# PRUEBA DE HABILIDADES PRÁCTICAS CCNA
# (DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN)

JACOBO CARVAJAL CARLOSAMA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
INGENIERIA ELECTRONICA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA (ECBTI)
PEREIRA, RISARALDA
2020

# PRUEBA DE HABILIDADES PRÁCTICAS CCNA
# (DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN)

JACOBO CARVAJAL CARLOSAMA

Trabajo final de Diplomado de Profundización CISCO Para optar el título de Ingeniero Electrónico

TUTOR

ING. PAULITA FLOR

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

INGENIERIA ELECTRONICA

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA (ECBTI)

PEREIRA, RISARALDA

2020

Nota de aceptación

_____

_____

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Pereira 30 noviembre de 2020

# GLOSARIO

Packet Tracer: Es un software/programa diseñado por la empresa “Cisco”, que nos permitirá crear un entorno virtual de simulación de redes.

Router: Dispositivo de capa de red que usa una o más métricas para determinar la ruta óptima a través de la cual se debe enviar el tráfico de red. Los Routers envían paquetes desde una red a otra basándose en la información de la capa de red.

Switch: es un dispositivo de capa 2, utilizado para conectar equipos en red formando lo que se conoce como una red de área local (LAN) y cuyas especificaciones técnicas siguen el estándar conocido como Ethernet (o técnicamente IEEE 802.3).

OSPF: Open Shortest Path First. Algoritmo de enrutamiento IGP jerárquico, de estado de enlace, propuesto como sucesor de RIP en la comunidad de Internet. Las características de OSPF incluyen enrutamiento por menor costo, enrutamiento de múltiples rutas y balanceo de carga.

Máscara wildcard: Cantidad de 32 bits que se usa de forma conjunta con una dirección IP para determinar cuáles son los bts de una dirección IP que se deben ignorar al comparar esa dirección con otra dirección IP. La máscara wildcard se especifíca al configurar las listas de acceso.

Métricas: Método por el cual un algoritmo de enrutamiento determina que una ruta es mejor que otra. Esta información se guarda en las tablas de enrutamiento. Las métricas incluyen ancho de banda, costo de comunicación, retraso, conteo de saltos, carga, MTU, costo de la ruta y confiabilidad.

Enrutamiento dinámico: Enrutamiento que se adapta automáticamente a los cambios de la topología de la red.

Enrutamiento estático: Enrutamiento que depende de rutas ingresadas manualmente en la tabla de enrutamiento.

Estado de enlace: Hace referencia al estado del enlace que incluye la dirección IP de la interfaz/la máscara de subred, el tipo de red, el costo del enlace y cualquier router vecino de ese enlace.

Gateways: Dispositivo de una red que sirve como punto de acceso a otra red.

Hosts: Sistema de computación de una red.

Interfaz: Conexión entre dos máquinas dando lugar a una comunicación entre ellas.

IP: Protocolo de Internet. Protocolo de capa de red en el stack TCP/IP que brinda un servicio de internetworking sin conexión. El IP suministra características de direccionamiento, especificación de tipo de servicio, fragmentación y re ensamblaje y seguridad.

Área OSFP: Conjunto lógico de segmentos de red y los dispositivos conectados. Por lo general, las áreas se conectan con otras áreas a través de Routers, con lo cual conforman un mismo sistema autónomo.

Adyacencia: Relación que se forma entre Routers vecinos seleccionados y nodos extremos con el fin de intercambiar información de enrutamiento. Utilizan un segmento de medios comunes.

Dirección IPV6 Es una etiqueta numérica usada para identificar una interfaz de red

Dirección unicast Una dirección unicast identifica un único interfaz de red. El protocolo de Internet entrega los paquetes enviados a una dirección unicast al interfaz específico

Dirección anycast: Una dirección anycast es asignada a un grupo de interfaces, normalmente de nodos diferentes

Dirección Mulitcast Una dirección multicast también es usada por múltiples interfaces, Un paquete enviado a una dirección multicast es entregado a todos los interfaces que se hayan unido al grupo multicast correspondiente.

Servidor FTP: Es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP (Transmission Control Protocol), basado en la arquitectura cliente-servidor

Servidor DNS Es una tecnología basada en una base de datos que sirve para resolver nombres en las redes, es decir, para conocer la dirección IP de la máquina donde está alojado el dominio al que queremos acceder

Un servidor Web: Es un programa que utiliza el protocolo de transferencia de híper texto, HTTP para servir los archivos que forman páginas Web a los usuarios, en respuesta a sus solicitudes, que son reenviados por los clientes HTTP de sus computadoras.

## RESUMEN

Durante el desarrollo de este documento se le dará solución a las dos situaciones planteadas como parte de un examen final da habilidades prácticas en el curso CCNA 2; el administrador de la red, deberá hacer la configuración e interconexión de los dispositivos que forman parte de la red, de acuerdo a lo requerido donde se puedan aplicar los conocimientos adquiridos durante este curso, la teoría y las habilidades que se han venido desarrollando con cada una de las prácticas realizadas y que han formado una capacidad técnica suficiente para desarrollar este proceso.



Palabras Clave: CCNA, Router, Switch, VLAN, ACL, DHCP, Protocolo OSPF, NAT, Switching, Packet Tracer.



## ABSTRACT

During the development of this document you will be given the solution to the two situations raised as part of a final exam of the practical practices in the CCNA 2 course; The network administrator must make the configuration and interconnection of the devices that are part of the network, according to what is required where the knowledge acquired during this course, the theory and the skills that have been developed with each one of the practices carried out and that have formed a sufficient technical capacity to develop this process.



Keywords: CCNA, Router, Switch, VLAN, ACL, DHCP, OSPF Protocol, NAT, Switching, Packet Tracer.

TABLA DE CONTENIDO

LISTA DE TABLAS

Pág.

LISTADO DE FIGURAS

# INTRODUCCION

En el desarrollo del DIPLOMADO DE PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN), se han desarrollado laboratorios por pasos, logrando entender y aplicar en los laboratorios propuestos, para el caso trabajando una red y practicando temas aprendidos sobre Networking, se trabajara el registro de las configuraciones de cada uno de los dispositivos, la descripción detallada del paso a paso de cada una de las etapas realizadas durante su desarrollo, el registro de los procesos de verificación de conectividad mediante el uso de comandos ping, traceroute, show ip route, entre otros. Se utilizó para la creación y el proceso de configuración de la red la herramienta de software Packet Tracer.

Estas pruebas de habilidades forman parte de las actividades evaluativas del Diplomado de Profundización CCNA, la cual busca identificar el grado de desarrollo de competencias y habilidades que fueron adquiridas a lo largo del desarrollo de este y a través del cual se pondrá a prueba los niveles de comprensión y solución de problemas relacionados con diversos aspectos.

# OBJETIVOS

## GENERAL

Implementar todas las habilidades prácticas, teóricas y experiencia por parte de los futuros ingenieros de Telecomunicaciones de la Universidad Nacional Abierta y a Distancia, para identificar y aplicar una solución a un caso o situación estudio de problema de Networking.

## ESPECIFICOS

Identificar que dispositivos utilizar para la construcción de una topología de red.

Realizar configuración básica a dispositivos de comunicación como Routers, Switch, Servidores.

Implementar seguridad en Switch, elaboración de Vlans e inter Vlan Routing.

Determinar la configuración necesaria para la implementación de OPSF, protocolo dinámico de Routing.

Implementar de DHCP y NAT en dispositivos de comunicación. Configurar y verificar listas de control de acceso ACL

Verificar conectividad entre los dispositivos de una topología.

DESARROLLO DEL ESCENARIO

Escenario 1

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

TOPOLOGIA RED ESCENARIO 1

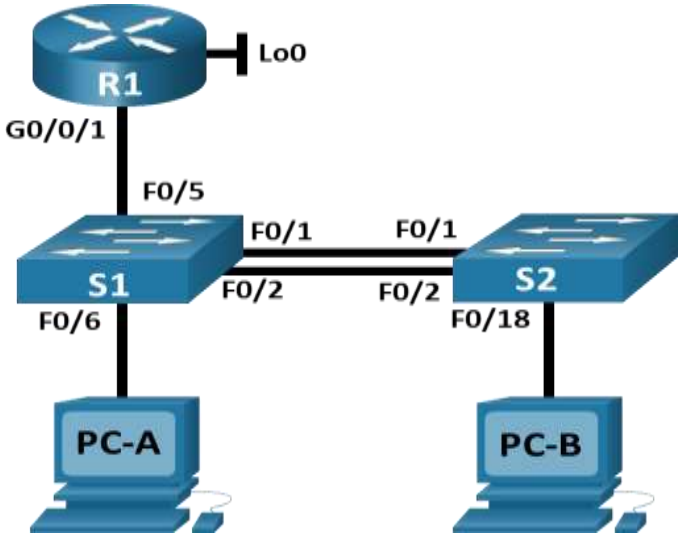



Figura 1.Topología red escenario 1

Tabla 1. Tabla de VLAN

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

Tabla 2. Tabla de asignación de direcciones

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

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

Instrucciones

Inicializar y Recargar y Configurar aspectos básicos de los dispositivos

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

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

Para el Router utilizamos los comandos de: En R1 podemos observar cómo eliminamos todos los archivos de startup-config de los Routers, se utilizó los siguientes comandos para eliminar los archivos que trae por defecto el router:

Router>enable
Router#erase startup-config
Router#reload

- Para el Switch 1 y 2 utilizamos los comandos de:

Para eliminar los archivos startup-config de los Switches se digitan los siguientes comandos:

Switch#erase startup-config
Switch#delete vlan.dad
Switch#reload

Switch#erase startup-config
Switch#delete vlan.dat
Switch#reload

**Nota:** Para eliminar toda la configuración de los dos Switches se utiliza el comando que utilizamos anteriormente, se digita en cada uno de los Switches que tengamos en la topología.

**Descripción:** Con los comandos se evidencia la eliminación de todas las configuraciones que se cargaron en los dispositivos de fábrica y se reinician con el fin de evitar afectación por la antigua configuración.

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

Switch>enable
Switch#show sdm prefer

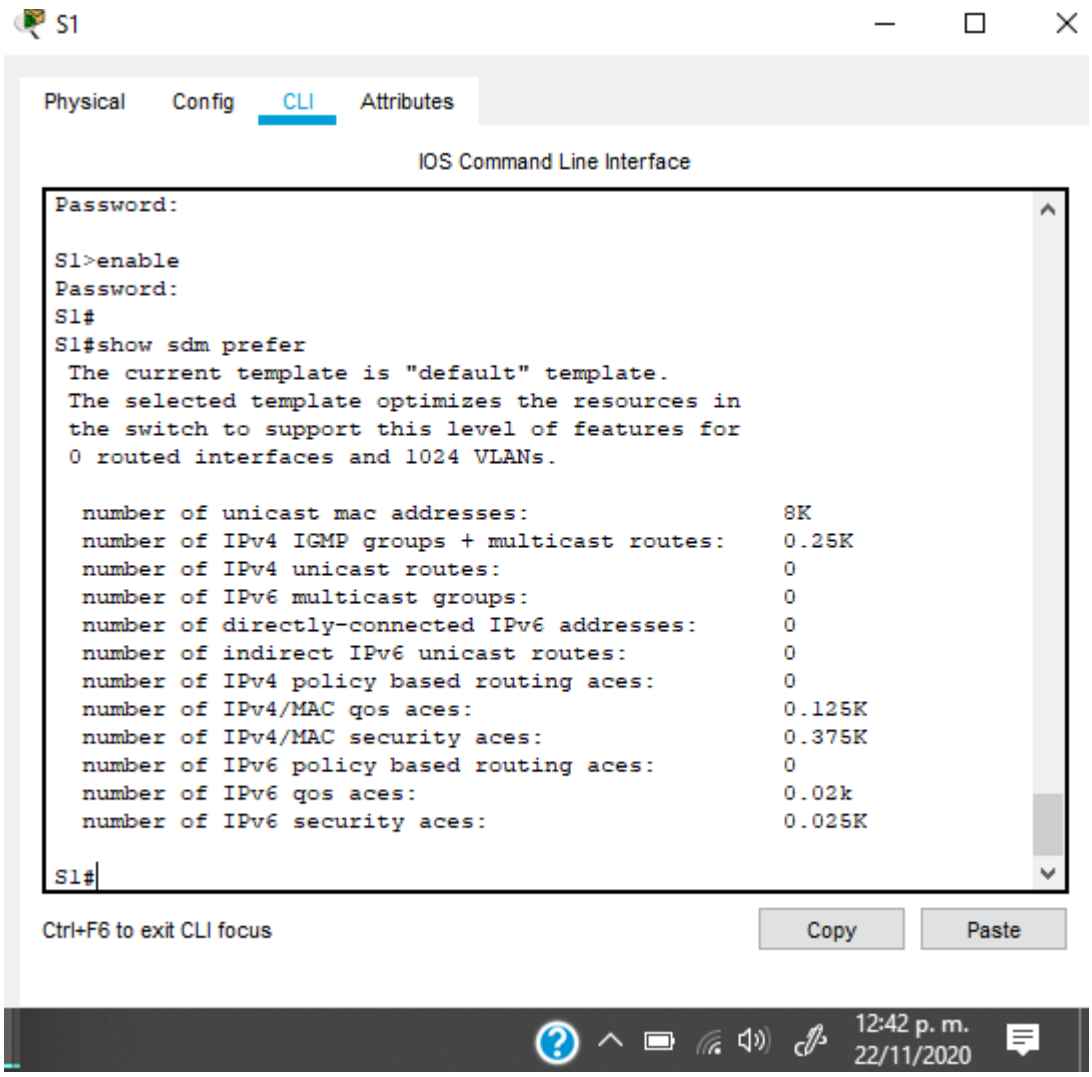


Figura 2. Configuración plantilla SDM en S1


Figura 3. Configuración plantilla SDM en S2

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

Paso 2: Configurar R1

Tabla 3. Configuración para R1

| **Tarea** | **Especificación** |
|---|---|
| Desactivar la búsqueda DNS | Router(config)#no ip domain lookup |
| Nombre del router | **R1**<br>Router(config)#hostname R1 |

| | |
|---|---|
| Nombre de dominio | **ccna-lab.com**<br><br>R1(config)#ip domain-name ccna-lab.com |
| Contraseña cifrada para el modo EXEC privilegiado | **ciscoenpass**<br><br>R1(config)#enable password ciscoenpass |
| Contraseña de acceso a la consola | **ciscoconpass**<br><br>R1(config)#enable secret **ciscoenpass**<br>R1(config)#line console 0<br>R1(config-line)#password **ciscoconpass**<br>R1(config-line)#login |
| Establecer la longitud mínima para las contraseñas | **10 caracteres**<br><br>R1(config)#security passwords min-length 10 |
| Crear un usuario administrativo en la base de datos local | Nombre de usuario: **admin**<br>Password: **admin1pass**<br><br>R1(config)#username admin secret admin1pass |
| Configurar el inicio de sesión en las líneas VTY para que use la base de datos local | R1(config)#line vty 0 15<br>R1(config-line)#login local |
| Configurar VTY solo aceptando SSH | R1(config-line)#transport input ssh |
| Cifrar las contraseñas de texto no cifrado | R1(config)#service password-encryption |
| Configure un MOTD Banner | R1(config)#banner motd &Unauthorized Access is Prohibited!& |
| Habilitar el routing IPv6 | R1(config)#ipv6 unicast-routing |
| | Establezca la descripción<br>Establece la dirección IPv4. |

| | |
|---|---|
| Configurar interfaz G0/0/1 y subinterfaces | Establezca la dirección local de enlace IPv6 como fe80: :1<br>Establece la dirección IPv6.<br>Activar la interfaz.<br>R1(config)#int g0/0/1.2<br>R1(config-subif)#encapsulation dot1q 2<br>R1(config-subif)#description Bikes<br>R1(config-subif)#ip address 10.19.8.1 255.255.255.192<br>R1(config-subif)#ipv6 address 2001:db8:acad:a::1/64<br>R1(config-subif)#ipv6 address fe80::1 link-local<br>R1(config-subif)#int g0/0/1.3<br>R1(config-subif)#description Trikes<br>R1(config-subif)#ip address 10.19.8.65 255.255.255.224<br>R1(config-subif)#encapsulation dot1q 3<br>R1(config-subif)#ip address 10.19.8.65 255.255.255.224<br>R1(config-subif)#ipv6 address 2001:db8:acad:b::1/64<br>R1(config-subif)#ipv6 address fe80::1 link-local<br>R1(config-subif)#int g0/0/1.4<br>R1(config-subif)#encapsulation dot1q 4<br>R1(config-subif)#description Management<br>R1(config-subif)#ip address 10.19.8.97 255.255.255.248<br>R1(config-subif)#ipv6 address 2001:db8:acad:c::1/64<br>R1(config-subif)#ipv6 address fe80::1 link-local<br>R1(config-subif)#int g0/0/1.6<br>R1(config-subif)#encapsulation dot1q 6 native<br>R1(config-subif)#description Native<br>R1(config-subif)#int g0/0/1<br>R1(config-if)#no shutdown |
| | Establezca la descripción<br>Establece la dirección IPv4.<br>Establece la dirección IPv6.<br>Establezca la dirección local de enlace IPv6 como **fe80::1** |

| | |
|---|---|
| Configure el Loopback0 interface | R1(config-if)#ip address 209.165.201.1 255.255.255.224<br>R1(config-if)#ipv6 address 2001:db8:acad:209::1/64<br>R1(config-if)#ipv6 address fe80::1 link-local<br>R1(config-if)#description Internet<br>R1(config-if)#exit |
| Generar una clave de cifrado RSA | Módulo de 1024 bits<br><br>R1(config)#crypto key generate rsa<br>The name for the keys will be: R1.ccna-lab.com<br>Choose the size of the key modulus in the range of 360 to 2048 for your |

**Descripción:** Se da nombre a el dispositivo, contraseña de acceso a la consola y acceso privilegiado, se incluyó un mensaje de inicio para configurar los parámetros básicos de seguridad de acceso y se cifran las contraseñas con el fin de aumentar la seguridad de estas.

Paso 3: Configure S1 y S2.

Las tareas de configuración incluyen lo siguiente:

Tabla 4. Configuración S1 y S2.

| **Tarea** | **Especificación** |
|---|---|
| Desactivar la búsqueda DNS. | Switch#configure terminal<br>Switch(config)#no ip domain-lookup<br><br>**Nota:** Para los dos Switch se procede de la misma forma |
| Nombre del switch | **S1 S2, según proceda**<br><br>Switch(config)#hostname S1<br>Switch(config)#hostname S2 |

| | |
|---|---|
| Nombre de dominio | **ccna-lab.com**<br>S1(config)#ip domain-name ccna-lab.com<br>S2(config)#ip domain-name ccna-lab.com |
| Contraseña cifrada para el modo EXEC privilegiado | **ciscoenpass**<br><br>S1(config)#enable secret ciscoenpass<br>S2(config)#enable secret ciscoenpass |
| Contraseña de acceso a la consola | **ciscoconpass**<br><br>S1(config)#line console 0<br>S1(config-line)#password ciscoconpass<br>S1(config-line)#login<br>S1(config-line)#exit<br>S2(config)#line console 0<br>S2(config-line)#password ciscoconpass<br>S2(config-line)#login<br>S2(config-line)#exit |
| Crear un usuario administrativo en la base de datos local | Nombre de usuario: **admin**<br>Password: **admin1pass**<br><br>S1(config)#username admin secret admin1pass<br>S2(config)#username admin secret admin1pass |
| Configurar el inicio de sesión en las líneas VTY para que use la base de datos local | S1(config)#line vty 0 15<br>S1(config-line)#login local<br><br>S2(config)#line vty 0 15<br>S2(config-line)#login local |
| Configurar las líneas VTY para que acepten únicamente las conexiones SSH | S1(config-line)#transport input ssh<br>S1(config-line)#exit<br><br>S2(config-line)#transport input ssh<br>S2(config-line)#exit |
| Cifrar las contraseñas de texto no cifrado | S1(config)#service password-encryption<br>S2(config)#service password-encryption |

| | |
|---|---|
| Configurar un MOTD Banner | S1(config)#banner motd &Acceso no autorizado, est prohibido!&<br><br>S2(config)#banner motd &Acceso no autorizado, est prohibido!& |
| Generar una clave de cifrado RSA | Módulo de 1024 bits<br><br>S1(config)#crypto key generate rsa modulus 1024<br>S1(config)#crypto key generate rsa<br><br>S2(config)#crypto key generate rsa modulus 1024<br>S2(config)#crypto key generate rsa |
| Configurar la interfaz de administración (SVI) | Establecer la dirección IPv4 de capa 3<br>Establezca la dirección local de enlace IPv6 como FE80: :98 para S1 y FE80: :99 para S2<br>Establecer la dirección IPv6 de capa 3<br><br>S1(config)#int vlan 4<br>S1(config-if)#ip address 10.19.8.98 255.255.255.248<br>S1(config-if)#ipv6 address 2001:db8:acad:c::98/64<br>S1(config-if)#ipv6 address fe80::98 link-local<br>S1(config-if)#description Management Interface<br>S1(config-if)#no shutdown<br>S1(config-if)#exit<br><br>S2(config)#int vlan 4<br>S2(config-if)#ip address 10.19.8.99 255.255.255.248<br>S2(config-if)#ipv6 address 2001:db8:acad:c::99/64<br>S2(config-if)#ipv6 address fe80::99 link-local<br>S2(config-if)#description Management Interface |

| | |
|---|---|
| | S2(config-if)#no shutdown<br>S2(config-if)#exit<br>S2(config)#ip default-gateway 10.19.8.97<br>S2(config)#S2(config)#int vlan 4<br>S2(config-if)#ip address 10.19.8.99 255.255.255.248<br>S2(config-if)#ipv6 address 2001:db8:acad:c::99/64<br>S2(config-if)#ipv6 address fe80::99 link-local<br>S2(config-if)#description Management Interface<br>S2(config-if)#no shutdown<br>S2(config-if)#exit |
| Configuración del gateway predeterminado | Configure la puerta de enlace predeterminada como 10.19.8.97 para IPv4<br>S1(config)#ip default-gateway 10.19.8.97<br>S2(config)#ip default-gateway 10.19.8.97 |

**Descripción:** Se da nombre a el dispositivo, contraseña de acceso a la consola y acceso privilegiado, se incluyó un mensaje de inicio para configurar los parámetros básicos de seguridad de acceso y se cifran las contraseñas con el fin de aumentar la seguridad de estas.

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

Paso 4: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 5. Configuración de S1

| Tarea | Especificación |
|---|---|
| Crear VLAN | VLAN 2, nombre Bikes<br>VLAN 3, nombre Trikes<br>VLAN 4, name Management<br>VLAN 5, nombre Parking<br>VLAN 6, nombre Native |

| | |
|---|---|
| | User Access Verification<br><br>S1#configure terminal<br>S1(config)#vlan 2<br>S1(config-vlan)#name Bikes<br>S1(config-vlan)#vlan 3<br>S1(config-vlan)#name Trikes<br>S1(config-vlan)#vlan 4<br>S1(config-vlan)#<br>S1(config-vlan)#name Management<br>S1(config-vlan)#vlan 5<br>S1(config-vlan)#name Parking<br>S1(config-vlan)#vlan 6<br>S1(config-vlan)#name Native |
| Crear troncos 802.1Q que utilicen la VLAN 6 nativa | Interfaces F0/1, F0/2 y F0/5<br>Interfaces G0/1, G0/2 y G0/5 (Por el Router Utilizado IRS 4321)<br><br>S1(config)#int g1/0/5<br>S1(config-if)#switchport trunk encapsulation dot1q<br>S1(config-if)#switchport mode trunk<br>S1(config-if)#switchport trunk native vlan 6<br>S1(config-if)#int range g1/0/1-2<br>S1(config-if-range)#<br>S1(config-if-range)#shutdown<br><br>S1(config-if-range)#channel-group 1 mode active<br>S1(config-if-range)# |
| Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2 | Usar el protocolo LACP para la negociación<br>S1(config-if-range)#int port-channel 1<br>S1(config-if)#switch trunk encapsulation dot1q<br>S1(config-if)#switchport mode trunk |

| | |
|---|---|
| | S1(config-if)#switchport trunk native vlan 6<br>S1(config-if)# |
| Configurar el puerto de acceso de host para VLAN 2 | Interface F0/6<br>S1(config-if)#int g1/0/6<br>S1(config-if)#switchport mode access<br>S1(config-if)#switchport access vlan 2 |
| Configurar la seguridad del puerto en los puertos de acceso | Permitir 3 direcciones MAC<br>S1(config-if)#switchport port-security<br>S1(config-if)#switchport port-security maximum 3<br>S1(config-if)#int range g1/0/3-4 |
| Proteja todas las interfaces no utilizadas | Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar<br><br>S1(config-if-range)#switchport mode access<br>S1(config-if-range)#switchport access vlan 5<br>S1(config-if-range)#description No esta en Uso<br>S1(config-if-range)#shutdown<br>S1(config-if-range)#int range g1/0/7-24<br>S1(config-if-range)#switchport mode access<br>S1(config-if-range)#switchport access vlan 5<br>S1(config-if-range)#description No esta en Uso<br>S1(config-if-range)#shutdown<br>S1(config-if-range)#int range g1/1/1-4<br>S1(config-if-range)#switchport mode access<br>S1(config-if-range)#switchport access vlan 5<br>S1(config-if-range)#description No esta en Uso<br>S1(config-if-range)#shutdown |

**Descripción:** Se realiza creación de las Vlan 2, 3 4, 5 y 6. Se establece comunicación entre los Switch de modo troncal con el fin de manejar el tráfico entre las Vlan.

Paso 1: Configure el S2.

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

Tabla 6. Configuración de S2

| Tarea | Especificación |
|---|---|
| Crear VLAN | VLAN 2, name Bikes<br>VLAN 3, name Trikes<br>VLAN 4, name Management<br>VLAN 5, nombre Parking<br>VLAN 6, nombre Native<br>S2(config-vlan)#vlan 2<br>S2(config-vlan)#name Bikes<br>S2(config-vlan)#vlan 3<br>S2(config-vlan)#name Trikes<br>S2(config-vlan)#vlan 4<br>S2(config-vlan)#name Management<br>S2(config-vlan)#vlan 5<br>S2(config-vlan)#name Parking<br>S2(config-vlan)#vlan 6<br>S2(config-vlan)#name Native |
| Crear troncos 802.1Q que utilicen la VLAN 6 nativa | Interfaces F0/1 y F0/2<br>S2(config)#int range g1/0/1-2<br>S2(config-if-range)#shutdown |
| Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2 | Usar el protocolo LACP para la negociación<br>S2(config-if-range)#switchport trunk encapsulation dot1q<br>S2(config-if-range)#switchport mode trunk<br>S2(config-if-range)#switchport trunk native vlan 6<br>S2(config-if-range)#channel-group 1 mode active<br>S2(config-if-range)#int port-channel 1 |

| | |
|---|---|
| | S2(config-if)#switchport trunk encapsulation dot1q<br>S2(config-if)#switchport mode trunk<br>S2(config-if)#switch trunk native vlan 6 |
| Configurar el puerto de acceso del host para la VLAN 3 | Interfaz F0/18S2(config-if)#int g1/0/18<br>S2(config-if)#switchport mode access<br>S2(config-if)#switchport access vlan 3 |
| Configure port-security en los access ports | permite 3 MAC addresses<br><br>S2(config-if)#switchport port-security<br>S2(config-if)#switchport port-security maximum 3 |
| Asegure todas las interfaces no utilizadas. | Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar<br>S2(config-if)#int range g1/0/3-17<br>S2(config-if-range)#switchport mode access<br>S2(config-if-range)#switchport access vlan 5<br>S2(config-if-range)#description No esta en Uso<br>S2(config-if-range)#shutdown<br>S2(config-if-range)#int range g1/0/19-24<br>S2(config-if-range)#switchport mode access<br>S2(config-if-range)#switchport access vlan 5<br>S2(config-if-range)#description No esta en Uso<br>S2(config-if-range)#shutdown<br>S2(config-if-range)#int range g1/1/1-4<br>S2(config-if-range)#switchport mode access<br>S2(config-if-range)#switchport access vlan 5<br>S2(config-if-range)#description No esta en Uso<br>S2(config-if-range)#shutdown |

**Descripción:** Se realiza creación de las Vlan 2, 3 4, 5 y 6. Se establece comunicación entre los Switch de modo troncal con el fin de manejar el tráfico entre las Vlan.

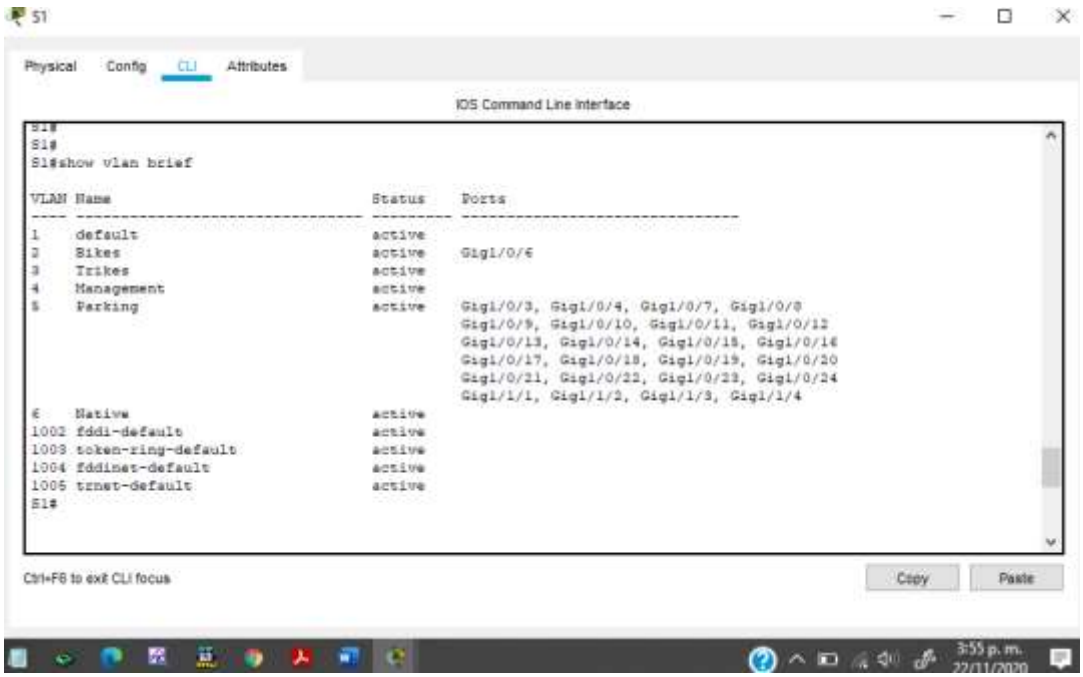



Figura 4. Show vlan brief en S1

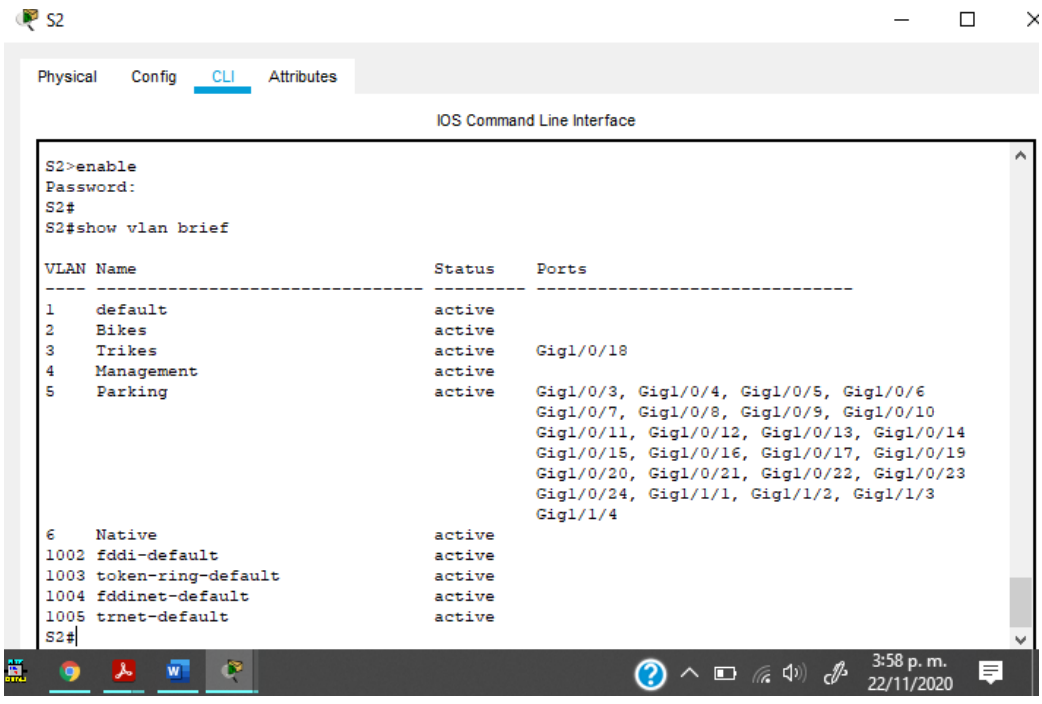



Figura 5. Show vlan brief en S2

Configurar soporte de host

Paso 2: Configure R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 7. Configuración de R1

| Tarea | Especificación |
|---|---|
| Configure Default Routing | Crear rutas predeterminadas para IPv4 e IPv6 que dirijan el tráfico a la interfaz Loopback 0<br><br>R1(config)#ip route 0.0.0.0 0.0.0.0 loopback 0<br>R1(config)#ipv6 route ::/0 loopback 0<br><br>Ambas rutas estáticas para llegar a internet |
| Configurar IPv4 DHCP para VLAN 2 | Cree un grupo DHCP para VLAN 2, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio ccna-a.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada<br><br>R1(config)#ip dhcp excluded-address10.19.8.1 10.19.8.52<br>R1(config)#ip dhcp pool VLAN2-Bikes<br>R1(dhcp-config)#network 10.19.8.0 255.255.255.192<br>R1(dhcp-config)#default-router 10.19.8.1<br>R1(dhcp-config)#domain-name ccna-a.net |
| Configurar DHCP IPv4 para VLAN 3 | Cree un grupo DHCP para VLAN 3, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio ccna-b.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada<br><br>R1(dhcp-config)#exit<br>R1(config)#ip dhcp excluded-address 10.19.8.65 10.19.8.84<br>R1(config)#ip dhcp pool VLAN3Trikes |

| | |
|---|---|
| | R1(dhcp-config)#network 10.19.8.64 255.255.255.224<br>R1(dhcp-config)#default-router 10.19.8.65<br>R1(dhcp-config)#domain-name ccna-b.net<br>R1(dhcp-config)# |

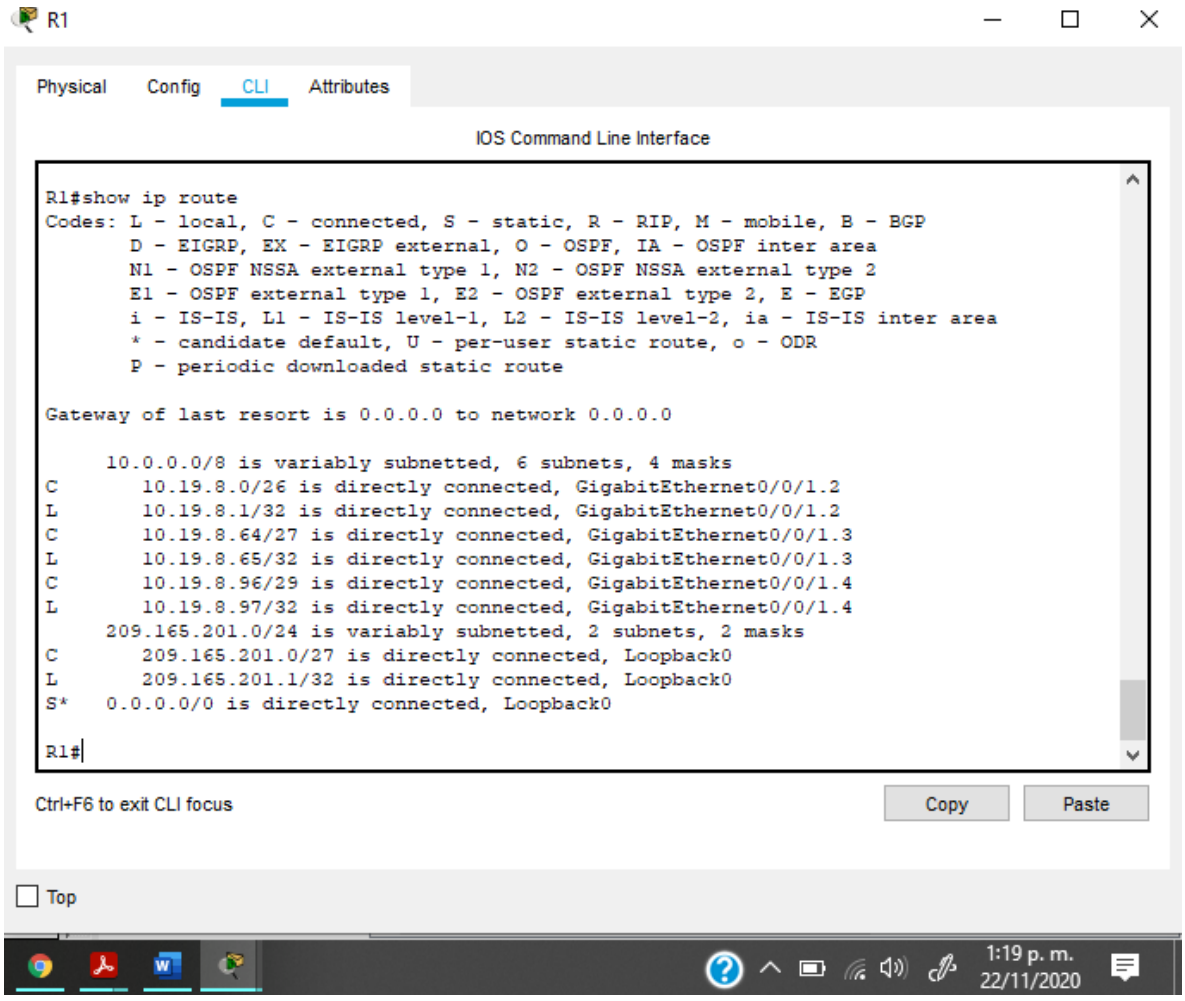



Figura 6. Configuración para R1

Paso 3: Configurar los servidores

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

Tabla 8. Configuración de red de PC-A

| **Configuración de red de PC-A** | |
|---|---|
| Descripción | *ccna-a.net* |
| Dirección física | *0040.0BC1.57DE* |
| Dirección IP | *10.19.8.53* |
| Máscara de subred | *255.255.255.192* |
| Gateway predeterminado | *FE80::1* |
| Gateway predeterminado IPv6 | *FE80::1* |

Tabla 9. Configuración de red de PC-B

| **Configuración de red de PC-B** | |
|---|---|
| Descripción | ccna-b.net |
| Dirección física | *00D0.BC46.1AA9* |
| Dirección IP | *10.19.8.85* |
| Máscara de subred | *255.255.255.224* |
| Gateway predeterminado | FE80::1 |
| Gateway predeterminado IPv6 | FE80::1 |

Configuración de red de PC-A


Figura 7. Ilustración 2. Configuración de red de PC-A

Configuración de red de PC-B


Figura 8. Configuración de red de PC-B

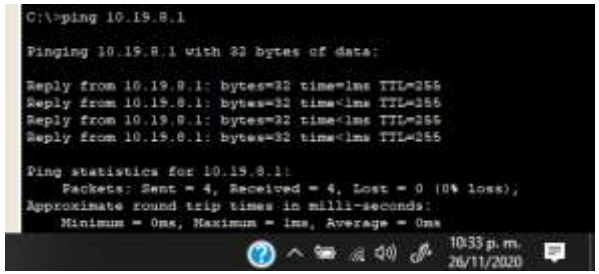
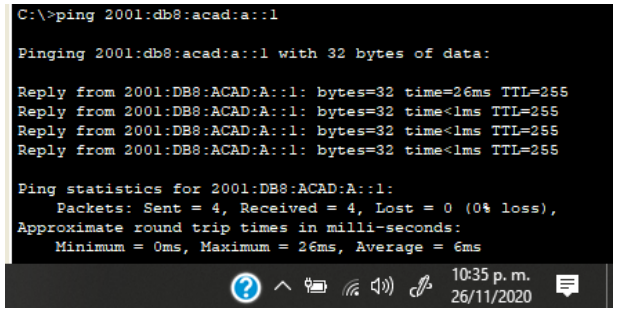
Probar y verificar la conectividad de extremo a extremo

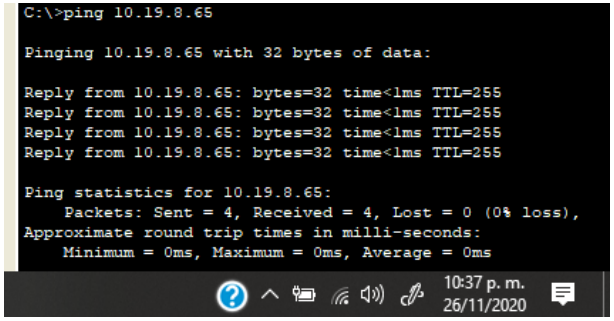
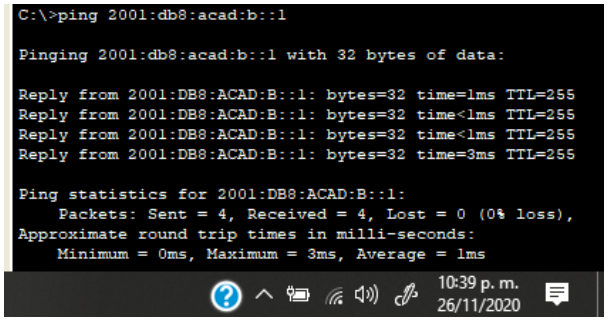
Use el comando ping para probar la conectividad IPv4 e IPv6 entre todos los dispositivos de red.

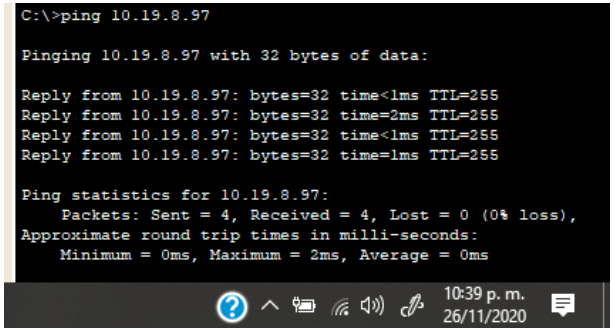
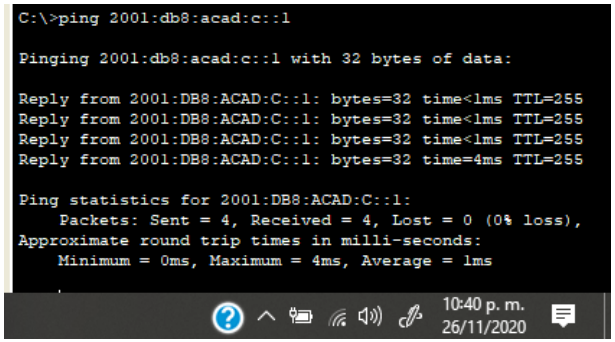
Nota: Si fallan los pings en las computadoras host, desactive temporalmente el firewall de la computadora y vuelva a realizar la prueba.

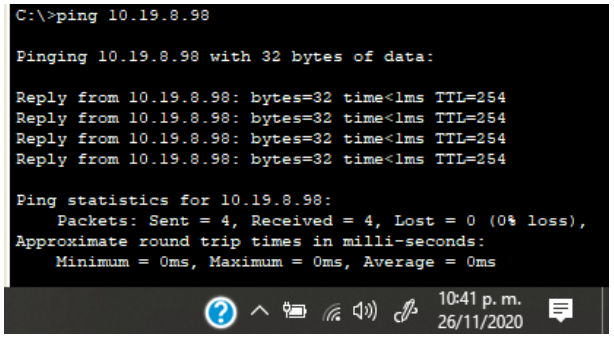
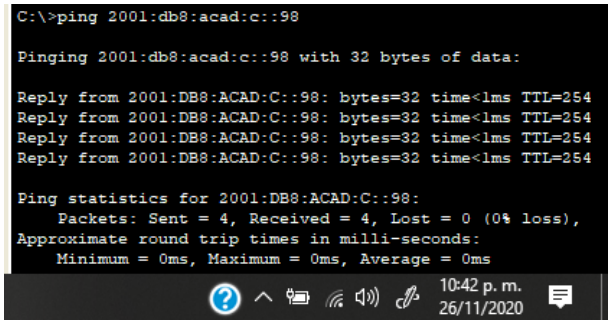
Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

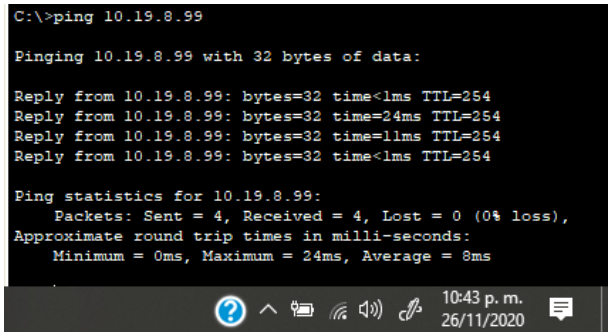
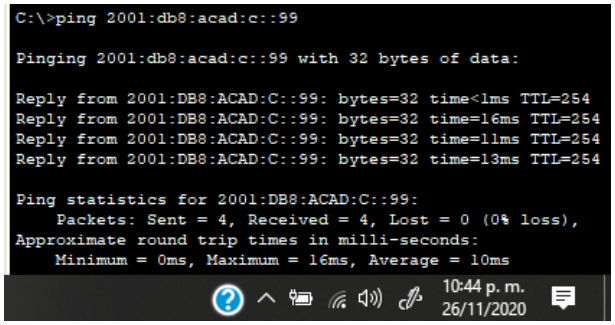
Tabla 10. Verificación de conectividad con cada dispositivo de red.

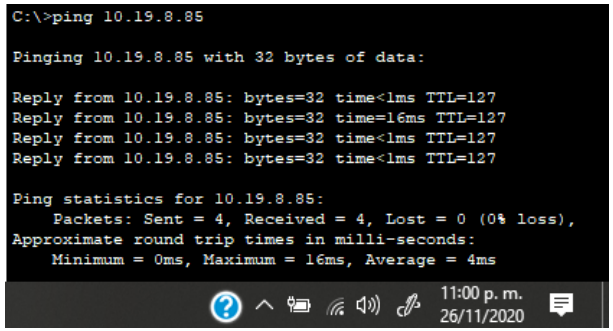
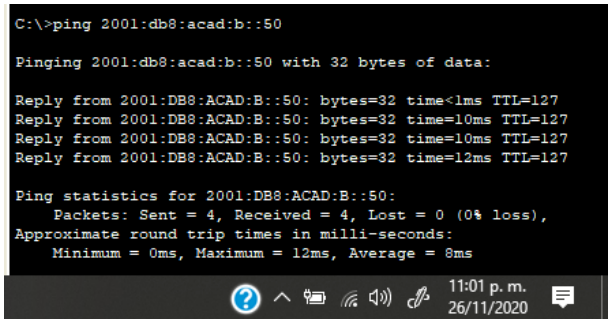
| Desde | A | de Internet | Dirección IP | Resultados de ping |
|---|---|---|---|---|
| PC-A | R1, G0/0/1.2 | Dirección | 10.19.8.1 |  <br>Figura 9. Ping desde PC-A a R1, G0/0/1.2 Dirección 10.19.8.1 |
| PC-A | R1, G0/0/1.2 | IPv6 | 2001:db8:acad:a: :1 |  <br>Figura 10. PING desde PC-A a R1, G0/0/1.2 IPv6 2001:db8:acad:a: :1 |

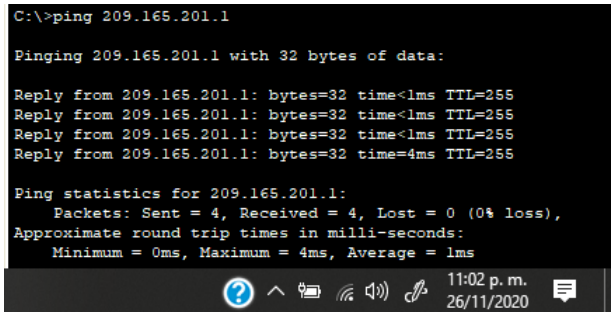
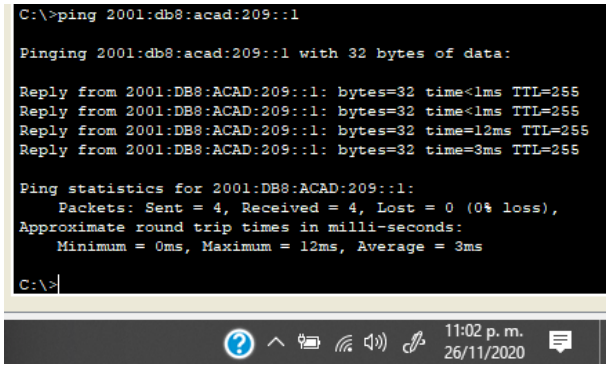
| Desde | A | de Internet | Dirección IP | Resultados de ping |
|---|---|---|---|---|
| PC-A | R1, G0/0/1.3 | Dirección | 10.19.8.65 |  <br>Figura 11. Ping desde PC-A a R1, G0/0/1.3 Dirección 10.19.8.65 |
| PC-A | R1, G0/0/1.3 | IPv6 | 2001:db8:acad:b: :1 |  <br>Figura 12. Ping desde PC-A a R1, G0/0/1.3 IPv6 2001:db8:acad:b: :1 |

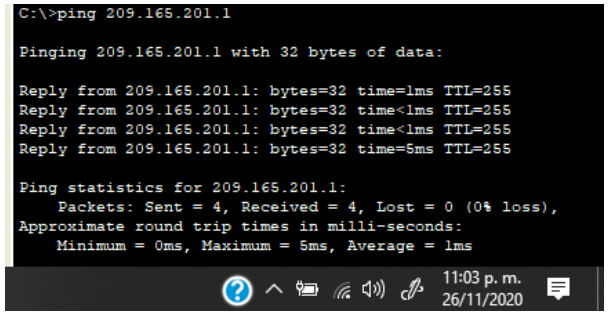
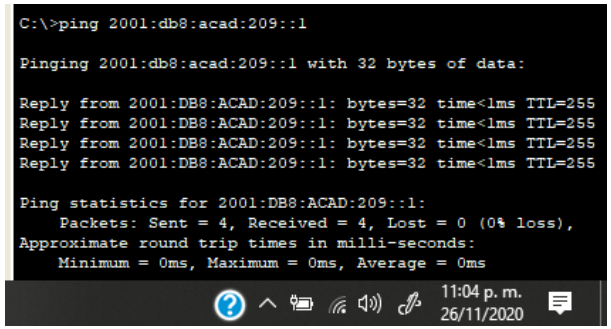
| Desde | A | de Internet | Dirección IP | Resultados de ping |
|---|---|---|---|---|
| PC-A | R1, G0/0/1.4 | Dirección | 10.19.8.97 |  <br>Figura 13. Ping desde PC-A a R1, G0/0/1.4 Dirección 10.19.8.97 |
| PC-A | R1, G0/0/1.4 | IPv6 | 2001:db8:acad:c: :1 |  <br>Figura 14. Ping desde PC-A a R1, G0/0/1.4 IPv6 2001:db8:acad:c: :1 |

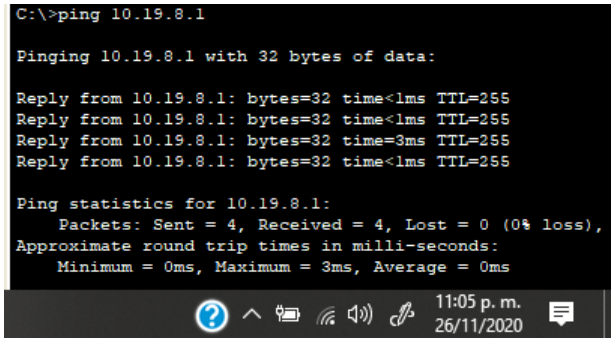
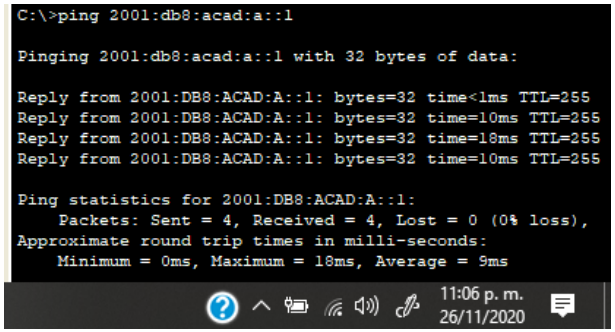
| Desde | A | de Internet | Dirección IP | Resultados de ping |
|---|---|---|---|---|
| PC-A | S1, VLAN 4 | Dirección | 10.19.8.98 |  <br>Figura 15. Ping desde PC-A a S1, VLAN 4 Dirección 10.19.8.98 |
| PC-A | S1, VLAN 4 | IPv6 | 2001:db8:acad:c: :98 |  <br>Figura 16. Ping desde PC-A a S1, VLAN 4 IPv6 2001:db8:acad:c: :98 |

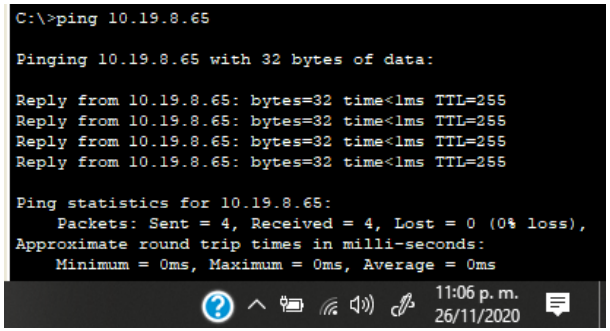
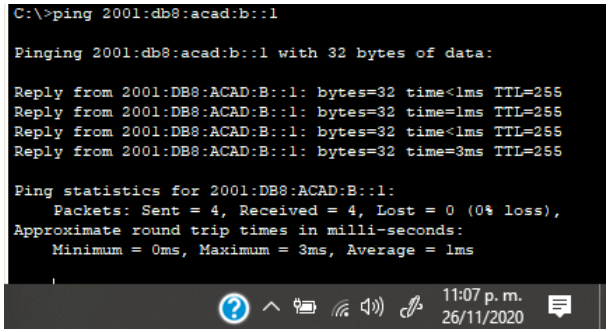
| Desde | A | de Internet | Dirección IP | Resultados de ping |
|---|---|---|---|---|
| PC-A | S2, VLAN 4 | Dirección | 10.19.8.99 |  <br>Figura 17. Ping desde PC-A a S2, VLAN 4 Dirección 10.19.8.99 |
| PC-A | S2, VLAN 4 | IPv6 | 2001:db8:acad:c: :99 |  <br>Figura 18. Ping desde PC-A a S2, VLAN 4 IPv6 2001:db8:acad:c: :99 |

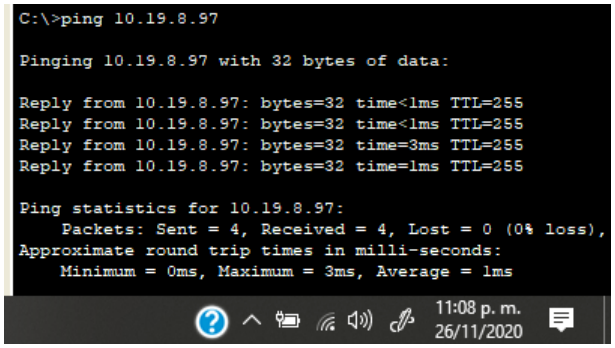
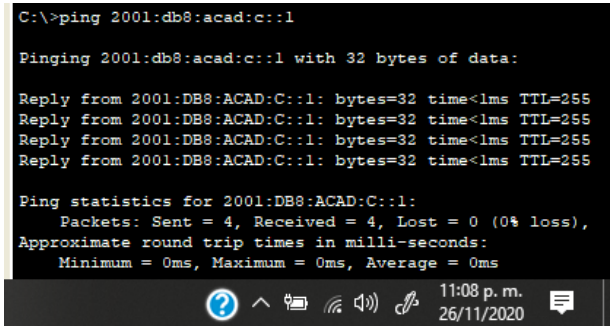
| Desde | A | de Internet | Dirección IP | Resultados de ping |
|---|---|---|---|---|
| PC-A | PC-B | Dirección | IP address will vary. |  <br>Figura 19. Ping desde PC-A a PC-B, Dirección IP address will vary. |
| PC-A | PC-B | IPv6 | 2001:db8:acad:b: :50 |  <br>Figura 20. Ping desde PC-A a PC-B, IPv6 2001:db8:acad:b: :50 |

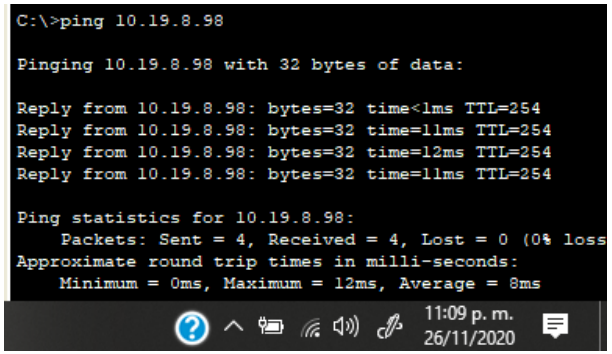
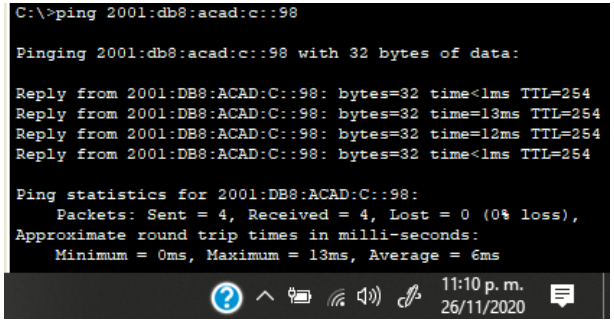
| Desde | A | de Internet | Dirección IP | Resultados de ping |
|---|---|---|---|---|
| PC-A | R1 Bucle 0 | Dirección | 209.165.201.1 |  <br>Figura 21. Ping desde PC-A a R1, Bucle 0 Dirección 209.165.201.1 |
| PC-A | R1 Bucle 0 | IPv6 | 2001:db8:acad:209: :1 |  <br>Figura 22. Ping desde PC-A a R1, Bucle 0 IPv6, 2001:db8:acad:209: :1 |

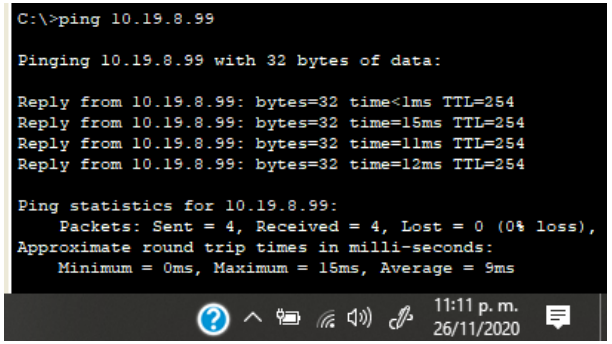
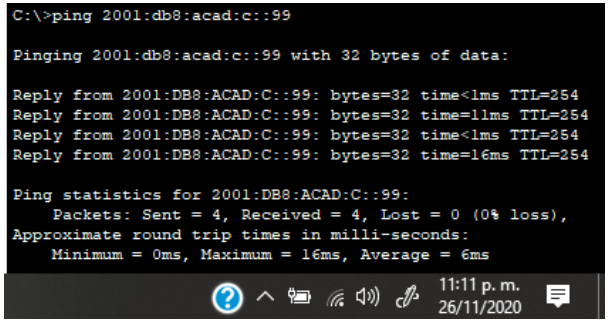
| Desde | A | de Internet | Dirección IP | Resultados de ping |
|---|---|---|---|---|
| PC-B | R1 Bucle 0 | Dirección | 209.165.201.1 |  <br>Figura 23. Ping desde PC-B a R1, Bucle 0 Dirección, 209.165.201.1 |
| PC-B | R1 Bucle 0 | IPv6 | 2001:db8:acad:209: :1 |  <br>Figura 24. Ping desde PC-B a R1, Bucle 0 IPv6 2001:db8:acad:209: :1 |

| Desde | A | de Internet | Dirección IP | Resultados de ping |
|---|---|---|---|---|
| PC-B | R1, G0/0/1.2 | Dirección | 10.19.8.1 |  <br>Figura 25. Ping desde PC-B a R1, G0/0/1.2 Dirección 10.19.8.1 |
| PC-B | R1, G0/0/1.2 | IPv6 | 2001:db8:acad:a: :1 |  <br>Figura 26. Ping desde PC-B a R1, G0/0/1.2 IPv6 2001:db8:acad:a: :1 |

| Desde | A | de Internet | Dirección IP | Resultados de ping |
|---|---|---|---|---|
| PC-B | R1, G0/0/1.3 | Dirección | 10.19.8.65 |  <br>Figura 27. Ping desde PC-B a R1, G0/0/1.3 Dirección 10.19.8.65 |
| PC-B | R1, G0/0/1.3 | IPv6 | 2001:db8:acad:b: :1 |  <br>Figura 28. Ping desde PC-B a R1, G0/0/1.3 IPv6 2001:db8:acad:b: :1 |

| Desde | A | de Internet | Dirección IP | Resultados de ping |
|---|---|---|---|---|
| PC-B | R1, G0/0/1.4 | Dirección | 10.19.8.97 |  <br>Figura 29. Ping desde PC-B a R1, G0/0/1.4 Dirección 10.19.8.97 |
| PC-B | R1, G0/0/1.4 | IPv6 | 2001:db8:acad:c: :1 |  <br>Figura 30. Ping desde PC-B a R1, G0/0/1.4 IPv6 2001:db8:acad:c: :1 |

| Desde | A | de Internet | Dirección IP | Resultados de ping |
|---|---|---|---|---|
| PC-B | S1, VLAN 4 | Dirección | 10.19.8.98 |  <br>Figura 31. Ping desde PC-B a S1, VLAN 4 Dirección 10.19.8.98 |
| PC-B | S1, VLAN 4 | IPv6 | 2001:db8:acad:c: :98 |  <br>Figura 32. Ping desde PC-B a S1, VLAN 4 IPv6 2001:db8:acad:c: :98 |

| Desde | A | de Internet | Dirección IP | Resultados de ping |
|---|---|---|---|---|
| PC-B | S2, VLAN 4 | Dirección | 10.19.8.99 |  <br>Figura 33. Ping desde PC-B a S2, VLAN 4 Dirección 10.19.8.99 |
| PC-B | S2, VLAN 4 | IPv6 | 2001:db8:acad:c: :99 |  <br>Figura 34. Ping desde PC-B a S2, VLAN 4 IPv6 2001:db8:acad:c: :99 |

Con el comando ping se procede a verificar la conectividad de extremo a extremo. Ping opera mediante el envío de paquetes de solicitud de eco del protocolo de mensajes de control de Internet (ICMP) al host de destino y la espera de una respuesta del ICMP. Puede registrar el tiempo de ida y vuelta y la pérdida de paquetes. Con resultado exitoso para cada una de las pruebas realizadas

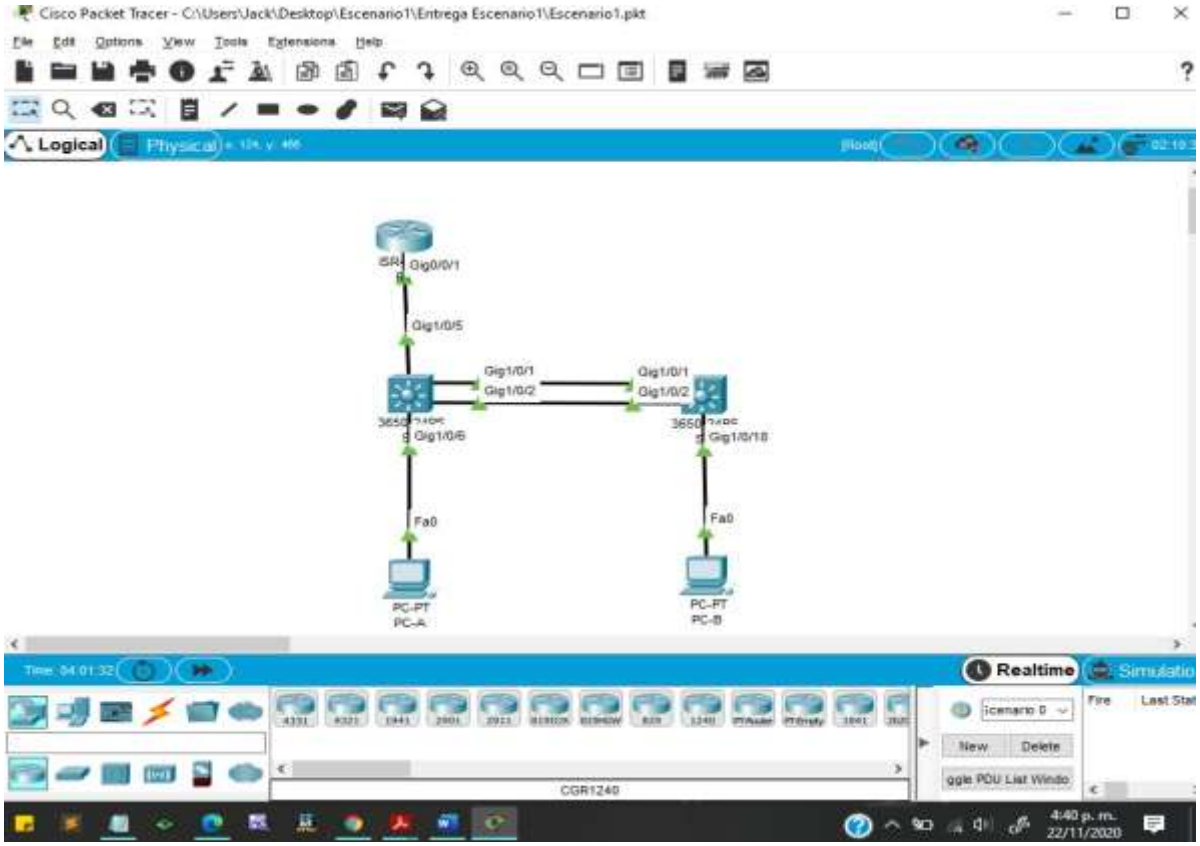



Figura 35. Red Escenario No 1 en funcionamiento.

Escenario 2

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

Topología

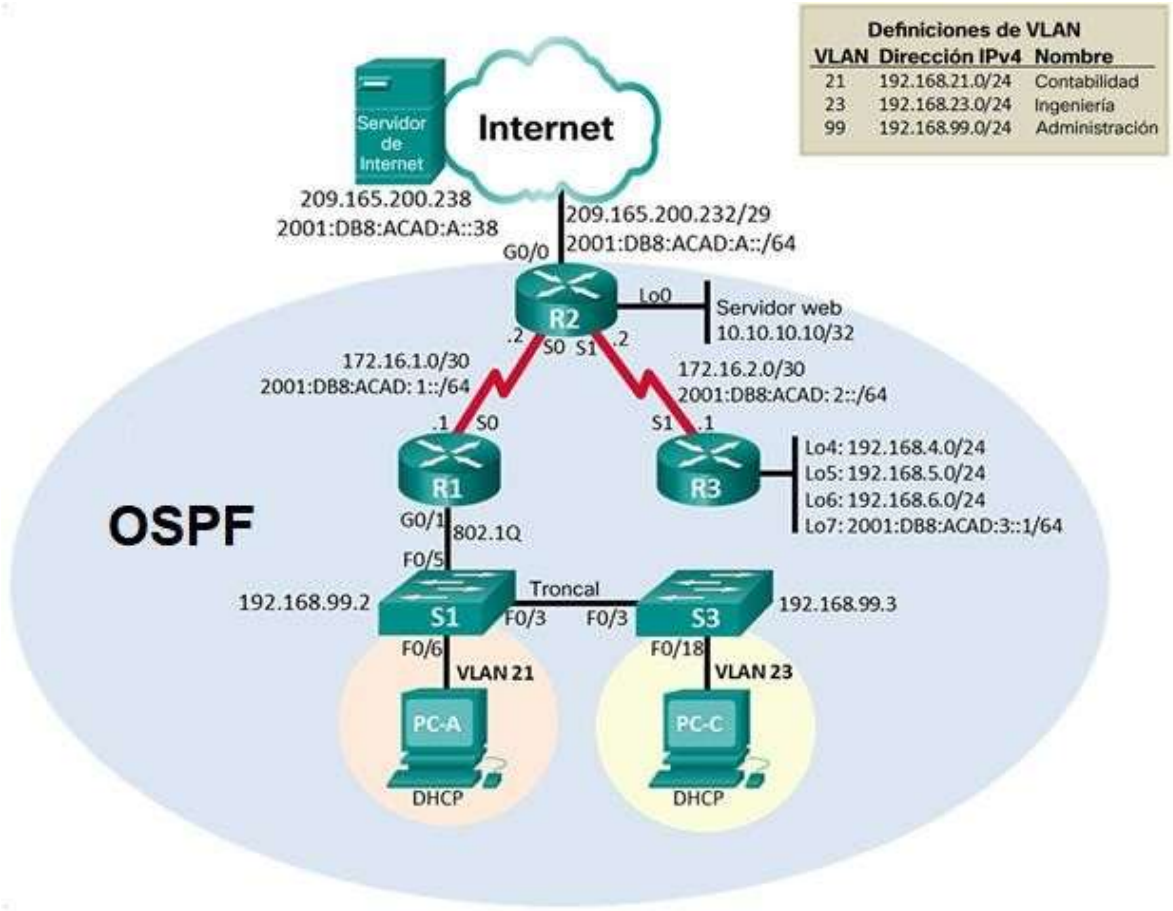



Figura 36. Topología Escenario 2

Parte 1: Inicializar dispositivos

Paso 1: Inicializar y volver a cargar los Routers y los Switches

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

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

Tabla 11. Configuración Routers y Switches

| Tarea | Comando de IOS |
|---|---|
| Eliminar el archivo startup-config de todos los Routers | Router#erase startup-config |
| Volver a cargar todos los Routers | Router#reload |
| Eliminar el archivo startup-config de todos los Switches y eliminar la base de datos de VLAN anterior | Switch#erase startup-config<br>Switch#delete vlan.dat |
| Volver a cargar ambos Switches | Switch#reload |
| Verificar que la base de datos de VLAN no esté en la memoria flash en ambos Switches | Switch#show flash<br>Directory of flash:/<br><br>1 -rw- 4414921 <no date> c2960-lanbase-mz.122-25.FX.bin<br><br>64016384 bytes total (59601463 bytes free)<br>Switch# |

Descripción: Con los comandos se evidencia la eliminación de todas las configuraciones que se cargaron en los dispositivos de fábrica y se reinician con el fin de evitar afectación por la antigua configuración.

Parte 2: Configurar los parámetros básicos de los dispositivos

Paso 1: Configurar la computadora de Internet

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

Tabla 12. Configuración de computadora 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:A::1 |

**Nota:** Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente en partes posteriores de esta práctica de laboratorio.

Descripción: En este paso se realiza la configuración de red para computadora de internet.

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 13. Configuración para R1

| Elemento o tarea de configuración | Especificación |
|---|---|
| Desactivar la búsqueda DNS | Router(config)#no ip domain-lookup |
| Nombre del router | R1<br>Router(config)#hostname R1 |
| Contraseña de exec privilegiado cifrada | class<br>R1(config)#enable secret class |
| Contraseña de acceso a la consola | cisco<br>R1(config-line)#password cisco |
| Contraseña de acceso Telnet | Cisco<br>R1(config-line)#password cisco |

| | |
|---|---|
| Cifrar las contraseñas de texto no cifrado | R1(config)#enable secret class<br>R1(config)#line console 0<br>R1(config-line)#passsword cisco<br>R1(config-line)#login<br>R1(config-line)#exit<br>R1(config-line)#line vty 0 15<br>R1(config-line)#password cisco<br>R1(config-line)#login<br>R1(config-line)#exit<br>R1(config-line)#service class<br>R1(config-line)#service password-encryption |
| Mensaje MOTD | Se prohibe el acceso no autorizado.<br>R1(config)#banner motd %Se prohbe el acceso no autorizado.% |

| | |
|---|---|
| Interfaz S0/0/0 | Establezca la descripción<br><br>R1(config-if)#description Connection to R2<br><br>Establecer la dirección IPv4 Consultar el diagrama de topología para conocer la información de direcciones<br><br>R1(config-if)#ip address 172.16.1.1 255.255.255.252<br><br>Establecer la dirección IPv6 Consultar el diagrama de topología para conocer la información de direcciones<br><br>R1(config-if)#ipv6 address 2001:db8:acad:1::1/64<br><br>Establecer la frecuencia de reloj en 128000<br><br>R1(config-if)#clock rate 128000<br>This command applies only to DCE interfaces<br>R1(config-if)#clock rate 128000<br>R1(config-if)#no shutdown<br><br>Activar la interfaz<br><br>R1(config-if)#no shutdown |
| Rutas predeterminadas | Configurar una ruta IPv4 predeterminada de S0/0/0<br><br>R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0<br><br>Configurar una ruta IPv6 predeterminada de S0/0/0<br><br>R1(config)#ipv6 route ::/0 s0/0/0<br>R1(config)# |

Nota: Todavía no configure G0/1.

Descripción: Se da nombre a el dispositivo, contraseña de acceso a la consola y acceso privilegiado, se incluyó un mensaje de inicio para configurar los parámetros básicos de seguridad de acceso y se cifran las contraseñas con el fin de aumentar la seguridad de estas.

Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Tabla 14. Configuración para R2

| **Elemento o tarea de configuración** | **Especificación** |
|---|---|
| Desactivar la búsqueda DNS | Router(config)#no ip domain-lookup |
| Nombre del router | R2<br>Router(config)#hostname R2 |
| Contraseña de exec privilegiado cifrada | Class<br>R2(config)#enable secret class |
| Contraseña de acceso a la consola | Cisco<br>R2(config-line)#password cisco |
| Contraseña de acceso Telnet | Cisco<br>R2(config-line)#password cisco |
| Cifrar las contraseñas de texto no cifrado | R2(config)#enable secret class<br>R2(config)#line console 0<br>R2(config-line)#passsword cisco<br>R2(config-line)#login<br>R2(config-line)#exit<br>R2(config-line)#line vty 0 15<br>R2(config-line)#password cisco<br>R2(config-line)#login<br>R2(config-line)#exit<br>R2(config-line)#service class<br>R2(config-line)#service password-encryption |

| | |
|---|---|
| Habilitar el servidor HTTP | R2(config)#ip http server<br>% Invalid input detected at '^' marker.<br><br>Packet Tracer no soporta este comando |
| Mensaje MOTD | Se prohibe el acceso no autorizado.<br><br>R2(config)#banner motd %Se prohibe el acceso no autorizado.% |
| Interfaz S0/0/0 | Establezca la descripción<br>R2(config)#int s0/0/0<br>R2(config-if)#description conection to R1<br><br>Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred.<br><br>R2(config-if)#ip address **172.16.1.2 255.255.255.252**<br><br>Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.<br><br>R2(config-if)#ipv6 address **2001:db8:acad:1::2/64**<br><br>Activar la interfaz<br><br>R2(config-if)#no shutdown |

| | |
|---|---|
| Interfaz S0/0/1 | Establecer la descripción<br>R2(config-if)#int s0/0/1<br>R2(config-if)#description Conection R3<br><br>Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.<br><br>R2(config-if)#ip address **172.16.2.2 255.255.255.252**<br><br>Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.<br><br>R2(config-if)#ipv6 address **2001:db8:acad:2::2/64**<br><br>Establecer la frecuencia de reloj en 128000.<br><br>R2(config-if)#clock rate 128000<br><br>Activar la interfaz<br>R2(config-if)#no shutdown |

| | |
|---|---|
| Interfaz G0/0 (simulación de Internet) | Establecer la descripción.<br>R2(config-if)#int g0/0<br>R2(config-if)#description Conection to Internet<br><br>Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.<br><br>R2(config-if)#ip address **209.165.200.233 255.255.255.248**<br><br>Establezca la dirección IPv6. Utilizar la primera dirección disponible en la subred.<br><br>R2(config-if)#ipv6 address **2001:db8:acad:a::1/64**<br><br>Activar la interfaz<br>R2(config-if)#no shutdown |
| Interfaz loopback 0 (servidor web simulado) | Establecer la descripción.<br><br>R2(config-if)#int loopback 0<br><br>R2(config-if)#description servidor web simulado<br><br>Establezca la dirección IPv4.<br><br>R2(config-if)#ip address **10.10.10.10 255.255.255.255** |
| Ruta predeterminada | Configure una ruta IPv4 predeterminada de G0/0.<br>R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0<br>R2(config)#ipv6 route ::/0 g0/0 |

Descripción: Se da nombre a el dispositivo, contraseña de acceso a la consola y acceso privilegiado, se incluyó un mensaje de inicio para configurar los parámetros básicos de seguridad de acceso y se cifran las contraseñas con el fin de aumentar la seguridad de estas.

Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Tabla 15. Configuración para R3

| **Elemento o tarea de configuración** | **Especificación** |
|---|---|
| Desactivar la búsqueda DNS | Router(config)#no ip domain-lookup |
| Nombre del router | R3<br>Router(config)#hostname R3 |
| Contraseña de exec privilegiado cifrada | Class<br>R3(config)#enable secret class |
| Contraseña de acceso a la consola | Cisco<br>R3(config-line)#password cisco |
| Contraseña de acceso Telnet | Cisco<br>R3(config-line)#password cisco |
| Cifrar las contraseñas de texto no cifrado | R3(config)#enable secret class<br>R3(config)#line console 0<br>R3(config-line)#passsword cisco<br>R3(config-line)#login<br>R3(config-line)#exit<br>R3(config-line)#line vty 0 15<br>R3(config-line)#password cisco<br>R3(config-line)#login<br>R3(config-line)#exit<br>R3(config-line)#service class<br>R3(config-line)#service password-encryption |
| Mensaje MOTD | Se prohibe el acceso no autorizado.<br><br>R3(config)#banner motd %Se prohIbe el acceso no autorizado.% |

| | |
|---|---|
| Interfaz S0/0/1 | Establecer la descripción<br><br>R3(config)#int s0/0/1<br>R3(config-if)#description Conection to R2<br><br>Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred.<br><br>R3(config-if)#ip address **172.16.2.1 255.255.255.252**<br><br>Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.<br><br>R3(config-if)#ipv6 address **2001:db8:acad:2::1/64**<br><br>Activar la interfaz<br><br>R3(config-if)#no shutdown |
| Interfaz loopback 4 | Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.<br><br>R3(config-if)#int loopback 4<br><br>R3(config-if)#ip address **192.168.4.1 255.255.255.0** |
| Interfaz loopback 5 | Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.<br><br>R3(config-if)#int loopback 5<br><br>R3(config-if)#ip address **192.168.5.1 255.255.255.0** |

| | |
|---|---|
| Interfaz loopback 6 | Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.<br><br>R3(config-if)#int loopback 6<br><br>R3(config-if)#ip address **192.168.6.1 255.255.255.0** |
| Interfaz loopback 7 | Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.<br><br>R3(config-if)#int loopback 7<br><br>R3(config-if)#ipv6 address **2001:db8:acad:3::1/64** |
| Rutas predeterminadas | Configure una ruta IPv4 predeterminada de S0/0/1.<br>R3(config-if)#exit<br>R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1<br><br>Configure una ruta IPv6 predeterminada de S0/0/1.<br>R3(config)#ipv6 route ::/0 s0/0/1 |

Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 16. Configuración para S1

| **Elemento o tarea de configuración** | **Especificación** |
|---|---|
| Desactivar la búsqueda DNS | Switch(config)#no ip domain-lookup |
| Nombre del switch | S1<br>Switch(config)#hostname S1 |

| | |
|---|---|
| Contraseña de exec privilegiado cifrada | Class<br>S1(config)#enable secret class |
| Contraseña de acceso a la consola | Cisco<br>S1(config-line)#password cisco |
| Contraseña de acceso Telnet | Cisco<br>S1(config-line)#password cisco |
| Cifrar las contraseñas de texto no cifrado | S1(config)#enable secret class<br>S1(config)#line console 0<br>S1(config-line)#passsword cisco<br>S1(config-line)#login<br>S1(config-line)#exit<br>S1(config-line)#line vty 0 15<br>S1(config-line)#password cisco<br>S1(config-line)#login<br>S1(config-line)#exit<br>S1(config-line)#service class<br>S1(config-line)#service password-encryption |
| Mensaje MOTD | Se prohíbe el acceso no autorizado.<br><br>S1(config)#banner motd %Se prohbe el acceso no autorizado.% |

Descripción: Se da nombre a el dispositivo, contraseña de acceso a la consola y acceso privilegiado, se incluyó un mensaje de inicio para configurar los parámetros básicos de seguridad de acceso y se cifran las contraseñas con el fin de aumentar la seguridad de estas.

Paso 6: Configurar S3

La configuración del S3 incluye las siguientes tareas:

Tabla 17. Configuración para S3

| Elemento o tarea de configuración | Especificación |
|---|---|
| Desactivar la búsqueda DNS | Switch#configure terminal<br>Switch(config)#no ip domain-lookup |
| Nombre del switch | S3<br>Switch(config)#hostname S3 |
| Contraseña de exec privilegiado cifrada | Class<br>S3(config)#enable secret class |
| Contraseña de acceso a la consola | Cisco<br>S3(config-line)#password cisco |
| Contraseña de acceso Telnet | Cisco<br>S3(config-line)#password cisco |
| Cifrar las contraseñas de texto no cifrado | S3(config)#enable secret class<br>S3(config)#line console 0<br>S3(config-line)#passsword cisco<br>S3(config-line)#login<br>S3(config-line)#exit<br>S3(config-line)#line vty 0 15<br>S3(config-line)#password cisco<br>S3(config-line)#login<br>S3(config-line)#exit<br>S3(config-line)#service class<br>S3(config-line)#service password-encryption |
| Mensaje MOTD | Se prohíbe el acceso no autorizado.<br>S3(config)#banner motd %Se prohbe el acceso no autorizado.% |

Paso 7: Verificar la conectividad de la red

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

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

Tabla 18. Conectividad de los dispositivos de red.

| Desde | A | Dirección IP | Resultados de ping |
|---|---|---|---|
| R1 | R2, S0/0/0 | 172.16.1.2 | R1#ping 172.16.1.2<br>Exitoso |
| R2 | R3, S0/0/1 | 172.16.2.1 | R2#ping 172.16.2.1<br>Exitoso |
| PC de Internet | Gateway predeterminado | 209.165.200.233 | C:\>ping 209.165.200.233<br>Exitoso |

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

Descripción: Con la ejecución de estas pruebas se puede verificar que la configuración fue correcta y se tienen intercambio de paquetes entre los dispositivos.

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

Paso 1: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 19. Configurar la seguridad del Switch, las VLAN y el Routing entre VLAN en S1

| Elemento o tarea de configuración | Especificación |
|---|---|
| Crear la base de datos de VLAN | Utilizar la tabla de equivalencias de VLAN para topología para crear y nombrar cada una de las VLAN que se indican<br><br>S1(config)#vlan 21<br>S1(config-vlan)#name CONTABILIDAD<br>S1(config-vlan)#vlan 23<br>S1(config-vlan)#name INGENIERIA<br>S1(config-vlan)#vlan 99<br>S1(config-vlan)#name ADMINISTRACION<br>S1(config-vlan)# |

| | |
|---|---|
| Asignar la dirección IP de administración. | Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S1 en el diagrama de topología<br><br>S1(config)#int vlan 99<br>S1(config-if)#ip address 192.168.99.2 255.255.255.0<br>S1(config-if)#no shutdown |
| Asignar el gateway predeterminado | Asigne la primera dirección IPv4 de la subred como el gateway predeterminado.<br><br>S1(config)#ip default-gateway 192.168.99.1 |
| Forzar el enlace troncal en la interfaz F0/3 | Utilizar la red VLAN 1 como VLAN nativa<br><br>S1(config)#int f0/3<br>S1(config-if)#switchport mode trunk |
| Forzar el enlace troncal en la interfaz F0/5 | Utilizar la red VLAN 1 como VLAN nativa<br><br>S1(config-if)#int f0/5<br>S1(config-if)#switchport mode trunk<br>S1(config-if)#switchport trunk native vlan 1 |
| Configurar el resto de los puertos como puertos de acceso | Utilizar el comando interface range<br><br>S1(config-if)#int range f0/1-2, f0/4, f0/6-24, g0/1-2<br>S1(config-if-range)#switchport mode access |
| Asignar F0/6 a la VLAN 21 | S1(config-if-range)#int f0/6<br>S1(config-if)#switchport access vlan 21 |
| Apagar todos los puertos sin usar | S1(config-if)#int range f0/1-2, f0/4, f0/7-24, g0/1-2<br>S1(config-if-range)#shutdown |

Descripción: Se realiza creación de las Vlan 21, 23 y 99. Se establece comunicación entre los Switch de modo troncal con el fin de manejar el tráfico entre las Vlan.

Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 20. Configuración en S3

| **Elemento o tarea de configuración** | **Especificación** |
|---|---|
| Crear la base de datos de VLAN | Utilizar la tabla de equivalencias de VLAN para topología para crear cada una de las VLAN que se indican Dé nombre a cada VLAN.<br>S3(config)#vlan 21<br>S3(config-vlan)# name CONTABILIDAD<br>S3(config-vlan)#vlan 23<br>S3(config-vlan)#name INGENIERIA<br>S3(config-vlan)#vlan 99<br>S3(config-vlan)#name ADMINISTRACION<br>S3(config-vlan)# |
| Asignar la dirección IP de administración | Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S3 en el diagrama de topología<br><br>S3(config)#int vlan 99<br>S3(config-if)#ip address 192.168.99.3 255.255.255.0<br>S3(config-if)#no shutdown |
| Asignar el gateway predeterminado. | Asignar la primera dirección IP en la subred como gateway predeterminado.<br><br>S3(config)#ip default-gateway 192.168.99.1 |
| Forzar el enlace troncal en la interfaz F0/3 | Utilizar la red VLAN 1 como VLAN nativa<br><br>S3(config)#int f0/3<br>S3(config-if)#switchport mode trunk<br>S3(config-if)#switchport trunk native vlan 1 |

| | |
|---|---|
| Configurar el resto de los puertos como puertos de acceso | Utilizar el comando interface range<br><br>S3(config-if)#int range f0/1-2, f0/4-24, g0/1-2<br>S3(config-if-range)#switchport mode access |
| Asignar F0/18 a la VLAN 23 | S3(config-if-range)#int f0/18<br>S3(config-if)#switchport access vlan 23 |
| Apagar todos los puertos sin usar | S3(config-if)#int range f0/1-2, f0/4-17, f0/19-24, g0/1-2<br>S3(config-if-range)#shutdown |

Descripción: Se realiza creación de las Vlan 21, 23 y 99. Se establece comunicación entre los Switch de modo troncal con el fin de manejar el tráfico entre las Vlan.

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 21. Configuración en R1

| **Elemento o tarea de configuración** | **Especificación** |
|---|---|
| Configurar la subinterfaz 802.1Q .21 en G0/1 | Descripción: VLAN 21<br><br>R1(config)#int g0/1.21<br>R1(config-subif)#description VLAN 21<br><br>Asignar la primera dirección disponible a esta interfaz<br><br>R1(config-subif)#encapsulation dot1q 21<br>R1(config-subif)#ip address **192.168.21.1 255.255.255.0** |

| | |
|---|---|
| Configurar la subinterfaz 802.1Q .23 en G0/1 | Descripción: VLAN 23<br><br>R1(config-subif)#int g0/1.23<br>R1(config-subif)#description VLAN 23<br><br>Asignar la primera dirección disponible a esta interfaz<br><br>R1(config-subif)#encapsulation dot1q 23<br>R1(config-subif)#ip address **192.168.23.1 255.255.255.0** |
| Configurar la subinterfaz 802.1Q .99 en G0/1 | Descripción: VLAN 99<br>R1(config-subif)#description VLAN 99<br>R1(config-subif)#encapsulation dot1q 99<br><br>Asignar la primera dirección disponible a esta interfaz<br>R1(config-subif)#ip address **192.168.99.1 255.255.255.0** |
| Activar la interfaz G0/1 | R1(config-subif)#int g0/1<br>R1(config-if)#no shutdown |

Descripción: Se realiza creación de las Vlan 21, 23 y 99. Se establece comunicación entre los Switch de modo troncal con el fin de manejar el tráfico entre las Vlan.

Paso 4: Verificar la conectividad de la red

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

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

Tabla 22. Verificación de conectividad de la red.

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

Descripción: La verificación de conectividad permitió verificar la correcta configuración de tráfico entre las Vlan.

Parte 4: Configurar el protocolo de routing dinámico OSPF

Paso 1: Configurar OSPF en el R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 23. Configuración de protocolo de routing dinámico OSPF.

| Elemento o tarea de configuración | Especificación |
|---|---|
| Configurar OSPF área 0 | R1(config)#router ospf 1 |
| Anunciar las redes conectadas directamente | Asigne todas las redes conectadas directamente.<br><br>R1(config)#router ospf 1<br>R1(config-router)#network 172.16.1.0 0.0.0.3 area 0<br>R1(config-router)#network 192.168.21.1 0.0.0.255 area 0<br>R1(config-router)#network 192.168.23.1 0.0.0.255 area 0<br>R1(config-router)#network 192.168.99.1 0.0.0.255 area 0 |

| | |
|---|---|
| Establecer todas las interfaces LAN como pasivas | R1(config-router)#passive-interface g0/1.21<br>R1(config-router)#passive-interface g0/1.23<br>R1(config-router)#passive-interface g0/1.99 |
| Desactive la sumarización automática | No está habilitado en Packet Tracer esta función |

Descripción: Se configura el protocolo OSPF con el fin de optimizar la comunicación entre Routers, ya 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 configuran con una máscara wildcard y no con una máscara de subred. La máscara wildcard representa las direcciones de enlaces o de host que pueden estar presentes.

Paso 2: Configurar OSPF en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla 24. Configuración OSPF en el R2

| **Elemento o tarea de configuración** | **Especificación** |
|---|---|
| Configurar OSPF área 0 | R2(config)#ipv6 unicast-routing<br>R2(config)#ipv6 router ospf 1<br>R2(config-rtr)#router-id 2.2.2.2 |

| | |
|---|---|
| Anunciar las redes conectadas directamente | **Nota:** Omitir la red G0/0.<br><br>R2(config)#int s0/0/0<br>R2(config-if)#ipv6 address 2001:db8:acad:1::2/64<br>R2(config-if)#ipv6 ospf 1 area 0<br>R2(config-if)#<br>06:17:07: %OSPFv3-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/0 from LOADING to FULL, Loading Done<br><br>R2(config-if)#no shutdown<br>R2(config-if)#exit<br>R2(config)#router ospf 1<br>R2(config-router)#network 172.16.1.0<br>R2(config-router)#network 172.16.1.0 0.0.0.3 area 0<br>R2(config-router)#<br>R2(config-router)#network 172.16.2.0 0.0.0.3 area 0<br>R2(config-router)#exit<br>R2(config)#ipv6 router ospf 1<br>R2(config-rtr)#int s0/0/1<br>R2(config-if)#ipv6 address 2001:db8:acad:2::2/64<br>R2(config-if)#ipv6 ospf 1 area 0<br>R2(config-if)#no shutdown<br>R2(config-if)# |
| Establecer la interfaz LAN (loopback) como pasiva | R2(config)#router ospf 1<br>R2(config-router)#passive-interface lo0 |
| Desactive la sumarización automática. | No está habilitado en Packet Tracer esta función |

Descripción: Se configura el protocolo OSPF con el fin de optimizar la comunicación entre Routers, ya 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 configuran con una máscara wildcard y no con una máscara de subred. La máscara wildcard representa las direcciones de enlaces o de host que pueden estar presentes.

Paso 3: Configurar OSPFv3 en el R2

La configuración del R3 incluye las siguientes tareas:

Tabla 25. Configuración OSPFv3 en el R2

| Elemento o tarea de configuración | Especificación |
|---|---|
| Configurar OSPF área 0 | R3(config)#router ospf 1<br>R3(config-rtr)#router-id 3.3.3.3<br>R3(config-router)#do show ip route connected |
| Anunciar redes IPv4 conectadas directamente | R3(config-router)#do show ip route connected<br>C 172.16.2.0/30 is directly connected, Serial0/0/1<br>C 192.168.4.0/24 is directly connected, Loopback4<br>C 192.168.5.0/24 is directly connected, Loopback5<br>C 192.168.6.0/24 is directly connected, Loopback6<br><br>R3(config-router)#network 172.16.2.0 0.0.0.3 area 0<br>R3(config-router)#network 172.16.2.0 0.0.0.3 area 0<br>03:58:23: %OSPF-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Serial0/0/1 fr<br>R3(config-router)#network 192.168.4.0 0.0.0.255 area 0<br>R3(config-router)#network 192.168.5.0 0.0.0.255 area 0<br>R3(config-router)#network 192.168.6.0 0.0.0.255 area 0 |
| Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas | R3(config-router)#passive-interface loopback 4<br>R3(config-router)#passive-interface loopback 5<br>R3(config-router)#passive-interface loopback 6 |

| | |
|---|---|
| Desactive la sumarización automática. | No está habilitado en Packet Tracer esta función |

Descripción: Se configura el protocolo OSPF con el fin de optimizar la comunicación entre Routers, ya 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 configuran con una máscara wildcard.

Paso 4: Verificar la información de OSPF

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

Tabla 26. Verificación de información de OSPF

| Pregunta | Respuesta |
|---|---|
| ¿Con qué comando se muestran la ID del proceso OSPF, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router? | Show ip route<br>Show ip ospf database<br>Show ip protocol |
| ¿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 \| section router ospf |

Descripción: Se verifica el protocolo OSPF mediante comandos en cada Router.

Parte 5: Implementar DHCP y NAT para IPv4

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

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 27. Implementación DHCP y NAT para IPv4 en R1.

| Elemento o tarea de configuración | Especificación |
|---|---|
| Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas | R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20 |

| | |
|---|---|
| Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas | R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20 |
| Crear un pool de DHCP para la VLAN 21. | **Nombre: ACCT**<br>R1(config)#ip dhcp pool ACCT<br>R1(dhcp-config)#network 192.168.21.0 255.255.255.0<br><br>**Servidor DNS: 10.10.10.10**<br>R1(dhcp-config)#dns-server 10.10.10.10<br><br>**Nombre de dominio: ccna-sa.com**<br>R1(dhcp-config)#domain-name ccna-sa.com<br><br>**Establecer el gateway predeterminado**<br>R1(dhcp-config)#default-router 192.168.21.1 |
| Crear un pool de DHCP para la VLAN 23 | Nombre: ENGNR<br>R1(dhcp-config)#ip dhcp pool ENGNR<br>R1(dhcp-config)#network 192.168.23.0 255.255.255.0<br><br>Servidor DNS: 10.10.10.10<br>R1(dhcp-config)#dns-server 10.10.10.10<br><br>Nombre de dominio: ccna-sa.com<br>R1(dhcp-config)#domain-name ccna-sa.com<br><br>Establecer el gateway predeterminado<br>R1(dhcp-config)#default-router 192.168.23.1 |

Descripción: Se configuran las VLAN estáticas en reserva, además se crea un poll de DHCP y NAT para cada VLAN.

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

La configuración del R2 incluye las siguientes tareas:

Tabla 28. Configuración de NAT estática y dinámica en el R2.

| **Elemento o tarea de configuración** | **Especificación** |
|---|---|
| Crear una base de datos local con una cuenta de usuario | Nombre de usuario: **webuser**<br><br>Contraseña: **cisco12345**<br><br>Nivel de privilegio: **15**<br><br>R2(config)#username webuser privilege 15 secret cisco12345 |
| Habilitar el servicio del servidor HTTP | R2(config)#ip http server<br>^<br>% Invalid input detected at '^' marker.<br><br>Packet Tracer no soporta este comando |
| Configurar el servidor HTTP para utilizar la base de datos local para la autenticación | R2(config)#ip http authentication local<br>^<br>% Invalid input detected at '^' marker.<br><br>Packet Tracer no soporta este comando |
| Crear una NAT estática al servidor web. | Dirección global interna: **209.165.200.229**<br>**Cambiamos por 209.165.200.237**<br><br>R2(config)#ip nat inside source static 10.10.10.10 209.165.200.237<br>R2(config)#int g0/0<br>R2(config-if)#ip nat outside<br>R2(config-if)#int s0/0/0<br>R2(config-if)#ip nat inside<br>R2(config-if)#int s0/0/1<br>R2(config-if)#ip nat inside |
| Asignar la interfaz interna y externa para la NAT estática | |

| | |
|---|---|
| Configurar la NAT dinámica dentro de una ACL privada | **Lista de acceso: 1**<br>**Permitir la traducción de las redes de Contabilidad y de Ingeniería en el R1**<br><br>R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255<br>R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255<br><br>**Permitir la traducción de un resumen de las redes LAN (loopback) en el R3**<br><br>R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255 |
| Defina el pool de direcciones IP públicas utilizables. | Nombre del conjunto: **INTERNET**<br>R2(config)#ip nat pool INTERNET<br><br>El conjunto de direcciones incluye:<br>**209.165.200.225** – **209.165.200.228**<br><br>R2(config)#ip nat pool INTERNET 209.165.200.233 209.165.200.236 netmask 255.255.255.248 |
| Definir la traducción de NAT dinámica | R2(config)#ip nat inside source list 1 pool INTERNET |

Descripción: Se configuran las VLAN estáticas en reserva, además se crea un poll de DHCP y NAT para cada VLAN.

Paso 3: Verificar el protocolo DHCP y la NAT estática

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

Tabla 29. Verificación protocolo DHCP y la NAT estática.

| Prueba | Resultados |
|---|---|
| Verificar que la PC-A haya adquirido información de IP del servidor de DHCP | Exitoso |
| Verificar que la PC-C haya adquirido información de IP del servidor de DHCP | Exitoso |
| Verificar que la PC-A pueda hacer ping a la PC-C<br>**Nota:** Quizá sea necesario deshabilitar el firewall de la PC. | Exitoso |
| Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.229) Iniciar sesión con el nombre de usuario **webuser** y la contraseña **cisco12345** | Packet Tracer no soporta este comando o este procedimiento. No se puede activar el Servidor Web en R2 |

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

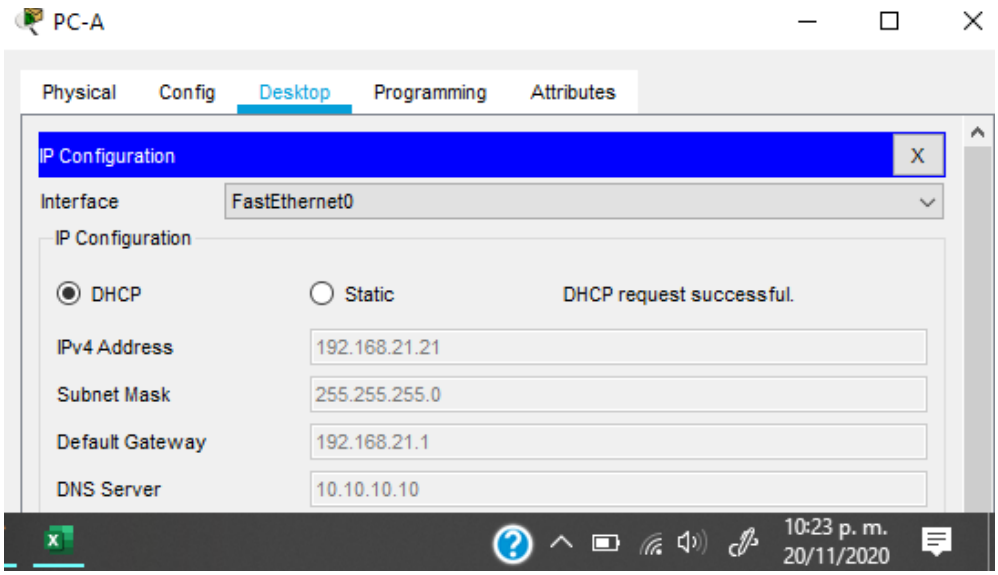



Figura 37. PC-A adquirido información de IP del servidor de DHCP

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

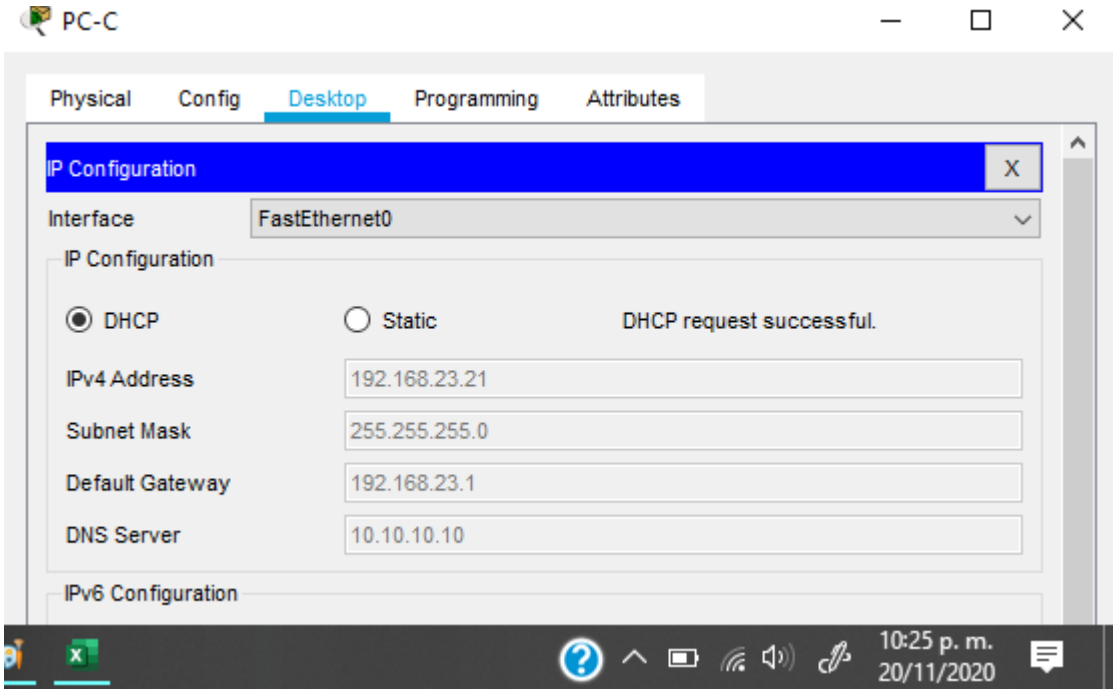



Figura 38. PC-C adquirido información de IP del servidor de DHCP

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

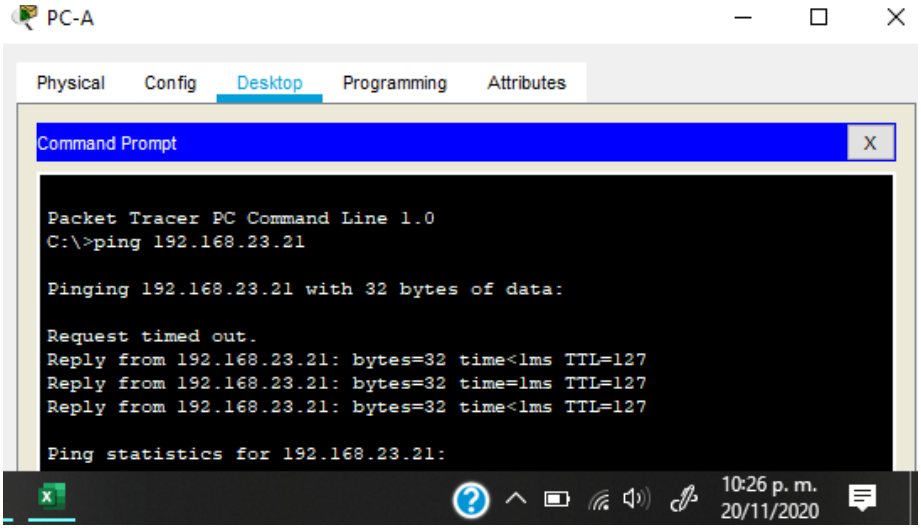



Figura 39. Verificar que la PC-A pueda hacer ping a la PC-C

Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.237) Iniciar sesión con el nombre de usuario **webuser** y la contraseña **cisco12345**

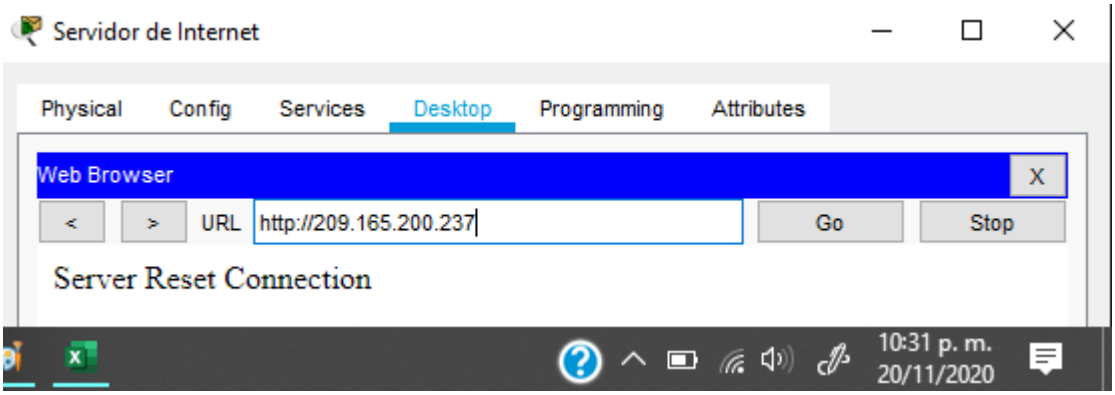



Figura 40. Utilizar un navegador web en la computadora de Internet

Parte 6: Configurar NTP

Tabla 30. Configuración NTP.

| Elemento o tarea de configuración | Especificación |
|---|---|
| Ajuste la fecha y hora en R2. | **5 de marzo de 2016, 9 a. m.**<br><br>R2#clock set 09:00:00 05 march 2016 |
| Configure R2 como un maestro NTP. | Nivel de estrato: **5**<br>R2(config)#ntp master 5 |
| Configurar R1 como un cliente NTP. | Servidor: **R2**<br><br>R1(config)#ntp server 172.16.1.2 |
| Configure R1 para actualizaciones de calendario periódicas con hora NTP. | R1(config)#ntp update-calendar |

| | |
|---|---|
| Verifique la configuración de NTP en R1. | R1#show ntp associations<br><br>address ref clock st when poll reach delay offset disp<br>*~172.16.1.2 127.127.1.1 5 5 16 17 6.00 -1.00 0.12<br>* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured |

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

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

Tabla 31. Restricción de acceso a las líneas VTY en el R2.

| Elemento o tarea de configuración | Especificación |
|---|---|
| Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2 | Nombre de la ACL: **ADMIN-MGT**<br><br>R2(config)#ip access-list standard ADMIN-MGT<br>R2(config-std-nacl)#permit host 172.16.1.1 |
| Aplicar la ACL con nombre a las líneas VTY | R2(config-line)#access-class ADMIN-MGT in |
| Permitir acceso por Telnet a las líneas de VTY | R2(config-line)#transport input telnet |
| Verificar que la ACL funcione como se espera | R1#telnet 172.16.1.2<br>Trying 172.16.1.2 ...Open Se prohibe el acceso no autorizado.<br><br>User Access Verification<br><br>Password: cisco<br>R2>enable<br>Password: class |

Verificar que la ACL funcione como se espera

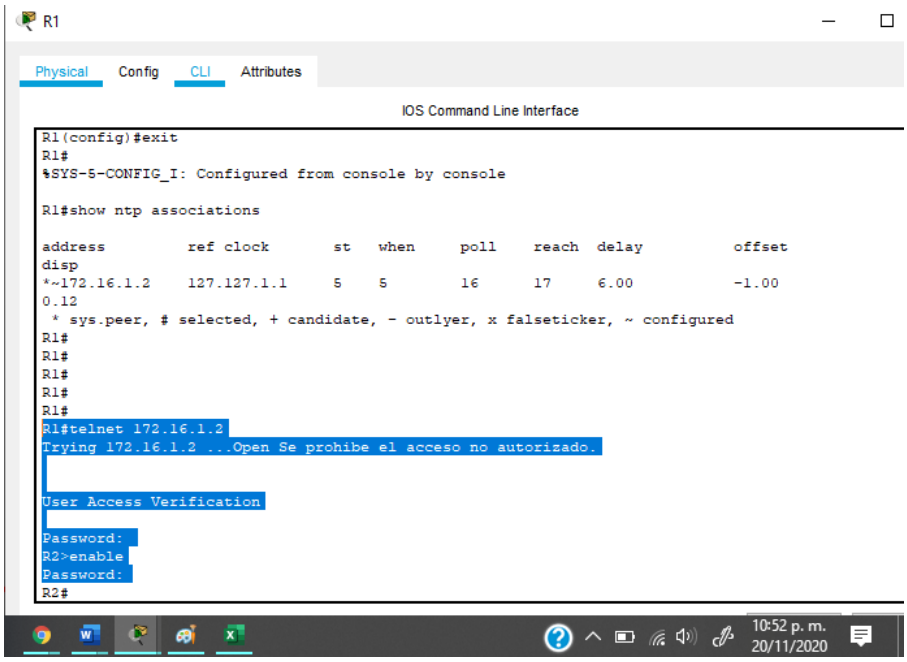



Figura 41. Verificación de la ACL funcione.

Conexión rechazada por el host remoto

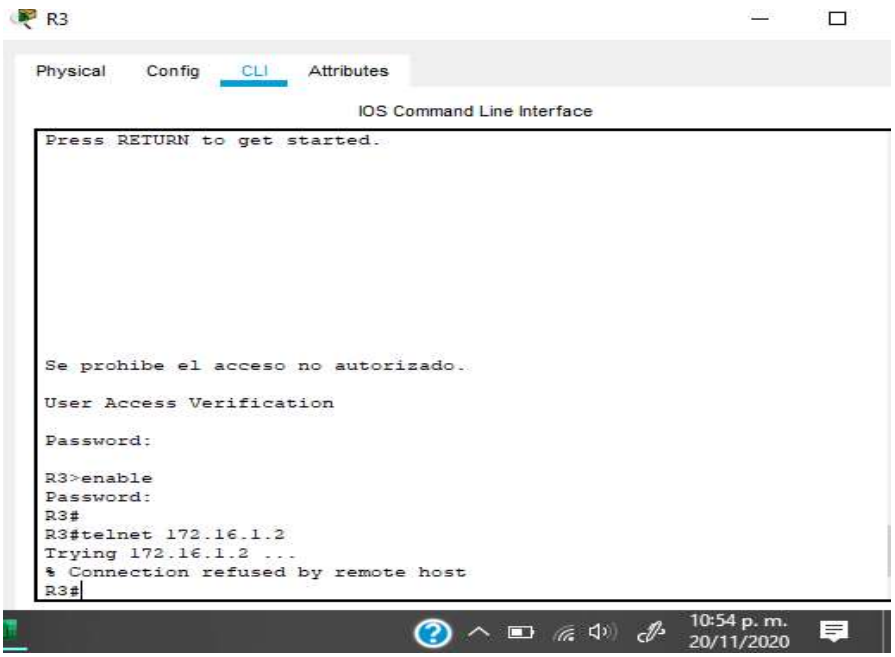



Figura 42. Ilustración 10. Conexión rechazada por el host remoto.

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

Tabla 32. Introducir el comando de CLI adecuado.

| 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**<br>Standard IP access list 1<br>10 permit 192.168.21.0 0.0.0.255<br>20 permit 192.168.23.0 0.0.0.255<br>30 permit 192.168.4.0 0.0.3.255<br>Standard IP access list ADMIN-MGT<br>10 permit host 172.16.1.1 (2 match(es))<br><br>R2#**show ip access-list**<br>Standard IP access list 1<br>10 permit 192.168.21.0 0.0.0.255<br>20 permit 192.168.23.0 0.0.0.255<br>30 permit 192.168.4.0 0.0.3.255<br>Standard IP access list ADMIN-MGT<br>10 permit host 172.16.1.1 (2 match(es)) |
| Restablecer los contadores de una lista de acceso | R2#clear ip access-list counters<br>^<br>% Invalid input detected at '^' marker.<br>R2#clear ip access-list ?<br>% Unrecognized command<br>R2#clear ip ?<br>bgp Clear BGP connections<br>dhcp Delete items from the DHCP database<br>nat Clear NAT<br>ospf OSPF clear commands<br>route Delete route table entries<br>R2#clear ip<br><br>Packet Tracer no soporta este comando |

| | |
|---|---|
| ¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica? | **R2#show ip interface**<br><br>**R2#show ip interface**<br>**GigabitEthernet0/0** is up, line protocol is up (connected)<br>Internet address is 209.165.200.233/29<br>Broadcast address is 255.255.255.255<br>Address determined by setup command<br>MTU is 1500 bytes<br>Helper address is not set<br>**Directed broadcast forwarding is disabled**<br>**Outgoing access list is not set**<br>**Inbound access list is not set** |
| ¿Con qué comando se muestran las traducciones NAT? | **Nota:** Las traducciones para la PC-A y la PC-C se agregaron a la tabla cuando la computadora de Internet intentó hacer ping a esos equipos en egl paso 2. Si hace ping a la computadora de Internet desde la PC-A o la PC-C, no se agregarán las traducciones a la tabla debido al modo de simulación de Internet en la red.<br><br>**R2#show ip nat translations**<br>Pro Inside global Inside local Outside local Outside global<br>--- 209.165.200.237 10.10.10.10 --- ---<br>tcp 209.165.200.237:80 10.10.10.10:80 209.165.200.238:1025209.165.200.238:1025 |
| ¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas? | |

Si hace ping a la computadora de Internet desde la PC-A o la PC-C

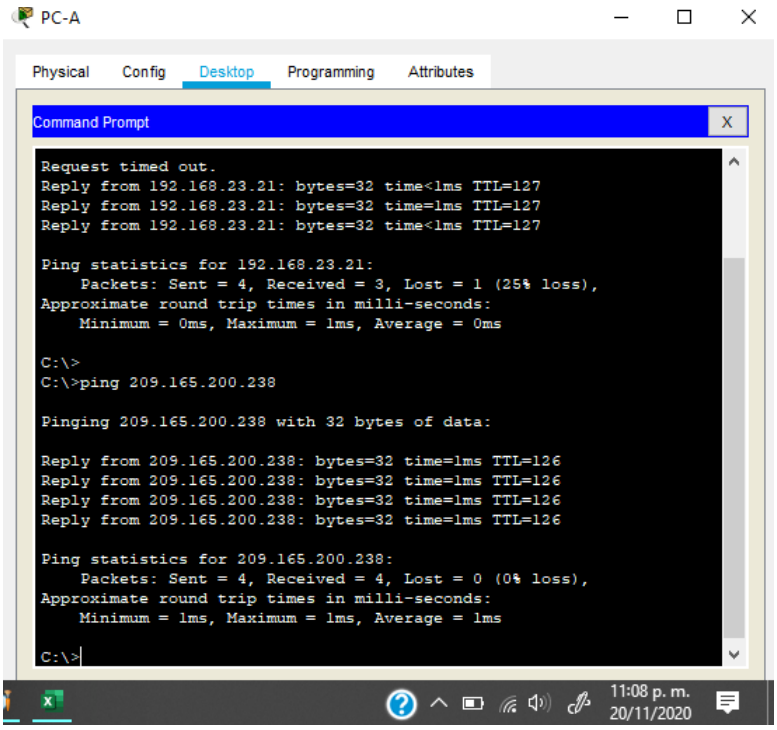



Figura 43. Realizar ping a la computadora de Internet desde la PC-A

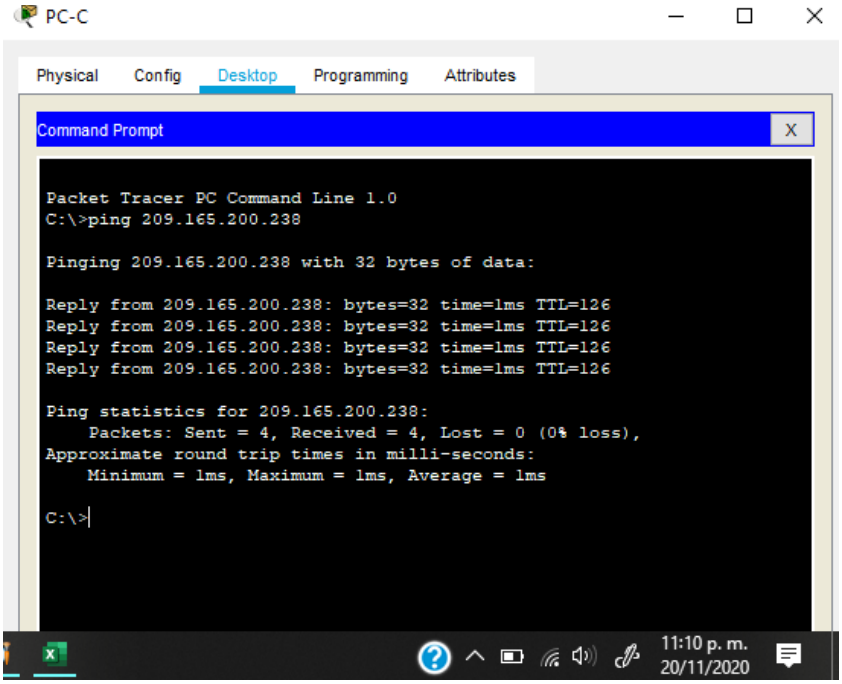



Figura 44. Realizar ping a la computadora de Internet desde la PC-C

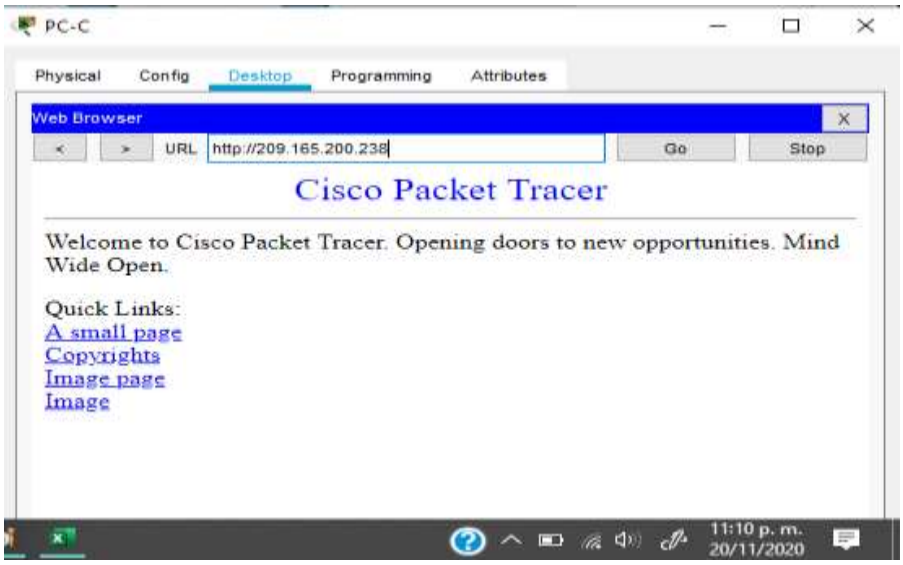



Figura 45. Conexión realizada con éxito desde PC-C a Internet

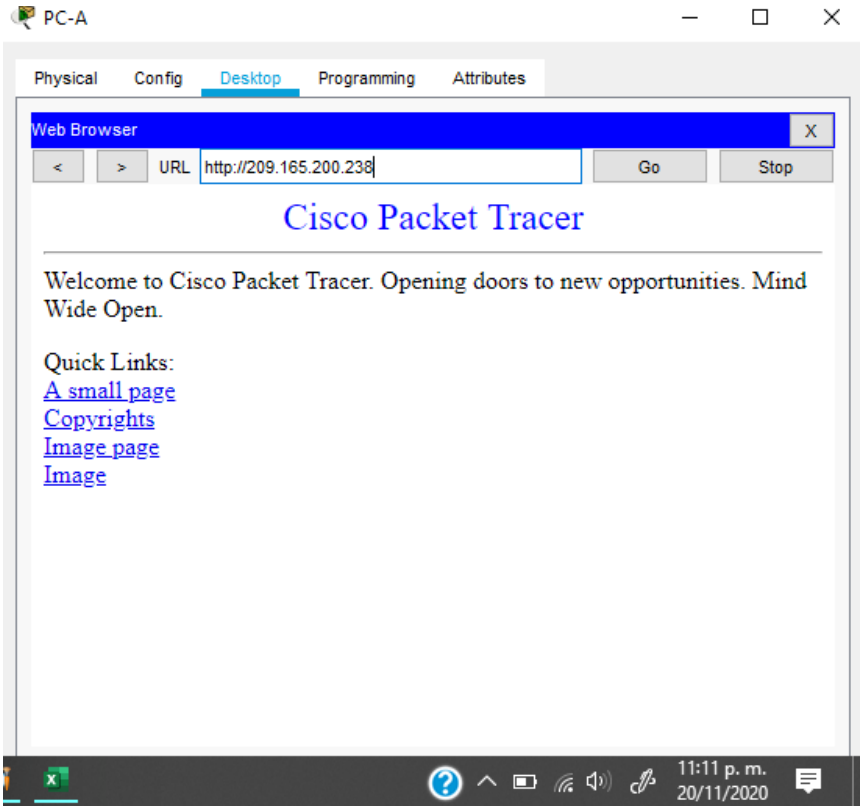



Figura 46. Conexión realizada con éxito desde PC-A a Internet

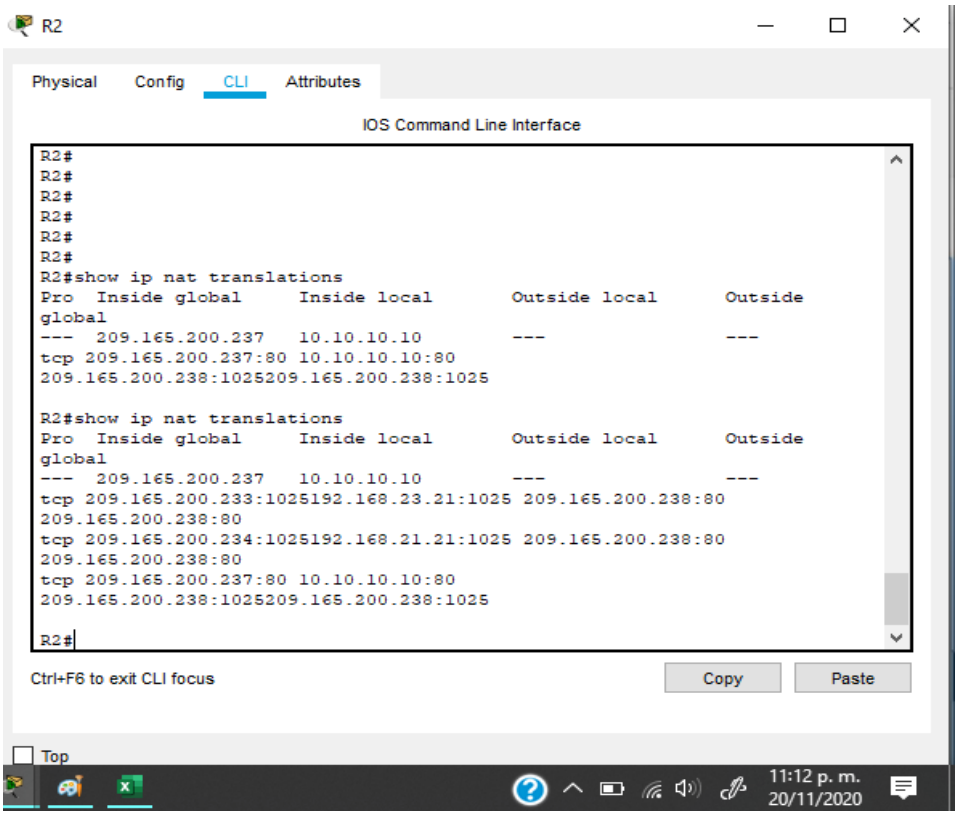



Figura 47. Verificación donde se muestran las traducciones NAT.

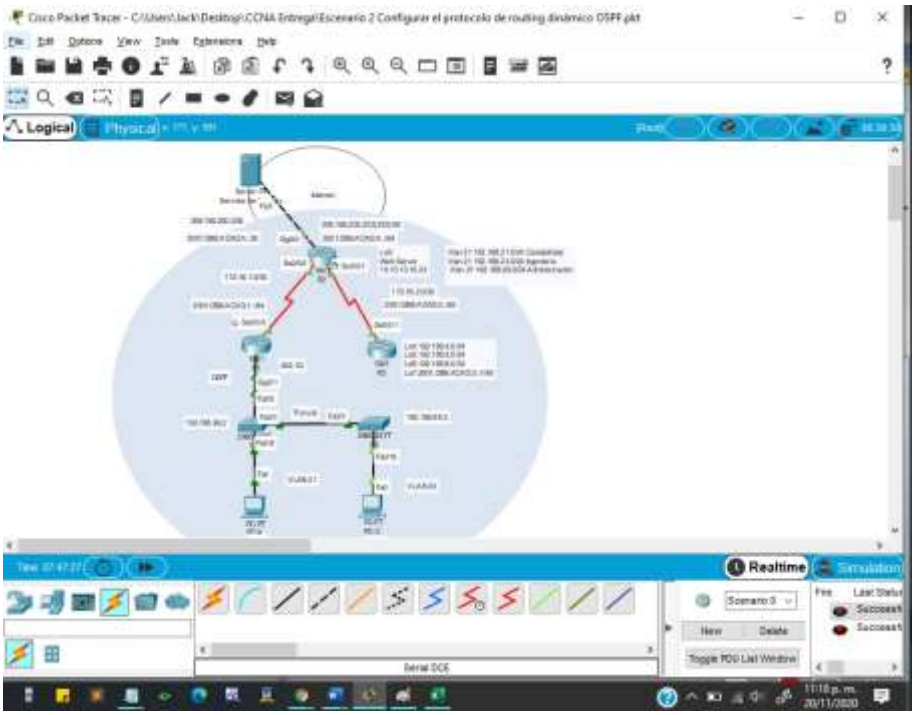



Figura 48. Red Escenario No 2 en funcionamiento.

# CONCLUSIONES

Utilizando el software de simulación Packet Tracer se logró crear y configurar las redes solicitadas en las que se configuraron Routers, Switches y equipos que admiten conectividad IPv4 e IPv6 para los hosts soportados. Los Routers y los Switches se configuraron para administrarlos de forma segura. Se configuro el enrutamiento entre VLAN, DHCP, Etherchannel y port-security.

Se puede concluir a través de la implementación y desarrollo de los escenarios 1 y 2 que existen diferentes comandos para realizar la configuración de los diferentes dispositivos aplicando aspectos de Networking, y utilizando comandos como: ping se procede a verificar la conectividad de extremo a extremo, este comando permite hacer una verificación del estado de una determinada conexión de un host local con al menos un equipo remoto contemplado en una red de tipo TCP/IP.

Cuando se lleve a cabo el rastreo desde un equipo con Windows, se utilizará el comando TRACERT, el cual determina la ruta a un destino mediante el envío de paquetes de eco de Protocolo de mensajes de control de Internet (ICMP) al destino. En estos paquetes, TRACERT usa valores de período de vida (TTL) IP variables. Dado que los enrutadores de la ruta deben disminuir el TTL del paquete como mínimo una unidad antes de reenviar el paquete, el TTL es, en realidad, un contador de saltos. Cuando el TTL del paquete de datos llega a cero (0), el enrutador devolverá un mensaje de CMP de "Tiempo agotado". Con el comando show ip route se mostrará el contenido de una tabla de enrutamiento IP. Esta tabla contiene entradas para todas las redes y subredes conocidas, así como un código que indica de qué forma se obtuvo la información.

# REFERENCIAS BIBLIOGRÁFICAS

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

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

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

Vesga, J. (2014). Diseño y configuración de redes con Packet Tracer [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgCT9VCtl_pLtPD9

Vesga, J. (2017). Ping y Tracer como estrategia en los procesos de Networking [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgTCtKY-7F5KIRC3

# ANEXOS

Anexo A: Enlaces para consulta y descarga de los Escenarios 1 y 2 de prueba de habilidades CISCO

https://drive.google.com/drive/folders/1LFIgW1qsHuMYr1s98vJMkuG1oYtRqihC?usp=sharing

Anexo B: Articulo científico, Configuración de una red pequeña mediante Software Packet Tracer v 7.3.1.0362

# Anexo B
# Configuración de una red pequeña mediante Software Packet Tracer v 7.3.1.0362

*Jacobo Carvajal Carlosama*
Universidad Nacional Abierta y a Distancia,
*jcarvajalc@unadvirtual.edu.co*

**Resumen**

**Las redes se han vuelto parte fundamental de nuestra interacción como seres humanos. Casi todas las organizaciones cuentan con su propio entorno de red, la cual, ya no está dedicada solamente a compartir y gestionar archivos, esta misma red ahora nos permite compartir aplicativos, consultar bases de datos, enviar correos electrónicos, servicio multimedia, navegar por internet y utilizar recursos como impresoras y access point.**
**El escenario ha sido desarrollado con el apoyo de la herramienta Packet Tracer, se configura e interconecta cada dispositivo; basado en los lineamientos para direccionamiento IP, protocolos de enrutamiento y otros aspectos de los componentes de topología de red**

***Palabras clave:*** **CCNA, Router, Switch, VLAN, DHCP Switching, Packet Tracer.**

**Abstract:**

***Networks have become a fundamental part of our interaction as human beings. Almost all organizations have their own network environment, which is no longer dedicated only to sharing and managing files, this same network now allows us to share applications, consult databases, send emails, multimedia service, surf the Internet. and use resources such as printers and access points.***
***The stage has been developed with the support of the Packet Tracer tool, each device is configured and interconnected; based on guidelines for IP addressing, routing protocols, and other aspects of network topology components***

***Keywords— CCNA, Router, Switch, VLAN, DHCP Switching, Packet Tracer***

## I. INTRODUCCIÓN

Los Switches, Routers y Access Point inalámbricos son los componentes básicos de la red. A través de ellos, los dispositivos conectados a la red pueden comunicarse entre sí y con otras redes (como Internet). Estos dispositivos realizan funciones muy diferentes en la red.
Los Switches son la base de la mayoría de las redes comerciales. El Switch actúa como un controlador, conectando computadoras, impresoras y servidores a la red, mientas que el Router actúa como un programador el cual analiza los datos enviados a través de la red, selecciona la mejor ruta para la transmisión de datos y luego los envía a lo largo del camino. Por último, se tiene el Acceso inalámbrico el cual es un dispositivo de red que interconecta dispositivos de comunicación inalámbrica para formar una red inalámbrica que interconecta dispositivos móviles o tarjetas de red. inalámbrico.

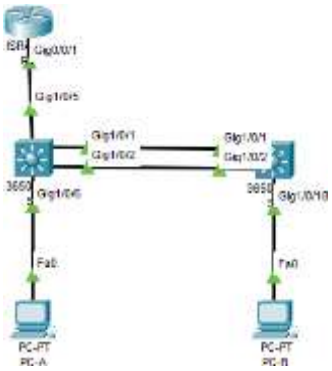
## II. METODOLOGIA

Este trabajo se desarrolla bajo el método independiente de auto aprendizaje, en este método es necesario utilizar y adoptar los medios tecnológicos proporcionados por la academia Cisco de la UNAD en el diplomado de profundización (diseño e implementación de soluciones integradas LAN / WAN. El desarrollo y diseño de la simulación, las redes y subredes se ponen en práctica en base a los conocimientos adquiridos en el desarrollo del seminario.
En este escenario, se realiza la configuración de los dispositivos en una red pequeña. Se deben realizar como parte inicial en cada dispositivo (Router, Switches), inicializar, recargar y configurar los ajustes básicos.
Posterior mente se procede con la configuración de la infraestructura de red (Vlan, Trunk Etherchanel), y configurar el soporte de host.
Por último, se realizará probar y verificar la conectividad de extremo a extremo de IPv4 e IPv6.

Para las pruebas de conectividad se utilizará el comando Ping. Ping es un comando o herramienta de diagnóstico que se puede utilizar para verificar el estado de conexión específico entre un host local y al menos una computadora remota en una red de tipo TCP/IP. El ping se usa generalmente para verificar errores de red. El funcionamiento de este mecanismo es muy sencillo y puede resultar muy útil.

Funciona enviando una serie de información a una dirección IP, host o servidor. A través del tiempo de espera de la respuesta a la transferencia de información, se determina el retraso de la respuesta, lo que también se denomina tiempo latencia

Figura 1. Topología de red



**Dispositivos de red intermediarios:** Los dispositivos intermedios conectan los terminales individuales a la red y pueden conectar varias redes individuales para formar una internetwork. Los dispositivos intermedios proporcionan conectividad y garantizan el flujo de datos en toda la red.

Estos dispositivos utilizan la dirección del terminal de destino, juntamente con información sobre las interconexiones de la red, para determinar la ruta que deben tomar los mensajes a través de la red.
Los Switches se utilizan para interconectar PC y distribuirles información en las redes de área local. Los Switches distribuyen las tramas de Ethernet a los dispositivos host identificados por las direcciones MAC de la tarjeta de interfaz de red.

Recursos necesarios 1 Router ISR44321, 2 Switch 3650-24PS y 2 PC. Software Packet Tracer v 7.3.1.0362

**Inicializar, recargar y configurar los ajustes básicos.**

Se procede a borrar las configuraciones de inicio y las VLAN del Router y vuelve a cargar los dispositivos.
Después de volver a cargar el Router, configura la plantilla SDM para admitir IPv6.
Borrar configuraciones de inicio para los Switch y Router mediante los siguientes comandos:
erase startup-config
reload
Switch1 y Switch 2 se configura la plantilla SDM para admitir IPv6. Mediante los siguientes comandos:
sdm prefiere dual-ipv4-and-ipv6 default
reload

Configuración en R1
Desactivar la búsqueda DNS medianete el comando: no ip domain lookup
Nombre del router: R1
Nombre de dominio: ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado:
R1(config)#enable password ciscoenpass
Contraseña de acceso a la consola:
R1(config-line)# password **ciscoconpass**
Establecer la longitud mínima para las contraseñas:
R1(config)#security passwords min-length 10
Crear un usuario administrativo en la base de datos local:
R1(config)#username admin secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local:
R1(config)#line vty 0 15
R1(config-line)#login local
Configurar VTY solo aceptando SSH:
R1(config-line)#transport input ssh
Cifrar las contraseñas de texto no cifrado: R1(config)#service password-encryption
Configure un MOTD Banner:
R1(config)#banner motd &Unauthorized Access is Prohibited!&
Habilitar el routing IPv6:
R1(config)#ipv6 unicast-routing
Configurar interfaz G0/0/1 y subinterfaces: Establezca la descripción, establece la dirección IPv4, establezca la dirección local de enlace IPv6 como fe80: :1, Establece la dirección IPv6.
R1(config)#int g0/0/1.2
R1(config-subif)#encapsulation dot1q 2
R1(config-subif)#description Bikes
R1(config-subif)#ip address 10.19.8.1 255.255.255.192
R1(config-subif)#ipv6 address 2001:db8:acad:a::1/64
R1(config-subif)#ipv6 address fe80::1 link-local

R1(config-subif)#int g0/0/1.3
R1(config-subif)#description Trikes
R1(config-subif)#ip address 10.19.8.65 255.255.255.224
R1(config-subif)#encapsulation dot1q 3
R1(config-subif)#ip address 10.19.8.65 255.255.255.224
R1(config-subif)#ipv6 address 2001:db8:acad:b::1/64
R1(config-subif)#ipv6 address fe80::1 link-local

R1(config-subif)#int g0/0/1.4
R1(config-subif)#encapsulation dot1q 4
R1(config-subif)#description Management
R1(config-subif)#ip address 10.19.8.97 255.255.255.248
R1(config-subif)#ipv6 address 2001:db8:acad:c::1/64
R1(config-subif)#ipv6 address fe80::1 link-local

R1(config-subif)#int g0/0/1.6

R1(config-subif)#encapsulation dot1q 6 native
R1(config-subif)#description Native
R1(config-subif)#int g0/0/1

Y activar la interfaz en R1(config-if)#no shutdown

Configure el Loopback0 interface: Establezca la descripción, establece la dirección IPv4, establece la dirección IPv6, establezca la dirección local de enlace IPv6 como fe80::1
R1(config-if)#description Internet
R1(config-if)#ip address 209.165.201.1 255.255.255.224
R1(config-if)#ipv6 address 2001:db8:acad:209::1/64
R1(config-if)#ipv6 address fe80::1 link-local

Se da nombre a el dispositivo, contraseña de acceso a la consola y acceso privilegiado, se incluyó un mensaje de inicio para configurar los parámetros básicos de seguridad de acceso y se cifran las contraseñas con el fin de aumentar la seguridad de estas.

Configuración en S1 y S2

Desactivar la búsqueda DNS: Switch(config)#no ip domain-lookup
Nombre del switch: Switch(config)#hostname S1
Switch(config)#hostname S2
Nombre de dominio ccna-lab.com:
S1(config)#ip domain-name ccna-lab.com
S2(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado ciscoenpass
S1(config)#enable secret ciscoenpass
S2(config)#enable secret ciscoenpass
Contraseña de acceso a la consola ciscoconpass
S1(config-line)#password ciscoconpass
S2(config-line)#password ciscoconpass
Crear un usuario administrativo en la base de datos local
Nombre de usuario:
S1(config)#username admin secret admin1pass
S2(config)#username admin secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local
S1(config)#line vty 0 15
S1(config-line)#login local
S2(config)#line vty 0 15
S2(config-line)#login local
Configurar las líneas VTY para que acepten únicamente las conexiones SSH
S1(config-line)#transport input ssh
S2(config-line)#transport input ssh
Cifrar las contraseñas de texto no cifrado
S1(config)#service password-encryption
S2(config)#service password-encryption
Configurar un MOTD Banner
S1(config)#banner motd &Acceso no autorizado, esta prohibido!&
S2(config)#banner motd &Acceso no autorizado, esta prohibido!&
Generar una clave de cifrado RSA Módulo de 1024 bits
S1(config)#crypto key generate rsa modulus 1024
S1(config)#crypto key generate rsa
S2(config)#crypto key generate rsa modulus 1024
S2(config)#crypto key generate rsa
Configurar la interfaz de administración (SVI), establecer la dirección IPv4 de capa 3, establezca la dirección local de enlace IPv6 como FE80: :98 para S1 y FE80: :99 para S2 y esEstablecer la dirección IPv6 de capa 3

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

S2(config)#int vlan 4
S2(config-if)#ip address 10.19.8.99 255.255.255.248
S2(config-if)#ipv6 address 2001:db8:acad:c::99/64
S2(config-if)#ipv6 address fe80::99 link-local
S2(config-if)#description Management Interface
S2(config-if)#no shutdown

S2(config)#ip default-gateway 10.19.8.97
S2(config)#S2(config)#int vlan 4
S2(config-if)#ip address 10.19.8.99 255.255.255.248
S2(config-if)#ipv6 address 2001:db8:acad:c::99/64
S2(config-if)#ipv6 address fe80::99 link-local
S2(config-if)#description Management Interface
S2(config-if)#no shutdown
Configuración del gateway predeterminado. Configure la puerta de enlace predeterminada como 10.19.8.97 para IPv4
S1(config)#ip default-gateway 10.19.8.97
S2(config)#ip default-gateway 10.19.8.97

Se da nombre a el dispositivo, contraseña de acceso a la consola y acceso privilegiado, se incluyó un mensaje de inicio para configurar los parámetros básicos de seguridad de acceso y se cifran las contraseñas con el fin de aumentar la seguridad de estas.

**A Configuración de la infraestructura de red (VLAN, Trunking, EtherChannel) en S1 y S2**

Crear VLAN: VLAN 2 nombre Bikes. VLAN 3, nombre Trikes, VLAN 4, name Management, VLAN 5, nombre Parking y VLAN 6, nombre Native

S1(config)#vlan 2
S1(config-vlan)#name Bikes

S1(config-vlan)#vlan 3
S1(config-vlan)#name Trikes
S1(config-vlan)#vlan 4
S1(config-vlan)#name Management
S1(config-vlan)#vlan 5
S1(config-vlan)#name Parking
S1(config-vlan)#vlan 6
S1(config-vlan)#name Native

Crear troncos 802.1Q que utilicen la VLAN 6 nativa.
Interfaces F0/1, F0/2 y F0/5
Interfaces G0/1, G0/2 y G0/5 (Por el Rauter Utilizado IRS 4321)
S1(config)#int g1/0/5
S1(config-if)#switchport trunk encapsulation dot1q
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 6
S1(config-if)#int range g1/0/1-2
S1(config-if-range)#shutdown
S1(config-if-range)#channel-group 1 mode active
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2 Usar el protocolo LACP para la negociación
S1(config-if-range)#int port-channel 1
S1(config-if)#switch trunk encapsulation dot1q
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 6

Configurar el puerto de acceso de host para VLAN 2, Interface F0/6
S1(config-if)#int g1/0/6
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 2
Configurar la seguridad del puerto en los puertos de acceso. Permitir 3 direcciones MAC
S1(config-if)#switchport port-security
S1(config-if)#switchport port-security maximum 3
S1(config-if)#int range g1/0/3-4

Proteja todas las interfaces no utilizadas. Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 5
S1(config-if-range)#description No esta en Uso
S1(config-if-range)#shutdown
S1(config-if-range)#int range g1/0/7-24
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 5
S1(config-if-range)#description No esta en Uso
S1(config-if-range)#shutdown
S1(config-if-range)#int range g1/1/1-4
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 5
S1(config-if-range)#description No esta en Uso
S1(config-if-range)#shutdown

Se realiza creación de las Vlan 2, 3 4, 5 y 6. Se establece comunicación entre los Switch de modo troncal con el fin de manejar el tráfico entre las Vlan.

Crear VLAN: VLAN 2 nombre Bikes. VLAN 3, nombre Trikes, VLAN 4, name Management, VLAN 5, nombre Parking y VLAN 6, nombre Native
S2(config)#vlan 2
S2(config-vlan)#name Bikes
S2(config-vlan)#vlan 3
S2(config-vlan)#name Trikes
S2(config-vlan)#vlan 4
S2(config-vlan)#name Management
S2(config-vlan)#vlan 5
S2(config-vlan)#name Parking
S2(config-vlan)#vlan 6
S2(config-vlan)#name Native

Crear troncos 802.1Q que utilicen la VLAN 6 nativa.
Interfaces F0/1 y F0/2
S2(config)#int range g1/0/1-2
S2(config-if-range)#shutdown

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

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

Configurar el puerto de acceso del host para la VLAN 3
Interfaz F0/18S2(config-if)#int g1/0/18

S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 3

Configure port-security en los access ports, permite 3 MAC addresses
S2(config-if)#switchport port-security
S2(config-if)#switchport port-security maximum 3

Asegure todas las interfaces no utilizadas. Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar
S2(config-if)#int range g1/0/3-17
S2(config-if-range)#switchport mode access
S2(config-if-range)#switchport access vlan 5
S2(config-if-range)#description No esta en Uso
S2(config-if-range)#shutdown

S2(config-if-range)#int range g1/0/19-24
S2(config-if-range)#switchport mode access
S2(config-if-range)#switchport access vlan 5
S2(config-if-range)#description No esta en Uso
S2(config-if-range)#shutdown
S2(config-if-range)#int range g1/1/1-4
S2(config-if-range)#switchport mode access
S2(config-if-range)#switchport access vlan 5
S2(config-if-range)#description No esta en Uso
S2(config-if-range)#shutdown

Se realiza creación de las Vlan 2, 3 4, 5 y 6. Se establece comunicación entre los Switch de modo troncal con el fin de manejar el tráfico entre las Vlan.

**Configurar soporte de host en R1**

Configure Default Routing. Crear rutas predeterminadas para IPv4 e IPv6 que dirijan el tráfico a la interfaz Loopback 0
R1(config)#ip route 0.0.0.0 0.0.0.0 loopback 0
R1(config)#ipv6 route ::/0 loopback 0
Ambas rutas estáticas para llegar a internet

Configurar IPv4 DHCP para VLAN 2. Cree un grupo DHCP para VLAN 2, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio ccna-a.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada

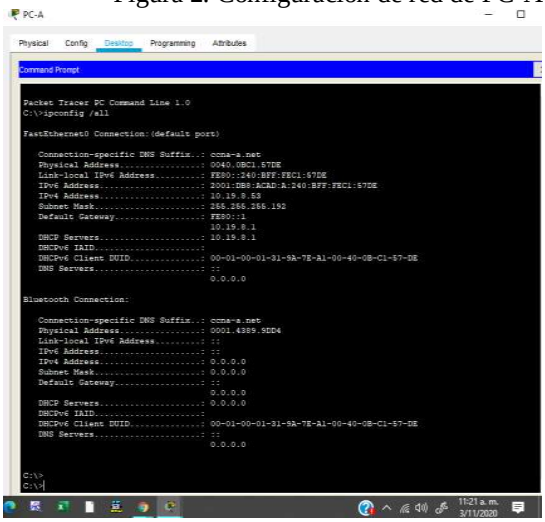
R1(config)#ip dhcp excluded-address 10.19.8.1 10.19.8.52
R1(config)#ip dhcp pool VLAN2-Bikes
R1(dhcp-config)#network 10.19.8.0 255.255.255.192
R1(dhcp-config)#default-router 10.19.8.1
R1(dhcp-config)#domain-name ccna-a.net

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

R1(config)#ip dhcp excluded-address 10.19.8.65 10.19.8.84
R1(config)#ip dhcp pool VLAN3Trikes
R1(dhcp-config)#network 10.19.8.64 255.255.255.224
R1(dhcp-config)#default-router 10.19.8.65
R1(dhcp-config)#domain-name ccna-b.net

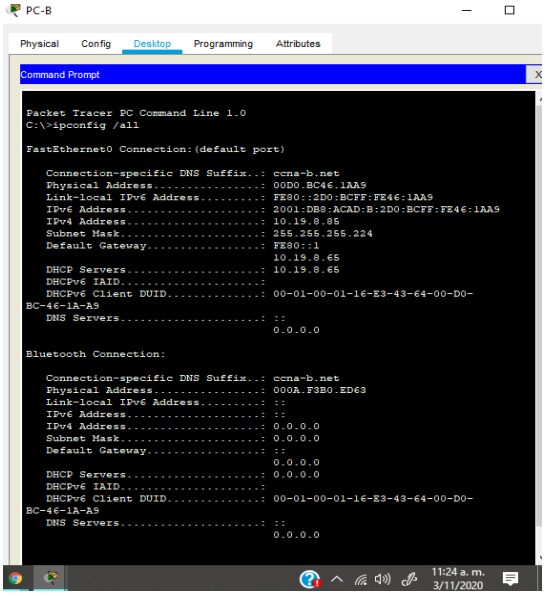
Configuración de red de PC-A
Descripción
Dirección física
Dirección IP
Máscara de subred
Gateway predeterminado
Gateway predeterminado IPv6

Figura 2. Configuración de red de PC-A




Configuración de red de PC-B
Descripción
Dirección física
Dirección IP
Máscara de subred
Gateway predeterminado
Gateway predeterminado IPv6

Figura 2. Configuración de red de PC-B




Probar y verificar la conectividad de extremo a extremo
Use el comando ping para probar la conectividad IPv4 e IPv6 entre todos los dispositivos de red.

Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas

correctivas para establecer la conectividad si alguna de las pruebas falla

Tabla 1. En la tabla se muestra verificación de conectividad con cada dispositivo de red.

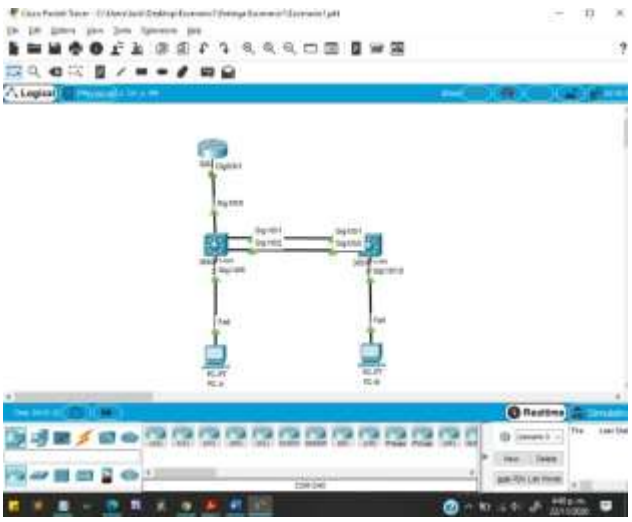
TABLA 1

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

Con el comando ping se procede a verificar la conectividad de extremo a extremo. Ping opera mediante el envío de paquetes de solicitud de eco del protocolo de mensajes de control de Internet (ICMP) al host de destino y la espera de una respuesta del ICMP. Puede registrar el tiempo de ida y vuelta y la pérdida de paquetes. Con resultado exitoso para cada una de las pruebas realizadas

.

Figura 4. Red Escenario No 1 en funcionamiento.



## III. REFERENCIAS


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

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

[3] Vesga, J. (2014). Diseño y configuración de redes con Packet Tracer [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgCT9VCtl_pLtPD9

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

[5] Vesga, J. (2017). Ping y Tracer como estrategia en los procesos de Networking [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgTCtKY-7F5KIRC3

## IV. BIOGRAFÍA

**Jacobo Carvajal Carlosama** (nacido en 1979 en la ciudad de Popayán, Cauca) es candidato para obtener el título de Ingeniero Electrónico de la Universidad Nacional Abierta y a Distancia. Tecnólogo en Electricidad industrial egresado del SENA, cuenta con quince (15) años de experiencia en el campo eléctrico, y ha ocupado cargos en el campo de operación y generación de energía, con niveles de tensión de 230/115/34.5/13.8 kV. Actualmente se desempeña como Especialista de Centro de Control para Petroeléctrica de los Llanos Ltd, El Sr. Carvajal realizo una investigación sobre la evaluación de habilidades del CCNNA Escenario No 1, en la que se configurarán los dispositivos en una red pequeña. Logrando los objetivos esperados de: inicializar, recargar y configurar los ajustes básicos del dispositivo, configurar las configuraciones de la infraestructura de red (VLAN, Trunking, Etherchannel), configurar el soporte de host y probar y verificar la conectividad de extremo a extremo IPv4 e IPv6.