# PRUEBA DE HABILIDADES CCNA 2020

JHON JAIRO TRUJILLO CAPERA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD

ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERÍA ECBTI

INGENIERÍA EN SISTEMAS

NEIVA – HUILA

2020

# PRUEBA DE HABILIDADES CCNA 2020

JHON JAIRO TRUJILLO CAPERA

TUTOR:

HÉCTOR JULIÁN PARRA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD

ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERÍA ECBTI

INGENIERÍA EN SISTEMAS

NEIVA - HUILA

2020

Nota de Aceptación

Presidente del

Jurado

Jurado

Jurado

Algeciras Huila 15 de mayo del 2020

## DEDICATORIA

A mis padres por brindarme ese apoyo siempre, esa voz de aliento, ese tú puedes, a todos nuestros compañeros durante la trayectoria del desarrollo del programa, hoy dedico este documento aquellos que cada día se especializan, que tienen metas claras y que luchan cada día para poder hacerlas realidad, con el fin de motivarlos y de decirles que nos es fácil pero tampoco por que sea difícil debemos dejarlo, un día llegaran a esta etapa de superación y evaluaran que todo el esfuerzo realizado valió la pena.

## AGRADECIEMIENTOS

A los tutores de la UNAD en especial al tutor del curso Hector Julian Parra por brindarnos asesoría constante en este proceso formativo, a nuestra universidad por brindar formación profesional de calidad en su modalidad virtual, también aquellas personas que me desearon éxito en mi carrera como futuro ingeniero de sistemas, una etapa más y muchas metas nuevas por cumplir, a ellos les dejare en este documento un gracias, son cortas las palabras para poder agradecer a todos los que participaron en este nuevo reto y a mis padres por su apoyo incondicional.

## TABLA DE CONTENIDO

Pág.

LISTA DE TABLAS

## LISTA DE FIGURAS

# GLOSARIO

**Conectividad:** Capacidad de establecer una conexión: una comunicación, un vínculo. El concepto suele aludir a la disponibilidad que tiene de un dispositivo para ser conectado a otro o a una red.

**Configurar:** Grupo de datos e información que caracteriza a diferentes elementos de una computadora, como pueden ser programas, aplicaciones o elementos de hardware / software. La configuración es lo que hace que cada parte de la computadora cumpla una función específica porque es lo que eventualmente la define.

**Encapsulamiento:** Proceso que interviene en el momento en que se envían los datos a través de una determinada Red, de modo que se pueden ordenar, administrar y hasta verificar si han llegado a destino, en qué estado, o si ha sido eficiente la operación, referida comúnmente como Encapsulamiento de Datos.

**Escenario:** Los escenarios son parte de una serie de comandos a veces denominados herramientas de análisis.

**Interfaz:** La conexión física y funcional que se establece entre dos aparatos, dispositivos o sistemas que funcionan independientemente uno del otro.

**Protocolo:** Un protocolo es un conjunto de reglas usadas por computadoras para comunicarse unas con otras a través de una red. Un protocolo es una convención o estándar que controla o permite la conexión, comunicación, y transferencia de datos entre dos puntos finales.

**Puerto:** Es una interfaz a través de la cual se pueden enviar y recibir los diferentes tipos de datos.

**Red:** Es un conjunto de equipos conectados por medio de cables, señales, ondas cualquier otro método de transporte de datos, que comparten información (archivos), recursos (CD-ROM, impresoras, etc.) y servicios (acceso a internet, email y chat)

**Router:** Un router es un dispositivo de hardware que permite la interconexión de ordenadores en red. El router o enrutador es un dispositivo que opera en capa tres de nivel de 3. Así, permite que varias redes u ordenadores se conecten entre sí y, por ejemplo, compartan una misma conexión de Internet.

**Topología:** Cadena de comunicación usada por los nodos que conforman una red para comunicarse.

**Trazas:** La traza de un algoritmo (o programa) indica la secuencia de acciones (instrucciones) de su ejecución, así como, el valor de las variables del algoritmo (o programa) después de cada acción (instrucción).

## RESUMEN

Afortunadamente Cisco, Líder mundial en la fabricación y comercialización de componentes de comunicación, ofrece la oportunidad de certificarse realizando los cursos CCNA. Según CISCO la certificación CCNA “Es una de las certificaciones más importantes dentro de la industria de la Tecnología de la Información. Esta certificación representa el nivel asociado, orientada a habilidades prácticas en el diagnóstico y solución de problemas específicos de redes.” (Cobos Domínguez, 2017).

Este proyecto hace parte de la prueba de habilidades de la certificación CCNA. Vamos a desarrollar dos escenarios prácticos utilizando la herramienta Packet Tracert y las temáticas: direccionamiento IP, Configuración Básica de Routers y detección de vecinos, seguridad en la red, balanceo de carga, Configuración de protocolo de enrutamiento EIGRP, creación de Vlans, Configuración de NAT estático y de sobrecarga y configuración de listas de control de acceso.



**Palabras clave**

**Cisco:** es una empresa global con sede en San José,1 California, Estados Unidos, principalmente dedicada a la fabricación, venta, mantenimiento y consultoría de equipos de telecomunicaciones.

**Ip:** Una dirección IP es un número que identifica de forma única a una interfaz en red de cualquier dispositivo conectado a ella que utilice el protocolo IP (Internet Protocol), que corresponde al nivel de red del modelo TCP/IP.

**Vlans:** es un acrónimo de virtual LAN (red de área local virtual), es un método para crear redes lógicas independientes dentro de una misma red física. Varias VLAN pueden coexistir en un único conmutador físico o en una única red física.

**Nat:** es un mecanismo utilizado por routers IP para intercambiar paquetes entre dos redes que asignan mutuamente direcciones incompatibles. Consiste en convertir, en tiempo real, las direcciones utilizadas en los paquetes

# INTRODUCCIÓN

Las configuraciones de redes permiten especificar la manera en la que un sistema se logra conectar con otros equipos y al internet, en donde se deben tener en cuenta un sin número de pasos para poder ejecutarlo de manera adecuada a través de ciertas ayudas que lograr completar el objetivo; por medio del cual los diferentes dispositivos lograr el objetivo empresarial de acceder a diferentes medios para comunicarse y realizar labores.

Teniendo en cuenta la etapa de transición que afronta el planeta, se puede observar que el avance de despliegue de infraestructura que permite la conectividad entre diferentes áreas y ubicaciones en tiempo real, relevamos la importancia de los conocimientos necesarios, la era digital necesita potenciales que ayuden a la innovación, para convertir ciudades y personas digitales, en el transcurso de este curso realizamos una serie de configuraciones que nos ayudaron a ampliar el conocimiento en el tema de conectividad, nos llevamos una idea de su funcionamiento y su método de parametrización, Como estudiante de Ingeniería de Sistemas y en medio de la era de la Información se hace necesario tener grandes conocimientos en redes de datos. Estos conocimientos nos permiten adaptarnos a un creciente mercado mundial que demanda a diario profesionales competitivos y con la capacidad para entender, diseñar e implementar redes de datos. Además, se hace necesario poder diagnosticar y dar solución a los problemas específicos sobre redes.

En esta ocasión se desarrollaron temáticas como la habilitación de interfaces, reconocimientos de protocolos de conexión y reconfiguración de una red con 3 zonas.

# OBJETIVOS

## Objetivo general

Fortalecer los conocimientos necesarios para el diseño de redes mediante el uso del modelo jerárquico de tres niveles, con el fin de optimizar el rendimiento de la red e incorporar de manera adecuada el uso de tecnologías y protocolos de conmutación y enrutamiento.

## Objetivos específicos

- Definir la topología de red a trabajar
- Conectar todos los equipos de red según lo requerido
- Realizar el respectivo enrutamiento para cada dispositivo de red
- Realizar la respectiva configuración a la red final para dar solución a los escenarios propuestos

## PLANTEAMIENTO DEL PROBLEMA

Definición del problema

Es necesario el conocimiento amplio entorno a las configuraciones de una red, que permitan la comunicación empresarial de una organización en las diferentes sedes ubicados en diferentes puntos geográficos de la ciudad, para ello es necesario de la aplicación de los conocimientos amplios entorno a la implementación de estos elementos que ayuden al crecimiento exponencial de la empresa.

Se dará solución a los dos escenarios allí especificados sobre la configuración de topologías de red y conectividad, implementando los diferentes protocolos y tecnología disponible para lograr el objetivo de esta fase final, con la ayuda frecuente en todo el tema de asesoría de nuestros tutores de la Universidad Nacional abierta y a Distancia.

## JUSTIFICACIÓN

La configuración de una red es indispensable dentro del funcionamiento de cualquier estructura organizacional que requiera de comunicación constante y mutua, es así, que nace la necesidad de crear una que permita y aplique los conocimientos adquiridos a través de ejemplos claros en torno al material de aprendizaje adquirido durante el proceso de formación en torno a los conocimientos sustentados; es así que por medio un programa simultaneo en donde se puedan ver los avances y la comunicación que se implementara para la empresa, se verán os resultados a través del visto bueno por parte del servidor dado para las aplicaciones.

Los siguientes escenarios se realizan para evaluar las competencias y conocimientos adquiridos con los módulos vistos CCNA1 y CCNA2, con el fin de afinar nuestros potenciales como futuros ingenieros de sistemas, podamos contar con los conocimientos necesarios para resolver los inconvenientes que se nos puedan presentar en el campo laboral, sin embargo el desarrollo de este ejercicio propone un nuevo método de solución con la implementación de OSPF, permitiendo indagar y lograr la solución del escenario propuesto.

Esta herramienta no solo pule las habilidades individuales; sino que también, implementa un escenario real en donde se pueden ir realizando acercamientos constantes a las operaciones llevadas desde un sistema de comunicación avanzado.

# MATERIALES Y MÉTODOS

## 5.1 Método

Este proyecto se realiza basado en el método cuantitativo debido a que consta de aplicación e implementación de una red de servicios para una organización, la cual requiere de resultados tangibles y numéricos de la viabilidad de la misma por medio de lo obtenido por el aplicativo utilizado.

En donde se implementarán diferentes fases de aplicación, seguida de pasos que permitan el seguimiento constante y la veracidad del mismo, para no incurrir en tantos errores, contando con una población específica a la que va dirigida y es permitir la comunicación dentro de una empresa ubicada en diferentes áreas urbanas dentro de una ciudad de muchos habitantes para poder hacer un seguimiento a las diferentes sucursales.

## 5.2 Materiales

Cisco packet tracer 7.1

Cisco packet tarcer 7.3

## DESARROLLO DEL ESCENARIO 1

**Descripción de escenarios propuestos para la prueba de habilidades**

**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.

### Topología

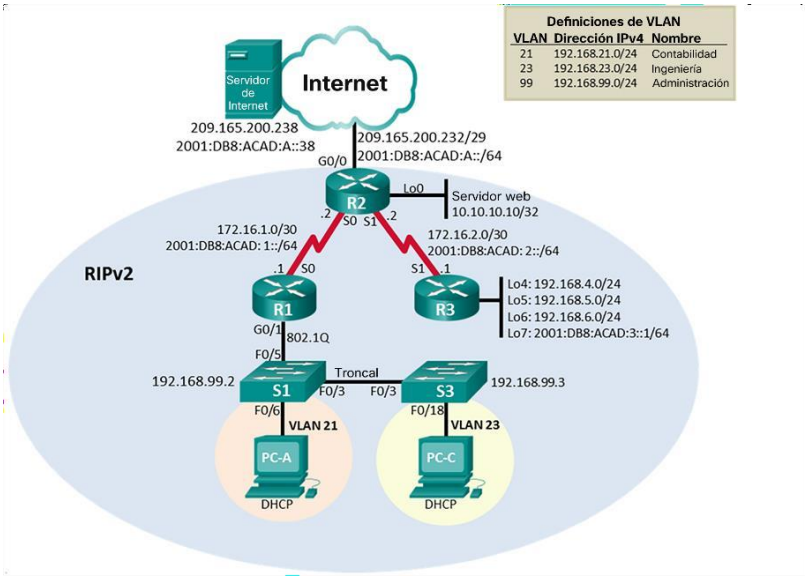



Figura 1 Topología escenario 1

### 6.1 Inicializar dispositivos

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.

Tabla No 1 Inicializar y volver a cargar los routers y los switches

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

6.2 Configurar los parámetros básicos de los dispositivos

Configurar la computadora de Internet

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

Tabla No 2: direccionamiento IP

| Elemento o tarea de configuración | Especificación |
|---|---|
| Dirección IPv4 | 209.165.200.230 |
| Máscara de subred para IPv4 | 255.255.255.248 |
| Gateway predeterminado | 209.165.200.225 |
| Dirección IPv6/subred | 2001:DB8:ACAD:A::38/64 |
| Gateway predeterminado IPv6 | 2001:DB8:ACAD:2::1 |

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

### 6.2.1 Configurar R1

Tabla N° 3 configuración de R1

| Elemento o tarea de configuración | Especificación |
|---|---|
| Desactivar la búsqueda DNS | Router>ena<br>Router#conf t<br>Router(config)#no ip domain-lookup |
| Nombre del router | Router(config)#hostname R1 |
| Contraseña de exec privilegiado cifrada | R1(config)#enable secret class |
| Contraseña de acceso a la consola | Line con 0<br>Pass cisco |
| Contraseña de acceso Telnet | R1(config)#line vty 0 4<br>R1(config)#line vty 0 4<br>R1(config-line)#login<br>R1(config-line)#exit |
| Cifrar las contraseñas de texto no cifrado | R1(config)#service password-encryption |
| Mensaje MOTD | R1(config)#Banner motd $Se prohbe el acceso no autorizado.$ |
| Interfaz S0/0/0 | R1(config)#interface s0/0/0<br>R1(config-if)#description conectado a R2<br>R1(config-if)#ip address 172.16.1.1 255.255.255.252<br>R1(config-if)#ipv6 address 2001:db8:acad:1::1/64<br>R1(config-if)#clock rate 128000<br>R1(config-if)#no shu<br>R1(config-if)#exit |
| Rutas predeterminadas | R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0<br>R1(config)#ipv6 route ::/0 s0/0/0 |

**Nota:** Todavía no configure G0/1.

### 6.2.2 Configurar R2

Tabla N° 4 configuración de R2

| Elemento o tarea de configuración | Especificación |
|---|---|
| Desactivar la búsqueda DNS | Router>ena<br>Router#conf t<br>Router(config)#no ip domain-lookup |
| Nombre del router | Router(config)#hostname R2 |
| Contraseña de exec privilegiado cifrada | R2(config)#enable secret class |
| Contraseña de acceso a la consola | R2(config)#line console 0<br>R2(config-line)#password cisco |
| Contraseña de acceso Telnet | R2(config-line)#login<br>R2(config-line)#line vty 0 4<br>R2(config-line)#password cisco<br>R2(config-line)#login |
| Cifrar las contraseñas de texto no cifrado | R2(config-line)#service password-encryption |
| Habilitar el servidor HTTP | R2(config)#ip http server (No acepta este cpmando) |
| Mensaje MOTD | R2(config)#Banner motd $Se prohbe el acceso no autorizado.$ |
| Interfaz S0/0/0 | R2(config)#interface s0/0/0<br>R2(config-if)#description conectado a R1<br>R2(config-if)#ip address 172.16.1.2 255.255.255.252<br>R2(config-if)#ipv6 address 2001:db8:acad:1::2/64<br>R2(config-if)#no shutdown<br>R2(config-if)#exit |

| | |
|---|---|
| Interfaz S0/0/1 | R2(config)#interface s0/0/1<br>R2(config-if)#des conectado a R3<br>R2(config-if)#ip address 172.16.2.2 255.255.255.252<br>R2(config-if)#ipv6 address 2001:db8:acad:2::2/64<br>R2(config-if)#clock rate 128000<br>R2(config-if)#no shu<br>R2(config-if)#exit |
| Interfaz G0/0 (simulación de Internet) | R2(config)#interface g0/0<br>R2(config-if)#des conectado a Internet<br>R2(config-if)#ip address 209.165.200.233 255.255.255.248<br>R2(config-if)#ipv6 address 2001:db8:acad:a::1/64<br>R2(config-if)#no shu<br>R2(config-if)#exit |
| Interfaz loopback 0 (servidor web simulado) | R2(config)#interface loopback 0<br>R2(config-if)#Ip add 10.10.10.1 255.255.255.252<br>R2(config-if)#exit |
| Ruta predeterminada | R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0<br>R2(config)#ipv6 route ::/0 g0/0<br>R2(config)#exit |

### 6.2.3 Configurar R3

Tabla N° 5 configuración de R3

| **Elemento o tarea de configuración** | **Especificación** |
|---|---|
| Desactivar la búsqueda DNS | Router>ena<br>Router#conf t<br>Router(config)#no ip domain-lookup |
| Nombre del router | Router(config)#hostname R3 |
| Contraseña de exec privilegiado cifrada | R3(config)#enable secret class |

| | |
|---|---|
| Contraseña de acceso a la consola | R3(config)#line console 0<br>R3(config-line)#password cisco<br>R3(config-line)#login |
| Contraseña de acceso Telnet | R3(config-line)#line vty 0 4<br>R3(config-line)#password cisco<br>R3(config-line)#login<br>R3(config-line)#exit |
| Cifrar las contraseñas de texto no cifrado | R3(config)#service password-encryption |
| Mensaje MOTD | R3(config)#Banner motd $Se prohbe el acceso no autorizado.$ |
| Interfaz S0/0/1 | R3(config)#interface s0/0/1<br>R3(config-if)#description connectado a R2<br>R3(config-if)#ip address 172.16.2.1 255.255.255.252<br>R3(config-if)#ipv6 address 2001:db8:acad:2::1/64<br>R3(config-if)#no shu<br>R3(config-if)#exit |
| Interfaz loopback 4 | R3(config)#interface loopback 4<br>R3(config-if)#ip address 192.168.4.1 255.255.255.0<br>R3(config-if)#exit |
| Interfaz loopback 5 | R3(config)#interface loopback 5<br>R3(config-if)#ip address 192.168.5.1 255.255.255.0<br>R3(config-if)#exit |
| Interfaz loopback 6 | R3(config)#interface loopback 6<br>R3(config-if)#ip address 192.168.6.1 255.255.255.0<br>R3(config-if)#exit |
| Interfaz loopback 7 | R3(config)#interface loopback 7<br>R3(config-if)#ipv6 address 2001:db8:acad:3::1/64<br>R3(config-if)#exit |

| | |
|---|---|
| Rutas predeterminadas | R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1<br>R3(config)#ipv6 route ::/0 s0/0/1<br>R3(config)#exit |

### 6.2.4 Configurar S1

Tabla N° 6 configuración de S1

| Elemento o tarea de configuración | Especificación |
|---|---|
| Desactivar la búsqueda DNS | Switch>ena<br>Switch#conf t<br>Switch(config)#no ip domain-lookup |
| Nombre del switch | Switch(config)#hostname S1 |
| Contraseña de exec privilegiado cifrada | S1(config)#enable secret class |
| Contraseña de acceso a la consola | S1(config)#line console 0<br>S1(config-line)#password cisco<br>S1(config-line)#login |
| Contraseña de acceso Telnet | S1(config-line)#line vty 0 4<br>S1(config-line)#password cisco<br>S1(config-line)#login<br>S1(config-line)#exit |
| Cifrar las contraseñas de texto no cifrado | S1(config)#service password-encryption |
| Mensaje MOTD | S1(config)#Banner motd $Se prohbe el acceso no autorizado.$<br>S1(config)#end |

### 6.2.5 Configurar el S3

Tabla N° 7 configuración de S3

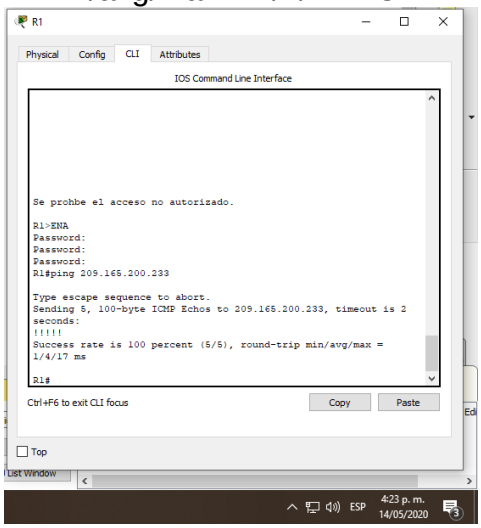
| Elemento o tarea de configuración | Especificación |
|---|---|
| Desactivar la búsqueda DNS | Switch>ena<br>Switch#conf t<br>Switch(config)#no ip domain-lookup |
| Nombre del switch | Switch(config)#hostname S3 |
| Contraseña de exec privilegiado cifrada | S3(config)#enable secret class |
| Contraseña de acceso a la consola | S3(config)#line console 0<br>S3(config-line)#password cisco<br>S3(config-line)#login |
| Contraseña de acceso Telnet | S3(config-line)#line vty 0 4<br>S3(config-line)#password cisco<br>S3(config-line)#login<br>S3(config-line)#exit |
| Cifrar las contraseñas de texto no cifrado | S3(config)#service password-encryption |
| Mensaje MOTD | S3(config)#Banner motd $Se prohbe el acceso no autorizado.$<br>S3(config)#end |

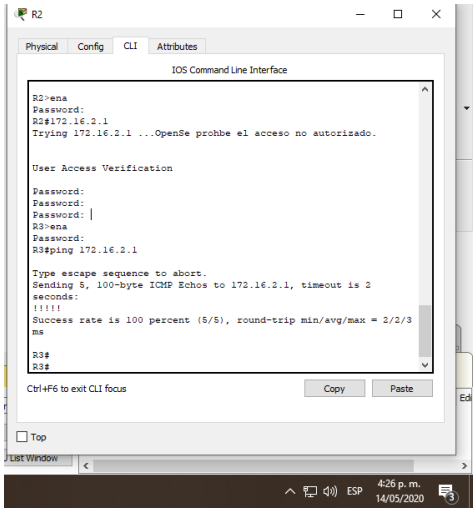
## 6.3 Verificar la conectividad de la red

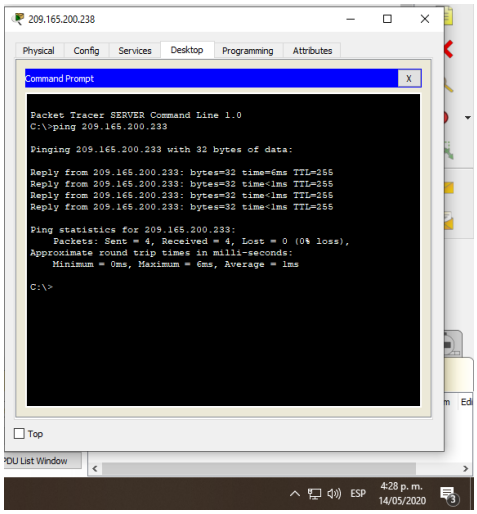
Utilice el comando **ping** para probar la conectividad entre los dispositivos de red.

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 N° 8 verificación de conectividad en la red

| Desde | A | Dirección IP | Resultados de ping |
|---|---|---|---|
| R1 | R2, S0/0/0 | 209.165.200.233 | R1#ping 209.165.200.233<br><br>Type escape sequence to abort.<br>Sending 5, 100-byte ICMP Echos to 209.165.200.233, timeout is 2 seconds:<br>!!!!!<br>Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/17 ms<br>  <br><br>Figura 2 verificación de<br><br>conectividad a 209.165.200.233 |
| R2 | R3, S0/0/1 | 172.16.2.1 | R3#ping 172.16.2.1<br><br>Type escape sequence to abort.<br>Sending 5, 100-byte ICMP Echos to 172.16.2.1, timeout is 2 seconds:<br>!!!!! |

| | | | |
|---|---|---|---|
| | | | Success rate is 100 percent (5/5), round-trip min/avg/max = 2/2/3 ms<br>  <br><br>Figura 3 verificación de conectividad a 172.16.2.1 |
| PC de Internet | Gateway predeterminado | 209.165.200.233 | C:\>ping 209.165.200.233<br><br>Pinging 209.165.200.233 with 32 bytes of data:<br><br>Reply from 209.165.200.233: bytes=32 time=6ms TTL=255<br>Reply from 209.165.200.233: bytes=32 time<1ms TTL=255<br>Reply from 209.165.200.233: bytes=32 time<1ms TTL=255<br>Reply from 209.165.200.233: bytes=32 time<1ms TTL=255<br><br>Ping statistics for 209.165.200.233: |

| | | | |
|---|---|---|---|
| | | | Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),<br>Approximate round trip times in milli-seconds:<br>Minimum = 0ms, Maximum = 6ms, Average = 1ms<br>  <br><br>Figura 4 resultados del pin a<br>209.165.200.233 |

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

## 6.4 Configurar la seguridad del switch, las VLAN y el routing entre VLAN

### 6.4.1 Configurar S1

Tabla N° 9 configuración de seguridad S1

| Elemento o tarea de configuración | Especificación |
|---|---|
| Crear la base de datos de VLAN | S1(config)#vlan 21<br>S1(config-vlan)#name contabilidad<br>S1(config-vlan)#vlan 23<br>S1(config-vlan)#name ingenieria<br>S1(config-vlan)#vlan 99<br>S1(config-vlan)#name administracion-nativa<br>S1(config-vlan)#exit |
| Asignar la dirección IP de administración. | S1(config)#interface vlan 99<br>S1(config-if)#<br>%LINK-5-CHANGED: Interface Vlan99, changed state to up<br>ip address 192.168.99.2 255.255.255.0<br>S1(config-if)#no shutdown |
| Asignar el gateway predeterminado | S1(config-if)#ip default-gateway 192.168.99.1 |
| Forzar el enlace troncal en la interfaz F0/3 | S1(config)#interface f0/3<br>S1(config-if)#switchport mode trunk<br>S1(config-if)#switchport trunk native vlan 99 |
| Forzar el enlace troncal en la interfaz F0/5 | S1(config)#interface f0/5<br>S1(config-if)#switchport mode trunk<br>S1(config-if)#switchport trunk native vlan 99 |
| Configurar el resto de los puertos como puertos de acceso | Int range fa0/1-2, fa0/4, fa0/6-24, g1/1-2<br>Swichtport mode access |

| | |
|---|---|
| Asignar F0/6 a la VLAN 21 | S1(config-if)#interface range f0/1-2, f0/4, f0/6-24, g0/1-2<br>S1(config-if-range)#switchport mode access |
| Apagar todos los puertos sin usar | S1(config-if)#interface range f0/1-2, f0/4, f0/7-24, g0/1-2<br>shutdown |

6.5 Configurar el S3

Tabla N° 10 configuración de S3

| **Elemento o tarea de configuración** | **Especificación** |
|---|---|
| Crear la base de datos de VLAN | S3(config)#vlan 21<br>S3(config-vlan)#name contabilidad<br>S3(config-vlan)#vlan 23<br>S3(config-vlan)#name ingenieria<br>S3(config-vlan)#vlan 99<br>S3(config-vlan)#name admimistracion<br>S3(config-vlan)#exit<br>S3(config)#interface vlan 99 |
| Asignar la dirección IP de administración | S3(config-if)#ip address 192.168.99.3 255.255.255.0<br>S3(config-if)#no shu<br>S3(config-if)#exit |
| Asignar el gateway predeterminado. | S3(config)#ip default-gateway 192.168.99.1 |
| Forzar el enlace troncal en la interfaz F0/3 | S3(config)#interface f0/3<br>S3(config-if)#switchport mode trunk<br>S3(config-if)#switchport trunk native vlan 1 |
| Configurar el resto de los puertos como puertos de acceso | S3(config-if)#interface range f0/1-2, f0/4-24, g0/1-2 |

| | |
|---|---|
| Asignar F0/18 a la VLAN 21 | S3(config-if-range)#switchport mode access<br>S3(config-if-range)#interface f0/18<br>S3(config-if)#switchport access vlan 23 |
| Apagar todos los puertos sin usar | S3(config-if)#interface range f0/1-2, f0/4-17, f0/19-24, g0/1-2<br>S3(config-if-range)#shu |

6.6 Configurar R1

Tabla N° 11 configuración de R1

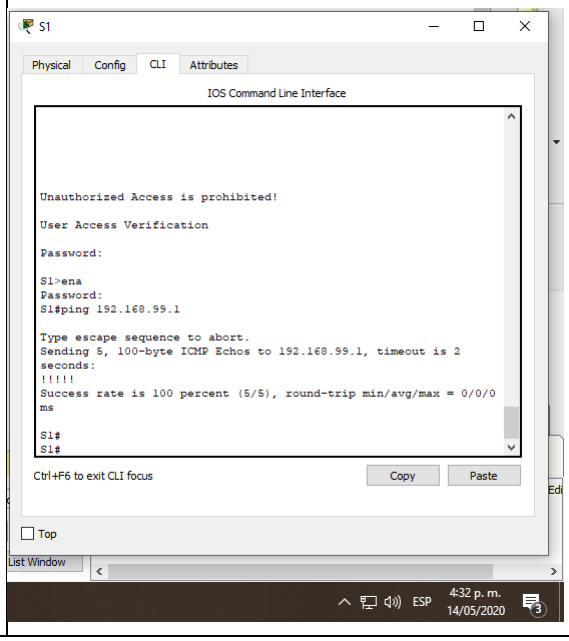
| **Elemento o tarea de configuración** | **Especificación** |
|---|---|
| Configurar la subinterfaz 802.1Q .21 en G0/1 | R1#ena<br>R1#conf t<br>R1(config)#interface g0/1.21<br>R1(config-subif)#description VLAN 21<br>R1(config-subif)#encapsulation dot1q 21<br>R1(config-subif)#ip address 192.168.21.1 255.255.255.0 |
| Configurar la subinterfaz 802.1Q .23 en G0/1 | R1(config-subif)#interface g0/1.23<br>R1(config-subif)#description VLAN 23<br>R1(config-subif)#encapsulation dot1q 23<br>R1(config-subif)#ip address 192.168.23.1 255.255.255.0 |
| Configurar la subinterfaz 802.1Q .99 en G0/1 | R1(config-subif)#interface g0/1.99<br>R1(config-subif)#description VLAN 99<br>R1(config-subif)#encapsulation dot1q 99<br>R1(config-subif)#ip address 192.168.99.1 255.255.255.0 |
| Activar la interfaz G0/1 | R1(config-subif)#interface g0/1<br>R1(config-if)#no shutdown |

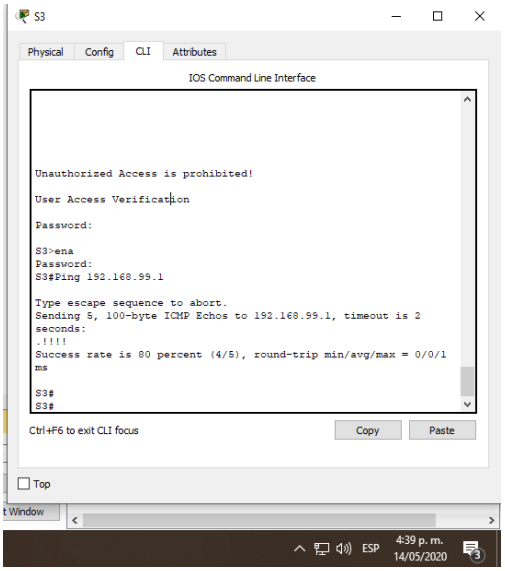
6.7 Verificar la conectividad de la red

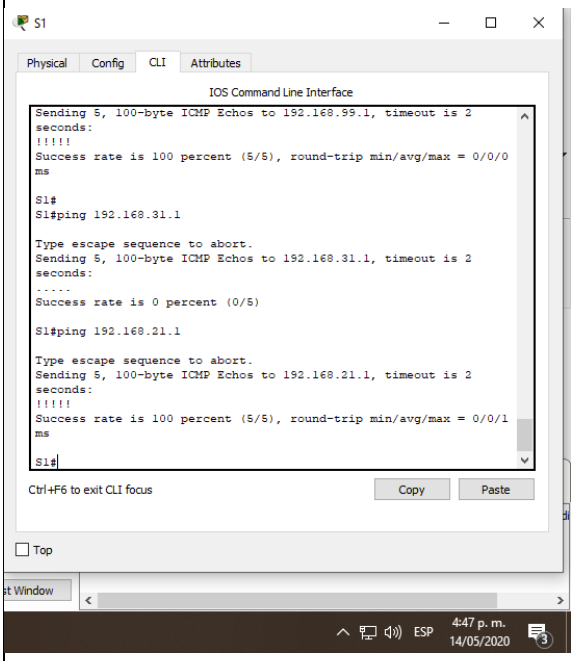
Utilice el comando **ping** para probar la conectividad entre los switches y el R1.

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 N° 12 verificación de conectividad mediante comando ping

| **Desde** | **A** | **Dirección IP** | **Resultados de ping** |
|---|---|---|---|
| S1 | R1, dirección VLAN 99 | Ping 192.168.99.1 | S1>ena<br>Password:<br>S1#ping 192.168.99.1<br><br>Type escape sequence to abort.<br>Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:<br>!!!!!<br>Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms<br>  |

| | | | |
|---|---|---|---|
| | | | Figura 5 Comprobación de conectividad a 192.168.99.1 |
| S3 | R1, dirección VLAN 99 | Ping 92.168.99.1 | S3>ena<br>Password:<br>S3#Ping 192.168.99.1<br>Type escape sequence to abort.<br>Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:<br>.!!!!<br>Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/1 ms<br>  <br><br>Figura 6 Comprobación de conectividad a 192.168.99.1 |
| S1 | R1, dirección VLAN 21 | 192.168.21.1 | S1#ping 192.168.21.1<br>Type escape sequence to abort.<br>Sending 5, 100-byte ICMP Echos to 192.168.21.1, timeout is 2 seconds:<br>!!!!! |

| | | | |
|---|---|---|---|
| | | | Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms<br>  <br><br>Figura 7 Comprobación de conectividad a 192.168.21.1 |
| S3 | R1, dirección VLAN 33 | 192.168.23.1 | S3#ping 192.168.23.1<br>Type escape sequence to abort.<br>Sending 5, 100-byte ICMP Echos to 192.168.23.1, timeout is 2 seconds:<br>!!!!!<br>Success rate is 100 percent (5/5), round-trip min/avg/max = 0/2/10 ms |

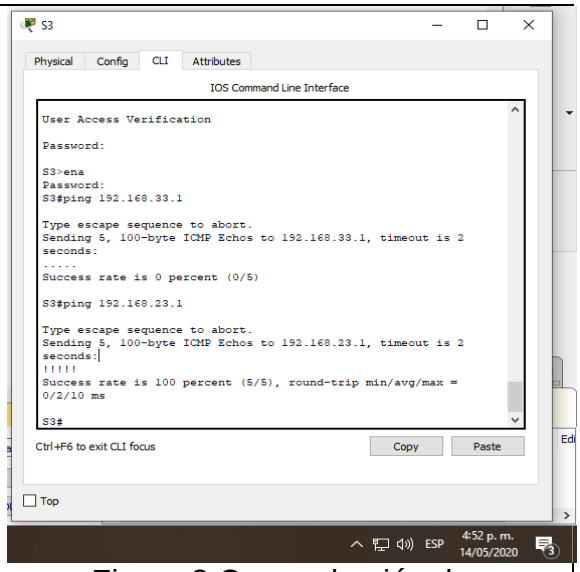



Figura 8 Comprobación de conectividad a 192.168.23.1

## 6.8 Configurar el protocolo de routing dinámico ripv2

### 6.8.1 Configurar RIPv2 en el R1

Tabla N° 13 protocolo routig dinamico RIPv2 de R1

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

| | |
|---|---|
| Anunciar las redes conectadas directamente | R1(config-router)#do show ip route connected<br>C 172.16.1.0/30 is directly connected, Serial0/0/0<br>C 192.168.21.0/24 is directly connected, GigabitEthernet0/1.21<br>C 192.168.23.0/24 is directly connected, GigabitEthernet0/1.23<br>C 192.168.99.0/24 is directly connected, GigabitEthernet0/1.99<br><br>R1(config-router)#network 172.16.1.0<br>R1(config-router)#network 192.168.21.0<br>R1(config-router)#network 192.168.23.0<br>R1(config-router)#network 192.168.99.0 |
| Establecer todas las interfaces LAN como pasivas | R1(config-router)#passive-interface g0/1.31<br>R1(config-router)#passive-interface g0/1.33<br>R1(config-router)#passive-interface g0/1.99<br>R1(config-router)# |
| Desactive la sumarización automática | R1(config-router)#no auto-summary |

### 6.8.2 Configurar RIPv2 en el R2

Tabla N° 14 configuración RIPv2 de R2

| Elemento o tarea de configuración | Especificación |
|---|---|
| Configurar RIP versión 2 | R2#ena<br>R2#conf t<br>Enter configuration commands, one per line. End with CNTL/Z.<br>R2(config)#router rip<br>R2(config-router)#version 2 |
| Anunciar las redes conectadas directamente | R2(config-router)#do show ip route connected<br>C 10.10.10.0/30 is directly connected, Loopback0<br>C 172.16.1.0/30 is directly connected, Serial0/0/0<br>C 172.16.2.0/30 is directly connected, Serial0/0/1<br>C 209.165.200.232/29 is directly connected, GigabitEthernet0/0<br><br>R2(config-router)#network 10.10.10.10<br>R2(config-router)#network 172.16.1.0<br>R2(config-router)#network 172.16.2.0 |
| Establecer la interfaz LAN (loopback) como pasiva | R2(config-router)#passive-interface loopback 0 |
| Desactive la sumarización automática. | R2(config-router)#no auto-summary |

6.9 Configurar RIPv3 en el R3

Tabla N° 15 configuración de RIPv3 de R3

| Elemento o tarea de configuración | Especificación |
|---|---|
| Configurar RIP versión 2 | R3(config)#router rip<br>R3(config-router)#version 2 |
| Anunciar redes IPv4 conectadas directamente | R3(config-router)#do show ip route connected<br>C 172.16.2.0/30 is directly connected, Serial0/0/1<br>C 192.168.4.0/24 is directly connected, Loopback4<br>C 192.168.5.0/24 is directly connected, Loopback5<br>C 192.168.6.0/24 is directly connected, Loopback6<br><br>R3(config-router)#network 172.16.2.0<br>R3(config-router)#network 192.168.4.0<br>R3(config-router)#network 192.168.5.0<br>R3(config-router)#network 192.168.6.0 |
| Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas | R3(config-router)#passive-interface loopback 4<br>R3(config-router)#passive-interface loopback 5<br>R3(config-router)#passive-interface loopback 6 |
| Desactive la sumarización automática. | R3(config-router)#no auto-summary |

### 6.9.1 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 N° 16 verificación de RIP en R3

| 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? | R3#show ip protocol |
| ¿Qué comando muestra solo las rutas RIP? | R3#show ip route rip |
| ¿Qué comando muestra la sección de RIP de la configuración en ejecución? | R3#show run |

6.10 Implementar DHCP Y NAT para ipv4

### 6.10.1 Configurar el R1 como servidor de DHCP para las VLAN 21 y 23

Tabla N° 17 configuración de DHCP y NAT en R1

| Elemento o tarea de configuración | Especificación |
|---|---|
| Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas | R1(config)#no ip dhcp excluded-address 192.168.21.1 192.168.1.20 |
| Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas | R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20 |

| | |
|---|---|
| Crear un pool de DHCP para la VLAN 21. | R1(dhcp-config)#dns-server 10.10.10.10<br>R1(dhcp-config)#domain-name ccna-sa.com<br>^<br>% Invalid input detected at '^' marker.<br>R1(dhcp-config)#ip dhcp pool ENGNR<br>R1(dhcp-config)#network 192.168.23.0 255.255.255.0<br>R1(dhcp-config)#default-router 192.168.23.1<br>R1(dhcp-config)#dns-server 10.10.10.10<br>R1(dhcp-config)#domain-name ccna-sa.com<br>^<br>% Invalid input detected at '^' marker<br>R1(dhcp-config)# |
| Crear un pool de DHCP para la VLAN 23 | Nombre: ENGNR<br>Servidor DNS: 10.10.10.10<br>Nombre de dominio: ccna-sa.com<br>Establecer el gateway predeterminado |

### 6.10.2 Configurar la NAT estática y dinámica en el R2

Tabla N° 18 configuración de NAT de R2

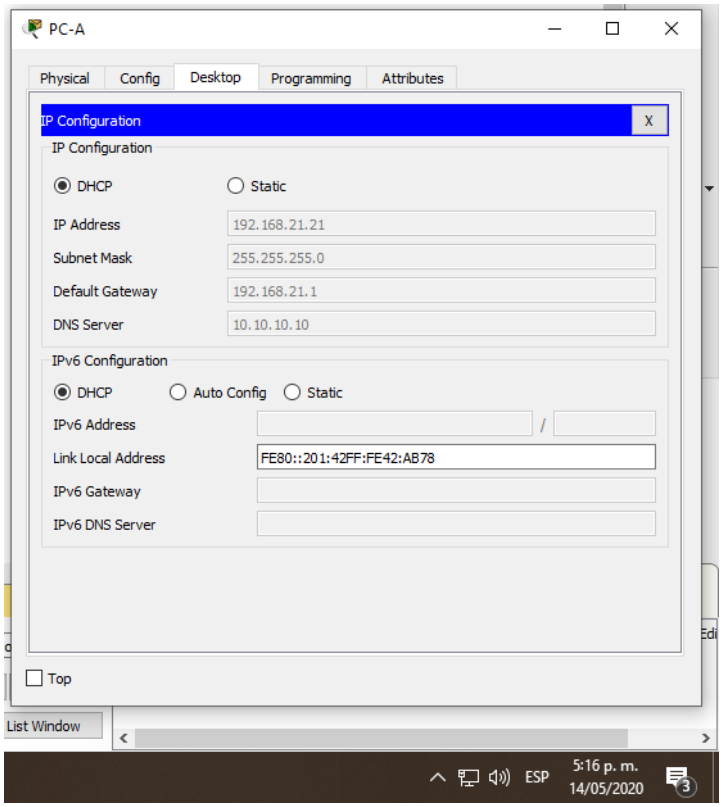
| Elemento o tarea de configuración | Especificación |
|---|---|
| Crear una base de datos local con una cuenta de usuario | R2#ena<br>R2#conf t<br>Enter configuration commands, one per line. End with CNTL/Z.<br>R2(config)#username webuser privilege 15 secret cisco12345 |
| Habilitar el servicio del servidor HTTP | R2(config)#ip http server |

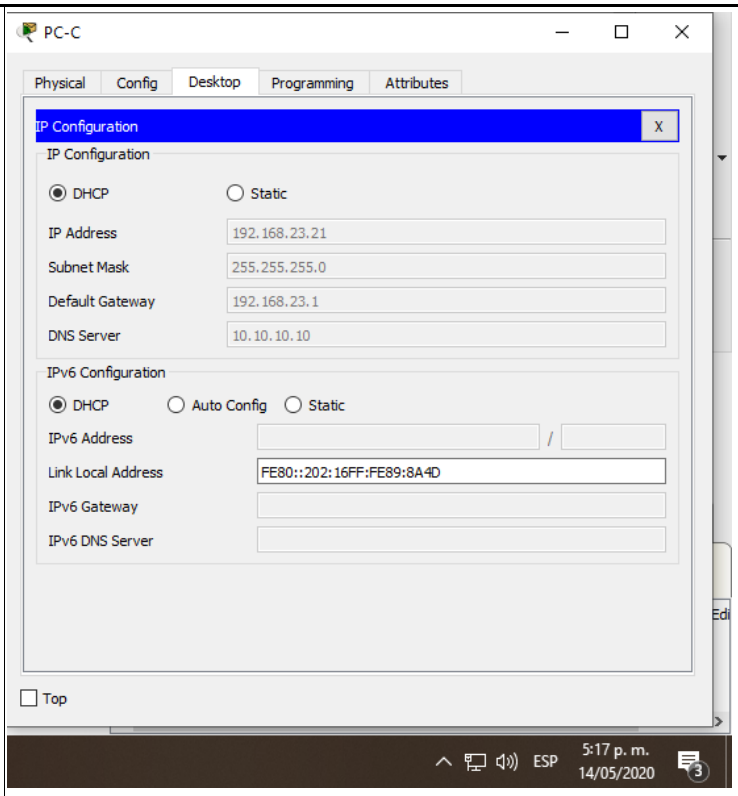
| | |
|---|---|
| Configurar el servidor HTTP para utilizar la base de datos local para la autenticación | R2(config-if)#ip http authentication local |
| Crear una NAT estática al servidor web. | R2(config-if)#ip nat inside source static 10.10.10.10 209.165.200.237 |
| Asignar la interfaz interna y externa para la NAT estática | R2(config)#interface g0/0<br>R2(config-if)#ip nat outside<br>R2(config-if)#interface s0/0/0<br>R2(config-if)#ip nat inside<br>R2(config-if)#interface s0/0/1<br>R2(config-if)#ip nat inside<br>R2(config-if)#exit |
| Configurar la NAT dinámica dentro de una ACL privada | Lista de acceso: 1<br>R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255<br>R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255<br>R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255 |
| Defina el pool de direcciones IP públicas utilizables. | R2(config)#ip nat pool INTERNET 209.165.200.233 209.165.200.236 NETMASK 255.255.255.248 |
| Definir la traducción de NAT dinámica | R2(config)#ip nat inside source list 1 pool INTERNET |

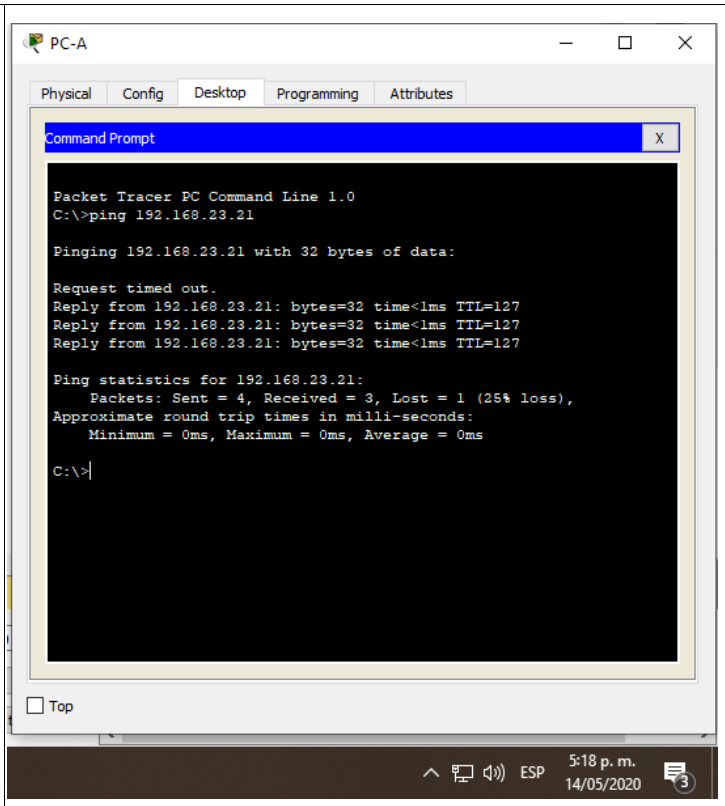
### 6.10.3 Verificar el protocolo DHCP y la NAT estática

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 N° 19 verificación de DHCP en PC-A y C

| Prueba | Resultados |
| --- | --- |
| Verificar que la PC-A haya adquirido información de IP del servidor de DHCP |  <br>Figura 9 Verificación de DHCP en PC-A |

| | |
|---|---|
| Verificar que la PC-C haya adquirido información de IP del servidor de DHCP |  <br>Figura 10 Verificación de DHCP en PC-C |

| | |
|---|---|
| Verificar que la PC-A pueda hacer ping a la PC-C<br>**Nota:** Quizá sea necesario deshabilitar el firewall de la PC. |  <br>Figura 11 Verificación de conectividad PC-A a PC-C |
| Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.237) Iniciar sesión con el nombre de usuario **webuser** y la contraseña **cisco12345** | El packet tracer no soporto el comando de activar el servidor, por esta razón no es posible ingresar al mismo desde el modo web |

### 6.10.4 Configurar NTP

Tabla N° 20 configuración de NTP

| Elemento o tarea de configuración | Especificación |
|---|---|
| Ajuste la fecha y hora en R2. | R2#clock set 09:00 05 march 2020 |

| | |
|---|---|
| Configure R2 como un maestro NTP. | No soportado el comando |
| Configurar R1 como un cliente NTP. | R1>en<br>Password:<br>R1#ena<br>R1#conf t<br>Enter configuration commands, one per line. End with CNTL/Z.<br>R1(config)#ntp server 172.16.1.2 |
| Configure R1 para actualizaciones de calendario periódicas con hora NTP. | R1(config)#ntp update-calendar<br>R1(config)#end |
| Verifique la configuración de NTP en R1. | R1>ena<br>Password:<br>Password:<br>R1#telnet 172.16.1.2<br>Trying 172.16.1.2 ...OpenSe<br>prohbe el acceso no autorizado.<br><br>User Access Verification<br><br>Password: |

## 6.11 CONFIGURAR Y VERIFICAR LAS LISTAS DE CONTROL DE ACCESO (ACL)

### 6.11.1 Restringir el acceso a las líneas VTY en el R2

Tabla N° 21 configuración de VTY en 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 | R2>ena<br>Password:<br>R2#ena<br>R2#conf t<br>Enter configuration commands, one per line. End with CNTL/Z.<br>R2(config)#ip access-list standard ADMIN-MGT |
| Aplicar la ACL con nombre a las líneas VTY | R2(config)#line vty 0 15 |
| Permitir acceso por Telnet a las líneas de VTY | R2(config-line)#access-class ADMIN-MGT in<br>R2(config-line)#transport input telnet |
| Verificar que la ACL funcione como se espera | |

### 6.11.2 Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente

Tabla N° 22 vista de lista de conexiones

| Descripción del comando | Entrada del estudiante (comando) |
|---|---|
| Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció | A continuación se especifica los comndos utilizaos para este punto:<br>R2#show access-list<br><br>Standard IP access list 1<br>10 permit 192.168.21.0 0.0.0.255<br>20 permit 192.168.23.0 0.0.0.255<br>30 permit 192.168.4.0 0.0.3.255<br>Standard IP access list ADMIN-MGT<br>10 permit host 172.16.1.1 (2 match(es)) |
| Restablecer los contadores de una lista de acceso | clear ip access-list counters<br>Rechaza el comando |
| ¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica? | R2#show ip interface |
| ¿Con qué comando se muestran las traducciones NAT? | R2#show ip nat translations |
| ¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas? | R2#clear ip nat translation |

## DESARROLLO DEL 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.

7.1 Topología de red escenario 2

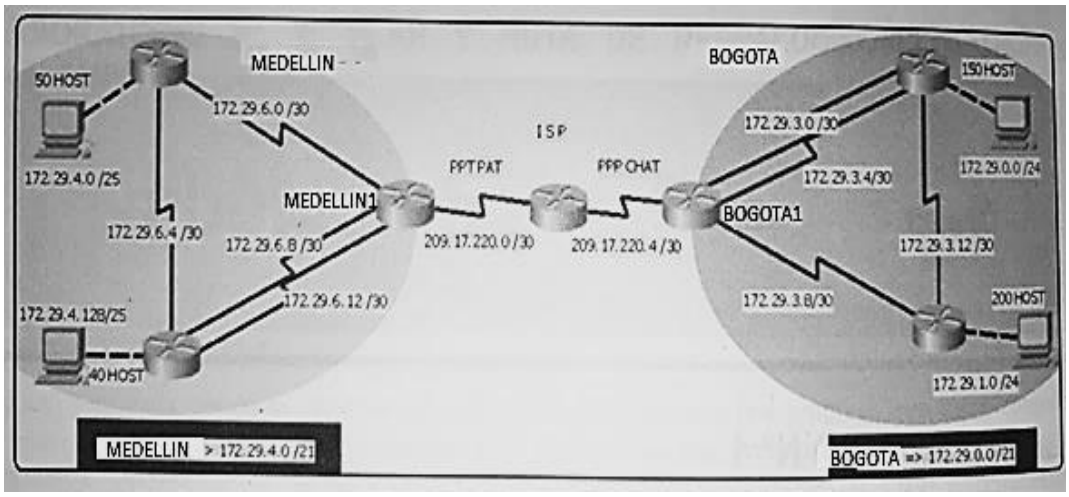



Figura 12 escenario 2

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.

## 7.2 Desarrollo y configuraciones iniciales

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).

### 7.2.1 configuracion Router IPS:

-enable
-config terminal
-hostname ISP
-interface s0/0/0
-ip address 209.17.220.1 255.255.255.252
-clock rate 4000000
-no shutdown
-interface s0/0/1
-ip address 209.17.220.5 255.255.255.252
-clock rate 4000000
-no shutdown

### 7.2.2 Configuracion Medellin 1

-enable
-config terminal
-hostname Medellin1
-interface s0/0/0
-ip address 209.17.220.2 255.255.255.252
-no shutdown
-interface s0/0/1
-ip address 172.29.6.1 255.255.255.252
-clock rate 4000000
-no shutdown
-interface s0/1/0
-ip address 172.29.6.9 255.255.255.252
-clock rate 4000000
-no shutdown
-interface s0/1/1
-ip address 172.29.6.13 255.255.255.252
-clock rate 4000000
-no shutdown

### 7.2.3 Configuracion Medellin 2

-enable
-config terminal
-hostname Medellin2
-interface s0/0/0
-ip address 172.29.6.2 255.255.255.252
-no shutdown
-interface s0/0/1
-ip address 172.29.6.5 255.255.255.252
-clock rate 4000000
-no shutdown
-interface g0/0
-ip address 172.29.4.1 255.255.255.128
-no shutdown

### 7.2.4 Configuracion Medellin 3

-enable
-config terminal
-hostname Medellin3
-interface s0/0/0
-ip address 172.29.6.10 255.255.255.252
-no shutdown
-interface s0/0/1
-ip address 172.29.6.14 255.255.255.252
-no shutdown
-interface s0/1/0

-ip address 172.29.6.6 255.255.255.252
-no shutdown
-interface g0/0
-ip address 172.29.4.129 255.255.255.128
-no shutdown
-interface s0/1/0
-ip address 172.29.3.14 255.255.255.252
-no shutdow

### 7.2.5 Configuración Bogotá 1:

-enable
-config terminal
-hostname Bogota1
-interface s0/0/0
-ip address 209.17.220.6 255.255.255.252
-no shutdown
-interface s0/0/1
-ip address 172.29.3.9 255.255.255.252
-clock rate 4000000
-no shutdown
-interface s0/1/0
-ip address 172.29.3.1 255.255.255.252
-clock rate 4000000
-no shutdown
-interface s0/1/1
-ip address 172.29.3.5 255.255.255.252
-clock rate 4000000
-no shutdown

### 7.2.6 Configuracion Bogotá 2:

-enable
-config terminal
-hostname Bogota2
-interface s0/0/0
-ip address 172.29.3.10 255.255.255.252
-no shutdown
-interface s0/0/1
-ip address 172.29.3.13 255.255.255.252
-clock rate 4000000
-no shutdown
-interface g0/0
-ip address 172.29.1.1 255.255.255.0
-no shutdown

### 7.2.7 Configuracion Bogotá 3:

-enable
-config terminal
-hostname Bogota3
-interface s0/0/0
-ip address 172.29.3.2 255.255.255.252
-no shutdown
-interface s0/0/1
-ip address 172.29.3.6 255.255.255.252
-no shutdown
-interface g0/0
-ip address 172.29.0.1 255.255.255.0
-no shutdown
-interface s0/1/0
-ip address 172.29.3.14 255.255.255.252
-no shutdown

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

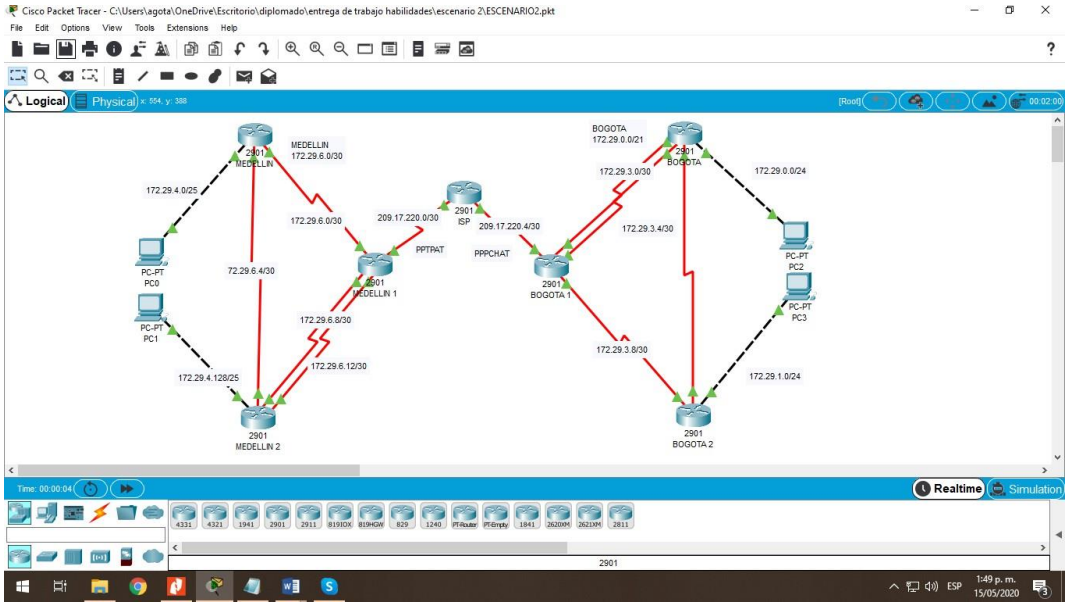



Figura 13 topologías escenario 2

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

### 7.3.1 Configuración del enrutamiento

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

- Iniciamos configurando los terminales con el direcionamiento solicitado, en esta ocasión dejaremos la descripcion de cada proceso y asi mismo el respectivo codigo o serie de comandos necesarios.

### 7.3.2 Enrutamiento OSPF en ISP:

-enable
-show ip route
-config terminal
-router ospf 1
-router-id 1.1.1.1
-network 209.17.220.0 0.0 0.255 area 0
-network 209.17.220.4 0.0 0.3 area 0

### 7.3.3 Enrutamiento OSPF en Medellin 1:

-enable
-show ip route
-config terminal
-router ospf 1
-router-id 2.2.2.2
-network 172.29.6.0 0.0 0.255 area 1
-network 172.29.6.8 0.0.0.3 area 1
-network 172.29.6.12 0.0.0.3 area 1
-network 209.17.220.0 0.0 0.3 area 0

### 7.3.4 Enrutamiento OSPF en Medellin 2:

-enable
-show ip route
-config terminal
-router ospf 1
-router-id 3.3.3.3
-network 172.29.4.0 0.0 0.255 area 1
-network 172.29.6.0 0.0.0.3 area 1
-network 172.29.6.4 0.0.0.3 area 1

### 7.3.5 Enrutamiento OSPF en Medellin 3:

-enable
-show ip route
-config terminal
-router ospf 1
-router-id 4.4.4.4
-network 172.29.4.128 0.0 0.255 area 1
-network 172.29.6.4 0.0.0.3 area 1
-network 172.29.6.4 0.0.0.3 area 1
-network 172.29.6.8 0.0.0.3 area 1
-network 172.29.6.12 0.0.0.3 area 1

### 7.3.6 Enrutamiento OSPF en Bogota 1:

-enable
-show ip route
-config terminal
-router ospf 1
-router-id 5.5.5.5
-network 172.29.3.0 0.0 0.255 area 2
-network 172.29.3.4 0.0.0.3 area 2
-network 172.29.3.8 0.0.0.3 area 2
-network 209.17.220.4 0.0 0.3 area 0

### 7.3.7 Enrutamiento OSPF en Bogota 2:

-enable
-show ip route
-config terminal
-router ospf 1
-router-id 6.6.6.6

-network 172.29.1.0 0.0 0.255 area 2
-network 172.29.3.8 0.0.0.3 area 2
-network 172.29.3.8 0.0.0.3 area 2
-network 172.29.3.12 0.0.0.3 area 2

### 7.3.8 Enrutamiento OSPF en Bogota 3:

-enable
-show ip route
-config terminal
-router ospf 1
-router-id 7.7.7.7
-network 172.29.0.0 0.0 0.255 area 2
-network 172.29.3.0 0.0.0.3 area 2
-network 172.29.3.4 0.0.0.3 area 2
-network 172.29.3.12 0.0.0.3 area 2

**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.

### 7.3.9 verificar config ospf en ISP:

-enable
-show ip ospf neighbor

### 7.3.10 verificar config ospf en medellin 1, 2, 3:

-enable
-show ip ospf neighbor

### 7.3.11 verificar config ospf en bogota 1, 2 y 3:

-enable
-show ip ospf neighbor

### 7.3.12 config ruta por defecto medellin 1:

-config terminal
-ip route 0.0.0.0 0.0.0.0 209.17.220.1
-router ospf 1
-default-information originate

### 7.3.13 verificamos en medellin 2 la config:

-enable
-show ip route

**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.

### 7.3.14 config ruta por defecto bogota 1:

-ena
-config terminal
-ip route 0.0.0.0 0.0.0.0 209.17.220.5
-router ospf 1
-default-information originate

### 7.3.15 configurar sumarizacion en el ISP:

-enable
-config terminal
-ip route 172.29.4.0 255.255.252.0 209.17.220.2
-ip route 172.29.0.0 255.255.252.0 209.17.220.6

### 7.3.16 configurar sumarizacion en el ISP:

-enable
-config terminal
-ip route 172.29.4.0 255.255.252.0 209.17.220.2
-ip route 172.29.0.0 255.255.252.0 209.17.220.6

### 7.3.17 Parte 2: Tabla de Enrutamiento.

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

Verificada y se ajusta a lo solicitado.

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

### 7.3.18 verificamos en bogota 3 la config:

-enable
-show ip route

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.

### 7.3.19 verificamos mediante ping en bogota 3:

-enable
-ping 172.29.3.1

### 7.3.20 verificamos balanceo estatico en bogota 1:

-enable
-show ip route

### 7.3.21 verificamos balanceo estatico en medellin 1:

-enable
-show ip route

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

### 7.3.22 verificamos redes conectadas a ISP:

-enable
- show ip route

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.

### 7.3.23 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.

Tabla N° 23 Lista de interface de conexión escenario 2

| 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 require |

7.4 Verificación del protocolo OSPF.

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

a. 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.

7.5 Configurar encapsulamiento y autenticación PPP.

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

### 7.5.1 Configuración CHAP en el Medellin 1:

-enable

-config terminal

-username ISP password cisco

-interface s0/0/0

-encapsulation ppp

-ppp authentication pap

-ppp pap sent-username Medellin1 password cisco

### 7.5.2 Configuracion CHAP en el ISP:

enable

config terminal

username Medellin1 password cisco

interface s0/0/0

encapsulation ppp

ppp authentication pap

ppp pap sent-username ISP password cisco

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

### 7.5.3 Configuración CHAP en el Bogotá 1:

-enable

-config terminal

-username ISP password cisco

-interface s0/0/0

-encapsulation ppp

-ppp authentication chap

7.6 : 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.

7.7 Al realizar el procedimiento obtenemos el siguiente resultado.

```
ISP>ena
Password:
ISP#ping 209.17.220.6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.17.220.6, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

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.

7.8 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.

### 7.8.1 configuacion servicio DHCP en medellin 2:

```
enable
config terminal
ip dhcp excluded-address 172.29.4.1 172.29.4.5
ip dhcp excluded-address 172.29.4.129 172.29.4.133
ip dhcp pool Medellin2
network 172.29.4.0 255.255.255.128
default-router 172.29.4.1
```

dns-server 8.8.8.8
exit

7.9 Comprobación de equipo con servicio DHCP

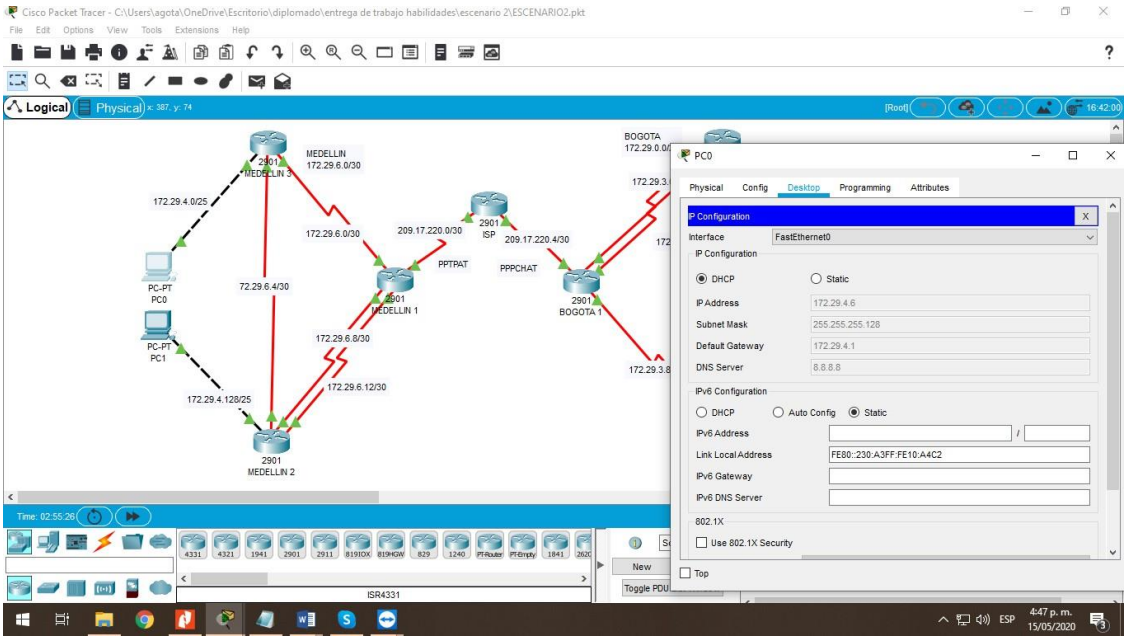


Figura 14 Verificación de DHCP

ip dhcp pool Medellin3
network 172.29.4.128 255.255.255.128
default-router 172.29.4.129
dns-server 8.8.8.8
exit

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

7.10 configuacion servicio DHCP en medellin 3:

enable
config terminal
interface g0/0
ip helper-address 172.29.6.5

7.11 Comprobación de pc con servicio DHCP

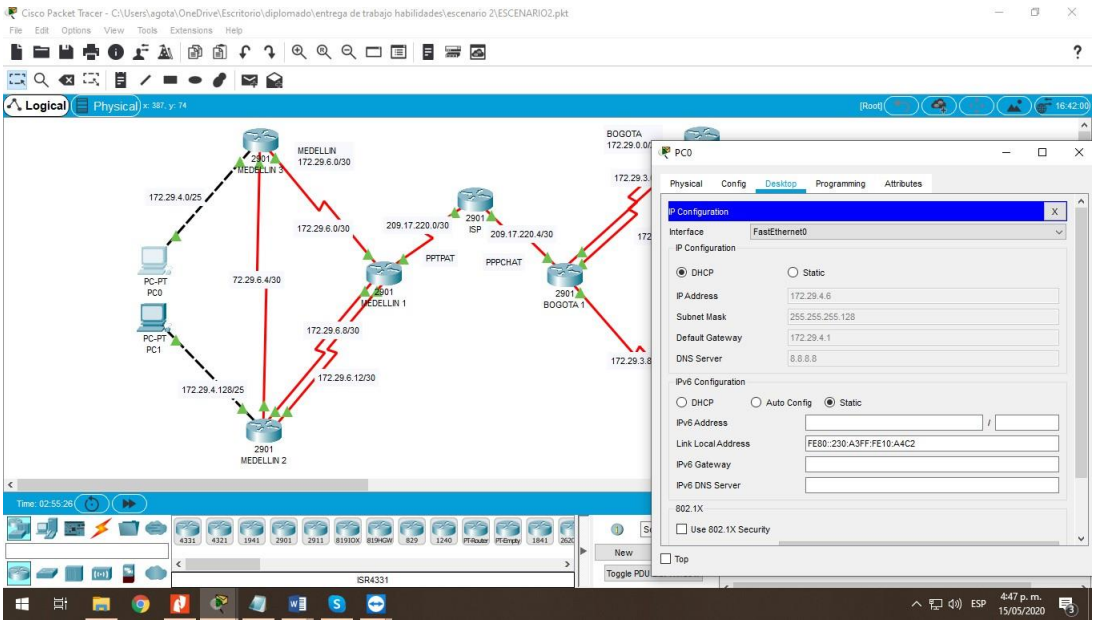



Figura 15 Verificación de DHCP

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

7.12 configuacion servicio DHCP en medellin 2:

enable
config terminal
ip dhcp excluded-address 172.29.4.1 172.29.4.5
ip dhcp excluded-address 172.29.4.129 172.29.4.133
ip dhcp pool Medellin2
network 172.29.4.0 255.255.255.128
default-router 172.29.4.1
dns-server 8.8.8.8
exit

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

7.13 configuacion servicio DHCP en Bogota 1:

-enable
-config terminal
-ip dhcp excluded-address 172.29.1.1 172.29.1.5
-ip dhcp excluded-address 172.29.0.1 172.29.0.5
-ip dhcp pool Bogota2
-network 172.29.1.0 255.255.255.0

-default-router 172.29.1.1
-dns-server 8.8.8.8
-ip dhcp pool Bogota3
-exit

## ANÁLISIS DEL DESARROLLO DEL PROYECTO

Realizar este tipo de práctica nos permite ampliar un poco más el conocimiento, sin embargo las prácticas en campo real siempre será las que nos defina qué tipo de profesional somos, vemos que muchos comandos durante el desarrollo de esta fase fueron rechazados así mismo el no poder vincular la totalidad de los comandos necesarios hace que no todo sea satisfactorio, adicionando que la practica en el desarrollo de los laboratorio remotos nos ayudan un poco más pero no es una plataforma estable todavía para poder brindar tanto horarios como disponibilidad funcional de los equipos.

Resaltar la calidad de formación que brinda la universidad y así mismo la vinculación con la plataforma cisco nos da seguridad y confianza de seleccionar hoy y mañana cuando otra generación solicite nuestra opinión.

## CONCLUSIONES

El uso de herramientas como packet tracer nos ayuda a ampliar los conocimientos mediante el desarrollo de laboratorios, que a su vez simulan el funcionamiento de redes resales.

El desarrollo y parametrización de los dos escenarios vistos me ayudaron a enriquecer mi vocabulario en comandos para parametrización de protocolos y enrutamientos

El uso de la plataforma de CISCO me ayudo a resolver dudas en cuanto a estructuración de una topología de red, brinda experiencia, enriquecimiento en temas de redes, reconocimiento y prestigio.

La implementación de protocolo IPV6 permitirán que en conjunto con MINTIC pueda realizar la migración en la entidad para la que trabajo.

## RECOMENDACIONES

Seguir trabajando en el desarrollo de este tipo de actividades que permitan el conocimiento y la implementación de necesidades a través del conocimiento de nuevos requerimientos que presente la población, debido a que las comunicaciones y la utilización de redes como apoyo es indispensable para el desarrollo de las empresas y toda la comunidad en general, es por eso que como futuro ingeniero de sistemas realizare trabajos mancomunados que no solo generen talleres por medio de aplicaciones de realidad sino que sean usadas en la vida real, generando la posibilidad de implementar a través de un negocio.

En esta ocasión es importante resaltar e incitar a que todas las personas que tengan la posibilidad de continuar con su carrera profesional escojan la profundización CISCO, brinda la simulación más parecida en el campo real, agregando que su formación es de calidad y realmente con la demostración de conocimiento se logran resultados exitosos

## REFERENCIAS BIBLIOGRÁFICAS

CISCO. (2017). Exploración de la red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module1/index.html#1.0.1.1

CISCO. (2017). Configuración de un sistema operativo de red. Fundamentos deNetworking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#2.0.1.1

CISCO. (2017). Protocolos y comunicaciones de red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#3.0.1.1

CISCO. (2017). Acceso a la red. Fundamentos de Networking. Recuperado de https://staticcourseassets.s3.amazonaws.com/ITN50ES/module2/index.html#4.0.1.1

CISCO. (2017). Ethernet. Fundamentos de Networking. Recuperado de https://static-course assets.s3.amazonaws.com/ITN50ES/module2/index.html#5.0.1.1

CISCO. (2017). Capa de red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#6.0.1.1

UNAD (2017). Diseño y configuración de redes con Packet Tracer [OVA]. Recuperado de https://1drv.ms/u/s!AmlJYei-NT1IhgCT9VCtl_pLtPD9

Vesga, J. (2019). Introducción al Laboratorio Remoto SmartLab [OVI]. Recuperado de http://hdl.handle.net/10596/24167