

**SOLUCIÓN DE DOS ESCENARIOS PRESENTES EN ENTORNOS
CORPORATIVOS BAJO EL USO DE TECNOLOGÍA CISCO**

DIANA CRISTINA HIDALGO VELÁSQUEZ

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
INGENIERÍA DE SISTEMAS
MANZANARES**

2020

**SOLUCIÓN DE DOS ESCENARIOS PRESENTES EN ENTORNOS
CORPORATIVOS BAJO EL USO DE TECNOLOGÍA CISCO**

DIANA CRISTINA HIDALGO VELÁSQUEZ

Trabajo de opción de grado

Tutor

Gustavo Adolfo Rodríguez

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA**

INGENIERÍA DE SISTEMAS

MANZANARES

2020

RESUMEN

Analizar el rol fundamental que desempeñan en la actualidad el mundo de las telecomunicaciones en el desarrollo de cada una de las actividades diarias del ser humano; debido a esto, al entender el funcionamiento a través de las redes de información es visto por la Universidad Nacional Abierta y a Distancia – UNAD, como una de las bases fundamentales en el desarrollo académico de los próximos Ingenieros de Sistemas , de allí surge el convenio con una de las mejores entidades en el mundo CISCO Networking Academy, y ha surgido la oferta del diplomado: “CISCO diseño e implementación de redes LAN-WAN”.

En donde cada estudiante dispone de dos módulos: el primero bajo el título de CCNA1: Switching y routing: Introducción a redes, el cual se enfoca en brindar la capacidad al estudiante de construir redes LAN simples, realizar configuraciones básicas para enrutadores e interruptores, e implementar esquemas de direccionamiento IP, el segundo CCNA2: Routing y switching: Principios básicos de routing y switching, ese encamina en presentar herramientas para configurar y solucionar problemas de enrutadores y cambia y resuelve problemas comunes con RIPv1, RIPv2, área única y área múltiple OSPF, LAN virtuales y enrutamiento entre VLAN en ambas redes IPv4 e IPv6, es por esto que como complemento y evaluación se dispone de la prueba de habilidades prácticas, la cual se desarrolla en este documento y que pretende demostrar al estudiante las aptitudes aprendidas durante el curso de profundización.

ABSTRACT

Analyze the fundamental role that the world of telecommunications currently plays in the development of each of the daily activities of the human being; Due to this, when understanding the operation through information networks, it is seen by the National Open and Distance University - UNAD, as one of the fundamental bases in the academic development of the next Systems Engineers, hence the agreement with one of the best entities in the world CISCO Networking Academy, and the offer of the diploma has emerged: "CISCO design and implementation of LAN-WAN networks".

Where each student has two modules: the first under the title of CCNA1: Switching and routing: Introduction to networks, which focuses on providing the student with the ability to build simple LAN networks, perform basic configurations for routers and switches, and implement IP addressing schemes, the second CCNA2: Routing and Switching: Routing and Switching Basics, that aims to introduce tools to configure and troubleshoot routers and change and solve common problems with RIPv1, RIPv2, single area, and multiple area OSPF , Virtual LANs and routing between VLANs in both IPv4 and IPv6 networks, that is why, as a complement and evaluation, the practical skills test is available, which is developed in this document and which aims to demonstrate to the student the skills learned during the course deepening.

GLORARIO

CCNA: Es una certificación entregada por la compañía Cisco sobre infraestructuras de red e internet.

CLI: Interfaz de línea de comandos sobre la cual se pueden generar instrucciones a los routers y switches de cisco.

CLIENTE: En el contexto cliente/Servidor, el cliente es quien realiza la petición a un servidor para obtener un recurso de red

DHCP: Es un protocolo de red tipo cliente/servidor, el cual se encarga de configurar de manera dinámica las direcciones IP entre los diferentes dispositivos que pertenecen a una red.

DIRECCIÓN IP: Dirección lógica de un dispositivo en la red.

DIRECCIÓN MAC. Dirección física de un dispositivo en la red.

INTERFAZ: se usa para nombrar la conexión funcional entre dos equipos de red, por lo general hace referencia al puerto físico de red de un router o Switch.

LAN: Red de área local, por lo general abarca red de una casa o un edificio.

NAT: Corresponde a la traducción de direcciones de red.

NTP: protocolo de internet para sincronizar la hora de los dispositivos conectados a la red.

SERVIDOR: En el contexto Cliente/Servidor, el servidor es el dispositivo que recibe peticiones de manera simultánea de varios clientes y entregando los recursos solicitados.

TOPOLOGIA: Es el mapa físico o lógico de cómo está construida una red.

VLAN: Red de área local virtual, permite crear varias redes lógicas totalmente independiente pero que usan el mismo medio físico.

VPN: la red privada virtual es una tecnología que permite acceder a recursos de una red privada da través de internet.

WAN: Red de área amplia, corresponde a una unión de varias redes locales, las cuales están físicamente distantes.

CLI: Interfaz de línea de comandos sobre la cual se pueden generar instrucciones los routers y switches de cisco.

CLIENTE: En el contexto cliente/Servidor, el cliente es quien realiza la petición a un servidor para obtener un recurso de red

DHCP: Es un protocolo de red tipo cliente/servidor, el cual se encarga de configurar de manera dinámica las direcciones IP entre los diferentes dispositivos que pertenecen a una red.

DIRECCIÓN IP: Dirección lógica de un dispositivo en la red.

DIRECCIÓN MAC. Dirección física de un dispositivo en la red.

INTERFAZ: se usa para nombrar la conexión funcional entre dos equipos de red, por lo general hace referencia al puerto físico de red de un router o Switch.

LAN: Red de área local, por lo general abarca red de una casa o un edificio.

NAT: Corresponde a la traducción de direcciones de red.

NTP: protocolo de internet para sincronizar la hora de los dispositivos conectados a la red.

SERVIDOR: En el contexto Cliente/Servidor, el servidor es el dispositivo que recibe peticiones de manera simultánea de varios clientes y entregando los recursos solicitados.

TOPOLOGIA: Es el mapa físico o lógico de cómo está construida una red.

VLAN: Red de área local virtual, permite crear varias redes lógicas totalmente independiente pero que usan el mismo medio físico.

VPN: la red privada virtual es una tecnología que permite acceder a recursos de una red privada da través de internet.

WAN: Red de área amplia, corresponde a una unión de varias redes locales, las cuales están físicamente distantes.

JUSTIFICACIÓN

La Universidad Nacional Abierta y a Distancia - UNAD, ofrece diferentes opciones de grado donde se encuentra la realización del DIPLOMADO DE PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN), el cual permite al estudiante la profundización específica en el tema de redes de comunicaciones, con él podremos lograr obtener el título de profesional y generar en nuestras hojas de vida un plus adicional; por el conocimiento que desarrollaremos y que en la actualidad en el ámbito laboral, es de bastante utilidad.

INDICE

INTRODUCCIÓN	1
OBJETIVOS.....	2
ESCENARIO 1	3
Parte 1: Inicializar dispositivos.....	4
Paso 1: Inicializar y volver a cargar los routers y los switches	4
Parte 2: Configurar los parámetros básicos de los dispositivos.....	6
Paso 1: Configurar la computadora de Internet.....	6
Paso 2: Configurar R1	6
Paso 3: Configurar R2.....	8
Paso 4: Configurar R3.....	10
Paso 5: Configurar S1	12
Paso 6: Configurar el S3	14
Paso 7: Verificar la conectividad de la red.....	15
Parte 3: Configurar la seguridad del switch, las VLAN y el routing entre VLAN.	19
Paso 1: Configurar S1	19
Paso 2: Configurar el S3	21
Paso 3: Configurar R1	23
Paso 4: Verificar la conectividad de la red.....	24
Parte 4: Configurar el protocolo de routing dinámico RIPv2	29
Paso 1: Configurar RIPv2 en el R1.....	29
Paso 2: Configurar RIPv2 en el R2.....	30
Paso 3: Configurar RIPv3 en el R3.....	31
Paso 4: Verificar la información de RIP	32
Parte 5: Implementar DHCP y NAT para IPv4.....	36
Paso 1: Configurar el R1 como servidor de DHCP para las VLAN 21 y 23	36
Paso 2: Configurar la NAT estática y dinámica en el R2	37
Paso 3: Verificar el protocolo DHCP y la NAT estática.....	39

Parte 6: Configurar NTP	42
Parte 7: Configurar y verificar las listas de control de acceso (ACL)	43
Paso 1: Restringir el acceso a las líneas VTY en el R2.....	43
Paso 2: Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente	44
Escenario 2.....	47
Parte 1: Configuración del enrutamiento.....	57
Paso 1: Configurar el enrutamiento en la red usando el protocolo OSPF versión 2, declare la red principal, desactive la sumarización automática	6
6	
Parte 2: Tabla de Enrutamiento	75
Parte 3: Deshabilitar la propagación del protocolo OSPF.....	79
Parte 4: Verificación del protocolo OSPF.....	84
Parte 5: Configurar encapsulamiento y autenticación PPP.....	95
Parte 6: Configuración de PAT	99
Parte 7: Configuración del servicio DHCP	103
CONCLUSIONES	110
BIBLIOGRAFIA.....	111
ANEXOS	112
Link archivos Packet Tracer.....	112

LISTA DE TABLAS

Tabla 1 Inicializar dispositivos.....	5
Tabla 2. Configurar la computadora de Internet.....	6
Tabla 3 Configurar R1.....	7
Tabla 4 Configurar Router 2.....	10
Tabla 5 Configurar router 3.....	12
Tabla 6 Configurar S1.....	13
Tabla 7 Configurar S3.....	14
Tabla 8 Verificar conectividad.....	15
Tabla 9 Seguridad S1.....	21
Tabla 10 Seguridad S3.....	22
Tabla 11 Configuración R1.....	23
Tabla 12 Verificaciones de conectividad.....	24
Tabla 13 Configuración RIP en R1.....	29
Tabla 14 Configuración RIP en R2.....	30
Tabla 15 Configuración RIP en R3.....	31
Tabla 16 Verificación de RIP.....	32
Tabla 17 DHCP y NAT IPv4 en R1.....	37
Tabla 18 DHCP y NAT IPv4 en R2.....	39
Tabla 19 Verificaciones DHCP y NAT.....	40
Tabla 20 Configuración NTP.....	42
Tabla 21 Continuación de ACL.....	43
Tabla 22 Visualización de Access list.....	45
Tabla 23 Configuración inicial de dispositivos.....	53
Tabla 24 Conexión física de los equipos.....	56
Tabla 25 Configuración de enrutamiento.....	65
Tabla 26 Configurar el enrutamiento en la red usando el protocolo OSPF versión 2.....	71
Tabla 27 Publicaciones de OSPF.....	73
Tabla 28 Sumarización de redes.....	74
Tabla 29 Propagación de OSPF.....	79
Tabla 30 Propagación de OSPF Bogota1.....	80
Tabla 31 Propagación de OSPF Bogota2.....	81
Tabla 32 Propagación de OSPF Bogota3.....	81
Tabla 33 Propagación de OSPF Medellin1.....	82
Tabla 34 Propagación de OSPF Medellin2.....	82
Tabla 35 Propagación de OSPF Medellin3.....	83
Tabla 36 Verificación protocolo OSPF MEDELLIN1 – BOGOTA1.....	86
Tabla 37 Verificación protocolo OSPF MEDELLIN2– BOGOTA2.....	89
Tabla 38 Verificación protocolo OSPF MEDELLIN3– BOGOTA3.....	93

Tabla 39 Verificación protocolo OSPF ISP	94
Tabla 40 Encapsulamiento PPP Medellín1 con ISP.....	96
Tabla 41 Encapsulamiento Bogotá	98
Tabla 42 Configuración de PAT	100
Tabla 43 Estadísticas NAT Router Bogota1.....	102
Tabla 44 Configuración del servicio DHCP	103
Tabla 45 Configuración del servicio broadcast.....	104
Tabla 46 Configuración Bogotá2 y Bogotá3 donde el router Bogotá2 debe ser el servidor DHCP	10
6	
Tabla 47 Configuración router Bogotá1 mensajes Broadcast	107

LISTA DE FIGURAS

Figura 1 Escenario 1	3
Figura 2 Topología	4
Figura 3 Pruebas de Ping desde Router 1 y Router 2.....	16
Figura 4 Pruebas de Ping desde Router 2 y Router 3.....	17
Figura 5 Pruebas de Ping desde PC a Gateway.....	18
Figura 6 Ping desde S1 a R1, dirección Vlan 99. Ping 192.168.99.1	25
Figura 7 Ping desde S3 a R1, dirección Vlan 99. Ping 192.168.99.1	26
Figura 8 Ping desde S1 a R1, dirección Vlan 21. Ping 192.168.21.1	27
Figura 9 Ping desde S3 a R1, dirección Vlan 23. Ping 192.168.23.1	28
Figura 10 Comando proceso RIP	33
Figura 11 Comando Rutas RIP	34
Figura 12 Configuración PC-A	39
Figura 13 Configuración PC-C	39
Figura 14 Conectividad entre PC-A y PC-C	39
Figura 15 Servidor Web 209.165.200.229	41
Figura 16 Verificación ACL	44
Figura 17 Comando show access-List	46
Figura 18 Escenario 2	47
Figura 19 Topología Red Escenario 2.....	54
Figura 20 Enrutamiento Router Bogotá1 y Medellín1.....	75
Figura 21 Enrutamiento Bogotá2 y Medellín2	76
Figura 22 Enrutamiento Bogotá3 y Medellín3	77
Figura 23 Enrutamiento ISP	78
Figura 24 Verificación protocolo OSPF MEDELLIN1 – BOGOTA1	84
Figura 25 Verificación protocolo OSPF MEDELLIN2– BOGOTA2	87
Figura 26 Verificación protocolo OSPF MEDELLIN3– BOGOTA3.....	90
Figura 27 Verificación protocolo OSPF ISP	93
Figura 28 Direccionamiento DHCP PC1 y PC2	105
Figura 29 Direccionamiento DHCP PC3	108
Figura 30 Topología de Red Final.....	109

INTRODUCCIÓN

Cabe resaltar la importancia de las telecomunicaciones en nuestra actualidad, en donde vemos con gran interés la expansión que se está logrando en este ámbito. Adicional, tenemos el tema de contingencia, que se presenta en nuestro tiempo, debido a la pandemia que estamos sobrellevando, es aquí donde se ha expuesto y desarrollado una necesidad básica de estar interconectados virtualmente, para seguir desarrollándonos en nuestras actividades cotidianas más simples; como trabajar, estudiar, estar en contacto con nuestros seres queridos, asistir virtualmente a eventos sociales de importancia personal, etc.

Es de gran satisfacción cursar este diplomado con Cisco Systems, una empresa catalogada como líder mundial en redes para Internet; de allí radica que la Universidad Nacional Abierta y a Distancia – UNAD haya decidido asociarse para brindar esta herramienta a sus futuros Ingenieros.

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

En este documento se desarrolla la solución un escenario propuesto, que condensa los conceptos teóricos y prácticos de los 2 módulos comprendidos en CCNA1 y CCNA2 los cuales comprenden Introducción a redes y Principios básicos de routing y switching, es indispensable el uso de la herramienta Cisco Packet Tracer para lograr el completo desarrollo y comprensión de la prueba.

OBJETIVOS

Objetivo General

Resolver la prueba de habilidades propuesta en el DIPLOMADO DE PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN), aplicando los conceptos básicos aprendidos en los módulos CCNA1 FUNDAMENTOS DE NETWORKING y CCNA2 PRINCIPIOS DE ENRUTAMIENTO ofrecidos por la Cisco Networking Academy.

Objetivos Específicos

- Desarrollo de la actividad por medio del uso de la herramienta Cisco Packet Tracer.
- Elegir los dispositivos requeridos para la topología de la red.
- Configurar el direccionamiento IP acorde con la topología de red para cada uno de los dispositivos que forman parte del escenario.
- Configurar VLANs, Puertos troncales, puertos de acceso, encapsulamiento, Inter-VLAN Routing y Seguridad en los Switches acorde a la topología de red establecida
- Configurar el protocolo de enrutamiento OSPFv2 bajo los criterios establecidos.
- Configurar cada dispositivo, según especificaciones exigidas.
- Comprobar la conectividad de los dispositivos de la red.

ESCENARIO 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.

Topología

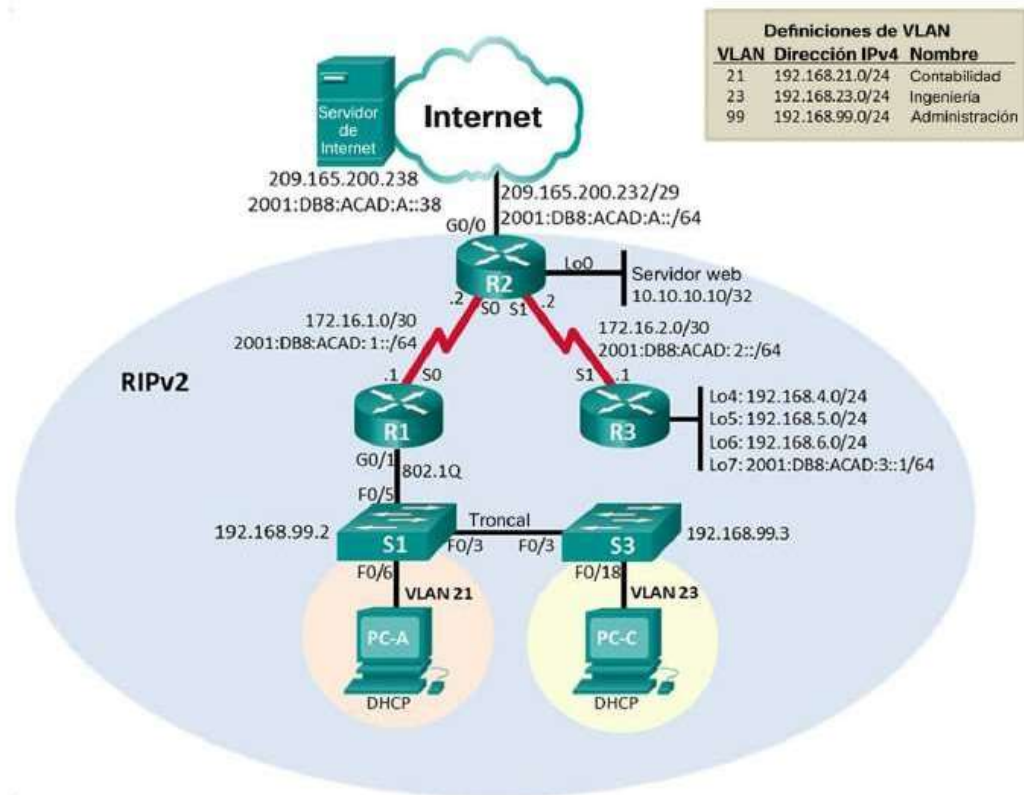


Figura 1 Escenario 1

Parte 1: Inicializar dispositivos

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

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

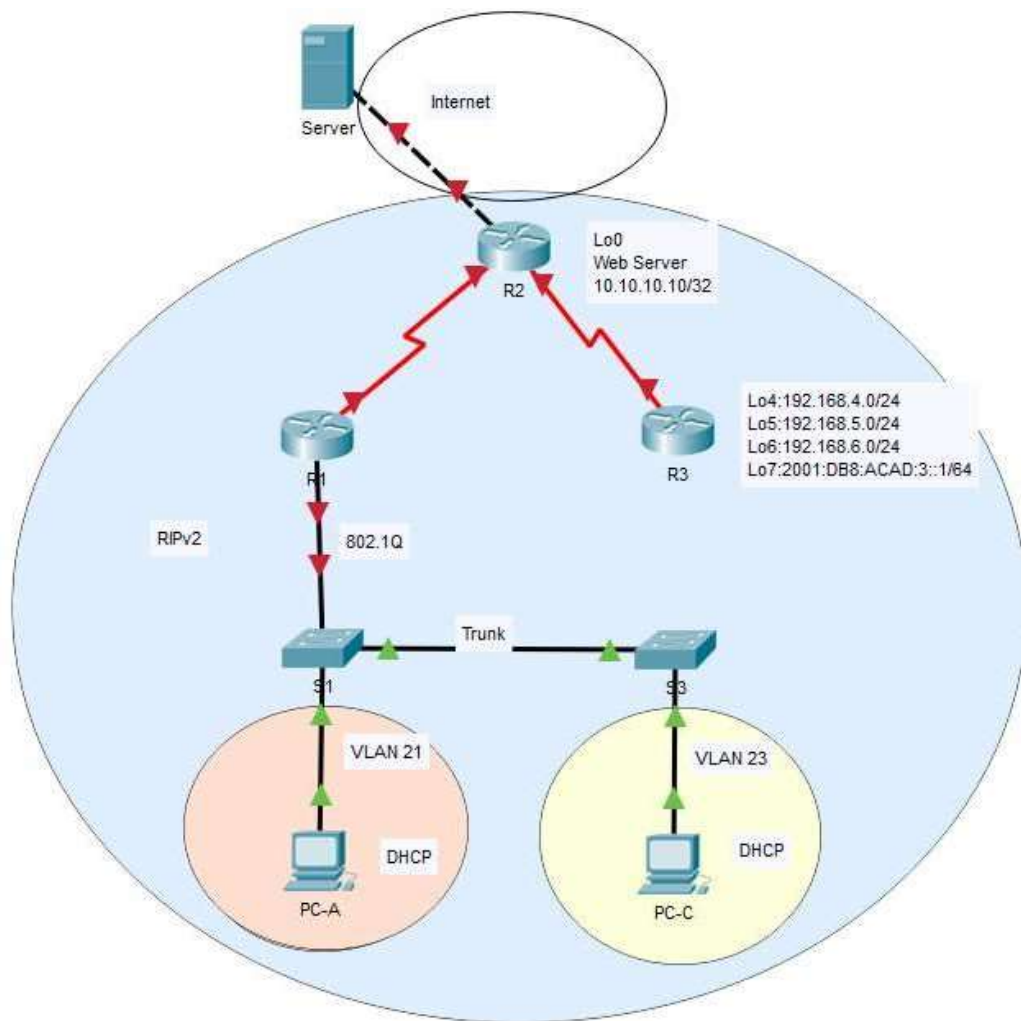


Figura 2 Topología

Antes de continuar, solicite al instructor que verifique la inicialización de los dispositivos.

A continuación, se realiza el borrado de configuración y reinicio de cada uno de los equipos, adicional se configuran los parámetros básicos de cada uno de ellos y se configura la computadora de Internet.

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	Router#erase startup-config
Volver a cargar todos los routers	Router#reload
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Switch#erase startup-config Switch#delete vlan.dat
Volver a cargar ambos switches	Switch#reload
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Switch#show flash

Tabla 1 Inicializar dispositivos.

Parte 2: Configurar los parámetros básicos de los dispositivos

Paso 1: Configurar la computadora de Internet

Las tareas de configuración del servidor de Internet incluyen lo siguiente (para obtener información de las direcciones IP, consulte la topología):

Se realiza la configuración del dispositivo *servidor_internet* para simular el acceso a la nube.

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::1

Tabla 2. Configurar la computadora de Internet

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Se presenta la configuración base del Router 1, donde se configura su nombre, contraseñas, mensaje motd y la configuración de interfaz serial para conexión con router2. Adicional a ello se configuran rutas predeterminadas para que queden asociadas a la interfaz s0/0/0.

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R1
Contraseña de exec privilegiado cifrada	R1(config)#enable secret class
Contraseña de acceso a la consola	R1(config)#line console 0 R1(config-line)#password cisco R1(config-line)#login
Contraseña de acceso Telnet	R1(config)#line vty 0 15 R1(config-line)#password cisco R1(config-line)#login
Cifrar las contraseñas de texto no cifrado	R1(config-line)#service password-encryption
Mensaje MOTD	R1(config)#banner motd #Se prohíbe el acceso no autorizado.#
Interfaz S0/0/0	R1(config)#int s0/0/0 R1(config-if)#Description Conexion R1 y R2 R1(config-if)#ip address 172.16.1.1 255.255.255.252 R1(config-if)#ipv6 address 2001:DB8:ACAD:1::1/64 R1(config-if)#clock rate 128000 R1(config-if)#no shutdown
Rutas predeterminadas	R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0 R1(config)#ipv6 route ::/0 s0/0/0

Tabla 3 Configurar R1

Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

A continuación, se realiza la configuración básica del Router 2, indicando su nombre, contraseñas, mensaje motd y configuración de interfaz g0/0 para simular conexión a internet. Adicionalmente se configuran rutas predeterminadas para que queden asociadas a la interfaz g0/0.

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R2
Contraseña de exec privilegiado cifrada	R2(config)#enable secret class
Contraseña de acceso a la consola	R2(config)#line console 0 R2(config-line)#password cisco R2(config-line)#login
Contraseña de acceso Telnet	R2(config)#line vty 0 15 R2(config-line)#password cisco R2(config-line)#login

Cifrar las contraseñas de texto no cifrado	R2(config)#service password-encryption
Habilitar el servidor HTTP	
Mensaje MOTD	R2(config)#banner motd #Se prohíbe el acceso no autorizado.#
Interfaz S0/0/0	R2(config)#int s0/0/0 R2(config-if)#description Conexion entre R2 y R1 R2(config-if)#ip address 172.16.1.2 255.255.255.252 R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64 R2(config-if)#no shutdown
Interfaz S0/0/1	R2(config)#int s0/0/1 R2(config-if)#description Conexion R2 y 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)#no shutdown
Interfaz G0/0 (simulación de Internet)	R2(config)#int g0/0 R2(config-if)#description Conexion R2 a Internet R2(config-if)#ip address 209.165.200.232 255.255.255.248 R2(config-if)#ip address 209.165.200.233 255.255.255.248 R2(config-if)#ipv6 address 2001:DB8:ACAD:A::2/64 R2(config-if)#no shutdown

<p>Interfaz loopback 0 (servidor web simulado)</p>	<pre>R2(config)#int loopback 0 R2(config-if)#description interface Loopback 0 R2(config-if)#ip address 10.10.10.10 255.255.255.255 R2(config-if)#no ip address 10.10.10.10 255.255.255.255 R2(config-if)#exit R2(config)#int g0/1 R2(config-if)#ip address 10.10.10.10 255.255.255.0 R2(config-if)#no shutdown</pre>
<p>Ruta predeterminada</p>	<pre>R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0 %Default route without gateway, if not a point-topoint interface, may impact performance R2(config)#ipv6 route ::/0 g0/0</pre>

Tabla 4 Configurar Router 2

Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Se presenta a continuación la configuración básica del Router 3, su nombre, contraseñas, mensaje motd y configuración de interfaz serial para conexión con Router 2. Además, configuran rutas predeterminadas para que queden asociadas a la interfaz s0/0/1, y también se configuran interfaces loopback.

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R3
Contraseña de exec privilegiado cifrada	R3(config)#enable secret class
Contraseña de acceso a la consola	R3(config)#line console 0 R3(config-line)#password cisco R3(config-line)#login
Contraseña de acceso Telnet	R3(config)#line vty 0 15 R3(config-line)#password cisco R3(config-line)#login
Cifrar las contraseñas de texto no cifrado	R3(config-line)#service password-encryption
Mensaje MOTD	R3(config)#banner motd #se prohíbe el acceso no autorizado.#
Interfaz S0/0/1	R3(config)#int s0/0/1 R3(config-if)#description conexion R2 y R3 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 shutdown

Interfaz loopback 4	R3(config)#int loopback 4 R3(config-if)#ip address 192.168.4.1 255.255.255.0
Interfaz loopback 5	R3(config)#int loopback 5 R3(config-if)#ip address 192.168.5.1 255.255.255.0
Interfaz loopback 6	R3(config-if)#int loopback 6 R3(config-if)#ip address 192.168.6.1 255.255.255.0
Interfaz loopback 7	R3(config)#int loopback 7 R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64
Rutas Predeterminadas	R3(config)#int s0/0/1 R3(config-if)#ip route 0.0.0.0 0.0.0.0 s0/0/1 %Default route without gateway, if not a point-to-point interface, may impact performance R3(config)#ipv6 route ::/0 s0/0/1

Tabla 5 Configurar router 3

Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Se realiza la configuración del Switch 1 donde se indica su nombre, contraseñas y mensaje motd.

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S1
Contraseña de exec privilegiado cifrada	S1(config)#enable secret class
Contraseña de acceso a la consola	S1(config)#line console 0 S1(config-line)#password cisco S1(config-line)#login
Contraseña de acceso Telnet	S1(config)#line vty 0 15 S1(config-line)#password cisco S1(config-line)#login
Cifrar las contraseñas de texto no cifrado	S1(config-line)#service password-encryption
Mensaje MOTD	S1(config)#banner motd #Se prohíbe el acceso no autorizado.#

Tabla 6 Configurar S1

Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Se realiza la configuración del Switch 3 donde se indica su nombre, contraseñas y mensaje motd.

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S3
Contraseña de exec privilegiado cifrada	S3(config)#enable secret class
Contraseña de acceso a la consola	S3(config)#line console 0 S3(config-line)#password cisco S3(config-line)#login
Contraseña de acceso Telnet	S3(config)#line vty 0 15 S3(config-line)#password cisco S3(config-line)#login
Cifrar las contraseñas de texto no cifrado	S3(config-line)#service password-encryption
Mensaje MOTD	S3(config)#banner motd #Se prohíbe el acceso no autorizado.#

Tabla 7 Configurar S3

Paso 7: Verificar la conectividad de la red

Utilice el comando ping para probar la conectividad entre los dispositivos de red.

Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

A continuación, se presentan las pruebas de conectividad realizadas mediante ping desde Router1 hacia Router2, y desde Router2 a Router3

Desde	a	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	Success rate is 100 percent (5/5), round-trip min/avg/max = 1/7/16 ms
R2	R3, S0/0/1	172.16.1.2	Success rate is 100 percent (5/5), round-trip min/avg/max = 1/7/12 ms
PC de Internet	Gateway predeterminado	209.165.200.233	Success

Tabla 8 Verificar conectividad.

Pantallazo de prueba de ping desde Router 1 y Router 2. Ping hacia la ip 172.16.1.2

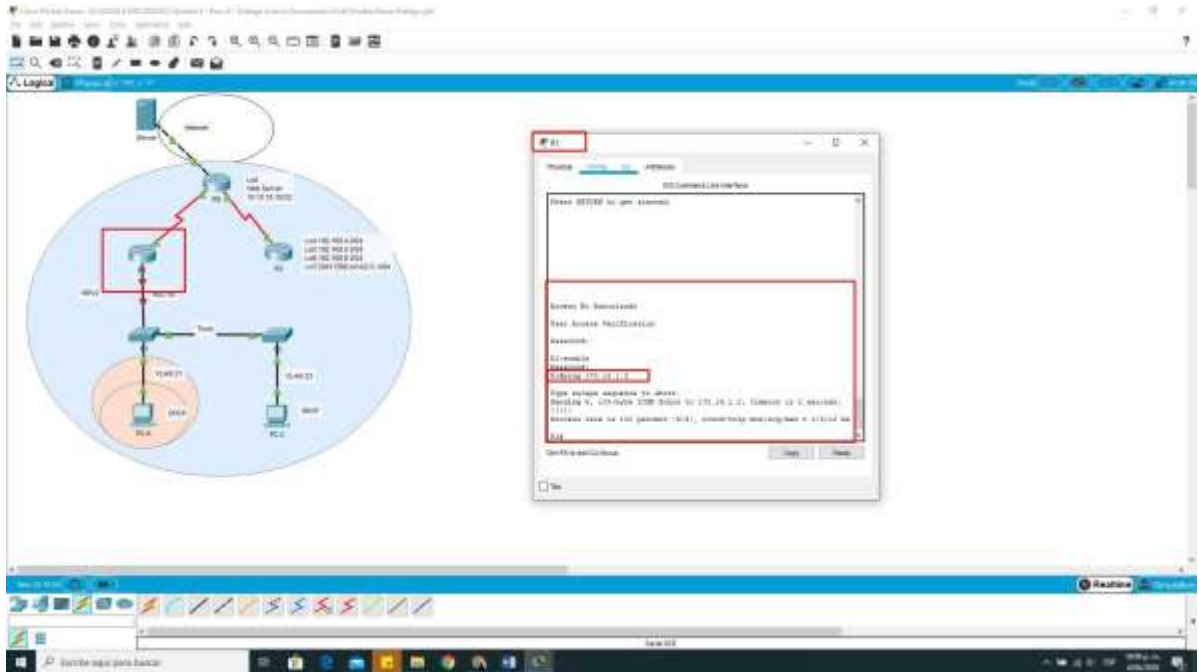


Figura 3 Pruebas de Ping desde Router 1 y Router 2

Pantallazo de prueba de ping desde PC de Internet a Gateway predeterminado.
Ping hacia la ip 209.165.200.233

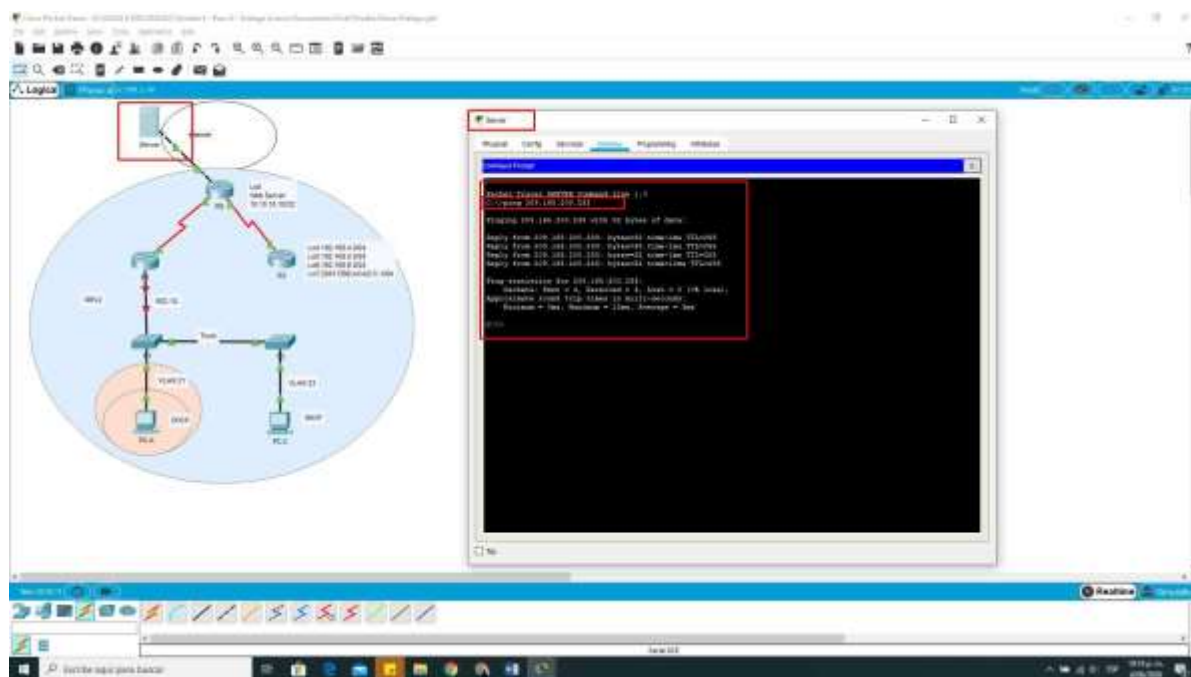


Figura 5 Pruebas de Ping desde PC a Gateway

Parte 3: Configurar la seguridad del switch, las VLAN y el routing entre VLAN

Paso 1: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Conforme a lo solicitado en la guía, se realiza la creación de base de datos de VLAN 21, VLAN 23 y VLAN 99, a las cuales se le asignan sus nombres correspondientes a cada área en este caso Contabilidad, Ingeniería y Administración en su respectivo orden, y se asigna el direccionamiento respectivo y la configuración del gateway predeterminado. Se establece la interfaz f0/5 como puerto troncal y los demás puertos se dejan en modo de acceso.

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	<pre>S1(config)#vlan 21 S1(config-vlan)#name Contabilidad S1(config-vlan)#exit S1(config)#vlan 23 S1(config-vlan)#name Ingenieria S1(config-vlan)#exit S1(config)#vlan 99 S1(config-vlan)#name Administracion S1(config-vlan)#exit</pre>

Asignar la dirección IP de administración.	<pre>S1(config)#interface vlan 99 S1(config-if)#ip address 192.168.99.2 255.255.255.0 S1(config-if)#no shutdown</pre>
Asignar el gateway predeterminado	<pre>S1(config)#ip default-gateway 192.168.99.1</pre>
Forzar el enlace troncal en la interfaz F0/3	<pre>S1(config)#int f0/3 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1</pre>
Forzar el enlace troncal en la interfaz F0/5	<pre>S1(config)#int f0/5 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1</pre>
Configurar el resto de los puertos como puertos de acceso	<pre>S1(config)#interface range f0/1, f0/2, f0/4, f0/7- 24, g0/1-2 S1(config-if-range)#switchport mode access</pre>
Asignar F0/6 a la VLAN 21	<pre>S1(config)#int f0/6 S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 21</pre>
Apagar todos los puertos sin usar	<pre>S1(config)#interface range f0/1-2 S1(config-if-range)#shutdown S1(config-if-range)#interface f0/4 S1(config-if)#shutdown S1(config-if)#interface range f0/7-24</pre>

	<pre>S1(config-if-range)#shutdown S1(config-if-range)#interface range g0/1-2 S1(config-if-range)#shutdown</pre>
--	---

Tabla 9 Seguridad S1

Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

En la configuración del Switch 3 se realiza la creación de las bases de datos de la VLAN 21, VLAN 23 y VLAN 99, a las cuales se le asignan sus nombres, correspondientes a cada área en este caso Contabilidad, Ingeniería y Administración en su respectivo orden, se configura el direccionamiento de la VLAN 99 y el puerto f0/3 como troncal, los demás puertos se dejan en modo de acceso. Cabe adicionar que los puertos que no están en uso se apagan.

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	<pre>S3(config)#vlan 21 S3(config-vlan)#name Contabilidad S3(config-vlan)#exit S3(config)#vlan 23 S3(config-vlan)#name Ingeniería S3(config-vlan)#exit S3(config)#vlan 99 S3(config-vlan)#name Administración S3(config-vlan)#exit</pre>

Asignar la dirección IP de administración	S3(config)#int vlan 99 S3(config-if)#ip address 192.168.99.3 255.255.255.0
Asignar el gateway predeterminado.	S3(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	S3(config)#int f0/3 S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	S3(config-if)#interface range f0/1-2, f0/4-17, f0/19-24, g0/1-2 S3(config-if-range)#switchport mode access S3(config-if-range)#exit
Asignar F0/18 a la VLAN 23	S3(config)#int f0/18 S3(config-if)#switchport mode access S3(config-if)#switchport access vlan 23
Apagar todos los puertos sin usar	S3(config-if)#interface range f0/1-2, f0/4-17, f0/19-24, g0/1-2 S3(config-if-range)#shutdown

Tabla 10 Seguridad S3

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Se presenta la configuración de las subinterfaces en la interfaz g0/1 para las redes VLAN 21, VLAN 23 y VLAN 99, mediante encapsulamiento dot1q.

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en 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
Configurar la subinterfaz 802.1Q .23 en G0/1	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
Configurar la subinterfaz 802.1Q .99 en G0/1	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
Activar la interfaz G0/1	R1(config)#int g0/1 R1(config-if)#no shutdown

Tabla 11 Configuración R1

Paso 4: Verificar la conectividad de la red

Utilice el comando ping para probar la conectividad entre los switches y el R1.

Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

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

Tabla 12 Verificaciones de conectividad

Captura del ping realizado desde Switch 3 a Router 1, dirección Vlan 99. Ping a la ip 192.168.99.1

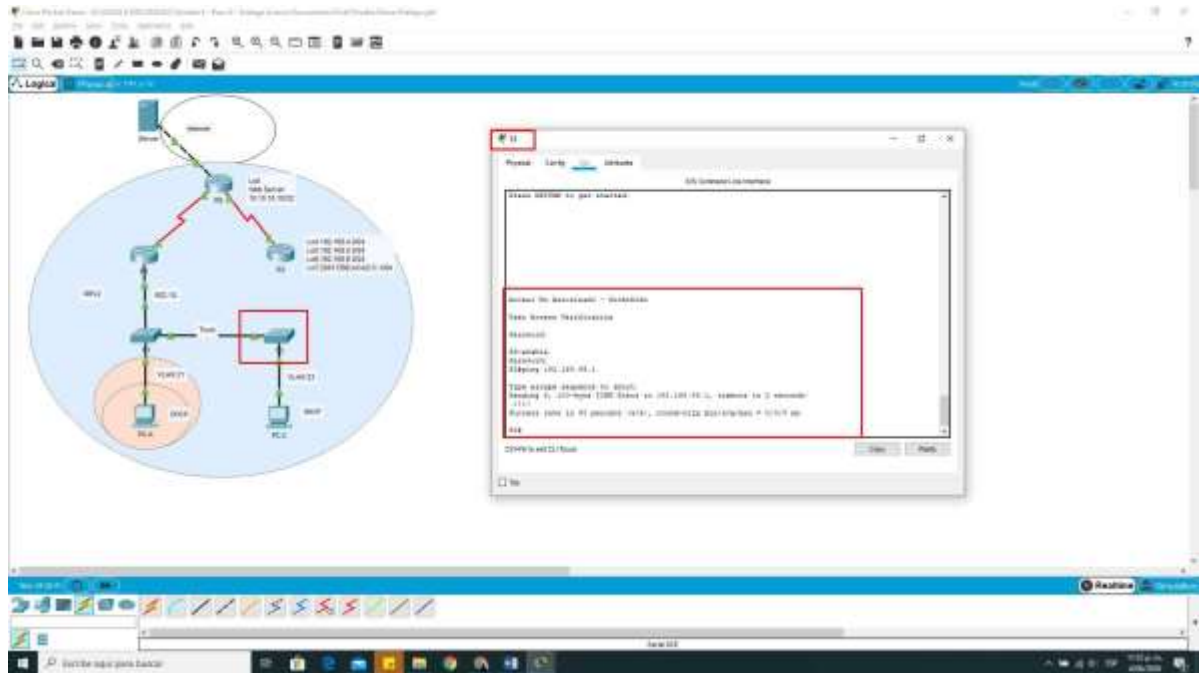


Figura 7 Ping desde S3 a R1, dirección Vlan 99. Ping 192.168.99.1

Captura del ping realizado desde Switch 1 a Router 1, dirección Vlan 21. Ping a la ip 192.168.21.1

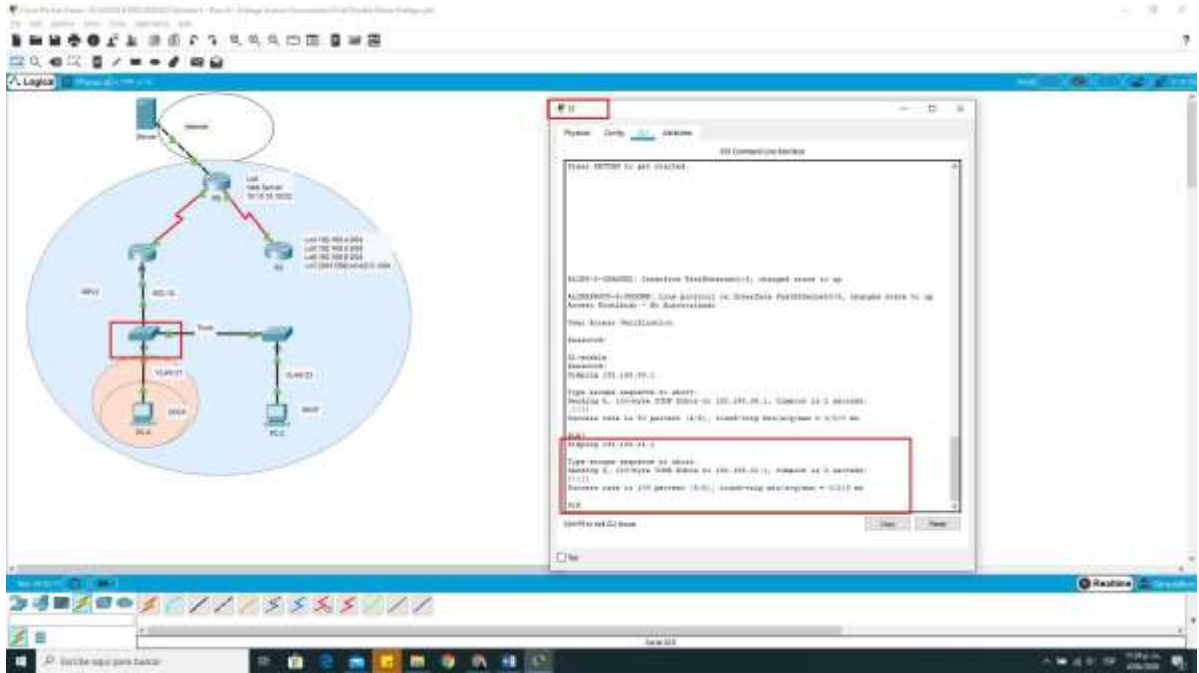


Figura 8 Ping desde S1 a R1, dirección Vlan 21. Ping 192.168.21.1

Parte 4: Configurar el protocolo de routing dinámico RIPv2

Paso 1: Configurar RIPv2 en el R1

Las tareas de configuración para R1 incluyen las siguientes:

A continuación, se presenta la configuración de RIP en Router 1, y se añaden las redes Vlan 21, Vlan 23, Vlan 99 y 170.16.1.0.

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	R1(config)#router rip R1(config-router)#ver 2
Anunciar las redes conectadas directamente	R1(config-router)#network 172.16.1.0 R1(config-router)#network 192.168.21.0 R1(config-router)#network 192.168.23.0 R1(config-router)#network 192.168.99.0
Establecer todas las interfaces LAN como pasivas	R1(config-router)#passive-interface g0/1.21 R1(config-router)#passive-interface g0/1.23 R1(config-router)#passive-interface g0/1.99
Desactive la summarización automática	R1(config-router)#no auto-summary

Tabla 13 Configuración RIP en R1

Paso 2: Configurar RIPv2 en el R2

La configuración del R2 incluye las siguientes tareas:

A continuación, se presenta la configuración de RIP versión 2 para el Router 2, y se añaden las redes 172.16.1.0 - 172.16.2.0 y la 10.10.10.0

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	R2(config)#router rip R2(config-router)#ver 2
Anunciar las redes conectadas directamente	R2(config-router)#network 172.16.1.0 R2(config-router)#network 172.16.2.0 R2(config-router)#network 10.10.10.0
Establecer la interfaz LAN (loopback) como pasiva	R2(config-router)#passive-interface loopback0
Desactive la sumarización automática.	R2(config-router)#no auto-summary

Tabla 14 Configuración RIP en R2

Paso 3: Configurar RIPv3 en el R3

La configuración del R3 incluye las siguientes tareas:

A continuación, se presenta la configuración de RIP versión 2 para el Router 3, y se añaden las redes 172.16.2.0 y las de loockback.

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	R3(config)#router rip R3(config-router)#version 2
Anunciar redes IPv4 conectadas directamente	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
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	R3(config-router)#passive-interface loopback4 R3(config-router)#passive-interface loopback5 R3(config-router)#passive-interface loopback6
Desactive la sumarización automática.	R3(config-router)#no auto-summary

Tabla 15 Configuración RIP en R3

Paso 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:

Se presenta el proceso de verificación de los enrutamientos mediante RIP y se analiza que estén configurados en el equipo Router 1.

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?	R3#show ip protocols
¿Qué comando muestra solo las rutas RIP?	R3#show ip route rip
¿Qué comando muestra la sección de RIP de la configuración en ejecución?	R3#show run section router rip R3#show run

Tabla 16 Verificación de RIP.

Captura de pantalla donde se evidencia la ejecución del comando “show run” del Router 1

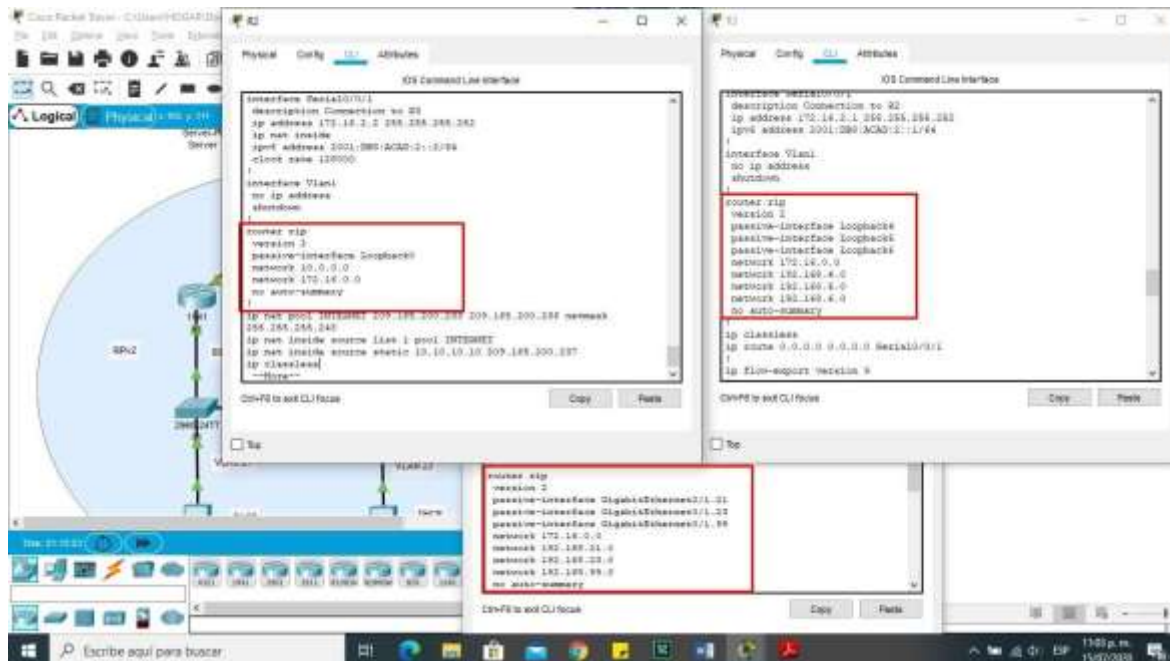


Figura 12 Comando show run

Parte 5: Implementar DHCP y NAT para IPv4

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

Las tareas de configuración para R1 incluyen las siguientes:

Se presenta la configuración del Router 1 y el servicio DHCP para que delegue direccionamiento a las redes Vlan 21 y Vlan 23, también se configura la reserva DHCP de las primeras 20 IPs para cada red.

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.21
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.21

Crear un pool de DHCP para la VLAN 21.	<pre>R1(config)#ip dhcp pool ACCT R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#network 192.168.21.0 255.255.255.0 R1(dhcp-config)#default-router 192.168.21.1</pre>
Crear un pool de DHCP para la VLAN 23	<pre>R1(config)#ip dhcp pool Ingeniria R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#default-router 192.168.23.1 R1(dhcp-config)#network 192.168.23.0 255.255.255.0</pre>

Tabla 17 DHCP y NAT IPv4 en R1

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

La configuración del R2 incluye las siguientes tareas:

Se realiza la configuración de NAT estática, para que desde internet el servidor con Lan 10.10.10.10 sea visible con la ip 209.165.200.229.

Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	<pre>R2(config)#username webuser privilege 15 secret cisco12345</pre>

Habilitar el servicio del servidor HTTP	R2(config)#ip http server
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	R2(config)#ip http authentication local
Crear una NAT estática al servidor web.	R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229
Asignar la interfaz interna y externa para la NAT estática	R2(config)#interface g0/0 R2(config-if)#ip nat outside R2(config)#interface s0/0/0 R2(config-if)#ip nat inside R2(config-if)#interface s0/0/1 R2(config-if)#ip nat inside
Configurar la NAT dinámica dentro de una ACL privada	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
Defina el pool de direcciones	R2(config)#ip nat pool INTERNET 209.165.200.233 209.165.200.236 netmask 255.255.255.248

IP públicas utilizables.	
Definir la traducción de NAT dinámica	R2(config)#ip nat inside source list 1 pool INTERNET

Tabla 18 DHCP y NAT IPv4 en R2

Paso 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.

Se procede a verificar el servicio DHCP tanto en PC-A como en PC-C y la conectividad entre los dos equipos realizando un ping a la ip 192.168.23.21.

Figura 12 Configuración PC-A

Figura 13 Configuración PC-C

Figura 14 Conectividad entre PC-A y PC-C

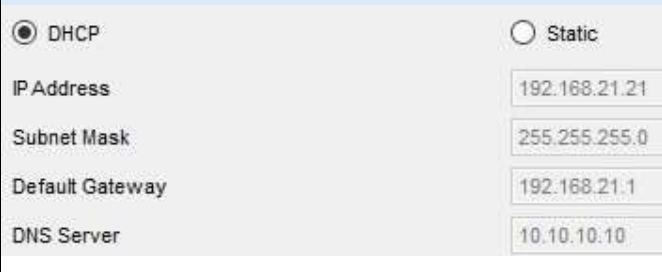
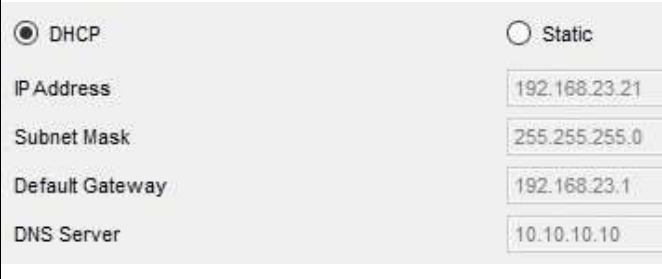
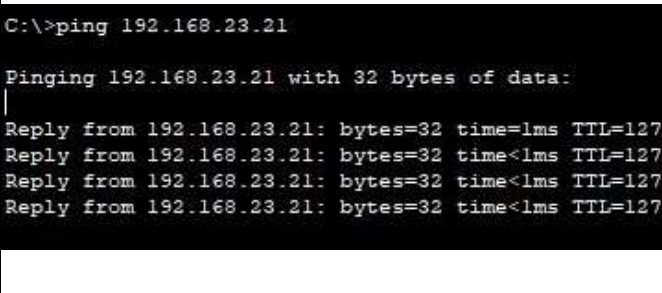
Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	 <p> <input checked="" type="radio"/> DHCP <input type="radio"/> Static IP Address: 192.168.21.21 Subnet Mask: 255.255.255.0 Default Gateway: 192.168.21.1 DNS Server: 10.10.10.10 </p>
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	 <p> <input checked="" type="radio"/> DHCP <input type="radio"/> Static IP Address: 192.168.23.21 Subnet Mask: 255.255.255.0 Default Gateway: 192.168.23.1 DNS Server: 10.10.10.10 </p>
Verificar que la PC-A pueda hacer ping a la PC-C Nota: Quizá sea necesario deshabilitar el firewall de la PC.	 <pre> C:\>ping 192.168.23.21 Pinging 192.168.23.21 with 32 bytes of data: Reply from 192.168.23.21: bytes=32 time=1ms TTL=127 Reply from 192.168.23.21: bytes=32 time<1ms TTL=127 Reply from 192.168.23.21: bytes=32 time<1ms TTL=127 Reply from 192.168.23.21: bytes=32 time<1ms TTL=127 </pre>
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	<p style="text-align: center;"><i>ip http server</i></p>

Tabla 19 Verificaciones DHCP y NAT.

Pantallazo donde se evidencia el ingreso al navegador web en la computadora de Internet, ingresando al servidor web con la siguiente ip (209.165.200.229). Se inicia sesión con el nombre de usuario **webuser** y la contraseña **cisco12345**.

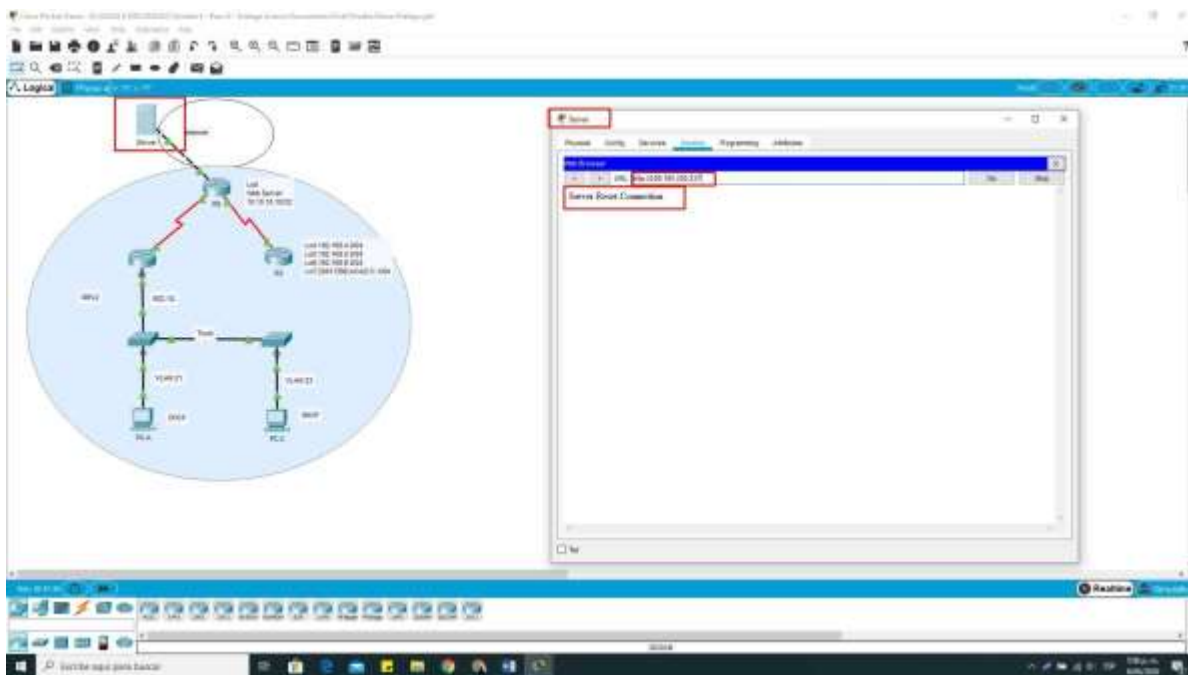


Figura 15 Servidor Web 209.165.200.229

Parte 6: Configurar NTP

Se realiza la configuración y ajuste de fecha y hora en el Router 2, adicional se establece que el Router 2 como maestro NTP, al Router 1 como cliente NTP y se establece para actualizaciones de calendario; finalmente se realiza verificación de las configuraciones realizadas.

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	R2#clock set 09:00:00 5 march 2016
Configure R2 como un maestro NTP.	R2(config)#ntp master 5
Configurar R1 como un cliente NTP.	R1(config)#ntp server 172.16.1.2
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	R1(config)#ntp update-calendar
Verifique la configuración de NTP en R1.	R1#show ntp associations

Tabla 20 Configuración NTP

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

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

A continuación, se establece que el Router 1 sea, el único que tenga conexión Telnet con Router 2, se asigna un nombre a la ACL y se verifica el funcionamiento de la configuración realizada.

Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	R2(config)#ip access-list standard ADMIN-MGT R2(config-std-nacl)#permit host 172.16.1.1
Aplicar la ACL con nombre a las líneas VTY	R2(config)#line vty 0 15 R2(config-line)#access-class ADMIN-MGT in
Permitir acceso por Telnet a las líneas de VTY	R2(config-line)#transport input telnet
Verificar que la ACL funcione como se espera	R1#telnet 172.16.1.2 R3#telnet 172.16.1.2

Tabla 21 Continuación de ACL

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	R2#show access-list R2#show ip access-list
Restablecer los contadores de una lista de acceso	R2#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?	R2#show ip interfaces
¿Con qué comando se muestran las traducciones NAT?	R2#show ip nat translations
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	R2#clear ip nat translation *

Tabla 22 Visualización de Access list.

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.

Topología de red

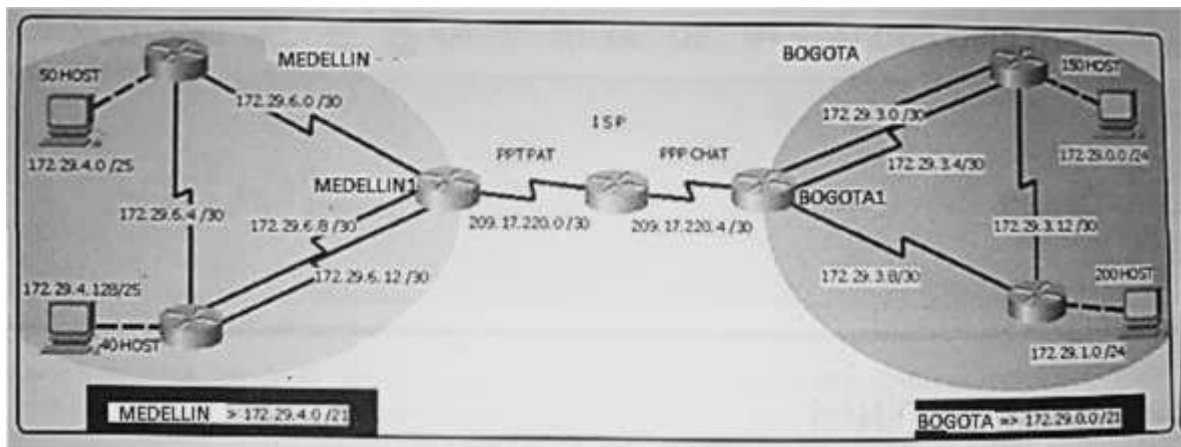


Figura 18 Escenario 2

Este escenario plantea el uso de OSPF como protocolo de enrutamiento, considerando que se tendrán 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).
- Realizar la conexión física de los equipos con base en la topología de red

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

A continuación, se presenta la configuración básica realizada al router ISP, el cual se conectará a cada uno de los router principales Medellin1 y Bogota1. Y adicional se presenta también la configuración básica realizada a cada uno de los routers de las redes de Bogotá y Medellin, configurando nombre de equipo, contraseñas, y mensaje motd.

Router	Comando
ISP	<pre> Router>enable Router#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Router(config)#no ip domain-lookup Router(config)#hostname ISP ISP(config)#enable secret class ISP(config)#line console 0 ISP(config-line)# password cisco ISP(config-line)# login ISP(config-line)# exit ISP(config)#line vty 0 15 ISP(config-line)# password cisco </pre>

	<pre>ISP(config-line)# login ISP(config-line)#service password-encryption ISP(config)#banner motd %Prohibido el acceso - No Autorizado por Diana Hidalgo!!!% ISP(config)#end ISP#wr %SYS-5-CONFIG_I: Configured from console by console Building configuration... [OK]</pre>
BOGOTA1	<pre>Router>enable Router#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Router(config)#no ip domain-lookup Router(config)#hostname BOGOTA1 BOGOTA1(config)#enable secret class BOGOTA1(config)#line console 0 BOGOTA1(config-line)# password cisco BOGOTA1(config-line)# login BOGOTA1(config-line)# exit BOGOTA1(config)#line vty 0 15 BOGOTA1(config-line)# password cisco BOGOTA1(config-line)# login BOGOTA1(config-line)#service password-encryption BOGOTA1(config)#banner motd %Prohibido el acceso - No Autorizado por Diana Hidalgo!!!% BOGOTA1(config)#end BOGOTA1# %SYS-5-CONFIG_I: Configured from console by console BOGOTA1#wr</pre>

	<pre>Building configuration... [OK]</pre>
BOGOTA2	<pre>Router>enable Router#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Router(config)#no ip domain-lookup Router(config)#hostname BOGOTA2 BOGOTA2(config)#enable secret class BOGOTA2(config)#line console 0 BOGOTA2(config-line)# password cisco BOGOTA2(config-line)# login BOGOTA2(config-line)# exit BOGOTA2(config)#line vty 0 15 BOGOTA2(config-line)# password cisco BOGOTA2(config-line)# login BOGOTA2(config-line)#service password-encryption BOGOTA2(config)#banner motd %Prohibido el acceso - No Autorizado por Diana Hidalgo!!!% BOGOTA2(config)#end BOGOTA2#wr Building configuration... [OK] BOGOTA2# %SYS-5-CONFIG_I: Configured from console by console</pre>
BOGOTA3	<pre>Router>enable Router#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Router(config)#no ip domain-lookup Router(config)#hostname BOGOTA3</pre>

	<pre> BOGOTA3(config)#enable secret class BOGOTA3(config)#line console 0 BOGOTA3(config-line)# password cisco BOGOTA3(config-line)# login BOGOTA3(config-line)# exit BOGOTA3(config)#line vty 0 15 BOGOTA3(config-line)# password cisco BOGOTA3(config-line)# login BOGOTA3(config-line)#service password-encryption BOGOTA3(config)#banner motd %Prohibido el acceso - No Autorizado por Diana Hidalgo!!!% BOGOTA3(config)#end BOGOTA3#wr %SYS-5-CONFIG_I: Configured from console by console </pre>
MEDELLIN1	<pre> Router>enable Router#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Router(config)#no ip domain-lookup Router(config)#hostname MEDELLIN1 MEDELLIN1(config)#enable secret class MEDELLIN1(config)#line console 0 MEDELLIN1(config-line)# password cisco MEDELLIN1(config-line)# login MEDELLIN1(config-line)# exit MEDELLIN1(config)#line vty 0 15 MEDELLIN1(config-line)# password cisco MEDELLIN1(config-line)# login MEDELLIN1(config-line)#service password-encryption </pre>

	<pre> MEDELLIN1(config)#banner motd %Prohibido el acceso - No Autorizado por Diana Hidalgo!!!% MEDELLIN1(config)#end MEDELLIN1#wr Building configuration... [OK] MEDELLIN1# %SYS-5-CONFIG_I: Configured from console by console </pre>
MEDELLIN2	<pre> Router>enable Router#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Router(config)#no ip domain-lookup Router(config)#hostname MEDELLIN2 MEDELLIN2(config)#enable secret class MEDELLIN2(config)#line console 0 MEDELLIN2(config-line)# password cisco MEDELLIN2(config-line)# login MEDELLIN2(config-line)# exit MEDELLIN2(config)#line vty 0 15 MEDELLIN2(config-line)# password cisco MEDELLIN2(config-line)# login MEDELLIN2(config-line)#service password-encryption MEDELLIN2(config)#banner motd %Prohibido el acceso - No Autorizado por Diana Hidalgo!!!% MEDELLIN2(config)#end MEDELLIN2#wr Building configuration... [OK] MEDELLIN2# </pre>

	%SYS-5-CONFIG_I: Configured from console by console
MEDELLIN3	<pre> Router>enable Router#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Router(config)#no ip domain-lookup Router(config)#hostname MEDELLIN3 MEDELLIN3(config)#enable secret class MEDELLIN3(config)#line console 0 MEDELLIN3(config-line)# password cisco MEDELLIN3(config-line)# login MEDELLIN3(config-line)# exit MEDELLIN3(config)#line vty 0 15 MEDELLIN3(config-line)# password cisco MEDELLIN3(config-line)# login MEDELLIN3(config-line)#service password-encryption MEDELLIN3(config)#banner motd %Prohibido el acceso - No Autorizado por Diana Hidalgo!!!% MEDELLIN3(config)#end MEDELLIN3#wr Building configuration... [OK] MEDELLIN3# %SYS-5-CONFIG_I: Configured from console by console </pre>

Tabla 23 Configuración inicial de dispositivos

Se presenta la conexión física de los equipos, tomando como base la topología de red dada:

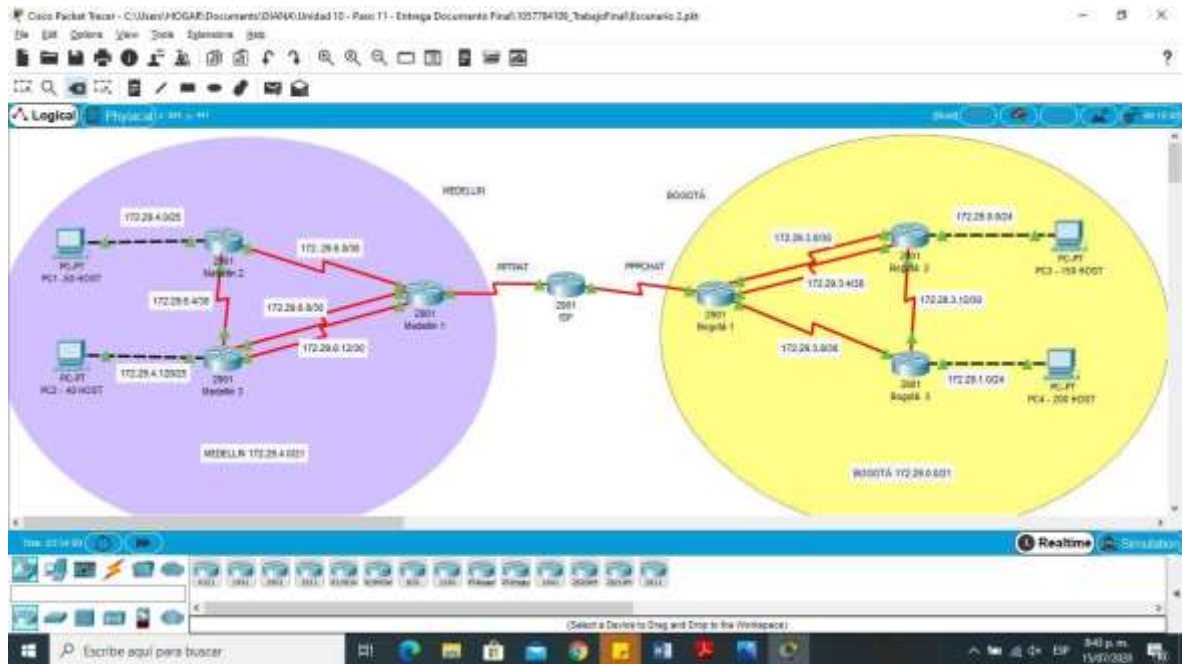


Figura 19 Topologia Red Escenario 2

A continuación, se presenta la tabla de conexión física de los equipos

ROUTER	INTERF AZ	IPV4	MASCARA	WILCARD	GATEW AY
ISP	Se0/0/0	209.17.220.1	255.255.255.252	0.0.0.3	N/A
	Se0/0/1	209.17.220.5	255.255.255.252	0.0.0.3	N/A
Medellin1	Se0/0/0	172.29.6.9	255.255.255.252	0.0.0.3	N/A
	Se0/0/1	172.29.6.1	255.255.255.252	0.0.0.3	N/A
	Se0/1/0	172.29.6.13	255.255.255.252	0.0.0.3	N/A
	Se0/1/1	209.17.220.2	255.255.255.252	0.0.0.3	N/A
Medellin2	Se0/0/0	172.29.6.5	255.255.255.252	0.0.0.3	N/A
	Se0/0/1	172.29.6.2	255.255.255.252	0.0.0.3	N/A
	G0/0	172.29.4.1	255.255.255.128	0.0.0.127	N/A
Medellin3	Se0/0/0	172.29.6.6	255.255.255.252	0.0.0.3	N/A
	Se0/0/1	172.29.6.10	255.255.255.252	0.0.0.3	N/A
	Se0/1/0	172.29.6.14	255.255.255.252	0.0.0.3	N/A
	G0/0	172.29.4.129	255.255.255.128	0.0.0.127	N/A
Bogota1	Se0/0/0	209.17.220.6	255.255.255.252	0.0.0.3	N/A
	Se0/0/1	172.29.3.1	255.255.255.252	0.0.0.3	N/A
	Se0/1/0	172.29.3.9	255.255.255.252	0.0.0.3	N/A
	Se0/1/1	172.29.3.5	255.255.255.252	0.0.0.3	N/A
Bogota2	Se0/0/0	172.29.3.2	255.255.255.252	0.0.0.3	N/A
	Se0/0/1	172.29.3.13	255.255.255.252	0.0.0.3	N/A
	Se0/1/0	172.29.3.6	255.255.255.252	0.0.0.3	N/A

	G0/0	172.29.0.1	255.255.255.0	0.0.0.255	N/A
Bogota3	Se0/0/0	172.29.3.10	255.255.255.252	0.0.0.3	N/A
	Se0/0/1	172.29.3.14	255.255.255.252	0.0.0.3	N/A
	G0/0	172.29.1.1	255.255.255.0	0.0.0.255	N/A
PC1	NIC	DHCP	255.255.255.128	0.0.0.127	172.29.4 .1
PC2	NIC	DHCP	255.255.255.128	0.0.0.127	172.29.4 .129
PC3	NIC	DHCP	255.255.255.0	0.0.0.255	172.29.0 .1
PC4	NIC	DHCP	255.255.255.0	0.0.0.255	172.29.1 .1

Tabla 24 Conexión física de los equipos

Parte 1: Configuración del enrutamiento

A continuación, se realiza la configuración de las interfaces s0/0/0 y s0/0/1, las cuales conectan al router ISP con Medellin1 y Bogota1 respectivamente.

Además, se presenta la configuración de todas las interfaces con el fin de establecer conexión entre todos los routers y dispositivos del lado de Bogotá, los direccionamientos se configuran de acuerdo a figura presentada Topología Red Escenario 2.

Adicional se realiza la configuración de todas las interfaces para establecer conexión entre todos los routers y dispositivos del lado de Medellín, los direccionamientos se configuran de acuerdo a figura presentada Topología Red Escenario 2.

Router	Comandos
ISP	<pre> ISP#configure terminal Enter configuration commands, one per line. End with CNTL/Z. ISP(config)#interface serial0/0/0 ISP(config-if)#description conexion ISP-MEDELLIN1 ISP(config-if)#ip address 209.17.220.1 255.255.255.252 ISP(config-if)#clock rate 128000 ISP(config-if)#no shutdown %LINK-5-CHANGED: Interface Serial0/0/0, changed state to down ISP(config-if)#interface serial0/0/1 ISP(config-if)#description conexion ISP-BOGOTA1 </pre>

	<pre> ISP(config-if)#ip address 209.17.220.5 255.255.255.252 ISP(config-if)#clock rate 128000 ISP(config-if)#no shutdown %LINK-5-CHANGED: Interface Serial0/0/1, changed state to down ISP(config-if)#end ISP# %SYS-5-CONFIG_I: Configured from console by console ISP#cop run st Destination filename [startup-config]? Building configuration... [OK] ISP# </pre>
MEDELLIN1	<pre> Password: MEDELLIN1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. MEDELLIN1(config)#interface serial0/0/0 MEDELLIN1(config-if)#description conexion MEDELLIN1.0 a MEDELLIN3.0 MEDELLIN1(config-if)#ip address 172.29.6.9 255.255.255.252 MEDELLIN1(config-if)#clock rate 128000 MEDELLIN1(config-if)#no shutdown %LINK-5-CHANGED: Interface Serial0/0/0, changed state to down MEDELLIN1(config-if)# MEDELLIN1(config-if)# MEDELLIN1(config-if)#interface serial0/0/1 MEDELLIN1(config-if)#description conexion MEDELLIN1 a MEDELLIN2 MEDELLIN1(config-if)#ip address 172.29.6.1 255.255.255.252 MEDELLIN1(config-if)#clock rate 128000 MEDELLIN1(config-if)#no shutdown %LINK-5-CHANGED: Interface Serial0/0/1, changed state to down MEDELLIN1(config-if)# MEDELLIN1(config-if)#interface serial0/1/0 MEDELLIN1(config-if)#description conexion MEDELLIN1.1 a MEDELLIN3.1 MEDELLIN1(config-if)#ip address 172.29.6.13 255.255.255.252 </pre>

	<pre> MEDELLIN1(config-if)#clock rate 128000 MEDELLIN1(config-if)#no shutdown %LINK-5-CHANGED: Interface Serial0/1/0, changed state to down MEDELLIN1(config)#interface serial0/1/1 MEDELLIN1(config-if)#description conexion MEDELLIN1 a ISP MEDELLIN1(config-if)#ip address 209.17.220.2 255.255.255.252 MEDELLIN1(config-if)#no shutdown MEDELLIN1(config-if)#end MEDELLIN1#cop run st %SYS-5-CONFIG_: Configured from console by console Destination filename [startup-config]? Building configuration... [OK] </pre>
MEDELLIN2	<pre> MEDELLIN2>en Password: MEDELLIN2#configure terminal Enter configuration commands, one per line. End with CNTL/Z. MEDELLIN2(config)#interface serial0/0/0 MEDELLIN2(config-if)#description conexion MEDELLIN2 a MEDELLIN3 MEDELLIN2(config-if)#ip address 172.29.6.5 255.255.255.252 MEDELLIN2(config-if)#no shutdown %LINK-5-CHANGED: Interface Serial0/0/0, changed state to down MEDELLIN2(config-if)# MEDELLIN2(config-if)# MEDELLIN2(config-if)#interface serial0/0/1 MEDELLIN2(config-if)#description conexion MEDELLIN2 a MEDELLIN1 MEDELLIN2(config-if)#ip address 172.29.6.2 255.255.255.252 MEDELLIN2(config-if)#clock rate 128000 This command applies only to DCE interfaces MEDELLIN2(config-if)#no shutdown MEDELLIN2(config-if)# %LINK-5-CHANGED: Interface Serial0/0/1, changed state to up </pre>

	<pre> MEDELLIN2(config-if)# MEDELLIN2(config-if)#interface g0/0 MEDELLIN2(config-if)#description conexion MEDELLIN2 a 50 host MEDELLIN2(config-if)#ip address 172.29.4.1 255.255.255.128 MEDELLIN2(config-if)#no shutdown MEDELLIN2(config-if)# %LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up MEDELLIN2(config-if)#end MEDELLIN2# %SYS-5-CONFIG_I: Configured from console by console </pre>
MEDELLIN3	<pre> MEDELLIN3>en Password: MEDELLIN3#configure terminal Enter configuration commands, one per line. End with CNTL/Z. MEDELLIN3(config)#interface serial0/0/0 MEDELLIN3(config-if)#description conexion MEDELLIN3 a MEDELLIN2 MEDELLIN3(config-if)#ip address 172.29.6.6 255.255.255.252 MEDELLIN3(config-if)#no shutdown MEDELLIN3(config-if)# %LINK-5-CHANGED: Interface Serial0/0/0, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up MEDELLIN3(config-if)#interface serial0/0/1 MEDELLIN3(config-if)#description conexion MEDELLIN3.1 a MEDELLIN1.1 MEDELLIN3(config-if)#ip address 172.29.6.10 255.255.255.252 MEDELLIN3(config-if)#clock rate 128000 This command applies only to DCE interfaces </pre>

	<pre> MEDELLIN3(config-if)#no shutdown MEDELLIN3(config-if)# %LINK-5-CHANGED: Interface Serial0/0/1, changed state to up MEDELLIN3(config-if)# %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up MEDELLIN3(config-if)#interface serial0/1/0 MEDELLIN3(config-if)#description conexion MEDELLIN3.0 a MEDELLIN1.0 MEDELLIN3(config-if)#ip address 172.29.6.14 255.255.255.252 MEDELLIN3(config-if)#no shutdown MEDELLIN3(config-if)# %LINK-5-CHANGED: Interface Serial0/1/0, changed state to up MEDELLIN3(config-if)# %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed state to up MEDELLIN3(config-if)#interface g0/0 MEDELLIN3(config-if)#description conexion MEDELLIN3 a 40 host MEDELLIN3(config-if)#ip address 172.29.4.129 255.255.255.128 MEDELLIN3(config-if)#no shutdown MEDELLIN3(config-if)#end MEDELLIN3#cop run st %LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up %SYS-5-CONFIG_: Configured from console by console Destination filename [startup-config]? Building configuration... [OK] MEDELLIN3# </pre>
BOGOTA1	<pre> BOGOTA1>en Password: BOGOTA1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. </pre>

<pre>BOGOTA1(config)#interface serial0/0/0 BOGOTA1(config-if)#description conexion BOGOTA1 a ISP BOGOTA1(config-if)#ip address 209.17.220.6 255.255.255.252 BOGOTA1(config-if)#clock rate 128000 This command applies only to DCE interfaces BOGOTA1(config-if)#no shutdown BOGOTA1(config-if)# %LINK-5-CHANGED: Interface Serial0/0/0, changed state to up BOGOTA1(config-if)# %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up BOGOTA1(config-if)#interface serial0/0/1 BOGOTA1(config-if)#description conexion BOGOTA1 a BOGOTA2 BOGOTA1(config-if)#ip address 172.29.3.1 255.255.255.252 BOGOTA1(config-if)#clock rate 128000 BOGOTA1(config-if)#no shutdown %LINK-5-CHANGED: Interface Serial0/0/1, changed state to down BOGOTA1(config-if)# BOGOTA1(config-if)# BOGOTA1(config-if)#interface serial0/1/0 BOGOTA1(config-if)#description conexion BOGOTA1 a BOGOTA3 BOGOTA1(config-if)#ip address 172.29.3.9 255.255.255.252 BOGOTA1(config-if)#clock rate 128000 BOGOTA1(config-if)#no shutdown %LINK-5-CHANGED: Interface Serial0/1/0, changed state to down BOGOTA1(config-if)# BOGOTA1(config-if)#interface serial0/1/1 BOGOTA1(config-if)#description conexion BOGOTA1 a BOGOTA2 BOGOTA1(config-if)#ip address 172.29.3.5 255.255.255.252 BOGOTA1(config-if)#clock rate 128000 BOGOTA1(config-if)#no shutdown BOGOTA1(config-if)# %LINK-5-CHANGED: Interface Serial0/1/1, changed state to up BOGOTA1(config-if)#end</pre>
--

	<pre> BOGOTA1# %SYS-5-CONFIG_I: Configured from console by console BOGOTA1# %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/1, changed state to up BOGOTA1#cop run st Destination filename [startup-config]? Building configuration... [OK] BOGOTA1# </pre>
BOGOTA2	<pre> BOGOTA2>en Password: BOGOTA2#configure terminal Enter configuration commands, one per line. End with CNTL/Z. BOGOTA2(config)#interface serial0/0/0 BOGOTA2(config-if)#description conexion BOGOTA2 a BOGOTA1 BOGOTA2(config-if)#ip address 172.29.3.2 255.255.255.252 BOGOTA2(config-if)#no shutdown BOGOTA2(config-if)# %LINK-5-CHANGED: Interface Serial0/0/0, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up BOGOTA2(config-if)#interface serial0/0/1 BOGOTA2(config-if)#description conexion BOGOTA2 a BOGOTA3 BOGOTA2(config-if)#ip address 172.29.3.13 255.255.255.252 BOGOTA2(config-if)#clock rate 128000 BOGOTA2(config-if)#no shutdown %LINK-5-CHANGED: Interface Serial0/0/1, changed state to down BOGOTA2(config-if)# BOGOTA2(config-if)#interface serial0/1/0 BOGOTA2(config-if)#description conexion BOGOTA2 a BOGOTA1 </pre>

	<pre> BOGOTA2(config-if)#ip address 172.29.3.6 255.255.255.252 BOGOTA2(config-if)#no shutdown BOGOTA2(config-if)# BOGOTA2(config-if)#interface serial0/1/0 BOGOTA2(config-if)#description conexion BOGOTA2 a BOGOTA1 BOGOTA2(config-if)#ip address 172.29.3.6 255.255.255.252 BOGOTA2(config-if)#clock rate 128000 This command applies only to DCE interfaces BOGOTA2(config-if)#no shutdown BOGOTA2(config-if)# BOGOTA2(config-if)# BOGOTA2(config-if)#interface g0/0 BOGOTA2(config-if)#description conexion BOGOTA2 a 150 host BOGOTA2(config-if)#ip address 172.29.0.1 255.255.255.0 BOGOTA2(config-if)#no shutdown BOGOTA2(config-if)#end BOGOTA2#cop run st Destination filename [startup-config]? %LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up %SYS-5-CONFIG_I: Configured from console by console Building configuration... [OK] </pre>
BOGOTA3	<pre> BOGOTA3>en Password: BOGOTA3#configure terminal Enter configuration commands, one per line. End with CNTL/Z. BOGOTA3(config)#interface serial0/0/0 BOGOTA3(config-if)#description conexion BOGOTA3 a BOGOTA1 BOGOTA3(config-if)#ip address 172.29.3.10 255.255.255.252 BOGOTA3(config-if)#no shutdown BOGOTA3(config-if)# </pre>

	<pre> %LINK-5-CHANGED: Interface Serial0/0/0, changed state to up BOGOTA3(config-if)# %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up BOGOTA3(config-if)#interface serial0/0/1 BOGOTA3(config-if)#description conexion BOGOTA3 a BOGOTA2 BOGOTA3(config-if)#ip address 172.29.3.14 255.255.255.252 BOGOTA3(config-if)#no shutdown BOGOTA3(config-if)# %LINK-5-CHANGED: Interface Serial0/0/1, changed state to up BOGOTA3(config-if)#interface g0/0 BOGOTA3(config-if)#description conexion BOGOTA3 a 200 host BOGOTA3(config-if)#ip address 172.29.1.1 255.255.255.0 BOGOTA3(config-if)#no shutdown BOGOTA3(config-if)#end BOGOTA3#cop run st %LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up %SYS-5-CONFIG_1: Configured from console by console %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up Destination filename [startup-config]? Building configuration... [OK] </pre>
--	--

Tabla 25 Configuración de enrutamiento

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

MEDELLIN1

```
MEDELLIN1>en
Password:
MEDELLIN1#config t
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN1(config)#router ospf 1
MEDELLIN1(config-router)#router-id 1.1.1.1
MEDELLIN1(config-router)#do sh ip route conn
C 172.29.6.0/30 is directly connected, Serial0/0/1
C 172.29.6.8/30 is directly connected, Serial0/0/0
C 172.29.6.12/30 is directly connected, Serial0/1/0
C 209.17.220.0/30 is directly connected, Serial0/1/1
MEDELLIN1(config-router)#network 172.29.6.0 0.0.0.3 area 0
MEDELLIN1(config-router)#network 172.29.8.0 0.0.0.3 area 0
MEDELLIN1(config-router)#no network 172.29.8.0 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
MEDELLIN1(config-router)#end
MEDELLIN1#
%SYS-5-CONFIG_I: Configured from console by console
MEDELLIN1#cop run st
Destination filename [startup-config]?
Building configuration...
[OK]
MEDELLIN1#
```

00:29:24: %OSPF-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Serial0/0/1 from LOADING to FULL,
Loading Done

MEDELLIN2

```
MEDELLIN2>en
Password:
MEDELLIN2#config t
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN2(config)#router ospf 1
MEDELLIN2(config-router)#router-id 2.2.2.2
MEDELLIN2(config-router)#do sh ip route conn
C 172.29.4.0/25 is directly connected, GigabitEthernet0/0
C 172.29.6.0/30 is directly connected, Serial0/0/1
C 172.29.6.4/30 is directly connected, Serial0/0/0
MEDELLIN2(config-router)#network 172.29.4.0 0.0.0.127 area 0
MEDELLIN2(config-router)#network 172.29.6.0 0.0.0.3 area 0
MEDELLIN2(config-router)#network 172.29.6.4 0.0.0.3 area 0
MEDELLIN2(config-router)#end
MEDELLIN2#cop run st
Destination filename [startup-config]?
%SYS-5-CONFIG_: Configured from console by console
Building configuration...
[OK]
MEDELLIN2#
00:50:46: %OSPF-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/1 from LOADING to FULL,
Loading Done
```

MEDELLIN3

```
MEDELLIN3>en
Password:
```

```
MEDELLIN3#config t
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN3(config)#router ospf 1
MEDELLIN3(config-router)#router-id 3.3.3.3
MEDELLIN3(config-router)#do sh ip route conn
C 172.29.4.128/25 is directly connected, GigabitEthernet0/0
C 172.29.6.4/30 is directly connected, Serial0/0/0
C 172.29.6.8/30 is directly connected, Serial0/0/1
C 172.29.6.12/30 is directly connected, Serial0/1/0
MEDELLIN3(config-router)#network 172.29.4.128 0.0.0.127 area 0
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)#end
MEDELLIN3#cop run st
%SYS-5-CONFIG_I: Configured from console by console
00:58:36: %OSPF-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/1 from LOADING to FULL,
Loading Done
00:58:36: %OSPF-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/1/0 from LOADING to FULL,
Loading Done
00:58:37: %OSPF-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Serial0/0/0 from LOADING to FULL,
Loading Done
```

BOGOTA1

```
BOGOTA1>en
Password:
BOGOTA1#config t
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA1(config)#router ospf 1
BOGOTA1(config-router)#router-id 4.4.4.4
BOGOTA1(config-router)#do sh ip route conn
C 172.29.3.0/30 is directly connected, Serial0/0/1
```

```
C 172.29.3.4/30 is directly connected, Serial0/1/1
C 172.29.3.8/30 is directly connected, Serial0/1/0

C 209.17.220.4/30 is directly connected, Serial0/0/0

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)#network 209.17.220.4 0.0.0.3 area 0
BOGOTA1(config-router)#end
BOGOTA1#cop run st
%SYS-5-CONFIG_I: Configured from console by console

Destination filename [startup-config]?
Building configuration...
[OK]
BOGOTA1#
```

BOGOTA2

```
BOGOTA2>en
Password:
BOGOTA2#config t
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA2(config)#router ospf 1
BOGOTA2(config-router)#router-id 5.5.5.5
BOGOTA2(config-router)#do sh ip route conn
C 172.29.0.0/24 is directly connected, GigabitEthernet0/0
C 172.29.3.0/30 is directly connected, Serial0/0/0
C 172.29.3.4/30 is directly connected, Serial0/1/0
C 172.29.3.12/30 is directly connected, Serial0/0/1

BOGOTA2(config-router)#network 172.29.0.0 0.0.0.255 area 0
BOGOTA2(config-router)#network 172.29.3.0 0.0.0.3 area 0
```

```
BOGOTA2(config-router)#network 172.29.3.4 0.0.0.3 area 0
BOGOTA2(config-router)#network 172.29.3.12 0.0.0.3 area 0

BOGOTA2(config-router)#end
BOGOTA2#cop run st
%SYS-5-CONFIG_I: Configured from console by console

Destination filename [startup-config]?
Building configuration...
[OK]
BOGOTA2#
01:07:25: %OSPF-5-ADJCHG: Process 1, Nbr 4.4.4.4 on Serial0/0/0 from LOADING to FULL,
Loading Done

01:07:25: %OSPF-5-ADJCHG: Process 1, Nbr 4.4.4.4 on Serial0/1/0 from LOADING to FULL,
Loading Done
```

BOGOTA3

```
BOGOTA3>en
Password:
BOGOTA3#config t
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA3(config)#router ospf 1
BOGOTA3(config-router)#router-id 6.6.6.6
BOGOTA3(config-router)#do sh ip route conn
C 172.29.1.0/24 is directly connected, GigabitEthernet0/0
C 172.29.3.8/30 is directly connected, Serial0/0/0
C 172.29.3.12/30 is directly connected, Serial0/0/1
BOGOTA3(config-router)#network 172.29.1.0 0.0.0.255 area 0
```

```
BOGOTA3(config-router)#network 172.29.3.8 0.0.0.3 area 0

BOGOTA3(config-router)#network 172.29.3.12 0.0.0.3 area 0
BOGOTA3(config-router)#network 172.29.3.12 0.0.0.3 area 0
BOGOTA3(config-router)#end
BOGOTA3#cop run st
Destination filename [startup-config]?
%SYS-5-CONFIG_I: Configured from console by console

01:11:21: %OSPF-5-ADJCHG: Process 1, Nbr 5.5.5.5 on Serial0/0/1 from LOADING to FULL,
Loading Done

Building configuration...
[OK]
BOGOTA3#
01:11:26: %OSPF-5-ADJCHG: Process 1, Nbr 4.4.4.4 on Serial0/0/0 from LOADING to FULL,
Loading Done
```

Tabla 26 Configurar el enrutamiento en la red usando el protocolo OSPF versión 2.

- a. 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.

Se realiza la configuración routers Bogota1 y Medellín1 para establecer una ruta determinada hacia el Router ISP. Y adicional se verifican las publicaciones OSPF

MEDELLIN1
<pre> MEDELLIN1# MEDELLIN1#config t Enter configuration commands, one per line. End with CNTL/Z. MEDELLIN1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.1 MEDELLIN1(config)#router ospf 1 MEDELLIN1(config-router)#default-information originate MEDELLIN1(config-router)#end MEDELLIN1#cop run st %SYS-5-CONFIG_I: Configured from console by console Destination filename [startup-config]? Building configuration... [OK] MEDELLIN1# </pre>
BOGOTA1
<pre> Password: BOGOTA1# BOGOTA1#config t Enter configuration commands, one per line. End with CNTL/Z. </pre>

```

BOGOTA1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.5
BOGOTA1(config)#router ospf 1
BOGOTA1(config-router)#default-information originate
BOGOTA1(config-router)#end
BOGOTA1#cop run st
Destination filename [startup-config]?
%SYS-5-CONFIG_I: Configured from console by console
Building configuration...
[OK]
BOGOTA1#

```

Tabla 27 Publicaciones de OSPF

- b. 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.**

Se realiza la configuración del Router ISP para establecer una ruta estática, que se encuentre expresamente dirigida de manera interna a Bogotá y Medellín

ISP

```

ISP>en
Password:
ISP#config t
Enter configuration commands, one per line. End with CNTL/Z.
ISP(config)#ip route 172.29.4.0 255.255.255.128 209.17.220.2
ISP(config)#ip route 172.29.0.0 255.255.255.0 209.17.220.6
ISP(config)#end
ISP#cop run st
Destination filename [startup-config]?

```

%SYS-5-CONFIG_I: Configured from console by console

Building configuration...

[OK]

ISP#

Tabla 28 Sumarizacion de redes

Parte 3: Deshabilitar la propagación del protocolo OSPF.

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

A continuación, se realiza el análisis de las interfaces que no requieren propagación del protocolo OSPF, y así mismo, se determinan las interfaces que no necesitan desactivación del protocolo. Mediante este análisis se obtiene la siguiente tabla de propagación de OSPF.

ROUTER	INTERFAZ
Bogota1	Serial 0/0/1; Serial 0/1/0; Serial 0/1/1
Bogota2	Serial 0/0/0; Serial 0/0/1
Bogota3	Serial 0/0/0; Serial 0/0/1; Serial 0/1/0
Medellin1	Serial 0/0/0; Serial 0/0/1; Serial 0/1/1
Medellin2	Serial 0/0/0; Serial 0/0/1
Medellin3	Serial 0/0/0; Serial 0/0/1; Serial 0/1/0
ISP	No lo requiere

Tabla 29 Propagación de OSPF

Conforme el análisis realizado se procede a realizar la configuración detallada de cada una de las interfaces en los routers que no requiere el servicio OSPF.

BOGOTA1 - Serial 0/0/0
<pre>BOGOTA1#config t Enter configuration commands, one per line. End with CNTL/Z. BOGOTA1(config)#router ospf 1 BOGOTA1(config-router)#passive-interface s0/1/1 BOGOTA1(config-router)#end BOGOTA1# BOGOTA1# 00:53:09: %OSPF-5-ADJCHG: Process 1, Nbr 5.5.5.5 on Serial0/1/1 from FULL to DOWN, Neighbor Down: Interface down or detached %SYS-5-CONFIG_I: Configured from console by console BOGOTA1#</pre>

Tabla 30 Propagación de OSPF Bogota1

BOGOTA2 - Serial 0/1/0 – G0/0

```
BOGOTA2>en
Password:
BOGOTA2#config t
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA2(config)#router ospf 1
BOGOTA2(config-router)#passive-interface s0/1/0
BOGOTA2(config-router)#passive-interface g0/0
BOGOTA2(config-router)#end
BOGOTA2#
%SYS-5-CONFIG_I: Configured from console by console

BOGOTA2#
```

Tabla 31 Propagación de OSPF Bogota2

BOGOTA3 - G0/0

```
BOGOTA3#config t
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA3(config)#router ospf 1
BOGOTA3(config-router)#passive-interface g0/0
BOGOTA3(config-router)#end
BOGOTA3#
%SYS-5-CONFIG_I: Configured from console by console

BOGOTA3#
```

Tabla 32 Propagación de OSPF Bogota3

MEDELLIN1 - Serial 0/1/0

```

MEDELLIN1>en
Password:
MEDELLIN1#config t
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN1(config)#router ospf 1
MEDELLIN1(config-router)#passive-interface s0/1/0
MEDELLIN1(config-router)#end
MEDELLIN1#
MEDELLIN1#
01:02:34: %OSPF-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial0/1/0 from FULL to DOWN,
Neighbor Down: Interface down or detached
%SYS-5-CONFIG_I: Configured from console by console
MEDELLIN1#

```

*Tabla 33 Propagación de OSPF Medellin1***MEDELLIN2 - G0/0**

```

MEDELLIN2>en
Password:
MEDELLIN2#config t
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN2(config)#router ospf 1
MEDELLIN2(config-router)#passive-interface g0/0
MEDELLIN2(config-router)#end
MEDELLIN2#
%SYS-5-CONFIG_I: Configured from console by console
MEDELLIN2#

```

Tabla 34 Propagación de OSPF Medellin2

MEDELLIN3 - G0/0

```
MEDELLIN3#config t
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN3(config)#router ospf 1
MEDELLIN3(config-router)#passive-interface g0/0
MEDELLIN3(config-router)#end
MEDELLIN3#
%SYS-5-CONFIG_I: Configured from console by console
MEDELLIN3#
```

Tabla 35 Propagación de OSPF Medellin3

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.

Mediante el siguiente pantallazo se realiza la verificación del protocolo OSPF en los routers Medellín 1 y Bogota 1.

```

Medellin1#
Medellin1#show ip protocols
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 1.1.1.1
  It is an autonomous system boundary router
  Redistributing External Routes from
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 8
  Routing for Networks:
    172.29.8.0 0.0.0.0 area 0
    172.29.8.8 0.0.0.0 area 0
    172.29.8.12 0.0.0.0 area 0
    229.17.120.0 0.0.0.0 area 0
  Passive Interface(s):
    Serial0/1/0
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1          110           00:07:36
    2.2.2.2          110           00:08:43
    3.3.3.3          110           00:08:46
    4.4.4.4          110           00:08:59
    5.5.5.5          110           00:14:57
    6.6.6.6          110           00:09:43
    7.7.7.7          110           00:09:44
  Database: (default is 110)

Medellin1#
Medellin1#

Bogota1#
Bogota1#show ip protocols
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 4.4.4.4
  It is an autonomous system boundary router
  Redistributing External Routes from
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 8
  Routing for Networks:
    172.29.8.0 0.0.0.0 area 0
    172.29.8.8 0.0.0.0 area 0
    172.29.8.12 0.0.0.0 area 0
    229.17.120.0 0.0.0.0 area 0
  Passive Interface(s):
    Serial0/1/1
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1          110           00:07:36
    2.2.2.2          110           00:10:00
    3.3.3.3          110           00:07:38
    4.4.4.4          110           00:17:18
    5.5.5.5          110           00:14:44
    6.6.6.6          110           00:10:00
    7.7.7.7          110           00:10:04
  Database: (default is 110)

Bogota1#
Bogota1#
Bogota1#
Bogota1#
Bogota1#show ip route
172.29.8.0/24 is subnetted, 4 subnets
O    172.29.8.0 [110]
O    172.29.8.8 [110]
O    172.29.8.12 [110]
O    229.17.120.0 [110]

```

Figura 24 Verificación protocolo OSPF MEDELLIN1 – BOGOTA1

Verificación del protocolo OSPF MEDELLIN1 – BOGOTA1

BOGOTA 1

BOGOTA1#show ip protocols

Routing Protocol is "ospf 1"

Outgoing update filter list for all interfaces is not set

Incoming update filter list for all interfaces is not set

Router ID 4.4.4.4

It is an autonomous system boundary router

Redistributing External Routes from,

Number of areas in this router is 1. 1 normal 0 stub 0 nssa

Maximum path: 4

Routing for Networks:

172.29.3.0 0.0.0.3 area 0

172.29.3.4 0.0.0.3 area 0

172.29.3.8 0.0.0.3 area 0

209.17.220.4 0.0.0.3 area 0

Passive Interface(s):

Serial0/1/1

Routing Information Sources:

Gateway Distance Last Update

1.1.1.1 110 00:07:53

2.2.2.2 110 00:10:00

3.3.3.3 110 00:07:15

4.4.4.4 110 00:17:16

5.5.5.5 110 00:16:44

6.6.6.6 110 00:10:00

7.7.7.7 110 00:10:01

Distance: (default is 110)

MEDELLIN1

MEDELLIN1#show ip protocols

Routing Protocol is "ospf 1"

Outgoing update filter list for all interfaces is not set

Incoming update filter list for all interfaces is not set

Router ID 1.1.1.1

It is an autonomous system boundary router

Redistributing External Routes from,

Number of areas in this router is 1. 1 normal 0 stub 0 nssa

Maximum path: 4

Routing for Networks:

172.29.6.0 0.0.0.3 area 0

172.29.6.8 0.0.0.3 area 0

172.29.6.12 0.0.0.3 area 0

209.17.220.0 0.0.0.3 area 0

Passive Interface(s):

Serial0/1/0

Routing Information Sources:

Gateway Distance Last Update

1.1.1.1 110 00:07:36

2.2.2.2 110 00:09:43

3.3.3.3 110 00:06:58

4.4.4.4 110 00:16:59

5.5.5.5 110 00:16:27

6.6.6.6 110 00:09:43

7.7.7.7 110 00:09:44

Distance: (default is 110)

MEDELLIN1#

Tabla 36 Verificación protocolo OSPF MEDELLIN1 – BOGOTA1

Mediante el siguiente pantallazo se realiza la verificación del protocolo OSPF en los routers Medellin 2 y Bogota 2.

The image shows two side-by-side screenshots of the Cisco IOS Command Line Interface (CLI) for routers Medellin 2 and Bogota 2. Both routers have the OSPF protocol configured and are in the process of verifying the configuration.

Router: Medellin 2

```

#configure ip protocols
Routing Protocol is "ospf 1"
  Logging update filter list for all interfaces is not set
  Logging update filter list for all interfaces is not set
  Router ID 2.2.2.2
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.16.4.0 0.0.0.127 area 0
    172.16.4.0 0.0.0.3 area 0
    172.16.4.0 0.0.0.3 area 0
  Neighbor Intervals:
  Neighbor Intervals:
  Routing Information Source:
  Distance: default is 110
  
```

Router: Bogota 2

```

#configure ip protocols
Routing Protocol is "ospf 1"
  Logging update filter list for all interfaces is not set
  Logging update filter list for all interfaces is not set
  Router ID 4.4.4.4
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.16.4.0 0.0.0.254 area 0
    172.16.4.0 0.0.0.3 area 0
    172.16.4.0 0.0.0.3 area 0
    172.16.4.0 0.0.0.3 area 0
  Neighboring Intervals:
  Neighbor Intervals:
  Routing Information Source:
  Distance: default is 110
  
```

Figura 25 Verificación protocolo OSPF MEDELLIN2– BOGOTA2

Verificación protocolo OSPF MEDELLIN2– BOGOTA2

BOGOTA2

BOGOTA2#show ip protocols

Routing Protocol is "ospf 1"

Outgoing update filter list for all interfaces is not set

Incoming update filter list for all interfaces is not set

Router ID 5.5.5.5

Number of areas in this router is 1. 1 normal 0 stub 0 nssa

Maximum path: 4

Routing for Networks:

172.29.0.0 0.0.0.255 area 0

172.29.3.0 0.0.0.3 area 0

172.29.3.4 0.0.0.3 area 0

172.29.3.12 0.0.0.3 area 0

Passive Interface(s):

GigabitEthernet0/0

Serial0/1/0

Routing Information Sources:

Gateway Distance Last Update

1.1.1.1 110 00:12:09

2.2.2.2 110 00:14:17

3.3.3.3 110 00:11:32

4.4.4.4 110 00:21:32

5.5.5.5 110 00:21:00

6.6.6.6 110 00:14:16

7.7.7.7 110 00:14:17

Distance: (default is 110)

BOGOTA2#

MEDELLIN2

```
MEDELLIN2#show ip protocols
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 2.2.2.2
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.29.4.0 0.0.0.127 area 0
    172.29.6.0 0.0.0.3 area 0
    172.29.6.4 0.0.0.3 area 0
  Passive Interface(s):
    GigabitEthernet0/0
  Routing Information Sources:
    Gateway Distance Last Update
    1.1.1.1 110 00:11:51
    2.2.2.2 110 00:13:58
    3.3.3.3 110 00:11:13
    4.4.4.4 110 00:21:14
    5.5.5.5 110 00:20:42
    6.6.6.6 110 00:13:58
    7.7.7.7 110 00:13:59
  Distance: (default is 110)
```

```
MEDELLIN2#
```

Tabla 37 Verificación protocolo OSPF MEDELLIN2– BOGOTA2

Verificación protocolo OSPF MEDELLIN3– BOGOTA3

BOGOTA3

```
Prohibido el acceso - No Autorizado por Diana Hidalgo!!
User Access Verification
Password:
BOGOTA3>en
Password:
BOGOTA3#show ip protocols
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 6.6.6.6
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.29.1.0 0.0.0.255 area 0
    172.29.3.8 0.0.0.3 area 0
    172.29.3.12 0.0.0.3 area 0
  Passive Interface(s):
    GigabitEthernet0/0
  Routing Information Sources:
  Gateway Distance Last Update
    1.1.1.1 110 00:16:07
    2.2.2.2 110 00:18:15
    3.3.3.3 110 00:15:29
    4.4.4.4 110 00:25:30
    5.5.5.5 110 00:24:58
    6.6.6.6 110 00:18:14
    7.7.7.7 110 00:18:15
  Distance: (default is 110)
BOGOTA3#
```

MEDELLIN3

Prohibido el acceso - No Autorizado por Diana Hidalgo!!!

User Access Verification

Password:

MEDELLIN3>en

Password:

MEDELLIN3#show ip protocols

Routing Protocol is "ospf 1"

Outgoing update filter list for all interfaces is not set

Incoming update filter list for all interfaces is not set

Router ID 3.3.3.3

Number of areas in this router is 1. 1 normal 0 stub 0 nssa

Maximum path: 4

Routing for Networks:

172.29.4.128 0.0.0.127 area 0

172.29.6.4 0.0.0.3 area 0

172.29.6.8 0.0.0.3 area 0

172.29.6.12 0.0.0.3 area 0

Passive Interface(s):

GigabitEthernet0/0

Routing Information Sources:

Gateway Distance Last Update

1.1.1.1 110 00:16:20

2.2.2.2 110 00:18:28

3.3.3.3 110 00:15:42

4.4.4.4 110 00:25:43

5.5.5.5 110 00:25:11

6.6.6.6 110 00:18:27

7.7.7.7 110 00:18:28

Distance: (default is 110)

MEDELLIN3#

Tabla 38 Verificación protocolo OSPF MEDELLIN3– BOGOTA3

Mediante el siguiente pantallazo se realiza la verificación del protocolo OSPF en el router ISP.

The screenshot displays a network simulation environment. On the left, a network diagram shows a central cloud labeled 'MEDELLIN 172.28.4.0/24'. Inside the cloud, there are three routers: 'R2011 Router 1' (IP 172.28.4.100), 'R2012 Router 2' (IP 172.28.4.101), and 'R2013 Router 3' (IP 172.28.4.102). Two hosts are connected to Router 1: 'PC-P1 50 HOST' (IP 172.28.4.200) and 'PC-P2 40 HOST' (IP 172.28.4.201). Router 1 is connected to Router 2 (IP 172.28.8.100) and Router 3 (IP 172.28.8.101). Router 2 is connected to Router 3 (IP 172.28.8.100). Router 3 is connected to an external router 'R2014 ISP' (IP 208.17.120.5/30). The right pane shows the OSPF command-line interface output, which includes the following text:

```

Tratando el comando -> Show ip ospf...
Done: Show ip ospf...
Success:
OSPF:
Success:
Showing ip protocols
Showing Protocol in 'Pengé 1'
Checking update filter list for all interfaces is not set
Checking update filter list for all interfaces is not set
Router ID 172.28.4.100
Number of areas in which router is 1. 1 normal 0 stub 0 nssa
Maximum paths: 0
Showing Rtr Neighbors:
208.17.120.5 0.0.0.0 area 0
208.17.120.4 0.0.0.0 area 0
Showing Information Sources:
Source          Distance    Last Update
1.1.1.1         100         00:00:01
2.2.2.2         100         00:00:00
3.3.3.3         100         00:00:00
4.4.4.4         100         00:00:00
5.5.5.5         100         00:00:00
6.6.6.6         100         00:00:00
7.7.7.7         100         00:00:00
Distance: default is 100

```

Figura 27 Verificación protocolo OSPF ISP

Verificación protocolo OSPF ISP

ISP

```
Prohibido el acceso - No Autorizado por Diana Hidalgo!!
User Access Verification
Password:
ISP>en
Password:
ISP#show ip protocols
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 7.7.7.7
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    209.17.220.0 0.0.0.3 area 0
    209.17.220.4 0.0.0.3 area 0
  Routing Information Sources:
  Gateway Distance Last Update
    1.1.1.1 110 00:18:31
    2.2.2.2 110 00:20:38
    3.3.3.3 110 00:17:53
    4.4.4.4 110 00:27:53
    5.5.5.5 110 00:27:21
    6.6.6.6 110 00:20:38
    7.7.7.7 110 00:20:38
  Distance: (default is 110)

ISP#
```

Tabla 39 Verificación protocolo OSPF ISP

Parte 5: Configurar encapsulamiento y autenticación PPP.

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

A continuación, se presenta el código detallado de la configuración del enlace entre el router Medellín 1 con el router ISP, configurado mediante autenticación PAT.

MEDELLIN 1

```
Prohibido el acceso - No Autorizado por Diana Hidalgo!!
User Access Verification
Password:
MEDELLIN1>en
Password:
MEDELLIN1#config t
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN1(config)#int s0/1/1
MEDELLIN1(config-if)#encapsulation ppp
MEDELLIN1(config-if)#exit
MEDELLIN1(config)#username ISP secret cisco
MEDELLIN1(config)#int s0/1/1
MEDELLIN1(config-if)#ppp authentication pap
MEDELLIN1(config-if)#ppp pap sent-username MEDELLIN pass cisco
MEDELLIN1(config-if)#exit
MEDELLIN1(config)#end
MEDELLIN1#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/1, changed state to down
01:31:35: %OSPF-5-ADJCHG: Process 1, Nbr 7.7.7.7 on Serial0/1/1 from FULL to DOWN,
Neighbor Down: Interface down or detached
%SYS-5-CONFIG_I: Configured from console by console
MEDELLIN1#
```

ISP

```
ISP>en
Password:
ISP#
ISP#
ISP#config t
Enter configuration commands, one per line. End with CNTL/Z.
ISP(config)#int s0/0/0
ISP(config-if)#encapsulation ppp
ISP(config-if)#exit
ISP(config)#int s0/0/1
ISP(config-if)#encapsulation ppp
ISP(config-if)#exit
ISP(config)#username MEDELLIN secret cisco
ISP(config)#end
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to down
01:35:39: %OSPF-5-ADJCHG: Process 1, Nbr 4.4.4.4 on Serial0/0/1 from FULL to DOWN,
Neighbor Down: Interface down or detached
ISP#
%SYS-5-CONFIG_I: Configured from console by console
ISP#
```

Tabla 40 Encapsulamiento PPP Medellín1 con ISP.

- b. El enlace Bogotá1 con ISP se debe configurar con autenticación CHAT.

Se presenta a continuación, el código detallado de la configuración del enlace entre el router Bogotá 1 con el router ISP, configurado mediante autenticación CHAT.

BOGOTA1 con ISP

BOGOTA1

```
BOGOTA1>en
Password:
BOGOTA1#config t
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA1(config)#int s0/0/0
BOGOTA1(config-if)#encapsulation ppp
BOGOTA1(config-if)#no shutdown
BOGOTA1(config-if)#exit
BOGOTA1(config)#username ISP secret cisco
BOGOTA1(config)#int s0/0/0
BOGOTA1(config-if)#ppp authentication chap
BOGOTA1(config-if)#exit
BOGOTA1(config)#end
BOGOTA1#
%SYS-5-CONFIG_I: Configured from console by console
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to down
BOGOTA1#
```

ISP

```
ISP#
ISP#config t
Enter configuration commands, one per line. End with CNTL/Z.
ISP(config)#int s0/0/0
ISP(config-if)#ppp pap sent-username ISP pass cisco
ISP(config-if)#exit
ISP(config)#username BOGOTA secret cisco
ISP(config)#int s0/0/1
ISP(config-if)#ppp authentication chap
ISP(config-if)#end
ISP#
%SYS-5-CONFIG_I: Configured from console by console
ISP#
```

Tabla 41 Encapsulamiento Bogotá

Parte 6: Configuración de PAT.

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

Mediante el siguiente código se realiza la configuración del PAT en el Router Medellin 1 y se realiza verificación de configuración mediante la realización de pings a la ips 172.29.6.2 - 172.29.6.10 y 172.29.6.14 los cuales deben ser satisfactorios.

MEDELLIN 1

```

Prohibido el acceso - No Autorizado por Diana Hidalgo!!!
User Access Verification
Password:
MEDELLIN1>en
Password:
MEDELLIN1#config t
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN1(config)#ip acc standard 50host
MEDELLIN1(config-std-nacl)#permit 172.29.4.0 0.0.0.127
MEDELLIN1(config-std-nacl)#exit
MEDELLIN1(config)#ip nat inside sour list 50host inter s0/1/1 overload

```

```

MEDELLIN1(config)#int s0/0/0
MEDELLIN1(config-if)#ip nat inside
MEDELLIN1(config-if)#exit
MEDELLIN1(config)#int s0/0/1
MEDELLIN1(config-if)#ip nat inside
MEDELLIN1(config-if)#int s0/1/0
MEDELLIN1(config-if)#ip nat inside
MEDELLIN1(config-if)#exit
MEDELLIN1(config)#int s0/1/1
MEDELLIN1(config-if)#ip nat outside
MEDELLIN1(config-if)#end
MEDELLIN1#
%SYS-5-CONFIG_I: Configured from console by console
MEDELLIN1#ping 172.29.6.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.6.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/11 ms

MEDELLIN1#ping 172.29.6.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.6.10, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/7 ms

MEDELLIN1#ping 172.29.6.14

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.6.14, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/7 ms

MEDELLIN1#

```

Tabla 42 Configuración de PAT.

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

En el siguiente código se realiza la configuración del NAT en el Router Bogotá 1 y se procede a la verificación de configuración mediante la realización de pings a la ips 172.29.3.2 - 172.29.3.6 y 172.29.3.10, los cuales se evidencia que son satisfactorios.

BOGOTA 1

```
User Access Verification
Password:
BOGOTA1>en
Password:
BOGOTA1#config t
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA1(config)#no ip access-list standard 150host
BOGOTA1(config)#ip access-list standard 150host
BOGOTA1(config-std-nacl)#permit 172.29.0.0 0.0.0.255
BOGOTA1(config-std-nacl)#exit
BOGOTA1(config)#ip nat inside source list 150host interface s0/0/0 overload
BOGOTA1(config)#int s0/0/0
BOGOTA1(config-if)#ip nat outside
BOGOTA1(config-if)#int s0/0/1
BOGOTA1(config-if)#ip nat inside
BOGOTA1(config-if)#int s0/1/0
```

```
BOGOTA1(config-if)#ip nat inside
BOGOTA1(config-if)#int s0/1/1
BOGOTA1(config-if)#ip nat inside
BOGOTA1(config-if)#exit
BOGOTA1(config)#end
BOGOTA1#
%SYS-5-CONFIG_I: Configured from console by console

BOGOTA1#ping 172.29.3.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.3.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms

BOGOTA1#ping 172.29.3.6

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.3.6, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/12 ms

BOGOTA1#ping 172.29.3.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.3.10, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/11 ms

BOGOTA1#
```

Tabla 43 Estadísticas NAT Router Bogota1

Parte 7: Configuración del servicio DHCP.

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

Se procede a realizar la configuración correspondiente en los router Medellin 2 y Medellin 3 para obtener el servicio del servidor DHCP, que en este caso será el router Medellín 2

MEDELLIN2
<pre> MEDELLIN2#config t Enter configuration commands, one per line. End with CNTL/Z. MEDELLIN2(config)#ip dhcp excluded-address 172.29.4.1 172.29.4.9 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)#dns-server 10.10.10.10 MEDELLIN2(dhcp-config)#exit MEDELLIN2(config)#ip dhcp excluded-address 172.29.4.129 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)#dns-server 10.10.10.10 MEDELLIN2(dhcp-config)#exit MEDELLIN2(config)#end MEDELLIN2# %SYS-5-CONFIG_I: Configured from console by console MEDELLIN2# </pre>

Tabla 44 Configuración del servicio DHCP

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

A continuación, se presenta el código de configuración del servicio broadcast en el router Medellín 3 hacia la ip del router Medellín 2.

MEDELLIN3

```
MEDELLIN3>en
Password:
MEDELLIN3#config t
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN3(config)#int g0/0
MEDELLIN3(config-if)#ip helper-address 172.29.6.5
MEDELLIN3(config-if)#exit
MEDELLIN3(config)#end
MEDELLIN3#copy run st
MEDELLIN3#copy run st
Destination filename [startup-config]?
%SYS-5-CONFIG_I: Configured from console by console

Building configuration...
[OK]
MEDELLIN3#
```

Tabla 45 Configuración del servicio broadcast.

En el siguiente pantallazo se evidencia que los dos equipos PC1 y PC2 de la red de Medellin, reciben satisfactoriamente la ip por medio del servidor DHCP configurado.

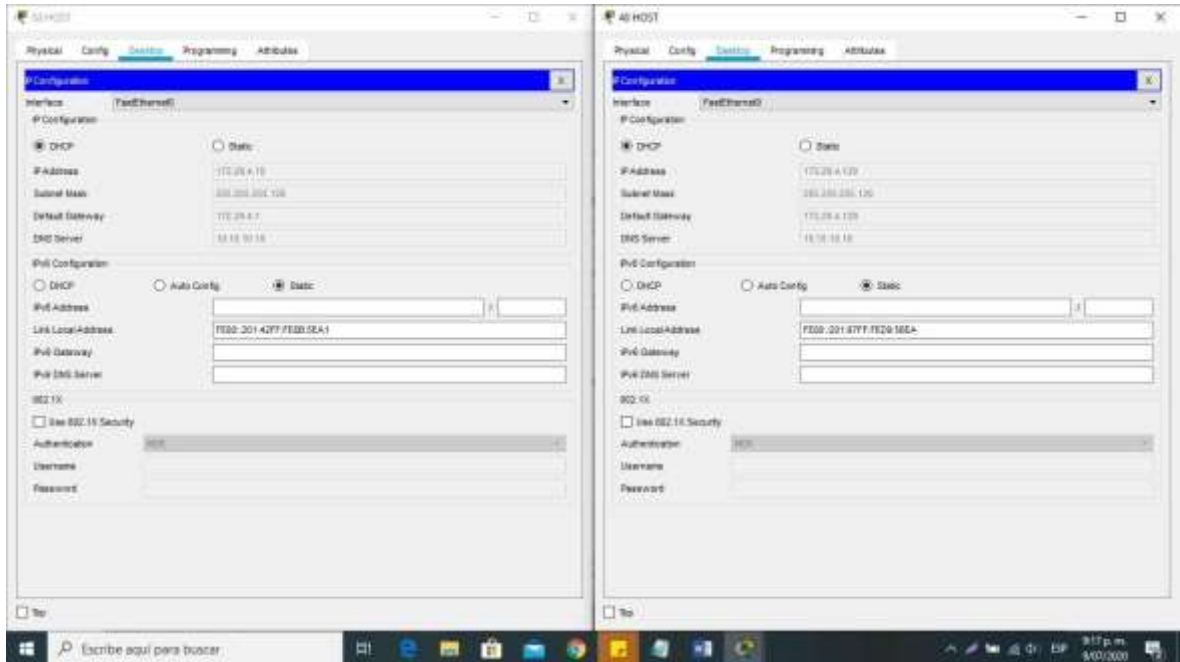


Figura 28 Direccionamiento DHCP PC1 y PC2

Verificación DHCP Red Bogotá2 y Bogotá3

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

Se procede a realizar la configuración correspondiente en los router Bogotá 2 y Bogotá 3, para obtener el servicio del servidor DHCP, que en este caso será el router Bogotá 2

BOGOTA2

```
BOGOTA2#config t
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA2(config)#ip dhcp excluded-address 172.29.0.1 172.29.0.9
BOGOTA2(config)#ip dhcp pool BOGOTA2
BOGOTA2(dhcp-config)#network 172.29.0.0 255.255.255.0
BOGOTA2(dhcp-config)#default-router 172.29.0.1
BOGOTA2(dhcp-config)#dns-server 10.10.10.10
BOGOTA2(dhcp-config)#exit
BOGOTA2(config)#ip dhcp excluded-address 172.29.1.1
BOGOTA2(config)#ip dhcp pool BOGOTA3
BOGOTA2(dhcp-config)#network 172.29.1.0 255.255.255.0
BOGOTA2(dhcp-config)#default-router 172.29.1.1
BOGOTA2(dhcp-config)#dns-server 10.10.10.10 172.29.1.9
BOGOTA2(dhcp-config)#end
BOGOTA2#copy run st
Destination filename [startup-config]?
%SYS-5-CONFIG_I: Configured from console by console

Building configuration...
[OK]
BOGOTA2#
```

Tabla 46 Configuración Bogotá2 y Bogotá3 donde el router Bogotá2 debe ser el servidor DHCP.

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

A continuación, se presenta el código de configuración del servicio broadcast en el router Bogotá 3 hacia la ip del router Bogotá 2.

BOGOTA3
<pre>BOGOTA3>en Password: BOGOTA3#config t Enter configuration commands, one per line. End with CNTL/Z. BOGOTA3(config)#int g0/0 BOGOTA3(config-if)#ip helper-address 172.29.6.13 BOGOTA3(config-if)#exit BOGOTA3(config)#end BOGOTA3#copy run st %SYS-5-CONFIG_I: Configured from console by console Destination filename [startup-config]? Building configuration... [OK] BOGOTA3#</pre>

Tabla 47 Configuración router Bogotá1 mensajes Broadcast

A continuación, se presenta el pantallazo de la topología de red configurada en el programa Packet Tracer, en el cual se evidencian activas todas las interfaces y los equipos que la componen.

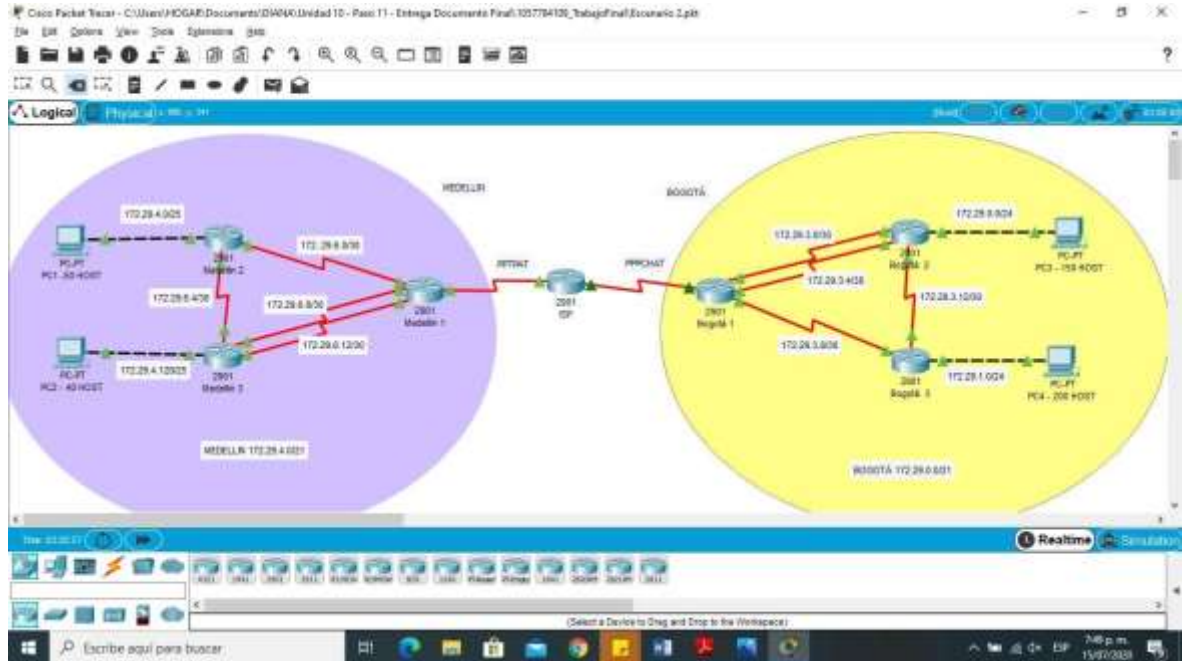


Figura 30 Topología de Red Final

CONCLUSIONES

En la configuración del direccionamiento IP acorde con la topología de red para del escenario dado, se debió tener presentes los elementos idóneos para la representación de la misma, así como el especial cuidado en las asignaciones de las IP's puesto que de allí deriva el éxito o el error al momento de realizar las respectivas pruebas.

Para la configuración del protocolo de enrutamiento del OSPFv2 se debe crear el proceso de OSPF desde la configuración global con el comando "router ospf", después se deben configurar los rangos de red mediante "network área", todas las interfaces que se incluyan mediante ese comando estarán participando en esa área de OSPF.

Cuando se implementa un servidor para la asignación de las direcciones de red es muy eficaz y práctica la asignación de direcciones de red, por esto un servidor DHCP es determinante a la hora de asignar direcciones de red a una gran cantidad de ordenadores obviando asignarlas una por una.

Las NAT son el único mecanismo utilizado para intercomunicar redes de distintas clases, consiste en transportar la información mediante paquetes a través del router sin importar la clase de la misma.

El comando ping es una opción muy frecuente para verificar conexión entre dispositivos para luego resolver problemas con la accesibilidad de dispositivos, además en conjunto con comando traceroute que se usa para realizar el seguimiento que los paquetes toman realmente al desplazarse hacia su destino, se constituyeron en herramientas fundamentales para determinar el éxito de las configuraciones realizadas en la tipología dada.

BIBLIOGRAFIA

CISCO NETWORKING ACADEMY. CCNA Exploration 4.0 - Módulo del curso de profundización CISCO Aspectos básicos del Networking. CISCO. 2013. 426 páginas.

CISCO NETWORKING ACADEMY. CCNA Exploration 4.0 - Guías de prácticas del curso de profundización CISCO Aspectos básicos del Networking. CISCO. 2013.

Cisco Networking Academy, MODULO DE ESTUDIO CCNA1 EXPLORATION (Network Fundamentals). Disponible en:

<http://www.mediafire.com/?9cq9h4jo23c1359>

Cisco Networking Academy, MODULO DE ESTUDIO CCNA2 EXPLORATION (Routing Protocols and Concepts). Disponible en:

<http://www.mediafire.com/?5y052miul2vezhj>

Mario A. Reyes Reynaud, 2011. Calculo de Subredes de Mexico. [Video]

Disponible en:

http://www.youtube.com/watch?v=Z7DM639rAmQ&list=PLaXGHu_K17nuWSyLNRtX7UvR2LcpTBK7P&index=5

ANEXOS

Link archivos Packet Tracer

https://drive.google.com/drive/folders/1dd8HZyj6w2_Qn8Hck5neolr-TIneS_bg?usp=sharing