SOLUCIÓN DE DOS ESCENARIOS BAJO EL USO DE TECNOLOGÍA CISCO

VÍCTOR ERNESTO BADILLO CAMARGO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
INGENIERÍA DE SISTEMAS
TUNJA
2020

SOLUCIÓN DE DOS ESCENARIOS BAJO EL USO DE TECNOLOGÍA CISCO

VÍCTOR ERNESTO BADILLO CAMARGO

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

DIRECTOR
PAULITA FLOR SALAZAR

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
INGENIERÍA DE SISTEMAS
TUNJA
2020

NOTA DE ACEPTACIÓN

_____
_____
_____
_____
_____
_____

_____
Firma del Presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

Tunja, 14 de diciembre de 2020

AGRADECIMIENTOS

A Dios primero que todo, a mis padres Isaac Badillo y Lucy Camargo que siempre han estado en todos los momentos de mi vida con su apoyo incondicional, a mi esposa Natalia y mis hijos Eliana, Victor, Julieta que son la razón para siempre estar mejorando personalmente. A todos aquellos que de una u otra forma han sido fuente de inspiración por su trabajo y dedicación les dedico este proyecto de vida.

CONTENIDO

INTRODUCCIÓN 14
Escenario 1 15
1. Instrucciones 17
Parte 1: Inicializar y Recargar y Configurar aspectos basicos de los dispositivos 17
Paso 1: Inicializar y volver a cargar el router y el switch 17
Configurar R1 17
Paso 2: Configure S1 y S2. 20
Parte 2: Configuración de la infraestructura de red (VLAN, Trunking, EtherChannel) 24
Paso 3: Configurar S1 24
Paso 4: Configure el S2. 26
Parte 2: Configurar soporte de host 30
Paso 1: Configure R1 30
Paso 2: Configurar los servidores 31
Parte 3: Probar y verificar la conectividad de extremo a extremo 32
Escenario 2 39
Parte 1: Inicializar dispositivos 39
Parte 2: Configurar los parámetros básicos de los dispositivos 40
Parte 3: Configurar la seguridad del switch, las VLAN y el routing entre VLAN 47
Parte 4: Configurar el protocolo de routing dinámico OSPF 52
Parte 5: Implementar DHCP y NAT para IPv4 55
Parte 6: Configurar NTP 59
Parte 7: Configurar y verificar las listas de control de acceso (ACL) 59
CONCLUSIONES 62
REFERENCIAS 63
ANEXOS 65

LISTA DE TABLAS

Tabla 1: VLAN 15
Tabla 2 : Asignación de direcciones.....16
Tabla 3 : Paso 2: Configurar R1.....17
Tabla 4: Paso 3: Configure S1 y S2. 20
Tabla 5 :Configuración de la infraestructura de red (VLAN) 24
Tabla 6 : Paso 5: Configure el S2.....27
Tabla 7: Paso 1: Configure R1 30
Tabla 8:Paso 2: Configurar los servidores 31
Tabla 9 :Configuración de red de PC-A 31
Tabla 10 : Parte 3: Probar y verificar la conectividad de extremo a extremo 32
Tabla 11 : Paso 1: Inicializar y volver a cargar los routers y los switches 40
Tabla 12 : Paso 1:Configurar la computadora de Internet 40
Tabla 13 : Paso 2:Configurar R1.....41
Tabla 14 : Paso 3:Configurar R2.....42
Tabla 15 : Paso 4: Configurar R3.....43
Tabla 16 : Paso 5: Configurar S1 45
Tabla 17 : Paso 6: Configurar el S3 46
Tabla 18: Paso 7: Verificar la conectividad de la red.....47
Tabla 19 : Paso 1: Configurar S1 48
Tabla 20 :Paso 2: Configurar el S3 49
Tabla 21 : Paso 3: Configurar R1.....50
Tabla 22 : Paso 4: Verificar la conectividad de la red 51
Tabla 23 : Paso 1: Configurar OSPF en el R1 52
Tabla 24 : Paso 2: Configurar OSPF en el R2 53
Tabla 25 : Paso 3: Configurar OSPFv3 en el R2 54
Tabla 26: Paso 4: Verificar la información de OSPF.....55
Tabla 27 : Paso 1: Configurar el R1 como servidor de DHCP para las V.....55

Tabla 28: Paso 2: Configurar la NAT estática y dinámica en el R2 56
Tabla 29: Paso 3: Verificar el protocolo DHCP y la NAT estática.....57
Tabla 30: Parte 6: Configurar NTP 59
Tabla 31: Paso 1: Restringir el acceso a las líneas VTY en el R2.....60
Tabla 32: Paso 2: Introducir el comando de CLI 60

TABLA DE ILUSTRACIONES

Ilustración 1 : Figura 1 Topología 15
Ilustración 2:Figura 2. Ping desde PC-A a R1 G0/0/1.2 IP 10.19.8.1 32
Ilustración 3: Figura 3. Ping desde PC-A a R1 G0/0/1.2 IPv6 2001:db8:acad:a::.. 32
Ilustración 4 : Figura 4. Ping desde PC-A a R1 G0/0/1.3 IP 10.19.8.65 33
Ilustración 5 : Figura 5. Ping desde PC-A a R1 G0/0/1.3 IPv6 2001:db8:acad:b:...33
Ilustración 6 : Figura 6. Ping desde PC-A a R1 G0/0/1.4 IP 10.19.8.97 33
Ilustración 7 : Figura 7. Ping desde PC-A a R1 G0/0/1.4 IPv6 2001:db8:acad:c: ..33
Ilustración 8 : Figura 8. Ping desde PC-A a S1 VLAN 4 IP 10.19.8.98.....34
Ilustración 9 : Figura 9. Ping desde PC-A a S1 VLAN 4 IPv6 2001:db8:acad:c: 34
Ilustración 10 : Figura 10. Ping desde PC-A a S2 VLAN 4 IP 10.19.8.99.....34
Ilustración 11 : Figura 11. Ping desde PC-A a S2 VLAN 4 IPv6 2001:db8:c:……..34
Ilustración 12: Figura 12. Ping desde PC-A a PC-B IP address will vary. 35
Ilustración 13 :Figura 13. Ping desde PC-A a PC-B IPv6 2001:db8:acad:b: :50 35
Ilustración 14 : Figura 14. Ping desde PC-A a R1 Bucle IP 209.165.201.1.....35
Ilustración 15 : Figura 15. Ping desde PC-A a R1 Bucle IPv6 2001:db. 35
Ilustración 16 : Figura 16. Ping desde PC-B a R1 Bucle 0 IP 209.165.201.1.....36
Ilustración 17 : Figura 17. Ping desde PC-B a R1 Bucle 0 IPv6 2001:db8 36
Ilustración 18 : Figura 18. Ping desde PC-B a R1 G0/0/1.2 IP 10.19.8.1 36
Ilustración 19 : Figura 19. Ping desde PC-B a R1 G0/0/1.2 IPv6 2001:db8:acad:a:.36
Ilustración 20 : Figura 20. Ping desde PC- a R1 G0/0/1.3 IP 10.19.8.65 37
Ilustración 21 : Figura 21. Ping desde PC-B a R1 IPv6 2001:db8:acad:b: :1 37
Ilustración 22 : Figura 22. Ping desde PC-B a R1 G0/0/1.4 IP 10.19.8.97 37
Ilustración 23 : Figura 23. Ping desde PC-B a R1 G0/0/1.4 IPv6 2001:db8: 37
Ilustración 24 : Figura 24. Ping desde PC-B a S1 VLAN 4 IP 10.19.8.98.....38
Ilustración 25 : Figura 25. Ping desde PC-B S1 VLAN IPv6 2001:db8:aca 38
Ilustración 26 : Figura 26 Ping desde PC-B a S2 VLAN 4 IP . 10.19.8.99.....38
Ilustración 27 : Figura 27. Ping desde PC-B a S2 VLAN 4 IPv6 2001:db8.....38
Ilustración 28 : Figura 28. Escenario 2 Topología.....39

Ilustración 29 : Figura 29 ping de R1 a R2 47
Ilustración 30 : Figura 30 ping de R2 a R3 47
Ilustración 31 : Figura 31 ping desde S1 a R1 VLAN 99 51
Ilustración 32 : Figura 32 ping desde S3 a R1 VLAN 99 51
Ilustración 33 : Figura 33 ping desde S1 a R1 VLAN 21 51
Ilustración 34 : Figura 34 ping desde S3 a R1 VLAN 23 51
Ilustración 35 : Figura 35. Verificación DHCP PC-A 57
Ilustración 36 : Figura 36. Verificación DHCP PC-C 58
Ilustración 37 : Figura 37. Verificación ping de PC-A a PC-C 58
Ilustración 38 : Figura 38. Servidor web 58
Ilustración 39 : Figura 39 Verificación ACL 60

GLOSARIO

Red: Interconexión de un número determinado de computadores mediante dispositivos alámbricos o inalámbricos que mediante impulsos eléctricos, ondas electromagnéticas u otros medios físicos, le permiten enviar.

Cisco: Empresa de origen estadounidense fabricante de dispositivos para redes locales y externa, también presta el servicio de soluciones de red, su objetivo es conectar a todos y demostrar las cosas asombrosas que se pueden lograr con una visión clara del futuro.

Servidor: Es una computadora que, formando parte de una red, provee servicios a otras computadoras denominadas clientes. También se suele denominar con la palabra servidor a una aplicación informática o programa que realiza algunas tareas en beneficio de otras aplicaciones llamadas clientes. Algunos servicios habituales son los servicios de archivos, que permiten a los usuarios almacenar y acceder a los archivos de una computadora y los servicios de aplicaciones, que realizan tareas en beneficio directo del usuario final.

Switch: Es un dispositivo digital de lógica de interconexión de redes de computadores que opera en la capa 2 (nivel de enlace de datos) del modelo OSI. Su función es interconectar dos o más segmentos de red, de manera similar a los puentes (bridges), pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red.

Routers: -Es un enrutador, elemento que marca el camino más adecuado para la transmisión de mensajes en una red completa, esta toma el mejor camino para enviar los datos dependiendo del tipo de protocolo que este cargado, cuenta con un procesador es el más robusto, tiene más procesadores y mucha más capacidad en sus respectivas memorias.

Cableado: -Los tipos de cableado de red más populares son: par trenzado, cable coaxial y fibra óptica, además se pueden realizar conexiones a través de radio o microondas, dependiendo el tipo de red y los requerimientos de la misma, velocidad y longitud se debe considerar el tipo de cable a utilizar
Ethernet. -es un estándar de redes de área local para computadores con acceso al medio por detección de la onda portadora y con detección de colisiones.

Protocolo: -es un sistema de reglas que permiten que dos o más entidades de un sistema de comunicación se comuniquen entre ellas para transmitir información por medio de cualquier tipo de variación de una magnitud física.

Dirección MAC: -media access control, es un identificador de 48 bits (6 bloques hexadecimales) que corresponde de forma única a una tarjeta o dispositivo de red. Se conoce también como dirección física, y es única para cada dispositivo.

LAN: Una red de área local es una red de computadoras que abarca un área reducida a una casa, un departamento o un edificio.

IP: Una dirección IP es un número que identifica, de manera lógica y jerárquica, a una Interfaz en red de un dispositivo que utilice el protocolo IP, que corresponde al nivel de red del modelo TCP/IP.
Modelo TCP/IP. - es una descripción de protocolos de red.

RESUMEN

A través de práctica simulada se obtienen dos estudios de caso topologías diferentes a desarrollar con el objetivo de aprender a configurar diferentes tipos de redes. CISCO la empresa que en cuanto a redes es una de las más experimentadas en diseño e implementación de redes. A través de su plataforma y programas cisco nos enseña a estructurar una red desde lo más básico

El diplomado permite captar la contextualización del uso fundamental de la redes de datos y de internet, también tenemos el uso y configuración de otros dispositivos como lo es la domótica salimos no solo de la parte de configurar computadores a manipular dispositivos remotamente como electrodomésticos o una simple bombilla de nuestra casa, la telefonía IP es también muy utilizada en las empresas y se puede enlazar con internet para no incurrir en gastos adicionales.

En este curso a través del uso de comandos y dispositivos cisco como routers, se aprendió configurar equipos bajo los protocolos IPV4, IPV6 en redes LAN Y WAN; estas redes van de la mano y una es la razón del desarrollo de la otra porque de una red o muchas redes pequeñas podemos enlazar a redes más grandes.

Las topologías presentadas en este informe son un ejemplo de múltiples casos de conexión y configuración por medio de dispositivos cisco además de configuraciones de seguridad tenemos también diferentes tipos de conexión en equipos de cómputo o hosts que representan el punto de acceso de las conexiones en estos dos escenarios.

PALABRAS CLAVE: enrutamiento, ping, ip, configuración, router, host, LAN.

Abstract

Through simulated practice we have to develop two case studies different topologies to develop in order to learn how to configure different types of networks. CISCO the company that in terms of networks is one of the most experienced in network design and implementation. Through its platform and programs, cisco teaches us to structure a network from the basics.

The diploma does not allow us to capture the contextualization of the fundamental use of the data networks and the internet, we also have the use and configuration of other devices such as home automation, we leave not only the part of configuring computers to remotely manipulate devices such as appliances or a simple light bulb of our house, IP telephony is also widely used in companies and can be linked to the internet to avoid incurring additional costs.

In this course, through the use of Cisco commands and devices such as routers, we learned how to configure equipment under the IPV4, IPV6 protocols in LAN and WAN networks; These networks go hand in hand and one is the reason for the development of the other because from one network or many small networks.

we can link to larger networks. The topologies presented in this report are an example of multiple connection and configuration cases through Cisco devices, in addition to security configurations, we also have different types of connection in computers or hosts that represent the access point of the connections in these two scenarios.

KEYWORDS: routing, ping, ip, configuration, router, host, LAN

INTRODUCCIÓN

En todos los ámbitos de la vida actual se es dependiente del acceso tecnológico, a nivel personal y empresarial es fundamental la interacción con redes e internet, de eso depende gran parte de las actividades sociales y laborales; es por eso que el aumento a gran escala de redes a nivel mundial. Todos estamos en conectividad constante, las noticias son de primera mano las transacciones bancarias y compras desde casa y a través del móvil son una realidad, lo que nos conecta y permite la comunicación en todos los ámbitos son la redes tanto físicas como inalámbricas y siempre serán las redes las que interconecten empresas y familias.

En cuanto al motivo que se aplica para la realización de la presente investigación no es más que la infraestructura utilizada en las comunicaciones e internet; las redes de datos son el centro del desarrollo mundial, desde las redes pequeñas hasta las más amplias representan avance y progreso.

El diplomado en desarrollo plantea dos casos a desarrollar para dar solución a requerimientos de red, la topología permite desarrollar soluciones de acceso a diferentes tipos de equipos como routers switches y computadoras, aprendimos a enlazar con proveedores ISP además de diferenciar los tipos de conectividad a través de programas de simulación que pueden mostrarnos tanto la conexión física como la lógica. Es importante resaltar la cantidad de medios y facilidades que actualmente nos permiten tener un análisis más completo del diseño e implementación de una red.

Escenario 1

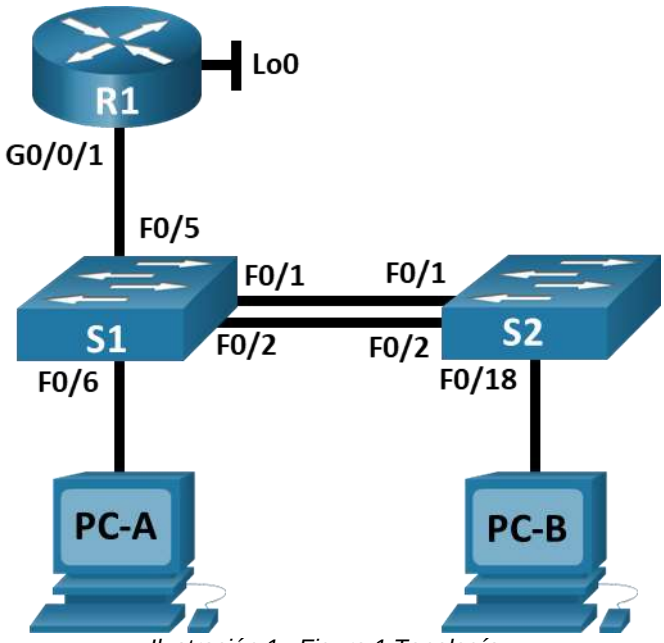


Ilustración 1 : Figura 1 Topología

Figura 1 Topología

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.

Tabla 1. VLAN

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

Tabla 2 : Asignación de direcciones

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
R1 G0/0/1.2	10.19.8.1 /26	No corresponde
R1 G0/0/1.2	2001:db8:acad:a: :1 /64	No corresponde
R1 G0/0/1.3	10.19.8.65 /27	No corresponde
R1 G0/0/1.3	2001:db8:acad:b: :1 /64	No corresponde
R1 G0/0/1.4	10.19.8.97 /29	No corresponde
R1 G0/0/1.4	2001:db8:acad:c: :1 /64	No corresponde
R1 G0/0/1.6	No corresponde	No corresponde
R1 Loopback0	209.165.201.1 /27	No corresponde
R1 Loopback0	2001:db8:acad:209: :1 /64	No corresponde
S1 VLAN 4	10.19.8.98 /29	10.19.8.97
VLAN S1 4	2001:db8:acad:c: :98 /64	No corresponde
S1 VLAN 4	fe80: :98	No corresponde
S2 VLAN 4	10.19.8.99 /29	10.19.8.97
S2 VLAN 4	2001:db8:acad:c: :99 /64	No corresponde
S2 VLAN 4	fe80: :99	No corresponde
PC-A NIC	Dirección DHCP para IPv4	DHCP para puerta de enlace predeterminada IPv4
PC-A NIC	2001:db8:acad:a: :50 /64	fe80::1
PC-B NIC	DHCP para dirección IPv4	DHCP para puerta de enlace predeterminada IPv4
PC-B NIC	2001:db8:acad:b: :50 /64	fe80::1

Nota: No hay ninguna interfaz en el router que admita VLAN 5.

1. Instrucciones

Parte 1: Inicializar y Recargar y Configurar aspectos basicos de los dispositivos

Paso 1: **Inicializar y volver a cargar el router y el switch**

- Borre las configuraciones de inicio y las VLAN del router y del switch y vuelva a cargar los dispositivos.
- Después de recargar el switch, configure la plantilla SDM para que admita IPv6 según sea necesario y vuelva a cargar el switch.
- Antes de continuar, solicite al instructor que verifique la inicialización de los dispositivos.

Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Como configuración inicial en el dispositivo principal R1, desactivamos la busqueda de DNS, además establecemos un nombre de dominio comun para la comunicación en todos los dispositivos de la red. En cuanto a la seguridad establecmos contraseña de acceso a la consola estableciendo longitud mínima de caracteres. En la configuración de la interfases se asignan las que muestra la tabla de direcciones, se configura la G0/0/1 y subinterfaces se configura el Loopback0 en la interface.

Tabla 3 : Paso 2: Configurar R1

Tarea	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R1
Nombre de dominio	router(config)# ip domain-lookup *router(config)#* ***ip domain-name <*** ccna-lab.com ***>*** router(config)# ip name-server <ip-servidor-DNS>
Contraseña cifrada para el modo EXEC privilegiado	Ciscoenpass R1(config)#enable secret ciscoconpass
Contraseña de acceso a la consola	Ciscoconpass R1(config)#line console 0 R1(config-line)#password ciscoenpass R1(config-line)#login
Establecer la longitud mínima para las contraseñas	Router(config)# security passwords min-length 10

Tarea	Especificación
Crear un usuario administrativo en la base de datos local	Nombre de usuario: **admin** Password: **admin1pass**
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	R1(config-line)#line vty 0 4 R1(config-line)#password ciscoenpass R1(config-line)#login
Configurar VTY solo aceptando SSH	R1(config)# ip ssh version 2 R1(config)# line vty 0 15 R1(config-line)# login local R1(config-line)# exit
Cifrar las contraseñas de texto no cifrado	R1(config-line)#service password-encryption
Configure un MOTD Banner	R1(config)#banner motd $Se prohibe el acceso no autorizado.$
Habilitar el routing IPv6	R1(config)#ipv6 unicast-routing

Tarea	Especificación
Configurar interfaz G0/0/1 y subinterfaces	R1(config-if)#interface GigabitEthernet0/0/1.2 R1(config-subif)#encapsulation dot1q 2 R1(config-subif)#description Bikes 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)#interface GigabitEthernet0/0/1.3 R1(config-subif)#encapsulation dot1q 3 R1(config-subif)#description Trikes 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)#interface GigabitEthernet0/0/1.4 R1(config-subif)#encapsulation dot1q 4 R1(config-subif)#description Management 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)#interface GigabitEthernet0/0/1.6 R1(config-subif)#encapsulation dot1q 6 native R1(config-subif)#description native

Tarea	Especificación
Configure el Loopback0 interface	R1(config-subif)#interface Loopback0 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-if)#no shutdown R1(config-if)#
Generar una clave de cifrado RSA	Módulo de 1024 bits

Paso 2: **Configure S1 y S2.**

Las tareas de configuración incluyen lo siguiente:

El escenario conformado por dos switch comunicados a traves de F0/1 y F0/2 deben ser configurados con los mismos pasos del dispositivo R1 su configuracion inicial como host, contraseñas, nombre de dominio S1 con VLAN 4 S2 con VLAN 4 IPV4, IPV6. Puertas de enlace predeterminadas.

Tabla 4: Paso 3: Configure S1 y S2.

Tarea	Especificación
Desactivar la búsqueda DNS.	switch(config)#no ip domain-lookup
Nombre del switch	switch(config)#hostname R1
Nombre de dominio	S1(config)#ip domain name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	**Ciscoenpass** S1(config)#enable secret ciscoenpass S1(config)#ip domain name ccna-lab.com

Tarea	Especificación
Contraseña de acceso a la consola	**Ciscoconpass** S1(config)#line console 0 S1(config-line)#password ciscoconpass S1(config-line)#login
Crear un usuario administrativo en la base de datos local	S1(config)#username admin password admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	S1(config-line)#line vty 0 15 S1(config-line)#login local S1(config-line)#transport input ssh S1(config-line)#exit
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S1(config)# ip ssh version 2 S1(config)# line vty 0 15 S1(config-line)# login local S1(config-line)# exit
Cifrar las contraseñas de texto no cifrado	S1(config-line)#service password-encryption
Configurar un MOTD Banner	S1(config)#banner motd $Se prohibe el acceso no autorizado.$
Generar una clave de cifrado RSA	S1(config)#ip domain-name span.com S1(config)#crypto key generate rsa general-keys modulus 1024 S1(config)#username Bob secret cisco S1(config)#line vty 0 4 S1(config-line)#login local S1(config-line) #transport insut ssh S1(config-line) #exit

Configurar la interfaz de administración (SVI)	**S1**(config-if)#interface vlan4 s1(config-subif)#description Management S1(config-if)#ip address 10.19.8.98 255.255.255.248 S1(config-if)#no shut S1(config-if)#ip default-gateway 10.19.8.97 S1(config)#exit S1(config-if)#ipv6 address 2001:db8:acad:c::98/64 S1(config-if)#ipv6 address FE80::98 link-local S1(config-if)#no shutdown S1(config-if)#end **S2** Switch>enable Switch#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#no ip domain-lookup Switch(config)#hostname S2 S2(config)#ip domain name ccna-lab.com S2(config)#enable secret ciscoenpass S2(config)#line vty 0 15 S2(config-line)#password ciscoconpass S2(config-line)#login S2(config-line)#transport input ssh S2(config-line)#exit S2(config)#service password-encryption S2(config)#banner motd #Unauthorized access is strictly prohibited. #

Tarea	Especificación
	S2(config)#crypto key generate rsa general-keys modulus 1024 The name for the keys will be: S2.ccna-lab.com % The key modulus size is 1024 bits % Generating 1024 bit RSA keys, keys will be non-exportable...[OK] *Mar 1 0:36:2.307: %SSH-5-ENABLED: SSH 1.99 has been enabled S2#configure terminal Enter configuration commands, one per line. End with CNTL/Z. S2(config)#interface vlan4 S2(config-if)#description Management S2(config-if)#ip address 10.19.8.99 255.255.255.248 S2(config-if)#no shutdown S2(config-if)#ipv6 address 2001:db8:acad:c::99/64 S2(config-if)#ipv6 address FE80::99 link-local S2(config-if)#no shutdown S2(config-if)#
Configuración del gateway predeterminado	S1(config)# interface vlan1 S1(config-vlan)#ip address 10.19.8.97 255.255.255.0 S1(config-vlan)# no shut

Parte 2: Configuración de la infraestructura de red (VLAN, Trunking, EtherChannel)

Paso 3: **Configurar S1**

La configuración del S1 incluye las siguientes tareas:

El paso 4 consiste en realizar varias configuraciones nombrar las VLAN en dispositivos S1, ademas de establecer el rango de las interfaces creando troncales de que utilicen VLAN 6 como nativas.

Tabla 5. Configuración de la infraestructura de red (VLAN, Trunking, EtherChannel)

Tarea	Especificación
Crear VLAN	S1(config)#vlan 2 S1(config-vlan)#name Bikes S1(config-vlan)#vlan 3 S1(config-vlan)#name Trikes S1(config-vlan)#vlan 4 S1(config-vlan)#name Management S1(config-vlan)#vlan 5 S1(config-vlan)#name Parking S1(config-vlan)#vlan 6 S1(config-vlan)#name Native
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	S1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. S1(config)#interface range f0/1-2 S1(config-if-range)#switchport trunk encapsulation dot1q S1(config-if-range)#switchport trunk native vlan 6 S1(config-if-range)# S1(config)#interface range f0/5 S1(config-if-range)#switchport trunk encapsulation dot1q S1(config-if-range)#switchport trunk native vlan 6 S1(config-if-range)#

Tarea	Especificación
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	S1(config)#interface range f0/1-2 S1(config-if-range)#channel-group 1 mode active S1(config-if-range)# Creating a port-channel interface Port-channel 1 S1(config-if-range)#interface port-channel 1 S1(config-if)#switchport mode trunk Command rejected: An interface whose trunk encapsulation is "Auto" can not be configured to "trunk" mode.. S1(config-if)#switchport trunk native vlan 6 S1(config-if)#
Configurar el puerto de acceso de host para VLAN 2	Interface F0/6 S1(config)#Interface F0/6 S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 2 S1(config-if)# %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down S1(config-if)#switchport port-security S1(config-if)#
Configurar la seguridad del puerto en los puertos de acceso	Permitir 3 direcciones MAC S1(config-if)#switchport port-security maximum 3

Tarea	Especificación
	Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar S1(config)#interface range f0/3-4 S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 5 S1(config-if-range)#description interface no use S1(config-if-range)# no shutdown S1(config)#interface range f0/7-24 S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 5 S1(config-if-range)#description interface no use S1(config-if-range)#no shutdown S1(config)#interface range g0/1-2 S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 5 S1(config-if-range)#description interface no use
Proteja todas las interfaces no utilizadas	S1(config-if-range)#no shutdown

Paso 4: **Configure el S2.**

S2 al igual que en S1 nombramos las VLAN creamos las troncales por VLAN 6 como nativa, creamos un grupo de puertos Etherchannel de capa 2 usando F0/1 y F0/2 además del VLAN 3 como acceso host.

Entre las tareas de configuración de S2 se incluyen las siguientes:

Tabla 6 : Paso 5: Configure el S2.

Tarea	Especificación
Crear VLAN	S2(config)#vlan 2 S2(config-vlan)#name Bikes S2(config-vlan)#vlan 3 S2(config-vlan)#name Trikes S2(config-vlan)#vlan 4 S2(config-vlan)#name Management S2(config-vlan)#vlan 5 S2(config-vlan)#name Parking S2(config-vlan)#vlan 6 S2(config-vlan)#name Native
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	Interfaces F0/1 y F0/2 S2#configure terminal Enter configuration commands, one per line. End with CNTL/Z. S2(config)#interface range f0/1-2 S2(config-if-range)#switchport trunk encapsulation dot1q S2(config-if-range)#switchport trunk native vlan 6 S2(config-if-range)#

Tarea	Especificación
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	Usar el protocolo LACP para la negociación S2(config)#interface range f0/1-2 S2(config-if-range)#channel-group 1 mode active S2(config-if-range)#Creating a port-channel interface Port-channel 1 S2(config-if-range)#interface port-channel 1 S2(config-if)#switchport mode trunk S2(config-if)#switchport trunk native vlan 6 S2(config-if)#
Configurar el puerto de acceso del host para la VLAN 3	Interfaz F0/18 S2(config)#Interface F0/18 S2(config-if)#switchport mode access S2(config-if)#switchport access vlan 3 S2(config-if)#switchport port-security S2(config-if)#
Configure port-security en los access ports	permite 3 MAC addresses permite 3 MAC addresses S2(config-if)#switchport port-security maximum 3

	Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar S2(config)#Interface F0/18 S2(config-if)#switchport mode access S2(config-if)#switchport access vlan 3 S2(config-if)#switchport port-security S2(config-if)#switchport port-security maximum 3 S2(config-if)#exit S2(config)#interface range f0/3-17 S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 5 S2(config-if-range)#description interface no use S2(config-if-range)#no shutdown S2(config-if-range)# S2(config-if-range)#interface range f0/19-24 S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 5 S2(config-if-range)#description interface no use S2(config-if-range)#no shutdown S2(config-if-range)# S2(config-if-range)#interface range g0/1-2 S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 5 S2(config-if-range)#description interface no use S2(config-if-range)#no shutdown
Asegure todas las interfaces no utilizadas.	S2(config-if-range)#

Parte 2: Configurar soporte de host

Paso 1: Configure R1

Las tareas de configuración para R1 incluyen las siguientes:

Importante esta parte de configuración del router, se crean las rutas predeterminadas y un grupo DHCP para VLAN 2 pool de las últimas 10 direcciones se configuran IPV4 en VLAN 6 también configuramos IPV4 para VLAN 3.excluyendo 86 a 95.

Tabla 7: Paso 1: Configure R1

Tarea		Especificación
Configure Default Routing	R1(config)#Interface Loopback 0 R1(config-if)#Ip route 0.0.0.0 0.0.0.0 Loopback 0 R1(config)#Ipv6 route ::/0 Loopback 0 R1(config)#	Crear rutas predeterminadas para IPv4 e IPv6 que dirijan el tráfico a la interfaz Loopback 0
Configurar IPv4 DHCP para VLAN 2	R1(config)#Ip dhcp pool vlan2-Bikes R1(dhcp-config)#Network 10.19.8.0 255.255.255.192 R1(dhcp-config)#Domain-name ccna-a.net R1(dhcp-config)#Default-router 10.19.8.1 R1(dhcp-config)#	Cree un grupo DHCP para VLAN 2, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio ccna-a.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada

Tarea		Especificación
Configurar DHCP IPv4 para VLAN 3	R1(config)#Ip dhcp pool vlan3-Trikes R1(dhcp-config)#Network 10.19.8.64 255.255.255.224 R1(dhcp-config)#Domain-name ccna-a.net R1(dhcp-config)#Default-router 10.19.8.65	Cree un grupo DHCP para VLAN 3, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio ccna-b.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada

Paso 2: **Configurar los servidores**

Configure los equipos host PC-A y PC-B para que utilicen DHCP para IPv4 y asigne estáticamente las direcciones IPv6 GUA y Link Local. Después de configurar cada servidor, registre las configuraciones de red del host con el comando **ipconfig /all**.

Tabla 8 Paso 2: Configurar los servidores

PC-A Network Configuration	
Descripción	*0002.1612.582D*
Dirección física	*00D0.D3B7.B10E*
Dirección IP	*10.19.8.54*
Máscara de subred	*255.255.255.192*
Gateway predeterminado	*FE80::1*
Gateway predeterminado IPv6	*FE80::1*

Tabla 9. Configuración de red de PC-A

Configuración de red de PC-A	
Descripción	*0000.0CE4.D30C*
Dirección física	*0002.1612.582D*
Dirección IP	*10.19.8.85*
Máscara de subred	*255.255.255.224*

Configuración de red de PC-A	
Gateway predeterminado	*FE80::1*
Gateway predeterminado IPv6	*FE80::1*

Parte 3: Probar y verificar la conectividad de extremo a extremo

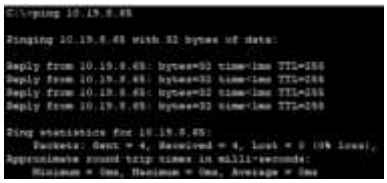
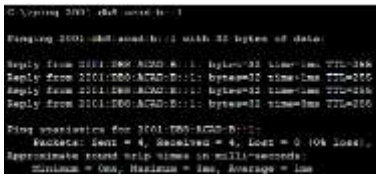
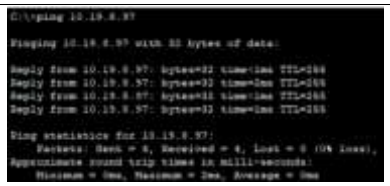
Use el comando ping para probar la conectividad IPv4 e IPv6 entre todos los dispositivos de red.

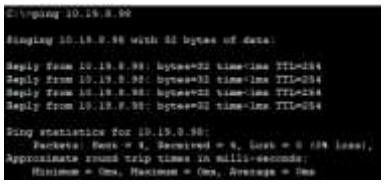
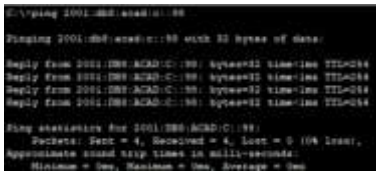
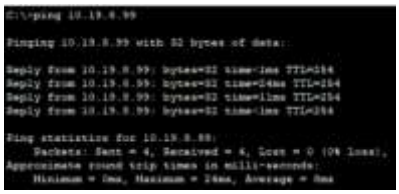
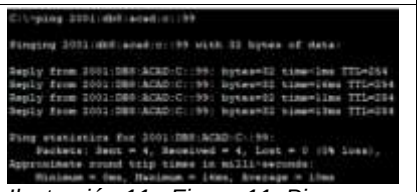
Nota: Si fallan los pings en las computadoras host, desactive temporalmente el firewall de la computadora y vuelva a realizar la prueba.

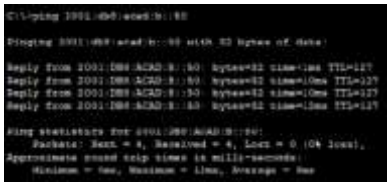
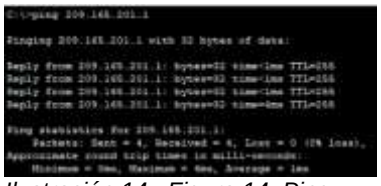
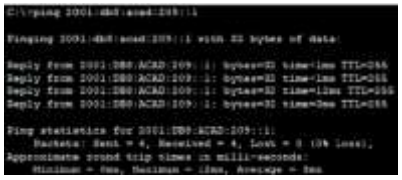
Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

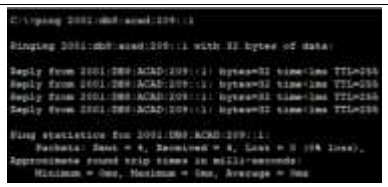
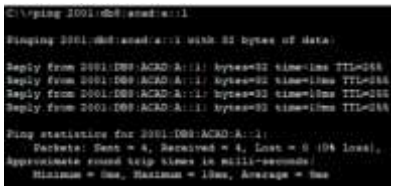
Tabla 10 : Parte 3: Probar y verificar la conectividad de extremo a extremo

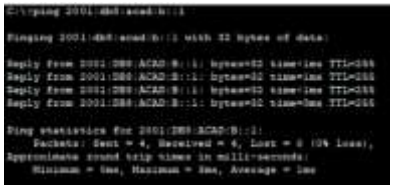
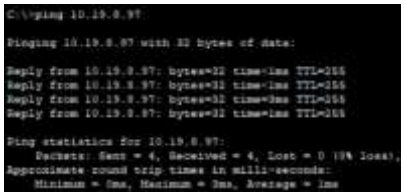
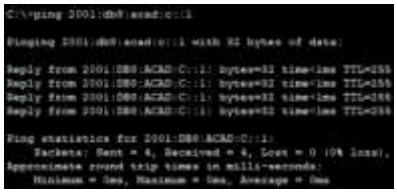
Desde	**A**	**de Internet**	**Dirección IP**	**Resultados de ping**
PC-A	R1, G0/0/1.2	Dirección	10.19.8.1	 *Ilustración 2:Figura 2. Ping desde PC-A a R1 G0/0/1.2 IP 10.19.8.1*
PC-A	*R1, G0/0/1.2*	IPv6	2001:db8:acad:a::1	 *Ilustración 3: Figura 3. Ping desde PC-A a R1 G0/0/1.2 IPv6 2001:db8:acad:a: :1*

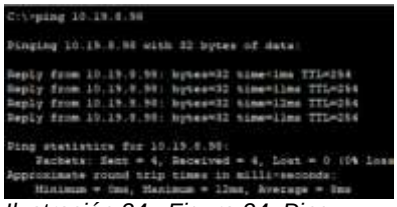
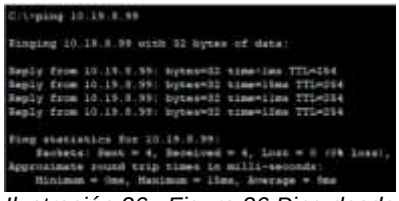
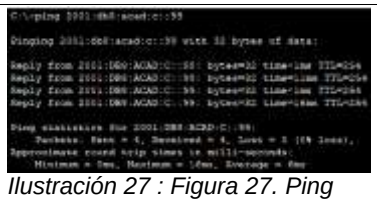
Desde	A	de Internet	Dirección IP	Resultados de ping
PC-A	R1, G0/0/1.3	Dirección	10.19.8.65	 *Ilustración 4 : Figura 4. Ping desde PC-A a R1 G0/0/1.3 IP 10.19.8.65*
PC-A	*R1, G0/0/1.3*	IPv6	2001:db8:acad:b::1	 *Ilustración 5 : Figura 5. Ping desde PC-A a R1 G0/0/1.3 IPv6 2001:db8:acad:b: :1*
PC-A	R1, G0/0/1.4	Dirección	10.19.8.97	 *Ilustración 6 : Figura 6. Ping desde PC-A a R1 G0/0/1.4 IP 10.19.8.97*
PC-A	*R1, G0/0/1.4*	IPv6	2001:db8:acad:c::1	 *Ilustración 7 : Figura 7. Ping desde PC-A a R1 G0/0/1.4 IPv6 2001:db8:acad:c: :1*

Desde	A	de Internet	Dirección IP	Resultados de ping
PC-A	S1, VLAN 4	Dirección	10.19.8.98	 *Ilustración 8 : Figura 8. Ping desde PC-A a S1 VLAN 4 IP 10.19.8.98*
PC-A	*S1, VLAN 4*	IPv6	2001:db8:acad:c: :98	 *Ilustración 9 : Figura 9. Ping desde PC-A a S1 VLAN 4 IPv6 2001:db8:acad:c: :98*
PC-A	S2, VLAN 4	Dirección	10.19.8.99.	 *Ilustración 10 : Figura 10. Ping desde PC-A a S2 VLAN 4 IP 10.19.8.99*
PC-A	*S2, VLAN 4*	IPv6	2001:db8:acad:c: :99	 *Ilustración 11 : Figura 11. Ping desde PC-A a S2 VLAN 4 IPv6 2001:db8:acad:c: :99*

Desde	A	de Internet	Dirección IP	Resultados de ping
PC-A	PC-B	Dirección	IP address will vary.	 *Ilustración 12: Figura 12. Ping desde PC-A a PC-B IP address will vary.*
PC-A	*PC-B*	IPv6	2001:db8:acad:b::50	 *Ilustración 13 :Figura 13. Ping desde PC-A a PC-B IPv6 2001:db8:acad:b::50*
PC-A	R1 Bucle 0	Dirección	209.165.201.1	 *Ilustración 14 : Figura 14. Ping desde PC-A a R1 Bucle IP 209.165.201.1*
PC-A	*R1 Bucle 0*	IPv6	2001:db8:acad:209::1	 *Ilustración 15 : Figura 15. Ping desde PC-A a R1 Bucle IPv6 2001:db8:acad:209::1*

Desde	A	de Internet	Dirección IP	Resultados de ping
PC-B	R1 Bucle 0	Dirección	209.165.201.1	 *Ilustración 16 : Figura 16. Ping desde PC-B a R1 Bucle 0 IP 209.165.201.1*
PC-B	*R1 Bucle 0*	IPv6	2001:db8:acad:209: :1	 *Ilustración 17 : Figura 17. Ping desde PC-B a R1 Bucle 0 IPv6 2001:db8:acad:209: :1*
PC-B	R1, G0/0/1.2	Dirección	10.19.8.1	 *Ilustración 18 : Figura 18. Ping desde PC-B a R1 G0/0/1.2 IP 10.19.8.1*
PC-B	*R1, G0/0/1.2*	IPv6	2001:db8:acad:a: :1	 *Ilustración 19 : Figura 19. Ping desde PC-B a R1 G0/0/1.2 IPv6 2001:db8:acad:a: :1*

Desde	A	de Internet	Dirección IP	Resultados de ping
PC-B	R1, G0/0/1.3	Dirección	10.19.8.65	 *Ilustración 20 : Figura 20. Ping desde PC- a R1 G0/0/1.3 IP 10.19.8.65*
PC-B	*R1, G0/0/1.3*	IPv6	2001:db8:acad:b::1	 *Ilustración 21 : Figura 21. Ping desde PC-B a R1 IPv6 2001:db8:acad:b: :1*
PC-B	R1, G0/0/1.4	Dirección	10.19.8.97	 *Ilustración 22 : Figura 22. Ping desde PC-B a R1 G0/0/1.4 IP 10.19.8.97*
PC-B	*R1, G0/0/1.4*	IPv6	2001:db8:acad:c::1	 *Ilustración 23 : Figura 23. Ping desde PC-B a R1 G0/0/1.4 IPv6 2001:db8:acad:c: :1*

Desde	A	de Internet	Dirección IP	Resultados de ping
PC-B	S1, VLAN 4	Dirección	10.19.8.98	 *Ilustración 24 : Figura 24. Ping desde PC-B a S1 VLAN 4 IP 10.19.8.98*
PC-B	*S1, VLAN 4*	IPv6	2001:db8:acad:c: :98	 *Ilustración 25 : Figura 25. Ping desde PC-B S1 VLAN IPv6 2001:db8:acad:c: :98*
PC-B	S2, VLAN 4	Dirección	10.19.8.99.	 *Ilustración 26 : Figura 26 Ping desde PC-B a S2 VLAN 4 IP . 10.19.8.99*
PC-B	*S2, VLAN 4*	IPv6	2001:db8:acad:c: :99	 *Ilustración 27 : Figura 27. Ping desde PC-B a S2 VLAN 4 IPv6 2001:db8:acad:c: :99*

Escenario 2

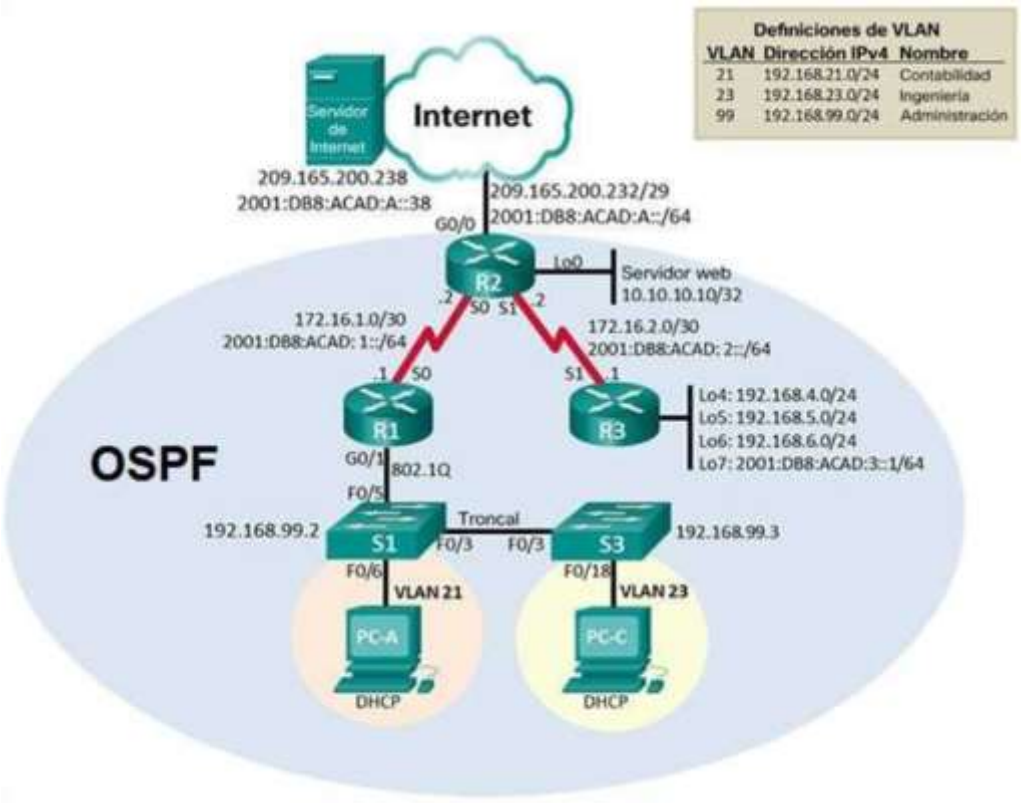


Ilustración 28 : Figura 28. Escenario 2 Topología

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

Parte 1: Inicializar dispositivos

Paso 1: Inicializar y volver a cargar los routers y los switches

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

Antes de continuar, solicite al instructor que verifique la inicialización de los dispositivos.

Eliminamos archivos de configuración en el dispositivo a configurar recargamos el router para empezar a configurar de ceros nombrando el dispositivo estableciendo contraseñas.

Tabla 11 : Paso 1: Inicializar y volver a cargar los routers y los switches

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

Parte 2: Configurar los parámetros básicos de los dispositivos

Paso 1: Configurar la computadora de Internet

Las tareas de configuración del servidor de Internet incluyen lo siguiente (para obtener información de las direcciones IP, consulte la topología): el cuadro de direcciones muestra el direccionamiento del host para acceso a internet.

Tabla 12 : Paso 1: Configurar la computadora 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:DB8:ACAD:A::2/64
Gateway predeterminado IPv6	2001:DB8:ACAD:2::1

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

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

R1 desactivar búsqueda de DNS nombrar el dispositivo establecer seguridad con cifrado, contraseñas configurando interfaz S0/0/0 IPV4 IPV6 con direcciones previamente establecidas.

Tabla 13 : Paso 2: Configurar R1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R1
Contraseña de exec privilegiado cifrada	R1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	R1(config)#line console 0 R1(config-line)#password ciscoconpass R1(config-line)#login
Contraseña de acceso Telnet	R1(config-line)#line vty 0 4 R1(config-line)#password ciscoconpass R1(config-line)#login
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Mensaje MOTD	R1(config)#banner motd $Se prohibe el acceso no autorizado.$
Interfaz S0/0/0	R1(config)#interface serial 0/0/0 R1(config-if)#description Connection to R2 R1(config-if)#ip address 172.16.1.1 255.255.255.252 R1(config-if)#ipv6 address 2001:DB8:ACAD:1::1/64 R1(config-if)#clock rate 128000 R1(config-if)#no shutdown
Rutas predeterminadas	R1(config)#ip route 0.0.0.0 0.0.0.0 serial 0/0/0 R1(config)#ipv6 route ::/0 s0/0/0

Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

En R2 realizamos configuración inicial hostname R2 desactivar búsqueda de DNS, configuramos con el direccionamiento establecido los puertos interfaz S0/0/0, S0/0/1, G0/0 ademas de la interfaz loopback con ip 10.10.10.10

Tabla 14 : Paso 3: Configurar R2

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R2
Contraseña de exec privilegiado cifrada	R2(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	R2(config)#line console 0 R2(config-line)#password ciscoconpass R2(config-line)#login
Contraseña de acceso Telnet	R2(config-line)#line vty 0 4 R2(config-line)#password ciscoconpass R2(config-line)#login
Cifrar las contraseñas de texto no cifrado	R2(config-line)#service password-encryption
Habilitar el servidor HTTP	R2(config)#ip http server
Mensaje MOTD	R2(config)#banner motd $Se prohibe el acceso no autorizado.$
Interfaz S0/0/0	R2(config)#interface serial 0/0/0 R2(config-if)#description Connection to R1 R2(config-if)#ip address 172.16.1.2 255.255.255.252 R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64 R2(config-if)#no shutdown

Interfaz S0/0/1	R2(config)#interface serial 0/0/1 R2(config-if)#description Connection to R3 R2(config-if)#ip address 172.16.2.2 255.255.255.252 R2(config-if)#ipv6 address 2001:DB8:ACAD:2::2/64 R2(config-if)#clock rate 128000 R2(config-if)#no shutdown
Interfaz G0/0 (simulación de Internet)	R2(config)#interface gigabitEthernet 0/0 R2(config-if)#description Connection to Internet R2(config-if)#ip address 209.165.200.233 255.255.255.248 R2(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64 R2(config-if)#no shutdown
Interfaz loopback 0 (servidor web simulado)	R2(config-if)#Interface Loopback0 R2(config-if)#ip address 10.10.10.10 255.255.255.255
Ruta predeterminada	R2(config)#ip route 0.0.0.0 0.0.0.0 gigabitEthernet 0/0 R2(config)#ipv6 route ::/0 gigabitEthernet 0/0

Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Configuración inicial como en todos los dispositivos además de configurar interfaz S0/0/1 IPV4 IPV6 con direcciones establecidas con el comando no shutdown activamos interfaz, este router trabajaría con interfaz loopback 4, 5, 6, 7 con direcciones en el rango 192.168.4.1, 192.168.5.1, 192.168.6.1, 192.168.7,1 mascara 255.255.255.0, establecemos rutas predeterminadas.

Tabla 15 : Paso 4: Configurar R3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R3

Contraseña de exec privilegiado cifrada	R3(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	R3(config)#line console 0 R3(config-line)#password ciscoconpass R3(config-line)#login
Contraseña de acceso Telnet	R3(config-line)#line vty 0 4 R3(config-line)#password ciscoconpass R3(config-line)#login
Cifrar las contraseñas de texto no cifrado	R3(config-line)#service password-encryption
Mensaje MOTD	R3(config)#banner motd $Se prohibe el acceso no autorizado.$
Interfaz S0/0/1	R3(config)#interface serial 0/0/1 R3(config-if)#description Connection to R2 R3(config-if)#ip address 172.16.2.1 255.255.255.252 R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64 R3(config-if)#no shutdown
Interfaz loopback 4	R3(config-if)#Interface Loopback4 R3(config-if)#ip address 192.168.4.1 255.255.255.0
Interfaz loopback 5	R3(config-if)#Interface Loopback5 R3(config-if)#ip address 192.168.5.1 255.255.255.0
Interfaz loopback 6	R3(config-if)#Interface Loopback6 R3(config-if)#ip address 192.168.6.1 255.255.255.0
Interfaz loopback 7	R3(config-if)#Interface Loopback7 R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64
Rutas predeterminadas	R3(config)#ip route 0.0.0.0 0.0.0.0 serial 0/0/1 R3(config)#ipv6 route ::/0 serial 0/0/1

Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

En este caso S1 se configura incialmente desactivando búsqueda de DNS configuración de seguridad con contraseñas y mensaje de MOTD.

Tabla 16 : Paso 5: Configurar S1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S1
Contraseña de exec privilegiado cifrada	S1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	S1(config)#line console 0 S1(config-line)#password ciscoconpass S1(config-line)#login
Contraseña de acceso Telnet	S1(config-line)#line vty 0 4 S1(config-line)#password ciscoconpass S1(config-line)#login
Cifrar las contraseñas de texto no cifrado	S1(config-line)#service password-encryption
Mensaje MOTD	S1(config)#banner motd $Se prohibe el acceso no autorizado.$

Para realizar la configuración de switch 3 S3, se realiza la misma configuración que en S1, pero con los datos que correspondan a la configuración de S3. Los datos de configuración se pueden evidenciar en la tabla a continuación

Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Dentro de la configuración del dispositivo switch se realiza igual que en router la inicialización del dispositivo.

Tabla 17 : Paso 6: Configurar el S3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S3
Contraseña de exec privilegiado cifrada	S3(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	S3(config)#line console 0 S3(config-line)#password ciscoconpass S3(config-line)#login
Contraseña de acceso Telnet	S3(config-line)#line vty 0 4 S3(config-line)#password ciscoconpass S3(config-line)#login
Cifrar las contraseñas de texto no cifrado	S3(config-line)#service password-encryption
Mensaje MOTD	S3(config)#banner motd $Se prohibe el acceso no autorizado.$

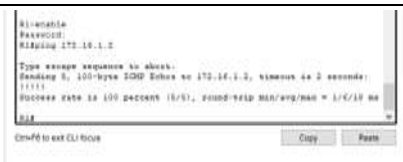
Paso 7: Verificar la conectividad de la red

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

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

Verificando la conectividad de los dispositivos se utiliza el comando ping desde los equipos los routers principales desde R1 a R2 por los puertos serial S0/0/0 hasta S0/0/1 direcciones 172.16.1.2 a 172.16.2.1

Tabla 18: Paso 7: Verificar la conectividad de la red

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	 *Ilustración 29 : Figura 29 ping de R1 a R2*
R2	R3, S0/0/1	172.16.2.1	 *Ilustración 30 : Figura 30 ping de R2 a R3*
PC de Internet	Gateway predeterminado	209.165.200.233	Pinging 2001:DB8:ACAD:A::1with 32 bytes of data:Replyfrom2001:DB8:ACAD:A::1:bytes=32 time<1ms TTL=255 Replyfrom2001:DB8:ACAD:A::1:bytes=32 time<1ms TTL=255 Replyfrom2001:DB8:ACAD:A::1:bytes=32 time<1ms TTL=255 Replyfrom2001:DB8:ACAD:A::1:bytes=32 time=1ms TTL=255Pingstatisticsfor 2001:DB8:ACAD:A::1:Packets: Sent = 4, Received= 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds:Minimum = 0ms, Maximum= 1ms, Average = 0ms

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

Paso 1: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Configurando la VLAN 21 con nombre contabilidad también la VLAN 23 con nombre ingeniería y VLAN 99 con nombre administración también asignamos el Gateway predeterminado establecemos troncales en F0/3 y F0/5 también rangos de los demás puertos de acceso

Tabla 19 : Paso 1: Configurar S1

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	S1(config)#vlan 21 S1(config-vlan)#name Contabilidad S1(config-vlan)#vlan 23 S1(config-vlan)#name Ingenieria S1(config-vlan)#vlan 99 S1(config-vlan)#name Administracion
Asignar la dirección IP de administración.	S1(config)#interface vlan 99 S1(config-if)#ip address 192.168.99.2 255.255.255.0 S1(config-if)#no shutdown
Asignar el gateway predeterminado	S1(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	S1(config)#interface fastEthernet 0/3 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1
Forzar el enlace troncal en la interfaz F0/5	S1(config-if)#interface fastEthernet 0/5 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	S1(config-if)#interface range f0/1-2, f0/4, f0/6-24, g0/1-2 S1(config-if-range)#switchport mode access
Asignar F0/6 a la VLAN 21	S1(config-if-range)#interface fastEthernet 0/6 S1(config-if)#switchport access vlan 21
Apagar todos los puertos sin usar	S1(config-if)#interface range f0/1-2, f0/4, f0/7-24, g0/1-2 S1(config-if-range)#shutdown

Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

En S3 creamos las VLAN al igual que en S1 contabilidad, ingeniería, y administración la VLAN 99 con la ip 192.168.99.3 ademas forzamos enlaces troncales en F0/3.

Tabla 20 :Paso 2: Configurar el S3

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	S3(config)#vlan 21 S3(config-vlan)#name Contabilidad S3(config-vlan)#vlan 23 S3(config-vlan)#name Ingenieria S3(config-vlan)#vlan 99 S3(config-vlan)#name Administracion
Asignar la dirección IP de administración	S3(config-vlan)#interface vlan 99 S3(config-if)#ip address 192.168.99.3 255.255.255.0 S3(config-if)#no shutdown
Asignar el gateway predeterminado.	S3(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	S3(config)#interface fastEthernet 0/3 S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	S3(config)#interface range f0/1-2, f0/4-24, g0/1-2 S3(config-if-range)#switchport mode access
Asignar F0/18 a la VLAN 21	S3(config-if-range)#interface fastEthernet 0/18 S3(config-if)#switchport access vlan 23
Apagar todos los puertos sin usar	S3(config-if)#interface range f0/1-2, f0/4-17, f0/19-24, g0/1-2 S3(config-if-range)#shutdown

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

En este paso configuramos subinterfaz 802.1Q-21 en G01 802.1Q-23 en G01

802.1Q-24 en G01 802.1Q-99 en G01 con encapsulación dot1Q-23 finalmente activamos la interfaz.

Tabla 21 : Paso 3: Configurar R1

Elemento o tarea de configuración	**Especificación**
Configurar la subinterfaz 802.1Q .21 en G0/1	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
Configurar la subinterfaz 802.1Q .23 en G0/1	R1(config-subif)#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
Configurar la subinterfaz 802.1Q .99 en G0/1	R1(config-subif)#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
Activar la interfaz G0/1	R1(config-subif)#int g0/1 R1(config-if)#no shutdown

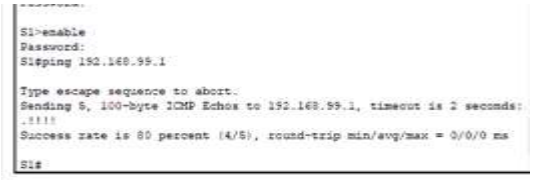
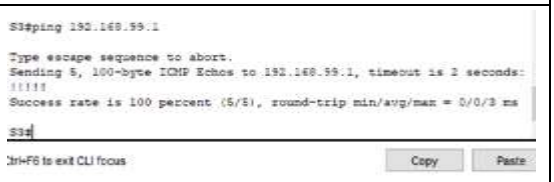
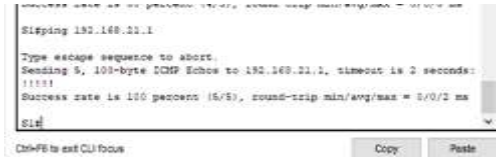
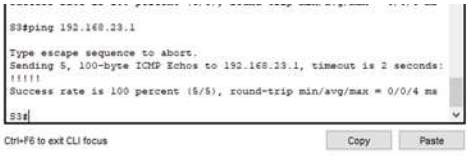
Paso 4: Verificar la conectividad de la red

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

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

Verificando desde S1 con ping a la VLAN 99 dirección ip 192.168.99.1 hacemos pin a esa dirección y a la VLAN 99 desde S3 a R1 a la dirección 192.168.99.1 encontrando respuesta satisfactoria en todas las pruebas.

Tabla 22 : Paso 4: Verificar la conectividad de la red

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	 *Ilustración 31 : Figura 31 ping desde S1 a R1 VLAN 99*
S3	R1, dirección VLAN 99	192.168.99.1	 *Ilustración 32 : Figura 32 ping desde S3 a R1 VLAN 99*
S1	R1, dirección VLAN 21	192.168.21.1	 *Ilustración 33 : Figura 33 ping desde S1 a R1 VLAN 21*
S3	R1, dirección VLAN 23	192.168.23.1	 *Ilustración 34 : Figura 34 ping desde S3 a R1 VLAN 23*

Parte 4: Configurar el protocolo de routing dinámico OSPF

Paso 1: Configurar OSPF en el R1

Las tareas de configuración para R1 incluyen las siguientes:

Este protocolo de enrutamiento abierto nos permite escalar las redes WAN, empezamos configurando el enlazando las direcciones pre establecidas con los puertos de R1 GigabitEthernet0/1.21, GigabitEthernet0/1.23, GigabitEthernet0/1.99

Tabla 23 : Paso 1: Configurar OSPF en el R1

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R2(config)#router ospf R2(config-router)#version 3
Anunciar las redes conectadas directamente	R1(config-router)#do show ip route connected C 172.16.1.0/30 is directly connected, Serial0/0/0 C 192.168.21.0/24 is directly connected, GigabitEthernet0/1.21 C 192.168.23.0/24 is directly connected, GigabitEthernet0/1.23 C 192.168.99.0/24 is directly connected, GigabitEthernet0/1.99 R1(config-router)#network 172.16.1.0 R1(config-router)#network 192.168.21.0 R1(config-router)#network 192.168.23.0 R1(config-router)#network 192.168.99.0
Establecer todas las interfaces LAN como pasivas	R1(config-router)#passive-interface gigabitEthernet 0/1.21 R1(config-router)#passive-interface gigabitEthernet 0/1.23 R1(config-router)#passive-interface gigabitEthernet 0/1.99

Desactive la sumarización automática	R1(config-router)#no auto-summary

Paso 2: Configurar OSPF en el R2

La configuración del R2 incluye las siguientes tareas:

En este paso configuramos también área 0 en R2 con sus loopback 0 en el serial 0/0/0 también anunciamos las redes conectadas, establecemos loopback como pasiva y desactivamos sumarizacion con el comando R2(config-router)#no auto-summary

Tabla 24 : Paso 2: Configurar OSPF en el R2

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R2(config)#router osfp R2(config-router)#version 3
Anunciar las redes conectadas directamente	R2(config-router)#do show ip route connected C 10.10.10.10/32 is directly connected, Loopback0 C 172.16.1.0/30 is directly connected, Serial0/0/0 C 172.16.2.0/30 is directly connected, Serial0/0/1 C 209.165.200.232/29 is directly connected, GigabitEthernet0/0 R2(config-router)#network 10.10.10.10 R2(config-router)#network 172.16.1.0 R2(config-router)#network 172.16.2.0
Establecer la interfaz LAN (loopback) como pasiva	R2(config-router)#passive-interface loopback 0
Desactive la sumarización automática.	R2(config-router)#no auto-summary

Paso 3: Configurar OSPFv3 en el R2

La configuración del R3 incluye las siguientes tareas:

En R3 configuramos área 0 como en los otros dispositivos igualmente anunciamos las redes conectadas y hacemos configuración del loopback como pasiva.

Tabla 25 : Paso 3: Configurar OSPFv3 en el R2

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R2(config)# ipv6 router ospf 1 R3(config-rtr)# router-id 3.3.3.3
Anunciar redes IPv4 conectadas directamente	R2(config-router)#do show ip route connected C 172.16.2.0/30 is directly connected, Serial0/0/1 C 192.168.4.0/24 is directly connected, Loopback4 C 192.168.5.0/24 is directly connected, Loopback5 C 192.168.6.0/24 is directly connected, Loopback6 R2(config-router)#network 172.16.2.0 R2(config-router)#network 192.168.4.0 R2(config-router)#network 192.168.5.0 R2(config-router)#network 192.168.6.0
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	R2(config-router)#passive-interface loopback 4 R2(config-router)#passive-interface loopback 5 R2(config-router)#passive-interface loopback 6
Desactive la sumarización automática.	R2(config-router)#no auto-summary

Paso 4: Verificar la información de OSPF

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

Los comandos utilizados para la verificación de OSPF son los mostrados a continuación.

Tabla 26: Paso 4: Verificar la información de 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?	R2#show ip protocols
¿Qué comando muestra solo las rutas OSPF?	R2#show ip route ospf
¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	R2#show run | section router ospf router ospf

Parte 5: Implementar DHCP y NAT para IPv4

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

Las tareas de configuración para R1 incluyen las siguientes:

Para implementar el NAT desde R1 como servidos DHCP reservamos de cada VLAN las primeras 20 direcciones VLAN 21 y 23.

Tabla 27 : Paso 1: Configurar el R1 como servidor de DHCP para las VLAN 21 y 23

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20

Crear un pool de DHCP para la VLAN 21.	R1(config)#ip dhcp pool ACCT R1(dhcp-config)#network 192.168.21.0 255.255.255.0 R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com R1(dhcp-config)#default-router 192.168.21.1
Crear un pool de DHCP para la VLAN 23	R1(dhcp-config)#ip dhcp pool ENGNR R1(dhcp-config)#network 192.168.23.0 255.255.255.0 R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com R1(dhcp-config)#default-router 192.168.23.1

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

La configuración del R2 incluye las siguientes tareas:

En el paso de NAT estatico y dinamico en R2 creamos bases de datos locales habilitamos el servidor http, creamos NAT estatica definimos el pool de direcciones y NAT dinámica.

Tabla 28: Paso 2: Configurar la NAT estática y dinámica en el R2

Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	R2(config)#username webuser privilege 15 secret cisco12345
Habilitar el servicio del servidor HTTP	R2(config)#ip http server
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	R2(config)#ip http authentication local
Crear una NAT estática al servidor web.	R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229
Asignar la interfaz interna y externa para la NAT estática	R2(config)#interface gigabitEthernet 0/0 R2(config-if)#ip nat outside R2(config-if)#int s0/0/0 R2(config-if)#ip nat inside R2(config-if)#int s0/0/1 R2(config-if)#ip nat inside

Configurar la NAT dinámica dentro de una ACL privada	R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255
Defina el pool de direcciones IP públicas utilizables.	R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248
Definir la traducción de NAT dinámica	R2(config)#ip nat inside source list 1 pool INTERNET

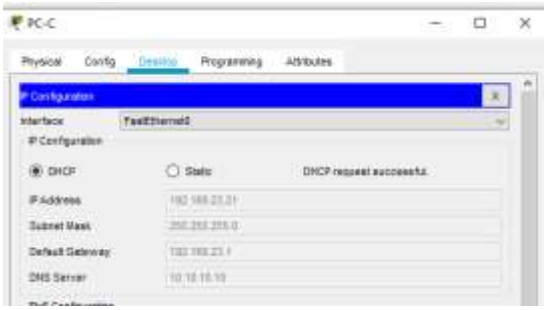
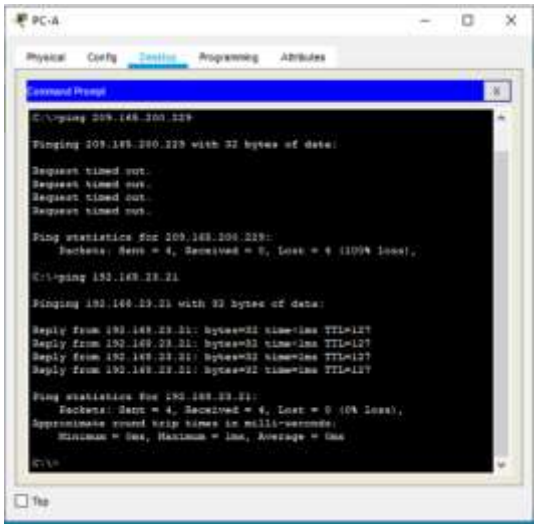
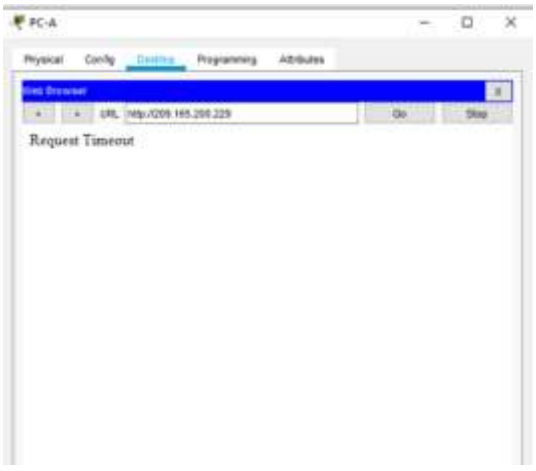
Paso 3: Verificar el protocolo DHCP y la NAT estática

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

A continuación las comprobaciones correspondientes al DHCP y NAT estática, podemos verificar como asigna direcciones dinámicas a los host PC-A y PC-C también responde el ping a las direcciones asignadas.

Tabla 29: Paso 3: Verificar el protocolo DHCP y la NAT estática

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	 *Ilustración 35 : Figura 35. Verificación DHCP PC-A*

Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	 *Ilustración 36 : Figura 36. Verificación DHCP PC-C*
Verificar que la PC-A pueda hacer ping a la PC-C **Nota:** Quizá sea necesario deshabilitar el firewall de la PC.	 *Ilustración 37 : Figura 37. Verificación ping de PC-A a PC-C*
Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.229) Iniciar sesión con el nombre de usuario **webuser** y la contraseña **cisco12345**	 *Ilustración 38 : Figura 38. Servidor web*

Parte 6: Configurar NTP

Para la configuración NTP ponemos a R2 como maestro y R1 como cliente con configuración de actualizaciones periódicas.

Tabla 30: Parte 6: Configurar NTP

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	**R2#clock set 09:00:00 05 march 2016**
Configure R2 como un maestro NTP.	R2(config)#ntp master 5
Configurar R1 como un cliente NTP.	R1(config)#ntp server 172.16.1.2
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	R1(config)#ntp update-calendar
Verifique la configuración de NTP en R1.	R1#show ntp associations address ref clock st when poll reach delay offset disp ~172.16.1.2 127.127.1.1 5 8 16 177 6.00 726223572452.00 0.12 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured

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

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

Creamos lista de acceso telnet entre R1 y R2 configyuramos nombre a las líneas VTY y permitimos el acceso por telnet.

Tabla 31: Paso 1: Restringir el acceso a las líneas VTY en el R2

Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	R2(config)#ip access-list standard ADMIN-MGT R2(config-std-nacl)#permit host 172.16.1.1
Aplicar la ACL con nombre a las líneas VTY	R2(config)#line vty 0 4 R2(config-line)#access-class ADMIN-MGT in
Permitir acceso por Telnet a las líneas de VTY	R2(config-line)#transport input telnet
Verificar que la ACL funcione como se espera	 *Ilustración 39 : Figura 39 Verificación ACL*

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

En esta parte introducimos los siguientes comandos para ver las listas de configuración del dispositivo.

Tabla 32: Paso 2: Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	R2#show ip access-lists
Restablecer los contadores de una lista de acceso	R2#clear access-list counters ip

¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	R2#show ip interface
¿Con qué comando se muestran las traducciones NAT?	R2#show ip nat translations
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	R2#clear ip nat translation

CONCLUSIONES

La configuración de una VLAN permite manejar un número más amplio de direcciones además de asignar un rango de puertos a la necesidad que pide la topología de la red. Se puede asignar a través de un router un puerto distintito en protocolo ipv4 o ipv6 dentro de las mismas redes, tener un rango distinto uno grande para enlazar y uno pequeño para administrar hots.

Se tiene claro que el direccionamiento es vital para la organización y diseño de una red de datos parte de este es enlazado con un rango o mascara que permite filtrar y dar selección de equipos interconectados para dar vía a hosts. Además de asignar direcciones es importante poner seguridad a nuestros dispositivos para que no tengan accesos externos de intrusos que puedan robar o afectar nuestra información.

REFERENCIAS

- CISCO. (2019). Exploración de la red. Fundamentos de Networking. Recuperado
- de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#1

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

- UNAD (2017). Diseño y configuración de redes con Packet Tracer [OVA] Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgCT9VCtl_pLtPD9 Vesga, J. (2019). Introducción al Laboratorio Remoto SmartLab [OVI]. Recuperado de http://hdl.handle.net/10596/24167

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

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

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

- UNAD (2017). PING y TRACER como estrategia en procesos de Networking
- [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgTCtKY-7F5KIRC3

- CISCO. (2019). Ethernet. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#5
- CISCO. (2019). Capa de red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#6

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

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

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

- CISCO. (2019). Capa de aplicación. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#10 •
- CISCO. (2019). Configuración de un sistema operativo de red. Fundamentos de Networking. Recuperado de: https://static-courseassets.s3.amazonaws.com/ITN6/es/index.html#11

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

- CISCO. (2019). Routing Estático. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-courseassets.s3.amazonaws.com/RSE6/es/index.html#2 UNAD (2017). Configuración de Switches y Routers [OVA]. Recuperado de

ANEXOS

Anexo A: Link Google Drive, archivo prueba de habilidades y escenarios en packet tracert.

https://drive.google.com/file/d/1uTg1C02hnk93vNjxV5LIXflAmUHR6Nc7/view?usp=sharing

Anexo B: Artículo científico sobre el escenario 2 de la prueba de habilidades.

Solución de escenario 2 Bajo la tecnología cisco

7174488
Víctor Ernesto Badillo Camargo
vebadilloc@unadvirtual.edu.co

Resumen - **:** A través de práctica simulada tenemos para desarrollar dos estudios de caso topologías diferentes a con el objetivo de aprender a configurar diferentes tipos de redes. CISCO la empresa que en redes es una de las más experimentadas en diseño e implementación de redes. A través de su plataforma y programas cisco nos enseña a estructurar una red desde lo más básico

El diplomado no deja captar la contextualización del uso fundamental de la redes de datos y de internet, también tenemos el uso y configuración de otros dispositivos como lo es la domótica salimos no solo de la parte de configurar computadores a manipular dispositivos remotamente como electrodomésticos o una simple bombilla de nuestra casa, la telefonía IP es también muy utilizada en las empresas y se puede enlazar con internet para no incurrir en gastos adicionales.

Introducción.

En todos los ámbitos de la vida actual somos dependientes del acceso tecnológico, a nivel personal y empresarial es fundamental la interacción con redes e internet, de eso depende gran parte de las actividades sociales y laborales; es por eso que el aumento a gran escala de redes a nivel mundial. Todos estamos en conectividad constante, las noticias son de primera mano las transacciones bancarias y compras desde casa y a través del móvil son una realidad, lo que nos conecta y permite la comunicación en todos los ámbitos son la redes tanto físicas como inalámbricas y siempre serán las redes las que interconecten empresas y familias.

En cuanto al motivo que nos trae a realizar esta investigación no es más que la infraestructura utilizada en las comunicaciones e internet; las redes de datos son el centro del desarrollo mundial, desde las redes pequeñas hasta las más amplias representan avance y progreso.

El diplomado en desarrollo nos plantea dos casos a desarrollar para dar solución a requerimientos de red, la topología permite desarrollar soluciones de acceso a diferentes tipos de equipos como routers switches y computadoras, aprendimos a enlazar con proveedores ISP además de diferenciar los tipos de conectividad a través de programas de simulación que pueden mostrarnos tanto la conexión física como la lógica. Es importante resaltar la cantidad de medios y facilidades que actualmente nos permiten tener un análisis más completo del diseño e implementación de una red.

Configuración de la topología escenario 2

Inicializar dispositivos

Eliminamos archivos de configuración en el dispositivo a configurar recargamos el router para empezar a configurar de ceros nombrando el dispositivo estableciendo contraseñas.

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

Configurar parámetros básicos de los dispositivos

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

direcciones muestra el direccionamiento del host para acceso a 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:DB8:ACAD:A::2/64
Gateway predeterminado IPv6	2001:DB8:ACAD:2::1

Configurar R1 desactivar búsqueda de DNS nombrar el dispositivo establecer seguridad con cifrado, contraseñas configurando interfaz S0/0/0 IPV4 IPV6 con direcciones previamente establecidas.

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R1
Contraseña de exec privilegiado cifrada	R1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	R1(config)#line console 0 R1(config-line)#password ciscoconpass R1(config-line)#login
Contraseña de acceso Telnet	R1(config-line)#line vty 0 4 R1(config-line)#password ciscoconpass R1(config-line)#login
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Mensaje MOTD	R1(config)#banner motd $Se prohibe el acceso no autorizado.$
Interfaz S0/0/0	R1(config)#interface serial 0/0/0 R1(config-if)#description Connection to R2 R1(config-if)#ip address 172.16.1.1 255.255.255.252 R1(config-if)#ipv6 address 2001:DB8:ACAD:1::1/64 R1(config-if)#clock rate 128000 R1(config-if)#no shutdown
Rutas predeterminadas	R1(config)#ip route 0.0.0.0 0.0.0.0 serial 0/0/0 R1(config)#ipv6 route ::/0 s0/0/0

Configurar R2 En R2 realizamos configuración inicial hostname R2 desactivar búsqueda de DNS, configuramos con el direccionamiento establecido los puertos interfaz S0/0/0, S0/0/1, G0/0 ademas de la interfaz loopback con ip 10.10.10.10

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R2
Contraseña de exec privilegiado cifrada	R2(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	R2(config)#line console 0 R2(config-line)#password ciscoconpass R2(config-line)#login
Contraseña de acceso Telnet	R2(config-line)#line vty 0 4 R2(config-line)#password ciscoconpass R2(config-line)#login
Cifrar las contraseñas de texto no cifrado	R2(config-line)#service password-encryption
Habilitar el servidor HTTP	R2(config)#ip http server
Mensaje MOTD	R2(config)#banner motd $Se prohibe el acceso no autorizado.$

Interfaz S0/0/0	R2(config)#interface serial 0/0/0 R2(config-if)#description Connection to R1 R2(config-if)#ip address 172.16.1.2 255.255.255.252 R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64 R2(config-if)#no shutdown
Interfaz S0/0/1	R2(config)#interface serial 0/0/1 R2(config-if)#description Connection to R3 R2(config-if)#ip address 172.16.2.2 255.255.255.252 R2(config-if)#ipv6 address 2001:DB8:ACAD:2::2/64 R2(config-if)#clock rate 128000 R2(config-if)#no shutdown
Interfaz G0/0 (simulación de Internet)	R2(config)#interface gigabitEthernet 0/0 R2(config-if)#description Connection to Internet R2(config-if)#ip address 209.165.200.233 255.255.255.248 R2(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64 R2(config-if)#no shutdown
Interfaz loopback 0 (servidor web simulado)	R2(config-if)#Interface Loopback0 R2(config-if)#ip address 10.10.10.10 255.255.255.255
Ruta predeterminada	R2(config)#ip route 0.0.0.0 0.0.0.0 gigabitEthernet 0/0 R2(config)#ipv6 route ::/0 gigabitEthernet 0/0

Configuración R3. Configuración inicial como en todos los dispositivos además de configurar interfaz S0/0/1 IPV4 IPV6 con direcciones establecidas con el comando no shutdown activamos interfaz, este router trabajaría con interfaz loopback 4, 5, 6, 7 con direcciones en el rango 192.168.4.1, 192.168.5.1, 192.168.6.1, 192.168.7,1 mascara 255.255.255.0, establecemos rutas predeterminadas.

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R3
Contraseña de exec privilegiado cifrada	R3(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	R3(config)#line console 0 R3(config-line)#password ciscoconpass R3(config-line)#login
Contraseña de acceso Telnet	R3(config-line)#line vty 0 4 R3(config-line)#password ciscoconpass R3(config-line)#login
Cifrar las contraseñas de texto no cifrado	R3(config-line)#service password-encryption
Mensaje MOTD	R3(config)#banner motd $Se prohibe el acceso no autorizado.$
Interfaz S0/0/1	R3(config)#interface serial 0/0/1 R3(config-if)#description Connection to R2 R3(config-if)#ip address 172.16.2.1 255.255.255.252 R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64 R3(config-if)#no shutdown
Interfaz loopback 4	R3(config-if)#Interface Loopback4 R3(config-if)#ip address 192.168.4.1 255.255.255.0
Interfaz loopback 5	R3(config-if)#Interface Loopback5 R3(config-if)#ip address 192.168.5.1 255.255.255.0
Interfaz loopback 6	R3(config-if)#Interface Loopback6 R3(config-if)#ip address 192.168.6.1 255.255.255.0

Interfaz loopback 7	R3(config-if)#Interface Loopback7 R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64
Rutas predeterminadas	R3(config)#ip route 0.0.0.0 0.0.0.0 serial 0/0/1 R3(config)#ipv6 route ::/0 serial 0/0/1

Configurar S1. En este caso S1 se configura incialmente desactivando búsqueda de DNS configuración de seguridad con contraseñas y mensaje de MOTD.

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Switch(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S1
Contraseña de exec privilegiado cifrada	S1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	S1(config)#line console 0 S1(config-line)#password ciscoconpass S1(config-line)#login
Contraseña de acceso Telnet	S1(config-line)#line vty 0 4 S1(config-line)#password ciscoconpass S1(config-line)#login
Cifrar las contraseñas de texto no cifrado	S1(config-line)#service password-encryption
Mensaje MOTD	S1(config)#banner motd $Se prohibe el acceso no autorizado.$

Configurar S3. Dentro de la configuración del dispositivo switch se realiza igual que en router la inicialización del dispositivo.

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Switch(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S3
Contraseña de exec privilegiado cifrada	S3(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	S3(config)#line console 0 S3(config-line)#password ciscoconpass S3(config-line)#login
Contraseña de acceso Telnet	S3(config-line)#line vty 0 4 S3(config-line)#password ciscoconpass S3(config-line)#login
Cifrar las contraseñas de texto no cifrado	S3(config-line)#service password-encryption
Mensaje MOTD	S3(config)#banner motd $Se prohibe el acceso no autorizado.$

Verificación de la conectividad. Verificando la conectividad de los dispositivos se utiliza el comando ping desde los equipos los routers principales desde R1 a R2 por los puertos serial S0/0/0 hasta S0/0/1 direcciones 172.16.1.2 a 172.16.2.1

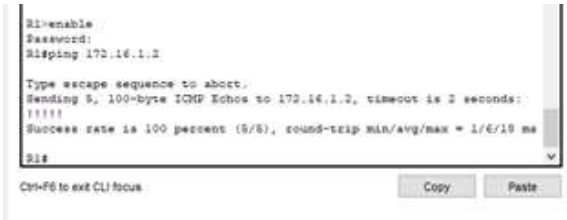


Figura 1. Ping desde R1 a R2 S0/0/0 IP 172.16.1.2

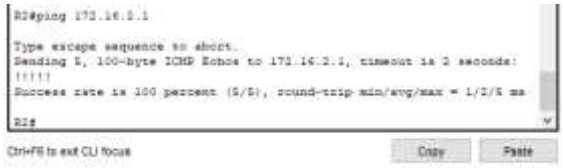


Figura 2. Ping desde R2 a R3 S0/0/1 IP 172.16.2.1

Configuración de la seguridad del switch las VLAN y el routing entre VLAN

Configurar S1. Configurando la VLAN 21 con nombre contabilidad también la VLAN 23 con nombre ingeniería y VLAN 99 con nombre administración también asignamos el Gateway predeterminado establecemos troncales en F0/3 y F0/5 también rangos de los demás puertos de acceso.

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	S1(config)#vlan 21 S1(config-vlan)#name Contabilidad S1(config-vlan)#vlan 23 S1(config-vlan)#name Ingenieria S1(config-vlan)#vlan 99 S1(config-vlan)#name Administracion
Asignar la dirección IP de administración.	S1(config)#interface vlan 99 S1(config-if)#ip address 192.168.99.2 255.255.255.0 S1(config-if)#no shutdown
Asignar el gateway predeterminado	S1(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	S1(config)#interface fastEthernet 0/3 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1
Forzar el enlace troncal en la interfaz F0/5	S1(config-if)#interface fastEthernet 0/5 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	S1(config-if)#interface range f0/1-2, f0/4, f0/6-24, g0/1-2 S1(config-if-range)#switchport mode access
Asignar F0/6 a la VLAN 21	S1(config-if-range)#interface fastEthernet 0/6 S1(config-if)#switchport access vlan 21
Apagar todos los puertos sin usar	S1(config-if)#interface range f0/1-2, f0/4, f0/7-24, g0/1-2 S1(config-if-range)#shutdown

Configurar S3. En S3 creamos las VLAN al igual que en S1 contabilidad, ingeniería, y administración la VLAN 99 con la ip 192.168.99.3 ademas forzamos enlaces troncales en F0/3

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	S3(config)#vlan 21 S3(config-vlan)#name Contabilidad S3(config-vlan)#vlan 23 S3(config-vlan)#name Ingenieria S3(config-vlan)#vlan 99 S3(config-vlan)#name Administracion
Asignar la dirección IP de administración	S3(config-vlan)#interface vlan 99 S3(config-if)#ip address 192.168.99.3 255.255.255.0 S3(config-if)#no shutdown
Asignar el gateway predeterminado.	S3(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	S3(config)#interface fastEthernet 0/3 S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	S3(config)#interface range f0/1-2, f0/4-24, g0/1-2 S3(config-if-range)#switchport mode access
Asignar F0/18 a la VLAN 21	S3(config-if-range)#interface fastEthernet 0/18 S3(config-if)#switchport access vlan 23
Apagar todos los puertos sin usar	S3(config-if)#interface range f0/1-2, f0/4-17, f0/19-24, g0/1-2 S3(config-if-range)#shutdown

Configurar R1. En este paso configuramos subinterfaz 802.1Q-21 en G01 802.1Q-23 en G01 802.1Q-24 en G01 802.1Q-99 en G01 con encapsulación dot1Q-23 finalmente activamos la interfaz.

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	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
Configurar la subinterfaz 802.1Q .23 en G0/1	R1(config-subif)#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
Configurar la subinterfaz 802.1Q .99 en G0/1	R1(config-subif)#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
Activar la interfaz G0/1	R1(config-subif)#int g0/1 R1(config-if)#no shutdown

Verificar la conectividad de red. Verificando desde S1 con ping a la VLAN 99 direccion ip 192.168.99.1 hacemos pin a esa dirección y a la VLAN 99 desde S3 a R1 a la dirección 192.168.99.1 encontrando respuesta satisfactoria en todas las pruebas.

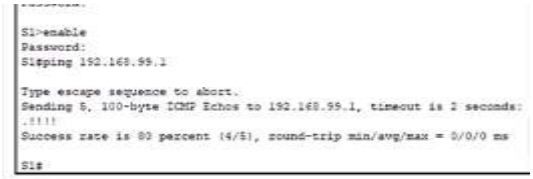


Figura 3. Ping desde S1 a R1 direccion VLAN IP 99 192.168.99.1

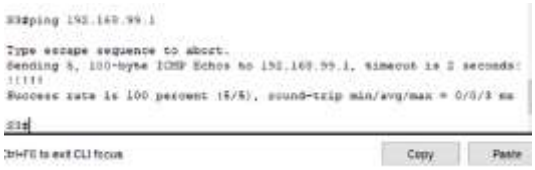


Figura 4. Ping desde S3 a R1 VLAN IP 99 192.168.99.1

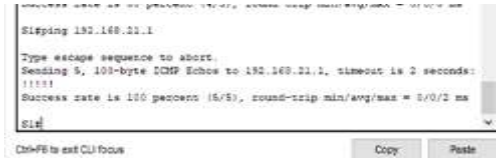


Figura 5. Ping desde S1 a R1 dirección VLAN IP 21 192.168.21.1

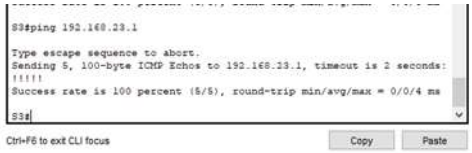


Figura 6. Ping desde S3 a R1 VLAN IP 23 192.168.23.1

Configurar protocolo routing dinamico OSPF

Configurar OSPF en el R1 Este protocolo de enrutamiento abierto nos permite escalar las redes WAN, empezamos configurando el enlazando las direcciones pre establecidas con los puertos de R1 GigabitEthernet0/1.21, GigabitEthernet0/1.23, GigabitEthernet0/1.99

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R2(config)#router ospf R2(config-router)#version 3

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

Configurar OSPF en el R2. En este paso configuramos también área 0 en R2 con sus loopback0 en el serial 0/0/0 también anunciamos las redes conectadas, establecemos loopback como pasiva y desactivamos sumarizacion con el comando R2(config-router)#no auto-summary

Elemento o tarea de configuración	**Especificación**
Configurar OSPF área 0	R2(config)#router osfp R2(config-router)#version 3
Anunciar las redes conectadas directamente	R2(config-router)#do show ip route connected C 10.10.10.10/32 is directly connected, Loopback0 C 172.16.1.0/30 is directly connected, Serial0/0/0 C 172.16.2.0/30 is directly connected, Serial0/0/1 C 209.165.200.232/29 is directly connected, GigabitEthernet0/0 R2(config-router)#network 10.10.10.10 R2(config-router)#network 172.16.1.0 R2(config-router)#network 172.16.2.0
Establecer la interfaz LAN (loopback) como pasiva	R2(config-router)#passive-interface loopback 0
Desactive la sumarización automática.	R2(config-router)#no auto-summary

Configurar OSPFv3 en R2. En R3 configuramos área 0 como en los otros dispositivos igualmente anunciamos las redes conectadas y hacemos configuración del loopback como pasiva.

Elemento o tarea de configuración	**Especificación**
Configurar OSPF área 0	R2(config)# ipv6 router ospf 1 R3(config-rtr)# router-id 3.3.3.3

Anunciar redes IPv4 conectadas directamente	R2(config-router)#do show ip route connected C 172.16.2.0/30 is directly connected, Serial0/0/1 C 192.168.4.0/24 is directly connected, Loopback4 C 192.168.5.0/24 is directly connected, Loopback5 C 192.168.6.0/24 is directly connected, Loopback6 R2(config-router)#network 172.16.2.0 R2(config-router)#network 192.168.4.0 R2(config-router)#network 192.168.5.0 R2(config-router)#network 192.168.6.0
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	R2(config-router)#passive-interface loopback 4 R2(config-router)#passive-interface loopback 5 R2(config-router)#passive-interface loopback 6
Desactive la sumarización automática.	R2(config-router)#no auto-summary

Verificar la información de OSPF. Los comandos utilizados para la verificación de OSPF son los mostrados a continuación.

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?	R2#show ip protocols
¿Qué comando muestra solo las rutas OSPF?	R2#show ip route ospf
¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	R2#show run | section router ospf router ospf

Implementar DHCP y NAT para IPv4

Configurar el R1 como servidor de DHCP para las VLAN 21 y 23. Para implementar el NAT desde R1 como servidos DHCP reservamos de cada VLAN las primeras 20 direcciones VLAN 21 y 23.

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

Configurar NAT estatica y dinámica en el R2 En el paso de NAT estatico y dinamico en R2 creamos bases de datos locales habilitamos el servidor http, creamos NAT estatica definimos el pool de direcciones y NAT dinámica.

Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	R2(config)#username webuser privilege 15 secret cisco12345
Habilitar el servicio del servidor HTTP	R2(config)#ip http server
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	R2(config)#ip http authentication local
Crear una NAT estática al servidor web.	R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229
Asignar la interfaz interna y externa para la NAT estática	R2(config)#interface gigabitEthernet 0/0 R2(config-if)#ip nat outside R2(config-if)#int s0/0/0 R2(config-if)#ip nat inside R2(config-if)#int s0/0/1 R2(config-if)#ip nat inside
Configurar la NAT dinámica dentro de una ACL privada	R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255
Defina el pool de direcciones IP públicas utilizables.	R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248
Definir la traducción de NAT dinámica	R2(config)#ip nat inside source list 1 pool INTERNET

Verificar el protocolo DHCP y la NAT estática. A continuación las comprobaciones correspondientes al DHCP y NAT estática, podemos verificar como asigna direcciones dinámicas a los host PC-A y PC-C también responde el ping a las direcciones asignadas.

Figura 7. Verificar que la PC-A haya adquirido información de IP del servidor de DHCP

Figura 8. Verificar que la PC-C haya adquirido información de IP del servidor de DHCP

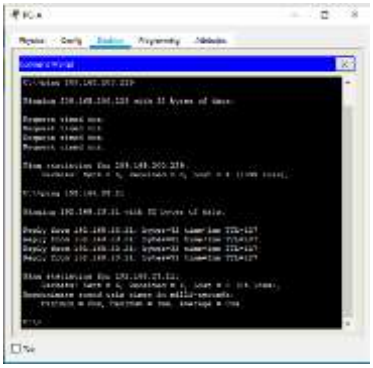


Figura 9. Verificar que la PC-A pueda hacer ping a la PC-C

Nota: Quizá sea necesario deshabilitar el firewall de la PC.

Figura 10. Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.229) Iniciar sesión con el nombre de usuario webuser y la contraseña cisco12345

Ningún control sobre la compresión o el número de bits por pixel. Usted debe abrir estos archivos de imagen en un programa como Microsoft Photo Editor y volver a guardarlos sin usar compresión, ya sea 1 ó 8 bits, y ya sea 600 o 220 dpi de resolución (Archivo | propiedades; Imagen | cambio de tamaño). Véase la Sección II-D2 para una explicación de número de bits y resolución. Si su programa de gráficos no puede exportar a TIFF, puede utilizar la misma técnica descrita para las tablas en el párrafo anterior.

Configuración NTP

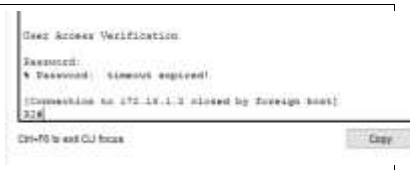
Para la configuración NTP ponemos a R2 como maestro y R1 como cliente con configuración de actualizaciones periódicas.

Elemento o tarea de configuración	**Especificación**
Ajuste la fecha y hora en R2.	**R2#clock set 09:00:00 05 march 2016**
Configure R2 como un maestro NTP.	R2(config)#ntp master 5
Configurar R1 como un cliente NTP.	R1(config)#ntp server 172.16.1.2
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	R1(config)#ntp update-calendar
Verifique la configuración de NTP en R1.	R1#show ntp associations address ref clock st when poll reach delay offset disp ~172.16.1.2 127.127.1.1 5 8 16 177 6.00 726223572452.000.12 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured

Configurar y verificar la lista de control de acceso.

Restringir el acceso a las líneas VTY en el R2. Creamos lista de acceso telnet entre R1 y R2 configyuramos nombre a las líneas VTY y permitimos el acceso por telnet.

Elemento o tarea de configuración	**Especificación**
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	R2(config)#ip access-list standard ADMIN-MGT R2(config-std-nacl)#permit host 172.16.1.1
Aplicar la ACL con nombre a las líneas VTY	R2(config)#line vty 0 4 R2(config-line)#access-class ADMIN-MGT in
Permitir acceso por Telnet a las líneas de VTY	R2(config-line)#transport input telnet

Verificar que la ACL funcione como se espera	 Figura 11. Verificación ACL

Introducción del comando de CLI En esta parte introducimos los siguientes comandos para ver las listas de configuración del dispositivo.

Descripción del comando	**Entrada del estudiante (comando)**
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	R2#show ip access-lists
Restablecer los contadores de una lista de acceso	R2#clear access-list counters ip
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	R2#show ip interface
¿Con qué comando se muestran las traducciones NAT?	R2#show ip nat translations
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	R2#clear ip nat translation

Figuras.

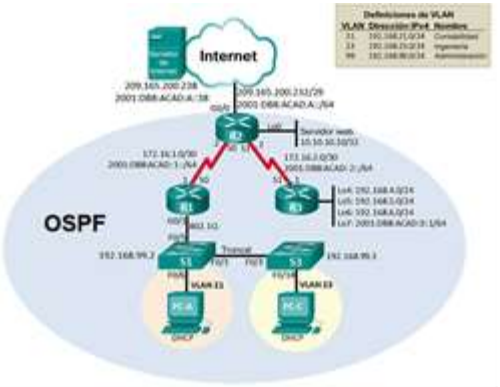


Figura 12. Topología del escenario 2

CONCLUSIONES

La configuración de una VLAN permite manejar un número más amplio de direcciones además de asignar un rango de puertos a la necesidad que pide la topología de la red.

Podemos asignar a través de un router un puerto distintito en protocolo ipv4 o ipv6 dentro de las mismas redes, tener un rango distinto uno grande para enlazar y uno pequeño para administrar hots.

Tenemos claro que el direccionamiento es vital para la organización y diseño de una red de datos parte de este es enlazado con un rango o mascara que permite filtrar y dar selección de equipos interconectados para dar vía a hosts. Además de asignar direcciones es importante poner seguridad a nuestros dispositivos para que no tengan accesos externos de intrusos que puedan robar o afectar nuestra información.

REFERENCES

CISCO. (2019). Exploración de la red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#1

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

UNAD (2017). Diseño y configuración de redes con Packet Tracer [OVA] Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgCT9VCtl_pLtPD9
Vesga, J. (2019). Introducción al Laboratorio Remoto SmartLab [OVI]. Recuperado de http://hdl.handle.net/10596/24167

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

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

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

UNAD (2017). PING y TRACER como estrategia en procesos de Networking
[OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgTCtKY-7F5KIRC3

CISCO. (2019). Ethernet. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#5 •
CISCO. (2019). Capa de red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#6

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

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

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

CISCO. (2019). Capa de aplicación. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#10 •
CISCO. (2019). Configuración de un sistema operativo de red. Fundamentos de Networking. Recuperado de: https://static-courseassets.s3.amazonaws.com/ITN6/es/index.html#11

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

CISCO. (2019). Routing Estático. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-courseassets.s3.amazonaws.com/RSE6/es/index.html#2
UNAD (2017). Configuración de Switches y Routers [OVA]. Recuperado de

BIOGRAFÍA

Víctor Ernesto Badillo Camargo nacido en Tunja año 1977 Tecnólogo en análisis y desarrollo de sistemas ADSI SENA. Ha trabajado en la parte de telecomunicaciones por 15 años, empresas como movistar, siemens, opegin, Colombia telecomunicaciones, desarrollando proyectos corporativos con módems, routers, radio enlaces, satelitales y gran parte de topología cisco. Como aspirante al título de ingeniero de sistemas se llevó a cabo este artículo con el fin de dar claridad sobre un escenario de red con topología y diferentes configuraciones, casos que permitieron tomar habilidades en el desarrollo de redes con tecnología cisco.