

DIPLOMADO DE PROFUNDIZACION CISCO PRUEBA DE HABILIDADES
PRÁCTICAS CCNA

DIEGO FERNANDO ALDANA RIAÑO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD ESCUELA DE
CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI

INGENIERÍA TELECOMUNICACIONES

PACHO CUNDINAMARCA

2020

DIPLOMADO DE PROFUNDIZACION CISCO PRUEBA DE HABILIDADES
PRÁCTICAS CCNA

DIEGO FERNANDO ALDANA RIAÑO

Diplomado de opción de grado presentado para optar el título de INGENIERO
TELECOMUNICACIONES

DIRECTOR:

ING. JOSE EGNACIO CARDONA

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

INGENIERÍA TELECOMUNICACIONES

PACHO CUNDINAMARCA

2020

NOTA DE ACEPTACIÓN

____ Firma del Presidente del Jurado

____ Firma del Jurado

____ Firma del Jurado

PACHO CUNDINAMARCA, 5 de diciembre de 2020

CONTENIDO

CONTENIDO.....	4
LISTA DE TABLAS	5
LISTA DE FIGURAS	6
GLOSARIO	7
RESUMEN.....	9
INTRODUCCION	10
DESARROLLO.....	11
ESCENARIO 1	11
GRAFICAS ESCENARIO 1	28
ESCENARIO 2	41
GRAFICAS ESCENARIO 2	59
CONCLUSIONES	63
BIBLIOGRAFIA.....	64
ANEXO	65

LISTA DE TABLAS

Table 1.tabla de vlans	11
Table 2.tabla de direcciones	12
Table 3.configuracion router 1	14
Table 4.configuracion s1	16
Table 5.configuracion s2	17
Table 6.estructura s1	19
Table 7.estructura s2	22
Table 8.soporte r1.....	24
Table 9.servidor PC A	25
Table 10.servidor pc B.....	25
Table 11.verificacion conectividad.....	26
Table 12 inicializacion dispositivos escenario 2	42
Table 13 configuracion del servidor de internet escenario 2	43
Table 14 configuracion R1 escenario 2	43
Table 15 configuracion R2 escenario 2	44
Table 16 configuracion R3escenario 2	45
Table 17 resultados de pruebas ping escenario 2	47
Table 18 configuracion S1 puertos troncales y accesos escenario 2	47
Table 19 configuracion s3 puertos troncales y accesos escenario 2	48
Table 20 configuracion R1 subinterface lan.....	49
Table 21resultados ping entre dispositivos escenario 2	50
Table 22 configuracion R1 OSPF	50
Table 23configuracion R2 OSPF	51
Table 24configuracion R2 OSPF v3.....	52
Table 25comandos CLI informacion OSPF.....	53
Table 26configuracion R1 DHCP escenario 2	53
Table 27configuracion Nat web	54
Table 28verificar dhcp y nat.....	55
Table 29configuracion NTP	56
Table 30 configuracion acceso ACL escenario	57
Table 31comanco CLI	57

LISTA DE FIGURAS

Figure 1.topologia	11
Figure 2	11
Figure 3.ping 10.19.8.1	28
Figure 4.ping 2001:db8:acad:a: :1	28
Figure 5.ping 10.19.8.65	29
Figure 6.ping 2001:db8:acad:b: :1	29
Figure 7.ping 10.19.8.97	30
Figure 8.ping 2001:db8:acad:c: :1.....	30
Figure 9.ping 10.19.8.98	31
Figure 10.ping 2001:db8:acad:c: :98.....	31
Figure 11.ping 10.19.8.99	32
Figure 12.ping 10.19.8.99	32
Figure 13.ping 10.19.8.85	33
Figure 14.ping 2001:db8:acad:b: :50	33
Figure 15.ping 209.165.201.1	34
Figure 16.ping 2001:db8:acad:209: :1	34
Figure 17.ping 209.165.201.1	35
Figure 18.ping 2001:db8:acad:209: :1	35
Figure 19.ping 10.19.8.1	36
Figure 20.ping 2001:db8:acad:a: :1	36
Figure 21.ping 10.19.8.65	37
Figure 22.ping 2001:db8:acad:b: :1	37
Figure 23.ping 10.19.8.97	38
Figure 24.ping 2001:db8:acad:c: :1.....	38
Figure 25.ping 10.19.8.98	39
Figure 26.ipconfig /all pc b.....	39
Figure 27.ipconfig /all pcA	40
Figure 28 Escenario 2	41
Figure 29ping de s1 a r1 vlan99	59
Figure 30ping de s3 a r1 vlan 99	59
Figure 31ping s1 a r1 vlan 21	60
Figure 32ping de s3 a r1 vlan 23	60
Figure 33 DHCP PC-A.....	61
Figure 34DHCP PC-C.....	61
Figure 35ping PC-A A PC-C	62
Figure 36NAVEGADOR WEB.....	62

GLOSARIO

Ipv6

El IPv6 es una actualización al protocolo IPv4, diseñado para resolver el problema de agotamiento de direcciones. Su desarrollo comenzó en diciembre de 1998 cuando Steve Deering y Robert Hinden, empleados de Cisco y Nokia publicaron una especificación formal del protocolo a través de un RFC12 y aún continúa su implementación.

Ipv4

El Protocolo de Internet versión 4 (en inglés, Internet Protocol version 4, IPv4), es la cuarta versión del Internet Protocol (IP), un protocolo de interconexión de redes basados en Internet

Vlans

Una VLAN, acrónimo de virtual LAN (red de área local virtual), es un método para crear redes lógicas independientes dentro de una misma red física

Routing

es la función de buscar un camino entre todos los posibles en una red de paquetes cuyas topologías poseen una gran conectividad. Dado que se trata de encontrar la mejor ruta posible, lo primero será definir qué se entiende por "mejor ruta" y en consecuencia cuál es la "métrica" que se debe utilizar para medirla.

Interface

se utiliza en informática para nombrar a la conexión funcional entre dos sistemas, programas, dispositivos o componentes de cualquier tipo, que proporciona una comunicación de distintos niveles, permitiendo el intercambio de información. Esto es un ejemplo de la realidad virtual. 1

OSPF

protocolo Primero la ruta más corta (OSPF = Open Shortest Path First – Protocolo abierto de los enlaces) es uno de los protocolos del estado-enlace más importantes. Es un protocolo estándar descrito en el RFC 2328 y la versión para IPv6 se publicó en el RFC 2740. Usa el algoritmo SPF para calcular el costo más

Bajo hasta un destino. Las actualizaciones de enrutamiento producen tráfico cuando ocurren cambios en la topología de la red.

NAT

La traducción de direcciones de red, también llamado enmascaramiento de IP o NAT (del inglés 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 (NTP) es un protocolo de Internet para sincronizar los relojes de los sistemas informáticos a través del enrutamiento de paquetes en redes con latencia variable. NTP utiliza UDP como su capa de transporte, usando el puerto 123. Está diseñado para resistir los efectos de la latencia variable.

RESUMEN

El diplomado de cisco nos muestra un primer escenario donde yo tengo como objetivo tener la capacidad de configurar una red pequeña donde muestre diversas configuraciones y protocolos de la marca cisco y manejar su herramienta packet tracer que es la que nos ayuda en la investigación y desarrollo de este sin necesidad de tener una maquina u equipo físico para aprender cisco y seguir un plan de investigación en las diversos foros y bibliografías de la marca cisco donde podemos lograr y configurar dicha estructura o red que nos propongamos y bien que solicite el escenario 1 donde este nos pide configurar ipv6 ipv4 dhcp link aggregation dhcp y rutas estáticas vlans nombres seguridad descripciones enrutamientos .

Realizando estos 2 escenarios he aprendido no solo a usar dispositivos cisco también me despejos muchas dudas y comprender los diferentes usos y problemáticas encontrados en las redes como routing y switching dar soluciones a problemáticas presentadas en empresas en solución de comunicaciones, resolver estos 2 ejercicios nos da a conocer diferentes soluciones que no tenia conocimiento y ahora me abre muchas posibilidades de seguir capacitando en la certificación en todos los niveles de este.

Palabras claves: ipv6, vlans, enrutamientos, dhcp, link aggregation

ABSTRACT

The Cisco Diploma shows us a first scenario where I have the objective of having the ability to configure a small network where it shows various configurations and protocols of the Cisco brand and manage its tool packet tracer, which is what helps us in the research and development of This without the need to have a machine or physical equipment to learn Cisco and follow a research plan in the various forums and bibliographies of the Cisco brand where we can achieve and configure said structure or network that we propose and if you request scenario 1 where it is It asks us to configure ipv6 ipv4 dhcp link aggregation dhcp and static routes vlans names security descriptions routes.

Carrying out these 2 scenarios, I have learned not only to use Cisco devices, but I also cleared many doubts and understand the different uses and problems found in networks such as routing and switching, giving solutions to problems presented in companies in communication solutions, solving these 2 exercises gives us to know different solutions that I was not aware of and now it opens up many possibilities for me to continue training in certification at all levels of this.

Keywords: ipv6, vlans, enrutamientos, dhcp, link aggregation

INTRODUCCION

El escenario 1 aprendemos a configurar una red pequeña que consta de un router con loopback 2 switch 2 pc o servidores donde configuramos 6 subinterface vlan 2 servidores dhcp versión4 y 4 subinterface ipv6, los servidores tienen que recibir ips automáticas del servidor dhcp y recibir ipv6 estos servidores tiene que tener respuesta a ping y gestión de todos los dispositivos que constan la red y direccionar su trafico al loopback la comunicación entre los 2 switch se realiza mediante un grupo de interface etherchannel, teniendo en cuenta todos esto se realiza configuraciones de vlans nativas en acceso y troncales para lograr etiquetar la red y darle seguridad de ruteo y seguridad encryptada de la red.

El escenario 2 nos resuelve la capacidad de crear una configuración de red donde la comunicación se realice por la ruta más corta y así tener una mejor respuesta de los dispositivos o salida hacia internet también nos resuelve la capacidad de tener un servidor ntp para tener horario y sincronizar relojes de nuestros dispositivos ya si tener una respuesta y horario exacto de los sucesos que se puedan presentar en nuestros dispositivos de red

DESARROLLO

ESCENARIO 1

Figure 1.topologia

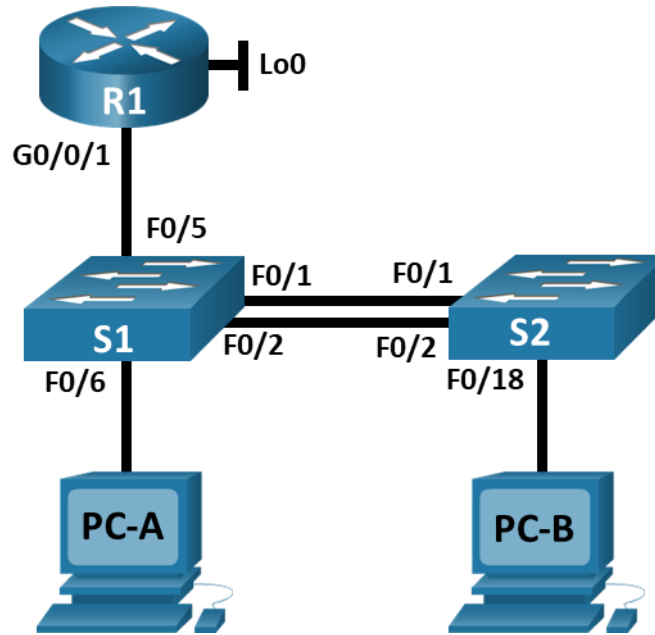


Figure 2

Tabla de VLAN

Table 1.tabla de vlans

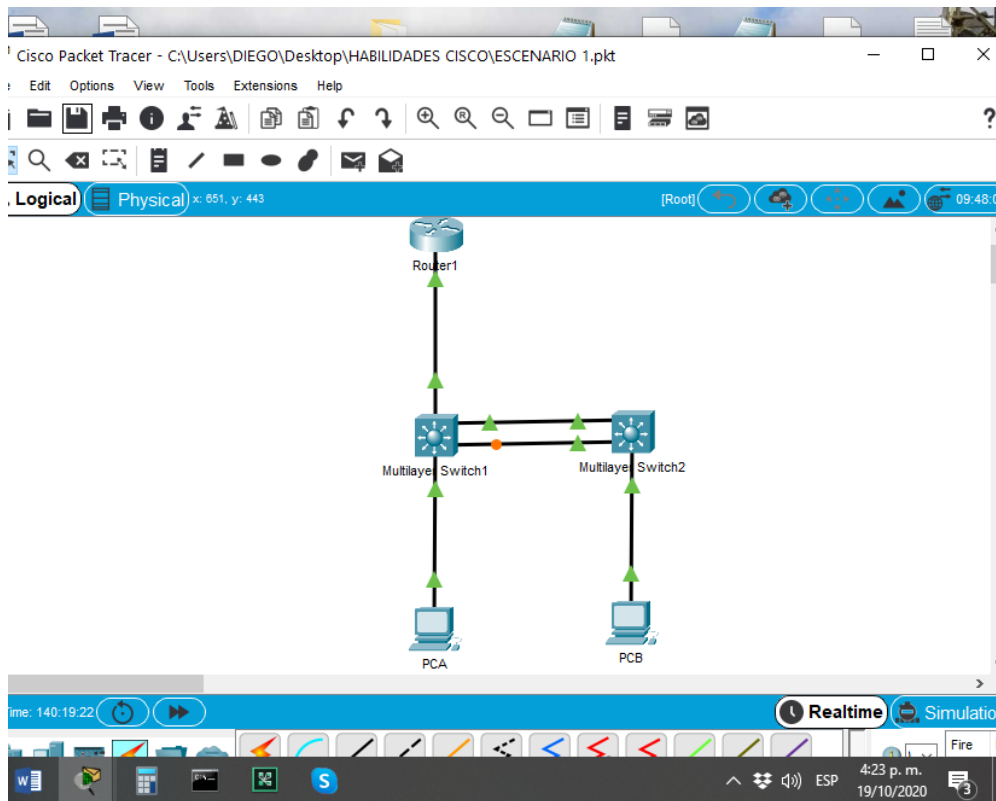
VLAN	Nombre de la VLAN
2	Bikes
3	Trikes
4	Management
5	Parking
6	Native

Tabla de asignación de direcciones

Table 2.tabla de direcciones

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

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



Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Se inició router y entrando a la consola desactivando la busca DNS como configuración inicial para luego volverlo activar y configurando el nombre de dominio. se realizó las configuraciones iniciales como nombre del dispositivo host o router R1 se configuro contraseña de consola y EXEC privilegiado para el acceso a la terminal de configuración se creó un nombre de usuario y contraseña para la base de datos local realizado esto se configuro las líneas vty 0 15 y mínima longitud de contraseñas para su seguridad solo se aceptó acceso remoto SSH y encriptación de cifrado RSA para generar claves secretas. Se configuro un mensaje de inicialización del router o banner,

Configuración loopback 0 ips versión6 y versión4 subinterface vlan y dhcp y link local

Table 3.configuracion router 1

Tarea	Especificación
Desactivar la búsqueda DNS	Router>enable Router#conf Router(config)#no ip domain-lookup
Nombre del router	Router#config Router(config)#hostname R1
Nombre de dominio	R1(config)#ip domain-lookup R1(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	R1(config)#line console 0 R1(config-line)#password ciscoenpass R1(config-line)#login
Contraseña de acceso a la consola	R1> enable R1 (config)# enable password ciscoconpass
Establecer la longitud mínima para las contraseñas	R1(config)#security password min-length 10 R1(config)#enable password 1234567890
Crear un usuario administrativo en la base de datos local	R1(config)#username admin password admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	R1(config)#line vty 0 15 R1(config-line)#login local
Configurar VTY solo aceptando SSH	R1(config-line)#transport input ssh
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Configure un MOTD Banner	R1(config)#banner motd "DIEGO ALDANA"
Habilitar el routing IPv6	R1(config)#ipv6 unicast-routing

Tarea	Especificación
Configurar interfaz G0/0/1 y subinterfaces	<pre> R1(config)#interface g0/0/1.2 R1(config-subif)#encapsulation dot1q 2 R1(config-subif)#ip address 10.19.8.1 255.255.255.192 R1(config-subif)#ipv6 address 2001:db8:acad:a::1/64 R1(config)#interface g0/0/1.3 R1(config-subif)#encapsulation dot1q 3 R1(config-subif)#ip address 10.19.8.65 255.255.255.224 R1(config-subif)#ipv6 address 2001:db8:acad:b: :1 /64 R1(config)#interface g0/0/1.4 R1(config-subif)#encapsulation dot1q 4 R1(config-subif)#ip address 10.19.8.97 255.255.255.248 R1(config-subif)#ipv6 address 2001:db8:acad:c: :1 /64 </pre>
Configure el Loopback0 interface	<pre> Establezca la descripción R1(config)#interface loopback0 R1(config-if)#ip address 209.165.201.1 255.255.255.224 R1(config)#interface loopback0 R1(config-if)#ipv6 address fe80::1 link- local </pre>
Generar una clave de cifrado RSA	<pre> R1(config)#crypto key generate rsa general-keys modulus 1024 </pre>

Configure S1 y S2.

Se realizaron las configuraciones iniciales como datos de administración y gestión nombre de host ip de gestión y Gateway predeterminando la seguridad de consola 0 la de EXE privilegiado y vty e incrypar y cifrarlas se le dio un banner o mensaje de inicio de sesión donde el mensaje fue mi nombre en mayúscula DIEGO ALDANA esta configuración se realizo en el s1 y s2 donde cada uno de estos equipos tenía su ipv4 y ipv6 diferente en cada dispositivo

Table 4.configuracion s1

Tarea	Especificación
Desactivar la búsqueda DNS.	swicht>enable swicht#conf swicht(config)#no ip domain-lookup
Nombre del switch	swicht#config swicht(config)#hostname S1
Nombre de dominio	S1(config)#ip domain-lookup S1(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	S1(config)#line console 0 S1(config-line)#password ciscoenpass S1(config-line)#login
Contraseña de acceso a la consola	S1> enable S1 (config)# enable password ciscoconpass
Crear un usuario administrativo en la base de datos local	S1(config)#username admin password admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	S1(config)#line vty 0 15 S1(config-line)#login local
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S1(config-line)#transport input ssh

Tarea	Especificación
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption
Configurar un MOTD Banner	S1(config)#banner motd "DIEGO ALDANA"
Generar una clave de cifrado RSA	S1(config)#crypto key generate rsa general-keys modulus 1024
Configurar la interfaz de administración (SVI)	S1(config)#interface vlan4 S1(config)#ip address 10.19.8.98 255.255.255.248 S1(config)#ip default-gateway 10.19.8.97 S1(config)#no shut S1(config)#interface vlan4 S1(config-if)#ipv6 address 2001:db8:acad:c::98/64 S1(config-if)#ipv6 address fe80::98 link-local S1(config-if)#exit
Configuración del gateway predeterminado	S1(config)#ip default-gateway 10.19.8.97

Configure S2.

Las tareas de configuración incluyen lo siguiente:

Table 5.configuracion s2

Tarea	Especificación
Desactivar la búsqueda DNS.	swicht>enable swicht#conf swicht(config)#no ip domain-lookup
Nombre del switch	swicht#config swicht(config)#hostname S2
Nombre de dominio	S1(config)#ip domain-lookup S1(config)#ip domain-name ccna-lab.com

Tarea	Especificación
Contraseña cifrada para el modo EXEC privilegiado	S1(config)#line console 0 S1(config-line)#password ciscoenpass S1(config-line)#login
Contraseña de acceso a la consola	S1> enable S1 (config)# enable password ciscoconpass
Crear un usuario administrativo en la base de datos local	S1(config)#username admin password admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	S2(config)#line vty 0 15 S2(config-line)#login local
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S2(config-line)#transport input ssh
Cifrar las contraseñas de texto no cifrado	S2(config)#service password-encryption
Configurar un MOTD Banner	S2(config)#banner motd "DIEGO ALDANA"
Generar una clave de cifrado RSA	S2(config)#crypto key generate rsa general-keys modulus 1024
Configurar la interfaz de administración (SVI)	S2(config)#interface vlan4 S2(config)#ip address 10.19.8.99 255.255.255.248 S2(config)#ip default-gateway 10.19.8.97 S2(config)#no shut S2(config)#interface vlan4 S2(config-if)#ipv6 address 2001:db8:acad:c::99/64 S2(config-if)#ipv6 address fe80::99 link-local S2(config-if)#exit
Configuración del gateway predeterminado	S2(config)#ip default-gateway 10.19.8.97

Configuración de la infraestructura de red (VLAN, Trunking, EtherChannel)

SWITCH 1 Y SWITCH 2

Se realizó la configuración donde se crearon 5 vlan con su respectivo nombre cada vlan de estas tiene como función servir un servicio diferente sobre la red, se configuro la red nativa vlan6 troncal y grupo de ethernet con el puerto 1 y 2 para hacer un etherchannel sobre capa2, se configuro el puerto 6 del switch 1 como acceso para etiquetarla con la vlan 2 para pasar el dhcp y el puerto 18 del switch 2 en acceso para que el pc b logre obtener dhcp y comunicación con la ipv6 siguiiente a esto para darle mas seguridad en la cantidad de conecciones por puerto se configuro los puertos accesos que solo dejara pasar un máximo de 3 mac address y se apagaron las interfaces no usadas

Configurar S1

La configuración del S1 incluye las siguientes tareas:

Table 6.estructura s1

Tarea	Especificación
Crear VLAN	S1(config)#vlan 2 S1(config-vlan)#name bikes S1(config)#vlan 3 S1(config-vlan)#name trikes S1(config)#vlan 4 S1(config-vlan)#name management S1(config)#vlan 5 S1(config-vlan)#name parking S1(config)#vlan 6 S1(config-vlan)#name native

Tarea	Especificación
<p>Crear troncos 802.1Q que utilicen la VLAN 6 nativa</p>	<pre> S1(config)#interface f0/1 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport trunk native vlan 6 S1(config)#interface f0/2 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport trunk native vlan 6 S1(config)#interface f0/5 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport trunk native vlan 6 </pre>
<p>Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2</p>	<pre> S1(config)#interface range f0/1-2 S1(config-if-range)#channel-group 1 mode S1(config-if-range)#interface port- channel 1 S1(config-if-range)#switchport trunk encapsulation dot1q S1(config-if-range)#switchport mode trunk S1(config-if-range)#switchport trunk allowed vlan all S1(config-if-range)#channel- protocol lacp </pre>

Tarea	Especificación
Configurar el puerto de acceso de host para VLAN 2	<pre>S1(config)#interface f0/6 S1(config-if)#switchport access vlan 2 S1(config-if)#no shut</pre>
Configurar la seguridad del puerto en los puertos de acceso	<pre>S1(config)#interface f0/6 S1(config-if)#switchport mode access S1(config-if)#switchport port-security S1(config-if)#switchport port-security maximum 3</pre>
Proteja todas las interfaces no utilizadas	<pre>S1(config)#interface range fastEthernet 0/3-4 S1(config-if-range)#shutdown S1(config)#interface range fastEthernet 0/7-24 S1(config-if-range)#shutdown S1(config)#interface range G0/1-2 S1(config-if-range)#shutdown</pre>

Configure el S2.

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

Table 7.estructura s2

Tarea	Especificación
Crear VLAN	S2(config)#vlan 2 S2(config-vlan)#name bikes S2(config)#vlan 3 S2(config-vlan)#name trikes S2(config)#vlan 4 S2(config-vlan)#name management S2(config)#vlan 5 S2(config-vlan)#name parking S2(config)#vlan 6 S2(config-vlan)#name native
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	S2(config)#interface f0/1 S2(config-if)#switchport mode trunk S2(config-if)#switchport trunk encapsulation dot1q S2(config-if)#switchport trunk native vlan 6 S2(config)#interface f0/2 S2(config-if)#switchport mode trunk S2(config-if)#switchport trunk encapsulation dot1q S2(config-if)#switchport trunk native vlan 6

Tarea	Especificación
<p>Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2</p>	<pre>S2(config)#interface range f0/1-2 S2(config-if-range)#channel-group 1 mode S2(config-if-range)#interface port-channel 1 S2(config-if-range)#switchport trunk encapsulation dot1q S2(config-if-range)#switchport mode trunk S2(config-if-range)#switchport trunk allowed vlan all S2(config-if-range)#channel-protocol lacp</pre>
<p>Configurar el puerto de acceso del host para la VLAN 3</p>	<pre>S2(config)#interface f0/18 S2(config-if)#switchport access vlan 2 S2(config-if)#no shut</pre>
<p>Configure port-security en los access ports</p>	<pre>S2(config)#interface f0/18 S2(config-if)#switchport mode access S2(config-if)#switchport port-security S2(config-if)#switchport port-security maximum 3</pre>

Tarea	Especificación
Asegure todas las interfaces no utilizadas.	<pre>S2(config)#interface range F0/3-17 S2(config-if-range)#shutdown S2(config)#interface range F0/19-24 S2(config-if-range)#shutdown S2(config)#interface range G0/1-2 S2(config-if-range)#shutdown S2(config)#interface range G0/1-2 S2(config-if-range)#shutdown</pre>

Configurar soporte de host

La configuración del router se creó unas rutas estáticas para que los segmentos ipv4 y ipv6 de direccionadas a loopback0 se crearon 2 servidores dhcp con 2 diferentes vlans para que cada una de estas llegaran al pc a y b pasando por estas vlan 2 direccionamiento ipv6 y lograr llegar a estos 2 servidores

Configure R1

Las tareas de configuración para R1 incluyen las siguientes:

Table 8.soporte r1

Tarea	Especificación
Configure Default Routing	<pre>R1(config)#ip route 0.0.0.0 0.0.0.0 loopback0 R1(config)#ipv6 route ::/0 loopback0</pre>
Configurar IPv4 DHCP para VLAN 2	<pre>ip dhcp pool RED1 network 10.19.8.0 255.255.255.192 default-router 10.19.8.1 dns-server 8.8.8.8 domain-name ccna-b.net ip dhcp excluded-address 10.19.8.1 10.19.8.58</pre>

Tarea	Especificación
Configurar DHCP IPv4 para VLAN 3	ip dhcp pool RED2 network 10.19.8.64 255.255.255.224 default-router 10.19.8.65 dns-server 8.8.8.8 domain-name ccna-b.net ip dhcp excluded-address 10.19.8.65 10.19.8.84

Configurar los servidores

Resultados de las configuraciones obtenidas de los pc A y B

ipconfig /all.

Table 9.servidor PC A

PC-A Network Configuration	
Descripción	FastEthernet0 C
Dirección física	00D0.BA76.14B3
Dirección IP	10.19.8.59
Máscara de subred	255.255.255.192
Gateway predeterminado	10.19.8.1
Gateway predeterminado IPv6	FE80::1

Table 10.servidor pc B

red de PC-B	
Descripción	FastEthernet0
Dirección física	00D0.D30A.21D1
Dirección IP	10.19.8.85
Máscara de subred	255.255.255.224
Gateway predeterminado	10.19.8.65
Gateway predeterminado IPv6	FE80::1

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.

Table 11.verificacion conectividad

Desde	A	de Internet	Dirección IP	Resultados de ping	
PC-A	R1, G0/0/1.2	Dirección	10.19.8.1	<i>ok</i>	
		IPv6	2001:db8:acad:a: :1	<i>ok</i>	
	R1, G0/0/1.3	Dirección	10.19.8.65	<i>ok</i>	
		IPv6	2001:db8:acad:b: :1	<i>ok</i>	
	R1, G0/0/1.4	Dirección	10.19.8.97	<i>ok</i>	
		IPv6	2001:db8:acad:c: :1	<i>ok</i>	
	S1, VLAN 4	Dirección	10.19.8.98	<i>ok</i>	
		IPv6	2001:db8:acad:c: :98	<i>no</i>	
	S2, VLAN 4	Dirección	10.19.8.99.	<i>ok</i>	
		IPv6	2001:db8:acad:c: :99	<i>no</i>	
	PC-B	PC-B	Dirección	IP address will vary.	<i>ok</i>
			IPv6	2001:db8:acad:b: :50	<i>ok</i>
R1 Bucle 0		Dirección	209.165.201.1	<i>ok</i>	
		IPv6	2001:db8:acad:209: :1	<i>ok</i>	
PC-B	R1 Bucle 0	Dirección	209.165.201.1	<i>ok</i>	
		IPv6	2001:db8:acad:209: :1	<i>ok</i>	

Desde	A	de Internet	Dirección IP	Resultados de ping
	R1, G0/0/1.2	Dirección	10.19.8.1	<i>ok</i>
		IPv6	2001:db8:acad:a :1	<i>ok</i>
	R1, G0/0/1.3	Dirección	10.19.8.65	<i>ok</i>
		IPv6	2001:db8:acad:b: :1	<i>ok</i>
	R1, G0/0/1.4	Dirección	10.19.8.97	<i>ok</i>
		IPv6	2001:db8:acad:c: :1	<i>ok</i>
	S1, VLAN 4	Dirección	10.19.8.98	<i>ok</i>
		IPv6	2001:db8:acad:c: :98	<i>no</i>
S2, VLAN 4	Dirección	10.19.8.99.	<i>ok</i>	
	IPv6	2001:db8:acad:c: :99	<i>no</i>	

GRAFICAS ESCENARIO 1

Figure 3.ping 10.19.8.1

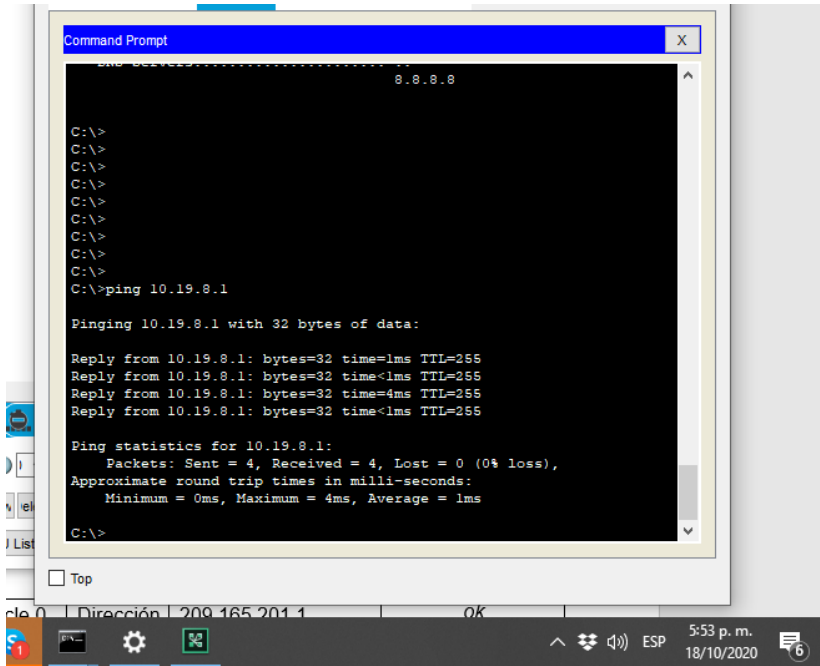


Figure 4.ping 2001:db8:acad:a::1

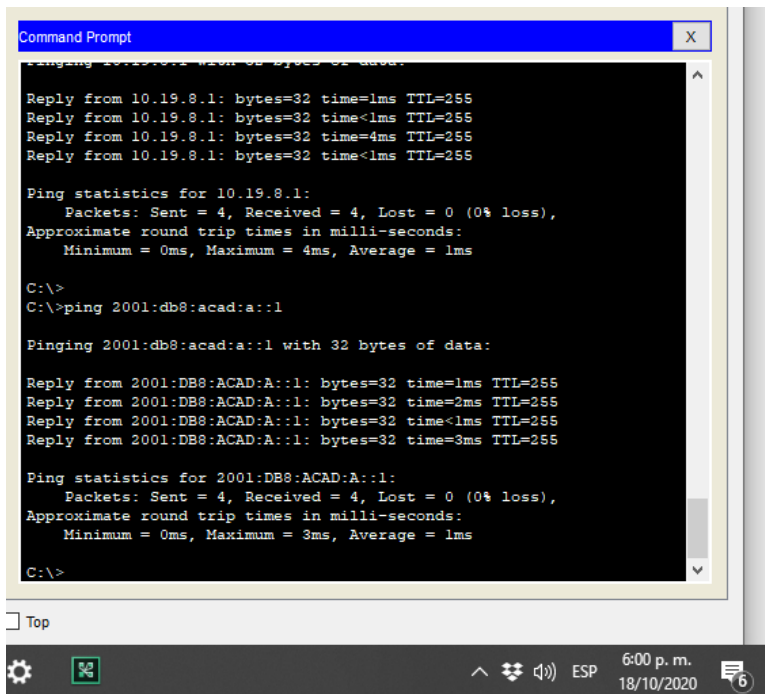


Figure 5.ping 10.19.8.65

```
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 3ms, Average = 1ms

ping 10.19.8.65

ping 10.19.8.65 with 32 bytes of data:

    from 10.19.8.65: bytes=32 time<1ms TTL=255
    from 10.19.8.65: bytes=32 time<1ms TTL=255
    from 10.19.8.65: bytes=32 time<1ms TTL=255
    from 10.19.8.65: bytes=32 time<1ms TTL=255

Ping statistics for 10.19.8.65:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Figure 6.ping 2001:db8:acad:b::1

```
Physical  Config  Desktop  Programming  Attributes

Command Prompt

Pinging 10.19.8.65 with 32 bytes of data:

Reply from 10.19.8.65: bytes=32 time<1ms TTL=255
Reply from 10.19.8.65: bytes=32 time<1ms TTL=255
Reply from 10.19.8.65: bytes=32 time<1ms TTL=255
Reply from 10.19.8.65: bytes=32 time<1ms TTL=255

Ping statistics for 10.19.8.65:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 2001:db8:acad:b::1

Pinging 2001:db8:acad:b::1 with 32 bytes of data:

Reply from 2001:DB8:ACAD:B::1: bytes=32 time=2ms TTL=255
Reply from 2001:DB8:ACAD:B::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:B::1: bytes=32 time=4ms TTL=255
Reply from 2001:DB8:ACAD:B::1: bytes=32 time=1ms TTL=255

Ping statistics for 2001:DB8:ACAD:B::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 4ms, Average = 1ms

C:\>
```

Figure 7.ping 10.19.8.97

```
Command Prompt
Pinging 2001:db8:acad:b::1 with 32 bytes of data:
Reply from 2001:DB8:ACAD:B::1: bytes=32 time=2ms TTL=255
Reply from 2001:DB8:ACAD:B::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:B::1: bytes=32 time=4ms TTL=255
Reply from 2001:DB8:ACAD:B::1: bytes=32 time=1ms TTL=255

Ping statistics for 2001:DB8:ACAD:B::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 4ms, Average = 1ms

C:\>PING 10.19.8.97

Pinging 10.19.8.97 with 32 bytes of data:

Reply from 10.19.8.97: bytes=32 time=1ms TTL=255
Reply from 10.19.8.97: bytes=32 time<1ms TTL=255
Reply from 10.19.8.97: bytes=32 time<1ms TTL=255
Reply from 10.19.8.97: bytes=32 time=1ms TTL=255

Ping statistics for 10.19.8.97:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

Figure 8.ping 2001:db8:acad:c::1

```
Command Prompt
Pinging 10.19.8.97 with 32 bytes of data:

Reply from 10.19.8.97: bytes=32 time=1ms TTL=255
Reply from 10.19.8.97: bytes=32 time<1ms TTL=255
Reply from 10.19.8.97: bytes=32 time<1ms TTL=255
Reply from 10.19.8.97: bytes=32 time=1ms TTL=255

Ping statistics for 10.19.8.97:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 2001:db8:acad:c::1

Pinging 2001:db8:acad:c::1 with 32 bytes of data:

Reply from 2001:DB8:ACAD:C::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:C::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:C::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:C::1: bytes=32 time<1ms TTL=255

Ping statistics for 2001:DB8:ACAD:C::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Figure 9. ping 10.19.8.98

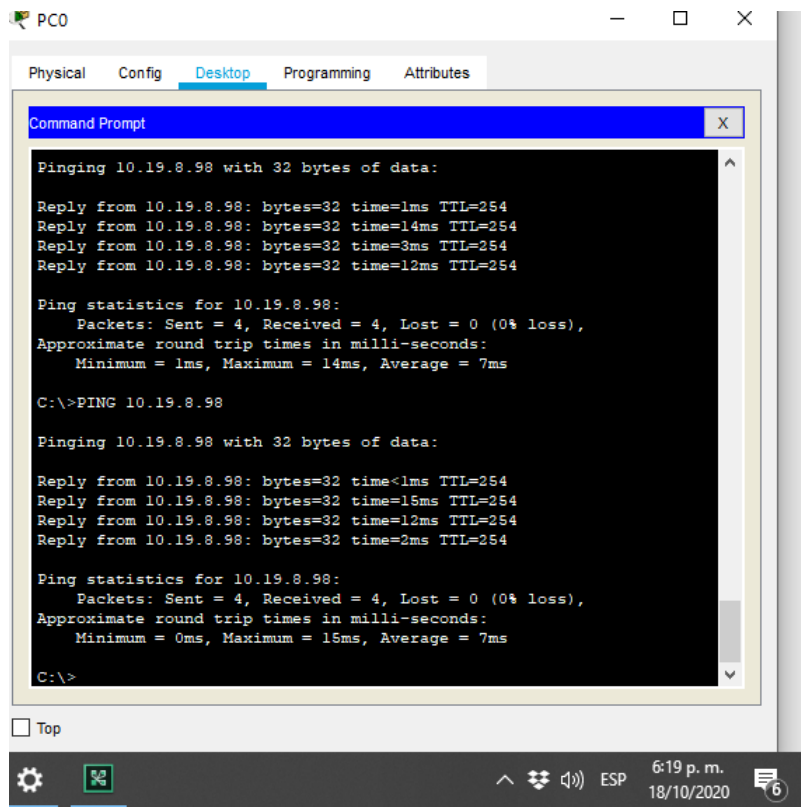


Figure 10. ping 2001:db8:acad:c::98

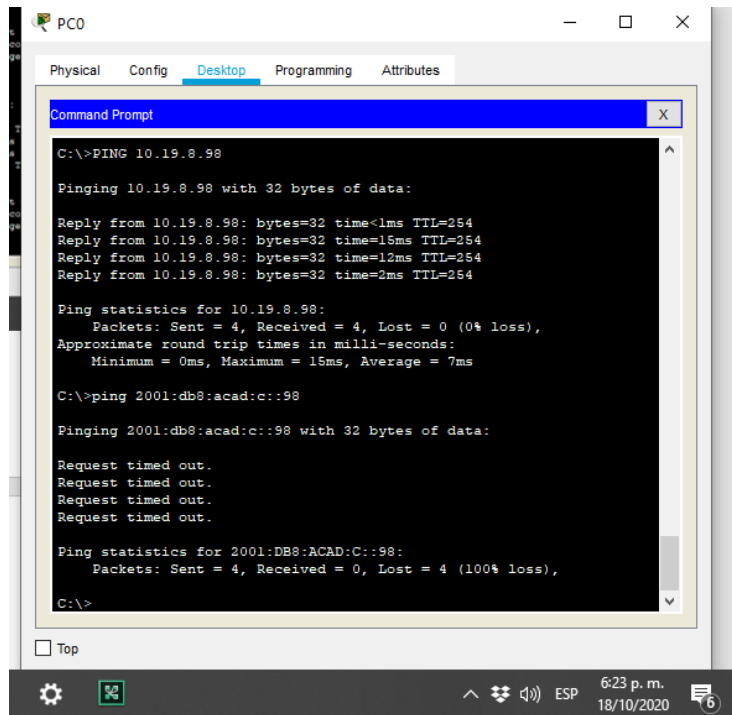
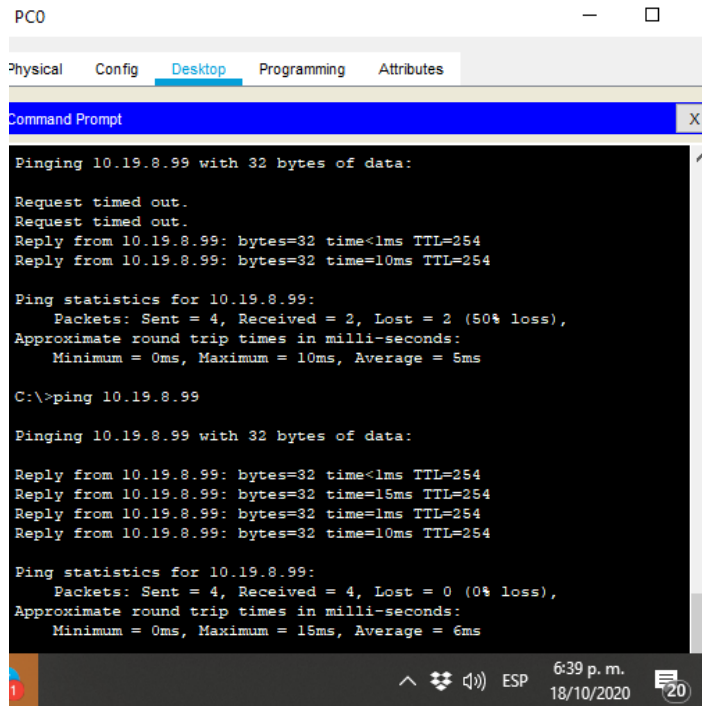


Figure 11.ping 10.19.8.99



```
PCO
Physical Config Desktop Programming Attributes
Command Prompt
Pinging 10.19.8.99 with 32 bytes of data:
Request timed out.
Request timed out.
Reply from 10.19.8.99: bytes=32 time<1ms TTL=254
Reply from 10.19.8.99: bytes=32 time=10ms TTL=254

Ping statistics for 10.19.8.99:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 5ms

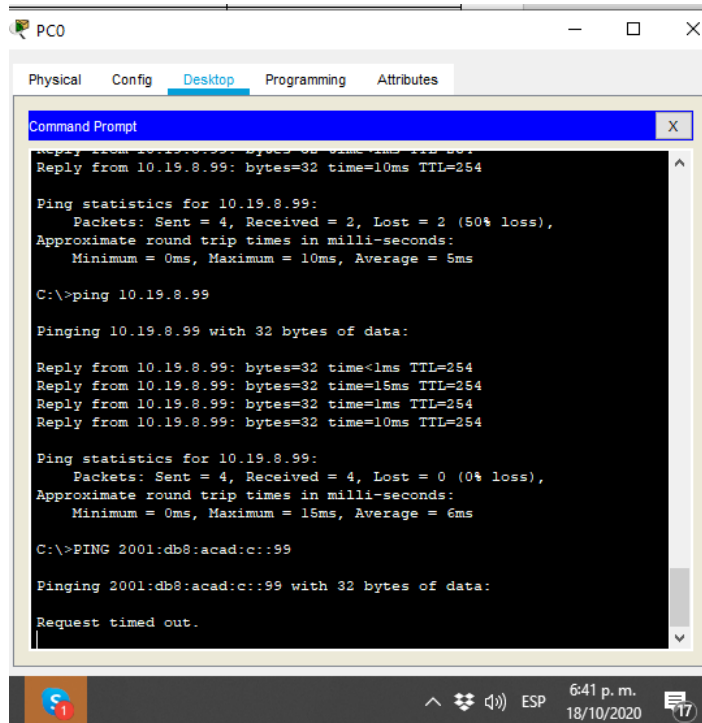
C:\>ping 10.19.8.99

Pinging 10.19.8.99 with 32 bytes of data:

Reply from 10.19.8.99: bytes=32 time<1ms TTL=254
Reply from 10.19.8.99: bytes=32 time=15ms TTL=254
Reply from 10.19.8.99: bytes=32 time=1ms TTL=254
Reply from 10.19.8.99: bytes=32 time=10ms TTL=254

Ping statistics for 10.19.8.99:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 15ms, Average = 6ms
```

Figure 12.ping 10.19.8.99



```
PCO
Physical Config Desktop Programming Attributes
Command Prompt
Reply from 10.19.8.99: bytes=32 time=10ms TTL=254
Reply from 10.19.8.99: bytes=32 time=10ms TTL=254

Ping statistics for 10.19.8.99:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 5ms

C:\>ping 10.19.8.99

Pinging 10.19.8.99 with 32 bytes of data:

Reply from 10.19.8.99: bytes=32 time<1ms TTL=254
Reply from 10.19.8.99: bytes=32 time=15ms TTL=254
Reply from 10.19.8.99: bytes=32 time=1ms TTL=254
Reply from 10.19.8.99: bytes=32 time=10ms TTL=254

Ping statistics for 10.19.8.99:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 15ms, Average = 6ms

C:\>PING 2001:db8:acad:c::99

Pinging 2001:db8:acad:c::99 with 32 bytes of data:

Request timed out.
```


Figure 13.ping 10.19.8.85

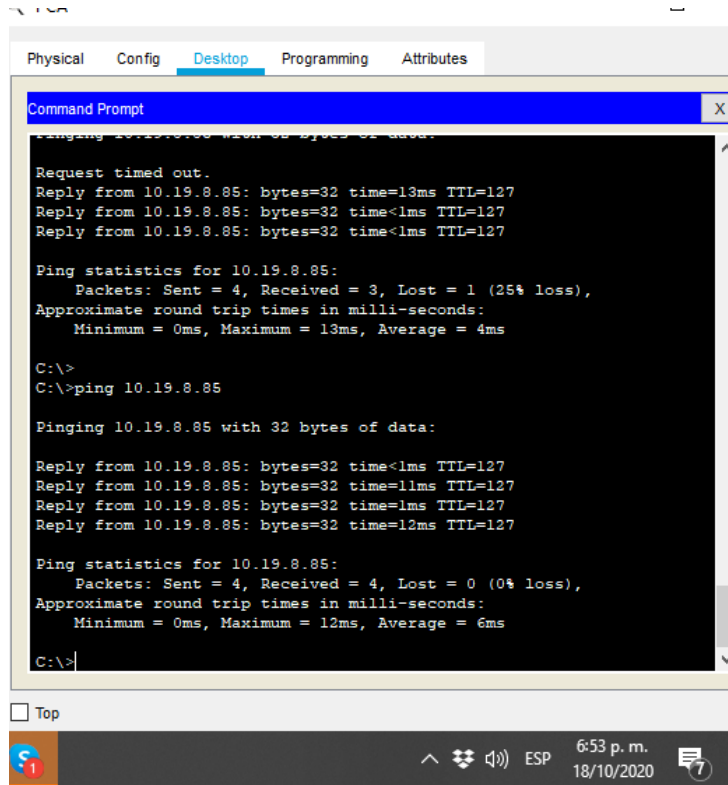


Figure 14.ping 2001:db8:acad:b::50

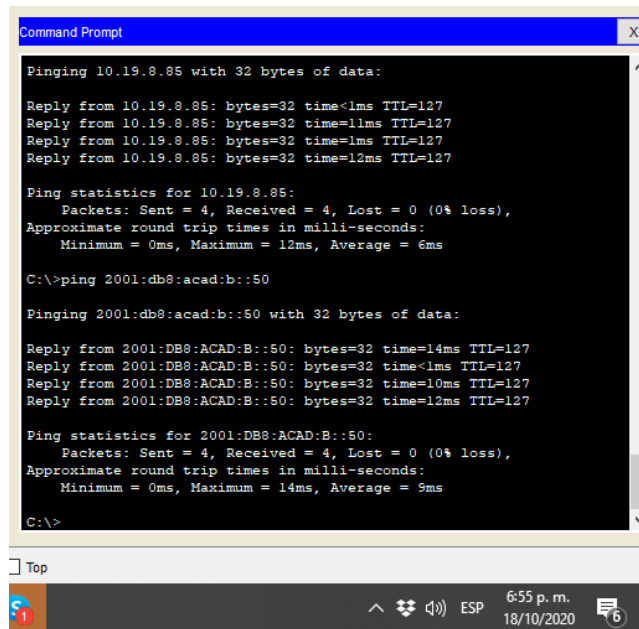


Figure 15. ping 209.165.201.1

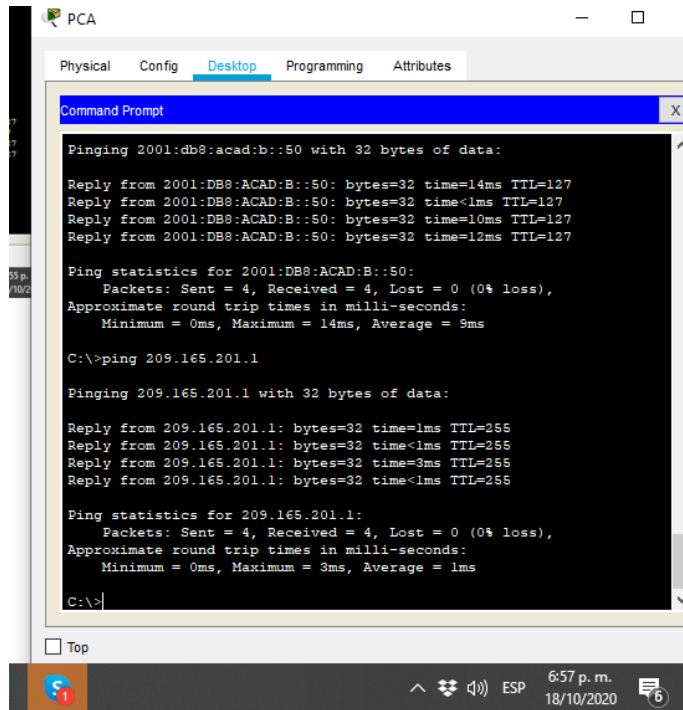


Figure 16. ping 2001:db8:acad:209::1

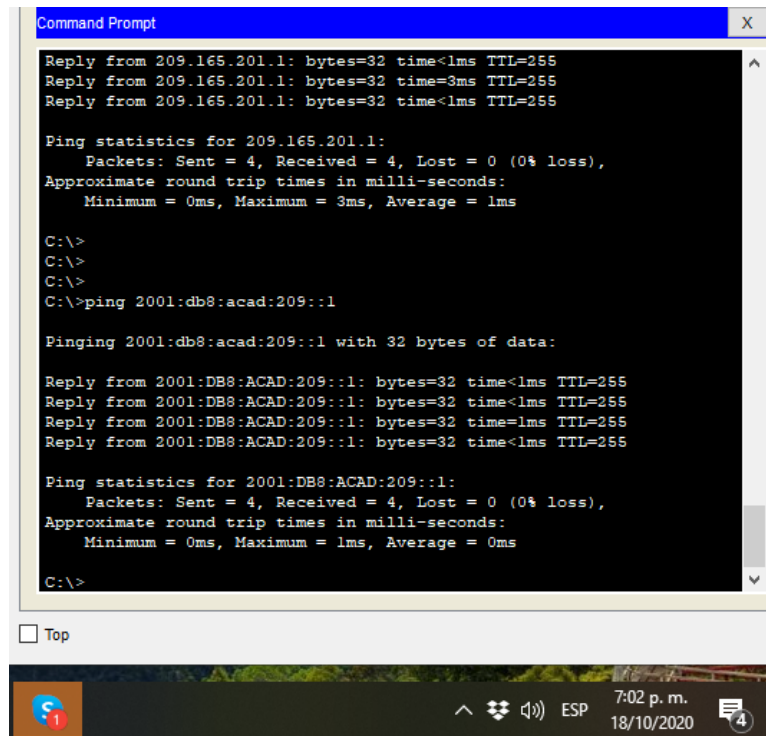


Figure 17.ping 209.165.201.1

```
Physical Config Desktop Programming Attributes
Command Prompt
Pinging 2001:db8:acad:b::50 with 32 bytes of data:
Reply from 2001:DB8:ACAD:B::50: bytes=32 time=12ms TTL=128
Reply from 2001:DB8:ACAD:B::50: bytes=32 time=1ms TTL=128
Reply from 2001:DB8:ACAD:B::50: bytes=32 time=2ms TTL=128
Reply from 2001:DB8:ACAD:B::50: bytes=32 time=25ms TTL=128

Ping statistics for 2001:DB8:ACAD:B::50:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 25ms, Average = 10ms

C:\>ping 209.165.201.1

Pinging 209.165.201.1 with 32 bytes of data:
Reply from 209.165.201.1: bytes=32 time=1ms TTL=255
Reply from 209.165.201.1: bytes=32 time<1ms TTL=255
Reply from 209.165.201.1: bytes=32 time<1ms TTL=255
Reply from 209.165.201.1: bytes=32 time<1ms TTL=255

Ping statistics for 209.165.201.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

Figure 18.ping 2001:db8:acad:209::1

```
PCB
Physical Config Desktop Programming Attributes
Command Prompt
Pinging 209.165.201.1 with 32 bytes of data:
Reply from 209.165.201.1: bytes=32 time=1ms TTL=255
Reply from 209.165.201.1: bytes=32 time<1ms TTL=255
Reply from 209.165.201.1: bytes=32 time<1ms TTL=255
Reply from 209.165.201.1: bytes=32 time<1ms TTL=255

Ping statistics for 209.165.201.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>PING 2001:db8:acad:209::1

Pinging 2001:db8:acad:209::1 with 32 bytes of data:
Reply from 2001:DB8:ACAD:209::1: bytes=32 time=1ms TTL=255
Reply from 2001:DB8:ACAD:209::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:209::1: bytes=32 time=3ms TTL=255
Reply from 2001:DB8:ACAD:209::1: bytes=32 time<1ms TTL=255

Ping statistics for 2001:DB8:ACAD:209::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 3ms, Average = 1ms

C:\>
```

Figure 19.ping 10.19.8.1

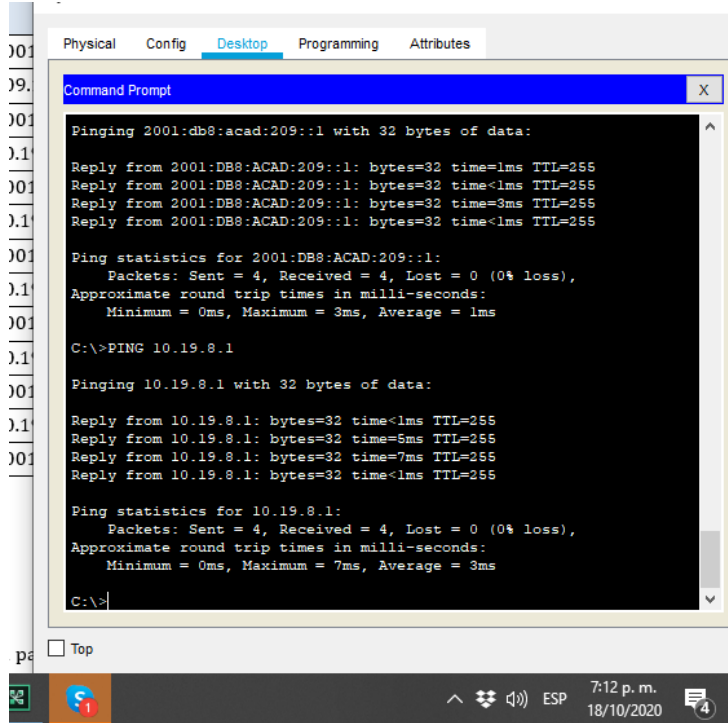


Figure 20.ping 2001:db8:acad:a::1

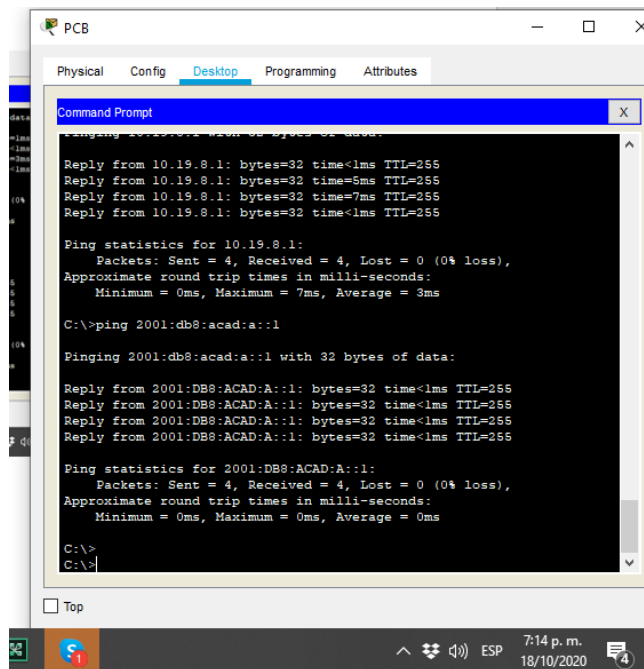


Figure 21. ping 10.19.8.65

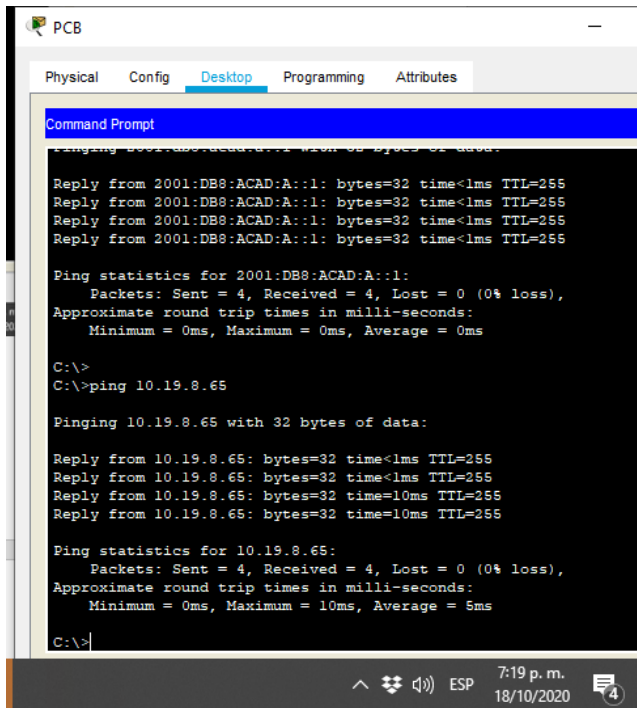


Figure 22. ping 2001:db8:acad:b::1

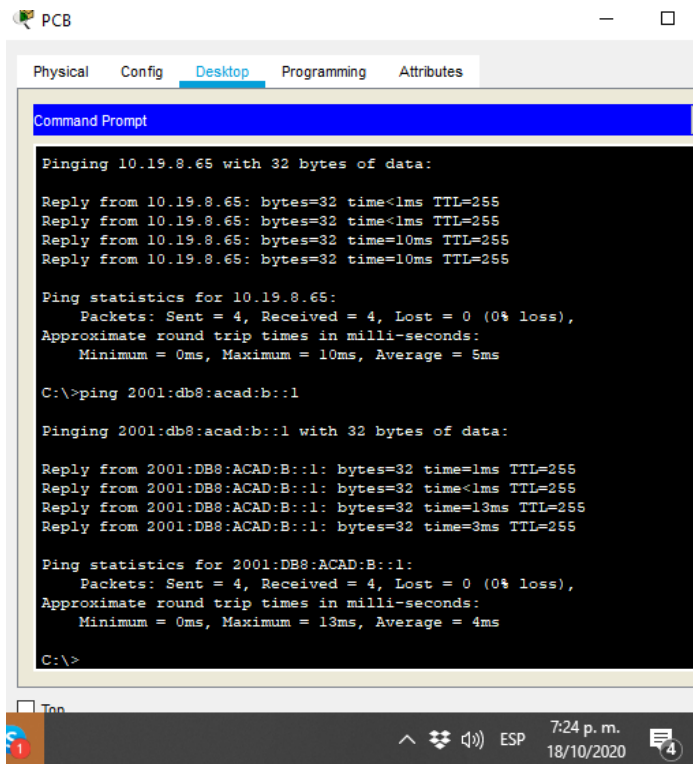


Figure 23. ping 10.19.8.97

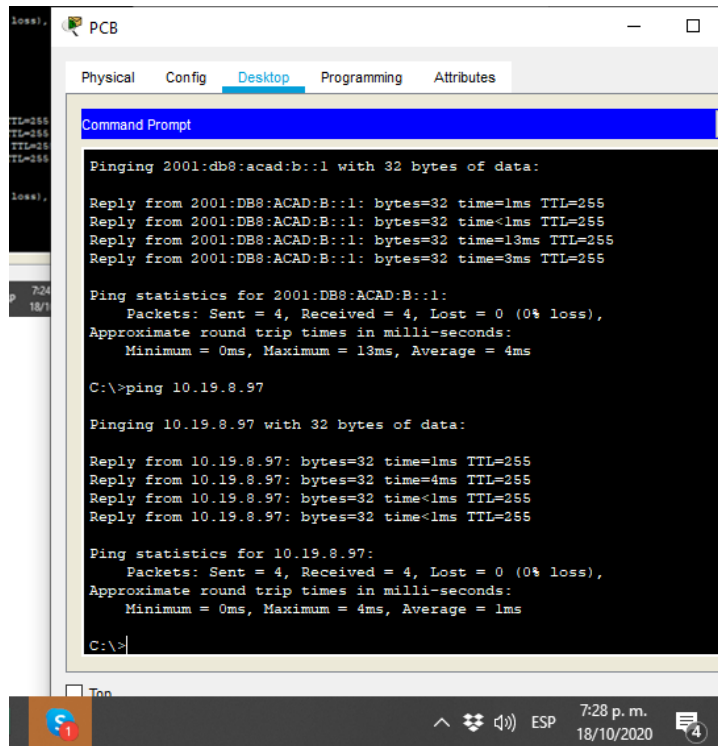


Figure 24. ping 2001:db8:acad:c::1

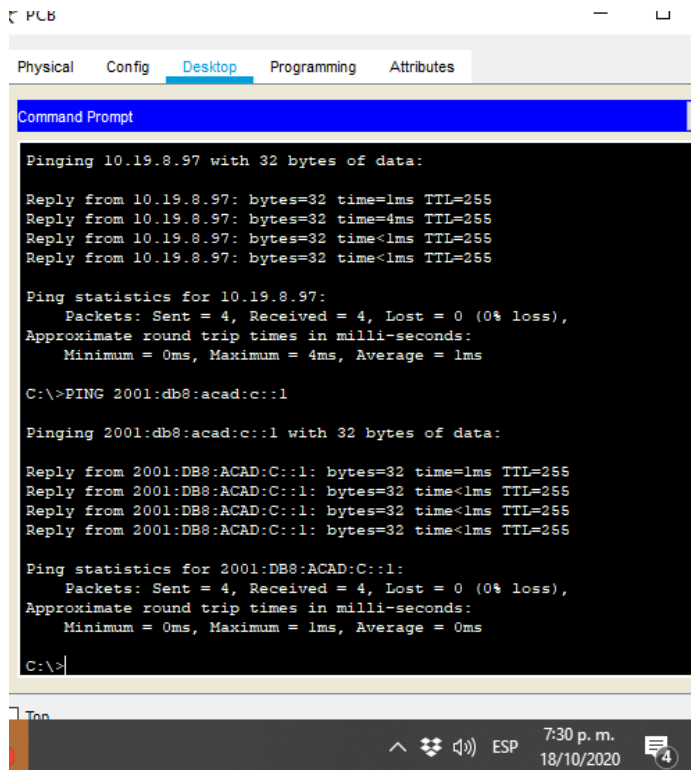


Figure 25. ping 10.19.8.98

```
PCB
Physical Config Desktop Programming Attributes
Command Prompt
Pinging 10.19.8.98 with 32 bytes of data:
Request timed out.
Reply from 10.19.8.98: bytes=32 time<1ms TTL=254
Reply from 10.19.8.98: bytes=32 time=3ms TTL=254

Ping statistics for 10.19.8.98:
    Packets: Sent = 3, Received = 2, Lost = 1 (34% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 3ms, Average = 1ms

Control-C
^C
C:\>ping 10.19.8.98

Pinging 10.19.8.98 with 32 bytes of data:

Reply from 10.19.8.98: bytes=32 time=1ms TTL=254
Reply from 10.19.8.98: bytes=32 time=13ms TTL=254
Reply from 10.19.8.98: bytes=32 time=3ms TTL=254
Reply from 10.19.8.98: bytes=32 time=3ms TTL=254

Ping statistics for 10.19.8.98:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 13ms, Average = 5ms

C:\>
```

Figure 26. ipconfig /all pc b

```
PCB
Physical Config Desktop Programming Attributes
Command Prompt
ipconfig /all

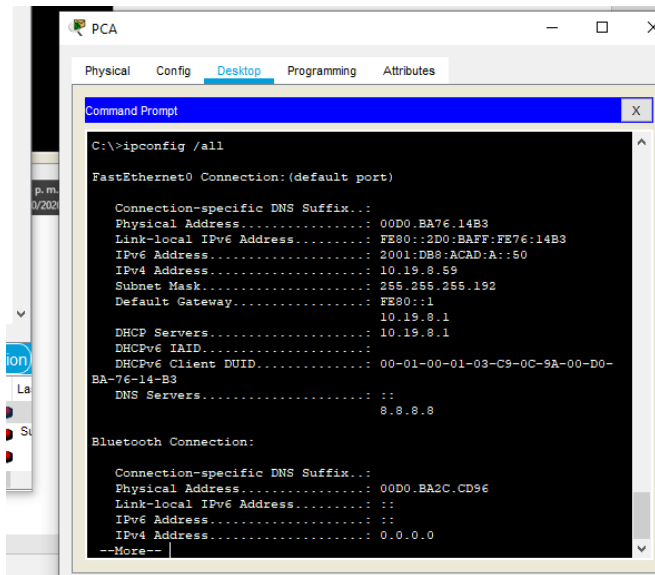
FastEthernet0 Connection: (default port)

    Connection-specific DNS Suffix... : ccna-b.net
    Physical Address. . . . . : 00D0.D30A.21D1
    Link-local IPv6 Address . . . . . : FE80::2D0:D3FF:FE0A:21D1
    IPv6 Address. . . . . : 2001:DB8:ACAD:B::50
    IPv4 Address. . . . . : 10.19.8.85
    Subnet Mask . . . . . : 255.255.255.224
    Default Gateway . . . . . : FE80::1
    . . . . . : 10.19.8.65
    DHCP Servers . . . . . : 10.19.8.65
    DHCPv6 IAID . . . . . :
    DHCPv6 Client DUID. . . . . : 00-01-00-01-09-04-5C-E6-00-D0-
D3-0A-21-D1
    DNS Servers . . . . . :
    . . . . . : 8.8.8.8

Bluetooth Connection:

    Connection-specific DNS Suffix... : ccna-b.net
    Physical Address. . . . . : 0002.167D.8307
    Link-local IPv6 Address . . . . . :
    IPv6 Address. . . . . :
    IPv4 Address. . . . . : 0.0.0.0
    Subnet Mask . . . . . : 0.0.0.0
    --More--
```

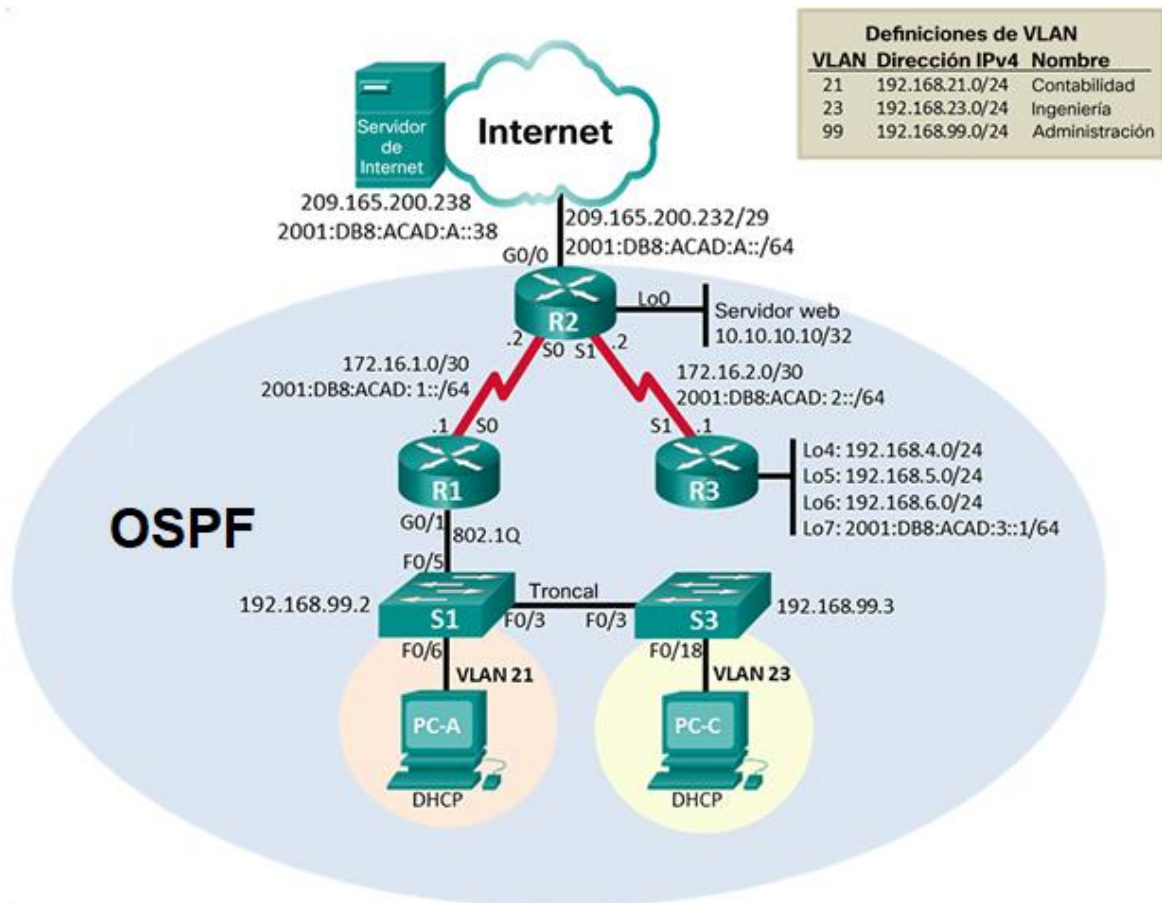
Figure 27. ipconfig /all pca

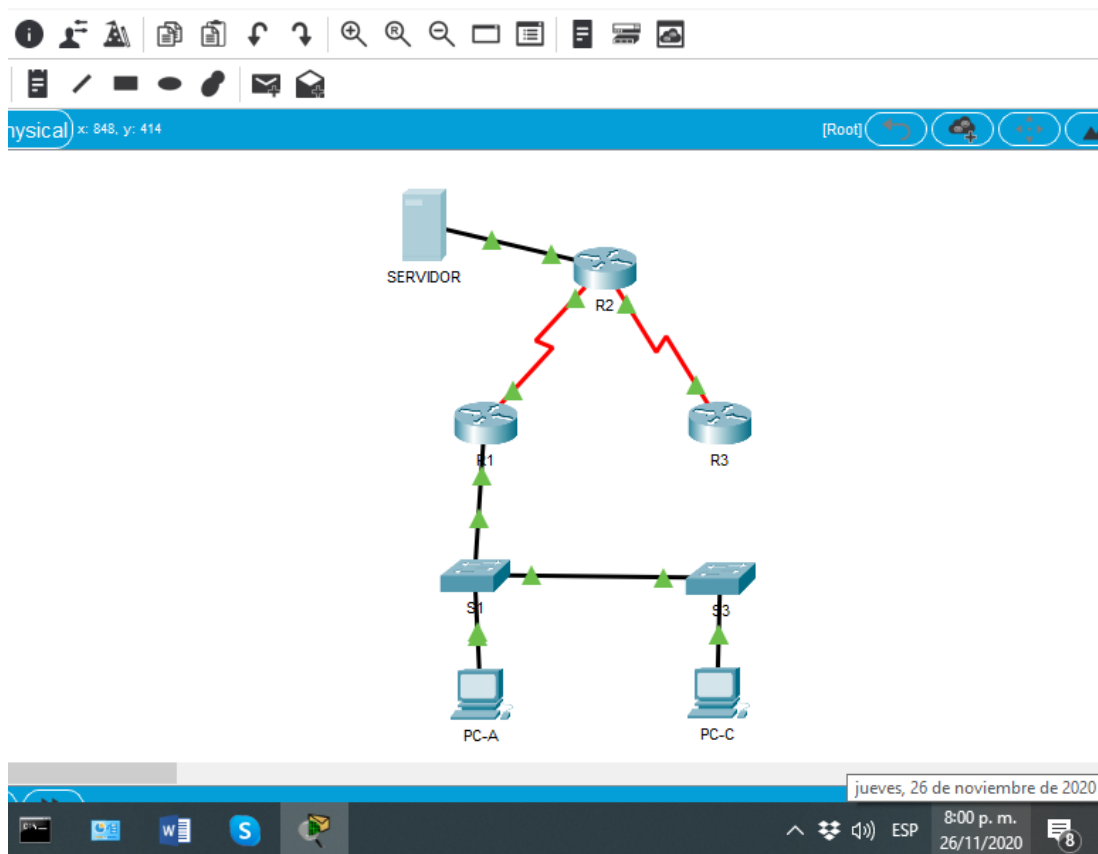


ESCENARIO 2

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

Figure 28 Escenario 2





Inicializar dispositivos todos los dispositivos del escenario 2

Inicializar y volver a cargar los routers y los switches se procedió a eliminar las configuraciones actuales para luego inicializar sus configuración por defecto

Table 12 inicializacion dispositivos escenario 2

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	#erase startup-config
Volver a cargar todos los routers	#reload
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	switch> enable switch# erase startup-config switch# delete flash:vlan.dat
volver a cargar ambos switches	switch#reload
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Switch#show vlan brief

Configurar los parámetros básicos de los dispositivos

Configurar la computadora de Internet

Las tareas de configuración del servidor de Internet incluyen lo siguiente dirección ip mascara Gateway y dns

Table 13 configuracion del servidor de internet escenario 2

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.240
Gateway predeterminado	209.165.200.225
Dirección IPv6/subred	2001:DB8:ACAD:A::38
Gateway predeterminado IPv6	2001:DB8:ACAD:2::1

Configurar R1

Configuración del router 1 donde se configura la seguridad de privilegio y consola e encriptación su mensaje de inicio y la configuración de ñas interfaces de entrada como de salida con sus rutas estáticas

Table 14 configuracion R1 escenario 2

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	No ip domain-lookup
Nombre del router	R1
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	Service password-encryption
Mensaje MOTD	#banner motd "se prohíbe el acceso no autorizado"
Interfaz S0/0/0	R1(config-if)#ip address 172.16.1.1 255.255.255.252 R1(config-if)#ipv6 address 2001:db8:acad:1::1/64 R1(config-if)#clock rate 128000 R1(config-if)#no shut
Rutas predeterminadas	Configurar una ruta IPv4 predeterminada de S0/0/0 Configurar una ruta IPv6 predeterminada de S0/0/0

Configurar R2

Configuración del router 2 donde se configura la seguridad de privilegio y consola e encriptación su mensaje de inicio y la configuración de ñas interfaces de entrada como de salida con sus rutas estáticas donde se agrega loopback y e interfaz de simulación de internet o web.

Table 15 configuracion R2 escenario 2

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	No ip domain-lookup
Nombre del router	R2
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	Service password-encryption

Habilitar el servidor HTTP	#banner motd "se prohíbe el acceso no autorizado"
Mensaje MOTD	Se prohíbe el acceso no autorizado.
Interfaz S0/0/0	interface Serial0/0/0 ip address 172.16.1.2 255.255.255.252 Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz
Interfaz S0/0/1	interface Serial0/0/1 ip address 172.16.2.1 255.255.255.252. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. clock rate 128000. No shut
Interfaz G0/0 (simulación de Internet)	interface GigabitEthernet0/0 ip address 209.165.200.233 255.255.255.248. Establezca la dirección IPv6. Utilizar la primera dirección disponible en la subred. No shut
Interfaz loopback 0 (servidor web simulado)	interface Loopback0 ip address 10.10.10.10 255.255.255.255
Ruta predeterminada	Configure una ruta IPv4 predeterminada de G0/0. Configure una ruta IPv6 predeterminada de G0/0.

Configurar R3

Configuración del router 3 donde se configura la seguridad de privilegio y consola e encriptación su mensaje de inicio y la configuración de ñas interfaces de entrada como de salida se agrega 4 loopback

Table 16 configuracion R3escenario 2

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	Service password-encryption
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	

Configurar S1

S1 se configura por el momento datos como nombre del dispositivo seguridad y mensaje de inicio

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	No ip domain-lookup
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	Service password-encryption
Mensaje MOTD	banner motd "se prohíbe el acceso no autorizado"

Verificar la conectividad de la red

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

Table 17 resultados de pruebas ping escenario 2

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	ok
R2	R3, S0/0/1	172.16.2.2	ok
PC de Internet	Gateway predeterminado	209.165.200.225	ok

Configurar S1

Se configura en el s1 la ip de administración de este los puertos troncales entre el router y switch y de acceso para el pc y se realiza el apagado de los puertos que no se van a utilizar

Table 18 configuracion S1 puertos troncales y accesos escenario 2

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	S1(config)#vlan 21 S1(config-vlan)#name contabilidad S1(config-vlan)#vlan 23 S1(config-vlan)#name ingenieria S1(config-vlan)#vlan 99 S1(config-vlan)#administracion
Asignar la dirección IP de administración.	S1(config-if)#ip address 192.168.99.2 255.255.255.0
Asignar el gateway predeterminado	S1(config-if)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	S1(config-if)#switchport trunk native vlan 1
Forzar el enlace troncal en la interfaz F0/5	S1(config-if)#switchport trunk native vlan 1

Configurar el resto de los puertos como puertos de acceso	S1(config-if)#interface range f0/1-2, f0/4, f0/6-24, g0/1-2 S1(config-if-range)#switchport mode access
Asignar F0/6 a la VLAN 21	S1(config-if)#switchport access vlan 21
Apagar todos los puertos sin usar	S1(config-if)#interface range f0/1-2, f0/4, f0/7-24, g0/1-2 S1(config-if-range)#shutdown

Configurar S3

Se configura en el s3 la ip de administración de este los puertos troncales entre el router y switch y de acceso para el pc y se realiza el apagado de los puertos que no se van a utilizar

Table 19 configuracion s3 puertos troncales y accesos escenario 2

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	S3(config)#vlan 21 S3(config-vlan)#name contabilidad S3(config-vlan)#vlan 23 S3(config-vlan)#name ingenieria S3(config-vlan)#vlan 99 S3(config-vlan)#administracion.
Asignar la dirección IP de administración	S3(config-if)#ip address 192.168.99.3 255.255.255.0
Asignar el gateway predeterminado.	S3(config-if)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	S3(config)#interface f0/3 S3(config-if)# S3(config-if)#switchport trunk native vlan 1

Configurar el resto de los puertos como puertos de acceso	S3(config-if)#interface range f0/1-2, f0/4-24, g0/1-2
Asignar F0/18 a la VLAN 21	S3(config)#interface f0/18 S3(config-if)#switchport access vlan 21
Apagar todos los puertos sin usar	S3(config)#interface range f0/1-2, f0/4-17, f0/19-24, g0/1-2

Configurar R1

Se configura router 1 las interfaces de administracion y la subinterfase encapsulada para el área de ingeniería y contabilidad con su segmento de ips para cada uno.

Table 20 configuracion R1 subinterface lan

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	R1(config)#interface g0/1.21 R1(config-subif)#description LAN de contabilidad R1(config-subif)#encapsulation dot1q 21 R1(config-subif)#ip address 192.168.21.1 255.255.255.0
Configurar la subinterfaz 802.1Q .23 en G0/1	R1(config-subif)#description LAN de ingenieria R1(config-subif)#encaptulation dot1q 23 R1(config-subif)#ip address 192.168.23.1 255.255.255.0

Configurar la subinterfaz 802.1Q .99 en G0/1	<pre>R1(config)#interface g0/1.99 R1(config-subif)#description LAN de administración R1(config-subif)#encapsulation dot1q 99 R1(config-subif)#ip address 192.168.99.1 255.255.255.0</pre>
Activar la interfaz G0/1	No shut

Verificar la conectividad de la red

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

Table 21 resultados ping entre dispositivos escenario 2

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

Configurar el protocolo de routing dinámico OSPF

Configurar OSPF en el R1 para identificar la ruta más corta entre nodos y evitar la congestión de este

Table 22 configuración R1 OSPF

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R1(config)#router ospf 1

Anunciar las redes conectadas directamente	<pre>R1(config-router)#network 172.16.1.0 0.0.0.3 area 0 R1(config-router)#network 192.168.21.0 0.0.0.255 area 0 R1(config-router)#network 192.168.23.0 0.0.0.255 area 0 R1(config-router)#network 192.168.99.0 0.0.0.255 area 0</pre>
Establecer todas las interfaces LAN como pasivas	<pre>R1(config-router)#passive- interface g0/1.21 R1(config-router)#passive- interface g0/1.23 R1(config-router)#passive- interface g0/1.99</pre>
Desactive la sumarización automática	<pre>R1(config-router)#router rip R1(config-router)#no auto- summary</pre>

Configurar OSPF en el R2

Configurar OSPF en el R2 para identificar la ruta más corta entre nodos y evitar la congestión de este

Table 23configuracion R2 OSPF

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R2(config)#router ospf 1

Anunciar las redes conectadas directamente	R2(config-router)#network 172.16.1.0 0.0.0.3 area 0 R2(config-router)#network 172.16.1.0 0.0.0.3 area 0 R2(config-router)#network 10.10.10.0 0.0.0.255 area 0
Establecer la interfaz LAN (loopback) como pasiva	R2(config-router)#passive- interface loopback0
Desactive la sumarización automática.	R2(config-router)#no auto- summary

Configurar OSPFv3 en el R2

La configuración del R3 incluye las siguientes tareas:

Table 24 configuración R2 OSPF v3

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R3(config)#router ospf 1
Anunciar redes IPv4 conectadas directamente	R3(config-router)#network 172.16.2.0 0.0.0.3 area 0
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	R3(config-router)#passive- interface lo4 R3(config-router)#passive- interface lo5 R3(config-router)#passive- interface lo6
Desactive la sumarización automática.	R3(config-router)#router rip R3(config-router)#no auto- summary

Verificar la información de OSPF

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

Table 25comandos CLI informacion 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?	R2#show ip ospf neighbor
¿Qué comando muestra solo las rutas OSPF?	R2#show ip route ospf
¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	R2#show ip protocols

Implementar DHCP y NAT para IPv4

Configurar el R1 como servidor de DHCP para las VLAN 21 y 23 que serian la interface de contabilidad e ingeniería excluyendo un numero de direcciones ips para configuración estática es los dispositivos de red

Table 26configuracion R1 DHCP escenario 2

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20
Crear un pool de DHCP para la VLAN 21.	R1(dhcp-config)#ip dhcp pool ACCT R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com R1(dhcp-config)#default-router 192.168.21.1 R1(dhcp-config)#network 192.168.21.0 255.255.255.0

<p>Crear un pool de DHCP para la VLAN 23</p>	<pre>R1(dhcp-config)#ip dhcp pool ENGNR R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com R1(dhcp-config)#default-router 192.168.23.1 R1(dhcp-config)#network 192.168.23.0 255.255.255.0</pre>
--	---

Configurar la NAT estática y dinámica en el R2

Configuración de nat en el router 2 para direccionar el trafico hacia la interface web y permitir lista de accesos

Table 27configuracion Nat web

Elemento o tarea de configuración	Especificación
<p>Crear una base de datos local con una cuenta de usuario</p>	<pre>R2(config)#username webuser password cisco12345 R2(config)#line console 0 R2(config-line)#login local R2(config)#line vty 0 15 R2(config-line)#login local</pre>
<p>Habilitar el servicio del servidor HTTP</p>	
<p>Configurar el servidor HTTP para utilizar la base de datos local para la autenticación</p>	

Crear una NAT estática al servidor web.	<pre>R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229 R2(config)#interface g0/0 R2(config-if)#ip nat outside R2(config-if)#interface lo0 R2(config-if)#ip nat inside R2(config-if)#</pre>
Asignar la interfaz interna y externa para la NAT estática	<pre>R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255</pre>
Configurar la NAT dinámica dentro de una ACL privada	<pre>R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255 R2(config)#access- list 1 permit 192.168.4.0 0.0.0.255</pre>
Defina el pool de direcciones IP públicas utilizables.	<pre>R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.229 netmask 255.255.255.248</pre>
Definir la traducción de NAT dinámica	<pre>R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255</pre>

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.

Table 28 verificar dhcp y nat

Prueba	Resultados
--------	------------

Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	ok
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	ok
Verificar que la PC-A pueda hacer ping a la PC-C Nota: Quizá sea necesario deshabilitar el firewall de la PC.	ok
Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.229) Iniciar sesión con el nombre de usuario webuser y la contraseña cisco12345	ok

Configurar NTP

Table 29 configuración NTP

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	R2#clock set 09:00:00 mar 5 2016
Configure R2 como un maestro NTP.	R2(config)#ntp authentication-key 5 md5 1511021F0725 7 R2(config)#ntp authenticate R2(config)#ntp trusted- key 5 R2(config)#ntp master R2(config)#ntp server pool.ntp.org

Configurar R1 como un cliente NTP.	Servidor: R2
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	ntp update-calendar
Verifique la configuración de NTP en R1.	show ntp

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

Restringir el acceso a las líneas VTY en el R2

Table 30 configuración acceso ACL escenario

Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	R2(config)#ip access-list standar ADMIN-MGT
Aplicar la ACL con nombre a las líneas VTY	R2(config-std-nacl)#permit host 172.16.1.1
Permitir acceso por Telnet a las líneas de VTY	R2(config)#line vty 0 15
Verificar que la ACL funcione como se espera	R2(config-line)#access-class ADMIN-MGT in

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

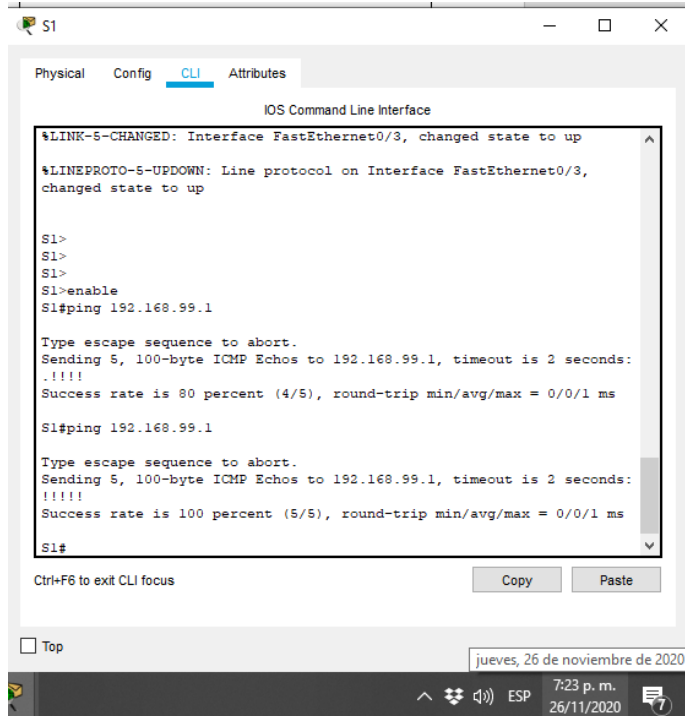
Table 31 comando CLI

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	Show access-lists

Restablecer los contadores de una lista de acceso	Clear ip Access-list counters
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en 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.
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	Clear ip nat translation

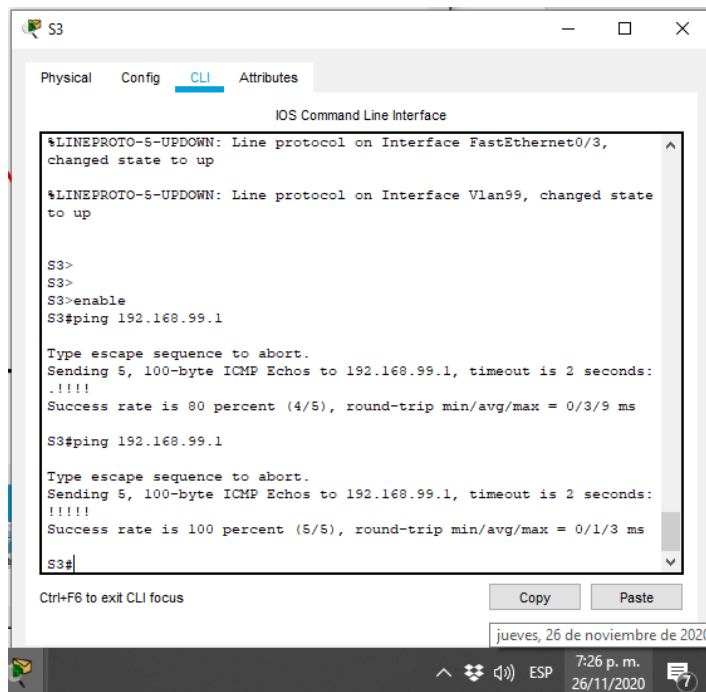
GRAFICAS ESCENARIO 2

Figure 29 ping de s1 a r1 vlan99



```
S1
Physical Config CLI Attributes
IOS Command Line Interface
%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3,
changed state to up
S1>
S1>
S1>
S1>enable
S1#ping 192.168.99.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/1 ms
S1#ping 192.168.99.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
S1#
```

Figure 30 ping de s3 a r1 vlan 99



```
S3
Physical Config CLI Attributes
IOS Command Line Interface
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3,
changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state
to up
S3>
S3>
S3>enable
S3#ping 192.168.99.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/3/9 ms
S3#ping 192.168.99.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/1/3 ms
S3#
```

Figure 31 ping s1 a r1 vlan 21

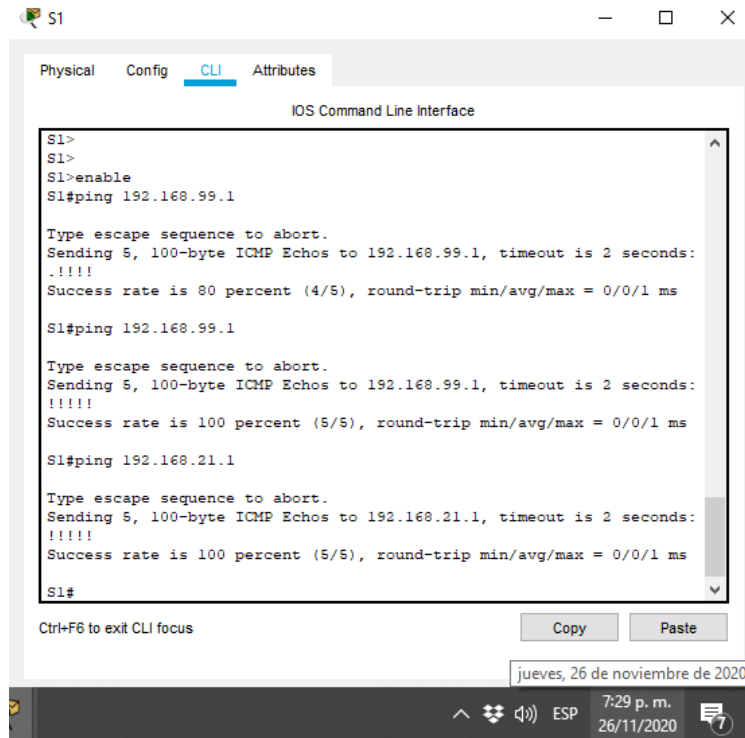


Figure 32 ping de s3 a r1 vlan 23

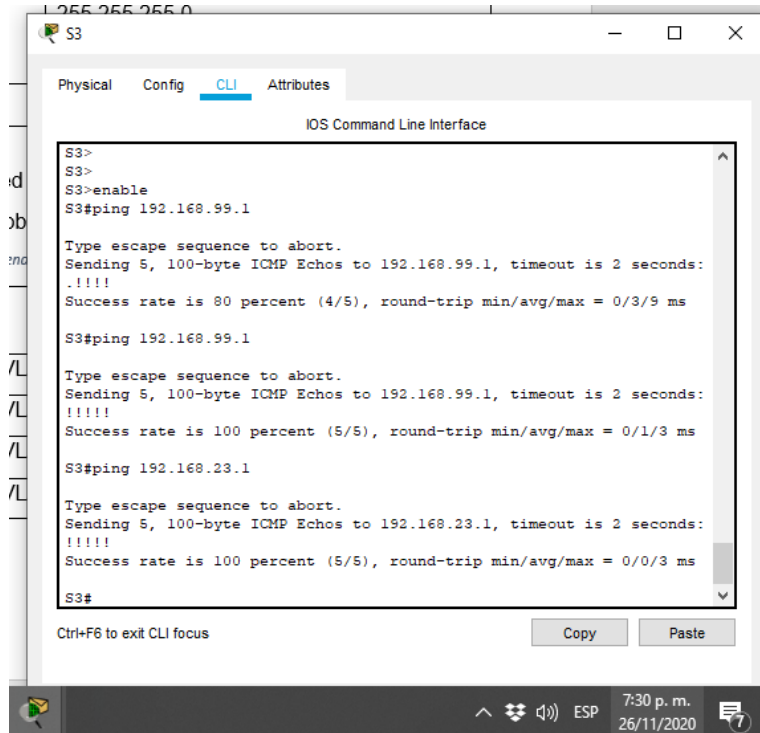


Figure 33 DHCP PC-A

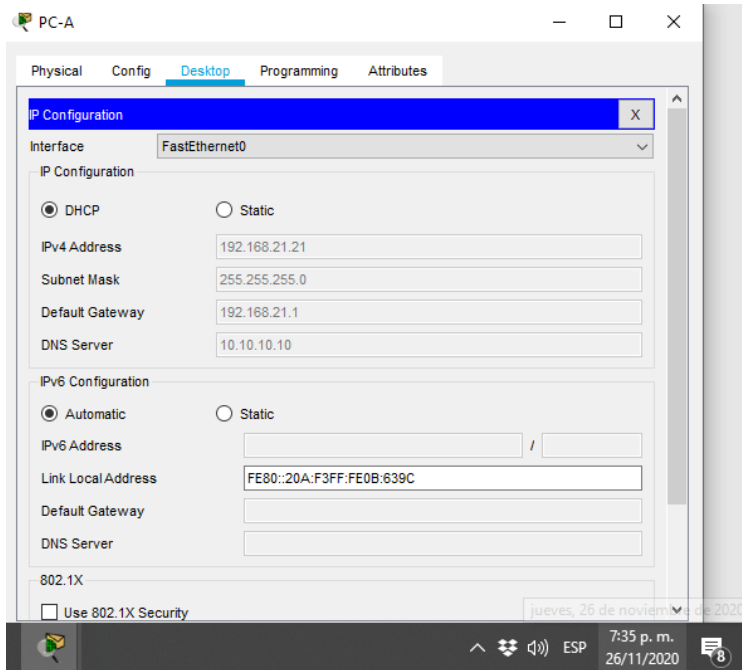


Figure 34 DHCP PC-C

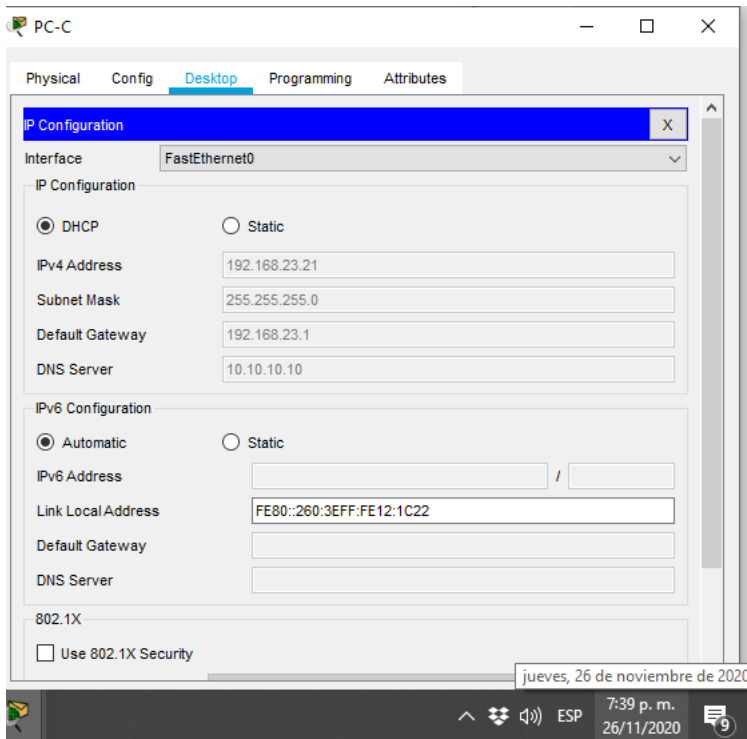


Figure 35 ping PC-A A PC-C

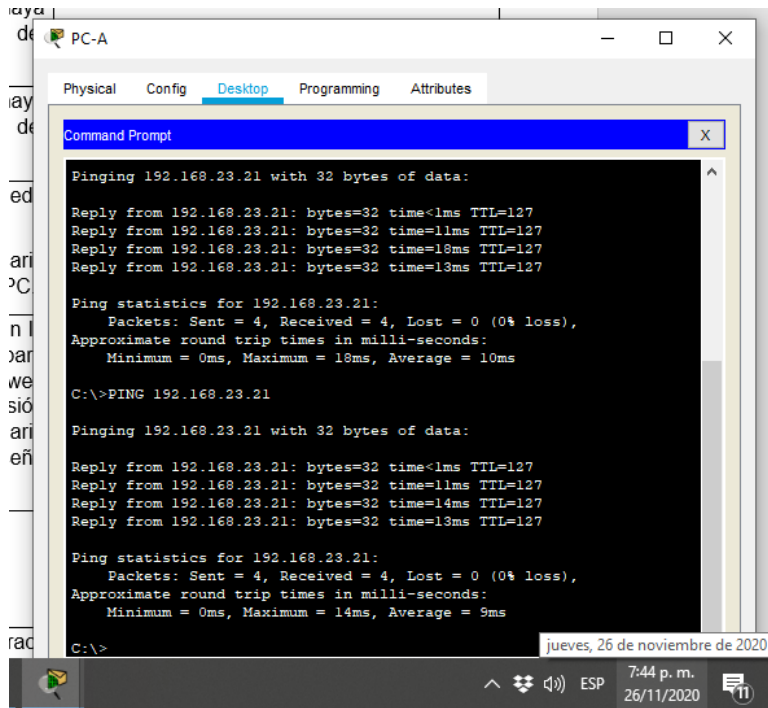
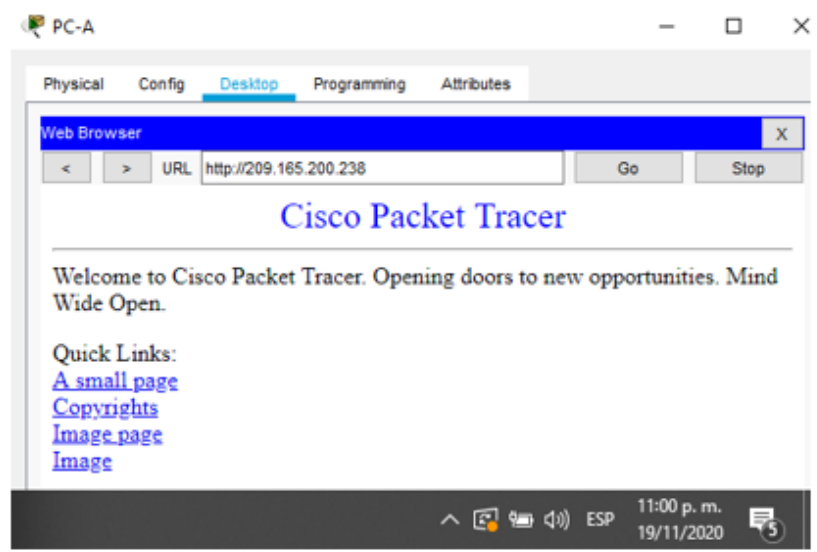


Figure 36 NAVEGADOR WEB



CONCLUSIONES

He logrado conocer y configurar un router cisco con subinterfaces vlan y habilitar dhcp y habilitar generar ipv6 y siendo todo esto comprobado y verificando el estado de conexión y respuestas de ping entre dispositivo dando conexiones correctas y respuestas correctas entre las diferentes ips que están configuradas en los diferentes dispositivo de la red.

Packet tracer emulador de cisco me permitio aprender la configuración y funcionamiento de un router y switch cisco esto me ayuda en a futuras configuraciones dado que tuviera la maquina física puedo realizar estas pruebas antes de en el emulador y después configuración en la maquina física

E configurado y dando respuestas satisfactorias en el escenario 2 comprendiendo el uso del nat para re direccionar y ospf para dar la ruta mas corta en la red y su salida hacia internet o dispositivo físico también el uso del ntp para tener actualizado y sincronizado el horario y lejos de nuestro dispositivos y asi un control de nuestra red en cualquier suceso en este ya si encontrar futuros errores en ellos

BIBLIOGRAFIA

Physical and Logical Infrastructure Requirements
Por Robert Barton, Jerome Henry, David Hucaby Oct 3, 2020

Ethernet Switching
Por Cisco Networking Academy Jul 15, 2020

Inter-VLAN Routing
Por Cisco Networking Academy Jul 29, 2020

Ethernet Switching
Por Cisco Networking Academy Jul 15, 2020

Implementing Inter-VLAN Routing
Por Scott Empson, Patrick Gargano Jun 3, 2020

IP Routing in the LAN
Por Wendell Odom Feb 13, 2020

configuración ACL packet tracer
Por Raúl Prieto Fernández 4 julio, 2019

<https://www.ciscopress.com/articles>

<http://www.mundocisco.com/>

<https://www.itesa.edu.mx/netacad/>

<https://www.raulprietofernandez.net/blog/packet-tracer/configuracion-de-acls-con-packet-tracer>

<https://neuromarketingytecnologia.com/configuracion-genera/>

<https://gist.github.com/GusGA/51e17fc59e701fcf0cb1c3a9cd92eabc>

<https://ccnadesdecero.es/como-configurar-router-cisco/>

ANEXO

Escenario 1

<https://drive.google.com/file/d/1qI8eZETiaGp54qHFiKWG0rFbquS20Ciw/view?usp=sharing>

Escenario 2

<https://drive.google.com/file/d/1PIBWYIPTmDxyYB3ODGhqMmalFsB-cjU9/view?usp=sharing>

Artículo de investigación

<https://drive.google.com/file/d/1DMPYI4aR0nXuWCOeFanyeKeZRHJFnfn/view?usp=sharing>