SOLUCIÓN DE DOS ESTUDIOS DE CASO BAJO EL USO DE TECNOLOGÍA CISCO

WILMAN DARÍO LOPEZ CARMONA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
PROGRAMA DE INGENIERÍA TELECOMUNICACIONES
MEDELLIN
2021

SOLUCIÓN DE DOS ESTUDIOS DE CASO BAJO EL USO DE TECNOLOGÍA CISCO

WILMAN DARÍO LOPEZ CARMONA

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

TUTOR: HÉCTOR MANUEL HERRERA HERRERA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
PROGRAMA DE INGENIERÍA TELECOMUNICACIONES
MEDELLIN
2021

NOTA DE ACEPTACIÓN:

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

Medellin, 16 de Julio de 2021

AGRADECIMIENTOS

Me corresponde dar gracias a DIOS y a todos los que de una u otra manera me permitieron la posibilidad de estar y a mi de poder hacer y culminar este diplomado, también agradezco a los compañeros y docentes de la Universidad Nacional Abierta y a Distancia, quienes, aportaron al desarrollo de competencias intelectuales y profesionales, con las cuales logre culminar los estudios, por lo anterior gracias, gracias y gracias.

TABLA DE CONTENIDOS

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

DNS (Nombre de dominio): traduce los nombres de hots a direcciones IP para serentendidos por la computadora.

IP (Internet protocolo): es una dirección única que permite comunicación a la mayoría deredes.

IPV4: Direcciones de 32 bits que se utiliza para identificar en dispositivo que está en unared.

IPV6: Direcciones de 128 bits, que se usa para identificar una red, es una actualización delas direcciones de IPV4.

Looback: Interface que dirige el tráfico hacia ellos mismos.

RESUMEN

El presente trabajo desarrolla dos escenarios donde se ponen a prueba los conocimientos adquiridos a lo largo del desarrollo de este diplomado, con la interacción y configuración de los dispositivos CISCO en los diferentes escenarios planteados y simulados, identificando las funciones de los mismos y aprovechando el conocimiento brindado por los compañeros y docentes de este curso, además de la gran herramienta que es el Internet, con la cual disponemos en la actualidad. Todo este compendio nos permitio conocer mas sobre la gran infraestructura de CISCO.

ABSTRACT

The present work develops two scenarios where the knowledge acquired throughout the development of this diploma is tested, with the interaction and configuration of the CISCO devices in the different scenarios proposed and simulated, identifying their functions and taking advantage of the knowledge provided by colleagues and teachers of this course, in addition to the great tool that is the Internet, with which we currently have. All this compendium allowed us to know more about the great infrastructure of CISCO.

INTRODUCCIÓN

Con el presente trabajo se pretende adquirir las habilidades necesarias en el manejo de herramientas de simulación y laboratorio como son packet tracer y GNS3, con el fin de simular escenarios LAN/WAN que permitan realizar un análisis sobre el comportamiento de los diversos protocolos y métricas de enrutamiento que se utilizan en el área de redes para lograr un conocimiento profundo de la configuración de los diferentes dispositivos y garantizando una excelente comunicación.

OBJETIVOS

OBJETIVO GENERAL

El estudiante deberá hacer un avance correspondiente al desarrollo de la temática establecida como alternativa de grado (50% del trabajo total). La modalidad adoptada por el diplomado de profundización se denomina “Proyecto Aplicado”, en donde el director del curso propone dos escenarios con características y requerimientos específicos, en donde el primer escenario será desarrollado acorde con las temáticas del módulo 1.

OBJETIVOS ESPECÍFICOS

El estudiante utiliza herramientas de simulación y laboratorios de acceso remoto con el fin de establecer escenarios LAN/WAN que permitan realizar un análisis sobre el comportamiento de diversos protocolos y métricas de enrutamiento.

El estudiante identifica las herramientas de supervisión y protocolos de administración de red disponibles en el IOS para resolver los problemas de las redes de datos, evaluando el desempeño de routers y switches, mediante el uso de comandos especializados en gestión de redes.

Solución de dos estudios de caso bajo el uso de tecnología CISCO

Escenario 1

Topología

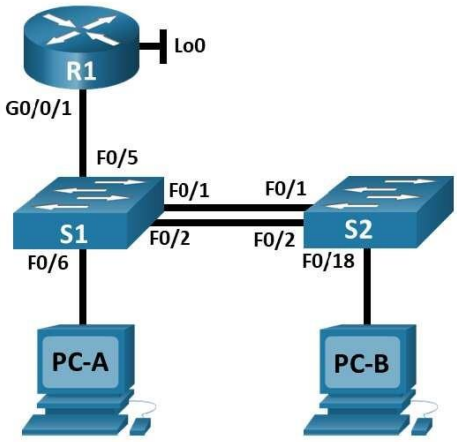


Ilustración 1. Topología general del escenario 1

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

Tabla de VLAN

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

Tabla 1. Distribución de Vlan para el escenario 1

Tabla de asignación de direcciones

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
R1 G0/0/1.2	10.21.5.1 /26	No corresponde
	2001:db5:acad:a: :1 /64	No corresponde
R1 G0/0/1.3	10.21.5.65 /27	No corresponde
	2001:db5:acad:b: :1 /64	No corresponde
R1 G0/0/1.4	10.21.5.97 /29	No corresponde
	2001:db5:acad:c: :1 /64	No corresponde
R1 G0/0/1.6	No corresponde	No corresponde
R1 Loopback0	209.165.201.1 /27	No corresponde
	2001:db8:acad:209: :1 /64	No corresponde
S1 VLAN 4	10.21.5.98 /29	10.21.5.97
	2001:db5:acad:c: :98 /64	No corresponde
	fe80: :98	No corresponde
S2 VLAN 4	10.21.5.99 /29	10.21.5.97
	2001:db5:acad:c: :99 /64	No corresponde
	fe80: :99	No corresponde
PC-A NIC	Dirección DHCP para IPv4	DHCP para puerta de enlace predeterminada IPv4
	2001:db5:acad:a: :50 /64	fe80::1
PC-B NIC	DHCP para dirección IPv4	DHCP para puerta de enlace predeterminada IPv4
	2001:db5:acad:b: :50 /64	fe80::1

Tabla 2. Asignación para el direccionamiento del escenario 1

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

EL ítem resaltado al parecer tiene un error por lo que se cambia en el proceso.

Parte 1: Inicializar, Recargar y Configurar aspectos básicos de los dispositivos.

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

Se borran las configuraciones de inicio y las VLAN tanto del router como de los switch, luego se vuelven a cargar los dispositivos.

Nota: Esta primera parte se revisa y no se detectan Vlans para borrar, se cambia nombre a los dispositivos, se borra configuración de inicio y se cargan de nuevo. Se utilizan los comandos siguientes: erase startup-config, delete Vlan.data, reload.

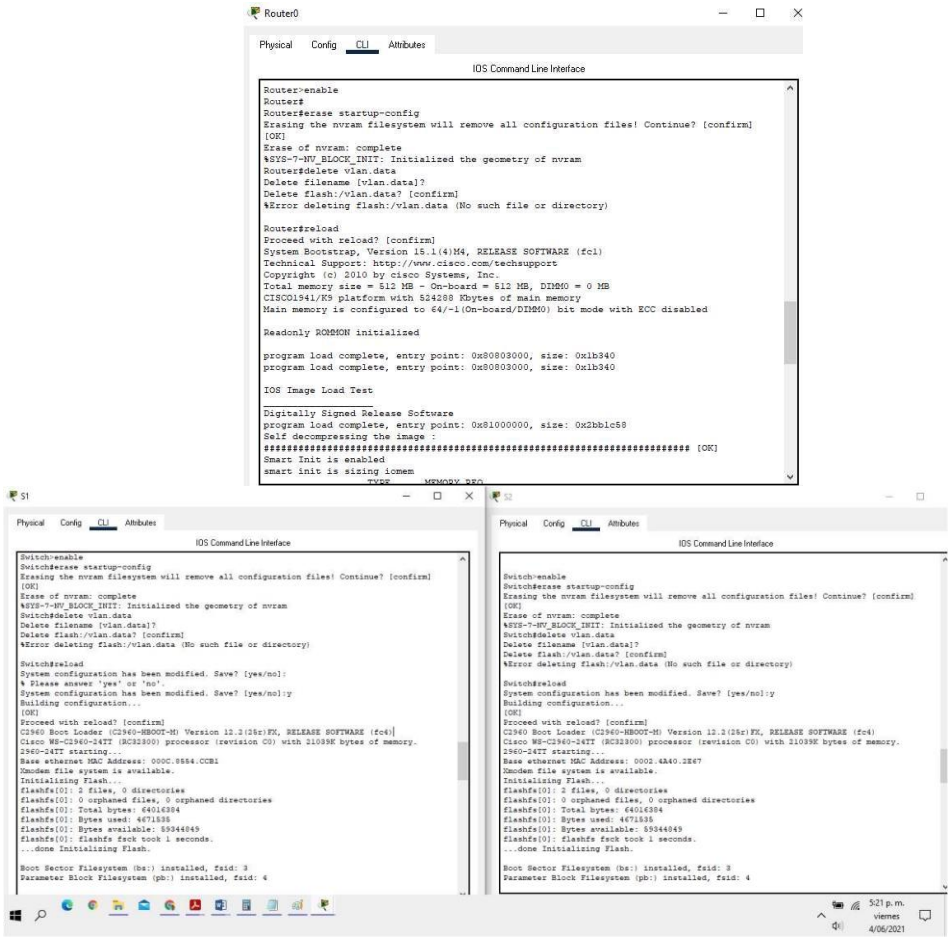


Ilustración 2.Comandos inicio configuración Router y Switchs

Nota: Se continua con la revisión y cambio de plantilla SDM en los Switchs, se cambia de plantilla “default” a “dual-IPv4-and-Ipv6 default” y se carga nuevamente la configuración. Los comandos utilizados fueron: show sdm prefer, sdm prefer dual-IPv4-and-Ipv6 default, reload.

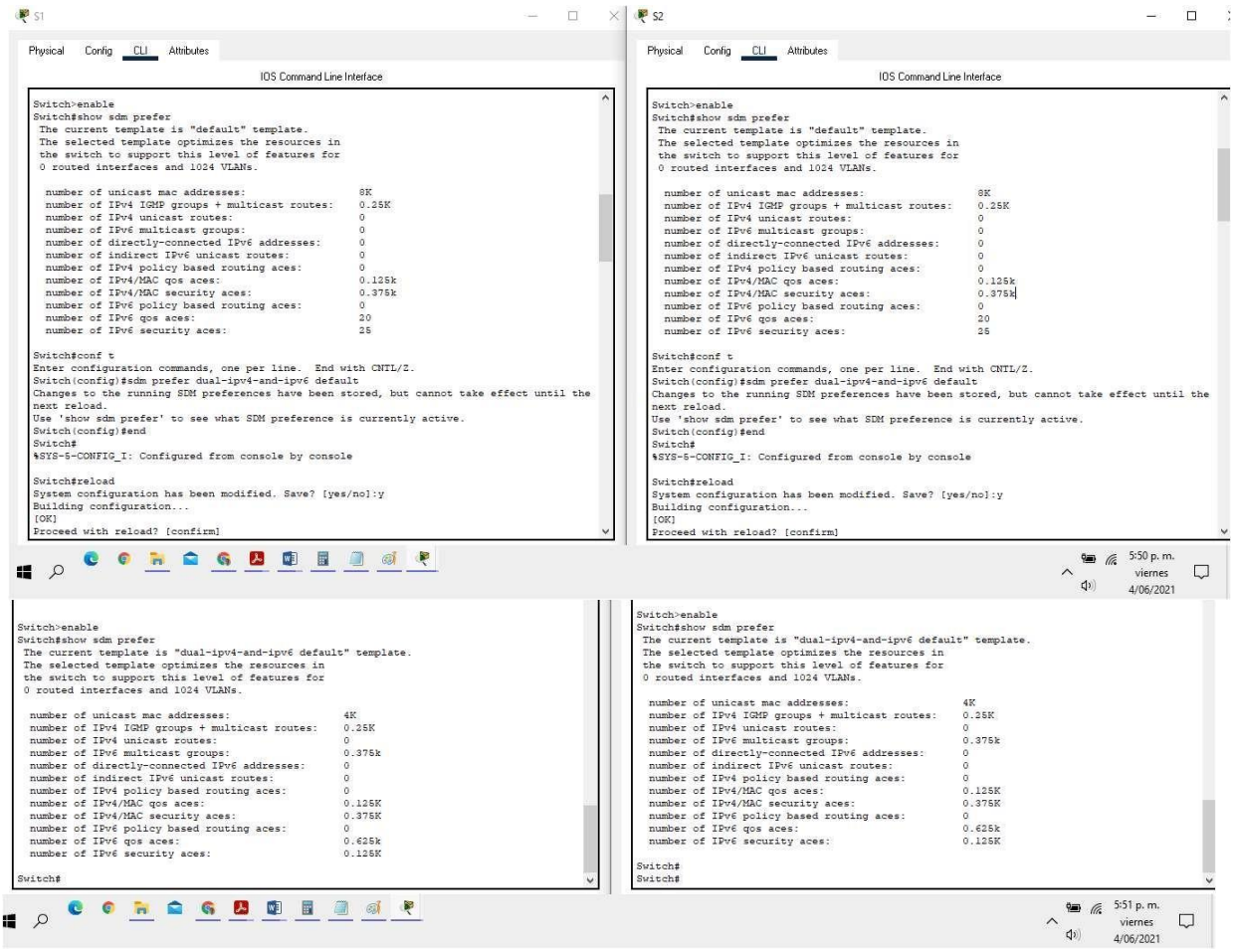


Ilustración 3. Configuración de la plantilla SDM para admitir IPv6-IPV4 en los Switchs

Código utilizado en imagen 3 para los 2 Switchs:

```
S1-S2#sh sdm prefer
The current template is "dual-ipv4-and-ipv6 default" template.
The selected template optimizes the resources in
the switch to support this level of features for
0 routed interfaces and 1024 VLANs.
number of unicast mac addresses:                  4K
number of IPv4 IGMP groups + multicast routes:    0.25K
number of IPv4 unicast routes:                    0
number of IPv6 multicast groups:                  0.375k
number of directly-connected IPv6 addresses:      0
number of indirect IPv6 unicast routes:           0
number of IPv4 policy based routing aces:         0
number of IPv4/MAC qos aces:                      0.125K
number of IPv4/MAC security aces:                 0.375K
number of IPv6 policy based routing aces:         0
number of IPv6 qos aces:                          0.625k
number of IPv6 security aces:                     0.125K
```

Paso 2: Configurar R1: Las tareas de configuración para R1 son las de la siguiente tabla:

Tarea	Especificación
Desactivar la búsqueda DNS	
Nombre del router	R1
Nombre de dominio	ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	ciscoenpass
Contraseña de acceso a la consola	ciscoconpass
Establecer la longitud mínima para las contraseñas	10 caracteres
Crear un usuario administrativo en la base de datos local	Nombre de usuario: **admin** Password: **admin1pass**
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	
Configurar VTY solo aceptando SSH	
Cifrar las contraseñas de texto no cifrado	
Configure un MOTD Banner	
Habilitar el routing IPv6	
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.
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**
Generar una clave de cifrado RSA	Módulo de 1024 bits

Tabla 3. Configuraciones para realizar en R1

Nota: A continuación, se realiza la primera parte de configuración inicial y básica de R1. Se utilizan los siguientes comandos: no ip domain-lookup, hostname, ip domain-name, enable secret, line console 0, password, login, security password min-length, username, transport input ssh, service password-encryption, banner motd.

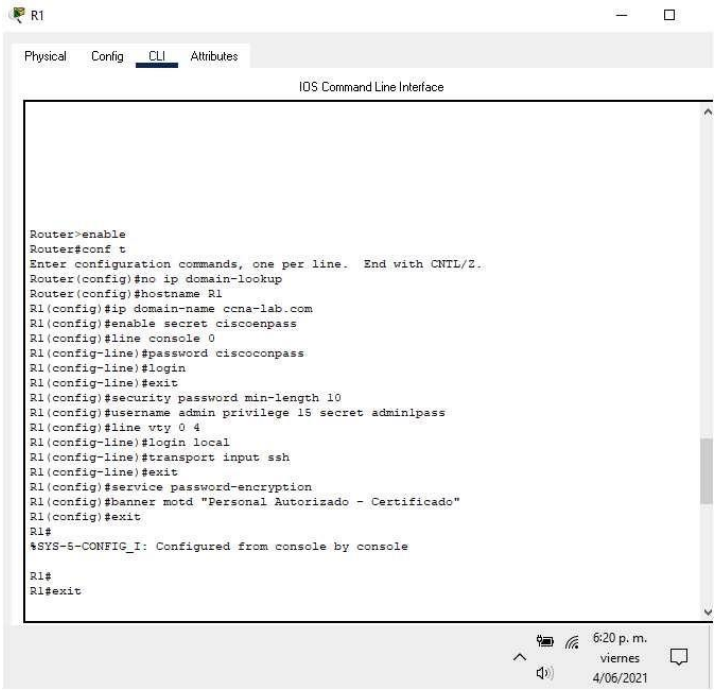


Ilustración 4. Configuración inicial de R1

Código utilizado en imagen 4 con el R1:

```
R1(config)#line vty 0 4
R1(config-line)#line vty 0 4
R1(config-line)#login local
R1(config-line)#line vty 0 4
R1(config-line)#line vty 0 4 transport input ssh
% Invalid input detected at '^' marker.
R1(config-line)#transport input ssh
R1(config-line)#exit
```

Nota: Se realiza configuración de R1 en su interfaz G0/1 y sus subinterfaces 1.2,1.3,1.4 y 1.6, además del link local. Se puede evidenciar algunas de las configuraciones realizadas anteriormente como el aviso inicial, nombre del Router y la seguridad. Algunos comandos utilizados: Interface, encapsulation, ip add, ipv6 add, description, no shutdown.

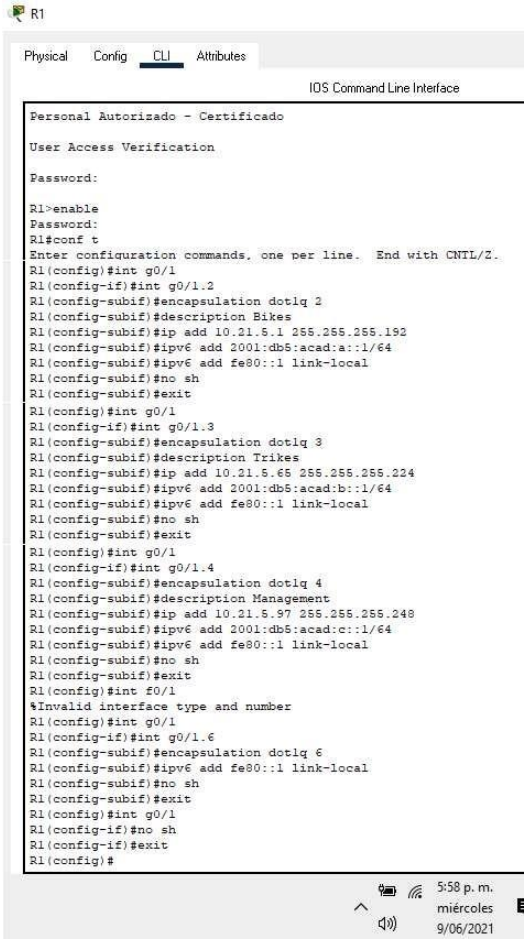


Ilustración 5. Configuración en R1, interfaz G0/1 y subinterfaces

Código utilizado en imagen 5 con R1:

```
R1(config)#int g0/1
R1(config-if)#int g0/1.2
R1(config-subif)#encapsulation dot1q 2
R1(config-subif)#description Bikes
R1(config-subif)#ip add 10.21.5.1 255.255.255.192
R1(config-subif)#ipv6 add 2001:db5:acad:a::1/64
R1(config-subif)#ipv6 add fe80::1 link-local
R1(config-subif)#no sh
R1(config-subif)#exit
R1(config)#int g0/1
R1(config-if)#int g0/1.3
R1(config-subif)#encapsulation dot1q 3
R1(config-subif)#description Trikes
R1(config-subif)#ip add 10.21.5.65 255.255.255.224
R1(config-subif)#ipv6 add 2001:db5:acad:b::1/64
R1(config-subif)#ipv6 add fe80::1 link-local
R1(config-subif)#no sh
R1(config-subif)#exit
R1(config)#int g0/1
R1(config-if)#int g0/1.4
R1(config-subif)#encapsulation dot1q 4
R1(config-subif)#description Management
R1(config-subif)#ip add 10.21.5.97 255.255.255.248
R1(config-subif)#ipv6 add 2001:db5:acad:c::1/64
R1(config-subif)#ipv6 add fe80::1 link-local
R1(config-subif)#no sh
R1(config-subif)#exit
R1(config)#int g0/1
R1(config-if)#int g0/1.6
R1(config-subif)#encapsulation dot1q 6
R1(config-subif)#ipv6 add fe80::1 link-local
R1(config-subif)#no sh
R1(config-subif)#exit
R1(config)#int g0/1
R1(config-if)#no sh
R1(config-if)#exit
R1#
```

Nota: Siguiendo con la configuración de R1, donde iniciamos configurando el Loopback 0 con IPv4 e IPv6, además del link local y por último se genera la clave

de cifrado RSA, con la cual determinamos el tamaño de la clave y el valor de encriptación que se deja el mínimo sugerido que es 1024. Los comandos utilizados son: interface loopback 0, IP add, IPv6 add, descript, no sh, crypto key generate rsa general-keys modulus 1024.

Se realiza un cambio en la dirección **IPv6** dado que en la guía aparece 2001:**db8**:acad:209::1/64 y para un direccionamiento efectivo de ser 2001:**db5**:acad:209::1/64.

Código utilizado en imagen 6 con R1:

```
R1(config)#int loopback0
R1(config-if)#ip add 209.165.201.1 255.255.255.224
R1(config-if)#ipv6 add 2001:db5:acad:209::1/64
R1(config-if)#ipv6 add fe80::1 link-local
R1(config-if)#no sh
R1(config-if)#exit
R1(config)#
```

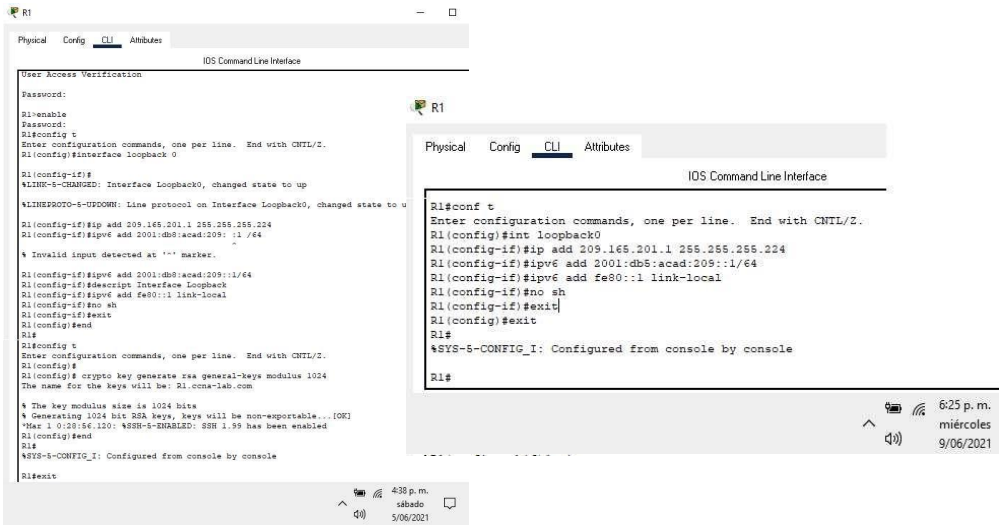


Ilustración 6. Configuración R1 con Interface loopback y Generación clave de cifrado RSA

Paso 3: Configure S1 y S2: las tareas de configuración están en la siguiente tabla:

Tarea	Especificación
Desactivar la búsqueda DNS.	
Nombre del switch	**S1 o S2, según proceda**
Nombre de dominio	**ccna-lab.com**
Contraseña cifrada para el modo EXEC privilegiado	**ciscoenpass**
Contraseña de acceso a la consola	**ciscoconpass**
Crear un usuario administrativo en la base de datos local	Nombre de usuario: **admin** Password: **admin1pass**
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	
Cifrar las contraseñas de texto no cifrado	
Configurar un MOTD Banner	
Generar una clave de cifrado RSA	**Módulo de 1024 bits**
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
Configuración del gateway predeterminado	Configure la puerta de enlace predeterminada como 10.21.5.97 para IPv4

Tabla 4. Configuraciones para realizar en los Switchs

Nota: En esta configuración de los Switchs, la primera parte es de la configuración general que maneja desde el cambio del nombre, se asocia al dominio, se ponen claves, usuario y configuración VTY para base de daos local y conexiones SSH, el aviso y manejo de clave de cifrado RSA. Los comandos utilizados son: no ip domain lookup, hostname, ip domain-name, enable secret, line con 0, password, login, username ### privilege 15 secret ###, line vty, login local, transport input ssh, service password-encryption, banner motd, crypto key generate rsa general-key modulus 1024.

Código empleado en la figura 7 con los dos Switchs:

```
S1-S2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S1-S2(config)#no ip domain-lookup
S1-S2(config)#ip domain-name ccna-lab.com
S1-S2(config)#line vty 0 4
S1-S2(config-line)#login local
S1-S2(config-line)#transport input ssh
S1-S2(config-line)#exit
S1-S2(config)#crypto key generate rsa general-key modulus 1024
% You already have RSA keys defined named S1.ccna-lab.com
% They will be replaced.
% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
*Mar 1 4:51:51.710: %SSH-5-ENABLED: SSH 1.99 has been enabled
S1-S2(config)#end
S1-S2#
```

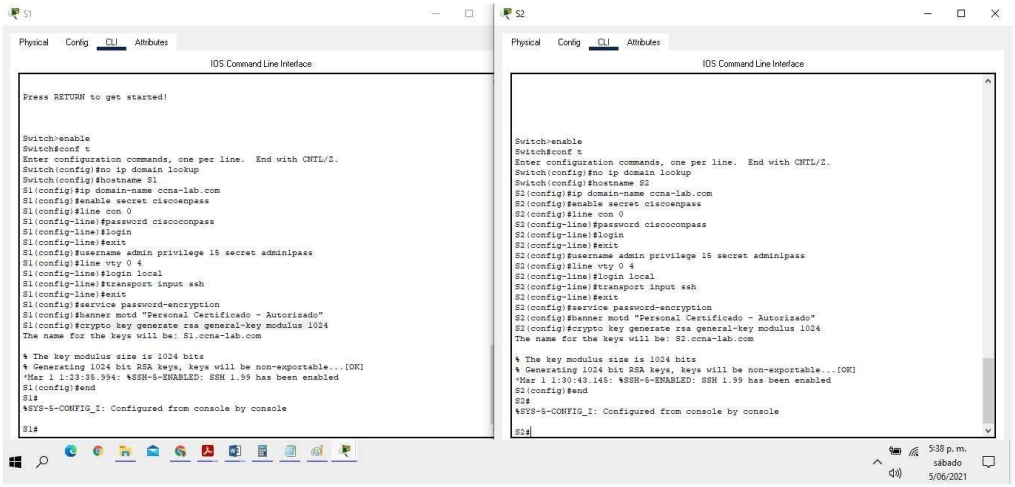


Ilustración 7. Configuración inicial de los Switchs

Nota: Continuando con la configuración de los Switchs, se interviene la interfaz de administración (SVI), donde se establece la dirección IPv4 y IPv6 de capa 3, la dirección local de enlace IPv6 para cada uno y por último la configuración de la puerta de enlace predeterminada.

Se utilizan los comandos: ipv6 unicast-routing, int vlan #, ip add, ipv6 add, ip default-gateway.

Código empleado en la figura 8 con los dos Switchs:

```
Personal Certificado - Autorizado
User Access Verification
Password:
S1-S2>enable
Password:
S1-S2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S1-S2(config)#int vlan 4
S1-S2(config-if)#description Management
S1(config-if)#ip add 10.21.5.98 255.255.255.248
S2(config-if)#ip add 10.21.5.99 255.255.255.248
S1-S2(config-if)#no sh
S1-S2(config-if)#ip default-gateway 10.21.5.97
S1(config)#end
S1-S2(config)#int vlan 4
S1(config-if)#ipv6 add 2001:db5:acad:c::98/64
S2(config-if)#ipv6 add 2001:db5:acad:c::99/64
S1(config-if)#ipv6 add fe80::98 link-local
S2(config-if)#ipv6 add fe80::99 link-local
S1-S2(config-if)#no sh
S1-S2(config-if)#exit
```

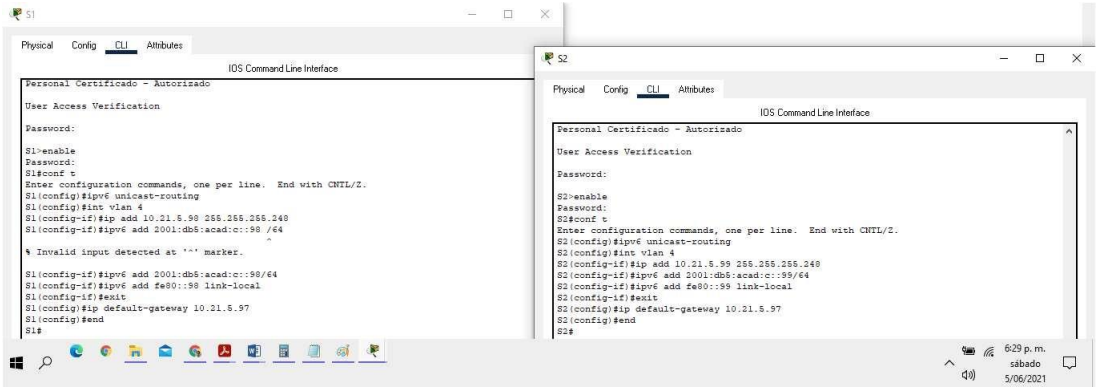


Ilustración 8. Configuración adicional para los Switchs con IPv4 e IPv6

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

Paso 1: Configuración del S1, las tareas a realizar se pueden ver en la siguiente tabla:

Tarea	Especificación
Crear VLAN	VLAN 2, nombre Bikes VLAN 3, nombre Trikes VLAN 4, name Management VLAN 5, nombre Parking VLAN 6, nombre Native
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	Interfaces F0/1, F0/2 y F0/5
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	Usar el protocolo LACP para la negociación
Configurar el puerto de acceso de host para VLAN 2	Interface F0/6
Configurar la seguridad del puerto en los puertos de acceso	Permitir 3 direcciones MAC
Proteja todas las interfaces no utilizadas	Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar

Tabla 5. Configuración de infraestructura de red en S1

Nota: Se realiza la configuración de infraestructura de red en S1 con las VLAN, los Trunk en las interfaces, creación de un grupo de puertos, configurar puerto de acceso con la seguridad y protección de interfaces no utilizadas.

Código e imagen de creación y verificación Vlans en S1:

```
User Access Verification
Password:
S1>enable
Password:
S1#conf T
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#vlan 2
S1(config-vlan)#name Bikes
S1(config-vlan)#exit
S1(config)#vlan 3
```

```
S1(config-vlan)#name Trikes
S1(config-vlan)#exit
S1(config)#vlan 4
S1(config-vlan)#name Management
S1(config-vlan)#exit
S1(config)#vlan 5
S1(config-vlan)#name Parking
S1(config-vlan)#exit
S1(config)#vlan 6
S1(config-vlan)#name Native
S1(config-vlan)#exit
S1(config)#exit
S1#
S1#sh vlan br
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gig0/1, Gig0/2
2    Bikes                             active
3    Trikes                            active
4    Management                        active
5    Parking                           active
6    Native                            active
```

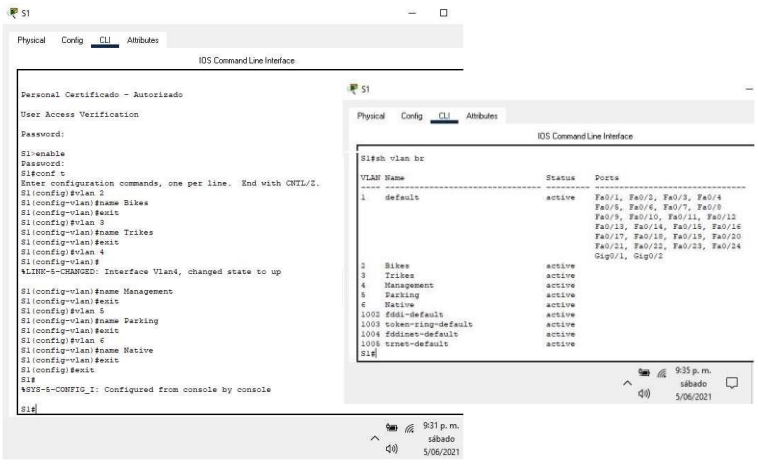


Ilustración 9. Creación y verificación de Vlans en S1

Código e imagen de configuración S1 “trunk” 802.1Q para utilizar la VLAN 6 nativa: el comando “switchport trunk encapsulation dot1Q”, no se requiere en este modelo de Switch se hace la configuración directa como se muestra a continuación.

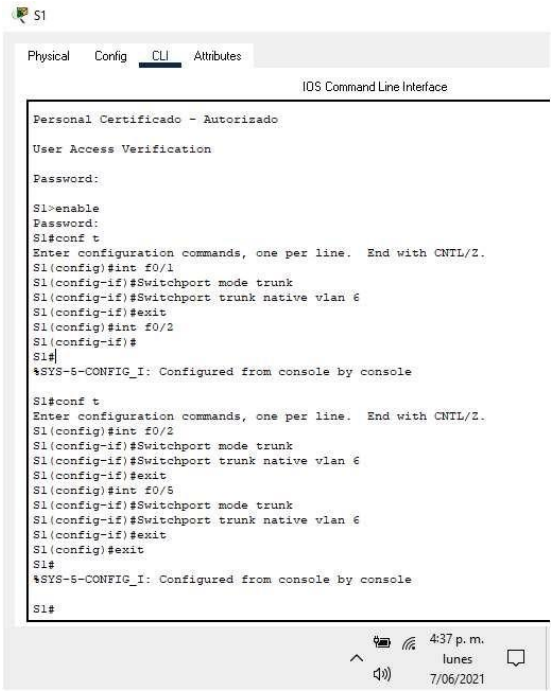


Ilustración 10. Configuración S1 “trunk” 802.1Q en VLAN 6 nativa

```
S1(config)#int f0/1
S1(config-if)#Switchport mode trunk
S1(config-if)#Switchport trunk native vlan 6
S1(config-if)#exit
S1(config)#int f0/2
S1(config-if)#Switchport mode trunk
S1(config-if)#Switchport trunk native vlan 6
S1(config-if)#exit
S1(config)#int f0/5
S1(config-if)#Switchport mode trunk
S1(config-if)#Switchport trunk native vlan 6
S1(config-if)#exit
S1(config)#exit
S1#
```

Código e imagen Verificación de configuración y uso de VLAN 6 “Nativa”:

S1#sh int f0/1 switchport - S1#sh int f0/2 switchport - S1#sh int f0/5 switchport
Name: Fa0/1 Name: Fa0/2 Name: Fa0/5
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 6 (Native)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: All
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none

Ilustración 11. Verificación configuración-uso VLAN 6 Nativa

Código e imagen de creación de un grupo de puertos EtherChannel de Capa 2 con las interfaces F0/1 y F0/2, Usar protocolo LACP para negociación:

Ilustración 12. Creación grupo de puertos EtherChannel capa 2 interfaces F0/1-2, con LACP

Personal Certificado - Autorizado
User Access Verification
Password:
S1>enable
Password:
Password:
S1#enable
S1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#int ran f0/1-2
S1(config-if-range)#channel-protocol lacp
S1(config-if-range)#channel-group 1 mode active
S1(config-if-range)#exit
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console
S1#sh ether
Channel-group listing:

Group: 1

Group state = L2

Ports: 2 Maxports = 16
Port-channels: 1 Max Port-channels = 16
Protocol: LACP
S1#

Código e imagen de configuración y verificación puerto de acceso de host para VLAN 2:

```
S1(config)#int f0/6
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 2
S1(config-if)#exit
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console
S1#sh vlan brief
VLAN Name Status Ports
---- -------------------------------- --------- -------------------------------
1 default active Po1, Fa0/1, Fa0/2, Fa0/3
Fa0/4, Fa0/7, Fa0/8, Fa0/9
Fa0/10, Fa0/11, Fa0/12, Fa0/13
Fa0/14, Fa0/15, Fa0/16, Fa0/17
Fa0/18, Fa0/19, Fa0/20, Fa0/21
Fa0/22, Fa0/23, Fa0/24, Gig0/1
Gig0/2
2 Bikes active Fa0/6
3 Trikes active
4 Management active
5 Parking active
6 Native active
```

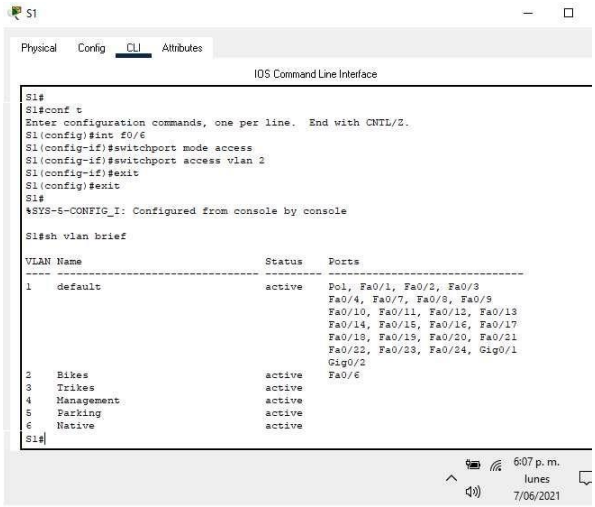


Ilustración 13. Configuración y verificación puerto de acceso de host para VLAN 2

Código e imagen de Configuración port-security en los access ports, permitir

3 MAC add:

```
S1(config)#int f0/6
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)#exit
S1(config)#exit
S1#
```

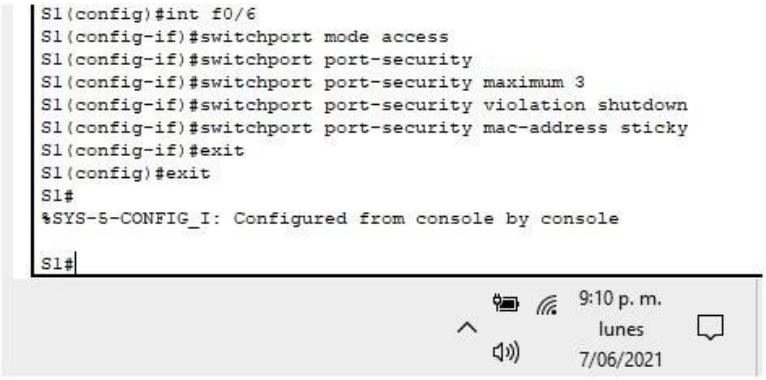


Ilustración 14. Configuración port-security en los access ports, validar 3 MAC add

Código e imagen proceso para protección de las interfaces no utilizadas:

S1(config)#int range g0/1-2, f0/3-4, f0/7-24
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 5
S1(config-if-range)#descript Proteccion Interfaces no utilizadas
S1(config-if-range)#sh
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to administratively down
S1(config-if-range)#switchport port-security
S1(config-if-range)#switchport port-security violation shutdown
S1(config-if-range)#exit
S1(config)#exit
S1#

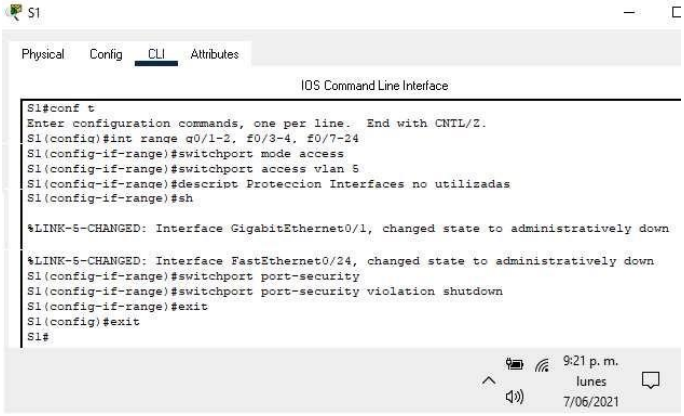


Ilustración 15. Proceso para protección de las interfaces no utilizadas

Paso 2: Configuración del S2, las tareas a realizar se pueden ver en la siguiente tabla:

Tarea	Especificación
Crear VLAN	VLAN 2, name Bikes VLAN 3, name Trikes VLAN 4, name Management VLAN 5, nombre Parking VLAN 6, nombre Native
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	Interfaces F0/1 y F0/2
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	Usar el protocolo LACP para la negociación
Configurar el puerto de acceso del host para la VLAN 3	Interfaz F0/18
Configure port-security en los access ports	permite 3 MAC addresses
Asegure todas las interfaces no utilizadas.	Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar

Tabla 6. Configuración de infraestructura de red en S2

Nota: Se realiza la configuración de infraestructura de red en S2 con las VLAN, los Trunk en las interfaces, creación de un grupo de puertos, configurar puerto de acceso con la seguridad y protección de interfaces no utilizadas.

Código e imagen de creación y verificación de Vlans en S2:

```
Personal Certificado - Autorizado
User Access Verification
Password:
S2>enable
Password:
S2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#vlan 2
S2(config-vlan)#name Bikes
S2(config-vlan)#exit
S2(config)#vlan 3
S2(config-vlan)#name Trikes
S2(config-vlan)#exit
S2(config)#vlan 4
S2(config-vlan)#
%LINK-5-CHANGED: Interface Vlan4, changed state to up
S2(config-vlan)#name Management
S2(config-vlan)#exit
S2(config)#vlan 5
S2(config-vlan)#name Parking
S2(config-vlan)#exit
S2(config)#vlan 6
S2(config-vlan)#name Nativa
S2(config-vlan)#exit
S2(config)#exit
S2#show vlan brief
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gig0/1, Gig0/2
2    Bikes                             active
3    Trikes                            active
4    Management                        active
5    Parking                           active
6    Nativa                            active
```

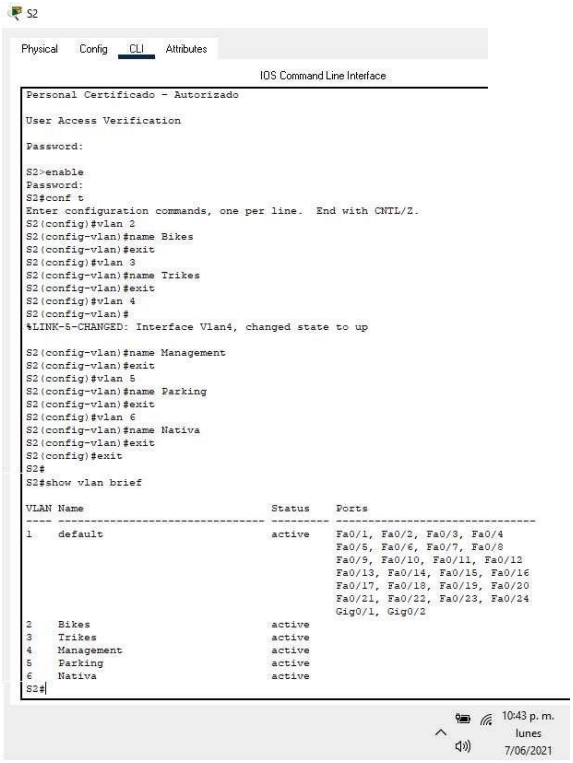


Ilustración 16. Creación y verificación Vlans S2

Código e imagen de configuración S2 “trunk” 802.1Q para utilizar la VLAN 6 nativa: el comando “switchport trunk encapsulation dot1Q”, no se requiere en este modelo de Switch se hace la configuración directa como se muestra a continuación.

```
Personal Certificado - Autorizado
User Access Verification
Password:
S2>enable
Password:
S2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#int f0/1
S2(config-if)#Switchport mode trunk
S2(config-if)#Switchport trunk native vlan 6
S2(config-if)#exit
```

```
S2(config)#int f0/2
S2(config-if)#Switchport mode trunk
S2(config-if)#Switchport trunk native vlan 6
S2(config-if)#exit
S2(config)#exit
S2#
```

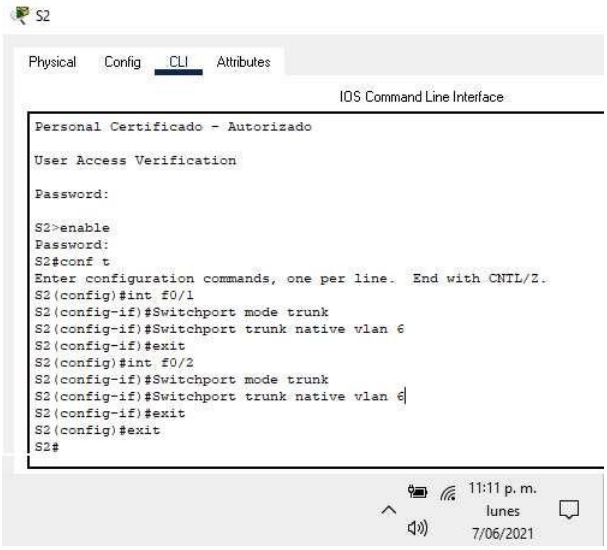


Ilustración 17. Configuración S2 "trunk" 802.1Q para VLAN 6 nativa

Código e imagen Verificación de configuración y uso de VLAN 6 "Nativa":

```
S2#show int f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 6 (Nativa)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
```

```
S2#show int f0/2 switchport
Name:  Fa0/1
```

Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: All
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none

Ilustración 18. Verificación de configuración y uso de VLAN 6 “Nativa”

Código e imagen de creación de un grupo de puertos EtherChannel de Capa 2 con las interfaces F0/1 y F0/2, Usar protocolo LACP para negociación:

```
Personal Certificado - Autorizado
User Access Verification
Password:
S2>enable
Password:
S2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#int ran f0/1-2
S2(config-if-range)#channel-protocol lacp
S2(config-if-range)#channel-group 1 mode passive
S2(config-if-range)#exit
S2(config)#exit
S2#
%SYS-5-CONFIG_I: Configured from
console by console
S2#sh ether
Channel-group listing:
----------------------
Group: 1
----------
Group state = L2
Ports: 2 Maxports = 16
Port-channels: 1 Max Port-channels = 16
Protocol: LACP
S2#
```

Ilustración 19. Creación grupo de puertos EtherChannel capa 2 interfaces F0/1-2, con LACP

Código e imagen de Configuración puerto de acceso del host VLAN 3 en Interfaz F0/18:

Personal Certificado - Autorizado
User Access Verification
Password:
S2>enable
Password:
S2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#int f0/18
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 3
S2(config-if)#exit
S2(config)#exit
S2#
%SYS-5-CONFIG_I: Configured from console by console
S2#sh vlan brief
VLAN Name Status Ports

```
---- -------------------------------- --------- -------------------------------
1    default                          active    Po1, Fa0/1, Fa0/2, Fa0/3
                                                Fa0/4, Fa0/5, Fa0/6, Fa0/7
                                                Fa0/8, Fa0/9, Fa0/10, Fa0/11
                                                Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                Fa0/16, Fa0/17, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gig0/1, Gig0/2
2    Bikes                            active
3    Trikes                           active    Fa0/18
4    Management                       active
5    Parking                          active
6    Nativa                           active
S2#
```

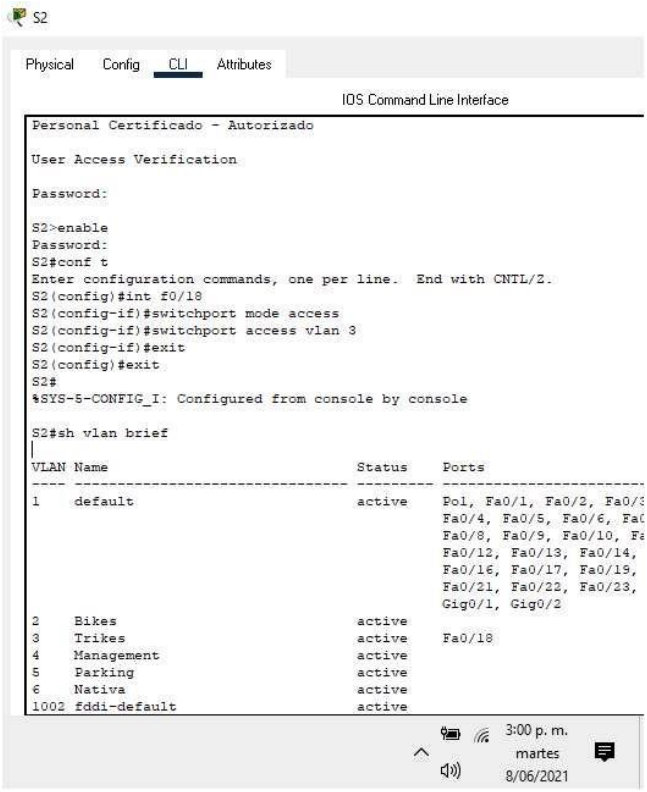


Ilustración 20. Configuración puerto de acceso del host VLAN 3 en Interfaz F0/18

Código e imagen de Configuración port-security en los access ports, permitir 3 MAC add:

```
S2(config)#int f0/18
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)#exit
S2(config)#exit
S2#
```

Ilustración 21. Configuración port-security en los access ports, validar 3 MAC add

Código e imagen de proceso para asegurar todas las interfaces no utilizadas, asignar a VLAN 5, establecer en modo de acceso, agregar una descripción y apagar:

```
User Access Verification
Password:
S2>enable
Password:
S2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#int ran g0/1-2, f0/3-4, f0/7-17, f0/19-24
S2(config-if-range)#switchport mode access
S2(config-if-range)#switchport access vlan 5
S2(config-if-range)#sh
%LINK-5-CHANGED: Interface GigabitEthernet0/1-2, changed state to
administratively down
%LINK-5-CHANGED: Interface FastEthernet0/3-4, changed state to
administratively down
%LINK-5-CHANGED: Interface FastEthernet0/7-24, changed state to
administratively down
S2(config-if-range)#switchport port-security
S2(config-if-range)#switchport port-security violation shutdown
S2(config-if-range)#exit
S2(config)#exit
S2#
```

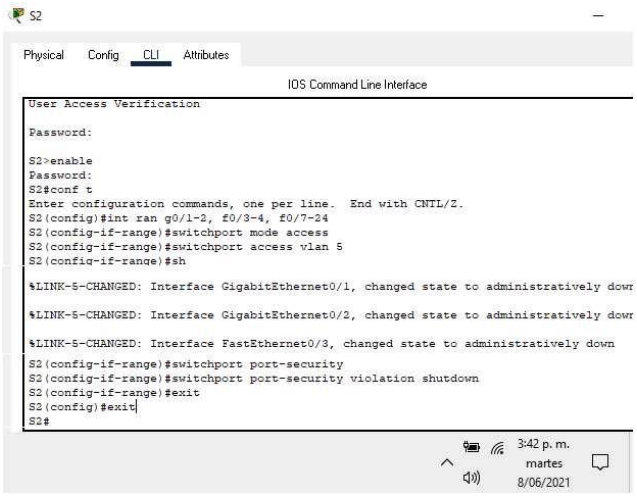


Ilustración 22. Proceso para asegurar todas las interfaces no utilizadas, asignar VLAN 5

Parte 3: Configurar soporte de host

Paso 1: Configuración del R1, las tareas a realizar se pueden ver en la siguiente tabla:

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
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

Tabla 7. Configuración de R1, su enrutamiento y activar DHCP en las Vlans

Nota: Esta configuración avanzada del Router 1 crea rutas predeterminadas IPv4 e IPv6 con tráfico por Loopback 0, también trabajar IPv4 con DHCP por Vlan 2 y 3, asignar subredes, nombre de dominio, puerta de enlace según indicación.

Código e imagen de la siguiente parte "Configure Default Routing":

```
Crear rutas predeterminadas para IPv4 e IPv6 que dirijan el tráfico a la interfaz
Loopback 0.
R1#
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#int loopback 0
R1(config-if)#ip route 0.0.0.0 0.0.0.0 loopback 0
%Default route without gateway, if not a point-to-point interface, may impact
performance
R1(config)#ipv6 route ::/0 loopback 0
R1(config)#exit
```

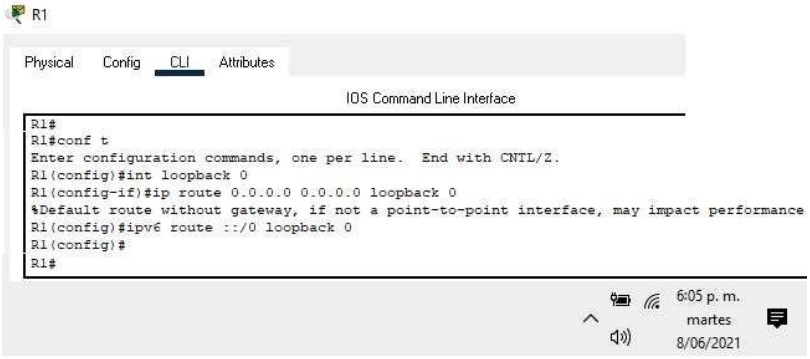


Ilustración 23. Configure Default Routing

Código e imagen de la Configuración IPv4 DHCP para VLAN 2 y VLAN3

Personal Autorizado - Certificado
User Access Verification
Password:
R1>enable
Password:
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip dhcp pool vlan2
R1(dhcp-config)#network 10.21.5.0 255.255.255.192
R1(dhcp-config)#default-router 10.21.5.1
R1(dhcp-config)#domain-name ccna-a.net
R1(dhcp-config)#ip dhcp excluded-address 10.21.5.2 10.21.5.51
R1(config)#exit
R1#
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip dhcp pool vlan3
R1(dhcp-config)#network 10.21.5.64 255.255.255.224
R1(dhcp-config)#default-router 10.21.5.65
R1(dhcp-config)#domain-name ccna-b.net
R1(dhcp-config)#ip dhcp excluded-address 10.21.5.66 10.21.5.83
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console
R1#

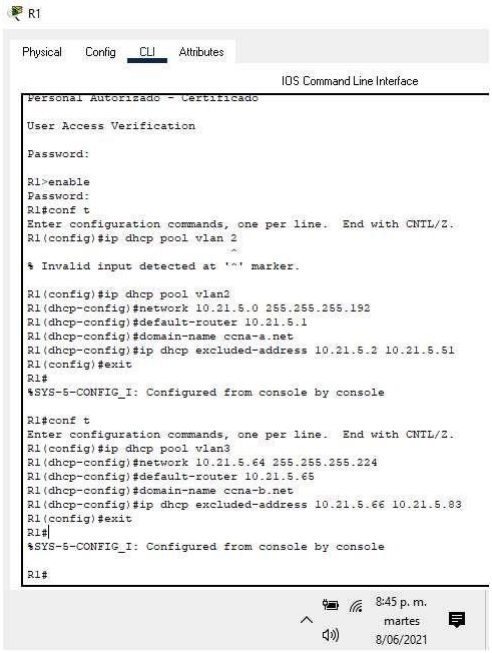


Ilustración 24. Configuración IPv4 DHCP para VLAN 2 y VLAN3

Paso 2: Configurar los servidores: Configure los equipos host PC-A y PC-B para que utilicen DHCP para IPv4 y asigne estáticamente las direcciones IPv6 GUA y Link Local. Después de configurar cada servidor, registre las configuraciones de red del host con el comando **ipconfig /all**.

PC-A Network Configuración	
Descripción	Usando el Comando “**ipconfig /all”**
Dirección física	0005.5EE3.A608
Dirección IP	10.21.5.52
Máscara de subred	255.255.255.192
Gateway predeterminado	10.21.5.1
Gateway predeterminado IPv6	FE80::1

Tabla 8. Configuración Red de PC-A

PC-B Network Configuración	
Descripción	Usando el Comando “**ipconfig /all”**
Dirección física	0090.21CD.5478
Dirección IP	10.21.5.84
Máscara de subred	255.255.255.224
Gateway predeterminado	10.21.5.65
Gateway predeterminado IPv6	FE80::1

Tabla 9. Configuración Red de PC-B

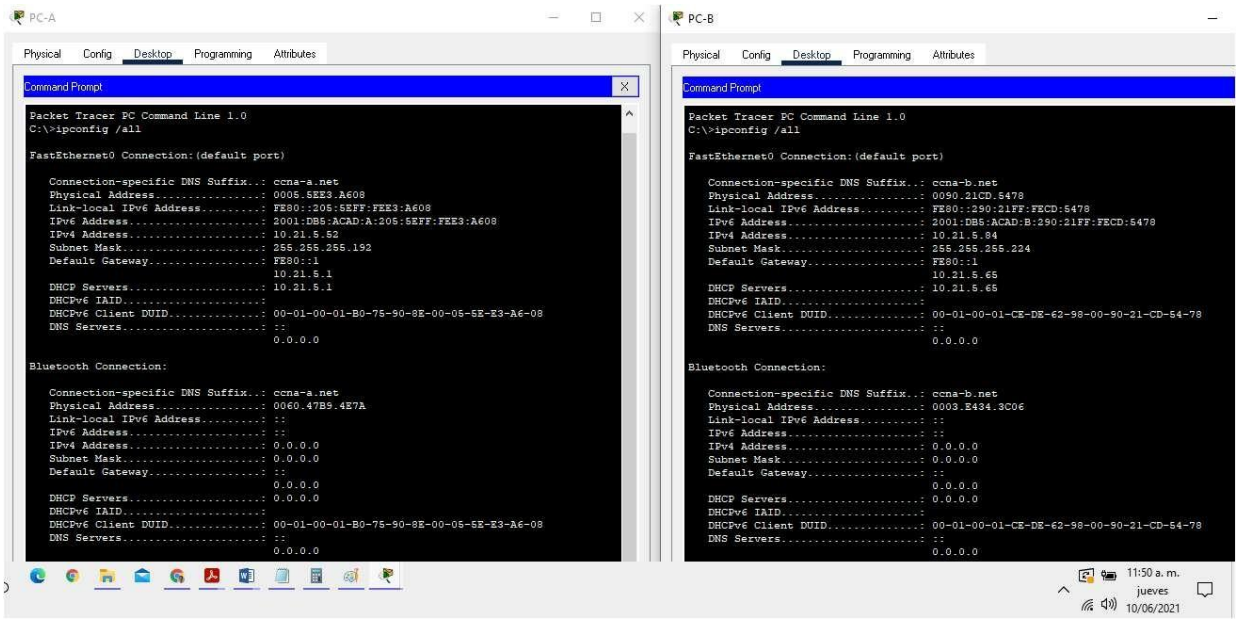


Ilustración 25. Configuración Red de PC-A y PC-B con comando “ipconfig /all”

Parte 4: 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:

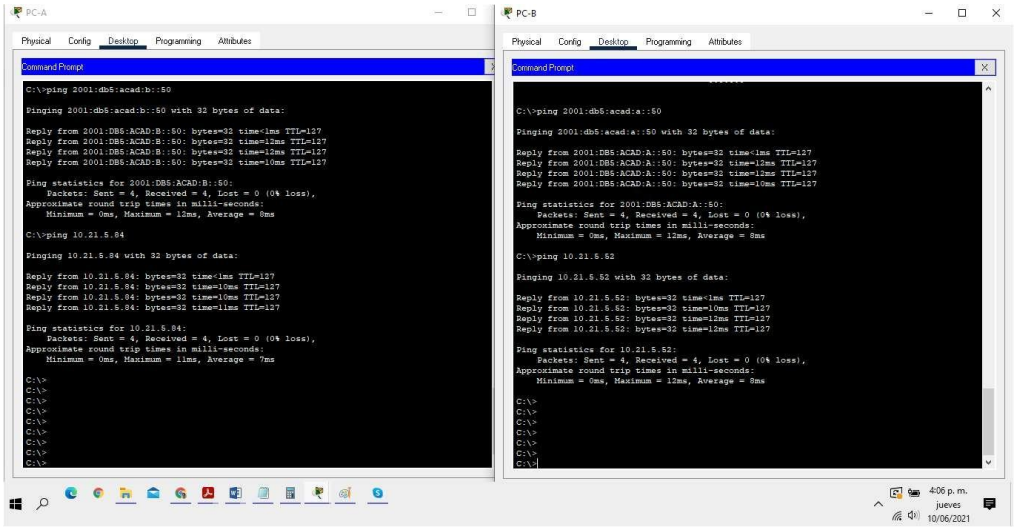


Ilustración 26. Uso del comando ping con IPv4 y IPv6 desde PC-A a PC-B y viceversa

Desde	A	de Internet	Dirección IP	Resultados Ping
PC-A	R1, G0/1.2	Dirección	10.21.5.1	Pérdidas 0%
		IPv6	2001:db5:acad:a::1	Pérdidas 0%
	R1, G0/1.3	Dirección	10.21.5.65	Pérdidas 0%
		IPv6	2001:db5:acad:b::1	Pérdidas 0%
	R1, G0/1.4	Dirección	10.21.5.97	Pérdidas 0%
		IPv6	2001:db5:acad:c::1	Pérdidas 0%
	S1, Vlan 4	Dirección	10.21.5.98	Pérdidas 0%
		IPv6	2001:db5:acad:c::98	**Pérdidas 100%**
	S2, Vlan 4	Dirección	10.21.5.99	Pérdidas 0%
		IPv6	2001:db5:acad:c::99	**Pérdidas 100%**
	PC-B	Dirección	10.21.5.84	Pérdidas 0%
		IPv6	2001:db5:acad:b::50	Pérdidas 0%
	R1 Bucle 0	Dirección	209.165.201.1	Pérdidas 0%
		IPv6	2001:db5:acad:209::1	Pérdidas 0%
PC-B	R1 Bucle 0	Dirección	209.165.201.1	Pérdidas 0%
		IPv6	2001:db5:acad:209::1	Pérdidas 0%
	R1, G0/1.2	Dirección	10.21.5.1	Pérdidas 0%
		IPv6	2001:db5:acad:a::1	Pérdidas 0%
	R1, G0/1.3	Dirección	10.21.5.65	Pérdidas 0%
		IPv6	2001:db5:acad:b::1	Pérdidas 0%
	R1, G0/1.4	Dirección	10.21.5.97	Pérdidas 0%
		IPv6	2001:db5:acad:c::1	Pérdidas 0%
	S1, Vlan 4	Dirección	10.21.5.98	Pérdidas 0%
		IPv6	2001:db5:acad:c::98	**Pérdidas 100%**
	S2, Vlan 4	Dirección	10.21.5.99	Pérdidas 0%
		IPv6	2001:db5:acad:c::99	**Pérdidas 100%**

Tabla 10. Conectividad de extremo a extremo desde PC-A y PC-B

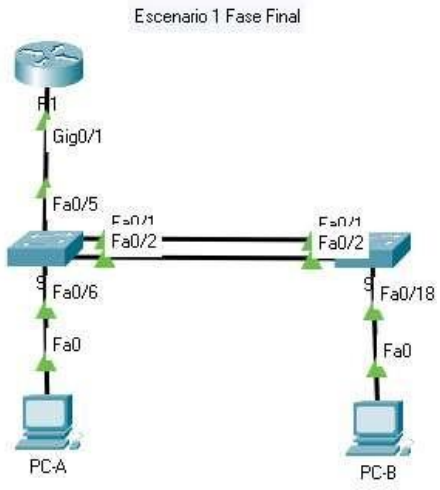


Ilustración 27.Esquema general en packet Tracer escenario 1

Escenario 2

Topología

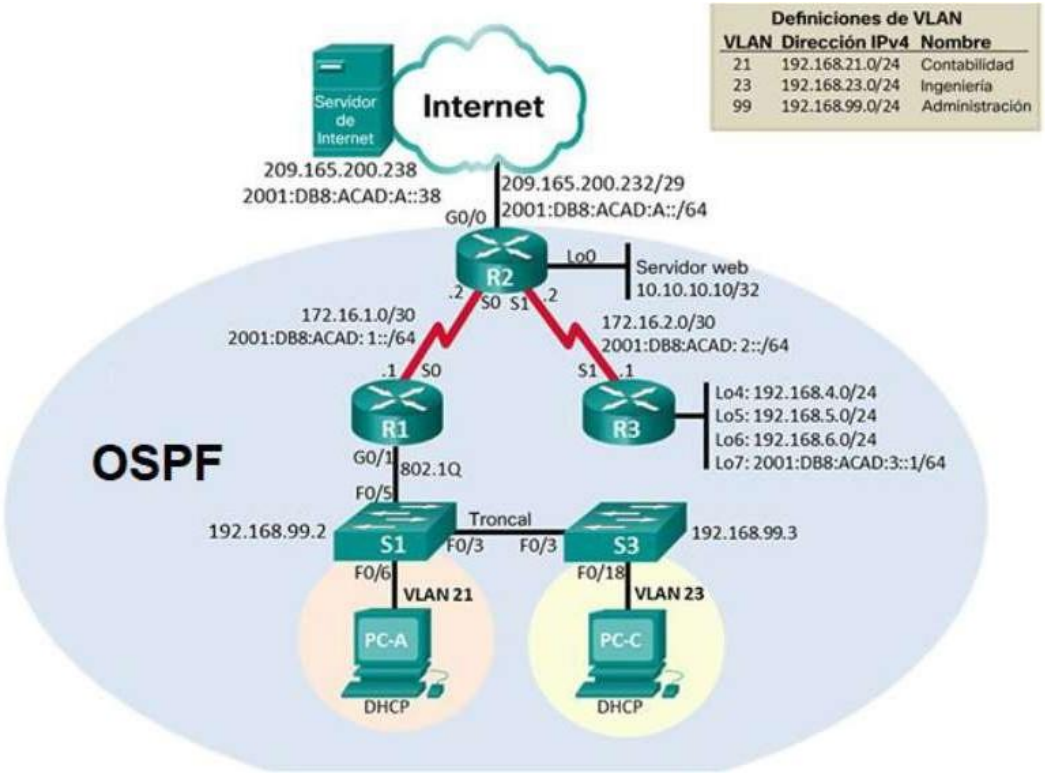


Ilustración 28. Topología general del escenario 2

Parte 1: Inicializar dispositivos

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

Nota, comandos utilizados e imágenes pertinentes: Se procede a eliminar las configuraciones de inicio y se cargan de nuevo los dispositivos.

Elemento o tarea de configuración	Especificación o comando IOS
Eliminar el archivo startup-config de todos los routers	Router>enable Router#erase startup-config Erasing the nvram filesystem will remove all configuration files! Continue? [confirm] [OK] Erase of nvram: complete %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram Router#reload Proceed with reload? [confirm]……..
Volver a cargar todos los routers	
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Switch>enable Switch#erase startup-config Erasing the nvram filesystem will remove all configuration files! Continue? [confirm] [OK] Erase of nvram: complete %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram Switch#delete vlan.dat Delete filename [vlan.dat]? Delete flash:/vlan.dat? [confirm] %Error deleting flash:/vlan.dat (No such file or directory) Switch#reload Proceed with reload? [confirm] C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(25r) FX, RELEASE SOFTWARE (fc4) Cisco WS-C2960-24TT (RC32300) processor (revision C0) with 21039K bytes of memory. 2960-24TT starting..... Loading "flash:/2960-lanbasek9-mz.150-2.SE4.bin"... ################################ [OK] Switch#dir flash Directory of flash:/ 1 -rw- 4670455 <no date> 2960-lanbasek9-mz.150-2.SE4.bin 64016384 bytes total (59345929 bytes free)
Volver a cargar ambos switches	
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	

Tabla 11. Tareas y comandos de IOS del paso 1 parte 1

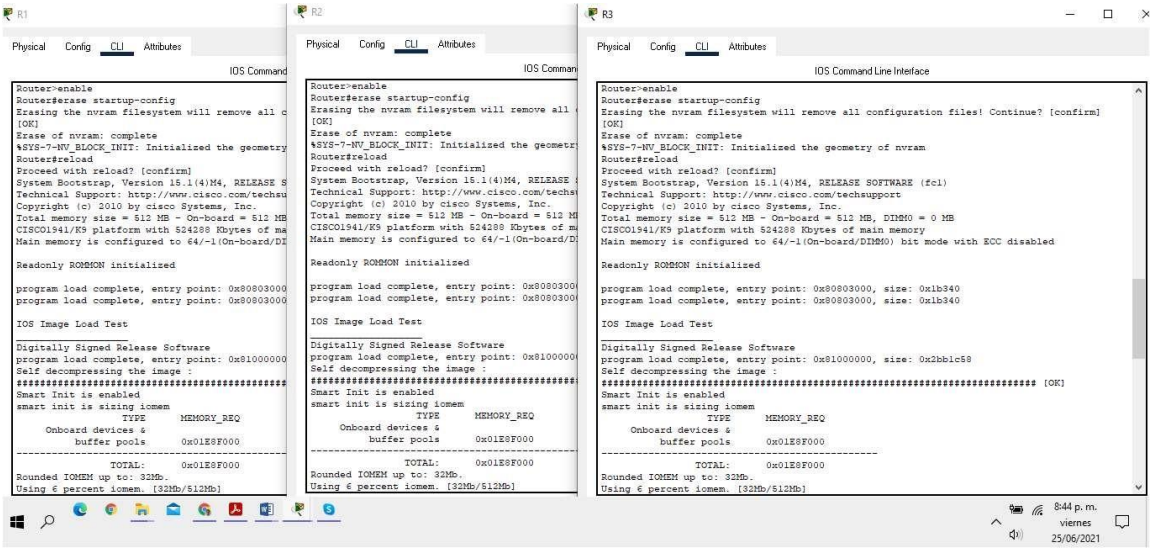


Ilustración 29. Inicialización y recarga de los Routers

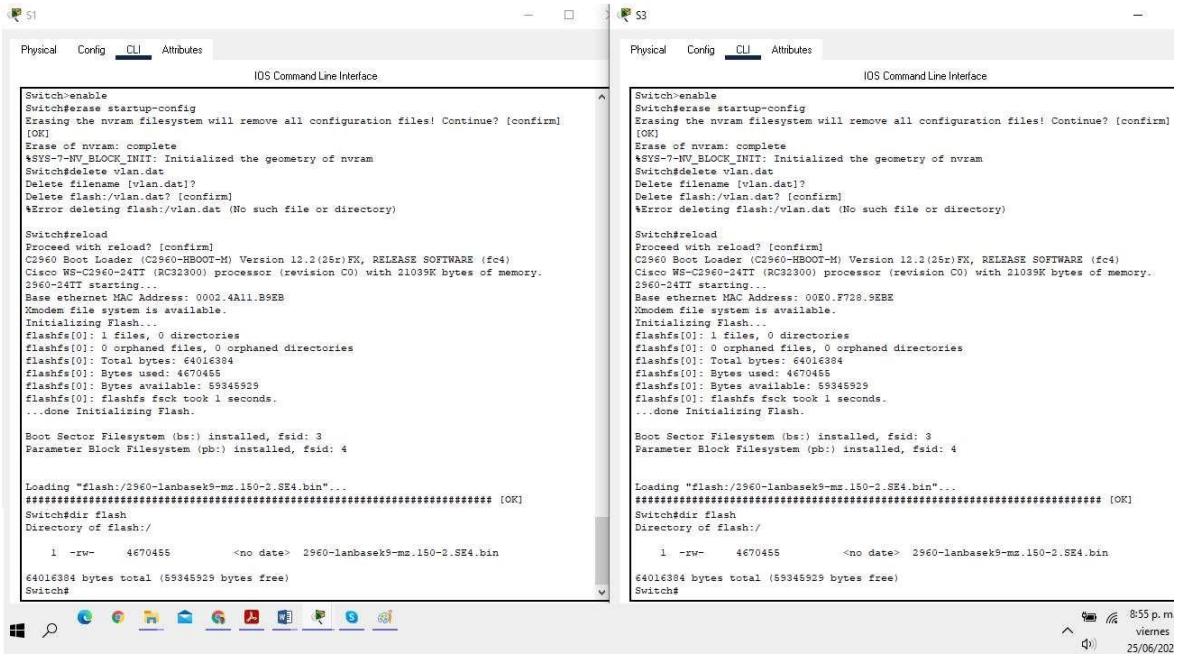


Ilustración 30. Inicialización y recarga de los Switchs

Parte 2: Configurar los parámetros básicos de los dispositivos

Paso 1: Configurar la computadora de Internet

Nota, comandos utilizados e imágenes pertinentes: Las tareas de configuración del servidor de Internet incluyen lo siguiente (para obtener información de las direcciones IP, consulte la topología).

Elemento o tarea de configuración	Especificación o comando IOS
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 /64
Gateway predeterminado IPv6	2001:DB8:ACAD:2::1

Tabla 12. Tareas y comandos de IOS paso1 parte 2, Computadora internet

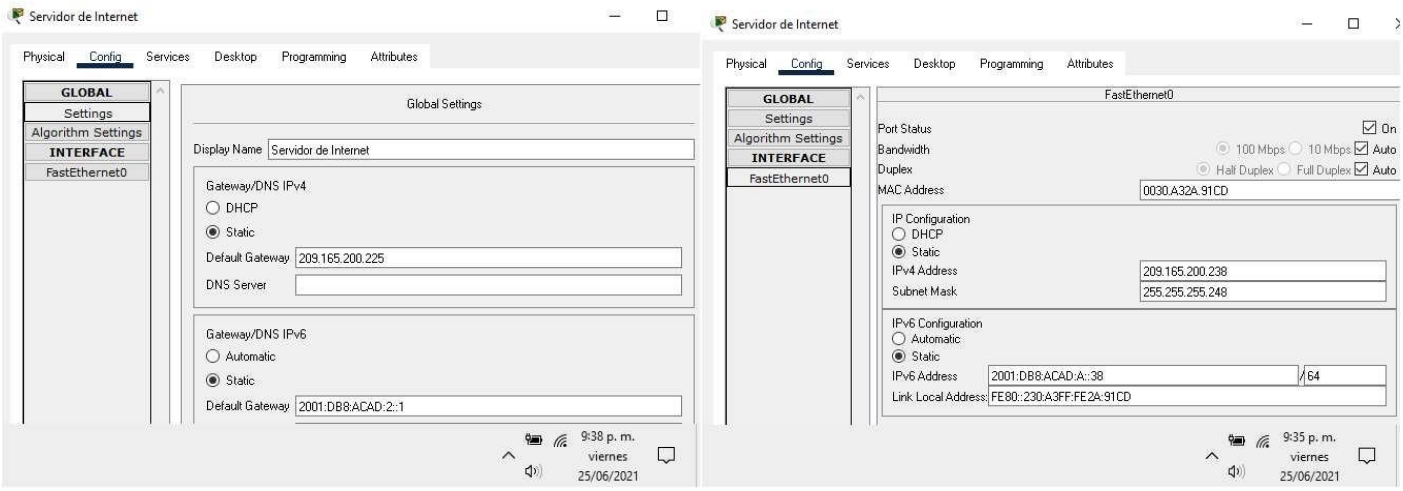


Ilustración 31. Configuración estática IPv4 - IPv6 de Servidor Internet

Paso 2: Configurar R1

Nota, comandos utilizados e imágenes pertinentes: Las tareas de configuración para R1 son las siguientes. Todavía no configure G0/1.

Elemento o tarea de configuración	Especificación o Comando IOS	
Desactivar la búsqueda DNS	Router>enable Router#conf t Router(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	cisco	R1(config)#line console 0 R1(config-line)#password cisco R1(config-line)#login R1(config-line)#exit
Contraseña de acceso Telnet	cisco	R1(config)#line vty 0 4 R1(config-line)#password cisco R1(config-line)#login R1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption	
Mensaje MOTD	Se prohíbe el acceso no autorizado	R1(config)#banner motd #Se prohibe el acceso no autorizado.#
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)#int s0/0/0 R1(config-if)#description R1 conexion R2 R1(config-if)#ip add 172.16.1.1 255.255.255.252 R1(config-if)#ipv6 add 2001:db8:acad:1::1/64 R1(config-if)#clock rate 128000 R1(config-if)#no sh %LINK-5-CHANGED: Interface Serial0/0/0, changed state to down 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 %Default route without gateway, if not a point-to-point interface, may impact performance R1(config)#ipv6 route ::/0 s0/0/0 R1(config-line)#exit

Tabla 13. Tareas y comandos de IOS paso2 parte 2, Router R1

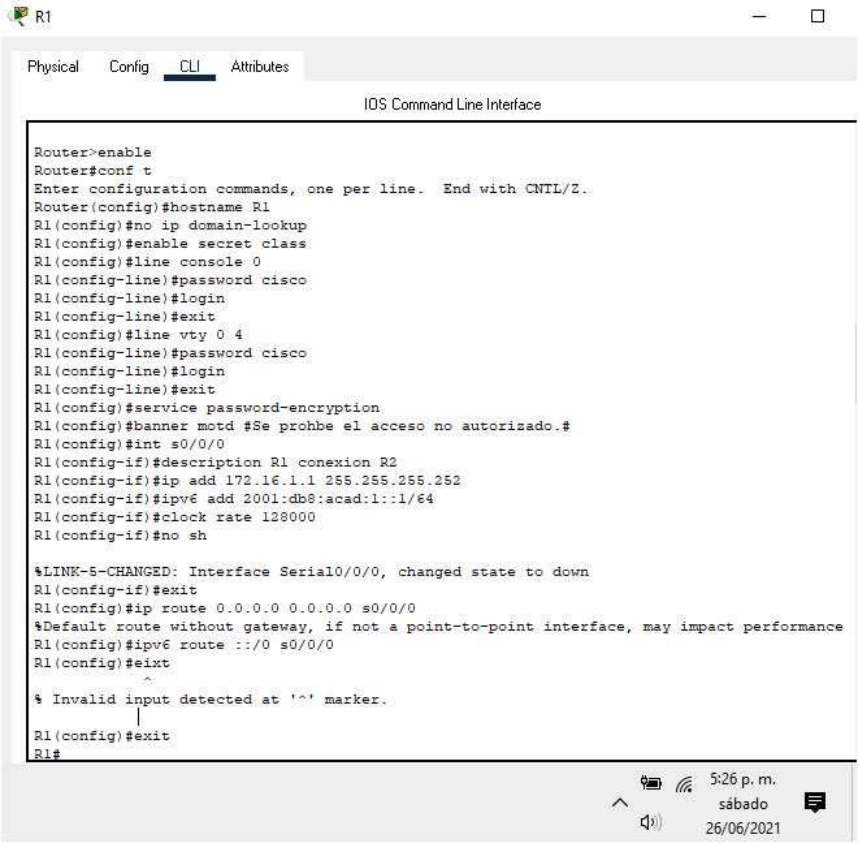


Ilustración 32. Configuración referente a la tabla 13 Router 1

Paso 3: Configurar R2

Nota, comandos utilizados e imágenes pertinentes: Las tareas de configuración para R2 son las siguientes.

En la habilitación del HTTP para este Router, se encuentra que la herramienta Packet Tracer no soporta o no admite el comando "ip http server", por lo que no es posible configurarlo.

Elemento o tarea de configuración	Especificación o Comando IOS	
Desactivar la búsqueda DNS	Router>enable Router#conf t Router(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 R2(config-line)#exit
Contraseña de acceso Telnet	cisco	R2(config)#line vty 0 4 R2(config-line)#password cisco R2(config-line)#login R2(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R2(config)#service password-encryption	
Habilitar el servidor HTTP	**Packet Tracert no admite el comando "ip HTTP server"** **R2(config)#ip http server** **% Invalid input detected at '^' marker.**	
Mensaje MOTD	Se prohíbe el acceso no autorizado	R2(config)#banner motd #Se prohibe 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. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz	R2(config)#int s0/0/0 R2(config-if)#description R2 conexion R1 R2(config-if)#ip add 172.16.1.2 255.255.255.252 R2(config-if)#ipv6 add 2001:db8:acad:1::2/64 R2(config-if)#clock rate 128000 R2(config-if)#no sh %LINK-5-CHANGED: Interface Serial0/0/0, changed state to down R2(config-if)#exit
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 conexion R3 R2(config-if)#ip add 172.16.2.2 255.255.255.252 R2(config-if)#ipv6 add 2001:DB8:ACAD:2::2/64 R2(config-if)#clock rate 128000 R2(config-if)#no sh %LINK-5-CHANGED: Interface Serial0/0/1, changed state to down R2(config-if)#exit

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 conexion Servidor Internet R2(config-if)#ip add 209.165.200.233 255.255.255.248 R2(config-if)#ipv6 add 2001:DB8:ACAD:A::1/64 R2(config-if)#no sh R2(config-if)# %LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
Interfaz loopback 0 (servidor web simulado)	Establecer la descripción. Establezca la dirección IPv4	R2(config-if)#int loopback 0 R2(config-if)# %LINK-5-CHANGED: Interface Loopback0, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up R2(config-if)#description R2 conexion servidor web simulado R2(config-if)#ip add 10.10.10.10 255.255.255.255 R2(config-if)#exit R2(config)#end R2#
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 R2(config)#exit

Tabla 14. Tareas y comandos de IOS paso 3 parte 2, Router R2

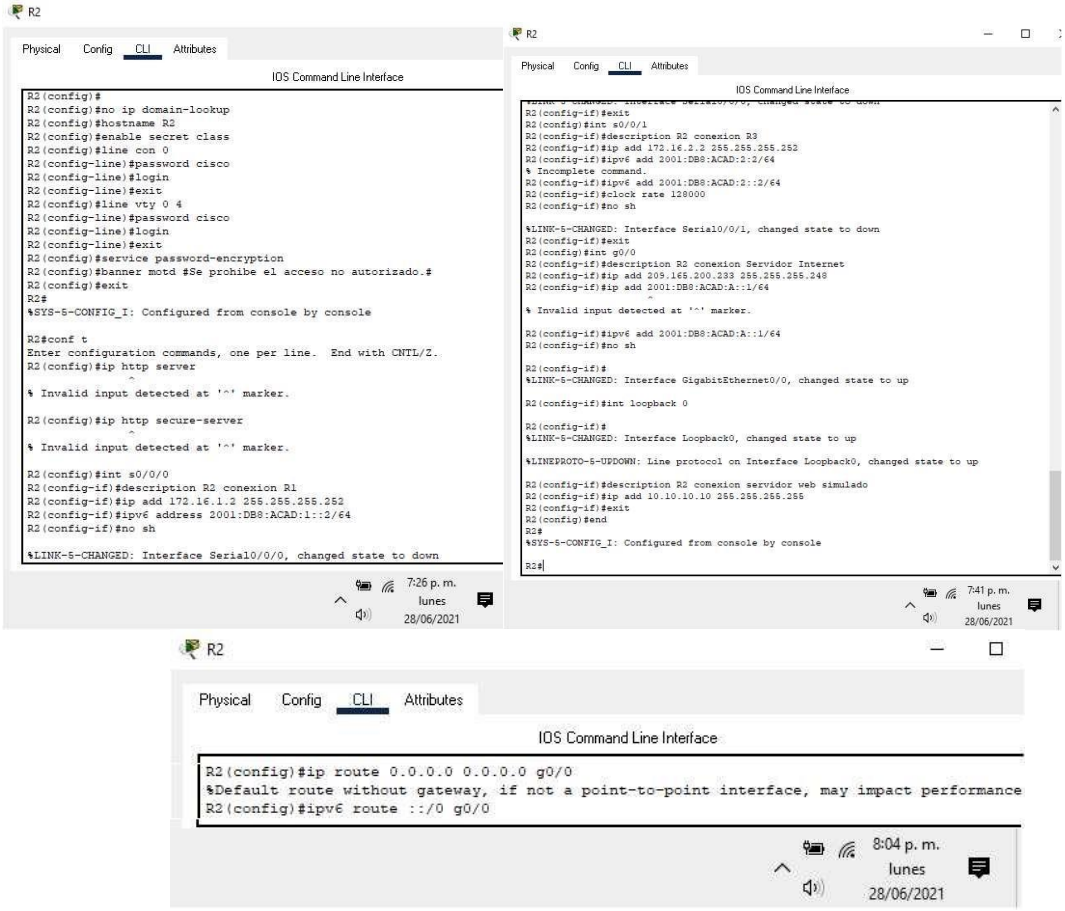


Ilustración 33. Configuración referente a la tabla 14 Router 2

Paso 4: Configurar R3

Nota, comandos utilizados e imágenes pertinentes: Las tareas de configuración para R3 son las siguientes.

Elemento o tarea de configuración	**Especificación o comando IOS**	
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup	
Nombre del router	R1	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)#password cisco R3(config-line)#login R3(config-line)#exit
Contraseña de acceso Telnet	cisco	R3(config)#line vty 0 4 R3(config-line)#password cisco R3(config-line)#login R3(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R3(config)#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 R3 conexion R2 R3(config-if)#ip add 172.16.2.1 255.255.255.252 R3(config-if)#ipv6 add 2001:DB8:ACAD:2::1/64 R3(config-if)#no sh %LINK-5-CHANGED: Interface Serial0/0/1, changed state to down R3(config-if)#exit
Interfaz loopback 4	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.	R3(config)#int 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)#description Interfaz Virtual Pruebas # 4 R3(config-if)#ip add 192.168.4.1 255.255.255.0 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)#description Interfaz Virtual Pruebas # 5 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)#description Interfaz Virtual Pruebas # 6 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.	R3(config)#int loopback 7 R3(config-if)# %LINK-5-CHANGED: Interface Loopback7, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback7, changed state to up R3(config-if)#description Interfaz Virtual Pruebas # 7 R3(config-if)#ipv6 add 2001:DB8:ACAD:3::1/64 R3(config-if)#exit
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 R3(config)#	

Tabla 15. Tareas y comandos de IOS paso 4 parte 2, Router R3

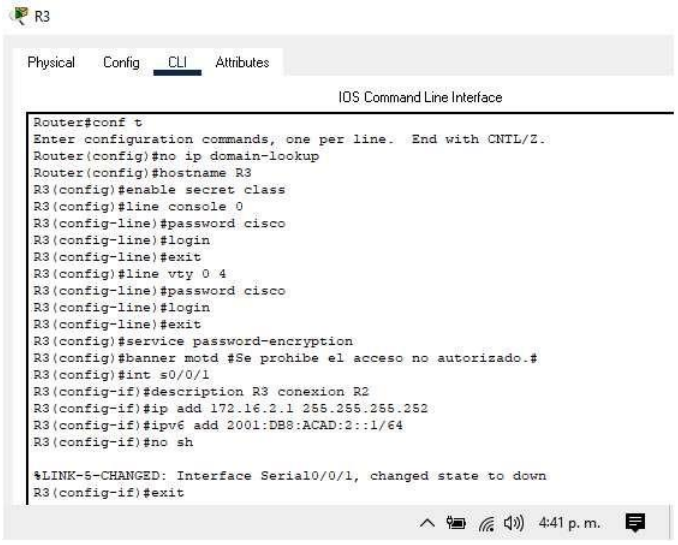


Ilustración 34. Configuración referente a la tabla 15 Router 3

Ilustración 35. Configuración referente a la tabla 15 Router 3

Paso 5: Configurar S1

Nota, comandos utilizados e imágenes pertinentes: Las tareas de configuración para S1 son las siguientes.

Elemento o tarea de configuración	**Especificación o comando IOS**	
Desactivar la búsqueda DNS	Switch(config)#no ip domain-lookup	
Nombre del switch	S1	Switch(config)#hostname S1
Contraseña de exec privilegiado cifrada	class	S1(config)#enable secret class

Contraseña de acceso a la consola	cisco	S1(config)#line console 0 S1(config-line)#password cisco S1(config-line)#login S1(config-line)#exit
Contraseña de acceso Telnet	cisco	S1(config)#line vty 0 4 S1(config-line)#password cisco S1(config-line)#login S1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption	
Mensaje MOTD	Se prohíbe el acceso no autorizado.	S1(config)#banner motd #Se prohibe el acceso no autorizado.# S1(config)#exit

Tabla 16. Tareas y comandos de IOS paso 5 parte 2, Switch 1

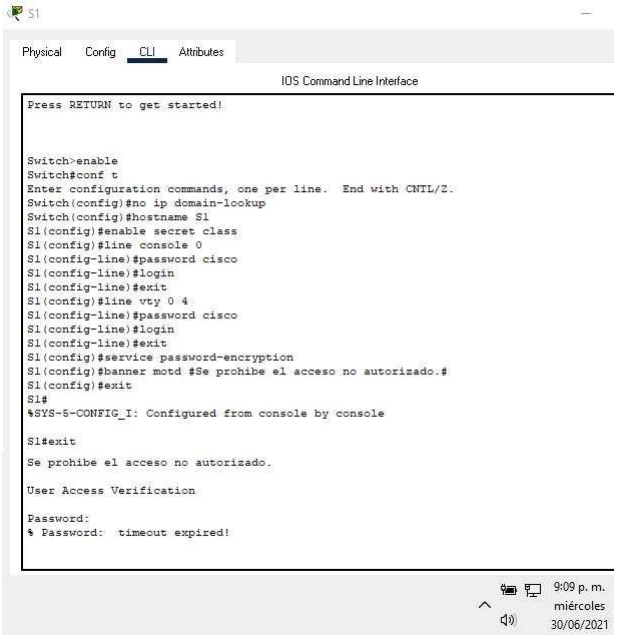


Ilustración 36. Configuración referente a la tabla 16 Switch 1

Paso 6: Configurar el S3

Nota, comandos utilizados e imágenes pertinentes: Las tareas de configuración para S3 son las siguientes.

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

Tabla 17. Tareas y comandos de IOS paso 6 parte 2, Switch 3

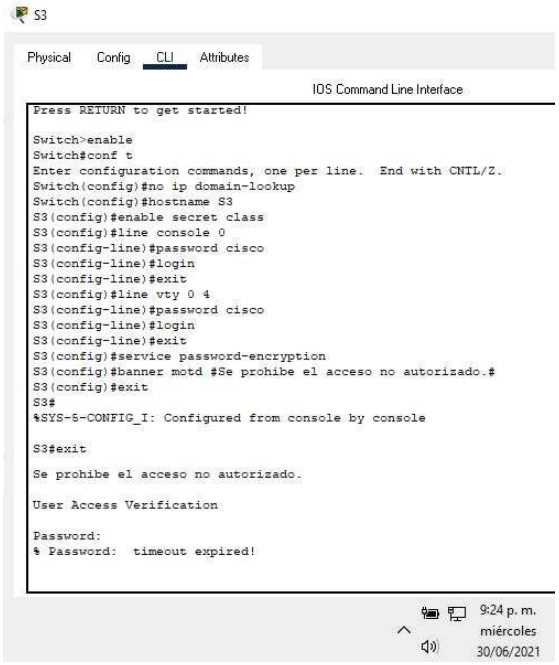


Ilustración 37. Configuración referente a la tabla 17 Switch 3

Paso 7: Verificar la conectividad de la red.

Nota, comandos utilizados e imágenes pertinentes: 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.

El ping realizado al Gateway predeterminado desde PC Internet, no tiene respuesta, esto debido a que se configura en el servidor, pero no hay equipos, redes o alguna otra instancia superior donde se tenga configurado este Gateway como dirección IP fija de un dispositivo o interface.

Desde	A	Dirección IP	Resultados Ping
R1	R2, S0/0/0	172.16.1.2	Ping 100% Satisfactorio
R2	R3, S0/0/1	172.16.2.1	Ping 100% Satisfactorio
PC de Internet	**Gateway predeterminado**	**209.165.200.225**	**No hay respuesta**

Tabla 18. Estado de conectividad entre dispositivos de la red

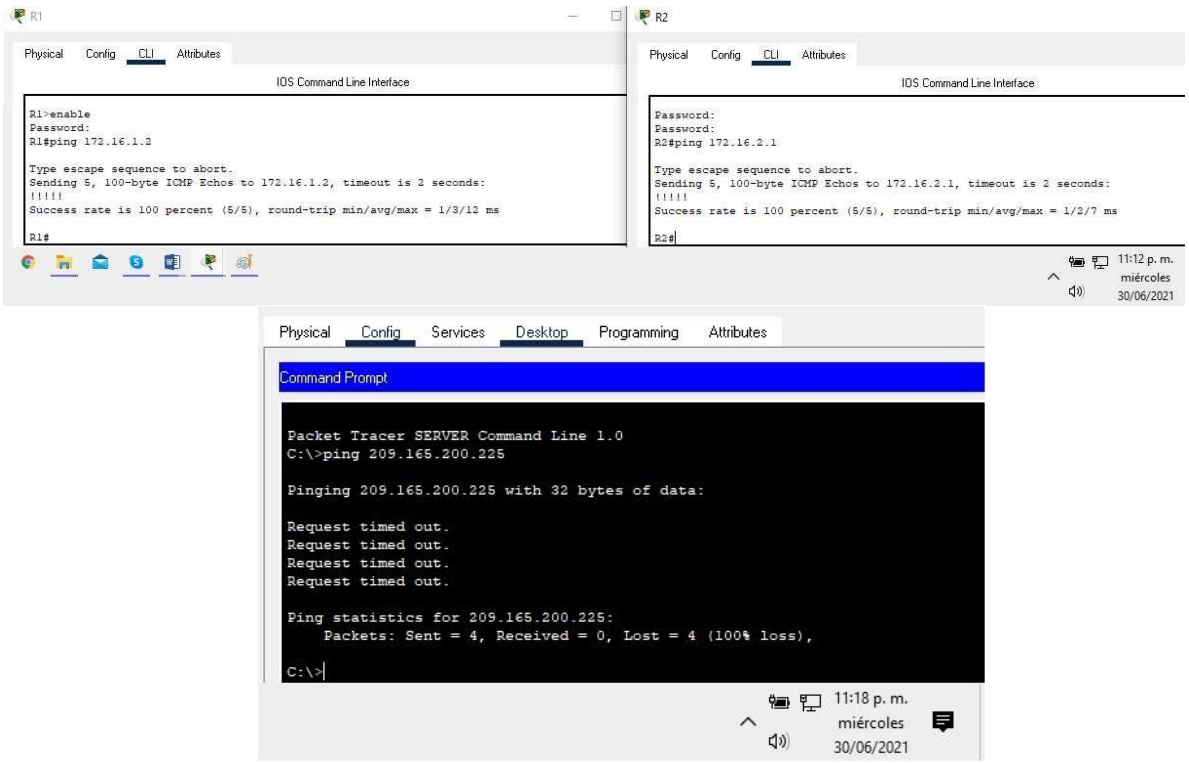


Ilustración 38. Verificación proceso tabla 18 entre Router y del PC internet a Gateway

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

Paso 1: Configurar S1

Nota, comandos utilizados e imágenes pertinentes: La configuración del S1 incluye las siguientes tareas

Elemento o tarea de configuración	Especificación	Comandos IOS
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 S1(config-vlan)#exit
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)# %LINK-5-CHANGED: Interface Vlan99, changed state to up S1(config-if)#ip add 192.168.99.2 255.255.255.0
Asignar el gateway predeterminado	Asigne la primera dirección IPv4 de la subred como el gateway predeterminado.	S1(config-if)#ip default-gateway 192.168.99.1 S1(config)#exit
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)# %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up S1(config-if)#switchport trunk native vlan 1 S1(config-if)#exit
Forzar el enlace troncal en la interfaz F0/5	Utilizar la red VLAN 1 como VLAN nativa	S1(config)#int f0/5 S1(config-if)#switchport mode trunk S1(config-if)# %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to down %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to up S1(config-if)#switchport trunk native vlan 1 S1(config-if)#exit
Configurar el resto de los puertos como	Utilizar el comando interface range	S1(config)#int range f0/1-2, f0/4, f0/6-24, g0/1-2 S1(config-if-range)#switchport mode access S1(config-if-range)#exit

puertos de acceso		
Asignar F0/6 a la VLAN 21	S1(config)#int f0/6 S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 21 S1(config-if)#exit	
Apagar todos los puertos sin usar	S1(config)#int range f0/1-2, f0/4, f0/7-24, g0/1-2 S1(config-if-range)#sh %LINK-5-CHANGED: Interface FastEthernet0/1-2, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/4, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/7-24, changed state to administratively down %LINK-5-CHANGED: Interface GigabitEthernet0/1-2, changed state to administratively down S1(config-if-range)#exit	

Tabla 19. Configuración Troncales y Vlans en S1

Ilustración 39. Configuración referente a la tabla 19 con S1

Paso 2: Configurar el S3

Nota, comandos utilizados e imágenes pertinentes: La configuración del S3 incluye las siguientes tareas.

Elemento o tarea de configuración	Especificación	Comandos IOS
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)#int vlan 99 S3(config-if)# %LINK-5-CHANGED: Interface Vlan99, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up S3(config-if)#ip add 192.168.99.3 255.255.255.0 S3(config-if)#exit
Asignar el gateway predeterminado.	Asignar la primera dirección IP en la subred como gateway predeterminado.	S3(config)#ip default-gateway 192.168.99.1 S3(config)#exit
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)#exit
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range	S3(config)#int range f0/1-2, f0/4-24, g0/1-2 S3(config-if-range)#switchport mode access S3(config-if-range)#exit
Asignar F0/18 a la VLAN 21	S3(config)#int f0/18 S3(config-if)#switchport access vlan 23 S3(config-if)#exit	
Apagar todos los puertos sin usar	S3(config)#int range f0/1-2, f0/4-17, f0/19-24, g0/1-2 S3(config-if-range)#sh %LINK-5-CHANGED: Interface FastEthernet0/1-2, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/4-17, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/19-24, changed state to administratively down %LINK-5-CHANGED: Interface GigabitEthernet0/1-2, changed state to administratively down S3(config-if)#exit	

Tabla 20. Configuración Troncales y Vlans en S3

Ilustración 40. Configuración referente a la tabla 20 con S3

Paso 3: Configurar R1

Nota, comandos utilizados e imágenes pertinentes: Las tareas de configuración para R1 incluyen las siguientes.

Elemento o tarea de configuración	Especificación	Comandos IOS
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)# %LINK-5-CHANGED: Interface GigabitEthernet0/1.21, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.21, changed state to up R1(config-subif)#encapsulation dot1Q 21 R1(config-subif)#description LAN de Contabilidad R1(config-subif)#ip add 192.168.21.1 255.255.255.0 R1(config-subif)#no sh R1(config-subif)#exit
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)# %LINK-5-CHANGED: Interface GigabitEthernet0/1.23, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.23, changed state to up R1(config-subif)#encapsulation dot1Q 23 R1(config-subif)#ip add 192.168.23.1 255.255.255.0 R1(config-subif)#description LAN de Ingeniera R1(config-subif)#no sh R1(config-subif)#exit
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)#int g0/1.99 R1(config-subif)# %LINK-5-CHANGED: Interface GigabitEthernet0/1.99, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.99, changed state to up R1(config-subif)#encapsulation dot1Q 99 R1(config-subif)#ip add 192.168.99.1 255.255.255.0 R1(config-subif)#description LAN de Administracion R1(config-subif)#no sh R1(config-subif)#exit
Activar la interfaz G0/1	R1(config)#int g0/1 R1(config-if)#no sh R1(config-if)#exit	

Tabla 21. Configuracion de subinterfaces 802.1Q con las Vlan en R1

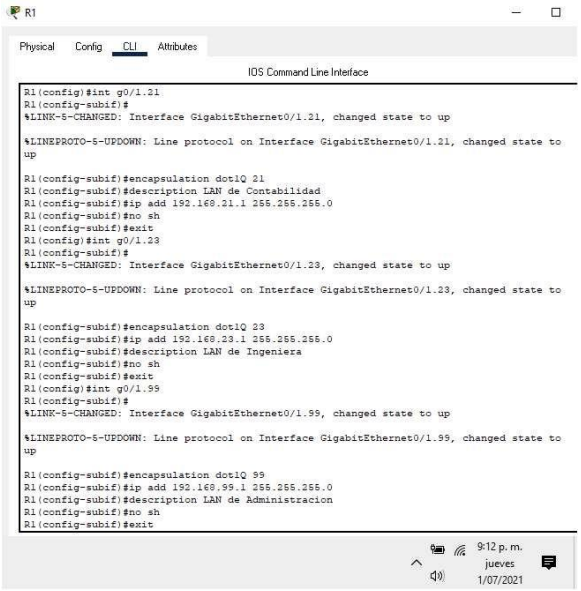


Ilustración 41. Configuracion referente a la tabla 21 con R1

Paso 4: Verificar la conectividad de la red

Nota, comandos utilizados e imágenes pertinentes: 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	A	Direccion IP	Reaultado de Ping
S1	R1, dirección VLAN 99	192.168.99.1	Ping 100% Satisfactorio
S3	R1, dirección VLAN 99	192.168.99.1	Ping 100% Satisfactorio
S1	R1, dirección VLAN 21	192.168.21.1	Ping 100% Satisfactorio
S3	R1, dirección VLAN 23	192.168.23.1	Ping 100% Satisfactorio

Tabla 22. Estado de conectividad entre dispositivos de la red y Vlan

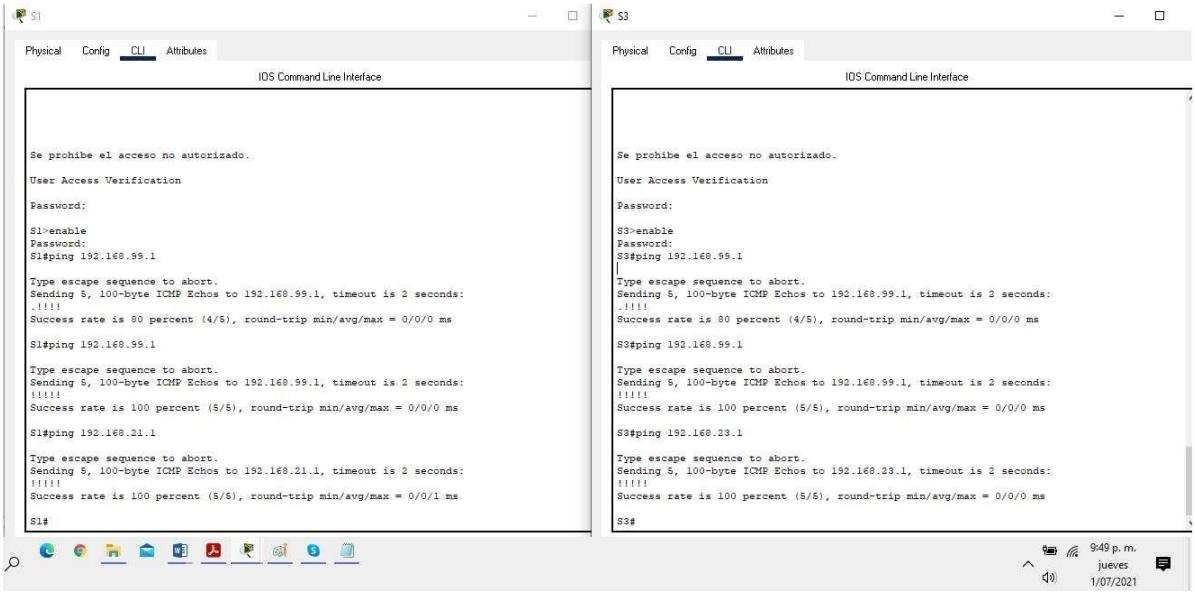


Ilustración 42. Verificación proceso tabla 22 entre Switchs y Router 1 con las Vlan

Parte 4: Configurar el protocolo de routing dinámico OSPF

Paso 1: Configurar OSPF en el R1

Nota, comandos utilizados e imágenes pertinentes: Las tareas de configuración para R1 incluyen las siguientes.

El protocolo OSPF permite a los dispositivos encontrar una vía más corta para su comunicación.

Se habilita el Router para manejar direcciones IPv6 con el comando “ipv6 unicast-routing”

Elemento o tarea de configuración	Especificación	Comandos IOS
Habilitar el routing IPv6 en el router	R1(config)#ipv6 unicast-routing	
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 R1(config-router)#exit
Establecer todas las interfaces LAN como pasivas	R1(config)#router ospf 1 R1(config-router)#passive-interface g0/1.21 R1(config-router)#passive-interface g0/1.23 R1(config-router)#passive-interface g0/1.99 R1(config-router)#exit	
Desactive la sumarización automática	R1(config)#router rip R1(config-router)#no auto-summary R1(config-router)#exit	

Tabla 23. Configuracion OSPF en R1

Ilustración 43. Configuracion OSPF referente a la tabla 23 en R1

Paso 2: Configurar OSPF en el R2

Nota, comandos utilizados e imágenes pertinentes: La configuración del R2 incluye las siguientes tareas.

Se habilita el Router para manejar direcciones IPv6 con el comando “ipv6 unicast-routing”

Elemento o tarea de configuración	Especificación	Comandos IOS
Habilitar el routing IPv6 en el router	R2(config)#ipv6 unicast-routing	
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 10.10.10.10 0.0.0.0 area 0 R2(config-router)#network 172.16.1.0 0.0.0.255 area 0 R2(config-router)# 00:04:40: %OSPF-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/0 from LOADING to FULL, Loading Done R2(config-router)#network 172.16.2.0 0.0.0.255 area 0
Establecer la interfaz LAN (loopback) como pasiva	R2(config-router)#passive-interface loopback 0 R2(config-router)#exit	

Desactive la sumarización automática	R2(config)#router rip R2(config-router)#no auto-summary R2(config-router)#exit R2(config)#

Tabla 24. Configuracion OSPF en R2

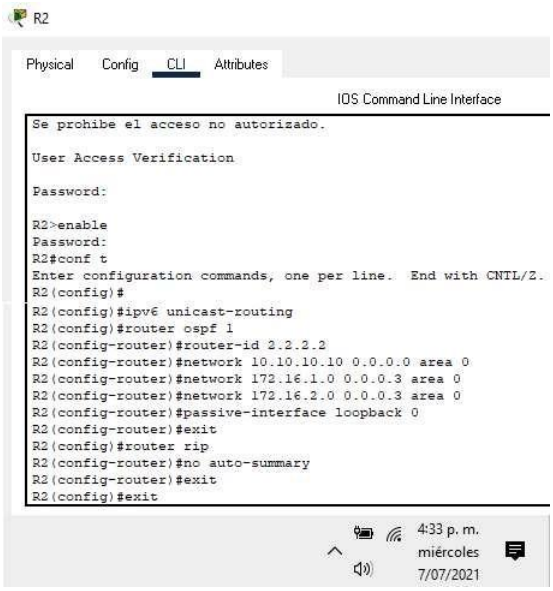


Ilustración 44. Configuracion OSPF referente a la tabla 24 en R2

Paso 3: Configurar OSPFv3 en R1, R2 y R3

Nota, comandos utilizados e imágenes pertinentes: La configuración del R1, R2 y R3 incluye las siguientes tareas.

Según guía indica R2 y R3, se decide realizar la configuración OSPFv3 en los 3 Routers R1, R2 y R3 y con cada interface de uso en cada uno.

Elemento o tarea de configuración	Comandos IOS
Configurar cada interface en uso con OSPFv3 en R1	R1(config)#int g0/1 R1(config-if)#ipv6 ospf 1 area 0 OSPFv3: No IPV6 enabled on this interface R1(config-if)#end R1(config)#int s0/0/0 R1(config-if)#ipv6 ospf 1 area 0 R1(config-if)# 04:39:07: %OSPFv3-5-ADJCHG: Process 1, Nbr 10.10.10.10 on Serial0/0/0 from LOADING to FULL, Loading Done R1(config-if)#exit
Configurar cada interface en uso con OSPFv3 en R2	R2(config)#int g0/0 R2(config-if)#ipv6 ospf 1 area 0 R2(config-if)#exit R2(config)#int s0/0/0 R2(config-if)#ipv6 ospf 1 area 0 R2(config-if)#exit R2(config)# 04:39:07: %OSPFv3-5-ADJCHG: Process 1, Nbr 192.168.99.1 on Serial0/0/0 from LOADING to FULL, Loading Done R2(config)#int s0/0/1 R2(config-if)#ipv6 ospf 1 area 0 R2(config-if)#exit R2(config)#exit
Habilitar el routing IPv6 en el router	R3(config)#ipv6 unicast-routing
Configurar cada interface en uso con OSPFv3 en R3	R3(config)#int s0/0/1 R3(config-if)#ipv6 ospf 1 area 0 R3(config-if)#exit R3(config)# 04:41:58: %OSPFv3-5-ADJCHG: Process 1, Nbr 10.10.10.10 on Serial0/0/1 from LOADING to FULL, Loading Done

Tabla 25. Configuracion Interfaces activas con OSPFv3 en R1, R2 y R3

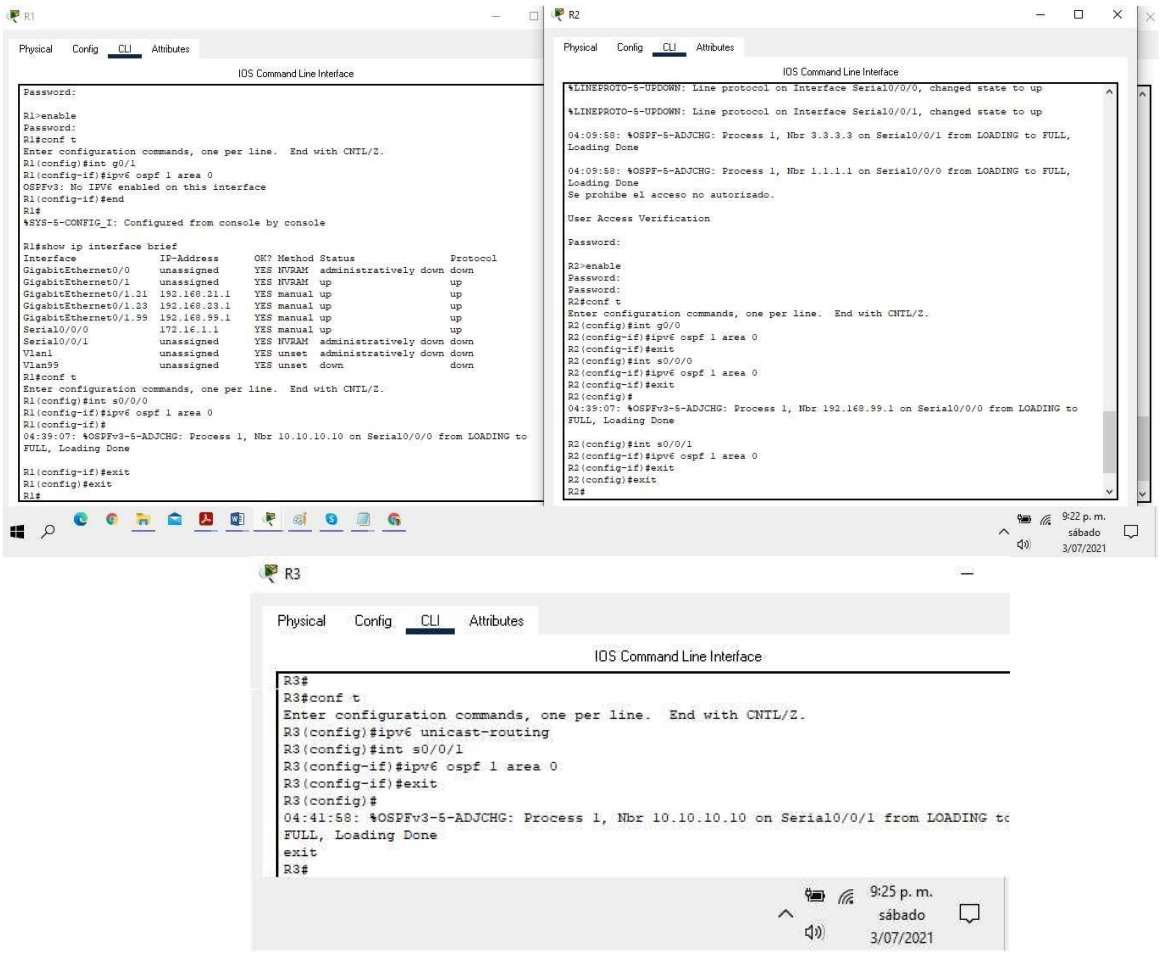


Ilustración 45. Configuracion referente a la tabla 25 con OSPFv3 en R1, R2 y R3

Paso 4: Configurar OSPF en el R3

Nota, comandos utilizados e imágenes pertinentes: La configuración del R3 incluye las siguientes tareas.

Se realiza la configuración adicional dado que en la guía el paso anterior no es claro, por lo que se configura también el OSPF para R3.

Elemento o tarea de configuración	Especificación	Comandos IOS
Habilitar el routing IPv6 en el router	R3(config)#ipv6 unicast-routing	
Configurar OSPF área 0	R3(config)#router ospf 1 R3(config-router)#router-id 3.3.3.3	
Anunciar las redes IPv4 conectadas directamente	R3(config-router)#network 172.16.2.0 0.0.0.3 area 0 R3(config-router)# 01:29:40: %OSPF-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Serial0/0/1 from LOADING to FULL, Loading Done R3(config-router)#network 192.168.4.0 0.0.0.255 area 0 R3(config-router)#network 192.168.5.0 0.0.0.255 area 0 R3(config-router)#network 192.168.6.0 0.0.0.255 area 0	
Establecer todas las interfaz de LAN IPv4 (loopback) como pasiva	R3(config-router)#passive-interface loopback 4 R3(config-router)#passive-interface loopback 5 R3(config-router)#passive-interface loopback 6 R3(config-router)#passive-interface loopback 7 R3(config-router)#exit	
Desactive la sumarización automática	R3(config)#router rip R3(config-router)#no auto-summary R3(config-router)#exit R3(config)#exit	

Tabla 26. Configuracion OSPF en R3

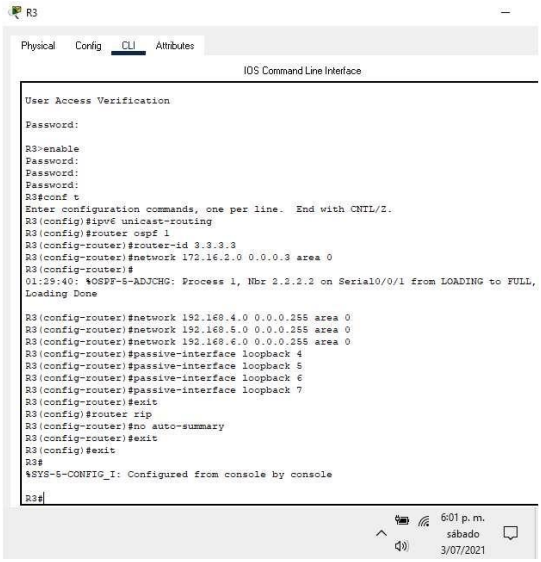


Ilustración 46. Configuracion OSPF referente a la tabla 26 en R3

Paso 5: Verificar la información de OSPF

Nota, comandos utilizados e imágenes pertinentes: Verifique que OSPF esté funcionando como se espera. Introduzca el comando de CLI adecuado para obtener la siguiente información.

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?	show ip ospf interface
¿Qué comando muestra solo las rutas OSPF?	show ip route ospf
¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	show run | sec router ospf

Tabla 27. Verificacion de información de OSPF

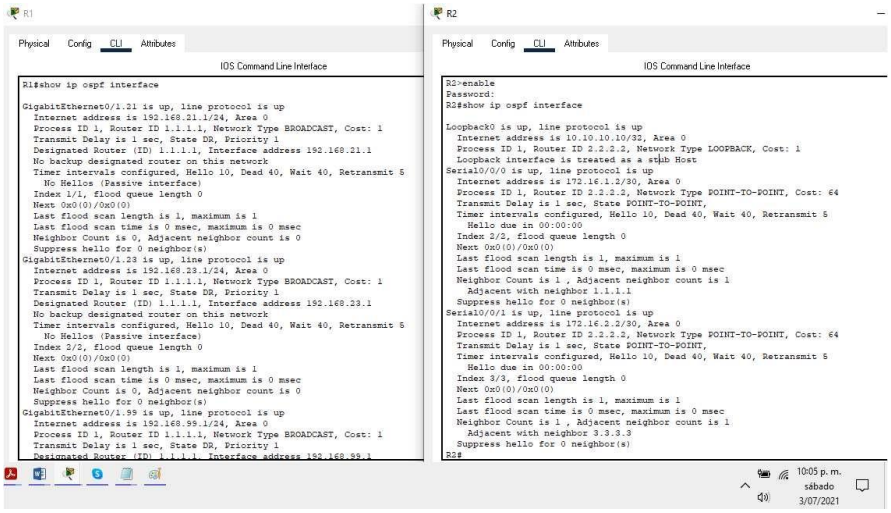


Ilustración 47. Verificacion comando "show ip ospf interface" en R1 y R2

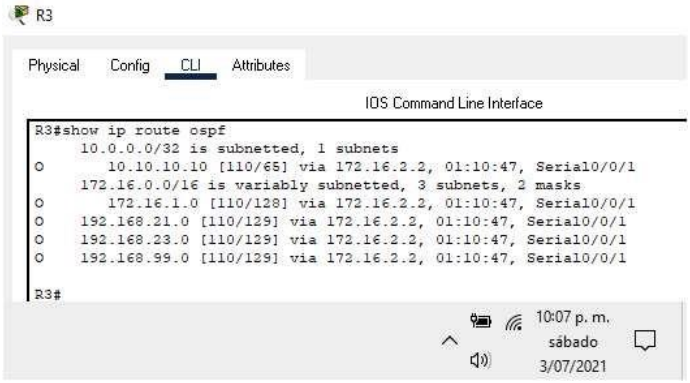


Ilustración 48. Verificacion comando "show ip route ospf" en R3

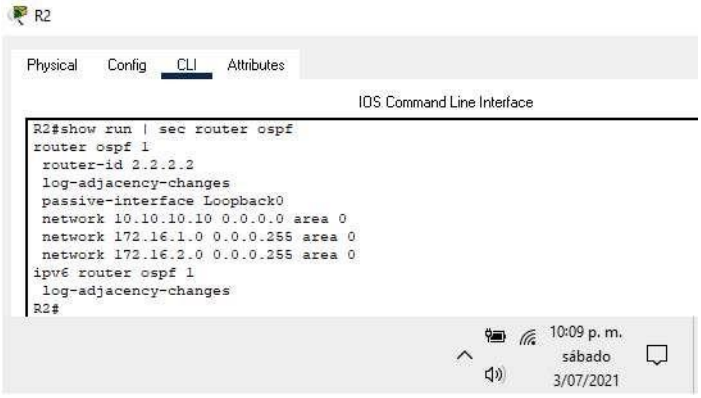


Ilustración 49. Verificacion comando "show run | sec router ospf" en R2

Parte 5: Implementar DHCP y NAT para IPv4

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

Nota, comandos utilizados e imágenes pertinentes: Las tareas de configuración para R1 incluyen las siguientes.

Elemento o tarea de configuración	Especificación	Comandos IOS
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)#network 192.168.21.0 255.255.255.0 R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com R1(dhcp-config)#default-router 192.168.21.1 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)#network 192.168.23.0 255.255.255.0 R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com R1(dhcp-config)#default-router 192.168.23.1 R1(dhcp-config)#exit

Tabla 28. Configuracion de R1 como servidor de DHCP para las VLAN 21 y 23

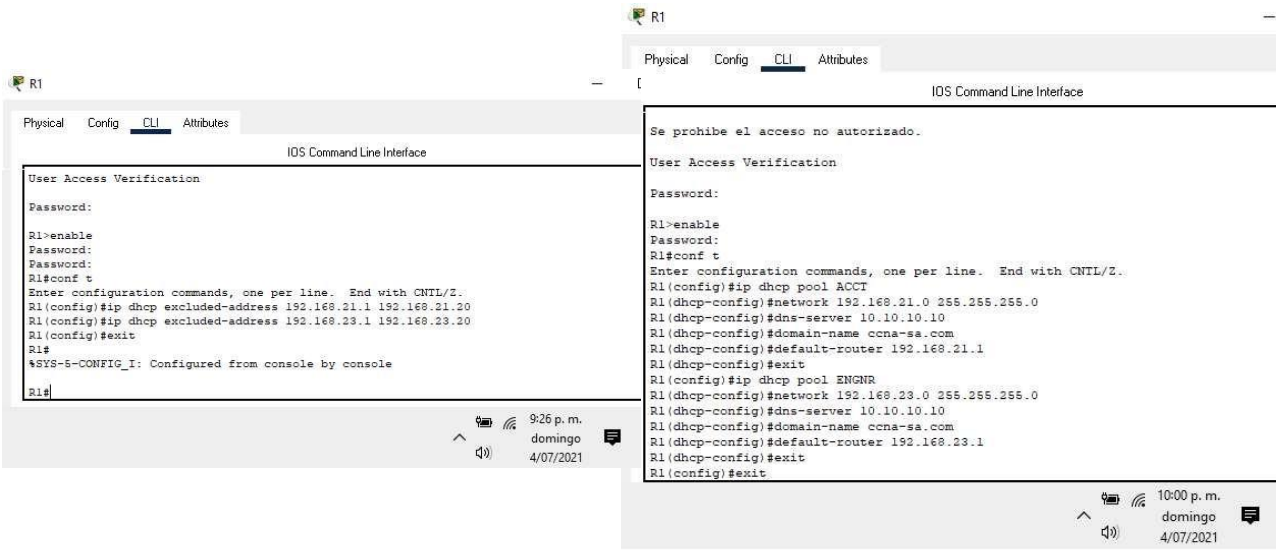


Ilustración 50. Verificacion de la tabla 28, R1 como DHCP para Vlan 21 y 23

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

Nota, comandos utilizados e imágenes pertinentes: La configuración del R2 incluye las siguientes tareas.

La parte de la NAT estática al servidor web se configura, mas no funcionara dado que vimos más atrás que los comandos HTTP en Packet Tracer no funcionaron para la creación de este servicio y menos servidor, por lo que se deja la aclaración.

Elemento o tarea de configuración	Especificación	Comandos IOS
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 % Invalid input detected at '^' marker.	
Configurar el servidor HTTP para utilizar la base de datos	R2(config)#ip http authentication local % Invalid input detected at '^' marker.	

local para la autenticación		
Crear una NAT estática al servidor web	**Dirección global interna: 209.165.200.229**	**R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229**
Asignar la interfaz interna y externa para la NAT estática	R2(config)#int g0/0 R2(config-if)#ip nat outside R2(config-if)#exit R2(config)#int loopback 0 R2(config-if)#ip nat inside R2(config-if)#exit	
Configurar la NAT dinámica dentro de una ACL privada	Lista de acceso: 1 Permitir la traducción de las redes de Contabilidad y de Ingeniería en el R1 Permitir la traducción de un resumen de las redes LAN (loopback) en el R3	R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.4.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.5.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.6.0 0.0.0.255 R2(config)#int s0/0/0 R2(config-if)#ip access-group 1 in R2(config-if)#exit R2(config)#int s0/0/1 R2(config-if)#ip access-group 1 in R2(config-if)#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**	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	

Tabla 29. Configuracion de la NAT estática y dinámica en R2

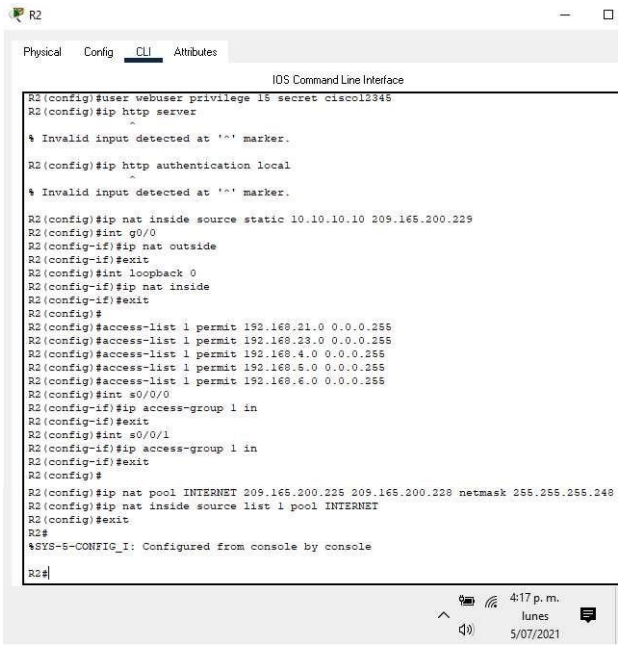


Ilustración 51. Verificacion de la tabla 29, configuracion NAT estática y dinámica en R2

Paso 3: Verificar el protocolo DHCP y la NAT estática

Nota, comandos utilizados e imágenes pertinentes: 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.

La revisión al servidor web no fue posible debido a la imposibilidad de configurar los servicios HTTP y HTTPS en los Router con Packet Tracer, dado que no son soportados por dicha aplicación.

Pruebas	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	Resultados óptimos con respuesta del servidor y datos del servidor, ver imagen 51.
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	Resultados óptimos con respuesta del servidor y datos del servidor, ver imagen 51.
Verificar que la PC-A pueda hacer ping a la PC-C Nota: Quizá sea necesario deshabilitar el firewall de la PC.	Resultados óptimos con respuesta entre los PCs, ver imagen 52.
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	Su respuesta es negativa, debido a la imposibilidad de configurar los servicios HTTP y HTTPS en los Router con Packet Tracer, dado que no son soportados por dicha aplicación.

Tabla 30. Comprobación de los protocolos DHCP y NAT en PCs y el navegador web.

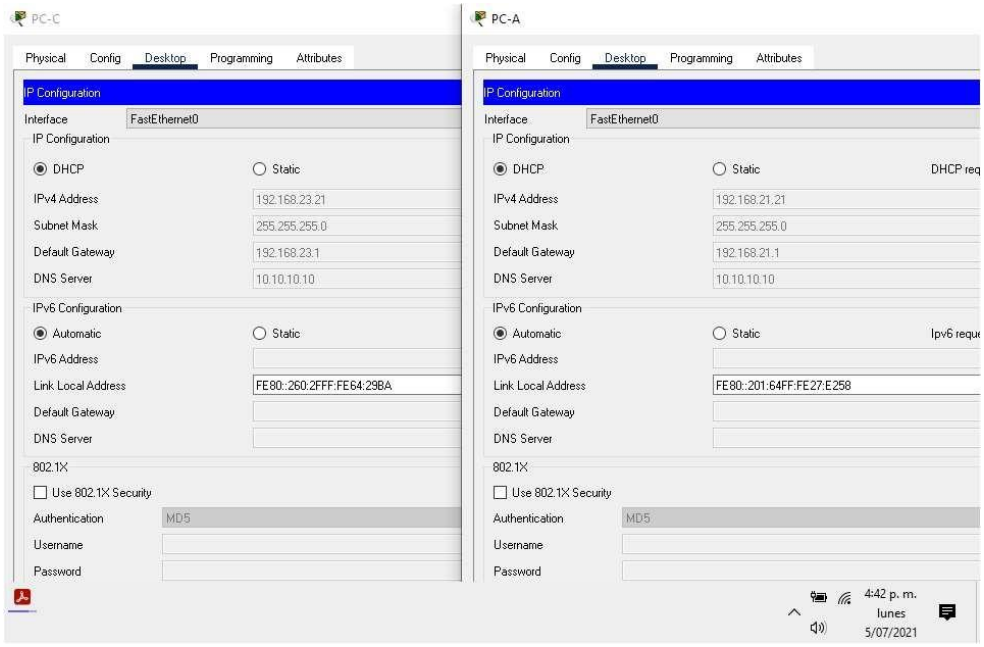


Ilustración 52. Verificación tabla 30, DHCP en los PCs

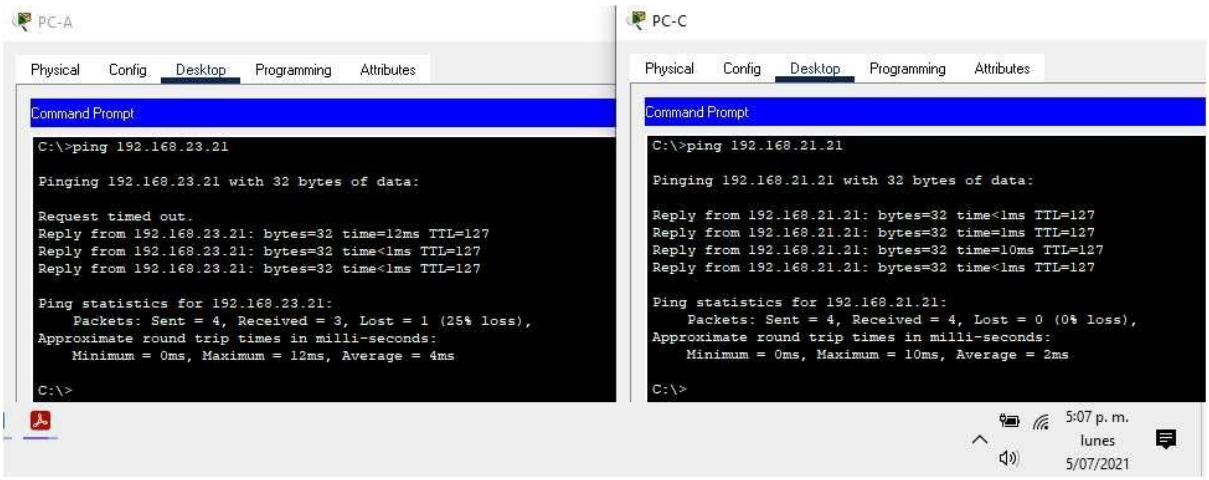


Ilustración 53. Verificación tabla 30, ping entre los PCs

Ilustración 54. Verificación tabla 30, llamado de Servidor Web

Parte 6: Configurar el servicio NTP, actualizar fecha y hora en los Router.

Nota: *Se requirió realizar actualización de la fecha y hora tanto en R1 como en R2 y además se utilizó un comando para sincronizar el NTP en R1.*

Elemento o tarea de configuración	Especificación	Comandos IOS
Ajuste la fecha y hora en R2	**5 de marzo de 2016, 9 a. m.**	R2#clock set 09:00:00 05 March 2016
Configure R2 como un maestro NTP	Nivel de estrato: 5	R2(config)#ntp master 5 R2(config)#exit
Configurar R1 como un cliente NTP	Servidor: R2	R1(config)#ntp server 172.16.1.2
Configure R1 para actualizaciones de calendario periódicas con hora NTP	R1(config)#ntp update-calendar R1(config)#exit	
Verifique la configuración de NTP en R1	R1#show ntp associations address ref clock st when poll reach delay offset disp ~172.16.1.2 .INIT. 16 - 64 0 0.00 0.00 0.12 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured R1#show clock detail 9:9:11.771 UTC Sat Mar 5 2016 Time source is NTP --- R2#show clock detail 9:9:19.297 UTC Sat Mar 5 2016 Time source is NTP	

Tabla 31. Configuracion NTP en R1 y R2

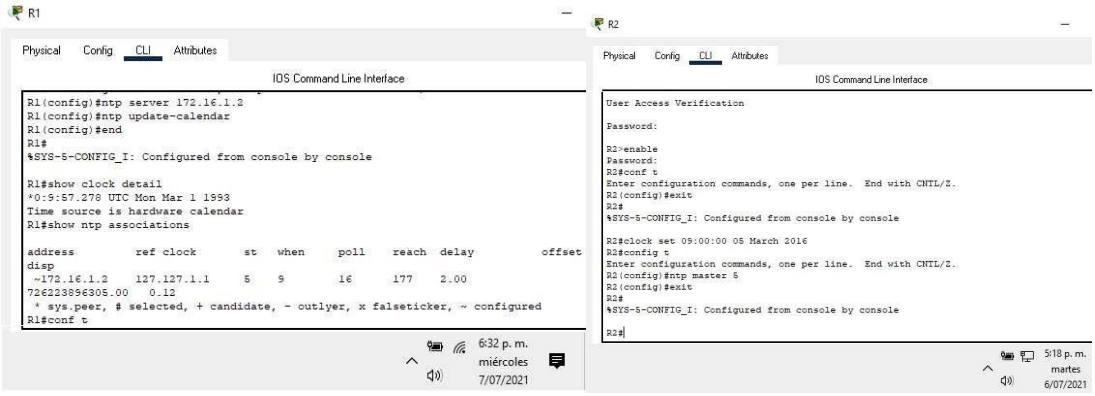


Ilustración 55. Verificación tabla 31, NTP en R1 y R2

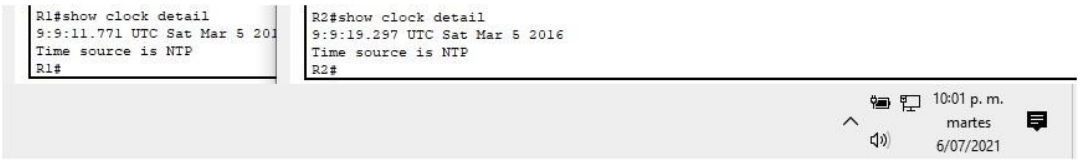


Ilustración 56. Verificación tabla 31, detalles NTP en los Router

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

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

Elemento o tarea de configuración	Especificación	Comandos IOS
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	
Permitir acceso por Telnet a las líneas de VTY	R2(config)#line vty 0 4 R2(config-line)#transport input telnet	
Verificar que la ACL funcione como se espera	R1#telnet 172.16.1.2 Trying 172.16.1.2 ..Open ** Se prohibe el acceso no autorizado ** User Access Verification Password: R2>enable Password: R2#exit [Connection to 172.16.1.2 closed by foreign host] R1#telnet 172.16.2.2 Trying 172.16.2.2 ..Open ** Se prohibe el acceso no autorizado ** User Access Verification Password: R2>enable Password: R2#exit [Connection to 172.16.2.2 closed by foreign host] R1#	

Tabla 32. Configuracion de ACL en los Routers

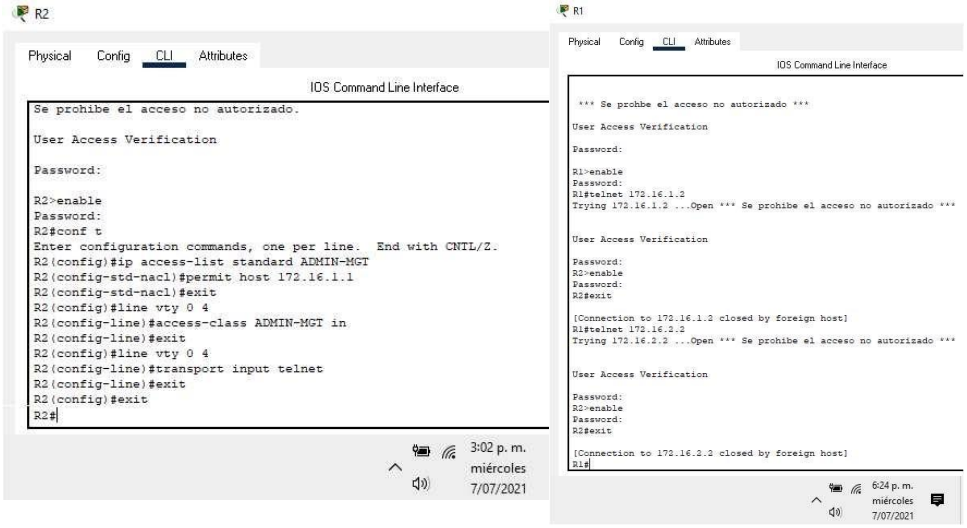


Ilustración 57. Verificacion de la tabla 32, ACL en los Routers

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

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	R2#show access-list Standard IP access list 1 10 permit 192.168.21.0 0.0.0.255 20 permit 192.168.23.0 0.0.0.255 30 permit 192.168.4.0 0.0.0.255 40 permit 192.168.5.0 0.0.0.255 50 permit 192.168.6.0 0.0.0.255 Standard IP access list ADMIN-MGT 10 permit host 172.16.1.1 (4 match(es))
Restablecer los contadores de una lista de acceso	R2#clear access-list counters
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	R2#show ip int s0/0/0 Serial0/0/0 is up, line protocol is up (connected) Internet address is 172.16.1.2/30 Broadcast address is 255.255.255.255
¿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	R2#show ip nat translations Pro - Inside global - Inside local - Outside local - Outside global --- 209.165.200.229 - 10.10.10.10 --- ---

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?	R2#conf t R2(config)#no ip nat inside source list 1 pool INTERNET

Tabla 33. Realizar y verificar tareas de la tabla.

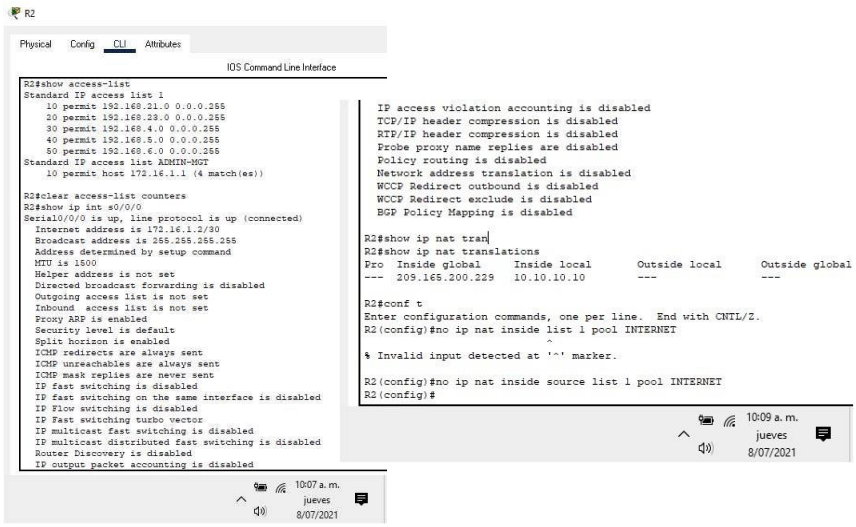


Ilustración 58. Verificacion tabla 33, comandos "show"

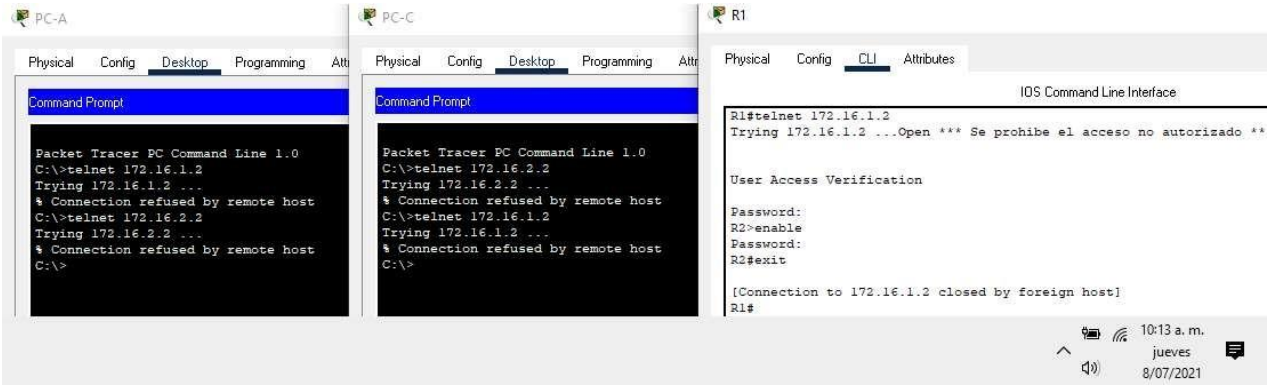


Ilustración 59. Verificacion tabla 33, comprobar eliminación NAT dinamicas

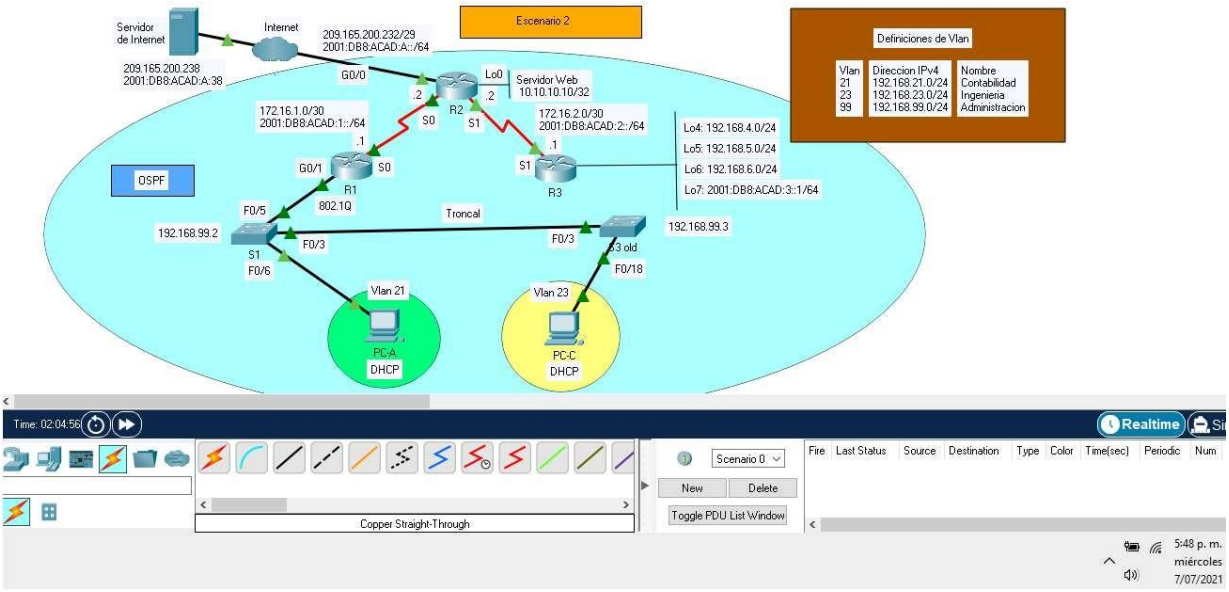


Ilustración 60. Esquema general en packet Tracer escenario 2

Conclusiones

Escenario 1

- Las configuraciones básicas de los dispositivos cisco, nos permiten establecer bases para la configuración de redes locales y poder llevarlas a topologías más grandes y de un nivel más profundo en cuestión de protocolos, configuración y comandos que se investigan y determinan la aplicabilidad del ejercicio.
- Para este escenario se logra determinar que, si se desea hacer ping a todas las direcciones IPv4 e IPv6, se debe cambiar por Switchs capa 3 dado que la configuración realizada fue con los Switchs 2960 y estos en la aplicación Packet Tracer no soportan dicha capa, lo que no permite que funcionen algunos comandos, la solución al problema es trabajar el escenario con los Switchs 3650 que si soportan la capa 3.
- Se encuentran algunos errores de copia de guía, los cuales se logran detectar y cambiar para continuar con la actividad, por ejemplo, la IPv6 de la NIC de la PC-A en la tabla inicial de configuración no corresponde con el escenario.
- Los protocolos y comandos difieren en ocasiones y dependen del dispositivo escogido y también del IOS que tenga este para realizar la configuración del ejercicio, además de la versión de la aplicación Packet Tracer.

- Se recomienda configurar las claves en los dispositivos de redes que se utilizaran, dado que son importantes y tienen la finalidad de evitar accesos no autorizados y evitar con esto los ataques a la red.
- Otro elemento de seguridad son las vlan, las cuales mantienen una segmentación propia de la red, con lo que limitamos el uso exclusivo de los dispositivos y usuarios de la red, logrando una división basada en departamentos, servicios o localidades.

Escenario 2

- En la Configuración del NTP se evidencia una dirección IP que inicia con 127, esta es una configuración interna que se guarda como protección en el caso que no se logre recuperar o configurar el NTP.
- Se encuentran algunos errores de copia de guía, los cuales se logran detectar y cambiar para continuar con la actividad, por ejemplo, en la parte 4 paso 3, donde se indica configurar el protocolo **OSPFv3**, pero no es claro si en R2 o R3, por lo que se decide configurar en los 3 router y poder tener con esto una configuración activa para las direcciones IPv6 en toda la topología.
- Es importante realizar un reinicio a los dispositivos, con el fin de no tener configuraciones previas o remanentes que puedan ocasionar inconsistencias con lo que se desea hacer en los equipos.

- Tanto en la parte 2 del paso 3 como en la parte 5 del paso 2 en la configuración del Router 2, no fue posible habilitar el servicio **HTTP** y/o **HTTPS**, ya que el dispositivo en la aplicación Packet Tracer, genera un error no soportado o no admitido con el comando **"ip http server"**, por lo que no es posible configurar estos servicios y tampoco la NAT estática al router que haría las veces de servidor web simulado, con el que se haría la prueba para acceder con usuario y clave en la parte 5 del paso 3.
- En la parte 2 del paso 7 en donde se verifica la conectividad, El ping realizado al Gateway predeterminado desde PC Internet, no tiene respuesta, esto debido a que se configura en el servidor, pero no hay equipos, redes o alguna otra instancia superior donde se tenga configurado este Gateway como dirección IP fija de un dispositivo o interface, por lo que su respuesta al ping es nula o de pérdida del 100%.

REFERENCIAS

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

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

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

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

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

- UNAD (2017). Configuración de Switches y Routers [OVA]. Recuperado de: https://1drv.ms/u/s!AmIJYei-NT1IhgL9QChD1m9EuGqC

- CISCO. (2019). VLAN. Principios de Enrutamiento y Conmutación. Recuperado de:https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#6

- Error en Switch 2960 con comando “switchport trunk encapsulation dot1Q”. Recuperado de: https://community.cisco.com/t5/other-network-architecture/2960-will-not-allow-quot-switchport-trunk-encapsulation-dot1q/td-p/2439012

ANEXOS

- Link de los archivos PKT con simulaciones en Packet Tracer de los escenarios 1 y 2: https://drive.google.com/drive/folders/1wHx2P468P4AhQMAKeI03b7-Kaesw9nkU?usp=sharing

- Link del repositorio del documento IEEE con las respectivas normas del resumen del escenario 2: https://drive.google.com/drive/folders/1_-KCBXlsWVAW_EvROgcRYoGKY_jqo3Ck?usp=sharing

98645607
Documento IEEE

Estudio y Desarrollo del Escenario 1 USO DE TECNOLOGÍA CISCO (Julio de 2021)

Wilman Darío López Carmona, Estudiante Ingeniería Telecomunicaciones UNAD

Resumen – Para este escenario se configurarán los dispositivos de una red pequeña. Los componentes a configurar son 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. Todo este escenario se realizará con la ayuda de la herramienta de Cisco Packet Tracer, la que nos permitirá además de las configuraciones antes mencionadas también el enrutamiento entre VLAN, DHCP, Etherchannel y port-security.

Índice de Términos – DNS, IP, IPv4, IPv6, Looback.

INTRODUCCIÓN

Este documento forma parte de las actividades evaluativas del Diplomado de Profundización CCNA, y busca identificar el grado de desarrollo de competencias y habilidades que fueron adquiridas a lo largo del diplomado. Lo esencial es poner a prueba los niveles de comprensión y solución de problemas relacionados con diversos aspectos de Networking.

Con el presente trabajo se pretende adquirir las habilidades necesarias en el manejo de la herramienta de simulación y laboratorio como packet tracer, con el fin de simular escenarios LAN/WAN que permitan realizar un análisis sobre el comportamiento de los diversos protocolos y métricas de enrutamiento que se utilizan en el área de redes para lograr un conocimiento profundo de la configuración de los diferentes dispositivos y garantizando una excelente comunicación.

METODOLOGÍA

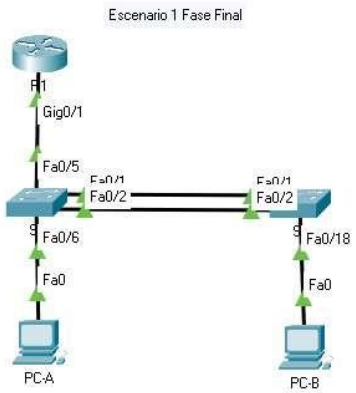
En este artículo se utilizó la metodología de investigación explicativa, donde se utilizarán herramientas de simulación y laboratorios de acceso remoto con el fin de establecer escenarios LAN/WAN que permitan realizar un análisis sobre el comportamiento de diversos protocolos y métricas de enrutamiento.

El estudiante identifica las herramientas de supervisión y protocolos de administración de red disponibles en el IOS para resolver los problemas de las redes de datos, evaluando el desempeño de routers y switches, mediante el uso de comandos especializados en gestión de redes.

EXPLICACIÓN DEL ESCENARIO Y SU TOPOLOGÍA

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

Fig.1. Topología general del escenario



Fuente: Propia

DESARROLLO DEL ESCENARIO Y SU TOPOLOGÍA

Iniciaremos teniendo presente las siguientes tablas: Vlans y asignación de direccionamiento.

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

Tabla 1. Distribución de Vlan para el escenario 1

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
R1 G0/0/1.2	10.21.5.1 /26	No corresponde
	2001:db5:acad:a: :1 /64	No corresponde
R1 G0/0/1.3	10.21.5.65 /27	No corresponde
	2001:db5:acad:b: :1 /64	No corresponde
R1 G0/0/1.4	10.21.5.97 /29	No corresponde
	2001:db5:acad:c: :1 /64	No corresponde
R1 G0/0/1.6	No corresponde	No corresponde
R1 Loopback0	209.165.201.1 /27	No corresponde
	2001:db8:acad:209: :1 /64	No corresponde
S1 VLAN 4	10.21.5.98 /29	10.21.5.97
	2001:db5:acad:c: :98 /64	No corresponde
	fe80: :98	No corresponde
S2 VLAN 4	10.21.5.99 /29	10.21.5.97
	2001:db5:acad:c: :99 /64	No corresponde
	fe80: :99	No corresponde
PC-A NIC	Dirección DHCP para IPv4	DHCP para puerta de enlace predeterminada IPv4
	2001:db5:acad:a: :50 /64	fe80::1
PC-B NIC	DHCP para dirección IPv4	DHCP para puerta de enlace predeterminada IPv4
	2001:db5:acad:b: :50 /64	fe80::1

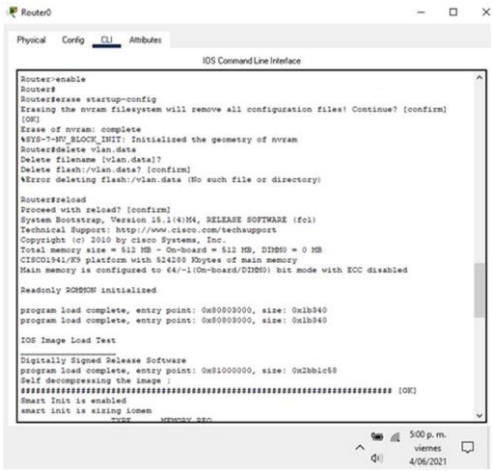
Tabla 2. Asignación para el direccionamiento del escenario 1

Parte 1: Inicializar, Recargar y Configurar aspectos básicos de los dispositivos

Pasos 1 al 3: Inicializar y volver a cargar el router y el switch, configurar R1, S1 y S2.

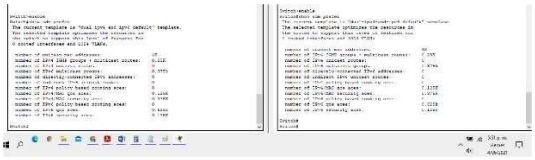
Se borran las configuraciones de inicio y las VLAN tanto del router como de los switch, luego se vuelven a cargar los dispositivos. Esta primera parte se revisa y no se detectan Vlans para borrar, se cambia nombre a los dispositivos, se borra configuración de inicio y se cargan de nuevo.

Fig.2. Comandos inicio configuración Router



Fuente: Propia

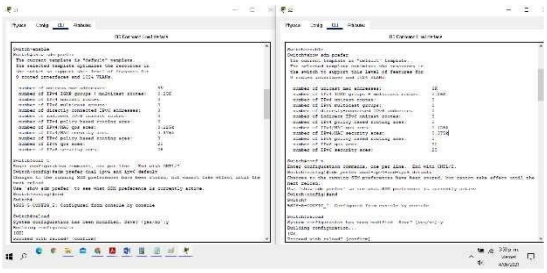
Fig.3. Comandos inicio configuración Switchs

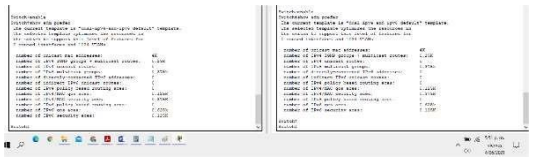


Fuente: Propia

Se continua con la revisión y cambio de plantilla SDM en los Switchs, se cambia de plantilla "default" a "dual-IPv4-and-Ipv6 default" y se carga nuevamente la configuración.

Fig.4. Configuración de la plantilla SDM para admitir IPv6-IPV4 en los Switchs





Fuente: Propia

Código utilizado en imagen 3 para los 2 Switchs:

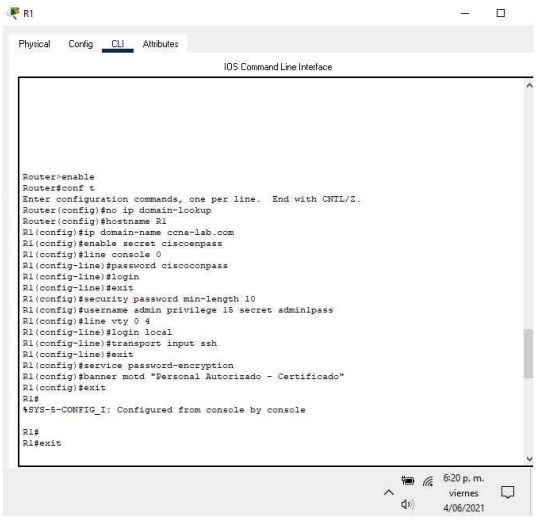
S1-S2#sh sdm prefer
The current template is "dual-ipv4-and-ipv6 default" template.
The selected template optimizes the resources in
the switch to support this level of features for 0 routed interfaces and 1024 VLANs.
number of unicast mac addresses: 4K
number of IPv4 IGMP groups + multicast routes: 0.25K
number of IPv4 unicast routes: 0
number of IPv6 multicast groups: 0.375k
number of directly-connected IPv6 addresses: 0
number of indirect IPv6 unicast routes: 0
number of IPv4 policy based routing aces: 0
number of IPv4/MAC qos aces: 0.125K
number of IPv4/MAC security aces: 0.375K
number of IPv6 policy based routing aces: 0
number of IPv6 qos aces: 0.625k
number of IPv6 security aces: 0.125K

Las tareas de configuración inicial y básica para R1 son las de la siguiente tabla.

Tarea	Especificación
Desactivar la búsqueda DNS	
Nombre del router	R1
Nombre de dominio	ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	ciscoenpass
Contraseña de acceso a la consola	ciscoconpass
Establecer la longitud mínima para las contraseñas	10 caracteres
Crear un usuario administrativo en la base de datos local	Nombre de usuario: **admin** Password: **admin1pass**
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	
Configurar VTY solo aceptando SSH	
Cifrar las contraseñas de texto no cifrado	
Configure un MOTD Banner	
Habilitar el routing IPv6	
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.
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**
Generar una clave de cifrado RSA	Módulo de 1024 bits

Tabla 3. Configuraciones para realizar en R1

Fig.5. Configuración inicial de R1



Fuente: Propia

Se continua la configuración de R1 en su interfaz G0/1 y sus subinterfaces 1.2, 1.3, 1.4 y 1.6, además del link local. Se puede evidenciar algunas de las configuraciones realizadas anteriormente como el aviso inicial, nombre del Router y la seguridad.

Código utilizado en R1:

R1(config)#int g0/1
R1(config-if)#int g0/1.2
R1(config-subif)#encapsulation dot1q 2
R1(config-subif)#description Bikes
R1(config-subif)#ip add 10.21.5.1

255.255.255.192
R1(config-subif)#ipv6 add 2001:db5:acad:a::1/64
R1(config-subif)#ipv6 add fe80::1 link-local
R1(config-subif)#no sh
R1(config-if)#int g0/1.3
R1(config-subif)#encapsulation dot1q 3
R1(config-subif)#description Trikes
R1(config-subif)#ip add 10.21.5.65 255.255.255.224
R1(config-subif)#ipv6 add 2001:db5:acad:b::1/64
R1(config-subif)#ipv6 add fe80::1 link-local
R1(config-subif)#no sh
R1(config-if)#int g0/1.4
R1(config-subif)#encapsulation dot1q 4
R1(config-subif)#description Management
R1(config-subif)#ip add 10.21.5.97 255.255.255.248
R1(config-subif)#ipv6 add 2001:db5:acad:c::1/64
R1(config-subif)#ipv6 add fe80::1 link-local
R1(config-subif)#no sh
R1(config-if)#int g0/1.6
R1(config-subif)#encapsulation dot1q 6
R1(config-subif)#ipv6 add fe80::1 link-local
R1(config-subif)#no sh
R1(config-subif)#exit
R1(config)#int g0/1
R1(config-if)#no sh
R1(config-if)#exit

Siguiendo con la configuración de R1, donde iniciamos configurando el Loopback 0 con IPv4 e IPv6, además del link local y por último se genera la clave de cifrado RSA, con la cual determinamos el tamaño de la clave y el valor de encriptación que se deja el mínimo sugerido que es 1024.

Se realiza un cambio en la dirección **IPv6** dado que en la guía aparece 2001:**db8**:acad:209::1/64 y para un direccionamiento efectivo de ser 2001:**db5**:acad:209::1/64.

Código utilizado en R1:

R1(config)#int loopback0
R1(config-if)#ip add 209.165.201.1 255.255.255.224
R1(config-if)#ipv6 add 2001:db5:acad:209::1/64
R1(config-if)#ipv6 add fe80::1 link-local
R1(config-if)#no sh

Tarea	Especificación
Desactivar la búsqueda DNS.	
Nombre del switch	**S1 o S2, según proceda**
Nombre de dominio	**ccna-lab.com**
Contraseña cifrada para el modo EXEC privilegiado	**ciscoenpass**
Contraseña de acceso a la consola	**ciscoconpass**
Crear un usuario administrativo en la base de datos local	Nombre de usuario: **admin** Password: **admin1pass**
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	
Cifrar las contraseñas de texto no cifrado	
Configurar un MOTD Banner	
Generar una clave de cifrado RSA	**Módulo de 1024 bits**
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
Configuración del gateway predeterminado	Configure la puerta de enlace predeterminada como 10.21.5.97 para IPv4

Tabla 4. Configuraciones para realizar en los Switchs

En esta configuración de los Switchs, la primera parte es de la configuración general que maneja desde el cambio del nombre, se asocia al dominio, se ponen claves, usuario y configuración VTY para base de daos local y conexiones SSH, el aviso y manejo de clave de cifrado RSA.

Código empleado en los dos Switchs:

S1-S2(config)#no ip domain-lookup
S1-S2(config)#ip domain-name ccna-lab.com
S1-S2(config)#line vty 0 4
S1-S2(config-line)#login local
S1-S2(config-line)#transport input ssh
S1-S2(config-line)#exit
S1-S2(config)#crypto key generate rsa general-key modulus 1024
% You already have RSA keys defined named S1.ccna-lab.com
% They will be replaced. % The key modulus size is 1024 bits. % Generating 1024 bit RSA keys, keys will be non-exportable...[OK] *Mar 1 4:51:51.710: %SSH-5-ENABLED: SSH 1.99 has been enabled
S1-S2(config)#end

Continuando con la configuración de los Switchs, se interviene la interfaz de administración (SVI), donde se establece la dirección IPv4 y IPv6 de capa 3, la dirección local de enlace IPv6 para cada uno y por último la configuración de la puerta de enlace predeterminada.

Código empleado en los dos Switchs:

```
Personal Certificado - Autorizado
User Access Verification
Password:
S1-S2>enable
Password:
S1-S2#conf t
S1-S2(config)#int vlan 4
S1-S2(config-if)#description Management
S1(config-if)#ip add 10.21.5.98
255.255.255.248
S2(config-if)#ip add 10.21.5.99
255.255.255.248
S1-S2(config-if)#no sh
S1-S2(config-if)#ip default-gateway 10.21.5.97
S1(config)#end
S1-S2(config)#int vlan 4
S1(config-if)#ipv6 add 2001:db5:acad:c::98/64
S2(config-if)#ipv6 add 2001:db5:acad:c::99/64
S1(config-if)#ipv6 add fe80::98 link-local
S2(config-if)#ipv6 add fe80::99 link-local
S1-S2(config-if)#no sh
```

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

Pasos 1 al 2: Configurar S1 y S2

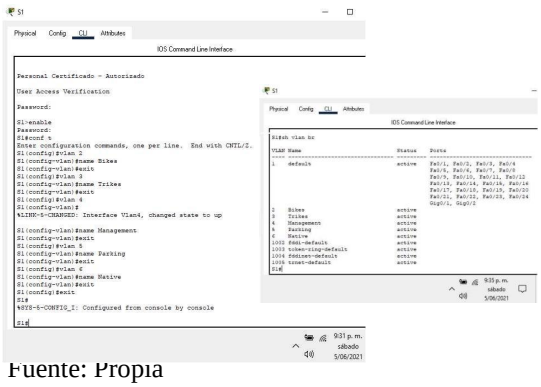
Las tareas a realizar se pueden ver en la siguiente tabla:

Tarea	Especificación
Crear VLAN	VLAN 2, nombre Bikes VLAN 3, nombre Trikes VLAN 4, name Management VLAN 5, nombre Parking VLAN 6, nombre Native
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	Interfaces F0/1, F0/2 y F0/5
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	Usar el protocolo LACP para la negociación
Configurar el puerto de acceso de host para VLAN 2	Interface F0/6
Configurar la seguridad del puerto en los puertos de acceso	Permitir 3 direcciones MAC
Proteja todas las interfaces no utilizadas	Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar

Tabla 5. Configuración de infraestructura de red en S1

Se realiza la configuración de infraestructura de red en S1 con las VLAN, los Trunk en las interfaces, creación de un grupo de puertos, configurar puerto de acceso con la seguridad y protección de interfaces no utilizadas.

Fig.6. *Creación y verificación de Vlans en S1*



Fuente: Propia

El comando "switchport trunk encapsulation dot1Q", no se requiere en este modelo de Switch se hace la configuración directa como se muestra a continuación.

Código empleado en S1

```
S1(config)#int f0/1
S1(config-if)#Switchport mode trunk
S1(config-if)#Switchport trunk native vlan 6
S1(config-if)#exit
S1(config)#int f0/2
S1(config-if)#Switchport mode trunk
S1(config-if)#Switchport trunk native vlan 6
S1(config-if)#exit
S1(config)#int f0/5
S1(config-if)#Switchport mode trunk
S1(config-if)#Switchport trunk native vlan 6
```

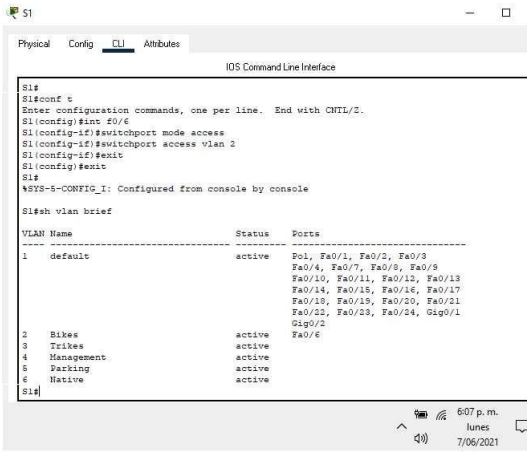
Fig.7. Verificación configuración-uso VLAN 6 Nativa

Fuente: Propia

Código de Creación grupo de puertos EtherChannel capa 2 interfaces F0/1-2, con LACP:

S1(config)#int ran f0/1-2
S1(config-if-range)#channel-protocol lacp
S1(config-if-range)#channel-group 1 mode active
S1(config-if-range)#exit
S1(config)#exit
S1#sh ether
Channel-group listing:
Group: 1
Group state = L2
Ports: 2 Maxports = 16
Port-channels: 1 Max Port-channels = 16
Protocol: LACP

Fig.8. Configuración y verificación puerto de acceso de host para VLAN 2.



Fuente: Propia

Código configuración port-security en los access ports, permitir 3 MAC add:

S1(config)#int f0/6
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)#exit

Código e imagen proceso para protección de las interfaces no utilizadas:

S1(config)#int range g0/1-2, f0/3-4, f0/7-24
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 5
S1(config-if-range)#descript Proteccion Interfaces no utilizadas
S1(config-if-range)#sh
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to administratively down
S1(config-if-range)#switchport port-security
S1(config-if-range)#switchport port-security violation shutdown
S1(config-if-range)#exit

Este paso del S2 es similar al del S1 se diferencia solo en las interfaces a configurar el resto es la misma configuración de infraestructura de red con las VLAN, Trunk en interfaces, creación grupo de puertos, configurar puerto de acceso con la seguridad y protección de interfaces no utilizadas, este proceso se deja indicado mas no se muestra evidencia por la similitud con el proceso del S1.

Tarea	Especificación
Crear VLAN	VLAN 2, name Bikes VLAN 3, name Trikes VLAN 4, name Management VLAN 5, nombre Parking VLAN 6, nombre Native
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	Interfaces F0/1 y F0/2
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	Usar el protocolo LACP para la negociación
Configurar el puerto de acceso del host para la VLAN 3	Interfaz F0/18
Configure port-security en los access ports	permite 3 MAC addresses
Asegure todas las interfaces no utilizadas.	Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar

Tabla 6. Configuración de infraestructura de red en S2

Parte 3: *Configurar soporte de host*

Pasos 1 al 2: Configuración avanzada de R1 y los PCs

Esta configuración avanzada del Router 1 crea rutas predeterminadas IPv4 e IPv6 con tráfico por Loopback 0, también trabajar IPv4 con DHCP por Vlan 2 y 3, asignar subredes, nombre de dominio, puerta de enlace según indicación.

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
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

Tabla 7. Configuración R1, enrutamiento y activar DHCP en las Vlans

Código IPv4 e IPv6 que dirijan el tráfico a la interfaz Loopback 0:

```
R1(config)#int loopback 0
R1(config-if)#ip route 0.0.0.0 0.0.0.0 loopback 0
%Default route without gateway, if not a point-to-point interface, may impact performance
R1(config)#ipv6 route ::/0 loopback 0
R1(config)#exit
```

Código configuración IPv4 DHCP para VLAN 2 y VLAN3:

```
R1(config)#ip dhcp pool vlan2
R1(dhcp-config)#network 10.21.5.0 255.255.255.192
R1(dhcp-config)#default-router 10.21.5.1
R1(dhcp-config)#domain-name ccna-a.net
R1(dhcp-config)#ip dhcp excluded-address 10.21.5.2 10.21.5.51
R1(config)#ip dhcp pool vlan3
R1(dhcp-config)#network 10.21.5.64 255.255.255.224
R1(dhcp-config)#default-router 10.21.5.65
R1(dhcp-config)#domain-name ccna-b.net
R1(dhcp-config)#ip dhcp excluded-address 10.21.5.66 10.21.5.83
```

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**.

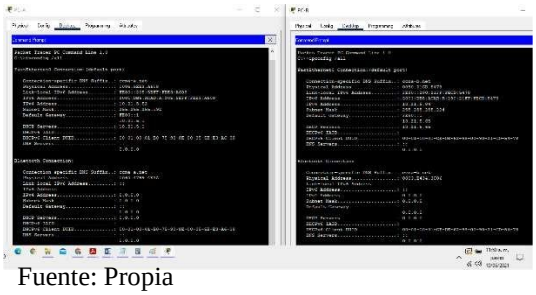
PC-A Network Configuración	
Descripción	Usando el Comando "**ipconfig /all**"
Dirección física	0005.5EE3.A608
Dirección IP	10.21.5.52
Máscara de subred	255.255.255.192
Gateway predeterminado	10.21.5.1
Gateway predeterminado IPv6	FE80::1

Tabla 8. Configuración Red de PC-A

PC-B Network Configuración	
Descripción	Usando el Comando "**ipconfig /all**"
Dirección física	0090.21CD.5478
Dirección IP	10.21.5.84
Máscara de subred	255.255.255.224
Gateway predeterminado	10.21.5.65
Gateway predeterminado IPv6	FE80::1

Tabla 9. Configuración Red de PC-B

Fig.9. Verificación Red PC-A y PC-B con "ipconfig /all"



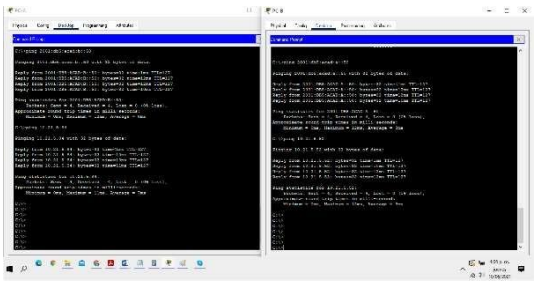
Fuente: Propia

Parte 4: *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.

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:

Fig.10. Uso comando ping IPv4 y IPv6 de PC-A a PC-B y viceversa



Fuente: Propia

Desde	A	de Internet	Dirección IP	Resultados Ping
PC-A	R1, G0/1.2	Dirección	10.21.5.1	Pérdidas 0%
		IPv6	2001:db5:acad:a::1	Pérdidas 0%
	R1, G0/1.3	Dirección	10.21.5.65	Pérdidas 0%
		IPv6	2001:db5:acad:b::1	Pérdidas 0%
	R1, G0/1.4	Dirección	10.21.5.97	Pérdidas 0%
		IPv6	2001:db5:acad:c::1	Pérdidas 0%
	S1, Vlan 4	Dirección	10.21.5.98	Pérdidas 0%
		IPv6	2001:db5:acad:c::98	Pérdidas 100%
	S2, Vlan 4	Dirección	10.21.5.99	Pérdidas 0%
		IPv6	2001:db5:acad:c::99	Pérdidas 100%
	PC-B	Dirección	10.21.5.84	Pérdidas 0%
		IPv6	2001:db5:acad:b::50	Pérdidas 0%
	R1 Bucle 0	Dirección	209.165.201.1	Pérdidas 0%
		IPv6	2001:db5:acad:209::1	Pérdidas 0%
PC-B	R1 Bucle 0	Dirección	209.165.201.1	Pérdidas 0%
		IPv6	2001:db5:acad:209::1	Pérdidas 0%
	R1, G0/1.2	Dirección	10.21.5.1	Pérdidas 0%
		IPv6	2001:db5:acad:a::1	Pérdidas 0%
	R1, G0/1.3	Dirección	10.21.5.65	Pérdidas 0%
		IPv6	2001:db5:acad:b::1	Pérdidas 0%
	R1, G0/1.4	Dirección	10.21.5.97	Pérdidas 0%
		IPv6	2001:db5:acad:c::1	Pérdidas 0%
	S1, Vlan 4	Dirección	10.21.5.98	Pérdidas 0%
		IPv6	2001:db5:acad:c::98	Pérdidas 100%
	S2, Vlan 4	Dirección	10.21.5.99	Pérdidas 0%
		IPv6	2001:db5:acad:c::99	Pérdidas 100%

Tabla 10. Conectividad de extremo a extremo desde PC-A y PC-B

CONCLUSIÓN

Las configuraciones básicas de los dispositivos Cisco, nos permiten establecer bases para la configuración de redes locales y poder llevarlas a topologías más grandes y de un nivel más profundo en cuestión de protocolos, configuración y comandos que se investigan y determinan la aplicabilidad del ejercicio.

Para este escenario se logra determinar que, si se desea hacer ping a todas las direcciones IPv4 e IPv6, se debe cambiar por Switchs capa 3 dado que la configuración realizada fue con los Switchs 2960 y estos en la aplicación Packet Tracer no soportan dicha capa, lo que no permite que funcionen algunos comandos, la solución al problema es trabajar el escenario con los Switchs 3650 que si soportan la capa 3.

Se encuentran algunos errores de copia de guía, los cuales se logran detectar y cambiar para continuar con la actividad, por ejemplo, la IPv6 de la NIC de la PC-A en la tabla inicial de configuración no corresponde con el escenario.

Los protocolos y comandos difieren en ocasiones y dependen del dispositivo escogido y también del IOS que tenga este para realizar la configuración del ejercicio, además de la versión de la aplicación Packet Tracer.

Se recomienda configurar las claves en los dispositivos de redes que se utilizaran, dado que son importantes y tienen la finalidad de evitar accesos no autorizados y evitar con esto los ataques a la red.

Otro elemento de seguridad son las vlan, las cuales mantienen una segmentación propia de la red, con lo que limitamos el uso exclusivo de los dispositivos y usuarios de la red, logrando una división basada en departamentos, servicios o localidades.

APÉNDICE

Link del repositorio de los archivos PKT con los escenarios 1 y 2:
https://drive.google.com/drive/folders/1qJTWvbm9_hfTuexTBPEuTZ7G3QPD6jbc?usp=sharing

Link del repositorio del documento IEEE resumen del escenario 2:
https://drive.google.com/drive/folders/1_-KCBXlsWVAW_EvROgcRYoGKY_jqo3Ck?usp=sharing

RECONOCIMIENTO

Un agradecimiento a los compañeros del Diplomado, a el Ingeniero Héctor Herrera y la Ingeniera Nancy Guaca, quienes me guiaron durante el proceso y desarrollo del curso y los escenarios propuestos.

REFERENCIAS

[1] CISCO. (s.f). Listas de control de acceso. Principios de Enrutamiento y Conmutación. {2017} Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module9/index.html#9.0.1.1

[2] CISCO. Enrutamiento Dinámico. Principios de Enrutamiento y Conmutación. {2017}. Recuperado de https://static-courseassets.s3.amazonaws.com/RSE50ES/module7/index.html#7.0.1.1

[3] CISCO. Configuración de Listas de Acceso IP. [Articulo de internet]. {2007}. Recuperado de https://www.cisco.com/c/es_mx/support/docs/security/ios firewall/23602-confaccesslists.html

[4] CISCO. (s.f.). Cisco Networking Academy. Obtenido de https://www.netacad.com/es

[5] Villagómez, Carlos. VLAN-Redes virtuales. {En línea}. {13 de septiembre de 2017} disponible en: (https://es.ccm.net/contents/286-vlan-redes-virtuales

[6] Villagómez, Carlos. El protocolo DHCP. {En línea}. {8 de marzo de 2017} disponible en: (https://es.ccm.net/contents/261-el-protocolo-dhcp).

Biografía Autor(es)

Wilman Darío López Carmona, nacido el 31 de octubre de 1976 en la ciudad de Medellín del Departamento de Antioquia, estudiante del pregrado de Ingeniera de Telecomunicaciones en la Universidad Nacional Abierta y a Distancia UNAD, seccional Medellín, Antioquia.