EVALUACIÓN PRUEBA DE HABILIDADES PRACTICAS CCNA

ANDERSON JAVIER QUINTERO ARGOTY

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BÁSICAS Y TECNOLOGÍAS

INGENIERÍA DE SISTEMAS

SAJ JUAN DE PASTO

2020

EVALUACIÓN PRUEBA DE HABILIDADES PRACTICAS CCNA

ANDERSON JAVIER QUINTERO ARGOTY

Diplomado de profundización cisco

Diseño e implementación de soluciones integradas LAN / WLAN

Tutor

Gustavo Adolfo Rodríguez

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BÁSICAS Y TECNOLOGÍAS

INGENIERÍA DE SISTEMAS

SAN JUAN DE PASTO

2020

Nota de aceptación

_____
_____
_____
_____

_____
Firma del presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

San Juan de Pasto, 07 de julio del 2020

CONTENIDO

LISTA DE TABLAS

LISTA DE ILUSTRACIONES

GLOSARIO

NETWORKING: El networking es una práctica común en el mundo empresarial y emprendedor. Es una palabra que ya se utiliza de forma cotidiana en el ámbito profesional y que hace referencia a eventos, tanto de tipo formal como informal, en los que puedes construir una red de contactos que te ayuden a generar oportunidades tanto de negocio como laborales.

ENRUTAMIENTO: es el proceso de reenviar paquetes entre redes, siempre buscando la mejor ruta (la más corta). Para encontrar esa ruta más óptima, se debe tener en cuenta la tabla de enrutamiento y algunos otros parámetros como la métrica, la distancia administrativa, el ancho de banda.

TOPOLOGÍA DE RED: se define como el mapa físico o lógico de una red para intercambiar datos. En otras palabras, es la forma en que está diseñada la red, sea en el plano físico o lógico. El concepto de red puede definirse como «conjunto de nodos interconectados». Un nodo es el punto en el que una curva se intercepta a sí misma. Lo que un nodo es concretamente depende del tipo de red en cuestión.

PACKET TRACER: de Cisco es un programa de simulación de redes que permite a los estudiantes experimentar con el comportamiento de la red y resolver preguntas del tipo «¿qué pasaría si...?».

RESUMEN

El presente trabajo se realiza en atención a los parámetros establecidos por la Universidad Nacional Abierta y a Distancia, en colaboración de la plataforma NETCAD de CISCO, en el desarrollo de los cursos CCNA1 y CCNA2, la aplicación de los conceptos adquiridos a lo largo del curso, son aplicados de manera progresiva en la construcción del trabajo final.

El presente trabajo se distribuye en el desarrollo de ejercicios prácticos, desarrollado en el simulador Packet tracer de CISCO, el escenario uno plantea el ejercicio de enrutamiento a través de la implementación del protocolo RIP versión 2, de igual manera la aplicación de conceptos para creación de un servidor web y la aplicación de conceptos para dirección ip dinámico, por intermedio de un router empleado como servidor DHCP, de igual manera la distribución de la redes por intermedio de VLAN debida administradas.

El segundo escenario plantea un problema para la interconexión de sedes ubicadas en diferentes ciudades, se utiliza el protocolo OSPF de manera interna para la propagación de la conectividad, de igual manera se emplean rutas estáticas en los router de borde para su salida a la red WAN, así mismo se emplean conceptos tales como uso de un router como servidor DCHP, protocolo de seguridad para las redes WAN por medio del encapsulamiento PPP bien sea CHAP o PAP.

INTRODUCCIÓN

La presente actividad está enfocada a la verificación de los conceptos aprendidos a lo largo del presente diplomado, por intermedio del presente documento se puede identificar la apropiación de conceptos y la habilidad a la hora de configurar los diferentes elementos que componen una red, identificando todas las capas del modelo OSI, y la aplicación de cada una de estas.

Con la presente actividad se busca identificar la comprensión y habilidades para la solución de problemas relacionados con los diversos aspectos de Networking, con base en lo anterior se plantea el desarrollo de dos (02) escenarios con la debida documentación y evidencias que permitan observar el desarrollo de cada uno de estos.

Para el primer escenario se trabajará en una red pequeña, donde se admitirá conectividad IPV4 e IPV6, aplicando el protocolo de routing dinámico RIPV2, protocolo de configuración de host dinámicos DHCP, traducción de direcciones de red dinámicas y estáticas NAT, lista de control de acceso ACL y protocolo de red NTP, servidor/cliente.

Para el segundo escenario se trabajará el uso del protocolo OSPF, considerando rutas por defecto redistribuidas, se habilitará el encapsulamiento PPP y su autenticación, proporción de servicio DHCP por parte de los router a la red LAN.

Al realizar las practicas se concluye con la actividad de verificación y conectividad plena de los dos escenarios planteados, demostrando así la capacidad para el desarrollo de este tipo de actividades.

OBJETIVOS

GENERAL

Implementar las habilidades y conocimientos adquiridos, mediante la aplicación de los diferentes conceptos prácticos en el desarrollo de los escenarios propuestos, con el fin de presentar las competencias adquiridas en el desarrollo del presente diplomado.

ESPECIFICOS

- ✓ Verificar los requisitos planteados en la guía de aprendizaje, con el fin de plantear las soluciones a las temáticas planteadas.

- ✓ Buscar la asesoría del caso, mediante charlas síncronas con los educadores del presente diplomado, con el fin de validar la presentación del documento final.

- ✓ Identificar los diferentes elementos que sean necesarios para la construcción de las topologías de red planteadas en la presente actividad.

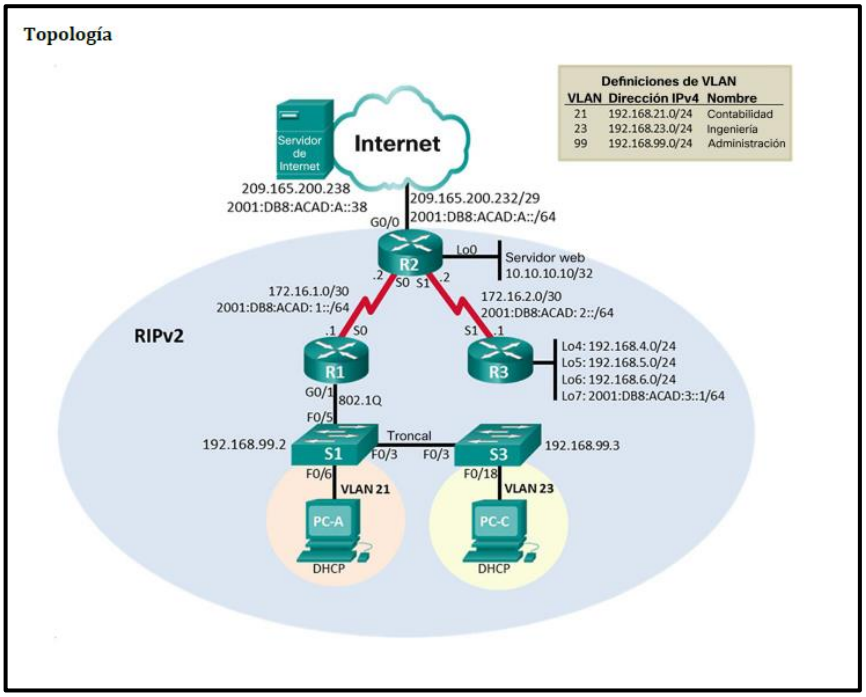
- ✓ Aplicar las diferentes configuraciones, de acuerdo con los protocolos señalados en cada caso, permitiendo la conectividad de los elementos empleados en cada topología.

- ✓ Validar la conectividad en cada uno de los escenarios, con el fin de validar la pertinencia de cada configuración, con el fin de realizar la entrega de un producto funcional.

ESCENARIO UNO

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

Ilustración 1. Topología Escenario Uno



Nota: recuperado de packet tracer Escenario 1. Autor Anderson Quintero

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.

El objetivo de la presente parte es el de eliminar el registro de configuración inicial de todos los dispositivos a utilizar en el desarrollo de la presente práctica.

Configuración realizada

Tabla 1. Eliminar Configuración Inicial

Dispositivo	Comandos Utilizados
Router 1	**R1>**Enable **R1#**erase startup-config **R1#** reload
Router 2	**R2>**Enable **R2#**erase startup-config **R2#** reload
Router 3	**R3>**Enable **R3#**erase startup-config **R3#** Reload
Switch 1	**S1>**Enable **S1#**erase startup-config **S1#**delete Vlan.dat **S1#** reload **S1#** show flash
Switch 3	**S3>**Enable **S3#**erase startup-config **S3#**delete Vlan.dat **S3#**reload **S3#**show flash

PARTE 2: CONFIGURAR LOS PARÁMETROS BÁSICOS DE LOS DISPOSITIVOS

Paso 1: Configurar la computadora de Internet

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

Tabla 2. Direccionamiento IP Servidor

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.233
Dirección IPv6/subred	2001:DB8:ACAD:A::38
Gateway predeterminado IPv6	2001:DB8:ACAD:A::1

En el presente paso se realiza la configuración del servidor WEB, se asigna el direccionamiento IPV4 e IPV6 que tendrá en la presente actividad.

Paso 2: Configurar R1

En el presente paso se realiza la configuración básica del Router 1, se configuran los parámetros básicos tales como nombre del host, contraseña telnet, líneas vty, encriptación de contraseñas, mensaje de advertencia, se deshabilita la búsqueda DNS, esta configuración inicial permite ajustar de una manera practica y segura los diferentes elementos que se utilizan en la topología.

Se realiza la descripción de la interfaz serial 0/0/0, asignación de dirección IPV4 e IPV6, se habilita el direccionamiento IPV6, se habilita la interfaz como DCE y se habilita el puerto utilizado por la interfaz, configuración realizada con el fin de garantizar la conectividad de la red.

Configuración realizada

Tabla 3. Configuración en Router 1

Dispositivo	Comandos Utilizados
Router 1	**R1>**Enable **R1#**configure terminal **R1(config)#**No ip domail-lookup **R1(config)#**Hostname R1 **R1(config)#**Enable secret class **R1(config)#**Line console 0 **R1(config-line)#**Password cisco **R1(config-line)#**Login **R1(config-line)#**Line vty 0 4 **R1(config-line)#**Password cisco **R1(config-line)#**Exit **R1(config)#**Service password-encryption **R1(config)#**Banner motd #SE PROHIBE EL ACCESO NO AUTORIZADO# **R1(config)#**Interface serial S0/0/0 **R1(config-if)#**Description CONECTADO A R2 **R1(config-if)#**Ip address 172.16.1.1 255.255.255.252 **R1(config-if)#**Ipv6 address 2001:db8:ACAD:1::1/64 **R1(config-if)#**Clock rate 128000 **R1(config-if)#**No shutdown **R1(config-if)#**exit **R1(config)#**Ipv6 unicast-routing **R1(config)#**Ip route 0.0.0.0 0.0.0.0 S0/0/0 **R1(config)#**Ipv6 route ::0/0 S0/0/0

Paso 3: Configurar R2

En el presente paso se realiza la configuración básica del Router 2, se configuran los parámetros básicos tales como nombre del host, contraseña telnet, líneas vty, encriptación de contraseñas, mensaje de advertencia, se deshabilita la búsqueda DNS, parámetros básicos que permiten describir de manera detallada cada elemento.

Se realiza la descripción de las interfaz serial 0/0/0, asignación de dirección IPV4 e IPV6, se habilita el direccionamiento IPV6 y se habilita el puerto utilizado por la interfaz, descripción interfaz serial 0/0/1, asignación dirección IPV4 e IPV6, se habilita la interfaz como DCE, se habilita el puerto utilizado por la interfaz, para finalizar se habilita el router como servidor HTTP, se habilita interfaz gigabit ethernet como simulador de internet, se establece dirección IPV4 a dirección loopback 0 como servidor web simulado y se establecen rutas predeterminadas IPV4 e IPV6.

Configuración realizada

Tabla 4. Configuración en Router 2

Dispositivo	Comandos Utilizados
Router 2	**R2>**Enable **R2#**configure terminal **R2(config)#**No ip domail-lookup **R2(config)#**Hostname R2 **R2(config)#**Enable secret class **R2(config)#**Line console 0 **R2(config-line)#**Password cisco **R2(config-line)#**Login **R2(config-line)#**Line vty 0 4 **R2(config-line)#**Password cisco **R2(config-line)#**Exit **R2(config)#**Service password-encryption **R2(config)#**Ip http server **R2(config)#**Banner motd #SE PROHIBE EL ACCESO NO AUTORIZADO# **R2(config)#**Interface serial S0/0/0 **R2(config-if)#**Description CONECTADO A R1 **R2(config-if)#**Ip address 172.16.1.2 255.255.255.252 **R2(config-if)#**Ipv6 address 2001:db8: ACAD:1::2/64 **R2(config-if)#**No shutdown **R2(config-if)#**exit **R2(config)#**Ipv6 unicast-routing **R2(config)#**Interface serial S0/0/1 **R2(config-if)#**Description CONECTADO A R3

	R2(config-if)#Ip address 172.16.2.2 255.255.255.252 **R2(config-if)#**Ipv6 address 2001:db8:ACAD:2::2/64 **R2(config-if)#**Clock rate 128000 **R2(config-if)#**No shutdown **R2(config-if)#**exit **R2(config)#**Ipv6 unicast-routing **R2(config)#**Ip route 0.0.0.0 0.0.0.0 S0/0/0 **R2(config)#**Ipv6 route ::0/0 S0/0/0 **R2(config)#**Interface g0/0 **R2(config-if)#**Description Simulador de internet **R2(config-if)#**Ip address 209.165.200.232 255.255.255.248 **R2(config-if)#**Ipv6 address 2001:DB8:ACAD:A::1/64 **R2(config-if)#**No shutdown **R2(config-if)#**exit **R2(config)#**Interface loopback 0 **R2(config-if)#**Ip address 10.10.10.10 255.255.255.255 **R2(config-if)#**Description Simulación servidor web **R2(config-if)#**exit **R2(config)#**Ip route 0.0.0.0 0.0.0.0 G0/0 **R2(config)#**Ipv6 route ::0/0 G0/0

Paso 4: Configurar R3

En el presente paso se realiza la configuración básica del Router 3, se configuran los parámetros básicos tales como nombre del host, contraseña telnet, líneas vty, encriptación de contraseñas, mensaje de advertencia, se deshabilita la búsqueda DNS, parámetros básicos que permiten describir de manera detallada cada elemento.

Se realiza la descripción de la interfaz serial 0/0/1, asignación de dirección IPV4 e IPV6, se habilita el direccionamiento IPV6 y se habilita el puerto utilizado por la interfaz, se habilitan interfaces loopback de la 4 a la 7, se establecen las descripciones y direcciones IPV4, utilizadas como servidores web simulados, para finalizar se asigna una ruta IPV4 e IPV6 predeterminada para la interfaz gigabit ethernet.

Configuración realizada

Tabla 5. Configuración en Router 3

Dispositivo	Comandos Utilizados
Router 3	**R3>**enable **R3#**confgiure terminal **R3(config)#**No ip domail-lookup **R3(config)#**Hostname R3

	R3(config)#Enable secret class **R3(config)#**Line console 0 **R3(config-line)#**Password cisco **R3(config-line)#**Login **R3(config-line)#**Line vty 0 4 **R3(config-line)#**Password cisco **R3(config-line)#**Exit **R3(config)#**Service password-encryption **R3(config)#**Banner motd #SE PROHIBE EL ACCESO NO AUTORIZADO# **R3(config)#**Interface serial S0/0/1 **R3(config-if)#**Description CONECTADO A R2 **R3(config-if)#**Ip address 172.16.2.1 255.255.255.252 **R3(config-if)#**Ipv6 address 2001:db8:ACAD:2::1/64 **R3(config-if)#**No shutdown **R3(config-if)#**Interface loopback 4 **R3(config-if)#**Ip address 192.168.4.1 255.255.255.0 **R3(config-if)#**Interface loopback 5 **R3(config-if)#**Ip address 192.168.5.1 255.255.255.0 **R3(config-if)#**Interface loopback 6 **R3(config-if)#**Ip address 192.168.6.1 255.255.255.0 **R3(config-if)#**Interface loopback 7 **R3(config-if)#**Ip address 2001:DB8:ACAD:3::1/64 **R3(config-if)#**exit **R3(config)#**Ipv6 unicast-routing **R3(config)#**Ip route 0.0.0.0 0.0.0.0 S0/0/1 **R3(config)#**Ipv6 route ::0/0 S0/0/1

Paso 5: Configurar S1

En el presente paso se realiza la configuración básica del Switch 1, se configuran los parámetros básicos tales como nombre del host, contraseña telnet, líneas vty, encriptación de contraseñas, mensaje de advertencia, se deshabilita la búsqueda de servidor DNS.

Configuración realizada

Tabla 6. Configuración en Switch 1

Dispositivo	Comandos Utilizados
Switch 1	**S1>**enable **S1#**configure terminal **S1(Config)#**No ip domail-lookup **S1(Config)#**Hostname S# **S1(Config)#**Enable secret class **S1(Config)#**Line console 0 **S1(Config-line)#**Password cisco

	S1(Config-line)#Login **S1(Config-line)#**Line vty 0 4 **S1(Config-line)#**Password cisco **S1(Config-line)#**Exit **S1(Config)#**Service password-encryption **S1(Config)#**Banner motd #SE PROHIBE EL ACCESO NO AUTORIZADO#

Paso 6: Configurar el S3

En el presente paso se realiza la configuración básica del Switch 3, se configuran los parámetros básicos tales como nombre del host, contraseña telnet, líneas vty, encriptación de contraseñas, mensaje de advertencia, se deshabilita la búsqueda de servidor DNS.

Configuración Realizada

Tabla 7. Configuración en Switch 3

Dispositivo	Comandos Utilizados
Switch 3	**S3>**enable **S3#**configure terminal **S3(Config)#**No ip domail-lookup **S3(Config)#**Hostname S# **S3(Config)#**Enable secret class **S3(Config)#**Line console 0 **S3(Config-line)#**Password cisco **S3(Config-line)#**Login **S3(Config-line)#**Line vty 0 4 **S3(Config-line)#**Password cisco **S3(Config-line)#**Exit **S3(Config)#**Service password-encryption **S3(Config)#**Banner motd #SE PROHIBE EL ACCESO NO AUTORIZADO#

Paso 7: Verificar la conectividad de la red

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

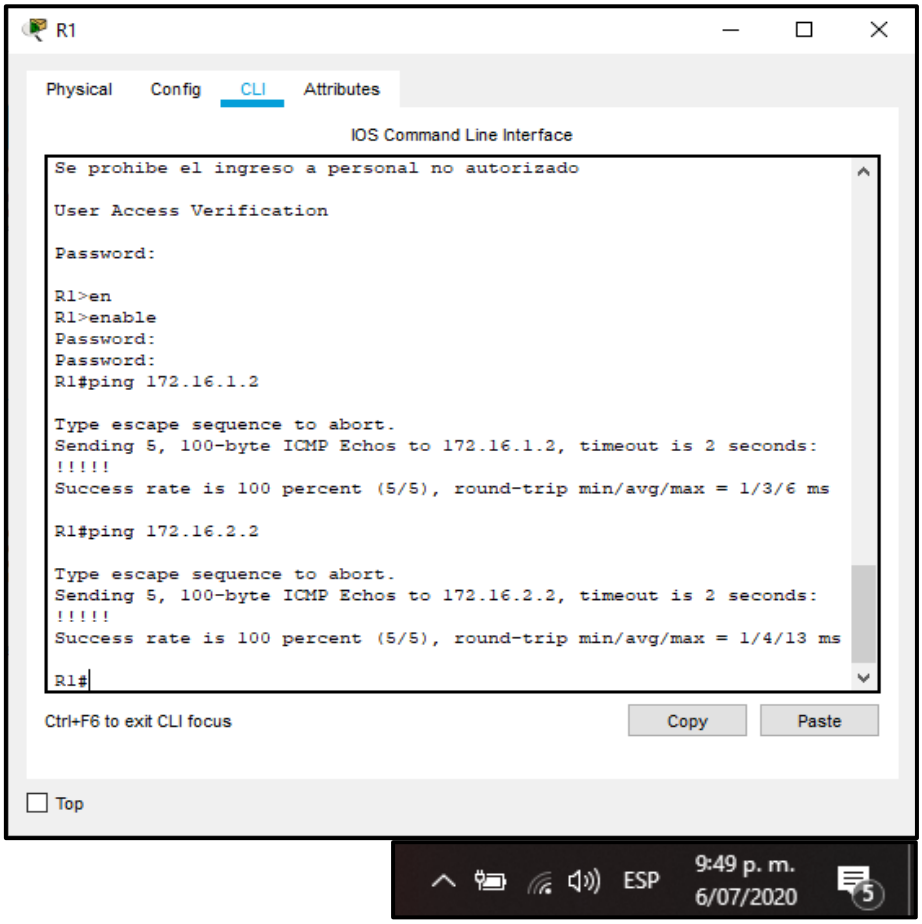
Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 8. Verificar Conectividad

Desde	A	Dirección IP	Resultado de Ping
R1	R2, S0/0/0	172.16.1.2 2001:DB8:ACAD:1::2	Satisfactorio
R2	R3, S0/0/1	172.16.2.1 2001:DB8:ACAD:2::1	Satisfactorio
PC de Internet	Gateway predeterminado	209.165.200.225 2001:DB8:ACAD:A::1	Satisfactorio

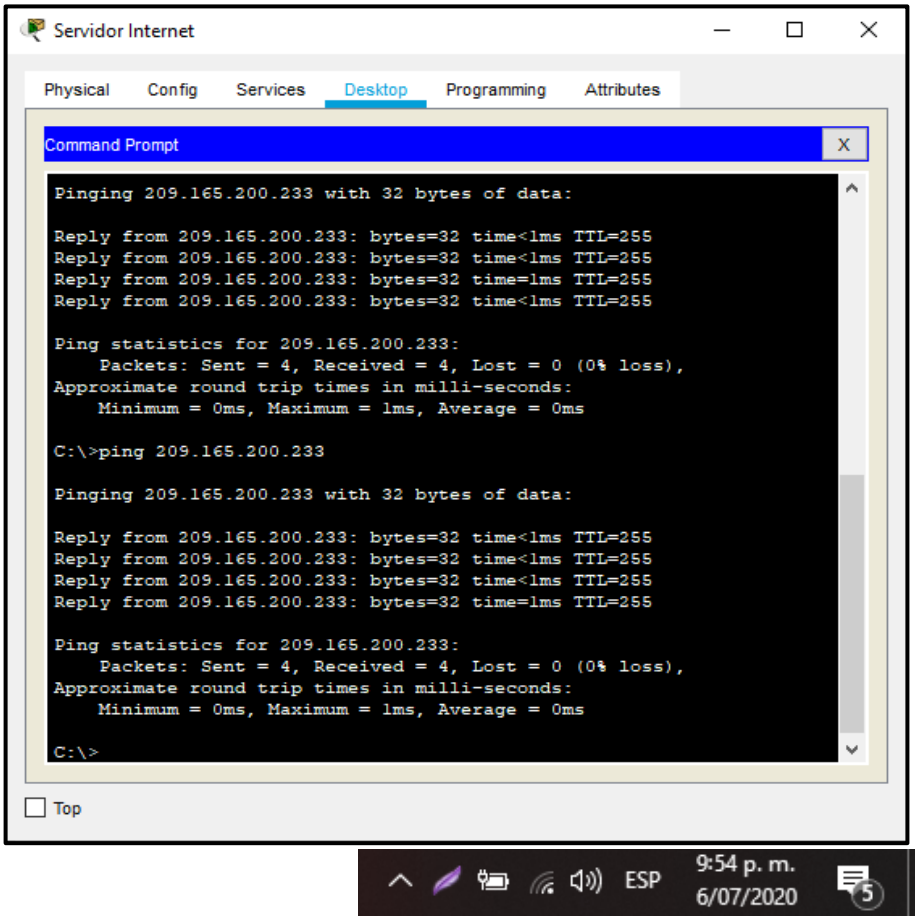
En el presente paso se verifica la conectividad que debe existir entre R1 y R2, de igual manera del PC de internet al Gateway predeterminado.

Ilustración 2. Verificar conectividad1.



Nota: recuperado de packet tracer Escenario 1. Autor Anderson Quintero

Ilustración 3. Verificar conectividad2



Nota: recuperado de packet tracer Escenario 1. Autor Anderson Quintero

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

Paso 1: Configurar S1

En el presente paso se realiza la creación de la base de datos de VLAN a utilizar, se crean y se nombran y crean las VLAN indicadas en el desarrollo del presente escenario, VLAN 21 contabilidad, VLAN 23 ingeniería, VLAN 99 administración, se realiza la asignación de las direcciones IP según la topología, se habilita como enlace troncal las interfaces F0/3 y F0/5 como VLAN nativas, se configuran los demás puertos como acceso, se asigna la interfaz F0/6 como puerto de acceso de la VLAN 21 y se apagan los puertos que no se utilizaran en el Switch.

Configuración Realizada

Tabla 9. Configuración de VLAN en Switch 1

Dispositivo	Comandos Utilizados
Switch 1	**S1(config)#**Vlan 21 **S1(config-vlan)#**Name CONTABILIDAD **S1(config-vlan)#**Vlan 23 **S1(config-vlan)#**Name INGENIERIA **S1(config-vlan)#**Vlan 99 **S1(config-vlan)#**Name ADMINISTRATIVA **S1(config-vlan)#**Exit **S1(config)#**interface vlan99 **S1(config-if)#**Ip address 192.168.99.2 255.255.255.0 **S1(config-if)#**Ip default-gateway 192.168.99.1 **S1(config-if)#**Interface f0/3 **S1(config-if)#**Switchport mode trunk **S1(config-if)#**Swichport native vlan1 **S1(config-if)#**Interface f0/5 **S1(config-if)#**Swichpoirt mode trunk **S1(config-if)#**Swichport native vlan1 **S1(config-if)#**Exit **S1(config)#**Interface range fa0/1-2, fa0/4,fa0/6-24 **S1(config-if-range)#**Switchport mode Access **S1(config-if-range)#**Exit **S1(config)#**Interface fa0/6 **S1(config-if)#**Swtichport mode Access vlan21 **S1(config-if)#**Interface range fa0/1-2, fa0/4, fa0/7-24 **S1(config-if-range)#**Shutdown

Paso 2: Configurar el S3

En el presente paso se realiza la creación de la base de datos de VLAN a utilizar, se crean y se nombran y crean las VLAN indicadas en el desarrollo del presente escenario, VLAN 21 contabilidad, VLAN 23 ingeniería, VLAN 99 administración, se realiza la asignación de las direcciones IP según la topología, se asigna como enlace troncal el puerto F0/3 para la VLAN 1 Nativa, se configuran los puertos restantes como acceso, se asigna el puerto F0/18 a la VLAN 21, por último se apagan los puertos sin utilizar.

Comandos Utilizados

Tabla 10. Configuración de Vlan en Switch 3

Dispositivo	Comandos Utilizados
Switch 3	**S3>**Enable

	S3#Configure terminal **S3(config)#**Vlan 21 **S3(config-vlan)#**Name CONTABILIDAD **S3(config-vlan)#**Vlan 23 **S3(config-vlan)#**Name INGENIERIA **S3(config-vlan)#**Vlan 99 **S3(config-vlan)#**Name ADMINISTRATIVA **S3(config-vlan)#**Exit **S3(config)#**interface vlan 99 **S3(config-if)#**Ip address 192.168.99.3 255.255.255.0 **S3(config-if)#**Ip default-gateway 192.168.99.1 **S3(config-if)#**Interface f0/3 **S3(config-if)#**Switchport mode trunk **S3(config-if)#**Swichport native vlan1 **S3(config-if)#**Interface f0/5 **S3(config-if)#**Swichpoirt mode trunk **S3(config-if)#**Swichport native vlan1 **S3(config-if)#**Exit **S3(config)#**Interface range fa0/1-2, fa0/4-24 **S3(config-if-range)#**Switchport mode Access **S3(config-if-range)#**Exit **S3(config)#**Interface fa0/18 **S3(config-if)#**Swtichport mode Access vlan 23 **S3(config-if)#**Interface range fa0/1-2, fa0/4-17, fa0/19-24 **S3(config-if-range)#**Shutdown

Paso 3: Configurar R1

En el presente paso se realiza la configuración de las subinterfaces del puerto gigabit ethernet 0/1, se asignan las vlan a las diferentes subinterfaces creadas con el número de VLAN correspondiente Subinterfaz 802.1Q.21 Vlan de contabilidad se le asigna la dirección IP disponible, Subinterfaz 802.1Q.23 Vlan de ingeniería se le asigna la dirección IP disponible, Subinterfaz 802.1Q.99 Vlan de administración se le asigna la dirección IP disponible, se activa la interfaz Gigabit ethernet 0/1.

Configuración realizada

Tabla 11. Configuración de subinterfaces en Router 1

Dispositivo	Comandos Utilizados
Router 1	**R1>**Enable **R1#**Configure terminal **R1(config)#**Interface fa0/0.21 **R1(config-subif)#**Description LAN DE CONTABILIDAD **R1(config-subif)#**Encapsulation dot1Q 21 **R1(config-subif)#**Ip address 192.168.21.1 255.255.255.0

	R1(config-subif)#Interface fa0/0.23 **R1(config-subif)#**Description LAN DE INGENIERIA **R1(config-subif)#**Encapsulation dot1Q 23 **R1(config-subif)#**Ip address 192.168.23.1 255.255.255.0 **R1(config-subif)#**Interface fa0/0.99 **R1(config-subif)#**Description LAN DE ADMINISTRACIÓN **R1(config-subif)#**Encapsulation dot1Q 99 **R1(config-subif)#**Ip address 192.168.99.1 255.255.25 **R1(config-subif)#**Exit **R1(config)#**Interface g0/0 **R1(config-if)#**No shutdown

Paso 4: Verificar la conectividad de la red

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

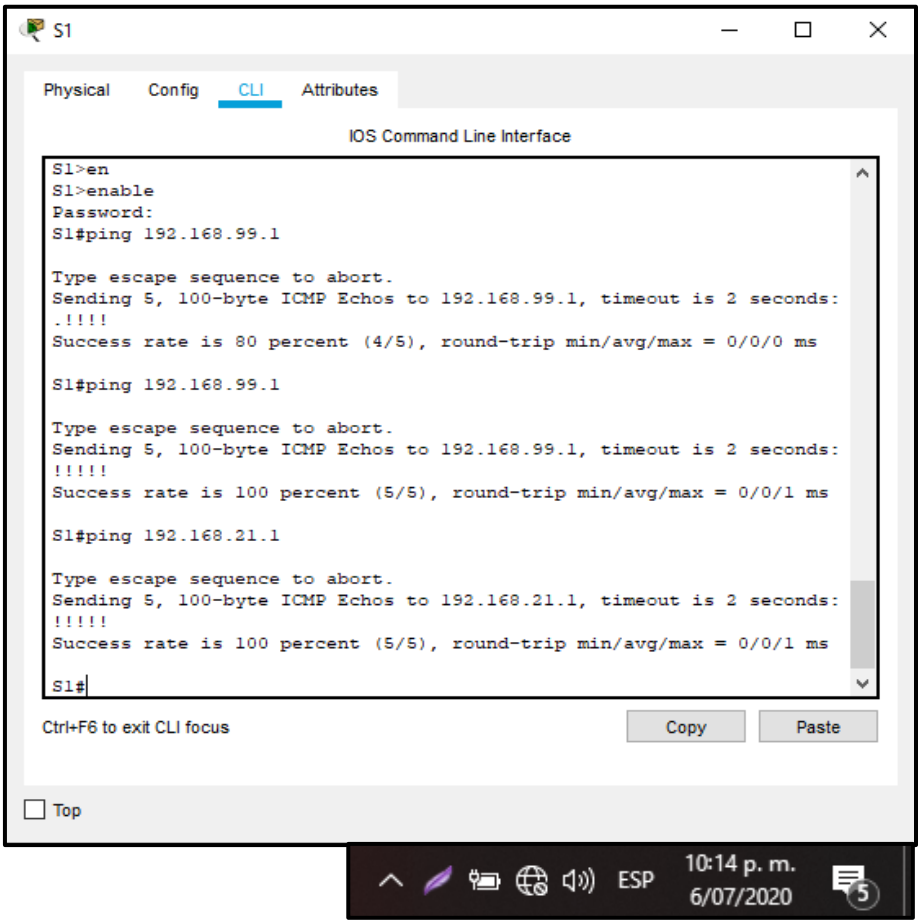
Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 12. Verificar Segunda Conectividad

Desde	A	Dirección IP	Resultado 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

En el presente paso se verifica la conectividad desde los Switch 1 y 3 a las direcciones ip de las subinterfaces del Router 1, se puede observar que existe conectividad en todas las subinterfaces, donde se evidencia la creación adecuada de las VLAN utilizadas en el desarrollo del presente ejercicio.

Ilustración 4. Verificar conectividad3



Nota: recuperado de packet tracer Escenario 1. Autor Anderson Quintero

Parte 4: Configurar el protocolo de routing dinámico RIPv2

Paso 1: Configurar RIPv2 en el R1

En el presente paso se realiza la configuración del protocolo de enrutamiento RIP versión 2, se anuncian las redes directamente conectadas, se establecen todas las interfaces utilizadas para las redes LAN, se establecen las interfases como pasivas, se desactiva la sumarización automática, ya en este momento la aplicación del protocolo de enrutamiento es fundamental para la conectividad de los elementos empleados en el ejercicio, se realiza la aplicación del protocolo dinámico RIPv2, se configura en cada uno de los router a vincular.

Configuración realizada

Tabla 13. Configuración Protocolo RIP en Router 1

Dispositivo	Comandos Utilizados
Router 1	**R1>**enable **R1#**Configure terminal **R1(config)#**Router rip **R1(config-router)#**Versión 2 **R1(config-router)#**do show ip route connected **R1(config-router)#**network 172.16.1.0 **R1(config-router)#**network 192.168.21.0 **R1(config-router)#**network 192.168.23.0 **R1(config-router)#**network 192.168.99.0 **R1(config-router)#**passive-interface g0/0.21 **R1(config-router)#**passive-interface g0/0.23 **R1(config-router)#**passive-interface g0/0.99 **R1(config-router)#**no auto-summary

Paso 2: Configurar RIPv2 en el R2

En el presente paso se realiza la configuración del protocolo de enrutamiento RIP versión 2, se anuncian las redes directamente conectadas a excepción de la rede Gigabit Ethernet 0/0, se establecen todas las interfaces utilizadas para las redes LAN, se establecen las interfases como pasivas, se desactiva la sumarización automática, ya en este momento la aplicación del protocolo de enrutamiento es fundamental para la conectividad de los elementos empleados en el ejercicio.

Configuración realizada

Tabla 14. Configuración Protocolo RIP en Router 2

Dispositivo	Comandos Utilizados
Router 2	**R2>**enable **R2#**Configure terminal **R2(config)#**Router rip **R2(config-router)#**Versión 2 **R2(config-router)#**do show ip route connected **R2(config-router)#**network 10.10.10.10 **R2(config-router)#**network 172.16.1.0 **R2(config-router)#**network 172.16.23.0 **R2(config-router)#**passive-interface loopback 0 **R2(config-router)#**no auto-summary

Paso 3: Configurar RIPv2 en el R3

En el presente paso se realiza la configuración del protocolo de enrutamiento RIP versión 2, se anuncian las redes directamente conectadas a excepción de la rede Gigabit Ethernet 0/0, se establecen todas las interfaces utilizadas para las redes LAN, se establecen las interfases como pasivas, se desactiva la sumarización automática, ya en este momento la aplicación del protocolo de enrutamiento es fundamental para la conectividad de los elementos empleados en el ejercicio.

Configuración realizada

Tabla 15. Configuración protocolo RIP en Router 3

Dispositivo	Comandos Utilizados
Router 3	**R3>**enable **R3#**Configure terminal **R3(config)#**Router rip **R3(config-router)#**Versión 2 **R3(config-router)#**do show ip route connected **R3(config-router)#**network 172.16.23.0 **R3(config-router)#**network 192.168.4.0 **R3(config-router)#**network 192.168.5.0 **R3(config-router)#**network 192.168.6.0 **R3(config-router)#**passive-interface loopback 4 **R3(config-router)#**passive-interface loopback 5 **R3(config-router)#**passive-interface loopback 6 **R3(config-router)#**no auto-summary **R3(config-router)#**end **R3#**show ip protocols **R3#**show ip route **R3#**show run | section rip

Paso 4: Verificar la información de RIP

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

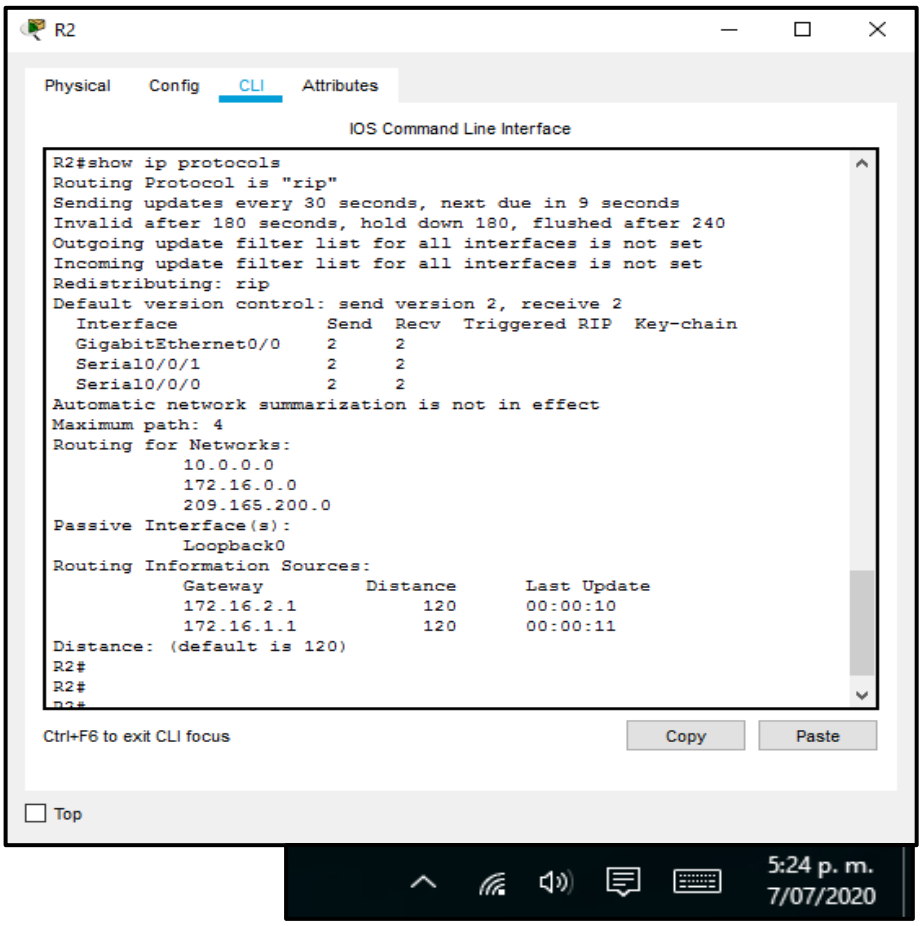
Tabla 16. Verificación Protocolo RIP

Pregunta	Respuesta
¿Con qué comando se muestran la ID del proceso RIP, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router?	Show ip protocols

¿Qué comando muestra solo las rutas RIP?	Show ip route rip
¿Qué comando muestra la sección de RIP de la configuración en ejecución?	Show run | section rip – no funciona en packe tracer

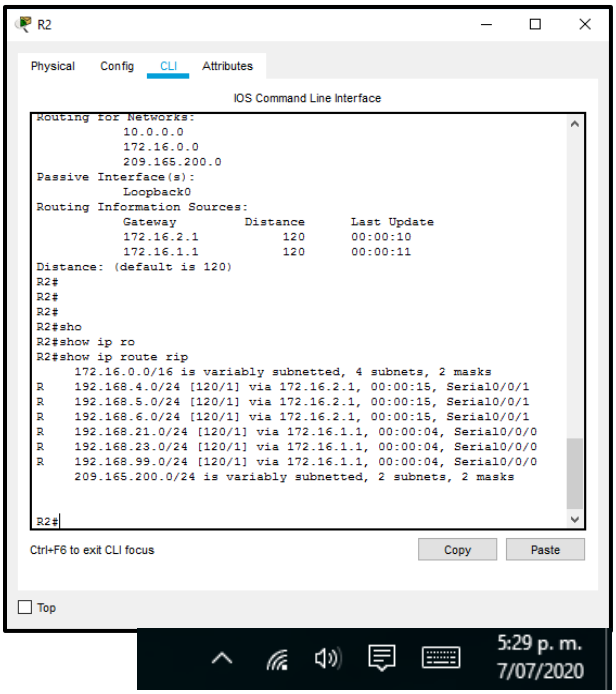
En este paso se verifica la implementación del protocolo RIP, se observan las ID de los router, las redes e interfases pasivas configuradas en el dispositivo, se observan las rutas RIP y la configuración de ejecución, en el presente paso se observa la correcta implementación del protocolo.

Ilustración 5. Verificación Protocolo RIP



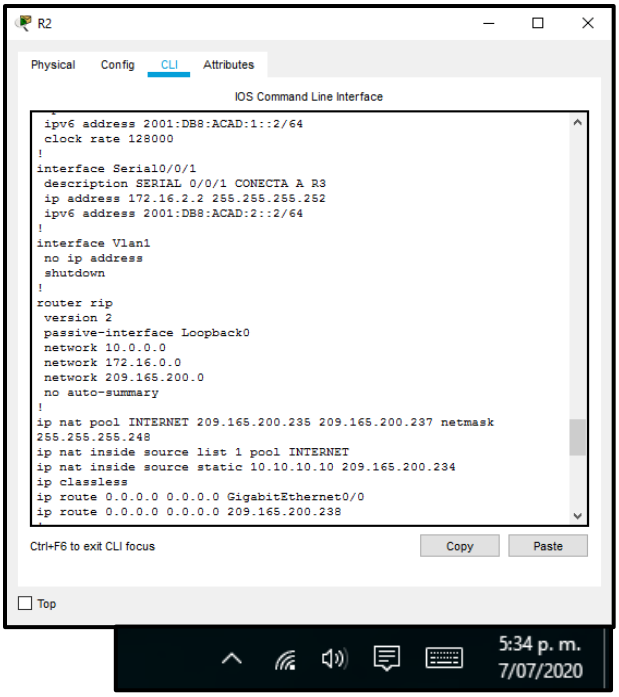
Nota: recuperado de packet tracer Escenario 1. Autor Anderson Quintero

Ilustración 6. Verificación Protocolo RIP_2



Nota: recuperado de packet tracer Escenario 1. Autor Anderson Quintero

Ilustración 7. Verificación Protocolo RIP_3



Nota: recuperado de packet tracer Escenario 1. Autor Anderson Quintero

Parte 5: Implementar DHCP y NAT para IPv4

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

En el presente paso se reservan las 20 primeras direcciones IP del segmento de direcciones asignadas para las VLAN 21 y 23, posteriormente en cada una de estas se realiza la creación del pool de DHCP para cada una de las VLAN.

Configuración realizada

Tabla 17. Creación Pool DHCP en Router 1

Dispositivo	Comandos Utilizados
Router 1	**R1>**enable **R1#**Configure terminal **R1(config)#**Ip dchp exclude-address 192.168.21.1 192.168.21.20 **R1(config)#**Ip dchp exclude-address 192.168.23.1 192.168.23.20 **R1(config)#**Ip dhcp pool ACCT **R1(dhcp-config)#**Network 192.168.21.0 255.255.255.0 **R1(dhcp-config)#**Dns-server 10.10.10.10 **R1(dhcp-config)#**Domain-name ccna-aa.com **R1(dhcp-config)#**Defalut router 1192.168.21.1 **R1(dhcp-config)#**Ip dhcp pool ENGNR **R1(dhcp-config)#**Network 192.168.23.0 255.255.255.0 **R1(dhcp-config)#**Dns-server 10.10.10.10 **R1(dhcp-config)#**Domain-name ccna-aa.com **R1(dhcp-config)#**Defalut router 1192.168.23.1

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

En el presente paso se realiza la configuración de NAT estática y dinámica en el router 2, en primera instancia se realiza la creación de una base de datos local, se procede habilitar el servicio del servidor HTTP, se configura el servidor de tal manera que pueda utilizar los datos locales para su autenticación, posteriormente se cea la NAT estática en el servidor web, se asignan las interfaces interna y externa a la NAT, se realiza la configuración de NAT dinámica en un ACL privada, se define el pool de direcciones IP utilizables y para finalizar se define la traducción de NATA dinámica.

Configuración realizada

Tabla 18. Configuración NAT en Router 2

Dispositivo	Comandos Utilizados
Router 2	**R2>**enable **R2**#Configure terminal **R2(config)**#Username Webuser privilege 15 secret cisco12345 **R2(config)**#Ip http server **R2(config)**#Ip http autententication local **R2(config)**#ip nat inside source static 10.10.10.10 209.165.200.234 **R2(config)**#Interface loopback 0 **R2(config-if)**#Ip nat inside **R2(config-if)**#Interface g0/0 **R2(config-if)**#Ip nat outside **R2(config-if)**#Exit **R2(config)**#Access-list 1 permit 192.168.21.0 0.0.0.255 **R2(config)**#Access-list 1 permit 192.168.23.0 0.0.0.255 **R2(config)**#Ip nat pool INTERNET 209.165.200.235 209.165.200.237 **R2(config)**#Netmask 255.255.255.248 **R2(config)**#Ip nat inside source list 1 pool INTERNET

Paso 3: Verificar el protocolo DHCP y la NAT estática

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

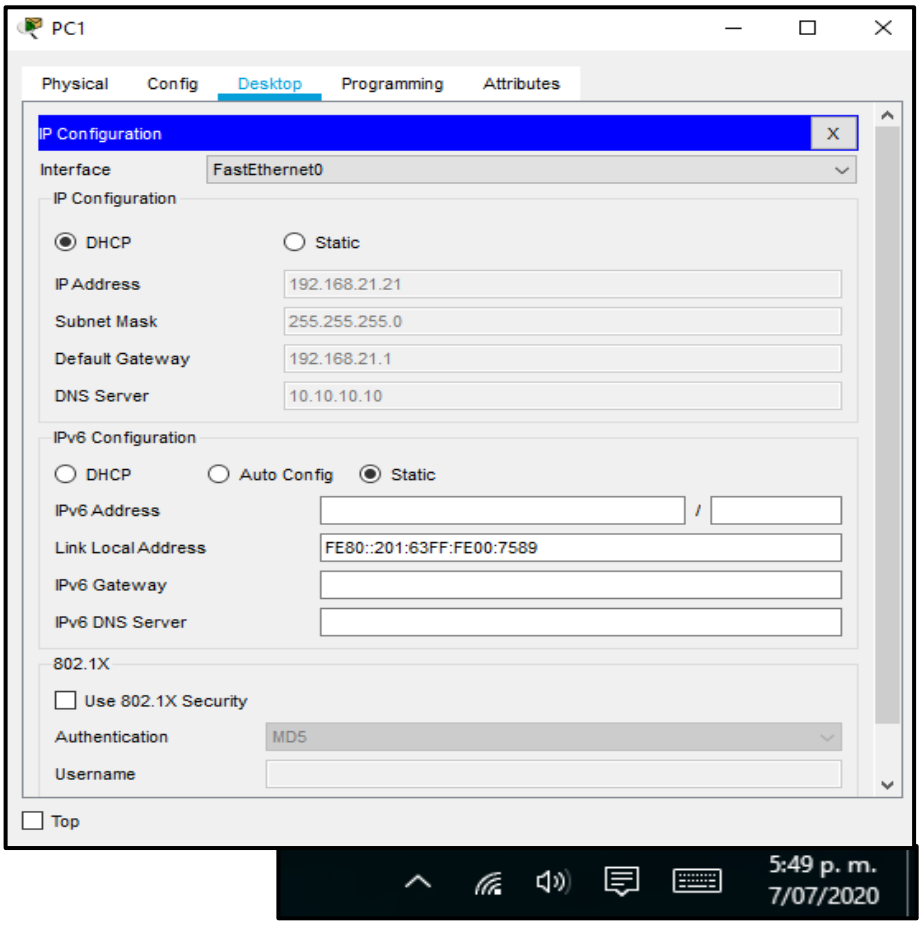
Tabla 19. Verificación protocolo DHCP y NAT

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	Direccionamiento automático
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	Direccionamiento automático
Verificar que la PC-A pueda hacer ping a la PC-C Nota: Quizá sea necesario deshabilitar el firewall de la PC.	Respuesta satisfactoria
Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.234) Iniciar sesión con el nombre de usuario webuser y la contraseña cisco12345	No soportado por packet tracer

Se verifica la información IP del servidor DHCP en cada uno de los hosts, se verifica la respuesta de cada uno de estos, se verifica el servicio WEB ingresando a la dirección global del servidor WEB.

En el presente paso se puede observar como el router inicia su función como servidor DHCP, se puede comprobar en los equipos de cómputo, teniendo en cuenta que cada uno de estos obtiene su dirección IP de manera automática, como se puede evidenciar en la siguiente ilustración.

Ilustración 8. Verificación Protocolo DHCP



Nota: recuperado de packet tracer Escenario 1. Autor Anderson Quintero

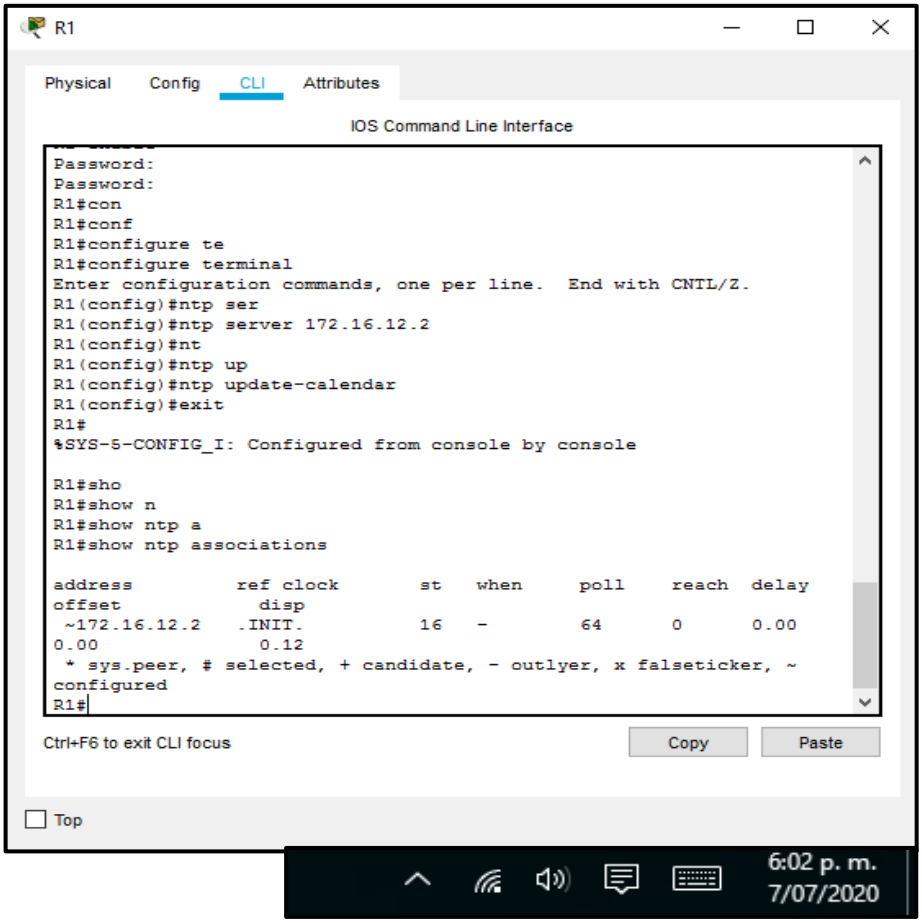
Parte 6: Configurar NTP

En el presente paso se ajusta la fecha y hora en el router 2, se procede a establecer a este como router maestro NTP, se configura al router 1 como cliente NTP, se configuran las actualizaciones de calendarios periódicos con hora NTP en router 1, por último, se verifica la configuración NTP en R1.

Configuración realizada

Dispositivo	Comandos Utilizados
Router 1	**R2(config)**#Clock set 9:00:00 march 5 2016 **R2(config)**#Ntp master 5
Router 2	**R1(config)**#Ntp server 172.16.1.2 ntp update-calendar **R1(config)**#Exit **R1**#Show ntp assosiations

Ilustración 9. Verificar configuración NTP



Nota: recuperado de packet tracer Escenario 1. Autor Anderson Quintero

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

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

En el presente paso, se realiza la configuración de las listas de control de acceso, se nombra una ACL que solo establezca una conexión telnet entre R1 y R2, se aplica la ACL con nombre para las líneas VTY, por último, se verifica su funcionamiento.

Configuración realizada

Dispositivo	Comandos Utilizados
Router 1	**R1(config)#**Telenet 172.16.1.2
Router 2	**R2(config)#**Ip Access-list standard ADMIN-MGT **R2(config-std-nacl)#**Permit host 172.16.1.1 **R2(config-std-nacl)#**Line vty 0 15 **R2(config-line)#**Access-list ADMIN-MGT in **R2(config-line)#**Transport input telnet

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

Tabla 20. Verificar NAT.

Descripción del Comando	Entrada del Estudiante
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	Show accest-lists
Restablecer los contadores de una lista de acceso	Clear Access-list
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	Show ip interface #Nombre interfaz#
¿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. Show ip nat trans

¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	No ip nat inside source list #Nombre lista#

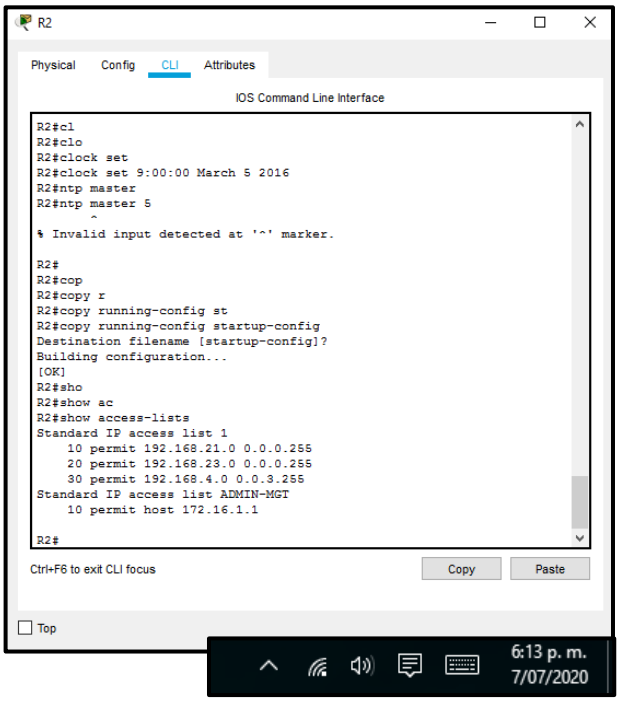
Fuente: Prueba de habilidades practicas CCNA – UNAD

En el presente paso, se verifican las coincidencias recibidas por la ACL desde la última vez que se restableció, se realiza el restablecimiento de la ACL, en seguida se verifica la ACL aplicada a una interfaz junto a su dirección IP, de igual manera se verifican las traducciones NAT y para finalizar se procede a practicar el cómo se eliminan las direcciones NAT dinámicas.

Configuración realizada

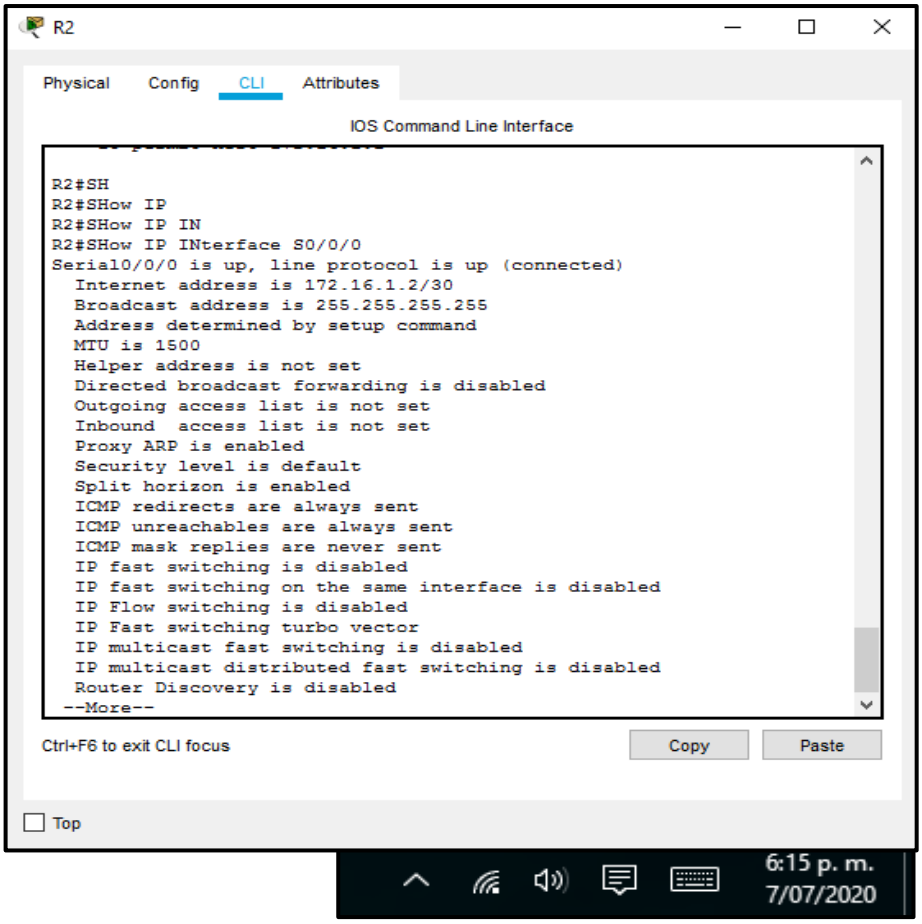
Dispositivo	Comandos Utilizados
Router 2	**R2#**Show Access-list **R2(config)#**Clear Access-list **R2(config)#**exit **R2#**Show ip interface S0/0/0 **R2#**Show ip nat trans **R2#**Configure terminal **R2(config)#**No ip nat inside source list #

Ilustración 10. Verificar ACL



Nota: recuperado de packet tracer Escenario 1. Autor Anderson Quintero

Ilustración 11. Verificar Interfaz



Nota: recuperado de packet tracer Escenario 1. Autor Anderson Quintero

ECENARIO 2

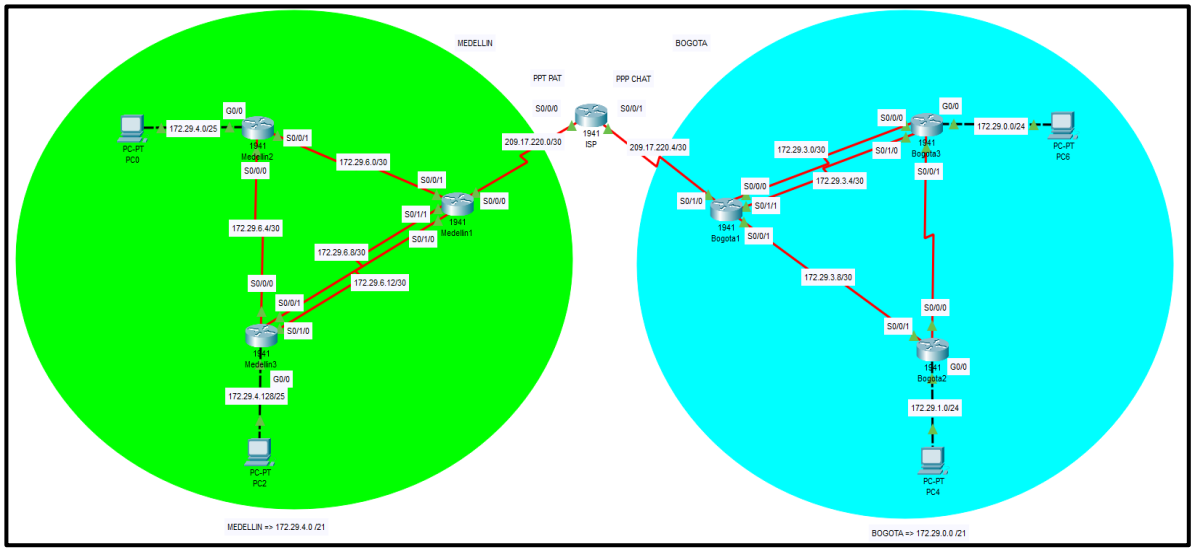
Desarrollo

Como trabajo inicial se debe realizar lo siguiente.

- ✓ Realizar las rutinas de diagnóstico y dejar los equipos listos para su configuración (asignar nombres de equipos, asignar claves de seguridad, etc.).

- ✓ Realizar la conexión física de los equipos con base en la topología de red

Ilustración 12. Topología escenario dos



Nota: recuperado de packet tracer Escenario 2. Autor Anderson Quintero

Parte 1: Configuración básica de los equipos

Paso 1: Realizar las rutinas de diagnóstico y dejar los equipos listos para su configuración (asignar nombres de equipos, asignar claves de seguridad, etc.).

En el presente paso se realiza la conexión de los diferentes elementos, se realiza la configuración básica de todos los elementos utilizados en el presente escenario, se estable nombre de host, seguridad de telnet y líneas vty, mensaje de restricción, encriptación de claves de seguridad y configuración del direccionamiento IPV4 de cada una de las interfaces, de igual manera se habilitan los puertos a utilizar en cada una de las redes y se verifica conectividad en la red.

Configuración realizada

Tabla 21. Configuración Básica Router Escenario 2

Dispositivo	Comandos Utilizados
Router ISP	**Router>**enable **Router#**configure terminal **Router(config)#**hostname ISP **ISP(config)#**enable secret class **ISP(config)#**line console 0 **ISP(config-line)#**password cisco **ISP(config-line)#**login **ISP(config-line)#**line vty 0 4 **ISP(config-line)#**password cisco **ISP(config-line)#**login **ISP(config-line)#**exit **ISP(config)#**banner motd #se prohíbe el acceso no autorizado# **ISP(config)#**service password-encryption **ISP(config)#**interface serial 0/0/0 **ISP(config-if)#**ip address 209.17.220.1 255.255.255.252 **ISP(config-if)#**description conecta a medellin1 **ISP(config-if)#**clock rate 128000 **ISP(config-if)#**no shutdown **ISP(config-if)#**interface serial 0/0/1 **ISP(config-if)#**ip address 209.17.220.5 255.255.255.252 **ISP(config-if)#**description conecta a Bogota1 **ISP(config-if)#**clock rate 128000 **ISP(config-if)#**no shutdown
Router Medellín 1	**Router>**enable **Router#**configure terminal **Router(config)#**hostname medellin1 **medellin1(config)#**enable secret class **medellin1(config)#**line console 0 **medellin1(config-line)#**password cisco **medellin1(config-line)#**login **medellin1(config-line)#**line vty 0 4 **medellin1(config-line)#**password cisco **medellin1(config-line)#**login **medellin1(config-line)#**exit **medellin1(config)#**banner motd #se prohíbe el acceso no autorizado# **medellin1(config)#**service password-encryption **medellin1(config)#**interface serial 0/0/0 **medellin1(config-if)#**ip address 209.17.220.2 255.255.255.252 **medellin1(config-if)#**description conecta a ISP **medellin1(config-if)#**no shutdown **medellin1(config-if)#**interface serial 0/0/1 **medellin1(config-if)#**ip address 172.29.6.1 255.255.255.252 **medellin1(config-if)#**description conecta a medellin2

	medellin1(config-if)#clock rate 128000 **medellin1(config-if)#**no shutdown **medellin1(config-if)#**interface serial 0/1/1 **medellin1(config-if)#**ip address 172.29.6.10 255.255.255.252 **medellin1(config-if)#**description conecta a medellin3 **medellin1(config-if)#**clock rate 128000 **medellin1(config-if)#**no shutdown **medellin1(config-if)#**interface serial 0/1/0 **medellin1(config-if)#**ip address 172.29.6.14 255.255.255.252 **medellin1(config-if)#**description conecta a medellin3 **medellin1(config-if)#**no shutdown
Router Medellín 2	**Router>**enable **Router#**configure terminal **Router(config)#**hostname medellin2 **medellin2(config)#**enable secret class **medellin2(config)#**line console 0 **medellin2(config-line)#**password cisco **medellin2(config-line)#**login **medellin2(config-line)#**line vty 0 4 **medellin2(config-line)#**password cisco **medellin2(config-line)#**login **medellin2(config-line)#**exit **medellin2(config)#**banner motd #se prohíbe el acceso no autorizado# **medellin2(config)#**service password-encryption **medellin2(config-if)#**interface serial 0/0/1 **medellin2(config-if)#**ip address 172.29.6.2 255.255.255.252 **medellin2(config-if)#**description conecta a medellin1 **medellin2(config-if)#**no shutdown **medellin2(config-if)#**interface serial 0/0/0 **medellin2(config-if)#**ip address 172.29.6.5 255.255.255.252 **medellin2(config-if)#**description conecta a medellin3 **medellin2(config-if)#**no shutdown **medellin2(config-if)#**interface g0/0 **medellin2(config-if)#**ip address 172.29.4.1 255.255.255.128 **medellin2(config-if)#**description conecta a red LAN **medellin2(config-if)#**no shutdown
Router Medellín 3	**Router>**enable **Router#**configure terminal **Router(config)#**hostname medellin3 **medellin3(config)#**enable secret class **medellin3(config)#**line console 0 **medellin3(config-line)#**password cisco **medellin3(config-line)#**login **medellin3(config-line)#**line vty 0 4 **medellin3(config-line)#**password cisco **medellin3(config-line)#**login **medellin3(config-line)#**exit **medellin3(config)#**banner motd #se prohíbe el acceso no autorizado# **medellin3(config)#**service password-encryption

	medellin3(config-if)#interface serial 0/0/0 **medellin3(config-if)#**ip address 172.29.6.6 255.255.255.252 **medellin3(config-if)#**description conecta a medellin2 **medellin3(config-if)#**no shutdown **medellin3(config-if)#**interface serial 0/0/1 **medellin3(config-if)#**ip address 172.29.6.9 255.255.255.252 **medellin3(config-if)#**description conecta a medellin1 **medellin3(config-if)#**no shutdown **medellin3(config-if)#**interface serial 0/1/0 **medellin3(config-if)#**ip address 172.29.6.13 255.255.255.252 **medellin3(config-if)#**description conecta a medellin1 **medellin3(config-if)#**no shutdown **medellin3(config-if)#**interface g0/0 **medellin3(config-if)#**ip address 172.29.4.128 255.255.255.128 **medellin3(config-if)#**description conecta a red LAN **medellin3(config-if)#**no shutdown
Router Bogotá 1	**Router>**enable **Router#**configure terminal **Router(config)#**hostname bogota1 **bogota1(config)#**enable secret class **bogota1(config)#**line console 0 **bogota1(config-line)#**password cisco **bogota1(config-line)#**login **bogota1(config-line)#**line vty 0 4 **bogota1(config-line)#**password cisco **bogota1(config-line)#**login **bogota1(config-line)#**exit **bogota1(config)#**banner motd #se prohíbe el acceso no autorizado# **bogota1(config)#**service password-encryption **bogota1(config)#**interface serial 0/1/0 **bogota1(config-if)#**ip address 209.17.220.6 255.255.255.252 **bogota1(config-if)#**description conecta a ISP **bogota1(config-if)#**no shutdown **bogota1(config-if)#**interface serial 0/0/0 **bogota1(config-if)#**ip address 172.29.3.1 255.255.255.252 **bogota1(config-if)#**description conecta a bogota3 **bogota1(config-if)#**clock rate 128000 **bogota1(config-if)#**no shutdown **bogota1(config-if)#**interface serial 0/1/1 **bogota1(config-if)#**ip address 172.29.3.5 255.255.255.252 **bogota1(config-if)#**description conecta a bogota3 **bogota1(config-if)#**no shutdown **bogota1(config-if)#**interface serial 0/0/1 **bogota1(config-if)#**ip address 172.29.3.10 255.255.255.252 **bogota1(config-if)#**description conecta a bogota2 **bogota1(config-if)#**no shutdown
Router Bogotá 2	**Router>**enable **Router#**configure terminal **Router(config)#**hostname bogota2

	bogota2(config)#enable secret class **bogota2(config)#**line console 0 **bogota2(config-line)#**password cisco **bogota2(config-line)#**login **bogota2(config-line)#**line vty 0 4 **bogota2(config-line)#**password cisco **bogota2(config-line)#**login **bogota2(config-line)#**exit **bogota2(config)#**banner motd #se prohíbe el acceso no autorizado# **bogota2(config)#**service password-encryption **bogota2(config-if)#**interface serial 0/0/1 **bogota2(config-if)#**ip address 172.29.3.9 255.255.255.252 **bogota2(config-if)#**description conecta a bogota1 **bogota2(config-if)#n**o shutdown **bogota2(config-if)#**interface serial 0/0/0 **bogota2(config-if)#**ip address 172.29.3.13 255.255.255.252 **bogota2(config-if)#**description conecta a bogota3 **bogota2(config-if)#**no shutdown **bogota2(config-if)#**interface g0/0 **bogota2(config-if)#**ip address 172.29.1.1 255.255.255.0 **bogota2(config-if)#**description conecta a red LAN **bogota2(config-if)#**no shutdown
Router Bogotá 3	**Router>**enable **Router#**configure terminal **Router(config)#**hostname bogota3 **bogota3(config)#**enable secret class **bogota3(config)#**line console 0 **bogota3(config-line)#**password cisco **bogota3(config-line)#**login **bogota3(config-line)#**line vty 0 4 **bogota3(config-line)#**password cisco **bogota3(config-line)#**login **bogota3(config-line)#**exit **bogota3(config)#**banner motd #se prohíbe el acceso no autorizado# **bogota3(config)#**service password-encryption **bogota3(config-if)#**interface serial 0/0/0 **bogota3(config-if)#**ip address 172.29.3.2 255.255.255.252 **bogota3(config-if)#**description conecta a bogota1 **bogota3(config-if)#**no shutdown **bogota3(config-if)#**interface serial 0/1/0 **bogota3(config-if)#**ip address 172.29.3.6 255.255.255.252 **bogota3(config-if)#**description conecta a bogota1 **bogota3(config-if)#**no shutdown **bogota3(config-if)#**interface serial 0/0/1 **bogota3(config-if)#**ip address 172.29.3.14 255.255.255.252 **bogota3(config-if)#**description conecta a bogota2 **bogota3(config-if)#**no shutdown **bogota3(config-if)#**interface g0/0 **bogota3(config-if)#**ip address 172.29.0.1 255.255.255.0

	bogota3(config-if)#description conecta a red LAN **bogota3(config-if)#**no shutdown

Parte 2: Configuración del enrutamiento

Paso 1: Configurar el enrutamiento en la red usando el protocolo OSPF versión 2, declare la red principal, desactive la sumarización automática.

Paso 2: 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

En el presente paso se habilita el protocolo ospf versión 2, se declara la red principal y el área con el que se trabajara que por defecto es la cero.

Configuración realizada

Tabla 22. Configuración Protocolo OSPF

Dispositivo	Comandos Utilizados
Router Medellín 1	**medellin1(config)#**router ospf 1 **medellin1(config)#**router id 1.1.1.1 **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)#**defalut-information originate
Router Medellín 2	**medellin2(config)#**router ospf 1 **medellin2(config)#** router id 2.2.2.2 **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)#**network 172.29.4.0 0.0.0.127 area 0 **medellin1(config-router)#**defalut-information originate
Router Medellín 3	**medellin3(config)#**router ospf 1 **medellin3(config)#** router id 3.3.3.3 **medellin3(config-router)#**network 172.29.6.8 0.0.0.3 area 0 **medellin3(config-router)#**network 172.29.6.12 0.0.0.3 area 0 **medellin3(config-router)#**network 172.29.6.4 0.0.0.3 area 0 **medellin3(config-router)#**network 172.29.4.128 0.0.0.127 area 0 **medellin3(config-router)#**defalut-information originate
Router Bogotá 1	**bogota1(config)#**router ospf 1 **bogota1(config)#** router id 4.4.4.4 **bogota1(config-router)#**network 172.29.3.0 0.0.0.3 area 0 **bogota1(config-router)#**network 172.29.3.4 0.0.0.3 area 0 **bogota1(config-router)#**network 172.29.3.8 0.0.0.3 area 0 **bogota1(config-router)#**defalut-information originate

Router Bogotá 2	**bogota2(config)#**router ospf 1 **bogota2(config)#**router id 5.5.5.5 **bogota2(config-router)#**network 172.29.3.12 0.0.0.3 area 0 **bogota2(config-router)#**network 172.29.3.8 0.0.0.3 area 0 **bogota2(config-router)#**network 172.29.1.0 0.0.0.255 area 0 **bogota2(config-router)#**defalut-information originate
Router Bogotá 3	**bogota3(config)#**router ospf 1 **bogota3(config)#** router id 6.6.6.6 **bogota3(config-router)#**network 172.29.3.0 0.0.0.3 area 0 **bogota3(config-router)#**network 172.29.3.4 0.0.0.3 area 0 **bogota3(config-router)#**network 172.29.3.12 0.0.0.3 area 0 **bogota3(config-router)#**network 172.29.0.0 0.0.0.255 area 0 **bogota3(config-router)#**defalut-information originate

Paso 3: 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.

En el presente paso se realiza la Sumarización de las redes internas de Bogotá y Medellín, en este caso las redes son 172.29.0.0 /24, 172.29.1.0/24, 172.29.4.0 /25 y 172.29.4.128 /25, para el presente caso según lo señalado en la guía se realizará con mascará /22, se realiza la configuración de las rutas estáticas para el vínculo del router ISP a la conectividad de la RED.

Configuración realizada

Tabla 23. Configuración rutas estáticas

Dispositivo	Comandos Utilizados
Router ISP	**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
Router Medellín 1	**medellin1(config)#**ip route 0.0.0.0 0.0.0.0 209.17.220.1
Router Bogotá 1	**bogota1(config)#**ip route 0.0.0.0 0.0.0.0 209.17.220.5

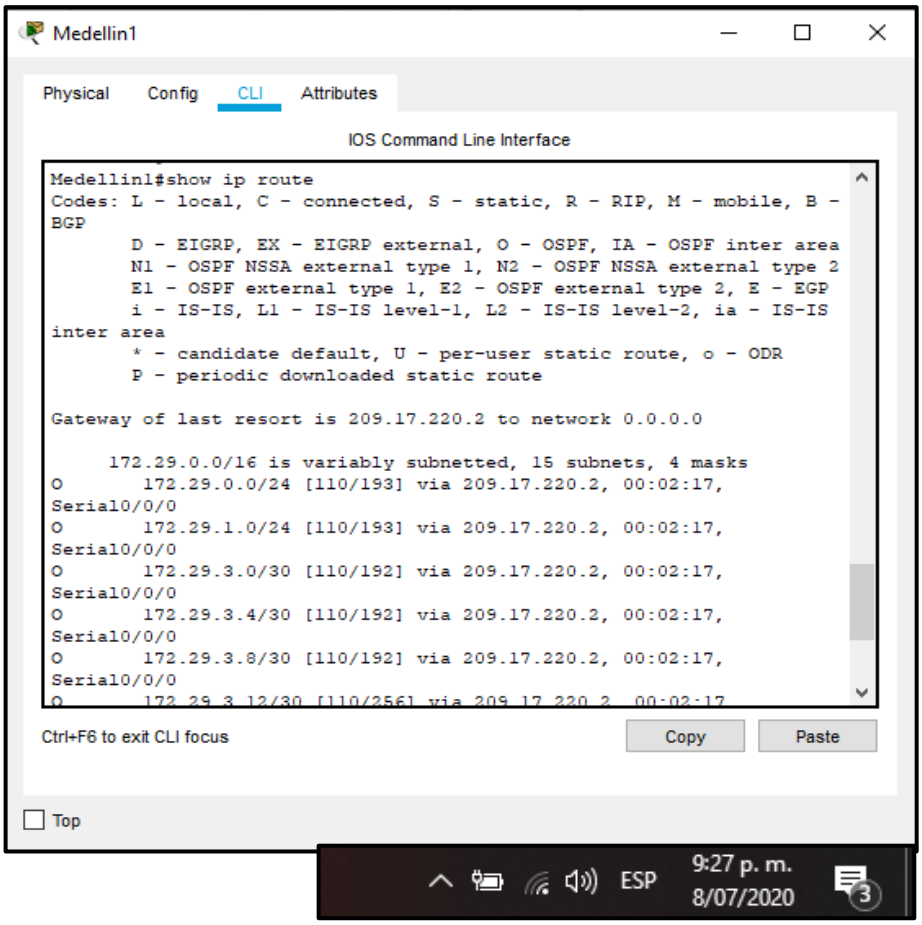
Parte 4: Tabla de Enrutamiento.

Paso 1: Verificar la tabla de enrutamiento en cada uno de los routers para comprobar las redes y sus rutas

Se procede a utilizar el comando show ip route, con el fin de verificar la tabla de enrutamiento de la red, para el presente ejemplo tomamos la imagen aplicada sobre

el router Medellin1, se puede observar el enrutamiento, donde se conocen las redes directamente conectadas y propagadas por el protocolo OSPF.

Ilustración 13. Verificar enrutamiento Router medellin1

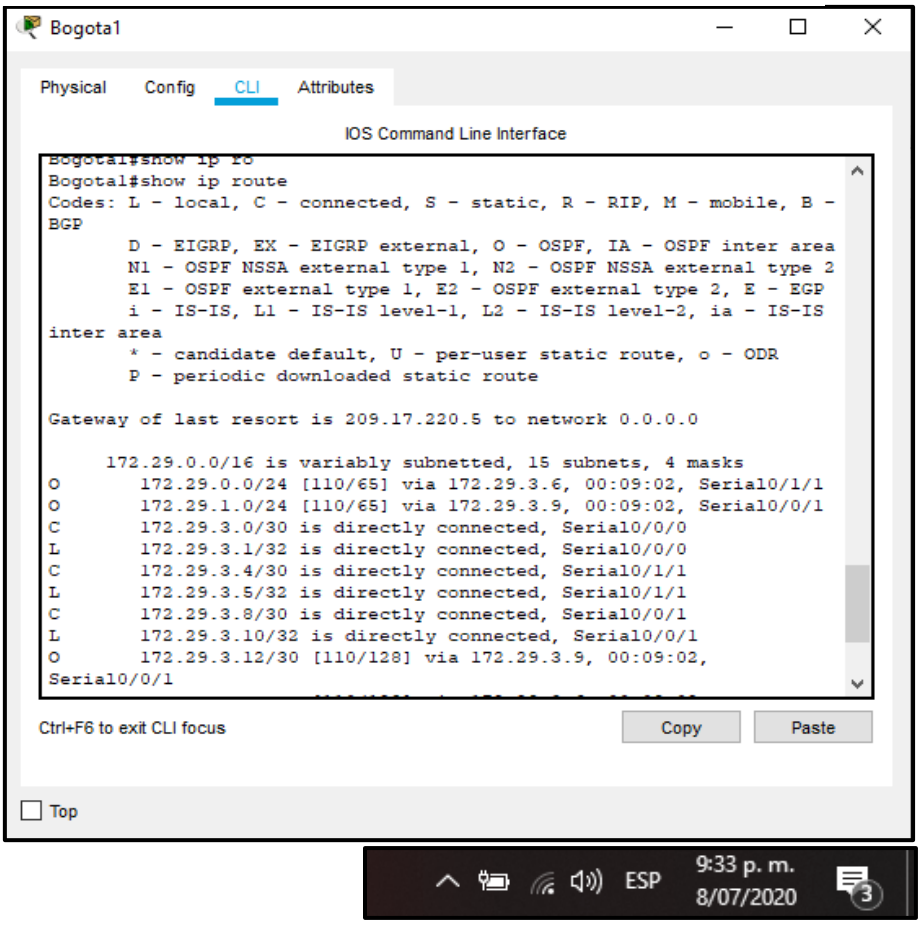


Nota: recuperado de packet tracer Escenario 2. Autor Anderson Quintero

Paso 2: Verificar el balanceo de carga que presentan los routers.

Se verifica la tabla de enrutamiento en los router principales de las ciudades, en este bogota1, con el fin de verificar la aplicación del protocolo OSPF y la distribución de las cargas, una vez se realice la configuración señalada en la guía de la actividad.

Ilustración 14. Verificar enrutamiento router Bogota1

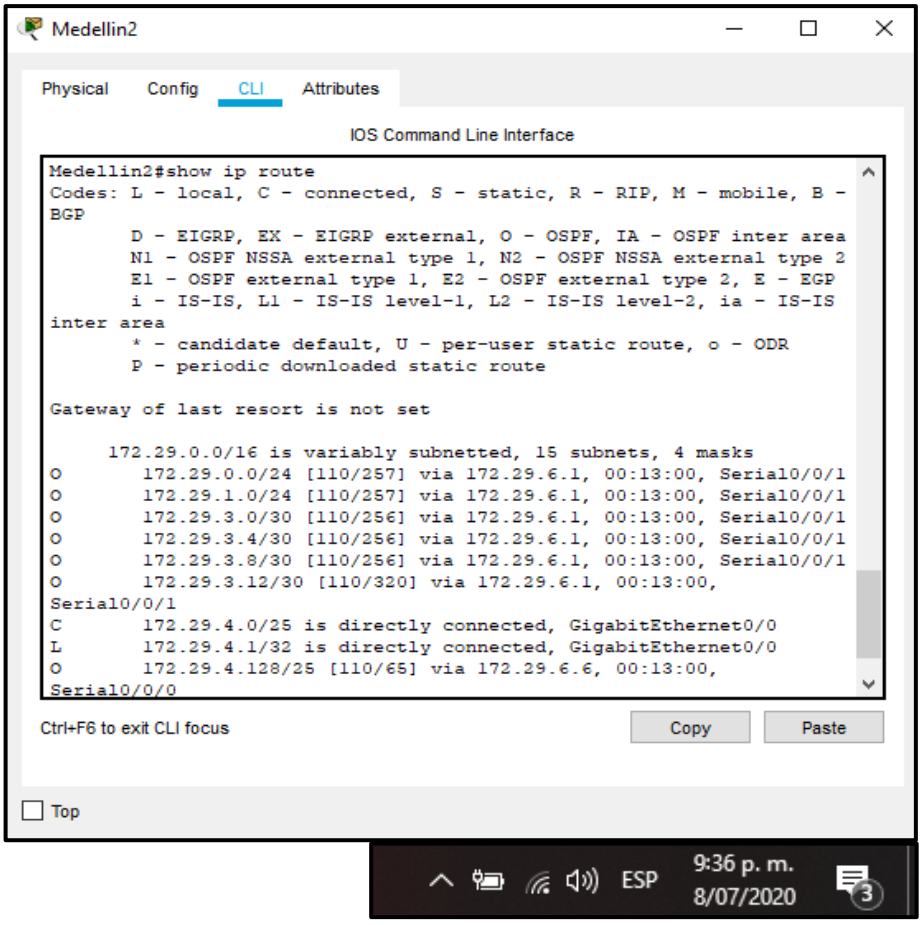


Nota: recuperado de packet tracer Escenario 2. Autor Anderson Quintero

Notas adicionales de la guía

- ✓ 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.
- ✓ 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.

Ilustración 15. Verificar enrutamiento router Medellin2



Nota: recuperado de packet tracer Escenario 2. Autor Anderson Quintero

Parte 5: Deshabilitar la propagación del protocolo OSPF

En el presente paso se desactivan las interfaces que no requieren la propagación del protocolo, en este caso se refiere a las redes las de cada uno de las ciudades, se aplica a las interfaces gigabit ethernet de los router medellin2, medellin3, bogota2 y bogota3.

Configuración realizada

Tabla 24. Deshabilitar propagación protocolo OSPF

Dispositivo	Comandos Utilizados
Router Medellín 2	**medellin1(config-router)**#passive-interface g0/0
Router Medellín 3	**medellin3(config-router)**#passive-interface g0/0

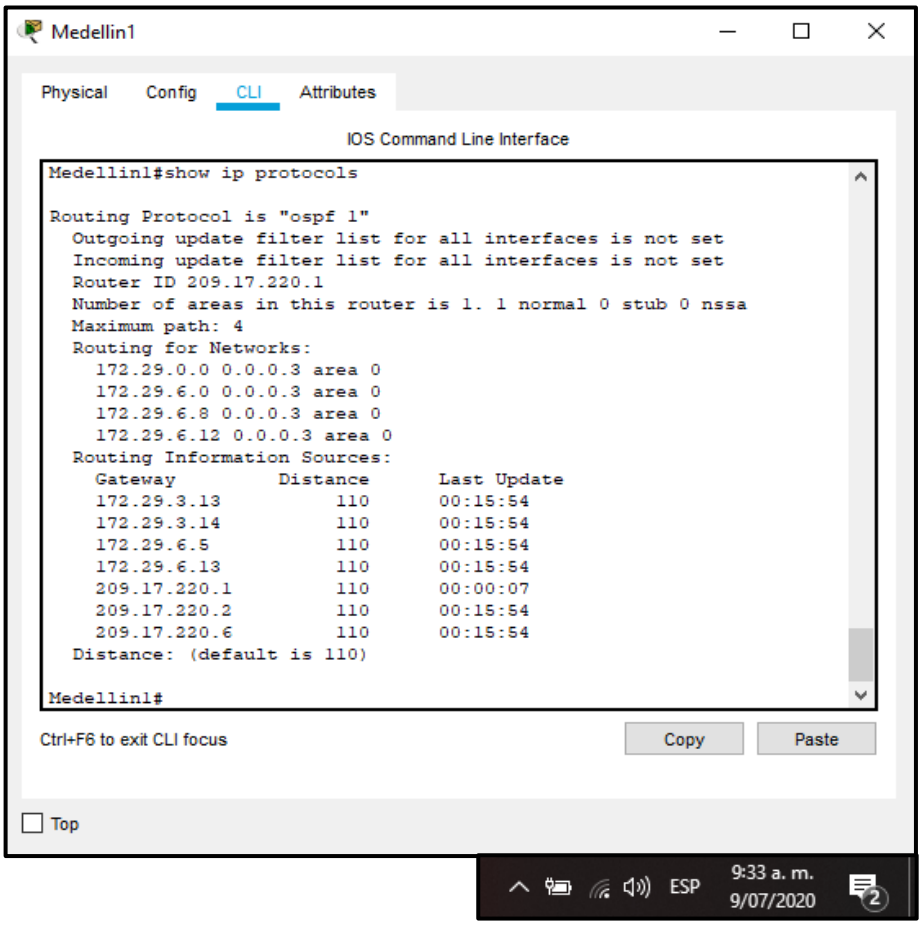
Router Bogotá 2	**bogota2(config-router)**#passive-interface g0/0
Router Bogotá 3	**bogota3(config-router)**#passive-interface g0/0

Parte 6: Verificación del protocolo OSPF.

Paso 1: 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.

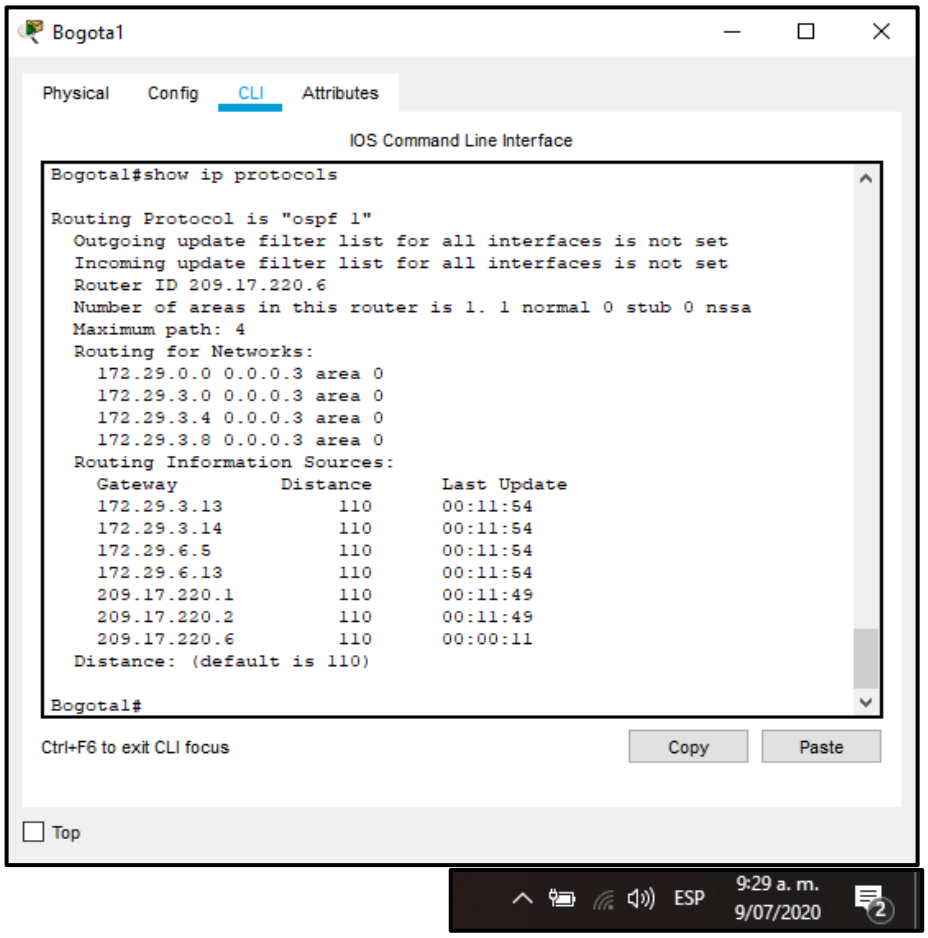
En el presente paso se verifica e los router principales de las ciudades el protocolo de enrutamiento utilizado, para el presente caso el protocolo OSPF.

Ilustración 16. Verificar Protocolo OSPF router Medellin1



Nota: recuperado de packet tracert Escenario 2. Autor Anderson Quintero

Ilustración 17. Verificar protocolo OSPF en router Bogota1

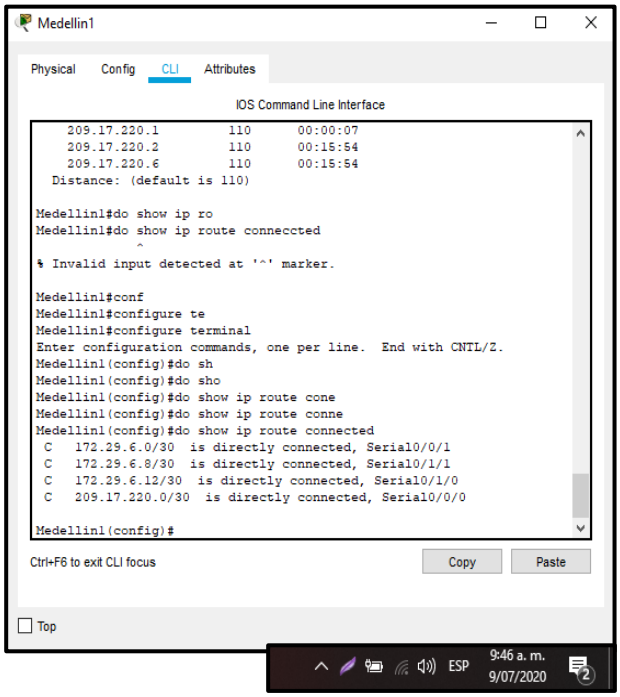


Nota: recuperado de packet tracer Escenario 2. Autor Anderson Quintero

Paso 2: 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.

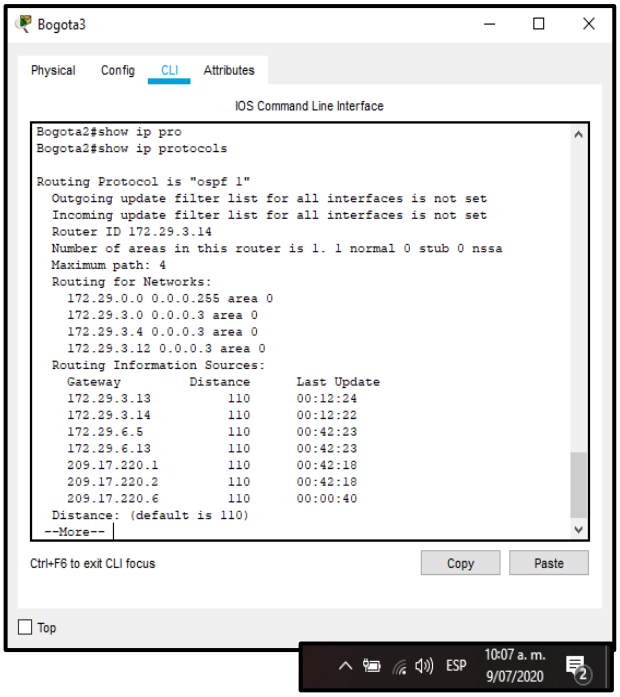
En el presente paso se continua la verificación del protocolo OSPF, en este caso se verificarán para complementar las rutas directamente conectadas, en el paso anterior se verifico el enrutamiento del protocolo, la presente sería una imagen complementaria de la conectividad de la tipología de red.

Ilustración 18. Verificar protocolo OSPF en router Medellin1



Nota: recuperado de packet tracer Escenario 2. Autor Anderson Quintero

Ilustración 19. Verificar protocolo OSPF en router Bogota3



Nota: recuperado de packet tracer Escenario 2. Autor Anderson Quintero

Parte 7: Configurar encapsulamiento y autenticación PPP

Paso 1: Según la topología se requiere que el enlace Medellín1 con ISP sea configurado con autenticación PAP.

En el presente paso se realiza la configuración del encapsulamiento y autenticación PPP, para el caso de ISP con enlace a Medellin1 se utilizará la autenticación PAP, que básicamente son medidas de seguridad para proteger la conexión WAN.

Tabla 25. Configurar autenticación PAP

Dispositivo	Comandos Utilizados
Router ISP	**ISP(config-if)#**int s0/0/0 **ISP(config-if)#** encapsulation ppp **ISP(config-if)#** ppp authenticacion pap **ISP(config-if)#** ppp pap sent-username ISP password cisco
Router Medellín1	**Medellin1(config-if)#**int s0/0/0 **Medellin1 (config-if)#** encapsulation ppp **Medellin1 (config-if)#** ppp authenticacion pap **Medellin1 (config-if)#** ppp pap sent-username Medellin1 password cisco

Paso 2: El enlace Bogotá1 con ISP se debe configurar con autenticación CHAT.

En el presente paso se realiza la configuración del encapsulamiento y autenticación PPP, para el caso de ISP con enlace a Medellin1 se utilizará la autenticación CHAP, que básicamente son medidas de seguridad para proteger la conexión WAN.

Tabla 26. Configurar autenticación CHAP

Dispositivo	Comandos Utilizados
Router ISP	**ISP(config)#**username Bogota1 password cisco **ISP(config-if)#**int s0/0/1 **ISP(config-if)#** encapsulation ppp **ISP(config-if)#** ppp authenticacion chap
Router Bogota1	**Bogota1(config)#** username ISP password cisco **Bogota1(config-if)#**int s0/1/0 **Bogota1(config-if)#** encapsulation ppp **Bogota1(config-if)#** ppp authenticacion chap

Parte 8 configuración de PAT

Notas de la guía

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.

Paso 1: 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.

Tabla 27. Configuración de PAT

Dispositivo	Comandos Utilizados
Router Medellin1	**Medellin1(config)#**ip accest-list standard LAN-MEDELLIN **Medellin1(config-std-nacl)#**permit 172.29.0.0 0.0.255.255 **Medellin1(config-std-nacl)#**exit **Medellin1(config)#**ip nat inside source list LAN-MEDELLIN interface s0/1/0 overload **Medellin1(config)#**interface s0/1/0 **Medellin1(config-if)#**ip nat outside **Medellin1(config-if)#**exit **Medellin1(config)#**interface s0/0/1 **Medellin1(config-if)#**ip nat outside **Medellin1(config-if)#**exit **Medellin1(config)#**interface s0/0/0 **Medellin1(config-if)#**ip nat outside **Medellin1(config-if)#**exit **Medellin1(config)#**interface s0/1/1 **Medellin1(config-if)#**ip nat outside **Medellin1(config-if)#**exit
Router Bogota1	**Bogota1(config)#**ip accest-list standard LAN-BOGOTA **Bogota1(config-std-nacl)#**permit 172.29.0.0 0.0.255.255 **Bogota1(config-std-nacl)#**exit **Medellin1(config)#**ip nat inside source list LAN-BOGOTA interface s0/1/0 overload **Bogota1(config)#**interface s0/0/0 **Bogota1(config-if)#**ip nat outside **Bogota1(config-if)#**exit **Bogota1(config)#**interface s0/0/1 **Bogota1(config-if)#**ip nat outside **Bogota1(config-if)#**exit **Bogota1(config)#**interface s0/1/0

	Medellin1(config-if)#ip nat outside **Medellin1(config-if)#**exit **Medellin1(config)#**interface s0/1/1 **Medellin1(config-if)#**ip nat outside **Medellin1(config-if)#**exit

Parte 9: Configuración del servicio DHCP

Paso 1: Configurar la red Medellín2 y Medellín3 donde el router Medellín 2 debe ser el servidor DHCP para ambas redes LAN.

En el presente paso se realizará la configuración al router Medellin2 como DHCP de las redes LAN de esta ciudad.

Tabla 28. Configuración router Medellin2 como DHCP

Dispositivo	Comandos Utilizados
Router Medellin2	**Medellin2(config)#**ip dhcp excluded-address 172.29.4.0 172.29.4.9 **Medellin2(config)#**ip dhcp pool MEDELLIN-LAN1 **Medellin2(dhcp-config)#**network 172.29.4.0 255.255.255.128 **Medellin2(dhcp-config)#**default-router 172.29.4.1 **Medellin2(dhcp-config)#**domain-name LAN1-MEDELLIN.COM **Medellin2(dhcp-config)#**exit **Medellin2(config)#**ip dhcp excluded-address 172.29.4.128 172.29.4.139 **Medellin2(config)#**ip dhcp pool MEDELLIN-LAN2 **Medellin2(dhcp-config)#**NETwork 172.29.4.128 255.255.255.128 **Medellin2(dhcp-config)#**default-router 172.29.4.129 **Medellin2(dhcp-config)#**domain-name LAN2-MEDELLIN.COM **Medellin2(dhcp-config)#**end
Router Medellin3	**Medellin3(config)#**interface g0/0 **Medellin3(config-if)#**ip helper-address 172.29.6.5

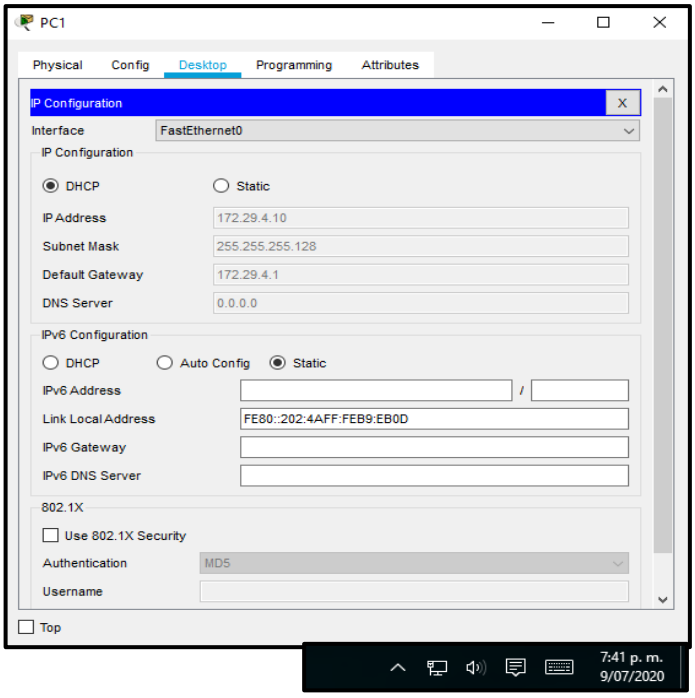
Paso 2: Configurar la red Bogotá2 y Bogotá3 donde el router Bogota2 debe ser el servidor DHCP para ambas redes Lan.

En el presente paso se realizará la configuración al router Medellin2 como DHCP de las redes LAN de esta ciudad.

Tabla 29. Configuración router Bogota2 como DCHP

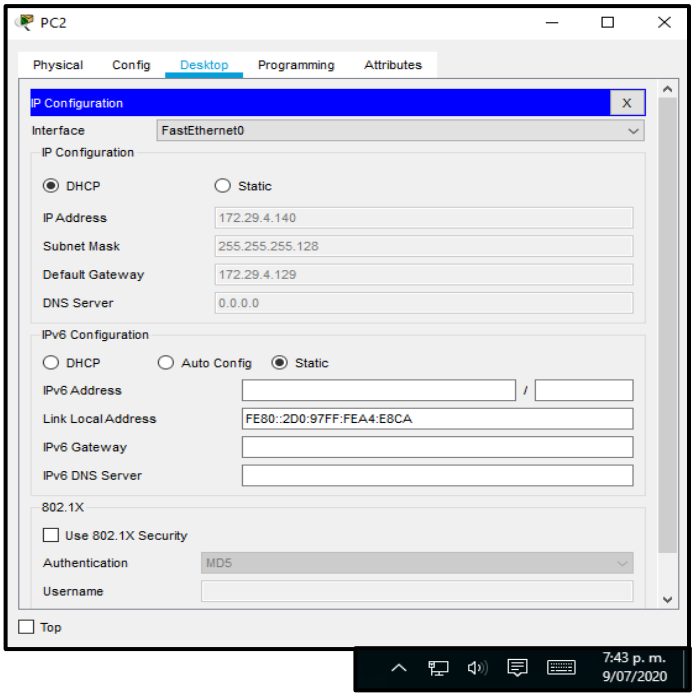
Dispositivo	Comandos Utilizados
Router Bogota2	**Bogota2(config)**#ip dhcp excluded-address 172.29.0.0 172.29.0.9 **Bogota2 (config)**#ip dhcp pool BOGOTA-LAN1 **Bogota2 (dhcp-config)**#network 172.29.0.0 255.255.255.0 **Bogota2 (dhcp-config)**#default-router 172.29.0.1 **Bogota2 (dhcp-config)**#domain-name LAN1-BOGOTA.COM **Bogota2 (dhcp-config)**#exit **Bogota2 (config)**#ip dhcp excluded-address 172.29.1.0 172.29.1.9 **Bogota2 (config)**#ip dhcp pool BOGOTA-LAN2 **Bogota2 (dhcp-config)**#NETwork 172.29.1.0 255.255.255.0 **Bogota2 (dhcp-config)**#default-router 172.29.1.1 **Bogota2 (dhcp-config)**#domain-name LAN2-BOGOTA.COM **Bogota2 (dhcp-config)**#end
Router **Bogota3**	**Bogota3(config)**#interface g0/0 **Bogota3(config-if)**#ip helper-address 172.29.3.13

Ilustración 20. DCHP LAN1 Medellín



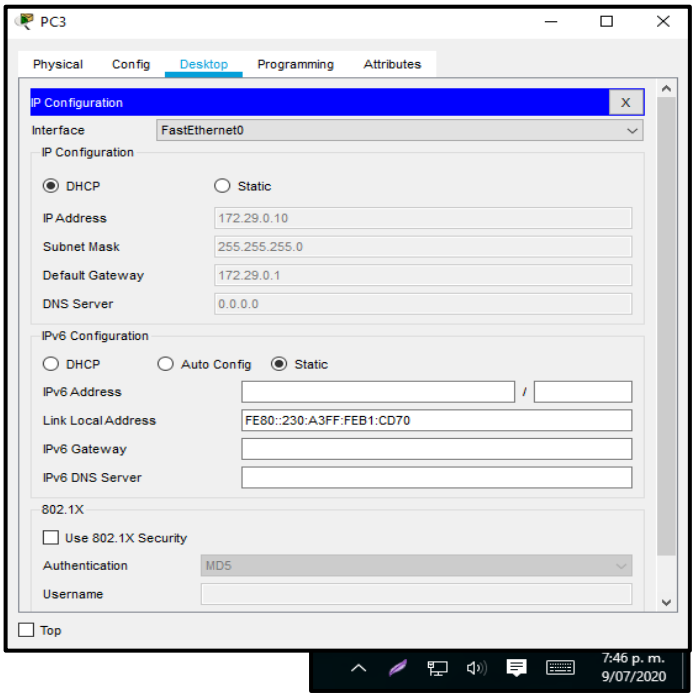
Nota: recuperado de packet tracer Escenario 2. Autor Anderson Quintero

Ilustración 21. DHCP LAN2 Medellín



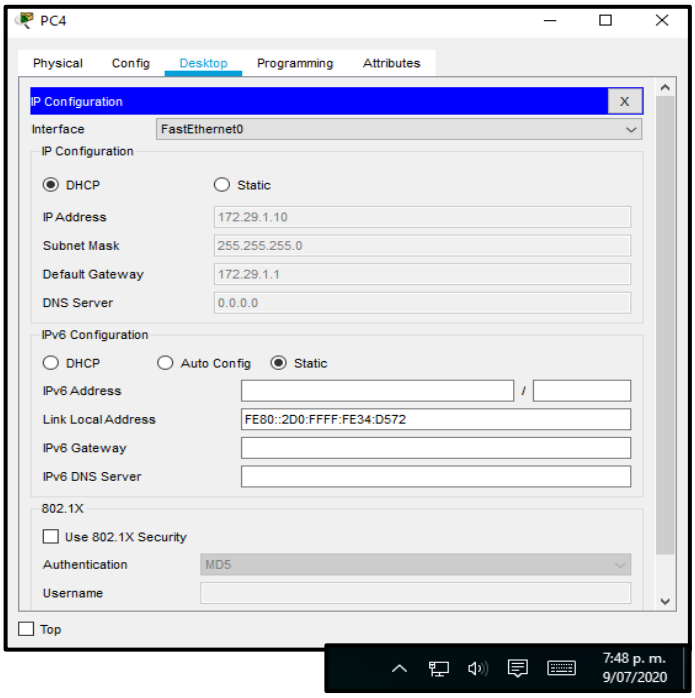
Nota: recuperado de packet tracer Escenario 2. Autor Anderson Quintero

Ilustración 22. DHCP LAN1 Bogotá



Nota: recuperado de packet tracer Escenario 2. Autor Anderson Quintero

Ilustración 23. DHCP LAN2 Bogotá



Nota: recuperado de packet tracer Escenario 2. Autor Anderson Quintero

CONCLUSIONES

- ✓ El presente trabajo permitió plantear las diferentes habilidades obtenidas a lo largo del desarrollo del curso, aplicación de competencias prácticas en la resolución de problemas de configuración real en una red empresarial, siempre aplicada al mejoramiento de la comunicación empresarial.

- ✓ La configuración básica aplicada a cada uno de los elementos, permite un campo practico de experiencia, teniendo en cuenta que es la configuración mínima aplicar en la construcción de una nueva red de comunicaciones.

- ✓ Los diferentes tipos de configuraciones realizadas en los diferentes elementos, se ajustan a las necesidades identificadas, se aplican los protocolos y se crean las diferentes redes que permiten la comunicación por diferentes medios, permitiendo así una red completa y ajustada detalladamente.

- ✓ Se realizan las configuraciones acordes al desarrollo de la guía, se realiza la configuración básica de cada elemento, se crean vlan y se configuran en las subinterfaces de los router, se simula un servidor web y http, se configura el direccionamiento dhcp en un rango asignado de direcciones ip, se aplica el protocolo rip versión 2, se configura NAT estática y dinámica dependiendo de las observaciones del documento, se estructura una red ajustada a las necesidades empresariales. Con base en lo anterior se culmina a satisfacción la prueba practica de conocimientos.

- ✓ Se aplica la configuración del protocolo OSPF versión como protocolo de enrutamiento dinámico, se observa su método de propagación e interconexión para dar a conocer las redes que no están directamente conectadas, el uso del protocolo se recomienda para redes de gran tamaño.

BIBLIOGRAFIA

CISCO. (2019). Configuración de un sistema operativo de red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#2

Vesga, J. (2014). Diseño y configuración de redes con Packet Tracer [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgCT9VCtl_pLtPD9

CISCO. (2019). Protocolos y comunicaciones de red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#3

CISCO. (2019). Acceso a la red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#4

CISCO. (2019). Ethernet. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#5

CISCO. (2019). Capa de red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#6

CISCO. (2019). Direccionamiento IP. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#7

CISCO. (2019). División de redesIP en subredes. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#8

CISCO. (2019). Capa de transporte. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#9

CISCO. (2019). Capa de aplicación. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#10

CISCO. (2019). Configuración de un sistema operativo de red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#11

CISCO. (2019). Conceptos de Routing. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#1

CISCO. (2019). Routing Estático. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#2

ANEXOS

LINK DE ACCESO ESCENARIOS PACKET TRACER

https://drive.google.com/drive/folders/1ekxvd96LScvTjDMnhk5IfHymcc0MW5CE?usp=sharing