SOLUCIÓN BAJO EL USO DE TECNOLOGÍA CISCO

DUBAN OLMEDO PALACIO OSORIO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BASICAS TECNOLOGIAS E INGENIERIAS

INGENIERIA DE TELECOMUNICACIONES

MEDELLIN, ANTIOQUIA

2020

SOLUCIÓN BAJO EL USO DE TECNOLOGÍA CISCO

DUBAN OLMEDO PALACIO OSORIO

ASESOR

NILSON ALBEIRO FERREIRA MANZANARES

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BASICAS TECNOLOGIAS E INGENIERIAS

INGENIERIA DE TELECOMUNICACIONES

MEDELLIN, ANTIOQUIA

2020

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____

_____

_____

Firma del Presidente de Jurado

_____

Firma del Jurado

_____

Firma del Jurado

Tabla de contenido

LISTA DE TABLAS

LISTA DE FIGURAS

RESUMEN

La práctica se desarrolla en torno a dos escenarios primero pretende abordar una red pequeña en las cuales se procede a conectar con IPV4 y IPV6 , donde se aplican diferentes protocolos como : seguridad de switches ,protocolo RIP,routing entre VLAN ,(NAT) dinámica y estática RIPV2 ,(ACL)lista de control de acceso, NTP(protocolo tiempo de red servidor cliente) y demás configuraciones básicas en los dispositivos.

En el segundo escenario se requiere que a través de configuraciones se permita el acceso y conectividad entre 2 ciudades, llevando a cabo diferentes configuraciones en los dispositivos de red, como los parámetros básicos en switches y routers como permitiendo así la administración de esta y especializados como la autenticación PPP, la implantación de ruting del protocolo OSPF, configuración PAP – CHAT – NAT y DHCP.

ABSTRACT

The practice is developed around two scenarios, the first one aims to address a small network in which it proceeds to connect with IPV4 and IPV6, where different protocols are applied such as: switch security, RIP protocol, routing between VLANs, (NAT) dynamic and static RIPV2, (ACL) access control list, NTP (network server client time protocol) and other basic settings on the devices.

In the second scenario, it is required that through configurations access and connectivity be allowed between 2 cities, carrying out different configurations on network devices, such as basic parameters in switches and routers, thus allowing the administration of this and specialized ones such as PPP authentication, implementation of OSPF protocol ruting, PAP - CHAT –NAT and DHCP configuration

GLOSARIO

DHCP: Protocolo que permite la configuración automática de red de los hosts de una red TCP/IP mediante un mecanismo de cliente-servidor.

DNS: (Domain name system, sistema de nombre de dominio) Un servicio que proporciona las directivas y los mecanismos de nomenclatura para la asignación de dominio.

NAT: (Network address translation, traducción de direcciones de red) Traducción de una dirección IP que se utiliza en una red a otra dirección IP conocida en otra red**.**

PING: Comando utilizado para comprobar si una determinada interfaz de red, se encuentra activa.

RIP: (Routing Information Protocol, protocolo de información de enrutamiento) Un protocolo de puerta de enlace interno que enruta paquetes IPv4 y mantiene la tabla de enrutamiento de todos los hosts en la LAN.

Router: Dispositivo que administra el tráfico de datos que circula en una red de computadoras.

Switch: ispositivo que permite la conexión de computadoras y periféricos a la red para que puedan comunicarse entre sí y con otras redes.

Tabla de enrutamiento: Tabla que contiene la información de enrutamiento para un paquete, que ayuda a determinar la mejor ruta de acceso para que el paquete llegue a destino.

Topología de red: Es el mapa físico o lógico de una red para intercambiar datos.

VLAN: (virtual local area network, red de área local virtual) Una subdivisión de una red de área local en la capa de enlace de datos de la pila de protocolo.

WLAN: siglas inglesas de Wireless Local Área Network, que es español significa Red de Área Local Inalámbrica.

1. INTRODUCCIÓN

El presente trabajo forma parte de las actividades evaluativas del Diplomado de Profundización CCNA, se presentan problemas relacionados con diversos aspectos de Networking que fueron vistos durante el desarrollo del diplomado. se desarrollan (2) escenarios en los cuales se documenta la solución de cada uno y se deja la evidencia de las configuraciones de los dispositivos, la descripción detallada del paso a paso de cada una de las etapas realizadas y el registro de los procesos de verificación de conectividad mediante el uso de comandos ping, traceroute, show ip route, entre otros.

El proceso es realizado en Packet Tracer y entre las configuraciones realizadas para el escenario (1) se encuentra: configuración básica del router, configuración de seguridad, configuración de RIV2, implementación DHCP y NAT, configuración NTP, etc.

Entre las configuraciones del escenario (2) se encuentran: configuración básica del router, enrutamiento, configuración de PAT, configuración DHCP, etc

2. OBJETIVOS

2.1. OBJETIVO GENERAL

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

2.2. OBJETIVOS ESPECIFICOS

Mediante Packet Tracer configurar una red pequeña para que admita conectividad IPV4 e IPV6, seguridad de switches, routing entre VLAN, el protocolo de routing dinámico RIPv2, el protocolo de configuración de hosts dinámicos (DHCP), la traducción de direcciones de red dinámicas y estáticas (NAT), listas de control de acceso (ACL) y el protocolo de tiempo de red (NTP) servidor/cliente

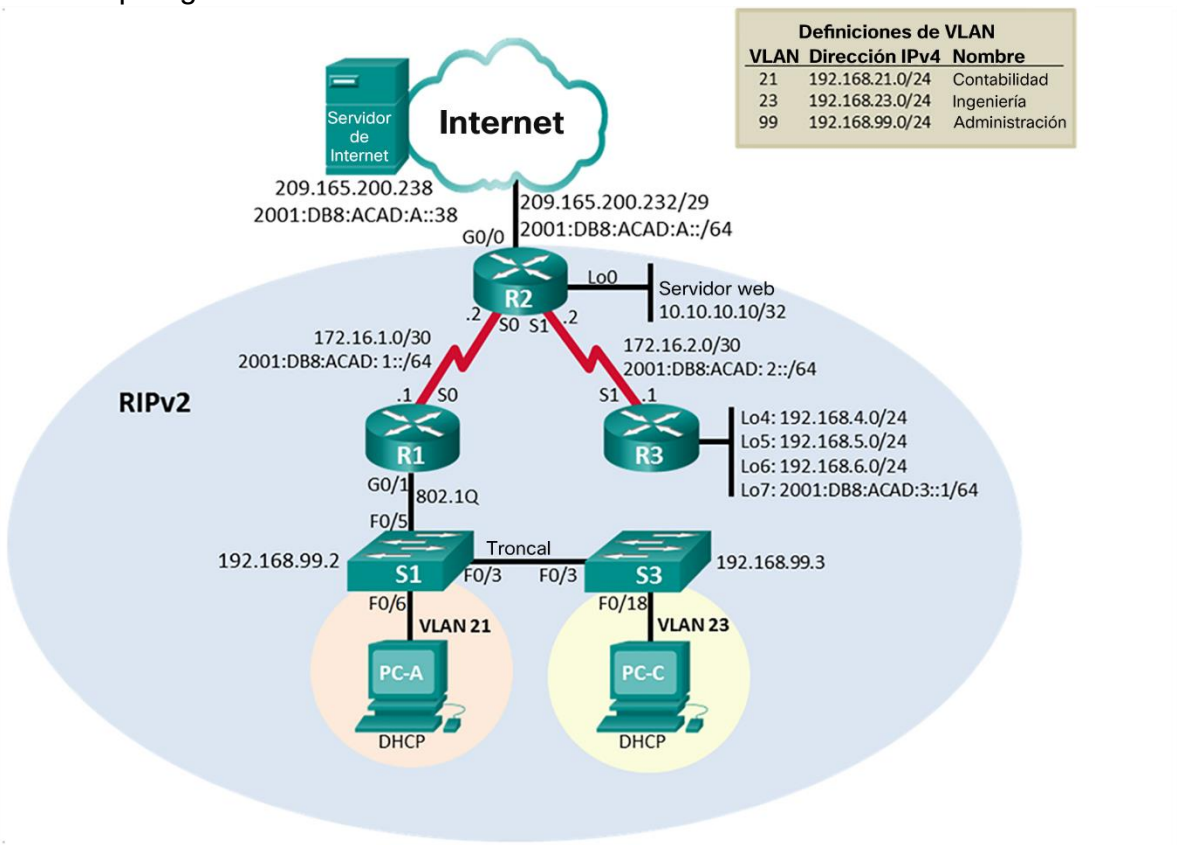
Configurar en interconectar los dispositivos que se encuentran en dos ciudades utilizando el protocolo OSPF habilitar encapsulamiento PPP y su autenticación, proporcionar servicio DHCP en las LAN y habilitar NAT de sobrecarga

3. ESCENARIO 1

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

3.1. TOPOLOGÍA

Topología de Red. Escenario 1



3.2. INICIALIZAR DISPOSITIVOS

Para este procedimiento se explica a continuación

3.2.1. Inicializar y volver a cargar los routers y los switches

Elimine las configuraciones de inicio y vuelva a cargar los dispositivos

Tabla 1. Inicializar y volver a cargar los R y S

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	• enable • 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	• enable • 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	• enable • show flash

- Este proceso se realiza cuando cuando se desea eliminar configuraciones no deseadas en los dispositivos

3.2.2. Configurar los parámetros básicos de los dispositivos

Configurar la computadora de internet

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

Tabla 2. Configurar la 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::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:A::1

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

- Se realiza la configuración inicial de los dispositivos con el fin de de generar un nombre de identificación en la red y los accesos de seguridad para estos.

- Se configuran los router R1-R2-R3 y S1-S3 esto con el fin de tener una identificación de la red y sus accesos de seguridad, como proteger el modo remoto de telnet y SSH, proteger el modo EXEC por privilegios, proteger todas las contraseñas en el archivo de configuración, proporcionarlas notificaciones legales y terminamos guardando la configuración.

3.2.3. Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 3. Configurar R1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	• enable • configure terminal • no ip domain-lookup
Nombre del router	• hostname R1
Contraseña de exec privilegiado cifrada	enable secret class
Contraseña de acceso a la consola	• line console 0 • password cisco • login
Contraseña de acceso Telnet	• line vty 0 15 • password cisco • login
Cifrar las contraseñas de texto no cifrado	• service password-encryption
Mensaje MOTD	• banner motd %se prohíbe el acceso no autorizado%
Interfaz S0/0/0	Establezca la descripción • interface s0/0/0 • description conección a R2 Establecer la dirección ipv4 consultar el diagrama de topología para conocer la información de direcciones • ip address 172.16.1.1 255.255.255.252 • no shutdown

Elemento o tarea de configuración	Especificación
	Establecer la dirección ipv6 consultar el diagrama de topología para conocer la información de direcciones • ipv6 address 2001:db8:acad:1::1/64 establecer la frecuencia de reloj en 128000 • clock rate 128000 activar la interfaz • no shutdown exit
Rutas predeterminadas	Configurar una ruta IPv4 predeterminada de S0/0/0 • ip route 0.0.0.0 0.0.0.0 s0/0/0 configurar una ruta ipv6 predeterminada de s0/0/0 ipv6 route ::/0 s0/0/0

Nota: Todavía no configure G0/1.

3.2.4. Configurar R2

La configuración del R2 incluye las siguientes tareas:

Tabla 4. Configurar R2

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	• enable • configure terminal • no ip domain-lookup
Nombre del router	• hostname R2
Contraseña de exec privilegiado cifrada	• enable secret class
Contraseña de acceso a la consola	• line console 0 • password cisco • login
Contraseña de acceso Telnet	• line vty 0 15 • password cisco • login
Cifrar las contraseñas de texto no cifrado	• service password-encryption
Habilitar el servidor HTTP	• ip http server
Mensaje MOTD	• banner motd %se prohíbe el acceso no autorizado%

Elemento o tarea de configuración	Especificación
Interfaz S0/0/0	Establezca la descripción • interface s0/0/0 • description conección a R1 Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. • ip address 172.16.1.2 255.255.255.252 Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. • ipv6 address 2001:db8:acad:1::2/64 Activar la interfaz • no shutdown
Interfaz S0/0/1	Establecer la descripción • interface s0/0/1 • description Conección a R3 Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. • ip address 172.16.2.2 255.255.255.252 Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. • ipv6 address 2001:db8:acad:2::2/64 Establecer la frecuencia de reloj en 128000. • clock rate 128000 Activar la interfaz • no shutdown

Elemento o tarea de configuración	Especificación
Interfaz G0/0 (simulación de Internet)	Establecer la descripción. • interferface g0/0 • description conección a internet Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. • ip address 209.165.200.233 255.255.255.248 Establezca la dirección IPv6. Utilizar la primera dirección disponible en la subred. • ipv6 address 2001:db8:acad:a::1/64 Activar la interfaz no shutdown
Interfaz loopback 0 (servidor web simulado)	Establecer la descripción. • interface loopback 0 • description servidor web simulado Establezca la dirección IPv4. • ip address 10.10.10.10 255.255.255.255 exit
Ruta predeterminada	Configure una ruta IPv4 predeterminada de G0/0. • ip route 0.0.0.0 0.0.0.0 g0/0 Configure una ruta IPv6 predeterminada de G0/0. • ipv6 route ::/0 g0/0

3.2.5. Configurar R3

La configuración del R3 incluye las siguientes tareas:

Tabla 5. Configurar R3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	• enable • configure terminal • no ip domain-lookup
Nombre del router	• hostname R3
Contraseña de exec privilegiado cifrada	• enable secret class
Contraseña de acceso a la consola	• line console 0 • password cisco • login
Contraseña de acceso Telnet	• line vty 0 15 • password cisco • login
Cifrar las contraseñas de texto no cifrado	• service password-encryption
Mensaje MOTD	• banner motd %se prohíbe el acceso no autorizado.%
Interfaz S0/0/1	Establecer la descripción • interface s0/0/1 • description conección r2 Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. • ip address 172.16.2.1 255.255.255.252 Establezca la dirección IPv6. Consulte el

Elemento o tarea de configuración	Especificación
	diagrama de topología para conocer la información de direcciones. Ipv6 address 2001:DB8:ACAD:2::1/64 Activar la interfaz no shutdown
Interfaz loopback 4	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. • interface loopback 4 ip address 192.168.4.1 255.255.255.0
Interfaz loopback 5	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. • interface loopback 5 ip address 192.168.5.1 255.255.255.0
Interfaz loopback 6	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. • interface loopback 6 ip address 192.168.6.1 255.255.255.0
Interfaz loopback 7	Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. • interface loopback 7 ipv6 address 2001:db8:acad:3::1/64
Rutas predeterminadas	Configure una ruta IPv4 predeterminada de s0/0/1 • ip route 0.0.0.0 0.0.0.0 s0/0/1 Configure una ruta IPv6 predeterminada de s0/0/1 ipv6 route ::/0 s0/0/1

3.2.6. Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 6. Configurar S1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	• enable • configure terminal • no ip domain-lookup
Nombre del switch	• hostname S1
Contraseña de exec privilegiado cifrada	• enable secret class
Contraseña de acceso a la consola	• line console 0 • password cisco • login
Contraseña de acceso Telnet	• line vty 0 15 • password cisco • login
Cifrar las contraseñas de texto no cifrado	• service password-encryption
Mensaje MOTD	• banner motd %se prohíbe el acceso no autorizado%

3.2.7. Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 7. Configurar S3

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

3.2.8. Verificar la conectividad de la red

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

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

Tabla 8. Verificar la Conectividad de la Red

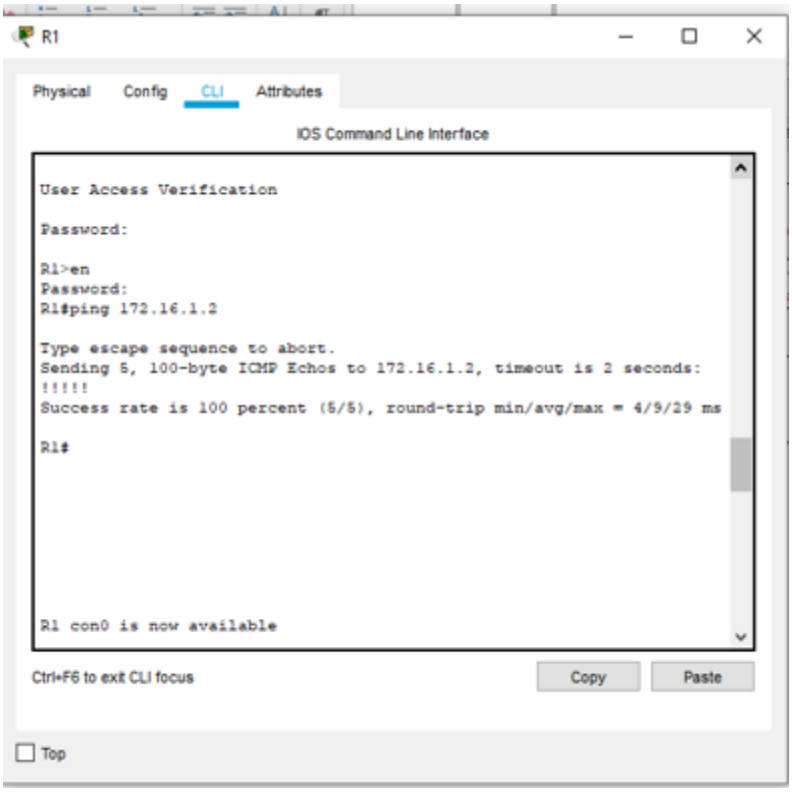
Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	Satisfactorio
R2	R3, S0/0/1	172.16.2.1	Satisfactorio
PC de Internet	Gateway predeterminado	209.165.200.233	Satisfactorio

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

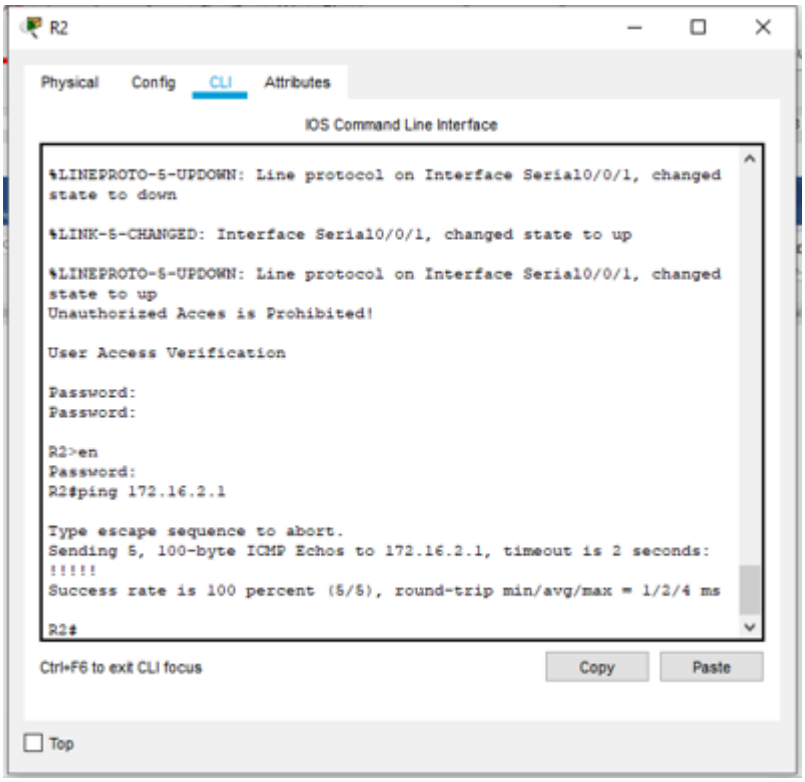
- Realizamos los ping correspondiente para la verificación de

comunicación entre routers y Gateway predeterminado.

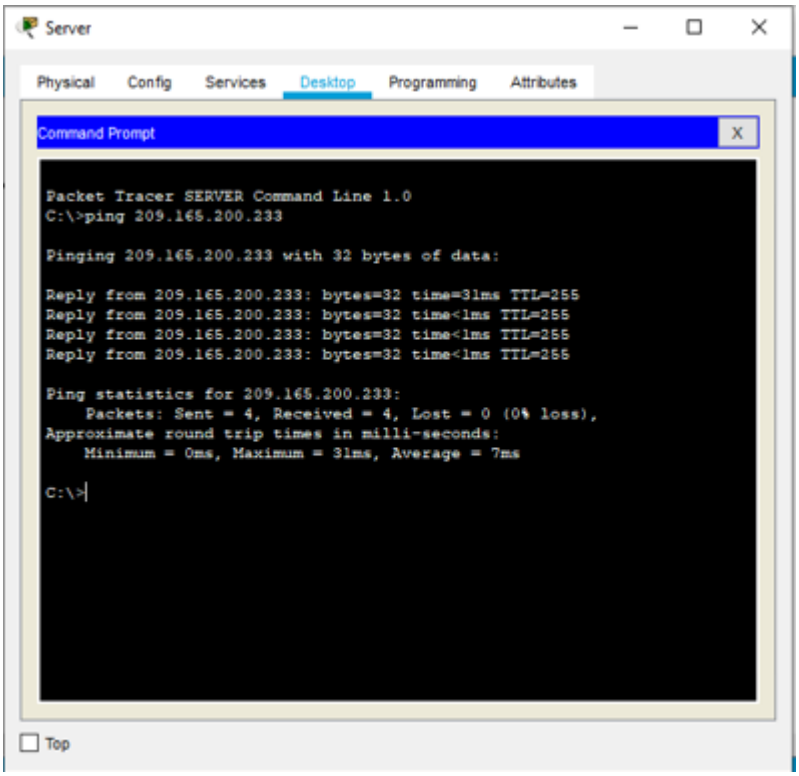
Registro fotográfico: Ping desde R1 a R2



Registro fotográfico: Ping de R2 a R3



Registro fotográfico: Ping al Gateway predeterminado



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

- Las diferentes estaciones se combinan en una solución de red independiente de su ubicación: siempre que estén conectadas entre sí en la misma LAN, es posible combinarlas mediante una VLAN. No supone ningún problema que la LAN abarque varios switches. Lo único importante es que el switch también sea compatible con la VLAN. La única manera de crear VLAN es utilizando switches gestionables .

A continuación, se presenta el paso a paso:

3.3.1. Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 9. Configurar la Seguridad. Configurar S1

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para topología para crear y nombrar cada una de las VLAN que se indican • enable • configure terminal • vlan 21 • name contabilidad • vlan 23 • name ingenieria • vlan 99 • name administracion • exit
Asignar la dirección IP de administración.	Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S1 en el diagrama de topología • interface vlan 99 • ip address 192.168.99.2 255.255.255.0 • no shutdown exit
Asignar el gateway predeterminado	Asigne la primera dirección IPv4 de la subred como el gateway predeterminado. Ip default-gateway 192.168.99.1

Elemento o tarea de configuración	Especificación
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa • interface f0/3 • switchport mode trunk switchport trunk native vlan 1
Forzar el enlace troncal en la interfaz F0/5	Utilizar la red VLAN 1 como VLAN nativa • interface f0/5 • switchport mode trunk switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range • interface range f0/1-2, f0/4, f0/6-24, g0/1-2 switchport mode access
Asignar F0/6 a la VLAN 21	• nterface f0/6 switchport access vlan 21
Apagar todos los puertos sin usar	• interface range f0/1-2, f0/4, f0/7-24, g0/1-2 shutdown

3.3.2. Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 10. Configurar la Seguridad. Configurar S3

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para topología para crear cada una de las VLAN que se indican Dé nombre a cada VLAN. • enable • configure terminal • vlan 21 • name accounting • vlan 23 • name engineering • vlan 99 • name management • exit
Asignar la dirección IP de administración	Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S3 en el diagrama detopología • interface vlan 99 • ip address 192.168.99.3 255.255.255.0 • no shutdown • exit
Asignar el gateway predeterminado.	Asignar la primera dirección IP en la subred como gateway predeterminado. • Ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa • interface f0/3 • switchport mode trunk • switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range • interface range f0/1-2, f0/4-24, g0/1-2 • switchport mode access
Asignar F0/18 a la VLAN 23	• interface f0/18 • switchport access vlan 23
Apagar todos los puertos sin usar	• interface-range f0/1-2, f0/4-17, f0/19-24, g0/1-2 shutdown

3.3.3. Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 11. Configurar la Seguridad. Configurar R1

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	Descripción: LAN de Contabilidad Asignar la VLAN 21 Asignar la primera dirección disponible a esta interfaz • enable • configure terminal • interface g0/1.21 • description lan de contabilidad • encapsulation dot1q 21 • ip address 192.168.21.1 255.255.255.0
Configurar la subinterfaz 802.1Q .23 en G0/1	Descripción: LAN de Ingeniería Asignar la VLAN 23 Asignar la primera dirección disponible a esta interfaz • interface g0/1.23 • description lan de ingenieria • encapsulation dot1q 23 • ip address 192.168.23.1 255.255.255.0
Configurar la subinterfaz 802.1Q .99 en G0/1	Descripción: LAN de Administración Asignar la VLAN 99 Asignar la primera dirección disponible a esta interfaz • nterface g0/1.99 • description lan de administracion • encapsulation dot1q 99 • ip address 192.168.99.1 255.255.255.0

Elemento o tarea de configuración	Especificación
Activar la interfaz G0/1	• int g0/1 • no shutdown

3.3.4. ERIFICAR LA CONECTIVIDAD DE LA RED

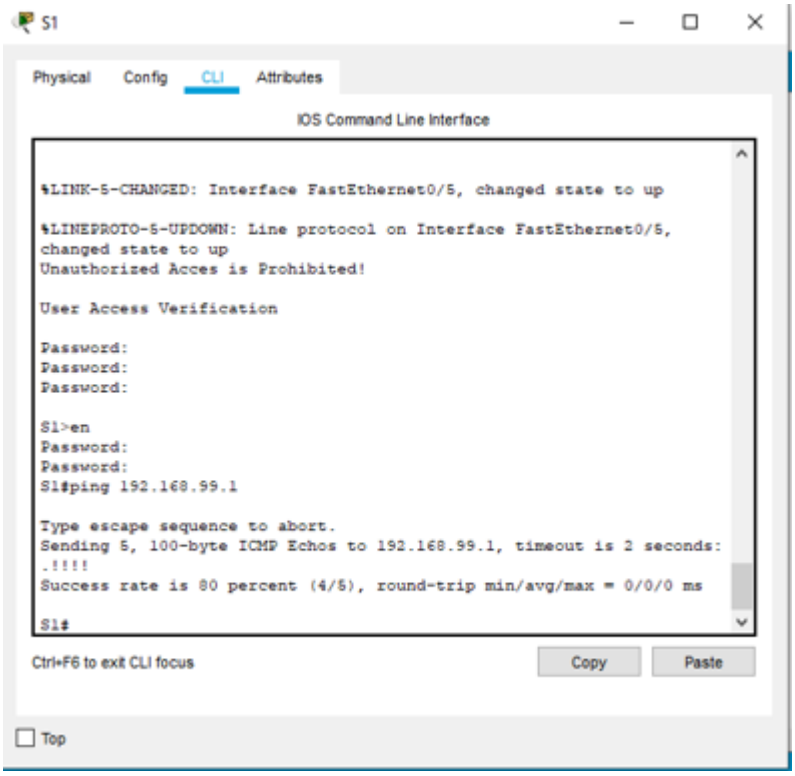
Utilice el comando **ping** para probar la conectividad entre los switches y el R1. Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 12. Configurar la Seguridad. Verificar la Conectividad de la Red

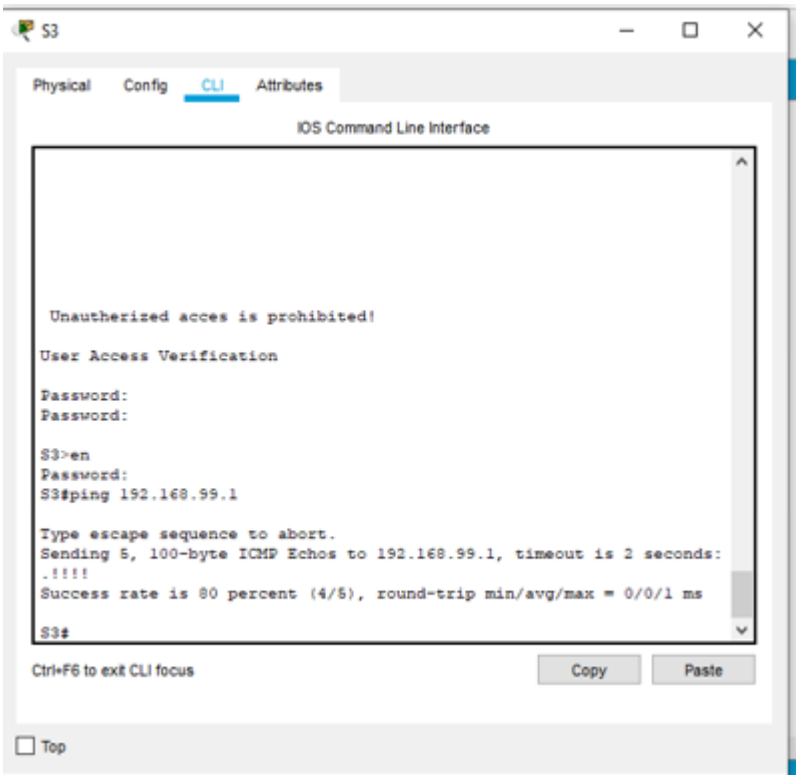
Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	Satisfactorio
S3	R1, dirección VLAN 99	192.168.99.1	Satisfactorio
S1	R1, dirección VLAN 21	192.168.21.1	Satisfactorio
S3	R1, dirección VLAN 23	192.168.23.1	Satisfactorio

- Realizamos los respectivos Pings encontrando todo satisfactorio

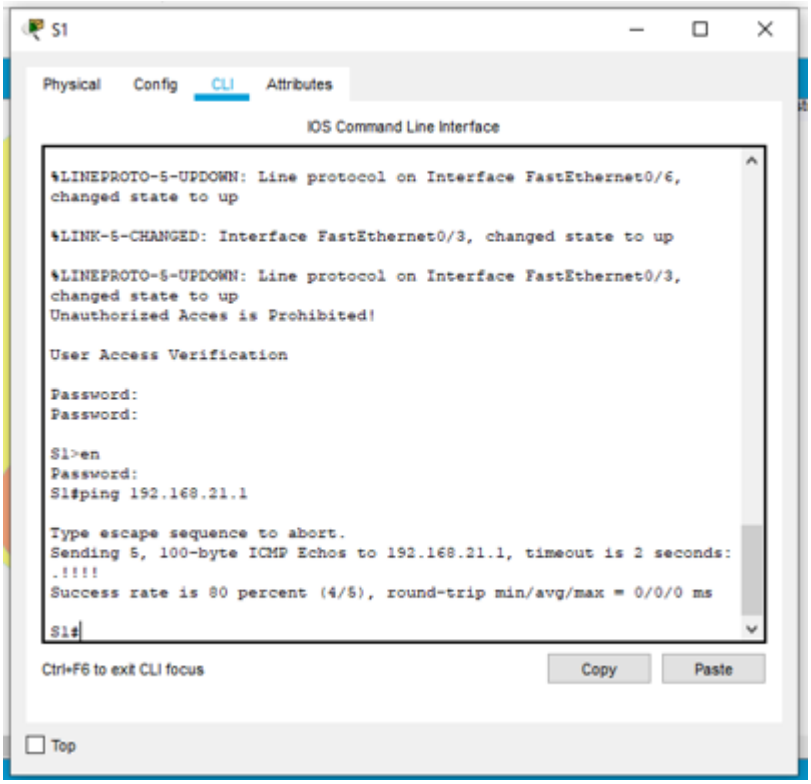
Registro fotográfico: ping de S1 a R1 Dirección VLAN 99 - 21



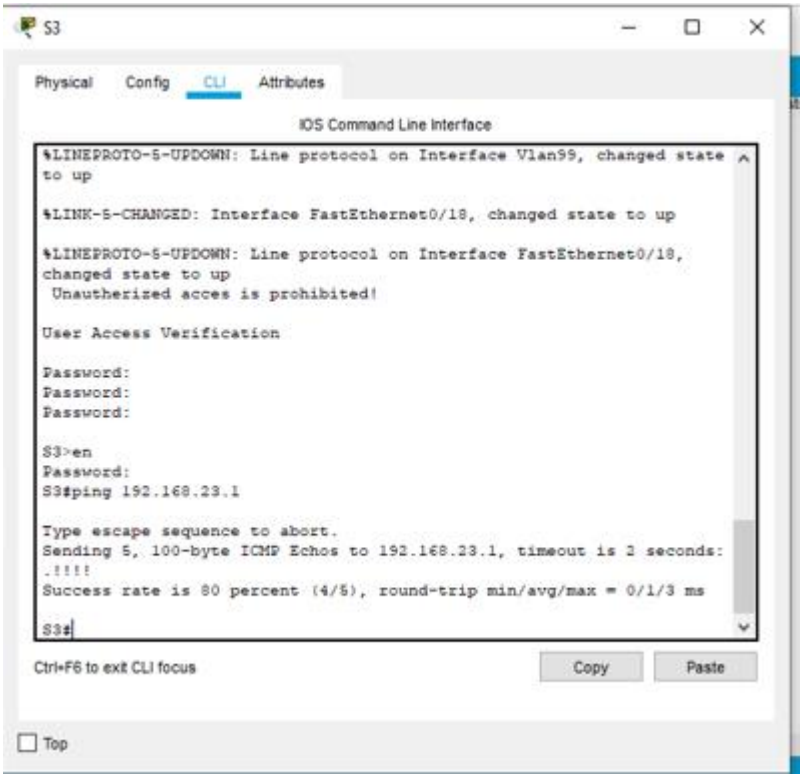
Registro fotográfico: ping de S3 a R1 Dirección VLAN 99 – 23



Registro fotográfico: ping de S1 a R1 Dirección VLAN 99 - 21



Registro fotográfico: ping de S3 a R1 Dirección VLAN 99 – 23



- Realizamos los respectivos Pings encontrando todo satisfactorio

3.4. CONFIGURAR EL PROTOCOLO DE ROUTING DINÁMICO RIPV2

- El protocolo interpreta las direcciones sin clase, así como la dirección “172.16.1.0/24” es interpretada como “172.16.1.0/24” a pesar de que esta dirección es clase B, es decir que no se toman en cuenta solo los dos primeros octetos, sino que los que se toman en cuenta son los que indica la máscara de subred.

3.4.1. CONFIGURAR RIPV2 EN EL R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 13. Configurar RIPV2 en el R1

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	• enable • configure terminal • router rip • versión 2 • do show ip route connected
Anunciar las redes conectadas directamente	Asigne todas las redes conectadas directamente. • network 172.16.1.0 • network 192.168.21.0 • network 192.168.23.0 • network 192.168.99.0
Establecer todas las interfaces LAN como pasivas	• passive-interface g0/1.21 • passive-interface g0/1.23 • passive-interface g0/1.99
Desactive la sumarización automática	• no auto-summary

CONFIGURAR RIPV2 EN EL R2

La configuración del R2 incluye las siguientes tareas:

Tabla 14. Configurar RIPV2 en el R2

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	• enable • configure terminal • router rip • versión 2 • do show ip route connected
Anunciar las redes conectadas directamente	**Nota:** Omitir la red G0/0. • network 10.10.10.10 • network 172.16.1.0 • network 172.16.2.0
Establecer la interfaz LAN (loopback) como pasiva	• passive-interface loopback 0
Desactive la sumarización automática.	• no auto-summary

3.4.2. CONFIGURAR RIPV3 EN EL R2

La configuración del R3 incluye las siguientes tareas:

Tabla 15. Configurar RIPV3 en el R2

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	• enable • configure terminal • router rip • versión 2 • do show ip route connected
Anunciar redes IPv4 conectadas directamente	• network 172.16.2.0 • network 192.168.4.0 • network 192.168.5.0 • network 192.168.6.0

Elemento o tarea de configuración	Especificación
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	• passive-interface loopback 4 • passive-interface loopback 5 • passive-interface loopback 6
Desactive la sumarización automática.	• no auto-summary

3.4.3. VERIFICAR LA INFORMACIÓN DE RIP

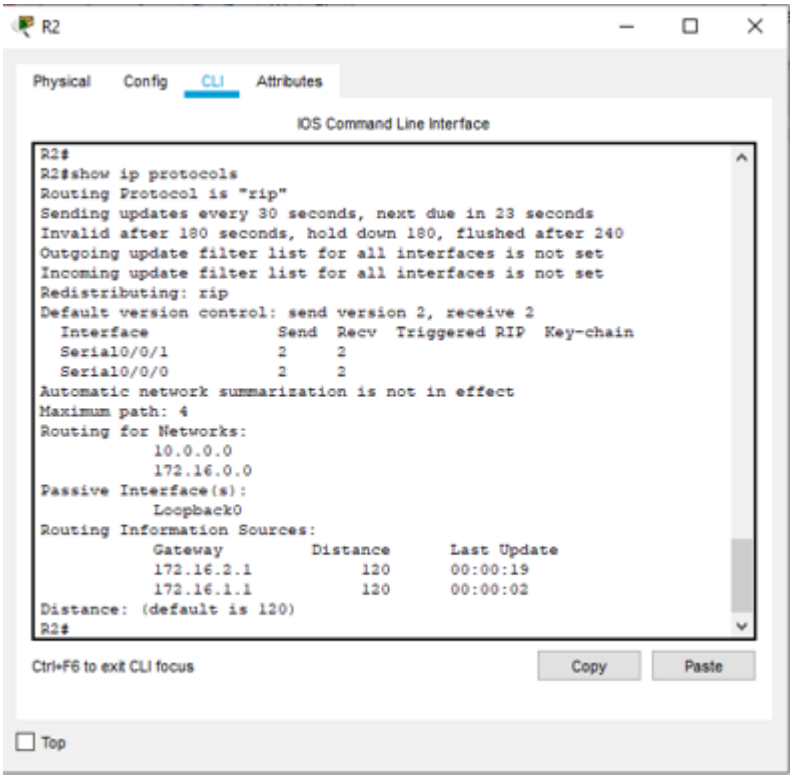
Verifique que RIP esté funcionando como se espera. Introduzca el comando de CLI adecuado para obtener la siguiente información:

- Se realiza el protocolo RIP en los router R1-R2-R3 que comprenden la red, con este protocolo logramos que todos los equipos en la red tengan comunicación entre sí, esto es debido a que los tres routers conocen como llegar a cada uno de los equipos.

Tabla 16. Verificar 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?	• enable • show ip protocols
¿Qué comando muestra solo las rutas RIP?	• show ip route rip
¿Qué comando muestra la sección de RIP de la configuración en ejecución?	• show run | section router rip

Registro Fotográfico. Verificar la Información de RIP



.

3.5. IMPLEMENTAR DHCP Y NAT PARA IPV4

3.5.1. CONFIGURAR EL R1 COMO SERVIDOR DE DHCP PARA LAS VLAN 21 Y23

- Se reservan las primeras 20 direcciones ip en la VLAN 21 para configuraciones estáticas que van desde 192.168.21.1 192.168.21.20 y en la VLAN 23 las primeras 20 serían 192.168.23.1 192.168.23.20 estas para el DHCP .

  La creación del pool para las VLAN 21 Y 23 que permiten acceso al servidor.

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 17. Configurar el R1 como servidor de DHCP

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	• enable • configure terminal • 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	• ip dhcp excluded-address 192.168.23.1 192.168.23.20
Crear un pool de DHCP para la VLAN 21.	Nombre: ACCT Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado • ip dhcp pool acct • network 192.168.21.0 255.255.255.0 • default-router 192.168.21.1 • dns-server 10.10.10.10 • domain-name ccna-sa.com

Elemento o tarea de configuración	Especificación
Crear un pool de DHCP para la VLAN 23	Nombre: ENGNR Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado • ip dhcp pool engnr • network 192.168.23.0 255.255.255.0 • default-router 192.168.23.1 • dns-server 10.10.10.10 • domain-name ccna-sa.com

3.5.2. CONFIGURAR LA NAT ESTÁTICA Y DINÁMICA EN EL R2

- Se creauna base local con una cuenta de usuario esta habilitará el servicio del servidor HTTP ,creando una dirección NAT estática direccionada al servidor con una ip global 209.165.200.237 y con una nat inside source static a la dirección 10.10.10.10 209.65.200-237 y asignamos las interfaces externas.
- Procedemos a crear una Access list privada con la NAT dinámica esta permite la traducción de un resumen de redes esto en el R3 , se define el pool de de ip publicas utilizables

La configuración del R2 incluye las siguientes tareas:

Tabla 18. Configurar la NAT estática y dinámica en el R2

Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	Nombre de usuario: **webuser** Contraseña: **cisco12345** Nivel de privilegio: **15** • enable • configure terminal • username webuser privilege 15 secret cisco12345
Habilitar el servicio del servidor HTTP	• ip http server
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	• ip http authentication local
Crear una NAT estática al servidor web.	Dirección global interna: **209.165.200.237** • ip nat inside source static 10.10.10.10 209.165.200.237
Asignar la interfaz interna y externa para la NAT estática	• interface g0/0 • ip nat outside • interface s0/0/0 • ip nat inside • interface s0/0/1

Elemento o tarea de configuración	Especificación
	• ip nat inside • exit
Configurar la NAT dinámica dentro de una ACL privada	Lista de acceso: 1 Permitir la traducción de las redes de Contabilidad y de Ingeniería en el R1 Permitir la traducción de un resumen de las redes LAN (loopback) en el R3 • access-list 1 permit 192.168.21.0 0.0.0.255 • access-list 1 permit 192.168.23.0 0.0.0.255 • 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: **209.165.200.233** – **209.165.200.236** • ip nat pool INTERNET 209.165.200.233 209.165.200.236 netmask 255.255.255.248
Definir la traducción de NAT dinámica	• ip nat inside source list 1 pool INTERNET

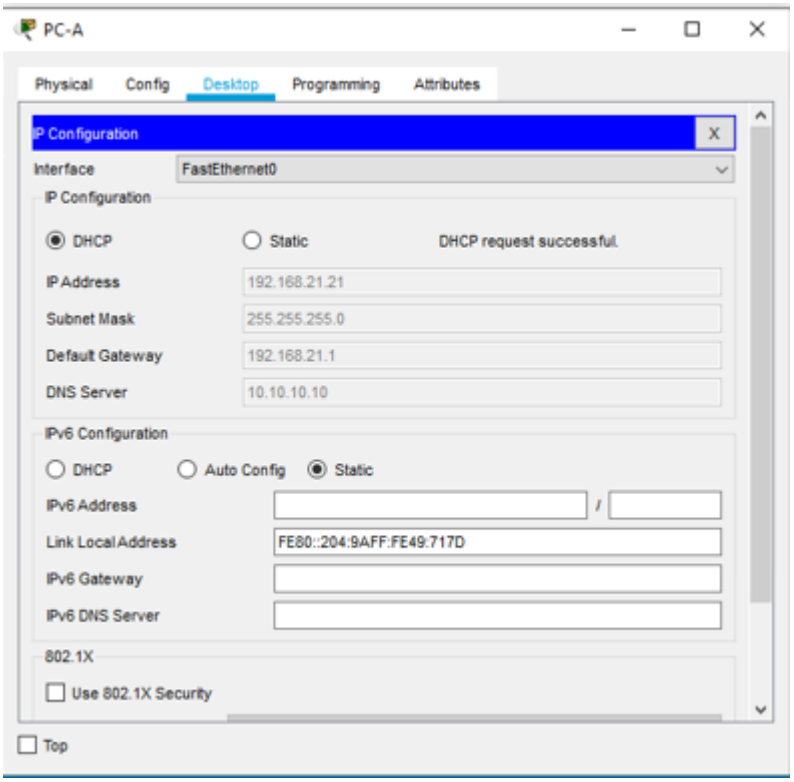
3.5.3. VERIFICAR EL PROTOCOLO DHCP Y LA NAT ESTÁTICA

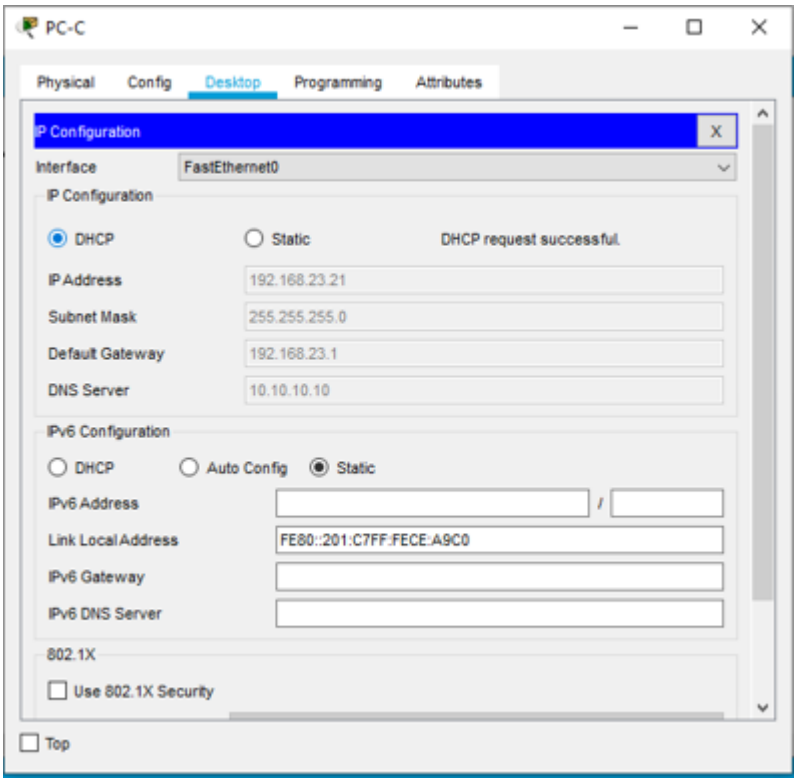
Utilice las siguientes tareas para verificar que las configuraciones de DHCP y NAT estática funcionen de forma correcta. Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

Tabla 19. Verificar el Protocolo DHCP y la NAT Estática

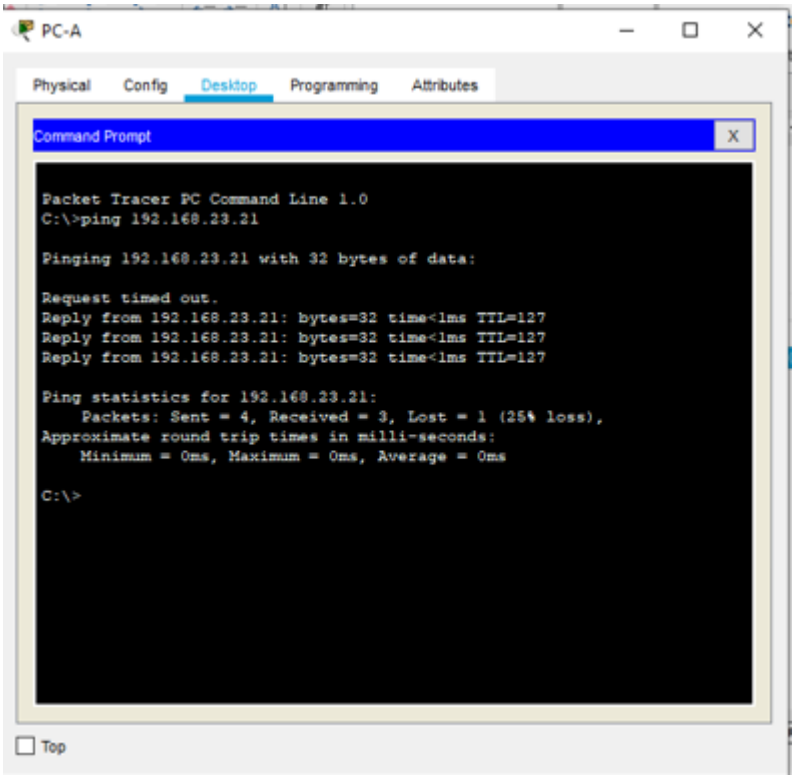
Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	• Satisfactorio
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	• Satisfactorio
Verificar que la PC-A pueda hacer ping a la PC-C **Nota:** Quizá sea necesario deshabilitar el firewall de la PC.	• Satisfactorio • Satisfactorio.
Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.237) Iniciar sesión con el nombre de usuario **webuser** y la contraseña **cisco12345**	• Satisfactorio.

Registro Fotográfico. Verificar IP en PC-A y PC-C del Servidor de DHCP

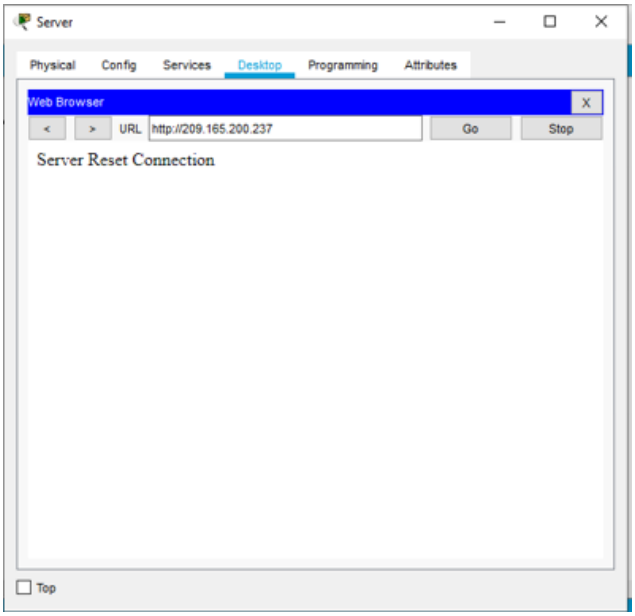




Registro Fotográfico. Ping PC-A a PC-C



Registro Fotográfico. Acceder al servidor web (209.165.200.237)



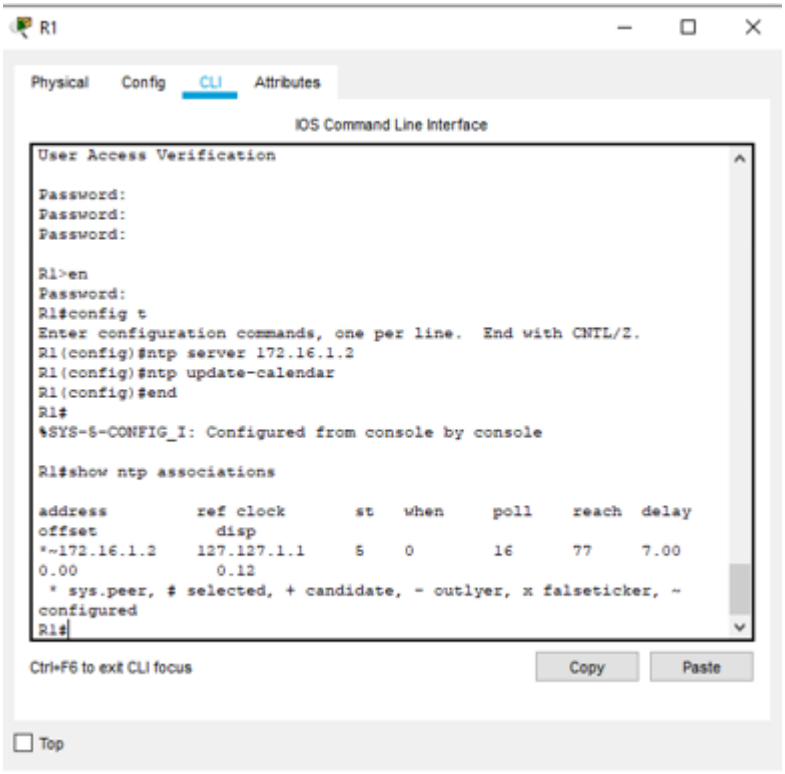
3.6. CONFIGURAR NTP

- Protegemos la hora y fechas en el R2 y como maestro en NTP

Tabla 20. Configurar NTP

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	**5 de marzo de 2016, 9 a. m.** • enable • clock set 09:00:00 05 mar 2016
Configure R2 como un maestro NTP.	Nivel de estrato: **5** • configure terminal • ntp master 5
Configurar R1 como un cliente NTP.	Servidor: **R2** • enable • configure terminal • ntp server 172.16.1.2
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	• ntp update-calendar • end
Verifique la configuración de NTP en R1.	• show ntp associations

Registro Fotográfico. Configuración NTP en R1



3.7. CONFIGURAR Y VERIFICAR LAS LISTAS DE CONTROL DE ACCESO (ACL)

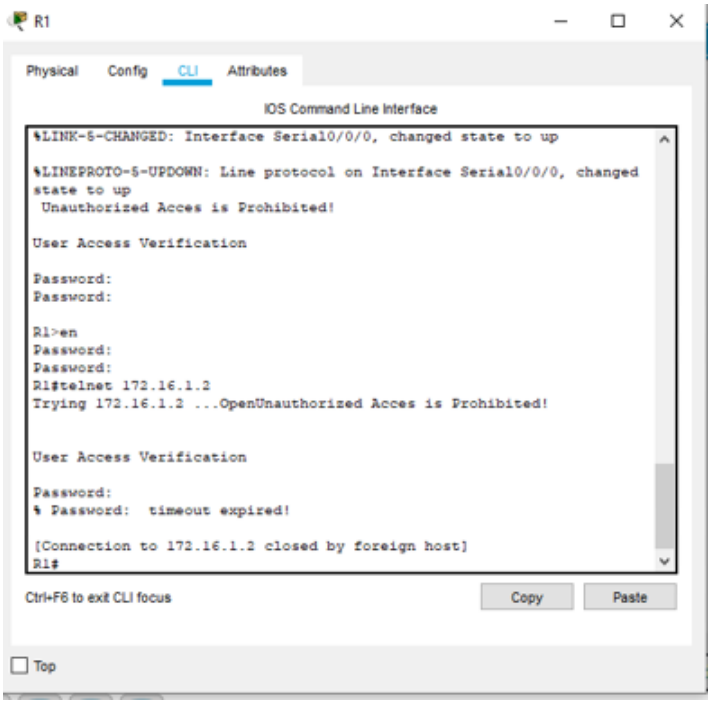
3.7.1. RESTRINGIR EL ACCESO A LAS LÍNEAS VTY EN EL R2

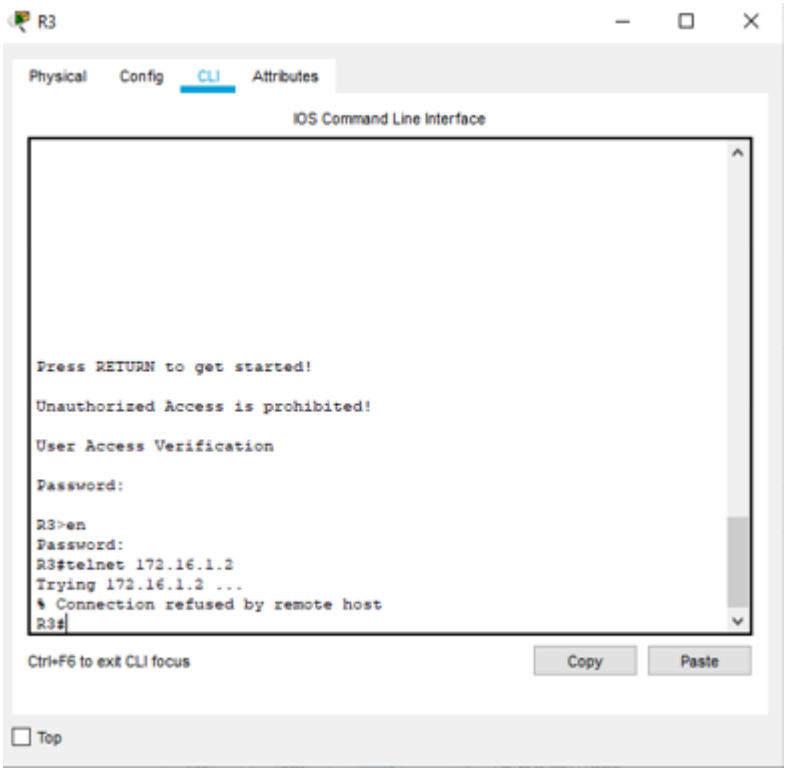
- Las listas de acceso extendidas y estándar se aplican a paquetes que viajan a través de un router, El objetivo de restringir el acceso vty es aumentar la seguridad de la red. También se logra el acceso a vty utilizando el protocolo Telnet para realizar una conexión no física con el router. Como resultado, hay solo un tipo de lista de acceso vty. Es necesario imponer idénticas restricciones a todas las líneas vty, ya que no es posible controlar a qué línea se conectará el usuario.

Tabla 21. Restringir el acceso a las lineas 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** • enable • configure terminal • ip access-list standard ADMIN- MGT • permit host 172.16.1.1 • exit
Aplicar la ACL con nombre a las líneas VTY	• line vty 0 15 • access-class ADMIN-MGT in
Permitir acceso por Telnet a las líneas de VTY	• transport input telnet
Verificar que la ACL funcione como se espera	• R1#telnet 172.16.1.2 • R3#telnet 172.16.1.2

Registro Fotográfico. Verificar el Acceso a las Líneas Vty En El R2


R1
Physical
Config
CLI
Attributes
IOS Command Line Interface
%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
Unauthorized Acces is Prohibited!
User Access Verification
Password:
Password:
R1>en
Password:
Password:
R1#telnet 172.16.1.2
Trying 172.16.1.2 ...OpenUnauthorized Acces is Prohibited!
User Access Verification
Password:
% Password: timeout expired!
[Connection to 172.16.1.2 closed by foreign host]
R1#
Ctrl+F6 to exit CLI focus
Copy
Paste
Top


R3
Physical
Config
CLI
Attributes
IOS Command Line Interface
Press RETURN to get started!
Unauthorized Access is prohibited!
User Access Verification
Password:
R3>en
Password:
R3#telnet 172.16.1.2
Trying 172.16.1.2 ...
% Connection refused by remote host
R3#
Ctrl+F6 to exit CLI focus
Copy
Paste
Top

3.7.2. INTRODUCIR EL COMANDO DE CLI ADECUADO QUE SE NECESITA PARA MOSTRAR LO SIGUIENTE:

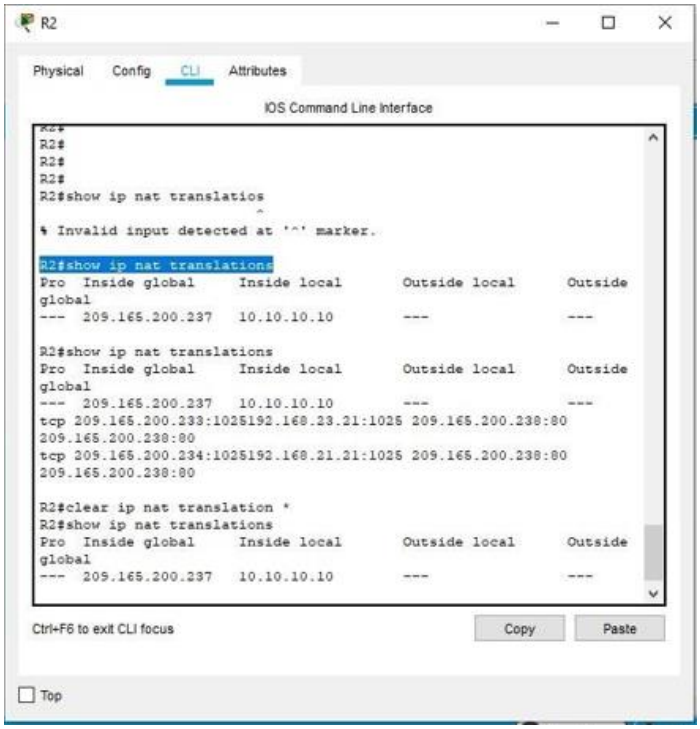
- En el ámbito de los dispositivos routers, las ACLs son listas de condiciones que se aplican al tráfico que viaja a través de la interfaz del router.

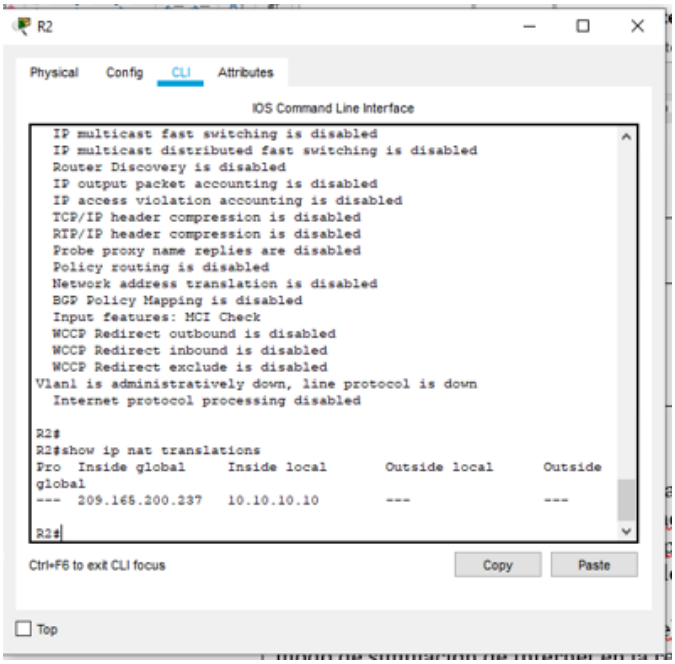
- Las ACL indican al router qué tipo de paquetes aceptar o rechazar en base a las condiciones establecidas en ellas y que permiten la administración del tráfico y aseguran el acceso, bajo esas condiciones, hacia y desde una red.

Tabla 22. Introducir el comando de CLI

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	• R2#show ip access-list
Restablecer los contadores de una lista de acceso	• R2#clear ip access-list (PT no soporta este comando)
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	• R2#show ip interface
¿Con qué comando se muestran las traducciones NAT?	**Nota:** Las traducciones para la PC-A y la PC-C se agregaron a la tabla cuando la computadora de Internet intentó hacer ping a esos equipos en el paso 2. Si hace ping a la computadora de Internet desde la PC-A o la PC-C, no se agregarán las traducciones a la tabla debido al modo de simulación de Internet en la red. • R2#Show ip nat translations
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	• R2#clear ip nat translation *

Registro Fotográfico. Comandos (show ip nat translations) y (clear ip nat translations)



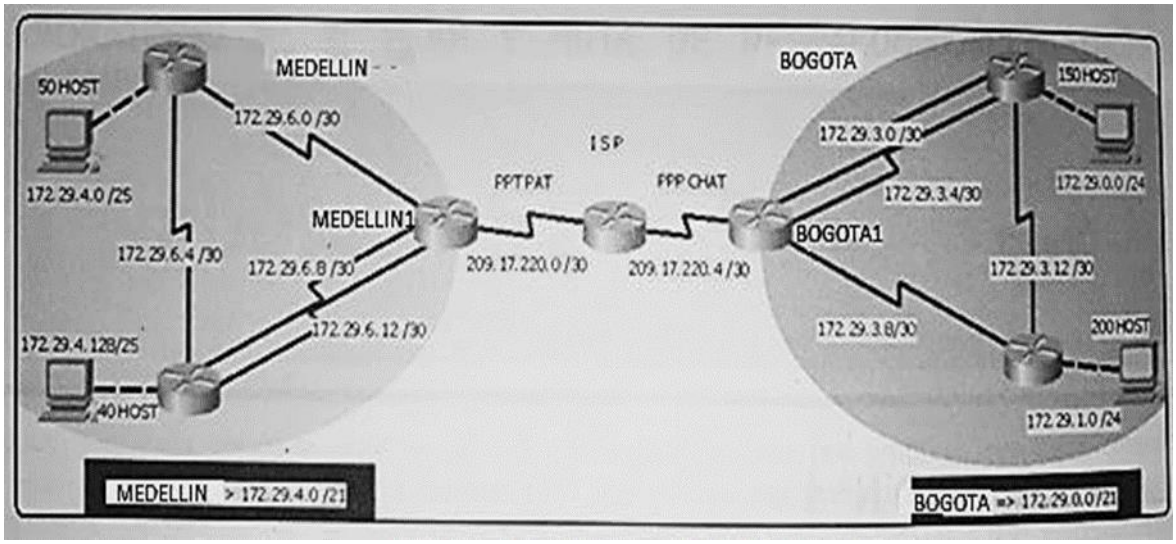


4. ESCENARIO 2

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.

4.1. TOPOLOGÍA DE RED

Figura 2. Topología de Red. Escenario 2



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

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

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

NAT de sobrecarga en los routers Bogota1 y medellin1.

Como trabajo inicial se debe realizar lo siguiente.
Realizar las rutinas de diagnóstico y dejar los equipos listos para su configuración (asignar nombres de equipos, asignar claves de seguridad, etc). Realizar la conexión fisica de los equipos con base en la topde red

4.1.1. CONFIGURACIÓN BÁSICA DE ROUTER

- enable
- configure terminal
- no ip domain-lookup
- hostname ISP
- enable secret class
- line console 0
- password cisco
- login
- line vty 0 15
- password cisco
- login
- service password-encryption
- banner motd %prohibido el acceso no autorizado%
- copy running-config startup-config

4.1.2. DIRECCIONAMIENTO

A continuación, se detalla el esquema de direccionamiento:

Tabla de direccionamiento

Sucursal	Equipo	Interfaz	Direccionamiento IP	Mascara de subred	Gateway
Medellín	Medellín 1	Se0/0/0	172.29.6.1	255.255.255.252	NA
		Se0/0/1	172.29.6.9	255.255.255.252	NA
		Se0/1/0	172.29.6.13	255.255.255.252	NA
		Se0/1/1	209.17.220.1	255.255.255.252	NA
	Medellín 2	Se0/0/0	172.29.6.2	255.255.255.252	NA
		Se0/1/1	172.29.6.5	255.255.255.252	NA
		G0/0	172.29.4.1	255.255.255.128	NA
	Medellín 3	Se0/0/1	172.29.6.10	255.255.255.252	NA
		Se0/1/0	172.29.6.14	255.255.255.252	NA
		Se0/1/1	172.29.6.6	255.255.255.252	NA
		G0/0	172.29.4.129	255.255.255.128	NA
	PC-MED 1	Fa0	DHCP		
	PC-MED 2	Fa0	DHCP		
Bogotá	Bogotá 1	Se0/0/0	172.29.3.1	255.255.255.252	NA
		Se0/1/1	172.29.3.5	255.255.255.252	NA
		Se0/0/1	172.29.3.9	255.255.255.252	NA
		Se0/1/0	209.17.220.5	255.255.255.252	NA
	Bogotá 3	Se0/0/0	172.29.3.2	255.255.255.252	NA
		Se0/1/1	172.29.3.6	255.255.255.252	NA
		Se0/1/0	172.29.3.13	255.255.255.252	NA
		G0/0	172.29.0.1	255.255.255.0	NA
	Bogotá 2	Se0/0/1	172.29.3.10	255.255.255.252	NA
		Se0/1/0	172.29.3.14	255.255.255.252	NA
		G0/0	172.29.1.1	255.255.255.0	NA
	PC-BOG 1	Fa0	DHCP		
	PC-BOG 2	Fa0	DHCP		
Proveedor	ISP	Se0/1/1	209.17.220.2	255.255.255.252	NA
		Se0/1/0	209.17.220.6	255.255.255.252	N/A

Medellin1-ISP

medellin1>enable
Password:
medellin1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
medellin1(config)#interface serial 0/1/1
medellin1(config-if)#description ENLACE A ISP
medellin1(config-if)#ip address 209.17.220.1 255.255.255.252
medellin1(config-if)#clock rate 128000
medellin1(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/1/1, changed state to down
medellin1(config-if)#

Medellin1-medellin2

medellin1>enable
Password: medellin1#configure
terminal
Enter configuration commands, one per line. End with CNTL/Z.
medellin1(config)#interface serial 0/0/0
medellin1(config-if)#description ENLACE A MEDELLIN2
medellin1(config-if)#ip address 172.29.6.1 255.255.255.252
medellin1(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
medellin1(config-if)#clock rate 128000
medellin1(config-if)#exit medellin1(config)#

Medellin1-medellin3 Enlace principal

medellin1>enable

Password:
medellin1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
medellin1(config)#interface serial 0/1/0
medellin1(config-if)#ip address 172.29.6.13 255.255.255.252
medellin1(config-if)#description ENLACE PRINCIPAL A MEDELLIN3
medellin1(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/1/0, changed state to down
medellin1(config-if)#

Medellin1-Medellin3 Enlace secundario

medellin1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
medellin1(config)#interface serial 0/0/1
medellin1(config-if)#ip address 172.29.6.9 255.255.255.252
medellin1(config-if)#description ENLACE SECUNDARIO A MEDELLIN3
medellin1(config-if)#no shutdown

Medellin2-Medellin1

Password:
medellin2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
medellin2(config)#interface serial 0/0/0
medellin2(config-if)#description ENLACE A MEDELLIN1
medellin2(config-if)#ip address 172.29.6.2 255.255.255.252

medellin2(config-if)#clock rate 128000
medellin2(config-if)#no shutdown

medellin2(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

Medellin2-Medellin3

medellin2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
medellin2(config)#interface serial 0/1/1
medellin2(config-if)#description ENLACE A MEDELLIN3
medellin2(config-if)#ip address 172.29.6.5 255.255.255.252
medellin2(config-if)#clock rate 128000
medellin2(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/1/1, changed state to down
medellin2(config-if)#
medellin2#
%SYS-5-CONFIG_I: Configured from console by console

medellin2#

Medellin2-Med2

medellin2>enable
Password:
medellin2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.

medellin2(config)#interface gigabitethernet 0/0
medellin2(config-if)#description ENLACE A LAN MEDELLIN 50 HOTS
medellin2(config-if)#ip address 172.29.4.1 255.255.255.128
medellin2(config-if)#no shutdown

medellin2(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state
to up

Medellin3-Medellin1 Enlace principal

medellin3>enable
Password:
medellin3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
medellin3(config)#interface serial 0/1/0
medellin3(config-if)#ip address 172.29.6.14 255.255.255.252
medellin3(config-if)#description ENLACE PRINCIPAL A MEDELLIN1
medellin3(config-if)#clock rate 128000
medellin3(config-if)#no shutdown
medellin3(config-if)#
%LINK-5-CHANGED: Interface Serial0/1/0, changed state to up

Medellin3-medellin2

medellin3>enable
Password:
medellin3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
medellin3(config)#interface serial 0/1/1

medellin3(config-if)#ip address 172.29.6.6 255.255.255.252
medellin3(config-if)#description ENLACE A MEDELLIN2
medellin3(config-if)#clock rate 128000
This command applies only to DCE interfaces
medellin3(config-if)#no shutdown

ISP-Medellin1

ISP>enable
Password:
ISP#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
ISP(config)#interface serial 0/1/1
ISP(config-if)#description ENLACE A MEDELLIN1
ISP(config-if)#ip address 209.17.220.2 255.255.255.252
ISP(config-if)#clock rate 128000
ISP(config-if)#no shutdown

Bogotá1-ISP

bogota1>enable
Password:
bogota1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
bogota1(config)#interface serial 0/1/0
bogota1(config-if)#description ENLACE A ISP bogota1(config-
if)#ip address 209.17.220.5 255.255.255.252
bogota1(config-if)#clock rate 128000

bogota1(config-if)#no shutdown

Bogotá1-Bogotá2 enlace principal

bogota1>enable
Password:
bogota1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
bogota1(config)#interface serial 0/0/0
bogota1(config-if)#description ENLACE PRINCIPAL A BOGOTA2
bogota1(config-if)#ip address 172.29.3.1 255.255.255.252
bogota1(config-if)#no shutdown

Bogota1-Bogotá3

bogota1>enable
Password:
bogota1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
bogota1(config)#interface serial 0/0/1
bogota1(config-if)#description ENLACE A BOGOTA3 bogota1(config-if)#ip address 172.29.3.9 255.255.255.252 bogota1(config-if)#no shutdown
Bogotá3-Bogotá1 Enlace principal

bogota3>enable
Password:
bogota3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
bogota3(config)#interface serial 0/0/0

bogota3(config-if)#description ENLACE PRINCIPAL A BOGOTA1
bogota3(config-if)#ip address 172.29.3.2 255.255.255.252
bogota3(config-if)#clock rate 128000
bogota3(config-if)#no shutdown

Bogota3-Bogotá 2

bogota3>enable
Password:
bogota3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
bogota3(config)#interface serial 0/1/0
bogota3(config-if)#description ENLACE A BOGOTA2
bogota3(config-if)#ip address 172.29.3.13 255.255.255.252
bogota3(config-if)#no shutdown

Bogotá3-Bog3

bogota3>enable
Password:
bogota3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
bogota3(config)#interface gigabitethernet 0/0
bogota3(config-if)#description ENLACE A LAN BOGOTA1 190 HOST
bogota3(config-if)#ip address 172.29.0.1 255.255.255.0
bogota3(config-if)#no shutdown

Bogotá 2 Bogota1

bogota2>enable

Password:
bogota2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
bogota2(config)#interface serial 0/0/1
bogota2(config-if)#description ENLACE A BOGOTA1
bogota2(config-if)#ip address 172.29.3.10 255.255.255.252
bogota2(config-if)#clock rate 128000
bogota2(config-if)#no shutdown
Bogotá2-Bogotá3

bogota2>enable
Password:
bogota2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
bogota2(config)#interface serial 0/1/0
bogota2(config-if)#description ENLACE A BOGOTA3
bogota2(config-if)#ip address 172.29.3.14 255.255.255.252
bogota2(config-if)#clock rate 128000
bogota2(config-if)#no shutdown

Bogotá2-Bog2

bogota2>enable
Password:
bogota2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
bogota2(config)#interface gigabitethernet 0/0
bogota2(config-if)#description ENLACE A LAN BOGOTA1 200 HOST
bogota2(config-if)#ip address 172.29.1.1 255.255.255.0
bogota2(config-if)#no shutdown

4.2. CONFIGURACIÓN DEL ENRUTAMIENTO

- Este protocolo ayuda abrir el camino más corto entre nodos, este mantiene la información topológica de sus áreas y las conecta con el resto de las áreas permitiendo encaminar paquetes a cualquier otro punto de la red.
  Realizamos este protocolo en los routers fronterizos y realizamos sus réplicas a sus áreas con el fin de extender el ruuting en cada una de ellas.

OSPF –Medellin1

```
medellin1>en
Password:
medellin1#config t
Enter configuration commands, one per line. End with CNTL/Z.
medellin1(config)#ospf 1
medellin1(config)#route ospf 1
medellin1(config-router)#do show ip route connected
C 172.29.6.0/30 is directly connected, Serial0/0/0
C 172.29.6.8/30 is directly connected, Serial0/0/1
C 172.29.6.12/30 is directly connected, Serial0/1/0
C 209.17.220.0/30 is directly connected, Serial0/1/1
medellin1(config-router)#network 172.29.6.0 0.0.0.3
medellin1(config-router)#network 172.29.6.0 0.0.0.3 area 0
medellin1(config-router)#network 172.29.6.8 0.0.0.3 area 0
medellin1(config-router)#network 172.29.6.12 0.0.0.3 area 0
medellin1(config-router)#passive-interface 0/1/1
medellin1(config-router)#passive-interface s0/1/1
medellin1(config-router)#
```

OSPF-Medellin2

Medellin2>en
Password:
Medellin2#config t
Enter configuration commands, one per line. End with CNTL/Z.
Medellin2(config)#route ospf 1
Medellin2(config-router)#do show ip route connected
C 172.29.4.0/25 is directly connected, GigabitEthernet0/0
C 172.29.6.0/30 is directly connected, Serial0/0/0
C 172.29.6.4/30 is directly connected, Serial0/1/1
Medellin2(config-router)#network 172.29.6.0 0.0.0.3 area 0
Medellin2(config-router)#network 172.29.6.4 0.0.0.3 area 0
Medellin2(config-router)#passive-interface g0/0
Medellin2(config-router)#

OSPF-Medeliin3

medellin3>en
Password:
medellin3#config t
Enter configuration commands, one per line. End with CNTL/Z.
medellin3(config)#route ospf 1
medellin3(config-router)#do show ip route connected
C 172.29.6.4/30 is directly connected, Serial0/1/1
C 172.29.6.8/30 is directly connected, Serial0/0/1
C 172.29.6.12/30 is directly connected, Serial0/1/0

medellin3(config-router)#network 172.29.6.4 0.0.0.3 area 0
medellin3(config-router)#network 172.29.6.8 0.0.0.3 area 0
medellin3(config-router)#network 172.29.6.12.0.0.3 area 0
medellin3(config-router)#passive-interface g0/0

OSPF-Bogotá1

Password:

Bogota1>en
Password:
Bogota1#config t
Enter configuration commands, one per line. End with CNTL/Z.
Bogota1(config)#route ospf 2
Bogota1(config-router)#do show ip route connected
C 172.29.3.0/30 is directly connected, Serial0/0/0
C 172.29.3.4/30 is directly connected, Serial0/1/1
C 172.29.3.8/30 is directly connected, Serial0/0/1
C 209.17.220.4/30 is directly connected, Serial0/1/0

Bogota1(config-router)#network 172.29.3.0 0.0.0.3 area 1
Bogota1(config-router)#network 172.29.3.4 0.0.0.3 area 1
Bogota1(config-router)#network 172.29.3.8 0.0.0.3 area 1
Bogota1(config-router)#passive-interface 0/1/0
Bogota1(config-router)#passive-interface s0/1/0
OSPF –Bogotá 2

Bogota2(config-router)#do show ip route connected
C 172.29.1.0/24 is directly connected, GigabitEthernet0/0
C 172.29.3.8/30 is directly connected, Serial0/0/1
C 172.29.3.12/30 is directly connected, Serial0/1/0

Bogota2(config-router)#network 172.29.3.8 0.0.0.3 area 1
Bogota2(config-router)#network 172.29.3.8 0.0.0.3 area 1
14:32:26: %OSPF-5-ADJCHG: Process 2, Nbr 209.17.220.5 on Serial0/0/1 from LOADING to FULL, Loading Done

Bogota2(config-router)#network 172.29.3.12 0.0.0.3 area 1
Bogota2(config-router)#
Bogota2(config-router)#passive-interface g0/0
Bogota2(config-router)#

OSPF-Bogotá 3

Bogota3(config-router)#do show ip route connected
C 172.29.3.0/30 is directly connected, Serial0/0/0
C 172.29.3.4/30 is directly connected, Serial0/1/1
C 172.29.3.12/30 is directly connected, Serial0/1/0
C 172.129.0.0/24 is directly connected, GigabitEthernet0/0

Bogota3(config-router)#network 172.29.3.0 0.0.0.3 area 1
Bogota3(config-router)#
14:27:46: %OSPF-5-ADJCHG: Process 2, Nbr 209.17.220.5 on Serial0/0/0 from LOADING to FULL, Loading Done

Bogota3(config-router)#network 172.29.3.4 0.0.0.3 area 1
Bogota3(config-router)#network 172.29.3.4 0.0.0.3 area 1

14:29:36: %OSPF-5-ADJCHG: Process 2, Nbr 209.17.220.5 on Serial0/1/1 from LOADING to FULL, Loading Done

Bogota3(config-router)#network 172.29.3.12 0.0.0.3 area 1
Bogota3(config-router)#
14:30:19: %OSPF-5-ADJCHG: Process 2, Nbr 172.29.3.14 on Serial0/1/0 from LOADING to FULL, Loading Done

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

Los routers Bogota1 y Medellín1 deberán añadir a su configuración de enrutamiento una ruta por defecto hacia el ISP y, a su vez, redistribuirla dentro de las publicaciones de OSPF.

Medellin1:

E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is 209.17.220.2 to network 0.0.0.0

172.29.0.0/16 is variably subnetted, 8 subnets, 3 masks
O 172.29.4.0/25 [110/65] via 172.29.6.2, 00:52:45, Serial0/0/0
C 172.29.6.0/30 is directly connected, Serial0/0/0

L 172.29.6.1/32 is directly connected, Serial0/0/0
O 172.29.6.4/30 [110/128] via 172.29.6.10, 00:52:45, Serial0/0/1
[110/128] via 172.29.6.2, 00:52:45, Serial0/0/0
C 172.29.6.8/30 is directly connected, Serial0/0/1
L 172.29.6.9/32 is directly connected, Serial0/0/1
C 172.29.6.12/30 is directly connected, Serial0/1/0
L 172.29.6.13/32 is directly connected, Serial0/1/0
209.17.220.0/24 is variably subnetted, 2 subnets, 2 masks
C 209.17.220.0/30 is directly connected, Serial0/1/1
L 209.17.220.1/32 is directly connected, Serial0/1/1
S* 0.0.0.0/0 [1/0] via 209.17.220.2

Bogotá1:

E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is 209.17.220.6 to network 0.0.0.0

172.29.0.0/16 is variably subnetted, 7 subnets, 2 masks
C 172.29.3.0/30 is directly connected, Serial0/0/0
L 172.29.3.1/32 is directly connected, Serial0/0/0
C 172.29.3.4/30 is directly connected, Serial0/1/1
L 172.29.3.5/32 is directly connected, Serial0/1/1
C 172.29.3.8/30 is directly connected, Serial0/0/1
L 172.29.3.9/32 is directly connected, Serial0/0/1

O 172.29.3.12/30 [110/128] via 172.29.3.2, 01:00:54, Serial0/0/0
[110/128] via 172.29.3.10, 01:00:54, Serial0/0/1
209.17.220.0/24 is variably subnetted, 2 subnets, 2 masks
C 209.17.220.4/30 is directly connected, Serial0/1/0
L 209.17.220.5/32 is directly connected, Serial0/1/0
S* 0.0.0.0/0 [1/0] via 209.17.220.6

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

Tabla 23. Red Sumarizada. Medellín

10101100	00011101	00000100	00000000	172.29.4.0/25
10101100	00011101	00000100	10000000	172.29.4.128/25
10101100	00011101	00000110	00000100	172.29.6.4/30
10101100	00011101	00000110	00001000	172.29.6.8/30
10101100	00011101	00000110	00001100	172.29.6.12/30
10101100	00011101	00000110	00000000	172.29.6.0/30
10101100	**00011101**	**00000100**	**00000000**	**172.29.4.0/22**

Red Sumarizada. Bogotá

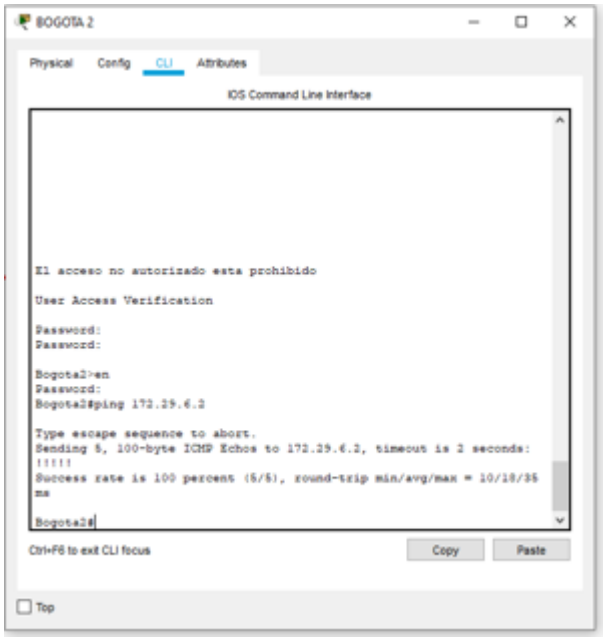
10101100	00011101	00000000	00000000	172.29.0.0/24
10101100	00011101	00000001	00000000	172.29.1.0/24

10101100	00011101	00000011	00001100	172.29.3.12/30
10101100	00011101	00000011	00001000	172.29.3.8/30
10101100	00011101	00000011	00000000	172.29.3.0/30
10101100	00011101	00000011	00000100	172.29.3.4/30
10101100	**00011101**	**00000000**	**00000000**	**172.29.0.0/22**

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

Con el comando ping, se comprueba conectividad entre Medellín y Bogotá

Registro Fotográfico. Conectividad entre Medellín y Bogotá



4.3. TABLA DE ENRUTAMIENTO.

Verificar la tabla de enrutamiento en cada uno de los routers para comprobar

las redes y sus rutas.

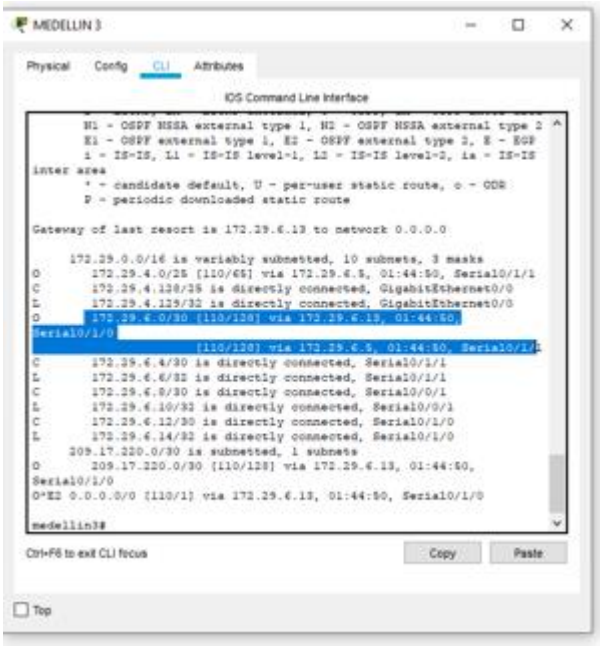
- Show ip route

  Registro Fotográfico. Tabla de Enrutamiento Medellín3

Verificar el balanceo de carga que presentan los routers.

- Show ip route

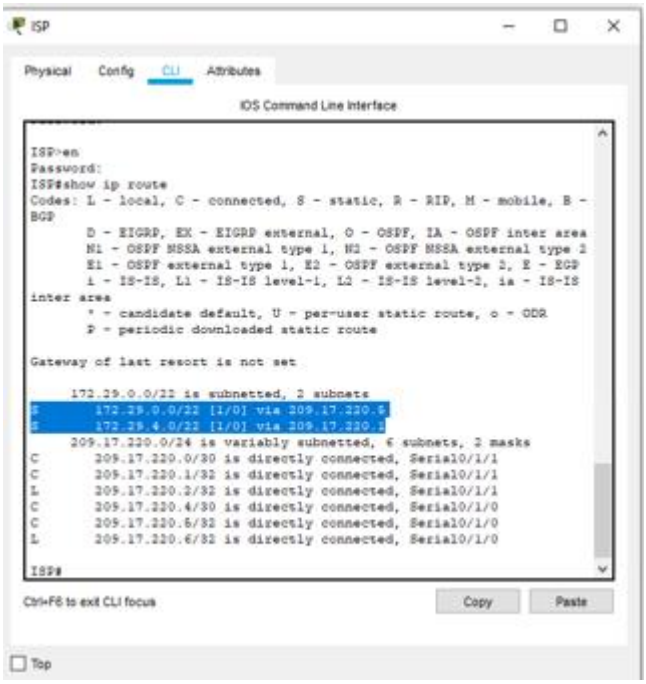
Se comprueba que para un destino tiene dos interfaces



Obsérvese en los routers Bogotá1 y Medellín1 cierta similitud por su ubicación, por tener dos enlaces de conexión hacia otro router y por la ruta por defecto que manejan.

Los routers Medellín2 y Bogotá2 también presentan redes conectadas directamente y recibidas mediante OSPF.

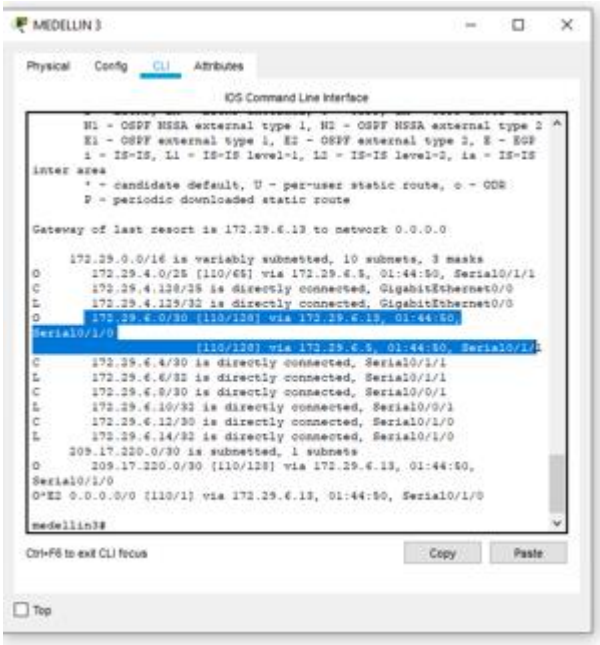
- Show ip route
  Registro Fotográfico. Rutas Estáticas ISP



Las tablas de los routers restantes deben permitir visualizar rutas redundantes para el caso de la ruta por defecto.

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

- El balanceo de carga hace referencia a rutas redundantes



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

4.4. DESHABILITAR LA PROPAGACIÓN DEL PROTOCOLO OSPF.

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

ROUTER	INTERFAZ
Bogota1	SERIAL0/0/1; SERIAL0/1/0; SERIAL0/1/1
Bogota2	SERIAL0/0/0; SERIAL0/0/1
Bogota3	SERIAL0/0/0; SERIAL0/0/1; SERIAL0/1/0
Medellín1	SERIAL0/1/0; SERIAL0/0/1; SERIAL0/1/1
Medellín2	SERIAL0/0/0; SERIAL0/0/1
Medellín3	SERIAL0/0/0; SERIAL0/0/1; SERIAL0/1/0
ISP	No lo requiere

```
BOGOTA1(config)#router ospf 1
BOGOTA1(config-router)#passive-interface s0/1/0

BOGOTA2(config)#router osp
BOGOTA2(config-router)#passive-interface g0/0

BOGOTA3(config)#router ospf 1
BOGOTA3(config-router)#passive-interface g0/0

MEDELLIN1(config)#router ospf 1
MEDELLIN1(config-router)#passive-interface s0/1/1

MEDELLIN2(config)#router ospf 1
MEDELLIN2(config-router)#passive-interface g0/0

MEDELLIN3(config)#router ospf 1
MEDELLIN3(config-router)#passive-interface g0/0
```

Estas configuraciones ya se hicieron al realizar el protocolo OSPF

4.5. VERIFICACIÓN DEL PROTOCOLO OSPF.

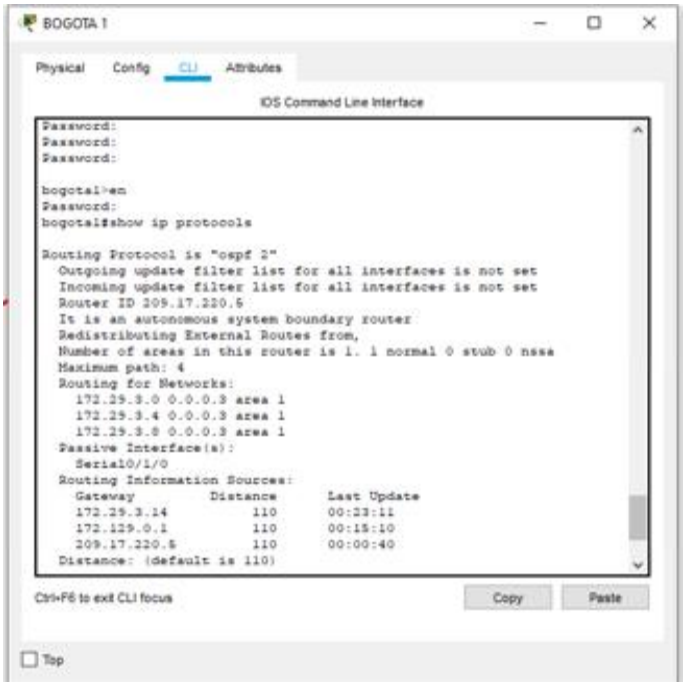
Verificar y documentar las opciones de enrutamiento configuradas en los routers, como el passive interface para la conexión hacia el ISP, la versión de OSPF y las interfaces que participan de la publicación entre otros datos.

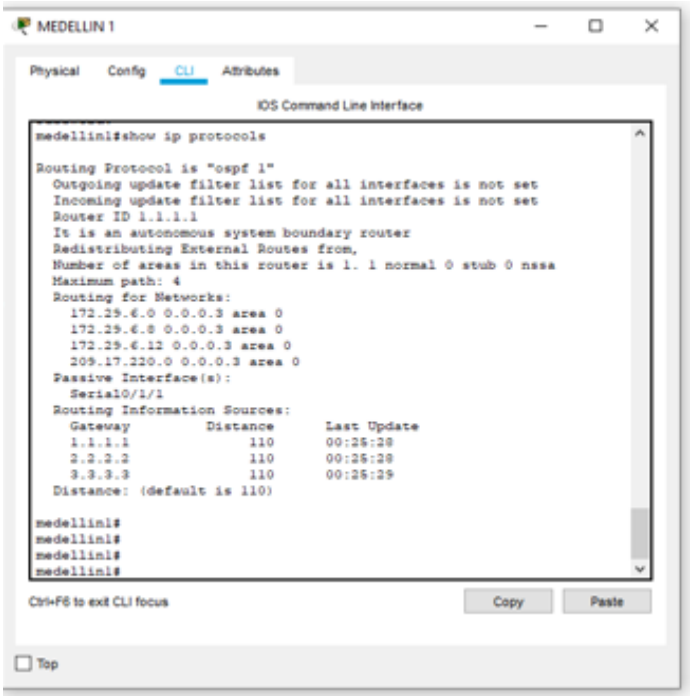
Para verificar el protocolo OSPF se utiliza el comando show ip protocols, el cual nos permite ver ID del router, las redes que anuncia el router, los vecinos de los que el router recibe actualizaciones y la distancia administrativa

predeterminada, que para OSPF es 110.

- MEDELLIN1#show ip protocols
- BOGOTA1#show ip protocols

Registro Fotográfico. Verificación Protocolo OSPF Bogotá1 Medellin1



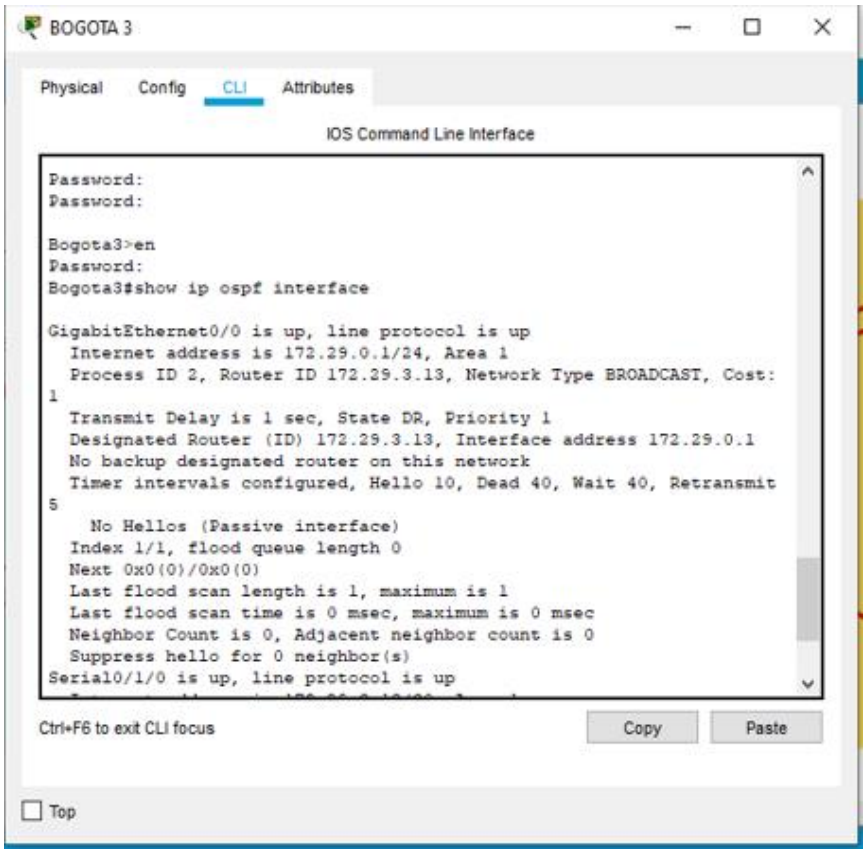


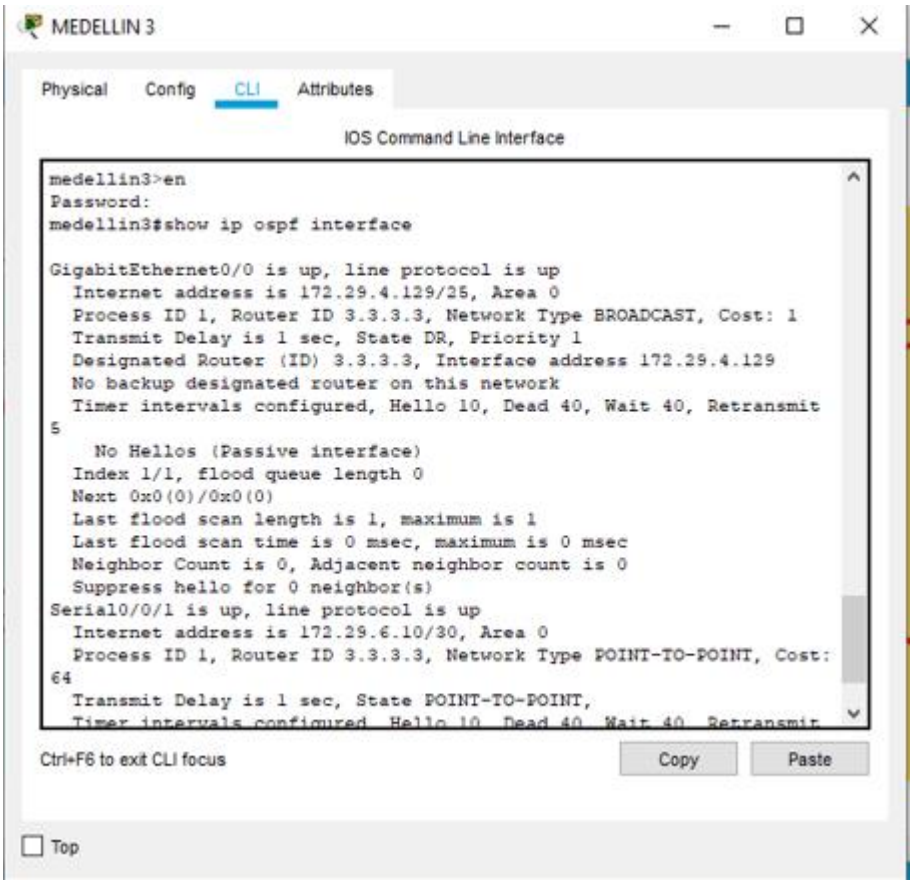
Verificar y documentar la base de datos de OSPF de cada router, donde se informa de manera detallada de todas las rutas hacia cada red.

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

- BOGOTA3#show ip ospf interface

Registro Fotográfico. Lista de Interfaces


BOGOTA 3
Physical
Config
CLI
Attributes
IOS Command Line Interface
Password:
Password:
Bogota3>en
Password:
Bogota3#show ip ospf interface
GigabitEthernet0/0 is up, line protocol is up
Internet address is 172.29.0.1/24, Area 1
Process ID 2, Router ID 172.29.3.13, Network Type BROADCAST, Cost:
1
Transmit Delay is 1 sec, State DR, Priority 1
Designated Router (ID) 172.29.3.13, Interface address 172.29.0.1
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit
5
No Hellos (Passive interface)
Index 1/1, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)
Serial0/1/0 is up, line protocol is up
Ctrl+F6 to exit CLI focus
Copy
Paste
Top



4.6. CONFIGURAR ENCAPSULAMIENTO Y AUTENTICACIÓN PPP.

Según la topología se requiere que el enlace medellín1 con ISP sea configurado con autenticación PAP

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

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

El enlace Bogotá1 con ISP se debe configurar con autenticación CHAP.

- ISP(config)#username BOGOTA1 password cisco
- ISP(config)#int s0/0/1
- ISP(config-if)#encapsulation ppp
- ISP(config-if)#ppp authentication chap

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

4.7. CONFIGURACIÓN DE PAT.

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

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

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

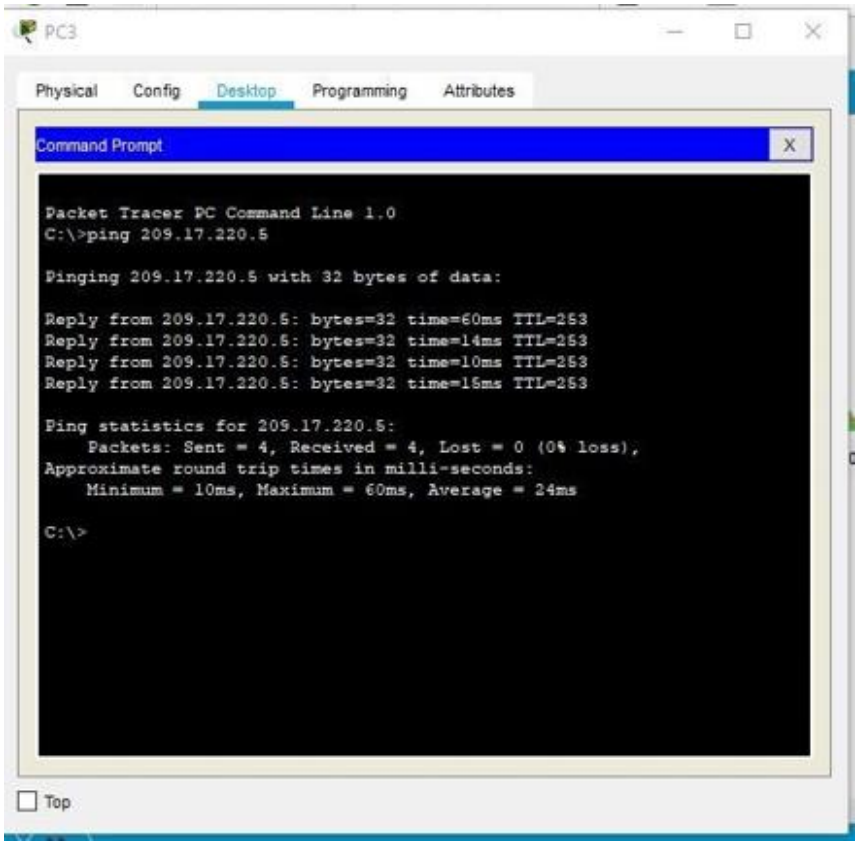
Proceda a configurar el NAT en el router Bogotá1. Compruebe que la traducción de direcciones indique las interfaces de entrada y de salida. Al realizar una prueba de ping, la dirección debe ser traducida automáticamente a la dirección de la interfaz serial 0/1/0 del router Bogotá1, cómo diferente puerto.

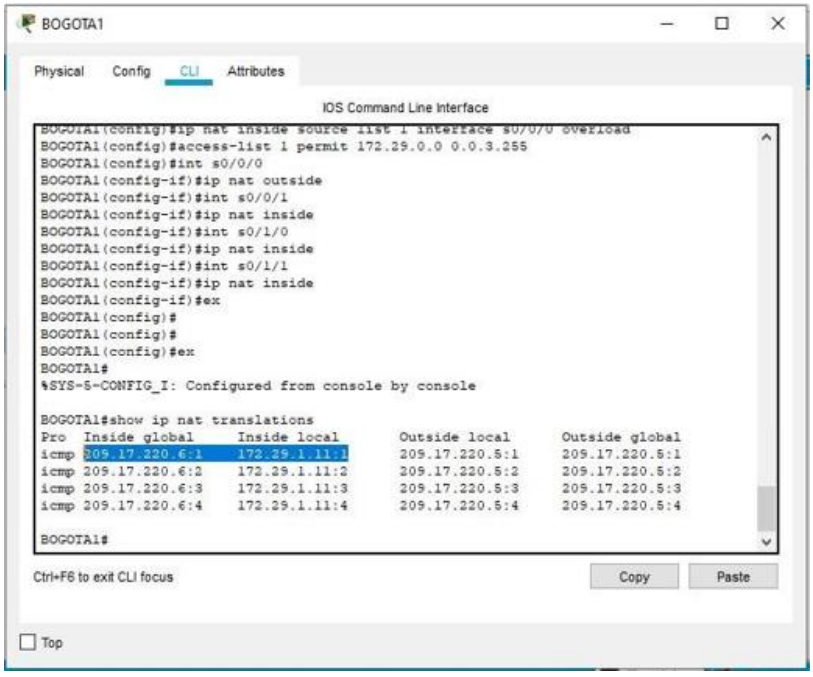
- BOGOTA1(config)#ip nat inside source list 1 interface s0/0/0 overload
- BOGOTA1(config)#access-list 1 permit 172.29.0.0 0.0.3.255
- BOGOTA1(config)#int s0/1/1

- BOGOTA1(config-if)#ip nat outside
- BOGOTA1(config-if)#int s0/0/0
- BOGOTA1(config-if)#ip nat inside
- BOGOTA1(config-if)#int s0/1/1
- BOGOTA1(config-if)#ip nat inside
- BOGOTA1(config-if)#int s0/1/1
- BOGOTA1(config-if)#ip nat inside

Se realiza prueba de ping y con el comando show ip nat translations se visualiza la traducción de la dirección automáticamente a la dirección de la interfaz serial 0/1/0 del router Bogotá1.

Registro Fotográfico. Comando show ip nat translations





4.8. CONFIGURACIÓN DEL SERVICIO DHCP.

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

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

- MEDELLIN2(config)#ip dhcp excluded-address 172.29.4.1 172.29.4.10
- MEDELLIN2(config)#ip dhcp excluded-address 172.29.4.129172.29.4.138
- MEDELLIN2(config)#ip dhcp pool PMED2
- MEDELLIN2(dhcp-config)#net 172.29.4.0 255.255.255.128
- MEDELLIN2(dhcp-config)#default-router 172.29.4.1
- MEDELLIN2(dhcp-config)#dns-server 8.8.8.8
- MEDELLIN2(dhcp-config)#ex

- MEDELLIN2(config)#ip dhcp pool MED3
- MEDELLIN2(dhcp-config)#net 172.29.4.128 255.255.255.128
- MEDELLIN2(dhcp-config)#default-router 172.29.4.129
- MEDELLIN2(dhcp-config)#dns-server 8.8.8.8

Acceso de PC1 a DHCP

MEDELLIN3(config)#int g0/0
MEDELLIN3(config-if)#ip helper-address 172.29.6.5
Configuración IP DHCP en PC0 y PC1 véase anexo 23
Configurar la red Bogotá2 y Bogotá3 donde el router Bogotá2 debe ser el servidor DHCP para ambas redes Lan.

Configure el router Bogotá1 para que habilite el paso de los mensajes Broadcast hacia la IP del router Bogotá2.

- BOGOTA2(config)#ip dhcp excluded-address 172.29.1.1 172.29.1.10
- BOGOTA2(config)#ip dhcp excluded-address 172.29.0.1 172.29.0.10
- BOGOTA2(config)#ip dhcp pool BOGOTA2
- BOGOTA2(dhcp-config)#net 172.29.1.0 255.255.255.0
- BOGOTA2(dhcp-config)#default-router 172.29.1.1
- BOGOTA2(dhcp-config)#dns-server 0.0.0.0
- BOGOTA2(dhcp-config)#ex

- BOGOTA2(config)#ip dhcp pool BOGOTA3
- BOGOTA2(dhcp-config)#net 172.29.0.0 255.255.255.0
- BOGOTA2(dhcp-config)#default-router 172.29.0.1
- BOGOTA2(dhcp-config)#dns-server

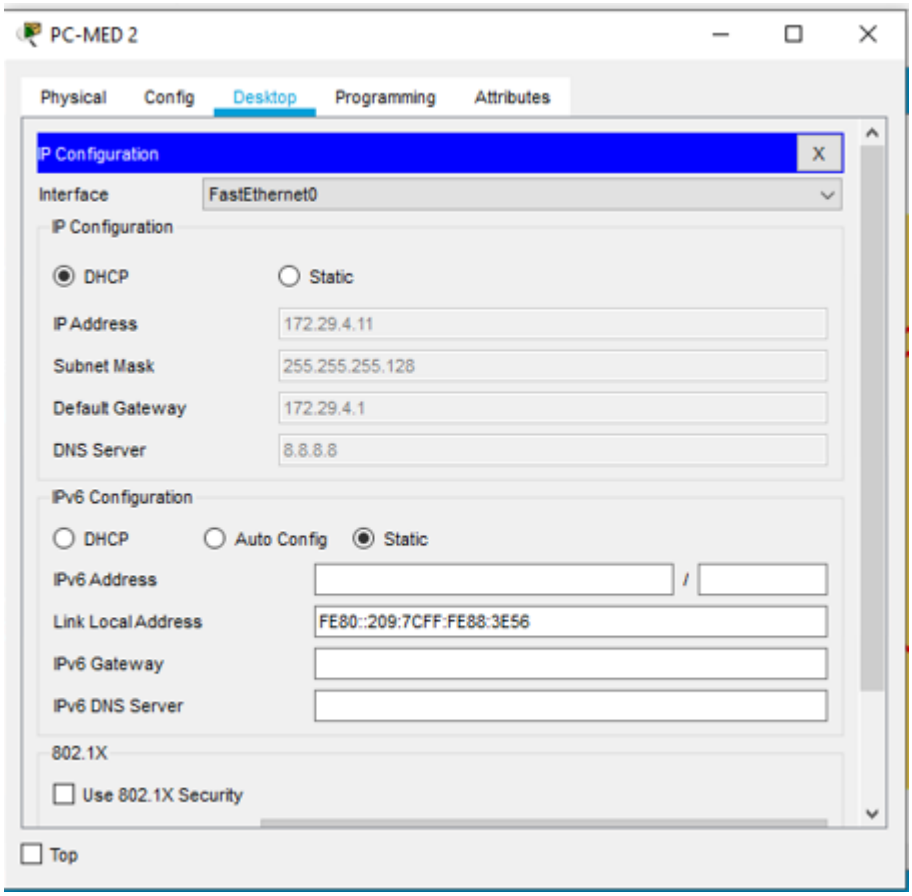
0.0.0.0 Acceso de PC2 a DHCP

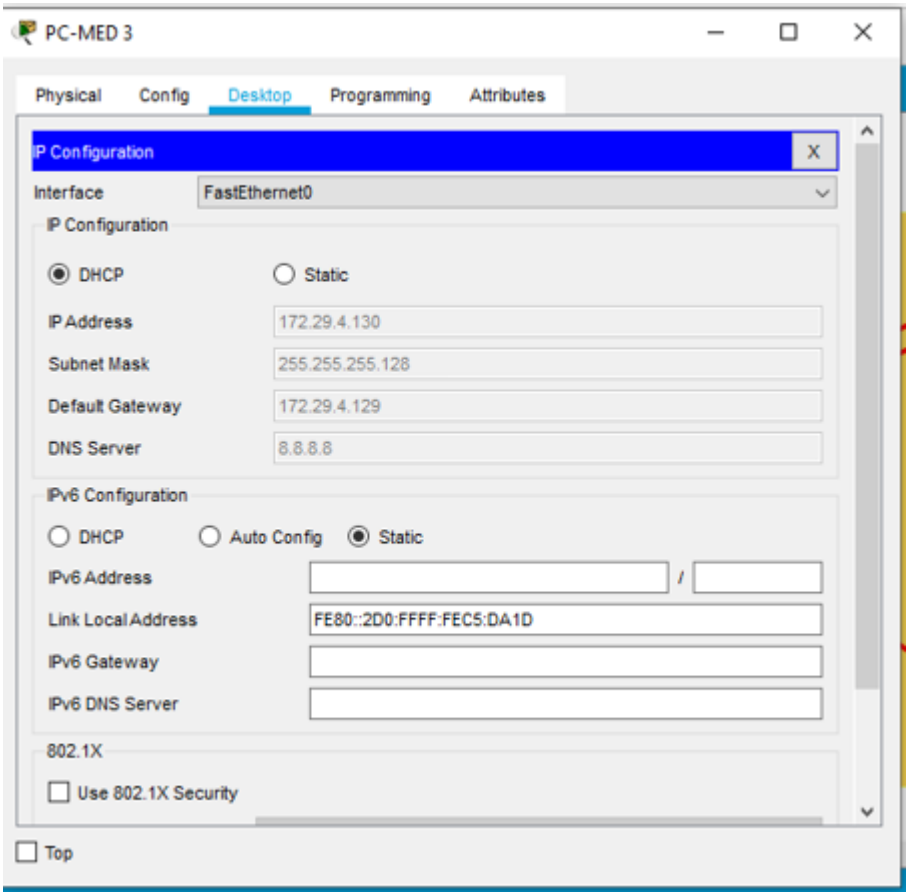
BOGOTA3(config)#int g0/0

BOGOTA3(config-if)#ip helper-address

172.29.3.13 Configuración IP DHCP en PC2 y PC3

Registro Fotográfico. Configuración IP DHCP PC0 – PC1




PC-MED 3
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IP Address
172.29.4.130
Subnet Mask
255.255.255.128
Default Gateway
172.29.4.129
DNS Server
8.8.8.8
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
/
Link Local Address
FE80::2D0:FFFF:FEC5:DA1D
IPv6 Gateway
IPv6 DNS Server
802.1X
Use 802.1X Security
Top

5. CONCLUSIONES

En el transcurso de todas las actividades en la plataforma cisco , se logran realizar de manera gradual los procedimientos básicos para la configuración de una red básica como compleja, donde se logra identificar, analizar y configurar dispositivos de red según las necesidades requeridas durante el desarrollo de toda la asignatura se logra comprender la importancia que debe tener todo equipo en la red, desde asignarle una ip hasta implementar protocolos de seguridad en las diferentes capaz y otros y otros apartados concluyendo así una red confiable y robusta.

Durante el aprendizaje del curso en el ámbito profesional ha aportado al conocimiento fundamental en mi perfil dando apreciaciones sobre temas relacionados con redes, me siento con plena confianza en abordar estos temas ya que el curso me brindo las suficientes bases para realizar argumentos técnicos en en la materia

BIBLIOGRAFIA

Cisco Networking Academy. En línea. Disponible en: https://www.netacad.com/es. Marzo 2020.

Cisco Networking Academy. En línea. Disponible en: https://www.netacad.com/es; 2020, ConfiguringBasic Single-Area OSPFv2. Marzo 2020.

CISCO. CCNA Exploration. Conceptos y protocolos de enrutamiento. Cuarta version. México. CISCO NETWORKING ACADEMY, 2011.

DI TOMMASO, Leandro. “configuración de VLANS con CISCO: Micro Ways” {En línea}. {6 agosto de 2009} disponible en: (https://www.mikroways.net/2009/08/05/configuracion-de-vlans-con-cisco/)

LÓPEZ BULLA, Ricardo. “Enrutamiento y configuración de redes: Fundación Universitaria del Área Andina” {En línea}. {10 septiembre de 2018} disponible en: (https://digitk.areandina.edu.co/bitstream/handle/areandina/1495/74%20ENRUTAMIENTO%20Y%20CONFIGURACI%C3%93N%20DE%20REDES.pdf?sequence=1&isAllowed=y)

VEATO, V. Tommaso. Redes locales y globales en línea. mayo de 2015. Disponible en: https://sites.google.com/site/redeslocalesyglobales/4-configuracion-de- red/2-configuracion-de-routers/6-configuracion-del-encaminamiento/2- encaminamiento-dinamico/6-protocolo-ospf/6-configuracion-del-protocolo-osp