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

PRUEBA DE HABILIDADES PRÁCTICAS CCNA

AYCHEL ANDREA GONZALEZ DIAZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD)
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA (ECBTI)
INGENIERÍA DE SISTEMAS
DUITAMA - BOYACA
2020

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

PRUEBA DE HABILIDADES PRÁCTICAS CCNA

AYCHEL ANDREA GONZALEZ DIAZ

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

DIRECTOR
JUAN CARLOS VESGA FERREIRA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD)
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA (ECBTI)
INGENIERÍA DE SISTEMAS
DUITAMA - BOYACA
2020

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____
Firma del presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

Duitama – Boyacá, 2020

AGRADECIMIENTOS

Agradezco en primer lugar a Dios por permitirme estar en este momento culminando mis estudios de Pregrado, por la salud y bienestar. Por otra parte, a mi familia en personas de mi alrededor que de una u otra manera me han apoyado para que pueda culminar mis estudios. También agradezco al apoyo del grupo de tutores y director del Diplomado los cuales son personas que nos guían en el caminar de los estudios; y en general a la Universidad por brindarme su espacio para realizar mis estudios de Pregrado.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

ACL (Lista de Control de accesos): 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.
Cliente: es una aplicación informática o un ordenador que consume un servicio remoto en otro ordenador conocido como servidor.
DHCP (protocolo de configuración dinámica de host): es un protocolo de red de tipo cliente/servidor mediante el cual un servidor DHCP asigna dinámicamente una dirección IP y otros parámetros de configuración de red.
Dirección MAC (Dirección Física): Identificador de 48 bits (6 bloques de dos caracteres hexadecimales [8 bits]) que corresponde de forma única a una tarjeta o dispositivo de red.
DNS (sistema de nombres de dominio): Sistema de nomenclatura jerárquico descentralizado para dispositivos conectados a redes IP como Internet o una red privada.
Etherchannel: es una tecnología de Cisco construida de acuerdo con los estándares 802.3 full-duplex Fast Ethernet. Permite la agrupación lógica de varios enlaces físicos Ethernet.
Gateway (Puerta de Enlace): Dispositivo que actúa de interfaz de conexión entre aparatos o dispositivos, y también posibilita compartir recursos entre dos o más ordenadores.
Host (anfitrión): se usa en informática para referirse a las computadoras u otros dispositivos (tabletas, móviles, portátiles) conectados a una red que proveen y utilizan servicios de ella.
Interfaz de red: es el software específico de red que se comunica con el controlador de dispositivo específico de red y la capa IP a fin de proporcionar a la capa IP una interfaz coherente con todos los adaptadores de red que puedan estar presentes.
IPv4: es la cuarta versión del Internet Protocol (IP), un protocolo de interconexión de redes basadas en Internet, usa direcciones de 32 bits, limitadas a 2^32 = 4.294.967.296 direcciones únicas, muchas las (LAN).
IPv6: es una actualización al protocolo IPv4, diseñado para resolver el problema de agotamiento de direcciones. Diseñado por Steve Deering de Xerox PARC, IPv6 está destinado a sustituir a IPv4.
Mascara de red: es una combinación de bits que sirve para delimitar el ámbito de una red de ordenadores. Su función es indicar a los dispositivos qué parte de la dirección IP es el número de la red, incluyendo la subred, y qué parte es la correspondiente al host.
NAT (Traducción de direcciones de red): Se trata de un sistema que se utiliza en las redes bajo el protocolo IP y que nos permite el intercambio de paquetes entre dos redes que tienen asignadas mutuamente direcciones IP incompatibles.
NTP (Network Time Protocol): 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): Protocolo de direccionamiento de tipo enlace-estado, desarrollado para las redes IP y basado en el algoritmo de primera vía más corta (SPF). OSPF es un protocolo de pasarela interior (IGP).
Ping: es una utilidad de diagnóstico en redes de computadoras que comprueba el estado de la comunicación del anfitrión local con uno o varios equipos remotos de una red que ejecuten IP.
Puerto: es una ranura que porta una computadora personal. Esta ranura tiene la capacidad de que se le introduzca un cable de red con el cual el dispositivo se conectará a la señal del router.
Red: es un conjunto de equipos nodos y software conectados entre sí por medio de dispositivos físicos o inalámbricos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de compartir información, recursos y ofrecer servicios.
Router (Encaminador): es un dispositivo que permite interconectar computadoras que funcionan en el marco de una red. Su función: se encarga de establecer la ruta que destinará a cada paquete de datos dentro de una red informática.
Servidor: es una aplicación en ejecución capaz de atender las peticiones de un cliente y devolverle una respuesta en concordancia.
SSH (Secure Shell): es el nombre de un protocolo y del programa que lo implementa cuya principal función es el acceso remoto a un servidor por medio de un canal seguro en el que toda la información está cifrada.
Switch (Conmutador): es el dispositivo digital lógico de interconexión de equipos que opera en la capa de enlace de datos del modelo OSI. Su función es interconectar dos o más host de manera similar a los puentes de red.
TelNet (Teletype Network): es el nombre de un protocolo de red que nos permite acceder a otra máquina para manejarla remotamente como si estuviéramos sentados delante de ella.
Trunking: es un sistema de radio en el que todas las comunicaciones van precedidas de un código de llamada similar a una telefónica; si nuestro equipo la recibe y no es el destinatario la emite de nuevo, actuando como repetidor.
VTY (líneas de terminal virtual del router): se utilizan solamente para controlar las conexiones Telnet entrantes. Son virtuales en el sentido que son una función de software; no hay hardware relacionado con ellas.
Wlan (red de área local inalámbrica): es un sistema de comunicación inalámbrico para minimizar las conexiones cableadas. Las redes de área local inalámbrica utilizan las ondas de radio para llevar la información de un punto a otro sin necesidad de un medio físico guiado.

RESUMEN

Para este informe se implementan los conocimientos adquiridos durante el Diplomado de Introducción a las redes y Principios básicos de routing y switching que ofrece CISCO y el cual nos permite conocer mas de cerca el funcionamiento de redes básicas y por medio de plataformas poder simular para aprender a configurar a través de comandos y así mismo verificar su correcto funcionamiento. Con el apoyo del entorno de conocimiento y del instructor se logra conocer, aplicar, verificar e implementar redes pequeñas a través de aplicaciones, desarrollando en los aprendices aptitudes necesarias para planificar e implementar redes. El material implementado facilita la manera en la que nosotros como estudiantes trabajamos, vivimos, y aprendemos mediante estrategias de comunicaciones de voz, video y otros datos.

ABSTRAC

For this report are implemented the acquired knowledge during the Diplomado in Introduction to networks and basic principles of routing and switching that Cisco offers and which allows to know us more closely the operation of core networks and through platforms to simulate to learn configure through commands and also verify its correct operation. With the support of the knowledge environment and the instructor, it is possible to know, apply, verify and implement small networks through applications, developing in the learners the necessary skills to plan and implement networks. The implemented material facilitates the way in which we as students work, live, and learn through voice, video and other data communication strategies.

INTRODUCCIÓN

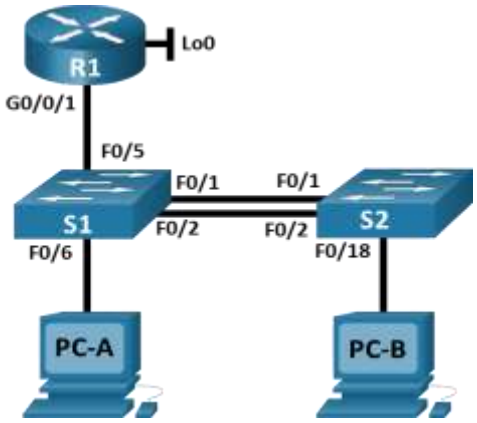
Hoy en día la humanidad tiene la necesidad de interactuar diariamente con cada innovación que se presenta, debido a que crece el interés de saber para qué y cómo funciona la tecnología en la mayoría de ámbitos. Además de ello la comunicación hoy en día se hace casi tan como el aire, el agua, los alimentos y un lugar para vivir. Es así como el día de hoy las redes se usan por casi toda la humanidad debido a que la necesidad de comunicarse por los diferentes medios implica el uso de dichas redes. Por medio del entorno implementado en el aprendizaje de la configuración básica, la arquitectura, los componentes y el funcionamiento de los routers y switches en una red pequeña, se logra dar paso a paso en el crecimiento como Ingeniero de Sistemas capaz de desarrollar y conocer acerca de las redes. Las redes tienen un impacto considerable en nuestras vidas, estas cambiaron la forma en que vivimos, trabajamos y jugamos. Es por ello que hoy en día las redes nos permiten comunicarnos, colaborar e interactuar como nunca antes, ya que las utilizamos de distintas formas, como en las aplicaciones web, la telefonía IP, la videoconferencia, los juegos interactivos, el comercio electrónico, la educación y más.

DESARROLLO PRUEBA DE HABILIDADES PRÁCTICAS CCNA

ESCENARIO 1

Topología

Figura 1. Topología propuesta para el 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 en Packet Tracer del Escenario 1

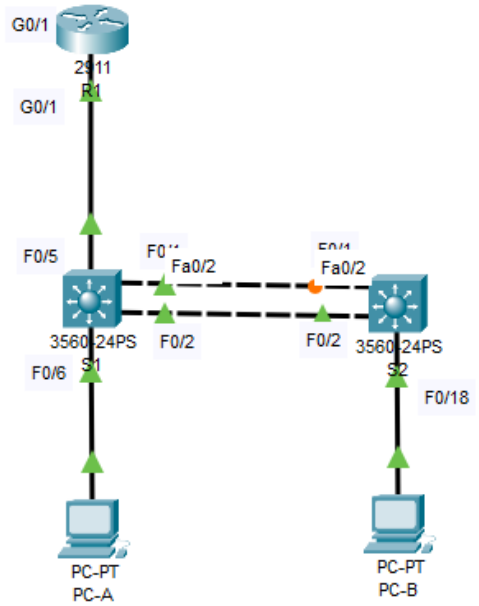


Tabla de asignación de direcciones

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

Tabla 1. Asignación de direcciones del Escenario 1

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

Tabla de VLAN

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

Tabla 2. VLAN para el Escenario 1

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

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

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

Router:

- Para borrar las configuraciones en el Router se utiliza el comando:

  Router# erase startup-config
- Enseguida para recargarlo se utiliza el comando:

  Router# reload

  Nota: Si se recibe este mensaje: "System configuration has been modified. Save? [yes/no]:" Responder no
- Luego se omite la configuración inicial diciendo no a este mensaje: "Would you like to enter the initial configuration dialog? [yes/no]: no"
- Por último, se pedirá que finalice el programa de instalación automática en donde se responderá con Si al siguiente mensaje: "Would you like to terminate autoinstall? [yes]:"

Switch:

- En el caso de los Switch, se eliminarán los archivos VLAN por medio del comando:

  Switch# delete vlan.dat
- Se mostrará un mensaje en el cual debe verificar el nombre del archivo a eliminar y enseguida se confirmará la eliminación del archivo presionando Enter al siguiente mensaje: "Delete flash:/vlan.dat? [confirm]"

- Pasamos a la eliminación del archivo de configuración por medio del comando:

  Switch# erase startup-config
- Por último, se recarga con el comando

  Switch# reload

  Nota: Si se recibe este mensaje: “System configuration has been modified. Save? [yes/no]:” Responder no
- Luego se omite la configuración inicial diciendo no a este mensaje: “Would you like to enter the initial configuration dialog? [yes/no]: no”

- Después de recargar el switch, configure la plantilla SDM para que admita IPv6 según sea necesario y vuelva a cargar el switch.
  - Para ver si la plantilla predeterminada “default” esta activa se ingresa el comando:

    S1# show sdm prefer
  - Si dicha plantilla es la predeterminada, establezca la preferencia de SDM por medio del comando:

    S1(config)#sdm prefer dual-ipv4-and-ipv6 Default
  - Enseguida para volver a cargar los Switch se utiliza el comando:

    S1#reload
  - Se verifica que la plantilla sea activada por medio del comando:

    S1# show sdm prefer
  - Por último, se habilita el enrutamiento de unidifusión IPv6 por medio del comando:

    S1(config)#ipv6 unicast-routing

    Nota: Se realiza la misma configuración para el segundo Switch

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

  Se verifica que los dispositivos hayan quedado correctamente inicializados y se procede con la configuración.

Paso 2: Configurar R1

La configuración para R1 incluyen las siguientes tareas:

Tarea	Especificación
Desactivar la búsqueda DNS	Para desactivar por completo la búsqueda DNS se utiliza el comando

	Router(config)# no ip domain-lookup
Nombre del router	Para establecer el nombre del router se utiliza el comando Router(config)# hostname R1
Nombre de dominio	Para definir un nombre de dominio predeterminado se usa el comando R1(config)#ip domain name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	Para establece la contraseña cifrada para el ingreso a modo privilegiado se utiliza el comando R1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	Para establecer la contraseña de acceso a la consola se usa los siguientes comandos que permiten su respectiva configuración R1(config)#line console 0 R1(config-line)#password ciscoconpass R1(config-line)#login
Establecer la longitud mínima para las contraseñas	Para establecer como longitud mínima para dicha contraseña de 10 caracteres se utiliza el comando R1(config)#security passwords min-length 10
Crear un usuario administrativo en la base de datos local	Nombre de usuario: **admin** Password: **admin1pass** Para la creación de un usuario con la respectiva contraseña se usa el comando R1(config)#username admin password admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	Para realizar la configuración de inicio de sesión VTY estableciendo una base de datos local se usa los comandos R1(config)#line vty 0 4 R1(config-line)#login local R1(config-line)#exit
Configurar VTY solo aceptando SSH	Para que VTY solo acepte SSH utilizamos los comandos R1(config)#crypto key generate rsa R1(config)#ip ssh version 2 R1(config)#line vty 0 4 R1(config-line)#transport input ssh
Cifrar las contraseñas de texto no cifrado	Para cifrar las contraseñas al mostrar los datos de configuración se utiliza el comando R1(config)#service password-encryption

Configure un MOTD Banner	Para establecer un mensaje de acceso no autorizado utilizamos el comando R1(config)#banner motd #Acceso no autorizado#
Habilitar el routing IPv6	Para habilitar el routing IPV6 se utiliza el comando R1(config)#ipv6 unicast-routing
Configurar interfaz G0/0/1 y subinterfaces	Para establecer la configuración de las interfaces del router siguiendo los lineamientos de la tabla se utilizan los siguientes comandos para cada interfaz: - **Interface gigabitEthernet 0/1.2** R1(config)#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 2001:db8:acad:a::1/64 R1(config-subif)# ipv6 address fe80::1 link-local R1(config-subif)#no shutdown - **Interface gigabitEthernet 0/1.3** R1(config)#interface gigabitEthernet 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 2001:db8:acad:b::1/64 R1(config-subif)#ipv6 address fe80::1 link-local R1(config-subif)#no shutdown - **Interface gigabitEthernet 0/1.4** R1(config)#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 2001:db8:acad:c::1/64 R1(config-subif)#ipv6 address fe80::1 link-local R1(config-subif)#no shutdown - **Interface gigabitEthernet 0/1.6** R1(config)#interface gigabitEthernet 0/0/1.6 R1(config-subif)#description VLAN 6 Native R1(config-subif)#encapsulation dot1Q 6 R1(config-subif)#no shutdown

Configure el Loopback0 interface	Para la configuración de la interfaz loopback 0 según la tabla de información de la red, se implementan los siguientes comandos R1(config)#interface loopback 0 R1(config-if)#description Interface Loopback 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)#no shutdown
Generar una clave de cifrado RSA	Con el siguiente comando se genera una clave de cifrado RSA utilizando una longitud de 1024 bits R1(config)#crypto key generate rsa

Tabla 3. Tareas para configuración de R1

Descripción tabla 3: Para el Escenario 1 se plantea la configuración del Router, en donde se desactiva la búsqueda DNS, se asigna el nombre de “R1” y de dominio, se le configuran contraseñas que permitan el acceso limitado al router, se crea un usuario administrativo, se estable el inicio de sesión VTY para que use base de datos local y acepte ssh, se establece un mensaje se acceso no autorizado cuando se realice ingreso de contraseña incorrecta, se habilita el routing IPV6, se configuran las diferentes interfaces y por último se asigna clave de cifrado rsa; Esta configuración es básica para el funcionamiento que se requiere para dicho escenario.

Paso 3: Configure S1 y S2.

Las tareas de configuración incluyen lo siguiente:

Tarea	Especificación
Desactivar la búsqueda DNS.	Para desactivar por completo la búsqueda DNS se utiliza el comando Switch(config)# no ip domain-lookup
Nombre del switch	Para establecer el nombre del Switch se utiliza el comando Switch(config)# hostname S1
Nombre de dominio	Para definir un nombre de dominio predeterminado se usa el comando S1(config)#ip domain name ccna-lab.com

Contraseña cifrada para el modo EXEC privilegiado	Para establece la contraseña cifrada para el ingreso a modo privilegiado se utiliza el comando S1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	Para establecer la contraseña de acceso a la consola se usa los siguientes comandos que permiten su respectiva configuración S1(config)#line console 0 S1(config-line)#password ciscoconpass S1(config-line)#login
Crear un usuario administrativo en la base de datos local	Nombre de usuario: **admin** Password: **admin1pass** Para la creación de un usuario con la respectiva contraseña se usa el comando S1(config)#username admin password admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	Para realizar la configuración de inicio de sesión VTY estableciendo una base de datos local se usa los comandos S1(config)#line vty 0 4 S1(config-line)#login local S1(config-line)#exit
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	Para que VTY solo acepte SSH utilizamos los comandos S1(config)#crypto key generate rsa S1(config)#ip ssh version 2 S1(config)#line vty 0 4 S1(config-line)#transport input ssh
Cifrar las contraseñas de texto no cifrado	Para cifrar las contraseñas al mostrar los datos de configuración se utiliza el comando S1(config)#service password-encryption
Configurar un MOTD Banner	Para establecer un mensaje de acceso no autorizado utilizamos el comando S1(config)#banner motd #Acceso no autorizado#
Generar una clave de cifrado RSA	Con el siguiente comando se genera una clave de cifrado RSA utilizando una longitud de 1024 bits S1(config)#crypto key generate rsa
Configurar la interfaz de administración (SVI)	Para la configuración de la interfaz administrativa (SVI) se usan los siguientes comandos para cada Switch: **- S1** S1(config)#interface vlan 4 S1(config-if)#ip address 10.19.8.98 255.255.255.248

	S1(config-if)#ipv6 address 2001:db8:acad:c::98/64 S1(config-if)#ipv6 address fe80::98 link-local S1(config-if)#no shutdown **- S2** S2(config)#interface vlan 4 S2(config-if)#ip address 10.19.8.99 255.255.255.248 S2(config-if)#ipv6 address 2001:db8:acad:c::99/64 S2(config-if)#ipv6 address fe80::99 link-local S2(config-if)#no shutdown
Configuración del gateway predeterminado	Para la configuración de la puerta de enlace predeterminada se usan los comandos: **- Para S1** S1(config)#ip default-gateway 10.19.8.97 **- Para S2** S2(config)#ip default-gateway 10.19.8.97

Tabla 4. Configuración de S1 y S2

Descripción tabla 4: En este caso se plantea la configuración de los dos Switchs usados en dicho Escenario 1, en donde se desactiva la búsqueda DNS, se asigna el nombre de "S1" y "S2" respectivamente y de dominio, se le configuran contraseñas que permitan el acceso limitado a los switchs, se crea un usuario administrativo, se estable el inicio de sesión VTY para que use base de datos local y acepte ssh, se establece un mensaje se acceso no autorizado cuando se realice ingreso de contraseña incorrecta, se genera clave de cifrado Rsa, se configuran las diferentes interfaces y por último se configura el Gateway predeterminado; Esta configuración es principal en cada uno de los switch para el funcionamiento que se requiere para dicho escenario.

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

Paso 1: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tarea	Especificación
Crear VLAN	Para crear las diferentes VLAN se utilizan los siguientes comandos para cada una de ellas: **- VLAN 2, nombre Bikes**

	S1(config)#vlan 2 S1(config-vlan)#name Bikes S1(config-vlan)#exit - **VLAN 3, nombre Trikes** S1(config)#vlan 3 S1(config-vlan)#name Trikes S1(config-vlan)#exit - **VLAN 4, name Management** S1(config)#vlan 4 S1(config-vlan)#name Management S1(config-vlan)#exit - **VLAN 5, nombre Parking** S1(config)#vlan 5 S1(config-vlan)#name Parking S1(config-vlan)#exit - **VLAN 6, nombre Native** S1(config)#vlan 6 S1(config-vlan)#name Native S1(config-vlan)#exit
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	Para la creación de troncos 802.1Q que utilicen la VLAN 6 nativa se utilizan los siguientes comandos - **Interfaz F0/1** S1(config)#interface range fastEthernet 0/1 S1(config-if-range)#switchport trunk encapsulation dot1Q S1(config-if-range)#switchport mode trunk S1(config-if-range)#switchport trunk native vlan 6 S1(config-if-range)#exit - **Interfaz F0/2** S1(config)#interface range fastEthernet 0/2

	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)#exit - **Interfaz F0/5** S1(config)#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 S1(config-if-range)#exit
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	Para la creación de un grupo de puertos EtherChannel de Capa 2 para el uso del protocolo LACP para la negociación se siguen los comandos S1(config)#interface range fastEthernet 0/1-2 S1(config-if-range)#channel-group 1 mode active S1(config-if-range)#interface port-channel 1 S1(config-if)#switchport trunk encapsulation dot1Q S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk allowed vlan all S1(config-if)#channel-protocol lacp
Configurar el puerto de acceso de host para VLAN 2	Para configurar el puerto de acceso para VLAN 2 a la interfaz F0/6 se siguen los comandos S1(config)#interface fastEthernet 0/6 S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 2 S1(config-if)#exit
Configurar la seguridad del puerto en los puertos de acceso	Para la configuración de seguridad del puerto se establen estos comandos en donde se permiten 3 direcciones MAC S1(config)#interface fastEthernet 0/6

	S1(config-if)#switchport mode access S1(config-if)#switchport port-security S1(config-if)#switchport port-security maximum 3
Proteja todas las interfaces no utilizadas	Para la protección de las interfaces no utilizadas se asigna a VLAN 5 y se establece en modo de acceso. - **Interfaces F0/3 y F0/4** S1(config)#interface range fastEthernet 0/3-4 S1(config-if)#switchport mode access S1(config-if)#description No Utilizada S1(config-if)#switchport access vlan 5 S1(config-if)#shutdown S1(config-if)#exit - **Interfaces F0/7 a F0/24** S1(config)#interface range fastEthernet 0/7-24 S1(config-if)#switchport mode access S1(config-if)#description No Utilizada S1(config-if)#switchport access vlan 5 S1(config-if)#shutdown S1(config-if)#exit - **Interfaces G0/1 y G0/2** S1(config)#interface range G0/1-2 S1(config-if)#switchport mode access S1(config-if)#description No Utilizada S1(config-if)#switchport access vlan 5 S1(config-if)#shutdown S1(config-if)#exit

Tabla 5. Configuración de tareas S1

Descripción tabla 5: En este caso se plantea la configuración de tareas que se requiere que cumpla el Switch 1 por medio de la creación de: las VLAN planteadas, los troncos para la VLAN 6 nativa por medio de las diferentes interfaces, y un grupo de puertos EtherChannel de capa 2 que usan las interfaces F0/1 y F0/2; Además la configuración de: los puertos host para la VLAN 2, la seguridad de los puertos de

acceso y la protección de las interfaces no utilizadas; Dicha configuración se realiza por medio de comandos dentro del S1.

Paso 2: Configure el S2.

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

Tarea	Especificación
Crear VLAN	Para crear las diferentes VLAN se utilizan los siguientes comandos para cada una de ellas: - **VLAN 2, nombre Bikes** S2(config)#vlan 2 S2(config-vlan)#name Bikes S2(config-vlan)#exit - **VLAN 3, nombre Trikes** S2(config)#vlan 3 S2(config-vlan)#name Trikes S2(config-vlan)#exit - **VLAN 4, name Management** S2(config)#vlan 4 S2(config-vlan)#name Management S2(config-vlan)#exit - **VLAN 5, nombre Parking** S2(config)#vlan 5 S2(config-vlan)#name Parking S2(config-vlan)#exit - **VLAN 6, nombre Native** S2(config)#vlan 6 S2(config-vlan)#name Native S2(config-vlan)#exit
Crear troncos 802.1Q que	Para la creación de troncos 802.1Q que utilicen la VLAN 6 nativa se utilizan los siguientes comandos - **Interfaz F0/1**

utilicen la VLAN 6 nativa	S2(config)#interface range fastEthernet 0/1 S2(config-if-range)#switchport trunk encapsulation dot1Q S2(config-if)#switchport mode trunk S2(config-if)#switchport trunk native vlan 6 S2(config)#exit - **Interfaz F0/2** S2(config)#interface range fastEthernet 0/2 S2(config-if-range)#switchport trunk encapsulation dot1Q S2(config-if)#switchport mode trunk S2(config-if)#switchport trunk native vlan 6 S2(config)#exit
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	Para crear un grupo de puertos EtherChannel Capa 2 para el uso en protocolo LACP para negociar se usan comandos S2(config)#interface range fastEthernet 0/1-2 S2(config-if)#channel-group 1 mode active S2(config-if-range)#interface port-channel 1 S2(config-if)#switchport trunk encapsulation dot1Q S2(config-if)#switchport mode trunk S2(config-if)#switchport trunk allowed vlan all S2(config-if)#channel-protocol lacp
Configurar el puerto de acceso del host para la VLAN 3	Para configurar el puerto de acceso para VLAN 3 a la interfaz F0/6 se siguen los comandos S2(config)#interface fastEthernet 0/18 S2(config-if)#switchport mode access S2(config-if)#switchport access vlan 3 S2(config-if)#exit
Configure port-security en los access ports	Para la configuración de seguridad del puerto se establen estos comandos en donde se permiten 3 direcciones MAC S2(config)#interface fastEthernet 0/18 S2(config-if)#switchport mode access

	S2(config-if)#switchport port-security S2(config-if)#switchport port-security maximum 3
Asegure todas las interfaces no utilizadas.	Para la protección de las interfaces no utilizadas se asigna a VLAN 5 y se establece en modo de acceso. - **Interfaces F0/3 y F0/17** S2(config)#interface range F0/3-17 S2(config-if)#switchport mode access S2(config-if)#description No Utilizada S2(config-if)#switchport access vlan 5 S2(config-if)#shutdown S2(config-if)#exit - **Interfaces F0/19 a F0/24** S2(config)#interface range F0/19-24 S2(config-if)#switchport mode access S2(config-if)#description No Utilizada S2(config-if)#switchport access vlan 5 S2(config-if)#shutdown S2(config-if)#exit - **Interfaces G0/1 y G0/2** S2(config)#interface range G0/1-2 S2(config-if)#switchport mode access S2(config-if)#description No Utilizada S2(config-if)#switchport access vlan 5 S2(config-if)#shutdown S2(config-if)#exit

Tabla 6. Configuración de tareas S2

Descripción tabla 6: En este caso se plantea la configuración de tareas que se requiere que cumpla el Switch 2 por medio de la creación de: las VLAN planteadas, los troncos para la VLAN 6 nativa por medio de las diferentes interfaces, y un grupo de puertos EtherChannel de capa 2 que usan las interfaces F0/1 y F0/2; Además la configuración de: los puertos host para la VLAN 3, la seguridad de los puertos de acceso y la protección de las interfaces no utilizadas; Dicha configuración se realiza por medio de comandos dentro del S2.

Parte 3: Configurar soporte de host

Paso 1: Configure R1

Las tareas de configuración para R1 incluyen las siguientes:

Tarea	Especificación
Configure Default Routing	Para la creación de rutas predeterminadas para IPv4 e IPv6 que dirijan el tráfico se realiza por medio del comando R1(config)#ip dhcp excluded-address 10.19.8.1 10.19.8.51
Configurar IPv4 DHCP para VLAN 2	Para crear un grupo DHCP para VLAN 2, compuesto por las últimas 10 direcciones de la subred solamente se utiliza el comando R1(config)#ip dhcp pool VLAN2 R1(config)#network 10.19.8.0 255.255.255.192 R1(config)#default-router 10.19.8.1 Para la asignación del nombre de dominio ccna-a.net y especificar la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada R1(config)#dns-server 10.19.8.51 R1(config)#domain-name ccna-a.net
Configurar DHCP IPv4 para VLAN 3	Para la creación de un grupo DHCP para VLAN 3, compuesto por las últimas 10 direcciones de la subred solamente. R1(config)#ip dhcp excluded-address 10.19.8.65 10.19.8.83 R1(config)#ip dhcp pool VLAN3 R1(dhcp-config)#network 10.19.8.64 255.255.255.224 Para la asignación del nombre de dominio ccna-b.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada R1(config)#default-router 10.19.8.65 R1(config)#dns-server 10.19.8.83 R1(config)#domain-name ccna-b.net

Tabla 7. Tareas de configuración de R1

Descripción tabla 7: En este paso se plantea la configuración de tareas que se requiere que cumpla el Router por medio de la configuración de rutas

predeterminadas, la configuración de grupo DHCP para la VLAN 2 y VLAN 3 respectivamente; de manera que el router establezca dichas características en su funcionamiento.

Paso 2: Configurar los servidores

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

PC-A Network Configuration	
Descripción	ccna-a.net
Dirección física	0050.0FAD.83C2
Dirección IP	169.254.131.194
Máscara de subred	*255.255.255.192*
Gateway predeterminado	*10.19.8.1*
Gateway predeterminado IPv6	*FE80::1*

Tabla 8. Configuración de PC-A

Descripción tabla 8: Se realiza la respectiva configuración directamente ingresando a los datos de red de la PC-A

Configuración de red de PC-B	
Descripción	*en blanco*
Dirección física	*en blanco*
Dirección IP	*en blanco*
Máscara de subred	*255.255.255.224*
Gateway predeterminado	*10.19.8.65*
Gateway predeterminado IPv6	*FE80::1*

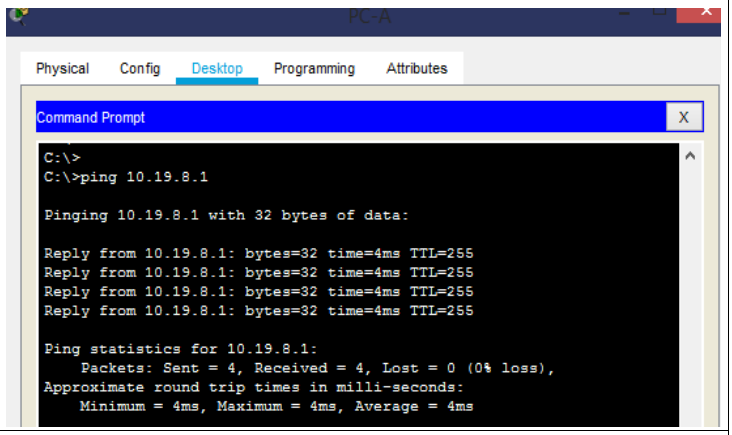
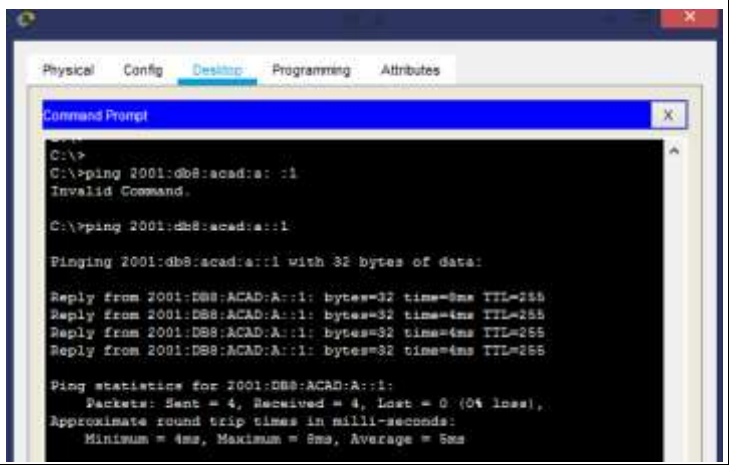
Tabla 9. Configuración PC-B

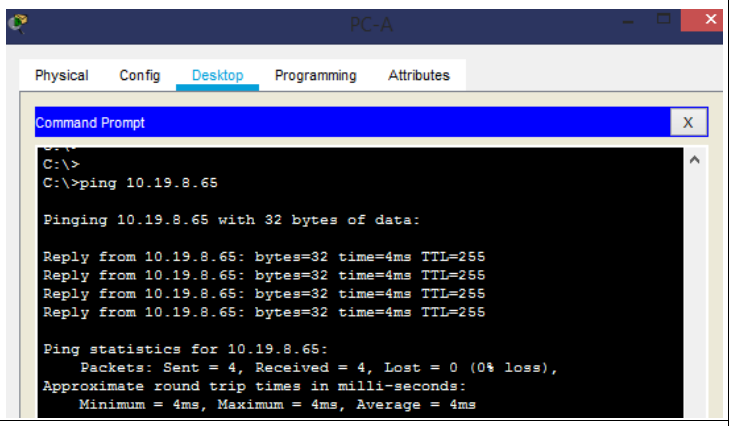
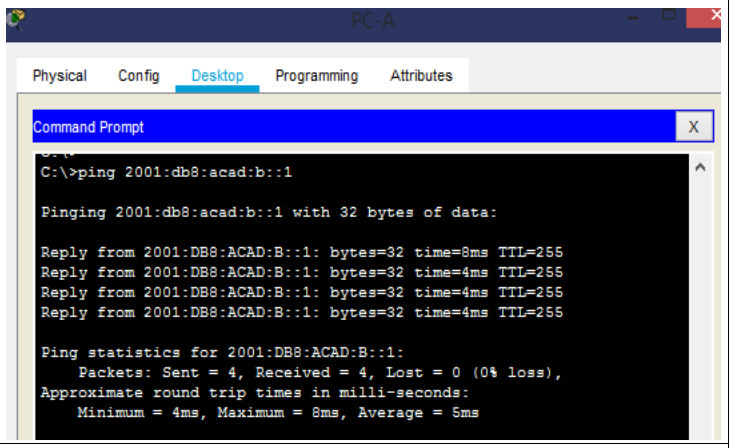
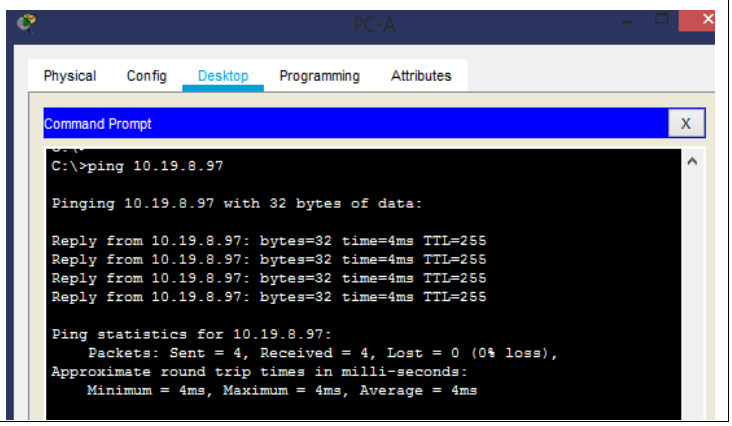
Descripción tabla 9: Se realiza la respectiva configuración directamente ingresando a los datos de red de la PC-B

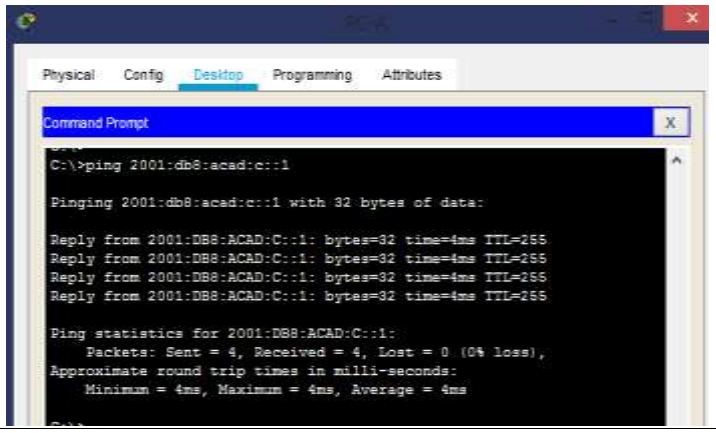
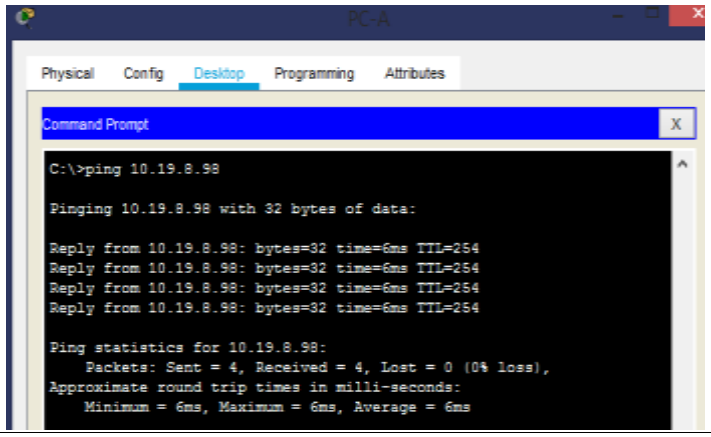
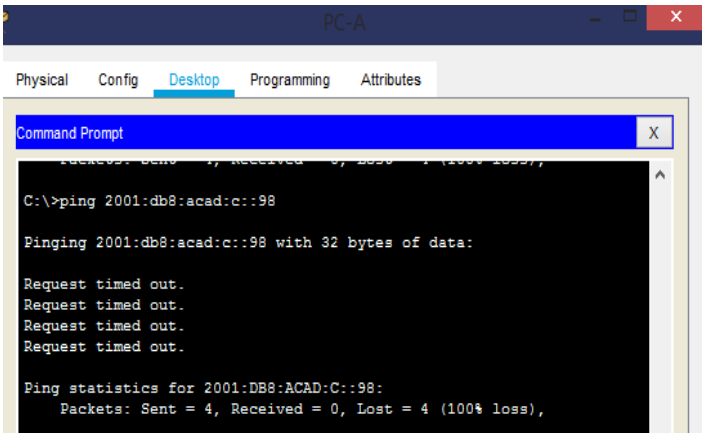
Parte 4: Probar y verificar la conectividad de extremo a extremo

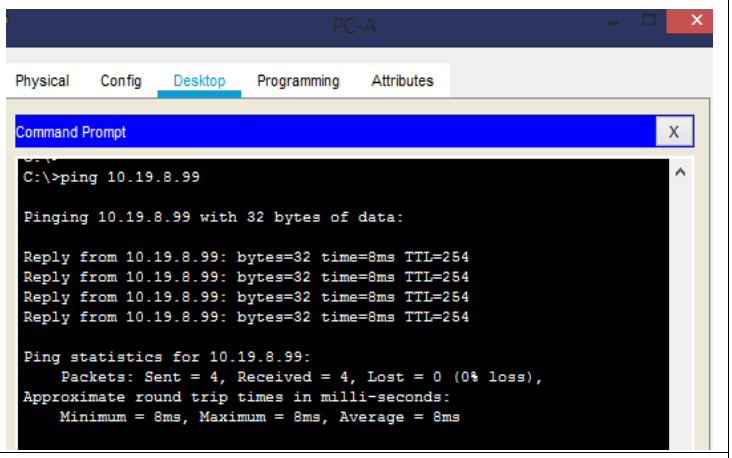
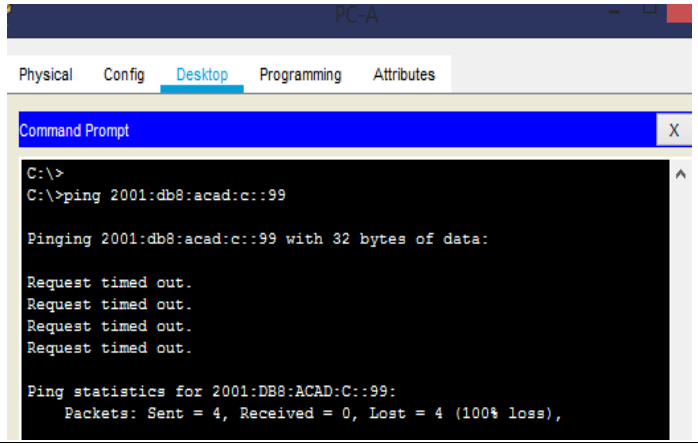
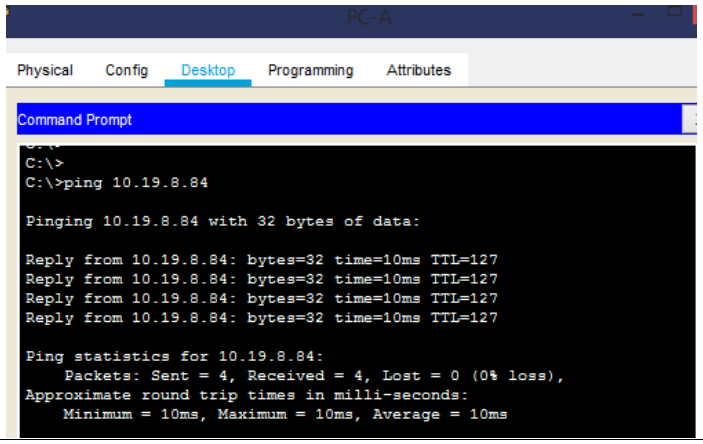
Use el comando ping para probar la conectividad IPv4 e IPv6 entre todos los dispositivos de red. Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red.

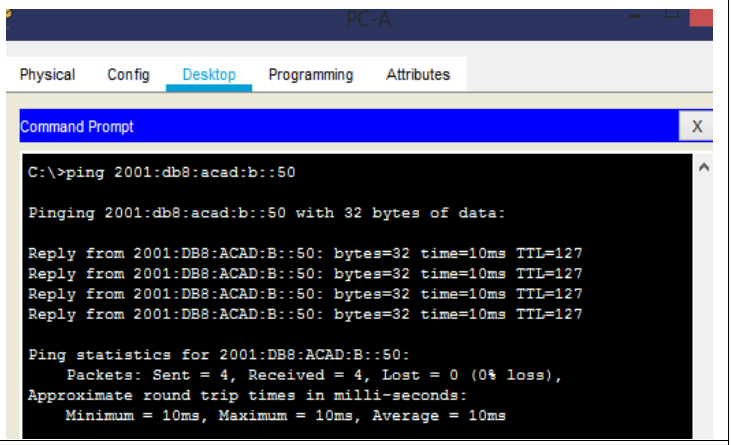
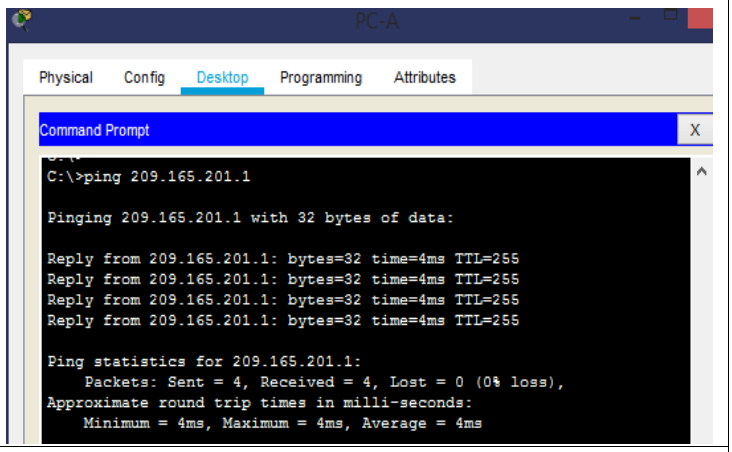
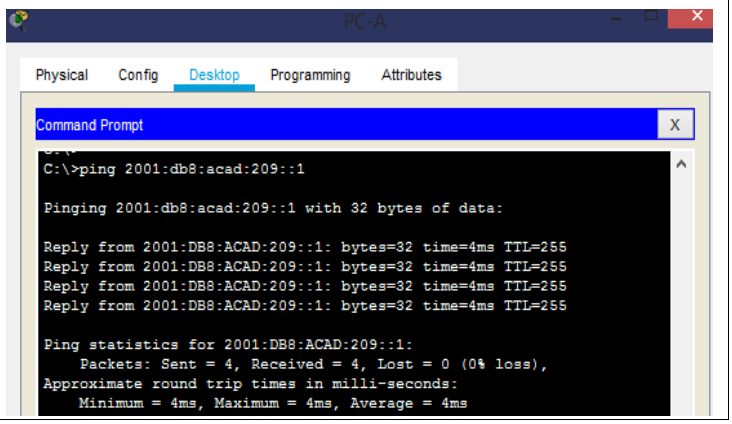
Nota: Si fallan los pings en las computadoras host, desactive temporalmente el firewall de la computadora y vuelva a realizar la prueba.

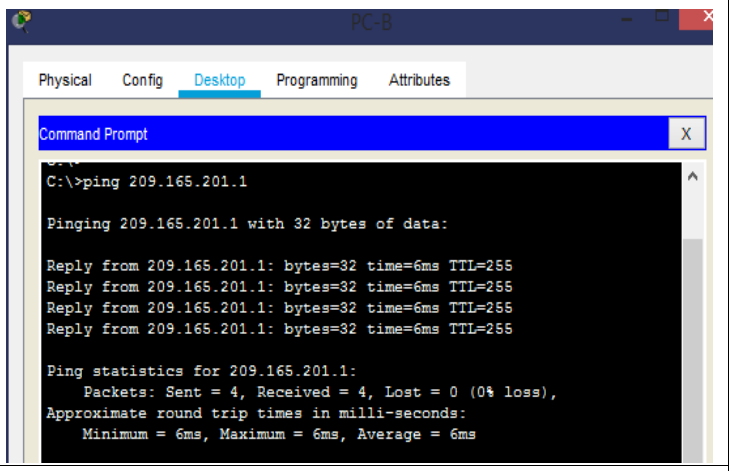
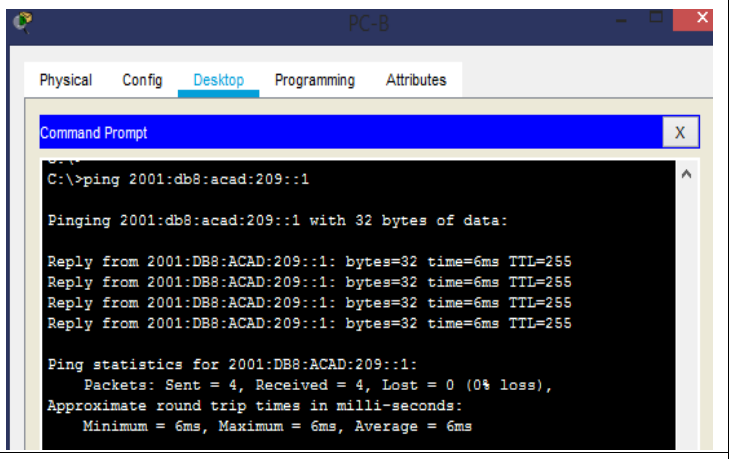
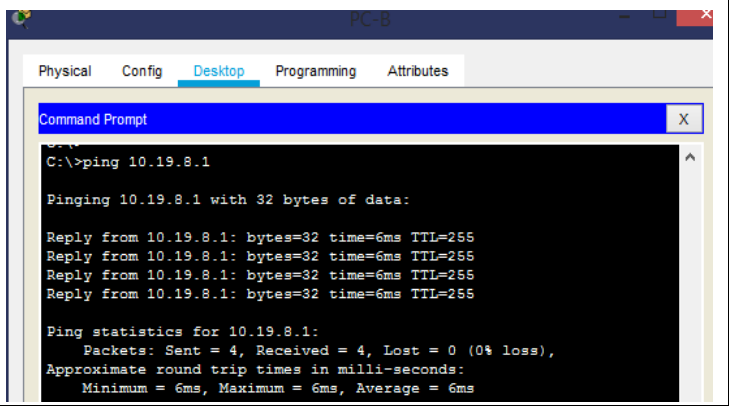
Desde	A	de Internet	Dirección IP	Resultados de ping
PC-A	R1, G0/0/1.2	Dirección	10.19.8.1	*Figura 3.Ping PcA- R1,G0/0/1.2 (IP)* 
PC-A	*R1, G0/0/1.2*	IPv6	2001:db8:acad:a::1	*Figura 4. Ping PcA-R1,G0/0/1.2 (IPv6)* 

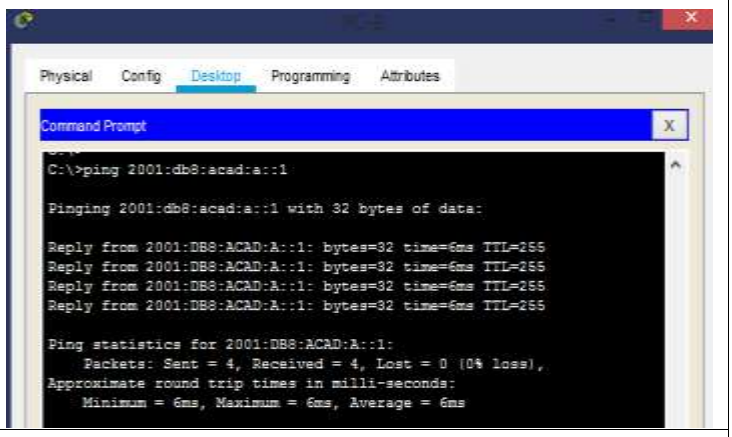
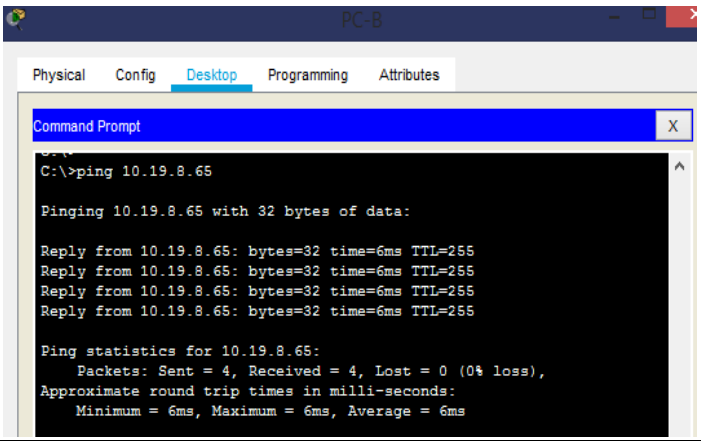
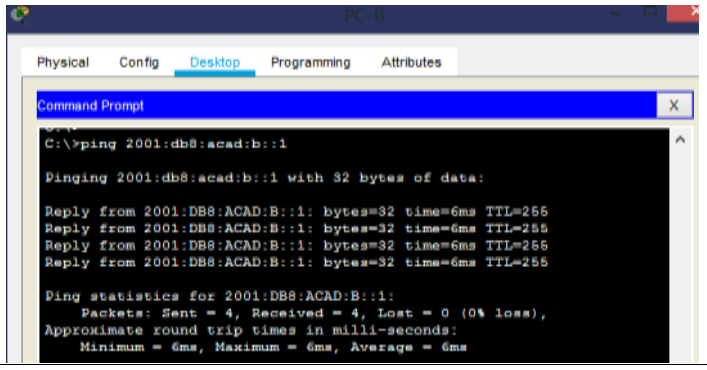
PC-A	R1, G0/0/ 1.3	Dirección	10.19.8.65	*Figura 5. Ping PcA-R1,G0/0/1.3 (IP)* 
PC-A	*R1, G0/0/ 1.3*	IPv6	2001:db8:acad:b: :1	*Figura 6.Ping PcA-R1,G0/0/1.3 (IPv6)* 
PC-A	R1, G0/0/ 1.4	Dirección	10.19.8.97	*Figura 7. Ping PcA-R1,G0/0/1.4 (IP)* 

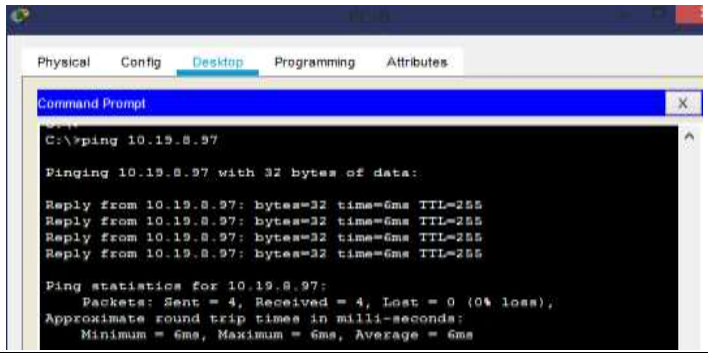
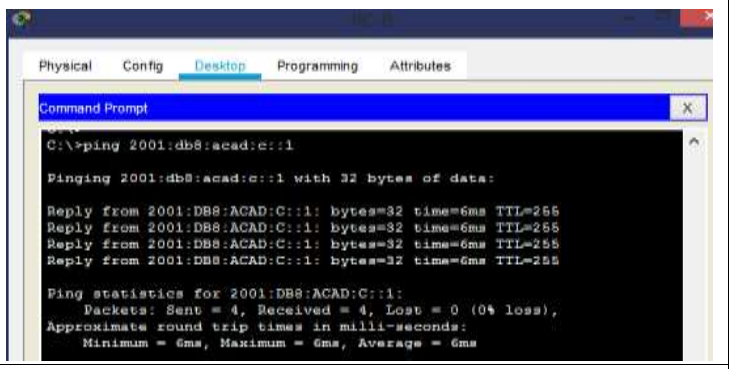
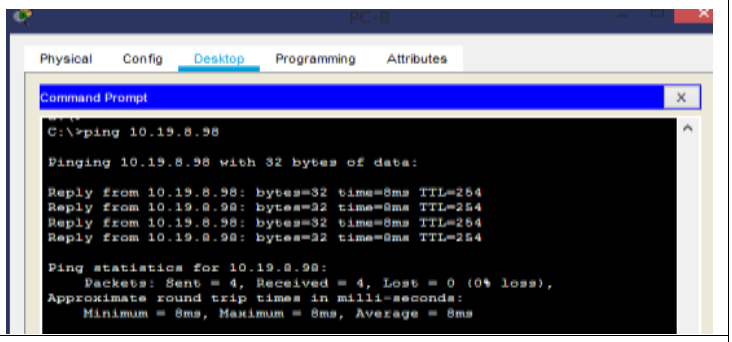
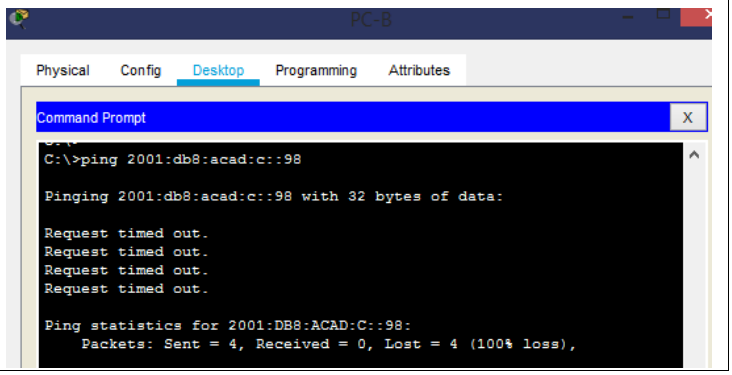
PC-A	*R1, G0/0/ 1.4*	IPv6	2001:db8:acad:c: :1	*Figura 8. Ping PcA-R1,G0/0/1.4 (IPv6)* 
PC-A	S1, VLAN 4	Dirección	10.19.8.98	*Figura 9. Ping PcA-S1,Vlan4(IP)* 
PC-A	*S1, VLAN 4*	IPv6	2001:db8:acad:c: :98	*Figura 10. Ping PcA-S1,Vlan4(IPv6)* 

PC-A	S2, VLAN 4	Dirección	10.19.8.99	*Figura 11. Ping PcA- S2,Vlan4 (IP)* 
PC-A	*S2, VLAN 4*	IPv6	2001:db8:acad:c: :99	*Figura 12. Ping PcA- S2,Vlan4 (IPv6)* 
PC-A	PC-B	Dirección	10.19.8.84	*Figura 13. Ping PcA-PcB(IP)* 

PC-A	*PC-B*	IPv6	2001:db8:acad:b: :50	*Figura 14. Ping PcA-PcB(IPv6)* 
PC-A	R1 Bucle 0	Dirección	209.165.201.1	*Figura 15. Ping PcA-R1,bucle 0 (IP)* 
PC-A	*R1 Bucle 0*	IPv6	2001:db8:acad:209: :1	*Figura 16. Ping PcA-R1, bucle 0 (IPv6)* 

PC-B	R1 Bucle 0	Dirección	209.165.201.1	*Figura 17.Ping PcB-R1, bucle 0 (IP)* 
PC-B	*R1 Bucle 0*	IPv6	2001:db8:acad:209: :1	*Figura 18. Ping PcB-R1, bucle 0 (IPv6)* 
PC-B	R1, G0/0/ 1.2	Dirección	10.19.8.1	*Figura 19. Ping PcB-R1,G0/0/1.2(IP)* 

PC-B	*R1, G0/0/ 1.2*	IPv6	2001:db8:acad:a: :1	*Figura 20. Ping PcB-R1, G0/0/1.2(IPv6)* 
PC-B	R1, G0/0/ 1.3	Dirección	10.19.8.65	*Figura 21. Ping PcB-R1, G0/0/1.3 (IP)* 
PC-B	*R1, G0/0/ 1.3*	IPv6	2001:db8:acad:b: :1	*Figura 22. Ping PcB-R1, G0/0/1.3 (IPv6)* 

PC-B	R1, G0/0/ 1.4	Dirección	10.19.8.97	*Figura 23. Ping PcB-R1, G0/0/1.4 (IP)* 
PC-B	*R1, G0/0/ 1.4*	IPv6	2001:db8:acad:c: :1	*Figura 24. Ping PcB-R1, G0/0/1.4 (IPv6)* 
PC-B	S1, VLAN 4	Dirección	10.19.8.98	*Figura 25. Ping PcB- S1, VLAN 4 (IP)* 
PC-B	*S1, VLAN 4*	IPv6	2001:db8:acad:c: :98	*Figura 26. Ping PcB- S1, VLAN 4 (IPv6)* 

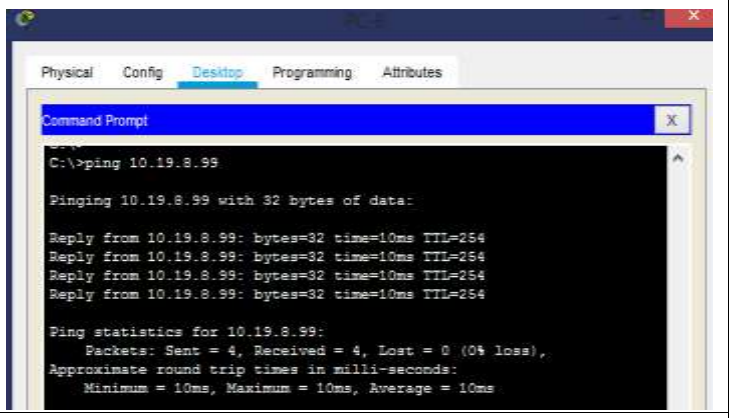
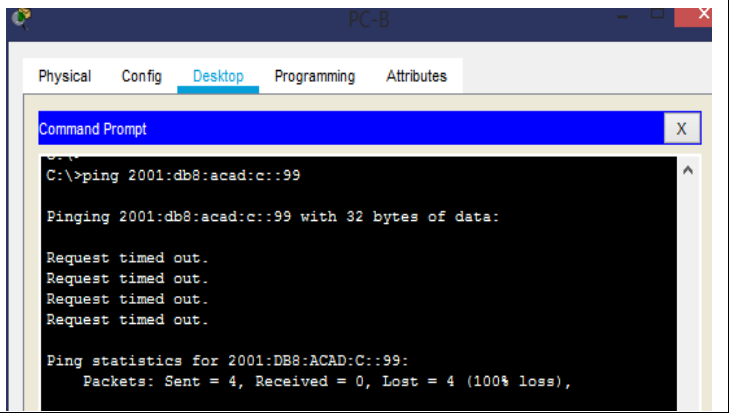
PC-B	S2, VLAN 4	Dirección	10.19.8.99.	*Figura 27. Ping PcB- S2, VLAN 4 (IP)* 
PC-B	*S2, VLAN 4*	IPv6	2001:db8:acad:c: :99	*Figura 28. Ping PcB- S2, VLAN 4 (IPv6)* 

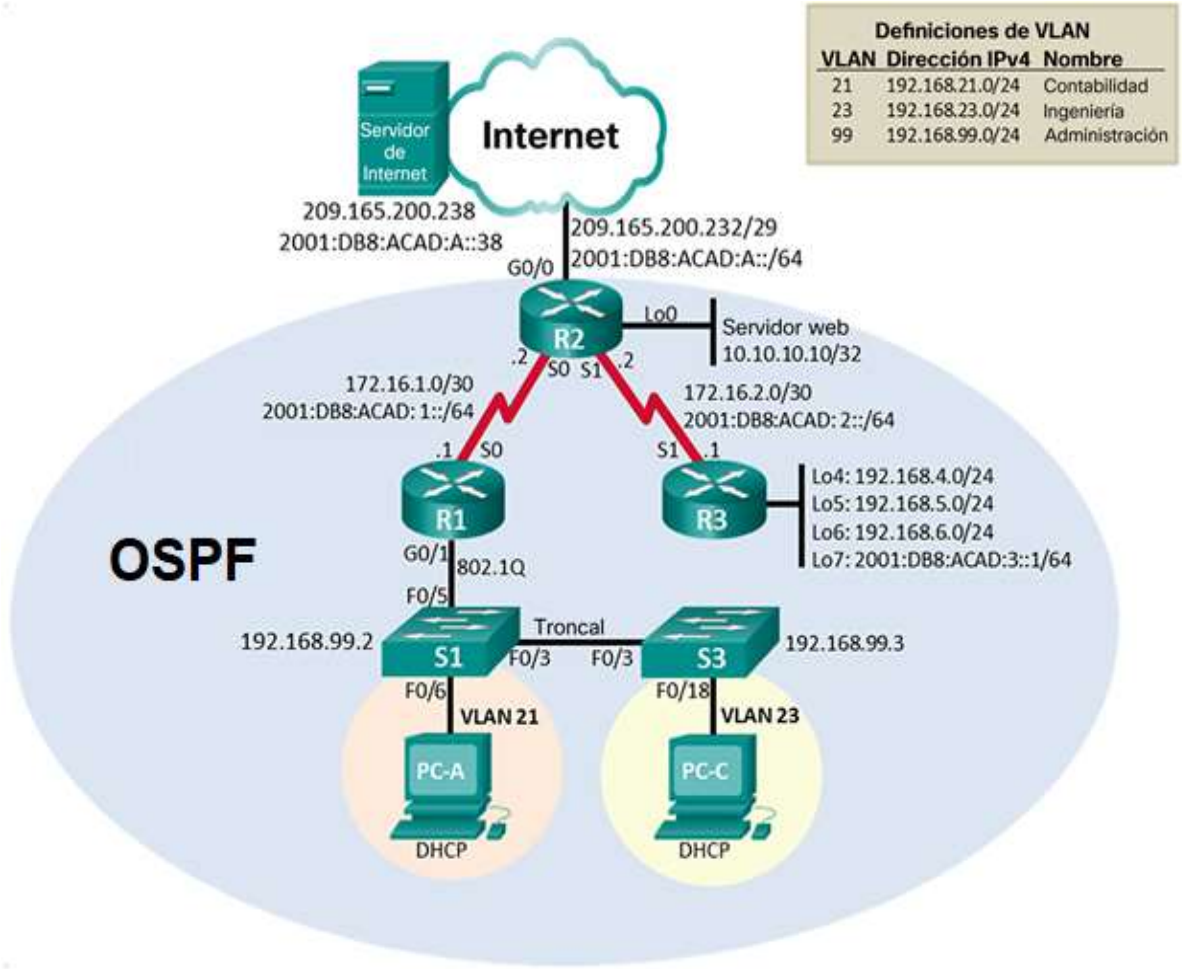
Tabla 10. Resultados ping en la red

Descripción tabla 10: Se realizaron los pings siguiendo la tabla establecida en donde se obtienen los resultados requeridos, es decir cada un de los pings fueron efectivos obteniendo respuesta tanto de las Ipv como Ipv6 destino.

ESCENARIO 2

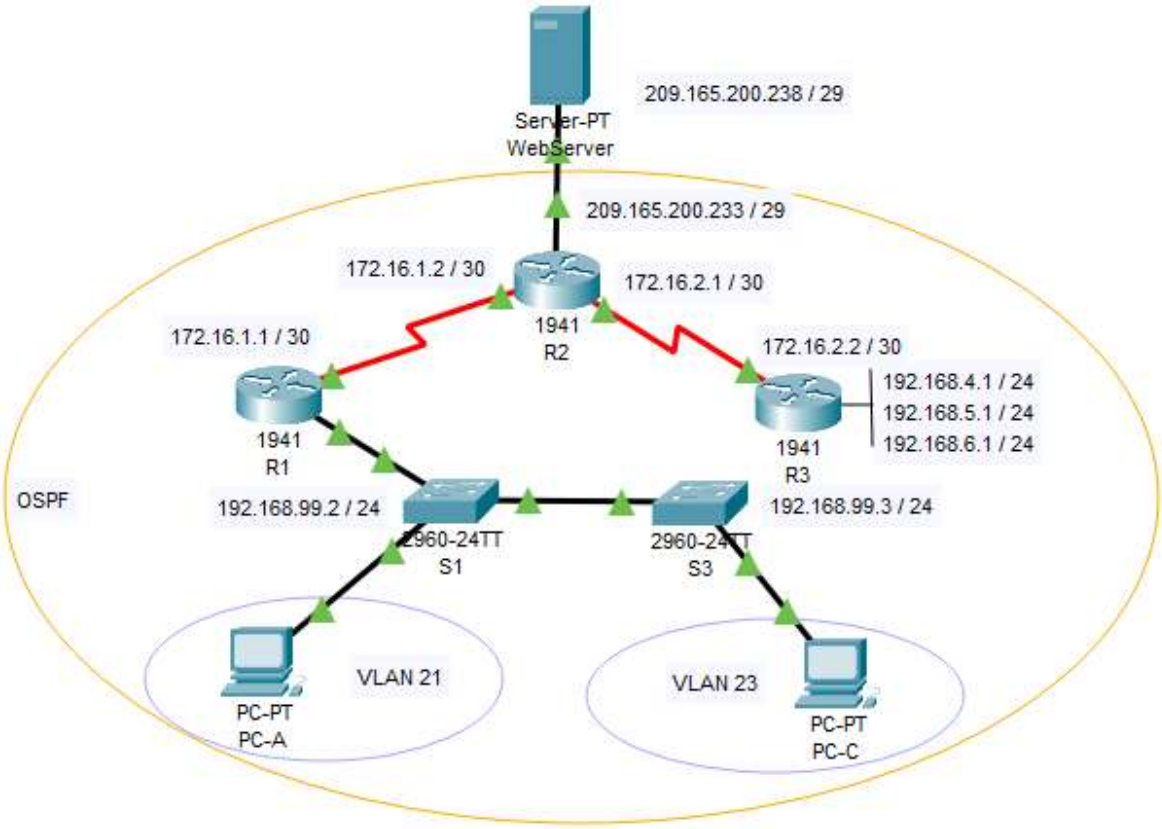
Topología

Figura 29. Topología Escenario 2



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

Figura 30. Topología del Escenario 2 simulada en Packet Tracer



Parte 5: Parte 1. Inicializar dispositivos

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

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

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

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	Para eliminar el archivo utilizamos el comando Router>enable Router#erase startup-config
Volver a cargar todos los routers	Para volver a cargar el router utilizamos el comando Router#reload

Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Al igual que en el router utilizamos el comando Switch>enable Switch#erase startup-config Para eliminar la base de datos Vlan utilizamos el comando Switch#delete vlan.dat
Volver a cargar ambos switches	Para realizar la carga de cada switch se utiliza el comando Switch#reload
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Para realizar esta verificación se puede usar el comando Switch#dir flash

Tabla 11. Inicialización de router y switches

Descripción tabla 11: Se realiza la inicialización de los routers y switchs por medio de los comandos mencionados en la tabla, de manera que estos queden sin configuración alguna para proceder a realizar la configuración desde cero de cada dispositivo.

Parte 6: Parte 2. Configurar los parámetros básicos de los dispositivos

Paso 1: Configurar la computadora de Internet

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

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.225
Dirección IPv6/subred	2001:DB8:ACAD:A::38
Gateway predeterminado IPv6	2001:DB8:ACAD:2::1

Tabla 12. Información del servidor

Descripción tabla 12: Se realiza la configuración de los parámetros básicos del servidor de internet teniendo en cuenta los datos dados; estos parámetros se configuran directamente ingresando a los datos de red del servidor.

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Para desactivar por completo la búsqueda DNS se utiliza el comando Router(config)# no ip domain-lookup
Nombre del router	Para establecer el nombre del router se utiliza el comando Router(config)# hostname R1
Contraseña de exec privilegiado cifrada	Para establece la contraseña cifrada para el ingreso a modo privilegiado se utiliza el comando R1(config)#enable secret class
Contraseña de acceso a la consola	Para establecer la contraseña de acceso a la consola se usa los siguientes comandos que permiten su respectiva configuración R1(config)#line console 0 R1(config-line)#password cisco R1(config-line)#login
Contraseña de acceso Telnet	Para establecer la contraseña de Telnet R1(config-line)#line vty 0 15 R1(config-line)#password cisco R1(config-line)#login
Cifrar las contraseñas de texto no cifrado	Para cifrar las contraseñas al mostrar los datos de configuración se utiliza el comando R1(config)#service password-encryption
Mensaje MOTD	Para establecer un mensaje de acceso no autorizado utilizamos el comando R1(config)#banner motd #Acceso no autorizado#

Interfaz S0/0/0	Para la diferente configuración a dicha interfaz utilizamos los comandos R1(config)#int s0/0/0 R1(config-if)#description connection to R2 R1(config-if)#ip add 172.16.1.1 255.255.255.252 R1(config-if)#ipv6 add 2001:db8:acad:1::1/64 R1(config-if)#clock rate 128000 R1(config-if)#no shutdown
Rutas predeterminadas	Para configurar una ruta IPv4 predeterminada de S0/0/0 utilizamos el comando R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0 Para configurar una ruta IPv6 predeterminada de S0/0/0 utilizamos el comando R1(config)#ipv6 route ::/0 s0/0/0

Tabla 13. Configuración básica R1

Nota: Todavía no configure G0/1.

Descripción tabla 13: Se realiza la configuración básica del Router 1, en donde se desactiva la búsqueda DNS, se asigna el nombre de "R1", se le configuran contraseñas que permitan el acceso limitado al router incluyendo de Telnet, se establece un mensaje se acceso no autorizado cuando se realice ingreso de contraseña incorrecta, se configuran las diferentes interfaces y por último se establen las rutas predeterminadas; Esta configuración es básica para el funcionamiento que se requiere para el Escenario 2.

Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Para desactivar por completo la búsqueda DNS se utiliza el comando Router(config)# no ip domain-lookup
Nombre del router	Para establecer el nombre del router se utiliza el comando Router(config)# hostname R2

Contraseña de exec privilegiado cifrada	Para establece la contraseña cifrada para el ingreso a modo privilegiado se utiliza el comando R2(config)#enable secret class
Contraseña de acceso a la consola	Para establecer la contraseña de acceso a la consola se usa los siguientes comandos que permiten su respectiva configuración R2(config)#line console 0 R2(config-line)#password cisco R2(config-line)#login
Contraseña de acceso Telnet	Para establecer la contraseña de Telnet R2(config-line)#line vty 0 15 R2(config-line)#password cisco R2(config-line)#login
Cifrar las contraseñas de texto no cifrado	Para cifrar las contraseñas al mostrar los datos de configuración se utiliza el comando R2(config)#service password-encryption
Habilitar el servidor HTTP	Para habilitar el servidor HTTP se utiliza el comando (sin embargo, este no funciona en este simulador) R2(config)#ip http server
Mensaje MOTD	Para establecer un mensaje de acceso no autorizado utilizamos el comando R2(config)#banner motd #Acceso no autorizado#
Interfaz S0/0/0	Para la diferente configuración a dicha interfaz utilizamos los comandos R2(config)#int s0/0/0 R2(config-if)#description connection to R1 R2(config-if)#ip add 172.16.1.2 255.255.255.252 R2(config-if)#ipv6 add 2001:db8:acad:1::2/64 R2(config-if)#no shutdown
Interfaz S0/0/1	Para la diferente configuración a dicha interfaz utilizamos los comandos R2(config)#int s0/0/1 R2(config-if)#description connection to R3 R2(config-if)#ip add 172.16.2.1 255.255.255.252 R2(config-if)#ipv6 add 2001:db8:acad:2::1/64 R2(config-if)#clock rate 128000 R2(config-if)#no shutdown

Interfaz G0/0 (simulación de Internet)	Para establecer la configuración de la interfaz del router siguiendo los lineamientos, se utilizan los siguientes comandos: R2(config-if)#interface gigabitEthernet 0/0 R2(config-if)#description connection to internet R2(config-if)#ip add 209.165.200.233 255.255.255.248 R2(config-if)#ipv6 add 2001:db8:acad:a::/64 R2(config-if)#no shutdown
Interfaz loopback 0 (servidor web simulado)	Para la configuración de la interfaz loopback 0, se implementan los siguientes comandos R2(config)#interface loopback 0 R2(config-if)# description Interface Loopback R2(config-if)#ip address 10.10.10.10 255.255.255.255 R2(config-if)#description servidor web simulado R2(config-if)#no shutdown R2(config-if)#exit
Ruta predeterminada	Para configurar una ruta IPv4 predeterminada de G0/0 utilizamos el comando R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0 Para configurar una ruta IPv6 predeterminada de G0/0 utilizamos el comando R2(config)#ipv6 route ::/0 g0/0

Tabla 14. Configuración básica R2

Descripción tabla 14: Se realiza la configuración básica del Router 2, en donde se desactiva la búsqueda DNS, se asigna el nombre de “R2”, se le configuran contraseñas que permitan el acceso limitado al router incluyendo de Telnet, se pretende habilitar el servidor HTTP(este no es posible en el simulador), se establece un mensaje se acceso no autorizado cuando se realice ingreso de contraseña incorrecta, se configuran las diferentes interfaces y por último se establen las rutas predeterminadas; Esta configuración es básica para el funcionamiento que se requiere para el Escenario 2.

Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Para desactivar por completo la búsqueda DNS se utiliza el comando Router(config)# no ip domain-lookup
Nombre del router	Para establecer el nombre del router se utiliza el comando Router(config)# hostname R3
Contraseña de exec privilegiado cifrada	Para establece la contraseña cifrada para el ingreso a modo privilegiado se utiliza el comando R3(config)#enable secret class
Contraseña de acceso a la consola	Para establecer la contraseña de acceso a la consola se usa los siguientes comandos que permiten su respectiva configuración R3(config)#line console 0 R3(config-line)#password cisco R3(config-line)#login
Contraseña de acceso Telnet	Para establecer la contraseña de Telnet R3(config-line)#line vty 0 15 R3(config-line)#pass cisco R3(config-line)#login
Cifrar las contraseñas de texto no cifrado	Para cifrar las contraseñas al mostrar los datos de configuración se utiliza el comando R3(config)#service password-encryption
Mensaje MOTD	Para establecer un mensaje de acceso no autorizado utilizamos el comando R3(config)#banner motd #Acceso no autorizado#
Interfaz S0/0/1	Para la diferente configuración a dicha interfaz utilizamos los comandos R3(config)#int s0/0/1 R3(config-if)#description connection to R2 R3(config-if)#ip add 172.16.2.2 255.255.255.252 R3(config-if)#ipv6 add 2001:db8:acad:2::2/64 R3(config-if)#no shutdown
Interfaz loopback 4	Para la configuración de la interfaz loopback 4, se implementan los siguientes comandos

	R3(config)#interface loopback 4 R3(config-if)# description Interface Loopback R3(config-if)#ip address 192.168.4.1 255.255.255.0 R3(config-if)#no shutdown
Interfaz loopback 5	Para la configuración de la interfaz loopback 5, se implementan los siguientes comandos R3(config)#interface loopback 5 R3(config-if)# description Interface Loopback R3(config-if)#ip address 192.168.5.1 255.255.255.0 R3(config-if)#no shutdown
Interfaz loopback 6	Para la configuración de la interfaz loopback 6, se implementan los siguientes comandos R3(config)#interface loopback 6 R3(config-if)# description Interface Loopback R3(config-if)#ip address 192.168.6.1 255.255.255.0 R3(config-if)#no shutdown
Interfaz loopback 7	Para la configuración de la interfaz loopback 7, se implementan los siguientes comandos R3(config)#interface loopback 7 R3(config-if)# description Interface Loopback R3(config-if)#ipv6 address 2001:db8:acad:3::1/64 R3(config-if)#no shutdown R3(config-if)#exit
Rutas predeterminadas	Para configurar una ruta IPv4 predeterminada de S0/0/1 utilizamos el comando R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1 Para configurar una ruta IPv6 predeterminada de S0/0/1 utilizamos el comando R3(config)#ipv6 route ::/0 s0/0/1

Tabla 15. Configuración básica R3

Descripción tabla 15: Se realiza la configuración básica del Router 3, en donde se desactiva la búsqueda DNS, se asigna el nombre de “R3”, se le configuran contraseñas que permitan el acceso limitado al router incluyendo de Telnet, se establece un mensaje se acceso no autorizado cuando se realice ingreso de contraseña incorrecta, se configuran las diferentes interfaces y por último se establen las rutas predeterminadas; Esta configuración es básica para el funcionamiento que se requiere para el Escenario 2.

Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Para desactivar por completo la búsqueda DNS se utiliza el comando Switch(config)# no ip domain-lookup
Nombre del switch	Para establecer el nombre del Switch se utiliza el comando Switch(config)# hostname S1
Contraseña de exec privilegiado cifrada	Para establece la contraseña cifrada para el ingreso a modo privilegiado se utiliza el comando S1(config)#enable secret class
Contraseña de acceso a la consola	Para establecer la contraseña de acceso a la consola se usa los siguientes comandos que permiten su respectiva configuración S1(config)#line console 0 S1(config-line)#password cisco S1(config-line)#login
Contraseña de acceso Telnet	Para establecer la contraseña de Telnet S1(config-line)#line vty 0 15 S1(config-line)#pass cisco S1(config-line)#login
Cifrar las contraseñas de texto no cifrado	Para cifrar las contraseñas al mostrar los datos de configuración se utiliza el comando S1(config)#service password-encryption
Mensaje MOTD	Para establecer un mensaje de acceso no autorizado utilizamos el comando S1(config)#banner motd #Acceso no autorizado#

Tabla 16. Configuración básica S1

Descripción tabla 16: Se realiza la configuración básica del Switch 1, en donde se desactiva la búsqueda DNS, se asigna el nombre de “S1”, se le configuran contraseñas que permitan el acceso limitado al router incluyendo de Telnet y se establece un mensaje se acceso no autorizado cuando se realice ingreso de contraseña incorrecta.

Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Para desactivar por completo la búsqueda DNS se utiliza el comando Switch(config)# no ip domain-lookup
Nombre del switch	Para establecer el nombre del Switch se utiliza el comando Switch(config)# hostname S3
Contraseña de exec privilegiado cifrada	Para establece la contraseña cifrada para el ingreso a modo privilegiado se utiliza el comando S3(config)#enable secret class
Contraseña de acceso a la consola	Para establecer la contraseña de acceso a la consola se usa los siguientes comandos que permiten su respectiva configuración S3(config)#line console 0 S3(config-line)#password cisco S3(config-line)#login
Contraseña de acceso Telnet	Para establecer la contraseña de Telnet S3(config-line)#line vty 0 15 S3(config-line)#pass cisco S3(config-line)#login
Cifrar las contraseñas de texto no cifrado	Para cifrar las contraseñas al mostrar los datos de configuración se utiliza el comando S3(config)#service password-encryption
Mensaje MOTD	Para establecer un mensaje de acceso no autorizado utilizamos el comando S3(config)#banner motd #Acceso no autorizado#

Tabla 17. Configuración básica S3

Descripción tabla 17: Se realiza la configuración básica del Switch 3, en donde se desactiva la búsqueda DNS, se asigna el nombre de “S3”, se le configuran contraseñas que permitan el acceso limitado al router incluyendo de Telnet y se establece un mensaje se acceso no autorizado cuando se realice ingreso de contraseña incorrecta.

Paso 7: Verificar la conectividad de la red

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

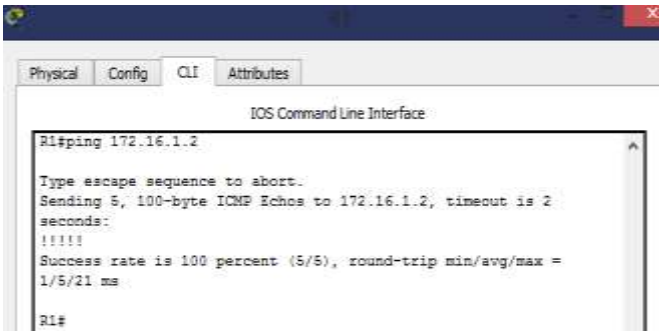
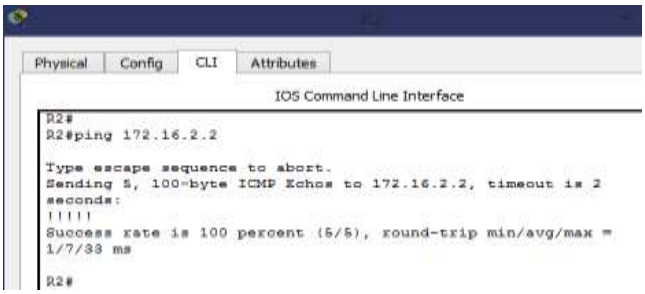
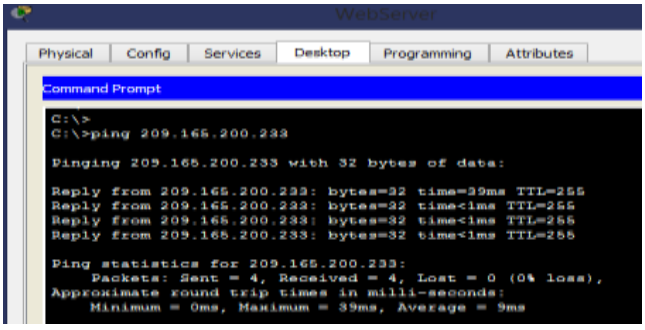
Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2/30	**El ping se realizo de manera correcta** *Figura 31. Ping prueba de conexión entre R1 y R2* 
R2	R3, S0/0/1	172.16.2.2/30	**El ping se realizo de manera correcta** *Figura 32. Ping de conexión entre R2 y R3* 
PC de Internet	R2, G0/0	209.165.200.233	**El ping se realizo de manera correcta** *Ilustración 33. Ping conexión PC y R2* 

Tabla 18. Verificación de conexión con configuración básica de los dispositivos

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

Descripción tabla 18: Se verifico la conexión por medio de ping entre los dispositivos con la configuración básica establecida, de manera que evidencio el correcto funcionamiento.

Parte 7: Parte 3. Configurar la seguridad del switch, las VLAN y el routing entre VLAN

Paso 1: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	Para crear las diferentes VLAN se utilizan los siguientes comandos para cada una de ellas: - **VLAN 21, nombre Contaduría** S1(config)#vlan 21 S1(config-vlan)#name Contaduria S1(config-vlan)#exit - **VLAN 23, nombre Ingeniería** S1(config-vlan)#vlan 23 S1(config-vlan)#name Ingeniería S1(config-vlan)#exit - **VLAN 99, nombre Administración** S1(config-vlan)#vlan 99 S1(config-vlan)#name Administración S1(config-vlan)#exit
Asignar la dirección IP de administración.	Para asignar la dirección IPv4 a la VLAN de Administración en base al diagrama de topología, se utilizan los siguientes comandos S1(config)#int vlan 99 S1(config-if)#ip add 192.168.99.2 255.255.255.0 S1(config-if)#no shutdown S1(config-if)#exit

Asignar el gateway predeterminado	Para asignar el gateway predeterminado, se utiliza el siguiente comando S1(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	Para utilizar la red VLAN 1 como VLAN nativa, se utilizan los comandos: S1(config)#int f0/3 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1
Forzar el enlace troncal en la interfaz F0/5	Para utilizar la red VLAN 1 como VLAN nativa, se usan los comandos: S1(config-if)#int f0/5 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	Para utilizar el comando interface range, se utilizan los comandos S1(config-if)#int range f0/1-2, f0/4, f0/6-24, g0/1-2 S1(config-if-range)#switchport mode access
Asignar F0/6 a la VLAN 21	Para la asignación del puerto F0/6 a la vlan 21, usamos el siguiente código: S1(config-if-range)#int f0/6 S1(config-if)#switchport access vlan 21
Apagar todos los puertos sin usar	Para apagarv los puertos que no están en uso se utiliza el comando: S1(config-if)#int range f0/1-2, f0/4, f0/7-24, g0/1-2 S1(config-if-range)#shutdown

Tabla 19. Configuración VLAN en el S1

Descripción tabla 19: En este paso se plantea la configuración de tareas que se requiere que cumpla el Switch 1 por medio de la creación de: las VLAN planteadas, la asignación de la Ip de administración, los troncos para la VLAN 1 nativa por medio de las diferentes interfaces; Además la configuración de: los puertos de acceso, la asignación de F0/6 ala la Vlan21 y finalmente apagar los puertos sin usar; Dicha configuración se realiza por medio de comandos dentro del S1

Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	Para crear las diferentes VLAN se utilizan los siguientes comandos para cada una de ellas: - **VLAN 21, nombre Contaduría** S3(config)#vlan 21 S3(config-vlan)#name Contaduria S3(config-vlan)#exit - **VLAN 23, nombre Ingeniería** S3(config-vlan)#vlan 23 S3(config-vlan)#name Ingeniería S3(config-vlan)#exit - **VLAN 99, nombre Administración** S3(config-vlan)#vlan 99 S3(config-vlan)#name Administración S3(config-vlan)#exit
Asignar la dirección IP de administración	Para asignar la dirección IPv4 a la VLAN de Administración en base al diagrama de topología, se utilizan los siguientes comandos S3(config)#int vlan 99 S3(config-if)#ip add 192.168.99.3 255.255.255.0 S3(config-if)#no shutdown S3(config-if)#exit
Asignar el gateway predeterminado.	Para asignar el gateway predeterminado, se utiliza el siguiente comando S3(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	Para utilizar la red VLAN 1 como VLAN nativa, se utilizan los comandos: S3(config)#int f0/3 S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	Para utilizar el comando interface range, se utilizan los comandos S3(config-if)#int range f0/1-2, f0/4-24, g0/1-2 S3(config-if-range)#switchport mode access

Asignar F0/18 a la VLAN 23	Para la asignación del puerto F0/18 a la vlan 23, usamos el siguiente código: S3(config-if-range)#int f0/18 S3(config-if)#switchport access vlan 23
Apagar todos los puertos sin usar	Para apagar los puertos que no están en uso se utiliza el comando: S3(config-if)#int range f0/1-2, f0/4-17, f0/19-24, g0/1-2 S3(config-if-range)#shutdown

Tabla 20. Configuración VLAN en el S2

Descripción tabla 20: En este paso se plantea la configuración de tareas que se requiere que cumpla el Switch 3 por medio de la creación de: las VLAN planteadas, la asignación de la Ip de administración, los troncos para la VLAN 1 nativa por medio de las diferentes interfaces; Además la configuración de los puertos de acceso, la asignación de F0/18 ala la Vlan23 y finalmente apagar los puertos sin usar; Dicha configuración se realiza por medio de comandos dentro del S3.

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	Para realizar la descripción de la LAN de Contabilidad, asignar la VLAN 21 y asignar la primera dirección disponible a esta interfaz, se utilizan los comandos: R1(config)#int g0/1.21 R1(config-subif)#description VLAN 21 R1(config-subif)#encapsulation dot1q 21 R1(config-subif)#ip add 192.168.21.1 255.255.255.0
Configurar la subinterfaz 802.1Q .23 en G0/1	Para realizar la descripción de la LAN de Ingeniería, asignar la VLAN 23 y asignar la primera dirección disponible a esta interfaz, se utilizan los comandos: R1(config-subif)#int g0/1.23 R1(config-subif)#description VLAN 23 R1(config-subif)#encapsulation dot1q 23 R1(config-subif)#ip add 192.168.23.1 255.255.255.0

Configurar la subinterfaz 802.1Q .99 en G0/1	Para realizar la descripción de la LAN de Administración, asignar la VLAN 99 y asignar la primera dirección disponible a esta interfaz, se utilizan los comandos: R1(config-subif)#int g0/1.99 R1(config-subif)#description VLAN 99 R1(config-subif)#encapsulation dot1q 99 R1(config-subif)#ip add 192.168.99.1 255.255.255.0
Activar la interfaz G0/1	Para realizar la activación de la interfaz G0/1 se utiliza el comando: R1(config-subif)#int g0/1 R1(config-if)#no shutdown

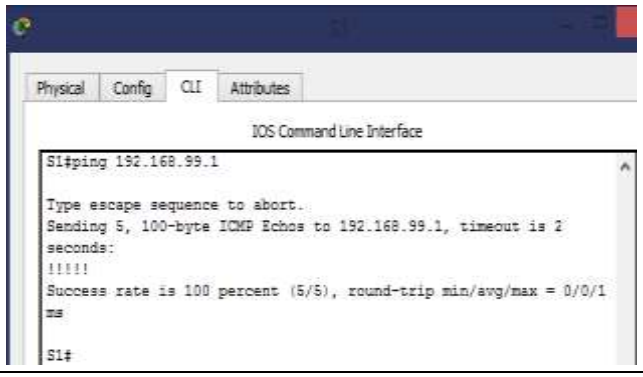
Tabla 21. Configuración de VLAN en R1

Descripción tabla 21: En este paso se plantea tareas que se requiere que cumpla el Router 1 por medio de la configuración de las subinterfaces 802.1Q.21, 802.1Q.23 y 802.1Q.99 en el puerto G0/1 y por último la activación de dicho puerto, de manera que estas queden enlazadas.

Paso 4: Verificar la conectividad de la red

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

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

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	**El ping se realizo de manera correcta** *Figura 34. Ping de S1 hacia R1* 

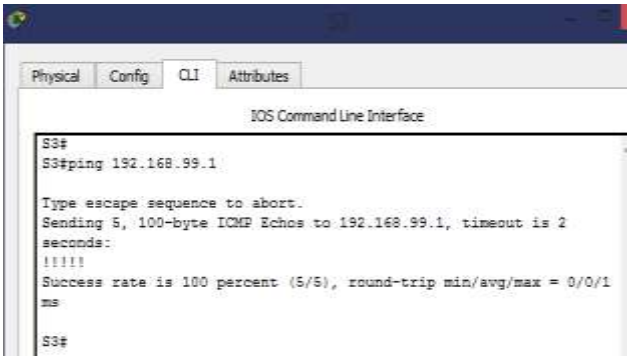
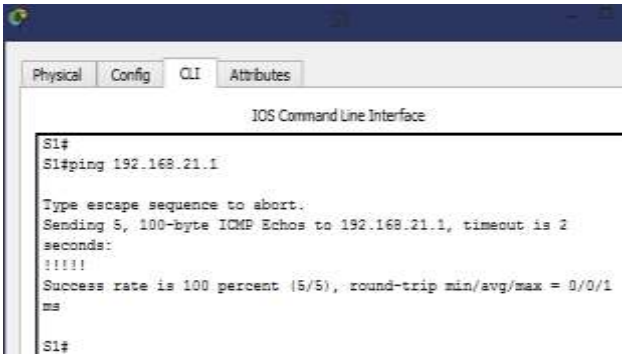
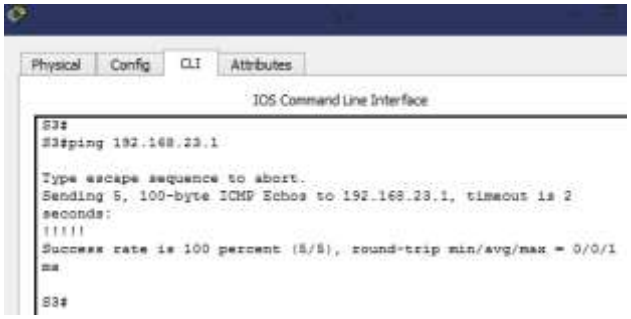
S3	R1, dirección VLAN 99	192.168.99.1	**El ping se realizo de manera correcta** *Figura 35. Ping de S3 hacia R1* 
S1	R1, dirección VLAN 21	192.168.21.1	**El ping se realizo de manera correcta** *Figura 36. Ping de S1 hacia R1* 
S3	R1, dirección VLAN 23	192.168.23.1	**El ping se realizo de manera correcta** *Figura 37. Ping de S3 hacia R1* 

Tabla 22. Verificación de conexión de la red

Descripción tabla 22: Se verifica la conexión de a red con la configuración básica y los parámetros dados tanto a los Switchs como a los Routers, de manera que se muestra el correcto funcionamiento y conexión entre dispositivos por medio del comando ping.

Parte 8: Parte 4. Configurar el protocolo de routing dinámico OSPF

Paso 1: Configurar OSPF en el R1

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	Para configurar Ospf área 0, se utiliza el comando: R1(config)# router ospf 1
Anunciar las redes conectadas directamente	Para asignar todas las redes conectadas directamente se utiliza los siguientes comandos: R1(config-router)# network 192.168.21.0 0.0.0.255 área 0 R1(config-router)# network 192.168.23.0 0.0.0.255 área 0 R1(config-router)# network 192.168.99.0 0.0.0.255 área 0 R1(config-router)# network 172.16.1.0 0.0.0.3 área 0
Establecer todas las interfaces LAN como pasivas	Para establecer las interfaces Lan como pasivas, se utiliza el siguiente comando: R1(config-router)# passive-interface g0/1 R1(config-router)# passive-interface s0/0/1
Desactive la sumarización automática	Para desactivar la sumarización automática, se utiliza el comando: R1(config-router)# no auto-summary R1(config-router)# end

Tabla 23. Configuración de OSPF en R1

Descripción tabla 23: Para este paso se realiza la configuración de OSPF área 0 en el R1, en donde se anuncian las redes conectadas directamente y se establecen las interfaces Lan como pasivas; de manera que este permita tomar el camino mas corto establecido por las indicaciones de conexión directa. Además, se desactiva la sumarización automática.

Paso 2: Configurar OSPF en el R2

La configuración del R2 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	Para configurar Ospf área 0, se utiliza el comando: R2(config)# router ospf 1
Anunciar las redes conectadas directamente	Para asignar las redes conectadas directamente se utilizan los comandos: R2(config-router)# network 172.16.1.0 0.0.0.3 área 0 R2(config-router)# network 172.16.2.0 0.0.0.3 área 0
Establecer la interfaz LAN (loopback) como pasiva	Para establecer las interfaces Lan(loopback) como pasivas, se utiliza el siguiente comando: R2(config-router)# passive-interface loopback 0
Desactive la sumarización automática.	Para desactivar la sumarización automática, se utiliza el comando: R2(config-router)# no auto-summary R2(config-router)# end

Tabla 24. Configuración de OSPF en R2

Descripción tabla 24: Para este paso se realiza la configuración de OSPF área 0 en el R2, en donde se anuncian las redes conectadas directamente y se establece la interfaz Lan (Loopback) como pasiva; de manera que este permita tomar el camino más corto establecido por esta indicación de conexión directa. Además, se desactiva la sumarización automática.

Paso 3: Configurar OSPF en el R3

La configuración del R3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	Para configurar Ospf área 0, se utiliza el comando: R3(config)# router ospf 1

Anunciar redes IPv4 conectadas directamente	Para asignar las redes conectadas directamente se utilizan los comandos: R3(config-router)# network 172.16.2.0 0.0.0.3 área 0 R3(config-router)# network 192.168.4.0 0.0.0.255 área 0 R3(config-router)# network 192.168.5.0 0.0.0.255 área 0 R3(config-router)# network 192.168.6.0 0.0.0.255 área 0
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	Para establecer las interfaces Lan(loopback) como pasivas, se utiliza el siguiente comando: R3(config-router)# passive-interface loopback 4 R3(config-router)# passive-interface loopback 5 R3(config-router)# passive-interface loopback 6
Desactive la sumarización automática.	Para desactivar la sumarización automática, se utiliza el comando: R2(config-router)# no auto-summary R2(config-router)# end

Tabla 25. Configuración de OSPF en R3

Descripción tabla 25: Para este paso se realiza la configuración de OSPF área 0 en el R3, en donde se anuncian las redes Ipv4 conectadas directamente y se establecen las interfaces Lan (Loopback) como pasivas; de manera que este permita tomar el camino más corto establecido por esta indicación de conexión directa. Además, se desactiva la sumarización automática.

Paso 4: Verificar la información de OSPF

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

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?	Para conocer la información configurada en OSPF utilizamos el comando: R1#show ip protocols

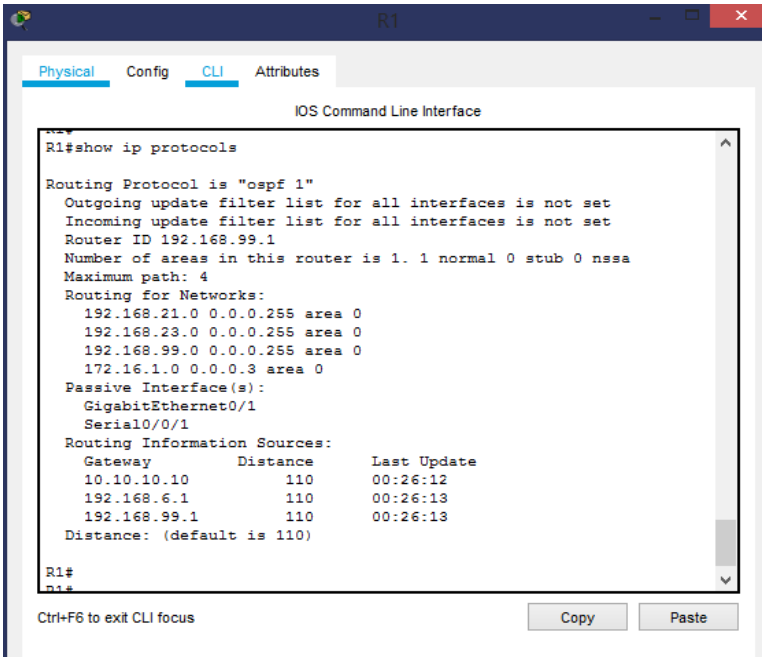
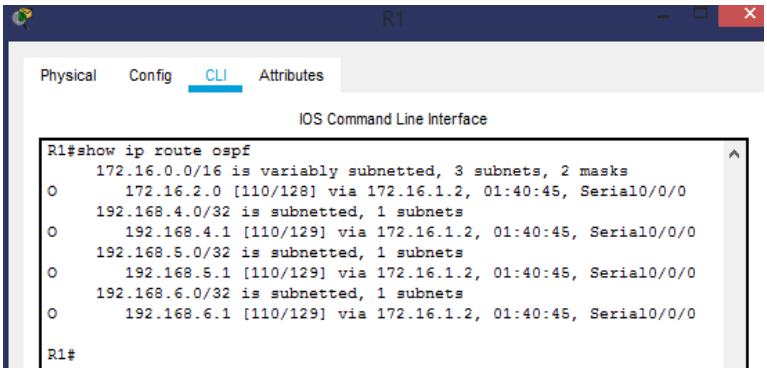
	Figura 38. Verificación de información configurada en OSPF 
¿Qué comando muestra solo las rutas OSPF?	Para mostrar solo las rutas OSPF descubiertas en la tabla de routing se utiliza el comando R1#show ip route ospf *Figura 39. Verificación de rutas OSPF* 
¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	Para conocer la sección de OSPF de la configuración en ejecución se utiliza el comando: R1#show ip ospf

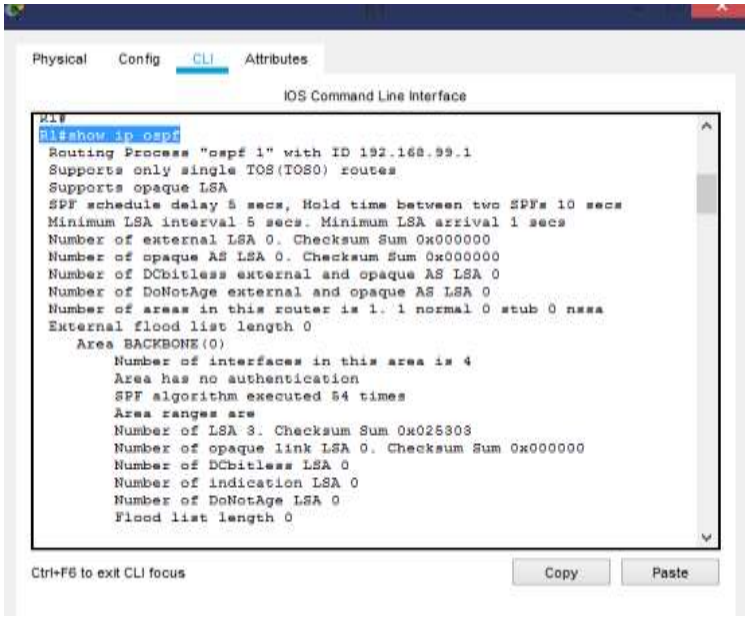
	Figura 40. Verificación de la OSPF en ejecución 

Tabla 26. Verificación de conexión con configuración OSPF

Descripción tabla 26: Se verifica la conexión con la configuración OSPF asignada a los dispositivos, por medio de los diferentes comandos que permiten mostrar el correcto funcionamiento de ello.

Parte 9: Parte 5. Implementar DHCP y NAT para IPv4

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

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	Para reservar las primeras 20 direcciones IP en la VLAN 21 se utiliza el comando: R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20

Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	Para reservar las primeras 20 direcciones IP en la VLAN 23 se utiliza el comando: R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20
Crear un pool de DHCP para la VLAN 21.	Para la creación de un pool de DHCP para la VLAN 21 se utiliza los comandos según las indicaciones: 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
Crear un pool de DHCP para la VLAN 23	Para la creación de un pool de DHCP para la VLAN 23 se utiliza los comandos según las indicaciones: R1(dhcp-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

Tabla 27. Configuración de R1 como servidor de DHCP

Descripción tabla 27: En este paso se configura el Router 1 como servidor DHCP para las Vlan 21 y 23, reservando las primeras 20 direcciones Ip para configuración estáticas en cada una de las Vlan mencionadas. Además, se crea un pool de DHPC para cada una de ellas.

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

La configuración del R2 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	Para crear una base de datos local con una cuenta de usuario se utiliza el comando: R2(config)#username webuser privilege 15 secret cisco12345 Nombre de usuario: **webuser** Contraseña: **cisco12345** Nivel de privilegio: **15**

Habilitar el servicio del servidor HTTP	Para habilitar el servicio del servidor HTTP se utiliza el comando: R2(config)#ip http server
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	**Nota**: Este comando no es soportado en packet tracer Para esta configuración y utilizar la base de datos local para la autenticación se utiliza el comando: R2(config)#ip http authentication local
Crear una NAT estática al servidor web.	Para crear una NAT estática al servidor web se utiliza los comandos: R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229
Asignar la interfaz interna y externa para la NAT estática	Para asignar la interfaz interna y externa para la NAT estática se utilizan los comandos: R2(config)#int g0/0 R2(config-if)#ip nat outside R2(config-if)#int s0/0/0 R2(config-if)#ip nat inside R2(config-if)#int s0/0/1 R2(config-if)#ip nat inside R2(config-if)#exit
Configurar la NAT dinámica dentro de una ACL privada	Para la configuración dentro de una ACL privada se usan los comandos: R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255
Defina el pool de direcciones IP públicas utilizables.	Para definir el pool de direcciones IP publicas utilizables se utiliza el comando: R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248
Definir la traducción de NAT dinámica	Para la definir la traducción de NAT dinámica se utiliza el comando: R2(config)#ip nat inside source list 1 pool INTERNET

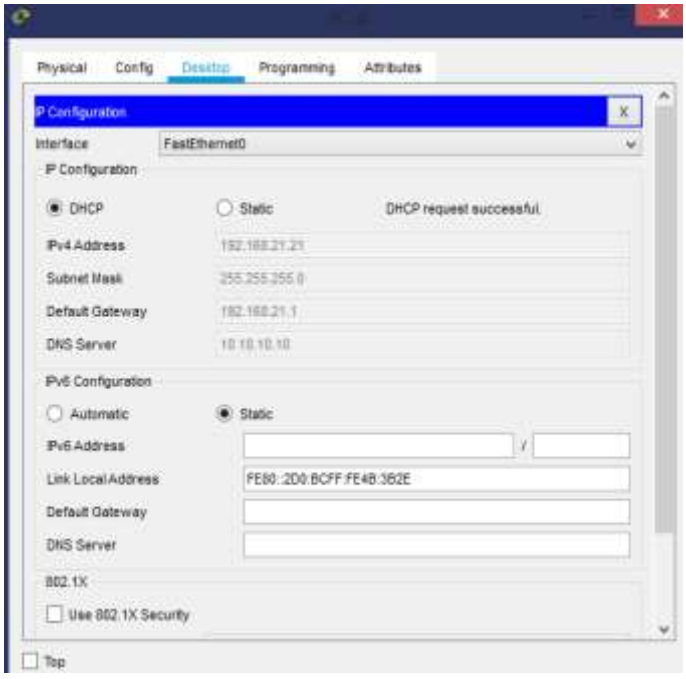
Tabla 28. Configuración de NAT estática y dinámica en R2

Descripción tabla 28: Para este paso se realiza la configuración NAT estática y dinámica en el Router 2 creando una base de datos local con cuenta se usuario, configurando el servidor Http para utilizar la base de datos local para la autenticación, además se crea una Nat estática al servidor web y se le asigna la

interfaz interna y externa; dicha Nat se configura dentro de una ACL privada. Por otra parte, se define el pool de direcciones Ip publicas utilizables y se define la traducciones de Nat dinámica.

Paso 3: Verificar el protocolo DHCP y la NAT estática

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

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	**Se hace la verificación en la PC-A** *Figura 41. Verificación DHCP en la PC-A* 

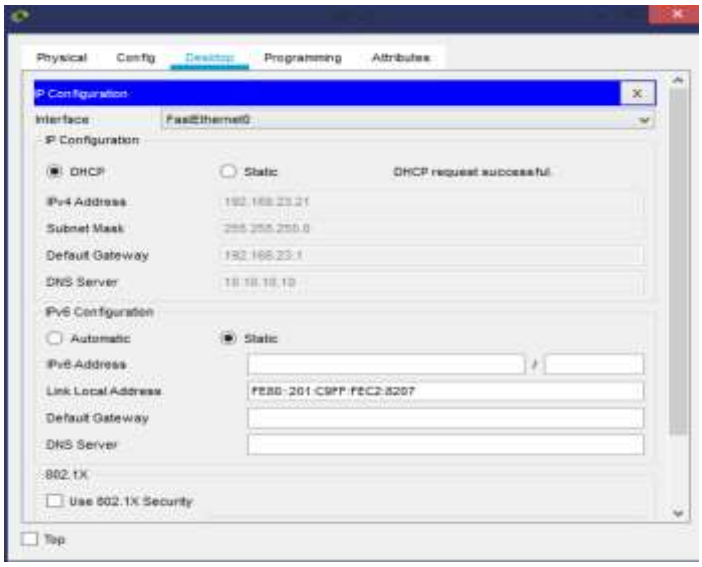
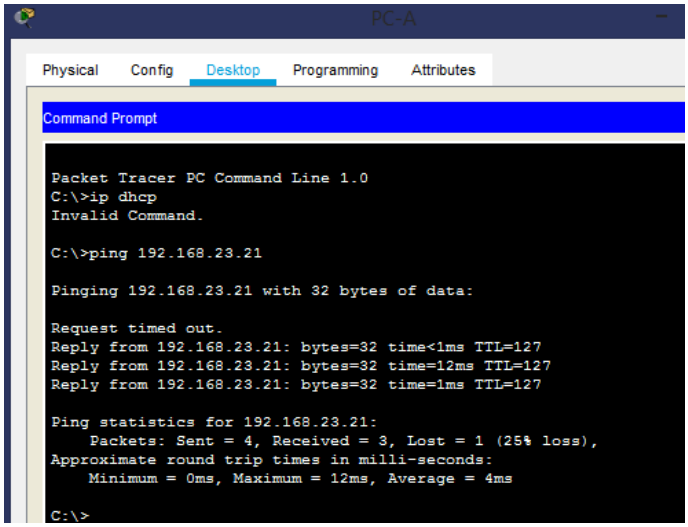
<table>
<tr>
<td>Verificar que la PC-C haya adquirido información de IP del servidor de DHCP</td>
<td><u>Se hace la verificación en la PC-C</u>
Figura 42. Verificación DHCP n la PC-B
 
</td>
</tr>
<tr>
<td>Verificar que la PC-A pueda hacer ping a la PC-C
Nota: Quizá sea necesario deshabilitar el firewall de la PC.</td>
<td><u>Se verifica a través del comando ping</u>
Figura 43. Verificación por medio de comando ping
 
</td>
</tr>
</table>

Tabla 29. Verificación de protocolo DHCP y NAT estática

Descripción tabla 29: Se verifica la conexión con la configuración DHCP y NAT asignada a los dispositivos, por medio del ingreso a la configuración de ellos y por último por medio del comando ping que permiten mostrar el correcto funcionamiento de ellos.

Parte 10: Parte 6. Configurar NTP

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	**5 de marzo de 2016, 9 a. m.** Para realizar estos ajustes según lo que se indica se utiliza el comando: R2#clock set 09:00:00 05 march 2016
Configure R2 como un maestro NTP.	Nivel de estrato: **5** Para asignar R2 como un maestro NTP se utiliza el comando: R2(config)#ntp master 5
Configurar R1 como un cliente NTP.	Servidor: **R2** Para configurar R1 como cliente NTP se utiliza el comando: R1(config)#ntp server 172.16.1.2
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	Para configurar R1 para actualizaciones de calendario periódicas con hora NTP se utiliza el comando: R1(config)#ntp update-calendar

Verifique la configuración de NTP en R1.	Para verificar la configuración de NTP en R1 se utiliza el comando:
	R1#show ntp associations
	`R1#show ntp associations`
	`address ref clock st when poll reach delay offset disp`
	`~172.16.1.2 127.127.1.1 5 13 16 7 2.00 725727144500.00 0.12`
	`* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured`

Tabla 30. Configuración NTP

Descripción tabla 30: Se configura NTP en el R1 y R2 por medio de los comandos mostrados en dicha tabla. Se ajusta fecha y hora en R2, se configura R2 como maestro, se configura R1 como cliente Ntp, y finalmente se verifica la configuración establecida.

Parte 11: Parte 7. Configurar y verificar las listas de control de acceso (ACL)

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

Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	Para realizar esta configuración se usan los comandos: R2(config)#ntp master 5 R2(config)#ip access-list standard ADMIN-MGT R2(config-std-nacl)#permit host 172.16.1.1 R2(config-std-nacl)#exit
Aplicar la ACL con nombre a las líneas VTY	Para aplicar la ACL se utiliza los comandos: R2(config)#line vty 0 15 R2(config-line)#access-class ADMIN-MGT in
Permitir acceso por Telnet a las líneas de VTY	Para permitir el acceso Telnet se usa el comando: R2(config-line)#transport input telnet

Verificar que la ACL funcione como se espera	Para hacer la verificación se hace mediante el comando:
	R1#telnet 172.16.1.2
	Figura 44. Verificación ACL
	`R2#telnet 172.16.1.2`
	`Trying 172.16.1.2 ...`
	`% Connection refused by remote host`

Tabla 31. Restricción de acceso VTY en R2

Descripción tabla 31: Se configura y verifica las listas de control de acceso por medio de la configuración de dicha lista que permite que solo R1 establezca conexión Telnet con R2, se aplica la Acl con nombre a las líneas Vty y se permite el acceso por Telnet a dichas líneas. Enseguida se verifica que la ACL funciones como se espera.

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

Descripción del comando	Entrada del estudiante (comando)

Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	Para mostrar las condiciones recibidas se utiliza el comando:
	R2#show ip access-list
	
	Figura 45. Coincidencias recibidas por lista de acceso
	
	`R2#show ip access-list`
	`Standard IP access list 1`
	`    10 permit 192.168.21.0 0.0.0.255 (10 match(es))`
	`    20 permit 192.168.23.0 0.0.0.255 (4 match(es))`
	`    30 permit 192.168.4.0 0.0.3.255`
	`Standard IP access list ADMIN-MGT`
	`    10 permit host 172.16.1.1`

Restablecer los contadores de una lista de acceso	Para restablecer los contadores se utiliza el comando: R2#clear ip access-list counters

¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	Para mostrar que ACL se aplica se utiliza el comando:
	R2# show ip interface
	
	Figura 46. ACL en una interfaz
	
	`R2#show ip interface`
	`GigabitEthernet0/0 is up, line protocol is up (connected)`
	`  Internet address is 209.165.200.233/29`
	`  Broadcast address is 255.255.255.255`
	`  Address determined by setup command`
	`  MTU is 1500 bytes`
	`  Helper address is not set`
	`  Directed broadcast forwarding is disabled`
	`  Outgoing access list is not set`
	`  Inbound  access list is not set`
	`  Proxy ARP is enabled`
	`  Security level is default`
	`  Split horizon is enabled`
	`  ICMP redirects are always sent`
	`  ICMP unreachables are always sent`
	`  ICMP mask replies are never sent`
	`  IP fast switching is disabled`
	`  IP fast switching on the same interface is disabled`
	`  IP Flow switching is disabled`
	`  IP Fast switching turbo vector`
	`  IP multicast fast switching is disabled`
	`  IP multicast distributed fast switching is disabled`
	`  Router Discovery is disabled`
	`--More--`

¿Con qué comando se muestran las traducciones NAT?	Para mostrar las traducciones NAT se utiliza el comando: R2#show ip nat translations *Figura 47. Traducciones NAT* R2#show ip nat translations Pro Inside global Inside local Outside local Outside global --- 209.165.200.229 10.10.10.10 --- --- tcp 209.165.200.225:1031192.168.21.21:1031 209.165.200.229:80 209.165.200.229:80 tcp 209.165.200.225:1032192.168.21.21:1032 209.165.200.229:80 209.165.200.229:80 tcp 209.165.200.225:1033192.168.21.21:1033 209.165.200.229:80 209.165.200.229:80 tcp 209.165.200.225:1034192.168.21.21:1034 209.165.200.229:80 209.165.200.229:80 tcp 209.165.200.225:1035192.168.21.21:1035 209.165.200.229:80 209.165.200.229:80 tcp 209.165.200.226:1025192.168.23.21:1025 209.165.200.229:80 209.165.200.229:80 tcp 209.165.200.226:1026192.168.23.21:1026 209.165.200.229:80 209.165.200.229:80 R2#
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	Para eliminar las traducciones de NAT dinámicas se usa el comando: R2#clear ip nat translation * *Figura 48. Eliminación de Traducciones NAT* R2#clear ip nat translation * R2# R2# R2#show ip nat translations Pro Inside global Inside local Outside local Outside global --- 209.165.200.229 10.10.10.10 --- --- R2#

Tabla 32. Comandos CLI

Descripción tabla 32: En este paso por medio de la pestaña Cli y el uso de comandos se muestran las coincidencias recibidas por una lista de acceso desde la ultima vez que se restableció, además se restablece los contadores de dicha lista de acceso y finalmente se muestra que ACL se aplica a una interfaz y la dirección en que se aplica. Por otra parte, se muestran las traducciones Nat y se indica el comando para eliminar dichas traducciones.

CONCLUSIONES

Escenario 1: Se implementa la configuración básica en redes, en donde implico realizar inicialización, carga y configuración básica de routers y swichts, configuración de host y la configuración de servidores, todo ello a través de comandos y seguidamente se verifico su correcto funcionamiento, haciendo que los dispositivos de la red pudieran interactuar de manera satisfactoria.

Escenario 2: Se implementa la configuración básica de los dispositivos realizando su inicialización, carga y configuración básica; Además se logra configurar Vlan, el protocolo Ospf, Dhcp, Nat y Ntp, dando asi la posibilidad de poner en práctica los conocimientos adquiridos durante el Diplomado y logrando finalmente que la red tenga los resultados esperados.

BIBLIOGRAFÍA

CISCO. (2019). Exploración de la red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#1

CISCO. (2019). Configuración de un sistema operativo de red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#2

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

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

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

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

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

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

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

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

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

CISCO. (2019). Configuración del Switch. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#5

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

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

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

ANEXO

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

Aychel Andrea González Díaz
UNAD (Universidad Nacional Abierta y a Distancia), aagonzalezd@unadvirtual.edu.co

Resumen

Para este informe se implementan los conocimientos adquiridos durante el Diplomado de Introducción a las redes y Principios básicos de routing y switching que ofrece CISCO y el cual nos permite conocer más de cerca el funcionamiento de redes básicas y por medio de plataformas poder simular para aprender a configurar a través de comandos y así mismo verificar su correcto funcionamiento. Con el apoyo del entorno de conocimiento y del instructor se logra conocer, aplicar, verificar e implementar redes pequeñas a través de aplicaciones, desarrollando en los aprendices aptitudes necesarias para planificar e implementar redes. El material implementado facilita la manera en la que nosotros como estudiantes trabajamos, vivimos, y aprendemos mediante estrategias de comunicaciones de voz, video y otros datos.

Palabras clave: CISCO, ipv4, ipv6, packet tracer, redes.

Abstract:

For this report are implemented the acquired knowledge during the Diplomado in Introduction to networks and basic principles of routing and switching that Cisco offers and which allows to know us more closely the operation of core networks and through platforms to simulate to learn configure through commands and also verify its correct operation. With the support of the knowledge environment and the instructor, it is possible to know, apply, verify and implement small networks through applications, developing in the learners the necessary skills to plan and implement networks. The implemented material facilitates the way in which we as students work, live, and learn through voice, video and other data communication strategies.

Keywords— CISCO, ipv4, ipv6, networks, packet tracer.

I. INTRODUCCIÓN

Hoy en día la humanidad tiene la necesidad de interactuar diariamente con cada innovación que se presenta, debido a que crece el interés de saber para qué y cómo funciona la tecnología en la mayoría de ámbitos. Además de ello la comunicación hoy en día se hace casi tan como el aire, el agua, los alimentos y un lugar para vivir. Es así como el día de hoy las redes se usan por casi toda la humanidad debido a que la necesidad de comunicarse por los diferentes medios implica el uso de dichas redes. Por medio del entorno implementado en el aprendizaje de la configuración básica, la arquitectura, los componentes y el funcionamiento de los routers y switches en una red pequeña, se logra dar paso a paso en el crecimiento como Ingeniero de Sistemas capaz de desarrollar y conocer acerca de las redes. Las redes tienen un impacto considerable en nuestras vidas, estas cambiaron la forma en que vivimos, trabajamos y jugamos. Es por ello que hoy en día las redes nos permiten comunicarnos, colaborar e interactuar como nunca antes, ya que las utilizamos de distintas formas, como en las aplicaciones web, la telefonía IP, la videoconferencia, los juegos interactivos, el comercio electrónico, la educación y más.

II. REPRESENTACIÓN Y CONFIGURACIÓN DE REDES PEQUEÑAS EN EL SIMULADOR PACKET TRACER

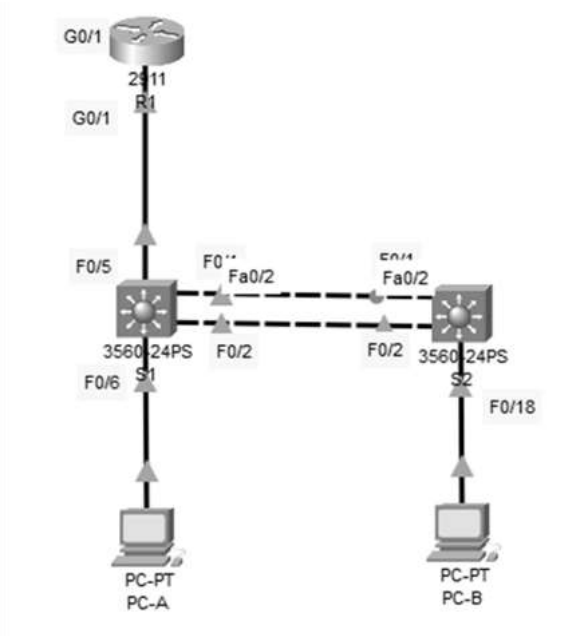
Hoy en día encontramos redes de todo tamaño, desde redes simples compuestas por dos PC, hasta redes que conectan millones de dispositivos con el objetivo de compartir recursos, ya sean de hardware o de software. Es así como se ve la importancia del uso de redes para la comunicación en todos los ámbitos de la cotidianidad. Por medio de la plataforma Cisco quien nos brindó los conocimientos básicos de redes, para la correcta conexión de los diferentes dispositivos en varios tipos de red y su configuración por medio de comandos los cuales permitieron que la conexión se hiciera de manera satisfactoria, y de esta manera exponer los conocimientos adquiridos en diferentes simulaciones de redes. De esta manera se exponen dos escenarios de redes simuladas en Packet Tracer obteniendo los siguientes resultados:

A. Escenario 1

Para este primer caso se plantea la configuración de los dispositivos de una red pequeña, en donde se pretende el

correcto funcionamiento y configuración de un router, un switch y equipos que admiten conectividad IPv4 e IPv6 para los hosts soportados; estos deben administrarse de forma segura. En la figura 1, podremos visualizar la simulación realizada:

Figura 49. Simulación de Escenario 1 en Packet Tracer



Resultados: Se implementa la configuración básica en redes, en donde implico realizar inicialización, carga y configuración básica de routers y swichts, configuración de host y la configuración de servidores, todo ello a través de comandos. Seguidamente se verifico su correcto funcionamiento por medio de pruebas de conexión entre dispositivos, haciendo que los dispositivos de la red pudieran interactuar de manera satisfactoria. Enseguida se muestra la figura 2 y la figura 3, de verificación de la conexión:

Figura 50. Ping desde el PC-A hacia el Router 1

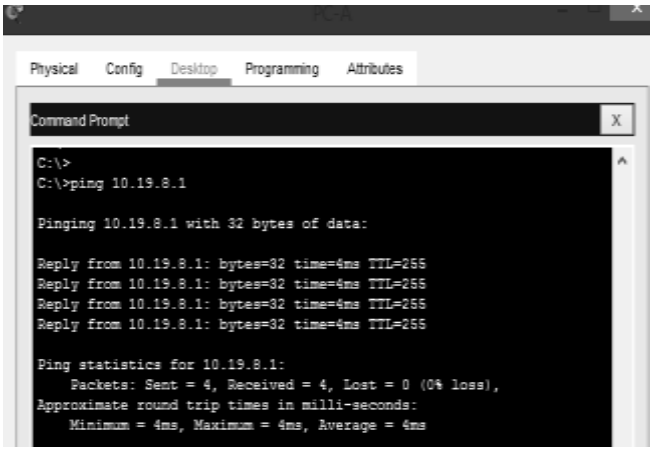
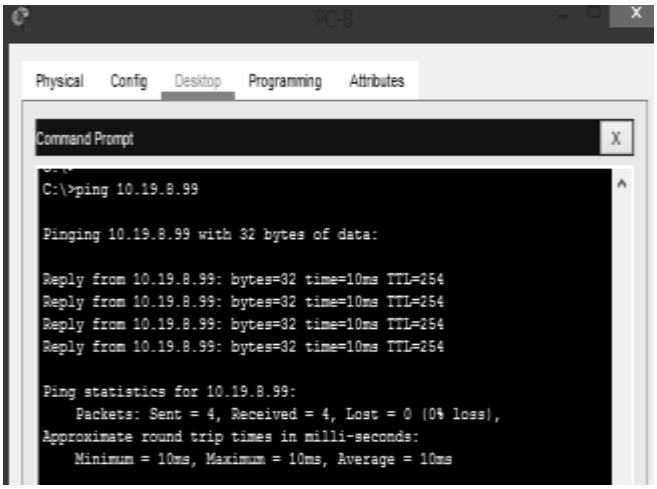


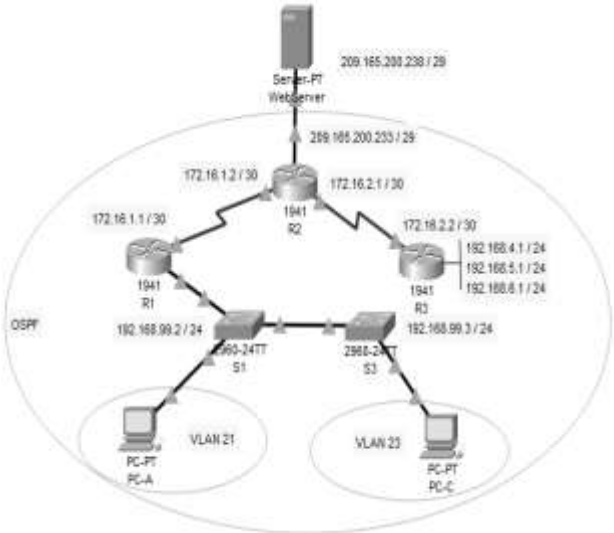
Figura 51. Ping desde la PC-B hacia el Swicht 2



B. Escenario 2

Para el segundo caso se plantea la configuración de una red pequeña que admita IPv4 e IPv6, además tenga 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. De esta manera se plantea la simulación representada en la figura 4:

Figura 52. Simulación del Escenario 2 en Packet Tracer



Resultados: Se implementa la configuración básica de los dispositivos realizando su inicialización, carga y configuración básica; Además se configuran las Vlan

planteadas, el protocolo Ospf, Dhcp, Nat y Ntp por medio de los comandos establecidos para cada uno de los dispositivos y tipo de configuración. De esta manera se da la posibilidad de poner en práctica los conocimientos adquiridos durante el Diplomado y logrando finalmente que la red tenga los resultados esperados. Enseguida se muestra la figura 5 y la figura 6, de verificación de la conexión:

Figura 53. Verificación de conexión por medio de Ping desde PC-A hacia PC-B

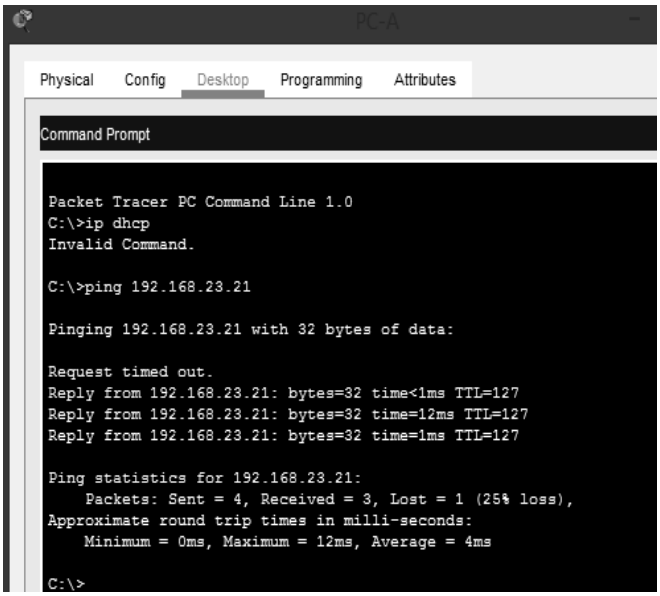


Figura 54. Verificación de información configurada en OSPF

III. CONCLUSIONES

Escenario 1: Se implementa la configuración básica en redes, en donde implico realizar inicialización, carga y configuración básica de routers y swichts, configuración de host y la configuración de servidores, todo ello a través de comandos y seguidamente se verifico su correcto funcionamiento, haciendo que los dispositivos de la red pudieran interactuar de manera satisfactoria.

Escenario 2: Se implementa la configuración básica de los dispositivos realizando su inicialización, carga y configuración básica; Además se logra configurar Vlan, el protocolo Ospf, Dhcp, Nat y Ntp, dando asi la posibilidad de poner en práctica los conocimientos adquiridos durante el Diplomado y logrando finalmente que la red tenga los resultados esperados.

IV. Referencias

[1] CISCO. (2019). Exploración de la red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#1E.

[2] CISCO. (2019). Configuración de un sistema operativo de red. Fundamentos de Networking. Recuperado de: https://static-course assets.s3.amazonaws.com/ITN6/es/index.html#2

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

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

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

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

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

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

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

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

[11] CISCO. (2019). Routing Dinámico. Principios de Enrutamiento y Conmutación. Recuperado de:

https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#3
[12] CISCO. (2019). Configuración del Switch. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#5
[13] CISCO. (2019). VLAN. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#6
[14] CISCO. (2019). NAT para IPv4. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#9
[15] CISCO. (2019). Detección, Administración y Mantenimiento de Dispositivos. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#10

BIOGRAFÍA

Aychel Andrea González Díaz (1994 -) nació en Duitama - Boyacá el 7 de febrero de 1994, cursó sus estudios de básica primaria y secundaria en el colegio Guillermo León Valencia de la ciudad de Duitama, en la actualidad se desempeña como estudiante activo en el programa de Ingeniería de Sistemas en la Universidad Nacional Abierta y a Distancia (UNAD).