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

JHON JEHIDER ALBARRACIN URRUTIA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGIA E INGENIERIA

DIPLOMADO EN PROFUNDIZACION CISCO CCNA

2020

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

JHON JEHIDER ALBARRACIN URRUTIA

DIPLOMADO DE OPCIÓN DE GRADO PRESENTADO PARA OPTAR EL TÍTULO DE INGENIERO DE SISTEMAS

DOCENTE:

DIEGO EDINSON RAMIREZ CLAROS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGIA E INGENIERIA

DIPLOMADO EN PROFUNDIZACION CISCO CCNA

2020

NOTA DE ACEPTACIÓN:

_____

_____

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

Bogotá, 07 de diciembre de 2020

Agradecimiento

A todo el cuerpo de docentes que conforman la Universidad Nacional Abierta y a Distancia, quienes, a lo largo de esta carrera, han aportado al desarrollo de competencias intelectuales y profesionales para lograr a la formación de futuros ingenieros hábiles en conocimiento y aplicabilidad del mismo en el ámbito de los sistemas.

Tabla de contenido

Lista de figuras

Lista de tablas

Resumen

El presente trabajo desarrolla dos escenarios donde se ponen a prueba los conocimientos que fueron adquiridos a lo largo del desarrollo de este diplomado, en la interacción y configuración de los dispositivos CISCO, identificando las funciones de los mismos y aprovechando al máximo el conocimiento brindado por los docentes de la materia, realizando las simulaciones pertinentes para identificar los diferentes protocolos de red y así poder optar por la mejor opción de acuerdo a la tipología utilizada.

Abstract

The present work develops two scenarios where the knowledge that was acquired throughout the development of this diploma is put to the test, in the interaction and configuration of the CISCO devices, identifying their functions and making the most of the knowledge provided by the teachers of the subject, carrying out the relevant simulations to identify the different network protocols and thus be able to choose the best option according to the type used.

Introducción

Con el desarrollo del presente diplomado se busca obtener una certificación en redes cisco, el cual en su trayectoria en el Mercado ha venido ofreciendo cursos de capacitación y entrenamiento en el ámbito de los sistemas a diferentes instituciones educativas, fortaleciendo las capacidades del profesional en un mundo de tecnologías que evoluciona de manera constante.

Es de anotar, que a través de los escenarios virtuales brindados por los software suministrados por CISCO buscan la interacción simulada con diferentes elementos que hacen parte de una red, logrando su programación a través de los códigos e instrucciones que buscan establecer una conexión correcta, para así poder llevar a la práctica estos conocimientos y ser competitivos en un mundo laboral.

Objetivos

General

Llevar a cabo la configuración solicitada en la prueba de habilidades en las dos redes LAN dispuesta para esta etapa del diplomado.

Específicos

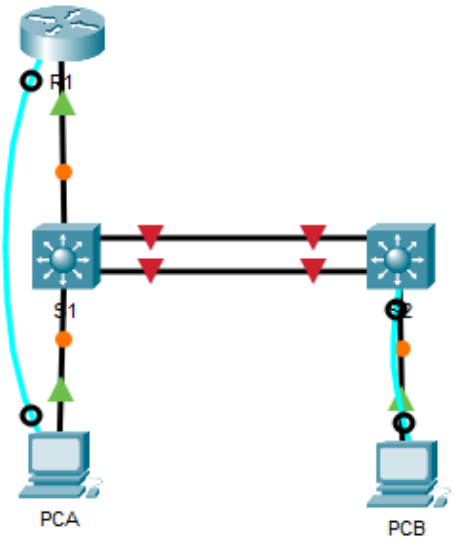
- Configurar los dispositivos (router, switch) para que se pueda llevar a cabo la conexión deseada.
- Realizar la creación de la VLAN en los diferentes dispositivos para así llevar a cabo el ejercicio de ambos escenarios.

- Emplear el protocolo OSPF y (DHCP) de acuerdo a cada escenario.

Escenario 1

En este primer escenario se configurarán los dispositivos de una red LAN, la cual está compuesta por un router, dos switch y dos equipos que admitan tanto la conectividad IPv4 como IPv6 para los hosts soportados. El router y el switch serán administrados de forma segura. Configurará el enrutamiento entre VLAN, DHCP, Etherchannel y port-security.

Figura 1. Topología del escenario 1



Fuente: autor

Tabla 1. Nombres de la 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

Inicializar dispositivos.
De acuerdo a lo solicitado en la guía se procede a inicializar, recargar y configurar aspectos básicos de los dispositivos router y swicht.

Tabla 3. Inicio y recarga de los router y swicht

Actividad	Código
Reinicio del router	Router>enable Router#erase startup-config
Volver a cargar el router	Router#reload
Reinicio del swicht	Switch>enable Switch#erase startup-config Switch#delete vlan.dat
Después de recargar el switch, configure la plantilla SDM para que admita IPv6 según sea necesario y vuelva a cargar el switch.	Switch>enable Switch#configure terminal Switch# sdm prefer dual-ipv4-and-ipv6 default Switch#reload

Configurar R1

Las tareas de configuración para R1 incluyen tareas que se relacionan en la siguiente tabla, donde se va asignar niveles de seguridad para el dispositivo como es la contraseña de manera cifrada, tanto al ingreso como en el acceso privilegiado, de igual forma la asignación de las direcciones ip a las interfaces que se van a utilizar en esta topología.

Tabla 4. Lista de comandos de configuración Router 1

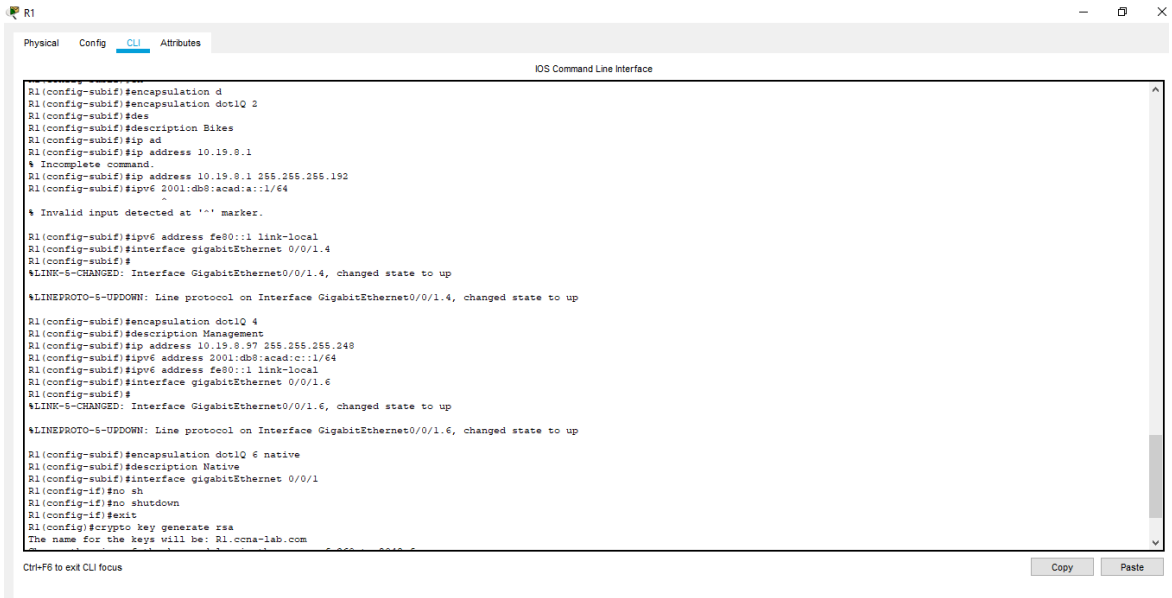
Tarea	Especificación
Desactivar la búsqueda DNS	Router>enable Router#configure terminal Router(config)#no ip domain-lookup
Nombre del router	Router>enable Router#configure terminal Router(config)#hostname R1
Nombre de dominio	Router#configure terminal Router(config)#ip domain-name ccna-lab.com

Tarea	Especificación
Contraseña cifrada para el modo EXEC privilegiado ciscoenpass	R1(config)#enable secret ciscoenpass R1(config)#line console 0 R1(config-line)#password ciscoconpass R1(config-line)#login
Contraseña de acceso a la consola	Router(config)# password ciscoconpass
Establecer la longitud mínima para las contraseñas de 10 caracteres	Router(config)#security passwords min-length 10
Crear un usuario administrativo en la base de datos local de nombre “admin”	R1(config)#username admin secret admin1pass R1(config)#line vty 0 15 R1(config-line)#login local
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local y creación de la contraseña admin1pass	R1(config)#line vty 0 15 R1(config-line)#login local R1(config)#username admin secret admin1pass
Configurar VTY solo aceptando SSH	R1(config-line)#transport input ssh
Cifrar las contraseñas de texto no cifrado	Router#conf terminal Router(config)#service password-encryption Router(config)#exit
Configure un MOTD Banner	R1(config)#banner motd %Acceso no autorizado%
Habilitar el routing IPv6	Router#configure terminal Router(config)#ipv6 unicast-routing

Tarea	Especificación
Configurar interfaz G0/0/1 y subinterfaces realizando los pasos que se relacionan a continuación. Configure el Loopback0 interface Establezca la descripción Establece la dirección IPv4. Establece la dirección IPv6. Establezca la dirección local de enlace IPv6 como fe80::1	R1(config)#interface gigabitEthernet 0/0/1.2 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)#interface gigabitEthernet 0/0/1.3 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)#interface gigabitEthernet 0/0/1.4 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)#interface gigabitEthernet 0/0/1.6 R1(config-subif)#encapsulation dot1Q 6 native R1(config-subif)#description Native R1(config-subif)#interface gigabitEthernet 0/0/1 R1(config-if)#no shutdown

Tarea	Especificación
Generar una clave de cifrado RSA	Módulo de 1024 bits R1(config)#crypto key generate rsa The name for the keys will be: R1.ccna-lab.com Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes. How many bits in the modulus [512]: 1024 % Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

Figura 2. Configuración R1



Fuente: Autor

Configure S1 y S2.

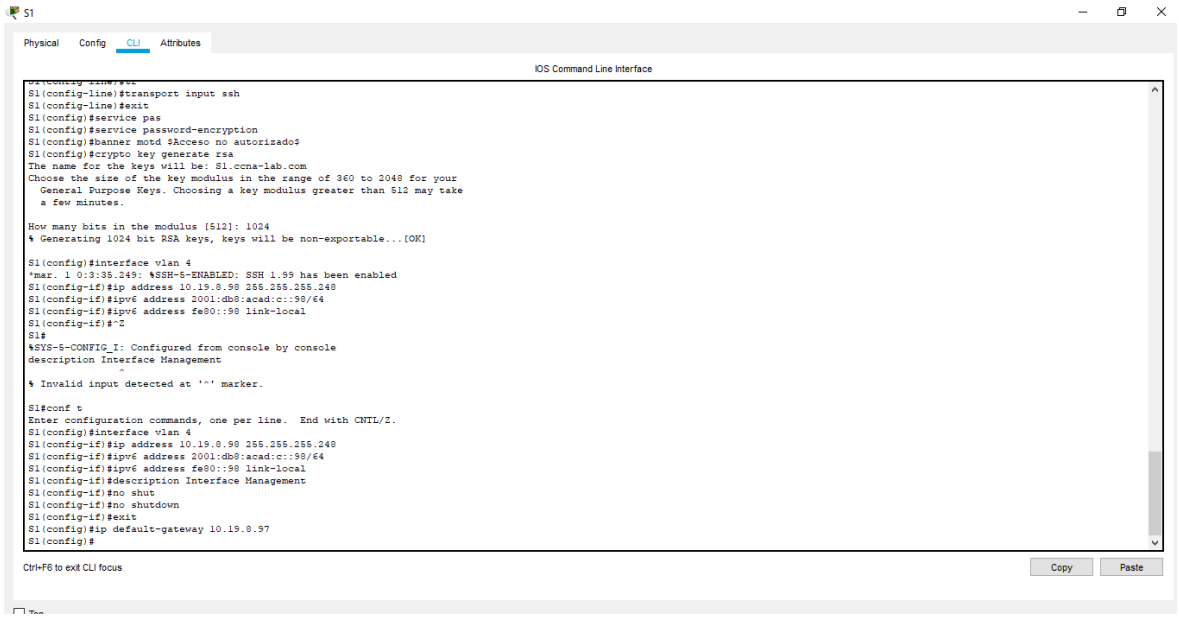
Las tareas de configuración para S1 y S2 incluyen tareas que se relacionan en la siguiente tabla, donde se va asignar niveles de seguridad para ambos dispositivos como es la contraseña de manera cifrada, tanto al ingreso como en el acceso privilegiado, de igual forma la asignación de las direcciones ip a las interfaces que se van a utilizar en esta topología.

Tabla 5. Lista de comandos para configuración del S1

Tarea	Especificación
Desactivar la búsqueda DNS.	Switch(config)#no ip domain lookup
Nombre del switch	Switch(config)#hostname S1
Nombre de dominio. ccna-lab.com	S1(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado ciscoenpass	S1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	S1(config)#line console 0 S1(config-line)#password ciscoconpass S1(config-line)#login
Crear un usuario administrativo en la base de datos local con el nombre de usuario: admin y password: admin1pass	S1(config)#username admin secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	S1(config)#line vty 0 15 S1(config-line)#login local
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S1(config-line)#transport input ssh S1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption

Tarea	Especificación
Configurar un MOTD Banner	S1(config)#banner motd %Acceso no autorizado%
Generar una clave de cifrado RSA	Módulo de 1024 bits S1(config)#crypto key generate rsa The name for the keys will be: S1.ccna-lab.com Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes. How many bits in the modulus [512]: 1024 % Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
Configurar la interfaz de administración (SVI) Establecer la dirección IPv4 de capa 3 Establezca la dirección local de enlace IPv6 como FE80: :98 para S1 y FE80: :99 para S2 Establecer la dirección IPv6 de capa 3	S1(config)#interface vlan 4 S1(config-if)#ip address 10.19.8.98 255.255.255.248 S1(config-if)#ipv6 address 2001:db8:acad:c::98/64 S1(config-if)#ipv6 address fe80::98 link-local S1(config-if)#description Interface Management S1(config-if)#no shutdown S1(config-if)#exit
Configuración del gateway predeterminado Configure la puerta de enlace predeterminada como 10.19.8.97 para IPv4	S1(config)#ip default-gateway 10.19.8.97

Figura 3. Configuración Swicht 1



Fuente: autor

Configuración de la infraestructura de red (VLAN, Trunking, EtherChannel)

Configurar S1

En la siguiente tabla se relacionará los comandos que se utilizan para la creación de la VLAN en nuestro Swicht, así como los troncos y el modo que configuraremos nuestros puertos de comunicación en nuestra topología.

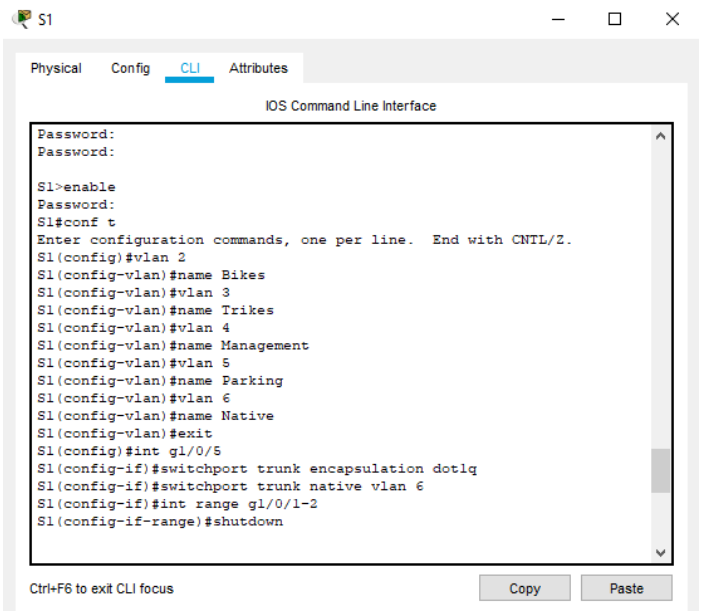
Tabla 6 lista de comandos creación VLAN en S1

Tarea	Especificación
Crear las VLAN en especificadas en la tabla 1. VLAN 2, nombre Bikes VLAN 3, nombre Trikes VLAN 4, name Management VLAN 5, nombre Parking VLAN 6, nombre Native	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

Tarea	Especificación
Crear troncos 802.1Q que utilicen la VLAN 6 nativa. Interfaces F0/1, F0/2 y F0/5	S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport trunk native vlan 6 S1(config-if)#int range g1/0/1-2 S1(config-if-range)#shutdown S1(config-if-range)#switchport trunk encapsulation dot1q S1(config-if-range)#switchport mode trunk S1(config-if-range)#switchport trunk native vlan 6
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2. Usar el protocolo LACP para la 1negociación	S1(config-if-range)#channel-group 1 mode active S1(config-if-range)#int port-channel 1 S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 6
Configurar el puerto de acceso de host para VLAN 2. Interface F0/6	S1(config-if)#int g1/0/6 S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 2
Configurar la seguridad del puerto en los puertos de acceso. Permitir 3 direcciones MAC	S1(config-if)#switchport port-security maximum 3

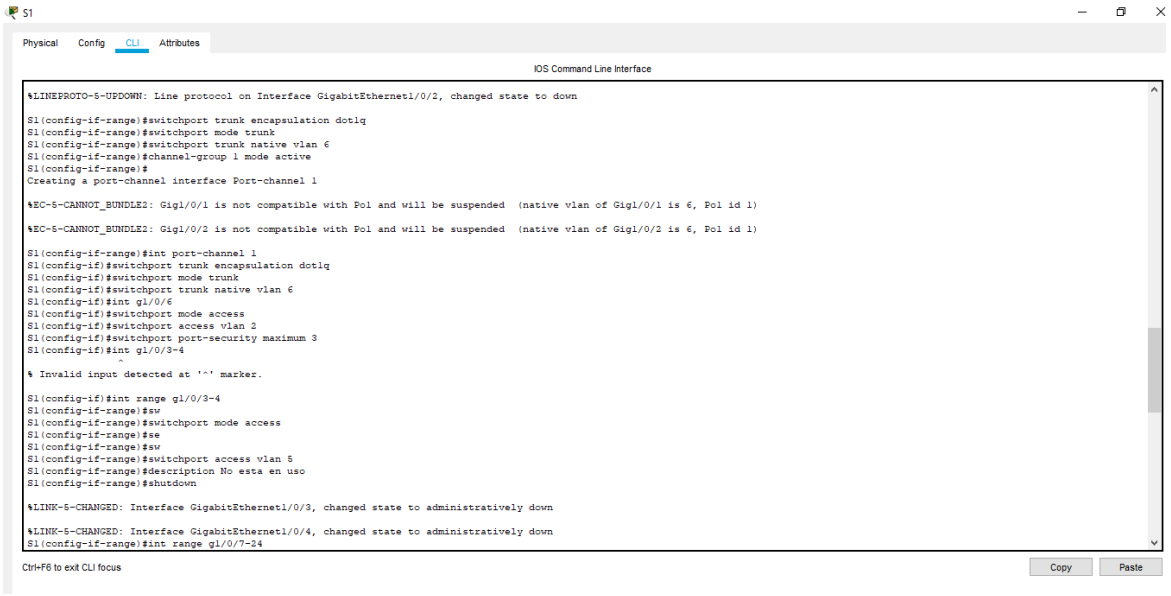
Tarea	Especificación
Proteja todas las interfaces no utilizadas Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar	S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 5 S1(config-if-range)#description No esta en uso S1(config-if-range)#shutdown S1(config-if-range)#int range g1/0/7-24 S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 5 S1(config-if-range)#description No esta en uso S1(config-if-range)#shutdown S1(config-if-range)#int range g1/1/1-4 S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 5 S1(config-if-range)#description No está en uso S1(config-if-range)#shutdown

Figura 4. Creación VLAN



Fuente: Autor

Figura 5. Configuración de troncales



Fuente: Autor

Configure el S2.

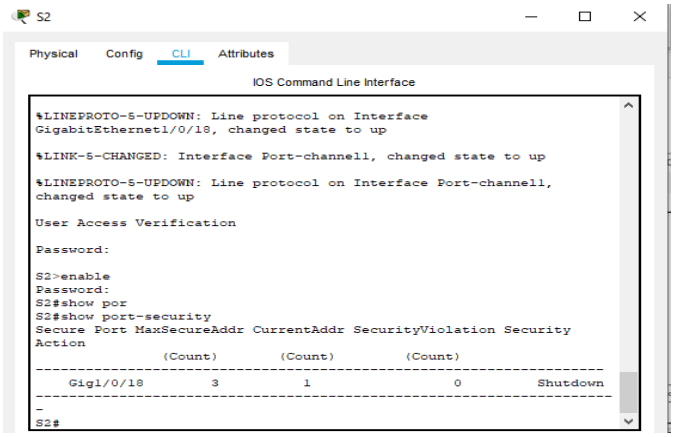
Entre las tareas de configuración de S2 se incluyen las mismas actividades que se realizaron anteriormente en el swicht 1:

Tabla 7. Lista de comandos para S2

Tarea	Especificación
Crear VLAN VLAN 2, name Bikes VLAN 3, name Trikes VLAN 4, name Management VLAN 5, nombre Parking VLAN 6, nombre Native	S2>enable S2#configure terminal 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 S2(config-vlan)#exit

Tarea	Especificación
Crear troncos 802.1Q que utilicen la VLAN 6 nativa Interfaces F0/1 y F0/2	S2(config)#int range g1/0/1-2 S2(config-if-range)#shutdown S2(config-if-range)#switchport trunk encapsulation dot1q S2(config-if-range)#switchport trunk native vlan 6
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2. Usar el protocolo LACP para la negociación	S2(config-if-range)#channel-group 1 mode active S2(config-if-range)#int port-channel 1 S2(config-if)#switchport trunk encapsulation dot1q S2(config-if)#switchport mode trunk S2(config-if)#switchport trunk native vlan 6
Configurar el puerto de acceso del host para la VLAN 3 Interfaz F0/18	S2(config-if)#int g1/0/18 S2(config-if)#switchport mode access S2(config-if)#switchport access vlan 3
Configure port-security en los access ports. Permite 3 MAC addresses	S2(config-if)#switchport port-security maximum 3
Asegure todas las interfaces no utilizadas. Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar	S2(config-if)#int g1/0/18 S2(config-if)#switchport mode access S2(config-if)#switchport access vlan 3 S2(config-if)#switchport port-security maximum 3 S2(config-if)#int range g1/0/3-17 S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 5 S2(config-if-range)#description No está en uso S2(config-if-range)#shutdown S2(config-if-range)#int range g1/0/19-24 S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 5 S2(config-if-range)#description No está en uso S2(config-if-range)#shutdown S2(config-if-range)#int range g1/1/1-4 S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 5 S2(config-if-range)#description No está en uso S2(config-if-range)#shutdown

Figura 6. Comprobación de la configuración



Fuente: Autor

Configurar soporte de host

Configure R1

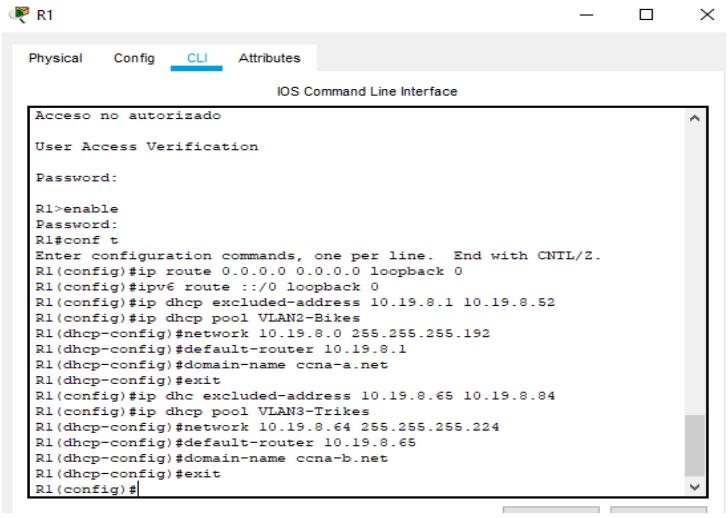
En la siguiente tabla se evidencia la lista de comandos utilizados para la configuración del Router 1, frente a la creación de las rutas predeterminadas tanto en el protocolo IPV4 y el IPV6, las cuales dirigirán el tráfico a la interfaz Loopback 0. Posteriormente la creación de un grupo DHCP para la Vlan 2 y 3.

Tabla 8. Lista de comandos configuración Router 1

Tarea	Especificación
Configure Default Routing. Crear rutas predeterminadas para IPv4 e IPv6 que dirijan el tráfico a la interfaz Loopback 0	R1(config)#ip route 0.0.0.0 0.0.0.0 loopback 0 R1(config)#ipv6 route ::/0 loopback 0

Tarea	Especificación
Configurar IPv4 DHCP para VLAN 2 Cree un grupo DHCP para VLAN 2, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio ccna-a.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada	R1(config)#ip dhcp excluded-address 10.19.8.1 10.19.8.52 R1(config)#ip dhcp pool VLAN2-Bikes R1(dhcp-config)#network 10.19.8.0 255.255.255.192 R1(dhcp-config)#default-router 10.19.8.1 R1(dhcp-config)#domain-name ccna-a.net
Configurar DHCP IPv4 para VLAN 3 Cree un grupo DHCP para VLAN 3, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio ccna-b.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada	R1(config)#ip dhc excluded-address 10.19.8.65 10.19.8.84 R1(config)#ip dhcp pool VLAN3-Trikes R1(dhcp-config)#network 10.19.8.64 255.255.255.224 R1(dhcp-config)#default-router 10.19.8.65 R1(dhcp-config)#domain-name ccna-b.net R1(dhcp-config)#exit

Figura 7. Configuración protocolo DHCP



Fuente: Autor

Configurar los servidores

Configurar 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.

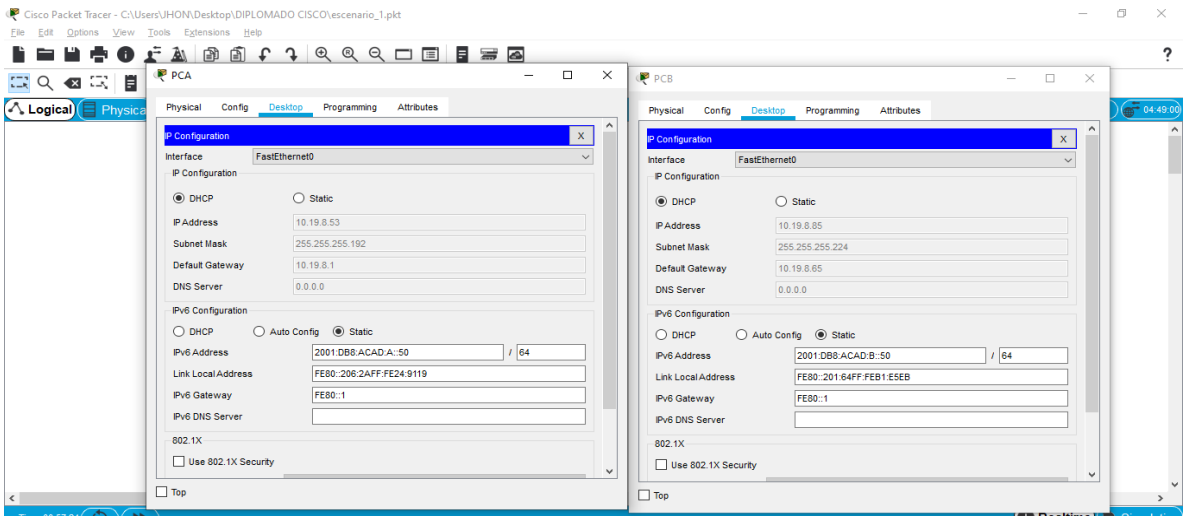
Tabla 9. Información del PC-A

PC-A Network Configuration	
Descripción	*Pc A*
Dirección física	*0006.2A24.9119*
Dirección IP	*10.19.8.53*
Máscara de subred	*255.255.255.192*
Gateway predeterminado	*10.19.8.1*
Gateway predeterminado IPv6	*FE80::1*

Tabla 10. Información del PC-B

Configuración de red de PC-B	
Descripción	*Pc B*
Dirección física	*0001.64B1.E5E*
Dirección IP	*10.19.8.85*
Máscara de subred	*255.255.255.224*
Gateway predeterminado	*10.19.8.65*
Gateway predeterminado IPv6	*FE80::1*

Figura 8. Verificación



Fuente: Autor

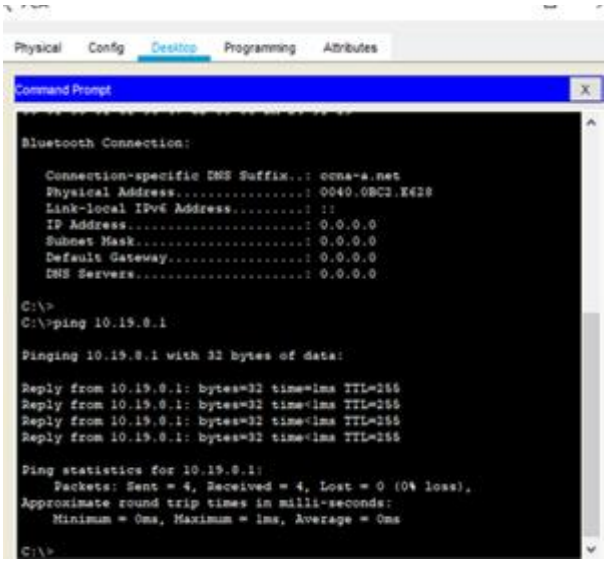
Probar y verificar la conectividad de extremo a extremo

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

Desde la PC-A a R1, G0/0/1.2 Dirección: 10.19.8.1

Se verifica que la conexión a través del ping sea correcta entre los dos dispositivos.

Figura 9. Ping 10.19.8.1

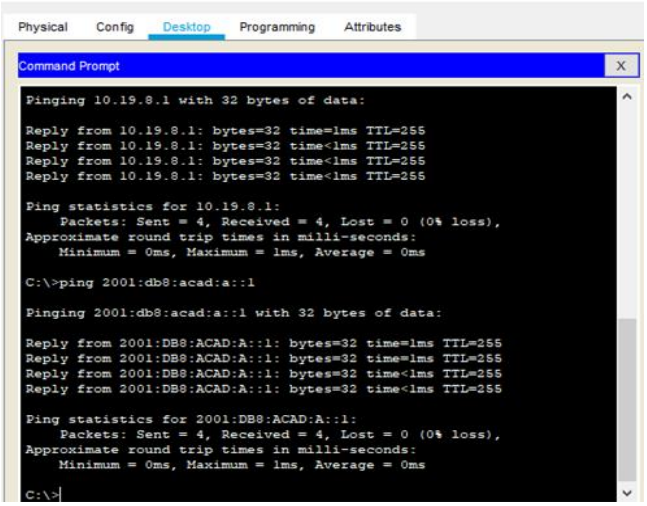


Fuente: Autor

Desde la PC-A a R1, G0/0/1.2 IPv6: 2001:db8:acad:a: :1

Se verifica que la conexión a través del ping sea correcta entre los dos dispositivos.

Figura 10. Ping 2001:db8:acad:a: :1

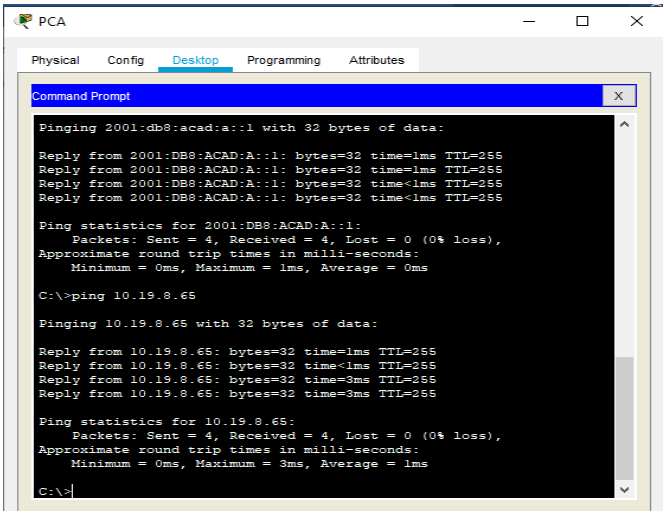


Fuente: Autor

Desde la PC-A a R1, G0/0/1.3 Dirección: 10.19.8.65

Se verifica que la conexión a través del ping sea correcta entre los dos dispositivos.

Figura 11 Ping 10.19.8.65

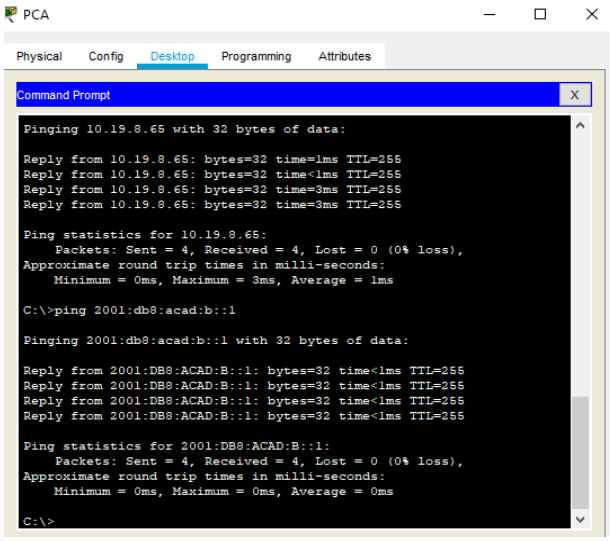


Fuente: Autor

Desde PC-A a R1, G0/0/1.3 IPv6 Dirección: 2001:db8:acad:b: :1

Se verifica que la conexión a través del ping sea correcta entre los dos dispositivos.

Figura 12. Ping 2001:db8:acad:b: :1

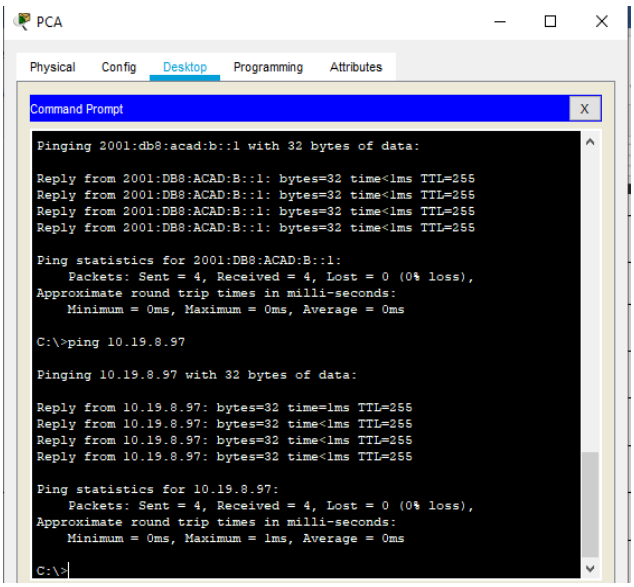


Fuente: Autor

Desde PC-A a R1, G0/0/1.4 Dirección: 10.19.8.97

Se verifica que la conexión a través del ping sea correcta entre los dos dispositivos.

Figura 13. Ping 10.19.8.97

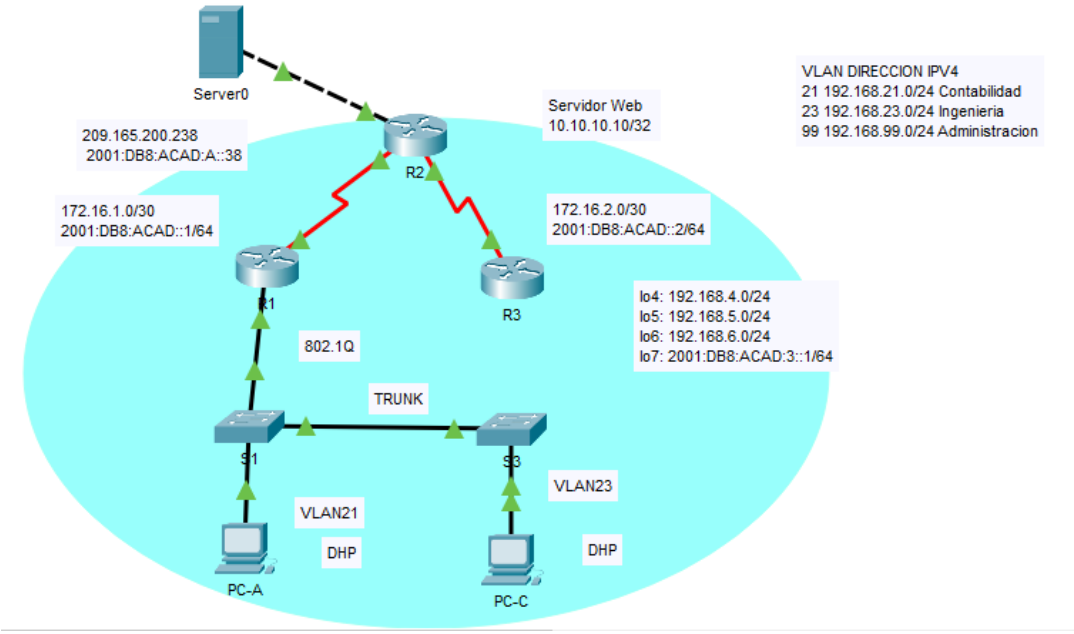


Fuente: Autor

Escenario 2

En el próximo escenario se llevarán a cabo configuraciones básicas vistas en prácticas anteriores, como lo es la asignación de un nombre, contraseña, inicialización de los dispositivos, creación de redes VLAN y trabajar en OSPF el cual es un protocolo de red para encaminamiento jerárquico de pasarela interior o Interior Gateway Protocol (IGP), donde utilizaremos un servidor de internet, 3 router, 2 swicht y 2 terminales host (PC A-B) como se establece en la siguiente topología.

Figura 14. Topología escenario 2



Fuente: Autor

Inicializar dispositivos

Inicializar y volver a cargar los routers y los switches

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

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

Tabla 11. Lista de comandos reinicio routers y 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	S1#erase startup-config S1#delete vlan.dat Delete flash:/vlan.dat? [confirm]
Volver a cargar ambos switches	S1#reload
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Switch>enable Switch#show flash: Directory of flash:/ 1 -rw- 4414921 <no date> c2960-lanbase-mz.122-25.FX.bin 64016384 bytes total (59601463 bytes free)

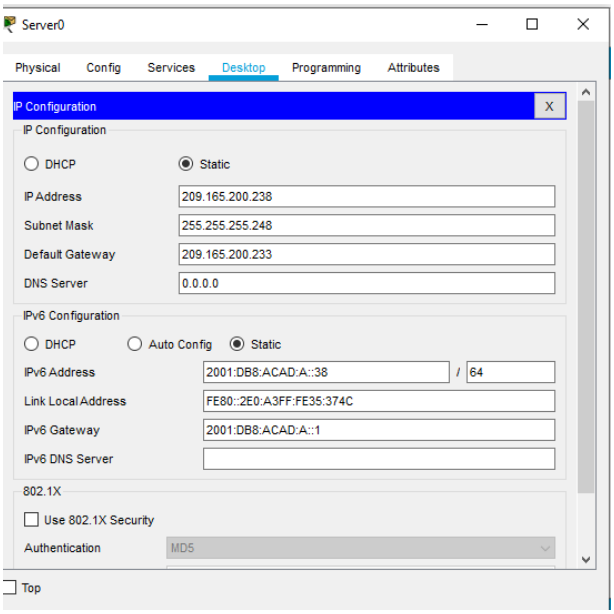
Configurar los parámetros básicos de los dispositivos

Configurar la computadora de Internet

Tabla 12. Especificaciones servidor de internet

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	2 255.255.255.248
Gateway predeterminado	209.165.200.233
Dirección IPv6/subred	2001:db8:acad:a::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:a::1

Figura 15. Dirección IP servidor.



Fuente: Autor

Configurar R1

Configurar el router 1, de acuerdo al paso a paso que se establece a continuación las cuales hacen referencia a la configuración inicial de este dispositivo, garantizando una seguridad en la implementación del router en una red.

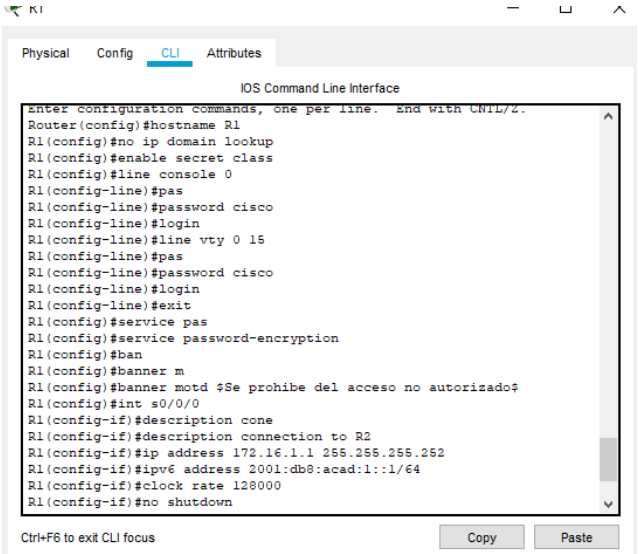
Tabla 13. Lista de comandos de configuración Router 1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	R1(config)#no ip domain-lookup
Nombre del router	R1 Router(config)#hostname R1
Contraseña de exec privilegiado cifrada	Class R1(config)#enable secret class
Contraseña de acceso a la consola	R1(config)#line console 0 R1(config-line)#password cisco R1(config-line)#login

Contraseña de acceso Telnet	Cisco R1(config-line)#line vty 0 15 R1(config-line)#password cisco R1(config-line)#login
Cifrar las contraseñas de texto no cifrado	R1(config-line)#service password-encryption
Mensaje MOTD Se prohíbe el acceso no autorizado.	R1(config)#banner motd $Se prohíbe el acceso no autorizado$
Interfaz S0/0/0 Establezca la descripción Establecer la dirección IPv4 Establecer la dirección IPv6 Establecer la frecuencia de reloj en 128000 Activar la interfaz	R1(config-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 Configurar una ruta IPv4 predeterminada de S0/0/0 Configurar una ruta IPv6 predeterminada de S0/0/0	R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0 %Default route without gateway, if not a point-to-point interface, may impact performance R1(config)#ipv6 route ::/0 s0/0/0

Nota: Todavía no configure G0/1.

Figura 16. Configuración R1



Fuente: Autor

Configurar R2

Se debe realizar la configuración del Router 2 de acuerdo a los pasos que se relacionan a continuación en la tabla con su respectiva lista de comandos.

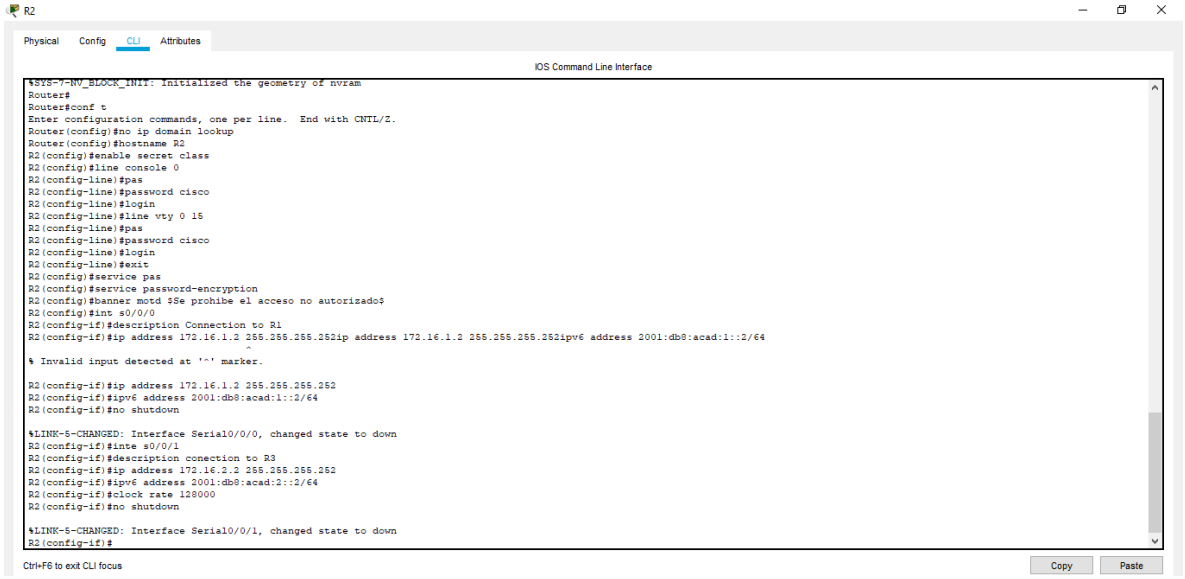
Tabla 14. Lista de comandos configuración Router 2

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	R2(config)#no ip domain-lookup
Nombre del router R2	Router(config)#hostname R2
Contraseña de exec privilegiado cifrada Class	R2(config)#enable secret class
Contraseña de acceso a la consola Cisco	R2(config)#line console 0 R2(config-line)#password cisco R2(config-line)#login
Contraseña de acceso Telnet Cisco	R2(config-line)#line vty 0 15 R2(config-line)#password cisco R2(config-line)#login
Cifrar las contraseñas de texto no cifrado	R2(config-line)#service password-encryption
Habilitar el servidor HTTP	R2(config)#ip http server
Mensaje MOTD Se prohíbe el acceso no autorizado.	R2(config)#banner motd $Se prohíbe el acceso no autorizado$
Interfaz S0/0/0 Establezca la descripción Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. Establezca la dirección IPv6. Activar la interfaz	R2(config)#inte s0/0/0 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 Establecer la descripción Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Establezca la dirección IPv6. Establecer la frecuencia de reloj en 128000. Activar la interfaz	R2(config-if)#inte s0/0/1 R2(config-if)#description conection 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) Establecer la descripción. Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Establezca la dirección IPv6. Utilizar la primera dirección disponible en la subred. Activar la interfaz	R2(config)#inte s0/0/0 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 R2(config-if)#inte s0/0/1 R2(config-if)#description conection 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 R2(config-if)#int g 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 2000:db8:acad:a::1/64 R2(config-if)#no shutdown
Interfaz loopback 0 (servidor web simulado) Establecer la descripción. Establezca la dirección IPv4.	R2(config-if)#ip address 10.10.10.10 255.255.255.255 R2(config-if)#description Web server R2(config-if)#exit

Ruta predeterminada Configure una ruta IPv4 predeterminada de G0/0. Configure una ruta IPv6 predeterminada de G0/0.	R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0 %Default route without gateway, if not a point-to-point interface, may impact performance R2(config)#ipv6 route ::/0 g0/0

Figura 17. Configuración R2



Fuente: Autor

Configurar R3

Se debe realizar la configuración del Router 2 de acuerdo a los pasos que se relacionan a continuación en la tabla con su respectiva lista de comandos.

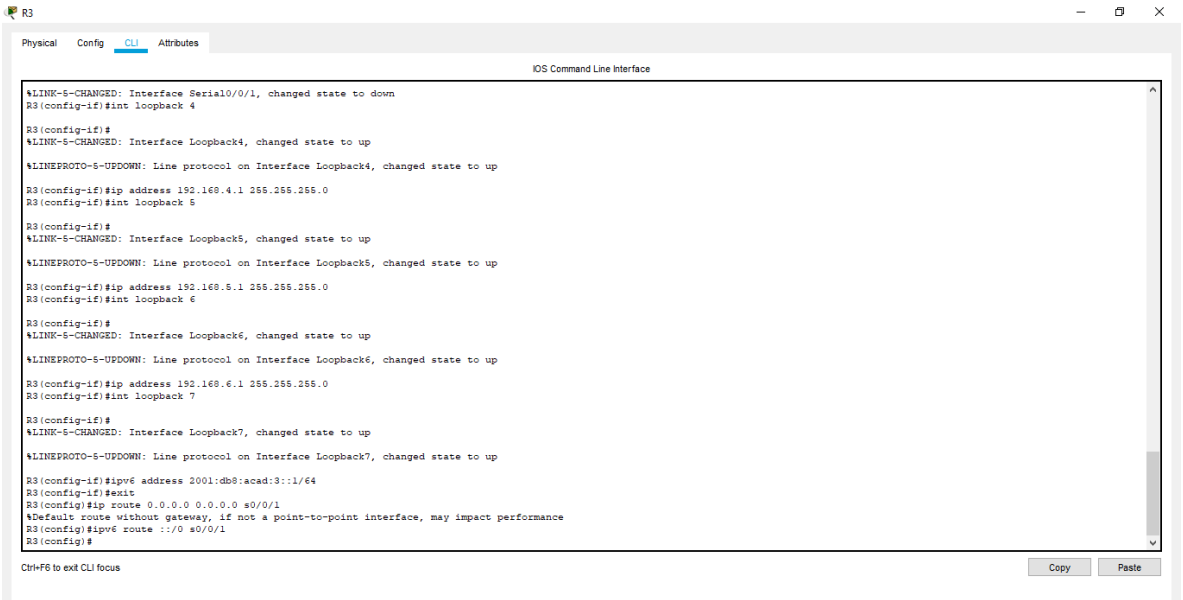
Tabla 15. Lista de comandos configuración Router 3.

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	R3(config)#no ip domain lookup

Nombre del router	Router>enable Router#configure terminal Router(config)#hostname R3
Contraseña de exec privilegiado cifrada	Class R3(config)#enable secret class
Contraseña de acceso a la consola	Cisco R3(config)#line console 0 R3(config-line)#pas R3(config-line)#password cisco R3(config-line)#login
Contraseña de acceso Telnet	Cisco R3(config-line)#line vty 0 15 R3(config-line)#pas R3(config-line)#password cisco R3(config-line)#login
Cifrar las contraseñas de texto no cifrado	R3(config-line)#service password encryption
Mensaje MOTD Se prohíbe el acceso no autorizado.	R3(config)#banner motd $Se prohibe el acceso no autorizado$
Interfaz S0/0/1 Establecer la descripción Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz	R3(config)#int s0/0/1 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 Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.	R3(config-if)#int loopback 4 R3(config-if)#ip address 192.168.4.1 255.255.255.0

Interfaz loopback 5 Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.	R3(config-if)#int loopback 5 R3(config-if)#ip address 192.168.5.1 255.255.255.0
Interfaz loopback 6 Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.	R3(config-if)#int loopback 6 R3(config-if)#ip address 192.168.6.1 255.255.255.0
Interfaz loopback 7 Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.	R3(config-if)#int loopback 7 R3(config-if)#ipv6 ad R3(config-if)#ipv6 address 2001:db8:acad:3::1/64
Rutas predeterminadas	R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1 %Default route without gateway, if not a point-to-point interface, may impact performance R3(config)#ipv6 route ::/0 s0/0/1

Figura 18. Configuración R3



Fuente: Autor

Configurar S1

Se debe configurar el switch número 1, asignándole la clave de acceso, cifrarla y un mensaje de advertencia a los usuarios que quieran ingresar sin acceso al dispositivo.

Tabla 16. Lista de comandos configuración S1.

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	S1(config)#no ip domain-lookup
Nombre del switch	S1 Switch(config)#hostname S1
Contraseña de exec privilegiado cifrada	Class S1(config)#enable secret class S1(config)#line console 0
Contraseña de acceso a la consola	Cisco S1(config-line)#password cisco S1(config-line)#login
Contraseña de acceso Telnet	Cisco S1(config-line)#line vty 0 15 S1(config-line)#password cisco S1(config-line)#login
Cifrar las contraseñas de texto no cifrado	S1(config-line)#service password-encryption
Mensaje MOTD Se prohíbe el acceso no autorizado.	S1(config)#banner mtd $Se prohibe el acceso no autorizado$

Configurar el S3

Se debe configurar el switch número 3, asignándole la clave de acceso, cifrarla y un mensaje de advertencia a los usuarios que quieran ingresar sin acceso al dispositivo.

Tabla 17. Lista de comandos configuración S3.

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	S3(config)#no ip domain-lookup
Nombre del switch	Switch>enable Switch#configure terminal Switch(config)#hostname S3
Contraseña de exec privilegiado cifrada “Class”	S3(config)#enable secret class S3(config)#line console 0
Contraseña de acceso a la consola “Cisco”	S3(config-line)#password cisco S3(config-line)#login
Contraseña de acceso Telnet “Cisco”	S3(config-line)#line vty 0 15 S3(config-line)#password cisco S3(config-line)#login
Cifrar las contraseñas de texto no cifrado	S3(config-line)#service password-encryption
Mensaje MOTD Se prohíbe el acceso no autorizado.	S3(config)#banner motd $Se prohibe el acceso no autorizado$

Verificar la conectividad de la red

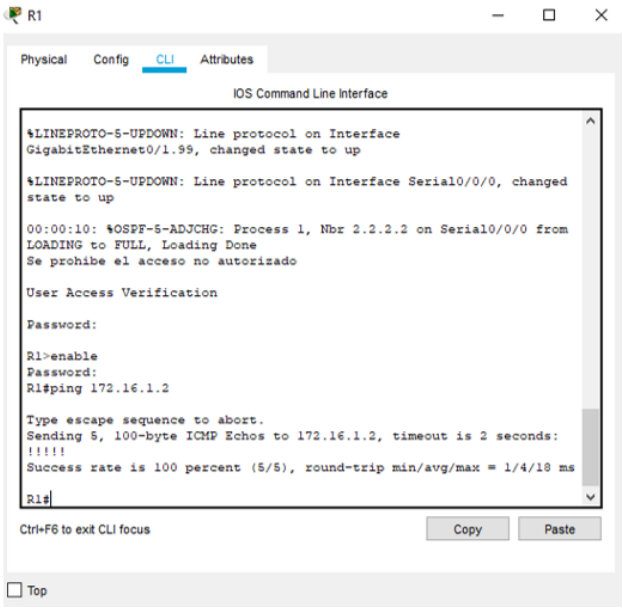
Utilice el comando ping para probar la conectividad entre los dispositivos de red.

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:

Desde R1 a R2, S0/0/0 dirección: 172.16.1.2

Probar conexión a través del código ping entre R1 y R2

Figura 19. Ping 170.16.1.2

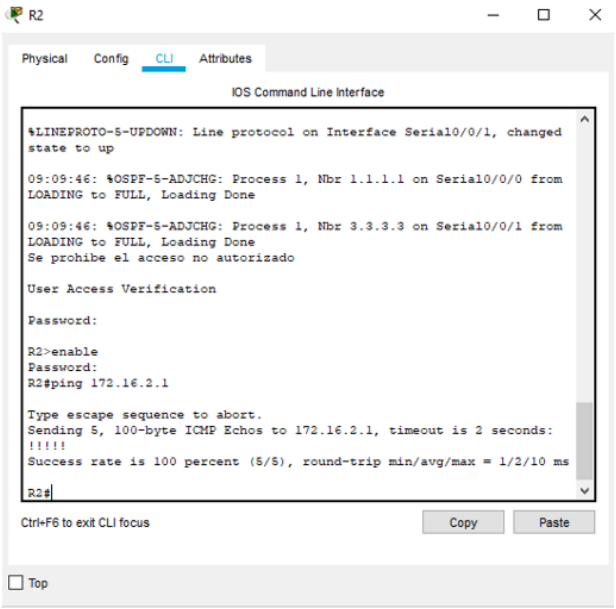


Fuente: Autor

Desde R2 a R3, S0/0/1 dirección: 172.16.2.1

Probar conexión a través del código ping entre R2 y R3

Figura 20. Ping 172.16.2.1

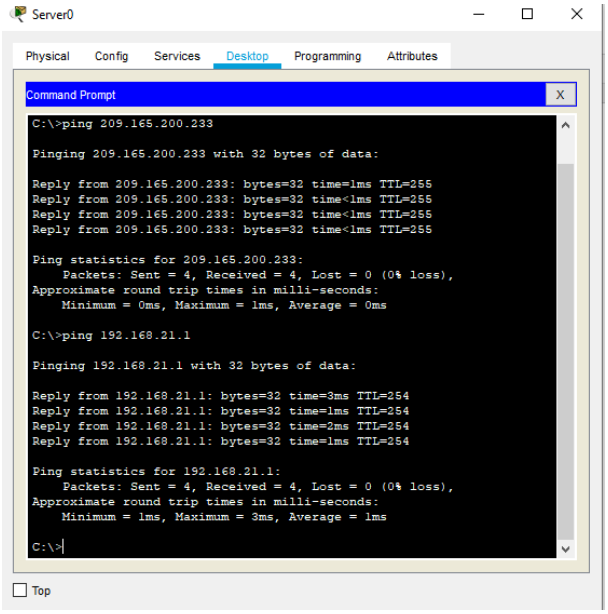


Fuente: Autor

Desde PC de Internet a Gateway predeterminado ping 209.165.200.233

Probar conexión a través servidor al Gateway predeterminado

Figura 21. Ping 209.165.200.233



Fuente: Autor

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

Configurar S1

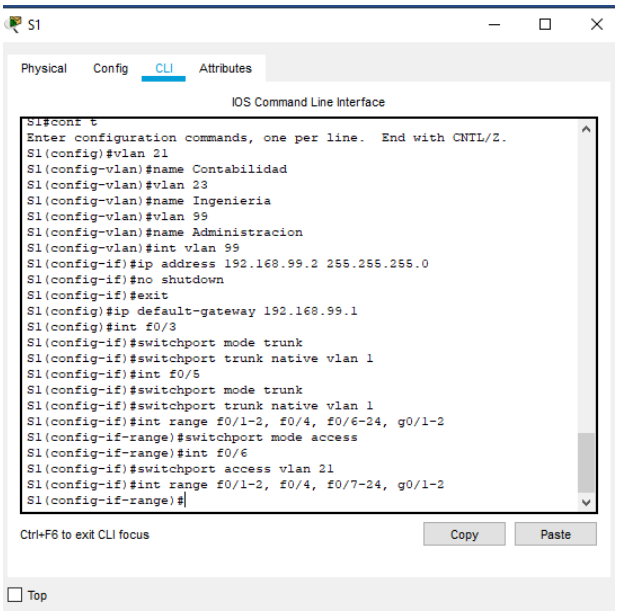
Configurar las vlan en S1 que se relacionan en la topología del escenario con el fin de asignar su dirección ip y el enlace troncal entre las interfaces de comunicación.

Tabla 18. Lista de comandos configuración Vlan en S1

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN Utilizar la tabla de equivalencias de VLAN para topología para crear y nombrar cada una de las VLAN que se indican.	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. Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S1 en el diagrama de topología	S1(config)#int vlan 99 S1(config-if)#ip address 192.168.99.2 255.255.255.0 S1(config-if)#no shutdown
Asignar el gateway predeterminado Asigne la primera dirección IPv4 de la subred como el gateway predeterminado.	S1(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3 Utilizar la red VLAN 1 como VLAN nativa	S1(config)#int f0/3 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1
Forzar el enlace troncal en la interfaz F0/5 Utilizar la red VLAN 1 como VLAN nativa	S1(config-if)#int f0/5 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso, Utilizar el comando interface range	S1(config-if)#int 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)#int f0/6 S1(config-if)#switchport access vlan 21
Apagar todos los puertos sin usar	S1(config-if)#int range f0/1-2, f0/4, f0/7-24, g0/1-2 S1(config-if-range)#shutdown

Figura 22. Configuración S1



Fuente: Autor

Configurar el S3

La configuración del S3 incluye la lista de comandos donde se incluyen las vlan que se establecieron en la topología de nuestra red, asignando las respectivas direcciones ip para su comunicación acertada con los demás dispositivos.

Tabla 19. Lista de comandos configuración S3

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN Utilizar la tabla de equivalencias de VLAN para topología para crear cada una de las VLAN que se indican Dé nombre a cada VLAN.	S3(config)#vlan 21 S3(config-vlan)#name Contabilidad S3(config-vlan)#vlan 23 S3(config-vlan)#name Ingenieria S3(config-vlan)#vlan 99 S3(config-vlan)#name Administracion S3(config-vlan)#exit
Asignar la dirección IP de administración. Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S3 en el diagrama de topología	S3(config-if)#ip address 192.168.99.3 255.255.255.0

Asignar la primera dirección IP en la subred como gateway predeterminado.	S3(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3. Utilizar la red VLAN 1 como VLAN nativa	S3(config)#int f0/3 S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso. Utilizar el comando interface range	S3(config-if)# int range 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)#int f0/18 S3(config-if)#switchport access vlan 23
Apagar todos los puertos sin usar	S3(config-if)#int range f0/1-2, f0/4-17, f0/19-24, g0/1-2 S3(config-if-range)#shutdown

Configurar R1

Las tareas de configuración para R1 en este cuadro hacen referencias a las redes LAN de nuestra topología asignando las direcciones ip y realizando una encapsulación de las mismas, se debe tener en cuenta que se están configurando las subinterfaces.

Tabla 20. Lista de comandos de configuración de R1

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1 Descripción: LAN de Contabilidad Asignar la VLAN 21 Asignar la primera dirección disponible a esta interfaz	R1(config)#int g0/1.21 R1(config-subif)#description VLAN21 R1(config-subif)#encapsulation d R1(config-subif)#encapsulation dot1Q 21 R1(config-subif)#ip ad 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)#int g0/1.23 R1(config-subif)#description VLAN 23 R1(config-subif)#encapsulation d 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 Descripción: LAN de Administración Asignar la VLAN 99 Asignar la primera dirección disponible a esta interfaz	R1(config-subif)#int g0/1.99 R1(config-subif)#description VLAN 99 R1(config-subif)#encapsulation dot1Q 99 R1(config-subif)#ip address 192.168.99.1 255.255.255.0
Activar la interfaz G0/1	R1(config-subif)#int g0/1 R1(config-if)#no shutdown

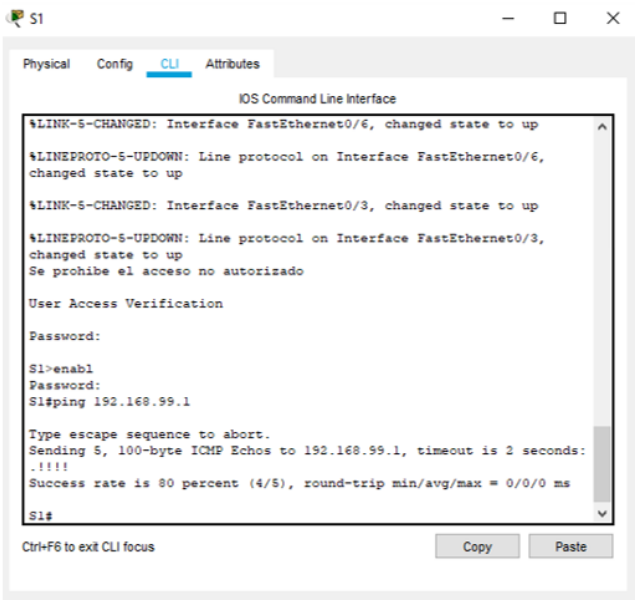
Verificar la conectividad de la red

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:

Desde S1 a R1, dirección VLAN 99 192.168.99.1

Figura 23. Ping 192.168.99.1

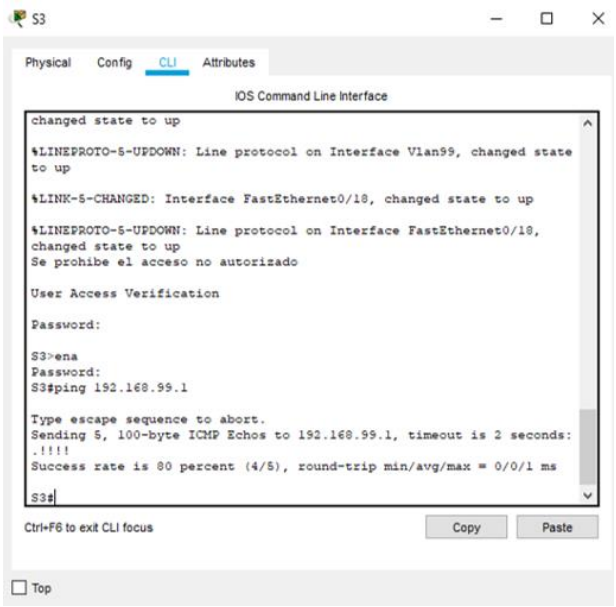


Fuente: Autor

Desde S3 a R1, dirección VLAN 99 192.168.99.1

A través del comando ping se verifica la conexión de S3 con la Vlan 99 de R1

Figura 24. Ping 192.168.99.1

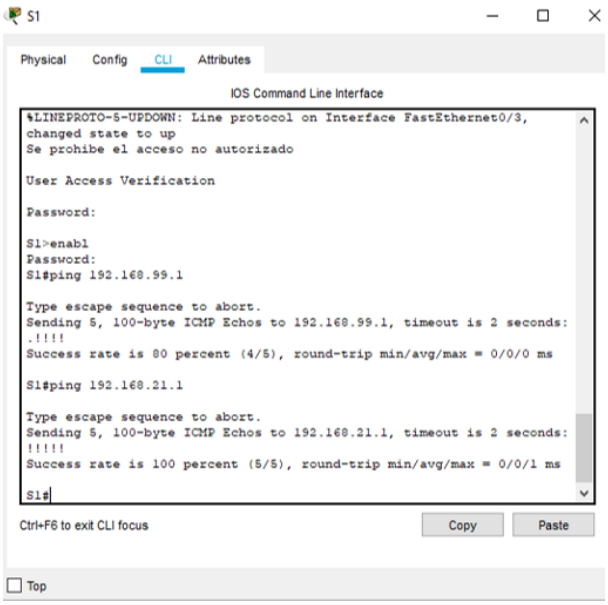


Fuente: Autor

Desde S1 a R1, dirección VLAN 21 192.168.21.1

A través del comando ping se verifica la conexión de S1 con la Vlan 21 de R1

Figura 25. Ping 192.168.21.1

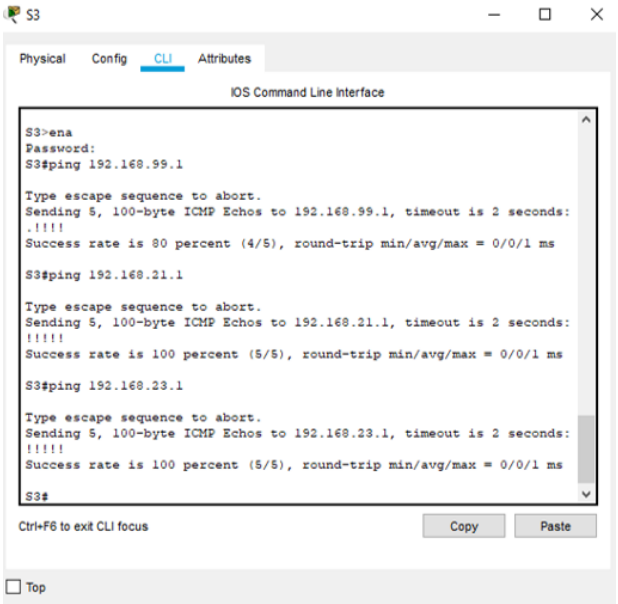


Fuente: Autor

Desde S3 a R1, dirección VLAN 23 192.168.23.1

A través del comando ping se verifica la conexión de S3 con la Vlan 23 de R1

Figura 26. Ping 192.168.23.1



Fuente: Autor

Configurar el protocolo de routing dinámico OSPF

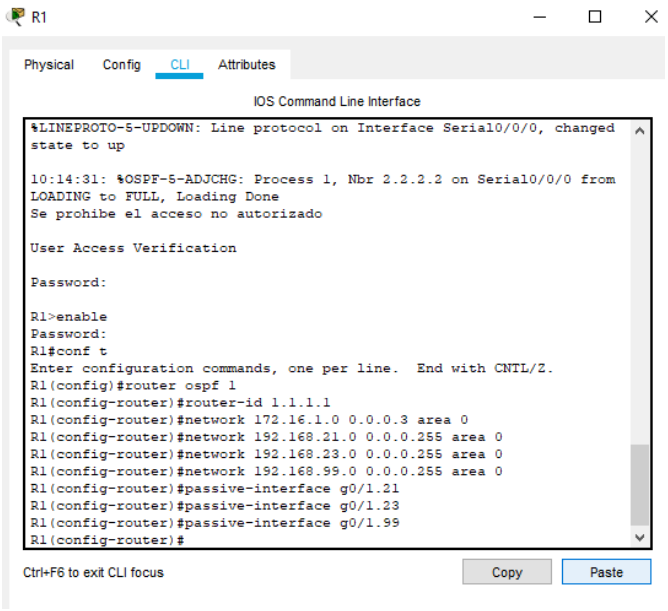
Configurar OSPF en el R1

Las tareas de configuración para R1 que se relacionan a continuación es del protocolo OSPF que hace referencia a encontrar la vía más corta para la comunicación entre los dispositivos.

Tabla 21. Lista de comandos OSPF en R1.

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R1(config)#router ospf 1 R1(config-router)#router-id 1.1.1.1
Anunciar las redes conectadas directamente. Asigne todas las redes conectadas directamente.	R1(config-router)#network 172.16.1.0 0.0.0.3 area 0 R1(config-router)#network 192.168.21.0 0.0.0.255 area 0 R1(config-router)#network 192.168.23.0 0.0.0.255 area 0 R1(config-router)#network 192.168.99.0 0.0.0.255 area 0
Establecer todas las interfaces LAN como pasivas	R1(config-router)#passive-interface g0/1.21 R1(config-router)#passive-interface g0/1.23 R1(config-router)#passive-interface g0/1.99
Desactive la sumarización automática	No auto-summary

Figura 27. Configuración OSPF en R1



Fuente: Autor

Configurar OSPF en el R2

Se va realizar el mismo procedimiento de configuración de R1 que vimos anteriormente mediante la metodología OSPF en el R2 a las redes de las cuales tiene acceso.

Tabla 22. Lista de comandos configuración OSPF en R2

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R2(config)#router ospf 1 R2(config-router)#router-id 2.2.2.2
Anunciar las redes conectadas directamente. Nota: Omitir la red G0/0.	R2(config-router)#network 172.16.2.0 0.0.0.3 area 0 R2(config-router)#network 172.16.2.0 0.0.0.3 area 0
Establecer la interfaz LAN (loopback) como pasiva	R2(config-router)#passive-interface g0/1
Desactive la sumarización automática.	No auto-summary

Configurar OSPFv3 en el R3

La configuración OSPF del área 0 en el Router 3, anunciando las respectivas direcciones ip y generando un comando para establecer las interfaces de la red LAN como pasivas.

Tabla 23. Lista de comandos OSPF en R 3

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R3(config)#router ospf 1 R3(config-router)#ro R3(config-router)#router-id 3.3.3.3 R3(config-router)#ne R3(config-router)#net
Anunciar redes IPv4 conectadas directamente	R3(config-router)#network 172.16.2.0 0.0.0.3 area 0 R3(config-router)#network 192.168.4.0 0.0.3.255 area 0
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	R3(config-router)#passive-interface loopback 4 R3(config-router)#passive-interface l R3(config-router)#passive-interface loopback 5 R3(config-router)#passive-interface loopback 6 R3(config-router)#passive-interface loopback 7
Desactive la sumarización automática.	No auto-summary

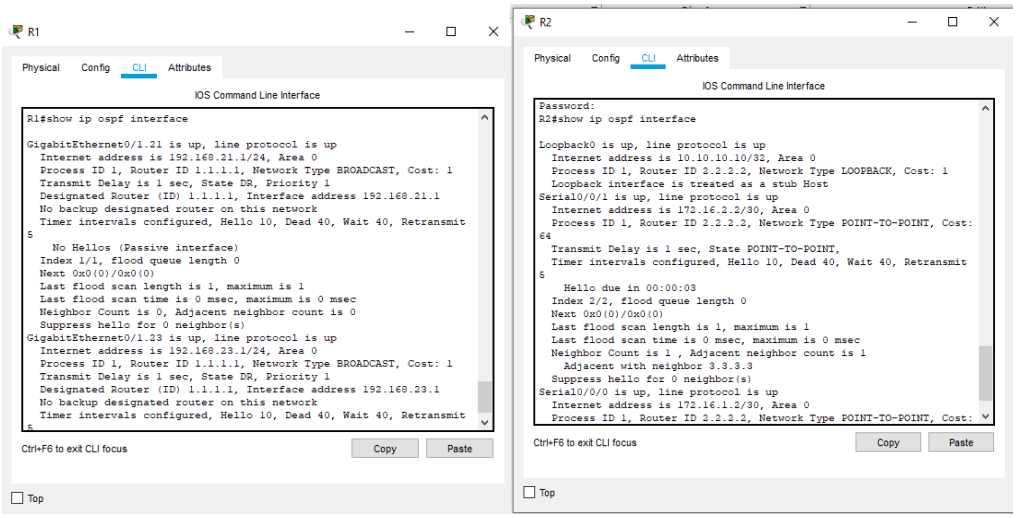
Verificar la información de OSPF

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

¿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?

show ip ospf interface

Figura 28. Ejecución del comando.

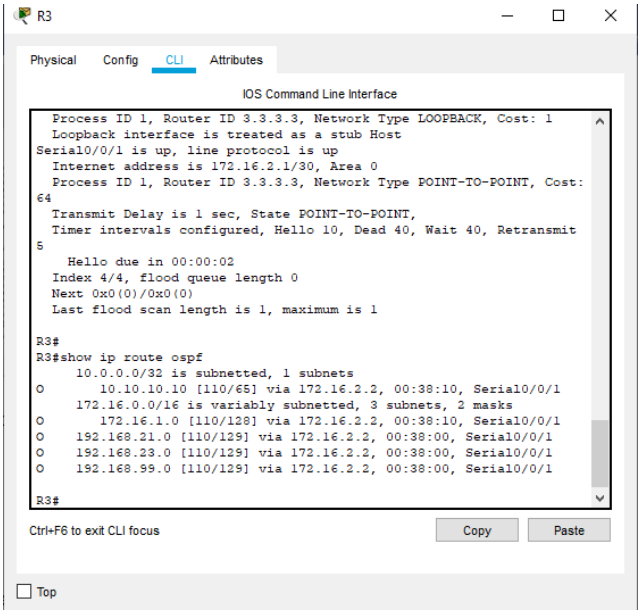


Fuente: Autor

¿Qué comando muestra solo las rutas OSPF?

R3# show ip route ospf

Figura 29. Comando show ip route ospf

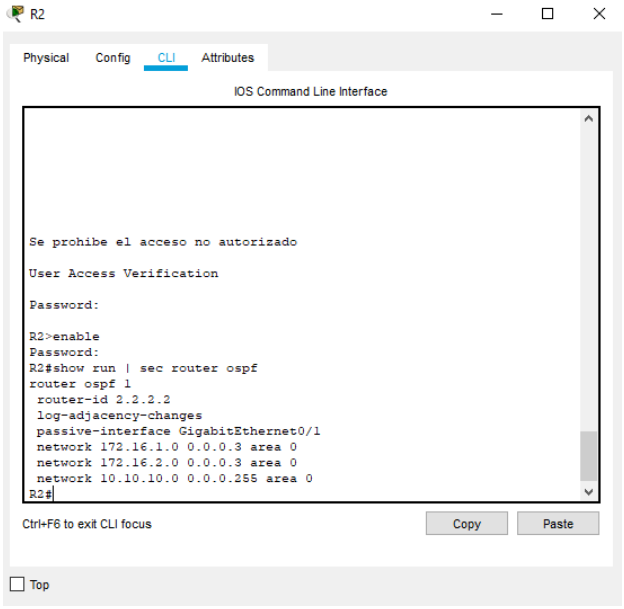


Fuente: Autor

¿Qué comando muestra la sección de OSPF de la configuración en ejecución?

show run | sec router ospf

Figura 30. Comando show run | sec router ospf



Fuente: Autor

Implementar DHCP y NAT para IPv4

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

Se va realizar una lista de comandos con el cual se piensa configurar R1 como un servidor DHCP para las VLAN 21 y 23, reservando unas direcciones ip para su configuración estática, así mismo la creación del pool para cada VLAN.

Tabla 24. Lista de comandos R1 como servidor DHCP

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

Crear un pool de DHCP para la VLAN 21. Nombre: ACCT Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado	R1(config)#ip dhcp pool ACCT R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com R1(dhcp-config)#default-router 192.168.21.1 R1(dhcp-config)#network 192.168.21.1 255.255.255.0
Crear un pool de DHCP para la VLAN 23. Nombre: ENGNR Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado	R1(dhcp-config)#ip dhcp pool ENGNR R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com R1(dhcp-config)#default-router 192.168.23.1 R1(dhcp-config)#network 192.168.23.0 255.255.255.0

Configurar la NAT estática y dinámica en el R2

La configuración del R2 lleva a cabo la creación de una base de datos local con su respectivo usuario, así como la configuración de la NAT estatice en el servidor y estableciendo las redes que harán parte de esta de forma dinámica.

Tabla 25. Lista de comandos configuración NAT en R2

Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario. Nombre de usuario: webuser Contraseña: cisco12345 Nivel de privilegio: 15	R2(config)#user 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.	Dirección global interna: 209.165.200.229
Asignar la interfaz interna y externa para la NAT estática	R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229

Configurar la NAT dinámica dentro de una ACL privada. Lista de acceso: 1 Permitir la traducción de las redes de Contabilidad y de Ingeniería en el R1 Permitir la traducción de un resumen de las redes LAN (loopback) en el R3	R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255
Defina el pool de direcciones IP públicas utilizables. Nombre del conjunto: INTERNET El conjunto de direcciones incluye: 209.165.200.225 – 209.165.200.228	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 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

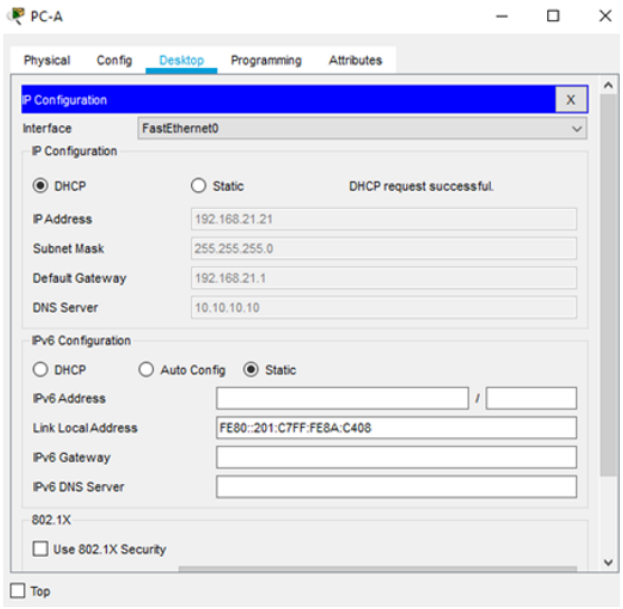
Verificar el protocolo DHCP y la NAT estática

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.

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

Una vez realizada la configuración del servidor DHCP ser verifica que los host obtengan la información solicitada.

Figura 31. PC-A con información del servidor DHCP

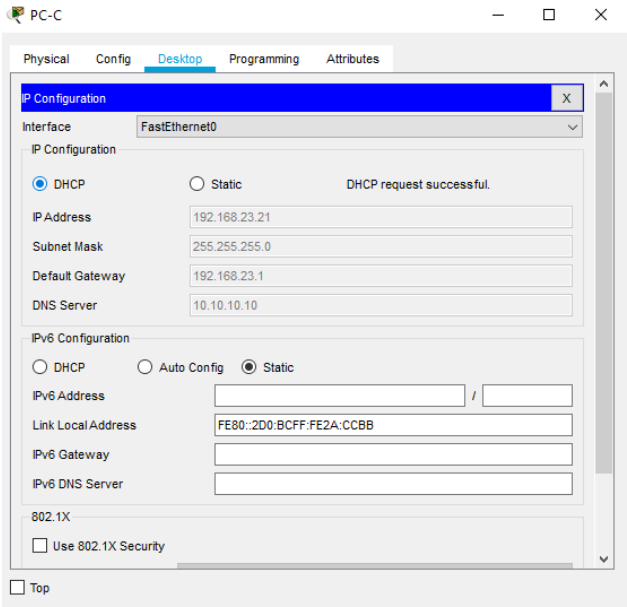


Fuente: Autor

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

Una vez realizada la configuración del servidor DHCP ser verifica que los host obtengan la información solicitada.

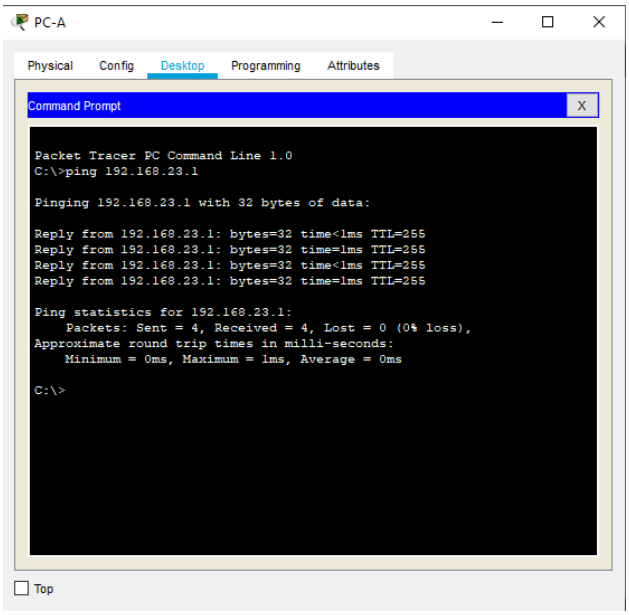
Figura 32. PC-B con información del servidor DHCP



Fuente: Autor

Verificar que la PC-A pueda hacer ping a la PC-C. Nota: Quizá sea necesario deshabilitar el firewall de la PC.

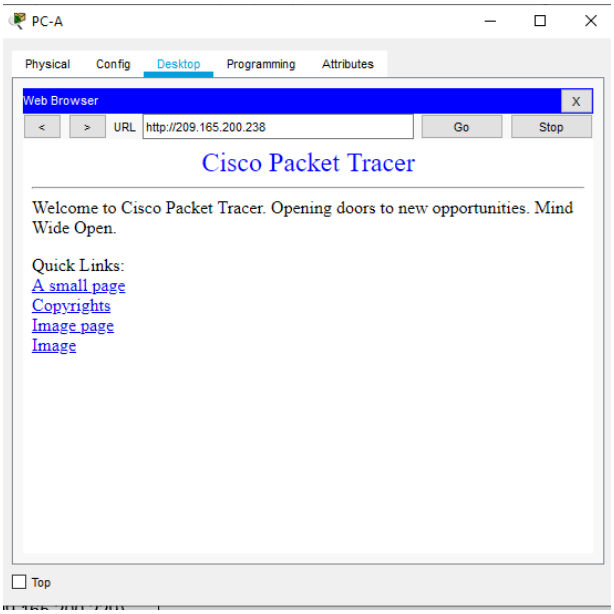
Figura 33. Ping PC-A a PC-C



Fuente: Autor

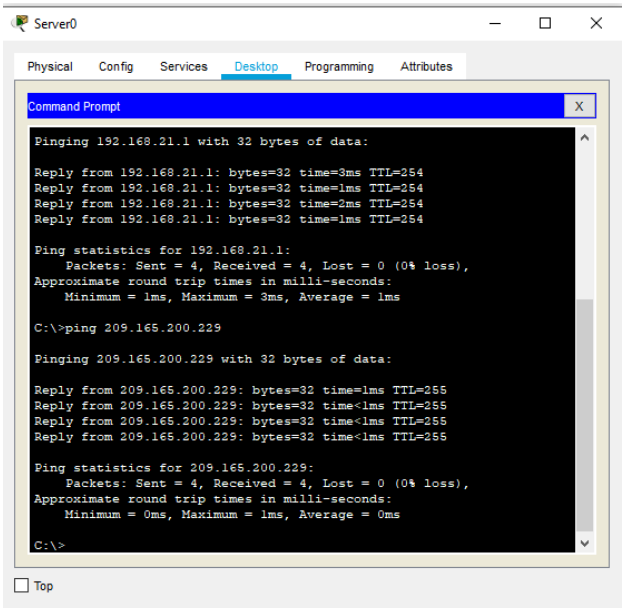
Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.229) Iniciar sesión con el nombre de usuario webuser y la contraseña cisco12345

Figura 34. Navegador WEB



Fuente: Autor

Figura 35. Ping 209.165.200.229



Fuente: Autor

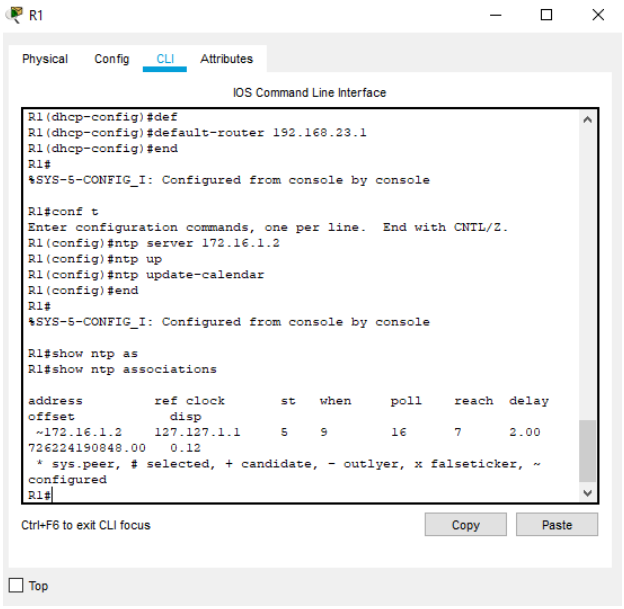
Configurar NTP

En este procedimiento se va realizar la configuración en R2 de la hora y fecha señalada en el ejercicio, configuración de maestro NTP, R1 como un cliente y las actuaciones de calendario de manera periódica en un lapso de una hora.

Tabla 26. Configuración de NTP en R1 y R2.

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2. 5 de marzo de 2016, 9 a. m.	R2#clock set 9:00:00 5 March 2016
Configure R2 como un maestro NTP. Nivel de estrato: 5	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

Figura 36. Configuración NTP en R1



Fuente: Autor

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

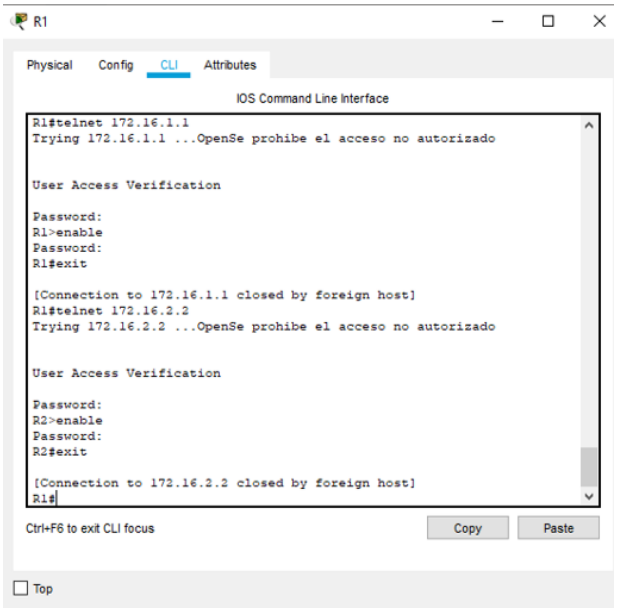
Restringir el acceso a las líneas VTY en el R2

Tabla 27. Configuración ACL en R2

Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2. Nombre de la ACL: ADMIN-MGT	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-cla ADMIN-MGT in
Verificar que la ACL funcione como se espera	telnet 172.16.14.2 Connection refused for foreign host telnet 172.16.14.2 Connection refused for foreign host

Permitir acceso por Telnet a las líneas de VTY

Figura 37. Acceso por Telnet



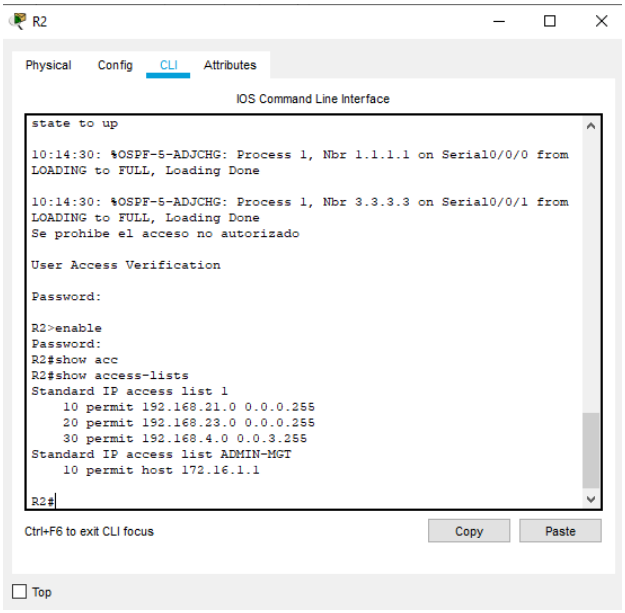
Fuente: Autor

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

Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció

R2#show access-lists

Figura 38. Ejecución comando show access-list



Fuente: Autor

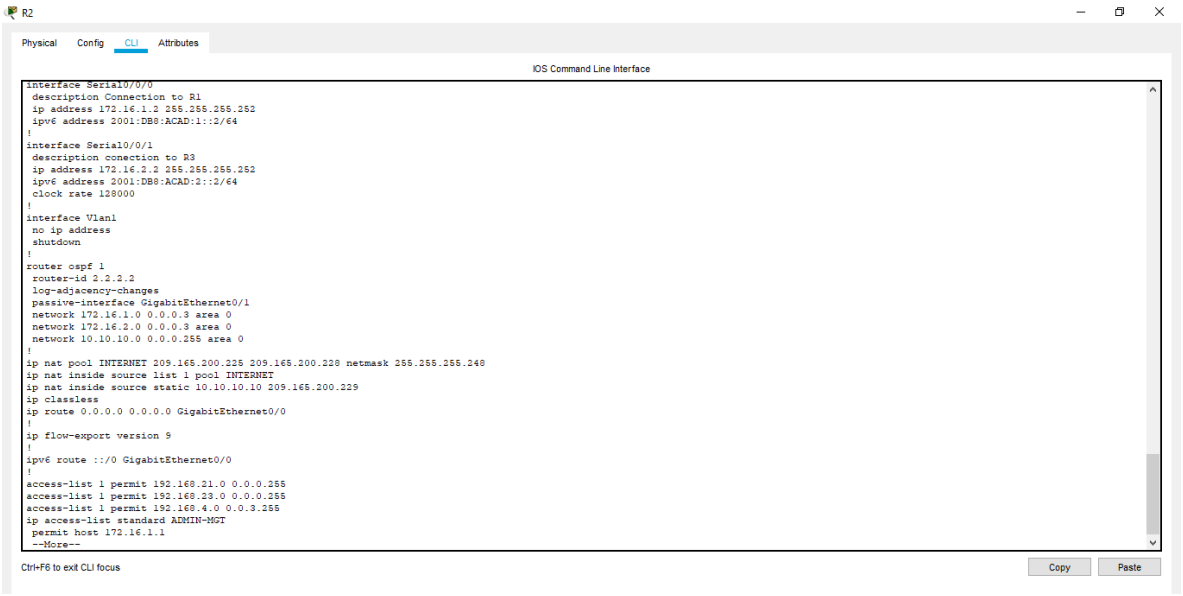
Restablecer los contadores de una lista de acceso

R2#clear ip access-list counters

¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?

R2#show running-config

Figura 39. Ejecución del comando show running-config

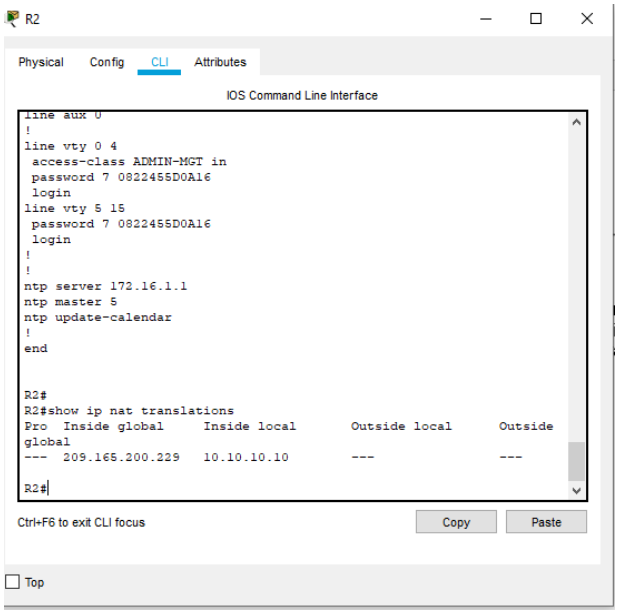


¿Con qué comando se muestran las traducciones NAT?

Nota: Las traducciones para la PC-A y la PC-C se agregaron a la tabla cuando la computadora de Internet intentó hacer ping a esos equipos en el paso 2. Si hace ping a la computadora de Internet desde la PC-A o la PC-C, no se agregarán las traducciones a la tabla debido al modo de simulación de Internet en la red.

R2#show ip nat translations

Figura 40. Ejecución del comando show ip nat translations



Fuente: Autor

¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?
Clear ip nat translations

Conclusiones

- A través del presente trabajo se puso en práctica los conocimientos adquiridos en el desarrollo del curso, es importante resaltar que se debe conocer la estructura de los equipos para poder aplicar la configuración adecuada y lograr la conexión en red esperada.

- Es importante en la configuración de una red asignar de manera correcta las direcciones ip a cada dispositivo y así con el protocolo configurado del router podrá tomar la mejor ruta y enviar el mensaje en el menor tiempo posible, de acuerdo a la metodología OSPF presente en el escenario número 2.

- Se logro identificar la diferencia entre LSO protocolos de enrutamiento RIP donde OSPF envía publicaciones del estado de enlace LSA a los router que pertenecen a la misma jerarquía mediante una multidifusión de IP, los cuales a través de su algoritmo buscan calcular la mejor ruta a cada host.

- Durante el desarrollo de los escenarios consulte diferentes citas bibliográficas que me orientaran al desarrollo de los protocolos DHCP y OSPF para lograr una configuración adecuada, de acuerdo a lo solicitado en la guía de actividades.

- La elaboración de estos escenarios me permitió llevar a cabo el conocimiento que aprendí durante el desarrollo del diplomado, generando los pasos básicos en la configuración de los dispositivos, generando niveles de seguridad y la verificación de conectividad, identificando de diferencia entre IPV4 y IPV6, teniendo un mayor campo de conocimiento con los diferentes ejercicios que se llevaron a cabo en las anteriores actividades.

- Importante resaltar la experiencia con un programa de simulación como lo es packet tracer, el cual se acerca a la realidad frente a la configuración de los dispositivos y dándome una cercanía con los códigos de programación y familiarizándome con esta familia como lo es CISCO, para así tener las competencias para llevarlo a la práctica.

Bibliografía

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

CISCO. (2019). DHCP. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#8

CISCO. (2019). Routing Dinámico. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#3

CISCO. (2019). DHCP. PRINCIPIOS DE ENRUTAMIENTO Y CONMUTACIÓN. RECUPERADO DE: HTTPS://STATIC-COURSE-ASSETS.S3.AMAZONAWS.COM/RSE6/ES/INDEX.HTML#8

CISCO. (2019). ROUTING DINÁMICO. PRINCIPIOS DE ENRUTAMIENTO Y CONMUTACIÓN. RECUPERADO DE: HTTPS://STATIC-COURSE-ASSETS.S3.AMAZONAWS.COM/RSE6/ES/INDEX.HTML#3

Anexos

Anexo 1.

Enlace de descarga de archivos de simulación

https://drive.google.com/drive/folders/1JlbsaACn9GnGGD6mlthIMKMQnOwkL64L?usp=sharing

Anexo 2.

Articulo

https://drive.google.com/drive/folders/16gpfdeWjG7rPDbmCWg5ClUDRew8V1UrC?usp=sharing

Escenario 1 SOLUCIÓN DE UN ESTUDIO DE CASO BAJO EL USO DE TECNOLOGÍA CISCO (diciembre de 2020)

Autor: Jhon Jehider Albarracin Urrutia

Estudiante de Ingeniería de Sistemas

Resumen - En este documento se llevará a cabo la configuración de un escenario que consta de una red LAN, la cual está compuesta por un router, dos switch y dos equipos que admitan tanto la conectividad IPv4 como IPv6 para los hosts soportados. El router y el switch serán administrados de forma segura. Se configurará el protocolo de enrutamiento DHCP y el enlace de

Índice de Términos – switch, router, host, DHCP, VLAN.

Introducción

Con el desarrollo del presente artículo se busca obtener una certificación en redes cisco, el cual en su trayectoria en el Mercado ha venido ofreciendo cursos de capacitación y entrenamiento en el ámbito de los sistemas a diferentes instituciones educativas, fortaleciendo las capacidades del profesional en un mundo de tecnologías que evoluciona de manera constante.

Es de anotar, que a través de los escenarios virtuales brindados por el software suministrado por CISCO buscan la interacción simulada con diferentes elementos que hacen parte de una red, logrando su programación a través de los códigos e instrucciones que buscan establecer una conexión correcta, para así poder llevar a la práctica estos conocimientos y ser competitivos en un mundo laboral.

Metodología

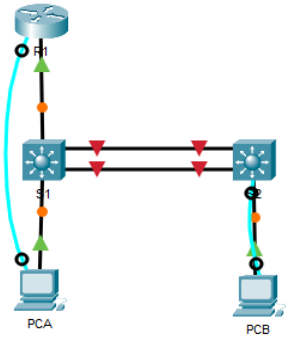
para este articulo opte por la metodología de investigación explicativa se llevaba a cabo para desarrollar de forma puntual un ejercicio que no se había realizado, o que no se había explicado bien con anterioridad. Su intención es proporcionar detalles donde existe una pequeña cantidad de información para lograr el desarrollo del ejercicio en su totalidad.

De acuerdo a lo anterior, en el presente artículo se utilizó desarrollara la configuración de los routers y swicht en una red LAN donde busca realizar la comunicación de los dispositivos en red a través del protocolo DHCP, con dos terminales y la asignación de redes VLAN dentro de la topología, se realizara el procedimiento de asignación de cambio de nombre de los host, asignaciones de direcciones IP y verificación de la conectividad a través del código ping entre los dispositivos, se tomaran las respectivas capturas de pantalla donde se evidencia el funcionamiento del protocolo.

Explicación de la topología a desarrollar

En este escenario se configurarán los dispositivos de una red LAN, la cual está compuesta por un router, dos switch y dos equipos que admitan tanto la conectividad IPv4 como IPv6 para los hosts soportados. El router y el switch serán administrados de forma segura. Configurará el enrutamiento entre VLAN, DHCP, Etherchannel y port-security.

Figura 1. Topología



Fuente: propia

Desarrollo de la actividad.

se crearán las VLAN con los siguientes nombres

2 Bikes
3 Trikes
4 Management
5 Parking

6 Native

TABLA 1.
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

Se procede a inicializar, recargar y configurar aspectos básicos de los dispositivos router y swicht con los siguientes códigos:

TABLA 2.

INICIO Y RECARGA DE LOS ROUTER Y SWICHT

Actividad	Código
Reinicio del router	Router>enable Router#erase startup-config
Volver a cargar el router	Router#reload
Reinicio del swicht	Switch>enable Switch#erase startup-config Switch#delete vlan.dat
Después de recargar el switch, configure la plantilla SDM para que admita IPv6 según sea necesario y vuelva a cargar el switch.	Switch>enable Switch#configure terminal Switch# sdm prefer dual-ipv4-and-ipv6 default Switch#reload

Las tareas de configuración para R1 incluyen tareas que se relacionan en la siguiente tabla, donde se va asignar niveles de seguridad para el dispositivo como es la contraseña de manera cifrada, tanto al ingreso como en el acceso privilegiado, de igual forma la asignación de las direcciones ip a las interfaces que se van a utilizar en esta topología.

TABLA 3.
LISTA DE COMANDOS DE CONFIGURACIÓN ROUTER 1

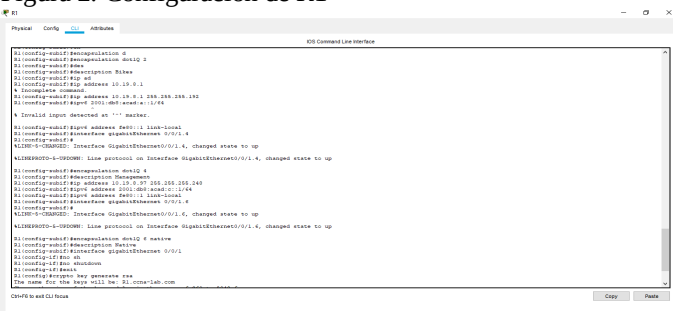
Tarea	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R1
Nombre de dominio	Router(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado ciscoenpass	R1(config)#enable secret ciscoenpass R1(config)#line console 0 R1(config-line)#password ciscoconpass R1(config-line)#login
Contraseña de acceso a la consola	Router(config)# password ciscoconpass
Establecer la longitud mínima para las contraseñas de 10 caracteres	Router(config)#security passwords min-length 10
Crear un usuario administrativo en la base de datos	R1(config)#username admin secret admin1pass R1(config)#line vty 0 15 R1(config-line)#login local

Tarea	Especificación
Configurar el inicio de sesión en las líneas VTY	R1(config)#line vty 0 15 R1(config-line)#login local R1(config)#username admin secret admin1pass
Configurar VTY solo aceptando SSH	R1(config-line)#transport input ssh
Cifrar las contraseñas	Router(config)#service password-encryption
Configure un MOTD Banner	R1(config)#banner motd %Acceso no autorizado%
Habilitar el routing IPv6	Router#configure terminal Router(config)#ipv6 unicast-routing
Configurar interfaz G0/0/1 y subinterfaces realizando los pasos que se relacionan a continuación.	Establezca la descripción Establece la dirección IPv4. Establezca la dirección local de enlace IPv6 como fe80: :1 Establece la dirección IPv6. Activar la interfaz. R1(config)#int g0/1 R1(config-if)#no shutdown
Generar una clave de cifrado RSA	R1(config)#crypto key generate rsa How many bits in the modulus [512]: 1024

Una vez tenemos nuestra configuración inicial del Router 1, realizaremos nuestra configuración de las loopback donde le asignaremos las direcciones Ip en la tabla de direcciones del inicio con el siguiente comando el cual será el mismo para todos.

Es de anotar, que se debe trabajar en las subinterfaces con la descripción de las vlan, como lo muestra la siguiente imagen:

Figura 2. Configuración de R1

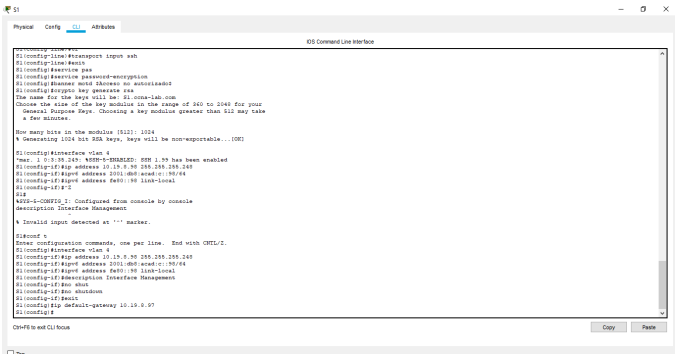


Las tareas de configuración para S1 y S2 incluyen tareas que se relacionan en la siguiente tabla, donde se va asignar niveles de seguridad para ambos dispositivos como es la contraseña de manera cifrada, tanto al ingreso como en el acceso privilegiado, de igual forma la asignación de las direcciones ip a las interfaces que se van a utilizar en esta topología.

TABLA 4.
LISTA DE COMANDOS PARA CONFIGURACIÓN DEL S1

Tarea	Especificación
Desactivar la búsqueda DNS.	Switch(config)#no ip domain lookup
Nombre del switch	Switch(config)#hostname S1
Nombre de dominio. ccna-lab.com	S1(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	S1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	S1(config)#line console 0 S1(config-line)#password ciscoconpass
Crear un usuario administrativo en la base de datos local	S1(config)#username admin secret admin1pass
Configurar el inicio de sesión en las líneas VTY	S1(config)#line vty 0 15 S1(config-line)#login local
Configurar las líneas VTY aceptar las conexiones SSH	S1(config-line)#transport input ssh
Cifrar las contraseñas	S1(config)#service password-encryption
Configurar un MOTD Banner	S1(config)#banner motd %Acceso no autorizado%
Generar una clave de cifrado RSA	Módulo de 1024 bits S1(config)#crypto key generate rsa [512]: 1024
Configurar la interfaz de administración (SVI) Establecer la dirección IPv4 de capa 3 Establezca la dirección local de enlace IPv6 como FE80: :98 para S1 y FE80: :99 para S2 Establecer la dirección IPv6 de capa 3	S1(config)#interface vlan 4 S1(config-if)#ip address 10.19.8.98 255.255.255.248 S1(config-if)#ipv6 address 2001:db8:acad:c::98/64 S1(config-if)#ipv6 address fe80::98 link-local S1(config-if)#description Interface Management S1(config-if)#no shutdown S1(config-if)#exit
Configure la puerta de enlace	S1(config)#ip default-gateway 10.19.8.97

Figura 3. Configuración S1



En la siguiente lista de códigos se encuentran los comandos que se utilizan para la creación de la VLAN en nuestro Swicht, así como los troncos y el modo que configuraremos nuestros puertos de comunicación en nuestra topología

TABLA 6
LISTA DE COMANDOS CREACIÓN VLAN EN S1

Tarea	Especificación
Crear las VLAN en especificadas en la tabla 1. VLAN 2, 3, 4, 5 y 6	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. Interfaces F0/1, F0/2 y F0/5	S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport trunk native vlan 6 S1(config-if)#int range g1/0/1-2 S1(config-if-range)#shutdown S1(config-if-range)#switchport trunk encapsulation dot1q S1(config-if-range)#switchport mode trunk S1(config-if-range)#switchport trunk native vlan 6
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2. Usar el protocolo LACP para la 1negociación	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)#int port-channel 1 S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 6
Configurar el puerto de acceso de host para VLAN 2. Interface F0/6	S1(config-if)#int g1/0/6 S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 2
Configurar la seguridad Permitir 3 direcciones MAC	S1(config-if)#switchport port-security maximum 3
Proteja todas las interfaces no utilizadas Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar	S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 5 S1(config-if-range)#description No esta en uso S1(config-if-range)#shutdown S1(config-if-range)#int range g1/0/7-24 S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 5 S1(config-if-range)#description No esta en uso S1(config-if-range)#shutdown S1(config-if-range)#int range g1/1/1-4 S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 5 S1(config-if-range)#description No está en uso S1(config-if-range)#shutdown

Figura 4. Creación VLAN

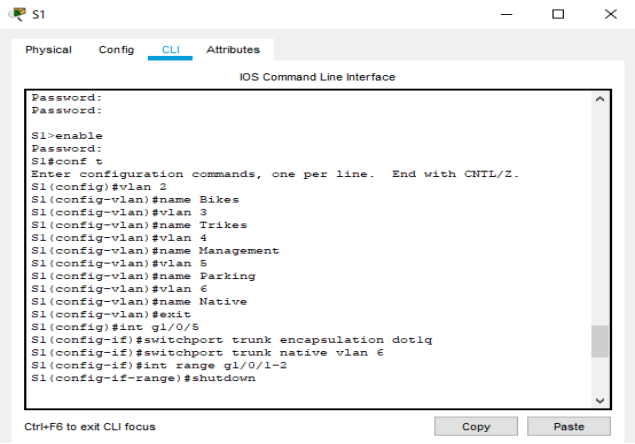
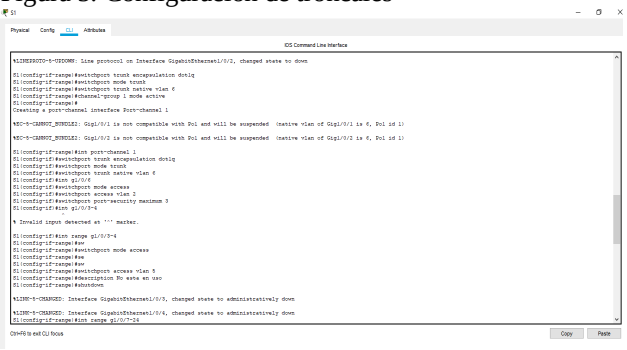


Figura 5. Configuración de troncales

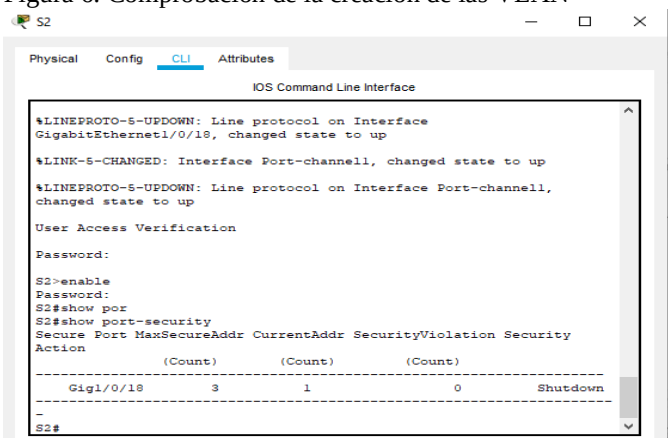


Entre las tareas de configuración de S2 se incluyen las mismas actividades que se realizaron anteriormente en el swicht, 1, como es la creación de las Vlan, configuraciones básicas de seguridad y cambio del nombre del dispositivo, y posteriormente la configuración de la creación de los troncos 802.1Q que utilizan la VLAN 6 en las mismas subinterfaces donde tenemos conexión con el S1:

TABLA 6.
LISTA DE COMANDOS PARA S2

Tarea	Especificación
Configurar el puerto de acceso del host para la VLAN 3 Interfaz F0/18	S2(config-if)#int g1/0/18 S2(config-if)#switchport mode access S2(config-if)#switchport access vlan 3
Configure port-security. Permite 3 MAC addresses	S2(config-if)#switchport port-security maximum 3
Asegure todas las interfaces no utilizadas. Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar	S2(config-if)#int g1/0/18 S2(config-if)#switchport mode access S2(config-if)#switchport access vlan 3 S2(config-if)#switchport port-security maximum 3 S2(config-if)#int range g1/0/3-17 S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 5 S2(config-if-range)#description No está en uso S2(config-if-range)#shutdown S2(config-if-range)#int range g1/0/19-24 S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 5 S2(config-if-range)#description No está en uso S2(config-if-range)#shutdown S2(config-if-range)#int range g1/1/1-4 S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 5 S2(config-if-range)#description No está en uso S2(config-if-range)#shutdown

Figura 6. Comprobación de la creación de las VLAN



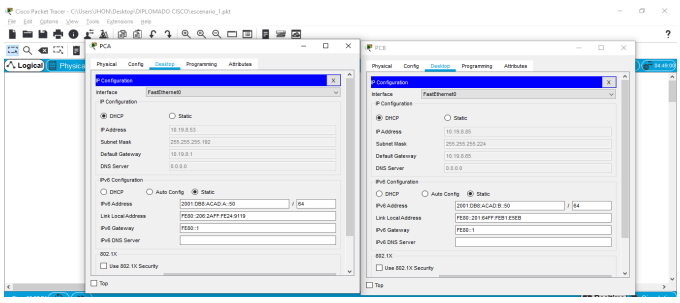
En la siguiente lista de códigos se evidencia los comandos utilizados para la configuración del Router 1, frente a la creación de las rutas predeterminadas tanto en el protocolo IPV4 y el IPV6, las cuales dirigirán el tráfico a la interfaz Loopback 0. Posteriormente la creación de un grupo DHCP para la Vlan 2 y 3.

TABLA 7.
LISTA DE COMANDOS CONFIGURACIÓN ROUTER 1

Tarea	Especificación
Configure Default Routing. Crear rutas predeterminadas para IPv4 e IPv6 que dirijan el tráfico a la interfaz Loopback 0	R1(config)#ip route 0.0.0.0 0.0.0.0 loopback 0 R1(config)#ipv6 route ::/0 loopback 0
Configurar IPv4 DHCP para VLAN 2 Cree un grupo DHCP para VLAN 2, compuesto por las últimas 10 direcciones de la subred solamente.	R1(config)#ip dhcp excluded-address 10.19.8.1 10.19.8.52 R1(config)#ip dhcp pool VLAN2-Bikes R1(dhcp-config)#network 10.19.8.0 255.255.255.192 R1(dhcp-config)#default-router 10.19.8.1 R1(dhcp-config)#domain-name ccna-a.net
Configurar DHCP IPv4 para VLAN 3 Cree un grupo DHCP para VLAN 3, compuesto por las últimas 10 direcciones de la subred solamente.	R1(config)#ip dhcp excluded-address 10.19.8.1 10.19.8.52 R1(config)#ip dhcp pool VLAN2-Bikes R1(dhcp-config)#network 10.19.8.0 255.255.255.192 R1(dhcp-config)#default-router 10.19.8.1 R1(dhcp-config)#domain-name ccna-a.net R1(dhcp-config)#exit R1(config)#ip dhc excluded-address 10.19.8.65 10.19.8.84 R1(config)#ip dhcp pool VLAN3-Trikes R1(dhcp-config)#network 10.19.8.64 255.255.255.224 R1(dhcp-config)#default-router 10.19.8.65 R1(dhcp-config)#domain-name ccna-b.net R1(dhcp-config)#exit

Verificación de las direcciones en los PC donde se evidencia que el protocolo DHCP se hay cumplido en la exclusión de las direcciones IP que dimos en nuestra configuración.

Figura 7. Verificación de las IP.



Para verificar que la configuración anterior realizada a los dispositivos se encuentra correcta se va realizar a continuación

la utilización del comando ping entre los dispositivos como se evidencia en las siguientes imágenes.

Figura 8. Desde la PC-A a R1, G0/0/1.2 Dirección: 10.19.8.1

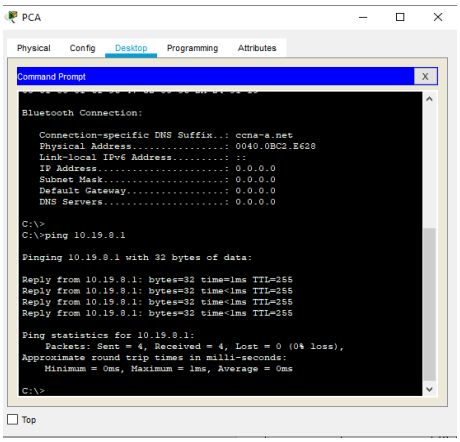


Figura 9. Desde la PC-A a R1, G0/0/1.2 IPv6: 2001:db8:acad:a: :1

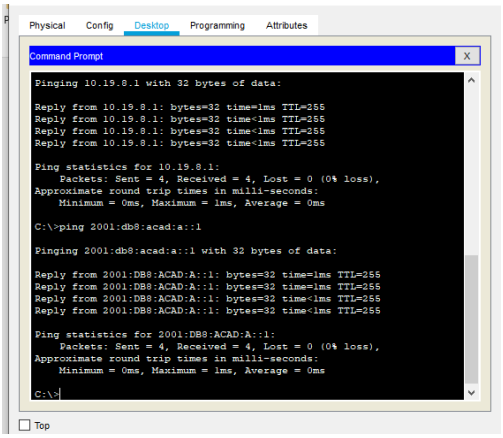
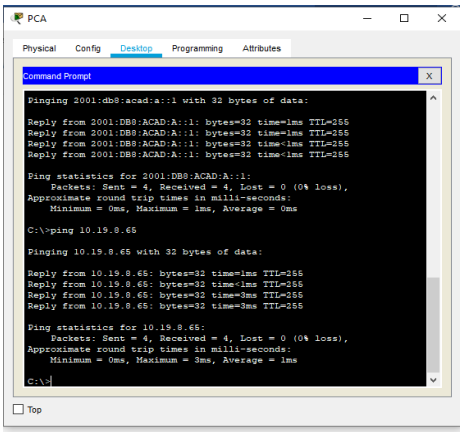


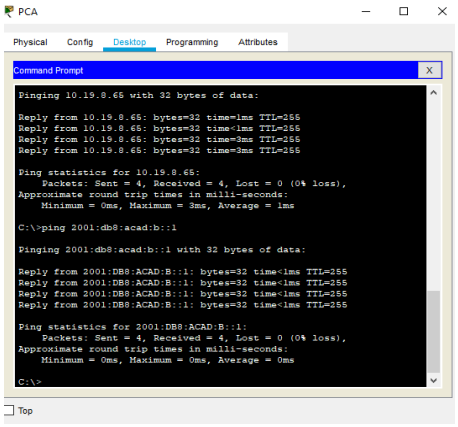
Figura 10. Ping 2001:db8:acad:a: :1

Desde la PC-A a R1, G0/0/1.3 Dirección: 10.19.8.65
Figura 5. Ping 10.19.8.65

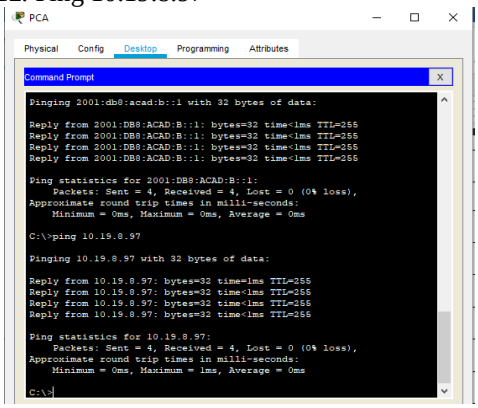


Desde PC-A a R1, G0/0/1.3 IPv6 Dirección: 2001:db8:acad:b: :1

Figura 11. Ping 2001:db8:acad:b: :1



Desde PC-A a R1, G0/0/1.4 Dirección: 10.19.8.97
Figura 12. Ping 10.19.8.97



IX. CONCLUSIÓN

Se debe ser muy profesional a la hora de realizar una configuración inicial de los dispositivos garantizando niveles de seguridad básicos, como lo es la asignación de contraseñas de manera cifrada que impida a cualquier persona que a través de un código pueda conocerla y acceder de manera no autorizada y vulnerar nuestra red.

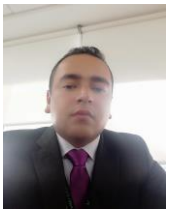
A través del presente trabajo se puso en práctica los conocimientos adquiridos en el desarrollo del curso, es importante resaltar que se debe conocer la estructura de los equipos para poder aplicar la configuración adecuada y lograr la conexión en red esperada.

Importante resaltar la experiencia con un programa de simulación como lo es packet tracer, el cual se acerca a la realidad frente a la configuración de los dispositivos y dándome una cercanía con los códigos de programación y familiarizándome con esta familia como lo es CISCO, para así tener las competencias para llevarlo a la práctica.

RECONOCIMIENTO

Agradecimiento al ingeniero DIEGO EDINSON RAMIREZ CLAROS que me guio durante el procedimiento de desarrollo del escenario propuesto en este escenario, el cual fue asignado como coordinador en el desarrollo del diplomado en profundización de redes CISCO. CCNA.

BIOGRAFIA



Albarracin Urrutia Jhon Jehider, nacido el 17 de febrero de 1989 en la ciudad de Villavicencio del Departamento del Meta, estudiante del pregrado de Ingeniera de Sistemas en la Universidad Nacional Abierta y a Distancia con sede en el municipio de Facatativá en el Departamento de Cundinamarca

REFERENCES

TANENBAUM, A. S. (2003). *REDES DE COMPUTADORAS*. PEARSON EDUCACIÓN.

BORONAT SEGUI, F. (2013). FUNCIONAMIENTO DEL PROTOCOLO DHCP.

CRISTÓBAL, Y. R., MARÍN, E. M., & SANTIESTEBAN, L. E. F. ANÁLISIS DE LA SEGURIDAD DEL PROTOCOLO IPV6 IPV6 PROTOCOL SECURITY ANALYSIS.

MEISEL, Y. D. (1998). COMPARACIÓN, VENTAJAS, PROBLEMAS Y UNA METODOLOGÍA PARA LA TRANSICIÓN DE IPV4 A IPV6 EN LAS REDES DE COMUNICACIONES. *INGENIERÍA Y DESARROLLO*, (3-4).

ARIGANELLO, E. (2008). *TÉCNICAS DE CONFIGURACIÓN DE ROUTERS CISCO*. GRUPO EDITORIAL RA-MA.

MATTURRO, G. (2007). INTRODUCCIÓN A LA CONFIGURACIÓN DE ROUTERS CISCO. *RECUPERADO DE: HTTPS://WWW. ORT. EDU. UY/FI/PDF/CONFIGURACIONROUTERSCISCOMATTURRO. PDF*.

ARIGANELLO, E. (2014). *REDES CISCO: GUÍA DE ESTUDIO PARA LA CERTIFICACIÓN CCNA ROUTING Y SWITCHING*. RA-MA.

CISCO. (2019). DIVISIÓN DE REDES IP EN SUBREDES. FUNDAMENTOS DE NETWORKING. RECUPERADO DE: HTTPS://STATIC-COURSE-ASSETS.S3.AMAZONAWS.COM/ITN6/ES/INDEX.HTML#8

CISCO. (2019). DHCP. PRINCIPIOS DE ENRUTAMIENTO Y CONMUTACIÓN. RECUPERADO DE: HTTPS://STATIC-COURSE-ASSETS.S3.AMAZONAWS.COM/RSE6/ES/INDEX.HTML#8

CISCO. (2019). ROUTING DINÁMICO. PRINCIPIOS DE ENRUTAMIENTO Y CONMUTACIÓN. RECUPERADO DE: HTTPS://STATIC-COURSE-ASSETS.S3.AMAZONAWS.COM/RSE6/ES/INDEX.HTML#3