TITULO

Solución de Dos Estudios de Caso Bajo el Uso de Tecnología CISCO

Diseño e Implementación de Soluciones Integradas LAN / WLAN Trabajo de Grado

Habilidades Prácticas CCNA

Autor

Camilo Camero Rojas

Director

ING. Juan Carlos Vesga

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD)

Escuela de Ciencias Básicas y Tecnologías e Ingeniería (ECBTI)

Diplomado de Profundización CISCO

Valle del Cauca, Tuluá

ABRIL 2020

TABLA DE CONTENIDO

INTRODUCCIÓN

La actividad prueba de habilidades diplomado de profundización CISCO, nos proveen 2 casos de estudio o 2 escenarios los cuales nosotros como estudiantes debemos de desarrollar, ya que trata sobre 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). Estas pueden implementarse en routers para aumentar la seguridad de una red bien sea en una empresa o en un hogar, implementar políticas de entrada y salida de paquetes de datos para ciertos equipos o host específicos.

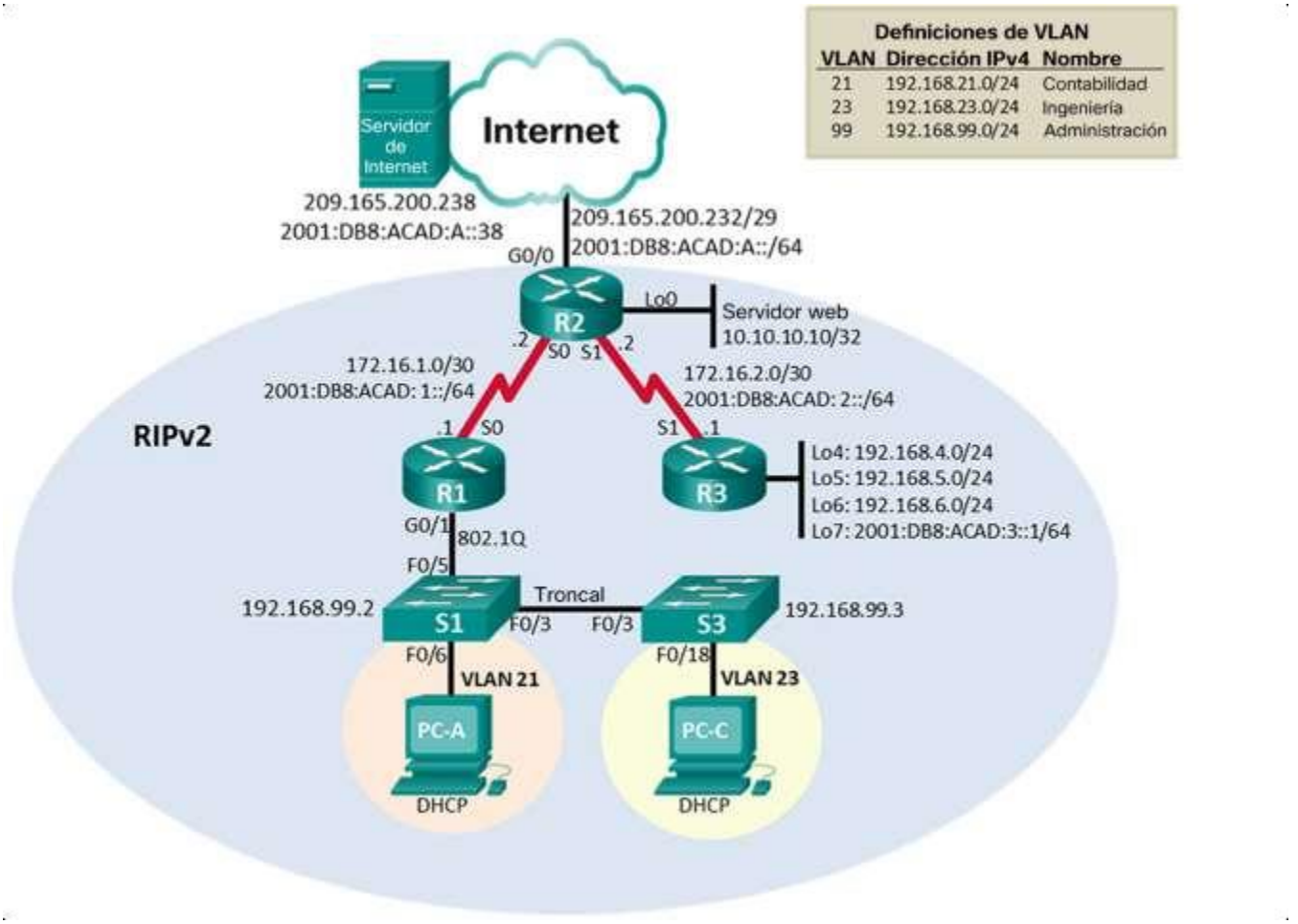
En el presente documento, se encuentra la solución a los 2 escenarios dados, comprendiendo la importancia de este diplomado, no solo para crecimiento personal e intelectual, sino también para nuestro crecimiento profesional, ya que el tener un certificado CISCO a nivel mundial, significa que al momento de aplicar a un empleo y en nuestra hoja de vida diga que somos avalados y certificados por CISCO, tenemos un poco más de oportunidades que otras personas, y la verdad es que con este diplomado y esta certificación uno obtiene mucho conocimiento, desde lo básico hasta lo más complejo y aprende a manejar, configurar todos los dispositivos que se usan en una red comúnmente a través del software Paket Tracer, lo hace aún más interesante porque es como si estuviéramos configurando un dispositivo en la vida real.

DESARROLLO DE LOS CASOS DE ESTUDIO

Escenario 1

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

Topología



Parte 1: Inicializar dispositivos

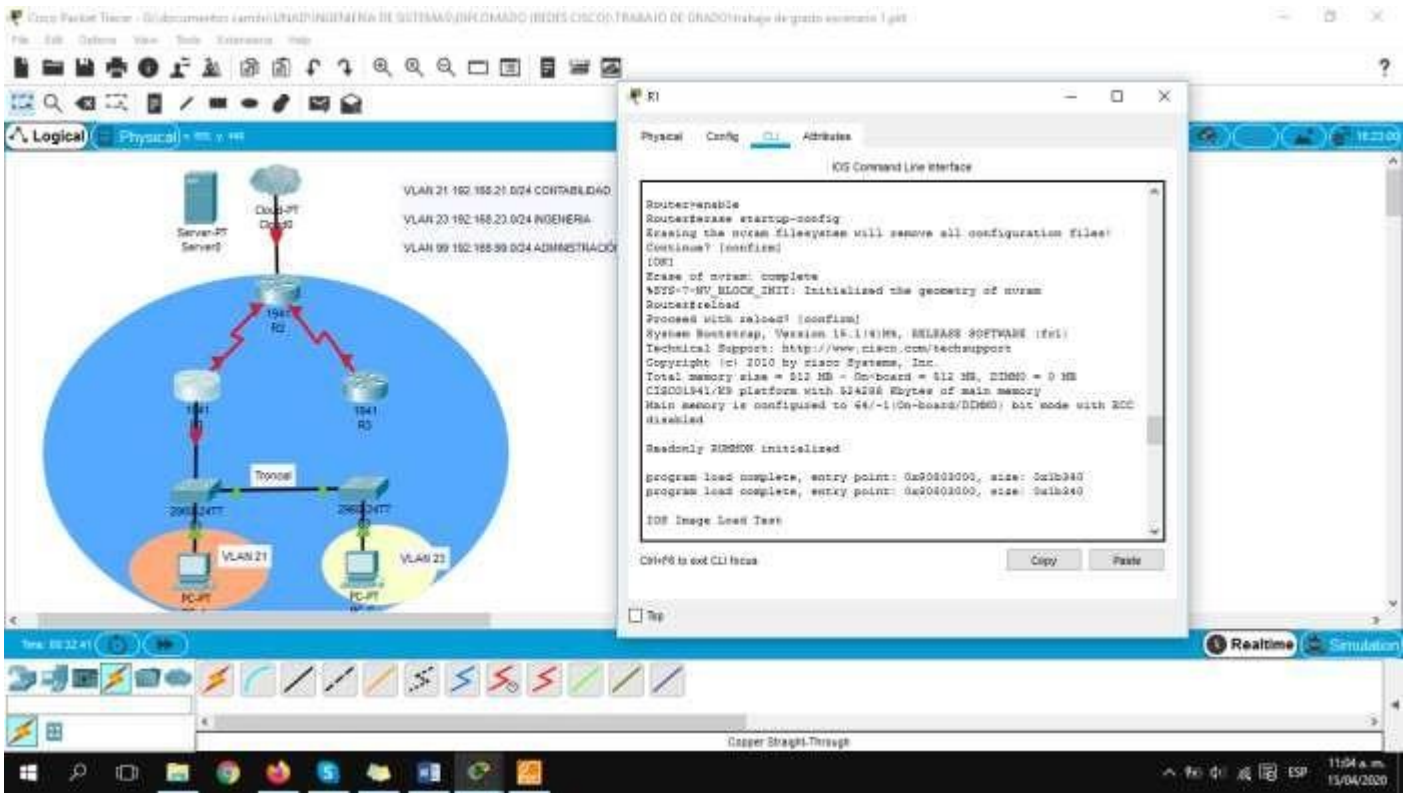
Paso 1: Inicializar y volver a cargar los routers y los switches

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

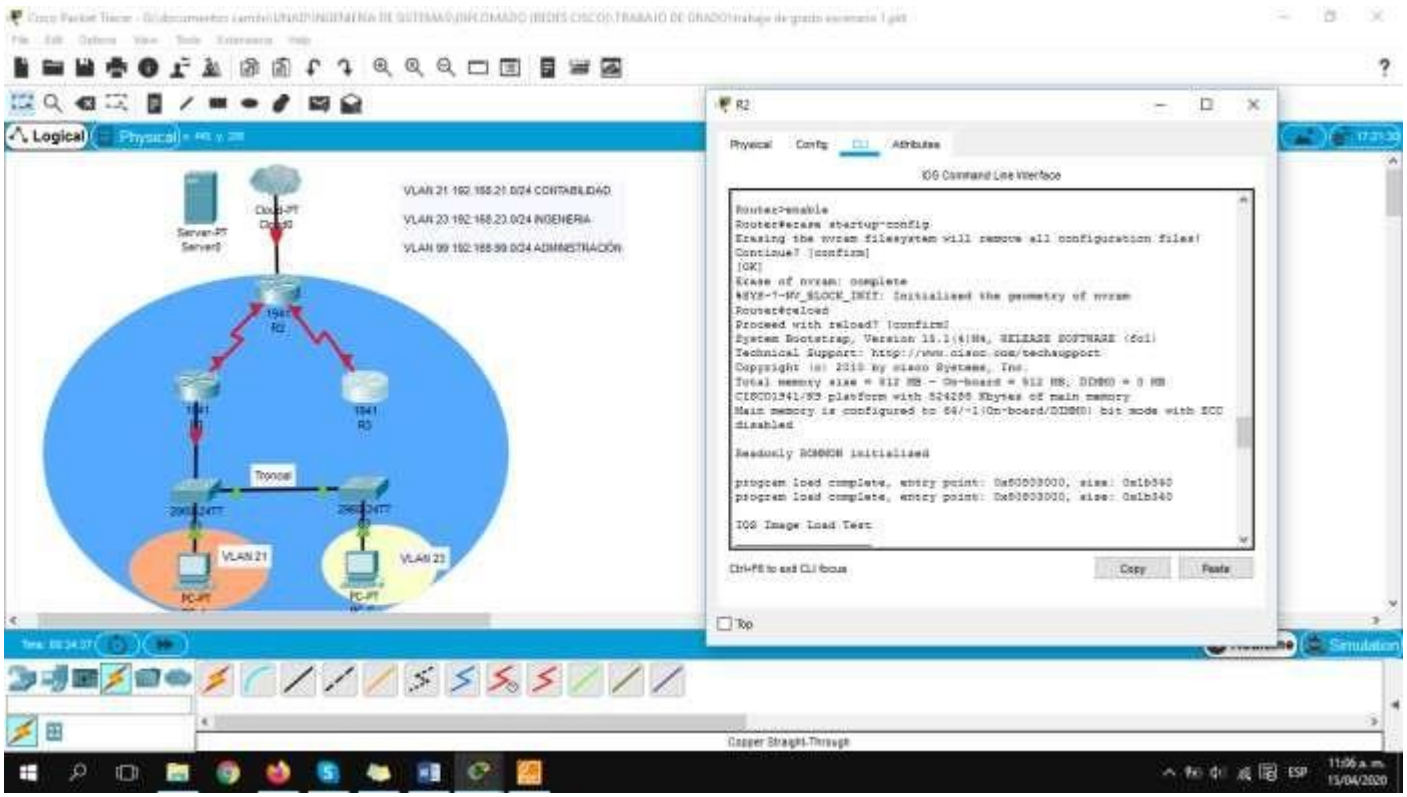
Antes de continuar, solicite al instructor que verifique la inicialización de los dispositivos.

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

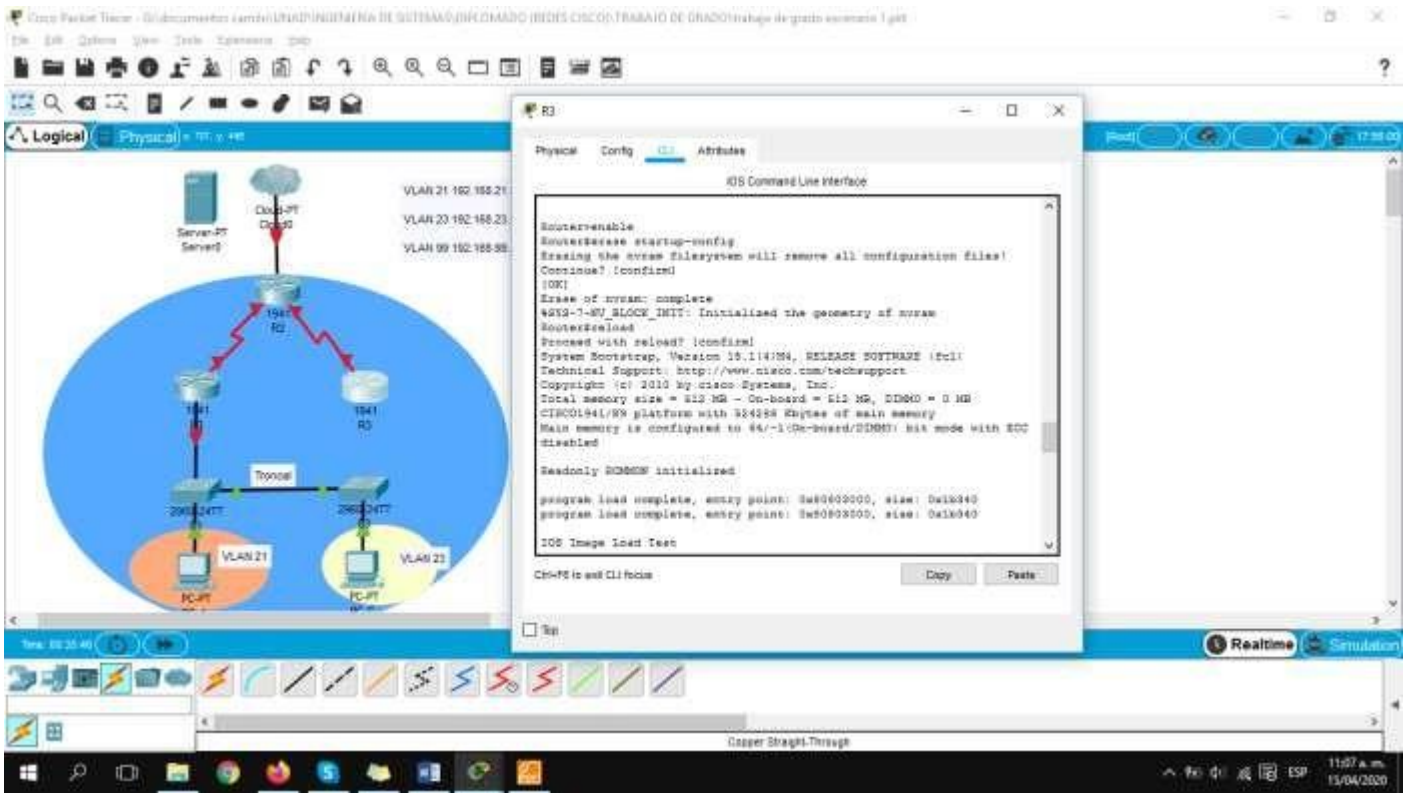
R1:


R1
Physical
Config
CLI
Attributes
IOS Command Line interface
Router>enable
Router#erase startup-config
Erasing the nvram filesystem will remove all configuration files!
Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
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.
Total memory size = 512 MB - On-board = 512 MB, DIMM0 = 0 MB
CISCO1941/K9 platform with 524288 Kbytes of main memory
Main memory is configured to 64/-1(On-board/DIMM0) bit mode with ECC disabled
Readonly ROMMON initialized
program load complete, entry point: 0x80803000, size: 0x1b340
program load complete, entry point: 0x80803000, size: 0x1b340
IOS Image Load Test
Ctrl+F6 to exit CLI focus
Copy
Paste
Top
Logical
Physical
VLAN 21 192.168.21.0/24 CONTABILIDAD
VLAN 23 192.168.23.0/24 INGENIERIA
Trunk
VLAN 21
VLAN 23
Realtime
Simulation
Copper Straight-Through

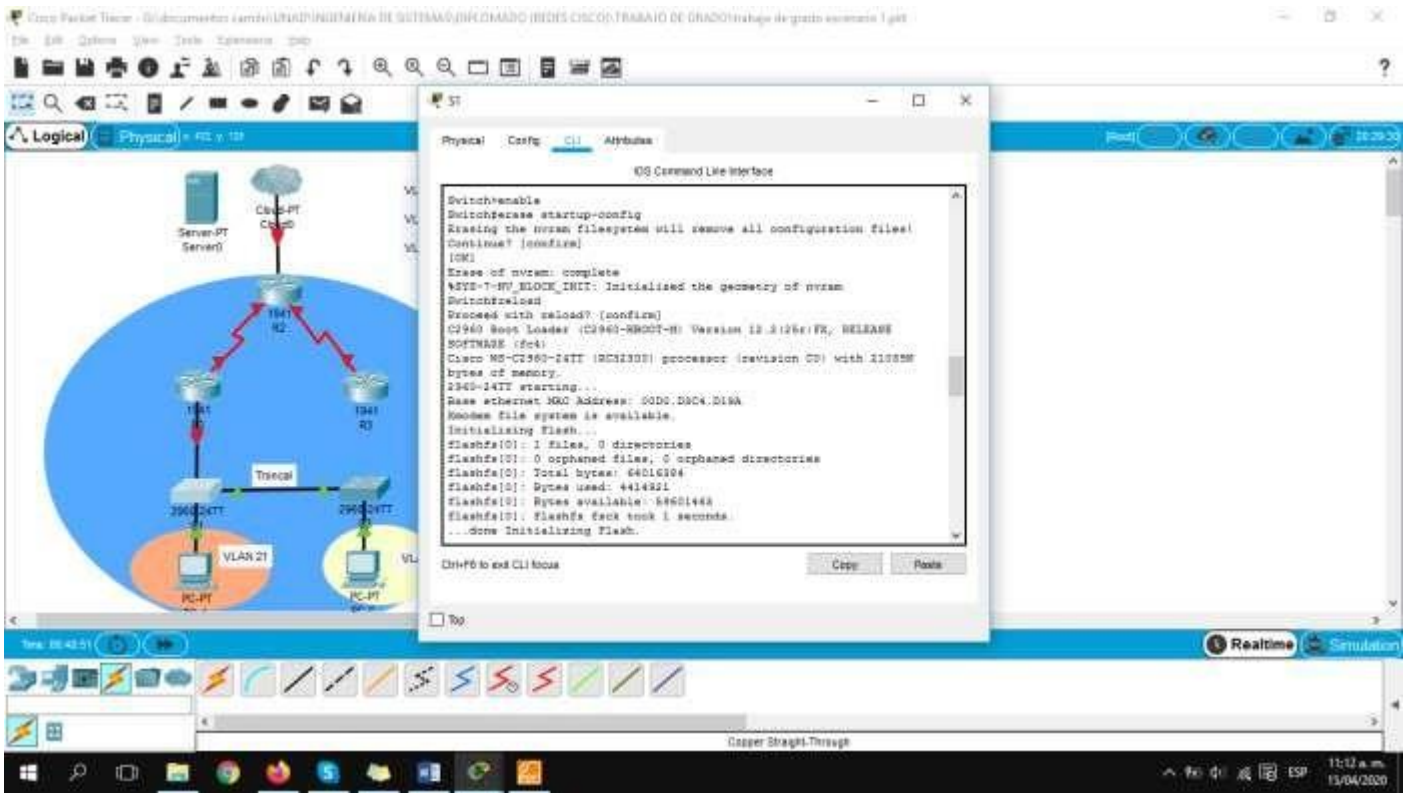
R2:


Logical
Physical
VLAN 21 192.168.21.0/24 CONTABILIDAD
VLAN 23 192.168.23.0/24 INGENIERIA
VLAN 99 192.168.99.0/24 ADMINISTRACIÓN
Server-PT
Server0
Cloud-PT
Cloud0
1941
R2
1941
R3
Trunk
VLAN 21
VLAN 23
PC-PT
R2
Physical
Config
CLI
Attributes
IOS Command Line Interface
Router>enable
Router#erase startup-config
Erasing the nvram filesystem will remove all configuration files!
Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
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.
Total memory size = 512 MB - On-board = 512 MB, DIMM0 = 0 MB
CISCO1941/K9 platform with 524288 Kbytes of main memory
Main memory is configured to 64/-1(On-board/DIMM0) bit mode with ECC disabled
Readonly ROMMON initialized
program load complete, entry point: 0x80803000, size: 0x1b340
program load complete, entry point: 0x80803000, size: 0x1b340
IOS Image Load Test
Ctrl+F6 to exit CLI focus
Copy
Paste
Top
Copper Straight-Through
ESP

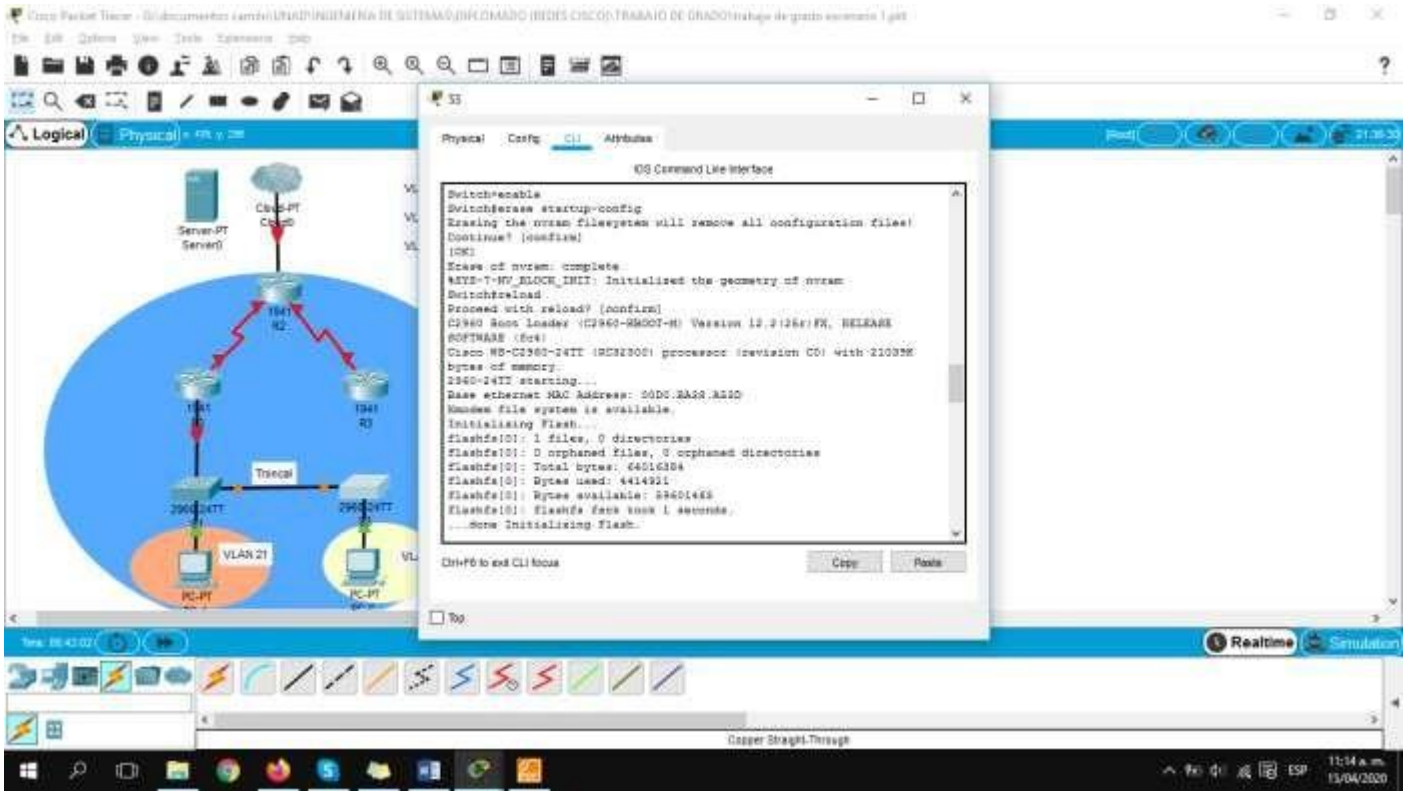
R3:


R3
Physical
Config
CLI
Attributes
IOS Command Line Interface
Router>enable
Router#erase startup-config
Erasing the nvram filesystem will remove all configuration files!
Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
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.
Total memory size = 512 MB - On-board = 512 MB, DIMM0 = 0 MB
CISCO1941/K9 platform with 524288 Kbytes of main memory
Main memory is configured to 64/-1(On-board/DIMM0) bit mode with ECC disabled
Readonly ROMMON initialized
program load complete, entry point: 0x80803000, size: 0x1b340
program load complete, entry point: 0x80803000, size: 0x1b340
IOS Image Load Test
Ctrl+F6 to exit CLI focus
Copy
Paste
Top
Logical
Physical
VLAN 21
VLAN 23
Realtime
Simulation
Copper Straight-Through

S1:


S1
Physical
Config
CLI
Attributes
IOS Command Line Interface
Switch>enable
Switch#erase startup-config
Erasing the nvram filesystem will remove all configuration files!
Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
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 (revision C0) with 21039K
bytes of memory.
2960-24TT starting...
Base ethernet MAC Address: 00D0.D3C4.D19A
Xmodem file system is available.
Initializing Flash...
flashfs[0]: 1 files, 0 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 64016384
flashfs[0]: Bytes used: 4414821
flashfs[0]: Bytes available: 59601563
flashfs[0]: flashfs fsck took 1 seconds.
...done Initializing Flash.
Ctrl+F6 to exit CLI focus
Copy
Paste
Top
Logical
Physical
Server-PT
Server0
Cisco-PT
Cloud0
1941
R2
1941
R1
1941
R3
Trsncal
VLAN 21
PC-PT
Realtime
Simulation
Copper Straight-Through

S2:



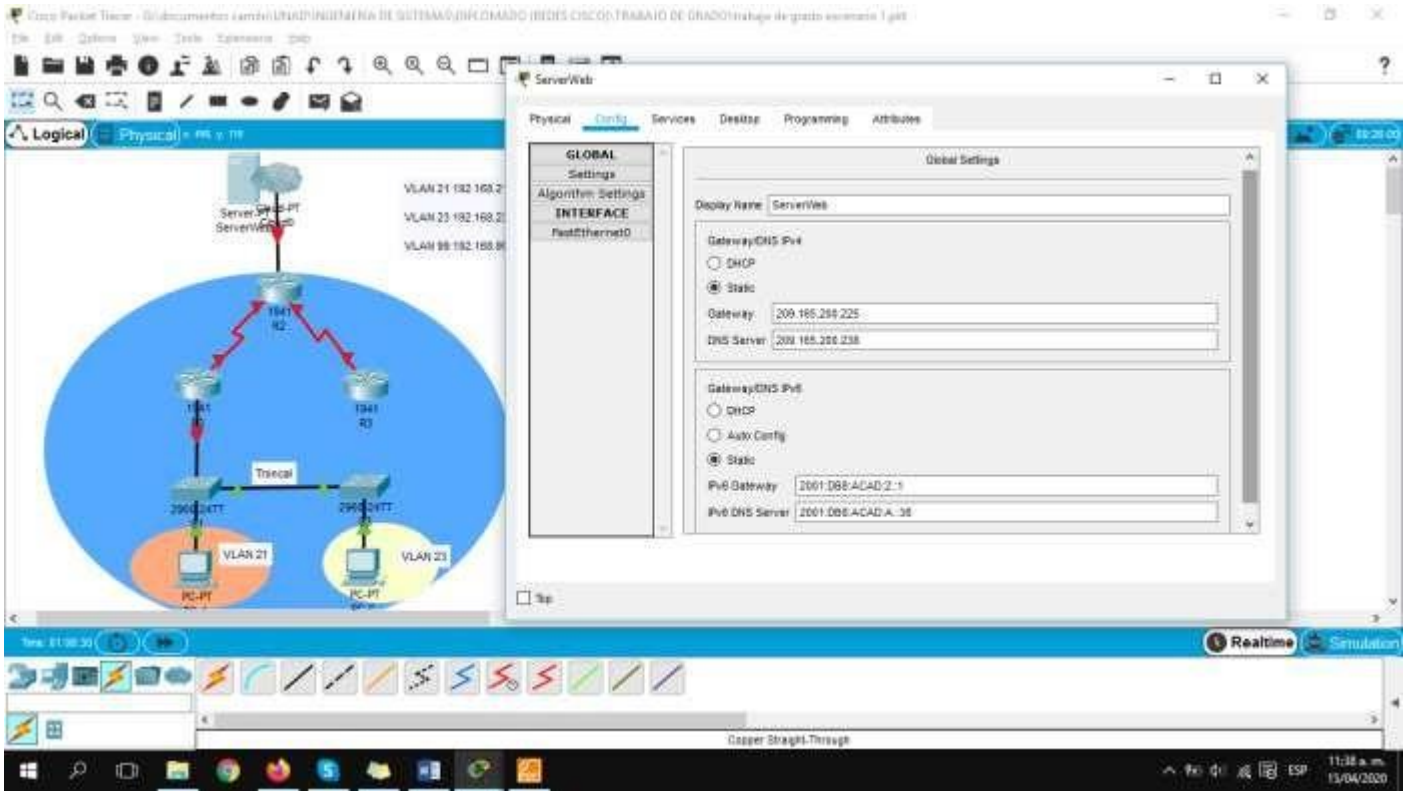
Parte 2: Configurar los parámetros básicos de los dispositivos

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):

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.225
Dirección IPv6/subred	2001:DB8:ACAD:A::38
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:

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	**Se prohíbe el acceso no autorizado.** R1(config)#banner motd #Se prohbe el acceso no autorizado!#
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

Establezca la descripción:
R1(config)#interface s0/0/0
R1(config-if)#description R1-R2

Establecer la dirección IPv4 Consultar el diagrama de topología para conocer la información de direcciones
R1(config-if)#ip address 172.16.1.1 255.255.255.252

Establecer la dirección IPv6 Consultar el diagrama de topología para conocer la información de direcciones
R1(config-if)#ipv6 address 2001:DB8:ACAD:1::/64

Establecer la frecuencia de reloj en 128000, Activar la interfaz
R1(config-if)#clock rate 128000
R1(config-if)#no shutdown

Configurar una ruta IPv4 predeterminada de S0/0/0
R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0

Configurar una ruta IPv6 predeterminada de S0/0/0

R1(config)#ipv6 route ::/0 s0/0/0

Nota: Todavía no configure G0/1.

Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

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	2>enable R2#config 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.** R2(config)#banner motd #Se prohbe 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.

Interfaz S0/0/0 Establezca

la descripción

R2(config)#interface s0/0/0
R2(config-if)#description R2-R1

Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred, Activar la interfaz

R2(config-if)#ip address 172.16.1.2 255.255.255.252
R2(config-if)#no shutdown

Establezca la descripción

R2(config)#interface s0/0/0
R2(config-if)#description R2-R1

Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones, Activar la interfaz

R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64
R2(config-if)#no shutdown

Interfaz S0/0/1 Establezca
la descripción
R2(config)#interface s0/0/1
R2(config-if)#description R2-R3

Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred, Activar la interfaz, Establecer la frecuencia de reloj en 128000.

R2(config-if)#ip address 172.16.2.2 255.255.255.252
R2(config-if)#clock rate 128000
R2(config-if)#no shutdown

Establezca la dirección IPv6. Utilizar la siguiente dirección disponible en la subred, Activar la interfaz, Establecer la frecuencia de reloj en 128000.

R2(config)#interface s0/0/1
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)
Establezca la descripción
R2(config)#interface g0/0
R2(config-if)#description R2-Internet

Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred, Activar la interfaz
R2(config-if)#ip address 209.165.200.233 255.255.255.248
R2(config-if)#no shutdown

Establezca la dirección IPv6. Utilizar la siguiente dirección disponible en la subred, Activar la interfaz
R2(config)#interface g0/0
R2(config-if)#description R2-Internet
R2(config-if)#ipv6 address 2001:DB8:ACAD:A::2/64
R2(config-if)#no shutdown

Interfaz loopback 0 (servidor web simulado)
Establecer la descripción.
R2(config)#interface loopback 0
Establezca la dirección IPv4.

R2(config-if)#ip address 10.10.10.10 255.255.255.0
R2(config-if)#no shutdown

Ruta predeterminada

Configure una ruta IPv4 predeterminada de G0/0.

R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0

Configure una ruta IPv6 predeterminada de G0/0.

R2(config)#ipv6 route ::/0 g0/0

Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

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 prohbe el acceso no autorizado!#
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.

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	

Establecer la descripción

R3(config)#interface s0/0/1

R3(config-if)#description R3-R2

Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred, Activar la interfaz

R3(config-if)#ip address 172.16.2.1 255.255.255.252

R3(config-if)#no shutdown

Interfaz loopback 4

Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.

R3(config)#interface loopback 4

R3(config-if)#ip address 192.168.4.1 255.255.255.0

Interfaz loopback 5

Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.

R3(config)#interface loopback 5

R3(config-if)#ip address 192.168.5.1 255.255.255.0

Interfaz loopback 6

Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.

R3(config)#interface loopback 6

R3(config-if)#ip address 192.168.6.1 255.255.255.0

Interfaz loopback 7

Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.

R3(config)#interface loopback 7

R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64

Rutas predeterminadas

R3(config)#interface s0/0/1

R3(config-if)#ip route 0.0.0.0 0.0.0.0 s0/0/1

R3(config)#interface s0/0/1

R3(config-if)#ipv6 route ::/0 s0/0/1

Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

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)#service pass S1(config-line)#service passw S1(config-line)#service password S1(config-line)#service password- S1(config-line)#service password-encryption
Mensaje MOTD	**Se prohíbe el acceso no autorizado.** S1(config)#banner motd #Se prohbe el acceso no autorizado!#

Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

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	**Se prohíbe el acceso no autorizado.** S3(config)#banner motd #Se prohbe el acceso no autorizado!#

Paso 7: Verificar la conectividad de la red

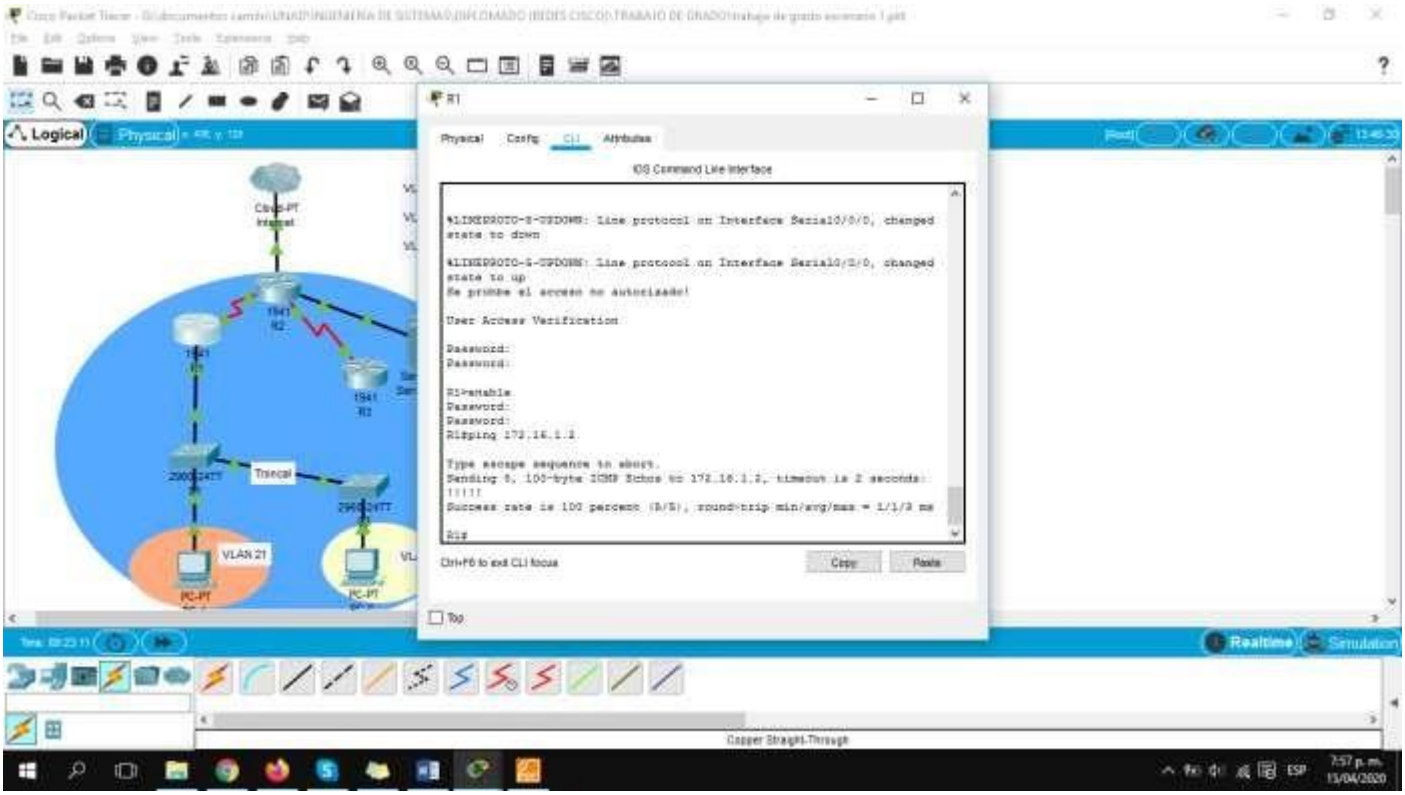
Utilice el comando **ping** para probar la conectividad entre los dispositivos de red.

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:

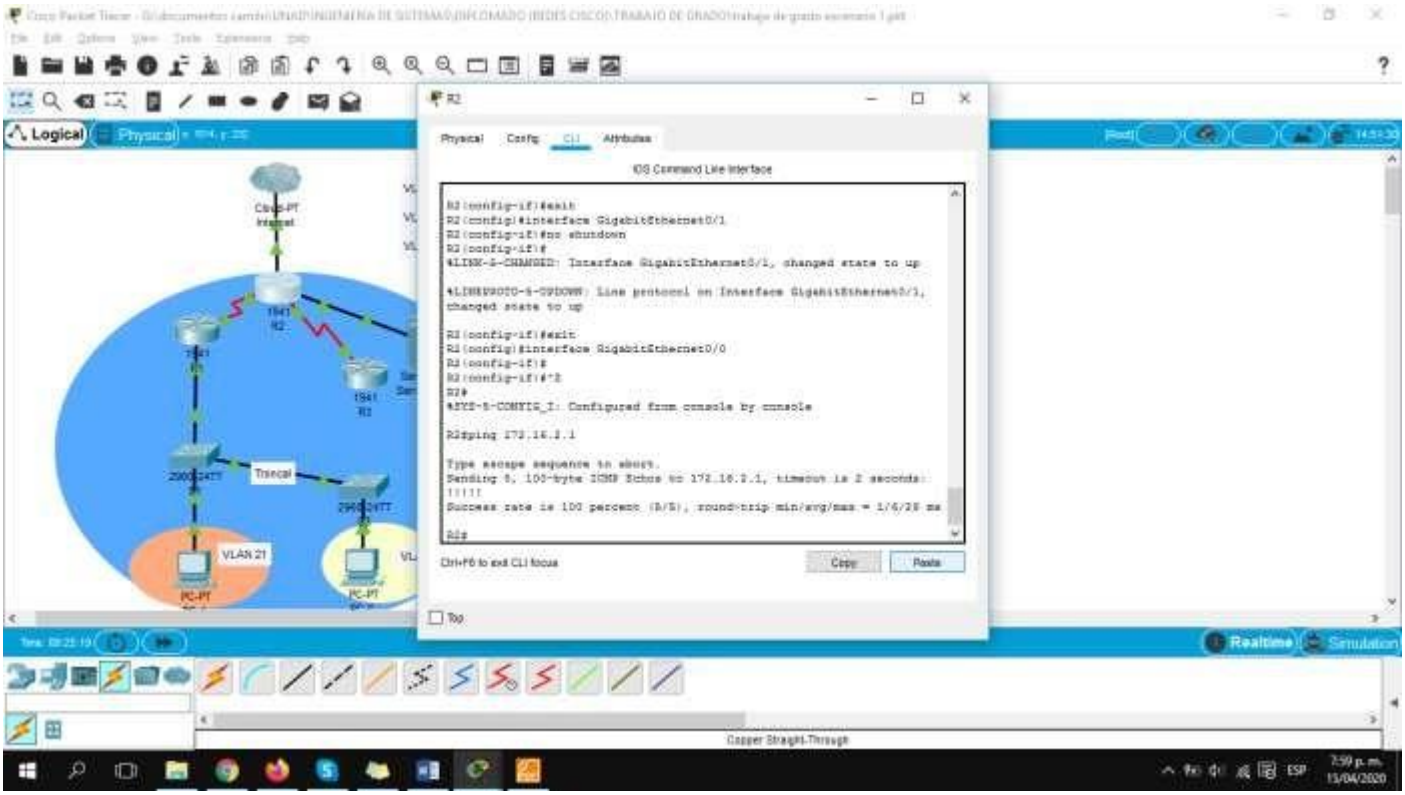
Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	EXITOSO
R2	R3, S0/0/1	172.16.2.1	EXITOSO
PC de Internet	Gateway predeterminado	10.10.10.10	EXITOSO

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

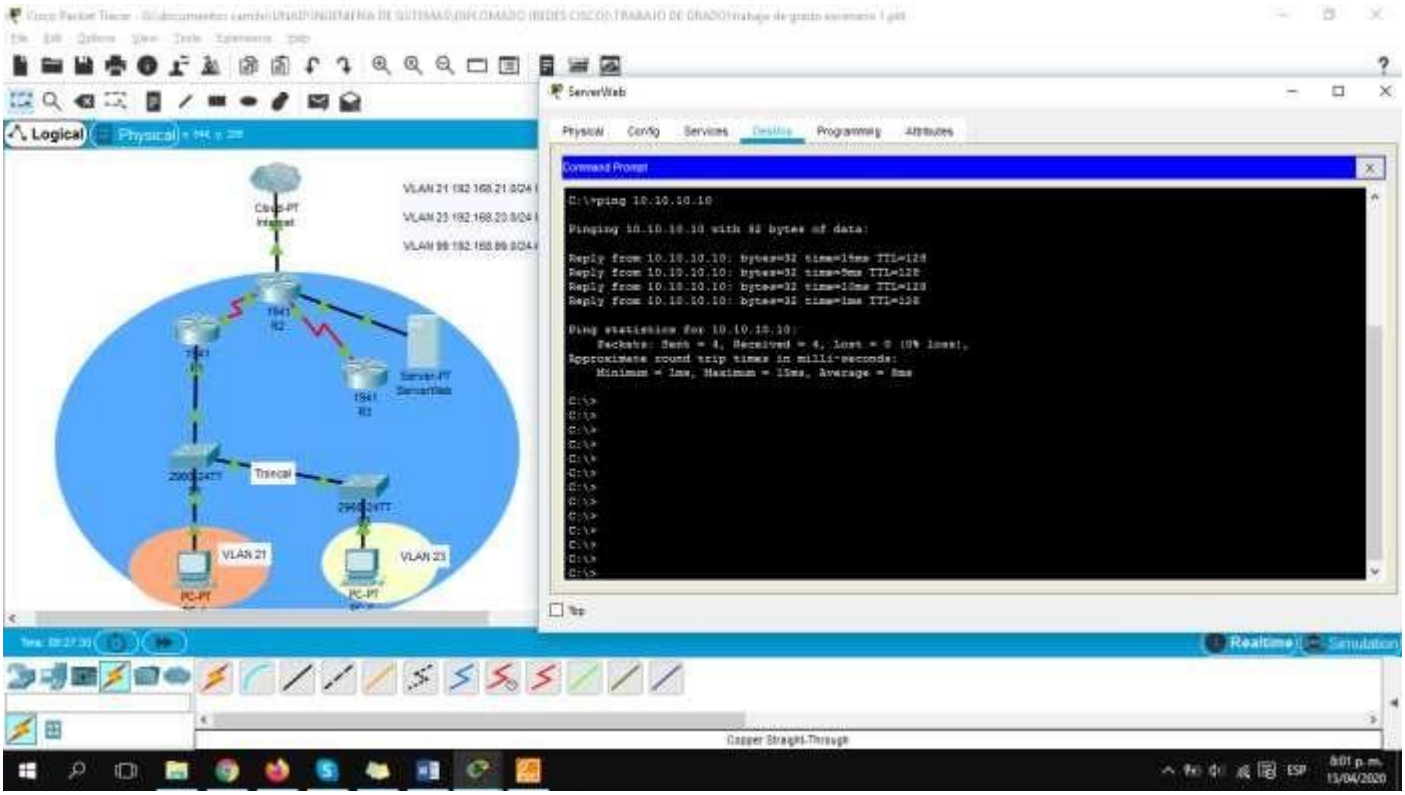
Ping, desde R1 a R2, (172.16.1.2**)**



Ping, desde R2 a R3, (172.16.2.1**)**



Ping, desde Pc de Internet a gateway, (10.10.10.10**)**



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:

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
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
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 nativa
Forzar el enlace troncal en la interfaz F0/5	Utilizar la red VLAN 1 como VLAN nativa
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range
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)#swi S1(config-if)#switchport access vlan 21
Apagar todos los puertos sin usar	

Crear la base de datos de VLAN

S1(config)#vlan 99
S1(config-vlan)#name Administracion
S1(config-vlan)#vlan 21
S1(config-vlan)#name Contabilidad
S1(config-vlan)#vlan 23
S1(config-vlan)#name Ingenieria
S1(config-vlan)#exit

Asigne la dirección IPv4 a la VLAN de administración.

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

Forzar el enlace troncal en la interfaz F0/3, Utilizar la red VLAN 1 como VLAN nativa.

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 nativa.

S1(config)#interface f0/5

S1(config-if)#switchport mode trunk

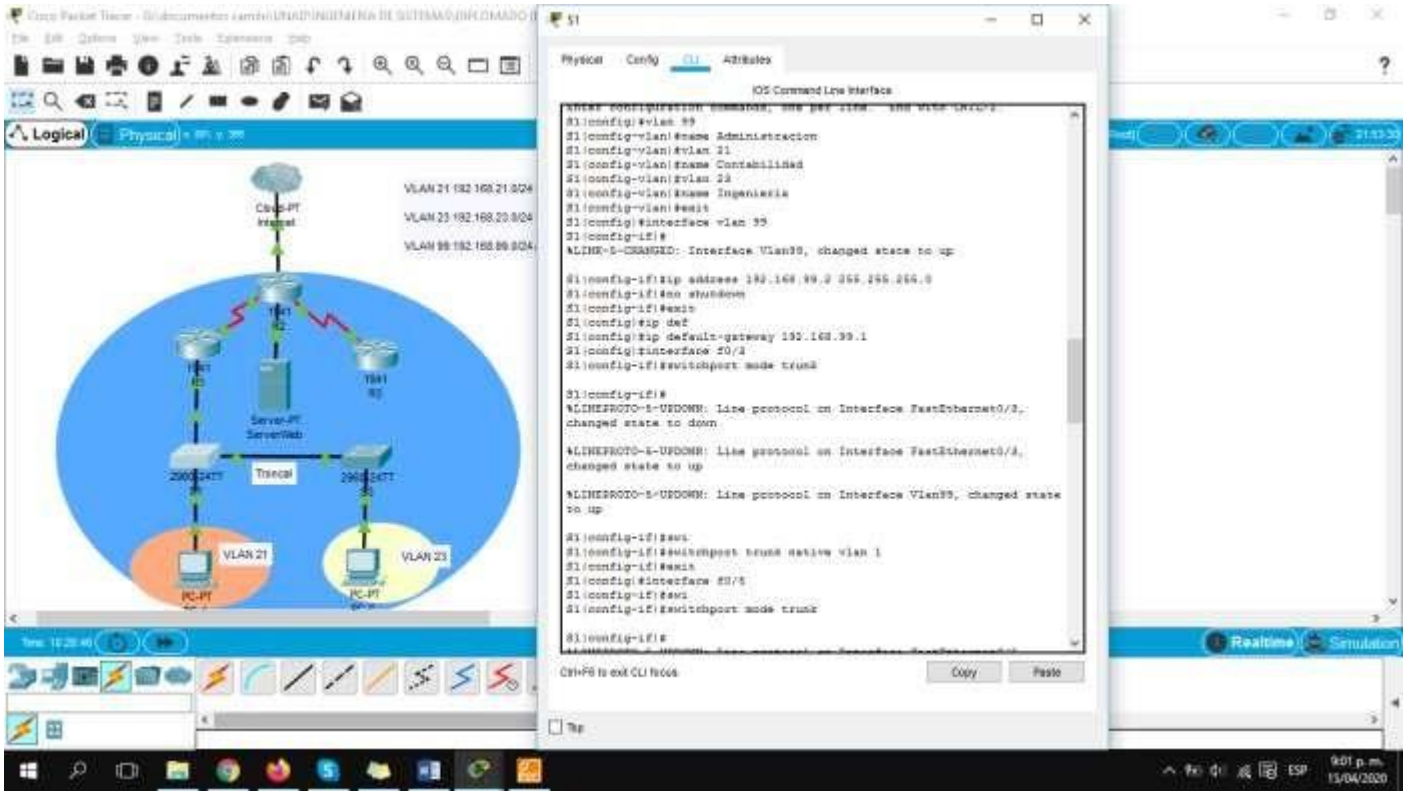
S1(config-if)#switchport trunk native vlan 1

S1(config-if)#exit

Configurar el resto de los puertos como puertos de acceso.

S1(config-if)#interface range f0/1, f0/2, f0/4, f0/7-24, g0/1-2

S1(config-if-range)#shutdown



Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

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.
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
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 nativa
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range
Asignar F0/18 a la VLAN 23	S3(config)#interface f0/8 S3(config-if)#no shutdown S3(config-if)#switchport mode Access S3(config-if)#switchport access vlan 23
Apagar todos los puertos sin usar	

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
```

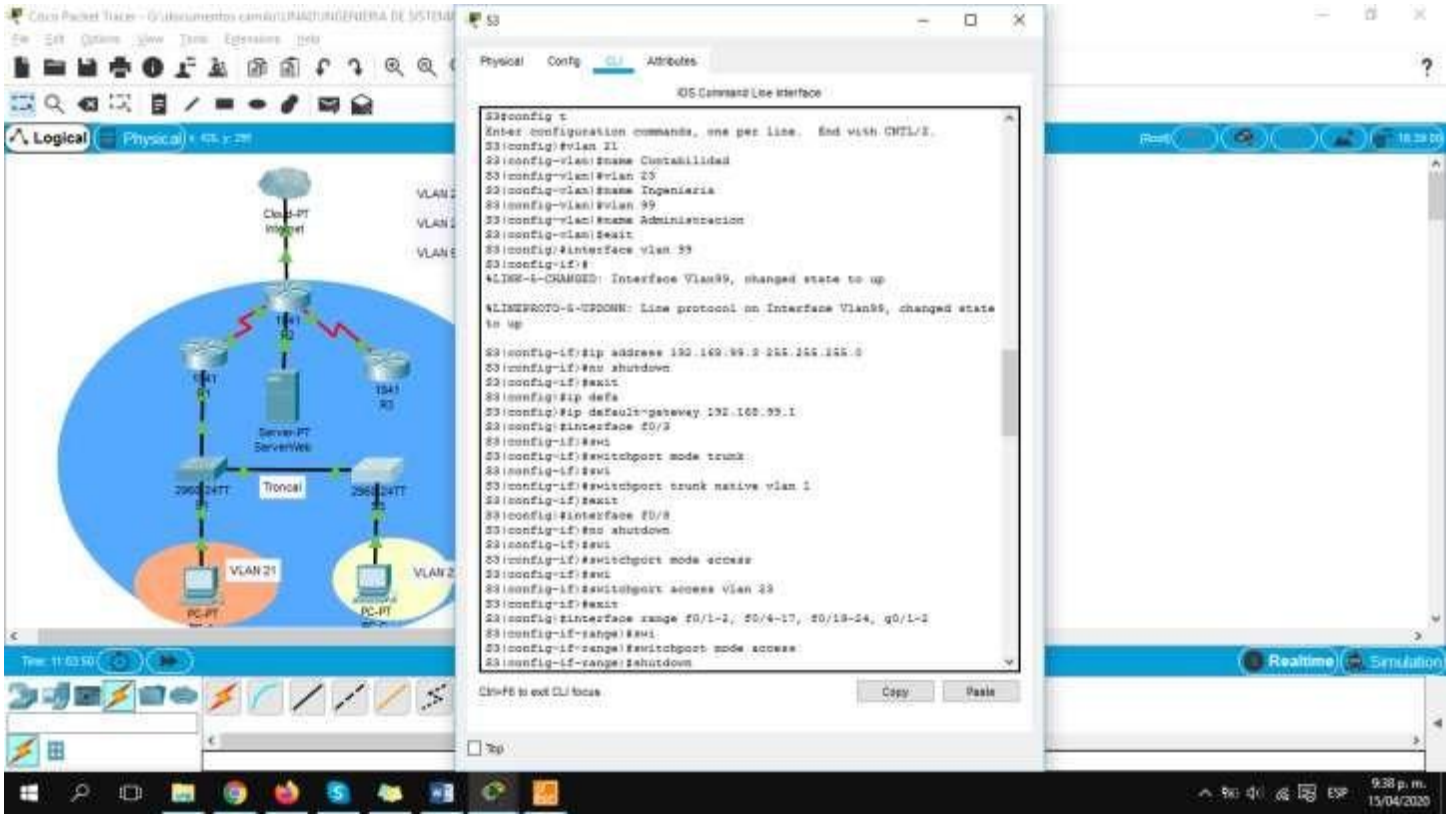
Asignar la dirección IP de administración

```
S3(config)#interface vlan 99
S3(config-if)#ip address 192.168.99.3 255.255.255.0
S3(config-if)#no shutdown
```

Forzar el enlace troncal en la interfaz F0/3, Utilizar la red VLAN 1 como VLAN nativa.

```
S3(config)#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)#swi
S3(config-if-range)#switchport mode access
S3(config-if-range)#shutdown



Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	Descripción: **LAN_Contabilidad** Asignar la VLAN 21 Asignar la primera dirección disponible a esta interfaz
Configurar la subinterfaz 802.1Q .23 en G0/1	Descripción: **LAN_Ingeniería** Asignar la VLAN 23 Asignar la primera dirección disponible a esta interfaz

Configurar la subinterfaz 802.1Q .99 en G0/1	Descripción: **LAN_Administración** Asignar la VLAN 99 Asignar la primera dirección disponible a esta interfaz
Activar la interfaz G0/1	

Configurar la subinterfaz 802.1Q .21 en G0/1

```
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 .21 en G0/1

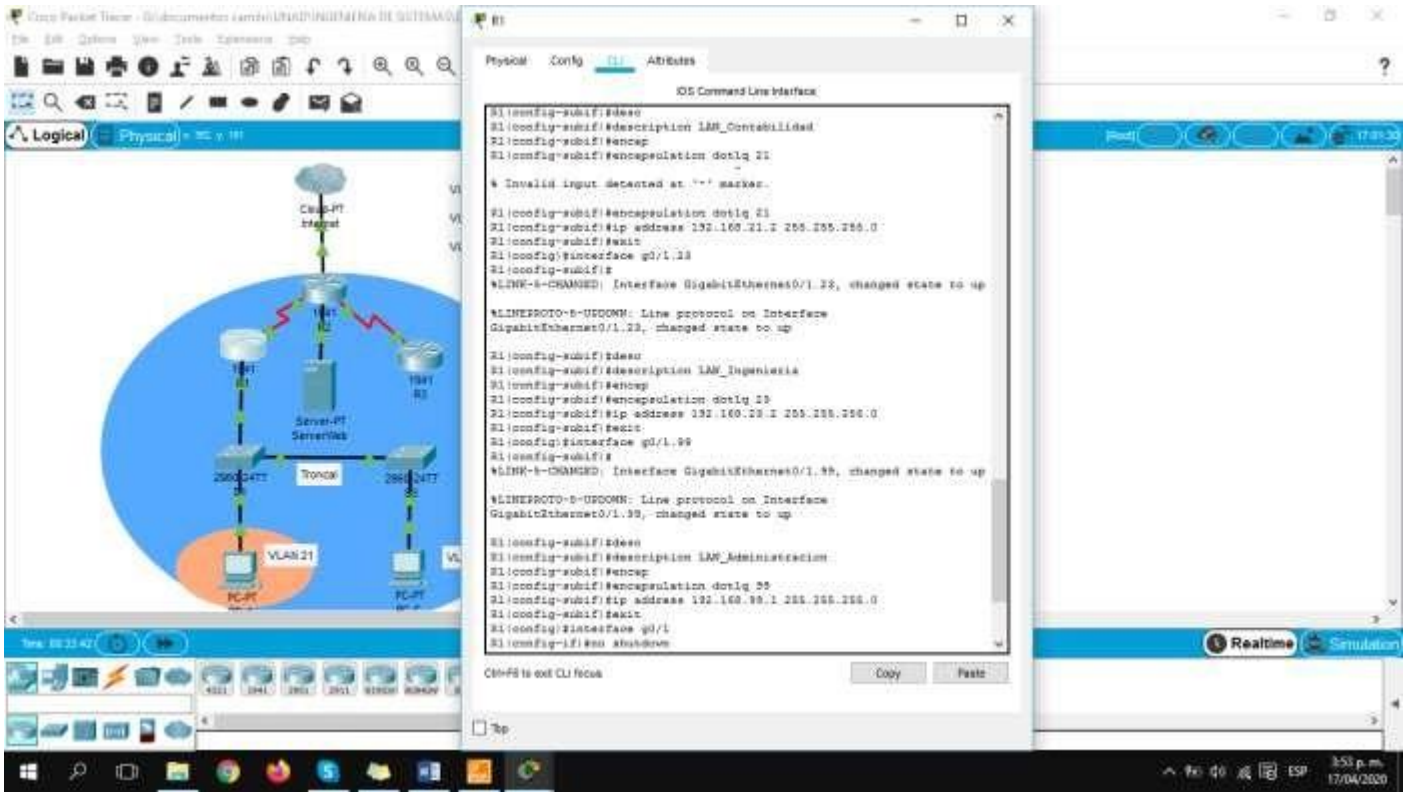
```
R1(config)#interface g0/1.23
R1(config-subif)#description LAN_Ingenieria
R1(config-subif)#encapsulation dot1q 23
R1(config-subif)#ip address 192.168.23.2 255.255.255.0
R1(config-subif)#exit
```

Configurar la subinterfaz 802.1Q .21 en G0/1

```
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)#interface g0/1
R1(config-if)#no shutdown
R1(config-if)#exit
```

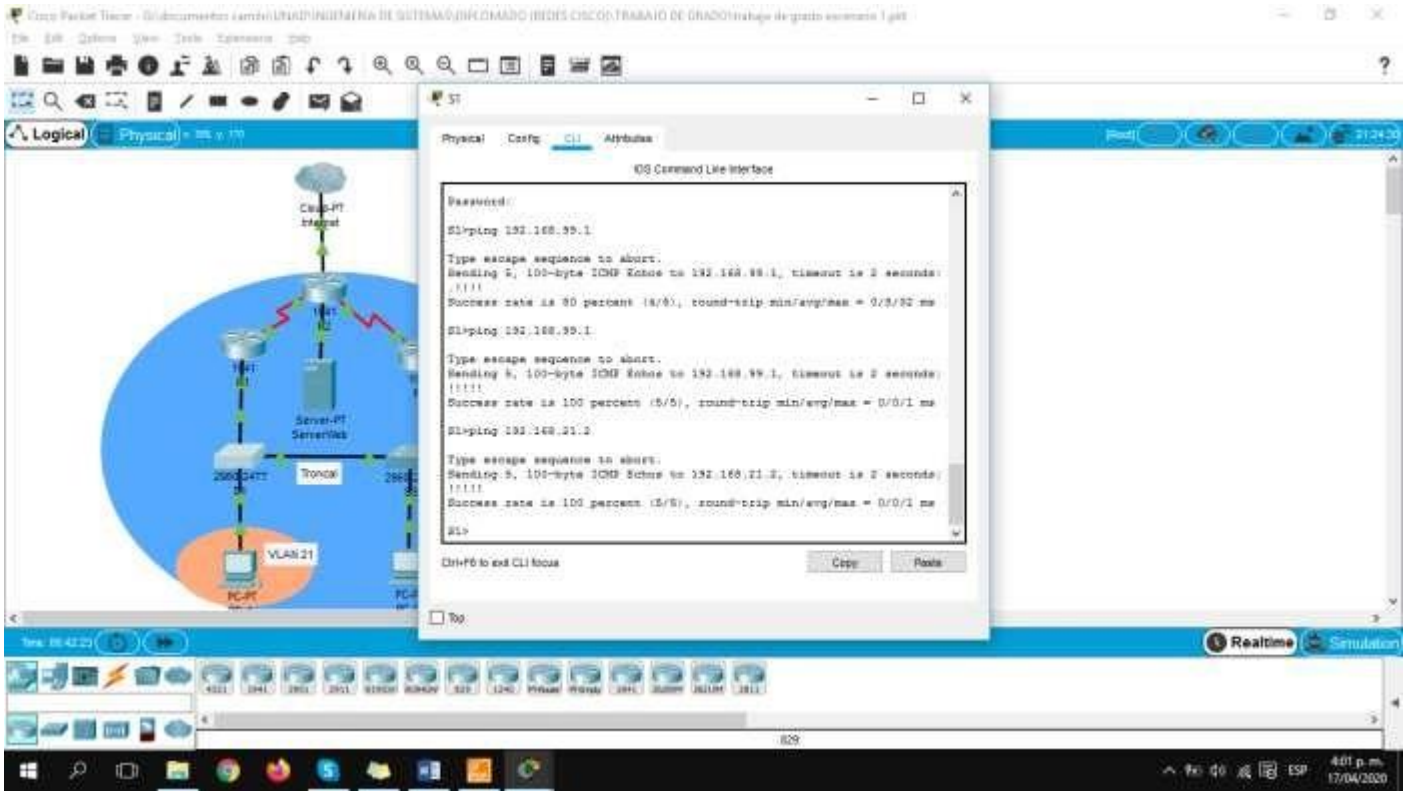


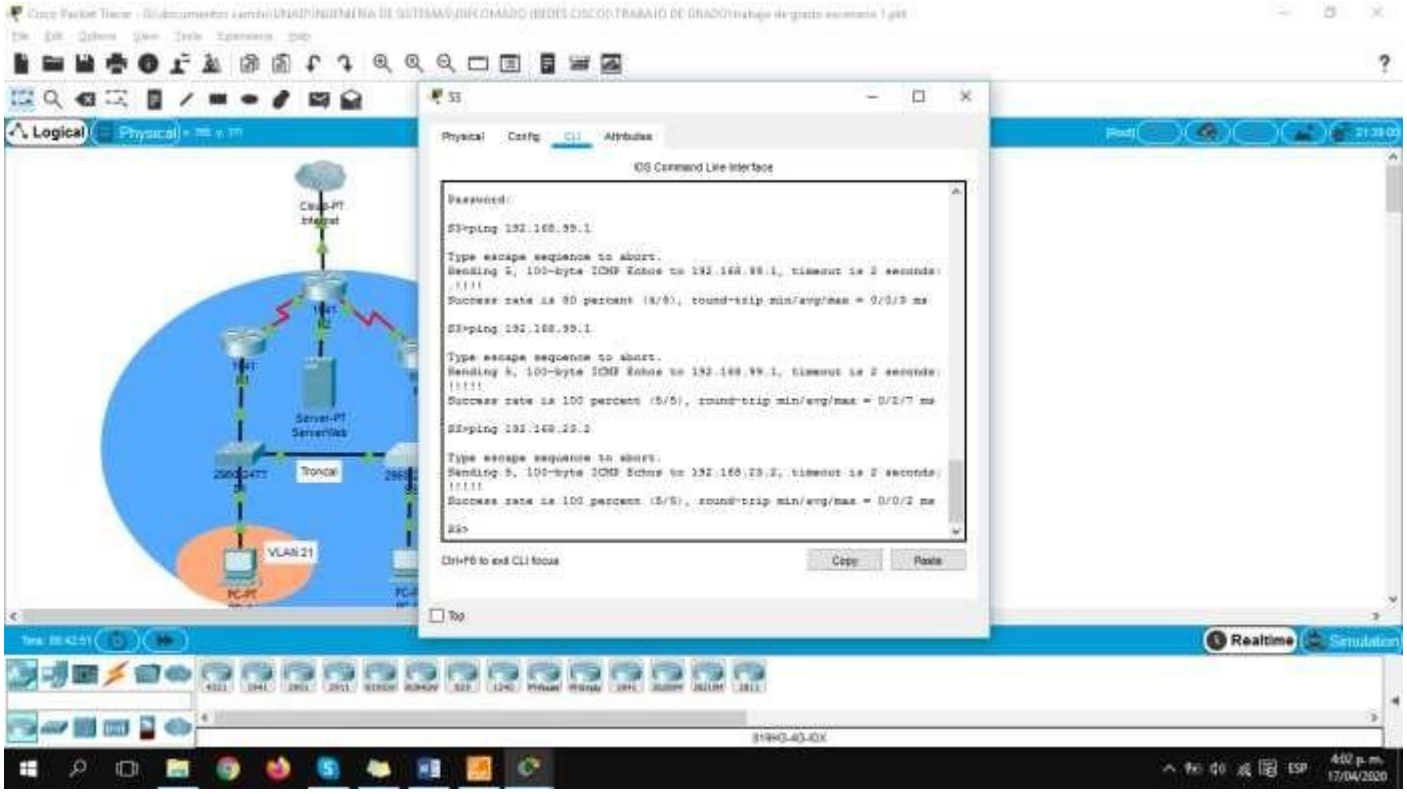
Paso 4: Verificar la conectividad de la red

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

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

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	EXITOSO
S3	R1, dirección VLAN 99	192.168.99.1	EXITOSO
S1	R1, dirección VLAN 21	192.168.21.2	EXITOSO
S3	R1, dirección VLAN 23	192.168.23.2	EXITOSO


S1
Physical
Config
CLI
Attributes
IOS Command Line Interface
Password:
S1>ping 192.168.99.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms
S1>ping 192.168.99.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
S1>ping 192.168.21.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.21.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
S1>
Ctrl+F6 to exit CLI focus
Copy
Paste
Top
Logical
Physical
Realtime
Simulation
Server-PT
ServerVlan
Troncal
VLAN 21
PC-PT


S3
Physical
Config
CLI
Attributes
IOS Command Line Interface
Password:
S3>ping 192.168.99.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms
S3>ping 192.168.99.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/7 ms
S3>ping 192.168.23.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.23.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/2 ms
S3>
Ctrl+F6 to exit CLI focus
Copy
Paste
Top
Logical
Physical
Realtime
Simulation
Server-PT
ServerVlan
Troncal
VLAN 21
PC-PT

Parte 4: Configurar el protocolo de routing dinámico RIPv2

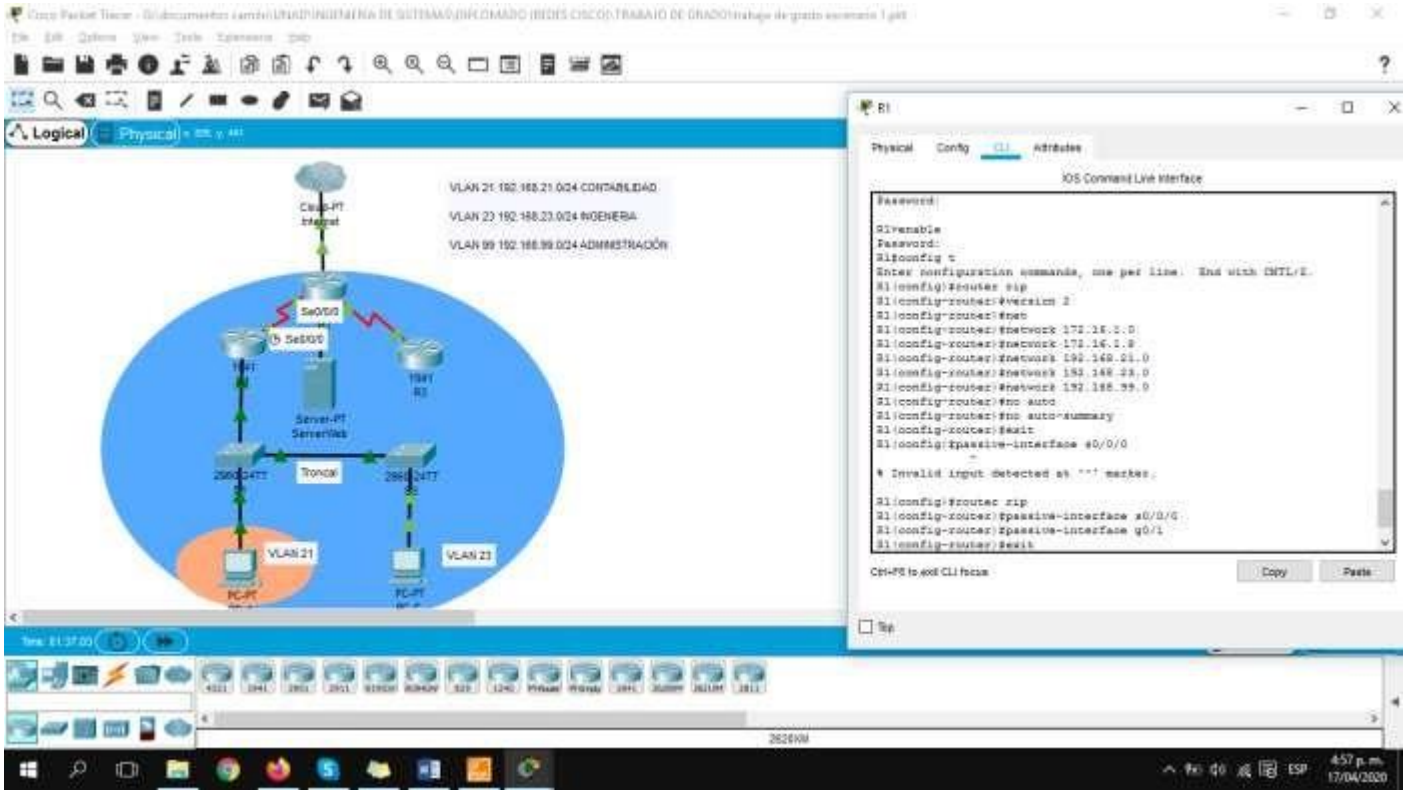
Paso 1: Configurar RIPv2 en el R1

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	
Anunciar las redes conectadas directamente	Asigne todas las redes conectadas directamente.
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

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



Paso 2: Configurar RIPv2 en el R2

La configuración del R2 incluye las siguientes tareas:

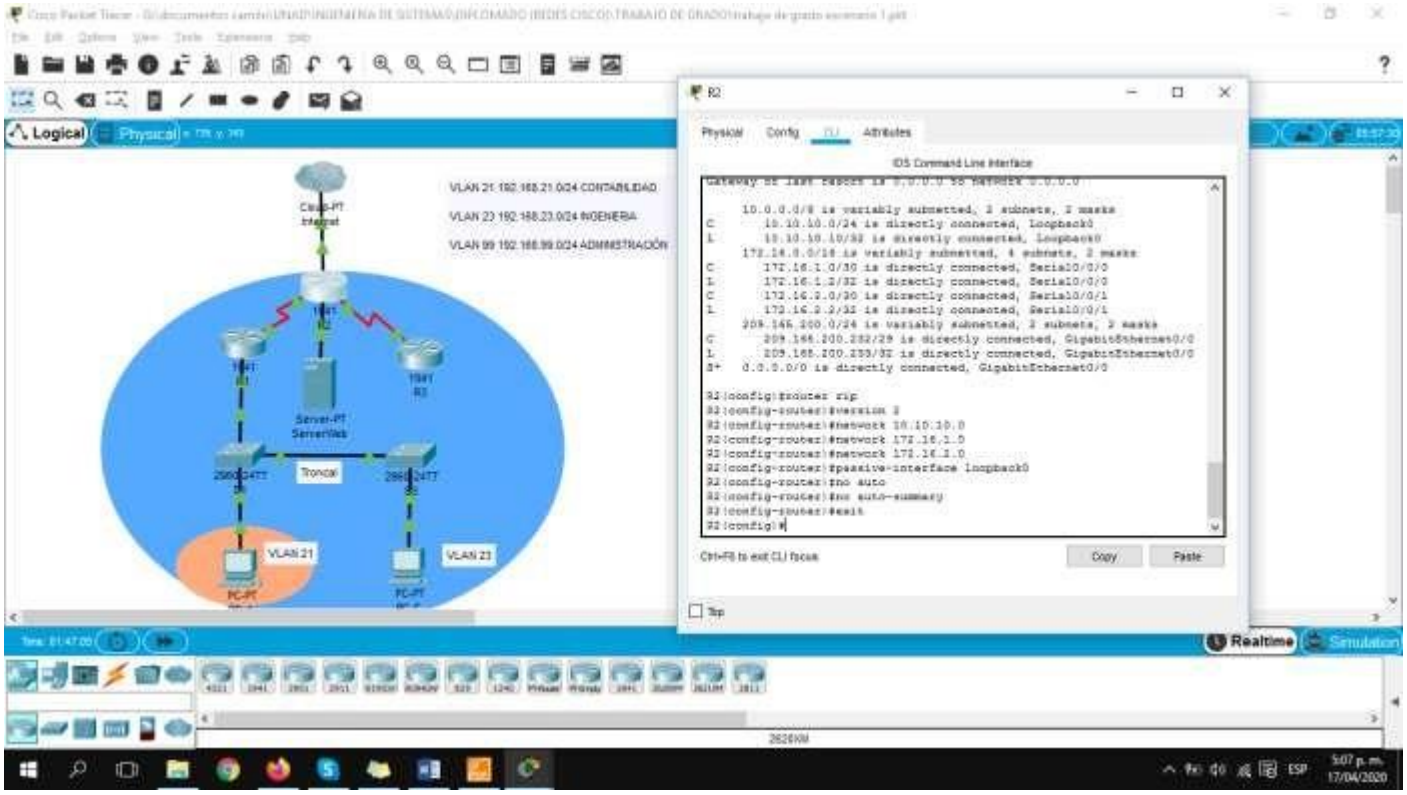
Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	
Anunciar las redes conectadas directamente	**Nota:** Omitir la red G0/0.
Establecer la interfaz LAN (loopback) como pasiva	R2(config-router)#passive-interface loopback0
Desactive la sumarización automática.	R2(config-router)#no auto-summary

Configurar RIP versión 2

R2(config)#router rip
R2(config-router)#version 2

Anunciar las redes conectadas directamente

R2(config-router)#network 10.10.10.0
R2(config-router)#network 172.16.1.0
R2(config-router)#network 172.16.2.0
R2(config-router)#exit



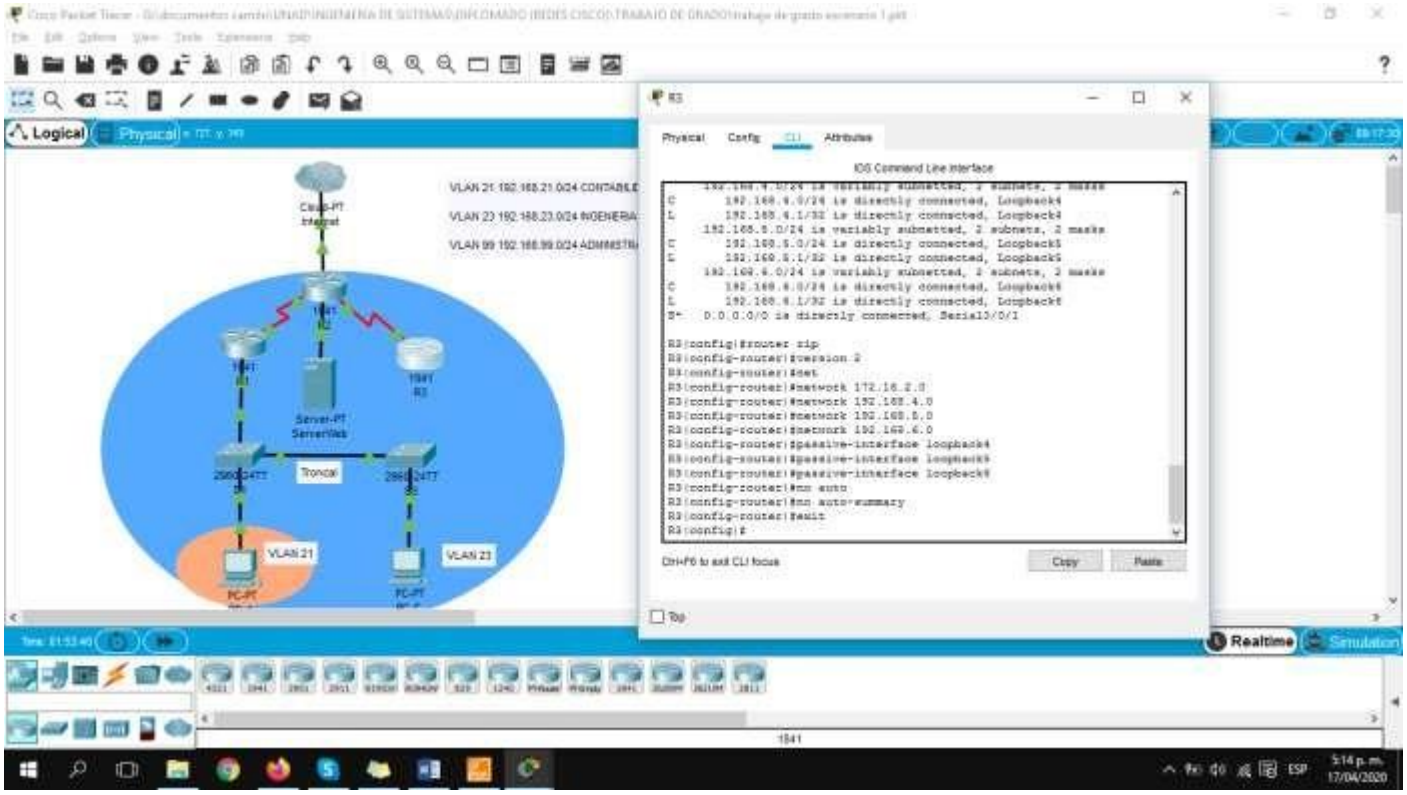
Paso 3: Configurar RIPv2 en el R3

La configuración del R3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	
Anunciar redes IPv4 conectadas directamente	
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

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



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:

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?	R1#show ip protocols
¿Qué comando muestra solo las rutas RIP?	R1#debug ip rip
¿Qué comando muestra la sección de RIP de la configuración en ejecución?	R1#show ip route

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:

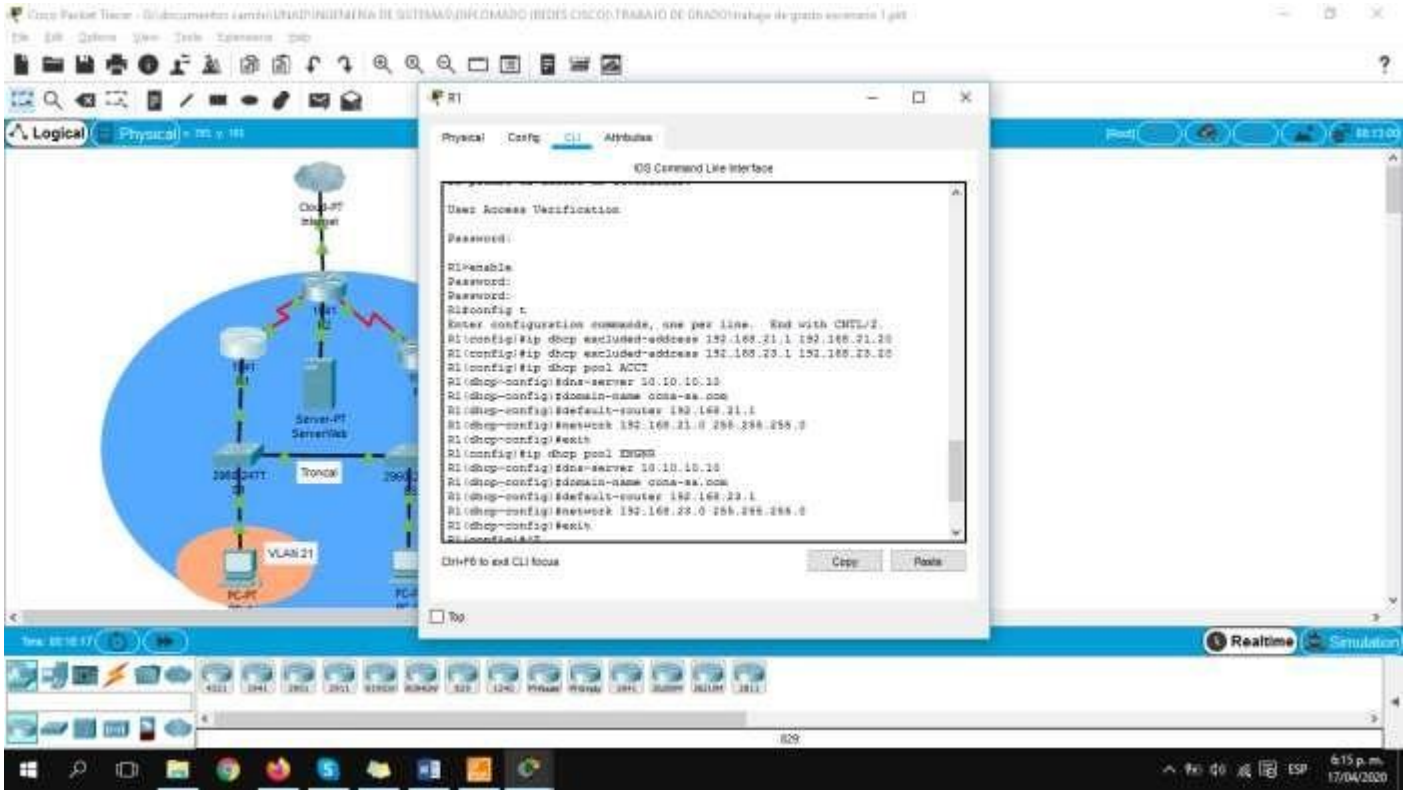
Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20
Crear un pool de DHCP para la VLAN 21.	Nombre: ACCT Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado
Crear un pool de DHCP para la VLAN 23	Nombre: ENGNR Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado

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:

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: **209.165.200.229**
Asignar la interfaz interna y externa para la NAT estática	

Configurar la NAT dinámica dentro de una ACL privada	Lista de acceso: 1 Permitir la traducción de las redes de Contabilidad y de Ingeniería en el R1 Permitir la traducción de un resumen de las redes LAN (loopback) en el R3
Defina el pool de direcciones IP públicas utilizables.	Nombre del conjunto: **INTERNET** El conjunto de direcciones incluye: **209.165.200.225 – 209.165.200.228**
Definir la traducción de NAT dinámica	

Crear una base de datos local con una cuenta de usuario

R2(config)#user webuser privilege 15 secret cisco12345

Asignar la interfaz interna y externa para la NAT estática.

R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229

R2(config)#interface g0/0

R2(config-if)#ip nat outside

R2(config-if)#interface g0/0

R2(config-if)#ip nat inside

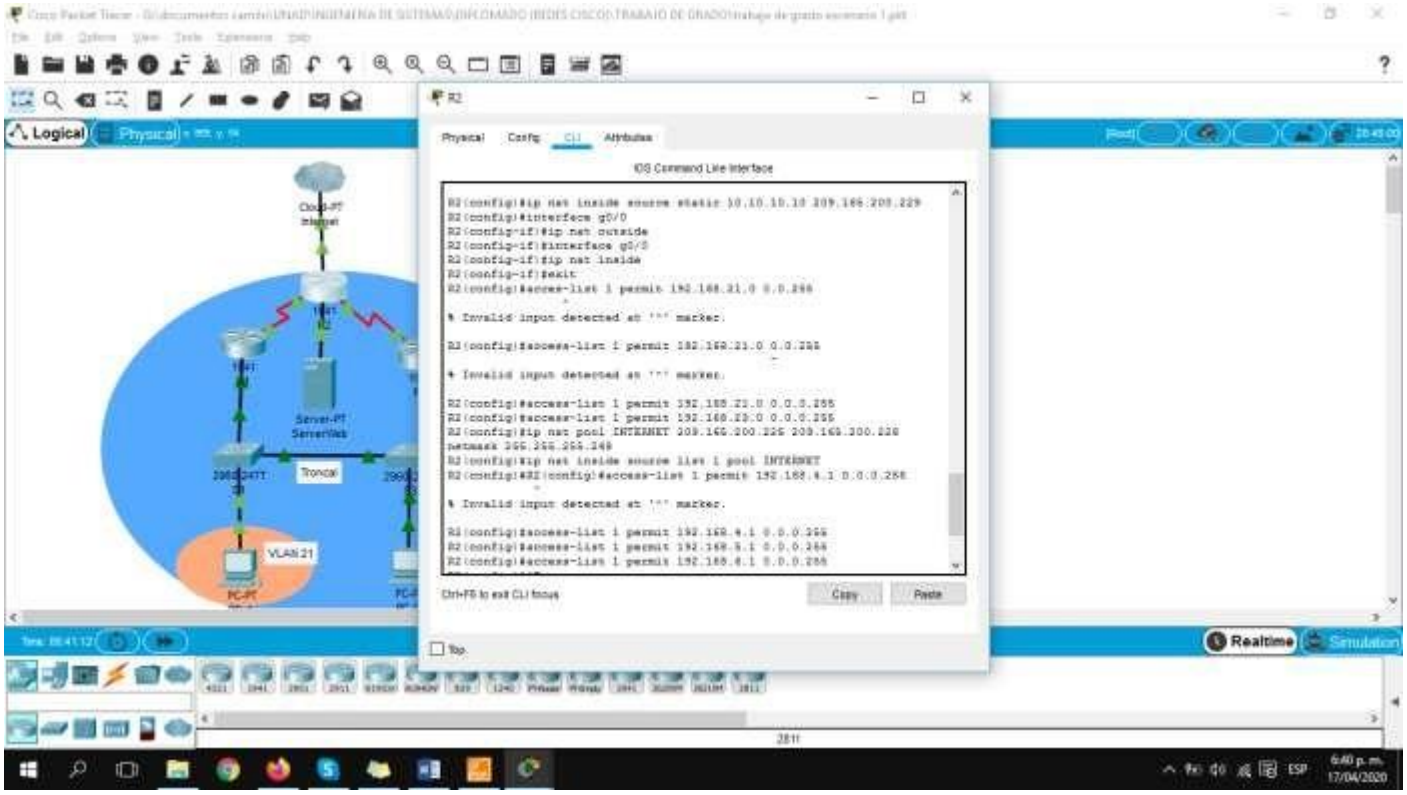
R2(config-if)#exit

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, Definir la traducción de NAT dinámica.

R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248
R2(config)#ip nat inside source list 1 pool INTERNET

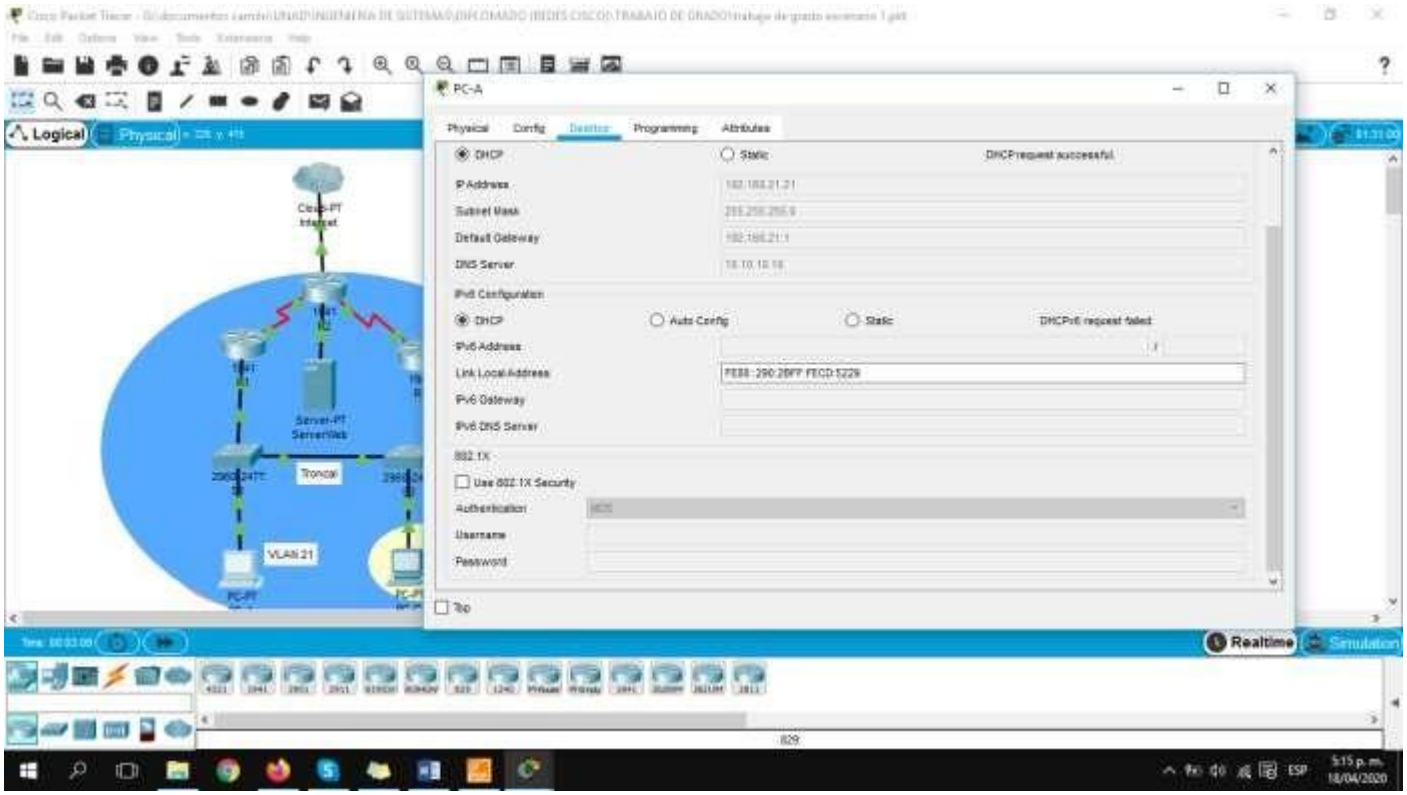


Paso 3: Verificar el protocolo DHCP y la NAT estática

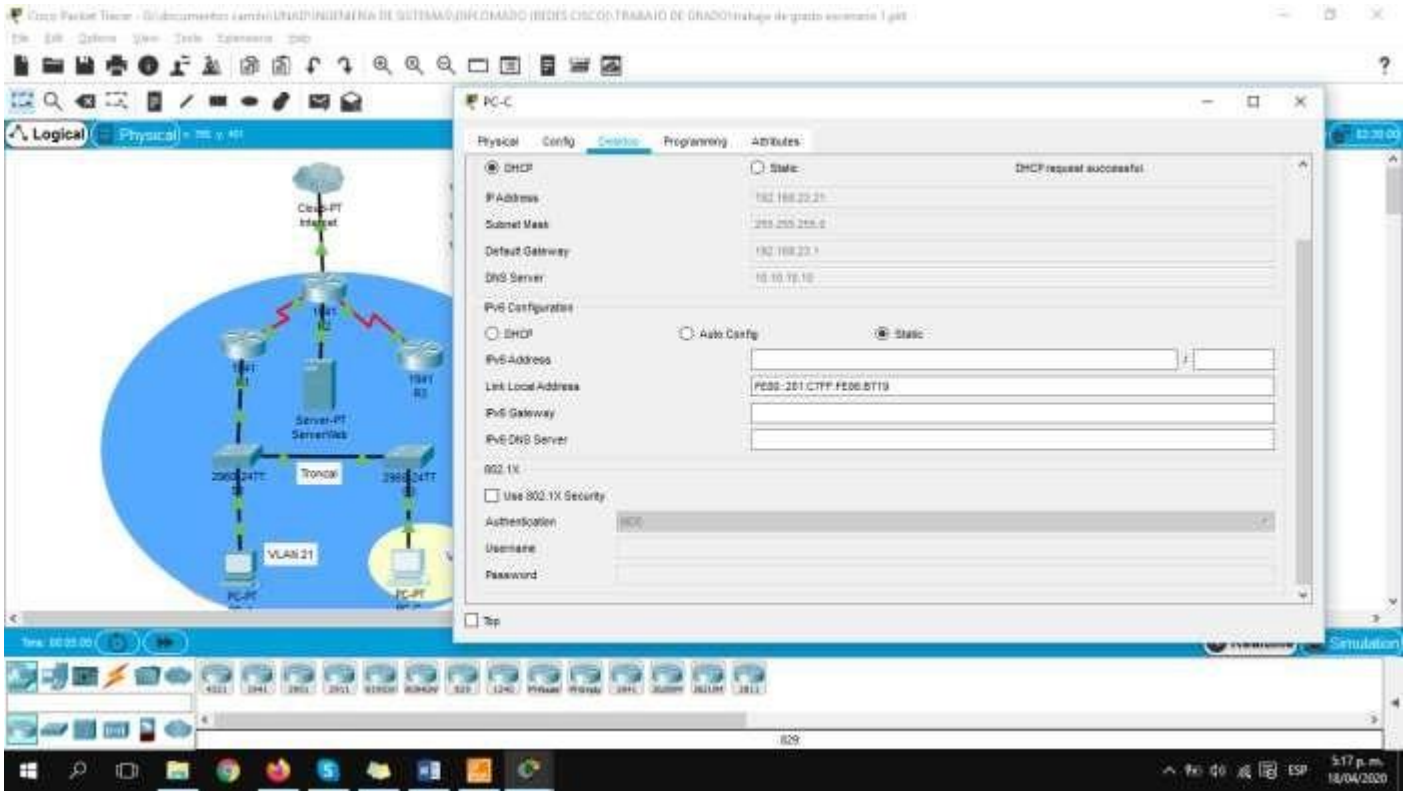
Utilice las siguientes tareas para verificar que las configuraciones de DHCP y NAT estática funcionen de forma correcta. Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

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.	Ping 192.168.23.21
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**	

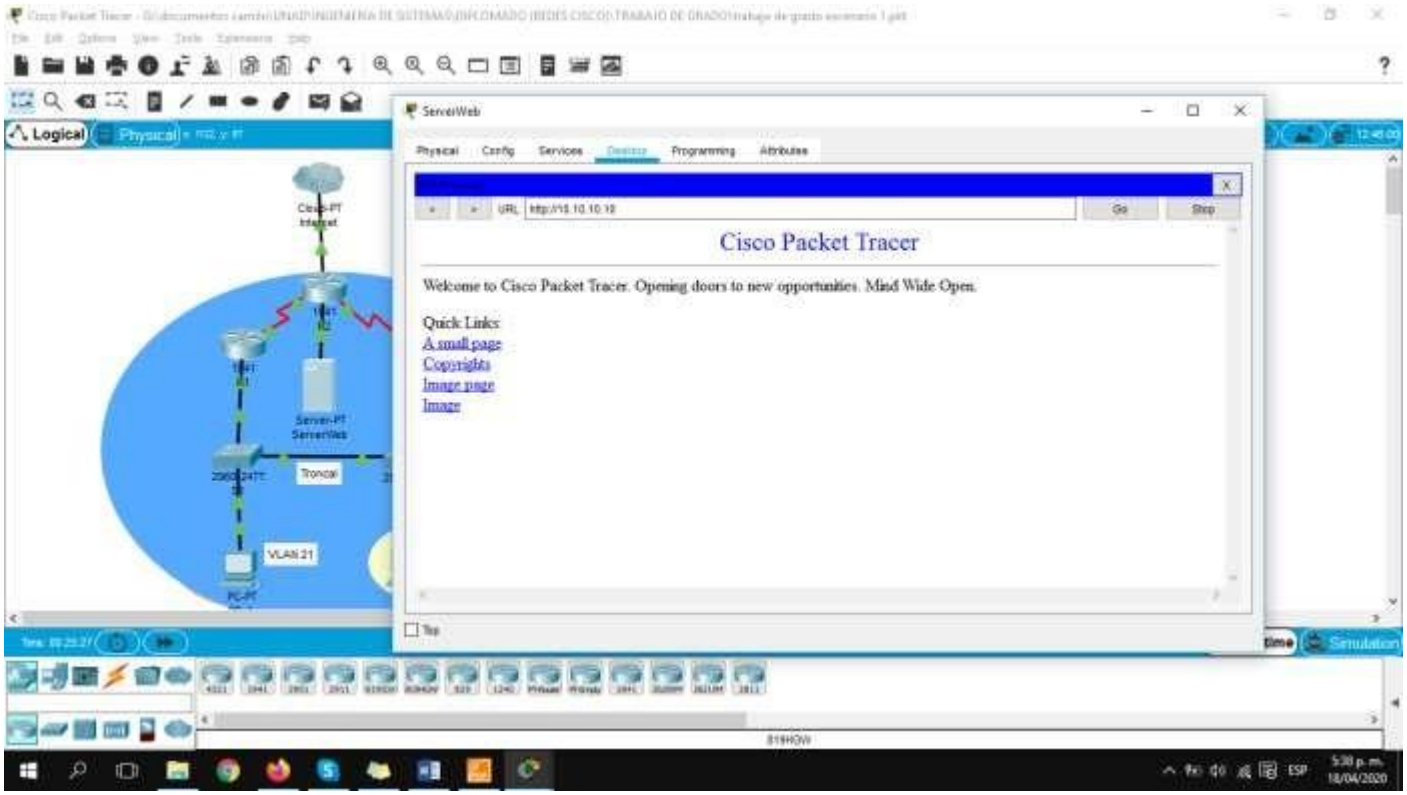
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP



Verificar que la PC-C haya adquirido información de IP del servidor de DHCP



Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.229)



Parte 6: Configurar NTP

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	**5 de marzo de 2016, 9 a. m.**
Configure R2 como un maestro NTP.	Nivel de estrato: **5** R2(config)#ntp master Stratum 5
Configurar R1 como un cliente NTP.	Servidor: **R2** R1(config)#ntp server 172.16.1.2
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	R1(config)#ntp update-calendar
Verifique la configuración de NTP en R1.	`R1(config)#do show ntp status`

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

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

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

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

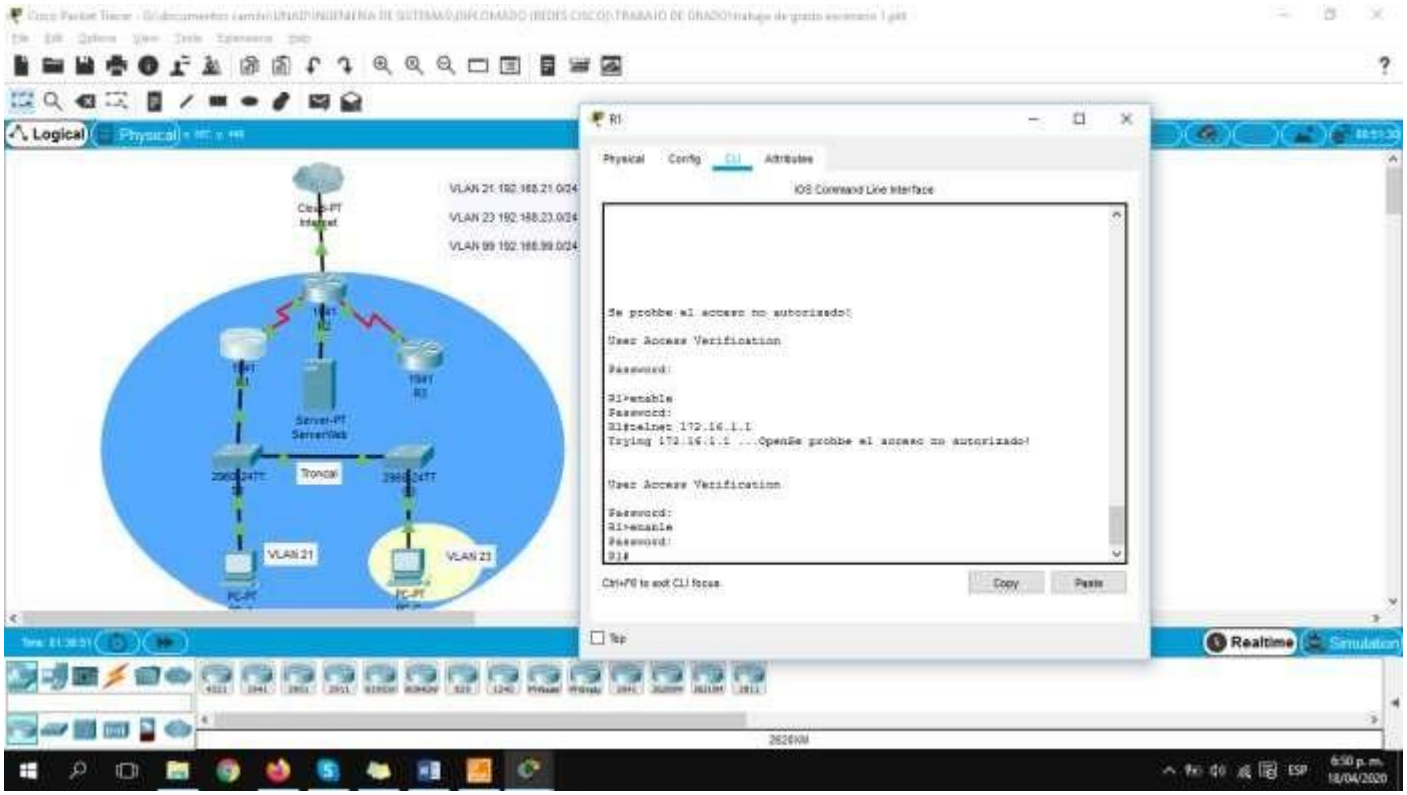
R2(config-std-nacl)#exit

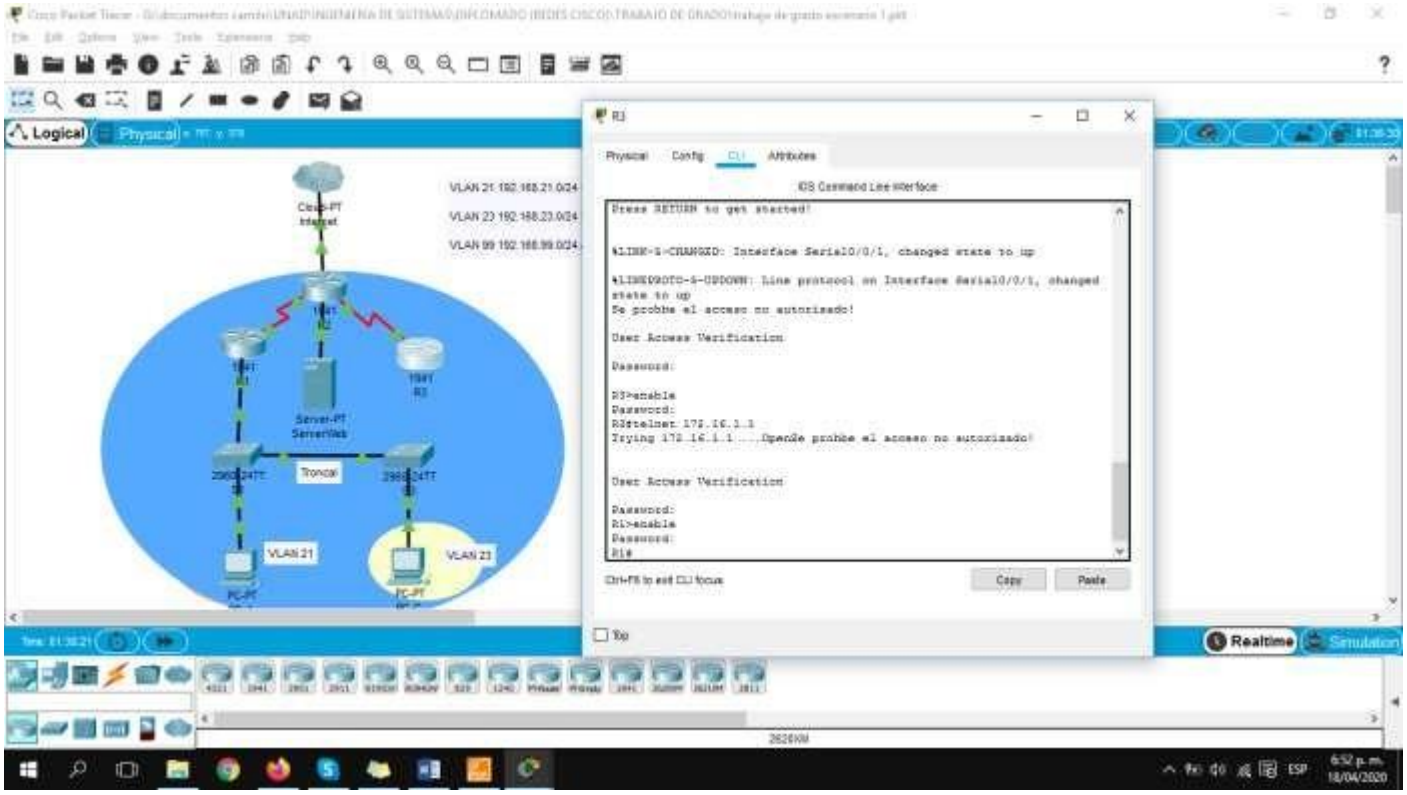
Aplicar la ACL con nombre a las líneas VTY, Permitir acceso por Telnet a las líneas de VTY

R2(config)#line vty 0 4
R2(config-line)#access-class ADMIN-MGT in

R2(config-line)#exit

Verificar que la ACL funcione como se espera:


R1
Physical
Config
CLI
Attributes
IOS Command Line Interface
Se probbe el accesso no autorizado!
User Access Verification
Password:
R1>enable
Password:
R1#telnet 172.16.1.1
Trying 172.16.1.1 ...Open Se probbe el accesso no autorizado!
User Access Verification
Password:
R1>enable
Password:
R1#
Ctrl+F6 to exit CLI focus
Copy
Paste
Top
Logical
Physical
VLAN 21 192.168.21.0/24
VLAN 23 192.168.23.0/24
VLAN 99 192.168.99.0/24
Cisco-PT Internet
Server-PT ServerWeb
Trunk
VLAN 21
VLAN 23
PC-PT
Realtime
Simulation


R1
Physical
Config
CLI
Attributes
IOS Command Line Interface
Press RETURN to get started!
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up
Se probbe el accesso no autorizado!
User Access Verification
Password:
R1>enable
Password:
R1#telnet 172.16.1.1
Trying 172.16.1.1 ...Open Se probbe el accesso no autorizado!
User Access Verification
Password:
R1>enable
Password:
R1#
Ctrl+F6 to exit CLI focus
Copy
Paste
Top
Logical
Physical
VLAN 21 192.168.21.0/24
VLAN 23 192.168.23.0/24
VLAN 99 192.168.99.0/24
Cisco-PT Internet
Server-PT ServerWeb
Trunk
VLAN 21
VLAN 23
PC-PT
Realtime
Simulation

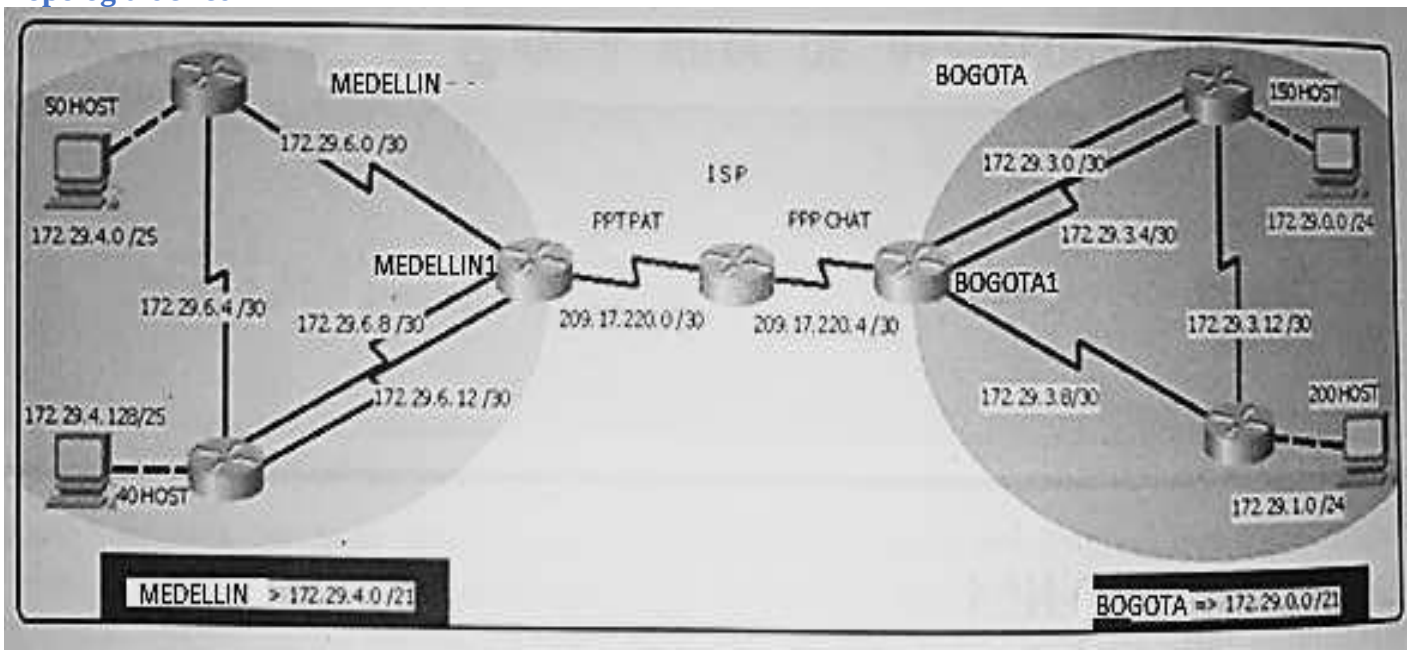
Paso 2: Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	Router(config)#show access-list
Restablecer los contadores de una lista de acceso	Router(config)#clear access-list counters
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	Router(config)#interface Fa0/1 Router(config-if)#ip access-group 1 out
¿Con qué comando se muestran las traducciones NAT?	Router(config)#show ip nat translations **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

Escenario 2

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

Topología de red



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.

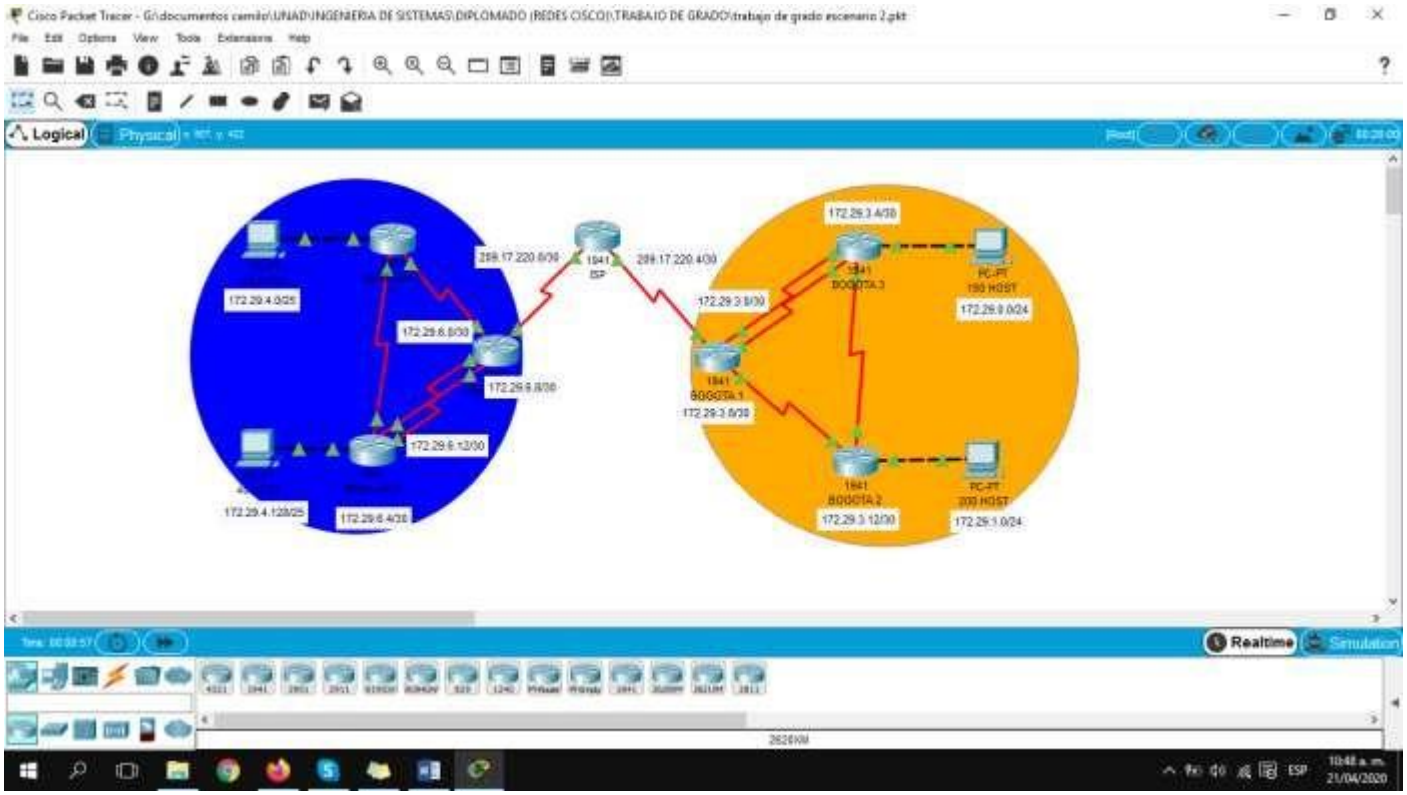
Debe configurar PPP en los enlaces hacia el ISP, con autenticación. Debe

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



Configuración a 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

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

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 2.2.2.2
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 3.3.3.3
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 4.4.4.4
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 0.0.0.255 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 0.0.0.255 area 0
MEDELLIN3(config-router)#network 172.29.6.4 0.0.0.3 area 0
MEDELLIN3(config-router)#network 172.29.6.8 0.0.0.3 area 0
MEDELLIN3(config-router)#network 172.29.6.12 0.0.0.3 area 0
MEDELLIN3(config-router)#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
```

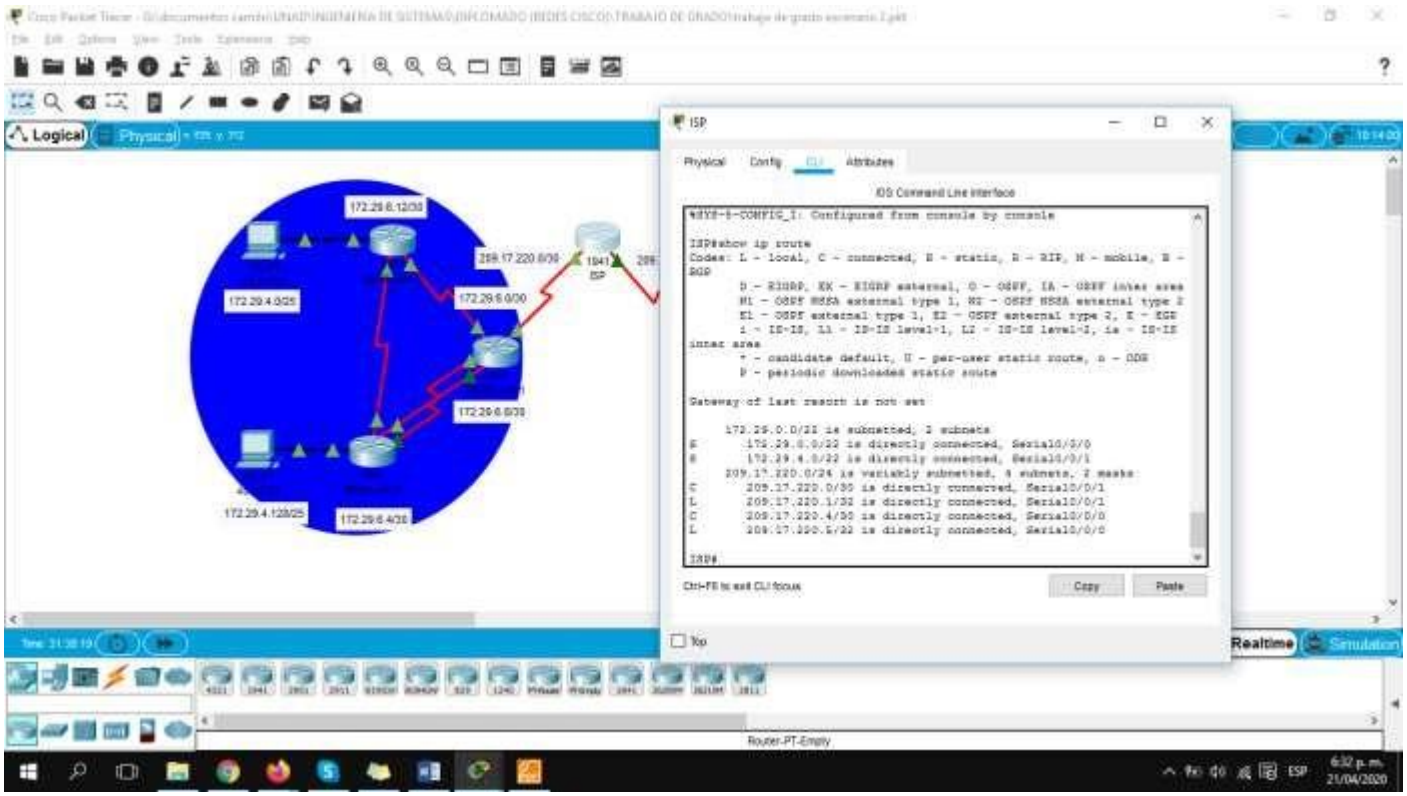
c. El router ISP deberá tener una ruta estática dirigida hacia cada red interna de Bogotá y Medellín para el caso se sumarizan las subredes de cada uno a /22.

```
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
```

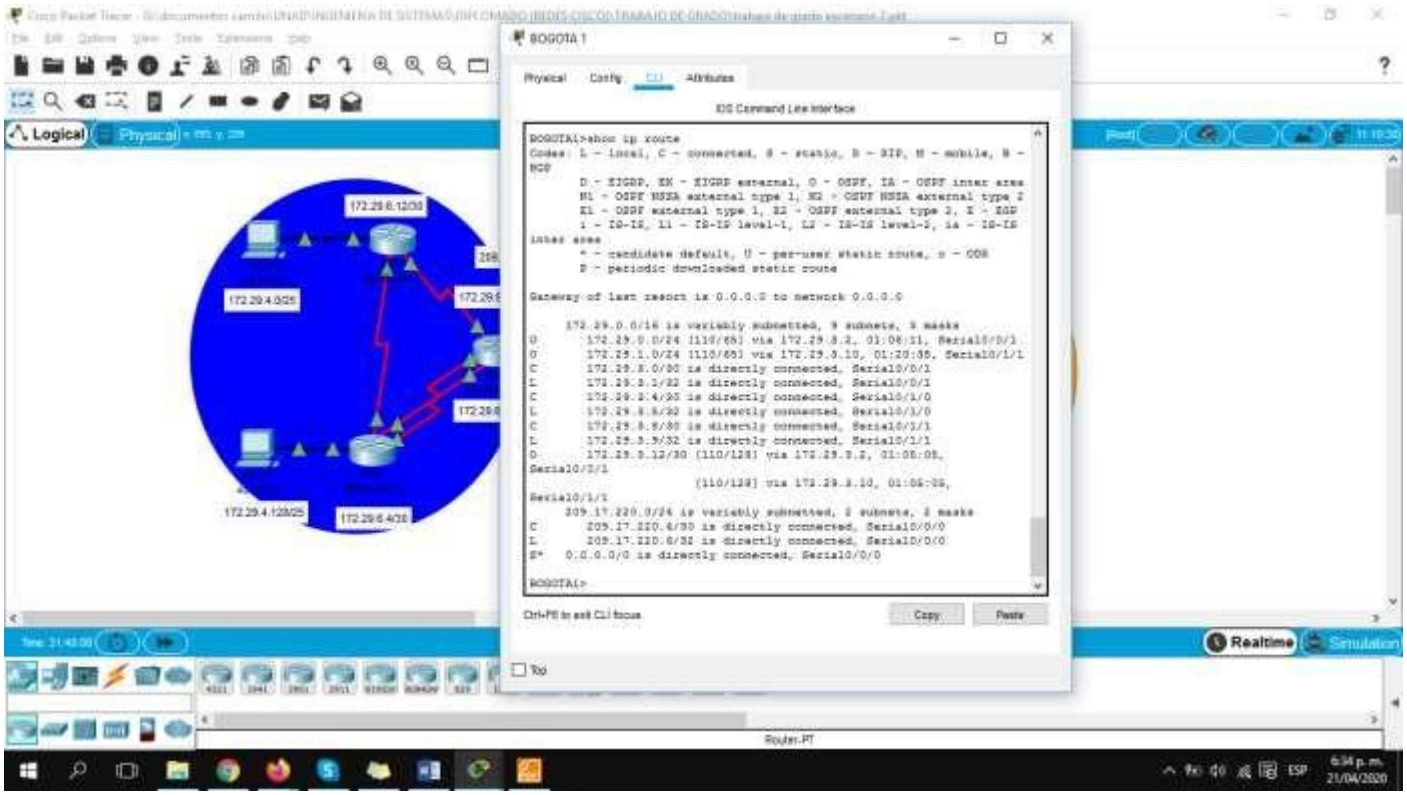
Parte 2: Tabla de Enrutamiento.

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.

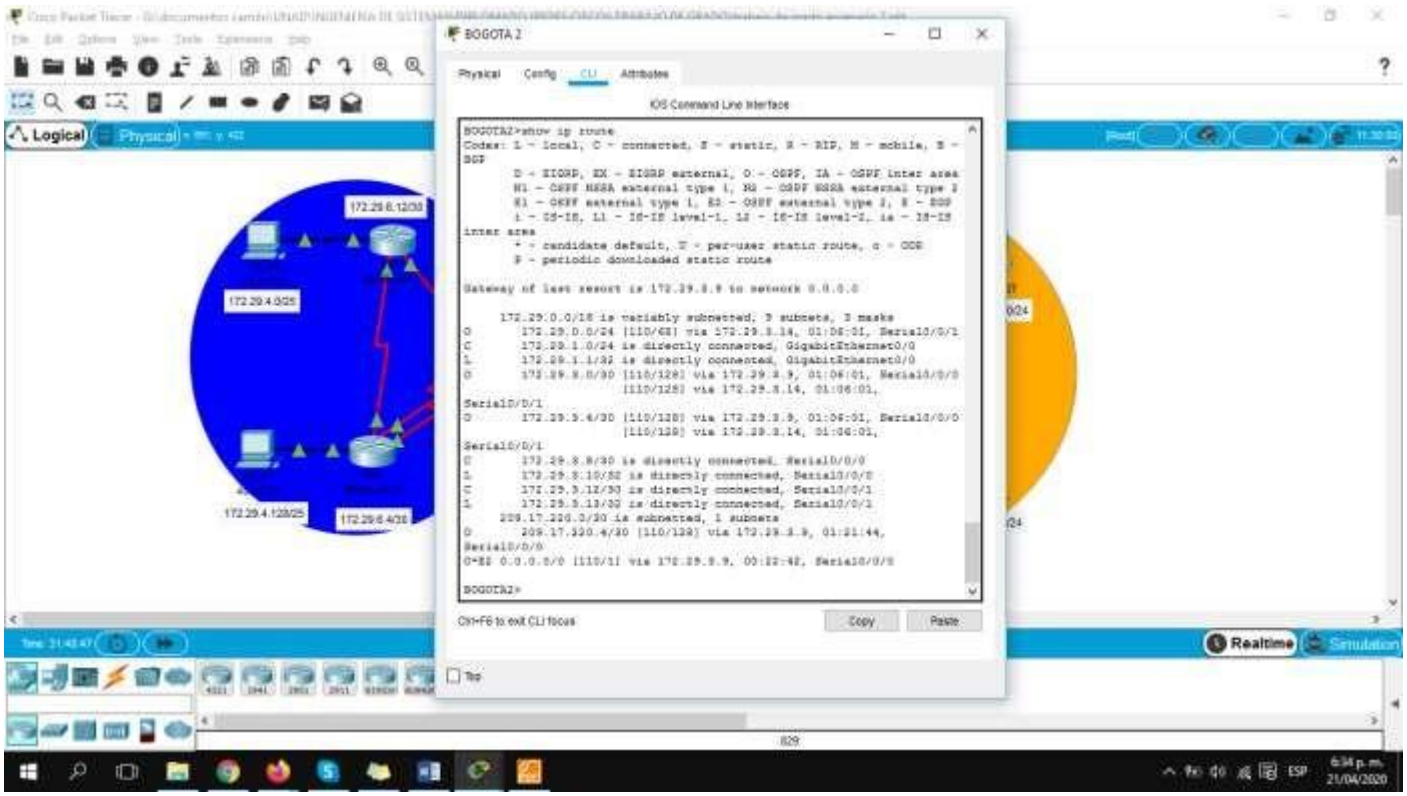
ISP:


ISP
Physical
Config
CLI
Attributes
IOS Command Line Interface
%SYS-5-CONFIG_I: Configured from console by console
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
C 172.29.0.0/22 is directly connected, Serial0/0/0
C 172.29.4.0/22 is directly connected, Serial0/0/1
209.17.220.0/24 is variably subnetted, 4 subnets, 2 masks
C 209.17.220.0/30 is directly connected, Serial0/0/1
L 209.17.220.1/32 is directly connected, Serial0/0/1
C 209.17.220.4/30 is directly connected, Serial0/0/0
L 209.17.220.5/32 is directly connected, Serial0/0/0
ISP#
Ctrl+F6 to exit CLI focus
Copy
Paste
Top
172.29.6.12/30
172.29.4.0/25
209.17.220.8/30
172.29.6.0/30
172.29.6.8/30
172.29.4.128/25
172.29.6.4/30
1941
Logical
Physical
Realtime
Simulation
Router-PT-Empty
ESP
6:32 p. m.
21/04/2020

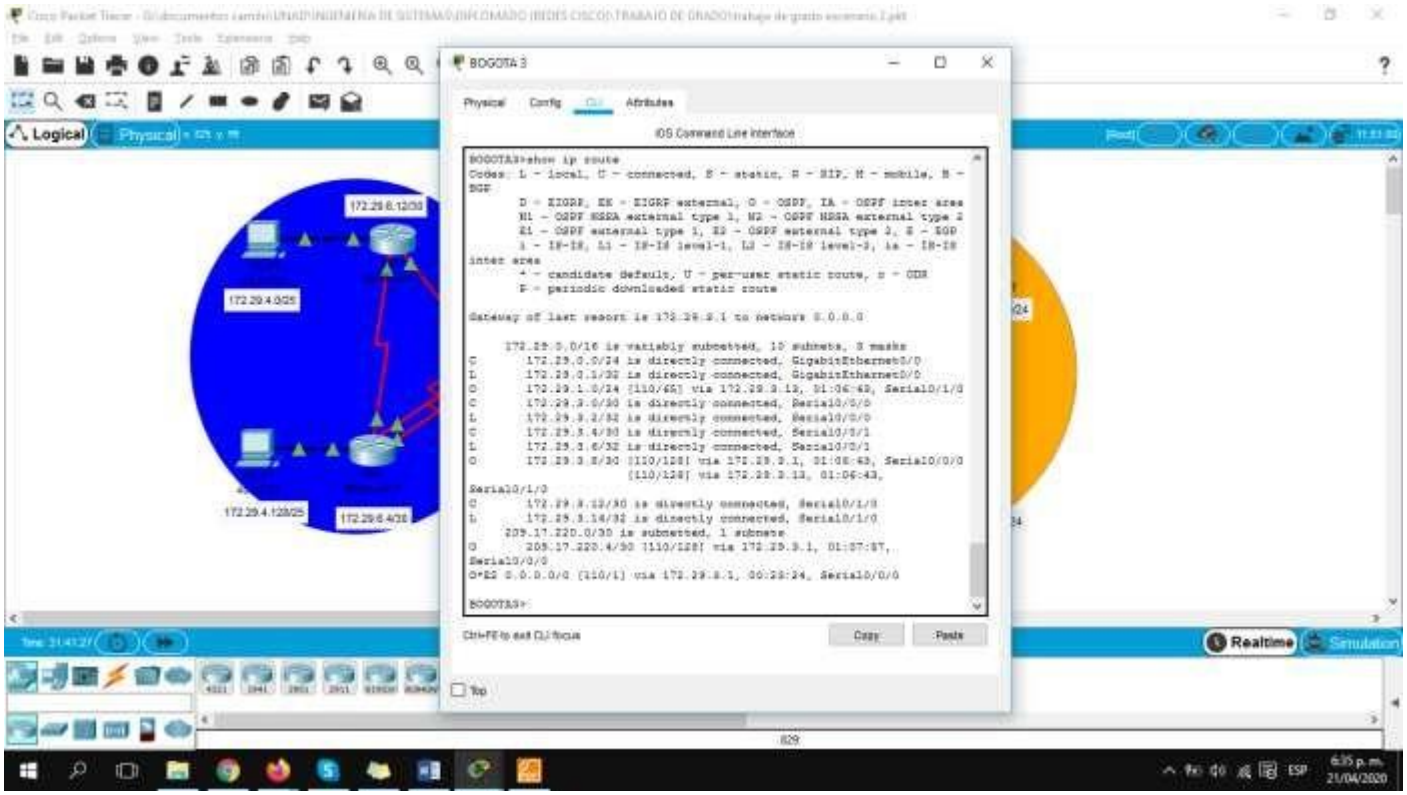
BOGOTA1:


BOGOTA 1
Physical
Config
CLI
Attributes
IOS Command Line Interface
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 0.0.0.0 to network 0.0.0.0
172.29.0.0/16 is variably subnetted, 9 subnets, 3 masks
O 172.29.0.0/24 [110/65] via 172.29.3.2, 01:06:11, Serial0/0/1
O 172.29.1.0/24 [110/65] via 172.29.3.10, 01:20:05, 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
C 172.29.3.4/30 is directly connected, Serial0/1/0
L 172.29.3.5/32 is directly connected, Serial0/1/0
C 172.29.3.8/30 is directly connected, Serial0/1/1
L 172.29.3.9/32 is directly connected, Serial0/1/1
O 172.29.3.12/30 [110/128] via 172.29.3.2, 01:06:06, Serial0/0/1
[110/128] via 172.29.3.10, 01:06:06, Serial0/1/1
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 is directly connected, Serial0/0/0
BOGOTA1>
Ctrl+F6 to exit CLI focus
Copy
Paste
Top
172.29.6.12/30
172.29.4.0/25
172.29.6.8/30
172.29.4.128/25
172.29.6.4/30
Logical
Physical
Realtime
Simulation
Router-PT
ESP
6:34 p. m.
21/04/2020

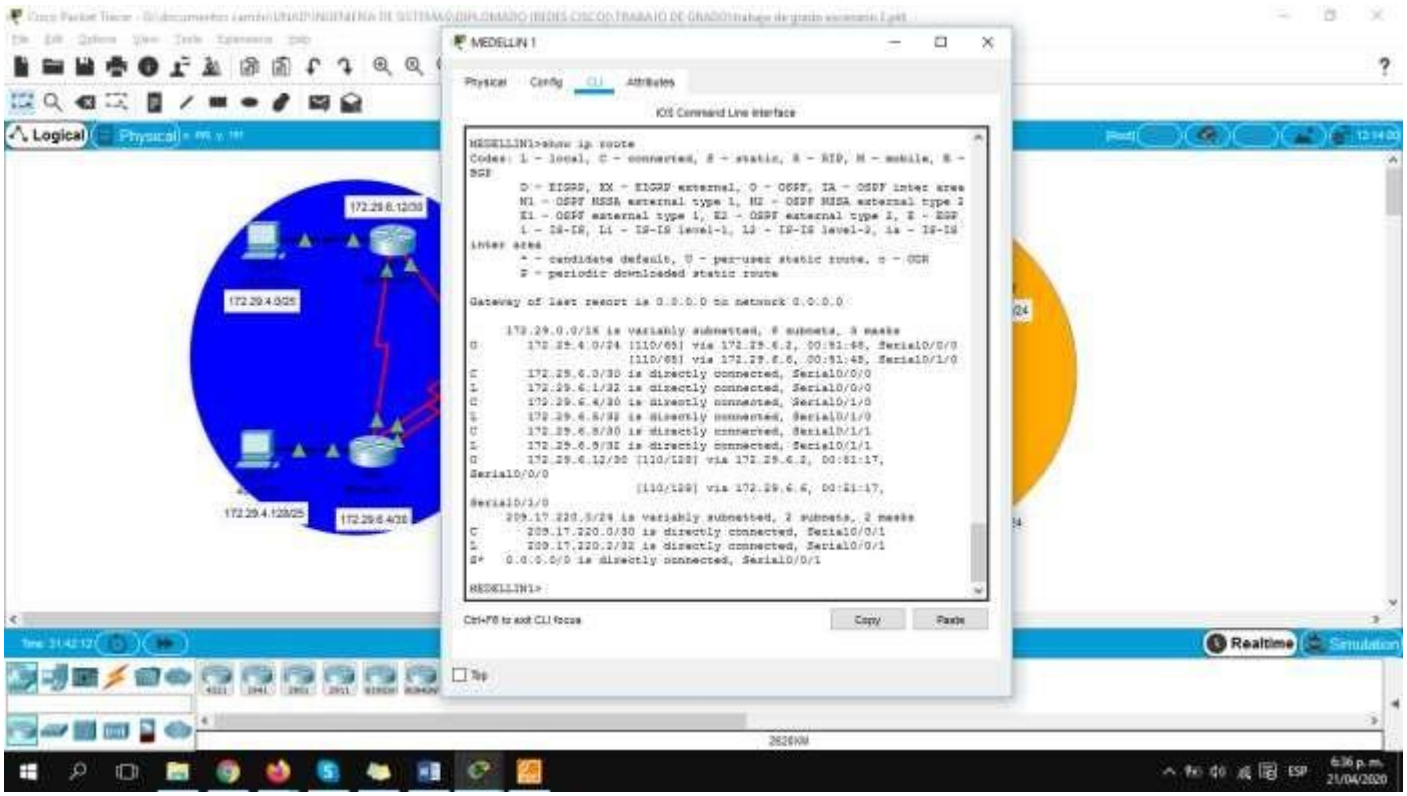
BOGOTA2:



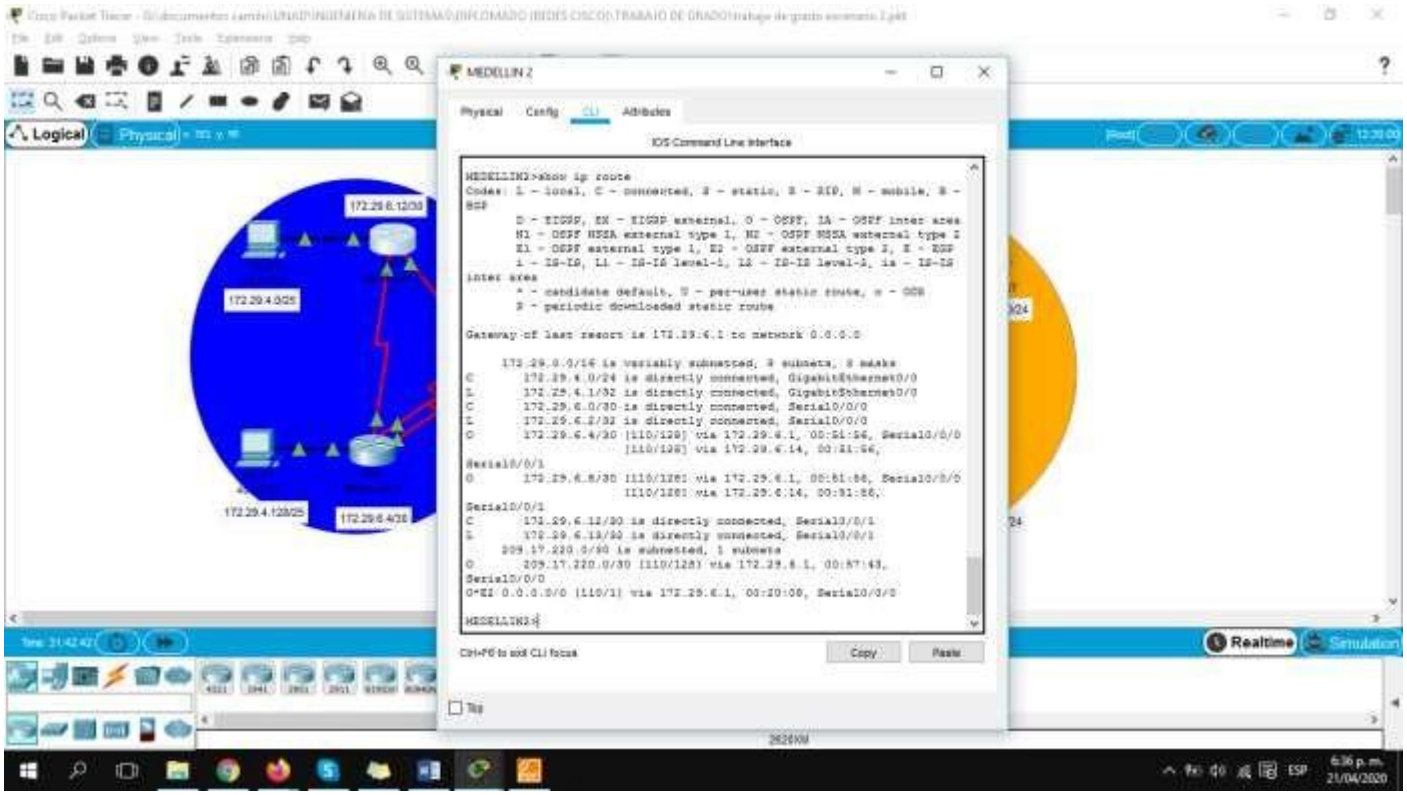
BOGOTA3:



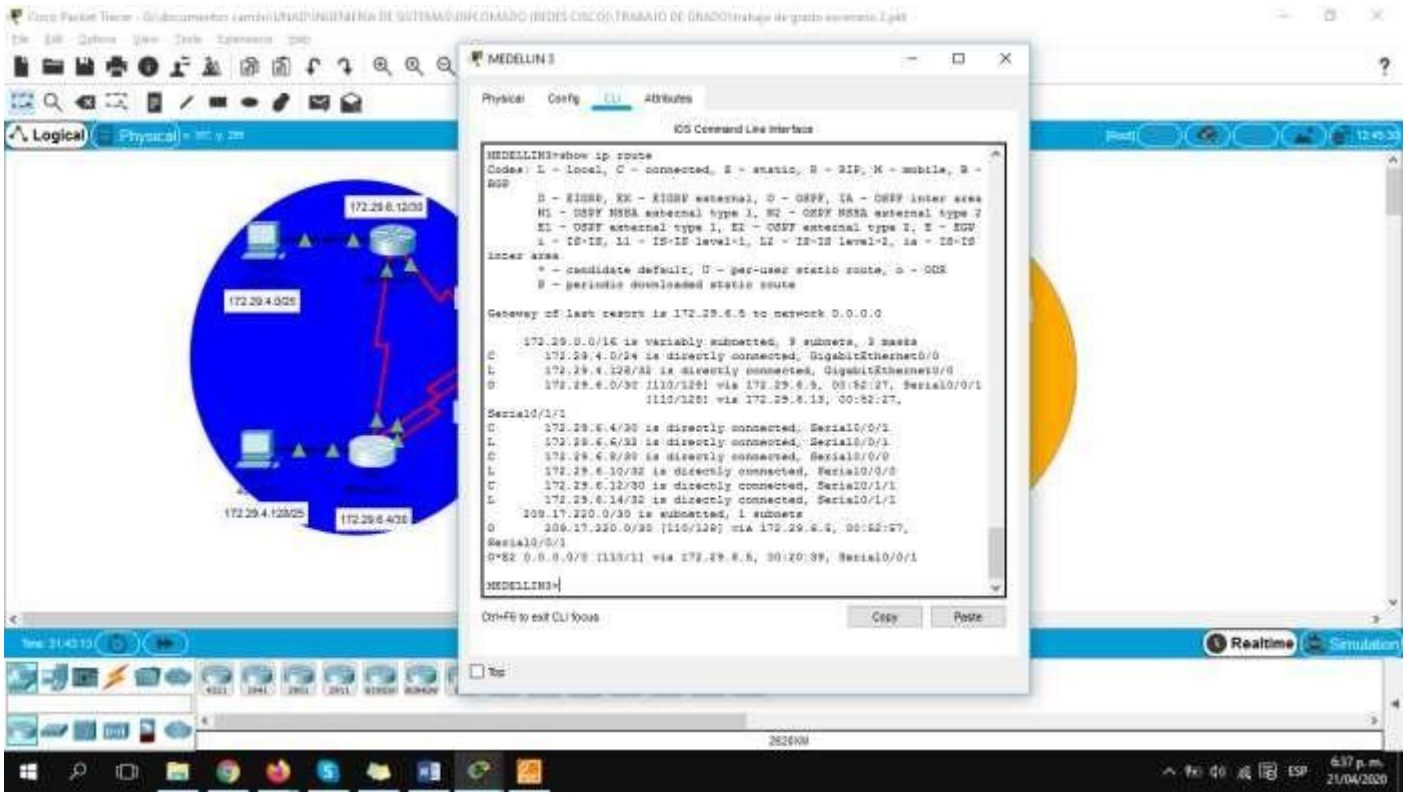
MEDELLIN1:



MEDELLIN2:



MEDELLIN3:



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 passive 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.

Parte 5: Configurar encapsulamiento y autenticación PPP.

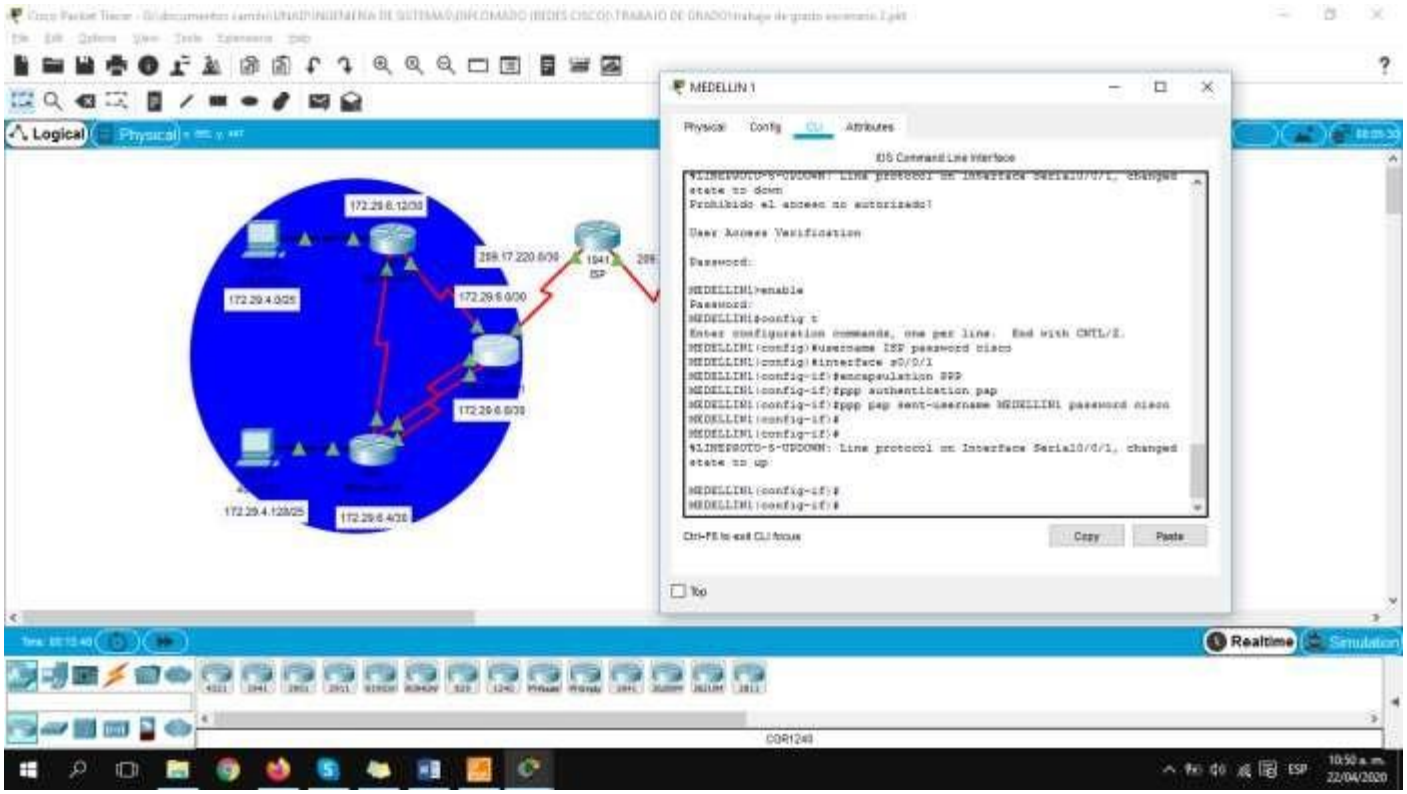
a. Según la topología se requiere que el enlace Medellín1 con ISP sea configurado con autenticación PAT.

ISP(config)#username MEDELLIN1 password cisco
ISP(config)#interface s0/0/1
ISP(config-if)#encapsulation PPP

ISP(config-if)#PPP authentication PAP

ISP(config-if)#PPP PAP sent-username ISP password cisco

MEDELLIN1(config)#username ISP password cisco
MEDELLIN1(config)#interface s0/0/1
MEDELLIN1(config-if)#encapsulation PPP
MEDELLIN1(config-if)#ppp authentication pap
MEDELLIN1(config-if)#ppp pap sent-username MEDELLIN1 password cisco

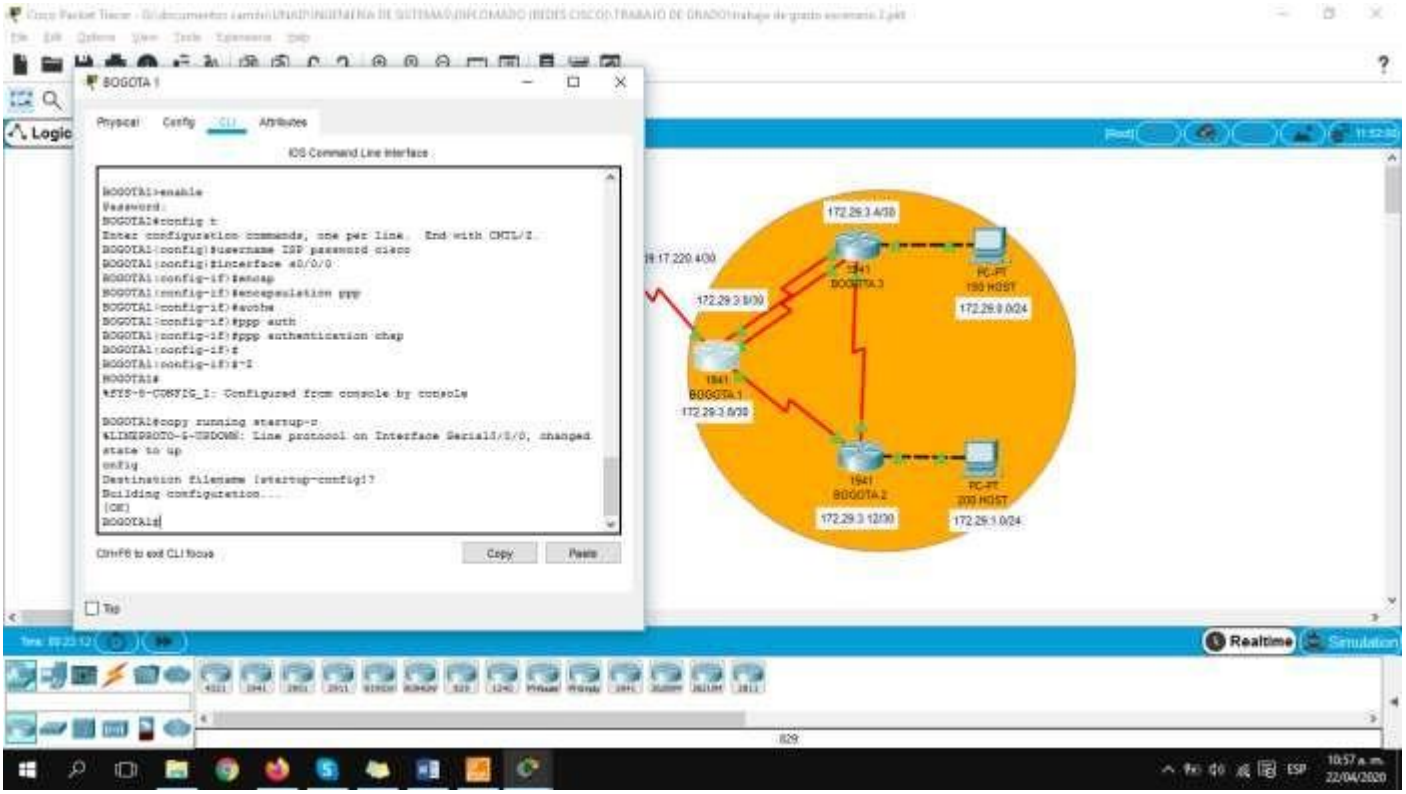


b. El enlace Bogotá1 con ISP se debe configurar con autenticación CHAT.

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

ISP(config-if)#ppp authentication chap

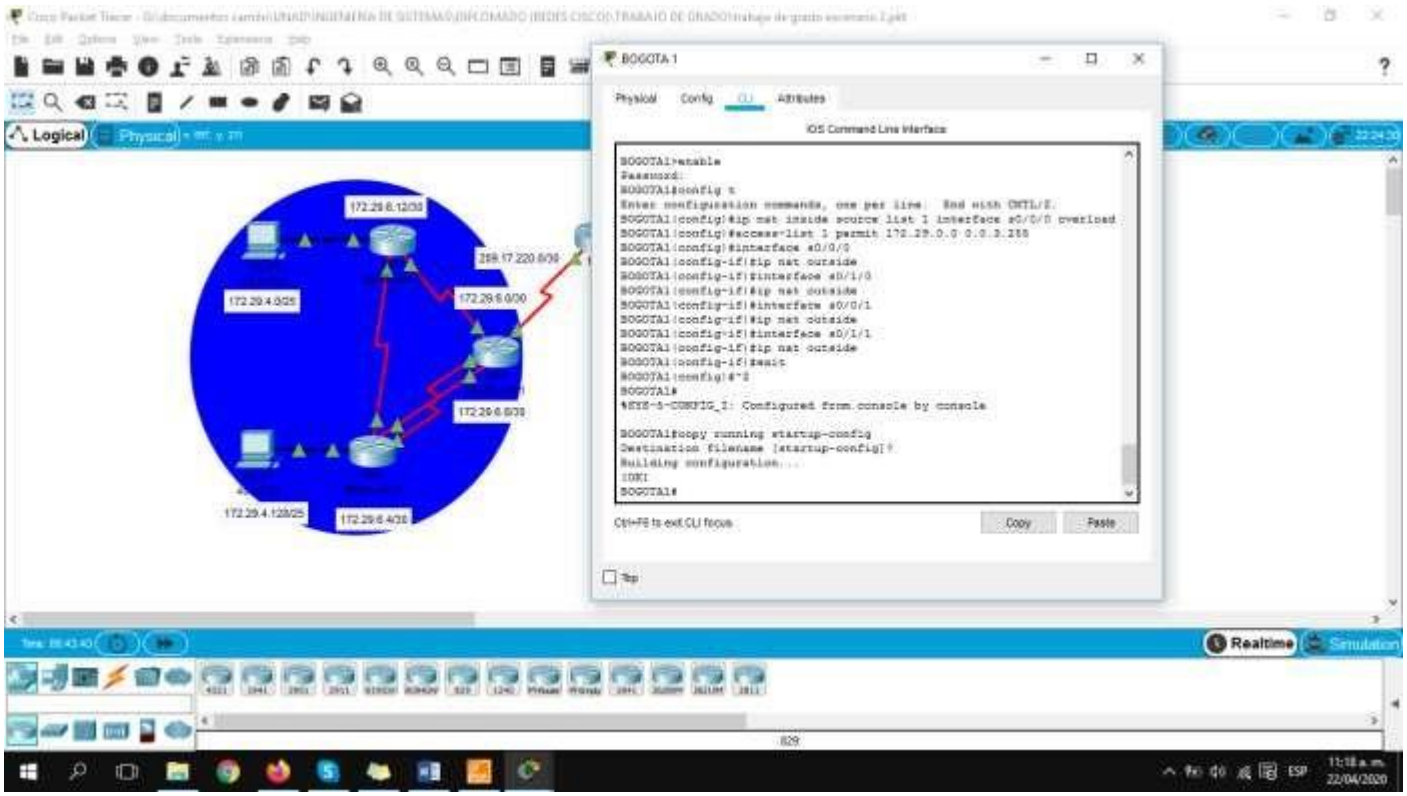
BOGOTA1(config)#username ISP password cisco
BOGOTA1(config)#interface s0/0/0
BOGOTA1(config-if)#encapsulation ppp
BOGOTA1(config-if)#ppp authentication chap



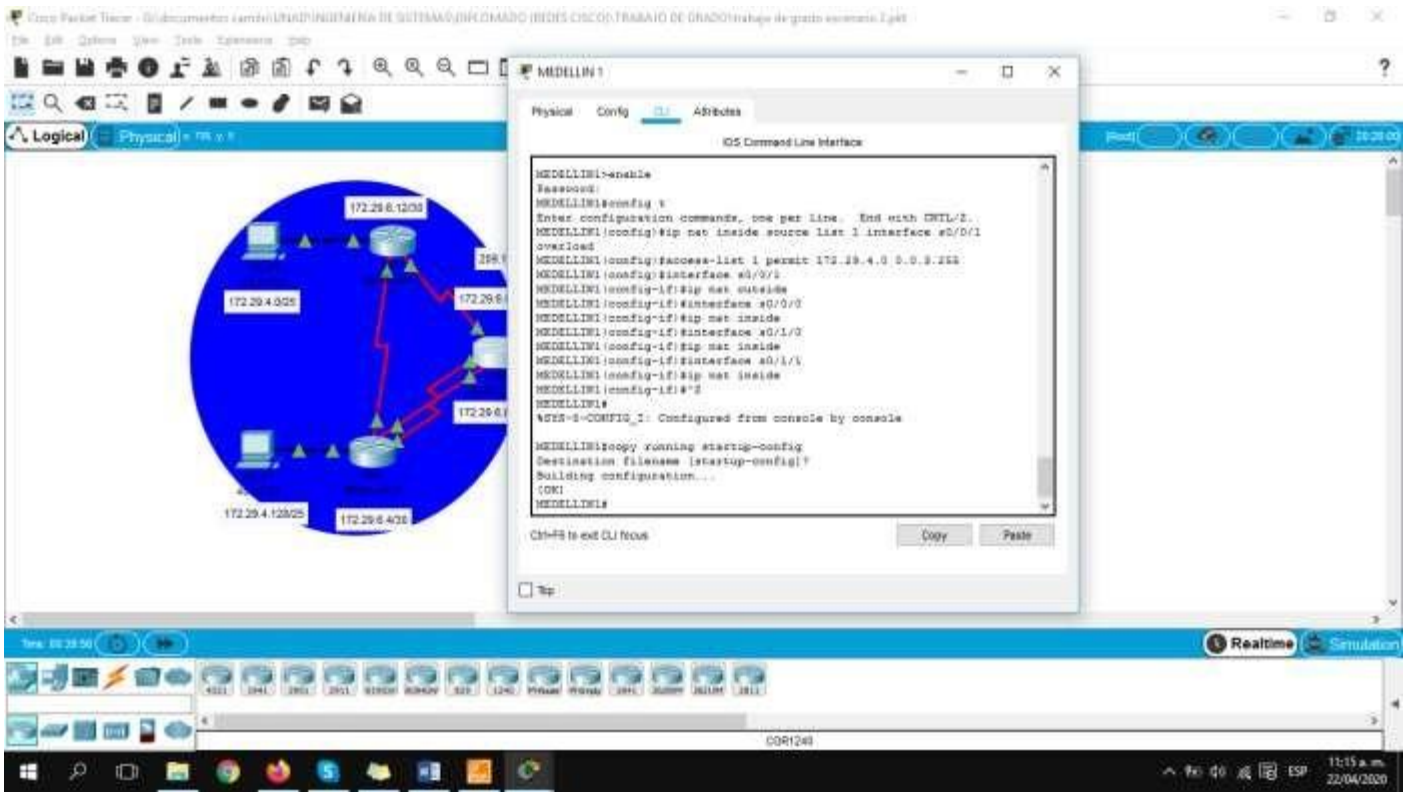
Parte 6: Configuración de PAT.

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 outside
BOGOTA1(config-if)#interface s0/1/0
BOGOTA1(config-if)#ip nat outside
BOGOTA1(config-if)#interface s0/0/1
BOGOTA1(config-if)#ip nat outside
BOGOTA1(config-if)#interface s0/1/1
BOGOTA1(config-if)#ip nat outside
BOGOTA1(config-if)#exit
```

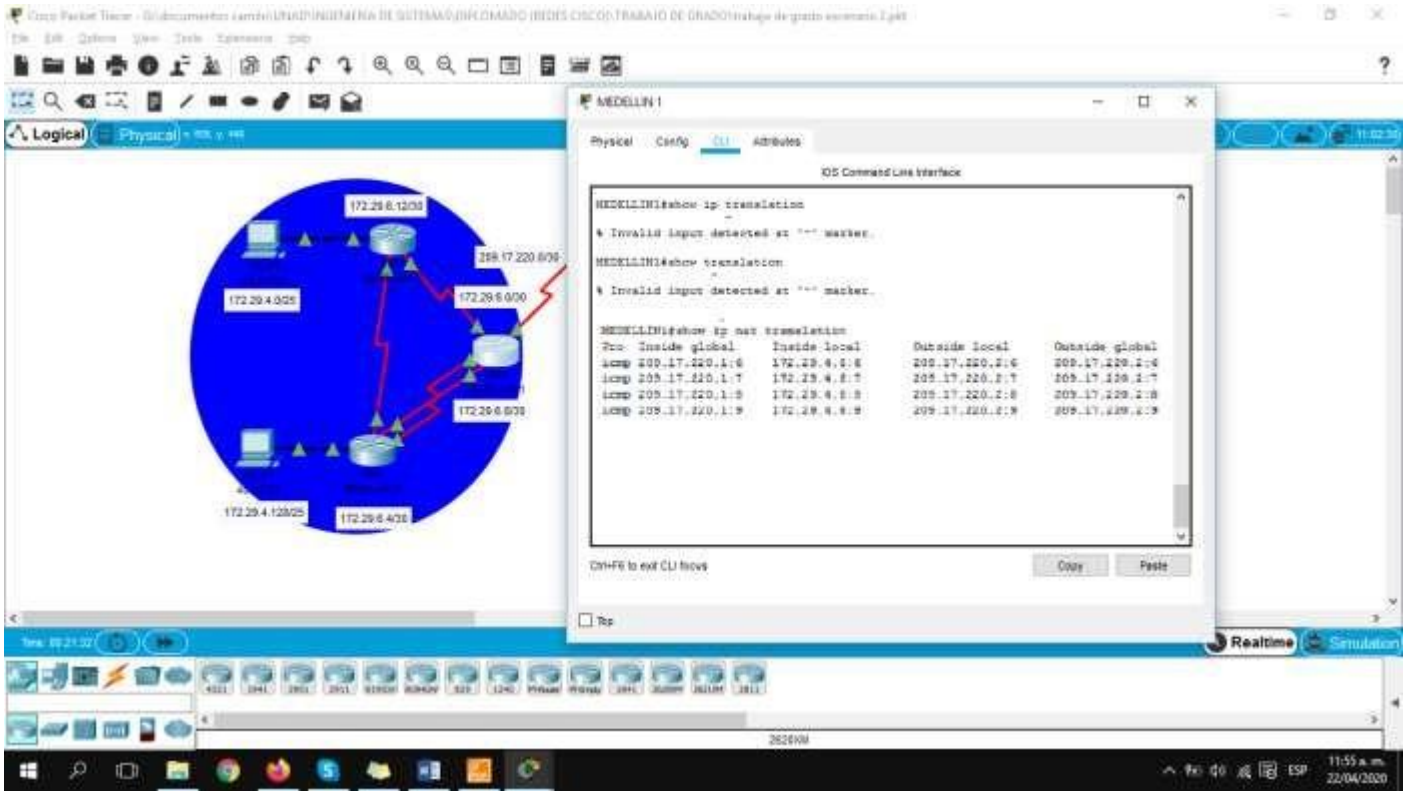



```
MEDELLIN1(config)#ip nat inside source list 1 interface s0/0/1 overload
MEDELLIN1(config)#access-list 1 permit 172.29.4.0 0.0.3.255
MEDELLIN1(config)#interface s0/0/1
MEDELLIN1(config-if)#ip nat outside
MEDELLIN1(config-if)#interface s0/0/0
MEDELLIN1(config-if)#ip nat inside
MEDELLIN1(config-if)#interface s0/1/0
MEDELLIN1(config-if)#ip nat inside
MEDELLIN1(config-if)#interface s0/1/1
MEDELLIN1(config-if)#ip nat inside
```


MEDELLIN1
Physical
Config
CLI
Attributes
IOS Command Line Interface
MEDELLIN1>enable
Password:
MEDELLIN1#config t
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN1(config)#ip nat inside source list 1 interface s0/0/1
overload
MEDELLIN1(config)#access-list 1 permit 172.29.4.0 0.0.0.255
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
MEDELLIN1(config-if)#^Z
MEDELLIN1#
%SYS-5-CONFIG_I: Configured from console by console
MEDELLIN1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
MEDELLIN1#
Ctrl+F6 to exit CLI focus
Copy
Paste
Top
Logical
Physical
Realtime
Simulation
172.29.4.0/25
172.29.4.128/25
172.29.6.4/30
CORE2811
ESP
11:15 a. m.
22/04/2020

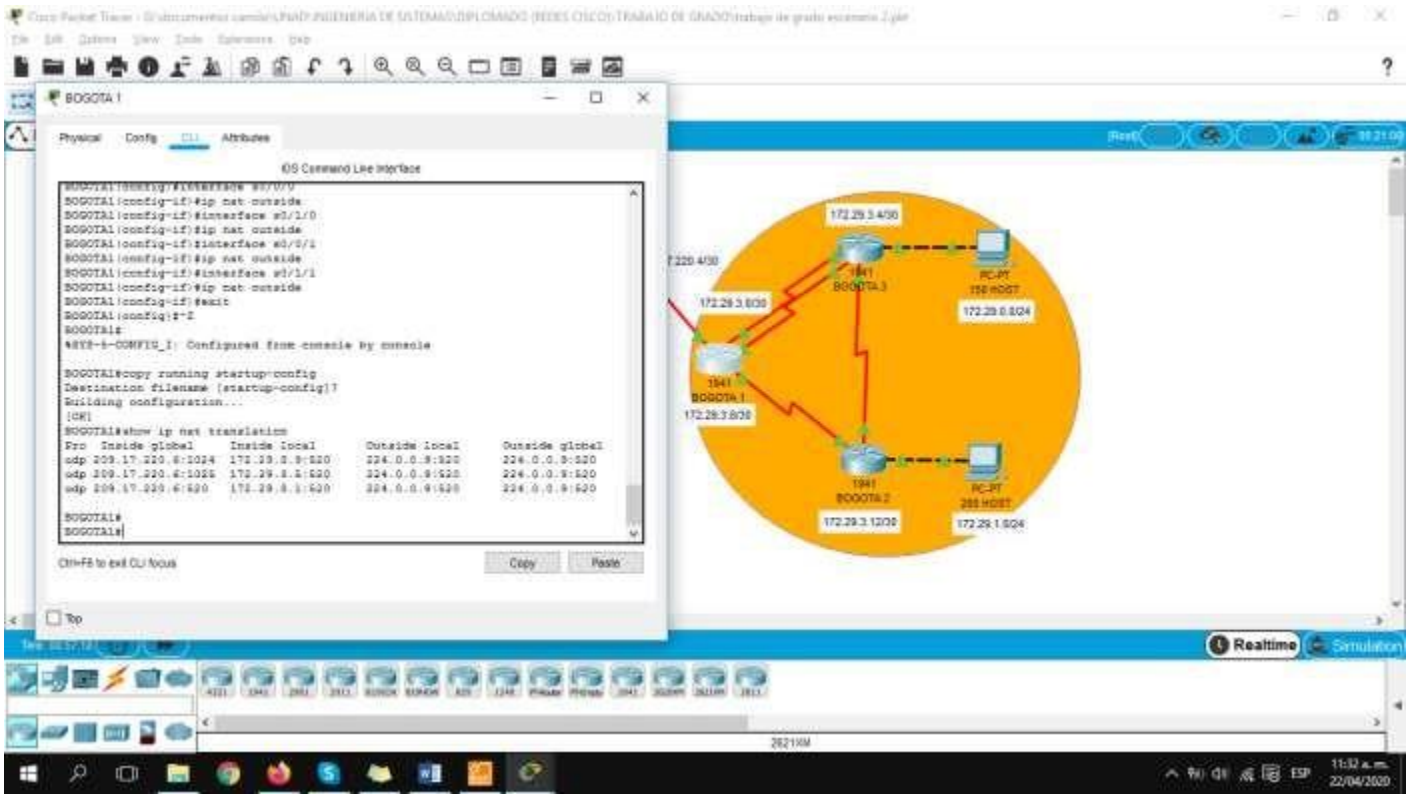
b. Después de verificar lo indicado en el paso anterior proceda a configurar el NAT en el router Medellín1. Compruebe que la traducción de direcciones indique las interfaces de entrada y de salida. Al realizar una prueba de ping, la dirección debe ser traducida automáticamente a la dirección de la interfaz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

MEDELLIN1



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

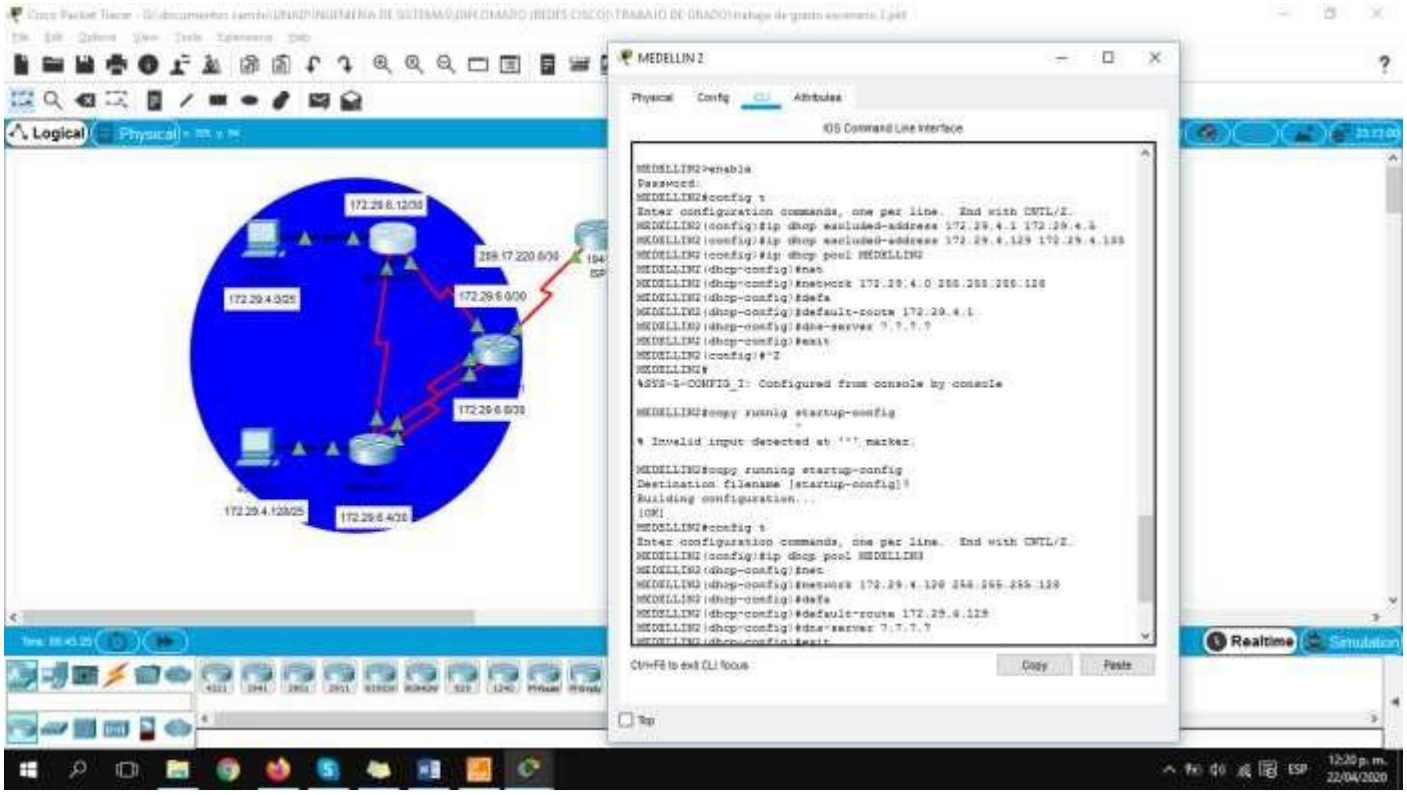
BOGOTA1



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.

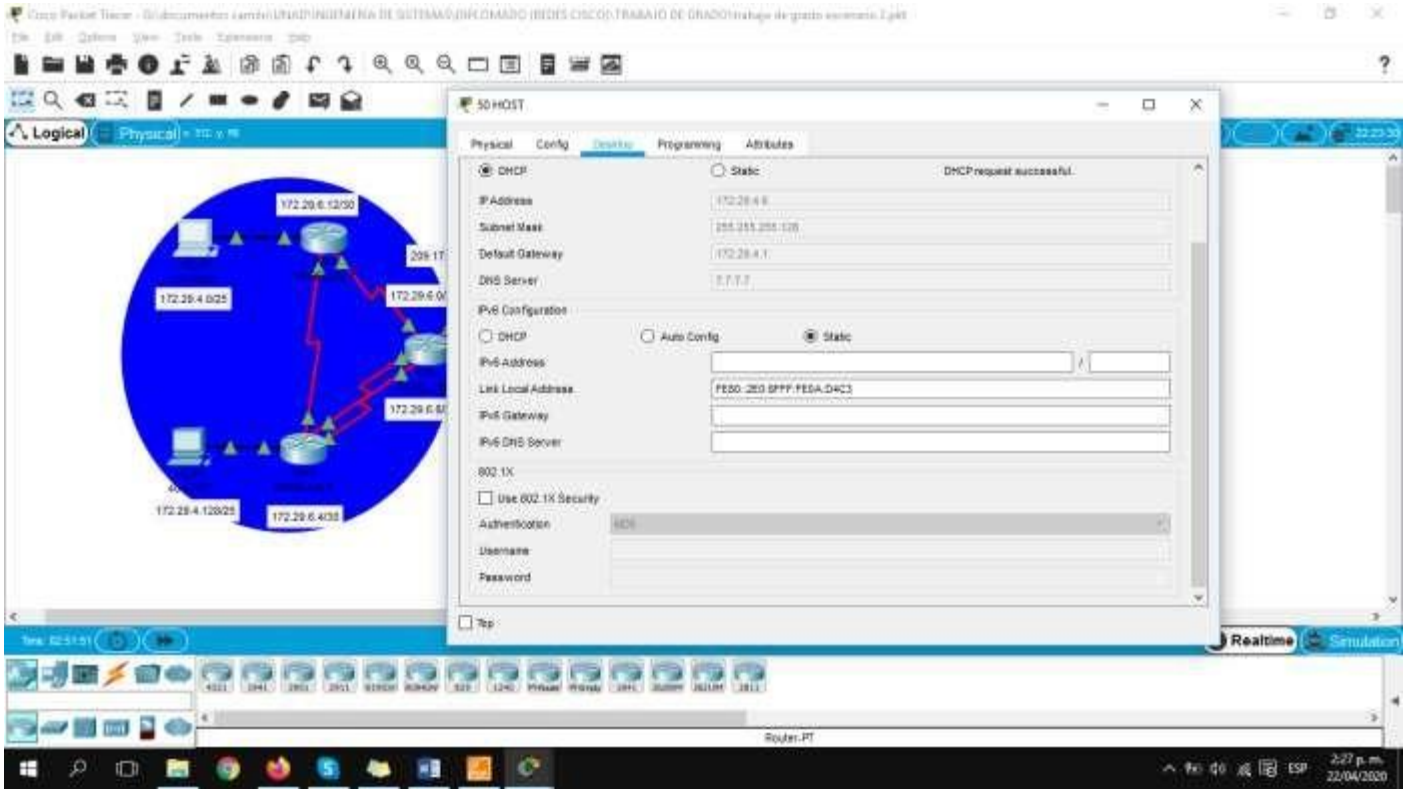
MEDELLIN2(config)#ip dhcp excluded-address 172.29.4.1 172.29.4.5
MEDELLIN2(config)#ip dhcp excluded-address 172.29.4.129 172.29.4.133
MEDELLIN2(config)#ip dhcp pool MEDELLIN2
MEDELLIN2(dhcp-config)#network 172.29.4.0 255.255.255.128
MEDELLIN2(dhcp-config)#default-route 172.29.4.1
MEDELLIN2(dhcp-config)#dns-server 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



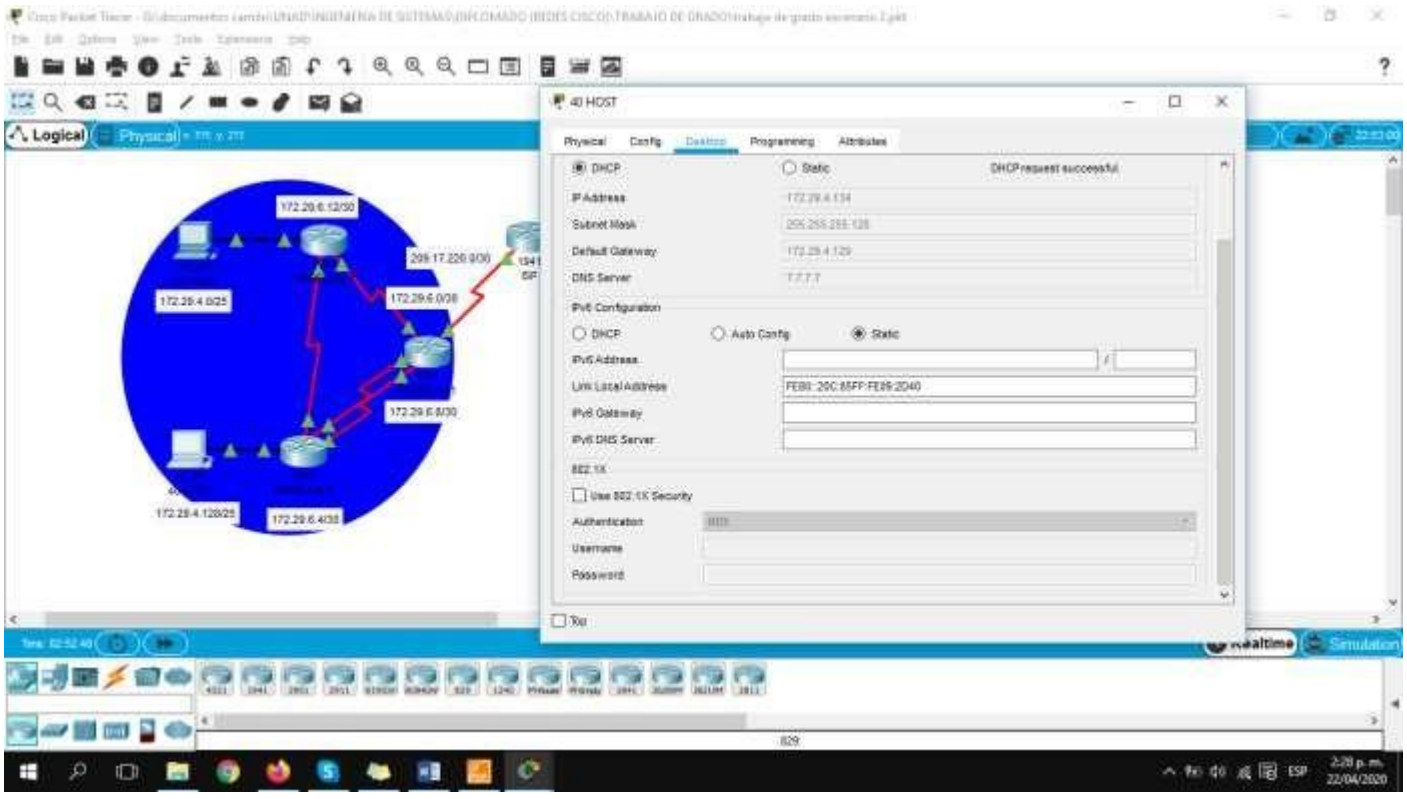
b. El router Medellín3 deberá habilitar el paso de los mensajes Broadcast hacia la IP del router Medellín2.

MEDELLIN3(config)#interface g0/0
MEDELLIN3(config-if)#ip helper-address 172.29.4.1

PC MEDELLIN 50 HOST:

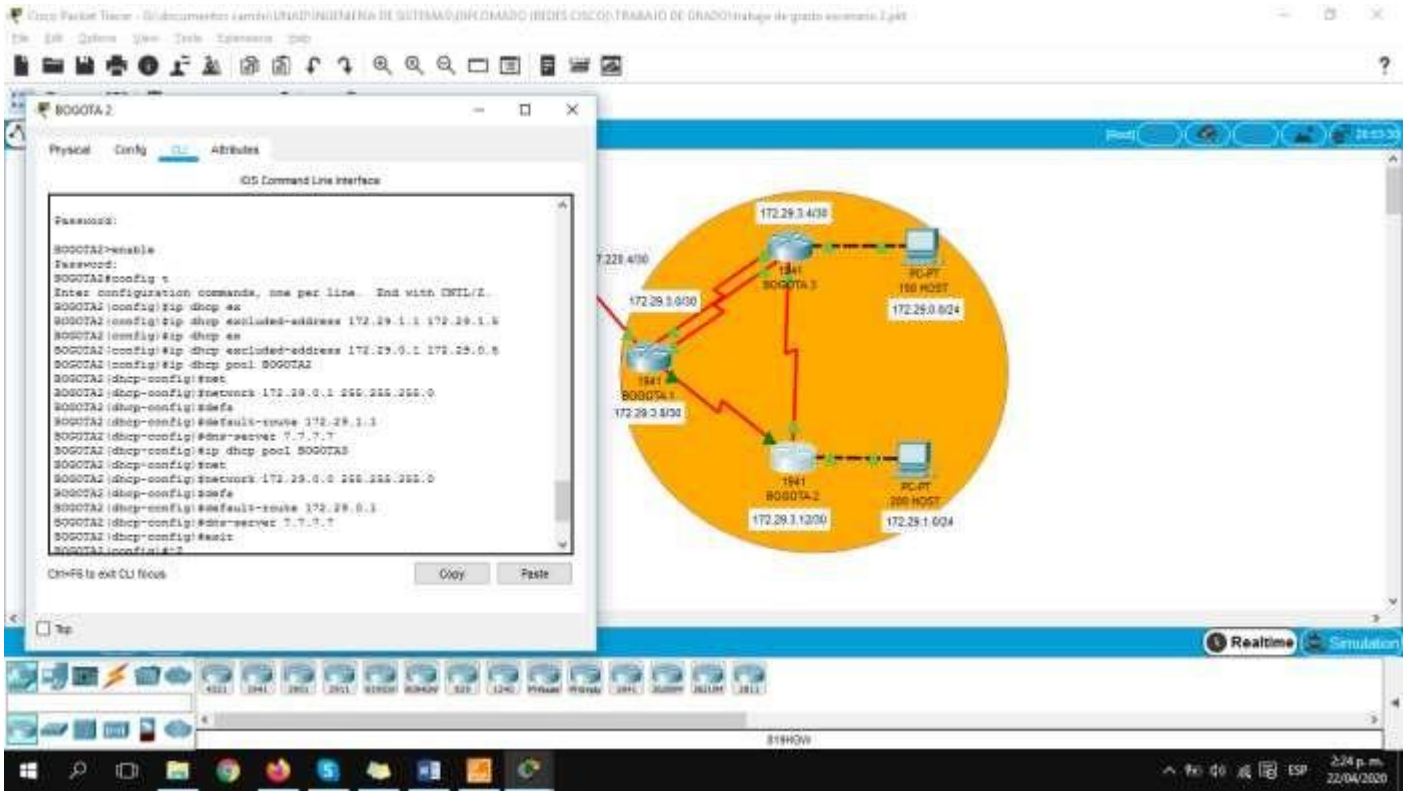


PC MEDELLIN 40 HOST:



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

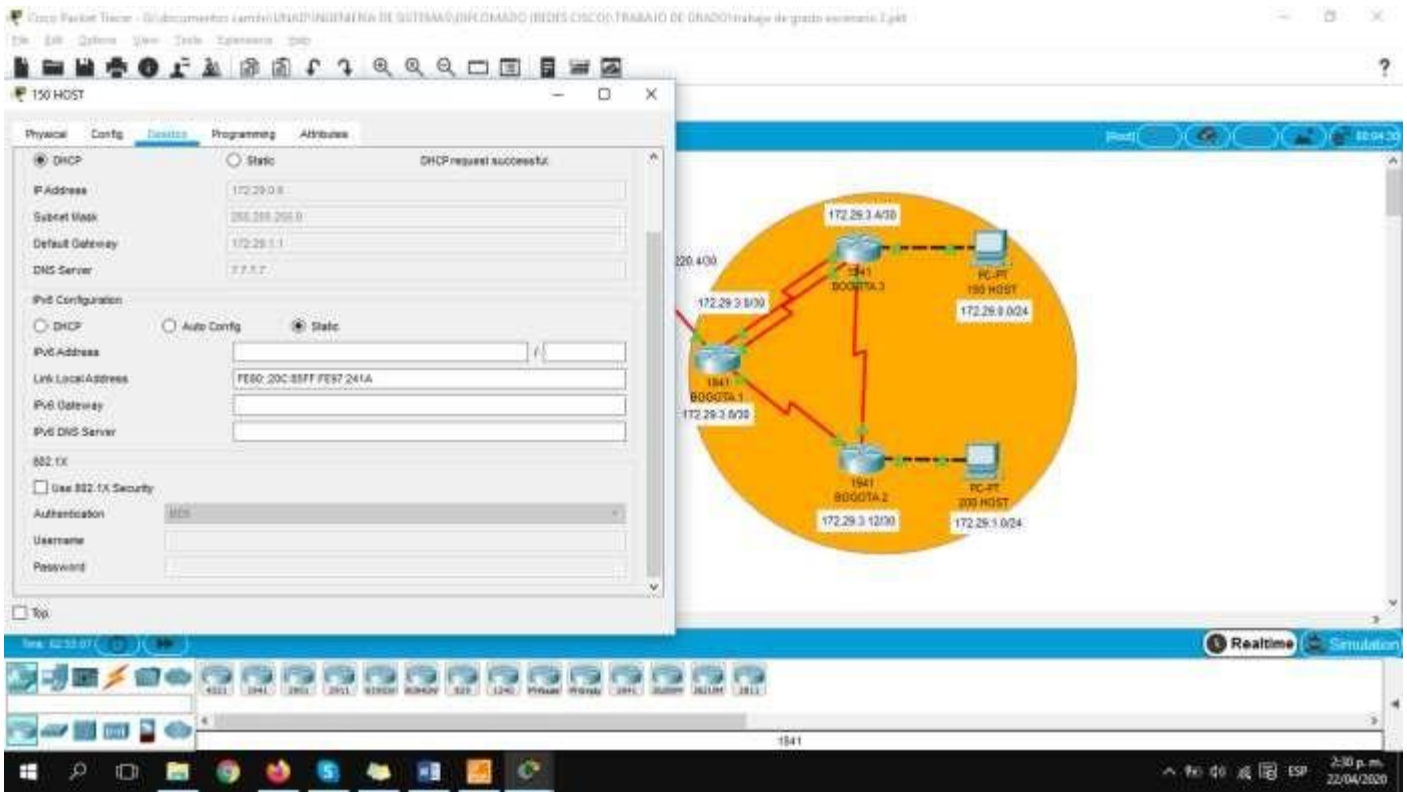
```
BOGOTA2(config)#ip dhcp excluded-address 172.29.1.1 172.29.1.5
BOGOTA2(config)#ip dhcp excluded-address 172.29.0.1 172.29.0.5
BOGOTA2(config)#ip dhcp pool BOGOTA2
BOGOTA2(dhcp-config)#network 172.29.1.0 255.255.255.0
BOGOTA2(dhcp-config)#default-route 172.29.1.1
BOGOTA2(dhcp-config)#dns-server 7.7.7.7
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
```



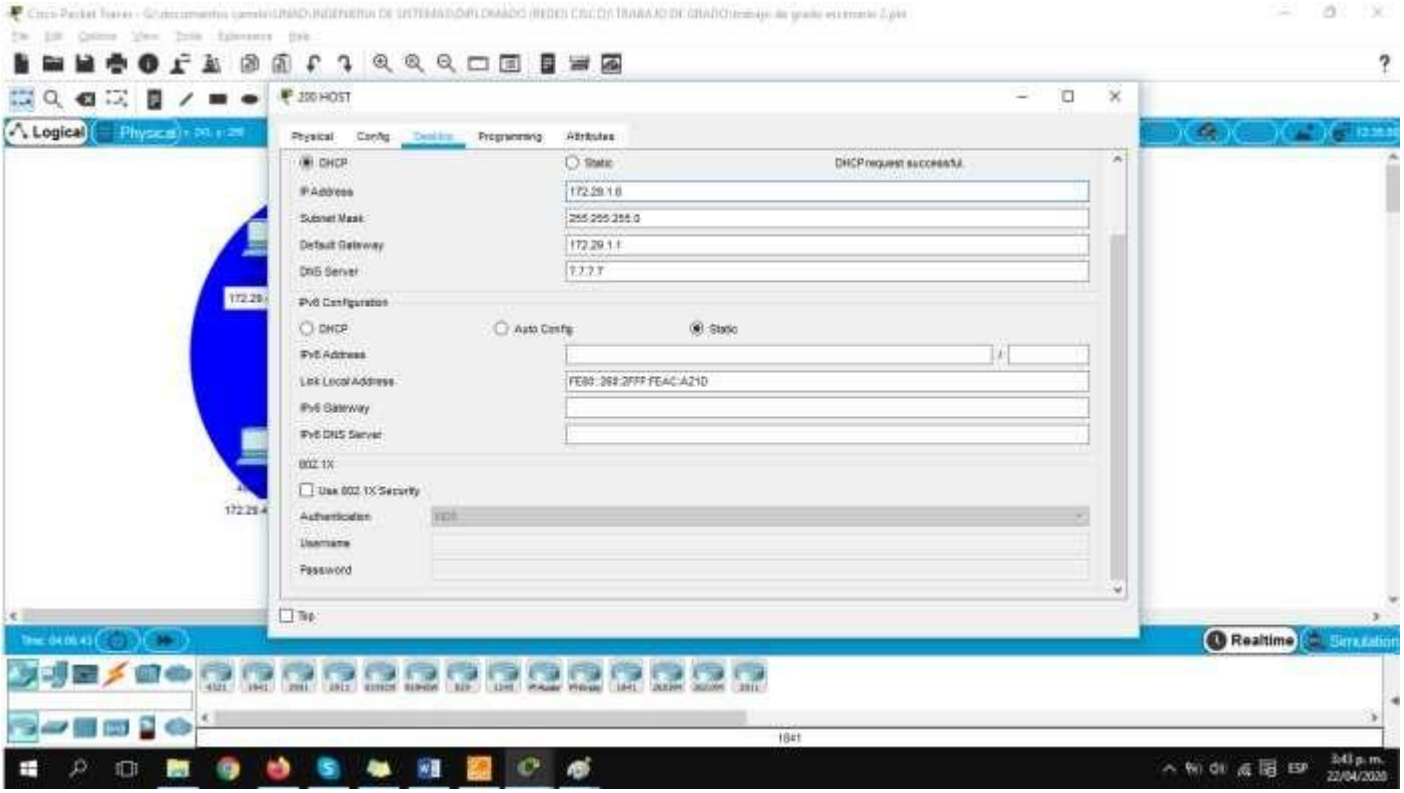
d. Configure el router Bogotá3 para que habilite el paso de los mensajes Broadcast hacia la IP del router Bogotá2.

```
BOGOTA3(config)#interface g0/0
BOGOTA3(config-if)#ip helper-address 172.29.1.1
BOGOTA3(config-if)#exit
```

PC BOGOTA 150 HOST:



PC BOGOTA 150 HOST:



CONCLUSIONES

Con el desarrollo de este trabajo de grado, llamado prueba de habilidades CCNA, se realiza un numero amplio de cosos o escenarios importantes para el buen desarrollo de los ejercicios propuestos, en este se ejecutan funciones como la de verificar una conexión entre los dispositivos proporcionada en la configuración inicial de la topología.

La práctica tiene un manual de instrucciones para la resolución de los ejercicios, en los cuales se aplicó diferentes estructuras como, por ejemplo, se armó una topología simple mediante cableado LAN Ethernet, se accedió a diferentes routers Cisco para su configuración, utilizando los métodos de acceso de consola, también se visualizó la configuración predeterminada de cada componente, antes de configurar los parámetros básicos.

Cuando se implementa un servidor para la asignación de la direcciones de red DHCP es muy importante la asignación de direcciones de red, por esto un servidor o como en este caso un router que hace las veces del servidor es determinante a la hora de asignar direcciones de red a una gran cantidad de ordenadores y así evita asignarlas una por una.

REFERENCIAS BIBLIOGRAFICAS

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. Calculo de Subredes de México. [Video] recuperado de: http://www.youtube.com/watch?v=Z7DM639rAmQ&list=PLaXGHu_K17nuWSyLNRtX7UvR2LcpTBK7P&index=5