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

ANDRÉS DARIO RUEDA FERREIRA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI
INGENIERÍA DE SISTEMAS
BOGOTÁ D.C.
2020

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

ANDRÉS DARIO RUEDA FERREIRA

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

DIRECTOR:
JOSÉ IGNACIO CARDONA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI
INGENIERÍA DE SISTEMAS
BOGOTÁ D.C.
2020

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____

_____

_____
Firma del presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

Bogotá D.C., 20 de septiembre de 2020

AGRADECIMIENTOS

Principalmente agradezco a Dios, quien me ha dado la facultad de poder entender y comprender la temática y de esta forma poder ponerla en práctica, en segundo a mi familia quien me ha estado acompañando y dando fortalece la poder seguir con los estudios que me encuentro realizando, de la misma mis docentes quien ha estado realizando el acompañamiento continuamente para garantizar que mis avances sean los adecuados y por último a mis amigos quienes han estado dispuestos a apoyarme en esos mementos difíciles.

CONTENIDO

LISTA DE TABLAS 6
LISTAS DE FIGURA 7
RESUMEN 9
ABSTRACT 9
INTRODUCCIÓN 10
DESARROLLO - ESCENARIO 1 11
INSTRUCCIONES 13
Parte 1: Inicializar y Recargar y Configurar aspectos básicos de los dispositivos 13
Parte 2: Configuración de la infraestructura de red (VLAN, Trunking, EtherChannel) 22
Parte 3: Configurar soporte de host 26
Parte 3: Probar y verificar la conectividad de extremo a extremo 28
DESARROLLO ESCENARIO 2 34
INSTRUCCIONES 34
Parte 1: Inicializar dispositivos 34
Parte 2: Configurar los parámetros básicos de los dispositivos 36
Parte 3: Configurar la seguridad del switch, las VLAN y el routing entre VLAN 47
Parte 4: Configurar el protocolo de routing dinámico OSPF 52
Parte 5: Implementar DHCP y NAT para IPv4 55
Parte 6: Configurar y verificar las listas de control de acceso (ACL) 61
CONCLUSIONES 66
REGENCIAS BIBLIOGRÁFICAS 67
Anexos 69
I. Link desarrollo de los escenarios 69
II. Link Articulo científico 69

LISTA DE TABLAS

Tabla 1. Escenario 1 - Nombre de la VLAN 12
Tabla 2. Escenario 1 - Asignación de direcciones.....12
Tabla 3. Escenario 1 - Configuración Router. 14
Tabla 4. Escenario 1 - Parámetros de configuración S1 y S2 18
Tabla 5. Escenario 1 - Configuración VLAN S1 22
Tabla 6. Escenario 1 - Configuración VLAN S2 24
Tabla 7. Escenario 1 - Tareas de configuración R1 26
Tabla 8. Escenario 1 - Configuración PC -A 27
Tabla 9. Escenario 1 - Configuración PC -B 27
Tabla 10. Escenario 1 - Comprobación de configuración.....28
Tabla 11. Escenario 2 - Inicializar routers y los switches 35
Tabla 12. Escenario 2 - Configuración servidor internet 36
Tabla 13. Escenario 2 - Configuración básica R1 37
Tabla 14. Escenario 2 - Configuración básica R2 38
Tabla 15. Escenario 2 - Configuración básica R3 41
Tabla 16. Escenario 2 - Configuración básica S1 43
Tabla 17. Escenario 2 - Configuración básica S3 45
Tabla 18. Escenario 2 - Verificación conectividad red.....46
Tabla 19. Escenario 2 - Configuración interface S1 47
Tabla 20. Escenario 2 - Configuración interface S3 49
Tabla 21. Escenario 2 - Configuración interface R1.....50
Tabla 22. Escenario 2 - Verificación red 51
Tabla 23. Escenario 2 - OSPF R1.....53
Tabla 24. Escenario 2 - OSPF R2.....53
Tabla 25. Escenario 2 - OSPFv3 R2 54
Tabla 26. Escenario 2 - Verificación OSPF.....55
Tabla 27. Escenario 2 - R1 DHCP R1.....56
Tabla 28. Escenario 2 - R1 DHCP R2.....57
Tabla 29. Escenario 2 - Verificación.....58
Tabla 30. Escenario 2 - Configuración NTP.....61
Tabla 31. Escenario 2 - VTY R2.....61
Tabla 32. Escenario 2 - CLI 62

LISTAS DE FIGURA

Figura 1. Escenario 1 - Topología 11
Figura 2. Escenario 1 - PC-A R1 1.2 IPv4 28
Figura 3. Escenario 1 - PC-A R1 1.2 IPv6 28
Figura 4. Escenario 1 - PC-A R1 1.3 IPv4 28
Figura 5. Escenario 1 - PC-A R1 1.3 IPv6 29
Figura 6. Escenario 1 - PC-A R1 1.4 IPv4 29
Figura 7. Escenario 1 - PC-A R1 1.4 IPv6 29
Figura 8. Escenario 1 - PC-A S1 IPv4 29
Figura 9. Escenario 1 - PC-A S1 IPv6 29
Figura 10. Escenario 1 - PC-A S2 IPv4 30
Figura 11. Escenario 1 - PC-A S2 IPv6 30
Figura 12. Escenario 1 - PC-A PC-B IPv4 30
Figura 13. Escenario 1 - PC-A PC-B IPv6 30
Figura 14. Escenario 1 - PC-A R1 IPv4 30
Figura 15. Escenario 1 - PC-A R1 IPv6 31
Figura 16. Escenario 1 - PC-B R1 IPv4 31
Figura 17. Escenario 1 - PC-B R1 IPv6 31
Figura 18. Escenario 1 - PC-B R1 1.2 IPv4 31
Figura 19. Escenario 1 - PC-B R1 1.2 IPv6 31
Figura 20. Escenario 1 - PC-B R1 1.3 IPv4 32
Figura 21. Escenario 1 - PC-B R1 1.3 IPv6 32
Figura 22. Escenario 1 - PC-B R1 1.4 IPv4 32
Figura 23. Escenario 1 - PC-B R1 1.4 IPv6 32
Figura 24. Escenario 1 - PC-B S1 IPv4 33
Figura 25. Escenario 1 - PC-B S1 IPv6 33
Figura 26. Escenario 1 - PC-B S2 IPv4 33
Figura 27. Escenario 1 - PC-B S2 IPv6 33
Figura 28. Escenario 2 - Topología Escenario 2 34
Figura 29. Escenario 2 - Servidor internet 36
Figura 30 Escenario 2 - Reultado R2 46
Figura 31 Escenario 2 - Reultado R3 46
Figura 32 Escenario 2 - Reultado Gateway 47
Figura 33. Escenario 2 - Resultado S1 VLAN 99 52
Figura 34 Escenario 2 - Resultado S3 -VLAN 99 52
Figura 35 Escenario 2 - Resultado S1 VLAN 21 52
Figura 36 Escenario 2 - Resultado S3 VLAN 23 52
Figura 37. Escenario 2 - DHCP PC-A 59

Figura 38. Escenario 2 - DHCP PC-C.....59
Figura 39. Escenario 2 - PC-A a PC-C.....60
Figura 40. Escenario 2 - Web 229.....60
Figura 41. Escenario 2 - NAT PC-A.....64
Figura 42. Escenario 2 - NAT R2.....65
Figura 43. Escenario 2 - Clear.....65

RESUMEN

En este trabajo podremos identificar las configuraciones a realizar una red aplicando el protocolo de IPV4 y IPV6, para ello se realiza la simulación de una red pequeña, en ayuda de la herramienta de Cisco Packet Tracer y emplean switch, router y host, y a cada uno de ellos se realiza las configuraciones necesarias, logrando una comunicación efectiva entre todos los elementos que los elementos que se encuentren conectados en una red.

Palabras clave:

Switch, router, host, IPv6, IPv4 interface, VLAN, DHCP, Etherchannel

ABSTRACT

In this work we will be able to identify the configurations to make a network by applying the IPV4 and IPV6 protocols, for this, the simulation of a small network is carried out, in aid of the Cisco Packet Tracer tool and they use switch, router and host, and each one From them, the necessary configurations are made, achieving effective communication between all the elements that are connected in a network.

Keywords:

Switch, router, host, IPv6, IPv4 interface, VLAN, DHCP, Etherchannel

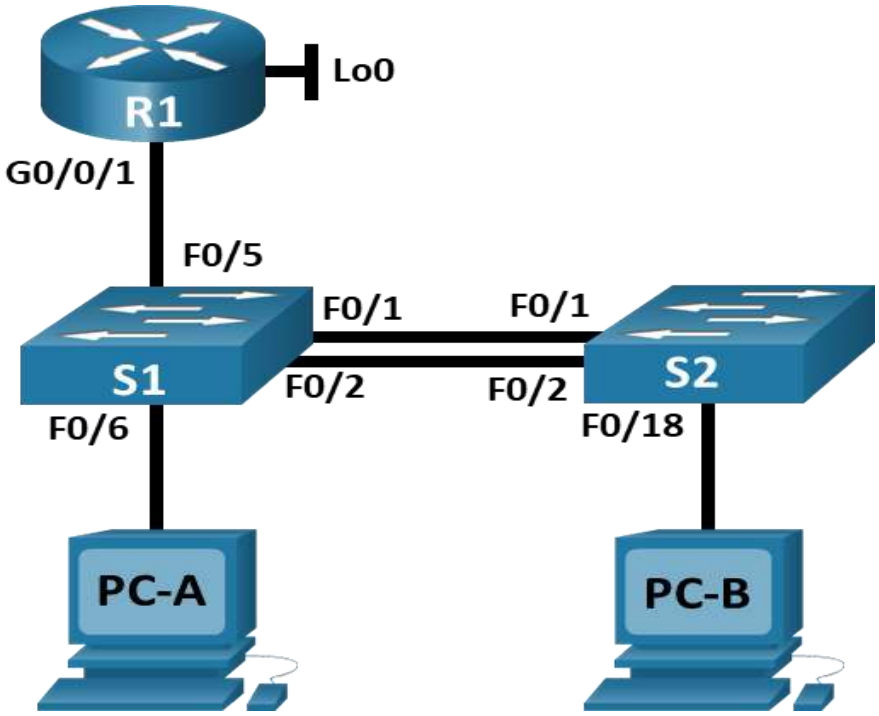
INTRODUCCIÓN

El diplomado de profundización Cisco, como opción de grado seleccionado para la carrera de Ingeniería a de sistema, con el fin de realizar la profundización en la creación de redes, el cual se encuentra basado en el curso de CCNP CISCO, el cual contiene un currículo en instalación, configuración en redes, permitiendo desarrollar las habilidades necesarias en el diseño, implementación, construcción e implementación, así mismo la detección y soluciones de los posibles problemas.

Con el fin de poder poner en práctica los conocimientos adquiridos en las configuraciones de un switch, router y host, durante el desarrollo del diplomado, y en ayuda herramienta de cisco packet tracer, se crea la simulación una red donde empleando el protocolo de IPv4 y IPV6, con los que se le realza la configuración de todos los elementos solicitados, logrando que la comunicación sea efectiva entre todos los dispositivos de interconexión empleados y los dispositivos de comunicación que se puedan llegar a conectar a la red.

DESARROLLO - ESCENARIO 1

Figura 1. Escenario 1 - Topología



En este escenario se configurarán los dispositivos de una red, para la cual se configuró un router, un switch y equipos que permiten la conectividad IPv4 y IPv6. Así mismo al router y el switch se le realiza la configuración administración de forma segura. Se configuró el enrutamiento entre VLAN, DHCP, Etherchannel y port-security.

Recursos necesarios

- 1 router (Cisco ISR4321 con software Cisco IOS versión 15.5 (3)S5)
- 2 switch (Cisco WS-C3650-24PS con Cisco IOS versión 16.3.2)
- 2 PC
- Cables de consola para configurar los dispositivos con Cisco IOS mediante los puertos de consola
- Cables Ethernet.

Tabla 1. Escenario 1 - Nombre de la VLAN

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

Tabla 2. Escenario 1 - Asignación de direcciones

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
R1 G0/0/1.2	10.19.8.1 /26	No corresponde
	2001:db8:acad:a: :1 /64	No corresponde
R1 G0/0/1.3	10.19.8.65 /27	No corresponde
	2001:db8:acad:b: :1 /64	No corresponde
R1 G0/0/1.4	10.19.8.97 /29	No corresponde
	2001:db8:acad:c: :1 /64	No corresponde
R1 G0/0/1.6	No corresponde	No corresponde
R1 Loopback0	209.165.201.1 /27	No corresponde
	2001:db8:acad:209: :1 /64	No corresponde
S1 VLAN 4	10.19.8.98 /29	10.19.8.97
	2001:db8:acad:c: :98 /64	No corresponde
	fe80: :98	No corresponde

S2 VLAN 4	10.19.8.99 /29	10.19.8.97
	2001:db8: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:db8:acad:a: :50 /64	fe80::1
PC-B NIC	DHCP para dirección IPv4	DHCP para puerta de enlace predeterminada IPv4
	2001:db8:acad:b: :50 /64	fe80::1

INSTRUCCIONES

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

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

El propósito inicializar y volver a cargar es permitir instale una configuración mínima en un router y de esta forma el administrador de red pueda realizar las configuraciones que sean necearías y adecuadas para la organización.

- Borrado de la configuración de inicio y las VLAN del router.

```
Router>enable                    // Ingreso al modo privilegiado
Router#erase startup-config      // Borrar el contenido de la NVRAM
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                    //Reinicia el router
```

- Borrado de la configuración de inicio y las VLAN del router.

```
Switch>
Switch>enable                    // Ingreso al modo privilegiado
Switch #erase startup-config     // Borrar el contenido de la NVRAM
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                                   //Reinicia el router
```

- Configuración de la plantilla SDM para que admita IPv6 switch.

```
S1#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:                         0.02k
number of IPv6 security aces:                    0.025K
```

Paso 2: Configurar R1

Con el fin de realizar las configuraciones iniciales de la máquina, como es establecer el nombre y las configuraciones de seguridad del route, se realiza el siguiente procedimiento, donde por medio de la consola se aplicada cada uno de los comandos que permite realizar las configuraciones tal como lo indica la siguiente tabla:

Basado en la siguiente tabla se realizó la configuración router 1 (R1),

Tabla 3. Escenario 1 - Configuración Router.

Tarea	Especificación
Desactivar la búsqueda DNS	
Nombre del router	R1
Nombre de dominio	ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	**enable secret** ciscoenpass

Tarea	Especificación
Contraseña de acceso a la consola	ciscoconpass
Establecer la longitud mínima para las contraseñas	10 caracteres
Crear un usuario administrativo en la base de datos local	Nombre de usuario: **admin** Password: **admin1pass**
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	
Configurar VTY solo aceptando SSH	
Cifrar las contraseñas de texto no cifrado	
Configure un MOTD Banner	
Habilitar el routing IPv6	
Configurar interfaz G0/0/1 y subinterfaces	Establezca la descripción Establece la dirección IPv4. Establezca la dirección local de enlace IPv6 como **fe80: :1** Establece la dirección IPv6. Activar la interfaz.
Configure el Loopback0 interface	Establezca la descripción Establece la dirección IPv4. Establece la dirección IPv6. Establezca la dirección local de enlace IPv6 como **fe80::1**
Generar una clave de cifrado RSA	Módulo de 1024 bits

- Desactivar la búsqueda DNS

```
Router>enable                          // Ingreso al modo privilegiado
Router#configure terminal              //Ingreso a la configura manualmente
Router(config)# no ip domain lookup    // Desactiva DNS
```

- Nombre Router

```
Router(config)# hostname R1
```

- Nombre de dominio
  R1(config)#ip domain-name ccna-lab.com *// Habilita la edición del nombre*

- Contraseña cifrada para el modo EXEC privilegiado
  R1(config)#enable secret ciscoenpass

- Contraseña de acceso a la consola
  R1(config)#line console *// Identifica la línea para configurar*
  R1(config-line)#password ciscoconpass *//Asignación de contraseña*
  R1(config-line)#login *//Asignación al verificación de contraseña*
  R1(config-line)#exit *// Salir de la configuración*

- Establecer la longitud mínima para las contraseñas
  R1(config)#security passwords min-length 10 *//especificación longitud mínima*

- Crear un usuario administrativo en la base de datos local
  R1(config-line)#username admin secret admin1pass

- Configurar el inicio de sesión en las líneas VTY para que use la base de datos local
  R1(config)#line vty 0 15
  R1(config-line)#login local
  R1(config-line)#transport input ssh
  R1(config-line)#exit

- Cifrar las contraseñas de texto no cifrado
  R1(config)#service password-encryption

- Configure un MOTD Banner
  R1(config)#banner motd # El acceso no autorizado está prohibido #

- Habilitar el routing IPv6
  R1(config)#ipv6 unicast-routing

- Configurar interfaz G0/0/1 y subinterfaces
  R1(config)#interface g0/1 *//Ingreso a la interface*
  R1(config-if)#description LAN interfaceG0/0/1 *//Realizar la descripción*
  R1(config-if)#ip address 10.19.8.1 255.255.255.192 *//Asignación de IPv4*
  R1(config-if)#ipv6 address fe80::1 link-local *//Asignación gateway*
  R1(config-if)#ipv6 address 2001:db8:acad:a::1/64 *//Asignación de IPv6*

  R1(config-if)# no shutdown *//Reinicia una interfaz desactivada*
  R1(config-if)#exit *//Salir de la configuración*

  R1(config)#interface g0/0/1.2 *//Ingreso a la interface*
  R1(config-subif)#encapsulation dot1Q 2 *//Encapsula*
  R1(config-subif)#description Bikes *//Realizar la descripción*
  R1(config-subif)#ip address 10.19.8.1 255.255.255.192 *//Asignación de IPv4*

```
R1(config-subif)#ipv6 address 2001:db8:acad:a::1/64      //Asignación de IPv6
R1(config-subif)#ipv6 address fe80::1 link-loca          //Asignación gateway

R1(config-subif)#interface g0/0/1.3                      //Ingreso a la interface
R1(config-subif)#encapsulation dot1Q 3                   //Encapsula
R1(config-subif)#description Trikes                      //Realizar la descripción
R1(config-subif)#ip address 10.19.8.65 255.255.255.224   //Asignación de IPv4
R1(config-subif)#ipv6 address 2001:db8:acad:b::1/64      //Asignación de IPv6
R1(config-subif)#ipv6 address fe80::1 link-local         //Asignación gateway

R1(config-subif)#interface g0/0/1.4                      //Ingreso a la
interface
R1(config-subif)#encapsulation dot1Q 4                   //Encapsula
R1(config-subif)#description Management                  //Realizar la
descripción
R1(config-subif)#ip address 10.19.8.97 255.255.255.248   //Asignación de IPv4
R1(config-subif)#ipv6 address 2001:db8:acad:c::1/64      //Asignación de IPv6
R1(config-subif)#ipv6 address fe80::1 link-local         //Asignación gateway

R1(config-subif)#interface g0/0/1.6                      //Ingreso a la
interface
R1(config-subif)#encapsulation dot1Q 6                   //Encapsula
R1(config-subif)#description Native                      //Realizar la
descripción

R1(config)#interface g0/0/1                              //Ingreso a la
interface
R1(config-if)#no shutdown                                //Reinicia una interfaz desactivada
```

- Configure el Loopback0 interface

```
R1(config)#interface loopback 0                          //Ingreso a la interface loopback
R1(config-if)#description LAN Loopback0                  //Realizar la descripción
R1(config-if)#ip address 209.165.201.1 255.255.255.224   //Asignación de IPv4
R1(config-if)#ipv6 address 2001:db8:acad:209::1/64       //Asignación de IPv4
R1(config-if)#ipv6 address fe80::1 link-local            //Asignación de IPv4
R1(config-if)# descripción Native                        //Realizar descripción
R1(config-if)#exit                                       //Salir de la
configuración
```

- Generar una clave de cifrado RSA

```
R1(config-if)#crypto key generate rsa
How many bits in the modulus [512]: 1024
```

Como resultado se desactiva las búsquedas de DNS, debido que cuando se escribe un comando de forma errada, el enruador empisa a resolver mediante una búsqueda de DNS, bloqueado el teclado, además de generar demoras el ingresar comandos de configuración.

Así mismo se realiza configuración de contraseñas, con el fin de restringir restringen el acceso a los routers. Se debe configurar contraseñas para las líneas de terminales virtuales y para la línea de consola. Las contraseñas usan para controlar

el acceso al modo EXEC privilegiado, de esta forma solo los usuarios autorizados puedan hacer cambios.

Como advertir al usuario que no tiene los permisos para acceder al los se realiza la configuración de un mensaje de advertencia, de esta forma le estamos dar al conocer de la restricción que tiene en el momento.

Otra configuración realizada corresponde a las interfaces, que son físicas y se enrutan a una VLAN, a estas se le asigna una IP, logrando que los dispositivos conectados a una red puedan comunicarse con el router mediante la interfaz física conectada a la misma VLAN. También la configuración de las subinterfaces que son interfaces virtuales mediante software que se encuentran asignadas a interfaces físicas. Cada subinterfaz se configura con su propia dirección IP, máscara de subred y asignación de VLAN única, lo que permite que una interfaz física única sea parte en forma simultánea de múltiples redes lógicas.

Paso 3: Configure S1 y S2.

Las tareas de configuración incluyen lo siguiente:

Tabla 4. Escenario 1 - Parámetros de configuración S1 y S2

Tarea	Especificación
Desactivar la búsqueda DNS.	
Nombre del switch	**S1 o S2, según proceda**
Nombre de dominio	**ccna-lab.com**
Contraseña cifrada para el modo EXEC privilegiado	**ciscoenpass**
Contraseña de acceso a la consola	**ciscoconpass**
Crear un usuario administrativo en la base de datos local	Nombre de usuario: **admin** Password: **admin1pass**
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	
Cifrar las contraseñas de texto no cifrado	

Tarea	Especificación
Configurar un MOTD Banner	
Generar una clave de cifrado RSA	**Módulo de 1024 bits**
Configurar la interfaz de administración (SVI)	Establecer la dirección IPv4 de capa 3 Establezca la dirección local de enlace IPv6 como **FE80: :98 para S1 y FE80: :99 para S2** Establecer la dirección IPv6 de capa 3
Configuración del gateway predeterminado	Configure la puerta de enlace predeterminada como 10.19.8.97 para IPv4

Configuración S1

- Desactivar la búsqueda DNS.

```
Switch >enable                                  // Ingreso al modo privilegiado
Switch #configure terminal                      //Ingreso a la configura manualmente
Switch(config)#no ip domain lookup
```

- Nombre del switch

```
Switch (config)#hostname S1 //Modifica el nombre del Switch
```

- Nombre de dominio

```
S1(config)#ip domain-name ccna-lab.com          // Habilita la edición del nombre
```

- Contraseña cifrada para el modo EXEC privilegiado

```
S1(config)#enable secret ciscoenpass // Especifica una capa de seguridad adicional
```

- Contraseña de acceso a la consola

```
S1(config)#line con 0                           // Identifica la línea para configurar
S1(config-line)#password ciscoconpass           //Asignación de contraseña
S1(config-line)#login                           //Asignación al verificación de contraseña
S1(config-line)#exit                                                  // Salir de la configuración
```

- Crear un usuario administrativo en la base de datos local

```
S1(config-line)#username admin secret admin1pass
```

- Configurar el inicio de sesión en las líneas VTY para que use la base de datos local

```
S1(config)#line vty 0 15
S1(config-line)#login local
```

- Configurar las líneas VTY para que acepten únicamente las conexiones SSH

```
S1(config-line)#transport input ssh
S1(config-line)#exit
```

- Cifrar las contraseñas de texto no cifrado

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

- Configurar un MOTD Banner

```
S1(config)#banner motd # El acceso no autorizado está prohibido#
```

- Generar una clave de cifrado RSA

```
S1(config)#crypto key generate rsa
How many bits in the modulus [512]: 1024
```

- Configurar la interfaz de administración (SVI)

```
S1(config)#interface vlan 4
S1(config-if)#ip address 10.19.8.98 255.255.255.248
S1(config-if)#ipv6 address 2001:db8:acad:c::98/64
S1(config-if)#ipv6 address fe80::98 link-local
S1(config-if)#description Management Interface
S1(config-if)#no shutdown
S1(config-if)#exit
```

- Configuración del gateway predeterminado

```
S1(config)#ip default-gateway 10.19.8.97
```

Configuración S2

- Desactivar la búsqueda DNS.

```
Switch >enable                                  // Ingreso al modo privilegiado
Switch #configure terminal                      //Ingreso a la configura manualmente
Switch(config)#no ip domain lookup
```

- Nombre del switch

```
Switch (config)#hostname S2 //Modifica el nombre del Switch
```

- Nombre de dominio

```
S2(config)#ip domain-name ccna-lab.com          // Habilita la edición del nombre
```

- Contraseña cifrada para el modo EXEC privilegiado

```
S2(config)#enable secret ciscoenpass // Especifica una capa de seguridad adicional
```

- Contraseña de acceso a la consola

```
S2(config)#line con 0                           // Identifica la línea para configurar
S2(config-line)#password ciscoconpass           //Asignación de contraseña
S2(config-line)#login                           //Asignación al verificación de contraseña
S2(config-line)#exit                            // Salir de la configuración
```

- Crear un usuario administrativo en la base de datos local
  S2(config-line)#username admin secret admin1pass

- Configurar el inicio de sesión en las líneas VTY para que use la base de datos local
  S2(config)#line vty 0 15
  S2(config-line)#login local

- Configurar las líneas VTY para que acepten únicamente las conexiones SSH
  S2(config-line)#transport input ssh
  S2(config-line)#exit

- Cifrar las contraseñas de texto no cifrado
  S2(config)#service password-encryption

- Configurar un MOTD Banner
  S2(config)#banner motd # El acceso no autorizado está prohibido#

- Generar una clave de cifrado RSA
  S2(config)#crypto key generate rsa
  How many bits in the modulus [512]: 1024

- Configurar la interfaz de administración (SVI)
  S2(config)#interface vlan 4
  S2(config-if)#ip address 10.19.8.99 255.255.255.248
  S2(config-if)#ipv6 address 2001:db8:acad:c::99/64
  S2(config-if)#ipv6 address fe80::98 link-local
  S2(config-if)#description Management Interface
  S2(config-if)#no shutdown
  S2(config-if)#exit

- Configuración del gateway predeterminado
  S1(config)#ip default-gateway 10.19.8.97

De igual forma como se realiza la configuración en los stwich, para ello se realizan gran parte los procedimientos que se efectuaron en los router, como es la desactiva las búsquedas de DNS.

Los demás procedimientos como la configuración de la contraseña y de las interfaces, se mantiene bajo los mismo parámetros y métricas que los router, y la finalidad es la misma.

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

Paso 1: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 5. Escenario 1 - Configuración VLAN 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

- Crear VLAN

```
S1(config)# vlan 2
S1(config-if)#name Bikes
S1 (config-vlan)#vlan 3
S1 (config-vlan)#name Management
S1 (config-vlan)#vlan 4
S1 (config-vlan)#name Management
S1 (config-vlan)#vlan 5
S1 (config-vlan)#name Parking
S1 (config-vlan)#vlan 6
S1 (config-vlan)#name Native
S1 (config-vlan)#exit
```

- Crear troncos 802.1Q que utilicen la VLAN 6 nativa

```
S1(config)#interface g1/0/5
S1(config-if)#switchport trunk encapsulation dot1q (#option)
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 6
S1(config-if)#exit

S1(config)#int range g1/0/1-2
S1(config-if-range)#shutdown
S1(config-if-range)#switchport trunk encapsulation dot1q
S1(config-if-range)#switchport mode trunk
S1(config-if-range)#switchport trunk native vlan 6
```

- Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2

```
S1(config-if-range)#channel-group 1 mode active
S1(config-if-range)#int port-channel 1
S1(config-if-range)#switchport trunk encapsulation dot1q
S1(config-if-range)#switchport mode trunk
S1(config-if-range)#switchport trunk native vlan 6
```

- Configurar el puerto de acceso de host para VLAN 2

```
S1(config-if)#interface g1/0/6
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 2
```

- Configurar la seguridad del puerto en los puertos de acceso

```
S1(config-if)#switchport port-security
S1(config-if)#switchport port-security maximum 3
```

- Proteja todas las interfaces no utilizadas

```
S1(config-if)#int range g1/0/3-4
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 5
S1(config-if-range)#description No esta en Uso
S1(config-if-range)#shutdown

S1(config-if)#int range g1/0/7-24
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 5
S1(config-if-range)#description No esta en Uso
S1(config-if-range)#shutdown

S1(config-if)#int range g1/1/1-4
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 5
S1(config-if-range)#description No esta en Uso
S1(config-if-range)#shutdown
```

Paso 2: Configure el S2.

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

Tabla 6. Escenario 1 - Configuración VLAN S2

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

- Crear VLAN

```
S2#configure terminal
S2 (config)# vlan 2
S2 (config-if)#name Bikes
S2 (config-vlan)#vlan 3
S2 (config-vlan)#name Management
S2 (config-vlan)#vlan 4
S2 (config-vlan)#name Management
S2 (config-vlan)#vlan 5
S2 (config-vlan)#name Parking
S2 (config-vlan)#vlan 6
S2 (config-vlan)#name Native
S2 (config-vlan)#exit
```

- Crear troncos 802.1Q que utilicen la VLAN 6 nativa

```
S2(config)#int range g1/0/1-2
S2(config-if-range)#shutdown
S2(config-if-range)#switchport trunk encapsulation dot1q
```

S2(config-if-range)#switchport mode trunk
S2(config-if-range)#switchport trunk native vlan 6

- Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2

S2(config-if-range)#channel-group 1 mode active
S2(config-if-range)#int port-channel 1
S2(config-if-range)#switchport trunk encapsulation dot1q
S2(config-if-range)#switchport mode trunk
S2(config-if-range)#switchport trunk native vlan 6

- Configurar el puerto de acceso del host para la VLAN 3

S1(config-if)#interface g1/0/18
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 3

- Configure port-security en los access ports

S2(config-if)#switchport port-security
S2(config-if)#switchport port-security maximum 3

- Asegure todas las interfaces no utilizadas.

S1(config-if)#int range g1/0/3-17
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 5
S1(config-if-range)#description No esta en Uso
S1(config-if-range)#shutdown

S1(config-if)#int range g1/0/19-24
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 5
S1(config-if-range)#description No esta en Uso
S1(config-if-range)#shutdown

S1(config-if)#int range g1/1/1-4
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 5
S1(config-if-range)#description No esta en Uso
S1(config-if-range)#shutdown

Para este paso se realiza la configuración del nombre de las VLAN, Los nombres de las VLAN funcionan de manera conjunta con el ID de VLAN. El ID de VLAN se asigna durante la configuración de la VLAN.

Así mismo las configuraciones de las tramas las cuales las empleara para el envió de paquetes. Es importante tener presente que el encabezado de la trama no contiene información que indique a qué VLAN pertenece la trama. Posteriormente, cuando las tramas de Ethernet se ubican en un enlace

troncal, necesitan información adicional sobre las VLAN a las que pertenecen. Esto se logra por medio de la utilización del encabezado de encapsulación 802.1Q.

Para el caso de la configuración del EtherChannel, su principal funcional es que pueda utilizar los enlaces de forma balanceado, si esta configuración no se realizara podría llegar a bloquear bloquearía todos los enlaces. Ya realizado todas estas configuraciones se le realiza una restricción de seguridad, que es detectar tres mac y solo a ellas dejarlas pertenecer a la red.

Parte 3: Configurar soporte de host

Paso 1: Configure R1

Tabla 7. Escenario 1 - Tareas de configuración 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

- Configure Default Routing

```
R1(config)#ip route 0.0.0.0 0.0.0.0 loopback 0
R1(config)#ipv6 route ::/0 loopback 0
```

- Configurar IPv4 DHCP para VLAN 2

```
R1(config)#ip dhcp excluded-address 10.19.8.1 10.19.8.52
R1(config)#ip dhcp pool VLAN2-Bikes
R1(dhcp-config)#network 10.19.8.0 255.255.255.192
R1(dhcp-config)#default-router 10.19.8.1
R1(dhcp-config)#domain-name ccna-a.net
R1(dhcp-config)#exit
```

- Configurar DHCP IPv4 para VLAN 3

```
R1(config)#ip dhcp excluded-address 10.19.8.65 10.19.8.84
R1(config)#ip dhcp pool VLAN3-Trikes
R1(dhcp-config)#network 10.19.8.64 255.255.255.224
R1(dhcp-config)#default-router 10.19.8.65
R1(dhcp-config)#domain-name ccna-b.net
R1(dhcp-config)#
```

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. Escenario 1 - Configuración PC -A

Configuración de red de PC-A	
Descripción	
Dirección física	FE80::210:11FF:FE4B:B981
Dirección IP	10.19.8.53
Máscara de subred	255.255.255.192
Gateway predeterminado	10.19.8.1
Gateway predeterminado IPv6	fe80::1

Tabla 9. Escenario 1 - Configuración PC -B

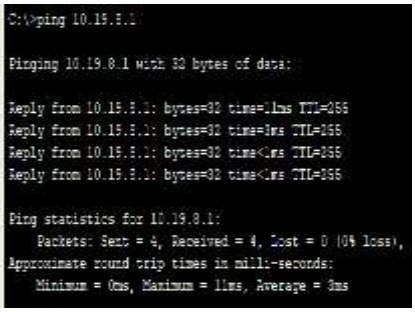
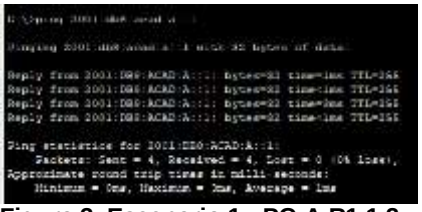
Configuración de red de PC-B	
Descripción	
Dirección física	FE80::201:96FF:FEA5:9054
Dirección IP	10.19.8.85
Máscara de subred	255.255.255.224
Gateway predeterminado	10.19.8.65
Gateway predeterminado IPv6	fe80::1

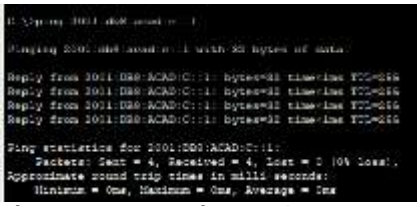
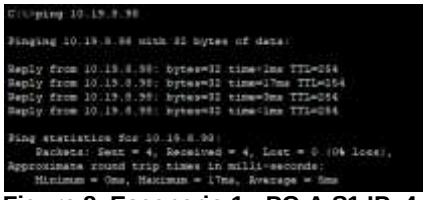
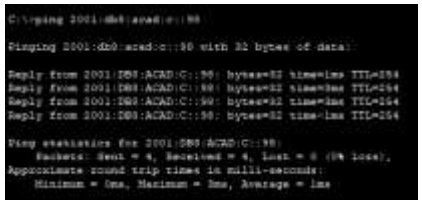
Se realiza la configuración de los PC conectado a la red, donde se el asigna una IP en las versiones de IPv4 y Pv6 de forma manual.

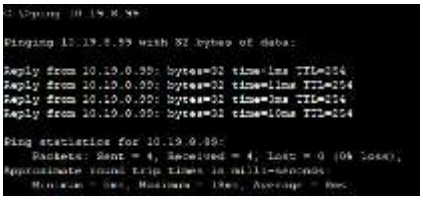
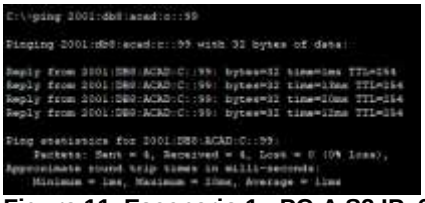
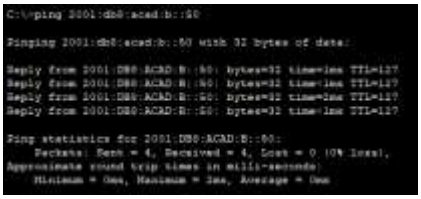
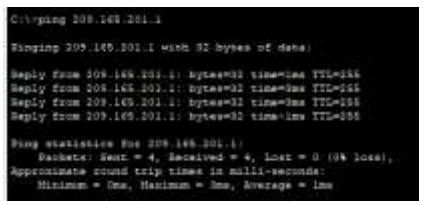
Parte 3: Probar y verificar la conectividad de extremo a extremo

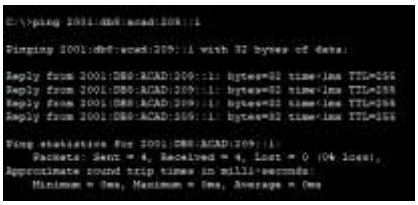
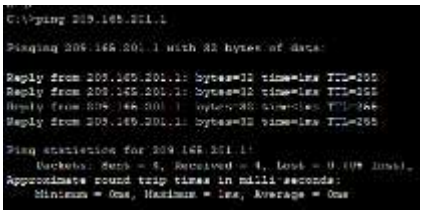
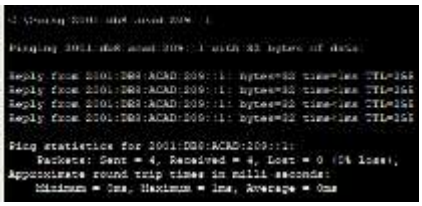
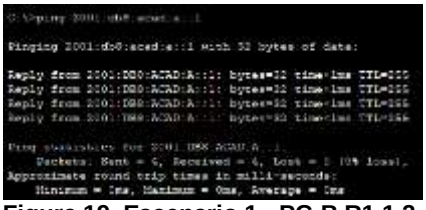
Use el comando ping para probar la conectividad IPv4 e IPv6 entre todos los dispositivos de red.

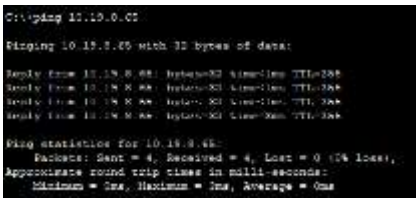
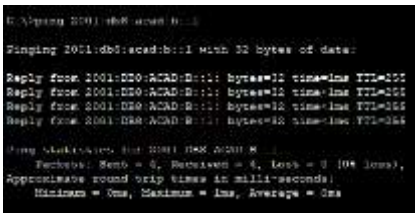
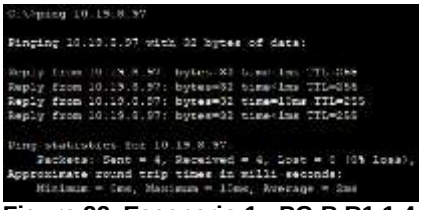
Tabla 10. Escenario 1 - Comprobación de configuración

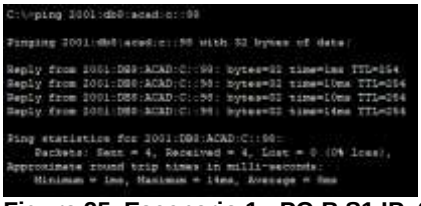
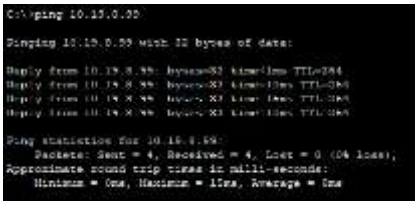
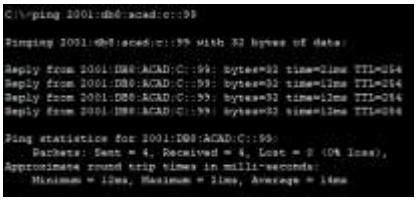
Desde	A	de Internet	Dirección IP	Resultados de ping
PC-A	R1, G0/0/1.2	Dirección	10.19.8.1	 **Figura 2. Escenario 1 - PC-A R1 1.2 IPv4**
		IPv6	2001:db8:acad:a: :1	 **Figura 3. Escenario 1 - PC-A R1 1.2 IPv6**
	R1, G0/0/1.3	Dirección	10.19.8.65	 **Figura 4. Escenario 1 - PC-A R1 1.3 IPv4**

Des de	A	de Internet	Dirección IP	Resultados de ping
		IPv6	2001:db8:acad:b: :1	 **Figura 5. Escenario 1 - PC-A R1 1.3 IPv6**
	R1, G0/0/1.4	Dirección	10.19.8.97	 **Figura 6. Escenario 1 - PC-A R1 1.4 IPv4**
		IPv6	2001:db8:acad:c: :1	 **Figura 7. Escenario 1 - PC-A R1 1.4 IPv6**
	S1, VLAN 4	Dirección	10.19.8.98	 **Figura 8. Escenario 1 - PC-A S1 IPv4**
		IPv6	2001:db8:acad:c: :98	 **Figura 9. Escenario 1 - PC-A S1 IPv6**

Desde	A	de Internet	Dirección IP	Resultados de ping
	S2, VLAN 4	Dirección	10.19.8.99.	 **Figura 10. Escenario 1 - PC-A S2 IPv4**
		IPv6	2001:db8:acad:c: :99	 **Figura 11. Escenario 1 - PC-A S2 IPv6**
	PC-B	Dirección	IP address will vary.	 **Figura 12. Escenario 1 - PC-A PC-B IPv4**
		IPv6	2001:db8:acad:b::50	 **Figura 13. Escenario 1 - PC-A PC-B IPv6**
	R1 Bucle 0	Dirección	209.165.201.1	 **Figura 14. Escenario 1 - PC-A R1 IPv4**

Desde	A	de Internet	Dirección IP	Resultados de ping
		IPv6	2001:db8:acad:209: :1	 **Figura 15. Escenario 1 - PC-A R1 IPv6**
PC-B	R1 Bucle 0	Dirección	209.165.201.1	 **Figura 16. Escenario 1 - PC-B R1 IPv4**
		IPv6	2001:db8:acad:209: :1	 **Figura 17. Escenario 1 - PC-B R1 IPv6**
	R1, G0/0/1.2	Dirección	10.19.8.1	 **Figura 18. Escenario 1 - PC-B R1 1.2 IPv4**
		IPv6	2001:db8:acad:a: :1	 **Figura 19. Escenario 1 - PC-B R1 1.2 IPv6**

Des de	A	de Internet	Dirección IP	Resultados de ping
	R1, G0/0/1.3	Dirección	10.19.8.65	 **Figura 20. Escenario 1 - PC-B R1 1.3 IPv4**
		IPv6	2001:db8:acad:b: :1	 **Figura 21. Escenario 1 - PC-B R1 1.3 IPv6**
	R1, G0/0/1.4	Dirección	10.19.8.97	 **Figura 22. Escenario 1 - PC-B R1 1.4 IPv4**
		IPv6	2001:db8:acad:c: :1	 **Figura 23. Escenario 1 - PC-B R1 1.4 IPv6**

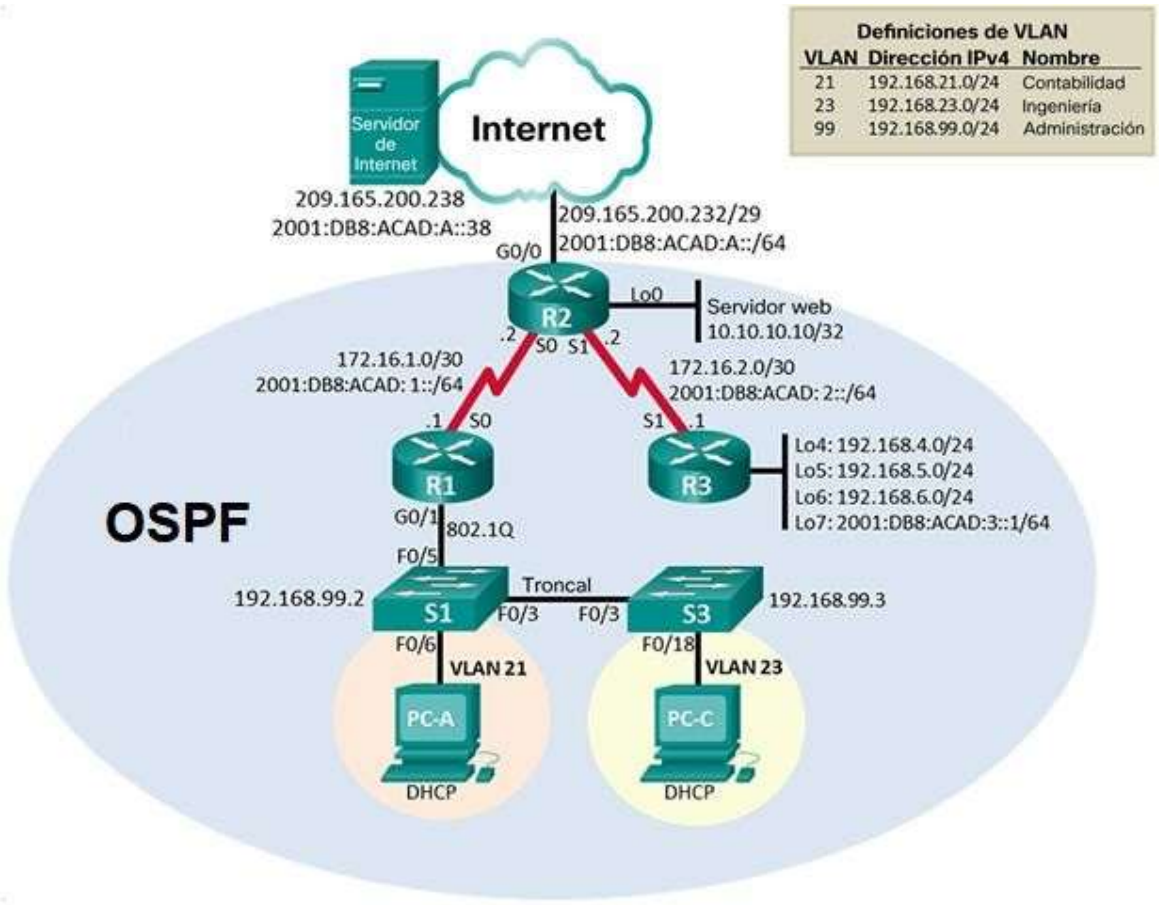
Desde	A	de Internet	Dirección IP	Resultados de ping
	S1, VLAN 4	Dirección	10.19.8.98	 **Figura 24. Escenario 1 - PC-B S1 IPv4**
		IPv6	2001:db8:acad:c: :98	 **Figura 25. Escenario 1 - PC-B S1 IPv6**
	S2, VLAN 4	Dirección	10.19.8.99.	 **Figura 26. Escenario 1 - PC-B S2 IPv4**
		IPv6	2001:db8:acad:c: :99	 **Figura 27. Escenario 1 - PC-B S2 IPv6**

Al finalizar de las configuraciones se realiza ping entre los diferentes hosts que se encuentran conectados en la VLAN, con esto se comprueba la comunicación desde el origen hacia varios hosts conectado a la red, para ello envía paquete ICMP y comprueba a entrega, con este diagnosticamos el estado, velocidad y calidad de la red

DESARROLLO ESCENARIO 2

Topología

Figura 28. Escenario 2 - Topología Escenario 2



En este escenario se configura una red para que admite conectividad IPv4 e IPv6, seguridad de switches, routing entre VLAN, el protocolo de routing dinámico OSPF, 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.

INSTRUCCIONES

Parte 1: Inicializar dispositivos

Paso1: Inicializar y volver a cargar los routers y los switches

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

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

Tabla 11. Escenario 2 - Inicializar routers y los switches

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	Erase startup-config 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

- Eliminar el archivo startup-config de todos los routers

```
Router>enable                          // Ingreso al modo privilegiado
Router#Erase startup-config            // Borrar el contenido de la NVRAM
    Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
    [OK]
    Erase of nvram: complete
```

- Volver a cargar todos los routers

```
Router#reload                          //Reinicia el router
        Proceed with reload? [confirm]
        Would you like to enter the initial configuration dialog? [yes/no]: n
        Press RETURN to get started!
Router>
```

- Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior

```
Switch>enable                          // Ingreso al modo privilegiado
Switch#Erase startup-config            // Borrar el contenido de la NVRAM
        Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
        [OK]
        Erase of nvram: complete
        %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Switch#delete vlan.dat                 // Borrar base de datos de VLAN
        Delete filename [vlan.dat]?
        Delete flash:/vlan.dat? [confirm]
        %Error deleting flash:/vlan.dat (No such file or directory)
Switch#reload                          //Reinicia el switch
        Proceed with reload? [confirm]
Switch>enable                          // Ingreso al modo privilegiado
Switch#Show flash                      //visualizar la memoria flash disponible
        Directory of flash:/
        1 -rw- 4414921 <no date> c2960-lanbase-mz.122-25.FX.bin
```

Parte 2: Configurar los parámetros básicos de los dispositivos

Paso1: Configurar la computadora de Internet

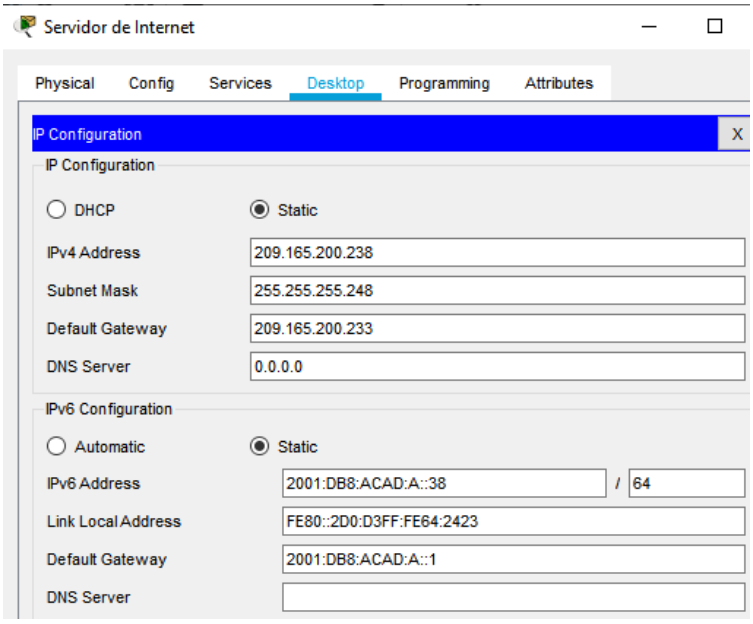
Las tareas de configuración del servidor de Internet incluyen lo siguiente (para obtener información de las direcciones IP, consulte la topología):

Tabla 12. Escenario 2 - Configuración servidor internet

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.233
Dirección IPv6/subred	2001:DB8:ACAD:A::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:A::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.

Figura 29. Escenario 2 - Servidor internet



Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 13. Escenario 2 - Configuración básica R1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	
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	
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

Nota: Todavía no configure G0/1.

- Desactivar la búsqueda DNS

```
Router>enable                              // Ingreso al modo privilegiado
Router#configure terminal                  //Ingreso a la configura manualmente
Router(config)# no ip domain lookup        // Desactiva DNS
```

- Nombre del router

```
Router(config)# hostname R1
```

- Contraseña de exec privilegiado cifrada

```
R1(config)#enable secret class
```

- Contraseña de acceso a la consola

```
R1(config)#line console 0                    // Identifica la línea para configurar
R1(config-line) #password cisco              //Asignación de contraseña
R1(config-line) #login                       //Asignación a la verificación de contraseña
R1(config-line) #exit                        // Salir de la configuración
```

- Contraseña de acceso Telnet

```
R1(config)#line vty 0 15
R1(config-line) # password cisco
R1(config-line) #login
R1(config-line) #exit
```

- Cifrar las contraseñas de texto no cifrado

```
R1(config)#service password-encryption
```

- Mensaje MOTD

```
R1(config)#banner motd # Se prohíbe el acceso no autorizado. #
```

- Interfaz S0/0/0

```
R1(config)#interface S0/0/0                      //Ingreso a la interface
R1(config-if) #description coneccion a R2        //Realizar la descripción
R1(config-if) #ip address 172.16.1.1 255.255.255.252   //Asignación de IPv4
R1(config-if) #ipv6 address 2001:db8:acad:1::1/64       //Asignación de IPv6
R1(config-if) #clock rate 128000                 //XXXXXXX
R1(config-if) # no shutdown                      // Habilita una interfaz
R1(config-if) #exit                              //Salir de la configuración
```

- Rutas predeterminadas

```
R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0
R1(config-if) #ipv6 route ::/0 s0/0/0
```

Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Tabla 14. Escenario 2 - Configuración básica R2

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	
Nombre del router	R2

Elemento o tarea de configuración	Especificación
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	
Habilitar el servidor HTTP	
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>enable                          // Ingreso al modo privilegiado
Router#configure terminal              //Ingreso a la configura manualmente
Router(config)# no ip domain lookup    // Desactiva DNS
```

- Nombre del router

```
Router(config)# hostname R2
```

- Contraseña de exec privilegiado cifrada

```
R2(config)#enable secret class
```

- Contraseña de acceso a la consola

```
R2(config)#line console 0              // Identifica la línea para configurar
R2(config-line) #password cisco        //Asignación de contraseña
R2(config-line) #login                 //Asignación a la verificación de contraseña
R2(config-line) #exit                  // Salir de la configuración
```

- Contraseña de acceso Telnet

```
R2(config)#line vty 0 15
R2(config-line) # password cisco
R2(config-line) #login
R2(config-line) #exit
```

- Cifrar las contraseñas de texto no cifrado

```
R2(config)#service password-encryption
```

- Habilitar el servidor HTTP

```
R2(config)#ip http server
```

- Configure un MOTD Banner

```
R2(config)# banner motd # Se prohíbe el acceso no autorizado. #
```

- Interfaz S0/0/0

```
R2(config)#interface S0/0/0                    //Ingreso a la interface
R2(config-if) #description coneccion a R1      //Realizar la descripción
R2(config-if) #ip address 172.16.1.2 255.255.255.252   //Asignación de IPv4
R2(config-if) #ipv6 address 2001:db8:acad:1::2/64      //Asignación de IPv6
R2(config-if) # no shutdown                    // Habilita una interfaz
R2(config-if) #exit                            //Salir de la configuración
```

- Interfaz S0/0/1

```
R2(config)#interface S0/0/1                    //Ingreso a la interface
R2(config-if) #description coneccion a R3      //Realizar la descripción
R2(config-if) #ip address 172.16.2.2 255.255.255.252   //Asignación de IPv4
R2(config-if) #ipv6 address 2001:db8:acad:2::2/64      //Asignación de IPv6
R2(config-if) #clock rate 128000               //XXXXXXX
R2(config-if) # no shutdown                    // Habilita una interfaz
R2(config-if) #exit                            //Salir de la configuración
```

- Interfaz G0/0 (simulación de Internet)

```
R2(config)#interface G0/0                                   //Ingreso a la interface
R2(config-if) #description coneccion a internte             //Realizar la descripción
R2(config-if) #ip address 209.165.200.233 255.255.255.248   //Asignación de IPv4
R2(config-if) #ipv6 address 2001:db8:acad:a::1/64           //Asignación de IPv6
R2(config-if) # no shutdown                                 // Habilita una interfaz
R2(config-if) #exit                                         //Salir de la configuración
```

- Interfaz loopback 0 (servidor web simulado)

```
R2(config)#interface loopback 0                             //Ingreso a la interface
R2(config-if) #description servidor web simulado            //Realizar la descripción
R2(config-if) #ip address 10.10.10.10 255.255.255.255       //Asignación de IPv4
R2(config-if) #exit                                         //Salir de la configuración
```

- Rutas predeterminadas

```
R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0
R2(config-if) #ipv6 route ::/0 g0/0
```

Paso 5: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Tabla 15. Escenario 2 - Configuración básica R3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	
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	
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.
Rutas predeterminadas	

- Desactivar la búsqueda DNS

```
Router>enable                          // Ingreso al modo privilegiado
Router#configure terminal              //Ingreso a la configura manualmente
Router(config)# no ip domain lookup    // Desactiva DNS
```

- Nombre del router

```
Router(config)# hostname R3
```

- Contraseña de exec privilegiado cifrada

```
R3(config)#enable secret class
```

- Contraseña de acceso a la consola

```
R3(config)#line console 0              // Identifica la línea para configurar
R3(config-line) #password cisco        //Asignación de contraseña
R3(config-line) #login                 //Asignación a la verificación de contraseña
R3(config-line) #exit                  // Salir de la configuración
```

- Contraseña de acceso Telnet

```
R3(config)#line vty 0 15
R3(config-line) # password cisco
R3(config-line) #login
R3(config-line) #exit
```

- Cifrar las contraseñas de texto no cifrado

```
R3(config)#service password-encryption
```

- Configure un MOTD Banner

```
R3(config)# banner motd # Se prohíbe el acceso no autorizado. #
```

- Interfaz S0/0/1

```
R3(config)#interface S0/0/1                          //Ingreso a la interface
R3(config-if) #description coneccion a R2            //Realizar la descripción
R3(config-if) #ip address 172.16.2.1 255.255.255.252 //Asignación de IPv4
R3(config-if) #ipv6 address 2001:db8: acad:2::1/64   //Asignación de IPv6
R3(config-if) # no shutdown                          // Habilita una interfaz
R3(config-if) #exit                                  //Salir de la configuración
```

- Interfaz loopback 4

```
R3(config)#interface loopback 4                    //Ingreso a la interface
R3(config-if) #description loopback 4              //Realizar la descripción
R3(config-if) #ip address 192.168.4.1 255.255.255.0   //Asignación de IPv4
R3(config-if) #exit
```

- Interfaz loopback 5

```
R3(config)#interface loopback 5                    //Ingreso a la interface
R3(config-if) #description loopback 5              //Realizar la descripción
R3(config-if) #ip address 192.168.5.1 255.255.255.0   //Asignación de IPv4
R3(config-if) #exit
```

- Interfaz loopback 6

```
R3(config)#interface loopback 6                    //Ingreso a la interface
R3(config-if) #description loopback 6              //Realizar la descripción
R3(config-if) #ip address 192.168.6.1 255.255.255.0   //Asignación de IPv4
R3(config-if) #exit
```

- Interfaz loopback 7

```
R3(config)#interface loopback 7                    //Ingreso a la interface
R3(config-if) #description loopback 7              //Realizar la descripción
R3(config-if) #ipv6 address 2001:db8: acad:3::1/64    //Asignación de IPv6
R3(config-if) #exit
```

- Rutas predeterminadas

```
R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1
R3(config-if) #ipv6 route ::/0 g0/0 s0/0/1
```

Paso 6: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 16. Escenario 2 - Configuración básica S1

Elemento o tarea de configuración	Especificación

Desactivar la búsqueda DNS	
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	
Mensaje MOTD	Se prohíbe el acceso no autorizado.

- Desactivar la búsqueda DNS

```
Switch>enable                          // Ingreso al modo privilegiado
Switch>configure terminal              //Ingreso a la configura manualmente
Switch> (config)# no ip domain lookup  // Desactiva DNS
```

- Nombre del router

```
Switch> (config)# hostname S1
```

- Contraseña de exec privilegiado cifrada

```
S1(config)#enable secret class
```

- Contraseña de acceso a la consola

```
S1 (config)#line console 0             // Identifica la línea para configurar
S1 (config-line) #password cisco       //Asignación de contraseña
S1 (config-line) #login                //Asignación a la verificación de contraseña
S1 (config-line) #exit                 // Salir de la configuración
```

- Contraseña de acceso Telnet

```
S1 (config)#line vty 0 15
S1 (config-line) # password cisco
S1 (config-line) #login
S1 (config-line) #exit
```

- Cifrar las contraseñas de texto no cifrado

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

- Configure un MOTD Banner

```
S1 (config)# banner motd # Se prohíbe el acceso no autorizado. #
```

Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 17. Escenario 2 - Configuración básica S3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	
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	
Mensaje MOTD	Se prohíbe el acceso no autorizado.

- Desactivar la búsqueda DNS

```
Switch>enable                          // Ingreso al modo privilegiado
Switch>configure terminal              //Ingreso a la configura manualmente
Switch> (config)# no ip domain lookup  // Desactiva DNS
```

- Nombre del router

```
Switch> (config)# hostname S3
```

- Contraseña de exec privilegiado cifrada

```
S3(config)#enable secret class
```

- Contraseña de acceso a la consola

```
S3 (config)#line console 0             // Identifica la línea para configurar
S3 (config-line) #password cisco       //Asignación de contraseña
S3 (config-line) #login                //Asignación a la verificación de contraseña
S3 (config-line) #exit                 // Salir de la configuración
```

- Contraseña de acceso Telnet

```
S3 (config)#line vty 0 15
```

S3 (config-line) # password cisco
S3 (config-line) #login
S3 (config-line) #exit

- Cifrar las contraseñas de texto no cifrado
  S3 (config)#service password-encryption

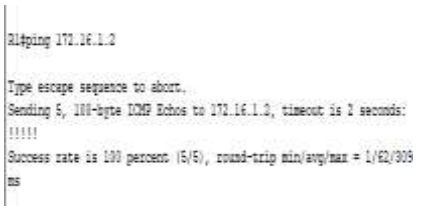
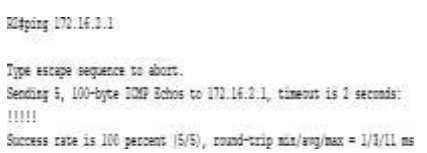
- Configure un MOTD Banner
  S3 (config)# banner motd # Se prohíbe el acceso no autorizado. #

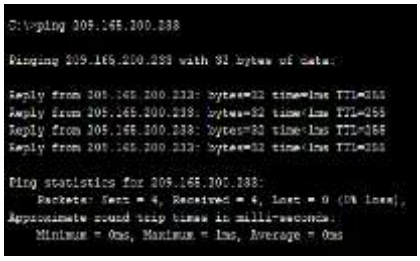
Paso 7: Verificar la conectividad de la red

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 18. Escenario 2 - Verificación conectividad red

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	 Figura 30 Escenario 2 - Reultado R2
R2	R3, S0/0/1	172.16.2.1	 Figura 31 Escenario 2 - Reultado R3

Desde	A	Dirección IP	Resultados de ping
PC de Internet	Gateway predeterminado	209.15.200.233	 Figura 32 Escenario 2 - Reultado Gateway

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

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

Paso 1: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 19. Escenario 2 - Configuración interface 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	
Apagar todos los puertos sin usar	

- Crear la base de datos de VLAN

```
S1(config)#Vlan 21
S1(config-vlan) #Name Contabilidad
S1(config-vlan) #Vlan 23
S1(config-vlan) #Name Ingenieria
S1(config-vlan) #Vlan 99
S1(config-vlan) #Name Administracion
```

- Asignar la dirección IP de administración.

```
S1(config)#interface vlan 99
S1(config-if) #ip address 192.168.99.2 255.255.255.0
S1(config-if) #no shutdown
S1(config-if) #exit
```

- Asignar el gateway predeterminado

```
S1(config)#ip default-gateway 192.168.99.1
```

- Forzar el enlace troncal en la interfaz F0/3

```
S1(config)#interface f0/3
S1(config-if) #Switchport mode trunk
S1(config-if) #Switchport trunk native vlan 1
S1(config-if) #exit
```

- Forzar el enlace troncal en la interfaz F0/5

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

- Configurar el resto de los puertos como puertos de acceso

```
S1(config)#interface range f0/1-2, f0/4, f0/6-24, g0/1-2
S1(config-if-range) #switchport mode access
S1(config-if-range) #exit
```

- Asignar F0/6 a la VLAN 21

```
S1(config)#interface f0/6
S1(config-if) #switchport access vlan 21
S1(config-if) #exit
```

- Apagar todos los puertos sin usar
  S1(config)#interface range f0/1-2, f0/4, f0/7-24, g0/1-2
  S1(config-if-range) #shutdown

Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 20. Escenario 2 - Configuración interface 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 23	
Apagar todos los puertos sin usar	

- Crear la base de datos de VLAN
  S3(config)#Vlan 21
  S3(config-vlan) #Name Contabilidad
  S3(config-vlan) #Vlan 23
  S3(config-vlan) #Name Ingenieria
  S3(config-vlan) #Vlan 99
  S3(config-vlan) #Name Administracion

- Asignar la dirección IP de administración.
  S3(config)#interface vlan 99
  S3(config-if) #ip address 192.168.99.3 255.255.255.0
  S3(config-if) #no shutdown
  S3(config-if) #exit

- Asignar el gateway predeterminado
  S3(config)#ip default-gateway 192.168.99.1

- Forzar el enlace troncal en la interfaz F0/3
  S3(config)#interface f0/3
  S3(config-if) #Switchport mode trunk
  S3(config-if) #Switchport trunk native vlan 1
  S3(config-if) #exit

- Configurar el resto de los puertos como puertos de acceso
  S3(config)#interface range f0/1-2, f0/4-24, g0/1-2
  S3(config-if-range) #switchport mode access
  S3(config-if-range) #exit

- Asignar F0/18 a la VLAN 23
  S3(config)#interface f0/18
  S3(config-if) #switchport access vlan 23
  S3(config-if) #exit

- Apagar todos los puertos sin usar
  S3(config)#interface range f0/1-2, f0/4-17, f0/19-24, g0/1-2
  S3(config-if-range) #shutdown

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 21. Escenario 2 - Configuración interface 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	

- Configurar la subinterfaz 802.1Q .21 en G0/1

```
R1(config)#interface g0/1.21
R1(config-subif)#description VLAN 21
R1(config-subif)#encapsulation dot1Q 21
R1(config-subif)#ip address 192.168.21.1 255.255.255.0
R1(config-subif)#exit
```

- Configurar la subinterfaz 802.1Q .23 en G0/1

```
R1(config)#interface g0/1.23
R1(config-subif)#description VLAN 23
R1(config-subif)#encapsulation dot1Q 23
R1(config-subif)#ip address 192.168.23.1 255.255.255.0
R1(config-subif)#exit
```

- Configurar la subinterfaz 802.1Q .99 en G0/1

```
R1(config)#interface g0/1.23
R1(config-subif)#description VLAN 23
R1(config-subif)#encapsulation dot1Q 23
R1(config-subif)#ip address 192.168.23.1 255.255.255.0
R1(config-subif)#exit
```

- Activar la interfaz G0/1

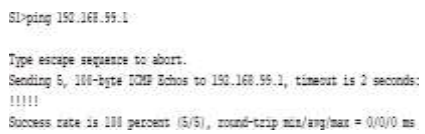
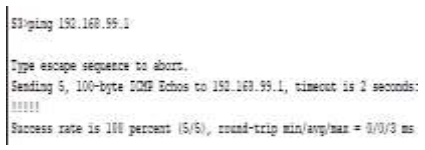
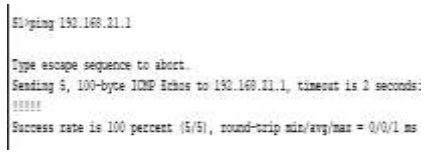
```
R1(config-if)#no shutdown
```

Paso 4: Verificar la conectividad de la red

Utilice el comando **ping** para probar la conectividad entre los switches y el R1. Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 22. Escenario 2 - Verificación red

Desde	A	Dirección IP	Resultados de ping

S1	R1, dirección VLAN 99	192.168.99.1	 Figura 33. Escenario 2 - Resultado S1 VLAN 99
S3	R1, dirección VLAN 99	192.168.99.1	 Figura 34 Escenario 2 - Resultado S3 -VLAN 99
S1	R1, dirección VLAN 21	192.168.21.1	 Figura 35 Escenario 2 - Resultado S1 VLAN 21
S3	R1, dirección VLAN 23	192.168.23.1	 Figura 36 Escenario 2 - Resultado S3 VLAN 23

Parte 4: Configurar el protocolo de routing dinámico OSPF

Paso 1: Configurar OSPF en el R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 23. Escenario 2 - OSPF R1

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	
Anunciar las redes conectadas directamente	Asigne todas las redes conectadas directamente.
Establecer todas las interfaces LAN como pasivas	
Desactive la sumarización automática	

- Configurar OSPF área 0

```
R1(config)#router rip
R1(config-router)#version 2
```

- Anunciar las redes conectadas directamente

```
R1(config-router)#do show ip route connected
        C 172.16.1.0/30 is directly connected, Serial0/0/0
        C 192.168.21.0/24 is directly connected, GigabitEthernet0/1.21
        C 192.168.23.0/24 is directly connected, GigabitEthernet0/1.23
        C 192.168.99.0/24 is directly connected, GigabitEthernet0/1.99
R1(config-router)#network 172.16.1.0
R1(config-router)#network 192.168.21.0
R1(config-router)#network 192.168.23.0
R1(config-router)#network 192.168.99.0
```

- Establecer todas las interfaces LAN como pasivas

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

- Desactive la sumarización automática.

```
R1(config-router)#no auto-summary
```

Paso 2: Configurar OSPF en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla 24. Escenario 2 - OSPF R2

Elemento o tarea de configuración	Especificación

Configurar OSPF área 0	
Anunciar las redes conectadas directamente	**Nota:** Omitir la red G0/0.
Establecer la interfaz LAN (loopback) como pasiva	
Desactive la sumarización automática.	

- Configurar OSPF área 0

```
R2(config)#router rip
R2(config-router)#version 2
```

- Anunciar las redes conectadas directamente

```
R2(config-router)#do show ip route connected
        C 10.10.10.10/32 is directly connected, Loopback0
        C 172.16.1.0/30 is directly connected, Serial0/0/0
        C 172.16.2.0/30 is directly connected, Serial0/0/1
        C 209.165.200.232/29 is directly connected, GigabitEthernet0/0
R2(config-router)#network 10.10.10.10
R2(config-router)#network 172.16.1.0
R2(config-router)#network 172.16.2.0
```

- Establecer la interfaz LAN (loopback) como pasiva

```
R2(config-router)#passive-interface loopback 0
```

- Desactive la sumarización automática.

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

Paso 3: Configurar OSPFv3 en el R2

La configuración del R3 incluye las siguientes tareas:

Tabla 25. Escenario 2 - OSPFv3 R2

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	
Anunciar redes IPv4 conectadas directamente	
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	
Desactive la sumarización automática.	

- Configurar OSPF área 0

```
R3(config)#router rip
R3(config-router)#version 2
```

- Anunciar las redes conectadas directamente

```
R3(config-router)#Do show ip route connected
        C 172.16.2.0/30 is directly connected, Serial0/0/1
        C 192.168.4.0/24 is directly connected, Loopback4
        C 192.168.5.0/24 is directly connected, Loopback5
        C 192.168.6.0/24 is directly connected, Loopback6
R3(config-router)#network 172.16.2.0
R3(config-router)#network 192.168.4.0
R3(config-router)#network 192.168.5.0
R3(config-router)#network 192.168.6.0
```

- 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
```

- Desactive la sumarización automática.

```
R3(config-router)#no auto-summary
```

Paso 5: Verificar la información de OSPF

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

Tabla 26. Escenario 2 - Verificación 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?	
¿Qué comando muestra solo las rutas OSPF?	
¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	

Parte 5: Implementar DHCP y NAT para IPv4

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

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 27. Escenario 2 - R1 DHCP R1

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	
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 IP en la VLAN 21 para configuraciones estáticas

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

- Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas

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

- Crear un pool de DHCP para la VLAN 21.

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

- Crear un pool de DHCP para la VLAN 23

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

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

La configuración del R2 incluye las siguientes tareas:

Tabla 28. Escenario 2 - R1 DHCP R2

Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	Nombre de usuario: **webuser** Contraseña: **cisco12345** Nivel de privilegio: **15**
Habilitar el servicio del servidor HTTP	
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	
Crear una NAT estática al servidor web.	Dirección global interna: **209.165.200.229**
Asignar la interfaz interna y externa para la NAT estática	
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
  R2(config)#username webuser privilege 15 secret cisco12345

- Habilitar el servicio del servidor HTTP
  R2(config)#ip http server

- Configurar el servidor HTTP para utilizar la base de datos local para la autenticación
  R2(config)#ip http autentication local

- Crear una NAT estática al servidor web.
  R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229

- Asignar la interfaz interna y externa para la NAT estática

```
R2(config)#interface g0/0
R2(config-if)#ip nat outside
R2(config-if)#exit
R2(config)#interface s0/0/0
R2(config-if)#ip nat outside
R2(config-if)#exit
R2(config)#interface s0/0/1
R2(config-if)#ip nat outside
R2(config-if)#exit
```

- Configurar la NAT dinámica dentro de una ACL privada

```
R2(config)#Access-list 1 permit 192.168.21.0 0.0.0.255
R2(config)#Access-list 1 permit 192.168.23.0 0.0.0.255
R2(config)#Access-list 1 permit 192.168.4.0 0.0.3.255
```

- Defina el pool de direcciones IP públicas utilizables.

```
R2(config)#ip nat pool INTERNET 209.165.200.233 209.165.200.236 netmask 255.255.255.248
```

- Definir la traducción de NAT dinámica

```
R2(config)#Ip nat inside source list 1 pool INTERNET
```

Paso 3: Verificar el protocolo DHCP y la NAT estática

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

Tabla 29. Escenario 2 - Verificación

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	
Verificar que la PC-A pueda hacer ping a la PC-C **Nota:** Quizá sea necesario deshabilitar el firewall de la PC.	

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**	

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

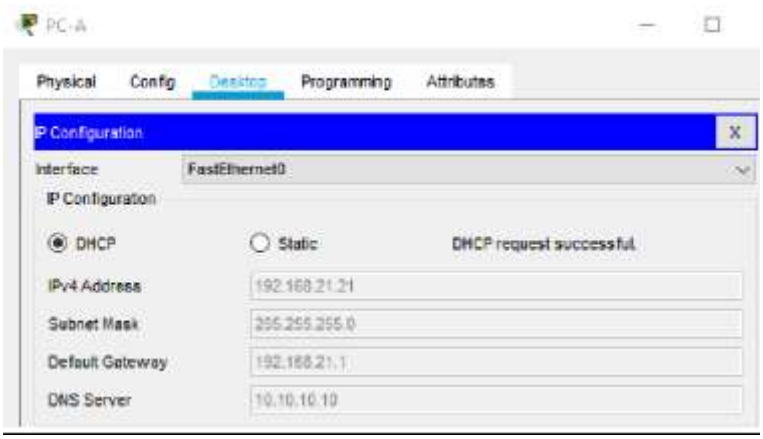


Figura 37. Escenario 2 - DHCP PC-A

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

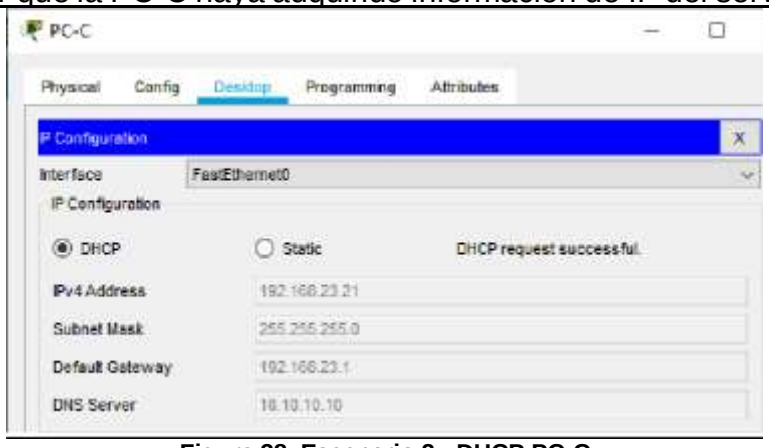


Figura 38. Escenario 2 - DHCP PC-C

- Verificar que la PC-A pueda hacer ping a la PC-C

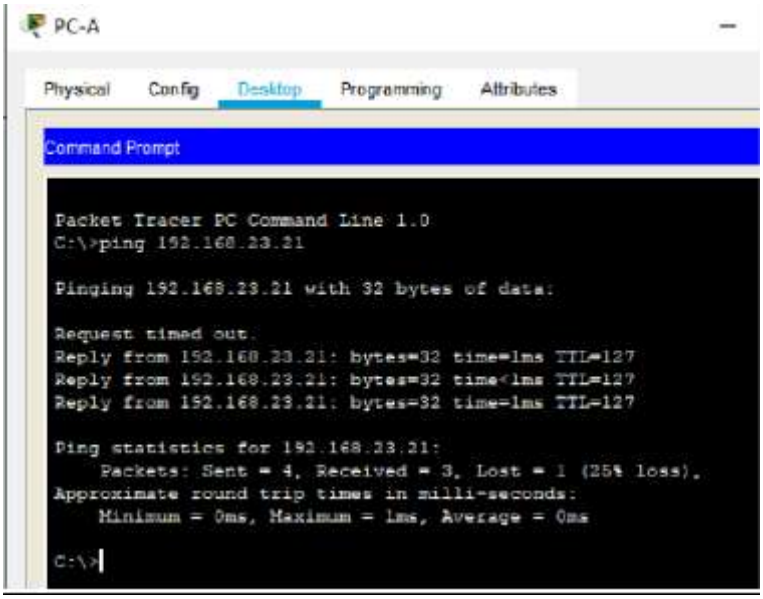


Figura 39. Escenario 2 - PC-A a PC-C

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

Figura 40. Escenario 2 - Web 229

Paso 4: Configurar NTP

Tabla 30. Escenario 2 - Configuración 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.	
Verifique la configuración de NTP en R1.	

- Ajuste la fecha y hora en R2.
  R2#clock set 09:00:00 05 mar 2016
  R2#show clock
  9:0:8.786 UTC Sat Mar 5 2016

- Configure R2 como un maestro NTP.
  R2(config)#ntp master 5

- Configurar R1 como un cliente NTP.
  R2(config)#Ntp server 172.16.1.2

- Configure R1 para actualizaciones de calendario periódicas con hora NTP.
  R2(config)#Ntp update-calendar

- Verifique la configuración de NTP en R1.
  R1#show nps associations

Parte 6: Configurar y verificar las listas de control de acceso (ACL)

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

Tabla 31. Escenario 2 - VTY R2

Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	Nombre de la ACL: **ADMIN-MGT**
Aplicar la ACL con nombre a las líneas VTY	
Permitir acceso por Telnet a las líneas de VTY	
Verificar que la ACL funcione como se espera	

- Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2
  R2(config)#ip access-list standard ADMIN-MGT
  R2(config-std-nacl)#permit host 172.16.1.1
  R2(config-std-nacl)#exit

- Aplicar la ACL con nombre a las líneas VTY
  R2(config)#line vty 0 5
  R2(config-line)#access-class ADMIN-MGT in

- Permitir acceso por Telnet a las líneas de VTY
  R2(config-line)#transport input telnet

- Verificar que la ACL funcione como se espera
  R1#telnet 172.16.1.2
  Trying 172.16.1.2 ...Open Se prohbe el acceso no autorizado.
  User Access Verification
  Password:
  R2>

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

Tabla 32. Escenario 2 - CLI

Descripción del comando	Entrada del estudiante (comando)

Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	
Restablecer los contadores de una lista de acceso	
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	
¿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.
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	

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

```
R2#show access-list
Standard IP access list 1
10 permit 192.168.21.0 0.0.0.255
20 permit 192.168.23.0 0.0.0.255
30 permit 192.168.4.0 0.0.3.255
Standard IP access list ADMIN-MGT
10 permit host 172.16.1.1 (2 match(es))

R2#show ip access-list
Standard IP access list 1
10 permit 192.168.21.0 0.0.0.255
20 permit 192.168.23.0 0.0.0.255
30 permit 192.168.4.0 0.0.3.255
Standard IP access list ADMIN-MGT
10 permit host 172.16.1.1 (2 match(es))
```

- Restablecer los contadores de una lista de acceso

```
R2: Clear ip Access-list counters
```

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

  R2#show ip interface
  GigabitEthernet0/0 is up, line protocol is up (connected)
  Internet address is 209.165.200.233/29
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound access list is not set

- ¿Con qué comando se muestran las traducciones NAT?

  R2#Show ip nat translations

Pro	Inside global	Inside local	Outside local	Outside global
---	209.165.200.229	10.10.10.10	---	---

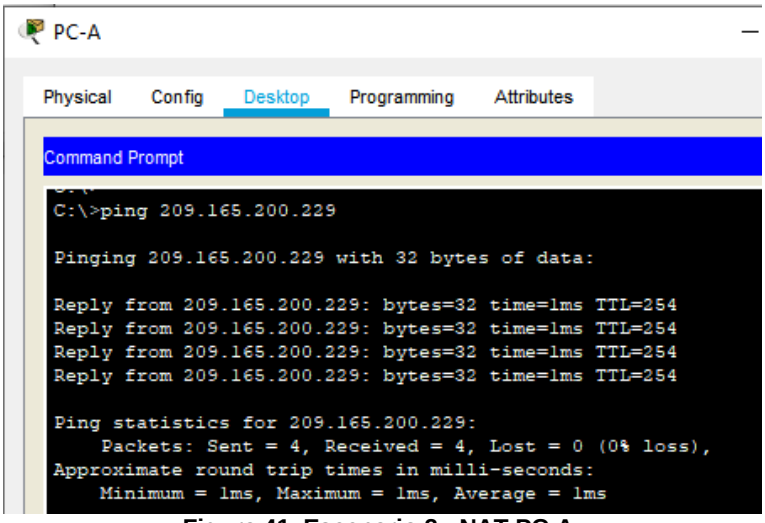


Figura 41. Escenario 2 - NAT PC-A

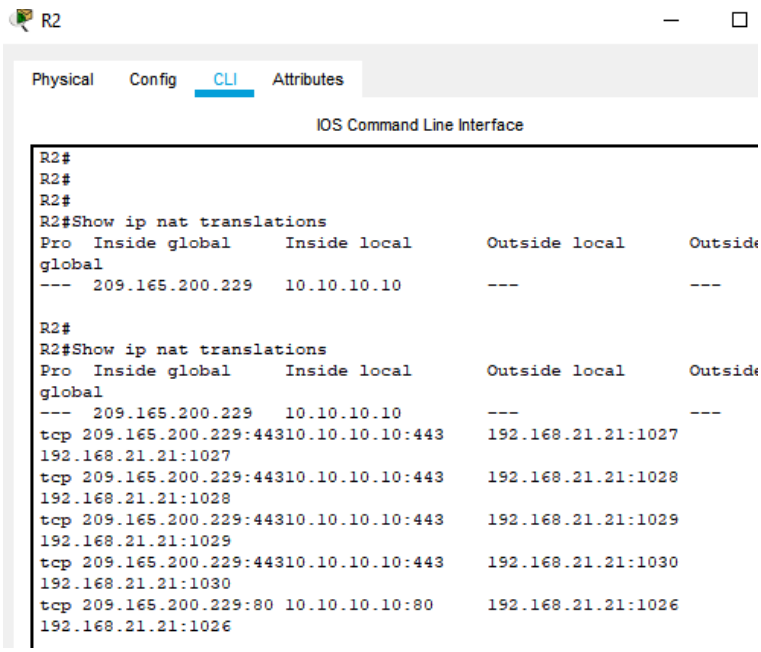


Figura 42. Escenario 2 - NAT R2

- ¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?
  R2#clear ip nat translation *

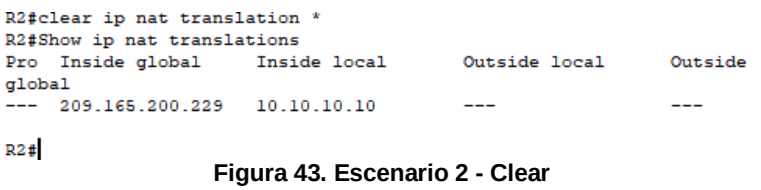


Figura 43. Escenario 2 - Clear

CONCLUSIONES

La utilización de las herramientas Packet Tracer Cisco, permite la creación de escenarios y de esta forma realizar el análisis del comportamiento de la red, basados en los protocolos y métricas de enrutamientos.

La configuración de Switch, creando protocolos de segmentaciones por VLAN, creando entornos empresariales y jerarquía adentro de una red

La identificación de problemas en la comunicación y configuración debido a las actualizaciones de IOS, lo cual permite realizar el análisis y la identificación y planteamiento de las soluciones.

REFERENCIAS BIBLIOGRÁFICAS

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

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

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

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

CISCO. (2019). Capa de transporte. Fundamentos de Networking. Recuperado de:

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

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

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

CISCO. (2019). Routing Estático. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#2

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

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

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

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

UNAD (2017). Principios de Enrutamiento [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgOyjWeh6timi_Tm

Anexos

I. **Link desarrollo de los escenarios**
https://drive.google.com/drive/folders/1IXSxJydBwUwTdpvX5Q-hLO1j9HQUBVqz?usp=sharing

II. **Link Articulo científico**
https://drive.google.com/drive/folders/1ykf0BwMY1Nif5RBs0N0m6ZFiYsMuZ9KR?usp=sharing