PRUEBA DE HABILIDADES PRÁCTICAS CCNP

BRAYAM BAUDILIO MARTÍNEZ PERDOMO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI

INGENIRIA DE TELECOMUNICACIONES

FLORENCIA, CAQUETÁ

2021

PRUEBA DE HABILIDADES PRÁCTICAS CCNP

BRAYAM BAUDILIO MARTÍNEZ PERDOMO

Diplomado de opción de grado presentado para optar el título deIngeniero
De Telecomunicaciones

HECTOR HERRERA

TUTOR ASESOR

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI

INGENIRIA DE TELECOMUNICACIONES

FLORENCIA, CAQUETÁ

2021

Nota de Aceptación

Presidente del Jurado

Jurado

Jurado

Florencia, 16 de julio del 2021.

DEDICATORIA

Este trabajo se lo dedico primero a Dios quien me dio la oportunidad de vivir y a nuestro señor Jesucristo quien no me ha abandonado en los momentos de mayor necesidad. Tambien va dedicado a mi señora madre Piedad Perdomo Fernández quien siempre me ha apoyado incondicionalmente para terminar esta carrera espectacular. No olvido a mis hermanos Víctor Martínez Perdomo y a Marily Martínez Perdomo quienes me han apoyado desde la distancia, junto con el afecto y cariño de hermanos que tienen y a la misma vida le doy un agradecimiento especial pues me ha enseñado que todo tiene un costo, nada es fácil y que los sueños se cumplen pero hay que luchar por ellos, porque solito no se hacen realidad, aunque uno se encuentra con obstáculos que le impide que las metas o sueños se cumplan, hay que ser fuerte y saberlo sobre llevar para tener la certeza, seguridad y felicidad de que si se pudo pasar aquella prueba que la vida te puso.

Este trabajo tambien está dedicado a todos los tutores con quien tuve la oportunidad de compartir todas sus enseñanzas, que me hicieron repetir trabajos e incluso algunas materias, pero que al fin de cuentas fue para mi bien propio. Sin ellos no estaría en esta etapa de mi vida para obtener el título de Ingeniero de Telecomunicaciones. Por último, a la Institución, a esta gran universidad y a todas las personas que lo conforman, desde la parte administrativa, consejo superior universitario, académico, rectoría y las demás estructuras que en estos momentos no recuerdo los nombres, a todos ellos muchas gracias.

AGRADECIMIENTOS

Mi Trabajo de gradado en el diplomado de profundización cisco prueba de habilidades prácticas ccnp está ligado a la oportunidad que Dios me ha dado de y de ser una persona de bien, adicionalmente agradezco a mi señora Madre por el apoyo incondicional para culminar la carrera, por los años de sacrificios personales y económicos, pero con una satisfacción de haber cumplido los objetivo propuestos, quiero finalmente agradecer al personal de docentes de esta institución, que me brindaron un apoyo importante mediante las asesorías y acompañamiento académico, durante el tiempo de aprendizaje para poder lograr los retos de adquirir conocimiento y convertirme en un buen profesional, entendí y comprendí que los retos son la clave para persistir a largo plazo las metas que uno se propone.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

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 especifica 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: Se adapta automáticamente a los cambios de la topología de la red.

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.

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.

BANNER MOTD: Es un comando que especifica el mensaje que se muestra como Mensaje del día, el primer mensaje que se muestra en una conexión entrante. Este comando define solo el mensaje; el comando motd - banner habilita o deshabilita la visualización.

DHCP: Significa protocolo de configuración de host dinámico y es un protocolo de red utilizado en redes IP donde un servidor DHCP asigna automáticamente una dirección IP y otra información a cada host en la red para que puedan comunicarse de manera eficiente con otros puntos finales.

ETHERCHANNEL: Es una tecnología de agregación de enlaces de puertos desarrollada por Cisco, que proporciona enlaces de alta velocidad tolerantes a fallas entre conmutadores, enrutadores y servidores. La tecnología EtherChannel permite que varios enlaces Ethernet físicos (Fast Ethernet o Gigabit Ethernet) se combinen en un canal lógico.

GATEWAY: Un Gateway (puerta de enlace) es un dispositivo, con frecuencia un ordenador, que permite interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación. Su propósito es traducir la información del protocolo utilizado en una red al protocolo usado en la red de destino.

NVRAM: La NVRAM o “Non-Volatile Random Access Memory”, es una memoria de acceso aleatorio no volátil capaz de almacenar información y no perderla al retirar la alimentación eléctrica del componente.

PORT-SECURITY: Es una característica de los switches Cisco que les permite retener las direcciones MAC conectadas a cada puerto del dispositivo y permitir solamente a esas direcciones MAC comunicarse a través de esa entrada del switch. Si un dispositivo con otra dirección MAC intenta comunicarse a través de esa esa entrada, port-security deshabilitará el puerto.

TRUNKING: En telecomunicaciones, el enlace troncal es una forma de proporcionar acceso a la red a muchos clientes compartiendo un conjunto de líneas o frecuencias en lugar de proporcionarlas individualmente.

VLAN: Acrónimo de virtual LAN (red de área local virtual), es un método para crear redes lógicas independientes dentro de una misma red física.1Varias VLAN pueden coexistir en un único conmutador físico o en una única red física.

RESUMEN

El diplomado de profundización CISCO, hace énfasis en realizar de manera correcta pruebas en un simulador para un aprendizaje practico, utilizando herramientas de acceso remoto con el fin de establecer escenarios en redes como LAN/WAN que nos permiten realizar un análisis profundo sobre el comportamiento de diversos protocolos y métricas de enrutamiento, atreves de la administración de redes disponibles en la IOS para resolver los problemas de datos que se presentan en diversos tipos de redes. Es así que nos permite evaluar el desempeño de routers y switches, utilizando el uso de comandos especializados en gestión de redes y compatibles con el protocolo SMNP, este diseña políticas de enrutamiento estático y/o dinámico, bajo un esquema de direccionamiento IP sin clase, para dar soluciones de red y conectividad escalables.

Durante el desarrollo del presente documento dará solución a dos situaciones planteadas como parte de un examen final da habilidades prácticas en el curso CCNA; en estos dos escenarios 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.

ABSTRACT

In this document you will find two scenarios of the CISCO CCNA in-depth diploma. Which in this case is the complement for my career (Telecommunications Engineering), its bases are based on the development of laboratories in a simulator, managing to understand and apply the two proposed scenarios; You will find the registry of the configurations of each of the devices, the detailed description of the step by step of each of the stages carried out during its development, the registry of the connectivity verification processes through the use of ping, traceroute, show commands. ip route, among others. The Packet Tracer software tool was used for the network creation and configuration process.

It can be affirmed by carrying out this activity how to advance in the development of strategies that seek the good performance of exercises through routers and switches, looking for a good configuration and then a good programming, in order to have the expected results, demonstrating and placing all the knowledge obtained in the course and then put it into practice, in order to present the best response to this phase that is important for the development of our career as engineers and at the same time recognize the importance of technology in a changing world that evolves more and more in post of digital communication.

INTRODUCCION

En este documento encontrara dos escenarios del diplomado de profundización CISCO CCNA. Que en este caso es el complemento para mi carrera (Ingeniería de Telecomunicaciones), sus bases se fundamentan en el desarrollado de laboratorios en un simulador, logrando entender y aplicar los dos escenarios propuestos; encontrara 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.

Se puede afirmar mediante la realización de esta actividad como avanzar en el desarrollo de estrategias que buscan el buen desempeño de ejercicios a través de routers y los switches buscando una buena configuración y luego una buena programación, para así, tener los resultados esperados demostrando y colocando todo el conocimiento obtenido en el curso y luego llevarlo a la práctica, para así, presentar la mejor respuesta a esta fase que es importante a para el desarrollo de nuestra carrera como ingenieros y al mismo tiempo reconocer la importancia de la tecnología en un mundo cámbiate que evoluciona cada vez más en post de la comunicación digital.

1 PLANTEAMIENTO DEL PROBLEMA – ESCENARIO 1

1.1 PLANTEAMIENTO ESPECÍFICO DEL PROBLEMA – ESCENARIO 1

Topología

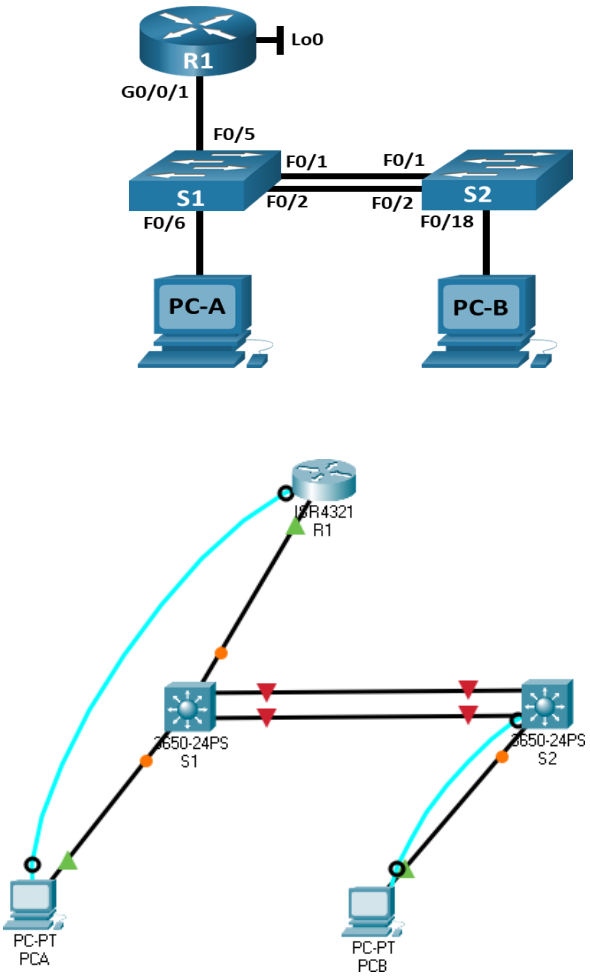


Figura 1-Implementación de la red-escenario-1

En este primer escenario se configurarán los dispositivos de una red pequeña. Debe configurar un router, un switch y equipos que admitan tanto la conectividad IPv4 como IPv6 para los hosts soportados. El router y el switch

también deben administrarse de forma segura. Configurará el enrutamiento entre VLAN, DHCP, Etherchannel y port-security.

Tabla de VLAN

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

Tabla 1- Vlan

Tabla de asignación de direcciones

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
R1 G0/0/1.2	10.21.5.1 /26	No corresponde
	2001:db5:acad:a: :1 /64	No corresponde
R1 G0/0/1.3	10.21.5.65 /27	No corresponde
	2001:db5:acad:b: :1 /64	No corresponde
R1 G0/0/1.4	10.21.5.97 /29	No corresponde
	2001:db5:acad:c: :1 /64	No corresponde
R1 G0/0/1.6	No corresponde	No corresponde
R1 Loopback0	209.165.201.1 /27	No corresponde
	2001:db8:acad:209: :1 /64	No corresponde
S1 VLAN 4	10.21.5.98 /29	10.21.5.97

	2001:db5:acad:c: :98 /64	No corresponde
	fe80: :98	No corresponde
S2 VLAN 4	10.21.5.99 /29 2001:db5:acad:c: :99 /64 fe80: :99	10.21.5.97 No corresponde No corresponde
PC-A NIC	Dirección DHCP para IPv4	DHCP para puerta de enlace predeterminada IPv4
	2001:db5:acad:a: :50 /64	fe80::1
PC-B NIC	DHCP para dirección IPv4 2001:db5:acad:b: :50 /64	DHCP para puerta de enlace predeterminada IPv4 fe80::1

Tabla 2-asignación de direcciones

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

1.2 Desarrollo específico del problema - Escenario 1

1.3 Inicializar y recargar y configurar aspectos básicos de los dispositivos

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

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

En R1

```
Router>en
Router#erase startup-config
Router#reload
```

En S1

```
Switch>en
Switch#erase startup-config
Switch#reload
```

En S2

```
Switch>en
Switch#erase startup-config
Switch#reload
```

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

En S1

```
Switch>en
Switch# config t
Switch(config)# sdm  prefer  dual-ipv4-and-ipv6  default
Switch(config)#exit
Switch#reload
```

En S2

```
Switch>en
Switch# config t
Switch(config)# sdm  prefer  dual-ipv4-and-ipv6  default
Switch(config)#exit
Switch#reload
```

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

Pasó 2: Configurar R1 - Las tareas de configuración para R1 incluyen las siguientes:

2.1. Desactivar la búsqueda DNS

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

2.2. Nombre del router – R1

```
Router>en
```

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

2.3. Nombre de dominio - ccna-lab.com

```
R1(config)# ip  domain  name  ccna-lab.com
```

2.4. Contraseña cifrada para el modo EXEC privilegiado - ciscoenpass

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

2.5. Contraseña de acceso a la consola - ciscoconpass

```
R1(config)#line console 0
R1(config-line)#password ciscoconpass
R1(config-line)#login
R1(config-line)#exit
R1(config)#
```

2.6. Establecer la longitud mínima para las contraseñas – 10 caracteres

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

2.1. Crear un usuario administrativo en la base de datos local - Nombre de usuario: admin - Password: admin1pass

```
R1(config)#username admin secret admin1pass
```

2.2. 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
```

2.3. Configurar VTY solo aceptando SSH

```
R1(config-line)#transport input ssh
R1(config-line)#exit
```

2.4. Cifrar las contraseñas de texto no cifrado

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

2.5. Configure un MOTD Banner

```
R1(config)#banner motd #Acceso No Autorizado – No Insista#
```

2.6. Habilitar el routing IPv6

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

2.7. Configurar interfaz G0/1 y subinterfaces

```
R1(config)# int  g0/1.2
R1(config-subif)#encapsulation dot1Q 2
R1(config-subif)#description Vlan-->Bikes
R1(config-subif)#ip address 10.21.5.1 255.255.255.192
R1(config-subif)#ipv6 address 2001:db5:acad:a::1/64
R1(config-subif)#ipv6 address fe80::1 link-local
R1(config-subif)#exit
```

```
R1(config)# int  g0/1.3
R1(config-subif)#encapsulation dot1Q 3
R1(config-subif)#description Vlan-->Trikes
R1(config-subif)#ip address 10.21.5.65 255.255.255.224
R1(config-subif)#ipv6 address 2001:db5:acad:b::1/64
R1(config-subif)#ipv6 address fe80::1 link-local
R1(config-subif)#exit
```

```
R1(config)#int g0/1.4
R1(config-subif)#encapsulation dot1Q 4
R1(config-subif)#description Vlan-->Management
R1(config-subif)#ip address 10.21.5.97 255.255.255.248
R1(config-subif)#ipv6 address 2001:db8:acad:c::1/64
R1(config-subif)#ipv6 address fe80::1 link-local
R1(config-subif)#exit
```

```
R1(config)#int g0/1.6
R1(config-subif)#encapsulation dot1Q 6
R1(config-subif)#description Vlan-->Native
R1(config-subif)#exit
```

```
R1(config)#int g0/1
R1(config-if)#no shutdown
```

2.8. Configure el Loopback0 interface

```
R1(config)#int Loopback 0
R1(config-if)#description Loopback
R1(config-if)#ip address 209.165.201.1 255.255.255.224
R1(config-if)#ipv6 address 2001:db8:acad:209::1/64
R1(config-if)#ipv6 address fe80::1 link-local
R1(config-if)#exit
```

2.9. Generar una clave de cifrado RSA - Módulo de 1024 bits

```
R1(config)#crypto key generate rsa
How many bits in the modulus [512]:
1024
```

Paso 3: Configure S1 y S2 - Las tareas de configuración incluyen lo siguiente:

3.1. Desactivar la búsqueda DNS.

S1 y S2

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

3.2. Nombre del switch – S1 y S2

S1

```
Switch(config)#hostname S1
S1(config)#
```

S2

```
Switch(config)#hostname S2
S2(config)#
```

3.3. Nombre de dominio

```
S1(config)# ip  domain  name  ccna-lab.com
S2(config)# ip  domain  name  ccna-lab.com
```

3.4. Contraseña cifrada para el modo EXEC privilegiado - ciscoenpass

```
S1(config)# enable  secret  ciscoenpass
S2(config)# enable  secret  ciscoenpass
```

3.5. Contraseña de acceso a la consola - ciscoconpass

```
S1(config)# line  console  0
S1(config-line)#password ciscoconpass
S1(config-line)#login
S1(config-line)#exit
```

```
S2(config)# line  console  0
S2(config-line)#password ciscoconpass
S2(config-line)#login
S2(config-line)#exit
```

3.6. Crear un usuario administrativo en la base de datos local - Nombre de usuario: admin - Password: admin1pass

```
S1(config)# username admin secret admin1pass
S2(config)# username admin secret admin1pass
```

3.7. 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
```

3.8 Configurar las líneas VTY para que acepten únicamente las conexiones SSH

```
S1(config-line)#transport input ssh
S1(config-line)#exit

S2(config-line)#transport input ssh
S2(config-line)#exit
```

3.9. Cifrar las contraseñas de texto no cifrado

```
S1(config)# service password-encryption
S2(config)# service password-encryption
```

3.10. Configurar un MOTD Banner

```
S1(config)#banner motd #Acceso No Autorizado – No Insista#
S2(config)#banner motd #Acceso No Autorizado – No Insista#
```

3.11. Generar una clave de cifrado RSA - Módulo de 1024 bits

```
S1(config)#crypto key generate rsa
How many bits in the modulus [512]: 1024

S2(config)#crypto key generate rsa
How many bits in the modulus [512]: 1024
```

3.12. Configurar la interfaz de administración (SVI)

```
S1(config)#int vlan 4
S1(config-if)#ip address 10.21.5.98 255.255.255.248
S1(config-if)#ipv6 address 2001:db5:acad:c::98/64
S1(config-if)#ipv6 address fe80::98 link-local
S1(config-if)#no shutdown
S1(config-if)#exit

S2(config)#int vlan 4
S2(config-if)#ip address 10.21.5.99 255.255.255.248
S2(config-if)#ipv6 address 2001:db5:acad:c::99/64
S2(config-if)#ipv6 address fe80::99 link-local
S2(config-if)#no shutdown
S2(config-if)#exit
```

3.13. Configuración del gateway predeterminado

```
S1(config)# ip  default-gateway  10.21.5.97
S2(config)# ip  default-gateway  10.21.5.97
```

1.4 Configuración de la infraestructura de red (VLAN, TRUNKING, ETHERCHANNEL)

Paso 4: Configurar S1 - La configuración del S1 incluye las siguientes tareas:

4.1. Crear VLAN

```
S1(config)#vlan 2
S1(config-vlan)#name Bikes
S1(config-vlan)#vlan 3
S1(config-vlan)#name Trikes
S1(config-vlan)#vlan 4
S1(config-vlan)#name Management
S1(config-vlan)#vlan 5
S1(config-vlan)#name Parking
S1(config-vlan)#vlan 6
S1(config-vlan)#name Native
S1(config-vlan)#exit
```

4.2. Crear troncos 802.1Q que utilicen la VLAN 6 nativa - Interfaces F0/1, F0/2 y F0/5

```
S1(config)#int f0/1
S1(config-if)#switchport trunk encapsulation dot1q
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 6
S1(config-if)#switchport trunk allowed vlan 2,3,4,5,6
S1(config-if)#exit

S1(config)#int f0/2
S1(config-if)#switchport trunk encapsulation dot1q
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 6
S1(config-if)#switchport trunk allowed vlan 2,3,4,5,6
S1(config-if)#exit

S1(config)#int f0/5
S1(config-if)#switchport trunk encapsulation dot1q
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 6
S1(config-if)#switchport trunk allowed vlan 2,3,4,5,6
S1(config-if)#exit
```

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

```
S1(config)#int f0/1
```

```
S1(config-if)#channel-group 1 mode active
S1(config-if)#exit


S1(config)#int f0/2
S1(config-if)#channel-group 1 mode active
S1(config-if)#exit
```

4.4. Configurar el puerto de acceso de host para VLAN 2 - Interface F0/6

```
S1(config)#int f0/6
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 2
```

4.5. Configurar la seguridad del puerto en los puertos de acceso - Permitir 3 direcciones MAC

```
S1(config-if)#switchport port-security maximum 3
```

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

```
S1(config)#int range f0/3-4
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 5
S1(config-if-range)#description Deshabilitada
S1(config-if-range)#no shutdown
S1(config-if-range)#exit


S1(config)#int range f0/7-24
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 5
S1(config-if-range)#description Desabilitada
S1(config-if-range)#no shutdown
S1(config-if-range)#exit


S1(config)#int range g0/1-2
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 5
S1(config-if-range)#description Desabilitada
```

```
S1(config-if-range)#no shutdown
S1(config-if-range)#exit
```

Paso 5: Configure el S2 - Entre las tareas de configuración de S2 se incluyen las siguientes:

5.1. Crear VLAN

```
S2(config)#vlan 2
S2(config-vlan)#name Bikes
S2(config-vlan)#vlan 3
S2(config-vlan)#name Trikes
S2(config-vlan)#vlan 4
S2(config-vlan)#name Management
S2(config-vlan)#vlan 5
S2(config-vlan)#name Parking
S2(config-vlan)#vlan 6
S2(config-vlan)#name Native
S2(config-vlan)#exit
```

5.2. Crear troncos 802.1Q que utilicen la VLAN 6 nativa - Interfaces F0/1 y F0/2

```
S2(config)#int f0/1
S2(config-if)#switchport trunk encapsulation dot1q
S2(config-if)#switchport mode trunk
S2(config-if)#switchport trunk native vlan 6
S2(config-if)#switchport trunk allowed vlan 2,3,4,5,6
S2(config-if)#exit
```

```
S2(config)#int f0/2
S2(config-if)#switchport trunk encapsulation dot1q
S2(config-if)#switchport mode trunk
S2(config-if)#switchport trunk native vlan 6
S2(config-if)#switchport trunk allowed vlan 2,3,4,5,6
S2(config-if)#exit
```

5.3. 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)#int f0/1
S2(config-if)#channel-group 1 mode active
S2(config-if)#exit

S2(config)#int f0/2
S2(config-if)#channel-group 1 mode active
S2(config-if)#exit
```

5.4. Configurar el puerto de acceso de host para VLAN 3 - Interface F0/18

```
S2(config)#int f0/18
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 3
```

5.5. Configure port-security en los access ports - permite 3 MAC addresses

```
S2(config-if)#switchport port-security maximum 3
```

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

```
S2(config)#int range f0/3-17
S2(config-if-range)#switchport mode access
S2(config-if-range)#switchport access vlan 5
S2(config-if-range)#description Desabilitada
S2(config-if-range)#no shutdown
S2(config-if-range)#exit

S2(config)#int range f0/19-24
S2(config-if-range)#switchport mode access
S2(config-if-range)#switchport access vlan 5
S2(config-if-range)#description Desabilitada
S2(config-if-range)#no shutdown
S2(config-if-range)#exit

S2(config)#int range g0/1-2
S2(config-if-range)#switchport mode access
S2(config-if-range)#switchport access vlan 5
S2(config-if-range)#description Desabilitada
```

```
S2(config-if-range)#no shutdown
S2(config-if-range)#exit
```

1.5 Configurar soporte de host

Paso 1: Configure R1 - Las tareas de configuración para R1 incluyen las siguientes:

1.1. 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
```

1.2. 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 10.21.5.1 10.19.8.52
R1(config)#ip dhcp pool Vlan2-Bikes
R1(dhcp-config)#network 10.21.5.0 255.255.255.192
R1(dhcp-config)#default-router 10.21.5.1
R1(dhcp-config)#domain-name ccna-a.net
R1(dhcp-config)#exit
```

1.3. 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 10.21.5.65 10.21.5.84
R1(config)#ip dhcp pool Vlan3-Trikes
R1(dhcp-config)#network 10.21.5.64 255.255.255.224
R1(dhcp-config)#default-router 10.21.5.65
R1(dhcp-config)#domain-name ccna-b.net
R1(dhcp-config)#exit
```

1.6 CONFIGURAR LOS SERVIDORES

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

PC-A Network Configuration	
Descripción	Información tomada con ipconfig /all
Dirección física	0001.967D.3B21
Dirección IP	10.21.5.55
Máscara de subred	255.255.255.192
PC-A Network Configuration	
Gateway predeterminado	10.21.5.1
Gateway predeterminado IPv6	*FE80::209:7CFF:FEA1:36A0* *2001:db5:acad:b::50/64*

Tabla 3-configuración equipo PC-A

Configuración de red de PC-B

Descripción	Información tomada con ipconfig /all
Dirección física	00E0.A38D.27C4
Dirección IP	10.21.5.53
Máscara de subred	255.255.0.0
Gateway predeterminado	10.21.5.66
Gateway predeterminado IPv6	*FE80::20C:CFFF:FEB6:5835* *2001:db5:acad:b::50/64*

Tabla 4-configuración equipo PC-B

Parte 3: 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:

1.7 Ping del PC-A - Router y switch’s

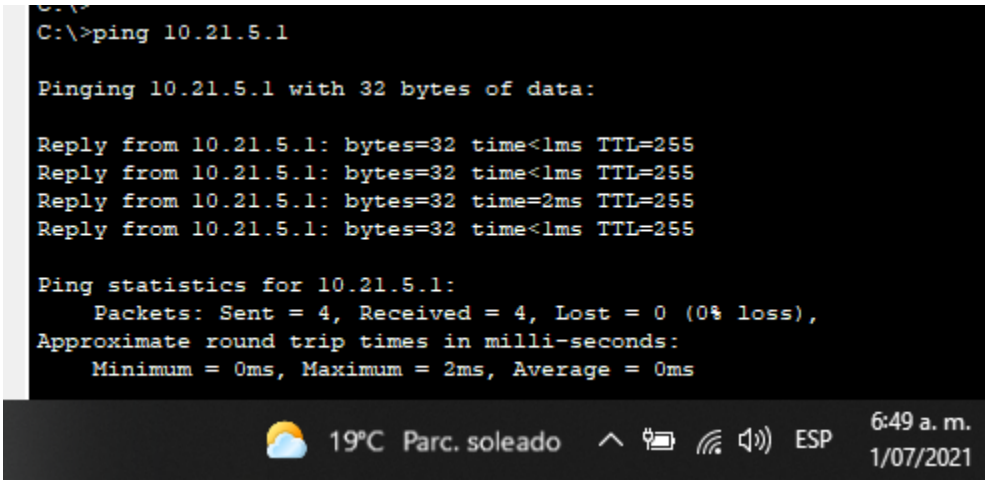


Figura 2-Ping PC-A-R1-10.21.5.1

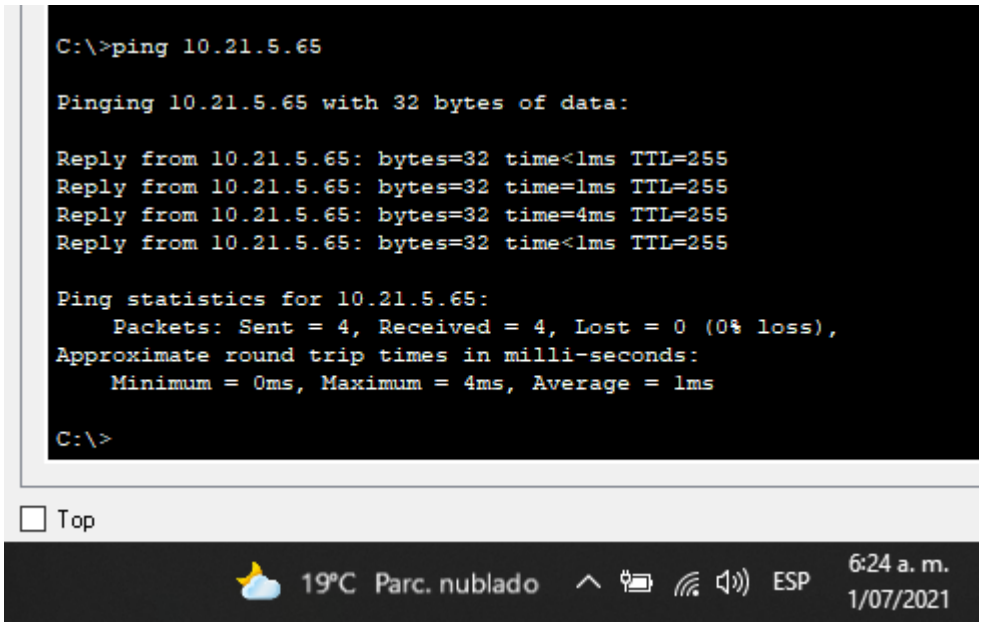


Figura 3- Ping PC-A-R1-10.21.5.65

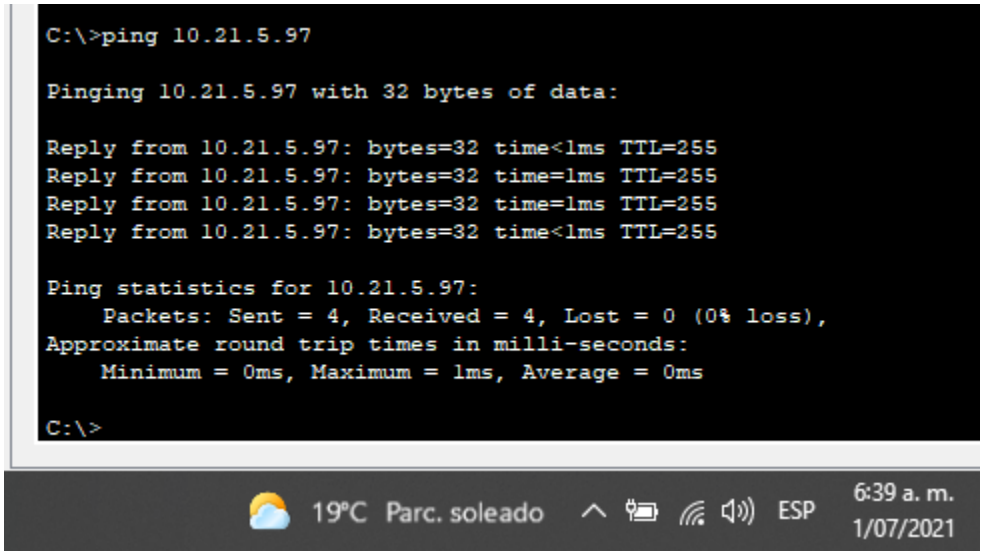


Figura 4- Ping PC-A-R1-10.21.5.97

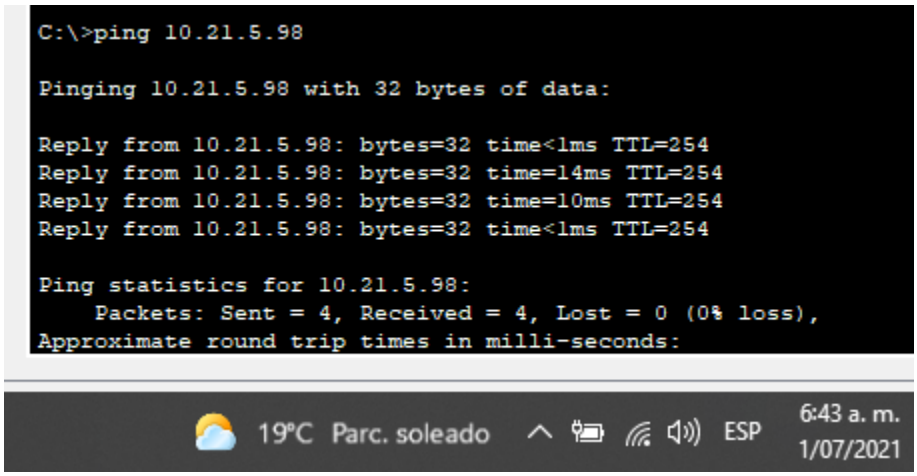


Figura 5-Ping PC-A-S1-10.21.5.98

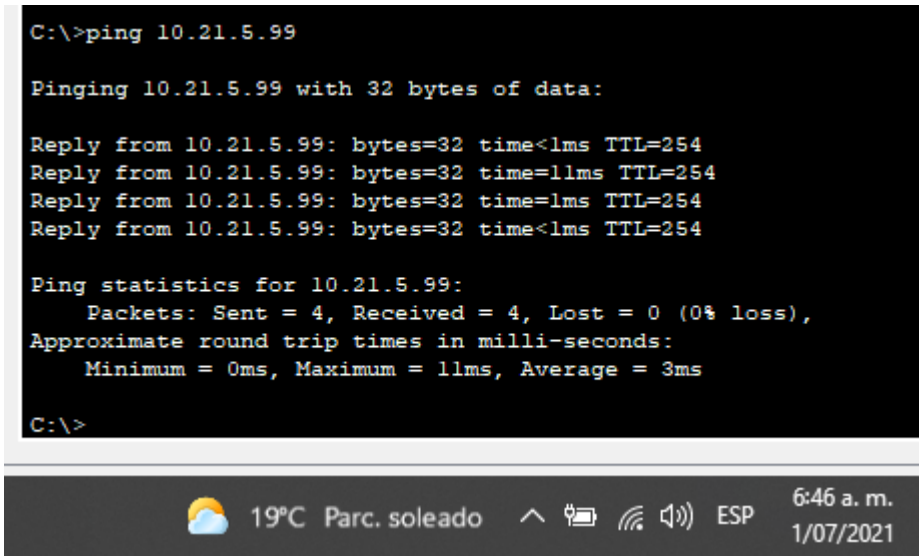


Figura 6-Ping PC-A-S2-10.21.5.99

1.8 Ping del PC-B - Router y switch's

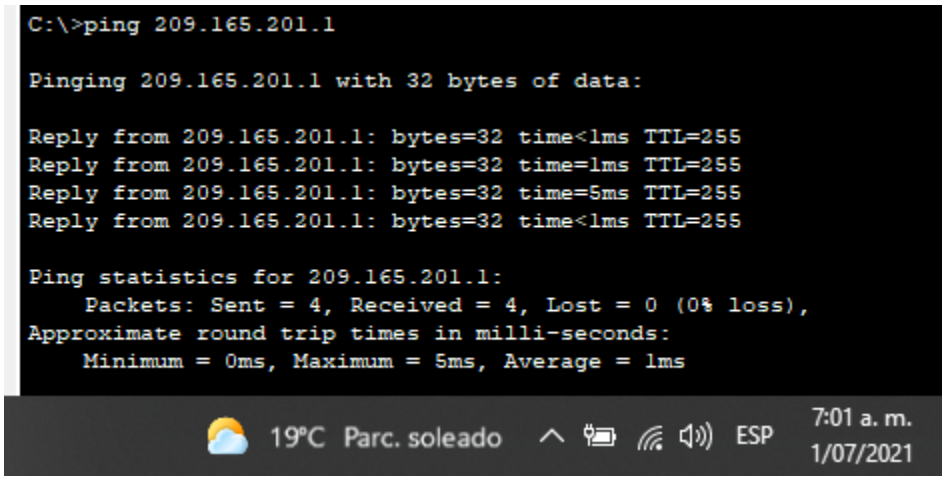


Figura 7- Ping PC-B-R1-209.165.201.1

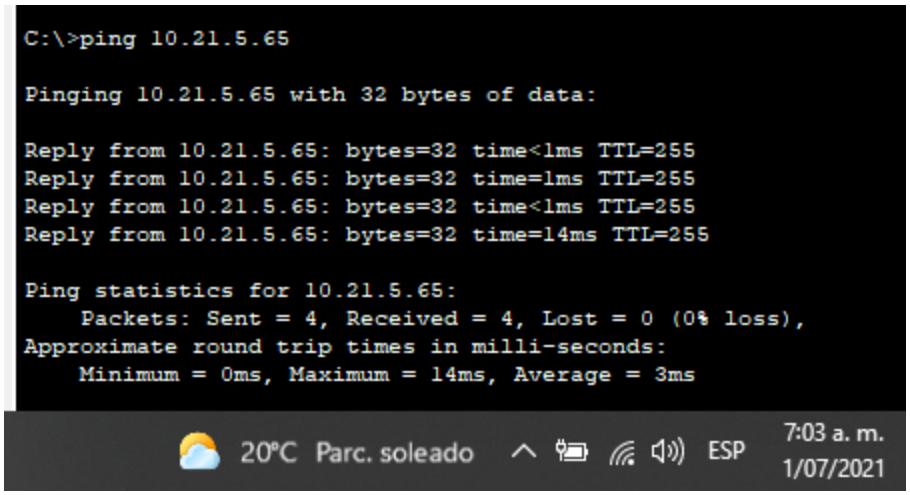


Figura 8- Ping PC-B-R1-10.21.5.65

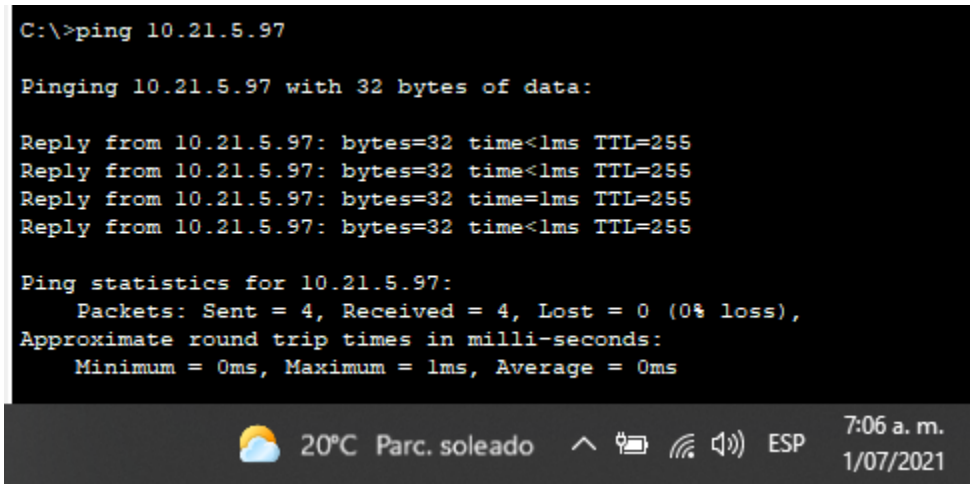


Figura 9- Ping PC-B-R1-10.21.5.97

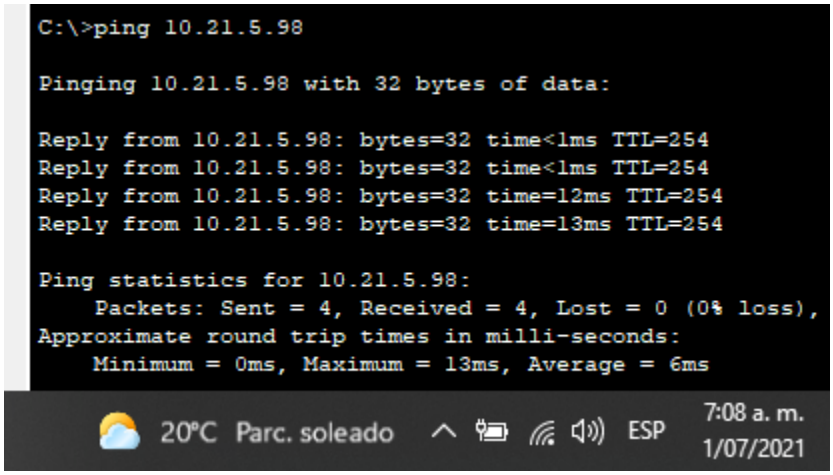


Figura 10- Ping PC-B-S1-10.21.5.98

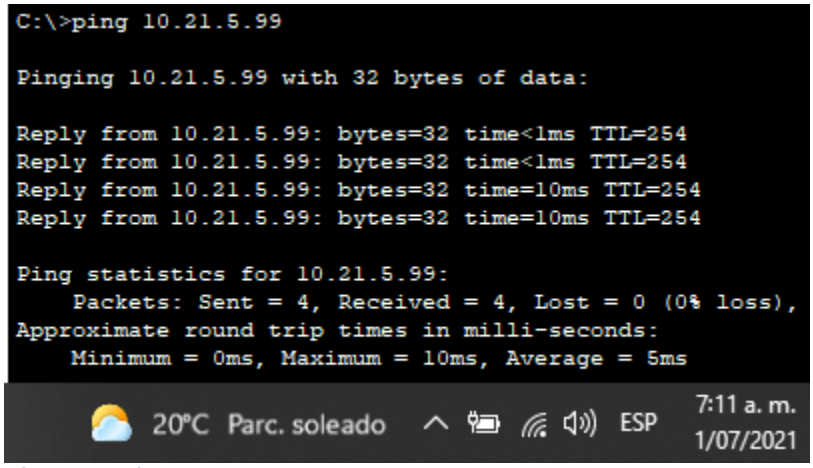


Figura 11 Ping PC-B-S2-10.21.5.99

Desde	A	de Internet	Dirección IP	Resultados de ping
PC-A	R1, G0/0/1.2	Dirección	10.21.5.1	*SI*
		IPv6	2001:db5:acad:a: :1	
	R1, G0/0/1.3	Dirección	10.21.5.65	*SI*
		IPv6	2001:db5:acad:b: :1	
	R1, G0/0/1.4	Dirección	10.21.5.97	*Si*
		IPv6	2001:db5:acad:c: :1	
	S1, VLAN 4	Dirección	10.21.5.98	*SI*
		IPv6	2001:db5:acad:c: :98	
	S2, VLAN 4	Dirección	10.21.5.99.	*SI*
		IPv6	2001:db5:acad:c: :99	
	PC-B	Dirección	IP address will vary.	*SI*
		IPv6	2001:db5:acad:b: :50	
	R1 Bucle 0	Dirección	209.165.201.1	
Desde	**A**	**de Internet**	**Dirección IP**	**Resultados de ping**
		IPv6	2001:db5:acad:209: :1	
PC-B	R1 Bucle 0	Dirección	209.165.201.1	
		IPv6	2001:db5:acad:209: :1	
	R1, G0/0/1.2	Dirección	10.21.5.1	*SI*
		IPv6	2001:db5:acad:a: :1	
	R1, G0/0/1.3	Dirección	10.21.5.65	*SI*
		IPv6	2001:db5:acad:b: :1	
	R1, G0/0/1.4	Dirección	10.21.5.97	*SI*

		IPv6	2001:db5:acad:c: :1	
	S1, VLAN 4	Dirección	10.21.5.98	*SI*
		IPv6	2001:db5:acad:c: :98	
	S2, VLAN 4	Dirección	10.21.5.99.	*SI*
		IPv6	2001:db5:acad:c: :99	

Tabla 5-resultados de ping

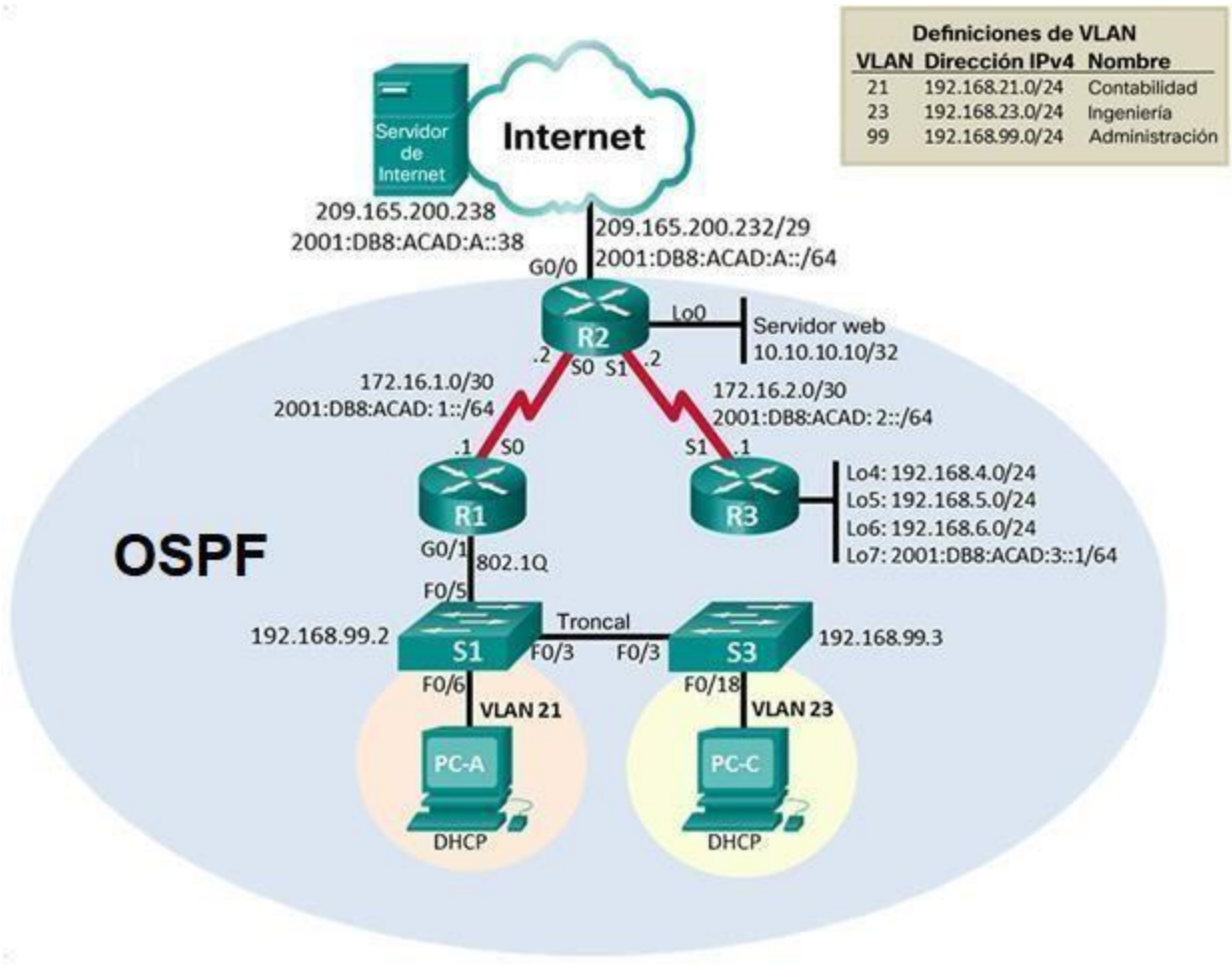
2 PLANTEAMIENTO DEL PROBLEMA – ESCENARIO 2

2.1 PLANTEAMIENTO ESPECÍFICO DEL PROBLEMA – ESCENARIO 2

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



2.2 Desarrollo específico del problema – Escenario 2

2.3 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.

1.1. Eliminar el archivo startup-config de todos los routers

```
Router>en
Router#erase startup-config
```

1.2. Volver a cargar todos los routers

```
Router#reload
```

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

```
Switch>en
Switch#erase startup-config
Switch#delete vlan.dat
```

1.4. Volver a cargar ambos switches

```
Switch#reload
```

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

```
Switch#dir flash:
```

2.4 Configurar los parámetros básicos de los dispositivos

Paso 1: Configurar la computadora de Internet

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

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.225
Dirección IPv6/subred	2001:DB8:ACAD:A::38 /64
Gateway predeterminado IPv6	2001:DB8:ACAD:2::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.

Paso 2: Configurar R1 - Las tareas de configuración para R1 incluyen las siguientes:

2.1. Desactivar la búsqueda DNS

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

2.2. Nombre del router

```
Router(config)#hostname R1
```

2.3. Contraseña de exec privilegiado cifrada

```
R1(config)#enable secret class
```

2.4. Contraseña de acceso a la consola

```
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#
```

2.5. Contraseña de acceso Telnet

```
R1(config)#line vty 0 15
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
```

2.6. Cifrar las contraseñas de texto no cifrado

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

2.7. Mensaje MOTD

```
R1(config)#banner motd ‘Prohibido el acceso no autorizado’
```

2.8. Configuración de la Interfaz S0/0/0

```
R1(config)# int  s0/0/0
R1(config-if)#description R1 --> R2
```

```
R1(config-if)#ip address 172.16.1.1 255.255.255.252
R1(config-if)#ipv6 address 2001:db8:acad:1::1/64
R1(config-if)# clock rate 128000
R1(config-if)#no shutdown
R1(config-if)#exit
```

2.9. Rutas predeterminadas

```
R1(config)#ip    route    0.0.0.0    0.0.0.0    s0/0/0
R1(config)# ipv6 route ::/0 s0/0/0
```

Nota: Todavía no configure G0/1.

2.5 Configurar R2

La configuración del R2 incluye las siguientes tareas:

3.1. Desactivar la búsqueda DNS

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

3.2. Nombre del router

```
Router(config)#hostname R2
R2(config)#
```

3.3. Contraseña de exec privilegiado cifrada

```
R2(config)#enable secret class
```

3.4. Contraseña de acceso a la consola

```
R2(config)#line console 0
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#exit
R2(config)#
```

3.5. Contraseña de acceso Telnet

```
R2(config)#line vty 0 15
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#exit
```

3.6. Cifrar las contraseñas de texto no cifrado

```
R2(config)#service password-encryption
```

3.7. Mensaje MOTD

```
R2(config)#banner motd 'Prohibido el acceso no autorizado'
```

3.8. Configuración de la Interfaz S0/0/0

```
R2(config)# int  s0/0/0
R2(config-if)#description R2 --> R1
R2(config-if)#ip address 172.16.1.2 255.255.255.252
R2(config-if)#ipv6 address 2001:db8:acad:1::2/64
R2(config-if)# clock rate 128000
R2(config-if)#no shutdown
R2(config-if)#exit
```

3.9. Configuración de la Interfaz S0/0/1

```
R2(config)# int  s0/0/1
R2(config-if)#description R2 --> R3
R2(config-if)#ip address 172.16.2.1 255.255.255.252
R2(config-if)#ipv6 address 2001:db8:acad:2::1/64
R2(config-if)# clock rate 128000
R2(config-if)#no shutdown
R2(config-if)#exit
```

3.10. Configuración de la Interfaz G0/0

```
R2(config)# int  g0/0
R2(config-if)#description R2 --> Internet
R2(config-if)#ip address 209.165.200.232 255.255.255.248
R2(config-if)#ipv6 address 2001:db8:acad:A::1/64
R2(config-if)#no shutdown
R2(config-if)#exit
```

3.11. Configuración de la Interfaz loopback 0

```
R2(config)# int  loopback  0
R2(config-if)#description R2 --> Loopback 0
R2(config-if)#ip address 10.10.10.10 255.255.255.255
R2(config-if)#exit
```

3.12. Rutas predeterminadas

```
R2(config)#ip    route    0.0.0.0    0.0.0.0    g0/0
R2(config)# ipv6 route ::/0 g0/0
```

2.6 Configurar R3

La configuración del R3 incluye las siguientes tareas:

4.1. Desactivar la búsqueda DNS

```
Router>en
```

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

4.2. Nombre del router

```
Router(config)#hostname R3
R3(config)#
```

4.3. Contraseña de exec privilegiado cifrada

```
R3(config)#enable secret class
```

4.4. Contraseña de acceso a la consola

```
R3(config)#line console 0
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#exit
R3(config)#
```

4.5. Contraseña de acceso Telnet

```
R3(config)#line vty 0 15
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#exit
```

4.6. Cifrar las contraseñas de texto no cifrado

```
R3(config)#service password-encryption
```

4.7. Mensaje MOTD

```
R3(config)#banner motd ‘Prohibido el acceso no autorizado’
```

4.8. Configuración de la Interfaz S0/0/1

```
R3(config)# int  s0/0/1
R3(config-if)#description R3 --> R2
R3(config-if)#ip address 172.16.2.2 255.255.255.252
R3(config-if)#ipv6 address 2001:db8:acad:2::2/64
R3(config-if)#no shutdown
R3(config-if)#exit
```

4.9. Configuración de la Interfaz loopback 4

```
R3(config)# int  loopback  4
R3(config-if)#description R3 --> Loopback 4
R3(config-if)#ip address 192.168.4.1 255.255.255.0  R3(config-if)#exit
```

4.10. Configuración de la Interfaz loopback 5

```
R3(config)# int  loopback  5
R3(config-if)#description R3 --> Loopback 5
R3(config-if)#ip address 192.168.5.1 255.255.255.0
R3(config-if)#exit
```

4.11. Configuración de la Interfaz loopback 6

```
R3(config)# int  loopback  6
R3(config-if)#description R3 --> Loopback 6
R3(config-if)#ip address 192.168.6.1 255.255.255.0
R3(config-if)#exit
```

4.12. Configuración de la Interfaz loopback 7

```
R3(config)# int  loopback  7
R3(config-if)#description R3 --> Loopback 7
```

```
R3(config-if)# ipv6 address 2001:db8:acad:3::1/64
R3(config-if)#exit
```

4.13. Rutas predeterminadas

```
R3(config)#ip    route    0.0.0.0    0.0.0.0    s0/0/1
R3(config)# ipv6 route ::/0 s0/0/1
```

2.7 Configurar S1

La configuración del S1 incluye las siguientes tareas:

5.1. Desactivar la búsqueda DNS

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

5.2. Nombre del switch

```
Switch(config)#hostname S1
S1(config)#
```

5.3. Contraseña de exec privilegiado cifrada

```
S1(config)#enable secret class
```

5.4. Contraseña de acceso a la consola

```
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#exit
S1(config)#
```

5.5. Contraseña de acceso Telnet

```
S1(config)#line vty 0 15
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#exit
```

5.6. Cifrar las contraseñas de texto no cifrado

```
S1(config)#service password-encryption
```

5.7. Mensaje MOTD

```
S1(config)#banner motd 'Prohibido el acceso no autorizado'
S1(config)#
```

2.8 Configurar S3

La configuración del S3 incluye las siguientes tareas:

6.1. Desactivar la búsqueda DNS

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

6.2. Nombre del switch

```
Switch(config)#hostname S3
S3(config)#
```

6.3. Contraseña de exec privilegiado cifrada

```
S3(config)#enable secret class
```

6.4. Contraseña de acceso a la consola

```
S3(config)#line console 0
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#exit
S3(config)#
```

6.5. Contraseña de acceso Telnet

```
S3(config)#line vty 0 15
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#exit
```

6.6. Cifrar las contraseñas de texto no cifrado

```
S3(config)#service password-encryption
```

6.7. Mensaje MOTD

```
S3(config)#banner motd 'Prohibido el acceso no autorizado'
```

2.9 Verificar la conectividad de la red

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

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

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	R1#ping 172.16.1.2 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
R2	R3, S0/0/1	172.16.2.2	R2#ping 172.16.2.2 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 172.16.2.2, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/7 ms
PC de Internet	Gateway predeterminado	209.165.200.225	….

Tabla 6- conectividad entre los dispositivos

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

2.10 Configurar la seguridad del switch, las vlan y el routing entre vlan

Paso 1: Configurar S1 - La configuración del S1 incluye las siguientes tareas:

1.1. 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

```
S1>en
S1#conf t
S1(config)#vlan 21
S1(config-vlan)#name Contabilidad
S1(config-vlan)#vlan 23
S1(config-vlan)#name Ingeniería
S1(config-vlan)#vlan 99
S1(config-vlan)#name Administración
S1(config-vlan)#exit
S1(config)#
```

1.2. 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

```
S1(config)#int vlan 99
S1(config-if)#ip address 192.168.99.2 255.255.255.0
S1(config-if)#
```

1.3. Asignar el gateway predeterminado - Asigne la primera dirección IPv4 de la subred como el gateway predeterminado.

```
S1(config-if)#ip default-gateway 192.168.99.1
S1(config)#
```

1.4. Forzar el enlace troncal en la interfaz F0/3 - Utilizar la red VLAN 1 como VLAN native

```
S1(config)#int f0/3
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 1
S1(config-if)#exit
```

1.5. Forzar el enlace troncal en la interfaz F0/5 - Utilizar la red VLAN 1 como VLAN native

```
S1(config)#int f0/5
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 1
S1(config-if)#exit
```

1.6. Configurar el resto de los puertos como puertos de acceso - Utilizar el comando interface range

```
S1(config)#int range f0/1-2, f0/4, f0/6-24, g0/1-2
S1(config-if-range)#switchport mode access
S1(config-if-range)#exit
```

1.7. Asignar F0/6 a la VLAN 21

```
S1(config)#int f0/6
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 21
S1(config-if)#exit
```

1.8. Apagar todos los puertos sin usar

```
S1(config)#int range f0/1-2, f0/4, f0/7-24, g0/1-2
S1(config-if-range)#shutdown
S1(config-if-range)#exit
```

2.11 configurar el S3

La configuración del S3 incluye las siguientes tareas:

2.1. 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.

```
S3>en
S3#conf t
S3(config)#vlan 21
S3(config-vlan)#name Contabilidad
S3(config-vlan)#vlan 23
S3(config-vlan)#name Ingeniería
S3(config-vlan)#vlan 99
S3(config-vlan)#name Administración
S3(config-vlan)#exit
S3(config)#
```

2.2. 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

```
S3(config)#int vlan 99
S3(config-if)#ip address 192.168.99.3 255.255.255.0
S3(config-if)#
```

2.3. Asignar el gateway predeterminado - Asignar la primera dirección IP en la subred como gateway predeterminado.

```
S3(config-if)#ip default-gateway 192.168.99.1
S3(config)#
```

2.4. Forzar el enlace troncal en la interfaz F0/3 - Utilizar la red VLAN 1 como VLAN native

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

2.5. Configurar el resto de los puertos como puertos de acceso - Utilizar el comando interface range

```
S3(config)#int range f0/1-2, f0/4-17, f0/19-24, g0/1-2
S3(config-if-range)#switchport mode access
```

2.6. Asignar F0/18 a la VLAN 23

```
S3(config)#int f0/18
S3(config-if)#switchport mode access
S3(config-if)#switchport access vlan 23
S3(config-if)#exit
```

2.7. Apagar todos los puertos sin usar

```
S3(config)#int range f0/1-2, f0/4-17, f0/19-24, g0/1-2
S3(config-if-range)#shutdown
S3(config-if-range)#exit
```

2.12 configurar el R1

Las tareas de configuración para R1 incluyen las siguientes:

3.1. Configurar la subinterfaz 802.1Q .21 en G0/1 – Descripción: LAN de Contabilidad - Asignar la VLAN 21 - Asignar la primera dirección disponible a esta interfaz.

```
R1>en
R1#conf t
R1(config)#int g0/1.21
R1(config-subif)#encapsulation dot1Q 21
R1(config-subif)#description LAN de Contabilidad
R1(config-subif)#ip address 192.168.21.1 255.255.255.0
R1(config-subif)#exit
```

3.2. Configurar la subinterfaz 802.1Q .23 en G0/1 - Descripción: LAN de Ingeniería - Asignar la VLAN 23 - Asignar la primera dirección disponible a esta interfaz.

```
R1(config)#int g0/1.23
R1(config-subif)#encapsulation dot1Q 23
R1(config-subif)#description LAN de Ingeniería
R1(config-subif)#ip address 192.168.23.1 255.255.255.0
R1(config-subif)#exit
```

3.3. Configurar la subinterfaz 802.1Q .99 en G0/1 - Descripción: LAN de Administración - Asignar la VLAN 99 - Asignar la primera dirección disponible a esta interfaz.

```
R1(config)#int g0/1.99
R1(config-subif)#encapsulation dot1Q 99
R1(config-subif)#description LAN de Administración
R1(config-subif)#ip address 192.168.99.1 255.255.255.0
R1(config-subif)#exit
```

3.4. Activar la interfaz G0/1

```
R1(config)#int g0/1
R1(config-if)#no shutdown
```

2.13 Verificar la conectividad de la red

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

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

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	S1#ping 192.168.99.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds: .!!!! Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms
S3	R1, dirección VLAN 99	192.168.99.1	S3# S3#ping 192.168.99.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds: .!!!! Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/2 ms

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

Tabla 7- conectividad entre los switches y el R1

2.14 Configurar el protocolo de routing dinámico OSPF

Paso 1: Configurar OSPF en el R1 - Las tareas de configuración para R1 incluyen las siguientes:

1.1. Configurar OSPF área 0

```
R1>en
R1#config t
R1(config)#router ospf 1
R1(config-router)#router-id 1.1.1.1
R1(config-router)#
```

1.2. Anunciar las redes conectadas directamente - Asigne todas las redes conectadas directamente.

```
R1(config-router)#network 172.16.1.0 0.0.0.3 area 0
R1(config-router)#network 192.168.21.0 0.0.0.255 area 0
R1(config-router)#network 192.168.23.0 0.0.0.255 area 0
R1(config-router)#network 192.168.99.0 0.0.0.255 area 0
R1(config-router)#
```

1.3. Establecer todas las interfaces LAN como pasivas

```
R1(config-router)#passive-interface g0/1.21
R1(config-router)#passive-interface g0/1.23
R1(config-router)#passive-interface g0/1.99
R1(config-router)#exit
```

1.4. Desactive la sumarización automática

```
R1(config)#router rip
R1(config-router)#no auto-summary
R1(config-router)#exit
```

2.15 Configurar OSPF en el R2

La configuración del R2 incluye las siguientes tareas:

2.1. Configurar OSPF área 0

```
R2>en
R2#conf t
R2(config)#router ospf 1
R2(config-router)#router-id 2.2.2.2
```

```
R2(config-router)#
```

2.2. Anunciar las redes conectadas directamente - Nota: Omitir la red G0/0.

```
R2(config-router)#network 172.16.1.0 0.0.0.3 area 0
R2(config-router)#network 172.16.2.0 0.0.0.3 area 0
R2(config-router)#network 10.10.10.0 0.0.0.255 area 0
R2(config-router)#
```

2.3. Establecer la interfaz LAN (loopback) como pasiva

```
R2(config-router)#passive-interface g0/1
R2(config-router)#exit
```

2.4. Desactive la sumarización automática

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

2.16 Configurar OSPFV3 EN EL R2

La configuración del R3 incluye las siguientes tareas:

3.1. Configurar OSPF área 0

```
R3>en
R3#conf t
R3(config)#router ospf 1
R3(config-router)#router-id 3.3.3.3
R3(config-router)#
```

3.2. Anunciar redes IPv4 conectadas directamente

```
R3(config-router)#network 172.16.2.0 0.0.0.3 area 0
R3(config-router)#network 192.168.4.0 0.0.3.255 area 0
R3(config-router)#
```

3.3. Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas

```
R3(config-router)#passive-interface loopback 4
R3(config-router)#passive-interface loopback 5
R3(config-router)#passive-interface loopback 6
R3(config-router)#passive-interface loopback 7
R3(config-router)#exit
```

3.4. Desactive la sumarización automática

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

2.17 Verificar la información de OSPF

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

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

2.18 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:

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

```
R1>en
R1#conf t
R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20
R1(config)#
```

1.2. 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
```

1.3. Crear un pool de DHCP para la VLAN 21. - Nombre: ACCT - Servidor DNS: 10.10.10.10 - Nombre de dominio: ccna-sa.com - Establecer el gateway predeterminado.

```
R1(config)#ip dhcp pool ACCT
R1(dhcp-config)#dns-server 10.10.10.10
R1(dhcp-config)#domain-name ccna-sa.com
R1(dhcp-config)#default-router 192.168.21.1
R1(dhcp-config)#exit
```

1.4. Crear un pool de DHCP para la VLAN 23 - Nombre: ENGNR - Servidor DNS: 10.10.10.10 - Nombre de dominio: ccna-sa.com - Establecer el gateway predeterminado.

```
R1(config)#ip dhcp pool ENGNR
R1(dhcp-config)#dns-server 10.10.10.10
R1(dhcp-config)#domain-name ccna-sa.com
R1(dhcp-config)#default-router 192.168.23.1
```

```
R1(dhcp-config)#exit
```

2.19 Configurar la NAT estática y dinámica en el R2

La configuración del R2 incluye las siguientes tareas:

2.1. Crear una base de datos local con una cuenta de usuario - Nombre de usuario: webuser - Contraseña: cisco12345 - Nivel de privilegio: 15.

```
R1(config)#user webuser privilege 15 secret cisco12345
```

2.2. Habilitar el servicio del servidor HTTP

```
R1(config)# ip http server
```
(comando no soportado por packet tracer)

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip http server
                  ^
% Invalid input detected at '^' marker.
```

Figura 12- comando no soportado por packet tracer

2.3. Configurar el servidor HTTP para utilizar la base de datos local para la autenticación

```
R1(config)# ip http authentication local
```

2.4. Crear una NAT estática al servidor web. - Dirección global interna: 209.165.200.229

```
R1(config)#ip nat inside source static 10.10.10.1 209.165.200.229
```

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

```
R1(config)#int g0/0
R1(config-if)#ip nat outside
R1(config-if)#exit
R1(config)#int g0/1
R1(config-if)#ip nat inside
R1(config-if)#exit
```

2.6. Configurar la NAT dinámica dentro de una ACL privada - Lista de acceso: 1 - Permitir la traducción de las redes de Contabilidad y de Ingeniería en el R1 - Permitir la traducción de un resumen de las redes LAN (loopback) en el R3

```
R1(config)#access-list 1 permit 192.168.21.0 0.0.0.255
R1(config)#access-list 1 permit 192.168.23.0 0.0.0.255
R1(config)#access-list 1 permit 192.168.4.0 0.0.3.255
R1(config)#
```

2.7. Defina el pool de direcciones IP públicas utilizables. - Nombre del conjunto: INTERNET - El conjunto de direcciones incluye: 209.165.200.225 – 209.165.200.228.

```
R1(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228
netmask 255.255.255.248
```

2.8. Definir la traducción de NAT dinámica

```
R1(config)#ip nat inside source list 1 pool INTERNET
```

2.20 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.

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

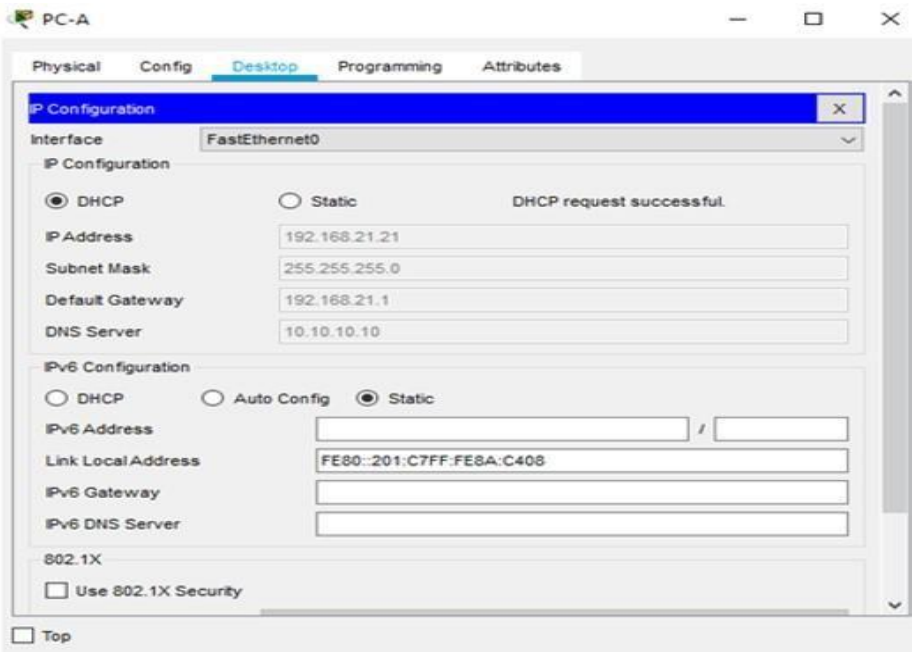


Figura 13- PC-A con información del servidor DHCP

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

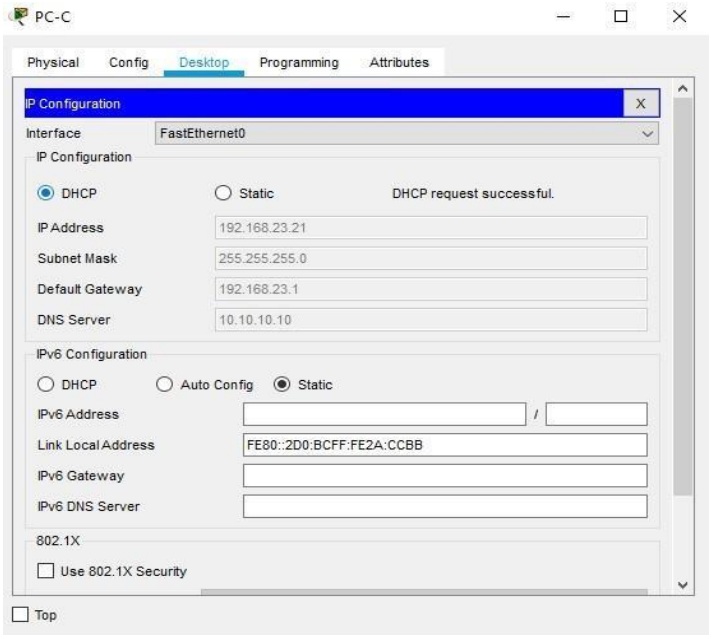


Figura 14- PC-B con información del servidor DHCP

Verificar que la PC-A pueda hacer ping a la PC-C. Nota: Quizá sea necesario deshabilitar el firewall de la PC.

Figura 33. Ping PC-A a PC-C

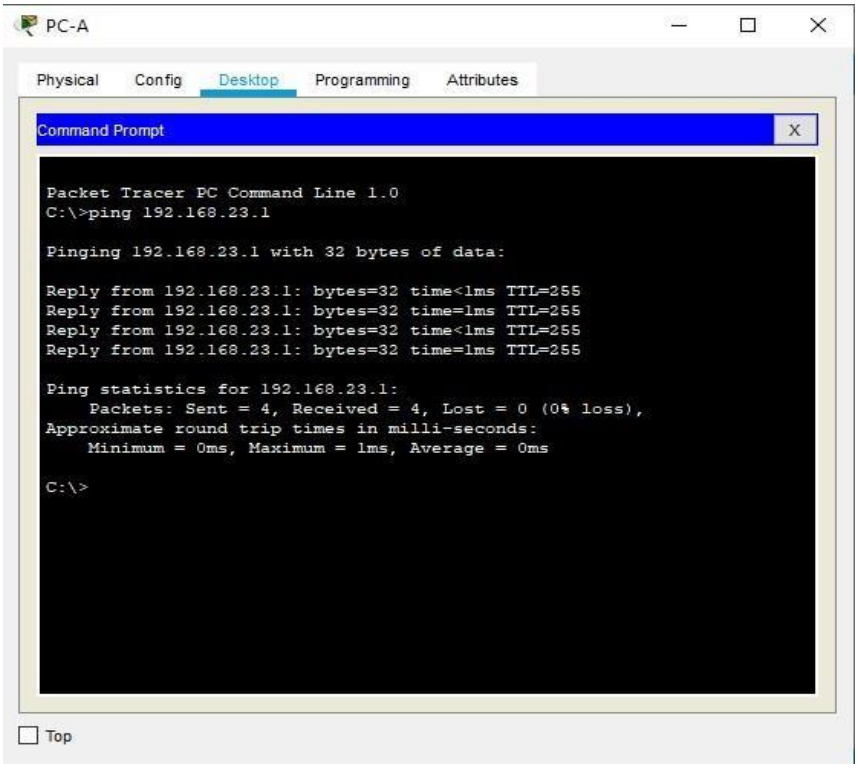


Figura 15- Ping PC-A a PC-C

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

Figura 34. Navegador WEB

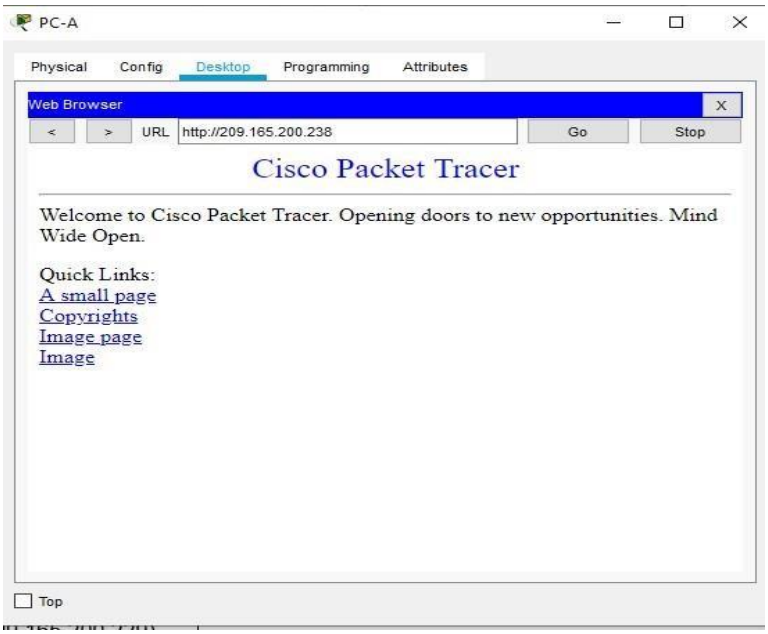


Figura 16- Navegador WEB

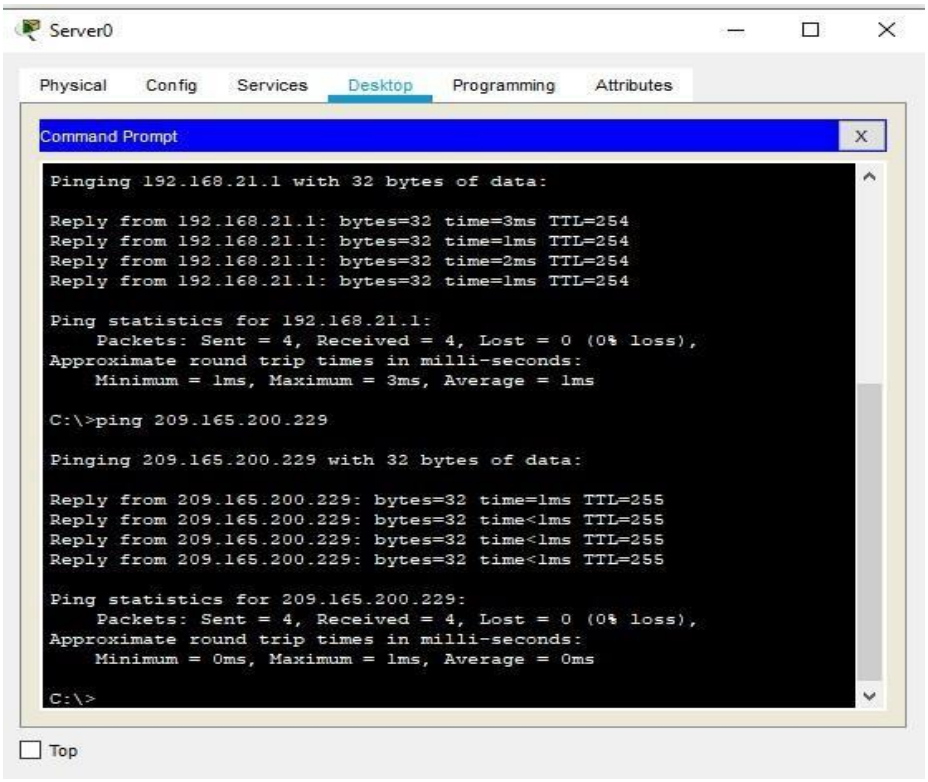


Figura 17-ping 209.165.200.229

2.21 CONFIGURAR NTP

6.1. Ajuste la fecha y hora en R2. - 5 de marzo de 2016, 9 a. m.

```
R2#clock set 09:00:00 5 March 2016
```

6.2. Configure R2 como un maestro NTP. - Nivel de estrato: 5

```
R2(config)#ntp master 5
```

6.3. Configurar R1 como un cliente NTP. - Servidor: R2

```
R1(config)# ntp server 172.16.1.1
```

6.4. Configure R1 para actualizaciones de calendario periódicas con hora NTP.

```
R1(config)# ntp update-calendar
```

6.5. Verifique la configuración de NTP en R1.

```
R1# show ntp associations
```

2.22 Configurar y verificar las listas de control de acceso (ACL)

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

1.1. Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2 - Nombre de la ACL: ADMIN-MGT

```
 R1#conf t
R1(config)#ip access-list standard ADMIN-MGT
R1(config)#host                    172.16.1.1
172.16.1.1(config)#
```

1.2. Aplicar la ACL con nombre a las líneas VTY

```
172.16.1.1(config)#line vty 0 4
172.16.1.1(config-line)#access-class ADMIN-MGT in
172.16.1.1(config-line)#exit
```

1.3. Verificar que la ACL funcione como se espera

```
172.16.1.1(config)#exit
 172.16.1.1#telnet 172.16.2.2
 172.16.1.1#telnet 172.16.2.1
 172.16.1.1#
```

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

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	Show ip access-lists
Restablecer los contadores de una lista de acceso	clear ip access-list counters
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en	show running-config

que se aplica?	
¿Con qué comando se muestran las traducciones NAT?	**Nota:** Las traducciones para la PC-A y la PCC se agregaron a la tabla cuando la computadora de Internet intentó hacer ping a esos equipos en el 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.
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	clear ip nat translation

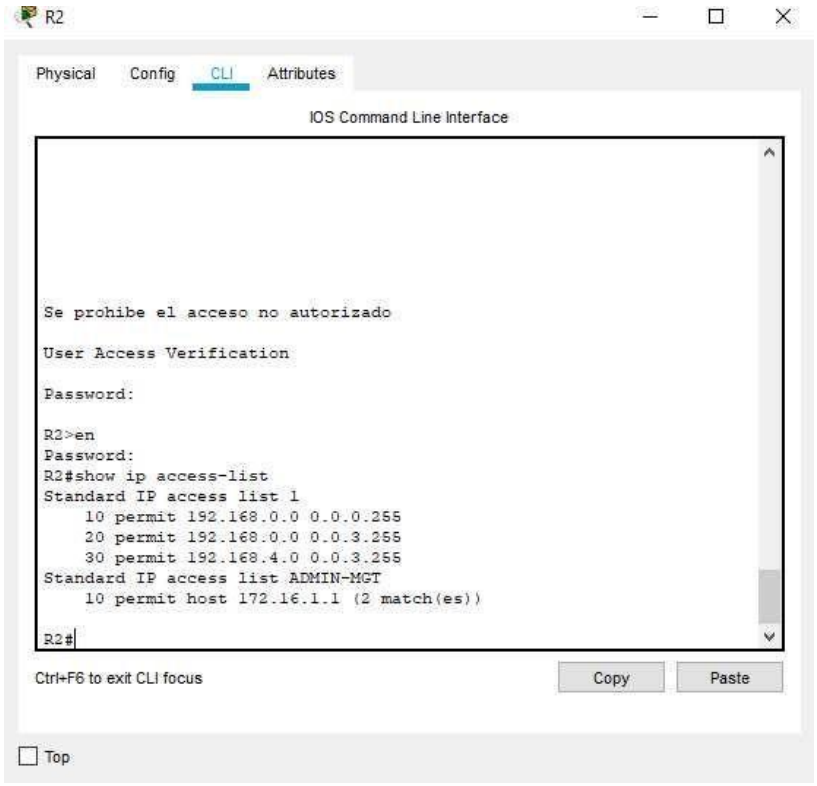


Figura 18- Show ip access-lists

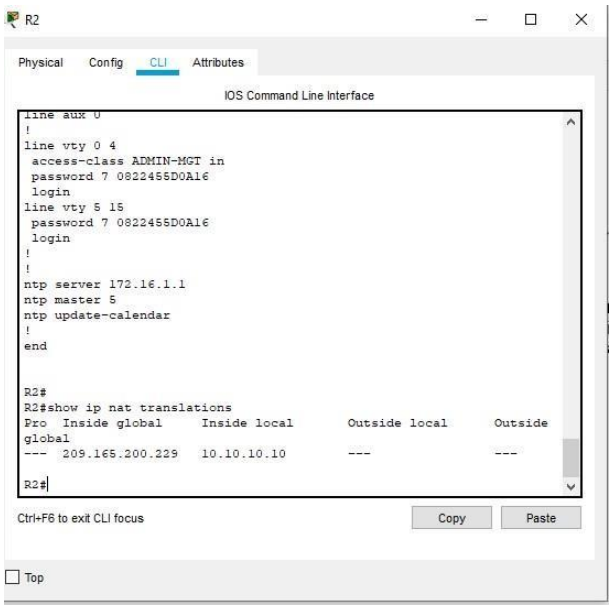


Figura 19- clear ip nat translation

3 PRUEBA DEL SISTEMA

R1 - Show running-config

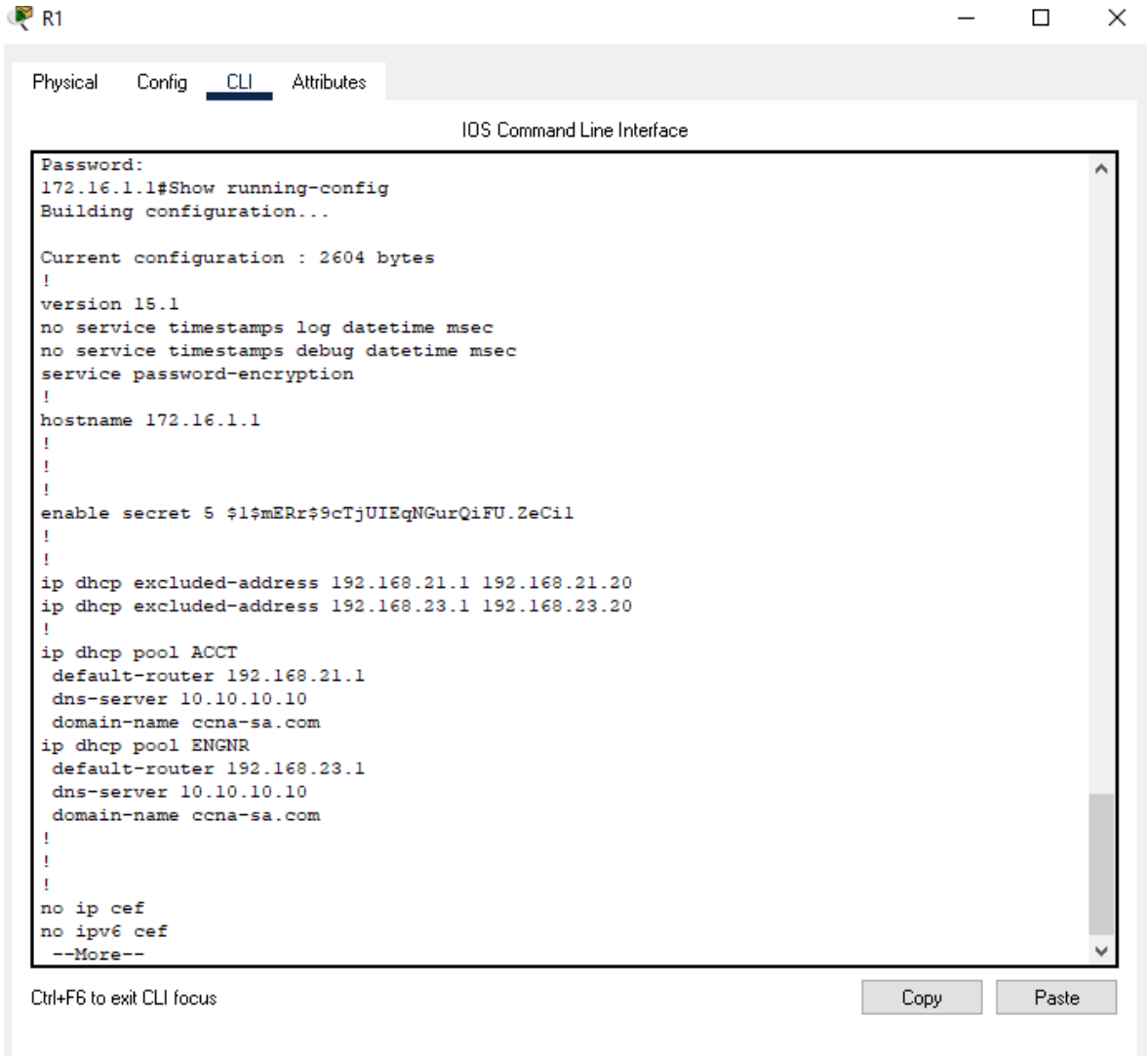


Figura 20-R1 - Show running-config 1

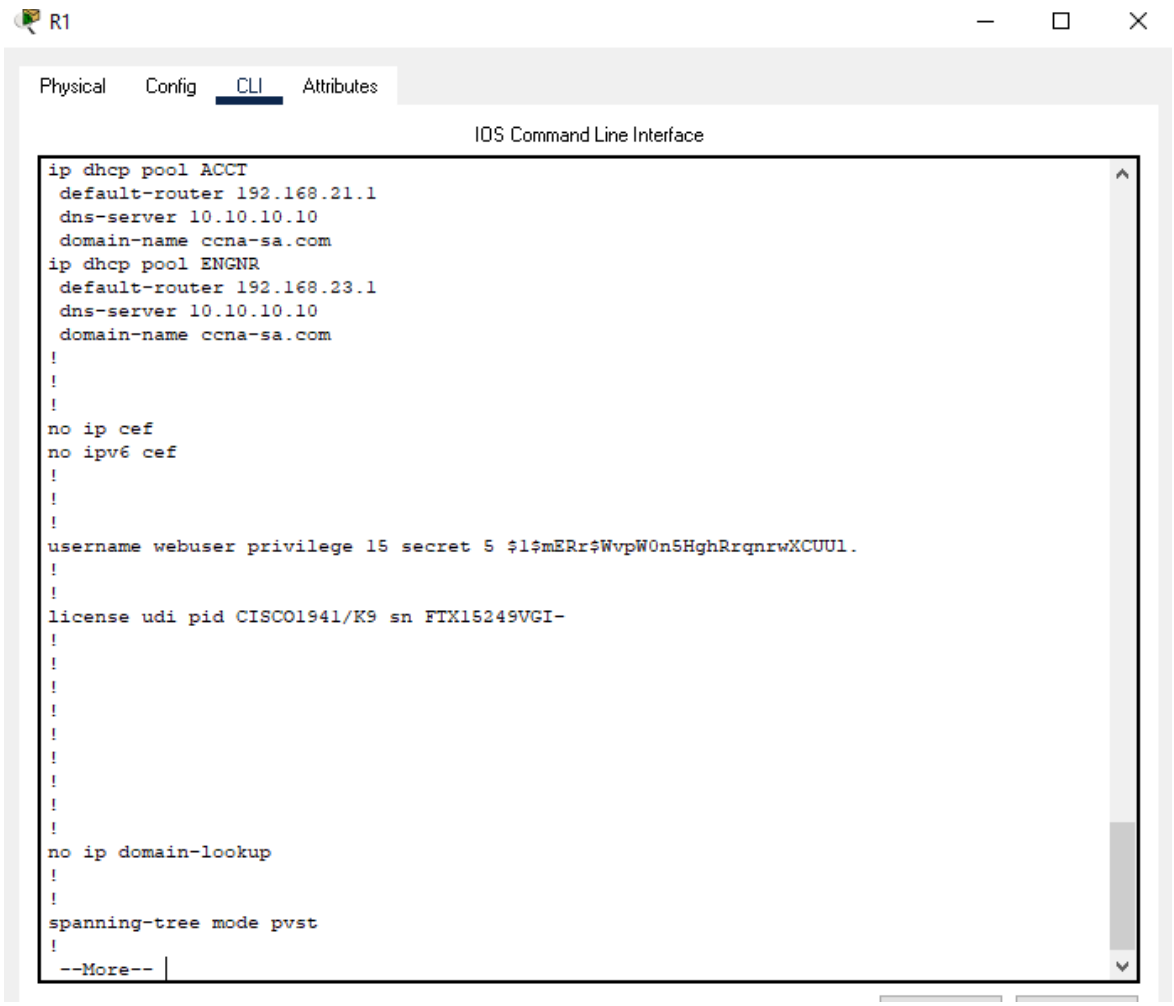


Figura 21 -R1 - Show running-config 2

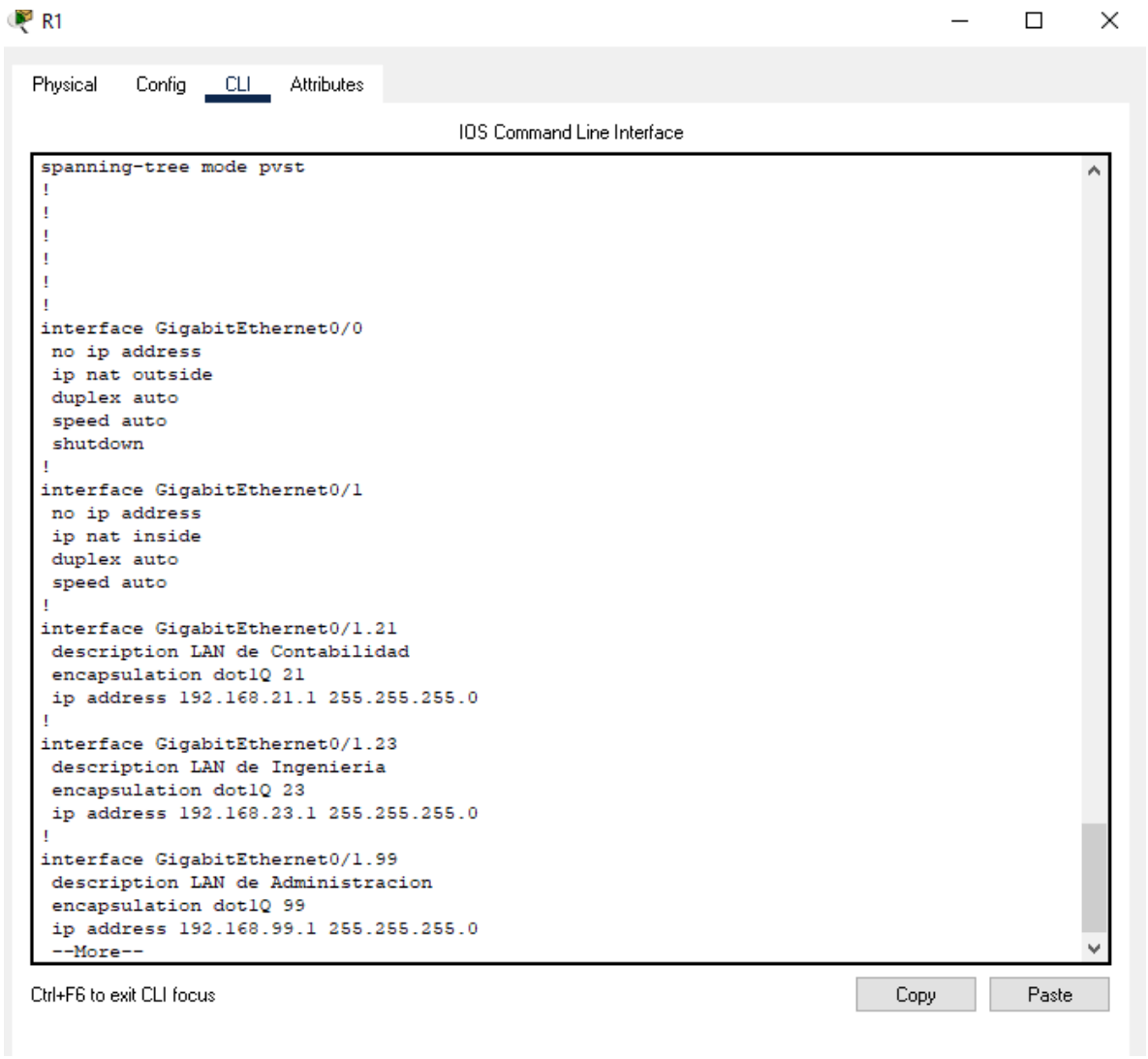


Figura 22-R1 - Show running-config 3

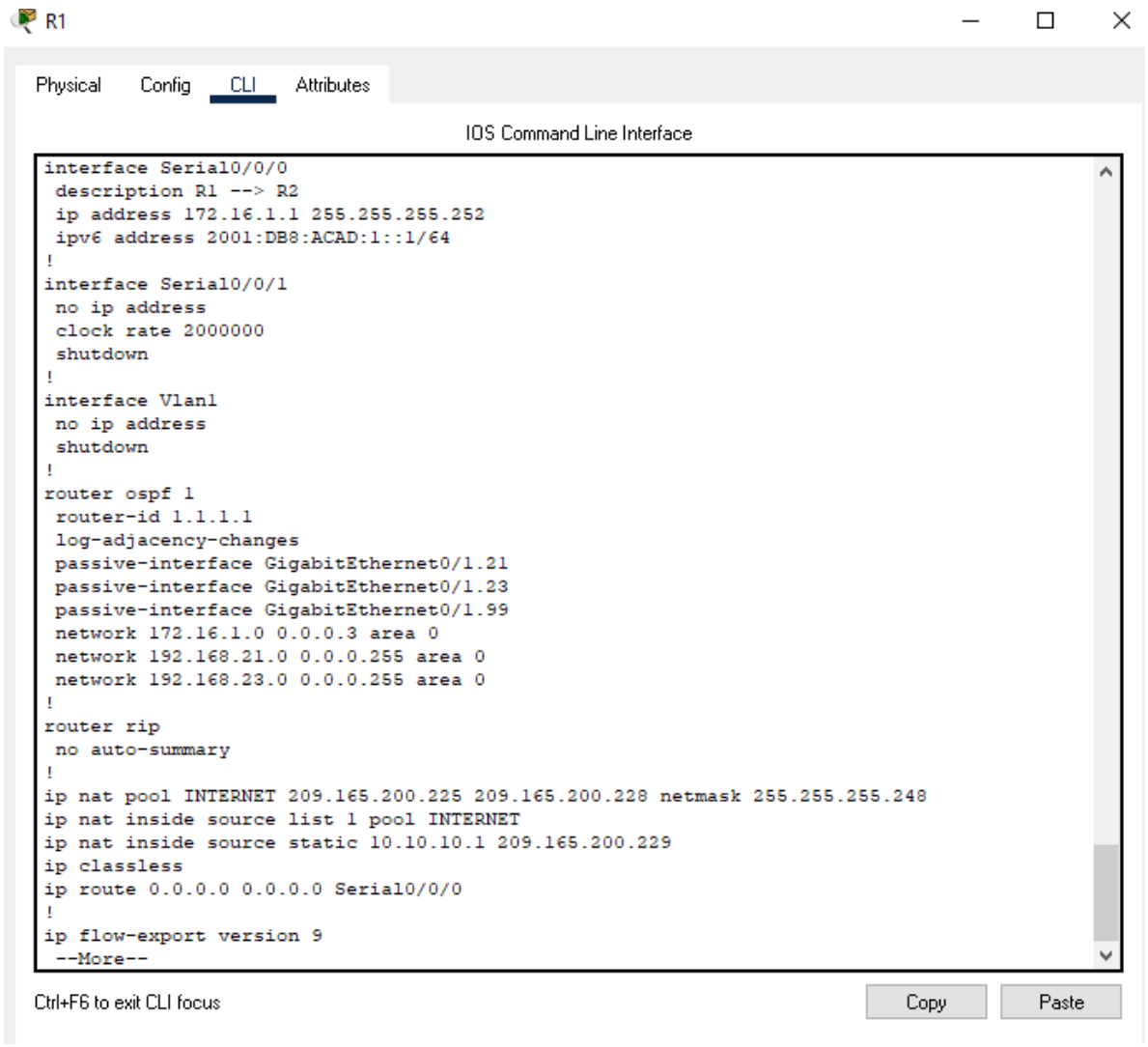


Figura 23-R1 - Show running-config 4

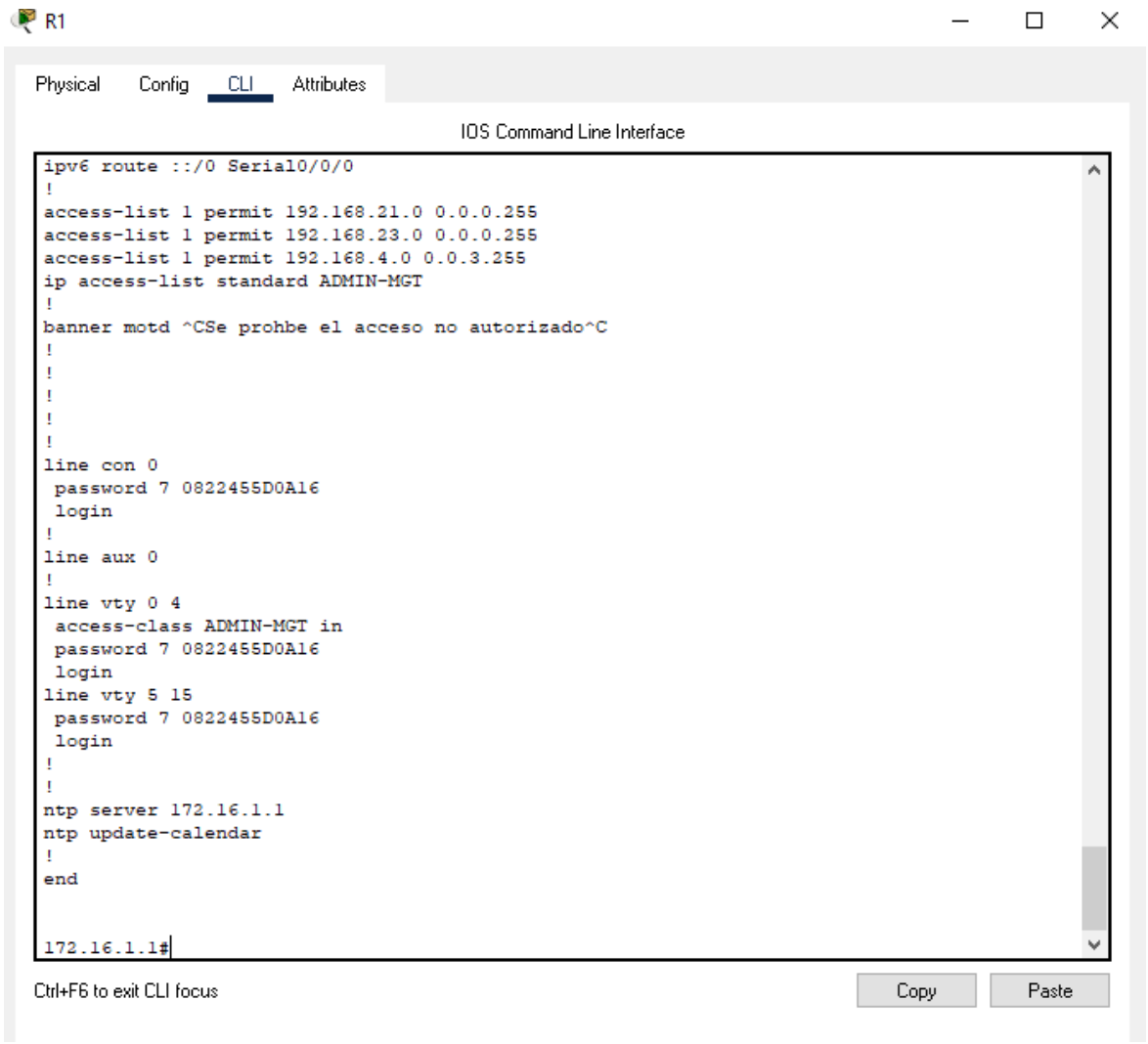


Figura 24-R1 - Show running-config 5

R2 - Show running-config

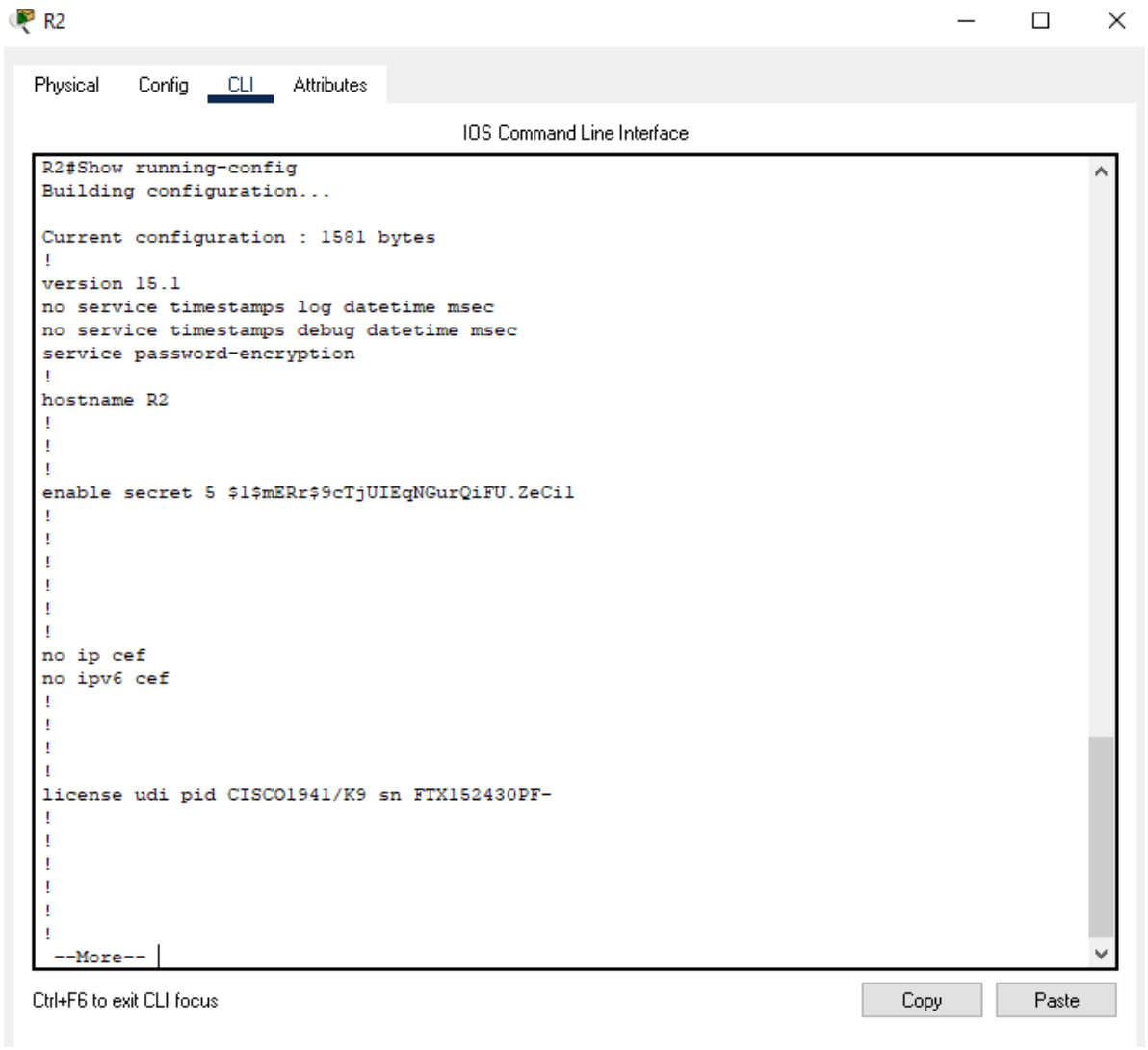


Figura 25-R2 - Show running-config 1 1

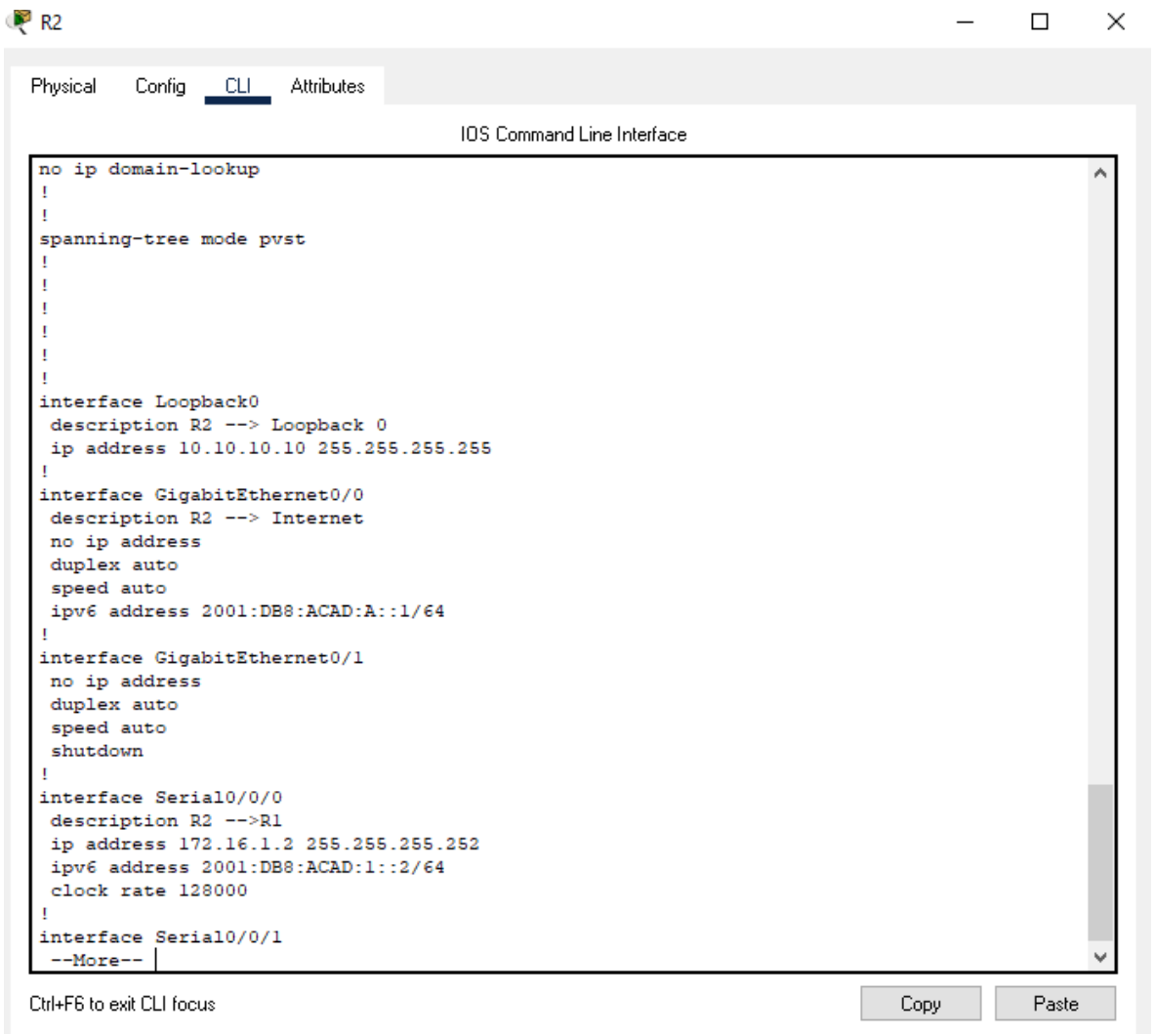


Figura 26-R2 - Show running-config 1 2

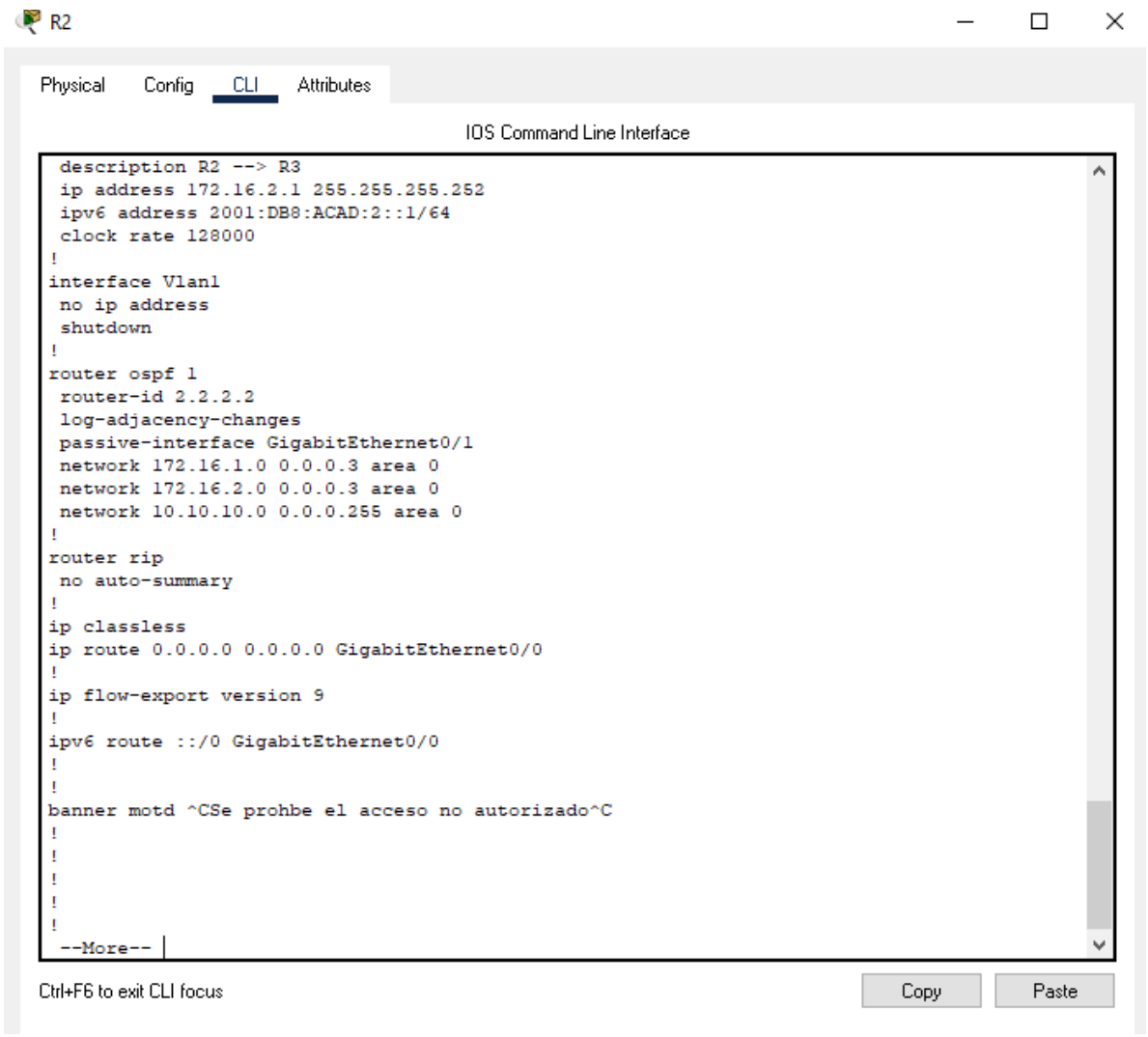


Figura 27-R2 - Show running-config 1 3

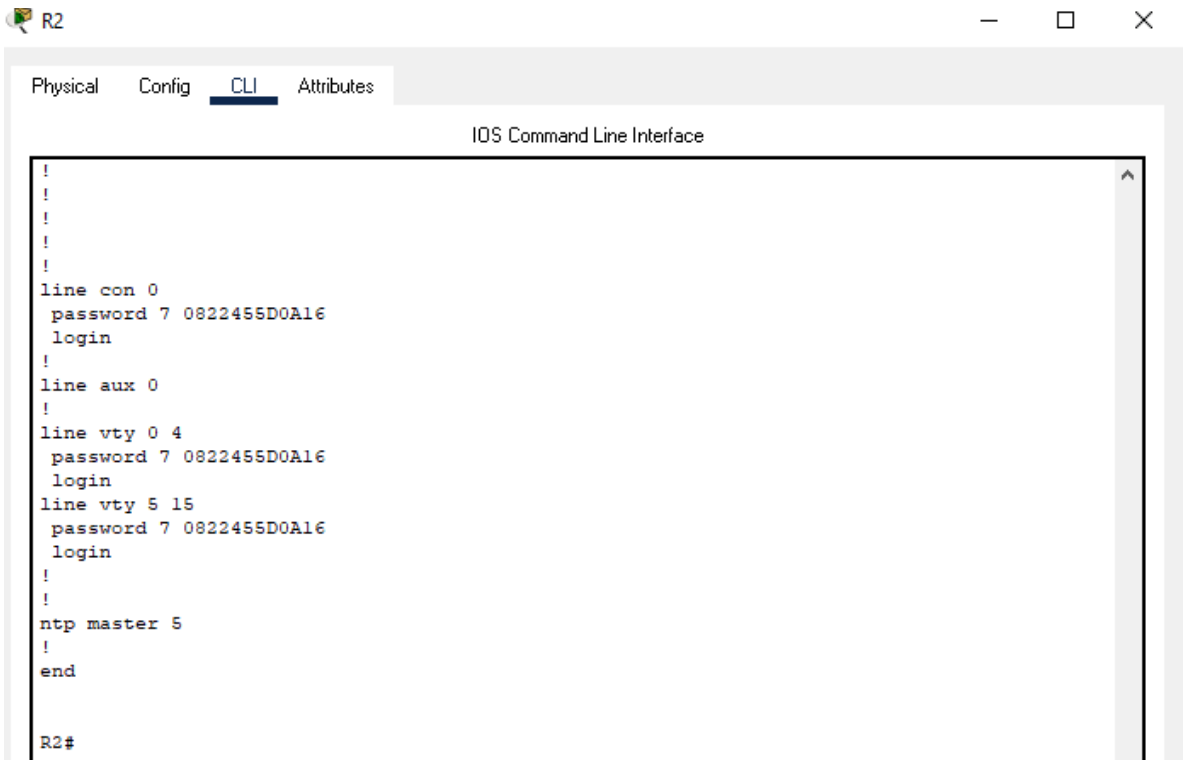


Figura 28-R2 - Show running-config 1 4

R3 - Show running-config

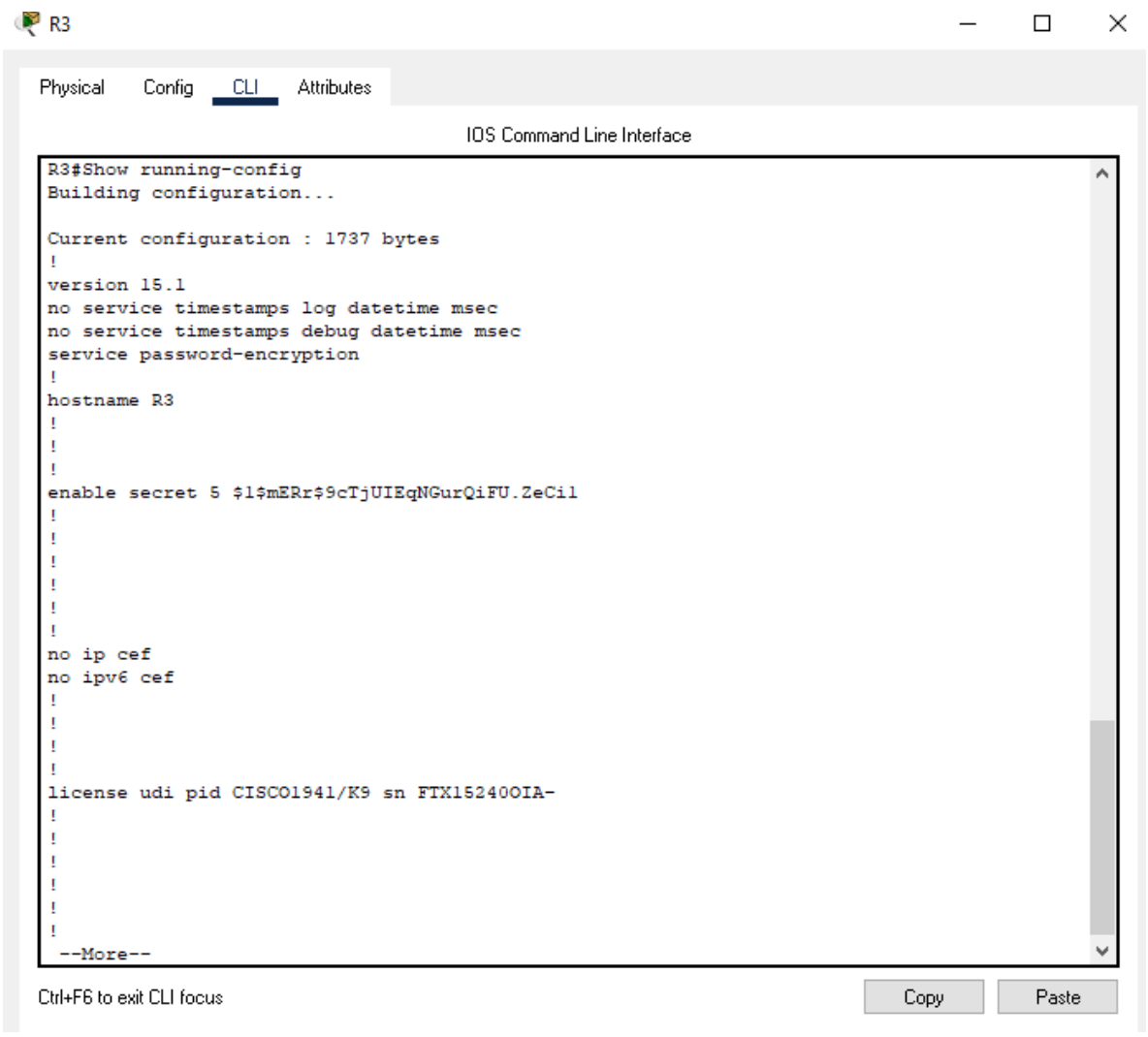


Figura 29-R3 - Show running-config 1 1

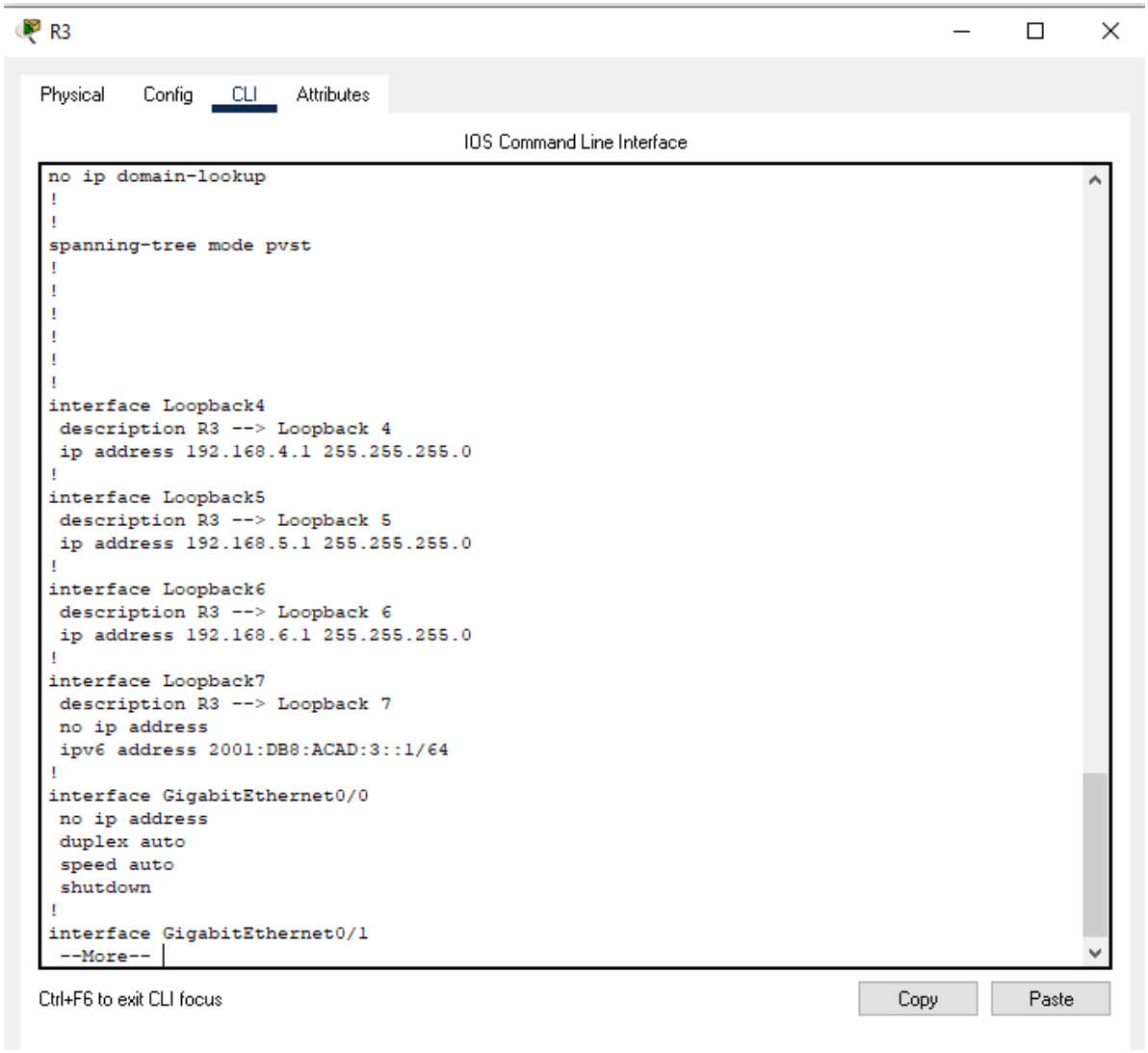


Figura 30-R3 - Show running-config 1 2

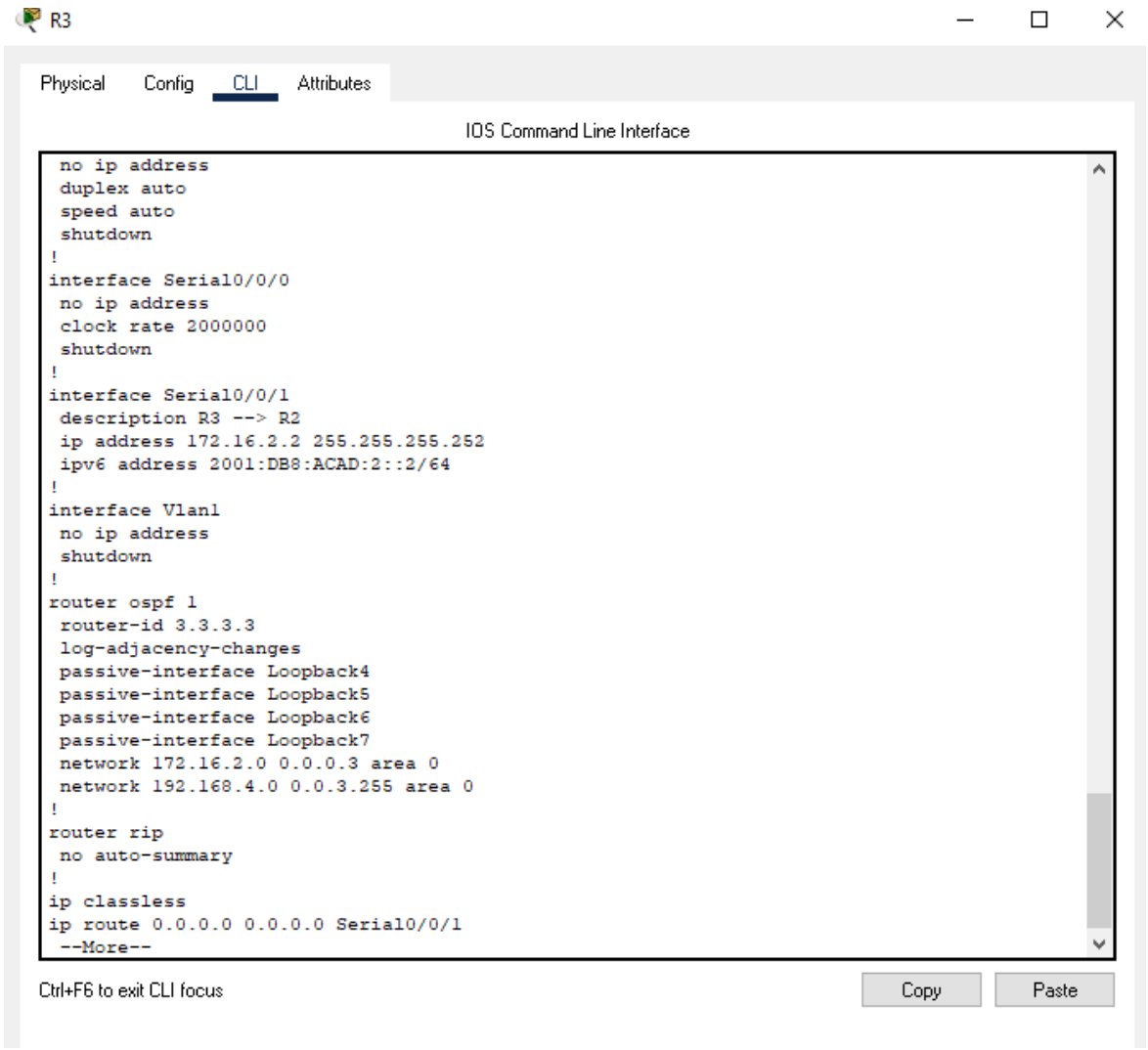


Figura 31-R3 - Show running-config 1 3

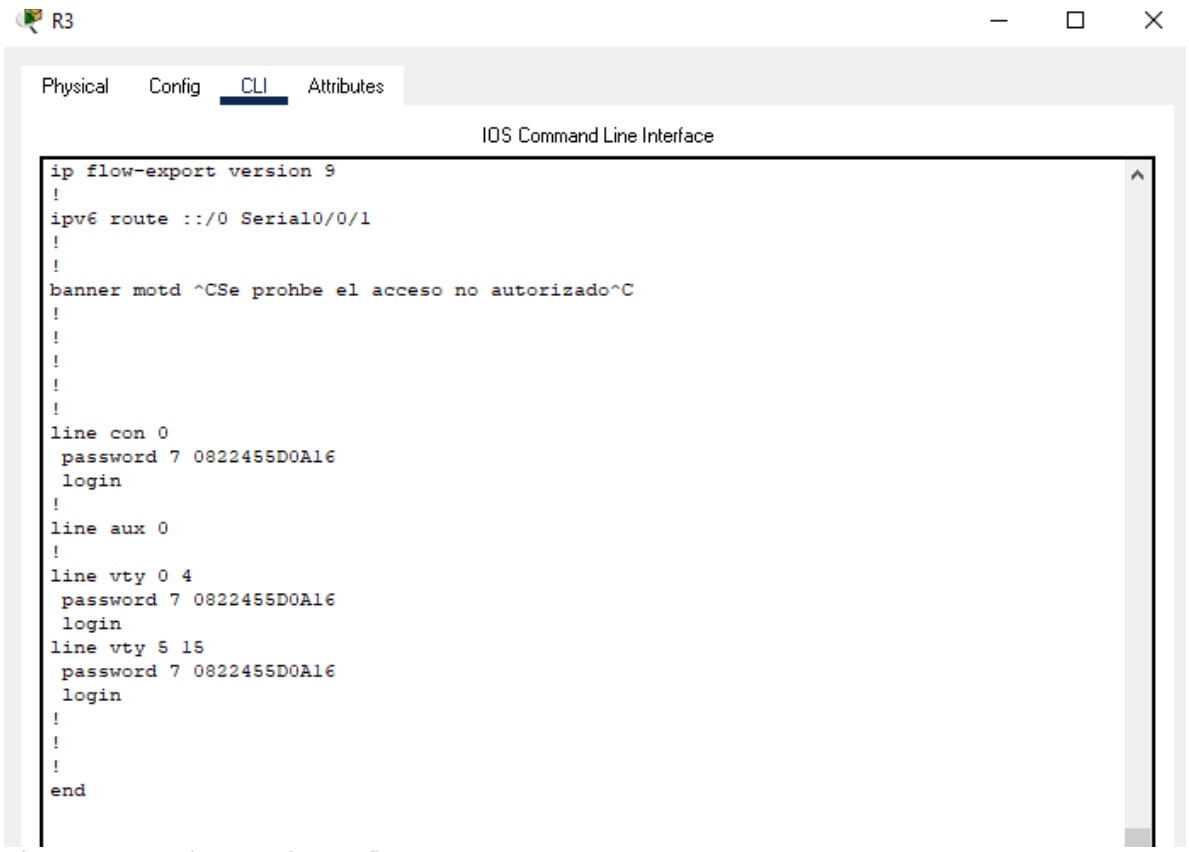


Figura 32-R3 - Show running-config 1 4

4 CONCLUSIONES

En la realización y desarrollo de la práctica de los dos escenarios, se aplicaron los conocimientos adquiridos en el curso del diplomado de profundización CISCO CCNA, buscando alternativas funcionales y propias en el desarrollo de la actividad como conocer la estructura de los equipos para aplicar los protocolos y comandos e implementar una conexión exitosa en la red.

Utilizando el software de simulación Packet Tracer se logra 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. Tanto los Routers y los Switches se configuraron de forma segura para su debida administración. Asignando de manera correcta las direcciones Ip a cada dispositivo donde se configuro el enrutamiento entre VLAN, DHCP, Etherchannel y port-security.

En el momento de dar solución a los escenarios, fue necesario consultar las diferentes fuentes bibliográficas para una mayor orientación sobre los protocolos DHCP y OSPF para lograr una adecuada configuración según lo solicitado en la guía de actividades.

Se llega a la conclusión que a través de la implementación y desarrollo de los escenarios 1 y 2 existen diferentes comandos para realizar la configuración de los diferentes dispositivos aplicando aspectos de Networking, y utilizando comandos como ping el cual procede a verificar la conectividad de extremo a extremo, determinada en una conexión de un host local con al menos un equipo remoto.

Es importante resaltar la experiencia con el simulador de Packet Tracer, el cual me dio una cercanía y similitud con los dispositivos de CISCO y los posibles casos que encontrare en la vida real.

5 BIBLIOGRAFÍA

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

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

CISCO. (2019). Listas de Control de Acceso. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#7

CISCO. (2019). DHCP. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#8

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

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

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

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

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

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

CISCO. (2019). DHCP. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#8

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

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

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

CISCO. (2019). Listas de Control de Acceso. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#7

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

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

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

Estudio y Desarrollo Del Escenario 1- Uso De Tecnología Cisco

Autor: Brayam Baudilio Martínez Perdomo

Estudiante de Ingeniería de Telecomunicaciones

Resumen – En el presente documento encontrara la configuración de un escenario realizado mediante el simulador de Packet Tracer (Cisco), el cual se implementa todos los comandos, reglas y principios para la configuración de una red LAN. Compuesta por un router, dos switch y dos pc; aplicando la conectividad IPV4 e IPV6, el cual serán administrados de forma segura, configurando el enrutamiento entre VLAN, DHCP, Etherchannel y port-security.

Índice de Términos – Lan, host, router, switch, vlan, dhcp, Etherchannel y port-security.

I. INTRODUCCION

En este artículo va detectar una red LAN pequeña, compuesta por 5 equipos (1 Router, 2 Switch y dos PC) el cual se va a configurar paso a paso, siguiendo los lineamientos de CISCO para los equipos desarrollados por ellos pero que en esta ocasión se desarrolla en el simulador de Packet Tracer, software desarrollado por dicha empresa. Se va a configurar los cinco equipos, pero son el router y los dos switch los dispositivos principales para la implementación de la red, estos deben admitir IPV4 e IPV6 para configurar el enrutamiento entre VLAN, DHCP, Etherchannel y port-security**.**

Debemos apuntar que los escenarios virtuales buscan la interacción del individuo con un caso hipotético de la vida real, el cual se asemejaría y debe dar solución a este, aprovechando dicha simulación para corregir los inconvenientes presentados en este espacio. Logrando establecer una conexión correcta por medio de comandos, códigos o instrucciones que requiere el programa y obtener con éxito, el correcto funcionamiento del sistema y llevar acabo la practica virtual al mundo real.

A. Metodología

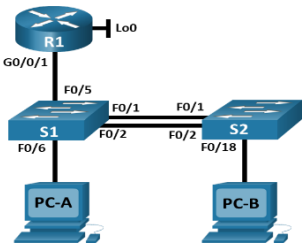
En este documento la metodología que se uso fue la investigación explicativa, en el cual se plantea una simulación de una red LAN, y se desarrollara con el software de Packet Tracer, donde observara detalladamente la explicación de cómo se dio solución a este ejercicio planteado y a la vez proporcionando información para su total desarrollo.

Según el planteamiento y metodología mencionada, se va a configurar una red LAN que consta de un router, dos switch y dos pc, donde por medio de protocolos, enrutamientos y la asignación de redes Vlan, se realizara la comunicación de los dispositivos dentro de la topología de la red. Se procederá con la asignación de nombre de los hosts (router y switch) asignación de direcciones IP, verificando su conectividad a través del código ping entre los dispositivos y se evidenciará su funcionamiento con capturas de pantalla.

B. Exposición del escenario y desarrollo de la topología

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

Figura 1. Topología – Red LAN



C. Desarrollo e implementación de la red

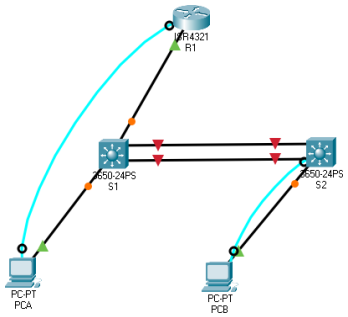


figura 1 - Brayam Martínez 1

Infraestructura de la red – Nombres de Vlan

2. Bikes
3. Trikes
4. Management
5. Parking
6. Native

Tabla 1.
Asignación de direcciones

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

Procedimiento para iniciar, recargar y configurar los aspectos básicos del router y los switchs.

Router R1:

Ini iar y recargar Router
Rou ter>en
Rou ter# era startup-config
Rou ter# reload

No mbre del Router
Rou ter config t
Rou ter (config)# hostname R1

Nombre del Dominio ccna-lab.com

R1(config)# ip domain name ccna-lab.com

Contraseña Modo EXEC Privilegiado y acceso a la consola

R1(config)#enable secret ciscoenpass
R1(config)#line console 0
R1(config-line)#password ciscoconpass
R1(config-line)#login
R1(config-line)#exit
R1(config)#

Longitud mínima para las contraseñas – 10 Caracteres

R1(config)#security passwords min-length 10

Crear un usuario administrativo en la base de datos local - Nombre de usuario: admin - Password: admin1pass

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
R1(config-line)#exit

Cifrar las contraseñas de texto no cifrado

R1(config)#service password-encryption

Configure un MOTD Banner

R1(config)#banner motd #Acceso No Autorizado – No Insista#

Habilitar el routing IPv6

R1(config)#ipv6 unicast-routing

Configurar interfaz G0/1 y subinterfaces

R1(config)# int g0/1.2
R1(config-subif)#encapsulation dot1Q 2
R1(config-subif)#description Vlan-->Bikes
R1(config-subif)#ip address 10.21.5.1 255.255.255.192
R1(config-subif)#ipv6 address 2001:db5:acad:a::1/64
R1(config-subif)#ipv6 address fe80::1 link-local
R1(config-subif)#exit

R1(config)# int g0/1.3
R1(config-subif)#encapsulation dot1Q 3
R1(config-subif)#description Vlan-->Trikes
R1(config-subif)#ip address 10.21.5.65 255.255.255.224
R1(config-subif)#ipv6 address 2001:db5:acad:b::1/64
R1(config-subif)#ipv6 address fe80::1 link-local
R1(config-subif)#exit

R1(config)#int g0/1.4
R1(config-subif)#encapsulation dot1Q 4
R1(config-subif)#description Vlan-->Management
R1(config-subif)#ip address 10.21.5.97 255.255.255.248
R1(config-subif)#ipv6 address 2001:db8:acad:c::1/64
R1(config-subif)#ipv6 address fe80::1 link-local
R1(config-subif)#exit

R1(config)#int g0/1.6
R1(config-subif)#encapsulation dot1Q 6
R1(config-subif)#description Vlan-->Native
R1(config-subif)#exit

R1(config)#int g0/1
R1(config-if)#no shutdown

Configure el Loopback0 interface

R1(config)#int Loopback 0
R1(config-if)#description Loopback
R1(config-if)#ip address 209.165.201.1 255.255.255.224
R1(config-if)#ipv6 address 2001:db8:acad:209::1/64
R1(config-if)#ipv6 address fe80::1 link-local
R1(config-if)#exit

Generar una clave de cifrado RSA - Módulo de 1024 bits

R1(config)#crypto key generate rsa
How many bits in the modulus [512]: 1024

Para la configuración de los Switchs S1 y S2 incluyen tareas que se relacionan con algunos de los pasos del router, donde se va asignar niveles de seguridad, como contraseña cifrada, tanto privilegiado como el de consola. De igual manera se asignará direcciones ip a las interfaces que se van a utilizar en esta topología.

Nota: Solo observara la configuración de S1 con sus respectivos comandos. Puesto que S2 tiene la misma similitud.

Iniciar y recargar Router

En S1
Switch>en
Switch#erase startup-config
Switch#reload

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

En S1 y S2
Switch>en
Switch# config t
Switch(config)# sdm prefer dual-ipv4-and-ipv6 default
Switch(config)#exit
Switch#reload

Desactivar la búsqueda DNS.

En S1 y S2
Switch>en
Switch# config t
Switch(config)#no ip domain-lookup

Nombre del switch – S1 y S2

En S1 y S2
Switch(config)#hostname S1
S1(config)#

Nombre de dominio

En S1 y S2
S1(config)# ip domain name ccna-lab.com

Contraseña cifrada para el modo EXEC privilegiado - ciscoenpass

En S1 y S2

S1(config)# enable secret ciscoenpass

Contraseña de acceso a la consola - ciscoconpass

En S1 y S2
S1(config)# line console 0
S1(config-line)#password ciscoconpass
S1(config-line)#login
S1(config-line)#exit

Crear un usuario administrativo en la base de datos local - Nombre de usuario: admin - Password: admin1pass

En S1 y S2
S1(config)# username admin secret admin1pass

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

En S1 y S2
S1(config)#line vty 0 15
S1(config-line)#login local

Configurar las líneas VTY para que acepten únicamente las conexiones SSH

En S1 y S2
S1(config-line)#transport input ssh
S1(config-line)#exit

Cifrar las contraseñas de texto no cifrado

En S1 y S2
S1(config)# service password-encryption

Configurar un MOTD Banner

En S1 y S2
S1(config)#banner motd #Acceso No Autorizado – No Insista#

Generar una clave de cifrado RSA - Módulo de 1024 bits

En S1 y S2
S1(config)#crypto key generate rsa
How many bits in the modulus [512]: 1024

Configurar la interfaz de administración (SVI)

En S1 y S2
S1(config)#int vlan 4
S1(config-if)#ip address 10.21.5.98 255.255.255.248
S1(config-if)#ipv6 address 2001:db5:acad:c::98/64
S1(config-if)#ipv6 address fe80::98 link-local
S1(config-if)#no shutdown
S1(config-if)#exit

Configuración del gateway predeterminado

En S1 y S2
S1(config)# ip default-gateway 10.21.5.97

D. Creación de Vlans para S1 y S2

Nota: Solo observara la configuración de S1 con sus respectivos comandos. Puesto que S2 tiene la misma similitud.

Crear VLAN
S1(config)#vlan 2
S1(config-vlan)#name Bikes
S1(config-vlan)#vlan 3
S1(config-vlan)#name Trikes

```
S1(config-vlan)#vlan 4
S1(config-vlan)#name Management
S1(config-vlan)#vlan 5
S1(config-vlan)#name Parking
S1(config-vlan)#vlan 6
S1(config-vlan)#name Native
S1(config-vlan)#exit
```

Crear troncos 802.1Q que utilicen la VLAN 6 nativa - Interfaces F0/1, F0/2 y F0/5

```
S1(config)#int f0/1
S1(config-if)#switchport trunk encapsulation dot1q
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 6
S1(config-if)#switchport trunk allowed vlan 2,3,4,5,6
S1(config-if)#exit

S1(config)#int f0/2
S1(config-if)#switchport trunk encapsulation dot1q
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 6
S1(config-if)#switchport trunk allowed vlan 2,3,4,5,6
S1(config-if)#exit


S1(config)#int f0/5
S1(config-if)#switchport trunk encapsulation dot1q
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 6
S1(config-if)#switchport trunk allowed vlan 2,3,4,5,6
S1(config-if)#exit
```

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

```
S1(config)#int f0/1
S1(config-if)#channel-group 1 mode active
S1(config-if)#exit

S1(config)#int f0/2
S1(config-if)#channel-group 1 mode active
S1(config-if)#exit
```

Configurar el puerto de acceso de host para VLAN 2 - Interface F0/6

```
S1(config)#int f0/6
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 maximum 3
```

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

```
S1(config)#int range f0/3-4
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 5
S1(config-if-range)#description Deshabilitada
S1(config-if-range)#no shutdown
S1(config-if-range)#exit

S1(config)#int range f0/7-24
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 5
S1(config-if-range)#description Desabilitada
S1(config-if-range)#no shutdown
S1(config-if-range)#exit

S1(config)#int range g0/1-2
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 5
S1(config-if-range)#description Desabilitada
S1(config-if-range)#no shutdown
S1(config-if-range)#exit
```

A continuación se evidencia los comandos en R1 para la creación de rutas predeterminadas tanto con el protocolo IPV4 e IPV6, el cual tendrá control en el trafico de la interfaz Loopback 0 y la creación DHCP para Vlan 2 y 3.

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
```

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 10.21.5.1 10.19.8.52
R1(config)#ip dhcp pool Vlan2-Bikes
R1(dhcp-config)#network 10.21.5.0 255.255.255.192
R1(dhcp-config)#default-router 10.21.5.1
R1(dhcp-config)#domain-name ccna-a.net
R1(dhcp-config)#exit
```

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 10.21.5.65 10.21.5.84
R1(config)#ip dhcp pool Vlan3-Trikes
R1(dhcp-config)#network 10.21.5.64 255.255.255.224
R1(dhcp-config)#default-router 10.21.5.65
R1(dhcp-config)#domain-name ccna-b.net
R1(dhcp-config)#exit

Para verificar que la configuración anterior realizada a los dispositivos se encuentra correcta se va realizar a utilizar el comando ping entre los dispositivos como se evidencia en las siguientes imágenes.

Ping del PC-A - Router y switch's

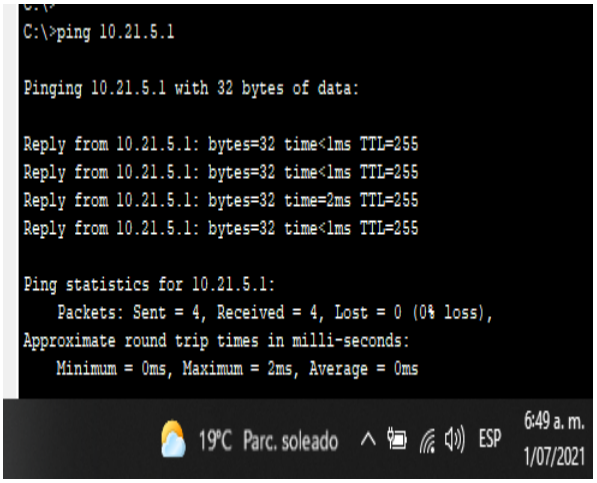


Figura 1-Ping PC-A-R1-10.21.5.1

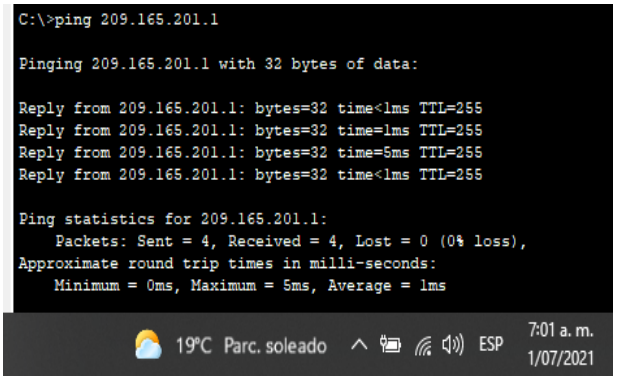


Figura 2- Ping PC-B-R1-209.165.201.1

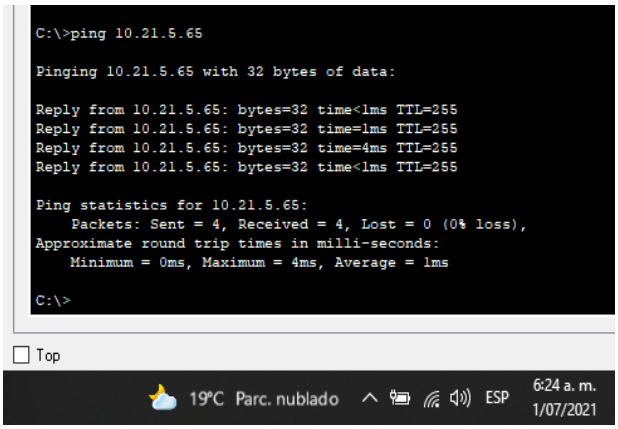


Figura 33- Ping PC-A-R1-10.21.5.65

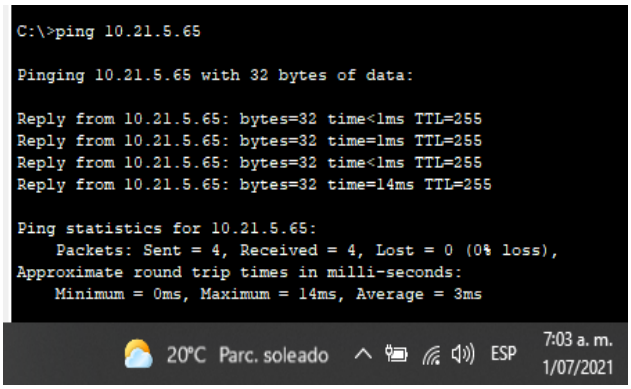


Figura 4- Ping PC-B-R1-10.21.5.65

IX. CONCLUSIÓN

Al realizar una configuración entre dispositivos de una red, sede debe garantizar los niveles de seguridad básicos, como la asignación de contraseñas de manera cifrada para impedir la intrusión de cualquier persona ajena y evitar la alteración y manipulación de la red como sus dispositivos.

Es así que en este trabajo se puso en práctica los conocimientos adquiridos a través del diplomado de profundización cisco CCNA, donde se resalta la estructura de los equipos, su funcionamiento y la referencia que puede o se debe utilizar según la red a implementar y poder explicar adecuadamente la configuración, protocolos y comandos para obtener una conexión exitosa.

Por otro lado, no hubiera servido adquirir tanto conocimiento, sino hubiese puesto en práctica. Gracias al simulador de Packet Tracer, se obtiene experiencias y lo podre aplicar a los casos que se presentes cuando desempeñe mi labor como ingeniero de telecomunicaciones y de esta manera no quedar a la deriva de ¿Qué hago? O ¿Cómo se hace? Por no contar con la experiencia adquirida a través del Software de CISCO y por supuesto de las enseñanzas de los tutores.

RECONOCIMIENTO

Un agradecimiento especial para el Ingeniero Hector Herrera y la Ingeniera Nancy Amparo Guaca que me guiaron durante el procedimiento y Desarrollo del curso, junto con el Desarrollo de los escenarios propuestos.

REFERENCIAS

[1] CISCO. (s.f). Listas de control de acceso. Principios de Enrutamiento y Conmutación. {2017} Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module9/index.html#9.0.1.1

[2] CISCO. Enrutamiento Dinámico. Principios de Enrutamiento y Conmutación. {2017}. Recuperado de https://static-courseassets.s3.amazonaws.com/RSE50ES/module7/index.html#7.0.1.1

[3] CISCO. Configuración de Listas de Acceso IP. [Articulo de internet]. {2007}. Recuperado de https://www.cisco.com/c/es_mx/support/docs/security/iosfirewall/23602-confaccesslists.html

[4] CISCO. (s.f.). Cisco Networking Academy. Obtenido de https://www.netacad.com/es

[5] Villagómez, Carlos. VLAN-Redes virtuales. {En línea}. {13 de septiembre de 2017} disponible en: (https://es.ccm.net/contents/286-vlan-redes-virtuales

[6] Villagómez, Carlos. El protocolo DHCP. {En línea}. {8 de marzo de 2017} disponible en: (https://es.ccm.net/contents/261-el-protocolo-dhcp).

BIOGRAFÍA

Martínez Perdomo Brayam Baudilio, nacido el 16 de noviembre de 1987 en la ciudad de Florencia – Departamento del Caquetá. Estudiante de pregrado de Ingeniería de Telecomunicaciones en la Universidad Nacional Abierta y A Distancia con sede en el municipio de Florencia (Caquetá).