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

LAURA NATALIA GALEANO RINCÓN

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍAS E INGENIERÍAS-ECBTI
INGENIERÍA DE SISTEMAS

TUNJA
2020

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

LAURA NATALIA GALEANO RINCÓN

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

TUTORA:
PAULITA FLOR SALAZAR

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍAS E INGENIERÍAS-ECBTI
INGENIERÍA DE SISTEMAS
TUNJA
2020

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____

_____

FIRMA DEL TUTOR

_____

FIRMA DEL JURADO

Tunja, 30 de Noviembre de 2020

AGRADECIMIENTOS

Gracias a mis queridos padres por ser los principales impulsadores de cada uno de mis sueños, gracias a ellos por brindarme su apoyo incondicional, gracias a mi madre por darme animo cada larga y agotadora noche que le dedique a este trabajo; gracias a mi padre por siempre desear lo mejor para mi vida, gracias por cada consejo y por cada una de sus palabras que me han guiado hasta este momento.

Gracias a la Unad, por brindarme la oportunidad de formarme en ella, por brindarme los recursos necesarios para mi aprendizaje, gracias a todos aquellos que directa o indirectamente me han colaborado con mi formación.

.

TABLA DE CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

DHCP: Es un servidor de Red el cual permite una asignación automática de direcciones IP, getaways predeterminadas, así como otros parámetros de red que necesiten los clientes.

Ipv4: El protocolo IPv4 es uno de los protocolos fundamentales de Internet, ya que es el que identifica los diferentes dispositivos conectados a la red.

Ipv6: Es la versión 6 del Protocolo de Internet, es el encargado de dirigir y encaminar los paquetes en la red.

Router: Es un dispositivo que administra el tráfico de datos que circula en una red de computadoras.

Vlan: Es una subred IP separada de manera lógica. Las VLAN permiten que redes de IP y subredes múltiples existan en la misma red conmutada.

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

ENRUTAMIENTO ESTATICO: El enrutamiento estático es la alternativa a los protocolos de enrutamiento, donde se especifican las redes de destino, por donde enviar la información y la distancia administrativa.

ENRUTAMIENTO DINAMICO: El enrutamiento adaptativo, también llamado enrutamiento dinámico, es un proceso para determinar la ruta óptima que debe seguir un paquete de datos a través de una red para llegar a un destino

específico.

LAN: Son las siglas de Local Área Network, Red de área local. Una LAN es una red que conecta los ordenadores en un área relativamente pequeña y predeterminada como (una habitación, un edificio, o un conjunto de edificios). NIC: (Network Information Center) es la autoridad que delega los nombres de Dominio a quienes los solicitan. El NIC es quien se encarga de registrar los dominios de un país.

OSPF: Es un protocolo de enrutamiento jerárquico de pasarela interior o IGP (Interior Gateway Protocol).

RESUMEN

El desarrollo de este trabajo tiene como finalidad aplicar los conceptos adquiridos en el Diplomado de CCNA en Cisco, donde se realiza el desarrollo del escenario 1 y el escenario 2, cada uno con diferente tipología las cuales se montan en el simulador de Packet Tracer. En el escenario 1 se crea una red que está compuesta por un Router, dos Switch y dos PC y luego se realiza la configuración del enrutamiento entre VLAN, DHCP, Etherchannel y port-security requerida por cada uno de los dispositivos, se verifica por medio de los diferentes comandos que la configuración sea correcta y que la red funcione como es solicitada. En el escenario 2 se crea una red que está compuesta por un Servidor de Internet, tres Router, dos Switch y dos PC y luego se realiza la configuración para que esta red admita conectividad IPv4 e IPv6, también seguridad de cada Switch, se genere routing entre VLAN, que cuente con el protocolo OSPF, el protocolo DHCP, las NAT, las ACL y el protocolo NTP, se verifica por medio de los diferentes comandos que la configuración sea correcta y que la red funcione como es solicitada.

Palabras Clave: CISCO, CCNA, Conmutación, Enrutamiento, Redes, Electrónica.

ABSTRACT

The purpose of the development of this work is to apply the concepts acquired in the CCNA Diploma at Cisco, where the development of scenario 1 and scenario 2 is carried out, each with a different typology, which are assembled in the Packet Tracer simulator. In scenario 1, a network is created that is composed of a Router, two Switches and two PCs and then the configuration of the routing between VLAN, DHCP, Etherchannel and port-security required by each of the devices is carried out, it is verified by means of of the different commands that the configuration is correct and that the network works as requested. In scenario 2, a network is created that is composed of an Internet Server, three Routers, two Switches and two PCs and then the configuration is carried out so that this network supports IPv4 and IPv6 connectivity, also security of each Switch, routing is generated between VLANs, which has the OSPF protocol, the DHCP protocol, the NATs, the ACLs and the NTP protocol, it is verified through the different commands that the configuration is correct and that the network works as requested.

Keywords: CISCO, CCNA, Switching, Routing, Networks, Electronics.

INTRODUCCIÓN

Esta prueba de habilidades hace parte del diplomado de profundización CCNA y se realiza con el fin de colocar en práctica el aprendizaje de las competencias y habilidades incluyendo los niveles de comprensión y la capacidad de resolver los diferentes problemas que se pueden presentar en las Networking, esto se realiza por medio de simulaciones donde se plantean diferentes escenarios LAN y WAN para poder analizar el comportamiento de protocolos y se evalúa el funcionamiento de routers y switches por medio de comandos específicos.

La implementación de los dos escenarios se desarrollan en el simulador de Packet Tracer el cual permite la implementación de cada Networking, la configuración sugerida en cada escenario y la verificación correspondiente para conocer la funcionalidad de cada Red y además permite hacer las modificaciones por si se presentan errores. El conocimiento adquirido se puede aplicar en las áreas de telecomunicaciones donde se emplea variedad de redes que se implementan y configuran para suplir necesidades que se presentan en el diario vivir, ya que la tecnología se ha dispersado por el mundo, siendo fundamental para la comunicación y manejo de información.

OBJETIVOS

Objetivo general

Conceptualizar y aplicar la temática de: conectividad IPv4, seguridad de Switch enrutamiento inter VLAN, OSPFv2, DHCP, NAT dinámica / estática y listas de control de acceso (ACL) mediante un caso práctico propuesto por el tutor del diplomado.

Objetivos específicos

- Crear la topología física y lógica de la red del escenario a desarrollarse.
- Configurar la topología, direccionamiento IP, protocolos de enrutamiento especificada en el escenario objeto de la prueba.
- Simular cada uno de los pasos propuestos en la evaluación evidenciando el paso a paso del desarrollo de la solución.

DESARROLLO DE LOS ESCENARIOS

1. ESCENARIO 1

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

Figura 1. Topología Escenario 1.

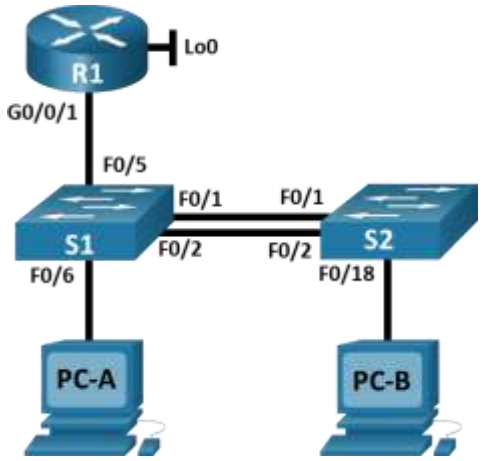
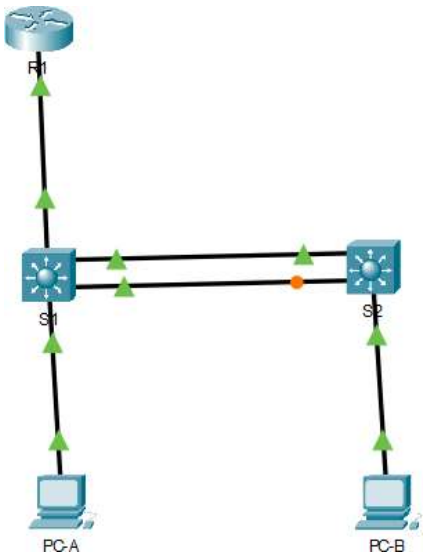


Figura 2. Simulación Escenario 1.



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

1.1 Paso 1: Inicializar y volver a cargar el Router y los switches

- ✓ Se procede a borrar las configuraciones de inicio del Router y se vuelve a cargar con el siguiente código de comandos:

  Router>enable ***(Ingresa a modo privilegiado)***
  Router# erase startup-config ***(Inicia el Router)***
  Erasing the nvram filesystem will remove all configuration files!
  Continue? [Confirm]
  [OK]
  Erase of nvram: complete
  %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
  Router# Reload ***(Vuelve a cargar el Router)***

- ✓ Se borra la configuración de inicio de los dos switches y se vuelven a cargar, luego se configura la plantilla SDM para que admita IPv6 y se vuelve a cargar los switches, esta configuración se realiza para los dos

switches con el siguiente código de comandos:

Switch>enable ***(Ingresa a modo privilegiado)***
Switch# erase startup-config ***(Inicia el Switch)***
Erasing the nvram filesystem will remove all configuration files!
Continue? [Confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Switch# Reload ***(Vuelve a cargar el Switch)***
Switch# config t ***(Ingresa a modo de configuración)***
Switch (config) # sdm prefer dual-ipv4-and-ipv6 default ***(Se configura la plantilla sdm)***
Switch (config) # exit
Switch# Reload

1.2 Paso 2: Procedimiento para la configuración R1

Se inicia la configuración del R1, después de haberlo inicializado y cargado nuevamente, se inicia desactivando la búsqueda DNS, luego se le asigna el nombre (R1), se le asigna el nombre del dominio (ccna-lab.com), se procede a asignarle la contraseña cifrada para el modo EXEC privilegiado (Ciscoenpass) y luego se le coloca la contraseña de acceso a la consola (Ciscoconpass), se le establece la longitud mínima para las contraseñas de 10 caracteres. Se crea un usuario administrativo en la base de datos local y luego se configura el inicio de sesión en las líneas VTY para que use la base de datos local esta vty se configura para que solo acepte SSH, se cifran las contraseñas de texto no cifrado, se configura un MOTD Banner y por último se habilita el routing ipv6.

Nota: Los comandos correspondientes para cada una de las configuraciones asignadas al R1 se muestran específicamente en la siguiente tabla.

Tabla 1. Tareas de configuración para R1

Tarea	Especificación
Desactivar la búsqueda DNS	Se ingresa a modo privilegiado, luego se ingresa a modo de configuración y en seguida se coloca el

	comando para desactivar la búsqueda DNS asi: Router>Enable Router# config t Router(config)#no ip domain-lookup
Nombre del Router	En modo de configuración se coloca el comando para asignarle el nombre al Router asi: Router(config)#hostname R1
Nombre de dominio	En modo de configuración se coloca el comando para asignarle el nombre de dominio asi: Router(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	En modo de configuración se coloca el comando para asignar la contraseña para el modo EXEC privilegiado R1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	En modo de configuración se coloca el comando para asignar la contraseña de acceso a la consola asi: R1(config)#line console 0 R1(config-line)#password ciscoconpass R1(config-line)#login R1(config-line)#exit
Establecer la longitud mínima para las contraseñas	En modo de configuración se coloca el comando para que se establezca la longitud mínima para las contraseñas de 10 caracteres R1(config)# security passwords min-length
Crear un usuario administrativo en la base de datos local	En modo de configuración se coloca el comando para crear un usuario administrativo en la base de datos local con el Nombre: **admin** y la contraseña: **admin1pass** asi: R1(config)#username admin secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	En modo de configuración se coloca el comando para configurar el inicio de sesión en las líneas VTY asi: R1(config)#line vty 0 15 R1(config-line)#login local
Configurar VTY solo aceptando SSH	En modo de configuración se coloca el comando para configurar VTY solo para que acepte SSH asi: R1(config-line)#transport input ssh R1(config-line)#exit

Cifrar las contraseñas de texto no cifrado	En modo de configuración se coloca el comando para cifrar las contraseñas de texto no cifradas asi: R1(config)#service password-encryption
Configure un MOTD Banner	En modo de configuración se coloca el comando para configurar un MOTD Banner con el fin de prohibir el acceso no autorizado asi: R1(config)#banner motd "Unauthorized access is prohibited and violators will be prosecuted to the full extent of the law"
Habilitar el routing IPv6	En modo de configuración se coloca el comando para habilitar el routing Ipv6 asi: R1(config)#ipv6 unicast-routing
Configurar interfaz G0/0/1 y subinterfaces	En modo de configuración se coloca los comandos para configurar la interfaz G0/0/1 y las subinterfaces asi: R1(config)#interface gigabitEthernet 0/0/1.2**(se configura la subinterfaz)** R1(config-subif)#encapsulation dot1q 2 R1(config-subif)#description Bikes **(Se establece la descripción)** R1(config-subif)#ip address 10.19.8.1 255.255.255.192 **(Se establece la dirección Ipv4)** R1(config-subif)#ipv6 address 2001:db8:acad:a::1/64**(Se establece la dirección IPv6.)** R1(config-subif)#ipv6 address FE80::1 link-local **(Se establece la dirección local de enlace IPv6)** R1(config-subif)#interface gigabitEthernet 0/0/1.3**(se configura la subinterfaz)** R1(config-subif)#description Trikes**(Se establece la descripción)** R1(config-subif)#encapsulation dot1q 3 R1(config-subif)#description Trikes**(Se establece la descripción)** 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)#interface gigabitEthernet 0/0/1.4**(se configura la subinterfaz)** R1(config-subif)#encapsulation dot1q 4 R1(config-subif)#description Management**(Se establece la descripción)** 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)#interface gigabitEthernet 0/0/1.6**(se configura la subinterfaz)** R1(config-subif)#encapsulation dot1q 6 Native R1(config-subif)#description Native R1(config-subif)#interface gigabitEthernet 0/0/1**(Interfaz g0/0/1)** R1(config-if)#no shutdown
Configure el Loopback0 interface	En modo de configuración de interfaz se coloca los comandos para configurar el Loopback0 asi: R1(config-if)#interface loopback 0 **(Se inicia configuración de Loopback0)** R1(config-if)#ip address 209.165.201.1 255.255.255.224 **(Se establece la dirección Ipv4)** R1 (config-if)#ipv6 address 2001:db8:acad:209::1/64**(Se establece la dirección IPv6.)** R1(config-if)#ipv6 address FE80::1 link-local **(Se establece la dirección local de enlace IPv6)** R1(config-if)#description loopback**(Se establece la descripción)** R1(config-if)#exit
Generar una clave de cifrado RSA	En modo de configuración se coloca el comando para generar una clave de cifrado RSA asi: R1(config)#crypto key generate rsa How many bits in the modulus [512]: 1024 R1(config)#exit

1.3 Paso 3: Se realiza la configuración al S1

Se inicia la configuración del S1, después de haberlo inicializado y cargado nuevamente, se procede a desactivar la búsqueda DNS, luego se le asigna el

nombre al switch(S1), se le asigna el nombre del dominio (ccna-lab.com), se procede a asignarle la contraseña cifrada para el modo EXEC privilegiado (Ciscoenpass) y luego se le coloca la contraseña de acceso a la consola (Ciscoconpass). Se crea un usuario administrativo en la base de datos local y luego se configura el inicio de sesión en las líneas VTY para que use la base de datos local, esta vty se configura para que solo acepte SSH, se cifran las contraseñas de texto no cifrado, se configura un MOTD Banner y se genera la clave de cifrado RSA, se configura la interfaz de administración SVI y por último se realiza la configuración del Gateway predeterminado.

Nota: Los comandos correspondientes para cada una de las configuraciones asignadas al S1 se muestran específicamente en la siguiente tabla.

Tabla 2: Configuración de S1.

Tarea	Especificación
Desactivar la búsqueda DNS.	Se ingresa a modo privilegiado, luego se ingresa a modo de configuración y en seguida se coloca el comando para desactivar la búsqueda DNS asi: Switch>Enable Switch# config t Switch (config)#no ip domain-lookup
Nombre del Switch	En modo de configuración se coloca el comando para asignarle el nombre al Switch asi: Switch(config)#hostname S1
Nombre de dominio	En modo de configuración se coloca el comando para asignarle el nombre de dominio asi: S1(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	En modo de configuración se coloca el comando para asignar la contraseña para el modo EXEC privilegiado S1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	En modo de configuración se coloca el comando para asignar la contraseña de acceso a la consola asi: S1(config)#line console 0 S1(config-line)#password ciscoconpass S1(config-line)#login S1(config-line)#exit

Crear un usuario administrativo en la base de datos local	En modo de configuración se coloca el comando para crear un usuario administrativo en la base de datos local con el Nombre: admin y la contraseña: admin1pass asi: S1(config)#username admin secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	En modo de configuración se coloca el comando para configurar el inicio de sesión en las líneas VTY asi: S1(config)#line vty 0 15 S1(config-line)#login local
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	En modo de configuración se coloca el comando para configurar VTY solo para que acepte SSH asi: S1(config-line)#transport input ssh S1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	En modo de configuración se coloca el comando para cifrar las contraseñas de texto no cifradas asi: S1(config)#service password-encryption
Configurar un MOTD Banner	En modo de configuración se coloca el comando para configurar un MOTD Banner con el fin de prohibir el acceso no autorizado asi: S1(config)#banner motd "Unauthorized access is prohibited and violators will be prosecuted to the full extent of the law"
Generar una clave de cifrado RSA	En modo de configuración se coloca el comando para generar una clave de cifrado RSA asi: S1(config)#crypto key generate rsa How many bits in the modulus [512]: 1024
Configurar la interfaz de administración (SVI)	En modo de configuración se coloca el comando para configurar la interfaz de administración (SVI) asi: S1(config)#interface vlan 4 **(Se utiliza para ingresar a la interfaz)** S1(config-if)#ip address 10.19.8.98 255.255.255.248 **(Se estable la dirección IPv4 de capa 3)** S1(config-if)#ipv6 address 2001:db8:acad:c::98/64 **(Se establece la dirección IPv6 de capa 3)** S1(config-if)#ipv6 address fe80::98 link-local **(Se establece la dirección local de enlace IPv6)**

	S1(config-if)#description Management **Se establece la descripción)** S1(config-if)#no shutdown **(Habilita la interfaz seleccionada)** S1(config-if)#exit
Configuración del gateway predeterminado	En modo de configuración se coloca el comando para la configuración del Gateway predeterminado asi: S1(config)#ip default-gateway 10.19.8.97 exit

1.4 Paso 4: Se realiza la configuración al S2

Se inicia la configuración del S2, después de haberlo inicializado y cargado nuevamente, se procede a desactivar la búsqueda DNS, luego se le asigna el nombre al Switch (S2), se le asigna el nombre del dominio (ccna-lab.com), se procede a asignarle la contraseña cifrada para el modo EXEC privilegiado (Ciscoenpass) y luego se le coloca la contraseña de acceso a la consola (Ciscoconpass). Se crea un usuario administrativo en la base de datos local y luego se configura el inicio de sesión en las líneas VTY para que use la base de datos local, esta vty se configura para que solo acepte SSH, se cifran las contraseñas de texto no cifrado, se configura un MOTD Banner y se genera la clave de cifrado RSA, se configura la interfaz de administración SVI y por último se realiza la configuración del Gateway predeterminado.

Nota: Los comandos correspondientes para cada una de las configuraciones asignadas al S2 se muestran específicamente en la siguiente tabla.

Tabla 3: Configuración de S2.

Tarea	Especificación
Desactivar la búsqueda DNS.	Se ingresa a modo privilegiado, luego se ingresa a modo de configuración y en seguida se coloca el comando para desactivar la búsqueda DNS asi: Switch>Enable Switch# config t Switch (config)#no ip domain-lookup

Nombre del Switch	En modo de configuración se coloca el comando para asignarle el nombre al Switch asi: Switch(config)#hostname S2
Nombre de dominio	En modo de configuración se coloca el comando para asignarle el nombre de dominio asi: S2(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	En modo de configuración se coloca el comando para asignar la contraseña para el modo EXEC privilegiado S2(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	En modo de configuración se coloca el comando para asignar la contraseña de acceso a la consola asi: S2(config)#line console 0 S2(config-line)#password ciscoconpass S2(config-line)#login S2(config-line)#exit
Crear un usuario administrativo en la base de datos local	En modo de configuración se coloca el comando para crear un usuario administrativo en la base de datos local con el Nombre: admin y la contraseña: admin1pass asi: S2(config)#username admin secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	En modo de configuración se coloca el comando para configurar el inicio de sesión en las líneas VTY asi: S2(config)#line vty 0 15 S2(config-line)#login local
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	En modo de configuración se coloca el comando para configurar VTY solo para que acepte SSH asi: S2(config-line)#transport input ssh S2(config-line)#exit
Cifrar las contraseñas de texto no cifrado	En modo de configuración se coloca el comando para cifrar las contraseñas de texto no cifradas asi: S2(config)#service password-encryption
Configurar un MOTD Banner	En modo de configuración se coloca el comando para configurar un MOTD Banner con el fin de prohibir el acceso no autorizado asi:

	S2(config)#banner motd "Unauthorized access is prohibited and violators will be prosecuted to the full extent of the law"
Generar una clave de cifrado RSA	En modo de configuración se coloca el comando para generar una clave de cifrado RSA asi: S2(config)#crypto key generate rsa How many bits in the modulus [512]: 1024
Configurar la interfaz de administración (SVI)	En modo de configuración se coloca el comando para configurar la interfaz de administración (SVI) asi: S2(config)#interface vlan 4 **(Se utiliza para ingresar a la interfaz)** S2(config-if)#ip address 10.19.8.99 255.255.255.248 **(Se estable la dirección IPv4 de capa 3)** S2(config-if)#ipv6 address 2001:db8:acad:c::99/64 **(Se establece la dirección IPv6 de capa 3)** S2(config-if)#ipv6 address fe80::99 link-local **(Se establece la dirección local de enlace IPv6)** S2(config-if)#description Management **Se establece la descripción)** S2(config-if)#no shutdown **(Habilita la interfaz seleccionada)** S2(config-if)#exit
Configuración del gateway predeterminado	En modo de configuración se coloca el comando para la configuración del Gateway predeterminado asi: S2(config)#ip default-gateway 10.19.8.97 exit

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

2.1 Paso 1: Se realiza la configuración al S1

Se inicia creando la Vlan Bikes, la Vlan Trikes, la Vlan Management, la Vlan Parking y la Vlan Native, luego se crea troncos 802.1Q que utilicen la VLAN 6 nativa, se crea un grupo de puertos EtherChannel de Capa 2 que usa interfaces F0/1 y F0/2, también se configura el puerto de acceso de host para VLAN 2 y por último se configura la seguridad del puerto en los puertos de acceso.

Nota: Los comandos correspondientes para cada una de las configuraciones asignadas al S1 se muestran específicamente en la siguiente tabla.

Tabla 4: Configuración de S1.

Tarea	Especificación
Crear VLAN	En modo de configuración se coloca el comando para crear las Vlan asi: S1#config t S1(config)#vlan 2 **(Se menciona la vlan)** S1(config-vlan)#name Bikes **(Se le coloca nombre a la vlan)** S1(config-vlan)#exit S1(config)#vlan 3**(Se menciona la vlan)** S1(config-vlan)#name Trikes **(Se le coloca nombre a la vlan)** S1(config-vlan)#exit S1(config)#vlan 4**(Se menciona la vlan)** S1(config-vlan)#name Management **(Se le coloca nombre a la vlan)** S1(config-vlan)#exit S1(config)#vlan 5 **(Se menciona la vlan)** S1(config-vlan)#name Parking **(Se le coloca nombre a la vlan)** S1(config-vlan)#exit S1(config)#vlan 6 **(Se menciona la vlan)** S1(config-vlan)#name Native **(Se le coloca nombre a la vlan)** S1(config-vlan)#exit

Crear troncos 802.1Q que utilicen la VLAN 6 nativa	En modo de configuración se coloca el comando para troncos 802.1Q que utilicen la Vlan nativa asi: S1#config t S1(config)#interface fastEthernet 0/5**(Se llama la int f0/5)** S1(config-if)#switchport trunk encapsulation dot1q **(Se configura en modo troncal)** S1(config-if)#switchport mode trunk**(Modo troncal)** S1(config-if)#switchport trunk native vlan 6 **(Se crea troncos a lo que utilice la vlan 6)** S1(config-if)#shutdown **(Inhabilita la interfaz)** S1(config-if)#exit S1(config)#interface range fastEthernet 0/1-2 **(Se configuran las int f0/1-2 ya que tienen los mismo parametros)** S1(config-if-range)#switchport trunk encapsulation dot1q **(Se configura en modo troncal)** S1(config-if)#switchport mode trunk **(Modo troncal)** S1(config-if)#switchport trunk native vlan 6 **(Se crea troncos a lo que utilice la vlan 6)** S1(config-if)#shutdown **(Inhabilita la interfaz)**
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	En modo configuración se usa el protocolo LACP para la negociación con el siguiente comando: S1#Config t S1(config)#interface range fastEthernet 0/1-2 **(Se configura las dos interfaces ya que tienen los mismos parámetros)**

	S1(config-if-range)#channel-group 1 mode active **(Se especifca que la interfaz debe usar el LACP)** S1(config-if-range)#exit S1(config)#interface port-channel 1 S1(config-if)#switchport trunk encapsulation dot1q **(Se configura en modo troncal)** S1(config-if)#switchport mode trunk**(Modo troncal)** S1(config-if)#switchport trunk native vlan 6 S1(config-if)#exit S1(config)#
Configurar el puerto de acceso de host para VLAN 2	En modo de configuración iniciamos llamamos la int f0/6 para configurar el puerto de acceso de host para Vlan 2 se utiliza el siguiente comando: S1#Config t S1(config)#nterface F0/6 **(se configura la int f0/6)** S1(config-if)#interface fastEthernet 0/6 S1(config-if)#switchport mode access**(Modo de acceso)** S1(config-if)#switchport access vlan 2**(Modo de acceso permanente a la vlan 2)** S1(config-if)#switchport port-security**(Habilita la seguridad de los puertos)**
Configurar la seguridad del puerto en los puertos de acceso	En modo de configuración de la interfaz se configura para que solo permitir 3 direcciones MAC con el siguiente comando: S1(config-if)#switchport port-security maximum 3

Proteja todas las interfaces no utilizadas	Acá se asigna a VLAN 5, se establece en modo de acceso, se agrega una descripción y se apagar para esto se utiliza el siguiente comando: S1#Config t S1(config)#interface range fastethernet 0/3-4 **(Se configura las dos interfaces ya que tienen los mismos parámetros)** S1 (config-if-range)#switchport mode access **(Modo de acceso)** S1 (config-if-range)#switchport access vlan 5 **(Modo de acceso permanente a la vlan 5)** S1 (config-if-range)#description fuera de servicio **(Se le coloca la descripcion)** S1 (config-if-range)#interface range fastethernet 0/7-24 **(Se configura las dos interfaces ya que tienen los mismos parámetros)** S1 (config-if-range)#switchport mode access**(Modo de acceso)** S1 (config-if-range)#switchport access vlan 5 **(Modo de acceso permanente a la vlan 5)** S1 (config-if-range)#description fuera de servicio **(Se le coloca la descripcion)** S1 (config-if-range)#shutdown **(Se apagan)** S1 (config-if-range)#exit S1(config)#interface range gigabitethernet 0/1-2 **(Se configura las dos interfaces ya que tienen los mismos parámetros)** S1 (config-if-range)#switchport mode access **(Modo de acceso)** S1 (config-if-range)#switchport access vlan 5 **(Modo de acceso permanente a la vlan 5)**

	S1 (config-if-range)#description fuera de servicio **(Se le coloca la descripcion)** S1 (config-if-range)#shutdown **(Se apagan)** S1 (config-if-range)#exit

2.2 Paso 2: Se realiza la configuración al S2

Se inicia creando la Vlan Bikes, la Vlan Trikes, la Vlan Management, la Vlan Parking y la Vlan Native, luego se crea troncos 802.1Q que utilicen la VLAN 6 nativa, se crea un grupo de puertos EtherChannel de Capa 2 que usa interfaces F0/1 y F0/2, también se configura el puerto de acceso de host para VLAN 2 y por último se configura la seguridad del puerto en los puertos de acceso.

Nota: Los comandos correspondientes para cada una de las configuraciones asignadas al S2 se muestran específicamente en la siguiente tabla.

Tabla 5: Configuración de S2.

Tarea	Especificación
Crear VLAN	En modo de configuración se coloca el comando para crear las Vlan asi: S2#config t S2(config)#vlan 2 **(Se menciona la vlan)** S2(config-vlan)#name Bikes **(Se le coloca nombre a la vlan)** S2(config-vlan)#exit S2(config)#vlan 3**(Se menciona la vlan)** S2(config-vlan)#name Trikes **(Se le coloca nombre a la vlan)**

	S2(config-vlan)#exit S2(config)#vlan 4**(Se menciona la vlan)** S2(config-vlan)#name Management **(Se le coloca nombre a la vlan)** S2(config-vlan)#exit S2(config)#vlan 5 **(Se menciona la vlan)** S2(config-vlan)#name Parking **(Se le coloca nombre a la vlan)** S2(config-vlan)#exit S2(config)#vlan 6 **(Se menciona la vlan)** S2(config-vlan)#name Native **(Se le coloca nombre a la vlan)** S2(config-vlan)#exit
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	En modo de configuración se coloca el comando para troncos 802.1Q que utilicen la Vlan nativa asi: S2#config t S2(config)#interface range fastEthernet 0/1-2 **(Se configuran las int f0/1-2 ya que tienen los mismo parametros)** S2(config-if-range)#switchport trunk encapsulation dot1q **(Se configura en modo troncal)** S2(config-if)#switchport mode trunk **(Modo troncal)** S2(config-if)#switchport trunk native vlan 6 **(Se crea troncos a lo que utilice la vlan 6)** S2(config-if)#shutdown **(Inhabilita la interfaz)**
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	En modo configuración se usa el protocolo LACP para la negociación con el siguiente comando: S2#Config t S2(config)#interface range fastEthernet 0/1-2 **(Se configura las dos interfaces ya que tienen los mismos parámetros)** S2(config-if-range)#channel-group 1 mode active **(Se especifca que la interfaz debe usar el LACP)** S2(config-if-range)#exit

	S2(config)#interface port-channel 1 S2(config-if)#switchport trunk encapsulation dot1q **(Se configura en modo troncal)** S2(config-if)#switchport mode trunk**(Modo troncal)** S2(config-if)#switchport trunk native vlan 6 S2(config-if)#exit S2(config)#exit
Configurar el puerto de acceso del host para la VLAN 3	En modo de configuración iniciamos llamamos la int f0/18 para configurar el puerto de acceso de host para Vlan 3 se utiliza el siguiente comando: S2#Config t S2(config)#nterface F0/18**(se configura la int f0/18)** S2(config-if)#interface fastEthernet 0/18 S2(config-if)#switchport mode access**(Modo de acceso)** S2(config-if)#switchport access vlan 3**(Modo de acceso permanente a la vlan 3)** S2(config-if)#switchport port-security**(Habilita la seguridad de los puertos)**
Configure port-security en los access ports	En modo de configuración de la interfaz se configura para que solo permitir 3 direcciones MAC con el siguiente comando: S2(config-if)# switchport port-security maximum 3
Asegure todas las interfaces no utilizadas.	Acá se asigna a VLAN 5, se establece en modo de acceso, se agrega una descripción y se apagar para esto se utiliza el siguiente comando: S2#Config t S2(config)#interface range fastethernet 0/3-17 **(Se configura las dos interfaces ya que tienen los mismos parámetros)** S2 (config-if-range)#switchport mode access **(Modo de acceso)**

	S2 (config-if-range)#switchport access vlan 5 **(Modo de acceso permanente a la vlan 5)** S2 (config-if-range)#description fuera de servicio **(Se le coloca la descripcion)** S2 (config-if-range)#shutdown **(Se apagan)** S2 (config-if-range)#interface range fastethernet 0/19-24 **(Se configura las dos interfaces ya que tienen los mismos parámetros)** S2 (config-if-range)#switchport mode access**(Modo de acceso)** S2 (config-if-range)#switchport access vlan 5 **(Modo de acceso permanente a la vlan 5)** S2 (config-if-range)#description fuera de servicio **(Se le coloca la descripcion)** S2 (config-if-range)#shutdown **(Se apagan)** S2 (config-if-range)#exit S2(config)#interface range gigabitethernet 0/1-2 **(Se configura las dos interfaces ya que tienen los mismos parámetros)** S2 (config-if-range)#switchport mode access **(Modo de acceso)** S2 (config-if-range)#switchport access vlan 5 **(Modo de acceso permanente a la vlan 5)** S2 (config-if-range)#description fuera de servicio **(Se le coloca la descripcion)** S2 (config-if-range)#shutdown **(Se apagan)** S2 (config-if-range)#exit

3. Parte 3: Configuración soporte de host

3.1 Paso 1: Configuración de R1

Se inicia configurando el Default routing donde se crean las rutas ipv4 e ipv6, luego se configura IPv4 DHCP para VLAN 2 y también para VLAN 3

Nota: Los comandos correspondientes para cada una de las configuraciones asignadas al R1 se muestran específicamente en la siguiente tabla.

Tabla 6: Configuración de R1.

Tarea	Especificación
Configure Default Routing	Se ingresa a modo configuración y se crea las rutas predeterminadas para IPv4 e IPv6 que dirijan el tráfico a la interfaz Loopback 0 asi: R1#Config t **(modo configuración)** R1(config)#ip route 0.0.0.0 0.0.0.0 loopback 0**(Ruta ipv4)** R1(config)#ipv6 route ::/0 loopback 0 **(Ruta Ipv6)** R1(config)#exit
Configurar IPv4 DHCP para VLAN 2	En modo de configuración se crea un grupo DHCP para VLAN 2. Se le asigna el nombre del dominio ccna-a.net y se especifica la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada con los siguientes comandos asi: R1#config t **(modo de configuración)** R1(config)#ip dhcp excluded-address 10.19.8.1 10.19.8.53**(Se exculuye el acceso al rango de direcciones)** R1(dhcp-config)#ip dhcp pool vlan2-Bikes **(Se inicia la configuración de la vlan 2)** R1(dhcp-config)#network 10.19.8.0 255.255.255.192 R1(dhcp-config)#default-router 10.19.8.1**(Se define el gateway)** R1(dhcp-config)#domain-name ccna-a.net **(Se le asigna el nombre del domino)** R1(dhcp-config)#exit R1(config)#exit

Configurar DHCP IPv4 para VLAN 3	En modo de configuración se crea un grupo DHCP para VLAN 3. Se le asigna el nombre del dominio ccna-b.net y se especifica la dirección de la puerta de enlace predeterminada como dirección de interfaz del Router para la subred involucrada con los siguientes comandos asi: R1#config t **(modo de configuración)** R1(config)#ip dhcp excluded-address 10.19.8.65 10.19.8.84 **(Se exculuye el acceso al rango de direcciones)** R1(dhcp-config)#ip dhcp pool vlan3-Trikes **Se inicia la configuración de la vlan 3)** R1(dhcp-config)#network 10.19.8.64 255.255.255.224 R1(dhcp-config)#default-router 10.19.8.56 **(Se define el gateway)** R1(dhcp-config)#domain-name ccna-a.net **(Se le asigna el nombre del domino)** R1(dhcp-config)#exit R1(config)#exit

3.2 Paso 2: Configuración de los servidores

Se inicia configurando los equipos host PC-A y PC-B para que utilicen DHCP para IPv4 y se procede a asignarle estáticamente las direcciones IPv6 GUA y Link Local. Luego se registran configuraciones de red del host con el comando ipconfig /all.

Nota: La configuración correspondiente para PC-A se encuentra asignada en la siguiente tabla.

Tabla 7: Configuración de PC-A

PC-A Network Configuration	
Descripción	*Se ingresa a la PC-A en la opción Desktop y luego en ip configuration donde se inicia colocando la opción de DHCP para Ipv4 y se observa que el acceso es correcto, y en ipv6 se asigna estáticamente las direcciones y el Link local.* Para registrar los siguientes datos se utiliza el comando ipconfig /all
Dirección física	*0001.C955.B531*
Dirección IP	*2001:db8:acad:a::50* *10.19.8.54*
Máscara de subred	*255.255.255.192*
Gateway predeterminado	*10.19.8.1*
Gateway predeterminado IPv6	*Fe80::1*

Figura 3. Comando ipconfig /all en PC-A.

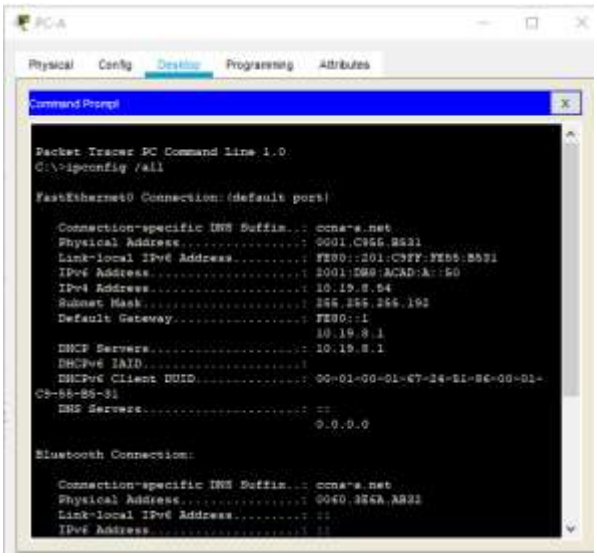
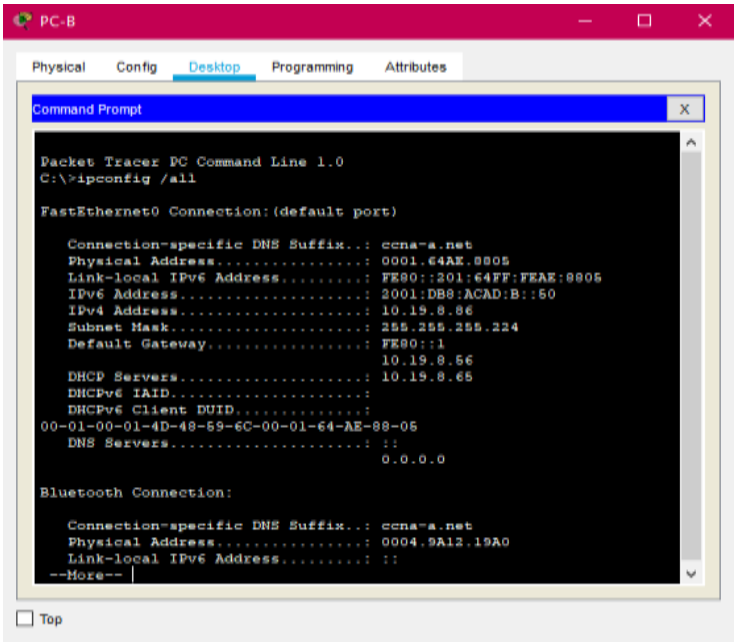


Tabla 8: Configuración de PC-B

Configuración de red de PC-B	
Descripción	*Se ingresa a la PC-A en la opción Desktop y luego en ip configuration donde se inicia colocando la opción de DHCP para Ipv4 y se observa que el acceso es correcto, y en ipv6 se asigna estáticamente las direcciones y el Link local.*
Dirección física	*0001.64AE.8805*
Dirección IP	2001:DB8:ACAD:B::50 *10.19.8.85*
Máscara de subred	*255.255.255.224*
Gateway predeterminado	*10.19.8.65*
Gateway predeterminado IPv6	*Fe80::1*

Figura 4. Comando ipconfig /all en PC-B.



4. Parte 4: Se prueba y verifica la conectividad de extremo a extremo

Se realiza la verificación desde las PC-A y PC-B y se observa que los resultados de los ping son satisfactorios, en la siguiente tabla se muestra desde donde se hace ping a donde con la ip correspondiente y luego se evidencia en cada figura tomada de cada verificación realizada.

Tabla 9: Verificación de conectividad de extremo a extremo

Desde	A	de Internet	Dirección IP	Resultados de ping
PC-A	R1, G0/0/1.2	Dirección	10.19.8.1	***Ok***
		IPv6	2001:db8:acad:a: :1	***Ok***
	R1, G0/0/1.3	Dirección	10.19.8.65	***Ok***
		IPv6	2001:db8:acad:b: :1	***Ok***
	R1, G0/0/1.4	Dirección	10.19.8.97	***Ok***
		IPv6	2001:db8:acad:c: :1	***Ok***
	S1, VLAN 4	Dirección	10.19.8.98	***Ok***
		IPv6	2001:db8:acad:c: :98	***Ok***
	S2, VLAN 4	Dirección	10.19.8.99.	***Ok***
		IPv6	2001:db8:acad:c: :99	***Ok***
	PC-B	Dirección	10.19.8.85	***Ok***
		IPv6	2001:db8:acad:b: :50	***Ok***
	R1 Bucle 0	Dirección	209.165.201.1	***Ok***
		IPv6	2001:db8:acad:209: :1	***Ok***
PC-B	R1 Bucle 0	Dirección	209.165.201.1	***Ok***
		IPv6	2001:db8:acad:209: :1	***Ok***

	R1, G0/0/1.2	Dirección	10.19.8.1	***Ok***
		IPv6	2001:db8:acad:a: :1	***Ok***
	R1, G0/0/1.3	Dirección	10.19.8.65	***Ok***
		IPv6	2001:db8:acad:b: :1	***Ok***
	R1, G0/0/1.4	Dirección	10.19.8.97	***Ok***
		IPv6	2001:db8:acad:c: :1	***Ok***
	S1, VLAN 4	Dirección	10.19.8.98	***Ok***
		IPv6	2001:db8:acad:c: :98	***Ok***
	S2, VLAN 4	Dirección	10.19.8.99.	***Ok***
		IPv6	2001:db8:acad:c: :99	***Ok***

Figura 5. Verificación de conectividad desde PC-A a las direcciones ip **10.19.8.1** e ip **2001:db8:acad:a::1**

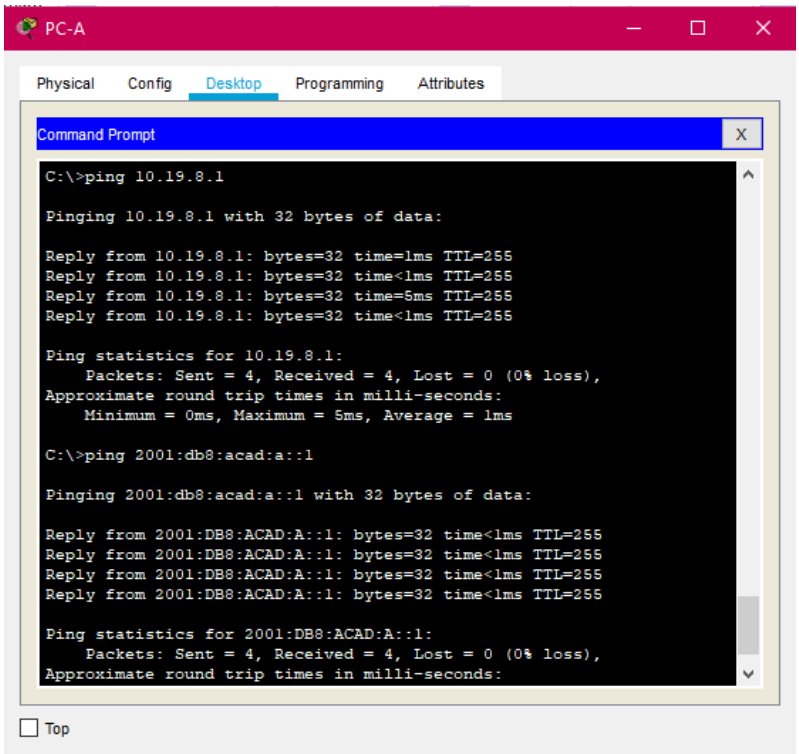


Figura 6. Verificación de conectividad desde la PC-A a la dirección ip **10.19.8.65**

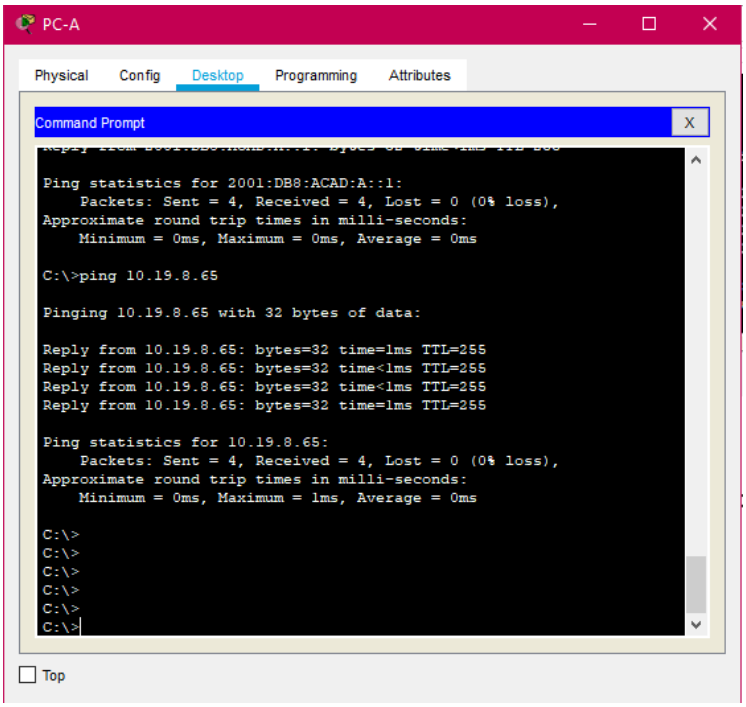


Figura 7. Verificación de conectividad desde la PC-A a la dirección ip **2001:db8:acad:b: :1**

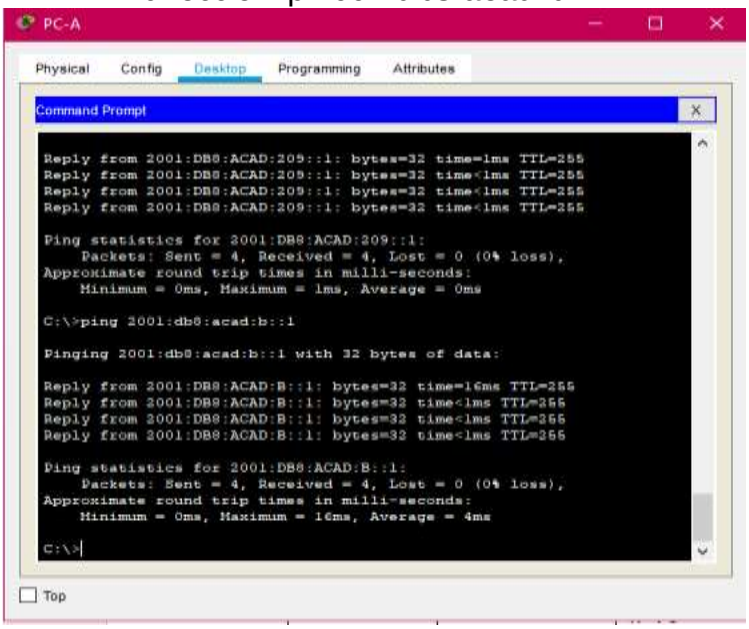


Figura 8. Verificación de conectividad desde la PC-A a la dirección ip **10.19.8.97**

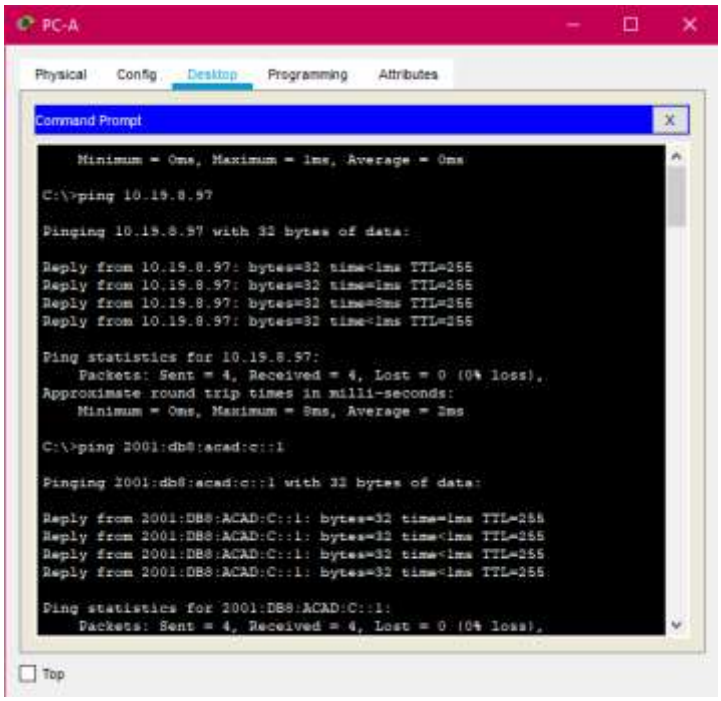


Figura 9. Verificación de conectividad a las direcciones ip **2001:db8:acad:c::1** e ip **10.19.8.98**

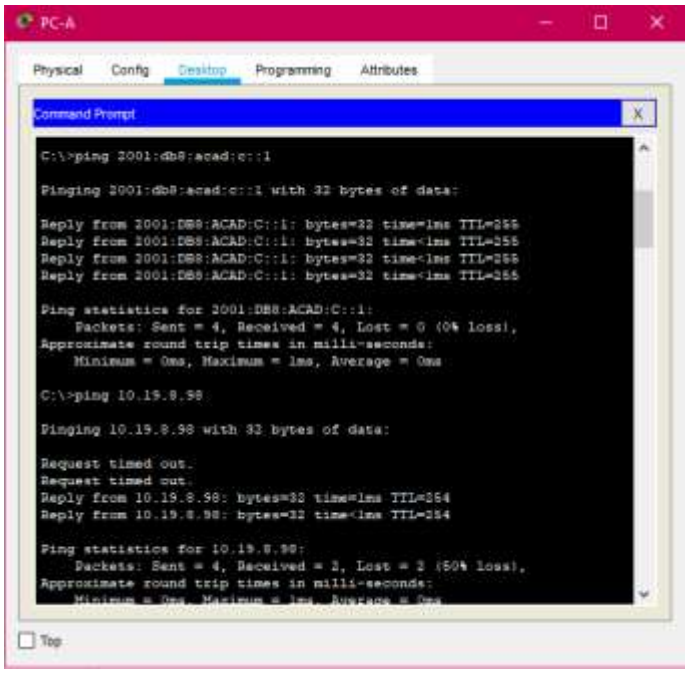


Figura 10. Verificación de conectividad desde la PC-A a la dirección ip **2001:db8:acad:c::98**

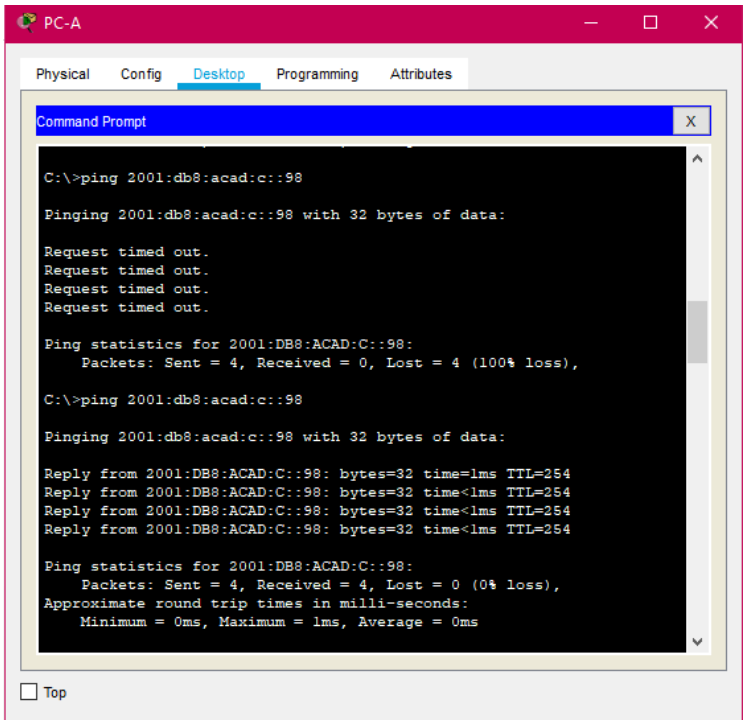


Figura 11. Verificación de conectividad a la dirección ip **10.19.8.99**

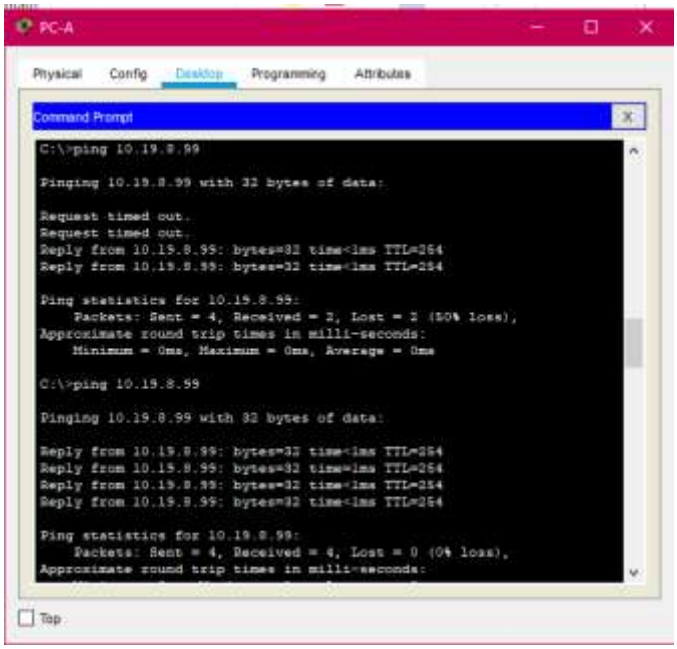


Figura 12. Verificación de conectividad desde PC-A a la dirección ip **2001:db8:acad:c: :99**

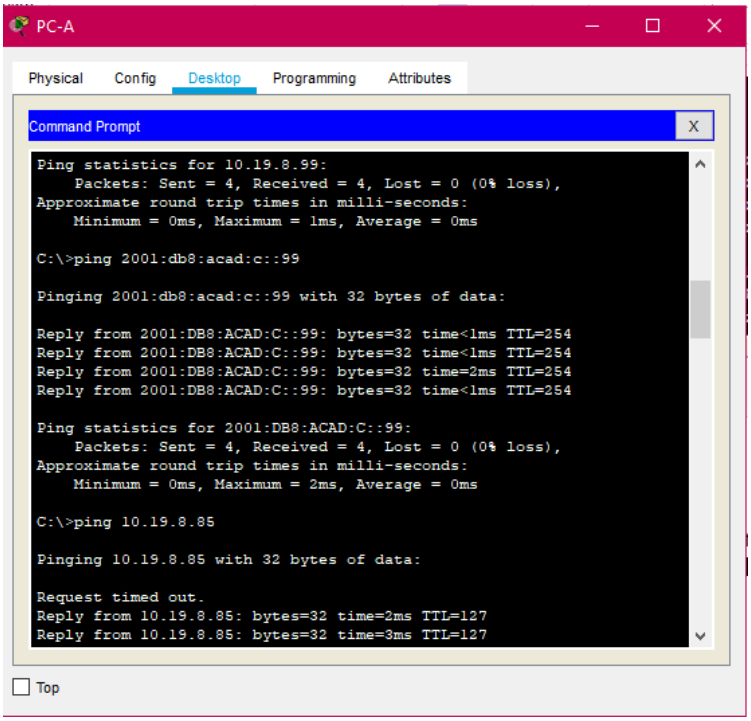


Figura 13. Verificación de conectividad desde la PC-A a las direcciones ip **10.19.8.85** e ip **2001:db8:acad:b: :50**

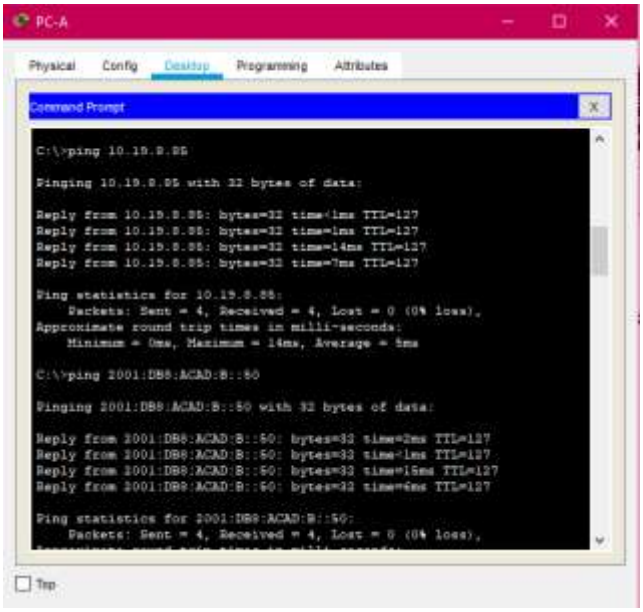


Figura 14. Verificación de conectividad desde la PC-A a las direcciones ip **209.165.201.1** e **ip 2001:db8:acad:209: :1**

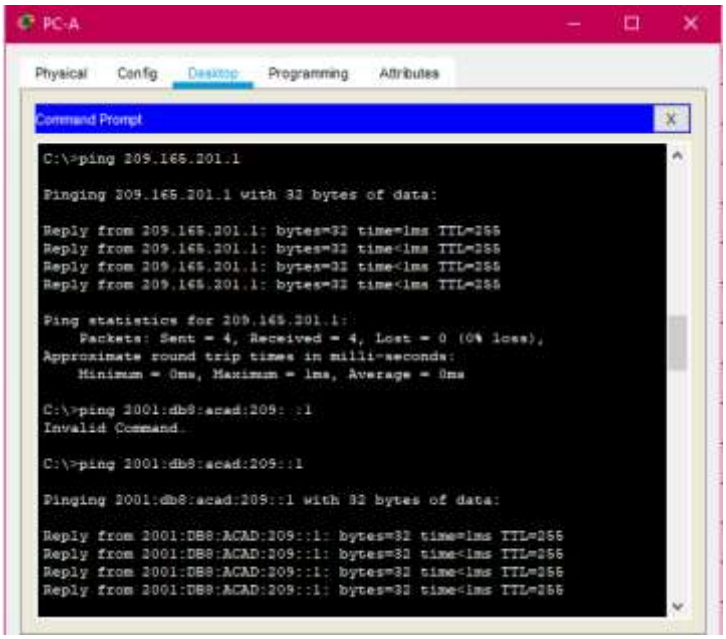


Figura 15. Verificación de conectividad desde PC-B a las direcciones ip **209.165.201.1** e ip **2001:db8:acad:209: :1**

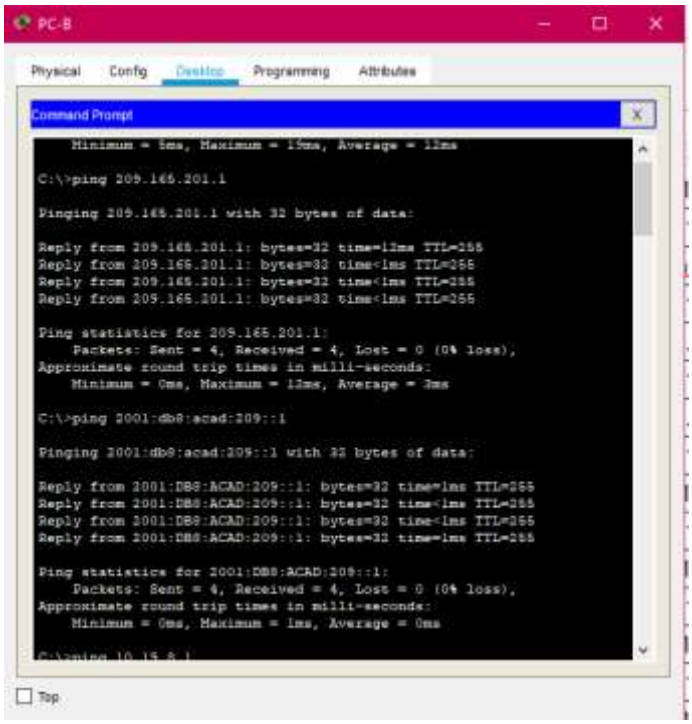


Figura 16. Verificación de conectividad desde PC-B a las direcciones ip **10.19.8.1** e ip **2001:db8:acad:a: :1**

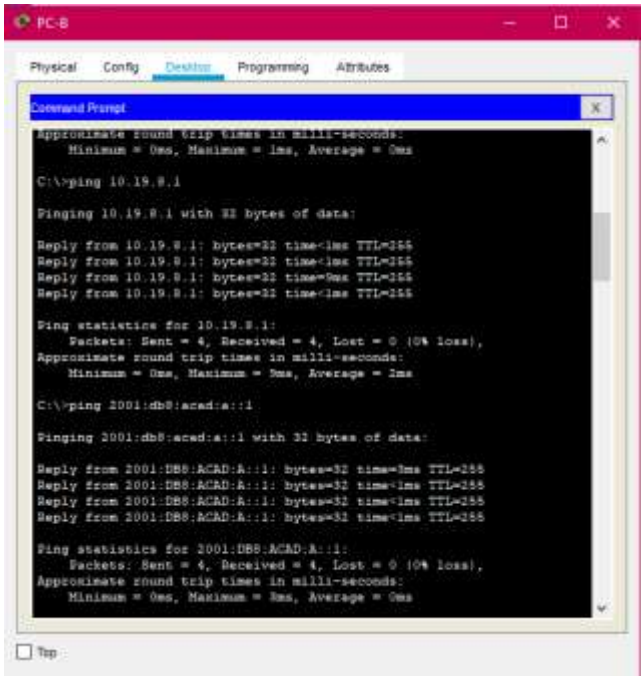


Figura 17. Verificación de conectividad desde PC-B a la dirección ip **10.19.8.65** e ip **2001:db8:acad:b: :1**

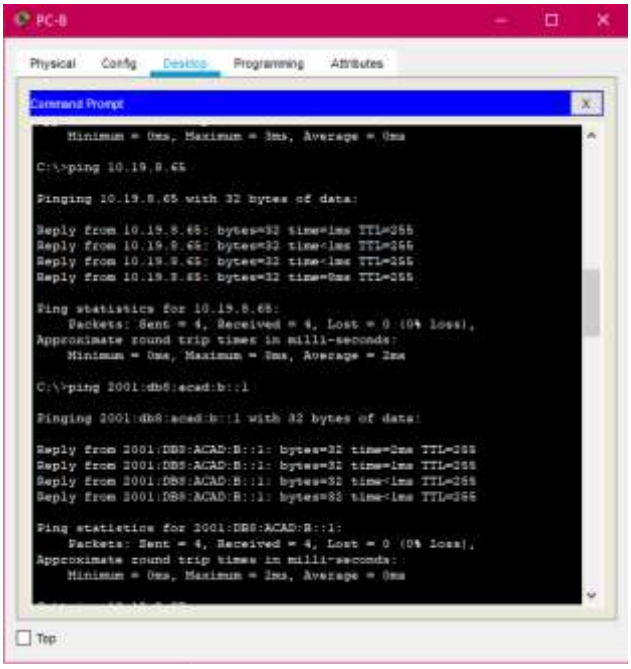


Figura 18. Verificación de conectividad desde PC-B a la dirección ip **10.19.8.97** e ip **2001:db8:acad:c: :1**

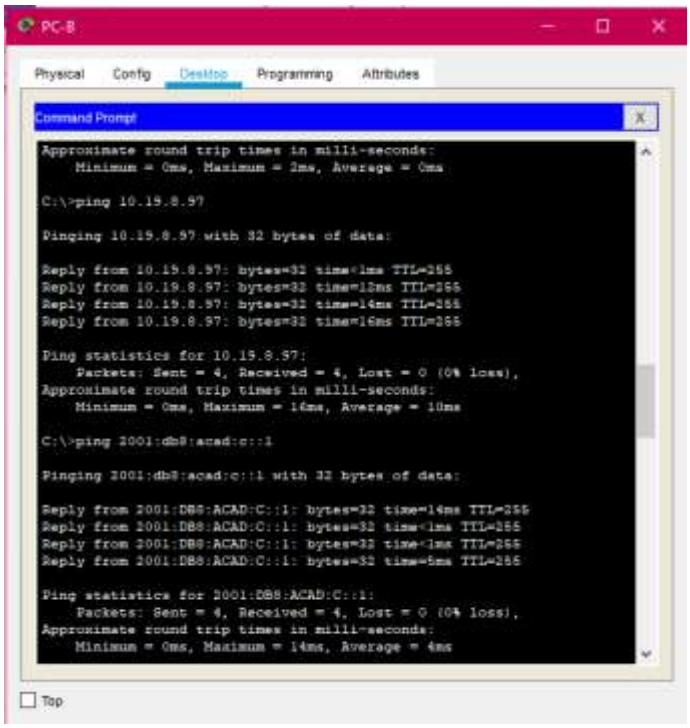


Figura 19. Verificación de conectividad desde PC-B a la dirección ip **10.19.8.98** e ip **2001:db8:acad:c: :98**

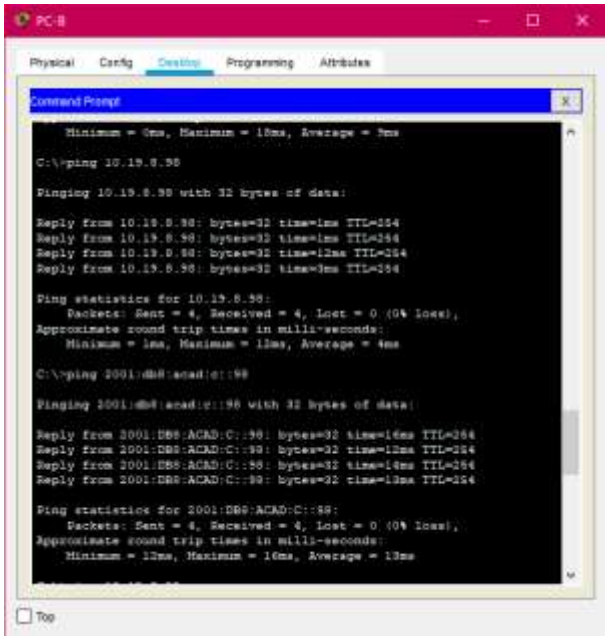
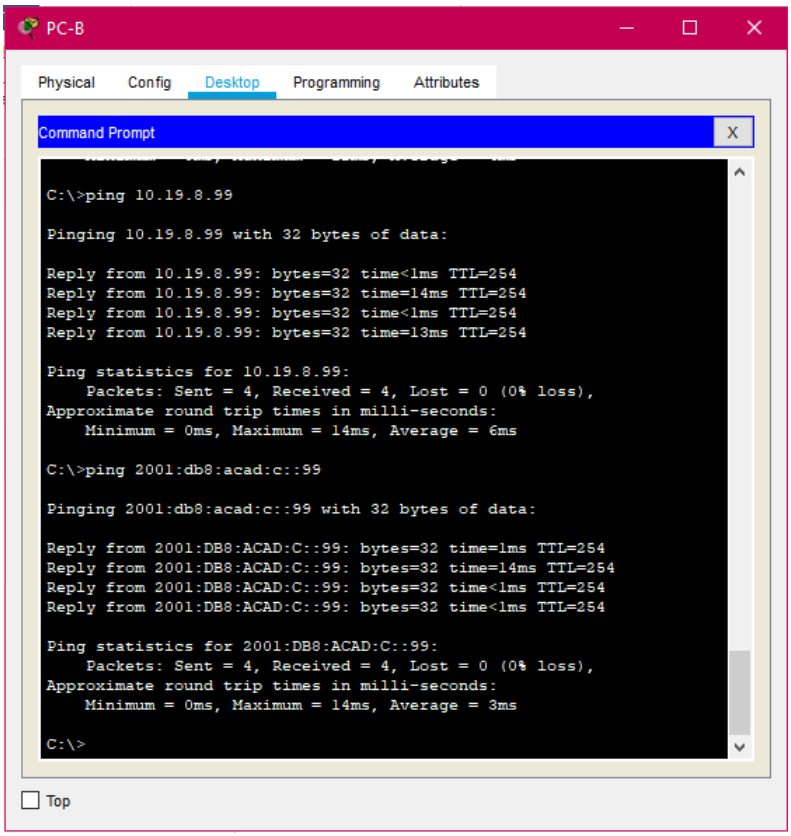


Figura 20. Verificación de conectividad desde la PC-B a la dirección ip **10.19.8.99** e ip **2001:db8:acad:c: :99**



2. ESCENARIO 2

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

Figura 21. Topología escenario 2.

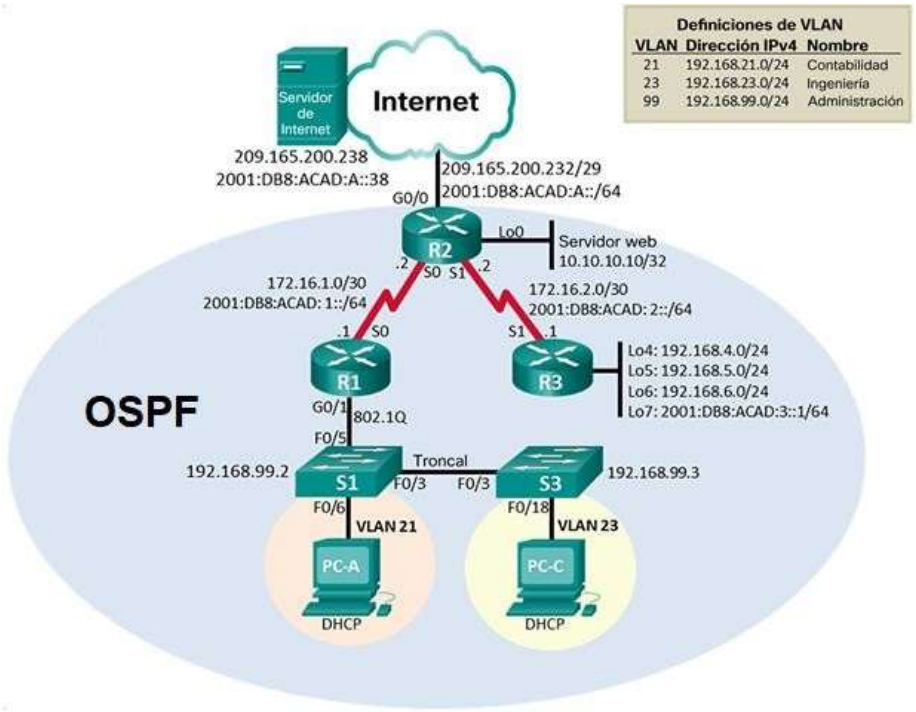
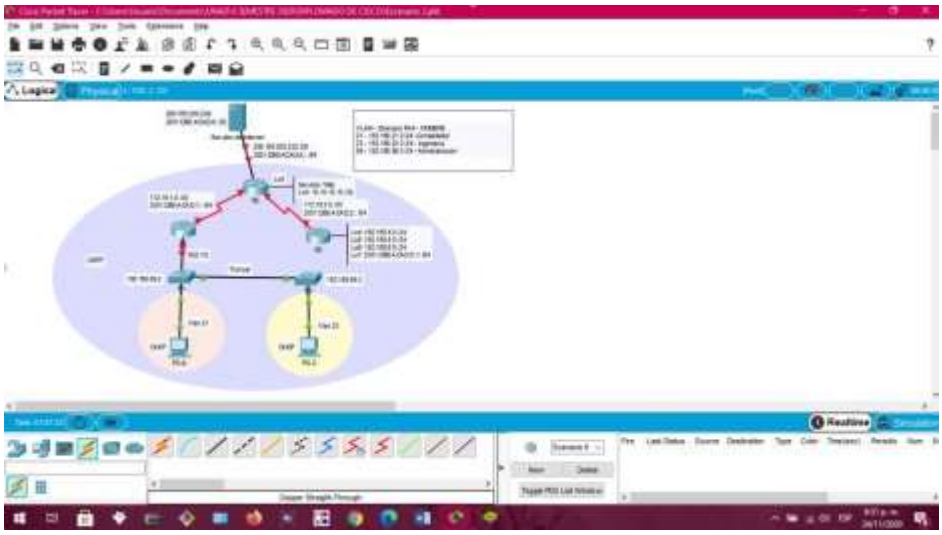


Figura 22. Simulación topología escenario 2.



1. Parte 1: Iniciar dispositivos

1.1 Paso 1: Inicializar y volver a cargar los Routers y los switches

Se elimina las configuraciones de inicio del R1, R2, R3, S1 y S3 y se vuelven a cargar.

Nota: La configuración correspondiente para iniciar y volver a cargar los dispositivos se muestra en la siguiente tabla.

Tabla 10: Configuración para iniciar y volver a cargar los dispositivos.

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	Se procede a borrar las configuraciones de inicio del Router con los siguientes comandos:

	R1 Router>enable ***(Ingresa a modo privilegiado)*** Router#erase startup-config ***(Inicia el Router)*** Erasing the nvram filesystem will remove all configuration files! Continue? [confirm] [OK] Erase of nvram: complete %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram **R2** Router>enable ***(Ingresa a modo privilegiado)*** Router#erase startup-config ***(Inicia el Router)*** Erasing the nvram filesystem will remove all configuration files! Continue? [confirm] [OK] Erase of nvram: complete %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram **R3** Router>enable ***(Ingresa a modo privilegiado)*** Router#erase startup-config ***(Inicia el Router)*** Erasing the nvram filesystem will remove all configuration files! Continue? [confirm] [OK] Erase of nvram: complete %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Volver a cargar todos los routers	Se carga cada Router con el siguiente comando: **R1** Router#Reload ***(Vuelve a cargar el Router)*** **R2** Router#Reload ***(Vuelve a cargar el Router)***

	R3 Router#Reload ***(Vuelve a cargar el Router)***
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Se inicia los dos switch y también se elimina la base de datos de Vlan anterior con los siguientes commandos: **S1** Switch>enable ***(Ingresa a modo privilegiado)*** Switch#erase startup-config ***(Inicia el Switch)*** Erasing the nvram filesystem will remove all configuration files! Continue? [confirm] [OK] Switch#delete vlan.dat **(Se elimina la base de datos vlan)** **S3** Switch>enable ***(Ingresa a modo privilegiado)*** Switch#erase startup-config ***(Inicia el Switch)*** Erasing the nvram filesystem will remove all configuration files! Continue? [confirm] [OK] Switch#delete vlan.dat **(Se elimina la base de datos vlan)**
Volver a cargar ambos switches	Se carga cada Switch con el siguiente comando: **S1** Switch #Reload ***(Vuelve a cargar el* Switch*)*** **S3** Switch #Reload ***(Vuelve a cargar el* Switch*)***
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Se verifica que la base de datos de Vlan no esté en la memoria flash en ambos Switch con el siguiente comando: Switch#Show flash **(Se verifica)**

Figura 23. Verificación con el comando Show flash en S1.

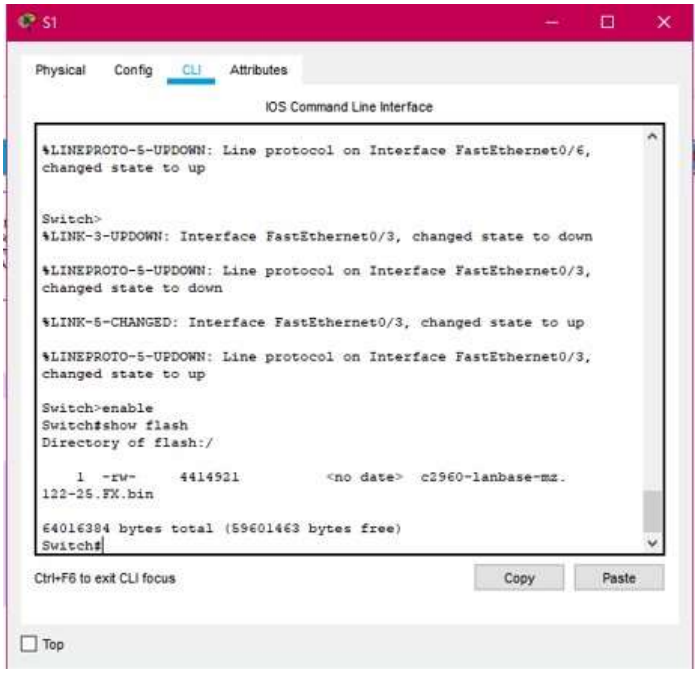
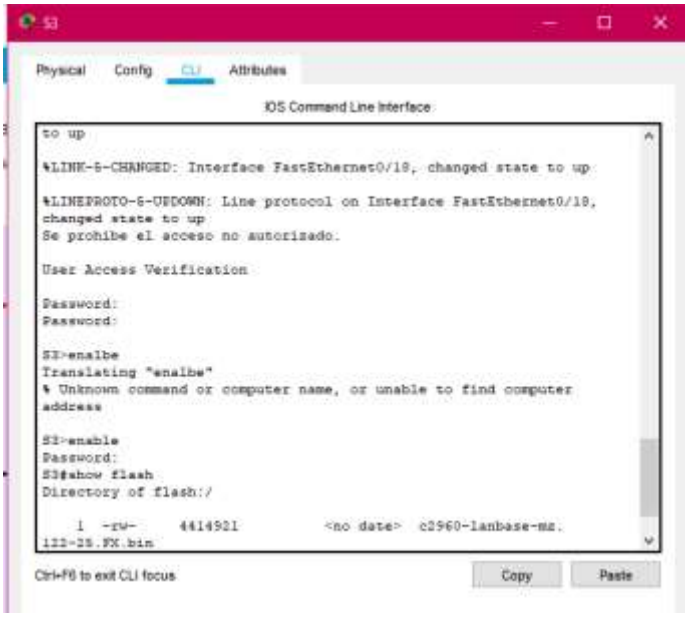


Figura 24. Verificación con el comando Show flash en S2.



2. Parte 2: Configuración los parámetros básicos de los dispositivos

2.1 Paso 1: Configuración de la computadora de internet

En el servidor de internet se va a la opción Desktop y luego a ip configuration y se asigna en static la información que se encuentra en la siguiente tabla.

Tabla 11: Configuración del Servidor de Internet.

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.233
Dirección IPv6/subred	2001:DB8:ACAD:A::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:2::1

2.2 Paso 2: Configuración del Router 1

Se inicia la configuración del R1, después de haberlo inicializado y cargado nuevamente, se inicia desactivando la búsqueda DNS, luego se le asigna el nombre (R1), se procede a asignarle la contraseña cifrada para el modo EXEC privilegiado (class) y luego se le coloca la contraseña de acceso a la consola (cisco), y la contraseña de acceso Telnet, se cifran las contraseñas de texto no cifrado, se configura un MOTD , se configura la int s0/0/0 y por ultimo las rutas predeterminadas.

Nota: Los comandos correspondientes para cada una de las configuraciones asignadas al R1 se muestran específicamente en la siguiente tabla.

Tabla 12: Configuración del R1.

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Se ingresa a modo privilegiado, luego se ingresa a modo de configuración y en seguida se coloca el comando para desactivar la búsqueda DNS asi: Router>Enable Router# config t Router(config)#no ip domain-lookup
Nombre del router	En modo de configuración se coloca el comando para asignarle el nombre al Router asi: Router(config)#hostname R1
Contraseña de exec privilegiado cifrada	En modo de configuración se coloca el comando para asignar la contraseña para el modo EXEC privilegiado R1(config)#enable secret class
Contraseña de acceso a la consola	En modo de configuración se coloca el comando para asignar la contraseña de acceso a la consola asi: R1(config)#line console 0 R1(config-line)#password cisco R1(config-line)#login R1(config-line)#exit
Contraseña de acceso Telnet	En modo de configuración se coloca el comando para asignar la contraseña de acceso Telnet asi: R1#(config)# line vty 0 15 R1#(config-line)# password cisco R1#(config-line)# login R1#(config-line)# exit

Cifrar las contraseñas de texto no cifrado	En modo de configuración se coloca el comando para cifrar las contraseñas de texto no cifradas asi: R1(config-line)#service password encryption
Mensaje MOTD	En modo de configuración se coloca el comando para configurar un MOTD Banner con el fin de prohibir el acceso no autorizado asi: R1(config)#banner motd #Se prohíbe el acceso no autorizado.#
Interfaz S0/0/0	En modo de configuración se coloca los comandos para configurar la interfaz S0/0/0 asi: R1(config)# int s0/0/0**(se configura la interfaz)** R1(config-if)#ip address 172.16.1.1 255.255.255.252 **(Se establece la dirección Ipv4)** R1(config-if)#ipv6 address 2001:DB8:ACAD:1::1/64 **(Se establece la dirección Ipv6)** R1(config-if)#clock rate 128000 **(Se establece la frecuencia del reloj)** R1(config-if)#no shutdown **(se active la interfaz)** R1(config-if)#exit
Rutas predeterminadas	En modo de configuración se configura las rutas predeterminadas de ipv4 e ipv6 con los siguientes comandos: R1(config)#ipv6 route ::/0 s0/0/0 **(Se configura la ruta ipv6)** R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0**(Se configura la ruta ipv4)**

2.3 Paso 3: Configuración del Router 2

Se inicia la configuración del R2, después de haberlo inicializado y cargado nuevamente, se inicia desactivando la búsqueda DNS, luego se le asigna el nombre (R2), se procede a asignarle la contraseña cifrada para el modo EXEC privilegiado (class) y luego se le coloca la contraseña de acceso a la consola (cisco), y la contraseña de acceso Telnet, se cifran las contraseñas de texto no cifrado, se configura un MOTD , se habilita el servidor HTTP, se configura la int s0/0/0, la int s0/0/1, la int g0/0 y la loopback 0 y por ultimo las rutas predeterminadas

Nota: Los comandos correspondientes para cada una de las configuraciones asignadas al R1 se muestran específicamente en la siguiente tabla.

Tabla 13: Configuración del R2.

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Se ingresa a modo privilegiado, luego se ingresa a modo de configuración y en seguida se coloca el comando para desactivar la búsqueda DNS asi: Router>Enable Router# config t Router(config)#no ip domain-lookup
Nombre del router	En modo de configuración se coloca el comando para asignarle el nombre al Router asi: Router(config)#hostname R2
Contraseña de exec privilegiado cifrada	En modo de configuración se coloca el comando para asignar la contraseña para el modo EXEC privilegiado asi: R2(config)#enable secret class

Contraseña de acceso a la consola	En modo de configuración se coloca el comando para asignar la contraseña de acceso a la consola asi: R2(config)#line console 0 R2(config-line)#password cisco R2(config-line)#login R2(config-line)#exit
Contraseña de acceso Telnet	En modo de configuración se coloca el comando para asignar la contraseña de acceso Telnet asi: R2#(config)# line vty 0 15 R2#(config-line)# password cisco R2#(config-line)# login R2#(config-line)# exit
Cifrar las contraseñas de texto no cifrado	En modo de configuración se coloca el comando para cifrar las contraseñas de texto no cifradas asi: R2(config-line)#service password encryption
Habilitar el servidor HTTP	En modo de configuración se habilita el servidor de HTTP con el siguiente comando: R2(config)#ip http server
Mensaje MOTD	En modo de configuración se coloca el comando para configurar un MOTD Banner con el fin de prohibir el acceso no autorizado asi: R2(config)#banner motd #Se prohíbe el acceso no autorizado.#

Interfaz S0/0/0	En modo de configuración se coloca los comandos para configurar la interfaz S0/0/0 asi: R2(config)#int s0/0/0**(se configura la interfaz)** R2(config-if)#description connection to R1 **(Se le coloca la descripción de la int)** R2(config-if)#ip address 172.16.1.2 255.255.255.252**(Se establece la dirección Ipv4)** R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64 **(Se establece la dirección Ipv6)** R2(config-if)#no shutdown**(se active la interfaz)**
Interfaz S0/0/1	En modo de configuración se coloca los comandos para configurar la interfaz S0/0/1 asi: R2(config-if)#int s0/0/1**(se configura la interfaz)** R2(config-if)#description connection to R3 **(Se le coloca la descripción de la int)** R2(config-if)#ip address 172.16.2.2 255.255.255.252 **(Se establece la dirección Ipv4)** R2(config-if)#ipv6 address 2001:DB8:ACAD:2::2/64 **(Se establece la dirección Ipv6)** R2(config-if)#clock rate 128000 **(Se establece la frecuencia del reloj)** R2(config-if)#no shutdown **(se active la interfaz)**

Interfaz G0/0 (simulación de Internet)	En modo de configuración se coloca los comandos para configurar la interfaz g0/0 asi: R2(config-if)#int g0/0**(se configura la interfaz)** R2(config-if)#description connection to Internet **(Se le coloca la descripción de la int)** R2(config-if)#ip address 209.165.200.233 255.255.255.248 **(Se establece la dirección Ipv4)** R2(config-if)#ipv6 address 2001:DB8:ACAD:a::2/64 **(Se establece la dirección Ipv6)** R2(config-if)#no shutdown **(se active la interfaz)**
Interfaz loopback 0 (servidor web simulado)	En modo de configuración se coloca los comandos para configurar la interfaz loopback 0 asi: R2(config-if)#int loopback 0 **(se configura la interfaz)** R2(config-if)#ip address 10.10.10.10 255.255.255.255**(Se establece la dirección Ipv4)** R2(config-if)#description simulated web server **(Se le coloca la descripción de la int)**
Ruta predeterminada	En modo de configuración se configura las rutas predeterminadas de ipv4 e ipv6 con los siguientes comandos: R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0**(Se configura la ruta ipv4)** R2(config)#ipv6 route ::/0 g0/0 **(Se configura la ruta ipv6)**

2.4 Paso 4: Configuración del Router 3

Se inicia la configuración del R3, después de haberlo inicializado y cargado nuevamente, se inicia desactivando la búsqueda DNS, luego se le asigna el

nombre (R1), se procede a asignarle la contraseña cifrada para el modo EXEC privilegiado (class) y luego se le coloca la contraseña de acceso a la consola (cisco), y la contraseña de acceso Telnet, se cifran las contraseñas de texto no cifrado, se configura un MOTD , se configura la int s0/0/1, int Loopback 4, int Loopback 5, int Loopback 6, int Loopback 7 y por ultimo las rutas predeterminadas.

Nota: Los comandos correspondientes para cada una de las configuraciones asignadas al R3 se muestran específicamente en la siguiente tabla.

Tabla 14: Configuración del R3.

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Se ingresa a modo privilegiado, luego se ingresa a modo de configuración y en seguida se coloca el comando para desactivar la búsqueda DNS asi: Router>Enable Router# config t Router(config)#no ip domain-lookup
Nombre del router	En modo de configuración se coloca el comando para asignarle el nombre al Router asi: Router(config)#hostname R3
Contraseña de exec privilegiado cifrada	En modo de configuración se coloca el comando para asignar la contraseña para el modo EXEC privilegiado asi: R3(config)#enable secret class

Contraseña de acceso a la consola	En modo de configuración se coloca el comando para asignar la contraseña de acceso a la consola asi: R3(config)#line console 0 R3(config-line)#password cisco R3(config-line)#login
Contraseña de acceso Telnet	En modo de configuración se coloca el comando para asignar la contraseña de acceso Telnet asi: R3(config-line)#line vty 0 15 R3(config-line)#password cisco R3(config-line)#login
Cifrar las contraseñas de texto no cifrado	En modo de configuración se coloca el comando para cifrar las contraseñas de texto no cifradas asi: R3(config-line)#service password-encryption
Mensaje MOTD	En modo de configuración se coloca el comando para configurar un MOTD Banner con el fin de prohibir el acceso no autorizado asi: R3(config)#banner motd #Se prohibe el acceso no autorizado. #
Interfaz S0/0/1	En modo de configuración se coloca los comandos para configurar la interfaz s0/0/1 asi: Router>enable Router#configure terminal Router(config)#int s0/0/1 **(se configura la interfaz)** Router(config-if)#description connection to R2 34 **(Se le coloca la descripción de la int)** Router(config-if)#ip address 172.16.2.1 255.255.255.252 **(Se establece la dirección Ipv4)** Router(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64 **(Se establece la dirección Ipv6)** Router(config-if)#no shutdown **(se active la interfaz)**

Interfaz loopback 4	En modo de configuración de la interfaz se coloca los comandos para configurar la interfaz loopback 4 asi: R3(config-if)#int loopback 4 **(se configura la interfaz)** R3(config-if)#ip address 192.168.4.1 255.255.255.0 **(Se establece la dirección Ipv4)**
Interfaz loopback 5	En modo de configuración de la interfaz se coloca los comandos para configurar la interfaz loopback 5 asi: R3(config-if)#int loopback 5 **(se configura la interfaz)** R3(config-if)#ip address 192.168.5.1 255.255.255.0 **(Se establece la dirección Ipv4)**
Interfaz loopback 6	En modo de configuración de la interfaz se coloca los comandos para configurar la interfaz loopback 6 asi: R3(config-if)#int loopback 6 **(se configura la interfaz)** R3(config-if)#ip address 192.168.6.1 255.255.255.0 **(Se establece la dirección Ipv4)**
Interfaz loopback 7	En modo de configuración de la interfaz se coloca los comandos para configurar la interfaz loopback 7 asi: R3(config-if)#int loopback 7 **(se configura la interfaz)** R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64**(Se establece la dirección Ipv6)**
Rutas predeterminadas	En modo de configuración se configura las rutas predeterminadas de ipv4 e ipv6 con los siguientes comandos: R3(config)#ip route 0.0.0.0 0.0.0.0 g0/0 **(Se configura la ruta ipv4)** R3(config)#ipv6 route ::/0 g0/0**(Se configura la ruta ipv6)**

2.5 Paso 5: Configuración del S1

Se inicia la configuración del S1, después de haberlo inicializado y cargado nuevamente, se inicia desactivando la búsqueda DNS, luego se le asigna el nombre (S1), se procede a asignarle la contraseña cifrada para el modo EXEC privilegiado (class) y luego se le coloca la contraseña de acceso a la consola (cisco), y la contraseña de acceso Telnet, se cifran las contraseñas de texto no cifrado, y por último se configura un MOTD.

Nota: Los comandos correspondientes para cada una de las configuraciones asignadas al S1 se muestran específicamente en la siguiente tabla.

Tabla 15: Configuración del S1.

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Se ingresa a modo privilegiado, luego se ingresa a modo de configuración y en seguida se coloca el comando para desactivar la búsqueda DNS asi: Switch>enable Switch#configure terminal Switch(config)#no ip domain-lookup
Nombre del switch	En modo de configuración se coloca el comando para asignarle el nombre al Switch asi: Switch(config)#hostname S1
Contraseña de exec privilegiado cifrada	En modo de configuración se coloca el comando para asignar la contraseña para el modo EXEC privilegiado asi: S1(config)#enable secret class

Contraseña de acceso a la consola	En modo de configuración se coloca el comando para asignar la contraseña de acceso a la consola asi: S1(config)#line console 0 S1(config-line)#password cisco S1(config-line)#login
Contraseña de acceso Telnet	En modo de configuración se coloca el comando para asignar la contraseña de acceso Telnet asi: S1(config-line)#line vty 0 15 S1(config-line)#password cisco S1(config-line)#login
Cifrar las contraseñas de texto no cifrado	En modo de configuración se coloca el comando para cifrar las contraseñas de texto no cifradas asi: S1(config-line)#service password-encryption
Mensaje MOTD	En modo de configuración se coloca el comando para configurar un MOTD Banner con el fin de prohibir el acceso no autorizado asi: S1(config)#banner motd #Se prohibe el acceso no autorizado.#

2.6 Paso 6: Configuración del S3

Se inicia la configuración del S3, después de haberlo inicializado y cargado nuevamente, se inicia desactivando la búsqueda DNS, luego se le asigna el nombre (S3), se procede a asignarle la contraseña cifrada para el modo EXEC privilegiado (class) y luego se le coloca la contraseña de acceso a la consola (cisco), y la contraseña de acceso Telnet, se cifran las contraseñas de texto no cifrado, y por último se configura un MOTD.

Nota: Los comandos correspondientes para cada una de las configuraciones asignadas al S3 se muestran específicamente en la siguiente tabla.

Tabla 16: Configuración del S3.

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Se ingresa a modo privilegiado, luego se ingresa a modo de configuración y en seguida se coloca el comando para desactivar la búsqueda DNS asi: Switch>enable Switch#configure terminal Switch(config)#no ip domain-lookup
Nombre del switch	En modo de configuración se coloca el comando para asignarle el nombre al Switch asi: Switch(config)#hostname S3
Contraseña de exec privilegiado cifrada	En modo de configuración se coloca el comando para asignar la contraseña para el modo EXEC privilegiado asi: S3(config)#enable secret class
Contraseña de acceso a la consola	En modo de configuración se coloca el comando para asignar la contraseña de acceso a la consola asi: S3(config)#line console 0 S3(config-line)#password cisco S3(config-line)#login
Contraseña de acceso Telnet	En modo de configuración se coloca el comando para asignar la contraseña de acceso Telnet asi: S3(config-line)#line vty 0 15 S3(config-line)#password cisco S3(config-line)#login
Cifrar las contraseñas de texto no cifrado	En modo de configuración se coloca el comando para cifrar las contraseñas de texto no cifradas asi: S3(config-line)#service password-encryption

Mensaje MOTD	En modo de configuración se coloca el comando para configurar un MOTD Banner con el fin de prohibir el acceso no autorizado asi: S3(config)#banner motd #Se prohibe el acceso no autorizado.#

2.7 Paso 7: Verificación de la conectividad a la red

Se utiliza el comando **ping** para verificar la conectividad entre los dispositivos

Nota: Se utiliza la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red.

Tabla 17: Verificación de la conectividad entre dispositivos

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	**Se verifica que la conexión es satisfactoria** R1#ping 172.16.1.2 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 1/22/76 ms
R2	R3, S0/0/1	172.16.2.1	**Se verifica que la conexión es satisfactoria** R2#ping 172.16.2.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 172.16.2.1, timeout is 2 seconds: !!!!!

			Success rate is 100 percent (5/5), round-trip min/avg/max = 1/9/14 ms
PC de Internet	Gateway predeterminado	209.165.200.233	**Se verifica que la conexión es satisfactoria** C:\>ping 209.165.200.233 Pinging 209.165.200.233 with 32 bytes of data: Reply from 209.165.200.233: bytes=32 time=1ms TTL=255 Reply from 209.165.200.233: bytes=32 time<1ms TTL=255 Reply from 209.165.200.233: bytes=32 time<1ms TTL=255 Reply from 209.165.200.233: bytes=32 time<1ms TTL=255 Ping statistics for 209.165.200.233: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 1ms, Average = 0ms

Figura 25. Verificación con el comando ping desde R1 a R2.

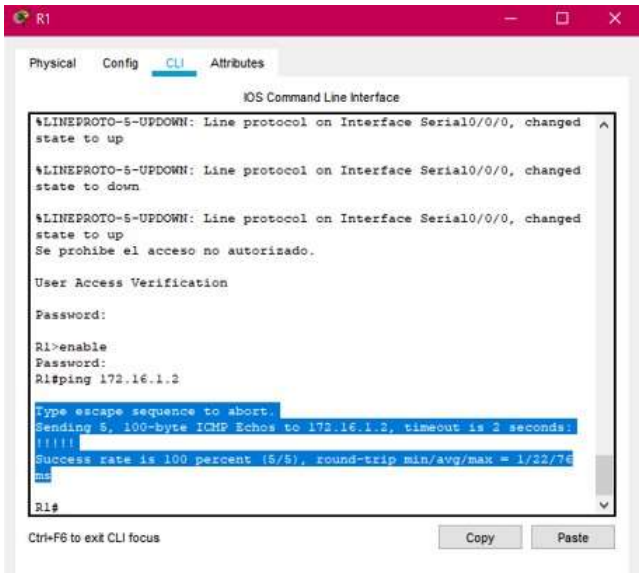


Figura 26. Verificación con el comando ping desde R2 a R3.

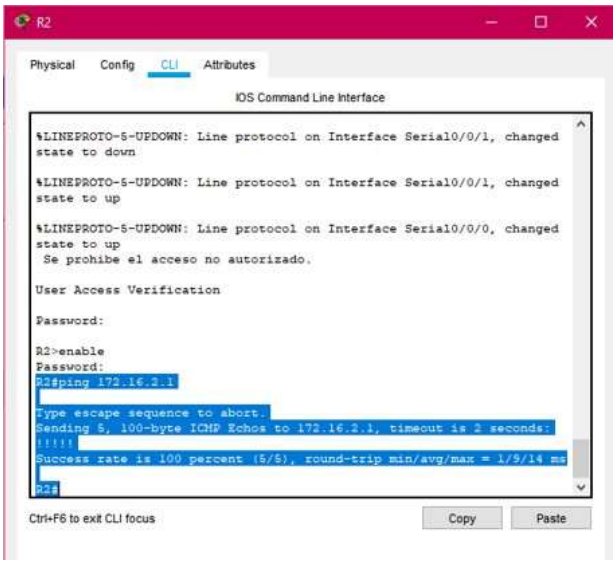
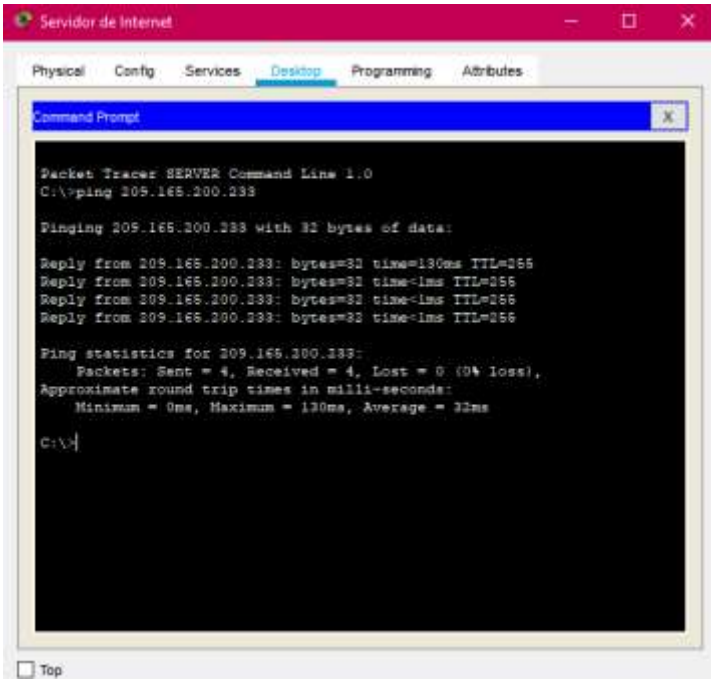


Figura 27. Verificación con el comando ping desde Servidor de Internet al Gateway predeterminado.



3. Parte 3: Configuración de la seguridad del switch, las VLAN y el routing entre VLAN

3.1 Paso 1: Configuración de S1

Se inicia creando la base de datos de Vlan, se le asigna la dirección ip de administrador, se le asigna el Gateway predeterminado, se hace forzar el enlace troncal en la interfaz F0/3, se hace forzar el enlace troncal en la interfaz F0/5, se Configura el resto de los puertos como puertos de acceso, se le asignar F0/6 a la VLAN 21 y por último se apagan todos los puertos sin usar.

Nota: En la siguiente tabla se encuentran especificados los comandos que se utilizaran para configurar el S1

Tabla 18: Configuración S1.

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	En modo de configuración se coloca el comando para crear la base de datos de Vlan asi: S1#configure terminal **(Modo configuración)** S1(config)#vlan 21**(Se accede a la vlan 21)** S1(config-vlan)#name Contabilidad**(Se coloca el nombre a la Vlan 21)** S1(config-vlan)#exit S1(config)#vlan 23. **(Se accede a la vlan 23)** S1(config-vlan)#name Ingenieria **(Se coloca el nombre a la Vlan 23)** S1(config-vlan)#exit S1(config)#vlan 99**(Se accede a la vlan 99)** S1(config-vlan)#name Administracion **(Se coloca el nombre a la Vlan 99)** S1(config-vlan)#exit
Asignar la dirección IP de administración.	En modo de configuración se le asigna la dirección Ip a la vlan 99 con el siguiente comando: S1#configure terminal **(modo de configuración)** S1(config)#int vlan 99 **(Se ingresa a configurar la vlan 99)** S1(config-if)#ip address 192.168.99.2 255.255.255.0 **(Se le asigna la dirección ip a la vlan 99)** S1(config-if)#no shutdown **(Se enciende la interfaz vlan 99)**
Asignar el gateway predeterminado	En modo de configuración se le asigna el gateway predeterminado con el siguiente comando: S1(config)#ip default-gateway 192.168.99.1

Forzar el enlace troncal en la interfaz F0/3	En modo de configuración se hace forar el enlace truncal en la int f0/3 con el siguiente comando: S1(config)#int f0/3 **(Se ingresa a configurar la int)** S1(config-if)#switchport mode trunk**(modo troncal)** S1(config-if)#switchport trunk native vlan 1
Forzar el enlace troncal en la interfaz F0/5	En modo de configuración se hace forzar el enlace truncal en la int f0/3 con el siguiente comando: S1(config)#int f0/5 **(Se ingresa a configurar la int)** S1(config-if)#switchport mode trunk **(modo troncal)** S1(config-if)#switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	En modo de configuración se coloca el rango de las interfaces para configurar los puertos de acceso con el siguiente comando: S1#configure terminal **(modo de configuración)** S1(config)#int range f0/1-2, f0/4, f0/6-24, g0/1-2**(Se menciona las interfaces para configurarlas)** S1(config-if-range)#switchport mode access**(modo de acceso)**
Asignar F0/6 a la VLAN 21	En modo de configuración se le asigna a la f0/6 a la vlan 21 con el siguiente comando S1#configure terminal S1(config)#int range f0/1-2, f0/4, f0/6-24, g0/1-2 **Se menciona las interfaces para configurarlas)** S1(config-if-range)#switchport mode access **(modo de acceso)** S1(config-if-range)#int f0/6**(se menciona la int para configurarla)** S1(config-if)#switchport access vlan 21**(se le asigna elmodo de acceso a la vlan 21)**

Apagar todos los puertos sin usar	En modo de configuración rango se coloca el comando para apagar los puertos sin usar asi: S1(config-if-range)#int range f0/1-2, f0/4, f0/7-24, g0/1-2 **(interfaces que se van a apagar)** S1(config-if-range)#shutdown **(Se apagan las interfaces)**

3.2 Paso 2: Configuración de S3

Se inicia creando la base de datos de Vlan, se le asigna la dirección ip de administrador, se le asigna el Gateway predeterminado, se hace forzar el enlace troncal en la interfaz F0/3, se Configura el resto de los puertos como puertos de acceso, se le asignar F0/18 a la VLAN 23 y por último se apagan todos los puertos sin usar.

Nota: En la siguiente tabla se encuentran especificados los comandos que se utilizaran para configurar el S3

Tabla 19: Configuración S3.

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	En modo de configuración se coloca el comando para crear la base de datos de Vlan asi: S3#configure terminal **(Modo configuración)** S3(config)#vlan 21**(Se accede a la vlan 21)** S3(config-vlan)#name Contabilidad**(Se coloca el nombre a la Vlan 21)** S3(config-vlan)#exit S3(config)#vlan 23. **(Se accede a la vlan 23)** S3(config-vlan)#name Ingenieria **(Se coloca el nombre a la Vlan 23)** S3(config-vlan)#exit S3(config)#vlan 99**(Se accede a la vlan 99)** S3(config-vlan)#name Administracion **(Se coloca el nombre a la Vlan 99)** S3(config-vlan)#exit

Asignar la dirección IP de administración	En modo de configuración se le asigna la dirección Ip a la vlan 99 con el siguiente comando: S3#configure terminal **(modo de configuración)** S3(config)#int vlan 99 **(Se ingresa a configurar la vlan 99)** S3(config-if)#ip address 192.168.99.3 255.255.255.0 **(Se le asigna la dirección ip a la vlan 99)** S3(config-if)#no shutdown **(Se enciende la interfaz vlan 99)**
Asignar el gateway predeterminado.	En modo de configuración se le asigna el gateway predeterminado con el siguiente comando: S3(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	En modo de configuración se hace forzar el enlace truncal en la int f0/3 con el siguiente comando: S3(config)#int f0/3 **(Se ingresa a configurar la int)** S3(config-if)#switchport mode trunk**(modo troncal)** S3(config-if)#switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	En modo de configuración se coloca el rango de las interfaces para configurar los puertos de acceso con el siguiente comando: S3(config-if)#interface range f0/1-2, f0/4-17, f0/19-24, g0/1-2 **(Se menciona las interfaces para configurarlas)** S3(config-if-range)#switchport mode access **(modo de acceso)** S3(config-if-range)#exit

Asignar F0/18 a la VLAN 21**(se modifica queda Vlan 23 ya que la topología aparece Vlan 23)**	En modo de configuración se le asigna a la f0/18 a la vlan 23 con el siguiente comando S3(config)#int f0/18 **(se menciona la int para configurarla)** S3(config-if)#switchport mode access **(Modo de acceso)** S3(config-if)#switchport access vlan 23**(se le asigna elmodo de acceso a la vlan 23)**
Apagar todos los puertos sin usar	En modo de configuración rango se coloca el comando para apagar los puertos sin usar asi: S3(config-if)#interface range f0/1-2, f0/4-17, f0/19-24, g0/1-2**(Interfaces que se van a pagar)** S3(config-if-range)#shutdown **(Se apagan las interfaces)**

3.3 Paso 3: Configuración de R1

Se inicia configurando desde la int g0/1 la subinterfaz 802.1Q .21 en G0/1, la subinterfaz 802.1Q .23 en G0/1 y la subinterfaz 802.1Q .99 en G0/1, por último se activa la int g0/1

Nota: En la siguiente tabla se encuentran especificados los comandos que se utilizaran para configurar el R1

Tabla 20: Configuración R1.

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	En modo de configuración se ingresa a la Int g0/1 para configurar la subinterfaz 802.1Q.21 con el siguiente comando: R1(config)#int g0/1.21**(Se inicia la configuración de la subinterfaz de g0/1)** R1(config-subif)#description LAN de Contabilidad **(se le asigna la descrición a la subinterfaz)** R1(config-subif)#encapsulation dot1q 21 R1(config-subif)#ip address 192.168.21.1 255.255.255.0 **(se le asigna la ip a la subinterfaz)**

Configurar la subinterfaz 802.1Q .23 en G0/1	En modo de configuración se ingresa a la Int g0/1 para configurar la subinterfaz 802.1Q.23 con el siguiente comando: R1(config)#int g0/1.23 **(Se inicia la configuración de la subinterfaz de g0/1)** R1(config-subif)#description LAN de Ingenieria **(se le asigna la descrición a la subinterfaz)** R1(config-subif)#encapsulation dot1q 23 R1(config-subif)#ip address 192.168.23.1 255.255.255.0 **(se le asigna la ip a la subinterfaz)**
Configurar la subinterfaz 802.1Q .99 en G0/1	En modo de configuración se ingresa a la Int g0/1 para configurar la subinterfaz 802.1Q.99 con el siguiente comando: R1(config)#int g0/1.99 **(Se inicia la configuración de la subinterfaz de g0/1)** R1(config-subif)#description LAN de Administracion **(se le asigna la descrición a la subinterfaz)** R1(config-subif)#encapsulation dot1q 99 R1(config-subif)#ip address 192.168.99.1 255.255.255.0 **(se le asigna la ip a la subinterfaz)**
Activar la interfaz G0/1	En modo de configuración se active la interfaz g0/1 con el siguiente comando: R1(config)#int g0/1**(se menciona la int para su configuración)** R1(config-if)#no shutdown **(Se activa la interfaz)**

3.4 Paso 4: Verificación

Se utiliza el comando **ping** para probar la conectividad entre los switches y el R1

Nota: Se utiliza la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red

Tabla 21: Verificación de la conectividad de la red

.

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	**El resultado es satisfactorio** S1#ping 192.168.99.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
S3	R1, dirección VLAN 99	192.168.99.1	**El resultado es satisfactorio** S3#ping 192.168.99.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
S1	R1, dirección VLAN 21	192.168.21.1	**El resultado es satisfactorio** S1#ping 192.168.21.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.21.1, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/2 ms
S3	R1, dirección VLAN 23	192.168.23.1	**El resultado es satisfactorio** S3#ping 192.168.23.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.23.1, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/2/10 ms

Figura 28. Verificación desde S1 a R1 vlan 99

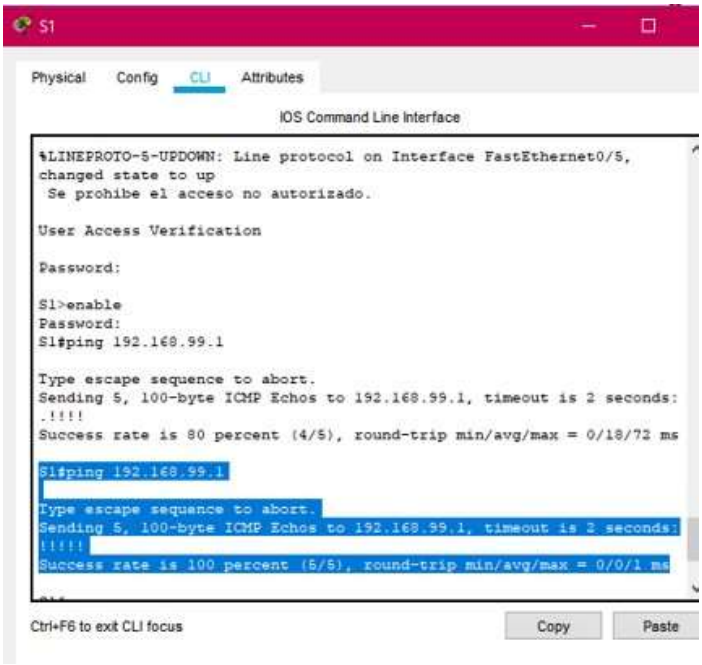


Figura 29. Verificación desde S3 a R1 vlan 99

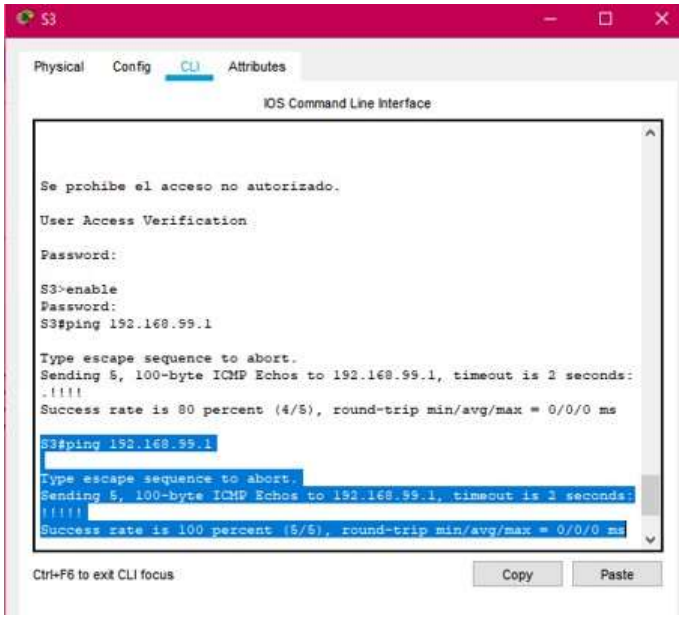


Figura 30. Verificación desde S1 a R1 vlan 21

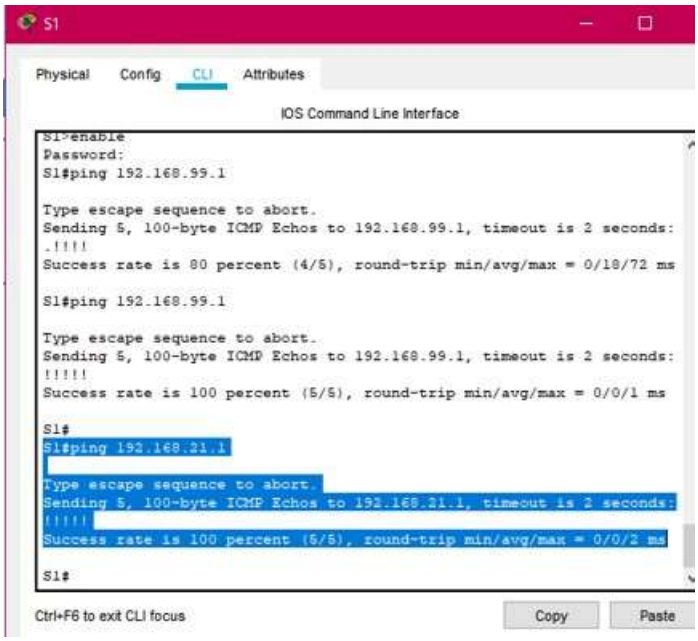


Figura 31. Verificación desde S3 a R1 vlan 23

4. Parte 4: Configuración del el protocolo de routing dinámico OSPF

4.1 Paso 1: Configuración OSPF en el R1

En la configuración de OSPF es necesario que el proceso de enrutamiento OSPF esté activo en el Router con las direcciones de red y la información de área especificadas. Las direcciones de red se configuraron con una máscara wildcard. La máscara wildcard son las direcciones de enlaces que estan presentes.

Nota: A continuación se tiene el comando utilizado para la configuración de Ospf en el R1.

R1(config)# router ospf 1 **(Se habilita el enrutamiento Ospf)**
R1(config-router)# network 172.16.1.0 0.0.0.3 area 0 **(Se especifica la red)**
R1(config-router)# network 192.168.21.0 0.0.0.255 area 0 **(Se especifica la red)**
R1(config-router)# network 192.168.23.0 0.0.0.255 area 0 **(Se especifica la red)**
R1(config-router)# network 192.168.99.0 0.0.0.255 area 0 **(Se especifica la red)**
R1(config-router)#exit
R1(config)# router ospf 1 **(Se habilita el enrutamiento Ospf)**
R1(config-router)# passive-interface g0/1.21**(evita la transmisión de mensajes de routing a través de una interfaz del router)**
R1(config-router)# passive-interface g0/1.23 **(se establece la int Lan como pasiva)**
R1(config-router)# passive-interface g0/1.99 **(se establece la int Lan como pasiva)**
R1(config-router)#no auto-summary **(Este comando se utiliza para configurar Rip no para Ospf)**
R1(config-router)#exit
R1#

4.2 Paso 2: Configuración OSPF en el R2

En la configuración de OSPF es necesario que el proceso de enrutamiento OSPF esté activo en el Router con las direcciones de red y la información de área especificadas. Las direcciones de red se configuraron con una máscara wildcard. La máscara wildcard son las direcciones de enlaces que estan presentes.

Nota: A continuación se tiene el comando utilizado para la configuración de Ospf en el R2.

R2(config)# router ospf 1 **(Se habilita el enrutamiento Ospf)**
R2(config-router)# network 10.10.10.10 0.0.0.0 area 0 **(Se especifica la red)**
R2(config-router)# network 172.16.1.0 0.0.0.3 area 0 **(Se especifica la red)**
R2(config-router)# network 172.16.2.0 0.0.0.3 area 0 **(Se especifica la red)**
R2(config-router)#exit
R2(config)# router ospf 1 **(Se habilita el enrutamiento Ospf)**
R2(config-router)# passive-interface Loopback0 **(se establece la int Lan como pasiva)**
R2(config-router)#no auto-summary **(Este comando se utiliza para configurar Rip)**
R2(config-router)#exit
R2#

4.3 Paso 3: Configuración OSPFv3 en el R3

En la configuración de OSPF es necesario que el proceso de enrutamiento OSPF esté activo en el Router con las direcciones de red y la información de área especificadas. Las direcciones de red se configuraron con una máscara wildcard. La máscara wildcard son las direcciones de enlaces que estan presentes.

Nota: A continuación se tiene el comando utilizado para la configuración de Ospf en el R3.

R3#config t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#ipv6 unicast-routing **(Se habilita ipv6 al router)**
R3(config)#ipv6 router ospf 1 **(Se habilita el enrutamiento Ospf)**
R3(config-rtr)#router-id 1.1.1.1 **(Se le coloca el id)**
R3(config-rtr)#interface s0/0/1 **(Se ingresa a la int)**
R3(config-if)#ipv6 ospf 1 area 0 **(Se menciona la area)**
R3(config-if)#exit
R3(config)#ipv6 router ospf 1**(Se habilita el enrutamiento Ospf)**
R3(config-rtr)#passive-interface Loopback4 **(se establece la int Lan como pasiva)**
R3(config-rtr)#passive-interface Loopback5 **(se establece la int Lan como pasiva)**

R3(config-rtr)#passive-interface Loopback6**(se establece la int Lan como pasiva)**
R3(config-rtr)#passive-interface Loopback7**(se establece la int Lan como pasiva)**
R3(config-rtr)#no auto-summary summary **(Este comando se utiliza para configurar Rip)**

R3(config-rtr)#exit
R3(config)#exit

4.4 Paso 4: Verificación de la información de Ospf

Se verifica que OSPF esté funcionando como se espera, introduciendo los comandos en CLI según se indica en la tabla 20.

Tabla 22. Verificación de Ospf

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

Figura 32. Comando show ip protocols en R1

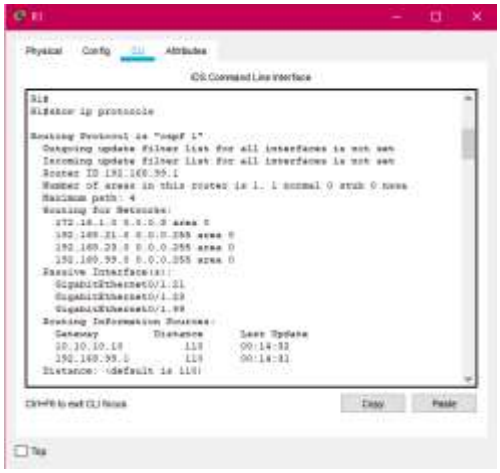


Figura 33. Comando show ip route ospf en R1

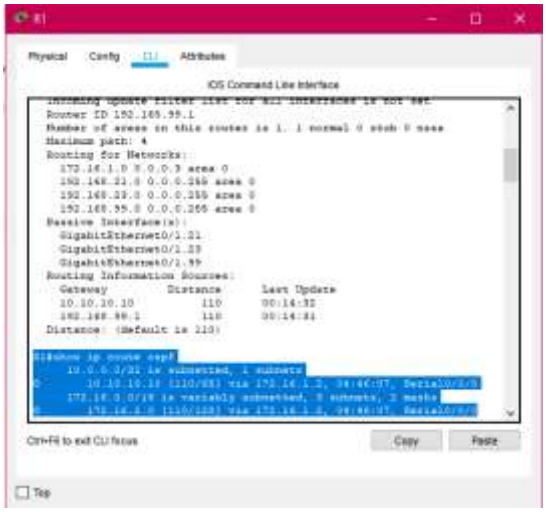
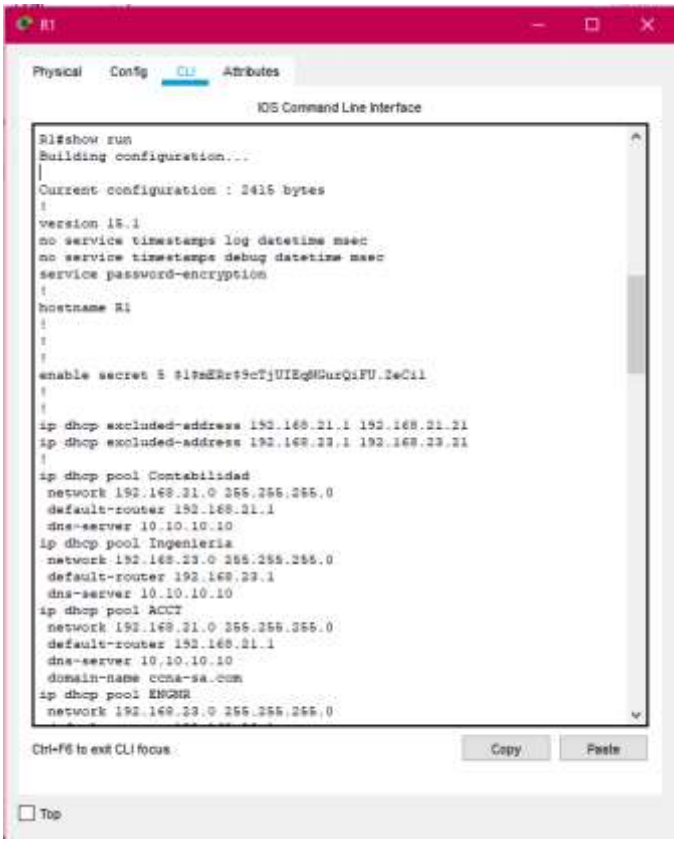


Figura 34 Comando show run en R1



5. Parte 5: Implementación de DHCP y NAT para IPv4

5.1 Paso 1: Configuración del R1 como servidor de DHCP para las VLAN 21 y 23

Se inicia reservando las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas, y las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas, se crear un pool de DHCP para la VLAN 21 y la VLAN 23 .

Nota: En la siguiente tabla esta la configuración del R1 como servidor de DHCP para las VLAN 21 y 23

Tabla 23. Configuración del R1

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	En modo de configuración se revan las primeras direcciones ip en la vlan 21 para configuraciones estaticas con el siguiente comando: R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.21
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	En modo de configuración se revan las primeras direcciones ip en la vlan 23 para configuraciones estaticas con el siguiente comando: R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.21

Crear un pool de DHCP para la VLAN 21.	En modo de configuración se crea un pool de DHCP para la Vlan 21 con los siguientes comandos: R1(config)#ip dhcp pool ACCT**(Se le asigna el nombre de ACCT)** R1(dhcp-config)#dns-server 10.10.10.10**(Se le asigna el servidor)** R1(dhcp-config)#network 192.168.21.0 255.255.255.0 **(dirección)** R1(dhcp-config)#default-router 192.168.21.1 **(Se le asigna el gateway)** R1(dhcp-config)#domain-name ccna-sa.com **(Se le asigna el nombre del dominio)**
Crear un pool de DHCP para la VLAN 23	R1(config)#ip dhcp pool ENGRN **(Se le asigna el nombre de ENGRN)** R1(dhcp-config)#dns-server 10.10.10.10 **(Se le asigna el servidor)** R1(dhcp-config)#network 192.168.23.0 255.255.255.0 **(dirección)** R1(dhcp-config)#default-router 192.168.23.1**(Se le asigna el gateway)** R1(dhcp-config)#domain-name ccna-sa.com**(Se le asigna el nombre del dominio)**

5.2 Paso 2: Configuración la NAT estática y dinámica en el R2

Se inicia reservando las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas, y las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas, se crear un pool de DHCP para la VLAN 21 y la VLAN 23 .

Nota: En la siguiente tabla esta la configuración del R2

Tabla 24. Configuración del R2

Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	En modo de configuración se crea una base de datos local con una Cuenta de usuario con el siguiente comando: R2(config)#username webuser privilege 15 secret cisco12345
Habilitar el servicio del servidor HTTP	R2(config)#ip http server **(Comando no soportado)**
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	R2(config)#ip http authentication local **(Comando no soportado)**
Crear una NAT estática al servidor web.	En modo de configuración se crea una NAT estatica al servidor web con el siguiente comando: 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	En modo de configuración se le asigna la interfaz interna y extrema para Nata estática con los siguientes comandos R2(config)#interface g0/0 R2(config-if)#ip nat outside R2(config)#interface s0/0/0 R2(config-if)#ip nat inside R2(config-if)#interface s0/0/1 R2(config-if)#ip nat inside
Configurar la NAT dinámica dentro de una ACL privada	En el modo de configuración se configurá la NAT dinámica dentro de una ACL privada con los siguientes 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.	En modo de configuración se define el pool de direcciones Ip públicas utilizables con el siguiente comando: R2(config)#ip nat pool INTERNET 209.165.200.233 209.165.200.236 netmask 255.255.255.248
Definir la traducción de NAT dinámica	En modo de configuración se define la traducción de NAT dinámica con el siguiente comando: R2(config)#ip nat inside source list 1 pool INTERNET

5.3 Paso 3: Verificación del protocolo DHCP y la NAT estática

Se realiza el ping entre los dispositivos mencionados en la siguiente tabla para la verificación del protocolo DHCP y la NAT estática

Tabla 25. Verificación del protocolo DHCP y la NAT estática

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	**Se observa que efectivamente la PC-A adquirió información de ip del servidor de DHCP:** Ipv4 Address: 192.168.21.22 Subnet Mask: 255.255.255.0 Default Gateway: 192.168.21.1 DNS ever: 10.10.10.10
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	**Se observa que efectivamente la PC-C adquirió información de ip del servidor de DHCP:** Ipv4 Address: 192.168.23.22 Subnet Mask: 255.255.255.0 Default Gateway: 192.168.23.1 DNS ever: 10.10.10.10

Verificar que la PC-A pueda hacer ping a la PC-C	**El resultado es satisfactorio al realizar el ping** C:\>ping 192.168.23.22 Pinging 192.168.23.22 with 32 bytes of data: Reply from 192.168.23.22: bytes=32 time<1ms TTL=127 Reply from 192.168.23.22: bytes=32 time<1ms TTL=127 Reply from 192.168.23.22: bytes=32 time<1ms TTL=127 Reply from 192.168.23.22: bytes=32 time<1ms TTL=127 Ping statistics for 192.168.23.22: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms
Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.238) Iniciar sesión con el nombre de usuario **webuser** y la contraseña **cisco12345**	**El resultado es satisfactorio** Cisco Packet Tracer Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open. Quick Links: A small page Copyrights Image page Image

Figura 35. Verificación de PC-A

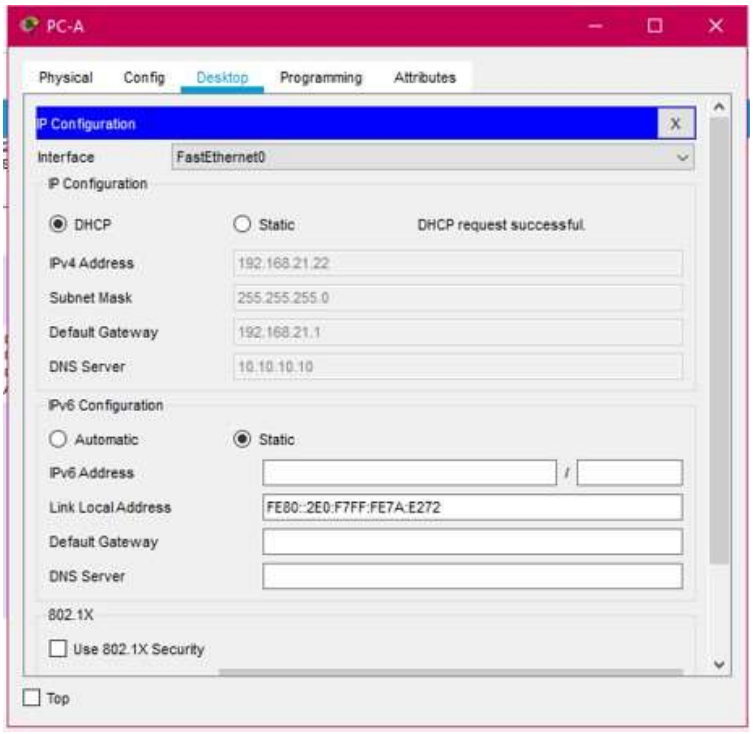


Figura 36. Verificación de PC-C

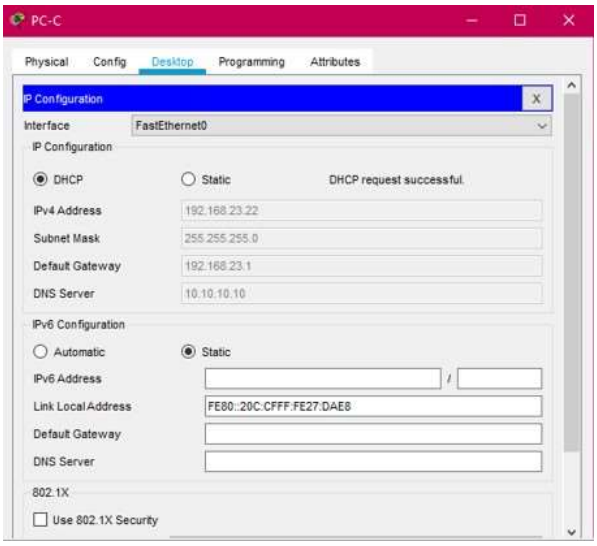


Figura 37. Verificación desde PC-A a PC-C

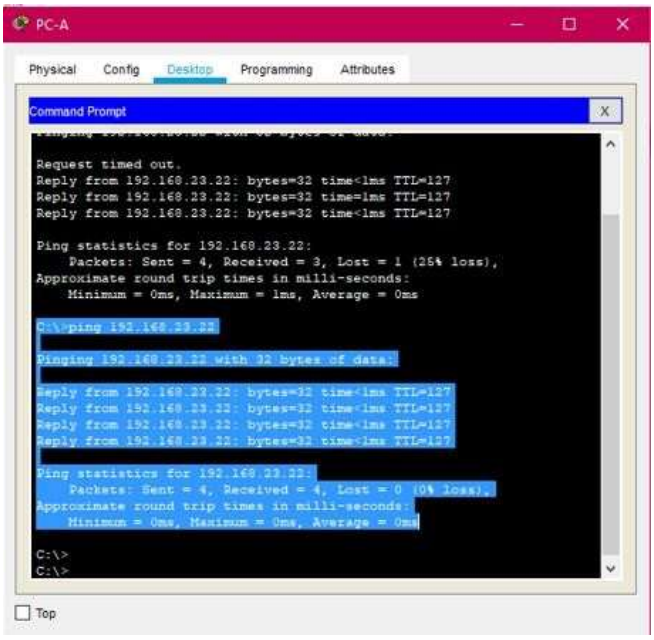
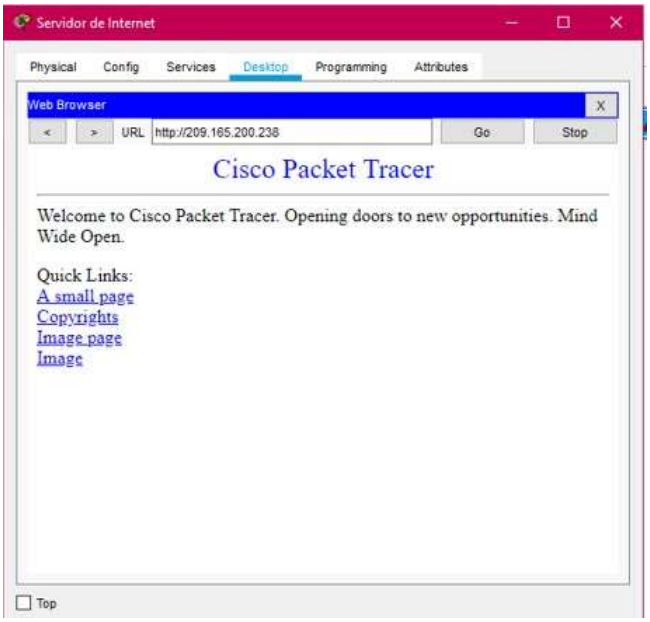


Figura 38. Verificación al Servidor de Internet



6. Parte 6: Configuración de NTP

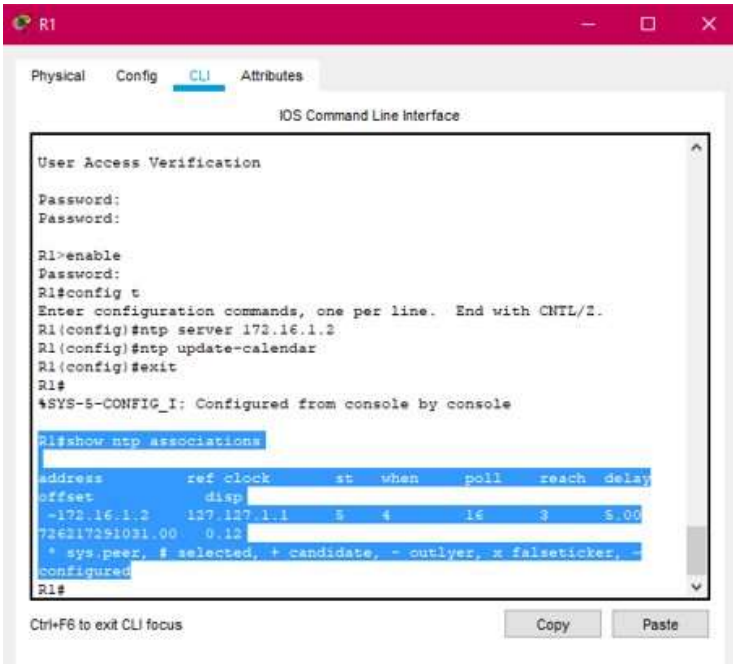
Se inicia con el ajuste de la fecha y la hora en el R2, se configurá R2 como un maestro NTP, luego se configura R1 como un cliente NTP y para

actualizaciones de calendario periódicas con hora NTPy por último se verifica la configuración de NTP en R1

Tabla 26. Configuración del NTP

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	Se configura la fecha y hora en el R2 con el siguiente comando R2#clock set 09:00:00 5 march 2016
Configure R2 como un maestro NTP.	En modo de configuración se configura R2 como un maestro NTP con el siguiente comando R2(config)#ntp master 5
Configurar R1 como un cliente NTP.	En modo de configuración se configura R1 como un cliente NTP con el siguiente comando: R1(config)#ntp server 172.16.1.2
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	En modo de configuración se configura el R1 para actualizaciones de calendario periódicas con hora NTP con el siguiente comando R1(config)#ntp update-calendar
Verifique la configuración de NTP en R1.	Con el siguiente comando se verifica R1#show ntp associations

Figura 39. Verificación NTP en R1



7. Parte 7: Configuración y verificación de las listas de control de acceso (ACL)

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

Se inicia configurando una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2, se aplica la ACL con nombre a las líneas VTY, se permite acceso por Telnet a las líneas de VTY y por último se verifica que la ACL funcione como se espera

Tabla 27. Restringir el acceso a líneas VTY en 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	En modo de configuración se configura una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2 con el siguiente comando. R2(config)#ip access-list standard ADMIN-MGT R2(config-std-nacl)#permit host 172.16.1.1
Aplicar la ACL con nombre a las líneas VTY	En modo de configuración se aplica la ACL con nombre a las líneas VTY con el siguiente comando R2(config)#line vty 0 15 R2(config-line)#access-class ADMIN-MGT in
Permitir acceso por Telnet a las líneas de VTY	En modo de configuración de la linea se permite el acceso por Telnet a las líneas VTY para R2 con el siguiente comando R2(config-line)#transport input telnet
Verificar que la ACL funcione como se espera	Se verifica que la ACL funcione correctamente con el siguiente comando en R1. R1#telnet 172.16.1.2

Figura 40. Verificación de la ACL en R1

7.2 Paso 2: Se introduce el comando de CLI adecuado que se necesita para mostrar lo siguiente

Tabla 28. Verificación de comandos

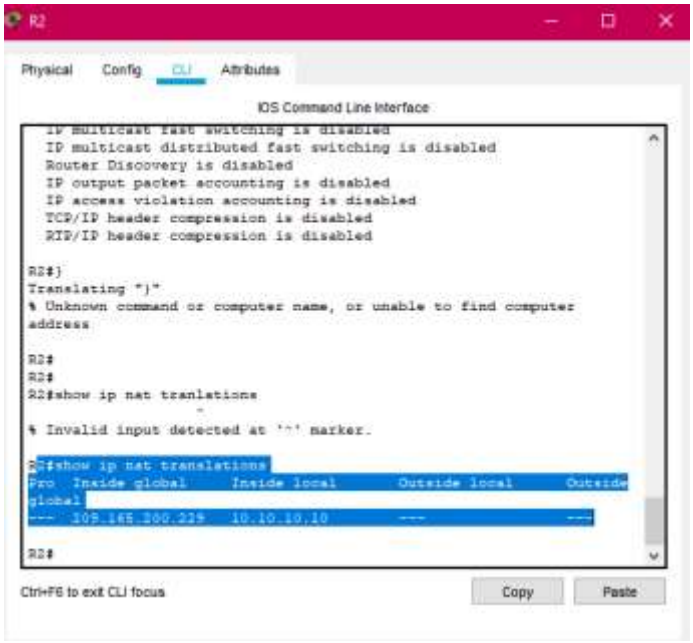
Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	R2#show access-list R2#show ip access-list
Restablecer los contadores de una lista de acceso	R2#clear ip access-list counters
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	R2#show ip interface
¿Con qué comando se muestran las traducciones NAT?	**R2#show ip nat translations**

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

Figura 41. Verificación del comando show access-list en R2

Figura 42. Verificación del comando show ip interface en R2

Figura 43. Verificación del comando show ip nat translations en R2



CONCLUSIONES

Al realizar las configuraciones de los dispositivos en cada red, se practicó los llamados comandos básicos los cuales son fundamentales para el funcionamiento correcto de cada dispositivo.

Al utilizar un servidor DHCP nos trae muchas ventajas, porque permite asignar y administrar las direcciones IP de una forma sencilla, práctica pero sobre todo eficiente y además disminuye el riesgo de duplicidad de direcciones Ip en la red evitando los problemas de conectividad.

Se puede decir que por las NAT, se detuvo el agotamiento de las direcciones IP válidas, ya que deja que varios hosts dentro de una red privada, obtenga acceso a Internet al usar pocas direcciones IP válidas.

BIBLIOGRAFIA

Curso CCNA2. Principios básicos de routing y switching. Recuperado el 27 de mayo del 2018 de: https://1314297.netacad.com/courses/654717

Froom, R., Frahim, E. (2015). CISCO Press (Ed). Spanning Tree Implementation. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. Recuperado de https://1drv.ms/b/s!AmIJYei-NT1IlnWR0hoMxgBNv1CJ

Lucas, M. (2009). Cisco Routers for the Desperate : Router and Switch Management, the Easy Way. San Francisco: No Starch Press. Recuperado de: http://bibliotecavirtual.unad.edu.co:2048/login?url=http://search.ebscohost.com/logi.aspx?direct=true&db=e000xww&AN=440032&lang=es&site=ehost-live

Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). EIGRP Implementation. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. Recuperado de https://1drv.ms/b/s!AmIJYei- NT1IlnMfy2rhPZHwEoWx

ANEXOS

Anexo A: Link del desarrollo de los escenarios 1 y 2

https://drive.google.com/drive/folders/1pG6K8jP-mi7kwpaIwssBbsfUEIj1uK-z?usp=sharing

Anexo B: Articulo Científico

https://drive.google.com/drive/folders/19us-Kfcvb7Oa4tohu-UpiBe9Uhdyc50Q?usp=sharing

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

Laura Natalia Galeano Rincón
Universidad Nacional Abierta y a Distancia, lngaleanor@unadvirtual.edu.co

Resumen

El desarrollo de este artículo científico tiene como finalidad aplicar en el escenario 2 los conceptos adquiridos en el diplomado de Cisco, este escenario 2 cuenta con una topología de una red pequeña que está compuesta por un Servidor de Internet, 3 Routers, 2 Switch y dos PC los cuales se configuran para que sea admitida la conectividad tanto de Ipv4 como de Ipv6, la seguridad de los Switches, el routing entre las Vlan, el protocolo (Ospf) que significa protocolo de routing dinámico, el protocolo (DHCP) que significa protocolo de configuración de host dinámicos, la traducción de redes dinámicas y estáticas, listas de control de acceso (ACL) y el protocolo de tiempo de red.

La funcionalidad de este escenario 2 se verifica por medio de comandos a cada dispositivo, y asi se prueba la conexión correcta de la red, dado el caso que la verificación no fuera satisfactoria se tendría que indagar que configuración esta incorrecta y proceder a solucionarlo.

Palabras clave: CISCO, CCNA, Conmutación, Enrutamiento, Redes, Electrónica.

Abstract:

The development of this scientific article aims to apply in scenario 2 the concepts acquired in the Cisco diploma, this scenario 2 has a topology of a small network that is composed of an Internet Server, 3 Routers, 2 Switches and two PCs which are configured to support both IPv4 and IPv6 connectivity, the security of the Switches, the routing between the Vlan, the protocol (Ospf) which means dynamic routing protocol, the protocol (DHCP) which means protocol dynamic host configuration, static and dynamic network translation, access control lists (ACLs), and network time protocol.

The function of this scenario 2 is verified by means of commands in each device, and thus the correct connection of the network is tested, in the event that the verification was not satisfactory, it should be found out which configuration is incorrect and proceed to solve it.

Keywords— CISCO, CCNA, Switching, Routing, Networks, Electronics.

I. Introducción

Hoy en día las redes nos conectan cada vez más. [1]Las personas se comunican en línea desde cualquier lugar. Las conversaciones que tienen lugar en las aulas pasan a las sesiones de chat de mensajes instantáneos, y los debates en línea continúan en el lugar de estudios. Diariamente, se desarrollan nuevos servicios para aprovechar la red.

En lugar de crear sistemas exclusivos e independientes para la prestación de cada servicio

nuevo, el sector de redes en su totalidad adoptó un marco de desarrollo que permite que los diseñadores comprendan las plataformas de red actuales y las mantengan. Al mismo tiempo, este marco se utiliza para facilitar el desarrollo de nuevas tecnologías, a fin de satisfacer las necesidades de las comunicaciones y las mejoras tecnológicas futuras.

[2]Para dar soporte a nuestras comunicaciones, el modelo OSI divide las funciones de una red de datos en capas. Cada capa trabaja con las capas superior e inferior para transmitir datos. Dos capas dentro del modelo OSI están tan relacionadas que, según el modelo TCP/IP, son básicamente una sola. Esas dos capas son la capa de enlace de datos y la capa física.

Se tiene que [3] Ethernet es la tecnología LAN predominante en el mundo. Ethernet funciona en la capa de enlace de datos y en la capa física. Los estándares del protocolo Ethernet definen muchos aspectos de la comunicación en red, incluido el formato, el tamaño, la temporización y la codificación de las tramas. Cuando se envían mensajes entre hosts a través de una red Ethernet, los hosts asignan un formato a los mensajes según la configuración de trama que especifican los estándares.

Si bien [4] el diseño, la implementación y la administración de un plan de asignación de direcciones IP eficaz aseguran que las redes puedan operar de manera eficaz y eficiente. Esto es así especialmente a medida que aumenta la cantidad de conexiones de host a una red. Comprender la estructura jerárquica de la dirección IP y cómo modificar esa jerarquía a fin de satisfacer con mayor eficiencia los requisitos de routing constituye una parte importante de la planificación de un esquema de asignación de direcciones IP.

Las estructuras de redes pequeñas, [5] el diseño de la red suele ser simple. La cantidad y el tipo de dispositivos incluidos se reducen considerablemente en comparación con una red más grande. En general, las topologías de red constan de un único Router y uno o más switches. Las redes pequeñas también pueden tener puntos de acceso inalámbrico (posiblemente incorporados al Router) y teléfonos IP. En cuanto a la conexión a Internet, las redes pequeñas normalmente tienen una única conexión WAN proporcionada por una conexión DSL, por cable o Ethernet.

La administración de una red pequeña requiere muchas de las mismas habilidades necesarias para administrar redes más grandes. La mayor parte del trabajo se centra en el mantenimiento y la resolución de problemas de equipos existentes, así como en la protección de los dispositivos y de la información de la red. La administración de las redes pequeñas está a cargo de un empleado de la empresa o de una persona contratada por esta, según el tamaño y el tipo de empresa.

[6] Los distintos dispositivos deben trabajar en conjunto sin inconvenientes para proporcionar una conexión rápida, segura y confiable entre los hosts. Los switches LAN proporcionan el punto de conexión a la red empresarial para los usuarios finales y también son los principales responsables del control de la información dentro del entorno LAN. Los routers facilitan la transmisión de información entre redes LAN y, en general, desconocen a los hosts individuales. Todos los servicios avanzados dependen de la disponibilidad de una infraestructura sólida de routing y switching que les sirva de base. Esta infraestructura se debe diseñar, implementar y administrar cuidadosamente para proporcionar una plataforma estable.

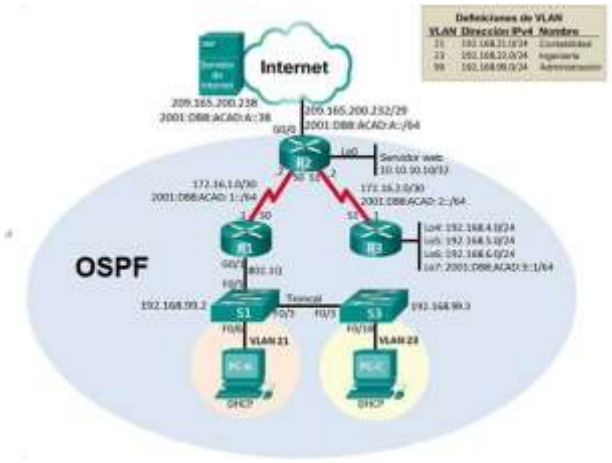
II. METODOLOGÍA

La metodología que se utiliza para la implementación del escenario dos de la prueba de habilidades se hace en base de una investigación de tipo aplicada ya que se trata de desarrollar de una forma adecuada para que se pueda transmitir paquetes de información en la red LAN entre Ipv4 e Ipv6 en los hosts. [7] La Investigación Aplicada tiene por objetivo resolver un determinado problema o planteamiento específico, enfocándose en la búsqueda y consolidación del conocimiento para su aplicación y, por ende, para el enriquecimiento del desarrollo cultural y científico. En la topología de red se plantea una topología de red LAN compuesta por dispositivos como Routers, Switches, hosts y cableado de consola donde se busca que puedan interactuar los dispositivos entre sí.

III. RESULTADOS

Partiendo de la topología propuesta en el escenario 2 se implementa configurando 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, se prueba y registra la red mediante los comandos comunes de CLI.

Figura 1. Topología Escenario 2



Se procede a realizar las configuraciones básicas de los dispositivos.

TABLA 1
Configuración de Servidor de Internet

Elemento o tarea de configuración	**Especificación**
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.233
Dirección IPv6/subred	2001:DB8:ACAD:A::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:2::1

Configuración Básica de Routers

Se realiza la configuración del R1, después de haberlo inicializado y cargado nuevamente, se inicia desactivando la búsqueda DNS, luego se le asigna el nombre (R1), se procede a asignarle la contraseña cifrada para el modo EXEC privilegiado (class) y luego se le coloca la contraseña de acceso a la consola (cisco), y la contraseña de acceso Telnet, se cifran las contraseñas de texto no cifrado, se configura un MOTD , se configura la int s0/0/0 y por ultimo las rutas predeterminadas.

Se realiza la configuración del R2, después de haberlo inicializado y cargado nuevamente, se inicia desactivando la búsqueda DNS, luego se le asigna el nombre (R2), se procede a asignarle la contraseña cifrada para el modo EXEC

privilegiado (class) y luego se le coloca la contraseña de acceso a la consola (cisco), y la contraseña de acceso Telnet, se cifran las contraseñas de texto no cifrado, se configura un MOTD , se habilita el servidor HTTP, se configura la int s0/0/0, la int s0/0/1, la int g0/0 y la loopback 0 y por ultimo las rutas predeterminadas

Se realiza la configuración del R3, después de haberlo inicializado y cargado nuevamente, se inicia desactivando la búsqueda DNS, luego se le asigna el nombre (R1), se procede a asignarle la contraseña cifrada para el modo EXEC privilegiado (class) y luego se le coloca la contraseña de acceso a la consola (cisco), y la contraseña de acceso Telnet, se cifran las contraseñas de texto no cifrado, se configura un MOTD , se configura la int s0/0/1, int Loopback 4, int Loopback 5, int Loopback 6, int Loopback 7 y por ultimo las rutas predeterminadas.

Configuración Básica de Switches

Se configura el S1, después de haberlo inicializado y cargado nuevamente, se inicia desactivando la búsqueda DNS, luego se le asigna el nombre (S1), se procede a asignarle la contraseña cifrada para el modo EXEC privilegiado (class) y luego se le coloca la contraseña de acceso a la consola (cisco), y la contraseña de acceso Telnet, se cifran las contraseñas de texto no cifrado, y por último se configura un MOTD.

Se configura el S3, después de haberlo inicializado y cargado nuevamente, se inicia desactivando la búsqueda DNS, luego se le asigna el nombre (S3), se procede a asignarle la contraseña cifrada para el modo EXEC privilegiado (class) y luego se le coloca la contraseña de acceso a la consola (cisco), y la contraseña de acceso Telnet, se cifran las contraseñas de texto no cifrado, y por último se configura un MOTD

Figura 2. Verificación con el comando ping desde R1 a R2

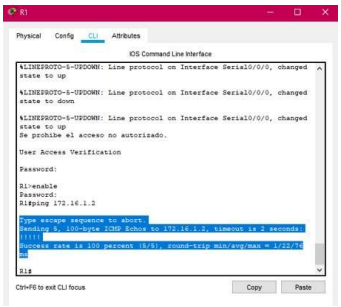


Figura 3. Verificación con el comando ping desde R2 a R3.

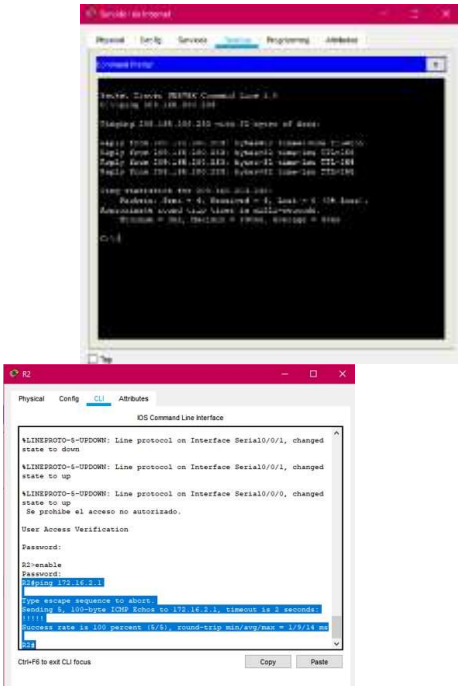


Figura 4. Verificación con el comando ping desde Servidor de Internet al Gateway predeterminado.

Configuración de la seguridad del switch, las VLAN y el routing entre VLAN

Se inicia configurando el S1 donde se crea la base de datos de Vlan, se le asigna la dirección ip de administrador, se le asigna el Gateway predeterminado, se hace forzar el enlace troncal en la interfaz F0/3, se hace forzar el enlace troncal en la interfaz F0/5, se Configura el resto de los puertos como puertos de acceso, se le asignar F0/6 a la VLAN 21 y por último se apagan todos los puertos sin usar.

En el S3 se crea la base de datos de Vlan, se le asigna la dirección ip de administrador, se le asigna el Gateway predeterminado, se hace forzar el enlace troncal en la interfaz F0/3, se Configura el resto de los puertos como puertos de acceso, se le asignar F0/18 a la VLAN 23 y por último se apagan todos los puertos sin usar.

Y por último se configura R1 donde se inicia configurando desde la int g0/1 la subinterfaz 802.1Q .21 en G0/1, la subinterfaz 802.1Q .23 en G0/1 y la subinterfaz 802.1Q .99 en G0/1, por último se activa la int g0/1

Figura 5. Verificación desde S1 a R1 vlan 99

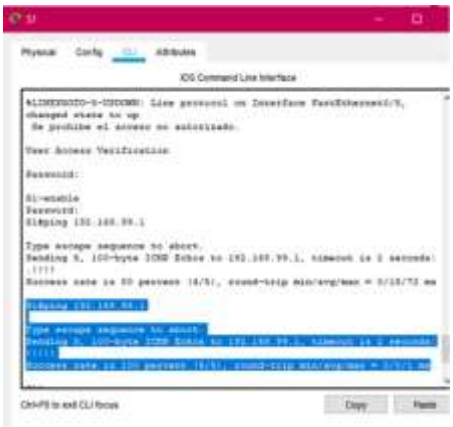
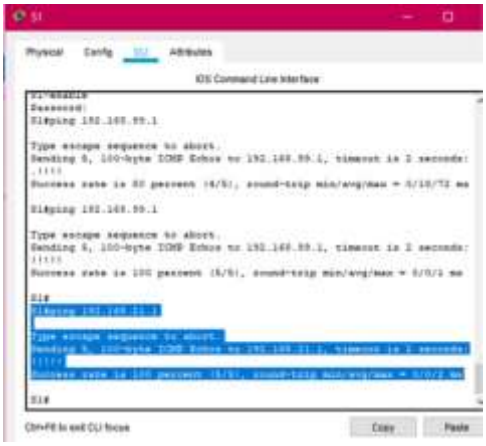


Figura 6. Verificación desde S3 a R1 vlan 99

Figura 7. Verificación desde S1 a R1 vlan 21



Configuración del el protocolo de routing dinámico OSPF

En la configuración de OSPF es necesario que el proceso de enrutamiento OSPF esté activo en los Routers con las direcciones de red y la información de área especificadas. Las direcciones de red se configuraron con una máscara wildcard. La máscara wildcard son las direcciones de enlaces que estan presentes.

TABLA 2
Comandos para Verificación de Ospf

Pregunta	Respuesta
¿Con qué comando se muestran la ID del proceso	Show ip protocols

OSPF, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router?	
¿Qué comando muestra solo las rutas OSPF?	show ip route ospf
¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	Show run

Figura 8 Verificación comando show run en R1

Implementación de DHCP y NAT para IPv4

[8] El uso de un servidor de DHCP centralizado permite a las organizaciones administrar todas las asignaciones de direcciones IP desde un único servidor. Esta práctica hace que la administración de direcciones IP sea más eficaz y asegura la coherencia en toda la organización, incluso en las sucursales.

[9] NAT proporciona la traducción de direcciones privadas a direcciones públicas. Esto permite que un dispositivo con una dirección IPv4 privada acceda a recursos fuera de su red privada, como los que se encuentran en Internet. La combinación de NAT con las direcciones IPv4 privadas resultó ser un método útil para preservar las direcciones IPv4 públicas. Se puede compartir una única dirección IPv4 pública entre cientos o incluso miles de dispositivos, cada uno configurado con una dirección IPv4 privada exclusiva.

En R1 se inicia reservando las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas, y las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas, se crear un pool de DHCP para la VLAN 21 y la VLAN 23 .

En R2 se reservan las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas, y las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas, se crear un pool de DHCP para la VLAN 21 y la VLAN 23 .

Figura 9. Verificación desde PC-A a PC-C

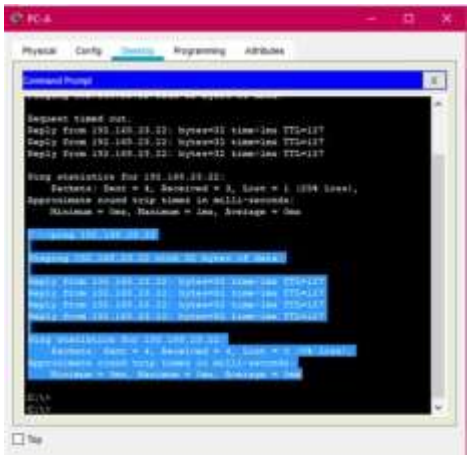


Figura 10. Verificación al Servidor de Internet

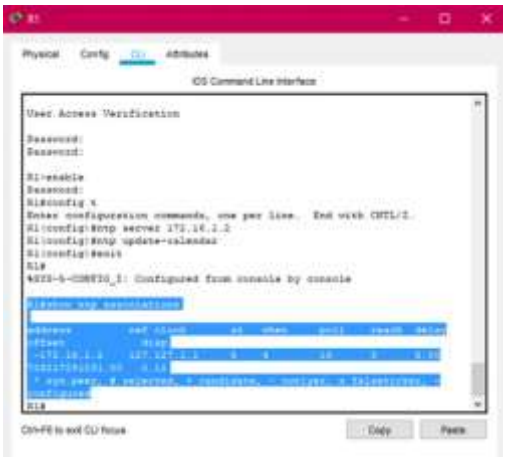
Configuración de NTP

[10] El Network Time Protocol (NTP) se puede utilizar en forma efectiva para sincronizar la hora en todos sus dispositivos de red, algo especialmente importante al tratar de comparar archivos de registro provenientes de diferentes dispositivos. Estos archivos de registro son generados por el protocolo syslog. Los mensajes de syslog se pueden capturar y enviar a un servidor syslog para facilitar las tareas de administración de dispositivos.

El mantenimiento de los dispositivos incluye asegurarse de que se haya una copia de respaldo de las imágenes y los archivos de configuración de Cisco IOS en una ubicación segura en caso de que la memoria del dispositivo se corrompa o se borre, ya sea por motivos maliciosos o involuntarios. El mantenimiento también incluye mantener actualizada la imagen de IOS.

La configuración de NTP se inicia con el ajuste de la fecha y la hora en el R2, se configurá R2 como un maestro NTP, luego se configura R1 como un cliente NTP y para actualizaciones de calendario periódicas con hora NTPy por último se verifica la configuración de NTP en R1

Figura 11. Verificación NTP en R1



Configuración y verificación de las listas de control de acceso (ACL)

Se inicia configurando una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2, se aplica la ACL con nombre a las líneas VTY, se permite acceso por Telnet a las líneas de VTY y por último se verifica que la ACL funcione como se espera.

Figura 12. Verificación de la ACL en R1

Ya para culminar se vefica con una serie de comando el funcionamiento adecuado de la red.

Figura 13. Verificación del comando show access-list en R2

Figura 14. Verificación del comando show ip interface en R2

IV. CONCLUSIONES

Al realizar las configuraciones de los dispositivos en cada red, se practicó los llamados comandos básicos los cuales son fundamentales para el funcionamiento correcto de cada dispositivo.

Al utilizar un servidor DHCP nos trae muchas ventajas, porque permite asignar y administrar las direcciones IP de una forma sencilla, práctica pero sobre todo eficiente y además disminuye el riesgo de duplicidad de direcciones Ip en la red evitando los problemas de conectividad.

Se puede decir que por las NAT, se detuvo el agotamiento de las direcciones IP válidas, ya que deja que varios hosts dentro de una red privada, obtenga acceso a Internet al usar pocas direcciones IP válidas.

V. Referencias

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

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

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

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

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

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

[7] Duoc UC Bibliotecas. (s. f.). Definición y propósito de la investigación aplicada. Definición y Propósito de la investigación aplicada. Recuperado 17 de noviembre de 2020, de http://www.duoc.cl/biblioteca/crai/definicion-y-proposito-de-la-investigacion-aplicada

[8] CISCO. (2019). DHCP. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-

assets.s3.amazonaws.com/RSE6/es/index.html#8

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

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

Biografía

Laura Galeano nació en Bogotá D. C Colombia, el 17 de Febrero de 1994, actual estudiante de la Universidad Nacional Abierta y a Distancia (Unad) en la Ingeniería de sistemas.

Cuenta con experiencia en análisis y desarrollo de sistemas de información, diseño gráfico, servicio al cliente, atención a la primera infancia, y acompañamiento comunidades víctimas y personas con condición de vulnerabilidad según criterios del gobierno. .