IMPLEMENTACION DE ESTUDIOS DE CASOS BAJO LA TECNOLOGIA CISCO

JORGE IVAN GIRALDO ALARCON

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIRIA DE TELECOMUNICACIONES
MEDELLIN- ANTIOQUIA
2021

IMPLEMENTACION DE ESTUDIOS DE CASOS BAJO LA TECNOLOGIA CISCO

JORGE IVAN GIRALDO ALARCON

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

DIRECTOR
NANCY AMPARO GUACA
TUTOR
HÉCTOR MANUEL HERRERA HERRERA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
MEDELLIN ANTIOQUIA
2021

Nota de aceptación:

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

Medellín, 16 de julio de 2021

AGRADECIMIENTOS

Este diplomado es la opción de grado donde culmino mi etapa de formación y continúo ejerciendo la profesional como ingeniero, agradezco a mi familia por el apoyo que me han brindado a lo largo de mis estudios y a la UNAD por brindarme esta gran oportunidad, las asesorías y acompañamiento académico, durante el tiempo de aprendizaje para poder lograr los retos deformación como profesional.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

ACL(lista de control de acceso) permiten controlar el flujo de tráfico en equipos de redes tales como routers y conmutadores, su principal característica es filtrar el tráfico ,permitiendo o denegando el tráfico de la red de acuerdo a las necesidades .

NETWORK conjunto de dispositivos interconectados entre si para comunicarse entre si.

VLAN(red de área virtual) es una tecnología para la creación de redes lógicas independientes dentro de una misma red física.

TRUNK es un enlace que se configura en uno o más suiches para permitir el tráfico de las distintas vlans configuradas, trabajan acerca del estándar IEE802.Q.

ACCES PORT es un tipo de conexión en un suiche utilizada para conectar un equipo virtual conectado que no conoce la VLAN.

INTERFACE se conoce como interface al medio que permite a una persona conectarse a un equipo.

GATEWAY Es el dispositivo que actúa de interfaz de conexión entre aparatos o dispositivos, traduce las direcciones de red, aplica la técnica de enmascaramiento de ip usada para dar acceso a internet.

DHCP(Dynamic host configuration protocol) es un servidor de red el cual permite la asignación automática de direcciones Ip, gateways predeterminadas. El dhcp envia todos los parámetros para que los clientes se comuniquen sin problema en la red.

DNS(domain name service)traduce los nombres de dominio aptos para la lectura humana.ejpla ip 269.2.200.2 equivale a www. jorgeservice.co.

ROUTER es un dispositivo que permite interconectar equipos que funcionan en el marco de una red, establece la ruta que destinara a cada paquete de datos dentro de la red.

SWITCH es un dispositivo diseñado para resolver problemas de rendimiento de la red, debido a bajos anchos de banda y embotellamientos. el suiche proporciona mayor ancho de banda, acelera la salida de paquetes, reduce el tiempo de espera y baja el costo por puerto.

MAC Media Access control) es un identificador de 48 bits (6 bloques de dos caracteres hexadecimales que corresponde de forma única a una tarjeta o dispositivo de red).

TELNET (Teletype Network) protocolo de red que permite el acceso a otro equipo para su control remotamente.

LOOPBACK es una interfaz de red virtual .su principal aplicación es dirigir el tráfico hacia ellos mismos, la creación del loopback crea un método de acceso directo para las aplicaciones y servicios TCP/IP que se ejecutan en el mismo dispositivo para comunicarse entre sí.

RESUMEN

Cisco Networking Academy es un programa global de educación en ciberseguridad y TI que se asocia con instituciones de aprendizaje de todo el mundo para empoderar a todas las personas con oportunidades profesionales.

El DIPLOMADO DE PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN) (OPCI) permite crear soluciones a través de del simulador packtracer para analizar diversos protocolos y procedimientos de enrutamiento, estático, dinámico, creación de servidores de DHCP y Web basado en un esquema de direccionamiento de IP y IPV6 para dar solución a los requerimientos de seguridad y de conectividad de las diferentes VLAN

A través de la aplicación del simulador se coloca en práctica los diferentes comandos en los suiches y router donde se logra identificar su comportamiento a la hora de la interconexión de los mismos, identificando la seguridad, la división de las sub redes y la comunicación.

ABSTRACT

Cisco Networking Academy is a global IT and cybersecurity education program that partners with learning institutions around the world to empower all people with career opportunities.

The CISCO DEEPENING DIPLOMA (DESIGN AND IMPLEMENTATION OF INTEGRATED LAN / WAN SOLUTIONS) (OPCI) allows you to create solutions through the packtracer simulator to analyze various protocols and routing procedures, static, dynamic, creation of DHCP servers and Web-based an IP and IPV6 addressing scheme to solve the security and connectivity requirements of the different VLANs

Through the application of the simulator, the different commands are put into practice in the switches and routers where it is possible to identify their behavior when interconnecting them, identifying security, the division of sub-networks and communication.

1. INTRODUCCIÓN

Este diplomado CISCO es importante porque permite afianzar los conocimientos adquiridos en el desarrollo de la carrera, colocando en practica la configuración de redes, enrutamiento y la creación de la VLAN.

Se plantea una metodología para la creación a través de simulación de las diferentes configuraciones de los dispositivos (routers, switches, pc).

Es muy importante el desarrollo de este proyecto dado que permite la preparación para la vida laboral de los futuros ingenieros contando con preparación en redes, permitiendo unificar los ejes del ser con el hacer y contar así con experiencia para unirse al mundo laboral en esta área.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

- Identificar y comprender el funcionamiento de las redes LAN/WAN, su configuración y análisis de seguridad de las mismas, mediante la herramienta de simulación packettrecert-basado en la tecnología cisco

2.2 OBJETIVOS ESPECIFICOS

- Comprender la configuración básica de los diferentes dispositivos
- Creación de vlan y troncales
- Enrutamiento estático y dinámico
- Configuración de interfaces en los suiches y router
- Configuraciones de seguridad

3. ESCENARIO 1

Topología

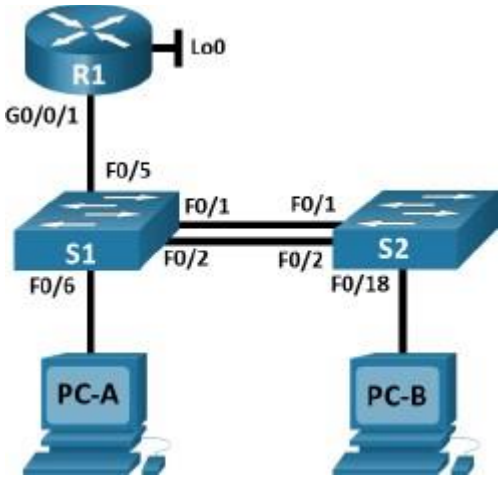


Ilustración 1 Topología a implementar escenario 1

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

Tabla 1 VLAN

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

Tabla de asignación de direcciones

Tabla 2 tabla 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

Parte 1: iniciar, Recargar y configurar aspectos básicos de los dispositivos.

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

• Borre las configuraciones de inicio y las VLAN del router y del switch y vuelva a cargar los dispositivos.

Se inicia el router y se ingresa al modo privilegiado y se eliminan las vlan y la configuración
Router>enable
Router#delete vlan.dat
Delete filename [vlan.dat]?
Delete flash:/vlan.dat? [confirm]
%Error deleting flash:/vlan.dat (No such file or directory)

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

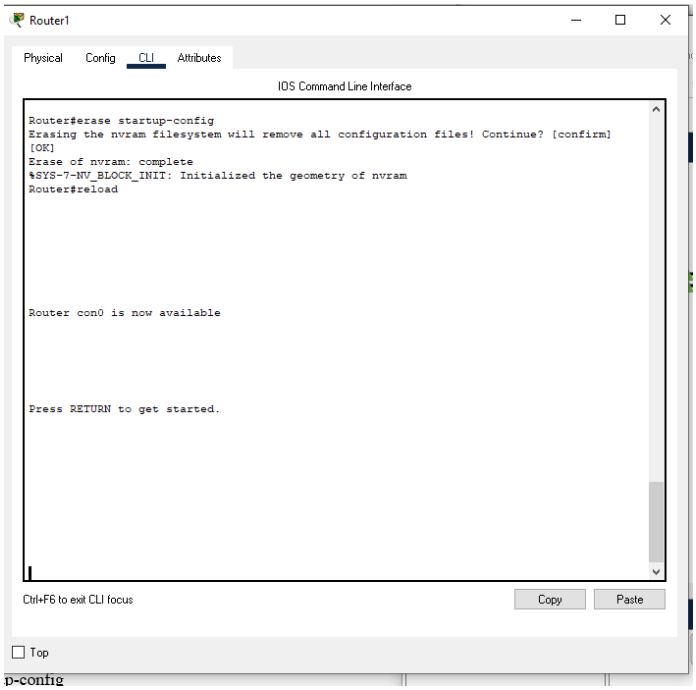


Ilustración 2 eliminar configuración

Se inicia el suiche y se ingresa al modo privilegiado y se eliminan las vlan y la configuración
Switch>enable
Switch#delete vlan.dat
Delete filename [vlan.dat]?
Delete flash:/vlan.dat? [confirm]
%Error deleting flash:/vlan.dat (No such file or directory)

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#reload

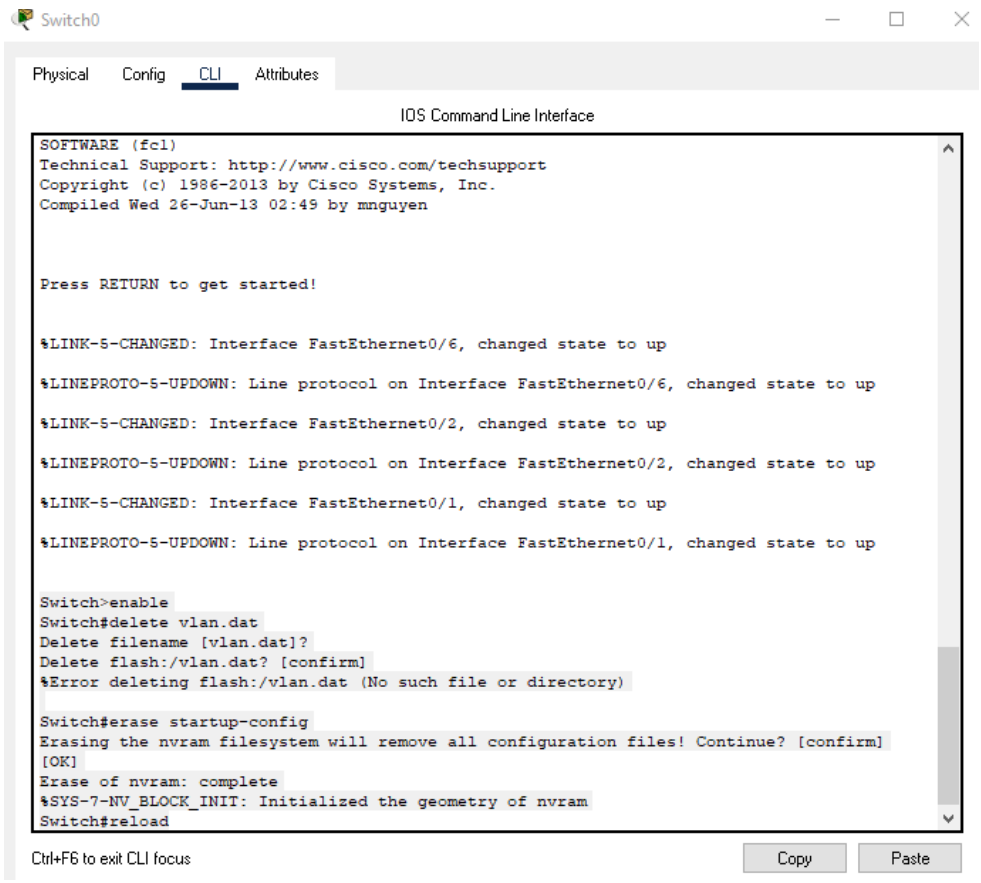


Ilustración 3 eliminar configuración y vlan.

• Después de recargar el switch, configure la plantilla SDM para que admita IPv6 según sea necesario y vuelva a cargar el switch.

S1# show sdm prefer

```
Switch>enable
Switch#show sdm prefer
 The current template is "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:                  8K
  number of IPv4 IGMP groups + multicast routes:    0.25K
  number of IPv4 unicast routes:                    0
  number of IPv6 multicast groups:                  0
  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:                          20
  number of IPv6 security aces:                     25

Switch#
```

Ilustración 4 preferencias de las plantillas sdm

pasos para asignar la plantilla dual-ipv4-and-ipv6

como la plantilla de SDM predeterminada:

S1# config t

S1(config)# **sdm prefer dual-ipv4-and-ipv6 default**

S1(config)# end

S1# reload

```
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#sdm prefer dual-ipv4-and-ipv6 default?
default
Switch(config)#sdm prefer dual-ipv4-and-ipv6 default
Changes to the running SDM preferences have been stored, but cannot take effect until the
next reload.
Use 'show sdm prefer' to see what SDM preference is currently active.
Switch(config)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console
reload
```

Ilustración 5 implementación del comando sdm prefer dual-ipv4-and-ipv6 default

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

Paso 2: configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 3 configuracion R1

Tarea	Especificación
Desactivar la búsqueda DNS	**no ip domain-lookup**
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	**Line vty 0 4**
Configurar VTY solo aceptando SSH	**Transport input ssh**
Cifrar las contraseñas de texto no cifrado	**Service password-encryption**
Configure un MOTD Banner	Banner motd #"acceso no autorizado"#
Habilitar el routing IPv6	Ipv6 unicast-routing
Configurar interfaz G0/0/1 y subinterfaces	Establezca la descripción Establece la dirección IPv4. Establezca la dirección local de enlace IPv6 como **fe80: :1** Establece la dirección IPv6. Activar la interfaz.
Configure el Loopback0 interface	Establezca la descripción Establece la dirección IPv4. Establece la dirección IPv6. Establezca la dirección local de enlace IPv6

	como
Generar una clave de cifrado RSA	Módulo de 1024 bits

Desactivar dominio

Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#**no ip domain-lookup**
Router(config)#exit

Cambio de nombre

Router(config)#hostname R1
R1(config)#exit

Configuración del dominio

R1>enable
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip domain-name ccna-lab.com
R1(config)#exit

Configuración contraseña modo privelegiado

R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#enable secret ciscoenpass
R1(config)#exit

Configuración primera línea de consola

R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#line console 0
R1(config-line)#pass ciscoconpass
R1(config-line)#login

R1(config-line)#exit

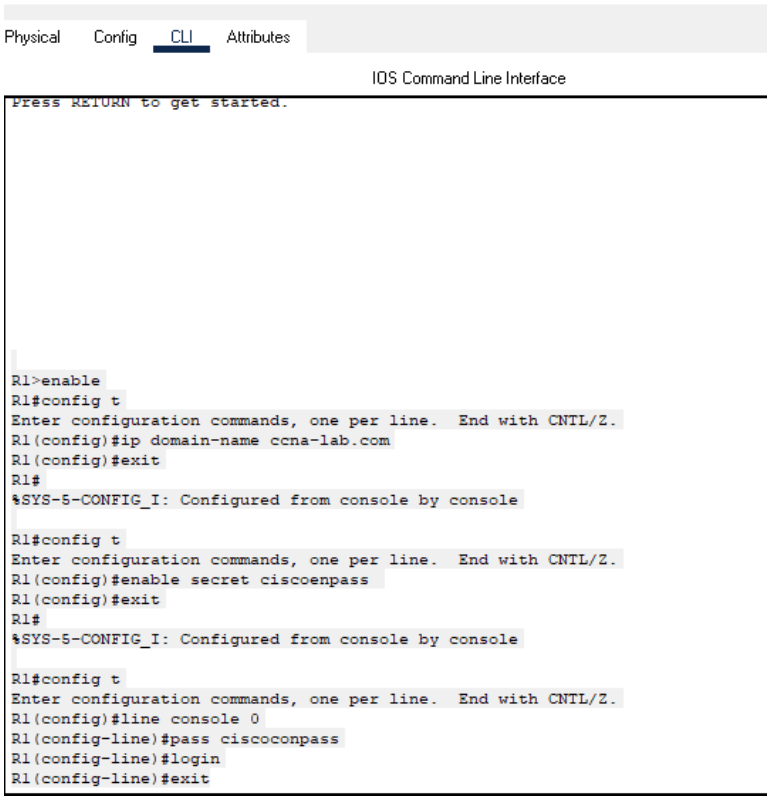


Ilustración 6 configuración dominio,pass linea 0 y linea privilegiado

Configuración longitud de contraseña

R1#config t
R1(config)#security passwords min-length 10
R1(config)#exit

Configuración de usuario admin

R1#config t
R1(config)#username admin secret admin1pass
R1(config)#

Configuración línea vty

R1(config)#do show line
Tty Line Typ Tx/Rx A Roty AccO AccI Uses Noise Overruns Int
* 0 0 CTY--------0 0 0/0 -
1 1 AUX 9600/9600--------0 0 0/0 -
2 2 VTY ------- 0 0 0/0 -

3 3 VTY ------- 0 0 0/0 -
4 4 VTY ------- 0 0 0/0 -
5 5 VTY ------- 0 0 0/0 -
6 6 VTY ------- 0 0 0/0 -
R1(config)#line vty 0 4
R1(config-line)#login local
R1(config-line)#exit
R1(config)#

Vty acotando solo ssh

R1(config)#username admin secret admin1pass
R1(config)#line vty 0 4
R1(config-line)#transport input ssh
R1(config-line)#login local
R1(config-line)#exit
R1(config)#ip ssh version 2
Please create RSA keys (of at least 768 bits size) to enable SSH v2. 1024
R1(config)#crypto R1.ccna-lab.com generate rsa
R1(config)#ip ssh version 2
Please create RSA keys (of at least 768 bits size) to enable SSH v2.

```
R1(config)#username admin secret  admin1pass
R1(config)#line vty 0 4
R1(config-line)#transport input ssh
R1(config-line)#login local
R1(config-line)#exit
R1(config)#ip ssh version 2
Please create RSA keys (of at least 768 bits size) to enable SSH v2.
R1(config)#crypto R1.ccna-lab.com generate rsa
                ^
% Invalid input detected at '^' marker.

R1(config)#crypto R1.ccna-lab.com generate rsa
                ^
% Invalid input detected at '^' marker.

R1(config)#crypto R1.ccna-lab.com generate rsa?
% Unrecognized command
R1(config)#crypto ccna-lab.com generate rsa?
% Unrecognized command
R1(config)#crypto key generate rsa
The name for the keys will be: R1.ccna-lab.com
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

R1(config)#
*Mar 1 1:25:32.870: %SSH-5-ENABLED: SSH 2 has been enabled
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

Ilustración 7 generación de acceso local ssh

Encriptación de contraseñas no cifradas

R1(config)#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#service password-encryption
R1(config)#

Configuración ip y ipv6
Configuracion de las subinterfaces

R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int g0/0/1.2
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 shutdown
R1(config-subif)#exit

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 shut
R1(config-subif)#exit

R1(config)#int g0/0/1.4
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 shut
R1(config-subif)#exit
R1(config)#do wr
Building configuration...
[OK]

R1(config)#int g0/0/1.5
R1(config-subif)#encapsulation dot1Q 5
R1(config-subif)#description Parking
R1(config-subif)#no sh
R1(config-subif)#exit

R1(config)#interface g0/0/1.6
R1(config-subif)#encapsulation dot1Q 6
R1(config-subif)#description Native
R1(config-subif)#no sh
R1(config-subif)#exit
R1(config)# do wr
R1(config)#

Interface loopback 0

R1(config)#interface loopback 0
R1(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up

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

R1(config-if)#ip add 209.165.201.1 255.255.255.224
R1(config-if)#no shut
R1(config-if)#ipv6 add 2001:db8:acad:209::1/64
R1(config-if)#do show ip interface brief
R1(config-if)#ipv6 add fe80::1 link-local
R1(config-if)#no sh
R1(config-if)#

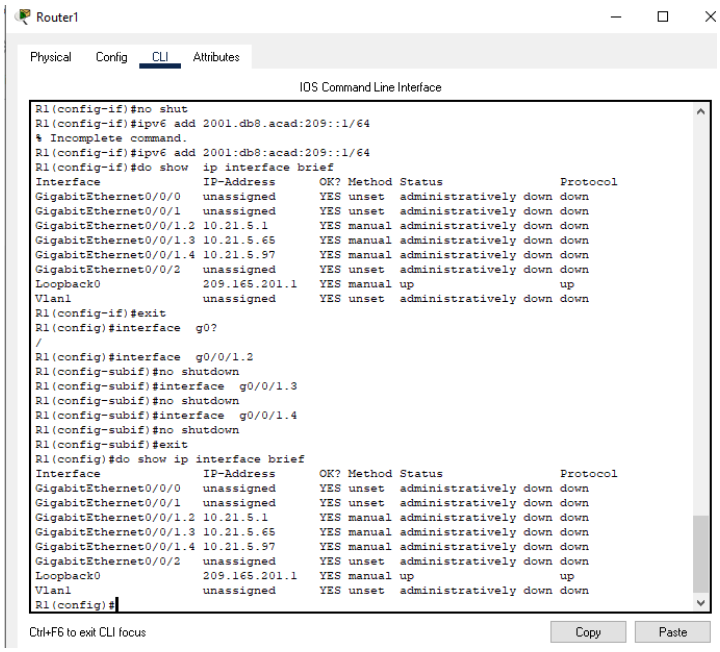


Ilustración 8 configuración ip y ipv6

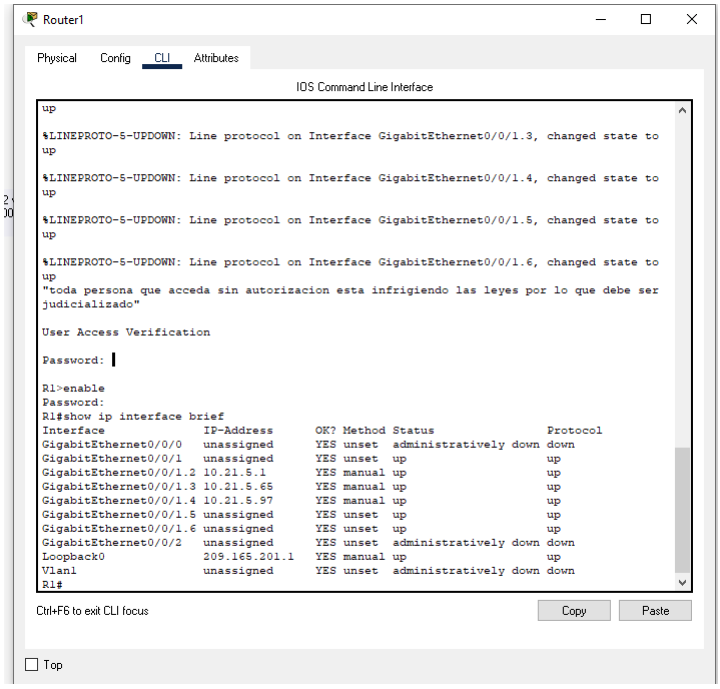


Ilustración 9 comando show ip interface brief

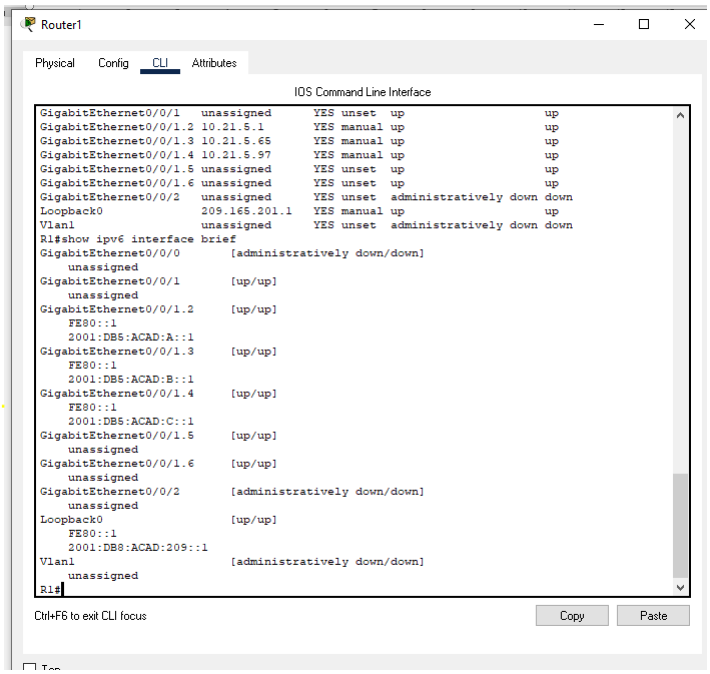


Ilustración 10 comando show ipv6 interface brief

Paso 3: Configure S1 y S2.

Las tareas de configuración incluyen lo siguiente:

Tabla 4 configuración S1 y S2

Tarea	Especificación
Desactivar la búsqueda DNS.	No ip domain-lookup
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	**Line vty 0 15**

Configurar las líneas VTY para que acepten únicamente las conexiones SSH	**Ip ssh version 2**
Cifrar las contraseñas de texto no cifrado	Service password encryption
Configurar un MOTD Banner	Banner motd #"acceso no autorizado"#
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

Desactivar DNS

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

CREACION DEL DOMINIO

S1(config)#ip domain-name ccna-lab.com
S1(config)#enable secret ciscoenpass
S1(config)#line console 0
S1(config-line)#pass ciscoconpass
S1(config-line)#login
S1(config-line)#exit
S1(config)#
S1(config)# line vty 0 15
S1(config-line)# login local
S1(config-line)#exit

S1(config)#line vty 0 15
S1(config-line)#transport input ssh
S1(config-line)#login local
S1(config-line)#exit

S1(config)#ip ssh version 2
Please create RSA keys (of at least 768 bits size) to enable SSH v2.
S1(config)#crypto key generate rsa
The name for the keys will be: S1.ccna-lab.com
Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes.
How many bits in the modulus [512]: **1024**
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

S1(config)#ip ssh version 2
*Mar 2 2:25:34.837: %SSH-5-ENABLED: SSH 2 has been enabled
S1#config t

Encriptación de pass

S1(config)#service password-encryption
S1(config)#exit

Configurar la interfaz de administración (SVI)
S1(config)#int vlan 4
S1(config-if)#ip address 10.21.5.98 255.255.255.248
S1(config-if)#ipv6 address 2001:db5:acad:c::98/64
S1(config-if)#ipv6 address fe80::98 link-local
S1(config-if)#no shutdown
S1(config-if)#exit

Default gateway

S1(config)# ip default-gateway 10.21.5.97

Configuración s2

Switch>enable
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.

Desativar DNS

Switch(config)#no ip domain-lookup
Switch(config)#hostname S2
S2(config)#username admin secret admin1pass

CREACION DE DOMINIO

S2(config)#ip domain-name ccna-lab.com
S2(config)#enable secret ciscoenpass
S2(config)#line console 0
S2(config-line)#pass ciscoconpass
S2(config-line)#login
S2(config-line)#exit
S2(config)#

Line vty

S2(config)# line vty 0 15
S2(config-line)# login local
S2(config-line)#exit

S2(config)#line vty 0 15
S2(config-line)#transport input ssh
S2(config-line)#login local
S2(config-line)#exit
S2(config)#ip ssh version 2
Please create RSA keys (of at least 768 bits size) to enable SSH v2.

S2(config)#crypto key generate rsa
The name for the keys will be: S1.ccna-lab.com
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.
How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

S2(config)#ip ssh version 2
*Mar 2 2:25:34.837: %SSH-5-ENABLED: SSH 2 has been enabled

Encriptación de pass

S2#config t
S2(config)#service password-encryption
S2(config)#exit
S2 config# banner motd "toda persona que ingrese sin autorización será judicializado según las leyes establecidas"

Configurar la interfaz de administración (SVI)

S2(config)#int vlan 4
S2(config-if)#ip address 10.21.5.99 255.255.255.248
S2(config-if)#ipv6 address 2001:db5:acad:c::99/64
S2(config-if)#ipv6 address fe80::99 link-local
S2(config-if)#no shutdown
S2(config-if)#exit

Default gateway

S2(config)# ip default-gateway 10.21.5.97

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

Paso 4: configure S1

La configuración del S1 incluye las siguientes tareas:

Tabla 5 configuración S1

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

CREACION DE LAS VLAN

```
S1#config 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)#vlan 5
S1(config-vlan)#name Native
S1(config-vlan)#do wr
S1(config-vlan)#exit

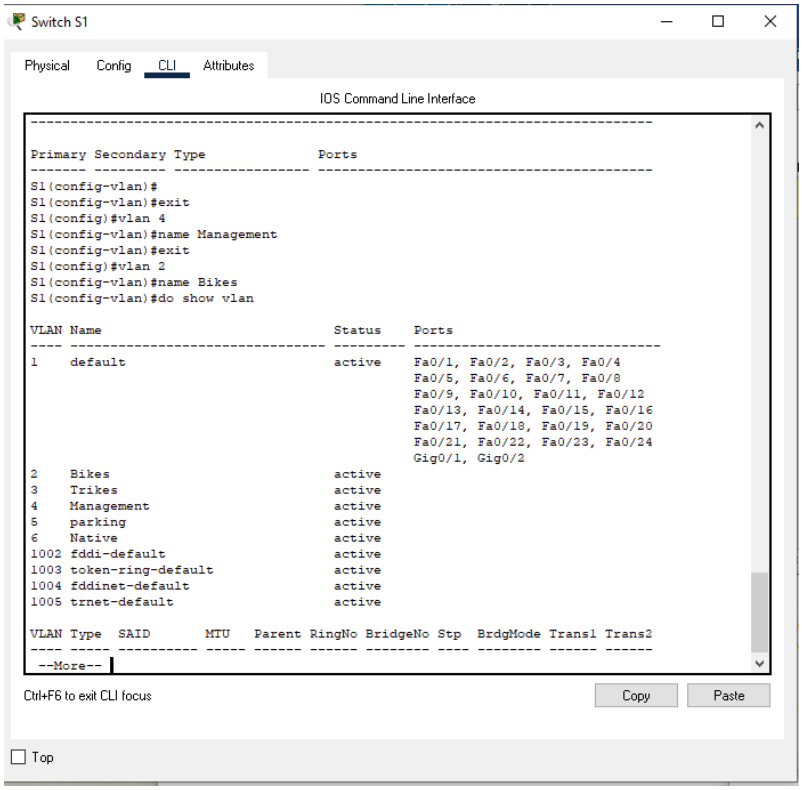


Ilustración 11 comando show vlan

Configuración mode acceso en las vlan

S1(config)#
S1(config)#interface f0/1
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 6
S1(config-if)#no sh

```
S1(config)#interface f0/2
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 6
S1(config-if)#no sh

S1(config-if)#interface f0/5
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 6
S1(config-if)#no sh
S1(config-if)#
```

Configuración mode trunk

```
S1(config)#int range f0/1-2, f0/5
S1(config-if-range)#switchport mode trunk
S1(config-if-range)#no shutdown
S1(config-if-range)#switchport trunk Native vlan 6
S1(config-if-range)#switchport trunk allowed vlan 2,3,4,6
```

Configuracion puerto de acceso para vlan 2

```
S1(config)#interface range f0/6
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 2
S1(config-if-range)#exit
S1(config)#do show vlan
```

Configuración ethernet channel

```
S1(config)#interface range f0/1,f0/2,f0/5
S1(config-if-range)#channel-group 1 mode active
S1(config-if-range)#interface port-channel 1
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk allowed vlan 2,3,4,5,6
S1(config-if)#do show etherchannel summary
```

Seguridad mac

```
S1(config)#
S1(config)#int f0/1
S1(config-if)#switchport mode acces
S1(config-if)#switchport port-security
S1(config-if)#switchport port-security maximum 3
```

```
S1(config-if)#exit
S1(config)#
S1(config)#int f0/2
S1(config-if)#switchport mode acces
S1(config-if)#switchport port-security
S1(config-if)#switchport port-security maximum 3
S1(config-if)#exit
S1(config)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan2, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan4, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan5, changed state to down

S1(config)#int f0/6
S1(config-if)#switchport mode acces
S1(config-if)#switchport port-security
S1(config-if)#switchport port-security maximum 3
S1(config-if)#exit
S1(config)#
```

Asegurar puertos

```
S1(config-if)#int range 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)#description not use
S1(config-if-range)#shut

S1(config-if-range)#int range g0/1-2
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 5
S1(config-if-range)#description not in use
S1(config-if-range)#sh
```

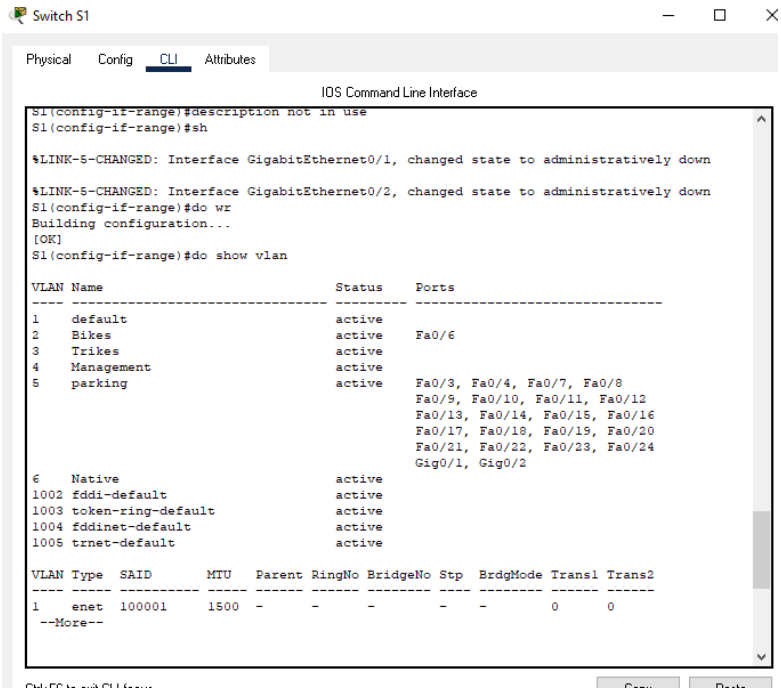


Ilustración 12 habilitado puerto f0/6

Paso 5: Configure el S2**.**

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

Tabla 6 Configuración S2

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
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 VLAN3	Interface F0/18

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

```
S2#config 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)#name Management
S2(config-vlan)#exit

S2(config-vlan)#vlan 5
S2(config-vlan)#name Native
S2(config-vlan)#do wr
S2(config-vlan)#exit
```

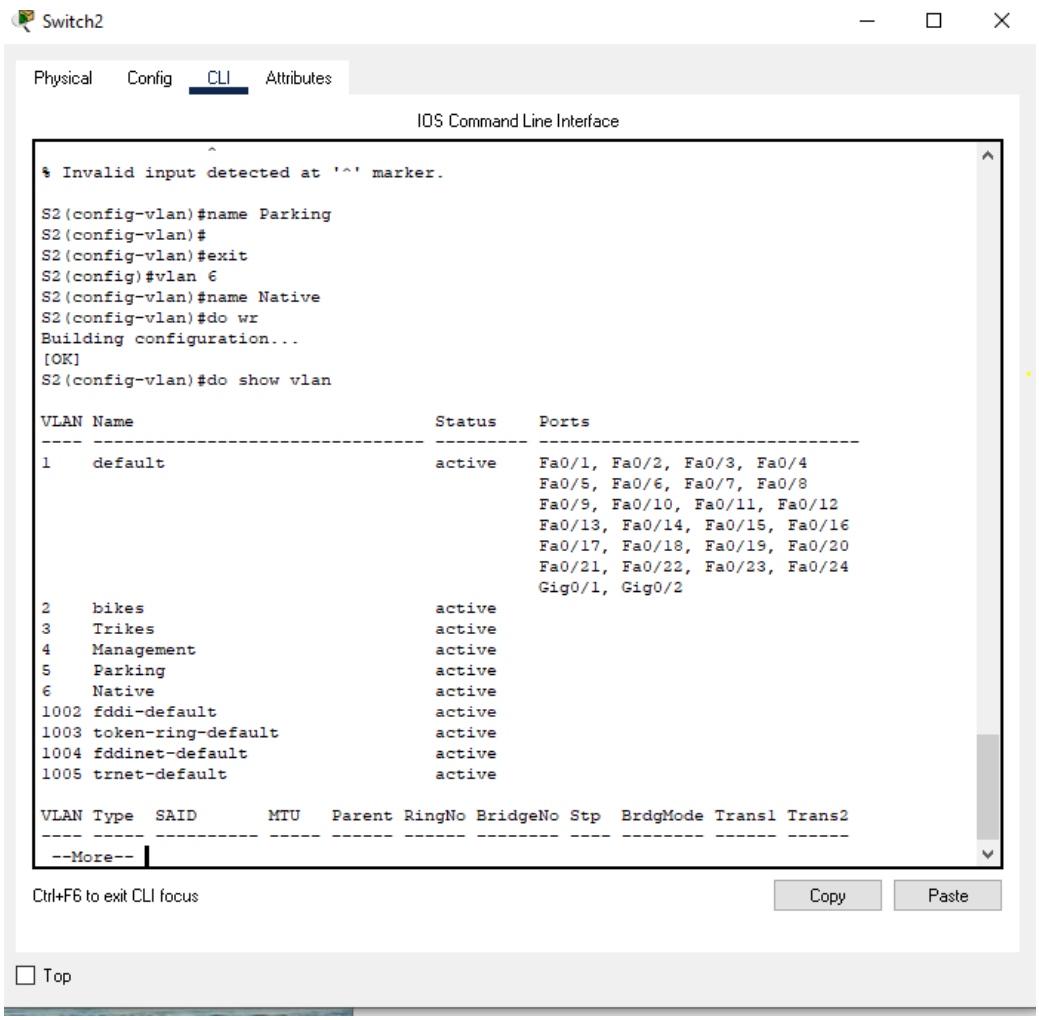


Ilustración 13 comando show vlan

S2#config t
S2(config)#interface f0/1
S2(config-if)#switchport mode acces
S2(config-if)#switchport access vlan 6
S2(config-if)#exit

S2(config)#int f0/2
S2(config-if)#switchport mode acces
S2(config-if)#switchport access vlan 6
S2(config-if)#exit

mode trunk

S2(config)#interface range f0/1-2
S2(config-if-range)#switchport mode trunk
S2(config-if-range)#no shutdown
S2(config-if-range)#switchport trunk native vlan 6
S2(config-if-range)#switchport trunk allowed vlan 2,3,4,6

Configuración puerto de acceso vlan

S2(config)#interface range f0/18
S2(config-if-range)#switchport mode access
S2(config-if-range)#switchport access vlan 3
S2(config-if-range)#do show vlan

Configuración ethernet channel

S2(config)#interface range f0/1-2
S2(config-if-range)#channel-group 1 mode active
S2(config-if-range)#interface port-channel 1
S2(config-if)#switchport mode trunk
S2(config-if)#switchport trunk allowed vlan 2,3,4 ,6
S2(config-if)#do show etherchannel summary

Seguridad mac

S2(config)#
S2(config)#int f0/1
S2(config-if)#switchport mode acces
S2(config-if)#switchport port-security
S2(config-if)#switchport port-security maximum 3
S2(config-if)#exit
S2(config)#
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/2 (1), with S1 FastEthernet0/2 (6).

S2(config)#int f0/2
S2(config-if)#switchport mode acces
S2(config-if)#switchport port-security
S2(config-if)#switchport port-security maximum 3
S2(config-if)#exit
S2(config)#

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan2, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan4, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan5, changed state to down

S2(config)#int f0/18
S2(config-if)#switchport mode acces
S2(config-if)#switchport port-security
S2(config-if)#switchport port-security maximum 3
S2(config-if)#exit
S2(config)#

Seguridad interfaces

S2(config)#int range f0/3-17,f0/19-24
S2(config-if-range)#switch mode access
S2(config-if-range)#switchpor access vlan 5
S2(config-if-range)#description not in use
S2(config-if-range)#sh

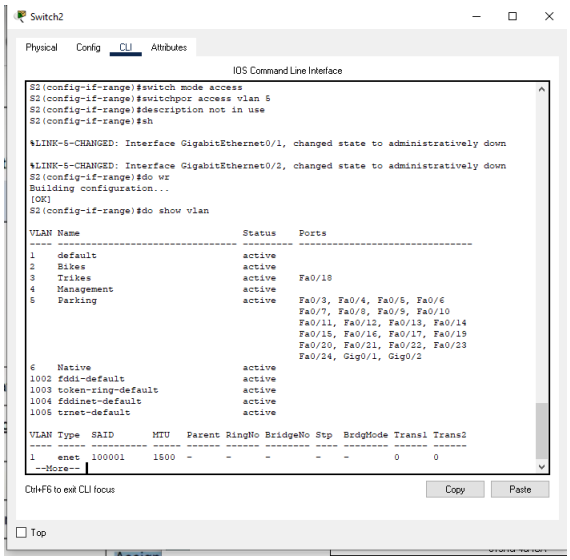


Ilustración 14 interface f0/18 asignada a vlan

Parte 2: configurar soporte host

Paso 1: configure R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 7 Configuracion R1

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

Default routa

```
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#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 ?
X:X:X:X::X/<0-128> IPv6 prefix
R1(config)#ipv6 route ::/0 loopback 0

R1(config)#
R1(config)#ip dhcp excluded-address 10.21.5.1 10.21.5.52
R1(config)#ip dhcp pool vlan2-bikes
R1(dhcp-config)#net 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)#exit
```

```
R1(config)#ip dhcp excluded-address 10.21.5.65 10.21.5.84
R1(config)#ip dhcp pool vlan3-Trikes
R1(dhcp-config)#net 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)#exit
R1(config)#do wr
Building configuration...
[OK]
R1(config)#
```

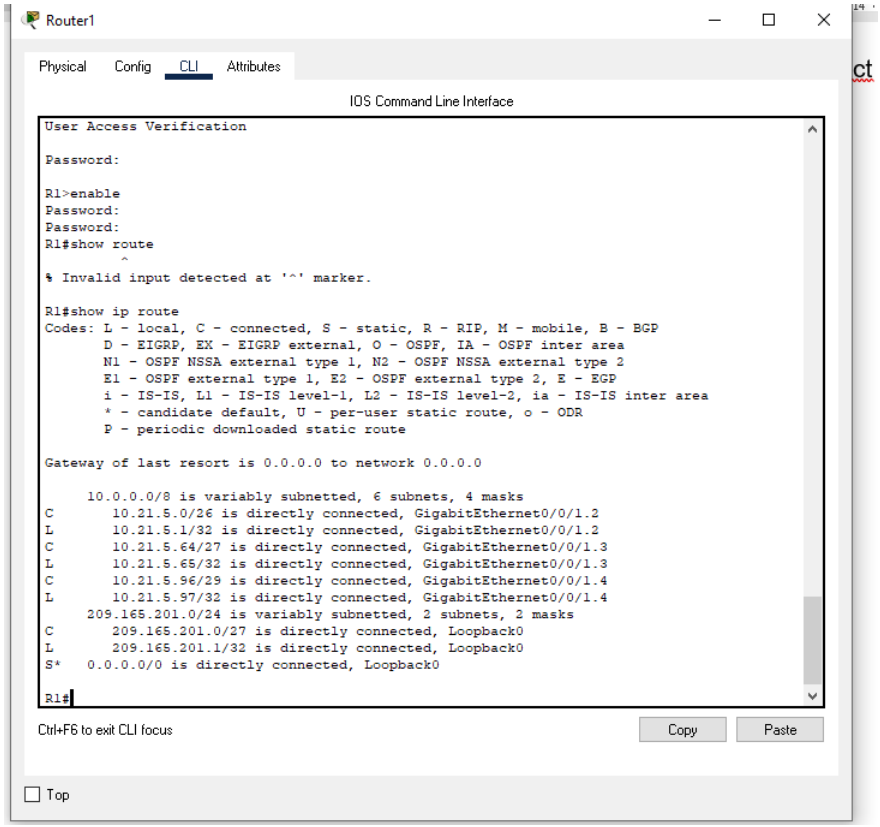


Ilustración 15 comando show ip route

Paso 2: Configurar los servidores

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

Tabla 8 configuración Network PC-A

PC-A Network Configuration	
Descripción	PCA
Dirección física	0001.4386.0127
Dirección IP	10.21.5.1
Máscara de subred	255.255.255.192

PC-A Network Configuration	
Gateway predeterminado	10.21.5.1
Gateway predeterminado IPv6	F80::1

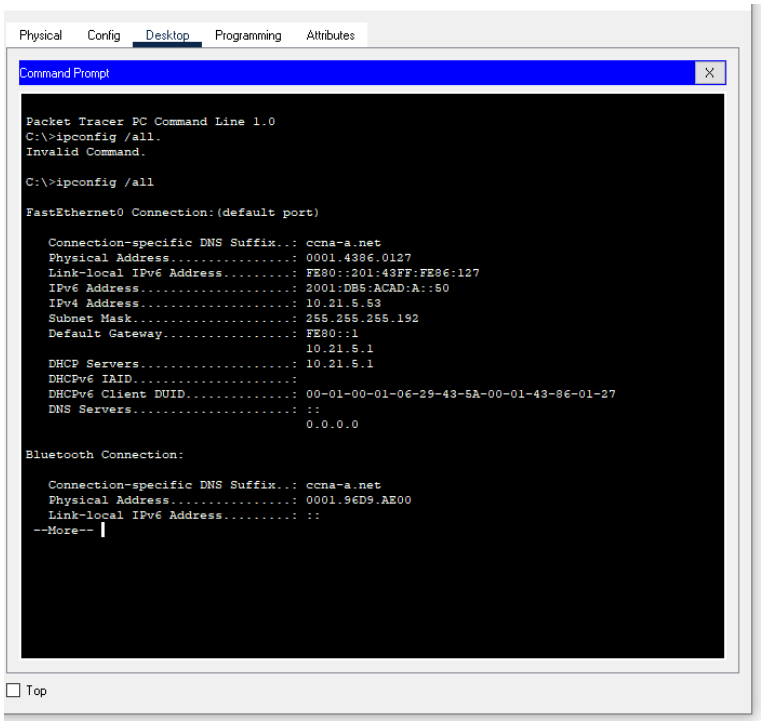


Ilustración 16 ipconfig /all pca

Tabla 9 configuración de Network PC-B

Configuración de red de PC-B	
Descripción	PC-B
Dirección física	00do.58.51E
Dirección IP	169.254.81.235
Máscara de subred	255.255.0.0
Gateway predeterminado	_____
Gateway predeterminado IPv6	FE80::1

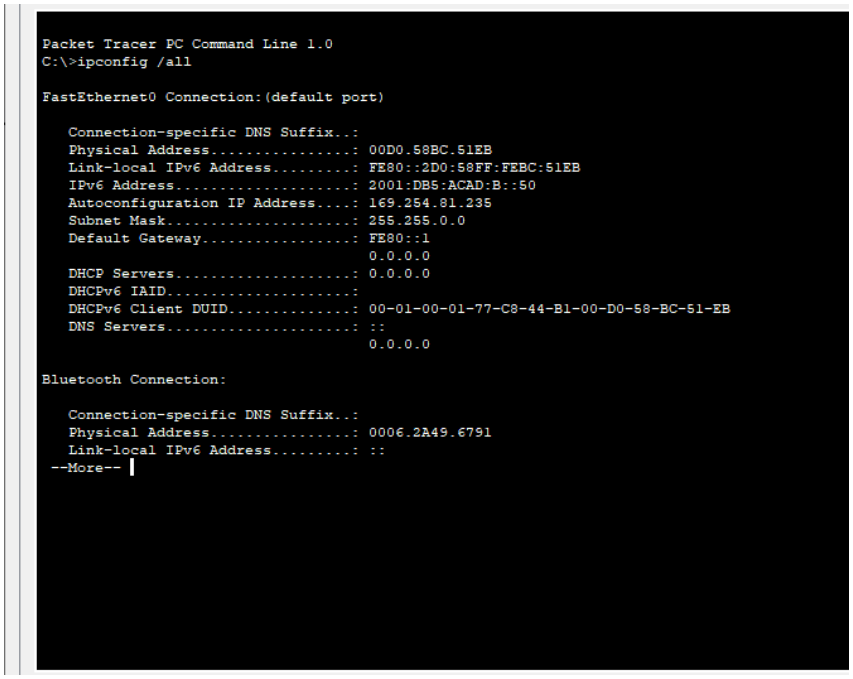


Ilustración 17 ipconfig /all pcb

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

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

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

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

Desde	A	de Internet	Dirección IP	Resultados de ping
PC-A	R1, G0/0/1.2	Dirección	10.21.5.1	ok
		IPv6	2001:db5:acad:a: :1	
	R1, G0/0/1.3	Dirección	10.21.5.65	ok
		IPv6	2001:db5:acad:b: :1	
	R1, G0/0/1.4	Dirección	10.21.5.97	ok
		IPv6	2001:db5:acad:c: :1	
	S1, VLAN 4	Dirección	10.21.5.98	ok
		IPv6	2001:db5:acad:c: :98	
	S2, VLAN 4	Dirección	10.21.5.99.	ok
		IPv6	2001:db5:acad:c: :99	
	PC-B	Dirección	IP address will vary.	
		IPv6	2001:db5:acad:b: :50	
	R1 Bucle 0	Dirección	209.165.201.1	

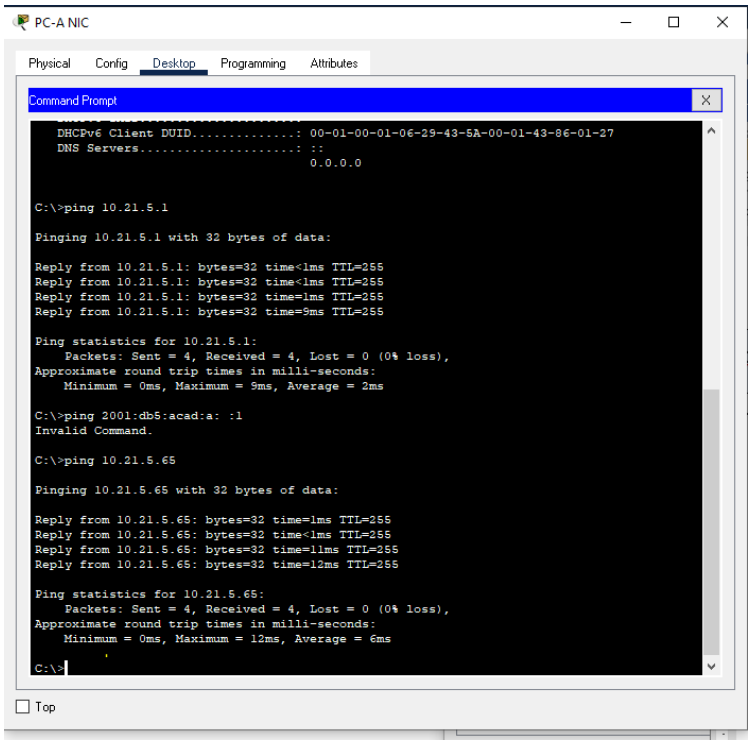


Ilustración 18 ping 10.21.5.1

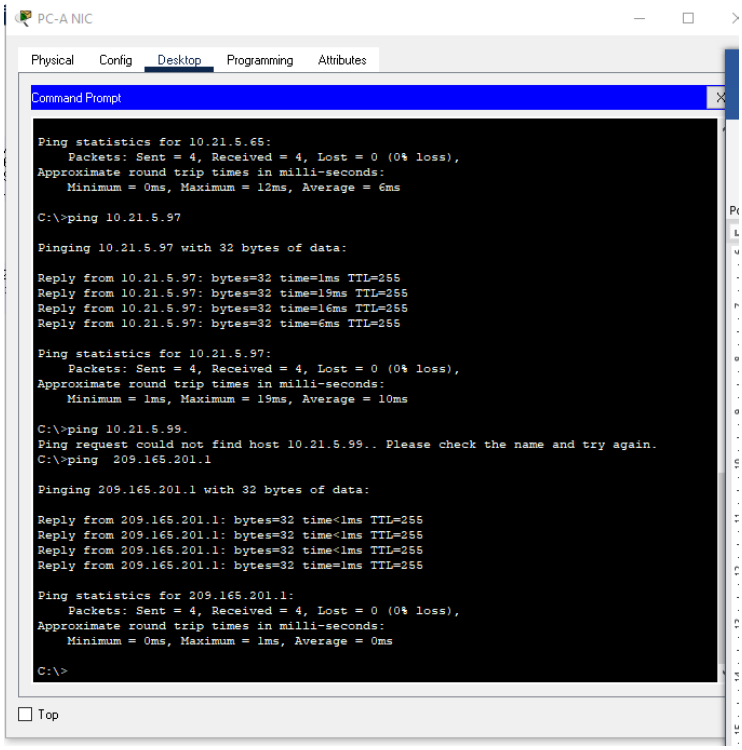
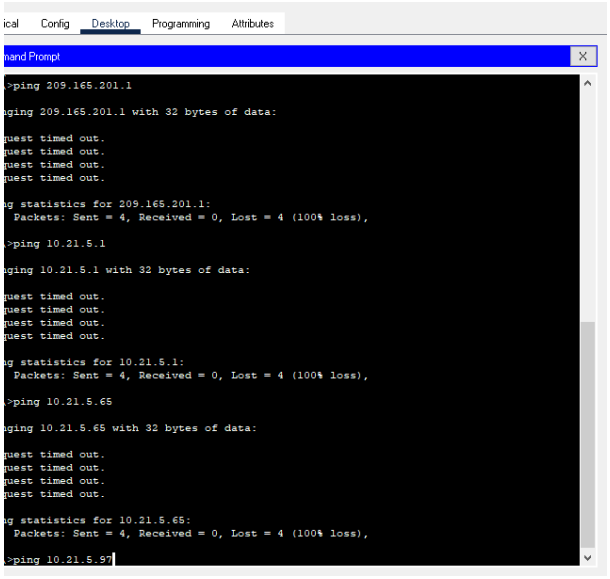
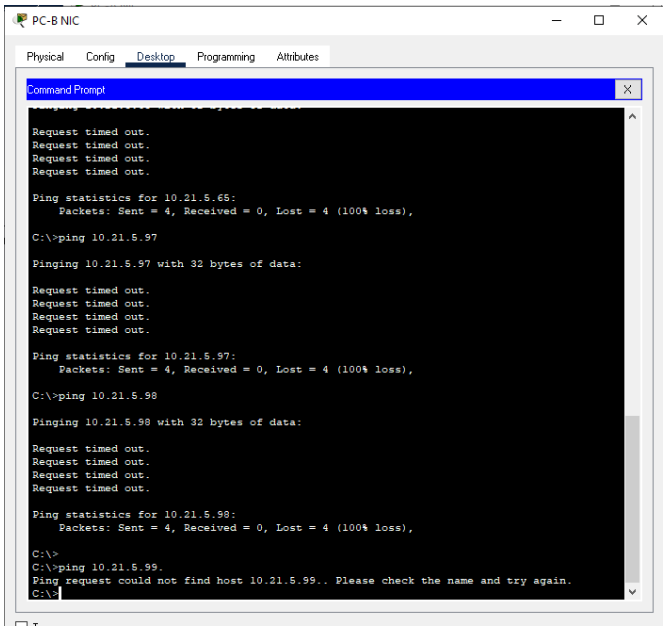


Ilustración 19 ping 10.21.5.99 10.21.5.97

Desde	A	de Internet	Dirección IP	Resultados de ping
		IPv6	2001:db5:acad:209: :1	
PC-B	R1 Bucle 0	Dirección	209.165.201.1	no
		IPv6	2001:db5:acad:209: :1	
	R1, G0/0/1.2	Dirección	10.21.5.1	no
		IPv6	2001:db5:acad:a: :1	
	R1, G0/0/1.3	Dirección	10.21.5.65	no
		IPv6	2001:db5:acad:b: :1	
	R1, G0/0/1.4	Dirección	10.21.5.97	no
		IPv6	2001:db5:acad:c: :1	
	S1, VLAN 4	Dirección	10.21.5.98	no
		IPv6	2001:db5:acad:c: :98	
	S2, VLAN 4	Dirección	10.21.5.99.	_____
		IPv6	2001:db5:acad:c: :99	

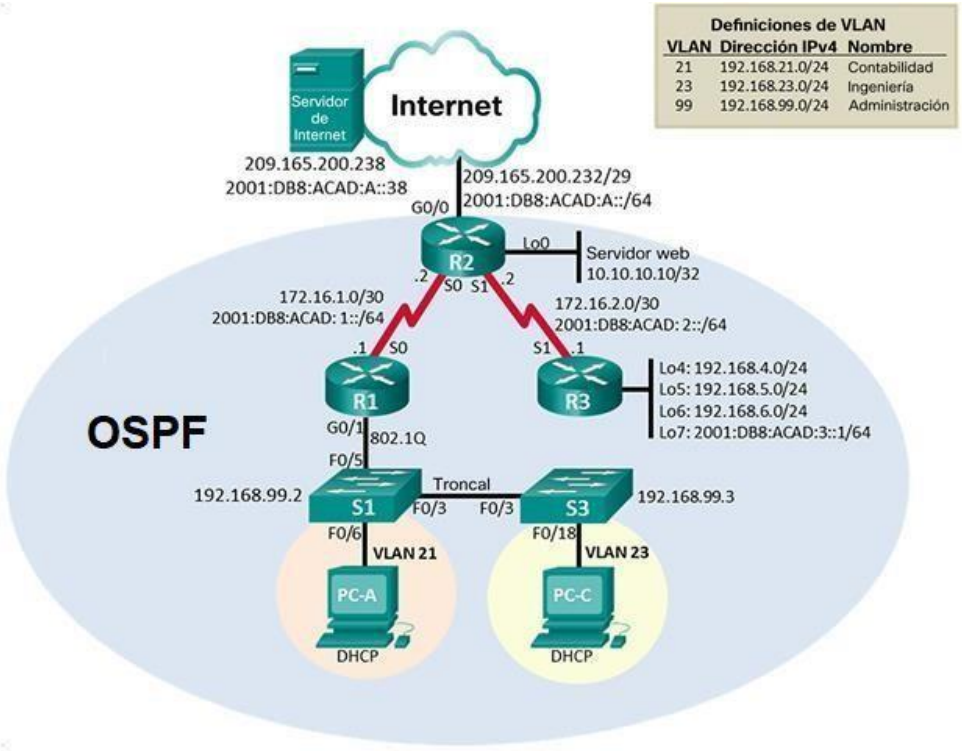



PC-B NIC
Physical
Config
Desktop
Programming
Attributes
Command Prompt
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 10.21.5.65:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 10.21.5.97
Pinging 10.21.5.97 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 10.21.5.97:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 10.21.5.98
Pinging 10.21.5.98 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 10.21.5.98:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>
C:\>ping 10.21.5.99.
Ping request could not find host 10.21.5.99.. Please check the name and try again.
C:\>

4. ESCENARIO 2

Se debe configurar una red pequeña para que admita conectividad IPv4 e IPv6, seguridad de switches, routing entre VLAN, el protocolo de routing dinámico OSPF, el protocolo de configuración de hosts dinámicos (DHCP), la traducción de direcciones de red dinámicas y estáticas (NAT), listas de control de acceso (ACL) y el protocolo de tiempo de red (NTP) servidor/cliente. Durante la evaluación, probará y registrará la red mediante los comandos comunes de CLI.

Topología



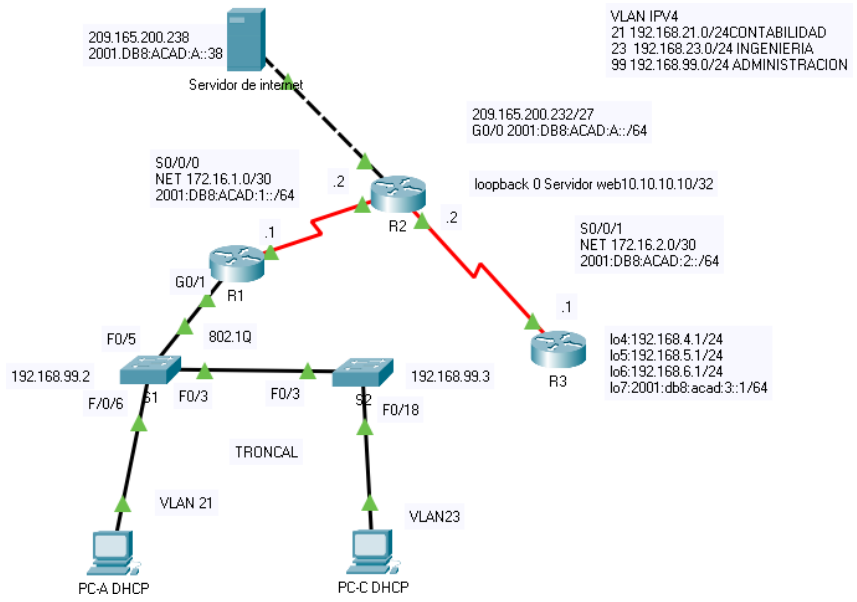


Ilustración 20 red implementada en packettrecer

Parte 1: inicializar dispositivos

Paso 1 inicializar y volver a cargar los routers y los switches

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

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

Tabla 10 iniciar y volver a cargar los dispositivos

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	**Erase startup-config**
Volver a cargar todos los routers	**reload**

Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	**Delete vlan.dat**
Volver a cargar ambos switches	**reload**
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	**Show flash**

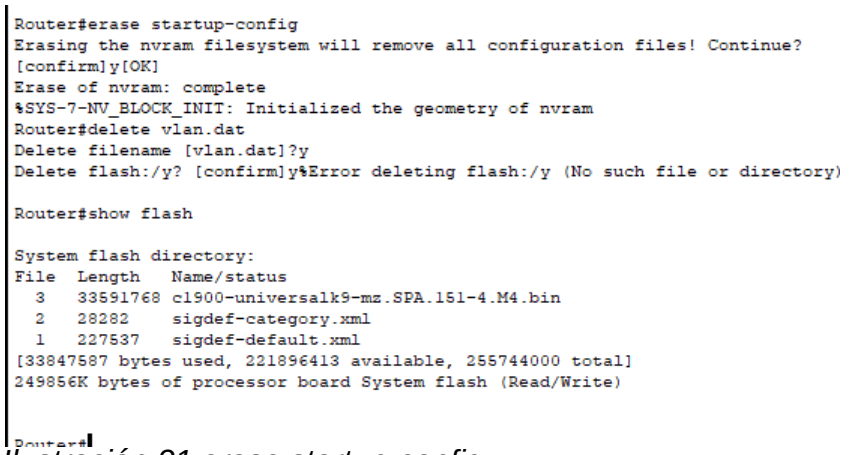


Ilustración 21 erase startup-config

Parte 2: Configurar los parámetros básicos de los dispositivos

Paso 1: configurar la computadora de internet

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

Tabla 11 configuración de pc de internet

Elemento o tarea de configuración	**Especificación**
Dirección IPv4	**209.165.200.238**
Máscara de subred para IPv4	255.255.255.224
Gateway predeterminado	209.165.200.225
Dirección IPv6/subred	2001:DB8:ACAD:A::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:2::1

Nota: Quizá sea necesario deshabilitar el firewall de las computadoras para que

los pings se realicen correctamente en partes posteriores de esta práctica de laboratorio.

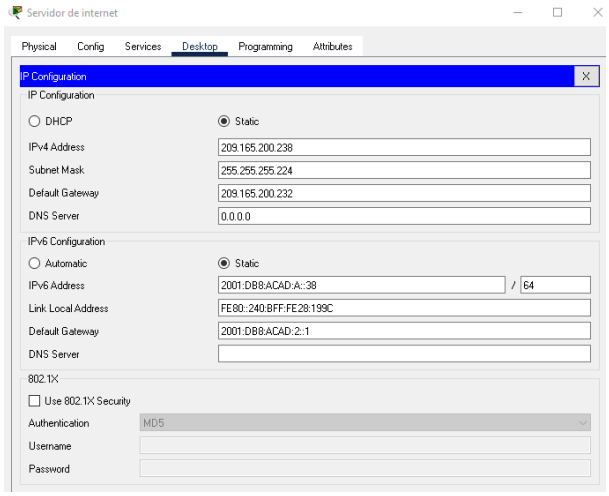


Ilustración 22 configuración pc de internet

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Nota: Todavía no configure G0/1.

Tabla 12 Configuración R1

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Router(config)#**no ip domain-lookup**
Nombre del router	R1
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	**Password service-encryption**
Mensaje MOTD	Se prohíbe 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
Rutas predeterminadas	Configurar una ruta IPv4 predeterminada de S0/0/0 Configurar una ruta IPv6 predeterminada de S0/0/0

Desactivar la búsqueda DNS

Router#config
Router(config)#no ip domain-lookup

Configuración básica

Router(config)#hostname R1
R1(config)#enable secret class
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit

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

Configuración de interfaces ipv4 y ipv6

```
R1(config)#int s0/0/0
R1(config-if)#ip add 172.16.1.1 255.255.255.252
R1(config-if)#clock rate 128000
R1(config-if)#no sh
R1(config-if)#ipv6 add 2001:DB8:ACAD:1::1/64
R1(config-if)#clock rate 128000
R1(config-if)#no sh
```

Ruteo por defecto

```
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
```

Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Tabla 13 configurar R1

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Router(config)#**no ip domain-lookup**
Nombre del router	R2
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	**Password service-encryption**
Habilitar el servidor HTTP	**ip http server** **ip http secure-server**

	ip http authentication local no esta disponible en simulador
Mensaje MOTD	Se prohíbe el acceso no autorizado.
Interfaz S0/0/0	Establezca la descripción Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz
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
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
Interfaz loopback 0 (servidor web simulado)	Establecer la descripción. Establezca la dirección IPv4.
Ruta predeterminada	Configure una ruta IPv4 predeterminada de G0/0. Configure una ruta IPv6 predeterminada de G0/0.

Desactivar la búsqueda DNS

Router(config)#no ip domain-lookup

Configuración básica

Router(config)#hostname R2
R2(config)#enable secret class
R2(config)#line console 0
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#exit
R2(config)#
R2(config)#line vty 0 15
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#exit
R2(config)#service password-encryption
R2(config)#banner motd ‘Prohibido el acceso no autorizado’

Configuración de interfaces ipv4 y ipv6

R2(config)# int s0/0/0
R2(config-if)#ip address 172.16.1.2 255.255.255.252
R2(config-if)#ipv6 address 2001:db8:acad:1::2/64
R2(config-if)# clock rate 128000
R2(config-if)#no shutdown
R2(config-if)#exit

R2(config)# int s0/0/1
R2(config-if)#ip address 172.16.2.1 255.255.255.252
R2(config-if)#ipv6 address 2001:db8:acad:2::1/64
R2(config-if)# clock rate 128000
R2(config-if)#no shutdown
R2(config-if)#exit

R2(config)# int g0/0
R2(config-if)#description R2 --> Internet
R2(config-if)#ip address 209.165.200.232 255.255.255.224
R2(config-if)#ipv6 address 2001:db8:acad:A::1/64
R2(config-if)#no shutdown
R2(config-if)#exit

Configuración interfaces loopback 0

R2(config)# int loopback 0
R2(config-if)#ip address 10.10.10.10 255.255.255.255
R2(config-if)#exit

Ruteo por defecto

R2(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0
R2(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1
R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0
ipV6 route ::/0 g0/0

Paso 4: configurar R3

La configuración del R3 incluye las siguientes tareas:

Tabla 14 Configuración R3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	**No ip domain-lookup**
Nombre del router	R3
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	**Password service-encryption**
Mensaje MOTD	Se prohíbe 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
Interfaz loopback 4	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.
Interfaz loopback 5	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.

Interfaz loopback 6	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.
Interfaz loopback 7	Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.

Desactivar la búsqueda DNS

Router(config)#no ip domain-lookup

Configuración básica

Router(config)#hostname R3
R3(config)#enable secret class
R3(config)#line console 0
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#exit
R3(config)#line vty 0 4
R3(config-line)#password cisco
R3(config-line)#exit
R3(config)#service password-encryption
R3(config)#banner motd #"se prohibe el acceso no autorizado"#

Configuración de interfaces ipv4 y ipv6

R3(config)#int s0/0/1
R3(config-if)#ip add 172.16.2.1 255.255.255.252
R3(config-if)#clock rate 128000
R3(config-if)#no sh
R3(config-if)#ipv6 add 2001:DB8:ACAD:2::1/64
R3(config-if)#clock rate 128000
R3(config-if)#no sh
R3(config-if)#exit

Configuración interfaces loopback 4,5,6 y 7

R3(config)#int loopback 4
R3(config-if)#ip add 192.168.4.1 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit

```
R3(config)#int loopback 5
R3(config-if)#ip add 192.168.5.1255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit

R3(config)#int loopback 6
R3(config-if)#ip add 192.168.6.1 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit

R3(config)#int loopback 7
R3(config-if)#ipv6 add 2001:DB8:ACAD:3::1/64
R3(config-if)#no shutdown
R3(config-if)#exit
```

Ruteo por defecto

```
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
```

Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 15 configuración s1

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	**No ip domain-lookup**
Nombre del switch	S1
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	**Service password-encryption**
Mensaje MOTD	Se prohíbe el acceso no autorizado.

Desactivar la búsqueda de DNS

Switch(config)#**no ip domain-lookup**

Configuración básica

Switch(config)#hostname S1
S1(config)#enable secret class
S1(config)#line console 0
S1(config-line)#pass cisco
S1(config-line)#login
S1(config-line)#exit
S1(config)#line vty 0 15
S1(config-line)#pass cisco
S1(config-line)#login
S1(config-line)#exit
S1(config)#service password-encryption
S1(config)#banner motd #"Se prohibe el acceso no autorizado."#

Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 16 configurar s3

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	**No ip domain-lookup**
Nombre del switch	S3
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	**service password-encryption**
Mensaje MOTD	Se prohíbe el acceso no autorizado.

Desativar la búsqueda de DNS

Switch(config)#**no ip domain-lookup**

Configuración Básica
Switch(config)#hostname S1
S1(config)#enable secret class
S1(config)#line console 0
S1(config-line)#pass cisco
S1(config-line)#login

```
S1(config-line)#exit
S1(config)#line vty 0 15
S1(config-line)#pass cisco
S1(config-line)#login
S1(config-line)#exit
S1(config)#service password-encryption
S1(config)#banner motd #"Se prohibe el acceso no autorizado."#
```

Paso 7: Verificar la conectividad de la red

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

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

Tabla 17 verificar la conectividad de la red

Desde	**A**	**Dirección IP**	**Resultados de ping**
R1	R2, S0/0/0	172.16.1.2	0k
R2	R3, S0/0/1	172.16.2.1	ok
PC de Internet	Gateway predeterminado	209.165.200.225	No

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

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

Paso 1: configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 18 configurar S1

Elemento o tarea de configuración	**Especificación**
Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para topología para crear y nombrar cada una de las VLAN que se indican
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
Asignar el gateway predeterminado	Asigne la primera dirección IPv4 de la subred como el gateway predeterminado.
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa
Forzar el enlace troncal en la interfaz F0/5	Utilizar la red VLAN 1 como VLAN nativa
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range
Asignar F0/6 a la VLAN 21	**Int f0/6** **Switchport mode access** **Swichport access VLAN21**
Apagar todos los puertos sin usar	**int range f0/1-2,f0/4,f0/7-24,g0/1-2** **sh**

Creación base de datos vlan

S1(config)#vlan 21
S1(config-vlan)#name contabilidad
S1(config-vlan)#vlan 23
S1(config-vlan)#name ingenieria
S1(config-vlan)#vlan 99
S1(config-vlan)#name administración

Asignación de interface a la vlan administración

S1(config-vlan)#int vlan 99
S1(config-if)#ip add 192.168.99.2 255.255.255.0
S1(config-if)#no sh

Asignación de puerta de enlace

S1(config)#ip defaul-gateway 192.168.99.1
S1(config-if)#exit

Creación de las troncales en las interfaces f0/3,f0/5

S1(config)#int f0/3
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 1
S1(config-if)#exit

S1(config)#int f0/5
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 1
S1(config-if)#exit

Habilitar puertos de acceso

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

S1(config)#int f0/6
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 21
S1(config-if)#exit

Deshabitar puertos que no estan en uso

S1(config)#int range f0/1-2,f0/4,f0/7-24,g0/1-2
S1(config-if-range)#sh

Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 19 configurar S3

Elemento o tarea de configuración	**Especificación**
Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para topología para crear cada una de las VLAN que se indican Dé nombre a cada VLAN.
Asignar la dirección IP de administración	Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S3 en el diagrama de topología
Asignar el gateway predeterminado.	Asignar la primera dirección IP en la subred como gateway predeterminado.
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range
Asignar F0/18 a la VLAN 21	**Int f0/18** **Switchport mode access** **Switchport access VLAN21**
Apagar todos los puertos sin usar	**int range f0/1-2,f0/4-17,f0/19-24,g0/1-2** **sh**

Creación de base de datos 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 administración

Asignación de interface a la vlan administración

S3(config)#int vlan 99
S3(config-if)#ip add 192.168.99.3 255.255.255.0

Asignación de puerta de enlace

S3(config-if)#ip default-gateway 192.168.99.1
S3(config)#exit

Creación de las troncales en las interface f0/3

S3(config)#int f0/3
S3(config-if)#switchport mode trunk
S3(config-if)#switchport trunk native vlan 1
S3(config-if)#exit

Habilitar puertos de acceso

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

S3(config)#int f0/18
S3(config-if)#switchport mode acces
S3(config-if)#switchport access vlan 21

Deshabitar puertos que no estan en uso

S3(config-if)#int range f0/1-2,f0/4-17,f0/19-24,g0/1-2
S3(config-if-range)#sh

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 20 configurar R1

Elemento o tarea de configuración	**Especificación**
Configurar la subinterfaz 802.1Q .21 en G0/1	Descripción: LAN de Contabilidad Asignar la VLAN 21 Asignar la primera dirección disponible a esta interfaz
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
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
Activar la interfaz G0/1	**Int g0/1** **No sh**

Configuración de subinterfaces 802.1Q .21, .23, .99 en g0/1

```
R1(config)#int g0/1.21
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)#int g0/1.23
R1(config-subif)#encapsulation dot1q 23
R1(config-subif)#description LAN de ingenieria
R1(config-subif)#ip add 192.168.23.1 255.255.255.0
R1(config-subif)#exit

R1(config)#int g0/1.99
R1(config-subif)#encapsulation dot1q 99
R1(config-subif)#description LAN de administracion
R1(config-subif)#ip add 192.168.99.1 255.255.255.0
R1(config-subif)#exit
R1(config)#int g0/1
R1(config-if)# no sh
```

Paso 4: Verificar la conectividad de la red

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

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

Tabla 21 Verificar conectividad de la red

Desde	**A**	**Dirección IP**	**Resultados de ping**
S1	R1, dirección VLAN 99	192.168.99.1	ok
S3	R1, dirección VLAN 99	192.168.99.1	ok
S1	R1, dirección VLAN 21	192.168.21.1	ok
S3	R1, dirección VLAN 23	192.168.23.1	ok

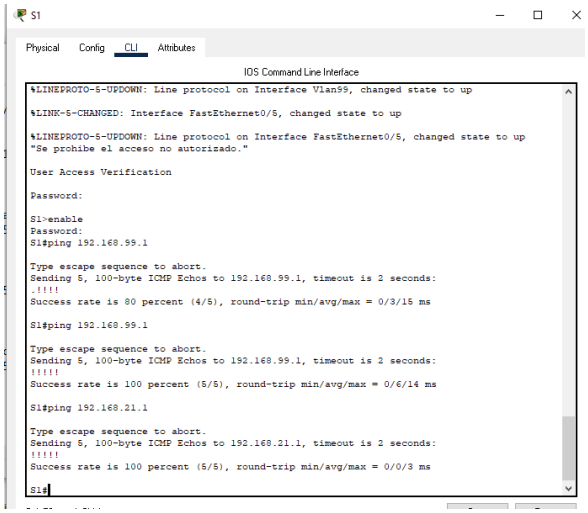


Ilustración 23 ping 192.168.99.1

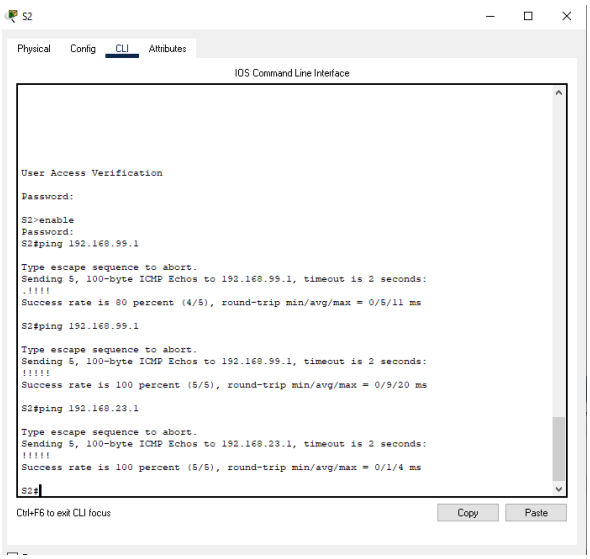


Ilustración 24 ping 192.168.23.1

Parte 4: Configurar el protocolo de routing dinámico OSPF

Paso 1: Configurar OSPF en el R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 22 Protocolo OSPF R1

Elemento o tarea de configuración	**Especificación**
Configurar OSPF área 0	**Router ospf 1**
Anunciar las redes conectadas directamente	network 172.16.1.0 0.0.0.3 area 0 network 192.168.21.0 0.0.0.255 area 0 network 192.168.1.23 0.0.0.255 area 0 network 192.168.1.99 0.0.0.255 area 0
Establecer todas las interfaces LAN como pasivas	**Passive-interface g0/1**
Desactive la sumarización automática	**Router rip** **No auto-summary**

Configuración OSPF área 0

R1(config)#router ospf 1
R1(config-router)#router-id 1.1.1.1

Anunciar 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 192.168.1.23 0.0.0.255 area 0
R1(config-router)#network 192.168.1.99 0.0.0.255 area 0
R1(config-router)#

Establecer todas las interfaces LAN como pasivas

R1(config-router)#passive-interface g0/1.21
R1(config-router)#passive-interface g0/1.23
R1(config-router)#passive-interface g0/1.99
R1(config-router)#exit

Desactive la sumarización automática

R1(config)#router rip
R1(config-router)#no auto-summary
02:51:14: %OSPF-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Serial0/0/0 from LOADING to FULL, Loading Done

Paso 2: Configurar OSPF en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla 23 Protocolo OSPF R2

Elemento o tarea de configuración	**Especificación**
Configurar OSPF área 0	**Router ospf 1**
Anunciar las redes conectadas directamente	**Nota:** Omitir la red G0/0.
Establecer la interfaz LAN (loopback) como pasiva	**Passive-interface g0/1**
Desactive la sumarización automática.	**router rip** **no auto-summary**

Configurar OSPF área 0

R2(config)#router ospf 1
R2(config-router)#router-id 2.2.2.2

Anunciar las redes conectadas directamente

```
R2(config-router)#network 172.16.1.0 0.0.0.3 area 0
R2(config-router)#network 172.16.2.0 0.0.0.3 area 0
R2(config-router)#network 10.10.10.10 0.0.0.255 area 0
R2(config-router)#
```

Establecer la interfaz LAN (loopback) como pasiva

```
R2(config-router)#passive-interface g0/1
R2(config-router)#exit
```

Desactive la sumarización automática.

```
R2(config)#router rip
R2(config-router)#no auto-summary
R2(config-router)#
```

Paso 3: Configurar OSPF en el R3

La configuración del R3 incluye las siguientes tareas:

Tabla 24 configuracion OSPF R3

Elemento o tarea de configuración	**Especificación**
Configurar OSPF área 0	**Router ospf 1**
Anunciar redes IPv4 conectadas directamente	**network 172.16.2.0 0.0.0.3 area 0** **network 192.168.4.0 0.0.3.255 area 0**
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	**passive-interface loopback**
Desactive la sumarización automática.	**router rip** **no auto-summary**

Configurar OSPF área 0

```
R3>en
R3#conf t
R3(config)#router ospf 1
R3(config-router)#router-id 3.3.3.3
R3(config-router)#
```

Anunciar redes IPv4 conectadas directamente

```
R3(config-router)#network 172.16.2.0 0.0.0.3 area 0
R3(config-router)#network 192.168.4.0 0.0.3.255 area 0
R3(config-router)#
```

Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas

```
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
```

Paso 4: Verificar la información de OSPF

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

Tabla 25 verificar OSPF

Pregunta	**Respuesta**
¿Con qué comando se muestran la ID del proceso OSPF, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router?	**Show ip protocols**
¿Qué comando muestra solo las rutas OSPF?	**Show ip route ospf**
¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	**Show running-config**

Parte 5: Implementar DHCP y NAT para IPv4

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

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 26 configurar R1 como servidor VLAN 21 Y 23

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	**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	**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
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

Reservar las primeras 20 direcciones vlan 21

R1(config)# ip dhcp excluded-address 192.168.21.1 192.168.21.20

Reservar las primeras 20 direcciones vlan 23

R1(config)# ip dhcp excluded-address 192.168.23.1 192.168.23.20

Crear un pool de DHCP para la VLAN 21.

R1(config)#ip dhcp pool vlan21
R1(dhcp-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)#

Crear un pool de DHCP para la VLAN 23

R1(config)#ip dhcp pool vlan23
R1(dhcp-config)#ip dhcp pool acct
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)#

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

La configuración del R2 incluye las siguientes tareas:

Tabla 27 configuración NAT estática y dinamica

Elemento o tarea de configuración	**Especificación**
Crear una base de datos local con una cuenta de usuario	Nombre de usuario: **webuser** Contraseña: **cisco12345** Nivel de privilegio: **15**
Habilitar el servicio del servidor HTTP	**No es valido en packet trecer**- ip http server
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	**No es valido en packet trecert**-ip http authentication
Crear una NAT estática al servidor web.	Dirección global interna: **209.165.200.229**
Asignar la interfaz interna y externa para la NAT estática	**ip nat outside** **ip nat inside**
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
Defina el pool de direcciones IP públicas utilizables.	Nombre del conjunto: **INTERNET** El conjunto de direcciones incluye: **209.165.200.225** – **209.165.200.228**
Definir la traducción de NAT dinámica	

Crear una base de datos local con una cuenta de usuario

```
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#user webuser privilege 15 secret cisco12345
Router(config)#ip http server “no valido en el simulador”
^
% Invalid input detected at '^' marker.
Router(config)#ip http authentication “no valido em el simulador”
^
% Invalid input detected at '^' marker.
```

Crear una NAT estática al servidor web.

```
Router(config)#ip nat  inside source static 10.10.10.10 209.165.200.229
```

Asignar la interfaz interna y externa para la NAT estática

```
Router(config)#int g0/0
Router(config-if)#ip nat outside
Router(config-if)#exit
Router(config)#

Router(config)#int g0/1
Router(config-if)#ip nat inside
Router(config-if)#exit
```

Configurar la NAT dinámica dentro de una ACL privada

```
Router(config)#access-list 1 permit 192.168.21.0 0.0.0.255
Router(config)#access-list 1 permit 192.168.23.0 0.0.0.255
Router(config)#access-list 1 permit 192.168.4.0 0.0.3.255
```

Defina el pool de direcciones IP públicas utilizables.

```
Router(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask
255.255.255.224
Router(config)#ip nat inside source list 1 pool INTERNET
```

Paso 3: Verificar el protocolo DHCP y la NAT estática

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

Tabla 28 verificar el protocolo DHCP y NAT estática

Prueba	**Resultados**
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	ok
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	Ok
Verificar que la PC-A pueda hacer ping a la PC-C **Nota:** Quizá sea necesario deshabilitar el firewall de la PC.	ok
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**	NO debido a que el simulador no permite crear los servicios http

Parte 6: Configurar NTP

Tabla 29 Configurar NTP

Elemento o tarea de configuración	**Especificación**
Ajuste la fecha y hora en R2.	**5 de marzo de 2016, 9 a. m.**
Configure R2 como un maestro NTP.	Nivel de estrato: **5**
Configurar R1 como un cliente NTP.	Servidor: **R2**
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	**ntp update-calendar**
Verifique la configuración de NTP en R1.	**Show ntp associations**

Ajuste la fecha y hora

R2#clock set 09:00:00 5 March 2016
R2#config t

Configure R2 como un maestro NTP.

R2(config)#ntp master 5

Configurar R1 como un cliente NTP.

R1(config)#ntp server 172.16.1.1

Configure R1 para actualizaciones de calendario periódicas con hora NTP.

R1(config)#ntp update-calendar

Verifique la configuración de NTP en R1.

R1(config)#do show ntp associations

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

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

Tabla 30 configurar listas de control (ACL)

Elemento o tarea de configuración	**Especificación**
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	Nombre de la ACL: **ADMIN-MGT** ip access-list standard ADMIN-MGT
Aplicar la ACL con nombre a las líneas VTY	line vty 0 4
Permitir acceso por Telnet a las líneas de VTY	access-class ADMIN-MGT in
Verificar que la ACL funcione como se espera	172.16.2.1#telnet172.16.2.2

Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2

R1(config)#ip access-list standard ADMIN-MGT

Aplicar la ACL con nombre a las líneas VTY

R1(config-std-nacl)#host 172.16.1.1

Permitir acceso por Telnet a las líneas de VTY

172.16.1.1(config)#line vty 0 4
172.16.1.1(config-line)#access-class ADMIN-MGT in
172.16.1.1(config-line)#exit
172.16.1.1(config)#exit

Verificar que la ACL funcione como se espera

172.16.1.1#telnet 172.16.2.2
172.16.1.2#telnet 172.16.2.1

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

Tabla 31 Comandos access list

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	**Show access list**
Restablecer los contadores de una lista de acceso	**Clear ip access-list counters**
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	**Show running-config**

¿Con qué comando se muestran las traducciones NAT?	**Nota:** Las traducciones para la PC-A y la PC-C se agregaron a la tabla cuando la computadora de Internet intentó hacer ping a esos equipos en el paso 2. Si hace ping a la computadora de Internet desde la PC-A o la PC-C, no se agregarán las traducciones a la tabla debido al modo de simulación de Internet en la red. **show ip nat translations**
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	**clear ip nat translation**

CONCLUSIONES

Con este diplomado se desarrolló, analizó y se identificó el comportamiento de la red, donde se configuran los dispositivos, se configuran las interfases, se crean las VLAN, las interfases LOOPBACK, se troncaliza las interfases, se creó un servidor de DHCP y Web.

Se configuran los diferentes dispositivos pc, router, suiche, desarrollas mediante los escenarios de la actividad.

Mediante los comandos SHOW se verifican las diferentes configuraciones de los dispositivos y su correcto funcionamiento, con el comando PING se identifica la conectividad y sus problemas.

Con el programa de simulación Packet Tracer se pone en práctica los diferentes comandos y tipos de configuración propuestos en los comandos.

Mediante el desarrollo del proceso se aplicaron los conocimientos adquiridos en CCNA 1 R&S: Introduction to Networks y CCNA 2 R&S: Routing and Switching Essentials.

BIBLIOGRAFÌA

CISCO. (2019). NAT para IPv4. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#9

CISCO. (2019). Detección, Administración y Mantenimiento de Dispositivos. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-courseassets.s3.amazonaws.com/RSE6/es/index.html#10

CISCO. (2019). Listas de Control de Acceso. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#7

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

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

CISCO. (2019). Capa de aplicación. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#10

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

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

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#2

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). Configuración del Switch. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#5

CISCO. (2019). Detección, Administración y Mantenimiento de Dispositivos. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#10

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

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-course-assets.s3.amazonaws.com/ITN6/es/index.html#8

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

CISCO. (2019). Listas de Control de Acceso. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#7

CISCO. (2019). NAT para IPv4. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#9

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

CISCO. (2019). Redes Conmutadas. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#4

ANEXOS

Enlace de las simulaciones en packettrecert

https://drive.google.com/drive/folders/1g3TKDxcBC91rDNFli2Gwd5LT0GPCrC12?usp=sharing

Diplomado De Profundización Cisco (Diseño E Implementación De Soluciones Integradas LAN / WAN)

Jorge Ivan Giraldo Alarcon *Universidad Nacional Abierta y a Distancia (UNAD), jigiraldoa@unadvirtual.edu.co*

Articulo

Resumen—Cisco Networking Academy es un programa global de educación en ciberseguridad y TI que se asocia con instituciones de aprendizaje de todo el mundo para empoderar a todas las personas con oportunidades profesionales.

El DIPLOMADO DE PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN) (OPCI) permite crear soluciones a través de del simulador packtracer para analizar diversos protocolos y procedimientos de enrutamiento, estático, dinámico, creación de servidores de DHCP y Web basado en un esquema de direccionamiento de IP y IPV6 para dar solución a los requerimientos de seguridad y de conectividad de las diferentes VLAN

A través de la aplicación del simulador se coloca en práctica los diferentes comandos en los suiches y router donde se logra identificar su comportamiento a la hora de la interconexión de los mismos, identificando la seguridad, la división de las sub redes y la comunicación.

Abstract--Cisco Networking Academy is a global IT and cybersecurity education program that partners with learning institutions around the world to empower all people with career opportunities.

The CISCO DEEPENING DIPLOMA (DESIGN AND IMPLEMENTATION OF INTEGRATED LAN / WAN SOLUTIONS) (OPCI) allows you to create solutions through the packtracer simulator to analyze various protocols and routing procedures, static, dynamic, creation of DHCP servers and Web-based an IP and IPV6 addressing scheme to solve the security and connectivity requirements of the different VLANs

Through the application of the simulator, the different commands are put into practice in the switches and routers where it is possible to identify their behavior when interconnecting them, identifying security, the division of sub-networks and communication.

INTRODUCCIÓN

Este diplomado CISCO es importante porque permite afianzar los conocimientos adquiridos en el desarrollo de la carrera, colocando en práctica la configuración de redes, enrutamiento y la creación de la VLAN.

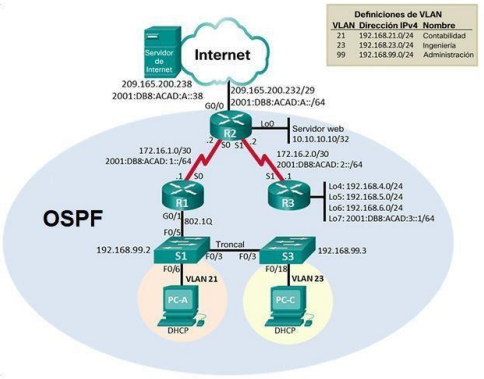
Se plantea una metodología para la creación a través de simulación de las diferentes configuraciones de los dispositivos (routers, switches, pc).

Es muy importante el desarrollo de este proyecto dado que permite la preparación para la vida laboral de los futuros ingenieros contando con preparación en redes, permitiendo unificar los ejes del ser con el hacer y contar así con experiencia para unirse al mundo laboral en esta área.

ESCENARIO 2

Se debe configurar una red pequeña para que admita conectividad IPv4 e IPv6, seguridad de switches, routing entre VLAN, el protocolo de routing dinámico OSPF, el protocolo de configuración de hosts dinámicos (DHCP), la traducción de direcciones de red dinámicas y estáticas (NAT), listas de control de acceso (ACL) y el protocolo de tiempo de red (NTP) servidor/cliente. Durante la evaluación, probará y registrará la red mediante los comandos comunes de CLI.

Topología



Ilustracion red implementada en packettrecer implementada

Parte 1: inicializar dispositivos

Paso 1 inicializar y volver a cargar los routers y los switches

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

.

Comandos IOS

Erase startup-config
Reload
Delete vlan.dat
Reload
show flash

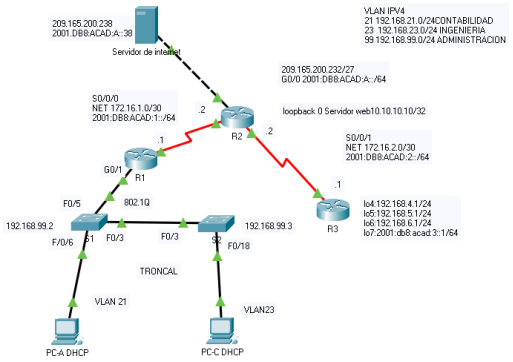
```
Router#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue?
[confirm]y[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Router#delete vlan.dat
Delete filename [vlan.dat]?y
Delete flash:/y? [confirm]y%Error deleting flash:/y (No such file or directory)

Router#show flash

System flash directory:
File  Length   Name/status
  3   33591768 c1900-universalk9-mz.SPA.151-4.M4.bin
  2   28282    sigdef-category.xml
  1   227537   sigdef-default.xml
[33847587 bytes used, 221896413 available, 255744000 total]
249856K bytes of processor board System flash (Read/Write)

Router#
```

Ilustración 25 erase startup-config

Parte 2: Configurar los parámetros básicos de los dispositivos

Paso 1: configurar la computadora de internet

Paso 1: Configurar la computadora de Internet



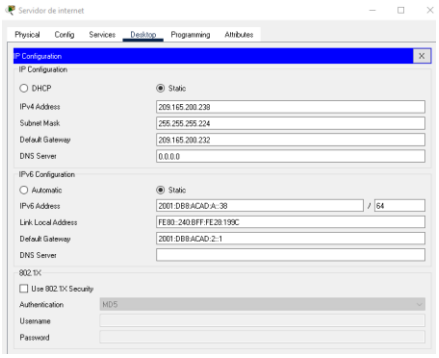


Ilustración 26 configuracion pc de internet

PASO 2:CONFIGURAR R1

Desactivar la búsqueda DNS

Router#config
Router(config)#no ip domain-lookup

Configuración básica

Router(config)#hostname R1
R1(config)#enable secret class
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#line vty 0 4
R1(config-line)#password cisco
R1(config-line)#exit
R1(config)#service password-encryption
R1(config)#banner motd #"se prohibe el acceso no autorizado"#
R1(config)#exit

Configuración de interfaces ipv4 y ipv6

R1(config)#int s0/0/0
R1(config-if)#ip add 172.16.1.1 255.255.255.252
R1(config-if)#clock rate 128000
R1(config-if)#no sh
R1(config-if)#ipv6 add 2001:DB8:ACAD:1::1/64
R1(config-if)#clock rate 128000
R1(config-if)#no sh

Ruteo por defecto

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

Paso 3: Configurar R2
La configuración del R2 incluye las siguientes tareas:

Desactivar la búsqueda DNS

Router(config)#no ip domain-lookup

Configuración básica

Router(config)#hostname R2
R2(config)#enable secret class
R2(config)#line console 0
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#exit
R2(config)#
R2(config)#line vty 0 15
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#exit
R2(config)#service password-encryption
R2(config)#banner motd 'Prohibido el acceso no autorizado'

Configuración de interfaces ipv4 y ipv6

R2(config)# int s0/0/0
R2(config-if)#ip address 172.16.1.2 255.255.255.252
R2(config-if)#ipv6 address 2001:db8:acad:1::2/64
R2(config-if)# clock rate 128000
R2(config-if)#no shutdown
R2(config-if)#exit

R2(config)# int s0/0/1
R2(config-if)#ip address 172.16.2.1 255.255.255.252
R2(config-if)#ipv6 address 2001:db8:acad:2::1/64
R2(config-if)# clock rate 128000
R2(config-if)#no shutdown
R2(config-if)#exit

R2(config)# int g0/0
R2(config-if)#description R2 --> Internet
R2(config-if)#ip address 209.165.200.232 255.255.255.248
R2(config-if)#ipv6 address 2001:db8:acad:A::1/64
R2(config-if)#no shutdown
R2(config-if)#exit

Configuración interfaces loopback 0

R2(config)# int loopback 0
R2(config-if)#ip address 10.10.10.10 255.255.255.255
R2(config-if)#exit

Ruteo por defecto

R2(config)#ip route 0.0.0.0 0.0 0.0 s0/0/0
R2(config)#ip route 0.0.0.0 0.0 0.0 s0/0/1
R2(config)#ip route 0.0.0.0 0.0 0.0 g0/0
ipV6 route ::/0 g0/0

PASO 4: CONFIGURAR R3

La configuración del R3 incluye las siguientes tareas:

Desactivar la búsqueda DNS

Router(config)#no ip domain-lookup

Configuración básica

Router(config)#hostname R3
R3(config)#enable secret class
R3(config)#line console 0
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#exit
R3(config)#line vty 0 4
R3(config-line)#password cisco
R3(config-line)#exit
R3(config)#service password-encryption
R3(config)#banner motd #"se prohibe el acceso no autorizado"#

Configuración de interfaces ipv4 y ipv6

R3(config)#int s0/0/1
R3(config-if)#ip add 172.16.2.1 255.255.255.252
R3(config-if)#clock rate 128000
R3(config-if)#no sh
R3(config-if)#ipv6 add 2001:DB8:ACAD:2::1/64
R3(config-if)#clock rate 128000
R3(config-if)#no sh
R3(config-if)#exit

Configuración interfaces loopback 4,5,6 y 7

R3(config)#int loopback 4
R3(config-if)#ip add 192.168.4.1 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit

R3(config)#int loopback 5
R3(config-if)#ip add 192.168.5.1255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit

R3(config)#int loopback 6
R3(config-if)#ip add 192.168.6.1 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit

R3(config)#int loopback 7
R3(config-if)#ipv6 add 2001:DB8:ACAD:3::1/64
R3(config-if)#no shutdown
R3(config-if)#exit

Ruteo por defecto

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

Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Desactivar la búsqueda de DNS

Switch(config)#**no ip domain-lookup**

Configuración básica

Switch(config)#hostname S1
S1(config)#enable secret class
S1(config)#line console 0
S1(config-line)#pass cisco
S1(config-line)#login
S1(config-line)#exit
S1(config)#line vty 0 15
S1(config-line)#pass cisco
S1(config-line)#login
S1(config-line)#exit
S1(config)#service password-encryption
S1(config)#banner motd #"Se prohibe el acceso no autorizado."#

Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Desativar la búsqueda de DNS

Switch(config)#**no ip domain-lookup**

Configuración Básica

Switch(config)#hostname S1
S1(config)#enable secret class
S1(config)#line console 0
S1(config-line)#pass cisco
S1(config-line)#login
S1(config-line)#exit
S1(config)#line vty 0 15
S1(config-line)#pass cisco
S1(config-line)#login
S1(config-line)#exit
S1(config)#service password-encryption
S1(config)#banner motd #"Se prohibe el acceso no autorizado."#

Paso 7: Verificar la conectividad de la red

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

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

Tabla 32 ping

Desde	A	Dirección IP	Resultados d ping
R1	R2, S0/0/0	172.16.1.2	0k
R2	R3, S0/0/1	172.16.2.1	ok
PC de Internet	Gateway predeterminado	209.165.200.225	No

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

PASO 1: CONFIGURAR S1

La configuración del S1 incluye las siguientes tareas:
Creación base de datos vlan

S1(config)#vlan 21
S1(config-vlan)#name contabilidad
S1(config-vlan)#vlan 23
S1(config-vlan)#name ingenieria
S1(config-vlan)#vlan 99
S1(config-vlan)#name administración

Asignación de interface a la vlan administración

S1(config-vlan)#int vlan 99
S1(config-if)#ip add 192.168.99.2 255.255.255.0
S1(config-if)#no sh

Asignación de puerta de enlace

S1(config)#ip defaul-gateway 192.168.99.1
S1(config-if)#exit

Creación de las troncales en las interfaces f0/3,f0/5

S1(config)#int f0/3
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 1
S1(config-if)#exit

S1(config)#int f0/5
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 1
S1(config-if)#exit

Habilitar puertos de acceso

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

S1(config)#int f0/6
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 21
S1(config-if)#exit

Deshabitar puertos que no estan en uso

S1(config)#int range f0/1-2,f0/4,f0/7-24,g0/1-2
S1(config-if-range)#sh

Paso 2:Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Creación de base de datos 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 administración

Asignación de interface a la vlan administración

S3(config)#int vlan 99
S3(config-if)#ip add 192.168.99.3 255.255.255.0

Asignación de puerta de enlace

S3(config-if)#ip default-gateway 192.168.99.1
S3(config)#exit

Creación de las troncales en las interface f0/3

S3(config)#int f0/3
S3(config-if)#switchport mode trunk
S3(config-if)#switchport trunk native vlan 1
S3(config-if)#exit

Habilitar puertos de acceso

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

S3(config)#int f0/18
S3(config-if)#switchport mode acces
S3(config-if)#switchport access vlan 21

Deshabitar puertos que no estan en uso

S3(config-if)#int range f0/1-2,f0/4-17,f0/19-24,g0/1-2
S3(config-if-range)#sh

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes
Configuración de subinterfaces 802.1Q .21, .23, .99 en g0/1

R1(config)#int g0/1.21
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)#int g0/1.23
R1(config-subif)#encapsulation dot1q 23
R1(config-subif)#description LAN de ingenieria
R1(config-subif)#ip add 192.168.23.1 255.255.255.0
R1(config-subif)#exit

R1(config)#int g0/1.99
R1(config-subif)#encapsulation dot1q 99
R1(config-subif)#description LAN de administracion
R1(config-subif)#ip add 192.168.99.1 255.255.255.0
R1(config-subif)#exit
R1(config)#int g0/1
R1(config-if)# no sh

Paso 4: Verificar la conectividad de la red

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

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

Tabla 33 Verificar conectividad de la red

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	ok
S3	R1, dirección VLAN 99	192.168.99.1	ok
S1	R1, dirección VLAN 21	192.168.21.1	ok
S3	R1, dirección VLAN 23	192.168.23.1	ok

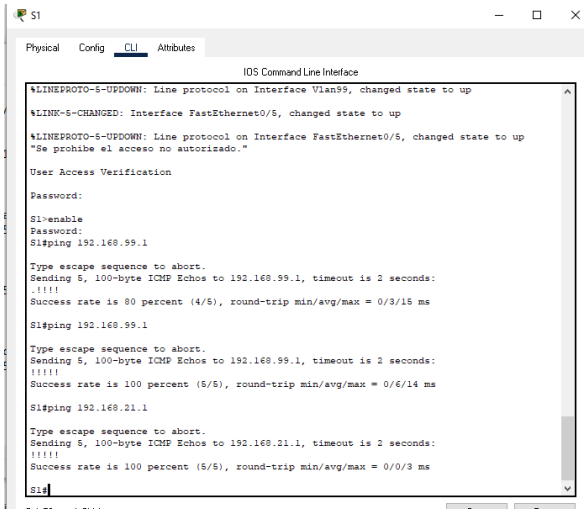


Ilustración 27 ping 192.168.99.1

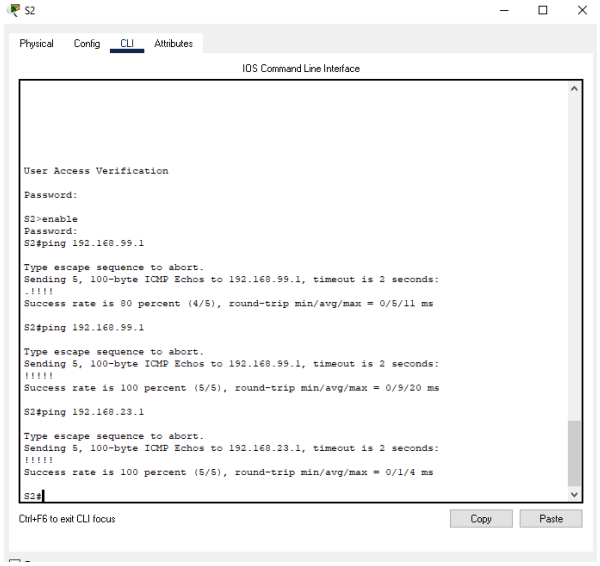


Ilustración 28 ping 192.168.23.1

Parte 4: Configurar el protocolo de routing dinámico OSPF

Configuración OSPF área 0

R1(config)#router ospf 1
R1(config-router)#router-id 1.1.1.1

Anunciar 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 192.168.1.23 0.0.0.255 area 0
R1(config-router)#network 192.168.1.99 0.0.0.255 area 0
R1(config-router)#

Establecer todas las interfaces LAN como pasivas

R1(config-router)#passive-interface g0/1.21
R1(config-router)#passive-interface g0/1.23
R1(config-router)#passive-interface g0/1.99
R1(config-router)#exit

Desactive la sumarización automática

R1(config)#router rip
R1(config-router)#no auto-summary
02:51:14: %OSPF-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Serial0/0/0 from LOADING to FULL, Loading Done

Paso 2: Configurar OSPF en el R2

La configuración del R2 incluye las siguientes tareas:

Configurar OSPF área 0

R2(config)#router ospf 1
R2(config-router)#router-id 2.2.2.2

Anunciar las redes conectadas directamente

R2(config-router)#network 172.16.1.0 0.0.0.3 area 0
R2(config-router)#network 172.16.2.0 0.0.0.3 area 0
R2(config-router)#network 10.10.10.10 0.0.0.255 area 0
R2(config-router)#

Establecer la interfaz LAN (loopback) como pasiva

R2(config-router)#passive-interface g0/1
R2(config-router)#exit

Desactive la sumarización automática.

R2(config)#router rip
R2(config-router)#no auto-summary
R2(config-router)#

Paso 3:Configurar OSPF en el R3

La configuración del R3 incluye las siguientes tareas:

PASO 1: CONFIGURAR OSPF EN EL R1

Configurar OSPF área 0

```
R3>en
R3#conf t
R3(config)#router ospf 1
R3(config-router)#router-id 3.3.3.3
R3(config-router)#
```

Anunciar redes IPv4 conectadas directamente

```
R3(config-router)#network 172.16.2.0 0.0.0.3 area 0
R3(config-router)#network 192.168.4.0 0.0.3.255 area 0
R3(config-router)#
```

Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas

```
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
```

Paso 4: Verificar la información de OSPF

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

Show ip protocols

Show ip route ospf

Show running-config

Reservar las primeras 20 direcciones vlan 21

```
R1(config)# ip dhcp excluded-address 192.168.21.1 192.168.21.20
```

Reservar las primeras 20 direcciones vlan 23

```
R1(config)# ip dhcp excluded-address 192.168.23.1 192.168.23.20
```

Crear un pool de DHCP para la VLAN 21.

```
R1(config)#ip dhcp pool vlan21
R1(dhcp-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)#
```

Crear un pool de DHCP para la VLAN 23

```
R1(config)#ip dhcp pool vlan23
R1(dhcp-config)#ip dhcp pool acct
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)#
```

Paso 2 configurar la NAT estatica y dinamica en R2

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

La configuración del R2 incluye las siguientes tareas:

Crear una base de datos local con una cuenta de usuario

```
Router#conf t
Router(config)#user webuser privilege 15 secret cisco12345
Router(config)#ip http server “no valido en el simulador”
^
% Invalid input detected at '^' marker.
Router(config)#ip http authentication “no valido em el simulador”
^
% Invalid input detected at '^' marker.
```

Crear una NAT estática al servidor web.

Router(config)#ip nat inside source static 10.10.10.10 209.165.200.229

Asignar la interfaz interna y externa para la NAT estática

Router(config)#int g0/0
Router(config-if)#ip nat outside
Router(config-if)#exit
Router(config)#

Router(config)#int g0/1
Router(config-if)#ip nat inside
Router(config-if)#exit

Configurar la NAT dinámica dentro de una ACL privada

Router(config)#access-list 1 permit 192.168.21.0 0.0.0.255
Router(config)#access-list 1 permit 192.168.23.0 0.0.0.255
Router(config)#access-list 1 permit 192.168.4.0 0.0.3.255

Defina el pool de direcciones IP públicas utilizables.

Router(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.224
Router(config)#ip nat inside source list 1 pool INTERNET

Paso 3: Verificar el protocolo DHCP y la NAT estática

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

Parte 6: Configurar NTP
Ajuste la fecha y hora

R2#clock set 09:00:00 5 March 2016
R2#config t

Configure R2 como un maestro NTP.

R2(config)#ntp master 5

Configurar R1 como un cliente NTP.

R1(config)#ntp server 172.16.1.1

Configure R1 para actualizaciones de calendario periódicas con hora NTP.

R1(config)#ntp update-calendar

Verifique la configuración de NTP en R1.

R1(config)#do show ntp associations

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

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

Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2

R1(config)#ip access-list standard ADMIN-MGT

Aplicar la ACL con nombre a las líneas VTY

R1(config-std-nacl)#host 172.16.1.1

Permitir acceso por Telnet a las líneas de VTY

172.16.1.1(config)#line vty 0 4
172.16.1.1(config-line)#access-class ADMIN-MGT in
172.16.1.1(config-line)#exit
172.16.1.1(config)#exit

Verificar que la ACL funcione como se espera

172.16.1.1#telnet 172.16.2.2
172.16.1.2#telnet 172.16.2.1

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

Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció **Show access list**
Restablecer los contadores de una lista de acceso **Clear ip access-list counters**
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica? **Show running-config**
¿Con qué comando se muestran las traducciones NAT? **show ip nat translations**
Qué comando se utiliza para eliminar las traducciones de NAT dinámicas? **clear ip nat translation**

CONCLUSIONES

Con este diplomado se desarrolló, analizó y se identificó el comportamiento de la red, donde se configuran los dispositivos, se configuran las interfases, se crean las VLAN, las interfases LOOPBACK, se troncaliza las interfases, se creó un servidor de DHCP y Web.

Se configuran los diferentes dispositivos pc, router, suiche, desarrollas mediante los escenarios de la actividad.

Mediante los comandos SHOW se verifican las diferentes configuraciones de los dispositivos y su correcto funcionamiento, con el comando PING se identifica la conectividad y sus problemas.

Con el programa de simulación Packet Tracer se pone en práctica los diferentes comandos y tipos de configuración propuestos en los comandos.

Mediante el desarrollo del proceso se aplicaron los conocimientos adquiridos en CCNA 1 R&S: Introduction to Networks y CCNA 2 R&S: Routing and Switching Essentials.

BIBLIOGRAFIA

CISCO. (2019). NAT para IPv4. Principios de Enrutamiento y Conmutación.
Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#9

CISCO. (2019). Detección, Administración y Mantenimiento de Dispositivos. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-courseassets.s3.amazonaws.com/RSE6/es/index.html#10

CISCO. (2019). Listas de Control de Acceso. Principios de Enrutamiento y
Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#7

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

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

CISCO. (2019). Capa de aplicación. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#10

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

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

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#2

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). Configuración del Switch. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#5

CISCO. (2019). Detección, Administración y Mantenimiento de Dispositivos. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#10

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

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-course-assets.s3.amazonaws.com/ITN6/es/index.html#8

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

CISCO. (2019). Listas de Control de Acceso. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#7

CISCO. (2019). NAT para IPv4. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#9

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

CISCO. (2019). Redes Conmutadas. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#4