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

HECTOR JHAIR LESMES CORREAL

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD-
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA-ECBTI-
INGENIERIA ELECTRONICA
BOGOTÁ
2020

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

HECTOR JHAIR LESMES CORREAL

INFORME FINAL PARA OPTAR POR EL TITULO DE INGENIERIA ELECTRONICA

Director
Phd. JUAN CARLOS VESGA

Tutor
Msc. HECTOR JULIAN PARRA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA-ECBTI-
INGENIERIA ELECTRONICA
BOGOTÁ
2020

Nota de Aceptación

Presidente del Jurado

Jurado

Jurado

Bogotá, 15 de Mayo de 2020

Dedico este trabajo principalmente a DIOS, a mi Abuelo Jorge Correal, Padres Nancy correal y Héctor Lesmes, Hermanos, Esposa Alejandra y Mi Hija Sara, a las personas que me acompañaron en este proceso y apoyaron con gran esmero en cumplir este sueño.

AGRADECIMIENTOS

Agradezco a DIOS por haberme dado la vida y permitirme el haber llegado hasta este momento tan importante de mi formación profesional y a mi familia, a la universidad nacional abierta y a distancia **UNAD** a la escuela de ciencias básicas, tecnología e ingeniería, a los tutores con los que lleve a cabalidad mis cursos a las diferentes empresas en las que emprendí labores en donde tuve que usar mis conocimientos adquiridos, agradecer a los Ingenieros Julián Camilo Gutiérrez y Mauro Alejandro Ávila por su total apoyo en este proceso de formación académica.

CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE ANEXOS

RESUMEN

En el siguiente trabajo se realiza el desarrollo de dos casos propuestos en el diplomado de profundización cisco (diseño e implementación de soluciones integradas LAN / WAN), en donde tenemos que aplicar las diferentes temáticas aprendidas en el transcurso y desarrollo del diplomado cisco como la configuración básica de dispositivos usados dentro de una red cisco, configuración de dispositivos en redes Vlan, configuración y sistema de seguridad, utilización del protocolo **OSPF**,Encapsulamiento y verificación de **PPP**, configuración de **DHCP** y **NAT.**

PALABRAS CLAVE:

WAN: Una red de área amplia, o WAN (Wide Área Network en inglés), es una red de computadoras que une varias redes locales, aunque sus miembros no estén todos en una misma ubicación física.

LAN: Entre las redes informáticas se encuentra la llamada red LAN, una sigla que refiere a Local Área Network (Red de Área Local). Estas redes vinculan computadoras que se hallan en un espacio físico pequeño, como una oficina o un edificio. La interconexión se realiza a través de un cable o de ondas

PING: Packet Internet Groper. Este comando se utiliza para comprobar si una determinada interfaz de red, de nuestra computadora o de otra, se encuentra activa. El PING envía paquetes al IP o host que se le indique, y nos dice cuanto tiempo demoró el paquete en ir y regresar, entre otras pocas informaciones.

OSPF: Abrir el camino más corto primero en español, es un protocolo de red para encaminamiento jerárquico de pasarela interior o Interior Gateway Protocol (IGP), que usa el algoritmo Dijkstra, para calcular la ruta más corta entre dos nodos.

1. INTRODUCCIÓN

Existe la necesidad en el mundo de adquirir conocimiento acerca de las redes, que junto con la tecnología, se han convertido en un pilar para la sociedad, en la que los técnicos tecnólogos e ingenieros resuelvan los diferentes problemas que se puedan presentar en la conectividad tanto como el mantenimiento y su debida administración.

Durante el desarrollo de este diplomado se han manejado las herramientas y configuraciones básicas para desarrollar a cabalidad la prueba de habilidades prácticas estos ejercicios propuestos nos servirán para administrar redes donde surgen diferente inconvenientes en los cuales los ingenieros deben solucionar y así afianzar con su conocimiento, utilizando protocolos de como OSPF o RIP configuración de Dhcp,Nat,Vlan así como los diferentes comandos utilizados para configurar cada uno de los componentes de una red, también conocer la topología y hacer las conexiones necesarias y utilizar las diferentes tarjetas que puede contener un router, un switch o un servidor al igual este programa de packet tracer de cisco es un buen simulador ya que los resultados están en tiempo real con los diferentes comandos para tazar y ver configuraciones aplicadas.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

- Que el estudiante sea capaz desarrollar los ejercicios propuestos con las herramientas tratadas a lo largo del diplomado conociendo varias el diseño de redes y las diferentes configuraciones en cada dispositivo solicitado.

2.2 OBJETIVOS ESPECÍFICOS

- Usar configuración básica de dispositivos en dispositivos de la red para garantizar cada una de los requerimientos de cliente o los ejercicios propuestos en los dos escenarios

- Usar configuraciones avanzadas para garantizar accesos y seguridad a las redes, usar configuraciones de DHCP, NAT, protocolos de encapsulamiento y verificación de ppp

3 PLANTEAMIENTO DEL PROBLEMA

3.1 DEFINICIÓN DEL PROBLEMA

Se han propuesto dos escenarios en los cuales debemos aplicar todo lo aprendido en el desarrollo del diplomado, en el primer escenario nos piden armar una red y aplicar la configuraciones básicas de consolas, utilizar el protocolo de routing dinámico RIPv2 realizar el montaje de host dinámicos (DHCP)y realizar listas de control de acceso,

En el segundo escenario se describe cómo solucionar un problema de conectividad de distintas áreas de una empresa la cual tiene sus sedes en Bogotá y, Medellín la cual necesita protocolos de enrutamiento y seguridad de acceso a datos.

3.2 JUSTIFICACIÓN

Como principal herramienta para el desarrollo de estos dos escenarios, es el conocimiento adquirido en el diplomado, el simulador y el entorno de CISCO PACKET TRACER, las diferentes configuraciones trabajadas, y comprobar que lo aprendido nos es útil para dar solución a cada uno de los ejercicios propuestos.

4.1 DESARROLLO DE ESCENARIO 1

Escenario 1:

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

TOPOLOGIA

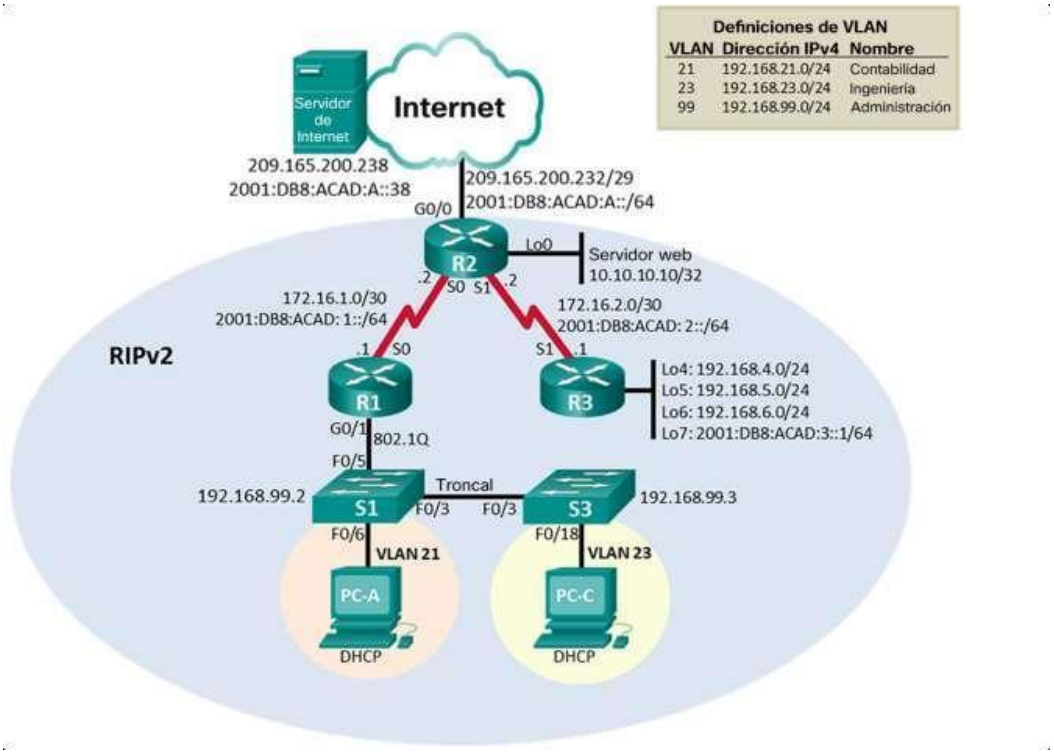


Figura 1. TOPOLOGIA DE RED ESCENARIO 1

Parte 1: Inicializar dispositivos

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

Elimine las configuraciones de inicio y vuelva a cargar los dispositivos. Antes de continuar, solicite al instructor que verifique la inicialización de los dispositivos.

Tabla 1. Inicialización

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	Router>enable Router#erase startup-config Erasing the nvram filesystem will remove all configuration files! Continue? [confirm] [OK]
Volver a cargar todos los routers	Router#reload Proceed with reload? [confirm] System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1) Technical Support: http://www.cisco.com/techsupport Copyright (c) 2010 by cisco Systems, Inc.
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Switch#delete vlan.dat Delete filename [vlan.dat]? Delete flash:/vlan.dat? [confirm]
Volver a cargar ambos switches	Switch#reload Proceed with reload? [confirm] C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(25r)FX, RELEASE SOFTWARE (fc4)Cisco WS-C2960-24TT (RC32300) processor (revisión C0) with 21039K bytes of memory. 2960-24TT starting...
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Switch>ena Switch#show flash Directory of flash:/ 1 -rw- 4414921 <no date> c2960-lanbase-mz.122-25.FX.bin 64016384 bytes total (59601463 bytes free) Switch#

Parte 2: Configurar los parámetros básicos de los dispositivos

Paso 1: Configurar la computadora de Internet

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

Tabla 2. Configuración parámetros básicos de 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:2::1

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

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 3. Configuracion R1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	R1
Contraseña de exec privilegiado cifrada	Class
Contraseña de acceso a la consola	Cisco
Contraseña de acceso Telnet	Cisco
Cifrar las contraseñas de texto no cifrado	R1(config)#enable secret class R1(config)#line console 0 R1(config-line)#pass R1(config-line)#password cisco R1(config-line)#login R1(config-line)#exit R1(config)#line vty 0 4 R1(config-line)#pass R1(config-line)#password cisco R1(config-line)#login R1(config-line)#exit R1(config)#service pass R1(config)#service password-encryption
Mensaje MOTD	R1(config)#banner motd %unauthorized access is prohibited%
Interfaz S0/0/0	Establezca la descripción Establecer la dirección IPv4 Consultar el diagrama de topología para conocer la información de direcciones Establecer la dirección IPv6 Consultar el diagrama de topología para conocer la información de direcciones Establecer la frecuencia de reloj en 128000 Activar la interfaz
Rutas predeterminadas	Configurar una ruta IPv4 predeterminada de S0/0/0 Configurar una ruta IPv6 predeterminada de S0/0/0

Nota: Todavía no configure G0/1.

Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Tabla 4. Configuracion de R2

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	R2
Contraseña de exec privilegiado cifrada	Class
Contraseña de acceso a la consola	Cisco
Contraseña de acceso Telnet	Cisco
Cifrar las contraseñas de texto no cifrado	R2>enable R2#conf t Enter configuration commands, one per line. End with CNTL/Z. R2(config)#enable secret class R2(config)#line console 0 R2(config-line)#pass R2(config-line)#password cisco R2(config-line)#login R2(config-line)#exit R2(config)#line vty 0 4 R2(config-line)#pass R2(config-line)#password cisco R2(config-line)#login R2(config-line)#exit R2(config)#service pass R2(config)#service password-encryption
Habilitar el servidor HTTP	R2(config)#ip http server
Mensaje MOTD	Se prohíbe el acceso no autorizado.

Interfaz S0/0/0	Establezca la descripción Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz
Interfaz S0/0/1	Establecer la descripción Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Establecer la frecuencia de reloj en 128000. Activar la interfaz
Interfaz G0/0 (simulación de Internet)	Establecer la descripción. Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Establezca la dirección IPv6. Utilizar la primera dirección disponible en la subred. Activar la interfaz
Interfaz loopback 0 (servidor web simulado)	Establecer la descripción. Establezca la dirección IPv4.
Ruta predeterminada	Configure una ruta IPv4 predeterminada de G0/0. Configure una ruta IPv6 predeterminada de G0/0.

Paso 4: Configurar R3

La Configuracion Del R3 incluye las siguientes tareas:

Tabla 5. Configuracion R3.

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	R3
Contraseña de exec privilegiado cifrada	Class
Contraseña de acceso a la consola	Cisco
Contraseña de acceso Telnet	Cisco
Cifrar las contraseñas de texto no cifrado	R3(config)#enable secret class R3(config)#line console 0 R3(config-line)#pass R3(config-line)#password cisco R3(config-line)#login R3(config-line)#exit R3(config)#line vty 0 4 R3(config-line)#pass R3(config-line)#password cisco R3(config-line)#login R3(config-line)#exit R3(config)#service pass R3(config)#service password-encryption
Mensaje MOTD	**Se prohíbe el acceso no autorizado.** R3(config)#banner motd #Se prohíbe el acceso no autorizado!#

Interfaz loopback 5	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.
Interfaz loopback 6	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.
Interfaz loopback 7	Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.
Rutas predeterminadas	
Interfaz S0/0/1	Establecer la descripción Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz
Interfaz loopback 4	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.

Paso 5: Configurar S1

La Configuracion del S1 incluye las siguientes tareas:

Tabla 6. Configuracion de **S1**

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch(config)#no ip domain-lookup
Nombre del switch	S1
Contraseña de exec privilegiado cifrada	Class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	S1(config)#enable secret class S1(config)#line console 0 S1(config-line)#pass S1(config-line)#password cisco S1(config-line)#login S1(config-line)#line vty 0 4 S1(config-line)#pass S1(config-line)#password cisco S1(config-line)#login S1(config-line)#service S1(config-line)#servicepass S1(config-line)#service passw S1(config-line)#service password S1(config-line)#service password- S1(config-line)#service password-encryption
Mensaje MOTD	S1(config)#banner motd #Se prohibe el acceso no autorizado!#.

Paso 6: Configurar el S3

La Configuracion Del S3 incluye las siguientes tareas:

Tabla 7. Configuracion de S3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch(config)#no ip domain-lookup
Nombre del switch	S3
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	S3(config)#enable secret class S3(config)#line console 0 S3(config-line)#pass S3(config-line)#password cisco S3(config-line)#login S3(config-line)#line vty 0 4 S3(config-line)#pass S3(config-line)#password cisco S3(config-line)#login S3(config-line)#service pass S3(config-line)#service password-encryption
Mensaje MOTD	S3(config)#banner motd #Se prohibe 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 de conectividad de red

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

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

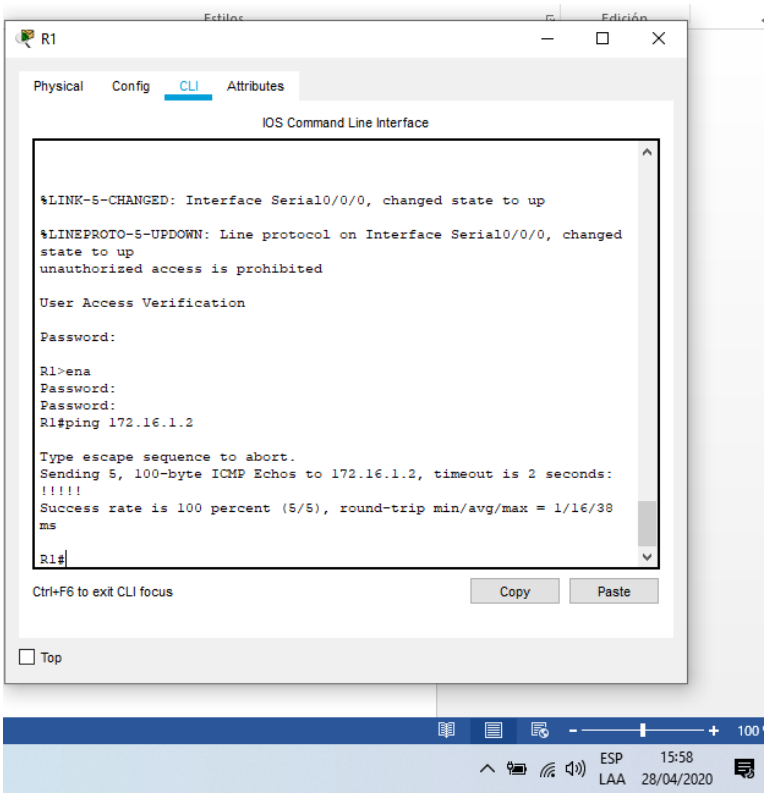


Figura 2. Ping, desde R1 a R2, (172.16.1.2)

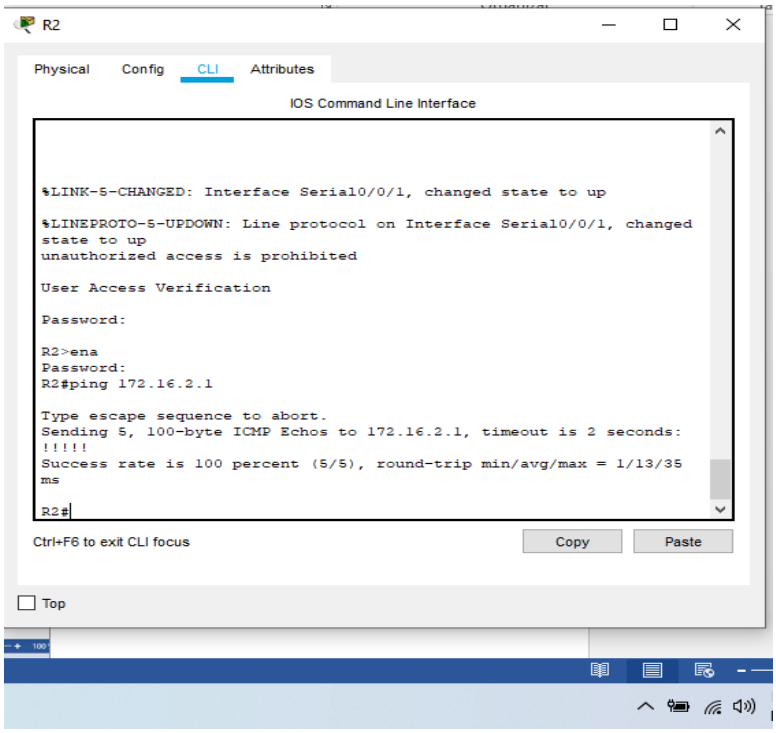


Figura 3. Ping, desde R1 a R2, (172.16.2.1)

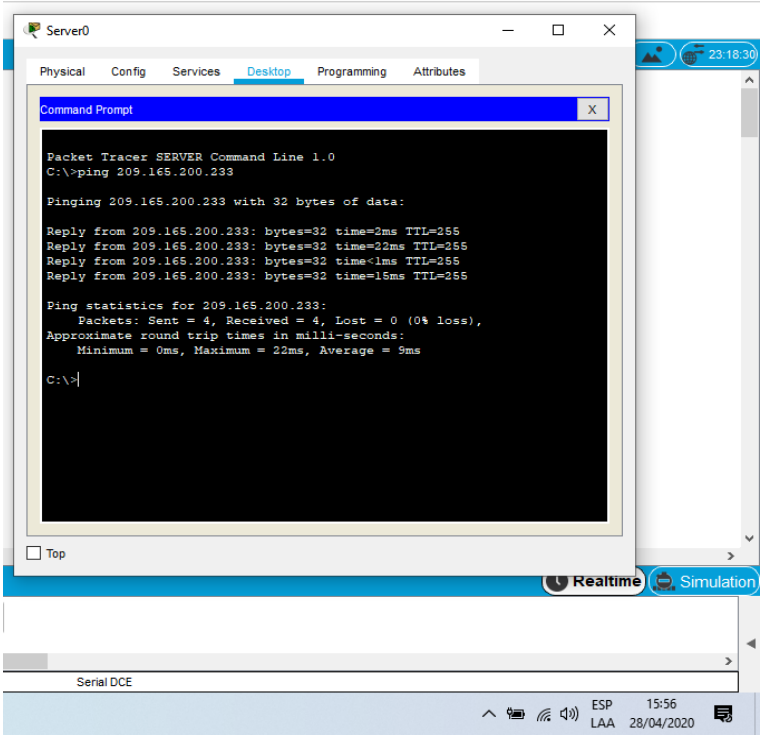


Figura 4.Prueba de ping desde Servidor de Internet a Gateway predeterminado.

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

Paso 1: Configurar S1

La configuración Del S1 incluye las siguientes tareas:

Tabla 9. Configuracion de la seguridad Del switch S1, las VLAN y el routing entre VLAN

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	**Utilizar la tabla de equivalencias de VLAN para topología para crear y nombrar cada una de las VLAN que se indican** S1(config)#vlan 99 S1(config-vlan)#name Administración S1(config-vlan)#vlan 21 S1(config-vlan)#name Contabilidad S1(config-vlan)#vlan 23 S1(config-vlan)#name Ingenieria S1(config-vlan)#exit
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(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)#exit
Asignar el gateway predeterminado	**Asigne la primera dirección IPv4 de la subred como el gateway predeterminado.** S1(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	**Utilizar la red VLAN 1 como VLAN native** S1(config)#interface f0/3 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1 S1(config-if)#exit

Forzar el enlace troncal en la interfaz F0/5	**Utilizar la red VLAN 1 como VLAN native** S1(config)#interface f0/5 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1 S1(config-if)#exit
Configurar el resto de los puertos como puertos de acceso	**Utilizar el comando interface range** S1(config-if)#interface range f0/1, f0/2, f0/4, f0/7-24, g0/1-2 S1(config-if-range)#shutdown
Asignar F0/6 a la VLAN 21	S1(config)#interface f0/6 S1(config-if)#swi S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 21
Apagar todos los puertos sin usar	S1(config-if-range)#shutdown

Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 10. Configuracion de la seguridad del switch S3, las VLAN y el routing entre VLAN

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	**Utilizar la tabla de equivalencias de VLAN para topología para crear cada una de las VLAN que se indican Dé nombre a cada VLAN.** 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 Administración
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(config)#interface vlan 99 S3(config-if)#ip address 192.168.99.3 255.255.255.0 S3(config-if)#no shutdown
Asignar el gateway predeterminado.	**Asignar la primera dirección IP en la subred como gateway predeterminado**. S3(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	**Utilizar la red VLAN 1 como VLAN native** S3config)#interface f0/3 S3(config-if)#swi S3(config-if)#switchport mode trunk S3(config-if)#swi 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, f0/4-17, f0/19-24, g0/1-2 S3(config-if-range)#switchport mode access S3(config-if-range)#shutdown
Asignar F0/18 a la VLAN 23s	S3(config)#int f0/18 S3(config-if)#switchport access vlan 23
Apagar todos los puertos sin usar	S3(config-if-range)#shutdown

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 11. Configuracion de LAN contabilidad, ingeniería y administración

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 R1(config)#interface g0/1.21 R1(config-subif)#description LAN_Contabilidad R1(config-subif)#encapsulation dot1q 21 R1(config-subif)#ip address 192.168.21.2 255.255.255.0 R1(config-subif)#exit
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)#interface g0/1.23 R1(config-subif)#description LAN_Ingenieria R1(config-subif)#encapsulation dot1q 23 R1(config-subif)#ip address 192.168.23.2 255.255.255.0 R1(config-subif)#exit
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)#interface g0/1.99 R1(config-subif)#description LAN_Administracion R1(config-subif)#encapsulation dot1q 99 R1(config-subif)#ip address 192.168.99.1 255.255.255.0 R1(config-subif)#exit
Activar la interfaz G0/1	R1(config-subif)#int g0/1 R1(config-if)#no shutdown

Paso 4: Verificar la conectividad de la red

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

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

Tabla 12. Verificación y pruebas de red VLAN

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

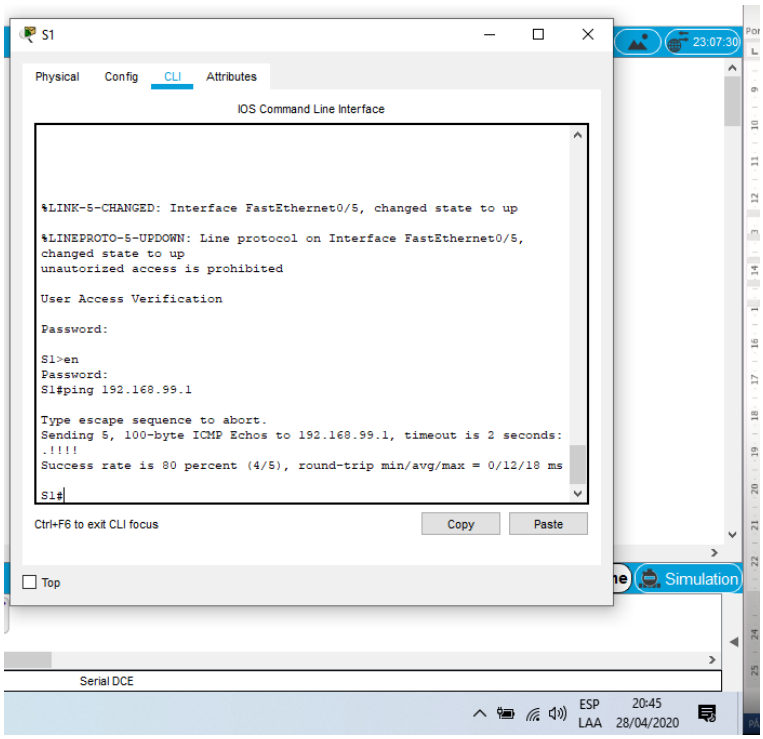


Figura 5.Ping Desde S1 A 192.168.99.1

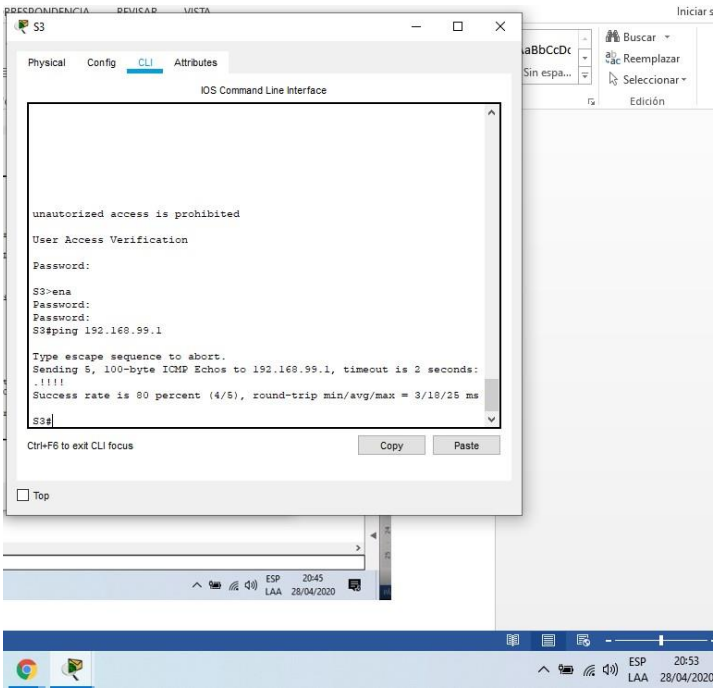


Figura 6.Ping desde s3 a 192.168.99.1

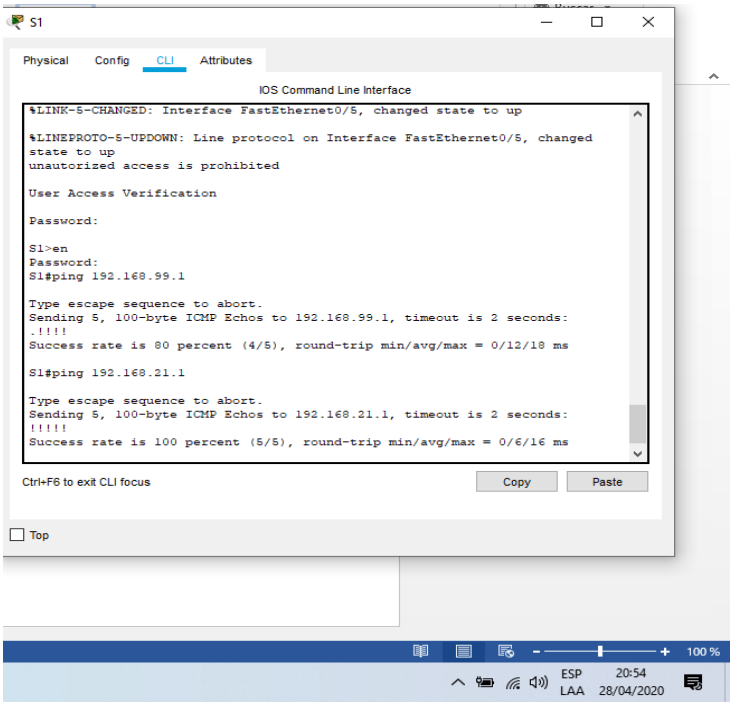


Figura 7.Ping de s1 a 192.168.21.1

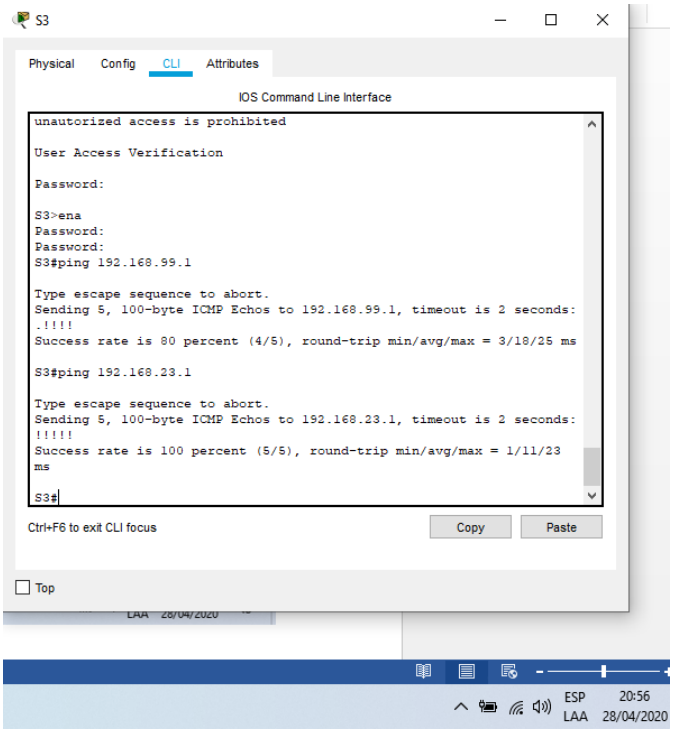


Figura 8.Ping desde S3 a 192.168.23.1

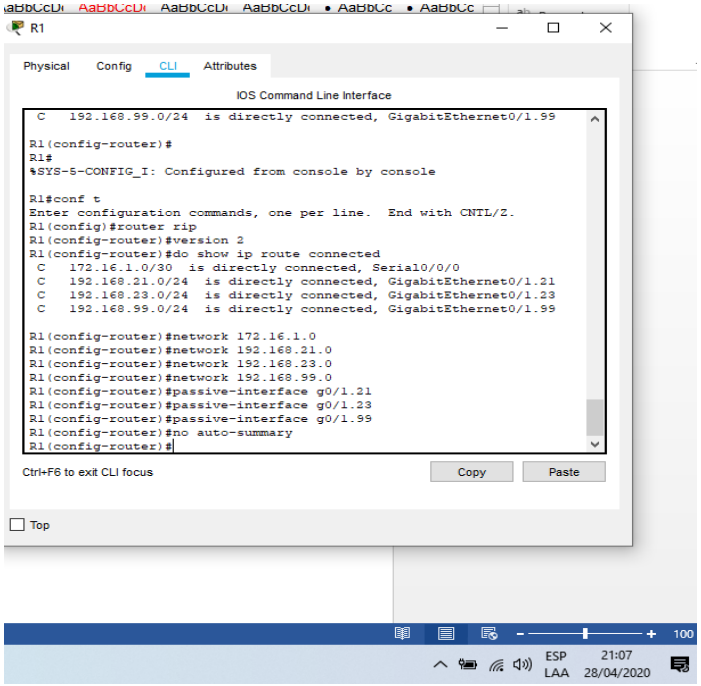
Parte 4: Configurar el protocolo de routing dinámico RIPv2

Paso 1: Configurar RIPv2 en el R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 13. Configuracion RIPv2 en el R1

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	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 172.16.1.8 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 s0/0/0 R1(config-router)#passive-interface g0/1
Desactive la sumarización automática	R1(config-router)#no auto-summary



.**Figura 9. Redes conectadas directamente en R1**

Paso 2: Configurar RIPv2 en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla 14. Configuracion 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	**Nota: Omitir la red G0/0.** R2(config-router)#network 10.10.10.0 R2(config-router)#network 172.16.1.0 R2(config-router)#network 172.16.2.0 R2(config-router)#exit
Establecer la interfaz LAN (loopback) como pasiva	R2(config-router)#passive-interface loopback0
Desactive la sumarización automática.	R2(config-router)#no auto-summary

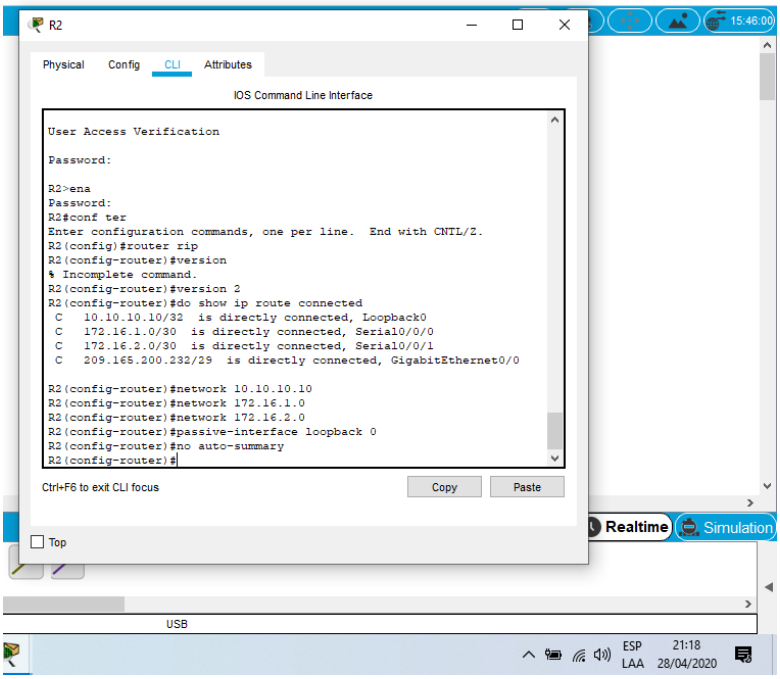


Figura 10. Redes conectadas directamente en R2

Paso 3: Configurar RIPv3 en el R2

La configuración del R3 incluye las siguientes tareas:

Tabla 15. Configuracion RIPv3 en el R2

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 R3(config-router)#exit
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	R3(config-router)#passive-interface loopback4 R3(config-router)#passive-interface loopback5 R3(config-router)#passive-interface loopback6
Desactive la sumarización automática.	R3(config-router)#no auto-summary

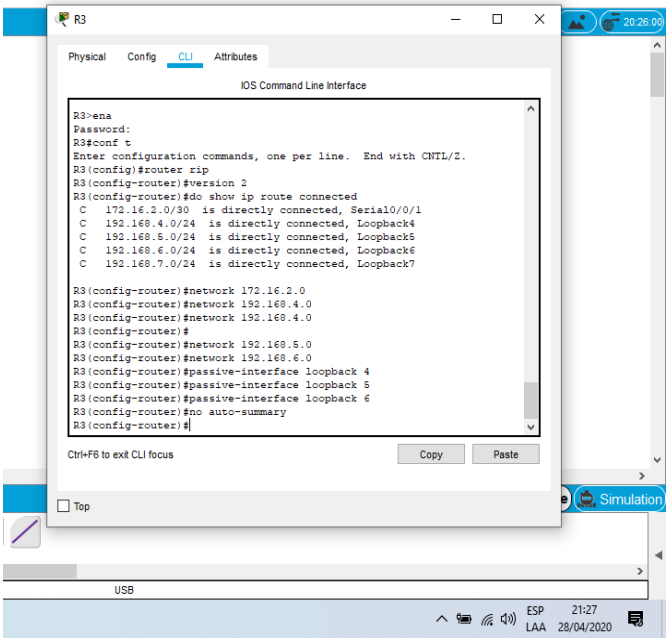


Figura 11. Redes conectadas directamente en R3

Paso 4: Verificar la información de RIP

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

Tabla 16.verificacion de información 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?	R3#show ip protocols
¿Qué comando muestra solo las rutas RIP?	R3#show ip route rip
¿Qué comando muestra la sección de RIP de la configuración en ejecución?	R3#show run

Parte 5: Implementar DHCP y NAT para IPv4

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

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 17.configuracion de R1 para implementar DHCP y NAT para IPv4

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

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

La configuración del R2 incluye las siguientes tareas:

Tabla 18. Configuracion de la NAT estática y dinámica en el R2

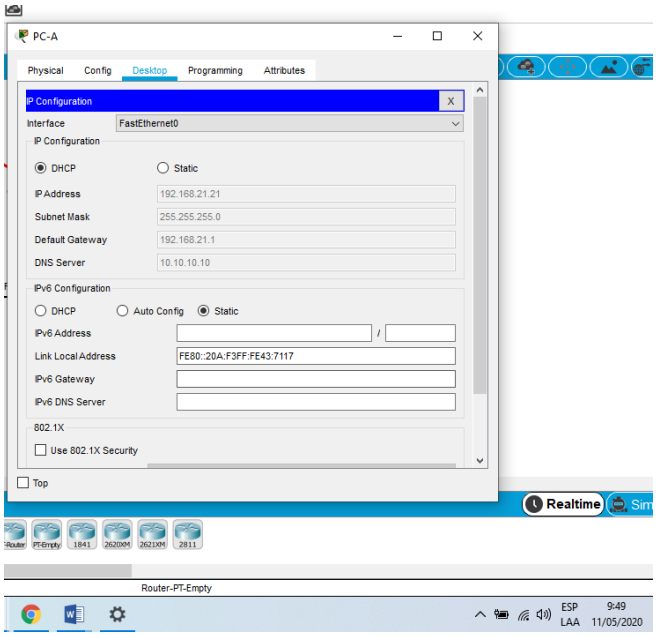
Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	Nombre de usuario: **webuser** Contraseña: **cisco12345** Nivel de privilegio: **15**
Habilitar el servicio del servidor HTTP	R2(config)#ip http server
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	R2(config)#ip http authentication local
Crear una NAT estática al servidor web.	Dirección global interna: **209.165.200.237**
Asignar la interfaz interna y externa para la NAT estática	R2(config)#ip nat inside source static 10.10.10.10 209.165.200.237 R2(config)#int g0/0 R2(config-if)#ip nat outside R2(config-if)#int s0/0/0 R2(config-if)#ip nat inside R2(config-if)#int 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 192.168.4.1 0.0.0.255 R2(config)#access-list 1 permit 192.168.5.1 0.0.0.255 R2(config)#access-list 1 permit 192.168.6.1 0.0.0.255
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**

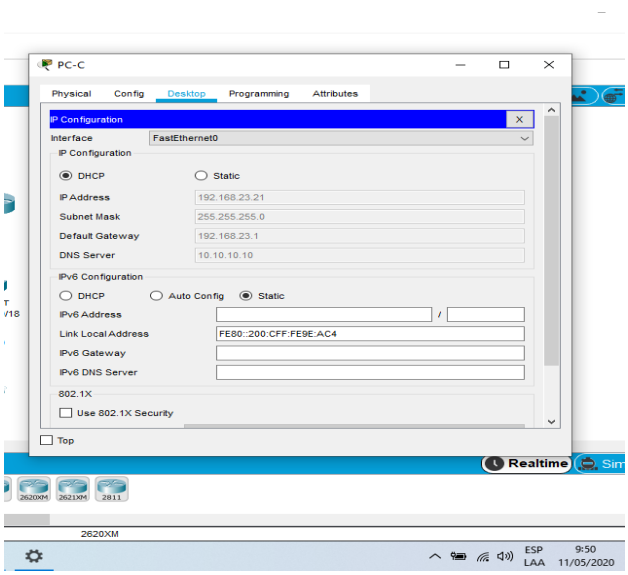
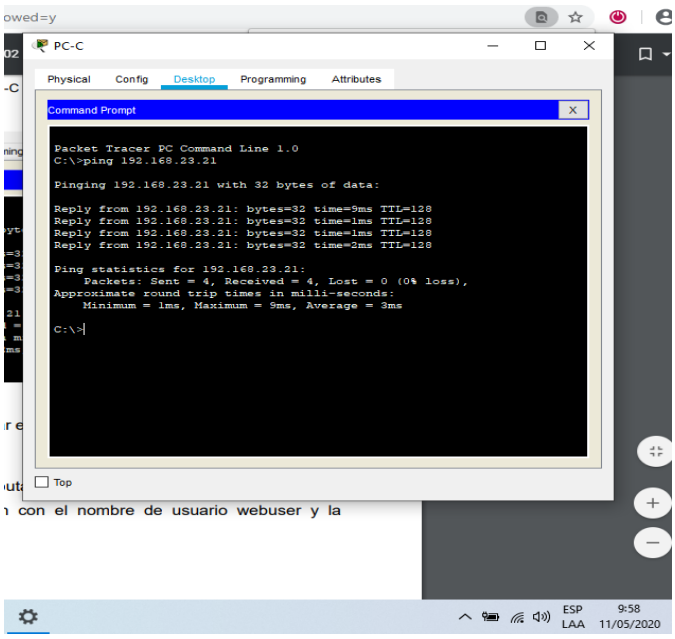
Definir la traducción de NAT dinámica	R2(config)#ip nat pool INTERNET 209.165.200.233 209.165.200.236 netmask 255.255.255.248

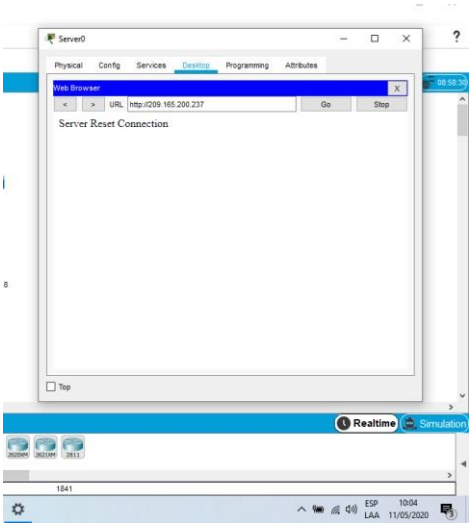
Paso 3: Verificar el protocolo DHCP y la NAT estática

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

Tabla 19. Verificar el protocolo DHCP y la NAT estática

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	

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

Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.229) Iniciar sesión con el nombre de usuario **webuser** y la contraseña **cisco12345**	

Parte 6: Configurar NTP

Tabla 20. Configuracion de NTP

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	R2#clock set 10:22:00 11 may 2020
Configure R2 como un maestro NTP.	Nivel de estrato: **5** R2(config)#ntp master 5 R2(config)#
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.	R1(config)#ntp update-calendar
Verifique la configuración de NTP en R1.	R1(config)#do show ntp status

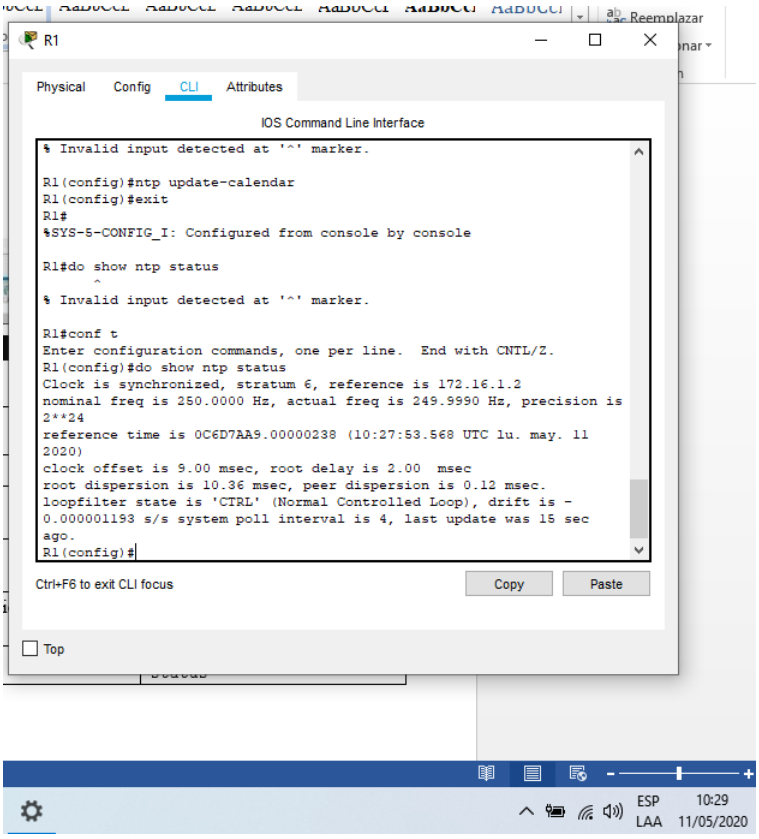


Figura 12.configuracion NTP

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

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

Tabla 21.configuracion 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	Nombre de la ACL: **ADMIN-MGT** R2(config)#ip access-list standard ADMIN-MGT R2(config-std-nacl)#permit host 172.16.1.1 R2(config-std-nacl)#exit
Aplicar la ACL con nombre a las líneas VTY	R2(config)#line vty 0 4 R2(config-line)#access-class ADMIN-MGT in R2(config-line)#exit

Permitir acceso por Telnet a las líneas de VTY	R2(config)#line vty 0 15 R2(config-line)#access-class ADMIN-MGT in R2(config-line)#transport input telnet
Verificar que la ACL funcione como se espera	

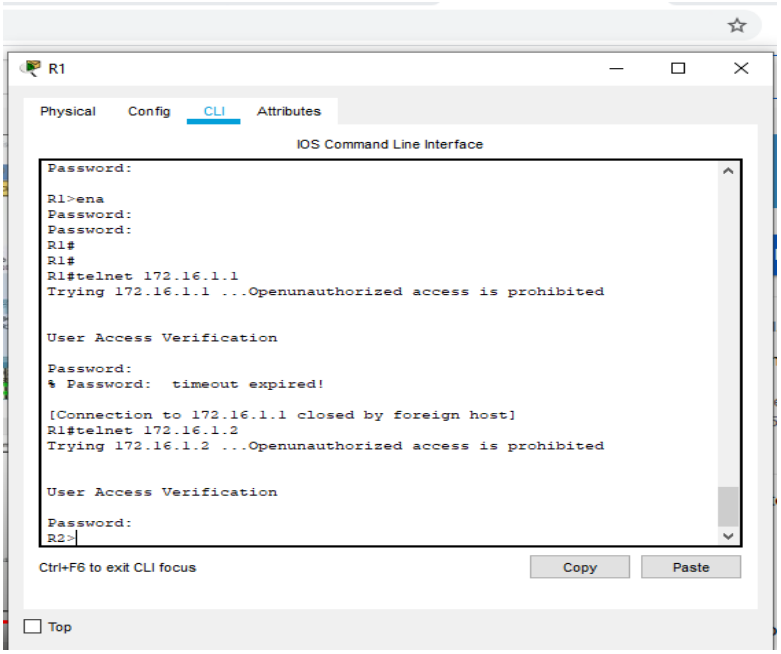


Figura 13.Prueba de Telnet de R1 a R2

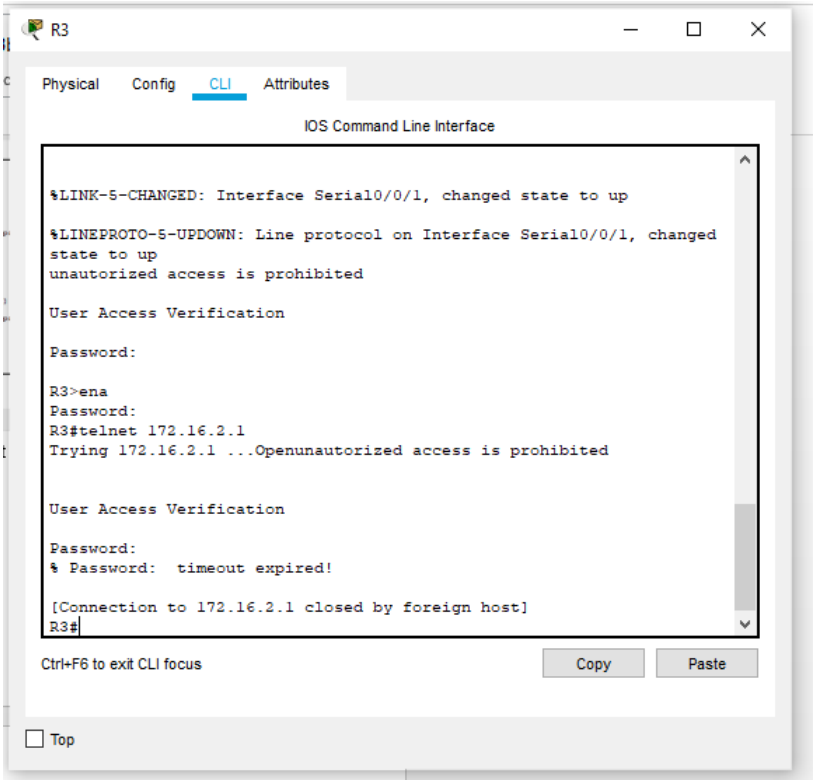


Figura 14.Prueba de Telnet de R3 a R2

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

Tabla 22. Verificación y demostración de configuraciones

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
Restablecer los contadores de una lista de acceso	R2#clear ip access-list counters
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	R2#show ip interface
¿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.
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	Router(config)#clear ip nat translation

4.2 DESARROLLO DE 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.

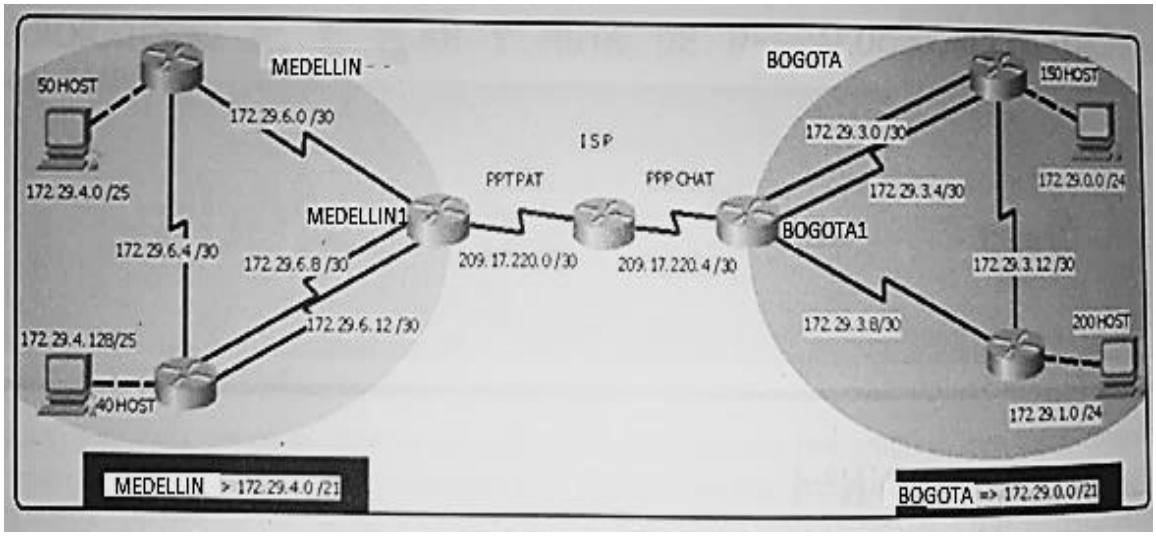


Figura15. Topología de red escenario 2

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

Los routers Bogota2 y medellin2 proporcionan el servicio DHCP a su propia red LAN y a los routers 3 de cada ciudad.
Debe configurar PPP en los enlaces hacia el ISP, con autenticación.
Debe habilitar NAT de sobrecarga en los routers Bogota1 y medellin1.

Desarrollo

Como trabajo inicial se debe realizar lo siguiente.

- Realizar las rutinas de diagnóstico y dejar los equipos listos para su configuración (asignar nombres de equipos, asignar claves de seguridad, etc).
- Realizar la conexión fisica de los equipos con base en la topología de red

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

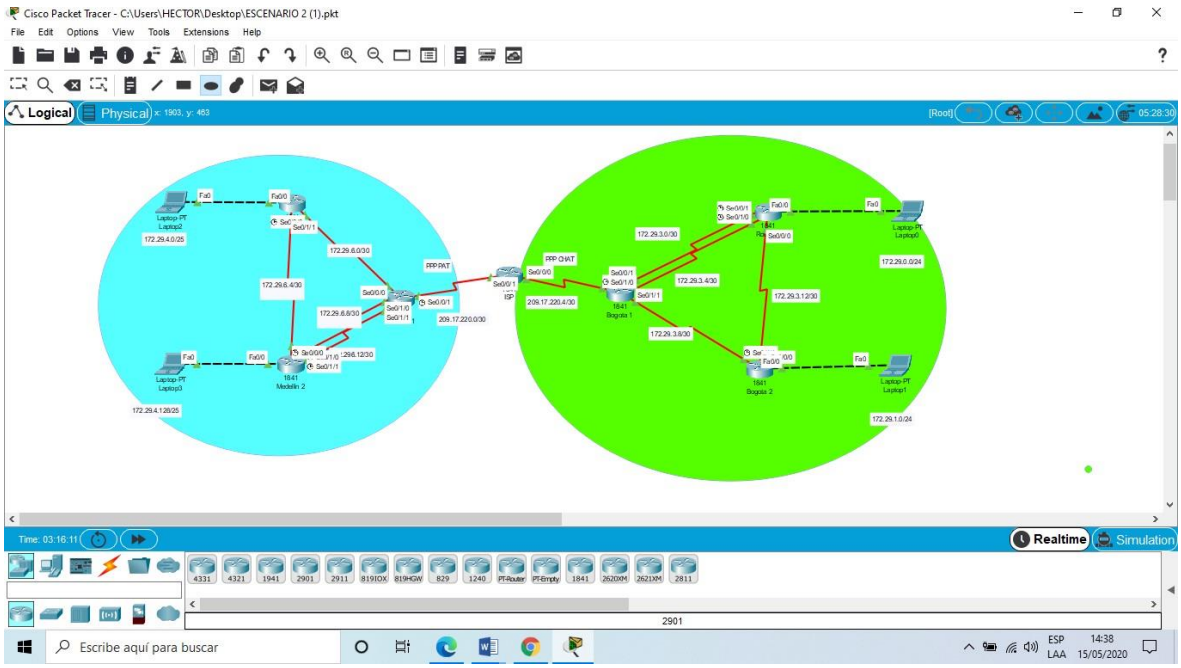


Figura 16. Topología de red escenario 2 estudiante.

Configuración de los routers:

Router(config)#no ip domain-lookup
Router(config)#service password-encryption
Router(config)#enable secret class
Router(config)#banner motd .Prohibido el acceso no autorizado.
Router(config)#line console 0
Router(config-line)#password cisco
Router(config-line)#login
Router(config-line)#line vty 0 4
Router(config-line)#password cisco
Router(config-line)#login
Router(config-line)#exit
Router(config)# Hostname ISP

Parte 1: Configuración del enrutamiento.

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

```
Bogota1(config)#router ospf 1
Bogota1(config-router)#router-id 1.1.1.1
Bogota1(config-router)#network 172.29.3.0 0.0.0.3 area 0
Bogota1(config-router)#network 172.29.3.4 0.0.0.3 area 0
Bogota1(config-router)#network 172.29.3.8 0.0.0.3 area 0
Bogota1(config-router)#network 209.17.220.4 0.0.0.3 area 0
Bogota1(config-router)#no auto-summary
```

```
Medellin1(config)#router ospf 1
Medellin1(config-router)#router-id 4.4.4.4
Medellin1(config-router)#network 172.29.6.0 0.0.0.3 area 0
Medellin1(config-router)#network 172.29.6.4 0.0.0.3 area 0
Medellin1(config-router)#network 172.29.6.8 0.0.0.3 area 0
Medellin1(config-router)#network 209.17.220.0 0.0.0.3 area 0
Medellin1(config-router)#no auto-summary
```

```
Bogota2(config)#router ospf 1
Bogota2(config-router)#router-id 2.2.2.2
Bogota2(config-router)#network 172.29.1.0 0.0.0.255 area 0
Bogota2(config-router)#network 172.29.3.8 0.0.0.3 area 0
Bogota2(config-router)#network 172.29.3.8 0.0.0.3 area 0
Bogota2(config-router)#network 172.29.3.12 0.0.0.3 area 0
Bogota2(config-router)#no auto-summary
Bogota2(config-router)#passive-interface g0/0
```

```
Bogota3(config)#router ospf 1
Bogota3(config-router)#router-id 3.3.3.3
Bogota3(config-router)#network 172.29.0.0 0.0.0.255 area 0
Bogota3(config-router)#network 172.29.3.0 0.0.0.3 area 0
Bogota3(config-router)#network 172.29.3.4 0.0.0.3 area 0
Bogota3(config-router)#network 172.29.3.12 0.0.0.3 area 0
Bogota3(config-router)#no auto-summary
Bogota3(config-router)#passive-interface g0/0

Medellin2(config)#router ospf 1
Medellin2(config-router)#router-id 5.5.5.5
Medellin2(config-router)#network 172.29.4.0 0.0.0.127 area 0
Medellin2(config-router)#network 172.29.6.0 0.0.0.3 area 0
Medellin2(config-router)#network 172.29.6.12 0.0.0.3 area 0
Medellin2(config-router)#no auto-summary
Medellin2(config-router)#passive-interface g0/0

Medellin3(config)#router ospf 1
Medellin3(config-router)#router-id 6.6.6.6
Medellin3(config-router)#network 172.29.4.0 0.0.0.127 area 0
Medellin3(config-router)#network 172.29.6.4 0.0.0.3 area 0
Medellin3(config-router)#network 172.29.6.8 0.0.0.3 area 0
Medellin3(config-router)#network172.29.6.120.0.0.3 area0
Medellin3(config-router)#passive-interface g0/0
Medellin3(config-router)#no auto-summary
```

b. Los routers Bogota1 y Medellín deberán añadir a su configuración de enrutamiento una ruta por defecto hacia el ISP y, a su vez, redistribuirla dentro de las publicaciones de OSPF.

```
Bogota1(config)#ip route 0.0.0.0 0.0.0.0 serial0/0/0
Bogota1(config)#router ospf 1
Bogota1(config-router)#default-information originate
```

```
Medellin1(config)#ip route 0.0.0.0 0.0.0.0 serial0/0/1
Medellin1(config)#router ospf 1
Medellin1(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 sumarizan las subredes de cada uno a /22.

```
ISP(config)#ip route 172.29.4.0 255.255.252.0 serial0/0/1
ISP(config)#ip route 172.29.0.0 255.255.252.0 serial0/0/0
```

Parte 2: Tabla de Enrutamiento.

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

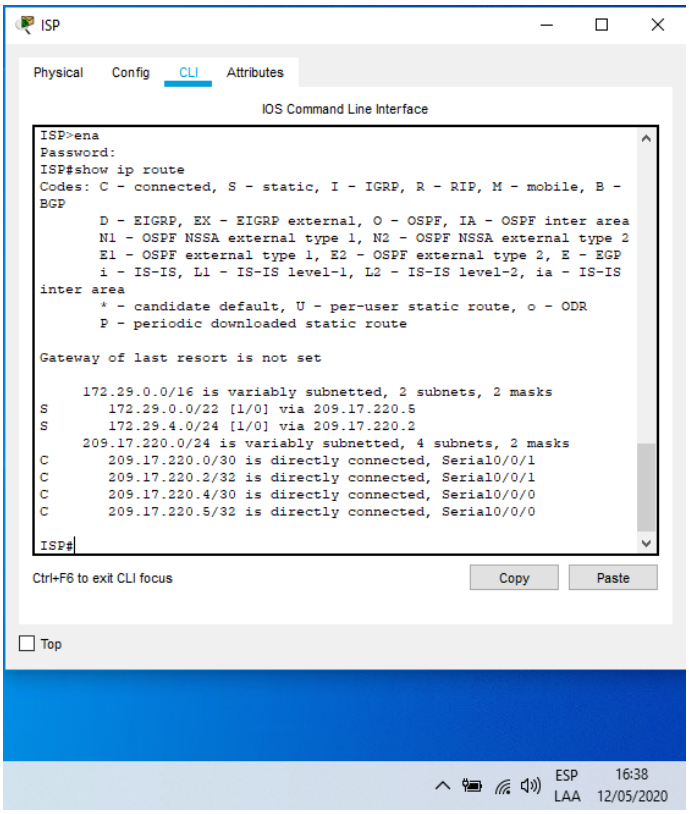


Figura17.configuracion ISP

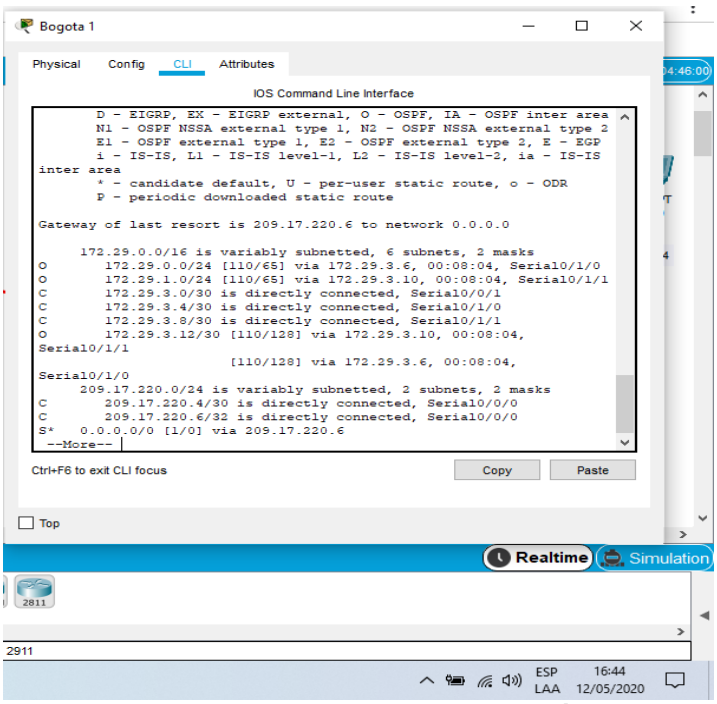


Figura18 .configuracion Bogotá1

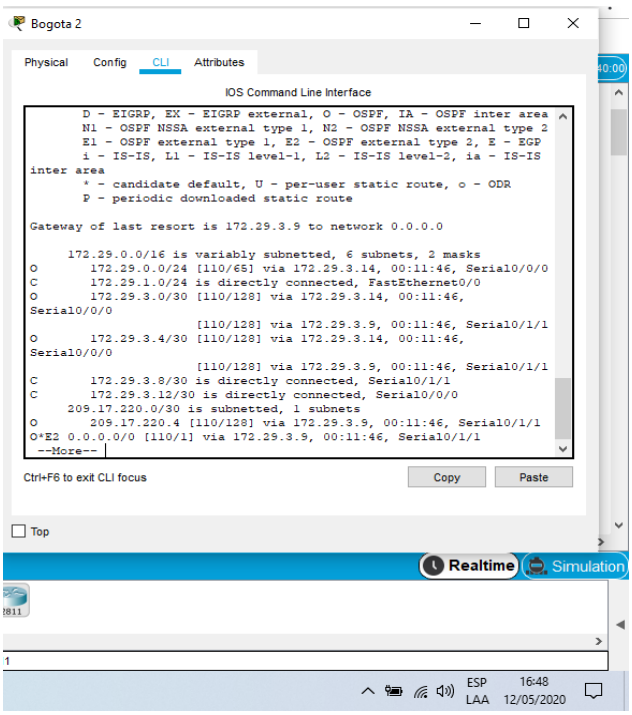


Figura 19.configuracion Bogotá 2

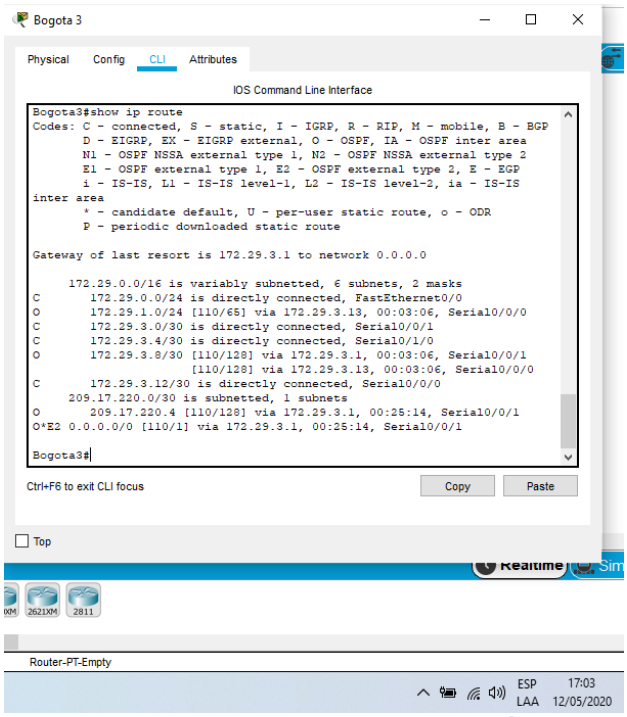


Figura 20.configuracion Bogotá 3:

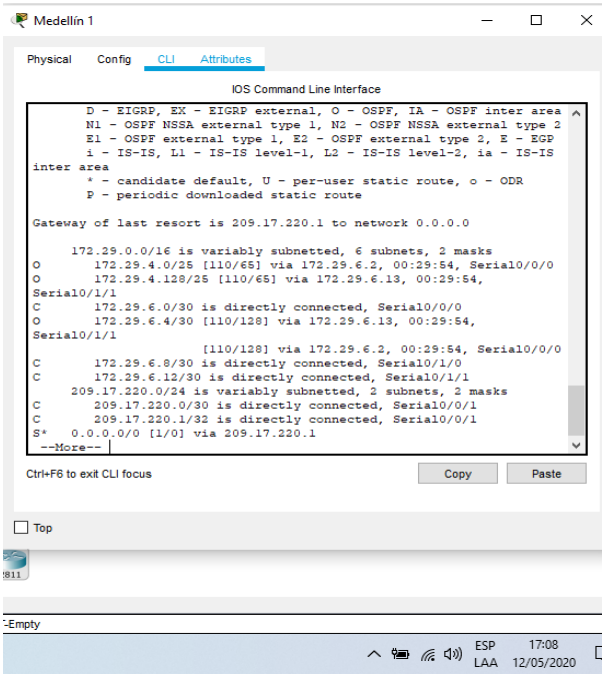


Figura 21.configuracion Medellín 1

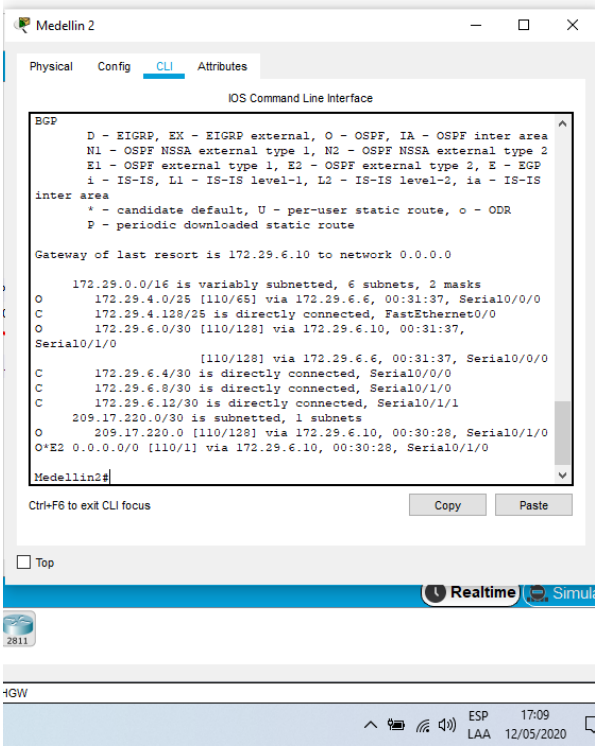


Figura 22. Configuración Medellín 2

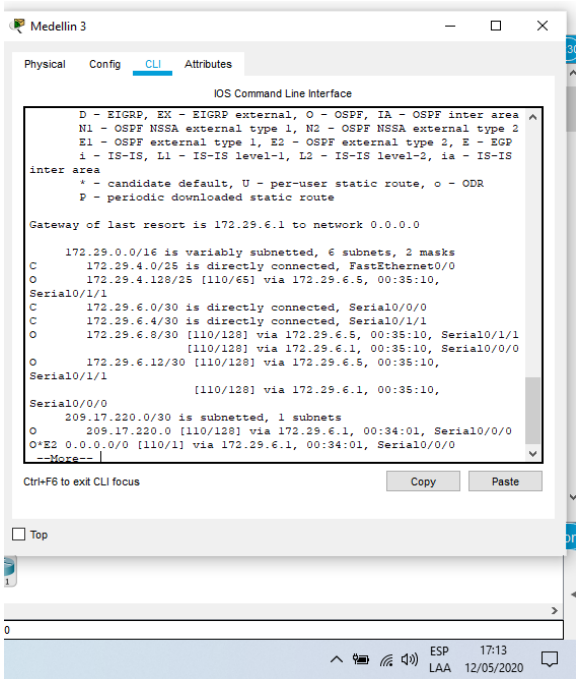


Figura 23 .configuracion Medellin 3

Parte 3: Deshabilitar la propagación del protocolo OSPF.

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

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

Parte 4: Verificación del protocolo OSPF.

a) Verificar y documentar las opciones de enrutamiento configuradas en los routers, como el pasiva interface para la conexión hacia el ISP, la versión de OSPF y las interfaces que participan de la publicación entre otros datos.

b) Verificar y documentar la base de datos de OSPF de cada router, donde se informa de manera detallada de todas las rutas hacia cada red.

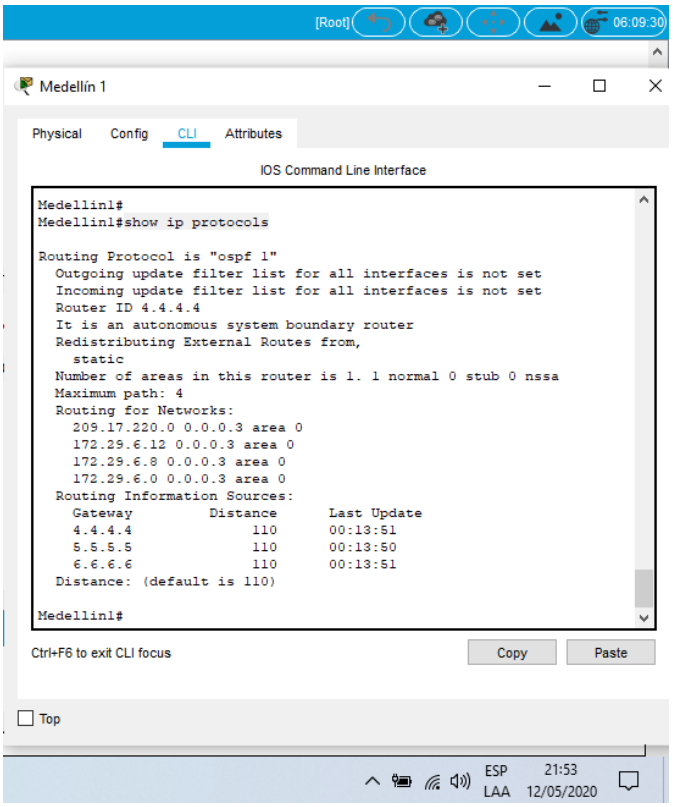


Figura 24. Show ip route protocols en Router Medellin1

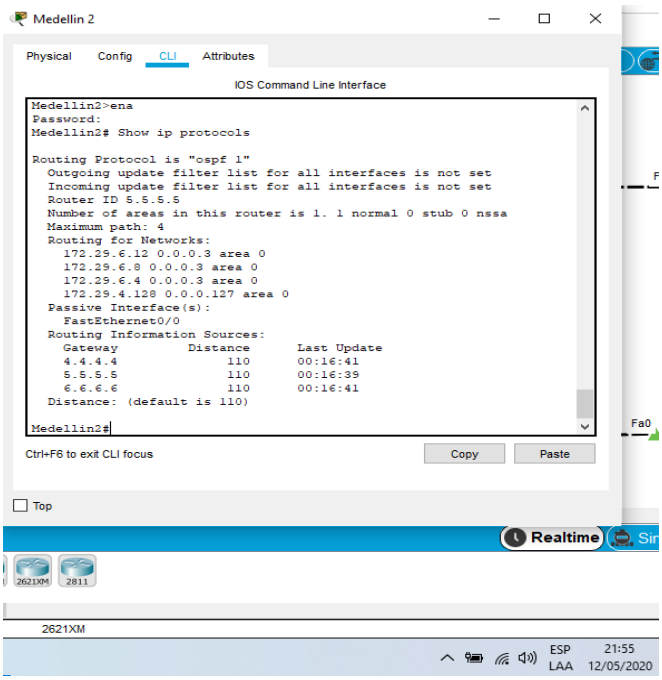


Figura 25.Show ip route protocols en Router Medellin2

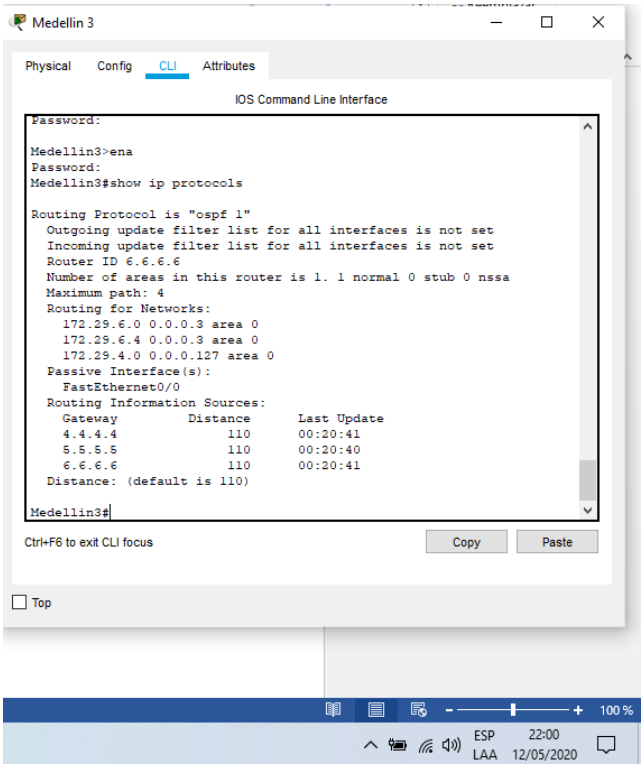


Figura 26. Show ip route protocols en Router Medellin3

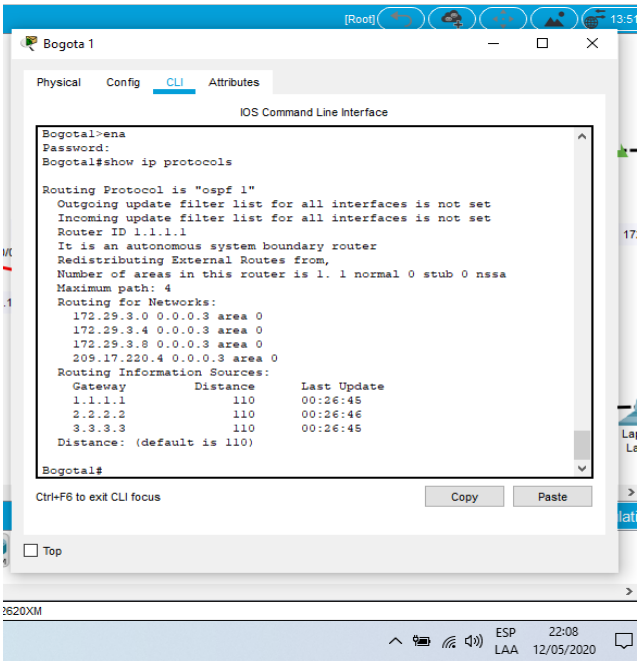


Figura 27.Show ip route protocols en Router Bogota1

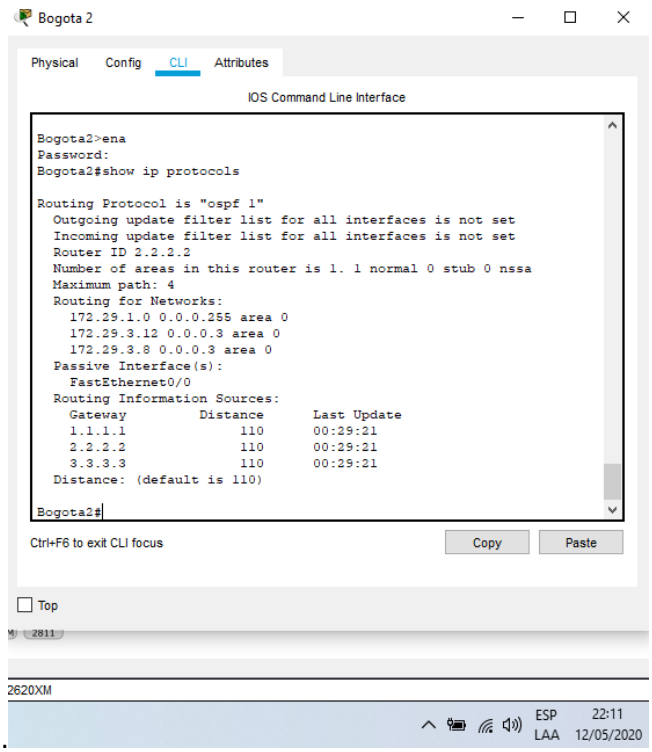


Figura 28.Show ip route protocols en Router Bogota2

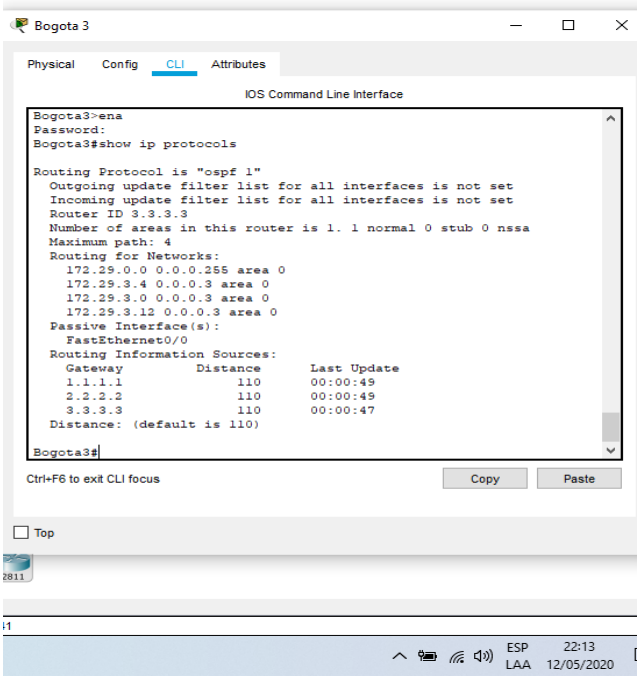


Figura 29 .Show ip route protocols en Router Bogota3

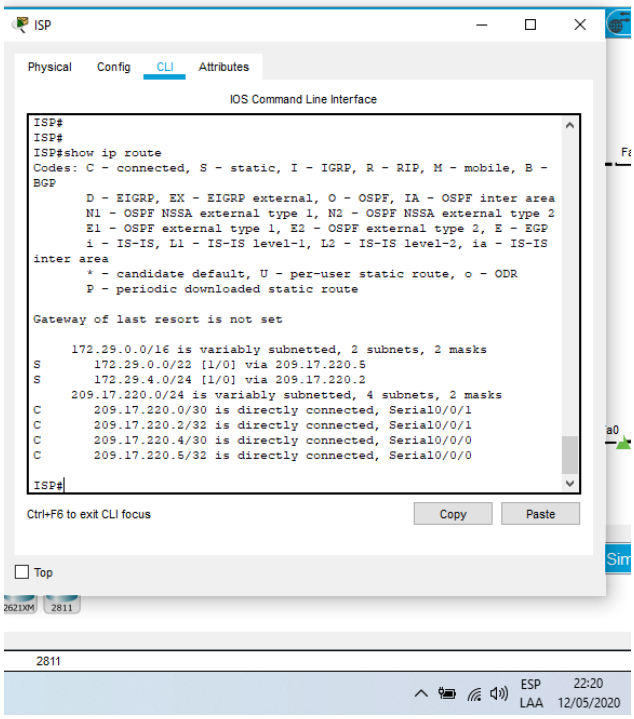


Figura 30.Show ip route protocols en Router ISP

Parte 5: Configurar encapsulamiento y autenticación PPP.

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

```
ISP(config)#username MED1 password MED
ISP(config)#interface s0/0/1
ISP(config-if)#encapsulation PPP
ISP(config-if)#PPP authentication PAP
ISP(config-if)#PPP PAP sent-username ISPMED password MED

Medellin1(config)#username ISMED password MED
Medellin1(config)#interface s0/0/1
Medellin1(config-if)#encapsulation ppp m
Medellin1(config-if)#ppp authentication pap
Medellin1(config-if)#ppp pap sent-username
MED1 password MED
```

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

```
ISP(config)#username BOGOTA1 password cisco
ISP(config)#interface s0/0/0
ISP(config-if)#encapsulation ppp
ISP(config-if)#ppp authentication chap

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

Parte 6: Configuración de PAT.

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

```
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 s0/0/0
Bogota1 (config-if)#ip nat inside
Bogota1 (config-if)#interface s0/1/0
Bogota1 (config-if)#ip nat inside
Bogota1 (config-if)#interface s0/0/1
Bogota1 (config-if)#ip nat inside
Bogota1 (config-if)#interface s0/1/1
Bogota1 (config-if)#ip nat inside
Bogota1 (config-if)#exit
```

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

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

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

Parte 7: Configuración del servicio DHCP.

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

```
Medellin2(config)#ip dhcp excluded-address 172.29.4.1 172.29.4.5
Medellin2(config)#ip dhcp excluded-address 172.29.4.129 172.29.4.133
Medellin2(config)#ip dhcp pool medellin2
Medellin2(dhcp-config)#network 172.29.4.0 255.255.255.128
Medellin2(dhcp-config)#default-route 172.29.4.1
Medellin2(dhcp-config)#dns-server 7.7.7.7
Medellin2(dhcp-config)#exit
Medellin2(config)#ip dhcp pool medellin3
Medellin2(dhcp-config)#network 172.29.4.128 255.255.255.128
Medellin2(dhcp-config)#default-route 172.29.4.129
Medellin2(dhcp-config)#dns-server 7.7.7.7
Medellin2 (dhcp-config)#exit
```

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

```
Medellin3 (config)#interface g0/0
Medellin3 (config-if)#ip helper-address 172.29.4.1
```

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

```
Bogota2(config)#ip dhcp excluded-address 172.29.1.1 172.29.1.5
Bogota2(config)#ip dhcp excluded-address 172.29.0.1 172.29.0.5
Bogota2 (config)#ip dhcp pool bogota2
Bogota2(dhcp-config)#network 172.29.1.0 255.255.255.0
Bogota2(dhcp-config)#default-route 172.29.1.1
Bogota2(dhcp-config)#dns-server 7.7.7.7
Bogota2(dhcp-config)#ip dhcp pool bogota3
Bogota2(dhcp-config)#network 172.29.0.0 255.255.255.0
Bogota2(dhcp-config)#default-route 172.29.0.1
Bogota2(dhcp-config)#dns-server 7.7.7.7
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(config)#interface g0/0
Bogota3(config-if)#ip helper-address 172.29.1.1
Bogota3(config-if)#exit
```

CONCLUSIONES

- Con la realización de esta prueba de habilidades practicas el estudiante toma las configuraciones necesarias para montar una topología de red asignar direcciones Ip, establecer cada dispositivo de red, saber qué tipo de cable va utilizar y que interface o direccionamiento va tomar adicionalmente brindar condiciones de seguridad para cada usuario con acceso a la red o topologías implementadas.

- A medida que los estudiantes desarrollaron este trabajo desarrollando cada uno de los ejercicios propuestos en cada uno de los trabajos colaborativos se desarrollaron procesamientos lógicos para armar cada una de las topologías, y culminar con estos dos ejercicios de una manera óptima en el simulador, adquirir los conocimientos de LAN /WAN

- La utilización del simulador de CISCO PACKET TRACER, y es importante es fácil de usar resuelve dudas y es muy didáctico te permite de una manera casi real, podemos obtener los resultados de las redes y su configuración.

- En el primer escenario se puede apreciar los modos de consola y los diferentes modos de seguridad y contraseñas que se pueden asignar a cada uno de los equipos que interactúan en el simulador.

BIBLIOGRAFIA

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

- CISCO NETWORKING. (21 de agosto de 2013). Comandos de configuración de dispositivos cisco. (slideshare, Ed.) Recuperado el 7 de marzo de 2020, de https://es.slideshare.net/samuelhuertasorjuela/comandos-de-configuracion-dedispositivos-cisco

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

- Victor E. Martínez G, V. E. (2018, 16 agosto). Configuración de rutas estáticas (static route) Router Cisco. Recuperado el 7 de marzo de 2020, de http://theosnews.com/2013/02/configuracion-de-rutas-estaticas-static-routerouter-cisco/