# DESARROLLO DE LA PRÁCTICA FINAL

ANGELMIRO MEJIA MALDONADO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍAS E INGENIERÍAS
INGENIERIA DE SISTEMAS
VALLEDUPAR, CESAR
2020

# DESARROLLO DE LA PRÁCTICA FINAL

ANGELMIRO MEJIA MALDONADO

PRUEBA DE HABILIDADES CCNA 2020

NILSON ALBEIRO FERREIRA MANZANARES
TUTOR

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍAS E INGENIERÍAS
INGENIERIA DE SISTEMAS
VALLEDUPAR, CESAR
2020

Nota de Aceptación

Firma del Tutor

Firma del Jurado

Valledupar, 18, Abril, 2020/ 22, Mayo 2020

Dedicatoria

Agradezco al Señor Padre Jehová por darme la inteligencia y sabiduría para poder estudiar y culminar mi carrera, por darme fortaleza y soporte en todas las dificultades, aunque arduo es el camino siempre con honestidad y perseverancia se culminan los proyectos.

A mi familia en en especial a mi madre quien desde los cielos celebrara cada triunfo, por ella fue quien me dirigió hasta que Jehová le permitió, por cada apoyo incondicional y en general profesional y quienes persistentemente han sido un gran apoyo tanto motivacional. A todos los seres especiales que me acompañaron en este curso aportando a mi formación profesional y como ser humano.

# AGRADECIMIENTOS

Primeramente doy gracias a Jehová por darme la vida, conocimiento y firmeza para concluir con éxito mis estudios profesionales, a mi papá que desde el paraíso me acompaño y me dio Ímpetu para continuar y no decaer en los obstáculos presentados en el camino, a mi esposa Karol Dayana Trespalacios Cruz por haberme tenido paciencia, a pesar de haber tenido momentos difíciles me brindo comprensión, cariño y afecto, a mis hijos Angel David, Juan Angel, Angelyka del Carmen por ser mi causa de motivación e iluminación para poder superarme cada día más y así poder formar un futuro mejor. A mi mamá y hermanos quienes con sus palabras de vigor no dejaron que desfalleciera y asimismo terminara con todas mis metas propuestas. A la Universidad Nacional Abierta y a Distancia por darme la formación necesaria para crecer personal y profesionalmente. A todos mis tutores que estuvieron acompañándome en este periodo de aprendizaje asesorándome y guiándome en este extenso camino.

CONTENIDO

INTRODUCCIÓN ..... 1
OBJETIVOS ..... 2
OBJETIVO GENERAL ..... 2
OBJETIVOS ESPECÍFICOS ..... 2
EVALUACIÓN – PRUEBA DE HABILIDADES PRÁCTICAS CCNA ..... 3
DESCRIPCIÓN DE ESCENARIOS PROPUESTOS PARA LA PRUEBA DE HABILIDADES ..... 4
1 ESCENARIO 1 ..... 4
1.1 Inicializar dispositivos ..... 6
1.1.1 Inicializar y volver a cargar los routers y los switches ..... 6
1.2 Configurar los parámetros básicos de los dispositivos ..... 6
1.2.1 Configurar la computadora de Internet ..... 6
1.2.2 Configurar R1 ..... 7
1.2.3 Configurar R3 ..... 10
1.2.4 Configurar S1 ..... 11
1.2.5 Configurar el S3 ..... 12
1.2.6 Verificar la conectividad de la red ..... 13
1.3 Configurar la seguridad del switch, las VLAN y el routing entre VLAN ..... 15
1.3.1 Configurar S1 ..... 15
1.3.2 Configurar el S3 ..... 16
1.3.3 Configurar R1 ..... 17
1.3.4 Verificar la conectividad de la red ..... 18
1.4 Configurar el protocolo de routing dinámico RIPv2 ..... 19
1.4.1 Configurar RIPv2 en el R1 ..... 19
1.4.2 Configurar RIPv2 en el R2 ..... 20
1.4.3 Configurar RIPv2 en el R3 ..... 21
1.4.4 Verificar la información de RIP ..... 21
1.4.5 Configurar el R1 como servidor de DHCP para las VLAN 21 y 23 ..... 24

1.4.6 Configurar la NAT estática y dinámica en el R2 ..... 25
1.4.7 Verificar el protocolo DHCP y la NAT estática ..... 26
1.5 Configurar NTP ..... 29
1.6 Configurar y verificar las listas de control de acceso (ACL) ..... 30
1.6.1 Restringir el acceso a las líneas VTY en el R2 ..... 30
1.7 Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente ..... 31
2 ESCENARIO 2 ..... 33
2.1 Inicializar dispositivos ..... 34
2.1.1 Inicializar y volver a cargar los routers y los switches ..... 34
2.2 Configuración del enrutamiento ..... 35
2.3 Tabla de Enrutamiento ..... 37
2.3.1 Verificar la tabla de enrutamiento en cada uno de los routers para comprobar las redes y sus rutas ..... 37
2.4 Deshabilitar la propagación del protocolo OSPF ..... 43
2.4.1 Verificación del protocolo OSPF ..... 44
2.5 Configurar encapsulamiento y autenticación PPP ..... 47
2.6 Configuración de PAT ..... 48
CONCLUSIONES ..... 52
BIBLIOGRAFÍA ..... 53

LISTA DE TABLAS


TABLA 1. TAREAS DE INICIALIZACIÓN 6
TABLA 2. TAREAS DE CONFIGURACIÓN BÁSICA 7
TABLA 3. CONFIGURACIÓN BÁSICA DE R2 8
TABLA 4. CONFIGURACION BÁSICA R3 10
TABLA 5. CONFIGURACIÓN BÁSICA DE S1 11
TABLA 6. CONFIGURACIÓN BÁSICA S3 12
TABLA 7. VERIFICAR CONECTIVIDAD DE RED 13
TABLA 8. CONFIGURACIÓN VLANS Y ROUTER-ON-STICK 15
TABLA 9. CONFIGURACION VLAN EN S3 16
TABLA 10. CONFIGURACION BASE DE R1 17
TABLA 11. VERIFICAR CONECTIVIDAD DE RED 18
TABLA 12. CONFIGURACION RIPV2 EN R1 19
TABLA 13. RIPV2 EN R2 20
TABLA 14. RIPV2 EN R3 21
TABLA 15. VERIFICACIÓN RIPV2 21
TABLA 16. IMPLEMENTACIÓN DHCP Y NAT 24
TABLA 17. SNAT Y PAT EN R2 25
TABLA 18. VERIFICACIÓN DHCP Y NAT 26
TABLA 19. TAREAS NTP 29
TABLA 20. TAREAS DE ACLS 30
TABLA 21. INFORMACIÓN DE COMANDOS 31
TABLA 22. TAREAS DE INICIALIZACIÓN 34
TABLA 23. CONFIGURACIÓN DE ENRUTAMIENTO 35
TABLA 24. RUTAS POR DEFECTO 36
TABLA 25. RUTAS ESTÁTICAS INTERNAS 36
TABLA 26. INTERFACES EXCLUIDAS DE PROPAGACIÓN OSPF 44
TABLA 27. CONFIGURACIÓN DE PROPAGACIÓN OSPF 44
TABLA 28. PROTOCOLO PPP (CHAP Y PAP) 47
TABLA 29. CONFIGURACION PAT 49
TABLA 30. CONFIGURACION DHCP 50

LISTA DE FIGURAS


FIGURA 1. TOPOLOGÍA ESCENARIO 1 4
FIGURA 2. TOPOLOGÍA GNS3 ESCENARIO 1 5
FIGURA 3. CONFIGURACION IP SERVER INTERNET 7
FIGURA 4. PING DE R1 A R2 14
FIGURA 5. PING DE R2 A R3 14
FIGURA 6.PING DE SERVER INET A GATEWAY 15
FIGURA 7.PING DE S1 A GATEWAY VLAN 99 19
FIGURA 8.PING DE S3 A GATEWAY VLAN 99 19
FIGURA 9.PING DE S1 A GATEWAY VLAN 21 19
FIGURA 10.PING DE S3 A GATEWAY VLAN 23 19
FIGURA 11.PROTOCOLOS DE ROUTING EN R1 22
FIGURA 12.PROTOCOLOS DE ROUTING EN R2 23
FIGURA 13. PROTOCOLOS DE ROUTING EN R3 24
FIGURA 14.PC-A 27
FIGURA 15.PC-C 27
FIGURA 16.PING PC-C A PC-A 28
FIGURA 17.INICIO DE SESIÓN SERVER WEB 28
FIGURA 18.NAVEGADOR WEB 29
FIGURA 19.ASOCIACIONES NTP EN R1 30
FIGURA 20.TELNET A R2 31
FIGURA 21.LISTAS DE ACCESO EN R2 31
FIGURA 22.NAT EN R2 32
FIGURA 23.TOPOLOGÍAS ESCENARIO 2 33
FIGURA 24.ISP 37
FIGURA 25.BOGOTA1 38
FIGURA 26.BOGOTA2 39
FIGURA 27.BOGOTA3 40
FIGURA 28.MEDELLIN1 40
FIGURA 29.MEDELLIN2 41
FIGURA 30.MEDELLIN3 41
FIGURA 31.BALANCEO DE CARGA MEDELLIN1 42
FIGURA 32.BALANCEO DE CARGA MEDELLIN2 42
FIGURA 33.BALANCEO DE CARGA BOGOTA1 42
FIGURA 34.DISTRIBUCIÓN DE CARGA 43
FIGURA 35.BASE DE DATOS OSPF ISP 45
FIGURA 36.BASE DE DATOS OSPF MEDELLIN1 45

FIGURA 37.BASE DE DATOS OSPF MEDELLIN2 45
FIGURA 38.BASE DE DATOS OSPF MEDELLIN3 46
FIGURA 39.BASE DE DATOS OSPF BOGOTA1 46
FIGURA 40.BASE DE DATOS OSPF BOGOTA2 46
FIGURA 41.BASE DE DATOS OSPF BOGOTA3 47
FIGURA 42.VERIFICACIÓN DEL PROTOCOLO PPP 48
FIGURA 43.TRADUCCIONES EN MEDELLIN1 48
FIGURA 44.TRADUCCIONES EN BOGOTA1 49
FIGURA 45.COMANDO SH IP DHCP BINDING EN MEDELLIN2 51

# GLOSARIO

IP: Protocolo de Internet. Protocolo de capa de red en el stack TCP/IP que brinda un servicio de internetworking sin conexión. El IP suministra características de direccionamiento, especificación de tipo de servicio, fragmentación y reensamblaje y seguridad.

IPv6: Protocolo de capa de red para trabajos de Internet conmutados por paquetes. Sucesor de IPv4 para uso general en Internet.

Algoritmo: Regla o proceso bien definido para llegar a la solución de un problema. En networking, suelen usarse los algoritmos para determinar el mejor camino para el tráfico desde un origen en particular a un destino en particular.

Cable: Medio de transmisión de cable de cobre o fibra óptica envuelto en una cubierta protectora.

Dominio: Parte del árbol de jerarquía de denominación que se refiere a las agrupaciones generales de redes basadas en el tipo de organización o geografía.

Ethernet: Especificación de LAN de banda base inventada por Xerox Corporation y desarrollada de forma conjunta por Xerox, Intel y Digital Equipment Corporation. Las redes Ethernet usan CSMA/CD y se ejecutan a través de varios tipos de cable a 10 Mbps. Ethernet es similar al conjunto de estándares IEEE 802.3.

Loopback: 127.0.0.1 es una dirección IP disponible en todos los dispositivos para ver si la tarjeta NIC de ese dispositivo funciona. Si se envía algo a 127.0.0.1, hace un loop back en sí misma y por consiguiente envía los datos a la NIC de ese dispositivo. Si se obtiene una respuesta positiva a un ping 127.0.0.1, se sabe que la tarjeta NIC funciona correctamente.

RAM: Memoria volátil que puede ser leída y escrita por un microprocesador.

ROM: Memoria no volátil que un microprocesador puede leer, pero no escribir.

# RESUMEN

La universidad nacional abierta y a distancia UNAD ha preparado para los estudiantes de pregrado el Diplomado de profundización cisco (Diseño e implementación de soluciones integradas LAN/WAN), como opción de grado. En el cual encontramos temas como la configuración de protocolos como RIPv2, OSPFv2, OSPFv3, DHCPv4 y DHCPv6 en switches y routers, diseñar e implementar NAT dinámicas y estáticas, listas de acceso bajo los protocolos IPv4 y IPv6, entre otros temas de gran categoría para consolidar nuestros conocimientos en networking. Para el progreso de esta actividad, es importante el uso de dos herramientas de simulación y emulación, una conocida como Packet Tracer y otra llamada GNS3, que además de simular la creación de una red, provee recursos a los estudiantes para proyectar y descubrir posibles errores en las prácticas reales de estas actividades, este documento es un material pedagógico que contiene los protocolos y estándares más recientes que se usan en la elaboración de redes para entidades públicas y privadas.



PALABRAS CLAVE: CISCO, GNS3, Packet Tracer

ABSTRACT

The national open and distance university UNAD has prepared for the undergraduate students the Cisco in-depth Diploma (Design and implementation of integrated LAN / WAN solutions), as a degree option. In which we find topics such as the configuration of protocols such as RIPv2, OSPFv2, OSPFv3, DHCPv4 and DHCPv6 in switches and routers, design and implement dynamic and static NAT, access lists under IPv4 and IPv6 protocols, among other topics of great category for consolidate our knowledge in networking. For the progress of this activity, it is important to use two simulation and emulation tools, one known as Packet Tracer and the other called GNS3, which in addition to simulating the creation of a network, provides students with resources to project and discover possible errors In the actual practices of these activities, this document is a pedagogical material that contains the latest protocols and standards that are used in the development of networks for public and private entities.

KEYWORDS: CISCO, GNS3, Packet Tracer

# INTRODUCCIÓN

La universidad nacional abierta y a distancia UNAD ha preparado para los estudiantes de pregrado el Diplomado de profundización cisco (Diseño e implementación de soluciones integradas Lan/Wan), como opción de grado. En el cual encontramos temas como la configuración de protocolos como RIPv2, OSPFv2, OSPFv3, DHCPv4 y DHCPv6 en switches y routers, diseñar e implementar NAT dinamicas y estaticas, listas de acceso bajo los protocolos IPv4 y IPv6, entre otros temas de gran categoría para consolidar nuestros conocimientos en networking. Para el progreso de esta actividad, es importante el uso de dos herramientas de simulación y emulación, una conocida como Packet Tracer y otra llamada GNS3, que además de simular la creación de una red, provee recursos a los estudiantes para proyectar y descubrir posibles errores en las prácticas reales de estas actividades, esta documento es un material pedagógico que contiene los protocolos y estándares más recientes que se usan en la elaboración de redes para entidades públicas y privadas.

# OBJETIVOS

## OBJETIVO GENERAL

Aplicar todas las habilidades y/o estrategias prácticas, teóricas y experiencia por parte de los futuros ingenieros de la Universidad Nacional Abierta y a Distancia, para examinar y emplear una solución a un asunto o escenario de estudio de inconveniente de Networking.

## OBJETIVOS ESPECÍFICOS

- ✔ Reconocer los procesos de comprobación de conectividad del uso de comandos ping, traceroute, show iproute, entre otros.

- ✔ Documentar la solución al escenario planteado.

## EVALUACIÓN – PRUEBA DE HABILIDADES PRÁCTICAS CCNA

La evaluación denominada “Prueba de habilidades prácticas”, forma parte de las actividades evaluativas del Diplomado de Profundización CCNA, y busca identificar el grado de desarrollo de competencias y habilidades que fueron adquiridas a lo largo del diplomado. Lo esencial es poner a prueba los niveles de comprensión y solución de problemas relacionados con diversos aspectos de Networking.

Para esta actividad, el estudiante dispone de cerca de dos semanas para realizar las tareas asignadas en cada uno de los dos (2) escenarios propuestos, acompañado de los respectivos procesos de documentación de la solución, correspondientes al registro de la configuración de cada uno de los dispositivos, la descripción detallada del paso a paso de cada una de las etapas realizadas durante su desarrollo, el registro de los procesos de verificación de conectividad mediante el uso de comandos ping, traceroute, show ip route, entre otros.

DESCRIPCIÓN DE ESCENARIOS PROPUESTOS PARA LA PRUEBA DE HABILIDADES

# 1 ESCENARIO 1

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

**TOPOLOGIA**

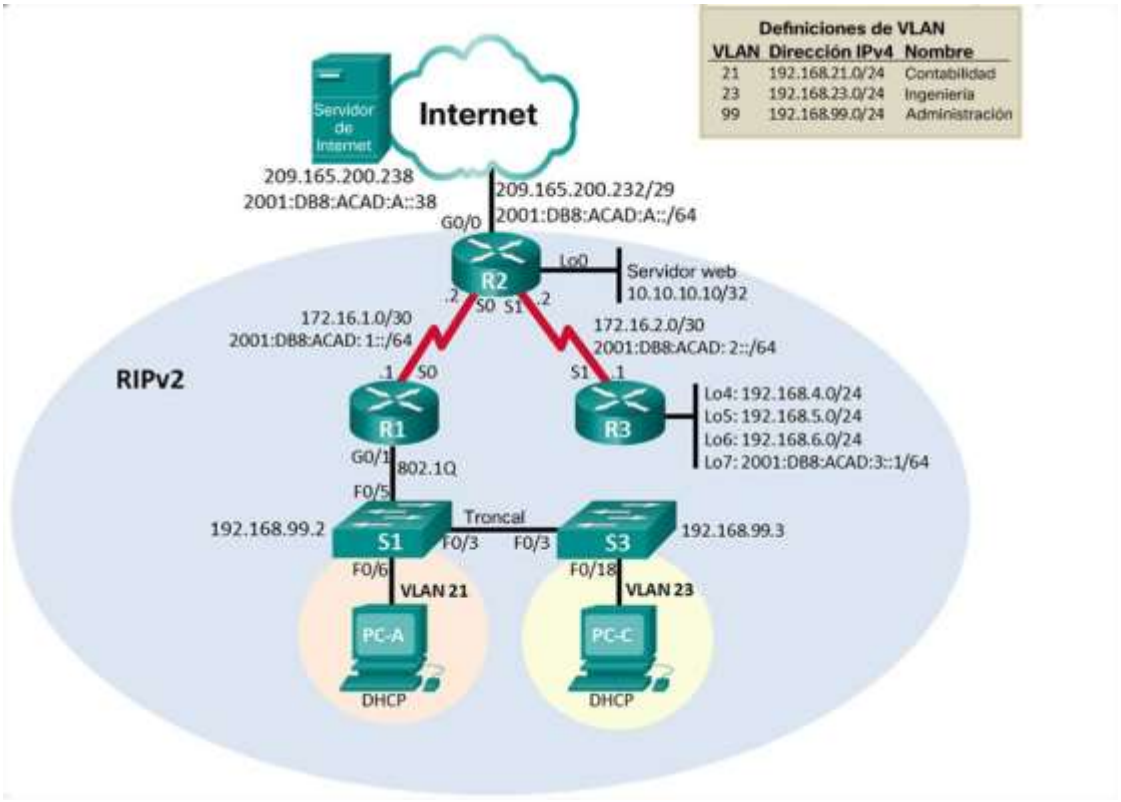



Figura 1. Topología Escenario 1

**TOPOLOGIA EN GNS3:**

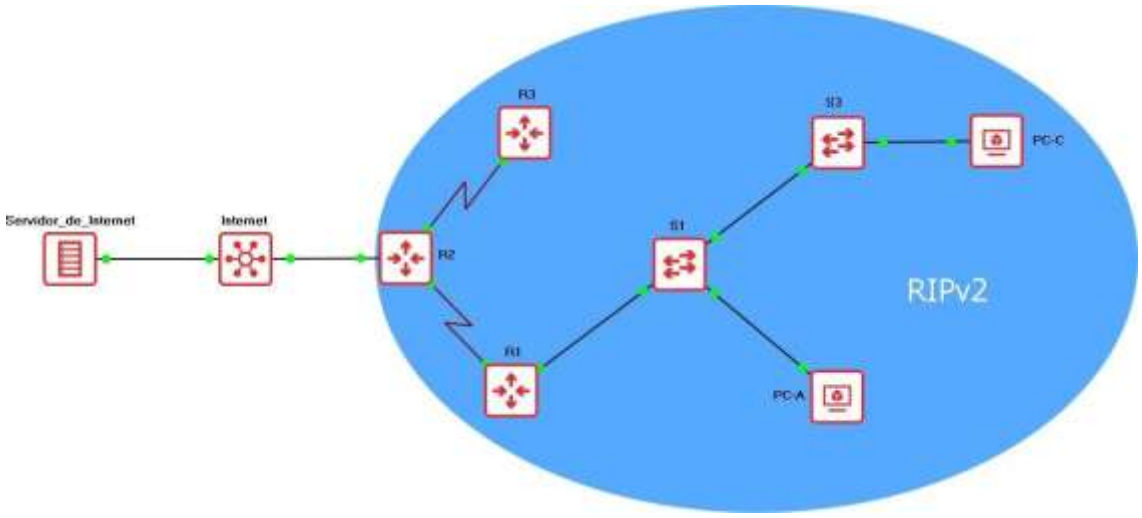



Figura 2. Topología GNS3 Escenario 1

## 1.1 Inicializar dispositivos

### 1.1.1 Inicializar y volver a cargar los routers y los switches

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

Tabla 1. Tareas de inicialización

| Tarea | Comando de IOS |
|---|---|
| Eliminar el archivo startup-config de todos los routers | 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# erase startup-config<br>Switch# delete flash:vlan.dat |
| 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# dir flash: \| show flash |

## 1.2 Configurar los parámetros básicos de los dispositivos

### 1.2.1 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):

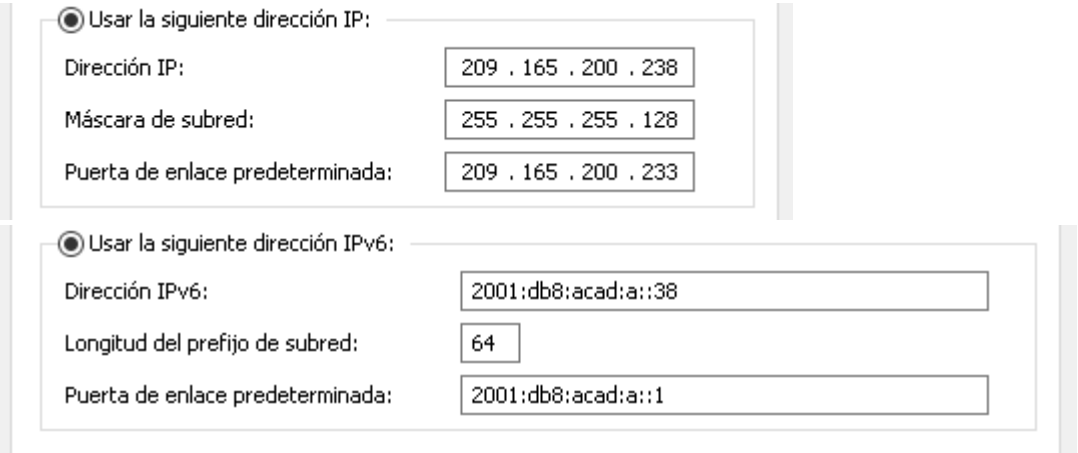



Figura 3. Configuracion IP Server Internet

### 1.2.2 Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

**Nota**: Todavía no configure G0/1.

Tabla 2. Tareas de configuración básica

| Tarea | Comando | Verificación |
|---|---|---|
| Desactivar la búsqueda DNS | no ip domain-lookup | R1# **show run** (Buscar: **no ip domain-lookup**) |
| Nombre del router | hostname R1 | (Buscar : **R1>** or **R1#** command prompt) |
| Contraseña de exec privilegiado cifrada | enable secret class | R1> **enable** (Escribir en modo usuario) |
| Contraseña de acceso a la consola | line con 0<br>password cisco<br>login | R1# **exit** (Escribir en privilegiado) |
| Contraseña de acceso Telnet | line vty 0 4<br>password cisco<br>login | R1# **show run** |

| | | |
|---|---|---|
| Cifrar las contraseñas de texto no cifrado | service password-encryption | R1# **show run** |
| Mensaje MOTD | banner motd @ Se prohíbe el acceso no autorizado @ | (verificar banner en el login) |
| Interfaz S0/0/0 | interface s0/0/0<br>description<br>Connection to R2<br>ip address<br>172.16.12.1<br>255.255.255.252<br>ipv6 address<br>2001:DB8:ACAD:12::1/64<br>clock rate 128000<br>no shutdown | R1# **show interface S0/0/0**<br>R1# **show controllers S0/0/0** |
| Rutas predeterminadas | ip route 0.0.0.0 0.0.0.0 s0/0/0<br>ipv6 route ::/0 s0/0/0 | R1# **show ip route**<br>R1# **show ipv6 route.** |

1.4 Configurar R2

La configuración del R2 incluye las siguientes tareas:

Tabla 3. Configuración básica de R2

| Tarea | Comando | **Verificación** |
|---|---|---|
| Deshabilitar busqueda DNS | no ip domain-lookup | R2# **show run** |
| Nombre | host R2 | (Observar el prompt) |
| Conntraseñas encriptadas | enable secret class | R2> **enable** |

| | | |
|---|---|---|
| Contraseña de consola | line con 0<br>password cisco<br>login | R2# **exit** |
| Contraseña de telnet | line vty 0 4<br>password cisco<br>login | R2# **show run** |
| Encriptar las contraseñas | service password-encryption | R2# **show run** |
| Habilitar server http | ip http server | R2# **show run \| include http** |
| MOTD banner | banner motd @ Se prohíbe el acceso no autorizado @ | (Verificar banner en el login) |
| Interfaz S0/0/0 | interface s0/0/0<br>description Connection to R1<br>ip add 172.16.1.2 255.255.255.252 ipv6 address 2001:DB8:ACAD:12::2/64<br>no shutdown | R2# **show interface S0/0/0** |
| Interfaz S0/0/1 | interface s0/0/1<br>description Connection to R3<br>ip add 172.16.2.2 255.255.255.252 ipv6 address 2001:DB8:ACAD:23::2/64<br>clock rate 128000<br>no shutdown | R2# **show interface S0/0/1**<br>R2# **show controllers S0/0/1** |
| | interface g0/0 | |

| | | |
|---|---|---|
| Interfaz G0/0 | description Connection to ISP<br>ip address 209.165.200.225 255.255.255.248<br>ipv6 address 2001:DB8:ACAD:2::1/64<br>no shutdown | R2# **show ip interface G0/0** |

### 1.2.3 Configurar R3

La configuración del R3 incluye las siguientes tareas:

Tabla 4. Configuración básica R3

| Tarea | Comando | Verificación |
|---|---|---|
| Desactivar la búsqueda DNS | no ip domain-lookup | R1# **show run** (Buscar: **no ip domain-lookup**) |
| Nombre del router | hostname R3 | (Buscar : **R3>** o **R3#** en el prompt) |
| Contraseña de exec privilegiado cifrada | enable secret class | R3> **enable** (Escribir en modo usuario) |
| Contraseña de acceso a la consola | line con 0<br>password cisco<br>login | R3# **exit** (Escribir en privilegiado) |
| Contraseña de acceso Telnet | line vty 0 4<br>password cisco<br>login | R3# **show run** |
| Cifrar las contraseñas de texto no cifrado | service password-encryption | R3# **show run** |
| Mensaje MOTD | banner motd @ Se prohíbe el acceso no autorizado @ | (verificar banner en el login) |

| | | |
|---|---|---|
| Interfaz S0/0/1 | interface s0/0/1<br>description Connection to R2<br>ip address 172.16.23.1 255.255.255.252<br>ipv6 address 2001:db8:acad:23::1/64<br>no shutdown | R3# **show interface S0/0/1** |
| Interfaz Loopback 4 | interface lo4<br>ip address 192.168.4.1 255.255.255.0 | R3# **show ip interface lo4** |
| Interfaz Loopback 5 | interface lo5<br>ip address 192.168.5.1 255.255.255.0 | R3# **show ip interface lo5** |
| Interfaz Loopback 6 | interface lo6<br>ip address 192.168.6.1 255.255.255.0 | R3# **show ip interface lo6** |
| Interfaz Loopback 7 | interface lo7<br>ipv6 address 2001:db8:acad:3::1/64 | R3# **show ip interface lo7** |
| Rutas predeterminadas | ip route 0.0.0.0 0.0.0.0 s0/0/1<br>ipv6 route ::/0 s0/0/1 | R1# **show ip route**<br>R1# **show ipv6 route.** |

### 1.2.4 Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 5. Configuración básica de S1

| Tarea | Comando | Verificación |
|---|---|---|
| Desactivar la búsqueda DNS | no ip domain-lookup | S1# **show run** (Buscar: **no ip domain-lookup**) |

| | | |
|---|---|---|
| Nombre del switch | hostname S1 | (Buscar : S**1>** o S**1#** en el command promt) |
| Contraseña de exec privilegiado cifrada | enable secret class | S1> **enable** (Escribir en modo usuario) |
| Contraseña de acceso a la consola | line con 0<br>password cisco<br>login | S1# **exit** (Escribir en privilegiado) |
| Contraseña de acceso Telnet | line vty 0 4<br>password cisco<br>login | S1# **show run** |
| Cifrar las contraseñas de texto no cifrado | service password-encryption | S1# **show run** |
| Mensaje MOTD | banner motd @ Se prohíbe el acceso no autorizado @ | (verificar banner en el login) |

### 1.2.5 Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 6. Configuración básica S3

| Tarea | Comando | Verificacion |
|---|---|---|
| Desactivar la búsqueda DNS | no ip domain-lookup | S3# **show run** (Buscar: **no ip domain-lookup**) |
| Nombre del switch | hostname S3 | (Buscar : S3**>** o S**1#** en el command promt) |
| Contraseña de exec privilegiado cifrada | enable secret class | S3> **enable** (Escribir en modo usuario) |
| Contraseña de acceso a la consola | line con 0<br>password cisco<br>login | S3# **exit** (Escribir en privilegiado) |

| | | |
|---|---|---|
| Contraseña de acceso Telnet | line vty 0 4<br>password cisco<br>login | S3# **show run** |
| Cifrar las contraseñas de texto no cifrado | service password-encryption | S3# **show run** |
| Mensaje MOTD | banner motd @ Se prohíbe el acceso no autorizado @ | (verificar banner en el login) |

### 1.2.6 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 7. Verificar conectividad de red

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

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

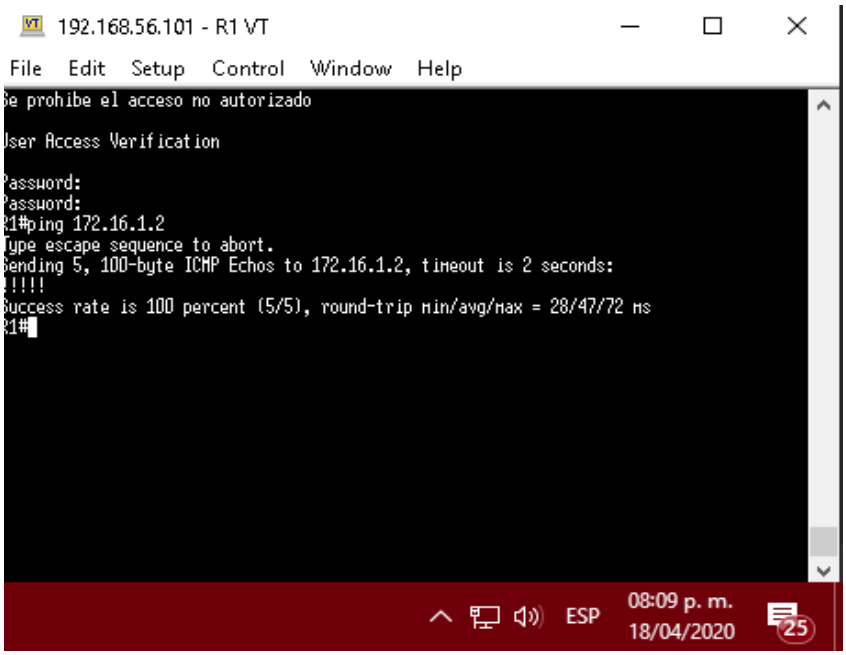



Figura 4. Ping de R1 a R2

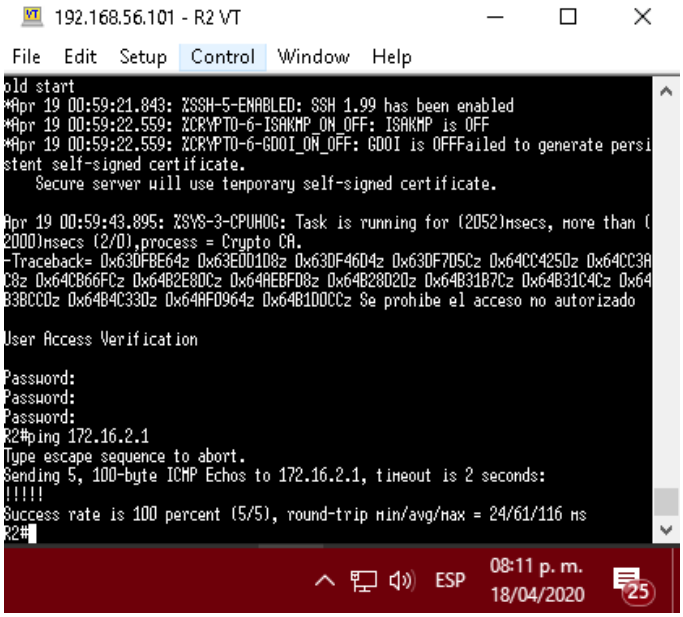



Figura 5. Ping de R2 a R3

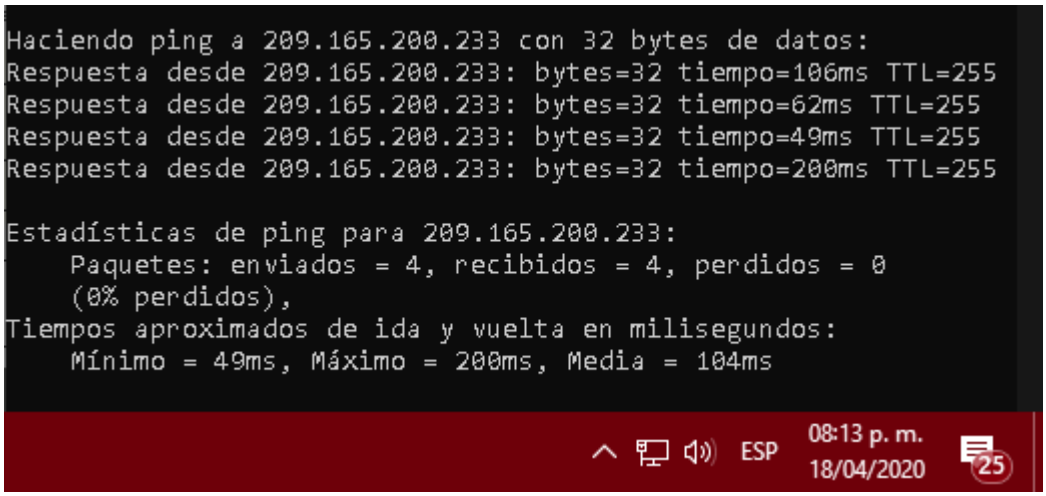


Figura 6.Ping de Server Inet a Gateway

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

### 1.3.1 Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 8.Configuración VLANS y Router-on-stick

| Tarea | Comando | Verificacion |
|---|---|---|
| Crear la base de datos de VLAN | vlan 21<br>name Contabilidad<br>vlan 23<br>name Ingenieria<br>vlan 99<br>name Administracion | S1# show vlan |
| Asignar la dirección IP de administración | interface vlan 99<br>ip address 192.168.99.2 255.255.255.0 | S1# show interface vlan 99 |
| Asignar el gateway predeterminado | ip default-gateway 192.168.99.1 | S1# show run \| section default |

| | | |
|---|---|---|
| Forzar el enlace troncal en la interfaz F0/3 | interface F0/3<br>switchport mode trunk<br>switchport trunk native vlan 1 | S1# show interface trunk |
| Forzar el enlace troncal en la interfaz F0/5 | interface F0/5<br>switchport mode trunk<br>switchport trunk native vlan 1 | S1# show interface trunk |
| Configurar el resto de los puertos como puertos de acceso | interface range F0/1-2, F0/4, F0/6-24, G0/1-2<br>switchport mode access | S1# show run \| begin interface |
| Asignar F0/6 a la VLAN 21 | interface F0/6<br>switchport access vlan 21 | S1# show run interface f0/6 |
| Apagar todos los puertos sin usar | interface range F0/1-2, F0/4, F0/7-24, G0/1-2<br>shutdown | S1# show ip interface brief |

### 1.3.2 Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 9. Configuración VLAN en S3

| Tarea | Comando | Verificacion |
|---|---|---|
| Crear la base de datos de VLAN | vlan 21<br>name Contabilidad<br>vlan 23<br>name Ingenieria<br>vlan 99<br>name Administracion | S3# show vlan |
| Asignar la dirección IP de administración | interface vlan 99<br>ip address 192.168.99.3 255.255.255.0 | S3# show interface vlan 99 |
| Asignar el gateway predeterminado | ip default-gateway 192.168.99.1 | S3# show run \| section default |

| | | |
|---|---|---|
| Forzar el enlace troncal en la interfaz F0/3 | interface F0/3<br>switchport mode trunk<br>switchport trunk native vlan 1 | S3# show interface trunk<br>S3# show run interface f0/3 |
| Configurar el resto de los puertos como puertos de acceso | interface range F0/1-2, F0/4, F0/6-24,<br>G0/1-2<br>switchport mode access | S3# show run \| begin interface |
| Configurar el resto de los puertos como puertos de acceso | interface range F0/1-2, F0/4, F0/6-24, G0/1-2<br>switchport mode access | S3# show run \| begin interface |
| Asignar F0/18 a la VLAN 23 | interface F0/18<br>switchport access vlan 23 | S3# show run interface f0/18 |
| Apagar todos los puertos sin usar | interface range F0/1-2, F0/4, F0/6-17,<br>F0/19-24, G0/1-2<br>shutdown | S3# show ip interface brief |

### 1.3.3 Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 10. Configuración base de R1

| Tarea | Comando | Verificacion |
|---|---|---|
| Configurar la subinterfaz 802.1Q .21 en G0/1 | interface g0/1.21<br>description LAN de contabilidad<br>encapsulation dot1q 21<br>ip address 192.168.21.1 255.255.255.0 | R1# show ip interface brief |
| Configurar la | | R1# show ip |

| | | |
|---|---|---|
| subinterfaz 802.1Q .23 en G0/1 | interface g0/1.23<br>description LAN de Ingenieria<br>encapsulation dot1q 23<br>ip address 192.168.23.1 255.255.255.0 | interface brief |
| Configurar la subinterfaz 802.1Q .99 en G0/1 | interface g0/1.99<br>description Lan de Administracion<br>encapsulation dot1q 99<br>ip address 192.168.99.1 255.255.255.0 | R1# show ip interface brief |
| Activar Interface G0/1 | interface g0/1<br>no shutdown | R1# show ip interface brief |

### 1.3.4 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 11. Verificar conectividad de red

| **Desde** | **A** | **Dirección IP** | **Resultados de ping** |
|---|---|---|---|
| S1 | R1, dirección VLAN 99 | 192.168.99.1 | Exitoso |
| S3 | R1, dirección VLAN 99 | 192.168.99.1 | Exitoso |
| S1 | R1, dirección VLAN 21 | 192.168.21.1 | Exitoso |
| S3 | R1, dirección VLAN 23 | 192.168.23.1 | Exitoso |

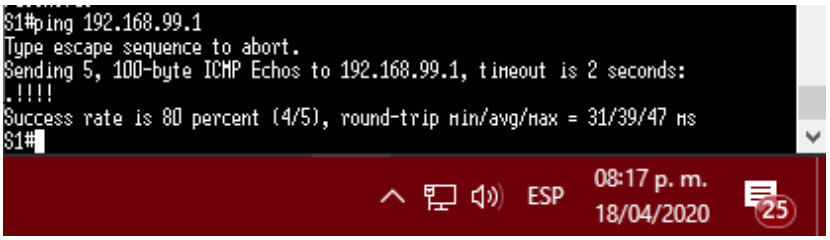



Figura 7.PING DE S1 A GATEWAY VLAN 99

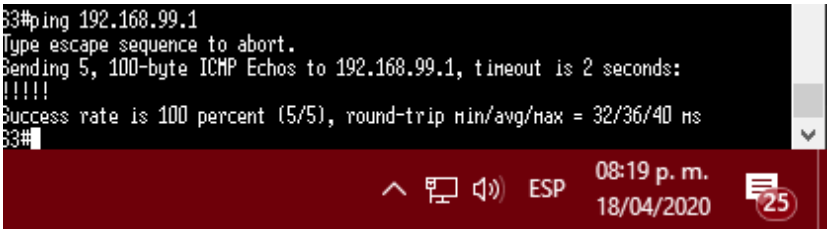



Figura 8.PING DE S3 A GATEWAY VLAN 99

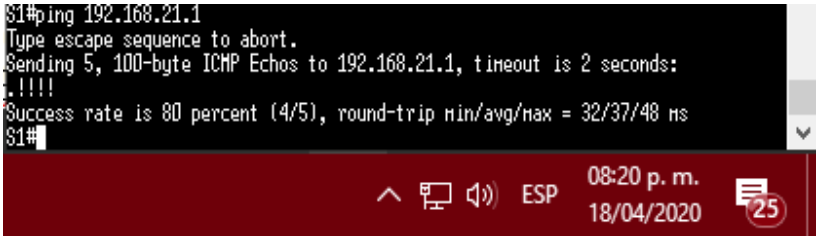



Figura 9.PING DE S1 A GATEWAY VLAN 21

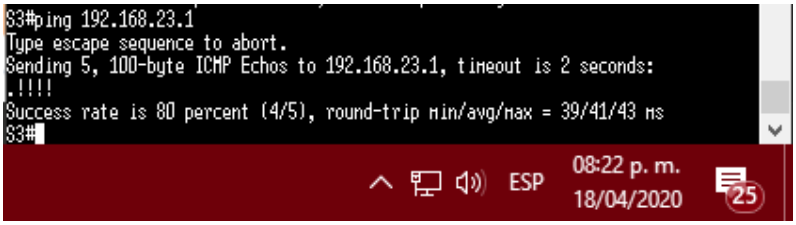



Figura 10.PING DE S3 A GATEWAY VLAN 23

## 1.4 Configurar el protocolo de routing dinámico RIPv2

### 1.4.1 Configurar RIPv2 en el R1

Tabla 12. Configuración RIPv2 en R1

| Tarea | Comando | Verificación |
|---|---|---|

| | | |
|---|---|---|
| Configurar RIP versión 2 | router rip<br>version 2 | R1# show run \| section router rip |
| Anunciar las redes conectadas directamente | network 172.16.1.0<br>network 192.168.21.0<br>network 192.168.23.0<br>network 192.168.99.0 | R1# show run \| section router rip |
| Establecer todas las interfaces LAN como pasivas | passive-interface g0/1.21<br>passive-interface g0/1.23<br>passive-interface g0/1.99 | R1# show ip protocols |
| Desactive la sumarización automática | no auto-summary | R1# show run \| section router rip |

### 1.4.2 Configurar RIPv2 en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla 13. RIPv2 en R2

| Tarea | Comando | Verificación |
|---|---|---|
| Configurar RIP versión 2 | router rip<br>version 2 | R2# show run \| section router rip |
| Anunciar las redes conectadas directamente | network 172.16.0.0<br>network 10.10.10.10 | R2# show run \| section router rip |
| Establecer todas las interfaces LAN como pasivas | passive-interface lo0 | R2# show ip protocols |
| Desactive la sumarización automática | no auto-summary | R2# show run \| section router rip |

### 1.4.3 Configurar RIPv2 en el R3

La configuración del R3 incluye las siguientes tareas:

Tabla 14. RIPv2 en R3

| Tarea | Comando | Verificación |
|---|---|---|
| Configurar RIP versión 2 | router rip<br>version 2 | R3# show run \| section router rip |
| Anunciar las redes conectadas directamente | network 172.16.0.0<br>network 192.168.4.0<br>network 192.168.5.0<br>network 192.168.6.0 | R3# show run \| section router rip |
| Establecer todas las interfaces LAN como pasivas | passive-interface lo4<br>passive-interface lo5<br>passive-interface lo6 | R3# show ip protocols |
| Desactive la sumarización automática | no auto-summary | R3# show run \| section router rip |

### 1.4.4 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 15. Verificación RIPv2

| **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 router RIP |

**R1**


Figura 11.Protocolos de routing en R1

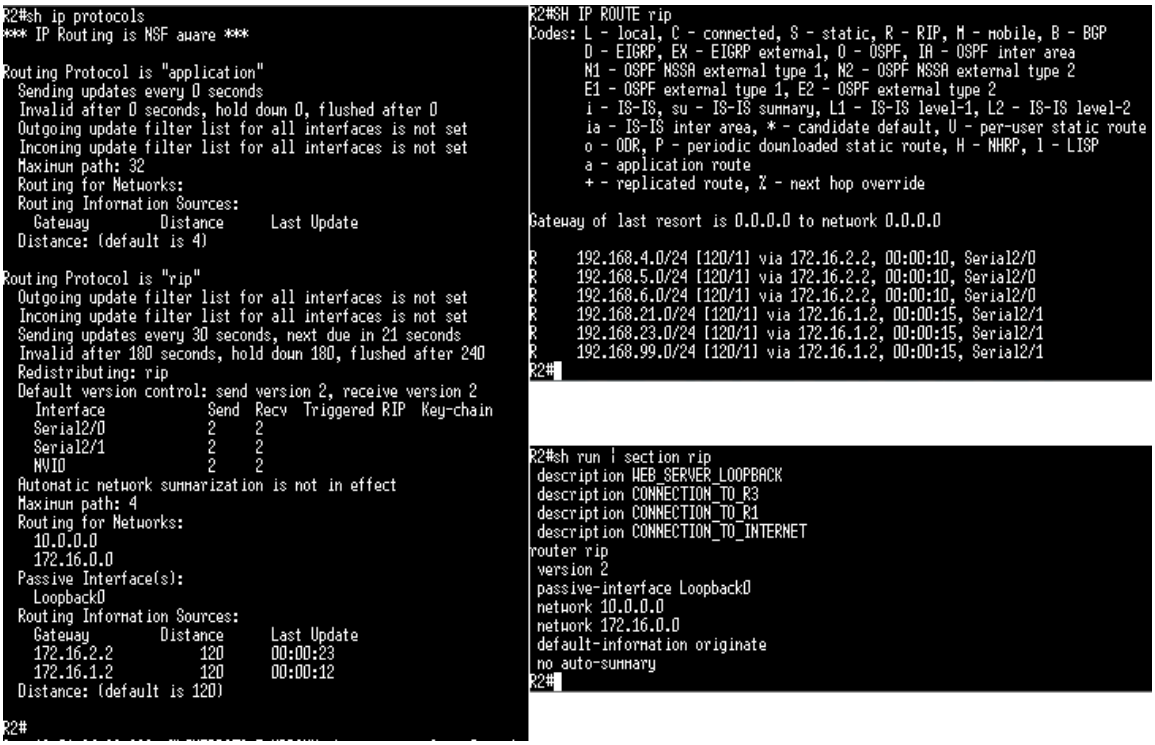



Figura 12.Protocolos de routing en R2

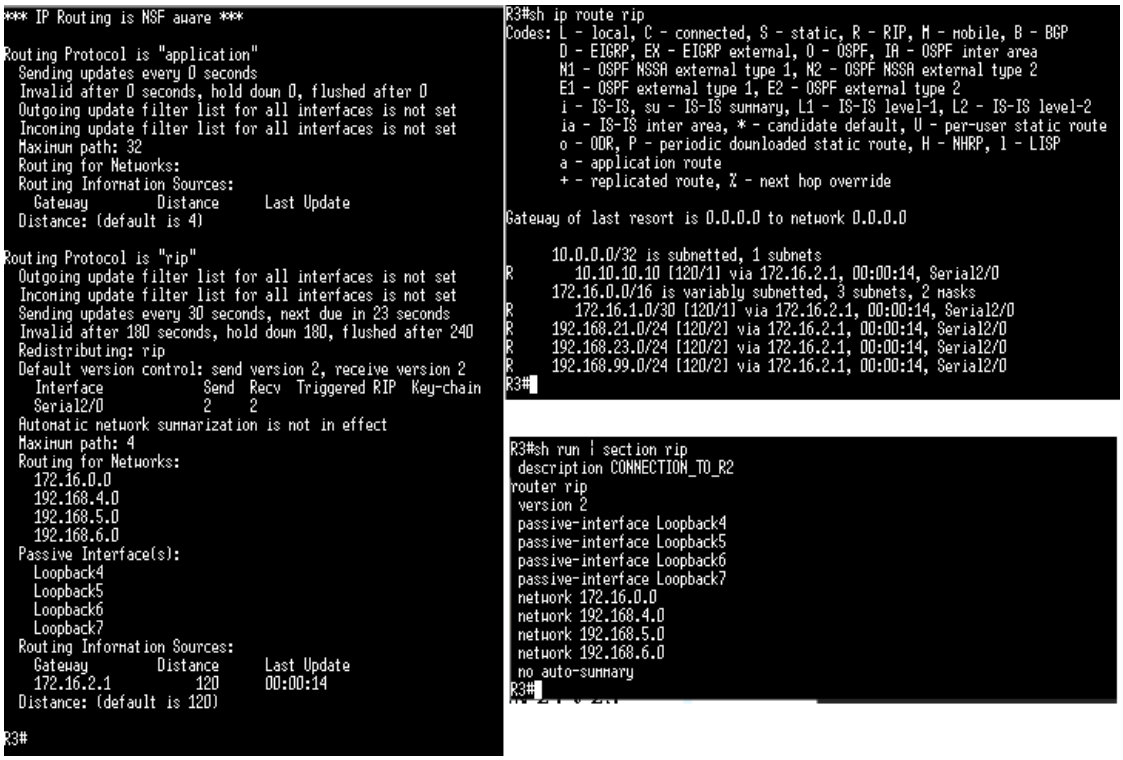



Figura 13. Protocolos de routing en R3

**Implementar DHCP y NAT para IPv4**

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

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 16. Implementación DHCP y NAT

| Tarea | Comando | Verificación |
|---|---|---|
| Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas | ip dhcp excluded-address 192.168.21.1 192.168.21.20 | R1# show run \| section dhcp |

| | | |
|---|---|---|
| Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas | ip dhcp excluded-address 192.168.23.1 192.168.23.20 | R1# show run \| section dhcp |
| Crear un pool de DHCP para la VLAN 21 | ip dhcp pool ACCT<br>network 192.168.31.0 255.255.255.0<br>dns-server 10.10.10.10<br>domain-name ccna-sa.com<br>default-router 192.168.31.1 | R1# show run \| section dhcp<br>R1# show ip dhcp bindings |
| Crear un pool de DHCP para la VLAN 23 | ip dhcp pool ENGNR<br>network 192.168.23.0 255.255.255.0<br>dns-server 10.10.10.10<br>domain-name ccna-sa.com<br>default-router 192.168.23.1 | R1# show run \| section dhcp<br>R1# show ip dhcp bindings |

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

La configuración del R2 incluye las siguientes tareas:

Tabla 17. SNAT y PAT en R2

| Tarea | Comando | Verificación |
|---|---|---|
| Crear una base de datos local con una cuenta de usuario | username webuser privilege 15 secret cisco12345 | R2# show run \| section username |
| Habilitar el servicio del servidor HTTP | ip http server | R2# show run \| section ip http |
| Configurar el servidor HTTP para utilizar la base de datos local para la autenticación | ip http authentication local | R2# show run \| section ip http |

| | | |
|---|---|---|
| Crear una NAT estática al servidor web. | ip nat inside source static 10.10.10.10 209.165.200.237 | R2# show ip nat translations |
| Asignar la interfaz interna y externa para la NAT estática | interface lo0<br>ip nat inside<br>interface g0/0<br>ip nat outside | R2# show run \| begin interface |
| Configurar la NAT dinámica dentro de una ACL privada. | access-list 1 permit 192.168.21.0 0.0.0.255 access-list 1 permit 192.168.23.0 0.0.0.255 access-list 1 permit 192.168.4.0 0.0.3.255 | R2# show access-lists |
| Defina el pool de direcciones IP públicas utilizables. | ip nat pool INTERNET 209.165.200.233 209.165.200.236 netmask 255.255.255.248 | R2# show run \| section ip nat |
| Definir la traducción de NAT dinámica | ip nat inside source list 1 pool INTERNET | R2# show run \| section ip nat |

### 1.4.7 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 18. Verificación DHCP y NAT

| **Prueba** | **Resultados** |
|---|---|
| Verificar que la PC-A haya adquirido información de IP del servidor de DHCP | Exitoso |
| Verificar que la PC-C haya adquirido información de IP del servidor de DHCP | Exitoso |
| Verificar que la PC-A pueda hacer ping a la PC-C<br>**Nota:** Quizá sea necesario | itoso |

| | |
|---|---|
| deshabilitar el firewall de la PC. | |
| 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** | Exitoso |

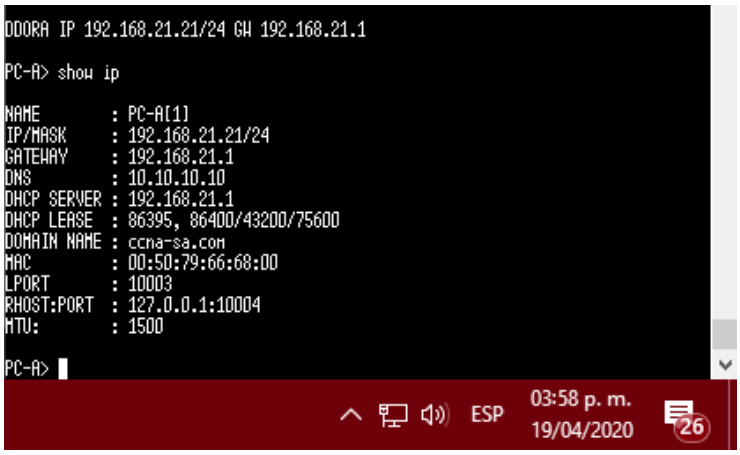


Figura 14.PC-A

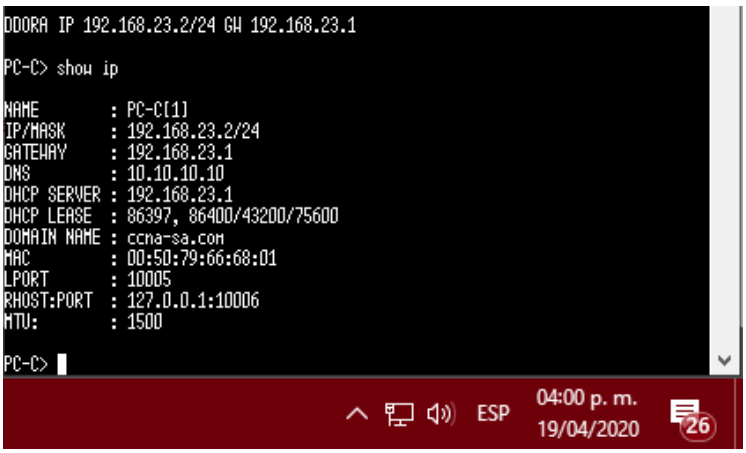


Figura 15.PC-C

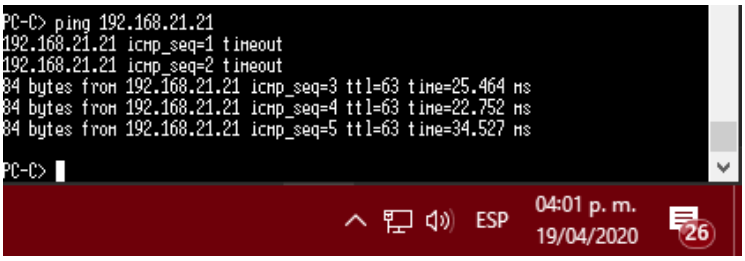



Figura 16.PING PC-C A PC-A

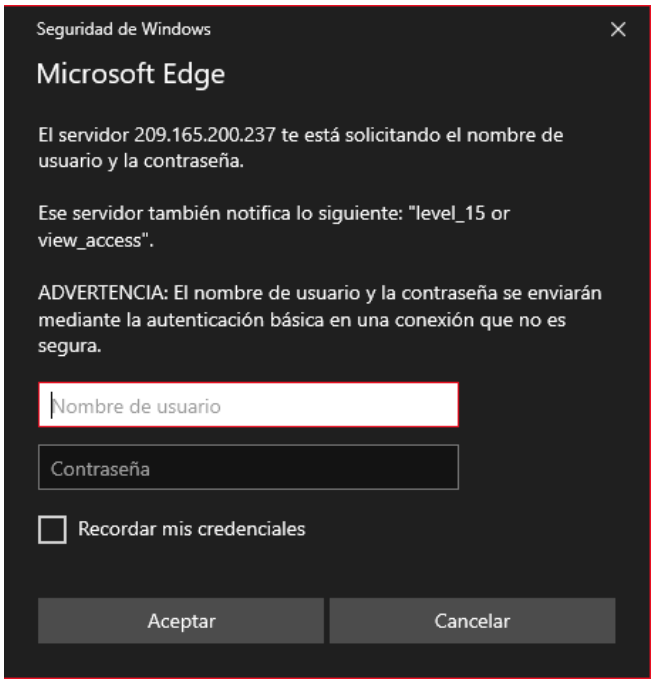



Figura 17.Inicio de sesión server web

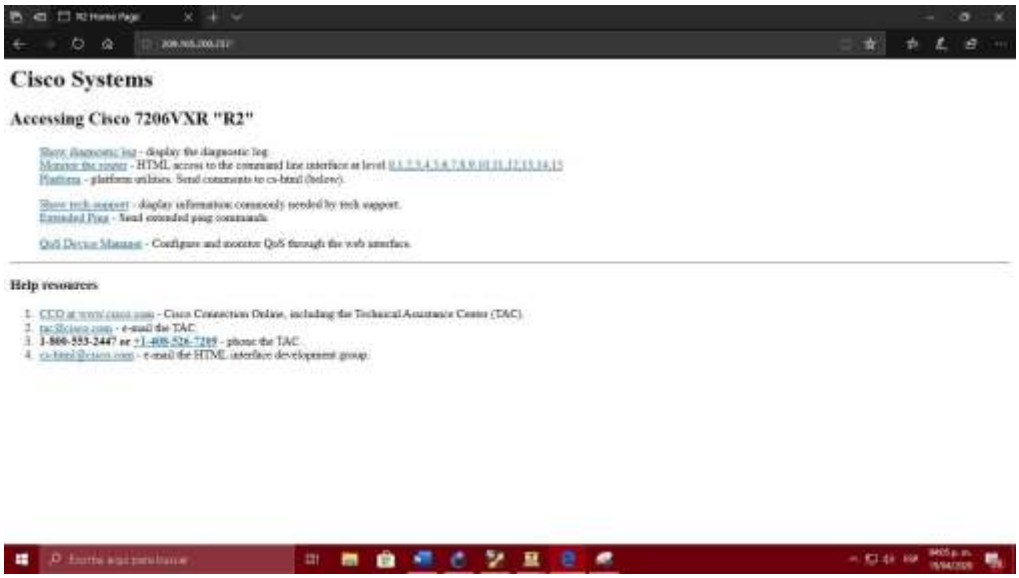



Figura 18.NAVEGADOR WEB

## 1.5 Configurar NTP

Tabla 19. Tareas NTP

| Tarea | Comando | Verificación |
|---|---|---|
| Ajuste la fecha y hora en R2. | R2# clock set 9:00:00 5 march 2016 | R2# show clock |
| Configure R2 como un maestro NTP | R2(config)# ntp master 5 | R2# Show run \| section ntp |
| Configurar R1 como un cliente NTP. | R1(config)# ntp server 172.16.1.2 | R1# show run \| section ntp |
| Configure R1 para actualizaciones de calendario periódicas con hora NTP. | R1 (config)# ntp update-calendar | R1# show run \| section ntp |

| | | |
|---|---|---|
| Verifique la configuración de NTP en R1. | R1# show ntp associations | R1# show ntp associations |

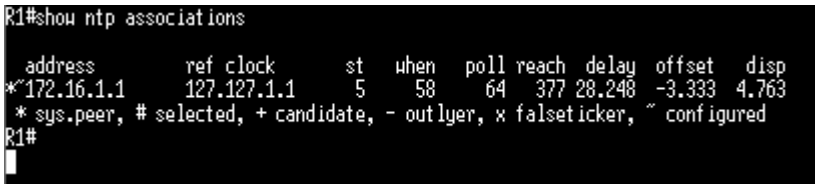



Figura 19.ASOCIACIONES NTP EN R1

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

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

Tabla 20. Tareas de ACLs

| Tarea | Comando | Verificación |
|---|---|---|
| Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2 | ip access-list standard ADMIN-MGT<br>permit host 172.16.1.1 | R2# show access-lists |
| Aplicar la ACL con nombre a las líneas VTY | line vty 0 4<br>access-class ADMIN-MGT in | R2# show run \| sec line vty |
| Permitir acceso por Telnet a las líneas de VTY | transport input telnet | R2# show run \| section vty |
| Hacer una conexión telnet con R2 | Exitoso | R1# telnet 172.16.1.1 |

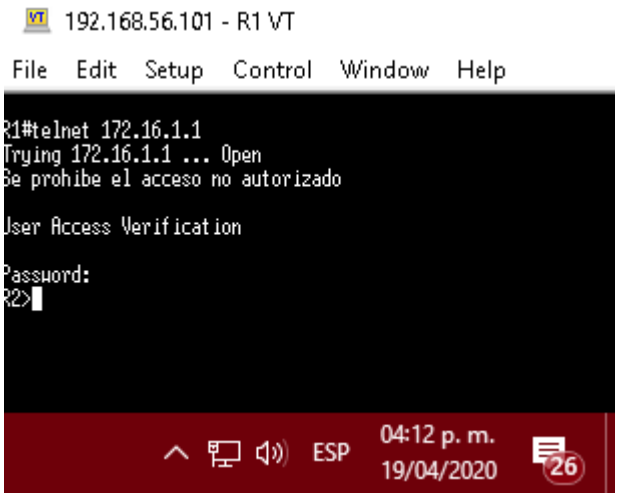
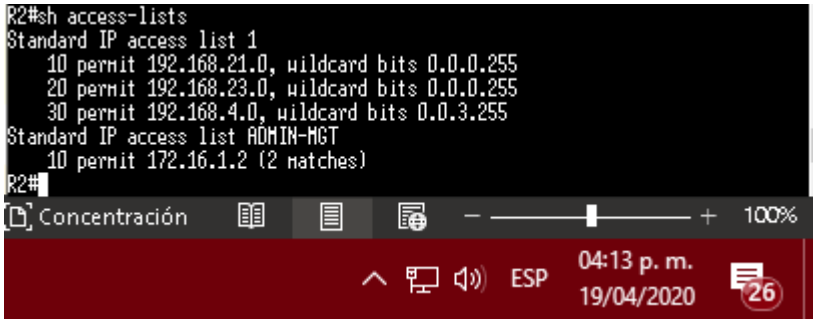
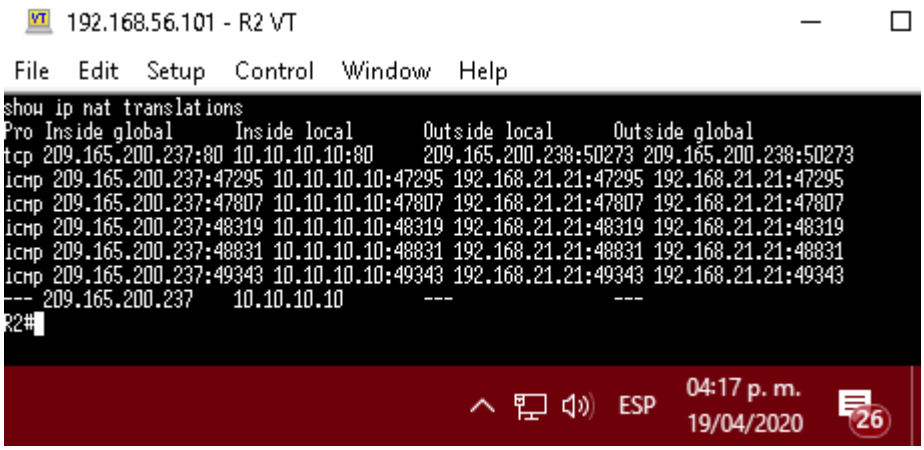



Figura 20.TELNET A R2

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

Tabla 21. Información de comandos

| **Descripción del comando** | **Entrada del estudiante (comando)** |
|---|---|
| Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció | Show access-list<br>  <br><br>Figura 21.LISTAS DE ACCESO EN R2 |
| Restablecer los contadores de una lista de acceso | clear ip access-list counters |
| ¿Qué comando se | Show ip interface |

| | |
|---|---|
| usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica? | |
| ¿Con qué comando se muestran las traducciones NAT? | show ip nat translations<br>  <br>Figura 22.NAT EN R2<br><br>**Nota:** Las traducciones para la PC-A y la PC-C se agregaron a la tabla cuando la computadora de Internet intentó hacer ping a esos equipos en el paso 2. Si hace ping a la computadora de Internet desde la PC-A o la PC-C, no se agregarán las traducciones a la tabla debido al modo de simulación de Internet en la red. |
| ¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas? | #clear ip nat translation * |

2 ESCENARIO 2

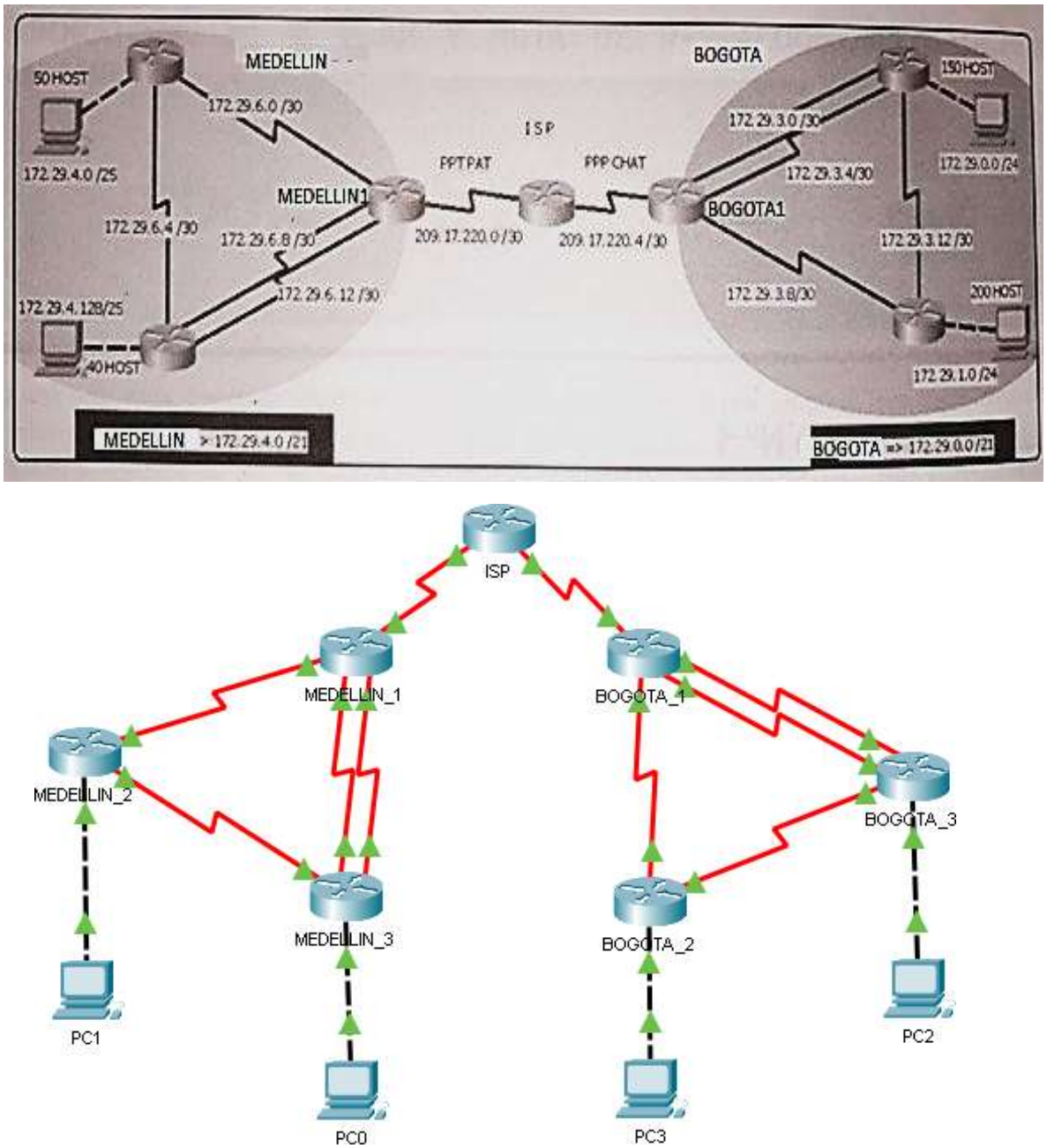



Figura 23.Topologías Escenario 2

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

## 2.1 Inicializar dispositivos

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).

### 2.1.1 Inicializar y volver a cargar los routers y los switches

Tabla 22. Tareas de Inicialización

| Tarea | Comando de IOS |
|---|---|
| Eliminar el archivo startup-config de todos los routers | Router# erase startup-config |
| Volver a cargar todos los routers | Router# reload |
| Desactivar la búsqueda DNS | no ip domain-lookup |
| Nombre del equipo | hostname {NOMBRE_DEL_EQUIPO} |
| Contraseña de exec privilegiado cifrada | enable secret class |
| Contraseña de acceso a la consola | line con 0<br>password cisco<br>login |
| Contraseña de acceso Telnet | line vty 0 4<br>password cisco<br>login |
| Cifrar las contraseñas de texto no cifrado | service password-encryption |

| | |
|---|---|
| Mensaje MOTD | banner motd # Se prohíbe el acceso no autorizado # |

• Realizar la conexión física de los equipos con base en la topología de red
Configurar la topología de red, de acuerdo con las siguientesespecificaciones.

## 2.2 Configuración del enrutamiento

Tabla 23. Configuración de enrutamiento

| Tarea | Comando de IOS |
|---|---|
| Enrutamiento OSPF en MEDELLIN1 | router ospf 1<br>network 172.29.6.0 0.0.0.3 área 0<br>network 172.29.6.8 0.0.0.3 área 0<br>network 172.29.6.12 0.0.0.3 área 0<br>network 209.17.220.0 0.0.0.3 área 0 |
| Enrutamiento OSPF en MEDELLIN2 | router ospf 1<br>network 172.29.4.0 0.0.0.127 área 0<br>network 172.29.6.0 0.0.0.3 área 0<br>network 172.29.6.4 0.0.0.3 área 0 |
| Enrutamiento OSPF en MEDELLIN3 | router ospf 1<br>network 172.29.4.128 0.0.0.127 área 0<br>network 172.29.6.4 0.0.0.3 área 0<br>network 172.29.6.8 0.0.0.3 área 0<br>network 172.29.6.12 0.0.0.3 área 0 |
| Enrutamiento OSPF en ISP | router ospf 1<br>network 209.17.220.0 0.0.0.3 área 0<br>network 209.17.220.4 0.0.0.3 área 0 |
| Enrutamiento OSPF en BOGOTA1 | router ospf 1<br>network 172.29.3.0 0.0.0.3 área 0<br>network 172.29.3.4 0.0.0.3 área 0<br>network 172.29.3.8 0.0.0.3 área 0<br>network 209.17.220.4 0.0.0.3 área 0 |
| Enrutamiento OSPF en BOGOTA2 | router ospf 1<br>network 172.29.1.0 0.0.0.255 área 0<br>network 172.29.3.8 0.0.0.3 área 0 |

| | |
|---|---|
| | network 172.29.3.12 0.0.0.3 área 0 |
| Enrutamiento OSPF en BOGOTA3 | router ospf 1<br>network 172.29.0.0 0.0.0.255 área 0<br>network 172.29.3.0 0.0.0.3 área 0<br>network 172.29.3.4 0.0.0.3 área 0<br>network 172.29.3.12 0.0.0.3 área 0 |

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

Tabla 24. Rutas por defecto

| **Tarea** | **Comando de IOS** |
|---|---|
| Ruta por defecto en BOGOTA1 y redistribución en ospf | ip route 0.0.0.0 0.0.0.0 Serial0/1/0<br>router ospf 1<br>redistribute static subnets |
| Ruta por defecto en MEDELLIN1 y redistribución en ospf | ip route 0.0.0.0 0.0.0.0 Serial0/1/0<br>router ospf 1<br>redistribute static subnets |

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

Tabla 25. Rutas estáticas internas

| **Tarea** | **Comando de IOS** |
|---|---|
| Configurar rutas estáticas hacia las redes internas en ISP | ip route 172.29.4.0 255.255.252.0 Serial0/3/0<br>ip route 172.29.4.128 255.255.255.128 Serial0/3/0<br>ip route 172.29.1.0 255.255.255.0 Serial0/3/1<br>ip route 172.29.0.0 255.255.252.0 |

| | |
|---|---|
| | Serial0/3/1 |

2.3 Tabla de Enrutamiento.

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

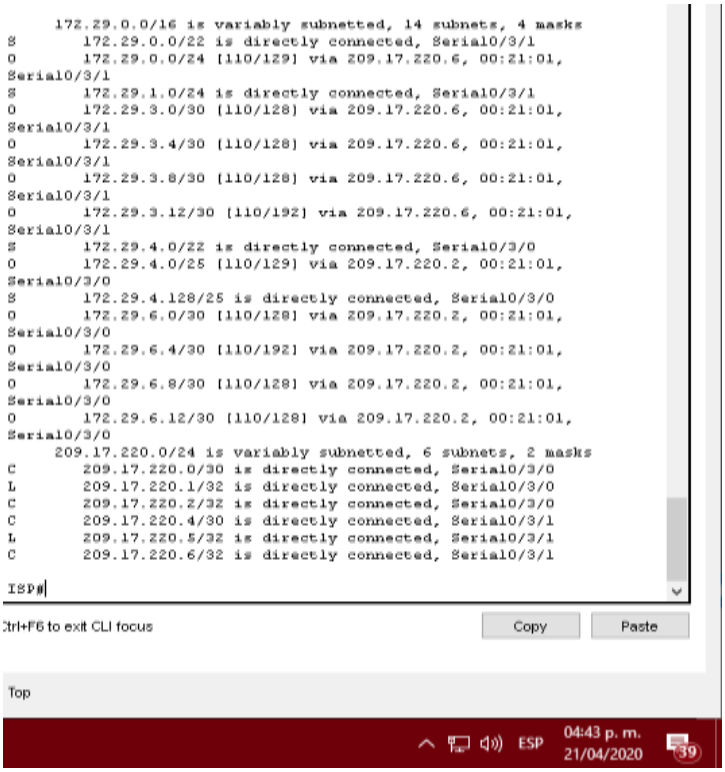



Figura 24.ISP

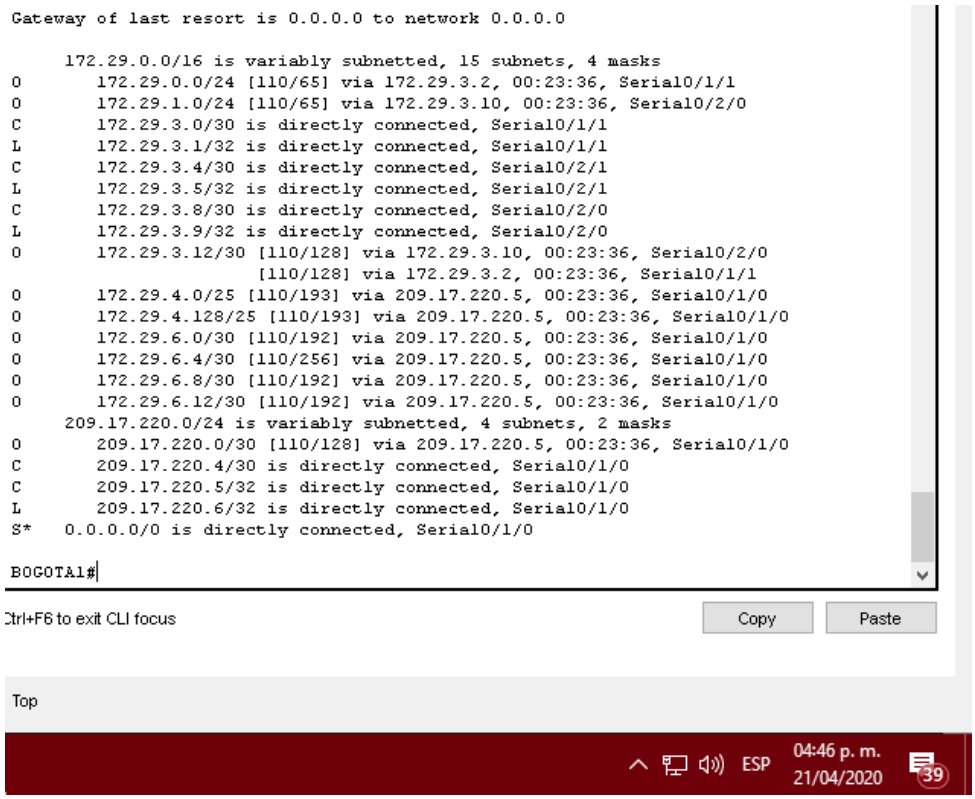


Figura 25.BOGOTA1

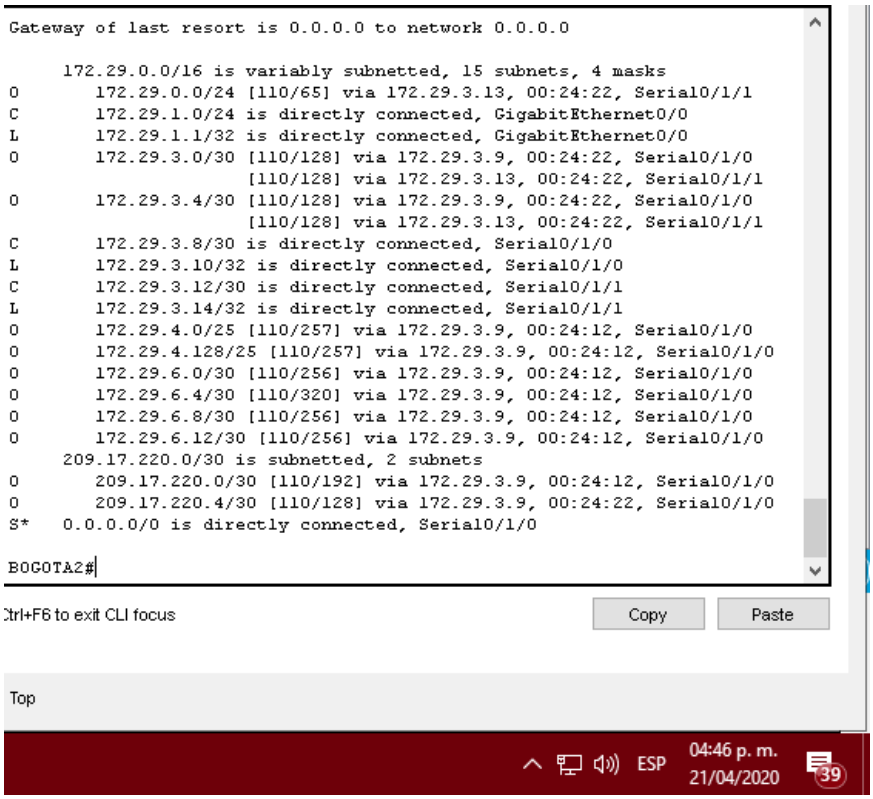


Figura 26.BOGOTA2

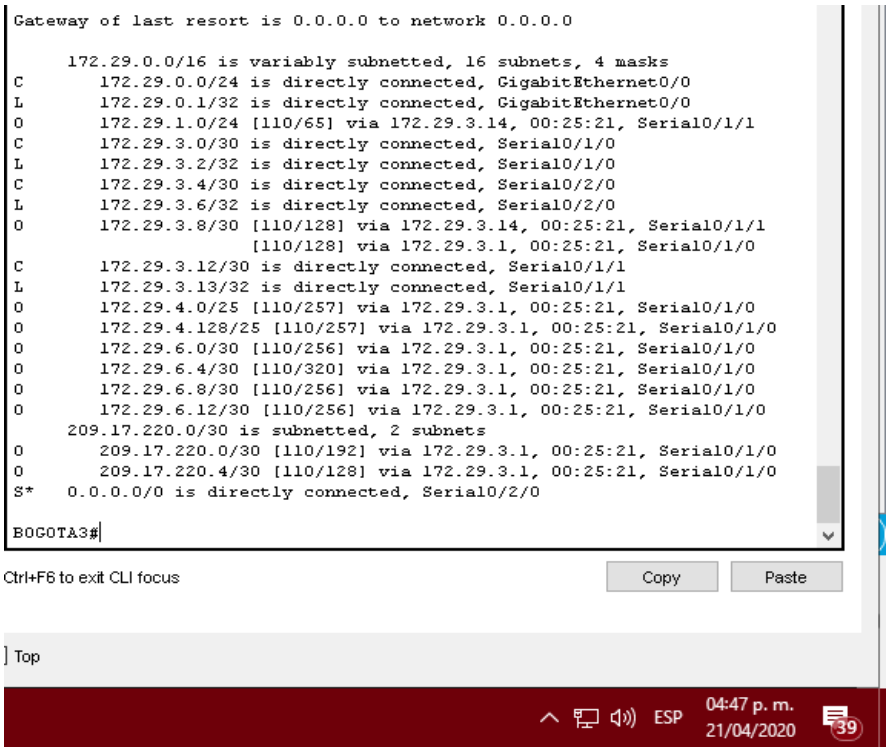



Figura 27.BOGOTA3

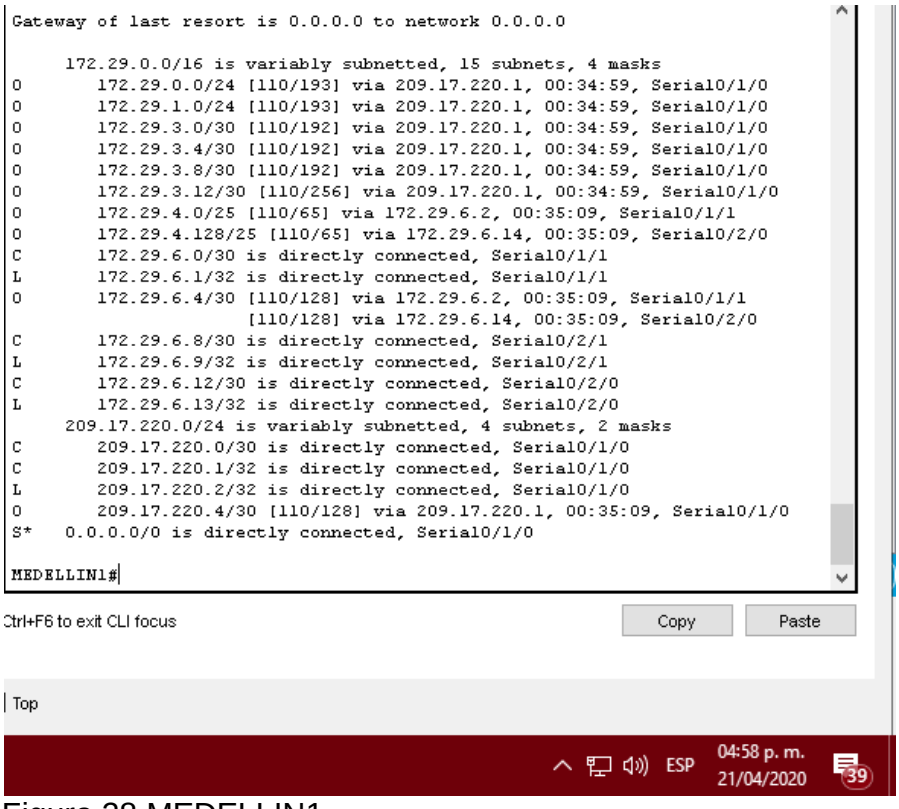



Figura 28.MEDELLIN1

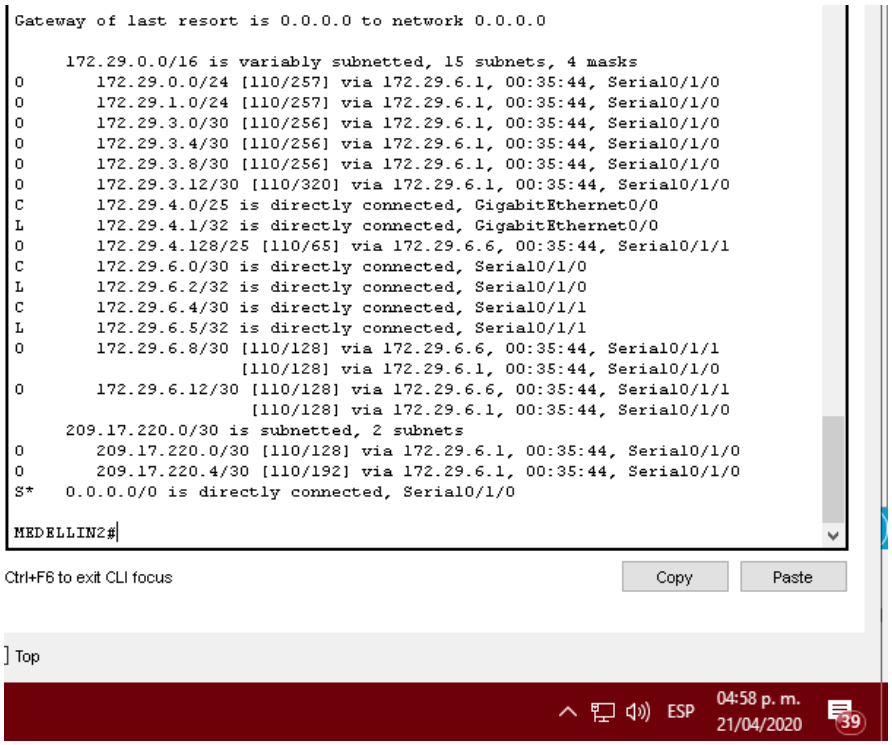



Figura 29.MEDELLIN2

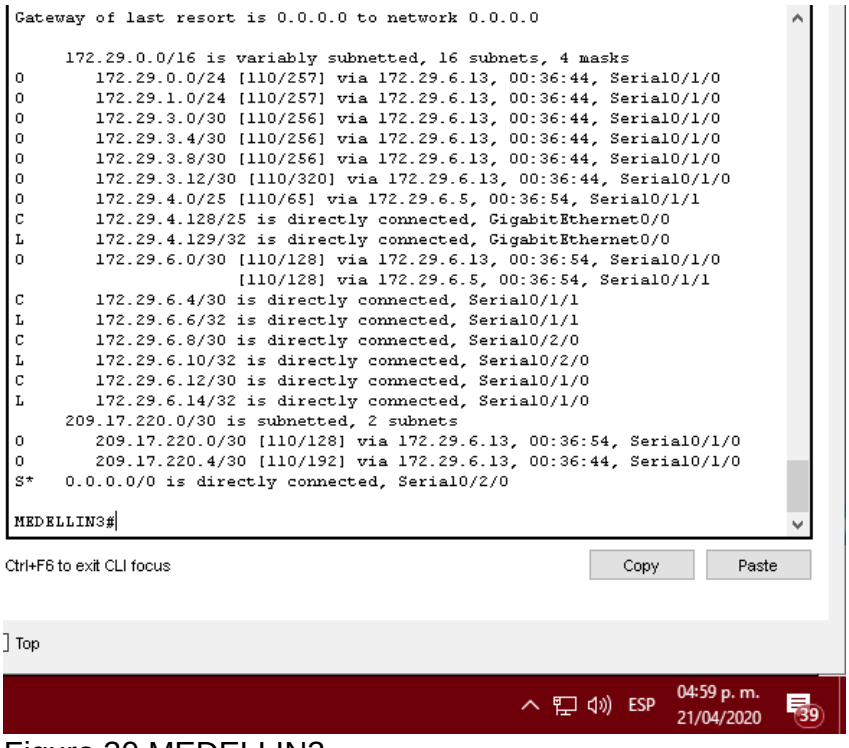



Figura 30.MEDELLIN3

2.3.1 Verificar el balanceo de carga que presentan los routers.

En las siguientes capturas de pantalla se pueden ver más descriptivamente los balanceos de carga de las redes configuradas.

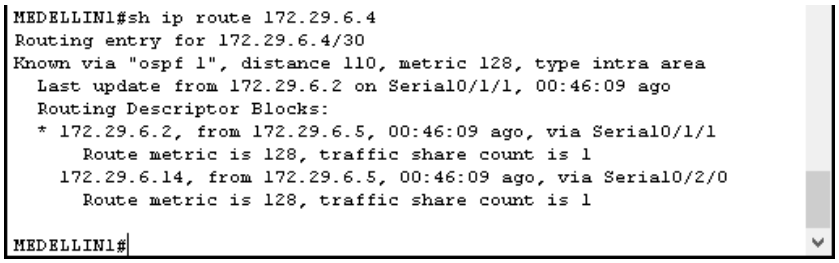



Figura 31.Balanceo de carga MEDELLIN1

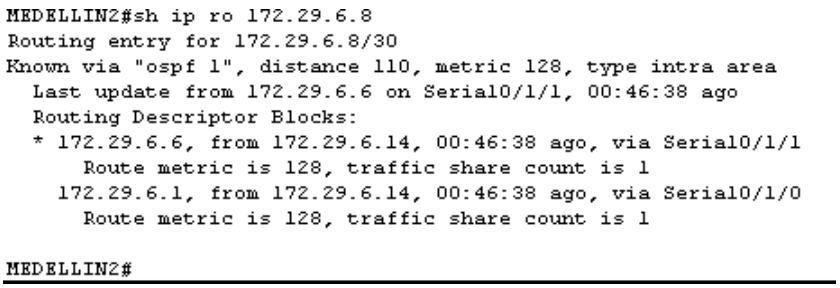



Figura 32.Balanceo de carga MEDELLIN2

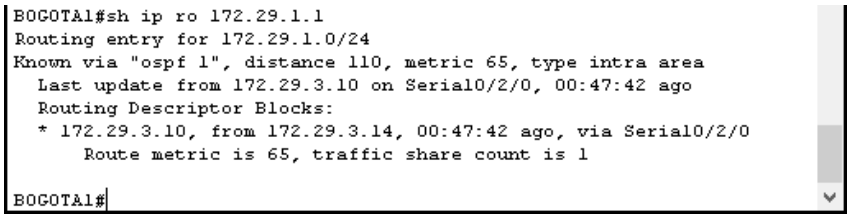



Figura 33.Balanceo de carga BOGOTA1

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.

De acuerdo a las imágenes anteriores, se puede observar la semejanza entre Bogotá 1 y Medellín 1, además se puede ver la similitud de la ubicación de acuerdo a la imagen proporcionada en el documento guía para efectuar la topología.

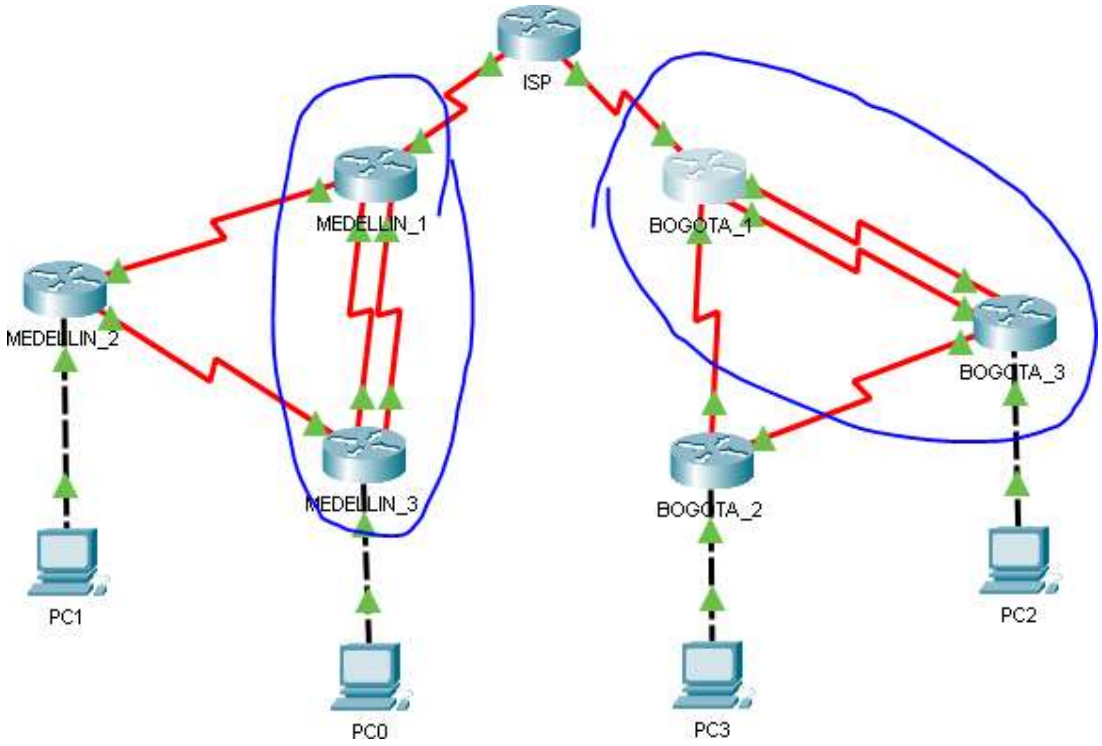



Figura 34.Distribución de carga

- Los routers Medellín2 y Bogotá2 también presentan redesconectadas 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.

2.4 Deshabilitar la propagación del protocolo OSPF

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

Tabla 26. Interfaces excluidas de propagación OSPF

| **ER** | **I** **AZ** |
|---|---|
| **ta1** | 0/0/1; SERIAL0/1/0; SERIAL0/1/1 |
| **ta2** | 0/0/0; SERIAL0/0/1 |
| **ta3** | 0/0/0; SERIAL0/0/1; SERIAL0/1/0 |
| **llín1** | 0/0/0; SERIAL0/0/1; SERIAL0/1/1 |
| **llín2** | 0/0/0; SERIAL0/0/1 |
| **llín3** | 0/0/0; SERIAL0/0/1; SERIAL0/1/0 |
| | requiere |

Tabla 27. Configuración de propagación OSPF

| **Tarea** | **Comando de IOS** |
|---|---|
| Deshabilitar propagación OSPF en MEDELLIN1 | router ospf 1<br>passive-interface s0/2/1 |
| Deshabilitar propagación OSPF en MEDELLIN2 | router ospf 1<br>passive-interface g0/0 |
| Deshabilitar propagación OSPF en MEDELLIN3 | router ospf 1<br>passive-interface g0/0 |
| Deshabilitar propagación OSPF en BOGOTA1 | router ospf 1<br>passive-interface s0/2/1 |
| Deshabilitar propagación OSPF en BOGOTA2 | router ospf 1<br>passive-interface g0/0 |
| Deshabilitar propagación OSPF en BOGOTA3 | router ospf 1<br>passive-interface g0/0 |

### 2.4.1 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.

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.

```
ISP#sh ip ospf database
            OSPF Router with ID (209.17.220.5) (Process ID 1)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link
count
209.17.220.5    209.17.220.5    1267        0x80000006 0x00b955 4
172.29.3.13     172.29.3.13     1269        0x80000008 0x004645 6
209.17.220.2    209.17.220.2    1269        0x80000009 0x00e4a8 7
172.29.6.5      172.29.6.5      1268        0x80000007 0x00bc78 5
172.29.6.14     172.29.6.14     1268        0x80000008 0x00aac1 6
172.29.3.14     172.29.3.14     1267        0x80000007 0x00b7df 5
209.17.220.6    209.17.220.6    1264        0x80000009 0x00276f 7
ISP#
```

Figura 35.Base de datos OSPF ISP

```
MEDELLIN1#sh ip ospf data
            OSPF Router with ID (209.17.220.2) (Process ID 1)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link
count
209.17.220.2    209.17.220.2    1304        0x80000009 0x00e4a8 7
172.29.3.13     172.29.3.13     1305        0x80000008 0x004645 6
172.29.6.5      172.29.6.5      1304        0x80000007 0x00bc78 5
172.29.6.14     172.29.6.14     1304        0x80000008 0x00aac1 6
209.17.220.5    209.17.220.5    1303        0x80000006 0x00b955 4
172.29.3.14     172.29.3.14     1303        0x80000007 0x00b7df 5
209.17.220.6    209.17.220.6    1300        0x80000009 0x00276f 7
MEDELLIN1#
```

Figura 36.Base de datos OSPF MEDELLIN1

```
MEDELLIN2#sh ip ospf data
            OSPF Router with ID (172.29.6.5) (Process ID 1)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link
count
172.29.6.5      172.29.6.5      1331        0x80000007 0x00bc78 5
172.29.3.13     172.29.3.13     1332        0x80000008 0x004645 6
209.17.220.2    209.17.220.2    1332        0x80000009 0x00e4a8 7
172.29.6.14     172.29.6.14     1331        0x80000008 0x00aac1 6
209.17.220.5    209.17.220.5    1331        0x80000006 0x00b955 4
172.29.3.14     172.29.3.14     1330        0x80000007 0x00b7df 5
209.17.220.6    209.17.220.6    1327        0x80000009 0x00276f 7
MEDELLIN2#
```

Figura 37.Base de datos OSPF MEDELLIN2

```
MEDELLIN3#sh ip ospf data
            OSPF Router with ID (172.29.6.14) (Process ID 1)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link
count
172.29.6.14     172.29.6.14     1361        0x80000008 0x00aacl 6
172.29.3.13     172.29.3.13     1363        0x80000008 0x004645 6
209.17.220.2    209.17.220.2    1362        0x80000009 0x00e4a8 7
172.29.6.5      172.29.6.5      1362        0x80000007 0x00bc78 5
209.17.220.5    209.17.220.5    1361        0x80000006 0x00b955 4
172.29.3.14     172.29.3.14     1361        0x80000007 0x00b7df 5
209.17.220.6    209.17.220.6    1358        0x80000009 0x00276f 7
MEDELLIN3#
```

Figura 38.Base de datos OSPF MEDELLIN3

```
BOGOTA1#sh ip ospf data
            OSPF Router with ID (209.17.220.6) (Process ID 1)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link
count
209.17.220.6    209.17.220.6    1386        0x80000009 0x00276f 7
172.29.3.13     172.29.3.13     1391        0x80000008 0x004645 6
209.17.220.2    209.17.220.2    1391        0x80000009 0x00e4a8 7
172.29.6.5      172.29.6.5      1390        0x80000007 0x00bc78 5
172.29.6.14     172.29.6.14     1390        0x80000008 0x00aacl 6
209.17.220.5    209.17.220.5    1390        0x80000006 0x00b955 4
172.29.3.14     172.29.3.14     1389        0x80000007 0x00b7df 5
BOGOTA1#
```

Figura 39.Base de datos OSPF BOGOTA1

```
BOGOTA2#sh ip ospf data
            OSPF Router with ID (172.29.3.14) (Process ID 1)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link
count
172.29.3.14     172.29.3.14     1440        0x80000007 0x00b7df 5
172.29.3.13     172.29.3.13     1442        0x80000008 0x004645 6
209.17.220.2    209.17.220.2    1442        0x80000009 0x00e4a8 7
172.29.6.5      172.29.6.5      1441        0x80000007 0x00bc78 5
172.29.6.14     172.29.6.14     1441        0x80000008 0x00aacl 6
209.17.220.5    209.17.220.5    1441        0x80000006 0x00b955 4
209.17.220.6    209.17.220.6    1438        0x80000009 0x00276f 7
BOGOTA2#
```

Figura 40.Base de datos OSPF BOGOTA2

```
BOGOTA3#sh ip ospf data
            OSPF Router with ID (172.29.3.13) (Process ID 1)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link
count
172.29.3.13     172.29.3.13     1480        0x80000008 0x004645 6
209.17.220.2    209.17.220.2    1480        0x80000009 0x00e4a8 7
172.29.6.5      172.29.6.5      1479        0x80000007 0x00bc78 5
172.29.6.14     172.29.6.14     1479        0x80000008 0x00aac1 6
209.17.220.5    209.17.220.5    1479        0x80000006 0x00b955 4
172.29.3.14     172.29.3.14     1478        0x80000007 0x00b7df 5
209.17.220.6    209.17.220.6    1476        0x80000009 0x00276f 7
BOGOTA3#
```

Figura 41.Base de datos OSPF BOGOTA3

2.5 Configurar encapsulamiento y autenticación PPP

a. Según la topología se requiere que el enlace Medellín1 con ISP sea configurado con autenticación PAP.
b. El enlace Bogotá1 con ISP se debe configurar con autenticación CHAP.

Tabla 28. Protocolo PPP (CHAP y PAP)

| Tarea | Comando de IOS |
|---|---|
| Habilitar autenticación PPP en MEDELLIN1 con PAP | username ISP secret 5 ISP<br><br>interface Serial0/1/0<br>encapsulation ppp<br>ppp authentication pap<br>ppp pap sent-username MEDELLIN1 password 0 MEDELLIN |
| Habilitar autenticación PPP en ISP con PAP y CHAP | username BOGOTA1 secret 5 BOGOTA1<br>username MEDELLIN1 secret 5 MEDELLIN1<br><br>interface Serial0/3/0<br>encapsulation ppp<br>ppp authentication pap<br>ppp pap sent-username ISP password 0 ISP<br><br>interface Serial0/3/1<br>encapsulation ppp |

| | |
|---|---|
| | ppp authentication chap |
| Habilitar autenticación PPP en BOGOTA1 con CHAP | username ISP secret 5 ISP<br><br>interface Serial0/1/0<br>encapsulation ppp<br>ppp authentication chap |

```
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 = 2/16/70
ms

MEDELLIN1#
```

Figura 42.Verificación del protocolo PPP

## 2.6 Configuración de PAT

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

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

```
MEDELLIN1#sh ip nat trans
Pro  Inside global     Inside local       Outside local      Outside
global
icmp 209.17.220.2:1024 172.29.4.133:1     209.17.220.1:1
209.17.220.1:1024
icmp 209.17.220.2:1    172.29.4.4:1       209.17.220.1:1
209.17.220.1:1
icmp 209.17.220.2:2    172.29.4.4:2       209.17.220.1:2
209.17.220.1:2

MEDELLIN1#
```

Figura 43.Traducciones en MEDELLIN1

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

```
BOGOTA1#sh ip nat trans
Pro  Inside global     Inside local       Outside local      Outside
global
icmp 209.17.220.6:1    172.29.0.2:1       209.17.220.5:1
209.17.220.5:1

BOGOTA1#
```

Figura 44.Traducciones en BOGOTA1

Tabla 29. Configuracion PAT

| Tarea | Comando de IOS |
|---|---|
| Configurar PAT en MEDELLIN1 | ip access-list standard HOST<br>permit 172.29.4.0 0.0.0.255<br><br>ip nat inside source list HOST interface Serial0/1/0 overload<br><br>interface Serial0/1/0<br>ip nat outside<br><br>interface Serial0/1/1<br>ip nat inside<br><br>interface Serial0/2/0<br>ip nat inside<br><br>interface Serial0/2/1<br>ip nat inside |
| Configurar PAT en BOGOTA1 | ip access-list standard HOST<br>permit 172.29.0.0 0.0.0.255<br><br>ip nat inside source list HOST interface Serial0/1/0 overload |

| | |
|---|---|
| | interface Serial0/1/0<br>ip nat outside<br><br>interface Serial0/1/1<br>ip nat inside<br><br>interface Serial0/2/0<br>ip nat inside<br><br>interface Serial0/2/1<br>ip nat inside |

## 2.7 Configuración del servicio DHCP

- Configurar la red Medellín2 y Medellín3 donde el router Medellín 2 debe ser el servidor DHCP para ambas redes Lan.
- El router Medellín3 deberá habilitar el paso de los mensajes broadcast hacia la IP del router Medellín2.
- Configurar la red Bogotá2 y Bogotá3 donde el router Medellín2 debe ser el servidor DHCP para ambas redes Lan.
- Configure el router Bogotá1 para que habilite el paso de los mensajes Broadcast hacia la IP del router Medellin2.

Tabla 30. Configuración DHCP

| Tarea | Comando de IOS |
|---|---|
| Configurar DHCP en MEDELLIN2 | ip dhcp excluded-address 172.29.4.1 172.29.4.3<br>ip dhcp excluded-address 172.29.4.129 172.29.4.132<br><br>ip dhcp pool MEDELLIN2 |

| | |
|---|---|
| | network 172.29.4.0 255.255.255.128<br>default-router 172.29.4.1<br>dns-server 8.8.4.4<br>ip dhcp pool MEDELLIN3<br>network 172.29.4.128 255.255.255.128<br>default-router 172.29.4.129<br>dns-server 8.8.4.4<br>ip dhcp pool BOGOTA2<br>network 172.29.0.0 255.255.255.0<br>default-router 172.29.0.1<br>dns-server 8.8.8.8<br>ip dhcp pool BOGOTA3<br>network 172.29.1.0 255.255.255.0<br>default-router 172.29.1.1<br>dns-server 8.8.8.8 |
| Habilitar paso de mensajes broadcast en MEDELLIN3 | interface GigabitEthernet0/0<br>ip helper-address 172.29.6.5 |
| Habilitar paso de mensajes broadcast en BOGOTA2 | interface GigabitEthernet0/0<br>ip helper-address 172.29.6.2 |
| Habilitar paso de mensajes broadcast en BOGOTA3 | interface GigabitEthernet0/0<br>ip helper-address 172.29.6.2 |
| Habilitar paso de mensajes broadcast en BOGOTA1 | Interface s0/2/0<br>ip helper-address 172.29.6.2<br><br>Interface s0/1/1<br>ip helper-address 172.29.6.2 |

```
MEDELLIN2#sh ip dhcp binding
IP address       Client-ID/              Lease expiration        Type
                 Hardware address
172.29.4.4       0060.4756.A222           --                     Automatic
172.29.4.133     000D.BDC2.81BD           --                     Automatic
172.29.0.2       0060.5C33.5B9E           --                     Automatic
172.29.1.2       0010.115C.301E           --                     Automatic
MEDELLIN2#
```

Figura 45.Comando sh ip dhcp binding en MEDELLIN2

# CONCLUSIONES

Examinando los contenidos analizados en el diplomado, podemos conceptualizar con claridad el termino de red, que no es más que un conjunto de equipos (computadoras y/o dispositivos) interconectados por medio de cables, señales, ondas o cualquier otro método de envío de datos, que comparten información o datos (archivos), recursos (Cd-rom, impresoras, etc.) y servicios (acceso a internet, e-mail, chat), etc.

El protocolo DHCP está diseñado fundamentalmente para economizar tiempo gestionando direcciones IP en una red grande. El servicio DHCP se encuentra activo en un servidor donde se centraliza la gestión de las direcciones IP de la red.

OSPF es un protocolo que gestiona un sistema autónomo (As) en áreas. Dichas áreas son grupos lógicos de routers cuya información se puede sintetizar para el resto de la red. Un área es una unidad de encaminamiento, es decir, todos los routers de la misma área mantienen la misma información topológica en su base de datos de estado-enlace.

Gracias a lo amigable que son todos los dispositivos CISCO, se hace posible el configurar muchos parámetros para que sea seguro su ingreso y manipulación del mismo, realizando los correspondientes ajustes y almacenarlos en la NVRAM, todo ayuda a la seguridad de la información.

# BIBLIOGRAFÍA

ARIGANELLO, Ernesto y SEVILLA BARRIENTOS, Enrique. Redes CISCO. Guía de estudio para la certificación. 2a ed. Distrito Federal México. Alfaomega Grupo Editor, 2011.

BENCHIMOL, D. Redes Cisco-Instalación y administración de hardware y Software. 20 de Enero del 2018.

CISCO. “Principios básicos de routing y switching: Listas de Control de Acceso”. {En línea}. {2 Mayo de 2020} disponible en: https://static-courseassets.s3.amazonaws.com/RSE503/es/index.html#9.0.1

SHAUGHNESSY, Tom. Manual de CISCO. 2000.