PRUEBA DE HABILIDADES PRÁCTICAS CCNA

DIEGO FERNANDO HENAO DEL RÍO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD).
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍAS E INGENIERÍAS
INGENIERÍA DE SISTEMAS
ARMENIA, QUINDÍO
2020

PRUEBA DE HABILIDADES PRÁCTICAS CCNA

DIEGO FERNANDO HENAO DEL RÍO

Trabajo de la opción de grado para optar el título de Ingeniero de Sistemas

ASESOR
NILSON ALBEIRO FERREIRA MANZANARES
Docente Ocasional

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍAS E INGENIERÍAS
INGENIERIA DE SISTEMAS
ARMENIA, QUINDÍO
2020

TABLA DE CONTENIDO

LISTA DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

El presente trabajo plantea darles solución a dos escenarios de red, poniendo en práctica las habilidades adquiridas durante el desarrollo de los cursos de profundización en redes de CCNA1 y CCNA2 de CISCO, el primer escenario consiste en configurar una pequeña red compuesta por tres routers, dos switches, un servidor de internet y dos equipos hosts, para que admita conectividad IPv4 e IPv6, seguridad de switches y el routing de VLAN, usando el protocolo de routing dinámico RIPv2 y el protocolo de configuración de hosts dinámicos (DHCP), asimismo la traducción de direcciones de red dinámicas y estáticas (NAT), se configuran y verifican las listas de control de acceso (ACL) y el protocolo de tiempo de red (NTP) servidor/cliente, a medida que se probará y registrará la red, haciendo uso de los comandos comunes de CLI.

En el segundo escenario presenta un reto un poco más complejo, ya que la red es un poco más grande, se trata de una empresa con varias sucursales en las ciudades de Medellín y Bogotá, para lo cual se deben configurar e interconectar entre sí cada uno de los dispositivos que forman parte de la red, acorde con los lineamientos establecidos para el direccionamiento IP, los protocolos de enrutamiento y los demás aspectos que hacen parte de la topología de red.

El protocolo de enrutamiento a utilizar en este escenario será el OSPF, teniendo en cuenta que posee rutas distribuidas por defecto, asimismo se realiza la configuración del encapsulamiento PPP y su respectiva autenticación, también se muestra el proceso de configuración para proporcionar el servicio DHCP a la propia red LAN y los routers de cada ciudad, para terminar se realiza la configuración de de PPP en los enlaces hacia el ISP con su respectiva autenticación y la traducción de direcciones de red dinámicas y estáticas NAT de sobrecarga en dos de los routers.

ABSTRACT

This work aims to provide a solution to two network scenarios, putting into practice the skills acquired during the development of the CISCO CCNA1 and CCNA2 network deepening courses. The first scenario consists of configuring a small network consisting of three routers, two switches, an internet server and two host computers, to support IPv4 and IPv6 connectivity, switch security and VLAN routing, using the RIPv2 dynamic routing protocol and the dynamic host configuration protocol (DHCP), also the translation dynamic and static network addresses (NAT), access control lists (ACLs) and network time protocol (NTP) server / client are configured and verified as the network will be tested and logged using common CLI commands.

In the second scenario, it presents a slightly more complex challenge, since the network is a little larger, it is a company with several branches in the cities of Medellín and Bogotá, for which each one must be configured and interconnected of the devices that are part of the network, according to the guidelines established for IP addressing, routing protocols and other aspects that are part of the network topology.

The routing protocol to be used in this scenario will be the OSPF, taking into account that it has distributed routes by default, the PPP encapsulation configuration and its respective authentication are also performed, the configuration process is also shown to provide the DHCP service to the LAN network and the routers of each city, to finish, the PPP configuration is made in the links to the ISP with their respective authentication and the translation of dynamic and static network addresses overload NAT in two of the routers.

GLOSARIO

RIPv2 (Routing Information Protocol versión 2): es uno de los protocolos de enrutamiento interior más sencillos y utilizados que a partir de la versión 2 introduce algunas mejoras críticas que la constituyeron en un recurso necesario para cualquier administrador de redes.

OSPF (Open Shortest Path First): OSPF es un protocolo de enrutamiento de estado del enlace basado en estándares abiertos. Es un protocolo de enrutamiento sofisticados y escalables. Este tipo de protocolo difiere de los protocolos por vector distancia. En OSPF el algoritmo basado en “primero la ruta libre más corta” determina la mejor ruta y de coste más bajo hacia el enlace.

IPv4 (Internet Protocol version 4), El Protocolo de Internet versión 4 es la cuarta versión del Internet Protocol (IP), un protocolo de interconexión de redes basados en Internet.

IPv6: es una actualización al protocolo IPv4, diseñado para resolver el problema de agotamiento de direcciones.

VLAN (red de área local virtual): acrónimo de virtual LAN, es un método para crear redes lógicas independientes dentro de una misma red física. Varias VLAN pueden coexistir en un único conmutador físico o en una única red física. Son útiles para reducir el dominio de difusión y ayudan en la administración de la red.

DHCP (Dynamic Host Configuration Protocol): el protocolo de configuración dinámica de host es un protocolo de red de tipo cliente/servidor mediante el cual un servidor DHCP asigna dinámicamente una dirección IP y otros parámetros de configuración de red a cada dispositivo en una red para que puedan comunicarse con otras redes IP.

NAT (Network Address Translation), La traducción de direcciones de red, también llamado enmascaramiento de IP o NAT es un mecanismo utilizado por routers IP para intercambiar paquetes entre dos redes que asignan mutuamente direcciones incompatibles. Consiste en convertir, en tiempo real, las direcciones utilizadas en los paquetes transportados. También es necesario editar los paquetes para permitir la operación de protocolos que incluyen información de direcciones dentro de la conversación del protocolo.

ACL (Access Control List): Una lista de control de acceso es un concepto de seguridad informática usado para fomentar la separación de privilegios. Es una forma de determinar los permisos de acceso apropiados a un determinado objeto, dependiendo de ciertos aspectos del proceso que hace el pedido.

NTP (Network Time Protocol) es un protocolo de Internet para sincronizar los relojes de los sistemas informáticos a través del enrutamiento de paquetes en redes con latencia variable. NTP utiliza UDP como su capa de transporte, usando el puerto 123. Está diseñado para resistir los efectos de la latencia variable.

PPP (Point-to-Point Protocol), Protocolo punto a punto, es un protocolo del nivel de enlace de datos, utilizado para establecer una conexión directa entre dos nodos de una red. Conecta dos enrutadores directamente sin ningún equipo u otro dispositivo de red entre medias de ambos.

ISP (Internet Service Provider) El proveedor de servicios de Internet, es la empresa que brinda conexión a Internet a sus clientes.

PAT (Port Address Translation) es una característica del estándar NAT, que traduce conexiones TCP y UDP hechas por un host y un puerto en una red externa a otra dirección y puerto de la red interna. Permite que una sola dirección IP sea utilizada por varias máquinas de la intranet.

INTRODUCCIÓN

Este trabajo se compone de dos escenarios los cuales se encuentran planteados como para la prueba de habilidades CCNA y la finalización del diplomado de profundización CISCO, como opción de grado, es así durante la implementación de las soluciones para ambos escenarios, se pondrán en práctica gran parte de lo aprendido, como lo son la configuración básica de equipos como switches y routers, servidores y equipos host, la implementación de protocolos de red, creación de redes VLAN, WAN y LAN, dando así un reforzamiento de casi todas las temáticas aprendidas.

OBJETIVOS

Para el escenario 1 con el fin de poner en funcionamiento la red, se plantean los siguientes objetivos:

Realizar la configuración de los routers y los switches.

Configurar la computadora de internet.

Configurar la seguridad de los switches, las VLAN y el routing entre VLAN.

Configurar el protocolo de routing dinámico RIPv2.

Configurar el router como servidor DHCP para la VLAN.

Configurar la NAT estática y dinámica en el router R2

Configurar NTP

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

Para el escenario 2 con el fin de poner en funcionamiento la red, se plantean los siguientes objetivos:

Configuración del enrutamiento de la red

Realizar la tabla de enrutamiento

Deshabilitar la propagación del protocolo OSPF

Verificar el protocolo OSPF

Configurar encapsulamiento y autenticación PPP

Configuración de PAT

Configuración del servicio DHCP

DESARROLLO 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.

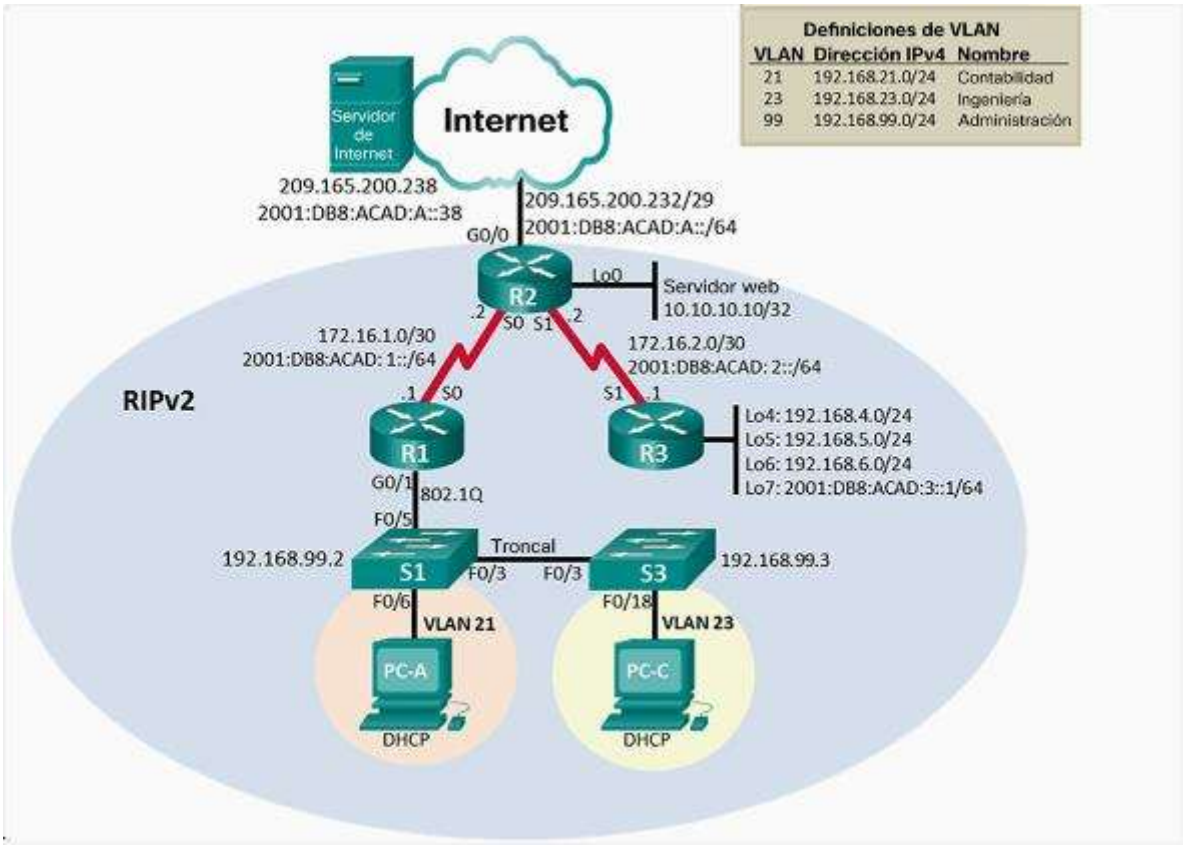


Figura 1 - Topología de Red Escenario 1

Parte 1: Inicialización dispositivos

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

Tabla 1 - Inicialización de Dispositivos

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	*Erase startup-config*
Volver a cargar todos los routers	*reload*
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	*Erase startup-config* *Delete vlan.dat*
Volver a cargar ambos switches	*reload*
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	*Show flash*

Eliminación de las configuraciones de inicio y vuelta a cargar de los dispositivos.
Eliminación del archivo startup-config de todos los routers

Para la eliminación del archivo startup-config de los routers, damos click en cada router, vamos a la pestaña CLI y digitamos el comando *enable* y luego el comando *erase startup-config* y cuando aparezca *Continue*?, damos *Enter* y confirmamos *así:*

Router R1, R2 y R3
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

Volver a cargar todos los routers

Para el cargue nuevamente de los routers, seguido digitamos el comando *reload así:*
Routers R1, R2 y R3

Router#reload

Proceed with reload? [confirm]

Confirmamos e inmediatamente los routers se vuelven a cargar.

Eliminación del archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior.

Para la eliminación del archivo startup-config de los switches, damos click en cada switch, vamos a la pestaña CLI y digitamos *enable* y luego el comando *erase startup-config* y cuando aparezca *Continue*?, damos *Enter* y confirmamos *así:*

Switches S1 Y S3

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

Para eliminar la base de datos de VLAN, procedemos a digitar el comando *delete vlan.dat,* confirmamos y listo así:

Switch#delete vlan.dat
Delete filename [vlan.dat]?
Delete flash:/vlan.dat? [confirm]

Volver a cargar ambos switches

Para el cargar nuevamente de los switches, seguido digitamos el comando *reload así:*

Switch#reload
Proceed with reload? [confirm]

Confirmamos e inmediatamente los switches se vuelven a cargar.

Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches

Para verificar que la base de datos de VLAN no está en la memoria flash, entramos a cada switch y digitamos el comando *show flash* y listo, inmediatamente nos muestra que efectivamente no está así:

Switches S1 y S2

Switch>enable
Switch#show flash
Directory of flash:/

1 -rw- 4414921 <no date> c2960-lanbase-mz.122-25.FX.bin

64016384 bytes total (59601463 bytes free)

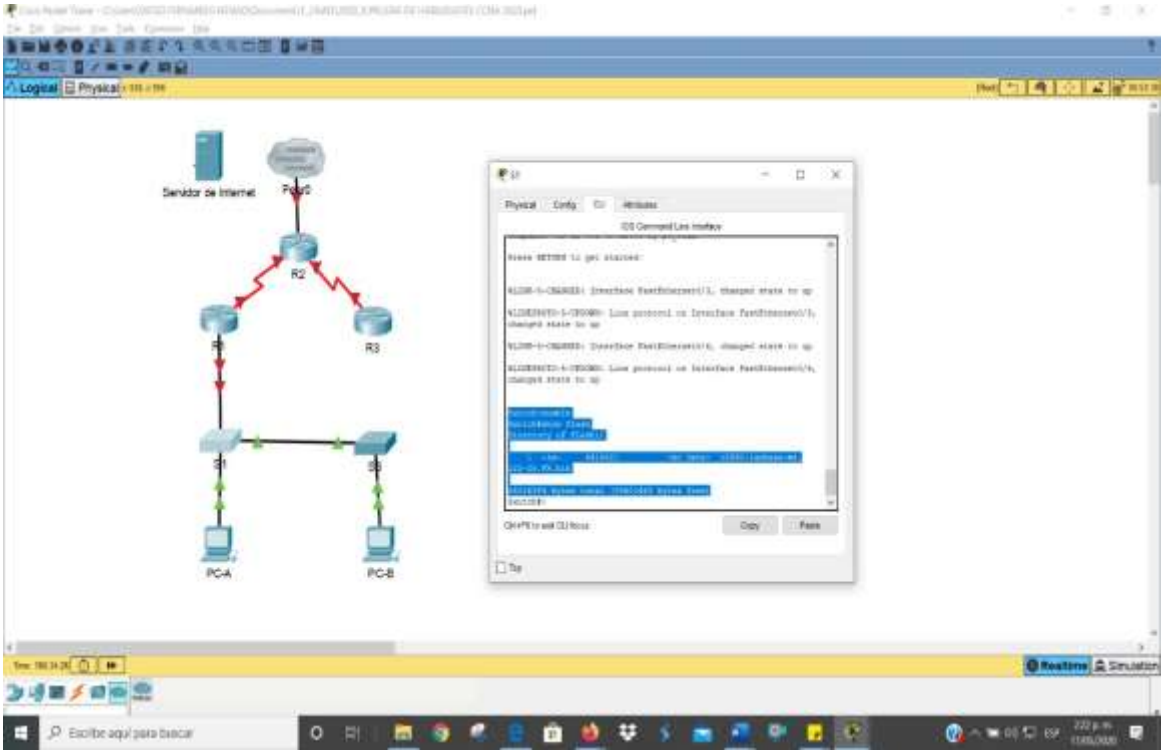


Figura 2 - Ejecución Comando Show Flash en S1

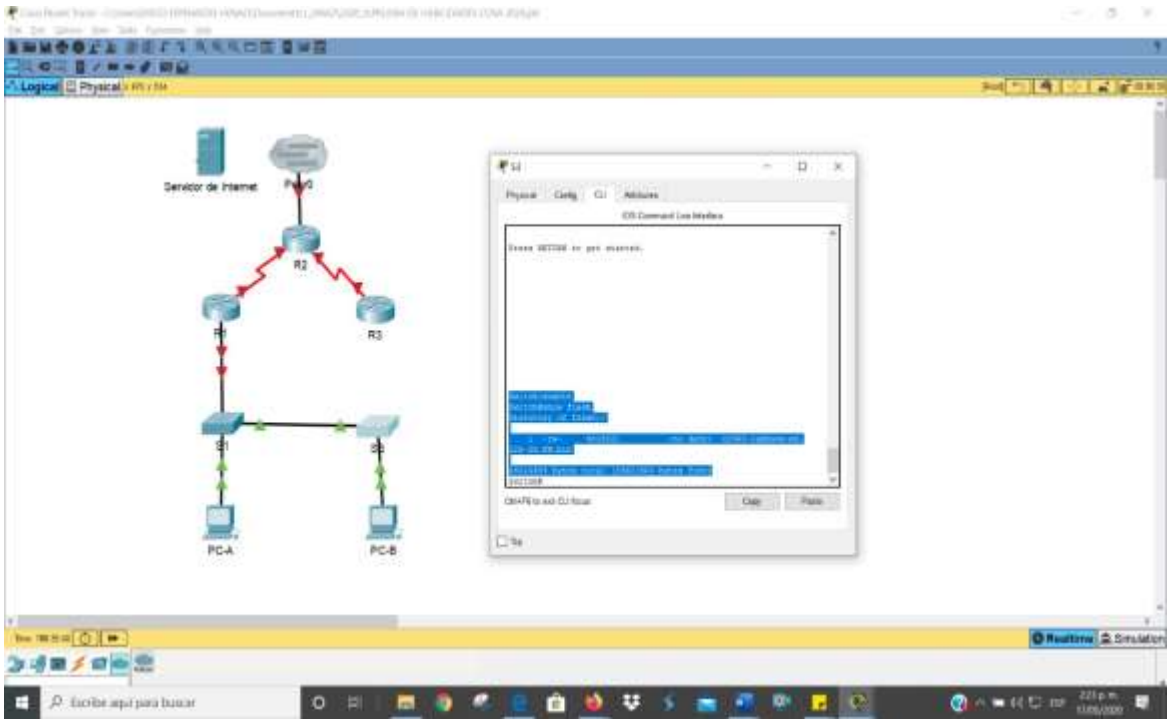


Figura 3 - Ejecución Comando Show Flash en S3

Parte 2: Configurar los parámetros básicos de los dispositivos

Paso 1: Configurar la computadora de Internet

Se procede entonces a dar click en la computadora de internet y se va a la pestaña *Desktop* y luego a la *Ip configuration y se* ingresan los datos de la siguiente tabla, de acuerdo a la información de la topología.

Tabla 2 - Configuración Computadora de Internet

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
Gateway predeterminado IPv6	2001:DB8:ACAD:2::1

Paso 2: Configurar R1

Tabla 3 - Configuración del Router R1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	*no Ip domain-lookup*
Nombre del router	*Hostname* 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	*Service Password-encryption*
Mensaje MOTD	*Banner motd* #Se prohíbe el acceso no autorizado#
Interfaz S0/0/0	R1(config)#int s0/0/0 R1(config-if)#description CONECTADO A R2 R1(config-if)#ip address 172.16.1.1 255.255.255.252 R1(config-if)#ipv6 address 2001:db8:acad:1::1/64 R1(config-if)#clock rate 128000 R1(config-if)#no shutdown R1(config)#ipv6 unicast-routing
Rutas predeterminadas	R1(config)#ip route 0.0.0.0 0.0.0.0 172.16.1.2 R1(config)#ipv6 route ::/0 s0/0/0

Ahora procedemos a configurar el primer router así:

Para desactivar la búsqueda DNS damos click en el router, vamos a la pestaña CLI y digitamos el comando *enable* y luego *config t* ara ingresar a la configuración de la terminal y posteriormente digitamos el comando *no ip domain-lookup* así:

Router>enable

Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup

Para asignar un nombre al router, simplemente ingresamos el comando *hostname* acompañado del nombre que deseamos darle al router en este caso R1 así:

Router(config)#hostname R1

Ahora vamos a asignar las contraseñas exec privilegiado cifrada, de acceso a la consola y de acceso a Telnet, todas encriptadas de la siguiente forma:

R1(config)#
R1(config)#enable secret class
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#line vty 0 4
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#service password-encryption

Y a continuación ingresamos el mensaje MOTD con el comando banner motd y entre los signos de numeral, dejamos el mensaje que queremos así:

R1(config)#banner motd #Se prohíbe el acceso no autorizado#

Seguimos con la configuración de la Interfaz S0/0/0, a la cual le estableceremos la descripción, la dirección IPv4, IPv6, la frecuencia de reloj en 128000 y por último activaremos la interfaz así:

R1(config)#int s0/0/0
R1(config-if)#description CONECTADO A R2
R1(config-if)#ip address 172.16.1.1 255.255.255.252
R1(config-if)#ipv6 address 2001:db8:acad:1::1/64
R1(config-if)#clock rate 128000
R1(config-if)#no shutdown
R1(config)#ipv6 unicast-routing

Configuramos las rutas predeterminadas de IPv4 e IPv6 como se muestra a continuación:

R1(config)#ip route 0.0.0.0 0.0.0.0 172.16.1.2
R1(config)#ipv6 route ::/0 s0/0/0

Paso 3: Configurar R2

Tabla 4 - Configuración del Router R2

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	*no Ip domain-lookup*
Nombre del router	*Hostname* 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	*Service Password-encryption*
Habilitar el servidor HTTP	
Mensaje MOTD	*Banner motd* #Se prohíbe el acceso no autorizado#
Interfaz S0/0/0	R2(config)#ipv6 unicast-routing R2(config)#int s0/0/0 R2(config-if)#description CONECTADO A R1 R2(config-if)#ip address 172.16.1.2 255.255.255.252 R2(config-if)#ipv6 address 2001:db8:acad:1::2/64 R2(config-if)#no shutdown

Interfaz S0/0/1	R2(config-if)#int s0/0/1 R2(config-if)#description CONECTADO A R3 R2(config-if)#ip address 172.16.2.2 255.255.255.252 R2(config-if)#ipv6 address 2001:db8:acad:2::2/64 R2(config-if)#clock rate 128000 R2(config-if)#no shutdown
Interfaz G0/0 (simulación de Internet)	R2(config-if)#int g0/1 R2(config-if)#description SIMULACION DE CONECTADO A INTERNET R2(config-if)#ip address 209.165.200.232 255.255.255.0 R2(config-if)#ipv6 address 2001:db8:acad:a::1/64 R2(config-if)#no shutdown
Interfaz loopback 0 (servidor web simulado)	R2(config)#int loopback 0 R2(config-if)#ip address 19.10.10.10 255.255.255.255 R2(config-if)#description SIMULACION SERVIDOR WEB
Ruta predeterminada	R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0 R2(config)#ipv6 route ::/0 g0/0

Ahora procedemos a configurar el segundo router así:

Para desactivar la búsqueda DNS damos click en el router, vamos a la pestaña CLI y digitamos el comando *enable* y luego *config t* ara ingresar a la configuración de la terminal y posteriormente digitamos el comando *no ip domain-lookup* así:

Router>enable
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup

Para asignar un nombre al router, simplemente ingresamos el comando *hostname* acompañado del nombre que deseamos darle al router en este caso R2 así:

Router(config)#hostname R2

Ahora vamos a asignar las contraseñas exec privilegiado cifrada, de acceso a la consola y de acceso a Telnet, todas encriptadas de la siguiente forma:

R2(config)#
R2(config)#enable secret class
R2(config)#line console 0
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#line vty 0 4
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#exit
R2(config)#service password-encryption

Y a continuación ingresamos el mensaje MOTD con el comando banner motd y entre los signos de numeral, dejamos el mensaje que queremos así:

R2(config)#banner motd #Se prohíbe el acceso no autorizado#

Seguimos con la configuración de la Interfaz S0/0/0, a la cual le estableceremos la descripción, la dirección IPv4, IPv6, y por último activaremos la interfaz así:

R2(config)#ipv6 unicast-routing
R2(config)#int s0/0/0
R2(config-if)#description CONECTADO A R1
R2(config-if)#ip address 172.16.1.2 255.255.255.252
R2(config-if)#ipv6 address 2001:db8:acad:1::2/64
R2(config-if)#no shutdown

Pasamos a configurar la interfaz S0/0/1

R2(config-if)#int s0/0/1
R2(config-if)#description CONECTADO A R3
R2(config-if)#ip address 172.16.2.2 255.255.255.252
R2(config-if)#ipv6 address 2001:db8:acad:2::2/64
R2(config-if)#clock rate 128000
R2(config-if)#no shutdown

Pasamos a configurar la interfaz G0/0 (Simulación de internet)

R2(config-if)#int g0/1
R2(config-if)#description SIMULACION DE CONECTADO A INTERNET
R2(config-if)#ip address 209.165.200.232 255.255.255.0
R2(config-if)#ipv6 address 2001:db8:acad:a::1/64
R2(config-if)#no shutdown

Configuramos la interfaz loopback 0 (servidor web simulado)

R2(config)#int loopback 0
R2(config-if)#ip address 19.10.10.10 255.255.255.255
R2(config-if)#description SIMULACION SERVIDOR WEB

Para terminar configuramos las rutas predeterminadas IPv4 e IPv6, para la G0/0 así:

R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0
R2(config)#ipv6 route ::/0 g0/0

Paso 4: Configurar R3

Tabla 5 - Configuración del Router R3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R3
Contraseña de exec privilegiado cifrada	R3(config)#enable secret class
Contraseña de acceso a la consola	R3(config)#line console 0 R3(config-line)#password cisco R3(config-line)#login
Contraseña de acceso Telnet	R3(config-line)#line vty 0 4 R3(config-line)#password cisco R3(config-line)#login

Cifrar las contraseñas de texto no cifrado	R3(config)#service password-encryption
Mensaje MOTD	R3(config)#banner motd #Se prohíbe el acceso no autorizado# .
Interfaz S0/0/1	R3(config)#int s0/0/1 R3(config-if)#description CONECTADO A R2 R3(config-if)#ip address 172.16.2.1 255.255.255.252 R3(config-if)#ipv6 address 2001:db8:acad:2::1/64 R3(config-if)#no shutdown
Interfaz loopback 4	R3(config)#int loopback 4 R3(config-if)#ip address 192.168.4.1 255.255.255.0
Interfaz loopback 5	R3(config)#int loopback 5 R3(config-if)#ip address 192.168.5.1 255.255.255.0
Interfaz loopback 6	R3(config)#int loopback 6 R3(config-if)#ip address 192.168.6.1 255.255.255.0
Interfaz loopback 7	R3(config)#int loopback 7 R3(config-if)#ip address 192.168.7.1 255.255.255.0
Rutas predeterminadas	R3(config-if)#ipv6 unicast-routing R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1 R3(config)#ipv6 route ::/0 s0/0/1

Ahora procedemos a configurar el tercer router así:

Para desactivar la búsqueda DNS damos click en el router, vamos a la pestaña CLI y digitamos el comando *enable* y luego *config t* ara ingresar a la configuración de la terminal y posteriormente digitamos el comando *no ip domain-lookup* así:

Router>enable
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup

Para asignar un nombre al router, simplemente ingresamos el comando *hostname* acompañado del nombre que deseamos darle al router en este caso R3 así:

Router(config)#hostname R3

Ahora vamos a asignar las contraseñas exec privilegiado cifrada, de acceso a la consola y de acceso a Telnet, todas encriptadas de la siguiente forma:

R3(config)#
R3(config)#enable secret class
R3(config)#line console 0
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#line vty 0 4
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#exit
R3(config)#service password-encryption

Y a continuación ingresamos el mensaje MOTD con el comando banner motd y entre los signos de numeral, dejamos el mensaje que queremos así:

R3(config)#banner motd #Se prohíbe el acceso no autorizado#

Seguimos con la configuración de la Interfaz S0/0/0, a la cual le estableceremos la descripción, la dirección IPv4, IPv6, y por último activaremos la interfaz así:

R3(config)#int s0/0/1
R3(config-if)#description CONECTADO A R2
R3(config-if)#ip address 172.16.2.1 255.255.255.252
R3(config-if)#ipv6 address 2001:db8:acad:2::1/64
R3(config-if)#no shutdown

Configuramos las interfaces loopback 4, 5, 6 y 7 así:

R3(config)#int loopback 4
R3(config-if)#ip address 192.168.4.1 255.255.255.0
R3(config)#int loopback 5
R3(config-if)#ip address 192.168.5.1 255.255.255.0

R3(config)#int loopback 6
R3(config-if)#ip address 192.168.6.1 255.255.255.0

R3(config)#int loopback 7
R3(config-if)#ip address 192.168.7.1 255.255.255.0

Para terminar configuramos las rutas predeterminadas IPv4 e IPv6 para la S0/0/1 así:

R3(config-if)#ipv6 unicast-routing
R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1
R3(config)#ipv6 route ::/0 s0/0/1

Paso 5: Configurar S1

Tabla 6 - Configuración del Switche S1

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

Ahora procedemos a configurar el primer switch, lo cual se realiza utilizando los mismos comandos que en los routers así:

Para desactivar la búsqueda DNS damos click en el switch, vamos a la pestaña CLI y digitamos el comando enable y luego config t para ingresar a la configuración de la terminal y posteriormente digitamos el comando no ip domain-lookup así:

Switch>enable
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ip domain-lookup

Para asignar un nombre al switch, simplemente ingresamos el comando hostname acompañado del nombre que deseamos darle al switch en este caso S1 así:

Switch(config)#hostname S1

Ahora vamos a asignar las contraseñas exec privilegiado cifrada, de acceso a la consola y de acceso a Telnet, todas encriptadas de la siguiente forma:

S1(config)#
S1(config)#enable secret class
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#line vty 0 4
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#exit
S1(config)#service password-encryption

Y a continuación ingresamos el mensaje MOTD con el comando banner motd y entre los signos de numeral, dejamos el mensaje que queremos así:

S1(config)#banner motd #Se prohíbe el acceso no autorizado#

Paso 6: Configurar S3

Tabla 7 - Configuración del Switch S3

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

Ahora procedemos a configurar el segundo switch, de la misma forma que lo hicimos con el S1 así:

Para desactivar la búsqueda DNS damos click en el switch, vamos a la pestaña CLI y digitamos el comando enable y luego config t para ingresar a la configuración de la terminal y posteriormente digitamos el comando no ip domain-lookup así:

Switch>enable
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ip domain-lookup

Para asignar un nombre al switch, simplemente ingresamos el comando hostname acompañado del nombre que deseamos darle al switch en este caso S1 así:

Switch(config)#hostname S3

Ahora vamos a asignar las contraseñas exec privilegiado cifrada, de acceso a la consola y de acceso a Telnet, todas encriptadas de la siguiente forma:

S3(config)#
S3(config)#enable secret class
S3(config)#line console 0
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#line vty 0 4
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#exit
S3(config)#service password-encryption

Y a continuación ingresamos el mensaje MOTD con el comando banner motd y entre los signos de numeral, dejamos el mensaje que queremos así:

S3(config)#banner motd #Se prohíbe el acceso no autorizado#

Paso 7: Verificar la conectividad de la red

Tabla 8 - Verificación de la conectividad de la red

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	Satisfactorio
R2	R3, S0/0/1	172.16..2.1	Satisfactorio
PC de Internet	Gateway predeterminado	209.165.200.233	Satisfactorio

Utilizando el comando ping probamos la conectividad entre los dispositivos de red así:

Desde R1 a R2

R1#ping 172.16.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds:
!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 3/5/8 ms

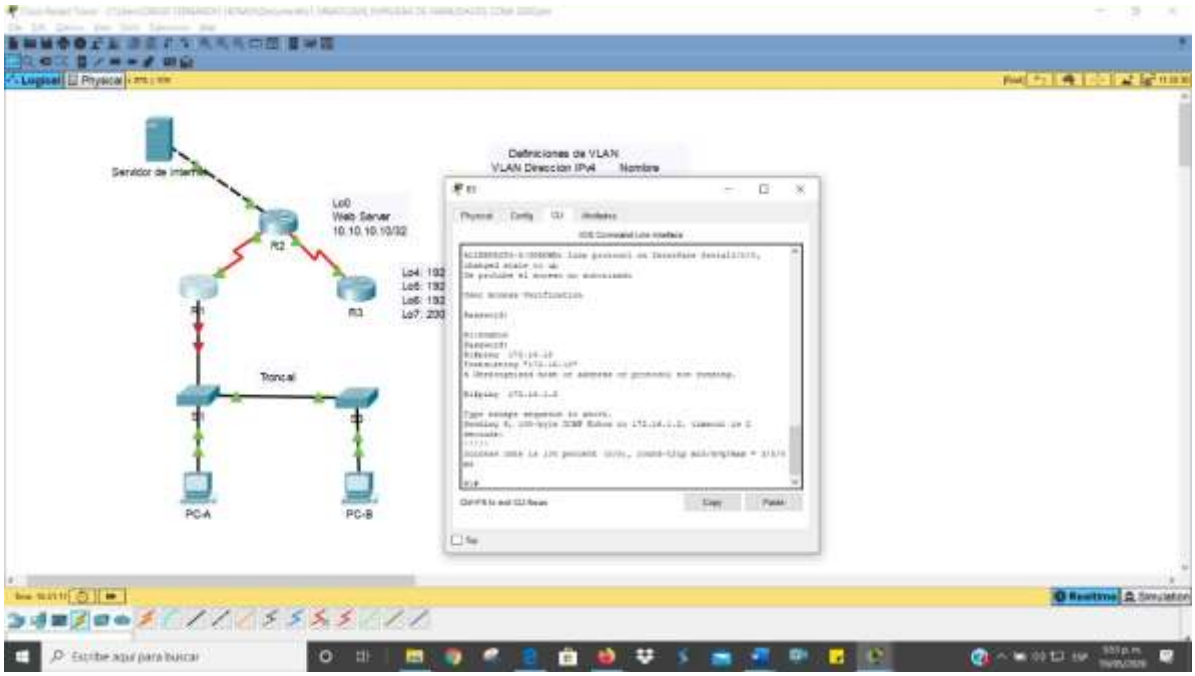


Figura 4 - Ping de R1 a R2

Desde R2 a R3

Password:
R2#ping 172.16.2.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/7 ms

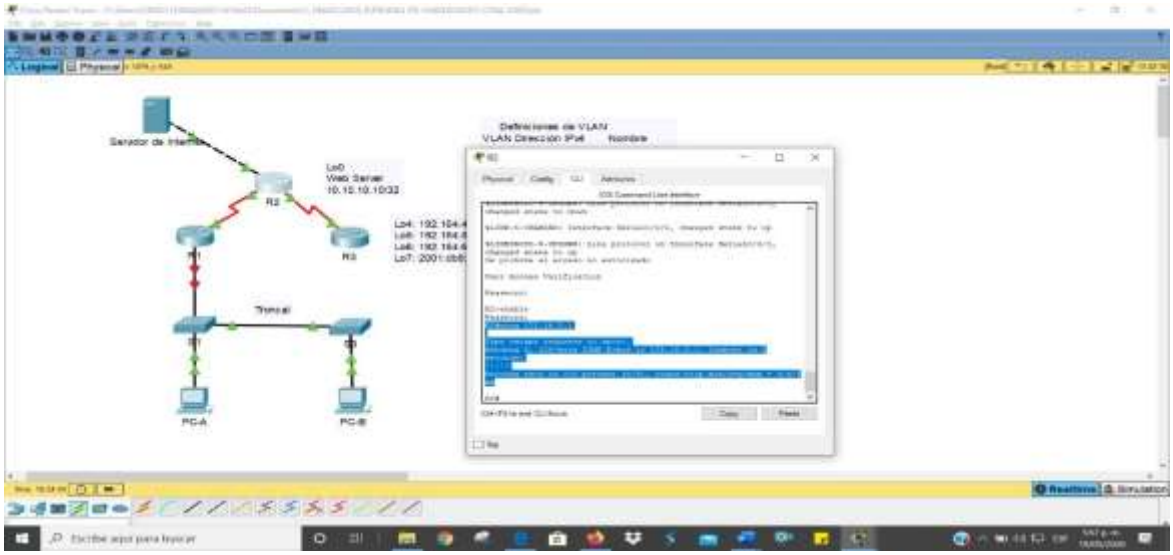


Figura 5 - Ping de R2 a R3

Desde Servidor de Internet a Gateway predeterminado

C:\>ping 209.165.200.233

Pinging 209.165.200.233 with 32 bytes of data:

Reply from 209.165.200.233: bytes=32 time<1ms TTL=255
Reply from 209.165.200.233: bytes=32 time<1ms TTL=255
Reply from 209.165.200.233: bytes=32 time<1ms TTL=255
Reply from 209.165.200.233: bytes=32 time<1ms TTL=255

Ping statistics for 209.165.200.233:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms

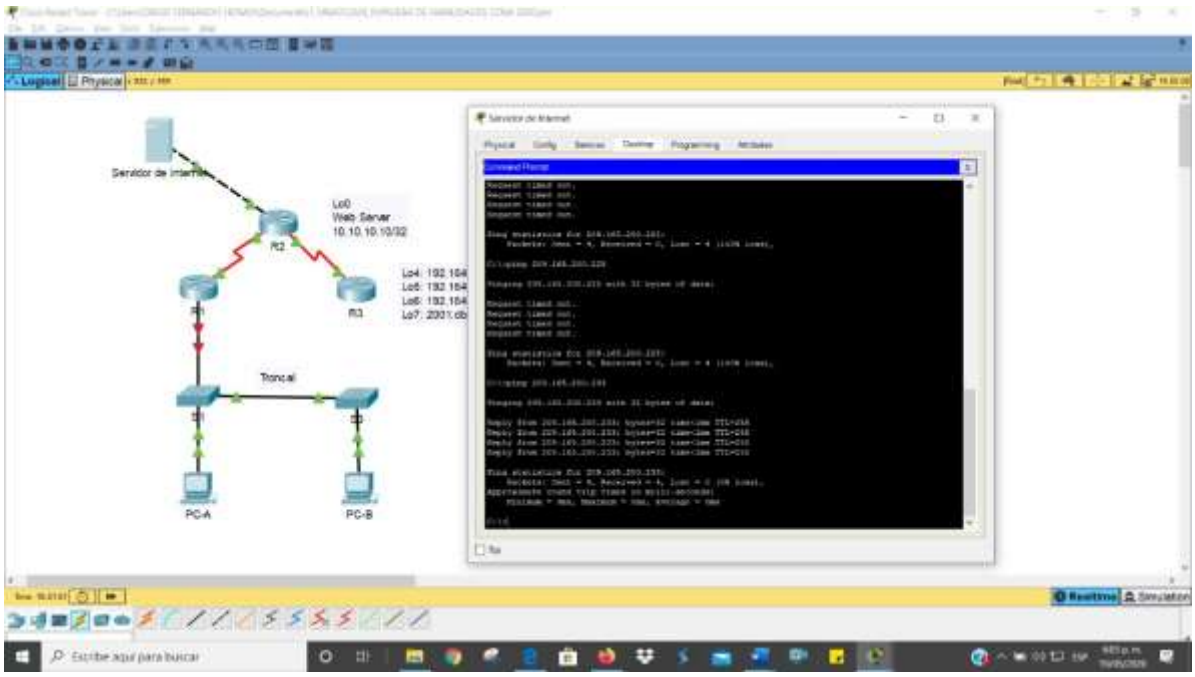


Figura 6 - Ping de Servidor de Internet a Gateway Predeterminado

Como se puede evidenciar todos los pings fueron exitosos.

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

Paso 1: Configurar S1

Tabla 9 - Configuración de las VLAN en el Switch S1

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	S1>enable S1#config t S1(config)#vlan 21 S1(config-vlan)#name Contabilidad S1(config-vlan)#vlan 23 S1(config-vlan)#name Ingenieria S1(config-vlan)#vlan 99 S1(config-vlan)#name Administracion

Asignar la dirección IP de administración.	S1(config)#int vlan 99 S1(config-if)# %LINK-5-CHANGED: Interface Vlan99, changed state to up S1(config-if)#ip address 192.168.99.2 255.255.255.0 S1(config-if)#no shutdown
Asignar el gateway predeterminado	S1(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	S1(config)#int f0/3 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1
Forzar el enlace troncal en la interfaz F0/5	S1(config-if)#int f0/5 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	S1(config-if)#int range f0/1-2, f0/4, f0/6-24, g0/1-2 S1(config-if-range)#switchport mode access+
Asignar F0/6 a la VLAN 21	S1(config-if-range)#int f0/6 S1(config-if)#switchport access vlan 21
Apagar todos los puertos sin usar	S1(config-if)#int range f0/1-2, f0/4, f0/7-24, g0/1-2 S3(config-if-range)#shutdown

La configuración del S1 incluye las siguientes tareas:

Procedemos a crear las bases de datos de las VLAN así:

S1>enable
S1#config t
S1(config)#vlan 21
S1(config-vlan)#name Contabilidad
S1(config-vlan)#vlan 23
S1(config-vlan)#name Ingenieria
S1(config-vlan)#vlan 99
S1(config-vlan)#name Administracion

Ahora asignamos la dirección IP de Administración

S1(config)#int vlan 99
S1(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up

S1(config-if)#ip address 192.168.99.2 255.255.255.0
S1(config-if)#no shutdown

Asignamos el Gateway predeterminado

S1(config)#ip default-gateway 192.168.99.1

Forzamos el enlace troncal en las interfaces F0/3 y F0/5, utilizando la red VLAN 1 como VLAN nativa.

S1(config)#int f0/3
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 1
S1(config-if)#int f0/5
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 1

Configuramos los puertos restantes como puertos de acceso, utilizando el comando *interface range.*

S1(config-if)#int range f0/1-2, f0/4, f0/6-24, g0/1-2
S1(config-if-range)#switchport mode access

Asignamos F0/6 a la VLAN 21

S1(config-if-range)#int f0/6
S1(config-if)#switchport access vlan 21

Por último realizamos el apagado de todos los puertos sin usar.

S1(config-if)#int range f0/1-2, f0/4, f0/7-24, g0/1-2
S3(config-if-range)#shutdown

Paso 2: Configurar S3

Tabla 10 - Configuración de las VLAN en el Switch S3

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	S3>enable S3#config t 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)#int vlan 99 S3(config-if)# %LINK-5-CHANGED: Interface Vlan99, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up S3(config-if)#ip address 192.168.99.3 255.255.255.0 S3(config-if)#no shutdown
Asignar el gateway predeterminado.	S3(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	S3(config)#int f0/3 S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	S3(config-if)#int range f0/1-2, f0/4-24, g0/1-2 S3(config-if-range)#switchport mode access
Asignar F0/18 a la VLAN 21	S3(config-if-range)#int f0/18 S1(config-if)#switchport access vlan 23
Apagar todos los puertos sin usar	S3(config-if)#int range f0/1-2, f0/4-17, f0/19-24, g0/1-2 S3(config-if-range)#shutdown

La configuración del S3 incluye las siguientes tareas:

Procedemos a crear las bases de datos de las VLAN así:

S3>enable
S3#config t
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

Ahora asignamos la dirección IP de Administración

S3(config)#int vlan 99
S3(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up

S3(config-if)#ip address 192.168.99.3 255.255.255.0
S3(config-if)#no shutdown

Asignamos el Gateway predeterminado

S3(config)#ip default-gateway 192.168.99.1

Forzamos el enlace troncal en las interfaz F0/3, utilizando la red VLAN 1 como VLAN nativa.

S3(config)#int f0/3
S3(config-if)#switchport mode trunk
S3(config-if)#switchport trunk native vlan 1

Configuramos los puertos restantes como puertos de acceso, utilizando el comando *interface range.*

S3(config-if)#int range f0/1-2, f0/4-24, g0/1-2
S3(config-if-range)#switchport mode access

Se asigna F0/18 a la VLAN 23

S3(config-if-range)#int f0/18
S1(config-if)#switchport access vlan 23

Por último se realiza el apagado de todos los puertos sin usar.

S3(config-if)#int range f0/1-2, f0/4-17, f0/19-24, g0/1-2
S3(config-if-range)#shutdown

Paso 3: Configuración R1

Tabla 11 - Configuración del R1

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	R1>enable R1#config t R1(config)#int g0/1.21 R1(config-subif)# R1(config-subif)#description LAN de Contabilidad R1(config-subif)#encapsulation dot1q 21 R1(config-subif)#ip address 192.168.21.1 255.255.255.0
Configurar la subinterfaz 802.1Q .23 en G0/1	R1>enable R1#config t R1(config)#int g0/1.23 R1(config-subif)# R1(config-subif)#description LAN de Ingeniería R1(config-subif)#encapsulation dot1q 23 R1(config-subif)#ip address 192.168.23.1 255.255.255.0

Configurar la subinterfaz 802.1Q .99 en G0/1	R1>enable R1#config t R1(config)#int g0/1.99 R1(config-subif)# R1(config-subif)#description LAN de Administración R1(config-subif)#encapsulation dot1q 99 R1(config-subif)#ip address 192.168.99.1 255.255.255.0
Activar la interfaz G0/1	R1(config-subif)#int g0/1 R1(config-if)#no shutdown

En este paso se realizan las tareas de configuración para R1, dentro de las cuales se incluyen las siguientes:

Se realiza la configuración de la subinterfaz 802.1Q.21 en G0/1 con la descripción LAN de Contabilidad y le asignamos la primera dirección disponible a esta interfaz.

R1>enable
R1#config t
R1(config)#int g0/1.21
R1(config-subif)#
R1(config-subif)#description LAN de Contabilidad
R1(config-subif)#encapsulation dot1q 21
R1(config-subif)#ip address 192.168.21.1 255.255.255.0

Configuramos la subinterfaz 802.1Q.23 en G0/1 con la descripción LAN de Ingeniería y le asignamos la primera dirección disponible a esta interfaz.

R1>enable
R1#config t
R1(config)#int g0/1.23
R1(config-subif)#
R1(config-subif)#description LAN de Ingeniería
R1(config-subif)#encapsulation dot1q 23
R1(config-subif)#ip address 192.168.23.1 255.255.255.0

Configuramos la subinterfaz 802.1Q.99 en G0/1 con la descripción LAN de Contabilidad y le asignamos la primera dirección disponible a esta interaz.

R1>enable
R1#config t
R1(config)#int g0/1.99
R1(config-subif)#
R1(config-subif)#description LAN de Administración
R1(config-subif)#encapsulation dot1q 99
R1(config-subif)#ip address 192.168.99.1 255.255.255.0

Para terminar activamos la interfaz G0/1

R1(config-subif)#int g0/1
R1(config-if)#no shutdown

Paso 4: Verificar la conectividad de la red

Tabla 12 - Verificación de la conectividad de la red

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.11	Satisfactorio
S3	R1, dirección VLAN 99	192.168.99.1	Satisfactorio
S1	R1, dirección VLAN 21	192.168.21.1	Satisfactorio
S3	R1, dirección VLAN 23	192.168.23.1	Satisfactorio

Se procede entonces a probar la conectividad entre los switches y el R1, con ayuda del comando ping así:

Desde S1 a R1 dirección VLAN 99

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 = 0/0/0 ms

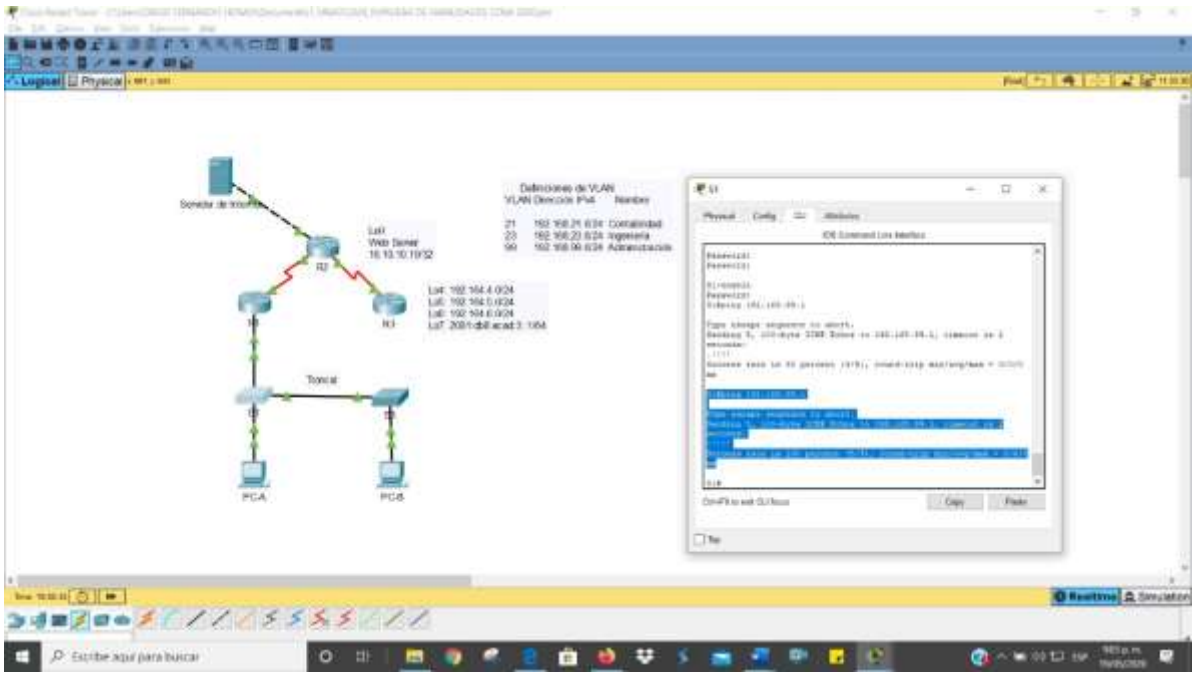


Figura 7 - Ping De S1 a R1 VLAN 99

Desde S3 a R1 dirección VLAN 99

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 = 0/0/1 ms

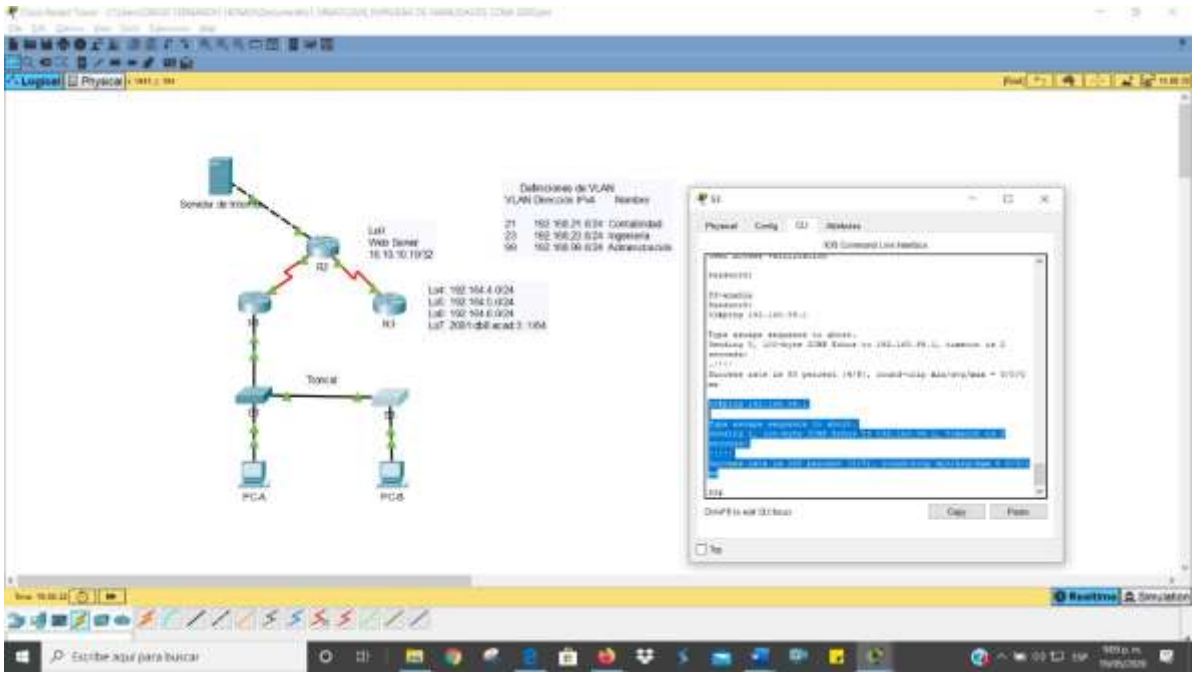


Figura 8 - Ping De S3 a R1 VLAN 99

Desde S1 a R1 dirección VLAN 21

S1#ping 192.168.21.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.21.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

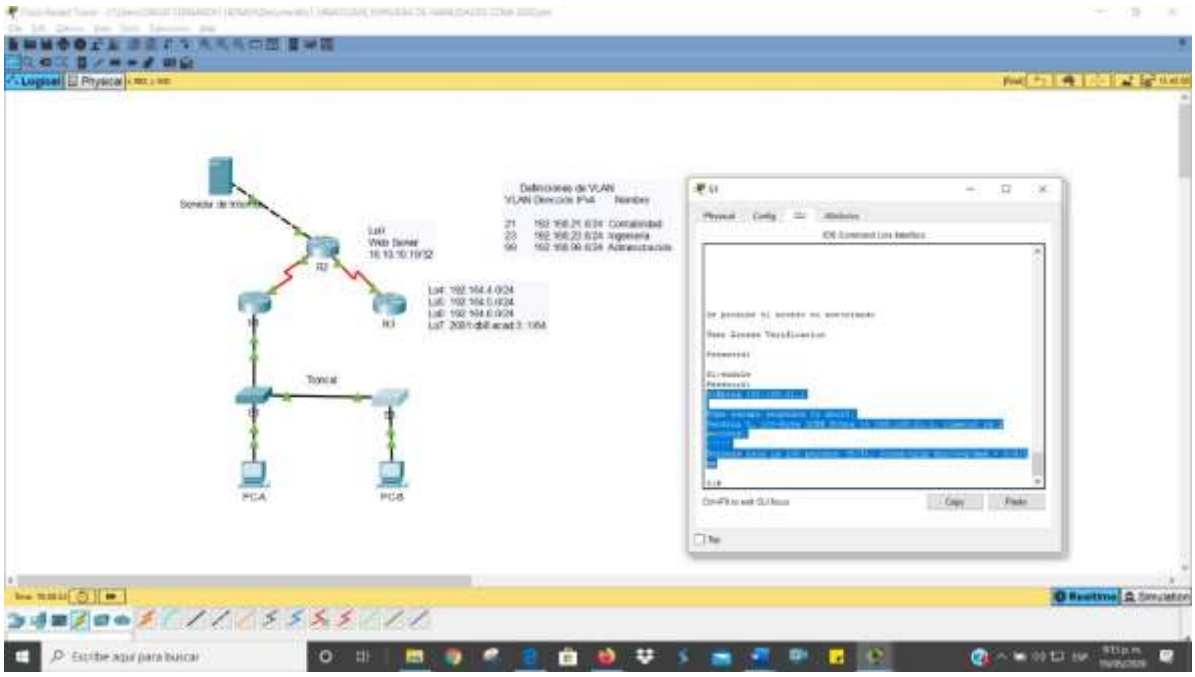


Figura 9 - Ping De S1 a R1 VLAN 21

Desde S3 a R1 dirección VLAN 23

S3#ping 192.168.23.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.23.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms

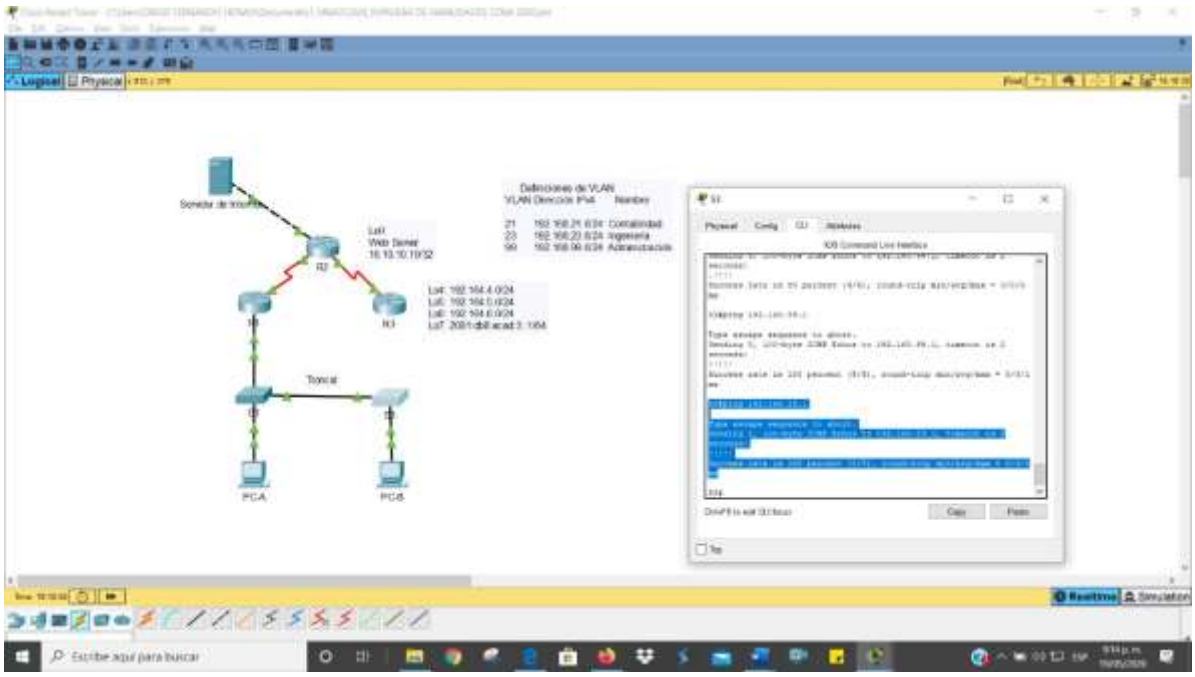


Figura 10 - Ping De S3 a R1 VLAN 23

Al terminar de realizar todos los pings, evidenciamos que todos fueron exitosos.

Parte 4: Configurar el protocolo de routing dinámico RIPv2

Paso 1: Configurar RIPv2 en el R1

Tabla 13 - Configuración de RIPv2 en el Router R1

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	R1>enable Password: R1#config t Enter configuration commands, one per line. End with CNTL/Z. R1(config)#router rip R1(config-router)#version 2

Anunciar las redes conectadas directamente	*R1(config-router)#do show ip route connected* *C 172.16.1.0/30 is directly connected, Serial0/0/0* *C 192.168.21.0/24 is directly connected, GigabitEthernet0/1.21* *C 192.168.23.0/24 is directly connected, GigabitEthernet0/1.23* *C 192.168.99.0/24 is directly connected, GigabitEthernet0/1.99* *R1(config-router)#* *R1(config-router)#network 172.16.1.0* *R1(config-router)#network 192.168.21.0* *R1(config-router)#network 192.168.23.0* *R1(config-router)#network 192.168.99.0*
Establecer todas las interfaces LAN como pasivas	*R1(config-router)#passive-interface g0/1.21* *R1(config-router)#passive-interface g0/1.23* *R1(config-router)#passive-interface g0/1.99*
Desactive la sumarización automática	R1(config-router)#no auto-summary

Los pasos para la configuración de RIPv2 en el R1 serían los siguientes:

R1>enable
Password:
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.

R1(config)#router rip
R1(config-router)#version 2

Luego procedemos a asignar y anunciar todas las redes conectadas directamente así:

R1(config-router)#do show ip route connected
C 172.16.1.0/30 is directly connected, Serial0/0/0
C 192.168.21.0/24 is directly connected, GigabitEthernet0/1.21
C 192.168.23.0/24 is directly connected, GigabitEthernet0/1.23
C 192.168.99.0/24 is directly connected, GigabitEthernet0/1.99
R1(config-router)#
R1(config-router)#network 172.16.1.0
R1(config-router)#network 192.168.21.0
R1(config-router)#network 192.168.23.0
R1(config-router)#network 192.168.99.0

Luego establecemos todas interfaces LAN como pasivas

R1(config-router)#passive-interface g0/1.21
R1(config-router)#passive-interface g0/1.23
R1(config-router)#passive-interface g0/1.99

Para terminar desactivamos la sumarización automática

R1(config-router)#no auto-summary

Paso 2: Configurar RIPv2 en el R2

Tabla 14 - Configuración del RIPv2 en el Router R2

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	*R2>enable* *Password:* *R2#config t* *Enter configuration commands, one per line. End with CNTL/Z.* *R2(config)#router rip* *R2(config-router)#version 2*

Anunciar las redes conectadas directamente	R2(config-router)#network 10.10.10.10 R2(config-router)#network 172.16.1.0 R2(config-router)#network 172.16.2.0 Nota: Omitir la red G0/0.
Establecer la interfaz LAN (loopback) como pasiva	R2(config-router)#passive-interface loopback 0
Desactive la sumarización automática.	R2(config-router)#no auto-summary

Los pasos para la configuración de RIPv2 en el R2 serían los siguientes:

R2>enable
Password:
R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#router rip
R2(config-router)#version 2

Luego procedemos a asignar y anunciar todas las redes conectadas directamente, excepto la red G0/0 así:

R2(config-router)#do show ip route connected
C 10.10.10.10/32 is directly connected, Loopback0
C 172.16.1.0/30 is directly connected, Serial0/0/0
C 172.16.2.0/30 is directly connected, Serial0/0/1
C 209.165.200.232/29 is directly connected, GigabitEthernet0/0

R2(config-router)#network 10.10.10.10
R2(config-router)#network 172.16.1.0
R2(config-router)#network 172.16.2.0

Luego establecemos la interface loopback como pasiva,
R2(config-router)#passive-interface loopback 0

R2(config-router)#no auto-summary
R2(config-router)#

Paso 3: Configurar RIPv2 en el R3

Tabla 15 - Configuración del RIPv2 en el Router R3

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	R3>enable Password: R3#config t Enter configuration commands, one per line. End with CNTL/Z. R3(config)#router rip R3(config-router)#version 2
Anunciar redes IPv4 conectadas directamente	R3(config-router)#network 172.16.2.0 R3(config-router)#network 192.168.4.0 R3(config-router)#network 192.168.5.0 R3(config-router)#network 192.168.6.0
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	R3(config-router)#passive-interface loopback 4 R3(config-router)#passive-interface loopback 5 R3(config-router)#passive-interface loopback 6
Desactive la sumarización automática.	R3(config-router)#no auto-summary

Los pasos para la configuración de RIPv2 en el R2 serían los siguientes:

R3>enable
Password:
R3#config t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#router rip
R3(config-router)#version 2

Luego procedemos a asignar y anunciar todas las redes conectadas directamente, pero primero verificamos cuáles rutas ip se encuentran conectadas al router.

R3(config-router)#do show ip route connected
C 172.16.2.0/30 is directly connected, Serial0/0/1
C 192.168.4.0/24 is directly connected, Loopback4
C 192.168.5.0/24 is directly connected, Loopback5
C 192.168.6.0/24 is directly connected, Loopback6

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

Luego establecemos todas las interfaces loopback como pasivas

R3(config-router)#passive-interface loopback 4
R3(config-router)#passive-interface loopback 5
R3(config-router)#passive-interface loopback 6

Y para terminar desactivamos al sumarización automática.

R3(config-router)#no auto-summary
R3(config-router)#

Paso 4: Verificar la información de RIP

Tabla 16 - Verificación de la Información de RIP

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

Para verificar la ID del proceso RIP, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router se utiliza el comando *show ip protocols.*

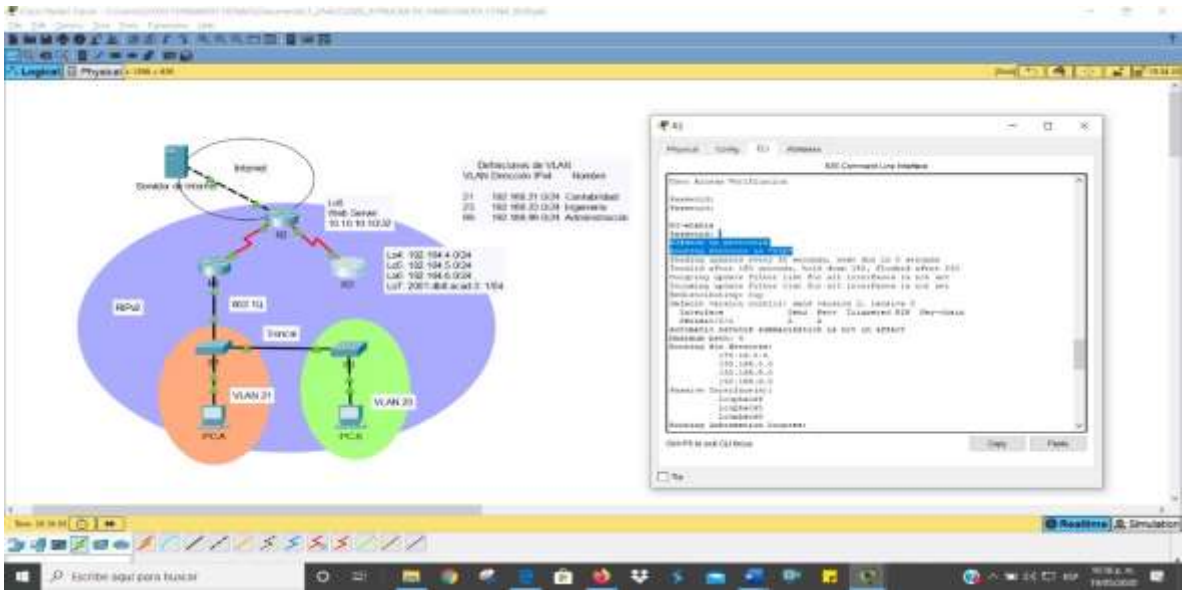


Figura 11 - Ejecución Comando Show Ip Protocols

Para mostrar únicamente las rutas RIP, se utiliza el comando *show ip*

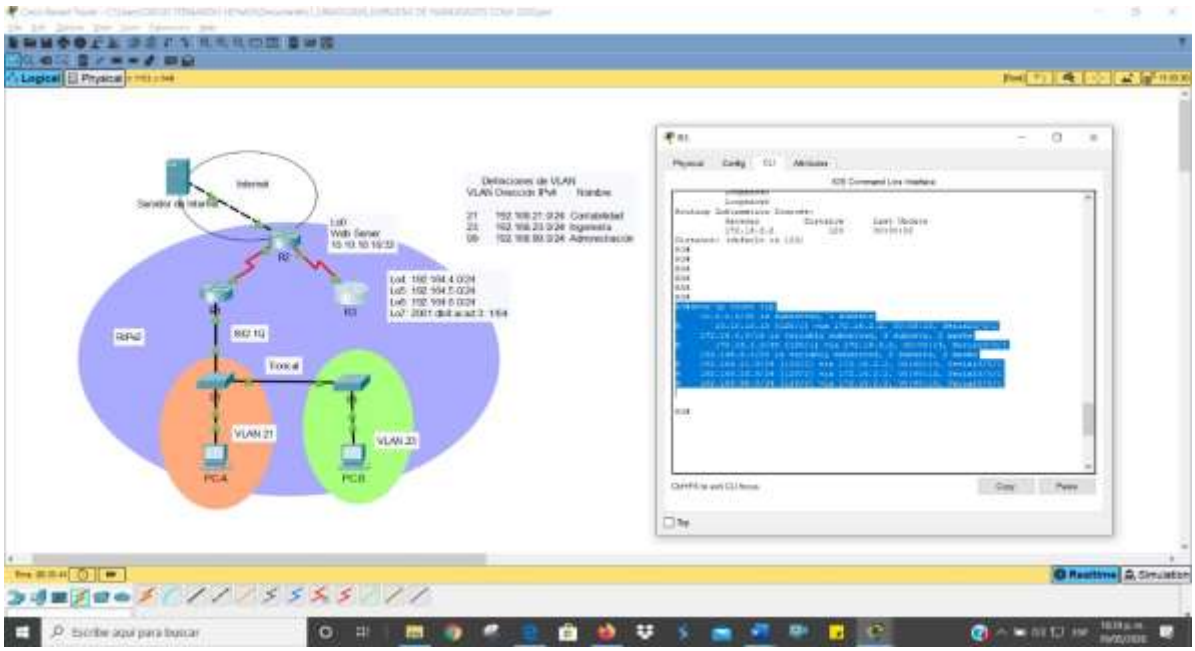


Figura 12 - Ejecución Comando Show Ip Route Rip

Para mostrar la sección de RIP de la configuración en ejecución se utiliza el comando *show run* | *section router rip*, pero como el packet tracer no recibió el comando utilizamos simplemente *show run.*

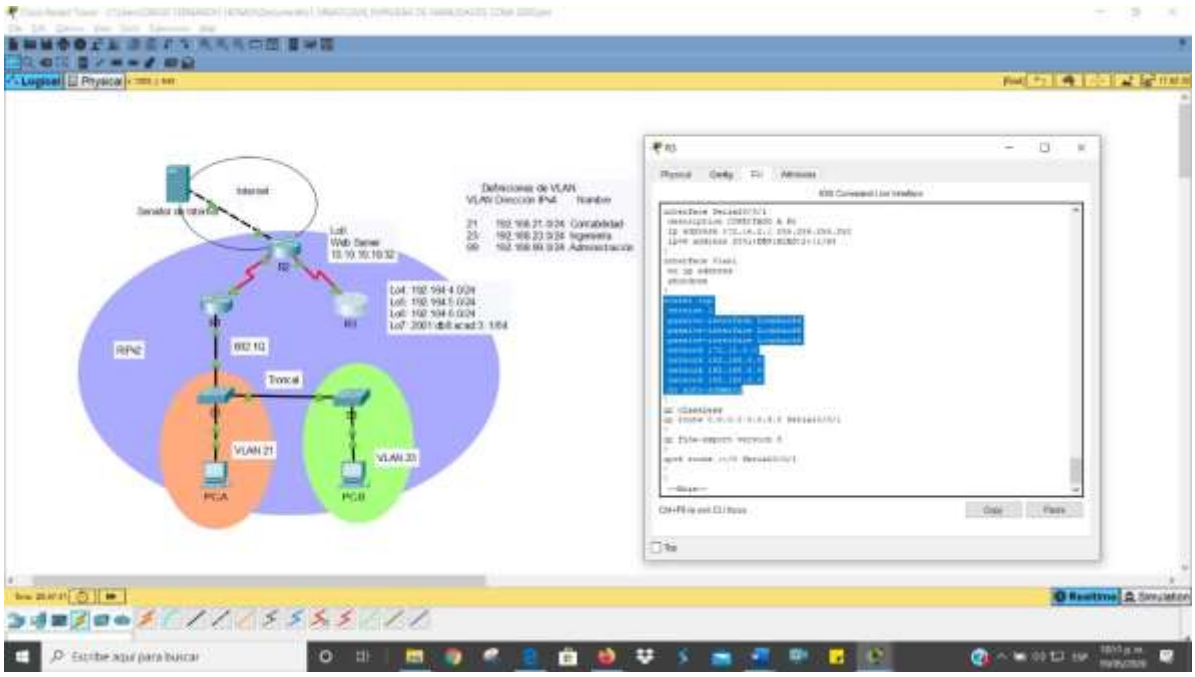


Figura 13 - Ejecución Comando Show Run

Parte 5: Implementar DHCP y NAT para IPv4

Tabla 17 - Configuración de DHCP para el Router R1 en Las VLAN 21 y 23

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	R1>enable Password: R1#config t Enter configuration commands, one per line. End with CNTL/Z. R1(config)# R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20

Crear un pool de DHCP para la VLAN 21.	R1(config)#ip dhcp pool ACCT R1(dhcp-config)#network 192.168.21.0 255.255.255.0 R1(dhcp-config)#default-router 192.168.21.1 R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com
Crear un pool de DHCP para la VLAN 23	R1(dhcp-config)#ip dhcp pool ENGNR R1(dhcp-config)#network 192.168.23.0 255.255.255.0 R1(dhcp-config)#default-router 192.168.23.1 R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com

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

Para configurar el router R1 como servidor de DHCP para las VLAN 21 y 23, debemos realizar los siguientes procedimientos:

Se reservan las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas.

R1>enable
Password:
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#
R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20

Se reservan 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

Creamos un pool de DHCP para la VLAN 21

R1(config)#ip dhcp pool ACCT
R1(dhcp-config)#network 192.168.21.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.21.1
R1(dhcp-config)#dns-server 10.10.10.10
R1(dhcp-config)#domain-name ccna-sa.com

Creamos un pool de DHCP para la VLAN 23

R1(dhcp-config)#ip dhcp pool ENGNR
R1(dhcp-config)#network 192.168.23.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.23.1
R1(dhcp-config)#dns-server 10.10.10.10
R1(dhcp-config)#domain-name ccna-sa.com

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

Tabla 18 – Configuración 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 *R2>enable* *Password:* *R2#config t* *R2(config)#username webuser privilege 15 secret cisco12345*
Habilitar el servicio del servidor HTTP	*R2(config)#ip http server*
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	*R2(config)#ip http authentication local*
Crear una NAT estática al servidor web.	*R2(config)#ip nat inside source static 10.10.10.10 209.165.200.237*
Asignar la interfaz interna y externa para la NAT estática	*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* *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 192.168.4.0 0.0.3.255
Defina el pool de direcciones IP públicas utilizables.	Nombre del conjunto: INTERNET El conjunto de direcciones incluye: 209.165.200.225 **–** 209.165.200.228 *R2(config)#ip nat pool INTERNET 209.165.200.233 209.165.200.236 netmask 255.255.255.248*
Definir la traducción de NAT dinámica	R2(config)#ip nat inside source list 1 pool INTERNET

La configuración de una NAT estática y dinámica en el R2 precisa de lo siguiente:

Se Crea una base de datos local con una cuenta de usuario con los siguientes datos:

Nombre de usuario: webuser
Contraseña: cisco12345
Nivel de privilegio: 15

R2>enable
Password:
R2#config t
R2(config)#username webuser privilege 15 secret cisco12345

Al tratar de habilitar el servicio del servidor HTTP, al igual que para configurarlo para utilizar la base de datos local para la autenticación; packet tracer no admite los comandos:

R2(config)#ip http server
^
% Invalid input detected at '^' marker.

R2(config)#ip http authentication local
^

% Invalid input detected at '^' marker.

Se crea una NAT estática al servidor web, utilizando la dirección global interna 209.165.200.237, porque si se utiliza la 209.165.200.229, no va a funcionar.

R2(config)#ip nat inside source static 10.10.10.10 209.165.200.237

Asignamos la interfaz interna y externa para la NAT estática

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
R2(config-if)#exit

Se configura la NAT dinámica dentro de una ACL privada, con lista de acceso 1 y permitiendo la traducción de las redes de Contabilidad y de Ingeniería, así como el resumen de las redes LAN (Loopback) en el R3.

R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255
R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255
R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255

Se define el pool de direcciones IP públicas utilizables así;

R2(config)#ip nat pool INTERNET 209.165.200.233 209.165.200.236 netmask 255.255.255.248

Para terminar se define la traducción de NAT dinámica

R2(config)#ip nat inside source list 1 pool INTERNET

Paso 3: Verificar el protocolo DHCP y la NAT estática

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	Satisfactorio
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	Satisfactorio
Verificar que la PC-A pueda hacer ping a la PC-C Nota: Quizá sea necesario deshabilitar el firewall de la PC.	Satisfactorio
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	No fue satisfactorio ya que Packet Tracer no aceptó los comandos para la configuración del servidor HTTP

A continuación se realizan algunas pruebas para verificar que las configuraciones de DHCP y NAT estática funcionen de forma correcta así:

Verificamos que la PC-A haya adquirido información de IP del servidor de DHCP y observamos que fue satisfactorio.

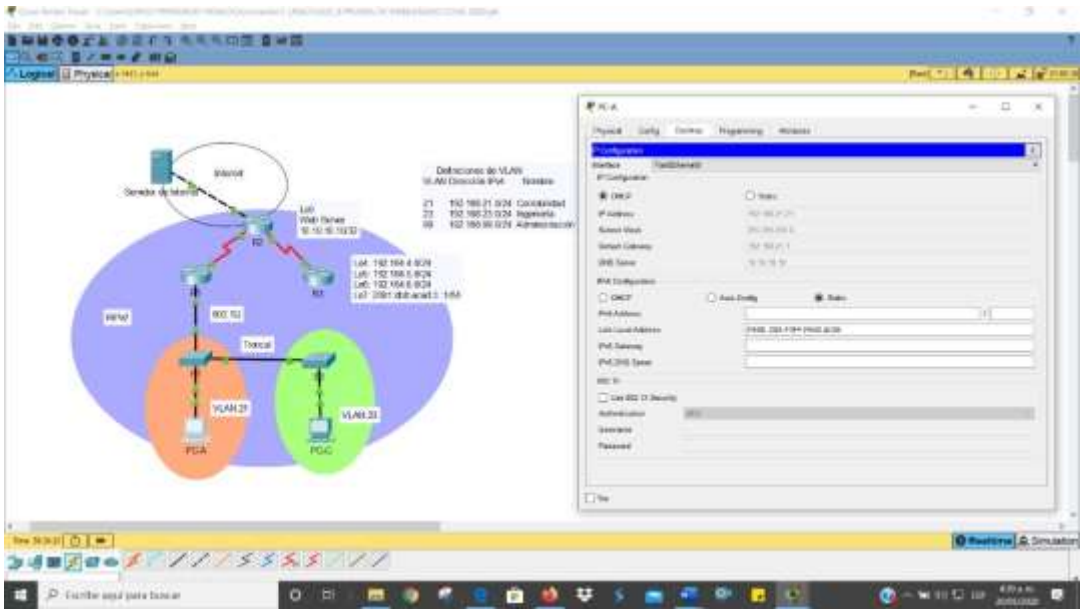


Figura 14 – Verificación Protocolo DHCP y NAT Estática de PC-A

Verificamos que la PC-B haya adquirido información de IP del servidor de DHCP y observamos que fue satisfactorio.

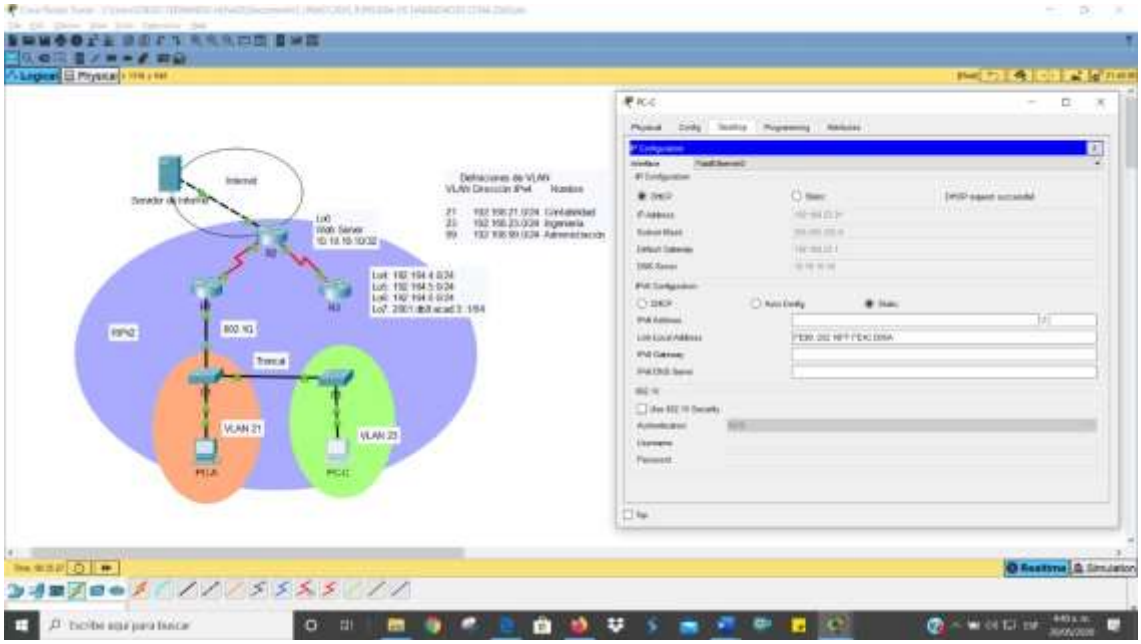


Figura 15 - Verificación Protocolo DHCP y NAT Estática de PC-C

Verificar que la PC-A pueda hacer ping a la PC-C, y observamos que fue satisfactorio.

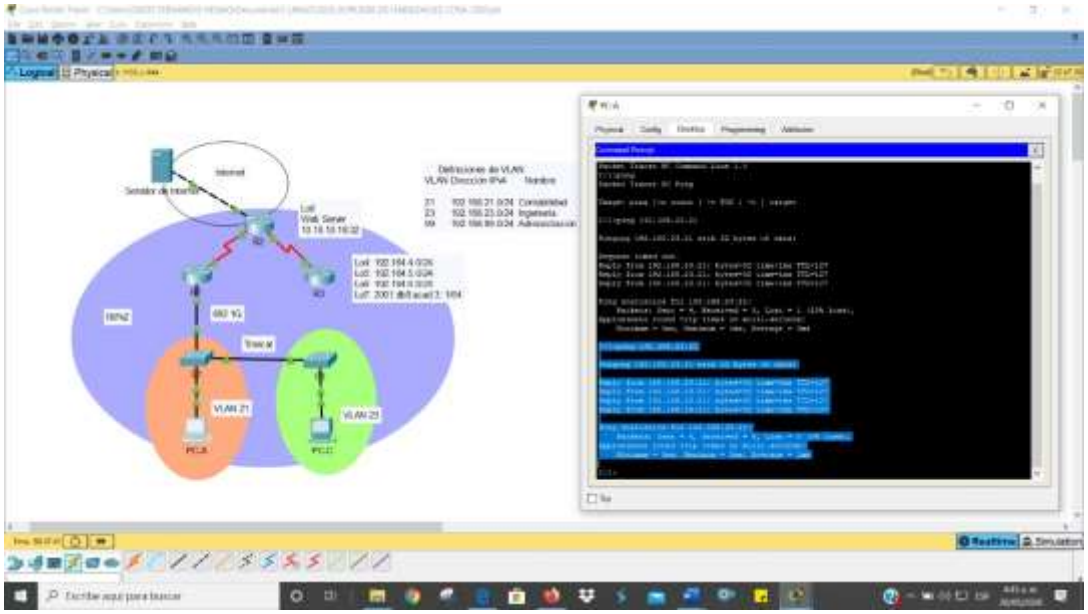


Figura 16 - Ping PC-A a PC-C

Al tratar de utilizar el navegador web en la computadora de Internet para acceder al servidor web (209.165.200.237) e iniciar sesión con el nombre de usuario webuser y la contraseña cisco12345, observamos que no es satisfactorio, recordemos que al tratar de habilitar el servidor HTTP, packet tracer no aceptó los comandos.

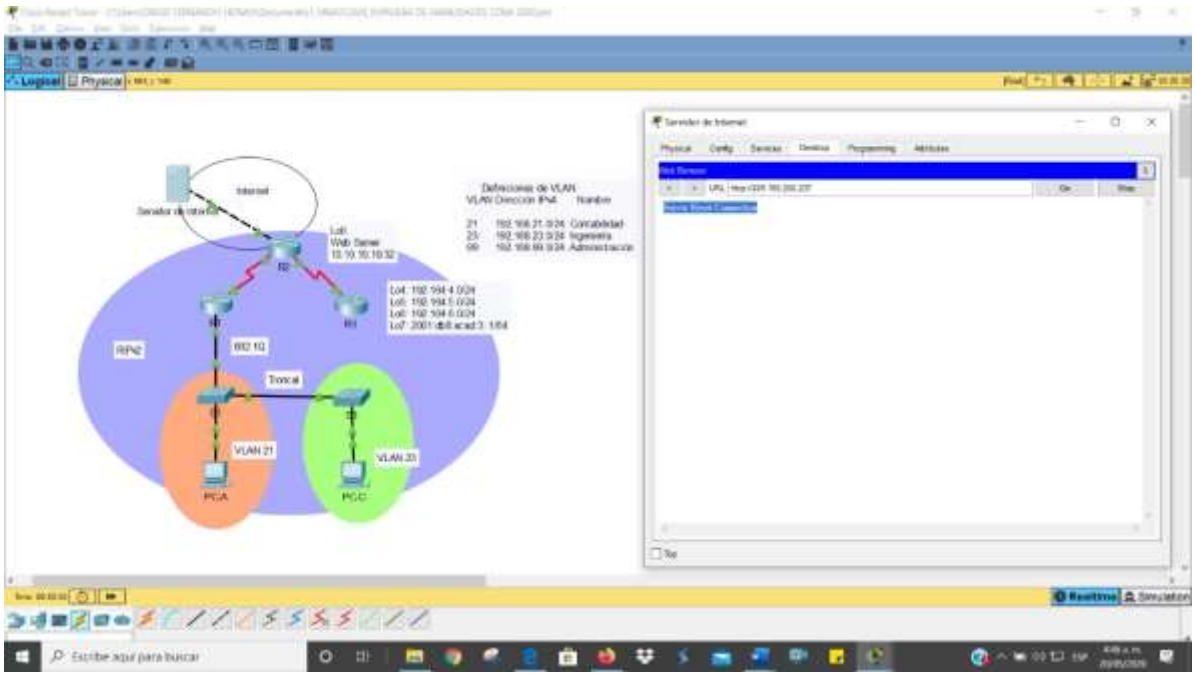


Figura 17 - Acceso Servidor Web

Parte 6: Configurar NTP

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	R2>enable Password: R2#clock set 4:48:00 20 may 2020
Configure R2 como un maestro NTP.	R2(config)#ntp master 5
Configurar R1 como un cliente NTP.	Servidor: R2 R1>enable Password: R1#config t 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#show ntp associations

Ajustamos la fecha y la hora en R2, a nuestra hora local

R2>enable
Password:
R2#clock set 4:48:00 20 may 2020

Configuramos R2 como un maestro NTP de nivel 5 con el siguiente comando:

R2(config)#ntp master 5

Configuramos R1 como un cliente NTP cuyo servidor sea R2 con los comandos a continuación:

R1>enable
Password:
R1#config t
R1(config)#ntp server 172.16.1.2

Configuramos R1 para actualizaciones de calendario periódicas con hora NTP con el siguiente comando:

R1(config)#ntp update-calendar

Para terminar con este paso, verificamos la configuración de NTP en R1, con el comando:

R1#show ntp associations
address ref clock st when poll reach delay offset disp
~172.16.1.2 127.127.1.1 5 11 16 37 13.00 858880394011.00 0.12
** sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured*
R1#

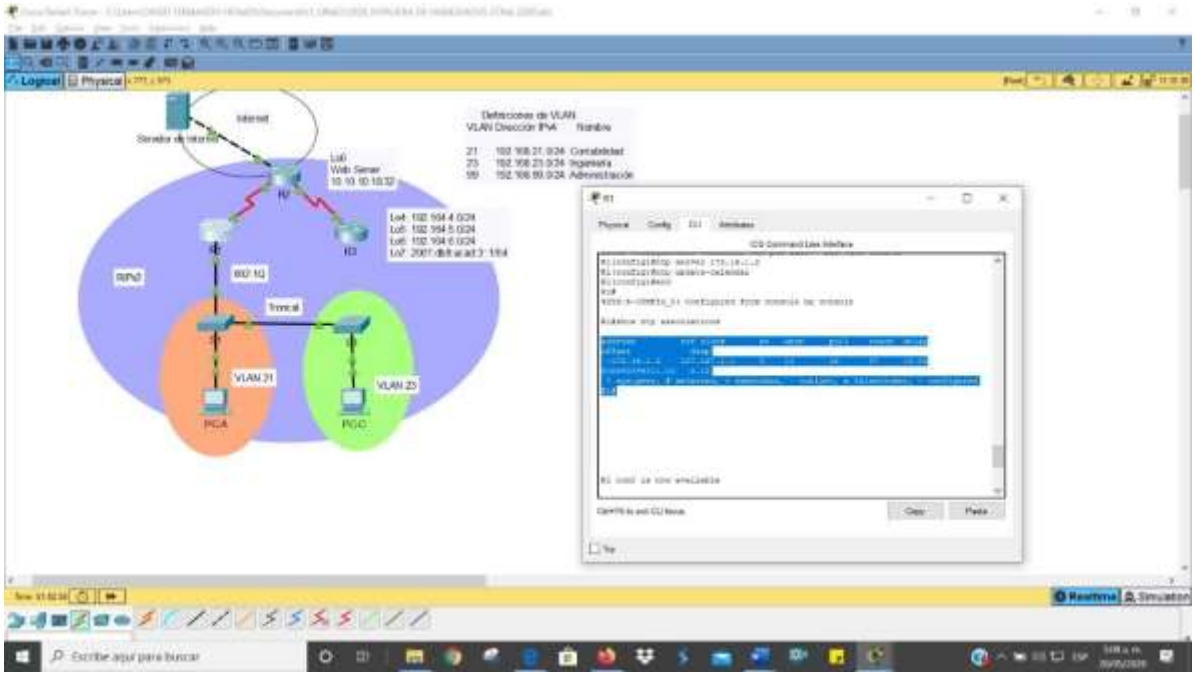


Figura 18 - Ejecución Comando ntp update-calendar

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 20 - Restricción del acceso a las líneas VTY en el R2

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

Permitir acceso por Telnet a las líneas de VTY	R2(config-line)#transport input telnet
Verificar que la ACL funcione como se espera	R1>enable Password: R1#telnet 172.16.1.2 Trying 172.16.1.2 ...OpenSe prohibe el acceso no autorizado User Access Verification Password: R2>

Para restringir el acceso a las líneas VTY en el R2, configuramos una lista de acceso con el nombre para permitir que sólo R1 establezca una conexión Telnet con R2, utilizamos el nombre ADMIN-MGT para la ACL así:

R2(config)#ip access-list standard ADMIN-MGT
R2(config-std-nacl)#permit host 172.16.1.1

Luego aplicamos la ACL con nombre a las líneas VTY

R2(config-std-nacl)#exit
R2(config)#line vty 0 15
R2(config-line)#access-class ADMIN-MGT in

Y permitimos acceso por Telnet a las líneas de VTY

R2(config-line)#transport input telnet

Y para terminar verificamos que la ACL está trabajando como lo esperado y desde R1, ingresamos al R2 y observamos que es satisfactorio.

R1>enable
Password:
R1#telnet 172.16.1.2
Trying 172.16.1.2 ...OpenSe prohibe el acceso no autorizado

User Access Verification
Password:
R2>

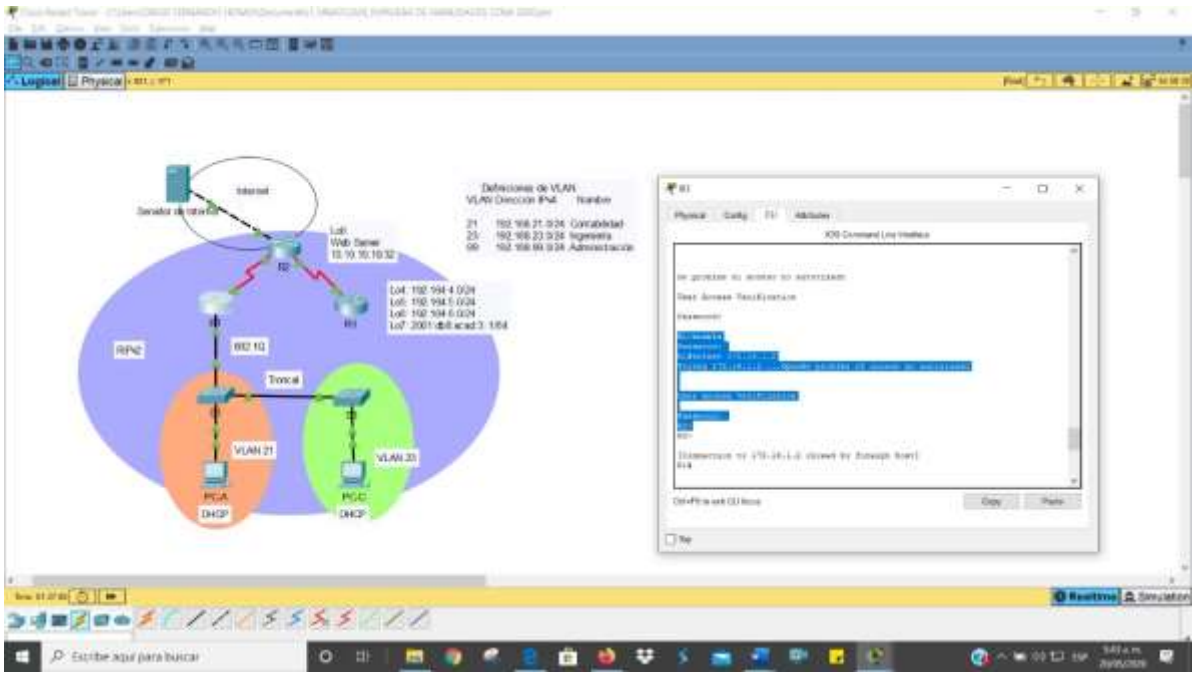


Figura 19 - Verificación ACL Para Acceso de R1 a R2

Y para continuar de verificar tratamos de ingresar desde R3 y observamos que no es posible tener acceso.

R3#telnet 172.16.1.2
Trying 172.16.1.2 ...
% Connection refused by remote host
R3#

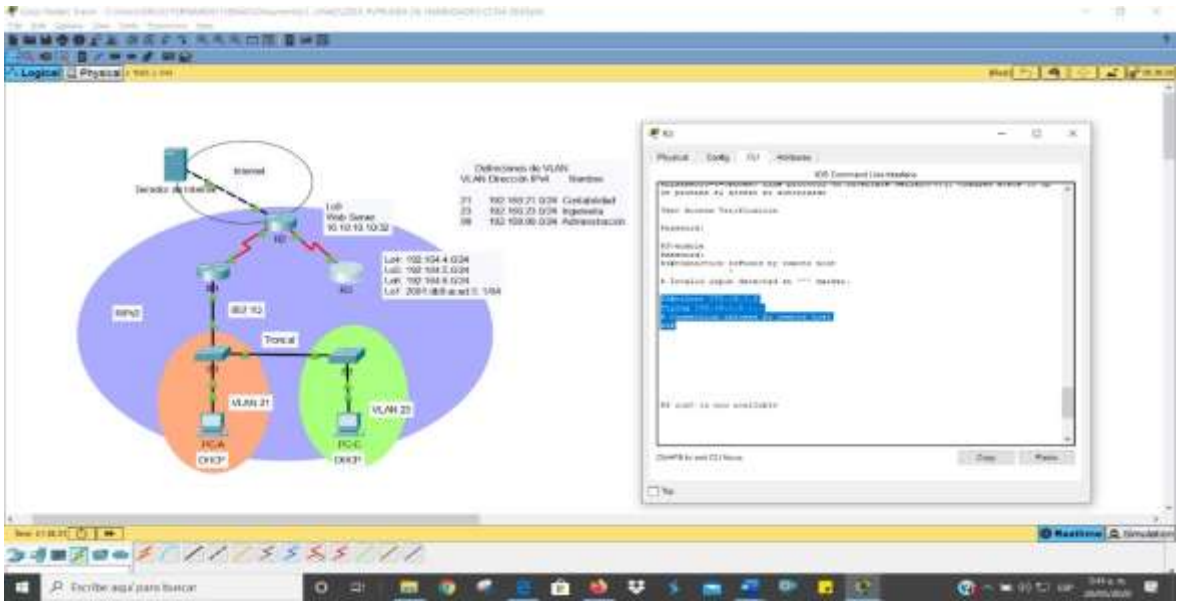


Figura 20 -Verificación ACL de Acceso Restringido de R1 a R3

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

Tabla 21 - Verificación de Listas de Acceso e Interfaces

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 Standard IP access list 1 10 permit 192.168.21.0 0.0.0.255 20 permit 192.168.23.0 0.0.0.255 30 permit 192.168.4.0 0.0.3.255 Standard IP access list ADMIN-MGT 10 permit host 172.16.1.1 (2 match(es)) R2#show ip access-list Standard IP access list 1 10 permit 192.168.21.0 0.0.0.255 20 permit 192.168.23.0 0.0.0.255 30 permit 192.168.4.0 0.0.3.255 Standard IP access list ADMIN-MGT 10 permit host 172.16.1.1 (2 match(es))
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?	R2#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?	R2#clear ip nat translation

Para mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció, utilizamos los comandos *show access-list o show ip access-list,* como se muestra a continuación.

R2#show access-list
Standard IP access list 1
10 permit 192.168.21.0 0.0.0.255
20 permit 192.168.23.0 0.0.0.255
30 permit 192.168.4.0 0.0.3.255
Standard IP access list ADMIN-MGT
10 permit host 172.16.1.1 (2 match(es))

R2#show ip access-list
Standard IP access list 1
10 permit 192.168.21.0 0.0.0.255
20 permit 192.168.23.0 0.0.0.255
30 permit 192.168.4.0 0.0.3.255
Standard IP access list ADMIN-MGT
10 permit host 172.16.1.1 (2 match(es))

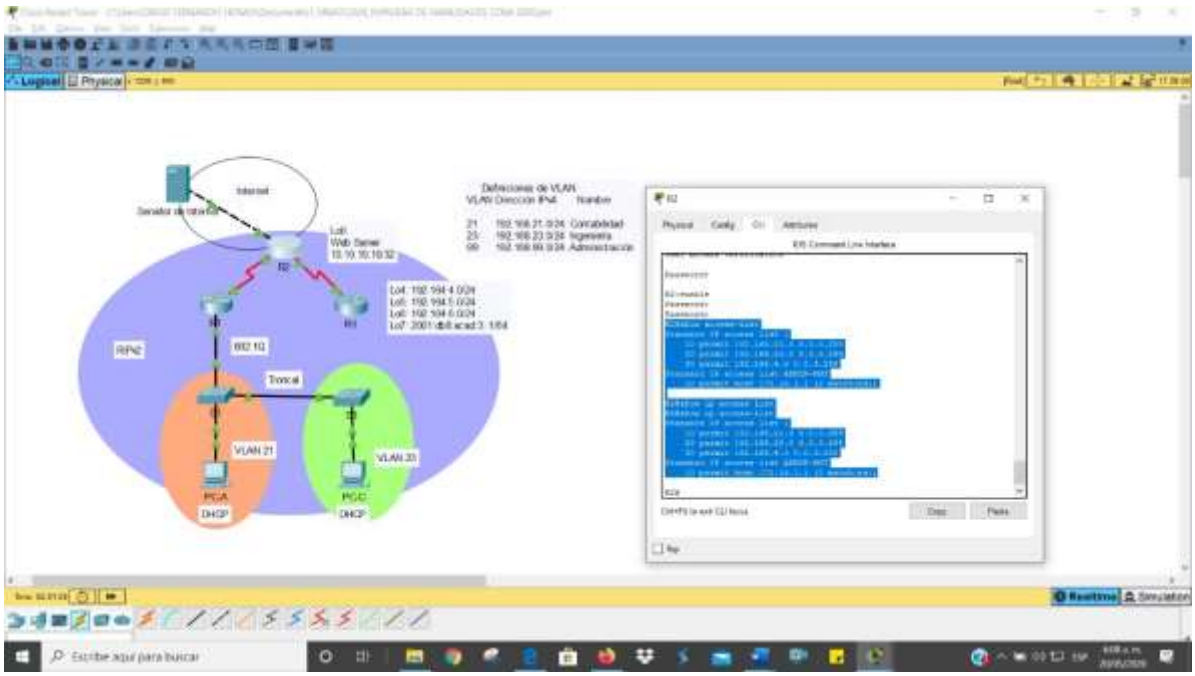


Figura 21 - Ejecución Comandos show access-list y show ip access-list

Para reiniciar los contadores de las líneas de acceso se utiliza el comando *clear ip access-list counters,* pero lamentablemente en esta ocasión no ha sido posible verificar, ya que packet tracer no soporta este comando.

R2#clear ip access-list counters
^
% Invalid input detected at '^' marker.

El comando que se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica es *show ip interface* como se muestra a continuación:

R2#show ip interface
GigabitEthernet0/0 is up, line protocol is up (connected)
Internet address is 209.165.200.233/29
Broadcast address is 255.255.255.255
Address determined by setup command
MTU is 1500 bytes
Helper address is not set
Directed broadcast forwarding is disabled
Outgoing access list is not set
Inbound access list is not set

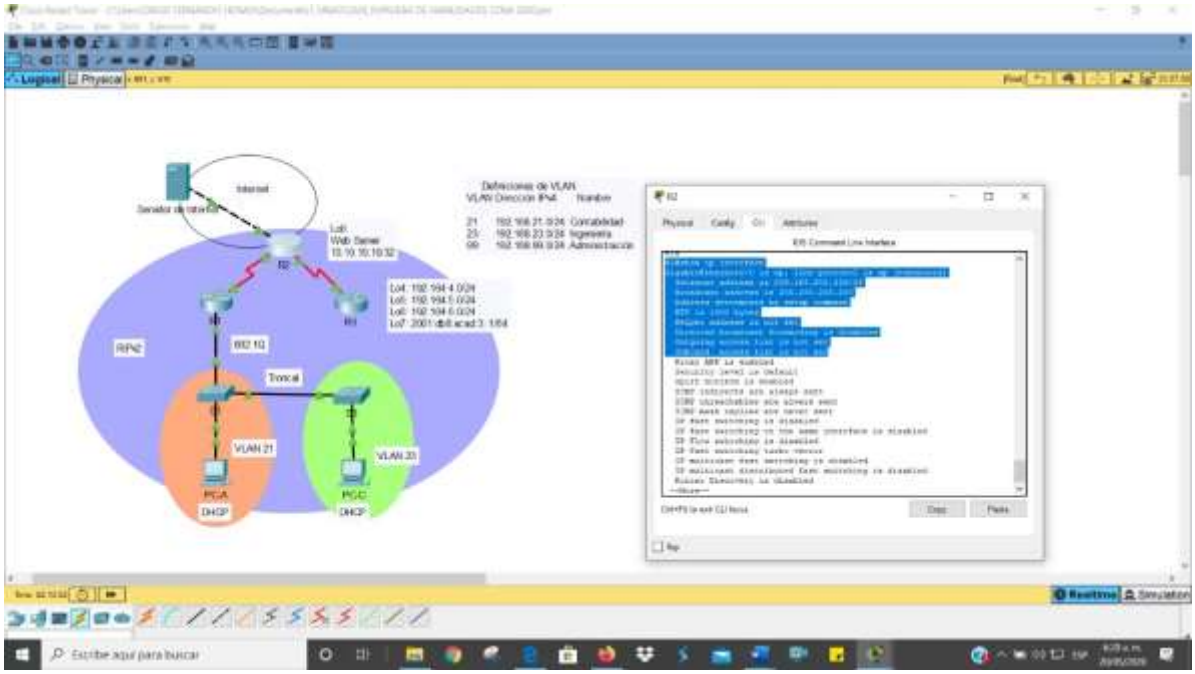


Figura 22 - Ejecución Comando Show Ip Interface

Para mostrar las traducciones de NAT, utilizamos el comando *show ip nat translations,* tal y como se muestra a continuación:

R2#show ip nat translations
Pro Inside global Inside local Outside local Outside global
--- 209.165.200.237 10.10.10.10 --- ---
tcp 209.165.200.237:80 10.10.10.10:80
209.165.200.238:1025209.165.200.238:1025
tcp 209.165.200.237:80 10.10.10.10:80
209.165.200.238:1026209.165.200.238:1026

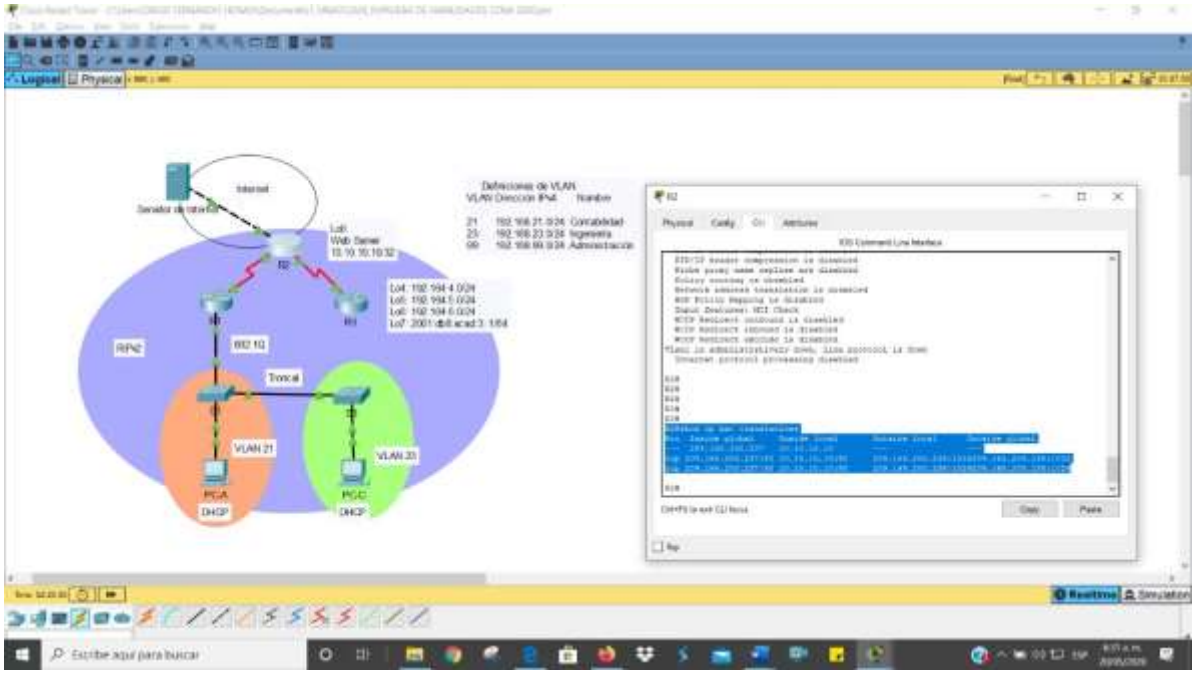


Figura 23 - Ejecución Comando Show Ip Translations

Y para eliminar las traducciones de NAT dinámicas, se utiliza el comando *clear ip nat translation* *

R2#clear ip nat translation *

Luego digitamos nuevamente el comando *show ip nat translations* y efectivamente observamos que se han borrado.

R2#show ip nat translations
Pro Inside global Inside local Outside local Outside global

--- 209.165.200.237 10.10.10.10 --- ---

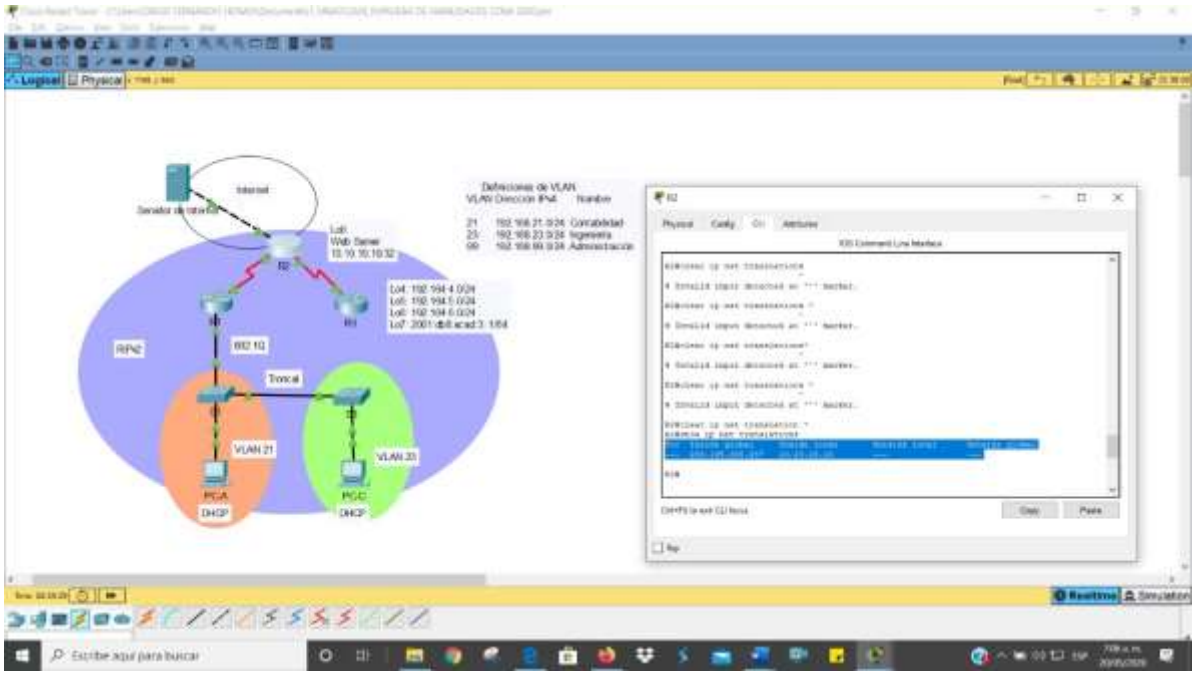


*Figura 24 - Ejecución Comandos clear ip nat translation * y show ip nat translations*

Ya para finalizar con todos pasos y verificar que efectivamente la red funciona y que la conectividad es satisfactoria, para lo cual a continuación se deja evidencia de los siguientes procesos:

Ping de PC-A a Servidor de Internet

Pinging 209.165.200.238 with 32 bytes of data:

Reply from 209.165.200.238: bytes=32 time=2ms TTL=126
Reply from 209.165.200.238: bytes=32 time=1ms TTL=126
Reply from 209.165.200.238: bytes=32 time=4ms TTL=126
Reply from 209.165.200.238: bytes=32 time=1ms TTL=126

Ping statistics for 209.165.200.238:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 4ms, Average = 2ms

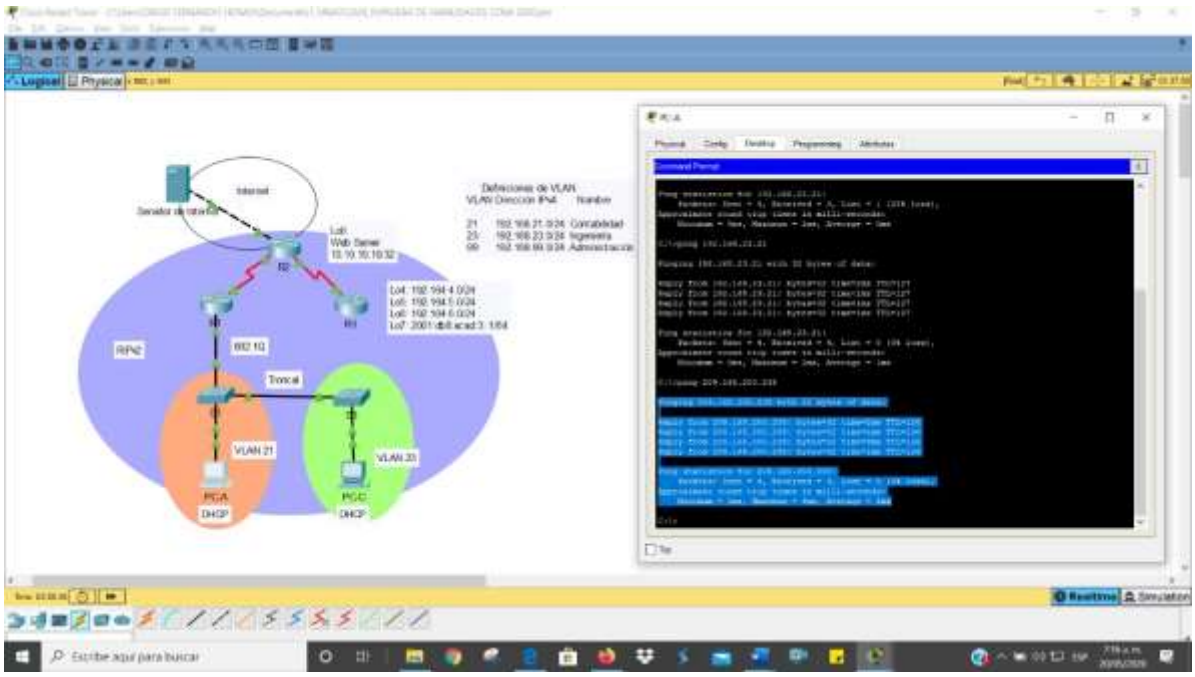


Figura 25 - Ping de PC-A a Servidor de Internet

Ping de PC-C a Servidor de Internet

C:\>ping 209.165.200.238

Pinging 209.165.200.238 with 32 bytes of data:

Reply from 209.165.200.238: bytes=32 time=2ms TTL=126
Reply from 209.165.200.238: bytes=32 time=12ms TTL=126
Reply from 209.165.200.238: bytes=32 time=1ms TTL=126
Reply from 209.165.200.238: bytes=32 time=2ms TTL=126

Ping statistics for 209.165.200.238:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 12ms, Average = 4ms

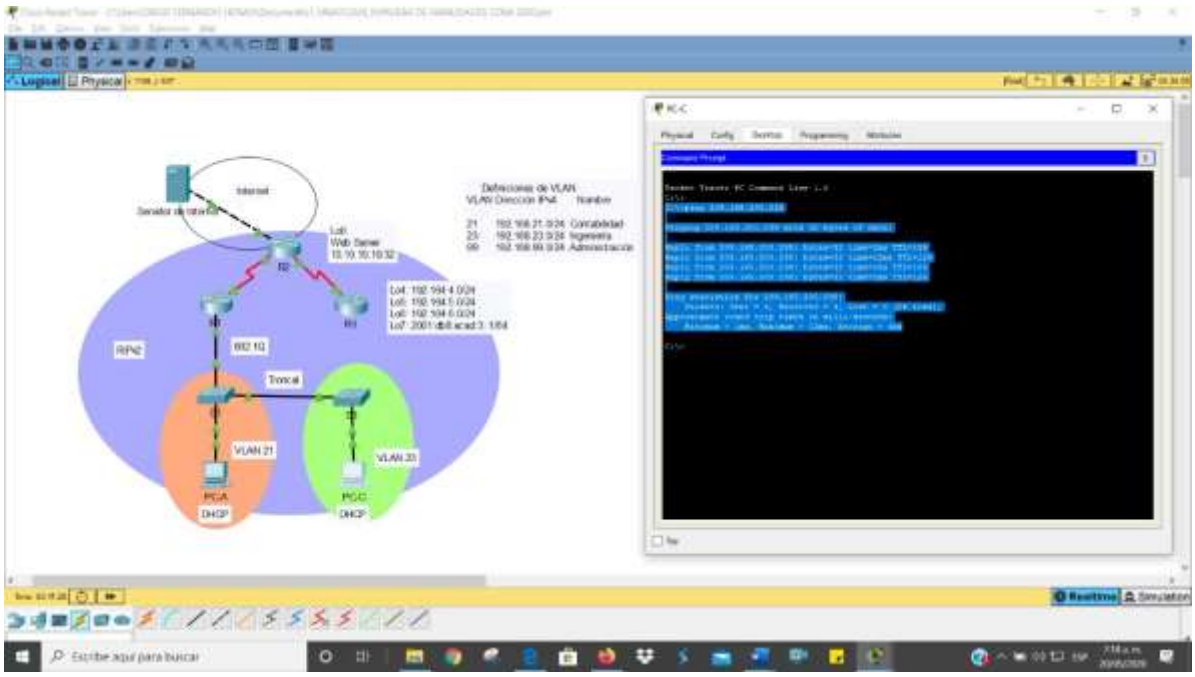


Figura 26 - Ping de PC-C a Servidor de Internet

Acceso desde PC-A al Servidor Web

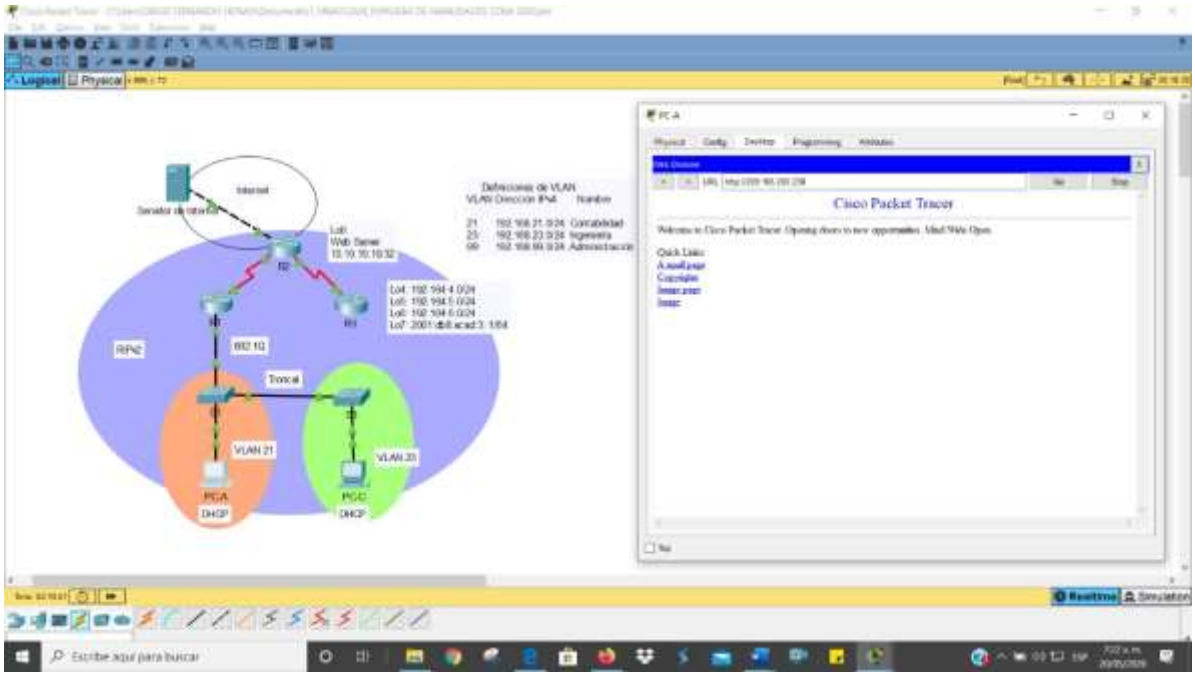


Figura 27 - Acceso de PC-A a Servidor Web

Acceso desde PC-C al Servidor Web

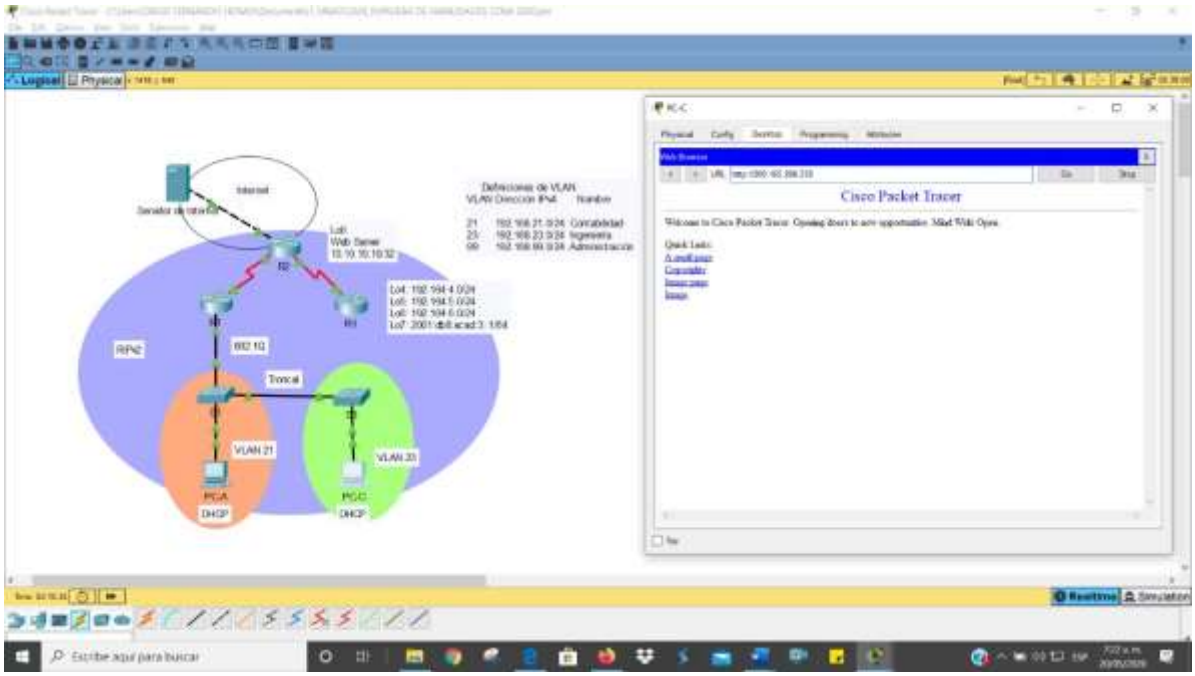
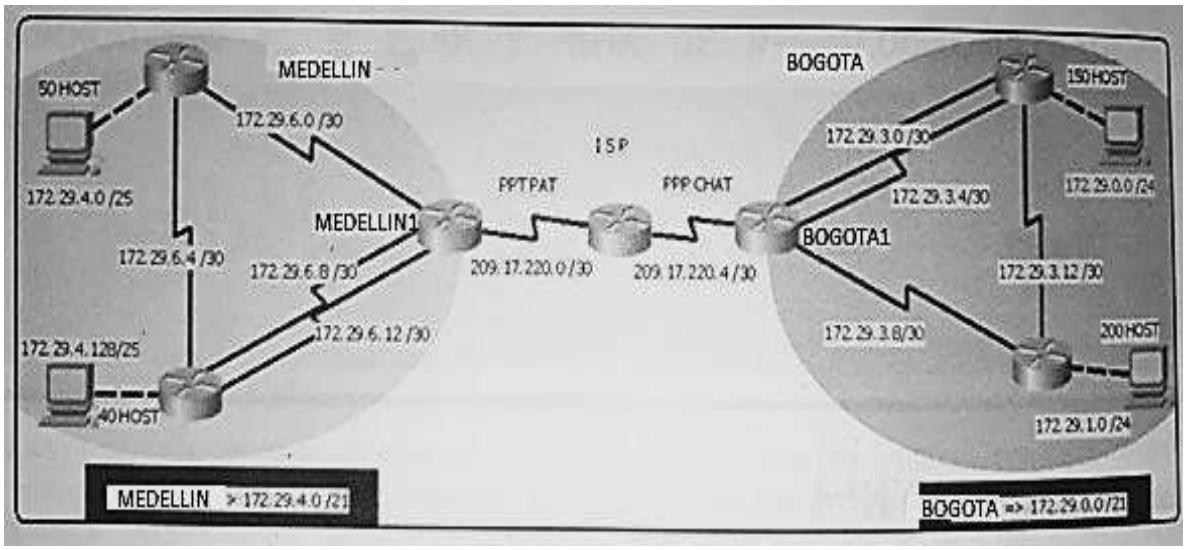


Figura 28 - Acceso de PC-C a Servidor Web

DESARROLLO ESCENARIO 2

ESCENARIO 2

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



Este escenario plantea el uso de OSPF como protocolo de enrutamiento, considerando que se 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.

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

Se debe habilitar NAT de sobrecarga en los routers Bogota1 y medellin1.

Parte 1: Configuración inicial de los equipos

Paso 1: Conexión física de los equipos

Lo primero que se realiza es realizar la conexión física de los equipos con base en la topología de red, de acuerdo como a como se muestra en la siguiente ilustración:

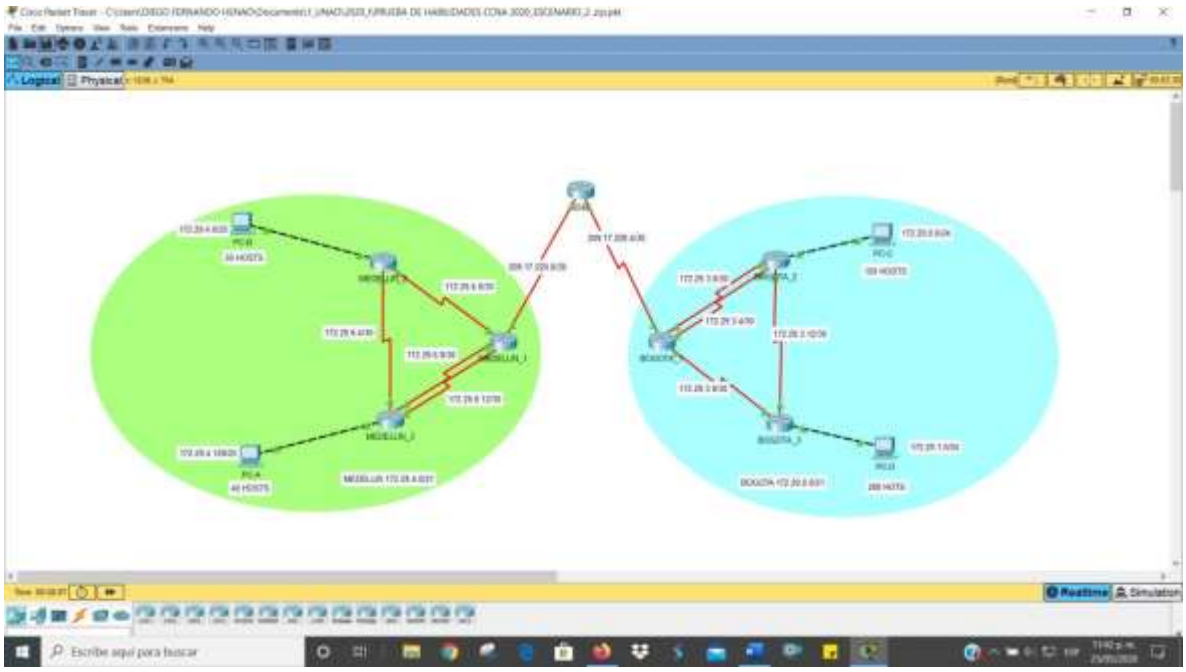


Figura 29 - Conexión Física de los Equipos

Paso 2: Configuración básica de los equipos:

Se procede a realizar las correspondientes rutinas de diagnóstico, para dejar los equipos listos para su configuración, como lo son inicializar y volver a cargar los routers.

Eliminación del archivo startup-config de todos los routers

Para la eliminación del archivo startup-config de los routers, damos click en cada router, vamos a la pestaña CLI y digitamos el comando *enable* y luego el comando *erase startup-config* y cuando aparezca *Continue*?, damos *Enter* y confirmamos *así:*

Routers MEDELLIN_1, MEDELLIN_2, MEDELLÍN_3, BOGOTÁ_1, BOGOTÁ_2, BOGOTÁ_3 E ISP

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

Volver a cargar todos los routers

Para el cargue nuevamente de los routers, seguido digitamos el comando *reload así:*

Routers Medellin_1, Medellin_2, Medellín_3, Bogotá_1, Bogotá_2, Bogotá_3 e ISP

Router#reload

Proceed with reload? [confirm]

Confirmamos e inmediatamente los routers se vuelven a cargar.

Paso 3: Configurar Routers Medellin_1, Medellin_2, Medellín_3, Bogotá_1, Bogotá_2, Bogotá_3 e ISP

En este paso se procede a configurar los parámetros básicos de cada uno de los routers

Configuración básica router ISP

Router>enable
Router#config t
Router(config)#no ip domain-lookup
Router(config)#hostname ISP
ISP(config)#enable secret class
ISP(config)#line console 0
ISP(config-line)#password cisco

ISP(config-line)#login
ISP(config-line)#line vty 0 4
ISP(config-line)#password cisco
ISP(config-line)#login
ISP(config-line)#exit
ISP(config)#service password-encryption
ISP(config)#banner motd #Se prohibe el acceso no autorizado#

Configuración básica router MEDELLIN_1

Router>enable
Router#config t
Router(config)#no ip domain-lookup
Router(config)#hostname MEDELLIN_1
MEDELLIN_1(config)#enable secret class
MEDELLIN_1(config)#line console 0
MEDELLIN_1(config-line)#password cisco
MEDELLIN_1(config-line)#login
MEDELLIN_1(config-line)#line vty 0 4
MEDELLIN_1(config-line)#password cisco
MEDELLIN_1(config-line)#login
MEDELLIN_1(config-line)#line vty 0 4
MEDELLIN_1(config-line)#password cisco
MEDELLIN_1(config-line)#login
MEDELLIN_1(config-line)#exit
MEDELLIN_1(config)#service password-encryption
MEDELLIN_1(config)#banner motd #Se prohibe el acceso no autorizado#

Configuración básica router MEDELLIN_2

Router>enable
Router#config t
Router(config)#no ip domain-lookup
Router(config)#hostname MEDELLIN_2
MEDELLIN_2(config)#enable secret class
MEDELLIN_2(config)#line console 0
MEDELLIN_2(config-line)#password cisco
MEDELLIN_2(config-line)#login
MEDELLIN_2(config-line)#line vty 0 4

MEDELLIN_2(config-line)#password cisco
MEDELLIN_2(config-line)#login
MEDELLIN_2(config-line)#exit
MEDELLIN_2(config)#service password-encryption
MEDELLIN_2(config)#banner motd #Se prohibe el acceso no autorizado#

Configuración básica router MEDELLIN_3

Router>enable
Router#config t
Router(config)#no ip domain-lookup
Router(config)#hostname MEDELLIN_3
MEDELLIN_3(config)#enable secret class
MEDELLIN_3(config)#line console 0
MEDELLIN_3(config-line)#password cisco
MEDELLIN_3(config-line)#login
MEDELLIN_3(config-line)#line vty 0 4
MEDELLIN_3(config-line)#password cisco
MEDELLIN_3(config-line)#login
MEDELLIN_3(config-line)#exit
MEDELLIN_3(config)#service password-encryption
MEDELLIN_3(config)#banner motd #Se prohibe el acceso no autorizado#

Configuración básica router BOGOTA_1

Router>enable
Router#config t
Router(config)#no ip domain-lookup
Router(config)#hostname BOGOTA_1
BOGOTA_1(config)#enable secret class
BOGOTA_1(config)#line console 0
BOGOTA_1(config-line)#password cisco
BOGOTA_1(config-line)#login
BOGOTA_1(config-line)#line vty 0 4
BOGOTA_1(config-line)#password cisco
BOGOTA_1(config-line)#login
BOGOTA_1(config-line)#exit
BOGOTA_1(config)#service password-encryption
BOGOTA_1(config)#banner motd #Se prohibe el acceso no autorizado#

Configuración básica router BOGOTA_2

Router>enable
Router#config t
Router(config)#no ip domain-lookup
Router(config)#hostname BOGOTA_2
BOGOTA_2(config)#enable secret class
BOGOTA_2(config)#line console 0
BOGOTA_2(config-line)#password cisco
BOGOTA_2(config-line)#login
BOGOTA_2(config-line)#line vty 0 4
BOGOTA_2(config-line)#password cisco
BOGOTA_2(config-line)#login
BOGOTA_2(config-line)#exit
BOGOTA_2(config)#service password-encryption
BOGOTA_2(config)#banner motd #Se prohibe el acceso no autorizado#

Configuración básica router BOGOTA_3

Router>enable
Router#config t
Router(config)#no ip domain-lookup
Router(config)#hostname BOGOTA_3
BOGOTA_3(config)#enable secret class
BOGOTA_3(config)#line console 0
BOGOTA_3(config-line)#password cisco
BOGOTA_3(config-line)#login
BOGOTA_3(config-line)#line vty 0 4
BOGOTA_3(config-line)#password cisco
BOGOTA_3(config-line)#login
BOGOTA_3(config-line)#exit
BOGOTA_3(config)#service password-encryption
BOGOTA_3(config)#banner motd #Se prohibe el acceso no autorizado#

Parte 2: Configuración del enrutamiento

Paso 1: Configuración Router ISP

Router>enable
Router#config t
Router(config)#hostname ISP

Configuración interfaz s0/0/0

ISP(config)#int s0/0/0
ISP(config-if)#description ISP_CONECTADO A MEDELLIN_1
ISP(config-if)#ip address 172.29.6.2 255.255.255.252
ISP(config-if)#clock rate 128000
ISP(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
ISP(config-if)#
ISP(config-if)#exit

Configuración interfaz s0/0/1

ISP(config)#int s0/0/1
ISP(config-if)#description ISP_CONECTADO A BOGOTA_1
ISP(config-if)#ip address.172.29.6.5 255.255.255.252
ISP(config-if)#clock rate 128000
ISP(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
ISP(config-if)#exit

Configuración del protocolo OSPFv2

ISP(config)#router ospf 1
ISP(config-router)#network 209.17.220.0 0.0.0.255 area 0
ISP(config-router)#network 172.29.6.4 0.0.0.3 area 0
ISP(config-router)# network 172.29.6.0 0.0.0.3 area 0
ISP(config-router)# network 172.29.4.0 0.0.0.127 area 0
ISP(config-router)# network 172.29.3.12 0.0.0.3 area 0
ISP(config-router)# network 172.29.3.8 0.0.0.3 area 0
ISP(config-router)# network 172.29.0.0 0.0.0.127 area 0
ISP(config-router)# network 172.29.4.0 0.0.0.3 area 0

Paso 2: Configuración Router MEDELLIN_1

Router>enable
Router#config t
Router(config)#hostname MEDELLIN_1

Configuración interfaz s0/0/0
MEDELLIN_1(config)#int s0/0/0
MEDELLIN_1(config-if)#description CONECTADO A ISP
MEDELLIN_1(config-if)#ip address 209.17.220.2 255.255.255.252
MEDELLIN_1(config-if)#clock rate 128000
MEDELLIN_1(config-if)#shutdown
MEDELLIN_1(config-if)#exit

Configuración interfaz s0/0/1

MEDELLIN_1(config)#int s0/0/1
MEDELLIN_1(config-if)#description CONECTADO A MEDELLIN_3
MEDELLIN_1(config-if)#ip address 172.29.6.13 255.255.255.252
MEDELLIN_1(config-if)#clock rate 128000
MEDELLIN_1(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
MEDELLIN_1(config-if)#exit

Configuración interfaz s0/1/0

MEDELLIN_1(config)#int s0/1/0
MEDELLIN_1(config-if)#description CONECTADO A MEDELLIN_3
MEDELLIN_1(config-if)#ip address 172.29.6.9 255.255.255.252
MEDELLIN_1(config-if)#clock rate 128000
MEDELLIN_1(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/1/0, changed state to down
MEDELLIN_1(config-if)#exit

Configuración interfaz s0/1/1

MEDELLIN_1(config)#int s0/1/1
MEDELLIN_1(config-if)#description CONECTADO A MEDELLIN_2
MEDELLIN_1(config-if)#ip address 172.29.6.1 255.255.255.252
MEDELLIN_1(config-if)#clock rate 128000

MEDELLIN_1(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/1/1, changed state to down
MEDELLIN_1(config-if)#exit

Configuración del protocolo OSPFv2

MEDELLIN_1(config)#router ospf 1
MEDELLIN_1(config-router)#network 172.29.6.4 0.0.0.3 area 0
MEDELLIN_1(config-router)#network 172.29.6.0 0.0.0.3 area 0
MEDELLIN_1(config-router)#network 172.29.4.0 0.0.0.3 area 0
MEDELLIN_1(config-router)#network 172.29.4.128 0.0.0.3 area 0

MEDELLIN_1(config)#router ospf 2
MEDELLIN_1(config-router)#network 172.29.6.0 0.0.0.255 area 1

Paso 3: Configuración Router MEDELLIN_2

Router>enable
Router#config t
Router(config)#hostname MEDELLIN_2

Configuración interfaz s0/0/0

MEDELLIN_2(config)#int s0/0/0
MEDELLIN_2(config-if)#description CONECTADO A MEDELLIN_1
MEDELLIN_2(config-if)#ip address 172.29.6.2 255.255.255.252
MEDELLIN_2(config-if)#clock rate 128000
MEDELLIN_2(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
MEDELLIN_2(config-if)#exit

Configuración interfaz s0/0/1

MEDELLIN_2(config)#int s0/0/1
MEDELLIN_2(config-if)#description CONECTADO A MEDELLIN_3

MEDELLIN_2(config-if)#ip address 172.29.6.5 255.255.255.252
MEDELLIN_2(config-if)#clock rate 128000
MEDELLIN_2(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
MEDELLIN_2(config-if)#exit

Configuración interfaz g0/0

MEDELLIN_2(config)#int g0/0
MEDELLIN_2(config-if)#description CONECTADO A PC-B
MEDELLIN_2(config-if)#ip address 172.29.4.1 255.255.255.128
MEDELLIN_2(config-if)#no shutdown
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
MEDELLIN_2(config-if)#exit

Configuración del protocolo OSPFv2

MEDELLIN_2(config)#router ospf 1
MEDELLIN_2(config-router)#network 172.29.6.4 0.0.0.3 area 0
MEDELLIN_2(config-router)#network 172.29.6.0 0.0.0.3 area 0
MEDELLIN_2(config-router)#network 172.29.4.0 0.0.0.127 area 0
MEDELLIN_2(config-router)#network 172.29.4.128 0.0.0.127 area 0
MEDELLIN_2(config-router)#network 172.29.6.8 0.0.0.3 area 0
MEDELLIN_2(config-router)#network 172.29.6.12 0.0.0.3 area 0

Paso 4: Configuración Router MEDELLIN_3

Router>enable
Router#config t
Router(config)#hostname MEDELLIN_3

Configuración interfaz s0/0/0

MEDELLIN_3(config)#int s0/0/0
MEDELLIN_3(config-if)#description CONECATADO A MEDELLIN_2

MEDELLIN_3(config-if)#ip address 172.29.6.6 255.255.255.252
MEDELLIN_3(config-if)#clock rate 128000
MEDELLIN_3(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
MEDELLIN_3(config-if)#exit

Configuración interfaz s0/0/1

MEDELLIN_3(config)#int s0/0/1
MEDELLIN_3(config-if)#description CONECTADO A MEDELLIN_1
MEDELLIN_3(config-if)#ip address 172.29.6.10 255.255.255.252
MEDELLIN_3(config-if)#clock rate 128000
MEDELLIN_3(config-if)#no shutdown
%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
MEDELLIN_3(config-if)#exit

Configuración interfaz s0/1/0
MEDELLIN_3(config)#int s0/1/0
MEDELLIN_3(config-if)#description CONECTADO A MEDELLIN_1
MEDELLIN_3(config-if)#ip address 172.29.6.14 255.255.255.252
MEDELLIN_3(config-if)#clock rate 128000
MEDELLIN_3(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/1/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed state to up
MEDELLIN_3(config-if)#exit
Configuración interfaz g0/0

MEDELLIN_3(config)#int g0/0
MEDELLIN_3(config-if)#description CONECTADO A PC-A
MEDELLIN_3(config-if)#ip address 172.29.4.129 255.255.255.128
MEDELLIN_3(config-if)#no shutdown
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
MEDELLIN_3(config-if)#exit

Configuración del protocolo OSPFv2

MEDELLIN_3(config)#router ospf 1
MEDELLIN_3(config-router)#network 172.29.6.4 0.0.0.3 area 0
MEDELLIN_3(config-router)#network 172.29.6.0 0.0.0.3 area 0
MEDELLIN_3(config-router)#network 172.29.4.0 0.0.0.127 area 0
MEDELLIN_3(config-router)#network 172.29.0.0 0.0.255.255 area 1

Paso 5: Configuración Router BOGOTA_1

Router>enable
Router#config t
Router(config)#hostname BOGOTA_1

Configuración interfaz s0/0/0

BOGOTA_1(config)#int s0/0/0
BOGOTA_1(config-if)#description CONECTADO A ISP
BOGOTA_1(config-if)#ip address 209.17.220.6 255.255.255.252
BOGOTA_1(config-if)#clock rate 128000
BOGOTA_1(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
BOGOTA_1(config-if)#exit

Configuración interfaz s0/0/1

BOGOTA_1(config)#int s0/0/1
BOGOTA_1(config-if)#description CONECTADO A BOGOTA_2
BOGOTA_1(config-if)#ip address 172.29.3.1 255.255.255.252
BOGOTA_1(config-if)#clock rate 128000
BOGOTA_1(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
BOGOTA_1(config-if)#exit

Configuración interfaz s0/1/0

BOGOTA_1(config)#int s0/1/0
BOGOTA_1(config-if)#description CONECTADO A BOGOTA_2
BOGOTA_1(config-if)#ip address 172.29.3.5 255.255.255.252
BOGOTA_1(config-if)#clock rate 128000
BOGOTA_1(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/1/0, changed state to down
BOGOTA_1(config-if)#exit

BOGOTA_1(config)#int s0/1/1
BOGOTA_1(config-if)#description CONECTADO A BOGOTA_3
BOGOTA_1(config-if)#ip address 172.29.3.9 255.255.255.252
BOGOTA_1(config-if)#clock rate 128000
BOGOTA_1(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
BOGOTA_1(config-if)#exit

Configuración del protocolo OSPFv2

BOGOTA_1(config)#router ospf 1
BOGOTA_1(config-router)#network 172.29.3.12 0.0.0.3 area 0
BOGOTA_1(config-router)#network 172.29.3.8 0.0.0.3 area 0
BOGOTA_1(config-router)#network 172.29.0.0 0.0.0.127 area 0
BOGOTA_1(config-router)#network 172.29.3.0 0.0.0.255 area 0
BOGOTA_1(config-router)#
08:08:55: %OSPF-5-ADJCHG: Process 1, Nbr 209.17.220.5 on Serial0/0/0 from LOADING to FULL, Loading Done

Paso 6: Configuración Router BOGOTA_2

Router>enable
Router#config t
Router(config)#hostname BOGOTA_2
Configuración interfaz s0/0/0

BOGOTA_2(config)#int s0/0/0
BOGOTA_2(config-if)#description CONECTADO A BOGOTA_1
BOGOTA_2(config-if)#ip address 172.29.3.2 255.255.255.252
BOGOTA_2(config-if)#clock rate 128000

BOGOTA_2(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
BOGOTA_2(config-if)#exit

Configuración interfaz s0/0/0

BOGOTA_2(config)#int s0/0/0
BOGOTA_2(config-if)#description CONECTADO A BOGOTA_1
BOGOTA_2(config-if)#ip address 172.29.3.2 255.255.255.252
BOGOTA_2(config-if)#clock rate 128000
BOGOTA_2(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up
BOGOTA_2(config)#exit

Configuración interfaz s0/0/1

BOGOTA_2(config)#int s0/0/1
BOGOTA_2(config-if)#description CONECTADO A BOGOTA_1
BOGOTA_2(config-if)#ip address 172.29.3.6 255.255.255.252
BOGOTA_2(config-if)#clock rate 128000
BOGOTA_2(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up
exit
BOGOTA_2(config)#exit
Configuración interfaz s0/1/0

BOGOTA_2(config)#int s0/1/0
BOGOTA_2(config-if)#description CONECTADO A BOGOTA_3
BOGOTA_2(config-if)#ip address 172.29.3.13 255.255.255.252
BOGOTA_2(config-if)#clock rate 128000
BOGOTA_2(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/1/0, changed state to down
BOGOTA_2(config-if)#exit

Configuración interfaz g0/0

BOGOTA_2(config)#int g0/0

BOGOTA_2(config-if)#description CONECTADO A BOGOTA PC-C
BOGOTA_2(config-if)#ip address 172.29.0.1 255.255.255.0
BOGOTA_2(config-if)#no shutdown
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
BOGOTA_2(config-if)#exit

Configuración del protocolo OSPFv2

BOGOTA_2(config)#router ospf 1
BOGOTA_2(config-router)#network 172.29.3.12 0.0.0.3 area 0
BOGOTA_2(config-router)#network 172.29.3.8 0.0.0.3 area 0
BOGOTA_2(config-router)#network 172.29.0.0 0.0.0.127 area 0
BOGOTA_2(config-router)#network 172.29.1.0 0.0.0.127 area 0

Paso 7: Configuración Router BOGOTA_3

Router>enable
Router#config t
Router(config)#hostname BOGOTA_3

Configuración interfaz s0/0/0

BOGOTA_3(config)#int s0/0/0
BOGOTA_3(config-if)#description CONECTADO CON BOGOTA_1
BOGOTA_3(config-if)#ip address 172.29.3.10 255.255.255.252
BOGOTA_3(config-if)#clock rate 128000
BOGOTA_3(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
BOGOTA_3(config-if)#exit

Configuración interfaz s0/0/1

BOGOTA_3(config)#int s0/0/1
BOGOTA_3(config-if)#description CONECTADO CON BOGOTA_2
BOGOTA_3(config-if)#ip address 172.29.3.14 255.255.255.252
BOGOTA_3(config-if)#clock rate 128000
BOGOTA_3(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up
BOGOTA_3(config-if)#exit

Configuración interfaz g0/0

BOGOTA_3(config)#int g0/0
BOGOTA_3(config-if)#description CONECTADO A PC-D
BOGOTA_3(config-if)#ip address 172.29.1.2 255.255.255.0
BOGOTA_3(config-if)#no shutdown
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
BOGOTA_3(config-if)#exit

Configuración del protocolo OSPFv2

BOGOTA_3(config)#router ospf 1
BOGOTA_3(config-router)#network 172.29.0.0 0.0.0.3 area 0

Configuración ruta estática en ISP

ISP>enable
ISP#config t
Enter configuration commands, one per line. End with CNTL/Z.
ISP(config)#ip route 172.29.4.0 255.255.252.0 s0/0/0
ISP(config)#ip route 172.29.0.0 255.255.252.0 s0/0/1
ISP(config)#ip route 172.29.1.0 255.255.255.0 s0/0/1
ISP(config)#ip route 172.29.4.128 255.255.255.128 s0/0/0
ISP(config)#exit

Configuración para la ruta estática predeterminada hacia la red de MEDELLIN:

MEDELLIN_1>enable
MEDELLIN_1#config t
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN_1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.1
MEDELLIN_1(config)#exit

Se realiza un ping en la red MEDELLIN desde PC-A a PC-B

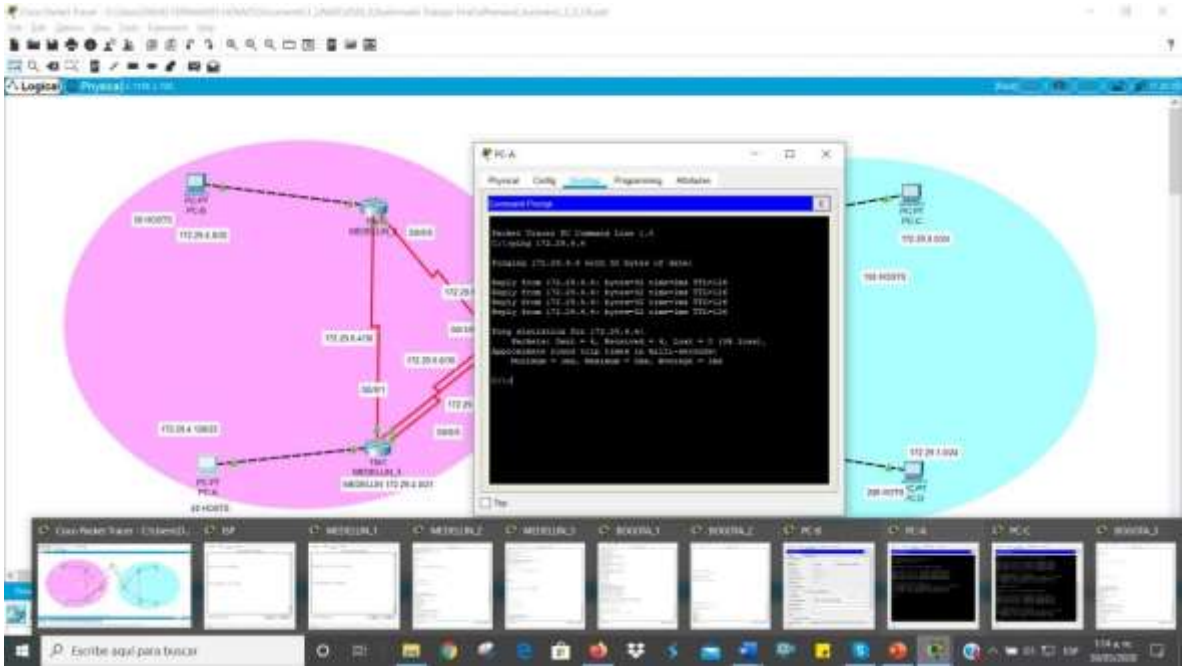


Figura 30 - ping en la red MEDELLIN desde PC-A a PC-B

Configuración para la ruta estática predeterminada hacia la red de BOGOTA:

BOGOTA_1>enable
BOGOTA_1#config t
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA_1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.5
BOGOTA_1(config)#exit

Se realiza un ping en la red BOGOTA desde PC-C a PC-D

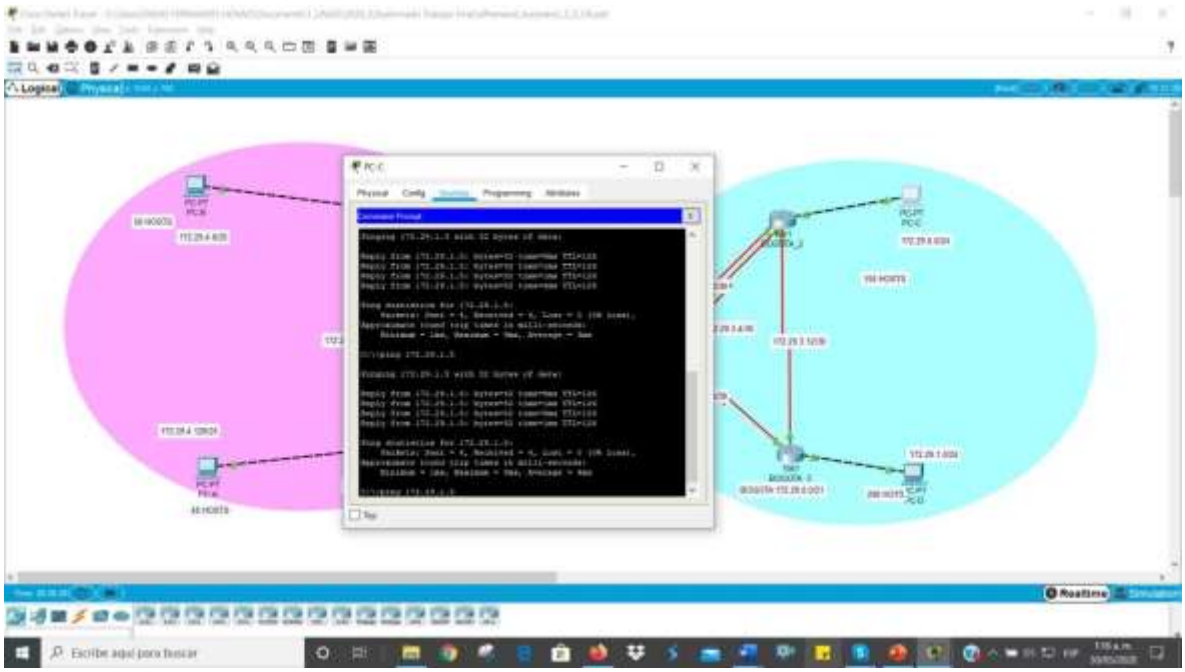


Figura 31 - ping en la red BOGOTA desde PC-C a PC-D

Parte 3: Deshabilitar la propagación del protocolo OSPF

Router MEDELLIN_1

MEDELLIN_1>enable
MEDELLIN_1#config t
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN_1(config)#router ospf 1
MEDELLIN_1(config-router)#passive-interface s0/0/1

Router MEDELLIN_2

MEDELLIN_2>enable
MEDELLIN_2#config t
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN_2(config)#router ospf 1
MEDELLIN_2(config-router)#passive-interface g0/0

Router MEDELLIN_3

MEDELLIN_3>enable
MEDELLIN_3#config t
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN_3(config)#router ospf 1
MEDELLIN_3(config-router)#passive-interface g0/0
MEDELLIN_3(config-router)#passive-interface s0/1/1

Router BOGOTA_1

BOGOTA_1>enable
BOGOTA_1#config t
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA_1(config)#router ospf 1
BOGOTA_1(config-router)#passive-interface s0/0/0

Router BOGOTA_2

BOGOTA_2>enable
BOGOTA_2#config t
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA_2(config)#router ospf 1
BOGOTA_2(config-router)#passive-interface g0/0
BOGOTA_2(config-router)#passive-interface s0/1/1

Router BOGOTA_3

BOGOTA_3>enable
BOGOTA_3#config t
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA_3(config)#router ospf 1
BOGOTA_3(config-router)#passive-interface g0/0

Parte 4: Verificación del protocolo OSPFv2

Router MEDELLIN_1

MEDELLIN_1>enable
MEDELLIN_1#show run

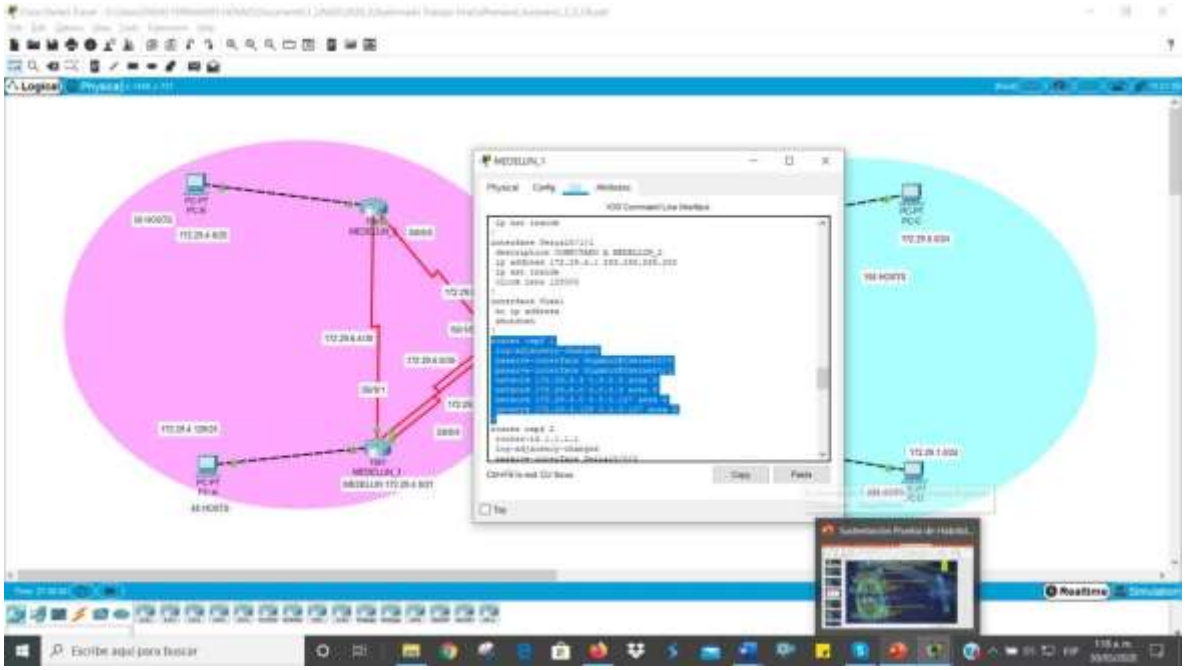


Figura 32 - Verificación del protocolo OSPFv2 en MEDELLIN_1

Router MEDELLIN_2

MEDELLIN_2>enable
MEDELLIN_2#show run

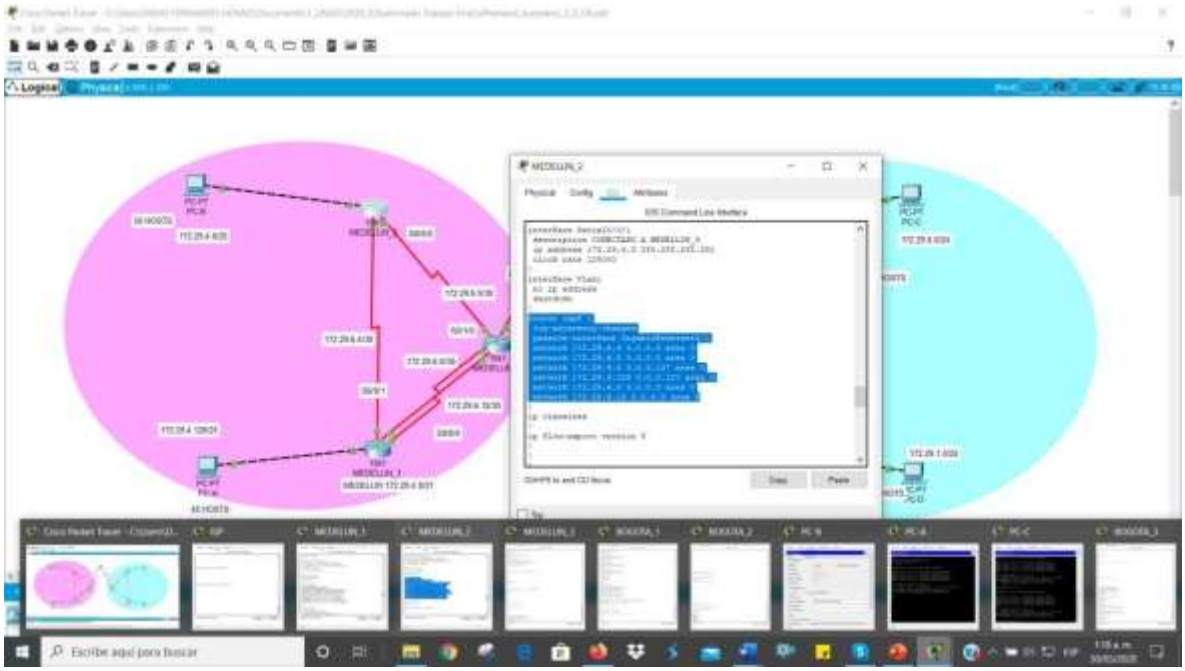


Figura 33 - Verificación del protocolo OSPFv2 en MEDELLIN_2

Router MEDELLIN_3

MEDELLIN_3>enable
MEDELLIN_3#show run

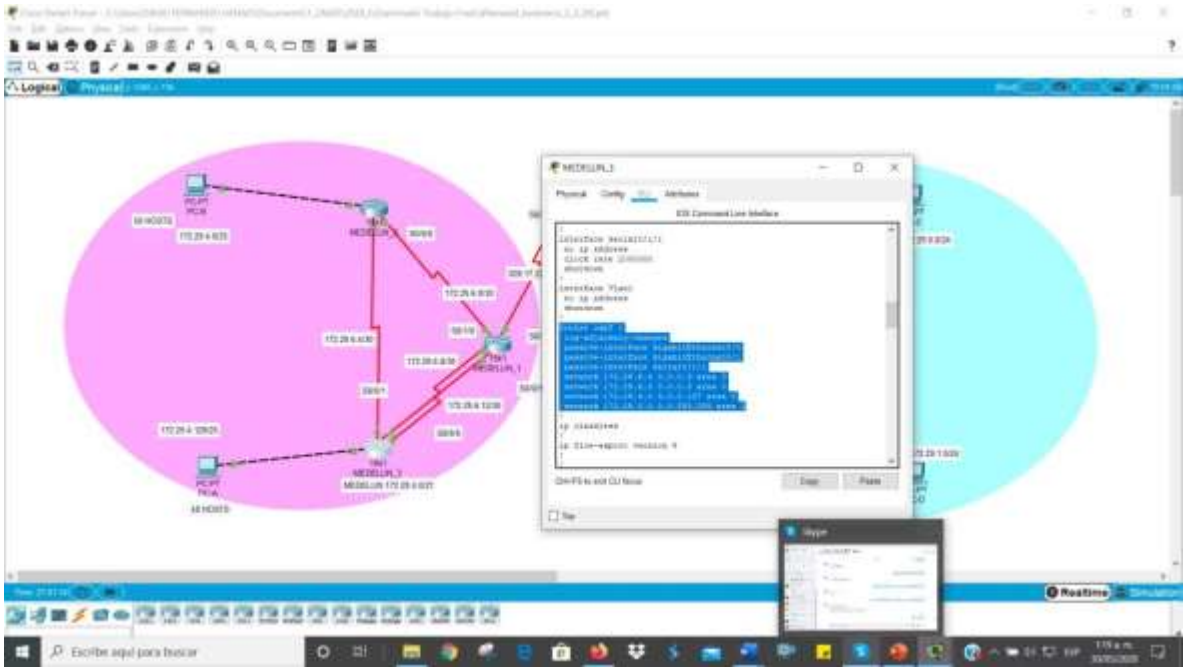


Figura 34 - Verificación del protocolo OSPFv2 en MEDELLIN_3

Router BOGOTA_1

BOGOTA_1>enable
BOGOTA_1#show run

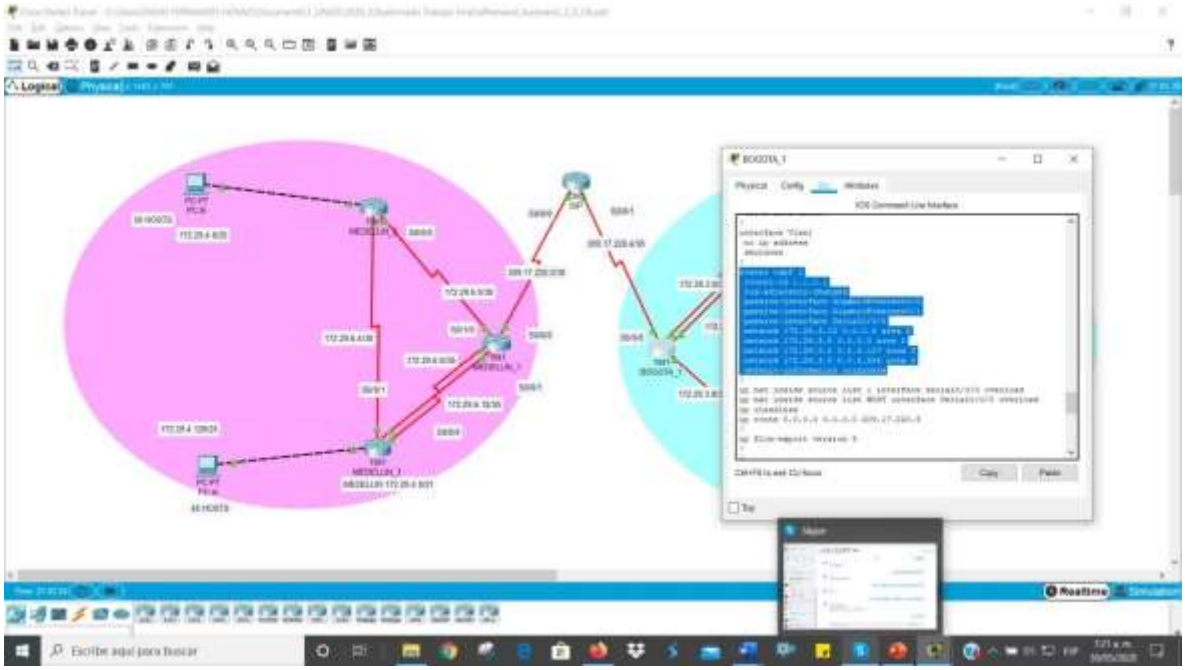


Figura 35 - Verificación del protocolo OSPFv2 en BOGOTA_1

Router BOGOTA_2

BOGOTA_2>enable
BOGOTA_2#show run

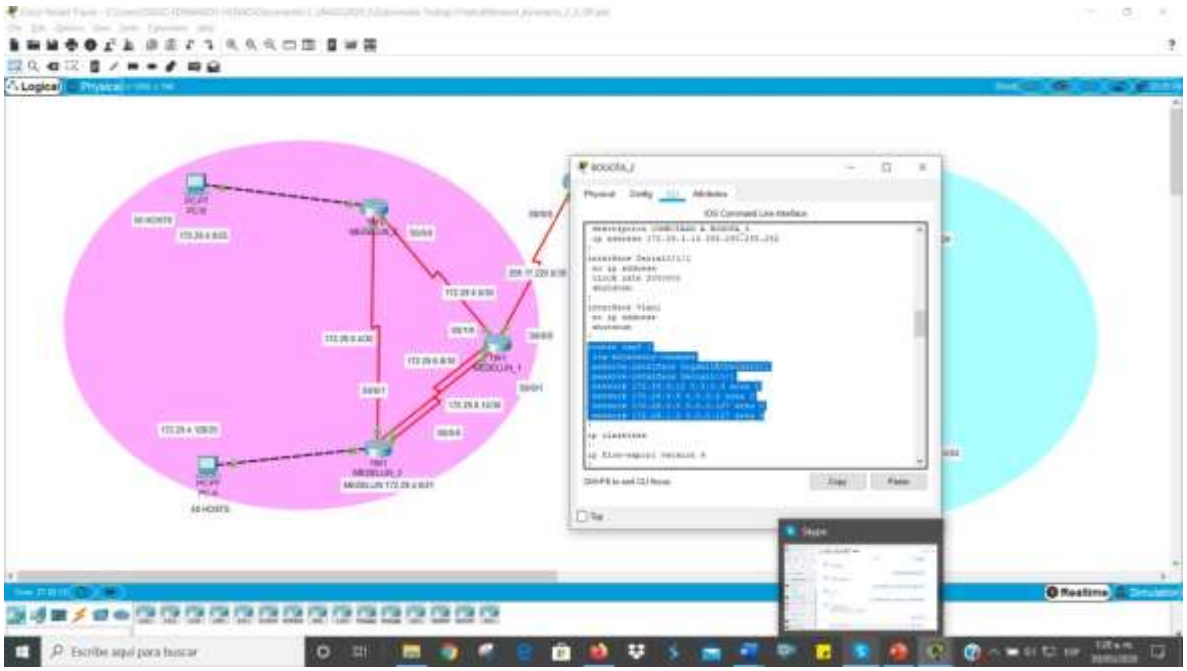


Figura 36 -Verificación del protocolo OSPFv2 en BOGOTA_2

Router BOGOTA_3

BOGOTA_3>enable
BOGOTA_3#show run

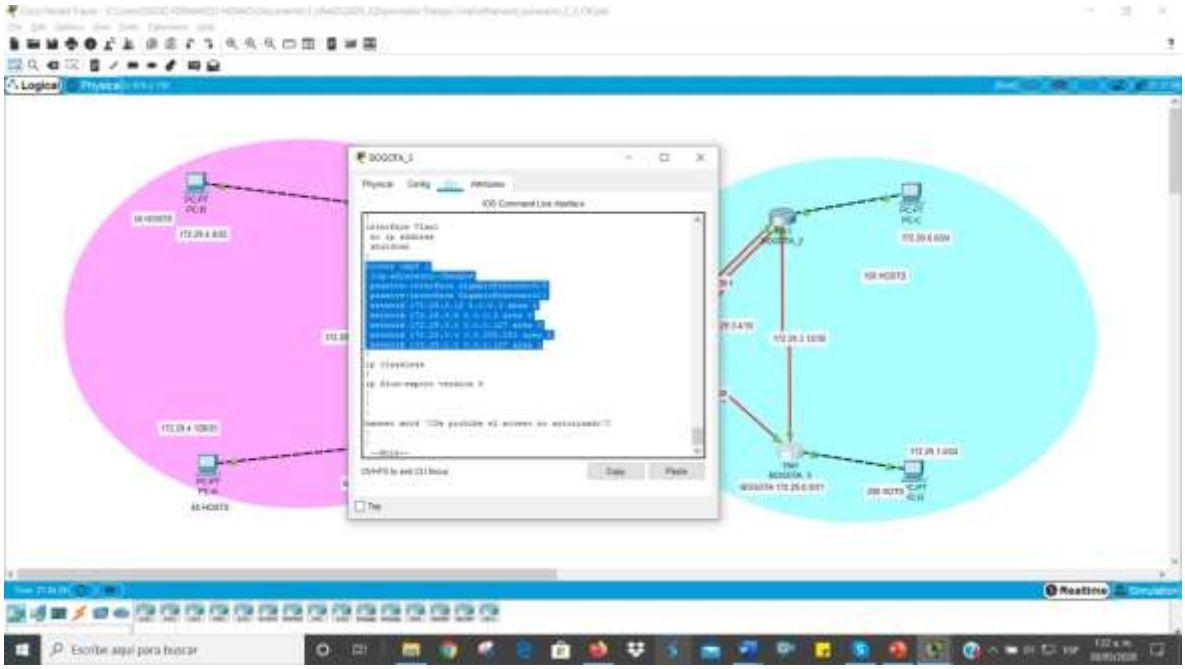


Figura 37 - Verificación del protocolo OSPFv2 en BOGOTA_3

Parte 5: Configuración del encapsulamiento y autenticación PPP

A continuación se muestra el procedimiento para realizar la configuración de los routers ISP, MEDELLIN_1 y BOGOTÁ_1, para estos puedan usar en determinadas interfaces el método de encapsulación PPP, para luego proceder a realizar el proceso de autenticación PAP en MEDELLIN_1 y CHAP en BOGOTA_1 y para lo cual realizaremos lo siguiente:

Proceso de habilitación método de encapsulamiento PPP:

Router MEDELLIN_1

MEDELLIN_1>enable
MEDELLIN_1#config t
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN_1(config)#int s0/0/0
MEDELLIN_1(config-if)#encapsulation PPP
MEDELLIN_1(config-if)#

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to down
18:57:39: %OSPF-5-ADJCHG: Process 1, Nbr 209.17.220.5 on Serial0/0/0 from FULL to DOWN, Neighbor Down: Interface down or detached
MEDELLIN_1(config-if)#no shutdown
MEDELLIN_1(config-if)#exit

Router BOGOTA_1

BOGOTA_1>enable
BOGOTA_1#config t
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA_1(config)#int s0/0/0
BOGOTA_1(config-if)#encapsulation PPP
BOGOTA_1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to down

BOGOTA_1(config-if)#no shutdown
BOGOTA_1(config-if)#exit

Router ISP

ISP(config)#int s0/0/0
ISP(config-if)#encapsulation PPP
ISP(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

ISP(config-if)#no shutdown
ISP(config-if)#exit
ISP(config)#
19:27:52: %OSPF-5-ADJCHG: Process 1, Nbr 209.17.220.2 on Serial0/0/0 from LOADING to FULL, Loading Done

ISP(config)#int s0/0/1
ISP(config-if)#encapsulation PPP
ISP(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up

ISP(config-if)#no shutdown
ISP(config-if)#exit

Proceso de autenticación PAP de PPP entre los routers MEDELLIN_1 y el Router ISP

Configuración PAP de PPP en ISP con MEDELLIN_1

ISP#config t
Enter configuration commands, one per line. End with CNTL/Z.
ISP(config)#username MEDELLIN_1 secret MEDELLIN
ISP(config)#int s0/0/0
ISP(config-if)#PPP authentication PAP
ISP(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to down
19:34:50: %OSPF-5-ADJCHG: Process 1, Nbr 209.17.220.2 on Serial0/0/0 from FULL to DOWN, Neighbor Down: Interface down or detached

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

Configuración PAP de PPP en MEDELLIN_1 con ISP

MEDELLIN_1>enable
MEDELLIN_1#config t
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN_1(config)#username ISP secret ISP
MEDELLIN_1(config)#int s0/0/0
MEDELLIN_1(config-if)#PPP authentication PAP
MEDELLIN_1(config-if)#PPP PAP sent-username MEDELLIN_1 password MEDELLIN
MEDELLIN_1(config-if)#exit

Configuración CHAP de PPP en ISP con BOGOTA_1

ISP>enable
ISP#config t
ISP(config)#username BOGOTA_1 secret BOGOTA

ISP(config)#int s0/0/1
ISP(config-if)#PPP authentication CHAP
ISP(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to down
ISP(config-if)#exit

Configuración CHAP de PPP en BOGOTA_1 con ISP

BOGOTA_1>enable
BOGOTA_1#config t
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA_1(config)#username ISP secret BOGOTA
BOGOTA_1(config)#int s0/0/0
BOGOTA_1(config-if)#PPP authentication CHAP
BOGOTA_1(config-if)#exit

A continuación procedemos a realizar ping al router ISP, para verificar la autenticación por PAP en el router MEDELLIN_1

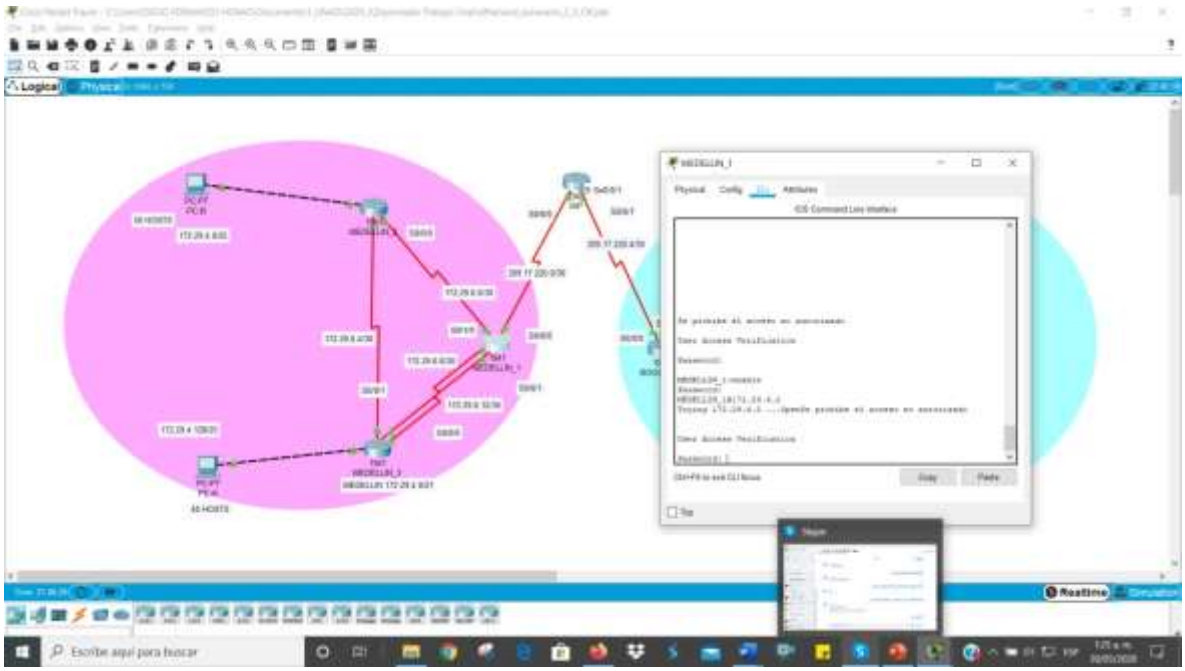


Figura 38 - Ping al Router ISP desde MEDELLIN_1

Ahora se procede a realizar ping al router ISP, para verificar la autenticación por CHAP en el router BOGOTA_1

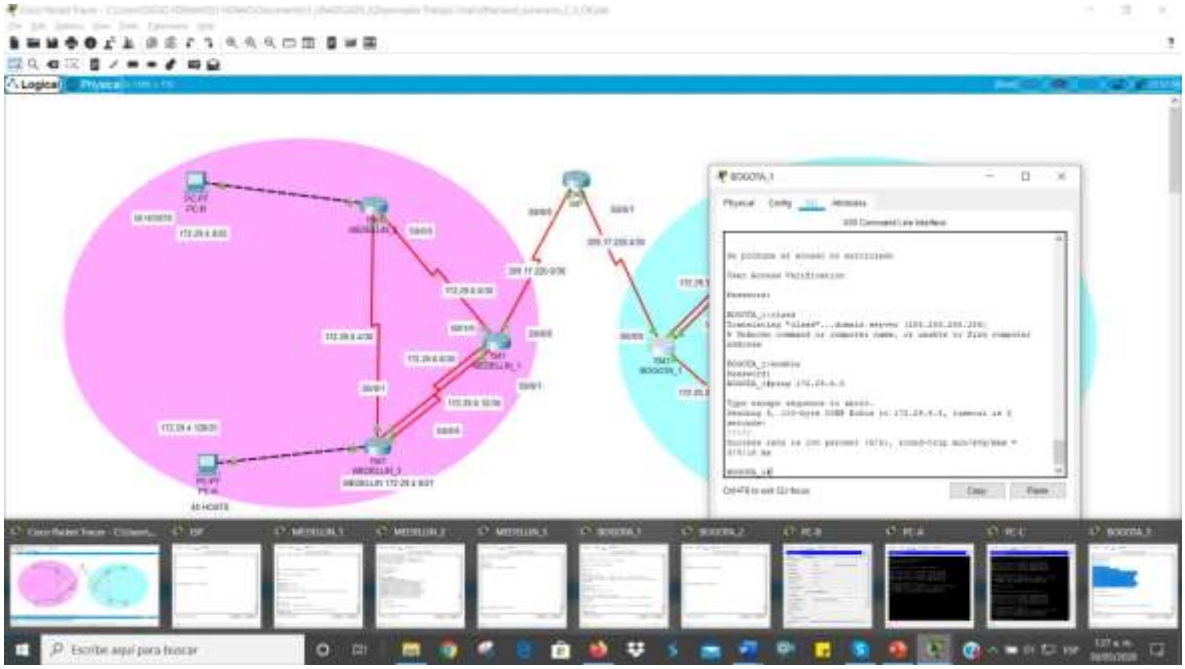


Figura 39 - Ping al Router ISP desde BOGOTA_1

Parte 6: Configuración de NAT

Paso 1: Configuración NAT en MEDELLIN_1

MEDELLIN_1>enable
MEDELLIN_1#config t
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN_1(config)#ip access-list standard HOST
MEDELLIN_1(config-std-nacl)#permit 172.29.4.0 0.0.0.255
MEDELLIN_1(config-std-nacl)#exit
MEDELLIN_1(config)#
MEDELLIN_1(config)#ip nat inside source list HOST interface s0/0/0 overload
MEDELLIN_1(config)#int s0/0/0
MEDELLIN_1(config-if)#ip nat outside
MEDELLIN_1(config-if)#exit
MEDELLIN_1(config)#int s0/0/1
MEDELLIN_1(config-if)#ip nat inside
MEDELLIN_1(config-if)#exit
MEDELLIN_1(config)#int s0/1/0
MEDELLIN_1(config-if)#ip nat inside
MEDELLIN_1(config-if)#int s0/1/1

MEDELLIN_1(config-if)#ip nat inside
MEDELLIN_1(config-if)#exit
%SYS-5-CONFIG_I: Configured from console by console
MEDELLIN_1#show ip nat translation

Paso 2: Configuración NAT en BOGOTA_1

BOGOTA_1>enable
BOGOTA_1#config t
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA_1(config)#ip access-list standard HOST
BOGOTA_1(config-std-nacl)#permit 172.29.0.0 0.0.0.255
BOGOTA_1(config-std-nacl)#exit
BOGOTA_1(config)#ip nat inside source list HOST interface s0/0/0 overload
BOGOTA_1(config)#int s0/0/0
BOGOTA_1(config-if)#ip nat outside
BOGOTA_1(config-if)#exit
BOGOTA_1(config)#int s0/0/1
BOGOTA_1(config-if)#ip nat inside
BOGOTA_1(config-if)#exit
BOGOTA_1(config)#int s0/1/0
BOGOTA_1(config-if)#ip nat inside
BOGOTA_1(config-if)#exit
BOGOTA_1(config)#int s0/1/1
BOGOTA_1(config-if)#ip nat inside
BOGOTA_1(config-if)#exit
BOGOTA_1(config)#exit
BOGOTA_1#
%SYS-5-CONFIG_I: Configured from console by console
BOGOTA_1#show ip nat translation

Paso 3: Verificación ping entre MEDELLIN_2 y MEDELLIN_1

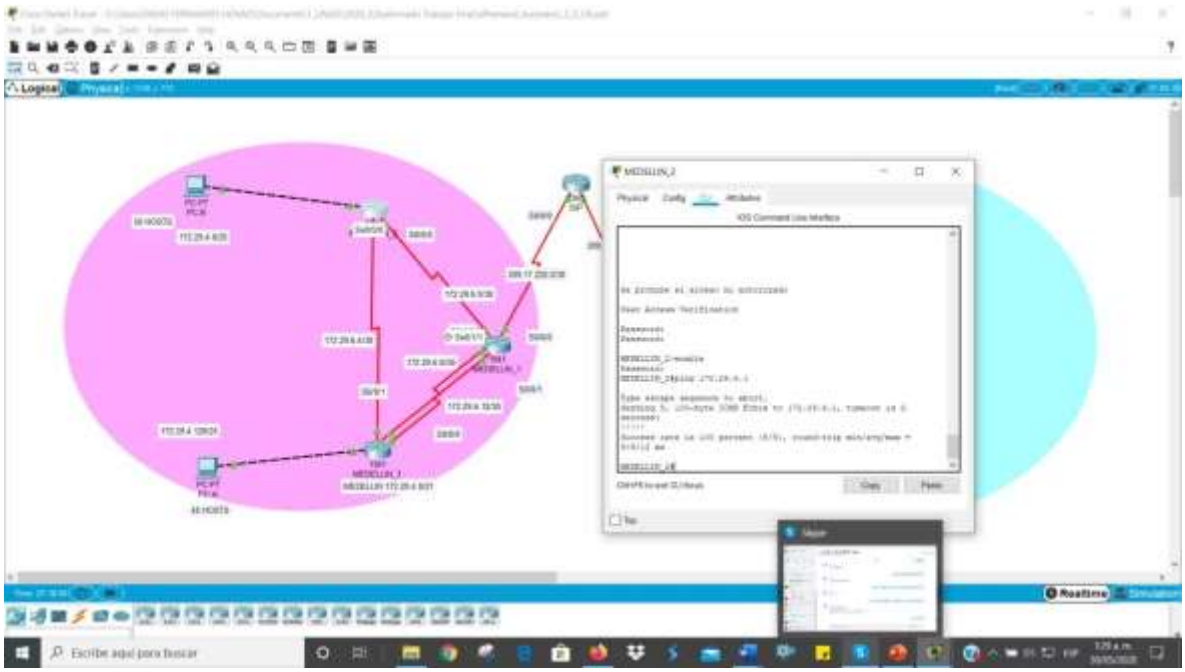


Figura 40 - ping entre MEDELLIN_2 y MEDELLIN_1

Parte 7: configuración del servicio DHCP

Paso 1: Configuración del servicio DHCP en el router MEDELLIN_2

```
MEDELLIN_2>enable
MEDELLIN_2#config t
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN_2(config)#
MEDELLIN_2(config)#ip dhcp excluded-address 172.29.4.1 172.29.4.3
MEDELLIN_2(config)#ip dhcp excluded-address 172.29.4.129 172.29.4.132
MEDELLIN_2(config)#ip dhcp pool MEDELLIN_2
MEDELLIN_2(dhcp-config)#network 172.29.4.0 255.255.255.128
MEDELLIN_2(dhcp-config)#default-router 172.29.4.1
MEDELLIN_2(dhcp-config)#dns-server 8.8.4.4
MEDELLIN_2(dhcp-config)#exit
MEDELLIN_2(config)#ip dhcp pool MEDELLIN_3
MEDELLIN_2(dhcp-config)#network 172.29.4.128 255.255.255.128
MEDELLIN_2(dhcp-config)#default-router 172.29.4.129
MEDELLIN_2(dhcp-config)#dns-server 8.8.4.4
MEDELLIN_2(dhcp-config)#exit
```

Continuando con la configuración del DHCP, se debe tener en cuenta que el router MEDELLIN_3 posee una red LAN conectada pero dicha red no realizar las veces

de servidor DHCP, por lo que se hace necesario configurar “ip helper” permitiendo así que sea un router de tránsito para llegar al router ejerciendo el roll de DHCP, debido a esto se debe utilizar el comando ip helper-address para atrapar los broadcasts y redireccionarlos hacia la ip del router de MEDELLIN_2 así:

MEDELLIN_3>enable
MEDELLIN_3#config t
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN_3(config)#int g0/0
MEDELLIN_3(config-if)#ip helper-address 172.29.6.5
MEDELLIN_3(config-if)#exit

Paso 2: Configuración del servicio DHCP en el router BOGOTA_2

BOGOTA_2>enable
BOGOTA_2#config t
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA_2(config)#ip dhcp excluded-address 172.29.0.1 172.29.0.4
BOGOTA_2(config)#ip dhcp excluded-address 172.29.1.1 172.29.1.4
BOGOTA_2(config)#ip dhcp pool BOGOTA_2
BOGOTA_2(dhcp-config)#network 172.29.1.0 255.255.255.0
BOGOTA_2(dhcp-config)#default-router 172.29.1.1
BOGOTA_2(dhcp-config)#dns-server 8.8.4.4
BOGOTA_2(dhcp-config)#exit
BOGOTA_2(config)#ip dhcp pool BOGOTA
BOGOTA_2(dhcp-config)#network 172.29.0.0 255.255.255.0
BOGOTA_2(dhcp-config)#default-router 172.29.0.1
BOGOTA_2(dhcp-config)#dns-server 8.8.4.4
BOGOTA_2(dhcp-config)#exit

Continuando con la configuración del DHCP, se debe tener en cuenta que el router BOGOTA_3 posee una red LAN conectada pero dicha red no realizar las veces de servidor DHCP, por lo que se hace necesario configurar “ip helper” permitiendo así que sea un router de tránsito para llegar al router ejerciendo el roll de DHCP, debido a esto se debe utilizar el comando ip helper-address para atrapar los broadcasts y redireccionarlos hacia la ip del router de BOGOTA_2 así:

BOGOTA_3>enable
BOGOTA_3#config t
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA_3(config)#int g0/0
BOGOTA_3(config-if)#ip helper-address 172.29.3.13
BOGOTA_3(config-if)#exit

BOGOTA_3(config)#

Aquí se puede evidenciar que

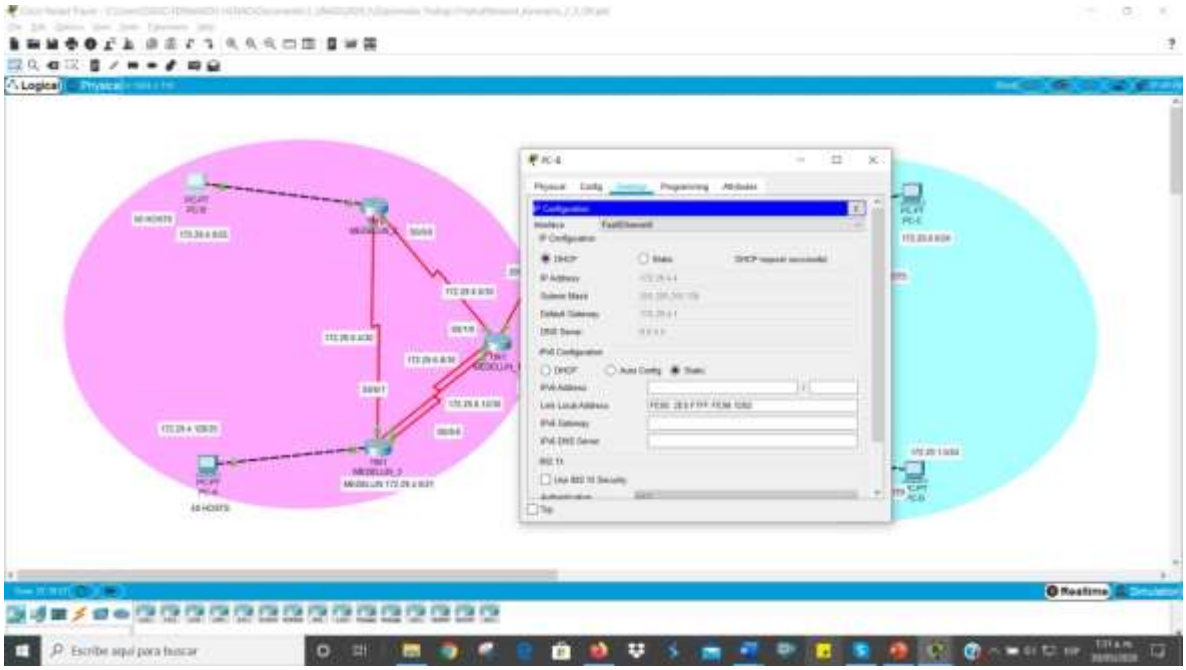


Figura 41 - Verificación DHCP en el PC-B

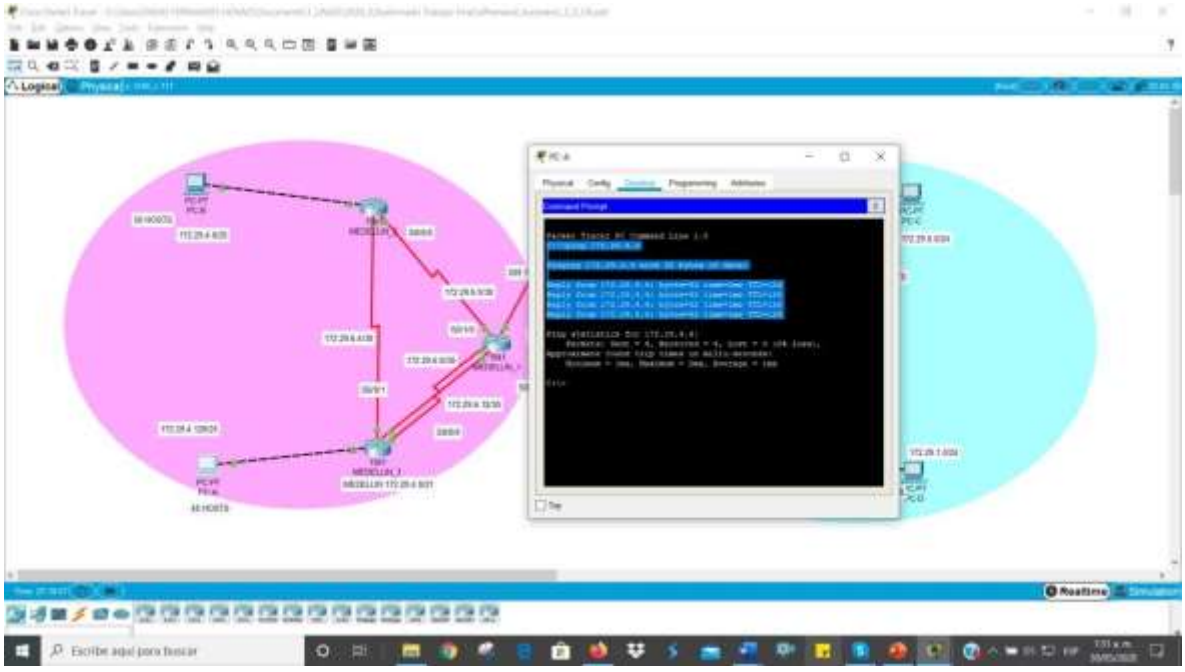


Figura 42 - Ping del PC-B al PC-A

CONCLUSIONES

Sin duda alguna una de las mayores conclusiones que podemos sacar del desarrollo de las prácticas a través de los dos escenarios propuestos es que se afianzan los conocimientos adquiridos durante el desarrollo del diplomado, el constante uso de la herramienta de simulación de Cisco Packet Tracer, nos permite ensayar un sin número de veces sin temor a equivocarnos, lo cual genera mucha tranquilidad y confianza y sobre todo agilidad para realizar las tareas propuestas.

Es de vital importancia comprender y poner en práctica las configuraciones de lo equipo de las redes, sus protocolos de seguridad, la forma de redireccionar el tráfico en la red, y la forma de acceder más fácilmente y de forma segura a los diferentes dispositivos.

En el escenario 2 pudimos evidenciar y poner en práctica la configuración del protocolo OSPF, así como entender el porqué de uso en determinadas configuraciones de red, por lo general es el protocolo más usado, porque es ideal para implementar soluciones a gran escala por su robustez.

También se pudo comprender el funcionamiento del DHCP, este protocolo también tiene funciones muy importantes dentro de una red, ya que facilita la administración de la red, evitando con ello los posibles conflictos derivados de una mala configuración en los hosts.

Otra de las conclusiones importantes es que al enmascarar la red interna y poder salir a través de una única dirección pública en internet, se obtienen grandes beneficios ahorrando direcciones IPv4.

BIBLIOGRAFÍA

CISCO, Networking Academy. “Packet Tracer: Conexión de un router a una LAN”. {En línea}. {8 mayo de 2020} disponible en: (https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#6.4.3.3).

CISCO, Networking Academy. “Packet Tracer: Configuración de los parámetros iniciales del switch”. {En línea}. {8 mayo de 2020} disponible en: (https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#2.2.3.3).

CISCO, Networking Academy. “Packet Tracer: Situación de división en subredes 1”. {En línea}. {8 mayo de 2020} disponible en: (https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#9.1.4.6).

CISCO, Networking Academy. “Packet Tracer: Situación de división en subredes 2”. {En línea}. {8 mayo de 2020} disponible en: (https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#9.1.4.7).

CISCO, Networking Academy. “Práctica de laboratorio: configuración de redes VLAN y enlaces troncales”. {En línea}. {8 mayo de 2020} disponible en: (https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#3.2.2.5).

CISCO, Networking Academy. “Práctica de laboratorio: implementación de seguridad de VLAN”. {En línea}. {8 mayo de 2020} disponible en: (https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#3.3.2.2).

CISCO, Networking Academy. “Packet Tracer: Configuring Router-on-a-Stick Inter VLAN Routing”. {En línea}. {8 mayo de 2020} disponible en: (https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#5.1.3.6).

CISCO, Networking Academy. “Packet Tracer: Layer 2 VLAN Security”. {En línea}. {8 mayo de 2020} disponible en: (https://static-course assets.s3.amazonaws.com/ITN6/es/index.html#6.5.1.3).

CISCO, Networking Academy. “Práctica de laboratorio: configuración básica de RIPv2 y RIPng”. {En línea}. {8 mayo de 2020} disponible en: (https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#7.3.2.4).

CISCO, Networking Academy. “Práctica de laboratorio: configuración de OSPFv2 básico de área única”. {En línea}. {8 mayo de 2020} disponible en: (https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#8.2.4.5).

CISCO, Networking Academy. “Práctica de laboratorio: configuración de OSPFv3 básico de área única”. {En línea}. {8 mayo de 2020} disponible en: (https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#8.3.3.6).

CISCO, Networking Academy. “Práctica de laboratorio: configuración de NAT dinámica y estática”. {En línea}. {8 mayo de 2020} disponible en: (https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#11.2.2.6).

CISCO, Networking Academy. “Práctica de laboratorio: configuración de un conjunto de NAT con sobrecarga y PAT”. {En línea}. {8 mayo de 2020} disponible en: (https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#11.2.3.7).

CISCO, Networking Academy. “Packet Tracer: Configure IP ACLs to Mitigate Attacks”. {En línea}. {8 mayo de 2020} disponible en: (https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#4.4.1.2).

CISCO, Networking Academy. “Packet Tracer: Configuring Standard ACLs”. {En línea}. {8 mayo de 2020} disponible en: (https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#9.2.1.10).

CISCO, Networking Academy. “Packet Tracer: Configuring Named Standard ACLs”. {En línea}. {8 mayo de 2020} disponible en: (https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#9.2.1.11).

CISCO, Networking Academy. “Packet Tracer: Configuring an ACL on VTY Lines”. {En línea}. {8 mayo de 2020} disponible en: (https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#9.2.3.3).

CISCO, Networking Academy. “Packet Tracer: Configuring IPv6 ACLs”. {En línea}. {8 mayo de 2020} disponible en: (https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#9.5.2.6).