primeras 20 IP con el fin de no asignarlas a través del protocolo DHCP.
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	Ip dhcp excluded-add 192.168.23.1 192.168.23.20 Sucede lo mismo en este caso, solo que aplicable a las direcciones IP de la vlan 23.

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 **Int g0/1.21** **Ip dhcp pool ACCT** **Dns-server 10.10.10.10** **Ip domain-name ccna.com** **Ip dhcp pool ACCT** **Default-router 192.168.21.1** **Network 192.168.21.0 255.255.255.0** **Exit** Se define la configuración del servidor DHCP, temas como la interfaz a la cual se aplica, nombre, nombre del dominio, router por defecto y la red contiene el gateway prederminado.
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 **Int g0/1.23** **Ip dhcp pool ENGNR** **Dns-server 10.10.10.10** **Ip domain-name ccna.com** **Ip dhcp pool ENGNR** **Default-router 192.168.23.1** **Network 192.168.23.0 255.255.255.0** **Exit**

4.2. Configurar la NAT estática y dinámica en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla 17. Configuración NAT para R2

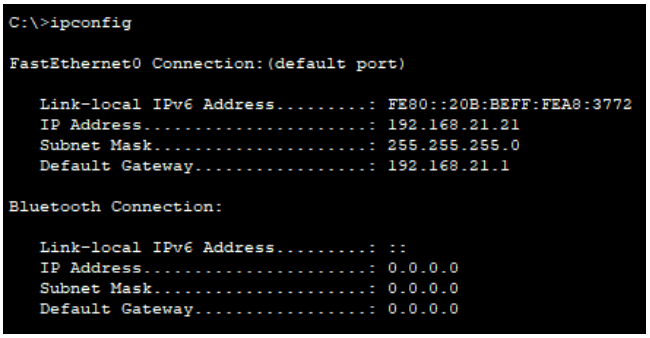
Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	Nombre de usuario: **webuser** Contraseña: **cisco12345** Nivel de privilegio: **15** **Config t** **User webuser privilege 15 secret cisco12345**
Habilitar el servicio del servidor HTTP	Este paso se omite dado que la topología incluye un servidor HTTP
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	**access-list 1 permit 192.168.21.0 0.0.0.255** **access-list 1 permit 192.168.23.0 0.0.0.255** **access-list 1 permit 192.168.99.0 0.0.0.255** como se observa se está dando acceso a las listas de direcciones de cada VLAN.
Crear una NAT estática al servidor web.	Dirección global interna: **209.165.200.229** Esta es la dirección con la cual se traducirán las direcciones a través del protocolo NAT
Asignar la interfaz interna y externa para la NAT estática	**Ip nat inside source static 10.10.10.10 209.165.200.229** Aquí se establecen la dirección interna 10.10.10.10 y su traducción de salida 209.165.200.229
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 **Ip nat inside source list 1 pool ACCT** **Ip nat inside source list 1 pool ENGNR** 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** **Ip nat pool INTERNET 2019.165.200.225 209.165.200.228 netmask 255.255.255.248**
Definir la traducción de NAT dinámica	La traducción de NAT dinámica consiste en el uso de IP privadas para dar acceso a internet, blindando la red para que host que no pertenecen a la misma puedan ingresar, su uso se basa en una tabla de direcciones IP (Privadas) asignadas a los host cuando realizan tráfico fuera de la red para acceso a internet, esta IP asignada se valida antes para verificar que no este siendo usada.

4.3. Verificar el protocolo DHCP y la NAT estática

Utilice las siguientes tareas para verificar que las configuraciones de DHCP y NAT estática funcionen de forma correcta. Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

Tabla 18. Verificación de configuración DHCP y NAT estática

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	La dirección IP asignada es 192.168.21.21 con netmask 255.255.255.0 

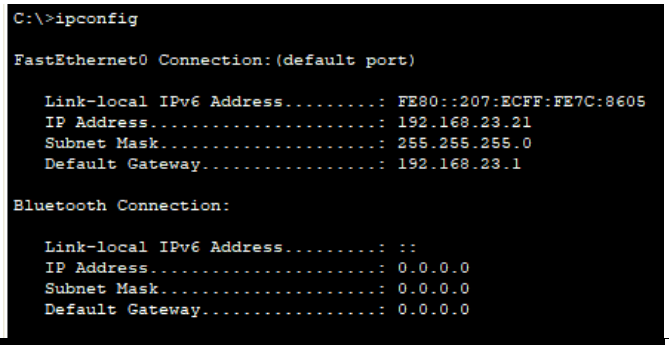
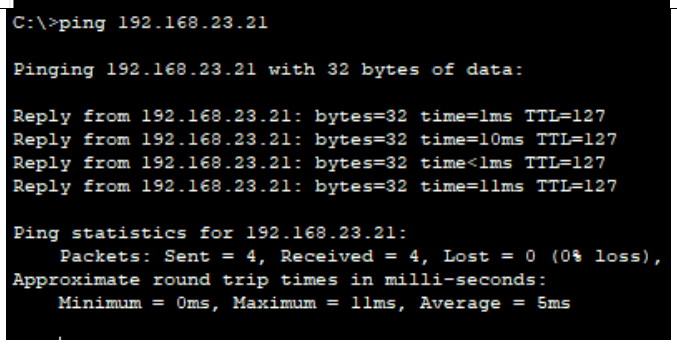
```
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Link-local IPv6 Address.....: FE80::20B:BEFF:FEA8:3772
   IP Address.....: 192.168.21.21
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: 192.168.21.1

Bluetooth Connection:

   Link-local IPv6 Address.....: ::
   IP Address.....: 0.0.0.0
   Subnet Mask.....: 0.0.0.0
   Default Gateway.....: 0.0.0.0
```

Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	La dirección IP asignada es 192.168.23.21 con netmask 255.255.255.0 
Verificar que la PC-A pueda hacer ping a la PC-C **Nota:** Quizá sea necesario deshabilitar el firewall de la PC.	
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**	No me fue posible desarrollar este punto dado que el equipo no me tomó la configuración de manera apropiada y por lo tanto no hubo el resultado esperado.

Con lo anterior se evidencia en su mayoría que el protocolo de asignación de direcciones DHCP está funcionando correctamente pues bajo los parámetros establecidos para cada pool de direcciones, fueron asignadas a los dispositivos host configurados para tal fin.

5. Configurar NTP

Tabla 19. Configuración NTP

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	**5 de marzo de 2016, 9 a. m.** **Clock set 09:00:00 March 5 2016**

Configure R2 como un maestro NTP.	Nivel de estrato: **5** **Ntp master 5**
Configurar R1 como un cliente NTP.	Servidor: **R2** **Ntp server 172.16.1.2**
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	**Ntp update-calendar**
Verifique la configuración de NTP en R1.	**Show ntp associations**

El servicio NTP permite sincronizar el tiempo entre los dispositivos de una misma red, uno de los Router se configura como maestro y en él se define la fecha y hora deseada para sincronizar los demás dispositivos, así al activar en el otro Router su sincronización del calendario todos los dispositivos estarán usando los mismos datos de fecha y hora establecidos en el Master. Cuando no existe este master el tiempo se actualiza con base a la información de la pila del dipositivo.

6. Configurar y verificar las listas de control de acceso (ACL)

6.1. Restringir el acceso a las líneas VTY en el R2

Tabla 20. Configuración de restricción de acceso a líneas 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** **ip access-list standar ADMIN-MGT** permit host 172.16.1.1 se informa cual es el host permitido para conexión a través de Telnet.
Aplicar la ACL con nombre a las líneas VTY	**Line vty 0 4** Se aplica la configuración ACL o lista de control de acceso a las líneas vty 0 4 asociadas a la conexión Telnet.
Permitir acceso por Telnet a las líneas de VTY	**Access-class ADMIN-MGT in** Brinda acceso a las lineas vty

Verificar que la ACL funcione como se espera	**show access-list**

6.2. Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente

Tabla 21. Tabla de comandos CLI

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	**show access-list**
Restablecer los contadores de una lista de acceso	**clear ip 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 Access-list**
¿Con qué comando se muestran las traducciones NAT?	**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 traslation ***

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 red.

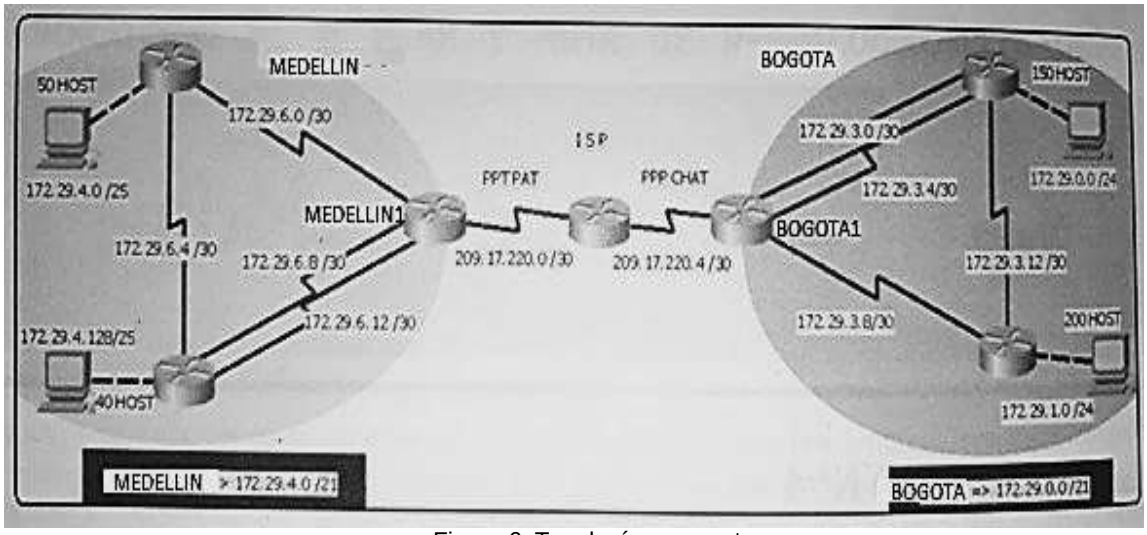


Figura 6. Topología propuesta

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.

Desarrollo
Como trabajo inicial se debe realizar lo siguiente.

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

Respuesta: en primer lugar, es necesario explicar que es el protocolo OSPF, es un protocolo de enrutamiento dinámico que tiene como función principal recolectar la información para armar las tablas de routing o ruteo.

Este protocolo mantiene 3 tablas: Ruteo: identificando el camino para alcanzar una red distante; adyacencias: que permite identificar a los vecinos para los intercambios OSPF; y topología: usada para conocer la topología completa de la red pues permite conocer sus rutas y el camino para alcanzar esas redes.

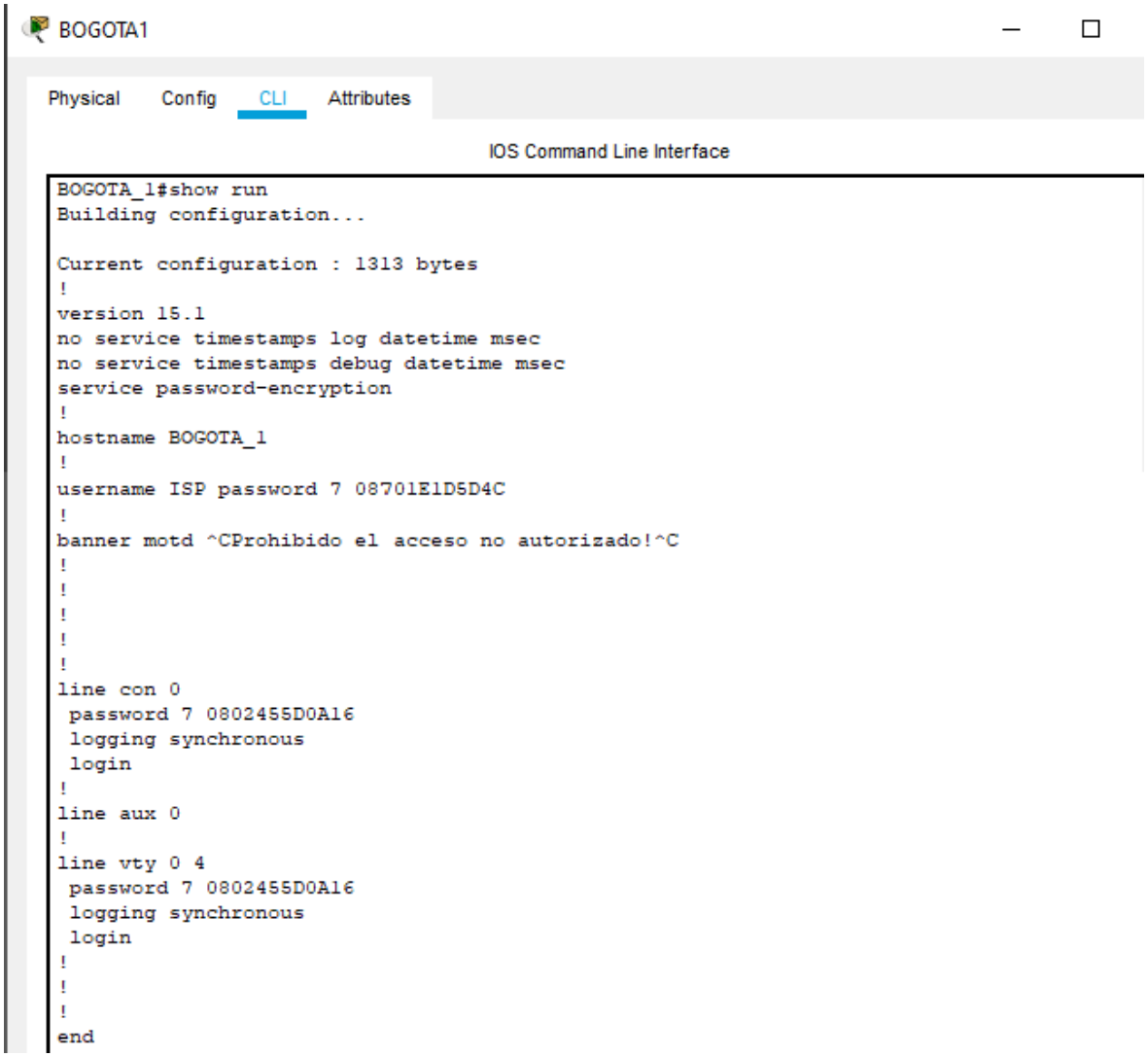


Figura 7. Evidencia configuración dispositivo con nombre, mensaje y claves

Realizar la conexión física de los equipos con base en la topología de red

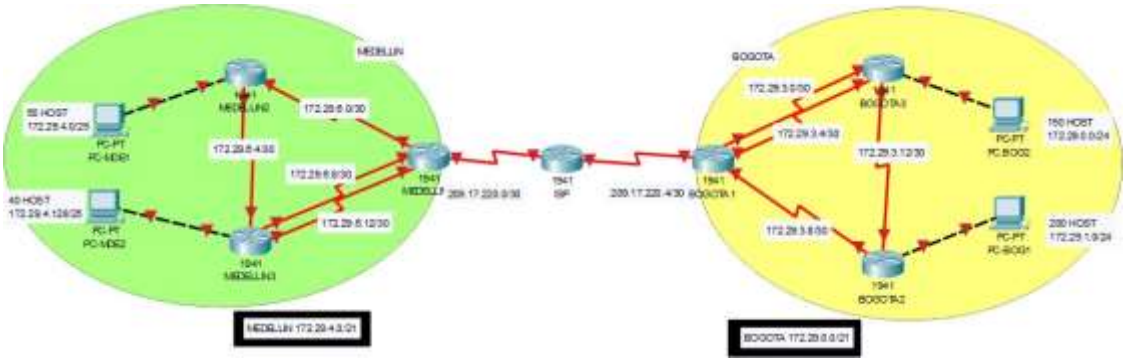


Figura 8. Topología diseñada

Configurar la topología de red, de acuerdo con las siguientes especificaciones.

7.1. Configuración del enrutamiento

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

Los routers Bogota1 y Medellín1 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.

```
     172.29.0.0/16 is variably subnetted, 6 subnets, 2 masks
C       172.29.3.0/30 is directly connected, Serial0/1/0
L       172.29.3.1/32 is directly connected, Serial0/1/0
C       172.29.3.4/30 is directly connected, Serial0/1/1
L       172.29.3.5/32 is directly connected, Serial0/1/1
C       172.29.3.8/30 is directly connected, Serial0/0/0
L       172.29.3.9/32 is directly connected, Serial0/0/0
     209.17.220.0/24 is variably subnetted, 3 subnets, 2 masks
C       209.17.220.4/30 is directly connected, Serial0/0/1
C       209.17.220.5/32 is directly connected, Serial0/0/1
L       209.17.220.6/32 is directly connected, Serial0/0/1
S*   0.0.0.0/0 [1/0] via 209.17.220.5

BOGOTA_1(config)#
```

Figura 9. Evidencia configuración ruta por defecto hacia ISP

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.

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

Verificar el balanceo de carga que presentan los routers.

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.

```
BOGOTA_2(config)#do show ip protocol

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 172.29.3.13
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.29.3.8 0.0.0.3 area 2
    172.29.3.12 0.0.0.3 area 2
    172.29.1.0 0.0.0.255 area 2
  Routing Information Sources:
    Gateway         Distance      Last Update
    172.29.3.13           110      00:00:36
    172.29.3.14           110      00:00:36
    209.17.220.6          110      00:03:47
  Distance: (default is 110)

BOGOTA_2(config)#
```

Figura 10. Evidencia configuración protocolo OSPF Router BOGOTA_2

Mediante el comando show ip protocol se evidencia el tipo de protocolo aplicado en cada uno de los Router, para el ejemplo se evidencia la configuración OSPF del Router Bogotá_2.

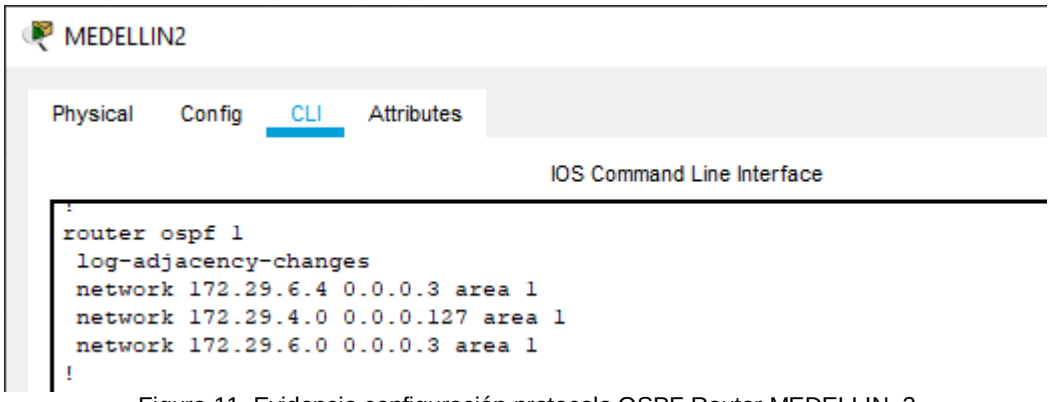


Figura 11. Evidencia configuración protocolo OSPF Router MEDELLIN_2

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.

7.2. Deshabilitar la propagación del protocolo OSPF.

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.

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

Las interfaces que no figuran en la tabla anterior, han sido configuradas como passive interface.

7.3. 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.

```
MEDELLIN_1#show ip protocol

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 209.17.220.2
  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 1
    172.29.6.8 0.0.0.3 area 1
    172.29.6.12 0.0.0.3 area 1
    209.17.220.0 0.0.0.3 area 1
  Passive Interface(s):
    Serial0/0/0
  Routing Information Sources:
    Gateway         Distance      Last Update
    172.29.6.5           110      00:05:40
    172.29.6.14          110      00:05:31
    209.17.220.2         110      00:29:15
  Distance: (default is 110)
```

Figura 12. Evidencia interfaces pasivas para no propagar OSPF

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.

Router	Tipo conexión	Dirección	Destino
MEDELLIN_1	LOCAL	172.29.6.2	MEDELLIN_2
MEDELLIN_1	LOCAL	172.29.6.9	MEDELLIN_3
MEDELLIN_1	LOCAL	172.29.6.13	MEDELLIN_3
MEDELLIN_1	LOCAL	209.17.220.2	ISP
MEDELLIN_1	OSPF	172.29.4.0 vía 172.29.6.1	PC-MED1 POR MEDELLIN_2
MEDELLIN_1	OSPF	172.29.4.128 vía 172.29.6.14	PC-MED2 POR MEDELLIN_3
MEDELLIN_1	OSPF	172.29.6.4 vía 172.29.6.1	MEDELLIN_3 POR MEDELLIN_2
MEDELLIN_1	OSPF	172.29.6.4 vía 172.29.6.14	MEDELLIN_2 POR MEDELLIN_3
MEDELLIN_1	STATIC	0.0.0.0 vía 209.17.220.1	CUALQUIER RED POR ISP
MEDELLIN_2	LOCAL	172.29.4.1	PC-MED1
MEDELLIN_2	LOCAL	172.29.6.1	MEDELLIN_1
MEDELLIN	LOCAL	172.29.6.5	MEDELLIN_3

_2			
MEDELLIN_2	OSPF	172.29.6.8 vía 172.29.6.5	MEDELLIN_1 POR MEDELLIN_3
MEDELLIN_2	OSPF	172.29.6.8 vía 172.29.6.2	MEDELLIN_3 POR MEDELLIN_1
MEDELLIN_2	OSPF	172.29.6.12 vía 172.29.6.5	MEDELLIN_1 POR MEDELLIN_3
MEDELLIN_2	OSPF	172.29.6.12 vía 172.29.6.2	MEDELLIN_3 POR MEDELLIN_1
MEDELLIN_2	OSPF	209.17.220.0 vía 172.29.6.2	ISP POR MEDELLIN_1
MEDELLIN_2	OSPF	172.29.4.128 vía 172.29.6.5	PC-MED2 POR MEDELLIN_3
MEDELLIN_3	LOCAL	172.29.4.129	PC-MED2
MEDELLIN_3	LOCAL	172.29.6.5	MEDELLIN_2

MEDELLIN_3	LOCAL	172.29.6.10	MEDELLIN_1
MEDELLIN_3	LOCAL	172.29.6.14	MEDELLIN_1
MEDELLIN_3	OSPF	172.29.4.0 VÍA 172.29.6.5	PC-MED1 POR MEDELLIN_2
MEDELLIN_3	OSPF	172.29.6.0 vía 172.29.6.9	MEDELLIN_2 POR MEDELLIN_1
MEDELLIN_3	OSPF	172.29.6.0 vía 172.29.6.5	MEDELLIN_1 POR MEDELLIN_2
MEDELLIN_3	OSPF	209.17.220.0 vía 172.29.6.9	ISP POR MEDELLIN_1
ISP	LOCAL	209.17.220.1	MEDELLIN_1
ISP	LOCAL	209.17.220.5	BOGOTA_1
BOGOTA_1	LOCAL	172.29.3.1	BOGOTA_3
BOGOTA_1	LOCAL	172.29.3.5	BOGOTA_3
BOGOTA_1	LOCAL	172.29.3.9	BOGOTA_2
BOGOTA_1	LOCAL	209.17.220.6	ISP
BOGOTA_1	OSPF	172.29.0.0 vía 172.29.3.2	PC-BOG2 POR BOGOTA_3
BOGOTA_1	OSPF	172.29.3.12 vía 172.29.3.2	BOGOTA_2 POR BOGOTA_3
BOGOTA_1	OSPF	172.29.3.12 vía 172.29.3.10	BOGOTA_3 POR BOGOTA_2
BOGOTA_1	STATIC	0.0.0.0 vía 209.17.220.5	CUALQUIER RED POR ISP
BOGOTA_2	LOCAL	172,29,0,1	PC-BOG1
BOGOTA_2	LOCAL	172,29,3,10	BOGOTA_1
BOGOTA_2	LOCAL	172,29,3,13	BOGOTA_3
BOGOTA_2	OSPF	172,29,3,0 vía 172,29,3,14	BOGOTA_1 POR BOGOTA_3
BOGOTA_2	OSPF	172,29,3,0 vía 172,29,3,9	BOGOTA_3 POR BOGOTA_1
BOGOTA_2	OSPF	172,29,3,4 vía 172,29,3,14	BOGOTA_1 POR BOGOTA_3
BOGOTA_2	OSPF	172,29,3,4 vía 172,29,3,9	BOGOTA_3 POR BOGOTA_1

BOGOTA_2	OSPF	209,17,220,4 vía 172,29,3,9	ISP POR BOGOTA_1
BOGOTA_3	LOCAL	172,29,0,1	PC_BOG2
BOGOTA_3	LOCAL	172,29,3,2	BOGOTA_1
BOGOTA_3	LOCAL	172,29,3,5	BOGOTA_1
BOGOTA_3	LOCAL	172,29,3,14	BOGOTA_2
BOGOTA_3	OSPF	172,29,3,8 vía 172,29,3,13	BOGOTA_1 POR BOGOTA_2
BOGOTA_3	OSPF	172,29,3,8 vía 172,29,3,5	BOGOTA_2 POR BOGOTA_1
BOGOTA_3	OSPF	209,17,220,4 vía 172,29,3,5	ISP POR BOGOTA_1

La tabla anterior se construye a base de generar el comando show ip route en cada uno de los Router de la topología.

7.4. Configurar encapsulamiento y autenticación PPP.

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

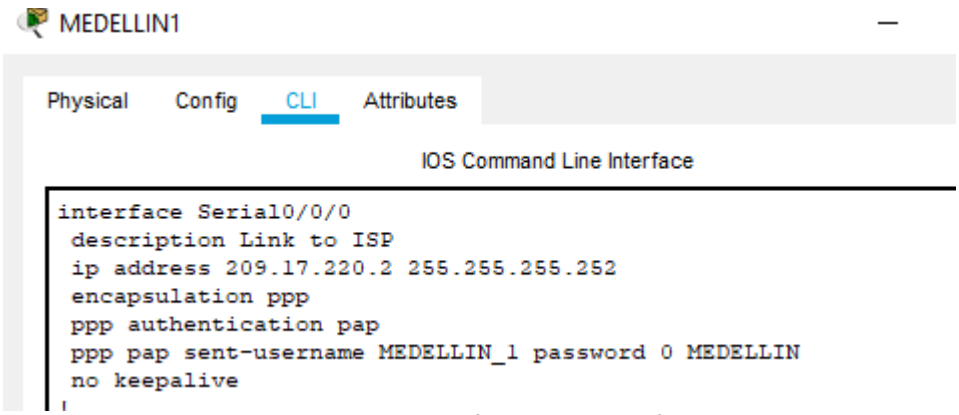


Figura 13. Evidencia configuración de autenticación PPP con PAP

Los códigos usados para configuración de PAP es:

En Medellín_1
Config t
Int S0/0/0
Encapsulation ppp
ppp autenthication pap
ppp pap sent-username MEDELLIN_1 password MEDELLIN
exit

En ISP
Config t
Int s0/0/0
Encapsulation ppp
ppp autenthication pap
ppp pap sent-username ISP password ISP
exit

El enlace Bogotá1 con ISP se debe configurar con autenticación CHAP.

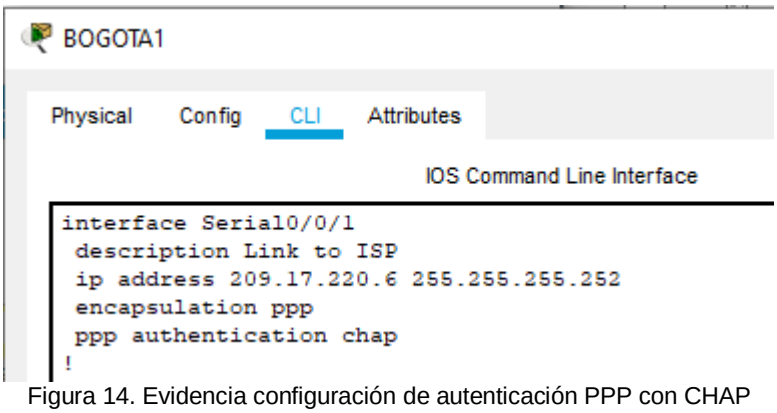


Figura 14. Evidencia configuración de autenticación PPP con CHAP

La configuración de CHAP se realiza así:

En ISP
Config t
Int s0/0/1
Encapsulation ppp
Ppp authentication chap
Exit

En BOGOTA_1
config t
Encapsulation ppp
Ppp authentication chap
Exit

7.4.1. Configuración de NAT

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.

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_1#ping 209.17.220.5

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.17.220.5, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
```

Figura 15. Evidencia ping correcto

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.

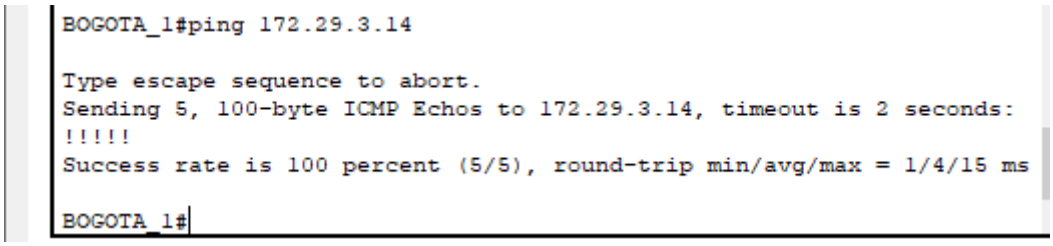


Figura 16. Evidencia ping correcto

7.4.2. Configuración del servicio DHCP.

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

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

La configuración de DHCP se realizó con los siguientes comandos:

Config t
Ip dhcp excluded-address 172.29.4.1 172.29.4.3 //Excluye las primeras 4 ip válidas
Ip dhcp excluded-address 172.29.4.129 172.29.4.132 //efectúa el mismo procedimiento
Ip dhcp pool MEDELLIN_2 //crea el pool y lo nombra
Network 172.29.4.0 255.255.255.128
Default Router 172.29.4.1
Dns-server 8.8.4.4.
Exit

Ip dhcp pool MEDELLIN_3
Network 172.29.4.128 255.255.255.128
Default Router 172.29.4.129
Dns-server 8.8.4.4
Exit

Ahora en el Router Medellin_2 se configura para recibir
Config t
Int g0/0
Ip helper-address 172.29.6.5 //define de donde procederá el direccionamiento DHCP para su LAN

La misma configuración es aplicada en BOGOTA_2

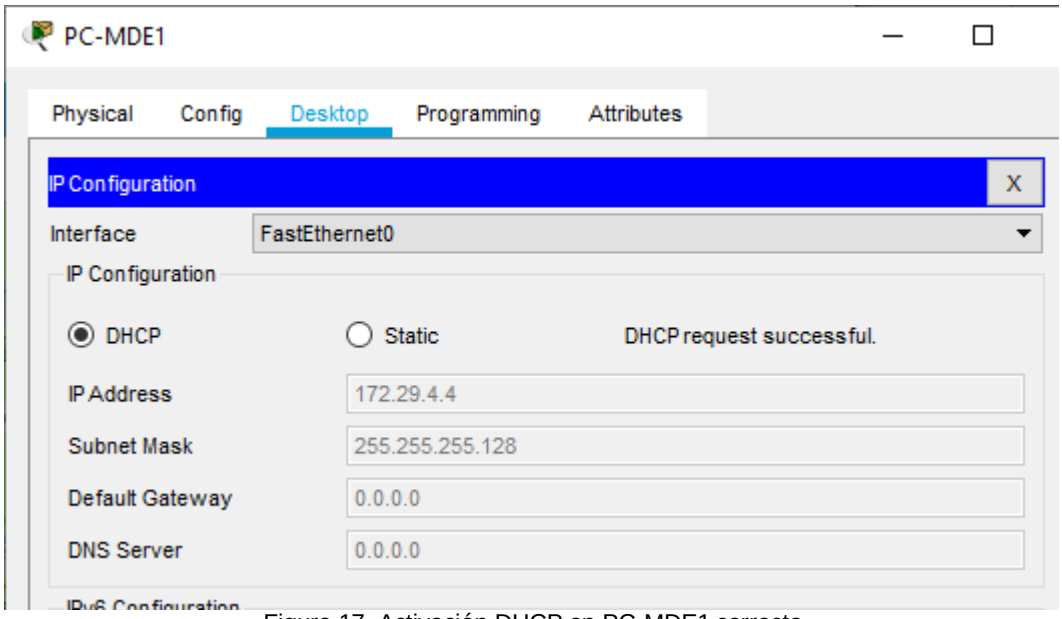


Figura 17. Activación DHCP en PC-MDE1 correcta

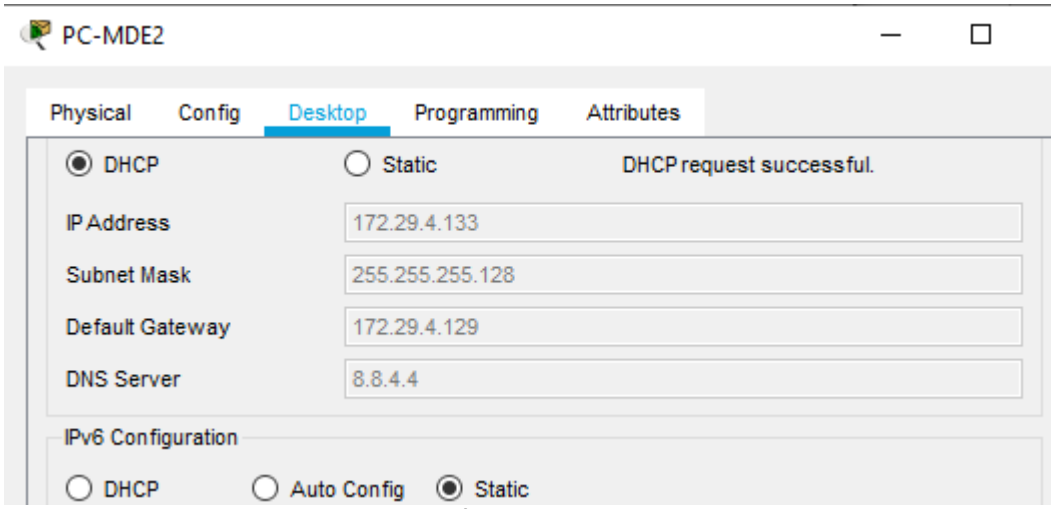


Figura 18. Activación DHCP en PC-MDE2 correcta

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

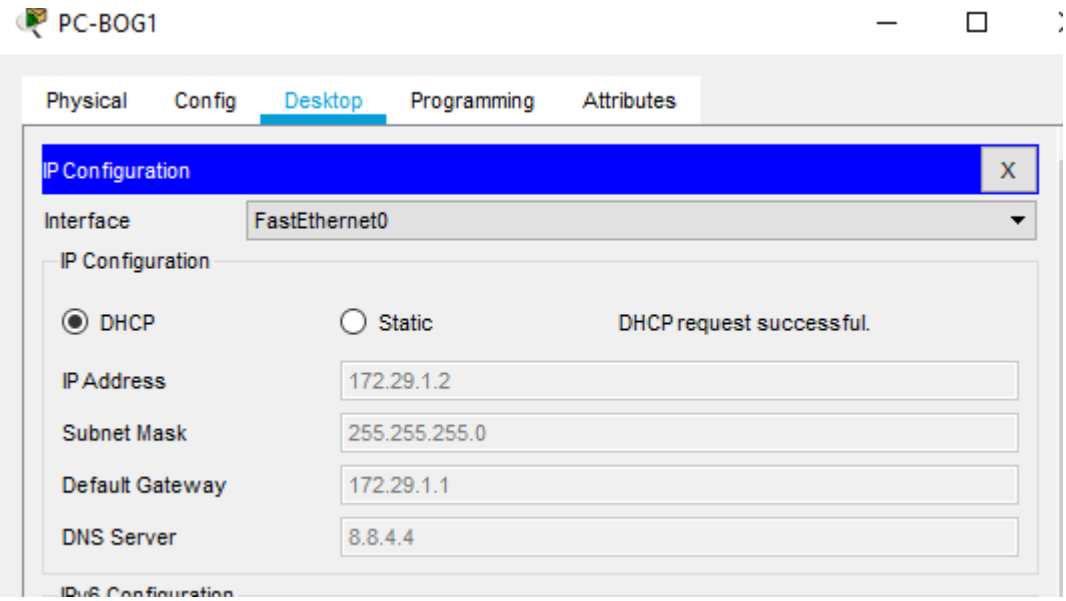


Figura 19. Activación DHCP en PC-BOG1 correcta

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

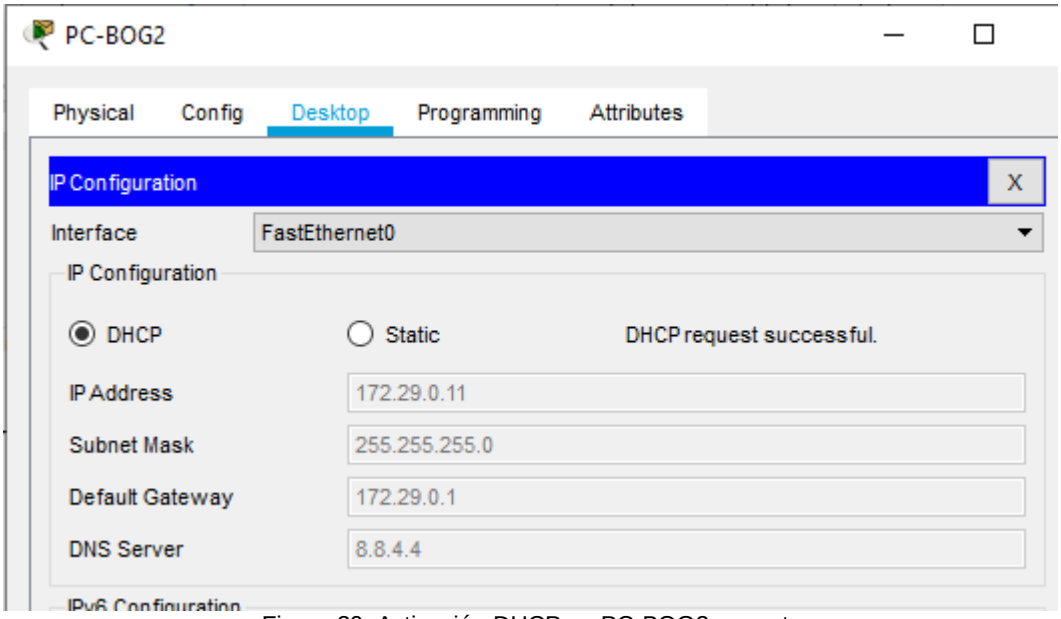


Figura 20. Activación DHCP en PC-BOG2 correcta

Se evidencia por parte de los host adscritos a Bogota_2 y Bogota_3, así como a Medellin_2 y Medellin_3, que han tomado las direcciones dentro del rango válido definido en la configuración.

CONCLUSIONES

- Las configuraciones de un dispositivo de capa 3, sin indispensables para que la articulación del resto de dispositivos sea efectiva dentro de una topología.
- Es importante conocer los diferentes protocolos de enrutamiento para garantizar la conectividad de los dispositivos finales (host) en una topología simulada.
- La herramienta Packet Tracer me permitió ahondar en un ambiente práctico con el cual podré simular posteriormente cualquier tipo de topología, ahorrando tiempo y dinero en la utilización de dispositivos físicos que en el simulador se pueden reconfigurar o eliminar y reemplazar muy fácilmente.
- El diplomado es un refuerzo de los conocimientos aprendidos en las materias CCNA1 y CCNA2, las cuales pude cursar en semestre anteriores, pero esta prueba práctica me permitió identificar las falencias en la cuales no estaba tan fuerte en mis conocimientos teóricos.
- La topología 1 me permitió ahondar conocimientos sobre direccionamiento RIPv2, además de la configuración de subinterfaces aplicables a la inclusión de VoIP en una red, no obstante, en este caso se uso para la configuración de VLAN en ambas subredes, se configura el Router como servidor DHCP y sus conexiones desde y hacia los Switch de modo troncal, a su vez, cada Switch se conecta a su LAN con modo de acceso.
- En la topología 2, la configuración de encapsulamiento PPP me dio la posibilidad de conocer este tipo de encapsulamiento que a lo largo del curso y en mis cursos de CCNA1 y CCNA2 no conocí, entendiendo que es una manera de encapsular la comunicación entre el ISP y los Router principales de cada red WAN.
- Finalmente, el uso frecuente de comandos me apoyo el proceso de aprendizaje pues con la práctica se crea recordación.

BIBLIOGRAFÍA

DansCourses. (Marzo de 2011). *Configure Subinterfaces and 802.1Q Inter-VLAN routing for the Cisco CCNA*. Obtenido de https://youtu.be/FQaABMZifKE

De Luca, R. (8 de Agosto de 2012). *Packet Tracer - Configurar PPP con CHAP - 2 min*. Obtenido de https://youtu.be/bgHvALyBPcg

MarioTechAcademy. (11 de Noviembre de 2013). *CS071 21.02 OSPF - Configuracion OSPF en Packet Tracer*. Obtenido de https://youtu.be/lw-IekHi9eY

NetAcad Cisco. (s.f.). *Modulos CCNA1 & CCNA2*. Obtenido de http://www.netacad.com