PRUEBA DE HABILIDADES PRÁCTICAS CCNA

VICTOR ADOLFO PALACIO BASTIDAS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍAS E INGENIERÍAS
INGENIERÍA ELECTRÓNICA
MEDELLIN, ANTIOQUIA
2020

PRUEBA DE HABILIDADES PRÁCTICAS CCNA

VICTOR ADOLFO PALACIO BASTIDAS

Trabajo de la opción de grado para optar al título de Ingeniero Electrónico

ASESOR
NILSON ALBEIRO FERREIRA MANZANARES
Docente Ocasional

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERIA
INGENIERÍA ELECTRÓNICA
MEDELLÍN, ANTIOQUIA
2020

CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

RESUMEN

En un mundo donde el desarrollo está marcado por el avance de la tecnología y la forma en como esta nos ayuda a comunicarnos para apoyar el continuo avance de la sociedad, cada vez es más importante contar con los recursos que nos ofrecen las redes y como estas se ajustan a las necesidades particulares de cada organización.

En el presente trabajo escrito se desarrollan dos escenarios que muestran los requerimientos más comunes de una red, entre ellos la disponibilidad, seguridad, servicios de red y autenticación entre otros, según los perfiles de los grupos de redes internas en cada escenario. Para aplicar en lo anterior los conceptos aprendidos de *switching and routing* y todo lo que implica su correspondiente implementación en cada topología según las necesidades particulares para cada aplicación.

PALABRAS CLAVE: Enrutamiento dinámico, topología, listas de acceso, servidor, cliente, encapsulamiento, IP.

ABSTRACT

In a world where development is marked by the advancement of technology and how it helps us communicate to support the continued advancement of society, it is increasingly important to have the resources that networks offer us and how are you they are adjusted to the particular needs of each organization.

In this written work, two scenarios are developed that show the most common requirements of a network, among them availability, security, network services and authentication, among others, according to the profiles of the groups of internal networks in each case. To carry out the above, the concepts learned from switching and routing and everything that implies their corresponding implementation in each topology according to the particular needs of each application.

GLOSARIO

CLIENTE: Es una entidad o dispositivo que realiza peticiones al servidor sobre servicios que este le puede otorgar, dependiendo de la configuración y del tipo de servicio establecido.

COMANDOS: Es una orden que tiene cierta sintaxis o regla y puede lograr modificar, ajustar o determinar el comportamiento del equipo, dispositivo o programa que lo reciba.

INTERFAZ: Es un componente que permite la interconexión física y lógica entre dos dispositivos y posibilita la comunicación entre ellos.

PROTOCOLO: Es un conjunto de reglas que deben seguir y aplicar las entidades que se desean comunicar para lograr el entendimiento entre ambas.

ROUTER: Es un dispositivo que se encarga de enrutar paquetes entre diferentes redes eligiendo la mejor ruta disponible.

TOPOLOGÍA: Es el mapa de la red que permite identificar los dispositivos, interfaces, ubicación y otros, dependiendo del ámbito físico ó lógico en el que se especifique.

SERVIDOR: Es una aplicación capaz de proporcionar servicios a los clientes para lo cual está configurado o programado.

SWITCH: Es un dispositivo que permite la conexión de redes.

1. INTRODUCCIÓN

En este documento se presenta el desarrollo de dos escenarios que permiten demostrar las habilidades obtenidas del curso realizado en Cisco ccna. El desarrollo de cada caso de estudio demuestra la aplicación de conceptos, técnicas y servicios aprendidos durante el desarrollo del diplomado de profundización, inicialmente en cada escenario se describen los requerimientos que deben cumplir basado en una aplicación deseada de red y posteriormente se muestra el desarrollo metódico de cada necesidad mostrando el procedimiento ejecutado para la configuración y pruebas de evaluación o verificación.

En el desarrollo de cada escenario se evidencia la aplicación de muchos de los conceptos aprendidos, como seguridad, confiabilidad, integridad y disponibilidad entre otros, permitiendo evidenciar la importancia de la aplicación y pertinencia de los diferentes protocolos de enrutamiento, servidores, listas de acceso, traductores de direcciones de red y procedimientos de seguridad y autenticación.
.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Aplicar los conceptos y habilidades aprendidos durante el Desarrollo del curso para resolver las necesidades de cada escenario y lograr que se cumpla con los requerimientos solicitados implementando para ello los protocolos de enrutamiento y configuración de dispositivos para lograr la comunicación.

2.2 OBJETIVOS ESPECÍFICOS

Configurar los dispositivos de cada red de manera que permitan la implementación de seguridad, autenticación, documentación de los enlaces y el establecimiento de advertencia a usuarios no autorizados.

Realizar el modelado de la red conforme a las necesidades expuestas en cada escenario asegurando la conexión de dispositivos y verificando el enlace entre ellos.

Implementar los protocolos de enrutamiento dinámico y estático solicitados en la versión requerida según las necesidades de cada escenario, y verificar utilizando los procedimientos, pruebas y tablas de enrutamiento.

Determinar y aplicar los procedimientos necesarios para la implementación de los servicios de red requeridos por cada escenario.

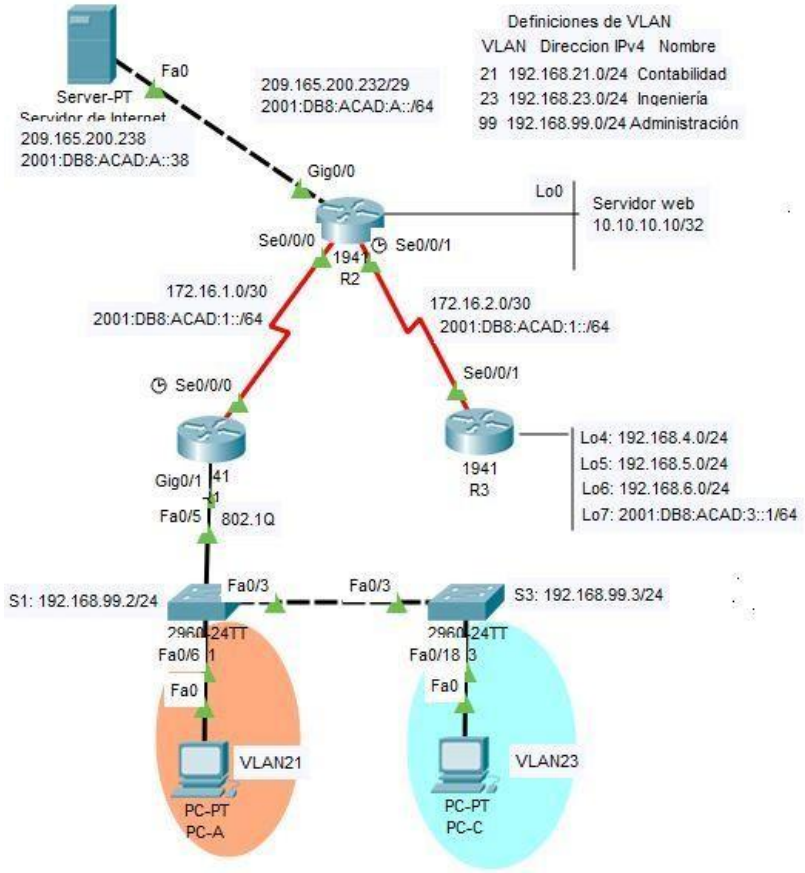
3. ESCENARIO 1

3.1 DESCRIPCIÓN DEL ESCENARIO 1

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

3.2 TOPOLOGÍA

Figura 1. Topología implementada en el escenario 1.



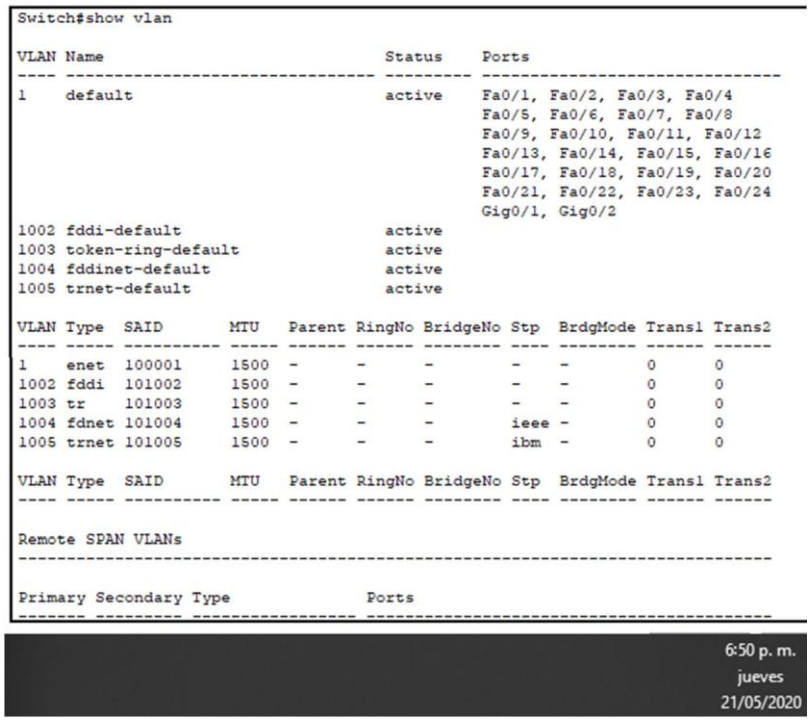
3.3 ICIALIZAR DISPOSITIVOS

La configuración inicial de dispositivos, principalmente routers y switches se realiza primero limpiando la configuración inicial en cada uno de los dispositivos que participan en la topología, para esto se ejecutan comandos que borran cualquier configuración que hubiera en memoria dejando cada dispositivo con los parámetros de fábrica, posteriormente se verifica que la información de configuración de VLANs en los switches esté con los parámetros de fabrica por medio de comandos de monitoreo como comandos *show*.

3.3.1 INICIALIZAR Y VOLVER A CARGAR LOS ROUTERS Y LOS SWITCHES

Tabla 1. Procedimiento para inicializar los dispositivos.

Tarea	**Comando de IOS**
Eliminar el archivo startup-config de todos los routers	La secuencia de comandos para eliminar las configuraciones iniciales es: Router>enable Router#erase startup-config Erasing the nvram filesystem will remove all configuration files! Continue? [confirm] [OK] Erase of nvram: complete
Volver a cargar todos los routers	Los comandos para volver a cargar los routers: Router#reload Proceed with reload? [confirm]
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	La secuencia de comandos para eliminar las configuraciones iniciales es: Switch#erase startup-config Erasing the nvram filesystem will remove all configuration files! Continue? [confirm] [OK] Erase of nvram: complete
Volver a cargar	La secuencia de comandos para Volver a cargar ambos

ambos switches	switches son: Switch#reload Proceed with reload? [confirm]
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	La siguiente secuencia de comandos sirve para verificar que la base de datos de las VLAN está asignada de fábrica: Figura 2. Resultado del comando show vlan. 

```
Switch#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gig0/1, Gig0/2
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------

Remote SPAN VLANs
------------------------------------------------------------------------------

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
```

3.4 CONFIGURAR LOS PARÁMETROS BÁSICOS DE LOS DISPOSITIVOS

En esta etapa se configura cada dispositivo que participa en la topología del escenario 1, para el dispositivo de Internet se configura los parámetros de dirección IPv4 e IPv6, la puerta de enlace predeterminada, la máscara y se aclara la asignación de dirección IPv6 comparada con la que se indica en la topología. La configuración de los routers incluye la asignación IPv4 e IPv6 para cada una de las interfaces que están conectadas, se configura el nombre, las claves de acceso de consola, líneas administrativas y de usuario privilegiado, todo este proceso se realiza siguiendo la secuencia de comandos indicada en cada tabla que se presenta a continuación.

3.4.1 CONFIGURAR LA COMPUTADORA DE INTERNET

Tabla 2. Configuración de la computadora de Internet

Elemento 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	En este caso la dirección indicada 2001:DB8:ACAD:2::1 está en una subnet diferente a la indicada en la topología /64, por tanto se configura con lo indicado en la topología la dirección IPv6 debería ser: 2001:DB8:ACAD:A::1

3.4.2 CONFIGURAR ROUTER 1

Tabla 3. Configuración del router 1.

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	R1>enable R1# configure terminal R1(config)#no ip domain-lookup
Nombre del router	Router>enable Router# configure terminal Router(config)#hostname R1
Contraseña de exec privilegiado cifrada	R1>enable R1# configure terminal R1(config)# enable secret class R1(config)# service password-encryption
Contraseña de acceso a la consola	R1>enable R1# configure terminal R1(config)#line console 0 R1(config-line)#password cisco R1(config-line)#login R1(config-line)#exit
Contraseña de acceso Telnet	R1#enable R1#configure terminal R1(config)#line vty 0 15 R1(config-line)# password cisco R1(config-line)#login R1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R1#enable R1#configure terminal R1(config)#service password-encryption R1(config)#exit
Mensaje MOTD	“Se prohíbe el acceso no autorizado.” R1#enable R1#configure terminal R1(config)#banner motd %Se prohibe el acceso no autorizado%

Interfaz S0/0/0	Establezca la descripción R1(config-if)# description connection to R2 R1>enable R1#configure terminal R1(config)# interface serial 0/0/0 R1(config-if)# ip address 172.16.1.1 255.255.255.252 Establecer la frecuencia de reloj en 128000 R1(config-if)# clock rate 128000 Activar la interfaz R1(config-if)# no shutdown R1>enable R1# configure terminal R1(config)# ipv6 unicast-routing R1(config)# interface serial 0/0/0 R1(config-if)# ipv6 address 2001:DB8:ACAD:1::1/64 Establecer la frecuencia de reloj en 128000 R1(config-if)# clock rate 128000 Activar la interfaz R1(config-if)# no shutdown
Rutas predeterminadas	Configurar una ruta IPv4 predeterminada de S0/0/0 R1(config)# ip route 0.0.0.0 0.0.0.0 s0/0/0 Configurar una ruta IPv6 predeterminada de S0/0/0 R1(config)# ipv6 route ::/0 serial 0/0/0

3.4.3 CONFIGURAR ROUTER 2

Tabla 4. Configuración del router 2.

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Router>enable Router#configure terminal R2(config)#no ip domain-lookup
Nombre del router	Router>enable Router#configure terminal Router(config)#hostname R2
Contraseña de exec privilegiado cifrada	R2>enable R2#configure terminal R2(config)# enable secret class R2(config)# service password-encryption
Contraseña de acceso a la consola	R2>enable R2#configure terminal R2(config)# line console 0 R2(config-line)# password cisco R2(config-line)# login R2(config-line)# exit
Contraseña de acceso Telnet	R2>enable R2#configure terminal R2(config)# line vty 0 15 R2(config-line)# password cisco R2(config-line)# login R2(config-line)# exit
Cifrar las contraseñas de texto no cifrado	R2>enable R2#configure terminal R2(config)# service password-encryption R2(config)# exit
Habilitar el servidor HTTP	R2(config)# ip http server

Mensaje MOTD	Se prohíbe el acceso no autorizado. R2>enable R2#configure terminal R2(config)# banner motd %Se prohibe el acceso no autorizado% R2(config)#exit
Interfaz S0/0/0	Establezca la descripción R2(config-if)# description connection to R1 R2>enable R2# configure terminal R2(config)# interface serial 0/0/0 R2(config-if)# ip address 172.16.1.2 255.255.255.252 Activar la interfaz R2(config-if)# no shutdown R2#enable R2# configure terminal R2(config)# interface serial 0/0/0 R2(config-if)# ipv6 address 2001:DB8:ACAD:1::2/64 Activar la interfaz R2(config-if)# no shutdown

Interfaz S0/0/1	R2(config-if)#description connection to R3 R2(config)# interface serial 0/0/1 R2(config-if)# ip address 172.16.2.2 255.255.255.252 Establecer la frecuencia de reloj en 128000. R2(config-if)# clock rate 128000 Activar la interfaz R2(config-if)# no shutdown R2(config-if)# ipv6 address 2001:DB8:ACAD:2::2/64 Establecer la frecuencia de reloj en 128000. R2(config-if)# clock rate 128000 Activar la interfaz R2(config-if)# no shutdown

Interfaz G0/0 (simulación de Internet)	R2(config-if)# description connection to Internet R2#enable R2#configure terminal R2(config-if)# ip address 209.165.200.233 255.255.255.248 Activar la interfaz R2(config-if)# no shutdown R2(config-if)# ipv6 address 2001:DB8:ACAD:A::1/64 Activar la interfaz R2(config-if)# no shutdown De la dirección IP asignada al servidor de Internet: 209.165.200.238 se hace una operación AND con la máscara indicada 248 (/29) para identificar la subnet: Operación AND: 1110 1110 -> 238 -> último octeto dierección IP 1111 1000 -> 248 -> Mascara indicada en topología 1110 1000 -> 232 -> Subnet a la que pertenece G0/0 209.165.200.232 -> Subnet 209.165.200.239 -> BroadCast Por tanto la primer dirección IP para G0/0 es: G0/0 -> 209.165.200.233
Interfaz loopback 0 (servidor web simulado)	Establecer la descripción. R2(config-if)# description Servidor web Establezca la dirección IPv4. R2>enable R2#configure terminal R2(config)# interface lo0 R2(config-if)# ip address 10.10.10.10 255.255.255.255

Ruta predeterminada	Configure una ruta IPv4 predeterminada de G0/0. R2(config)# ip route 0.0.0.0 0.0.0.0 g0/0 Configure una ruta IPv6 predeterminada de G0/0. R2(config)# ipv6 route ::/0 g0/0

3.4.4 CONFIGURAR ROUTER 3

Tabla 5. Configuración del router 3.

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	R3>enable R3#configure terminal R3(config)#no ip domain-lookup
Nombre del router	R3 Router>enable Router# configure terminal Router(config)# hostname R3
Contraseña de exec privilegiado cifrada	R3>enable R3#configure terminal R3(config)# enable secret class R3(config)# servece password-encryption
Contraseña de acceso a la consola	R3>enable R3#configure terminal R3(config)# line console 0 R3(config-line)# password cisco R3(config-line)# login R3(config-line)# exit

Contraseña de acceso Telnet	R3>enable R3#configure terminal R3(config)# line vty 0 15 R3(config-line)# password cisco R3(config-line)# login R3(config-line)# exit
Cifrar las contraseñas de texto no cifrado	R3>enable R3#configure terminal R3(config)# service password-encryption R3(config)# exit
Mensaje MOTD	R3>enable R3#configure terminal R3(config)# banner motd %Se prohibe el acceso no autorizado% R3(config)# exit
Interfaz S0/0/1	Router(config-if)# description connetion to R2 R3>enable R3#configure terminal R3(config)# interface serial 0/0/1 R3(config-if)# ip address 172.16.2.1 255.255.255.252 Activar la interfaz R3(config-if)# no shutdown R3(config)# interface serial 0/0/1 R3(config-if)# ipv6 address 2001:DB8:ACAD:2::1/64 Activar la interfaz R3(config-if)# no shutdown
Interfaz loopback 4	R3>enable R3#configure terminal R3(config)# interface lo4 R3(config-if)# ip address 192.168.4.1 255.255.255.0 R3(config-if)# description Loopback 4

Interfaz loopback 5	R3>enable R3#configure terminal R3(config-if)# ip address 192.168.5.1 255.255.255.0 R3(config-if)# description Loopback 5
Interfaz loopback 6	R3>enable R3#configure terminal R3(config-if)# ip address 192.168.6.1 255.255.255.0 R3(config-if)# description Loopback 6
Interfaz loopback 7	R3>enable R3#configure terminal R3(config-if)# ipv6 address 2001:DB8:ACAD:3::1/64 R3(config-if)# description Loopback 7

3.4.5 CONFIGURAR S1

Tabla 6. Configuración del S1

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Switch>enable Switch#configure terminal Switch(config)# no ip domain-lookup
Nombre del switch	Switch>enable Switch#configure terminal Switch(config)# hostname S1
Contraseña de exec privilegiado cifrada	S1>enable S1#configure terminal S1(config)# enable secret class S1(config)# service password-encryption

Contraseña de acceso a la consola	S1>enable S1#configure terminal S1(config)# line console 0 S1(config-line)# password cisco S1(config-line)# login S1(config-line)# exit
Contraseña de acceso Telnet	S1>enable S1#configure terminal S1(config)# line vty 0 15 S1(config-line)# password cisco S1(config-line)# login S1(config-line)# exit
Cifrar las contraseñas de texto no cifrado	S1>enable S1#configure terminal S1(config)# service password-encryption S1(config)# exit
Mensaje MOTD	Se prohíbe el acceso no autorizado. S1>enable S1#configure terminal S1(config)# banner motd %Se prohibe el acceso no autorizado% S1(config)# exit

3.4.6 CONFIGURAR S3

Tabla 7. Configuración del S3

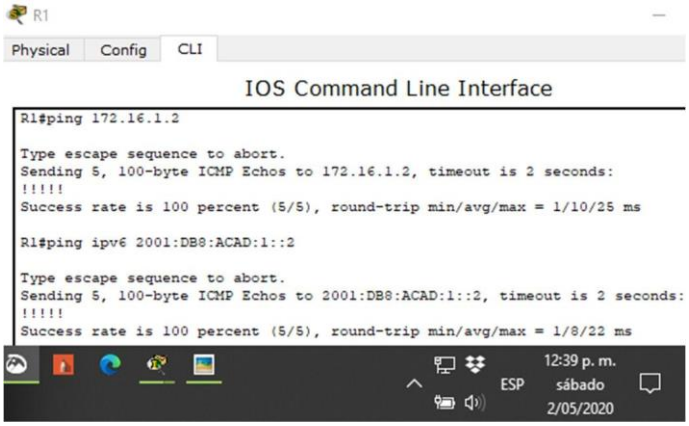
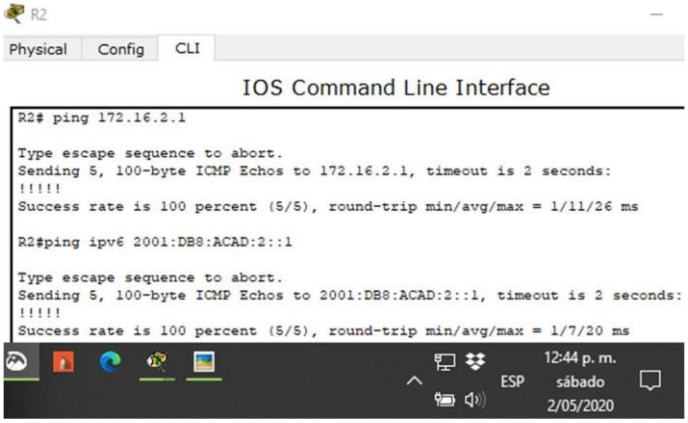
Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Switch>enable Switch#configure terminal Switch(config)# no ip domain-lookup
Nombre del switch	Switch>enable Switch#configure terminal Switch(config)# no ip domain-lookup Switch(config)# hostname S3

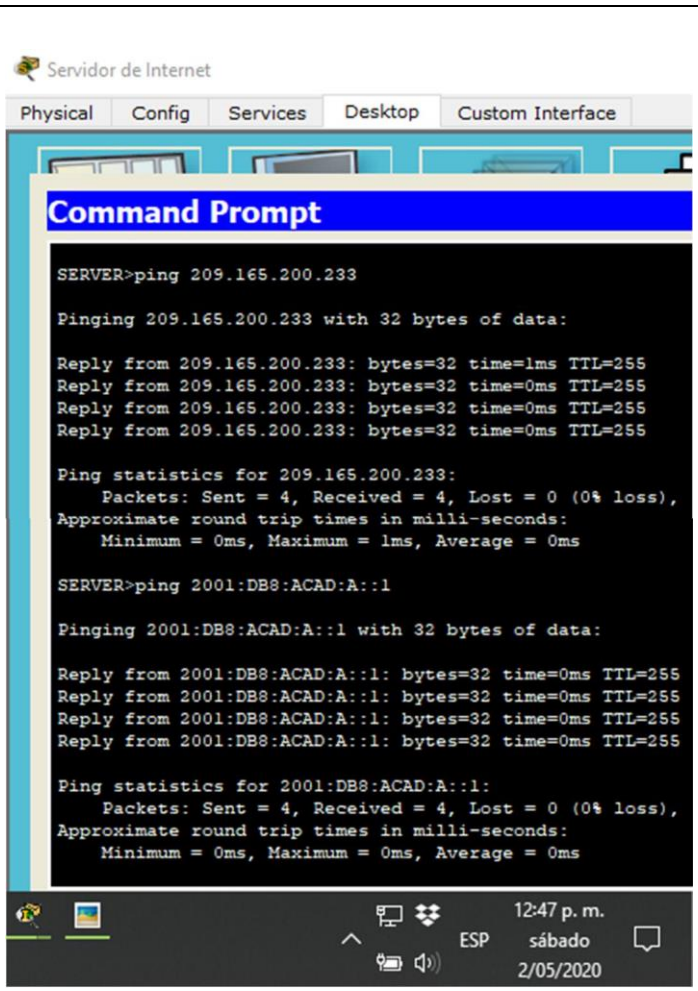
Contraseña de exec privilegiado cifrada	S3>enable S3#configure terminal S3(config)# enable secret class S3(config)# service password-encryption
Contraseña de acceso a la consola	S3>enable S3#configure terminal S3(config)# line console 0 S3(config-line)# password cisco S3(config-line)# login S3(config-line)# exit
Contraseña de acceso Telnet	S3>enable S3#configure terminal S3(config)# line vty 0 15 S3(config-line)# password cisco S3(config-line)# login S3(config-line)# exit
Cifrar las contraseñas de texto no cifrado	S3>enable S3#configure terminal S3(config)# service password-encryption S3(config)# exit
Mensaje MOTD	Se prohíbe el acceso no autorizado. S3>enable S3#configure terminal S3(config)# banner motd %Se prohibe el acceso no autorizado% S3(config)# exit

3.4.7 VERIFICAR LA CONECTIVIDAD DE LA RED

Por medio del comando ping se prueba la conectividad entre los dispositivos de la red. Para realizar la probar la conectividad de forma metódica se muestra la siguiente tabla donde se indica el enlace probado la dirección IP evaluada y se valida el resultado por medio del resultado presentado por la consola.

Tabla 8. Verificación de conectividad usando el comando ping

De sde	**A**	**Dirección IP**	**Resultados de ping**
R1	R2, S0/0/0	172.16.1.2 2001:DB8:ACAD:1::2	Figura 3. Ping verificación conectividad R1 
R2	R3, S0/0/1	172.16.2.1 2001:DB8:ACAD:2::1	Figura 4. Ping verificación conectividad R2 
PC de	Gatew ay	209.165.200 .233	Figura 5. Ping verificación conectividad PC de Internet

Internet	predeter-minado	2001:DB8:ACAD:A::1	

3.5 CONFIGURAR LA SEGURIDAD DEL SWITCH, LAS VLAN Y EL ROUTING ENTRE VLAN

Con base en las tablas presentadas en la topología se procede a configurar cada VLAN, se asignan nombres para cada una de ellas, luego se asocian a la dirección de administración, se configuran los puertos troncales y modos de operación para cada puerto, este procedimiento se aplica a cada uno de los switches ajustándolo al puerto y VLAN que le corresponde. En el router se configuran las subinterfaces 802.1Q, con el propósito de asegurar el direccionamiento entre las VLANS y estas se asocian a la interface g0/1 a la que están físicamente conectadas en el router, al final se muestra la verificación del proceso validando la comunicación por medio de comandos ping entre VLAN y los dispositivos asociados a estas e indicados en la topología.

3.5.1 CONFIGURAR S1

Tabla 9. Configuración del S1

Elemento o tarea de configuración	**Especificación**
Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para topología para crear y nombrar cada una de las VLAN que se indicant S1>enable Password: S1# configure terminal S1(config)# vlan 21 S1(config-vlan)# name Contabilidad S1(config-vlan)# vlan 23 S1(config-vlan)# name Ingenieria S1(config-vlan)# vlan 99 S1(config-vlan)# name Administracion S1(config-vlan)#end

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 S1# configure terminal S1(config)# interface vlan 99 S1(config-if)# ip address 192.168.99.2 255.255.255.0 S1(config-if)# no shutdown S1(config-if)# end
Asignar el gateway predeterminado	Asigne la primera dirección IPv4 de la subred como el gateway predeterminado. S1# configure terminal S1(config)# ip default-gateway 192.168.99.1 S1(config)# end
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa S1# configure terminal S1(config)# interface Fa0/3 S1(config-if)# switchport mode trunk S1(config-if)# switchport trunk native vlan 1
Forzar el enlace troncal en la interfaz F0/5	Utilizar la red VLAN 1 como VLAN nativa S1# configure terminal S1(config)# interface Fa0/5 S1(config-if)# switchport mode trunk S1(config-if)# switchport trunk native vlan 1 S1(config-if)# no shutdown
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range S1# configure terminal S1(config)#interface range fa0/4, fa0/1-2, fa0/7-24, gi0/1-2 S1(config-if-range)# switchport mode access
Asignar F0/6 a la VLAN 21	S1# configure terminal S1(config)# interface Fa0/6 S1(config-if)# switchport access vlan 21 S1(config-if)# switchport mode access S1(config-if)# end
Apagar todos los puertos sin usar	S1#configure terminal S1(config)#interface range fa0/4, fa0/1-2, fa0/7-24, gi0/1-2 S1(config-if-range)# shutdown

3.5.2 CONFIGURAR S3

Tabla 10. Configuración del S3

Elemento o tarea de configuración	**Especificación**
Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para topología para crear cada una de las VLAN que se indican Dé nombre a cada VLAN. S3> enable Password: S3# configure terminal S3(config)# vlan 21 S3(config-vlan)# name Contabilidad S3(config-vlan)# vlan 23 S3(config-vlan)# name Ingenieria S3(config-vlan)# vlan 99 S3(config-vlan)# name Administracion S3(config-vlan)# end
Asignar la dirección IP de administración	Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S3 en el diagrama de topología S3# configure terminal S3(config)# interface vlan 99 S3(config-if)# ip address 192.168.99.3 255.255.255.0 S3(config-if)# no shutdown S3(config-if)# end
Asignar el gateway predeterminado.	Asignar la primera dirección IP en la subred como gateway predeterminado. S3# configure terminal S3(config)# ip default-gateway 192.168.99.1 S3(config)# end

Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa S3# configure terminal S3(config)# interface Fa0/3 S3(config-if)# switchport mode trunk S3(config-if)# switchport trunk native vlan 1 S3(config-if)# end
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range S3# configure terminal S3(config)# interface range fa0/19 - 24, fa0/1 - 2, fa0/4 - 17, gi0/1 - 2 S3(config-if-range)# switchport mode access S3(config-if-range)# exit
Asignar F0/18 a la VLAN 21 según la topología es a la VLAN 23	S3# configure terminal S3(config)# interface Fa0/18 S3(config-if)# switchport access vlan 23 S1(config-if)# switchport mode access S3(config-if)# end
Apagar todos los puertos sin usar	S3#configure terminal S3(config)#interface range fa0/19 - 24, fa0/1 - 2, fa0/4 - 17, gi0/1 - 2 S3(config-if-range)# shutdown

3.5.3 CONFIGURAR R1

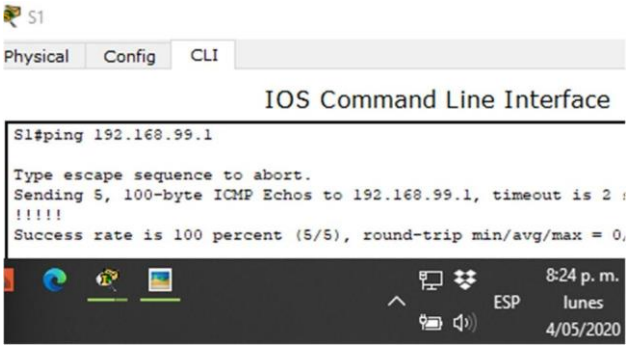
Tabla 11. Configuración del R1

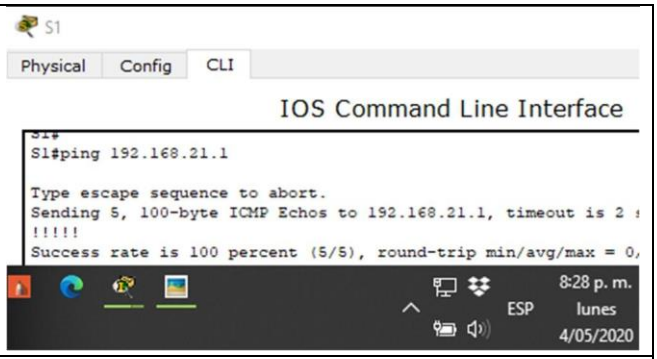
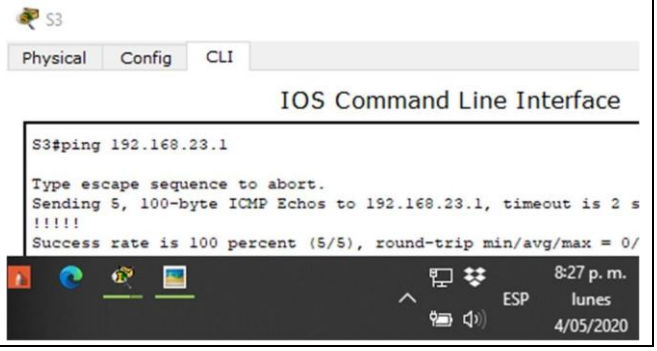
Elemento o tarea de configuración	**Especificación**
Configurar la subinterfaz 802.1Q .21 en G0/1	Descripción: LAN de Contabilidad Asignar la VLAN 21 Asignar la primera dirección disponible a esta interfaz de R1>enable Password: R1#configure terminal R1(config)#interface g0/1.21 R1(config-subif)#description VLAN 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	Descripción: LAN de Ingeniería Asignar la VLAN 23 Asignar la primera dirección disponible a esta interfaz R1(config-subif)#interface 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	Descripción: LAN de Administración Asignar la VLAN 99 Asignar la primera dirección disponible a esta interfaz R1(config-subif)#interface 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-subif)#interface g0/1 R1(config-if)#no shutdown

3.5.4 VERIFICAR LA CONECTIVIDAD DE LA RED

Se utiliza el comando ping para probar la conectividad entre los switches y el R1. En la siguiente tabla se evidencia de forma metódica la conectividad con cada dispositivo de red.

Tabla 12. Verificación de conectividad de la red

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	Figura 6. Ping verificación conectividad S1 a R1 VLAN99 
S3	R1, dirección VLAN 99	192.168.99.1	Figura 7. Ping verificación conectividad S3 a R1 VLAN99 
S1	R1, dirección VLAN 21	192.168.21.1	Figura 8. Ping verificación conectividad S1 a R1 VLAN 21

			
S3	R1, dirección VLAN 23	192.168.23.1	Figura 9. Ping verificación conectividad S3 a R1 VLAN 23 

3.6 CONFIGURAR EL PROTOCOLO DE ROUTING DINÁMICO RIPv2

La configuración del protocolo de enrutamiento dinámico RIPv2 consiste en que cada router anuncie las rutas que tiene directamente conectadas, para esto en el modo de configuración privilegiada se aplican los comandos que permiten configurar el protocolo con su respectiva versión, las redes que tiene directamente conectadas y las interfaces pasivas para evitar anuncios por estas. En las tablas presentadas a continuación, se muestra el paso a paso para realizar la configuración de RIPv2 en cada router.

3.6.1 CONFIGURAR RIPv2 EN EL R1

Tabla 13. Configuración de RIPv2 en el R1

Elemento o tarea de configuración	**Especificación**
Configurar RIP versión 2	R1>enable Password: R1# configure terminal R1(config)# router rip R1(config-router)# version 2
Anunciar las redes conectadas directamente	Asigne todas las redes conectadas directamente. R1# configure terminal R1(config)# router rip R1(config-router)# version 2 R1(config-router)# network 172.16.1.0 R1(config-router)# network 192.168.21.0 R1(config-router)# network 192.168.23.0 R1(config-router)# network 192.168.99.0
Establecer todas las interfaces LAN como pasivas	R1(config-router)# passive-interface g0/1
Desactive la sumarización automática	R1(config-router)# no auto-summary

3.6.2 CONFIGURAR RIPv2 EN EL R2

Tabla 14. Configuración de RIPv2 en el R2

Elemento o tarea de configuración	**Especificación**
Configurar RIP versión 2	R2>enable Password: R2(config)# router rip R2(config-router)# version 2
Anunciar las redes conectadas directamente	Nota: Omitir la red G0/0. R2(config-router)# network 172.16.1.0 R2(config-router)# network 172.16.2.0
Establecer la interfaz LAN (loopback) como pasiva	R2(config-router)# passive-interface lo0
Desactive la sumarización automática.	R2(config-router)# no auto-summary

3.6.3 CONFIGURAR RIPv2 EN EL R3

Tabla 15. Configuración de RIPv2 en el R3

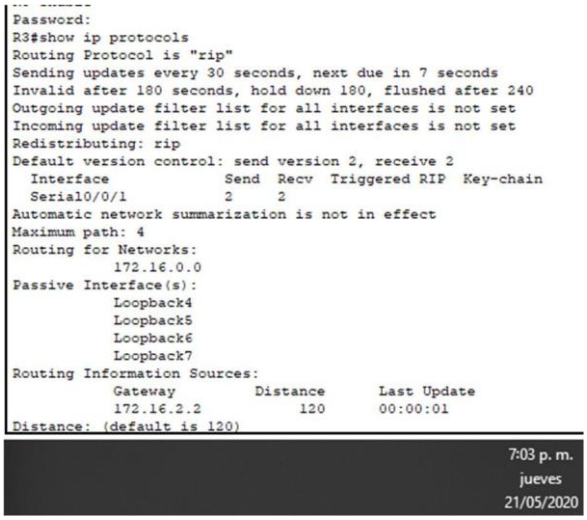
Elemento o tarea de configuración	**Especificación**
Configurar RIP versión 2	R3>enable Password: R3# configure terminal R3(config)# router rip R3(config-router)# version 2
Anunciar redes IPv4 conectadas directamente	R3(config-router)# network 172.16.2.0

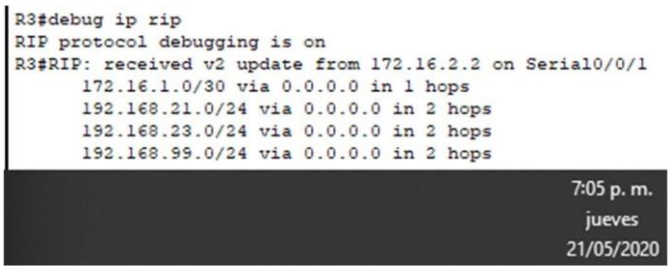
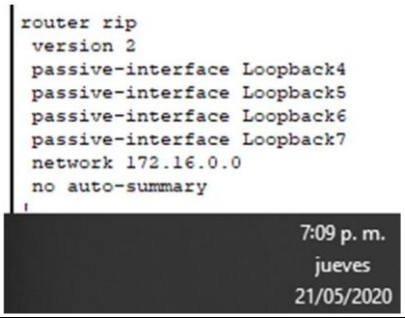
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	R3(config-router)# passive-interface lo4 R3(config-router)# passive-interface lo5 R3(config-router)# passive-interface lo6 R3(config-router)# passive-interface lo7
Desactive la sumarización automática.	R3(config-router)# no auto-summary

3.6.4 VERIFICACIÓN DE LA INFORMACIÓN RIP

La verificación del protocolo RIP se muestra en la siguiente tabla que describe los comandos que evidencian el funcionamiento como se espera:

Tabla 16. Verificación 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 protocols Figura 10. Resultado del comando show ip protocols. 
¿Qué comando muestra solo las rutas RIP?	Debug ip rip Figura 11. Resultado del comando debug ip rip.

	
¿Qué comando muestra la sección de RIP de la configuración en ejecución?	Show running-config Figura 12. Resultado del comando show running-config. 

3.7 IMPLEMENTAR DHCP Y NAT PARA IPv4

La configuración del servicio DHCP permiten básicamente la asignación dinámica de direcciones IP mientras que NAT permite la traducción de estas. A continuación se muestra el procedimiento para configurar cada uno de estos servicios en los routers y posteriormente se valida la configuración por medio de comandos que monitorean parámetros de estos servicios, como por ejemplo el comando de consola ipconfig /all que muestra la configuración y asignación dinámica del protocolo DHCP

3.7.1 CONFIGURAR EL R1 COMO SERVIDOR DHCP PARA LAS VLAN21 Y 23

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 17. Configuración de R1 como servidor de DHCP

Elemento o tarea de configuración	**Especificación**
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	R1# configure terminal R1(config)# 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	R1(config)# ip dhcp excluded-address 192.168.23.1 192.168.23.20

Crear un pool de DHCP para la VLAN 21.	Nombre: ACCT R1(config)# ip dhcp pool ACCT Servidor DNS: 10.10.10.10 R1(dhcp-config)# dns-server 10.10.10.10 Nombre de dominio: ccna-sa.com R1(dhcp-config)# domain-name ccna-lab.com Establecer el gateway predeterminado R1(dhcp-config)# default-router 192.168.21.1
Crear un pool de DHCP para la VLAN 23	Nombre: ENGNR R1(config)# ip dhcp pool ENGNR Servidor DNS: 10.10.10.10 R1(dhcp-config)# dns-server 10.10.10.10 Nombre de dominio: ccna-sa.com R1(dhcp-config)# domain-name ccna-lab.com Establecer el gateway predeterminado R1(dhcp-config)# default-router 192.168.23.1

3.7.2 CONFIGURAR LA NAT ESTÁTICA Y DINÁMICA EN EL R2

La configuración del R2 incluye las siguientes tareas:

Tabla 18. Configuración del R2 con NAT estática y dinámica

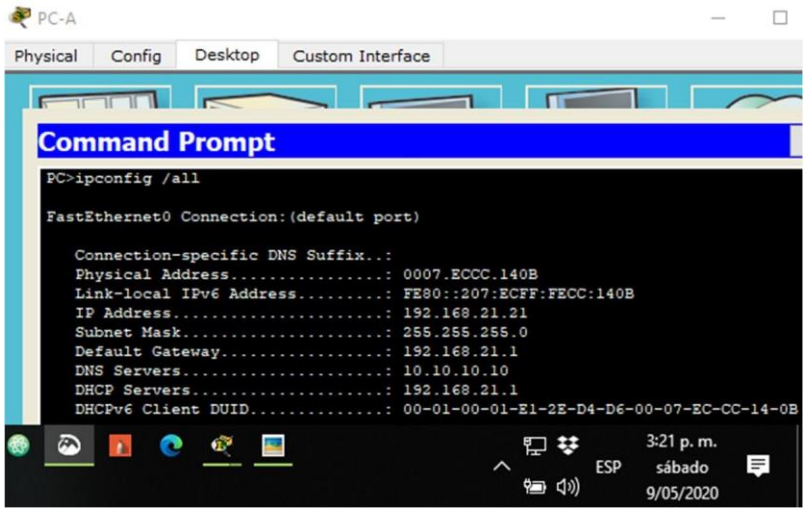
Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	Nombre de usuario: webuser Contraseña: cisco12345 Nivel de privilegio: 15 R2(config)# username webuser privilege 15 secret cisco12345
Habilitar el servicio del servidor HTTP	R2(config)# ip http server
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.	Dirección global interna: 209.165.200.229 En este caso y como se demostró en se debe configurar la Direccion global interna: 209.165.200.238 R2(config)# ip nat inside source static 209.165.200.238 209.165.200.229
Asignar la interfaz interna y externa para la NAT estática	R2(config)# interface s0/0/0 R2 (config-if)# ip nat inside R2 (config-if)# interface g0/0 R2 (config-if)# ip nat outside
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 Lista de acceso: 1 R2 (config)# access-list 1 permit 192.168.21.0 0.0.31.255 Lista de acceso: 2 R2 (config)# access-list 2 permit 192.168.4.0 0.0.7.255

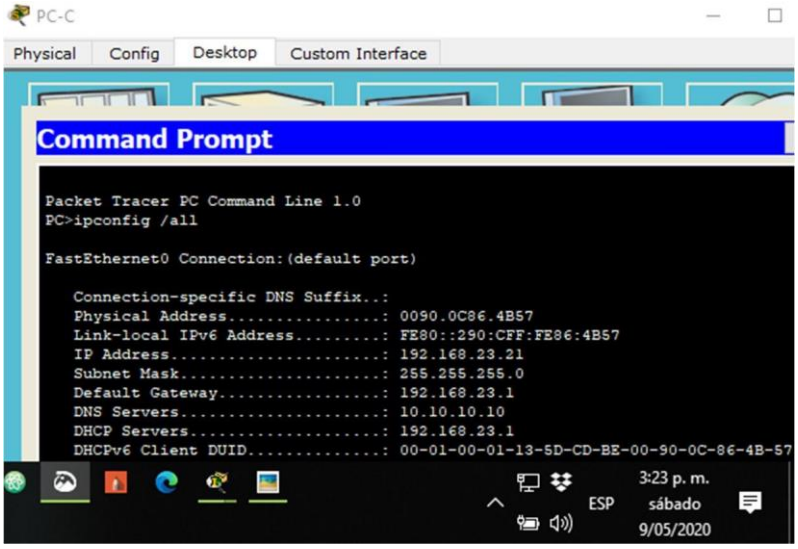
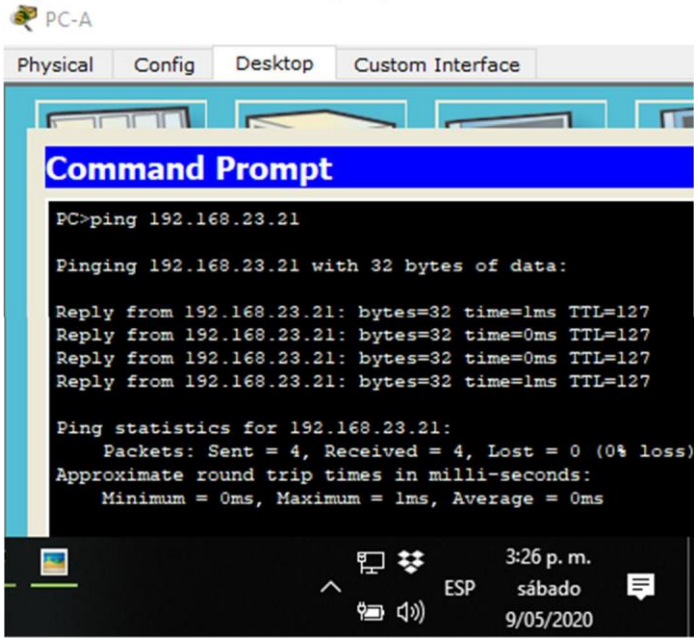
Defina el pool de direcciones IP públicas utilizables.	Nombre del conjunto: INTERNET El conjunto de direcciones incluye: 209.165.200.225 – 209.165.200.228 R2(config)# ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248
Definir la traducción de NAT dinámica	R2(config)# ip nat inside source list 1 pool INTERNET R2(config)# ip nat inside source list 2 pool INTERNET

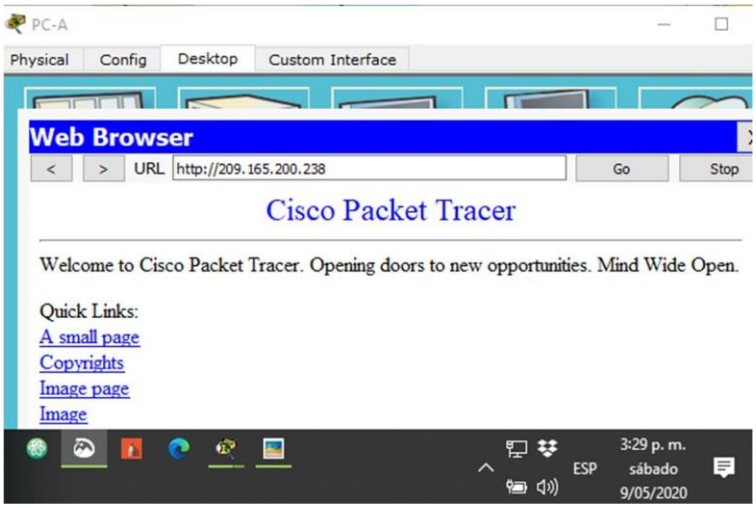
3.7.3 VERIFICAR EL PROTOCOLO DHCP Y LA NAT ESTÁTICA

Para verificar las tareas de configuración de DHCP y NAT estática se muestra el siguiente procedimiento con el respectivo resultado que permite validar dicha configuración.

Tabla 19. Verificación del protocolo DHCP y NAT estática

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	Figura 13. Asignación IP a PC-A por DHCP 

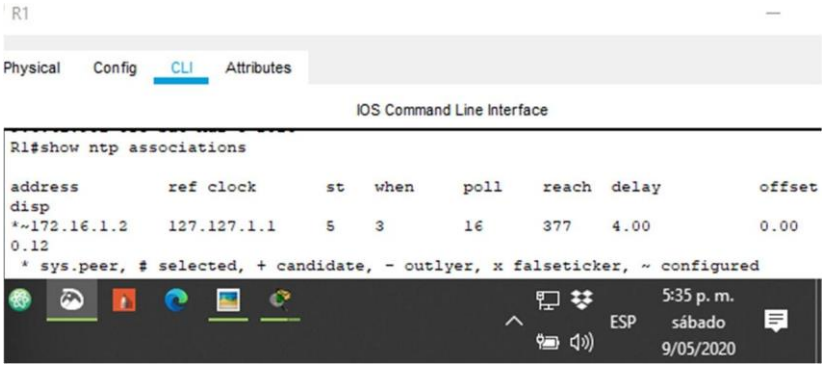
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	Figura 14. Asignación IP a PC-C por DHCP 
Verificar que la PC-A pueda hacer ping a la PC-C Nota: Quizá sea necesario deshabilitar el firewall de la PC.	Figura 15. Verificación ping de PC-A a PC-C 

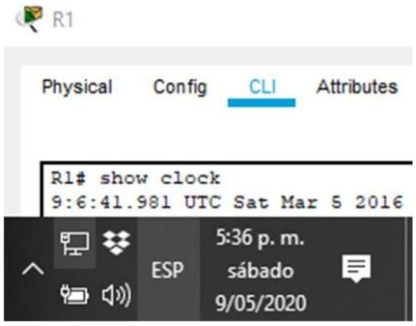
Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.229) Iniciar sesión con el nombre de usuario webuser y la contraseña cisco12345 Dado que la computadora se configuró con la ip 209.165.200.238 se utiliza la PC para acceder a ella.	Figura 16. Navegador web para acceder a servidor web 

3.8 CONFIGURAR NTP

La configuración del protocolo NTP permite la sincronización de la fecha y hora en los dispositivos que participan en una red y que están configurados para tal propósito, en el procedimiento que se muestra a continuación se indica el paso a paso para configurar el *router* R2 como maestro NTP y el *router* R1 como cliente, al final se valida la configuración por medio del comando *show clock* que muestra la configuración de fecha y hora entregada por el maestro NTP.

Tabla 20. Configuración de NTP

Elemento o tarea de configuración	**Especificación**
Ajuste la fecha y hora en R2.	5 de marzo de 2016, 9 a. m. R2 # clock set 09:00:00 mar 5 2016
Configure R2 como un maestro NTP.	Nivel de estrato: 5 R2 (config)# ntp master 5
Configurar R1 como un cliente NTP.	Servidor: R2 R1(config)# ntp server 172.16.1.2
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	Figura 17. Actualizaciones periódicas con hora. 

Verifique la configuración de NTP en R1.	R1# show clock Figura 18. Verificación de la configuración NTP 

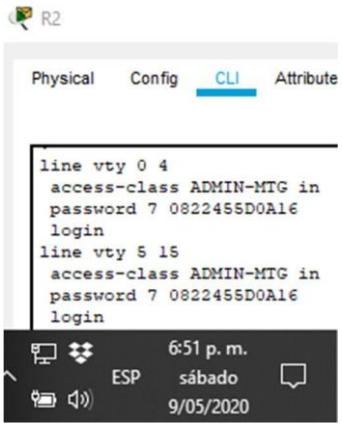
3.9 CONFIGURAR Y VERIFICAR LAS LISTAS DE CONTROL DE ACCESO (ACL)

La seguridad es uno de los parámetros mas importantes en la configuración de redes, las listas de control de acceso permiten restringir el uso y proteger la red ante intrusos, en el siguiente procedimiento se indica la creación, y configuración de una ACL para permitir que solo R1 pueda establecer conexión telnet con R2, también se valida que dicha configuración funciona como se espera por medio del comando de monitoreo show access-list en R2.

3.9.1 RESTRINGIR EL ACCESO A LAS LINEAS VTY EN EL R2

Tabla 21. Restricción de acceso a las líneas VTY en el R2

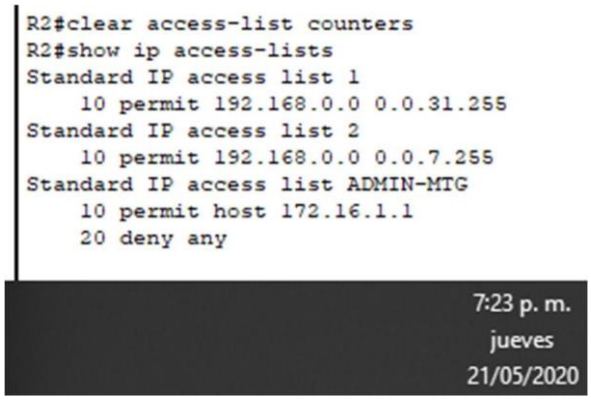
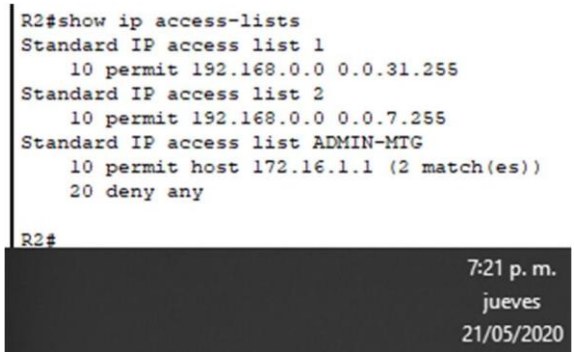
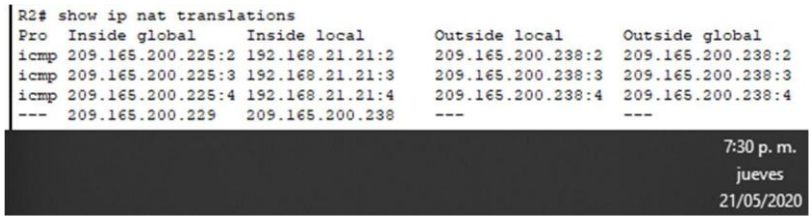
Elemento o tarea de configuración	**Especificación**
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	Nombre de la ACL: ADMIN-MGT R2(config)# ip access-list standard ADMIN-MTG R2(config-std-nacl)# permit host 172.16.1.1 R2(config-std-nacl)# deny any
Aplicar la ACL con nombre a las líneas VTY	R2(config)# line vty 0 15
Permitir acceso por Telnet a las líneas de VTY	R2(config-line)# access-class ADMIN-MTG in

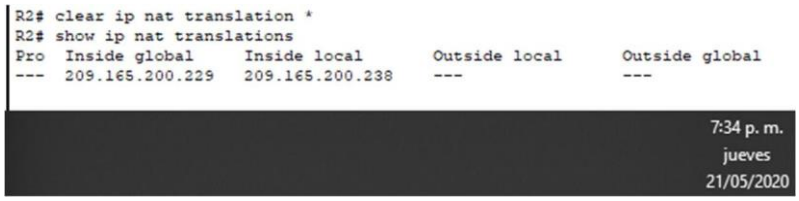
Verificar que la ACL funcione como se espera	R2(config)# show access-lists Figura 19. Verificación de funcionamiento de ACL. 

3.9.2 INTRODUCCIR EL COMANDO CLI ADECUADO QUE SE NECESITA PARA MOSTRAR LO SIGUIENTE

Tabla 22. Comando CLI adecuado para mostrar la información

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-lists Figura 20. Resultado del comando show access-list. 

Restablecer los contadores de una lista de acceso	R2(config)# clear access-list counters Figura 21. Resultado del comando clear 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 access-lists Figura 22. Resultado del comando show ip access-lists 
¿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 debido al modo de simulación de Internet en la red. R2#show ip nat translations Figura 23. Resultado del comando show ip nat translations. 

¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	R2#clear ip nat translation* Figura 24. Resultado del comando show ip nat translations. 

4. ESCENARIO 2

4.1 DESCRIPCION DEL 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.

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.

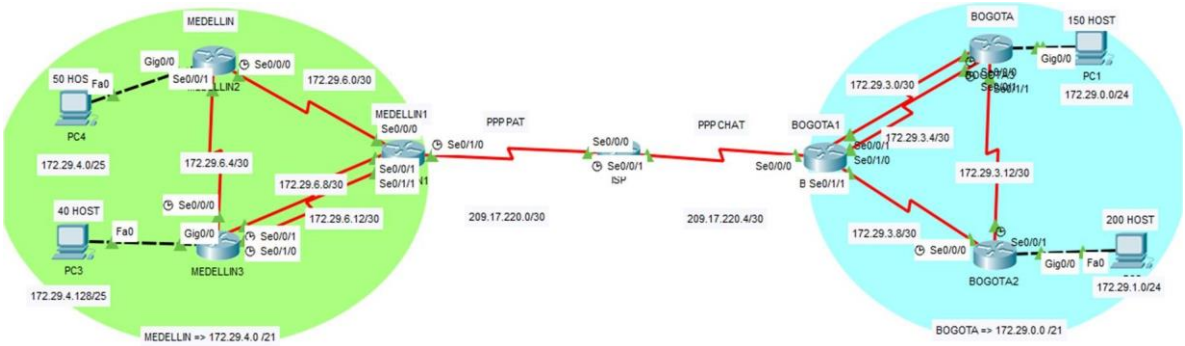
Como trabajo inicial se debe realizar lo siguiente.
Realizar las rutinas de diagnóstico y dejar los equipos listos para su configuración (asignar nombres de equipos, asignar claves de seguridad, etc).

Para todos los routers se realiza la configuración básica siguiendo el procedimiento descrito a continuación:

4.2 TOPOLOGÍA

En la siguiente figura se puede apreciar los enlaces establecidos entre los dispositivos que hacen parte de la topología del escenario 2 y en base en esta se desarrollan las actividades que hacen parte de este escenario.

Figura 25. Topología implementada en el escenario 2.



4.3 RUTINAS DE DIAGNOSTICO Y CONFIGURACIÓN INICIAL DE DISPOSITIVOS

Entre las actividades desarrolladas para la configuración de dispositivos está la asignación de nombres para los equipos, configuración de interfaces, claves para la consola, usuario privilegiado y líneas administrativas. Estas configuraciones genéricas son aplicadas en todos los routers que participan en este escenario y se describen en detalle a continuación para cada dispositivo.

4.3.1 CONFIGURACIÓN INICIAL Y RUTINA DE DIAGNOSTICO MEDELLÍN1

Tabla 23. Configuración router Medellín1

Descripción del comando	**Comandos**
Realizar las rutinas de diagnóstico y	Router>enable Router#configure terminal

dejar los equipos listos para su configuración (asignar nombres de equipos, asignar claves de seguridad, etc.)	Router(config)#hostname MEDELLIN1 MEDELLIN1(config)# no ip domain-lookup 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)# exit MEDELLIN1(config)# banner motd %Se prohibe el acceso no autorizado!% MEDELLIN1(config)# exit
Configuración de interfaces	MEDELLIN1#configure terminal MEDELLIN1(config)# interface serial0/0/0 MEDELLIN1(config-if)# ip address 172.29.6.2 255.255.255.252 MEDELLIN1(config-if)# description connection to MEDELLIN2 MEDELLIN1(config-if)# no shutdown MEDELLIN1(config-if)# interface serial0/0/1 MEDELLIN1(config-if)# ip address 172.29.6.10 255.255.255.252 MEDELLIN1(config-if)# description connection to MEDELLIN3 MEDELLIN1(config-if)# no shutdown MEDELLIN1(config-if)# interface serial0/1/1 MEDELLIN1(config-if)# ip address 172.29.6.13 255.255.255.252 MEDELLIN1(config-if)# description connection to MEDELLIN3 MEDELLIN1(config-if)# no shutdown MEDELLIN1(config-if)# interface serial0/1/0 MEDELLIN1(config-if)# ip address 209.17.220.1 255.255.255.252

	MEDELLIN1(config-if)# description connection to ISP MEDELLIN1(config-if)# clock rate 64000 MEDELLIN1(config-if)# no shutdown

4.3.2 CONFIGURACIÓN INICIAL Y RUTINA DE DIAGNOSTICO MEDELLÍN2

Tabla 24. Configuración router Medellín2

Descripción del comando	**Comandos**
Realizar las rutinas de diagnóstico y dejar los equipos listos para su configuración (asignar nombres de equipos, asignar claves de seguridad, etc)	Router>enable Router# configure terminal Router(config)# hostname MEDELLIN2 MEDELLIN2(config)# no ip domain-lookup 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)# exit MEDELLIN2(config)# banner motd %Se prohibe el acceso no autorizado!% MEDELLIN2(config)# exit
Configuración de interfaces	MEDELLIN2#configure terminal Enter configuration commands, one per line. End with CNTL/Z. MEDELLIN2(config)#interface serial0/0/0 MEDELLIN2(config-if)# ip address 172.29.6.1 255.255.255.252 MEDELLIN2(config-if)# description connection to MEDELLIN1 MEDELLIN2(config-if)# clock rate 64000 MEDELLIN2(config-if)# no shutdown

	MEDELLIN2(config-if)#interface serial0/0/1 MEDELLIN2(config-if)# ip address 172.29.6.6 255.255.255.252 MEDELLIN2(config-if)# description connection to MEDELLIN3 MEDELLIN2(config-if)# no shutdown MEDELLIN2(config)#interface g0/0 MEDELLIN2(config-if)# ip address 172.29.4.1 255.255.255.128 MEDELLIN2(config-if)# description connection to 50Hosts_PC4 MEDELLIN2(config-if)# no shutdown

4.3.3 CONFIGURACIÓN INICIAL Y RUTINA DE DIAGNOSTICO MEDELLÍN3

Tabla 25. Configuración router Medellín3

Descripción del comando	**Comandos**
Realizar las rutinas de diagnóstico y dejar los equipos listos para su configuración (asignar nombres de equipos, asignar claves de seguridad, etc)	Router>enable Router# configure terminal Router(config)# hostname MEDELLIN3 MEDELLIN3(config)# no ip domain-lookup 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)# exit MEDELLIN3(config)# banner motd %Se prohibe el acceso no autorizado!% MEDELLIN3(config)# exit
Configuración de interfaces	MEDELLIN3>enable Password:

	MEDELLIN3#configure terminal MEDELLIN3(config)# interface serial0/0/0 MEDELLIN3(config-if)# ip address 172.29.6.5 255.255.255.252 MEDELLIN3(config-if)# description connection to MEDELLIN2 MEDELLIN3(config-if)# clock rate 64000 MEDELLIN3(config-if)# no shutdown MEDELLIN3(config-if)# interface serial0/0/1 MEDELLIN3(config-if)# ip address 172.29.6.9 255.255.255.252 MEDELLIN3(config-if)# description connection to MEDELLIN1 MEDELLIN3(config-if)# clock rate 64000 MEDELLIN3(config-if)# no shutdown MEDELLIN3(config-if)# interface serial0/1/0 MEDELLIN3(config-if)# ip address 172.29.6.14 255.255.255.252 MEDELLIN3(config-if)# description connection to MEDELLIN1 MEDELLIN3(config-if)# clock rate 64000 MEDELLIN3(config-if)# no shutdown MEDELLIN3(config)# interface g0/0 MEDELLIN3(config-if)# ip address 172.29.4.129 255.255.255.128 MEDELLIN3(config-if)# description connection to 40Hosts_PC3 MEDELLIN3(config-if)# no shutdown

4.3.4 CONFIGURACIÓN INICIAL Y RUTINA DE DIAGNOSTICO BOGOTÁ1

Tabla 26. Configuración router Bogotá1

Descripción del comando	Comandos
Realizar las rutinas de diagnóstico y dejar los equipos listos para su configuración (asignar nombres de equipos, asignar claves de seguridad, etc)	Router>enable Router# configure terminal Router(config)# hostname BOGOTA1 BOGOTA1(config)# no ip domain-lookup 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)# exit BOGOTA1(config)# banner motd %Se prohibe el acceso no autorizado!% BOGOTA1(config)# exit
Configuración de interfaces	BOGOTA1# configure terminal BOGOTA1(config)# interface serial0/0/0 BOGOTA1(config-if)# ip address 209.17.220.5 255.255.255.252 BOGOTA1(config-if)# description connection to ISP BOGOTA1(config-if)# no shutdown BOGOTA1(config-if)# interface serial0/1/0 BOGOTA1(config-if)# ip address 172.29.3.1 255.255.255.252 BOGOTA1(config-if)# description connection to BOGOTA3 BOGOTA1(config-if)# no shutdown BOGOTA1(config-if)# interface serial0/0/1 BOGOTA1(config-if)# ip address 172.29.3.5 255.255.255.252 BOGOTA1(config-if)# description connection to BOGOTA3 BOGOTA1(config-if)# no shutdown

	BOGOTA1(config-if)# interface serial0/1/1 BOGOTA1(config-if)# ip address 172.29.3.9 255.255.255.252 BOGOTA1(config-if)# description connection to BOGOTA2 BOGOTA1(config-if)# no shutdown

4.3.5 CONFIGURACIÓN INICIAL Y RUTINA DE DIAGNOSTICO BOGOTÁ2

Tabla 27. Configuración router Bogotá2

Descripción del comando	**Comandos**
Realizar las rutinas de diagnóstico y dejar los equipos listos para su configuración (asignar nombres de equipos, asignar claves de seguridad, etc.)	Router>enable Router#configure terminal Router(config)# hostname BOGOTA2 BOGOTA2(config)# no ip domain-lookup 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)# exit BOGOTA2(config)# banner motd %Se prohibe el acceso no autorizado!% BOGOTA2(config)# exit
Configuración de interfaces	BOGOTA2(config)# interface serial0/0/0 BOGOTA2(config-if)# ip address 172.29.3.10 255.255.255.252 BOGOTA2(config-if)# description connect to BOGOTA1 BOGOTA2(config-if)# clock rate 64000 BOGOTA2(config-if)# no shutdown

	BOGOTA2(config-if)# interface serial0/0/1 BOGOTA2(config-if)# ip address 172.29.3.14 255.255.255.252 BOGOTA2(config-if)# description connect to BOGOTA3 BOGOTA2(config-if)# clock rate 64000 BOGOTA2(config-if)# no shutdown BOGOTA2(config-if)# interface g0/0 BOGOTA2(config-if)# ip address 172.29.1.1 255.255.255.0 BOGOTA2(config-if)# description connect to 200Hosts BOGOTA2(config-if)# no shutdown

4.3.6 CONFIGURACIÓN INICIAL Y RUTINA DE DIAGNOSTICO BOGOTÁ3

Tabla 28. Configuración router Bogotá3

Descripción del comando	**Comandos**
Realizar las rutinas de diagnóstico y dejar los equipos listos para su configuración (asignar nombres de equipos, asignar claves de seguridad, etc.)	Router>enable Router#configure terminal Router(config)# hostname BOGOTA3 BOGOTA3(config)# no ip domain-lookup 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)# exit BOGOTA3(config)# banner motd %Se prohibe el acceso no autorizado!% BOGOTA3(config)# exit
Configuración de	BOGOTA3(config-if)# interface serial0/0/0

interfaces	BOGOTA3(config-if)# ip address 172.29.3.6 255.255.255.252 BOGOTA3(config-if)# description connection to BOGOTA1 BOGOTA3 (config-if)# clock rate 64000 BOGOTA3(config-if)# no shutdown BOGOTA3(config-if)# interface serial0/0/1 BOGOTA3(config-if)# ip address 172.29.3.2 255.255.255.252 BOGOTA3(config-if)# description connection to BOGOTA1 BOGOTA3 (config-if)# clock rate 64000 BOGOTA3(config-if)# no shutdown BOGOTA3(config-if)# interface serial0/1/0 BOGOTA3(config-if)# ip address 172.29.3.13 255.255.255.252 BOGOTA3(config-if)# description connection to BOGOTA2 BOGOTA3 (config-if)# clock rate 64000 BOGOTA3(config-if)# no shutdown BOGOTA3(config)# interface g0/0 BOGOTA3(config-if)# ip address 172.29.0.1 255.255.255.0 BOGOTA3(config-if)# description connect to 150Host_PC1 BOGOTA3(config-if)# no shutdown

4.3.7 CONFIGURACIÓN INICIAL Y RUTINA DE DIAGNOSTICO ISP

Tabla 29. Configuración router ISP

Descripción del comando	**Comandos**
Realizar las rutinas de diagnóstico y	Router>enable Router#configure terminal

dejar los equipos listos para su configuración (asignar nombres de equipos, asignar claves de seguridad, etc)	Router(config)# hostname ISP ISP(config)# no ip domain-lookup 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 ISP(config-line)# login ISP(config-line)# exit ISP(config)# banner motd %Se prohibe el acceso no autorizado!% ISP(config)# exit
Configuración de interfaces	ISP(config)# interface serial0/0/0 ISP(config-if)# ip address 209.17.220.2 255.255.255.252 ISP(config-if)# description connect to MEDELLIN1 ISP(config-if)# clock rate 64000 This command applies only to DCE interfaces ISP(config-if)# no shutdown ISP(config-if)# interface serial0/0/1 ISP(config-if)# ip address 209.17.220.6 255.255.255.252 ISP(config-if)# description connect to BOGOTA1 ISP(config-if)# clock rate 64000 ISP(config-if)# no shutdown

4.4 TABLA DE DIRECCIONAMIENTO SEGÚN TOPOLOGÍA

En la siguiente tabla es posible apreciar la dirección IP asignada a la interfaz de cada dispositivo, el enlace realizado entre dispositivos y la masca de subred para cada uno de estos.

Tabla 30 Tabla de direccionamiento según topología

Dispositivo	Interfaz	Dirección IP	Máscara Subred
Bogota1 a Bogota3	Se0/0/1	172.29.3.5	255.255.255.252
Bogota1 a Bogota3	Se0/1/0	172.29.3.1	255.255.255.252
Bogota1 a Bogota2	Se0/1/1	172.29.3.9	255.255.255.252
Bogota1 a ISP	Se0/0/0	209.17.220.5	255.255.255.252
Bogota3 a Bogota1	Se0/0/0	172.29.3.6	255.255.255.252
Bogota3 a Bogota1	Se0/0/1	172.29.3.2	255.255.255.252
Bogota3 a Bogota2	Se0/1/0	172.29.3.13	255.255.255.252
Bogota3 a 150Hosts	G0/0	172.29.0.1	255.255.255.0
Bogota2 a Bogota1	Se0/0/0	172.29.3.10	255.255.255.252
Bogota2 a Bogota3	Se0/0/1	172.29.3.14	255.255.255.252
Bogota2 a 200Hosts	G0/0	172.29.1.1	255.255.255.0
Medellin1 a Medellin3	Se0/0/1	172.29.6.10	255.255.255.252
Medellin1 a Medellin3	Se0/1/1	172.29.6.13	255.255.255.252
Medellin1 a Medellin2	Se0/0/0	172.29.6.2	255.255.255.252
Medellin1 a ISP	Se0/1/0	209.17.220.1	255.255.255.252
Medellin3 a Medellin1	Se0/0/1	172.29.6.9	255.255.255.252
Medellin3 a Medellin1	Se0/1/0	172.29.6.14	255.255.255.252
Medellin3 a Medellin2	Se0/0/0	172.29.6.5	255.255.255.252
Medellin3 a 40Host	G0/0	172.29.4.129	255.255.255.128
Medellin2 a Medellin1	Se0/0/0	172.29.6.1	255.255.255.252
Medellin2 a Medellin3	Se0/0/1	172.29.6.6	255.255.255.252
Medellin2 a 50Host	G0/0	172.29.4.1	255.255.255.128
ISP a Medellin1	Se0/0/0	209.17.220.2	255.255.255.252
ISP a Bogota1	Se0/0/1	209.17.220.6	255.255.255.252

4.5 CONFIGURACIÓN DEL ENRUTAMIENTO

El protocolo de enrutamiento dinámico aplicado en este escenario es OSPF, a continuación se muestra el detalle de configuración realizado en cada router y posteriormente se valida dicha configuración mostrando las rutas aprendidas por medio de la aplicación de este protocolo.

Tabla 31 Procedimiento de configuración del enrutamiento.

Procedimiento	Comandos
a. Configurar el enrutamiento en la red usando el protocolo OSPF versión 2, declare la red principal, desactive la sumarización automática.	BOGOTA1>enable Password: BOGOTA1#configure terminal BOGOTA1(config)# router ospf 1 BOGOTA1(config-router)# router-id 1.1.1.1 BOGOTA1(config-router)# network 172.29.3.0 0.0.0.255 area 0 BOGOTA1(config-router)# network 209.17.220.0 0.0.0.255 area 0 BOGOTA2(config)# router ospf 1 BOGOTA2(config-router)# router-id 2.2.2.2 BOGOTA2(config-router)# network 172.29.0.0 0.0.255.255 area 0 BOGOTA3(config)# router ospf 1 BOGOTA3(config-router)# router-id 3.3.3.3 BOGOTA3(config-router)# network 172.29.0.0 0.0.255.255 area 0 MDELLIN1(config)# router ospf 1 MDELLIN1(config-router)# router-id 1.1.1.1 MDELLIN1(config-router)# network 172.29.6.0 0.0.0.255 area 0 MDELLIN1(config-router)# network 209.17.220.0 0.0.0.255 area 0

	MEDELLIN2(config)# router ospf 1 MEDELLIN2(config-router)# router-id 2.2.2.2 MEDELLIN2(config-router)# network 172.29.0.0 0.0.255.255 area 0 MEDELLIN3(config)# router ospf 1 MEDELLIN3(config-router)# router-id 3.3.3.3 MEDELLIN3(config-router)# network 172.29.0.0 0.0.255.255 area 0
b. Los routers Bogota1 y Medellín1 deberán añadir a su configuración de enrutamiento una ruta por defecto hacia el ISP y, a su vez, redistribuirla dentro de las publicaciones de OSPF.	BOGOTA1>enable Password: BOGOTA1#configure terminal BOGOTA1(config)# ip route 0.0.0.0 0.0.0.0 209.17.220.6 BOGOTA1(config)# router ospf 1 BOGOTA1(config-router)# router-id 1.1.1.1 BOGOTA1(config-router)#default-information originate MEDELLIN1>enable Password: MEDELLIN1#configure terminal MEDELLIN1(config)# ip route 0.0.0.0 0.0.0.0 209.17.220.2 MEDELLIN1(config)# router ospf 1 MEDELLIN1(config-router)# router-id 1.1.1.1 MEDELLIN 1(config-router)#default-information originate
c. El router ISP deberá tener una ruta estática dirigida hacia cada red interna de Bogotá y Medellín para el caso se sumariza las subredes de cada uno a /22.	ISP (config) # ip route 209.17.0.0 255.255.252.0 serial 0/0/0 ISP (config) # ip route 209.17.0.0 255.255.252.0 serial 0/0/1

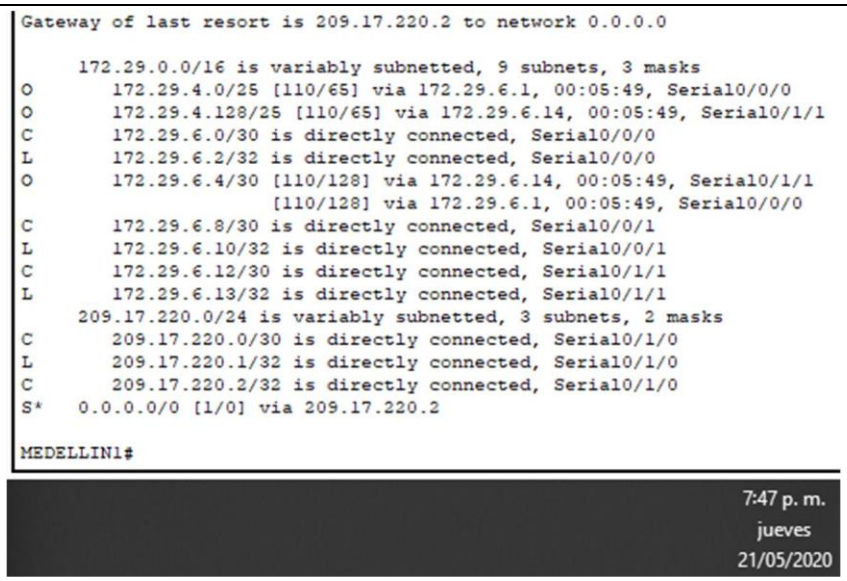
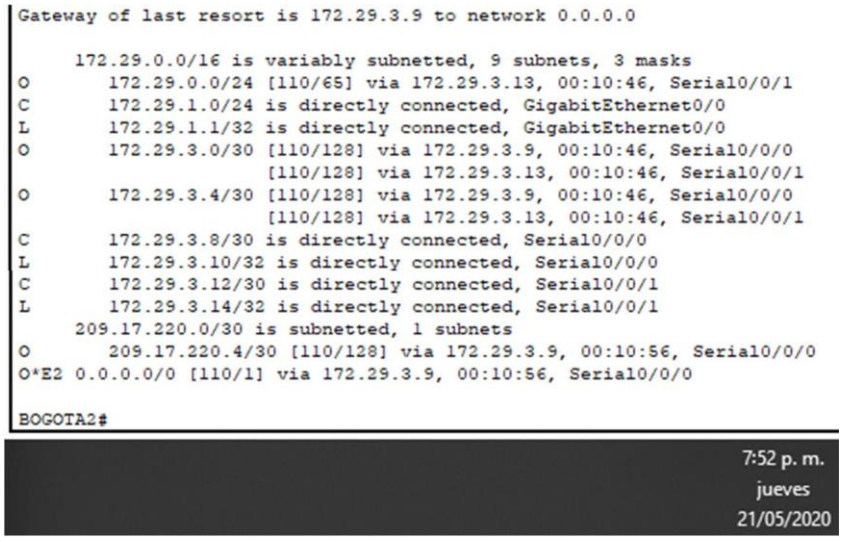
4.6 TABLA DE ENRUTAMIENTO

En el procedimiento detallado a continuación, se verifica en las tablas de enrutamiento el protocolo OSPF en cada router, redes aprendidas, rutas, balanceo de cargas, redundancia de rutas y rutas por defecto en cada router. Se muestra también las similitudes entre *routers* que tienen funciones similares en cada lado de la topología.

Tabla 32 Procedimiento de verificación de enrutamiento y balanceo en cada dispositivo.

Procedimiento	**Resultados obtenidos en cada dispositivos**

a. Verificar la tabla de enrutamiento en cada uno de los routers para comprobar las redes y sus rutas.
 	
b. Verificar el balanceo de carga que presentan los routers.
 	
c. Obsérvese en los routers Bogotá1 y Medellín1 cierta similitud por su ubicación, por tener dos enlaces de conexión hacia otro router y
	Bogotá1
	Figura 26. Resultado del comando show ip route en Bogotá 1.
	
	`Gateway of last resort is 209.17.220.6 to network 0.0.0.0`
	
	`     172.29.0.0/16 is variably subnetted, 9 subnets, 3 masks`
	`O       172.29.0.0/24 [110/65] via 172.29.3.2, 00:00:55, Serial0/1/0`
	`O       172.29.1.0/24 [110/65] via 172.29.3.10, 00:00:55, Serial0/1/1`
	`C       172.29.3.0/30 is directly connected, Serial0/1/0`
	`L       172.29.3.1/32 is directly connected, Serial0/1/0`
	`C       172.29.3.4/30 is directly connected, Serial0/0/1`
	`L       172.29.3.5/32 is directly connected, Serial0/0/1`
	`C       172.29.3.8/30 is directly connected, Serial0/1/1`
	`L       172.29.3.9/32 is directly connected, Serial0/1/1`
	`O       172.29.3.12/30 [110/128] via 172.29.3.2, 00:00:55, Serial0/1/0`
	`                      [110/128] via 172.29.3.10, 00:00:55, Serial0/1/1`
	`     209.17.220.0/24 is variably subnetted, 3 subnets, 2 masks`
	`C       209.17.220.4/30 is directly connected, Serial0/0/0`
	`L       209.17.220.5/32 is directly connected, Serial0/0/0`
	`C       209.17.220.6/32 is directly connected, Serial0/0/0`
	`S*   0.0.0.0/0 [1/0] via 209.17.220.6`
	
	`BOGOTA1#`
	
	7:43 p. m.
	jueves
	21/05/2020
	
	Medellín1
	Figura 27. Resultado del comando show ip route en Medellín 1.

por la ruta por defecto que manejan.	
d. Los routers Medellín2 y Bogotá2 también presentan redes conectadas directamente y recibidas mediante OSPF. e. Las tablas de los routers restantes deben permitir visualizar rutas redundantes para el caso de la ruta por defecto.	**Bogotá2** Figura 28. Resultado del comando show ip route en Bogotá 2.  **Medellín2** Figura 29. Resultado del comando show ip route en Medellín 2.

	Gateway of last resort is 172.29.6.2 to network 0.0.0.0 172.29.0.0/16 is variably subnetted, 9 subnets, 3 masks C 172.29.4.0/25 is directly connected, GigabitEthernet0/0 L 172.29.4.1/32 is directly connected, GigabitEthernet0/0 O 172.29.4.128/25 [110/65] via 172.29.6.5, 00:12:54, Serial0/0/1 C 172.29.6.0/30 is directly connected, Serial0/0/0 L 172.29.6.1/32 is directly connected, Serial0/0/0 C 172.29.6.4/30 is directly connected, Serial0/0/1 L 172.29.6.6/32 is directly connected, Serial0/0/1 O 172.29.6.8/30 [110/128] via 172.29.6.2, 00:12:54, Serial0/0/0 [110/128] via 172.29.6.5, 00:12:54, Serial0/0/1 O 172.29.6.12/30 [110/128] via 172.29.6.2, 00:12:54, Serial0/0/0 [110/128] via 172.29.6.5, 00:12:54, Serial0/0/1 O*E2 0.0.0.0/0 [110/1] via 172.29.6.2, 00:12:54, Serial0/0/0 MEDELLIN2# 7:55 p. m. jueves 21/05/2020
f. El router ISP solo debe indicar sus rutas estáticas adicionales a las directamente conectadas.	**ISP** Figura 30. Resultado del comando show ip route en ISP. Gateway of last resort is not set 172.29.0.0/30 is subnetted, 3 subnets S 172.29.3.0/30 is directly connected, Serial0/0/1 S 172.29.3.4/30 is directly connected, Serial0/0/1 S 172.29.3.8/30 is directly connected, Serial0/0/1 209.17.220.0/24 is variably subnetted, 4 subnets, 2 masks C 209.17.220.1/32 is directly connected, Serial0/0/0 C 209.17.220.4/30 is directly connected, Serial0/0/1 C 209.17.220.5/32 is directly connected, Serial0/0/1 L 209.17.220.6/32 is directly connected, Serial0/0/1 ISP# 7:56 p. m. jueves 21/05/2020

4.7 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. Se detalla el procedimiento realizado para configurar las interfaces pasivas en cada *router.*

Tabla 33 Procedimiento para deshabilitar la propagación del protocolo OSPF

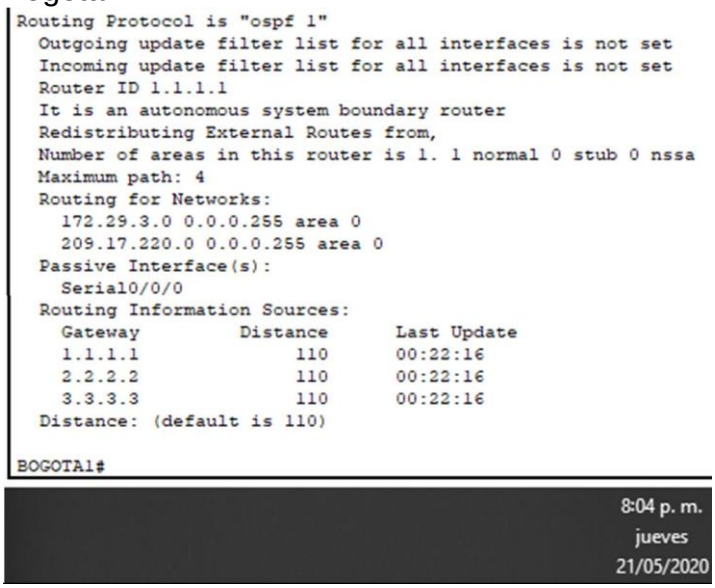
Router	Interfaz
Bogota1	SERIAL0/0/1; SERIAL0/1/0; SERIAL0/1/1 BOGOTA1>enable BOGOTA1# configure terminal BOGOTA1(config)# router ospf 1 BOGOTA1(config-router)# passive-interface serial0/0/0 BOGOTA1(config-router)# end
Bogota2	SERIAL0/0/0; SERIAL0/0/1 BOGOTA2>enable Password: BOGOTA2# configure terminal BOGOTA2(config)# router ospf 1 BOGOTA2(config-router)# passive-interface g0/0 BOGOTA2(config-router)# end
Bogota3	SERIAL0/0/0; SERIAL0/0/1; SERIAL0/1/0 BOGOTA3>enable BOGOTA3#configure terminal BOGOTA3(config)# router ospf 1 BOGOTA3(config-router)# passive-interface g0/0 BOGOTA3(config-router)# end
Medellín1	SERIAL0/0/0; SERIAL0/0/1; SERIAL0/1/1 MEDELLIN1>enable MEDELLIN1# configure terminal

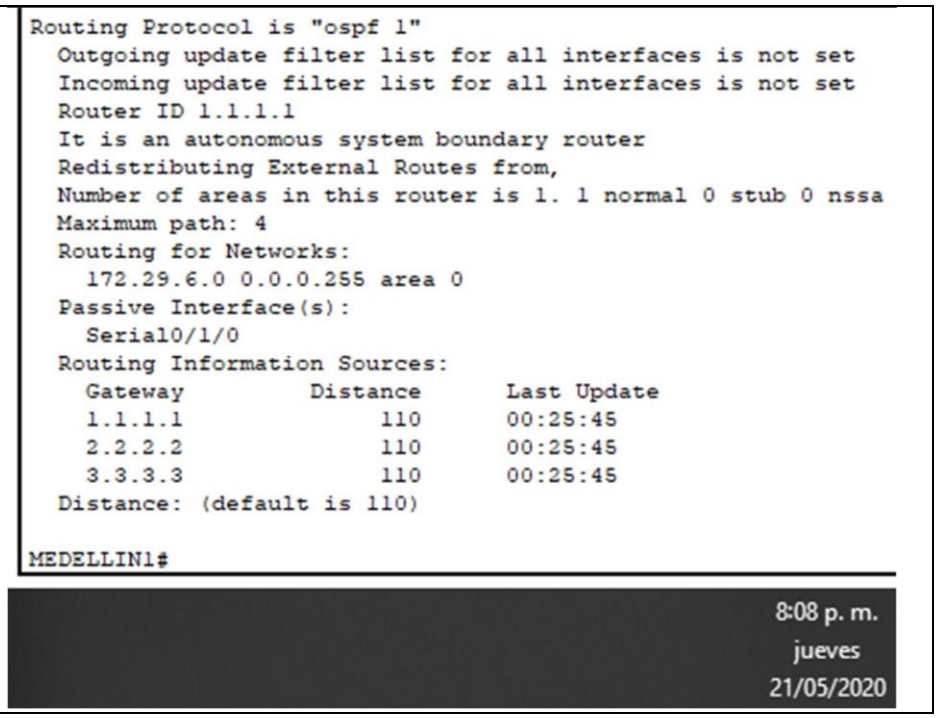
	MEDELLIN1(config)# router ospf 1 MEDELLIN1(config-router)# passive-interface serial0/1/0 MEDELLIN1(config-router)# end
Medellín2	SERIAL0/0/0; SERIAL0/0/1 MEDELLIN2>enable MEDELLIN2# configure terminal MEDELLIN2(config)# router ospf 1 MEDELLIN2(config-router)# passive-interface g0/0 MEDELLIN2(config-router)# end
Medellín3	SERIAL0/0/0; SERIAL0/0/1; SERIAL0/1/0 MEDELLIN3>enable MEDELLIN3# configure terminal MEDELLIN3(config)# router ospf 1 MEDELLIN3(config-router)# passive-interface g0/0 MEDELLIN3(config-router)# end
ISP	No lo requiere

4.8 VERIFICACIÓN DEL PROTOCOLO OSPF

a. A continuación se verifica y documenta las opciones de enrutamiento configuradas en los routers, como las interfaces pasivas para la conexión hacia el ISP, la versión de OSPF y las interfaces que participan de la publicación entre otros datos.

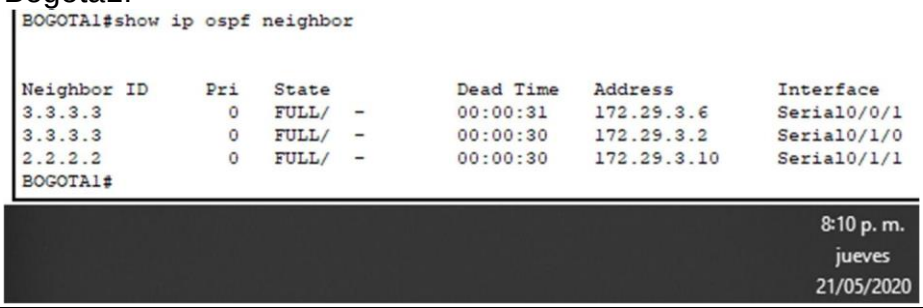
Tabla 34 Procedimiento para verificar el protocolo OSPF

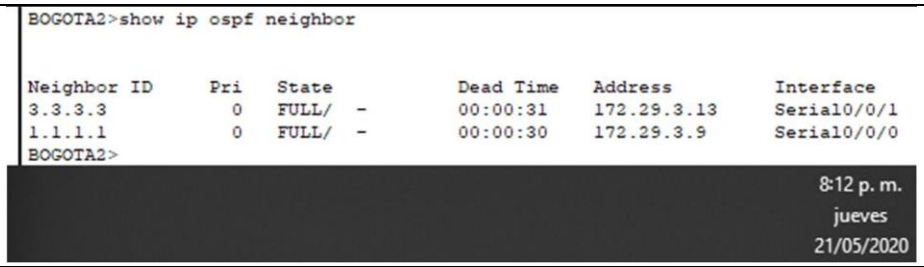
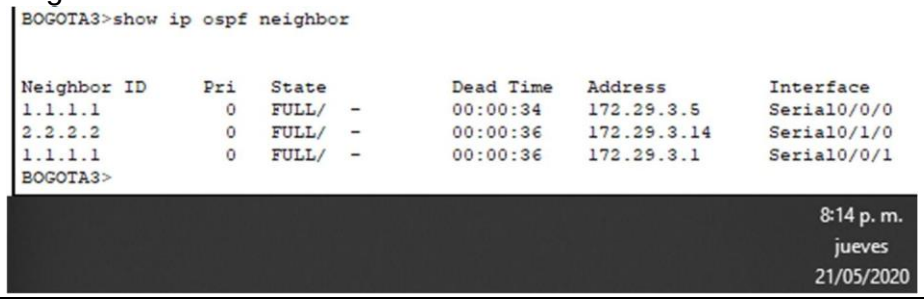
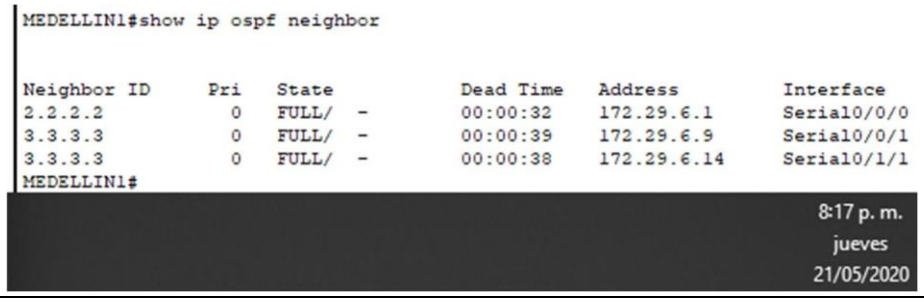
Router	Documentacion ospf
Bogota1	BOGOTA1#show ip protocols Figura 31. Resultado del comando show ip protocols en Bogotá1. 
Medellin1	MEDELLIN1# show ip protocols Figura 32. Resultado del comando show ip protocols en Medellín1.

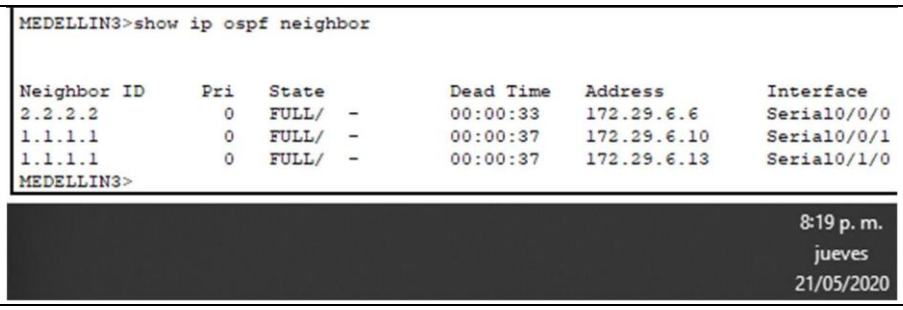
	

b. Por medio de comandos de monitoreo es posible verificar y documentar la base de datos de OSPF de cada router, donde se informa de manera detallada todas las rutas hacia cada red. Este procedimiento es aplicado en cada router para validar la configuración realizada.

Tabla 35 Procedimiento para verificar el protocolo OSPF en cada router

Router	Rutas hacia cada red
Bogota1	BOGOTA1# show ip ospf neighbor Figura 33. Resultado del comando show ip ospf neighbor en Bogotá1. 
Bogota2	BOGOTA2# show ip ospf neighbor Figura 34. Resultado del comando show ip ospf neighbor en Bogotá2.

	
Bogota3	BOGOTA3# show ip ospf neighbor Figura 35. Resultado del comando show ip ospf neighbor en Bogotá3. 
Medellín1	MEDELLIN1# show ip ospf neighbor Figura 36. Resultado del comando show ip ospf neighbor en Medellin1. 
Medellín2	MEDELLIN2#show ip ospf neighbor Figura 37. Resultado del comando show ip ospf neighbor en Medellin2. 
Medellín3	MEDELLIN3# show ip ospf neighbor Figura 38. Resultado del comando show ip ospf neighbor en Medellin3.

```
MEDELLIN3>show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
2.2.2.2           0   FULL/  -        00:00:33    172.29.6.6      Serial0/0/0
1.1.1.1           0   FULL/  -        00:00:37    172.29.6.10     Serial0/0/1
1.1.1.1           0   FULL/  -        00:00:37    172.29.6.13     Serial0/1/0
MEDELLIN3>
```

8:19 p. m.
jueves
21/05/2020

4.9 CONFIGURAR ENCAPSULAMIENTO Y AUTENTICACIÓN PPP

Para mejorar aspectos de seguridad en la red se realiza el procedimiento de configuración de dos protocolos de autenticación PAP y CHAP, con esto es posible que el router ISP pueda validar los *routers* clientes Medellín 1 y Bogotá 1. La autenticación para el router de Medellín 1 es PAP y la autenticación para el router de Bogotá 1 es CHAP.

Tabla 36 Procedimiento para configurar el encapsulamiento y autenticación ppp

Procedimiento	**Comandos**
a. Según la topología se requiere que el enlace Medellín1 con ISP sea configurado con autenticación PAP.	ISP#configure terminal ISP(config)# username MEDELLIN1 password MEDELLIN1 ISP(config)# interface serial 0/0/0 ISP(config-if)# encapsulation ppp ISP(config-if)# ppp authentication pap MEDELLIN1#configure terminal MEDELLIN1(config)# interface serial 0/1/0 MEDELLIN1(config-if)# encapsulation ppp MEDELLIN1(config-if)# ppp pap sent-username MEDELLIN1 password MEDELLIN1(config-if)# end
b. El enlace Bogotá1 con ISP se debe configurar con autenticación CHAP.	ISP>enable ISP# configure terminal ISP(config)#Username BOGOTA1 password BOGOTA1 ISP(config)#interface serial0/0/1 ISP(config-if)# encapsulation ppp ISP(config-if)# ppp authentication chap ISP(config-if)# end BOGOTA1> enable BOGOTA1# configure terminal BOGOTA1(config)# username ISP password BOGOTA1

	BOGOTA1(config)# interface s0/0/0 BOGOTA1(config-if)# encapsulation ppp BOGOTA1(config-if)# ppp authentication chap BOGOTA1(config-if)# end

4.10 CONFIGURACION DE PAT

La configuración de NAT en los routers de Bogotá 1 y Medellín 1 permite la traducción de direcciones pero también hará que solo exista comunicación hasta el *router* ISP, a continuación se muestra el proceso de configuración y verificación de NAT en los *routers* mencionados.

Tabla 37 Procedimiento para configurar pat

Procedimiento	**Comandos**
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	MEDELLIN1>enable Password: MEDELLIN1# configure terminal MEDELLIN1(config)# ip nat inside source list 1 interface s0/1/0 overload MEDELLIN1(config)# access-list 1 permit 172.29.0.0 0.0.255.255 MEDELLIN1(config)# interface serial0/1/0 MEDELLIN1(config-if)# ip nat outside MEDELLIN1(config-if)# interface serial0/1/1 MEDELLIN1(config-if)# ip nat inside MEDELLIN1(config-if)# interface serial0/0/1 MEDELLIN1(config-if)# ip nat inside MEDELLIN1(config-if)# interface serial0/0/0 MEDELLIN1(config-if)# ip nat inside MEDELLIN1(config-if)# end MEDELLIN1# show ip nat translations Pro Inside global Inside local Outside local Outside global icmp 209.17.220.1:1 172.29.6.1:1 209.17.220.6:1 209.17.220.6:1 icmp 209.17.220.1:2 172.29.6.1:2 209.17.220.6:2 209.17.220.6:2 icmp 209.17.220.1:3 172.29.6.1:3 209.17.220.6:3 209.17.220.6:3 icmp 209.17.220.1:4 172.29.6.1:4 209.17.220.6:4

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.	209.17.220.6:4 icmp 209.17.220.1:5 172.29.6.1:5 209.17.220.6:5 209.17.220.6:5
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.	BOGOTA1# configure terminal BOGOTA1(config)# ip nat inside source list 1 interface s0/0/0 overload BOGOTA1(config)# access-list 1 permit 172.29.0.0 0.0.3.255 BOGOTA1(config)# interface serial0/0/0 BOGOTA1(config-if)# ip nat outside BOGOTA1(config-if)# interface serial0/1/1 BOGOTA1(config-if)# ip nat inside BOGOTA1(config-if)# interface serial0/1/0 BOGOTA1(config-if)# ip nat inside BOGOTA1(config-if)# interface serial0/0/1 BOGOTA1(config-if)# end BOGOTA1# show ip nat translations Pro Inside global Inside local Outside local Outside global icmp 209.17.220.5:10 172.29.3.2:10 209.17.220.6:10 209.17.220.6:10 icmp 209.17.220.5:6 172.29.3.2:6 209.17.220.6:6 209.17.220.6:6 icmp 209.17.220.5:7 172.29.3.2:7 209.17.220.6:7 209.17.220.6:7 icmp 209.17.220.5:8 172.29.3.2:8 209.17.220.6:8 209.17.220.6:8 icmp 209.17.220.5:9 172.29.3.2:9 209.17.220.6:9 209.17.220.6:9

4.11 CONFIGURACION DEL SERVICIO DHCP

El protocolo DHCP se utiliza principalmente para asignar de forma dinámica direcciones IP, en el proceso que se describe a continuación se configura un servidor DHCP en Medellín 2 y Bogotá 2 mientras que Medellín 3 y Bogotá 3 permitirán el paso de mensajes broadcast para que se asigne la dirección a las redes que estos routers tienen conectadas.

Tabla 38 Procedimiento para configurar el servicio DHCP

Procedimiento	**Comandos**
a. Configurar la red Medellín2 y Medellín3 donde el router Medellín 2 debe ser el servidor DHCP para ambas redes Lan.	MEDELLIN2>enable Password: MEDELLIN2# configure terminal MEDELLIN2(config)# ip dhcp excluded-address 172.29.4.1 172.29.4.7 MEDELLIN2(config)# ip dhcp excluded-address 172.29.4.129 172.29.4.136 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(config)# ip dhcp pool MEDELLIN3 MEDELLIN2(dhcp-config)# network 172.26.4.128 255.255.255.128 MEDELLIN2(dhcp-config)# default-router 172.29.4.129 MEDELLIN2(dhcp-config)# dns-server 10.10.10.10 MEDELLIN2(dhcp-config)# exit
b. El router Medellín3 deberá habilitar el paso de los mensajes broadcast hacia la IP del router Medellín2.	MEDELLIN3>enable Password: MEDELLIN3# configure terminal MEDELLIN3(config)# interface g0/0 MEDELLIN3(config-if)# ip helper-address 172.29.6.6 MEDELLIN3(config-if)# exit

c. Configurar la red Bogotá2 y Bogotá3 donde el router Bogotá2 debe ser el servidor DHCP para ambas redes Lan.	BOGOTA2> enable Password: BOGOTA2# configure terminal BOGOTA2(config)# ip dhcp excluded-address 172.29.1.1 172.29.1.7 BOGOTA2(config)# ip dhcp pool BOGOTA2 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 BOGOTA2(dhcp-config)# exit BOGOTA2# configure terminal BOGOTA2(config)# ip dhcp excluded-address 172.29.0.1 172.29.0.7 BOGOTA2(config)# ip dhcp pool BOGOTA3 BOGOTA2(dhcp-config)# network 172.29.0.0 255.255.255.0 BOGOTA2(dhcp-config)# default-router 172.29.0.1 BOGOTA2(dhcp-config)# dns-server 10.10.10.10 BOGOTA2(dhcp-config)# exit
d. Configure el router Bogotá3 para que habilite el paso de los mensajes Broadcast hacia la IP del router Bogotá2.	BOGOTA3>enable Password: BOGOTA3# configure terminal Enter configuration commands, one per line. End with CNTL/Z. BOGOTA3(config)# interface g0/0 BOGOTA3(config-if)# ip helper-address 172.29.3.14 BOGOTA3(config-if)# exit

CONCLUSIONES

Por medio de la implementación metódica de los comandos involucrados en los procesos de configuración de los diferentes dispositivos y aplicando los criterios aprendidos sobre cada uno de los conceptos de enrutamiento, seguridad, listas de acceso y servicios de red, fue posible lograr la conectividad más los servicios de red solicitados en cada uno de los escenarios propuestos.

Con los escenarios desarrollados se puede evidenciar las destrezas obtenidas y la aplicación de conceptos al lograr los objetivos de implementación solicitados, tal como los protocolos de enrutamiento OSPF, RIP, listas de accesos y conectividad tanto en IPv4 como IPv6, además de la adaptación de estos mismos a las necesidades expuestas que reflejan sus requerimientos particulares en cada aplicación.

De acuerdo con los resultados y procedimientos demostrados en las pruebas de comunicación y tablas de enrutamiento, fue posible implementar exitosamente los protocolos y servicios de red solicitados.

BIBLIOGRAFÍA

CISCO. DHCP. Principios de Enrutamiento y Conmutación. {en línea}. {5 abril de 2020} disponible en: https://static-course-assets.s3.amazonaws.com/RSE50ES/module10/index.html#10.0.1.1

CISCO. “Enrutamiento Dinámico. Principios de Enrutamiento y Conmutación”. {en línea}. {6 mayo de 2020} disponible en: https://static-courseassets.s3.amazonaws.com/RSE50ES/module7/index.html#7.0.1.1

CISCO. Listas de control de acceso. Principios de Enrutamiento y Conmutación. {en línea}. {18 abril de 2020} disponible en: https://static-course-assets.s3.amazonaws.com/RSE50ES/module9/index.html#9.0.1.1

CISCO. OSPF de una sola área. Principios de Enrutamiento y Conmutación. {en línea}. {29 abril de 2020} disponible en: https://static-course-assets.s3.amazonaws.com/RSE50ES/module8/index.html#8.0.1.1

CISCO. Traducción de direcciones IP para IPv4. Principios de Enrutamiento y Conmutación. {en línea}. {19 marzo de 2020} disponible en: https://static-course-assets.s3.amazonaws.com/RSE50ES/module11/index.html#11.0.1.1

WENDELL. Odom, CCNA Routing and Switching ICND 200-15 Official Cert Guide, Indianapolis, IN 46240 USA, Pearson Education Inc, 2016, 1452