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

MARIA ALEJANDRA POLANCO ANDRADE

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA

PROGRAMA INGENIERÍA DE SISTEMAS

BOGOTÁ D.C.

OCTUBRE DE 2020

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

MARIA ALEJANDRA POLANCO ANDRADE

Diplomado de profundización CISCO (Diseño e implementación de soluciones integradas LAN/WAN)

DIRECTOR-TUTOR

ING. JOSÉ IGNACIO CARDONA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA

PROGRAMA INGENIERÍA DE SISTEMAS

BOGOTÁ D.C.

OCTUBRE DE 2020

NOTA ACEPTACION

_____
_____
_____
_____
_____

_____
Firma del presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

Bogotá, (Noviembre 30, 2020)

DEDICATORIA

En primer lugar, a Dios , pues es mi motor y guía en cada paso, a mi Mamá por ser mi bastón y fortaleza, mi hermana por ser mi orgullo y aliento, mi papá en Sus enseñanzas y rectitud.

AGRADECIMIENTO

Agradezco la dedicación y esfuerzo en cada hora dada de catedra, el tiempo empleado en explicaciones por temas que tal vez se requerían de mayor profundización, por la atención y disposición por el Director y Tutor de este Diplomado y demás asignaturas que hicieron realidad el termino de este peldaño en mi vida.

El entregar este Trabajo en culminación del Diplomado de Profundización Cisco, me llena de alegría , emoción y orgullo, al poder dar el logro a mi familia, quienes siempre estuvieron hay en mi cansancio y tenían una palabra de aliento para yo tener fuerzas y seguir luchando. Agradezco a mis compañeros, que estuvieron en apoyo y salvamento. En general, Gracias.

TABLA DE CONTENIDO

RESUMEN **7**

GLOSARIO **7**

INTRODUCCIÓN **9**

OBJETIVO GENERAL **10**

OBJETIVOS ESPECIFICOS **10**

ESCENARIO NO.1 ..... **11**

PARTE 1: INICIALIZAR Y RECARGAR Y CONFIGURAR ASPECTOS BÁSICOS DE LOS DISPOSITIVOS 12

Paso 1. Inicializar y volver a carga el Router y el Switch *12*

Paso 2. Configurar R1. ..... *15*

Paso 3. Configurar S1 Y S2 ..... *25*

PARTE 2: CONFIGURACIÓN DE LA INFRAESTRUCTURA DE RED (VLAN, TRUNKING, ETHERCHANNEL). 32

Paso 1. Configuración S1. ..... *32*

Paso 2. Configure el S2. ..... *38*

PARTE 3. CONFIGURAR SOPORTE HOST 42

Paso 1: Configuración R1 ..... *42*

Paso2. Configurar los Servidores *45*

PARTE 4: PROBAR Y VERIFICAR LA CONECTIVIDAD DE EXTREMO A EXTREMO 45

ESCENARIO 2 ..... **48**

PARTE 1: INICIALIZAR DISPOSITIVOS 49

Paso 1. Inicializar y volver a cargar los routers y los switches *49*

PARTE 2. CONFIGURAR LOS PARÁMETROS BÁSICOS DE LOS DISPOSITIVOS 51

Paso 1. Configurar la computadora de Internet *51*

Paso 2: Configurar R1 ..... *52*

Paso 2: Configurar R2 ..... *56*

Paso 3: Configurar R3 ..... *62*

Paso 4: Configurar S1 ..... *68*

Paso 5: Configurar el S3 ..... *71*

Paso 6: Verificar la conectividad de la red *74*

PARTE 3: CONFIGURAR LA SEGURIDAD DEL SWITCH, LAS VLAN Y EL ROUTING ENTRE VLAN 74

Paso 1. Configurar S1 ..... *74*

Paso 2: Configurar el S3 ..... *78*

Paso 3: Configurar R1 ..... *81*

Paso 4: Verificar la conectividad de la red *83*

PARTE 4: CONFIGURAR EL PROTOCOLO DE ROUTING DINÁMICO OSPF 83

Paso 1: Configurar OSPF en el R1. ..... *83*

Paso 2: Configurar OSPF en el R2. ..... *84*

Paso 3: Configurar OSPF en el R3. ..... *84*

Paso 4: Verificar la información de OSPF *85*

PARTE 5: IMPLEMENTAR DHCP Y NAT PARA IPV4. 85

Paso 1: Configurar el R1 como servidor de DHCP para las VLAN 21 y 23 ..... *85*

Paso 2: Configurar la NAT estática y dinámica en el R2 ..... *86*

Paso 3: Verificar el protocolo DHCP y la NAT estática *87*

CONCLUSIONES 88

LINK ESCENARIOS PACKET TRACER 88

BIBLIOGRAFÍA **89**

RESUMEN

En el presente trabajo se desarrolla con el fin de poner en práctica las 10 Unidades vistas en el presente Diplomado de Profundización, donde se evidencia los conocimientos y habilidades adquiridos, lo cual forja a nivel profesional un ser integro.

Dichas habilidades desarrolladas permitirán al individuo administrar, diseñar y gestionar sistemas en tecnologías de información y comunicaciones, donde se enfocará en la gestión y organización de Redes.

El primer Escenario está basado en las primeras 5 Unidades vistas y el Segundo Escenario (un poco más complejo) abarca las 10 Unidades estudiadas.

GLOSARIO

TELECOMUNICACIONES: Conjunto de medios de comunicación a distancia o transmisión de palabras, sonidos, imágenes o datos en forma de impulsos o señales electrónicas o electromagnéticas.

REDES: interconexión de un número determinado de computadores (o de redes, a su vez) mediante dispositivos alámbricos o inalámbricos que, mediante impulsos eléctricos, ondas electromagnéticas u otros medios físicos, les permiten enviar y recibir información en paquetes de datos, compartir sus recursos y actuar como un conjunto organizado.

LAN: es la abreviatura de Local Area Network. Estas redes vinculan computadoras que se hallan en un espacio físico pequeño (Área limitada), como una oficina o un edificio. La interconexión se realiza a través de un cable o de ondas.

ROUTER: es un dispositivo que permite interconectar computadoras que funcionan en el marco de una red. Su función: se encarga de establecer la ruta que destinará a cada paquete de datos dentro de una red informática.

SWITCH: es un dispositivo que se utiliza para conectar equipos en red, formando una red de área local (LAN) y se encargan de la interconexión de dispositivos cableados, que siguen las especificaciones técnicas del estándar Ethernet.

SUBNETTING: hace referencia a la subdivisión de una red en varias subredes. El subneteo permite a los administradores de red, por ejemplo, dividir una red empresarial en varias subredes sin hacerlo público en Internet. Esto se traduce en que el router que establece la conexión entre la red e Internet se especifica como dirección única, aunque puede

que haya varios hosts ocultos. Así, el número de hosts que están a disposición del administrador aumenta considerablemente.

DIRECCIÓN IP: es un conjunto de números que identifica, de manera lógica y jerárquica, a una interfaz en la red (elemento de comunicación/conexión) de un dispositivo (computadora, laptop, teléfono inteligente) que utilice el protocolo (Internet Protocol) o, que corresponde al nivel de red del modelo TCP/IP.

IPV4: Cuarta versión del Internet Protocol (IP), es una representación numérica que identifica una interfaz concreta de manera única en la red. Las direcciones IPv4 tienen una longitud de 32 bits, que permite un máximo de 4 294 967 296 (232) direcciones únicas.

IPV6: es el sucesor del primer protocolo de direccionamiento de Internet, Internet Protocol versión 4 (IPv4). A diferencia de IPv4, que utiliza una dirección IP de 32 bits, las direcciones IPv6 tienen un tamaño de 128 bits. Por lo tanto, IPv6 tiene un espacio de direcciones mucho más amplio que IPv4.

LACP: permite agrupar varios puertos físicos para formar un único canal lógico. LACP permite que un switch negocie un grupo automático mediante el envío de paquetes LACP al peer.

SERVIDOR: Un servidor es un equipo informático que forma parte de una red y provee servicios a otros equipos cliente.

INTRODUCCIÓN

La comunicación es cada vez más ágil, más posible, más real, y es una de las funciones y habilidades dadas a través de las redes de datos y/o redes informáticas, teniendo en cuenta, que todo es un sistema comprendido a nivel hardware y software, bajo el concepto de emisor y receptor, permitiendo compartir recursos e información.

A medida de la evolución, evidenciamos diversos tipos de Red: LAN (Red de Área Local), PAN (Red de Área Personal), MAN (Red de área Metropolitana), WLAN (Red de área local inalámbrica), WAN (Red de área de gran alcance), entre otras. Aunque todas tiene la misma finalidad de interconectar, se diferencian en la escala o grado de alcance de la Red (como se evidencia en sus nombres).

La conectividad a través de la red depende o se despliega desde la configuración de los dispositivos activos, la conexión física (cableado estructurado), punto de red del usuario final, y es allí donde vamos a trabajar en la configuración y simulación de dos escenarios, poniendo en práctica todas las habilidades aprendidas y adquiridas.

Estas habilidades se enfocan en temas con sus comandos a utilizar como:

1. Contraseña al modo privilegiado: Tanto en Router y Switch´s: enable secret Contraseña.
2. Contraseña para acceder por Consola: Tanto en Router y Switch's, desde el modo config: line console 0 -> password contraseña -> login.
3. Encriptación de Contraseña: desde el modo config: service password-encryption.
4. Eliminar y/o Guardar la configuración de un Router y Switch´s: erase Startup-config // copy running-config startup-config.
5. Creación de Vlans, enrutamiento, Dual-stack, entre otros.

La lógica y el manejo de estos conceptos se hará necesario para lograr un éxito en los escenarios.

OBJETIVO GENERAL

Realizar los dos Escenarios propuestos por el Tutor evaluando las habilidades adquiridas en las 10 UNIDADES vista en este Diplomado, donde se forja conocimientos de Redes enfocadas en ambientes productivos.

OBJETIVOS ESPECIFICOS

1. Forjar conocimientos básicos de Networking, mecanismos de comunicación y acceso a la Red.
2. Desarrollar las habilidades en comunicaciones en ethernet y capas superiores, identificando direccionamiento IP y capacidades de Subnetting.
3. Elaborar en los escenarios dispuestos por el tutor, la puesta en funcionamiento de enrutamiento estático, enrutamiento dinámico, direccionamiento estático, direccionamiento dinámico, creación de Vlans, entre otros.

ESCENARIO No.1.

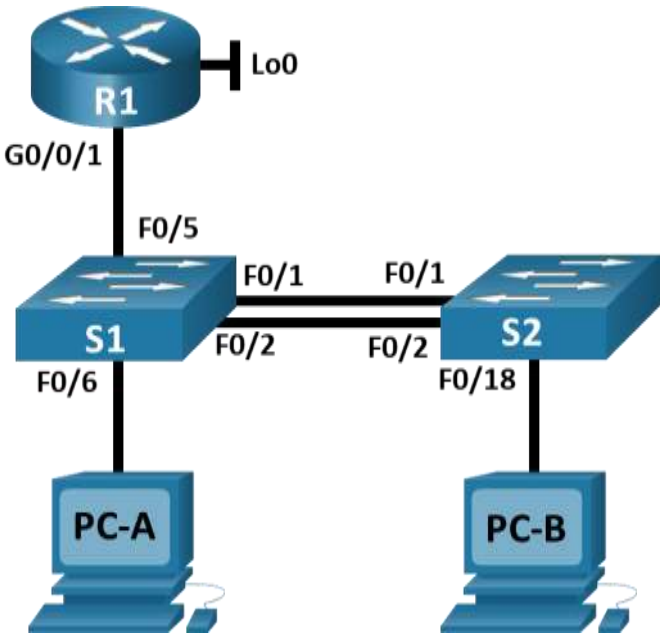


Tabla de VLAN

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

Tabla de asignación de direcciones

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
R1 G0/0/1.2	10.19.8.1 /26	No corresponde
R1 G0/0/1.2	2001:db8:acad:a: :1 /64	No corresponde
R1 G0/0/1.3	10.19.8.65 /27	No corresponde
	2001:db8:acad:b: :1 /64	No corresponde
R1 G0/0/1.4	10.19.8.97 /29	No corresponde
R1 G0/0/1.4	2001:db8:acad:c: :1 /64	No corresponde

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
R1 G0/0/1.6	No corresponde	No corresponde
R1 Loopback0	209.165.201.1 /27	No corresponde
R1 Loopback0	2001:db8:acad:209: :1 /64	No corresponde
S1 VLAN 4	10.19.8.98 /29	10.19.8.97
	2001:db8:acad:c: :98 /64	No corresponde
	fe80: :98	No corresponde
S2 VLAN 4	10.19.8.99 /29	10.19.8.97
S2 VLAN 4	2001:db8:acad:c: :99 /64	No corresponde
S2 VLAN 4	fe80: :99	No corresponde
PC-A NIC	Dirección DHCP para IPv4	DHCP para puerta de enlace predeterminada IPv4
	2001:db8:acad:a: :50 /64	fe80::1
PC-B NIC	DHCP para dirección IPv4	DHCP para puerta de enlace predeterminada IPv4
PC-B NIC	2001:db8:acad:b: :50 /64	fe80::1

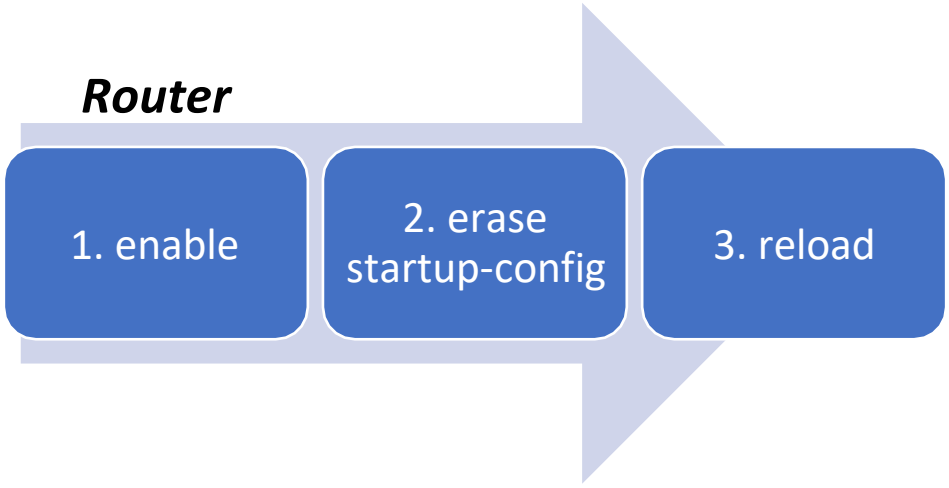
Nota: No hay ninguna interfaz en el Router que admita VLAN 5.

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

Paso 1. Inicializar y volver a carga el Router y el Switch

En el presente paso desarrollamos las instrucciones dadas por el Tutor, teniendo en cuenta los comandos ejecutados y la explicación de cada uno, así:

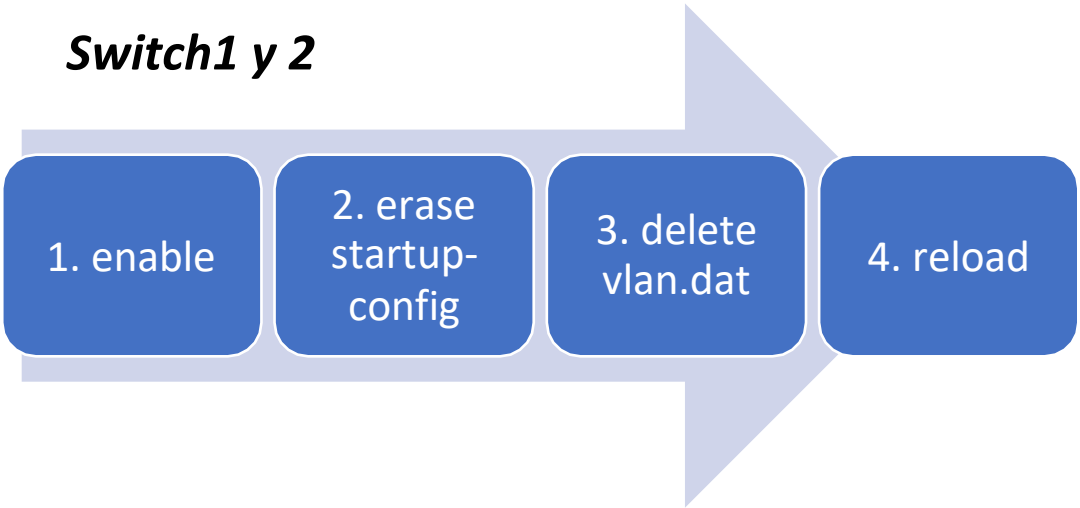
a. Borre las configuraciones de inicio, las VLAN del router y del switch, luego vuelva a cargar los dispositivos.



1. Ingreso al modo privilegiado.
2. Se elimina el Startup-config, situado en la NRAM, la cual es una copia de seguridad de la configuración del router.
3. Reload, función de reinicio del dispositivo, ayudando a ejecutar los cambios.

Sintaxis:

Router>enable
Router#erase startup-config
(confirm)
Router#reload
(confirm)

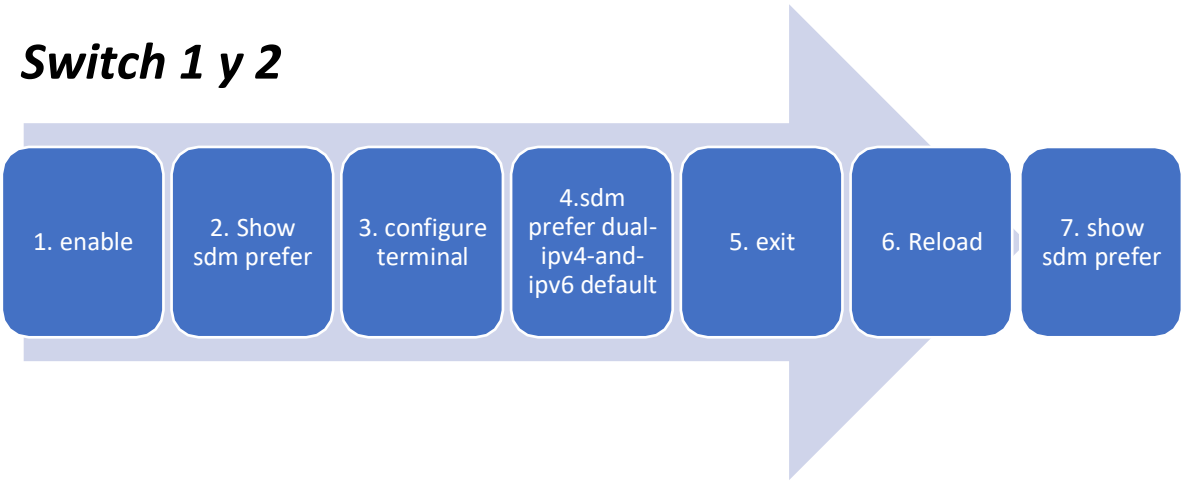


1. Ingreso al modo privilegiado.
2. Se elimina el Startup-config, situado en la NRAM, la cual es una copia de seguridad de la configuración del router.
3. Delete vlan.dat, borra la información de Vlan , en la memoria flash que contiene dicha información.
4. Reload, función de reinicio del dispositivo, ayudando a ejecutar los cambios.

Sintaxis:

Switch> enable
Switch# erase startup-config
(confirmar)
Switch#delete vlan.dat
Switch#Reload
(confirmar)

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



1. enable: Ingreso al modo privilegiado usuario.
2. Show sdm prefer: Se valida la plantilla de enrutamiento (Al evidenciar que no esta habilitada para direccionamiento IPV6, su enrutamiento y que está plantilla no admite routing estático, seguimos con nuestro comando, si está omitimos el siguiente paso)
3. Config: Ingresamos a un nivel privilegiado de configuración, con acceso a más opciones de comandos.
4. Sdm prefer dual-ipv4-and-ipv6 default: Se cambia la plantilla, Habilita el direccionamiento IPV6.
5. Exit: Se sale del nivel de permisos que se encuentre, al nivel inferior siguiente.
6. Reload: función de reinicio del dispositivo, ayudando a ejecutar los cambios.
7. Show sdm prefer: Se valida la plantilla.

SINTAXIS:

Switch>enable
Switch# show sdm prefer
Switch# config terminal
Switch(config)# sdm prefer dual-ipv4-and-ipv6 default
Switch(config)#exit
Switch#Reload
Confirmar
Switch>enable
Switch#Show sdm prefer

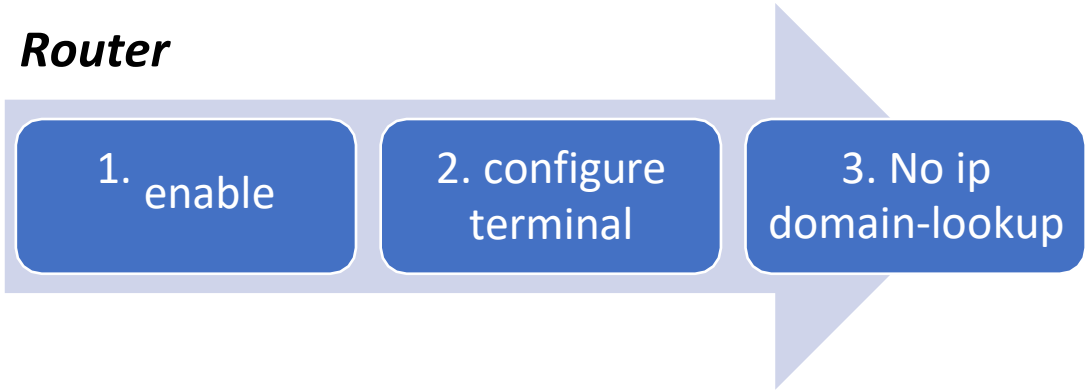
```
S1#show sdm prefer
 The current template is "desktop IPv4 and IPv6 default" template.
 The selected template optimizes the resources in
 the switch to support this level of features for
 8 routed interfaces and 1024 VLANs.

  number of unicast mac addresses:                  2K
  number of IPv4 IGMP groups + multicast routes:    1K
  number of IPv4 unicast routes:                    3K
    number of directly-connected IPv4 hosts:        2K
    number of indirect IPv4 routes:                 1K
  number of IPv6 multicast groups:                  1.125k
  number of directly-connected IPv6 addresses:      2K
  number of indirect IPv6 unicast routes:           1K
  number of IPv4 policy based routing aces:         0
  number of IPv4/MAC qos aces:                      0.5K
  number of IPv4/MAC security aces:                 1K
  number of IPv6 policy based routing aces:         0
  number of IPv6 qos aces:                          0.625k
  number of IPv6 security aces:                     0.5K
```

Paso 2. Configurar R1.

En este paso, seguimos instrucciones del tutor, donde se configura de ceros el Router y sus interfaces, así:

a. Desactivar la búsqueda DNS



3. no ip domain-lookup: Desactiva la traducción de nombres a dirección del dispositivo.

SINTAXIS:

Router>enable
Router#config t
Router (Config)#no ip domain-lookup

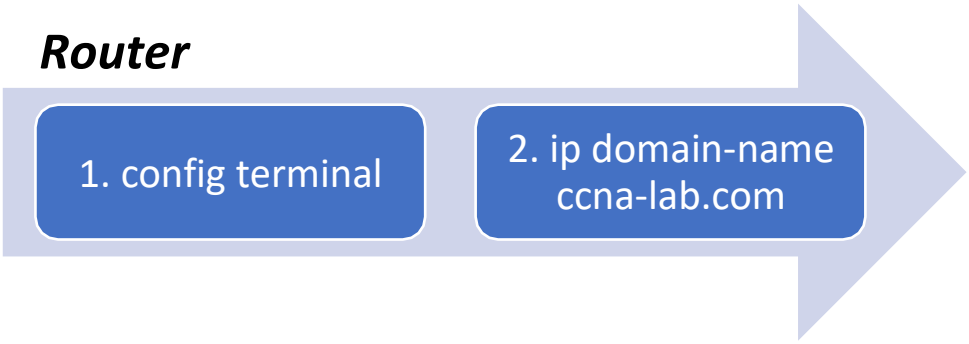
b. Nombre del Router

2. Hostname R1: Desde el modo de configuración, se digita el comando en el Router y/o Switch, cambiando el nombre del dispositivo.

SINTAXIS:

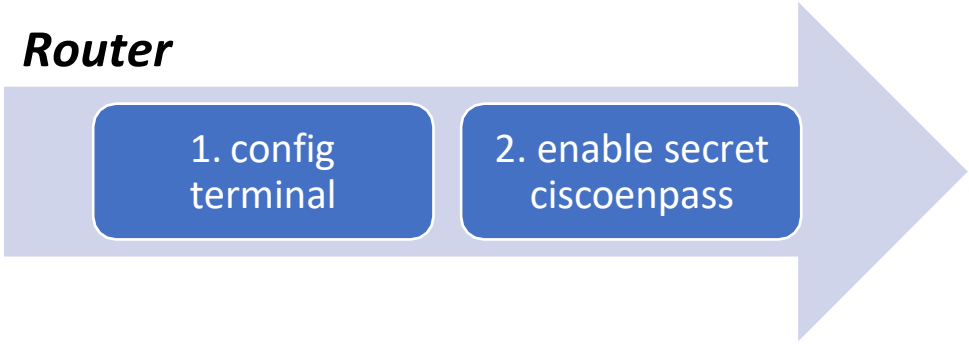
Router#config t
Router(config)# Hostname R1
R1(config)#

c. Nombre del Dominio (ccna-lab.com):



2. ip domain-name “Nombre del Dominio”, Comando para asignar nombre al Dominio del Router.

d. Contraseña cifrada para el modo EXCE privilegiado (ciscoenpass).



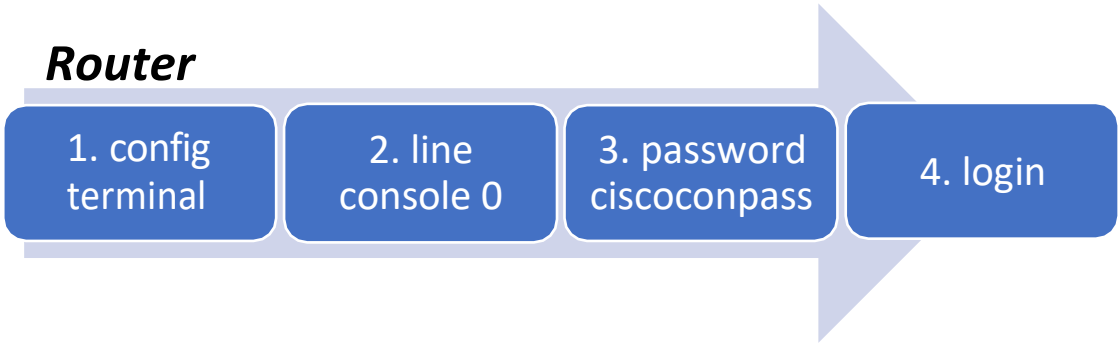
2. Enable secret “contraseña”: Se utiliza para restringir el acceso al modo EXEC privilegiado, adicional, que brinda un nivel de cifrado.

SINTAXIS:

R1>enable
R1#config terminal

R1(config)#enable secret ciscoenpass

e. Contraseña de acceso a la consola (ciscoconpass)

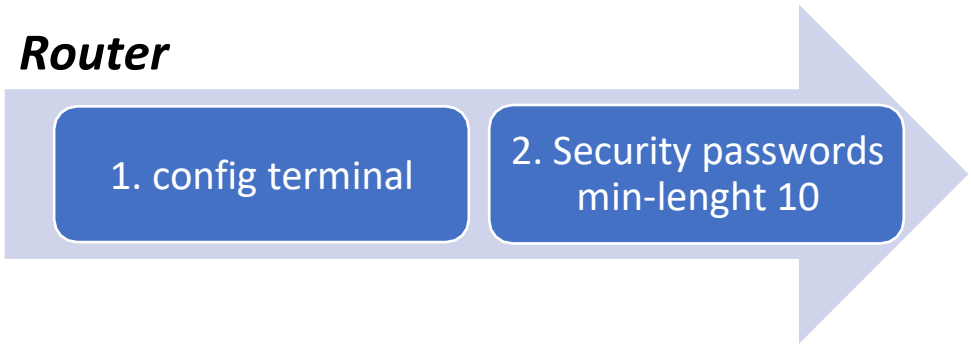


2. line console 0: se usa para ingresa al modo de configuración de la línea de consola, el cero representa la interfaz de consola.
3. password (contraseña): Se usa para especificar la contraseña para la línea de consola.
4. login: configura el Router para que requiera la autenticación al iniciar la sesión.

SINTAXIS:

R1#config t
R1(config) #line con 0
R1(config-line) #password ciscoconpass
R1(config-line) #login

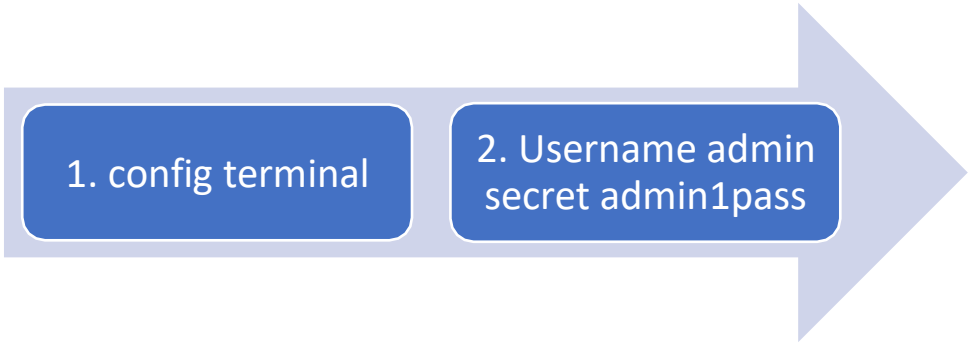
f. Establecer la longitud mínima para las contraseñas (10 caracteres)



2. Security passwords min-lenght 10: Es un comando que restringe el uso de contraseña cortas, siendo un mínimo de caracteres de 10 (en este caso).
SINTAXIS:

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

g. Crear un usuario administrativo en la base de datos local (Nombre de Usuario: admin, password: admin1pass).

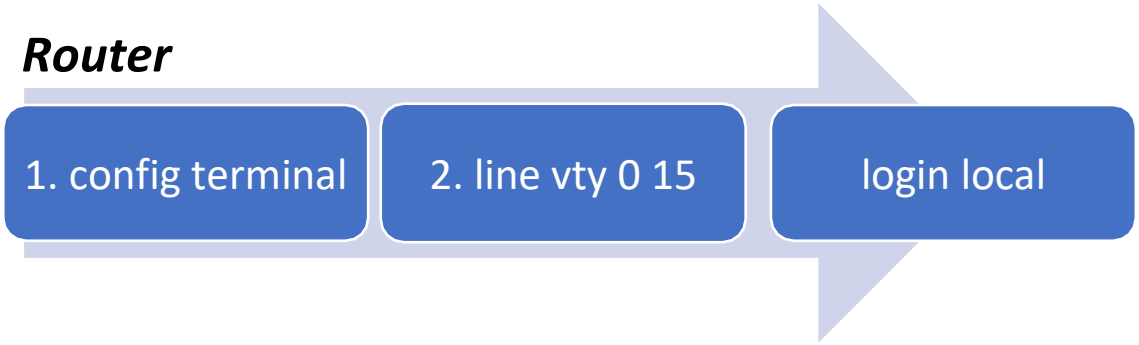


2. Username admin secret admin1pass: Se utiliza para crear un usuario en la base de datos local, donde en Username se especifica el Nombre_Usuario y secret (Contraseña_cifrada).

SINTAXIS:

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

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

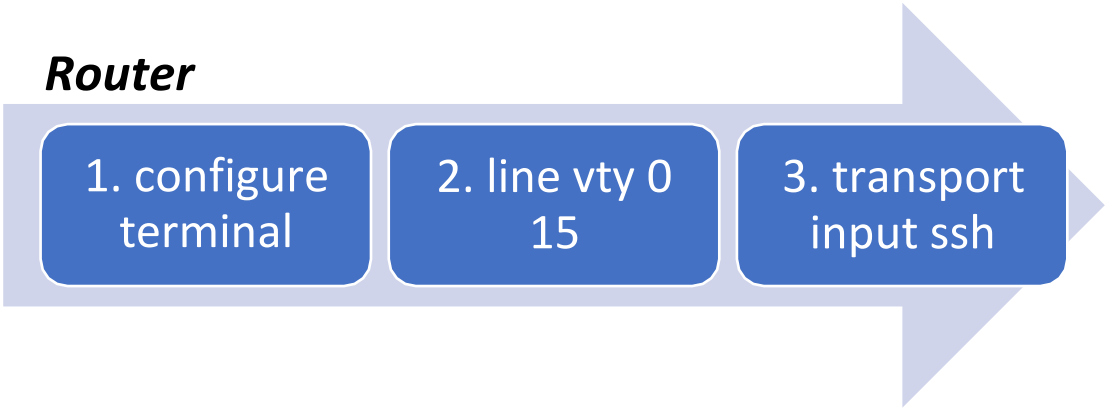


2. Los puertos VTY están enumerados del 0 a 15 y son utilizados para establecer sesiones Telnet, por ende, se ingresa a la configuración y se configura el usuario local (admin).

SINTAXIS:

R1#config t
R1(config)# line vty 0 15
R1(config)# login local

i. Configurar VTY solo aceptando SSH

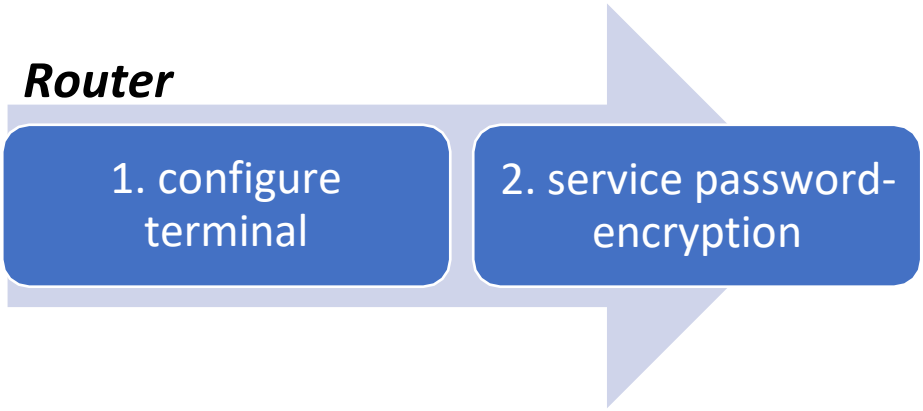


2. Volvemos a la configuración VTY o si no nos salimos seguimos en está.
3. transport input ssh: Se utiliza para acceder solo por SSH.

SINTAXIS:

R1#configure terminal
R1(config)#line vty 0 15
R 1(config-line) #transport input ssh

j. Cifrar las contraseñas de texto no cifrado.

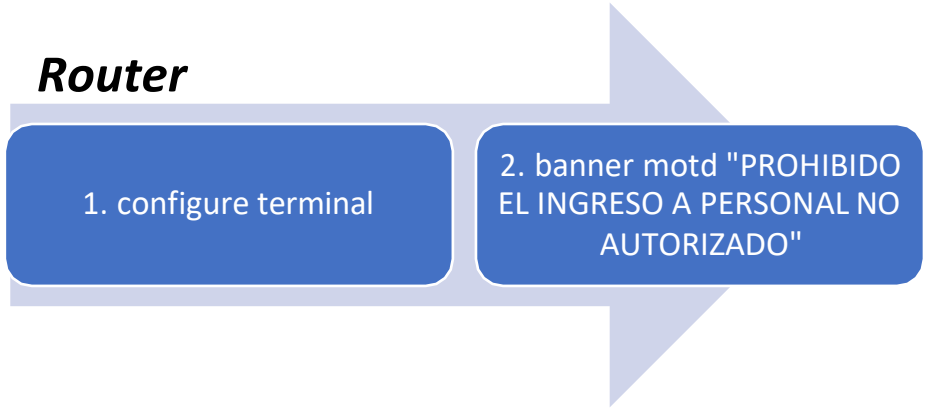


2. Service password-encryption: Se encarga de aplicar un cifrado a todas las contraseñas que se encuentren sin cifrar.

SINTAXIS:

R1#configure terminal
R1(config)#service password-encryption

k. Configure un MOTD Banner

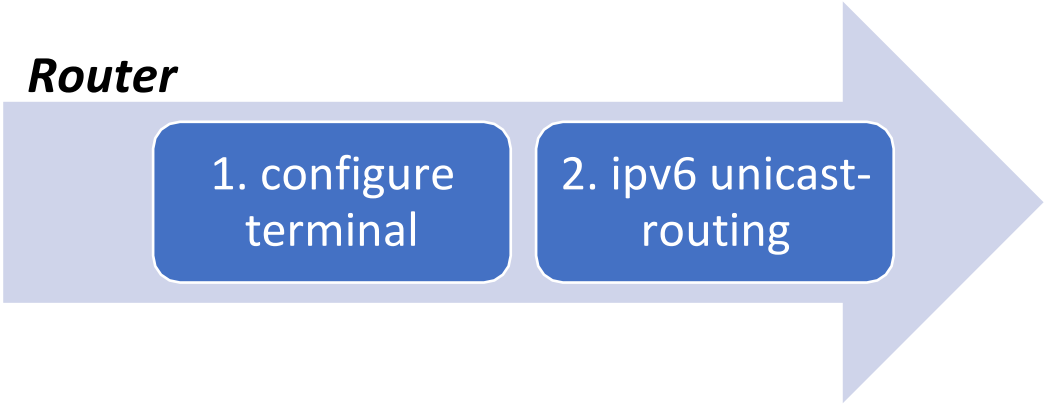


2. banner motd “Mensaje”: Es un Mensaje de aviso al ingreso del dispositivo configurado.

SINTAXIS:

R1#configure terminal
R1(config)#banner motd "PROHIBIDO EL INGRESO DE PERSONAL NO AUTORIZADO"

l. Habilitar el routing ipv6.



2. ipv6 unicast-routing: Permite el enrutamiento de paquetes Ipv6 entre las diferentes interfaces del Router.

SINTAXIS:
R1#configure terminal
R1(config)#ipv6 unicast-routing

m. Configurar interfaz G0/0/1 y subinterfaces

Primero debemos tener en cuenta el direccionamiento asignado por cada interfaz y subinterfaces

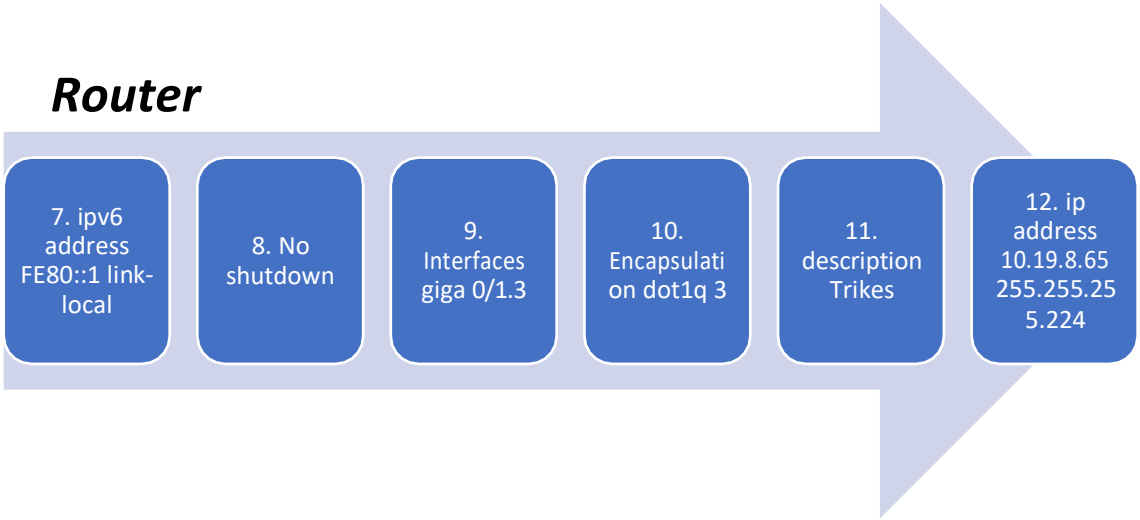
2. Se configura la subinterfaz G0/1.2, ingresando a la configuración.

3. Encapsulation dot1q “Vlan_id”, para habilitar 802.1Q y asociar una vlan específica a la subinterfaz.

4. Description: Descripción de la Subinterfaz

5. ip address (direccionamiento Ipv4): Se le asigna a la Subinterfaz el direccionamiento Ipv4 asignado.

6. ipv6 address (direccionamiento ipv6): Se le asigna a la interfaz el direccionamiento Ipv6 asignado.



7.Ipv6 address FE80::1 link-local: Se establece la dirección local del enlace ipv6, permitiendo que un dispositivo se comunique con otros dispositivos con ipv6 habilitado en el mismo enlace.

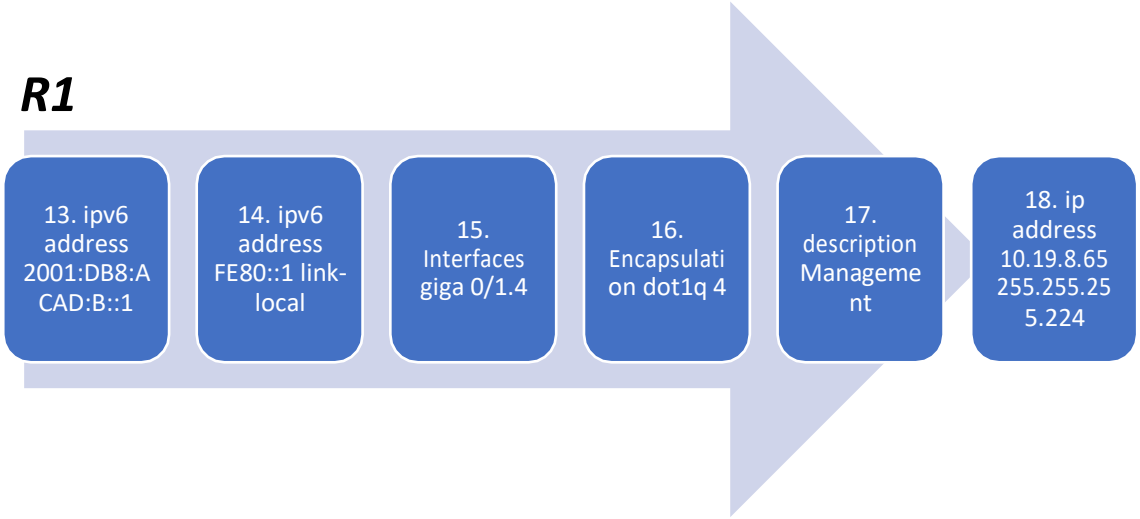
8. No Shutdown: Enciende la Interfaz.

9. Interfaces gig 0/1.3: El comando se utiliza para “invocar” la subinterfaz a seguir configurando.

10. Encapsulation dot1q 3: Encapsulation dot1q “Vlan_id”, para habilitar 802.1Q y asociar una vlan específica a la subinterfaz.

11. Description: Descripción de la Subinterfaz

12. ip address 10.19.8.65 255.255.255.224, Se le asigna a la Subinterfaz el direccionamiento Ipv4 asignado.



13. ipv6 address (direccionamiento ipv6): Se le asigna a la interfaz el direccionamiento Ipv6 asignado.

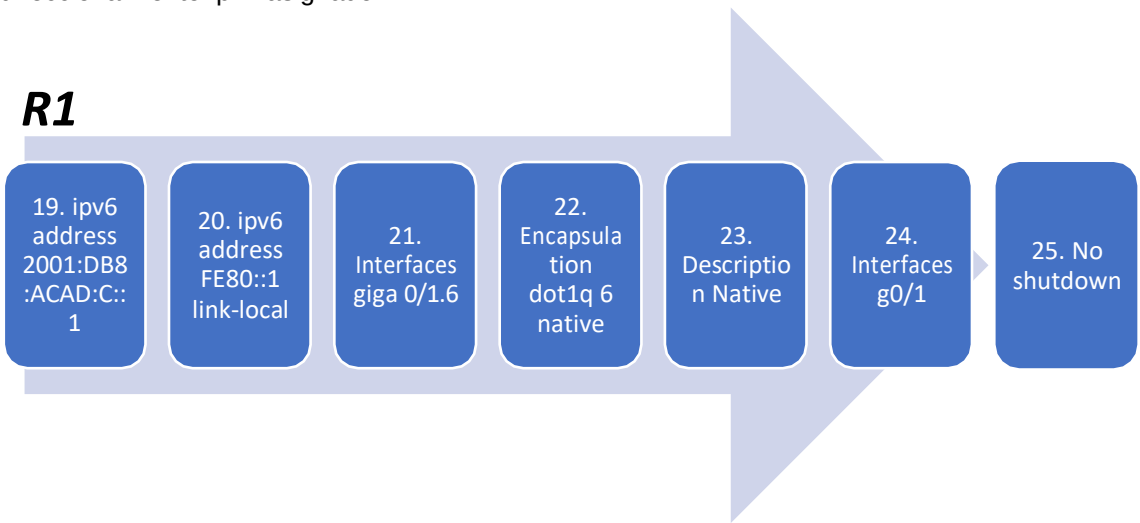
14. Ipv6 address FE80::1 link-local: Se establece la dirección local del enlace ipv6, permitiendo que un dispositivo se comunique con otros dispositivos con ipv6 habilitado en el mismo enlace.

15. Interfaces gig 0/1.4: El comando se utiliza para “invocar” la subinterfaz a seguir configurando.

16. Encapsulation dot1q 3: Encapsulation dot1q “Vlan_id”, para habilitar 802.1Q y asociar una vlan específica a la subinterfaz.

17. Description: Descripción de la Subinterfaz.

18. ip address 10.19.8.97 255.255.255.248, Se le asigna a la Subinterfaz el direccionamiento Ipv4 asignado.



19. ipv6 address 2001:DB8:ACAD:C::1/64, Se le asigna a la interfaz el direccionamiento Ipv6 asignado.

20. Ipv6 address FE80::1 link-local: Se establece la dirección local del enlace ipv6, permitiendo que un dispositivo se comunique con otros dispositivos con ipv6 habilitado en el mismo enlace

21. Interfaces gig 0/1.6: El comando se utiliza para “invocar” la subinterfaz a seguir configurando.

22. Encapsulation dot1q 6 native, Encapsulation dot1q “Vlan_id”, para habilitar 802.1Q y asociar una vlan específica a la subinterfaz, en este caso, al corresponder native se escribe.

23. Description Native, Descripción de la Subinterfaz, no se configura ipv4, ni ipv6 al no estar asignado.

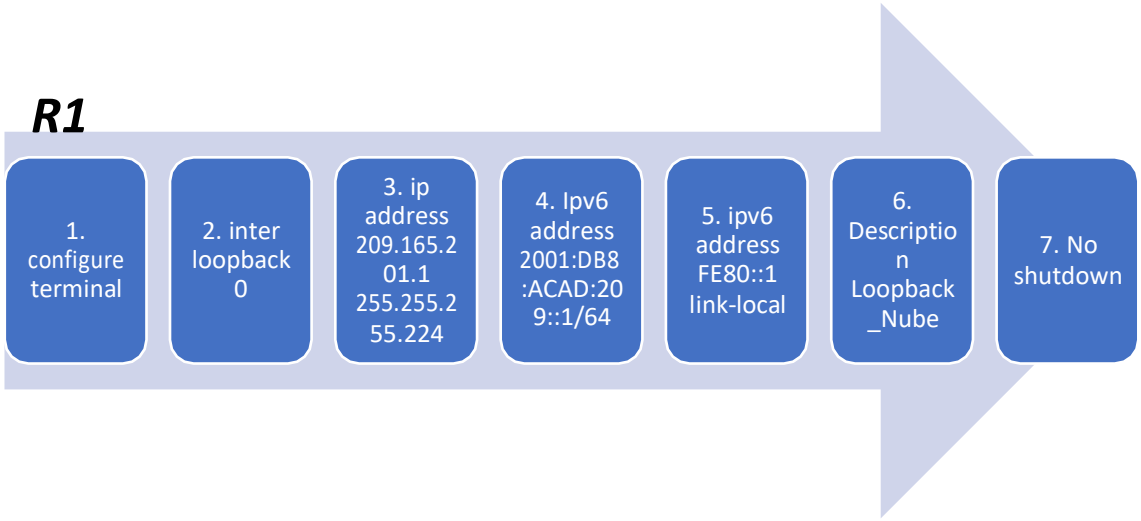
24. Interfaces g0/1, nos vamos a la interfaz general y prendemos la interfaz.

25. no shutdown.

SINTAXIS.

```
R1(config)#inter gigabitEthernet 0/1
R1(config)#inter gigabitEthernet 0/1.2
R1(config-subif) #encapsulation dot1Q 2
R1(config-subif) #description Bikes
R1(config-subif) #ip address 10.19.8.1 255.255.255.192
R1(config-subif) #ipv6 address 2001:db8:acad:a::1/64
R1(config-subif) #ipv6 address fe80::1 link-local
R1(config)#inter gigabitEthernet 0/1.3
R1(config-subif)#encapsulation dot1Q 3
R1(config-subif)#description Trikes
R1(config-subif)#ip address 10.19.8.65 255.255.255.224
R1(config-subif)#ipv6 address 2001:db8:acad:b::1/64
R1(config-subif)#ipv6 address fe80::1 link-local
R1(config)#inter gigabitEthernet 0/1.4
R1(config-subif)#encapsulation dot1Q 4
R1(config-subif)#description Management
R1(config-subif)#ip address 10.19.8.97 255.255.255.248
R1(config-subif)#ipv6 address 2001:db8:acad:c::1/64
R1(config-subif)#ipv6 address fe80::1 link-local
R1(config)#interface gigabitEthernet 0/1.6
R1(config-subif)#encapsulation dot1Q 6
R1(config-subif)#description Parking
R1(config-subif)#exit
R1(config)#inter gigabitEthernet 0/1
R1(config-if)#no shutdown
```

n. 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).

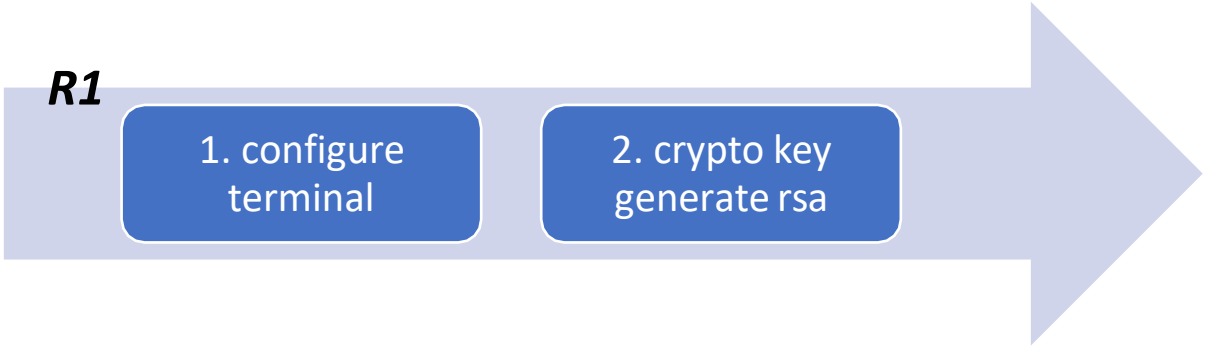


2. Interfaces loopback 0, se habilita e ingresa a configuración, esta interfaz es lógica interna del Router.
3. Ip address 209.165.201.1 255.255.255.224, se establece el direccionamiento ipv4 según lo ordenado.
4. Ipv6 address 2001:DB8:ACAD:209::1/64, Se le asigna a la interfaz el direccionamiento Ipv6 asignado.
5. Ipv6 address FE80::1 link-local: Se establece la dirección local del enlace ipv6, permitiendo que un dispositivo se comunique con otros dispositivos con ipv6 habilitado en el mismo enlace
6. Description, Descripción de la Interfaz.

SINTAXIS.

R1(config)#inter loopback 0
R1(config-if) #ip address 209.165.201.1 255.255.255.224
R1(config-if) #ipv6 address 2001:db8:acad:209::1/64
R1(config-if) #ipv6 address FE80::1 link-local
R1(config-if) #i Description Loopback_Nude

o. Generar una clave de cifrado RSA (Modulo de 1024 bits).



2.crypto key generate rsa, este comando da el tamaño al cifrado de las llaves en este caso de 1024 bits de longitud.

SINTAXIS.

R1(config)#crypto key generate rsa
The name for the keys will be: R1.ccna-lab.com

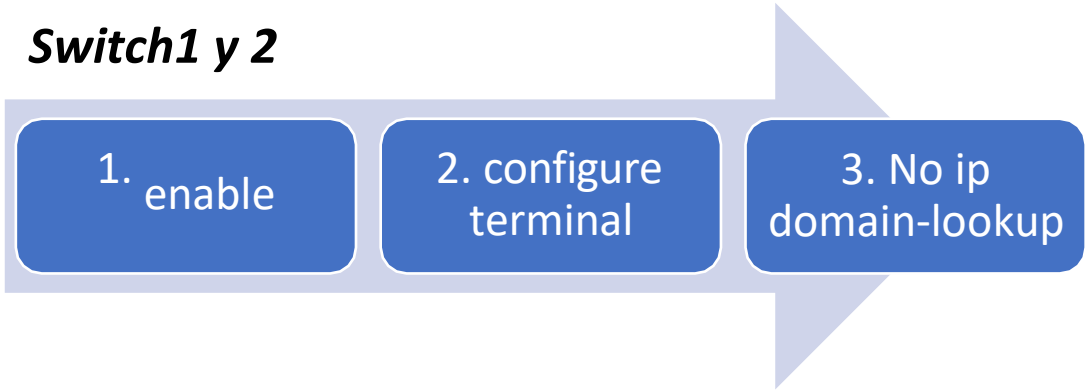
Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes.
How many bits in the modulus [512]: 1024

% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

Paso 3. Configurar S1 Y S2

En este paso procedemos a configurar cada Switch siguiendo las instrucciones del tutor, así:

a. Desactivar la búsqueda DNS.



. no ip domain-lookup: Desactiva la traducción de nombres a dirección del dispositivo.

SINTAXIS:

Switch>enable
Switch #config t
Switch (Config)#no ip domain-lookup

b. Nombre del Switch.

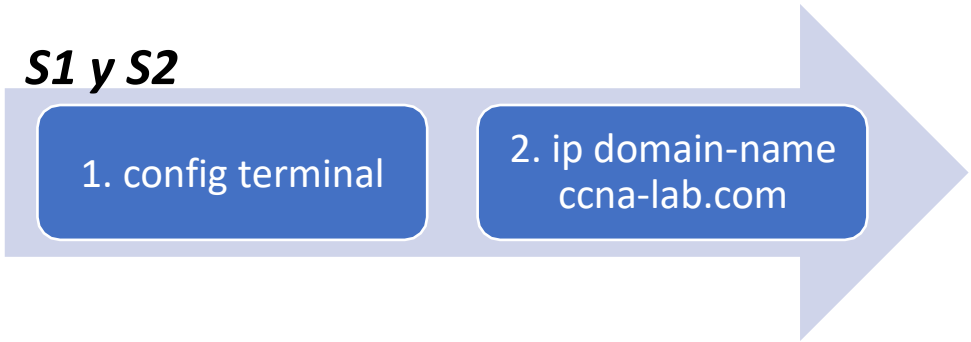
2. Hostname S1 o S2: Desde el modo de configuración, se digita el comando en el Router y/o Switch, cambiando el nombre del dispositivo.

SINTAXIS:

Switch1#config t
Switch1(config)# Hostname S1
S1(config)#

Switch2#config t
Switch2(config)# Hostname S2
S2(config)#

c. Nombre del Dominio:

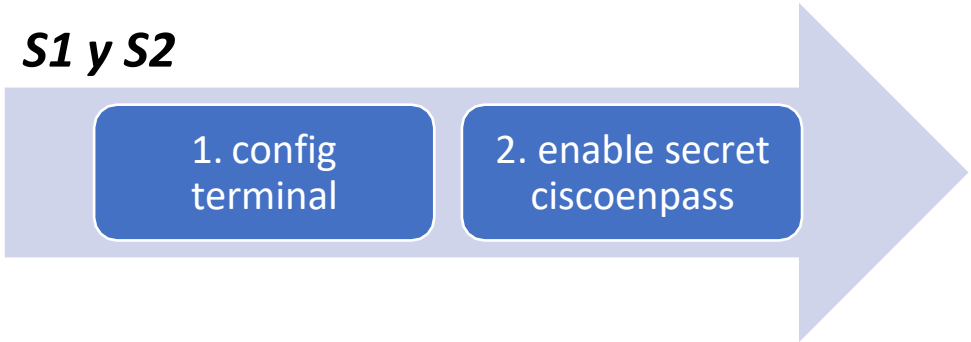


2. ip domain-name “Nombre del Dominio”, Comando para asignar nombre al Dominio del Router.
SINTAXIS:

S1#config ter
S1(config)#ip domain-name ccna-lab.com

S2#config ter
S2(config)#ip domain-name ccna-lab.com

d. Contraseña cifrada para el modo EXEC privilegiado (Ciscoenpass)



2. Enable secret “contraseña”: Se utiliza para restringir el acceso al modo EXEC privilegiado, adicional, que brinda un nivel de cifrado.

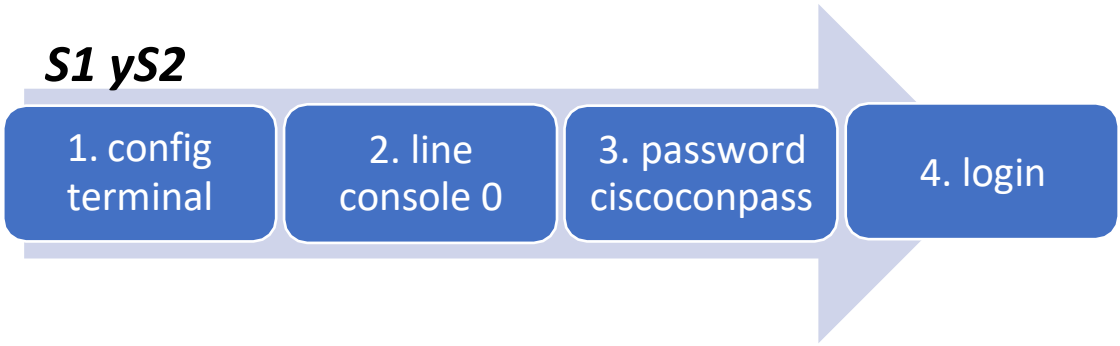
SINTAXIS:

S1>enable

S1#config terminal
S1(config)#enable secret ciscoenpass

S2>enable
S2#config terminal
S2(config)#enable secret ciscoenpass

e. Contraseña de acceso a la consola (Ciscoconpass)



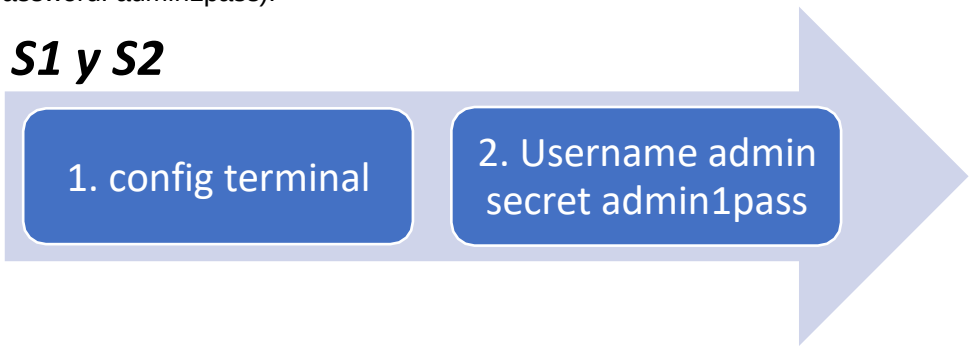
2. line console 0: se usa para ingresa al modo de configuración de la línea de consola, el cero representa la interfaz de consola.
3. password (contraseña): Se usa para especificar la contraseña para la línea de consola.
4. login: configura el Router para que requiera la autenticación al iniciar la sesión.

SINTAXIS:

S1#config t
S1(config) #line con 0
S1(config-line) #password ciscoconpass
S1(config-line) #login

S2#config t
S2(config) #line con 0
S2(config-line) #password ciscoconpass
S2(config-line) #login

f. Crear un usuario administrativo en la base de datos local (Nombre de usuario: admin Password: admin1pass).

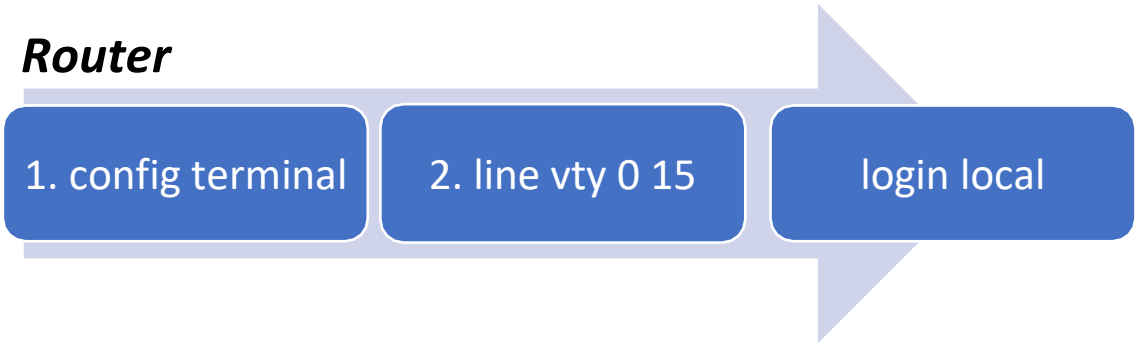


2. Username admin secret admin1pass: Se utiliza para crear un usuario en la base de datos local, donde en Username se especifica el Nombre_Usuario y secret (Contraseña_cifrada).

SINTAXIS:

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

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



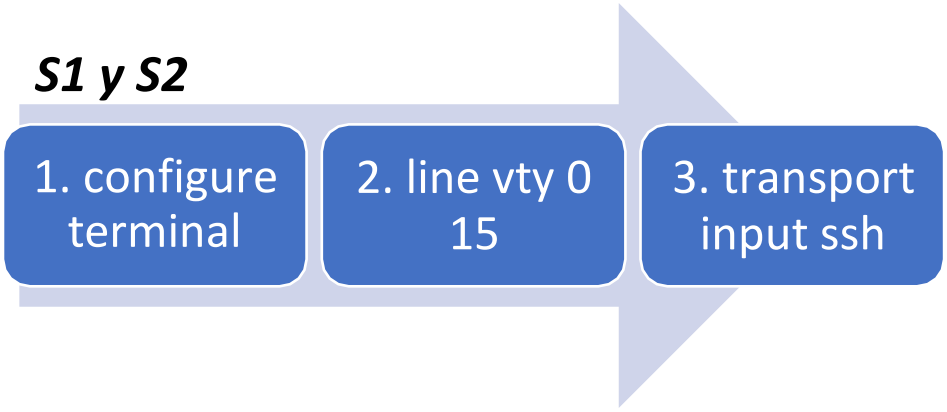
2. Los puertos VTY están enumerados del 0 a 15 y son utilizados para establecer sesiones Telnet, por ende, se ingresa a la configuración y se configura el usuario local (admin).

SINTAXIS:

S1#config t
S1(config)# line vty 0 15
S1(config)# login local

S2#config t
S2(config)# line vty 0 15
S2(config)# login local

h. Configurar las líneas VTY para que acepten únicamente las conexiones SSH



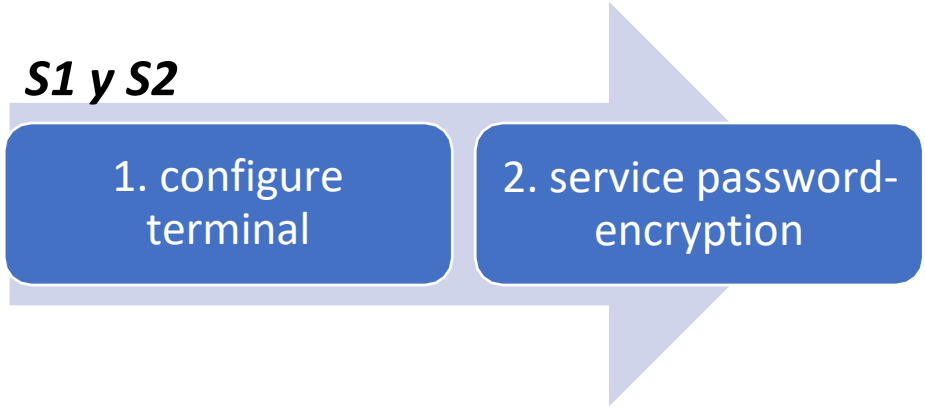
2. Volvemos a la configuración VTY o si no nos salimos seguimos en está.
3. transport input ssh: Se utiliza para acceder solo por SSH.

SINTAXIS:

S1#configure terminal
S1(config)#line vty 0 15
S1(config-line) #transport input ssh

S2#configure terminal
S2(config)#line vty 0 15
S2(config-line) #transport input ssh

i. Cifrar las contraseñas de texto no cifrado



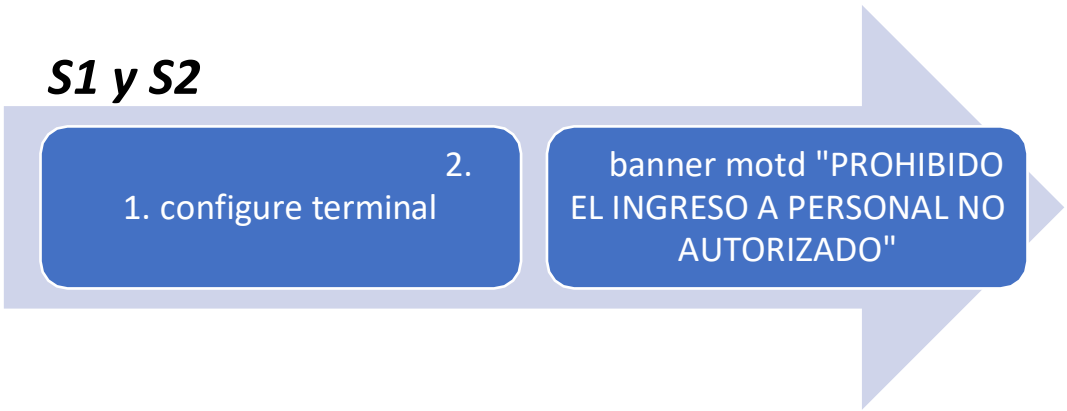
2. Service password-encryption: Se encarga de aplicar un cifrado a todas las contraseñas que se encuentren sin cifrar.

SINTAXIS:

S1#configure terminal
S1(config)#service password-encryption

S2#configure terminal
S2(config)#service password-encryption

j. Configurar un MOTD Banner



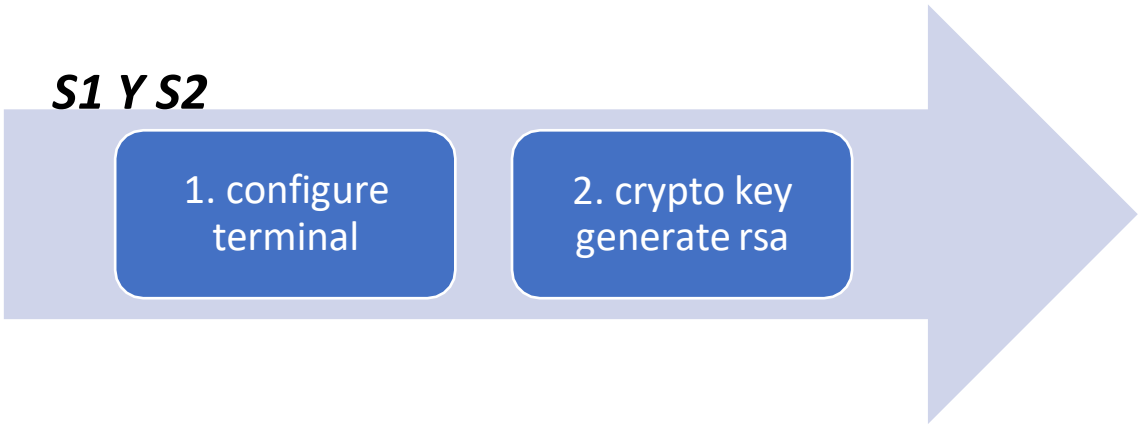
2. banner motd “Mensaje”: Es un Mensaje de aviso al ingreso del dispositivo configurado.

SINTAXIS:

S1#configure terminal
S1(config)#banner motd "PROHIBIDO EL INGRESO DE PERSONAL NO AUTORIZADO"

S2#configure terminal
S2(config)#banner motd "PROHIBIDO EL INGRESO DE PERSONAL NO AUTORIZADO"

k. Generar una clave de cifrado RSA



2.crypto key generate rsa, este comando da el tamaño al cifrado de las llaves en este caso de 1024 bits de longitud.

SINTAXIS.

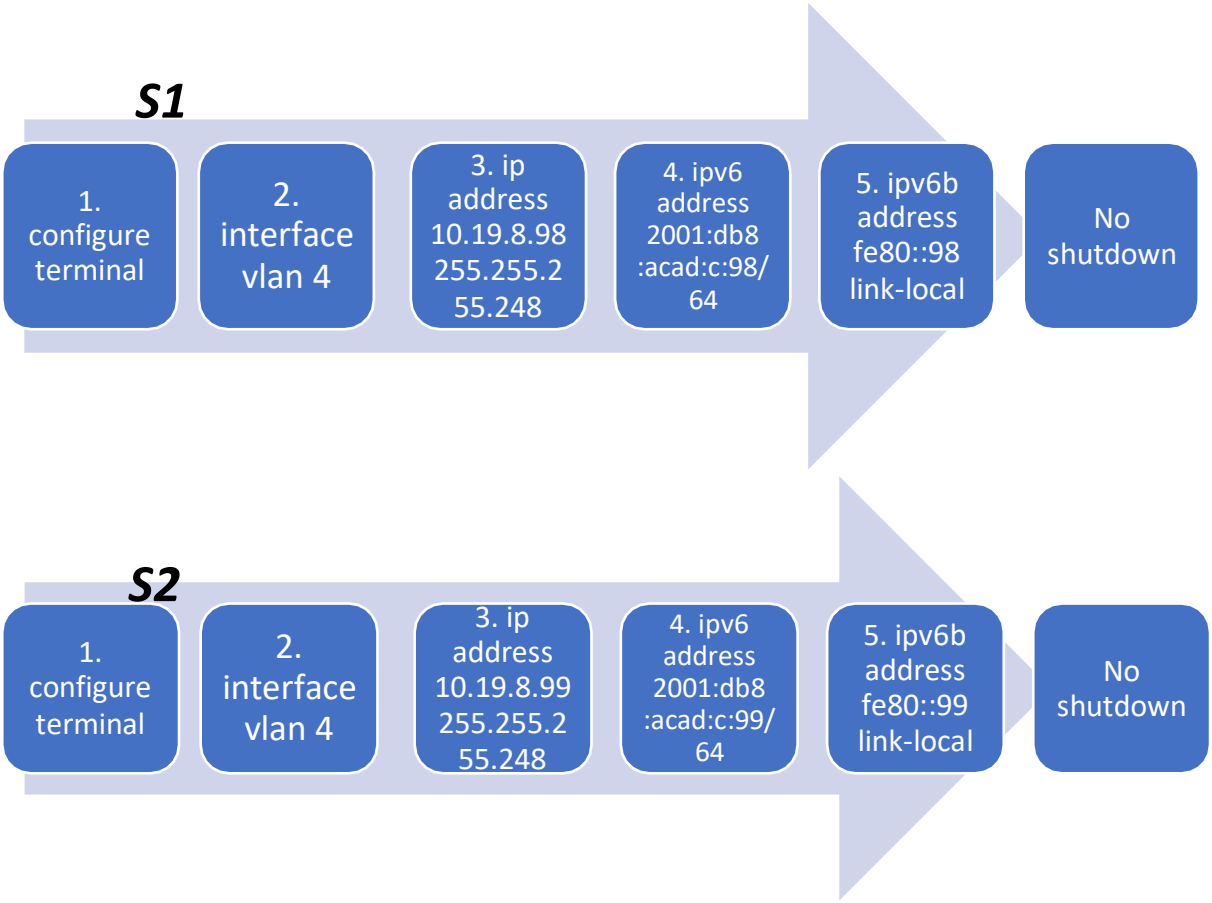
S1(config)#crypto key generate rsa
The name for the keys will be: R1.ccna-lab.com
Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes.
How many bits in the modulus [512]: 1024

% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

S2(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]

l. 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.



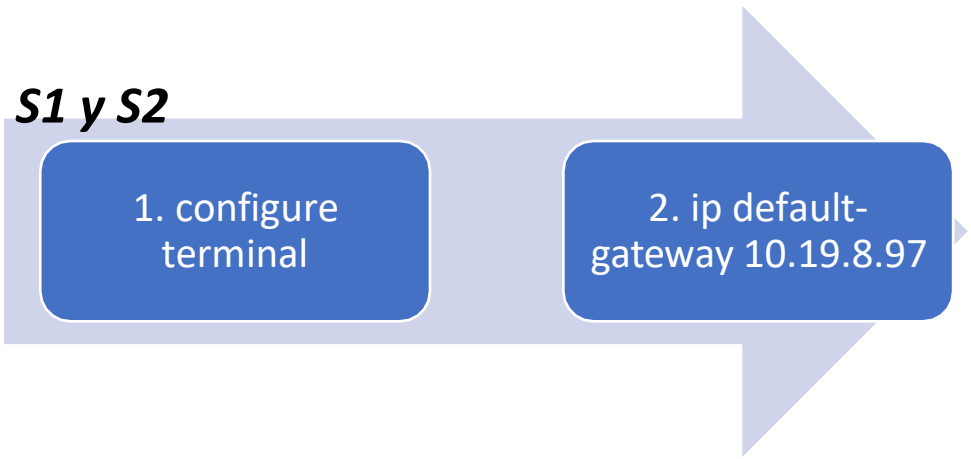
2. Se ingresa al modo configuración de la interfaz Vlan 4 que será la de administración.
3. Se configura el direccionamiento IPV4- Capa 3 según la asignación en la tabla.
4. Se configura el direccionamiento IPV6 – Capa 3 según la asignación en la tabla .
5. Se configura el enlace local.
6. No Shutdown, enciende la interfaz.

SINTAXIS.

```
S1(config)#inter 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)#no Shutdown

S2(config)#inter 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::99 link-local
S2(config-if) #no Shutdown
```

m. Configuración del gateway predeterminado



Nota: Para IPV6 se deja dinámica, sin embargo, para los ping se recomienda poner una ipv6 gateway.

2. ip default-gateway 10.19.8.97: Es la ruta predeterminada o ruta por defecto que se le asigna al dispositivo.

SINTAXIS

S1(config)# ip default-gateway 10.19.8.97

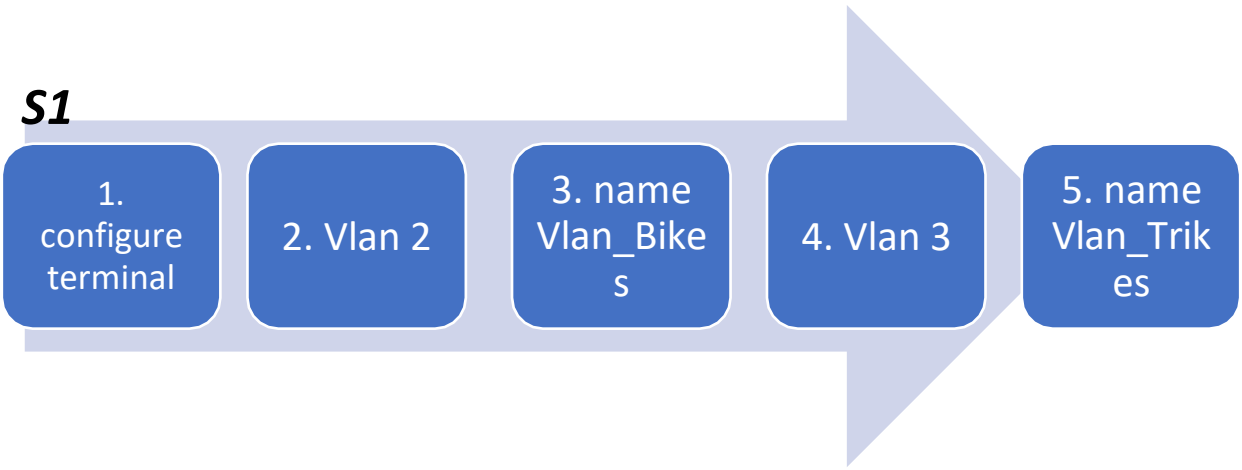
S2(config)# ip default-gateway 10.19.8.97

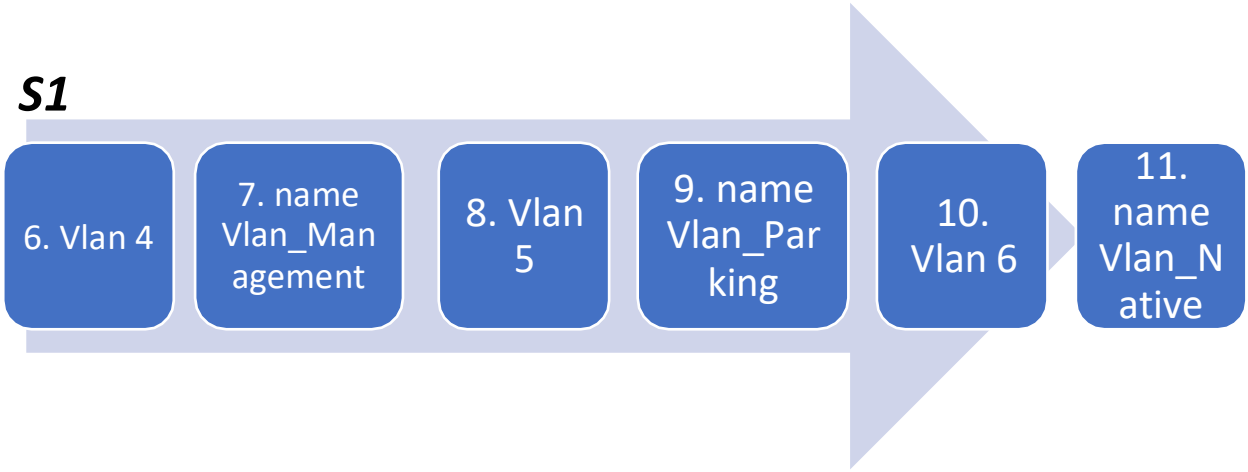
Parte 2: Configuración de la infraestructura de Red (Vlan, Trunking, EtherChannel).

Paso 1. Configuración S1.

En este paso configuramos el Switch 1 según las instrucciones dadas por el tutor, para seguir formando exitosamente el Escenario No.1

a. Crear VLAN



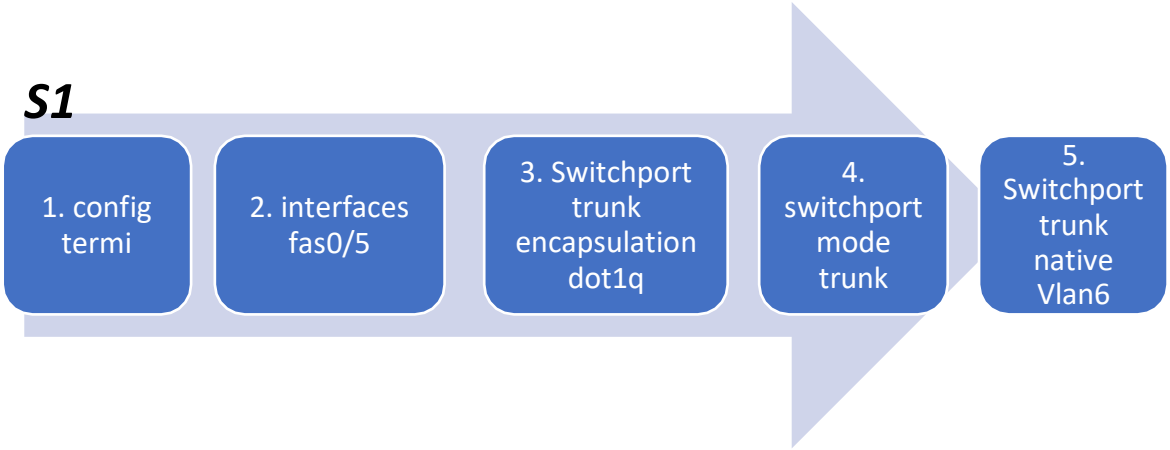


Se realiza la creación de las Vlans y los nombres correspondientes.

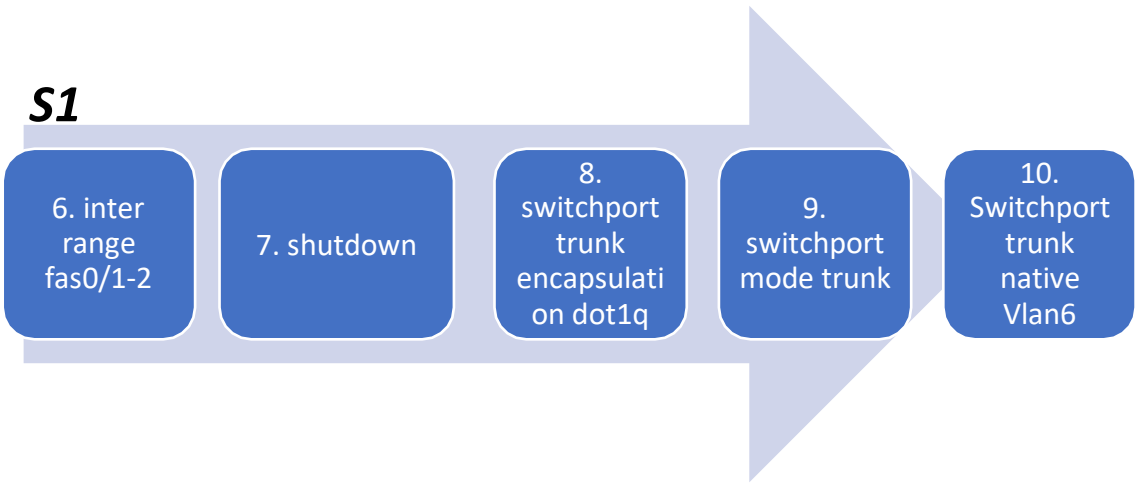
SINTAXIS:

```
S1(config)#vlan 2
S1(config-vlan)#name Vlan_Bikes
S1(config-vlan)#vlan 3
S1(config-vlan)#name Vlan_Trikes
S1(config-vlan)#vlan 4
S1(config-vlan)#name Vlan_management
S1(config-vlan)#vlan 5
S1(config-vlan)#name Vlan_Parking
S1(config-vlan)#vlan 6
S1(config-vlan)#name Vlan_Native
```

b. Crear troncos 802.1Q que utilicen la Vlan 6 nativa (Interfaces F0/1, F0/2 y F0/5).



2. Se ingresa a la interfaz 0/5 ya que es una de las que utilizaran la Vlan 6 Native
3. Permite un enlace troncal bajo el método de encapsulamiento.
4. Se menciona la creación del enlace troncal, para las Vlans y todos los Switch.
5. Switchport trunk native Vlan6.

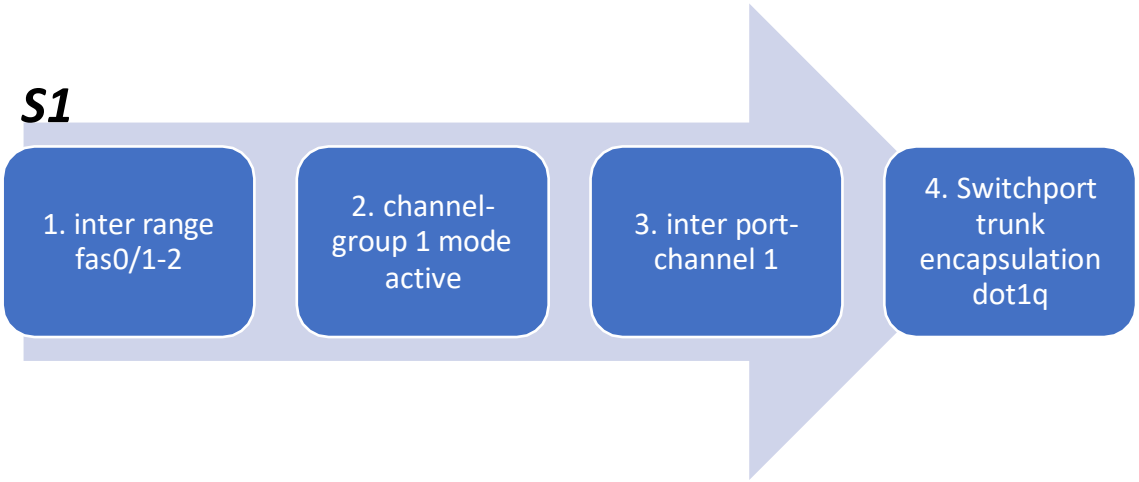


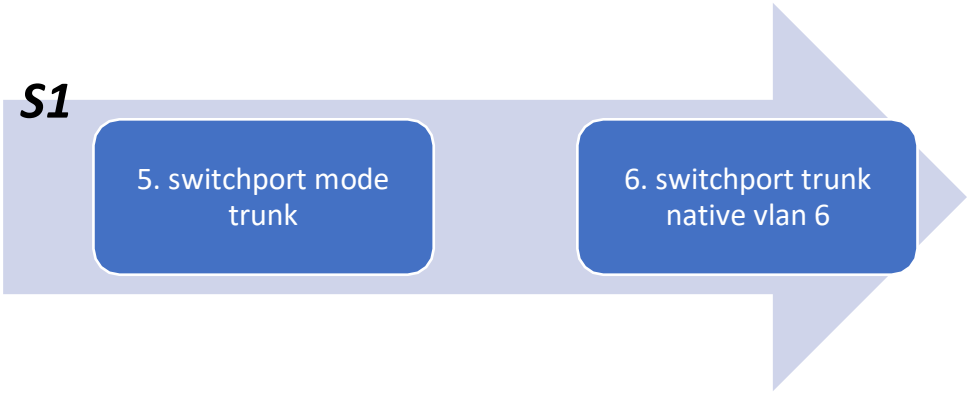
6. Utilizo un rango para abarcar el fa 0/1 y 0/2, dando la misma configuración
7.Se apaga las interfaces debido a que después configuramos el etherchannel.
8. Permite un enlace troncal bajo el método de encapsulamiento.
9. Se menciona la creación del enlace troncal, para las Vlans y todos los Switch.
10. Switchport trunk native Vlan6.

SINTAXIS:

S1(config)#inter fastEthernet 0/5
S1(config-if) #switchport trunk encapsulation dot1q
S1(config-if) #switchport mode trunk
S1(config-if) #switchport trunk native vlan 6
S1(config)#exit
S1(config)#int range fast 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

c. Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2 (Usar el protocolo LACP para la negociación).





2. channel-group 1 mode active: construimos un canal de puerto LACP dinámico, el cual agrupa múltiples enlaces físico para formar un enlace lógico aumentando un ancho de banda de los enlaces.
3. inter port-channel 1, ingresamos a la interfaz para configurarla.
4. Comenzamos a utilizar los mismos comandos conocidos para configurar las troncales.
5. Configuramos el puerto de modo troncal.
6. Se coloca de modo troncal la Vlan 6 Native

SINTAXIS:

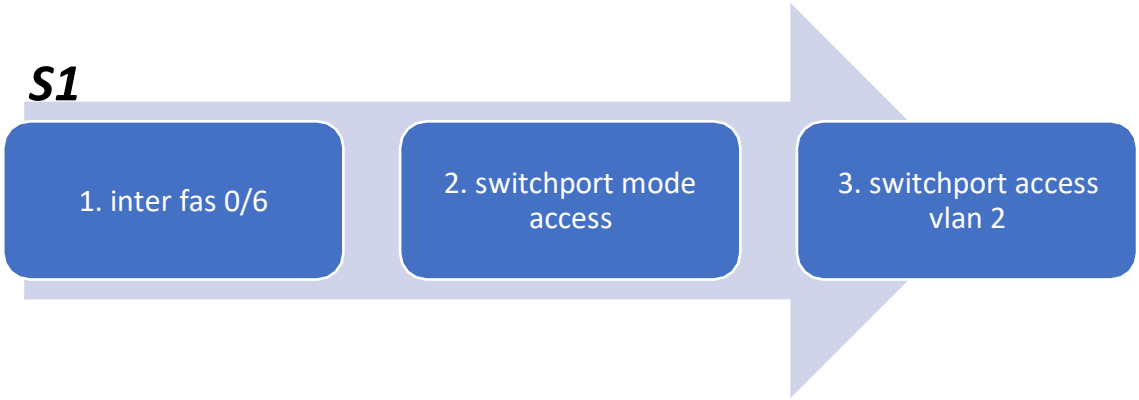
S1(config)#int range fast 0/1-2
S1(config-if-range) #channel-group 1 mode active
S1(config-if-range) #
Creating a port-channel interface Port-channel 1

%EC-5-CANNOT_BUNDLE2: Fa0/1 is not compatible with Po1 and will be suspended (native vlan of Fa0/1 is 6, Po1 id 1)

%EC-5-CANNOT_BUNDLE2: Fa0/2 is not compatible with Po1 and will be suspended (native vlan of Fa0/2 is 6, Po1 id 1)

S1(config-if-range) #inter port-channel 1
S1(config-if) #switchport trunk encapsulation dot1q
S1(config-if) #switchport mode trunk
S1(config-if) #switchport trunk native vlan 6

d. Configurar el puerto de acceso de host para VLAN 2 (interface F0/6)



1. Se ingresa a la interfaz a configurar.
2. Switchport mode Access, la interfaz cambia al modo de acceso permanente.
3. Switchport Access vlan_id, se configura únicamente con una Vlan asignada de forma estática.

SINTAXIS:

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

e. Configurar la seguridad del puerto en los puertos de acceso (Permitir 3 direcciones MAC).

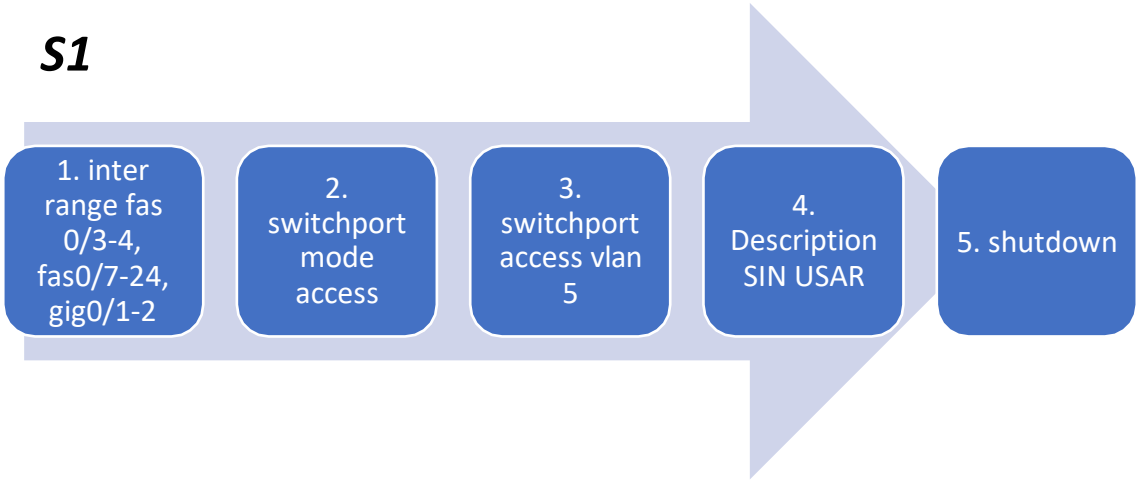
1. En la misma interfaz vamos a configurar un máximo de 3 direcciones MAC permitidas.
2. Switchport port-security, Habilita la seguridad en el puerto con la configuración.
3. Switchport port-security máximum No., nos permite retener o definir una cantidad de direcciones MAC permitidas en la interfaz.

SINTAXIS:

```
S1(config)#Inter Fa0/6
S1(config-if) #switchport port-security
S1(config-if) #switchport port-security maximum 3
```

f. Proteja todas las interfaces no utilizadas (Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar)

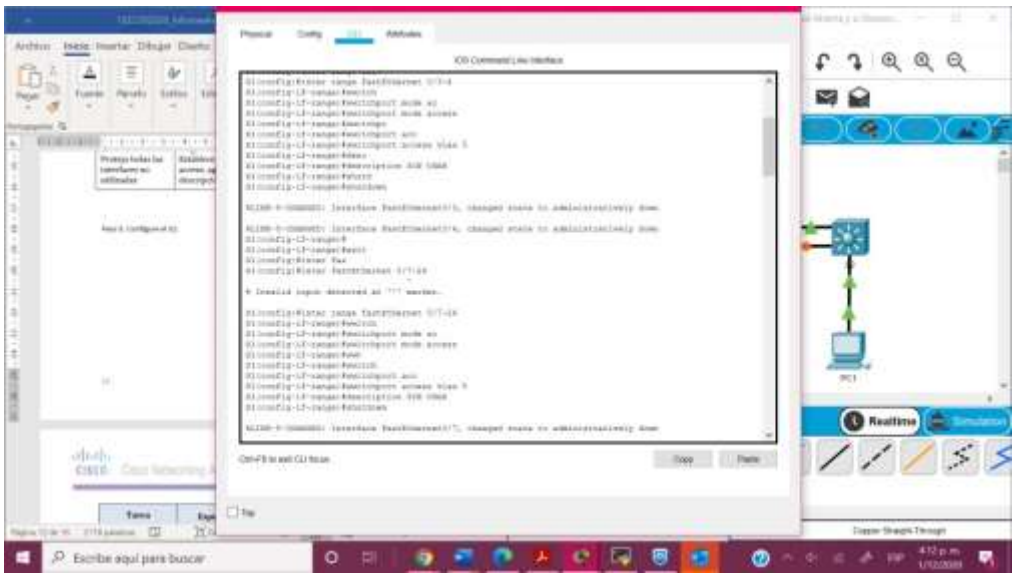
1.



1. Se escoge el rango de interfaces a configurar.
2. Switchport mode Access, la interfaz cambia al modo de acceso permanente.
3. Switchport Access vlan_id, se configura únicamente con una Vlan asignada de forma estática.
4. Se le asigna una Description, en este caso son los puertos que están sin funcionamiento o sin USAR según la topología del caso.
5. Para proteger de que no puedan conectarse y tener acceso, apagamos los puertos.

SINTAXIS:

S1(config)#interface range fastEthernet 0/3-4, fastEthernet 0/7-24, gigabitEthernet 0/1-2
S1(config-if-range) #switchport mode access
S1(config-if-range) #switchport access vlan 5
S1(config-if-range) #description SIN USAR
S1(config-if-range) #shutdown

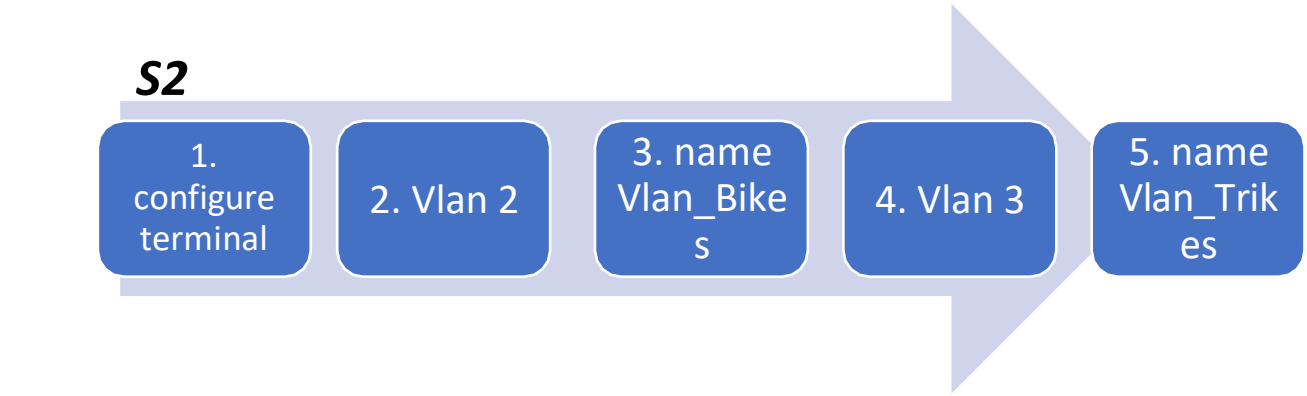


Paso 2. Configure el S2.

En este paso configuramos el Switch 2 según las instrucciones dadas por el tutor, para seguir formando exitosamente el Escenario No.1

a. Crear Vlan (VLAN 2, name Bikes, VLAN 3, name Trikes, VLAN 4, name Management, VLAN 5, name Parking, VLAN 6, name Native).

   NOTA: Al configurar las credenciales en pasos anteriores, le va a pedir las contraseñas mencionadas.

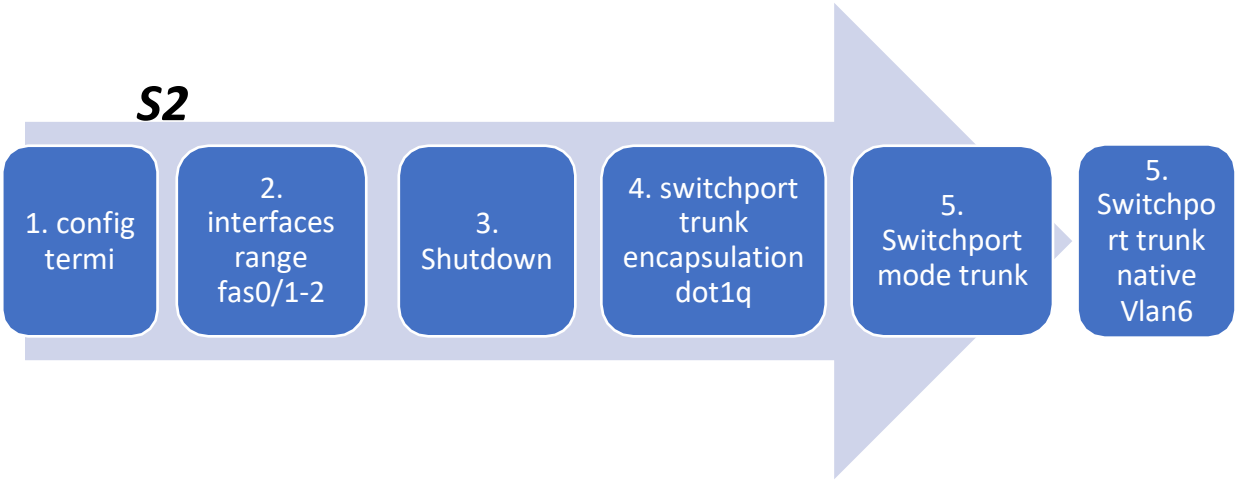


Se realiza la creación de las Vlans y los nombres correspondientes.

SINTAXIS:

```
S2(config)#vlan 2
S2(config-vlan) #name Vlan_Bikes
S2(config-vlan) #vlan 3
S2(config-vlan) #name Vlan_Trikes
S2(config-vlan) #vlan 4
S2(config-vlan) #name Vlan_management
S2(config-vlan) #vlan 5
S2(config-vlan) #name Vlan_Parking
S2(config-vlan) #vlan 6
S2(config-vlan) #name Vlan_Native
```

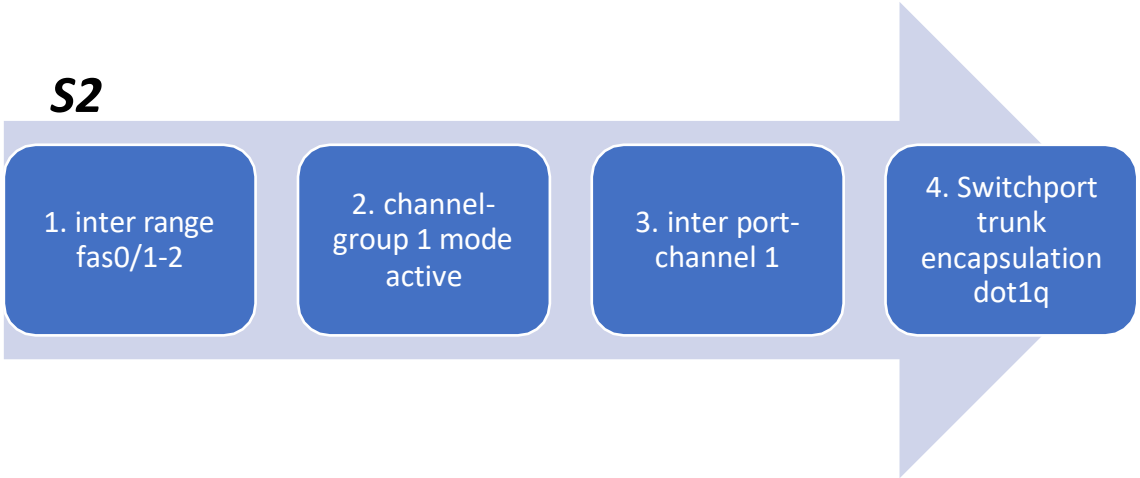
b. Crear troncos 802.1Q que utilicen la VLAN 6 nativa (Interfaces F0/1 y F0/2)

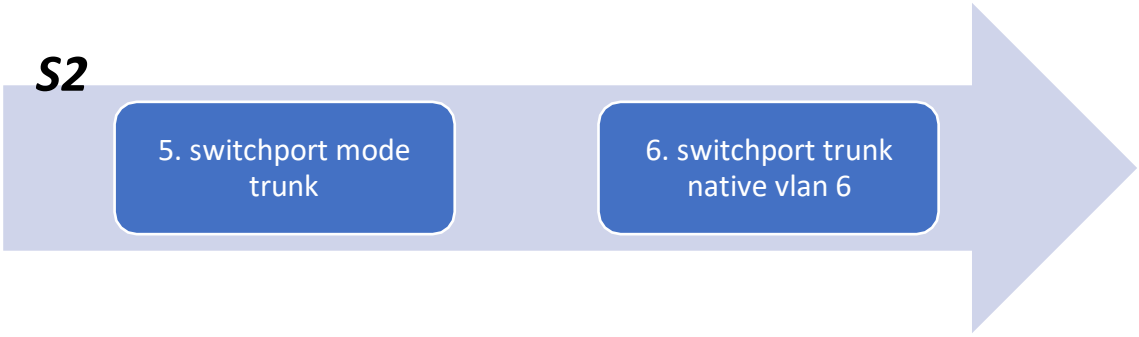


2. Se ingresa al rango de interfaz 0/1-2 ya que es una de las que utilizaran la Vlan 6 Native
3. Apagamos puertos pensando en el siguiente paso de configuración de etherchannel.
4. Permite un enlace troncal bajo el método de encapsulamiento (Esto en caso de algunos Switch otros ya cuentan con esta función y no es necesario especificar el comando).
5. Se menciona la creación del enlace troncal, para las Vlans y todos los Switch.
6. Switchport trunk native Vlan6.
SINTAXIS:

S2(config)#inter range fast 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

c. Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2 (Usar el protocolo LACP para la negociación).



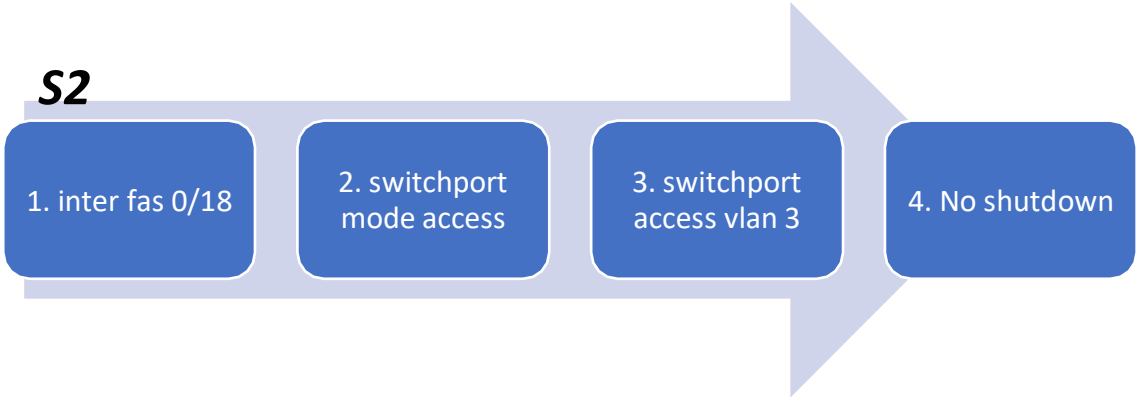


2. channel-group 1 mode active: construimos un canal de puerto LACP dinámico, el cual agrupa múltiples enlaces físico para formar un enlace lógico aumentando un ancho de banda de los enlaces.
3. inter port-channel 1, ingresamos a la interfaz para configurarla.
4. Comenzamos a utilizar los mismos comandos conocidos para configurar las troncales.
5. Configuramos el puerto de modo troncal.
6. Se coloca de modo troncal la Vlan 6 Native

SINTAXIS:

```
S2(config-if-range) #inter range fast 0/1-2
S2(config-if-range) #channel-group 1 mode active
S2(config-if-range) #inter port-channel 1
S2(config-if)#switchport trunk encapsulation dot1q
S2(config-if) #switchport mode trunk
S2(config-if) #switchport trunk native vlan 6
```

d. Configurar el puerto de acceso del host para la VLAN 3(interfaz F0/18).



1. Se ingresa a la interfaz a configurar.
2. Switchport mode Access, la interfaz cambia al modo de acceso permanente.
3. Switchport Access vlan_id, se configura únicamente con una Vlan asignada de forma estática.

SINTAXIS:

```
S2(config)#inter fast 0/18
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 3
S2(config-if)#no shutdown
```

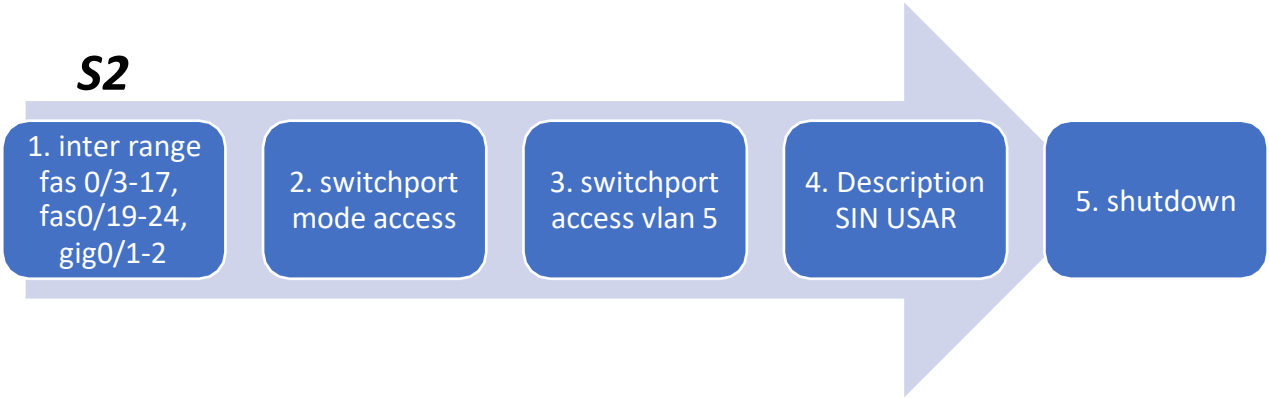
e. Configure port-security en los access ports (Permite 3 MAC addresses).

1. En la misma interfaz vamos a configurar un máximo de 3 direcciones MAC permitidas.
2. Switchport port-security, Habilita la seguridad en el puerto con la configuración.
3. Switchport port-security máximum No., nos permite retener o definir una cantidad de direcciones MAC permitidas en la interfaz.

SINTAXIS:

S2(config)#Inter Fa0/18
S2(config-if) #switchport port-security
S2(config-if) #switchport port-security maximum 3

f. Asegure todas las interfaces no utilizadas (Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar).



1. Se escoge el rango de interfaces a configurar.
2. Switchport mode Access, la interfaz cambia al modo de acceso permanente.
3. Switchport Access vlan_id, se configura únicamente con una Vlan asignada de forma estática.
4. Se le asigna una Description, en este caso son los puertos que están sin funcionamiento o sin USAR según la topología del caso.
5. Para proteger de que no puedan conectarse y tener acceso, apagamos los puertos.

SINTAXIS:

S2(config)# interface range fastEthernet 0/3-17, fastEthernet 0/19-24, gigabitEthernet 0/1-2

S2(config-if-range) #switchport mode access
S2(config-if-range) #switchport access vlan 5
S2(config-if-range) #description SIN USAR
S2(config-if-range) #shutdown

NOTA: ANTES DE PASAR A LA SIGUIENTE PARTE SE DEBEN ACTIVAR LAS INTERFACES LACP, EN AMBOS SWITCH.

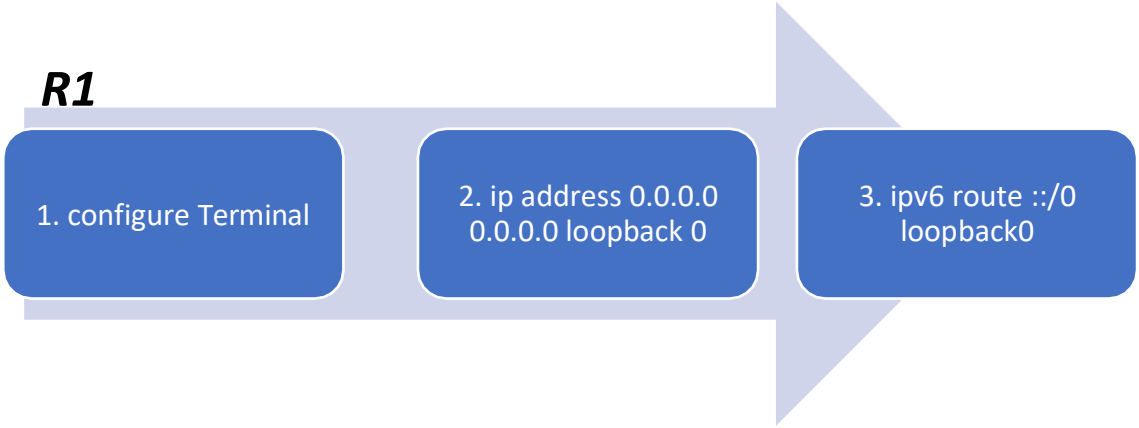
Parte 3. Configurar soporte host.

Paso 1: Configuración R1.

El siguiente paso se da para configurar el Router a nivel de enrutamiento.

a. Configure Default Routing (Crear rutas predeterminadas para IPv4 e IPv6 que dirijan el tráfico a la interfaz Loopback 0).

Se ingresa al Router con Credenciales especificadas y configuradas.



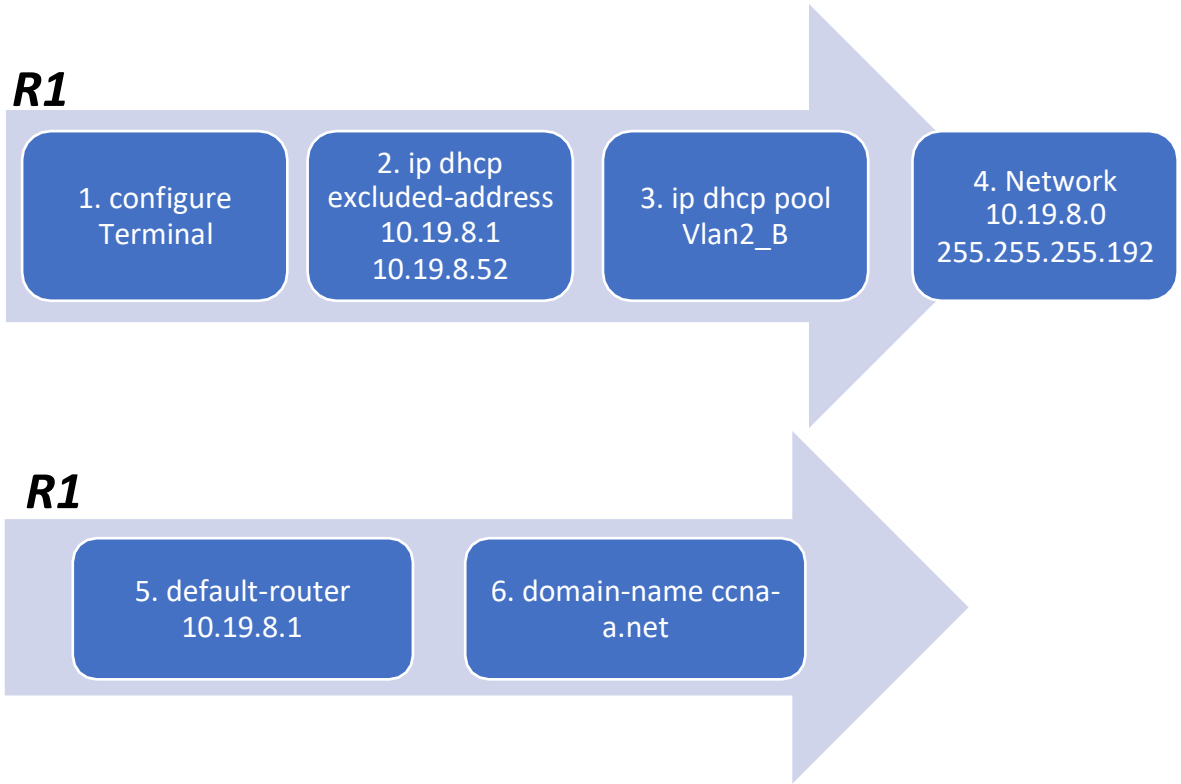
2. Se configura la ruta por defecto en direccionamiento IPV4 en la interfaz Loopback 0 que simula la salida hacia internet.
3. Se configura la ruta por defecto en direccionamiento IPV6 en la interfaz Loopback 0 que simula la salida hacia internet.

SINTAXIS:
R1#config t
R1(config)#ip route 0.0.0.0 0.0.0.0 loopback 0

R1(config)#ipv6 route ::/0 loopback 0

b. 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)

VLAN	Network	Excluidos DHCP	Utilizable
Vlan 2 Bikes	10.19.8.0/26	10.19.8.1-10.19.8.52	10.19.8.53- 10.19.8.62
Vlan 3 Trikes	10.19.8.64/27	10.19.8.65-10.19.8.84	10.19.8.85- 10.19.8.94



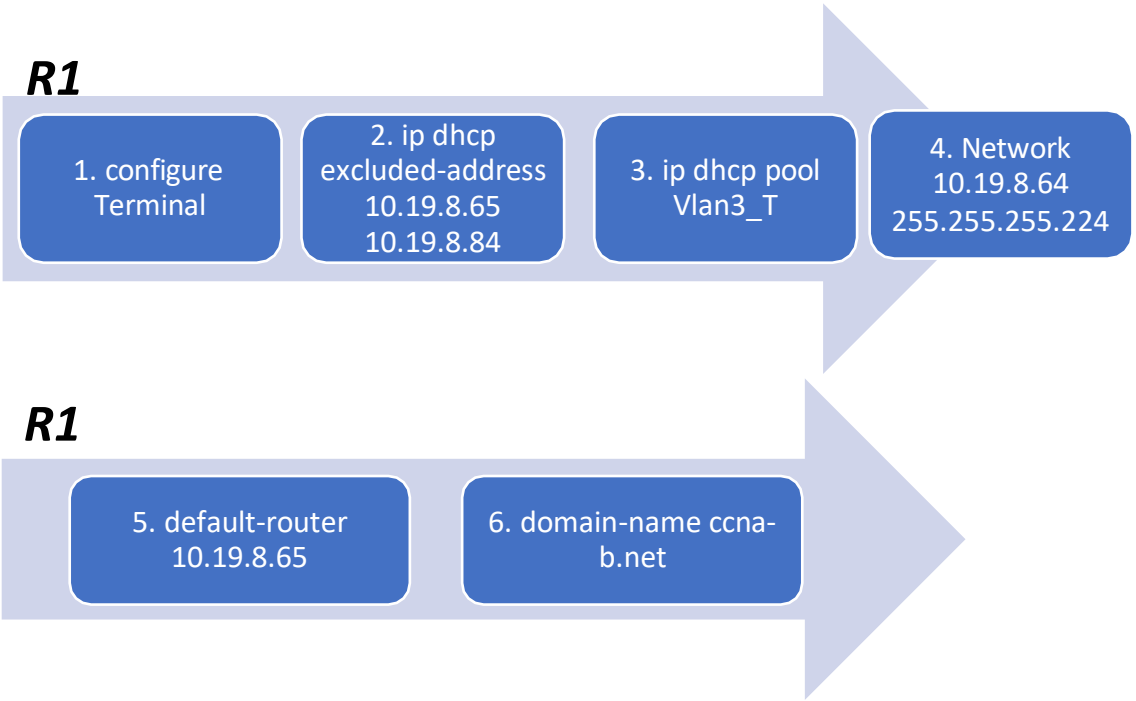
2. ip dhcp excluded-address (Rango de direccionamiento), se utiliza para excluir direcciones especificas o un rango de ellas, es decir, al momento de asignar direccionamiento dinámico a los equipos este rango de direccionamiento no será entregado por el dhcp al equipo.
3. Ip dhcp pool Vlan2_B, se crea el dhcp y configura.
4. Se describe la red para el DHCP.
5. Se configura la Ruta por defecto.
6. Se configura el Dominio ccna-a.net

SINTAXIS:

R1(config)#ip dhcp excluded-address 10.19.8.1 10.19.8.52
R1(config)#ip dhcp pool Vlan2_B
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

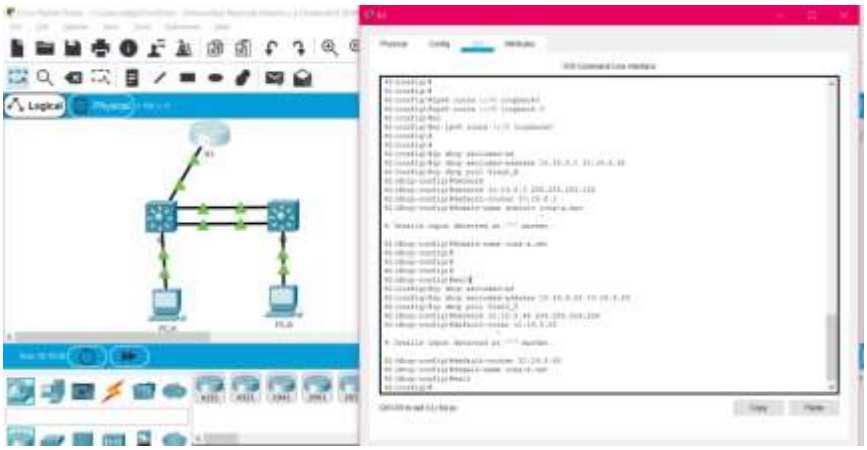
c. Configurar DHCP IPv4 para VLAN 3 (Cree un grupo DHCP para VLAN 3, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio ccna-b.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del Router para la subred involucrada).



2. ip dhcp excluded-address (Rango de direccionamiento), se utiliza para excluir direcciones especificas o un rango de ellas, es decir, al momento de asignar direccionamiento dinámico a los equipos este rango de direccionamiento no será entregado por el dhcp al equipo.
3. Ip dhcp pool Vlan3_T, se crea el dhcp y configura.
4. Se describe la red para el DHCP.
5. Se configura la Ruta por defecto.
6. Se configura el Dominio ccna-b.net

SINTAXIS:

R1(config)#ip dhcp excluded-address 10.19.8.65 10.19.8.84
R1(config)#ip dhcp pool Vlan3_T
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

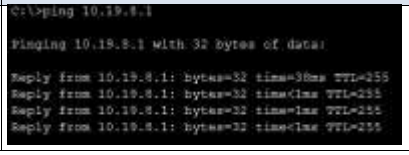


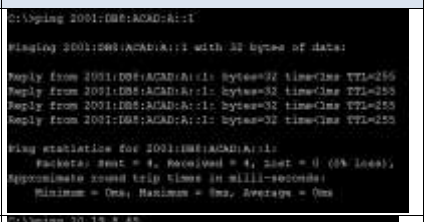
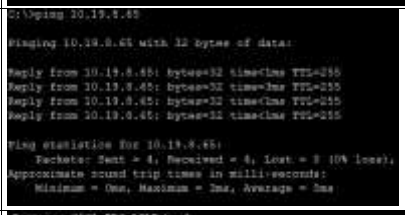
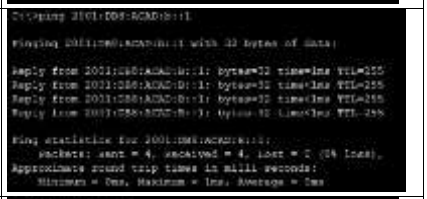
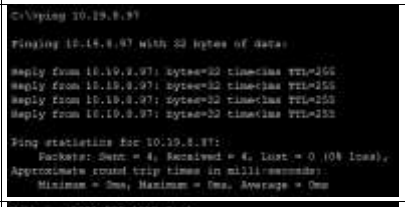
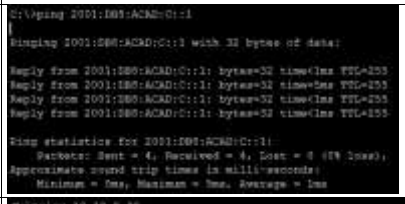
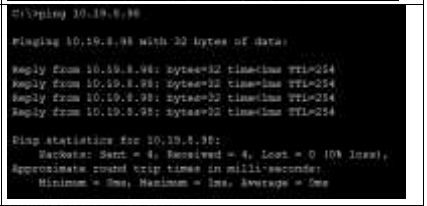
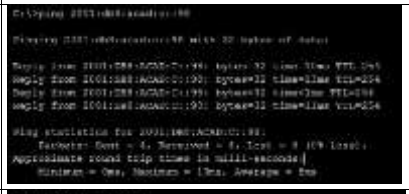
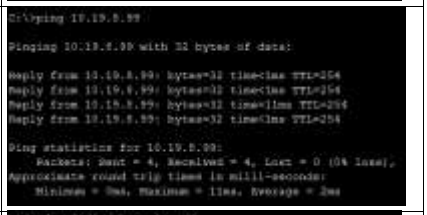
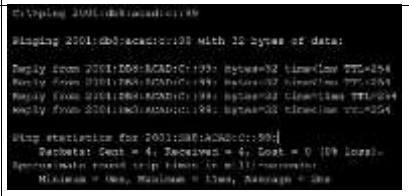
Paso2. Configurar los Servidores

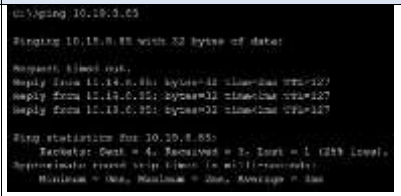
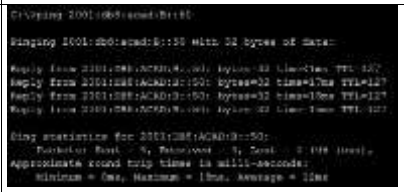
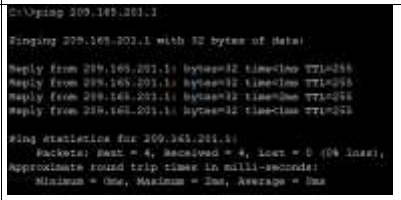
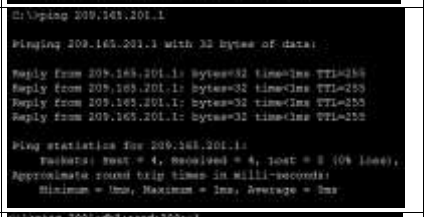
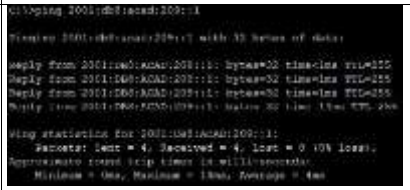
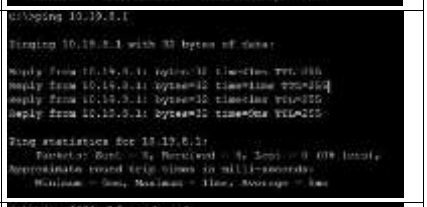
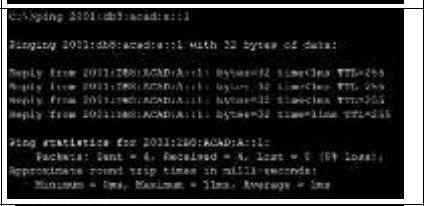
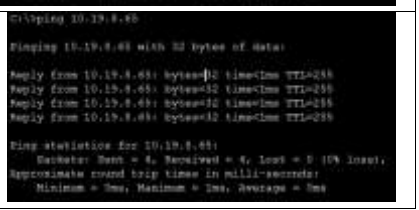
PC-A Network Configuration	
Descripción	*Direccionamiento Equipo A*
Dirección física	*0004.9AAA.1997*
Dirección IP	*10.19.8.53*
Máscara de subred	*255.255.255.192*
Gateway predeterminado	*10.19.8.1*
Gateway predeterminado IPv6	*FE80::1*

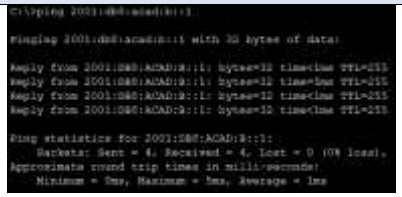
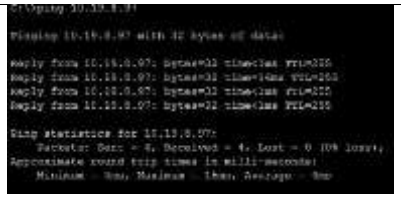
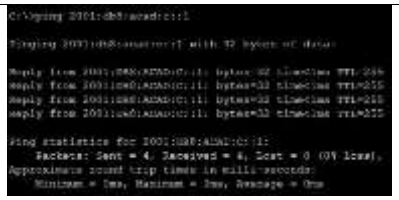
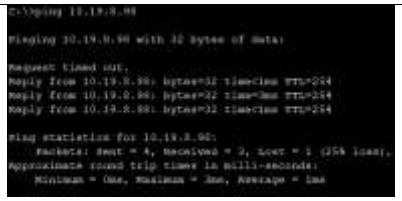
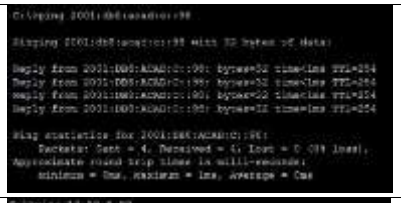
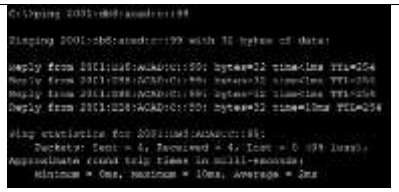
PC-B Network Configuration	
Descripción	*Direccionamiento Equipo B*
Dirección física	*0001.C9AD.23AD*
Dirección IP	*10.19.8.85*
Máscara de subred	*255.255.255.224*
Gateway predeterminado	*10.19.8.65*
Gateway predeterminado IPv6	*FE80::1*

Parte 4: Probar y verificar la conectividad de extremo a extremo

Desde	**Dirección IP**	**Resultados de ping**
PC-A	10.19.8.1	

Desde	Dirección IP	Resultados de ping
	2001:db8:acad:a: :1	
	10.19.8.65	
	2001:db8:acad:b: :1	
	10.19.8.97	
	2001:db8:acad:c: :1	
	10.19.8.98	
	2001:db8:acad:c: :98	
	10.19.8.99.	
	2001:db8:acad:c: :99	

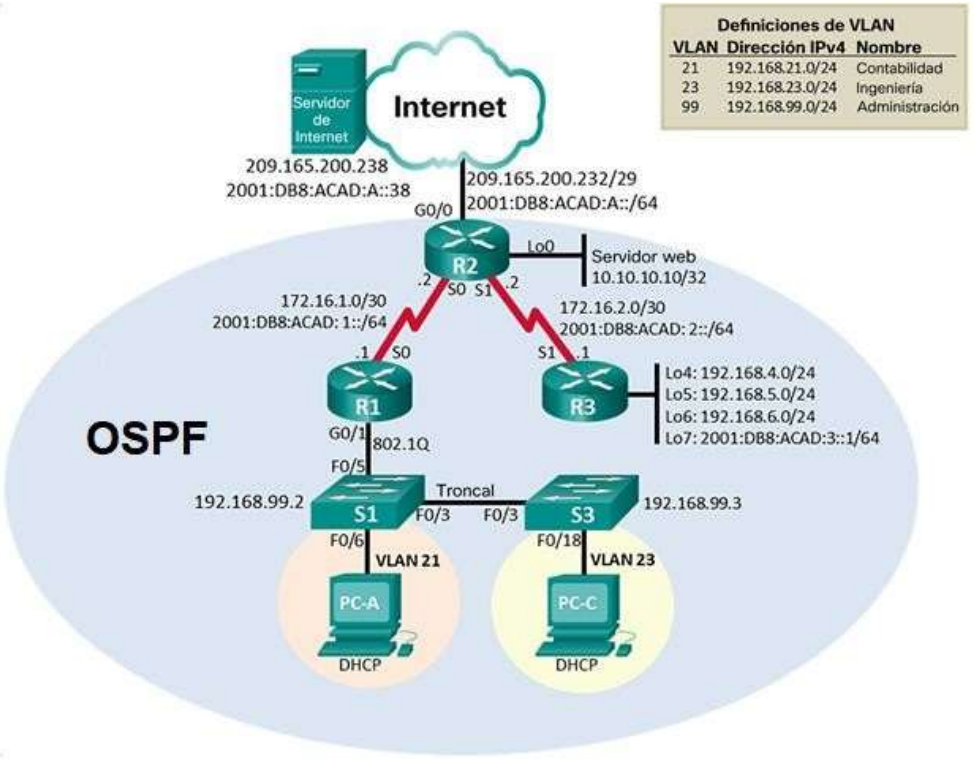
Desde	Dirección IP	Resultados de ping
	IP address will vary.	
	2001:db8:acad:b: :50	
	209.165.201.1	
	2001:db8:acad:209: :1	
PC-B	209.165.201.1	
	2001:db8:acad:209: :1	
	10.19.8.1	
	2001:db8:acad:a: :1	
	10.19.8.65	

Desde	Dirección IP	Resultados de ping
	2001:db8:acad:b: :1	
	10.19.8.97	
	2001:db8:acad:c: :1	
	10.19.8.98	
	2001:db8:acad:c: :98	
	10.19.8.99.	
	2001:db8:acad:c: :99	

gg

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.



Parte 1: Inicializar dispositivos.

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

a. Eliminar el archivo startup-config de todos los routers y volver a cargar todos los Routers.

1. Ingreso al modo privilegiado.

2. Se elimina el Startup-config, situado en la NRAM, la cual es una copia de seguridad de la configuración del router.
3. Reload, función de reinicio del dispositivo, ayudando a ejecutar los cambios.

   Sintaxis:

   Router>enable
   Router#erase startup-config
   (confirm)
   Router#reload
   (confirm)

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

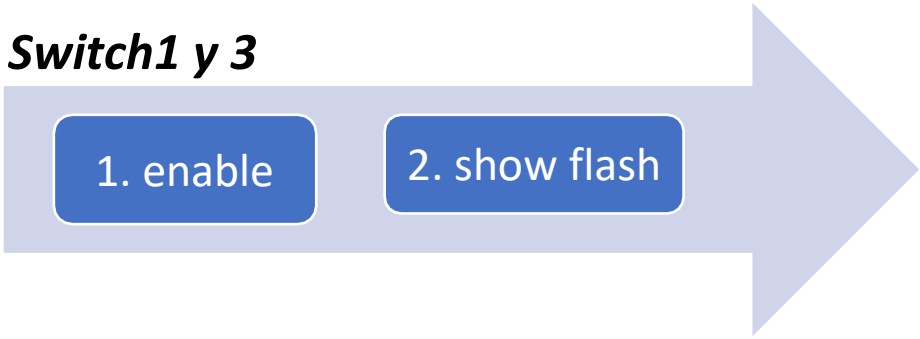
1. Ingreso al modo privilegiado.
2. Se elimina el Startup-config, situado en la NRAM, la cual es una copia de seguridad de la configuración del router.
3. Delete vlan.dat, borra la información de Vlan , en la memoria flash que contiene dicha información.
4. Reload, función de reinicio del dispositivo, ayudando a ejecutar los cambios.

   Sintaxis:

   Switch> enable
   Switch# erase startup-config
   (confirmar)
   Switch#delete vlan.dat
   Switch#Reload
   (confirmar)

c. Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches.

Switch1 y 3



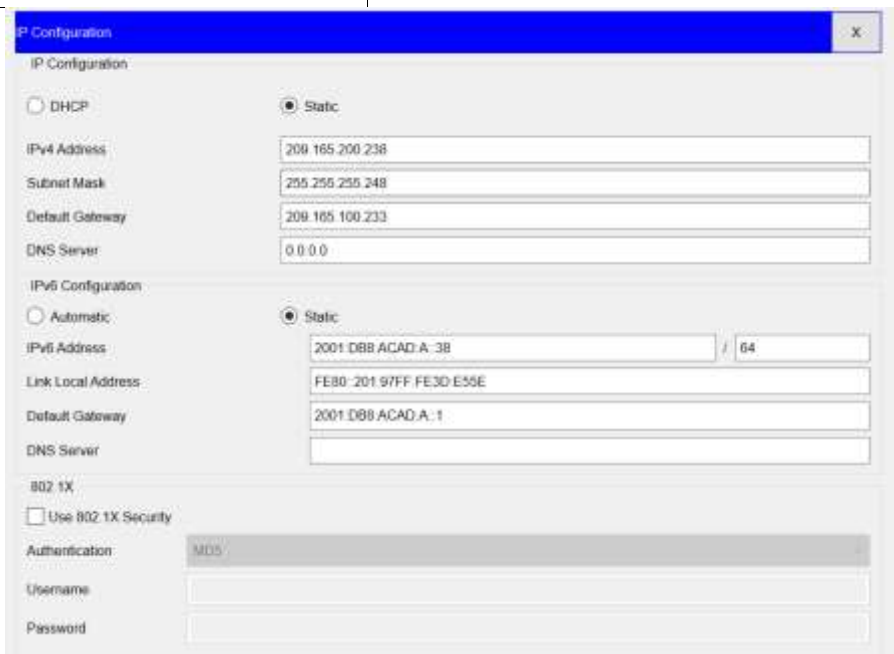
2. Se valida que el archivo vlan.dat no este cargado, lo cual es así, debido a que lo eliminamos anteriormente.

Parte 2. Configurar los parámetros básicos de los dispositivos

Paso 1. Configurar la computadora de Internet

En el siguiente paso, veremos las tareas de configuración del servidor de Internet incluyen lo siguiente, así:

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
Gateway predeterminado IPv6	2001:DB8:ACAD:2::1



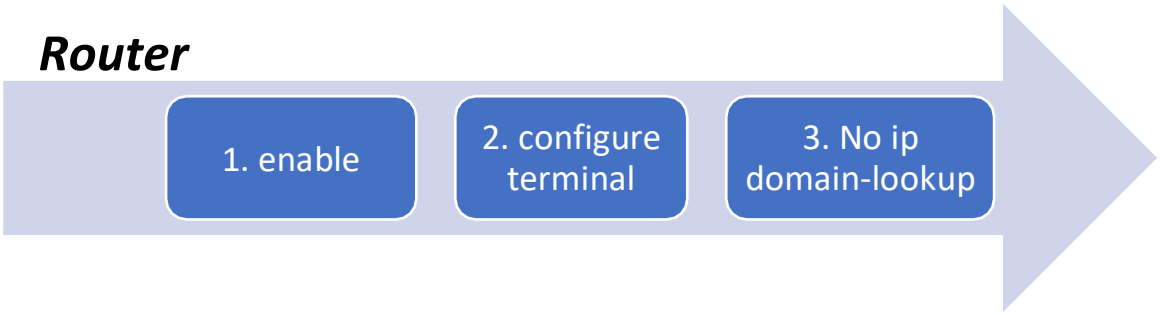
- Esta incorrecta la puerta de enlace ya que es la Primera Ip disponible en la red, siendo, 209.165.200.233.

- El prefijo cubre la sesión 2001:DB8:ACAD:A, lo cual se debe cambiar el default Gateway propuesto por el Tutor.

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

a. Desactivar la búsqueda DNS



3. no ip domain-lookup: Desactiva la traducción de nombres a dirección del dispositivo.

SINTAXIS:

```
Router>enable
Router#config t
Router (Config)#no ip domain-lookup
```

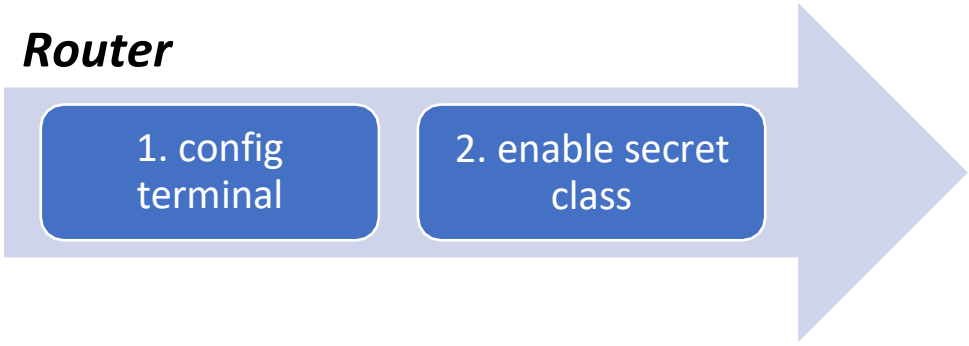
b. Nombre del Router (R1)

2. Hostname R1: Desde el modo de configuración, se digita el comando en el Router y/o Switch, cambiando el nombre del dispositivo.

SINTAXIS:

```
Router#config t
Router(config)# Hostname R1
R1(config)#
```

c. Contraseña de exec privilegiado cifrada (Class)

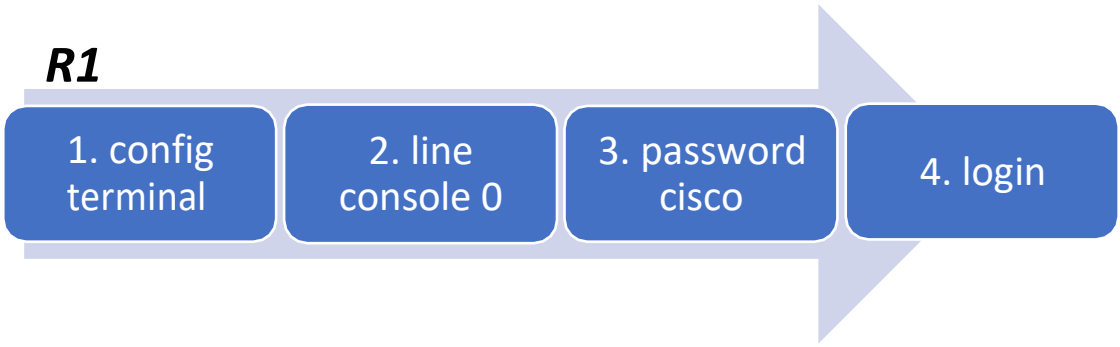


2. Enable secret “contraseña”: Se utiliza para restringir el acceso al modo EXEC privilegiado, adicional, que brinda un nivel de cifrado.

SINTAXIS:

R1>enable
R1#config terminal
R1(config)#enable secret class

d. Contraseña de acceso a la consola (cisco).

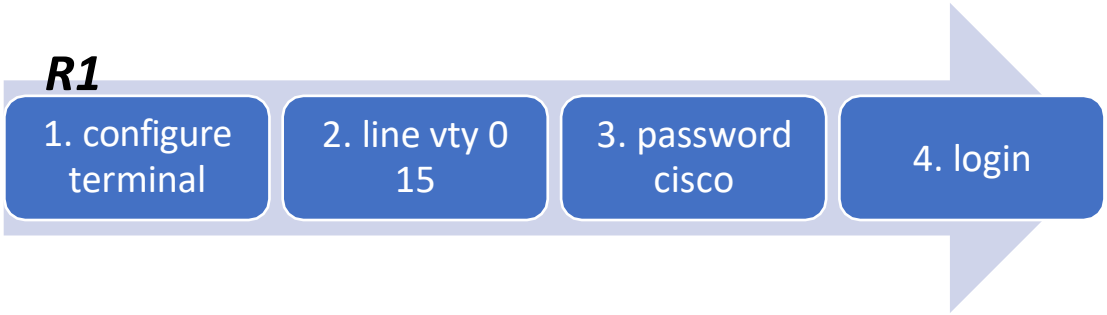


2. line console 0: se usa para ingresa al modo de configuración de la línea de consola, el cero representa la interfaz de consola.
3. password (contraseña): Se usa para especificar la contraseña para la línea de consola.
4. login: configura el Router para que requiera la autenticación al iniciar la sesión.

SINTAXIS:

R1#config t
R1(config) #line con 0
R1(config-line) #password cisco
R1(config-line) #login

e. Contraseña de acceso Telnet (cisco)



2. Vamos a la configuración de acceso a TELNET
3. Se configura la contraseña del acceso.

SINTAXIS:

R1#configure terminal
R1(config)#line vty 0 15
R1(config-line) #password cisco
R1(config-line) #login

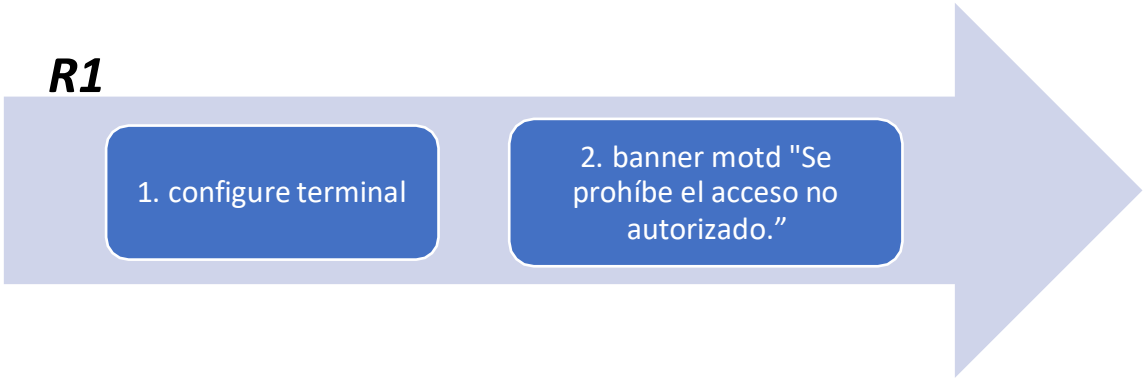
f. Cifrar las contraseñas de texto no cifrado.

2. Service password-encryption: Se encarga de aplicar un cifrado a todas las contraseñas que se encuentren sin cifrar.

SINTAXIS:

R1#configure terminal
R1(config)#service password-encryption

g. Mensaje MOTD "Se prohíbe el acceso no autorizado."

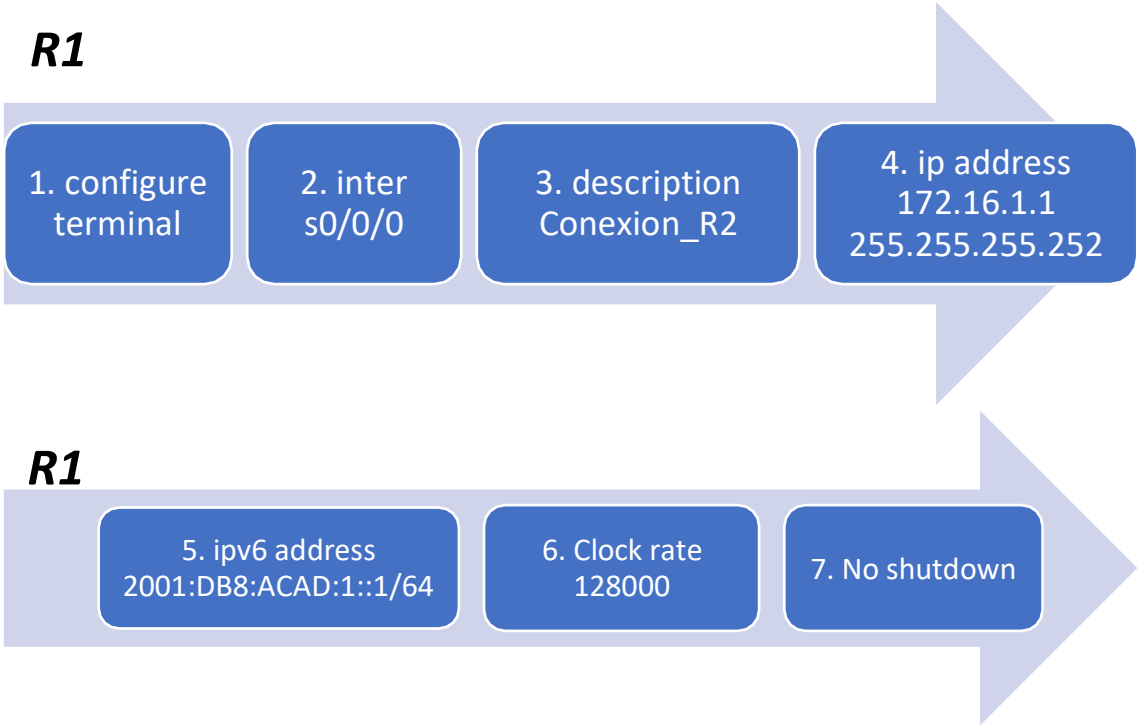


2. banner motd “Mensaje”: Es un Mensaje de aviso al ingreso del dispositivo configurado.

SINTAXIS:

R1#configure terminal
R1(config)#banner motd " Se prohíbe el acceso no autorizado.”

h. 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).



2. Se ingresa a la interfaz a configurar.
3. Descripción de la interfaz.
4. ip address, se le asigna la ip dada según la topología para la interfaz.
5. Se configura el direccionamiento ipv6 según la topología.
6. Se configura la frecuencia del reloj en 128000.
7. Se prende la interfaz.

SINTAXIS:

R1#configure terminal
R1(config)#inter s0/0/0
R1(config-if) #description Conexión_R2
R1(config-if) #ip address 172.16.1.1 255.255.255.252
R1(config-if) #ip address 2001:DB8:ACAD:1::1/64
R1(config-if) # Clock rate 128000
R1(config-if) #no shutdown

i. Rutas predeterminadas (Configurar una ruta IPv4 predeterminada de S0/0/0, configurar una ruta IPv6 predeterminada de S0/0/0)

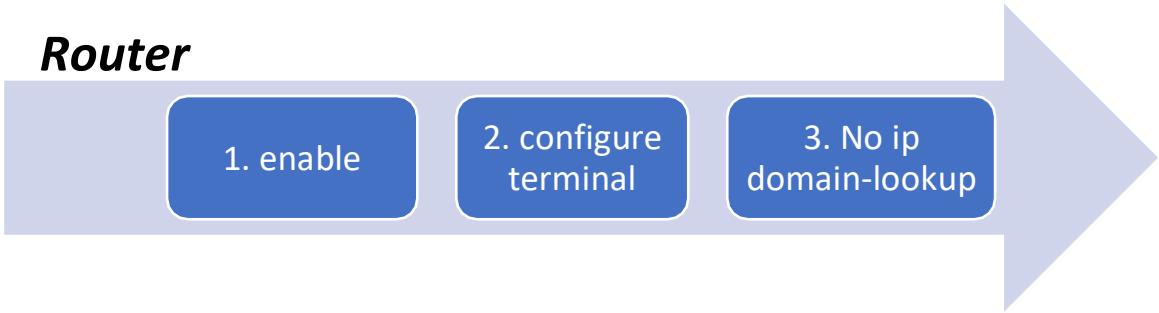
2. Se configura una ruta estática por defecto en direccionamiento IPV4 para la interfaz S0/0/0.
3. Se configura una ruta estática por defecto en direccionamiento IPV6 para la interfaz S0/0/0.

SINTAXIS:

R1#configure terminal
R1(config)#inter s0/0/0
R1(config-if) #Ip route 0.0.0.0 0.0.0.0 s0/0/0
R1(config-if) #ipv6 route ::/0 s0/0/0

Paso 2: Configurar R2

a. Desactivar la búsqueda DNS

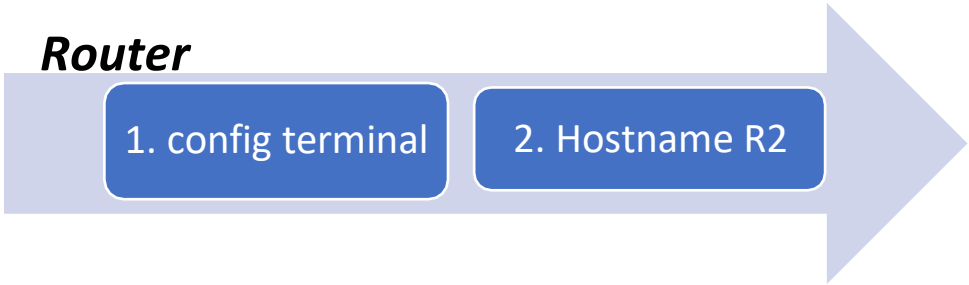


3. no ip domain-lookup: Desactiva la traducción de nombres a dirección del dispositivo.

SINTAXIS:

Router>enable
Router#config t
Router (Config)#no ip domain-lookup

b. Nombre del Router

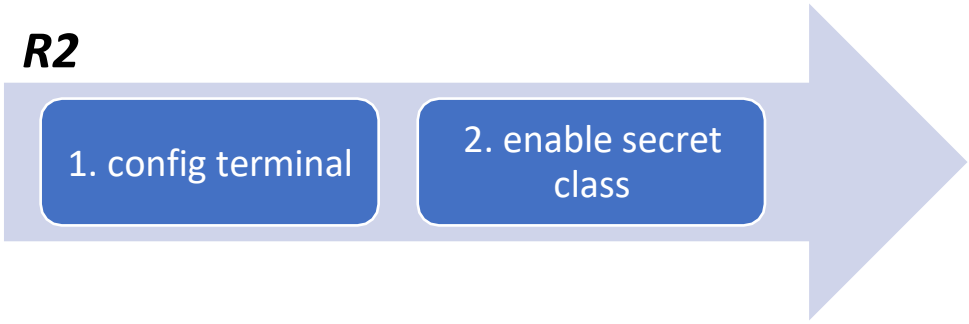


2. Hostname R2: Desde el modo de configuración, se digita el comando en el Router y/o Switch, cambiando el nombre del dispositivo.

SINTAXIS:

Router#config t
Router(config)# Hostname R2
R2(config)#

c. Contraseña de exec privilegiado cifrada (class).

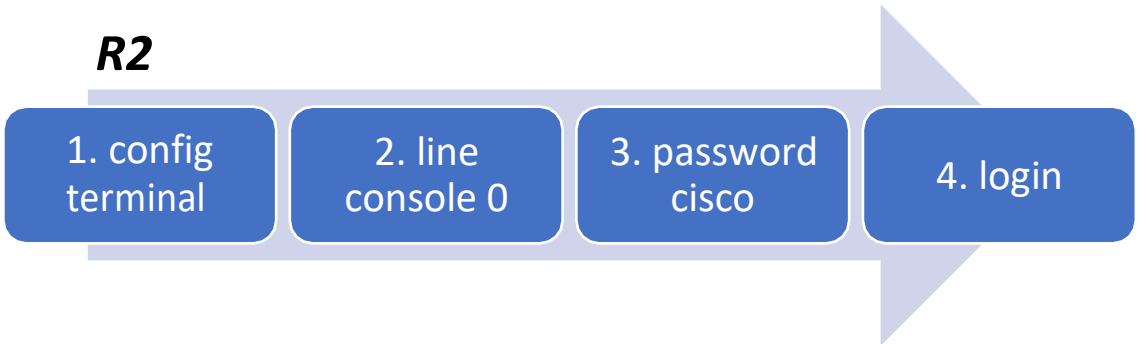


2. Enable secret “contraseña”: Se utiliza para restringir el acceso al modo EXEC privilegiado, adicional, que brinda un nivel de cifrado.

SINTAXIS:

R2>enable
R2#config terminal
R2(config)#enable secret class

d. Contraseña de acceso a la consola (cisco)



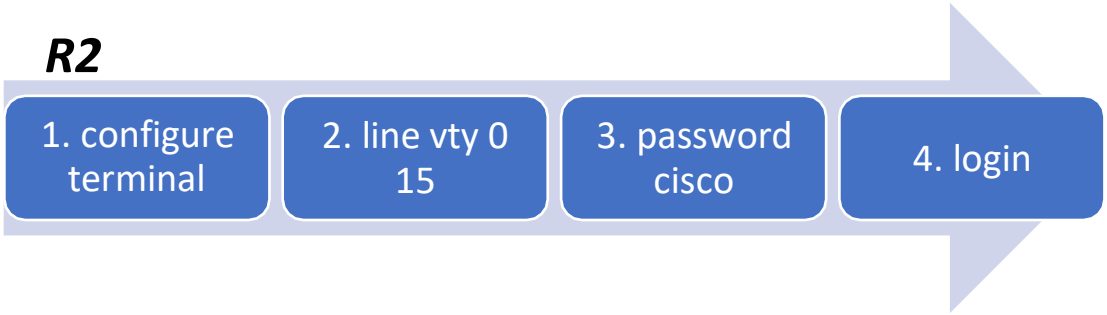
2. line console 0: se usa para ingresa al modo de configuración de la línea de consola, el cero representa la interfaz de consola.

3. password (contraseña): Se usa para especificar la contraseña para la línea de consola.
4. login: configura el Router para que requiera la autenticación al iniciar la sesión.

SINTAXIS:

R2#config t
R2(config) #line con 0
R2(config-line) #password cisco
R2(config-line) #login

e. Contraseña de acceso Telnet (cisco).



2. Vamos a la configuración de acceso a TELNET
3. Se configura la contraseña del acceso.

SINTAXIS:

R2#configure terminal
R2(config)#line vty 0 15
R2(config-line) #password cisco
R2(config-line) #login

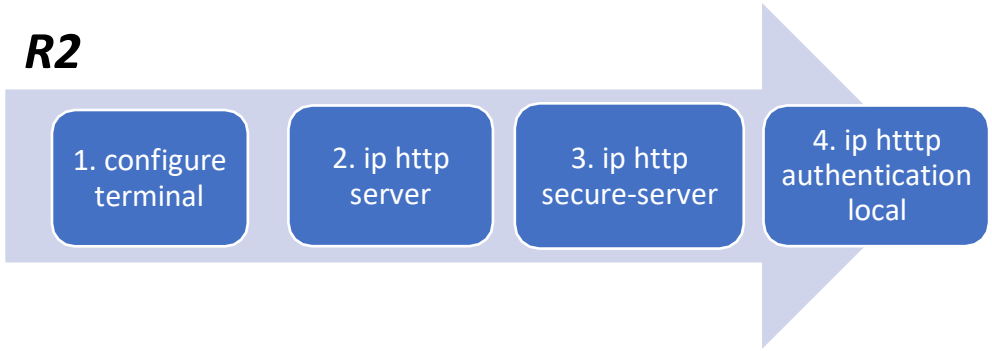
f. Cifrar las contraseñas de texto no cifrado.

2. Service password-encryption: Se encarga de aplicar un cifrado a todas las contraseñas que se encuentren sin cifrar.

SINTAXIS:

R2#configure terminal
R2(config)#service password-encryption

g. Habilitar el servidor HTTP

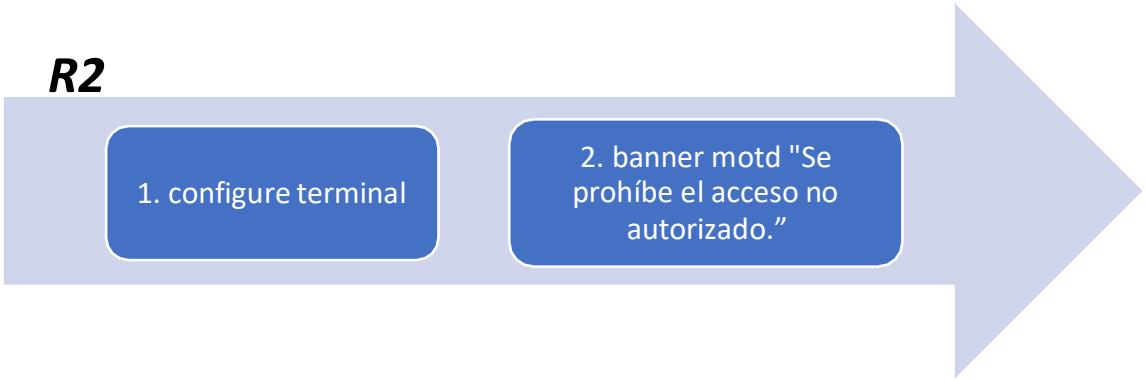


Se habilita la opción de http y htttps.

SINTAXIS:

R2(config)# ip http server
R2(config)# ip http secure-server
R2(config)# ip http authentication local

h. Mensaje MOTD.

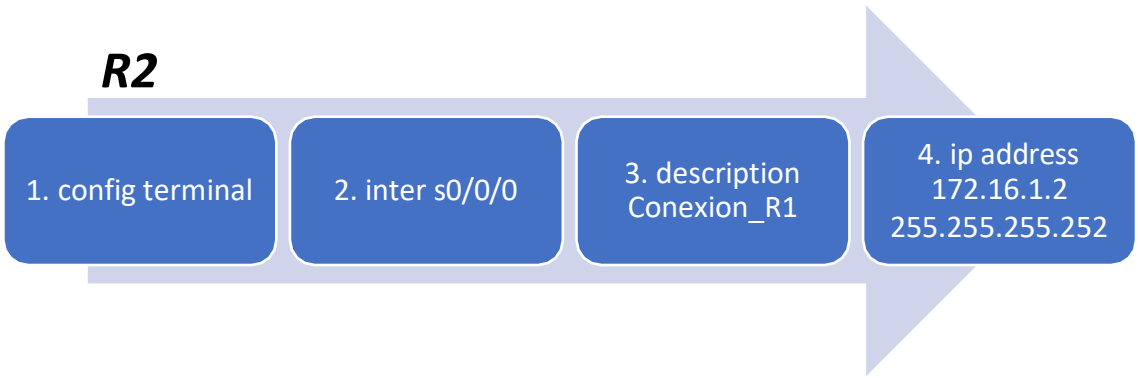


2. banner motd “Mensaje”: Es un Mensaje de aviso al ingreso del dispositivo configurado.

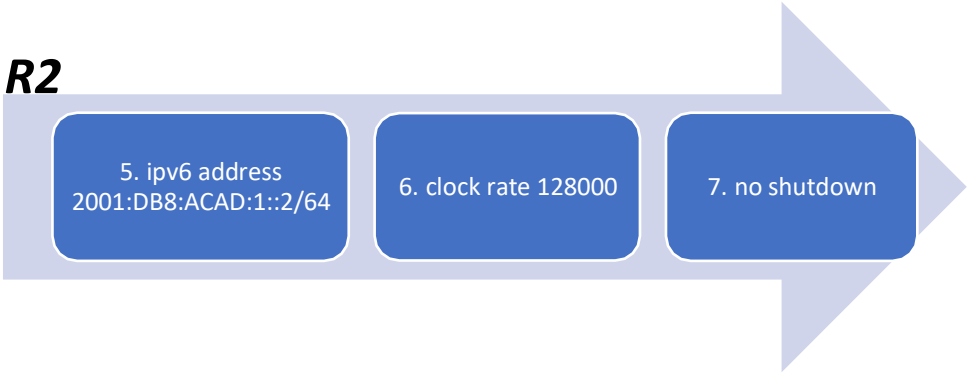
SINTAXIS:

R2#configure terminal
R2(config)#banner motd " Se prohíbe el acceso no autorizado.”

i. Interfaz S0/0/0 (Establecer la descripción, dirección ipv4 utilizando la primera dirección disponible en la subred, direccionamiento Ipv6, establecer la frecuencia de reloj en 128000, activar la interfaz)



2. Se ingresa a la Interfaz Serial 0/0/0, para configurarla.
3. Se crea la descripción de la interfaz.
4. Se configura el direccionamiento ipv4 en la interfaz mencionada.

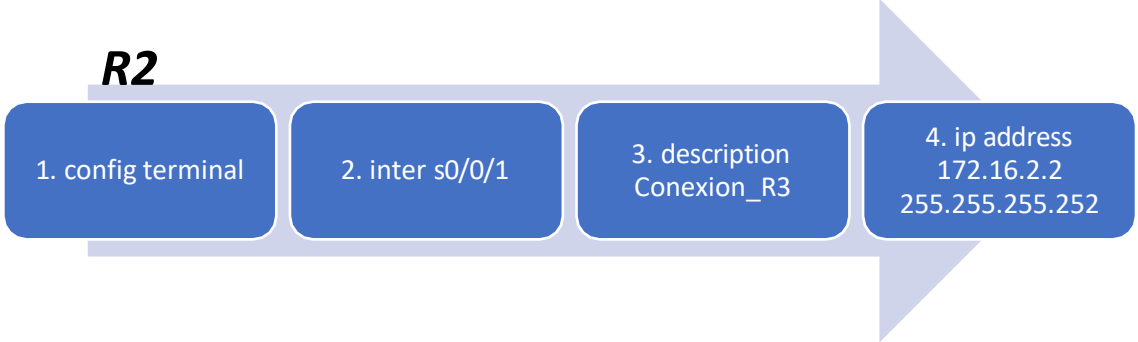


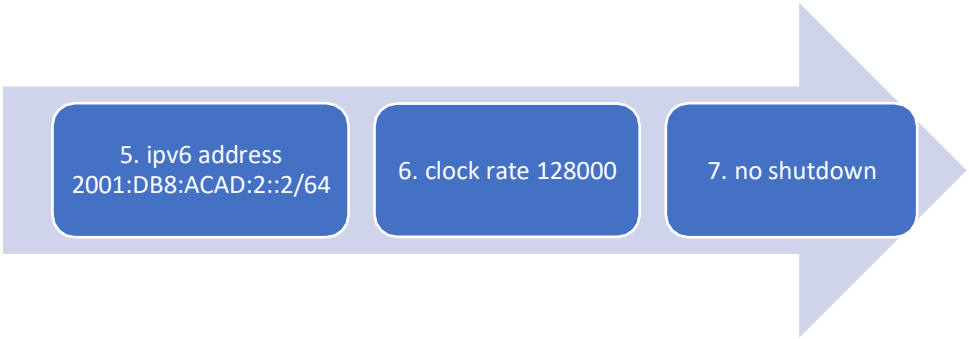
5. Se configura el direccionamiento Ipv6 en la interfaz mencionada.
6. Se configura la frecuencia del reloj en 128000.
7. Se prende la interfaz.

SINTAXIS:

```
R2#configure terminal
R2(config)#inter s0/0/0
R2(config-if) #description Conexión_R1
R2(config-if) #ip address 172.16.1.2 255.255.255.252
R2(config-if) #ip address 2001:DB8:ACAD:1::2/64
R2(config-if) # Clock rate 128000
R2(config-if) # no shutdown
```

j. Interfaz S0/0/1 (Establecer la descripción, dirección ipv4 utilizando la primera dirección disponible en la subred, direccionamiento Ipv6, establecer la frecuencia de reloj en 128000, activar la interfaz)

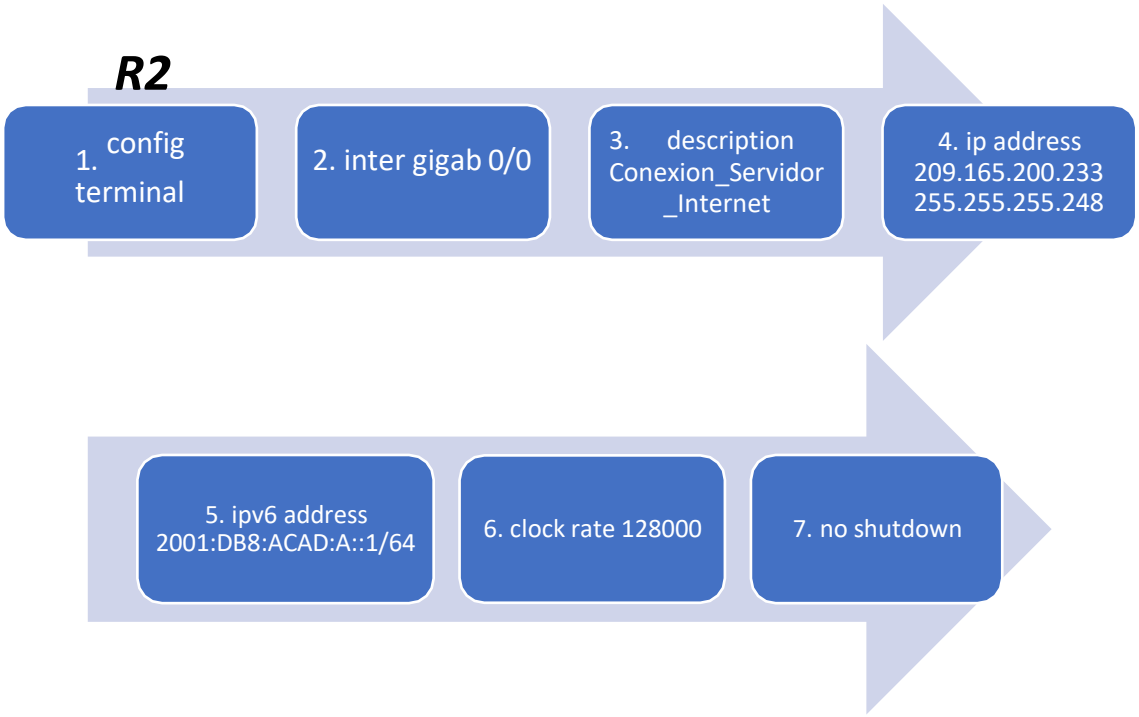




SINTAXIS:

R2#configure terminal
R2(config)#inter s0/0/1
R2(config-if) #description Conexión_R3
R2(config-if) #ip address 172.16.2.2 255.255.255.252
R2(config-if) #ip address 2001:DB8:ACAD:2::2/64
R2(config-if) # Clock rate 128000
R2(config-if) # no shutdown

k. Interfaz G0/0 (simulación de Internet)(Establecer la descripción, dirección ipv4 utilizando la primera dirección disponible en la subred, direccionamiento Ipv6, establecer la frecuencia de reloj en 128000, activar la interfaz)

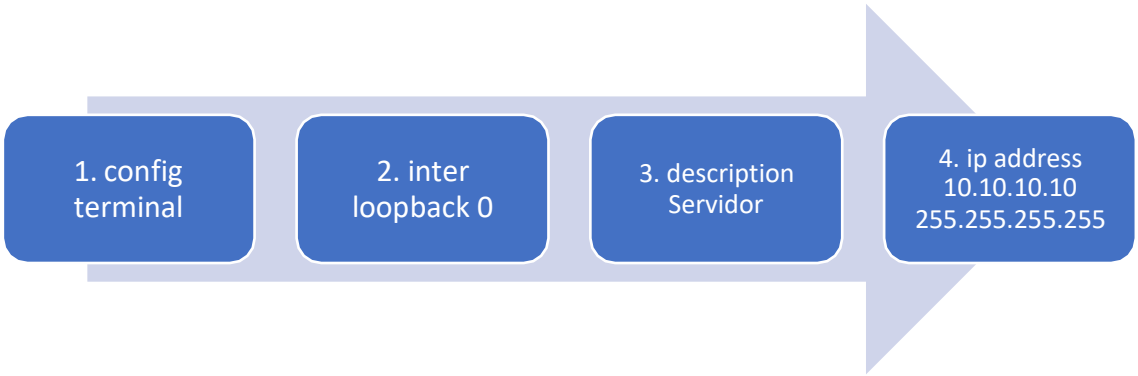


SINTAXIS:

R2#configure terminal
R2(config)#inter gi 0/0
R2(config-if) #description Conexion_Servidor_Internet
R2(config-if) #ip address 209.165.200.233 255.255.255.248
R2(config-if) #ip address 2001:DB8:ACAD:A::1/64
R2(config-if) # Clock rate 128000

R2(config-if) # no shutdown

l. Interfaz loopback 0 (servidor web simulado).



Establecemos en la interfaz loopback 0 la descripción y el direccionamiento Ipv4 según la topología.

SINTAXIS:

R2#configure terminal
R2(config)#inter loopback 0
R2(config-if) #description Servidor
R2(config-if) #ip address 10.10.10.10. 255.255.255.255

m. Ruta predeterminada

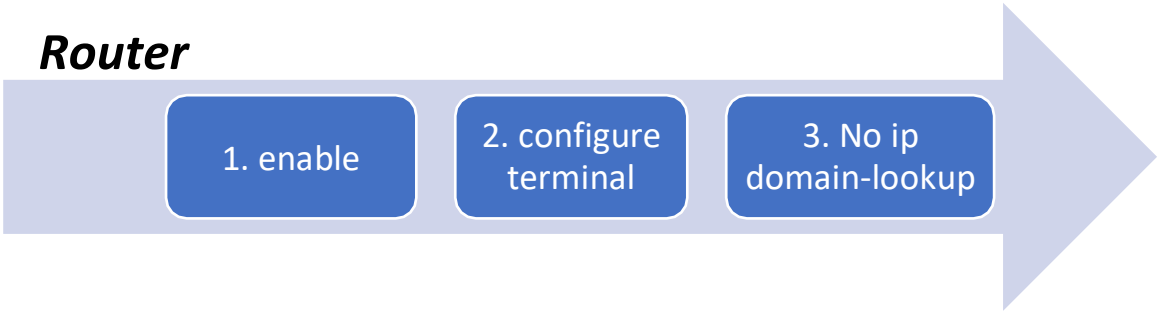
2. Se configura una ruta estática por defecto en direccionamiento IPV4 para la interfaz G0/0.
3. Se configura una ruta estática por defecto en direccionamiento IPV6 para la interfaz G0/0.

SINTAXIS:

R2#configure terminal
R2(config)#inter G0/0
R2(config-if) #Ip route 0.0.0.0 0.0.0.0 s0/0/0
R2(config-if) #ipv6 route ::/0 G0/0

Paso 3: Configurar R3

a. Desactivar la búsqueda DNS

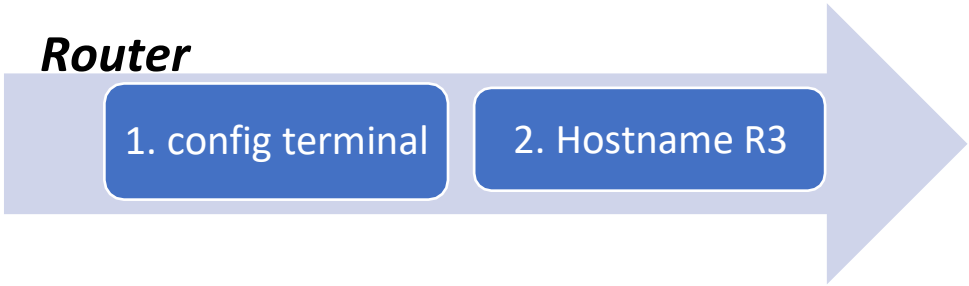


3. no ip domain-lookup: Desactiva la traducción de nombres a dirección del dispositivo.

SINTAXIS:

Router>enable
Router#config t
Router (Config)#no ip domain-lookup

b. Nombre del Router

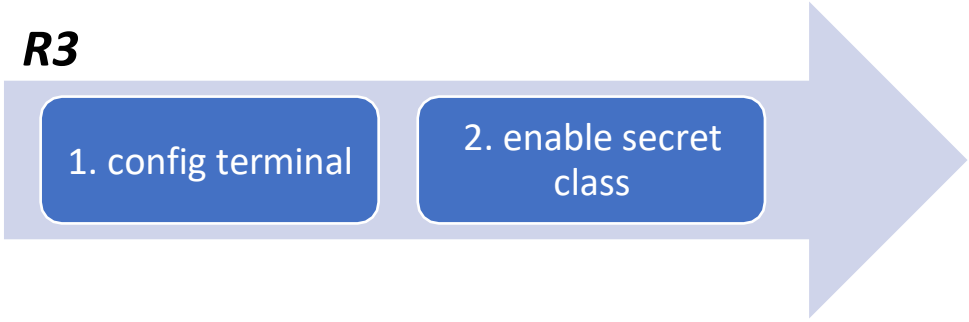


2. Hostname R3: Desde el modo de configuración, se digita el comando en el Router y/o Switch, cambiando el nombre del dispositivo.

SINTAXIS:

Router#config t
Router(config)# Hostname R3
R3(config)#

c. Contraseña de exec privilegiado cifrada (class).

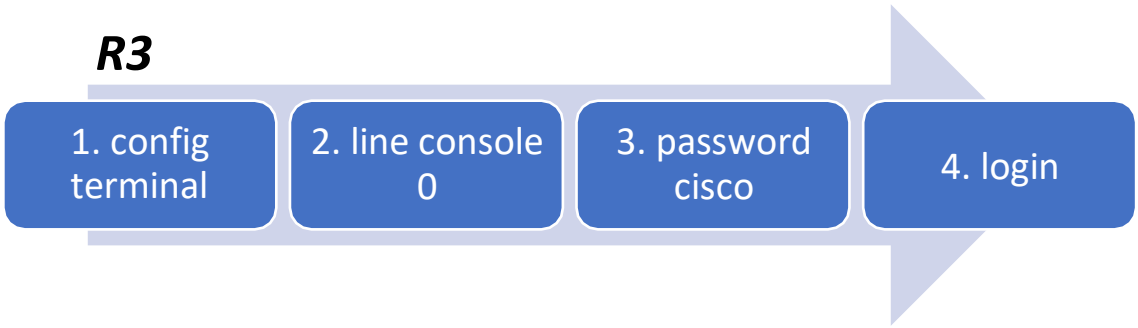


2. Enable secret “contraseña”: Se utiliza para restringir el acceso al modo EXEC privilegiado, adicional, que brinda un nivel de cifrado.

SINTAXIS:

R3>enable
R3#config terminal
R3(config)#enable secret class

d. Contraseña de acceso a la consola (cisco)

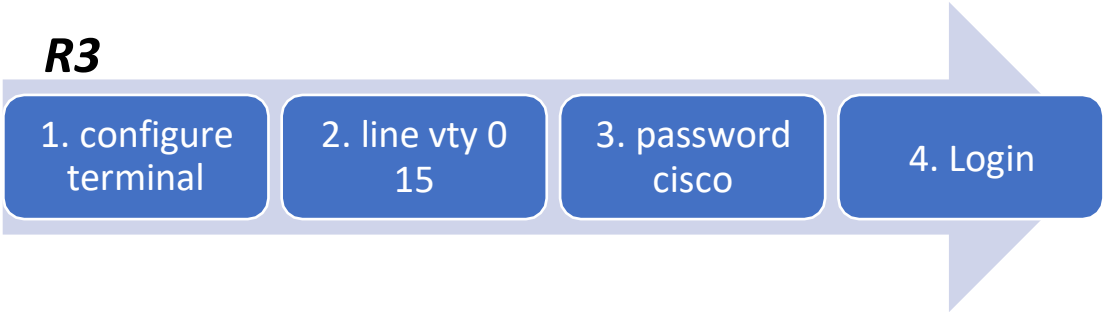


2. line console 0: se usa para ingresa al modo de configuración de la línea de consola, el cero representa la interfaz de consola.
3. password (contraseña): Se usa para especificar la contraseña para la línea de consola.
4. login: configura el Router para que requiera la autenticación al iniciar la sesión.

SINTAXIS:

R3#config t
R3(config) #line con 0
R3(config-line) #password cisco
R3(config-line) #login

e. Contraseña de acceso Telnet (cisco).



2. Vamos a la configuración de acceso a TELNET
3. Se configura la contraseña del acceso.

SINTAXIS:

R3#configure terminal
R3(config)#line vty 0 15
R3(config-line) #password cisco
R3(config-line) #login

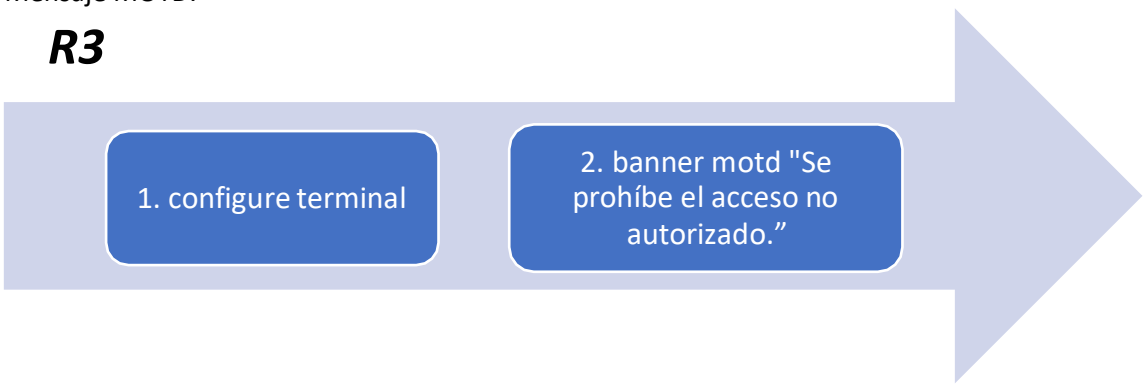
f. Cifrar las contraseñas de texto no cifrado.

2. Service password-encryption: Se encarga de aplicar un cifrado a todas las contraseñas que se encuentren sin cifrar.

SINTAXIS:

R3#configure terminal
R3(config)#service password-encryption

g. Mensaje MOTD.

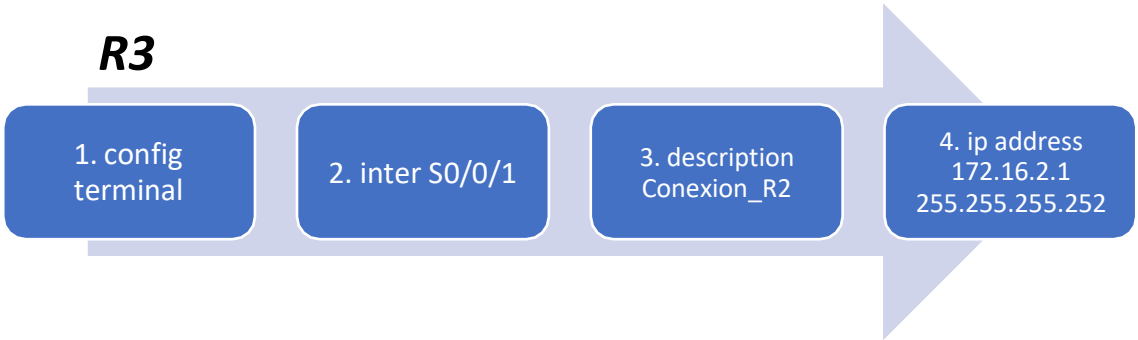


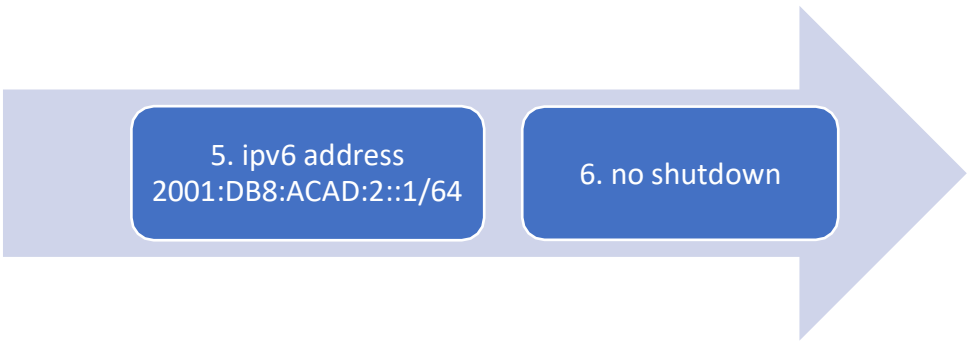
2. banner motd “Mensaje”: Es un Mensaje de aviso al ingreso del dispositivo configurado.

SINTAXIS:

R3#configure terminal
R3(config)#banner motd " Se prohíbe el acceso no autorizado.”

h. Interfaz S0/0/1 (Establecer la descripción, dirección ipv4 utilizando la primera dirección disponible en la subred, direccionamiento Ipv6, activar la interfaz).





SINTAXIS:

R3#configure terminal
R3(config)#inter S0/0/1
R3(config-if) #description Conexion_R2
R3(config-if) #ip address 172.16.2.1 255.255.255.252
R3(config-if) #ip address 2001:DB8:ACAD:2::1/64
R3(config-if) # no shutdown

i. Interfaz loopback 4

Utilizamos la primera dirección ip disponible en la red.

SINTAXIS:

R3#configure terminal
R3(config)#inter loopback 4
R3(config-if) #ip address 192.168.4.1 255.255.255.0

j. Interfaz loopback 5

Utilizamos la primera dirección ip disponible en la red.

SINTAXIS:

R3#configure terminal
R3(config)#inter loopback 5
R3(config-if) #ip address 192.168.5.1 255.255.255.0

k. Interfaz loopback 6

Utilizamos la primera dirección ip disponible en la red.

SINTAXIS:

R3#configure terminal
R3(config)#inter loopback 6
R3(config-if) #ip address 192.168.6.1 255.255.255.0

l. Interfaz loopback 7

Utilizamos direccionamiento ipv6 disponible en la red.

SINTAXIS:

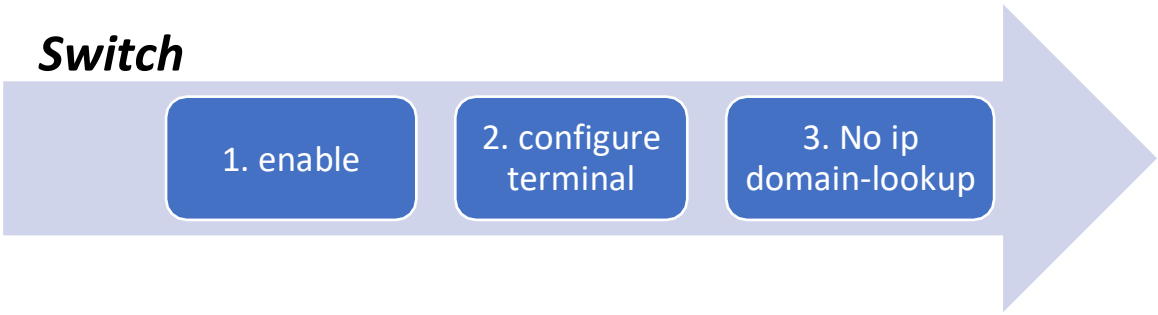
R3#configure terminal
R3(config)#inter loopback 7
R3(config-if) #ipv6 address 2001:FB8:ACAD:3::1/64

m. Rutas predeterminadas.

Se configura la ruta estática por defecto.

Paso 4: Configurar S1

a. Desactivar la búsqueda DNS

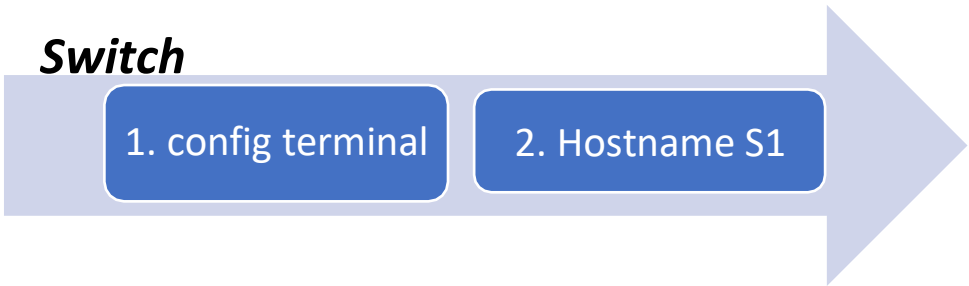


3. no ip domain-lookup: Desactiva la traducción de nombres a dirección del dispositivo.

SINTAXIS:

```
Switch>enable
Switch#config t
Switch (Config)#no ip domain-lookup
```

b. Nombre del Router

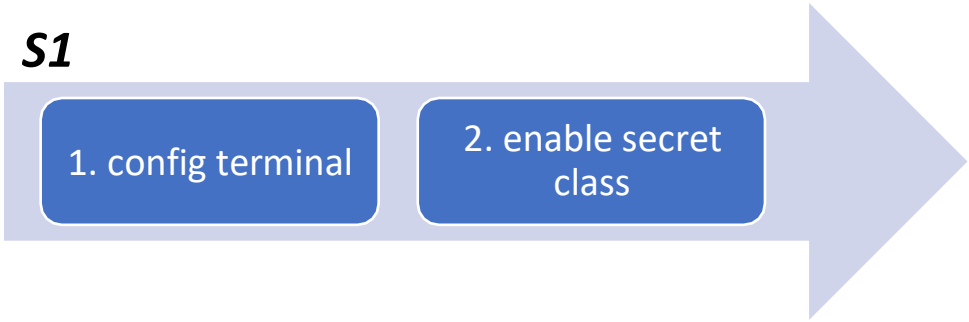


2. Hostname S1: Desde el modo de configuración, se digita el comando en el Router y/o Switch, cambiando el nombre del dispositivo.

SINTAXIS:

```
Switch#config t
Switch(config)# Hostname S1
S1(config)#
```

c. Contraseña de exec privilegiado cifrada (class).

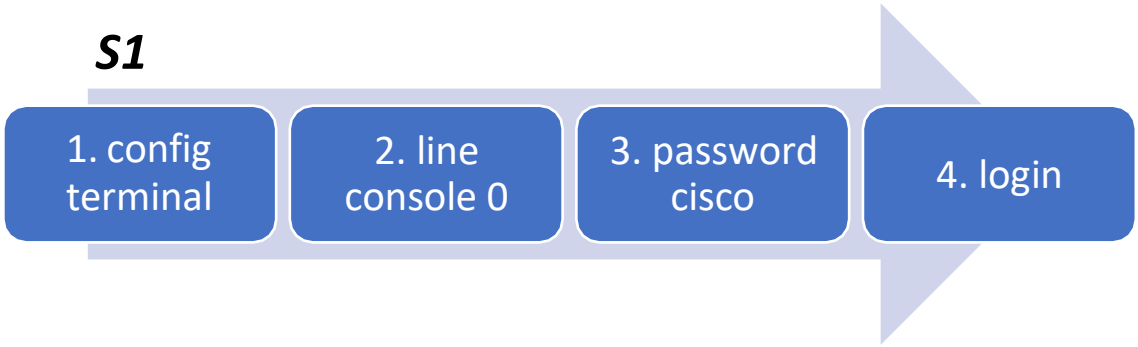


2. Enable secret “contraseña”: Se utiliza para restringir el acceso al modo EXEC privilegiado, adicional, que brinda un nivel de cifrado.

SINTAXIS:

S1>enable
S1#config terminal
S1(config)#enable secret class

d. Contraseña de acceso a la consola (cisco)

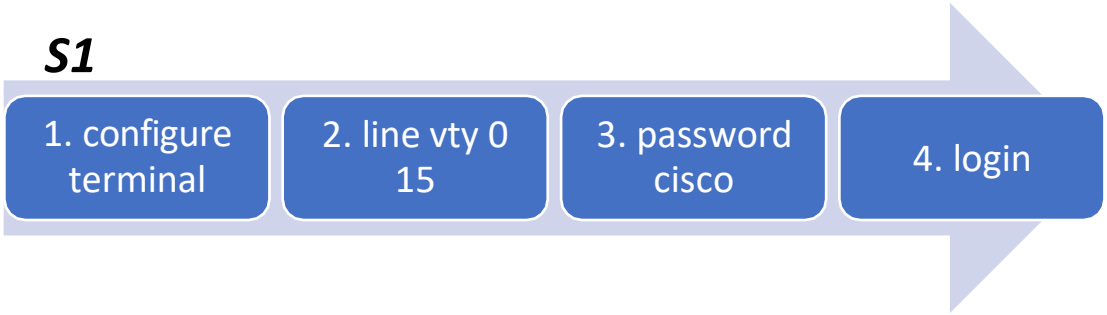


2. line console 0: se usa para ingresa al modo de configuración de la línea de consola, el cero representa la interfaz de consola.
3. password (contraseña): Se usa para especificar la contraseña para la línea de consola.
4. login: configura el Router para que requiera la autenticación al iniciar la sesión.

SINTAXIS:

S1#config t
S1(config) #line con 0
S1(config-line) #password cisco
S1(config-line) #login

e. Contraseña de acceso Telnet (cisco).



2. Vamos a la configuración de acceso a TELNET
3. Se configura la contraseña del acceso.

SINTAXIS:

S1#configure terminal
S1(config)#line vty 0 15
S1(config-line) #password cisco
S1(config-line) #login

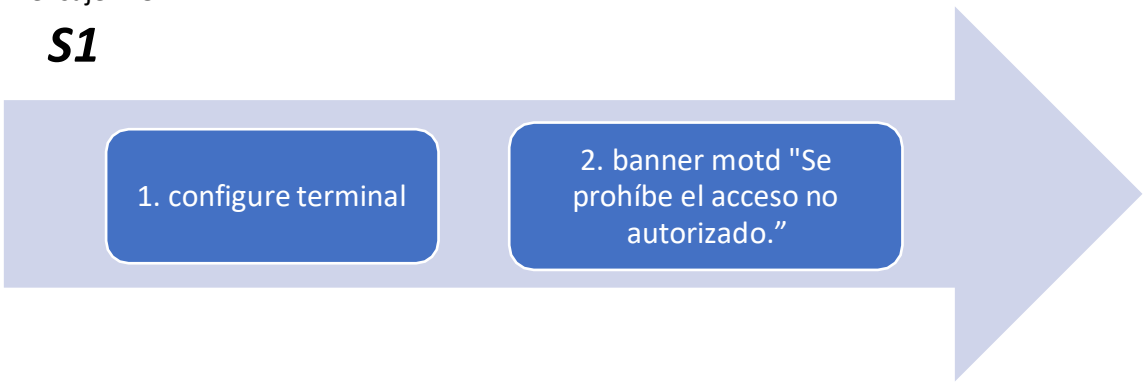
f. Cifrar las contraseñas de texto no cifrado.

2. Service password-encryption: Se encarga de aplicar un cifrado a todas las contraseñas que se encuentren sin cifrar.

SINTAXIS:

S1#configure terminal
S1(config)#service password-encryption

g. Mensaje MOTD.



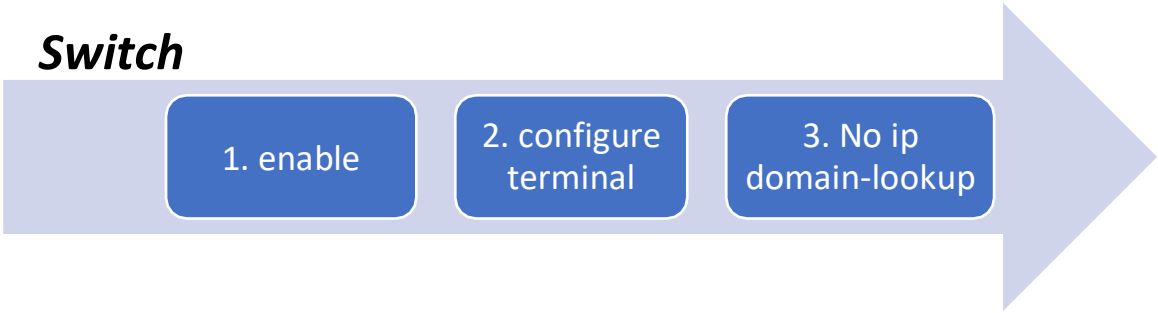
2. banner motd “Mensaje”: Es un Mensaje de aviso al ingreso del dispositivo configurado.

SINTAXIS:

S1#configure terminal
S1(config)#banner motd " Se prohíbe el acceso no autorizado."

Paso 5: Configurar el S3

a. Desactivar la búsqueda DNS

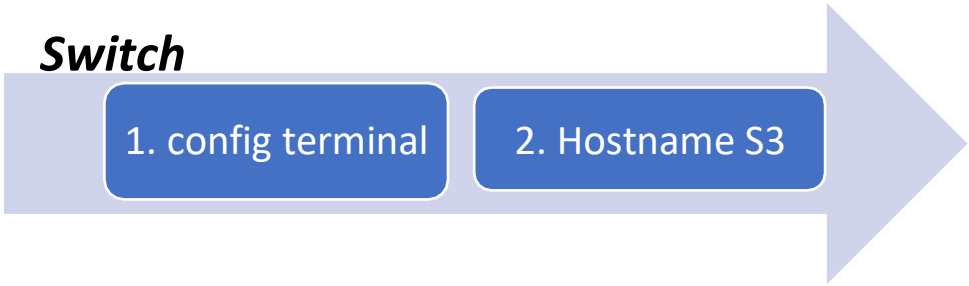


3. no ip domain-lookup: Desactiva la traducción de nombres a dirección del dispositivo.

SINTAXIS:

Switch>enable
Switch#config t
Switch (Config)#no ip domain-lookup

b. Nombre del Router

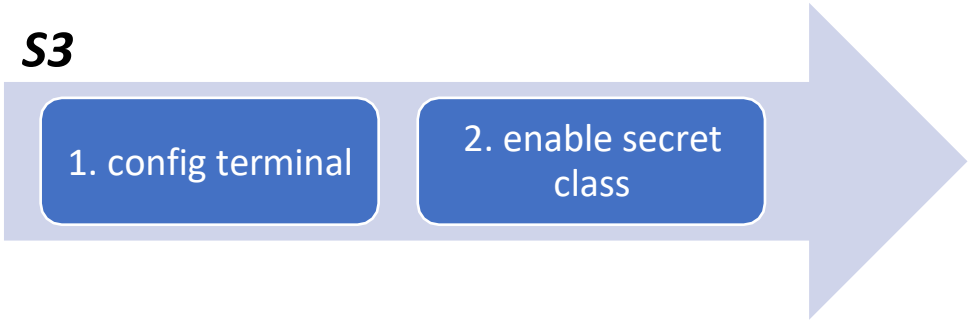


2. Hostname S3: Desde el modo de configuración, se digita el comando en el Router y/o Switch, cambiando el nombre del dispositivo.

SINTAXIS:

Switch#config t
Switch(config)# Hostname S3
S3(config)#

c. Contraseña de exec privilegiado cifrada (class).

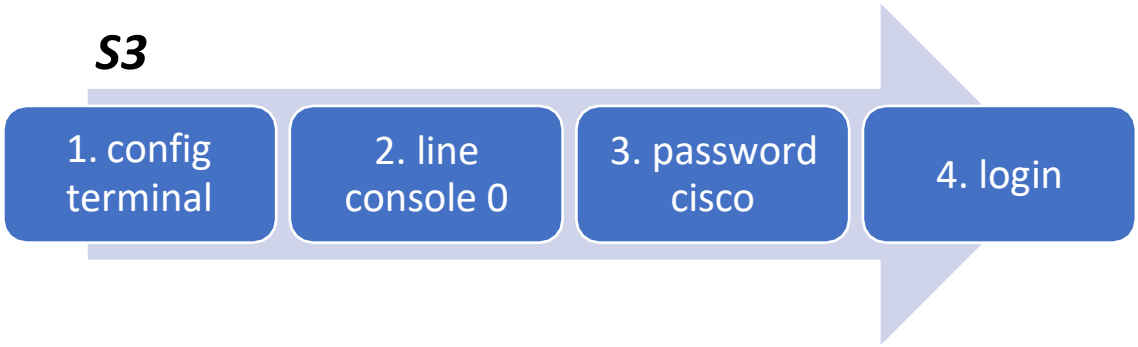


2. Enable secret “contraseña”: Se utiliza para restringir el acceso al modo EXEC privilegiado, adicional, que brinda un nivel de cifrado.

SINTAXIS:

S3>enable
S3#config terminal
S3(config)#enable secret class

d. Contraseña de acceso a la consola (cisco)

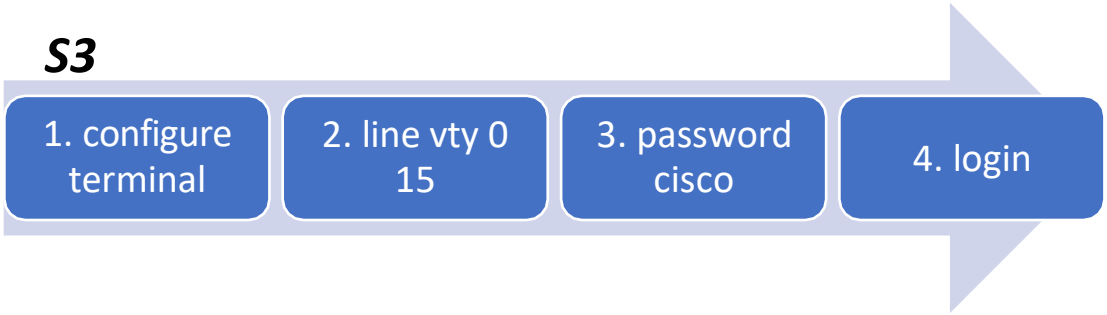


2. line console 0: se usa para ingresa al modo de configuración de la línea de consola, el cero representa la interfaz de consola.
3. password (contraseña): Se usa para especificar la contraseña para la línea de consola.
4. login: configura el Router para que requiera la autenticación al iniciar la sesión.

SINTAXIS:

S3#config t
S3(config) #line con 0
S3(config-line) #password cisco
S3(config-line) #login

e. Contraseña de acceso Telnet (cisco).



2. Vamos a la configuración de acceso a TELNET
3. Se configura la contraseña del acceso.

SINTAXIS:

S3#configure terminal
S3(config)#line vty 0 15
S3(config-line) #password cisco
S3(config-line) #login

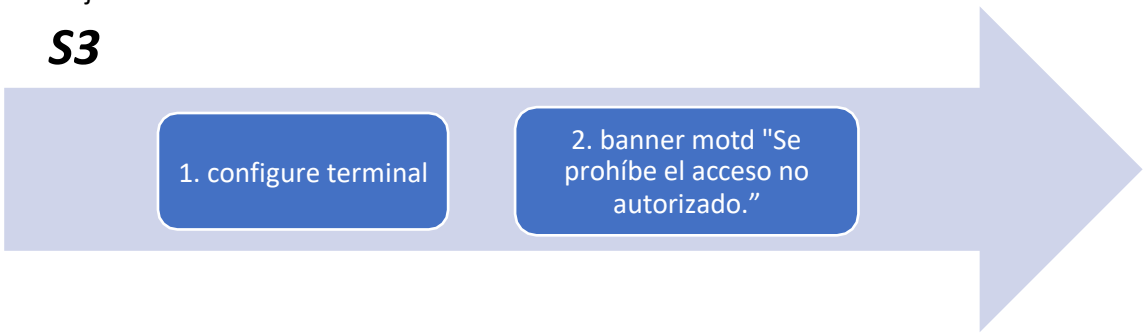
f. Cifrar las contraseñas de texto no cifrado.

2. Service password-encryption: Se encarga de aplicar un cifrado a todas las contraseñas que se encuentren sin cifrar.

SINTAXIS:

S3#configure terminal
S3(config)#service password-encryption

g. Mensaje MOTD.



2. banner motd “Mensaje”: Es un Mensaje de aviso al ingreso del dispositivo configurado.

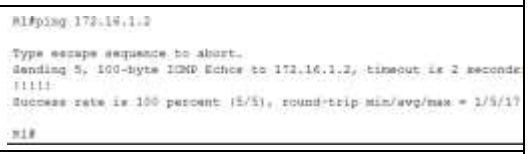
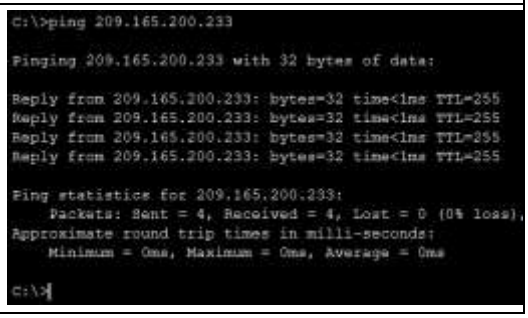
SINTAXIS:

S3#configure terminal
S3(config)#banner motd " Se prohíbe el acceso no autorizado."

Paso 6: Verificar la conectividad de la red

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

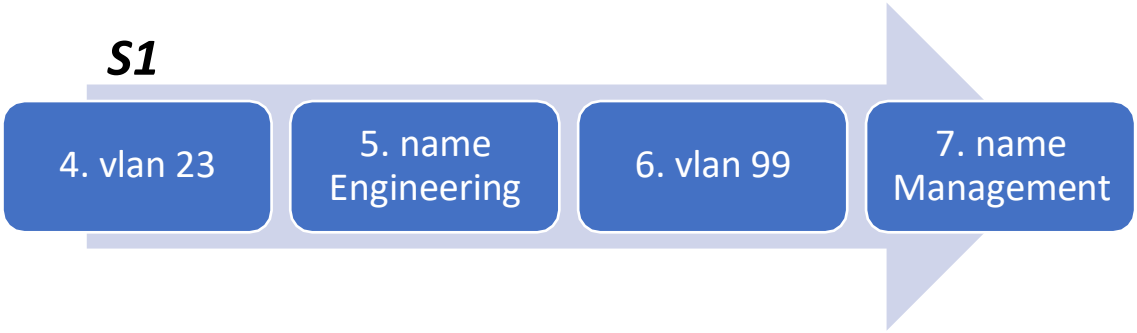
Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Desde	Dirección IP	Resultados de ping
R1	172.16.1.2	
R2	172.16.2.1	
PC de Internet	209.165.200.233	

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

Paso 1. Configurar S1

a. Crear la base de datos de VLAN

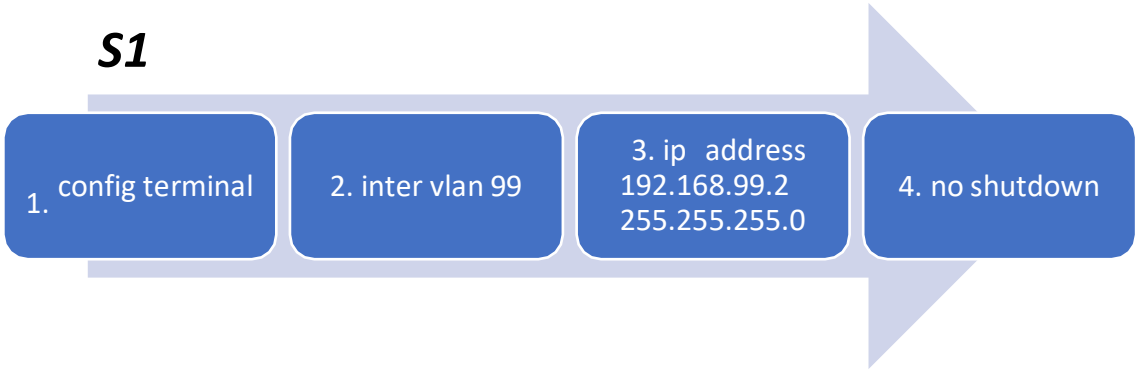


Se crean las Vlan según la tabla.

SINTAXIS:

S1#configure terminal
S1(config)#vlan 21
S1(config)#name Accounting
S1(config)#vlan 23
S1(config)#name Engineering
S1(config)#vlan 99
S1(config)#name Management

b. Asignar la dirección IP de administración.

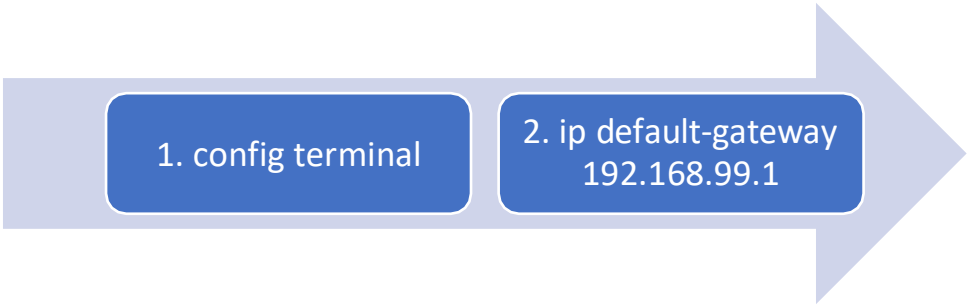


Se configura la vlan de administración Vlan 99(en este caso), utilizando la ip asignada para el S1 en el diagrama de la topología. Se activa la interfaz de vlan.

SINTAXIS:

S1#configure terminal
S1(config)#inter vlan 99
S1(config-if) #ip address 192.168.99.2 255.255.255.0
S1(config-if) # no shutdown

c. Asignar el gateway predeterminado.

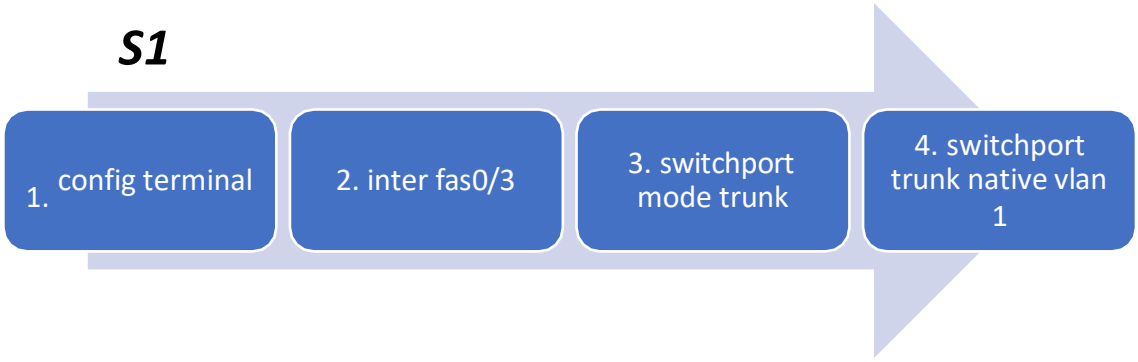


SINTAXIS:

S1#configure terminal

S1(config)#Ip default-gateway 192.168.99.1

d. Forzar el enlace troncal en la interfaz F0/3, utilizando la Vlan 1 como Vlan Native.



SINTAXIS:

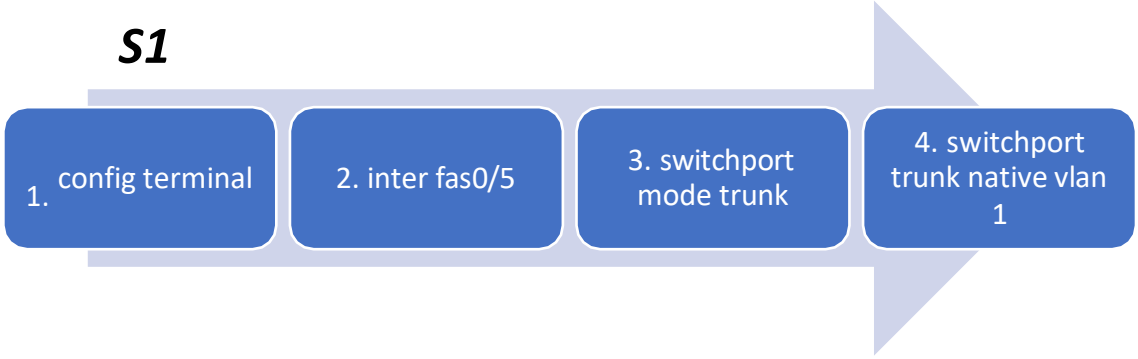
S1#configure terminal

S1(config)#inter f0/3

S1(config-if) #switchport mode trunk

S1(config-if) #switchport trunk native vlan 1

e. Forzar el enlace troncal en la interfaz F0/5, utilizando la Vlan 1 como Vlan Native.



SINTAXIS:

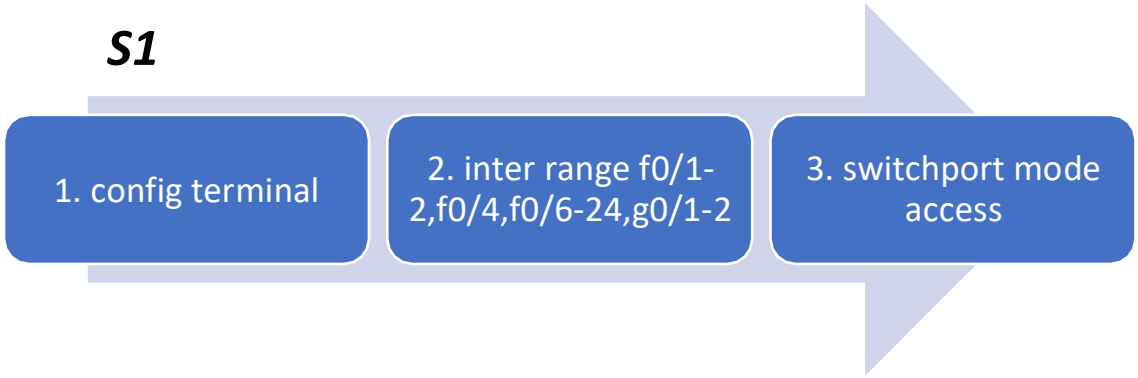
S1#configure terminal

S1(config)#inter f0/5

S1(config-if) #switchport mode trunk

S1(config-if) #switchport trunk native vlan 1

f. Configurar el resto de los puertos como puertos de acceso.



SINTAXIS:

S1#configure terminal

S1(config)# inter range f0/1-2,f0/4,f0/6-24,g0/1-2

S1(config-if-range) # switchport mode access

g. Asignar F0/6 a la VLAN 21

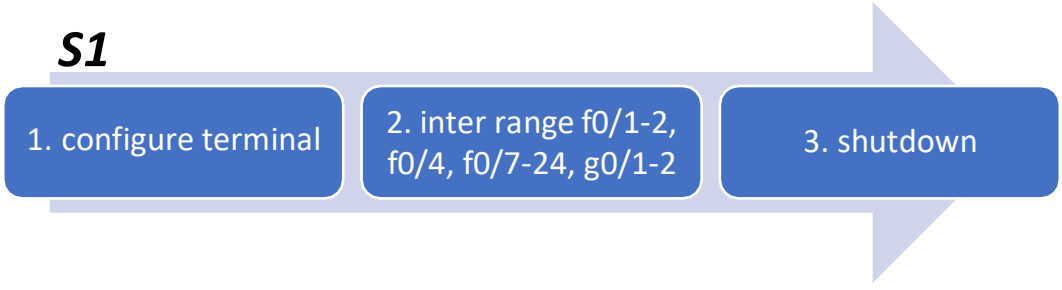
SINTAXIS:

S1#configure terminal

S1(config)# inter f0/6

S1(config-if) # switchport access vlan 21

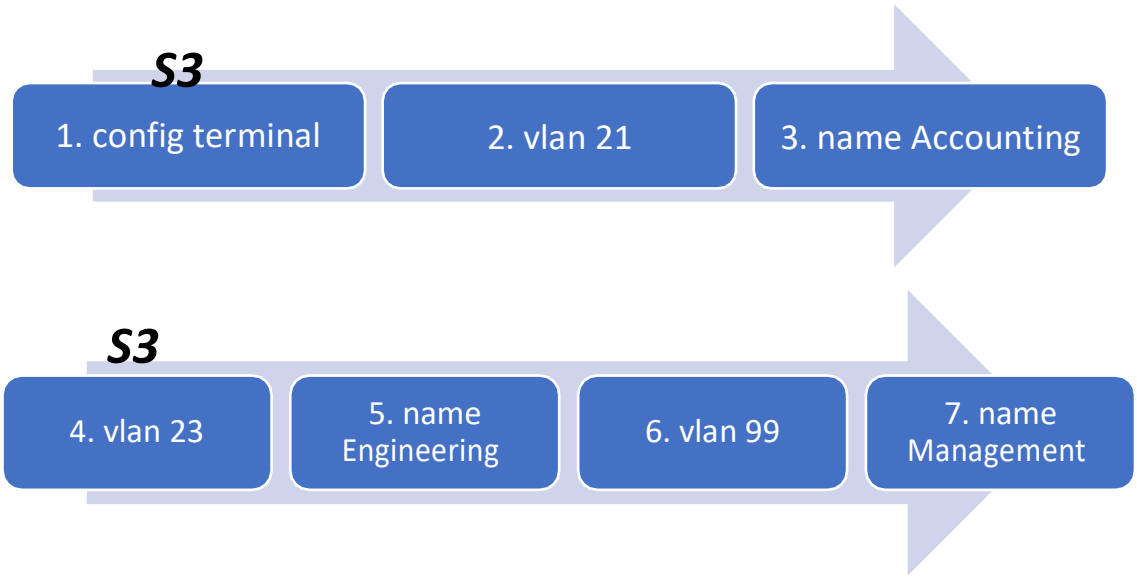
h. Apagar todos los puertos sin usar.



S1#configure terminal
S1(config)# inter range f0/1-2, f0/4, f0/7-24, g0/1-2
S1(config-if-range) # shutdown

Paso 2: Configurar el S3

a. Crear la base de datos de VLAN

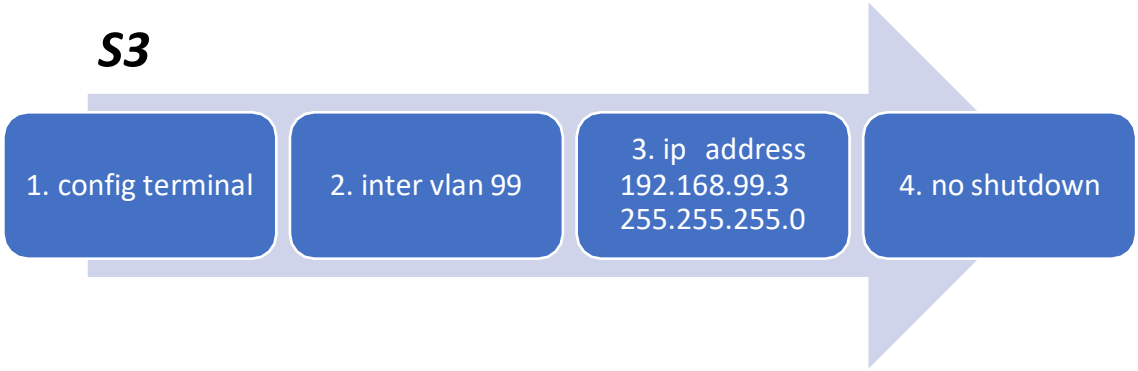


Se crean las Vlan según la tabla.

SINTAXIS:

S3#configure terminal
S3(config)#vlan 21
S3(config)#name Accounting
S3(config)#vlan 23
S3(config)#name Engineering
S3(config)#vlan 99
S3(config)#name Management

b. Asignar la dirección IP de administración.



Se configura la vlan de administración Vlan 99(en este caso), utilizando la ip asignada para el S3 en el diagrama de la topología. Se activa la interfaz de vlan.

SINTAXIS:

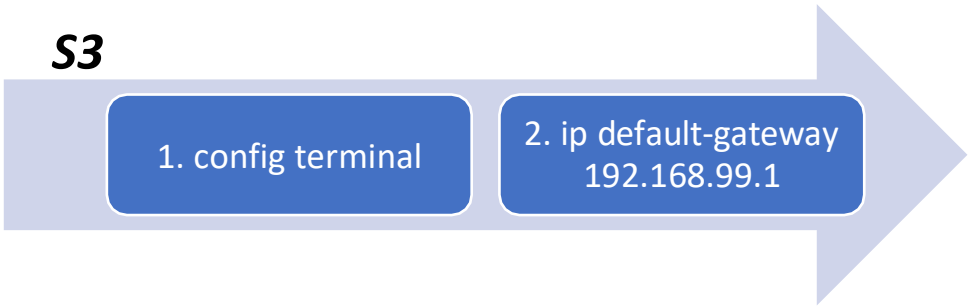
S3#configure terminal

S3(config)#inter vlan 99

S3(config-if) #ip address 192.168.99.3 255.255.255.0

S3(config-if) # no shutdown

c. Asignar el gateway predeterminado.

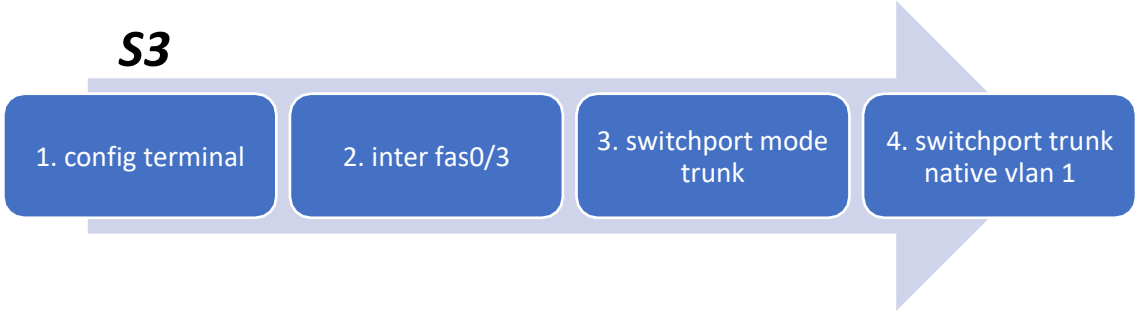


SINTAXIS:

S3#configure terminal

S3(config)#Ip default-gateway 192.168.99.1

d. Forzar el enlace troncal en la interfaz F0/3, utilizando la Vlan 1 como Vlan Native.

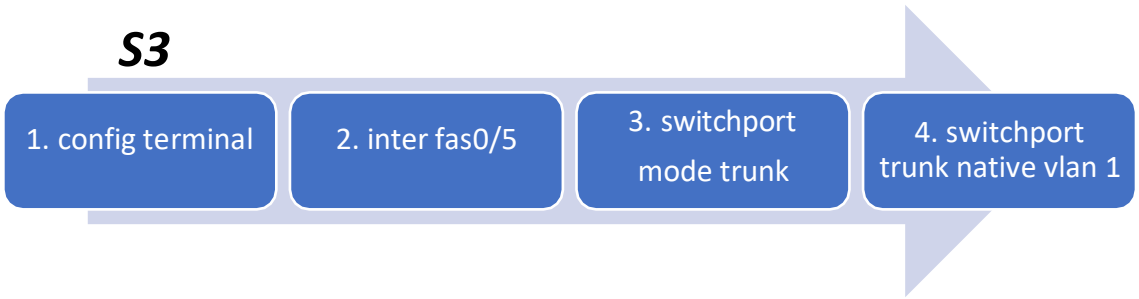


SINTAXIS:

S3#configure terminal

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

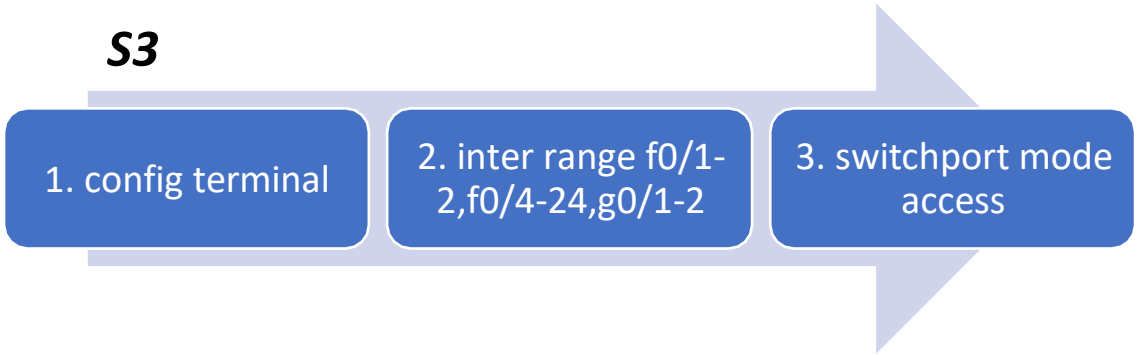
e. Forzar el enlace troncal en la interfaz F0/5, utilizando la Vlan 1 como Vlan Native.



SINTAXIS:

S3#configure terminal
S3(config)#inter f0/5
S3(config-if) #switchport mode trunk
S3(config-if) #switchport trunk native vlan 1

f. Configurar el resto de los puertos como puertos de acceso.



SINTAXIS:

S3#configure terminal
S3(config)# inter range f0/1-2, f0/4-24, g0/1-2
S3(config-if-range) # switchport mode access

g. Asignar F0/18 a la VLAN 23

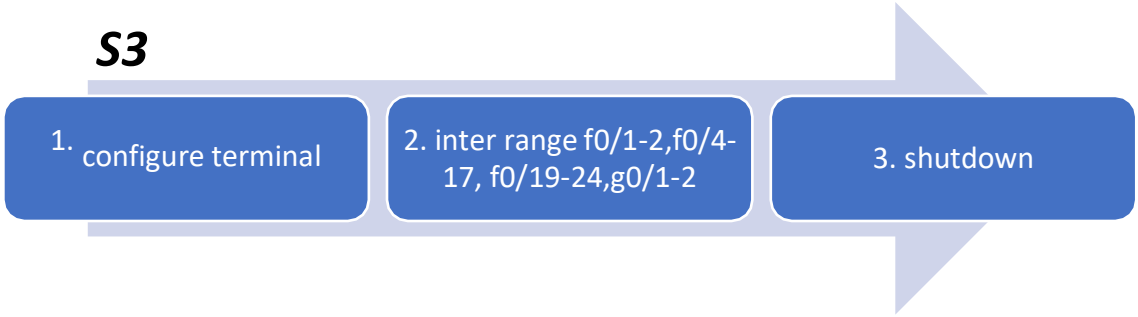
SINTAXIS:

S3#configure terminal

S3(config)# inter f0/18

S3(config-if) # switchport access vlan 23

h. Apagar todos los puertos sin usar.



S3#configure terminal

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

S3(config-if-range) # shutdown

Paso 3: Configurar R1

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

En la Subinterfaz g0/1.21, se realiza la descripción correspondiente , se le asigna la Vlan 21 y se le asigna la primera dirección disponible de esta interfaz.

SINTAXIS:

R1#configure terminal

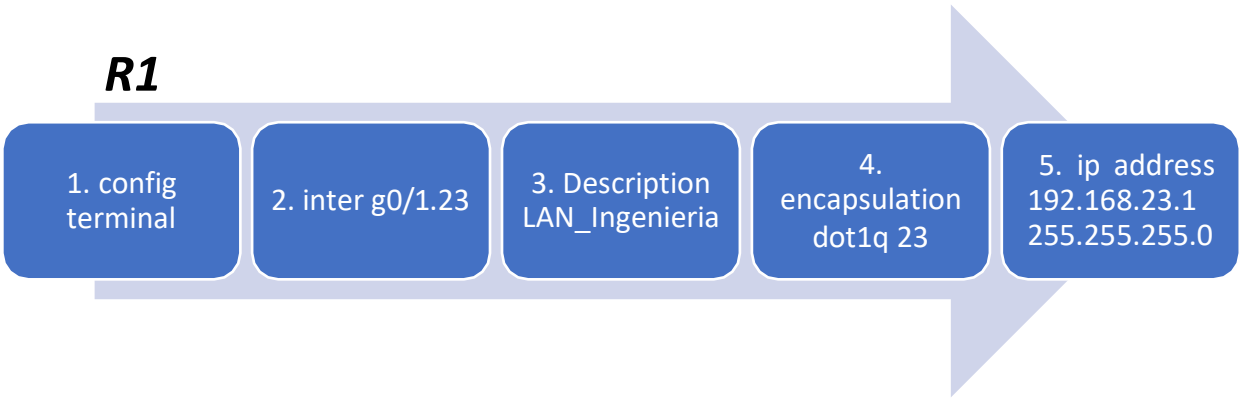
R1(config)# inter g0/1.21

R1(config-if) # Description LAN_Contabilidad

R1(config-if) # encapsulation dot1q 21

R1(config-if) # ip address 192.168.21.1 255.255.255.0

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



En la Subinterfaz g0/1.23, se realiza la descripción correspondiente , se le asigna la Vlan 23 y se le asigna la primera dirección disponible de esta interfaz.

SINTAXIS:

R1#configure terminal

R1(config)# inter g0/1.23

R1(config-if) # Description LAN_Ingenieria

R1(config-if) # encapsulation dot1q 23

R1(config-if) # ip address 192.168.23.1 255.255.255.0

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

En la Subinterfaz g0/1.23, se realiza la descripción correspondiente , se le asigna la Vlan 99 y se le asigna la primera dirección disponible de esta interfaz.

SINTAXIS:

R1#configure terminal

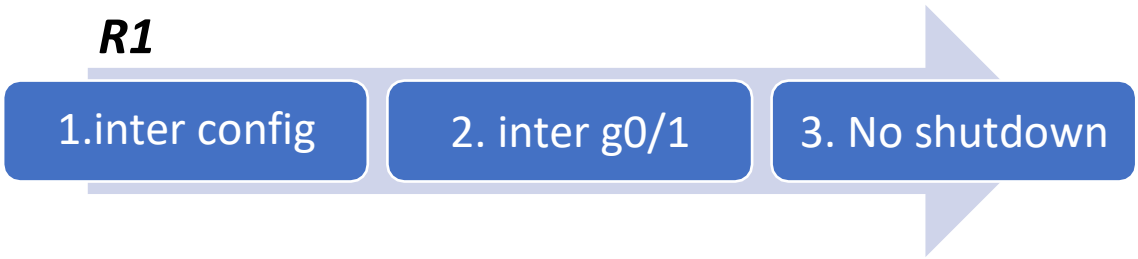
R1(config)# inter g0/1.99

R1(config-if) # Description LAN_Administracion

R1(config-if) # encapsulation dot1q 99

R1(config-if) # ip address 192.168.99.1 255.255.255.0

d. Activar la interfaz G0/1



R1#configure terminal

R1(config)# inter g0/1

R1(config)# 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:

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	S1#ping 192.168.99.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
S3	R1, dirección VLAN 99	192.168.99.1	S3#ping 192.168.99.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
S1	R1, dirección VLAN 21	192.168.21.1	S1#ping 192.168.21.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.21.1, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
S3	R1, dirección VLAN 23	192.168.23.1	S3#ping 192.168.23.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.23.1, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/5/11 ms

Parte 4:Configurar el protocolo de routing dinámico OSPF

Paso 1: Configurar OSPF en el R1.

a. Configurar OSPF área 0

```
R1(config)#router ospf 1
R1(config-router)#netwr
R1(config-router)#net
R1(config-router)#network 172.16.1.0 0.0.0.255 area 0
R1(config-router)#network 192.168.21.0 0.0.0.255 area 0
R1(config-router)#network 192.168.23.0 0.0.0.255 area 0
R1(config-router)#network 192.168.99.0 0.0.0.255 area 0
```

b. 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
```

c. Desactive la sumarización automática.

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

Paso 2: Configurar OSPF en el R2.

a. Configurar OSPF área 0

```
R2(config)#router ospf 1
R2(config-router)#networ
R2(config-router)#network 10.10.10.10 0.0.0.255 area 0
R2(config-router)#networ 172.16.1.0 0.0.0.255 area 0
R2(config-router)#networ 172.16.2.0 0.0.0.255 area 0
```

b. Establecer la interfaz LAN (loopback) como pasiva

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

c. Desactive la sumarización automática.

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

Paso 3: Configurar OSPF en el R3.

a. Configurar OSPF área 0

```
R3(config)#router ospf 1
R3(config-router)#network 172.16.2.0 0.0.0.255 area 0
R3(config-router)#network 192.168.4.0 0.0.0.255 area 0
R3(config-router)#network 192.168.5.0 0.0.0.255 area 0
R3(config-router)#network 192.168.6.0 0.0.0.255 area 0
```

b. 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

c. Desactive la sumarización automática.

R3(config-router)#no auto summary

Paso 4: Verificar la información de OSPF

Pregunta	Respuesta
¿Con qué comando se muestran la ID del proceso OSPF, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router?	Show ip Protocols Show ip ospf interface brief
¿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 | section

Parte 5:Implementar DHCP y NAT para IPV4.

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

a. Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas

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

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

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

c. 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

d. 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

```
ip dhcp excluded-address 192.168.21.1 192.168.21.20
ip dhcp excluded-address 192.168.23.1 192.168.23.20
!
ip dhcp pool ACCT
 network 192.168.21.0 255.255.255.0
 default-router 192.168.21.1
 dns-server 10.10.10.10
 domain-name ccna-sa.com
ip dhcp pool ENGNR
 network 192.168.23.0 255.255.255.0
 default-router 192.168.23.1
 dns-server 10.10.10.10
 domain-name ccna-sa.com
```

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

a. Crear una base de datos local con una cuenta de usuario (Nombre de Usuario:webuser,contraseña:cisco12345, Nivel de Privilegio:15).

   SINTAXIS:

   R2#configure terminal
   Enter configuration commands, one per line. End with CNTL/Z.
   R2(config)#username webuser privilege 15 secret cisco12345

b. Habilitar el servicio del servidor HTTP

   SINTAXIS:

   R2#configure terminal
   R2(config)#ip http server

c. Crear una NAT estática al servidor web.

   Se cambio la dirección global interna propuesta por el ejercicio debido a que no se encuentra en el rango del direccionamiento 209.165.200.232/29

   SINTAXIS:

   R2#configure terminal
   R2(config)# ip nat inside source static 10.10.10.10 209.165.200.237

d. Asignar la interfaz interna y externa para la NAT estática.

   SINTAXIS:

R2(config)#inter g0/0
R2(config-if)#ip nat outside
R2(config-if)#inter s0/0/0
R2(config-if)#ip nat inside
R2(config-if)#inter s0/0/1
R2(config-if)#ip nat inside

e. Configurar la NAT dinámica dentro de una ACL privada

SINTAXIS:

R2(config)#access-list 1 per
R2(config)#access-list 1 permit 192.168.21.00.0.0.255
R2(config)#access-list 1 permit 192.168.23.00.0.0.255
R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255

f. 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).**

SINTAXIS:

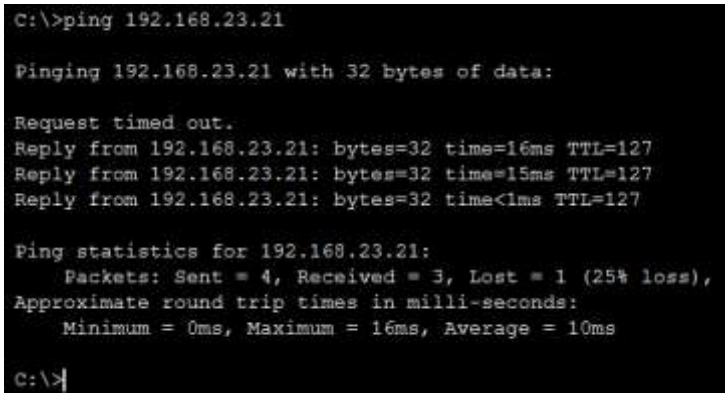
R2(config)#
R2(config)#ip nat pool INTERNET 209.165.200.233 209.165.200.236 netmask 255.255.255.248

g. 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

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**	No soporta el código http server. 

CONCLUSIONES

- Los comandos y protocolos utilizados en el informe y elaboración del escenario son útiles, para la simulación de una red, que incluye Dual-stak, Direccionamiento DHCP, conectividad, entre otras funcionalidades.
- Un LACP permite agrupar varios puertos físicos para formar un único canal lógico y tener una mayor disponibilidad de los servicios.
- La conectividad nos ayuda a la comunicación, envió y recepción de información.
- Un Tabla de enrutamiento tiene una Ip de Origen y Una de destino.
- El ospf es un protocolo de direccionamiento de tipo enlace-estado, desarrollado para las redes IP.

LINK ESCENARIOS PACKET TRACER

https://1drv.ms/u/s!Ag-0tHwwntlXuDI-N8F9skkRORVt?e=hBBu30 (Cisco, Configure NAT to Enable Communication Between Overlapping Networks, 2016)

BIBLIOGRAFIA

- Cisco. (23 de Agosto de 2005). Configuración de ejemplo para la autenticación en OSPF. Obtenido de https://www.cisco.com/c/es_mx/support/docs/ip/open-shortest-path-first-ospf/13697-25.html

- Cisco. (27 de octubre de 2011). Basic Router Configuration Using Cisco Configuration Professional. Obtenido de https://www.cisco.com/c/en/us/support/docs/cloud-systems-management/configuration-professional/111999-basic-router-config-ccp-00.html

- Cisco. (27 de octubre de 2011). Configuring LACP (802.3ad) Between a Catalyst 6500/6000 and a Catalyst 4500/4000. Obtenido de https://www.cisco.com/c/en/us/support/docs/lan-switching/etherchannel/19642-126.html

- Cisco. (24 de febrero de 2016). DHCPv6 using the Prefix Delegation Feature Configuration Example. Obtenido de https://www.cisco.com/c/en/us/support/docs/ip/ip-version-6-ipv6/113141-DHCPv6-00.html

- Cisco. (14 de octubre de 2016). Configure NAT to Enable Communication Between Overlapping Networks. Obtenido de https://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/200726-Configure-NAT-to-Enable-Communication-Be.html

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

- 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). 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

- 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#10g

Diplomado de Profundización CISCO: SOLUCIÓN DE DOS ESTUDIOS DE CASO BAJO EL USO DE TECNOLOGÍA CISCO

María Alejandra Polanco Andrade CC. 1022392030

Resumen – El presente trabajo desarrolla los dos escenarios propuestos por el tutor, donde se pone en práctica la temática vista como: Generalidades Networking, Mecanismos de Comunicación y acceso a la Red, Comunicaciones Sobre ethernet, Direccionamiento Ip y Subnetting, Comunicaciones en Capas superiores, enrutamiento estático, dinámico y conmutación, Vlans, Direccionamiento IP y ACL, NAT, PAT y Gestión de Equipos en Networking.

Abstract:

The present work develops the two scenarios proposed by the tutor, where the topic seen as: General Networking, Communication Mechanisms and Network access, Communications Over Ethernet, IP Addressing and Subnetting, Communications in higher Layers, static routing is put into practice , dynamic and switching, Vlans, IP Addressing and ACL, NAT, PAT and Equipment Management in Networking.

Palabras Clave: Networking, Direccionamiento Ip, NAT, Vlans.

I. INTRODUCCION

La comunicación es cada vez más ágil, más posible, más real, y es una de las funciones y habilidades dadas a través de las redes de datos y/o redes informáticas, teniendo en cuenta, que todo es un sistema comprendido a nivel hardware y software, bajo el concepto de emisor y receptor, permitiendo compartir recursos e información.

A medida de la evolución, evidenciamos diversos tipos de Red: LAN (Red de Área Local), PAN (Red de Área Personal), MAN (Red de área Metropolitana), WLAN (Red de área local inalámbrica), WAN (Red de área de gran alcance), entre otras. Aunque todas tiene la misma finalidad de interconectar, se diferencian en la escala o grado de alcance de la Red (como se evidencia en sus nombres).

La conectividad a través de la red depende o se despliega desde la configuración de los dispositivos activos, la conexión física (cableado estructurado), punto de red del usuario final, y es allí donde vamos a trabajar en la configuración y simulación de dos escenarios, poniendo en práctica todas las habilidades aprendidas y adquiridas.

Estas habilidades se enfocan en temas con sus comandos a utilizar como:

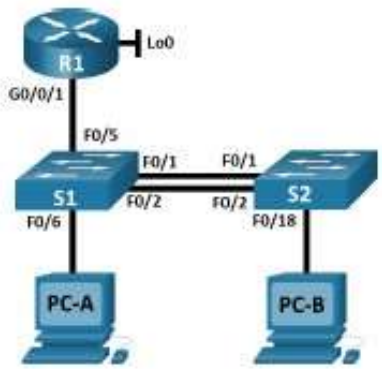
1. Contraseña al modo privilegiado: Tanto en Router y Switch´s: enable secret Contraseña.
2. Contraseña para acceder por Consola: Tanto en Router y Switch's, desde el modo config: line console 0 -> password contraseña -> login.
3. Encriptación de Contraseña: desde el modo config: service password-encryption.
4. Eliminar y/o Guardar la configuración de un Router y Switch´s: erase Startup-config // copy running-config startup-config.
5. Creación de Vlans, enrutamiento, Dual-stack, entre otros.

La lógica y el manejo de estos conceptos se hará necesario para lograr un éxito en los escenarios.

II. METODOLOGIA.

Se realiza un trabajo de dos escenarios, en la aplicación Packet Tracer, así:

ESCENARIO I



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

```
Router>enable
Router#erase startup-config
(confirm)
Router#reload
(confirm)
```

```
Switch> enable
Switch# erase startup-config
(confirmar)
Switch#delete vlan.dat
Switch#Reload
(confirmar)
```

Se configura la plantilla SDM para que admita IPV6.

```
Switch>enable
Switch# show sdm prefer
Switch# config terminal
Switch(config)# sdm prefer dual-ipv4-and-ipv6 default
Switch(config)#exit
Switch#Reload
Confirmar
Switch>enable
Switch#Show sdm prefer
```

Paso 2. Configurar R1.

```
Router>enable
Router#config t
Router (Config)#no ip domain-lookup
```

```
Router#config t
Router(config)# Hostname R1
R1(config)#
```

```
R1>enable
R1#config terminal
R1(config)#enable secret ciscoenpass
```

```
R1#config t
R1(config) #line con 0
R1(config-line) #password ciscoconpass
R1(config-line) #login
```

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

```
R1#config t
R1(config)# Username admin secret admin1pass
```

```
R1#config t
R1(config)# line vty  0 15
R1(config)# login local
```

```
R1#configure terminal
R1(config)#line vty 0 15
R 1(config-line) #transport input ssh
```

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

```
R1#configure terminal
R1(config)#banner motd "PROHIBIDO EL INGRESO DE
PERSONAL NO AUTORIZADO"
```

a. Habilitar el routing ipv6.

```
R1#configure terminal
R1(config)#ipv6 unicast-routing
```

b. Configurar interfaz G0/0/1 y subinterfaces

```
R1(config)#inter gigabitEthernet 0/1
R1(config)#inter gigabitEthernet 0/1.2
R1(config-subif) #encapsulation dot1Q 2
R1(config-subif) #description Bikes
R1(config-subif) #ip address 10.19.8.1 255.255.255.192
R1(config-subif) #ipv6 address 2001:db8:acad:a::1/64
R1(config-subif) #ipv6 address fe80::1 link-local
R1(config)#inter gigabitEthernet 0/1.3
R1(config-subif)#encapsulation dot1Q 3
R1(config-subif)#description Trikes
R1(config-subif)#ip address 10.19.8.65 255.255.255.224
R1(config-subif)#ipv6 address 2001:db8:acad:b::1/64
R1(config-subif)#ipv6 address fe80::1 link-local
R1(config)#inter gigabitEthernet 0/1.4
R1(config-subif)#encapsulation dot1Q 4
R1(config-subif)#description Management
R1(config-subif)#ip address 10.19.8.97 255.255.255.248
R1(config-subif)#ipv6 address 2001:db8:acad:c::1/64
R1(config-subif)#ipv6 address fe80::1 link-local
R1(config)#interface gigabitEthernet 0/1.6
R1(config-subif)#encapsulation dot1Q 6
R1(config-subif)#description Parking
R1(config-subif)#exit
R1(config)#inter gigabitEthernet 0/1
R1(config-if)#no shutdown
```

c. Configure el Loopback0 interface (Establezca la descripción, Establece la dirección IPv4, Establece la dirección IPv6, Establezca la dirección local de enlace IPv6 como fe80::1).

```
R1(config)#inter loopback 0
R1(config-if) #ip address 209.165.201.1 255.255.255.224
R1(config-if) #ipv6 address 2001:db8:acad:209::1/64
R1(config-if) #ipv6 address FE80::1 link-local
R1(config-if) #i Description Loopback_Nude
```

```
R1(config)#crypto key generate rsa
```

Paso 3. Configurar S1 Y S2

```
Switch>enable
Switch #config t
Switch (Config)#no ip domain-lookup

Switch1#config t
Switch1(config)# Hostname S1
S1(config)#

Switch2#config t
Switch2(config)# Hostname S2
S2(config)#

S1#config ter
S1(config)#ip domain-name ccna-lab.com

S2#config ter
S2(config)#ip domain-name ccna-lab.com

S1>enable
S1#config terminal
S1(config)#enable secret ciscoenpass

S2>enable
S2#config terminal
S2(config)#enable secret ciscoenpass

S1#config t
S1(config) #line con 0
S1(config-line) #password ciscoconpass
S1(config-line) #login

S2#config t
S2(config) #line con 0
S2(config-line) #password ciscoconpass
S2(config-line) #login

S1#config t
S1(config)# Username admin secret admin1pass

S1#config t
S1(config)# line vty  0 15
S1(config)# login local

S2#config t
S2(config)# line vty  0 15
S2(config)# login local

S1#configure terminal
S1(config)#line vty 0 15
S1(config-line) #transport input ssh

S2#configure terminal
S2(config)#line vty 0 15
S2(config-line) #transport input ssh

S1#configure terminal
S1(config)#service password-encryption

S2#configure terminal
S2(config)#service password-encryption

S1#configure terminal
S1(config)#banner motd "PROHIBIDO EL
INGRESO DE PERSONAL NO AUTORIZADO"

S2#configure terminal
S2(config)#banner motd "PROHIBIDO EL
INGRESO DE PERSONAL NO AUTORIZADO"

S1(config)#crypto key generate rsa
S2(config)#crypto key generate rsa
```

a. Configurar la interfaz de administración (SVI), Establecer la dirección IPv4 de capa 3 , Establezca la dirección local de enlace IPv6 como FE80: :98 para S1 y FE80: :99 para S2 , Establecer la dirección IPv6 de capa 3.

```
S1(config)#inter 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)#no Shutdown

S2(config)#inter 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::99 link-local
S2(config-if) #no Shutdown
```

b. Configuración del gateway predeterminado

Nota: Para IPV6 se deja dinámica, sin embargo, para los ping se recomienda poner una ipv6 gateway.

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

S2(config)# ip default-gateway 10.19.8.97
```

Parte 2: Configuración de la infraestructura de Red (Vlan, Trunking, EtherChannel).

Paso 1. Configuración Switch S1 y S2

```
S1(config)#vlan 2
S1(config-vlan)#name Vlan_Bikes
```

```
S1(config-vlan)#vlan 3
S1(config-vlan)#name Vlan_Trikes
S1(config-vlan)#vlan 4
S1(config-vlan)#name Vlan_management
S1(config-vlan)#vlan 5
S1(config-vlan)#name Vlan_Parking
S1(config-vlan)#vlan 6
S1(config-vlan)#name Vlan_Native
```

a. Crear troncos 802.1Q que utilicen la Vlan 6 nativa (Interfaces F0/1, F0/2 y F0/5).

```
S1(config)#inter fastEthernet 0/5
S1(config-if) #switchport trunk encapsulation dot1q
S1(config-if) #switchport mode trunk
S1(config-if) #switchport trunk native vlan 6
S1(config)#exit
S1(config)#int range fast 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
```

b. Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2 (Usar el protocolo LACP para la negociación).

```
S1(config)#int range fast 0/1-2
S1(config-if-range) #channel-group 1 mode active
S1(config-if-range) #inter port-channel 1
S1(config-if) #switchport trunk encapsulation dot1q
S1(config-if) #switchport mode trunk
S1(config-if) #switchport trunk native vlan 6
```

c. Configurar el puerto de acceso de host para VLAN 2 (interface F0/6)

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

d. Configurar la seguridad del puerto en los puertos de acceso (Permitir 3 direcciones MAC).

```
S1(config)#Inter Fa0/6
S1(config-if) #switchport port-security
        S1(config-if) #switchport port-security
        maximum 3
```

e. Proteja todas las interfaces no utilizadas (Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar)

```
S1(config)#interface range fastEthernet 0/3-4,
fastEthernet 0/7-24, gigabitEthernet 0/1-2
S1(config-if-range) #switchport mode access
S1(config-if-range) #switchport access vlan 5
S1(config-if-range) #description SIN USAR
S1(config-if-range) #shutdown
```

f. En el Switch 2 - Configurar el puerto de acceso del host para la VLAN 3(interfaz F0/18).

```
S2(config)#inter fast 0/18
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 3
S2(config-if)#no shutdown
```

g. Configure port-security en los access ports (Permite 3 MAC addresses).

```
S2(config)#Inter Fa0/18
S2(config-if) #switchport port-security
S2(config-if) #switchport port-security
maximum 3
```

h. Asegure todas las interfaces no utilizadas (Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar).

```
S2(config)# interface range fastEthernet 0/3-17,
fastEthernet 0/19-24, gigabitEthernet 0/1-2
S2(config-if-range) #switchport mode access
S2(config-if-range) #switchport access vlan 5
S2(config-if-range) #description SIN USAR
S2(config-if-range) #shutdown
```

Parte 3. Configurar soporte host.

Paso 1: Configuración R1.

a. Configure Default Routing (Crear rutas predeterminadas para IPv4 e IPv6 que dirijan el tráfico a la interfaz Loopback 0).

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

b. 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)

VLAN	Network	Excluidos	Utilizable

		DHCP	
Vlan 2 Bikes	10.19.8.0/26	10.19.8.1-10.19.8.52	10.19.8.53-10.19.8.62
Vlan 3 Trikes	10.19.8.64/27	10.19.8.65-10.19.8.84	10.19.8.85-10.19.8.94

R1(config)#ip dhcp excluded-address 10.19.8.1 10.19.8.52
R1(config)#ip dhcp pool Vlan2_B
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

c. Configurar DHCP IPv4 para VLAN 3 (Cree un grupo DHCP para VLAN 3, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio ccna-b.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del Router para la subred involucrada).

R1(config)#ip dhcp excluded-address 10.19.8.65 10.19.8.84
R1(config)#ip dhcp pool Vlan3_T
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

Paso2. Configurar los Servidores

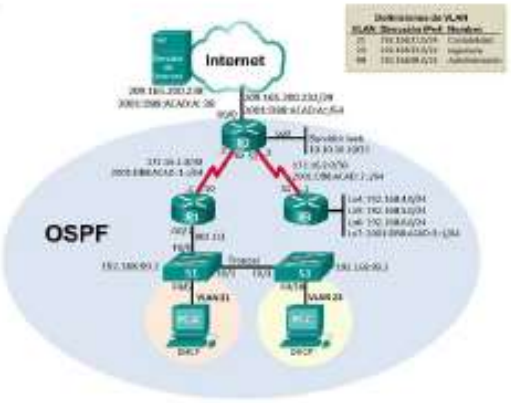
a. PC-A

PC-A Network Configuration	
Descripción	*Direccionamiento Equipo A*
Dirección física	*0004.9AAA.1997*
Dirección IP	*10.19.8.53*
Máscara de subred	*255.255.255.192*
Gateway predeterminado	*10.19.8.1*
Gateway predeterminado IPv6	*FE80::1*

b. PC-B

PC-B Network Configuration	
Descripción	*Direccionamiento Equipo B*
Dirección física	*0001.C9AD.23AD*
Dirección IP	*10.19.8.85*
Máscara de subred	*255.255.255.224*
Gateway predeterminado	*10.19.8.65*
Gateway predeterminado IPv6	*FE80::1*

ESCENARIO II



Configurar los parámetros básicos de los dispositivos

Paso 1. Configurar la computadora de Internet

En el siguiente paso, veremos las tareas de configuración del servidor de Internet incluyen lo siguiente, así:

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
Gateway predeterminado IPv6	2001:DB8:ACAD:2::1

- Esta incorrecta la puerta de enlace ya que es la Primera Ip disponible en la red, siendo, 209.165.200.233.
- El prefijo cubre la sesión 2001:DB8:ACAD:A, lo cual se debe cambiar el default Gateway propuesto por el Tutor.

Configurar R1

```
Router#config t
Router(config)# Hostname R1
R1(config)#
R1(config)#enable secret class
R1(config) #line con 0
R1(config-line) #password cisco
R1(config-line) #login
R1(config-line) #exit
R1(config)#line vty 0 15
R1(config-line) #password cisco
R1(config-line) #login
R1(config-line) #exit
R1(config)#service password-encryption
R1#configure terminal
R1(config)#banner motd " Se prohíbe el acceso no autorizado."
```

a. Interfaz S0/0/0 (Establezca la descripción , establecer la dirección IPv4 Consultar el diagrama de topología para conocer la información de direcciones, establecer la dirección IPv6 Consultar el diagrama de topología para conocer la información de direcciones , establecer la frecuencia de reloj en 128000, activar la interfaz).

```
R1#configure terminal
R1(config)#inter s0/0/0
R1(config-if) #description Conexión_R2
R1(config-if) #ip address 172.16.1.1
255.255.255.252
R1(config-if) #ip address 2001:DB8:ACAD:1::1/64
R1(config-if) # Clock rate 128000
R1(config-if) #no shutdown
```

b. Rutas predeterminadas (Configurar una ruta IPv4 predeterminada de S0/0/0, configurar una ruta IPv6 predeterminada de S0/0/0)

```
R1#configure terminal
R1(config)#inter s0/0/0
R1(config-if) #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

```
Router>enable
Router#config t
Router (Config)#no ip domain-lookup

Router#config t
Router(config)# Hostname R2
R2(config)#

R2>enable
R2#config terminal
R2(config)#enable secret class

R2#config t
R2(config) #line con 0
R2(config-line) #password cisco
R2(config-line) #login

R2#configure terminal
R2(config)#line vty 0 15
R2(config-line) #password cisco
R2(config-line) #login

R2#configure terminal
R2(config)#service password-encryption

R2(config)# ip http server
R2(config)# ip http secure-server
R2(config)# ip http authentication local

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

a. Interfaz S0/0/0 (Establecer la descripción, dirección ipv4 utilizando la primera dirección disponible en la subred, direccionamiento Ipv6, establecer la frecuencia de reloj en 128000, activar la interfaz)

```
R2#configure terminal
R2(config)#inter s0/0/0
R2(config-if) #description Conexión_R1
R2(config-if) #ip address 172.16.1.2
255.255.255.252
R2(config-if) #ip address 2001:DB8:ACAD:1::2/64
```

```
R2(config-if) # Clock rate 128000
R2(config-if) # no shutdown
```

b. Interfaz S0/0/1 (Establecer la descripción, dirección ipv4 utilizando la primera dirección disponible en la subred, direccionamiento Ipv6, establecer la frecuencia de reloj en 128000, activar la interfaz)

```
R2#configure terminal
R2(config)#inter s0/0/1
R2(config-if) #description Conexión_R3
R2(config-if) #ip address 172.16.2.2
255.255.255.252
R2(config-if) #ip address 2001:DB8:ACAD:2::2/64
R2(config-if) # Clock rate 128000
R2(config-if) # no shutdown
```

c. Interfaz G0/0 (simulación de Internet)(Establecer la descripción, dirección ipv4 utilizando la primera dirección disponible en la subred, direccionamiento Ipv6, establecer la frecuencia de reloj en 128000, activar la interfaz)

```
R2#configure terminal
R2(config)#inter gi 0/0
R2(config-if) #description
Conexion_Servidor_Internet
R2(config-if) #ip address 209.165.200.233
255.255.255.248
R2(config-if) #ip address 2001:DB8:ACAD:A::1/64
R2(config-if) # Clock rate 128000
R2(config-if) # no shutdown
```

d. Interfaz loopback 0 (servidor web simulado).

```
R2#configure terminal
R2(config)#inter loopback 0
R2(config-if) #description Servidor
R2(config-if) #ip address 10.10.10.10.
255.255.255.255
```

e. Ruta predeterminada

```
R2#configure terminal
R2(config)#inter G0/0
R2(config-if) #Ip route 0.0.0.0 0.0.0.0 s0/0/0
R2(config-if) #ipv6 route ::/0 G0/0
```

Paso 4: Configurar R3

```
Router>enable
Router#config t
Router (Config)#no ip domain-lookup

Router#config t
Router(config)# Hostname R3
R3(config)#

R3>enable
R3#config terminal
R3(config)#enable secret class

R3#config t
R3(config) #line con 0
R3(config-line) #password cisco
R3(config-line) #login

R3#configure terminal
R3(config)#line vty 0 15
R3(config-line) #password cisco
R3(config-line) #login

R3#configure terminal
R3(config)#service password-encryption

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

a. Interfaz S0/0/1 (Establecer la descripción, dirección ipv4 utilizando la primera dirección disponible en la subred, direccionamiento Ipv6, activar la interfaz).

```
R3#configure terminal
R3(config)#inter S0/0/1
R3(config-if) #description Conexion_R2
R3(config-if) #ip address 172.16.2.1
255.255.255.252
R3(config-if) #ip address 2001:DB8:ACAD:2::1/64
R3(config-if) # no shutdown
```

Interfaz loopback 4

Utilizamos la primera dirección ip disponible en la red.

```
R3#configure terminal
R3(config)#inter loopback 4
R3(config-if) #ip address 192.168.4.1 255.255.255.0
```

Interfaz loopback 5

Utilizamos la primera dirección ip disponible en la red.

```
R3#configure terminal
R3(config)#inter loopback 5
R3(config-if) #ip address 192.168.5.1 255.255.255.0
```

Interfaz loopback 6

Utilizamos la primera dirección ip disponible en la red.

```
R3#configure terminal
R3(config)#inter loopback 6
R3(config-if) #ip address 192.168.6.1 255.255.255.0
```

Interfaz loopback 7

Utilizamos direccionamiento ipv6 disponible en la red.

```
R3#configure terminal
R3(config)#inter loopback 7
R3(config-if) #ipv6 address 2001:FB8:ACAD:3::1/64
```

Se configura la ruta estática por defecto.

Paso 5:Configurar S1

```
Switch>enable
Switch#config t
Switch (Config)#no ip domain-lookup

Switch#config t
Switch(config)# Hostname S1
S1(config)#

S1>enable
S1#config terminal
S1(config)#enable secret class

S1#config t
S1(config) #line con 0
S1(config-line) #password cisco
S1(config-line) #login

S1#configure terminal
S1(config)#line vty 0 15
S1(config-line) #password cisco
S1(config-line) #login

S1#configure terminal
S1(config)#service password-encryption

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

Paso 5:Configurar el S3

```
Switch>enable
Switch#config t
Switch (Config)#no ip domain-lookup

Switch#config t
Switch(config)# Hostname S3
S3(config)#

S3>enable
S3#config terminal
S3(config)#enable secret class

S3#config t
S3(config) #line con 0
S3(config-line) #password cisco
S3(config-line) #login

S3#configure terminal
S3(config)#line vty 0 15
S3(config-line) #password cisco
S3(config-line) #login

S3#configure terminal
S3(config)#service password-encryption

S3#configure terminal
S3(config)#banner motd " Se prohíbe el acceso no autorizado."
```

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

Paso 1. Configurar S1

```
S1#configure terminal
S1(config)#vlan 21
S1(config)#name Accounting
S1(config)#vlan 23
S1(config)#name Engineering
S1(config)#vlan 99
S1(config)#name Management

S1#configure terminal
S1(config)#inter vlan 99
S1(config-if) #ip address 192.168.99.2 255.255.255.0
S1(config-if) # no shutdown

S1#configure terminal
S1(config)#Ip default-gateway 192.168.99.1
```

a. Forzar el enlace troncal en la interfaz F0/3, utilizando la Vlan 1 como Vlan Native.

```
S1#configure terminal
S1(config)#inter f0/3
S1(config-if) #switchport mode trunk
S1(config-if) #switchport trunk native vlan 1
```

b. Forzar el enlace troncal en la interfaz F0/5, utilizando la Vlan 1 como Vlan Native.

```
S1#configure terminal
S1(config)#inter f0/5
```

S1(config-if) #switchport mode trunk
S1(config-if) #switchport trunk native vlan 1

c. Configurar el resto de los puertos como puertos de acceso.

S1#configure terminal
S1(config)# inter range f0/1-2,f0/4,f0/6-24,g0/1-2
S1(config-if-range) # switchport mode access

d. Asignar F0/6 a la VLAN 21

S1#configure terminal
S1(config)# inter f0/6
S1(config-if) # switchport access vlan 21

e. Apagar todos los puertos sin usar.

S1#configure terminal
S1(config)# inter range f0/1-2, f0/4, f0/7-24, g0/1-2
S1(config-if-range) # shutdown

Paso 2:Configurar el S3

S3#configure terminal
S3(config)#vlan 21
S3(config)#name Accounting
S3(config)#vlan 23
S3(config)#name Engineering
S3(config)#vlan 99
S3(config)#name Management

a. Asignar la dirección IP de administración.

S3#configure terminal
S3(config)#inter vlan 99
S3(config-if) #ip address 192.168.99.3 255.255.255.0
S3(config-if) # no shutdown

b. Asignar el gateway predeterminado.

S3#configure terminal
S3(config)#Ip default-gateway 192.168.99.1

c. Forzar el enlace troncal en la interfaz F0/3, utilizando la Vlan 1 como Vlan Native.

S3#configure terminal
S3(config)#inter f0/3
S3(config-if) #switchport mode trunk
S3(config-if) #switchport trunk native vlan 1

d. Forzar el enlace troncal en la interfaz F0/5, utilizando la Vlan 1 como Vlan Native.

S3#configure terminal
S3(config)#inter f0/5
S3(config-if) #switchport mode trunk
S3(config-if) #switchport trunk native vlan 1

e. Configurar el resto de los puertos como puertos de acceso.

S3#configure terminal
S3(config)# inter range f0/1-2, f0/4-24, g0/1-2
S3(config-if-range) # switchport mode access

f. Asignar F0/18 a la VLAN 23

S3#configure terminal
S3(config)# inter f0/18
S3(config-if) # switchport access vlan 23

g. Apagar todos los puertos sin usar.

S3#configure terminal
S3(config)# inter range f0/1-2, f0/4-17, f0/19--24, g0/1-2
S3(config-if-range) # shutdown

Paso 3:Configurar R1

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

En la Subinterfaz g0/1.21, se realiza la descripción correspondiente , se le asigna la Vlan 21 y se le asigna la primera dirección disponible de esta interfaz.

R1#configure terminal
R1(config)# inter g0/1.21
R1(config-if) # Description LAN_Contabilidad
R1(config-if) # encapsulation dot1q 21
R1(config-if) # ip address 192.168.21.1 255.255.255.0

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

En la Subinterfaz g0/1.23, se realiza la descripción correspondiente , se le asigna la Vlan 23 y se le asigna la primera dirección disponible de esta interfaz.

R1#configure terminal
R1(config)# inter g0/1.23
R1(config-if) # Description LAN_Ingenieria
R1(config-if) # encapsulation dot1q 23
R1(config-if) # ip address 192.168.23.1 255.255.255.0

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

En la Subinterfaz g0/1.23, se realiza la descripción correspondiente , se le asigna la Vlan 99 y se le asigna la primera dirección disponible de esta interfaz.

R1#configure terminal
R1(config)# inter g0/1.99
R1(config-if) # Description LAN_Administracion
R1(config-if) # encapsulation dot1q 99
R1(config-if) # ip address 192.168.99.1 255.255.255.0

```
R1#configure terminal
R1(config)# inter g0/1
R1(config)# No shutdown
```

Parte 4:Configurar el protocolo de routing dinámico OSPF

Paso 1:Configurar OSPF en el R1.

a. Configurar OSPF área 0

```
R1(config)#router ospf 1
R1(config-router)#netwr
R1(config-router)#net
R1(config-router)#network 172.16.1.0 0.0.0.255 area 0
R1(config-router)#network 192.168.21.0 0.0.0.255 area 0
R1(config-router)#network 192.168.23.0 0.0.0.255 area 0
R1(config-router)#network 192.168.99.0 0.0.0.255 area 0
```

b. 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
```

c. Desactive la sumarización automática.

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

Paso 2: Configurar OSPF en el R2.

a. Configurar OSPF área 0

```
R2(config)#router ospf 1
R2(config-router)#networ
R2(config-router)#network 10.10.10.10 0.0.0.255 area 0
R2(config-router)#networ 172.16.1.0 0.0.0.255 area 0
R2(config-router)#networ 172.16.2.0 0.0.0.255 area 0
```

b. Establecer la interfaz LAN (loopback) como pasiva

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

c. Desactive la sumarización automática.

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

Paso 3: Configurar OSPF en el R3.

a. Configurar OSPF área 0

```
R3(config)#router ospf 1
R3(config-router)#network 172.16.2.0 0.0.0.255 area 0
R3(config-router)#network 192.168.4.0 0.0.0.255 area 0
R3(config-router)#network 192.168.5.0 0.0.0.255 area 0
R3(config-router)#network 192.168.6.0 0.0.0.255 area 0
```

b. 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
```

c. Desactive la sumarización automática.

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

Parte 5:Implementar DHCP y NAT para IPV4.

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

a. Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas

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

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

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

c. 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
```

d. 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
```

```
ip dhcp excluded-address 192.168.21.1 192.168.21.20
ip dhcp excluded-address 192.168.23.1 192.168.23.20
!
ip dhcp pool ADMIN
 network 192.168.21.0 255.255.255.0
 default-router 192.168.21.1
 dns-server 10.10.10.10
 domain-name ccna-sa.com
ip dhcp pool ENGNR
 network 192.168.23.0 255.255.255.0
 default-router 192.168.23.1
 dns-server 10.10.10.10
 domain-name ccna-sa.com
```

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

a. Crear una base de datos local con una cuenta de usuario (Nombre de Usuario:webuser,contraseña:cisco12345, Nivel de Privilegio:15).

R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#username webuser privilege 15 secret cisco12345

b. Habilitar el servicio del servidor HTTP

R2#configure terminal
R2(config)#ip http server

c. Crear una NAT estática al servidor web.

Se cambio la dirección global interna propuesta por el ejercicio debido a que no se encuentra en el rango del direccionamiento 209.165.200.232/29

R2#configure terminal
R2(config)# ip nat inside source static 10.10.10.10 209.165.200.237

d. Asignar la interfaz interna y externa para la NAT estática.

R2(config)#inter g0/0
R2(config-if)#ip nat outside
R2(config-if)#inter s0/0/0
R2(config-if)#ip nat inside
R2(config-if)#inter s0/0/1
R2(config-if)#ip nat inside

e. Configurar la NAT dinámica dentro de una ACL privada

R2(config)#access-list 1 per
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

f. Defina el pool de direcciones IP públicas utilizables (Nombre del Conjunto: INTERNET, El conjunto de direcciones incluye: 209.165.200.225 – 209.165.200.228).

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

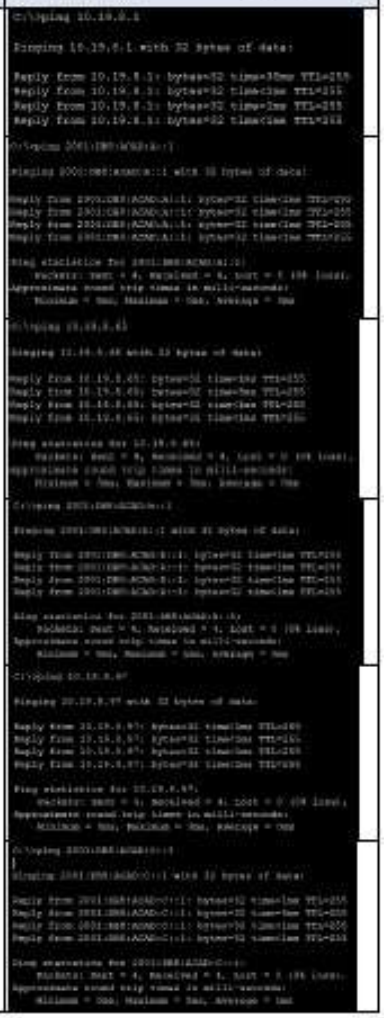
g. Definir la traducción de NAT dinámica.

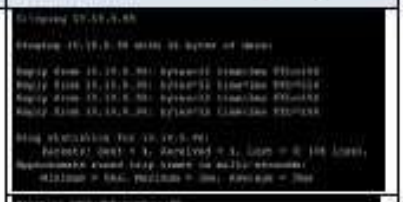
R2(config)#ip nat inside source list 1 pool INTERNET

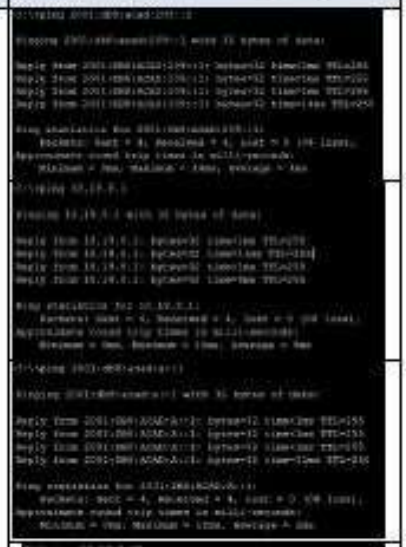
III. RESULTADOS

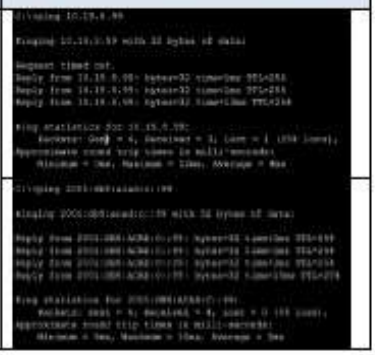
ESCENARIO I

Parte 1. Probar y verificar la conectividad de extremo a extremo

Desde	Resultados de ping
PC-A	

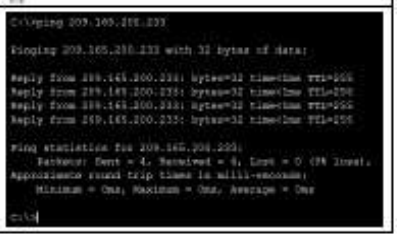
Desde	Resultados de ping
	
	
	
	
	
	
	
PC-B	

Desde	Resultados de ping
	
	
	
	
	
	
	

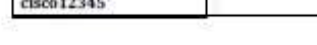
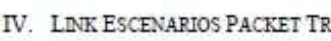
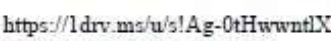
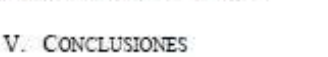
Desde	Resultados de ping
	

ESCENARIO II

Parte 1. Verificar la conectividad de la red.

Desde	Dirección IP	Resultados de ping
R1	172.16.1.2	
R2	172.16.2.1	
PC de Internet	209.165.200.233	

Parte 2. Verificar la conectividad de la red

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

Parte 3. Verificar la información de OSPF

Pregunta	Respuesta
¿Con qué comando se muestran la ID del proceso OSPF, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router?	Show ip Protocols Show ip ospf interface brief
¿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 | section

Parte 4. Verificar el protocolo DHCP y la NAT estática

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**	No soporta el código http server.  Request Timeout

IV. LINK ESCENARIOS PACKET TRACE

https://1drv.ms/u/s!Ag-0tHwwntlXuDI-N8F9skkRORVt?e=hBBu30

V. CONCLUSIONES

- Los comandos y protocolos utilizados en el informe y elaboración del escenario son útiles, para la simulación de una red, que incluye Dual-stak, Direccionamiento DHCP, conectividad, entre otras funcionalidades.

- Un LACP permite agrupar varios puertos físicos para formar un único canal lógico y tener una mayor disponibilidad de los servicios.
- La conectividad nos ayuda a la comunicación, envió y recepción de información.
- Un Tabla de enrutamiento tiene una Ip de Origen y Una de destino.
- El ospf es un protocolo de direccionamiento de tipo enlace-estado, desarrollado para
las redes IP.

VI. REFERENCIAS BIBLIOGRÁFICAS.

- Cisco. (23 de Agosto de 2005). Configuración de ejemplo para la autenticación en OSPF. Obtenido de https://www.cisco.com/c/es_mx/support/docs/ip/open-shortest-path-first-ospf/13697-25.html
- Cisco. (27 de octubre de 2011). Basic Router Configuration Using Cisco Configuration Professional. Obtenido de https://www.cisco.com/c/en/us/support/docs/cloud-systems-management/configuration-professional/111999-basic-router-config-ccp-00.html
- Cisco. (27 de octubre de 2011). Configuring LACP (802.3ad) Between a Catalyst 6500/6000 and a Catalyst 4500/4000. Obtenido de https://www.cisco.com/c/en/us/support/docs/lan-switching/etherchannel/19642-126.html
- Cisco. (24 de febrero de 2016). DHCPv6 using the Prefix Delegation Feature Configuration Example. Obtenido de https://www.cisco.com/c/en/us/support/docs/ip/ip-version-6-ipv6/113141-DHCPv6-00.html
- Cisco. (14 de Octubre de 2016). Configure NAT to Enable Communication Between Overlapping Networks. Obtenido de https://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/200726-Configure-NAT-to-Enable-Communication-Be.html
- UNAD (2017). Configuración de Switches y Routers [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgL9QChD1m9EuGqC
- 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). 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
- 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