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

YESID ARLEY MARROQUÍN RUÍZ

JOSÉ IGNACIO CARDONA
TUTOR

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA

INGENIERIA DE SISTEMAS

BOGOTÁ

2020

NOTAS DE ACEPTACION

_____

_____

_____

_____

_____

_____

_____
Firma de presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

Bogotá, 28 de noviembre de 2020

AGRADECIMIENTOS

Quiero agradecer principalmente a Dios y mi madre que están en el cielo guiándome y acompañándome en este camino para culminar con éxito este trabajo, me hicieron sentir fuerte y motivado y me dieron el don de encaminar una vida llena de aprendizajes para hoy alcanzar un logro profesional.

Además, quiero reconocer a mi esposa, Andrea Roncancio quien estuvo a mi lado en este proceso dándome fortaleza, consejos y apoyo que también fueron fundamentales para la elaboración del trabajo.

Por último, agradezco a todos los docentes de la Universidad Abierta y a distancia UNAD que nos guiaron y acompañaron en este proceso, entregándonos su tiempo, dedicación y conocimientos muy necesarios para poder cumplir y lograr este objetivo tan importante de ser profesionales.

INDICE GENERAL

INDICE DE FIGURAS

INDICE DE TABLAS

1. GLOSARIO

VLAN: Acrónimo de virtual LAN (red de área local virtual), es un método para crear redes lógicas independientes dentro de una misma red física.

GATEWAY: puerta de enlace o pasarela, es un dispositivo dentro de una red de comunicaciones, que permite a través de sí mismo, acceder a otra red.

NTP: Network Time Protocol es un protocolo de Internet para sincronizar los relojes de los sistemas informáticos a través del enrutamiento de paquetes en redes con latencia variable.

OSPF: Open Shortest Path First (OSPF), Abrir el camino más corto primero en español, es un protocolo de red para encaminamiento jerárquico de pasarela interior o Interior Gateway Protocol (IGP), que usa el algoritmo Dijkstra, para calcular la ruta más corta entre dos nodos.

TRUNK: Es una configuración de canal para puertos de switch que estén en una red Ethernet, que posibilita que se pueda pasar varias VLAN por un único link.

LOOPBACK: Es una dirección especial que los hosts utilizan para dirigir el tráfico hacia ellos mismos. La dirección de loopback crea un método de acceso directo para las aplicaciones y servicios TCP/IP que se ejecutan en el mismo dispositivo para comunicarse entre sí.

HOST: Es cualquier computadora o máquina conectada a una red mediante un número de IP definido y un dominio, que ofrece recursos, información y servicios a sus usuarios.

2. RESUMEN

Para esta actividad la cual es una prueba de habilidades prácticas se desarrollan dos escenarios propuestos que buscan identificar el grado de desarrollo de competencias y habilidades adquiridas comprensión y solución de problemas relacionados con diversos aspectos de Networking.

En el primer escenario se configuran equipos de una red pequeña utilizando router, switch y host los cuales se configuran con direccionamiento IPv4 e IPv6 y VLAN para luego analizar y verificar la conectividad en este tipo de redes, la verificación del correcto funcionamiento se realizar utilizando el protocolo ping.

En el segundo escenario también se configura una red pequeña pero se configura el protocolo de enrutamiento OSPF, DHCP, NAT, ACL, y NTP creando una red más robusta y segura, se desarrolla en entorno simulado con el software Packet Tracert.

PALABRAS CLAVE: PACKET TRACERT, PING, NETWORKING, INTERFACE, ROUTER, SWITCH, VLAN.

3. ABSTRACT

In the present work, a scenario based on a network topology proposed as a test of skills is developed, it is composed of several network devices which are a Cisco 4321 router, two Cisco 3560 switches and two hosts. All devices are configured and interconnected by simulated UTP cable connections as transmission media. Using the Packet Tracersoftware that Cisco offers us as a tool to practice what we have learned in this course, packet routing, equipment security configurations and troubleshooting processes are verified and analyzed for problem solving. For this simulation, the main configurations used are IPv4 and IPv6 addressing, VLAN creation and routing and configuration of an etherchannel with port security. Developing this practice means acquiring the knowledge and skills that the labor market demands to understand how a network works and to be able to diagnose connectivity and maintenance problems.

KEYWORKS: PACKET TRACERT, PING, NETWORKING, INTERFACE, ROUTER, SWITCH, VLAN.

4. INTRODUCCIÓN

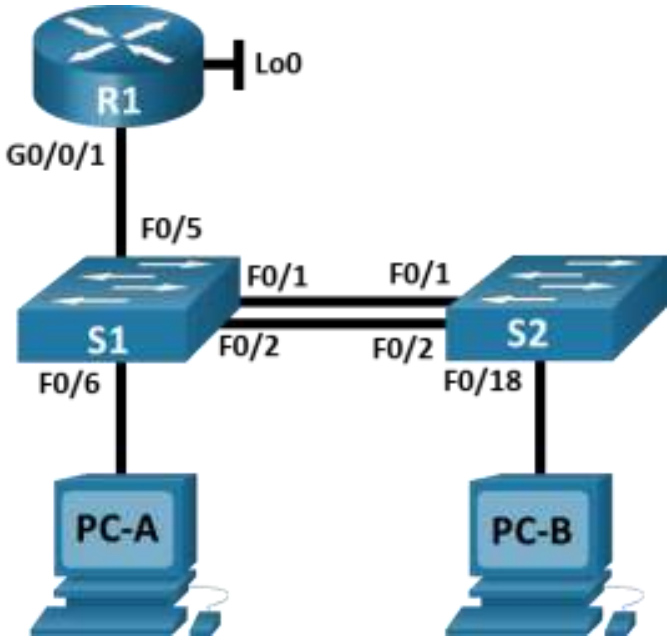
El desarrollo de este diplomado de profundización en la plataforma Cisco nos da la oportunidad de adquirir los conocimientos y practicas necesarias en el mantenimiento y construcción de redes de comunicaciones. El diplomado se basa en investigación y prácticas simuladas en el software Packet Tracer de la plataforma Cisco donde se permite identificar cada uno de los elementos que componen una red, los esquemas de direccionamiento y su importancia en las capas de comunicación, protocolos de ruteo y su importancia y funcionamiento en la red.

Se desarrollan dos escenarios con diferentes topologías de red donde se conectan y configuran los equipos en el software Packet Tracert, el cual nos permite también conocer una imagen real de cada equipo con sus interfaces permitiendo una mejor comprensión de la topología ya que así es como encontraremos los escenarios de red en la vida real.

Cada dispositivo de la red es configurado por línea de comandos utilizando naturalmente lo aprendido en el estudio de cada capítulo, analizando el comportamiento de cada equipo, la funcionalidad de cada protocolo configurado y como se procesa y transporta la información entre dispositivos. Para confirmar el correcto funcionamiento y configuraciones se desarrollan pruebas de conectividad entre dispositivos y host en el entorno de simulación Packet Tracer principalmente usando el protocolo ping que nos ayuda a confirmar la comunicación y alcanzabilidad en una red.

5. ESCENARIO 1

Figura 1. Topología de Red Escenario 1



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

Figura 2. Simulación del escenario 1 en Packet Tracert

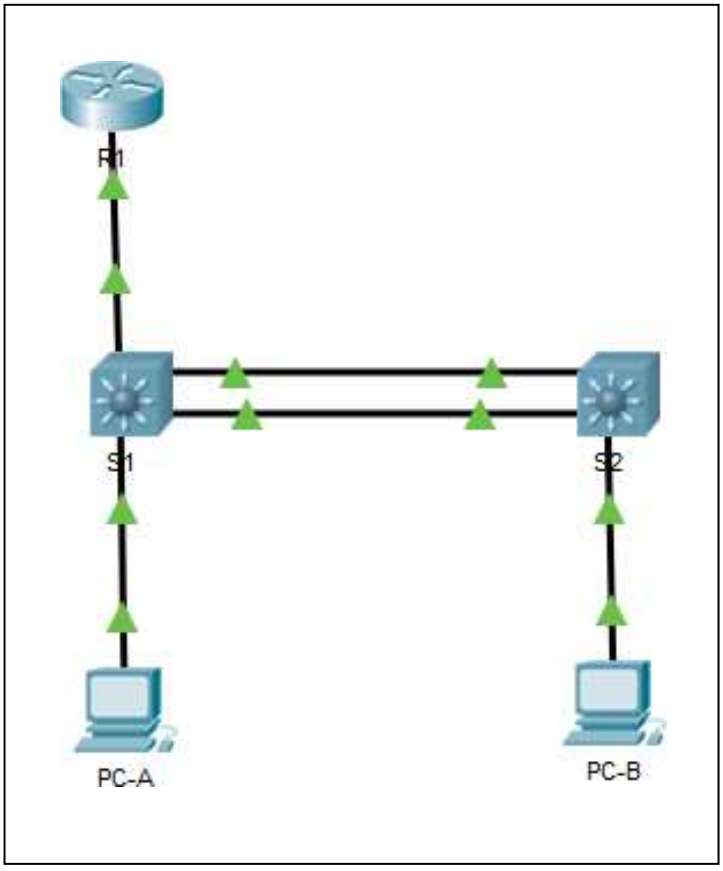


Tabla 1. Asignación de Nombres de VLAN

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

Se recomienda siempre poner un nombre a las vlan para identificar en una red el servicio que se transporta por cada una de ellas.

Tabla 2. Asignación de direcciones IP para los dispositivos

Dispositivo / interface	Dirección IP / Prefijo	Puerta de enlace predeterminada
R1 G0/0/1.2	10.19.8.1 /26	No corresponde
	2001:db8:acad:a: :1 /64	No corresponde
R1 G0/0/1.3	10.19.8.65 /27	No corresponde
	2001:db8:acad:b: :1 /64	No corresponde
R1 G0/0/1.4	10.19.8.97 /29	No corresponde
	2001:db8:acad:c: :1 /64	No corresponde
R1 G0/0/1.6	No corresponde	No corresponde
R1 Loopback0	209.165.201.1 /27	No corresponde
	2001:db8:acad:209: :1 /64	No corresponde
S1 VLAN 4	10.19.8.98 /29	10.19.8.97
	2001:db8:acad:c: :98 /64	No corresponde
	fe80: :98	No corresponde
S2 VLAN 4	10.19.8.99 /29	10.19.8.97
	2001:db8:acad:c: :99 /64	No corresponde
	fe80: :99	No corresponde
PC-A NIC	Dirección DHCP para IPv4	DHCP para puerta de enlace predeterminada IPv4
	2001:db8:acad:a: :50 /64	fe80::1
PC-B NIC	DHCP para dirección IPv4	DHCP para puerta de enlace predeterminada IPv4
	2001:db8:acad:b: :50 /64	fe80::1

Los dispositivos de red deben tener configurada una dirección Ip para que funcione el protocolo TCP/IP, para la práctica se utiliza direccionamiento IPv4 e IPv6.

6. Inicializar y Recargar y Configurar aspectos basicos de los dispositivos

6.1 Inicializar y volver a cargar el router y el switch

En el diseño del primer escenario de red se seleccióna un router cisco 4321, dos switch cisco 3560 y dos equipos host. Al ingresar al router se ingresa al modo EXEC privilegiado con el comando **enable**, luego se elimina la configuración de inicio de la memoria de acceso no volátil NVRAM con el comando **erase startup-config**, allí el router pide confirmar esta acción, luego de confirmar se reinicia el router con el comando **reload**. Esto es recomendado al iniciar la configuración de un dispositivo ya que este puede tener configuraciones anteriores que generen problemas en mi red e impidan el corecto funcionamiento.

Router 1

```
Router>enable
Router# erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Router#reload
Proceed with reload? [confirm]
```

Luego se realiza el proceso en cada uno de los switch, primero se ingresa al modo EXEC privilegiado con el comando **enable**, luego se elimina el archivo con vlan creadas anteiormente en el switch con el comando **delete vlan.dat** y luego se elimina la configuración de inicio de la memoria de acceso no volátil NVRAM con el comando **erase startup-config**, allí el router pide confirmar esta acción, luego de confirmar se reinicia el router con el comando reload.

Switch 1

```
Switch>enable
Switch#delete vlan.dat
Delete filename [vlan.dat]?
Delete flash:/vlan.dat? [confirm]
Switch# erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Switch#reload
Proceed with reload? [confirm]
```

Switch 2

Switch>enable
Switch#delete vlan.dat
Delete filename [vlan.dat]?
Delete flash:/vlan.dat? [confirm]
Switch# erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Switch#reload
Proceed with reload? [confirm]

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

Por defecto la plantilla SDM de los switch no admite IPv6, generalmente viene habilitada la plantilla default y debemos legir la plantilla adecuada de acuerdo a la utilización que se va a dar al equipo. Para confirmar que plantilla tiene habilitada el switch se ingresa al modo EXEC privilegiado y se da el comando **show sdm prefer**, para que el switch admita IPv6 se habilita la plantilla adecuada ingresando al modo de configuración global con el comando **configure terminal**, luego se aplica el comando **sdm prefer dual-ipv4-and-ipv6 default**, al aplicarlo se muestra un mensaje informando que se debe reiniciar el switch para que tome los cambios, se procede a reiniciar con el comando **reload**, luego de reiniciar se confirma con el comando **show sdm prefer** y aparece la nueva plantilla habilitada.

Nota: Se trabaja con switch cisco C3560 ya que ni el switch 2950 ni el switch 2960 tienen esta opción de habilitar plantilla que soporte IPv6 en Packet tracert.

Switch 1

Switch>enable

Switch#show sdm prefer

Switch#configure terminal

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

Changes to the running SDM preferences have been stored, but cannot take effect until the next reload.

Use 'show sdm prefer' to see what SDM preference is currently active.

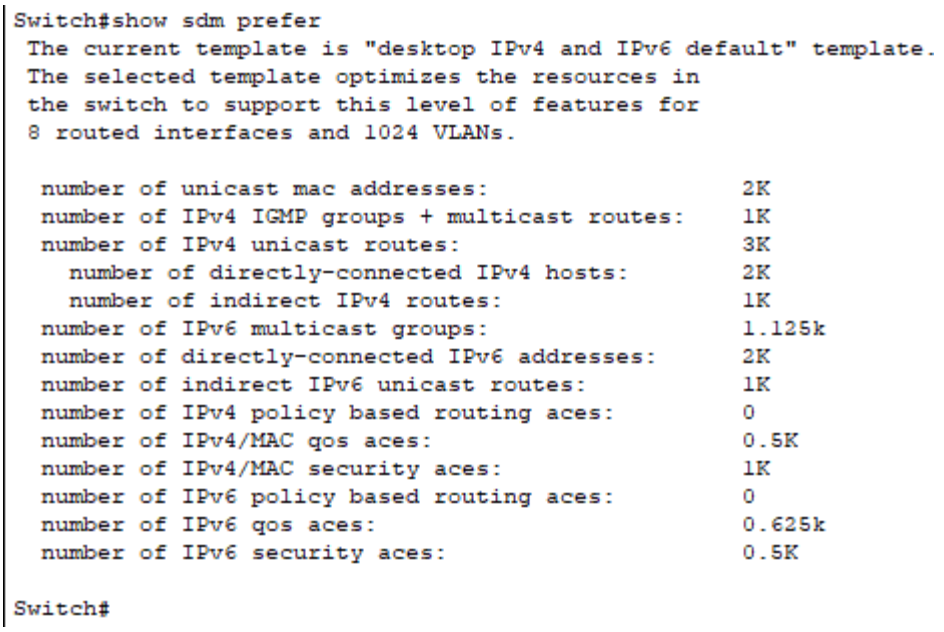
Switch(config)#exit

Switch#reload

Switch>enable

Switch#show sdm prefer

Figura 3. Verificación de plantilla SDM en switch 1



```
Switch#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

Switch#
```

Switch 2

Switch>enable

Switch#show sdm prefer

Switch#configure terminal

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

Changes to the running SDM preferences have been stored, but cannot take effect until the next reload.

Use 'show sdm prefer' to see what SDM preference is currently active.

Switch(config)#exit

Switch#reload

Switch>enable

Switch#show sdm prefer

Figura 4. Verificación de plantilla SDM en switch 1

```
Switch#
Switch#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

Switch#
```

6.2 Configuración de router 1

Tabla 3. Tareas de configuración realizadas en router 1

Tarea	Especificación
Desactivar la búsqueda DNS	Router#configure terminal Router(config)#no ip domain-lookup Router(config)# Se deben ingresar los comandos de configuración desde modo configuración global al cual se accede con **configure terminal**, luego el comando **no ip domain-lookup** desactiva la traducción de nombres a dirección del dispositivo, se ahorra tiempo cuando se escribe mal un comando y el dispositivo no tratara de traducirlo.

Tarea	Especificación
Nombre del router	Router(config)#hostname R1 Se debe cambiar el nombre de cada dispositivo usando el comando **hostname** para identificarlo en la red fácilmente.
Nombre de dominio	R1(config)#ip domain name ccna-lab.com Este comando define un nombre de dominio predeterminado que el IOS del dispositivo utiliza para completar los nombres del host incompetentes.
Contraseña cifrada para el modo EXEC privilegiado	R1(config)#enable secret ciscoenpass Este comando proporciona mayor seguridad a la contraseña de enable ya que la encripta con MD5.
Contraseña de acceso a la consola	R1(config)#line console 0 R1(config-line)#password ciscoconpass R1(config-line)#login R1(config-line)#exit En este paso lo que se hace es configurar un password que debe escribir todo aquel que trate de acceder por el puerto de consola al dispositivo.
Establecer la longitud mínima para las contraseñas	R1(config)#security passwords min-length 10 Con este comando se establece una longitud mínima para las contraseñas de 10 caracteres, esto da mayor seguridad para que no se usen contraseñas cortas.
Crear un usuario administrativo en la base de datos local	R1(config)#username admin password admin1pass En este paso lo que se hizo fue crear un usuario y password en la base de datos local que es alterno al password de vty y consola si se especifica para usarse.

Tarea	Especificación
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	R1(config)#line vty 0 4 R1(config-line)#login local En este paso se habilita el acceso por las líneas vty las cuales permiten el acceso a un dispositivo cisco a través de telnet o ssh. Por lo general un dispositivo cisco tiene 16 lineas vty. Al escribir el comando **login local** se le indica al router que ya no le haga caso al password configurado en el line vty sino que busque el usuario y password de la base de datos local creado en el paso anterior.
Configurar VTY solo aceptando SSH	R1(config)#line vty 0 4 R1(config-line)#transport input ssh R1(config-line)#exit Con este commando **transport input ssh** le decimos al router que solamente permita conexiones con ssh la cual es la más recomendada para usarse porque es más segura que telnet.
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption Este commando aplica un cifrado básico a los password que se encuentren sin encriptar.
Configure un MOTD Banner	R1(config)# banner motd # Prohibido el acceso sin autorizacion a este dispositivo!# Es importante configurar este mensaje en cada dispositivo y sirve para notificaciones legales y advertencias para todo aquel que se conecte al dispositivo.
Habilitar el routing IPv6	R1(config)#ipv6 unicast-routing Por defecto IPv6 esta desactivado en un dispositivo cisco y se aplica este comando para activarlo en el router.

Tarea	Especificación
Configurar interface G0/0/1 y subinterfaces	R1(config)#interface gigabitEthernet 0/0/1 R1(config-if)#description Conexion_Switch R1(config-if)#no shutdown R1(config-if)#interface gigabitEthernet 0/0/1.2 R1(config-subif)#description Vlan_2_Bikes R1(config-subif)#encapsulation dot1Q 2 R1(config-subif)#ip address 10.19.8.1 255.255.255.192 R1(config-subif)#ipv6 address fe80::1 link-local R1(config-subif)#ipv6 address 2001:db8:acad:a::1/64 R1(config-subif)#interface gigabitEthernet 0/0/1.3 R1(config-subif)#description Vlan_3_Trikes R1(config-subif)#encapsulation dot1Q 3 R1(config-subif)#ip address 10.19.8.65 255.255.255.224 R1(config-subif)#ipv6 address fe80::1 link-local R1(config-subif)#ipv6 address 2001:db8:acad:b::1/64 R1(config-if)#interface gigabitEthernet 0/0/1.4 R1(config-subif)#description Vlan_4_Management R1(config-subif)#encapsulation dot1Q 4 R1(config-subif)#ip address 10.19.8.97 255.255.255.248 R1(config-subif)#ipv6 address fe80::1 link-local R1(config-subif)#ipv6 address 2001:db8:acad:c::1/64 R1(config-subif)#interface gigabitEthernet 0/0/1.6 R1(config-subif)#description Vlan_6_Nativa R1(config-subif)#encapsulation dot1Q 6 R1(config-subif)#exit R1(config)# En este paso se configuran varias subinterfaces, primero se debe activar la interface física en este caso Ge 0/0/1 para que suban las subinterfaces creadas.

Tarea	Especificación
	Luego a cada subinterface se le da una descripción para identificarlas y se ponen las subinterfaces con el número de vlan tal que coincida con las vlan que se crearan en los switches más adelante. Luego en cada subinterface se configuran los direccionamientos IPv4, IPv6 y una dirección IPv6 link-local la cual permite que un dispositivo se comunique con otros dispositivos con IPv6 habilitado en el mismo enlace y solo en ese enlace.
Configure el Loopback0 interface	R1(config)#interface loopback 0 R1(config-if)#description loopback_Pruebas 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)#exit R1(config)# La interface loopback es una interface lógica interna del router. Esta no se asigna a un puerto físico y, por lo tanto, nunca se puede conectar a otro dispositivo, la interface loopback es útil para pruebas.
Generar una clave de cifrado RSA	R1(config)#crypto key generate rsa general-keys modulus 1024 En este paso se generan las claves secretas unidireccionales para que el router encripte el tráfico SSH. La clave se utiliza para encriptar y descifrar datos. Para crear esta clase de encriptación se usa este comando donde el modulo determina el tamaño de la clave.

6.3. Configuración de switch 1

Tabla 4. Tareas de configuración realizadas en switch 1

Tarea	Especificación
Desactivar la búsqueda DNS.	Switch# configure terminal Switch(config)#no ip domain-lookup El comando **no ip domain-lookup** desactiva la traducción de nombres a dirección del dispositivo, se ahorra tiempo cuando se escribe mal un comando y el dispositivo no tratara de traducirlo.
Nombre del switch	Switch(config)#hostname S1 Se debe cambiar el nombre de cada dispositivo usando el comando **hostname** para identificarlo en la red fácilmente.
Nombre de dominio	S1(config)#ip domain-name ccna-lab.com Este comando define un nombre de dominio predeterminado que el IOS del dispositivo utiliza para completar los nombres del host incompetentes.
Contraseña cifrada para el modo EXEC privilegiado	S1(config)#enable secret ciscoenpass Este comando proporciona mayor seguridad a la contraseña de enable ya que la encripta con MD5.
Contraseña de acceso a la consola	S1(config)#line console 0 S1(config-line)#password ciscoconpass S1(config-line)#login En este paso lo que se hace es configurar un password que debe escribir todo aquel que trate de acceder por el puerto de consola al dispositivo.
Crear un usuario administrativo en la base de datos local	S1(config-line)#username admin password admin1pass En este paso lo que se hizo fue crear un usuario y password en la base de datos local que es alterno al password de vty y consola si se especifica para usarse.

Tarea	Especificación
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	S1(config)#line vty 0 4 S1(config-line)#login local S1(config-line)#exit En este paso se habilita el acceso por las líneas vty las cuales permiten el acceso a un dispositivo cisco a través de telnet o ssh. Por lo general un dispositivo cisco tiene 16 líneas vty. Al escribir el comando **login local** se le indica al router que ya no le haga caso al password configurado en el line vty sino que busque el usuario y password de la base de datos local creado en el paso anterior.
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S1(config)#line vty 0 4 S1(config-line)#transport input ssh S1(config-line)#exit Con este commando **transport input ssh** le decimos al router que solamente permita conexiones con ssh la cual es la más recomendada para usarse porque es más segura que telnet.
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption Este commando aplica un cifrado básico a los password que se encuentren sin encriptar.
Configurar un MOTD Banner	S1(config)#banner motd # Prohibido el acceso sin autorizacion a este dispositivo!# Es importante configurar este mensaje en cada dispositivo y sirve para notificaciones legales y advertencias para todo aquel que se conecte al dispositivo.

Tarea	Especificación
Generar una clave de cifrado RSA	S1(config)#crypto key generate rsa general-keys modulus 1024 En este paso se generan las claves secretas unidireccionales para que el router encripte el tráfico SSH. La clave se utiliza para encriptar y descifrar datos. Para crear esta clase de encriptación se usa este comando donde el modulo determina el tamaño de la clave.
Configurar la interface de administración (SVI)	S1(config)#interface vlan 4 S1(config-if)#description Management S1(config-if)#ip address 10.19.8.98 255.255.255.248 S1(config-if)#ipv6 address FE80::98 link-local S1(config-if)#ipv6 address 2001:db8:acad:c::98/64 S1(config-if)#no shutdown S1(config-if)#exit En este paso se crea interface para dministración del switch tanto con direccionamiento IPv4 como IPv6, se crea como interface vlan 4 y para que funcione se debe crear la vlan 4 en el switch lo cual se hará en otro paso.
Configuración del gateway predeterminado	S1(config)#ip default-gateway 10.19.8.97 Si el switch se va a administrar de forma remota desde redes que no están conectadas directamente, se debe configurar con un gateway predeterminado, en este caso el gateway es la IP que está configurada en el router en la subinterface de Management.

6.4 Configuración de switch 2

Tabla 5. Tareas de configuración realizadas en switch 2

Tarea	Especificación
Desactivar la búsqueda DNS.	Switch#configure terminal Switch(config)#no ip domain-lookup El comando **no ip domain-lookup** desactiva la traducción de nombres a dirección del dispositivo, se ahorra tiempo cuando se escribe mal un comando y el dispositivo no tratara de traducirlo.
Nombre del switch	Switch(config)#hostname S2 S2(config)# Se debe cambiar el nombre de cada dispositivo usando el comando **hostname** para identificarlo en la red fácilmente.
Nombre de dominio	S2(config)#ip domain-name ccna-lab.com Este comando define un nombre de dominio predeterminado que el IOS del dispositivo utiliza para completar los nombres del host incompetentes.
Contraseña cifrada para el modo EXEC privilegiado	S2(config)#enable secret ciscoenpass Este comando proporciona mayor seguridad a la contraseña de enable ya que la encripta con MD5.
Contraseña de acceso a la consola	S2(config)#line console 0 S2(config-line)#password ciscoconpass S2(config-line)#login S2(config-line)#exit En este paso lo que se hace es configurar un password que debe escribir todo aquel que trate de acceder por el puerto de consola al dispositivo.

Tarea	Especificación
Crear un usuario administrativo en la base de datos local	S2(config)#username admin password admin1pass En este paso lo que se hizo fue crear un usuario y password en la base de datos local que es alterno al password de vty y consola si se especifica para usarse.
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	S2(config)#line vty 0 4 S2(config-line)#login local S2(config-line)#exit En este paso se habilita el acceso por las líneas vty las cuales permiten el acceso a un dispositivo cisco a través de telnet o ssh. Por lo general un dispositivo cisco tiene 16 líneas vty. Al escribir el comando **login local** se le indica al router que ya no le haga caso al password configurado en el line vty sino que busque el usuario y password de la base de datos local creado en el paso anterior.
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S2(config)#line vty 0 4 S2(config-line)#transport input ssh S2(config-line)#exit Con este commando **transport input ssh** le decimos al router que solamente permita conexiones con ssh la cual es la más recomendada para usarse porque es más segura que telnet.
Cifrar las contraseñas de texto no cifrado	S2(config)#service password-encryption Este commando aplica un cifrado básico a los password que se encuentren sin encriptar.
Configurar un MOTD Banner	S2(config)#banner motd # Prohibido el acceso sin autorizacion a este dispositivo!# Es importante configurar este mensaje en cada dispositivo y sirve para notificaciones legales y advertencias para todo aquel que se conecte al dispositivo.

Tarea	Especificación
Generar una clave de cifrado RSA	S2(config)#crypto key generate rsa general-keys modulus 1024 En este paso se generan las claves secretas unidireccionales para que el router encripte el tráfico SSH. La clave se utiliza para encriptar y descifrar datos. Para crear esta clase de encriptación se usa este comando donde el modulo determina el tamaño de la clave.
Configurar la interface de administración (SVI)	S2(config)#interface vlan 4 S2(config-if)#description Management S2(config-if)#ip address 10.19.8.99 255.255.255.248 S2(config-if)#ipv6 address FE80::99 link-local S2(config-if)#ipv6 address 2001:db8:acad:c::99/64 S2(config-if)#no shutdown S2(config-if)#exit S2(config)# En este paso se crea interface para dministración del switch tanto con direccionamiento IPv4 como IPv6, se crea como interface vlan 4 y para que funcione se debe crear la vlan 4 en el switch lo cual se hará en otro paso.
Configuración del gateway predeterminado	S2(config)#ip default-gateway 10.19.8.97 Si el switch se va a administrar de forma remota desde redes que no están conectadas directamente, se debe configurar con un gateway predeterminado, en este caso el gateway es la IP que está configurada en el router en la subinterface de Management.

7. Configuración de la infraestructura de red (VLAN, Trunking, EtherChannel)

7.1 Configuración de switch 1

Tabla 6. Tareas de configuración realizadas en switch 1

Tarea	Especificación
Crear VLAN	S1#configure terminal S1(config)#vlan 2 S1(config-vlan)#name Bikes S1(config-vlan)#vlan 3 S1(config-vlan)#name Trikes S1(config-vlan)#vlan 4 S1(config-vlan)#name Management S1(config-vlan)#vlan 5 S1(config-vlan)#name Parking S1(config-vlan)#vlan 6 S1(config-vlan)#name Native S1(config-vlan)#end S1# En este paso se crean todas las vlan que se van a usar ya que por defecto el switch solo tiene creada la vlan 1. Se podrían crear varias vlan al tiempo si son consecutivas pero es mejor crear una a una para ponerles un nombre.

Tarea	Especificación
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	S1(config)#interface fastEthernet 0/1 S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 6 Ahora en este paso se configuran los puertos troncales, dentro de la interface por ser esta referencia de switch se debe confirmar el tipo de encapsulameinto con el commando **switchport trunk encapsulation dot1q**, luego con el comando **switchport mode trunk** se pone el puerto en modo troncal. También se aplica el comando **switchport trunk native vlan 6** el cual permite la vlan 6 como nativa la cual lleva tráfico sin etiqueta útil para antiguos dispositivos que no entienden 802.1Q. Este paso se repite en las interfaces Fe0/2 y Fe 0/5. S1(config-if)#interface fastEthernet 0/2 S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 6 S1(config-if)#interface fastEthernet 0/5 S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 6

Tarea	Especificación
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	S1(config)#interface port-channel 1 S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 6 S1(config)#interface range fastEthernet 0/1-2 S1(config-if-range)#switchport trunk encapsulation dot1q S1(config-if-range)#switchport mode trunk S1(config-if-range)#switchport trunk native vlan 6 S1(config-if-range)#channel-group 1 mode active S1(config-if-range)#no shutdown En este paso se crea un etherchannel el cual permite realizar una agrupación lógica de varios enlaces físicos Ethernet y así funcionarán como un único enlace. Primero se crea la interface port-channel en te caso la 1 con el comando **interface port-channel 1**, se selecciona el tipo de encapsulación dot1q con el comando **switchport trunk encapsulation dot1q,** se pone la interface en modo trunk con el comando **switchport mode trunk** y se indica a la interface cual será la vlan nativa con el comando **switchport trunk native vlan 6.** Luego se configuran los puertos físicos del switch que formaran el etherchannel, se pueden configurar los dos puertos al mismo tiempo con el comando **interface range fastEthernet 0/1-2,** se selecciona el tipo de encapsulación dot1q con el comando **switchport trunk encapsulation dot1q,** se pone la interface en modo trunk con el comando **switchport mode trunk** y se indica a la interface cual será la vlan nativa con el comando **switchport trunk native vlan 6,** por último se selecciona el cannel-group ya que pueden haber varios con el comando **channel-group 1 mode active**, cuando se configure el swich 2 este se puede crear en modo activo o pasivo lo importante es que en uno de los switch exista uno activo.

Tarea	Especificación
Configurar el puerto de acceso de host para VLAN 2	S1(config)#interface fastEthernet 0/6 S1(config-if)#description conexion_PCA S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 2 S1(config-if)#no shutdown S1(config-if)#exit En este paso se configura el puerto en donde se conecta el PCA el cual se debe conectar en acceso, para dejar el puerto en acceso se hace con el comando **switchport mode access** y para especificar la vlan que deseamos permitir se pone el comando **switchport access vlan 2.**
Configurar la seguridad del puerto en los puertos de acceso	S1(config)#interface fastEthernet 0/6 S1(config-if)#switchport port-security S1(config-if)#switchport port-security maximum 3 Con el comando **switchport port-security** se habilita la seguridad del puerto restringiendo cantidad de MAC en este caso permitirá solo una, para especificar otra cantidad de MAC en este caso 3 damos el comando **switchport port-security maximum 3.**

Tarea	Especificación
Proteja todas las interfaces no utilizadas	S1(config)#interface range fastEthernet 0/3-4 S1(config-if-range)#description Parking S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 5 S1(config-if-range)#shutdown S1(config-if-range)#interface range fastEthernet 0/7-24 S1(config-if-range)#description Parking S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 5 S1(config-if-range)#shutdown S1(config)#interface range gigabitEthernet 0/1-2 S1(config-if-range)#description Parking S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 5 S1(config-if-range)#shutdown En este paso por seguridad se dejan deshabilitadas las interfaces del switch que no serán usadas, se puede hacer con el comando interface range para puertos que sean consecutivos, se permite la vlan 5 la cual no se usa y se deja una descripción informando que la interface no está en uso, por último se apagan los puertos con el comando **shutdown** estando dentro de las interfaces.

7.2 Configuración de switch 2

Tabla 7. Tareas de configuración realizadas en switch 2

Tarea	Especificación
Crear VLAN	S2#configure terminal S2(config)#vlan 2 S2(config-vlan)#name Bikes S2(config-vlan)#vlan 3 S2(config-vlan)#name Trikes S2(config-vlan)#vlan 4 S2(config-vlan)#name Management S2(config-vlan)#vlan 5 S2(config-vlan)#name Parking S2(config-vlan)#vlan 6 S2(config-vlan)#name Native S2(config-vlan)#end S2# En este paso se crean todas las vlan que se van a usar ya que por defecto el switch solo tiene creada la vlan 1. Se podrían crear varias vlan al tiempo si son consecutivas, pero es mejor crear una a una para ponerles un nombre.

Tarea	Especificación
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	S2(config)#interface fastEthernet 0/1 S2(config-if)#switchport trunk encapsulation dot1q S2(config-if)#switchport mode trunk S2(config-if)#switchport trunk native vlan 6 S2(config-if)#interface fastEthernet 0/2 S2(config-if)#switchport trunk encapsulation dot1q S2(config-if)#switchport mode trunk S2(config-if)#switchport trunk native vlan 6 Ahora en este paso se configuran los puertos troncales, dentro de la interface por ser esta referencia de switch se debe confirmar el tipo de encapsulameinto con el commando **switchport trunk encapsulation dot1q**, luego con el comando **switchport mode trunk** se pone el puerto en modo troncal. También se aplica el comando **switchport trunk native vlan 6** el cual permite la vlan 6 como nativa la cual lleva tráfico sin etiqueta útil para antiguos dispositivos que no entienden 802.1Q. Este paso se repite en las interfaces Fe0/1 y Fe 0/2.

Tarea	Especificación
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	S2#configure terminal S2(config)#interface port-channel 1 S2(config-if)#switchport trunk encapsulation dot1q S2(config-if)#switchport mode trunk S2(config-if)#switchport trunk native vlan 6 S2(config)#interface range fastEthernet 0/1-2 S2(config-if-range)#switchport trunk encapsulation dot1q S2(config-if-range)#switchport mode trunk S1(config-if-range)#switchport trunk native vlan 6 S2(config-if-range)#channel-group 1 mode passive S2(config-if-range)#no shutdown En este paso se crea un etherchannel el cual permite realizar una agrupación lógica de varios enlaces físicos Ethernet y así funcionarán como un único enlace. Primero se crea la interface port-channel en te caso la 1 con el comando **interface port-channel 1**, se selecciona el tipo de encapsulación dot1q con el comando **switchport trunk encapsulation dot1q,** se pone la interface en modo trunk con el comando **switchport mode trunk** y se indica a la interface cual será la vlan nativa con el comando **switchport trunk native vlan 6.** Luego se configuran los puertos físicos del switch que formaran el etherchannel, se pueden configurar los dos puertos al mismo tiempo con el comando **interface range fastEthernet 0/1-2,** se selecciona el tipo de encapsulación dot1q con el comando **switchport trunk encapsulation dot1q,** se pone la interface en modo trunk con el comando **switchport mode trunk** y se indica a la interface cual será la vlan nativa con el comando **switchport trunk native vlan 6,** por último se selecciona el cannel-group ya que pueden haber varios con el comando **channel-group 1 mode passive**, cuando se configure el swich 1 debe estar en activo. Se recomienda dejar los switch activo-activo o activo-pasivo.

Tarea	Especificación
Configurar el puerto de acceso del host para la VLAN 3	S2(config)#interface fastEthernet 0/18 S2(config-if)#description Conexion_PCB S2(config-if)#switchport mode access S2(config-if)#switchport access vlan 3 S2(config-if)#no shutdown S2(config-if)#exit En este paso se configura el puerto en donde se conecta el PCB el cual se debe conectar en acceso, para dejar el puerto en acceso se hace con el comando **switchport mode access** y para especificar la vlan que deseamos permitir se pone el comando **switchport access vlan 3.**
Configure port-security en los access ports	S2(config)#interface fastEthernet 0/18 S2(config-if)#switchport port-security S2(config-if)#switchport port-security maximum 3 Con el comando **switchport port-security** se habilita la seguridad del puerto restringiendo cantidad de MAC en este caso permitirá solo una, para especificar otra cantidad de MAC en este caso 3 damos el comando **switchport port-security maximum 3.**

Tarea	Especificación
Asegure todas las interfaces no utilizadas.	S2(config)#interface range fastEthernet 0/3-17 S2(config-if-range)#description Parking S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 5 S2(config-if-range)#shutdown S2(config)#interface range fastEthernet 0/19-24 S2(config-if-range)#description Parking S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 5 S2(config-if-range)#shutdown S2(config)#interface range gigabitEthernet 0/1-2 S2(config-if-range)#description Parking S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 5 S2(config-if-range)#shutdown En este paso por seguridad se dejan deshabilitadas las interfaces del switch que no serán usadas, se puede hacer con el comando interface range para puertos que sean consecutivos, se permite la vlan 5 la cual no se usa y se deja una descripción informando que la interface no está en uso, por último se apagan los puertos con el comando shutdown estando dentro de las interfaces.

8. Configurar soporte de host

8.1 Configuración de router 1

Tabla 8. Tareas de configuración realizadas en router 1

Tarea	Especificación
Configure Default Routing	R1(config)#ip route 0.0.0.0 0.0.0.0 loopback 0 R1(config)#ipv6 route ::/0 loopback 0 Se crean en este paso rutas por defecto o predeterminadas para direccionamiento IPv4 e IPv6 para que se direccionen todos los paquetes dirigidos a redes que no estén en la tabla de enrutamiento a la interface loopback 0.
Configurar IPv4 DHCP para VLAN 2	R1(config)#ip dhcp excluded-address 10.19.8.1 10.19.8.52 R1(config)#ip dhcp pool vlan2 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 En este paso se configura el protocolo dhcp usando la red IPv4 10.19.8.0/26 el cual asignará automáticamente direcciones IP de esta red. Inicialmente con el comando **ip dhcp excluded-address 10.19.8.1 10.19.8.52** se excluyen las direcciones que no se quiere que sean asignadas. Luego con el comando **ip dhcp pool vlan2** se crea un pool de direcciones con un nombre que deseemos, luego se indica cual será la red del pool creado con el comando **network 10.19.8.0 255.255.255.192,** por último se indica cual será la ip default la cual es la ip que está en el router con esa red con el comando **default-router 10.19.8.1** y por último con el comando **domain-name ccna-a.net** definimos el nombre del dominio.

Tarea	Especificación
Configurar DHCP IPv4 para VLAN 3	R1(config)#ip dhcp excluded-address 10.19.8.65 10.19.8.84 R1(config)#ip dhcp pool vlan3 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 En este paso se repite la configuración del protocolo dhcp del paso anterior con la diferencia que ahora se hace con la red de la vlan 3 **10.19.8.64/27.**

8.2 Configuración de los servidores

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

En este paso sobre el simulador Packet Tracer se verifica en cada PC que el direccionamiento IPv4 se haya asignado automáticamente, y por otro lado el direccionamiento IPv6 se configura manualmente, luego con ayuda de el comando **ipconfig /all** y el comando **ipv6config** se verifica en cada PC que estén los direccionamientos configurados correctamente IPv4 e IPv6 respectivamente.

Tabla 9. Configuración de red de PC-A

Configuración de red de PC-A	
Descripción	Fastethernet0
Dirección física	0009.7C97.23B7
Dirección IP	10.19.8.53
Máscara de subred	255.255.255.192
Gateway predeterminado	10.19.8.1
Gateway predeterminado IPv6	FE80::1

Tabla 10. Configuración de red de PC-B

Configuración de red de PC-B	
Descripción	Fastethernet0
Dirección física	00D0.FF6B.14E3
Dirección IP	10.19.8.85
Máscara de subred	255.255.255.224
Gateway predeterminado	10.19.8.65
Gateway predeterminado IPv6	FE80::1

En las siguientes imágenes se deja la evidencia de los direccionamientos configurados tanto en el PC-A como en el PC-B.

Figura 5. Direccionamiento registrado en PC-A

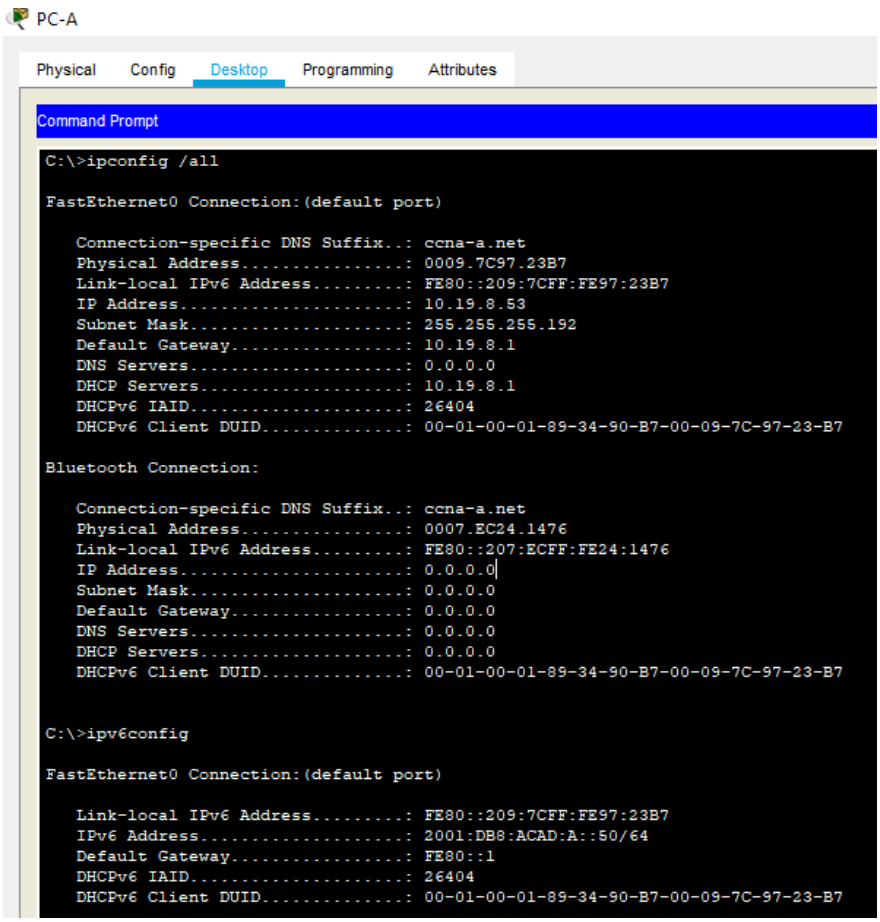
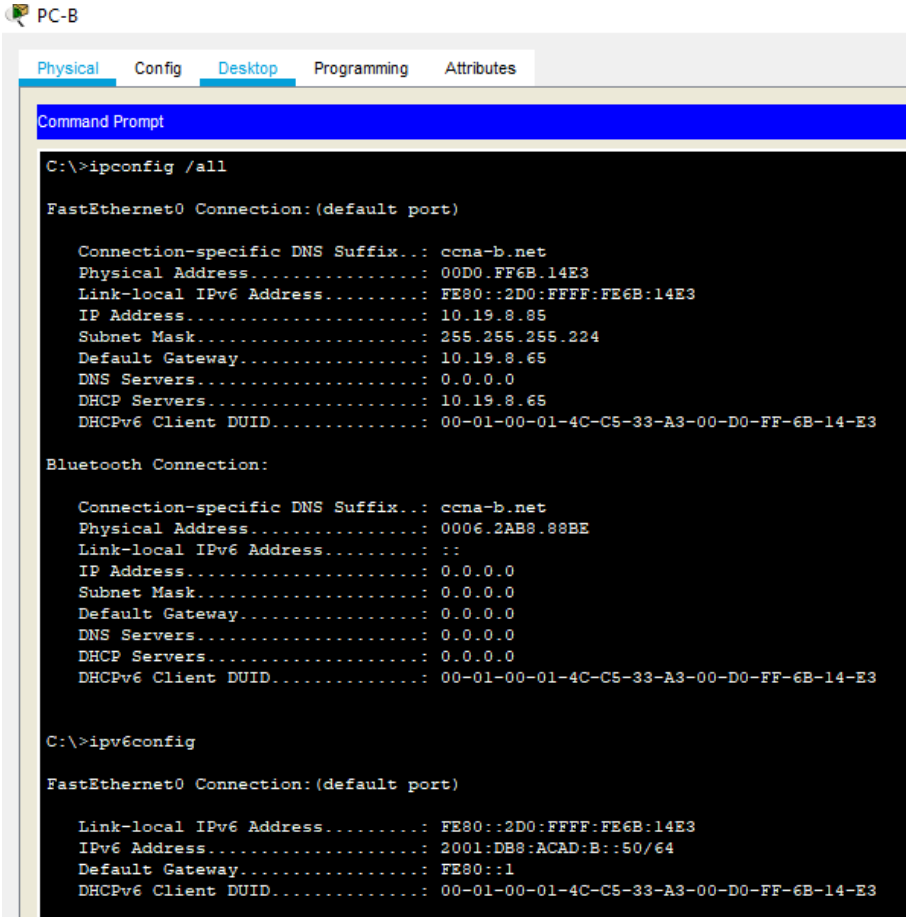


Figura 6. Direccionamiento registrado en PC-B



8.3 Probar y verificar la conectividad de extremo a extremo

En este paso verifica la conectividad entre dispositivos usando el comando ping, el comando ping (Packet Internet Groper) es un método muy común para resolver problemas la accesibilidad de dispositivo. Utiliza dos mensajes de consulta del Protocolo de mensajes de control de Internet (ICMP), solicitudes de eco ICMP y respuestas de eco ICMP para determinar si un host remoto se encuentra activo. El comando ping también calcula la cantidad de tiempo necesario para recibir la respuesta de eco.

Tabla 11. Verificación de conectividad extremo a extremo

Desde	A	de Internet	Dirección IP	Resultados de ping
PC-A	R1, G0/0/1.2	Dirección	10.19.8.1	Responde correctamente,ver figura 6
		IPv6	2001:db8:acad:a::1	Responde correctamente, ver figura 6
	R1, G0/0/1.3	Dirección	10.19.8.65	Responde correctamente, ver figura 6
		IPv6	2001:db8:acad:b::1	Responde correctamente, ver figura 6
	R1, G0/0/1.4	Dirección	10.19.8.97	Responde correctamente, ver figura 6
		IPv6	2001:db8:acad:c::1	Responde correctamente, ver figura 6
	S1, VLAN 4	Dirección	10.19.8.98	Responde correctamente, ver figura 7
		IPv6	2001:db8:acad:c::98	Responde correctamente, ver figura 7
	S2, VLAN 4	Dirección	10.19.8.99	Responde correctamente, ver figura 7
		IPv6	2001:db8:acad:c::99	Responde correctamente, ver figura 7
	PC-B	Dirección	10.19.8.55	Responde correctamente, ver figura 8
		IPv6	2001:db8:acad:b: :50	Responde correctamente, ver figura 8
	R1 Bucle 0	Dirección	209.165.201.1	Responde correctamente, ver figura 8

Desde	A	de Internet	Dirección IP	Resultados de ping
		IPv6	2001:db8:acad:209::1	Responde correctamente, ver figura 8
PC-B	R1 Bucle 0	Dirección	209.165.201.1	Responde correctamente, ver figura 9
		IPv6	2001:db8:acad:209::1	Responde correctamente, ver figura 9
	R1, G0/0/1.2	Dirección	10.19.8.1	Responde correctamente, ver figura 9
		IPv6	2001:db8:acad:a::1	Responde correctamente, ver figura 9
	R1, G0/0/1.3	Dirección	10.19.8.65	Responde correctamente, ver figura 9
		IPv6	2001:db8:acad:b::1	Responde correctamente, ver figura 9
	R1, G0/0/1.4	Dirección	10.19.8.97	Responde correctamente, ver figura 10
		IPv6	2001:db8:acad:c::1	Responde correctamente, ver figura 10
	S1, VLAN 4	Dirección	10.19.8.98	Responde correctamente, ver figura 10
		IPv6	2001:db8:acad:c::98	Responde correctamente, ver figura 10
	S2, VLAN 4	Dirección	10.19.8.99.	Responde correctamente, ver figura 10
		IPv6	2001:db8:acad:c::99	Responde correctamente, ver figura 10

A continuación, se deja evidencia con pantallazos tomados en los PC-A y PCB con los resultados de los ping realizados, todos responden correctamente confirmando la conectividad entre los dispositivos.

Figura 7. Resultados PING desde el PC-A

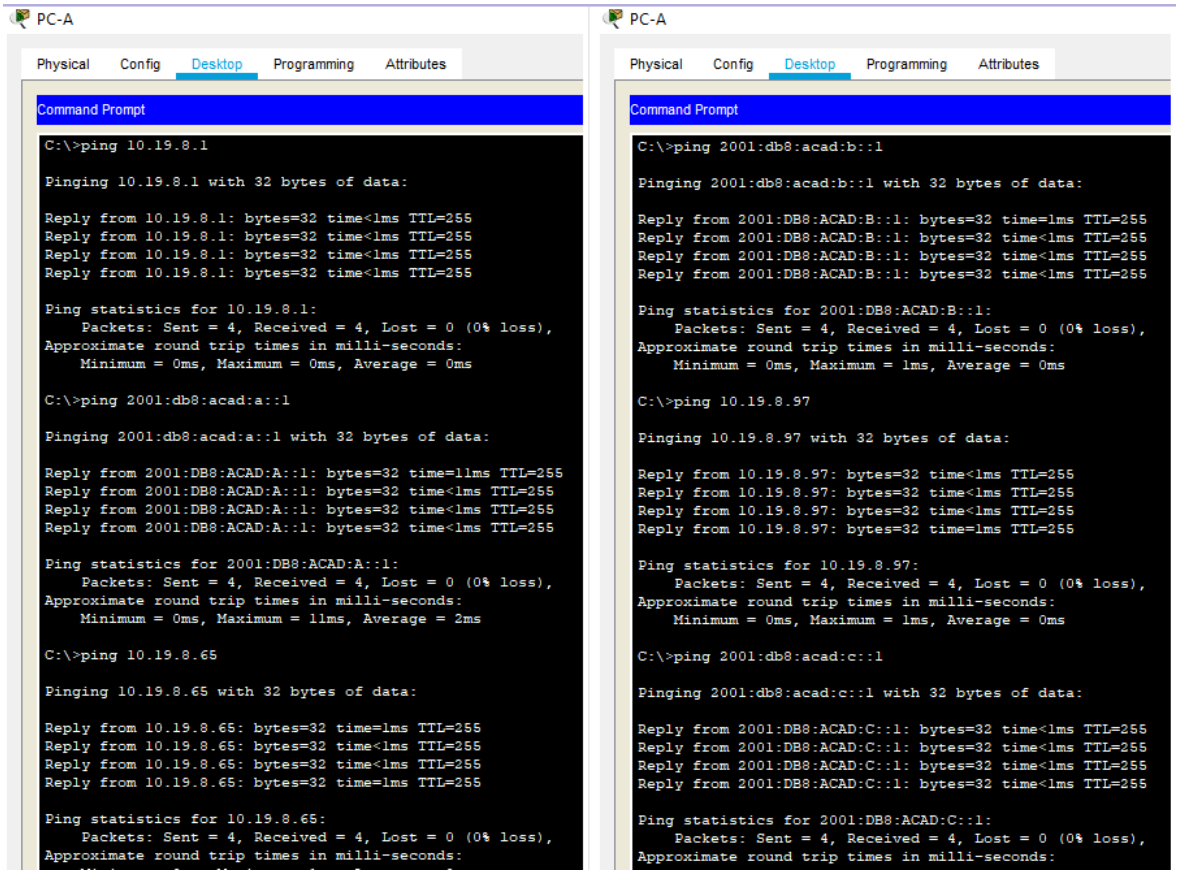


Figura 8. Resultados PING desde el PC-A

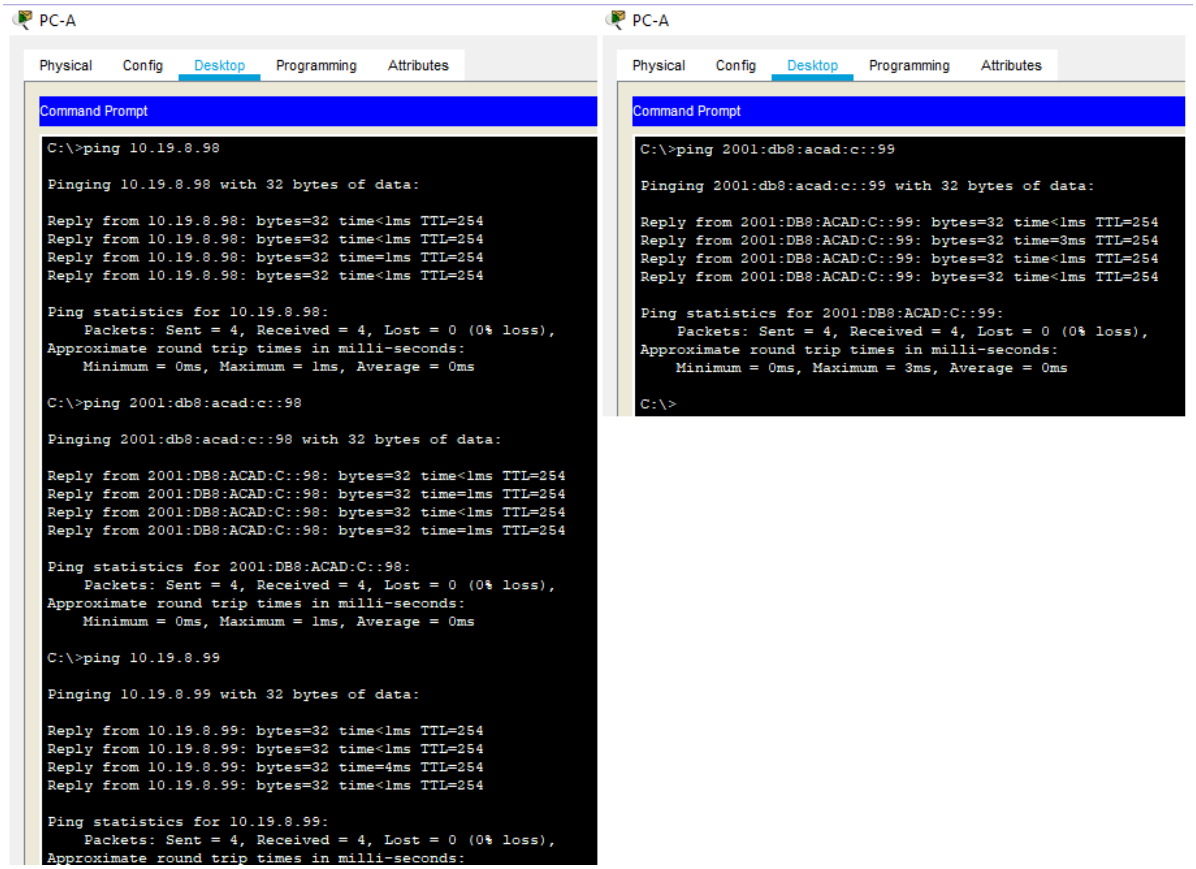


Figura 9. Resultados PING desde el PC-A

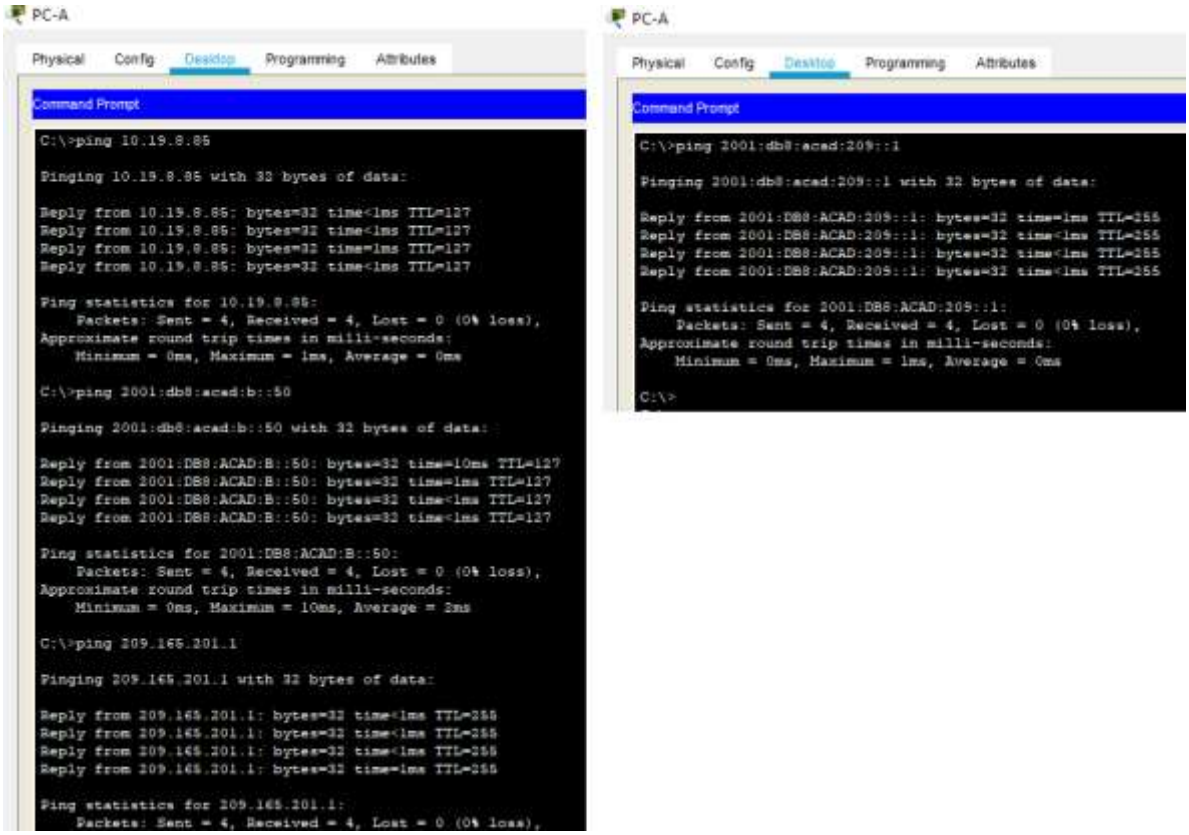


Figura 10. Resultados PING desde el PC-B

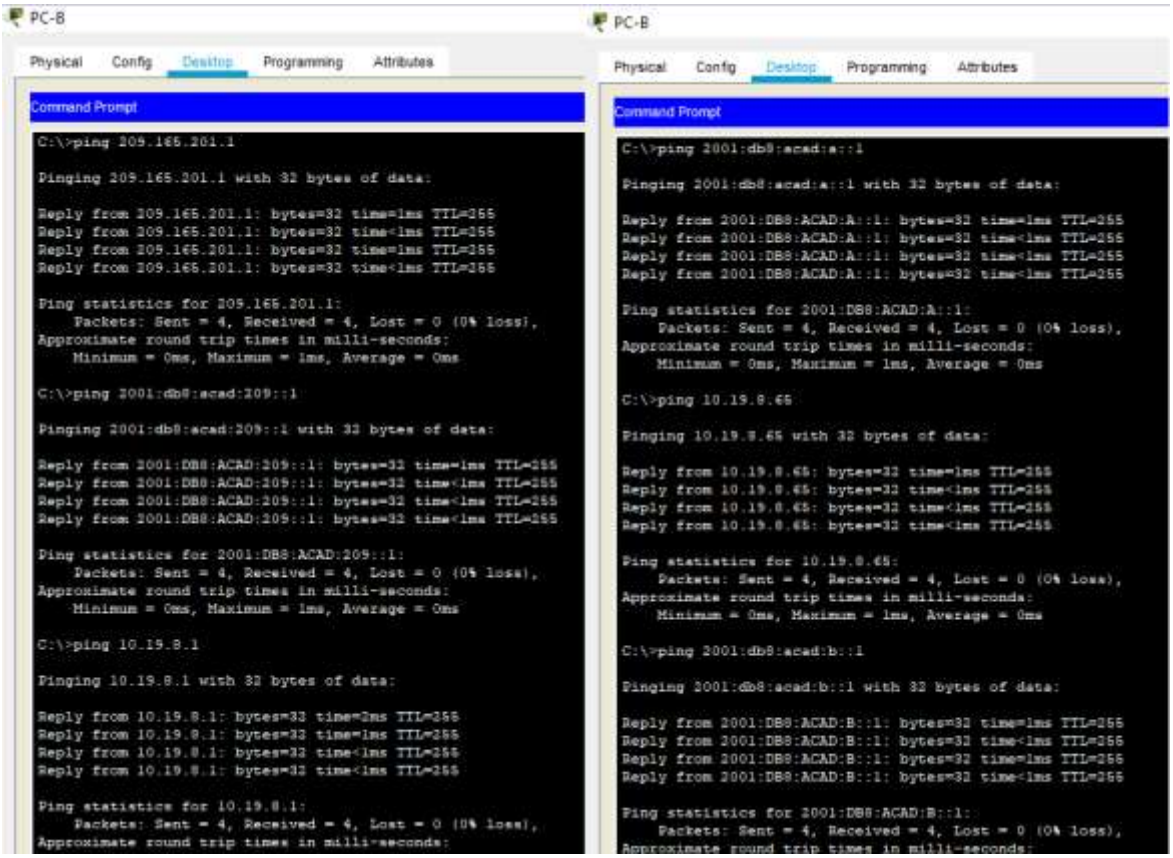
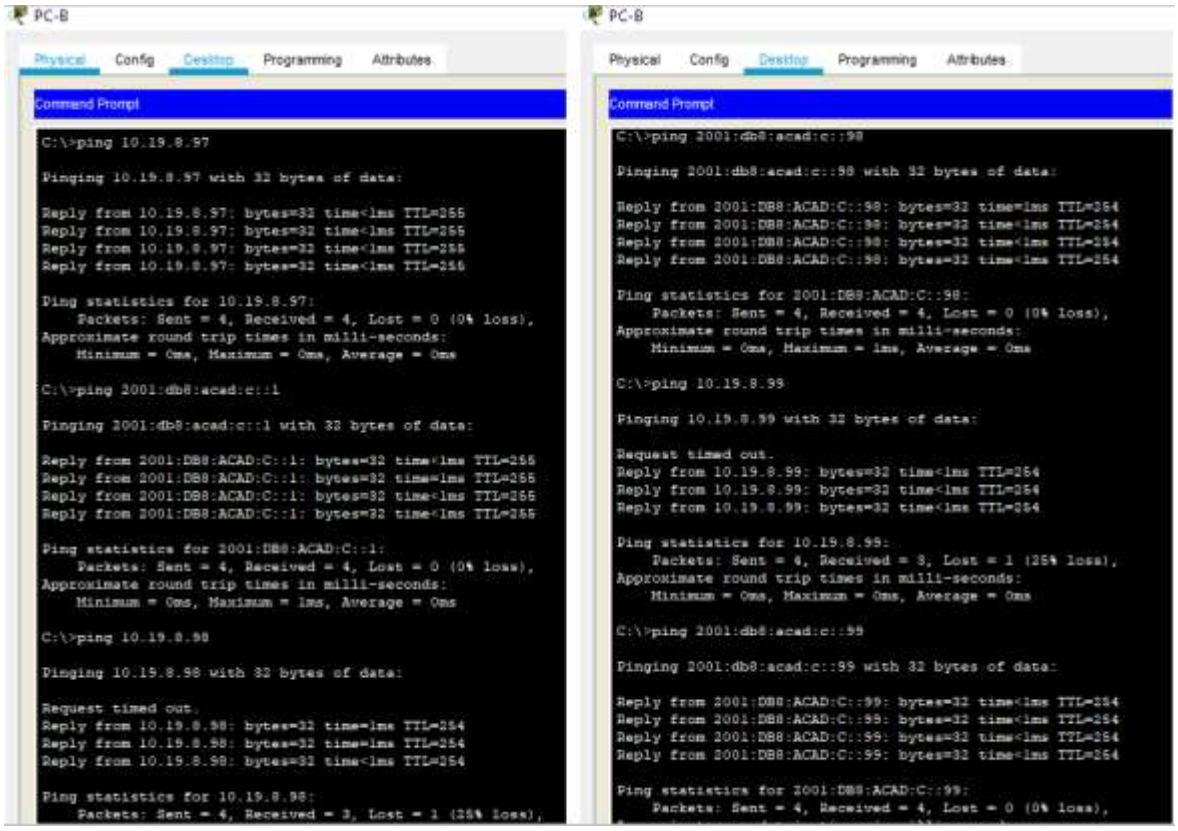


Figura 11. Resultados PING desde el PC-B



9. ESCENARIO 2

En este segundo escenario se configura 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.

Figura 12. Topología de Red Escenario 2

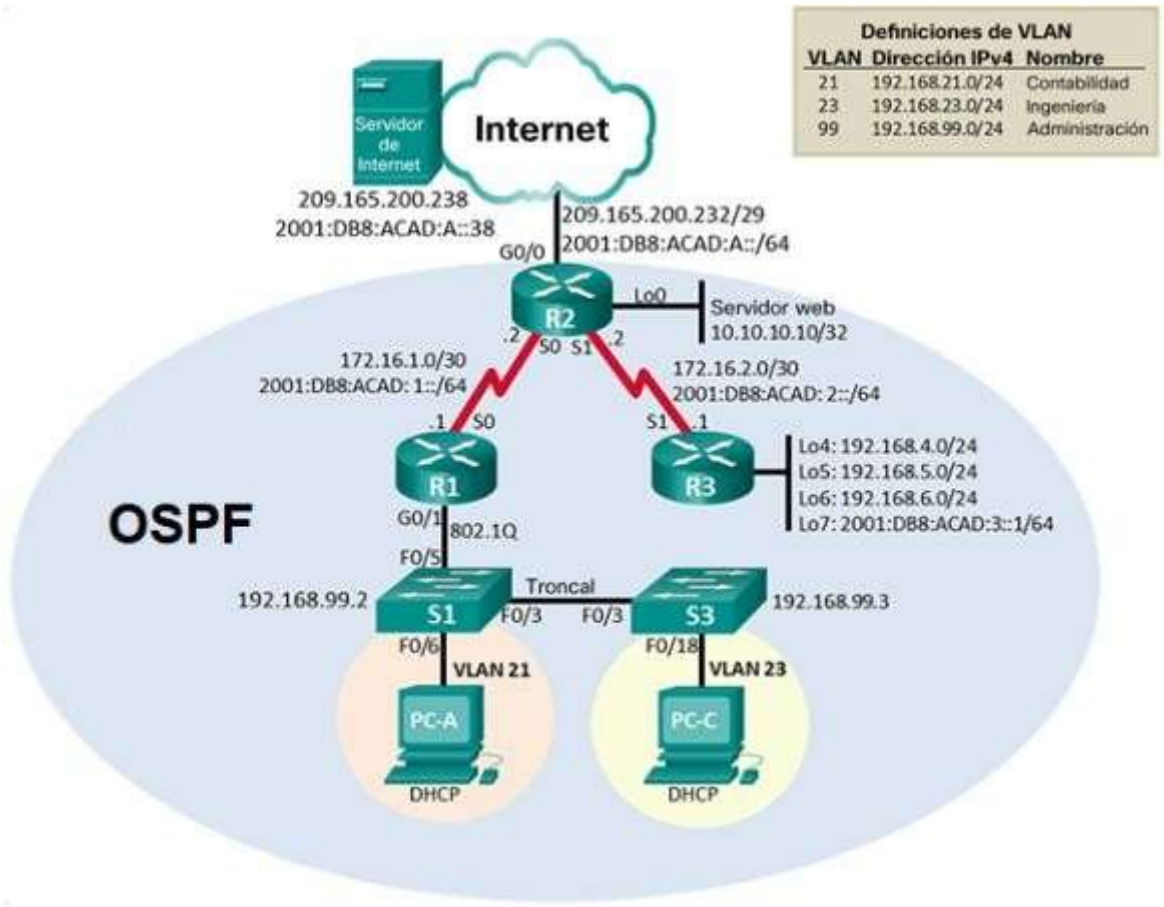
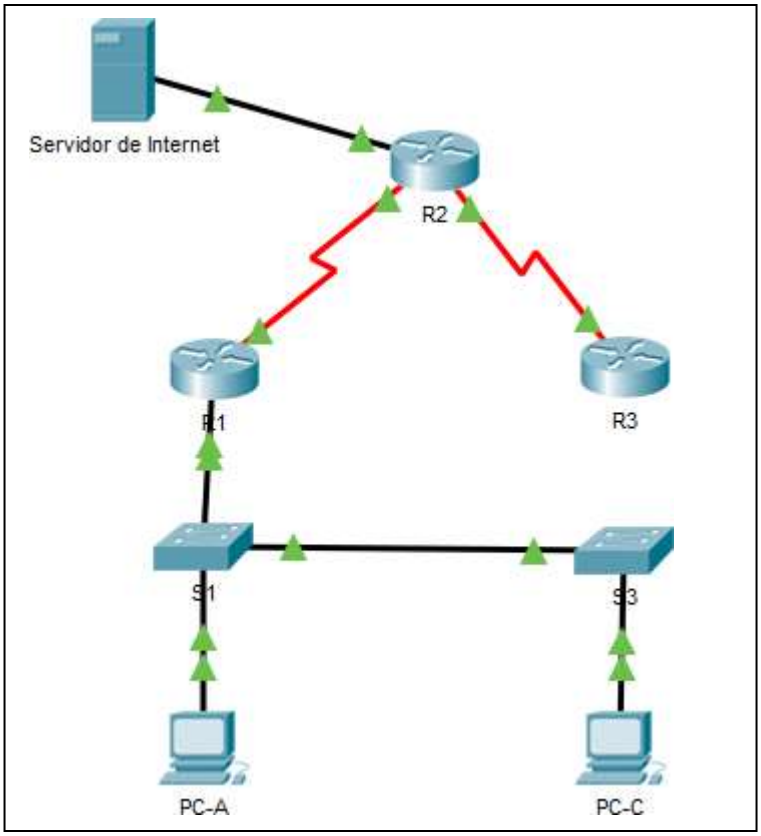


Figura 13. Simulación del escenario 2 en Packet Tracert



10. Inicializar dispositivos

10.1 Inicializar y volver a cargar los routers y los switches

En el segundo escenario de red se selecciónan tres router cisco 1941, dos switch cisco 2960, dos equipos host y un servisor . Al ingresar al router se ingresa al modo EXEC privilegiado con el comando **enable**, luego se elimina la configuración de inicio de la memoria de acceso no volátil NVRAM con el comando **erase startup-config**, allí el router pide confirmar esta acción, luego de confirmar se reinicia el router con el comando **reload**. Esto es recomendado al iniciar la configuración de un dispositivo ya que este puede tener configuraciones anteriores que generen problemas en mi red e impidan el corecto funcionamiento.

Tabla 12. Inicialización y recarga de router y switch

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	Router>enable Router#erase startup-config Erasing the nvram filesystem will remove all configuration files! Continue? [confirm] [OK] Erase of nvram: complete %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram Router# Al ingresar al router se ingresa al modo EXEC privilegiado con el comando **enable**, luego se elimina la configuración de inicio de la memoria de acceso no volátil NVRAM con el comando **erase startup-config**, se hace en cada router.
Volver a cargar todos los routers	Router#reload Proceed with reload? [confirm] System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1) Technical Support: http://www.cisco.com/techsupport Copyright (c) 2010 by cisco Systems, Inc.

	Total memory size = 512 MB - On-board = 512 MB, DIMM0 = 0 MB CISCO1941/K9 platform with 524288 Kbytes of main memory Main memory is configured to 64/-1(On-board/DIMM0) bit mode with ECC disabled Readonly ROMMON initialized Con el comando **reload** el router se reinicia y arranca nuevamente, se hace en cada router.
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Switch>enable Switch#delete vlan.dat Delete filename [vlan.dat]? Delete flash:/vlan.dat? [confirm] Switch#erase startup-config Erasing the nvram filesystem will remove all configuration files! Continue? [confirm] [OK] Erase of nvram: complete %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram Switch# se elimina el archivo con vlan creadas anteiormente en el switch con el comando **delete vlan.dat** y luego se elimina la configuración de inicio de la memoria de acceso no volátil NVRAM con el comando **erase startup-config.**
Volver a cargar ambos switches	Switch#reload Proceed with reload? [confirm] C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(25r)FX, RELEASE SOFTWARE (fc4) Cisco WS-C2960-24TT (RC32300) processor (revision C0) with 21039K bytes of memory. 2960-24TT starting... Base ethernet MAC Address: 000C.CF5A.009E Xmodem file system is available. Initializing Flash... flashfs[0]: 1 files, 0 directories

	flashfs[0]: 0 orphaned files, 0 orphaned directories flashfs[0]: Total bytes: 64016384 flashfs[0]: Bytes used: 4414921 flashfs[0]: Bytes available: 59601463 flashfs[0]: flashfs fsck took 1 seconds. ...done Initializing Flash. Boot Sector Filesystem (bs:) installed, fsid: 3 Parameter Block Filesystem (pb:) installed, fsid: 4 Loading "flash:/c2960-lanbase-mz.122-25.FX.bin"... ################ Con el comando **reload** el switch se reinicia y arranca nuevamente, se hace en cada switch.
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Switch#show flash Directory of flash:/ 1 -rw- 4414921 <no date> c2960-lanbase-mz.122-25.FX.bin 64016384 bytes total (59601463 bytes free) Switch# Con el comando **show flash** se puede ver los archivos de la memoria flash y se confirma que no este una base de datos de vlan.

11. Configurar los parámetros básicos de los dispositivos

11.1 Configurar la computadora de Internet

En este paso se realiza configuración de direccionamientos en el servidor de internet el cual es un computador conectado a internet que tiene como funciones principales almacenar páginas web, administrar bases de datos y responder a las solicitudes de los navegadores de los internautas.

Tabla 13. Direccionamientos configurados servidor de internet

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.233
Dirección IPv6/subred	2001:DB8:ACAD:A::38
Gateway predeterminado IPv6	2001:DB8:ACAD:2::1

11.2 Configuración de router 1

Tabla 14. Tareas de configuración en el router 1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router>enable Router# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Router(config)#no ip domain-lookup Router(config)# El comando **no ip domain-lookup** desactiva la traducción de nombres a dirección del dispositivo, se ahorra tiempo cuando se escribe mal un comando y el dispositivo no tratara de traducirlo.

Nombre del router	Router(config)#hostname R1 R1(config)# Se debe cambiar el nombre de cada dispositivo usando el comando **hostname** para identificarlo en la red fácilmente.
Contraseña de exec privilegiado cifrada	R1(config)#enable secret class Este comando proporciona mayor seguridad a la contraseña de enable ya que la encripta con MD5.
Contraseña de acceso a la consola	R1(config)#line console 0 R1(config-line)#password cisco R1(config-line)#login En este paso lo que se hace es configurar un password que debe escribir todo aquel que trate de acceder por el puerto de consola al dispositivo.
Contraseña de acceso Telnet	R1(config)#line vty 0 15 R1(config-line)#password cisco R1(config-line)#login En este paso se habilita el acceso por las líneas vty las cuales permiten el acceso a un dispositivo cisco a través de telnet o ssh. Por lo general un dispositivo cisco tiene 16 lineas vty. Al escribir el comando **password cisco**, y luego **login**, se le indica al router que debe permitir ingreso solo si se introduce esa contraseña establecida.
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption Este commando aplica un cifrado básico a los password que se encuentren sin encriptar.
Mensaje MOTD	R1(config)#banner motd # Se prohibe el acceso no autorizado!# Es importante configurar este mensaje en cada dispositivo y sirve para notificaciones legales y advertencias para todo aquel que se conecte al dispositivo.

Interface S0/0/0	R1(config)#interface serial 0/0/0 R1(config-if)#description Conexion_R2 R1(config-if)#ip address 172.16.1.1 255.255.255.252 R1(config-if)#ipv6 address 2001:DB8:ACAD:1::1/64 R1(config-if)#clock rate 128000 R1(config-if)#no shutdown %LINK-5-CHANGED: Interface Serial0/0/0, changed state to down R1(config-if)# En este paso se configura la interface serial 0/0/0 poniéndole una descripción, se configura el direccionamiento IPv4 e IPv6 y el clock rate por ser una conexión serial DCE.
Rutas predeterminadas	R1(config-if)#ip route 0.0.0.0 0.0.0.0 serial0/0/0 %Default route without gateway, if not a point-to-point interface, may impact performance R1(config)#ipv6 route ::/0 serial 0/0/0 R1(config)# Se crean en este paso rutas por defecto o predeterminadas para direccionamiento IPv4 e IPv6 para que se direccionen todos los paquetes dirigidos a redes que no estén en la tabla de enrutamiento a la interface serial 0/0/0

Nota: Todavía no se configura G0/1en este paso como lo pide el ejercicio.

11.3 Configuración de router 2

Tabla 15. Tareas de configuración en el router 1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router>enable Router#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Router(config)#no ip domain-lookup Router(config)# El comando **no ip domain-lookup** desactiva la traducción de nombres a dirección del dispositivo, se ahorra tiempo cuando se escribe mal un comando y el dispositivo no tratara de traducirlo.
Nombre del router	Router(config)#hostname R2 Se debe cambiar el nombre de cada dispositivo usando el comando **hostname** para identificarlo en la red fácilmente.
Contraseña de exec privilegiado cifrada	R2(config)#enable secret class Este comando proporciona mayor seguridad a la contraseña de enable ya que la encripta con MD5.
Contraseña de acceso a la consola	R2(config)#line console 0 R2(config-line)#password cisco R2(config-line)#login En este paso lo que se hace es configurar un password que debe escribir todo aquel que trate de acceder por el puerto de consola al dispositivo.

Contraseña de acceso Telnet	R2(config)#line vty 0 15 R2(config-line)#password cisco R2(config-line)#login En este paso se habilita el acceso por las líneas vty las cuales permiten el acceso a un dispositivo cisco a través de telnet o ssh. Por lo general un dispositivo cisco tiene 16 lineas vty. Al escribir el comando **password cisco**, y luego **login**, se le indica al router que debe permitir ingreso solo si se introduce esa contraseña establecida.
Cifrar las contraseñas de texto no cifrado	R2(config)#service password-encryption Este commando aplica un cifrado básico a los password que se encuentren sin encriptar.
Habilitar el servidor HTTP	R2(config)#ip http server ^ % Invalid input detected at '^' marker. R2(config)# Packet tracerno soporta este comando, este comando se usa para habilitar servidor http.
Mensaje MOTD	R2(config)#banner motd # Se prohibe el acceso no autorizado!# Es importante configurar este mensaje en cada dispositivo y sirve para notificaciones legales y advertencias para todo aquel que se conecte al dispositivo.

Interface S0/0/0	R2(config)#interface serial 0/0/0 R2(config-if)#description conexion_R1 R2(config-if)#ip address 172.16.1.2 255.255.255.252 R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64 R2(config-if)#no shutdown R2(config-if)# %LINK-5-CHANGED: Interface Serial0/0/0, changed state to up R2(config-if)# En este paso se configura la interface serial 0/0/0 poniendole una descripción, se configura el direccionameinto IPv4 e IPv6 y se habilita con el comando **no shutdown.**
Interface S0/0/1	R2(config)#interface serial 0/0/1 R2(config-if)#description conexion_R3 R2(config-if)#ip address 172.16.2.2 255.255.255.252 R2(config-if)#ipv6 address 2001:DB8:ACAD:2::2/64 R2(config-if)#clock rate 128000 R2(config-if)#no shutdown %LINK-5-CHANGED: Interface Serial0/0/1, changed state to down R2(config-if)# En este paso se configura la interface serial 0/0/1 poniendole una descripción, se configura el direccionameinto IPv4 e IPv6 y el clock rate por ser una conexión serial DCE. Se habilita la interface con el comando **no shutdown.**

Interface G0/0 (simulación de Internet)	R2(config)#interface gigabitEthernet 0/0 R2(config-if)#description conexion_Internet R2(config-if)#ip address 209.165.200.233 255.255.255.248 R2(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64 R2(config-if)#no shutdown R2(config-if)# %LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up R2(config-if)# En este paso se configura la interface gigabitEthernet 0/0 poniendole una descripción, se configura el direccionameinto IPv4 e IPv6 y se habilita con el comando **no shutdown.**
Interface loopback 0 (servidor web simulado)	R2(config)#interface loopback 0 R2(config-if)#description servidor web simulado R2(config-if)#ip address 10.10.10.10 255.255.255.255 R2(config-if)# En este paso se configura la interface loopback 0 la cual es una interface lógica, poniéndole una descripción y se configura el direccionamiento IPv4, esta interface es para simulación y no va asociada a un puerto físico.
Ruta predeterminada	R2(config)#ip route 0.0.0.0 0.0.0.0 giga0/0 %Default route without gateway, if not a point-to-point interface, may impact performance R2(config)#ipv6 route ::/0 giga0/0 R2(config)# Se crean en este paso rutas por defecto o predeterminadas para direccionamiento IPv4 e IPv6 para que se direccionen todos los paquetes dirigidos a redes que no estén en la tabla de enrutamiento a la interface Giga 0/0.

11.4 Configuración de router 3

Tabla 16. Tareas de configuración en el router 3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router>enable Router#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Router(config)#no ip domain-lookup Router(config)# El comando **no ip domain-lookup** desactiva la traducción de nombres a dirección del dispositivo, se ahorra tiempo cuando se escribe mal un comando y el dispositivo no tratara de traducirlo.
Nombre del router	Router(config)#hostname R3 R3(config)# Se debe cambiar el nombre de cada dispositivo usando el comando **hostname** para identificarlo en la red fácilmente.
Contraseña de exec privilegiado cifrada	R3(config)#enable secret class Este comando proporciona mayor seguridad a la contraseña de enable ya que la encripta con MD5.
Contraseña de acceso a la consola	R3(config)#line console 0 R3(config-line)#password cisco R3(config-line)#login En este paso lo que se hace es configurar un password que debe escribir todo aquel que trate de acceder por el puerto de consola al dispositivo.

Contraseña de acceso Telnet	R3(config)#line vty 0 15 R3(config-line)#password cisco R3(config-line)#login En este paso se habilita el acceso por las líneas vty las cuales permiten el acceso a un dispositivo cisco a través de telnet o ssh. Por lo general un dispositivo cisco tiene 16 lineas vty. Al escribir el comando **password cisco**, y luego **login**, se le indica al router que debe permitir ingreso solo si se introduce esa contraseña establecida.
Cifrar las contraseñas de texto no cifrado	R3(config)#service password-encryption Este commando aplica un cifrado básico a los password que se encuentren sin encriptar.
Mensaje MOTD	R3(config)#banner motd # Se prohibe el acceso no autorizado!# Es importante configurar este mensaje en cada dispositivo y sirve para notificaciones legales y advertencias para todo aquel que se conecte al dispositivo.
Interface S0/0/1	R3(config)#interface serial 0/0/1 R3(config-if)#description conexion_R2 R3(config-if)#ip address 172.16.2.1 255.255.255.252 R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64 R3(config-if)#no shutdown R3(config-if)# %LINK-5-CHANGED: Interface Serial0/0/1, changed state to up R3(config-if)# En este paso se configura la interface serial 0/0/1 poniéndole una descripción, se configura el direccionamiento IPv4 e IPv6 y se habilita con el comando **no shutdown.**

Interface loopback 4	R3(config-if)#interface loopback 4 R3(config-if)#ip address 192.168.4.1 255.255.255.0 En este paso se configura la interface loopback 4 la cual es una interface lógica, se configura el direccionamiento IPv4, esta interface es para simulación y no va asociada a un puerto físico.
Interface loopback 5	R3(config)#interface loopback 5 R3(config-if)#ip address 192.168.5.1 255.255.255.0 En este paso se configura la interface loopback 5 la cual es una interface lógica, se configura el direccionamiento IPv4, esta interface es para simulación y no va asociada a un puerto físico.
Interface loopback 6	R3(config)#interface loopback 6 R3(config-if)#ip address 192.168.6.1 255.255.255.0 En este paso se configura la interface loopback 6 la cual es una interface lógica, se configura el direccionamiento IPv4, esta interface es para simulación y no va asociada a un puerto físico.
Interface loopback 7	R3(config-if)#interface loopback 7 R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64 En este paso se configura la interface loopback 7 la cual es una interface lógica, se configura el direccionamiento IPv6, esta interface es para simulación y no va asociada a un puerto físico.

Rutas predeterminadas	R3(config)#ip route 0.0.0.0 0.0.0.0 serial 0/0/1 %Default route without gateway, if not a point-to-point interface, may impact performance R3(config)#ipv6 route ::/0 serial 0/0/1 R3(config)# Se crean en este paso rutas por defecto o predeterminadas para direccionamiento IPv4 e IPv6 para que se direccionen todos los paquetes dirigidos a redes que no estén en la tabla de enrutamiento a la interface serial 0/0/1.

11.5 Configuración de switch 1

Tabla 17. Tareas de configuración en el switch 1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch>enable Switch#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#no ip domain-lookup El comando **no ip domain-lookup** desactiva la traducción de nombres a dirección del dispositivo, se ahorra tiempo cuando se escribe mal un comando y el dispositivo no tratara de traducirlo.
Nombre del switch	Switch(config)#hostname S1 Se debe cambiar el nombre de cada dispositivo usando el comando **hostname** para identificarlo en la red fácilmente.

Contraseña de exec privilegiado cifrada	S1(config)#enable secret class Este comando proporciona mayor seguridad a la contraseña de enable ya que la encripta con MD5.
Contraseña de acceso a la consola	S1(config)#line console 0 S1(config-line)#password cisco S1(config-line)#login En este paso lo que se hace es configurar un password que debe escribir todo aquel que trate de acceder por el puerto de consola al dispositivo.
Contraseña de acceso Telnet	S1(config)#line vty 0 15 S1(config-line)#password cisco S1(config-line)#login En este paso se habilita el acceso por las líneas vty las cuales permiten el acceso a un dispositivo cisco a través de telnet o ssh. Por lo general un dispositivo cisco tiene 16 lineas vty. Al escribir el comando **password cisco**, y luego **login**, se le indica al router que debe permitir ingreso solo si se introduce esa contraseña establecida.
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption Este commando aplica un cifrado básico a los password que se encuentren sin encriptar.
Mensaje MOTD	S1(config)#banner motd # Se prohibe el acceso no autorizado!# Es importante configurar este mensaje en cada dispositivo y sirve para notificaciones legales y advertencias para todo aquel que se conecte al dispositivo.

11.6 Configuración del switch 3

Tabla 18. Tareas de configuración en el switch 3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#no ip domain-lookup El comando **no ip domain-lookup** desactiva la traducción de nombres a dirección del dispositivo, se ahorra tiempo cuando se escribe mal un comando y el dispositivo no tratara de traducirlo.
Nombre del switch	Switch(config)#hostname S3 Se debe cambiar el nombre de cada dispositivo usando el comando **hostname** para identificarlo en la red fácilmente.
Contraseña de exec privilegiado cifrada	S3(config)#enable secret class Este comando proporciona mayor seguridad a la contraseña de enable ya que la encripta con MD5.
Contraseña de acceso a la consola	S3(config)#line console 0 S3(config-line)#password cisco S3(config-line)#login En este paso lo que se hace es configurar un password que debe escribir todo aquel que trate de acceder por el puerto de consola al dispositivo.

Contraseña de acceso Telnet	S3(config)#line vty 0 15 S3(config-line)#password cisco S3(config-line)#login En este paso se habilita el acceso por las líneas vty las cuales permiten el acceso a un dispositivo cisco a través de telnet o ssh. Por lo general un dispositivo cisco tiene 16 lineas vty. Al escribir el comando **password cisco**, y luego **login**, se le indica al router que debe permitir ingreso solo si se introduce esa contraseña establecida.
Cifrar las contraseñas de texto no cifrado	S3(config)#service password-encryption Este commando aplica un cifrado básico a los password que se encuentren sin encriptar.
Mensaje MOTD	S3(config)#banner motd # Se prohibe el acceso no autorizado!# Es importante configurar este mensaje en cada dispositivo y sirve para notificaciones legales y advertencias para todo aquel que se conecte al dispositivo.

12. Verificar la conectividad de la red

En este paso verifica la conectividad entre dispositivos usando el comando ping, el comando ping (Packet Internet Groper) es un método muy común para resolver problemas la accesibilidad de dispositivo. Utiliza dos mensajes de consulta del Protocolo de mensajes de control de Internet (ICMP), solicitudes de eco ICMP y respuestas de eco ICMP para determinar si un host remoto se encuentra activo. El comando ping también calcula la cantidad de tiempo necesario para recibir la respuesta de eco.

Tabla 19. Verificación de la conectividad de la red

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	Responde correctamente, ver figura 13
R2	R3, S0/0/1	172.16.2.1	Responde correctamente, ver figura 14
PC de Internet	Gateway predeterminado	209.265.200.233	Responde correctamente, ver figura 15

A continuación, las evidencias de los ping realizados en el entorno de simulación de Cisco Packet Tracerpara este paso.

Figura 14. Verificación de conectividad de router 1 a router 2

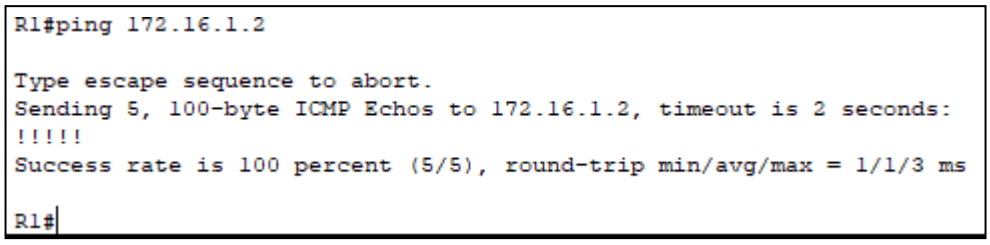
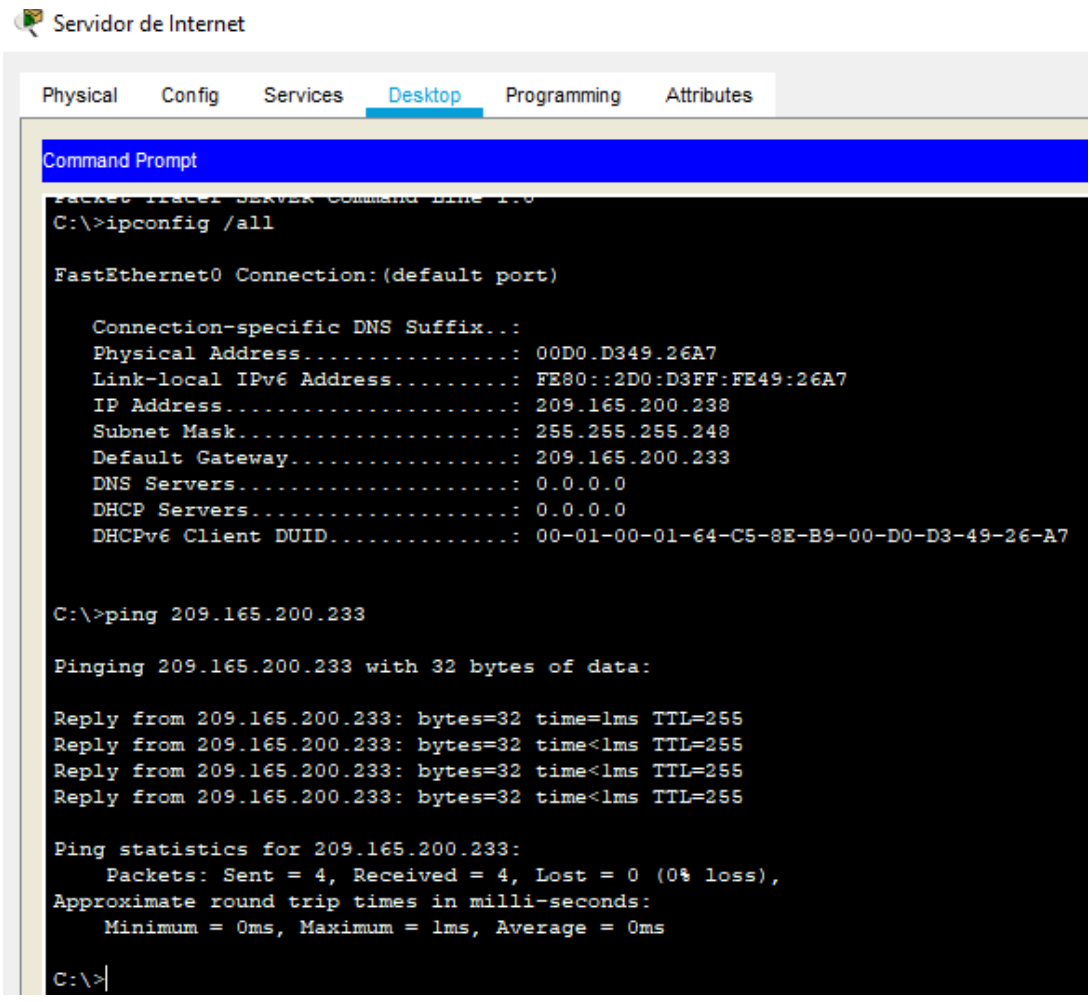


Figura 15. Verificación de conectividad de router 2 a router 3

```
R2#ping 172.16.2.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms

R2#
```

Figura 16. Verificación de conectividad de PC de internet a gateway



13. Configurar la seguridad del switch, las VLAN y el routing entre VLAN

13.1 Configuración de switch 1

Tabla 20. Tareas de configuración realizadas en switch 1

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	S1(config)#vlan 21 S1(config-vlan)#name contabilidad S1(config-vlan)#exit S1(config)#vlan 23 S1(config-vlan)#name ingenieria S1(config-vlan)#exit S1(config)#vlan 99 S1(config-vlan)#name administracion S1(config-vlan)# En este paso se crean todas las vlan que se van a usar ya que por defecto el switch solo tiene creada la vlan 1. Se podrían crear varias vlan al tiempo si son consecutivas, pero es mejor crear una a una para ponerles un nombre.
Asignar la dirección IP de administración.	S1(config)#interface vlan 99 S1(config-if)#description administracion switch S1(config-if)#ip address 192.168.99.2 255.255.255.0 S1(config-if)#no shutdown S1(config-if)# Se crea una interface vlan con la vlan 99 que es la de administración con el comando **interface vlan 99**, luego dentro de esta interface se configura una descripción y direccionamiento IPv4, por último con el comando **no shutdown** activamos la interface.

Asignar el gateway predeterminado	S1(config)#ip default-gateway 192.168.99.1 Si el switch se va a administrar de forma remota desde redes que no están conectadas directamente, se debe configurar con un gateway predeterminado que será la IP 192.168.99.1 que irá en el router.
Forzar el enlace troncal en la interface F0/3	S1(config)#interface fastEthernet 0/3 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1 S1(config-if)#no shutdown Con el comando **switchport mode trunk** se forza al Puerto a trabajar en troncal y permitira todas las vlan a menos que se definan en un listado. Por defecto la vlan 1 es la vlan nativa sin embargo se pone el commando **switchport trunk native vlan 1.**
Forzar el enlace troncal en la interface F0/5	S1(config)#interface fastEthernet 0/5 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1 S1(config-if)#no shutdown Con el comando **switchport mode trunk** se forza al Puerto a trabajar en troncal y permitirá todas las vlan a menos que se definan en un listado. Por defecto la vlan 1 es la vlan 74ative sin embargo se pone el commando **switchport trunk native vlan 1.**
Configurar el resto de los puertos como puertos de acceso	S1(config)#interface range fa 0/1-2, fa 0/4, fa 0/6-24, g0/1-2 S1(config-if-range)#switchport mode access Con ayuda del comando interface range se puede seleccionar varios puertos al mismo tiempo en caso de que la configuración sea repetitiva en cada uno de ellos, con el comando **switchport mode access** se deja en puerto en acceso pero se debe definir una vlan.

Asignar F0/6 a la VLAN 21	S1(config)#interface fastEthernet 0/6 S1(config-if)#description conexion PC-A S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 21 En este paso se pone el puerto en modo acceso con el comando **switchport mode access** y se le indica al switch que en este puerto permita la conectividad en acceso por la vlan 21 con el comando **switchport access vlan 21.**
Apagar todos los puertos sin usar	S1(config)#interface range fa 0/1-2, fa 0/4, fa 0/7-24, g0/1-2 S1(config-if-range)#shutdown En este paso se seleccionan todos los puertos en una misma línea con ayuda del comando **interface range**, luego de haber nombrado todos los puertos deseados en la línea se pueden apagar todos al mismo tiempo con el comando **shutdown.**

13.2 Configuración de switch 3

Tabla 21. Tareas de configuración realizadas en switch 3

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	S3#configure terminal S3(config)#vlan 21 S3(config-vlan)#name contabilidad S3(config-vlan)#vlan 23 S3(config-vlan)#name ingenieria S3(config-vlan)#vlan 99 S3(config-vlan)#name administración En este paso se crean todas las vlan que se van a usar ya que por defecto el switch solo tiene creada la vlan 1. Se podrían crear varias vlan al tiempo si son consecutivas pero es mejor crear una a una para ponerles un nombre.

Asignar la dirección IP de administración	S3(config-if)#interface vlan 99 S3(config-if)#description administracion switch S3(config-if)#ip address 192.168.99.3 255.255.255.0 S3(config-if)#no shutdown Se crea una interface vlan con la vlan 99 que es la de administración con el comando **interface vlan 99**, luego dentro de esta interface se configura una descripción y direccionamiento IPv4, por último con el comando **no shutdown** activamos la interface.
Asignar el gateway predeterminado.	S3(config)#ip default-gateway 192.168.99.1 Si el switch se va a administrar de forma remota desde redes que no están conectadas directamente, se debe configurar con un gateway predeterminado que será la IP 192.168.99.1 que irá en el router.
Forzar el enlace troncal en la interface F0/3	S3(config)#interface fastEthernet 0/3 S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1 Con el comando **switchport mode trunk** se forza al puerto a trabajar en troncal y permitirá todas las vlan a menos que se definan en un listado. Por defecto la vlan 1 es la vlan nativa sin embargo se pone el commando **switchport trunk native vlan 1.**
Configurar el resto de los puertos como puertos de acceso	S3(config)#interface range fa 0/1-2, fa0/4-24, g0/1-2 S3(config-if-range)#switchport mode access Con ayuda del comando interface range se puede seleccionar varios puertos al mismo tiempo en caso de que la configuración sea repetitiva en cada uno de ellos, con el comando **switchport mode access** se deja en puerto en acceso pero se debe definir una vlan.

Asignar F0/18 a la VLAN 23	S3(config)#interface fastEthernet 0/18 S3(config-if)#description conexion PC-C S3(config-if)#switchport mode access S3(config-if)#switchport access vlan 23 En este paso se pone el puerto en modo acceso con el comando **switchport mode access** y se le indica al switch que en este puerto permita la conectividad en acceso por la vlan 21 con el comando **switchport access vlan 23.**
Apagar todos los puertos sin usar	S3(config)#interface range fa 0/1-2, fa0/4-17, fa0/19-24, g0/1-2 S3(config-if-range)#shutdown En este paso se seleccionan todos los puertos en una misma línea con ayuda del comando **interface range**, luego de haber nombrado todos los puertos deseados en la línea se pueden apagar todos al mismo tiempo con el comando **shutdown.**

13.3. Configuración de router 1

Tabla 22. Tareas de configuración realizadas en router 1

Elemento o tarea de configuración	Especificación
Configurar la subinterface 802.1Q .21 en G0/1	R1(config)#interface gigabitEthernet 0/1.21 R1(config-subif)#description LAN_Contabilidad R1(config-subif)#encapsulation dot1q 21 R1(config-subif)#ip address 192.168.21.1 255.255.255.0 En este paso se crean subinterfaces que son interfaces virtuales sobre un puerto físico, así el router podrá mantener separado el tráfico de cada subinterfaces la cual va asociada a una vlan en este caso la vlan 21.

Configurar la subinterface 802.1Q .23 en G0/1	R1(config)#interface gigabitEthernet 0/1.23 R1(config-subif)#description LAN_Ingenieria R1(config-subif)#encapsulation dot1q 23 R1(config-subif)#ip address 192.168.23.1 255.255.255.0 En este paso se crean subinterfaces que son interfaces virtuales sobre un puerto físico, así el router podrá mantener separado el tráfico de cada subinterfaces la cual va asociada a una vlan en este caso la vlan 23.
Configurar la subinterface 802.1Q .99 en G0/1	R1(config)#interface gigabitEthernet 0/1.99 R1(config-subif)#description LAN_Administracion R1(config-subif)#encapsulation dot1q 99 R1(config-subif)#ip address 192.168.99.1 255.255.255.0 En este paso se crean subinterfaces que son interfaces virtuales sobre un puerto físico, así el router podrá mantener separado el tráfico de cada subinterfaces la cual va asociada a una vlan en este caso la vlan 99.
Activar la interface G0/1	R1(config)#interface gigabitEthernet 0/1 R1(config-if)#no shutdown En este paso se habilita el puerto físicio Giga0/1 lo cual es necesario para que suban también las subinterfaces que van asociadas a este puerto.

14. Verificar la conectividad de la red

En este paso verifica la conectividad entre dispositivos usando el comando ping, el comando ping (Packet Internet Groper) es un método muy común para resolver problemas la accesibilidad de dispositivo. Utiliza dos mensajes de consulta del Protocolo de mensajes de control de Internet (ICMP), solicitudes de eco ICMP y respuestas de eco ICMP para determinar si un host remoto se encuentra activo. El comando ping también calcula la cantidad de tiempo necesario para recibir la respuesta de eco.

Tabla 23. Verificación de conectividad entre dispositivos

Desde	A	Dirección IP	Resultados de ping
S1	R1, IP VLAN 99	192.168.99.1	Responde correctamente, ver figura 16
S3	R1, IP VLAN 99	192.168.99.1	Responde correctamente, ver figura 17
S1	R1, IP VLAN 21	192.168.21.1	Responde correctamente, ver figura 16
S3	R1, IP VLAN 23	192.168.23.1	Responde correctamente, ver figura 17

A continuación las evidencias de los ping realizados en el entorno de simulación de Cisco Packet Tracerpara este paso.

Figura 17. Verificación de conectividad de switch 1 a router 1

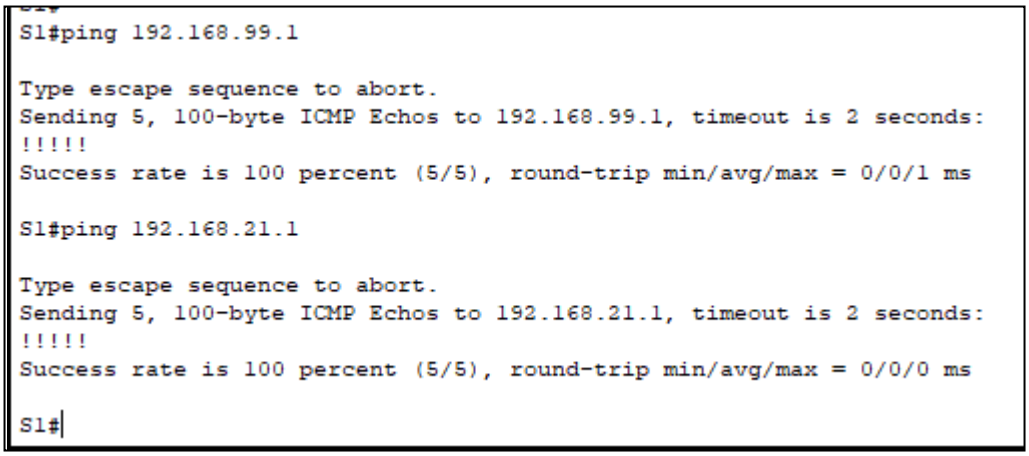
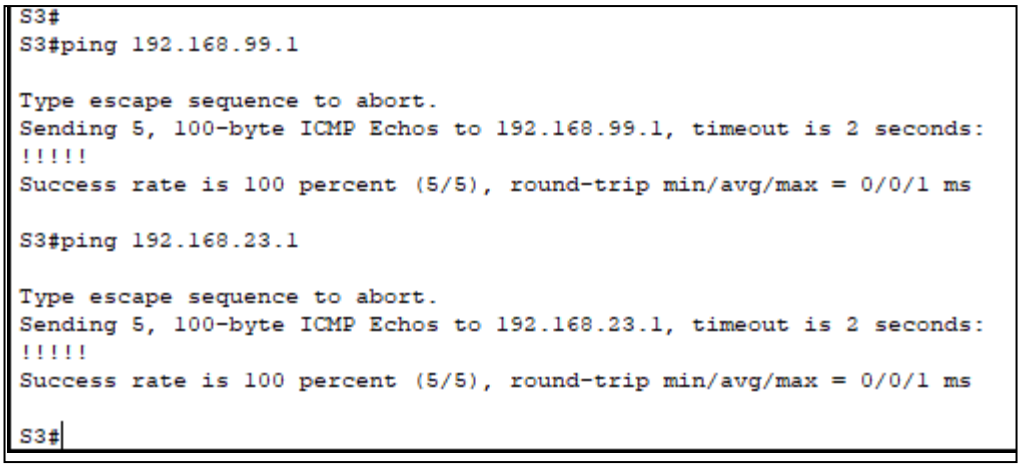


Figura 18. Verificación de conectividad de switch 3 a router 1



15. Configuración del protocolo de routing dinámico OSPF

15.1 Configuración de protocolo OSPF en el router 1

Tabla 24. Tareas de configuración realizadas en el router 1

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R1(config)#router ospf 1 R1(config-router)#router-id 1.1.1.1 En este paso se habilita se habilita el protocolo de enrutamiento OSPF en el router, se configura el ID 1 y el router ID 1.1.1.1 que identifica el dispositivo que origina o procesa información del protocolo, por defecto cuando el OSPF es área única se deja 0.
Anunciar las redes conectadas directamente	R1(config-router)#network 172.16.1.0 0.0.0.3 area 0 R1(config-router)#network 192.168.21.0 0.0.0.255 area 0 R1(config-router)#network 192.168.23.0 0.0.0.255 area 0 R1(config-router)#network 192.168.99.0 0.0.0.255 area 0 En este paso se especifican las redes por las que se enviarán los mensajes de actualización de rutas. Cada red se debe identificar con un área a la cual pertenece y se configuran con la máscara wildcard.
Establecer todas las interfaces LAN como pasivas	R1(config-router)#passive-interface gigabitEthernet 0/1.21 R1(config-router)#passive-interface gigabitEthernet 0/1.23 R1(config-router)#passive-interface gigabitEthernet 0/1.99 En este paso se usa el comando passive-interface que evita que se envíen actualizaciones de routing a través de la interface de router especificada. Esto se hace comúnmente para reducir el tráfico en las redes LAN.
Desactive la sumarización automática	Al ingresar este commando **no auto-summary** le decimos al router que no sumarize las rutas que tiene. Es de gran utilidad cuando no tenemos redes contiguas, sin embargo OSPF no autosumariza.

15.2 Configuración de protocolo OSPF en el router 2

Tabla 25. Tareas de configuración realizadas en el router 2

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R2(config)#router ospf 1 R2(config-router)#router-id 2.2.2.2 En este paso se habilita se habilita el protocolo de enrutamiento OSPF en el router, se configura el ID 1 y el router ID 1.1.1.1 que identifica el dispositivo que origina o procesa información del protocolo, por defecto cuando el OSPF es área única se deja 0.
Anunciar las redes conectadas directamente	R2(config-router)#network 172.16.1.0 0.0.0.3 area 0 R2(config-router)#network 172.16.2.0 0.0.0.3 area 0 En este paso se especifican las redes por las que se enviarán los mensajes de actualización de rutas. Cada red se debe identificar con un área a la cual pertenece y se configuran con la máscara wildcard.
Establecer la interface LAN (loopback) como pasiva	R2(config-router)#passive-interface loopback 0 En este paso se usa el comando passive-interface que evita que se envíen actualizaciones de routing a través de la interface de router especificada. Esto se hace comúnmente para reducir el tráfico en las redes LAN.
Desactive la sumarización automática.	Al ingresar este commando **no auto-summary** le decimos al router que no sumarize las rutas que tiene. Es de gran utilidad cuando no tenemos redes contiguas, sin embargo OSPF no autosumariza.

15.3 Tareas de configuración de protocolo OSPFv3 en el router 3

Tabla 26. Tareas de configuración realizadas en el router 2

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R3(config)#ipv6 router ospf 1 R3(config-rtr)#router-id 3.3.3.3 En este paso se habilita se habilita el protocolo de enrutamiento OSPF en el router, OSPFv3 está definido para redes IPv6 al contrario de la versión OSPFv2 definida para IPv4. se configura el ID 1 y el router ID 3.3.3.3 que identifica el dispositivo que origina o procesa información del protocolo.
Anunciar redes IPv4 conectadas directamente	R3(config)#interface serial 0/0/1 R3(config-if)#ipv6 ospf 1 área 0 En este paso no se usa como en la versión OSPFv2 La instrucción network se eliminó en OSPFv3. En cambio, el routing OSPFv3 se habilita en el nivel de la interface.
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	R3(config-rtr)#passive-interface loopback 4 R3(config-rtr)#passive-interface loopback 5 R3(config-rtr)#passive-interface loopback 6 R3(config-rtr)#passive-interface loopback 7 En este paso se usa el comando passive-interface que evita que se envíen actualizaciones de routing a través de la interface de router especificada. Esto se hace comúnmente para reducir el tráfico en las redes LAN.
Desactive la sumarización automática.	Al ingresar este commando **no auto-summary** le decimos al router que no sumarize las rutas que tiene. Es de gran utilidad cuando no tenemos redes contiguas, sin embargo OSPF no autosumariza.

16. Verificar la información de OSPF

En este paso se verifica el funcionamiento del protocolo OSPF, básicamente OSPF traza un mapa completo de toda la red y luego escoge el camino de menor costo basándose en dicho mapa. Con este protocolo cada enrutador posee un mapa completo de toda la red.

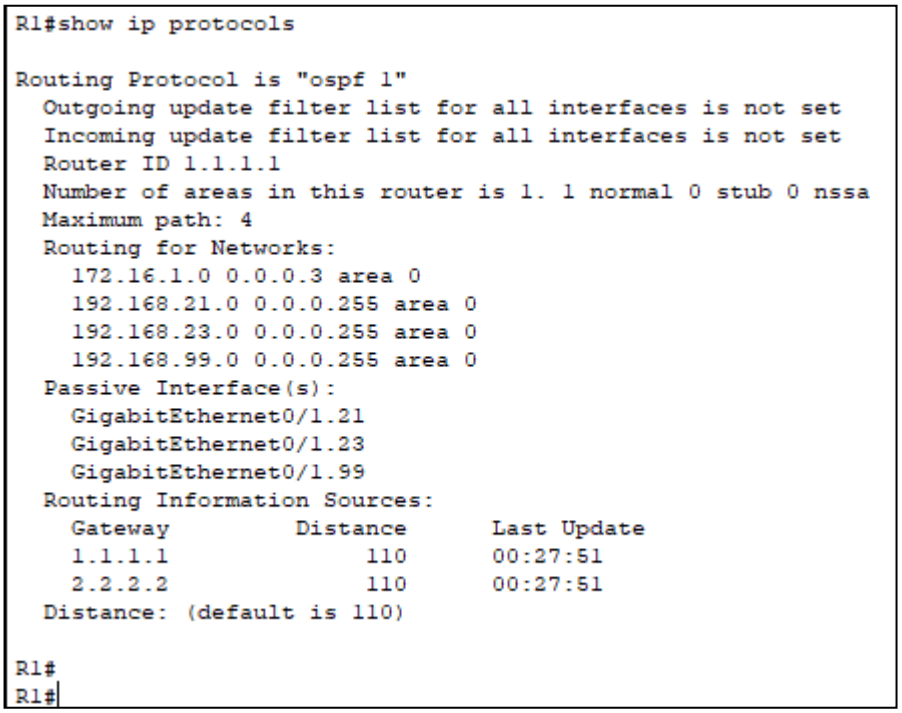
OSPF es un protocolo de estado de enlace; en otras palabras, basa su funcionamiento en estados de conexión de red, o bien en enlaces. En OSPF, el componente más importante a la hora de calcular la topología es el estado de cada enlace en cada enrutador.

Tabla 27. Verificación del funcionamiento del protocolo OSPF

Pregunta	Respuesta
¿Con qué comando se muestran la ID del proceso OSPF, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router?	R1#show ip protocols Al aplicar este commando en el router se muestra esta información, ver figura 18
¿Qué comando muestra solo las rutas OSPF?	R1#show ip route ospf Este comando se utiliza para mostrar solo las rutas OSPF, ver figura 19
¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	**show running-config ospf** es una posibilidad y otro comando es **show running-config | section** pero el simulador Packet tracerno los soporta.

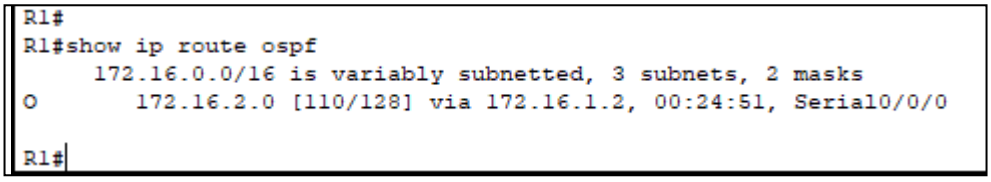
A continuación las imágenes tomadas de la simulación del escenario en el software Packet Traceren donde se confirma el funcionamiento del OSPF.

Figura 19. Verificación del funcionamiento de OSPF



```
R1#show ip protocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 1.1.1.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.16.1.0 0.0.0.3 area 0
    192.168.21.0 0.0.0.255 area 0
    192.168.23.0 0.0.0.255 area 0
    192.168.99.0 0.0.0.255 area 0
  Passive Interface(s):
    GigabitEthernet0/1.21
    GigabitEthernet0/1.23
    GigabitEthernet0/1.99
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1              110      00:27:51
    2.2.2.2              110      00:27:51
  Distance: (default is 110)

R1#
R1#
```

Figura 20. Verificación del funcionamiento de OSPF



```
R1#
R1#show ip route ospf
     172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
O       172.16.2.0 [110/128] via 172.16.1.2, 00:24:51, Serial0/0/0

R1#
```

17. Implementar DHCP y NAT para IPv4

DHCP funciona sobre un servidor central (servidor, estación de trabajo o incluso un PC) el cual asigna direcciones IP a otras máquinas de la red. Este protocolo puede entregar información IP en una LAN o entre varias VLAN. Esta tecnología reduce el trabajo de un administrador, que de otra manera tendría que visitar todos los ordenadores o estaciones de trabajo uno por uno.

El protocolo NAT, que significa Network Adress Translation o Traducción de direcciones de red en español se utiliza en las redes bajo el protocolo IP y nos permite el intercambio de paquetes entre dos redes que tienen asignadas mutuamente direcciones IP incompatibles.

17.1 Configuración de router 1 como servidor de DHCP para VLAN 21 y 23

Tabla 28. Tareas de configuración realizadas en el router 1

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20 Para excluir direcciones específicas se utiliza el comando **ip dhcp excluded-address**, así se excluyen las direcciones indicadas y no serán asignadas por el protocolo dhcp a ningún dispositivo.
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20 Para excluir direcciones específicas se utiliza el comando **ip dhcp excluded-address**, así se excluyen las direcciones indicadas y no serán asignadas por el protocolo dhcp a ningún dispositivo.

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 En este paso se configura el pool dhcp con el comando **ip dhcp pool** con un nombre especifico. Con el comando **network** se define la red a utilizar, con el comando **default-router** se define el gateway predeterminado y con el comando **dns-server** se configura la dirección del servidor DNS que estara disponible, y con el comando **domain-name** se define un dominio.
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 En este paso se configura el pool dhcp con el comando **ip dhcp pool** con un nombre especifico. Con el comando **network** se define la red a utilizar, con el comando **default-router** se define el gateway predeterminado y con el comando **dns-server** se configura la dirección del servidor DNS que estara disponible, y con el comando **domain-name** se define un dominio.

17.2 Configurar la NAT estática y dinámica en el Router 2

El NAT estático consiste básicamente en un tipo de NAT en el cuál se mapea una dirección IP privada con una dirección IP pública de forma estática. De esta manera, cada equipo en la red privada debe tener su correspondiente IP pública asignada para poder acceder a Internet.

Por otro lado el NAT dinámico mejora varios aspectos del NAT estático dado que utiliza un pool de IPs públicas para un pool de IPs privadas que serán mapeadas de forma dinámica y a demanda.

Tabla 29. Tareas de configuración realizadas en el router 2

Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	R2(config)#username webuser privilege 15 secret cisco12345 En este paso se crea un usuario y contraseña con contraseña cifrada que se usará para ingresar al servidor web.
Habilitar el servicio del servidor HTTP	R2(config)#ip http server ^ % Invalid input detected at '^' marker. R2(config)# Packet Tracerno soporta este comando el cual se utiliza para activar el servidor http en el router que por defecto viene deshabilitado.
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	R2(config)#ip authentication local ^ % Invalid input detected at '^' marker. R2(config)# Packet Tracerno soporta este comando que se utiliza para habilitar la autenticación con el password creado anteriormente en la base de datos local.

Crear una NAT estática al servidor web.	R2(config)#ip nat inside source static 10.10.10.10 209.165.200.237 En este paso se configura el mapa estático para indicarle al router que traduzca entre la dirección privada del servidor interno 10.10.10.10 y la dirección pública 209.165.200.237.
Asignar la interface interna y externa para la NAT estática	R2(config)#interface gigabitEthernet 0/0 R2(config-if)#ip nat outside R2(config-if)#interface serial 0/0/1 R2(config-if)#ip nat inside En este paso se define cual será la interface de entrada y la de salida para las traslaciones.
Configurar la NAT dinámica dentro de una ACL privada	R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255 En este paso se crean las listas de control de acceso para cada red, esta lista de acceso permitirá que se traduzcan las redes allí permitidas.
Defina el pool de direcciones IP públicas utilizables.	R2(config)#ip nat pool INTERNET 209.165.200.233 209.165.200.236 netmask 255.255.255.248 En este paso se definen el conjunto de direcciones ip públicas utilizables.
Definir la traducción de NAT dinámica	R2(config)#ip nat inside source list 1 pool INTERNET En este paso se configura la NAT dinámica que utiliza un conjunto de direcciones públicas y las asigna según el orden de llegada las direcciones que están disponibles.

17.3 Verificar el protocolo DHCP y la NAT estática

Tabla 30. Verificación del funcionamiento de protocolos DHCP y NAT

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	Recibió por DHCP la dirección 192.168.21.21/24, ver figura 20
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	Recibió por DHCP la dirección 192.168.23.21/24, ver figura 21
Verificar que la PC-A pueda hacer ping a la PC-C	Responde el ping correctamente, ver figura 22
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**	Esta prueba no se puede realizar en Packet tracer ya que el simulador no recibe el comando **ip http server** en el router, en una práctica real debería funcionar y nos logueamos con el usuario y password configurados.

Figura 21. Verificación de direccionamiento automático en PC-A

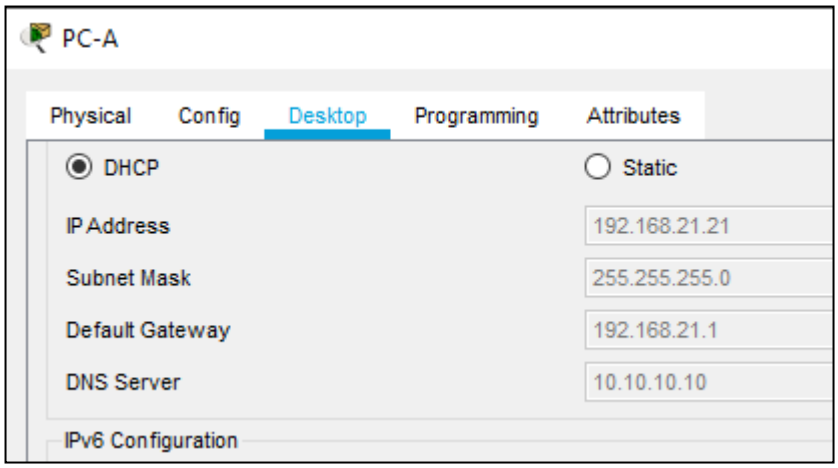
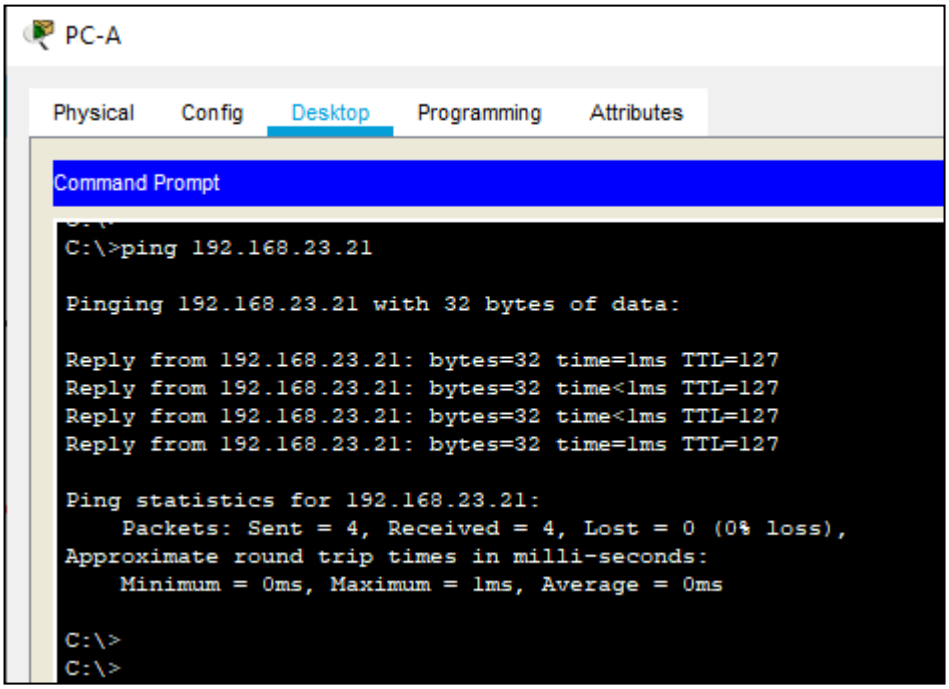


Figura 22. Verificación de direccionamiento automático en PC-C

Figura 23. Verificación de conectividad de PC-A a PC-C



18. Configurar NTP

Network Time Protocol (NTP) es un protocolo de Internet para sincronizar los relojes de los sistemas informáticos a través del enrutamiento de paquetes en redes con latencia variable. NTP utiliza UDP como su capa de transporte, usando el puerto 123. Está diseñado para resistir los efectos de la latencia variable.

Tabla 31. Tareas de configuración en router 2

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	R2#clock set 02:07:00 26 november 2020 Se configura la hora y fecha actualizada con este comando, es útil por ejemplo cuando se van a revisar los log de eventos y ver la hora correcta de cada evento.
Configure R2 como un maestro NTP.	R2(config)#ntp master 5 Con este comando se indica al router 2 que sea el servidor NTP autoritario, incluso si el sistema no se sincroniza a una fuente horaria exterior, el número 5 al final del comando indica el nivel de estrato en la jerarquia de servidores.
Configurar R1 como un cliente NTP.	R1(config)#ntp server 172.16.1.2 En este comando se inica la ip del servidor con el que sesincronizará la hora correcta.
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	R1(config)#ntp update-calendar Esto provoca que NTP actualice periódicamente (cada hora) el chip del reloj en routers de mayor capacidad.
Verifique la configuración de NTP en R1.	Con el comando **show ntp associations** se verifica que el dispositivo esta sincronizado con el servidor de NTP 172.16.1.2. ver figura 23.

Figura 24. Verificación de conectividad de PC-A a PC-C

```
R1#show ntp associations

address         ref clock       st   when     poll    reach  delay          offset            disp
 ~172.16.1.2    127.127.1.1     5    9        16      37     2.00           875308880457.00   0.12
 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
R1#
```

19. Configurar y verificar las listas de control de acceso (ACL)

Una lista de control de accesos (ACL) es una serie de instrucciones que controlan que en un router se permita el paso o se bloqueen los paquetes IP de datos, que maneja el equipo según la información que se encuentra en el encabezado de los mismos.

19.1 Restringir el acceso a las líneas VTY en el R2

Tabla 32. Tareas de configuración en router 2

Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	R2(config)#ip access-list standard ADMIN-MGT R2(config-std-nacl)#permit host 172.16.1.1 R2(config-std-nacl)#exit En este paso se configura una ACL estándar para que solo el router 1 pueda establecer conexión telnet con el router 2. Las ACL estándar comparan la dirección de origen de los paquetes IP con las direcciones configuradas en la ACL para controlar el tráfico.
Aplicar la ACL con nombre a las líneas VTY	R2(config)#line vty 0 15 R2(config-line)#access-class ADMIN-MGT in Luego de crear la ACL en el paso anterior ahora se aplica la ACL a las líneas vty del router para que funcione.
Permitir acceso por Telnet a las líneas de VTY	R2(config-line)#transport input telnet Se especifica en las líneas vty que permita el acceso por telnet con este comando.
Verificar que la ACL funcione como se espera	R1#telnet 172.16.1.2 Con este comando se confirma que ingresa sin problema el router 1 al router 2 y se verifica que no permita ingresar desde el router 3 como debe ser R3# telnet 172.16.1.2. Ver figura

Figura 25. Verificación de funcionamiento de la ACL

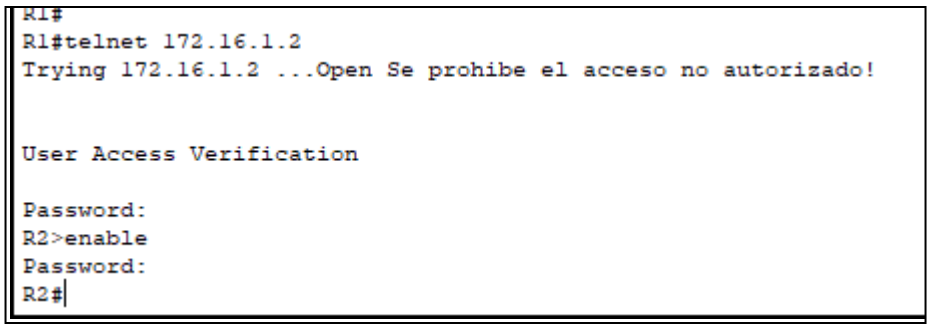
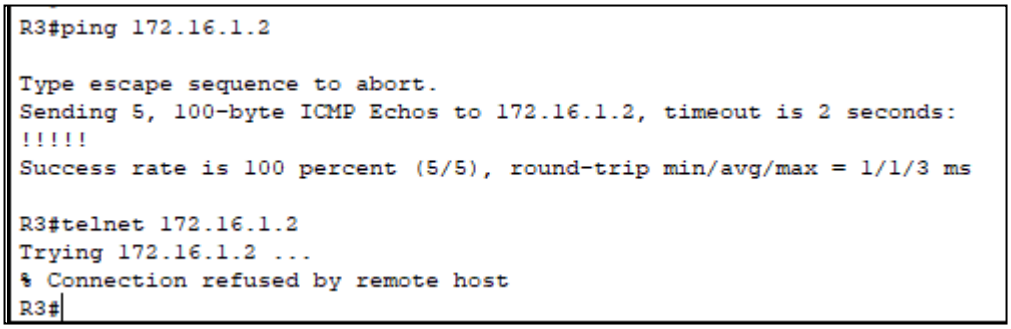


Figura 26. Verificación de funcionamiento de la ACL

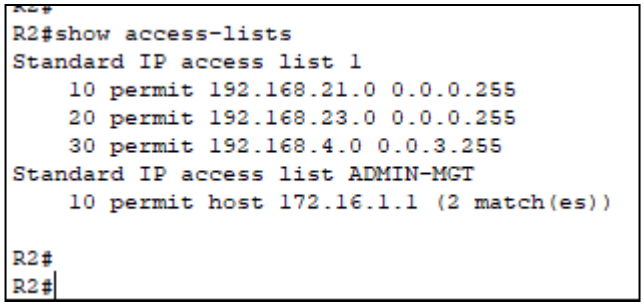


20. Introducir el comando de CLI adecuado para mostrar lo siguiente

Tabla 33. Comandos de verificación de Access-lis y NAT

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	R2# show access-lists En este paso al aplicar este comando se muestran las coincidencias que pueden ir aumentando, siempre el dispositivo hará un seguimiento de las estadísticas de coincidencias. Ver figura 24
Restablecer los contadores de una lista de acceso	R2#clear access-list counters Con este comando se pueden borrar los contadores, se puede utilizer solo o con el numero o nombre de un acces-list específica.
¿Qué comando se usa para mostrar qué ACL se aplica a una interface y la dirección en que se aplica?	R2#show ip interface Con este comando se verifica la ACL en la interface y el sentido en el que se aplicó. Ver figura 25.
¿Con qué comando se muestran las traducciones NAT?	R2#show ip nat translations Este comando muestra los detalles de las asignaciones de NAT, el comando muestra todas las traducciones estáticas que se configuraron y todas las traducciones dinámicas que se crearon a causa del tráfico. Ver figura 26
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	R2#clear ip nat translation * Con este comando se borran todas las traducciones de la tabla, es últil borrar las entradas dinámicas al probar la configuración NAT. Ver figura 29.

Figura 27. Verificación de coincidencias en access-list



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

R2#
R2#
```

Figura 28. Verificación de acces-list en interface

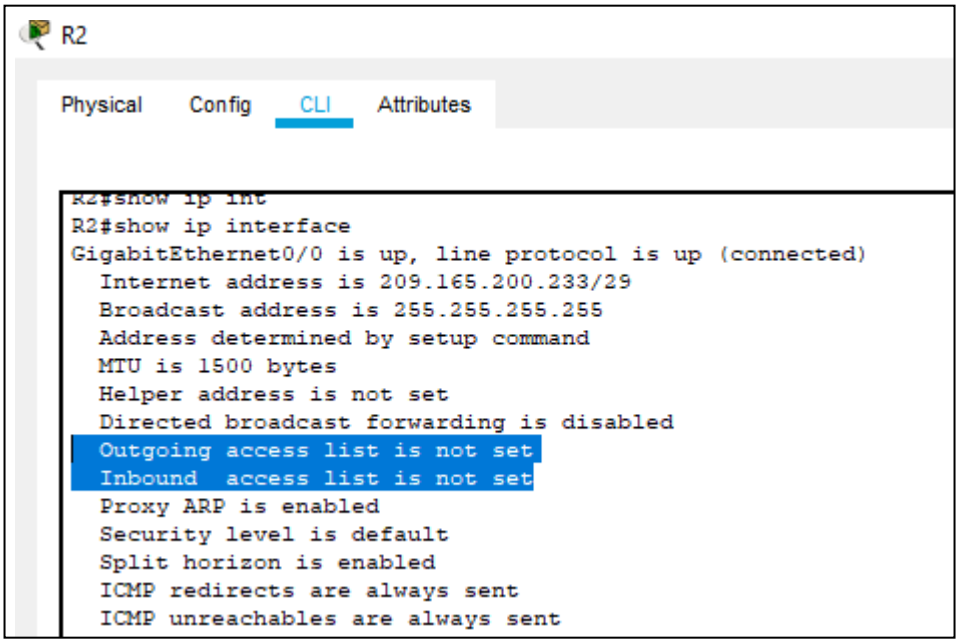
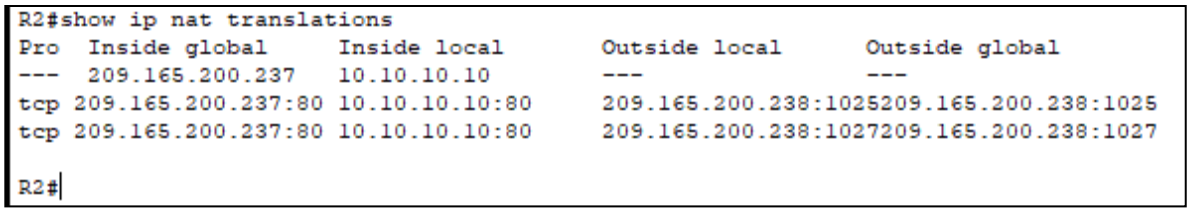


Figura 29. Verificación de traducciones NAT



```
R2#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
---  209.165.200.237   10.10.10.10        ---                ---
tcp 209.165.200.237:80 10.10.10.10:80     209.165.200.238:1025209.165.200.238:1025
tcp 209.165.200.237:80 10.10.10.10:80     209.165.200.238:1027209.165.200.238:1027

R2#
```

Figura 30. Verificación de conectividad de PC-A a servidor de internet

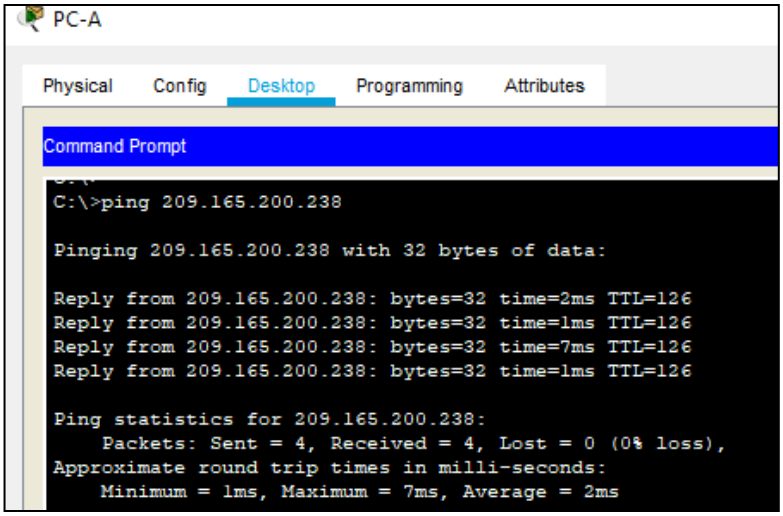


Figura 31. Verificación de conectividad de PC-C a servidor de internet

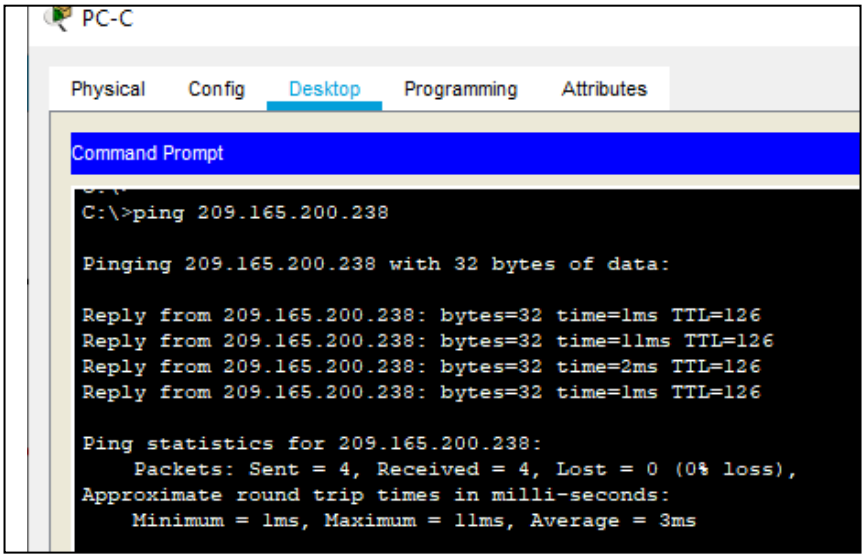


Figura 32. Eliminación de traducciones NAT dinámicas

```
R2#clear ip nat translation *
R2#
R2#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
---  209.165.200.237   10.10.10.10        ---                ---

R2#
```

CONCLUSIONES

El enrutamiento es fundamental para cualquier red de datos, ya que transfiere información a través de una internetwork de origen a destino. Los routers son dispositivos que se encargan de transferir paquetes de una red a la siguiente.

Existen protocolos de enrutamiento estático y dinámicos, el enrutamineto estático es generado por el propio administrador mientras que, con un protocolo de enrutamiento dinámico, el administrador sólo se encarga de configurar el protocolo de enrutamiento mediante comandos IOS, en todos los routers de la red y estos automáticamente intercambiarán sus tablas de enrutamiento con sus routers vecinos.

Una VLAN es un método para crear redes lógicas independientes dentro de una misma red física. Una de las ventajas principales de utilizar una VLAN es que reduce la latencia y la carga de tráfico de la red y los dispositivos, lo que ahorra recursos y mejora la eficacia del sistema.

Una de las principales ventajas del protocolo DHCP es que facilita la administración de las direcciones IP. En una red sin DHCP, debe asignar manualmente las direcciones IP. Debe asignar una dirección IP exclusiva a cada cliente y configurar cada uno de los clientes de modo individual.

El software Packet Tracer permite recrear un ambiente de red, con el fin de detectar y corregir errores en los sistemas de comunicaciones antes de colocarlo en ambiente real basados en la capas del modelo OSI.

Secure Shell (SSH) es un conjunto de estándares, también llamado protocolo, que brinda seguridad en las comunicaciones o transferencia de datos, entre el servidor remoto y el equipo cliente. Todos los datos son cifrados para garantizar que no es posible interceptar y ver el contenido de esas comunicaciones.

Los direccionadores o sistemas de una red OSPF, después de haberse asegurado de que sus interfaces son funcionales, envían en primer lugar paquetes Hello, utilizando el protocolo Hello por sus interfaces OSPF, para descubrir vecinos. Vecinos son los direccionadores o sistemas que tienen interfaces con la red común. Después, los direccionadores o sistemas vecinos intercambian sus bases de datos de enlace-estado para establecer adyacencias.

BIBILIOGRAFÍA

Cardona, I. (2020). Inicio de sesión de Adobe Connect. Retrieved 31 October 2020, from http://conferencia2.unad.edu.co/ecbti2020_4_1/

CISCO. (2014). Protocolos y comunicaciones de red. Fundamentos de Networking. Recuperado de:https://static-courseassets.s3.amazonaws.com/ITN50ES/module7/index.html#7.1.1.4

CISCO. (2020, 21 abril). Configure InterVLAN Routing on Layer 3 Switches. Configure InterVLAN Routing on Layer 3 Switches. https://www.cisco.com/c/en/us/support/docs/lan-switching/inter-vlanrouting/41860-howto-L3-intervlanrouting.html

Ramirez, D. (2020). Web Diplomado de Profundizacion Redes Cisco Unidad 4 y 5. Retrieved 31 October 2020, from http://conferencia2.unad.edu.co/p71qnm0eiq6s/?proto=true

Sepulveda, M. (2019). Configuración de 802 1Q y VLAN Nativa Cisco CCNA. Retrieved 31 October 2020, from https://www.youtube.com/watch?v=SvWghtGPPQ

Zalasar, P. (2020). CIPA 2 Prueba de Habilidades Diplomado Cisco (2020-10-16 at 16:04 GMT-7). Retrieved 31 October 2020, from https://drive.google.com/file/d/1XTTmvwmU_Z4SDMoRom6HeJSAJiqj_Q6/view

Calero Romero, J. (2014). EtherChannel03: EtherChannel. Ejemplo práctico I. Protocolo LACP. Retrieved 31 October 2020, from https://www.youtube.com/watch?v=SvWght-GPPQ

SIMULACIÓN DE UN ESCENARIO DE RED COMÚN EN EL MUNDO LABORAL O COPORPORATIVO BASADO EN TECNOLOGÍA CISCO

SIMULATION OF A COMMON NETWORK SCENARIO IN THE WORLD OF WORK OR CORPORATE BASED ON CISCO TECHNOLOGY

Yesid Arley Marroquín Ruiz
Universidad Abierta y a Distancia UNAD, yamarroquinr@unadvirtual.edu.co
Bogotá, Colombia

RESUMEN

En el presente trabajo se desarrollan un escenario basados en una topología de red propuesta como prueba de habilidades, esta se compone de varios dispositivos de red los cuales son un router cisco 4321, dos switch cisco 3560 y dos host. Todos los dispositivos se configuran y se interconectan por conexiones simuladas de cable UTP como medios de transmisión. Utilizando el software Packet Tracerque nos ofrece Cisco como herramienta para practicar lo aprendido en este diplomado se verifica y analiza el enrutamiento de paquetes, las configuraciones de seguridad de los equipos y procesos de troubleshooting para solución de problemas. Para esta simulación las configuraciones principales que usan son de direccionamiento IPv4 e IPv6, creación y enrutamiento de VLAN y configuración de un etherchannel con seguridad de puertos. Desarrollar esta práctica significa adquirir los conocimientos y las destrezas que el mercado laboral demanda para entender el funcionamiento de una red y estar en capacidad de diagnosticar problemas de conectividad y mantenimiento de ella.

Palabras clave: topología, protocolo, Vlan, troubleshooting, etherchannel.

ABSTRACT

In the present work, a scenario based on a network topology proposed as a test of skills is developed, it is composed of several network devices which are a Cisco 4321 router, two Cisco 3560 switches and two hosts. All devices are configured and interconnected by simulated UTP cable connections as transmission media. Using the Packet Tracersoftware that Cisco offers us as a tool to practice what we have learned in this course, packet routing, equipment security configurations and troubleshooting processes are verified and analyzed for problem solving. For this simulation, the main configurations used are IPv4 and IPv6 addressing, VLAN creation and routing and configuration of an etherchannel with port security. Developing this practice means acquiring the knowledge and skills that the labor

market demands to understand how a network works and to be able to diagnose connectivity and maintenance problems.

Keywords: Protocol, Topology, Vlan, Interfaces, Router, Switch.

I. INTRODUCCIÓN

El escenario se desarrolla completamente en entorno simulado en el software Packet Tracer el cual es creado por la compañía Cisco donde se pueden simular gran cantidad de equipos de la marca permitiendo conocerlos en imágenes detalladas de puertos y conexiones, configuraciones por línea comandos tal como se realizaría en la vida real para tener un mejor entendimiento aplicando los comandos de configuración aprendidos a lo largo del estudio de los módulos del diplomado.

Se inicia realizando la selección de los dispositivos en Packet Tracer necesarios para el desarrollo de la actividad, para cual de utiliza un router ISR/4321, dos switches de la referencia 3560 y dos PC o host para realizar las pruebas finales de conectividad extremo a extremo. Este paso de selección de dispositivos es muy importante entenderla ya que seleccionar el dispositivo incorrecto puede interrumpir el desarrollo del ejercicio, por ejemplo en la selección del switch se debe utilizar uno referencia 3560 o superior que soporte comandos avanzados de configuraciones para capa 3 y direccionamiento IPv6 que no soportan equipos muy antiguos, esto enriquece y fortalece las competencias de un ingeniero diseñador de red por ejemplo para elegir los equipos adecuados en una solución de red y ayuda a solucionar problemas básicos que se pueden presentar en un escenario real por falta de compatibilidad o soporte de protocolos o funcionamientos en un equipo de red.

Se continúa realizando las conexiones de todos los dispositivos de acuerdo a la topología prestando principal atención en la conexión de los puertos que conforman el etherchannel el cual es uno de los puntos más importantes de comprender y configurar y que es una solución de conectividad muy usada principalmente en los entornos corporativos o en las redes de grandes proveedores de servicios de internet o conectividad.

Continuando se procede a configurar los equipos no sin antes asegurarse como buena medida de borrar posibles configuraciones anteriores que puedan afectar mi red que normalmente están almacenadas en la NVRAM. También para un correcto desarrollo del escenario antes de empezar a configurar se debe tener en cuenta las características de las plantillas base que tienen los switch de fábrica y vienen preconfiguradas para ciertos tipos de funcionamiento, en este caso como se usa

direccionamiento IPv6 se debe seleccionar la plantilla interna adecuada antes de realizar la configuración del dispositivo.

Otro aspecto importante a tener en cuenta en el desarrollo del escenario es antes de concentrarse en la configuración de aspectos de conectividad como direccionamientos o enrutamientos se debe realizar las configuraciones básicas de seguridad de acceso como son las contraseñas, nombre de los equipos, mensajes de alertas de violaciones de seguridad, tipo de conexiones permitidas como buena práctica para aplicarla siempre en los entornos de la vida práctica de una red. Otra parte importante desarrollada en esta práctica es la configuración de direccionamientos donde se desarrollan habilidades adquiridas de subnetting, además el uso en la práctica de IPv6 la cual, aunque es muy conocida todavía no se usa tan comúnmente, pero es muy importante conoce su funcionamiento el cual es aplicado en este ejercicio ya que cada vez más se está haciendo muy común.

II. METODOLOGÍA

[1] En el desarrollo de esta práctica se trabaja de una forma tipo investigativa y aplicada utilizando los dispositivos de red y conocimientos adquiridos para encontrar la forma de poner a funcionar el esquema de red hasta llegar a unos resultados exitosos logrando tener conectividad entre todos los dispositivos en especial entre los host los cuales podemos simular como dos sedes geográficamente distantes que se conectan gracias a esta solución implementada en el ejercicio.

[12] Este tipo de metodología persigue resolver un problema específico u obtener una aplicación práctica concreta, para lo que suele ser imprescindible el conocimiento obtenido previamente mediante investigación básica. Dicho de otro modo, todo proceso de investigación que aplique de forma práctica conocimientos y teorías sería investigación aplicada.

En la topología de red se tiene una red LAN separada por conformada por un equipo enrutador y dos switches los cuales tienen una doble conexión troncalizada permitiendo el paso de todas las vlan ya que no se restringe ninguna con una configuración particular y muy interesante par aplicar en la práctica la cual un etherchannel el cual tiene varios usos y dos de los más importantes son que permite la suma del ancho de banda total de cada puerto simulando un solo canal de alta velocidad y la otra es la redundancia en caso de que una de la dos conexiones troncales falle.

En la topología propuesta todos los dispositivos interactúan entre ellos y se puede tener conectividad correcta luego de realizar el ejercicio gracias a la correcta configuración y propagación de vlan sobre los puertos principalmente las cuales permiten que el tráfico viaje ente los puertos

conectados de cada dispositivo permitiendo y restringiendo conectividad según lo permitido en la configuración década puerto.

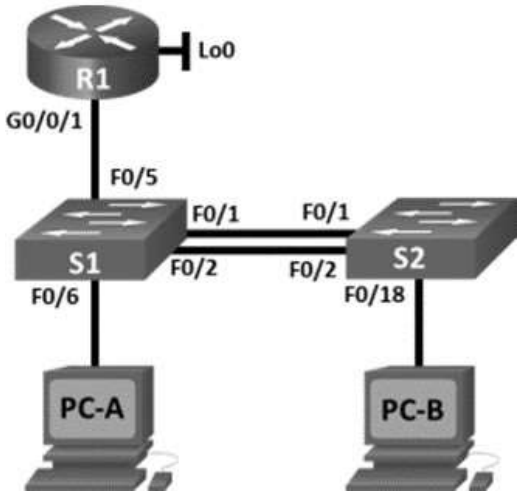
Para obtener y analizar los resultados del ejercicios se utiliza el método experimental el cual también es conocido como científico-experimental, se caracteriza porque permite que el investigador manipule y controle las variables de una investigación tanto como pueda, con la intención de estudiar las relaciones que existen entre estas. Precisamente esto este método se aplica ya que para configurar cada dispositivo fue necesario verificar y cambiar varias veces algunas configuraciones hasta obtener los resultados esperados de conectividad manipulando cada configuración en cada equipo. Este método experimental en resumen se trata de un proceso que se utiliza para investigar fenómenos, adquirir nuevos conocimientos o corregir e integrar conocimientos previos.

Los resultados de la metodología de la experimentación obtenidos al ejecutar el escenario uno propuesto nos lleva a diseñar e implementar técnicas de mantenimiento y prevención de administración de la red LAN, y porque no configurarla para crecimiento o expansión.

III. RESULTADOS

Luego de plasmar en el software de simulación de redes con dispositivos cisco Packet Tracer propuesta en la figura 1, donde se realiza selección de equipos adecuados, conexiones entre dispositivos, configuraciones equipo por equipo por medio de línea de comandos los cuales no fueron solo para ingresar configuración sino para revisar y verificar el correcto funcionamiento de los protocolos y funciones configuradas, se pasa a la ejecución y verificación de pruebas y resultados.

Figura 1. Topología de Red Escenario 1



[4] Luego de plasmar en el software de simulación de redes con dispositivos cisco Packet Tracer propuesta en la figura 1, donde se realiza selección de equipos adecuados, conexiones entre dispositivos, configuraciones equipo por equipo por medio de línea de comandos los cuales no fueron solo para ingresar configuración sino para revisar y verificar el correcto funcionamiento de los protocolos y funciones configuradas, se pasa a la ejecución y verificación de pruebas y resultados.

Esto se hace principalmente a través de una gama de comandos de verificación que generalmente inician con la palabra show, los diversos comandos show se pueden utilizar para visualizar información sobre el sistema, examinar el contenido de los archivos de configuración del router y diagnosticar fallos. Tanto en el modo privilegiado como en el modo de usuario, el comando show? muestra una lista de los comandos show disponibles.

[5] El número de comandos disponibles en modo privilegiado es mayor que en el modo de usuario. Puede verificar la conectividad desde la interfaz mediante el comando ping.

Los routers Cisco envían cinco pings consecutivos y miden los tiempos de ida y vuelta mínimos, medios y máximos. Los signos de exclamación verifican la conectividad.

Tabla 1. Direccionamiento IP configurado

Dispositivo / interface	Dirección IP / Prefijo	Puerta de enlace predeterminada
R1 G0/0/1.2	10.19.8.1 /26	No corresponde
	2001:db8:acad:a::1 /64	No corresponde
R1 G0/0/1.3	10.19.8.65 /27	No corresponde
	2001:db8:acad:b::1 /64	No corresponde
R1 G0/0/1.4	10.19.8.97 /29	No corresponde
	2001:db8:acad:c::1 /64	No corresponde
R1 G0/0/1.6	No corresponde	No corresponde
R1 Loopback0	209.165.201.1 /27	No corresponde
	2001:db8:acad:209::1 /64	No corresponde
S1 VLAN 4	10.19.8.98 /29	10.19.8.97
	2001:db8:acad:c::98 /64	No corresponde
	fe80::98	No corresponde
S2 VLAN 4	10.19.8.99 /29	10.19.8.97
	2001:db8:acad:c::99 /64	No corresponde
	fe80::99	No corresponde
PC-A NIC	Dirección DHCP para IPv4	DHCP para puerta de enlace predeterminada IPv4
	2001:db8:acad:a::50 /64	fe80::1
PC-B NIC	DHCP para dirección IPv4	DHCP para puerta de enlace predeterminada IPv4
	2001:db8:acad:b::50 /64	fe80::1

En la tabla 1 se observa los direccionamientos utilizados en todos los dispositivos e interfaces incluyendo los host con los cuales se prueba al finalizar el ejercicio la conectividad con el protocolo el protocolo ping.

Tabla 2. Nombre de las vlan

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

[3] Se crean 5 vlan en los dispositivos las cuales es muy recomendable nombrarlas con el fin de que se pueda conocer qué servicio transporta cada una de ellas sobre todo cuando ha pasado bastante tiempo y deseamos realizar mantenimiento. El nombre que se le da a las vlan se encuentra en la tabla 2.

Pero las vlan no solamente se deben configurar en los switch, también es necesario para tener resultados esperados configurar las vlan en los router lo cual se puede hacer con la creación de subinterfaces que son interfaces virtuales que trabajan sobre un puerto físico y se pueden crear

varias sobre un mismo puerto como se observa en la figura 2.

Figura 2. Configuración de interfaces del router

```
interface GigabitEthernet0/0/1
 description Conexion_Switch
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/0/1.2
 description Vlan_2_Bikes
 encapsulation dot1Q 2
 ip address 10.19.8.1 255.255.255.192
 ipv6 address FE80::1 link-local
 ipv6 address 2001:DB8:ACAD:A::1/64
!
interface GigabitEthernet0/0/1.3
 description Vlan_3_Trikes
 encapsulation dot1Q 3
 ip address 10.19.8.65 255.255.255.224
 ipv6 address FE80::1 link-local
 ipv6 address 2001:DB8:ACAD:B::1/64
!
interface GigabitEthernet0/0/1.4
 description Vlan_4_Management
 encapsulation dot1Q 4
 ip address 10.19.8.97 255.255.255.248
 ipv6 address FE80::1 link-local
 ipv6 address 2001:DB8:ACAD:C::1/64
!
interface GigabitEthernet0/0/1.6
 description Vlan_6_Nativa
 encapsulation dot1Q 6
 no ip address
```

Luego de configurar los dispositivos y antes de empezar a probar conectividad se realiza una verificación de creación de vlan en los puertos correctos del swicth con ayuda del comando show vlan brief.

Figura 3. Verificación de vlan en switch

```
S1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active
2    Bikes                            active    Fa0/6
3    Trikes                           active
4    Management                       active
5    Parking                          active    Fa0/3, Fa0/4, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gig0/1, Gig0/2
6    Native                           active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
S1#
```

También se realiza una verificación y confirmación de los puertos configurados en trunk y se puede observar en la figura 4. Estos puertos troncales se configuran permitiendo todas las vlan que sean creadas en el switch sin embargo también se pueden poner en configuración troncal permitiendo solo algunas vlan definidas.

Figura 4. Verificación de interfaces trunk

```
S1#show interfaces tr
S1#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Po1         on           802.1q         trunking      6
Fa0/6       on           802.1q         trunking      6

Port        Vlans allowed on trunk
Po1         1-1005
Fa0/6       1-1005

Port        Vlans allowed and active in management domain
Po1         1,2,3,4,5,6
Fa0/6       1,2,3,4,5,6

Port        Vlans in spanning tree forwarding state and not pruned
Po1         1,2,3,4,5,6
Fa0/6       1,2,3,4,5,6

S1#
```

En los switch uno y switch tres se realiza una configuración de etherchannel la cual como se ha mencionado tiene varias características y dos de las más importantes son que permite sumar los anchos de banda de los puertos conectados y agrupados en el etherchannel y también permiten tener doble disponibilidad de conexión que en la vida real y para canales de transporte de arto tráfico permiten tener una disponibilidad mayor en caso de falla.

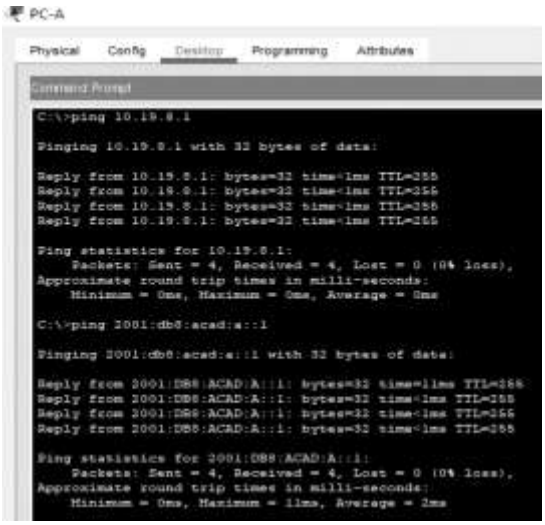
Figura 5. Verificación de etherchannel

```
S1#show etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------

1      Po1(SU)         LACP      Fa0/1(P) Fa0/2(P)
S1#
```

[2] Como último paso se realizan las pruebas finales de conectividad lo cual se hace en una red utilizando el comando ping el cual es permitido no solo en dispositivos cisco sino también en la mayoría de los dispositivos de red el cual se utiliza como herramienta de diagnóstico que permite verificar la conexión a un equipo remoto dentro de una red TCP/IP.

Ejemplo de resultado exitoso de conectividad entre el PC-A y el router 1, así mismo entre todos los dispositivos la conectividad fue exitosa. Ver figura 6.

Figura 6. Verificación de conectividad entre dispositivos.



IV. CONCLUSIONES

Luego de realizar la práctica de simulación del escenario 1 propuesto inicialmente se puede concluir que por medio de la tecnología y herramientas de simulación como Packet Tracer se puede obtener y poner en práctica conocimientos enriquecedores para la vida profesional para luego ponerlos en marcha en un escenario real.

Los dispositivos de red requieren una configuración adecuada y previamente se debe tener un diseño y selección correcta para poder llevar a cabo la configuración y obtener los resultados esperados, se deben conocer los equipos físicamente, tipos de interfaces y características de cada equipo antes de proceder.

[6] Es importante comprender el modelo OSI el cual brinda a todas las persona que trabajan con redes entendimiento en la forma de transferencia de los paquetes y entendimiento de las redes de comunicación, OSI hacen que sea posible la comunicación entre dos computadores, desde cualquier parte del mundo, también nos permite hacer posible que accedamos a los distintos servicios de la Red.

Los procesos de configuración se deben realizar en un orden determinado y se recomienda siempre realizar las configuraciones de seguridad como contraseñas encriptadas. El orden de las configuraciones es importante para no olvidar una parte de ellas y se debe verificar paso a paso lo aplicado ya

que configurar todos los dispositivos y probar solo al final dificulta más encontrar una posible falla.

V. REFERENCIAS

[1] Duoc UC Bibliotecas. (s. f.). Definición y propósito de la investigación aplicada. Definición y Propósito de la investigación aplicada. Recuperado 19 de noviembre de 2020, de

http://www.duoc.cl/biblioteca/crai/definicion-y-proposito-de-la-investigacion-aplicada.

[2] Introducción al conjunto de protocolos TCP/IP. (s. f.). docs.oracle.com. Recuperado 14 de noviembre de 2020, de

https://docs.oracle.com/cd/E19957-01/820-2981/6nei0r0r9/index.html

[3] CISCO. (s. f.-b). Enlace ISL y 802.1Q entre switches de configuración fija Catalyst Layer 2 y ejemplo de configuración de switches CatOS. cisco.com. Recuperado 3 de noviembre de 2020, de

https://www.cisco.com/c/en/us/support/docs/lan-switching/8021q/8758-43.html

[4] Networking Academy (2020 11 Noviembre). Cisco Packet Tracer recuperado 29 de noviembre de https://www.netacad.com/es/courses/packet-tracer

[5] CISCO. (s. f.-b). Los niveles de privilegio de IOS no pueden ver la configuración completa en ejecución. Cisco.com. Recuperado 11 de noviembre de 2020, de https://www.cisco.com/c/es_mx/support/docs/security-vpn/terminal-access-controller-access-control-system-tacacs-/23383-showrun.html

[6] Introducción al conjunto de protocolos TCP/IP. (s. f.). docs.oracle.com. Recuperado 17 de noviembre de 2020, de https://docs.oracle.com/cd/E19957-01/820-2981/6nei0r0r9/index.html