

**Solución De Dos Escenarios Presentes En Entornos Corporativos Bajo El
Uso De Tecnología Cisco**

CESAR AUGUSTO PICHICA SONS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
INGENIERÍA DE SISTEMAS
LA PLATA HUILA
2020

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

CESAR AUGUSTO PICHICA SONS

GUSTAVO ADOLFO RODRIGUEZ
Tutor

**DIPLOMADO DE PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN
DE SOLUCIONES INTEGRADAS LAN / WAN)**

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
INGENIERÍA DE SISTEMAS
LA PLATA HUILA
2020

Nota de aceptación

Firma del presidente del jurado

Firma del jurado

Firma del jurado

La Plata Huila, 10 de julio de 2020

Resumen

Con el desarrollo de esta actividad se busca identificar el nivel de desarrollo competitivo y habilidades obtenidas a lo largo del diplomado de profundización cisco, en el cual como estudiante disponemos de dos escenarios propuestos que abarca las temáticas de todas las unidades del curso.

Abstract

With the development of this activity, we seek to identify the level of competitive development and skills obtained throughout the Cisco in-depth course, in which as a student we have two proposed scenarios that cover the themes of all the units of the course.

Contenido

LISTA DE FIGURAS	8
LISTA DE TABLAS	9
INTRODUCCIÓN	10
OBJETIVOS.....	11
Objetivo General.....	11
Objetivo Especifico	11
ESCENARIO 1	12
Parte 1: Inicializar dispositivos.....	13
Paso 1: Inicializar y volver a cargar los routers y los switches	13
Parte 2: Configurar los parámetros básicos de los dispositivos.....	13
Paso 1: Configurar la computadora de Internet.....	13
Paso 2: Configurar R1.....	14
Paso 3: Configurar R2.....	15
Paso 4: Configurar R3.....	16
Paso 5: Configurar S1.....	17
Paso 6: Configurar el S3.....	18
Paso 7: Verificar la conectividad de la red	18
Parte 3: Configurar la seguridad del switch, las VLAN y el routing entre VLAN 20	
Paso 1: Configurar S1	20
Paso 2: Configurar el S3	21
Paso 3: Configurar R1.....	22
Paso 4: Verificar la conectividad de la red	23
Parte 4: Configurar el protocolo de routing dinámico RIPv2	25
Paso 1: Configurar RIPv2 en el R1	25
Paso 2: Configurar RIPv2 en el R2	26
Paso 3: Configurar RIPv2 en el R3.....	26
Paso 4: Verificar la información de RIP.....	27
Parte 5: Implementar DHCP y NAT para IPv4	28
Paso 1: Configurar el R1 como servidor de DHCP para las VLAN 21 y 23..	28
Paso 2: Configurar la NAT estática y dinámica en el R2.....	29

Paso 3: Verificar el protocolo DHCP y la NAT estática	29
Parte 6: Configurar NTP	32
Parte 7: Configurar y verificar las listas de control de acceso (ACL)	33
Paso 1: Restringir el acceso a las líneas VTY en el R2	33
Paso 2: Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente	35
ESCENARIO 2.....	37
Desarrollo	37
Configuración de direccionamiento en routers	40
Parte 1: Configuración del enrutamiento	42
Parte 2: Tabla de Enrutamiento.....	45
Parte 3: Deshabilitar la propagación del protocolo OSPF.....	49
Parte 4: Verificación del protocolo OSPF.	50
Parte 5: Configurar encapsulamiento y autenticación PPP.	51
Parte 6: Configuración de PAT.....	52
Parte 7: Configuración del servicio DHCP.....	54
CONCLUSIÓN	56
REFERENCIAS BIBLIOGRAFICAS.....	57

LISTA DE FIGURAS

Figura 1 Topología.....	12
Figura 2 Ping de R1 a R2	19
Figura 3 Ping de R2 a R3	19
Figura 4 Ping de PC de internet a Gateway predeterminado.....	20
Figura 5 Ping de S1 a R1, dirección VLAN 99	23
Figura 6 Ping de S3 a R1, dirección VLAN 99	24
Figura 7 Ping de S1 a R1, dirección VLAN 21	24
Figura 8 Ping de S3 a R1, dirección VLAN 23	25
Figura 9 show ip protocols	27
Figura 10 show ip route rip	27
Figura 11 show ip route	28
Figura 12 Verificación que PC-A tome IP del servidor de DHCP	30
Figura 13 Verificación que PC-C tome IP del servidor de DHCP	31
Figura 14 Ping de PC-A a PC-C	31
Figura 15 Acceso al servidor web (209.165.200.229).....	32
Figura 16 Configuración de NTP en R1	33
Figura 17 Ingreso a R1 mediante Telnet.....	34
Figura 18 Acceso rechazado desde el R3 por Telnet	34
Figura 19 show access-list.....	35
Figura 20 Show ip nat translations.....	36
Figura 21 Clear ip nat translation	36
Figura 22 Topología de red escenario 2	37
Figura 23 Topología de red realizada en PKT	38
Figura 24 Verificación por comando show ip route conexión con ISP	44
Figura 25 Verificación conectividad entre Medellín y Bogotá.....	45
Figura 26 Verificación de enrutamiento router Bogota2.....	45
Figura 27 Verificación de enrutamiento router Bogota3.....	46
Figura 28 Verificación de balanceo de carga en router Meedelin3	46
Figura 29 Verificación doble enlace router bogota1	47
Figura 30 Verificación doble enlace router Medellin1	47
Figura 31 Redes conectadas directamente y recibidas mediante OSPF	48
Figura 32 redes conectadas directamente y recibidas mediante OSPF	48
Figura 33 Rutas conectadas directamente ISP	49
Figura 34 Verificación del protocolo OSPF en ruter Bogota1 y Medellin1	50
Figura 35 BOGOTA3 show ip ospf interface.....	51
Figura 36 Ping desde Medellin1 a las direcciones de las interfaces	53
Figura 37 PC1_MED y PC2_MED dirección ip a través de DHCP	54
Figura 38 PC1_BOG y PC2_BOG dirección ip a través de DHCP	55

LISTA DE TABLAS

Tabla 1 Inicializar dispositivos.....	13
Tabla 2 Parámetros básicos de los dispositivos	13
Tabla 3 Configuración R1	14
Tabla 4 Configuración R2	15
Tabla 5 Configuración R3	16
Tabla 6 Configuración S1	17
Tabla 7 Configuración S3	18
Tabla 8 Verificación conectividad de la red.....	18
Tabla 9 Configuración de VLAN en S1	20
Tabla 10 Configuración de S3.....	21
Tabla 11 Configuración de R1	22
Tabla 12 Verificación de conectividad.....	23
Tabla 13 Configuración de RIPv2 en el R1	25
Tabla 14 Configuración de RIPv2 en el R2.....	26
Tabla 15 Configuración RIPv2 en el R3.....	26
Tabla 16 Verificación de la información de RIP	27
Tabla 17 Configuración de R1 como servidor de DHCP para las VLAN 21 y 23 ...	28
Tabla 18 Configuración de NAT estática y dinámica en el R2	29
Tabla 19 Verificación el protocolo DHCP y la NAT estática	30
Tabla 20 Configuración NTP	32
Tabla 21 Configuración y verificación de las listas de control de acceso (ACL)	33
Tabla 22 Verificación mediante el comando de CLI.....	35
Tabla 23 Direccionamiento interfaz routers	39
Tabla 24 Deshabilitar la Propagación del Protocolo OSPF.....	49

INTRODUCCIÓN

Los ejercicios prácticos de la prueba de habilidades del diplomado de profundización CISCO, nos proveen el siguiente escenario en el cual nosotros debemos desarrollar, así experimentar todos los temas que hemos visto hasta el momento tanto en la plataforma cisco, como en las diferentes actividades y laboratorios que hemos realizado, lo cual contiene temas como, protocolos de routing dinámico (RIPv2), configuración de servers DHCP, Network Address Translation (NAT), Listas de control de acceso (ACL). Esto puede implementarse en routers para aumentar la seguridad de una red, implementar políticas de entrada y salida de paquetes de datos para ciertos equipos o host específicos.

OBJETIVOS

Objetivo General

Identificar el grado de desarrollo de competencias y habilidades que fueron adquiridas a lo largo del diplomado. Lo esencial es poner a prueba los niveles de comprensión y solución de problemas relacionados con diversos aspectos de Networking.

Objetivo Especifico

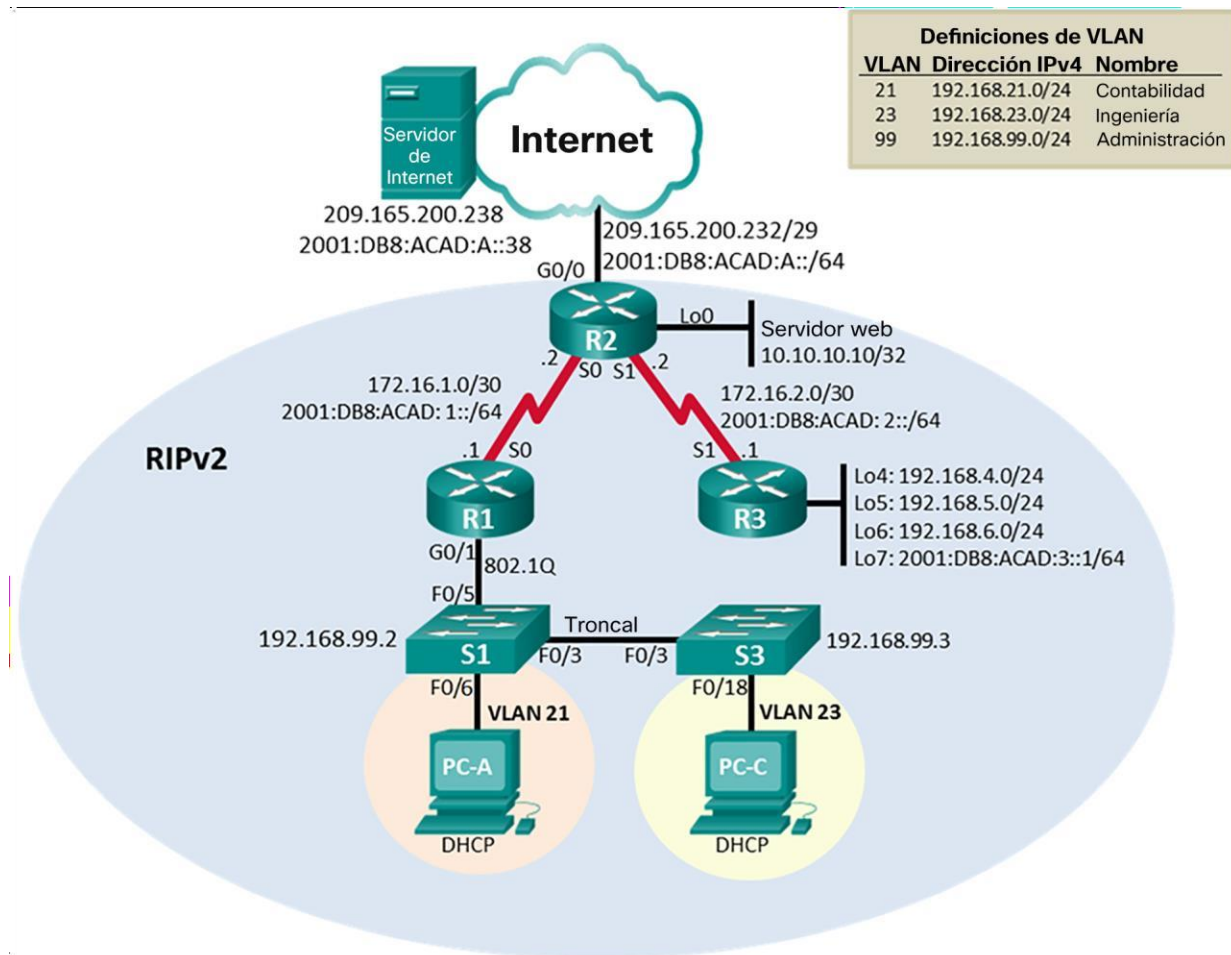
- Mediante Packet Tracer configurar una red pequeña para que admita conectividad IPV4 e IPV6, seguridad de switches, routing entre VLAN, el protocolo de routing dinámico RIPv2, el protocolo de configuración de hosts dinámicos (DHCP), la traducción de direcciones de red dinámicas y estáticas (NAT), listas de control de acceso (ACL) y el protocolo de tiempo de red (NTP) servidor/cliente
- Configurar e interconectar los dispositivos que se encuentran en dos ciudades utilizando el protocolo OSPF habilitar encapsulamiento PPP y su autenticación, proporcionar servicio DHCP en las LAN y habilitar NAT de sobrecarga

ESCENARIO 1

Con este escenario se evaluará lo practicado en las unidades 1 a 6 del diplomado de profundización.

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.

Figura 1 Topología



Parte 1: Inicializar dispositivos

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

Ejecutamos los siguientes comandos en los distintos routers y switches para cerciorarnos de que no haya rastros de configuraciones anteriores.

Tabla 1 Inicializar dispositivos

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

Parte 2: Configurar los parámetros básicos de los dispositivos

Paso 1: Configurar la computadora de Internet

Realizamos la configuración del servidor de Internet de acuerdo a la topología sugerida en el presente escenario.

Tabla 2 Parámetros básicos de los dispositivos

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.233
Dirección IPv6/subred	2001:DB8:ACAD:A::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:A::1

Paso 2: Configurar R1

Para la configuración del router R1 iniciamos con los parámetros que se consignan en la tabla a continuación y exceptuamos la configuración de la interfaz G0/1 por el momento.

Tabla 3 Configuración R1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R1
Contraseña de exec privilegiado cifrada	R1(config)#enable secret class
Contraseña de acceso a la consola	R1(config)#line console 0 R1(config-line)#password cisco R1(config-line)#login
Contraseña de acceso Telnet	R1(config-line)#line vty 0 15 R1(config-line)#password cisco R1(config-line)#login
Cifrar las contraseñas de texto no cifrado	R1(config-line)#service password-encryption
Mensaje MOTD	R1(config)#banner motd %se prohíbe el acceso no autorizado%
Interfaz S0/0/0	R1(config)#interface s0/0/0 R1(config-if)#description coneccion a R2 R1(config-if)#ip address 172.16.1.1 255.255.255.252 R1(config-if)#no shutdown R1(config-if)#ipv6 address 2001:db8:acad:1::1/64 R1(config-if)#clock rate 128000 R1(config-if)#no shutdown R1(config-if)#exit
Rutas predeterminadas	R1(config-if)#ip route 0.0.0.0 0.0.0.0 s0/0/0 R1(config-if)#ipv6 route ::/0 s0/0/0

Nota: Todavía no configure G0/1.

Paso 3: Configurar R2

En esta parte ya realizamos la configuración para internet y el loopback, configuramos los parámetros del router R2 consignados en la tabla a continuación.

Tabla 4 Configuración R2

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R2
Contraseña de exec privilegiado cifrada	R2(config)#enable secret class
Contraseña de acceso a la consola	R2(config)#line console 0 R2(config-line)#password cisco R2(config-line)#login
Contraseña de acceso Telnet	R2(config-line)#line vty 0 15 R2(config-line)#password cisco R2(config-line)#login
Cifrar las contraseñas de texto no cifrado	R2(config-line)#service password-encryption
Habilitar el servidor HTTP	R2(config)#ip http server
Mensaje MOTD	R2(config)#banner motd %se prohíbe el acceso no autorizado%
Interfaz S0/0/0	R2(config)#interface s0/0/0 R2(config-if)#description conexión a R1 R2(config-if)#ip address 172.16.1.2 255.255.255.252 R2(config-if)#ipv6 address 2001:db8:acad:1::2/64 R2(config-if)#no shutdown
Interfaz S0/0/1	R2(config-if)#interface s0/0/1 R2(config-if)#description Conexión a R3 R2(config-if)#ip address 172.16.2.2 255.255.255.252 R2(config-if)#ipv6 address 2001:db8:acad:2::1/64 R2(config-if)#clock rate 128000 R2(config-if)#no shutdown

Interfaz G0/0 (simulación de Internet)	R2(config-if)#interface g0/0 R2(config-if)#description conectado a servidor de internet R2(config-if)#ip address 209.165.200.233 255.255.255.248 R2(config-if)#ipv6 address 2001:db8:acad:a::1/64 R2(config-if)#no shutdown
Interfaz loopback 0 (servidor web simulado)	R2(config-if)#interface loopback 0 R2(config-if)#description servidor web simulado. R2(config-if)#ip address 10.10.10.10 255.255.255.255
Ruta predeterminada	R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0 R2(config)#ipv6 route ::/0 g0/0

Paso 4: Configurar R3

Al igual que en los otros routers se realiza la configuración del router R3 según los parámetros que se indican en la siguiente tabla aumentando en esta parte las interfaces loopback 4,5,6 y 7.

Tabla 5 Configuración R3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R3
Contraseña de exec privilegiado cifrada	R3(config)#enable secret class
Contraseña de acceso a la consola	R3(config)#line console 0 R3(config-line)#password cisco R3(config-line)#login
Contraseña de acceso Telnet	R3(config-line)#line vty 0 15 R3(config-line)#password cisco R3(config-line)#login
Cifrar las contraseñas de texto no cifrado	R3(config-line)#service password-encryption
Mensaje MOTD	R3(config)#banner motd %Se prohíbe el acceso no autorizado.%

Interfaz S0/0/1	R3(config)#interface s0/0/1 R3(config-if)#description coneccion R2 R3(config-if)#ip address 172.16.2.1 255.255.255.252 R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64 R3(config-if)#no shutdown
Interfaz loopback 4	R3(config)#interface loopback 4 R3(config-if)#ip address 192.168.4.1 255.255.255.0
Interfaz loopback 5	R3(config)#interface loopback 5 R3(config-if)#ip address 192.168.5.1 255.255.255.0
Interfaz loopback 6	R3(config)#interface loopback 6 R3(config-if)#ip address 192.168.6.1 255.255.255.0
Interfaz loopback 7	R3(config)#interface loopback 7 R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64
Rutas predeterminadas	R3(config-if)#ip route 0.0.0.0 0.0.0.0 s0/0/1 R3(config-if)#ipv6 route ::/0 s0/0/1

Paso 5: Configurar S1

Para los Switches S1 y S3 configuramos de acuerdo con la topología propuesta, utilizando los comandos requeridos para cada una de las tareas indicadas de acuerdo a la información que se consigna en sus respectivas tablas a continuación.

Tabla 6 Configuración S1

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

Paso 6: Configurar el S3

Tabla 7 Configuración S3

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

Paso 7: Verificar la conectividad de la red

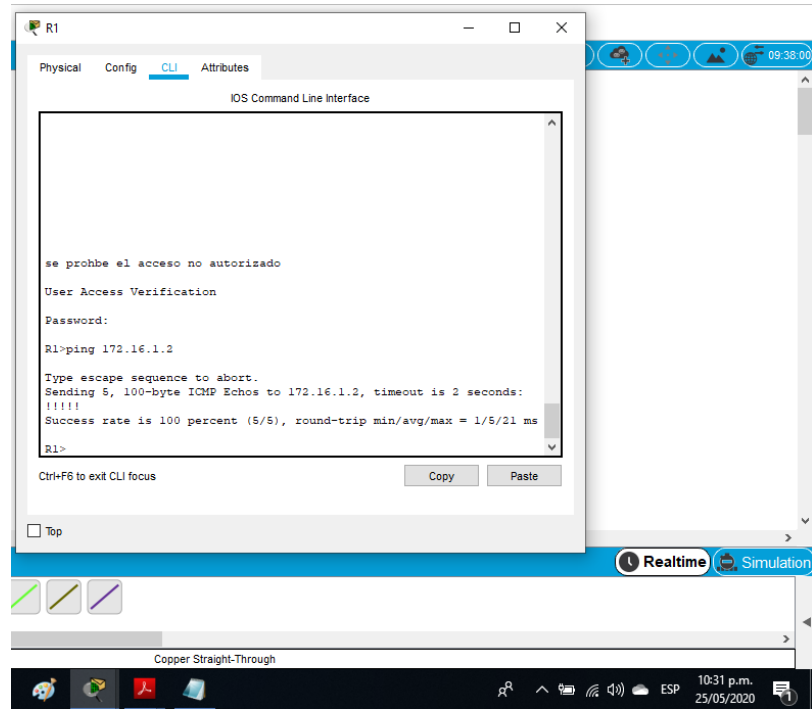
Utilice el comando **ping** para probar la conectividad entre los dispositivos de red. Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla

Tabla 8 Verificación conectividad de la red

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	Exitoso
R2	R3, S0/0/1	172.16.2.1	Exitoso
PC de Internet	Gateway predeterminado	209.165.200.233	Exitoso

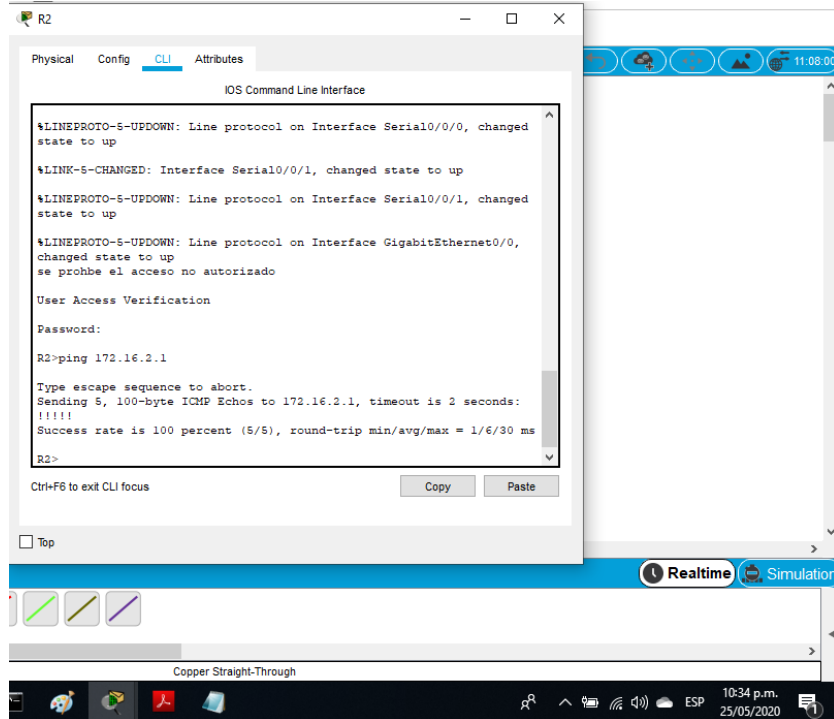
Nota: Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

Figura 2 Ping de R1 a R2



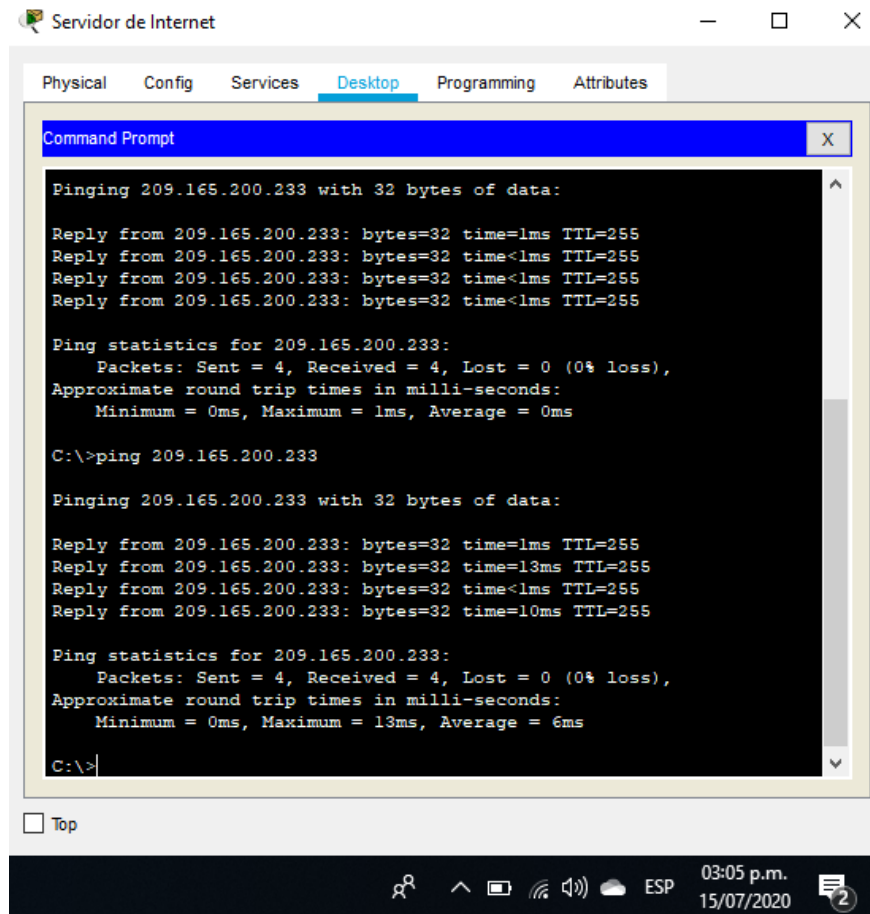
Autor: Fuente propia

Figura 3 Ping de R2 a R3



Autor: Fuente propia

Figura 4 Ping de PC de internet a Gateway predeterminado



Autor: Fuente propia

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

Paso 1: Configurar S1

En la configuración del Switch S1 se realizan la creación de las VLAN de las áreas de contabilidad, ingeniería y administración junto con la configuración que se emite en la siguiente tabla:

Tabla 9 Configuración de VLAN en S1

Elemento o tarea de configuración	Especificación
Crear la base de datos	S1(config)#vlan 21 S1(config-vlan)#name Contabilidad

de VLAN	S1(config-vlan)#vlan 23 S1(config-vlan)#name Ingenieria S1(config-vlan)#vlan 99 S1(config-vlan)#name Administracion
Asignar la dirección IP de administración.	S1(config)#interface vlan99 S1(config-if)#ip address 192.168.99.2 255.255.255.0 S1(config-if)#no shutdown
Asignar el gateway predeterminado	S1(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	S1(config)#interface f0/3 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1
Forzar el enlace troncal en la interfaz F0/5	S1(config)#interface f0/5 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	S1(config)#interface range f0/1-2, f0/4, f0/6-24, g0/1-2 S1(config-if-range)#switchport mode access
Asignar F0/6 a la VLAN 21	S1(config)#interface f0/6 S1(config-if)#switchport access vlan 21
Apagar todos los puertos sin usar	S1(config)#interface range f0/1-2, f0/4, f0/7-24, g0/1-2 S1(config-if-range)#shutdown

Paso 2: Configurar el S3

Al igual que el paso anterior se realiza la siguiente configuración en S3, se crean las VLAN para identificar las áreas, se asigna su respectivo direccionamiento, así como puerta predeterminada y se configuran puertos de acceso, puertos utilizados y sin usar como se muestra en la siguiente tabla:

Tabla 10 Configuración de S3

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	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

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

Paso 3: Configurar R1

Volvemos con el router R1 y realizamos la configuración de subinterfaces y direccionamiento tal como lo vemos en la siguiente tabla:

Tabla 11 Configuración de R1

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	R1(config)#interface g0/1.21 R1(config-subif)#description LAN de Contabilidad R1(config-subif)#encapsulation dot1q 21 R1(config-subif)#ip address 192.168.21.1 255.255.255.0
Configurar la subinterfaz 802.1Q .23 en G0/1	R1(config)#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	R1(config)#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)#interface g0/1 R1(config-if)#no shutdown

Paso 4: Verificar la conectividad de la red

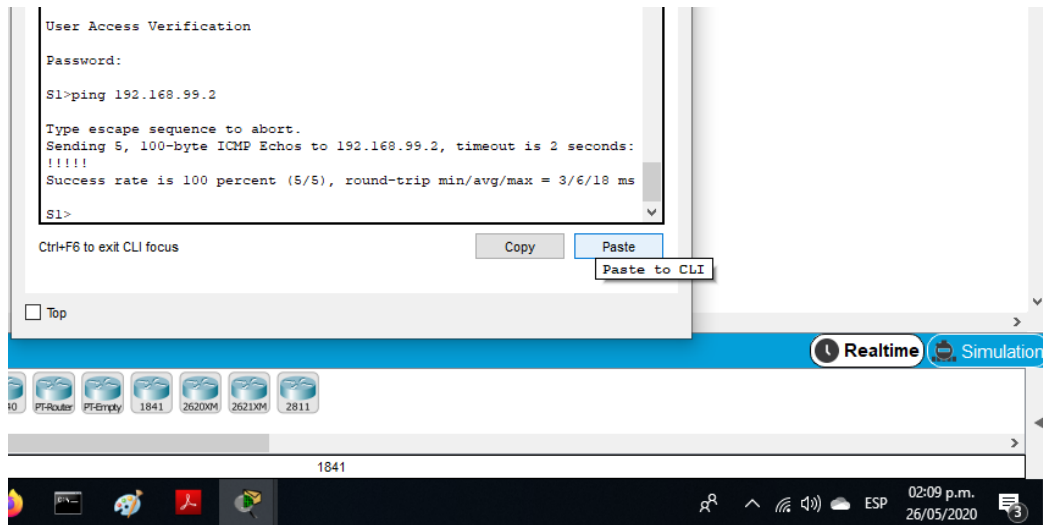
Verificamos la anterior mente configurado mediante el comando **ping** entre los switches y el R1.

Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red.

Tabla 12 Verificación de conectividad

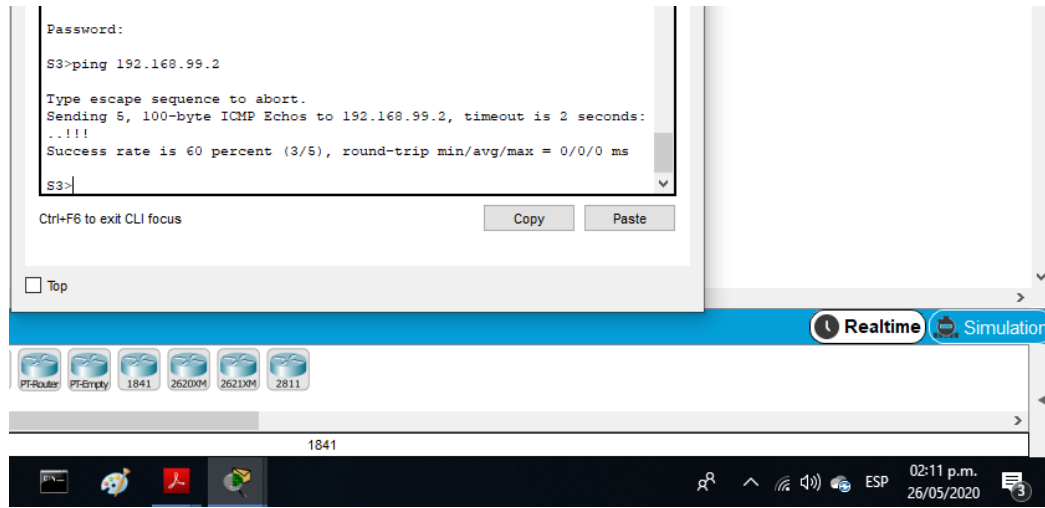
Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.2	Exitoso
S3	R1, dirección VLAN 99	192.168.99.2	Exitoso
S1	R1, dirección VLAN 21	192.168.21.2	Exitoso
S3	R1, dirección VLAN 23	192.168.23.2	Exitoso

Figura 5 Ping de S1 a R1, dirección VLAN 99



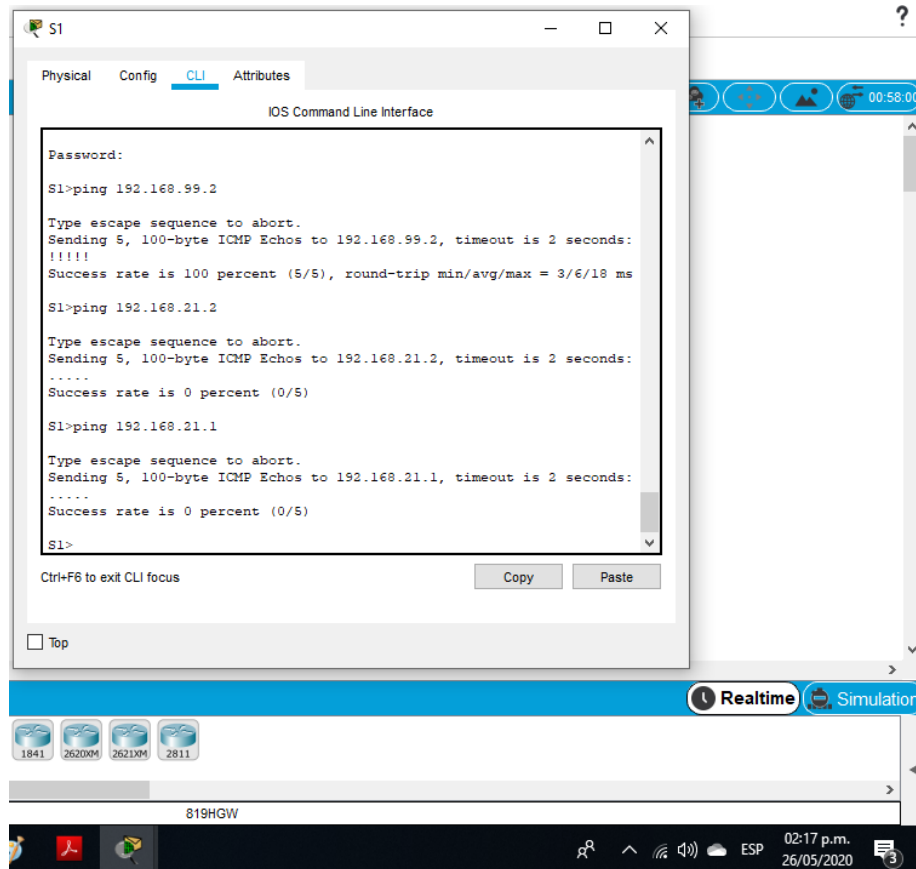
Autor: Fuente propia

Figura 6 Ping de S3 a R1, dirección VLAN 99



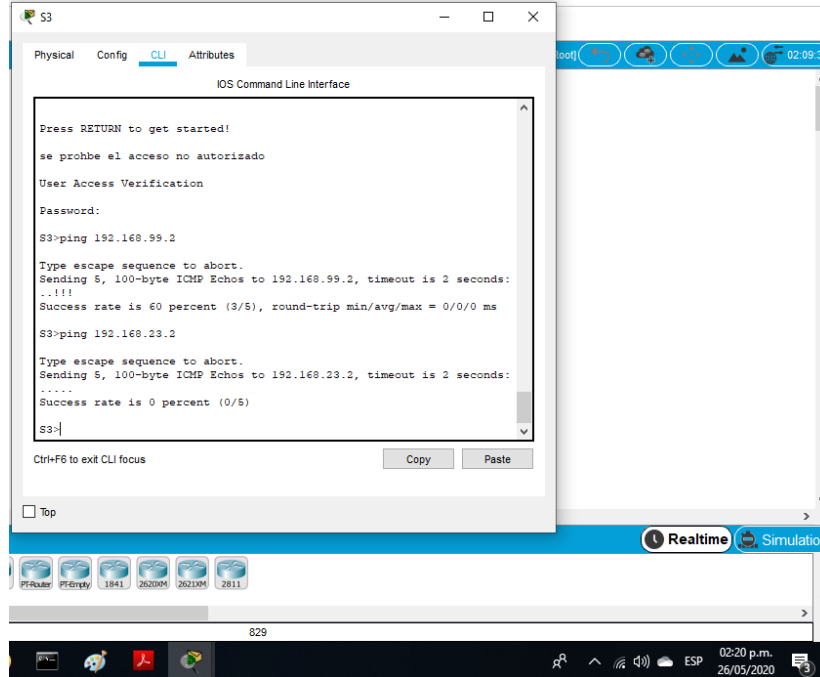
Autor: Fuente propia

Figura 7 Ping de S1 a R1, dirección VLAN 21



Autor: Fuente propia

Figura 8 Ping de S3 a R1, dirección VLAN 23



Autor: Fuente propia

Parte 4: Configurar el protocolo de routing dinámico RIPv2

Paso 1: Configurar RIPv2 en el R1

En esta parte se realiza configuración de RIPv2 en R1, para intercambiar datos entre las redes que se encuentran conectadas, así calcular la ruta más corta para llegar a su destino, mediante saltos que se generan.

Tabla 13 Configuración de RIPv2 en el R1

Elemento o tarea de configuración	Especificación
Configurar RIPv2	R1(config)#router rip R1(config-router)#version 2
Anunciar las redes conectadas directamente	R1(config-router)#network 172.16.1.0 R1(config-router)#network 192.168.21.0 R1(config-router)#network 192.168.23.0 R1(config-router)#network 192.168.99.0
Establecer las interfaces LAN como pasivas	R1(config-router)#passive-interface g0/1.21 R1(config-router)#passive-interface g0/1.23 R1(config-router)#passive-interface g0/1.99
Desactive la sum. automática	R1(config-router)#no auto-summary

Paso 2: Configurar RIPv2 en el R2

Configuramos RIPv2, se anuncian todas las redes conectadas directamente a R2, omitimos la red perteneciente G0/0, establecemos la interfaz LAN (loopback) como pasiva en G0/1, (Packer Tracer no soporta servidor http) y se desactiva la sumarización automática.

Tabla 14 Configuración de RIPv2 en el R2

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	R2(config)#router rip R2(config-router)#version 2
Anunciar las redes conectadas directamente	R2(config-router)#network 10.10.10.10 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 loopback0
Desactive la sumarización automática.	R2(config-router)#no auto-summary

Paso 3: Configurar RIPv2 en el R3

Configuramos RIPv2 en el router R3 según la topología, especificando rutas de cada conexión y establecemos las interfaces LAN como pasivas

Tabla 15 Configuración RIPv2 en el R3

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	R3(config)#router rip R3(config-router)#version 2
Anunciar redes IPv4 conectadas directamente	R3(config-router)#network 172.16.2.0 R3(config-router)#network 192.168.4.0 R3(config-router)#network 192.168.5.0 R3(config-router)#network 192.168.6.0
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	R3(config-router)#passive-interface loopback 4 R3(config-router)#passive-interface loopback 5 R3(config-router)#passive-interface loopback 6
Desactive la sum. Auto.	R3(config-router)#no auto-summary

Paso 4: Verificar la información de RIP

Utilizamos los siguientes comandos de CLI para obtener información de las configuraciones RIP realizadas anteriormente:

Tabla 16 Verificación de la información de RIP

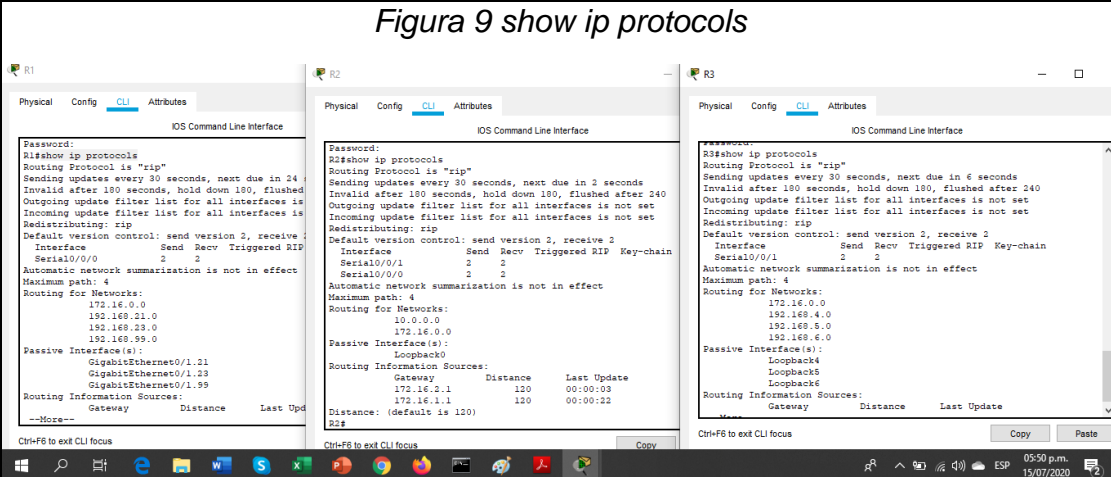
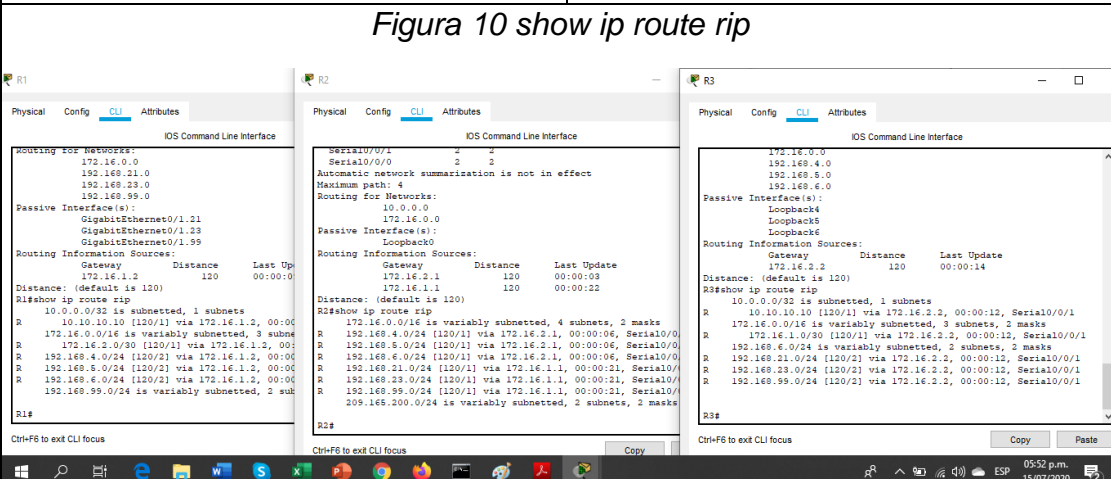
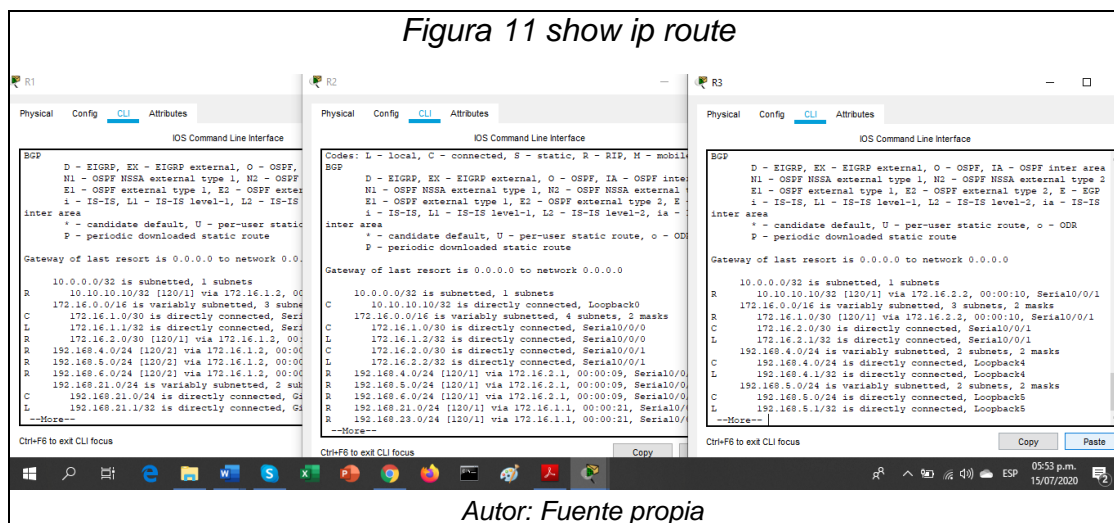
Pregunta	Respuesta
<p>¿Con qué comando se muestran la ID del proceso RIP, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router?</p>	<p>show ip protocols</p>
<p>Figura 9 show ip protocols</p> 	
<p><i>Autor: Fuente propia</i></p>	
<p>¿Qué comando muestra solo las rutas RIP?</p>	<p>show ip route rip</p>
<p>Figura 10 show ip route rip</p> 	
<p><i>Autor: Fuente propia</i></p>	
<p>¿Qué comando muestra la sección de RIP de la configuración en ejecución?</p>	<p>show ip route</p>

Figura 11 show ip route



Autor: Fuente propia

Parte 5: Implementar DHCP y NAT para IPv4

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

Configuramos el router R1 como servidor DHCP para las VLAN 21 y 23 basándonos en los parámetros que se ven en la tabla a continuación:

Tabla 17 Configuración de R1 como servidor de DHCP para las VLAN 21 y 23

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20
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.	R1(config)#ip dhcp pool ACCT R1(dhcp-config)#network 192.168.21.0 255.255.255.0 R1(dhcp-config)#default-router 192.168.21.1 R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com
Crear un pool de DHCP para la VLAN 23	R1(dhcp-config)#ip dhcp pool ENGR R1(dhcp-config)#network 192.168.23.0 255.255.255.0 R1(dhcp-config)#default-router 192.168.23.1 R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com

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

La configuración para el router R2 establecemos NAT estática y dinámica, se crea una la base de datos local y así dar acceso de usuarios, se habilita el servicio HTTP y establecemos una lista de acceso privada con las direcciones autorizadas para poder ingresar. Lo anterior con los parámetros en la tabla siguiente:

Tabla 18 Configuración de NAT estática y dinámica en el R2

Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	R2(config)#username webuser privilege 15 secret cisco12345
Habilitar el servicio del servidor HTTP	R2(config)#ip http server <i>Nota: comando no disponible en esta versión de pkt</i>
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	R2(config)#ip http authentication local <i>Nota: comando no disponible en esta versión de pkt</i>
Crear una NAT estática al servidor web.	R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229
Asignar la interfaz interna y externa para la NAT estática	R2(config)#interface g0/0 R2(config-if)#ip nat outside R2(config-if)#interface s0/0/0 R2(config-if)#ip nat inside R2(config-if)#interface s0/0/1 R2(config-if)#ip nat inside
Configurar la NAT dinámica dentro de una ACL privada	R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255
Defina el pool de direcciones IP públicas utilizables.	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

Paso 3: Verificar el protocolo DHCP y la NAT estática

Para verificar la eficacia de la anterior configuración realizada usamos las siguientes tareas para verificar el funcionamiento de DHCP y NAT estática. Se mostrarán los resultados en las tablas a continuación son sus respectivos comando e ilustración.

Tabla 19 Verificación el protocolo DHCP y la NAT estática

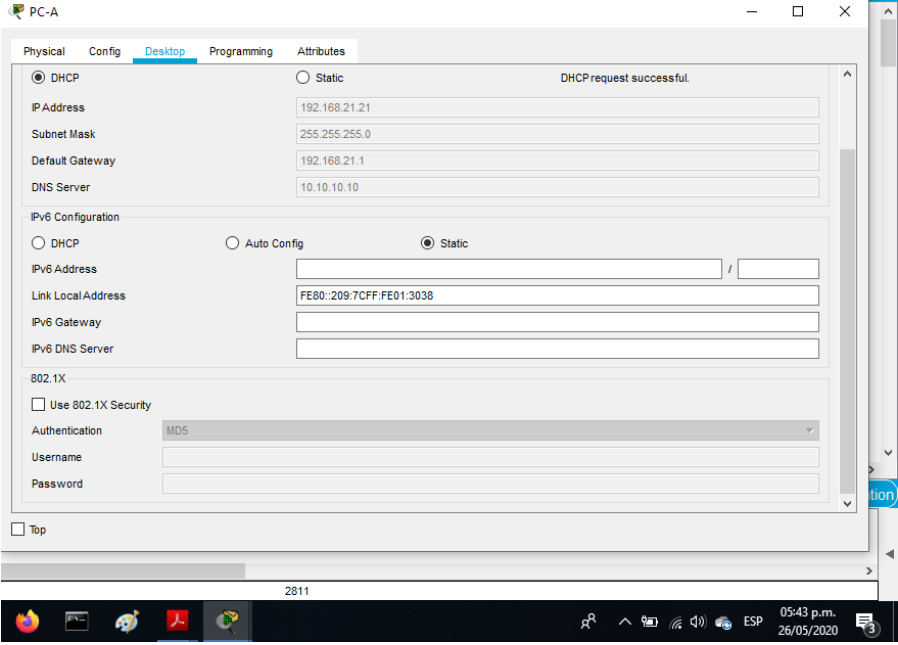
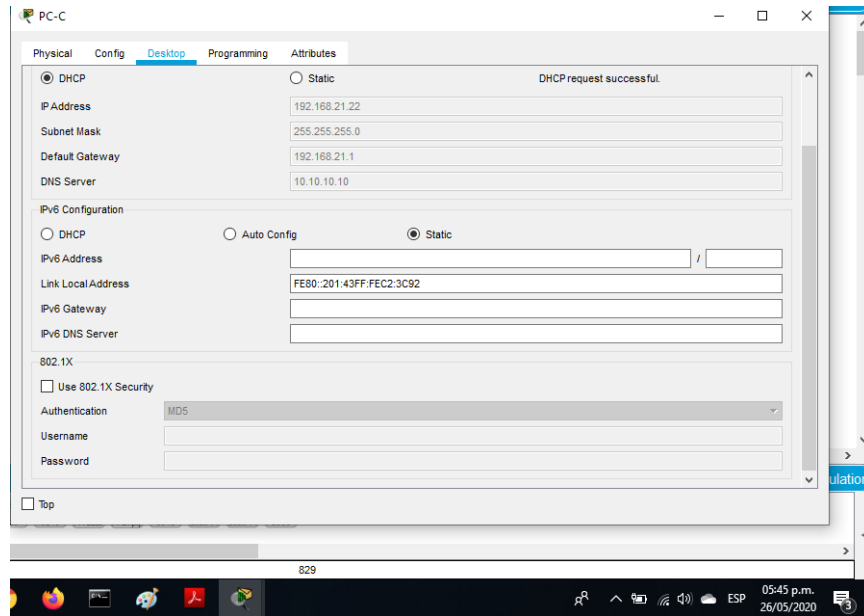
Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	Exitoso
<p style="text-align: center;"><i>Figura 12 Verificación que PC-A tome IP del servidor de DHCP</i></p>  <p style="text-align: center;"><i>Autor: Fuente propia</i></p>	
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	Exitosos

Figura 13 Verificación que PC-C tome IP del servidor de DHCP

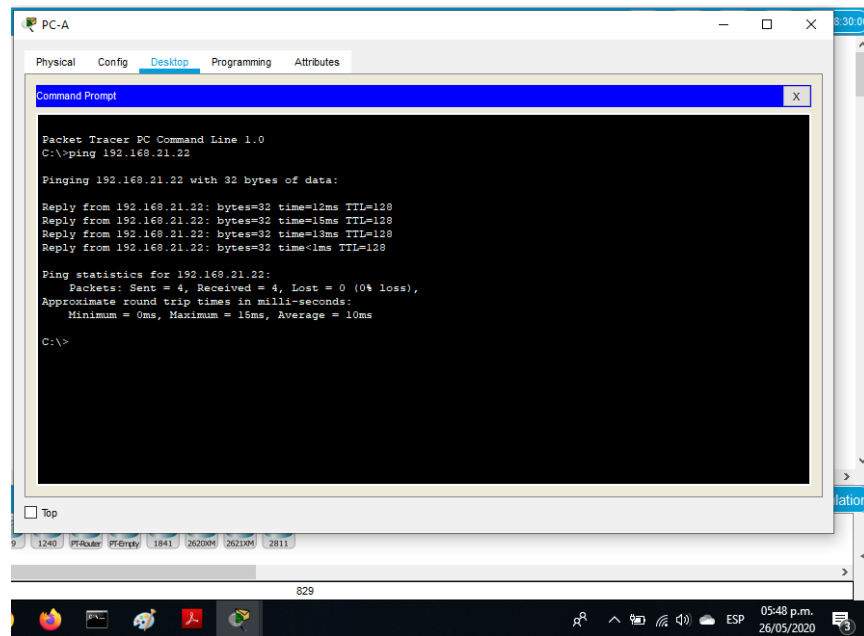


Autor: Fuente propia

Verificar que la PC-A pueda hacer ping a la PC-C

Exitosos

Figura 14 Ping de PC-A a PC-C

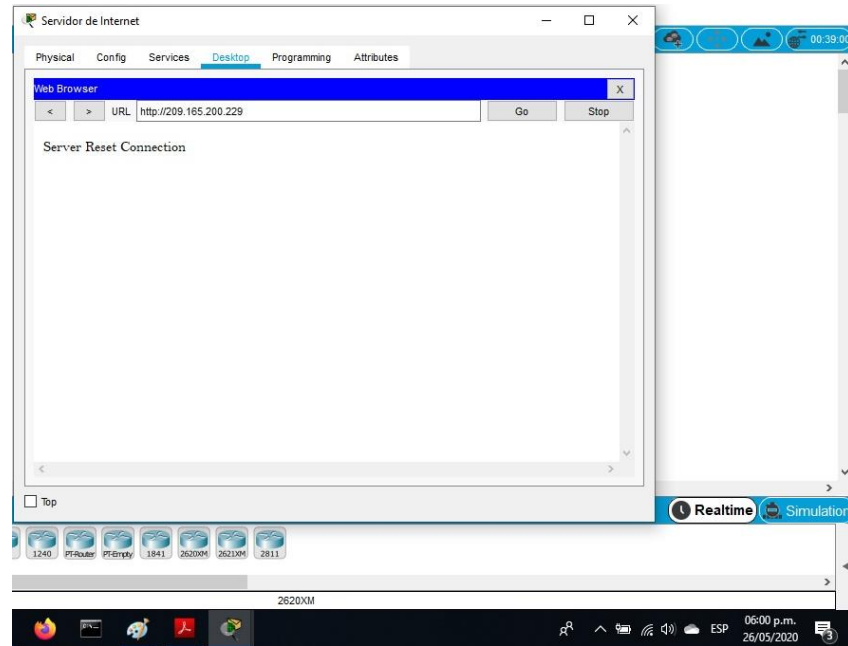


Autor: Fuente propia

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**

Exitoso

Figura 15 Acceso al servidor web (209.165.200.229)



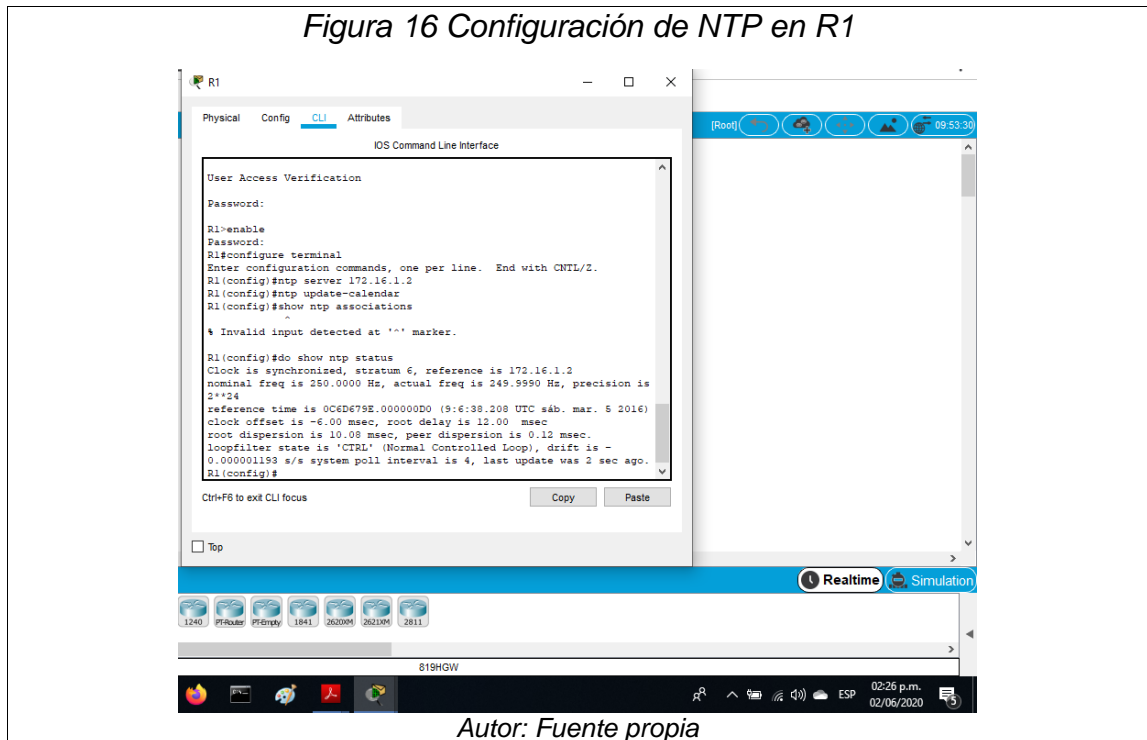
Parte 6: Configurar NTP

Con esta configuración es un protocolo para la sincronización de cada reloj entre dispositivos, el router R2 maneja un NTP maestro 5 y el router R1 es un cliente de R2, con esto, NTP controla las latencias. Para ellos se realiza la configuración en la tabla a continuación:

Tabla 20 Configuración NTP

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

Figura 16 Configuración de NTP en R1



Autor: Fuente propia

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

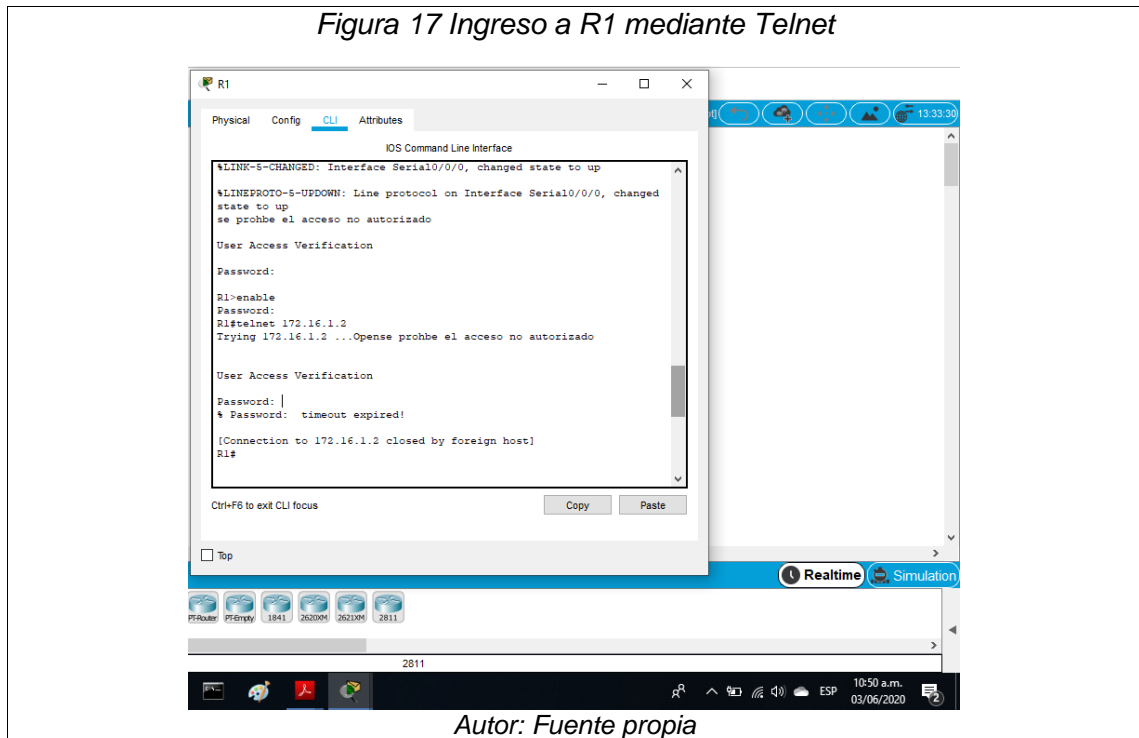
Paso 1: Restringir el acceso a las líneas VTY en el R2

En esta parte restringimos las líneas VTY en el router R2, logrando acceso remoto desde el modo EXEC desde el router R1 con esta línea, se realiza los pasos que se ven a continuación en la tabla y posteriormente verificamos su funcionamiento que se evidencian en las imágenes continuas:

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

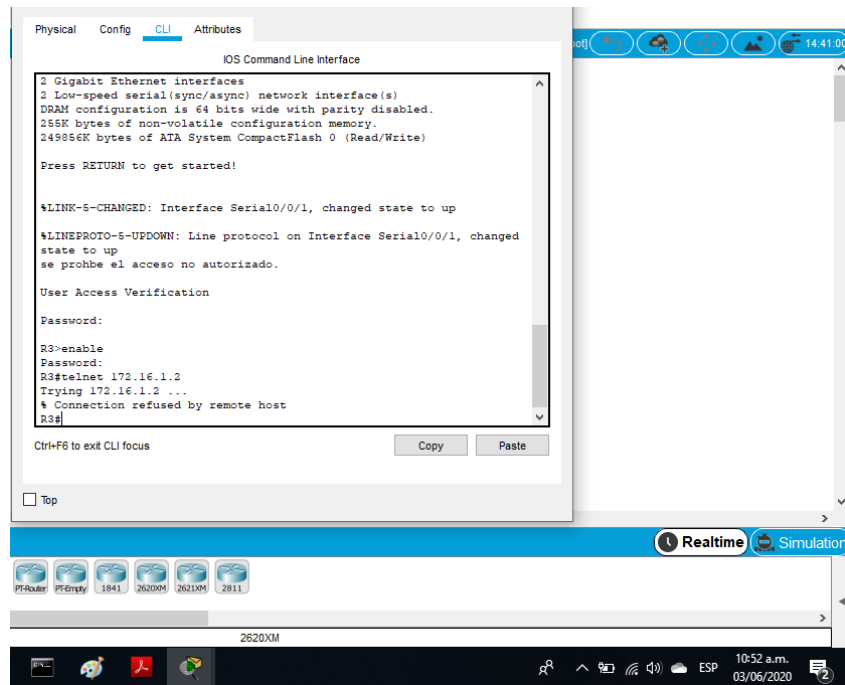
Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	R2(config)#ip access-list standard ADMIN-MGT R2(config-std-nacl)#permit host 172.16.1.1
Aplicar la ACL con nombre a las líneas VTY	R2(config)#line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

Figura 17 Ingreso a R1 mediante Telnet



Autor: Fuente propia

Figura 18 Acceso rechazado desde el R3 por Telnet



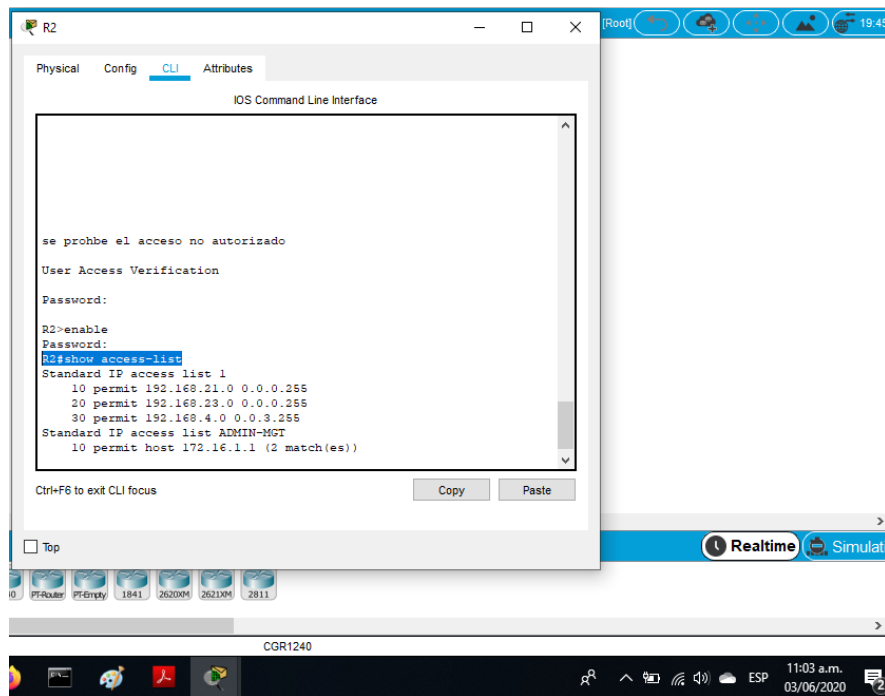
Autor: Fuente propia

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

Tabla 22 Verificación mediante el 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	R2#show access-list

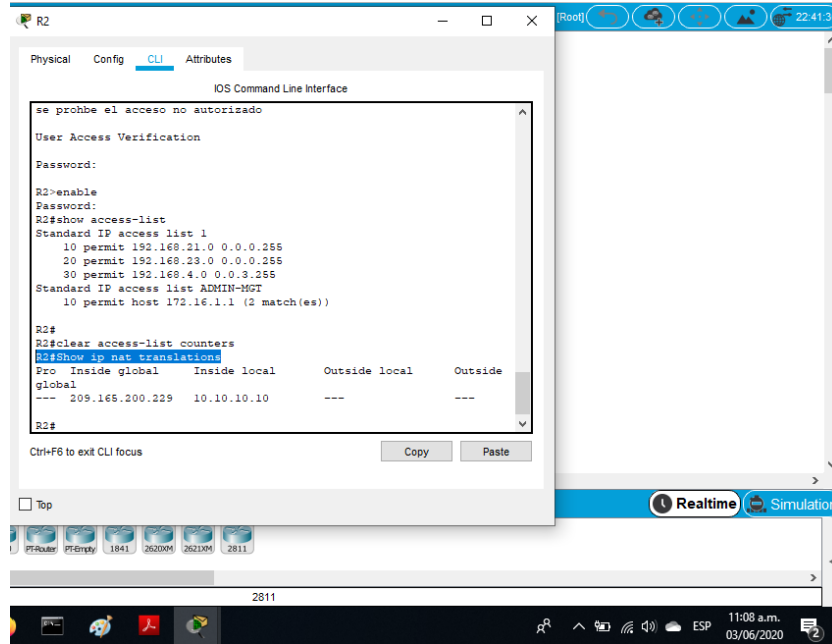
Figura 19 show access-list



Autor: Fuente propia

Restablecer los contadores de una lista de acceso	R2#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 interface buscar sh run
¿Con qué comando se muestran las traducciones NAT?	R2#Show ip nat translations

Figura 20 Show ip nat translations

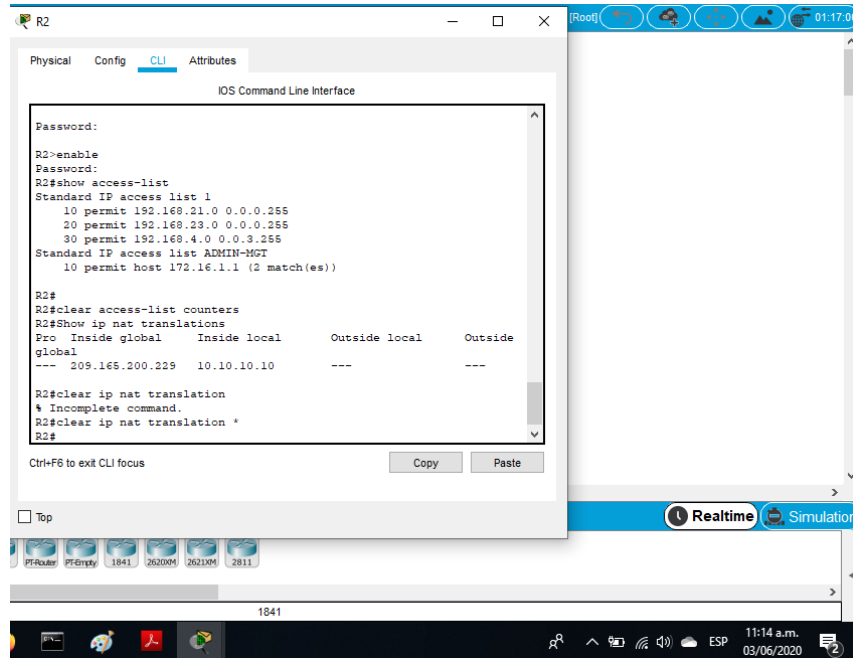


Autor: Fuente propia

¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?

R2#clear ip nat translation

Figura 21 Clear ip nat translation

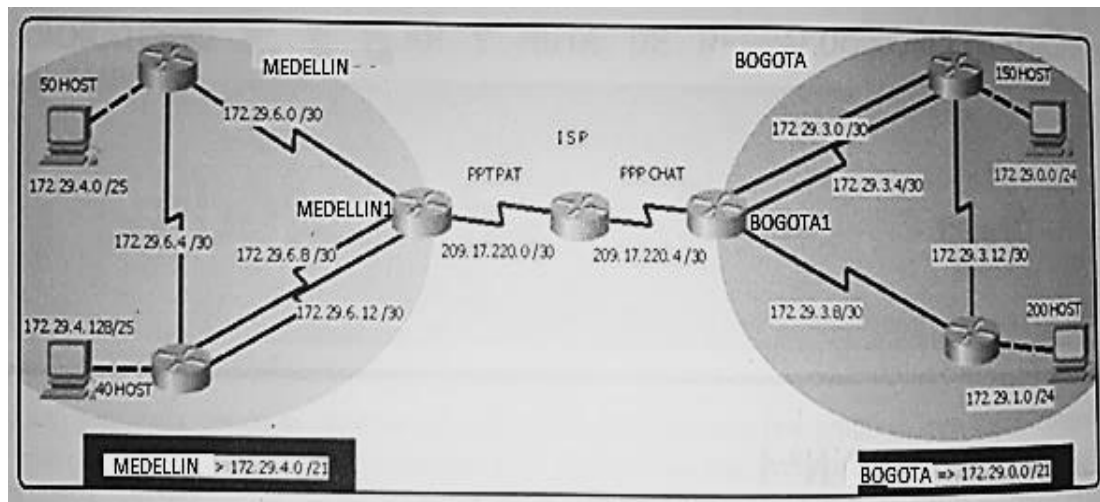


Autor: Fuente propia

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 22 Topología de red escenario 2



Este escenario plantea el uso de OSPF como protocolo de enrutamiento, considerando que se tendrán rutas por defecto redistribuidas; asimismo, habilitar el encapsulamiento PPP y su autenticación.

Los ROUTERS Bogota2 y medellin2 proporcionan el servicio DHCP a su propia red LAN y a los ROUTERS 3 de cada ciudad.

Debe configurar PPP en los enlaces hacia el ISP, con autenticación.

Debe habilitar NAT de sobrecarga en los routers Bogota1 y medellin1.

Desarrollo

Iniciamos realizando las diferentes rutinas de diagnóstico para dejar los equipos listos para su configuración, asignamos nombres de equipos, claves de seguridad, encriptación de contraseñas y mensajes de acceso no autorizado en cada equipo.

A continuación, indican los comandos utilizados para llevar a cabo la iniciación correspondiente:

ISP

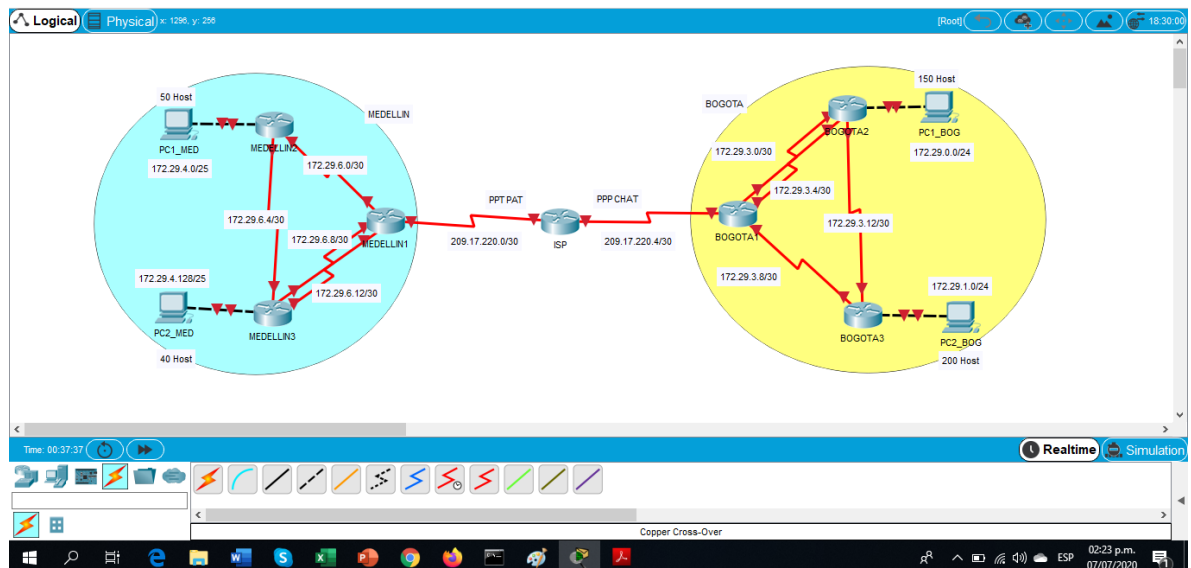
```
Router>enable
Router#configure terminal
Router(config)#no ip domain-lookup
Router(config)#hostname ISP
ISP(config)#enable secret class
ISP(config)#line console 0
ISP(config-line)#password cisco
ISP(config-line)#login
ISP(config-line)#line vty 0 15
ISP(config-line)#password cisco
ISP(config-line)#service password-encryption
ISP(config)#banner motd "Se prohíbe el acceso no autorizado."
```

En los demás routers la configuración es igual solo cambian los hostname.

```
Router(config)#hostname Medellin1
Router(config)#hostname Medellin2
Router(config)#hostname Medellin3
Router(config)#hostname Bogota1
Router(config)#hostname Bogota2
Router(config)#hostname Bogota3
```

En la siguiente ilustración de muestra cómo se realizar la conexión física de los equipos con base en la topología de red y de acuerdo con las especificaciones planteadas.

Figura 23 Topología de red realizada en PKT



Autor: Fuente propia

Para facilitar el trabajo se plantea la siguiente tabla con las diferentes interfaces y sus respectivos direccionamientos y así llevar a cabo la configuración correcta de los equipos a trabajar.

Tabla 23 Direccionamiento interfaz routers

Dispositivo	Interfaz	Conexión a	Dirección IP	Mascara de Subred	Gateway predeterminado
Medellín1	S0/0/0	ISP	209.17.220.2	255.255.255.252	N/A
	S0/0/1	Medellín2	172.29.6.1	255.255.255.252	N/A
	S0/1/0	Medellín3	172.29.6.9	255.255.255.252	N/A
	S0/1/1	Medellín3	172.29.6.13	255.255.255.252	N/A
Medellín2	S0/0/0	Medellín1	172.29.6.2	255.255.255.252	N/A
	S0/0/1	Medellín3	172.29.6.5	255.255.255.252	N/A
	G0/0	PC1_MED	172.29.4.1	255.255.255.128	N/A
Medellín3	S0/0/0	Medellín1	172.29.6.10	255.255.255.252	N/A
	S0/0/1	Medellín2	172.29.6.6	255.255.255.252	N/A
	S0/1/0	Medellín1	172.29.6.14	255.255.255.252	N/A
	G0/0	PC2_MED	172.29.4.129	255.255.255.128	N/A
Bogotá1	S0/0/0	ISP	209.17.220.6	255.255.255.252	N/A
	S0/0/1	Bogota2	172.29.3.1	255.255.255.252	N/A
	S0/1/0	Bogota3	172.29.3.9	255.255.255.252	N/A
	S0/1/1	Bogota2	172.29.3.5	255.255.255.252	N/A
Bogotá2	S0/0/0	Bogota1	172.29.3.2	255.255.255.252	N/A
	S0/0/1	Bogota3	172.29.3.13	255.255.255.252	N/A
	S0/1/0	Bogota1	172.29.3.6	255.255.255.252	N/A
	G0/0	PC1_BOG	172.29.0.1	255.255.255.0	N/A
Bogotá3	S0/0/0	Bogota1	172.29.3.10	255.255.255.252	N/A
	S0/0/1	Bogota2	172.29.3.14	255.255.255.252	N/A
	G0/0	PC2_BOG	172.29.1.1	255.255.255.0	N/A
ISP	S0/0/0	Medellín1	209.17.220.1	255.255.255.252	N/A
	S0/0/1	Bogota1	209.17.220.5	255.255.255.252	N/A
PC1_MED	Fa0	Medellín2	DHCP	255.255.255.128	172.29.4.1
PC2_MED	Fa0	Medellín3	DHCP	255.255.255.128	172.29.4.129
PC1_BOG	Fa0	Bogota2	DHCP	255.255.255.0	172.29.0.1
PC2_BOG	Fa0	Bogota3	DHCP	255.255.255.0	172.29.1.1

Con base en la tabla continuamos realizando las configuraciones en los distintos equipos con sus respectivas características planteadas:

Configuración de direccionamiento en interfaz de cada router.

```
Medellin1#configure terminal
Medellin1(config)#int s0/0/0
Medellin1(config-if)#description Conexion a ISP
Medellin1(config-if)#ip address 209.17.220.2 255.255.255.252
Medellin1(config-if)#clock rate 128000
Medellin1(config-if)#no shutdown
Medellin1(config-if)#int s0/0/1
Medellin1(config-if)#description Conexion a Medellin2
Medellin1(config-if)#ip address 172.29.6.1 255.255.255.252
Medellin1(config-if)#clock rate 128000
Medellin1(config-if)#no shutdown
Medellin1(config-if)#int s0/1/0
Medellin1(config-if)#description Conexion a Medellin3
Medellin1(config-if)#ip address 172.29.6.9 255.255.255.252
Medellin1(config-if)#clock rate 128000
Medellin1(config-if)#no shutdown
Medellin1(config-if)#int s0/1/1
Medellin1(config-if)#description Conexion a Medellin3
Medellin1(config-if)#ip address 172.29.6.13 255.255.255.252
Medellin1(config-if)#clock rate 128000
Medellin1(config-if)#no shutdown
Medellin1(config-if)#
```

```
Medellin2(config)#int s0/0/0
Medellin2(config-if)#description Conexion a Medellin1
Medellin2(config-if)#ip address 172.29.6.2 255.255.255.252
Medellin2(config-if)#clock rate 128000
Medellin2(config-if)#no shutdown
Medellin2(config-if)#int s0/0/1
Medellin2(config-if)#description Conexion a Medellin3
Medellin2(config-if)#ip address 172.29.6.5 255.255.255.252
Medellin2(config-if)#clock rate 128000
Medellin2(config-if)#no shutdown
Medellin2(config-if)#int g0/0
Medellin2(config-if)#description Conexion a PC1_MED
Medellin2(config-if)#ip address 172.29.4.1 255.255.255.128
Medellin2(config-if)#no shutdown
```

```
Medellin3(config)#int s0/0/0
Medellin3(config-if)#description Conexion a Medellin1
Medellin3(config-if)#ip address 172.29.6.10 255.255.255.252
Medellin3(config-if)#clock rate 128000
Medellin3(config-if)#no shutdown
```



```
Medellin3(config-if)#int s0/0/1
Medellin3(config-if)#description Conexion a Medellin2
Medellin3(config-if)#ip address 172.29.6.6 255.255.255.252
Medellin3(config-if)#clock rate 128000
Medellin3(config-if)#no shutdown
Medellin3(config-if)#int s0/1/0
Medellin3(config-if)#description Conexion a Medellin1
Medellin3(config-if)#ip address 172.29.6.14 255.255.255.252
Medellin3(config-if)#clock rate 128000
Medellin3(config-if)#no shutdown
Medellin3(config-if)#int g0/0
Medellin3(config-if)#description Conexion a PC2_MED
Medellin3(config-if)#ip address 172.29.4.129 255.255.255.128
Medellin3(config-if)#no shutdown
```

```
Bogota1(config)#int s0/0/0
Bogota1(config-if)#description Conexion a ISP
Bogota1(config-if)#ip address 209.17.220.6 255.255.255.252
Bogota1(config-if)#clock rate 128000
Bogota1(config-if)#no shutdown
Bogota1(config-if)#int s0/0/1
Bogota1(config-if)#description Conexion a Bogota2
Bogota1(config-if)#ip address 172.29.3.1 255.255.255.252
Bogota1(config-if)#clock rate 128000
Bogota1(config-if)#no shutdown
Bogota1(config-if)#int s0/1/0
Bogota1(config-if)#description Conexion a Bogota3
Bogota1(config-if)#ip address 172.29.3.9 255.255.255.252
Bogota1(config-if)#clock rate 128000
Bogota1(config-if)#no shutdown
Bogota1(config-if)#int s0/1/1
Bogota1(config-if)#description Conexion a Bogota2
Bogota1(config-if)#ip address 172.29.3.5 255.255.255.252
Bogota1(config-if)#clock rate 128000
Bogota1(config-if)#no shutdown
```

```
Bogota2(config)#int s0/0/0
Bogota2(config-if)#description Conexion a Bogota1
Bogota2(config-if)#ip address 172.29.3.2 255.255.255.252
Bogota2(config-if)#clock rate 128000
Bogota2(config-if)#no shutdown
Bogota2(config-if)#int s0/0/1
Bogota2(config-if)#description Conexion a Bogota3
Bogota2(config-if)#ip address 172.29.3.13 255.255.255.252
Bogota2(config-if)#clock rate 128000
```

```
Bogota2(config-if)#no shutdown
Bogota2(config-if)#int s0/1/0
Bogota2(config-if)#description Conexion a Bogota1
Bogota2(config-if)#ip address 172.29.3.6 255.255.255.252
Bogota2(config-if)#clock rate 128000
Bogota2(config-if)#no shutdown
Bogota2(config-if)#int g0/0
Bogota2(config-if)#description Conexion a PC1_BOG
Bogota2(config-if)#ip address 172.29.0.1 255.255.255.0
Bogota2(config-if)#no shutdown
Bogota3(config)#int s0/0/0
Bogota3(config-if)#description Conexion a Bogota1
Bogota3(config-if)#ip address 172.29.3.10 255.255.255.252
Bogota3(config-if)#clock rate 128000
Bogota3(config-if)#no shutdown
Bogota3(config-if)#int s0/0/1
Bogota3(config-if)#description Conexion a Bogota2
Bogota3(config-if)#ip address 172.29.3.14 255.255.255.252
Bogota3(config-if)#clock rate 128000
Bogota3(config-if)#no shutdown
Bogota3(config-if)#int g0/0
Bogota3(config-if)#description Conexion a PC2_BOG
Bogota3(config-if)#ip address 172.29.1.1 255.255.255.0
Bogota3(config-if)#no shutdown

ISP(config)#int s0/0/0
ISP(config-if)#description Conexion a Medellin1
ISP(config-if)#ip address 209.17.220.1 255.255.255.252
ISP(config-if)#clock rate 128000
ISP(config-if)#no shutdown
ISP(config-if)#int s0/0/1
ISP(config-if)#description Conexion a Bogota1
ISP(config-if)#ip address 209.17.220.5 255.255.255.252
ISP(config-if)#clock rate 128000
ISP(config-if)#no shutdown
```

Parte 1: Configuración del enrutamiento

En esta parte se realiza la configuración del enrutamiento en la red usando el protocolo OSPF versión 2, declaramos la red principal, desactivamos la sumarización automática en cada router exceptuando el router ISP. Tal como se muestra en las siguientes líneas de comando:

```
Medellin1(config)#router ospf 1
Medellin1(config-router)#router-id 1.1.1.1
Medellin1(config-router)#net 172.29.6.0 0.0.0.3 area 0
Medellin1(config-router)#net 172.29.6.8 0.0.0.3 area 0
Medellin1(config-router)#net 172.29.6.12 0.0.0.3 area 0
```

```
Medellin2(config)#router ospf 1
Medellin2(config-router)#router-id 2.2.2.2
Medellin2(config-router)#net 172.29.4.0 0.0.0.255 area 0
Medellin2(config-router)#net 172.29.6.0 0.0.0.3 area 0
Medellin2(config-router)#net 172.29.6.4 0.0.0.3 area 0
```

```
Medellin3(config)#router ospf 1
Medellin3(config-router)#router-id 3.3.3.3
Medellin3(config-router)#net 172.29.4.128 0.0.0.255 area 0
Medellin3(config-router)#net 172.29.6.4 0.0.0.3 area 0
Medellin3(config-router)#net 172.29.6.8 0.0.0.3 area 0
Medellin3(config-router)#net 172.29.6.12 0.0.0.3 area 0
```

```
Bogota1(config)#router ospf 1
Bogota1(config-router)#router-id 4.4.4.4
Bogota1(config-router)#net 172.29.3.0 0.0.0.3 area 0
Bogota1(config-router)#net 172.29.3.4 0.0.0.3 area 0
Bogota1(config-router)#net 172.29.3.8 0.0.0.3 area 0
```

```
Bogota2(config)#router ospf 1
Bogota2(config-router)#router-id 5.5.5.5
Bogota2(config-router)#net 172.29.0.0 0.0.0.255 area 0
Bogota2(config-router)#net 172.29.3.0 0.0.0.3 area 0
Bogota2(config-router)#net 172.29.3.4 0.0.0.3 area 0
Bogota2(config-router)#net 172.29.3.12 0.0.0.3 area 0
```

```
Bogota3(config)#router ospf 1
Bogota3(config-router)#router-id 6.6.6.6
Bogota3(config-router)#net 172.29.1.0 0.0.0.255 area 0
Bogota3(config-router)#net 172.29.3.8 0.0.0.3 area 0
Bogota3(config-router)#net 172.29.3.12 0.0.0.3 area 0
```

Configuramos los routers Bogota1 y Medellín con una ruta por defecto hacia el ISP y, que a su vez, reparta en las publicaciones de OSPF, como se indica en las siguientes líneas de comando:

```
Medellin1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.1
Medellin1(config)#router ospf 1
Medellin1(config-router)#default-information originate
```

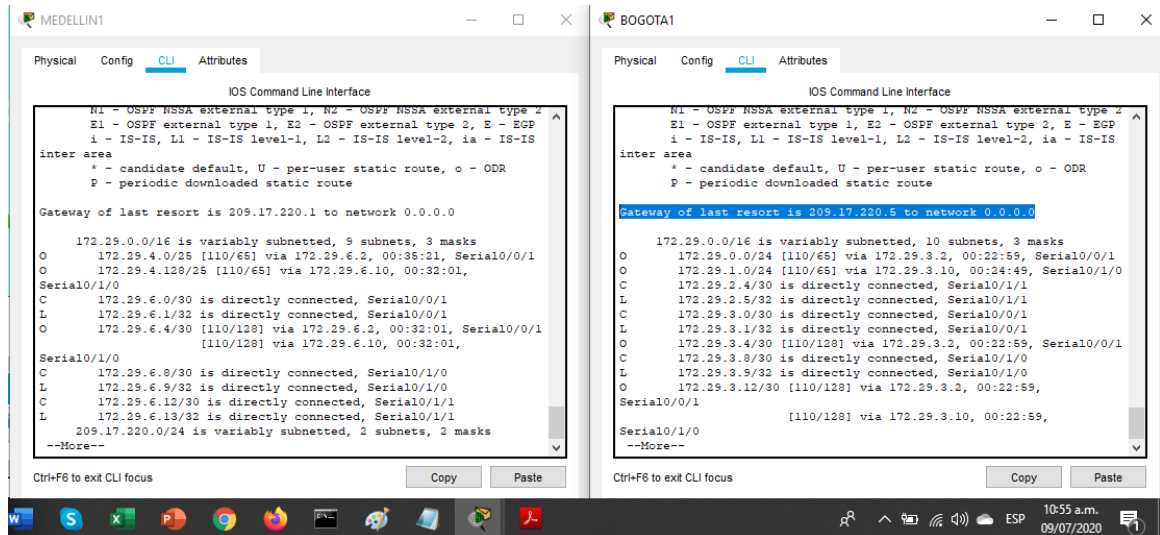
```

Bogota1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.5
Bogota1(config)#router ospf 1
Bogota1(config-router)#default-information originate

```

Se valida la configuración realizada mediante el comando “show ip route” como se muestra en la ilustración:

Figura 24 Verificación por comando show ip route conexión con ISP



Autor: Fuente propia

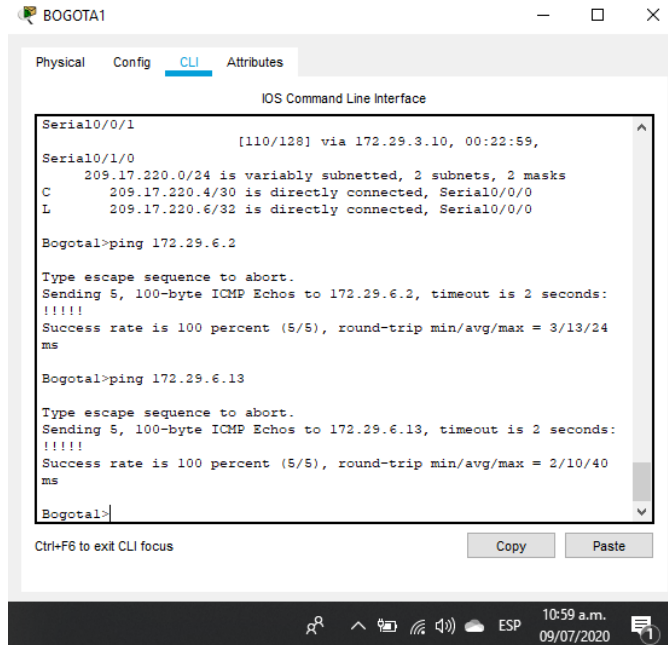
Se configura el router ISP con una ruta estática dirigida hacia cada red interna de Bogotá y Medellín para el caso se suman las subredes de cada uno a /22, tal como se especifica en las siguientes líneas de comando y se realiza verificación mediante el comando ping como se ve en la próxima ilustración:

```

ISP(config)#ip route 172.29.4.0 255.255.252.0 209.17.220.2
ISP(config)#ip route 172.29.0.0 255.255.252.0 209.17.220.6

```

Figura 25 Verificación conectividad entre Medellín y Bogotá



```
BOGOTA1
Physical Config CLI Attributes
IOS Command Line Interface
Serial0/0/1 [110/128] via 172.29.3.10, 00:22:59,
Serial0/1/0
  209.17.220.0/24 is variably subnetted, 2 subnets, 2 masks
C   209.17.220.4/30 is directly connected, Serial0/0/0
L   209.17.220.6/32 is directly connected, Serial0/0/0

Bogota1>ping 172.29.6.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.6.2, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/13/24
ms

Bogota1>ping 172.29.6.13

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.6.13, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/10/40
ms

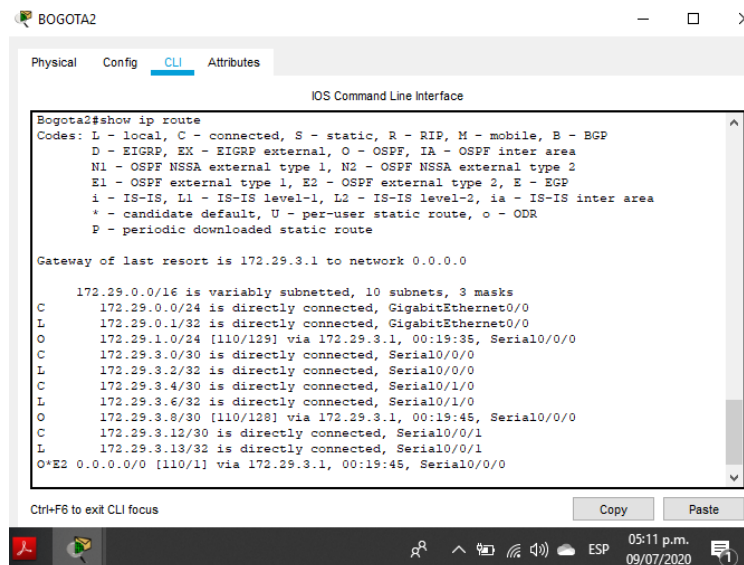
Bogota1>
```

Autor: Fuente propia

Parte 2: Tabla de Enrutamiento.

Mediante el comando show ip route se verifica la tabla de enrutamiento en cada uno de los routers para comprobar las redes y sus rutas anteriormente configuradas:

Figura 26 Verificación de enrutamiento router Bogota2



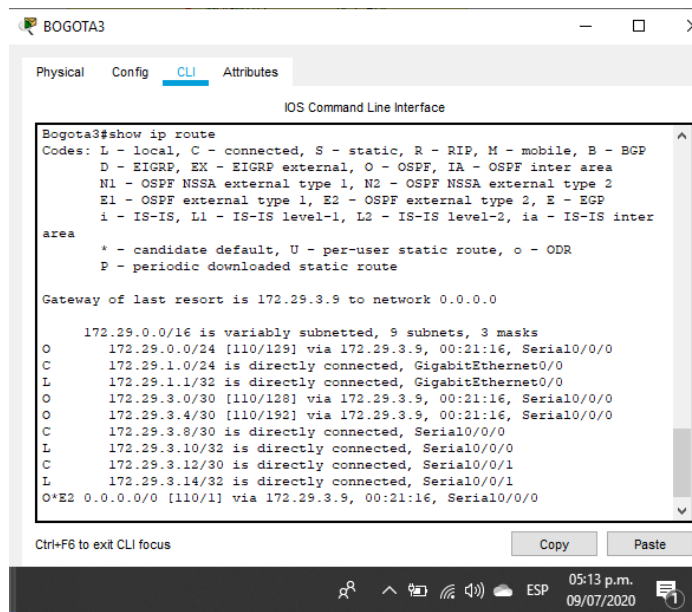
```
BOGOTA2
Physical Config CLI Attributes
IOS Command Line Interface
Bogota2#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 172.29.3.1 to network 0.0.0.0

 172.29.0.0/16 is variably subnetted, 10 subnets, 3 masks
C   172.29.0.0/24 is directly connected, GigabitEthernet0/0
L   172.29.0.1/32 is directly connected, GigabitEthernet0/0
O   172.29.1.0/24 [110/129] via 172.29.3.1, 00:19:35, Serial0/0/0
C   172.29.3.0/30 is directly connected, Serial0/0/0
L   172.29.3.2/32 is directly connected, Serial0/0/0
C   172.29.3.4/30 is directly connected, Serial0/1/0
L   172.29.3.6/32 is directly connected, Serial0/1/0
O   172.29.3.8/30 [110/128] via 172.29.3.1, 00:19:45, Serial0/0/0
C   172.29.3.12/30 is directly connected, Serial0/0/1
L   172.29.3.13/32 is directly connected, Serial0/0/1
O*E2 0.0.0.0/0 [110/1] via 172.29.3.1, 00:19:45, Serial0/0/0
```

Autor: Fuente propia

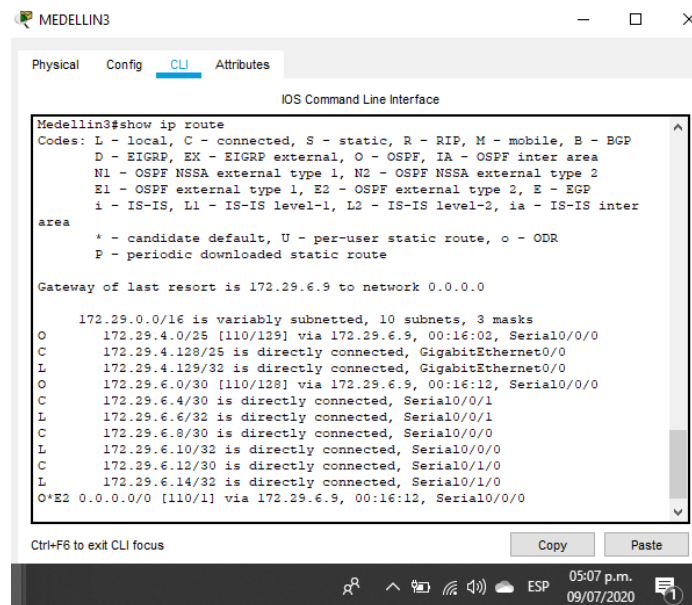
Figura 27 Verificación de enrutamiento router Bogota3



Autor: Fuente propia

Verificar el balanceo de carga que presentan los routers.

Figura 28 Verificación de balanceo de carga en router Meedelin3



Autor: Fuente propia

Podemos evidenciar 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.

Figura 29 Verificación doble enlace router bogota1

```
Bogota1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
       area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 209.17.220.5 to network 0.0.0.0

172.29.0.0/16 is variably subnetted, 10 subnets, 3 masks
O   172.29.0.0/24 [110/65] via 172.29.3.2, 00:17:42, Serial0/0/1
O   172.29.1.0/24 [110/65] via 172.29.3.10, 00:17:42, Serial0/1/0
C   172.29.2.4/30 is directly connected, Serial0/1/1
L   172.29.2.5/32 is directly connected, Serial0/1/1
C   172.29.3.0/30 is directly connected, Serial0/0/1
L   172.29.3.1/32 is directly connected, Serial0/0/1
O   172.29.3.4/30 [110/128] via 172.29.3.2, 00:17:42, Serial0/0/1
C   172.29.3.8/30 is directly connected, Serial0/1/0
L   172.29.3.9/32 is directly connected, Serial0/1/0
O   172.29.3.12/30 [110/128] via 172.29.3.10, 00:17:42, Serial0/1/0
    [110/128] via 172.29.3.2, 00:17:42, Serial0/0/1
209.17.220.0/24 is variably subnetted, 2 subnets, 2 masks
C   209.17.220.4/30 is directly connected, Serial0/0/0
L   209.17.220.6/32 is directly connected, Serial0/0/0
S*  0.0.0.0/0 [1/0] via 209.17.220.5
```

Autor: Fuente propia

Figura 30 Verificación doble enlace router Medellin1

```
Medellin1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 209.17.220.1 to network 0.0.0.0

172.29.0.0/16 is variably subnetted, 9 subnets, 3 masks
O   172.29.4.0/25 [110/65] via 172.29.6.2, 00:09:12, Serial0/0/1
O   172.29.4.128/25 [110/65] via 172.29.6.10, 00:09:12, Serial0/1/0
C   172.29.6.0/30 is directly connected, Serial0/0/1
L   172.29.6.1/32 is directly connected, Serial0/0/1
O   172.29.6.4/30 [110/128] via 172.29.6.10, 00:09:12, Serial0/1/0
    [110/128] via 172.29.6.2, 00:09:12, Serial0/0/1
C   172.29.6.8/30 is directly connected, Serial0/1/0
L   172.29.6.9/32 is directly connected, Serial0/1/0
C   172.29.6.12/30 is directly connected, Serial0/1/1
L   172.29.6.13/32 is directly connected, Serial0/1/1
209.17.220.0/24 is variably subnetted, 2 subnets, 2 masks
C   209.17.220.0/30 is directly connected, Serial0/0/0
L   209.17.220.2/32 is directly connected, Serial0/0/0
S*  0.0.0.0/0 [1/0] via 209.17.220.1
```

Autor: Fuente propia

En las ilustraciones siguientes podemos ver los routers Medellín2 y Bogotá2 que también presentan redes conectadas directamente y recibidas mediante OSPF.

Figura 31 Redes conectadas directamente y recibidas mediante OSPF

```
MEDELLIN2
Physical Config CLI Attributes
IOS Command Line Interface
Medellin2#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is 172.29.6.1 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 [110/129] via 172.29.6.1, 00:13:58, Serial0/0/0
C 172.29.6.0/30 is directly connected, Serial0/0/0
L 172.29.6.2/32 is directly connected, Serial0/0/0
C 172.29.6.4/30 is directly connected, Serial0/0/1
L 172.29.6.5/32 is directly connected, Serial0/0/1
O 172.29.6.8/30 [110/128] via 172.29.6.1, 00:14:08, Serial0/0/0
O 172.29.6.12/30 [110/128] via 172.29.6.1, 00:14:08, Serial0/0/0
O*E2 0.0.0.0/0 [110/1] via 172.29.6.1, 00:14:08, Serial0/0/0
Medellin2#
```

Autor: Fuente propia

Figura 32 redes conectadas directamente y recibidas mediante OSPF

```
BOGOTA2
Physical Config CLI Attributes
IOS Command Line Interface
Bogota2#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is 172.29.3.1 to network 0.0.0.0

172.29.0.0/16 is variably subnetted, 10 subnets, 3 masks
C 172.29.0.0/24 is directly connected, GigabitEthernet0/0
L 172.29.0.1/32 is directly connected, GigabitEthernet0/0
O 172.29.1.0/24 [110/129] via 172.29.3.1, 00:19:35, Serial0/0/0
C 172.29.3.0/30 is directly connected, Serial0/0/0
L 172.29.3.2/32 is directly connected, Serial0/0/0
C 172.29.3.4/30 is directly connected, Serial0/1/0
L 172.29.3.6/32 is directly connected, Serial0/1/0
O 172.29.3.8/30 [110/128] via 172.29.3.1, 00:19:45, Serial0/0/0
C 172.29.3.12/30 is directly connected, Serial0/0/1
L 172.29.3.13/32 is directly connected, Serial0/0/1
O*E2 0.0.0.0/0 [110/1] via 172.29.3.1, 00:19:45, Serial0/0/0
```

Autor: Fuente propia

Se configuran los routers restantes de tal forma que sus tablas permitan 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, como se logra ver en las siguientes figuras:

Figura 33 Rutas conectadas directamente ISP

```

ISP#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B -
BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       I - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     172.29.0.0/22 is subnetted, 2 subnets
S       172.29.0.0/22 [1/0] via 209.17.220.6
S       172.29.4.0/22 [1/0] via 209.17.220.2
     209.17.220.0/24 is variably subnetted, 4 subnets, 2 masks
C       209.17.220.0/30 is directly connected, Serial0/0/0
L       209.17.220.1/32 is directly connected, Serial0/0/0
C       209.17.220.4/30 is directly connected, Serial0/0/1
L       209.17.220.5/32 is directly connected, Serial0/0/1
ISP#
  
```

Autor: Fuente propia

Parte 3: Deshabilitar la propagación del protocolo OSPF.

a. Con base en la siguiente tabla se realiza la configuración para no propagar las publicaciones por interfaces que no lo requieran se deshabilitan la propagación del protocolo OSPF, como se indica a continuación:

Tabla 24 Deshabilitar la Propagación del Protocolo OSPF

ROUTER	INTERFAZ
Bogota1	SERIAL0/0/1; SERIAL0/1/0; SERIAL0/1/1
Bogota2	SERIAL0/0/0; SERIAL0/0/1
Bogota3	SERIAL0/0/0; SERIAL0/0/1; SERIAL0/1/0
Medellín1	SERIAL0/0/0; SERIAL0/0/1; SERIAL0/1/1
Medellín2	SERIAL0/0/0; SERIAL0/0/1

Medellín3	SERIAL0/0/0; SERIAL0/0/1; SERIAL0/1/0
ISP	No lo requiere

```
Bogota1(config)#router ospf 1
Bogota1(config-router)#passive-interface s0/0/0
```

```
Bogota2(config)#router ospf 1
Bogota2(config-router)#passive-interface g0/0
```

```
Bogota3(config)#router ospf 1
Bogota3(config-router)#passive-interface g0/0
```

```
Medellin1(config)#router ospf 1
Medellin1(config-router)#passive-interface s0/1/0
```

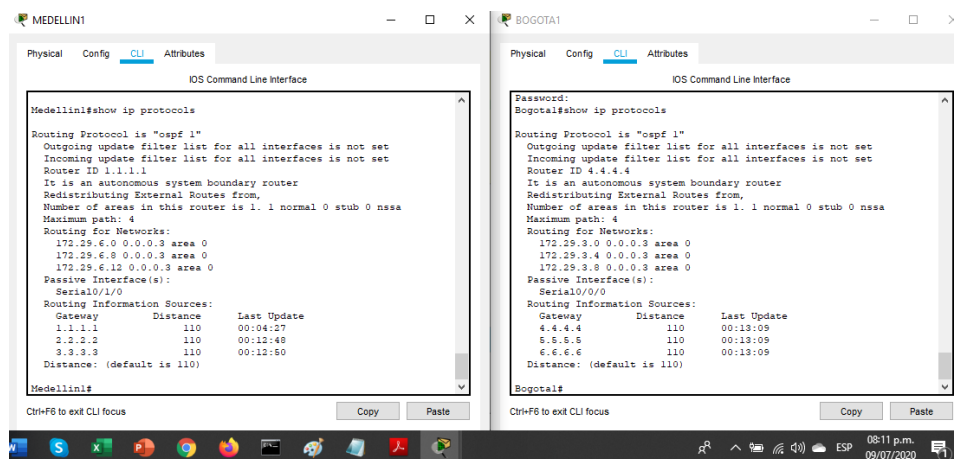
```
Medellin2(config)#router ospf 1
Medellin2(config-router)#passive-interface g0/0
```

```
Medellin3(config)#router ospf 1
Medellin3(config-router)#passive-interface g0/0
```

Parte 4: Verificación del protocolo OSPF.

Utilizamos el comando “show ip protocols” para verificar 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.

Figura 34 Verificación del protocolo OSPF en ruter Bogota1 y Medellin1

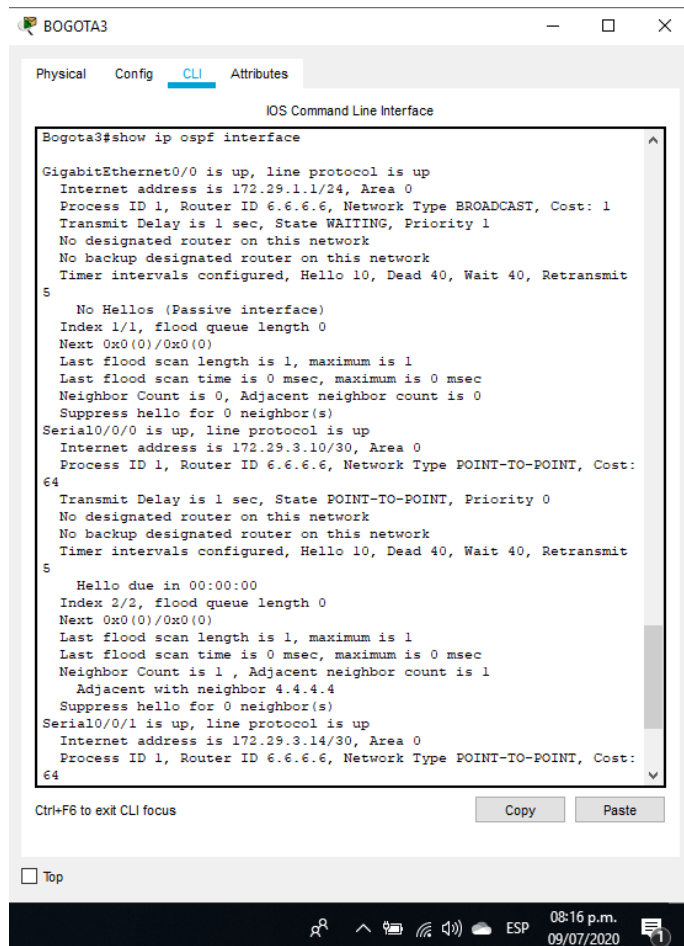


Autor: Fuente propia

Mediante el comando “show ip ospf interface se verifica la base de datos de OSPF de cada router, donde se informa de manera detallada de todas las rutas hacia cada red. Como lo vemos a continuacon

A través del comando show ip ospf interface se puede obtener una lista detallada de todas las interfaces.

Figura 35 BOGOTA3 show ip ospf interface



```
Bogota3#show ip ospf interface
GigabitEthernet0/0 is up, line protocol is up
  Internet address is 172.29.1.1/24, Area 0
  Process ID 1, Router ID 6.6.6.6, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State WAITING, Priority 1
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit
  5
    No Hellos (Passive interface)
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
Serial0/0/0 is up, line protocol is up
  Internet address is 172.29.3.10/30, Area 0
  Process ID 1, Router ID 6.6.6.6, Network Type POINT-TO-POINT, Cost:
  64
  Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit
  5
    Hello due in 00:00:00
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 4.4.4.4
  Suppress hello for 0 neighbor(s)
Serial0/0/1 is up, line protocol is up
  Internet address is 172.29.3.14/30, Area 0
  Process ID 1, Router ID 6.6.6.6, Network Type POINT-TO-POINT, Cost:
  64
```

Autor: Fuente propia

Parte 5: Configurar encapsulamiento y autenticación PPP.

Realizamos las respectivas configuraciones según la topología para que el enlace Medellín1 con ISP sea configurado con autenticación PAT como se muestra en las siguientes líneas de código:

```
Medellin1(config)#username ISP password cisco
Medellin1(config)#int s0/0/0
Medellin1(config-if)#encapsulation ppp
Medellin1(config-if)#ppp authentication chap
Medellin1(config-if)#encapsulation ppp
Medellin1(config-if)#ppp authentication pap
Medellin1(config-if)#ppp pap sent-username
Medellin1 password cisco
```

```
ISP(config)#username Medellin1 password cisco
ISP(config)#int s0/0/0
ISP(config-if)#encapsulation ppp
ISP(config-if)#ppp authentication pap
ISP(config-if)#ppp pap sent-username ISP password cisco
```

De igual forma se realiza los respectivo para el enlace Bogotá1 con ISP con autenticación CHAT, mediante las siguientes líneas de código:

```
ISP(config)#username Bogota1 password cisco
ISP(config)#int s0/0/1
ISP(config-if)#encapsulation ppp
ISP(config-if)#ppp authentication chap
```

```
Bogota1(config)#username ISP password cisco
Bogota1(config)#int s0/0/0
Bogota1(config-if)#encapsulation ppp
Bogota1(config-if)#ppp authentication chap
```

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 procedemos a configurar el NAT en el router Medellín1 y así comprobamos que la traducción de direcciones indique las interfaces de entrada y de salida. Y los verificamos 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.

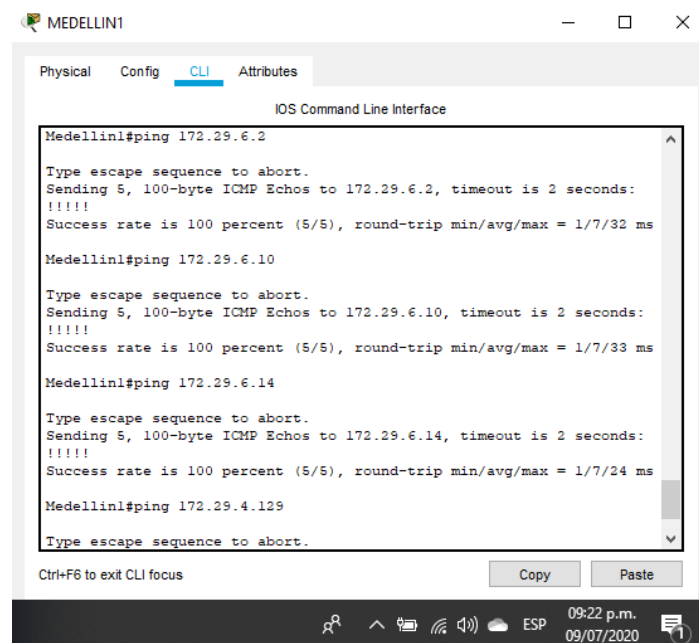
```
Medellin1(config)#ip nat inside source list 1 interface s0/0/0 overload
Medellin1(config)#access-list 1 permit 172.29.4.0 0.0.3.255
Medellin1(config)#int s0/0/0
Medellin1(config-if)#ip nat outside
```

```
Medellin1(config-if)#int s0/0/1
Medellin1(config-if)#ip nat inside
Medellin1(config-if)#int s0/1/0
Medellin1(config-if)#ip nat inside
Medellin1(config-if)#int s0/1/1
Medellin1(config-if)#ip nat inside
```

Luego procedemos a configurar el NAT en el router Bogotá1 y comprobamos que la traducción de direcciones este indicando las interfaces de entrada y de salida. Y lo verificamos 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(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)#int s0/0/0
Bogota1(config-if)#ip nat outside
Bogota1(config-if)#int s0/0/1
Bogota1(config-if)#ip nat inside
Bogota1(config-if)#int s0/1/0
Bogota1(config-if)#ip nat inside
Bogota1(config-if)#int s0/1/1
Bogota1(config-if)#ip nat inside
```

Figura 36 Ping desde Medellin1 a las direcciones de las interfaces



The screenshot shows a terminal window titled 'MEDELLIN1' with tabs for 'Physical', 'Config', 'CLI', and 'Attributes'. The 'CLI' tab is active, displaying the 'IOS Command Line Interface'. The terminal output shows four successful ping commands from 'Medellin1' to the following IP addresses: 172.29.6.2, 172.29.6.10, 172.29.6.14, and 172.29.4.129. Each ping command is followed by a series of five exclamation marks (!!!!!) and a success rate of 100 percent (5/5). The round-trip times are 1/7/32 ms for the first three pings and 1/7/24 ms for the last one. The terminal also shows the prompt 'Type escape sequence to abort.' before each ping command. At the bottom of the terminal window, there are 'Copy' and 'Paste' buttons and a status bar with the text 'Ctrl+F6 to exit CLI focus'. The system tray at the bottom of the window shows the time as 09:22 p.m. on 09/07/2020.

Autor: Fuente propia

Parte 7: Configuración del servicio DHCP.

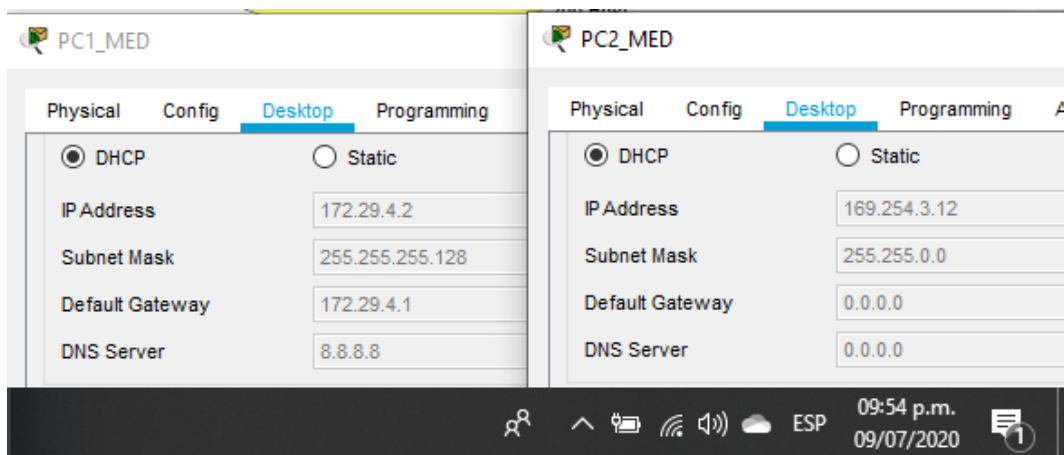
En este paso vamos a configurar la red Medellín2 y Medellín3 donde el router Medellín 2 es el servidor DHCP para ambas redes LAN.

El router Medellín3 se habilita para el paso de los mensajes broadcast hacia la IP del router Medellín2 mediante las siguiente líneas de código:

```
Medellin2(config)#ip dhcp excluded-address 172.29.4.1 172.29.4.10
Medellin2(config)#ip dhcp excluded-address 172.29.4.129 172.29.4.138
Medellin2(config)#ip dhcp pool MEDELLIN2
Medellin2(dhcp-config)#net 172.29.4.0 255.255.255.128
Medellin2(dhcp-config)#default-router 172.29.4.1
Medellin2(dhcp-config)#dns-server 0.0.0.0
Medellin2(dhcp-config)#exit
Medellin2(config)#ip dhcp pool MEDELLIN3
Medellin2(dhcp-config)#net 172.29.4.128 255.255.255.128
Medellin2(dhcp-config)#default-router 172.29.4.129
Medellin2(dhcp-config)#dns-server 0.0.0.0
Medellin2(dhcp-config)#exit
```

```
Medellin3(config)#int g0/0
Medellin3(config-if)#ip helper-address 172.29.6.5
```

Figura 37 PC1_MED y PC2_MED dirección ip a través de DHCP



Autor: Fuente propia

Vamos finalizando con la configuración de la red Bogotá2 y Bogotá3 donde el router Medellín2 es el servidor DHCP para ambas redes LAN.

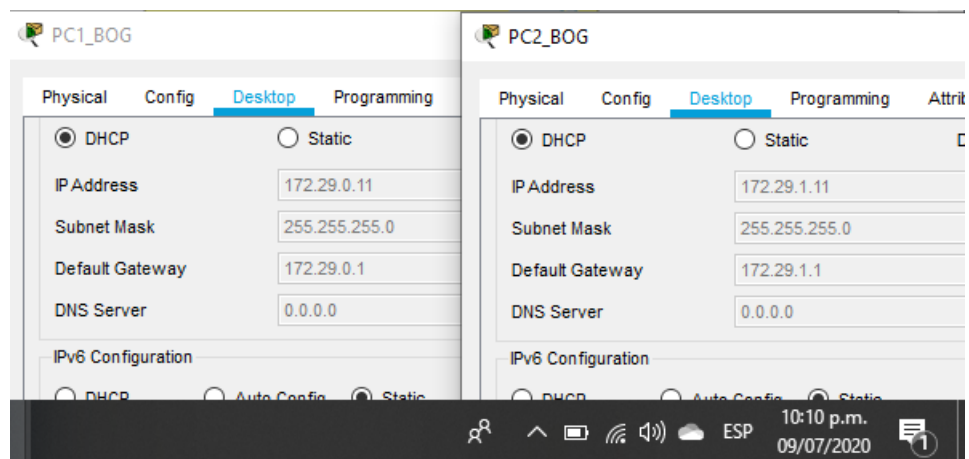
Se configura el router Bogotá1 para que habilite el paso de los mensajes

Broadcast hacia la IP del router Bogotá2 a continuación se especifica la configuración y se verifica como se ve en la siguiente figura:

```
Bogota2(config)#ip dhcp excluded-address 172.29.1.1 172.29.1.10
Bogota2(config)#ip dhcp excluded-address 172.29.0.1 172.29.0.10
Bogota2(config)#ip dhcp pool BOGOTA2
Bogota2(dhcp-config)#net 172.29.1.0 255.255.255.0
Bogota2(dhcp-config)#default-router 172.29.1.1
Bogota2(dhcp-config)#dns-server 0.0.0.0
Bogota2(dhcp-config)#exit
Bogota2(config)#ip dhcp pool BOGOTA3
Bogota2(dhcp-config)#net 172.29.0.0 255.255.255.0
Bogota2(dhcp-config)#default-router 172.29.0.1
Bogota2(dhcp-config)#dns-server 0.0.0.0
```

```
Bogota3(config)#int g0/0
Bogota3(config-if)#ip helper-address 172.29.3.13
```

Figura 38 PC1_BOG y PC2_BOG dirección ip a través de DHCP



Autor: Fuente propia

Archivos PRUEBA_DE_HABILIDADES_CCNA_2020_16-02_ECENARIO_1 y 2
<https://drive.google.com/drive/folders/1vmrmYTz78OVcyhhJXwhyuwiBMUCVqIRN?usp=sharing>

CONCLUSIÓN

Con este escenario se realiza la configuración de una red pequeña en donde se implementan los protocolos IPV4 e IPV6.

Se configura la seguridad del switch, las VLAN y routing entre VLAN, también se utiliza 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

Se logra entender al configurar e interconectar los dispositivos que se encuentran en dos ciudades utilizando el protocolo OSPF y habilitando el encapsulamiento PPP y su autenticación, finalmente se proporciona el servicio DHCP en las LAN y se habilita NAT de sobrecarga en los router.

Así logramos evidenciar por nuestros propios medios apoyo del tutor y diferentes herramientas que nos brindan para aclarar y obtener un buen desempeño durante el desarrollo del escenario propuesto.

REFERENCIAS BIBLIOGRAFICAS

Archivos PRUEBA_DE_HABILIDADES_CCNA_2020_16-02_ECENARIO_1 y 2
<https://drive.google.com/drive/folders/1vmrmYTz78OVcyhhJXwhyuwiBMUCVqIRN?usp=sharing>

Cisco Networking Academy, MODULO DE ESTUDIO CCNA1(Network Fundamentals). Recuperado de: <http://www.mediafire.com/?9cq9h4jo23c1359>

Cisco Networking Academy, MODULO DE ESTUDIO CCNA2 (Routing Protocols and Concepts). Recuperado de: <http://www.mediafire.com/?5y052miul2vezhj>

Cisco CCNA – configuración DHCP en un router. Recuperado de: <http://blog.capacityacademy.com/2014/01/09/cisco-ccna-como-configurar-dhcp-encisco-router/>

Cisco CCNA - configuración troncal 802.1Q. En un switch recuperado de: https://www.cisco.com/c/es_mx/support/docs/switches/catalyst-4000-seriesswitches/24064-171.html

CISCO. CCNA. Enrutamiento entre VLANs. Principios de Enrutamiento y Conmutación. Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE50ES/module5/index.html#5.0.1.1>

Reyes Reynaud, M, A. 2011. Cálculo de Subredes de México. [Video] recuperado de:
http://www.youtube.com/watch?v=Z7DM639rAmQ&list=PLaXGHu_K17nuWSyLNRtX7UvR2LcpTBK7P&index=5