DIPLOMADO DE PROFUNDIZACIÓN CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNA ll

ANDRES CAMILO CAMACHO RAMIREZ

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

DIPLOMADO DE PROFUNDIZACIÓN CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNA ll

ANDRES CAMILO CAMACHO RAMIREZ

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

DIRECTOR:

JOSE IGNACIO CARDONA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERIA -ECBTI
INGENIERIA DE SISTEMAS
BOGOTA
2020

NOTA DE ACEPTACIÓN

_____
_____

_____
_____
_____
_____
_____

_____
Firma del presidente del jurado

_____
Firma de jurado

_____
Firma de jurado

BOGOTA, 30 DE NOVIEMBRE DE 2020

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

TOPOLOGÍA DE RED: Es el mapa lógico de un diseño de una red con el fin de intercambio de información.

ETHERCHANNEL: Tecnología Que permite a dos o más puertos físicos convertirse en un puerto lógico para tener una mayor capacidad con lo es disponibilidad y ancho de banda.

DNS: Es la nomenclatura que comprende el sistema de nombre de dominios el cual también sirve para direccionar los dominios al servidor correspondiente.

VLAN: Tipo de red virtual vincula a una red física lo cual permite tener varias redes virtuales dentro de una red física.

GATEWAY: Permite la interconexión de redes con diferentes protocolos dando la traducción de información necesaria del protocolo de inicio al de destino.

TRUNK: Configuración para switch que se encuentren dentro de la misma red ethernet para manejar varias redes Vlan por solo un cable de conexión.

RESUMEN

El presente documento compila los resultados de solución para los 2 escenarios propuestos en el diplomado de profundización cisco el cual es opción de grado para el programa de ingeniería de sistemas.

El procedimiento a seguir es la aplicación de los conocimientos de las unidades de aprendizaje y de las evaluaciones de capítulos, se aplica el diseño de las topologías con el uso de la herramienta packet tracer en la cual se diseñan las interfaces y se generan el enrutamiento de las redes de los equipos entre redes VLAN, DHCP, Etherchannel por medio de los comandos de configuración aprendidos para dar solución de los ejercicios y luego finalizar la comprobación de su funcionamiento por medio de pruebas de comunicación entre equipos que componen la topología verificando que los paquetes de información viajen por la redes creadas y lleguen a los dispositivos de destino.

ABSTRACT

This document compiles the solution results for the 2 scenarios proposed in the Cisco in-depth diploma course, which is a degree option for the systems engineering program.

The procedure to follow is the application of the knowledge of the learning units and the chapter evaluations, the design of the topologies is applied with the use of the packet tracer tool in which the interfaces are designed and the routing of the networks of the equipment between VLANs, DHCP, Etherchannel through the configuration commands learned to solve the exercises and then finalize the verification of its operation by means of communication tests between equipment that make up the topology, verifying that the packets of information travel through the created networks and reach the destination devices.

INTRODUCCION

El objetivo de aprendizaje del diplomado CISCO es el uso fluido de las herramientas de redes LAN -WAN por medio de la aplicación de protocolos de enlace VLAN, DHCP, Etherchanel, port security, OSPF, direcciones de red dinámicas y estáticas (NAT), listas de control de acceso (ACL) para generar comunicación entre dispositivos de red como PC, Router, Swicth , servidores.

El desarrollo del primer escenario corresponde a la implementación de enrutamientos VLAN, DHCP, Etherchannel y port - security, este proceso se desarrolla en el direccionamiento para comunicaciones desde los PC al Router buscando un enlace a pesar de tener redes diferentes en el sistema de comunicaciones.

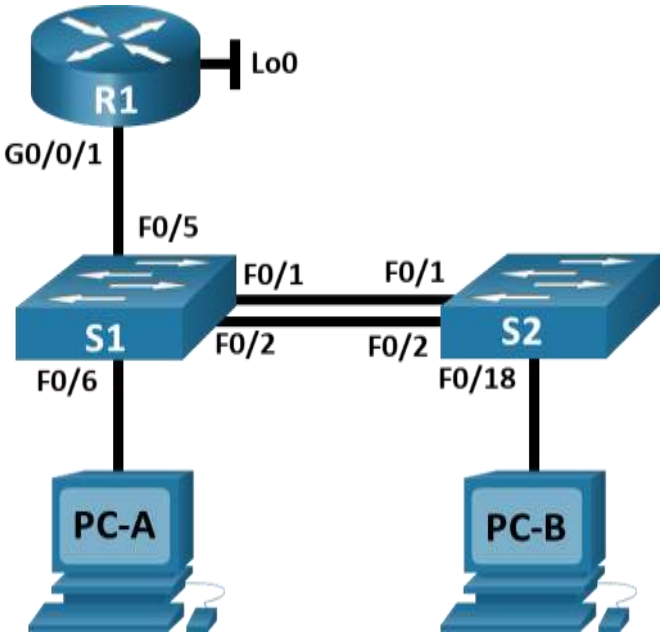
El segundo escenario corresponde al uso de conectividad IPV4, IPV6, protocolo OSPF, DHCP, NAT, ACL, NTP y comandos CLI, dentro del cual se ejecuta la conectividad de los protocolos mencionados entre los pc y el servidor del sistema, esta implementación es basada en protocolos de acceso con las respectivas seguridades.

Descripción de escenarios propuestos para la prueba de habilidades

Escenario 1

Topología

Figura 1. Topología Escenario 1



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

Tabla 1 VLAN

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

VLAN	Nombre de la VLAN
6	Native

Tabla de asignación de direcciones

Tabla 2. Asignación 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

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
PC-B NIC	2001:db8:acad:b: :50 /64	fe80::1

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

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.

Figura 2, Inicialización de Router

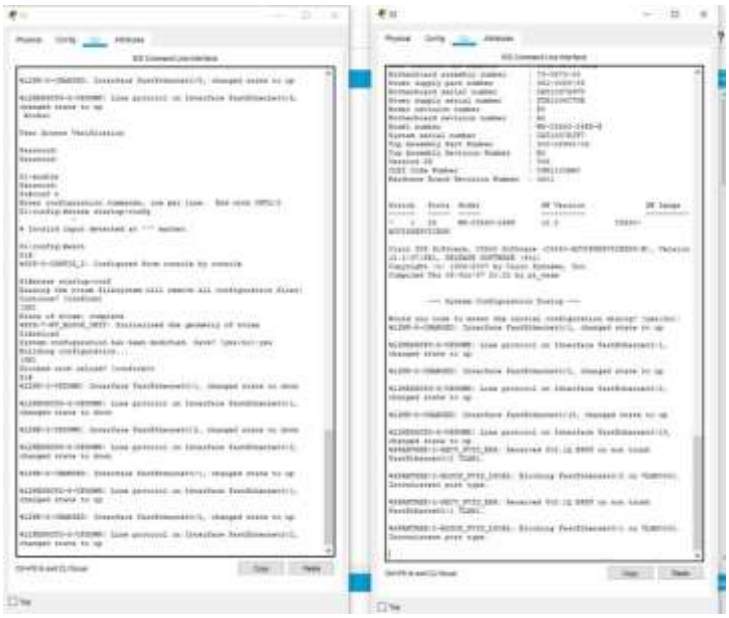
Se genero los comandos de borrar configuración inicial y racargar en los swicth y Router para no tener redes vlan o configuraciones previas.

Switch#erase startup-config

Switch#delete vlan.data

Switch# reload

Figura 3. Inicialización de Switch 1-2



Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 3. Configurar R1

Tarea	Especificación
Desactivar la búsqueda DNS	R1(config)#no ip domain-loockup
Nombre del router	Router(config)#hostname R1
Nombre de dominio	ccna-lab.com R1(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	Router(config)#hostname R1

Tarea	Especificación
Contraseña de acceso a la consola	R1(config)#line console 0 R1(config-line)#password ciscoconpass R1(config-line)#login
Establecer la longitud mínima para las contraseñas	R1(config-line)#security passwords min-length 10
Crear un usuario administrativo en la base de datos local	Nombre de usuario: **admin** Password: **admin1pass** R1(config)#username admin privilege 15 secret admin1pass R1(config)#line vty 0 4 R1(config-line)#login local R1(config-line)#transport input ssh R1(config-line)#service password-encrytion
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	R1(config)#line vty 0 15 R1(config-line)#transport input ssh R1(config-line)#login local R1(config-line)#exit
Configurar VTY solo aceptando SSH	R1(config)#line vty 0 4 R1(config-line)#login local
Cifrar las contraseñas de texto no cifrado	R1(config-line)#service password- encrytion
Configure un MOTD Banner	R1(config)#banner motd $ ACCESO NO AUTORIZADO $
Habilitar el routing IPv6	R1(config)#ipv6 unicast-routing

Configurar interfaz G0/0/1 y subinterfaces	Establezca la descripción Establece la dirección IPv4. Establezca la dirección local de enlace IPv6 como **fe80: :1** Establece la dirección IPv6. Activar la interfaz. R1(config)#int g0/1 R1(config-if)#description red a S1 R1(config-if)#ipv6 add fe80::1 ink-local ^ % Invalid input detected at '^' marker. R1(config-if)#ipv6 add fe80::1 link-local R1(config-if)#no shutdown R1(config-if)# %LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up R1(config-if)#exit R1(config)#int g0/1.2 R1(config-subif)# %LINK-5-CHANGED: Interface GigabitEthernet0/1.2, changed state to up R1(config-subif)#encapsulation dot1q 2 R1(config-subif)#ip add 10.19.8.1 % Incomplete command. R1(config-subif)#ip add 10.19.8.1 255.255.255.192 R1(config-subif)#ipv6 add 2001:db8:acad::1/64 R1(config-subif)#ipv6 add 2001:db8:acad:a::1/64 R1(config-subif)#no ipv6 add 2001:db8:acad::1/64 R1(config-subif)#ipv6 add 2001:db8:acad:a::1/64 R1(config-subif)#ipv6 add fe80::1 link-local R1(config-subif)#exit R1(config)#int g0/1.3

	R1(config-subif)# %LINK-5-CHANGED: Interface GigabitEthernet0/1.3, changed state to up R1(config-subif)#encapsultaion dot1q 3 ^ % Invalid input detected at '^' marker. R1(config-subif)#encapsulation dot1q 3 R1(config-subif)#ip add 10.19.8.65 255.255.255.224 R1(config-subif)#ipv6 add 2001:db8:acad:b::1/64 R1(config-subif)#ipv6 add fe80::1 link-local R1(config-subif)#exit R1(config)#int g0/1.4 R1(config-subif)# %LINK-5-CHANGED: Interface GigabitEthernet0/1.4, changed state to up R1(config-subif)#encapsulation dot1q 4 R1(config-subif)#ip add 10.19.8.97 255.255.255.248 R1(config-subif)#ipv6 2001:db8:acad:c::1/64 ^ % Invalid input detected at '^' marker. R1(config-subif)#ipv6 add 2001:db8:acad:c::1/64 R1(config-subif)#ipv6 add fe80::1 link-local R1(config-subif)#exit R1(config)#int g0/1.6 R1(config-subif)# %LINK-5-CHANGED: Interface GigabitEthernet0/1.6, changed state to up R1(config-subif)#encapsulation dot1q 6 R1(config-subif)#exit

Tarea	Especificación
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-if)#description int loopback 0 R1(config-if)#ip address 209.165.201.1 255.255.255.224 R1(config-if)#ipv6 add 2001:db8:acad:209::1/64 R1(config-if)#ipv6 add fe80::1 link-local R1(config-if)#no shutdown R1(config-if)#exit R1(config)#ipv6 unicast-routing
Generar una clave de cifrado RSA	How many bits in the modulus [512]: 1024 % Generating 1024 bit RSA keys, keys will be non-exportable...[OK] R1(config)#crypto key generate rsa general-key modulus 1024

Tarea	Especificación
Interpretación de comandos realizados	Generamos el código correspondiente a las instrucciones de usuario administrativo, inicio de sesión en las líneas VTY, cifrar las contraseñas, configurar VTY solo aceptando SSH, configure un MOTD Banner, habilitar el routing IPv6, configurar interfaz G0/0/1 y subinterfaces, configure el Loopback0 interface, generar una clave de cifrado RSA , con estas instrucciones logramos generar un usuario administrador con seguridades y cifrar las contraseñas usadas, general un mensaje en caso de error en el ingreso, también habilitamos que el Router funcione con direccionamiento IPV6 ya que inicialmente solo funciona con IPV4, se generó la configuración de la interface de entrada que va al Switch 1 y las subinterfaces que van derivadas de este puerto.

Paso 3 : Configure S1 y S2.

Las tareas de configuración incluyen lo siguiente:

Tabla 4. Configure S1 y S2

Tarea	Especificación
Desactivar la búsqueda DNS.	S1>enable S1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. S1(config)#no ip domain-lookup S2(config)#no ip domain-lookup
Nombre del switch	S1(config)#hostname R1
Nombre de dominio	ccna-lab.com S1(config)#ip domain-name ccna-lab.com S2(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	Ciscoenpass S1>en S1#confi Configuring from terminal, memory, or network [terminal]? Enter configuration commands, one per line. End with CNTL/Z. S1(config)#enable secret ciscoenpass

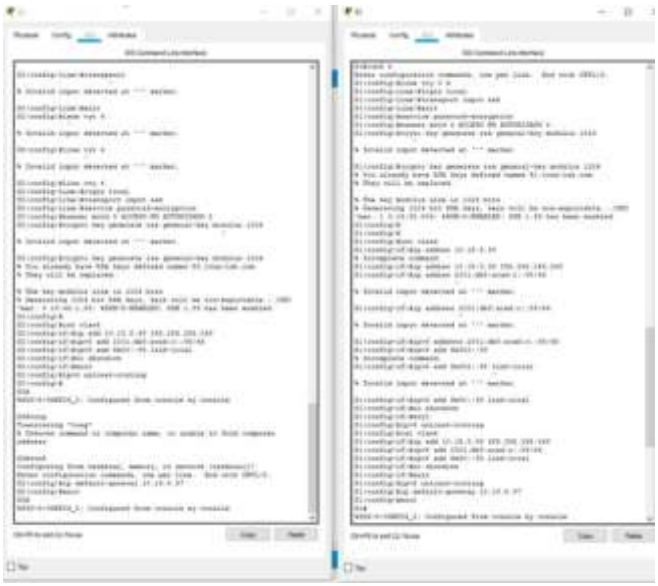
Tarea	Especificación
Contraseña de acceso a la consola	Ciscoconpass S1(config)#line console 0 S1(config-line)#password ciscoconpass S1(config-line)#login S1(config-line)#line vty 0 15 S1(config-line)#service pass S1(config)#exit S2(config)#line console 0 S2(config-line)#password ciscoconpass S2(config-line)#login S2(config-line)#line vty 0 15 S2(config-line)#service pass S2(config)#exit
Crear un usuario administrativo en la base de datos local	Nombre de usuario: **admin** Password: **admin1pass** S1(config)#username admin privilege 15 secret admin1pass S2(config)#username admin privilege 15 secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	S1(config)#line vty 0 4 S1(config-line)#login local S2(config)#line vty 0 4 S2(config-line)#login local
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S1(config-line)#transport input ssh S2(config-line)#transport input ssh

Tarea	Especificación
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption S2(config)#service password-encryption
Configurar un MOTD Banner	S1(config)#banner motd $ ACCESO NO AUTORIZADO $ S2(config)#banner motd $ ACCESO NO AUTORIZADO $
Generar una clave de cifrado RSA	**Módulo de 1024 bits** S1(config)#crypto key generate rsa general-key modulus 1024 S2(config)#crypto key generate rsa general-key modulus 1024

	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)#int vlan4 S1(config-if)#ip addres 10.19.8.98 % Incomplete command. S1(config-if)#ip addres 10.19.8.98 255.255.255.248 S1(config-if)#ip addres 2001:db8:acad:c::98/64 ^ % Invalid input detected at '^' marker. S1(config-if)#ip address 2001:db8:acad:c::98/64 ^ % Invalid input detected at '^' marker. S1(config-if)#ipv6 address 2001:db8:acad:c::98/64 S1(config-if)#ipv6 add fe802::98 % Incomplete command. S1(config-if)#ipv6 add fe802::98 link-local ^ % Invalid input detected at '^' marker. S1(config-if)#ipv6 add fe80::98 link-local S1(config-if)#no shutdown S1(config-if)#exit S1(config)#ipv6 unicast-routing S1(config)#
Configurar la interfaz de administración (SVI)	S2(config)#int vlan4

Tarea	Especificación
	S2(config-if)#ip addres 10.19.8.98 255.255.255.248 S2(config-if)#ip address 2001:db8:acad:c::98/64 S2(config-if)#ipv6 address 2001:db8:acad:c::98/64 S2(config-if)#ipv6 add fe802::99 % Incomplete command. S2(config-if)#ipv6 add fe80::99 link-local S2(config-if)#no shutdown S2(config-if)#exit S2(config)#ipv6 unicast-routing
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 S2(config)#ip default-gateway 10.19.8.97

Figura 4. Configuración DNS, VTY,MOTD , RSA, SVI para Switch 1-2



En este punto se realizo cambiar el nombre del Switch a R1, se elimino el sistema de búsqueda DNS, generamos un nombre de dominio en el R1, generamos un sistema de seguridad con claves para proteger el acceso a la consola, y se genero un usuario de administrador de base de datos , configuramos el VTY para que solo reciba conexiones SSH, ciframos las claves de acceso en general, damos un mensaje den caso de error de ingreso, se creo el modulo RSA de 1024 bits y se configuro el Svi capa 3 con las direcciones IPV4-IPV6 para los dos equipos Switch.

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

Paso 3: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 5. Configuración de la infraestructura de red

Tarea	Especificación
Crear VLAN	VLAN 2, nombre Bikes VLAN 3, nombre Trikes VLAN 4, name Management VLAN 5, nombre Parking VLAN 6, nombre Native Figura # 5 Configuración Vlan Switch 1 

Tarea	Especificación
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	Interfaces F0/1, F0/2 y F0/5 S1(config)#interfa f0/1 S1(config-if)#switchport mode trunk S1(config-if)# %EC-5-CANNOT_BUNDLE2: Fa0/1 is not compatible with Po1 and will be suspended (vlan mask is different) S1(config)#interfa f0/2 S1(config-if)#switchport mode trunk S1(config-if)# %EC-5-CANNOT_BUNDLE2: Fa0/2 is not compatible with Po1 and will be suspended (native vlan of Fa0/2 is 6, Po1 id 1) S1(config)#interface f0/5 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 6 S1(config-if)#switchport trunk allowed vlan 2,3,4,5,6 S1(config-if)#exit S1(config)#

Tarea	Especificación
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	S1(config-if)#interface range f0/1-2 S1(config-if-range)#channel-group 1 mode active S1(config-if-range)# %EC-5-CANNOT_BUNDLE2: Fa0/1 is not compatible with Po1 and will be suspended (vlan mask is different)
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

Tarea	Especificación
Configurar la seguridad del puerto en los puertos de acceso	Permitir 3 direcciones MAC S1#conf t Enter configuration commands, one per line. End with CNTL/Z. S1(config)#interface gigabitethernet 0/1 S1(config-if)#switchport mode access S1(config-if)#switchport port-security S1(config-if)#switchport port-security maximum 3 S1(config-if)#switchport port-security violation shutdown S1(config-if)#switchport port-security mac-address sticky S1(config-if)#end
Proteja todas las interfaces no utilizadas	S1(config)#interface range f0/3-4, f0/7-24 S1(config-if-range)#switchport mode access S1(config-if-range)#switchport acces vlan 5 S1(config-if-range)#description protejer interfaces no utilizadas S1(config-if-range)#shotdown S1(config-if-range)#switchport port-security S1(config-if-range)#switchport port-security maximum 1 S1(config-if-range)#switchport port-security violation shutdown

Tarea	Especificación
Interpretación de comandos realizados	Dentro de este punto se crearon las redes Vlan 2,3,4,5,6 para el direccionamiento siguiente de las subredes, se generaron las conexión de troncos en la interface f0/5 con el fin de dirigir las subredes y se aplicaron los comandos correspondientes al crear una grupos de puertos etherchannel de capa 2 para las interfaces 1-2, se genero el permiso para que la Vlan 2 ingrese por host en el puerto F0/6, se dio protección en los puertos de acceso para solo tener 3 direcciones MAC y por último se realizó la protección de todos los puertos que no se usan en la configuración.

Paso4 : Configure el S2.

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

Tabla 6. Configurar 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 Figura 6 # Vlan Switch 2 

Tarea	Especificación
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	Interfaces F0/1 y F0/2 S2(config)#interface f0/2 S2(config-if)#switchport mode trunk S2(config-if)# %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan4, changed state to down
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
Configurar el puerto de acceso del host para la VLAN 3	S2(config)#interface f0/18 S2(config-if)#switchport mode access S2(config-if)#switchport access vlan 3

Tarea	Especificación
Configure port-security en los access ports	permite 3 MAC addresses S2#conf t Enter configuration commands, one per line. End with CNTL/Z. S2(config)#interface gigabitethernet 0/1 S2(config-if)#switchport mode access S2(config-if)#switchport port-security S2(config-if)#switchport port-security maximum 3 S2(config-if)#switchport port-security violation shutdown S2(config-if)#switchport port-security mac-address sticky S2(config-if)#end
Asegure todas las interfaces no utilizadas.	S2(config)#interface range f0/3-4, f0/7-24 S2(config-if-range)#switchport mode access S2(config-if-range)#switchport acces vlan 5 S2(config-if-range)#description protejer interfaces no utilizadas S2(config-if-range)#shutdown S2(config-if-range)#switchport port-security S2(config-if-range)#switchport port-security maximum 1 S2(config-if-range)#switchport port-security violation shutdown

Tarea	Especificación
Interpretación de comandos realizados	Dentro de este punto se crearon las redes Vlan 2,3,4,5,6 para el direccionamiento siguiente de las subredes, se generaron las conexión de troncos en la interface f0/5 con el fin de dirigir las subredes y se aplicaron los comandos correspondientes al crear una grupos de puertos etherchannel de capa 2 para las interfaces 1-2, se generó el permiso para que la Vlan 3 ingrese por host en el puerto F0/18, se dio protección en los puertos de acceso para solo tener 3 direcciones MAC y por último se realizó la protección de todos los puertos que no se usan en la configuración.

Tabla 7. Configurar R1

Parte 2. Configurar soporte de host

Paso 4: Configure R1

Las tareas de configuración para R1 incluyen las siguientes:

Tarea	Especificación
Configure Default Routing	Crear rutas predeterminadas para IPv4 e IPv6 que dirijan el tráfico a la interfaz Loopback 0

Configurar IPv4 DHCP para VLAN 2	Cree un grupo DHCP para VLAN 2, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio ccna-a.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada R1(config)#ip dhcp excluded-address 10.19.8.245 10.19.8.255 R1(config)#ip dhcp pool % Incomplete command. R1(config)#ip dhcp % Incomplete command. R1(config)#ip dhcp pool VLAN2 R1(dhcp-config)#DNS-SERVER 209.165.201.1 R1(dhcp-config)#domain-name ccna-a.net R1(dhcp-config)#default-router 10.19.8.1 255.255.225.192 ^ % Invalid input detected at '^' marker. R1(dhcp-config)#default-router 10.19.8.1 R1(dhcp-config)#default-router 10.19.8.2 R1(dhcp-config)#default-router 10.19.8.1 255.255.255.192 ^ % Invalid input detected at '^' marker. R1(dhcp-config)#default-router 10.19.8.1 R1(dhcp-config)#default-router 10.19.8.2 R1(dhcp-config)#network 10.19.8.1 255.255.255.192 R1(dhcp-config)#exit R1(config)#ip dhcp excluded-address 10.19.8.1 10.19.8.52 R1(config)#ip dhcp pool vlan 2 ^ % Invalid input detected at '^' marker. R1(config)#ip dhcp pool vlan2 R1(dhcp-config)#network 10.19.8.0

Tarea	Especificación
	% Incomplete command. 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)#dns-server 209.165.200.225 R1(dhcp-config)#exit
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 dhcp excluded-address 10.19.8.234 10.19.8.244 R1(config)#ip dhcp pool vlan3 R1(dhcp-config)#dns-server 209.165.201.1 R1(dhcp-config)#domain-name ccna-a.net R1(dhcp-config)#default-router 10.19.8.66 R1(dhcp-config)#network 10.19.8.65 % Incomplete command. R1(dhcp-config)#network 10.19.8.65 255.255.255.224 R1(dhcp-config)#exit R1(config)#ip dhcp excluded-address 10.19.8.65 10.19.8.84 R1(config)#ip dhcp pool vlan2 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-a.net R1(dhcp-config)#dns-server 209.165.200.225 R1(dhcp-config)#exit

Tarea	Especificación
Interpretación de comandos realizados	En este paso generamos la configuración de DHCP con un grupo de las 10 últimas direcciones para la red Vlan 2 y 3 en IPV4, se les asigno el correspondiente dominio ccna-b.net y se dejo la puerta de enlace configurada para el acceso.

Paso 5: 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. Configurar servidores

PC-A Network Configuration	
Descripción	*en* Ajustes PC-A
Dirección física	00D0.FF32.C9E3
Dirección IP	*en* 10.19.8.53
Máscara de subred	*en* 255.255.255.192
Gateway predeterminado	*en* 10.19.8.1
Gateway predeterminado IPv6	*en* FE80::1

Figura # 7 configuración PC-A

Se genero la configuración del PC-A para que tenga los valores de red ajustados para conexión con los Switch correspondientes en nivel IPV4 e IPV6.

Tabla 9. Configurar red PC-A

Configuración de red de PC-A	
Descripción	Ajuste PC-B
Dirección física	0030.A338.20B8
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. Configuración PC-B

Se genero la configuración del PC-A para que tenga los valores de red ajustados para conexión con los Switch correspondientes en nivel IPV4 e IPV6.

Parte 2: 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. Prueba de conectividad

Desde	A	de Internet	Dirección IP	Resultados de ping
PC-A	R1, G0/0/1.2	Dirección	10.19.8.1	CORRECTO
PC-A	*R1, G0/0/1.2*	IPv6	2001:db8:acad:a: :1	CORRECTO
PC-A	R1, G0/0/1.3	Dirección	10.19.8.65	CORRECTO
PC-A	*R1, G0/0/1.3*	IPv6	2001:db8:acad:b: :1	NO CORRECTO
PC-A	R1, G0/0/1.4	Dirección	10.19.8.97	CORRECTO
PC-A	*R1, G0/0/1.4*	IPv6	2001:db8:acad:c: :1	NO CORRECTO
PC-A	S1, VLAN 4	Dirección	10.19.8.98	NO CORRECTO
PC-A	*S1, VLAN 4*	IPv6	2001:db8:acad:c: :98	NO CORRECTO
PC-A	S2, VLAN 4	Dirección	10.19.8.99.	NO CORRECTO
PC-A	*S2, VLAN 4*	IPv6	2001:db8:acad:c: :99	NO CORRECTO
PC-A	PC-B	Dirección	IP address will vary.	NO CORRECTO
PC-A	*PC-B*	IPv6	2001:db8:acad:b: :50	NO CORRECTO
PC-A	R1 Bucle 0	Dirección	209.165.201.1	NO CORRECTO
PC-A	*R1 Bucle 0*	IPv6	2001:db8:acad:209: :1	NO CORRECTO
PC-B	R1 Bucle 0	Dirección	209.165.201.1	NO CORRECTO
PC-B	*R1 Bucle 0*	IPv6	2001:db8:acad:209: :1	NO CORRECTO

Desde	A	de Internet	Dirección IP	Resultados de ping
PC-B	R1, G0/0/1.2	Dirección	10.19.8.1	CORRECTO *bl*
PC-B	*R1, G0/0/1.2*	IPv6	2001:db8:acad:a: :1	NO CORRECTO
PC-B	R1, G0/0/1.3	Dirección	10.19.8.65	CORRECTO
PC-B	*R1, G0/0/1.3*	IPv6	2001:db8:acad:b: :1	CORRECTO
PC-B	R1, G0/0/1.4	Dirección	10.19.8.97	CORRECTO
PC-B	*R1, G0/0/1.4*	IPv6	2001:db8:acad:c: :1	NO CORRECTO
PC-B	S1, VLAN 4	Dirección	10.19.8.98	NO CORRECTO
PC-B	*S1, VLAN 4*	IPv6	2001:db8:acad:c: :98	NO CORRECTO
PC-B	S2, VLAN 4	Dirección	10.19.8.99.	NO CORRECTO
PC-B	*S2, VLAN 4*	IPv6	2001:db8:acad:c: :99	NO CORRECTO

Figura 9.

Ping PC-A a R1,G0/0/1.2 IPV4

Figura 10.

Ping PC_A a R1, G0/0/1.3

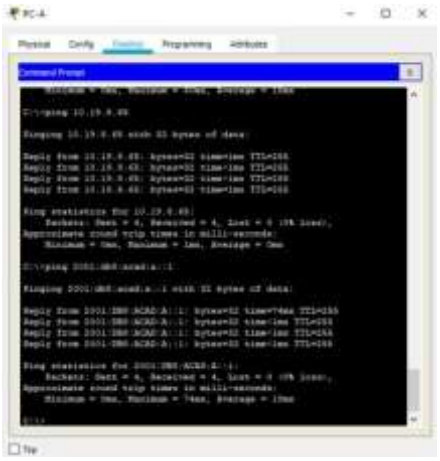


Figura 11.

Ping PC-A a R1, G0/0/1.2 IPV6

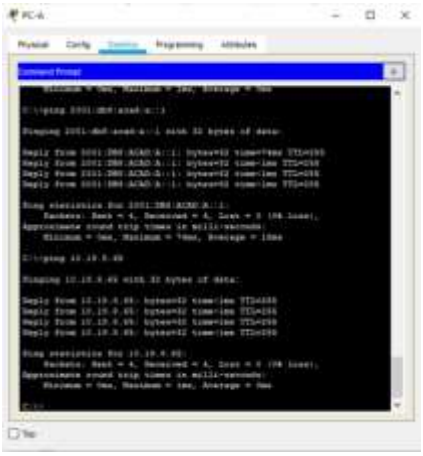


Figura 12.

Ping PC_A a R1, G0/0/1.4

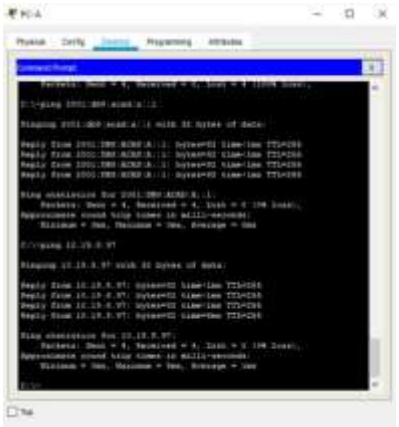


Figura 13.

PC-B a R1, G0/0/1.2 IPV4

Figura 14.

PC-B a R1, G0/0/1.3 IPV6

Figura 15.

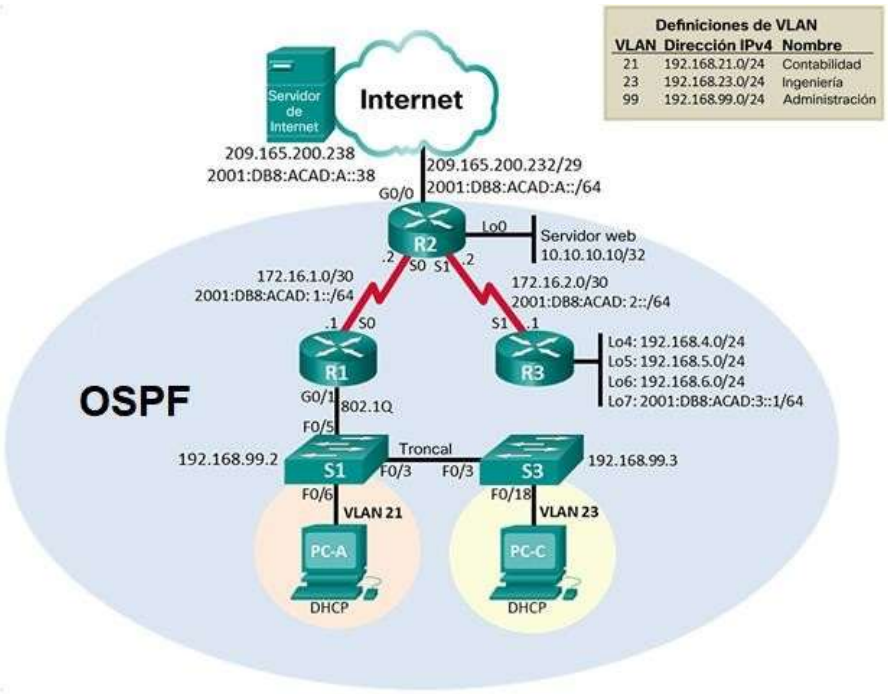
Ping PC-B a R1, G0/0/1.4

Escenario 2

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.

Topología

Figura 16. Escenario 2



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.

Tabla 11. Iniciar y volver a cargar Router y Switches

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	R1#enable R1#erase startup-config R2#enable R2#erase startup-config R3#enable R3#erase startup-config
Volver a cargar todos los routers	R1#reload R2#reload R3#reload
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	S1>enable S1#erase startup-config Switch#conf t Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#no vlan 1 Default VLAN 1 may not be deleted S1#delete vlan.dat Delete filename [vlan.dat]? Delete flash:/vlan.dat? [confirm] S2>enable S2#erase startup-config Switch#conf t Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#no vlan 1 Default VLAN 1 may not be deleted S2#delete vlan.dat Delete filename [vlan.dat]? Delete flash:/vlan.dat? [confirm] S3>enable S3#erase startup-config Switch#conf t

	Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#no vlan 1 Default VLAN 1 may not be deleted S3#delete vlan.dat Delete filename [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	S1#show vlan brief
Interpretación de comandos realizados	Se realizaron los comandos necesarios para la configuración de los router eliminando los archivos de inicio y nuevamente cargando slos dispositivos. También se verifica que la VLAN no este en 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):

Tabla 12. Configuración de 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::38
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:

Tabla 13. Configurar R1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router>enable Router#conf t Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R1
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	R1(config-line)#service pass R1(config)#enable secret cisco R1(config)#enable secret class R1(config)#username Telnet privilege 15 secret cisco R1(config)#line vty 0 15 R1(config-line)#transport input ssh R1(config-line)#login local R1(config-line)#exit R1(config)#crypto key generate rsa % Please define a domain-name first. R1(config)#ip domain-name ccna-mlab.com R1(config)#crypto key generate rsa
Mensaje MOTD	Se prohíbe el acceso no autorizado. R1(config)#service pass R1(config)#banner motd $ Se prohibe el acceso no autorizado $ R1(config)#end

Interfaz S0/0/0	Establezca la descripción Establecer la dirección IPv4 Consultar el diagrama de topología para conocer la información de direcciones Establecer la dirección IPv6 Consultar el diagrama de topología para conocer la información de direcciones Establecer la frecuencia de reloj en 128000 Activar la interfaz R1(config)# R1(config)#interface Serial0/0/0 R1(config-if)#interface Serial0/0/0 R1(config-if)#ip add % Incomplete command. R1(config-if)#ip add 172.16.1.1 % Incomplete command. R1(config-if)#ip add 172.16.1.1 255.255.255.252 R1(config-if)#ipv6 address 2001:DB8:ACAD:1::/64 R1(config-if)#clock rate 128000 R1(config-if)#no shutdown R1(config-if)#exit
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 R1(config)#ipv6 route ::/0 s0/0/0

Interpretación de comandos realizados	En este paso realizamos la configuración del R1 en al cual asignamos el nombre dimos la contraseña cifrada y contraseña de consola luego se cifro todas la contraseñas y se genera el mensaje MOTD en caso de acceso prohibido, se asignó la dirección IPV4 e IPV6 y luego se asigna rutas predeterminadas a IPV4 e IPV6

Nota: Todavía no configure G0/1.

Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Tabla 14. Configurar R2

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	R2>enable R2#conf t R2(config)#no ip domain-lookup
Nombre del router	R2
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco

Cifrar las contraseñas de texto no cifrado	R2(config-line)#service pass R2(config)#enable secret cisco R2(config)#enable secret class R2(config)#username Telnet privilege 15 secret cisco R2(config)#line vty 0 15 R2(config-line)#transport input ssh R2(config-line)#login local R2(config-line)#exit R2(config)#crypto key generate rsa % Please define a domain-name first. R2(config)#ip domain-name ccna-mlab.com R2(config)#crypto key generate rsa
Habilitar el servidor HTTP	R2(config)#ip http server
Mensaje MOTD	Se prohíbe el acceso no autorizado. R2(config)#service pass R2(config)#banner motd $ Se prohibe el accesp no autorizado $ R2(config)#end

Interfaz S0/0/0	Establezca 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 R2(config)#int s0/0/0 *mar. 1 0:24:22.524: RSA key size needs to be at least 768 bits for ssh version 2 *mar. 1 0:24:22.524: %SSH-5-ENABLED: SSH 1.5 has been enabled R2(config-if)#description r2-r1 R2(config-if)#ip add 172.16.1.2 255.255.255.252 R2(config-if)#clok rate 128000 R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64 R2(config-if)#no shutdown R2(config-if)#

Interfaz S0/0/1	Establecer la descripción Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Establecer la frecuencia de reloj en 128000. Activar la interfaz R2(config)#int s0/0/1 R2(config-if)#description r2-r3 R2(config-if)#ip add 172.16.2.1 255.255.255.252 R2(config-if)#clock rate 128000 R2(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64 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)#int g0/0 R2(config-if)#description r2-internet R2(config-if)#ip address 209.165.200.233 25..255.255.248 ^ % Invalid input detected at '^' marker. R2(config-if)#ip address 209.165.200.233 255.255.255.248 R2(config-if)#no shuitdown ^ % Invalid input detected at '^' marker. R2(config-if)#no shutdown R2(config-if)# %LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up R2(config-if)#exit R2(config)#int g0/0 R2(config-if)#description r2-internet R2(config-if)#ipv6 address 2001:DB8:ACAD:A::2/64 R2(config-if)#no shutdown

Interfaz loopback 0 (servidor web simulado)	Establecer la descripción. Establezca la dirección IPv4. R2(config)#inte loopback 0 R2(config-if)# %LINK-5-CHANGED: Interface Loopback0, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up R2(config-if)#ip address 10.10.10.10 255.255.255.0 R2(config-if)#no shutdown
Ruta predeterminada	Configure una ruta IPv4 predeterminada de G0/0. Configure una ruta IPv6 predeterminada de G0/0. R2(config-if)#ip address 10.10.10.10 255.255.255.0 R2(config-if)#no shutdown R2(config-if)#ip route 0.0.0.0 0.0.0.0 g0/0 R2(config)#ipv6 route ::/0 g0/0 R2(config)#
Interpretación de comandos realizados	Se genero la configuración del router 2 asignado el nombre S2, desactivando la búsqueda DNS, se genera clave cifrada de consola y de exce privilegiado, habilitamos el servidor HTTP, se genero el mensaje en caso de ingreso erróneo, luego configuramos la interface G0/0 asignado su respectiva dirección Ipv4 e IPV6, al igual se configuran las interfaces S0/0/0 e S0/0/1 con sus respectivas direcciones IPV4 e IPV6 y la frecuencia del reloj en 128000

Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Tabla 15. Configurar R3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	R3>enable R3#conf t R3(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R3
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	router>enable router#conf t Enter configuration commands, one per line. End with CNTL/Z. r3(config)#no ip domain-lookup r3(config)#hostname r3 r3(config)#enable secret class r3(config)#line console 0 r3(config-line)#password cisco r3(config-line)#login r3(config-line)#exit r3(config)#line vty 04 r3(config-line)#password cisco r3(config-line)#login r3(config-line)#exit

	r3(config)#service password-encryption r3(config)#banner motd $ se prohibe el accesso no autorizado $ r3(config)#username Telnet privilege 15 secret cisco r3(config)#line vty 0 15 r3(config-line)#transport input ssh r3(config-line)#login local r3(config-line)#exit r3(config)#cryto generate rsa ^ % Invalid input detected at '^' marker. r3(config)#ip domain-name ccna-mlab.com r3(config)#crypto keygenerate rsa ^
Mensaje MOTD	Se prohíbe el acceso no autorizado. r3(config)#banner motd $ se prohibe el accesso 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)#interfac s0/0/1 r3(config-if)#description r3-r2

	r3(config-if)#ip address 172.16.2.1 255.255.255.252 r3(config-if)#no shutdown r3(config-if)#
Interfaz loopback 4	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. r3(config)#interface loopback 4 r3(config-if)# %LINK-5-CHANGED: Interface Loopback4, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback4, changed state to up r3(config-if)#ip add 192.165.4.1 255.255.255.0 r3(config-if)#exit
Interfaz loopback 5	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. r3(config)#int loopback 5 r3(config-if)# %LINK-5-CHANGED: Interface Loopback5, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback5, changed state to up r3(config-if)#ip add 192.168.5.1 255.255.255.0 r3(config-if)#exit

Interfaz loopback 6	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. r3(config)#int loopback 6 r3(config-if)# %LINK-5-CHANGED: Interface Loopback6, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback6, changed state to up r3(config-if)#ip add 192.168.6.1 255.255.255.0 r3(config-if)#exit
Interfaz loopback 7	Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. s
Rutas predeterminadas	r3(config)#int s0/0/1 r3(config-if)#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 ::/. S0/0/1 ^ % Invalid input detected at '^' marker. r3(config)#ipv6 route ::/0 S0/0/1
Interpretación de comandos realizados	Generamos la configuración del router 3 asignando el nombre r3, general claves a consola a exce privilegiado y Telnet todas ellas cifradas, así como l mensaje MOTD de acceso no autorizado, luego se agregaron las direcciones IPV4 e IPV6 a las interfaces s0/0/1 así como las loopback de 4 a 7 ,y culminamos asignando rutas predeterminadas. .

Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 16. Configurar S1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch>enable Switch#conf t Switch(config)#no ip domain
Nombre del switch	Swicth(config)#hostname S1
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	S1(config)#enable secret cisco S1(config)#line console 0 S1(config-line)#password cisco S1(config-line)#login S1(config-line)#line vty 0 15 S1(config-line)#service pass S1(config)#enable secret class S1(config)#username cisco privilege 15 secret cisco S1(config)#line vty 0 15 S1(config-line)#transport input ssh S1(config-line)#login local S1(config-line)#exit S1(config)#crypto key generate rsa % Please define a domain-name first. S1(config)#ip domain-name first S1(config)#cryto key generate rsa

Mensaje MOTD	Se prohíbe el acceso no autorizado. S1(config)#service pass S1(config)#banner motd $ Se prohibe el acceso no autorizado $ S1(config)#end
Interpretación de comandos realizados	En el configuración del Swicth 1 se desactivo la búsqueda DNS y se nombro como S1, generamos claves de consola, exce y Telnet, luego ciframos las contraseñas y generamos mensaje MOTD de acceso prohibido.

Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 17. Configurar S3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch>enable Switch#conf t Switch(config)#no ip domain
Nombre del switch	S3
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco

Cifrar las contraseñas de texto no cifrado	S3(config)#enable secret cisco S3(config)#line console 0 S3(config-line)#password cisco S3(config-line)#login S3(config-line)#line vty 0 15 S3(config-line)#service pass S3(config)#enable secret pass S3(config)#username cisco privilege 15 secret cisco S3(config)#line vty 0 15 S3(config-line)#trasnport input ssh ^ % Invalid input detected at '^' marker. S3(config-line)#transport input ssh S3(config-line)#login local S3(config-line)#exit S3(config)#crypto key generate rsa % Please define a domain-name first. S3(config)#ip domain-name firts S3(config)#crypto key generate rsa
Mensaje MOTD	Se prohíbe el acceso no autorizado. S3(config)#service pass S3(config)#banner motd $ Se prohibe el acceso no autorizado $ S3(config)#end
Interpretación de comandos realizados	Se genero la configuración de desactivar servicio DNS , se asignó el nombre S3 y dimos contraseñas a consola , exce, Telnet , luego ciframos todas las contraseñas y generamos el mensaje MOTD de acceso prohibido

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:

Tabla 18. Verificar la conectividad de red

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	R1#ping 172.16.1.2 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/12 ms R1#
R2	R3, S0/0/1	172.16.1.2	R2#ping 172.16.1.2 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 2/4/13 ms R2# Type escape sequence to abort.

			Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 8/14/26 ms
PC de Internet	Gateway predeterminado	209.165.200.225	Packet Tracer PC Command Line 1.0 C:\>ping 209.165.200.225 Pinging 209.165.200.225 with 32 bytes of data: Reply from 209.165.200.225: bytes=32 time=31ms TTL=255 Reply from 209.165.200.225: bytes=32 time<1ms TTL=255 Reply from 209.165.200.225: bytes=32 time<1ms TTL=255 Reply from 209.165.200.225: bytes=32 time<1ms TTL=255

			Ping statistics for 209.165.200.225: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 31ms, Average = 7ms C:\>
Interpretación de comandos realizados		En este paso realizamos pruebas de comunicaciones entre dispositivos por medio de la instrucción ping	

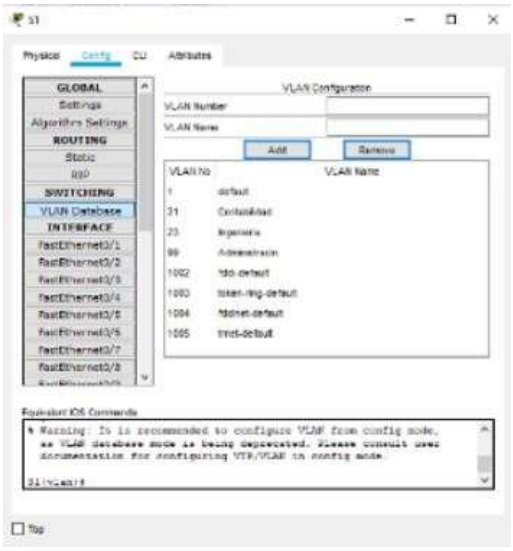
Nota: Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

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:

Tabla 19. Configurar la seguridad de Switch las Vlan

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 Figura 17. Vlan base de datos 
Asignar la dirección IP de administración.	Asigne la dirección IPv4 a la VLAN de administración. 192.168.99.2 255.255.255.0 Utilizar la dirección IP asignada al S1 en el diagrama de topología
Asignar el gateway predeterminado	Asigne la primera dirección IPv4 de la subred como el gateway predeterminado.

Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan % Incomplete command. S1(config-if)#switchport trunk native vlan 1 S1(config-if)#exit S1(config)#
Forzar el enlace troncal en la interfaz F0/5	Utilizar la red VLAN 1 como VLAN nativa S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan1 ^ % Invalid input detected at '^' marker. S1(config-if)#switchport trunk native vlan 1 S1(config-if)#end
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range S1(config)#int range f0/1-2,f0/4,f0/7-24 S1(config-if-range)#shutdown
Asignar F0/6 a la VLAN 21	S1(config-if)#exit S1(config)#int f0/6 S1(config-if)#switport mode acces ^ % Invalid input detected at '^' marker. S1(config-if)#switcport mode access ^ % Invalid input detected at '^' marker. S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 21 S1(config-if)#exit S1(config)#
Interpretación de comandos realizados	En este punto realizamos la creación de la subredes Vlan en el S1, asignamos la dirección de administrador, generamos el Gateway predeterminado, se generaron enlaces troncales en F0/3, F0/5 y se configuraron los puertos restantes como puertos de acceso, se asigna a F0/6 a la Vlan 21

Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 20. Configurar 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.
Asignar la dirección IP de administración	Asigne la dirección IPv4 a la VLAN de administración. 192.168.99.3 255.255.255.0 Utilizar la dirección IP asignada al S3 en el diagrama de topología
Asignar el gateway predeterminado.	Asignar la primera dirección IP en la subred como gateway predeterminado.
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa S3(config)#int f0/3 S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1 S3(config-if)#end S3# %SYS-5-CONFIG_I: Configured from console by console
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range S3(config)#int range f0/4-17 S3(config-if-range)#switchport mode access S3(config-if-range)#end S3# %SYS-5-CONFIG_I: Configured from console by console

Asignar F0/18 a la VLAN 21	S3(config)#int f0/18 S3(config-if)#switchport mode access S3(config-if)#switchport access vlan 21 S3(config-if)#exit S3(config)#
Apagar todos los puertos sin usar	S3(config)#int range f0/4-17, f0/4-17,f0/19-24 S3(config-if-range)#shotdown
Interpretación de comandos realizados	En este punto generamos la configuración en el S3 creando la base de datos vlan , generamos una dirección IP al administrador , asignamos el gateway predeterminado, generamos enlaces troncales en F0/3 y configuramos el resto de puertos como acceso, asignamos a la F0/18 la subred Vlan 21 y apagamos los puertos que no se van a usar.

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 21. Configurar 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 LAN_Contabilidad R1(config-subif)#encapsulation dot1q 21 R1(config-subif)#ip address 192.168.21.2 255.255.255.0 R1(config-subif)#exit R1(config)#

Configurar la subinterfaz 802.1Q .23 en G0/1	Descripción: LAN de Ingeniería Asignar la VLAN 23 Asignar la primera dirección disponible a esta interfaz R1(config)#int g0/1.23 R1(config-subif)#description LAN_Ingenieria R1(config-subif)#encapsulation dot1q 23 R1(config-subif)#ip address 192.168.23.2 255.255.255.0 R1(config-subif)#exit R1(config)#
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)#description LAN_Administracin R1(config-subif)#encapsulation dot1q 99 R1(config-subif)#ip address 192.168.99.1 255.255.255.0 R1(config-subif)#exit
Activar la interfaz G0/1	R1(config)#int g0/1 R1(config-if)#no shutdown R1(config-if)#exit R1(config)#
Interpretación de comandos realizados	En este paso configuramos el R1 la subinterfaz 802.1Q para las Vlan 21,23,99 en las cuales asignamos direcciones IPV4 y luego activamos la interfaz G0/1.

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:

Tabla 22. Verificar la conectividad de red

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	POSITIVO S1#ping 192.168.99.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms Figura 18. Ping S1 a R1 192.168.99.1 

S3	R1, dirección VLAN 99	192.168.99.1	POSITIVO S3#ping 192.168.99.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/1/4 ms Figura 19. Ping S3 a R1 192.168.99.1 
S1	R1, dirección VLAN 21	192.168.21.2	POSITIVO S1#ping 192.168.21.2 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.21.2, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/6 ms

			 Figura 20. Ping S1 a R1 192.168.21.2
S3	R1, dirección VLAN 23	192.168.23.2	POSITIVO S3#ping 192.168.23.2 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.23.2, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/1/4 ms S3# S3# Figura 21. Ping S1 a R1 192.168.23.2

			
Interpretación de comandos realizados		En este punto realizamos las pruebas correspondientes a comunicaciones entre los dispositivos usando las direcciones IP previamente configuradas y todos los pings realizados fueron exitosos.	

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:

Tabla 23. Configurar OSPF en el R1

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

Anunciar las redes conectadas directamente	Asigne todas las redes conectadas directamente. R1(config-router)#network 172.16.1.0 255.255.255.252 area 0 R1(config-router)#network 172.16.1.8 255.255.255.252 area 0 R1(config-router)#network 192.168.21.0 255.255.255.0 area 0 R1(config-router)#network 192.168.23.0 255.255.255.0 area 0 R1(config-router)#network 192.168.99.0 255.255.255.0 area 0 R1(config-router)#
Establecer todas las interfaces LAN como pasivas	R1(config-router)#passive-interface s0/0/0 R1(config-router)#passive-interface g0/1
Desactive la sumarización automática	R1(config)#router rip R1(config-router)# no auto-summary R1(config-router)#end
Interpretación de comandos realizados	En este paso configuramos OSPF para enrutamiento dentro de la red del R1donde anunciamos las redes que se conectan a este equipo y generamos las redes LAN como pasivas , luego se desactivo la sumarización automática

Paso 2: Configurar OSPF en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla 24. Configurar OSPF en el R2

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R2(config)#router ospf 1
Anunciar las redes conectadas directamente	**Nota:** Omitir la red G0/0. R2(config-router)#network 10.10.10.10 255.255.255.255 are 0 R2(config-router)#network 10.10.10.10 255.255.255.255 area 0 R2(config-router)#network 172.16.1.0 255.255.255.252 area 0 R2(config-router)#network 172.16.2.0 255.255.255.252 area 0 R2(config-router)#exit
Establecer la interfaz LAN (loopback) como pasiva	R2(config-router)#passive-interface loopback0
Desactive la sumarización automática.	R2(config)#router rip R2(config-router)#no auto-summary R2(config-router)#exit
Interpretación de comandos realizados	En este punto generamos la configuración del protocolo OSPF de enrutamiento para el R2 , anunciamos cuales con las redes conectadas a este dispositivo , colocamos la LAN como pasiva y se desactivo la sumarización automática.

Paso 3: Configurar OSPFv3 en el R2

La configuración del R3 incluye las siguientes tareas:

Tabla 25. Configurar OSPFv3 en el R2

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	r3(config)#router ospf 1
Anunciar redes IPv4 conectadas directamente	r3(config-router)#network 172.16.2.0 255.255.255.252 area 0 08:01:40: %OSPF-5-ADJCHG: Process 1, Nbr 10.10.10.10 on Serial0/0/1 from LOADING to FULL, Loading Done r3(config-router)#network 192.168.4.0 255.255.255.0 area 0 r3(config-router)#network 192.168.5.0 255.255.255.0 area 0 r3(config-router)#network 192.168.6.0 255.255.255.0 area 0 r3(config-router)#exit
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	r3(config-router)#passive-interface loopback4 r3(config-router)#passive-interface loopback5 r3(config-router)#passive-interface loopback6
Desactive la sumarización automática.	r3(config-router)#no auto-summary r3(config-router)#end

Interpretación de comandos realizados	Se genero la configuración de OSPF para el R2 donde anunciamos cuales son las redes IPV4 conectadas directamente, luego colocamos todas las LAN IPV4 como pasivas y desactivamos la sumarización automática.

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:

Tabla 26. 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?	R1#show ip protocols Routing Protocol is "ospf 1" Outgoing update filter list for all interfaces is not set Incoming update filter list for all interfaces is not set Router ID 192.168.99.1 Number of areas in this router is 1. 1 normal 0 stub 0 nssa Maximum path: 4 Routing for Networks: 172.16.1.0 0.0.0.3 area 0 172.16.1.8 0.0.0.3 area 0 192.168.21.0 0.0.0.255 area 0 192.168.23.0 0.0.0.255 area 0 192.168.99.0 0.0.0.255 area 0 Passive Interface(s):

	GigabitEthernet0/1 Serial0/0/0 Routing Information Sources: Gateway Distance Last Update 192.168.99.1 110 00:05:52 Distance: (default is 110)
¿Qué comando muestra solo las rutas OSPF?	R1#show ip ospf Routing Process "ospf 1" with ID 192.168.99.1 Supports only single TOS(TOS0) routes Supports opaque LSA SPF schedule delay 5 secs, Hold time between two SPFs 10 secs Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs Number of external LSA 0. Checksum Sum 0x000000 Number of opaque AS LSA 0. Checksum Sum 0x000000 Number of DCbitless external and opaque AS LSA 0 Number of DoNotAge external and opaque AS LSA 0 Number of areas in this router is 1. 1 normal 0 stub 0 nssa External flood list length 0 Area BACKBONE(0) Number of interfaces in this area is 4 Area has no authentication

	SPF algorithm executed 4 times Area ranges are Number of LSA 1. Checksum Sum 0x005a5f Number of opaque link LSA 0. Checksum Sum 0x000000 Number of DCbitless LSA 0 Number of indication LSA 0 Number of DoNotAge LSA 0 Flood list length 0
¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	R1#show ip ospf interface Serial0/0/0 is up, line protocol is up Internet address is 172.16.1.1/30, Area 0 Process ID 1, Router ID 192.168.99.1, Network Type POINT-TO-POINT, Cost: 64 Transmit Delay is 1 sec, State POINT-TO-POINT, Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5 No Hellos (Passive interface) Index 1/1, flood queue length 0 Next 0x0(0)/0x0(0) Last flood scan length is 1, maximum is 1 Last flood scan time is 0 msec, maximum is 0 msec Suppress hello for 0 neighbor(s)

	GigabitEthernet0/1.21 is up, line protocol is up Internet address is 192.168.21.2/24, Area 0 Process ID 1, Router ID 192.168.99.1, Network Type BROADCAST, Cost: 1 Transmit Delay is 1 sec, State DR, Priority 1 Designated Router (ID) 192.168.99.1, Interface address 192.168.21.2 No backup designated router on this network Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5 Hello due in 00:00:07 Index 2/2, flood queue length 0 Next 0x0(0)/0x0(0) --More--
Interpretación de comandos realizados	En este paso usamos el comando show ip protocols para mostrar el ID del proceso, el comando show ip ospf para mostrar las rutas OSPF, el comando show ip ospf interface que no s muestra la selección OSPF de la configuración en ejecución.

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:

Tabla 27. Configurar R1 como servidor de DHCP para Vlan 21y23

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)# R1(config)#ip dhcp pool ACCT R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com R1(dhcp-config)#default-router 192.168.21.1 R1(dhcp-config)#network 192.168.21.0 255.255.255.0 R1(dhcp-config)#exit
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(config)#ip dhcp pool ENGNR R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com R1(dhcp-config)#default-router 192.168.23.1 R1(dhcp-config)#network 192.168.23.0 255.255.255.0 R1(dhcp-config)#exit R1(config)#

Interpretación de comandos realizados	En este paso asignamos 20 direcciones IP a las Vlan 21 para configuraciones estáticas y lo mismo aplicado a la Vlan 23, creamos protocolo DHCP para general configuraciones automáticas dentro de la red en las Vlan 21 y Valn 23

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

La configuración del R2 incluye las siguientes tareas:

Tabla 28: Configurar NAT estática y dinámica en el 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**
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 R2(config)#interface g0/0 R2(config-if)#ip nat outside R2(config-if)#interface g0/0 R2(config-if)#ip nat inside R2(config-if)#exit R2(config)#

Configurar la NAT dinámica dentro de una ACL privada	Lista de acceso: 1 Permitir la traducción de las redes de Contabilidad y de Ingeniería en el R1 Permitir la traducción de un resumen de las redes LAN (loopback) en el R3 R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.4.1 0.0.0.255 R2(config)#access-list 1 permit 192.168.5.1 0.0.0.255 R2(config)#access-list 1 permit 192.168.6.1 0.0.0.255 R2(config)#exit
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**
Definir la traducción de NAT dinámica	R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248 R2(config)#ip nat inside source list 1 pool INTERNET R2(config)#
Interpretación de comandos realizados	En este paso creamos la base da datos local, habilitamos el servidor HTTP, luego hicimos que HTTP use la base de datos local para autenticación, creamos una NAT estática al servidor Web y asignamos red interna y externa a NAT estática.

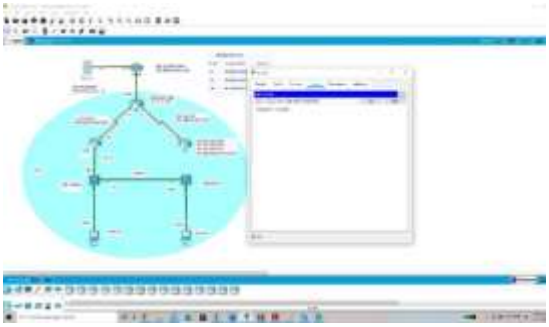
Paso 3: Verificar el protocolo DHCP y la NAT estática

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.

Tabla 29. Verificar el protocolo DHCP y la NAT estática

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	Figura 22. PC-A adquiere IP de DHCP 
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	Figura 23. PC-C Adquiere IP de DHCP 
Verificar que la PC-A pueda hacer ping a la PC-C **Nota:** Quizá sea necesario deshabilitar el firewall de la PC.	Realizamos el Ping a la dirección 192.168.23.21

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 24 . Prueba servidor Web 209.165.200.229 
Interpretación de comandos realizados	En este paso verificamos que se adquiriera la información del IP del servidor DHCP y realizamos ping de PC-a a PC-C siendo positivo

Parte 6: Configurar NTP

Tabla 30. Configurar NTP

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	**5 de marzo de 2016, 9 a. m.** R2#clock set 9:0:00 05 March 2016
ConfigureR2 como un maestro NTP.	Nivel de estrato: **5** R2(config)#ntp master 5
Configurar R1 como un cliente NTP.	Servidor: **R2**
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	R2(config)#ntp update-calendar
Verifique la configuración de NTP en R1.	R2#show ntp associations

Interpretación de comandos realizados	En este paso configuramos NTP para sincronizar los relojes, ajustamos la fecha y hora del R2 y luego el R1 para que verifique los datos del R2

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

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

Tabla 31. 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	Nombre de la ACL: **ADMIN-MGT** R2(config)#ip access-list standard ADMIN-MGT R2(config-std-nacl)#permit host 172.16.1.1 R2(config-std-nacl)#exit
Aplicar la ACL con nombre a las líneas VTY	R2(config)#line vty 0 4 R2(config-line)#access-class ADMIN-MGT in R2(config-line)#exit

Permitir acceso por Telnet a las líneas de VTY	R1(config)#exit R1# %SYS-5-CONFIG_I: Configured from console by console Telnet 172.16.1.1 Trying 172.16.1.1 ...Open Se prohibe el acceso no autorizado User Access Verification Password:
Verificar que la ACL funcione como se espera	Figura 25. Verificación ACL 
Interpretación de comandos realizados	En este paso configuramos al acceso que l R1 establezca conexión con R2 y permitimos el acceso de Telnet a líneas VTY

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

Tabla 32. Introducir comando CLI

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	**R(config)#show access-list**
Restablecer los contadores de una lista de acceso	**R(config)#clear access-list counters**
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	**R(config)#interface fa0/1** **R(confg)#ip Access-group 1out**
¿Con qué comando se muestran las traducciones NAT?	**R(conf)# show ip nat translations** **Nota:** Las traducciones para la PC-A y la PC-C se agregaron a la tabla cuando la computadora de Internet intentó hacer ping a esos equipos en el paso 2. Si hace ping a la computadora de Internet desde la PC-A o la PC-C, no se agregarán las traducciones a la tabla debido al modo de simulación de Internet en la red.
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	**R(config)#clear ip nat translation**
Interpretación de comandos realizados	En este paso usamos los comandos CLI para mostrar la respectiva información de coincidencias recibidas den listas de acceso , restablecer los contadores de lista de acceso, ver las traducciones NAT, eliminar traducciones NAT dinámicas.

CONCLUSIONES

Dentro de este curso comprendimos como se realiza una topología de red basada en la herramienta packet tracer la cual nos permitió simular como sería un escenario real de configuración de equipos y de cableado de los mismos dando una visión clara de cómo debe ser la instalación de los mismos de manera física.

Identificamos los protocolos necesarios para el direccionamiento de redes y subredes (Vlan , DHCP, Etherchannel NAT) que debemos configurar en cada dispositivo de red así como identificar cual en el uso correcto de los puertos físicos de los equipos para permitir su configuración y dar el direccionamiento de la información correcta de los datos.

Identificamos los protocolos de seguridad usados para la configuración de Router, Switch, PC los cuales son muy necesarios para dar seguridad a los parámetros de configuración, bases de datos entre otro para que la red siempre sea estable y no cualquier usuario pueda modificar parámetros de la misma.

Comprendimos como se debe realizar el enrutamiento entre redes diferentes con el fin de llegar a una conexión exitosa que nos permitiera enviar paquetes de datos de equipo a equipos sin perdida de datos, estas configuraciones son de alta utilidad para la aplicación en redes reales de nuestra vida profesional donde aplicaremos estos conocimientos para diseño de nuevas redes así como soporte de las ya existentes.

REFERENCIAS BIBLIOGRAFICAS

CISCO 2005, Configuración de ejemplo para la autenticación en OSPF, Recuperado de https://www.cisco.com/c/es_mx/support/docs/ip/open-shortest-path-first-ospf/13697-25.html

CISCO 20016, Configure NAT to Enable Communication Between Overlapping Networks, Recuperado de https://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/200726-Configure-NAT-to-Enable-Communication-Be.html

CISCO 20016, Configure NAT to Enable Communication Between Overlapping Networks, Recuperado de https://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/200726-Configure-NAT-to-Enable-Communication-Be.html

CISCO 2005, Configuración dinámica de opciones del servidor DHCP, Recuperado de https://www.cisco.com/c/en/us/support/docs/ip/dynamic-address-allocation-resolution/22920-dhcp-ser.html

CISCO 2005, Configuración de EtherChannel y enlace troncal 802.1Q entre switches de configuración fija Catalyst L2 y un enrutador (enrutamiento InterVLAN), Recuperado de https://www.cisco.com/c/en/us/support/docs/switches/catalyst-2950-series-switches/24042-158.html

CISCO 2019, Ejemplo de configuración de contraseñas de puerto auxiliar, consola y Telnet en routers Cisco, Recuperado de https://www.cisco.com/c/es_mx/support/docs/ios-nx-os-software/ios-software-releases-110/45843-configpasswords.html

ANEXOS

Anexo 1

Enlace descarga escenarios

https://drive.google.com/file/d/1Ok3yo-rVYf6g5qYDh5zazFw4zF7qyAml/view?usp=sharing

Anexo 2

Articulo científico IEEE

https://drive.google.com/file/d/1ihGlQgNnJjKDOS4L-E20LP0dVzgXIwKY/view?usp=sharing