PRUEBA DE HABILIDADES CCNA 2020

RUBERTH DAGOBERTO PALMA ARIZALA

UNIVERSIDAD NACIONAL Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA
PROGRAMA INGENIERIA DE SISTEMAS
SAN JUAN DE PASTO - NARIÑO
2020

PRUEBA DE HABILIDADES CCNA 2020

RUBERTH DAGOBERTO PALMA ARIZALA

Trabajo de grado para optar por el título de Ingeniero en Sistemas

HECTOR JULIAN PARRA

Tutor

UNIVERSIDAD NACIONAL Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA
PROGRAMA INGENIERIA DE SISTEMAS
SAN JUAN DE PASTO - NARIÑO
2020

Nota de Aceptación

_____

_____

_____

_____
Presidente del Jurado

_____
Jurado

_____
Jurado

San Juan de Pasto 26, 05, 2020

Dedicatoria:

A mi madre, esposa e hijo quienes fueron mi inspiración y fuente de apoyo en todo mi proceso de formación profesional.

AGRADECIMIENTOS

Agradezco a Dios por darme la salud, capacidad intelectual y física de afrontar mis estudios, llenando mi vida de bendiciones y poniendo en mis manos todas las herramientas para culminar esta etapa de formación profesional.

A mi madre, mi esposa y mi hijo por brindarme el espacio de sus vidas y entregar su energía emocional para impulsar mis sueños.

TABLA DE CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

CISCO SYSTEMS: es una empresa global principalmente dedicada a la fabricación, venta, mantenimiento y consultoría de equipos de telecomunicaciones.

TOPOLOGIA: es la rama de las matemáticas dedicada al estudio de aquellas propiedades de los cuerpos geométricos que permanecen inalteradas por transformaciones continuas. Es una disciplina que estudia las propiedades de los espacios topológicos y las funciones continuas.

NETWORKING: es una estrategia que consiste en ampliar nuestra red de contactos profesionales con el empleo de redes sociales de tipo profesional, haciendo que el Networking sea una estrategia muy usada por empresas, por ejemplo: en Linkedin las empresas buscan nuevas alianzas estratégicas o profesionales.

ENRUTAMIENTO: o ruteo es la función de buscar un camino entre todos los posibles en una red de paquetes cuyas topologías poseen una gran conectividad.

IPv4: Es un sistema direccional de 32 bits usado para identificar un dispositivo en una red. Es el sistema direccional usado en la mayoría de las redes informáticas, incluyendo Internet.

IPv6: Es un sistema direccional del 128-bit usado para identificar un dispositivo en una red. Es el sucesor al IPv4 y a la mayoría de la versión reciente del sistema direccional usado en las redes informáticas. El IPv6 se está desarrollando actualmente en todo el mundo. Un direccionamiento del IPv6 se representa en ocho campos de los números hexadecimales, cada campo que contiene 16 bits. Un direccionamiento del IPv6 se divide en dos porciones, cada parte integrada por 64 bits. La primera parte que es la dirección de red, y la segunda parte la dirección de host.

Conectividad: es la capacidad de un dispositivo de conectarse con otro dispositivo de una forma autónoma.
Dirección IP: es un direccionamiento utilizado para identificar un dispositivo en la red.

DNS: (sistema de nombres de dominio) es la nomenclatura utilizada para asociar información de dominio y la dirección IP de cada uno de los dispositivos que conforman o acceden a una red.
DHCP: (Protocolo de configuración dinámica de host) de tipo cliente/servidor en el que un servidor cuenta con un listado de direcciones IP dinámicas y las asigna a los clientes en el momento en el que se encuentran disponibles.

Encapsulamiento: es el proceso en el que los datos que se encuentran dispuestos para ser enviados a través de una red se ubican en paquetes con la capacidad de ser administrados y rastreados por el administrador de la red.

NAT. protocolo con el cual se intercambian o transportan paquetes entre dos redes normalmente incompatibles.

OSPF: protocolo de enrutamiento desarrollado para redes IP, de tipo enlace-estado.

Ping: comando utilizado para realizar un diagnóstico de estado de comunicación entre dos o más equipos en el cual se puede determinar la velocidad, calidad y estado de red.

Protocolos de enrutamiento: conjunto de reglas que permiten determinar la mejor ruta para enviar paquetes de datos entre routers.

Puertos troncales: enlace punto a punto para enviar y recibir el tráfico entre routers o switches.

RESUMEN

Con el presente trabajo se busca que los estudiantes profundicemos en el campo de las Redes y las Telecomunicaciones de tal forma que estemos en capacidad de responder a la demanda creciente de personal especializado en el área de las Tecnologías de la Información, acompañado de un alto componente práctico, mediante el uso de herramientas de simulación por medio del software Packet Tracer y laboratorios remotos.

PALABRAS CLAVE: “Redes, Telecomunicaciones, Packet Tracer, simulación, laboratorios”.

1. INTRODUCCIÓN

Por medio del presente trabajo, se abordarán las diferentes temáticas relacionadas con el proceso de aprendizaje realizado durante el desarrollo del Diplomado de Profundización CCNA, específicamente en la implementación de dos escenarios propuestos en los cuales se realizará la configuración de cada uno de los dispositivos que comprende el diseño físico, la ejecución de los diferentes comandos de programación para la verificación de su conectividad.

Se pretende dar a conocer los contenidos aprendidos durante el diplomado, mediante el cual se aplicará enrutamiento, parámetros de seguridad y acceso en distintos dispositivos en la red, sin pasar por alto las configuraciones OSPF, RIP, NAT, verificación de ACL. las cuales se implementan en routers para mayor seguridad de una red o aplicar políticas de entrada y salida de paquetes para equipos específicos.

Así mismo se realiza la configuración de servidores DHCP, siendo este un protocolo de difusión que funciona de manera predeterminada en donde sus paquetes no cruzan por medio de enrutadores. La función de un agente de retransmisión DHCP es recibir cualquier difusión DHCP de la subred y la reenviar a la dirección IP determinada en una subred diferente.

La implementación de este escenario se realizará por medio de la simulación en el software Packet Tracer. El cual nos permite experimentar con la topología física y analizar el comportamiento de toda la red del escenario propuesto.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Dar solución al escenario propuesto como trabajo final del diplomado de profundización CCNA, desarrollando cada uno de los conocimientos adquiridos sobre la implementación y diseño de la topología física y lógica de una red.

2.2 OBJETIVOS ESPECÍFICOS

- Emplear comandos de configuración avanzada en routers, implementando RIP, OSPF y enrutamiento estático; bajo un esquema de direccionamiento IP sin clase, para dar soluciones de red y conectividad escalables, mediante el uso de los principios de enrutamiento y conmutación de paquetes en ambientes LAN y WAN.

- Utilizar herramientas de simulación y laboratorios de acceso remoto con el fin de establecer escenarios LAN/WAN que permitan realizar un análisis sobre el comportamiento de diversos protocolos y métricas de enrutamiento, evaluando el comportamiento de enrutadores, a través de comandos de administración de tablas de enrutamiento, bajo el uso de protocolos de vector distancia y estado enlace.

3. PLANTEAMIENTO DEL PROBLEMA

3.1 DEFINICIÓN DEL PROBLEMA

El presente trabajo articula en su contenido diversas temáticas que permiten abordar el núcleo problémico: Gestión de Sistemas y Servicios de Telecomunicaciones. Las telecomunicaciones como herramienta para la competitividad global con visión socio humanística, en donde hay un aprendizaje mediante la creación de una red empresarial eficaz y escalable; así como a través de instalar, configurar, supervisar, y solucionar problemas en los equipos pertenecientes a la infraestructura de una red convergente.

3.2 JUSTIFICACIÓN

Es importante estar en la capacidad de solucionar problemas responder a la demanda creciente de personal especializado en el área de las Tecnologías de la Información, acompañado de un alto componente práctico, mediante el uso de herramientas de simulación Packet Tracer y laboratorios remotos.

Para este fin contamos con herramientas de gran experiencia efectiva como la configuración de sistemas operativos de red, protocolos de comunicación, mecanismos de acceso al medio y características de la capa de red, la capa de transporte, asignación de direcciones IP, subnetting y capa de aplicación.

Además, analizamos la forma adecuada de diseñar y configurar soluciones soportadas en el uso de dispositivos de conmutación acorde con las topologías de red requeridas bajo el uso de protocolos basados en STP y VLANs bajo una arquitectura jerárquica.

Por otra parte, contamos con la orientación para utilizar el enrutamiento estático, enrutamiento dinámico, enrutamiento mediante protocolos de estado enlace, listas de acceso, asignación dinámica de direcciones IP y traducciones de direcciones IP mediante NAT.

4. DESARROLLO DE LOS ESCENARIOS

4.1 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

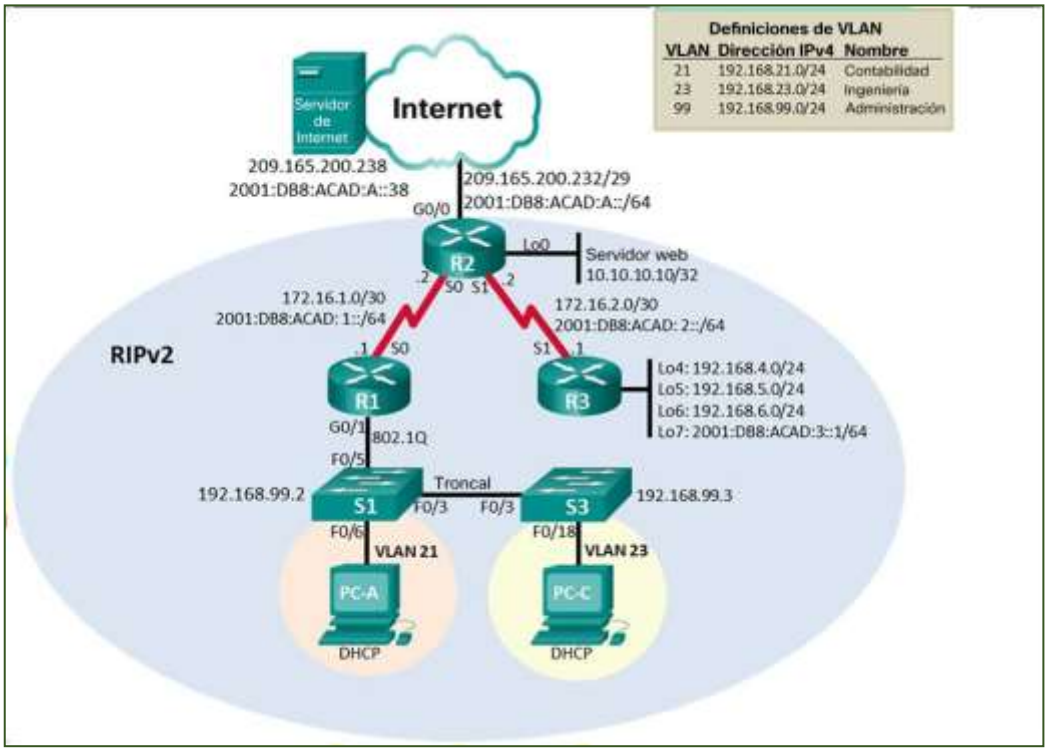


Figura 1 Escenario 1

4.1.1 Inicializar dispositivo

Inicializar y volver a cargar los routers y los switches

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

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

Tabla 1 configuración básica del software del routers y switches

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	Introducimos el siguiente código 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	Para borrar introducimos este código 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	Utilizamos el siguiente código Show vlan brief

4.1.2 Configurar los parámetros básicos de los dispositivos

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):

Tabla 2 Configuración del servidor de internet según la topología

Elemento o tarea de configuración	Especificación
Dirección IPv4	Se ingresa al server en la pestaña desktop y ubicamos la ip configuración buscamos la pestaña o casilla de IPV4 Introducimos la ruta 209.165.200.230
Máscara de subred para IPv4	Se ingresa al server en la pestaña desktop y ubicamos la ip configuración buscamos la pestaña o casilla de subred Mask Introducimos la ruta 255.255.255.248
Gateway predeterminado	Se ingresa al server en la pestaña desktop y ubicamos la ip configuración buscamos la pestaña o casilla Default Gateway Introducimos la ruta 209.165.200.225
Dirección IPv6/subred	Se ingresa al server en la pestaña desktop y ubicamos la ip configuración buscamos la pestaña o casilla IPV6 Address Introducimos la ruta 2001:DB8:ACAD:A::92
Gateway predeterminado IPv6	Se ingresa al server en la pestaña desktop y ubicamos la ip configuración buscamos la pestaña o casilla Gateway de IPV6 Introducimos la ruta 2001:DB8:ACAD:2::1

Nota: Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente en partes posteriores de esta práctica de laboratorio.

4.1.3 Configurar básicas R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 3 Configuración del Router 1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Se ingresa el código: No ip domain-lookup
Nombre del router	Se ingresa el código: hostname R1
Contraseña de exec privilegiado cifrada	Se ingresa el código: enable secret Class
Contraseña de acceso a la consola	Se ingresa el código: line con 0 password Cisco
Contraseña de acceso Telnet	Se ingresa el código: line vty 0 4
Cifrar las contraseñas de texto no cifrado	Se ingresa el código: service password-encryption
Mensaje MOTD	Se ingresa el código: banner motd ¡Se 21rohíbe el acceso no autorizado!
Interfaz S0/0/0	Establezca la descripción se hace con este código: interface serial 0/0/0 description 1 Establecer la dirección Ipv4 Consultar el diagrama de topología para conocer la información de direcciones es: 172.16.1.0/30
Rutas predeterminadas	Establecer la dirección Ipv6 Consultar el diagrama de topología para conocer la información de direcciones es:

	2001:DB8:ACAD:1::/64 Establecer la frecuencia de reloj en 128000 Activar la interfaz int s0/0/0 clock rate 128000 Configurar una ruta Ipv4 predeterminada de S0/0/0 El código es interface serial 0/0/0 ip address 172.16.1.2 255.255.255.0 Configurar una ruta Ipv6 predeterminada de S0/0/0 interface Serial0/0/0 ipv6 address 2001:DB8:ACAD:1::1/64

4.1.4 Configurar básicas R2

La configuración del R2 incluye las siguientes tareas:

Tabla 4 Configuración del R2

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Se ingresa el código: no ip domain-lookup
Nombre del router	Se ingresa el código: hostname R2
Contraseña de exec privilegiado cifrada	Se ingresa el código: enable secret Class
Contraseña de acceso a la consola	Se ingresa el código: line con 0 password Cisco
Contraseña de acceso Telnet	Se ingresa el código: line vty 0 4 password Cisco

Cifrar las contraseñas de texto no cifrado	Se ingresa el código: service password-encryption
Habilitar el servidor HTTP	Dado que no se puede utilizar los comandos ip http server se emplea un servidor dentro de la topología ip nat inside source static 10.10.10.10 209.165.200.229 int f0/0 ip nat outside int f0/1 ip nat inside
Mensaje MOTD	Se ingresa el código: banner motd! ¡Se prohíbe el acceso no autorizado!
Interfaz S0/0/0	Establezca la descripción interface serial 0/0/0 description R2 a R1 Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. ip address 172.16.1.2 255.255.255.0 Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz int s0/0/0 ipv6 address 2001:DB8:ACAD:2::/64
Interfaz S0/0/1	Establecer la descripción Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. int s0/0/1 ip address 172.16.2.1 255.255.255.0 Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. ipv6 address 2001:DB8:ACAD:3::/64

	Establecer la frecuencia de reloj en 128000. clock rate 128000 Activar la interfaz
Interfaz G0/0 (simulación de Internet)	Establecer la descripción.
Interfaz loopback 0 (servidor web simulado)	Establecer la descripción. Establezca la dirección IPv4. Entramos al desktop y seleccionamos ip Configuración y escribimos en las casillas Ip address 10.10.10.10
Ruta predeterminada	Configure una ruta IPv4 predeterminada de G0/0. ip address 172.16.1.3 255.255.255.0 Configure una ruta IPv6 predeterminada de G0/0. ipv6 address 2001:DB8:ACAD:A: :/64

4.1.5 Configurar R3

La configuración del R3 incluye las siguientes tareas:

Tabla 5 Configuración del R3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Se ingresa el código: no ip domain-look
Nombre del router	Se ingresa el código: hostname R3
Contraseña de exec	Se ingresa el código:

privilegiado cifrada	line con 0
Contraseña de acceso a la consola	Se ingresa el código: line con 0 password Cisco
Contraseña de acceso Telnet	Se ingresa el código: line vty 0 password Cisco
Cifrar las contraseñas de texto no cifrado	Se ingresa el código: service password-encryption
Mensaje MOTD	Se ingresa el código: banner motd !Se prohíbe el acceso no autorizado!
Interfaz S0/0/0 Interfaz S0/0/1	Establecer la descripción interface serial 0/0/0 description 1 Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. 172.16.2.0/30 Se utilize int s0/0/1 ip address 172.16.2.6 255.255.255.252 Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. 2001:DB8:ACAD:2::/64 Se utilize ipv6 address 2001:DB8:ACAD:2::/64 Activar la interfaz
Interfaz loopback 4	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. int lo4 ip address 192.168.4.2 255.255.255.0
Interfaz loopback 5	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. int lo5

	ip address 192.168.5.2 255.255.255.0
Interfaz loopback 6	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. int lo6 ip address 192.168.6.2 255.255.255.0
Interfaz loopback 7	Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. int lo7 ipv6 address 2001:DB8:ACAD:3::1/64

4.1.6 Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 6 Switches 1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Se ingresa el Código: no ip domain-look
Nombre del switch	Se ingresa el Código: hostname S1
Contraseña de exec privilegiado cifrada	Se ingresa el código: enable secret Class
Contraseña de acceso a la consola	Se ingresa el código: line con 0 password Cisco
Contraseña de acceso Telnet	Se ingresa el código: line vty 0 4 password Cisco
Cifrar las contraseñas de texto no cifrado	Se ingresa el código: service password-encryption

Mensaje MOTD	Se ingresa el código: banner motd #Se prohíbe el acceso no autorizado#

4.1.7 Configurar S3

La configuración del S3 incluye las siguientes tareas:

Tabla 7 Switches 3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Se ingresa el Código: no ip domain-lookup
Nombre del switch	Se ingresa el código: hostname S3
Contraseña de exec privilegiado cifrada	Se ingresa el código: enable secret Class
Contraseña de acceso a la consola	Se ingresa el código: line con 0 password Cisco
Contraseña de acceso Telnet	Se ingresa el código: line vty 0 4 password Cisco
Cifrar las contraseñas de texto no cifrado	Se ingresa el código: service password-encryption
Mensaje MOTD	Se ingresa el código: banner motd #Se prohíbe el acceso no autorizado#

4.1.7 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:

Tabla 8 Verificando la red

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.1	Si
R2	R3, S0/0/1	172.16.2.2	Si
PC de Internet	Gateway predeterminado	209.165.200.229	Si

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

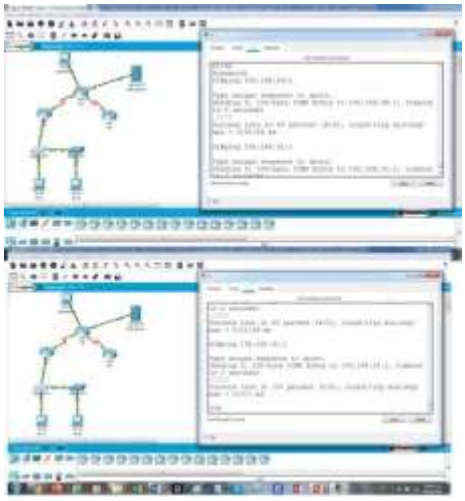


Figura 2 Verificaciones de ping en los R1 a R2

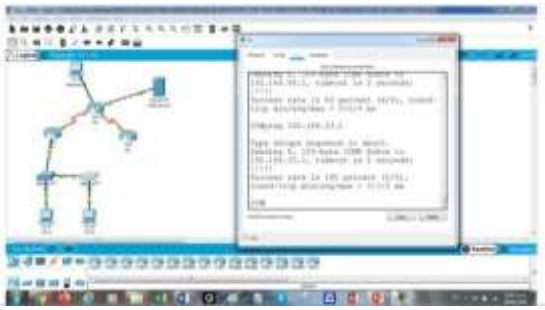


Figura 3 Verficaciones de Ping R2 a R3

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

4.1.8 Configurar S1 de la seguridad en VLAN

La configuración del S1 incluye las siguientes tareas:

Tabla 9 Seguridad del switches uno de VLAN

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para topología para crear y nombrar cada una de las VLAN que se indican vlan 21 name Contabilidad vlan 23 name Ingeniería vlan 99 name Administracion
Asignar la dirección IP de administración.	Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S1 en el diagrama de topología Ingresamos el siguiente código int vlan 99 ip address 192.168.99.1 255.255.255.0 int vlan 21 p address 192.168.21.1 255.255.255.0 int vlan 23 ip address 192.168.23.1 255.255.255.0
Asignar el gateway predeterminado	Asigne la primera dirección IPv4 de la subred como el gateway predeterminado. Escribimos el siguiente código: ip default-Gateway 192.168.199.3

Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa int f0/3 switchport mode trunk switchport trunk native vlan 1
Forzar el enlace troncal en la interfaz F0/5	Utilizar la red VLAN 1 como VLAN nativa utilizamos el siguiente código: int f0/5 switchport mode trunk switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range int range f0/2, f0/4, f0/6-23 switch mode access int f0/1
Asignar F0/6 a la VLAN 21	Utilizamos los siguientes códigos interface f0/6 switchport mode access switchport access vlan 21
Apagar todos los puertos sin usar	Ingresamos el siguiente código: interface range f0/1-24

4.1.9 Configurar S3 de la seguridad en VLAN

La configuración del S3 incluye las siguientes tareas:

Tabla 10 de seguridad del switches tres de VLAN

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para topología para crear cada una de las VLAN que se indican Dé nombre a cada VLAN. vlan 21 name Contabilidad vlan 23

	name Ingeniería vlan 99 name Administracion Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S3 en el diagrama de topología int vlan 99 ip address 192.168.99.2 255.255.255.0
Asignar la dirección IP de administración	int vlan 21 ip address 192.168.21.2 255.255.255.0 int vlan 23 ip address 192.168.23.2 255.255.255.0
Asignar el gateway predeterminado.	Asignar la primera dirección IP en la subred como gateway predeterminado. ip default-gateway 192.168.199.2
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa int f0/3 switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range int range fa0/1-2, fa0/4-24 switchport mode access
Asignar F0/18 a la VLAN 21	Ingresamos el siguiente código: int f0/18 switchport mode access switchport access vlan 21
Apagar todos los puertos sin usar	Ingresamos el siguiente código: int range f0/1-2, f0/4-17, f0/19-24

4.2.0 Configurar las subinterfaces en R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 11 Configuración del Router de la subinterfaz

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	Descripción: LAN de Contabilidad Asignar la VLAN 21 Hacemos el siguiente código: int g0/1.1 description LAN de Contabilidad encapsulation dot1Q 21 Asignar la primera dirección disponible a esta encapsulation dot1Q 21 ip address 192.168.21.4 255.255.255.0 interfaz
Configurar la subinterfaz 802.1Q .23 en G0/1	Descripción: LAN de Ingeniería Introducimos el siguiente código int g0/1.2 Asignar la primera dirección disponible a esta interfaz encapsulation dot1Q 23 ip address 192.168.23.4 255.255.255.0
Configurar la subinterfaz 802.1Q .99 en G0/1	Descripción: LAN de Administración Asignar la VLAN 99 int g0/1.3 description LAN de Administracion encapsulation dot1Q 99 Asignar la primera dirección disponible a esta interfaz ip address 192.168.99.4 255.255.255.0
Activar la interfaz G0/1	No shutdown

4.2.1 Verificar la conectividad de la red VLAN

- 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:

Tabla 12 Verificación de la conectividad de la red

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.2	si
S3	R1, dirección VLAN 99	192.168.99.2	Si
S1	R1, dirección VLAN 21	192.168.21.1	si
S3	R1, dirección VLAN 23	192.168.23.2	si

```
S1#ping 192.168.99.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/3/9 ms

S1#
```

Figura 4 Verificación de conectividad en S1 a R1 Packet Tracer

```
S3#ping 192.168.99.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.2, timeout is 2 seconds:
..!!!
Success rate is 60 percent (3/5), round-trip min/avg/max = 0/0/0 ms
```

Figura 5 Verificación de Conectividad en S3 a R1 Packet Tracer

4.2.2 Configurar el protocolo de routing dinámico RIPv2

Configurar RIPv2 en el R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 13 Configurar el protocolo de routing uno, dinámico RIPv2

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	Ejecutamos el siguiente código: router ospf 1
Anunciar las redes conectadas directamente	Asigne todas las redes conectadas directamente. router-id 2.2.2.2 network 192.168.21.0 0.0.0.255 area 0 network 192.168.23.0 0.0.0.255 area 0 network 192.168.99.0 0.0.0.255 area 0
Establecer todas las interfaces LAN como pasivas	Ponemos el código: passive-interface g0/1.1 passive-interface g0/1
Desactive la sumarización automática	Ponemos el código: router rip no auto-summary

4.2.3 Configurar RIPv2 en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla 14 Configurar el protocolo de routing dos, dinámico RIPv2

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	router ospf 1
Anunciar las redes conectadas directamente	Nota: Omitir la red G0/0.
Establecer la interfaz LAN (loopback) como pasiva	router ospf 2 router-id 2.2.2.2 network 172.16.1.0 0.0.0.3 area 0 network 172.16.2.0 0.0.0.3 area 0 network 10.10.10.10 0.0.0.255 area 0 passive-in passive-interface g0/1
Desactive la sumarización automática.	no auto-summary

4.2.4 Configurar RIPv3 en el R2

La configuración del R3 incluye las siguientes tareas:

Tabla 15 Configuración del protocolo de routing tres, dinámico RIPv2

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	router ospf 1
Anunciar redes IPv4 conectadas directamente	network 172.16.3.0 0.0.0.3 area 0

Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	network 192.168.4.0 0.0.3.255 area 0 passive-interface lo4 passive-interface lo5 passive-interface lo6 passive-interface lo7
Desactive la sumarización automática.	no auto-summary

4.2.5 Verificar la información de RIP

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

Tabla 16 Verificación la información de RIP

Pregunta	Respuesta
¿Con qué comando se muestran la ID del proceso RIP, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router?	show ip ospf neig
¿Qué comando muestra solo las rutas RIP?	show ip ospf interface
¿Qué comando muestra la sección de RIP de la configuración en ejecución?	Show ip protocols

4.2.6 Implementar DHCP y NAT para IPv4

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

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 17 Implementar DHCP y NAT para IPv4 en el R1

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	ip dhcp excluded-address 192.168.21.1 192.168.21.20
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	ip dhcp excluded-address 192.168.23.1 192.168.23.20
Crear un pool de DHCP para la VLAN 21.	Nombre: ACCT Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado Introducimos el siguiente código ip dhcp pool ACCT dns-server 10.10.10.10 ip domain-name ccna.com ip dhcp pool ACCT default-router 192.168.21.1 network 192.168.21.0 255.255.255.0

Crear un pool de DHCP para la VLAN 23	Nombre: ENGNR Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado ip dhcp pool ENGNR dns-server 10.10.10.10 default-router 192.168.23.1 network 192.168.23.0 255.255.255.0 ip domain-name ccna.com

4.2.7 Configurar la NAT estática y dinámica en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla 18 Configurar la NAT estática y dinámica en el R2

Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	Nombre de usuario: webuser Contraseña: cisco12345 Nivel de privilegio: 15 user webuser privilege 15 secret Cisco
Habilitar el servicio del servidor HTTP	No soporta el código HTTP
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	access-list 1 permit 192.168.21.0 0.0.0.255 access-list 1 permit 192.168.23.0 0.0.0.255 access-list 1 permit 192.168.99.0 0.0.0.255
Crear una NAT estática al servidor web.	Dirección global interna: 209.165.200.229

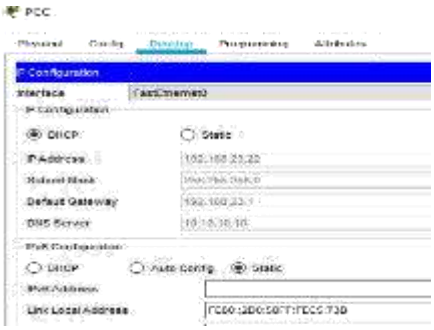
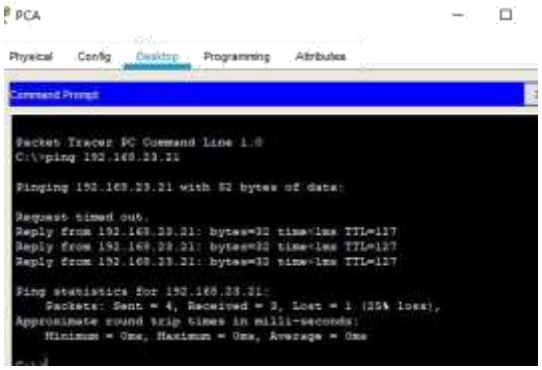
Asignar la interfaz interna y externa para la NAT estática	ip nat inside source static 10.10.10.10 209.165.200.229
Configurar la NAT dinámica dentro de una ACL privada	Lista de acceso: 1 Permitir la traducción de las redes de Contabilidad y de Ingeniería en el R1 Permitir la traducción de un resumen de las redes LAN (loopback) en el R3
Defina el pool de direcciones IP públicas utilizables.	Nombre del conjunto: INTERNET El conjunto de direcciones incluye: 209.165.200.225 – 209.165.200.228
Definir la traducción de NAT dinámica	ip nat pool Internet 209.165.200.229 209.165.200.228 netmask 255.255.255.248

4.2.8 Verificar el protocolo DHCP y la NAT estática

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

Tabla 19 Verificar el protocolo DHCP y la NAT estática

Prueba	Resultados
Verificar que la PC-A haya adquirido información d IP del servidor DHCP	 **Figura 6 Verificación de la PC-A información de IP del servidor de DHCP**

Verificar que la PC-A pueda hacer ping a la PC-C Quizá sea necesario deshabilitar el firewall de la PC	 **Figura 7 Verificación de la PC-C información de IP del servidor de DHCP** Hacen ping del PC-A al PC-C  **Figura 8 Verificación que la PC-A pueda hacer**
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	user webuser privilege 15 secret cisco12345  **Figura 9 Iniciación de sesión de servidor web**

4.2.9 Configurar NTP

Tabla 20 Configuración NTP

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	clock set 09:00:00 may 05 2016
Configure R2 como un maestro NTP.	Nivel de estrato: 5
Configurar R1 como un cliente NTP.	Servidor: R2
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	ntp server 209.165.200.229
Verifique la configuración de NTP en R1.	show ntp associations

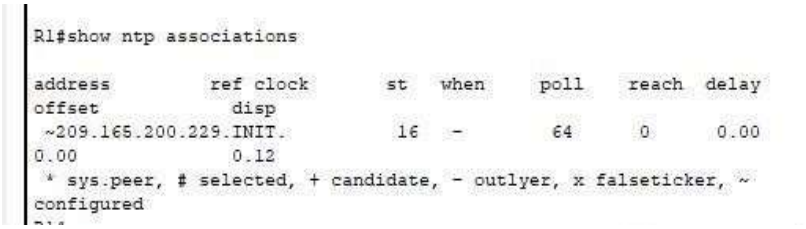


Figura 10 Verifique la configuración de NTP en R1

4.3.0 Configurar y verificar las listas de control de acceso (ACL)

Restringir el acceso a las líneas VTY en el R2

Tabla 21 Configuración y verificación las listas de control de acceso (ACL)

Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	Nombre de la ACL: ADMIN-MGT
Aplicar la ACL con nombre a las líneas VTY	permit host 172.16.1.1
Permitir acceso por Telnet a las líneas de VTY	access-class ADMIN-MGT in
Verificar que la ACL funcione como se espera	show access-lists

```
R2#
R2# show access-lists
Standard IP access list 1
    10 permit 192.168.21.0 0.0.0.255
    20 permit 192.168.23.0 0.0.0.255
    30 permit 192.168.99.0 0.0.0.255
Standard IP access list ADMIN-MGT
    10 permit host 172.16.1.1
Extended IP access list 100
    10 permit tcp any host 209.165.200.229 eq www
    20 permit icmp any any echo-reply

R2#
```

Figura 11 Verificar que la ACL funcione como se espera

4.3.1 Ingresar comandos de CLI

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

Tabla 22 Comando de CLI

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	show access-list
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	ip access-list standard 2 18 permit 172.22.1.1
¿Con qué comando se muestran las traducciones NAT?	Nota: Las traducciones para la PC-A y la PC-C se agregaron a la tabla cuando la computadora de Internet intentó hacer ping a esos equipos en el paso 2. Si hace ping a la computadora de Internet desde la PC-A o la PC-C, no se agregarán las traducciones a la tabla
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	debido al modo de simulación de Internet en la red. clear ip nat translation *

5. ESCENARIO 2

Una empresa posee sucursales distribuidas en las ciudades de Bogotá y Medellín, en donde el estudiante será el administrador de la red, el cual deberá configurar e interconectar entre sí cada uno de los dispositivos que forman parte del escenario, acorde con los lineamientos establecidos para el direccionamiento IP, protocolos de enrutamiento y demás aspectos que forman parte de la topología de red.

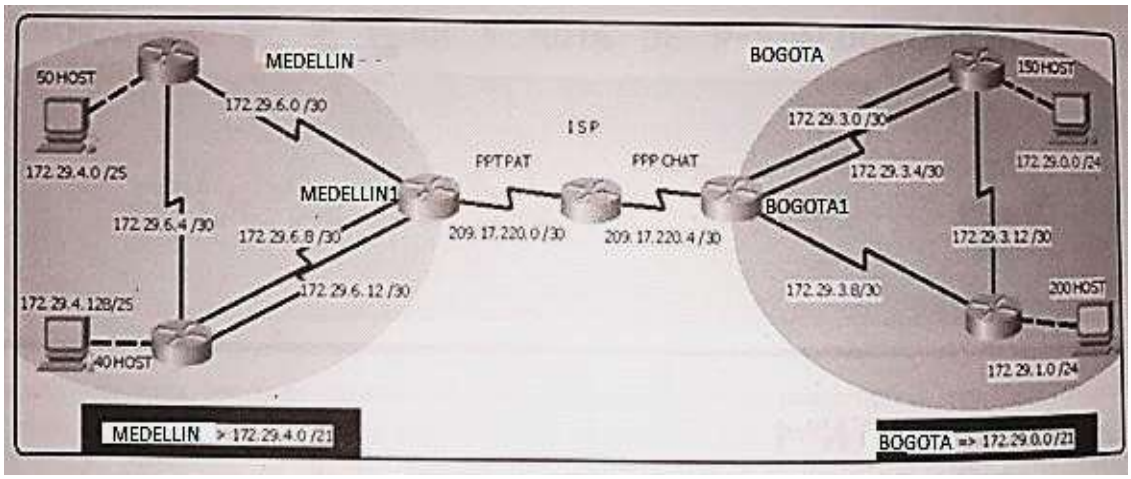


Figura 12 Topología de red escenario 1 propuesto

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.

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.

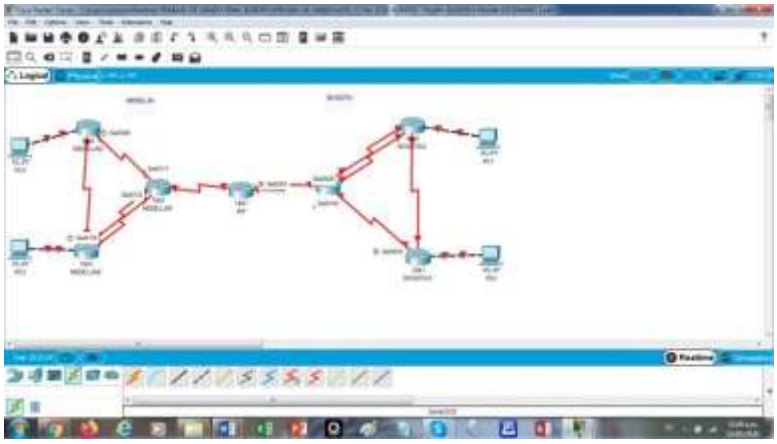


Figura 13 Topología del Escenario 2 desarrollado

5.1 CONFIGURACION DE LOS ROUTER EN GENERAL

Enter configuration commands, one per line. End with
CNTL/Z.

5.1.1 Parte 1: Configuración del enrutamiento

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

• Los routers Bogota1 y 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.

• 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.

5.1.2 Configuración del Router de la ISP con los siguientes comandos

Router(config)#hostname ISP

ISP(config)#INT S0/0
ISP(config)#INT S0/0/0
ISP(config-if)#Description ISP A MEDELLIN

ISP(config-if)#IP ADD 209.17.220.1 255.255.255.252

ISP(config-if)#CLOCK RATE 128000
ISP(config)#INT S0/0/1

ISP(config-if)#Description ISP A BOGOTA
ISP(config-if)#IP ADD 209.17.220.5 255.255.255.252

ISP(config-if)#CLOCK RATE 128000

ISP(config)#Router Rip
ISP(config-router)#VERSION 2

ISP(config-router)#NEtwork 209.17.220.0
ISP(config-router)#NO AUTo-summary

ISP#COPY Running-config STartup-config

Destination filename [startup-config]?
Building configuration...

[OK]

5.1.3 Configuración del Route de MEDELLIN con las rutas

```
Router(config)#Hostname MEDELLIN
MEDELLIN(config)#INT S0/0/0

MEDELLIN(config-if)#DEScription MEDELLIN A ISP

MEDELLIN(config-if)#IP ADDRESS 209.17.220.2 255.255.255.252

MEDELLIN(config-if)#CLOCK RATE 128000
MEDELLIN(config-if)# Shutdown

MEDELLIN(config)#INT S0/1/1

MEDELLIN(config-if)#DESCRIPTION MEDELLIN A MEDELLIN1
MEDELLIN(config-if)#IP ADDRESS 172.29.6.13 255.255.255.252

MEDELLIN(config-if)#CLOCK RATE 128000

MEDELLIN(config-if)#INT S0/1/0
MEDELLIN(config-if)#Description MEDELLIN1 A MEDELLIN
MEDELLIN(config-if)#IP ADDRESS 172.29.6.9 255.255.255.252
MEDELLIN(config-if)#CLOCK RATE 128000
MEDELLIN(config-if)#EXIT

MEDELLIN(config)#INT S0/0/1

MEDELLIN(config-if)#Description MEDELLIN A MEDELLIN2
MEDELLIN(config-if)#IP ADDRESS 172.29.6.1 255.255.255.252

MEDELLIN(config-if)#CLOCK RATE 128000
MEDELLIN(config-if)#EXIT

MEDELLIN(config)#ROUTER Rip
MEDELLIN(config-router)#VERSION 2

MEDELLIN(config-router)#Network 172.29.0.0
```

MEDELLIN(config-router)#NO Auto-summary

MEDELLIN(config)#EXIT
MEDELLIN#COPY Running-config STartup-config

5.1.4 Configuración del ROUTER Y LE PONEMOS MEDELLIN2

Router(config)#HOSTNAME MEDELLIN_2

MEDELLIN_2(config)#Interface S0/0/0

MEDELLIN_2(config-if)#Description MEDELLIN2 A Medellin
MEDELLIN_2(config-if)#IP ADDRESS 172.29.6.2 255.255.255.252

MEDELLIN_2(config-if)#CLOCK RATE 128000
MEDELLIN_2(config-if)#EXI

MEDELLIN_2(config)#INT S0/0/1

MEDELLIN_2(config-if)#DESCRIPTION MEDELLIN2 A MEDELLIN1
MEDELLIN_2(config-if)#IP ADDRESS 172.29.6.5 255.255.255.252

MEDELLIN_2(config-if)#CLOCK RATE 128000
MEDELLIN_2(config-if)#EXI

MEDELLIN_2(config)#INT G0/0

MEDELLIN_2(config-if)#DESCRIPTION MEDELLIN2 A PC2
MEDELLIN_2(config-if)#IP ADDRESS 172.29.4.1 255.255.255.128

MEDELLIN_2(config-if)#CLOCK RATE 128000
MEDELLIN_2(config-if)#EXI

MEDELLIN_2(config)#ROUTE RIP
MEDELLIN_2(config-router)#ROUTE RIP
MEDELLIN_2(config-router)#VERSION 2

MEDELLIN_2(config-router)#Network 172.29.0.0
MEDELLIN_2(config-router)#NO AUTO-SUMMARY

5.1.5 Configuración del ROUTER y le ponemos MEDELLIN1

Router(config)#Hostname MEDELLEN1

MEDELLEN1(config)#INT S0/0/0
MEDELLEN1(config-if)#DESCRIPTION MEDELLIN1_A_MEDELLIN

MEDELLEN1(config-if)#IP ADDRESS 172.29.6.14 255.255.255.252
MEDELLEN1(config-if)#CLOCK RATE 18000
MEDELLEN1(config-if)#EXIT

MEDELLEN1(config)#INT S0/0/1

MEDELLEN1(config-if)#DESCription MEDELLIN A MEDELLIN1
MEDELLEN1(config-if)#IP ADDRESS 172.29.6.10 255.255.255.252

MEDELLEN1(config-if)#CLOCK RATE 128000

MEDELLEN1(config-if)#INT S0/1/0
MEDELLEN1(config-if)#DESCRIPTION MEDELLIN1 A MEDELLIN2
MEDELLEN1(config-if)#CLOKRATE 128000

MEDELLEN1(config-if)#INT G0/0
MEDELLEN1(config-if) #Description MEDELLIN1 A PC3

MEDELLEN1(config-if)#IP ADDRESS 172.29.4.2 255.255.255.252
MEDELLEN1(config-if)#CLOCK RATE 128000

MEDELLEN1(config-if)#ROTER RIP
MEDELLEN1(config-if)#EXI

MEDELLEN1(config)#ROUTER RIP
MEDELLEN1(config-router)#VERSION 2

MEDELLEN1(config-router)#Network 172.29.0.0
MEDELLEN1(config-router)#NO Auto-summary

5.1.6 Configuración del Route con el nombre de BOGOTA

BOGOTA(config)#Interface Serial 0/0/0
BOGOTA(config-if)#Description BOGOTA A ISP
BOGOTA(config-if)#IP ADDRESS 209.17.220.6 255.255.255.252
BOGOTA(config-if)#CLOCK RATE 128000
BOGOTA(config-if)#Shutdown
BOGOTA(config)#Interface Serial 0/0/1
BOGOTA(config-if)#DESCRIPtion BOGOTA A BOGOTA2
BOGOTA(config-if)#IP ADDRESS 172.29.31.1 255.255.255.252
BOGOTA(config-if)#CLOCK RATE 128000

BOGOTA(config)#Interface Serial 0/1/0
BOGOTA(config-if)#DESCIPTION BOGOTA2 A BOGOTA
BOGOTA(config-if)#Description BOGOTA2 A BOGOTA
BOGOTA(config-if)#IP ADDRESS 172.29.3.5 255.255.255.252
BOGOTA(config-if)#CLOCK RATE 128000

BOGOTA(config)#Interface Serial 0/1/1 BOGOTA(config-
if)#DESCription BOGOTA A BOGOTA1
BOGOTA(config-if)#IP ADDRESS 172.29.3.9 255.255.255.252
BOGOTA(config-if)#CLOCK RATE 128000

BOGOTA(config-if)#ROUTE RIP
BOGOTA(config-router)#ROUTE RIP
BOGOTA(config-router)#VERSION 2
BOGOTA(config-router)#Network 172.29.0.0
BOGOTA(config-router)#NO Auto-summary

BOGOTA#COPY Running-config STartup-config
Destination filename [startup-config]?

Building configuration...
[OK]

5.1.7 configuración del Route y le ponemos el nombre BOGOTA2

Router(config)#Hostname BOGOTA_2

BOGOTA_2(config)#INTerface S0/0/0
BOGOTA_2(config-if)#DESCRIPTION BOGOTA_2 A BOGOTA

BOGOTA_2(config-if)#IP ADDRRES 172.29.3.2 255.255.255.252
BOGOTA_2(config-if)#IP ADDRESS 172.29.3.2 255.255.255.252

BOGOTA_2(config-if)#CLOCK RATE 128000
BOGOTA_2(config-if)#EXI

BOGOTA_2(config)#INTerface S0/0/1

BOGOTA_2(config-if)#DESCRIPTION BOGOTA A BOGOTA2
BOGOTA_2(config-if)#IP ADDRESS 172.29.3.6 255.255.255.252

BOGOTA_2(config-if)#CLOCK RATE 128000
BOGOTA_2(config-if)#EXI

BOGOTA_2(config)#INTerface S0/1/1

BOGOTA_2(config-if)#DESCRIPTION BOGOTA2 A BOGOTA1
BOGOTA_2(config-if)#IP ADDRESS 172.29.3.13 255.255.255.252

BOGOTA_2(config-if)#CLOCK RATE 128000

BOGOTA_2(config-if)#INT G0/0
BOGOTA_2(config-if)#description BOGOTA A PCC

BOGOTA_2(config-if)#IP ADDRESS 172.29.0.1 255.255.255.0
BOGOTA_2(config-if)#CLOCK RATE 128000

BOGOTA_2(config-if)#EXI
BOGOTA_2(config)#ROUTER RIP

BOGOTA_2(config-router)#VERSION 2
BOGOTA_2(config-router)#Network
172.29.0.0 BOGOTA_2(config-router)#NO
Auto-summary

5.1.8 Configuración del Route y le ponemos el nombre de BOGOTA_1

Router(config)#

Router(config)#INT
Router(config)#INTerface S0/0/0

Router(config-if)#DESCRIPTION BOGOTA1 A BOGOTA1
Router(config-if)#IP ADDRESS 172.29.3.10 255.255.255.252

Router(config-if)#CLOCK RATE 128000

Router(config-if)#Interface S0/0/1 Router(config-
if)#DESCRIPTION BOGOTA1 A BOGOTA2
Router(config-if)#IP ADDRESS 172.29.3.14
255.255.255.252 Router(config-if)#CLOCK RATE 128000
Router(config-if) #EXI

Router(config)#INT G0/0
Router(config-if)#description BOGOTA1 A PCA

Router(config-if)#IP ADDRESS 172.29.1.1 255.255.255.0
Router(config-if)#CLOCK RATE 128000

Router(config-if)#EXI

Router(config)#ROUTER RIP
Router(config-router)#VERSION 2

Router(config-router)#Network 172.29.0.0
Router(config-router)#NO auto-summary
Router(config-router)#exit

Router#copy running-config startup-config
Destination filename [startup-config]?

Building configuration...
[OK]

Router(config)#hostname bogota_1

d. 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.

Respuesta:

ISP(config)#IP ROUTE 172.29.4.0 255.255.252.0 172.29.0.0

ISP(config)#IP ROUTE 172.29.0.0 255.255.252.0 172.29.0.0
ISP(config)#IP ROUTE 172.29.4.128 255.255.252.128 172.29.0.0

5.1.9 CONFIGURAMOS EL ROUTER DE ISP A MEDELLIN

MEDELLIN(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.1

5.2.0 CONFIGURAMOS EL ROUTER DE ISP A BOGOTA

BOGOTA(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.5

5.2.1 Parte 2: Tabla de Enrutamiento.

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

Ingresamos el comando en CLI en el router:

Show ip route

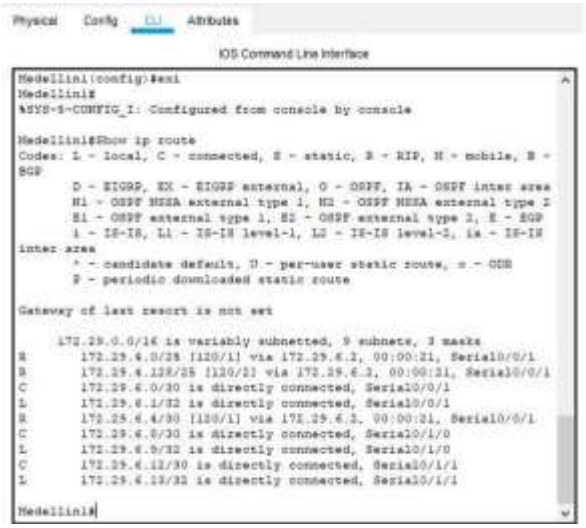


Figura 14 Enrutamiento

5.2.2 Verificar el balanceo de carga que presentan los routers.

Se utiliza el código sh ip route en los router de Medellín y Bogotá

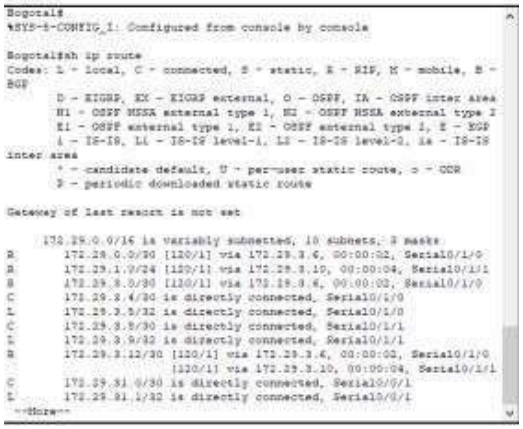


Figura 15 Código sh ip route en Bogotá

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

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

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

• El router ISP solo debe indicar sus rutas estáticas adicionales a las directamente conectadas.

5.2.3 Parte 3: Deshabilitar la propagación del protocolo OSPF.

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

Se configura las tablas con las rutas que no están en uso

Tabla 23 Des habilitación de la propagación del protocolo OSPF

ROUTER	INTERFAZ
Bogotá	G0/0 G0/1
Bogota_1	SERIAL0/0/0 SERIAL0/1/1 G0/0 G0/1
Bogota_2	G0/0 G0/1

Medellín	G0/0 G0/1
Medellín_1	SERIAL0/0/0; SERIAL0/0/1
Medellín_2	G0/1
ISP	No lo requiere

Se hace en cada route MEDELLIN

MEDELLIN(config)#router rip
MEDELLIN(config-router)#version 2
MEDELLIN(config-router)#passive-interface
g0/1 MEDELLIN(config-router)#exit

MEDELLIN(config)#router rip
MEDELLIN(config-router)#router rip
MEDELLIN(config-router)#version 2
MEDELLIN(config-router)#passive-interface
g0/0 MEDELLIN(config-router)#exi

5.2.4 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. Utilizamos el comando show ip protocols como se puede visualizar en la gráfica 18

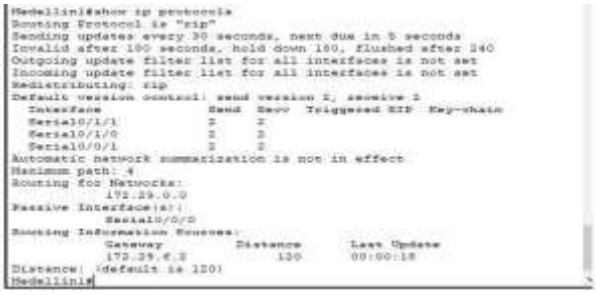


Figura 16 Verificación del protocolo OSPF en MEDELLIN

• 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.

Utilizamos el código en el comando del router en BOGOTA1

do show ip route connected

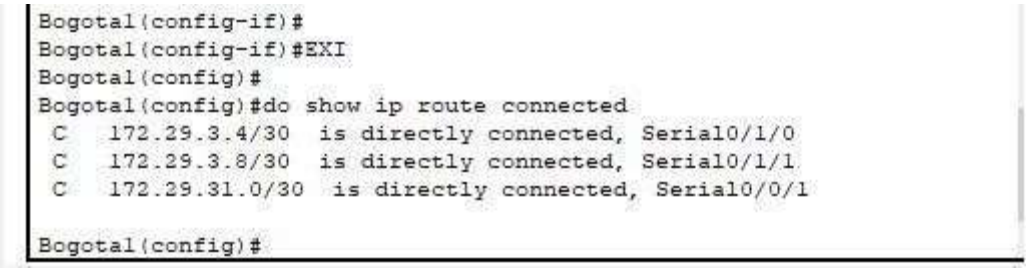


Figura 17 Verificar de OSPF del router BOGOTA1

5.2.5 Parte 5: Configurar encapsulamiento y autenticación PPP.

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

• El enlace Bogotá1 con ISP se debe configurar con autenticación CHAT.

Hacemos una secuencia para encapsular la información y poder conectar los res route Medellin y Bogota, Isp

Medellin

MEDELLIN(config)#int s0/0/0
MEDELLIN(config-if)#encapsulation ppp

Bogota
BOGOTA(config)#int s0/0/0
BOGOTA(config-if)#encapsulation ppp

ISP(config)#int s0/0/0

ISP(config-if)#encapsulation ppp

ISP(config-if)#int s0/0/1

ISP(config-if)#encapsulation ppp

se configurar con autenticación CHAT, en los router de ISP Y MEDELLIN

ISP(config)#username MEDELLIN secret
MEDELLIN1 ISP(config)#INT S0/0/0

ISP(config-if)#PPP AUTHENTICATION PAP
ISP(config-if)#PPP PAP SENT-USERNAME ISP PASSWORD
ISP

CONFIGURAMOS EL ROUTE MEDELLIN

MEDELLIN(config)#USERNAME ISP SECRET ISP
MEDELLIN(config)#INT S0/0/0

MEDELLIN(config-if)#PPP AUTHENTICATION PAP
MEDELLIN (config-if)#PPP PAP SENT-USERNAME MEDELLEN PASSWORD

MEDELLIN(config-if)#

A hora configuramos la ISP hacia Bogota

ISP(config)#username BOGOTA SECRET BOGOTA

ISP(config)#INT S0/0/1
ISP(config-if)#PPP AUTHENTICATION CHAP

Se configura de Bogota a Isp

BOGOTA(config)#username ISP SECRET
BOGOTA BOGOTA(config)#INT S0/0/0

BOGOTA(config-if)#PPP AUTHENTICATION
CHAP BOGOTA(config-if)#EXI

VERIFICAMOS CON PING LOS ROUTE

HACEMOS PING en los router de Medellin hacia ISP y Bogotá hacia ISP con él por la ruta 209.17.220.1

5.2.6 Parte 6: Configuración de PAT.

• En la topología, si se activa NAT en cada equipo de salida (Bogotá1 y Medellín1), los routers internos de una ciudad no podrán llegar hasta los routers internos en el otro extremo, sólo existirá comunicación hasta los routers Bogotá1, ISP y Medellín1.

• Después de verificar lo indicado en el paso anterior proceda a configurar el NAT en el router Medellín1. Compruebe que la traducción de direcciones indique las interfaces de entrada y de salida. Al realizar una prueba de ping, la dirección debe ser traducida automáticamente a la dirección de la interfaz serial 0/1/0 del router Medellín1, cómo diferente puerto.

• 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.

5.2.7 Configuramos la NAT en cada equipo en route de Medellín

MEDELLIN(config)#ip access-list Standard host
MEDELLIN(config-std-nacl)#permit 172.29.4.0
0.0.0.225 MEDELLIN(config-std-nacl)#exit

```
MEDELLIN(config)#ip nat inside source list host interface
s0/0/0
MEDELLIN(config)#int s0/0/0
MEDELLIN(config-if)#ip nat outside

MEDELLIN(config-if)#exit
MEDELLIN(config)#int s0/1/1

MEDELLIN(config-if)#ip nat outside
MEDELLIN(config-if)#exit

MEDELLIN(config)#int s0/1/0
MEDELLIN(config-if)#ip nat outside

MEDELLIN(config-if)#exit
MEDELLIN(config)#int s0/0/1

MEDELLIN(config-if)#ip nat outside
MEDELLIN(config-if)#exit
```

5.2.8 Parte 7: Configuración del servicio DHCP.

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

- El router Medellín2 deberá habilitar el paso de los mensajes broadcast hacia la IP del router Medellín1.

```
MEDELLIN_2(config)#ip dhcp excluded-address 172.29.4.129 172.29.4.132
MEDELLIN_2(config)#ip dhcp pool MEDELLIN_2
MEDELLIN_2(dhcp-config)#network 172.29.4.0 255.255.255.128
MEDELLIN_2(dhcp-config)#default-server 172.29.4.2

MEDELLIN_2(dhcp-config)#default-route 172.29.4.2
MEDELLIN_2(dhcp-config)#dns-server 2.2.2.2

MEDELLIN_2(dhcp-config)#exit
```

MEDELLIN_2(config)#dhcp pool M

MEDELLIN_2(config)#IP dhcp pool MEDELLIN1

MEDELLIN_2(dhcp-config)#NETWORK 172.29.4.128
255.255.255.128 MEDELLIN_2(dhcp-config)#DEFAUL-ROUTER
172.29.4.129 MEDELLIN_2(dhcp-config)#DEFAULT-ROUTER
172.29.4.129 MEDELLIN_2(dhcp-config)#DNS-SERVER 2.2.2.2
MEDELLIN_2(dhcp-config)#EXI

5.2.9 Configuración el route de Medellin_1, sobre le protocolo DHCP

MEDELLEN1(config)#INT G0/0
MEDELLEN1(config-if)#IP HELPER-ADDRES
172.29.6.5 MEDELLEN1(config-if)#EXI

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

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

5.3.0 En pesamos a configurar el DHCP en los route Bogota 1 y 2

BOGOTA_2(config)#ip dhcp excluded-address 172.29.0.1 172.29.0.4

BOGOTA_2(config)#ip dhcp pool BOGOTA_2
BOGOTA_2(dhcp-config)#network 172.29.1.0 255.255.255.0

BOGOTA_2(dhcp-config)#default-router 172.29.1.1
BOGOTA_2(dhcp-config)#dns-server 2.2.2.2

BOGOTA_2(config)#ip dhcp pool BOGOTA1
BOGOTA_2(dhcp-config)#Network 172.29.0.0 255.255.255.0

BOGOTA_2(dhcp-config)#DEFAULT-ROUTER 172.29.0.1

BOGOTA_2(dhcp-config)#dns-server 2.2.2.2
bogota_1(config)#INT G0/0

bogota_1(config-if)#IP HELPER-ADDRES
172.29.3.13
bogota_1(config-if)#EXI

Figura 18 DHCP en la PC0 de Medellin2

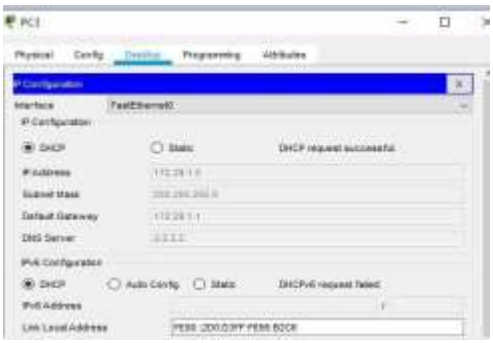


Figura 19 DHCP en la PC3 de Bogota2

CONCLUSIONES

Con la búsqueda del desarrollo de esta actividad de habilidades practica se realizaron diferentes tareas las cuales jugaron un papel importante para llegar a la solución de los ejercicios propuestos, mediante estos se ejecutaron funciones de verificación de una conexión entre los dispositivos dispuestos en la configuración inicial de la topología, se configura la ACL de los Routers, cuyo fin es mitigar los ataques de manera remota, además de la verificación de la funcionalidad de las actividades ejecutadas anteriormente (ACL) cuya función es permitir el acceso de direcciones IP específicas, dando seguridad de que únicamente el administrador del computador tenga permiso para acceder al router mediante telnet o SSH.

En el segundo escenario nos apoyamos en los conocimientos del primer escenario teniendo en cuenta que en el ejercicio vimos solo router y pc, y configuramos los router principales con características distintas y lo di vimos entre zonas.

En el trascurso de todas las actividades en la plataforma cisco, se logró realizar de manera gradual los procedimientos básicos para configuración de una red básica como compleja, donde se logra identificar, analizar y configurar dispositivos de red según las necesidades requeridas, durante todo el desarrollo de la asignatura se logra comprender la importancia que debe tener todo equipo de red a la hora de asignar las direcciones IP, hasta implementar protocolos de seguridad en las diferentes capaz y otros apartados más permitiendo una red confiable y robusta.

Durante todo el aprendizaje como estudiante de carrera profesional en sistemas, el Curso de CISCO ha aportado a mis conocimientos en gran medida, gracias a eso mi perfil se vuelve más competente en el ámbito laboral y personal, gracias a que el conocimiento adquirido me abre mas puertas de trabajo para alcanzar mis objetivos y metas.

BIBLIOGRAFÍA

- CISCO. (2017). Acceso a la red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#4.0.1.1

- CISCO. (2017). Capa de red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#6.0.1.1

- CISCO. (2017). Ethernet. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#5.0.1.1

- CISCO. (2017). Exploración de la red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module1/index.html#1.0.1.1

- CISCO. (2017). Protocolos y comunicaciones de red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#3.0.1.1

- UNAD (2017). Diseño y configuración de redes con Packet Tracer [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgCT9VCtl_pLtPD9

- Vesga, J. (2019). Introducción al Laboratorio Remoto SmartLab [OVI]. Recuperado de http://hdl.handle.net/10596/24167