SOLUCIÓN DE DOS ESCENARIOS PRESENTES EN ENTORNOS CORPORATIVOS BAJO EL USO DE TECNOLOGÍA CISCO

FAIVER CABRERA CORREA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA DE SISTEMAS
FLORENCIA
2020

SOLUCIÓN DE DOS ESCENARIOS PRESENTES EN ENTORNOS CORPORATIVOS BAJO EL USO DE TECNOLOGÍA CISCO

FAIVER CABRERA CORREA

Diplomado de opción de grado presentado para optar el título de INGENIERO DE SISTEMAS

DIRECTOR:
INGENIERO JUAN CARLOS VESGA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA DE SISTEMAS
FLORENCIA
2020

NOTA DE ACEPTACIÓN

Firma del presidente del Jurado

Firma del Jurado

Firma del Jurado

Florencia, 30 de noviembre del 2020

CONTENIDO

CONTENIDO 4

LISTA DE FIGURAS 6

LISTA DE TABLAS 8

GLOSARIO 9

RESUMEN 11

ABSTRACT 11

INTRODUCCIÓN 13

DESARROLLO 14

1. Escenario 1: 14

1.1. Inicializar 15

1.1.1. Recargar los dispositivos 15

1.1.1.1. Configurar la plantilla SDM para que admita IPv6 16

1.1.2. Configuración del Router R1 17

1.1.3. Configuración de los Switches S1 y S2 20

1.1.4. Configuración de la infraestructura de red para cada Switch (VLAN, Trunking, EtherChannel) 22

1.2. Configurar soporte de host 25

1.2.1. Configurar soporte R1 25

1.2.2. Configurar de Host 28

1.2.3. Probar la conectividad de extremo a extremo 28

2. Escenario 2: 38

2.1. Inicializar 38

2.1.1. Recargar los dispositivos 38

2.2. Configuraciones iniciales de los dispositivos. 39

2.2.1. Configuración de servidor de Internet 39

2.2.2. Configuración del Router 1. 39

2.2.3. Configuración del Router 2. 41

2.2.4. Configuración del Router 3. 42

2.2.5. Configuración del Switch 1. 43

2.2.6. Configuración del Switch 3. 44
2.2.7. Verificar conectividad. 45
2.3. Configurar la seguridad del switch, las Vlan y el Routing entre Vlan. 46
2.3.1. Configuración del Switch 1. 46
2.3.2. Configuración del Switch 3. 47
2.3.3. Configuración del Router 1. 48
2.3.4. Verificar conectividad. 49
2.4. Configurar el protocolo de Routing Dinámico OSPF 50
2.4.1. OSPF en Router 1 50
2.4.2. OSPF en Router 2 51
2.4.3. OSPF en Router 3 51
2.4.4. Verificar OSPF 52
2.5. Implementar DHCP y NAT para IPv4 52
2.5.1. Configurar R1 como servidor DHCP para las VLAN 21 y VLAN 23. 52
2.5.2. Configurar NAT estática y dinámica en R2. 53
2.5.3. Verificar el protocolo DHCP y la NAT estática. 55
2.5.4. onfigurar NAT. 56
2.6. Configurar y verificar las listas de control de acceso ACL 57
2.6.1. Restricción líneas VTY en R2. 57
2.6.2. Comando CLI para verificar. 58
CONCLUSIONES 61
BIBLIOGRAFÍA 62
ANEXOS 64

LISTA DE FIGURAS

Figura 1 Escenario 1 (Elaboración propia nov-2020)..... 14
Figura 2 Ver configuración SDM (Elaboración propia nov-2020) 16
Figura 3 Ping desde PC-A a R1 G0/0/1.2 ipv4 (Elaboración propia nov-2020)..... 29
Figura 4 Ping desde PC-A a R1 G0/0/1.2 ipv6 (Elaboración propia nov-2020)..... 29
Figura 5 Ping desde PC-A a R1 G0/0/1.3 ipv4 (Elaboración propia nov-2020)..... 29
Figura 6 Ping desde PC-A a R1 G0/0/1.3 ipv6 (Elaboración propia nov-2020)..... 30
Figura 7 Ping desde PC-A a R1 G0/0/1.4 ipv4 (Elaboración propia nov-2020)..... 30
Figura 8 desde PC-A a R1 G0/0/1.4 ipv6 (Elaboración propia nov-2020)..... 30
Figura 9 Ping desde PC-A a al S1 de la Vlan.4 ipv4 (Elaboración propia nov-2020) 31
Figura 10 Ping desde PC-A a al S1 de la Vlan.4 ipv6 (Elaboración propia nov-2020) 31
Figura 11 Ping desde PC-A a al S2 de la Vlan.4 ipv4 (Elaboración propia nov-2020) 31
Figura 12 Ping desde PC-A a al S2 de la Vlan.4 ipv6 (Elaboración propia nov-2020) 32
Figura 13 Ping de la PC-A a PC-B ipv4 (Elaboración propia nov-2020) 32
Figura 14 Ping desde PC-A a PC-B con ipv6 (Elaboración propia nov-2020)..... 32
Figura 15 Ping desde PC-A a interface lógica R1 Bucle 0 ipv4 (Elaboración propia nov-2020)
.....33
Figura 16 Ping desde PC-A a interface lógica R1 Bucle 0 ipv6 (Elaboración propia nov-2020)
.....33
Figura 17 Ping desde PC-B a interface lógica R1 Bucle 0 ipv4 (Elaboración propia nov-2020)
.....33
Figura 18 Ping desde PC-B a interface lógica R1 Bucle 0 ipv6 (Elaboración propia nov-2020)
.....34
Figura 19 Ping de PC-B a R1 G0/0/1.2 ipv4 (Elaboración propia nov-2020) 34
Figura 20 Ping desde PC-B a R1 G0/0/1.2 con ipv6 (Elaboración propia nov-2020) 34
Figura 21 Ping de PC-B a R1 G0/0/1.3 ipv4 (Elaboración propia nov-2020) 35
Figura 22 Ping de PC-B a R1 G0/0/1.3 ipv6 (Elaboración propia nov-2020) 35
Figura 23 Ping de PC-B a R1 G0/0/1.4 ipv4 (Elaboración propia nov-2020) 35
Figura 24 Ping desde PC-B a R1 G0/0/1.4 con ipv6(Elaboración propia nov-2020) 36
Figura 25 Ping desde PC-B a al S1 de la Vlan.4 ipv4 (Elaboración propia nov-2020) 36
Figura 26 Ping desde PC-B a al S1 de la Vlan.4 ipv6(Elaboración propia nov-2020) 36
Figura 27 Ping de PC-B a S2 de la Vlan. 4 ipv4 (Elaboración propia nov-2020)..... 37
Figura 28 Ping desde PC-B a al S2 de la Vlan.4 ipv6 (Elaboración propia nov-2020) 37
Figura 29 Escenario 2 (Elaboración propia nov-2020)..... 38
Figura 30 Ping R1-R2, S0/0/0 (Elaboración propia nov-2020) 45
Figura 31 Ping R2-R3, S0/0/1(Elaboración propia nov-2020) 45
Figura 32 Ping servidor internet - Gateway predeterminado (Elaboración propia nov-2020) 45 Figura
33 Ping S1 a R1 Vlan 99 (Elaboración propia nov-2020)..... 49
Figura 34 Ping S3 a R1 Vlan 99(Elaboración propia nov-2020) 49
Figura 35 Ping S1 a R1 Vlan 21(Elaboración propia nov-2020) 50
Figura 36 Ping S3 a R1 Vlan 23(Elaboración propia nov-2020) 50
Figura 37 Información DHCP PC-A (Elaboración propia nov-2020) 55
Figura 38 Información DHCP PC-C (Elaboración propia nov-2020)..... 55

Figura 39Ping entre PC(Elaboración propia nov-2020) 56
Figura 40 Ping al web server (Elaboración propia nov-2020)..... 56
Figura 41 Telnet de R1 a R2 (Elaboración propia nov-2020)..... 58
Figura 42 Telnet de R3 a R2 (Elaboración propia nov-2020)..... 58
Figura 43 Verificar las ACL (Elaboración propia nov-2020) 59
Figura 44 Verificar las interface de la ACL configurada (Elaboración propia nov-2020)..... 60
Figura 45 Verificar las NAT(Elaboración propia nov-2020)..... 60

LISTA DE TABLAS

Tabla 1 Tabla de direccionamiento 14
Tabla 2 Recargar los dispositivos 15
Tabla 3 Configuración inicial R3 18
Tabla 4.Configuración de los Switches S1 y S2 21
Tabla 5 Configuración de infraestructura de red en los Switch 23
Tabla 6 Configuración soporte R1 27
Tabla 7 Configuración PC-A 28
Tabla 8 Configuración PC-B 28
Tabla 9 Recargo de dispositivos 38
Tabla 10 Direccionamiento Servidor de Internet 39
Tabla 11 Configuración inicial R1 40
Tabla 12 Configuración inicial en R2 41
Tabla 13 Configuración inicial R3 42
Tabla 14 Configuración inicial S1 44
Tabla 15 Configuración inicial S3 44
Tabla 16 Verificar conectividad 45
Tabla 17 Configuración S1 46
Tabla 18 Configuración S3 47
Tabla 19 Configuración encapsulación R1 48
Tabla 20 Verificar conectividad de switch a router 49
Tabla 21 OSPF R1 50
Tabla 22 OSPF R2 51
Tabla 23 OSPF R3 52
Tabla 24 R1 como server DHCP 53
Tabla 25 Configuración NAT R2 54
Tabla 26 Verificar protocolo DHCP y NAT 55
Tabla 27 Configuración del reloj y NTP 56
Tabla 28 Configuración de lista de acceso 58
Tabla 29 Verificar la configuración ACL 59

GLOSARIO

IEEE: Institute of Electrical and Electronics Engineers organización técnico profesional dedicada a la estandarización; Es la mayor asociación internacional sin fines de lucro formada por profesionales de las nuevas tecnologías, como ingenieros en eléctricos, ingenieros en electrónica, ingenieros en sistemas, ingenieros en telecomunicación y muchos más.

Interfaz: Conocida como NIC, abreviatura para su término en inglés network interface card. Se trata de un hardware adaptador de red capaz de habilitar la conexión de red entre un dispositivo y otro, PC, Router, Switch entre otros.

IPV4: Sistema direccional de 32 bites, divididos por 4 octetos de 8 bites cada uno, es usado para distinguir lógicamente un dispositivo en una red.

IPV6: Sistema direccional de 128 bites, representados en 8 campos de 16 bites cada uno usando la notación es en hexadecimal, es usado para distinguir lógicamente un dispositivo en una red, y es el sucesor de IPV4.

Loopback: Es una interfaz lógica interna del router no asignada a un puerto físico y, por lo tanto, nunca se puede conectar a otro dispositivo. La interfaz loopback es útil para probar y administrar un dispositivo Cisco IOS, ya que asegura que por lo menos una interfaz esté siempre disponible. Por ejemplo, se puede usar con fines de prueba, como la prueba de procesos de routing interno, mediante la emulación de redes detrás del router.

Line VTY: Líneas de acceso al dispositivo son de dos clases puertos seriales y conexiones de red virtuales, usadas para configurar la restricción de acceso a direcciones IP a las que se les permite acceder remotamente al proceso de EXEC del router.

Mascara de subred: Al estar un dispositivo dentro de una red se le asigna una dirección IP, sin embargo esta dirección está acompañada por una máscara de subred que entre otras cosas sirve para identificar el tipo de red a la que pertenece un dispositivo con el que se establezca una conexión.

Mascara Wilchard: Máscara de bits que indica qué partes de una dirección de IP son relevantes para la ejecución de una determinada acción resaltando los bits significativos de una dirección.

Nvram: Non-volatile random access memory - memoria de acceso aleatorio no volátil, este dispositivo hardware es una memoria de acceso aleatorio que es capaz de almacenar información y no perderla al retirar la alimentación eléctrica del componente; presentes en todos los dispositivos electrónicos que usan un firmware

para su funcionamiento. PC, teléfonos, routers y en general los dispositivos programables.

Ping: Packet Internet Groper - Herramienta de diagnóstico o comando utilizado para verificar el estado de una conexión o host local con al menos un equipo remoto contemplado en una red de tipo TCP/IP.

Router: Los Switches conectan dispositivos en una red, y los Routers conectan diferentes redes, creando los caminos y mejores rutas para que viajen los datos de forma rápida y segura.

Seguridad de puerto: Forma de aumentar la seguridad de la red. Puede ser configurada en un grupo específico de la agregación del puerto o del link (RETRASO) la seguridad puede consiste en restricciones o incluso la inhabilitar el puerto.

Switch: Componente fundamental en el desarrollo de Internet, su funcionamiento consiste en recibir paquetes de datos y direccionarlos al destinatario correcto, hoy en día ya se pueden configurar varios dispositivos desde un mismo tablero de administración y de forma remota.

Subnetting: Concepto que consiste en la subdivisión de una red IPv4 en varias subredes para evitar el desperdicio de direcciones IP.

Tracert: También conocido como tracerroute en Linux, es una herramienta que nos va a dar información acerca de la ruta que toma un paquete que será enviado desde nuestro equipo hasta un host de destino, bien sea en una red local o en Internet a un dominio en concreto.

VLAN: Red de área local virtual (VLA N) es una red de switch que es dividida en segmentos lógicamente por la función, el área, o la aplicación, sin consideración alguna hacia las ubicaciones físicas de los usuarios. Los VLAN son un grupo de host o los puertos que pueden ser situados dondequiera en una red sino comunicar como si estén en el mismo segmento físico.

RESUMEN

En el desarrollo del primer escenario de la prueba de habilidades para el diplomado CCNA2, empezamos a implementar la solución de una red que integra VLAN, DHCP, direccionamiento IPV4 e IPV6 simultáneamente, también presentas las configuraciones básicas y necesarias para el proceso de seguridad de los equipos intermedio de capa 2 y 3 de la red.

Se configuran los enlaces troncales necesarios para el correcto funcionamiento de la red habilitando las interfaces físicas y lógicas necesarias para el funcionamiento de la misma y deshabilitando los puertos innecesarios de los dispositivos para mejorar la seguridad en la red.

Por otra parte en el escenario número dos, se presenta una red al cual también se le realizan los parámetros básicos de configuración como seguridad de acceso, configuración de interfaces mediante el direccionamiento IPv4 e IPv6, configurando los enlaces troncales, creación y configuración de las VLAN para los dispositivos, configuración del ruteo dinámico mediante el protocolo OSPF.

Se configuran los host de modo que estos queden en VLANS diferentes a las cuales se les asigna una dirección de forma dinámica en base a un subnetting que se estableció en la topología. Los servidores que se implementan son el de internet y el web dichas redes difieren del tipo de direccionamiento implementado en las redes finales para los hosts, así se simula la conectividad de operaciones con otras redes.

Palabras Clave: Capa3, CCNA, DHCP, enlaces, host, interfaces, OSPF, protocolos, puertos, red, subnetting, ruteo dinámico, ruteo estático troncales, VLAN.

ABSTRACT

In the development of the first scenario of the skills test for the CCNA2 diploma, we began to implement the solution of a network that integrates VLAN, DHCP, IPV4 and IPV6 addressing simultaneously, it also presents the basic and necessary configurations for the security process of the Layer 2 and 3 intermediate equipment on the network.

The trunks necessary for the correct operation of the network are configured by enabling the physical and logical interfaces necessary for its operation and disabling the unnecessary ports of the devices to improve network security.

On the other hand, in scenario number two, a network is presented to which the basic configuration parameters such as access security, interface configuration through IPv4 and IPv6 addressing, configuring the trunk links, creation and configuration of VLANs, is presented. for devices, configuration of dynamic routing using the OSPF protocol.

The hosts are configured so that they are in different VLANS to which an address is assigned dynamically based on a subnetting that was established in the topology. The servers that are implemented are the internet and the web, these networks differ from the type of addressing implemented in the final networks for the hosts, thus the connectivity of operations with other networks is simulated.

Keywords: CCNA2, VLAN, DHCP, Layer 2, Layer 3, trunks, interfaces, ports, networ, subnetting, OSPF, protocols, host, dynamic routing, static routing.

INTRODUCCIÓN

Los escenarios 1 y 2 son una de las actividades de diplomado de profundización cisco, Network Fundamentals (CCNA1 R&S) y Routing and Switching Fundamentals (CCNA2 R&S), obligatorio para presentar la sustentación final del mencionado diplomado, con la aprobación del mismo se aspira se otorgue la opción de grado para la carrera ingeniería de sistemas.

Dichos Escenarios son topologías de redes que usan simultáneamente direccionamiento IPV4 e IPV6 basados en protocolos seguros para la conectividad y que representen la mejor eficacia en su funcionamiento.

Se realizan las simulaciones implementando configuraciones básicas, medias y avanzadas para representar el funcionamiento de manera eficiente y estable en el caso de las dos topologías presentadas. Estas configuraciones son prácticas teniendo en cuenta que estas topologías pueden y son implementadas en las organizaciones por su gran desempeño como redes convergentes.

Tras el desarrollo de los escenarios presentados se promueve el estado que crea la necesidad de incrementar la investigación como estudiante y/o profesional para brindar soluciones eficientes de manera dinámica en pro de las organizaciones en implementando redes escalables y conmutadas.

DESARROLLO

1. **Escenario 1:**

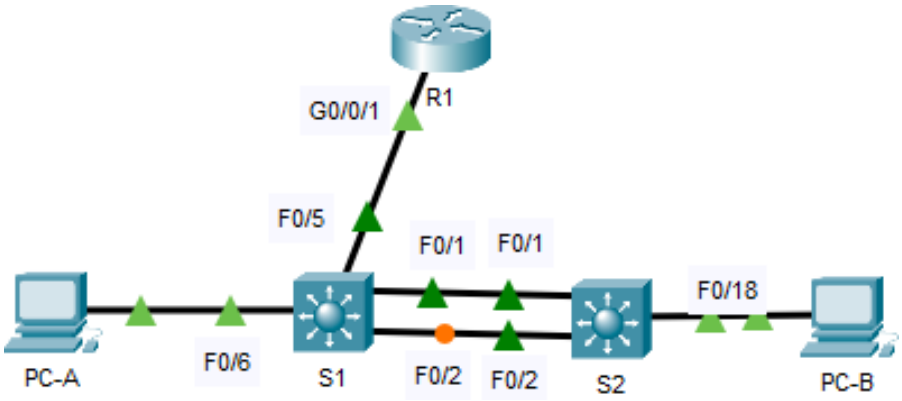


Figura 1 Escenario 1 (Elaboración propia nov-2020)

Usando la siguiente tabla de direcciones para configurar la red que permita simultáneamente IPV6 e IPV4, con una administración con protocolos de seguridad.

Tabla 1 Tabla de direccionamiento

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
R1 G0/0/1.2	10.19.8.1 /26	No corresponde
R1 G0/0/1.2	2001:db8:acad:a: :1 /64	No corresponde
R1 G0/0/1.3	10.19.8.65 /27	No corresponde
R1 G0/0/1.3	2001:db8:acad:b: :1 /64	No corresponde
R1 G0/0/1.4	10.19.8.97 /29	No corresponde
R1 G0/0/1.4	2001:db8:acad:c: :1 /64	No corresponde
R1 G0/0/1.6	No corresponde	No corresponde
R1 Loopback0	209.165.201.1 /27	No corresponde
R1 Loopback0	2001:db8:acad:209: :1 /64	No corresponde
S1 VLAN 4	10.19.8.98 /29	10.19.8.97
VLAN S1 4	2001:db8:acad:c: :98 /64	No corresponde
S1 VLAN 4	fe80: :98	No corresponde
S2 VLAN 4	10.19.8.99 /29	10.19.8.97
S2 VLAN 4	2001:db8:acad:c: :99 /64	No corresponde
S2 VLAN 4	fe80: :99	No corresponde
PC-A NIC	Dirección DHCP para IPv4	DHCP para puerta de enlace predeterminada IPv4

PC-A NIC	2001:db8:acad:a: :50 /64	fe80::1
PC-B NIC	DHCP para dirección IPv4	DHCP para puerta de enlace predeterminada IPv4
PC-B NIC	2001:db8:acad:b: :50 /64	fe80::1

(Elaboración propia nov-2020)

1.1. Inicializar

1.1.1. Recargar los dispositivos

Accedemos a la interfaz del Router y de los Switchs para realizar los procesos de inicialización y recarga. Esto se usa para eliminar cualquier configuración anterior que tengan los dispositivos que puedan crear interferencias con las nuevas que se le deseen aplicar.

Tabla 2 Recargar los dispositivos

Descripción	Script
Con el comando erase startup-config podemos eliminar la configuración de inicio de la memoria de acceso aleatorio no volátil (NVRAM).	Router>enable Router#erase startup-config Erasing the nvram filesystem will remove all configuration files! Continue? [confirm] [OK]
Con el comando reload podemos eliminar una configuración antigua de la memoria y recargarlo nuevamente. Seguidamente confirmamos el proceso con la tecla enter.	Router# Router#reload Proceed with reload? [confirm]
Con el comando erase startup-config podemos eliminar la configuración de inicio de la memoria de acceso aleatorio no volátil (NVRAM).	Switch>en Switch#erase startup-config
Verificar con show flash la información de la memoria flash para verificar el estado de las memorias.	Switch# show flash

En el caso de tener el archivo vlan.dat lo eliminamos, confirmamos el nombre del archivo a eliminar y seguidamente el proceso.	Switch#delete vlan.dat
Con el comando reload podemos eliminar una configuración antigua de la memoria y recargarlo nuevamente. Seguidamente confirmamos el proceso con la tecla enter.	Switch#reload

(Elaboración propia nov-2020)

1.1.1.1. Configurar la plantilla SDM para que admita IPv6

La configuración de la plantilla SDM, es utilizada para activar el funcionamiento del direccionamiento IPV4 en conjunto de IPV6, ingresando al modo de configuración global, seguidamente digitamos *sdm prefer dual-ipv4-and-ipv6 default*.

Switch(config)# sdm prefer dual-ipv4-and-ipv6 default

Este comando solo producirá efecto en la próxima reiniciada del Switch por lo tanto debemos:

Switch(config)#end
Switch# reload

Una vez reiniciado podemos verificar con el siguiente comando:

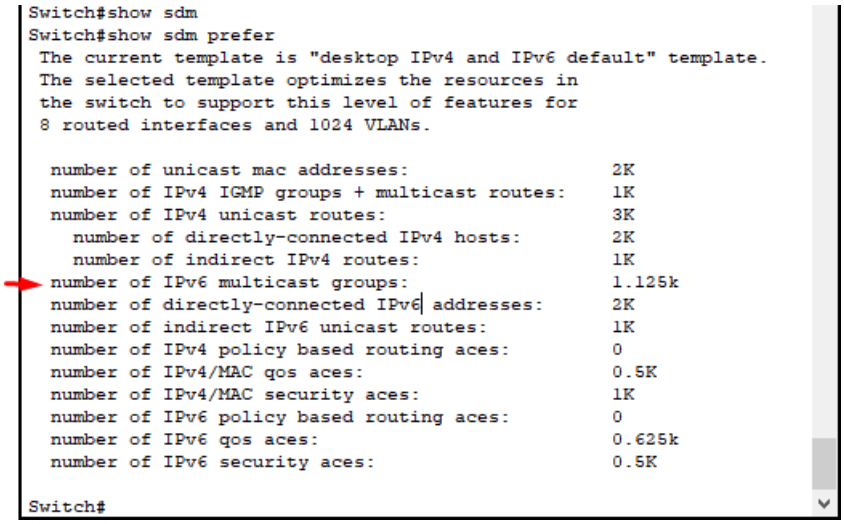


Figura 2 Ver configuración SDM (Elaboración propia nov-2020)

1.1.2. Configuración del Router R1

En este punto de configuración inicial del Router empezamos con desactivar la búsqueda de DNS, esto evita que el router intente traducir una palabra mal escrita a una dirección IP proceso que tarda un tiempo de un minuto en cada equivocación; especificamos el nombre del Router y especifica el nombre de dominio DNS.

Asignamos una contraseña cifrada para el modo EXEC privilegiado y una para el acceso a la consola - es el primer filtro de seguridad del router; usaremos el siguiene comando para crear un usuario administrativo en la base de datos local R1(config)# **username <nombre> [privilege <nivel>] [password[<tipo-cifrado>] <contraseña>],** <nombre> es el nombre de usuario, <nivel> entre 0 y 15, representa el nivel de privilegios del usuario (nivel 15 es el modo privilegiado y nivel 0 es el modo usuario), <tipo-cifrado> 0 para contraseñas no encriptadas y 7 para contraseñas ocultas y <contraseña> contraseña que debe introducir el usuario para ingresar al router (1 a 25 caracteres).
Se pueden crear usuarios con distintos niveles de privilegios. Existen 15 niveles de privilegio:

- Nivel 1: Predefinido para el acceso a nivel de usuario.
- Niveles 2 al 14: Privilegios personalizables.
- Nivel 15: Predefinido para el modo enable.

Otras de las configuraciones son las líneas VTY para habilitar las sesiones remotas entrantes por SSH Secure Shell, evitando otro tipo de conexiones. Se configurarían protocolos de seguridad como el modo de encriptación. Habilitamos el Routing-ipv6 que permite enrrutar paquetes IPv6 entre las distintas interfaces del Router con un identificador para una sola interfaz, en un solo nodo.

Configuramos y prendemos la interfaz G0/0/1 y sus subinterfaces (2,3,4 y 6) desde el modo de configuración global e ingresando a cada interfaz, habilitamos la encapsulación IEEE 802.1Q del tráfico en cada una de las subinterfaz, al igual que sus direcciones ip tomadas de la tabla de direccionamiento (**ver tabla 1**), se agrega una descrición y se habilita con el comando *no shutdown.* Se configura la interface

lógica Loopback del Router y sus finalidades son solo de prueba y no está asignada a un puerto físico.

Generamos una clave RSA de módulo 1024 bits siendo el rango entre 350 a 4096 bits y se recomienda usar 1024 para que no tarde tanto en el proceso de encriptar y desencriptar.

Por último guardamos toda la configuración en ejecución en el archivo de inicio de la memoria de acceso aleatorio no volátil

R1# **copy running-config startup-config**

Con el siguiente comando podemos ver toda la configuración

R1#**show running-config**

Tabla 3 Configuración inicial R3

Tarea	Script CLI
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R1
Nombre de dominio	R1(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	R1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola- es el primer filtro de seguridad del router	R1(config)#line console 0 R1(config-line)#password ciscoconpass R1(config-line)#login
Longitud mínima para la contraseña de 10 caracteres	R1(config)#security passwords min-length 10
Crear un usuario administrativo en la base de datos local	R1(config)#
Configurar el inicio de sesión en las líneas de terminal virtual VTY para que use la base de datos local	R1(config)#line vty 0 15 R1(config-line)#login local
Configurar VTY solo aceptando SSH	R1(config-line)#transport input ssh R1(config-line)#exit
Cifrar las contraseñas de texto no cifrado, Impide que personas sin autorización puedan ver las contraseñas en el archivo de configuración	R1(config)# Service password-encryption
Configure un MOTD Banner, Mensaje de inicio	R1(config)# banner motd #Bienvenido por favor ingrese sus credenciales#
Habilitar el routing IPv6	R1(config)# ipv6 unicast-routing

Configurar interfaz G0/0/1 y subinterfaces Establezca la descripción Establece la dirección IPv4. Establezca la dirección local de enlace IPv6 como fe80: :1 Establece la dirección IPv6. Activar la interfaz.	1. R1# configure terminal R1(config)# interface g0/0/1.2 R1(config-subif)# encapsulation dot1q 2 R1(config-subif)#ip address 10.19.8.1 255.255.255.192 R1(config-subif)#ipv6 address 2001:db8:acad:a::1/64 R1(config-subif)#description "Vlan corresponde a dependencia Bikes" R1(config-subif)#ipv6 address fe80::1 link-local R1(config-subif)#no shutdown R1(config-subif)#exit 2. R1#conf t R1(config)#int g0/0/1.3 R1(config-subif)#encapsulation dot1Q 3 R1(config-subif)#ip address 10.19.8.65 255.255.255.224 R1(config-subif)#ipv6 address 2001:db8:acad:b::1/64 R1(config-subif)#ipv6 address fe80::1 link-local R1(config-subif)#description "Vlan corresponde a dependencia Trikes" R1(config-subif)#no shutdown R1(config-subif)#exit R1(config)#exit 3. R1#conf t R1(config)#int g0/0/1.4 R1(config-subif)#encapsulation dot1Q 4 R1(config-subif)#ip address 10.19.8.97 255.255.255.248 R1(config-subif)#ipv6 address 2001:db8:acad:c::1/64 R1(config-subif)#ipv6 address fe80::1 link-local R1(config-subif)#description "Vlan corresponde a dependencia Management" R1(config-subif)#no shutdown R1(config-subif)#exit R1(config)#exit

	4. R1(config-subif)#interface g0/0/1.6 R1(config-subif)#encapsulation dot1q 6 Native R1(config-subif)#description "Vlan corresponde subred native" 5. R1(config-subif)#interface g0/0/1 R1(config-if)#no sh
Configure el Loopback0 interface Establezca la descripción Establece la dirección IPv4. Establece la dirección IPv6. Establezca la dirección local de enlace IPv6 como fe80::1	R1#conf t R1(config)#int loopback 0 R1(config-if)#ip address 209.165.201.1 255.255.255.224 R1(config-if)#ipv6 address 2001:db8:acad:209::1/64 R1(config-if)#description "Configuracion interface lógica Loopback0" R1(config-if)#no shutdown R1(config-if)#exit R1(config)#exit
Generar una clave de cifrado RSA, Módulo de 1024 bits	R1(config)#crypto key generate rsa general-keys modulus 1024

(Elaboración propia nov-2020)

1.1.3. Configuración de los Switches S1 y S2

Realizamos la configuración a los Switches, en algunos pasos similar a la que se le realizó al Router y cumpliendo funciones similares; Como desactivar el DNS, asignar nombres para identificarlos en la red, asignación de nombre de dominio, contraseñas para el acceso a la consola y el modo privilegiado, creación de usuarios administrativos en la base de datos local, configuraciones de las líneas VTY para las conexiones remotas SSH, cifrar las contraseñas, configuración del banner y asignación de cifrado RSA.

Se configuran las interfaces VLAN según tabla de direccionamiento (**ver tabla 1**), estableciendo el direccionamiento IPV4 e IPV6 y el Link-local en la interface VLAN 4, para todos estos pasos se debe prender la interface con el comando *no shutdown;* en este paso por último configuramos la puerta de enlace predeterminada para IPV4 10.19.8.97

Tabla 4.Configuración de los Switches S1 y S2

Tarea	Script CLI
Desactivar la búsqueda DNS.	Switch(config)#no ip domain-lookup
Nombre del switch S1 o S2, según proceda	S1 Switch(config)#hosname S1 S2 Switch(config)#hosname S2
Nombre de dominio ccna-lab.com	S1(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado ciscoenpass	S1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola. ciscoconpass	S1(config)#line console 0 S1(config-line)#password ciscoconpass S1(config-line)#login
Crear un usuario administrativo en la base de datos local Nombre de usuario: admin Password: admin1pass	S1(config)#username admin secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	S1(config)#line vty 0 15 S1(config-line)#login local
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S1(config-line)#transport input ssh S1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	S1(config)#Service password-encryption
Configurar un MOTD Banner	S1(config)#banner motd #Bienvenido al Switch 1 por favor ingrese sus credenciales#
Generar una clave de cifrado RSA Módulo de 1024 bits	S1(config)#crypto key generate rsa general-keys modulus 1024
Configurar la interfaz de administración (Switch Virtual Interface) (SVI) interfaz virtual, no vinculada a ningún puerto físico del dispositivo. Establecer la dirección IPv4 de capa 3 Establezca la dirección local de enlace IPv6 como FE80: :98 para S1 y FE80: :99 para S2	S1 S1#configure terminal S1(config)#interface vlan 4 S1(config-if)#ip address 10.19.8.98 255.255.255.248 S1(config-if)#ipv6 add 2001:db8:acad:c::98/64 S1(config-if)#ipv6 address fe80::98 link-local S1(config-if)#no shutdown S1(config-if)#exit

Establecer la dirección IPv6 de capa 3	S2 S1#configure terminal S1(config)#interface vlan 4 S1(config-if)#ip address 10.19.8.99 255.255.255.248 S1(config-if)#ipv6 add 2001:db8:acad:c::99/64 S1(config-if)#ipv6 address fe80::99 link-local S1(config-if)#no shutdown S1(config-if)#exit
Configuración del gateway predeterminado como 10.19.8.97 para IPv4	S1(config)#ip default-gateway 10.19.8.97

(Elaboración propia nov-2020)

1.1.4. Configuración de la infraestructura de red para cada Switch (*VLAN, Trunking, EtherChannel)*

S1 y S2

Configuramos las VLAN en cada Switch de la misma forma, ingresando al modo de configuración global, ingresamos a cada interface de las VLAN y cuando el indicador del comando este como *(config-vlan)#* así podemos agregar el nombre. Siguiendo la topología (**ver figura 1**) podemos usar el comando *S1(config-vlan)#do sh vlan br* para ver las VLAN creadas. Notaremos que el S1 tiene tres conexiones troncales dos con S2 y una con R1, por las interfaces g1/0/1-2 y g1/0/5 y S2 tiene dos conexiones troncales con S1 por las interfaces g1/0/1-2; prendemos el modo troncal, pero apagamos las interfaces g1/0/1-2 de cada Switch e ingresamos el tipo de encapsulación (802.1Q) en estos puerto y se agregan a la VLAN nativa 6.

La tecnología EtherChannel es construida de acuerdo con los estándares 802.3 full-duplex Fast Ethernet. La cual permite la agrupación lógica de varios enlaces físicos Ethernet mediante los protocolos LACP/PAgP. Para conectar los dos Switch mediante dos enlaces físicos usamos el protocolo LACP (Link Aggregation Control Protocolo) donde los puertos deben estar en un dispositivo en modo activo y para el otro pasivo.

Se configuran los puertos de acceso de los Switch donde están conectados los Host y se agregan a las VLAN que corresponde como se muestra en la tabla (**Ver tabla 5**); a estas interfaces fa0/6 y fa0/18 según corresponden las conexiones de los host en los Switch configurando la seguridad permitiendo un máximo de 3 MAC distintas para por cada puerto y con el comando *switchport port-security mac-address sticky*

activamos el aprendizaje sin modificaciones, con el comando *S1#sh port-security int fa0/6* podemos verificar la seguridad del puerto fa0/6.

Otro paso importante es proteger los puertos no utilizados, ingresamos desde cada Switch a las interfaces para la SVI no utilizadas, establecemos el puerto en modo de acceso los asignamos a la VLAN 5, agregamos una descripción y apagamos los puertos con el comando *shutdown.*

Por últimos prendemos los puertos de los Switch g1/1/1-2

Tabla 5 Configuración de infraestructura de red en los Switch

Tarea	Script CLI
Crear VLAN VLAN 2, name Bikes VLAN 3, name Trikes VLAN 4, name Management VLAN 5, name Parking VLAN 6, name Native	S1>enable S1#configure terminal S1(config)# vlan 2 S1(config-vlan)#name Bikes S1(config-if)#exit S1(config)# vlan 3 S1(config-vlan)#name Trikes S1(config)# vlan 4 S1(config-vlan)#name Management S1(config)# vlan 5 S1(config-vlan)#name Parking S1(config)# vlan 6 S1(config-vlan)#name Native S1(config-if)#no shutdown S1(config-if)#exit
Crear troncos 802.1Q que utilicen la VLAN 6 nativa S1 Interfaces F0/1, F0/2 y F0/5 S2 Interfaces F0/1 y F0/2	S1 S1#conf t S1(config)#int g1/0/5 S1(config-if-range)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 6 S1(config)#int range g1/0/1-2 S1(config-if-range)shutdown S1(config-if-range)#switchport trunk encapsulation dot1q S1(config-if-range)#switchport mode trunk S1(config-if-range)#switchport trunk native vlan 6

	S2 S2(config)#int range g1/0/1-2 S2(config-if-range)shutdown S2(config-if-range)#switchport trunk encapsulation dot1q S2(config-if-range)#switchport mode trunk S2(config-if-range)#switchport trunk native vlan 6
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2 Usar el protocolo LACP para la negociación	S1 S1(config-if-range)#channel-group 1 mode active S1(config-if-range)#int port-channel 1 S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 6 S2 S1(config-if-range)#channel-group 1 mode active S1(config-if-range)#int port-channel 1 S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 6
Configurar el puerto de acceso de host. S1 Para VLAN 2 Interface F0/6 S2 Para VLAN 3 Interfaz F0/18	S1 S1(config)#int g1/0/6 S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 2 S2 S2(config)#int g1/0/18 S2(config-if)#switchport mode access S2(config-if)#switchport access vlan 3
Configurar la seguridad del puerto en los puertos de acceso Permitir 3 direcciones MAC	S1 S1(config)#int fa0/6 S1(config-if)#switchport mode access S1(config-if)#switchport port-security S1(config-if)#switchport port-security maximum 3

	S2 S2(config)#int g1/0/18 S2(config-if)#switchport mode access S2(config-if)#switchport port-security S2(config-if)#switchport port-security maximum 3
Proteja todas las interfaces no utilizadas Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar	S1 S1(config)#int range g1/0/3,g1/0/4,g1/0/7-24S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 5 S1(config-if-range)#description "Puertos de la Vlan 5 off" S1(config-if-range)#shutdown S1(config-if-range)#end S1(config)#int range Gig1/1/1, Gig1/1/2, Gig1/1/3, Gig1/1/4 S2 S2(config)#int range g1/0/3-17,g1/0/19-24 S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 5 S2(config-if-range)#description "Puertos de la Vlan 5 off" S2(config-if-range)#shutdown S2(config)#int range g1/0/19-24 S2(config)#int range Gig1/1/1, Gig1/1/2, Gig1/1/3, Gig1/1/4

(Elaboración propia nov-2020)

1.2. Configurar soporte de host

1.2.1. Configurar soporte R1

Para establecer el Default Routing IPV6 configuramos en los switch *S1(config)#ipv6 route ::/0 2001:db8:acad:c::*1 ingresando al modo de configuración global, podemos verificar la configuración con el comando *sh ip route br*

Nos piden activar en la VLAN 2 y VLAN 4 el protocolo DHCP, asignando las últimas 10 direcciones utilizables de cada subinterface, para esto verificamos la tabla de direccionamiento (**Ver tabla 1**) y identificamos los bits que pertenecen al identificador de red de la dirección IPV4 y la máscara de subred, tomando el octeto completo, esto lo hacemos para identificar la dirección de BROADCAST en cada subinterface. Podemos realizar el cálculo matemático utilizando la operación OR de la IP con el inverso (NOT) de su máscara de red/subred.

	AND	OR
00	0	0
01	0	1
10	0	1
11	1	1

O utilizamos una calculadora online como la que encontramos en la siguiente dirección http://labvirtual.webs.upv.es/ipcalc.html ahí calcularemos entre otras cosas las direcciones utilizables de la subred.

Direcciones utilizables para la VLAN2 10.19.8.1 hasta la 10.19.8.62

Direcciones utilizables para la VLAN3 10.19.8.65 hasta 10.19.8.94

Activamos el servicio DHCP con el comando *service dhcp* y asignamos un nombre al Pool de direccionamiento para este caso colocamos el nombre de la subred, asignamos la puerta de enlace predeterminada y podemos adicional asignar un servidor DNS, por ultimo excluimos las direcciones para cada caso teniendo en cuenta de permitir las últimas 10 direcciones de la subred en cada VLAN.

Después de aplicar estas configuraciones guardamos toda la configuración en ejecución en el archivo de inicio de la memoria de acceso aleatorio no volátil NVRAM y reiniciamos los dispositivos (*reload*)

Podemos verificar estas configuraciones con el comando *sh ip dhcp binding*

Tabla 6 Configuración soporte R1

Tarea	Script
Configure Default Routing Crear rutas predeterminadas para IPv4 e IPv6 que dirijan el tráfico a la interfaz Loopback 0	R1(config)#ip route 0.0.0.0 0.0.0.0 loopback 0 R1(config)#ipv6 route ::/0 loopback 0
Configurar IPv4 DHCP para VLAN 2 Cree un grupo DHCP para VLAN 2, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio ccna-a.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada	R1(config)#service dhcp R1(config)#ip dhcp pool Bikes ~~R1(dhcp-config)#dns-server 10.19.8.3~~ R1(dhcp-config)#exit R1(config)#ip dhcp excluded-address 10.19.8.**1** 10.19.8.52 R1(config)#ip dhcp pool Bikes R1(dhcp-config)#network 10.19.8.**0** 255.255.255.192 R1(dhcp-config)#default-router 10.19.8.**1** R1(dhcp-config)#domain-name ccna-a.net
Configurar DHCP IPv4 para VLAN 3 Cree un grupo DHCP para VLAN 3, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio ccna-b.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada	~~R1(dhcp-config)#dns-server 10.19.8.67~~ R1(config)#ip dhcp excluded-address 10.19.8.6**5** 10.19.8.84 R1(config)#ip dhcp pool Trikes R1(dhcp-config)#network 10.19.8.6**4** 255.255.255.224 R1(dhcp-config)#default-router 10.19.8.65 R1(dhcp-config)#domain-name ccna-b.net

(Elaboración propia nov-2020)

1.2.2. Configurar de Host

Para este paso ingresamos a cada Host y activamos la detección de redes por IPV4 y configuramos manualmente las direcciones IPV6 según la tabla de direccionamiento (**Ver tabla 1**)

Tabla 7 Configuración PC-A

Configuración de red de PC-A	
Dirección física	0030.F213.7D33
Dirección IP	10.19.8.53 2001:DB8:ACAD:A:230:F2FF:FE13:7D33
Máscara de subred	255.255.255.192
Gateway predeterminado	10.19.8.1
Gateway predeterminado IPv6	FE80::1

(Elaboración propia nov-2020)

Tabla 8 Configuración PC-B

Configuración de red de PC-B	
Dirección física	0040.0B97.33E0
Dirección IP	10.19.8.85 2001:DB8:ACAD:B::50/64
Máscara de subred	255.255.255.224
Gateway predeterminado	10.19.8.65
Gateway predeterminado IPv6	2001:DB8:ACAD:B:240:BFF:FE97:33E0
Link-local	FE80::1

(Elaboración propia nov-2020)

1.2.3. Probar la conectividad de extremo a extremo

PC-A

Desde PC-A A G0/0/1.2

```
C:\>ping 10.19.8.1

Pinging 10.19.8.1 with 32 bytes of data:

Reply from 10.19.8.1: bytes=32 time=2ms TTL=255
Reply from 10.19.8.1: bytes=32 time<1ms TTL=255
Reply from 10.19.8.1: bytes=32 time<1ms TTL=255
Reply from 10.19.8.1: bytes=32 time=2ms TTL=255

Ping statistics for 10.19.8.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 1ms
```

Figura 3 Ping desde PC-A a R1 G0/0/1.2 ipv4 (Elaboración propia nov-2020)

```
C:\>ping 2001:db8:acad:a::1

Pinging 2001:db8:acad:a::1 with 32 bytes of data:

Reply from 2001:DB8:ACAD:A::1: bytes=32 time=69ms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time=11ms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time=5ms TTL=255

Ping statistics for 2001:DB8:ACAD:A::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 69ms, Average = 21ms
```

Figura 4 Ping desde PC-A a R1 G0/0/1.2 ipv6 (Elaboración propia nov-2020)

```
C:\>ping 10.19.8.65

Pinging 10.19.8.65 with 32 bytes of data:

Reply from 10.19.8.65: bytes=32 time=1ms TTL=255
Reply from 10.19.8.65: bytes=32 time<1ms TTL=255
Reply from 10.19.8.65: bytes=32 time<1ms TTL=255
Reply from 10.19.8.65: bytes=32 time<1ms TTL=255

Ping statistics for 10.19.8.65:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Figura 5 Ping desde PC-A a R1 G0/0/1.3 ipv4 (Elaboración propia nov-2020)

```
C:\>ping 2001:db8:acad:a::1

Pinging 2001:db8:acad:a::1 with 32 bytes of data:

Reply from 2001:DB8:ACAD:A::1: bytes=32 time=21ms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time=34ms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time<1ms TTL=255

Ping statistics for 2001:DB8:ACAD:A::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 34ms, Average = 13ms
```

Figura 6 Ping desde PC-A a R1 G0/0/1.3 ipv6 (Elaboración propia nov-2020)

```
C:\>ping 10.19.8.97

Pinging 10.19.8.97 with 32 bytes of data:

Reply from 10.19.8.97: bytes=32 time<1ms TTL=255
Reply from 10.19.8.97: bytes=32 time=11ms TTL=255
Reply from 10.19.8.97: bytes=32 time=11ms TTL=255
Reply from 10.19.8.97: bytes=32 time=39ms TTL=255

Ping statistics for 10.19.8.97:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 39ms, Average = 15ms

C:\>
```

Figura 7 Ping desde PC-A a R1 G0/0/1.4 ipv4 (Elaboración propia nov-2020)

```
C:\>ping 2001:db8:acad:c::1

Pinging 2001:db8:acad:c::1 with 32 bytes of data:

Reply from 2001:DB8:ACAD:C::1: bytes=32 time=14ms TTL=255
Reply from 2001:DB8:ACAD:C::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:C::1: bytes=32 time=20ms TTL=255
Reply from 2001:DB8:ACAD:C::1: bytes=32 time=34ms TTL=255

Ping statistics for 2001:DB8:ACAD:C::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 34ms, Average = 17ms
```

Figura 8 desde PC-A a R1 G0/0/1.4 ipv6 (Elaboración propia nov-2020)

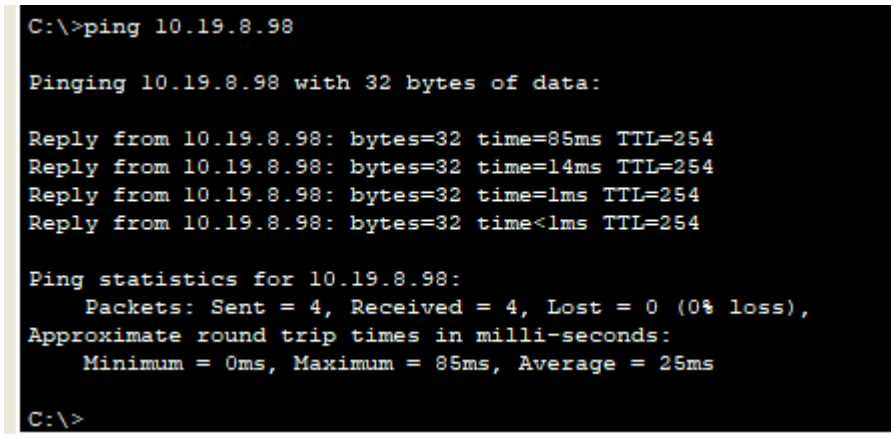


Figura 9 Ping desde PC-A a al S1 de la Vlan.4 ipv4 (Elaboración propia nov-2020)

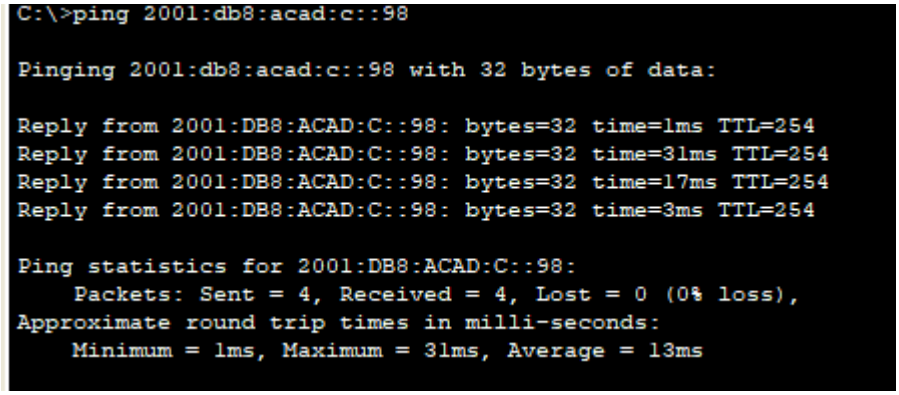


Figura 10 Ping desde PC-A a al S1 de la Vlan.4 ipv6 (Elaboración propia nov-2020)

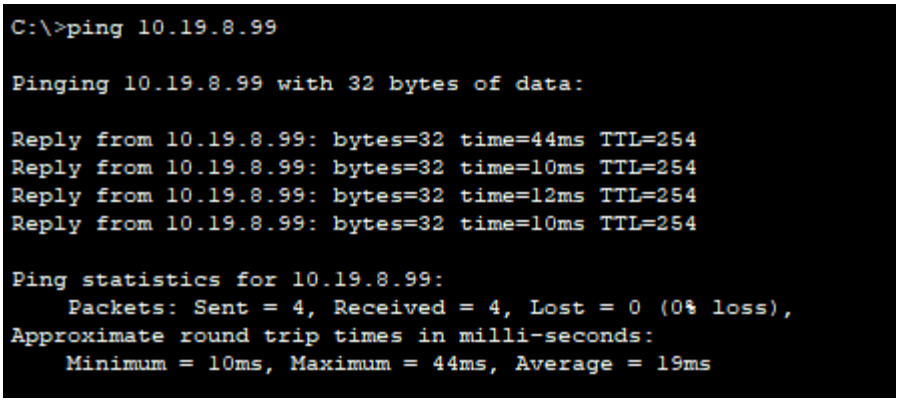


Figura 11 Ping desde PC-A a al S2 de la Vlan.4 ipv4 (Elaboración propia nov-2020)

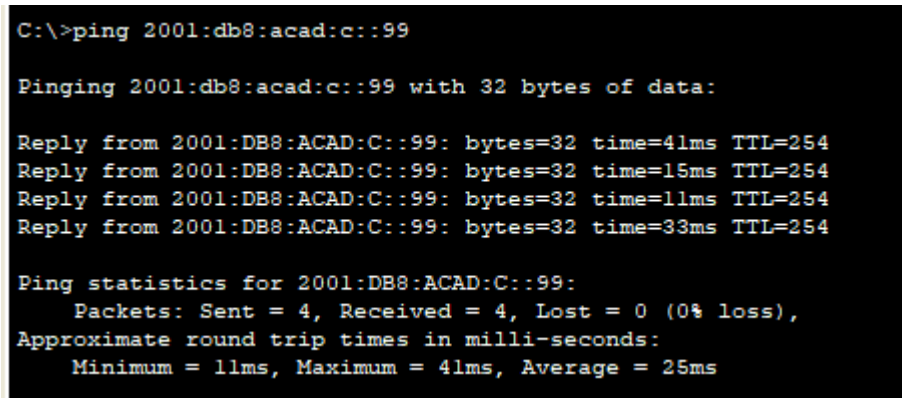


Figura 12 Ping desde PC-A a al S2 de la Vlan.4 ipv6 (Elaboración propia nov-2020)

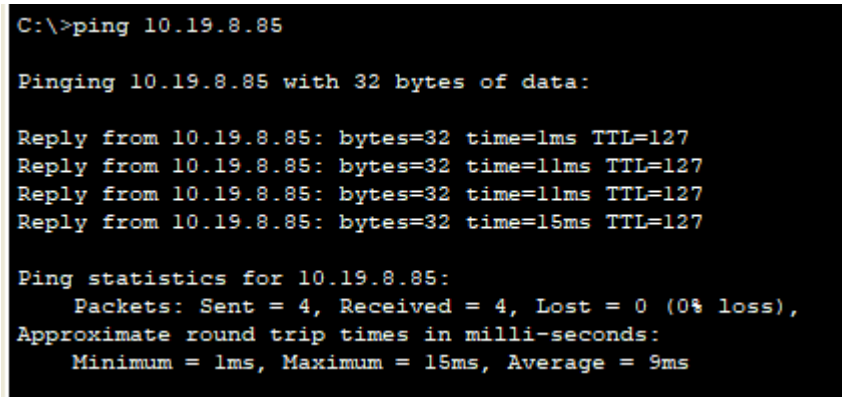


Figura 13 Ping de la PC-A a PC-B ipv4 (Elaboración propia nov-2020)

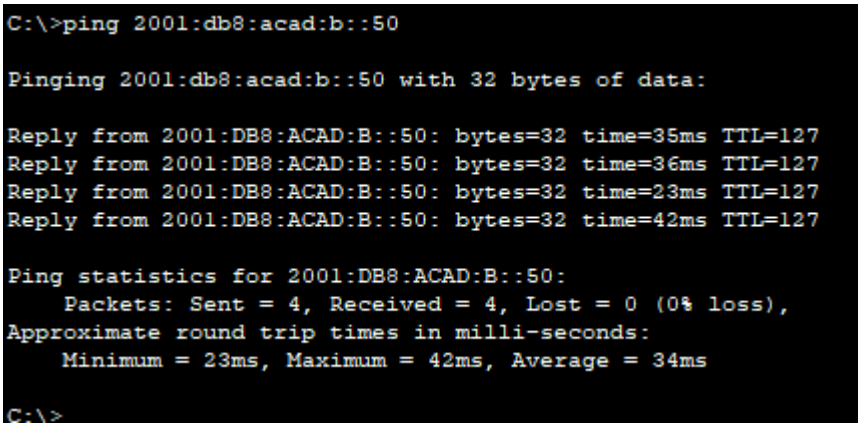


Figura 14 Ping desde PC-A a PC-B con ipv6 (Elaboración propia nov-2020)

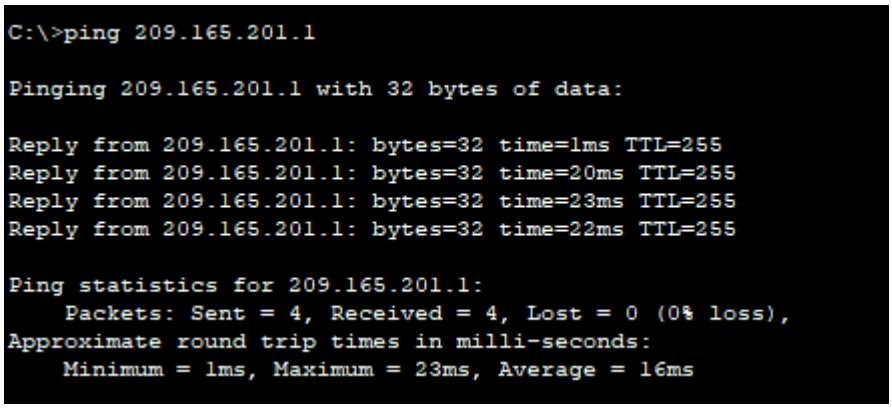


Figura 15 Ping desde PC-A a interface lógica R1 Bucle 0 ipv4 (Elaboración propia nov-2020)

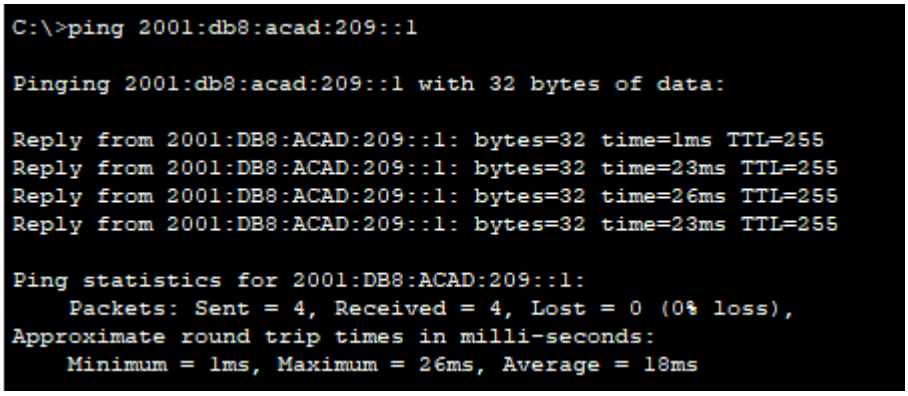


Figura 16 Ping desde PC-A a interface lógica R1 Bucle 0 ipv6 (Elaboración propia nov-2020)

PC-B

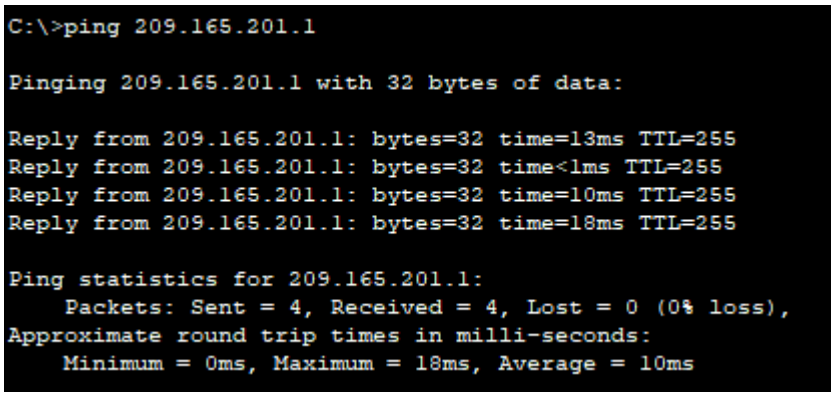


Figura 17 Ping desde PC-B a interface lógica R1 Bucle 0 ipv4 (Elaboración propia nov-2020)

```
C:\>ping 2001:db8:acad:209::1

Pinging 2001:db8:acad:209::1 with 32 bytes of data:

Reply from 2001:DB8:ACAD:209::1: bytes=32 time=1ms TTL=255
Reply from 2001:DB8:ACAD:209::1: bytes=32 time=17ms TTL=255
Reply from 2001:DB8:ACAD:209::1: bytes=32 time=16ms TTL=255
Reply from 2001:DB8:ACAD:209::1: bytes=32 time<1ms TTL=255

Ping statistics for 2001:DB8:ACAD:209::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 17ms, Average = 8ms
```

Figura 18 Ping desde PC-B a interface lógica R1 Bucle 0 ipv6 (Elaboración propia nov-2020)

```
C:\>ping 10.19.8.1

Pinging 10.19.8.1 with 32 bytes of data:

Reply from 10.19.8.1: bytes=32 time=1ms TTL=255
Reply from 10.19.8.1: bytes=32 time=20ms TTL=255
Reply from 10.19.8.1: bytes=32 time=20ms TTL=255
Reply from 10.19.8.1: bytes=32 time=13ms TTL=255

Ping statistics for 10.19.8.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 20ms, Average = 13ms
```

Figura 19 Ping de PC-B a R1 G0/0/1.2 ipv4 (Elaboración propia nov-2020)

```
C:\>ping 2001:db8:acad:a::1

Pinging 2001:db8:acad:a::1 with 32 bytes of data:

Reply from 2001:DB8:ACAD:A::1: bytes=32 time=1ms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time<1ms TTL=255

Ping statistics for 2001:DB8:ACAD:A::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Figura 20 Ping desde PC-B a R1 G0/0/1.2 con ipv6 (Elaboración propia nov-2020)

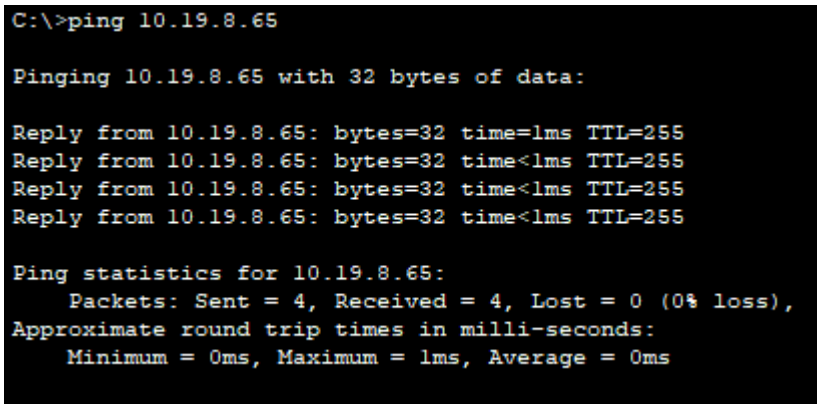


Figura 21 Ping de PC-B a R1 G0/0/1.3 ipv4 (Elaboración propia nov-2020)

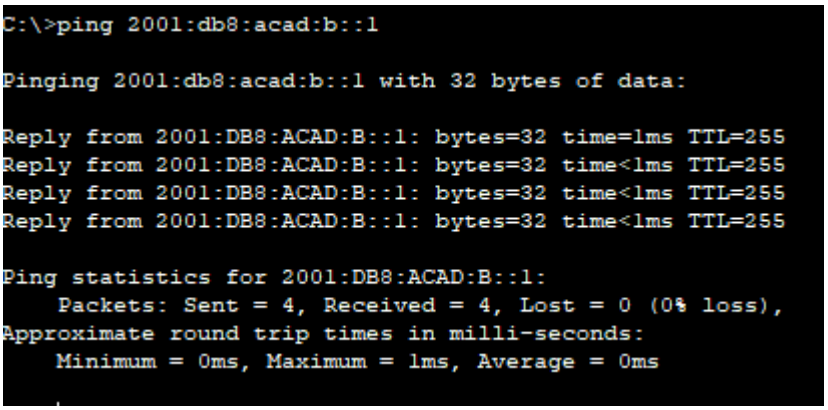


Figura 22 Ping de PC-B a R1 G0/0/1.3 ipv6 (Elaboración propia nov-2020)

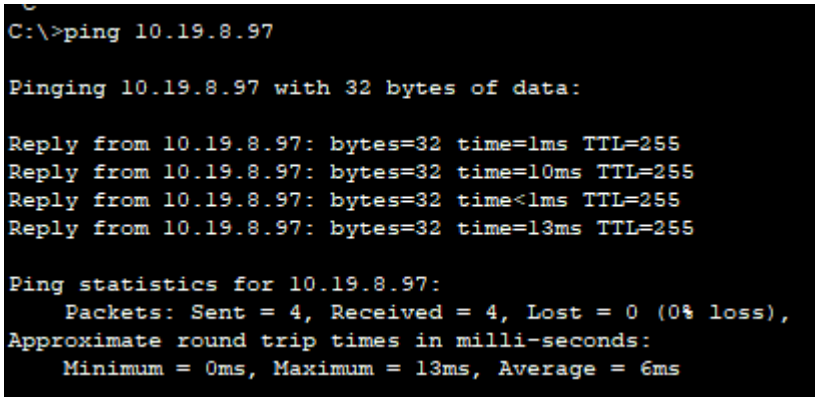


Figura 23 Ping de PC-B a R1 G0/0/1.4 ipv4 (Elaboración propia nov-2020)

```
C:\>ping 2001:db8:acad:c::1

Pinging 2001:db8:acad:c::1 with 32 bytes of data:

Reply from 2001:DB8:ACAD:C::1: bytes=32 time=20ms TTL=255
Reply from 2001:DB8:ACAD:C::1: bytes=32 time=32ms TTL=255
Reply from 2001:DB8:ACAD:C::1: bytes=32 time=32ms TTL=255
Reply from 2001:DB8:ACAD:C::1: bytes=32 time<1ms TTL=255

Ping statistics for 2001:DB8:ACAD:C::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 32ms, Average = 21ms
```

Figura 24 Ping desde PC-B a R1 G0/0/1.4 con ipv6(Elaboración propia nov-2020)

```
C:\>ping 10.19.8.98

Pinging 10.19.8.98 with 32 bytes of data:

Reply from 10.19.8.98: bytes=32 time=11ms TTL=254
Reply from 10.19.8.98: bytes=32 time=13ms TTL=254
Reply from 10.19.8.98: bytes=32 time=14ms TTL=254
Reply from 10.19.8.98: bytes=32 time=17ms TTL=254

Ping statistics for 10.19.8.98:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 11ms, Maximum = 17ms, Average = 13ms
```

Figura 25 Ping desde PC-B a al S1 de la Vlan.4 ipv4 (Elaboración propia nov-2020)

```
C:\>ping 2001:db8:acad:c::98

Pinging 2001:db8:acad:c::98 with 32 bytes of data:

Reply from 2001:DB8:ACAD:C::98: bytes=32 time=22ms TTL=254
Reply from 2001:DB8:ACAD:C::98: bytes=32 time=11ms TTL=254
Reply from 2001:DB8:ACAD:C::98: bytes=32 time=28ms TTL=254
Reply from 2001:DB8:ACAD:C::98: bytes=32 time=23ms TTL=254

Ping statistics for 2001:DB8:ACAD:C::98:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 11ms, Maximum = 28ms, Average = 21ms
```

Figura 26 Ping desde PC-B a al S1 de la Vlan.4 ipv6(Elaboración propia nov-2020)

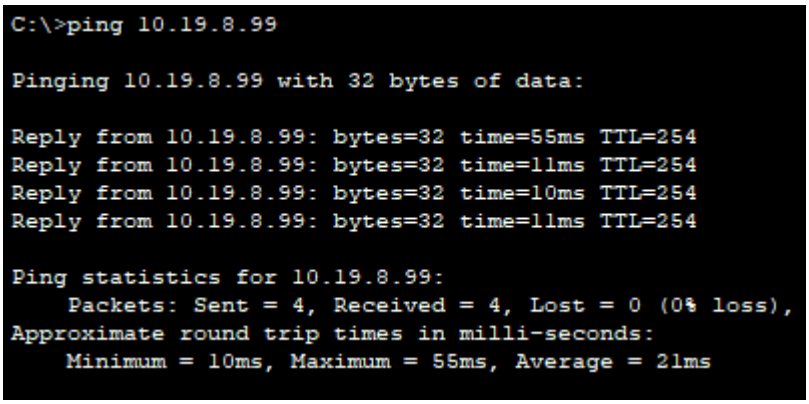


Figura 27 Ping de PC-B a S2 de la Vlan. 4 ipv4 (Elaboración propia nov-2020)

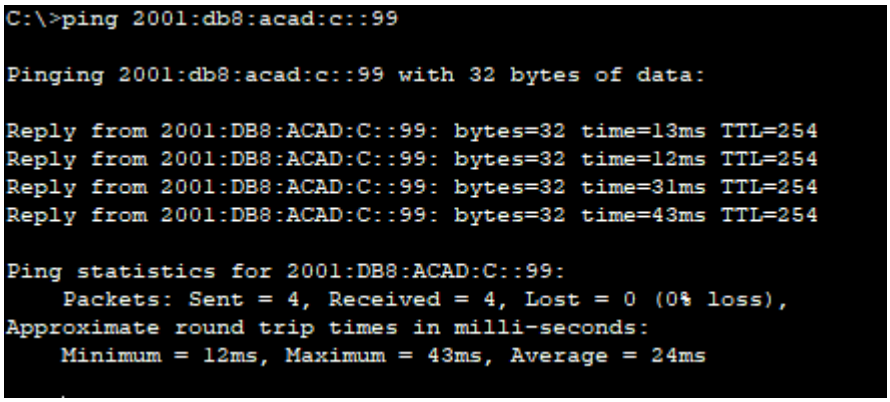


Figura 28 Ping desde PC-B a al S2 de la Vlan.4 ipv6 (Elaboración propia nov-2020)

2. Escenario 2:

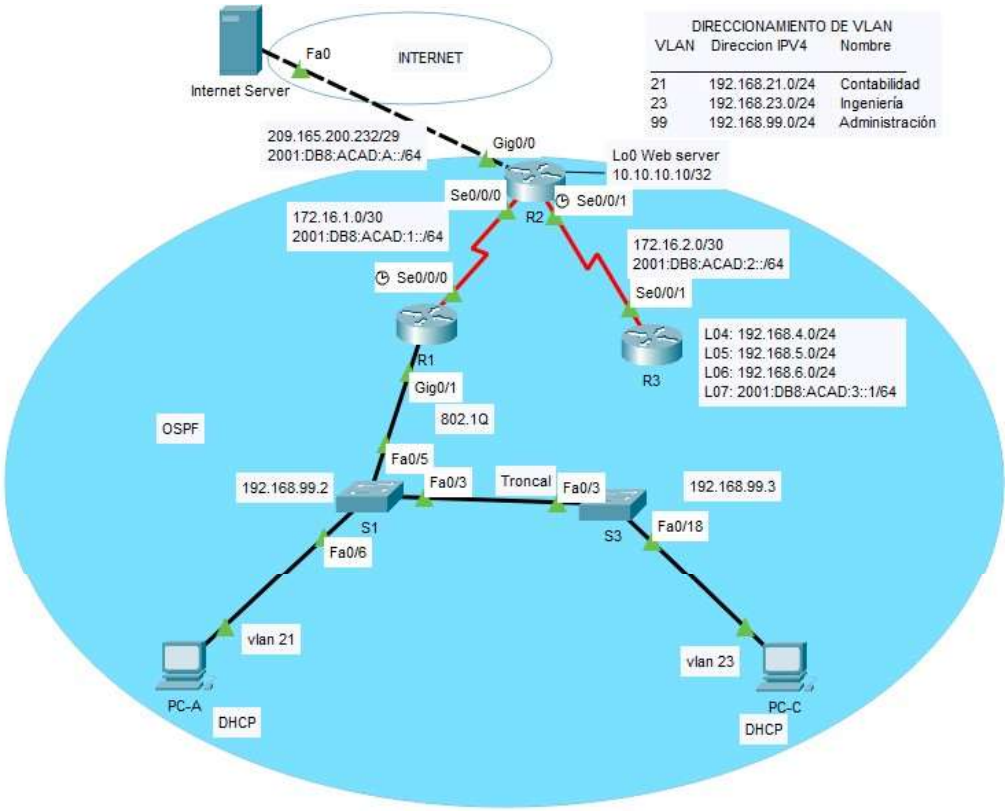


Figura 29 Escenario 2 (Elaboración propia nov-2020)

En la (figura 29) encontramos la topología que debemos implementar, teniendo en cuenta específicamente las conexiones señaladas y el direccionamiento IP.

2.1. Inicializar

2.1.1. Recargar los dispositivos

Tabla 9 Recargo de dispositivos

Tarea	Comando de IOS
Eliminamos el archivo de configuración de inicio startup-config de los Routers.	Router>enable Router#erase startup-config Erasing the nvram filesystem will remove all configuration files! Continue? [confirm] [OK]

Volver a cargar los routers	Router#reload Proceed with reload? [confirm]
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Switch>en Switch#erase startup-config Switch#delete vlan.dat
Recargar los switches	Switch#reload
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Switch# show flash

(Elaboración propia nov-2020)

2.2. Configuraciones iniciales de los dispositivos.

2.2.1. Configuración de servidor de Internet

Se realiza el subneteo teniendo en cuenta la dirección de subred 209.165.200.232/29; dada la máscara de la red se tiene que la primera dirección utilizable es la 209.165.200.233 (Será para el Gateway) y la última es la 209.165.200.238 que es la que se le asigna al servidor de internet.

Siendo la dirección 2001:DB8:ACAD:A::38/64 la IPV6 del servidor, entonces 2001:DB8:ACAD:A::1 debe ser su Gateway.

Se recomienda deshabilitar el firewall de las computadoras para que no haya interferencias en los ping de conexión.

Tabla 10 Direccionamiento Servidor de Internet

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.233
Dirección IPv6/subred	2001:DB8:ACAD:A::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:A::1

(Elaboración propia nov-2020)

2.2.2. Configuración del Router 1.

Las configuraciones básicas consisten en desactivar la búsqueda DNS, nombre, contraseña EXEC cifrada, contraseña a la consola, contraseña al TELNET en modo cifrado. Agregaremos un mensaje de inicio.

Pasamos a configurar la interface serial0/0/0, agregando una descripción, una IPv4 e IPv6, configuramos en este puerto la velocidad de reloj en 128000 para la conexión entre los dos Router mediante este puerto serial y activamos esta interface.

Establecemos las rutas predeterminadas para dirigir los paquetes a redes que no se encuentren en la tabla de direccionamiento.

Tabla 11 Configuración inicial R1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	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	R1(config)#line console 0 R1(config-line)#password cisco R1(config-line)#login
Contraseña de acceso Telnet	R1(config-line)#line vty 0 15 R1(config-line)#password cisco R1(config-line)#login
Cifrar las contraseñas de texto no cifrado	R1(config-line)#service password-encryption
Mensaje MOTD Se prohíbe el acceso no autorizado.	R1(config)#banner motd %Acceso no autorizado al R1%
Interfaz S0/0/0 Establezca la descripción Establecer la dirección IPv4 Establecer la dirección IPv6 Establecer la frecuencia de reloj en 128000 Activar la interfaz	R1(config)#int s0/0/0 R1(config-if)#description conexion con R2 R1(config-if)#ip address 172.16.1.1 255.255.255.252 R1(config-if)#ipv6 address 2001:db8:acad:1::1/64 R1(config-if)#clock rate 128000 R1(config-if)#no shutdown
Rutas predeterminadas en IPv4 e IPv6 para S0/0/0	R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0 R1(config)#ipv6 route ::/0 s0/0/0

(Elaboración propia nov-2020)

2.2.3. Configuración del Router 2.

Continuamos realizando las configuraciones iniciales esta vez para el R2, a diferencia de R1 aquí habilitamos la funcional de HTTP server, también configuramos la interface serial 0/0/0 con IPv4 e IPv6, la interface Serial 0/0/1, la GigabitEthernet0/0 y la interface Loopback 0 (servidor web simulado-interface para pruebas logicas). Para este caso, se habilita en el puerto S0/0/1 la velocidad del reloj a 1280000.

Establecemos las rutas predeterminadas para dirigir los paquetes a redes que no se encuentren en la tabla de direccionamiento.

Tabla 12 Configuración inicial en R2

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	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 R2(config-line)#password cisco R2(config-line)#login
Contraseña de acceso Telnet	R2(config-line)#line vty 0 15 R2(config-line)#password cisco 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
Mensaje MOTD	R2(config)#banner motd %Acceso no autorizado al R2%
Interfaz S0/0/0 Establezca la descripción Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. Establezca la dirección IPv6. Activar la interfaz	R2(config)#int s0/0/0 R2(config-if)#description conexion con R1 R2(config-if)#ip address 172.16.1.2 255.255.255.252 R2(config-if)#ipv6 address 2001:db8:acad:1::2/64 R2(config-if)#no shutdown
Interfaz S0/0/1 Establecer la descripción Establezca la dirección IPv4. Establezca la dirección IPv6.	R2(config)#int s0/0/1 R2(config-if)#description conexion con R3 R2(config-if)#ip address 172.16.2.2 255.255.255.252

Establecer la frecuencia de reloj en 128000. Activar la interfaz	R2(config-if)#ipv6 address 2001:db8:acad:2::2/64 R2(config-if)#clock rate 128000 R2(config-if)#no shutdown
Interfaz G0/0 (simulación de Internet) Establecer la descripción. Establezca la dirección IPv4. Establezca la dirección IPv6. Activar la interfaz	R2(config-if)#int g0/0 R2(config-if)#des R2(config-if)#description conexion a internet R2(config-if)#ip address 209.165.200.233 255.255.255.248 R2(config-if)#ipv6 address 2001:db8:acad:a::11/64 R2(config-if)#no shutdown
Interfaz loopback 0 Establecer la descripción. Establezca la dirección IPv4.	R2(config-if)#int loopback 0 R2(config-if)#ip address 10.10.10.10 255.255.255.255 R2(config-if)#description simulacion de servidor web
Ruta predeterminada en IPv4 e IPv6 de G0/0.	R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0 R2(config)#ipv6 route ::/0 g0/0

(Elaboración propia nov-2020)

2.2.4. Configuración del Router 3.

Continuamos realizando las configuraciones iniciales ahora para el R3; configuramos la interface serial 0/0/1 con IPv4 e IPv6 y la interface Loopback 4, 5 6 con IPv4 y la interface Loopback 7 con direccionamiento IPv6.

Configuramos las rutas predeterminadas en la interface S0/0/1.

Tabla 13 Configuración inicial R3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	Router(config)#Hostname R3
Contraseña de exec privilegiado cifrada	R2(config)#enable secret class

Contraseña de acceso a la consola	R3(config)#line console 0 R3(config-line)#password cisco R3(config-line)#login
Contraseña de acceso Telnet	R3(config-line)#line vty 0 15 R3(config-line)#password cisco R3(config-line)#login
Cifrar las contraseñas de texto no cifrado	R3(config-line)#service password-encryption
Mensaje MOTD	R3(config)#banner motd %Acceso no autorizado al R3%
Interfaz S0/0/1 Establecer la descripción Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. Establezca la dirección IPv6. Activar la interfaz	R3(config)#int s0/0/1 R3(config-if)#description conexion con R2 R3(config-if)#ip address 172.16.2.1 255.255.255.252 R3(config-if)#ipv6 address 2001:db8:acad:2::1/64 R3(config-if)#no shutdown
Interfaz loopback 4 Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.	R3(config-if)#int loopback 4 R3(config-if)#ip address 192.168.4.1 255.255.255.0
Interfaz loopback 5 Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.	R3(config-if)#int loopback 5 R3(config-if)#ip address 192.168.5.1 255.255.255.0
Interfaz loopback 6 Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.	R3(config-if)#int loopback 6 R3(config-if)#ip address 192.168.6.1 255.255.255.0
Interfaz loopback 7 Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones	R3(config-if)#int loopback 7 R3(config-if)#ipv6 address 2001:db8:acad:3::1/64
Rutas predeterminadas	R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1 R3(config)#ipv6 route ::/0 s0/0/1

(Elaboración propia nov-2020)

2.2.5. Configuración del Switch 1.

Realizamos configuraciones iniciales un tanto similares a los routers, configuraciones de seguridad, nombre, encriptar las contraseñas y mensajes de ingreso de mismo modo para S1 y S3.

Tabla 14 Configuración inicial S1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	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 S1(config-line)#password cisco S1(config-line)#login
Contraseña de acceso Telnet	S1(config-line)#line vty 0 15 S1(config-line)#password cisco S1(config-line)#login
Cifrar las contraseñas de texto no cifrado	S1(config-line)#service password-encryption
Mensaje MOTD	S1(config)#banner motd %Prohibido el acceso no autorizado a S1%

(Elaboración propia nov-2020)

2.2.6. Configuración del Switch 3.

Tabla 15 Configuración inicial S3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	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 S3(config-line)#password cisco S3(config-line)#login
Contraseña de acceso Telnet	S3(config-line)#line vty 0 15 S3(config-line)#password cisco S3(config-line)#login
Cifrar las contraseñas de texto no cifrado	S3(config-line)#service password-encryption

Mensaje MOTD	S3(config)#banner motd %Prohibido el acceso no autorizado a S3%

(Elaboración propia nov-2020)

2.2.7. Verificar conectividad.

Verificamos que exista una conexión desde R1 a R2, de R2 a R3 y del servidor de Internet a su puerta de enlace.

Tabla 16 Verificar conectividad

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	R1#ping 172.16.1.2	R1#ping 172.16.1.2 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 1/5/18 ms Figura 30 Ping R1-R2, S0/0/0 (Elaboración propia nov-2020)
R2	R3, S0/0/1	R2#ping 172.16.2.1	R2#ping 172.16.2.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 172.16.2.1, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 1/6/27 ms Figura 31 Ping R2-R3, S0/0/1(Elaboración propia nov-2020)
PC de Internet	Gateway predeterminado	ping 209.165.200.233	Packet Tracer SERVER Command Line 1.0 C:\>ping 209.165.200.233 Pinging 209.165.200.233 with 32 bytes of data: Reply from 209.165.200.233: bytes=32 time=25ms TTL=255 Reply from 209.165.200.233: bytes=32 time=19ms TTL=255 Reply from 209.165.200.233: bytes=32 time<1ms TTL=255 Reply from 209.165.200.233: bytes=32 time<1ms TTL=255 Ping statistics for 209.165.200.233: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 25ms, Average = 11ms Figura 32 Ping servidor internet - Gateway predeterminado (Elaboración propia nov-2020)

(Elaboración propia nov-2020)

2.3. Configurar la seguridad del switch, las Vlan y el Routing entre Vlan.

2.3.1. Configuración del Switch 1.

Creamos la base de datos de las VLANS y les asignamos un nombre según lo indicado en la (figura 29), asignando a la VLAN 99 la dirección 192.168.99.2 y activándola; Asignamos la primera dirección de la subred como Gateway y asignamos las interfaces F0/3 y f0/5 como enlaces troncales, dichos puertos se asignan a la VLAN 1. Las interfaces fa0/1-2, fa0/4, fa0/6-24, g0/1-2 se configuran como puertos de acceso, por último la interface fa0/6 se agrega a la VLAN 21 siendo este el puerto donde se conecta la PC-A y apagamos los puertos sin utilizar.

Tabla 17 Configuración S1

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN y nombrarlas	S1(config)#vlan 21 S1(config-vlan)#name Contabilidad S1(config-vlan)#vlan 23 S1(config-vlan)#name Ingenieria S1(config-vlan)#vlan 99 S1(config-vlan)#name Administracion
Asignación de la dirección IPv4 a la VLAN de administración.	S1(config)#int vlan 99 S1(config-if)#ip address 192.168.99.2 255.255.255.0 S1(config-if)#no shutdown
Asignación de la primera dirección IPv4 de la subred como el Gateway predeterminado.	S1(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3 Utilizar la red VLAN 1 como VLAN nativa	S1(config)#int f0/3 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1
Forzar el enlace troncal en la interfaz F0/5 Utilizar la red VLAN 1 como VLAN nativa	S1(config)#int f0/5 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1

Configurar el resto de los puertos como puertos de acceso Utilizar el comando interface range	S1(config-if-range)#int range fa0/1-2, fa0/4, fa0/6-24, g0/1-2 S1(config-if-range)#switchport mode access
Asignar F0/6 a la VLAN 21	S1(config-if-range)#int fa0/6 S1(config-if)#switchport access vlan 21
Apagar todos los puertos sin usar	S1(config-if)#int range fa0/1-2, fa0/4, fa0/7-24, g0/1-2 S1(config-if-range)#shutdown

(Elaboración propia nov-2020)

2.3.2. Configuración del Switch 3.

Creamos la base de datos de las VLANS asignando los nombres según lo indicado en la (figura 29), asignando a la VLAN 99 la dirección 192.168.99.3 y activándola; Asignamos la primera dirección de la subred como Gateway; asignamos la interfaz F0/3 como enlace troncal y este se agrega a la VLAN 1. Las interfaces fa0/1-2, fa0/4-24, g0/1-2 se configuran como puertos de acceso, por último la interface fa0/18 a la VLAN 23 siendo este el puerto donde se conecta la PC-B y apagamos los puertos sin utilizar.

Tabla 18 Configuración S3

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN Utilizar la tabla de equivalencias de VLAN para topología para crear cada una de las VLAN que se indican Dé nombre a cada VLAN.	S3(config)#vlan 21 S3(config-vlan)#name Contabilidad S3(config-vlan)#vlan 23 S3(config-vlan)#name Ingenieria S3(config-vlan)#vlan 99 S3(config-vlan)#name Administracion
Asigne la dirección IPv4 a la VLAN de administración.	S3(config-vlan)#exit S3(config)#int vlan 99 S3(config-if)#ip address 192.168.99.3 255.255.255.0 S3(config-if)#no shutdown
Asignar el gateway predeterminado.	S3(config)#ip default-gateway 192.168.99.1

Asignar la primera dirección IP en la subred como gateway predeterminado.	
Forzar el enlace troncal en la interfaz F0/3 Utilizar la red VLAN 1 como VLAN nativa	S3(config)#int fa0/3 S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso Utilizar el comando interface range	S3(config-if)#int range fa0/1-2, fa0/4-24, g0/1-2 S3(config-if-range)#switchport mode access
Asignar F0/18 a la VLAN 23	S3(config)#int fa0/18 S3(config-if)#switchport access vlan 23
Apagar todos los puertos sin usar	S3(config-if)#int range fa0/1-2, fa0/4-17, fa0/19-24, g0/1-2 S3(config-if-range)#sh S3(config-if-range)#shutdown

(Elaboración propia nov-2020)

2.3.3. Configuración del Router 1.

Para habilitar la encapsulación IEEE 802.1Q del tráfico en la subinterfaz G0/1 de las VLAN 21, 23 y 99 y le asignamos la primera dirección IPv4 disponible para cada caso. Por último se enciende la interface física.

Tabla 19 Configuración encapsulación R1

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1 Descripción: LAN de Contabilidad Asignar la VLAN 21	R1(config)#int g0/1.21 R1(config-subif)#description vlan 21 R1(config-subif)#encapsulation dot1Q 21 R1(config-subif)#ip address 192.168.21.1 255.255.255.0
Configurar la subinterfaz 802.1Q .23 en G0/1 Descripción: LAN de Ingeniería Asignar la VLAN 23	R1(config-subif)#int g0/1.23 R1(config-subif)#description vlan 23 R1(config-subif)#encapsulation dot1Q 23

Asignar la primera dirección disponible a esta interfaz	R1(config-subif)#ip address 192.168.23.1 255.255.255.0
Configurar la subinterfaz 802.1Q .99 en G0/1 Descripción: LAN de Administración Asignar la VLAN 99 Asignar la primera dirección disponible a esta interfaz	R1(config-subif)#int g0/1.99 R1(config-subif)#description vlan 99 R1(config-subif)#encapsulation dot1Q 99 R1(config-subif)#ip address 192.168.99.1 255.255.255.0
Activar la interfaz G0/1	R1(config-subif)#int g0/1 R1(config-if)#no shutdown

(Elaboración propia nov-2020)

2.3.4. Verificar conectividad.

Realizamos los ping desde los Switches a los Router 1 y 2 a las Vlan indicadas, ingresando al modo de comando CII desde la interface de cada Switch.

Tabla 20 Verificar conectividad de switch a router

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	S1#ping 192.168.99.1	S1#ping 192.168.99.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms Figura 33 Ping S1 a R1 Vlan 99 (Elaboración propia nov-2020)
S3	R1, dirección VLAN 99	S3#ping 192.168.99.1	S3#ping 192.168.99.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms *Figura 34 Ping S3 a R1 Vlan 99(Elaboración propia nov-2020)*

S1	R1, dirección VLAN 21	S1#ping 192.168.21.1	S1#ping 192.168.21.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.21.1, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/4/18 ms *Figura 35 Ping S1 a R1 Vlan 21(Elaboración propia nov-2020)*
S3	R1, dirección VLAN 23	S3#ping 192.168.23.1	S3#ping 192.168.23.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.23.1, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 2/15/23 ms *Figura 36 Ping S3 a R1 Vlan 23(Elaboración propia nov-2020)*

(Elaboración propia nov-2020)

2.4. Configurar el protocolo de Routing Dinámico OSPF

El Open Shortest Path First (OSPF), es un protocolo de red para elegir el camino más corto para enrutar los paquetes. La configuración en los tres routers consiste en agregar a cada uno las redes a las que están conectados, usando los Wildcards en lugar de la marcara de red; un ejemplo de wildcard es 0.0.0.255 el cual corresponde a la máscara 255.255.255.0.

Los Process ID va desde 1 hasta 65535 para este caso usamos 1 y el ID de área entre 0 y 4294967295, que para este caso se pide usar 0.

Se activan las interfaces pasivas como se indican en cada tabla, esto evitara las actualizaciones en la interface. Por ultimo de desactiva la sumarización automática

2.4.1. OSPF en Router 1

Tabla 21 OSPF R1

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R1(config)#router ospf 1

Anunciar las redes conectadas directamente Asigne todas las redes conectadas directamente.	R1(config-router)#network 172.16.1.0 0.0.0.3 area 0 R1(config-router)#network 192.168.21.0 0.0.0.255 area 0 R1(config-router)#network 192.168.23.0 0.0.0.255 area 0 R1(config-router)#network 192.168.99.0 0.0.0.255 area 0
Establecer todas las interfaces LAN como pasivas	R1(config-router)#passive-interface g0/1.21 R1(config-router)#passive-interface g0/1.23 R1(config-router)#passive-interface g0/1.99
Desactive la sumarización automática	R1(config-router)#no auto-summary

(Elaboración propia nov-2020)

2.4.2. OSPF en Router 2

Tabla 22 OSPF R2

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R2(config)#router ospf 1
Anunciar las redes conectadas directamente Nota: Omitir la red G0/0.	R2(config-router)#network 10.10.10.0 0.0.0.255 area 0 R2(config-router)#network 172.16.1.0 0.0.0.3 area 0 R2(config-router)#network 172.16.2.0 0.0.0.3 area 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

(Elaboración propia nov-2020)

2.4.3. OSPF en Router 3

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R3(config)#router ospf 1

Anunciar redes IPv4 conectadas directamente Ver las redes conectadas R3(config-router)#do show ip route connected	R3(config-router)# network 172.16.2.0 0.0.0.3 area 0 R3(config-router)#network 192.168.4.0 0.0.0.255 area 0 R3(config-router)#network 192.168.5.0 0.0.0.255 area 0 R3(config-router)#network 192.168.6.0 0.0.0.255 area 0
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	R3(config-router)#passive-interface loopback 4 R3(config-router)#passive-interface loopback 5 R3(config-router)#passive-interface loopback 6
Desactive la sumarización automática.	R3(config-router)#no auto-summary

(Elaboración propia nov-2020)

2.4.4. Verificar OSPF

Tabla 23 OSPF R3

Pregunta	Respuesta
¿Con qué comando se muestran la ID del proceso OSPF, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router?	R3# show ip protocols
¿Qué comando muestra solo las rutas OSPF?	R3# show ip route ospf
¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	R3#show running-config | section router ospf

(Elaboración propia nov-2020)

2.5. Implementar DHCP y NAT para IPv4

2.5.1. Configurar R1 como servidor DHCP para las VLAN 21 y VLAN 23.

En el R1 se realiza exclusión de direcciones para configuraciones estáticas en las VLAN 21 y VLAN 23; se crean un pool DHCP para cada caso asignando un nombre y dirección de servidor de dominio al igual que un nombre y un Gateway (La primera IP de la red en cada VLAN).

Tabla 24 R1 como server DHCP

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20 R1(R1(config)#ip dhcp pool Contabilidad
Crear un pool de DHCP para la VLAN 21. Nombre: ACCT Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado	R1(config)#ip dhcp pool ACCT R1(dhcp-config)#network 192.168.21.0 255.255.255.0 R1(dhcp-config)#default-router 192.168.21.1 R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com
Crear un pool de DHCP para la VLAN 23 Nombre: ENGNR Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado	R1(dhcp-config)#ip dhcp pool ENGNR R1(dhcp-config)#network 192.168.23.0 255.255.255.0 R1(dhcp-config)#default-router 192.168.23.1 R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com

(Elaboración propia nov-2020)

2.5.2. Configurar NAT estática y dinámica en R2.

Desde el modo de configuración global en R2 establecemos un usuario y contraseña para la base de datos local, habilitamos el servicio de servidor HTTP, quien para este caso desde el simulador no es soportado, como tampoco lo es el comando para establecer el uso de la base de datos para el servidor HTTP.

A la NAT estática se le crea asignando la dirección del web server, recordando que el rango de la IP esta entre la…233 a la…238, sin embargo ya hay unas IPs asignadas.

Observando la topología (*Ver figura 29*) verificamos cuales son las interfaces internas y externas para asignarlas a la NAT estática.

Configuramos las listas de acceso 1, permitiendo la traducción de las redes de Contabilidad y de Ingeniería en el R1 y la traducción de la loopback en R3 con las máscaras inversas.

Definimos el pool del conjunto de las direcciones públicas y la traducción de NAT dinámica.

Tabla 25 Configuración NAT R2

Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario Nombre de usuario: webuser Contraseña: cisco12345 Nivel de privilegio: 15	R2(config)#username webuser privilege 15 secret cisco12345
Habilitar el servicio del servidor HTTP	R2(config)#ip http server → no soportado por el simulador
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	R2(config)#ip http authentication local → no soportado por el simulador
Crear una NAT estática al servidor web. Dirección global interna: 209.165.200.237-234-236	R2(config)#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)#int g0/0 R2(config-if)#ip nat outside R2(config-if)#int s0/0/0 R2(config-if)#ip nat outside R2(config-if)#int s0/0/1 R2(config-if)#ip nat outside
Configurar la NAT dinámica dentro de una ACL privada Lista de acceso: 1 Permitir la traducción de las redes de Contabilidad y de Ingeniería en el R1 Permitir la traducción de un resumen de las redes LAN (loopback) en el R3	R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255
Defina el pool de direcciones IP públicas utilizables. Nombre del conjunto: INTERNET El conjunto de direcciones incluye:	R2(config)#ip nat pool INTERNET 209.165.200.233 209.165.200.236 netmask 255.255.255.248

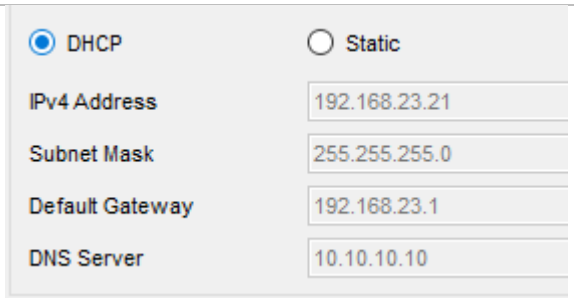
209.165.200.225 – 209.165.200.236	
Definir la traducción de NAT dinámica	R2(config)#ip nat inside source list 1 pool INTERNET

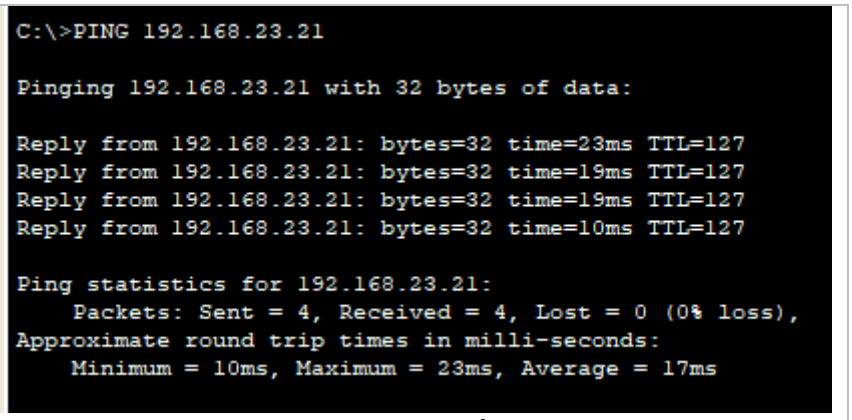
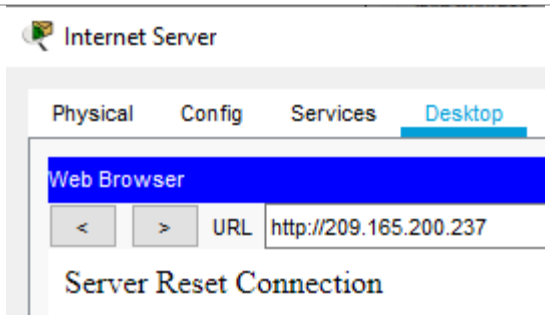
(Elaboración propia nov-2020)

2.5.3. Verificar el protocolo DHCP y la NAT estática.

Verificamos la configuración y conectividad según el caso que se presenta.

Tabla 26 Verificar protocolo DHCP y NAT

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	 Figura 37 Información DHCP PC-A (Elaboración propia nov-2020)
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	 Figura 38 Información DHCP PC-C (Elaboración propia nov-2020)

Verificar que la PC-A pueda hacer ping a la PC-C Nota: Quizá sea necesario deshabilitar el firewall de la PC.	 Figura 39Ping entre PC(Elaboración propia nov-2020)
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	 Figura 40 Ping al web server (Elaboración propia nov-2020) NO SOPORTADO POR EL SIMULADOR DE REDES

(Elaboración propia nov-2020)

2.5.4. onfigurar NAT.

Ajustamos las siguientes configuraciones como la hora del reloj en R2, El protocolo NTP permite que los dispositivos de red sincronicen la configuración de la hora con un servidor NTP; Para ello verificamos la configuración con el comando que se menciona desde la consola de R1, adicional con el comando *show ntp status,* encontramos información del estado de sincronización.

Tabla 27 Configuración del reloj y NTP

Elemento o tarea de configuración	Especificación

Ajuste la fecha y hora en R2.	R2#clock set 7:22:00 10 nov 2020
Configure R2 como un maestro NTP. Nivel de estrato: 5	R2(config)#ntp master 5
Configurar R1 como un cliente NTP. Servidor: R2	R1(config)#ntp server 172.16.1.2
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	R1(config)#ntp update-calendar R1(config)#end
Verifique la configuración de NTP en R1.	R1#show ntp associations address ref clock st when poll reach delay offset disp ~172.16.1.2 127.127.1.1 5 6 16 17 2.00 874046225632.00 0.12 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured R1# *Ilustración 1 Verificar configuración NTP en R1 (Elaboración propia nov-2020)*

(Elaboración propia nov-2020)

2.6. Configurar y verificar las listas de control de acceso ACL

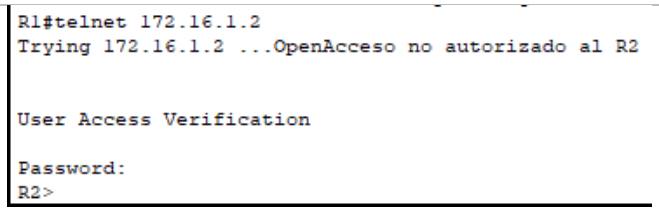
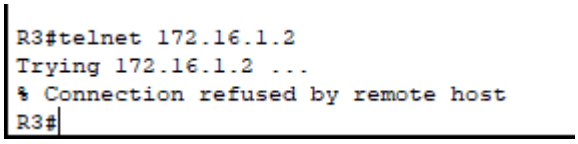
2.6.1. Restricción líneas VTY en R2.

Mediante la configuración siguiente, se establece el acceso exclusivo para que R1 establezca conexión con R2 mediante Telnet; creando una lista de acceso estándar con el nombre ADMIN-MGT con el permiso exclusivo.

Se configuran la ACL con un nombre de línea VTY permitiendo su acceso.

Por último se verifica la conexión realizando pruebas desde R1 y R3 donde se puede denotar que si se establece la conexión desde R1 hacia R2, pero no de R3 a R2.

Tabla 28 Configuración de lista de acceso

Elemento o tarea de configuración	Especificación
Configuración de lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2 Nombre de la ACL: ADMIN-MGT	R2(config)#ip access-list standard ADMIN-MGT R2(config-std-nacl)#permit host 172.16.1.2 R2(config-std-nacl)#exit
Aplicar la ACL con nombre a las líneas VTY	R2(config)#line vty 0 15 R2(config-line)#access-class ADMIN-MGT in
Permitir acceso por Telnet a las líneas de VTY	R2(config-line)#transport input telnet R2(config-line)#
Verificar que la ACL funcione como se espera Usando la contraseña cisco para el ingreso desde R1 ingreso a R2	 Figura 41 Telnet de R1 a R2 (Elaboración propia nov-2020)  Figura 42 Telnet de R3 a R2 (Elaboración propia nov-2020)

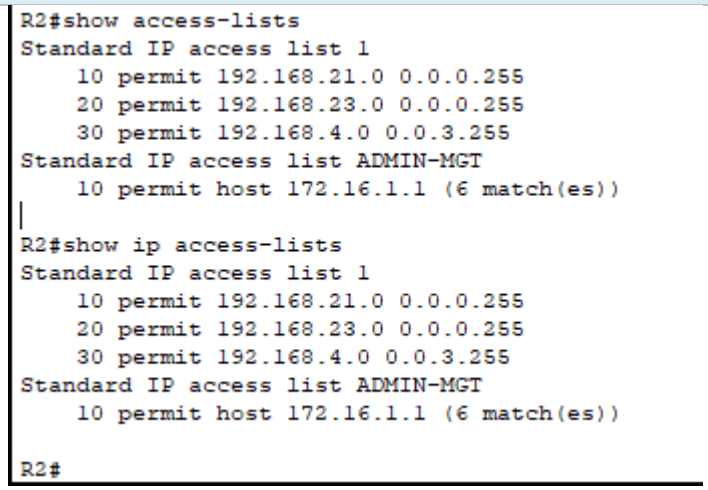
(Elaboración propia nov-2020)

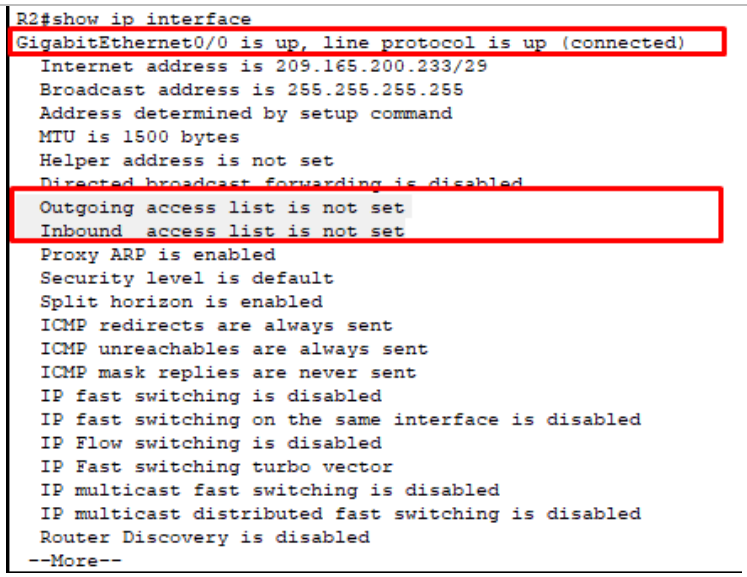
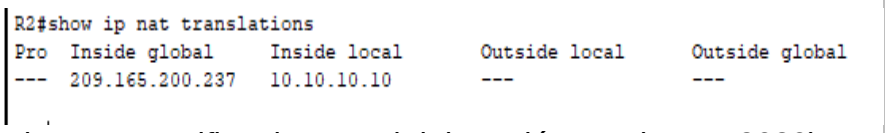
2.6.2. Comando CLI para verificar.

Se verifican las coincidencias de las listas de acceso desde la última vez que se restableció y podemos notar que hay seis coincidencias del puerto S0/0/0 del R1; posterior a ello restablecemos el contador de las listas de acceso.

Podemos verificar con el comando indicado en la tabla la interface donde se ha configurado la lista de acceso, también el comando con el que se verifican las traducciones NAT.

Tabla 29 Verificar la configuración ACL

Descripción del comando	Entrada del estudiante (comando)
Coincidencias recibidas por una lista de acceso desde el último reinicio.	 Figura 43 Verificar las ACL (Elaboración propia nov-2020)
Restablecer los contadores de una lista de acceso	R2#clear access-list counters

¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	 Figura 44 Verificar las interface de la ACL configurada (Elaboración propia nov-2020)
¿Con qué comando se muestran las traducciones NAT?	Nota: Las traducciones para la PC-A y la PC-C se agregaron a la tabla cuando la computadora de Internet intentó hacer ping a esos equipos en el paso 2. Si hace ping a la computadora de Internet desde la PC-A o la PC-C, no se agregarán las traducciones a la tabla debido al modo de simulación de Internet en la red.  Figura 45 Verificar las NAT(Elaboración propia nov-2020) Hacer ping al servidor web desde los pc y en el navegador.
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	R2#clear ip nat translation *

CONCLUSIONES

En el desarrollo del escenario uno, se creó una red con una topología básica sin embargo cuenta con implementaciones de seguridad y configuraciones un tanto robustas que garantizan su eficacia y desempeño. La conexión troncal entre los Switches esta implementada mediante la configuración Etherchanel LACP, el cual garantiza un acceso no interrumpido si alguna de las dos conexiones llegase a fallar; se realizó una configuración de seguridad de puerto en el switch que prevé acceso restringido para personas con equipos sospechosos o no autorizados.

Para el segundo escenario se realizan configuraciones de seguridad un tanto similares al primer escenario, sin embargo se implementa la conexión para un servidor web mediante una interface loopback y un servidor de internet según las indicaciones; entre los routers se establece una configuración de modo que permita el acceso a configuraciones remotas a los routers (en este caso solo se configuro el R2 para que pueda ser accedido desde R1 por una sola interface mediante una IP especifica) se realizan configuraciones como la implementación del servidor DHCP mediante uno de los routers.

BIBLIOGRAFÍA

Ariganello, E. (2016). *REDES CISCO. Guía de estudio para la certificación CCNA Routing y Switching. 4ª edición actualizada*. Grupo Editorial RA-MA.

Ariganello, E. (2010). Redes CISCO. CCNP a fondo. Guía de estudio para profesionales. Grupo Editorial RA-MA.

Ariganello, E. (2013). Redes cisco. Guía de estudio para la certificación CCNA security. Grupo Editorial RA-MA.

Arévalo Medina, E. F., & Bejarano Criollo, A. L. (2016). Evaluación de los protocolos IGP IPv4 e IPv6 soportados por el IOS de Cisco enfocado a la prestación del servicio IPTV en la ESPOCH (Bachelor's thesis, Escuela Superior Politécnica de Chimborazo).

Aprendaredes () Calculadora IP Recuperado de: https://aprendaredes.com/cgi-bin/ipcalc/ipcalc_cgi1

Barsotti Herrera, A., & Martelo Quiroz, M. Á. (2012). Configuración y optimización de switches administrables multicapa para garantizar tolerancia a fallas, escalabilidad y calidad en el servicio.

Boronat Segui, F. (2015). Configuración DHCP en routers CISCO.

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

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

Garcia Palacio, G. A. (2018). Aplicación de configuración básica en Routers, Switch y Servidores-Diplomado de profundización cisco (diseño e implementación de soluciones integradas LAN/WAN).

Kloth, R. (2001). U.S. Patent No. 6,208,649. Washington, DC: U.S. Patent and Trademark Office.

Saavedra, J. (2019) Diseño de Redes Modernas. Recuperado de: http://juancarlossaavedra.me/2019/06/diseno-de-redes-modernas/

Universitat politécnica de valencia () Calculadora IP. Recuperado de: http://labvirtual.webs.upv.es/ipcalc.html

Velte, T. J., & Velte, A. T. (2008). Manual de CISCO (No. 004.6 V4). McGraw-Hill Interamericana.

ANEXOS

ANEXO1

Enlace de descarga de archivos de simulación

https://drive.google.com/drive/folders/1jB2O-doBV_iM9nrBok39qBbqP3k9_B3k?usp=sharing

ANEXO 2

Artículo Científico IEEE

https://drive.google.com/drive/folders/14rfCdm-FVFU9aOcFUhcbEXRn6yPpAiTU?usp=sharing