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

DARWIN OSWALDO DORADO PUERCHAMBUD

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA – ECBTI
INGENIERIA DE SISITEMAS
PASTO
2020

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

DARWIN OSWALDO DORADO PUERCHAMBUD

DIPLOMADO DE PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN)

TUTOR: PAULITA FLOR

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA – ECBTI
INGENIERIA DE SISITEMAS
PASTO
2020

Nota de aceptación

Firma del presidente del jurado

Firma de jurado

Firma del jurado

PASTO, 5 de diciembre 2020

DEDICATORIA

Todos los estudios realizados, han hecho que sea una mejor persona en todos los ámbitos de mi vida, por eso quiero agradecer a Dios, a mi familia, a toda la Universidad (UNAD) tanto como compañeros de trabajo, como a todos los tutores, que hicieron posible que culmine con éxito esta hermosa Carrera

CONTENIDO

Pág.

LISTA DE FIGURAS

Pág.

Lista de Tablas

GLOSARIO

ACL (Access control list): Una lista de control de acceso o ACL es un concepto de seguridad informática usado para fomentar la separación de privilegios. Es una forma de determinar los permisos de acceso apropiados a un determinado objeto, dependiendo de ciertos aspectos del proceso que hace el pedido.

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.

IPv4 (Internet Protocol version 4, IPv4): El Protocolo de Internet versión 4, un protocolo de interconexión de redes basados en Internet, y que fue la rimera versión implementada en 1983 para la producción de ARPANET. Definida en el RFC 791, el IPv4 usa direcciones de 32 bits, limitadas a 4 294 967 296 direcciones únicas, muchas de las cuales están dedicadas a redes locales (LAN).

NAT (Network Address Translation): Es un mecanismo utilizado por routers IP para intercambiar paquetes entre dos redes que asignan mutuamente direcciones incompatibles.

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

PAT (Port Address Translation): Es una característica del estándar NAT, que traduce conexiones TCP y UDP hechas por un host y un puerto en una red externa a otra dirección y puerto de la red interna. Permite que una sola dirección IP sea utilizada por varias máquinas de la intranet. Con PAT, una IP externa puede responder hasta a ~64000 direcciones internas.

SDM es la abreviatura de Security Device Manager. Una herramienta de mantenimiento basada en una interfaz web desarrollada por Cisco. En la actualidad se entrega preinstalado en la mayoría de los enrutadores nuevos de Cisco, y se puede ejecutar desde el dispositivo (Router o Switch) o desde el PC.

VLAN es un acrónimo que deriva de una expresión inglesa: virtual LAN. Esa expresión, por su parte, alude a una sigla ya que LAN significa Local Area Network. De este modo, podemos afirmar que la idea de VLAN refiere a una red de área local (lo que conocemos como LAN) de carácter virtual.

RESUMEN

En el presente trabajo se realiza el desarrollo de dos escenarios de Networking que fueron propuestos por el director del curso, acompañado de los respectivos procesos de documentación de la solución, correspondientes al registro de la configuración de cada uno de los dispositivos de red, la descripción detallada del paso a paso de cada uno de los escenarios y el registro de los procesos de verificación de conectividad mediante el uso de comandos ping y show.

Para lograr los resultados propuestos se utilizó la herramienta de Packet Tracer, con la documentación suministrada en el entorno de conocimientos de las unidades presentadas para el curso.

Para el desarrollo de los escenarios se revisó las topologías presentadas y las tablas de configuración de los dispositivos, con estos datos se logra crear el diseño y la programación en el programa mencionado Packet Tracer.

Palabras Calve: Redes, Topologías, Dispositivos de red

ABSTRACT

In this work the development of two Networking scenarios that were proposed by the course director is carried out, accompanied by the respective solution documentation processes, corresponding to the registration of the configuration of each of the devices, the detailed description of the step-by-step of each one of the scenarios and the registration of the connectivity verification processes by using the ping and show commands.

To achieve the proposed results, the Packet Tracer tool was used, with the documentation provided in the knowledge environment of the units presented for the course.

For the development of the scenarios, the presented topologies and the device configuration tables were reviewed, with these data it is possible to create the design and programming in the mentioned Packet Tracer program.

Keywords: Networks, Topologies, Network Devices.

INTRODUCCION

En el presente trabajo se consiguió desarrollar dos escenarios de networking, con dos topologías de redes distintas, de las cuales se logró obtener las aptitudes necesarias para planificar e implementar redes LAN y WAN en pequeñas o medianas empresas . Para cualquier profesional, el conocimiento acerca del funcionamiento de estas tecnologías de la información y la comunicación, se han convertido en un reto; ya que hoy en día toda la información que manejamos a través de los equipos de cómputo, dispositivos móviles y demás se basan en las redes. Lo importante es poder implementar y administrar una red funcional para una empresa, con el fin de tener un control sobre ella que ayudara a identificar posibles fallas de forma más rápida o poder expandir de forma eficiente.

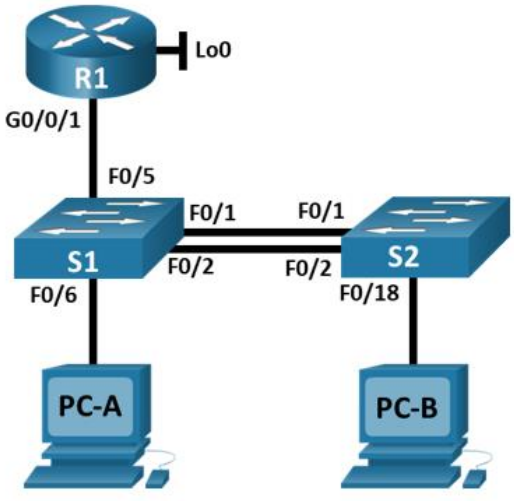
Se Identifican las herramientas de supervisión y protocolos de administración de red disponibles en el IOS para resolver los problemas de las redes de datos, evaluando el desempeño de Routers y Switches, mediante el uso de comandos especializados en gestión de redes.

Entrando más profundo en el tema de las redes debemos saber que ellas nos permiten una comunicación en varios ámbitos, como pueden ser las redes sociales, páginas web, chat, video llamadas, entre estas muchas más, todo esto con el fin de interactuar de muchas maneras.

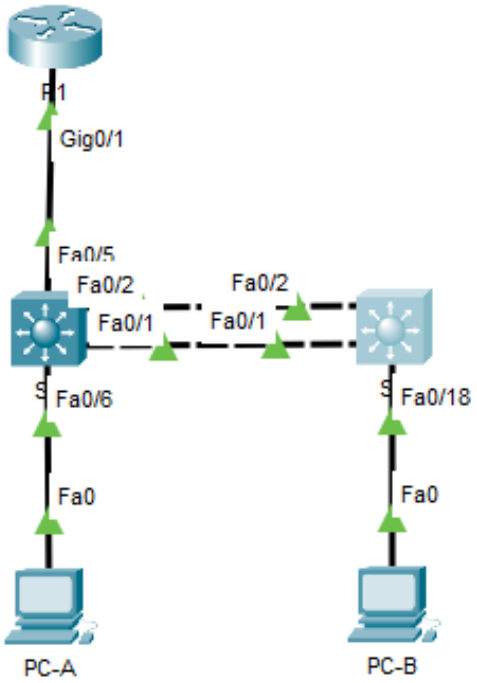
Ahora se precisará en el aprendizaje de la arquitectura, los componentes y el funcionamiento de los diferentes dispositivos de red que se pueden utilizar para una red.

1 ESCENARIO UNO

Topología



Figuras 1. Topología escenario uno



Figuras 2. Topología en packet tracer

Una vez realizado la topología en packet tracer procedemos a realizar la configuración de los dispositivos tanto de Router como del Switch según la tabla de direcciones proporcionada.

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

1.1 PARTE 1: INICIALIZAR Y RECARGAR Y CONFIGURAR ASPECTOS BASICOS DE LOS DISPOSITIVOS

1.1.1 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.
- Antes de continuar, solicite al instructor que verifique la inicialización de los dispositivos.

Para reinicializar utilizaremos dos comandos uno para borrar toda la configuración (erase startup-config**)** y el otro para reiniciar el sistema (Reload). Aplicaremos estos comandos para el router. También podemos utilizar este **show flash** comando que se utiliza para visualizar la memoria flash disponible y la cantidad utilizada

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

- Aplicando estos tres comandos desde la consola del Switch logramos realizar la reinicializarían del dispositivos, procedemos a realizar esta configuración en los dos dispositivos S1 y S2

```
Switch>en
Switch# show flash
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.
- Para actualizar las listas sdm simplemente utilizamos el comando #**sdm prefer dual-ipv4-and-ipv6 routing**

```
Switch>en
Switch#conf t.
Switch(config)#sdm prefer dual-ipv4-and-ipv6 routing
```

- Guardamos la configuración con el siguiente comando y reiniciamos

Switch#copy run start
Switch#reload
Switch>

Realizamos lo mismo en ambos switchs

1.1.2 Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 2. Configurar R1

Tarea	Especificación
Desactivar la búsqueda DNS	Para la desactivación utilizamos el comando **no ip domain-lookup**
Nombre del router	R1 lo realizamos con el comando hostname
Nombre de dominio	ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	ciscoenpass
Contraseña de acceso a la consola	ciscoconpass
Establecer la longitud mínima para las contraseñas	10 caracteres
Crear un usuario administrativo en la base de datos local	Nombre de usuario: **admin** Password: **admin1pass**
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	Las líneas VTY son las líneas de terminal virtual del router, que se utilizan solamente para controlar las conexiones Telnet entrantes.
Configurar VTY solo aceptando SSH	Se utiliza el comando transport input ssh en el modo de configuración line vty para permitir sólo SSH.
Cifrar las contraseñas de texto no cifrado	El comando service password-encryption aplica un cifrado débil a todas las contraseñas sin cifrar.
Configure un MOTD Banner	Con el banner podemos dejar un mensaje de advertencia si el caso.
Habilitar el routing IPv6	Para realizar la habilitación se utilizara el comando 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. Activar la interfaz.
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**
Generar una clave de cifrado RSA	Módulo de 1024 bits

- Ingresamos a la configuración del Router con configure terminal se puede escribir de forma abreviada (conf t)

Router#
Router# conf t

- Para la desactivación de búsquedas DNS utilizamos el comando **no ip domain-lookup** con el objetivo que no empiece a realizar búsquedas dns si colocamos algún comando mal**.**
- Realizamos el cambio del nombre del router con **hostname** y el nombre que le vayamos a poner con el objetivo de identificar cada dispositivo

Router(config)#no ip domain-lookup
Router(config)#hostname R1

- Ahora asignamos un nombre de dominio con **ip domain-name** y el nombre que le vayamos a poner

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

- Para configurar una contraseña local en niveles de acceso de usuario utilizamos **enable secret** y la contraseña a utilizar, con el objetivo de poner seguridad a nuestros dispositivos no realicen cambios personas no autorizadas

R1(config)#enable secret ciscoenpass

- Los siguientes comandos se usan en el modo de configuración global para establecer una contraseña para la línea de consola: aquí agregamos un nivel mas de seguridad

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

- Para Crear un usuario administrativo y contraseña en la base de datos local utilizamos los siguientes comados: el objetivo es tener un usuario adicional como administrador.

```
R1(config-line)#exit
R1(config)#enable secret level 10 admin1pass
R1(config)#username admin privilege 10 secret admin1pass
```

- El comando que utilizamos para establecer una contraseña en las líneas vty es el siguiente:

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

- Por ultimo para la encriptación de las contraseñas asignadas tanto para la consola como para la línea de comandos utilizamos el siguiente comando , el tener nuestras contraseñas cifradas evitamos ser hackeados.

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

```
R1(config)#ip ssh version 2
Please create RSA keys (of at least 768 bits size) to enable SSH v2.
```

- Se utiliza el comando **transport input ssh** en el modo de configuración line vty para permitir sólo SSH y también colocamos un nivel de seguridad 15 para ssh con su contraseña. El objetivo de utilizar ssh es porque es mucho mas seguro acceder al dispositivo de forma remota.

```
R1(config)#line vty 0 15
R1(config-line)#transport input ssh
R1(config-line)#login local
R1(config)#username R1 privilege 15 secret ciscoenpass
R1(config)#enable secret ciscoenpass ssh
```

- Con el siguiente comando colocamos un mensaje de advertencia para ingresar al dispositivo.

```
R1(config)#banner motd "Acceso solo para Administradores"
```

- Para realizar la habilitación se utilizara el comando **ipv6 unicast-routing**

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

- Con los siguientes comandos ingresaremos a la interfaz g0/1 del router y asignaremos las ips de las subredes según la *Tabla 3. Asignación de direcciones* una vez creadas no olvidar encender la interfaz con el comando no shutdown. Para poder lograr la conexión entre dispositivos necesariamente se requiere la configuración de direcciones ip en las interfaces.

```
R1(config)#int g0/1.2
R1(config- subif)#ip add 10.19.8.1 255.255.255.192
R1(config-subif)#encapsulation dot1Q 2
R1(config-subif)#ipv6 add 2001:db8:acad:a::1/64
R1(config-line)#exit
R1(config)#int g0/1.3
R1(config-subif)#ip add 10.19.8.65 255.255.255.224
R1(config-subif)#encapsulation dot1Q 3
R1(config-subif)#ipv6 add 2001:db8:acad:b::1/64
R1(config-line)#exit
R1(config-subif)#int g0/1.4
R1(config-subif)#ip add 10.19.8.97 255.255.255.248
R1(config-subif)#encapsulation dot1Q 4
R1(config-subif)#ipv6 add 2001:db8:acad:c::1/64
R1(config-subif)#exit
R1(config)#int g0/1
R1(config-if)#no shutdown
```

- De igual forma asignamos las ips loopback según la tabla de direcciones de la siguiente manera. El objetivo de activar la interfaz loopback es porque es útil para probar y administrar un dispositivo Cisco IOS, ya que asegura que por lo menos una interfaz esté siempre disponible.

```
R1#conf t
R1(config)# int Loopback0
R1(config-if)#
R1(config-if)#ip add 209.165.201.1 255.255.255.224
R1(config-if)#ipv6 add 2001:db8:acad:209::1/64
```

1.1.3 Paso 3: Configure S1 y S2.

Las tareas de configuración incluyen lo siguiente:

Tabla 4. Configuracion S1 y S2

Tarea	Especificación
Desactivar la búsqueda DNS.	Para la desactivación utilizamos el comando **no ip domain-lookup**
Nombre del switch	**S1 o S2, según proceda**
Nombre de dominio	**ccna-lab.com**
Contraseña cifrada para el modo EXEC privilegiado	**ciscoenpass**
Contraseña de acceso a la consola	**ciscoconpass**
Crear un usuario administrativo en la base de datos local	Nombre de usuario: **admin** Password: **admin1pass**
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	Las líneas VTY son las líneas de terminal virtual del router, que se utilizan solamente para controlar las conexiones Telnet entrantes.
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	Se utiliza el comando transport input ssh en el modo de configuración line vty para permitir sólo SSH.
Cifrar las contraseñas de texto no cifrado	El comando service password-encryption aplica un cifrado débil a todas las contraseñas sin cifrar.
Configurar un MOTD Banner	Con el banner podemos dejar un mensaje de advertencia si el caso.
Generar una clave de cifrado RSA	**Módulo de 1024 bits**
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** Establecer la dirección IPv6 de capa 3

Configuración del gateway predeterminado	Configure la puerta de enlace predeterminada como 10.19.8.97 para IPv4

- Ingresamos a la configuración del Switch con enable y configure terminal se puede escribir de forma abreviada (en, conf t)

SWITCH 1
Switch> en
Switch# conf t
Enter configuration commands, one per line. End with CNTL/Z.

- Para la desactivación de búsquedas DNS utilizamos el comando **no ip domain-lookup**
- Realizamos el cambio del nombre del Switch con **hostname** y el nombre que le vayamos a poner

Switch(config)#no ip domain-lookup
Switch(config)#hostname S1

- Ahora asignamos un nombre de dominio con **ip domain-name** y el nombre que le vayamos a poner

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

- Para configurar una contraseña local en niveles de acceso de usuario utilizamos **enable secret** y la contraseña a utilizar

S1(config)#enable secret ciscoenpass

- Los siguientes comandos se usan en el modo de configuración global para establecer una contraseña para la línea de consola:

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

- Se utiliza el comando **transport input ssh** en el modo de configuración line vty para permitir sólo SSH y también colocamos un nivel de seguridad 15 para ssh con su contraseña.

```
S1(config)#line vty 0 15
S1(config-line)#transport input ssh
S1(config-line)#login local
S1(config-line)#password ciscoconpass
S1(config-line)#login
S1(config-line)#exit
```

- Con el siguiente comando colocamos un mensaje de advertencia para ingresar al dispositivo

```
S1(config)#banner motd "Acceso solo para Administradores"
```

- Por ultimo para la encriptación de las contraseñas asignadas tanto para la consola como para la línea de comandos utilizamos el siguiente comando.

```
S1(config)#crypto key generate rsa
```

.

- Con los siguientes comandos ingresaremos a la interfaz del Swicth y crearemos las vlan y asignaremos las ips según la *Tabla 5. Asignación de direcciones* una vez creadas no olvidar encender la interfaz con el comando no shutdown.

```
S1(config)#interface vlan 4
S1(config-if)#ip add 10.19.8.98 255.255.255.248
S1(config-if)#ip default-gateway 10.19.8.97
S1(config-if)#ipv6 add 2001:db8:acad:c::98/64
S1(config-if)#ipv6 add fe80::98 link-local
S1(config-if)#description Management interface
S1(config-if)#no shut
S1(config)# exit.
S1#
```

- Realizamos los mismos pasos para el SWITCH 2

```
SWITCH 2
Switch> en
Switch# conf t
```

- Para la desactivación de búsquedas DNS utilizamos el comando **no ip domain-lookup**
- Realizamos el cambio del nombre del Switch con **hostname** y el nombre que le vayamos a poner

```
Switch(config)#no ip domain-lookup
Switch(config)#hostname S2
```

- Ahora asignamos un nombre de dominio con ip domain-name y el nombre que le vayamos a poner

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

- Para configurar una contraseña local en niveles de acceso de usuario utilizamos **enable secret** y la contraseña a utilizar

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

- Los siguientes comandos se usan en el modo de configuración global para establecer una contraseña para la línea de consola:

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

- Se utiliza el comando **transport input ssh** en el modo de configuración line vty para permitir sólo SSH y también colocamos un nivel de seguridad 15 para ssh con su contraseña.

```
S2(config)#line vty 0 15
S2(config-line)#transport input ssh
S2(config-line)#login local
S2(config-line)#password ciscoconpass
S2(config-line)#login
S2(config-line)#exit
```

- Con el siguiente comando colocamos un mensaje de advertencia para ingresar al dispositivo.

```
S2(config)#banner motd "Acceso solo para Administradores"
```

- Por último para la encriptación de las contraseñas asignadas tanto para la consola como para la línea de comandos utilizamos el siguiente comando

S2(config)#crypto key generate rsa

- Con los siguientes comandos ingresaremos a la interfaz del Swicth y crearemos las vlan y asignaremos las ips según la *Tabla 6. Asignación de direcciones* una vez creadas no olvidar encender la interfaz con el comando no shutdown.

```
S2(config)#int vlan 4
S2(config-if)#ip add 10.19.8.99 255.255.255.248
S2(config-if)#ipv6 add 2001:db8:acad:c::99/64
S2(config-if)#ipv6 add fe80::99 link-local
S2(config-if)#description Management interface
S2(config-if)#no shut
S2(config)# exit.
S2#
```

1.2 PARTE 2: CONFIGURACIÓN DE LA INFRAESTRUCTURA DE RED (VLAN, TRUNKING, ETHERCHANNEL)

1.2.1 Paso 4: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 7. Configuracion S1

Tarea	Especificación
Crear VLAN	VLAN 2, nombre Bikes VLAN 3, nombre Trikes VLAN 4, name Management VLAN 5, nombre Parking VLAN 6, nombre Native
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	Interfaces F0/1, F0/2 y F0/5
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	Usar el protocolo LACP para la negociación
Configurar el puerto de acceso de host para VLAN 2	Interface F0/6

Configurar la seguridad del puerto en los puertos de acceso	Permitir 3 direcciones MAC
Proteja todas las interfaces no utilizadas	Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar

- Como Podemos darnos cuenta al ingresar al swicth ya nos solicita contraseña tanto para entrar a la consola , como para la configuración del dispositivo, Digitamos las asignadas anteriormente.

Press RETURN to get started!
Acceso solo para Administradores
User Access Verification
Password:
S1>en
Password:
S1#
S1#config t
Enter configuration commands, one per line. End with CNTL/Z.

- Con los siguientes comandos que miramos a continuación creamos las vlan y les colocamos los nombres según la tabla 4. Configuración S1.
- La creación de vlan nos permite segmentar los equipos y limitar el acceso entre ellos por temas de seguridad.

S1(config)#vlan 2
S1(config-vlan)#name Bikes
S1(config-vlan)#exit
S1(config)#vlan 3
S1(config-vlan)#name Trikes
S1(config-vlan)#exit
S1(config)#vlan 4
S1(config-vlan)#
%LINK-5-CHANGED: Interface Vlan4, changed state to up
S1(config-vlan)#name Management
S1(config-vlan)#exit
S1(config)#vlan 5
S1(config-vlan)#name Parking
S1(config-vlan)#exit
S1(config)#vlan 6
S1(config-vlan)#name Native
S1(config-vlan)#exit
S1(config)#

S1#config t

- Con los siguientes comandos asignamos cada vlan a la interfaz correspondiente en el modo troncal.

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)#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)#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)#exit
S1(config)#int range fa0/1-2
S1(config-if)#switchport trunk native vlan 6
S1(config-if-range)#switchport trunk encapsulation dot1q
S1(config-if-range)#switchport mode trunk
S1(config-if-range)#switchport trunk native vlan 6
S1(config-if-range)#channel-group 2 mode active
S1(config-if-range)#no shutdown
S1#config t

- En esta Interfaz no colocamos modo troncal si no modo acceso.

S1(config)#interface f0/6
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 2
S1(config-if)#exit
S1#config t
Enter configuration commands, one per line. End with CNTL/Z.

- Configuráramos la seguridad de los puertos solicitados en los puertos de acceso

S1(config)#int fa0/1
S1(config-if)#switchport mode Access
S1(config-if)#switchport port-security
S1(config-if)#switchport port-security maximum 3
S1(config-if)#switchport port-security violation shutdown

S1(config-if)#switchport port-security mac-address 0001.64E6.8833
S1(config-if)#switchport port-security mac-address sticky
S1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#int range fa0/19-22
S1(config-if-range)#switchport access vlan 5
S1(config-if-range)#shutdown
S1(config-if-range)# exit
S1(config)#

1.2.2 Paso 5: Configure el S2.

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

Tabla 8. Configuracion S2

Tarea	Especificación
Crear VLAN	VLAN 2, name Bikes VLAN 3, name Trikes VLAN 4, name Management VLAN 5, nombre Parking VLAN 6, nombre Native
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	Interfaces F0/1 y F0/2
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	Usar el protocolo LACP para la negociación
Configurar el puerto de acceso del host para la VLAN 3	Interfaz F0/18
Configure port-security en los access ports	permite 3 MAC addresses
Asegure todas las interfaces no utilizadas.	Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar

- Con los siguientes comandos que miramos a continuación creamos las vlan y les colocamos los nombres según la tabla 5. Configuración S2.

S2#config t

S2(config)#vlan 2
S2(config-vlan)#name Bikes
S2(config-vlan)#exit
S2(config)#vlan 3
S2(config-vlan)#name Trikes
S2(config-vlan)#exit
S2(config)#vlan 4
S2(config-vlan)#
S2(config-vlan)#name Management
S2(config-vlan)#exit
S2(config)#vlan 5
S2(config-vlan)#name Parking
S2(config-vlan)#exit
S2(config)#Vlan 6
S2(config-vlan)#name Native
S2(config-vlan)#exit
S2(config)#
S2#
S2#config t
Enter configuration commands, one per line. End with CNTL/Z.

- Con los siguientes comandos asignamos cada vlan a la interfaz correspondiente en el modo troncal.

S2(config)#int f0/1
S2(config)#switchport trunk encapsulation dot1q
S2(config-if)#switchport mode trunk
S2(config-if)#switchport trunk native vlan 6
S2(config-if)#exit
S2(config)#
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-range)#channel-group 1 mode auto
S2(config-if-range)# Creating a port-channel interface Port-channel 1
S2(config-if)#exit
S2(config)#
S2(config)#int range f0/1-2
S2(config-if)#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 2 mode active

S2(config-if-range)#no shutdown
S2(config-if-range)#exit
S2(config)#
S2(config)#int f0/18
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 3
S2(config-if)#exit

- Configuráramos la seguridad de los puertos solicitados en los puertos de acceso

S2(config)#int fa0/2
S2(config-if)#switchport mode access
S2(config-if)#switchport port-security maximum 3
S2(config-if)#switchport port-security violation protect
S2(config-if)#switchport port-security mac-address sticky
S2#conf t
Enter configuration commands, one per line. End with CNTL/Z.

- Con el siguiente comando apagamos el rango de interfaces que no se utilizaran

S2(config)#int range f0/19-22
S2(config-if-range)#switchport access vlan 5
S2(config-if-range)#shutdown

1.3 PARTE 3: CONFIGURAR SOPORTE DE HOST

1.3.1 Paso 1: Configure R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 9. Configuracion R1

Tarea	Especificación
Configure Default Routing	Crear rutas predeterminadas para IPv4 e IPv6 que dirijan el tráfico a la interfaz 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
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

- De esta forma asignamos las ips loopback según la tabla de direcciones de la siguiente manera.

```
R1#conf t
R1(config)#int lo0
R1(config-if)#ip address 209.165.201.1 255.255.255.192
R1(config-if)#no shut
R1(config-if)#ex
R1(config)#
R1(config)#int lo0
R1(config-if)#ipv6 address 2001:db8:acad:209::1/64
R1(config-if)#ex
```

- Para realizar la habilitación de ipv6 utilizara el comando **ipv6 unicast-routing**

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

Para crear el grupo DHCP para la vlan 2 realizamos lo siguiente:

```
R1(config)#ip dhcp pool vlan2
R1(dhcp-config)#network 10.19.8.0 255.255.255.192
R1(dhcp-config)#default-router 10.19.8.1
R1(config-if)#ex
```

- Para crear el grupo DHCP para la vlan 3 realizamos lo siguiente:

```
R1(config)#ip dhcp pool vlan3
R1(dhcp-config)#network 10.19.8.64 ? A.B.C.D Network mask
R1(dhcp-config)#network 10.19.8.64 255.255.255.192
R1(dhcp-config)#default-router 10.19.8.65
R1(dhcp-config)#exit
```

1.3.2 Paso 2: Configurar los servidores

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

Tabla 10. Configuracion Servidores

PC-A Network Configuration	
Descripción	*PC-A*
Dirección física	*0001.631A.0098*
Dirección IP	*10.19.8.2*
Máscara de subred	*255.255.255.192*
Gateway predeterminado	*10.19.8.1*
Gateway predeterminado IPv6	*2001:DB8:ACAD:A::1*

Tabla 11. Configuracion PC-A

Configuración de red de PC-A	
Descripción	*PC-B*
Dirección física	*0003.2356.0035*
Dirección IP	*10.19.8.86*
Máscara de subred	*255.255.255.224*
Gateway predeterminado	*10.19.8.65*
Gateway predeterminado IPv6	*2001:DB8:ACAD:B::1*

1.4 PARTE 4: PROBAR Y VERIFICAR LA CONECTIVIDAD DE EXTREMO A EXTREMO

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

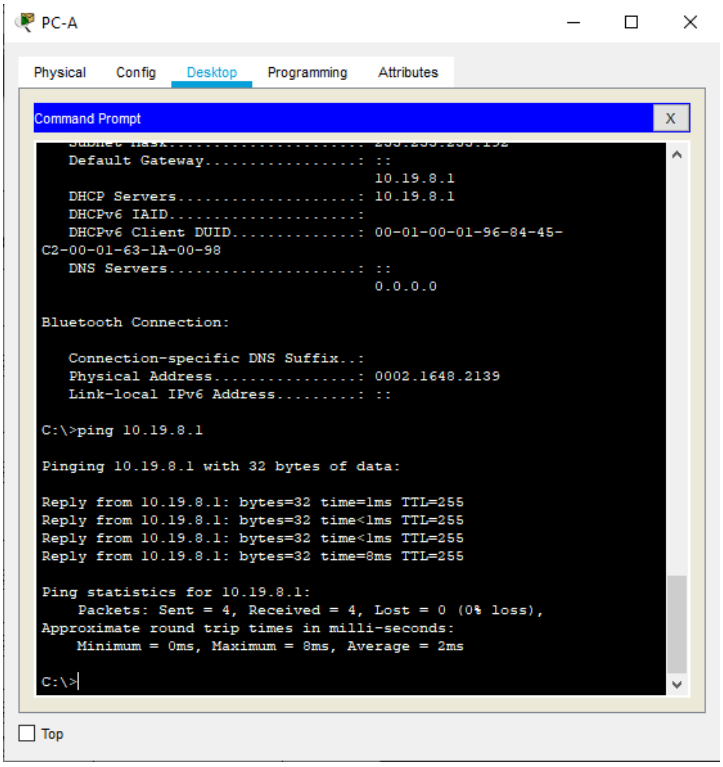
Nota: Si fallan los pings en las computadoras host, desactive temporalmente el firewall de la computadora y vuelva a realizar la prueba.

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:

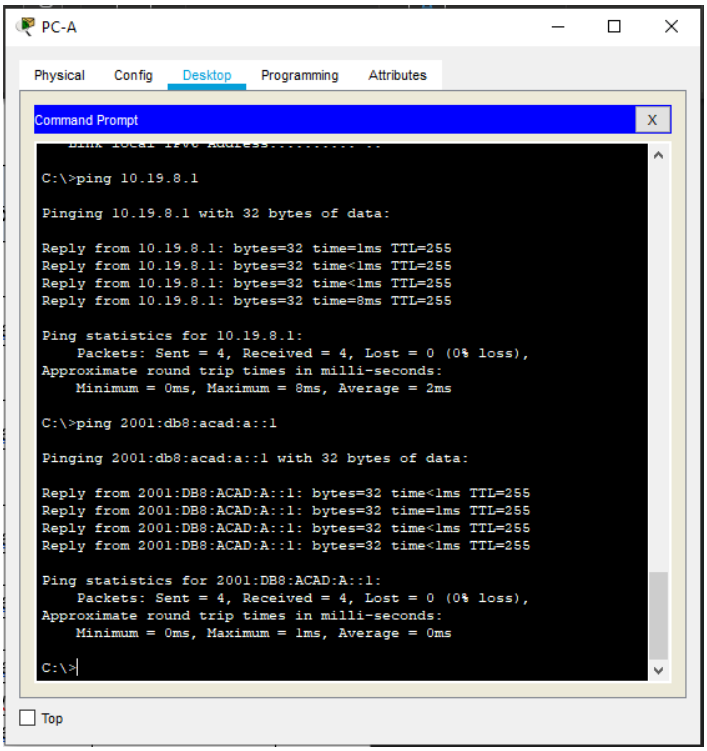
Tabla 12. Verificación de conectividad

Desde	A	de Internet	Dirección IP	Resultados de ping
PC-A	R1, G0/0/1.2	Dirección	10.19.8.1	*Figura 3.*
		IPv6	2001:db8:acad:a::1	*Figura 4.*
	R1, G0/0/1.3	Dirección	10.19.8.65	*Figura 5.*
		IPv6	2001:db8:acad:b::1	*Figura 6.*
	R1, G0/0/1.4	Dirección	10.19.8.97	*Figura 7.*
		IPv6	2001:db8:acad:c: :1	*Figura 8.*
	S1, VLAN 4	Dirección	10.19.8.98	*Figura 9.*
		IPv6	2001:db8:acad:c: :98	*Figura 10.*
	S2, VLAN 4	Dirección	10.19.8.99.	*Figura 11.*
		IPv6	2001:db8:acad:c: :99	*Figura 12.*
	PC-B	Dirección	IP address will vary.	*Figura 13.*
		IPv6	2001:db8:acad:b: :50	*Figura 14.*
	R1 Bucle 0	Dirección	209.165.201.1	*Figura 15.*
		IPv6	2001:db8:acad:209: :1	*Figura 16.*
PC-B	R1 Bucle 0	Dirección	209.165.201.1	*Figura 17.*
		IPv6	2001:db8:acad:209: :1	*Figura 18.*
	R1, G0/0/1.2	Dirección	10.19.8.1	*Figura 19.*
		IPv6	2001:db8:acad:a: :1	*Figura 20.*
	R1, G0/0/1.3	Dirección	10.19.8.65	*Figura 21.*
		IPv6	2001:db8:acad:b: :1	*Figura 22.*
	R1, G0/0/1.4	Dirección	10.19.8.97	*Figura 23.*
		IPv6	2001:db8:acad:c: :1	*Figura 24.*

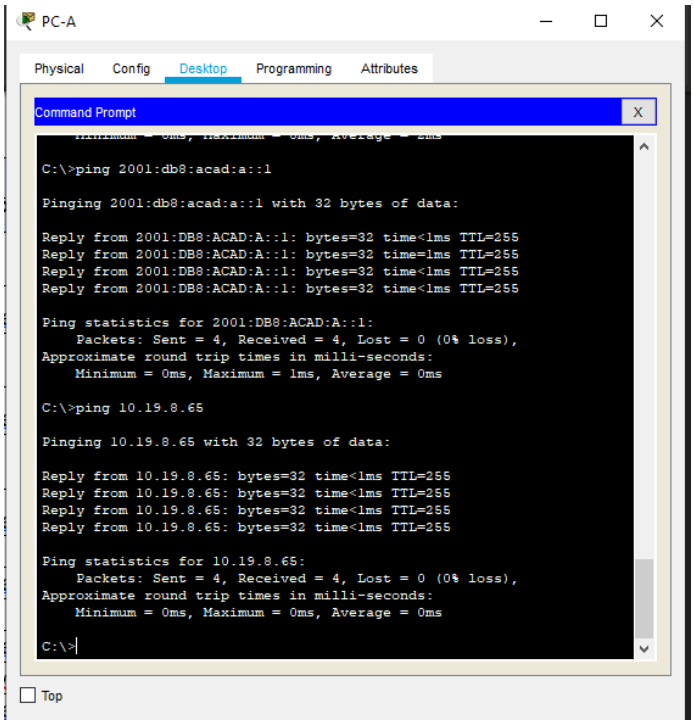
	S1, VLAN 4	Dirección	10.19.8.98	*Figura 25.*
		IPv6	2001:db8:acad:c: :98	*Figura 26.*
	S2, VLAN 4	Dirección	10.19.8.99.	*Figura 27.*
		IPv6	2001:db8:acad:c: :99	*Figura 28.*



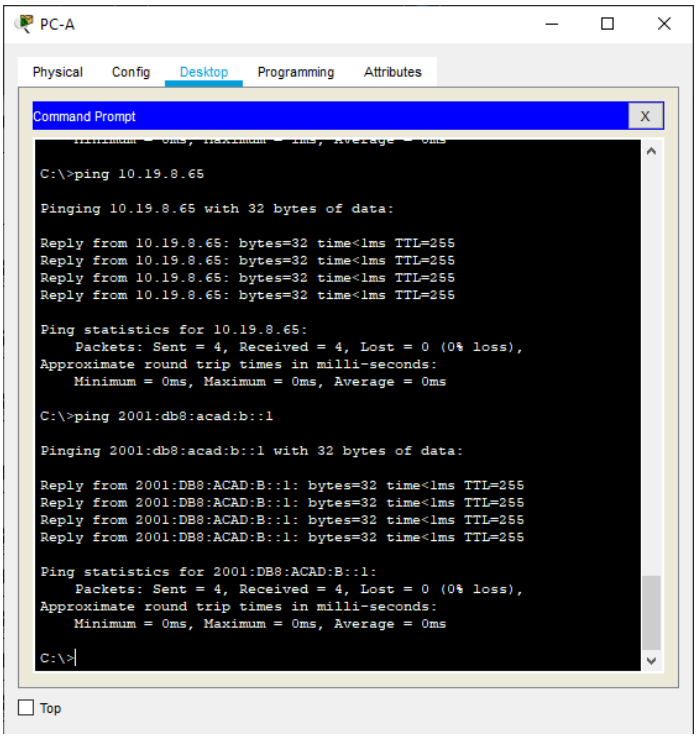
Figuras 3. Ping PC-A a 10.19.8.1



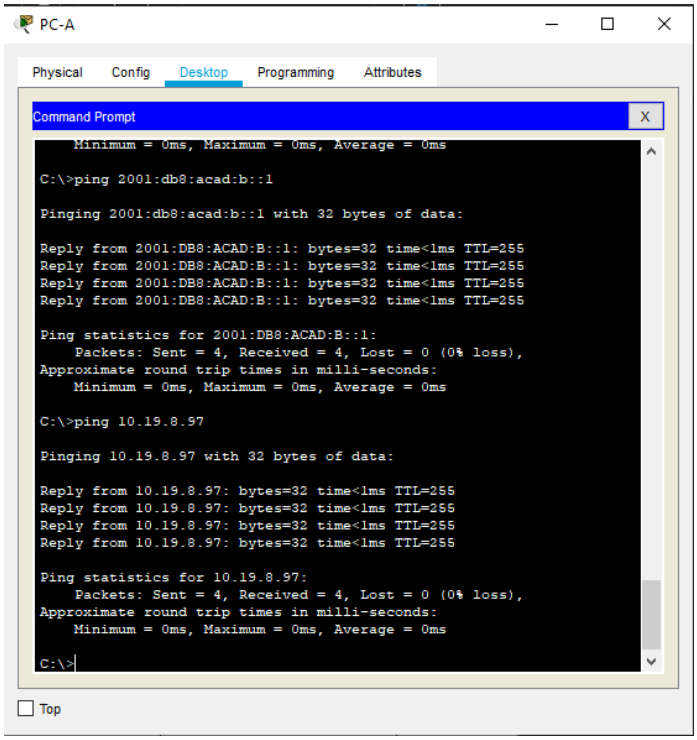
Figuras 4. Ping PC-A a 2001:db8:acad:a::1



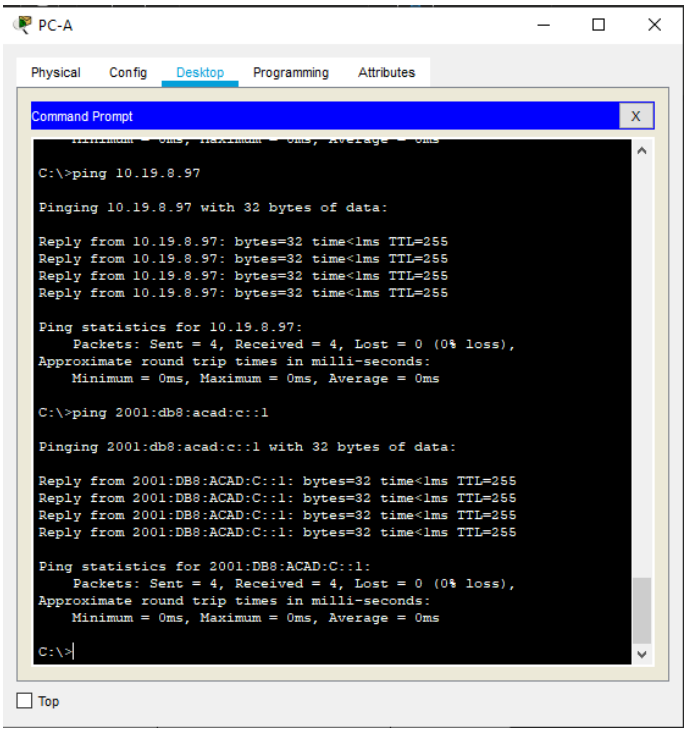
Figuras 5. Ping PC-A a 10.19.8.65



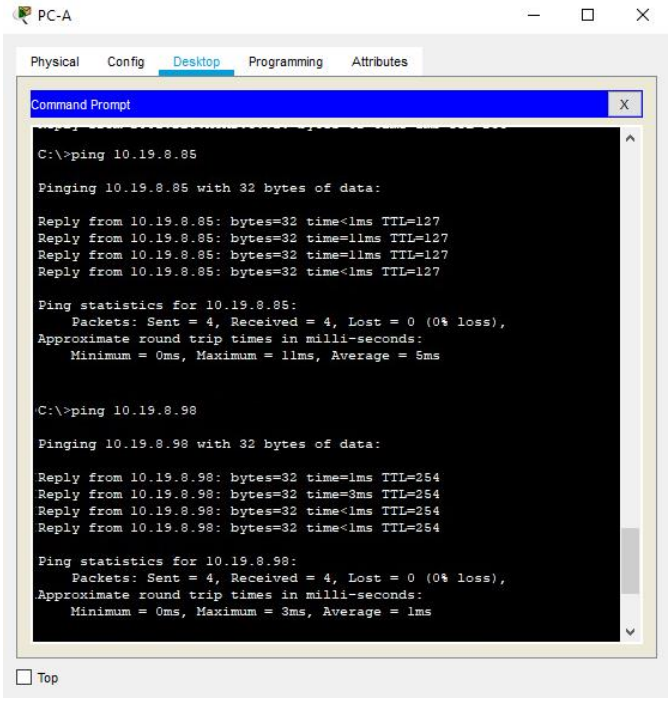
Figuras 6. Ping PC-A a 2001:db8:acad:b::1



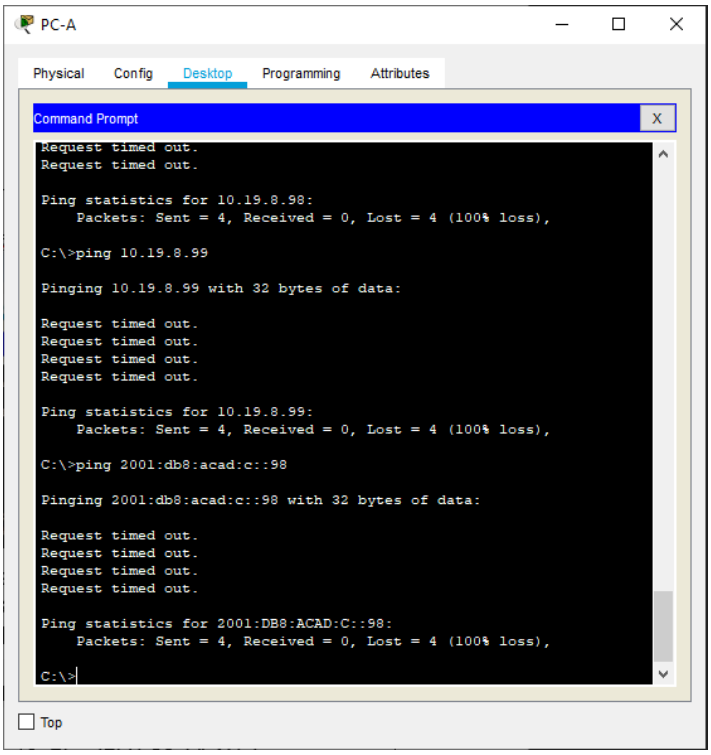
Figuras 7. Ping PC-A a 10.19.8.97



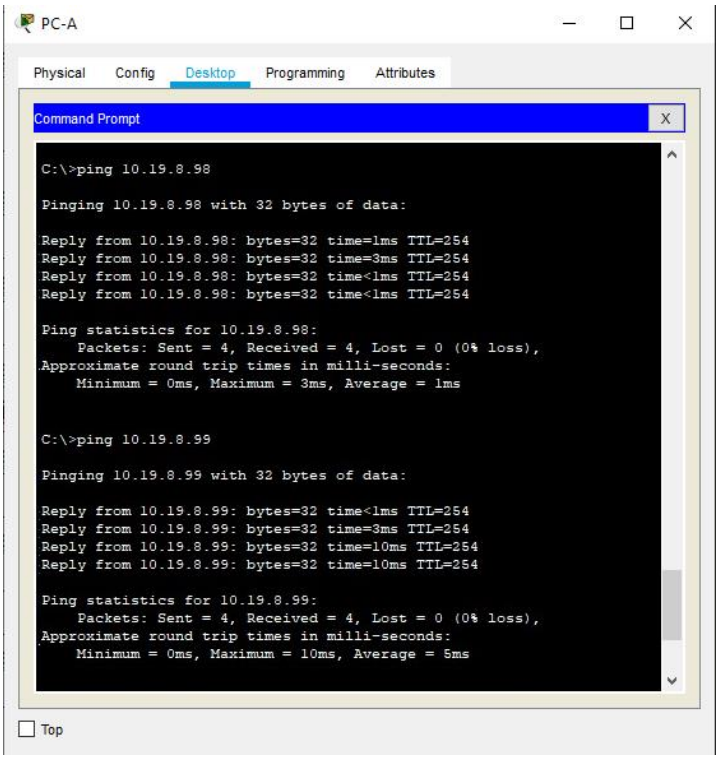
Figuras 8. Ping PC-A a 2001:db8:acad:c::1



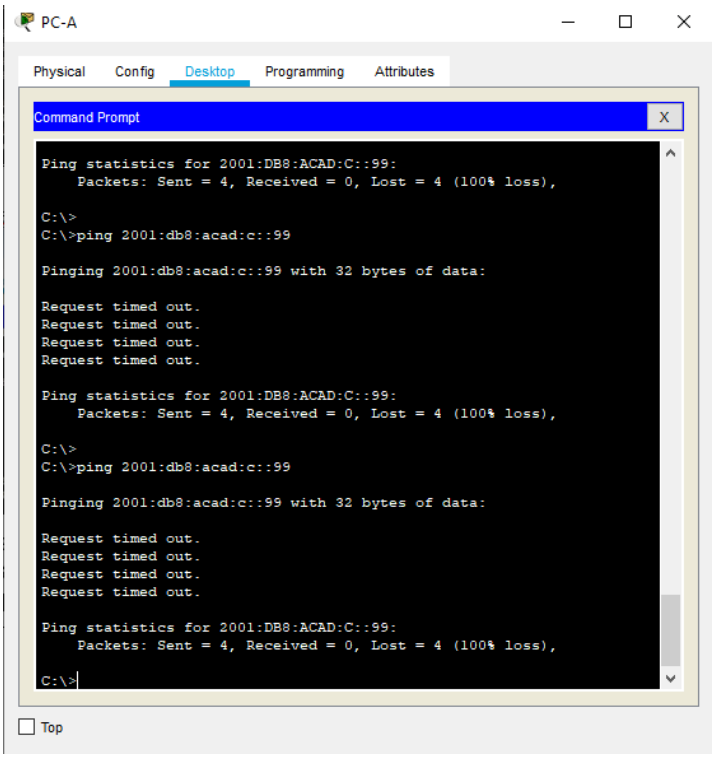
Figuras 9. Ping PC-A a 10.19.8.98



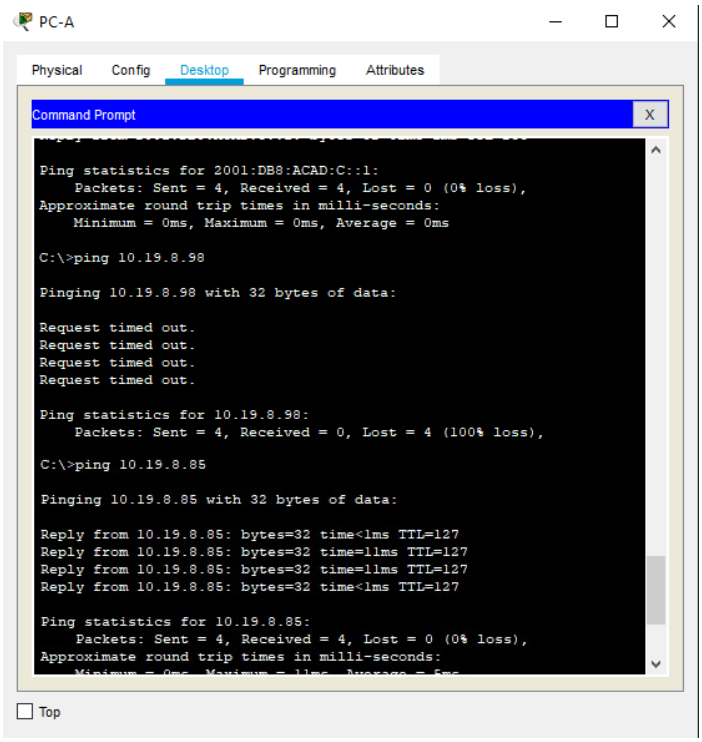
Figuras 10. Ping PC-A a 2001:db8:acad:c::98



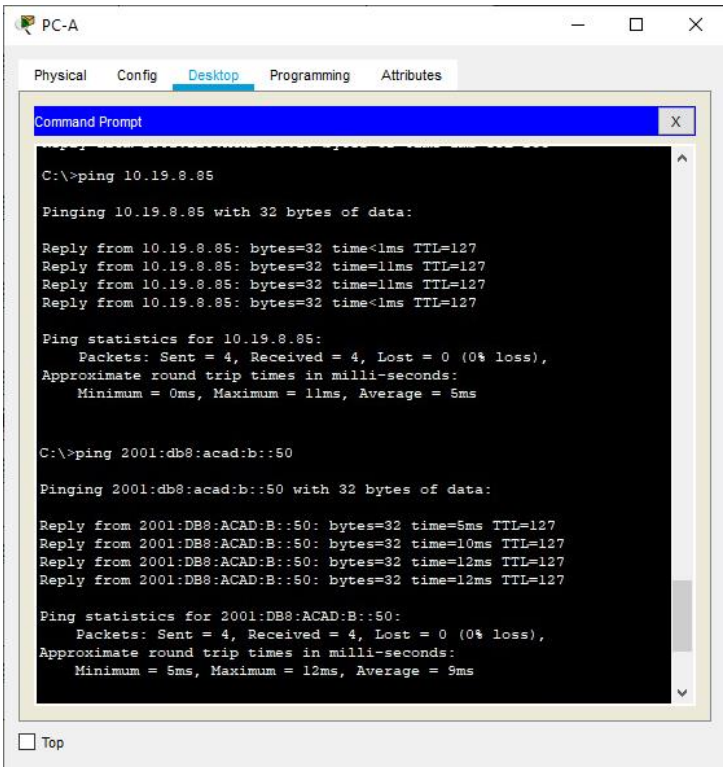
Figuras 11. Ping PC-A a 10.19.8.99



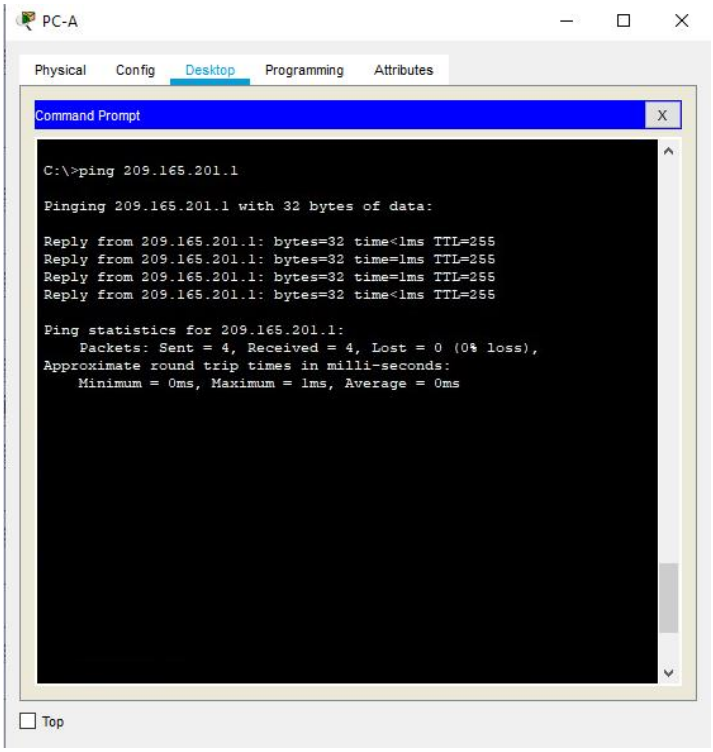
Figuras 12. Ping PC-A a 2001:db8:acad:c::99



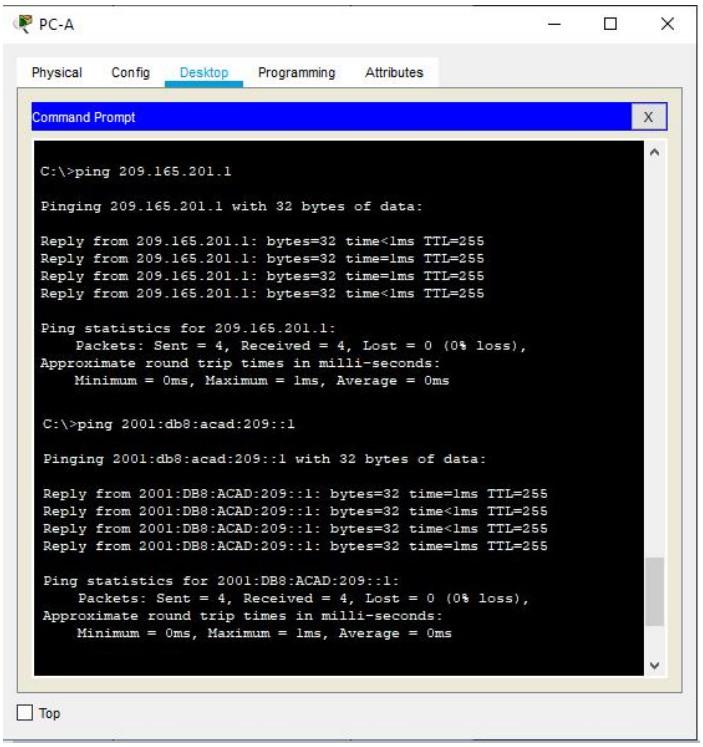
Figuras 13. Ping PC-A a 10.19.8.85



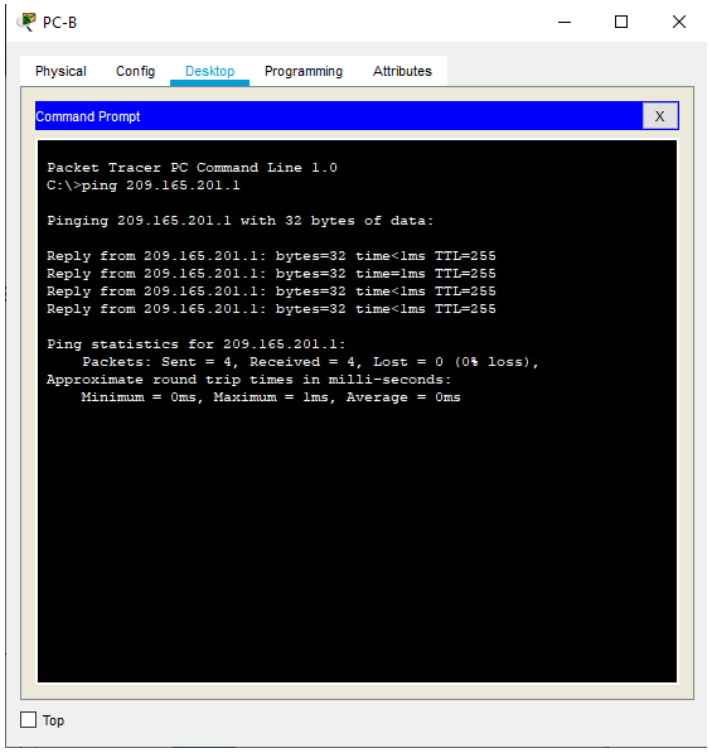
Figuras 14. Ping PC-A a 2001:db8:acad:b::50



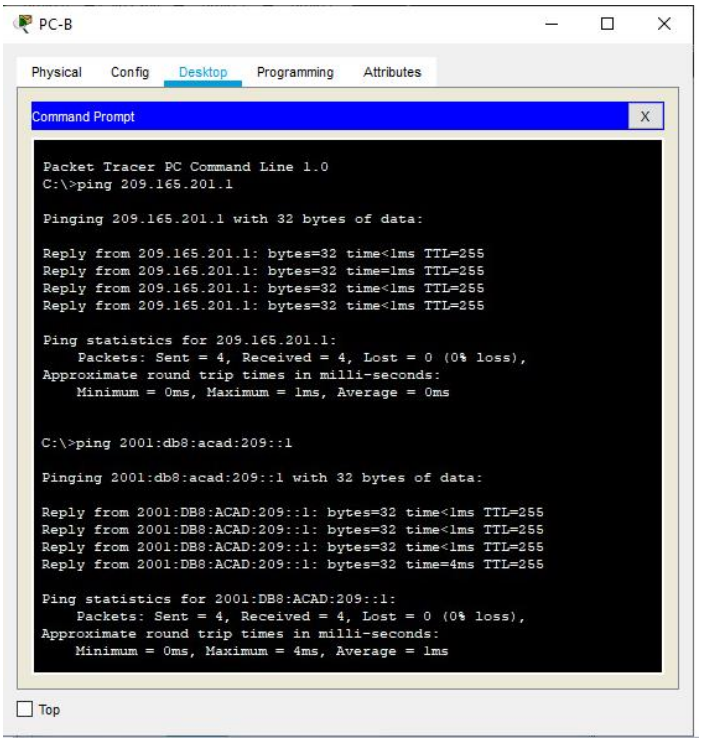
Figuras 15. Ping PC-A a 209.165.201.1



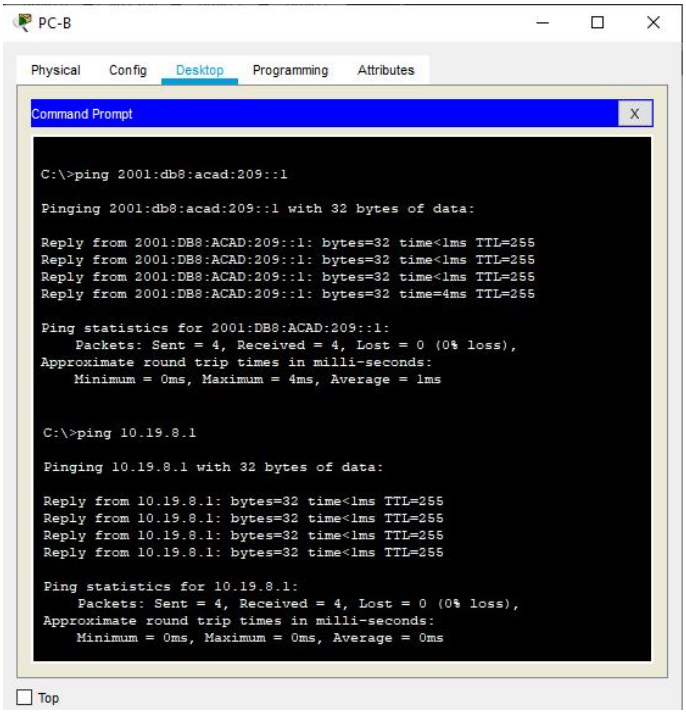
Figuras 16. Ping PC-A a 2001:db8:acad:209::1



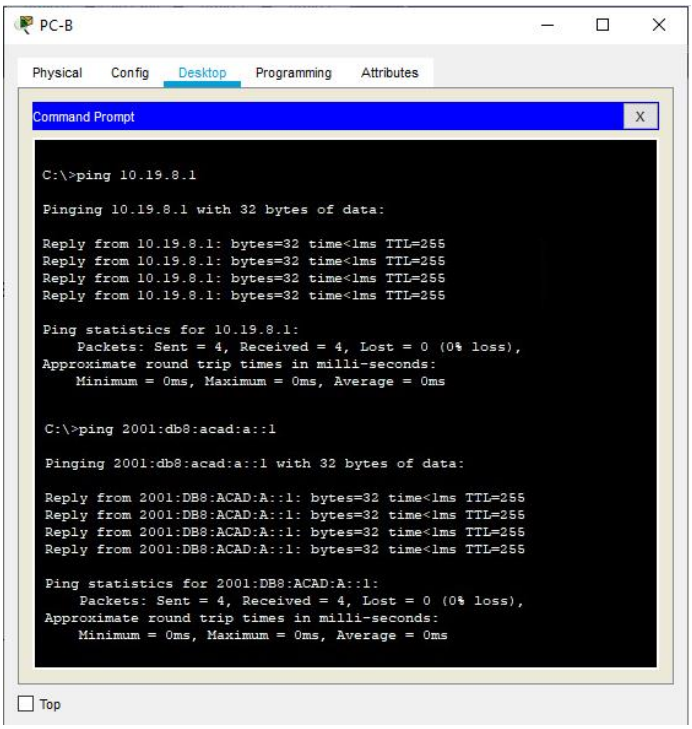
Figuras 17. Ping PC-B a 209.165.201.1



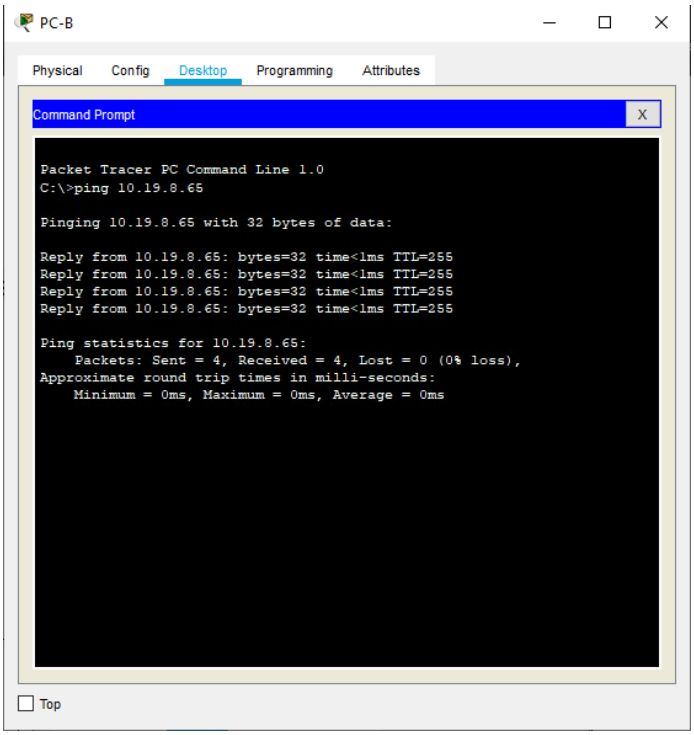
Figuras 18. Ping PC-B a 2001:db8:acad:209::1



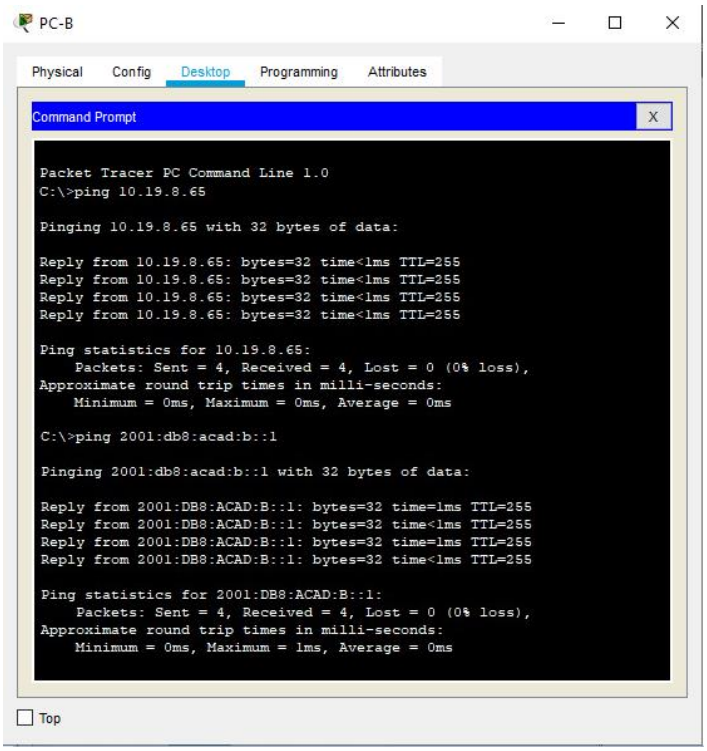
Figuras 19. Ping PC-B a 10.19.8.1



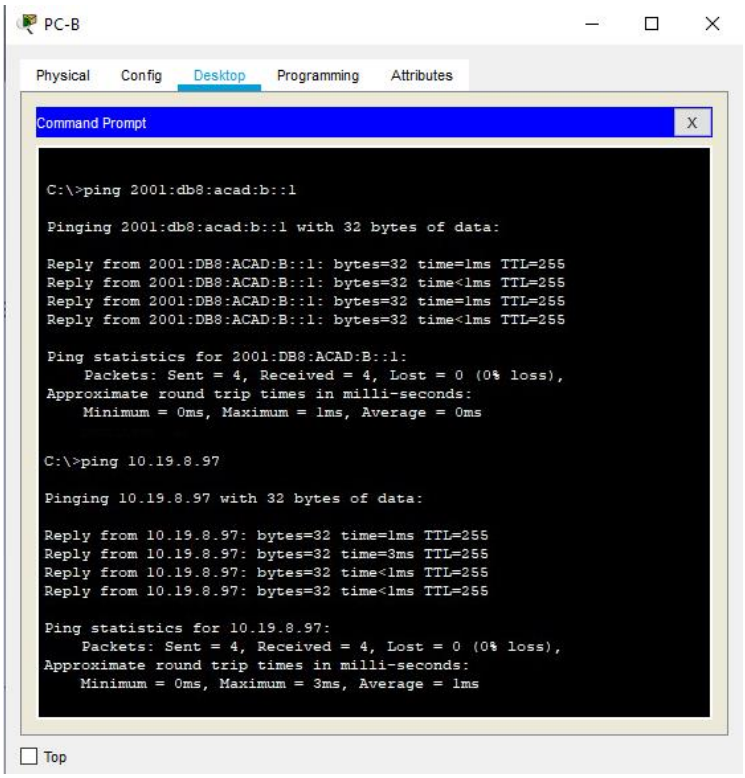
Figuras 20. Ping PC-B a 2001:db8:acad:a::1



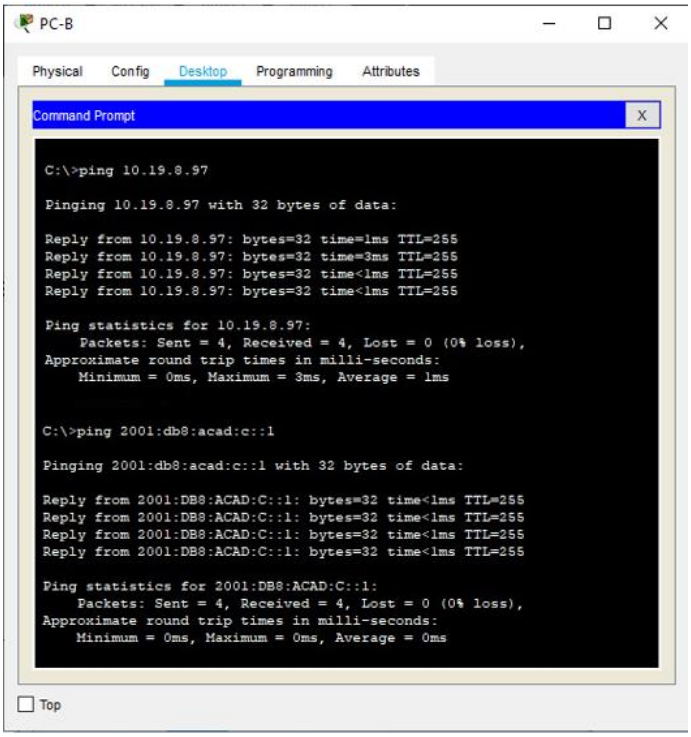
Figuras 21. Ping PC-B a 10.19.8.65



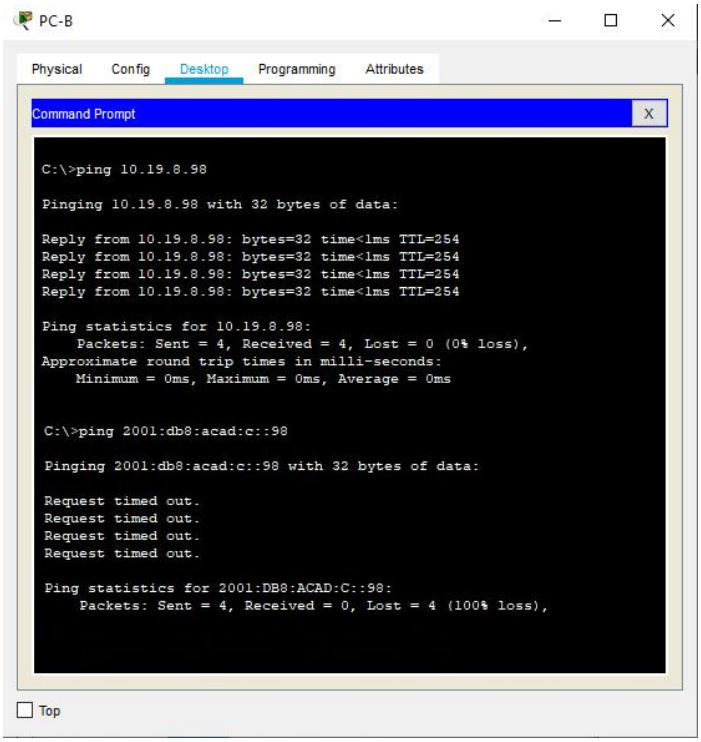
Figuras 22. Ping PC-B a 2001:db8:acad:b::1



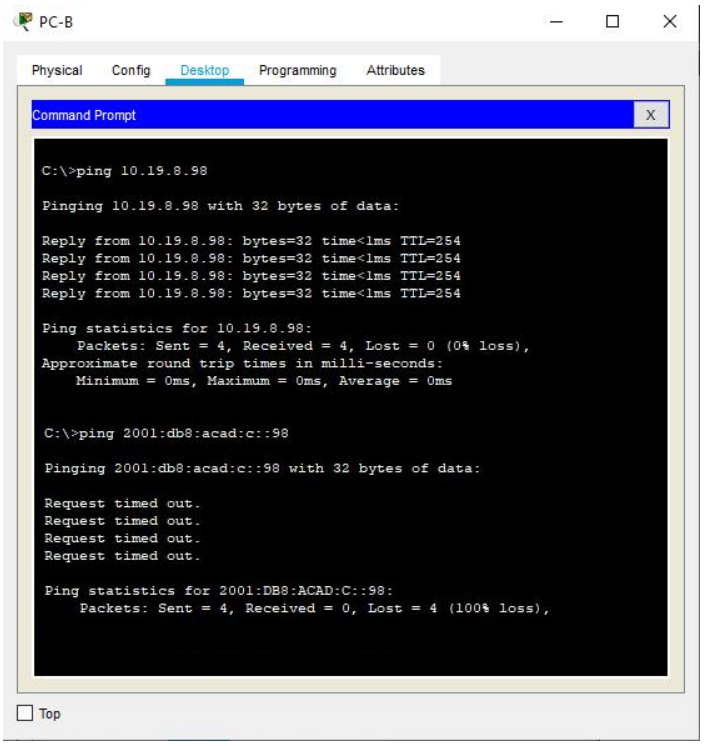
Figuras 23. Ping PC-B a 10.19.8.97



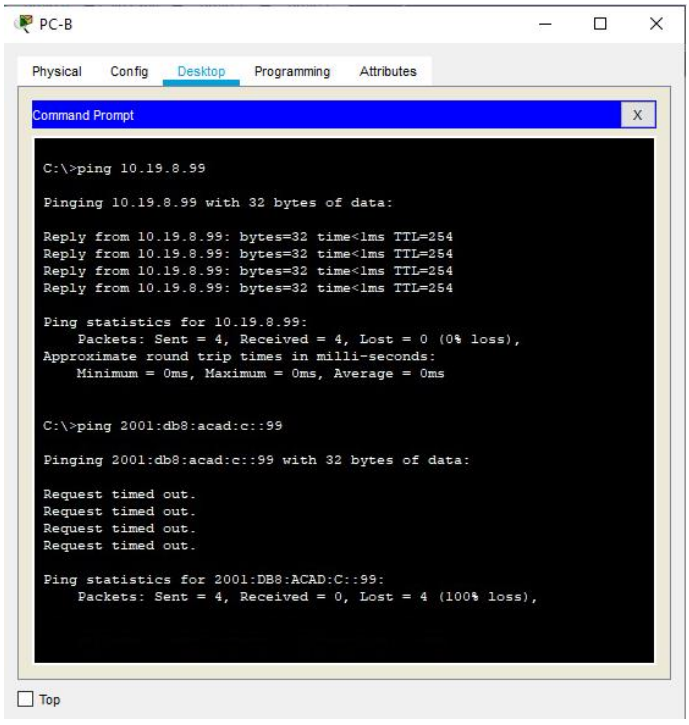
Figuras 24. Ping PC-B a 2001:db8:acad:c::1



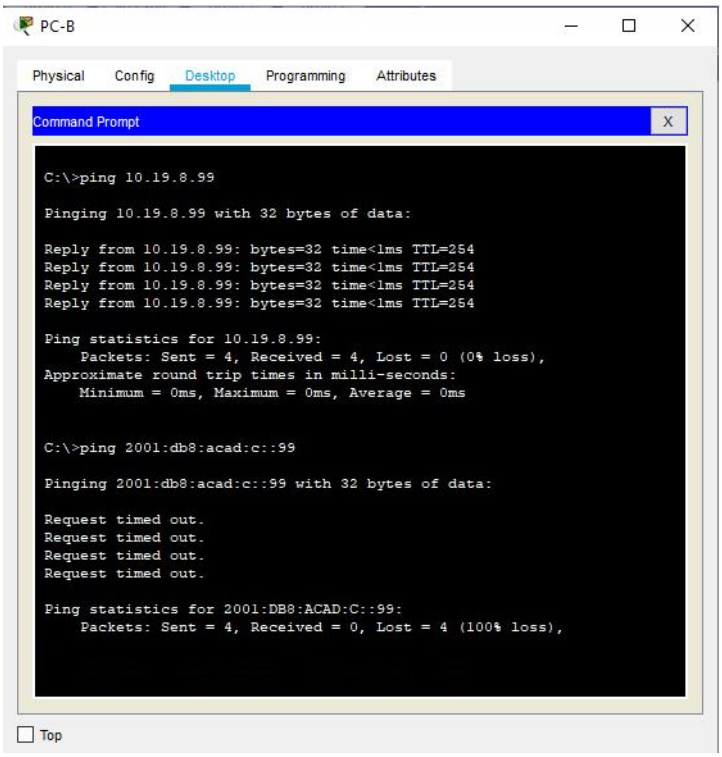
Figuras 25. Ping PC-B a 10.19.8.98



Figuras 26. Ping PC-B a 2001:db8:acad:c::99

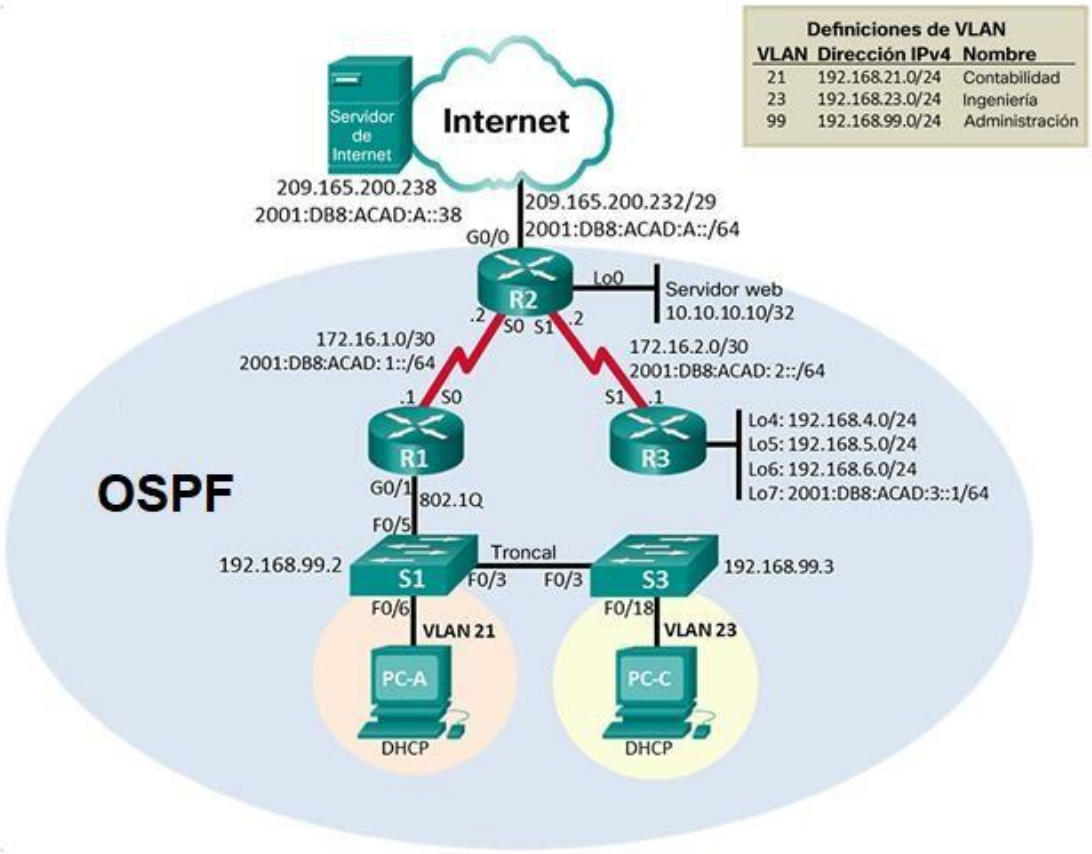


Figuras 27. Ping PC-B a 10.19.8.99

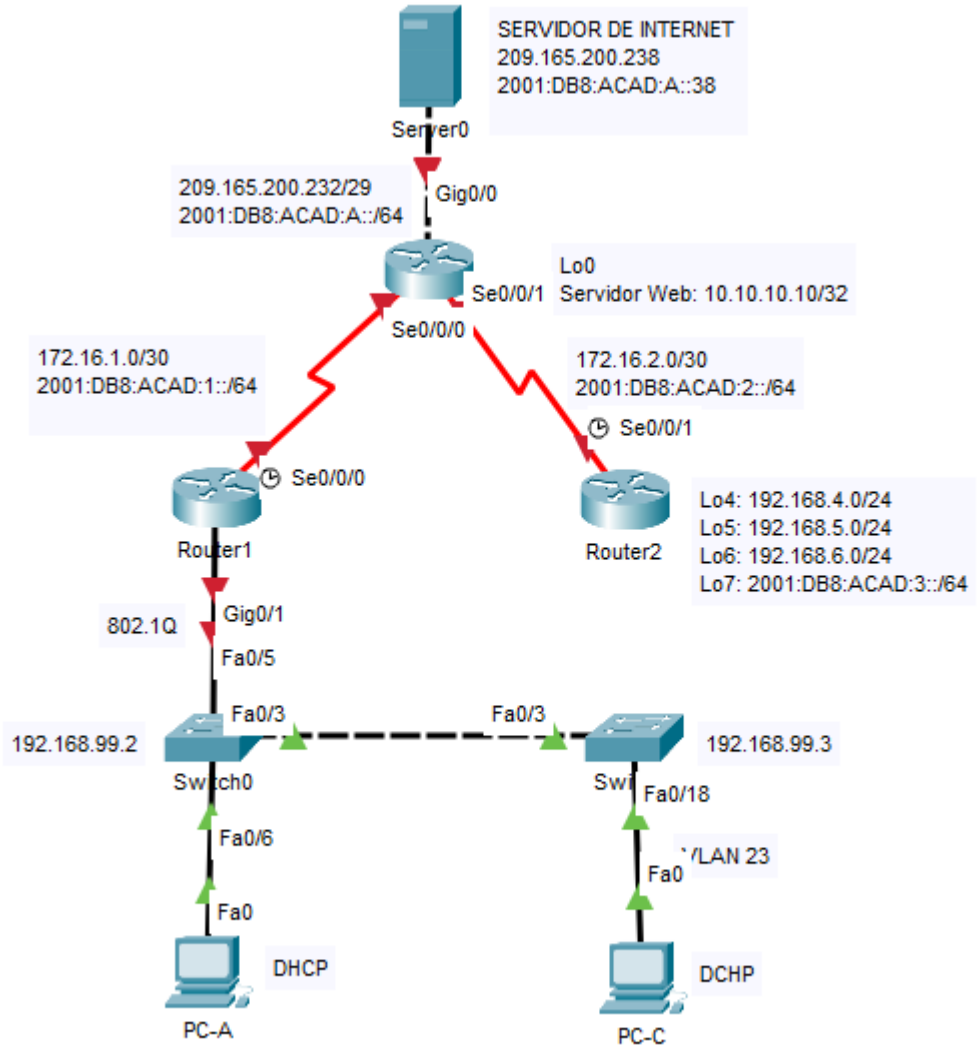


Figuras 28. Ping PC-B a 2001:db8:acad:c::99

2 ESCENARIO DOS



Figuras 29. Topología escenario dos



Figuras 30. Topología en Packet Tracer

2.1 PARTE 1: INICIALIZAR DISPOSITIVOS

2.1.1 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 13. Inicialzar Dispositivos

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	Router> Router>en Router#erase startup-config Continue? [confirm]y[OK]
Volver a cargar todos los routers	Router> Router>en Router#reload Proceed with reload? [confirm]y
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Switch> Switch>en Switch#erase startup-config Continue? [confirm]y[OK]0 Switch> Switch>en Switch#delete vlan.dat Switch#
Volver a cargar ambos switches	Switch> Switch>en Switch#reload Proceed with reload? [confirm]y
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Switch> Switch>en Switch#show flash: Switch#exit

2.2 PARTE 2: CONFIGURAR LOS PARÁMETROS BÁSICOS DE LOS DISPOSITIVOS

2.2.1 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 14. Configuracion 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	209.165.200.225
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.

2.2.2 Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 15. Configurar R1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Para la desactivación utilizamos el comando **no ip domain-lookup**
Nombre del router	R1 lo realizamos con el comando hostname
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	El comando service password-encryption aplica un cifrado débil a todas las contraseñas sin cifrar.
Mensaje MOTD	Se prohíbe el acceso no autorizado.
Interfaz S0/0/0	Establezca la descripción Establecer la dirección IPv4 Consultar el diagrama de topología para conocer la información de direcciones Establecer la dirección IPv6 Consultar el diagrama de topología para conocer la información de direcciones Establecer la frecuencia de reloj en 128000 Activar la interfaz
Rutas predeterminadas	Configurar una ruta IPv4 predeterminada de S0/0/0 Configurar una ruta IPv6 predeterminada de S0/0/0

- Ingresamos a la configuración del Router con configure terminal se puede escribir de forma abreviada (conf t)

```
Router>en
Router #config t
```

- Para la desactivación de búsquedas DNS utilizamos el comando **no ip domain-lookup**
- Realizamos el cambio del nombre del router con **hostname** y el nombre que le vayamos a poner

```
Router(config)# no ip domain-lookup
Router(config)#hostname R1
```

- Para configurar una contraseña local en niveles de acceso de usuario utilizamos **enable secret** y la contraseña a utilizar

```
R1(config)#enable secret class
R1(config)#line con 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config)#end
R1>en
R1#config t
```

- Los siguientes comandos se usan en el modo de configuración global para establecer una contraseña para la línea de consola

```
R1(config)#line vty 0 4
R1(config-line)#password cisco
R1(config-line)#login
R1(config)#end
R1>en
R1#config t
```

- para la encriptación de las contraseñas asignadas tanto para la consola como para la línea de comandos utilizamos el siguiente comando

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

- Con el siguiente comando colocamos un mensaje de advertencia para ingresar al dispositivo.

R1(config)#banner motd “Acceso permitido solo para Administradores”

- Con los siguientes comandos ingresaremos a cada interfaz del router y asignaremos las ips según la tabla de direcciones una vez creadas no olvidar encender la interfaz con el comando no shutdown.

```
R1(config)#int serial 0/0/0
R1(config-if)#ip add 172.16.1.1 255.255.255.252
R1(config-if)#ipv6 add 2001:DB8:ACAD:1::1/64
R1(config-if)#clock rate 128000
R1(config-if)#description ROUTER1
R1(config-if)#no shut
R1(config)#end
R1>en
R1#config t
R1(config)#ip route 0.0.0.0 0.0.0.0 serial 0/0/0
R1(config)#ipv6 route ::/0 serial 0/0/0
R1(config)#end
```

2.2.3 Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Tabla 16. Configurar R2

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Para la desactivación utilizamos el comando **no ip domain-lookup**
Nombre del router	R2 lo realizamos con el comando hostname
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	El comando service password-encryption aplica un cifrado débil a todas las contraseñas sin cifrar.
Habilitar el servidor HTTP	Utilizamos el comando ip http server
Mensaje MOTD	Se prohíbe el acceso no autorizado.

Interfaz S0/0/0	Establezca la descripción Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz
Interfaz S0/0/1	Establecer la descripción Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Establecer la frecuencia de reloj en 128000. Activar la interfaz
Interfaz G0/0 (simulación de Internet)	Establecer la descripción. Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Establezca la dirección IPv6. Utilizar la primera dirección disponible en la subred. Activar la interfaz
Interfaz loopback 0 (servidor web simulado)	Establecer la descripción. Establezca la dirección IPv4.
Ruta predeterminada	Configure una ruta IPv4 predeterminada de G0/0. Configure una ruta IPv6 predeterminada de G0/0.

Router>en
Router #config t

- Para la desactivación de búsquedas DNS utilizamos el comando **no ip domain-lookup**
- Realizamos el cambio del nombre del router con **hostname** y el nombre que le vayamos a poner

Router(config)# no ip domain-lookup
Router(config)#hostname R2

- Para configurar una contraseña local en niveles de acceso de usuario utilizamos **enable secret** y la contraseña a utilizar

```
R2(config)#enable secret class
R2(config)#line con 0
R2(config-line)#password cisco
R2(config-line)#login
R2(config)#end
R2>en
R2#config t
```

- Los siguientes comandos se usan en el modo de configuración global para establecer una contraseña para la línea de consola

```
R2(config)#line vty 0 4
R2(config-line)#password cisco
R2(config-line)#login
R2(config)#end
R2>en
R2#config t
```

- para la encriptación de las contraseñas asignadas tanto para la consola como para la línea de comandos utilizamos el siguiente comando

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

- habilitamos el servidor http con el siguiente comando.

```
R2(config)#ip http-server
R2(config)#end
R2>en R2#config t
```

- Con el siguiente comando colocamos un mensaje de advertencia para ingresar al dispositivo.

```
R2(config)#banner motd “Acceso permitido solo para Administradores”
```

- Con los siguientes comandos ingresaremos a *cada interfaz* del router y asignaremos las ips según la tabla de direcciones una vez creadas no olvidar encender la interfaz con el comando ***no shutdown*** *y* con el comando **description** podemos escribir algo que identifique la configuración de cada interfaz.

```
R2(config)#int s0/0/0
R2(config-if)#description ROUTER2
```

```
R2(config-if)#ip add 172.16.1.2 255.255.255.252
R2(config-if)#ipv6 add 2001:db8:acad:1::2/64
R2(config-if)#no shut
R2(config-if)#exit
R2(config)#int s0/0/1
R2(config-if)#description ROUTER3
R2(config-if)#ip add 172.16.2.2 255.255.255.252
R2(config-if)#ipv6 add 2001:db8:acad:2::2/64
R2(config-if)#clock rate 128000
R2(config-if)#no shut
R2(config-if)#exit
R2(config)#inter g0/0
R2(config-if)#description Servidor Internet
R2(config-if)#ip add 209.165.200.233 255.255.255.248
R2(config-if)#ipv6 add 2001:db8:acad:A::1/64
R2(config-if)#no shut
R2(config-if)#exit
R2(config-f)#int loopback 0
R2(config-if)#description Servidor Web
R2(config-if)#ip add 10.10.10.10 255.255.255.255
R2(config-if)#exit
R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0
R2(config)#ipv6 route ::/0 g0/0
R2(config)#end
```

2.2.4 Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Tabla 17. Configurar R3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	
Nombre del router	R3
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	

Mensaje MOTD	Se prohíbe el acceso no autorizado.
Interfaz S0/0/1	Establecer la descripción Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz
Interfaz loopback 4	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.
Interfaz loopback 5	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.
Interfaz loopback 6	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.
Interfaz loopback 7	Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.
Rutas predeterminadas	

Router>en
Router #config t

- Para la desactivación de búsquedas DNS utilizamos el comando **no ip domain-lookup**
- Realizamos el cambio del nombre del router con **hostname** y el nombre que le vayamos a poner

Router(config)# no ip domain-lookup
Router(config)#hostname R3

- Para configurar una contraseña local en niveles de acceso de usuario utilizamos **enable secret** y la contraseña a utilizar

R3(config)#enable secret class
R3(config)#line con 0
R3(config-line)#password cisco
R3(config-line)#login

R3(config)#end
R3>en
R3#config t

- Los siguientes comandos se usan en el modo de configuración global para establecer una contraseña para la línea de consola:

R3(config)#line vty 0 4
R3(config-line)#password cisco
R3(config-line)#login
R3(config)#exit

- Para la encriptación de las contraseñas asignadas tanto para la consola como para la línea de comandos utilizamos el siguiente comando

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

- Con el siguiente comando colocamos un mensaje de advertencia para ingresar al dispositivo.

R3(config)#banner motd “Acceso Permitido Solo para Administradores”

- Con los siguientes comandos ingresaremos a *cada interfaz* del router y asignaremos las ips según la tabla de direcciones una vez creadas no olvidar encender la interfaz con el comando ***no shutdown*** *y* con el comando **description** podemos escribir algo que identifique la configuración de cada interfaz.

R3config)#inter s0/0/1
R3(config-if)#description Router3
R3(config-if)#ip add 172.16.2.1 255.255.255.252
R3(config-if)#ipv6 add 2001:db8:acad:2::1/64
R2(config-if)#no shut
R2(config-if)#exit
R3(config)#interface loopback 4
R3(config-if)#ip add 192.168.4.1 255.255.255.0
R3(config-if)#exit
R3(config)#interface loopback 5
R3(config-if)#ip add 192.168.5.1 255.255.255.0
R3(config-if)#exit
R3(config)#interface loopback 6
R3(config-if)#ip add 192.168.6.1 255.255.255.0
R3(config-if)#exit

R3(config)#interface loopback 7
R3(config-if)#ipv6 add 2001:db8:acad:3::1/64
R3(config-if)#exit
R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1
R3(config)#ipv6 route ::/0 s0/0/1
R3(config-if)#end

2.2.5 Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 18. Configurar S1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	
Nombre del switch	S1
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	
Mensaje MOTD	Se prohíbe el acceso no autorizado.

Switch>en
Switch#config t

- Para la desactivación de búsquedas DNS utilizamos el comando **no ip domain-lookup**
- Realizamos el cambio del nombre del router con **hostname** y el nombre que le vayamos a poner

Switch(config)# no ip domain-lookup
Switch(config)#hostname S1

- Para configurar una contraseña local en niveles de acceso de usuario utilizamos **enable secret** y la contraseña a utilizar

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

- Los siguientes comandos se usan en el modo de configuración global para establecer una contraseña para la línea de consola.

```
S1#config t
S1(config)#line con 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config)#end
S1>en
S1#config t
```

- El comando que utilizamos para establecer una contraseña en las líneas vty es el siguiente:

```
S1(config)#line vty 0 4
S1(config-line)#password cisco
S1(config-line)#login
S1(config)#end
S1>en
S1#config t
```

- para la encriptación de las contraseñas asignadas tanto para la consola como para la línea de comandos utilizamos el siguiente comando

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

- Con el siguiente comando colocamos un mensaje de advertencia para ingresar al dispositivo.

```
S1(config)#banner motd “Acceso solo permitido para Administradores”
S1(config)#end
```

2.2.6 Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 19. Configurar S3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	
Nombre del switch	S3
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco

Cifrar las contraseñas de texto no cifrado	
Mensaje MOTD	Se prohíbe el acceso no autorizado.

Switch>en
Switch#config t

- Para la desactivación de búsquedas DNS utilizamos el comando **no ip domain-lookup**
- Realizamos el cambio del nombre del router con **hostname** y el nombre que le vayamos a poner

Switch(config)# no ip domain-lookup
Switch(config)#hostname S3

- Para configurar una contraseña local en niveles de acceso de usuario utilizamos **enable secret** y la contraseña a utilizar

S3(config)#enable secret class
S3(config)#line con 0
S3(config-line)#password cisco
S3(config-line)#login
S3(config)#end

- Los siguientes comandos se usan en el modo de configuración global para establecer una contraseña para la línea de consola:

S3>en
S3#config t
S3(config)#line vty 0 4
S3(config-line)#password cisco
S3(config-line)#login
S3(config)#end

- para la encriptación de las contraseñas asignadas tanto para la consola como para la línea de comandos utilizamos el siguiente comando

S3>en
S3#config t
S3(config)#service password-encryption

- Con el siguiente comando colocamos un mensaje de advertencia para ingresar al dispositivo.

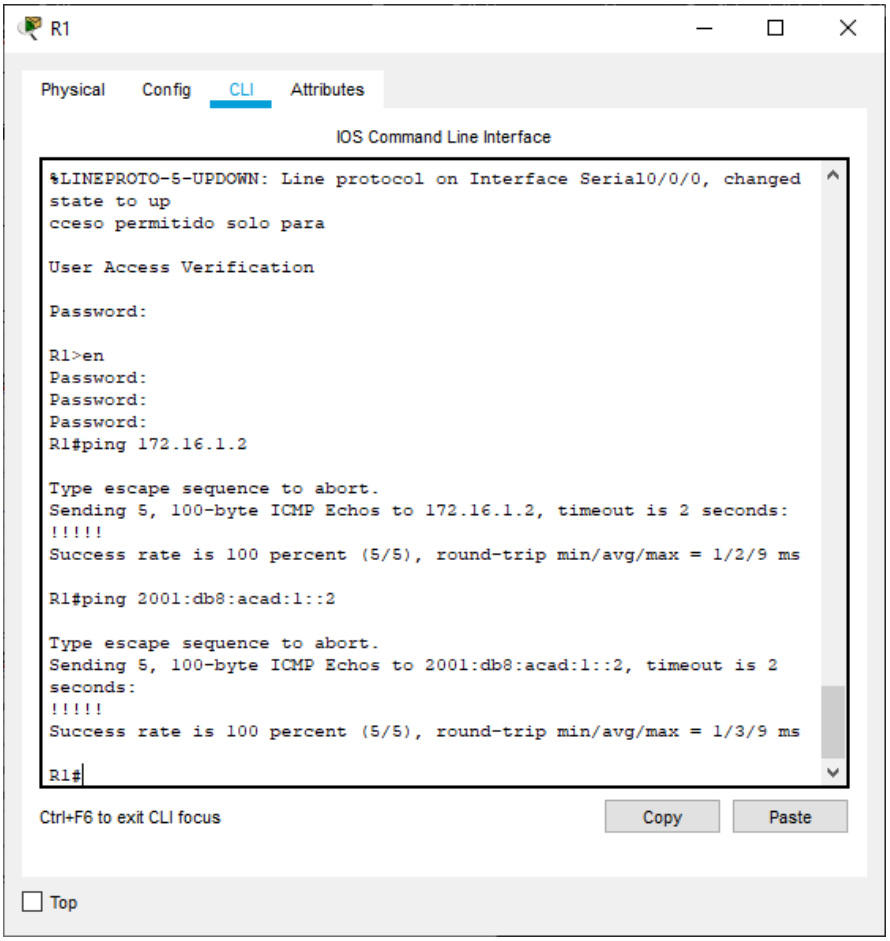
S3(config)#banner motd “Acceso ´permitido solo para Administradores”
S3(config)#end

2.2.7 Paso 7: Verificar la conectividad de la red

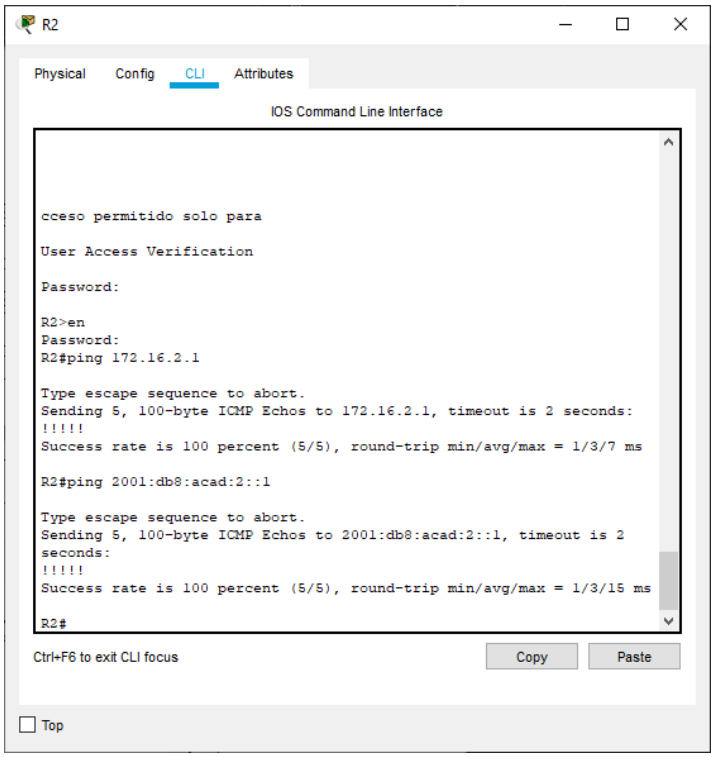
Utilice el comando ping para probar la conectividad entre los dispositivos de red. Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 20. Verificacion de Conectividad

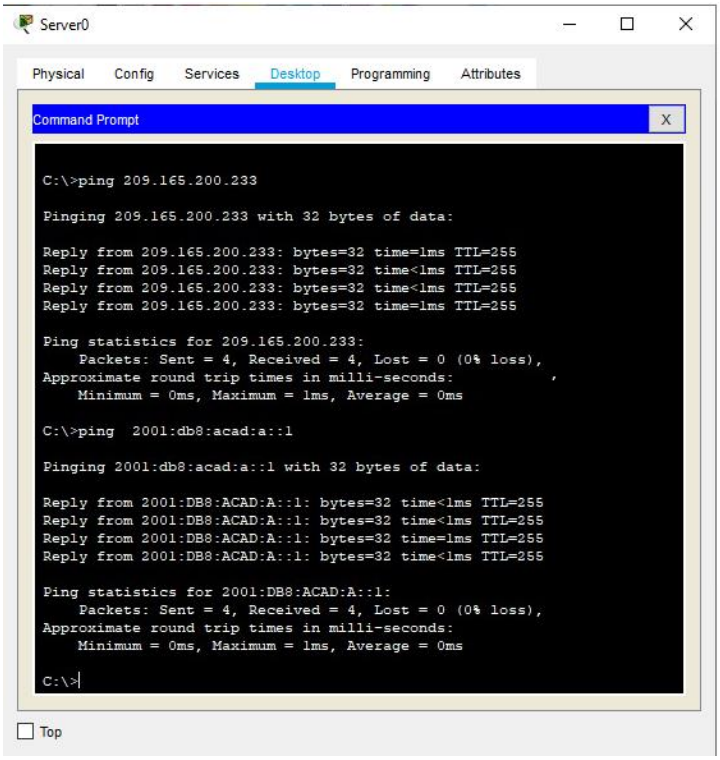
Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2 2001:db8:acad:1::2	*Figura 31*
R2	R3, S0/0/1	172.16.2.1 2001:db8:acad:2::1	*Figura 32*
PC de Internet	Gateway predeterminado	209.165.200.233 2001:db8:acad:a::1	*Figura 33*



Figuras 31. Ping R1 a 172.16.1.2 y 2001:db8:acad:1::2



Figuras 32. Ping R2 a 172.16.2.1 y 2001:db8:acad:2::1



Figuras 33. Ping Server0 a 209.165.100.233

2.3 PARTE 3: CONFIGURAR LA SEGURIDAD DEL SWITCH, LAS VLAN Y EL ROUTING ENTRE VLAN

2.3.1 Paso 1: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 21. Configuración 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
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
Asignar el gateway predeterminado	Asigne la primera dirección IPv4 de la subred como el gateway predeterminado.
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa
Forzar el enlace troncal en la interfaz F0/5	Utilizar la red VLAN 1 como VLAN nativa
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range
Asignar F0/6 a la VLAN 21	
Apagar todos los puertos sin usar	

- Con los siguientes comandos que miramos a continuación creamos las vlan y les colocamos los nombres según tabla 18. Configuración S1

```
S1>en
S1#config t
S1(config)#vlan 21
S1(config)#name Contabilidad
S1(config-vlan)#exit
S1(config)#vlan 23
S1(config)#name Ingenieria
S1(config-vlan)#exit
S1(config)#vlan 99
S1(config)#name Administracion
S1(config-vlan)#exit
```

- Con los siguientes comandos asignamos las ips a las vlan creadas

S1(config)#int vlan 99
S1(config-if)#ip add 192.168.99.2 255.255.255.0
S1(config)#exit

- Colocamos la puerta de enlace predeterminada para la vlan 99

S1(config)#ip default-gateway 192.168.99.1

- Con los siguientes comandos configuramos las interfaces 3 y 5 con la vlan solicitadas.

S1(config)#int fa0/3
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 1
S1(config-if)#exit
S1(config)#int fa0/5
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 1
S1(config-if)#exit

- Con este comando colocamos las interfaces 1 y 2 en modo acceso

S1(config)#int range fa0/1 - fa0/2
S1(config-if-range)#switchport mode access

- Con este comando colocamos las interfaces de 7 al 24 en modo acceso

S1(config-if-range)#inter range fa0/7 - fa0/24
S1(config-if-range)#switchport mode access
S1(config-if-range)#exit
S1(config)#int fa0/4
S1(config-if)#switchport mode access
S1(config-if)#exit

- Con el comando switchport access asignamos la vlan 21 a la interfaz 6

S1(config)#inter fa0/6
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 21
S1(config-if)#exit

- Con este comando escogemos el rango de interfaces que vamos apagar en este caso de 1 y 2.

S1(config)#inter range fa0/1 - fa0/2
S1(config-if-range)#shut

- Con este comando escogemos el rango de interfaces que vamos a pagar en este caso de 7 a 24.

S1(config-if-range)#inter range fa0/7 - fa0/24
S1(config-if-range)#shut
S1(config-if-range)#exit
S1(config)#inter fa0/4
S1(config-if)#shut
S1(config-if)#end

2.3.2 Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 22. Configuracion 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.
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
Asignar el gateway predeterminado.	Asignar la primera dirección IP en la subred como gateway predeterminado.
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range
Asignar F0/18 a la VLAN 21	
Apagar todos los puertos sin usar	

Con los siguientes comandos que miramos a continuación creamos las vlan y les colocamos los nombres según tabla 19 configuración S3
S3>en
S3#config t
S3(config)#vlan 21
S3(config)#name Contabilidad
S3(config)#vlan 23
S3(config)#name Ingenieria
S3(config)#vlan 99
S3(config)#name Administracion
S3(config)#exit

- Con los siguientes comandos asignamos las ips a las vlan creadas

S3(config)#int vlan 99
S3(config-if)#ip add 192.168.99.3 255.255.255.0
S3(config)#exit

- Colocamos la puerta de enlace prederterminada para la vlan 99

S3(config)#ip default-gateway 192.168.99.1

- Con los siguientes comandos configuramos las interfaces 3 con la vlan 1 solicitadas.

S3(config)#inter fa0/3
S3(config-if)#switchport mode trunk
S3(config-if)#switchport trunk native vlan 1
S3(config-if)#exit

- Con este comando colocamos las interfaces 1 y 2 en modo acceso

S3(config)#inter range fa0/1 - fa0/2
S3(config-if-range)#switchport mode access
S3(config-if-range)#exit

- Con este comando colocamos las interfaces 4 al 17 en modo acceso

S3(config)#inter range fa0/4 - fa0/17
S3(config-if-range)#switchport mode access
S3(config-if-range)#exit

- Con este comando colocamos las interfaces 19 al 24 en modo acceso

S3(config)#inter range fa0/19 - fa0/24
S3(config-if-range)#switchport mode access
S3(config-if-range)#exit

- Con este comando colocamos las interfaces 18 en modo acceso

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

- Con este comando apagamos el rango de interfaces 1 y 2

S3(config)#inter range fa0/1 - fa0/2
S3(config-if-range)#shut

- Con este comando apagamos el rango de interfaces 4 al 17

S3(config-if-range)#inter range fa0/4 - fa0/17
S3(config-if-range)#shut

- Con este comando apagamos el rango de interfaces 19 al 24

S3(config-if-range)#inter range fa0/19 - fa0/24
S3(config-if-range)#shut
S3(config-if)#end

2.3.3 Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:
Tabla 23. Configuracion R1

Elemento o tarea de configuración	Especificación
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
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
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
Activar la interfaz G0/1	

- Con los siguientes comandos ingresaremos a *la interfaz g0/1* del router y asignaremos las ips *de las subredes* según la Tabla 24. Asignación de direcciones una vez creadas no olvidar encender la interfaz con el comando no shutdown.

R1>en
R1#config t

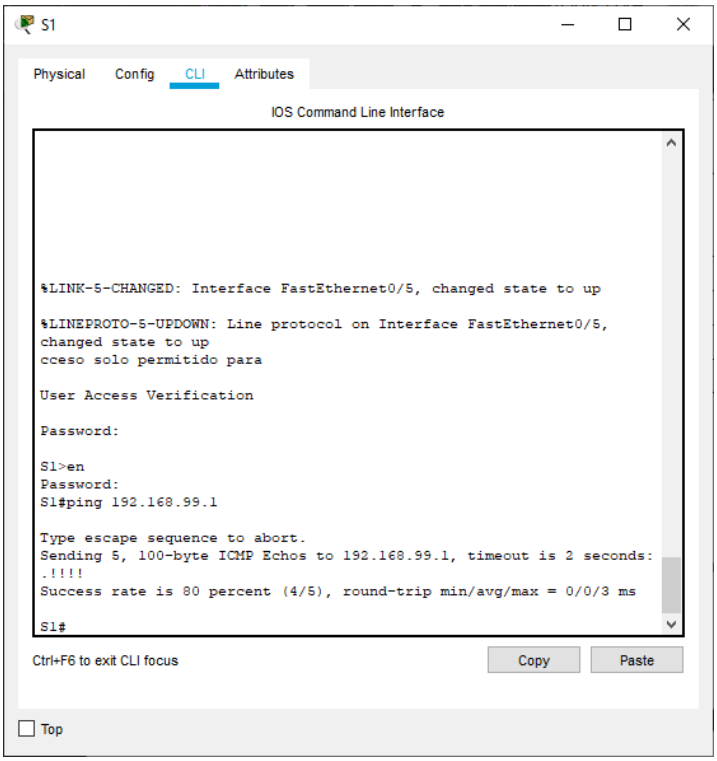
R1(config)#int g0/1.21
R1(config-if)#des LAN de Contabilidad
R1(config-if)#encap dot1q 21
R1(config-subif)#ip add 192.168.21.1 255.255.255.0
R1(config-subif)#exit
R1(config)#int g0/1.23
R1(config-if)#des LAN de Ingenieria
R1(config-if)#encap dot1q 23
R1(config-subif)#ip add 192.168.23.1 255.255.255.0
R1(config-subif)#exit
R1(config)#inter g0/1.99
R1(config-if)#des LAN de Administracion
R1(config-if)#encap dot1q 99
R1(config-subif)#ip add 192.168.99.1 255.255.255.0
R1(config-subif)#exit
R1(config)#inter g0/1
R1(config)#no shut
R1(config)#end

2.3.4 Paso 4: Verificar la conectividad de la red

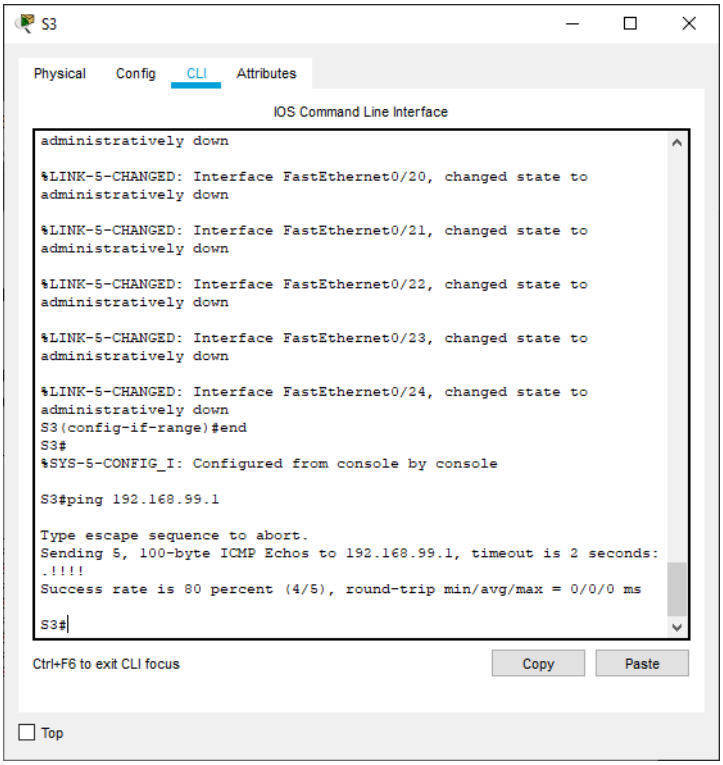
Utilice el comando ping para probar la conectividad entre los switches y el R1.
Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 25. Verificacion de Conectividad

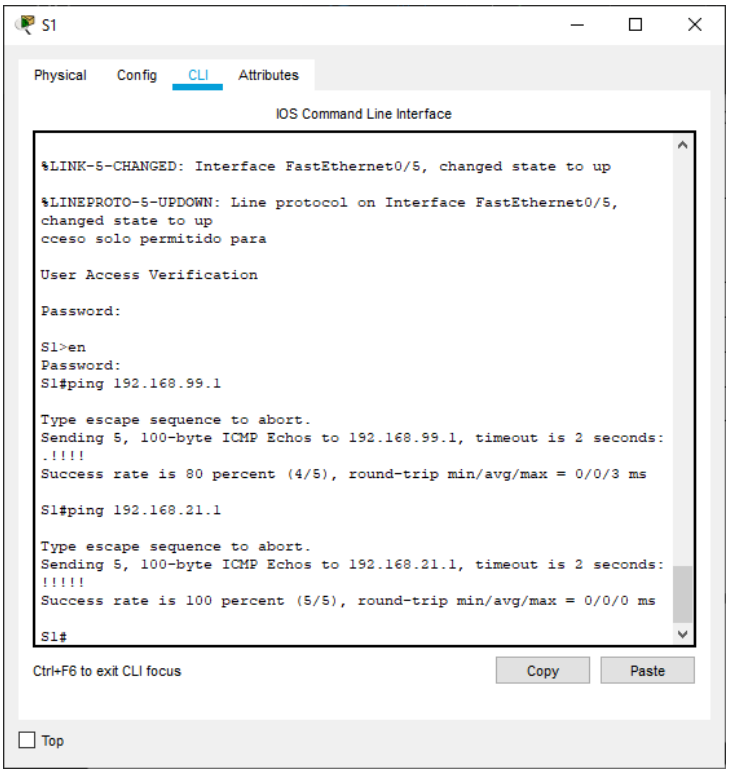
Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	*Figura 34*
S3	R1, dirección VLAN 99	192.168.99.1	*Figura 35*
S1	R1, dirección VLAN 21	192.168.21.1	*Figura 36*
S3	R1, dirección VLAN 23	192.168.23.1	*Figura 37*



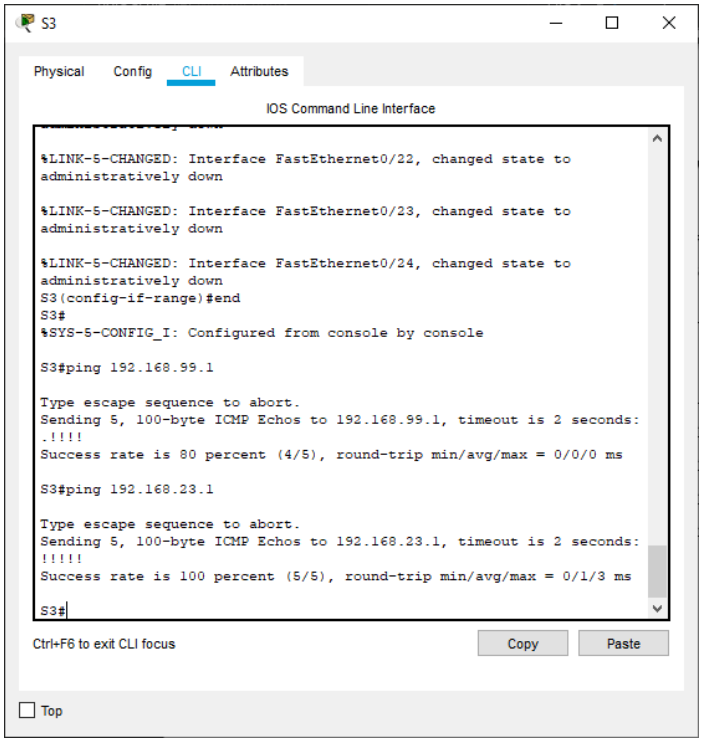
Figuras 34. Ping S1 a 192.168.99.1



Figuras 35. Ping S3 a 192.168.99.1



Figuras 36. Ping S1 a 192.168.21.1



Figuras 37. Ping S3 a 192.168.23.1

2.4 PARTE 4: CONFIGURAR EL PROTOCOLO DE ROUTING DINÁMICO OSPF

2.4.1 Paso 1: Configurar OSPF en el R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 26. Configuracion OSPF en R1

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	
Anunciar las redes conectadas directamente	Asigne todas las redes conectadas directamente.
Establecer todas las interfaces LAN como pasivas	
Desactive la sumarización automática	

- Para habilitar la autenticación en OSPF para intercambiar la información de actualización de ruteo de una forma segura utilizamos la siguiente configuracion.

```
R1>en
R1#config t
R1(config)#router ospf 1
R1(config-router)#exit
R1(config)#router ospf 10
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)#network 172.16.1.0 0.0.0.3 area 0
```

- Establecemos todas las interfaces LAN como pasivas de la siguiente forma.

```
R1(config-router)#passive-interface g0/1
R1(config-router)#end
R1>en
R1#config t
R1(config)#router ospf 10
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)#network 172.16.1.0 0.0.0.3 area 0
```

R1(config-router)#end

2.4.2 Paso 2: Configurar OSPF en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla 27. Configurar OSPF en R2

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	
Anunciar las redes conectadas directamente	**Nota:** Omitir la red G0/0.
Establecer la interfaz LAN (loopback) como pasiva	
Desactive la sumarización automática.	

- Para habilitar la autenticación en OSPF para intercambiar la información de actualización de ruteo de una forma segura utilizamos la siguiente configuracion.

R2>en
R2#config t
R2(config)#router ospf 10
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

- Para establecer la interfaz LAN (loopback) como pasiva utilizamos el siguiente comando.

R2(config-router)#passive-interface loopback 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)#end

2.4.3 Paso 3: Configurar OSPFv3 en el R2

La configuración del R3 incluye las siguientes tareas:

Tabla 28. Configuracion OSPFV3 en R2

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	
Anunciar redes IPv4 conectadas directamente	
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	

Desactive la sumarización automática.	

- Para habilitar la autenticación en OSPF para intercambiar la información de actualización de ruteo de una forma segura utilizamos la siguiente configuracion.

```
R3>en
R3#config t
R3(config)#router ospf 1
```

- Establecemos todas las interfaces de LAN IPv4 (Loopback) como pasivas de la siguiente forma.

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

2.4.4 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 29. Verificación de información en 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 ospf interface
¿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 | sec router ospf

2.4.5 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 30. Configuración R1 DHCP y NAT

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	
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
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

- Para reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas realizamos los siguiente:

```
R1>en
R1#config t
R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20
R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20
R1(config)#ip dhcp pool ACCT
R1(dhcp-config)#network 192.168.21.0 255.255.255.0
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
```

Tabla 31. Configuacion HTTP.

Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	Nombre de usuario: **webuser** Contraseña: **cisco12345** Nivel de privilegio: **15**

Habilitar el servicio del servidor HTTP	
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	
Crear una NAT estática al servidor web.	Dirección global interna: **209.165.200.229**
Asignar la interfaz interna y externa para la NAT estática	
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
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**
Definir la traducción de NAT dinámica	

R1(dhcp-config)#exit
R1(config)#ip dhcp pool ENGNR
R1(dhcp-config)#network 192.168.23.0 255.255.255.0
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)#end

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

La configuración del R2 incluye las siguientes tareas:

- Con el siguiente comando creamos una base de datos local con una cuenta de usuario

R2>en
R2#config t
R2(config)#username webuser privilege 15 password cisco12345

- Habilitarmos el servicio del servidor HTTP con el siguiente comando.

R2(config)#ip http server

- Configuramos el servidor HTTP para utilizar la base de datos local para la autenticación de la siguiente forma:

R2(config)#ip http authentication local
R2(config)#ip nat inside source static 209.165.200.233 209.165.200.229

- Asignamos la interfaz interna y externa para la NAT estática de esta forma:

R2(config)#int g0/0
R2(config-if)#ip nat outside
R2(config-if)exit
R2(config)#int s0/0/0
R2(config-if)#ip nat inside
R2(config-if)#exit

- Es así como creamos una lista de acceso para Configurar la NAT dinámica dentro de una ACL privada

R2(config)#ip access-list standard 1
R2(config-std-nacl)#permit 192.168.21.0 0.0.0.255
R2(config-std-nacl)#permit 192.168.23.0 0.0.0.255
R2(config-std-nacl)#exit
R2(config)#int s0/0/1
R2(config-if)#ip nat outside
R2(config-if)#exit

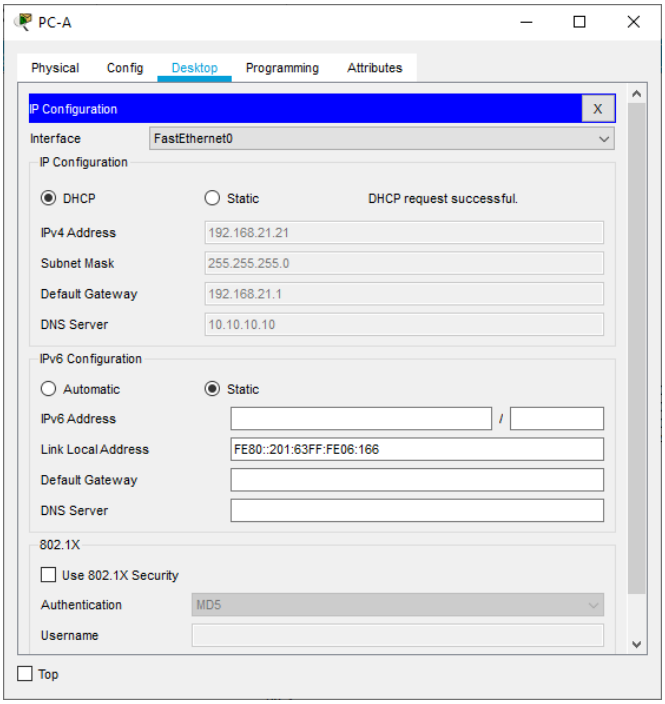
- Definimos el pool de direcciones IP públicas utilizables de la siguiente forma.

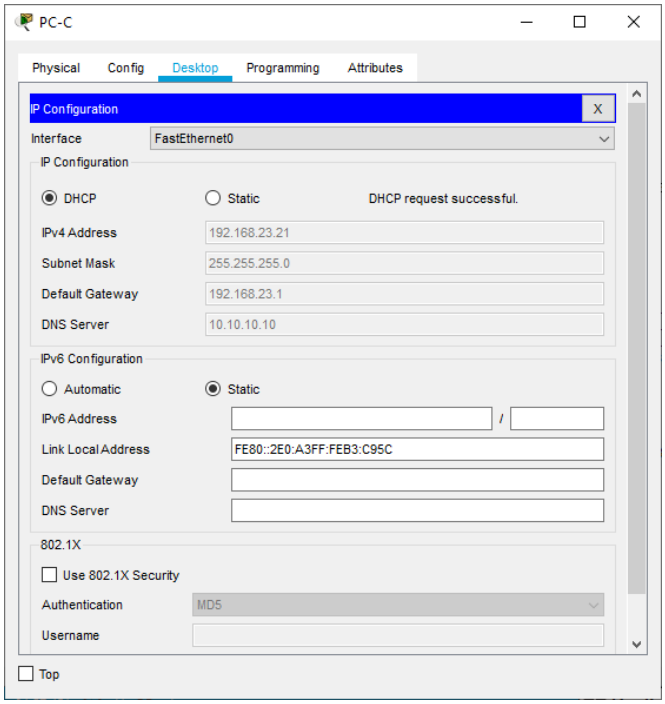
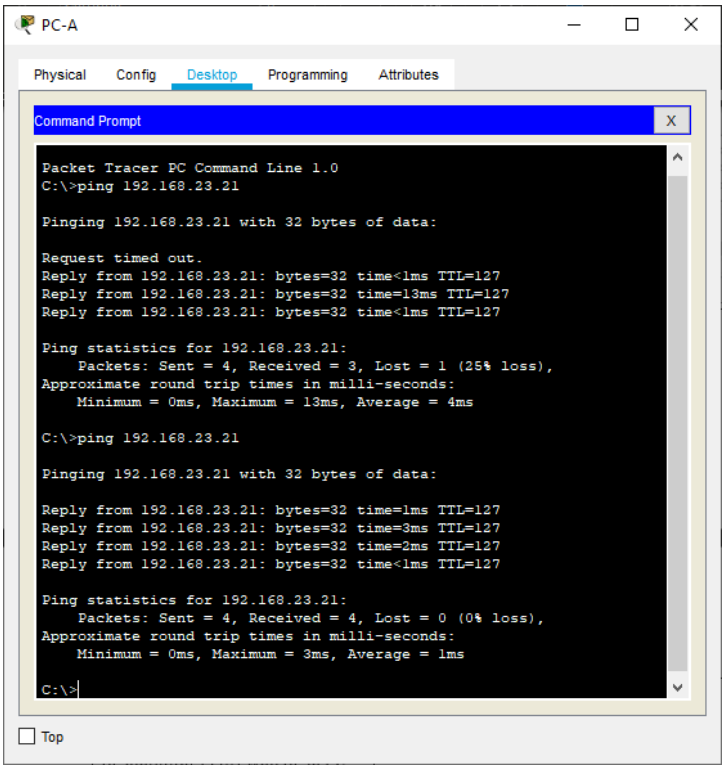
R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248
R2(config)#ip nat inside source list 1 pool INTERNET
R2(config)#end

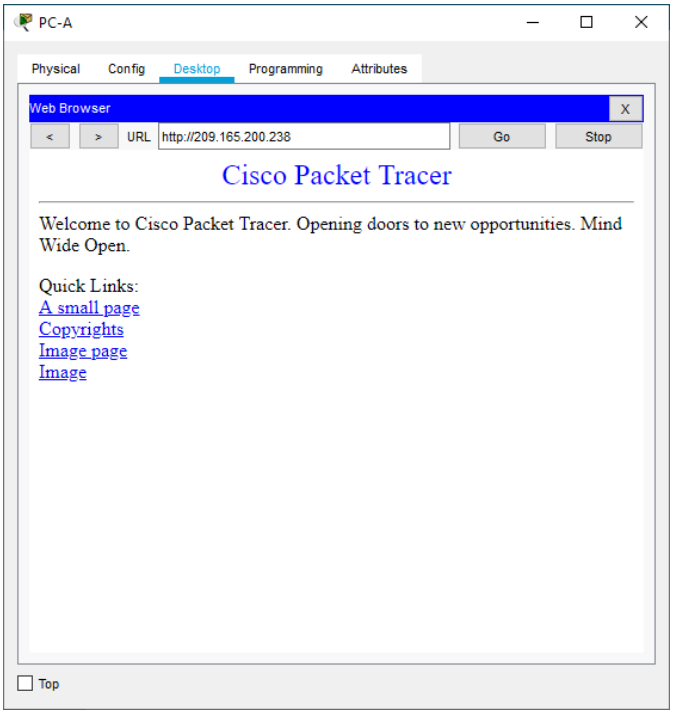
2.4.7 Paso 3: Verificar el protocolo DHCP y la NAT estática

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 32. Verificacion de Protoclo DCHP y NAT

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	 *Figuras 38. Configuración PC-A*

Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	 *Figuras 39. Configuración PC-C*
Verificar que la PC-A pueda hacer ping a la PC-C **Nota:** Quizá sea necesario deshabilitar el firewall de la PC.	 *Figuras 40. Ping PC-A a PC-C*

Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.238) Iniciar sesión con el nombre de usuario **webuser** y la contraseña **cisco12345**	

Figuras 41. Verificación Sitio Web

2.5 PARTE 6: CONFIGURAR NTP

Tabla 33. Configuración NTP.

Elemento o tarea de configuración	**Especificación**
Ajuste la fecha y hora en R2.	**5 de marzo de 2016, 9 a. m.**
Configure R2 como un maestro NTP.	Nivel de estrato: **5**
Configurar R1 como un cliente NTP.	Servidor: **R2**
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	
Verifique la configuración de NTP en R1.	

- Configuramos el NTP de la siguiente forma:

R2>en
R2#clock set 09:00:00 March 5 2016
R2#config t
R2(config)#ntp master 5
R1(config)#ntp server 172.16.1.2
R1(config)#ntp update-calendar
R2(config)end

R1#show ntp association

address ref clock st when poll reach delay offset disp
~172.16.1.2 127.127.1.1 5 0 16 277 7.00 726206256104.00 0.12
* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured

2.6 PARTE 7: CONFIGURAR Y VERIFICAR LAS LISTAS DE CONTROL DE ACCESO (ACL)

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

Tabla 34. Configuración Control de Acceso

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**
Aplicar la ACL con nombre a las líneas VTY	
Permitir acceso por Telnet a las líneas de VTY	
Verificar que la ACL funcione como se espera	

- Configuamos la ACL segun lo solicitado de la siguiente manera.

R2>en
R2#config t
R2(config)#ip access-list extended ADMIN-MGT
R2(config-ext-nacl)#permit ip host 172.16.1.1 any
R2(config-ext-nacl)exit

- Aplicamos la ACL con nombre a las líneas VTY de la siguiente forma.

R2(config)#line vty 0 4
R2(config-line)#access-class ADMIN-MGT in
R2(config-line)#exit
R2(config-line)#transport input telnet
R2(config-line)#end

- así se permite el acceso a telnet al R2

R1#telnet 172.16.1.2
Trying 172.16.1.2 ...Opencceso permitido solo para

User Access Verification

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

Tabla 35. Comandos CLI

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 show ip access-lists <acl number> show ip access-lists <acl name>
Restablecer los contadores de una lista de acceso	clear access-list counters clear access-list counters <acl number> clear access-list counters <acl name>
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	show ip interface
¿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 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. show ip nat translations

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

3 CONCLUCIONES

El desarrollo de estas prácticas en Packet Tracer permite tener un acercamiento más profundo en lo relacionado a la configuración de dispositivos de comunicaciones, al igual que aclarar dudas sobre las diferentes pruebas a realizar para validar las configuraciones aplicadas.

Estos elementos de diseño de redes enriquecen las experiencias de aprendizaje, evidenciado una serie de pasos e imágenes que permiten instruir a cada lector de este documento permitiendo formar expectativas, conocimiento tecnológico de la importancia en estar al tanto de los cambios que se realizan en la protección de los datos de cada cliente, empresa o red digital que hay en diferentes lugares dependiendo de su situación organizacional.

La finalidad encontrada es dar a conocer todas las posibles configuraciones en los dispositivos de red, como un mecanismo para compartir recursos, por lo cual debemos conectar físicamente los ordenadores en la cual se puede transmitirse datos a larga distancia, interconectando facilidades de comunicación entre diferentes localidades de un país.

Lo básico es saber escoger un tipo de red, elegir los protocolos a utilizar y elegir el sistema operativo de red.

BIBLIOGRAFIA

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

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

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

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

ANEXOS

Anexo A. Simulaciones en Packet Tracer

https://drive.google.com/file/d/1ZQ_56VDX0vGJ4ThfsgSmWrJk74RPZ5_D/view?usp=sharing

Anexo B. Articulo Científico

IMPLEMENTACION DE UNA SOLUCION INTEGRAL PARA LA SEGURIDAD DE UNA RED PEQUEÑA.

Darwin Dorado
Universidad Nacional Abierta y a Distancia UNAD, dodoradop@unadvirtual.edu.co

Resumen

Al realizar la implementación de una red para una empresa es muy probable que en el camino se encuentre con varios tropiezos, ya sea de configuración o de los dispositivos en cuestión de hardware, que de aquí la importancia de generar una prevención con los procesos fundamentales para la realización de buenas prácticas en cuanto a tomar modelos de prolongar métodos de seguridad en las organizaciones al implementar diferentes modos de comunicación mundial por medio de la aplicación de comandos que permitirán tener una red totalmente segura y funcional. Por esta razón, el escenario número dos escogidos para el presente proyecto.
Se realizarán las modificaciones necesarias para mejorar en todo aspecto las características de la red de datos y las comunicaciones del escenario propuesto, ya que la red ha presentado varios conflictos. *

La seguridad de los dispositivos que se administran toman una gran importancia ya que hoy en día las empresas deben de brindar una seguridad alta para no perder o ser vulnerada la seguridad de los datos a través de distintas conexiones que permiten descargar una gran cantidad de posibilidades de riesgos informáticos con la aparición de nuevas aplicaciones que permiten que los usuarios activen o generen información de datos que pueden activar amenazas a los sistemas computarizados que se encuentran en una red.

Palabras clave: Conectividad, Redes, Comunicaciones, Seguridad en Redes, VPN

Abstract:

When implementing a network for a company, it is very likely that on the way you will encounter several obstacles, either in the configuration or in the hardware in question, which hence the importance of generating prevention with the fundamental processes for the realization of good practices in terms of taking models of prolonging security methods in organizations by implementing different modes of global communication through the application of commands that will allow to have a totally secure and functional network. For this reason, the number one scenario chosen for this project.

The necessary modifications will be made to improve in all aspects the characteristics of the data network and the communications of the proposed scenario, since the network has presented several conflicts. *

The security of the devices that are managed take on great importance since today companies must provide high security so as not to lose or be compromised the security of the data through different connections that allow downloading a large number of possibilities of Computer risks with the appearance of new applications that allow users to activate or generate data information that can activate threats to computerized systems found on a network.
Keywords: Connectivity, Networks, Router, Network Security, VPN

4 INTRODUCCIÓN

Trabajando en el desarrollo de nuevos equipos y sistemas, la tecnología permite optimizar y mejorar la administración, la comunicación y los servicios de las redes de datos, facilitando a los usuarios el manejo y procesamiento de información. Con la descripción general del artículo se desea influir en la importancia que cada estudiante debe de poner en práctica y conocimiento métodos básicos de

buenas prácticas del tema de seguridad informática para las redes de comunicación y conectividad dentro de empresas lo que establece es una serie de documentos especiales que certifican que el conocimiento de las comunicaciones en redes permite establecer una administración desde las centrales en las que lo esencial es poder sobre guardar la protección de posibles ataques e impedimento de las comunicaciones que hay entre lo emisores y los receptores de información digital que se vive hoy en el mundo.

A nivel internacional, la ciberdefensa y la ciberseguridad están declaradas como unas de las mayores prioridades en términos de seguridad, ya que uno de los retos a nivel global en la actualidad es la necesidad de poder tratar adecuadamente la información.

Con la topología escogida la cual incentiva el conocer los elementos especiales en el trabajo, también se pretende introducir al lector o pioneros estudiantes de la carrera profesional de Ingeniería de Sistema lo importante de realizar las practicas, cursos en los cuales pueden entender e implementar los conocimientos en un mundo real que constantemente está realizando grandes cambios de ciberseguridad en las empresas y lo realizan con normas básicas que se tenían desde tiempo atrás en el que la comunicación era elitista y hoy es elemento de la comunidad.

5 ANALISIS DE LA RED

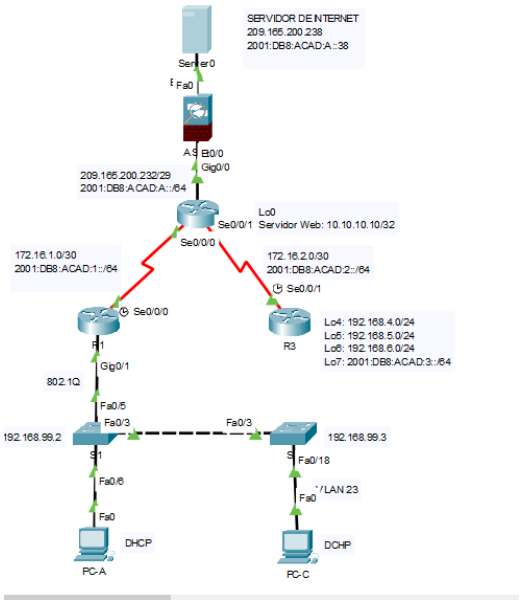
Se realizó un estudio de la estructura de la red del escenario escogido, para determinar cómo es el funcionamiento de la red y establecer los conflictos y las necesidades que tiene la misma. Básicamente la estructura de la red de datos, consta de un Router 4331 proporcionado por Packet Tracer para facilitar el acceso a internet a todas las computadoras del diseño de red, se identifica que no se cuenta con ningún firewall por lo cual es aquí donde se sugiere un firewall CISCO ASA 5505 que controla el acceso a los servicios y protege la red de datos, dos router más para el servidor web y otro para las sedes. el mismo está conectado a un switch cisco 3560 capa dos no configurable de 24 puertos, el cual tiene una conexión en cascada con otro switch de las mismas características los cuales vinculan a todas las computadoras y servidores. Para tener un panorama claro de los problemas que puede tener la red de datos se establecen posibles puntos de falla .

6 PARTE TÉCNICA DEL ARTÍCULO

El objetivo de utilizar un Firewall es tener una herramienta de software o hardware que tiene como propósito filtrar las conexiones que ingresan a la red interna de la organización o empresa, así como también las conexiones de red que se dirigen hacia el exterior de la misma. Se implementa como un **mecanismo de control** de acceso lógico.

Los ciscos ASA pueden funcionar en 2 modos: enrutado y transparente. En modo enrutado el equipo actúa como equipo de capa tres y envía los paquetes basándose en la dirección IP del destinatario, en cambio en modo transparente el equipo actúa como equipo de capa 2, parecido a un bridge o switch y las tramas que se envían están basadas en la dirección MAC (Media Access Control) del destino.

Para nuestra actividad inicial se utiliza en modo trunk o enrutado ya que el modo transparente solo se encuentra en el dispositivo físicamente. se va a realizar un desarrollo de un paso a paso de un ejercicio de conexión de red en donde se aplicara una serie de comandos de acceso para realizar una buena conexión que va con parámetros iniciales básicos que generan un inicio, una buena práctica para la realización de conexiones de red en un ambiente simulado el cual nos puede llegar a generar un gran conocimiento al realizar prácticas en una pequeña o mediana empresa la cual necesitan que los estudiantes tengan un nivel de conocimiento para brindar seguridad y conexión a los datos que se requieren por ello en este se presentaran un escenario con una topología la cual vamos a integrar y diseñar con una programación inicial desde cero para culminar a una conexión eficiente y completa.



Figuras 42. Topología con Firewall ASA

Lo inicial es darle las conexiones necesarias para que se genere la conexión entre sí de los dispositivos por ello el programa nos brinda los enlaces necesarios como lo es el cable de cobre directo el cual me permitirá generar las conexiones entre los dispositivos, al unir cada dispositivo se genera las siguientes opciones que se nombraran a continuación al unir el Router que brinde una capacidad para transportar datos se utiliza en Gigabit/Ethernet lo cual proporciona una mayor estabilidad para esta red, al realizar la unión con el Swith este permitirá una conexión por medio de FastEthernet la entrada inicial que se va brindando.

El Cisco ASA 5505 ofrece las siguientes ventajas:
• Un Diseño modular que ofrece: IPS, antivirus, antispam, anti phishing y filtrado de URLs.
• Más escalabilidad y funcionalidades.
• Soporta Secure Sockets Layer (SSL) VPN.
• Seguridad en las comunicaciones unificadas avanzadas (video/
audio).

En el firewall Asa cisco 5500 configuramos las Vlan 1 como entrada (inside) y la vlan 2 como salida (outside) y en las interfaces Ethernet 0/0 y la 0/1 como lo indica la Figura 2.

```
Port          Link   VLAN   IP Address         IPv6 Address
Ethernet0/0   Up     2      --                 <not set>
Ethernet0/1   Up     1      --                 <not set>
Ethernet0/2   Down   1      --                 <not set>
Ethernet0/3   Down   1      --                 <not set>
Ethernet0/4   Down   1      --                 <not set>
Ethernet0/5   Down   1      --                 <not set>
Ethernet0/6   Down   1      --                 <not set>
Ethernet0/7   Down   1      --                 <not set>
Vlan1         Up     1      192.168.1.1/24     <not set>
Vlan2         Up     2      209.165.200.237/29 <not set>
Hostname: ciscoasa

Physical Location: Intercity, Home City, Corporate Office, Main Wiring Closet
```

Figuras 43. Configuración Firewall Asa 5500

Hay que tener en cuenta que para la que funcione las configuraciones de las ip en las vlan en el servidor Asa no dejara pasar los paquetes por seguridad es por eso que toca crear las ACL o listas de acceso de los paquetes que vamos a permitir. Para realizamos la configuración con los siguientes comandos:

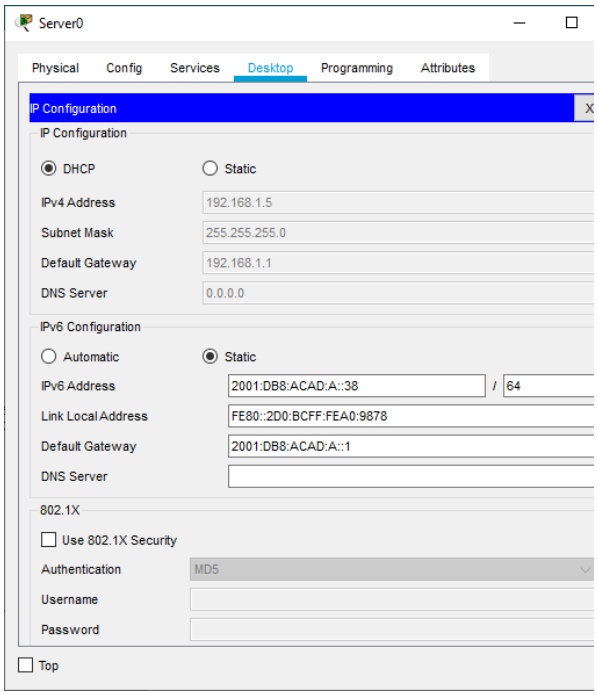
- Class-map inspection_defaul
- Macht default-inspection-traffic
- Policy-map global_policy
- Class inspection_defaul
- Inspect icmp
- Service-policy global_policy global

Cada router permita manejar una comunicación, conexión de todos los dispositivos entre si permitiendo generar un soporte entre la red interna que se está creando de acuerdo a la topología dada, se visualiza un red pequeña en donde se generar conexión a dos equipos con un excelente soporte pero esta debe de brindar facilidad de acceso entre ellas por eso es importante generar una buena administración para eso le damos nombres específicos a cada VLAN en los dos Switch que tenemos para conectar las PC o terminales la sintaxis que a continuación vamos a desarrollar permite visualizar una series de comandos que permite generar cambios para un mayor control en el tráfico de datos que se sugiere para la red.

Un Switch debería tener conexiones Gigabit Ethernet para garantizarnos así la máxima velocidad de la red local libre de cuellos de botella. Si, por ejemplo, nuestra red es Gigabit Ethernet y conectamos un router Fast Etherner 10/100, todas las conexiones que pasen a través de él quedarán limitadas a dicha velocidad máxima,

algo que no podemos permitir si, por ejemplo, tenemos una conexión de 120 megas, 200 megas o 300 megas de fibra óptica.

El Firewall Asa 5500 también tiene habilitado DHCP por defecto es por eso que le asigno una ip al servidor de internet de forma dinámica.

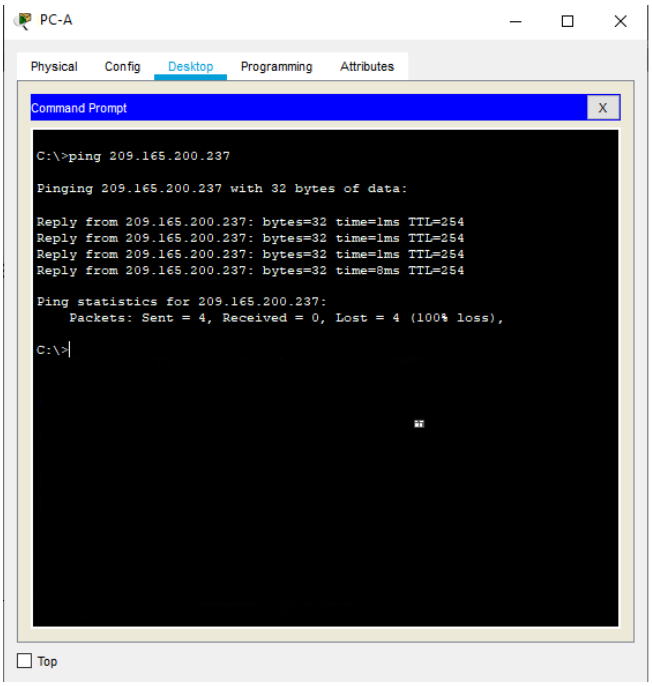


Figuras 44. Asignacion DHCP.

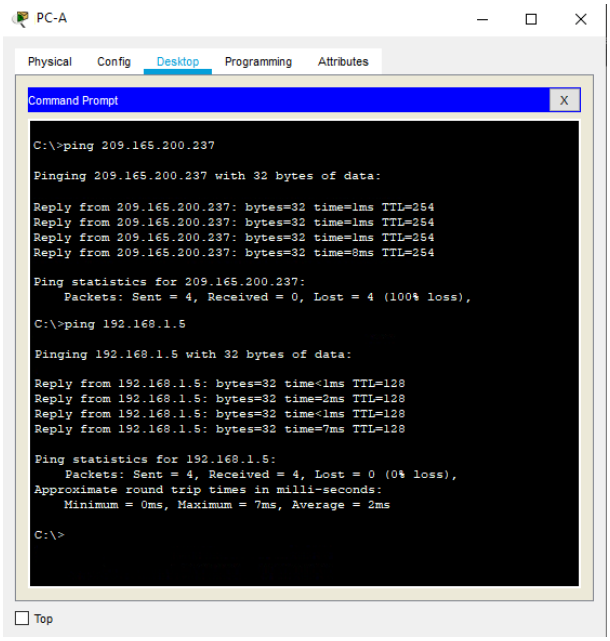
AL realizar las modificaciones dentro de nuestro programa de ejemplo podemos visualizar que al realizar las respectivas consultas en cada terminal o equipo de usuario me permitirá la administración de cada uno en el cual podríamos administrar primero que todo que tenga siempre una IP fija lo que permitirá su conexión sin repeticiones o falla de conectividad La asignación de direcciones con DHCP se basa en un modelo cliente-servidor: el terminal que quiere conectarse solicita la configuración IP a un servidor DHCP que, por su parte, recurre a una base de datos que contiene los parámetros de red asignables. Este servidor, componente de cualquier router ADSL moderno, puede asignar los siguientes parámetros al cliente con ayuda de la información de su base de datos:

7 RESULTADOS

Por último, realizamos la prueba de conectividad de la PC-A hasta el Firewall asa y de igual forma hasta el servidor de internet.

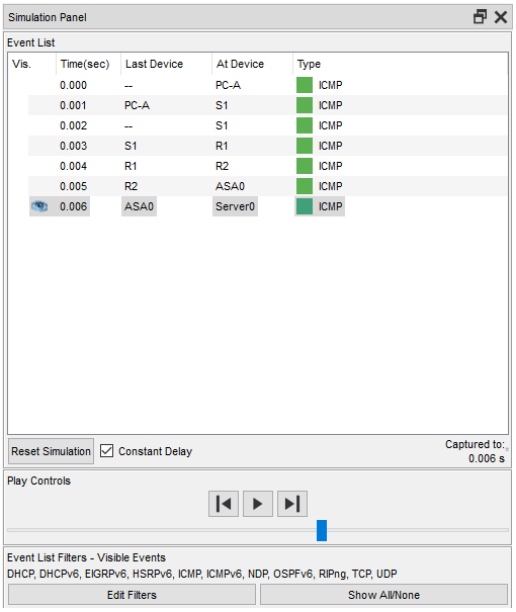


Figuras 45. Ping PC-A a Servidor Firewall Asa



Figuras 46. Ping PC-A a Servidor de Internet

Verificamos con el simulador que los paquetes ICMP llegan del la PCA al Servidor de internet pasando por el Firewall ASA.



Con la implementación del firewall en este escenario se logra que todo el tráfico que proviene o va hacia Internet pasa a través de él. De esta forma el firewall tiene la capacidad de cerciorarse que este tráfico es conforme a las políticas de seguridad del sistema. Estas políticas definen la accesibilidad y los niveles de restricción tanto de los servicios disponibles en Internet como los que se ofrecen en la red interna. Estas políticas son controladas a través de un solo punto central: el punto de conexión de la red con Internet.

8 REFERENCIAS

I. 1884), S. C. (2000). *Cisco Systems*. Obtenido de https://www.cisco.com/c/dam/global/es_es/assets/docs/safe_wp1.pdf

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

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

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

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

II. Libre, U. (2016). *Programa Ingeniería de Sistemas y Telemática*. Obtenido de https://repository.unilibre.edu.co/bitstream/handle/10901/10815/Tesis-Final.pdf?sequence=1&isAllowed=y

BIOGRAFÍA

Darwin Dorado nació en Pasto, Nariño Colombia el, 13 de enero de 1983. Estudiante de la Universidad Nacional Abierta y a Distancia UNAD, y estudio ingeniería de sistemas.

realizó sus estudios primarios en Escual San Vicente, continuo sus estudios secundarios en el Colegio San Felipe Neri, donde obtiene el título de Bachiller Académico. Completo sus estudios en el SENA con un Certificado en Mantenimiento de equipos de cómputo y trabaja en una microfinanciera llamada Contactar como profesional de Tics.