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

OSCAR MAURICIO RIASCOS PUPIALES

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA –UNAD ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA –ECBTI
INGENIERIA DE SISTEMAS
PASTO
2020

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

OSCAR MAURICIO RIASCOS PUPIALES

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

DIRECTOR
PAULITA FLOR ZALASAR

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA – ECBTI
INGENIERIA DE SISTEMAS
PASTO
2020

NOTAS DE ACEPTACION

_____

_____

_____

_____

_____

_____

Firma de presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

SAN JUAN DE PASTO, 20 de octubre 2020

AGRADECIMIENTOS

En este punto culminante de alcanzar el titulo como Ingeniero de sistemas, no puedo ignorar el agradecimiento a todo aquello que me impulso, me levanto, me motivo y hizo posible alcanzar un sueño.

Dios fuente de sabiduria e inteligencia quien consede los dones y talentos para formar al hombre de tal manera que pueda superar los obstaculos y temores que se presentan en la peregrinacion del mundo. Es el quien dio la esperanza de que la felicidad puede ser el premio de una vida llena de sacrificio y dedicacion; a El la gracia de la obtencion de este titulo.

A mi madres Maria Helena de Riascos que gracias a su carisma de madre y docente, trasmitio la fe y los valores eticos y morales que el hombre debe de conoser y sentir para mantenenerse firme en la rectitud, responsabilidad y el respeto por los demas.
A mi padre Jose Rafael Riascos que esta en el cielo y que muy joven partio de este mundo, para convertirse en ese compañero silencioso en el dia y la noche.

A la segunda comunidad Neocatecumenal de Santiago Apostol que me invito a formar parte de la iglesia y que permanentemente oraron por mi para que fuera posibles renovar mi vida y espiritu.

A todos los docentes y formadores de la Universidad Abierta y Adistancia UNAD que participaron en este proceso de formacion, ya que gracias a su dedicacion y empeño, transmitieron su conocimiento con la intencion de brindarme las herramientas necesaria para ejercer una profesion al servicio de los demas.

INDICE GENERAL

LISTA DE TABLAS

LISTA DE FIGURAS

1. GLOSARIO

Host: Es un dispositivo anfitrión que se encargan de almacenar datos de tipo binario dentro de la funcionalidad de una red.

Ping: El ping es el tiempo de transmisión de paquetes a través de la red, entre dispositivos o host.

Show run (show running-config): comando de Reuters y switch que se encargan de dar un reporte o diagnostico del estado de configuración del dispositivo que se ejecuta en la RAM.

SDM templates: son plantillas creadas para los dispositivos CISCO para sacar el mejor rendimiento en cobertura y configuración de la red.

Gatewey: es la dirección de un dispositivo o host que cumple la función de enlace de comunicación con otra red diferente con protocolos de compatibilidad.

2. RESUMEN

El diplomado de profundización cisco (diseño e implementación de soluciones integradas lan / wan) plantea dos laboratorio o escenarios mediante gráficas, en donde se visualizan dos topologías diferentes de red. Están diseñadas para investigar y adquirir los conocimientos básicos sobre la configuración de los dispositivos que participan en una red, mediante el programa de simulación Packet Tracer. Esta interface agrupa diferentes tipos de dispositivos como Switch, routers, PC´s, servidores, cables, etc., con las diferentes características y configuraciones que se pueden encontrar en una topología real.

Los dispositivos de este entorno de laboratorio están diseñados para hacer las configuraciones necesarias de las topologías de red (Escenarios), en donde los resultados son expresados mediante la simulación del envió de archivos, pings entre equipos y visualización de páginas que demuestran el éxito de la configuración de red.

Palabras claves: *Topologías, Packet Tracer, interface, Red, Switch, Router*

3. ABSTRACT

The Cisco in-depth diploma (design and implementation of integrated lan / wan solutions) proposes two laboratories or scenarios using graphs, where two different network topologies are visualized. They are designed to investigate and acquire basic knowledge about the configuration of devices participating in a network, using the Packet Tracer simulation program. This interface groups different types of devices such as switches, routers, PCs, servers, cables, etc., with the different characteristics and configurations that can be found in a real topology.

The devices in this laboratory environment are designed to make the necessary configurations of the network topologies (Scenarios), where the results are expressed through the simulation of the sending of files, pings between equipment and display of pages that demonstrate the success of the Network Configuration.

Keywords: *Topologies, Packet Tracer, interface, Network, Switch, Router*

4. INTRODUCCION

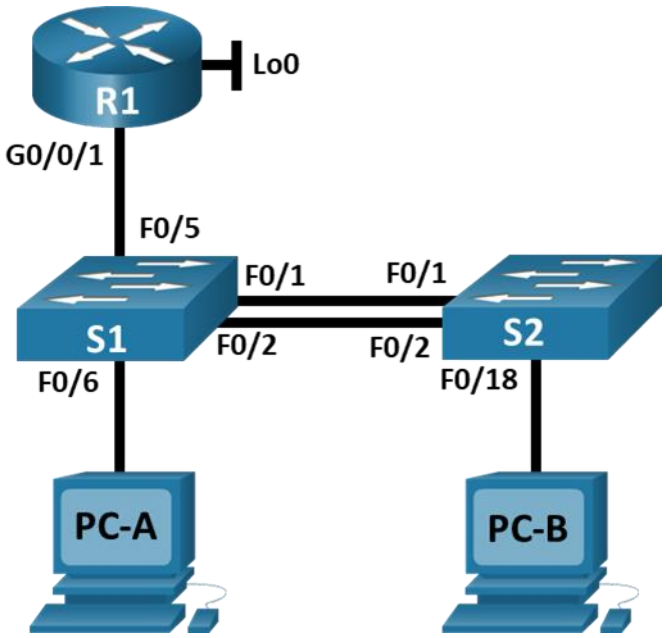
El diplomado de profundización CISCO está diseñado para alcanzar logros que fortalezcan los conocimientos para analizar, interpretar, diseñar, configurar y conectar Una red LAN /WAN en escenarios con diferentes características. Las redes están expresadas mediante topologías graficas en donde se identifican cada una de las partes principales que participan en una red de datos, como los medios de comunicación, clientes o host que hacen parte de receptores y transmisores de información, servidores etc., que forman parte del hardware y el software que se encarga de la funcionalidad y configuración de los dispositivos como el IOS, para que procesen la información y la compartan mediante las capas a través de protocolos.

Los dos escenario o topología de red está compuesto por switchs y un routers, los cuales están configurados con las características básicas que les permita ser identificados en la red como el hostname, las Vlan, password de seguridad, bloqueo de accesos etc., para que puedan estar en estados de conexión en el momento de la transmisión de datos mediante los medios de comunicación(cables). Además, cuenta con dos terminales (Host) que son los receptores y transmisores entre los canales y dispositivos que transmiten la información.

Para garantizar la correcta configuración de los dispositivos y funcionamiento de la red, se hacen pruebas de envío de paquetes desde los terminales (host) mediante comandos como Ping (proceso de latencia), en donde se estable la conexión correcta con cada interface; estas pruebas son realizadas en el programa de simulación de redes Packet Tracer en el entorno de laboratorio virtual de aprendizaje.

5. Ecsenario 1

Figura 1. Topología de red del escenario 1



En este primer escenario se configurarán los dispositivos de una red pequeña. Debe configurar un router, un switch y equipos que admitan tanto la conectividad IPv4 como IPv6 para los hosts soportados. El router y el switch también deben administrarse de forma segura. Configurará el enrutamiento entre VLAN, DHCP, Etherchannel y port-security.

Figura 2. Simulación del escenario 1

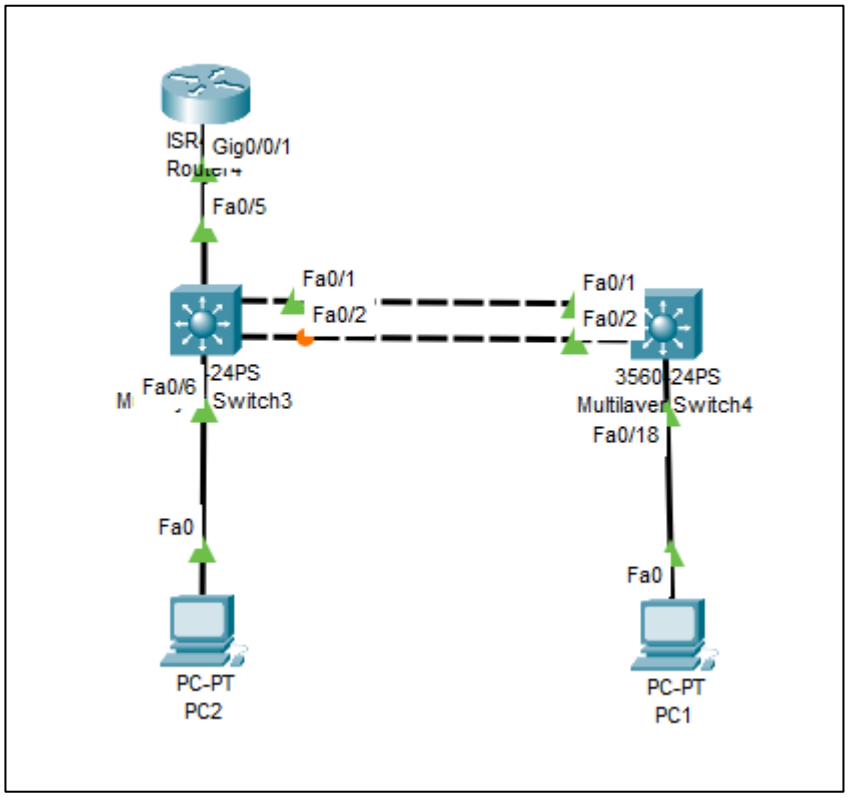


Tabla 1. Asignación de Nombres de VLAN

VLAN	Nombre de la VLAN
2	Bikes
3	Trikes
4	Management
5	Parking
6	Native

Las VLAN de la configuración de la red están asignadas con un nombre especifico

Tabla 2. Asignación de direcciones de los dispositivos

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
R1 G0/0/1.2	10.19.8.1 /26	No corresponde
	2001:db8:acad:a: :1 /64	No corresponde
R1 G0/0/1.3	10.19.8.65 /27	No corresponde
	2001:db8:acad:b: :1 /64	No corresponde
R1 G0/0/1.4	10.19.8.97 /29	No corresponde
	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
	2001:db8:acad:209: :1 /64	No corresponde
S1 VLAN 4	10.19.8.98 /29	10.19.8.97
	2001:db8:acad:c: :98 /64	No corresponde
	fe80: :98	No corresponde
S2 VLAN 4	10.19.8.99 /29	10.19.8.97
	2001:db8:acad:c: :99 /64	No corresponde
	fe80: :99	No corresponde
PC-A NIC	Dirección DHCP para IPv4	DHCP para puerta de enlace predeterminada IPv4
	2001:db8:acad:a: :50 /64	fe80::1
PC-B NIC	DHCP para dirección IPv4	DHCP para puerta de enlace predeterminada IPv4
	2001:db8:acad:b: :50 /64	fe80::1

Los dispositivos e interfaces están identificados mediante direccionamiento Ipv4 e Ipv6 cada uno con las puertas de enlace necesarias para el funcionamiento de la topología de red

6. Inicializar y Recargar y Configurar aspectos basicos de los dispositivos

6.1. Inicializar y volver a cargar el Router y el Switch

Para el diseño del primer escenario de red se contará con dos Switch 3560 capa 3, un router 1142 CISCO y dos terminales o host. Se debe de reiniciar el router y los dos Swtich para borrar la información de la NVRAM mediante el modo exe de usuario para evita problemas de configuración; en el proceso de reinicio los dispositivos cargaran el IOS que está instalado por defecto. El switch de 3560 de capa 3 no tiene activada las características de IPv6, lo que es necesario activar las características de la plantilla SDM (Switch Database Management) para activar las preferencias.

Borrar la información de NVRAM

Switch#erase startup-config
Switch#reload

Activar características SDM

Switch>enable
Switch#configure terminal
Switch(config)#sdm prefer dual-ipv4-and-ipv6 default
Switch(config)#exit
Switch#reload

7. Configuration de Router 1142 CISCO

El router esta diseñado para trabajar en el enrutamiento de los paquetes mediante los protocolos de capa. Esto hace que detecte y determine la ruta de destino mas adecuado para encaminarlo en los enlaces establecidos.

7.1. Desactivar la busqueda de DNS

La busqueda de DNS esta activada por defecto en el enrutador; es necesario que se desactive esta busqueda desde el modo exe privilegiado para que no se desactive el teclado y se hebite la perdida de tiempo en los procesos de configuracion.

```
Router>enable
Router#configure terminal
Router(config)#no ip domain-lookup
```

7.2. Configuracion de nombre de dominio y seguridad

Para organizar la admnistracion de la red es necesario asignarle al router un nombre en la topologia de red, nombre de dominio para identificarlo en el internet y configurar la seguridad con la que el admnistrador ingresara desde el exe de usuario y configuracion global.Es necesario configurar una longitud minima en la contraseña como requisito para las credenciales de usuario.

```
Router(config)#hostname R1
R1(config)#ip domain-name ccna-lab.com
R1(config)#enable secret ciscoenpass
R1(config)#line console 0
R1(config-line)#password ciscoenpass
R1(config-line)#login
R1(config-line)#exit
R1(config)#security passwords min-length 10
```

7.3. Configuracion de acceso de Administrador local y remoto

Para tener acceso al enrutador local y remotamente se debe configura las lineas VTY puerto virtuales para habilitar las conexiones SSH(Secure Shell). Esta configuracion de protocolo permite encriptar las contraeñas de administradores para hebitar que terceras personas identifiquen el password. Ademas se otorga al administrador privilegios de configuracion de exe privilegiado, que le brinda tener acceso a toda los comandos de configuracion del router. Esta configuracion se la realiza desde exe privilegiado en donde cifrar las contraseñas de texto no cifrado por seguridad. Se configura un mensaje de prevencion (BANNER) en donde se informa que solo tiene acceso las personas encargadas de la administracion de la red; tambien se ejecuta un camando que guarda la configuracion del enrutador desde exe de usuario.

```
R1(config)#username admin privilege 15  secret Admin1pass
R1(config)#line vty 0 4
R1(config-line)#login local
R1(config-line)#exit
R1(config)#line vty 0 4
R1(config-line)#transport input ssh
R1(config-line)#service password-encryption
R1(config)#banner motd # ACCESO AUTORIZADO A PERSONAL ADM #
R1(config)#exit
R1#copy running-config startup-config
```

7.4. Habilitar el routing IPv6

Desde el modo exe privilegiado se debe configurar el router para enrutar paquetes de Ipv6, ya que los enrutadores bienen configuados predeterminadamente para IPv4.

R1(config)#ipv6 unicast-routing

7.5. Configurar interfaz G0/0/1 y subinterfaces

El router 1142 de CISCO utilza interfases fisicar Gigabit eternet 0/0/0 y 0/0/1. En este caso en la interface Gigabit eternet 0/0/1 se configuran subinterfaces identificadas como g0/0/1.2, g0/0/1.3, g0/0/1.4, g0/0/1.6 las cuales 3 de ellas tienen asignaciones de direcciones Ipv4 e Ipv6 con los correspondientes rangos de mascaras. A cada subinterface se configura el enlace truncal para hacer el enrutamiento de las subinterfaces y en el caso de Ipv6 se coloca la puerta de enlace predeterminada. Esta configuracion se Hace desde el modo exe privilegiado anexandole una descripcion de configuracion de la interface Gigabit eternet 0/0/1 y levantando el servicio de las interfaces con el comando no shutdown.

Configuracion interface y Subinterface

R1#configure terminal
R1(config)#interface gigabitEthernet 0/0/1
R1(config-if)#description " Configuracion de Interfaces y subinterfaces "
R1(config-if)#no shutdown
R1(config-if)#interfa 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)#ipv6 address FE80::1 link-local
R1(config-subif)#no shutdown
R1(config-subif)#exit
R1(config)#interfa 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)#no shutdown
R1(config-subif)#exit
R1(config)#interfa 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)#no shutdown
R1(config-subif)#exit
R1(config)#interfa g0/0/1.6
R1(config-subif)#no shutdown
R1(config-subif)# exit
```

7.6. Configure el Loopback0 interface

La configuracion de la interface virtual loopback0 sirve para la comprobacion TCP/IP; Esta interface se la configura desde el modo exe privilegiado en donde se le asigna una descipcion, una direccion Ipv4 con la correspondiente mascara, la direccion Ipv6 y la puerta de enlace

predeterminada; Tambien se le asigna un nombre de dominio con el que pueda ser identificado en el red de internet con la encriptacion mediante la clave de cifrado RSA.

```
R1#configure terminal
R1(config)#interface loopback 0
R1(config-if)#description " Configurar interfaz 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)#ipv6 address fe80::1 link-local
R1(config)#ip domain-name ccna-lab.com
R1(config)#crypto key generate rsa general-key modulus 1024
R1(config)#exit
```

8. Configuracion Switch 1 (3560 capa 3) CISCO

El switch 3560 de capa 3 CISCO cuenta con la version IOS Version 12.2(37)SE1, RELEASE SOFTWARE (fc1), en donde se relizaran las configuraciones pertinentes según la topoligia de red. Este dispositvo se encarga de establecer la conexión con el host creando una red LAN o local.

8.1. Desactivar la busqueda de DNS

La busqueda de DNS esta activada por defecto en el conmutador; es necesario que se desactive esta busqueda desde el modo exe privilegiado para que no se desactive el teclado y se hebite la perdida de tiempo en los procesos de configuracion.

Switch>enable
Switch#configure terminal
Switch(config)#no ip domain-lookup

8.2. Configuracion de nombre de dominio y seguridad

Para organizar la admnistracion de la red es necesario asignarle al switch un nombre en la topologia de red, nombre de dominio para ser identificado por el router y configurar la seguridad con la que el admnistrador ingresara desde el exe de usuario y configuracion global.Es necesario configurar una longitud minima en la contraseña como requisito para las credenciales de usuario.

Switch>enable
Switch#configure terminal
Switch(config)#hostname S1
S1(config)#ip domain-name ccna-lab.com
S1(config)#enable secret ciscoenpass
S1(config)#line console 0
S1(config-line)#password ciscoenpass
S1(config-line)#login
S1(config)#username admin privilege 15 secret admin1pass
S1(config-line)#exit

8.3. Configuracion de acceso de Administrador local y remoto

Para tener acceso al conmutador local y remotamente se debe configura las lineas VTY puerto virtuales para habilitar las conexiones SSH(Secure Shell). Esta configuracion de protocolo permite encriptar las contraeñas de administradores para hebitar que terceras personas identifiquen el

password. Ademas se otorga al administrador privilegios de configuracion de exe privilegiado, que le brinda tener acceso a toda los comandos de configuracion del switch 1. Esta configuracion se la realiza desde exe privilegiado en donde cifrar las contraseñas de texto no cifrado por seguridad. Se configura un mensaje de prevencion (BANNER) en donde se informa que solo tiene acceso las personas encargadas de la administracion de la red; tambien se ejecuta un camando que guarda la configuracion del enrutador desde exe de usuario.

```
Switch#configure terminal
S1(config)#line vty 0 4
S1(config-line)#login local
S1(config-line)#exit
S1(config)#line vty 0 4
S1(config-line)#transport input ssh
S1(config-line)#service password-encryption
S1(config)#banner motd # ACCESO AUTORIZADOA A PERSONAL ADM A
S1 #
S1(config)#crypto key generate rsa general-key modulus 1024
S1(config)#exit
S1#copy running-config startup-config
S1#
```

8.4. Configurar la interfaz de administración (SVI)

En el switch 1 se configura el administrador SVI en la interface Vlan 4 como un enlace virtual, que es asia donde se dirigiran todos los paquetes de informacion de los puertos del switch asociados a esta vlan; en donde se le

asigna una Ipv4 con la correspondiente mascara y la Ipv6 con la puerta de enlace predetrminada.Mediante un comando se hace el levantamiento del enlace y se le asigna una direccion ip estatica como Gateway predeterminado desde la interface vlan 4. A todos estos procesos hay que eplicar el comando de guardar la informacion.

```
S1#configure terminal
S1#ip routing
S1(config)#interface vlan 4
S1(config-if)#ip address 10.19.8.98 255.255.255.248
S1(config-if)#no shutdown
S1(config-if)#end
S1#copy running-config startup-config
S1#
S1#configure terminal
S1(config)#interface vlan 4
S1(config-if)#ipv6 address fe80::98 link-local
S1(config-if)#ipv6 address 2001:db8:acad:c::98/64
S1(config-if)#no shutdown
S1(config-if)#exit
S1(config)#exit
S1#
S1#copy running-config startup-config
S1#
S1#configure terminal
S1(config)#interface vlan 4
S1(config-if)#ip default-gateway 10.19.8.97
```

S1(config)#exit

9. Configuracion Switch 2 (3560 capa 3) CISCO

El switch 3560 de capa 3 CISCO cuenta con la version IOS Version 12.2(37)SE1, RELEASE SOFTWARE (fc1), en donde se relizaran las configuraciones pertinentes según la topoligia de red. Este dispositvo se encarga de establecer la conexión con el host creando una red LAN o local.

9.1. Desactivar la busqueda de DNS

La busqueda de DNS esta activada por defecto en el conmutador; es necesario que se desactive esta busqueda desde el modo exe privilegiado para que no se desactive el teclado y se hebite la perdida de tiempo en los procesos de configuracion.

Switch>enable
Switch#configure terminal
Switch(config)#no ip domain-lookup

9.2. Configuracion de nombre de dominio y seguridad

Para organizar la admnistracion de la red es necesario asignarle al switch un nombre en la topologia de red, nombre de dominio para ser identificado por el router y configurar la seguridad con la que el admnistrador ingresara desde el exe de usuario y configuracion global.Es necesario configurar una longitud minima en la contraseña como requisito para las credenciales de usuario.

```
Switch>enable
Switch#configure terminal
Switch(config)#hostname S2
S2(config)#ip domain-name ccna-lab.com
S2(config)#enable secret ciscoenpass
S2(config)#line console 0
S2(config-line)#password ciscoenpass
S2(config-line)#login
S2(config)#username admin privilege 15  secret admin1pass
```

9.3. Configuracion de acceso de Administrador local y remoto

Para tener acceso al conmutador local y remotamente se debe configura las lineas VTY puerto virtuales para habilitar las conexiones SSH(Secure Shell). Esta configuracion de protocolo permite encriptar las contraeñas de administradores para hebitar que terceras personas identifiquen el password. Ademas se otorga al administrador privilegios de configuracion de exe privilegiado, que le brinda tener acceso a toda los comandos de configuracion del switch 2. Esta configuracion se la realiza desde exe privilegiado en donde cifrar las contraseñas de texto no cifrado por seguridad. Se configura un mensaje de prevencion (BANNER) en donde se informa que solo tiene acceso las personas encargadas de la administracion de la red; tambien se ejecuta un camando que guarda la configuracion del enrutador desde exe de usuario.

```
Switch>enable
Switch#configure terminal
S2(config)#line vty 0 4
```

S2(config-line)#login local
S2(config-line)#exit
S2(config)#line vty 0 4
S2(config-line)#transport input ssh
S2(config-line)#service password-encryption
S2(config)#banner motd # ACCESO AUTORIZADOA A PERSONAL ADM A S2 #
S2(config)#crypto key generate rsa general-key modulus 1024
S2(config)#exit
S2#copy running-config startup-config
S1#

9.4. Configurar la interfaz de administración (SVI)

En el switch 2 se configura el administrador SVI en la interface Vlan 4 como un enlace virtual, que es asia donde se dirigiran todos los paquetes de informacion de los puertos del switch asociados a esta vlan; en donde se le asigna una Ipv4 con la correspondiente mascara y la Ipv6 con la puerta de enlace predetrminada.Mediante un comando se hace el levantamiento del enlace y se le asigna una direccion ip estatica como Gateway predeterminado desde la interface vlan 4. A todos estos procesos hay que eplicar el comando de guardar la informacion.

S2#configure terminal
S2(config)#interface vlan 4
S2(config-if)#ip address 10.19.8.99 255.255.255.248
S2(config-if)#no shutdown
S2(config-if)#end

```
S2#copy running-config startup-config
S2#configure terminal
S2(config)#interface vlan 4
S2(config-if)#ipv6 address fe80::99 link-local
S2(config-if)#ipv6 address 2001:db8:acad:c::99/64
S2(config-if)#no shutdown
S2(config-if)#exit
S2(config)#exit
S2#copy running-config startup-config
S2#configure terminal
S2(config)#interface vlan 4
S2(config-if)#ip default-gateway 10.19.8.97
S2(config)# exit
```

10. Configuración de la infraestructura de red Switch 1 (VLAN, Trunking, EtherChannel)

10.1. Creacion de VLAN en Switch 1

Las VLAN son inlaces logicos de red por donde puede pasar paquetes de informacion de manera independiente dentro de una interface fisica. Los conmutadores o Switch estan diseñados para crear VLANS que les permita tener mas cobertura de host en una red LAN. En el Switch 1 se crean 5 vlan con un nombre que las identifique en la red LAN, desde el modo de ese privilegiado.

```
S1#configure terminal
S1(config)#vlan 4
S1(config-vlan)#name Management
S1(config-vlan)#end
S1#configure terminal
S1(config)#vlan 3
S1(config-vlan)#name Trikes
S1(config-vlan)#end
S1#configure terminal
S1(config)#vlan 2
S1(config-vlan)#name Bikes
S1(config-vlan)#end
S1#configure terminal
S1(config)#vlan 5
S1(config-vlan)#name Parking
S1(config-vlan)#end
S1#configure terminal
S1(config)#vlan 6
S1(config-vlan)#name Native
S1(config-vlan)#end
S1#
```

10.2. Crear troncos 802.1Q que utilicen la VLAN 6 nativa

El enlace tronca permite crear un tunel por el cual pueden pasar diferentes VLAN desde un punto a otro; los troncos 802.1Q utilizaran la VLAN 6 nativa para la conexión entre el enrutador 1 y enrutador 2, dando paso a las VLAN 2, 3, 4, 5 y 6 que fueron creadas con anterioridad. Esta configuracion esta

ligada a los puertos de enlace fisico fastEthernet 0/1 y fastEthernet 0/2. Tambien se crea un tronco 802.1Q con el puerto de enlace fisico fastEthernet 0/5 con la VLAN 6 para que se comunique con el router y funcione como un tunel de paso de VLANS de diferente tipo.

Troncos 802.1Q VLAN nativa fastEthernet 0/1 y fastEthernet 0/2

```
S1#configure terminal
S1(config)#interface range fastEthernet 0/1-2
S1(config-if-range)#switchport mode trunk
S1(config-if-range)#switchport trunk native vlan 6
S1(config-if-range)#switchport trunk allowed vlan 2,3,4,5,6
S1(config-if-range)# switchport trunk encapsulation dot1q
S1(config-if-range)#end
```

Troncos 802.1Q VLAN nativa fastEthernet 0/5

```
S1#configure terminal
S1(config)#interface range fastEthernet 0/5
S1(config-if-range)#switchport mode trunk
S1(config-if-range)#switchport trunk native vlan 6
S1(config-if-range)#switchport trunk allowed vlan 2,3,4,5,6
S1(config-if-range)# switchport trunk encapsulation dot1q
S1(config-if-range)#end
```

10.3. EtherChannel de Capa 2

Con la agrupacion de puertos fisicos entre dos dispositivos mediante EthernetChannel se garantiza el aumento de la transferencia de informacion. Los puertos de fastEthernet 0/1 y fastEthernet 0/2 entre los dos enrutadores, son configurados desde el modo exe privilegado en donde se aplica el protocolo LACP (Link Aggregation Control Protocol) y acresentar la velocidad.

```
S1#configure terminal
S1(config)#interface range fastEthernet 0/1-2
S1(config-if-range)#channel-protocol lacp
S1(config-if-range)#channel-group 2 mode active
S1(config-if-range)#exit
```

10.4. Acceso de host para VLAN

Los accesos de VLAN de host son equipos que estan conectados al enrutador en un puerto fisico y ademas esta asignado a un VLAN determinada. Mediante el modo privlegiado se puede acceder a la configuracion de este acceso; se debe aclarar que el modo acceso permite conectar una sola VLAN.

```
S1#configure terminal
S1(config)#interface fastEthernet 0/6
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 2
S1(config-if)#exit
```

10.5. Configurar la seguridad del puerto en los puertos de acceso

En el Switch 1 se brinda seguridad a los puertos de accesos, otorgando el acceso a 3 direcciones Mac que podran conectarse al enrutador. Este acceso es configurado desde el modo provilegiado asignandole el enlace de una VLAN.

```
S1#configure terminal
S1(config)#interface fastEthernet 0/10
S1(config-if)#switchport mode access
S1(config-if)#switchport port-security maximum 3
S1(config-if)#switchport port-security violation shutdown
S1(config-if)#switchport port-security mac-address 0001.422C.C5B3
S1(config-if)#switchport port-security mac-address 0001.C97B.6173
S1(config-if)#switchport port-security mac-address 0002.1671.8082
S1(config-if)#end
```

10.6. Asegure todas las interfaces no utilizadas

Desde el modo privilegiado se asegura las interfaces que no se estan utilizando, se le agrega un descripcion del estado de la interface, se establece un modo de acceso y se procede al apagado del puerto. Esta configuracion se la asigna a una VLAN determinada.

```
S1#configure terminal
S1(config)#interface range f0/3-4,f0/7-9,f0/11-24
S1(config-if-range)#switchport mode access
```

S1(config-if-range)#switchport access vlan 5
S1(config-if-range)#description " Asignacionde seguridad VLAN 5 "
S1(config-if-range)# shutdown
S1(config-if-range)#end

11. Configuración de la infraestructura de red Switch 1 (VLAN, Trunking, EtherChannel)

11.1. Creacion de VLAN en Switch 2

Las VLAN son inlaces logicos de red por donde puede pasar paquetes de informacion de manera independiente dentro de una interface fisica. Los conmutadores o Switch estan diseñados para crear VLANS que les permita tener mas cobertura de host en una red LAN. En el Switch 1 se crean 5 vlan con un nombre que las identifique en la red LAN, desde el modo de ese privilegiado.

S2#configure terminal
S2(config)#vlan 4
S2(config-vlan)#name Management
S2(config-vlan)#end
S2#configure terminal
S2(config)#vlan 2
S2(config-vlan)#name Bikes
S2(config-vlan)#end
S2# configure terminal
S2(config)#vlan 3

S2(config-vlan)#name Trikes
S2(config-vlan)#end
S2#configure terminal
S2(config)#vlan 5
S2(config-vlan)#name Parking
S2(config-vlan)#end
S2#configure terminal
S2(config)#vlan 6
S2(config-vlan)#name Native
S2(config-vlan)#end

11.2. Crear troncos 802.1Q que utilicen la VLAN 6 nativa

El enlace tronca permite crear un tunel por el cual pueden pasar diferentes VLAN desde un punto a otro; los troncos 802.1Q utilizaran la VLAN 6 nativa para la conexión entre el enrutador 1 y enrutador 2, dando paso a las VLAN 2, 3, 4, 5 y 6 que fueron creadas con anterioridad. Esta configuracion esta ligada a los puertos de enlace fisico fastEthernet 0/1 y fastEthernet 0/2.

S2#configure terminal
S2(config)#interface range fastEthernet 0/1-2
S2(config-if-range)#switchport mode trunk
S2(config-if-range)#switchport trunk native vlan 6
S2(config-if-range)#switchport trunk allowed vlan 2,3,4,5,6
S2(config-if-range)# switchport trunk encapsulation dot1q
S2(config-if-range)#end

11.3. EtherChannel de Capa 2

Con la agrupacion de puertos fisicos entre dos dispositivos mediante EthernetChannel se garantiza el aumento de la transferencia de informacion. Los puertos de fastEthernet 0/1 y fastEthernet 0/2 entre los dos enrutadores, son configurados desde el modo exe privilegado en donde se aplica el protocolo LACP (Link Aggregation Control Protocol) y acresentar la velocidad.

S2#configure terminal
S2(config)#interface range fastEthernet 0/1-2
S2(config-if-range)#channel-protocol lacp
S2(config-if-range)#channel-group 2 mode passive
S2(config-if-range)#exit

11.4. Acceso de host para VLAN

Los accesos de VLAN de host son equipos que estan conectados al enrutador en un puerto fisico y ademas esta asignado a un VLAN determinada. Mediante el modo privlegiado se puede acceder a la configuracion de este acceso; se debe aclarar que el modo acceso permite conectar una sola VLAN.

S2#configure ter
S2#configure terminal
S2(config)#interface fastEthernet 0/18
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 3
S2(config-if)#exit

11.5. Configurar la seguridad del puerto en los puertos de acceso

En el Switch 2 se brinda seguridad a los puertos de accesos, otorgando el acceso a 3 direcciones Mac que podran conectarse al enrutador. Este acceso es configurado desde el modo provilegiado asignandole el enlace de una VLAN.

```
S2#configure terminal
S2(config)#interface fastEthernet 0/10
S2(config-if)#switchport mode access
S2(config-if)#switchport port-security maximum 3
S2(config-if)#switchport port-security violation shutdown
S2(config-if)#switchport port-security mac-address 0001.422C.C5B3
S2(config-if)#switchport port-security mac-address 0001.C97B.6173
S2(config-if)#switchport port-security mac-address 0002.1671.8082
S2(config-if)#end
```

11.6. Asegure todas las interfaces no utilizadas

Desde el modo privilegiado se asegura las interfaces que no se estan utilizando, se le agrega un descripcion del estado de la interface, se establece un modo de acceso y se procede al apagado del puerto. Esta configuracion se la asigna a una VLAN determinada.

```
S2#configure terminal
S2(config)#interface range f0/3-9,f0/11-17,f0/19-24
S2(config-if-range)#switchport mode access
S2(config-if-range)#switchport access vlan 5
```

S2(config-if-range)#description " Asignacionde seguridad VLAN 5 "

S2(config-if-range)#end

S2#

12. Configurar soporte de host

12.1. Configure Default Routing en Router

Crear rutas predeterminadas para IPv4 e IPv6 que dirijan el tráfico a la interfaz

R1(config)#ip route 0.0.0.0 0.0.0.0 10.19.8.98
R1(config)#ip route 0.0.0.0 0.0.0.0 10.19.8.99

12.2. Configurar IPv4 DHCP para VLAN 2

Para este soporte de Host se cree un grupo DHCP para VLAN 2,.se asigna un nombre de dominio y se especifica la dirección de la puerta de enlace predeterminada como dirección de interfaz del router.

R1#
R1#configure terminal
R1(config)#ip dhcp pool vlan2
R1(dhcp-config)#network 10.19.1.0 255.255.255.0
R1(dhcp-config)#default-router 10.19.1.1
R1(dhcp-config)#exit
R1(config)#ip domain-name ccna-a.net
R1(dhcp-config)#dns-server 10.0.0.10
R1(dhcp-config)#exit
R1(config)#

12.3. Configurar IPv4 DHCP para VLAN 3

Para este soporte de Host se cree un grupo DHCP para VLAN 2,.se asigna un nombre de dominio y se especifica la dirección de la puerta de enlace predeterminada como dirección de interfaz del router.

```
R1#
R1#configure terminal
R1(config)#ip dhcp pool vlan3
R1(dhcp-config)#network 10.19.1.0 255.255.255.0
R1(dhcp-config)#default-router 10.19.1.1
R1(dhcp-config)#exit
R1(config)#ip domain-name ccna-a.net
R1(dhcp-config)#dns-server 10.0.0.10
R1(dhcp-config)#exit
R1(config)#
```

Se excluye las ip que se asignan la red para que no entre en conflicto los host.

```
R1#
R1#configure terminal
R1# ip dhcp excluded-address 10.19.1.1 10.19.1.99
```

13. Configuracion de PC de la red

El PC1 y el PC2 son configurados con una Ipv6 estatica y la puerta de enlace predeterminada para realizar las pruebas de conexión de la topologia de red, al configurar el DHCP del router se activan de manera automatica las IP dinamicas en cada PC.

Tabla 3. Informacion de la configuracion de red PC 1

Configuración de red de PC-A	
Descripción	
Dirección física	0001.632E.9D49
Dirección IP	169.254.232.83
Máscara de subred	255.255.0.0
Gateway predeterminado	0.0.0.0
Gateway predeterminado IPv6	0.0.0.0

El host 1 estan conectados a la red de manera dinamica y estatica mediante Ipv4 e Ipv6

Tabla 4. Informacion de la configuracion de red PC 2

Configuración de red de PC-A	
Descripción	
Dirección física	0040.0B11.9605
Dirección IP	169.254.150.5
Máscara de subred	255.255.0.0
Gateway predeterminado	0.0.0.0
Gateway predeterminado IPv6	0.0.0.0

El host 2 estan conectados a la red de manera dinamica y estatica mediante Ipv4 e Ipv6

14. Probar y verificar la conectividad de extremo a extremo

Figura 3. Ping a IP 10.19.8.1 PC1

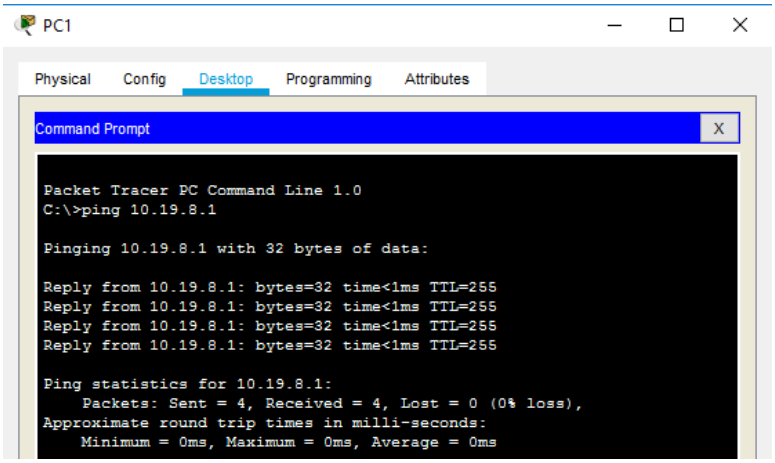


Figura 4. Ping a IP 10.19.8.65 PC1

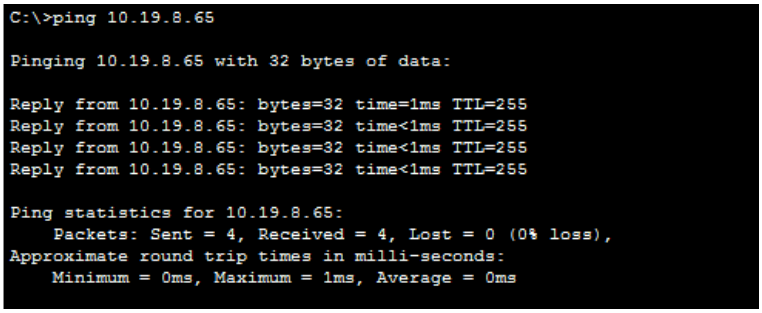


Figura 5. Ping a IP 10.19.8.97 PC1

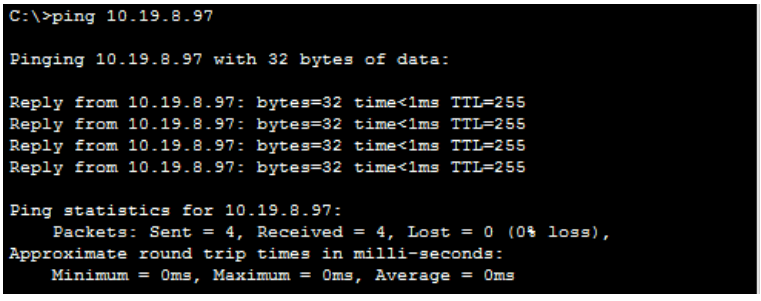


Figura 6. Ping a IPV6 2001:db8:acad:b: :50PC1

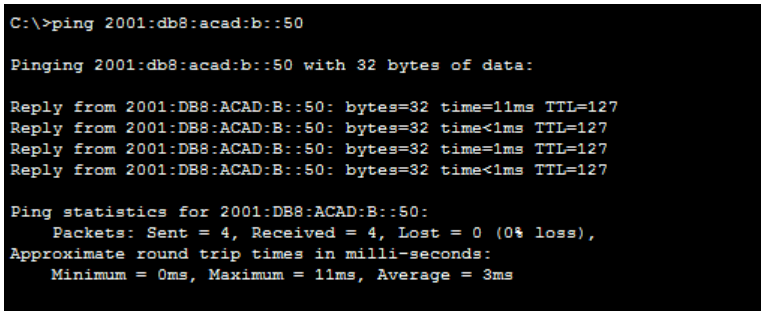


Figura 7. Ping a IP 10.19.8.97 PC1

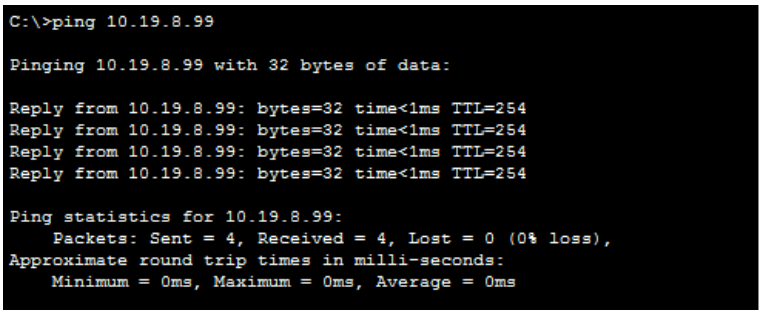


Figura 8. Ping a IP 209.165.201.1 PC1

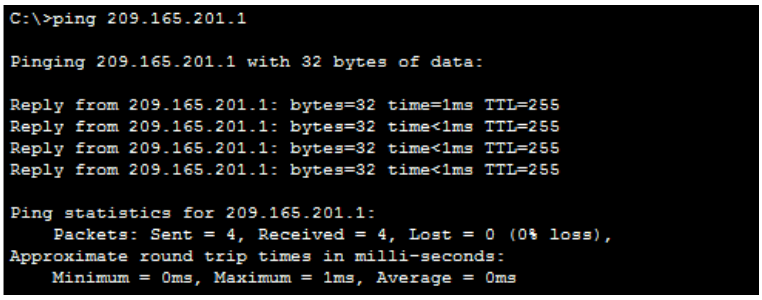


Figura 9. Ping a IPv6 2001:db8:acad:a: :1 PC1

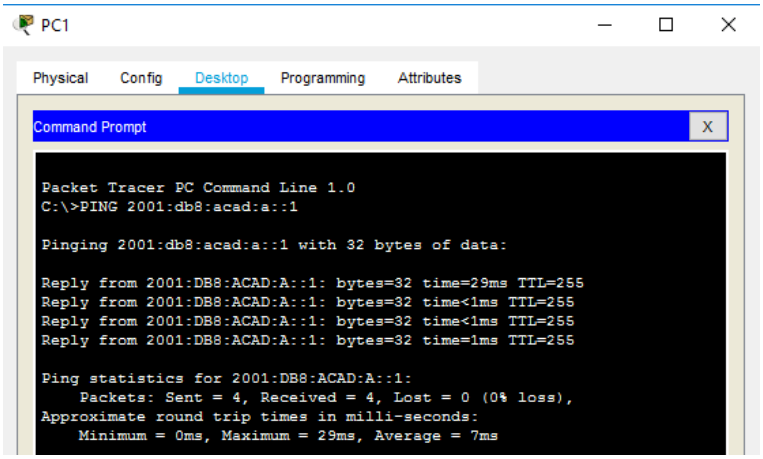


Figura 10. Ping a IPv6 2001:db8:acad:b: :1 PC1

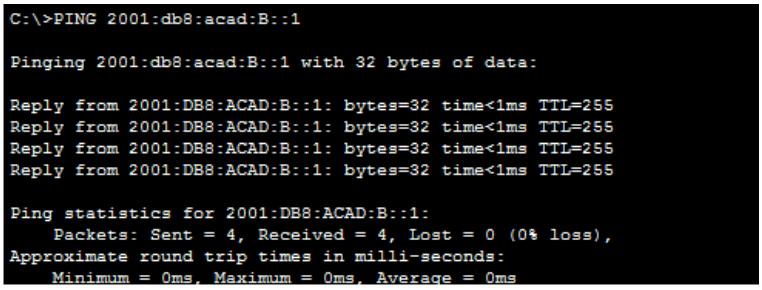


Figura 11. Ping a IPv6 2001:db8:acad:c: :1 PC1

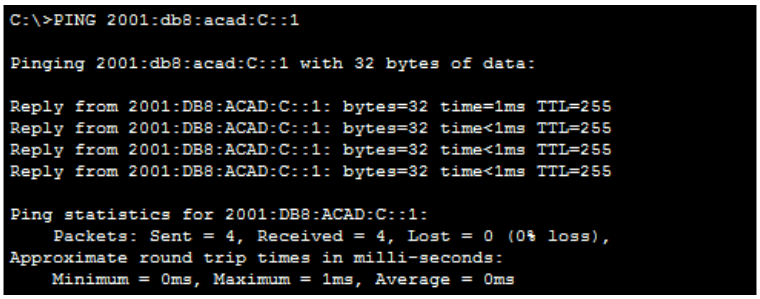


Figura 12. Ping a IPv6 2001:db8:acad:209: :1 PC1

```
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<1ms TTL=255
Reply from 2001:DB8:ACAD:209::1: bytes=32 time<1ms 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 = 1ms, Average = 0ms
```

Figura 13. Ping a IP 10.19.8.1 PC 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=1ms 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<1ms 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 = 1ms, Average = 0ms
```

Figura 14. Ping a IPv6 2001:db8:acad:b::50 PC 2

```
C:\>ping 2001:db8:acad:b::50

Pinging 2001:db8:acad:b::50 with 32 bytes of data:

Reply from 2001:DB8:ACAD:B::50: bytes=32 time=4ms TTL=128
Reply from 2001:DB8:ACAD:B::50: bytes=32 time=4ms TTL=128
Reply from 2001:DB8:ACAD:B::50: bytes=32 time=1ms TTL=128
Reply from 2001:DB8:ACAD:B::50: bytes=32 time=4ms TTL=128

Ping statistics for 2001:DB8:ACAD:B::50:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 4ms, Average = 3ms
```

Figura 15. Ping a IP 10.19.8.97 PC 2

```
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=1ms TTL=255
Reply from 10.19.8.97: bytes=32 time<1ms TTL=255
Reply from 10.19.8.97: bytes=32 time<1ms 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 = 1ms, Average = 0ms
```

Figura 16. Ping a IP 10.19.8.99 PC 2

```
C:\>ping 10.19.8.99

Pinging 10.19.8.99 with 32 bytes of data:

Reply from 10.19.8.99: bytes=32 time<1ms TTL=254
Reply from 10.19.8.99: bytes=32 time=1ms TTL=254
Reply from 10.19.8.99: bytes=32 time<1ms TTL=254
Reply from 10.19.8.99: bytes=32 time=7ms TTL=254

Ping statistics for 10.19.8.99:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 7ms, Average = 2ms
```

Figura 17. Ping a IP 209.165.201.1 PC 2

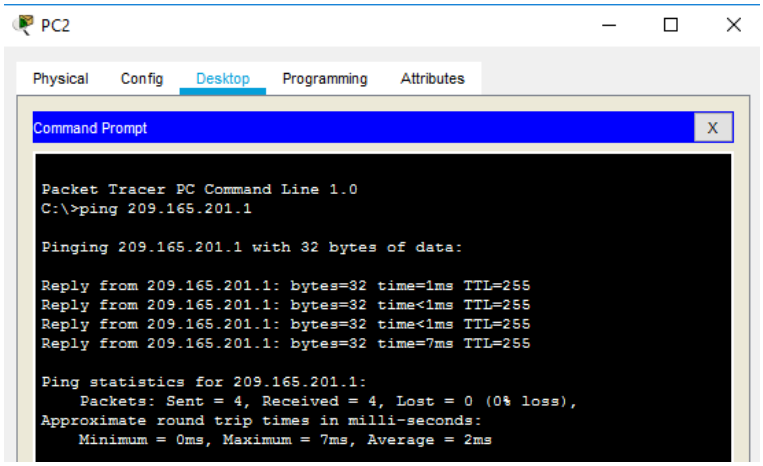


Figura 18. Ping a IPv6 2001:db8:acad:209::1 PC 2

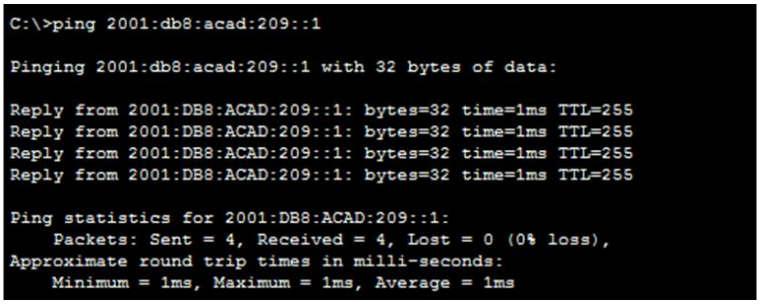


Figura 19. Ping a IPv6 2001:db8:acad:a::1 PC 2

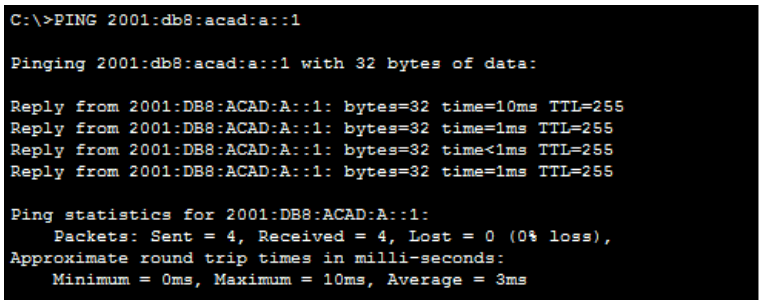


Figura 20. Ping a IPv6 2001:db8:acad:b::1 PC 2

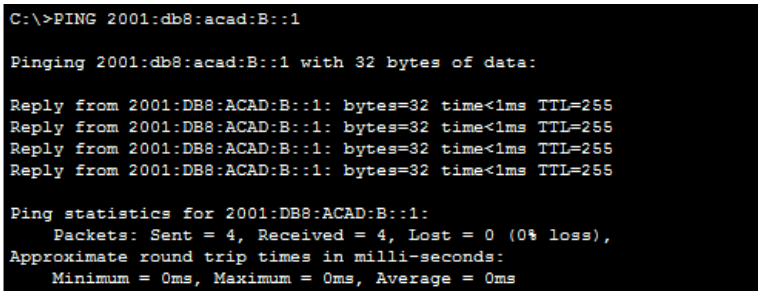


Figura 21. Ping a IPv6 2001:db8:acad:c::1 PC 2

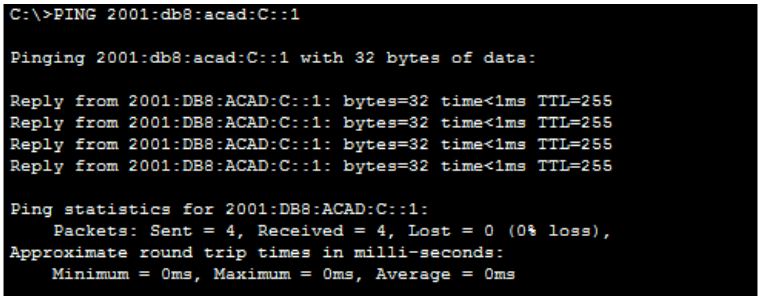


Figura 22. Ping a IP 209.165.201.1 PC 2

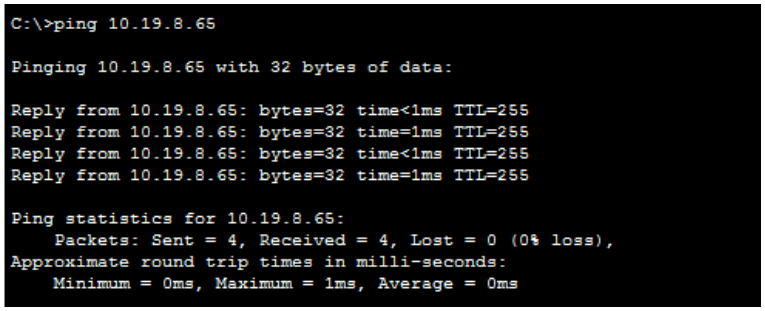
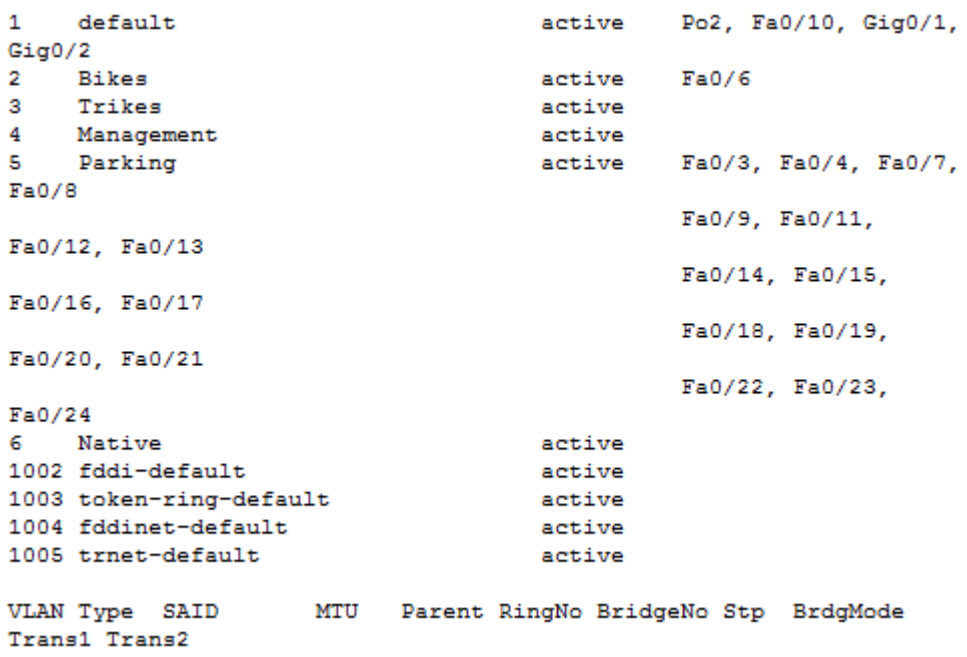
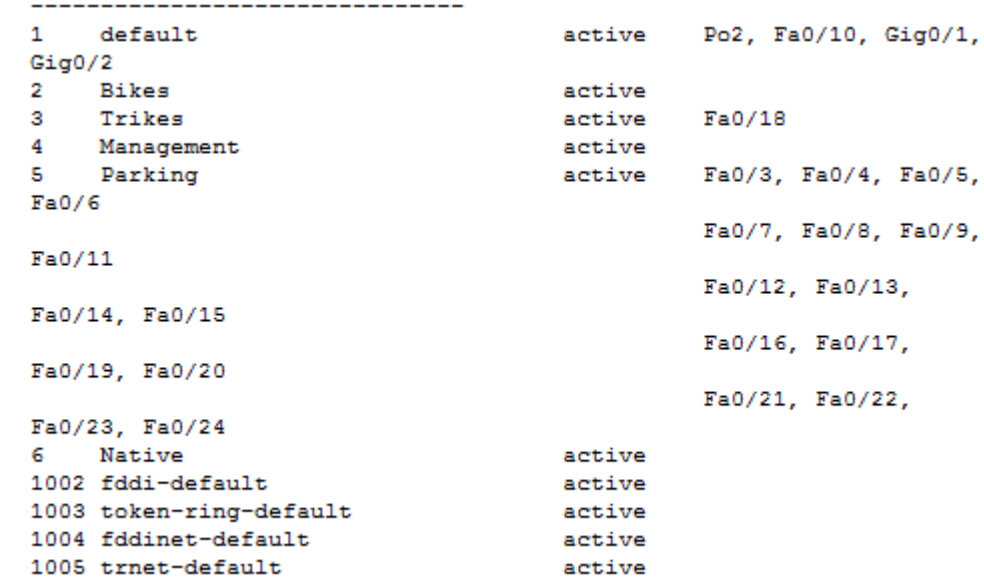


Figura 23. Vlans de Switch 1



```
------------------------------
1    default                          active    Po2, Fa0/10, Gig0/1,
Gig0/2
2    Bikes                            active    Fa0/6
3    Trikes                           active
4    Management                       active
5    Parking                          active    Fa0/3, Fa0/4, Fa0/7,
Fa0/8
                                                Fa0/9, Fa0/11,
Fa0/12, Fa0/13
                                                Fa0/14, Fa0/15,
Fa0/16, Fa0/17
                                                Fa0/18, Fa0/19,
Fa0/20, Fa0/21
                                                Fa0/22, Fa0/23,
Fa0/24
6    Native                           active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode
Trans1 Trans2
```

Figura 24. Vlans de Switch 2



```
------------------------------
1    default                          active    Po2, Fa0/10, Gig0/1,
Gig0/2
2    Bikes                            active
3    Trikes                           active    Fa0/18
4    Management                       active
5    Parking                          active    Fa0/3, Fa0/4, Fa0/5,
Fa0/6
                                                Fa0/7, Fa0/8, Fa0/9,
Fa0/11
                                                Fa0/12, Fa0/13,
Fa0/14, Fa0/15
                                                Fa0/16, Fa0/17,
Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22,
Fa0/23, Fa0/24
6    Native                           active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

Figura 25. EtherChannel de Capa 2 Switch 1

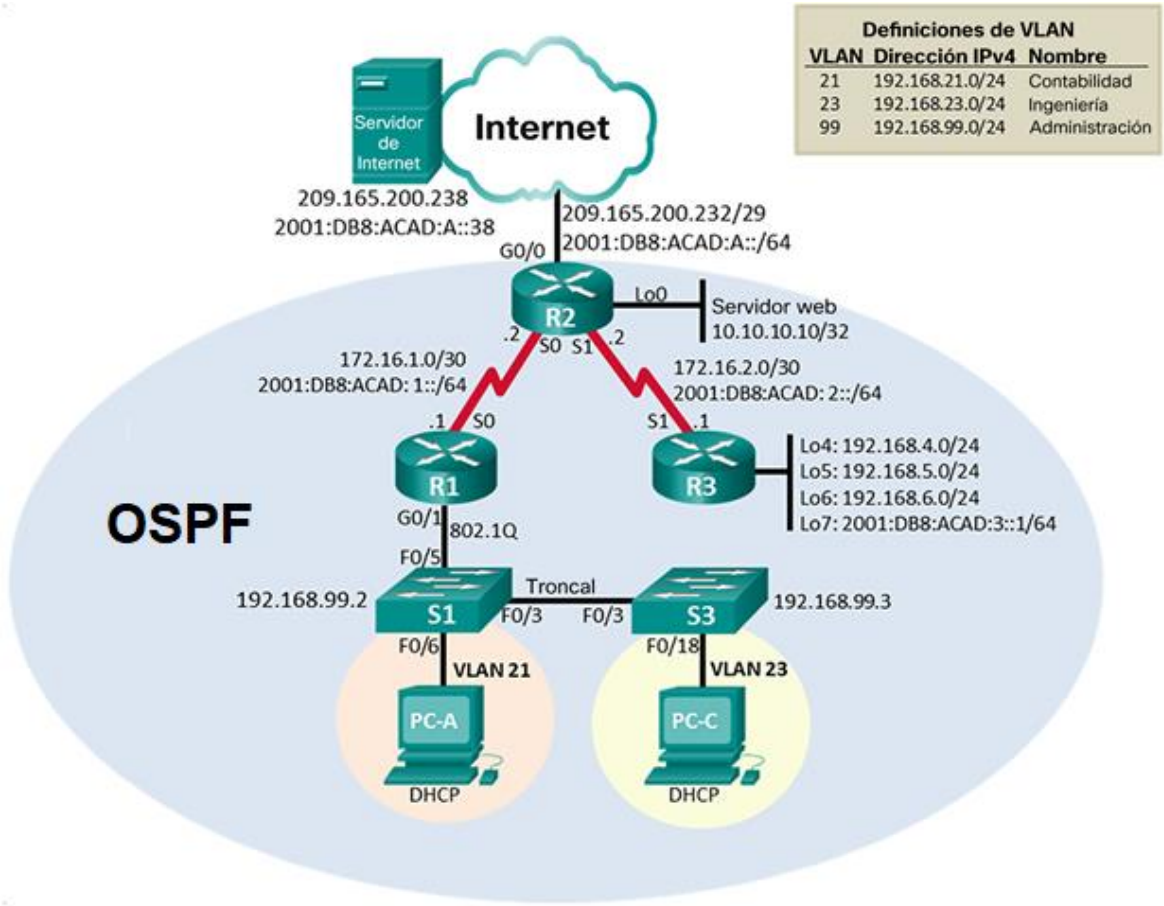
```
Access Mode VLAN: 6 (Native)

S1#show
S1#show et
S1#show etherchannel sum
S1#show etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------
+-----------------------------------------------

2      Po2(SD)           LACP   Fa0/1(I) Fa0/2(I)
S1#
```

Figura 26. EtherChannel de Capa 2 Switch 2

```
Password:
S2#sho
S2#show ter
S2#show eth
S2#show etherchannel summ
S2#show etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------
+-----------------------------------------------

2      Po2(SD)           LACP   Fa0/1(I) Fa0/2(I)
S2#
```

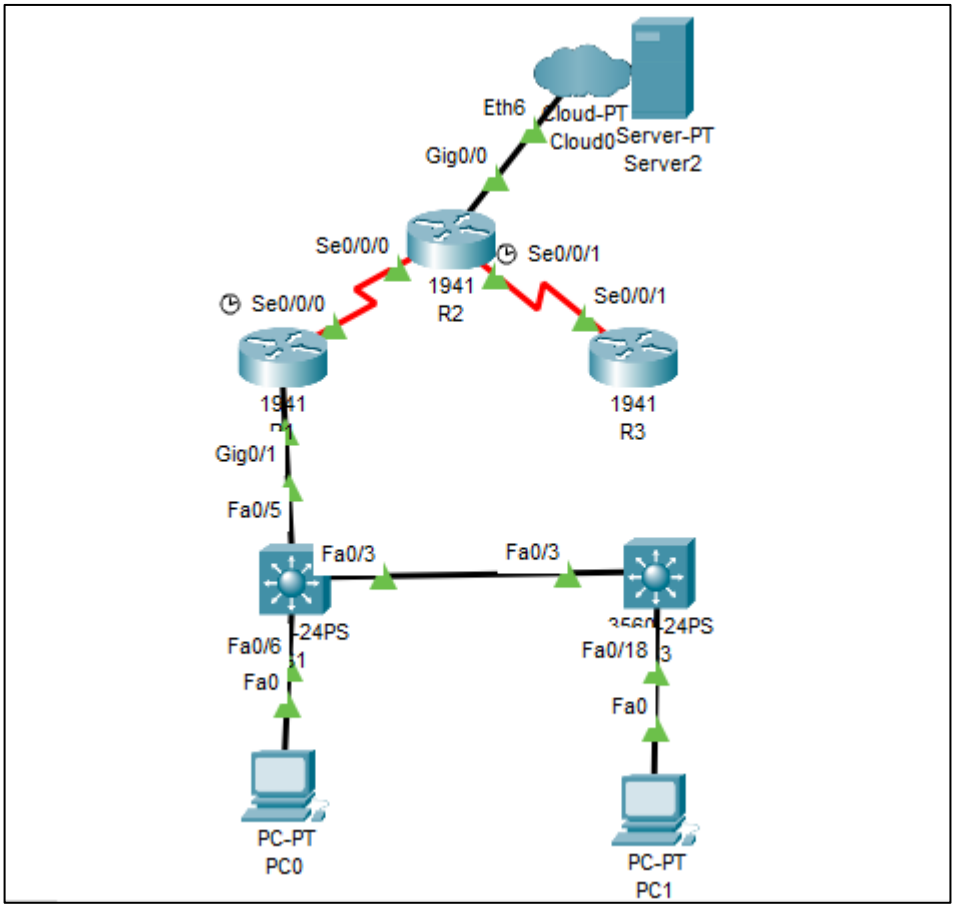
15. Ecsenario 2

Figura 27. Topología de red del escenario 2



Se debe configurar una red pequeña para que admita conectividad IPv4 e IPv6, seguridad de switches, routing entre VLAN, el protocolo de routing dinámico OSPF, 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.

Figura 28. Simulación del escenario 2



16. Inicializar y Recargar y Configurar aspectos basicos de los dispositivos

16.1. Inicializar y volver a cargar el Router y el Switch

Para el diseño del segundo escenario de red se contará con dos Switch 3560 capa 3, tres router 1142 CISCO, dos terminales o host, un clout-PT que hace las veces de nube y un servidor PT. Se debe de reiniciar los router y los dos Swtich para borrar la información de la NVRAM mediante el modo exe de usuario para evita problemas

de configuración; en el proceso de reinicio los dispositivos cargaran el IOS que está instalado por defecto.

Borrar la información de NVRAM en Switch

Switch#erase startup-config

Switch#reload

Borrar la información de NVRAM en Router

Router#erase startup-config

Router#reload

Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches

Switch#show flash

System flash directory:

File Length Name/status

3 8662192 c3560-advipservicesk9-mz.122-37.SE1.bin

2 28282 sigdef-category.xml

1 227537 sigdef-default.xml

[8918011 bytes used, 55098373 available, 64016384 total]

63488K bytes of processor board System flash (Read/Write)

17. Configurar los parámetros básicos de los dispositivos

17.1. Configurar la computadora de Internet

La configuracion del servidor de internet estan relacionadas en la siguiente

Tabla en donde se encuentra la informacion de la direccion ipv4 con su correspondiente mascara, la ipv6 con la subred y los gateway prefeterminados de los dos tipos de direcciones IP.

Tabla 5. Configuracion del 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	209.165.200.225
Dirección IPv6/subred	2001:D88:ACAD:A::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:2::1

La tabla cuenta con la informacion de las IP estaticas de equipo de servicio de internet

18. Configurar Router 1

Para organizar la admnistracion de la red es necesario desactivar la DNS en el enrutador, asignarle al router un nombre en la topologia de red, nombre de dominio para identificarlo en el internet y configurar la seguridad con la que el admnistrador ingresara desde el exe de usuario y configuracion global.

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname R1
R1(config)#enable secret class
```

R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit

18.1. Configuracion de acceso de Administrador local y remoto

Para tener acceso al enrutador local y remotamente se debe configura las lineas VTY puerto virtuales para habilitar las conexiones Telnet. Esta configuracion se la realiza desde exe privilegiado en donde se le asigna una contraseña y cifrar las contraseñas de texto no cifrado por seguridad. Se configura un mensaje de prevencion (BANNER) en donde se informa el acceso no autorizado a la administracion de la red.

R1(config)#line vty 0 4
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#service password-encryption
R1(config)#banner motd #Se prohibe el acceso no autorizado#

18.2. Configuracion de Interface

El router 1142 de CISCO utilza interfases fisicar Serial 0/0/0 y 0/0/1. En este caso en la interface Serial 0/0/0 en donde se establece una descripcion de configuracion, se les asigna las direcciones Ipv4 e Ipv6 con los correspondientes rangos de mascaras, estableciendo la frecuencia de reloj de la interface. Esta configuracion se hace desde el modo exe privilegiado y

levantando el servicio de las interfaces con el comando no shutdown; para luego hacer la grabacion de la configuracion.

```
R1>enable
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface serial 0/0/0
R1(config-if)#description CONFIGURACION ROUTER 1
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
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
R1(config-if)#exit
R1(config)#exit
R1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```

18.3. Rutas predeterminadas de interface

Se configura las rutas estaticas en la interface serial 0/0/0 desde el exe privilegiado, en los dos tipos de direcciones Ipv4 e Ipv6 para que almacene todos los paquetes en una sola ruta; se habilita el ruteo de ipv6 y no se configura todavia interface GigabitEternet 0/1

R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0
%Default route without gateway, if not a point-to-point interface, may impact performance
R1(config)#ipv6 route ::/0 s0/0/0
R1(config)#ipv6 Unicast-routing
R1(config)# exit

19. Configurar router 2

Para organizar la admnistracion de la red es necesario desactivar la DNS en el enrutador, asignarle al router un nombre en la topologia de red, nombre de dominio para identificarlo en el internet y configurar la seguridad con la que el admnistrador ingresara desde el exe de usuario y configuracion global.

Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname R2
R2(config)#enable secret class
R2(config)#line console 0
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#exit

19.1. Configuracion de acceso de Administrador local y remoto

Para tener acceso al enrutador local y remotamente se debe configura las lineas VTY puerto virtuales para habilitar las conexiones Telnet. Esta configuracion se la realiza desde exe privilegiado en donde se le asigna una contraseña y cifrar las contraseñas de texto no cifrado por seguridad. Se configura un mensaje de prevencion (BANNER) en donde se informa el acceso no autorizado a la administracion de la red.

```
R2(config)#line vty 0 4
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#exit
R2(config)#service password-encryption
R2(config)#banner motd #Se prohibe el acceso no autorizado#
```

19.2. Configuracion de Interface serial 0/0/0

En el router 1142 de CISCO se configura la interface fisicar Serial 0/0/0, en donde se establece una descripcion de configuracion, se les asigna las direcciones Ipv4 e Ipv6 con los correspondientes rangos de mascaras. Esta configuracion se hace desde el modo exe privilegiado y levantando el servicio de las interfaces con el comando no shutdown con el correspondiente comando de guardar la configuracion.

```
R2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#interface serial 0/0/0
R2(config-if)#description CONFIGURACION ROUTER 2
```

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

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
R2(config-if)#exit
R2#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R2#

19.3. Configuracion de Interface serial 0/0/1

En el router 1142 de CISCO se configura la interface fisicar Serial 0/0/1, en donde se establece una descripcion de configuracion, se les asigna las direcciones Ipv4 e Ipv6 con los correspondientes rangos de mascaras, estableciendo la frecuencia de reloj de la interface. Esta configuracion se hace desde el modo exe privilegiado y levantando el servicio de las interfaces con el comando no shutdown.

R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#interface serial 0/0/1
R2(config-if)#description CONFIGURACION R2
R2(config-if)#ip address 172.16.2.2 255.255.255.252
R2(config-if)#ipv6 address 2001:DB8:ACAD:2::2/64
R2(config-if)#clock rate 128000
R2(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
R2(config-if)#exit
R2#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R2#

19.4. Configuracion de Interface GigabitEternet 0/1

En el router 1142 de CISCO se configura la interface fisicar GigabitEternet 0/0, en donde se establece una descripcion de configuracion, se les asigna las direcciones Ipv4 e Ipv6 con los correspondientes rangos de mascaras. Esta configuracion se hace desde el modo exe privilegiado y levantando el servicio de las interfaces con el comando no shutdown con el correspondiente comando de guardar la configuracion.

R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#interface gigabitEthernet0/0
R2(config-if)#description CONFIGURACION R2 A INTERNET
R2(config-if)#ip address 209.165.200.232 255.255.255.0
R2(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64
R2(config-if)#no shutdown
R2(config-if)#exit
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up

R2#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R2#

19.5. Interfaz loopback 0 (servidor web simulado)

Se configura esta interface logica con una direccion ipv4 con la correspondiente mascara, colocandola en modo activo y una descripcion de configuracion.

R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#interface loopback 0

R2(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up

R2(config-if)#description " Configurar interfaz loopback 0 "
R2(config-if)#ip address 10.10.10.10 255.255.255.255
R2(config-if)#exit

19.6. Ruta predeterminada gigabitEthernet 0/0

Se configura las rutas estaticas en la interface gigabitEthernet 0/0, desde el exe privilegiado, en los dos tipos de direcciones Ipv4 e Ipv6 para que almacene todos los paquetes en una sola ruta.

R2(config)#ip route 0.0.0.0 0.0.0.0 gigabitEthernet 0/0
%Default route without gateway, if not a point-to-point interface, may impact performance
R2(config)#ipv6 route ::/0 gigabitEthernet 0/0
R2(config)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
R2(config)# exit

20. Configurar router 3

Para organizar la admnistracion de la red es necesario desactivar la DNS en el enrutador, asignarle al router un nombre en la topologia de red, nombre de dominio para identificarlo en el internet y configurar la seguridad con la que el admnistrador ingresara desde el exe de usuario y configuracion global**.**

Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname R3

R3(config)#enable secret class
R3(config)#line console 0
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#exit

20.1. Configuracion de acceso de Administrador local y remoto

Para tener acceso al enrutador local y remotamente se debe configura las lineas VTY puerto virtuales para habilitar las conexiones Telnet. Esta configuracion se la realiza desde exe privilegiado en donde se le asigna una contraseña y cifrar las contraseñas de texto no cifrado por seguridad. Se configura un mensaje de prevencion (BANNER) en donde se informa el acceso no autorizado a la administracion de la red y se digita el comando de guardar.

R3(config)#line vty 0 4
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#exit
R3(config)#service password-encryption
R3(config)#banner motd #Se prohibe el acceso no autorizado#exit
R3#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R3#

20.2. Configuracion de Interface serial 0/0/1

En el router 1142 de CISCO se configura la interface fisicar Serial 0/0/1, en donde se establece una descripcion de configuracion, se les asigna las direcciones Ipv4 e Ipv6 con los correspondientes rangos de mascaras. Esta configuracion se hace desde el modo exe privilegiado y levantando el servicio de las interfaces con el comando no shutdown con el correspondiente comando de guardar la configuracion.

```
R3#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#interface serial 0/0/1
R3(config-if)#description CONFIGURACION R3
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
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
R3(config-if)#exit
```

20.3. Interfaz loopback 4

Se configura esta interface logica con la primera direccion ipv4 de la subred con la correspondiente mascara y colocandola en modo activo.

```
R3(config)#interface loopback 4
R3(config-if)#
%LINK-5-CHANGED: Interface Loopback4, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback4, changed state to up
```

R3(config-if)#ip address 192.168.4.1 255.255.255.0
R3(config-if)#exit

20.4. Interfaz loopback 5

Se configura esta interface logica con la primera direccion ipv4 de la subred con la correspondiente mascara y colocandola en modo activo.

R3(config)#interface loopback 5
R3(config-if)#
%LINK-5-CHANGED: Interface Loopback5, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback5, changed state to up
R3(config-if)#ip address 192.168.5.1 255.255.255.0
R3(config-if)#exit

20.5. Interfaz loopback 6

Se configura esta interface logica con la primera direccion ipv4 de la subred con la correspondiente mascara y colocandola en modo activo.

R3(config)#interface loopback 6
R3(config-if)#
%LINK-5-CHANGED: Interface Loopback6, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback6, changed state to up

R3(config-if)#ip address 192.168.6.1 255.255.255.0
R3(config-if)#exit

20.6. Interfaz loopback 7

Se configura esta interface logica con la direccion ipv6 establecida, se activa el ruteo de ipv6 y se graba la configuracion con el comando respectivo.

R3(config)#interface loopback 7
R3(config-if)#
%LINK-5-CHANGED: Interface Loopback7, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback7, changed state to up
R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64
R3(config-if)#exit
R3(config)#ipv6 unicast-routing
R3(config)#exit
R3#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R3#

20.7. Ruta predeterminada interface serial 0/0/1

Se configura las rutas estaticas en la interface serial 0/0/1, desde el exe privilegiado, en los dos tipos de direcciones Ipv4 e Ipv6 para que almacene todos los paquetes en una sola ruta.

```
R3#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1
%Default route without gateway, if not a point-to-point interface, may impact performance
R3(config)#ipv6 route ::/0 s0/0/1
R3(config)#
```

21. Configuracion de Switch 1

El switch 3560 de capa 3 CISCO cuenta con la version IOS Version 12.2(37)SE1, RELEASE SOFTWARE (fc1), en donde se relizaran las configuraciones pertinentes según la topoligia de red. Este dispositvo se encarga de establecer la conexión con el host creando una red LAN o local. Para organizar la admnistracion de la red es necesario desactivar la DNS en el conmutador, asignarle al switch un nombre en la topologia de red, nombre de dominio para identificarlo en el internet y configurar la seguridad con la que el admnistrador ingresara desde el exe de usuario y configuracion global**.**

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#no ip domain-lookup
Switch(config)#hostname S1
```

S1(config)#enable secret class
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
(config-line)#exit

21.1. Configuracion de acceso de Administrador local y remoto

Para tener acceso al Switch 1 local y remotamente se debe configura las lineas VTY puerto virtuales para habilitar las conexiones Telnet. Esta configuracion se la realiza desde exe privilegiado en donde se le asigna una contraseña y cifrar las contraseñas de texto no cifrado por seguridad. Se configura un mensaje de prevencion (BANNER) en donde se informa que el acceso no autorizado a la administracion de la red y se digita el comando de guardar.

S1(config)#line vty 0 4
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#exit
S1(config)#service password-encryption
S1(config)#banner motd #Se prohibe el acceso no autorizado#
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console
S1#copy running-config startup-config
Destination filename [startup-config]?

Building configuration...
[OK]
S1#

22. Configuracion de Switch 3

El switch 3560 de capa 3 CISCO cuenta con la version IOS Version 12.2(37)SE1, RELEASE SOFTWARE (fc1), en donde se relizaran las configuraciones pertinentes según la topoligia de red. Este dispositvo se encarga de establecer la conexión con el host creando una red LAN o local. Para organizar la admnistracion de la red es necesario desactivar la DNS en el conmutador, asignarle al switch 3 un nombre en la topologia de red, nombre de dominio para identificarlo en el internet y configurar la seguridad con la que el admnistrador ingresara desde el exe de usuario y configuracion global.

Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ip domain-lookup
Switch(config)#hostname S3
S3(config)#enable secret class
S3(config)#line console 0
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#exit

22.1. Configuracion de acceso de Administrador local y remoto

Para tener acceso al Switch 3 local y remotamente se debe configura las lineas VTY puerto virtuales para habilitar las conexiones Telnet. Esta configuracion se la realiza desde exe privilegiado en donde se le asigna una contraseña y cifrar las contraseñas de texto no cifrado por seguridad. Se configura un mensaje de prevencion (BANNER) en donde se informa el acceso no autorizado a la administracion de la red y se digita el comando de guardar.

```
S3(config)#line vty 0 4
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#exit
S3(config)#service password-encryption
S3(config)#banner motd #Se prohibe el acceso no autorizado#
S3(config)#exit
S3#
%SYS-5-CONFIG_I: Configured from console by console
S3#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
S3#
```

23. Verificar la conectividad de red

Tabla 6. Pruebas de conectividad mediante comando ping

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	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 = 1/3/9 ms R1#
R2	R3, S0/0/1	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 = 1/6/8 ms R2#
PC de Internet	Gateway predeterminado	209.165.200.238	Packet Tracer SERVER Command Line 1.0 C:\>ping 209.165.200.238 Pinging 209.165.200.238 with 32 bytes of data: Reply from 209.165.200.238: bytes=32 time=2ms TTL=128 Reply from 209.165.200.238: bytes=32 time<1ms TTL=128 Reply from 209.165.200.238: bytes=32 time=1ms TTL=128 Reply from 209.165.200.238: bytes=32 time<1ms TTL=128 Ping statistics for 209.165.200.238:

			Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 2ms, Average = 0ms **C:\>**

Los resultados de las pruebas en el R1, R2 y PC de internet determinan la conexión de los dispositivos

24. Configurar la seguridad del switch, las VLAN y el routing entre VLAN

24.1. Crear la base de datos de VLAN en el Switch 1

Se crean y se les asigna un nombre a las vlan según la topologia de red

S1>enable

Password:

S1#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

S1(config)#ip routing

S1(config)#vlan 21

S1(config-vlan)#name Contabilidad

S1(config-vlan)#vlan 99

S1(config-vlan)#name Administracion

S1(config-vlan)#vlan 23

S1(config-vlan)#name Ingenieria

S1(config-vlan)#exit

24.1.1. Asignar la direccion IP de administrador

Segun la topologia de red, se configura la ipv4 y la mascara de red del administrador de la vlan 99

```
S1(config)#interface vlan 99
S1(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up
S1(config-if)#ip add
S1(config-if)#ip address 192.168.99.2 255.255.255.0
S1(config-if)#exit
```

24.1.2. Asignacion de Gatway y configuracion de enlaces troncales

Se asigna la primera direccion Ipv4 del switch de la subred como gateway predeterminado; se configura los enlaces troncales forzando a las interfaces fastEthernet 0/5 y fastEthernet 0/3 a que utilice la red VLAN 1 como VLAN nativa.

```
S1(config)#ip default-gateway 192.168.99.1
S1(config)#interface fastEthernet 0/3
S1(config-if)#switchport trunk encapsulation dot1q
S1(config-if)#switchport mode trunk

S1(config-if)#
```

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up

S1(config-if)#switchport trunk native vlan 1
S1(config-if)#exit
S1(config)#interface fastEthernet 0/5
S1(config-if)#switchport trunk encapsulation dot1q
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 1
S1(config-if)#exit

24.1.3. Configuracion de puertos y asignacion de VLAN

Los puertos restantes del switch uno se los habilita como puerto de acceso, apagando aquellos puertos que no estan en uso y se asigna a la interface FastEthernet 0/6 como puerto de acceso de la vlan 21.

S1(config)#interface range fa0/1-2, fa0/4, fa0/6-24
S1(config-if-range)#switchport mode access
S1(config-if-range)#exit
S1(config)#interface range f0/6
S1(config-if-range)#switchport access vlan 21

S1(config-if-range)#exit
S1(config)#interface range fa0/1-2,fa0/4,fa0/7-24,gi0/1-2
S1(config-if-range)#shutdown

24.2. Crear la base de datos de VLAN en el Switch 3

Se crean y se les asigna un nombre a las vlan según la topologia de red

S3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S3(config)#ip routing
S3(config)#vlan 21
S3(config-vlan)#name Contabilidad
S3(config-vlan)#vlan 99
S3(config-vlan)#name Administracion
S3(config-vlan)#vlan 23
S3(config-vlan)#name Ingenieria
S3(config-vlan)#exit

24.2.1. Asignar la direccion IP de administrador

Segun la topologia de red, se configura la ipv4 y la mascara de red del administrador de la vlan 99

S3(config)#interface vlan 99
S3(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up

```
S3(config-if)#ip address 192.168.99.3 255.255.255.0
S3(config-if)#exit
```

24.2.2. Asignacion de Gatway y configuracion de enlaces troncales

Se asigna la primera direccion Ipv4 del switch de la subred como gateway predeterminado; se configura el enlace troncal forzando a la interface fastEthernet 0/3 a que utilice la red VLAN 1 como VLAN nativa.

```
S3(config)#ip default-gateway 192.168.99.1
S3(config)#interface fastEthernet 0/3
S3(config-if)#switchport trunk encapsulation dot1q
S3(config-if)#switchport mode trunk
S3(config-if)#switchport trunk native vlan 1
S3(config-if)#exit
```

24.2.3. Configuracion de puertos y asignacion de VLAN

Los puertos restantes del switch 3 se los habilita como puerto de acceso, apagando aquellos puertos que no estan en uso y se asigna a la interface FastEthernet 0/18 como puerto de acceso de la vlan 21.

```
S3(config)#interface range fa0/1-2,fa0/4-24,gi0/1-2
S3(config-if-range)#switchport mode access
S3(config-if-range)#exit
S3(config)#interface fastEthernet 0/18
S3(config-if)#switchport access vlan 21
```

S3(config-if)#exit
S3(config)#interface range fa0/1-2,fa0/4-17,fa0/19-24,gi0/1-2
S3(config-if-range)#shutdown

25. Configurar la subinterfaz G0/1 en Router 1

25.1. Configurar la subinterfaz 802.1Q .21 en G0/1

En el router 1 se configura la interface gigabitEthernet 0/1, la cual se divide en subinterface 802.1Q .21 donde se asigna la primera direccion ip disponible, la cual se le hace una descripcion con el nombre proporcionado a la subinterface y asiganada a la Vlan 21.

R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#interface gigabitEthernet 0/1.21
R1(config-subif)#description LAN de Contabilidad
R1(config-subif)#encapsulation dot1q 21
R1(config-subif)#ip address 192.168.21.1 255.255.255.0
R1(config-subif)#exit

25.2. Configurar la subinterfaz 802.1Q .23 en G0/1

En el router 1 se configura la interface gigabitEthernet 0/1, la cual se divide en subinterface 802.1Q .23 donde se asigna la primera direccion ip disponible, la cual se le hace una descripcion con el nombre proporcionado a la subinterface y asiganada a la Vlan 23.

R1(config)#interface gigabitEthernet 0/1.23

R1(config-subif)#description LAN de Ingenieria
R1(config-subif)#encapsulation dot1q 23
R1(config-subif)#ip address 192.168.23.1 255.255.255.0
R1(config-subif)#exit

25.3. Configurar la subinterfaz 802.1Q .99 en G0/1

En el router 1 se configura la interface gigabitEthernet 0/1, la cual se divide en subinterface 802.1Q .99 donde se asigna la primera direccion ip disponible, la cual se le hace una descripcion con el nombre proporcionado a la subinterface y asiganada a la Vlan 99.

R1(config)#interface gigabitEthernet 0/1.99
R1(config-subif)#description LAN de Administracion
R1(config-subif)#encapsulation dot1q 99
R1(config-subif)#ip address 192.168.99.1 255.255.255.0
R1(config-subif)#exit

Se activa la interface gigabitEthernet 0/1 con el correspondiente comando para levantar las subinterfaces.

R1(config)#interface gigabitEthernet 0/1
R1(config-if)#no shutdown
R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
%LINK-5-CHANGED: Interface GigabitEthernet0/1.21, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.21, changed state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/1.23, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.23, changed state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/1.99, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.99, changed state to up

R1(config-if)#exit

R1(config)#exit

R1#

26. Verificar la conectividad de red

Tabla 7. Pruebas de conexión de las VLAN

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	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
S3	R1, dirección VLAN 99	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
S1	R1, dirección VLAN 21	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 = 0/0/2 ms
S3	R1, dirección VLAN 23	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 = 0/0/1 ms

La pruebas de conexion de los Swtich hacia los router confirman la configuracion exitosa de las VLAN

27. Configurar el protocolo de routing dinámico OSPF

27.1. Configurar OSPF en el R1

En el router 1 se configura OSPF(Open Shortest Path First) que es el protocolo que se encarga de abrir el camino mas corto entre dos nodos. Esta configuracion se le realiza en el area 0 según la topologia de red en donde se anuncia y se asigna todas las redes conectadas directamente, se establece todas la interfaces LAN como pasivas y automaticamente se desactiva la sumarizacion.

R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#router ospf 10

```
R1(config-router)#router-id 1.1.1.1
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
R1(config-router)#passive-interface Serial0/0/0
R1(config-router)#passive-interface GigabitEthernet0/1.21
R1(config-router)#passive-interface GigabitEthernet0/1.23
R1(config-router)#passive-interface GigabitEthernet0/1.99
R1(config-router)#exit
```

27.2. Configurar OSPF en el R2

En el router 2 se configura OSPF(Open Shortest Path First) que es el protocolo que se encarga de abrir el camino mas corto entre dos nodos. Esta configuracion se le realiza en el area 0 según la topologia de red en donde se anuncia y se asigna todas las redes conectadas directamente descartando la interface GigabitEthernet0/0, se establecer la interfaz LAN (loopback) como pasiva y automaticamente se desactiva la sumarizacion.

```
R2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#router ospf 10
R2(config-router)#router-id 2.2.2.2
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
R2(config-router)#network 10.10.10.10 0.0.0.0 area 0
R2(config-router)#passive-interface loopback 0
```

R2(config-router)#exit
R2(config)#exit

27.3. Configurar OSPFv3 en el R3

En el router 3 se configura OSPFv3 (Open Shortest Path First) que es el protocolo que se encarga de abrir el camino mas corto entre dos nodos y encaminar prefijos con Ipv6. Esta configuracion se le realiza en el area 0 según la topologia de red en donde se anuncia y se asigna todas las redes conectadas directamente con Ipv4, se establece todas las interfaces de LAN IPv4 (Loopback) como pasivas y automaticamente se desactiva la sumarizacion.

R3#configure terminal
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#router ospf 10
R3(config-router)#router-id 3.3.3.3
R3(config-router)#network 172.16.2.0 0.0.0.3 area 0
R3(config-router)#
04:24:11: %OSPF-5-ADJCHG: Process 10, Nbr 2.2.2.2 on Serial0/0/1 from LOADING to FULL, Loading Done
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
R3(config-router)#passive-interface loopback 4
R3(config-router)#passive-interface loopback 5

R3(config-router)#passive-interface loopback 6

R3(config-router)#exit

R3(config)#exit

R3#

28. Verificar la información de OSPF

Tabla 8. Comandos de verificacion de informacion OSPF

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?	Router#show ip protocols
¿Qué comando muestra solo las rutas OSPF?	Router#show ip route ospf
¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	R1#show ip route

La verificacion de la informacion OSPF permite organizar la administracion de la red LAN

29. Implementar DHCP y NAT para IPv4

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

Se reservar las primeras 20 direcciones IP en la VLAN 21 y la VLAN 23 para configuraciones estáticas

R1#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.30

R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.30

29.2. Crear un pool de DHCP para la VLAN 21

En el router 1 se crea el servidor DHCP pool de la VLAN 21 con un nombre para ser identificado en la red LAN, las direcciones del servidor DNS, el nombre del dominio y el gateway predeterminado.

```
R1(config)#ip dhcp pool ACCT
R1(dhcp-config)#dns-server 10.10.10.10
R1(dhcp-config)#domain-name ccna-sa.com
R1(dhcp-config)#default-router 192.168.21.1
R1(dhcp-config)#network 192.168.21.0 255.255.255.0
R1(dhcp-config)#exit
```

29.3. Crear un pool de DHCP para la VLAN 23

En el router 1 se crea el servidor DHCP pool de la VLAN 23 con un nombre para ser identificado en la red LAN, las direcciones del servidor DNS, el nombre del dominio y el gateway predeterminado.

```
R1(config)#ip dhcp pool ENGNR
R1(dhcp-config)#dns-server 10.10.10.10
R1(dhcp-config)#domain-name ccna-sa.com
R1(dhcp-config)#default-router 192.168.23.1
R1(dhcp-config)#network 192.168.23.0 255.255.255.0
R1(dhcp-config)#exit
R1(config)#exit
R1#
```

30. Configurar la NAT estática y dinámica en el R2

30.1. Crear una base de datos local con una cuenta de usuario

La traduccion de direcciones de red (NAT) brinda la conexión directa con direcciones internas estaticas locales con las globales y dinamicamente en las redes LAN. Se crea una base de datos locales con nombre de usario, contraseña y privilegios, posteriormente se debe de habilitar el servicio de servidor de HTTP para configurarlo de tal manera que se pueda para utilizar la base de datos local para la autenticación.

```
R2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#user webuser privilege 15 secret cisco12345
```

Crear una NAT estática al servidor web con una dirección global interna asignada y establecer la interfaz interna y externa para la NAT estática.

```
R2(config)# ip nat inside source static 10.10.10.10 209.165.200.229
R2(config)#interface gigabitEthernet 0/0
R2(config-if)#ip nat outside
R2(config-if)#exit
R2(config)#interface gigabitEthernet 0/0
R2(config-if)#ip nat inside
R2(config-if)#exit
```

30.2. Configurar la NAT dinámica dentro de una ACL privada

Se asigna un codigo de acceso de lista, en donde se permitir la traducción de las redes asignadas en el R1 y 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 192.168.4.1 0.0.0.255
R2(config)#access-list 1 permit 192.168.5.1 0.0.0.255
R2(config)#access-list 1 permit 192.168.6.1 0.0.0.255

Defina el pool de direcciones IP públicas utilizables en un conjunto de nombres con el nombre de INTERNET; El conjunto de direcciones incluye: 209.165.200.225 – 209.165.200.228 y se define la traducción de NAT dinámica.

R2(config)# ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248
R2(config)#ip nat inside source list 1 pool INTERNET
R2(config)#exit
R2#
%SYS-5-CONFIG_I: Configured from console by console
R2#

31. Configurar NTP

Tabla 9. Sincronizacion de los relojes a través del enrutamiento

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2. **20:48:00 p.m 13 nov 2020**	R2#clock set 20:48:00 13 nov 2020 R2#show clock detail 20:48:10.365 UTC Fri Nov 13 2020 Time source is user configuration R2#

Configure R2 como un maestro NTP. **Nivel de estrato: 5**	R2#configure terminal Enter configuration commands, one per line. End with CNTL/Z. R2(config)#ntp master 5 R2(config)#exit R2# %SYS-5-CONFIG_I: Configured from console by console **R2#**
Configurar R1 como un cliente NTP. **Servidor: R2**	R1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. 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)#exit R1# %SYS-5-CONFIG_I: Configured from console by console
Verifique la configuración de NTP en R1.	R1#show ntp status Clock is synchronized, stratum 6, reference is 172.16.1.2 nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision is 2**24 reference time is 0C6E0E8F.0000026E (20:58:55.622 UTC vie. nov. 13 2020) clock offset is -1.00 msec, root delay is 2.00 msec root dispersion is 10.06 msec, peer dispersion is 0.12 msec. loopfilter state is 'CTRL' (Normal Controlled Loop), drift is - 0.000001193 s/s system poll interval is 4, last update was 4 sec ago. R1# R1#show ntp associations address ref clock st when poll reach delay offset disp

	*~172.16.1.2 127.127.1.1 5 11 16 377 4.00 0.00 0.12 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured R1#

NTP es un protocolo de internet de sincronizacion de paquetes dependiendo de la sincronzacion de los relojes en la red LAN.

32. Configurar y verificar las listas de control de acceso (ACL)

32.1. Restringir el acceso a las líneas VTY en el R2

Se configura una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2 asignandole un de la ACL, permisos de acceso por telnet y aplicar la ACL con nombre a las lineas de VTY y revisar el funcionamiento.

R2>enable
Password:
R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ip access-list standard ADMIN-MGT
R2(config-std-nacl)#permit host 172.16.1.1
R2(config-std-nacl)#exit
R2(config)#line vty 0 4
R2(config-line)#access-class ADMIN-MGT in
R2(config-line)#exit

32.2. Comando CLI

Tabla 10. Comando de CLI para reflejar informacion

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	Router(config)#show access-list
Restablecer los contadores de una lista de acceso	Router(config)#clear access-list counters
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	Router(config)#interface Fa0/1 Router(config-if)#ip access-group 1 out
¿Con qué comando se muestran las traducciones NAT?	Router(config)#show ip nat translations 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?	Router(config)#clear ip nat translation

La tabla muestra informacion de algunos comandos utilizados en la configuracion de Router

33. Verificar el protocolo DHCP y la NAT estática

Figura 29. PC-A información de IP del servidor de DHCP

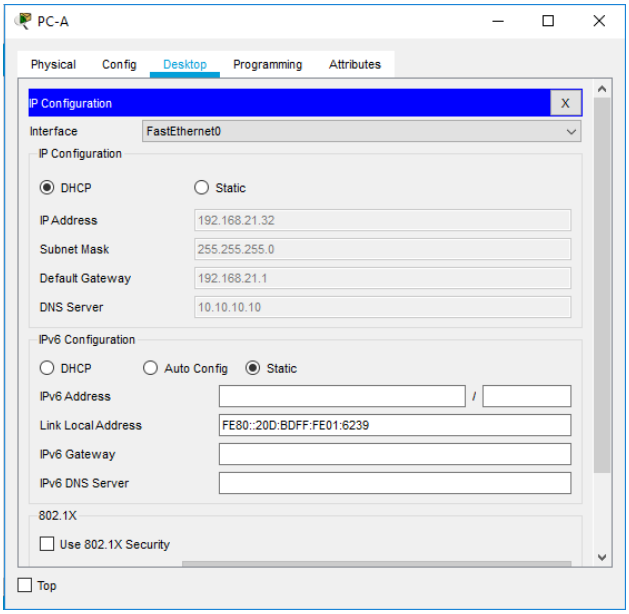


Figura 30. PC-C información de IP del servidor de DHCP

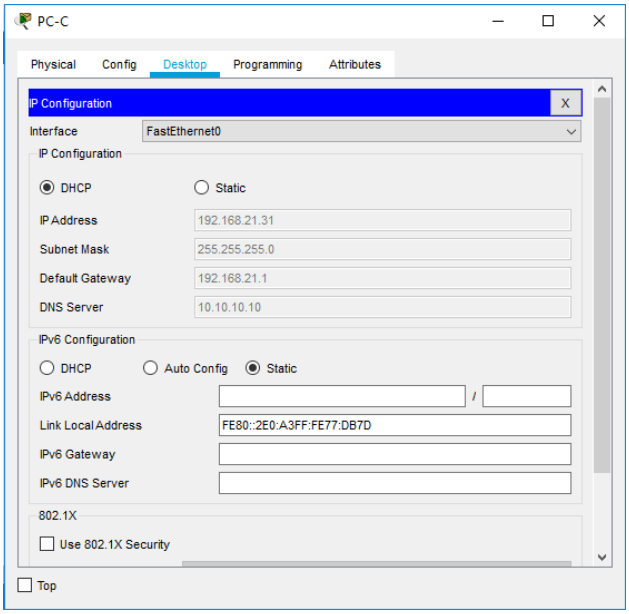


Figura 31. Ping de PC-A a PC-C

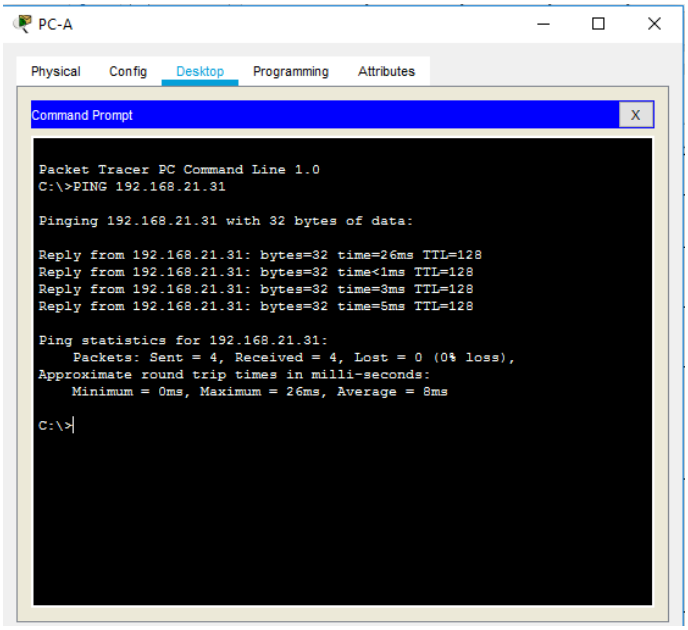
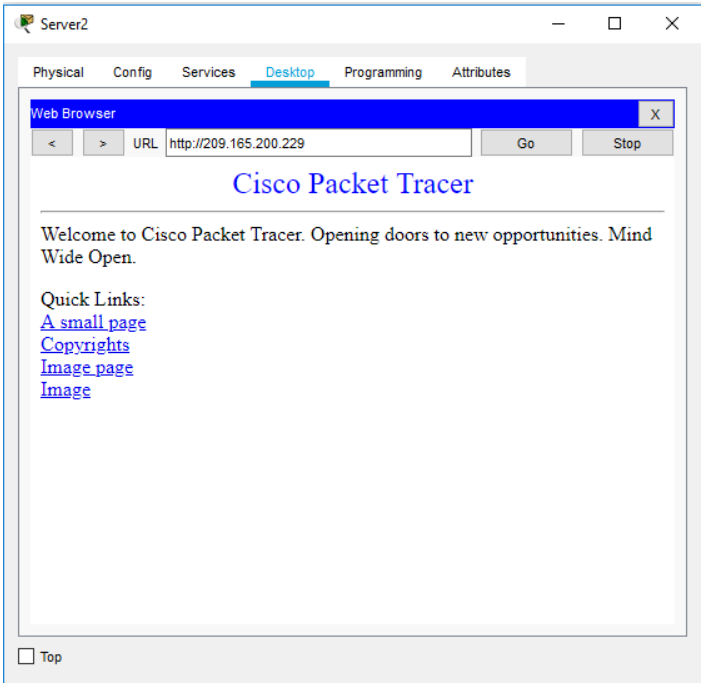


Figura 32. Prueba de navegador Web



CONCLUSIONES

Las practicas de laboratorio de simulacion de dos ecsenarios o topologias de red LAN, permiten el aprendizaje de el funcionamiento de una red desde el conocimiento de los diferentes terminales, conexión de cables con puertos, configuracion de los dispositivos mediante protocolos modelo OSI, administracion de redes y seguridad de puntos de conexion de red.

Los dispositivos como el router y switch CISCO estan diseñados para enlazarse a travez de protocolos de redes de host, que se adaptan al modelo OSI (Open Systems Interconnection), para garantizar la transmision de paquetes enlazados con las capa 2 y capa 3 de las redes LAN y WAN.

Los ejercicios relacionados a las dos topologias de red, resaltan las configuraciones basicas de los enrutadores y conmutadores para las buenas practicas en la administracion de una red. Reseteo de dispositivos, configuracion de password de seguridad a modo usuario y privilegiado, configuracion de administradores locales y remotos mediante SSH o telnet, encriptacion de contraseñas, descripciones, mensajes de seguridad (BANNER), configuracion de protocolos e interfaces logicas y fisicas, etc., garantizan los conocimiento para el perfil del administrador de red.

BIBLIOGRAFIA

Calero Romero, J. (2014). EtherChannel03: EtherChannel. Ejemplo práctico I. Protocolo LACP. Retrieved 31 October 2020, from https://www.youtube.com/watch?v=SvWght-GPPQ

Cardona, I. (2020). Inicio de sesión de Adobe Connect. Retrieved 31 October 2020, from http://conferencia2.unad.edu.co/ecbti2020_4_1/

CISCO. (2014). Protocolos y comunicaciones de red. Fundamentos de Networking. Recuperado de:https://static-course-assets.s3.amazonaws.com/ITN50ES/module7/index.html#7.1.1.4

CISCO. (2020, 21 abril). Configure InterVLAN Routing on Layer 3 Switches. Configure InterVLAN Routing on Layer 3 Switches. https://www.cisco.com/c/en/us/support/docs/lan-switching/inter-vlan-routing/41860-howto-L3-intervlanrouting.html

Gustavo Lobato Clara. (2014, 24 mayo). CURSO 7-1 Explicacion de protocolo OSPF [Vídeo]. You tube. https://www.youtube.com/watch?v=dwT5du44t_8

Matturro, G. M., Barrio, G. M., & Baccino, D. B. (2007, diciembre). Introducción a la Configuración de routers Cisco. Universidad ORT Uruguay. https://www.ort.edu.uy/fi/pdf/configuracionroutersciscomatturro.pdf

Ramirez, D. (2020). Web Diplomado de Profundizacion Redes Cisco Unidad 4 y 5. Retrieved 31 October 2020, from http://conferencia2.unad.edu.co/p71qnm0eiq6s/?proto=true

Sepulveda, M. (2019). Configuración de 802 1Q y VLAN Nativa Cisco CCNA. Retrieved 31 October 2020, from https://www.youtube.com/watch?v=SvWght-GPPQ

Zalasar, P. (2020). CIPA 2 Prueba de Habilidades Diplomado Cisco (2020-10-16 at 16:04 GMT-7). Retrieved 31 October 2020, from https://drive.google.com/file/d/1XTTmvwmU_Z-4SDMoRom6HeJSAJiqj_Q6/view

SOLUCIÓN DE UN ESCENARIO PRESENTE EN ENTORNOS CORPORATIVOS BAJO EL USO DE TECNOLOGÍA CISCO

Oscar Mauricio Riascos Pupiales
Universidad Abierta y a Distancia UNAD, omriascosp@unadvirtual.edu.co

Resumen

En el desarrollo del escenario uno se expone gráficamente una topología de red, compuesta por una serie de dispositivos como Router, Switch, host y los medios de transmisión (cables) que en conjunto permite el envío de paquetes de información entre los terminales. Cada dispositivo esta configurado con los protocolos adecuados para enrutar, conmutar, recibir y enviar datos mediante el modelo de referencia OSI en el entorno de simulación Packet Tracer.
La configuración de los routers y Switch CISCO están diseñados para trabajar en Ipv4 con formato de 32 bits y también Ipv6 como protocolo estándar para remplazar en el futuro a Ipv4; En el escenario se demuestra el acoplamiento de las dos IP en función de una misma red. La administración de la red LAN esta basada en las configuraciones básicas de los puntos de conexión (switch y router), garantizando la protección de la red, eficiencia en la solución de problemas de conexión, expansión de la topología y mantenimientos preventivos y correctivos de la red.

Palabras clave: Protocolo, topología, Vlan, Interfaces, Enrutador, Conmutador

Abstract:

In the development of scenario one, a network topology is graphically exposed, composed by a series of devices such as Router, Switch, host and the transmission media (cables) that together allow the sending of information packets between the terminals. Each device is configured with the appropriate protocols to route, switch, receive and send data through the OSI reference model through the Packet Tracer simulation environment.

The configuration of CISCO routers and switches are designed to work in IPv4 with 32-bit format and also IPv6 as a standard protocol to replace IPv4 in the future; The scenario demonstrates the coupling of the two IPs based on the same network. The administration of the LAN network is based on basic configurations of connection points (switch and router), guaranteeing the protection of network, efficiency in solving connection problems, expansion of topology and preventive and corrective maintenance of the network. net.

Keywords— Protocol, Topology, Vlan, Interfaces, Router, Switch.

I. INTRODUCCIÓN

La configuración del escenario uno esta conformado por dos switch de capa 3 referencia 3560, un router con referencia 1142 CISCO y dos hosts. [1] Los modelos de switch Catalyst 3560, 3750, las Catalyst 4500/4000 Series con el Sup II+ o posteriores, o bien las Catalyst 6500/6000 Series que ejecuten el Cisco IOS System Software soportan las funciones básicas del ruteo InterVLAN en todas sus versiones de software soportadas. El switch 3560 utiliza la versión IOS 12.2(37) SE1, permitiendo el ruteo de InterVLAN y activación de Ipv6. [2] Una vez identificado los dispositivos que cumplieran con los requisitos necesarios para formar la topología de la red LAN, se ejecutan comandos para borrar el contenido de la NVRAM en los puntos de conexión y no presente problemas al momento de la configuración. [3] El switch 3560 maneja la característica de que la plantilla SDM no esta activada; es necesario al inicio de la configuración del dispositivo activar esta característica con el comando respectivo y ejecutar un reload para Ipv6.

[4] Una vez organizados los dispositivos en el entorno de laboratorio de simulación Packet Tracer, se configuran los nodos (Switch y router) con los protocolos necesarios para poder interactuar con el Interconexión de Sistemas Abiertos (Modelo OSI) e intercambien paquetes de información. [5] El router como el switch manejan en su gran mayoría comandos de configuración semejantes ya que pertenecen a la misma fuente de producción CISCO. [6] De forma predeterminada, hay tres niveles de comando en el router: Nivel de privilegio 0: incluye los comandos disable, enable, exit, help y logout.; Nivel de privilegio 1: es el nivel normal en Telnet e incluye todos los comandos de nivel de usuario en la petición de entrada router>. Nivel de privilegio 15: incluye todos los comandos de nivel de habilitación en la petición de entrada router#. La configuración de los accesos del administrador de la red LAN, establecen contraseñas

para el modo usuario y modo privilegiado con la encriptación correspondiente. Habilitar accesos con password a administradores locales y remotos con los privilegios necesario para hacer cambios en los dispositivos desde SSH (Secure Shell). [7] El protocolo SSH utiliza encriptación para asegurar la conexión entre un cliente y un servidor; esta configuración de protocolo permite encriptar las contraseñas de administradores para evitar que terceras personas identifiquen el password.

[8] La configuración de Ipv4 e Ipv6 en los conmutadores con las correspondientes máscaras, aseguran la interacción de las dos IP en el momento de hacer pruebas conexión. [9] La creación de Vlan como enlaces lógicos son determinantes en la creación de troncos 802.1Q que utilicen la VLAN nativa para la conexión de la red LAN. [10] DHCP le permite asignar automáticamente direcciones IP reutilizables a clientes DHCP; Se agregan otras configuraciones que son utilizadas para la interconexión de redes como DHCP para crear Ip dinámicas en los hosts, [11] Etherchannel aumentar el ancho de banda y port-security en los casos de bloquear puerto como medidas de prevención y seguridad.

II. METODOLOGIA

La metodología con la cual se plantea el desarrollo del escenario uno se basa en una investigación de tipo aplicada ya que se busca encontrar una solución para que se pueda transmitir paquetes de información en la red LAN entre Ipv4 e Ipv6 en los hosts. [12] La Investigación Aplicada tiene por objetivo resolver un determinado problema o planteamiento específico, enfocándose en la búsqueda y consolidación del conocimiento para su aplicación y, por ende, para el enriquecimiento del desarrollo cultural y científico. En la topología de red se plantea una topología de red LAN compuesta por dispositivos como Router, Switch, host y medios de conexión (cables) que se propone una configuración que puedan interactuar entre ellos y se pueda dar solución a ciertas condiciones de uso.[13] La investigación aplicada también se le denomina activa o dinámica, ya que depende de sus descubrimientos y aportes teóricos; los enrutadores como los conmutadores CISCO están en constante desarrollo y actualización; desde las versiones de las IOS que permiten utilizar ciertas características que puedan adaptarse al modelo OSI como las plantillas SDM que habilitan la Ipv6 en los Switch 3560 de capa 3, hasta los comandos ipv6 unicast-routing que los habilita en el Router 1142.

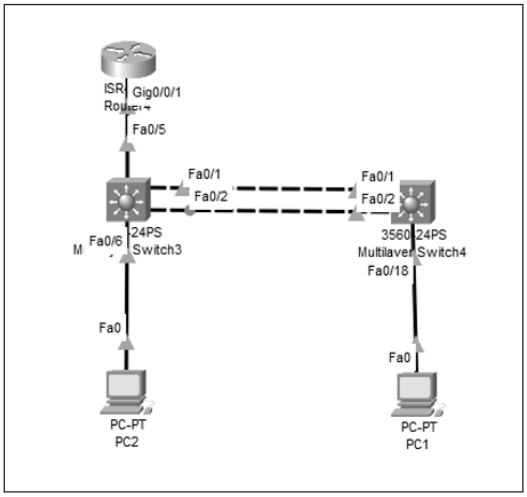
También el método experimental es utilizado para obtener los resultados en la solución de la conexión de los dispositivos del escenario uno . [14] De manera general, el objetivo de la experimentación consiste en identificar las causas por las que se producen determinados resultados. Al aplicarla a la Ingeniería de Sistemas (IS), la experimentación nos ayuda a identificar y comprender distintos aspectos así como conexiones involucradas en el desarrollo y mantenimiento de productos software. Esta identificación de aspectos y conexiones permite validar o refutar con hechos las creencias y prácticas que basamos en el desarrollo y mantenimiento de productos software. Los router y switch CISCO esta diseñados para adaptarse a los protocolos de comunicación estándar modelo OSI en una red LAN. [15] Para adecuar los dispositivos se los adapto con algunos protocolos de capa 5,6 y 7 de aplicación, sesión y presentación como equivalentes, utilizando protocolos TCP/IP como NFS, NIS, DNS, LDAP, telnet, ftp, rlogin, rsh, rcp, RIP, RDISC, SNMP y otros. Capa 4 de transporte protocolos como TCP, UDP, SCTP; capa 3 de red-internet con protocolos como IPv4, IPv6, ARP, ICMP; capa 2 de datos equivalente al vinculo de datos con PPP, IEEE 802.2 y la capa 1 siendo la red física con los protocolos como Ethernet (IEEE 802.3), Token Ring, RS-232, FDDI y otros. Basados en esta información de transmisión de datos para red, se identifica los motivos de los parámetros de protocolos como causas que son relevantes para el funcionamiento de la topología de red del primer escenario.

Los resultados de la metodología de la experimentación llevan a diseñar e implementar técnicas de mantenimiento y prevención de administración de la red LAN.

III. RESULTADOS

A partir de la topología de red escenario uno, se plantean una serie de configuraciones de los dispositivos CISCO de la red LAN que, son implementadas en un entorno de simulación Packet Tracer para hacer las pruebas de funcionalidad y respuesta a las configuraciones planteadas.

Figura 1. Topología Escenario1



Para las pruebas de laboratorio, se brinda una serie de datos que identificaran los enlaces virtuales y físicos de las interfaces para el envio de paquetes. Información como el

nombre de las VLAN y las direcciones de los switchs y routers en Ipv4 e Ipv6 que establezcan conexión de datos.

TABLA 1
NOMBRE DE VLAN

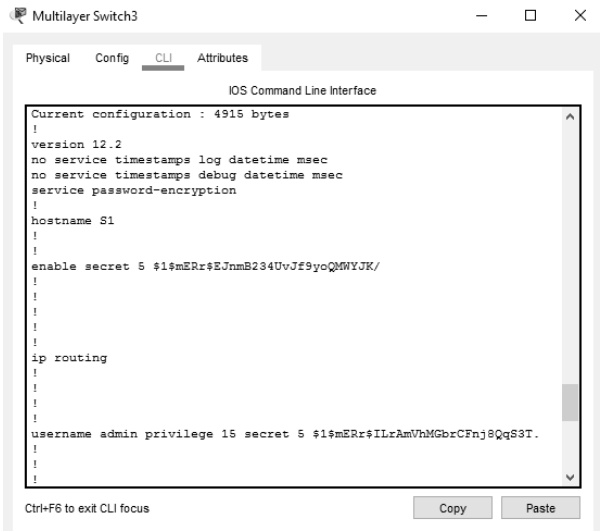
VLAN	Nombre de la VLAN
2	Bikes
3	Trikes
4	Management
5	Parking
6	Native

TABLA 2
ASIGNACIÓN DE DIRECCIONES DE LOS DISPOSITIVOS

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
R1 G0/0/1.2	10.19.8.1 /26	No corresponde
	2001:db8:acad:a: :1 /64	No corresponde
R1 G0/0/1.3	10.19.8.65 /27	No corresponde
	2001:db8:acad:b: :1 /64	No corresponde
R1 G0/0/1.4	10.19.8.97 /29	No corresponde
	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
	2001:db8:acad:209: :1 /64	No corresponde
S1 VLAN 4	10.19.8.98 /29	10.19.8.97
	2001:db8:acad:c: :98 /64	No corresponde
	fe80: :98	No corresponde
S2 VLAN 4	10.19.8.99 /29	10.19.8.97
	2001:db8:acad:c: :99 /64	No corresponde
	fe80: :99	No corresponde
PC-A NIC	Dirección DHCP para IPv4	DHCP para puerta de enlace predeterminada IPv4
	2001:db8:acad:a: :50 /64	fe80::1
PC-B NIC	DHCP para dirección IPv4	DHCP para puerta de enlace predeterminada IPv4
	2001:db8:acad:b: :50 /64	fe80::1

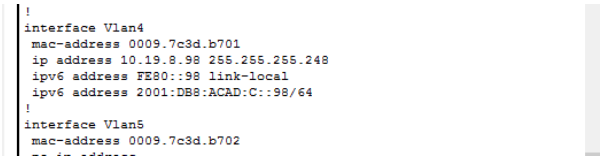
Para la administración de los dispositivos de la topología de red, se configura los enrutadores y conmutador el ingreso a los dispositivos con contraseñas en modo usuario y modo privilegiado; También algunas características que le permitan ser identificados en la red como el nombre con el comando hostname, acceso remotamente mediante Telnet o SSH y con encriptación de contraseñas que brinden seguridad en la administración de la red.

Figura 2. Topología Escenario1



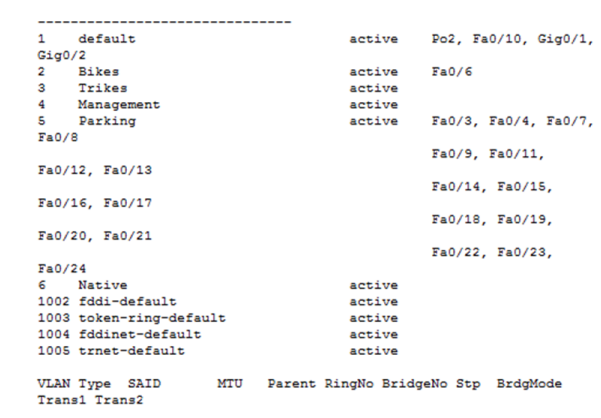
Las direcciones Ipv6 e Ipv4 son incorporadas al router y switchs con le segmentación necesaria para que interactúen con el tráfico de paquetes en la red.

Figura 3. Configuración Ipv4 e Ipv6



Las Vlans como enlaces lógicos dentro de la interface son creadas en los dispositivos de red, debidamente renombradas para que puedan tener acceso al tráfico de paquetes de información entre host. Los accesos se habilitan en los puertos físicos FastEternet, GigabitEternet y subinterfaces con las condiciones necesaria para que el transporte de paquetes sea direccionado mediante una Vlan Nativa. La configuración de troncos 802.1Q o encapsulamiento admite que se utilice un solo medio físico por donde transitan diferentes redes(VLAN) como protocolo que se adapte am modelo OSI de redes.

Figura 4. Creación de VLANS



La topología de red LAN del escenario uno proporciona una configuración de EtherChannel entre el Swich uno y dos, por donde transitan los enlaces lógicos de las Vlan bikes, trikes, Management y Parkin en las interfaces lógicas FastEternet 1 y 2. EtherChannel garantiza el ancho de banda entre dispositivos, garantizando la tolerancia de fallos, la garantía de proporcionar una señal estable con dos enlaces físicos de conexión FastEternet 1 y 2 y distribución de envió de paquetes por dos enlaces equilibrando cargas.

EtherChannel se adapta a los estándares CISCO 802.3 full-duplex.

Figura 5. Configuración EtherChannel

```
Password:
S2#sho
S2#show ter
S2#show eth
S2#show etherchannel summ
S2#show etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------
+-----------------------------------------------

2      Po2(SD)           LACP   Fa0/1(I) Fa0/2(I)
S2#
```

Para garantizar la configuración establecida en los puntos de conexión de la red LAN, se realizan las pruebas mediante latencia (ping), que se envía de extremo a extremo mediante los hosts, con las respuestas positivas en donde refleja el tiempo de medición en milisegundos la subida y bajada de conexión. Las pruebas son realizadas con el router y los switchs desde los terminales, en donde se evidencia que los hosts han adquirido una ip dinámica ya que el router fue configurado con el protocolo DHCP cliente/servidor.

Figura 6. Ping IP 10.19.8.1 PC1

```
Packet Tracer PC Command Line 1.0
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<1ms 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

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 = 0ms, Average = 0ms
```

Figura 7. Ping IP 10.19.8.65 PC1

```
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 8. Ping a IPV6 2001:db8:acad:b: :50PC1

```
C:\>ping 2001:db8:acad:b::50

Pinging 2001:db8:acad:b::50 with 32 bytes of data:

Reply from 2001:DB8:ACAD:B::50: bytes=32 time=11ms TTL=127
Reply from 2001:DB8:ACAD:B::50: bytes=32 time<1ms TTL=127
Reply from 2001:DB8:ACAD:B::50: bytes=32 time=1ms TTL=127
Reply from 2001:DB8:ACAD:B::50: bytes=32 time<1ms TTL=127

Ping statistics for 2001:DB8:ACAD:B::50:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 11ms, Average = 3ms
```

Figura 9. Ping a IPv6 2001:db8:acad:b::50 PC 2

```
C:\>ping 2001:db8:acad:b::50

Pinging 2001:db8:acad:b::50 with 32 bytes of data:

Reply from 2001:DB8:ACAD:B::50: bytes=32 time=4ms TTL=128
Reply from 2001:DB8:ACAD:B::50: bytes=32 time=4ms TTL=128
Reply from 2001:DB8:ACAD:B::50: bytes=32 time=1ms TTL=128
Reply from 2001:DB8:ACAD:B::50: bytes=32 time=4ms TTL=128

Ping statistics for 2001:DB8:ACAD:B::50:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 4ms, Average = 3ms
```

Figura10. Ping a IPv6 2001:db8:acad:209::1 PC 2

```
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=1ms TTL=255
Reply from 2001:DB8:ACAD:209::1: bytes=32 time=1ms 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 = 1ms, Maximum = 1ms, Average = 1ms
```

IV. CONCLUSIONES

Las prácticas de laboratorio de simulación de dos escenarios o topologías de red LAN, permiten el aprendizaje del funcionamiento de una red desde el conocimiento de los diferentes terminales, conexión de cables con puertos, configuración de los dispositivos mediante protocolos modelo OSI, administración de redes y seguridad de puntos de conexión de red.

Los dispositivos como el router y switch CISCO están diseñados para enlazarse a través de protocolos de redes de

host, que se adaptan al modelo OSI (Open Systems Interconnection), para garantizar la transmisión de paquetes enlazados con las capas 2 y capa 3 de las redes LAN y WAN.

Los ejercicios relacionados a las dos topologías de red, resaltan las configuraciones básicas de los enrutadores y conmutadores para las buenas prácticas en la administración de una red. Reseteo de dispositivos, configuración de password de seguridad a modo usuario y privilegiado, configuración de administradores locales y remotos mediante SSH o telnet, encriptación de contraseñas, descripciones, mensajes de seguridad (BANNER), configuración de protocolos e interfaces lógicas y físicas, etc., garantizan los conocimientos para el perfil del administrador de red.

V. Referencias

[1] CISCO. (s. f.). Configurar routing interVLAN en switches de capa 3. CISCO.COM. Recuperado 22 de noviembre de 2020, de https://www.cisco.com/c/es_mx/support/docs/lan-switching/inter-vlan-routing/41860-howto-L3-intervlanrouting.html

[2] Problemas causados por el acceso simultáneo a la NVRAM del enrutador. (s. f.). CISCO.COM. Recuperado 14 de noviembre de 2020, de https://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/ios-software-releases-124-mainline/46942-nvram.html#req

[3] OpenWebinars. (2019, 26 abril). Cisco: Configuración de SDM Templates [Vídeo]. YouTube.com. https://www.youtube.com/watch?v=L4bwV5M6hkk

[4] Asmoday S.A. (2016, 17 febrero). Cómo se utiliza el programa Packet Tracer (cisco). Asmodaysa.com. https://asmodaysacom.wordpress.com/2016/02/17/como-se-utiliza-el-programa-packet-tracer-cisco/

[5] Cabrera, C. C. (2020, 23 marzo). Configuración básica de routers/switches cisco: CCNAv7 ITN mod2. Cesarcabrera.inf. https://cesarcabrera.info/configuracion-basica-de-routers-switches-cisco-ccnav7-itn-mod2/

[6] CISCO. (s. f.-b). Los niveles de privilegio de IOS no pueden ver la configuración completa en ejecución. Cisco.com. Recuperado 10 de noviembre de 2020, de https://www.cisco.com/c/es_mx/support/docs/security-vpn/terminal-access-controller-access-control-system-tacacs-/23383-showrun.html

[7] SSH. (s. f.). SSH (Secure Shell). ssh.com. Recuperado 9 de noviembre de 2020, de https://www.ssh.com/ssh/

[8] Guerreros de la Red Michely Lopez. (2019, 7 enero). Packet Tracer - Configurar Tunel IPV6 a IPV4 en Router cisco | Routing OSPF RIPV6 [Vídeo]. YouTube.com. https://www.youtube.com/watch?v=5mWMjAIPA8o

[9] CISCO. (s. f.-b). Enlace ISL y 802.1Q entre switches de configuración fija Catalyst Layer 2 y ejemplo de configuración de switches CatOS. cisco.com. Recuperado 3 de noviembre de 2020, de https://www.cisco.com/c/en/us/support/docs/lan-switching/8021q/8758-43.html

[10] CISCO. (s. f.-a). Configuración dinámica de opciones del servidor DHCP. Cisco.com. Recuperado 1 de noviembre de 2020, de https://www.cisco.com/c/en/us/support/docs/ip/dynamic-address-allocation-resolution/22920-dhcp-ser.html

[11] CISCO. (s. f.-b). Configurar el enlace del EtherChannel y del 802.1Q entre los switches de configuración fija del Catalyst L2 y los switches de Catalyst que ejecutan CatOS. Cisco.com. Recuperado 29 de octubre de 2020, de https://www.cisco.com/c/es_mx/support/docs/switches/catalyst-4000-series-switches/23408-140.html

[12] Duoc UC Bibliotecas. (s. f.). Definición y propósito de la investigación aplicada. Definición y Propósito de la investigación aplicada. Recuperado 17 de noviembre de 2020, de http://www.duoc.cl/biblioteca/crai/definicion-y-proposito-de-la-investigacion-aplicada.

[13] Hernández, R. Fernández, C. y Baptista, P. (2014). Metodología de la Investigación. Venezuela. McGraw-Hill Education.

[14] Gómez, Omar S.& Aguilar Vera, Raul & Ucán Pech, Juan. (2018). Experimentación de Ingeniería de Software.

[15] Introducción al conjunto de protocolos TCP/IP. (s. f.). docs.oracle.com. Recuperado 21 de noviembre de 2020, de https://docs.oracle.com/cd/E19957-01/820-2981/6nei0r0r9/index.html