PRUEBA DE HABILIDADES PRÁCTICAS CCNA2

KEVIN DAVID OÑATE VILLA

UNIVERSIDAD NACIONAL ABIERTA Y ADISTANCIA UNAD
INGENIERÍA DE SISTEMAS
DIPLOMADO CISCO
VALLEDUPAR
2020

DESARROLLO PRUEBA DE HABILIDADES
PRÁCTICAS CCNA2

KEVIN DAVID OÑATE VILLA

INFORME DE CONFIGURACION DE DOS ESCENARIOS CON TECNOLOGIA CISCO PARA OPTAR POR EL TITULO DE INGENIERO DE SISTEMAS.

TUTOR: HECTOR JULIAN PARRA

UNIVERSIDAD NACIONAL ABIERTA Y ADISTANCIA UNAD
INGENIERÍA DE SISTEMAS
DIPLOMADO CISCO
VALLEDUPAR
2020

Nota de Aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Valledupar, 03 de Mayo de 2020

Dedicatoria:

Doy gracias a Dios, a cada uno de mis familiares y tutores que me motivaron a seguir adelante y lograr culminar satisfactoriamente esta gran etapa que estoy dando en mi vida profesional.

AGRADECIMIENTOS

Dedico mis agradecimientos principalmente a Dios por toda la sabiduría que me regala para poder desempeñarme, en segundo lugar, a mis abuelos, mis padres y familiares quienes siempre han sido una base fundamental en mi crecimiento como un ser integral formado en conocimientos y valores.

También expreso mi gratitud con cada uno de mis tutores y compañeros que al interactuar crecimos juntos aprendiendo nuestras habilidades e intercambiando nuestros conocimientos.

CONTENIDO

LISTA DE TABLAS

LISTA DE GRÁFICAS

GLOSARIO

DHCP: 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.

MASCARA DE SUBRED: La máscara de subred o subneting señala qué bytes (o qué porción) de su dirección es el identificador de la red. La máscara consiste en una secuencia de unos seguidos de una secuencia de ceros con el mismo tamaño que una dirección IP (32 bits, o lo que es lo mismo 4 bytes), por ejemplo, una máscara de 20 bits se escribiría 255.255.240.0, es decir como una dirección IP con 20 bits en 1 seguidos por 12 bits en 0, pero para facilitar su lectura se escribe separando bloques de 8 bits (1 byte) con puntos y escribiéndolos en decimal. La máscara determina todos los parámetros de una subred: dirección de red, dirección de difusión (broadcast) y direcciones asignables a nodos de red (hosts).

ROUTER: Es un dispositivo que proporciona conectividad a nivel de red o nivel tres en el modelo OSI. Su función principal consiste en enviar o encaminar paquetes de datos de una red a otra, es decir, interconectar subredes.

RESUMEN

En la solución de esta prueba de habilidades, se abordarán ejercicios mediante dos escenarios dando las soluciones a los problemas planteados como parte de un examen final da habilidades prácticas en el curso CCNA 2;

El primer escenario del problema consiste en: 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.

Y el segundo escenario del problema consiste en: 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.

PALABRAS CLAVE: Configurar, Interface, IP, NAT, Red, Routing, Switches.

1. INTRODUCCIÓN

En la presente prueba de habilidades abordamos dos escenarios bien completos donde demostraremos lo aprendido en los módulos que hemos venido adelantando en cisco.

El primer escenario configuraremos 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.
Y en el segundo escenario 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.

En la solución de estos escenarios se configuran servidores DHCP, el cual es un protocolo de difusión que trabaja de forma predeterminada en donde sus paquetes no pasan a través de enrutadores además se emplean los routers y Switches, que soportan una gran variedad de servicios de red, y que nos permiten a los usuarios conectarnos a la misma.
Algunos de estos servicios pueden restringirse o desactivarse, lo que mejora la seguridad sin que la operación de la red se vea afectada, sin embargo, aunque esto representa un nivel básico de aseguramiento de red.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Demostrar las habilidades prácticas y teóricas desarrolladas a lo largo del diplomado cisco dando solución a los escenarios propuestos para esta evaluación de habilidades.

2.2 OBJETIVOS ESPECÍFICOS

Establecer conectividad entre los dispositivos necesarios siguiendo topologías de red indicadas.

Implementar las topologías según los requerimientos.

Configurar los protocolos de enrutamientos necesarios para lograr las conexiones.

Comprobar a través de comandos como Ping que las conexiones establecidas están bien configuradas.

3 PLANTEAMIENTO DEL PROBLEMA

3.1 DEFINICIÓN DEL PROBLEMA

Tenemos dos problemas por solucionar a continuación los describimos:
El primer escenario configuraremos 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.
Y en el segundo escenario 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.

3.2 JUSTIFICACIÓN

En los escenarios propuestos se debe configurar por medio de comandos y protocolos ya establecidos lo que nos permite demostrar las habilidades prácticas y teóricas desarrolladas a lo largo del diplomado cisco dando solución a los escenarios propuestos para esta evaluación de habilidades.
El desarrollo de problemas como estos permite fortalecer los conocimientos adquiridos implementando topologías de red y configuraciones de los dispositivos logrando los enrutamientos propuestos.

4. MARCO TEÓRICO

Uso del simulador de redes Cisco Packet Tracer: es un programa de simulación de redes que permite a los estudiantes experimentar con el comportamiento de la red y resolver preguntas.

Características: soporta un conjunto de Protocolos de capa de aplicación simulados, al igual que enrutamiento básico con RIP, OSPF, y EIGRP.. Aunque Packet Tracer provee una simulación de redes funcionales, utiliza solo un pequeño número de características encontradas en el hardware real corriendo una versión actual del Cisco IOS. Packet Tracer no es adecuado para redes en producción.

En este programa se crea la topología física de la red simplemente arrastrando los dispositivos a la pantalla. Luego haciendo clic sobre ellos se puede ingresar a sus consolas de configuración. Allí están soportados todos los comandos del Cisco IOS e incluso funciona el "tab completion". Una vez completada la configuración física y lógica de la red, también se pueden hacer simulaciones de conectividad (pings, traceroutes) todo ello desde las mismas consolas incluidas.

Una de las grandes ventajas de utilizar este programa es que permite "ver" (opción "Simulation") cómo deambulan los paquetes por los diferentes equipos (switchs, routers, PC), además de poder analizar de forma rápida el contenido de cada uno de ellos en las diferentes "capas" y "datos".

5. MATERIALES Y MÉTODOS

5.1 MATERIALES

Los materiales que se usaron en el desarrollo del primer escenario son:

1 Servidor de internet
3 Router
2 Switch 2960
2 PC
Cables Serial y Ethernet

Los materiales que se usaron en el desarrollo del segundo escenario son:

7 Router
4 PC
Cables Serial y Ethernet

5.2 METODOLOGÍA

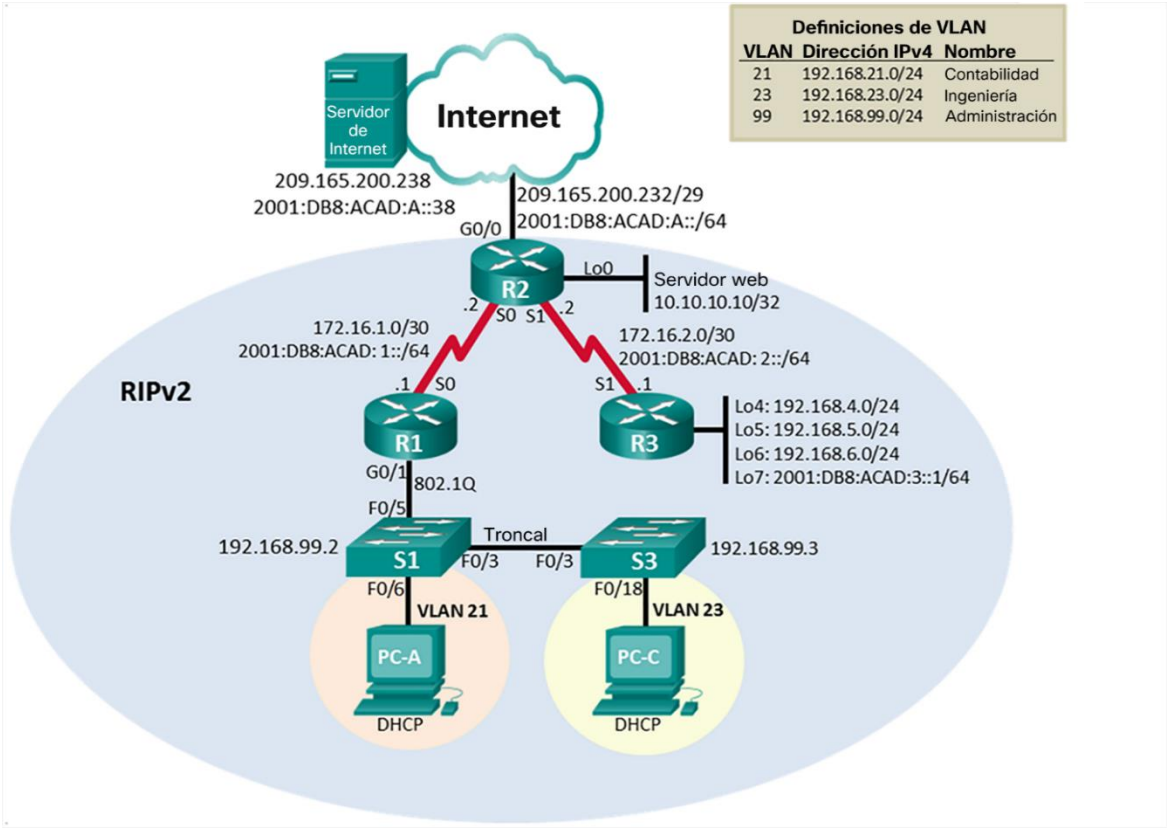
En el desarrollo del trabajo diseñamos las topologías, aprovechamos las tablas para los direccionamientos IP y utilizamos OSPF como protocolo de enrutamiento, considerando que se tendrán rutas por defecto redistribuidas; asimismo, habilitar el encapsulamiento PPP y su autenticación.

6 DESARROLLO DEL PROYECTO

6.1 DESARROLLO DEL ESCENARIO 1:

Escenario 1: Se debe configurar una red pequeña para que admita conectividad IPv4 e IPv6, seguridad de switches, routing entre VLAN, el protocolo de routing dinámico RIPv2, el protocolo de configuración de hosts dinámicos (DHCP), la traducción de direcciones de red dinámicas y estáticas (NAT), listas de control de acceso (ACL) y el protocolo de tiempo de red (NTP) servidor/cliente. Durante la evaluación, probará y registrará la red mediante los comandos comunes de CLI.

Topología



Gráfica 1. Topología Escenario 1

Parte 1: Inicializar dispositivos

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

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

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

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	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	Dir.flash show vlan show vlan brief

Tabla 1. Inicialización de routers y switch

Parte 2: Configurar los parámetros básicos de los dispositivos

Paso 1: Configurar la computadora de Internet

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

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.225
Dirección IPv6/subred	2001:DB8: ACAD: A::38
Gateway predeterminado IPv6	2001:DB8: ACAD:2::1

Tabla 2. Configuración de la computadora de Internet

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

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	No ip domain-lookup
Nombre del router	Hostname R1
Contraseña de exec privilegiado cifrada	Enable secret class
Contraseña de acceso a la consola	Line con 0 Enable password Cisco
Contraseña de acceso Telnet	Line vty 0 4 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 conexion a R2 Establecer la dirección IPv4: Ip address 172.16.1.1 255.255.255.252 Establecer la dirección IPv6: 2001:DB8: ACAD:1::1 Establecer la frecuencia de reloj en 128000: Clock rate 128000 Activar la interfaz: No shutdown

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 address 2001:DB8: ACAD:1::1/64

Tabla 3. Configuración de router R1

Nota: Todavía no configure G0/1.

Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	No ip domain-lookup
Nombre del router	Hostname R2
Contraseña de exec privilegiado cifrada	Enable secret class
Contraseña de acceso a la consola	Line con 0 Enable password Cisco login
Contraseña de acceso Telnet	Line vty 0 4 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 $

Interfaz S0/0/0	Establezca la descripción: Interface s0/0/0 Description conexion a R1 Establecer la dirección IPv4: Ip address 172.16.1.2 255.255.255.252 Establecer la dirección IPv6: 2001:DB8: ACAD:1::2 Activar la interfaz: No shutdown
Interfaz S0/0/1	Establezca la descripción: Interface s0/0/1 Description conexion a R3 Establecer la dirección IPv4: Ip address 172.16.2.1 255.255.255.252 Establecer la dirección IPv6: 2001:DB8: ACAD:2::1 Establecer la frecuencia de reloj en 128000. Clock rate 128000 Activar la interfaz No shutdown
Interfaz G0/0 (simulación de Internet)	Establecer la descripción: Interface g0/0 Description internet Establezca la dirección IPv4: Ip addresss 209.165.200.233 255.255.255.248 Establezca la dirección IPv6: 2001:DB8: ACAD: A::33 Activar la interfaz No shutdown
Interfaz loopback 0 (servidor web simulado)	Establecer la descripción: Interface g0/1 Description conexion a servidor WWW Establezca la dirección IPv4: Ip address 10.10.10.10 255.255.255.0

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 address 2001:DB8: ACAD: A:33/64

Tabla 4. Configuración de router R2

Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	No ip domain-lookup
Nombre del router	Hostname R3
Contraseña de exec privilegiado cifrada	Enable secret class
Contraseña de acceso a la consola	Line con 0 Enable password Cisco
Contraseña de acceso Telnet	Line vty 0 4 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	Establezca la descripción: Interface s0/0/1 Description conexion a R2 Establecer la dirección IPv4: Ip address 172.16.2.2 255.255.255.252 Establecer la dirección IPv6: 2001:DB8: ACAD:2::2 Activar la interfaz: No shutdown
Interfaz loopback 4	Establezca la dirección IPv4: Interface lo4

	Ip address 192.168.4.1 255.255.255.0
Interfaz loopback 5	Establezca la dirección IPv4: Interface lo5 Ip address 192.168.5.1 255.255.255.0
Interfaz loopback 6	Establezca la dirección IPv4: Interface lo6 Ip address 192.168.6.1 255.255.255.0
Interfaz loopback 7	Establezca la dirección IPv6: 2001:DB8: ACAD:3::2
Rutas predeterminadas	Ip route 0.0.0.0 0.0.0.0 s0/0/1

Tabla 5. Configuración de router R3

Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	No ip domain-lookup
Nombre del switch	Hostname S1
Contraseña de exec privilegiado cifrada	Enable secret class
Contraseña de acceso a la consola	Line con 0 Enable password Cisco
Contraseña de acceso Telnet	Line vty 0 4 Password Cisco login
Cifrar las contraseñas de texto no cifrado	Service password-encryption
Mensaje MOTD	Banner motd $ Se prohíbe el acceso no autorizado $

Tabla 6. Configuración de Switch S1

Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	No ip domain-lookup
Nombre del switch	Hostname S3
Contraseña de exec privilegiado cifrada	Enable secret class
Contraseña de acceso a la consola	Line con 0 Enable password Cisco
Contraseña de acceso Telnet	Line vty 0 4 Password Cisco login
Cifrar las contraseñas de texto no cifrado	Service password-encryption
Mensaje MOTD	Banner motd $ Se prohíbe el acceso no autorizado $

Tabla 7. Configuración de Switch S3

Paso 7: Verificar la conectividad de la red

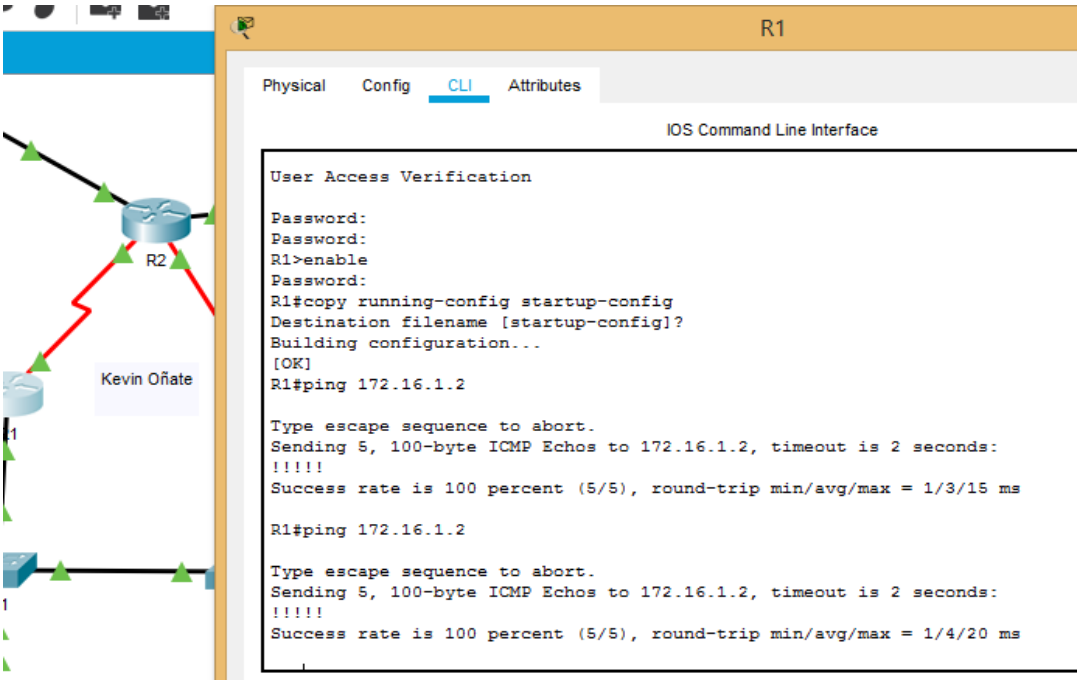
Utilice el comando **ping** para probar la conectividad entre los dispositivos de red.

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

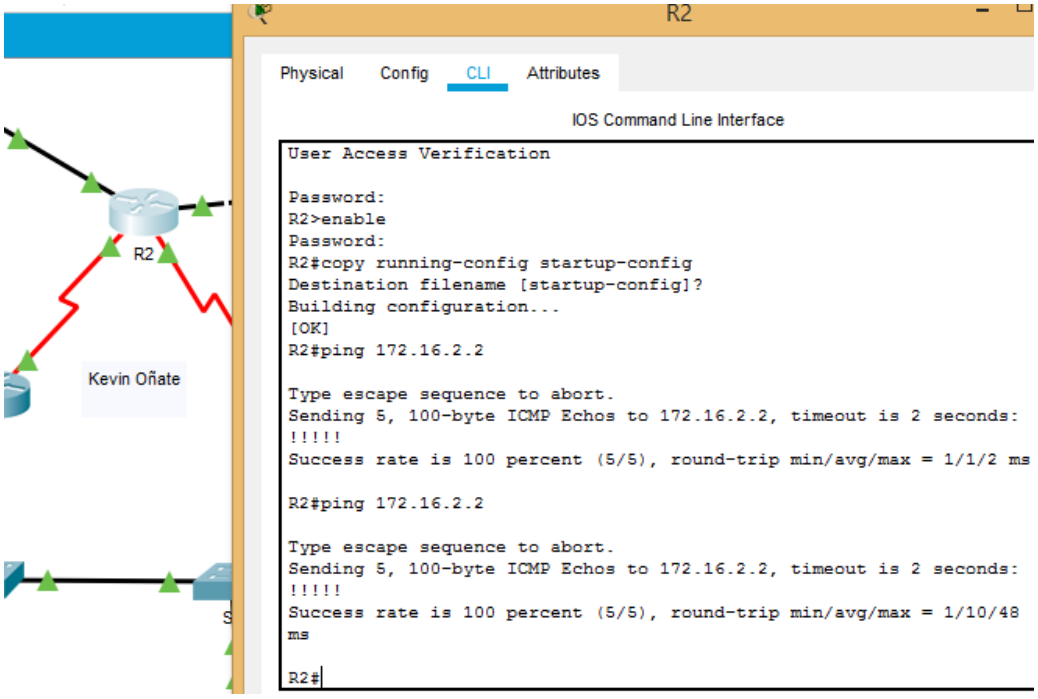
Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	si
R2	R3, S0/0/1	172.16.2.2	si
PC de Internet	Gateway predeterminado	209.165.200.225	si

Tabla 8. Verificación de conectividad

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



Gráfica 2. Ping desde R1



Gráfica 3. Ping desde R2

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

Paso 1: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para topología para crear y nombrar cada una de las VLAN que se indicant: Enable Configure terminal Vlan 21 Name Contabilidad Vlan 33 Name Ingenieria Vlan 99 Name Administracion
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
Asignar el gateway predeterminado	Asigne la primera dirección IPv4 de la subred como el 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 fa0/3 Switchport mode trunk Switchport mode trunk native vlan 1
Forzar el enlace troncal en la interfaz F0/5	Utilizar la red VLAN 1 como VLAN nativa: Interface fa0/5 Switchport mode trunk Switchport mode trunk native vlan 1

Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range: Interface range fa0/1-2, fa0/4, fa0/6-24, g0/1-2 Switchport mode access
Asignar F0/6 a la VLAN 21	Switch trunk native vlan 21: Interface fa0/6 Switchport mode access Switchport mode access native vlan 21
Apagar todos los puertos sin usar	Interface range fa0/1-2, fa0/4, fa0/7-24, g0/1-2 shutdown

Tabla 9. Configuración de vlan en Switch S1

Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Elemento o tarea de configuración	**Especificación**
Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para topología para crear y nombrar cada una de las VLAN que se indicant: Enable Configure terminal Vlan 21 Name Contabilidad Vlan 33 Name Ingenieria Vlan 99 Name Administracion
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 192.168.99.3 255.255.255.0
Asignar el gateway predeterminado.	Asigne la primera dirección IPv4 de la subred como el 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 fa0/3 Switchport mode trunk Switchport mode trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range: Interface range fa0/1-2, fa0/4, fa0/6-24 Switchport mode access
Asignar F0/18 a la VLAN 21	Switch trunk native vlan 23: Interface fa0/18 Switchport mode access Switchport mode access native vlan 23
Apagar todos los puertos sin usar	Interface range fa0/1-2, fa0/4-17, fa0/19-24, g0/1-2 shutdown

Tabla 10. Configuración de vlan en Switch S3

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	Descripción: LAN de Contabilidad: Interface g0/1.21 Encapsulation dot1q 21 Description LAN de Contabilidad Asignar la VLAN 21 Asignar la primera dirección disponible a esta interfaz: Ip address 192.168.21.1 255.255.255.0
Configurar la subinterfaz 802.1Q .23 en G0/1	Descripción: LAN de Ingeniería: Interface g0/1.23 Encapsulation dot1q 23 Description LAN de Ingenieria Asignar la VLAN 23 Asignar la primera dirección disponible a esta interfaz: Ip address 192.168.23.1 255.255.255.0

Configurar la subinterfaz 802.1Q .99 en G0/1	Descripción: LAN de Administración: Interface g0/1.99 Encapsulation dot1q 99 Description LAN de Administracion Asignar la VLAN 99 Asignar la primera dirección disponible a esta interfaz: Ip address 192.168.99.1 255.255.255.0
Activar la interfaz G0/1	No shutdown

Tabla 11. Configuración de vlan en Router R1

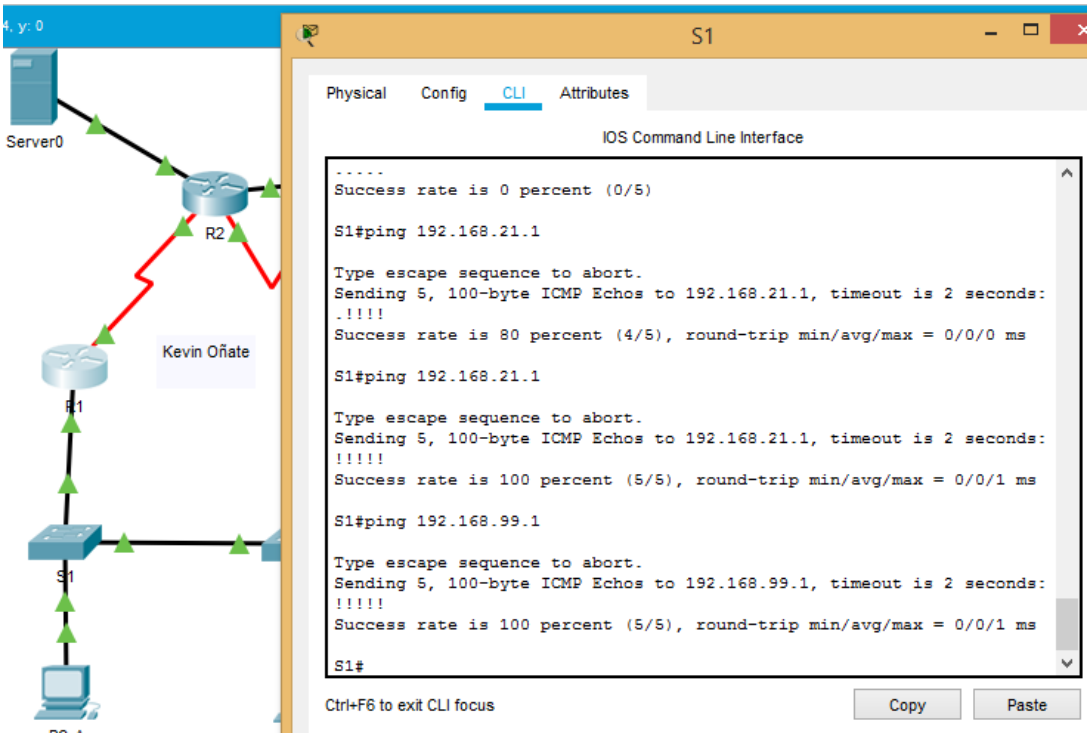
Paso 4: Verificar la conectividad de la red

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

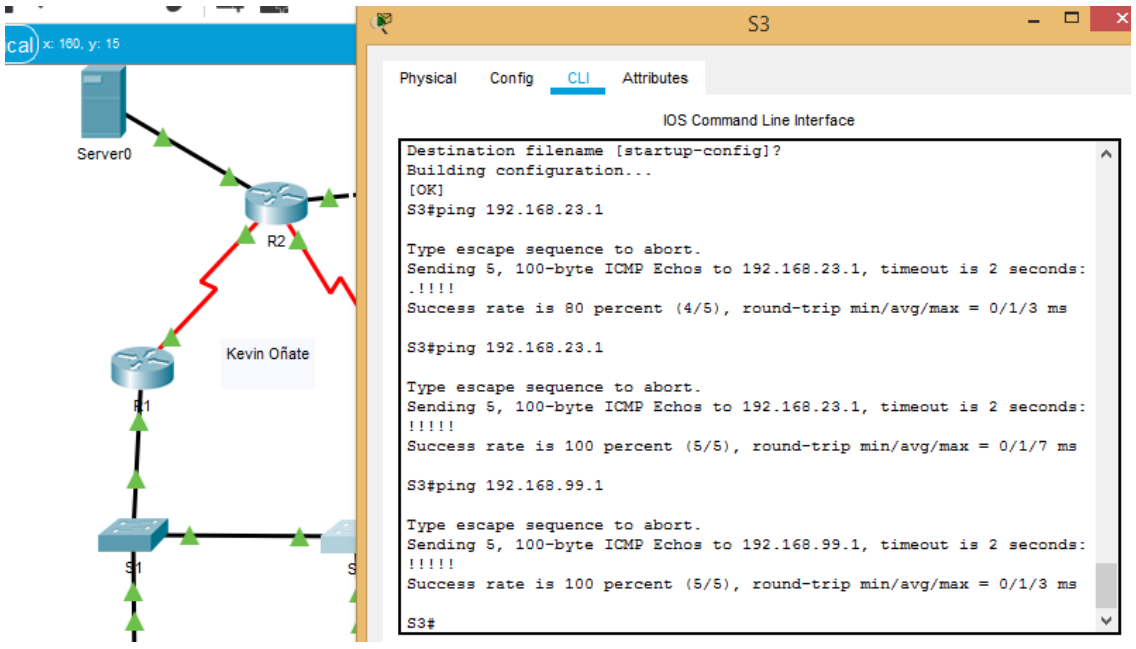
Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

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

Tabla 12. Verificación conectividad de vlan



Gráfica 4. Ping desde S1



Gráfica 5. Ping desde S3

Parte 4: Configurar el protocolo de routing dinámico RIPv2

Paso 1: Configurar RIPv2 en el R1

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	Router rip Version 2
Anunciar las redes conectadas directamente	Asigne todas las redes conectadas directamente. Network 192.168.4.0
Establecer todas las interfaces LAN como pasivas	passive
Desactive la sumarización automática	No auto summary

Tabla 13. Configuración RIPv2 en R1

Paso 2: Configurar RIPv2 en el R2

La configuración del R2 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	Router rip Version 2
Anunciar las redes conectadas directamente	**Nota:** Omitir la red G0/0.
Establecer la interfaz LAN (loopback) como pasiva	Passive l
Desactive la sumarización automática.	No auto summary

Tabla 14. Configuración RIPv2 en R2

Paso 3: Configurar RIPv2 en el R3

La configuración del R3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	Router rip Version 2
Anunciar redes IPv4 conectadas directamente	Network 192.168.4.0
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	passive
Desactive la sumarización automática.	No auto summary

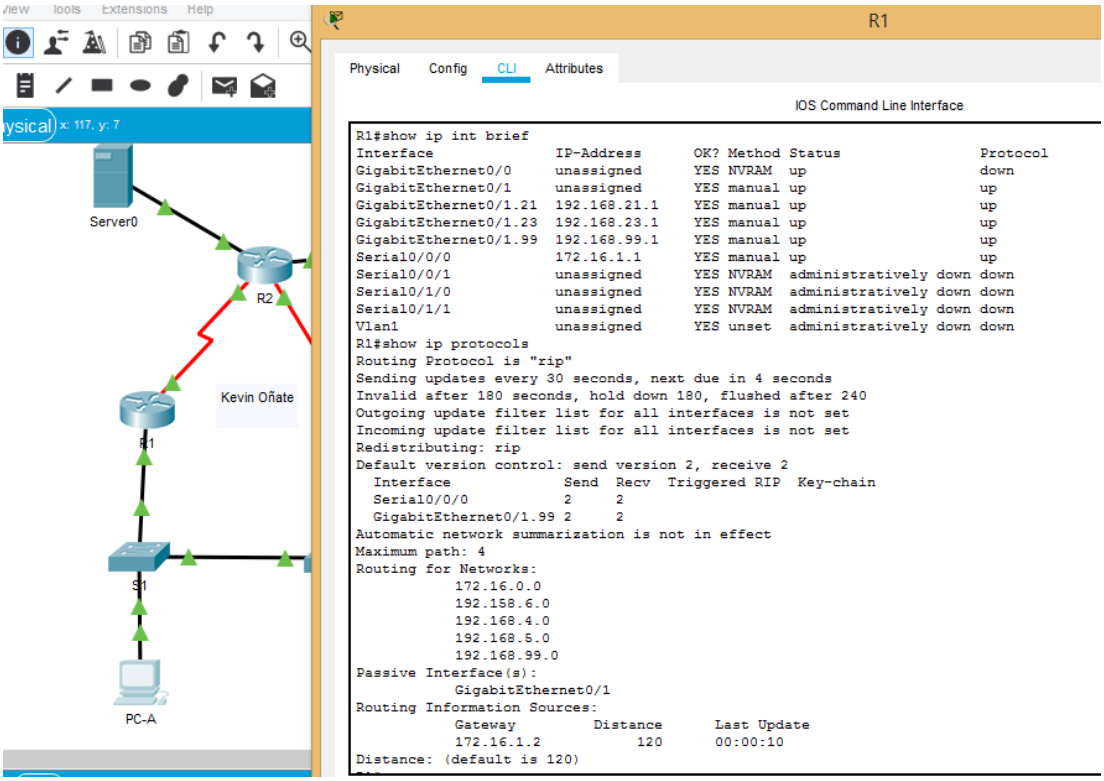
Tabla 15. Configuración RIPv2 en R3

Paso 4: 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?	Show ip int brief Show ip protocols
¿Qué comando muestra solo las rutas RIP?	si
¿Qué comando muestra la sección de RIP de la configuración en ejecución?	Muestran sus propias subredes

Tabla 16. Verificación de la información RIPv2

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



Gráfica 6. Rutas y proceso RIP

Parte 5: Implementar DHCP y NAT para IPv4

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

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	Enable Configure terminal Ip dchp excluded-address 192.168.21.1 192.168.21.20
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	Enable Configure terminal Ip dchp excluded-address 192.168.23.1 192.168.23.20

Crear un pool de DHCP para la VLAN 21.	Nombre: ACCT Ip dhcp pool ACCT Servidor DNS: 10.10.10.10 Dns-server 10.10.10.10 Nombre de dominio: ccna-sa.com Domain-name ccna-sa.com Establecer el gateway predeterminado Default-router 192.168.21.1
Crear un pool de DHCP para la VLAN 23	Nombre: ENGNR Ip dhcp pool ENGNR Servidor DNS: 10.10.10.10 Dns-server 10.10.10.10 Nombre de dominio: ccna-sa.com Domain-name ccna-sa.com Establecer el gateway predeterminado: Default-router 192.168.23.1

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

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

La configuración del R2 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	Nombre de usuario: **webuser** Contraseña: **cisco12345** Nivel de privilegio: **15** **User 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: **209.165.200.229** ip nat inside source static 10.10.10.10 209.165.200.229

Asignar la interfaz interna y externa para la NAT estática	Interface g0/0 Ip nat outside Interface g0/1 Ip nat inside
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: **209.165.200.225 – 209.165.200.228:** Ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248
Definir la traducción de NAT dinámica	Ip nat source inside list 1 pool INTERNET

Tabla 18. Configuración R2 NAT estática y dinámica

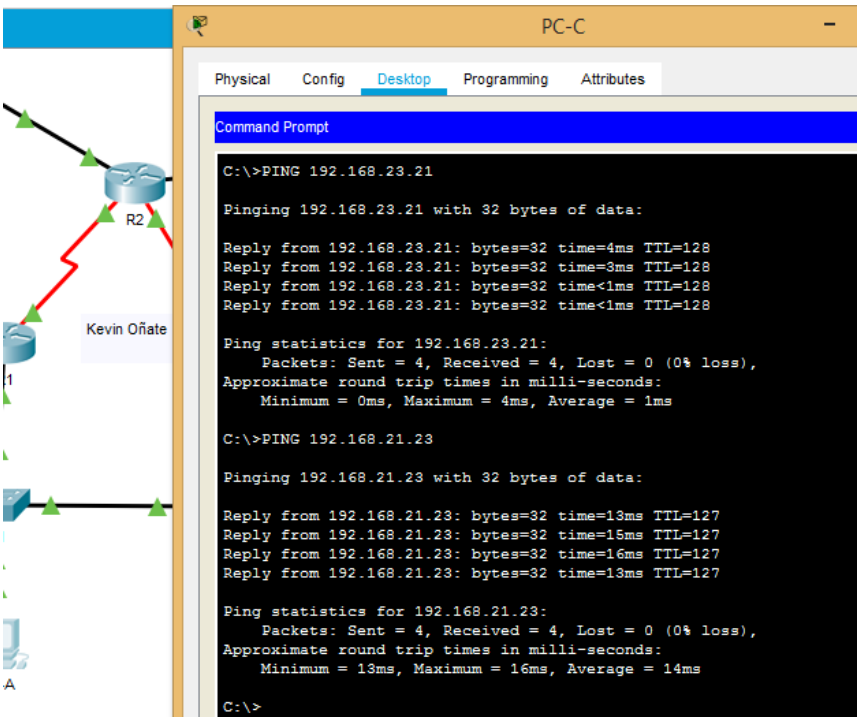
Paso 3: Verificar el protocolo DHCP y la NAT estática

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	IP: 192.168.21.23 NETMASK: 255.255.255.0 GATEWAY: 192.168.21.1 DNS-SERVER: 10.10.10.10

Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	IP: 192.168.23.21 NETMASK: 255.255.255.0 GATEWAY: 192.168.21.1 DNS-SERVER: 10.10.10.10
Verificar que la PC-A pueda hacer ping a la PC-C **Nota:** Quizá sea necesario deshabilitar el firewall de la PC.	SI
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**	Nos muestra la pagina web

Tabla 19. Verificación 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.



Gráfica 7. Configuraciones DHCP y NAT

Parte 6: Configurar NTP

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	**5 de marzo de 2016, 9 a. m.** Clock set 9:00:00 Mar 05 2016
Configure R2 como un maestro NTP.	Nivel de estrato: **5** **Ntp master 5**
Configurar R1 como un cliente NTP.	Servidor: **R2** **Ntp master 1** **Configure terminal** **Ntp server pool.ntp.org**
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	Ntp update-calendar
Verifique la configuración de NTP en R1.	Show ntp status Show ntp associations

Tabla 20. Configuración R1 NTP

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

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

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**
Aplicar la ACL con nombre a las líneas VTY	Line vty 0 4 Access-class ADMIN-MGT in

Permitir acceso por Telnet a las líneas de VTY	telnet 172.16.2.2 connection refused for foreign host telnet 172.16.2.1 connection refused for foreign host
Verificar que la ACL funcione como se espera	si

Tabla 21. Configuración R2 VTY

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

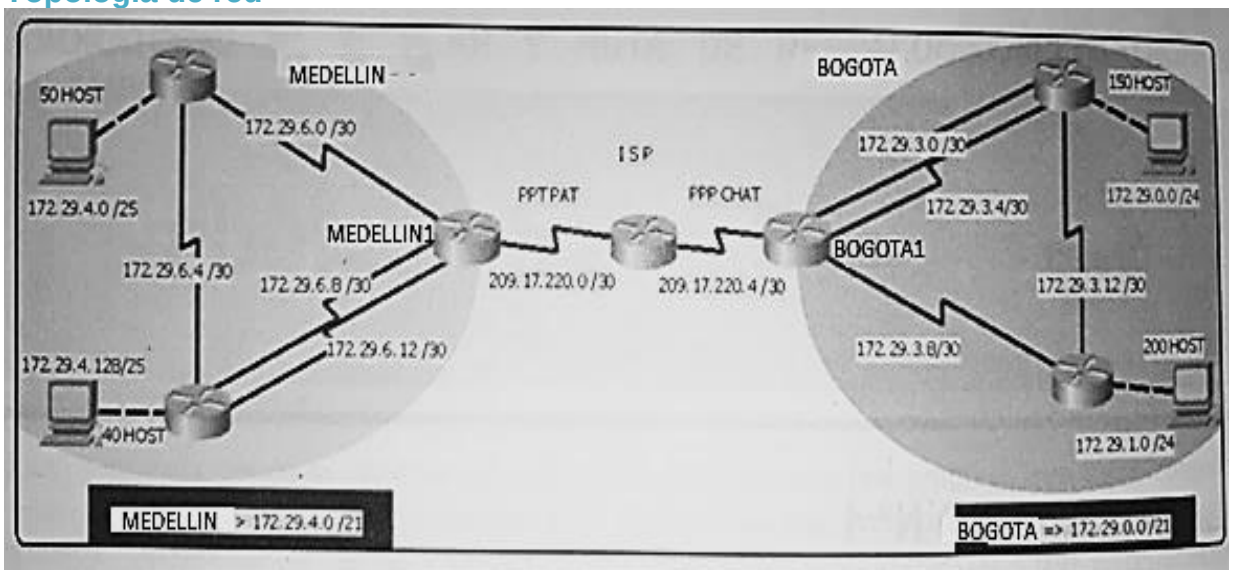
Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	Show access-lists
Restablecer los contadores de una lista de acceso	Clear ip access-list counters
¿Qué comando se usa para mostrar qué ACL se aplica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

Tabla 22. Configuración del comando de CLI

6.2 ANÁLISIS DEL 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.

Topología de red



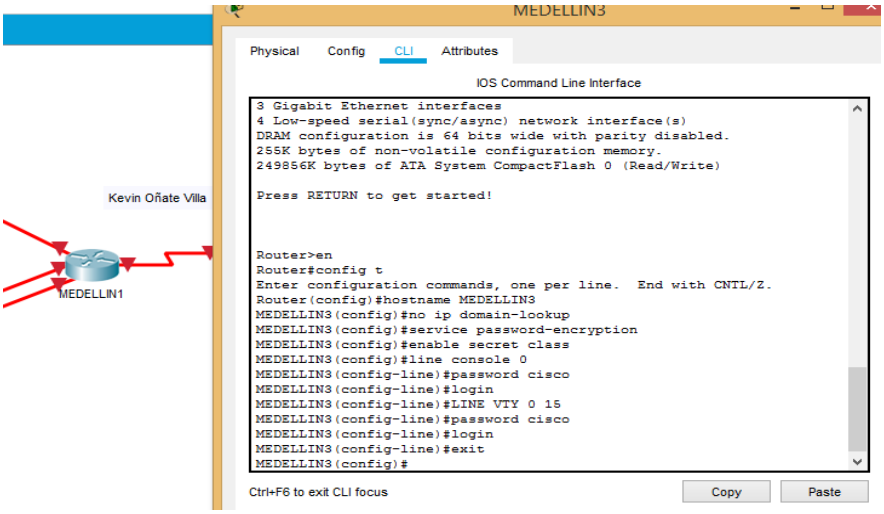
Gráfica 8. Topología Escenario 2

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

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

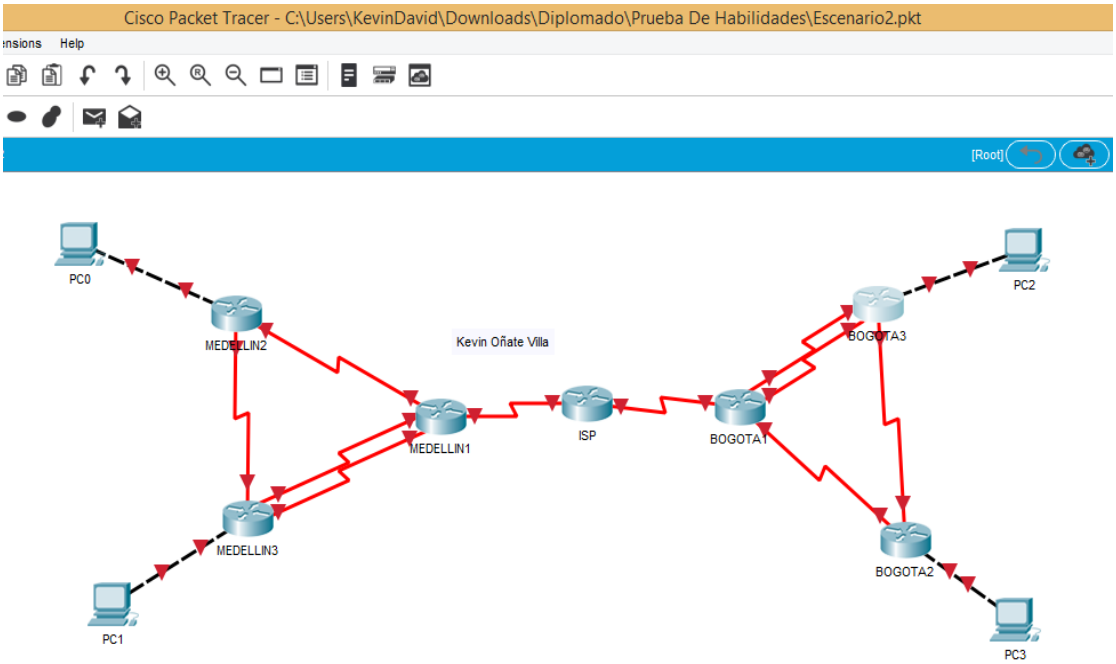
Desarrollo
Como trabajo inicial se debe realizar lo siguiente.
- Realizar las rutinas de diagnóstico y dejar los equipos listos para su configuración (asignar nombres de equipos, asignar claves de seguridad, etc).

Desarrollamos lo siguiente con cada uno de los equipos:



Gráfica 9. Rutinas de diagnosticos

- Realizar la conexión fisica de los equipos con base en la topología de red Configurar la topología de red, de acuerdo con las siguientes especificaciones. Nos queda asi:

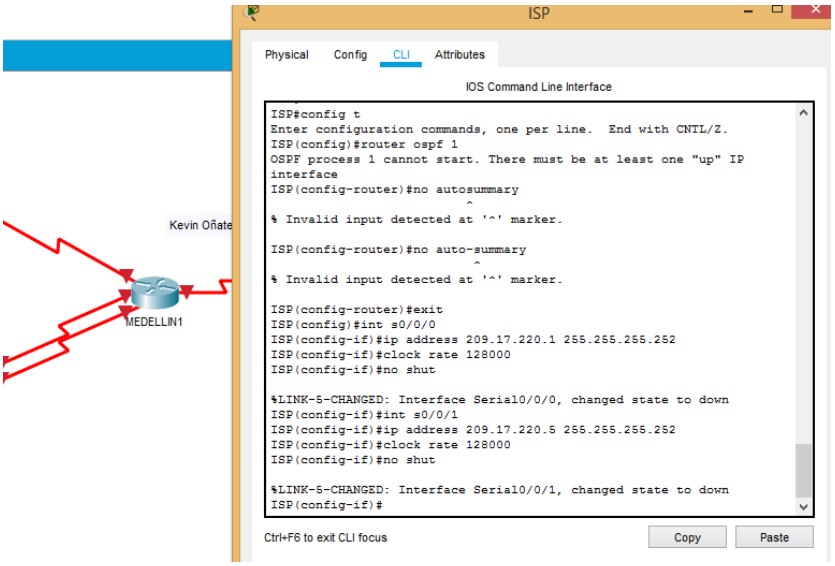


Gráfica 10. Topología Escenario 2 en rojo

Parte 1: Configuración del enrutamiento

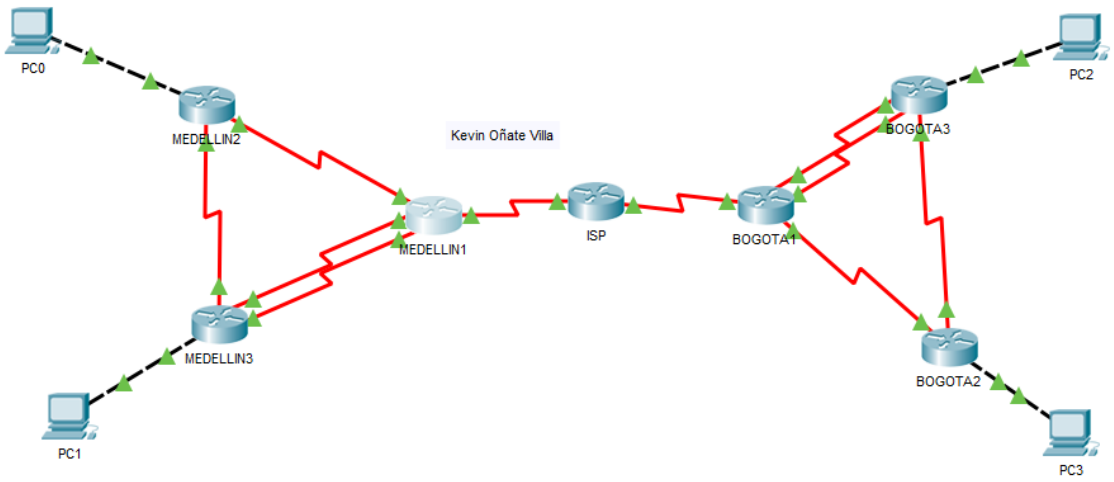
a. Configurar el enrutamiento en la red usando el protocolo OSPF versión 2, declare la red principal, desactive la sumarización automática.

Usamos el protocolo OSPF para cada una de las configuraciones como lo visualizamos en el router nombrado ISP:



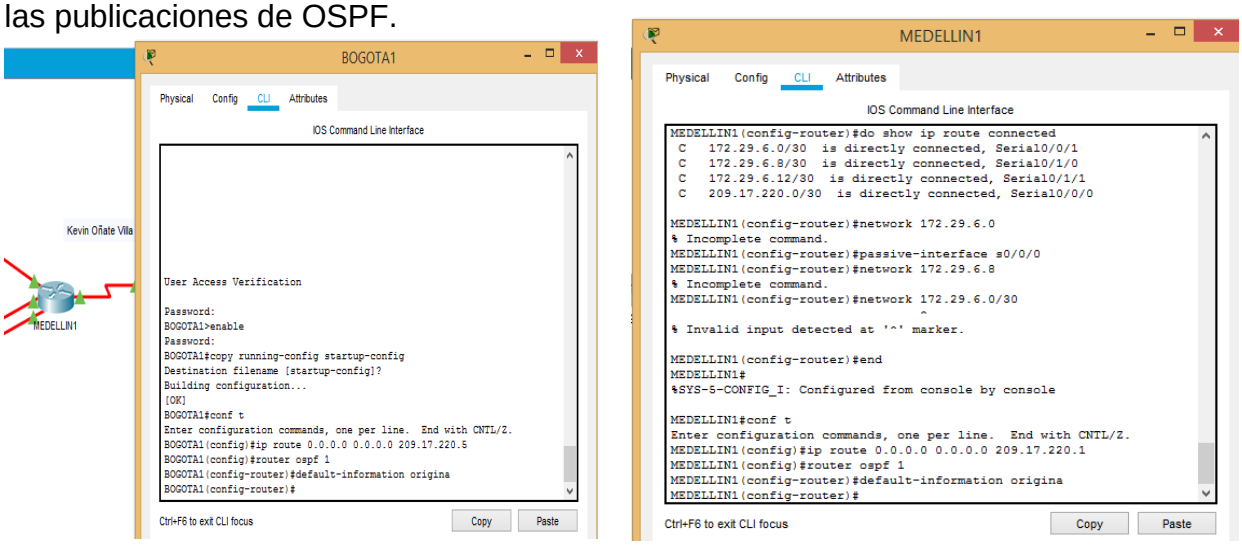
Gráfica 11. ISP

Cuando terminamos las configuraciones nos queda la siguiente topologia:



Gráfica 12. Topología Escenario 2 en Verde

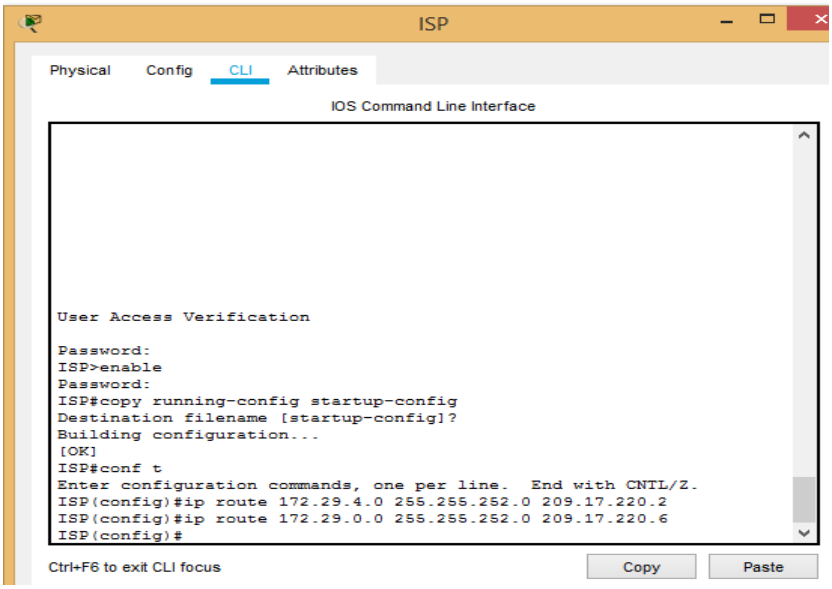
b. Los routers Bogota1 y Medellín deberán añadir a su configuración de enrutamiento una ruta por defecto hacia el ISP y, a su vez, redistribuirla dentro de las publicaciones de OSPF.



Gráfica 13. Routers

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

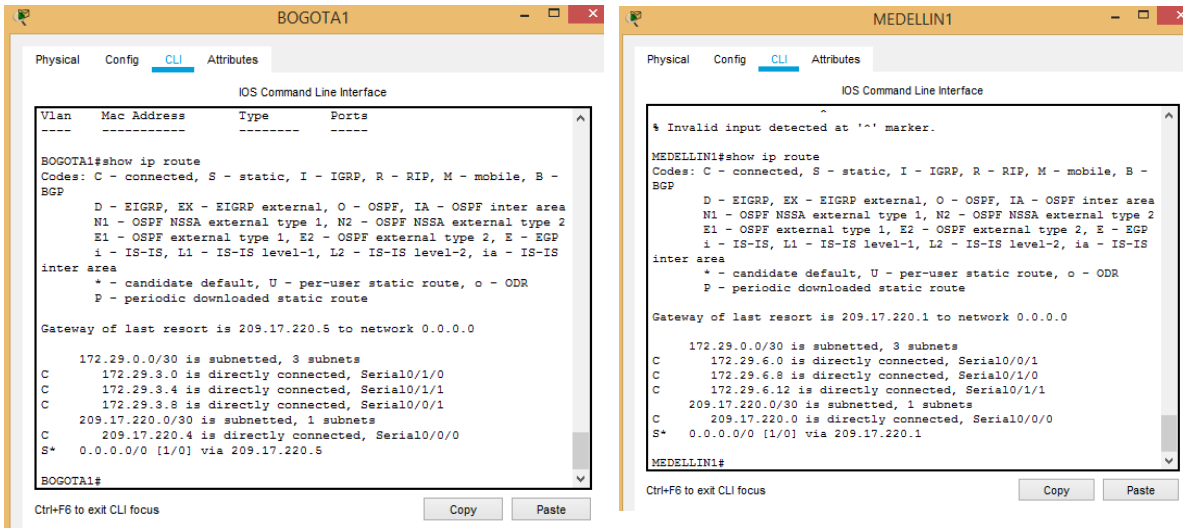
Configuramos ISP para una ruta estatica



Gráfica 14. ISP con ruta estática

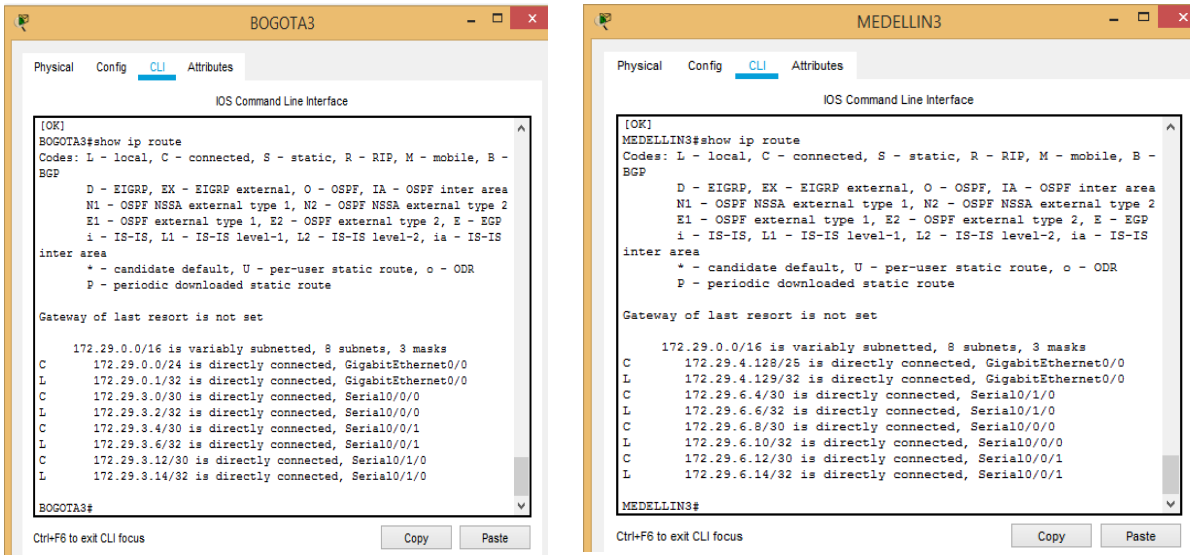
Parte 2: Tabla de Enrutamiento.

a. Verificar la tabla de enrutamiento en cada uno de los routers para comprobar las redes y sus rutas.



Gráfica 15. Verificación de rutas asignada

b. Verificar el balanceo de carga que presentan los routers.



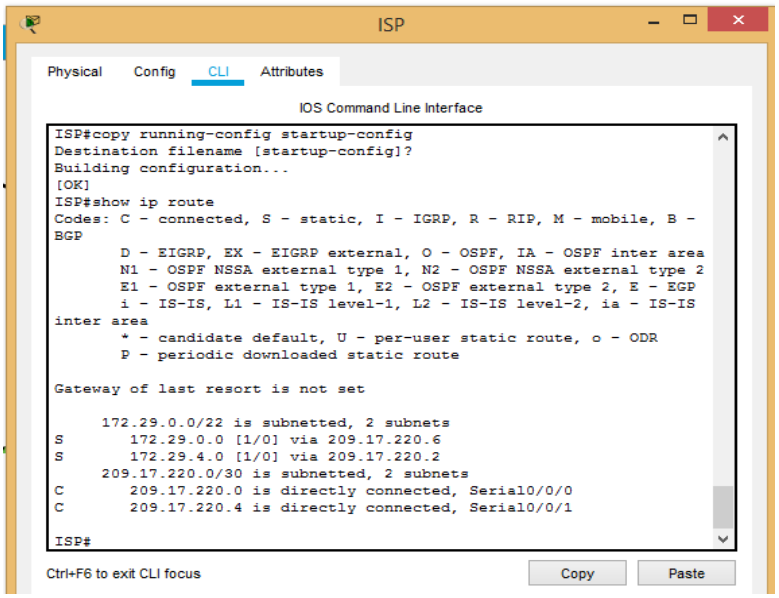
Gráfica 16. Balance de carga

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

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

e. Las tablas de los routers restantes deben permitir visualizar rutas redundantes para el caso de la ruta por defecto.
f. El router ISP solo debe indicar sus rutas estáticas adicionales a las directamente conectadas.

A continuacion damos solucion a ls puntos c,d,e,y f:



Gráfica 17. ISP Indicando rutas estáticas

Parte 3: Deshabilitar la propagación del protocolo OSPF.

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

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

Tabla 23. Deshabilitar la propagación del protocolo OSPF

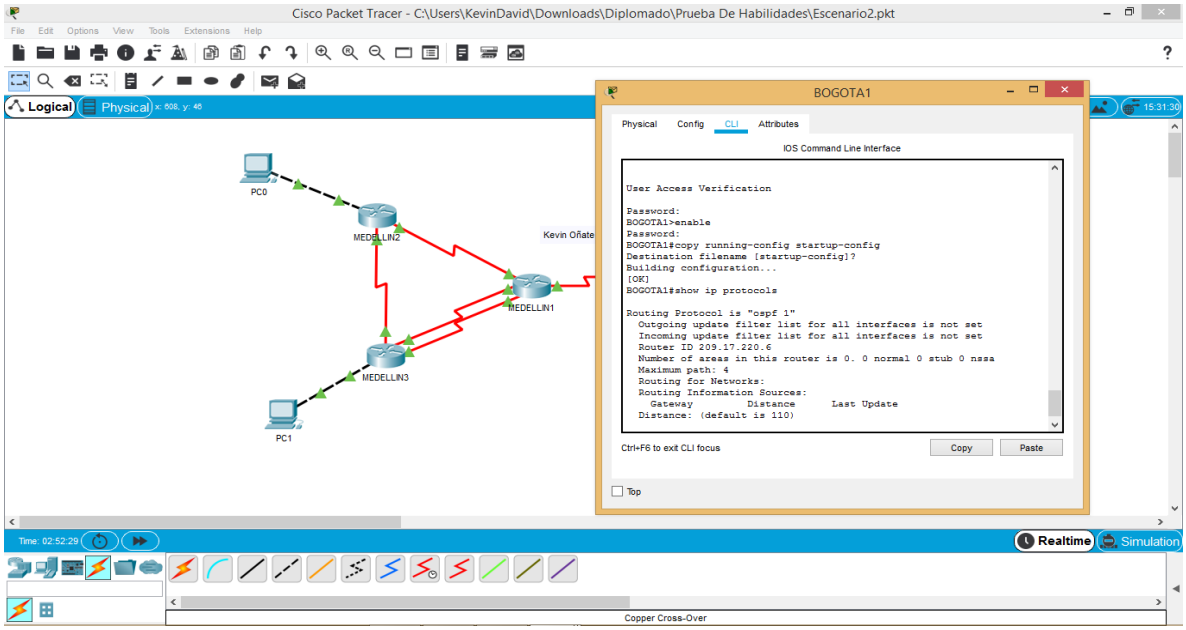
Este paso lo realizamos al inicio cuando configuramos OSPF.

Parte 4: Verificación del protocolo OSPF.

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

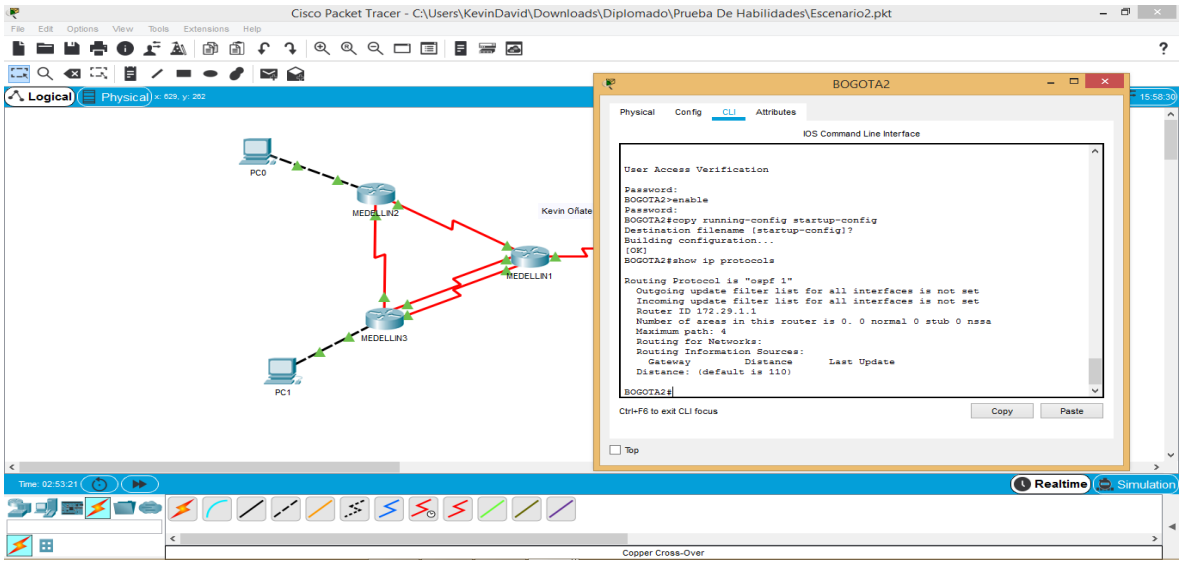
Enrutamientos:

BOGOTA1:



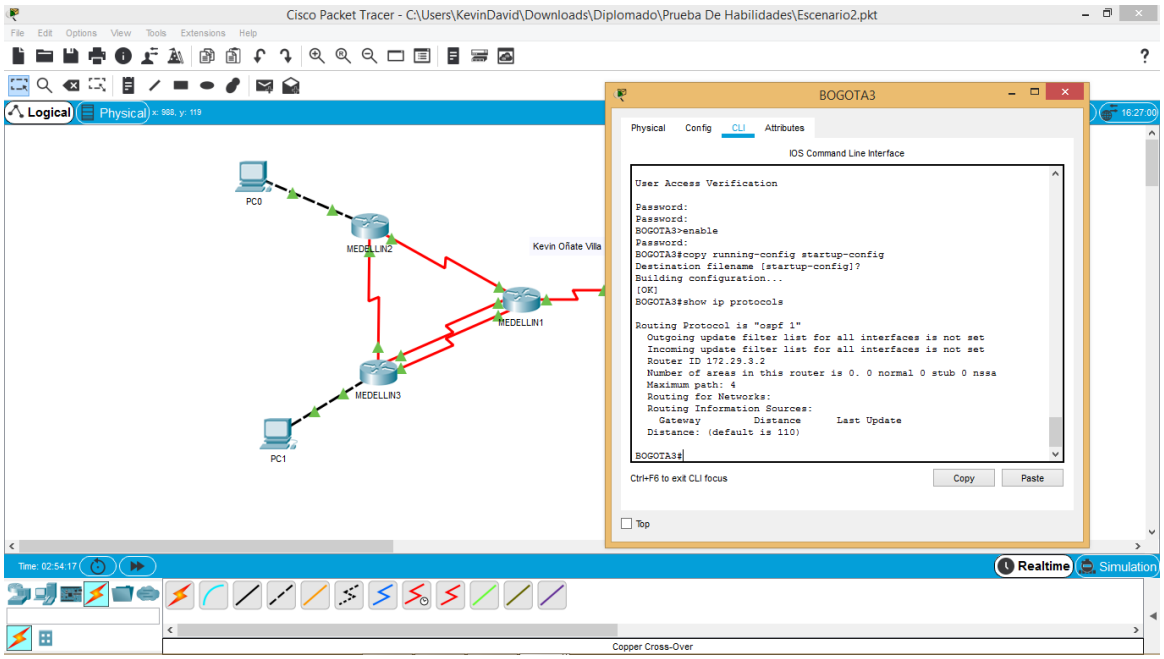
Gráfica 18. Router BOGOTA1

BOGOTA2:



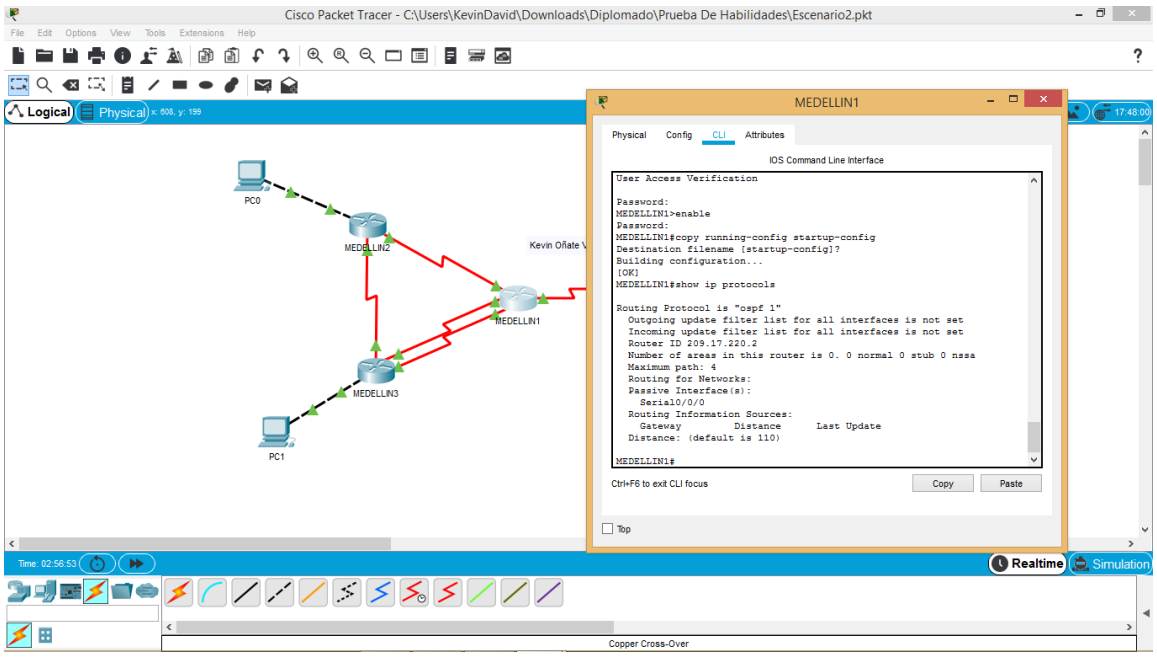
Gráfica 19. Router BOGOTA2

BOGOTA3:



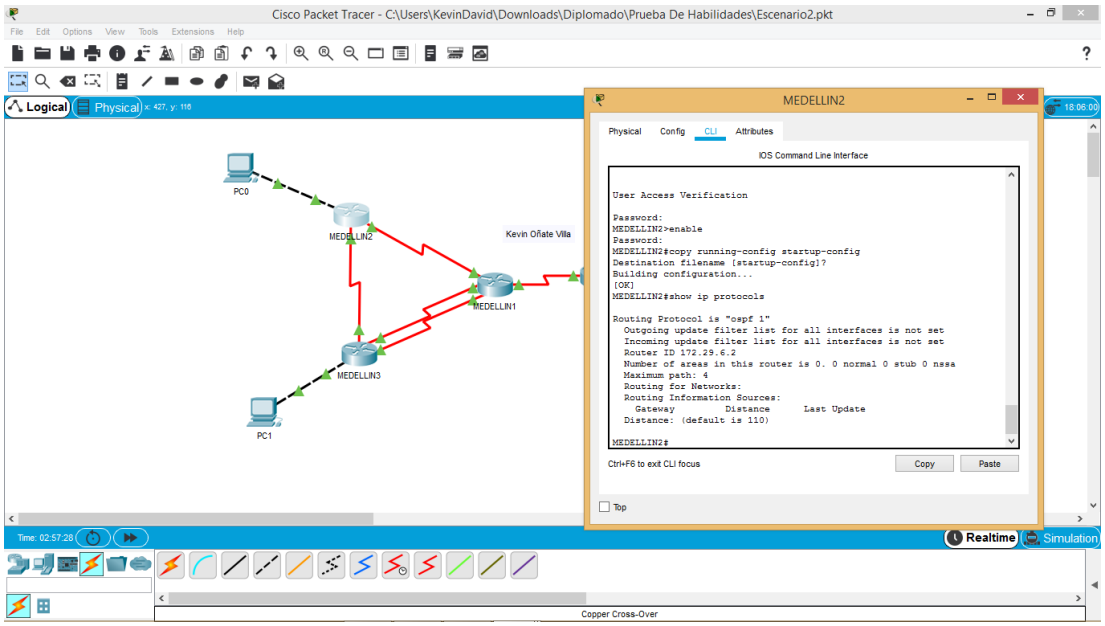
Gráfica 20. Router BOGOTA3

MEDELLIN1:



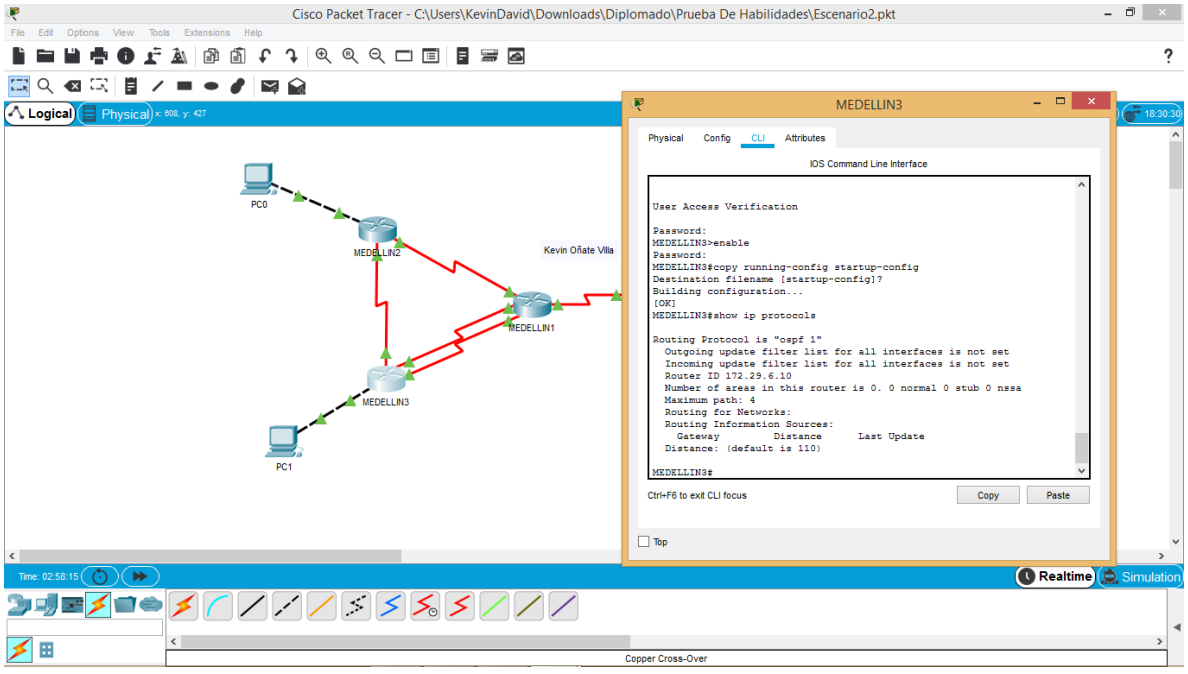
Gráfica 21. Router MEDELLIN1

MEDELLIN2:



Gráfica 22. Router MEDELLIN2

MEDELLIN3:



Gráfica 23. Router MEDELLIN3

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

MEDELLIN1:

Router(config-router) #do show ip route connected

C 172.29.6.0/30 is directly connected, Serial0/0/1

C 172.29.6.8/30 is directly connected, Serial0/1/0

C 172.29.6.12/30 is directly connected, Serial0/1/1

C 209.17.220.0/30 is directly connected, Serial0/0/0

BOGOTA1:

Router(config-router) #do show ip route connected

C 172.29.3.0/30 is directly connected, Serial0/1/0

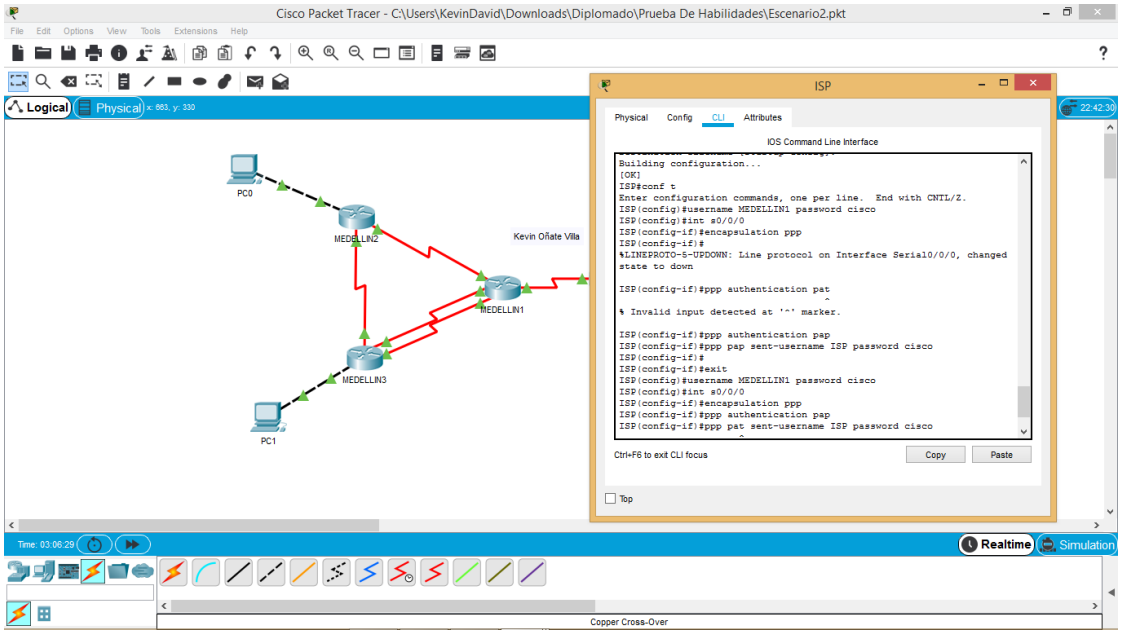
C 172.29.3.4/30 is directly connected, Serial0/1/1

C 172.29.3.8/30 is directly connected, Serial0/0/1

C 209.17.220.4/30 is directly connected, Serial0/0/0

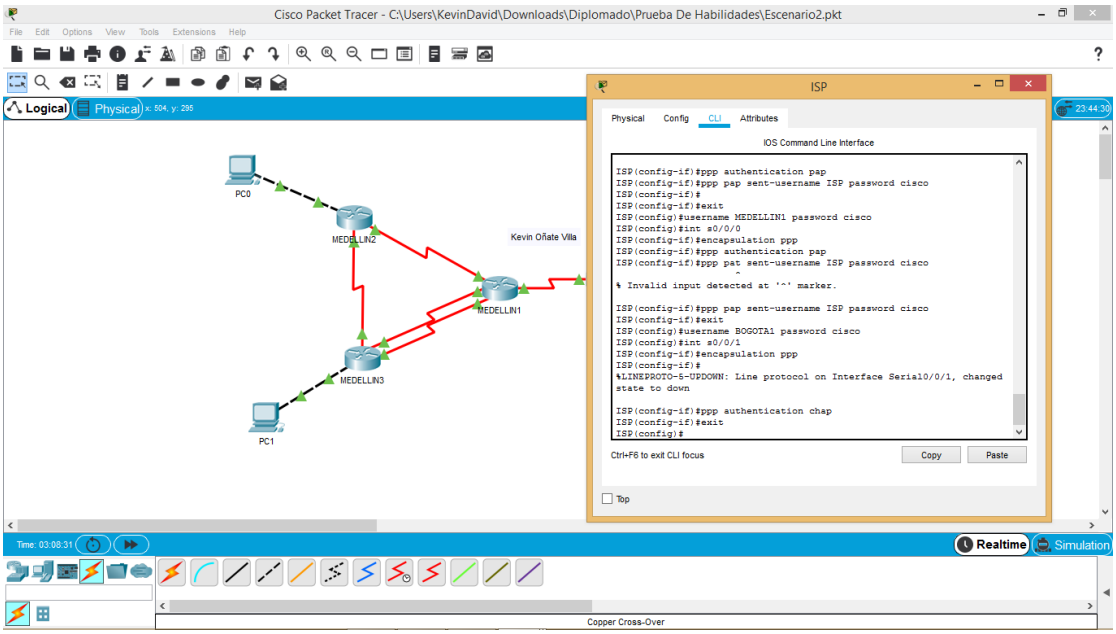
Parte 5: Configurar encapsulamiento y autenticación PPP.

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

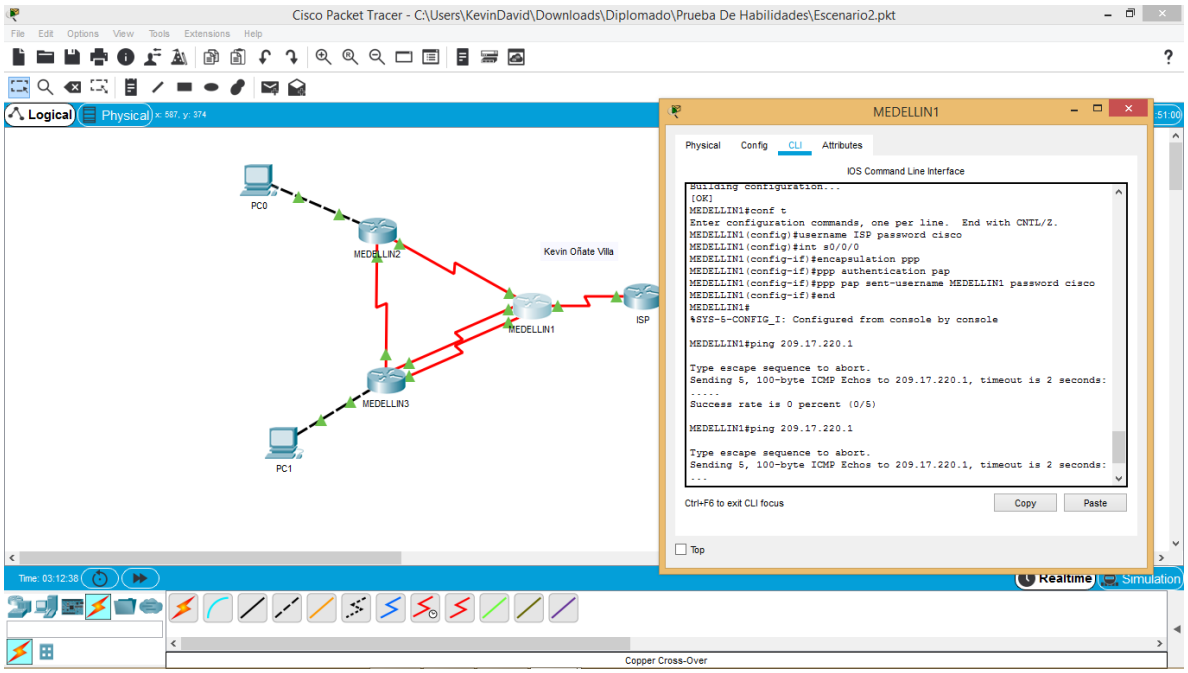


Gráfica 24. Encapsulamiento

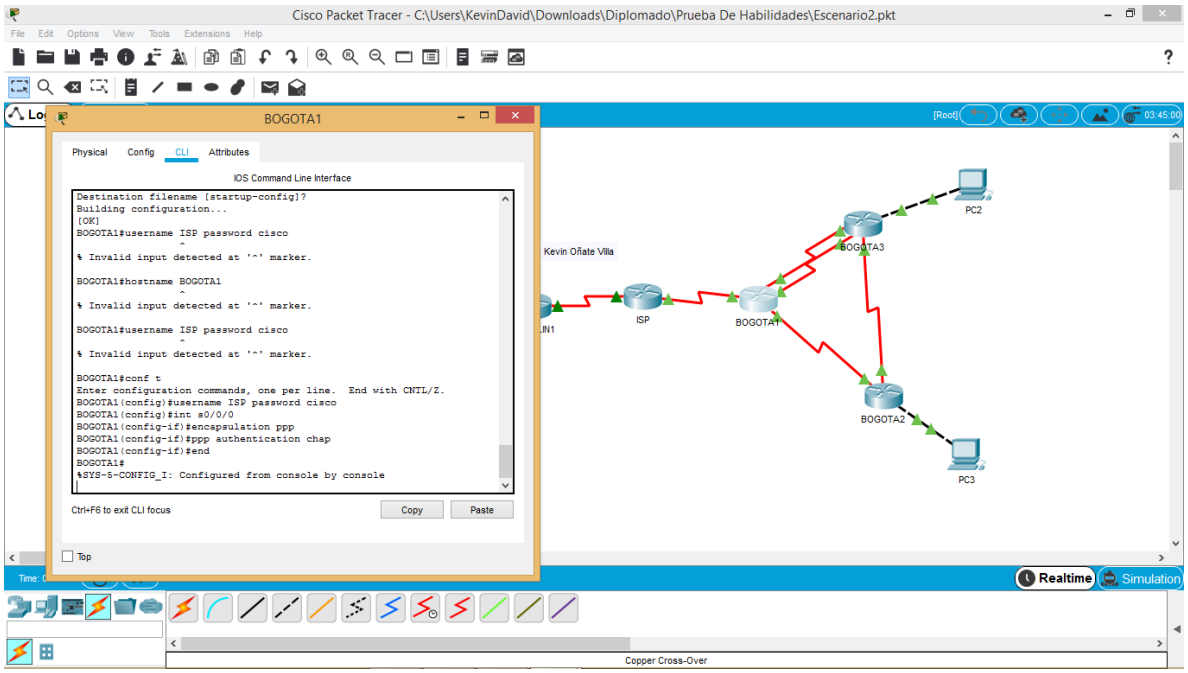
b. El enlace Bogotá1 con ISP se debe configurar con autenticación CHAT.



Gráfica 25. Router ISP CHAT



Gráfica 26. Router MEDELLIN 1 CHAT



Gráfica 27. Router BOGOTA 1 CHAT

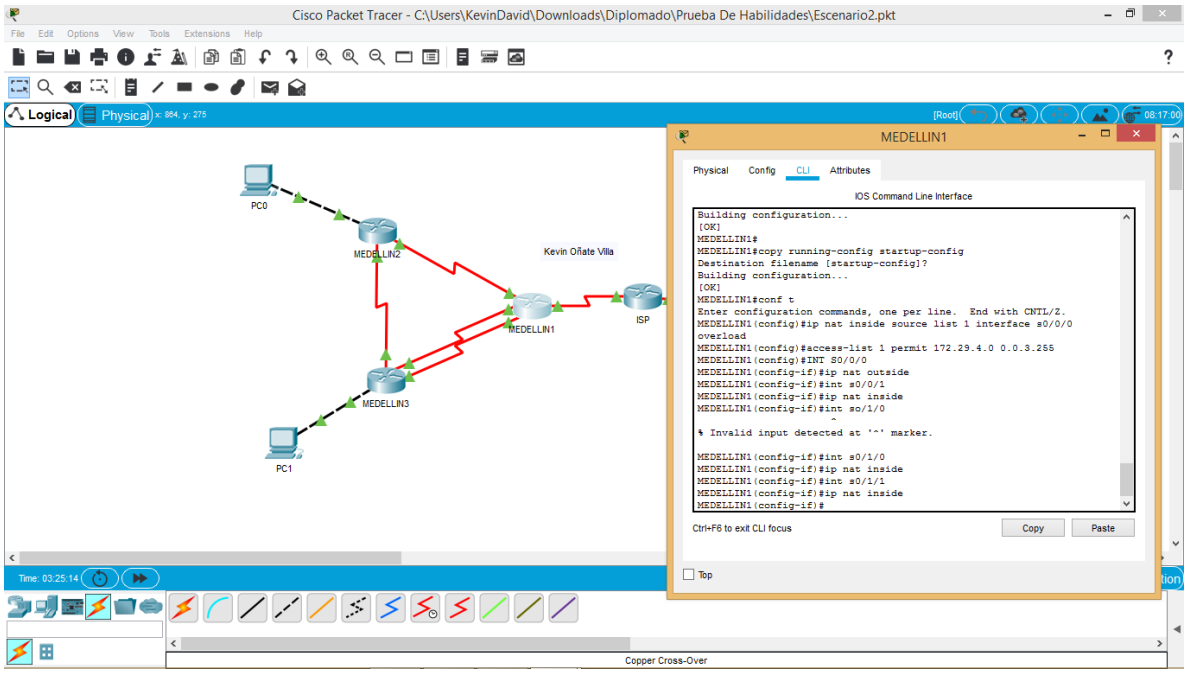
Parte 6: Configuración de PAT.

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

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

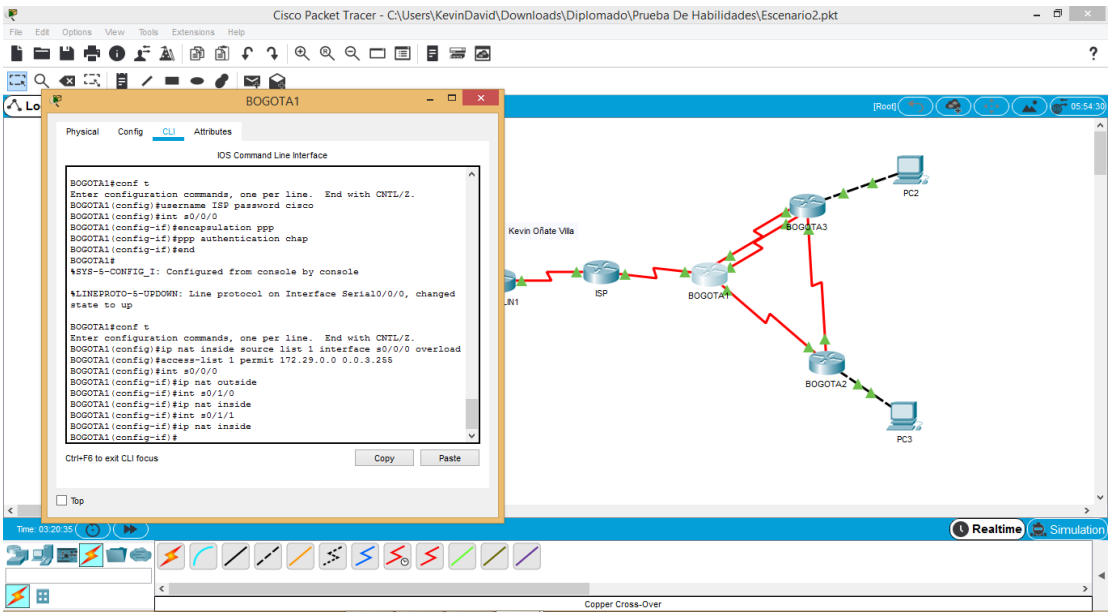
c. Proceda a configurar el NAT en el router Bogotá1. Compruebe que la traducción de direcciones indique las interfaces de entrada y de salida. Al realizar una prueba de ping, la dirección debe ser traducida automáticamente a la dirección de la interfaz serial 0/1/0 del router Bogotá1, cómo diferente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

MEDELLIN1:



Gráfica 28. Router MEDELLIN1 PAT

BOGOTA1:

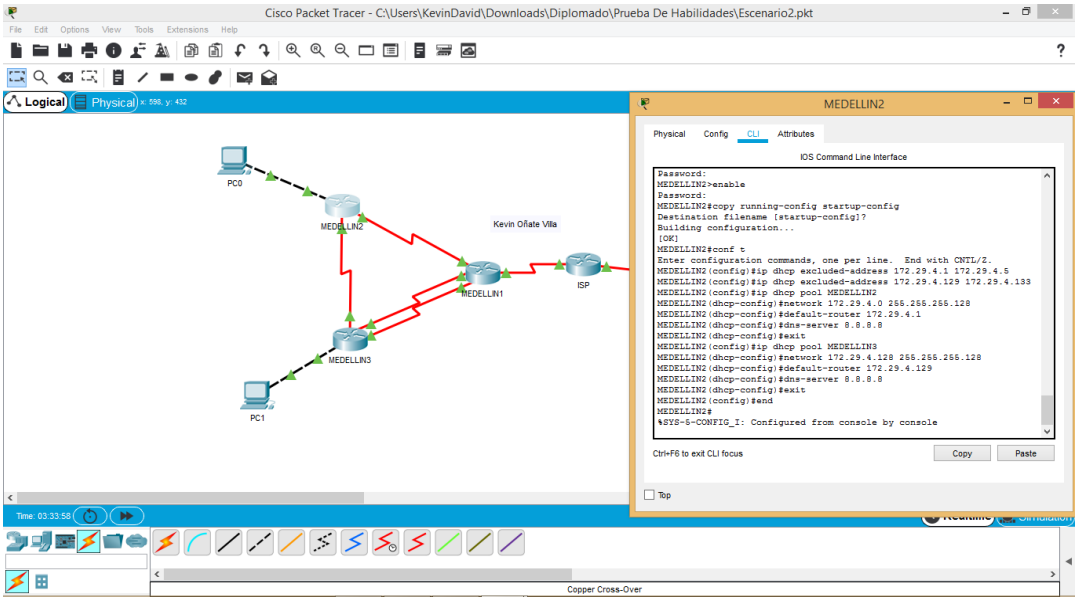


Gráfica 29. Router BOGOTA1 PAT

Parte 7: Configuración del servicio DHCP.

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

MEDELLIN2:

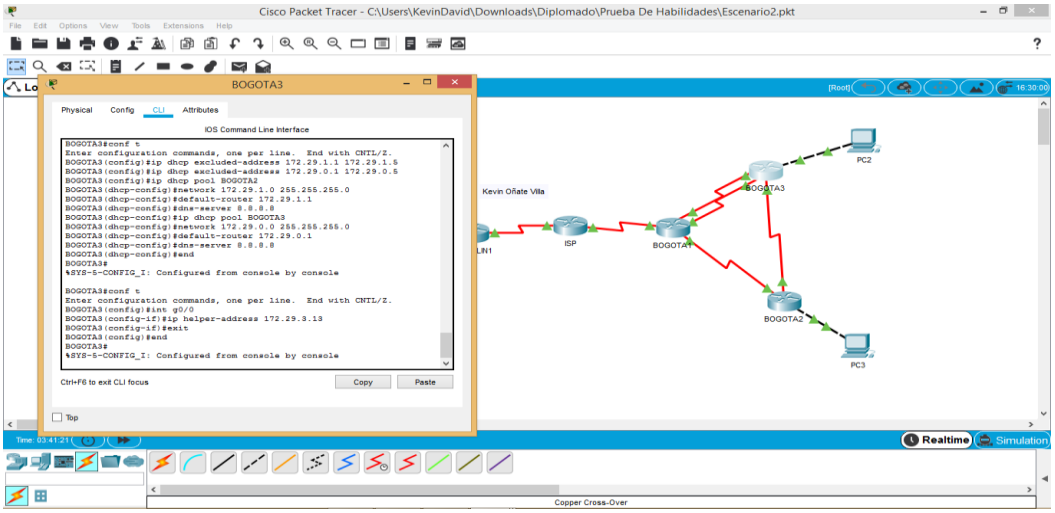


Gráfica 30. Router MEDELLIN2 PAT

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

c. Configurar la red Bogotá2 y Bogotá3 donde el router Medellín2 debe ser el servidor DHCP para ambas redes LAN.

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



Gráfica 31. Router BOGOTA3 DCHP LAN

7. CONCLUSIONES

Se demostró las habilidades prácticas y teóricas desarrolladas a lo largo del diplomado cisco dando solución a los escenarios propuestos para esta evaluación de habilidades.

Se establece conectividad entre los dispositivos necesarios siguiendo topologías de red indicadas.

Se utilizo varios protocolos para lograr la correcta conexión y funcionamiento de las topologías propuestas además de muchos equipos como los routers que son dispositivos que favorecen la conexión de una red con otra, este es el responsable de la entrega de los paquetes a través de varias redes. La implementación del protocolo NAT se hace para conservar las direcciones IPV4 publicas logrando que las redes que tengamos utilicen IPV4 privadas internamente.

Se logra Implementar las topologías según los requerimientos.

Se Configuran los protocolos de enrutamientos necesarios para lograr las conexiones, esto se comprueba a través de comandos como Ping que las conexiones establecidas están bien configuradas.

8. BIBLIOGRAFÍA

CISCO. (2014). Exploración de la red. Fundamentos de Networking. Recuperado de https://static-courseassets.s3.amazonaws.com/ITN50ES/module1/index.html#1.0.1.1

CISCO. (2014). Capa de Transporte. Fundamentos de Networking. Recuperado de https://static-courseassets.s3.amazonaws.com/ITN50ES/module7/index.html#7.0.1.1

CISCO. (2014). Asignación de direcciones IP. Fundamentos de Networking. Recuperado de https://static-courseassets.s3.amazonaws.com/ITN50ES/module8/index.html#8.0.1.1

Cómo referenciar libros: http://normasicontec.org/como-hacer-referencias-de-libros-con-normas-icontec/

Cómo referenciar fuentes electrónicas (Sitios web, videos, etc.): http://normasicontec.org/referencias-electronicas-en-normas-icontec-parte-2/ y http://normasicontec.org/referencias-electronicas-normas-icontec/

9.ANEXOS

Configuración R1

Enable
Erase startup-config
Reload
No ip domain-lookup
Hostname R1
Enable secret class
Line con 0
Enable password Cisco
Line vty 0 4
Password Cisco
login
Service password-encryption
Banner motd $ Se prohíbe el acceso no autorizado $
Interface s0/0/0
Description conexion a R2
Ip address 172.16.1.1 255.255.255.252
Ipv6 address 2001:DB8: ACAD:1::1
Clock rate 128000
No shutdown
Ip route 0.0.0.0 0.0.0.0 s0/0/0
Ipv6 address 2001:DB8: ACAD:1::1/64

Configuración R2

Enable
Erase startup-config
Reload
No ip domain-lookup
Hostname R2
Enable secret class
Line con 0
Enable password Cisco
Line vty 0 4
Password Cisco
login
Service password-encryption
Ip http server
Banner motd $ Se prohíbe el acceso no autorizado $
Interface s0/0/0
Description conexion a R1
Ip address 172.16.1.2 255.255.255.252
Ipv6 address 2001:DB8: ACAD:1::2
No shutdown
Interface s0/0/1
Description conexion a R3
Ip address 172.16.2.1 255.255.255.252
Ipv6 address 2001:DB8: ACAD:2::1
Clock rate 128000
No shutdown
Interface g0/0
Description internet
Ip addresss 209.165.200.233 255.255.255.248
Ipv6 address 2001:DB8: ACAD: A::33
No shutdown
Interface g0/1
Description conexion a servidor WWW
Ip address 10.10.10.10 255.255.255.0
ip route 0.0.0.0 0.0.0.0 g0/0
Ipv6 address 2001:DB8: ACAD: A:33/64

Configuración R3

Enable
Erase startup-config
Reload
No ip domain-lookup
Hostname R3
Enable secret class
Line con 0
Enable password Cisco
Line vty 0 4
Password Cisco
login
Service password-encryption
Banner motd $ Se prohíbe el acceso no autorizado $
Interface s0/0/1
Description conexion a R2
Ip address 172.16.2.2 255.255.255.252
Ipv6 address 2001:DB8: ACAD:2::2
No shutdown
Interface lo4
Ip address 192.168.4.1 255.255.255.0
Interface lo5
Ip address 192.168.5.1 255.255.255.0
Interface lo6
Ip address 192.168.6.1 255.255.255.0
Interface lo7
Ipv6 address 2001:DB8: ACAD:3::2
Ip route 0.0.0.0 0.0.0.0 s0/0/1

Configuración S1

Delete vlan.dat
Reload
Dir.flash
Show vlan
Show vlan brief
Enable
Configure terminal
Vlan 21
Name Contabilidad
Vlan 33
Name Ingenieria
Vlan 99
Name Administracion
Interface vlan 99
Ip address 192.168.99.2 255.255.255.0
Ip default-gateway 192.168.99.1
Interface fa0/3
Switchport mode trunk
Switchport mode trunk native vlan 1
Interface fa0/5
Switchport mode trunk
Switchport mode trunk native vlan 1
Interface range fa0/1-2, fa0/4, fa0/6-24, g0/1-2
Switchport mode Access
Interface fa0/6
Switchport mode access
Switchport mode access native vlan 21
Interface range fa0/1-2, fa0/4, fa0/7-24, g0/1-2
Shutdown

Configuración S3

Delete vlan.dat
Reload
Dir.flash
Show vlan
Show vlan brief
Enable
Configure terminal
Vlan 21
Name Contabilidad
Vlan 33
Name Ingenieria
Vlan 99
Name Administracion
Interface vlan 99
Ip address 192.168.99.3 255.255.255.0
Ip default-gateway 192.168.99.1
Interface fa0/3
Switchport mode trunk
Switchport mode trunk native vlan 1
Interface range fa0/1-2, fa0/4, fa0/6-24
Switchport mode Access
Interface fa0/18
Switchport mode access
Switchport mode access native vlan 23
Interface range fa0/1-2, fa0/4-17, fa0/19-24, g0/1-2
Shutdown