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

JEISSON HUMBERTO HERNANDEZ HERNANDEZ

DIRECTOR DE CURSO
INGENIERO JUAN CARLOS VESGA FERREIRA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
INGENIERÍA DE SISTEMAS
VILLAVICENCIO - META
NOVIEMBRE, 2020

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

PRUEBA DE HABILIDADES CCNA II - 2020

Trabajo de la opción de grado para optar al título de Ingeniero de Sistemas

PRESENTADO POR:
JEISSON HUMBERTO HERNANDEZ

PRESENTADO A:
INGENIERO JUAN CARLOS VESGA FERREIRA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
INGENIERÍA DE SISTEMAS
VILLAVICENCIO - META

NOVIEMBRE, 2020

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____

_____
Firma del presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

Villavicencio, 30 de noviembre de 2020

CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

GLOSARIO

ETHERCHANNEL: es una tecnología de Cisco construida de acuerdo con los estándares 802.3 full-duplex Fast Ethernet. Permite la agrupación lógica de varios enlaces físicos Ethernet, esta agrupación es tratada como un único enlace y permite sumar la velocidad nominal de cada puerto físico Ethernet usado y así obtener un enlace troncal de alta velocidad.

ENLACE TRONCAL: es un enlace punto a punto, entre dos dispositivos de red, que transporta más de una VLAN. Un enlace troncal de VLAN le permite extender las VLAN a través de toda una red. Cisco admite IEEE 802.1Q para la coordinación de enlaces troncales en interfaces Fast Ethernet y Gigabit Ethernet. Más adelante en esta sección, aprenderá acerca de 802.1Q.

IEEE 802.1Q: también conocido como dot1Q, fue un proyecto del grupo de trabajo 802 de la IEEE para desarrollar un mecanismo que permita a múltiples redes compartir de forma transparente el mismo medio físico, sin problemas de interferencia entre ellas (Trunking).

LÍNEA VTY: son las líneas de terminal virtual del router, que se utilizan solamente para controlar las conexiones Telnet entrantes. Son virtuales en el sentido que son una función de software; no hay hardware relacionado con ellas. Aparecen en la configuración como line vty 0 4.

NAT: En redes, NAT significa Network Adress Translation o Traducción de direcciones de red en español. Se trata de un sistema que se utiliza en las redes bajo el protocolo IP y que nos permite el intercambio de paquetes entre dos redes que tienen asignadas mutuamente direcciones IP 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.

OSPF: Open Shortest Path First (OSPF), Abrir el camino más corto primero en español, es un protocolo de red para encaminamiento jerárquico de pasarela interior o Interior Gateway Protocol (IGP), que usa el algoritmo Dijkstra, para calcular la ruta más corta entre dos nodos.

PLANTILLA SDM: son plantillas propietarias de Cisco, que nos permiten configurar los switches de forma que se les saque un mayor rendimiento, en función de lo que vayan a trabajar.

RESUMEN

En este documento se configurarán dos topologías de red correspondientes a 2 escenarios. El primer escenario está compuesto por un router R1 modelo 4331, dos switch S1 y S2 modelo 3560 y en cada switch va conectado un host con nombre PC-A y PC-B respectivamente. El segundo escenario se compone de 3 router 1941, un servidor de internet, dos switch S1 y S2 modelo 3560 y en cada switch hay conectado un PC con nombres PC-A y PC-C respectivamente.

Los dispositivos interconectados no presentan ninguna configuración al inicio del ejercicio y se van configurando poco a poco ingresando comandos que son de direccionamiento, enrutamiento, seguridad, encriptación, encapsulación entre otros que nos permitirán al final del ejercicio tener una red segura bajo IPv4 e IPv6 con un nivel de seguridad aceptable y un funcionamiento óptimo aplicable a cualquier empresa.

PALABRAS CLAVES: ENCAPSULACIÓN; ENRUTAMIENTO; ETHERCHANNEL; IPV6; NAT; NTP; OSPF; TRONCAL.

ABSTRACT

In this document, two network topologies corresponding to 2 scenarios will be configured. The first scenario is made up of a router R1 model 4331, two switches S1 and S2 model 3560 and a host named PC-A and PC-B respectively is connected to each switch. The second scenario consists of 3 1941 routers, an internet server, two model 3560 switches S1 and S2, and a PC with names PC-A and PC-C respectively is connected to each switch.

The interconnected devices do not present any configuration at the beginning of the exercise and are being configured little by little by entering commands that are addressing, routing, security, encryption, encapsulation among others that will allow us at the end of the exercise to have a secure network under IPv4 and IPv6 with an acceptable level of security and optimal operation applicable to any company.

KEY WORDS: ENCAPSULATION; ETHERCHANNEL; IPV6; NAT; NTP; OSPF; ROUTING; TRUNK.

INTRODUCCIÓN

La red de internet se compone de varios dispositivos interconectados entre si enviando y recibiendo paquetes de un lado a otro, al principio eran pocos dispositivos, luego esta tecnología se fue aplicando a las empresas y finalmente se aplicó a hogares que actualmente gozan de servicio de internet.

Todos los equipos conectados al servicio de internet e incluso los que hacen parte de redes pequeñas como redes LAN funcionaban y aun funcionan con direcciones IPv4, pero al día de hoy tenemos tantísimos dispositivos conectados a redes de internet que requieren de un direccionamiento IP con mayor capacidad ya que IPv4 se ha visto limitada, es por eso que se implementó IPv6.

Una dirección IPv4 tiene un tamaño de 32 bits y una IPv6 tiene un total de 128 bits siendo así IPv6 capaz de albergar muchos mas host que IPv4 por lo que es capaz de soportar la cantidad de dispositivos que se conectan actualmente, teniendo en cuenta que al día de hoy hasta las neveras cuentan con servicio de conexión por wifi. En este documento veremos muchos aspectos en configuración de Router y de Switch incluyendo también la asignación de direcciones IP dinámicas y estáticas, la seguridad en los dispositivos, la conexión por túnel entre dos dispositivos iguales, la división de la red en redes virtuales más pequeñas lo que mejora la eficiencia y velocidad de la red y la implementación de protocolos como OSPF, NAT y NTP que mejoran el funcionamiento de la red.

Descripción de escenarios propuestos para la prueba de habilidades

Escenario 1
Topología

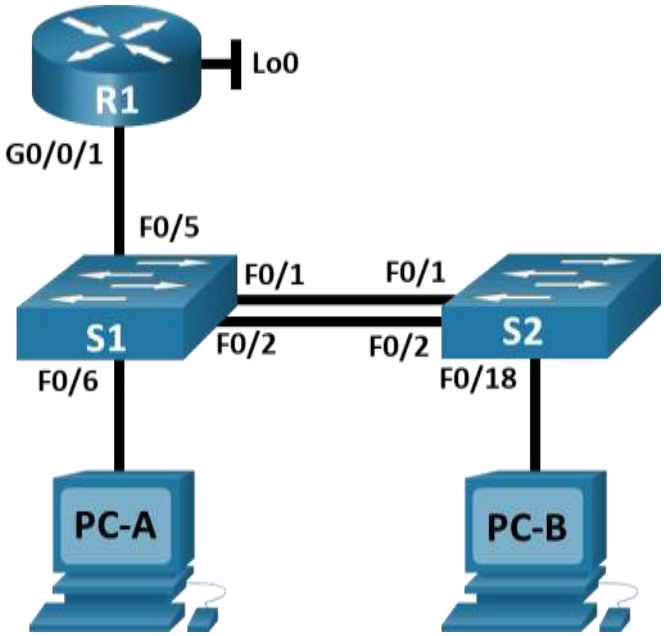


Figura 1: Topología Original escenario 1

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

1. Se selecciona una router 4331, se agrega a la topología y lo renombramos como R1, este router soporta direcciones IPv4 e IPv6, además tiene 3 puertos G0/0.

2. Seleccionamos 2 switch 3560, los agregamos a la topología y los nombramos S1 y S2 respectivamente, estos SW tienen 24 puertos F0/0 y 2 puertos G0/0.

3. Seleccionamos 2 PC de escritorio, los agregamos a la topología y los nombramos PC-A y PC-B respectivamente.

4. Conectamos con un tipo de conexión automático el R1 al S1.

5. Conectamos con un tipo de conexión automático S1 a S2 y hacemos lo mismo desde S2 hacia S1.

6. Conectamos con un tipo de conexión automático S1 a PC-A.

7. Conectamos con un tipo de conexión automático S2 a PC-B.

Con lo anterior habremos terminado de crear nuestra topología para proceder a configurarla.

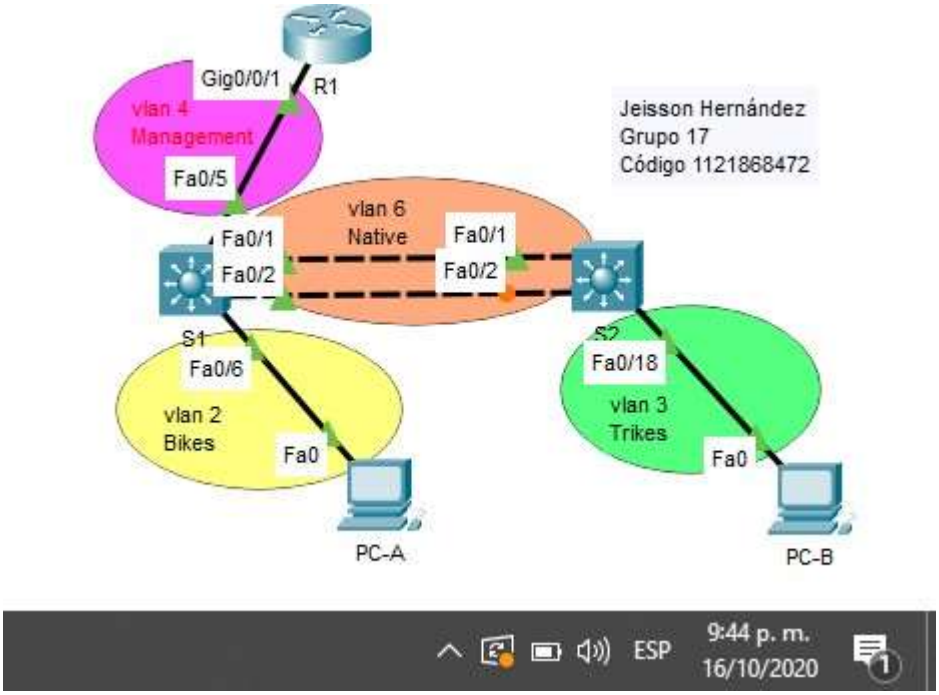


Figura 2: Topología Packet Tracer escenario 1

Tabla de VLAN

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

Tabla 1: VLAN

Tabla de asignación de direcciones

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
R1 G0/0/1.2	10.19.8.1 /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

Tabla 2: Asignación de direcciones

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

Instrucciones

Parte 1: Inicializar y Recargar y Configurar aspectos básicos

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.

Tarea	Comando
Borrar el archivo startup-config en el router	Router#erase startup-config Erasing the nvram filesystem will remove all configuration files! Continue? [confirm] [OK] Erase of nvram: complete %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Volver a cargar el router	Router#reload Proceed with reload? [confirm] Initializing Hardware ... no valid BOOT image found Final autoboot attempt from default boot device... Located isr4300-universalk9.16.06.04.SPA.bin ##
Borrar el archivo de configuración inicial en cada switch.	Switch#erase startup-config Erasing the nvram filesystem will remove all configuration files! Continue? [confirm] [OK] Erase of nvram: complete %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Eliminar el archivo de configuración vlan.dat en los switch	Switch#del vlan.dat Delete filename [vlan.dat]? Delete flash:/vlan.dat? [confirm] %Error deleting flash:/vlan.dat (No such file or directory)
Volver a cargar los switch	Switch#reload Proceed with reload? [confirm] C3560 Boot Loader (C3560-HBOOT-M) Version 12.2(25r)SEC, RELEASE SOFTWARE (fc4) cisco WS-C3560-24PS (PowerPC405) processor (revision P0) with 122880K/8184K bytes of memory. 3560-24PS starting... Loading "flash:/c3560-advipservicesk9-mz.122-37.SE1.bin"... ## [OK]

Tabla 3: Borrar la configuración de Switch y Router

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

Tarea	Especificación
Observar la plantilla predeterminada del S1 y S2	Switch#show sdm prefer The current template is "desktop default" template. The selected template optimizes the resources in the switch to support this level of features for 8 routed interfaces and 1024 VLANs. number of unicast mac addresses: 6K number of IPv4 IGMP groups + multicast routes: 1K number of IPv4 unicast routes: 8K number of directly-connected IPv4 hosts: 6K number of indirect IPv4 routes: 2K number of IPv4 policy based routing aces: 0 number of IPv4/MAC qos aces: 0.5K number of IPv4/MAC security aces: 1K
Configurar la plantilla SDM para que admita IPv6	Switch(config)#sdm prefer dual-ipv4-and-ipv6 Default Changes to the running SDM preferences have been stored, but cannot take effect until the next reload. Use 'show sdm prefer' to see what SDM preference is currently active.
Volver a cargar los switch	Switch#reload Proceed with reload? [confirm] C3560 Boot Loader (C3560-HBOOT-M) Version 12.2(25r)SEC, RELEASE SOFTWARE (fc4) cisco WS-C3560-24PS (PowerPC405) processor (revision P0) with 122880K/8184K bytes of memory. 3560-24PS starting... Loading "flash:/c3560-advipservicesk9-mz.122-37.SE1.bin"... ## [OK]

Tarea	Especificación
Observar la nueva plantilla del S1 y el S2	Switch#show sdm prefer The current template is "desktop IPv4 and IPv6 default" template. The selected template optimizes the resources in the switch to support this level of features for 8 routed interfaces and 1024 VLANs. number of unicast mac addresses: 2K number of IPv4 IGMP groups + multicast routes: 1K number of IPv4 unicast routes: 3K number of directly-connected IPv4 hosts: 2K number of indirect IPv4 routes: 1K number of IPv6 multicast groups: 1.125k number of directly-connected IPv6 addresses: 2K number of indirect IPv6 unicast routes: 1K number of IPv4 policy based routing aces: 0 number of IPv4/MAC qos aces: 0.5K number of IPv4/MAC security aces: 1K number of IPv6 policy based routing aces: 0 number of IPv6 qos aces: 0.625k number of IPv6 security aces: 0.5K
Habilitar el enrutamiento de unidifusión de IPv6 globalmente	Switch(config)#ipv6 unicast-routing

Tabla 4: Plantilla SDM IPv6

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

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tarea	Especificación
Desactivar la búsqueda DNS	Router>enable Router#config t Router(config)#no ip domain-lookup
Nombre del router	Router#config t Router(config)#hostname R1 R1(config)#
Nombre de dominio	R1(config)#ip domain name ccna-lab.com

Tarea	Especificación
Contraseña cifrada para el modo EXEC privilegiado	R1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	R1(config)#line console 0 R1(config-line)#password ciscoconpass R1(config-line)#login
Establecer la longitud mínima para las contraseñas	R1#config t R1(config)#security passwords min-length 10
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 4 R1(config-line)#login local R1(config-line)#exit
Configurar VTY solo aceptando SSH	R1(config)#crypto key generate rsa The name for the keys will be: R1.ccna-lab.com Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes. How many bits in the modulus [512]: 1024 % Generating 1024 bit RSA keys, keys will be non-exportable...[OK] R1(config)#ip ssh version 2 *mar. 2 3:2:13.506: %SSH-5-ENABLED: SSH 1.99 has been enabled R1(config)#line vty 0 4 R1(config-line)#transport input ssh
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption R1#copy running-config startup-config
Configure un MOTD Banner	R1#config t R1(config)#banner motd "Authorized Access Only"
Habilitar el routing IPv6	R1(config)#ipv6 unicast-routing

Tarea	Especificación
Configurar interfaz G0/0/1 y subinterfaces	R1(config)#interface gigabitEthernet 0/0/1.2 R1(config-subif)#description VLAN 2 Bikes R1(config-subif)#encapsulation dot1Q 2 R1(config-subif)#ip address 10.19.8.1 255.255.255.192 R1(config-subif)# ipv6 address fe80::1 link-local R1(config-subif)#ipv6 address 2001:db8:acad:a::1/64 R1(config-subif)#no shutdown R1(config)#interface gigabitEthernet 0/0/1.3 R1(config-subif)#description VLAN 3 Trikes R1(config-subif)#encapsulation dot1Q 3 R1(config-subif)#ip address 10.19.8.65 255.255.255.224 R1(config-subif)#ipv6 address fe80::1 link-local R1(config-subif)#ipv6 address 2001:db8:acad:b::1/64 R1(config-subif)#no shutdown R1(config)#interface gigabitEthernet 0/0/1.4 R1(config-subif)#description VLAN 4 Management R1(config-subif)#encapsulation dot1Q 4 R1(config-subif)#ip address 10.19.8.97 255.255.255.248 R1(config-subif)#ipv6 address fe80::1 link-local R1(config-subif)#ipv6 address 2001:db8:acad:c::1/64 R1(config-subif)#no shutdown R1(config)#interface gigabitEthernet 0/0/1.6 R1(config-subif)#description VLAN 6 Native R1(config-subif)#encapsulation dot1Q 6 R1(config-subif)#no shutdown
Configure el Loopback0 interface	R1(config)#interface loopback 0 R1(config-if)#description Interface Loopback R1(config-if)#ip address 209.165.201.1 255.255.255.224 R1(config-subif)#ipv6 address fe80::1 link-local R1(config-subif)#ipv6 address 2001:db8:acad:209::1/64 R1(config-subif)#no shutdown

Tarea	Especificación
Generar una clave de cifrado RSA	R1(config)#crypto key generate rsa The name for the keys will be: R1.ccna-lab.com Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes. How many bits in the modulus [512]: 1024 % Generating 1024 bit RSA keys, keys will be non-exportable...[OK] R1#copy running-config startup-config Destination filename [startup-config]? Building configuration... [OK]

Tabla 5: Configurar R1

Paso 3: Configure S1 y S2.

Las tareas de configuración incluyen lo siguiente:

Tarea	Especificación
Desactivar la búsqueda DNS.	Switch>enable Switch#config t Switch(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S1 S1(config)#
Nombre de dominio	S1(config)#ip domain name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	S1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	S1(config)#line console 0 S1(config-line)#password ciscoconpass S1(config-line)#login
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 4 S1(config-line)#login local S1(config-line)#exit

Tarea	Especificación
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S1(config)#crypto key generate rsa The name for the keys will be: S1.ccna-lab.com Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes. How many bits in the modulus [512]: 1024 % Generating 1024 bit RSA keys, keys will be non-exportable...[OK] S1(config)#ip ssh version 2 *mar. 2 17:18:29.490: %SSH-5-ENABLED: SSH 1.99 has been enabled S1(config)#line vty 0 4 S1(config-line)#transport input ssh
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption S1#copy run star
Configurar un MOTD Banner	S1#config t S1(config)#banner motd "Authorized Access Only"
Generar una clave de cifrado RSA	S1(config)#crypto key generate rsa The name for the keys will be: S1.ccna-lab.com Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes. How many bits in the modulus [512]: 1024 % Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

Tarea	Especificación
Configurar la interfaz de administración (SVI)	S1(config)#interface vlan 4 S1(config-if)#ip address 10.19.8.98 255.255.255.248 S1(config-if)#ipv6 address fe80::98 link-local S1(config-if)#ipv6 address 2001:db8:acad:c::98/64 S1(config-if)#no shutdown S2(config)#interface vlan 4 S2(config-if)#ip address 10.19.8.99 255.255.255.248 S2(config-if)#ipv6 address fe80::99 link-local S2(config-if)#ipv6 address 2001:db8:acad:c::99/64 S2(config-if)#no shutdown
Configuración del gateway predeterminado	S1(config)#ip default-gateway 10.19.8.97 S2(config)#ip default-gateway 10.19.8.97

Tabla 6: Configure S1 y S2

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

Paso 1: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tarea	Especificación
Crear VLAN	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)#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
Crear troncal 802.1Q que utilicen la VLAN 6 nativa	S1(config)#interface range fastEthernet 0/1-2 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)#exit S1(config)#interface fastEthernet 0/5 S1(config-if)#switchport trunk encapsulation dot1Q S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 6 S1(config)#exit

Tarea	Especificación
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	S1(config)#interface range fastEthernet 0/1-2 S1(config-if-range)#channel-group 1 mode active S1(config-if-range)#interface port-channel 1 S1(config-if)#switchport trunk encapsulation dot1Q S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk allowed vlan all S1(config-if)#channel-protocol lacp
Configurar el puerto de acceso de host para VLAN 2	S1(config)#interface fastEthernet 0/6 S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 2 S1(config-if)#exit
Configurar la seguridad del puerto en los puertos de acceso	*El único puerto de acceso es el f0/6 ya que los demás puertos usados son trunk es por esto que solo se configura la seguridad en f0/6* S1(config)#interface fastEthernet 0/6 S1(config-if)#switchport mode access S1(config-if)#switchport port-security S1(config-if)#switchport port-security maximum 3
Proteja todas las interfaces no utilizadas	S1(config)#interface range fastEthernet 0/3-4 S1(config-if)#switchport mode access S1(config-if)#description No Utilizada S1(config-if)#switchport access vlan 5 S1(config-if)#shutdown S1(config-if)#exit S1(config)#interface range fastEthernet 0/7-24 S1(config-if)#switchport mode access S1(config-if)#description No Utilizada S1(config-if)#switchport access vlan 5 S1(config-if)#shutdown S1(config-if)#exit S1(config)#interface range G0/1-2 S1(config-if)#switchport mode access S1(config-if)#description No Utilizada S1(config-if)#switchport access vlan 5 S1(config-if)#shutdown S1(config-if)#exit

Tabla 7: Configurar S1

Paso 2: Configure el S2.

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

Tarea	Especificación
Crear VLAN	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)#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
Crear troncal 802.1Q que utilicen la VLAN 6 nativa	S2(config)#interface range fastEthernet 0/1-2 S2(config-if-range)#switchport trunk encapsulation dot1Q S2(config-if)#switchport mode trunk S2(config-if)#switchport trunk native vlan 6 S2(config)#exit
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	S2(config)#interface range fastEthernet 0/1-2 S2(config-if)#channel-group 1 mode active S2(config-if-range)#interface port-channel 1 S2(config-if)#switchport trunk encapsulation dot1Q S2(config-if)#switchport mode trunk S2(config-if)#switchport trunk allowed vlan all S2(config-if)#channel-protocol lacp
Configurar el puerto de acceso del host para la VLAN 3	S2(config)#interface fastEthernet 0/18 S2(config-if)#switchport mode access S2(config-if)#switchport access vlan 3 S2(config-if)#exit

Tarea	Especificación
Configure port-security en los access ports	*El único puerto de acceso es el f0/18 ya que los demás puertos usados son trunk es por esto que solo se configura seguridad en f0/18* S2(config)#interface fastEthernet 0/18 S2(config-if)#switchport mode access S2(config-if)#switchport port-security S2(config-if)#switchport port-security maximum 3
Asegure todas las interfaces no utilizadas.	S2(config)#interface range F0/3-17 S2(config-if)#switchport mode access S2(config-if)#description No Utilizada S2(config-if)#switchport access vlan 5 S2(config-if)#shutdown S2(config-if)#exit S2(config)#interface range F0/19-24 S2(config-if)#switchport mode access S2(config-if)#description No Utilizada S2(config-if)#switchport access vlan 5 S2(config-if)#shutdown S2(config-if)#exit S2(config)#interface range G0/1-2 S2(config-if)#switchport mode access S2(config-if)#description No Utilizada S2(config-if)#switchport access vlan 5 S2(config-if)#shutdown S2(config-if)#exit

Tabla 8:Configure el S2

Parte 2: Configurar soporte de host

Paso 1: Configure R1

Las tareas de configuración para R1 incluyen las siguientes:

Tarea	Especificación
Configure Default Routing	R1(config)#ip route 0.0.0.0 0.0.0.0 loopback0 R1(config)#ipv6 route ::/0 loopback0

Tarea	Especificación
Configurar DHCP IPv4 para VLAN 2	*---A continuación, se excluyen las primeras 50 ips dejando únicamente para su uso las 10 últimas ips---* R1(config)#ip dhcp excluded-address 10.19.8.1 10.19.8.51 R1(config)#ip dhcp pool VLAN2 R1(config)#network 10.19.8.0 255.255.255.192 R1(config)#default-router 10.19.8.1 R1(config)#dns-server 10.19.8.51 R1(config)#domain-name ccna-a.net
Configurar DHCP IPv4 para VLAN 3	*---A continuación, se excluyen las primeras 18 ips dejando únicamente para su uso las 10 últimas ips---* R1(config)#ip dhcp excluded-address 10.19.8.65 10.19.8.83 R1(config)#ip dhcp pool VLAN3 R1(dhcp-config)#network 10.19.8.64 255.255.255.224 R1(config)#default-router 10.19.8.65 R1(config)#dns-server 10.19.8.83 R1(config)#domain-name ccna-b.net

Tabla 9:Configure R1

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**.

Configuración de red de PC-A	
Descripción	*ccna-a.net*
Dirección física	*000C.851A.9A47*
Dirección IP	*10.19.8.52*
Máscara de subred	*255.255.255.192*
Gateway predeterminado	*10.19.8.1*
Gateway predeterminado IPv6	*FE80::1*

Tabla 10: Configuración de red de PC-A

Configuración de red de PC-B	
Descripción	*ccna-b.net*
Dirección física	*00D0.BADA.933E*
Dirección IP	*10.19.8.84*
Máscara de subred	*255.255.255.224*
Gateway predeterminado	*10.19.8.65*
Gateway predeterminado IPv6	*FE80::1*

Tabla 11: Configuración de red de PC-B

Parte 3: Probar y verificar la conectividad de extremo a extremo

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

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

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

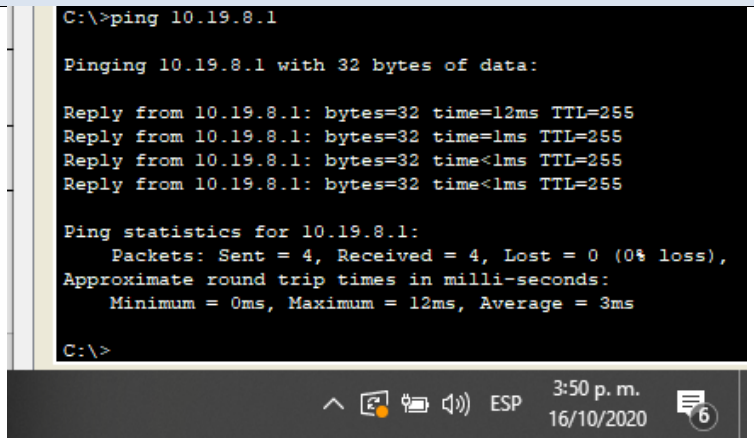
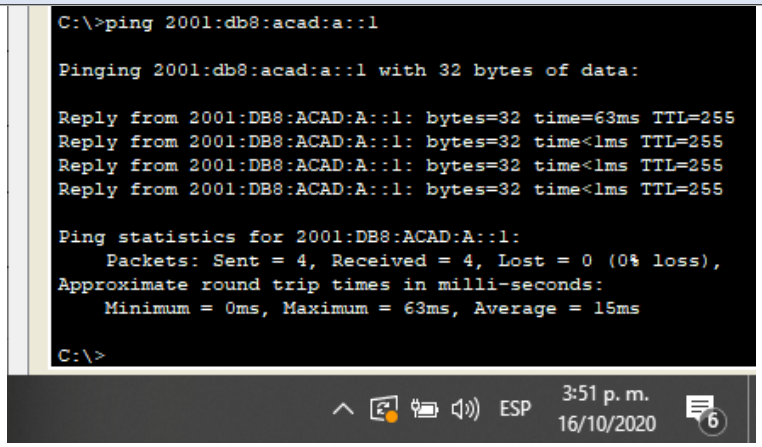
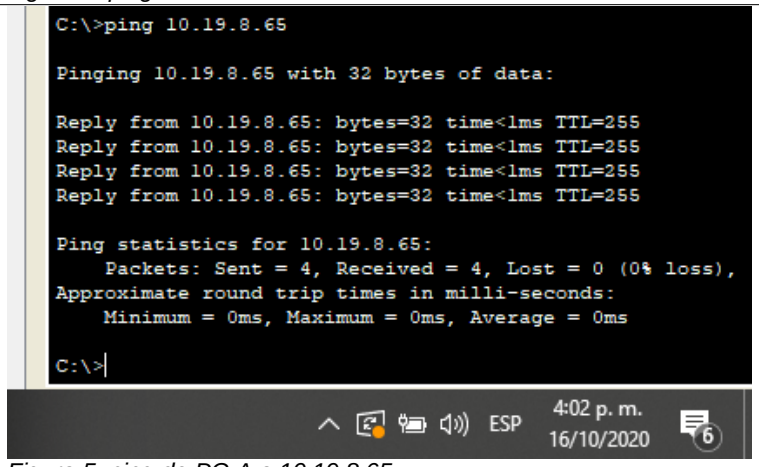
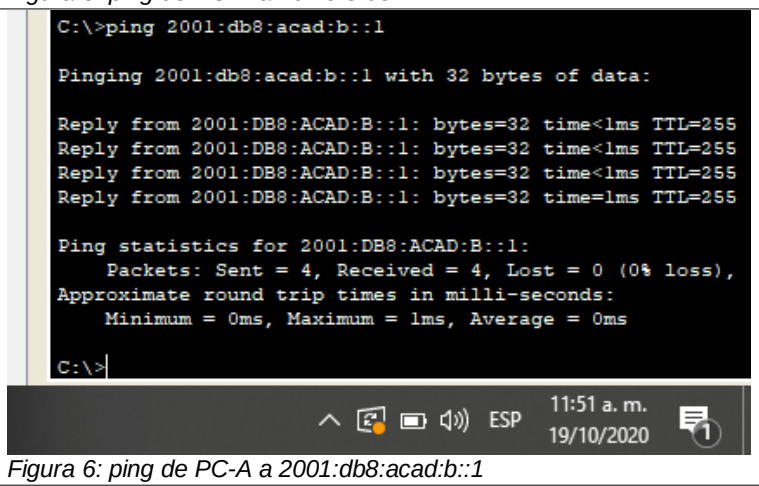
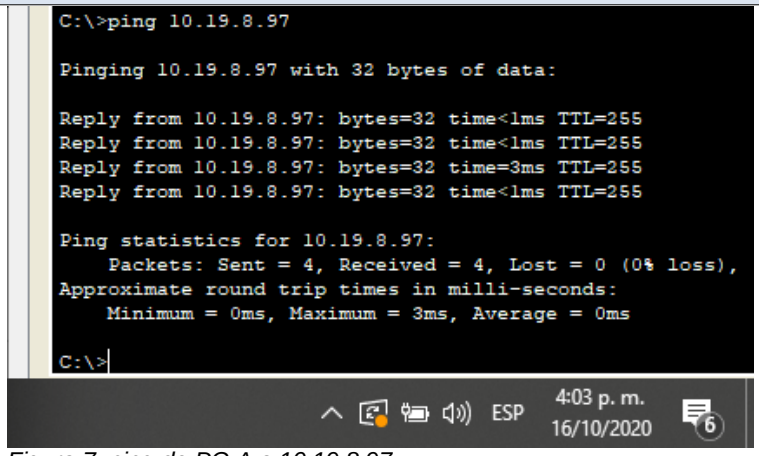
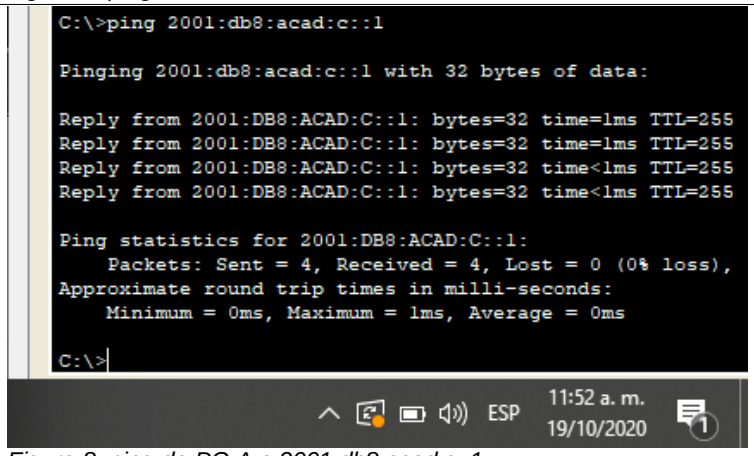
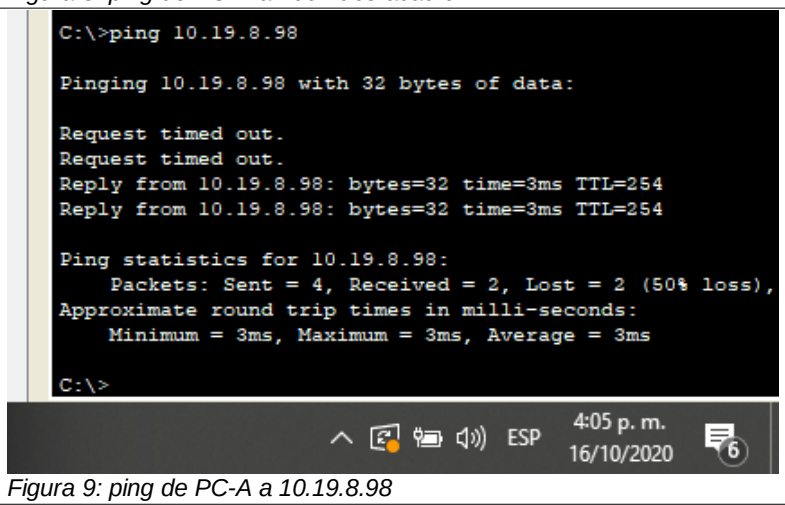
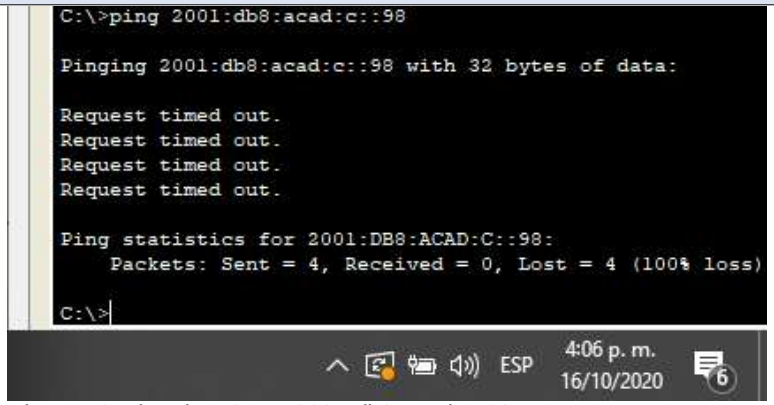
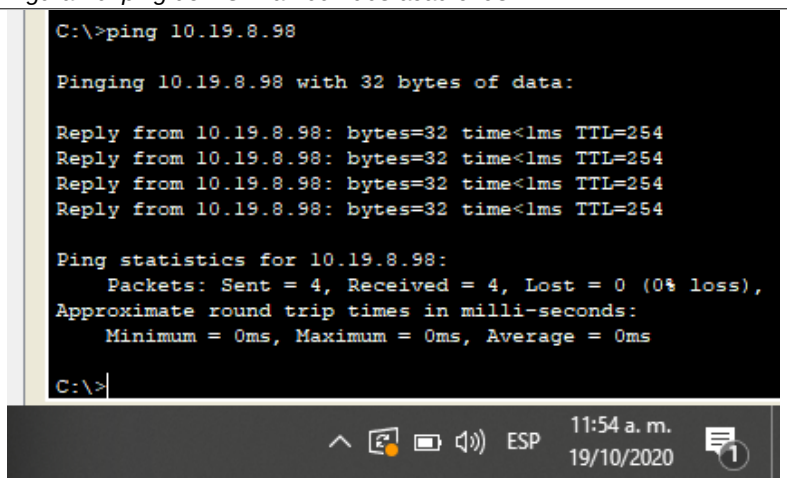
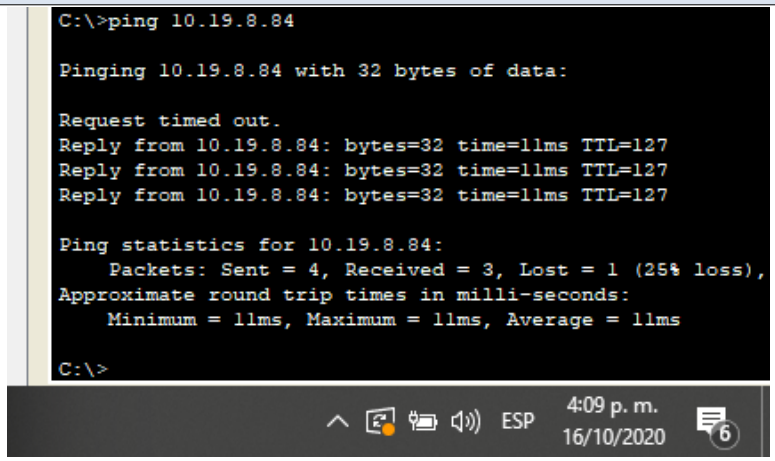
Desde	A	de Internet	Dirección IP	Resultados de ping
PC-A	R1, G0/0/1.2	Dirección	10.19.8.1	

Figura 3: ping de PC-A a 10.19.8.1

Desde	A	de Internet	Dirección IP	Resultados de ping
PC-A		IPv6	2001:db8:acad:a::1	 *Figura 4: ping de PC-A a 2001:db8:acad:a::1*
PC-A	R1, G0/0/1.3	Dirección	10.19.8.65	 *Figura 5: ping de PC-A a 10.19.8.65*
PC-A		IPv6	2001:db8:acad:b::1	 *Figura 6: ping de PC-A a 2001:db8:acad:b::1*

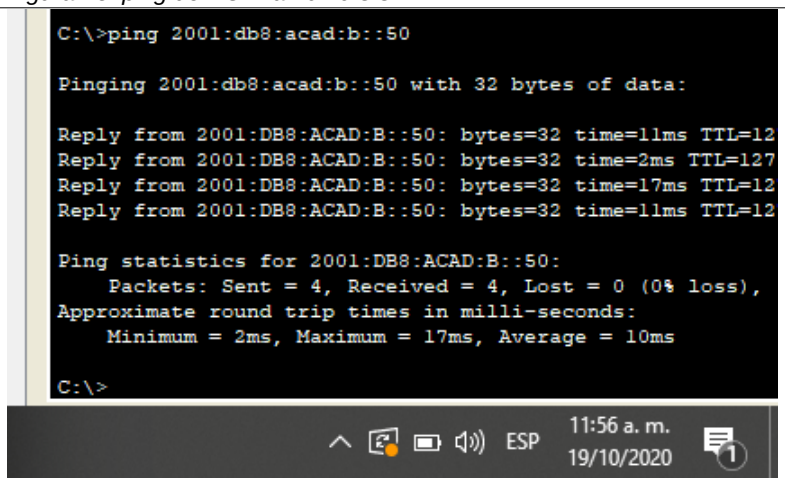
Desde	A	de Internet	Dirección IP	Resultados de ping
PC-A	R1, G0/0/1.4	Dirección	10.19.8.97	 *Figura 7: ping de PC-A a 10.19.8.97*
PC-A		IPv6	2001:db8:acad:c::1	 *Figura 8: ping de PC-A a 2001:db8:acad:c::1*
PC-A	S1, VLAN 4	Dirección	10.19.8.98	 *Figura 9: ping de PC-A a 10.19.8.98*

Desde	A	de Internet	Dirección IP	Resultados de ping
PC-A		IPv6	2001:db8:acad:c::98	 *Figura 10: ping de PC-A a 2001:db8:acad:c::98*
PC-A	S2, VLAN 4	Dirección	10.19.8.99	 *Figura 11: ping de PC-A a 10.19.8.99*
PC-A		IPv6	2001:db8:acad:c::99	 *Figura 12: ping de PC-A a 2001:db8:acad:c::99*

Desde	A	de Internet	Dirección IP	Resultados de ping
PC-A	PC-B	Dirección	IP address will vary.	

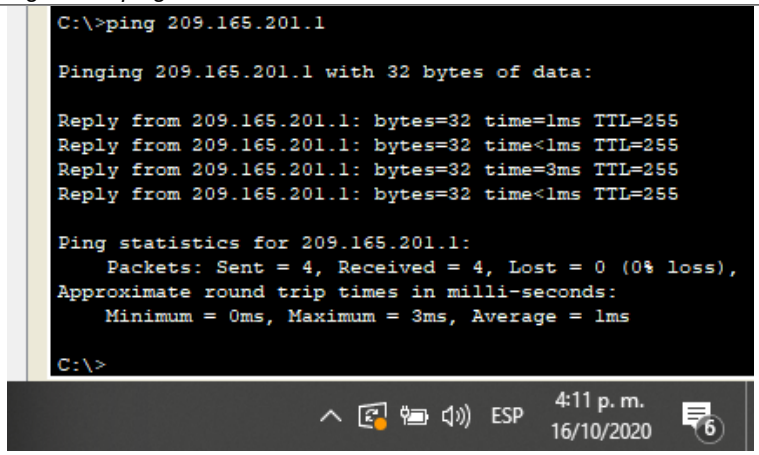
```
C:\>ping 10.19.8.84

Pinging 10.19.8.84 with 32 bytes of data:

Request timed out.
Reply from 10.19.8.84: bytes=32 time=11ms TTL=127
Reply from 10.19.8.84: bytes=32 time=11ms TTL=127
Reply from 10.19.8.84: bytes=32 time=11ms TTL=127

Ping statistics for 10.19.8.84:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 11ms, Maximum = 11ms, Average = 11ms

C:\>
```


Figura 13: ping de PC-A a 10.19.8.84

PC-A		IPv6	2001:db8:acad:b::50	

```
C:\>ping 2001:db8:acad:b::50

Pinging 2001:db8:acad:b::50 with 32 bytes of data:

Reply from 2001:DB8:ACAD:B::50: bytes=32 time=11ms TTL=12
Reply from 2001:DB8:ACAD:B::50: bytes=32 time=2ms TTL=127
Reply from 2001:DB8:ACAD:B::50: bytes=32 time=17ms TTL=12
Reply from 2001:DB8:ACAD:B::50: bytes=32 time=11ms TTL=12

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 = 2ms, Maximum = 17ms, Average = 10ms

C:\>
```


Figura 14: ping de PC-A a 2001:db8:acad:b::50

PC-A	R1 Bucle 0	Dirección	209.165.201.1	

```
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=3ms 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 = 3ms, Average = 1ms

C:\>
```


Figura 15: ping de PC-A a 209.165.201.1

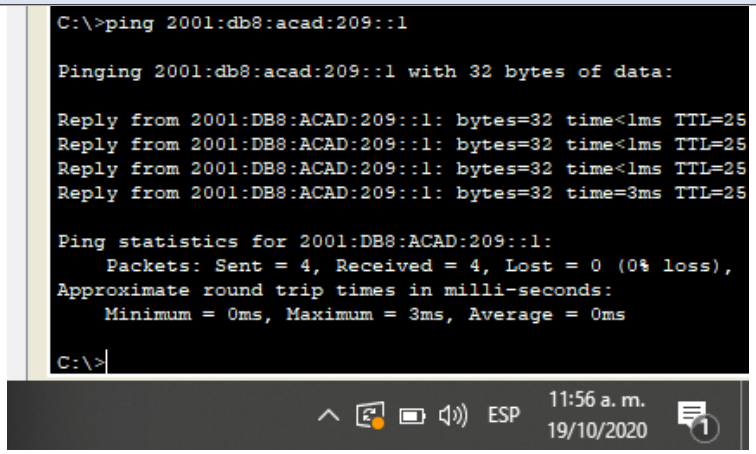
<table>
<tr><th>Desde</th><th>A</th><th>de Internet</th><th>Dirección IP</th><th>Resultados de ping</th></tr>
<tr><td>PC-A</td><td></td><td>IPv6</td><td>2001:db8:acad:209::1</td><td> 

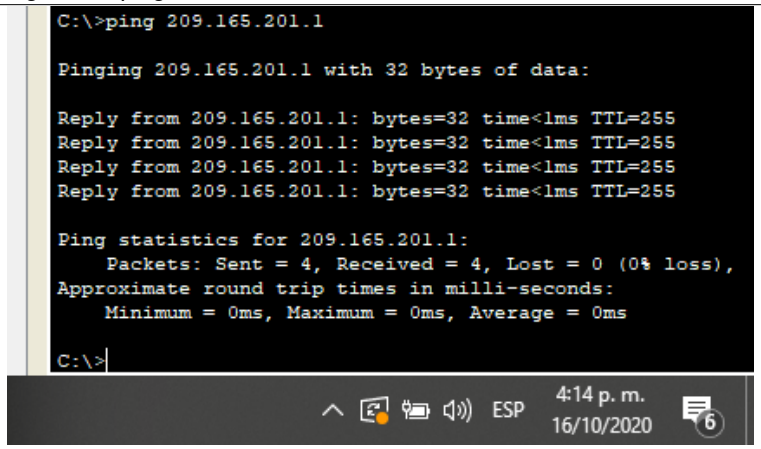
Figura 16: ping de PC-A a 2001:db8:acad:209::1</td></tr>
<tr><td rowspan="2">PC-B</td><td rowspan="2">R1 Bucle 0</td><td>Dirección</td><td>209.165.201.1</td><td> 

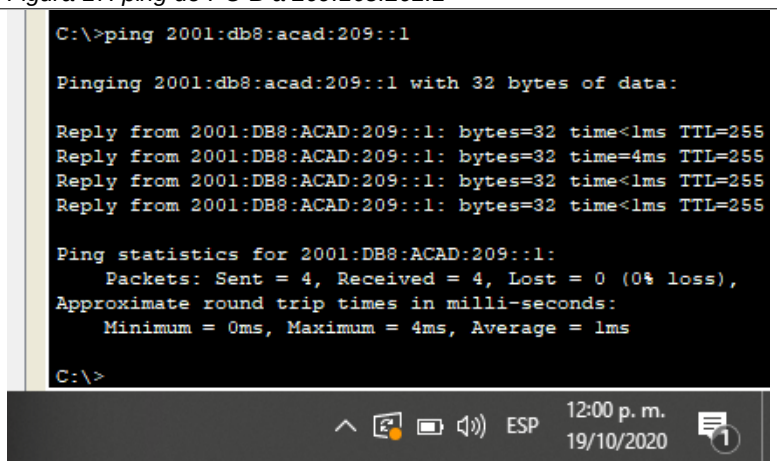
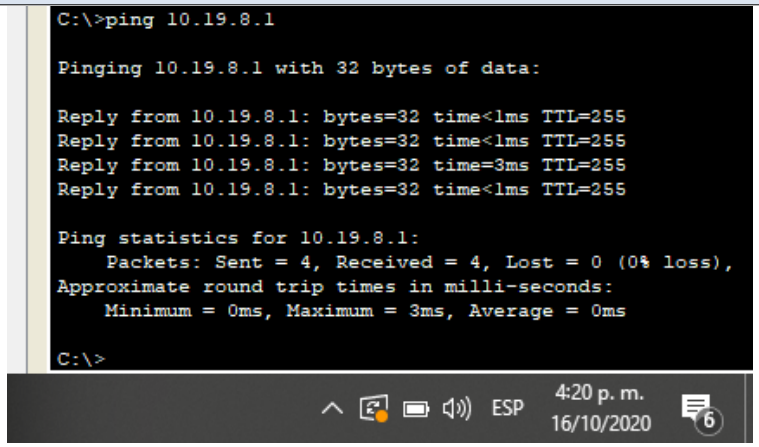
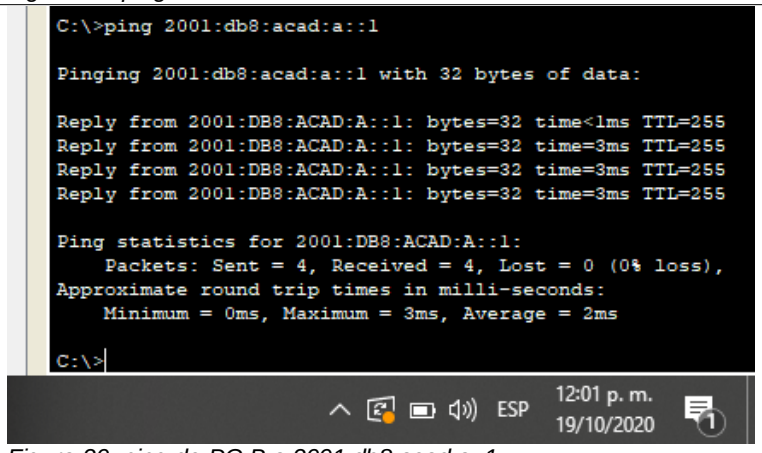
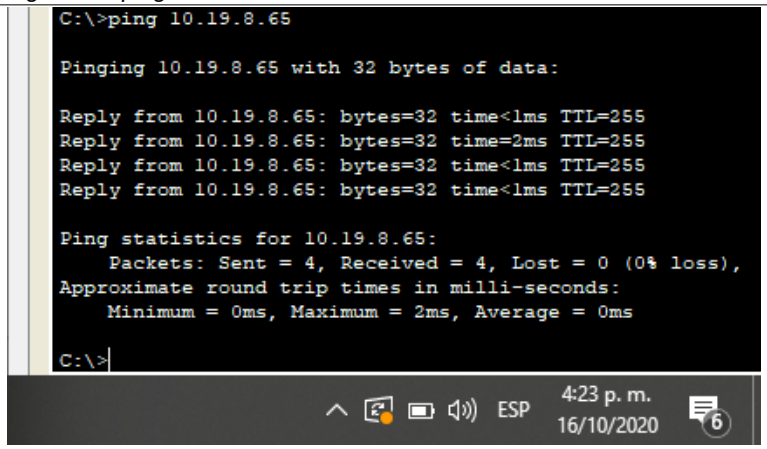
Figura 17: ping de PC-B a 209.165.201.1</td></tr>
<tr><td>IPv6</td><td>2001:db8:acad:209::1</td><td> 

Figura 18: ping de PC-B a 2001:db8:acad:209::1</td></tr>
</table>

Desde	A	de Internet	Dirección IP	Resultados de ping
PC-B	R1, G0/0/1.2	Dirección	10.19.8.1	 *Figura 19: ping de PC-B a 10.19.8.1*
PC-B		IPv6	2001:db8:acad:a::1	 *Figura 20: ping de PC-B a 2001:db8:acad:a::1*
PC-B	R1, G0/0/1.3	Dirección	10.19.8.65	 *Figura 21: ping de PC-B a 10.19.8.65*

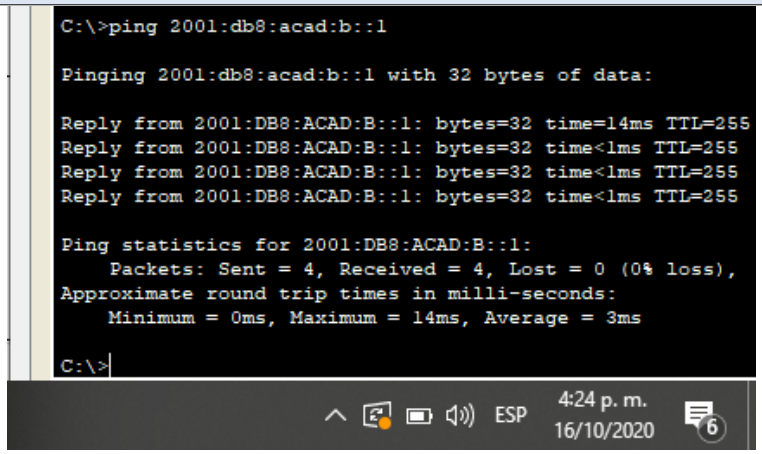
<table>
<tr><th>Desde</th><th>A</th><th>de Internet</th><th>Dirección IP</th><th>Resultados de ping</th></tr>
<tr><td rowspan="3">PC-B</td><td rowspan="3">R1, G0/0/1.4</td><td>IPv6</td><td>2001:db8:acad:b::1</td><td> 

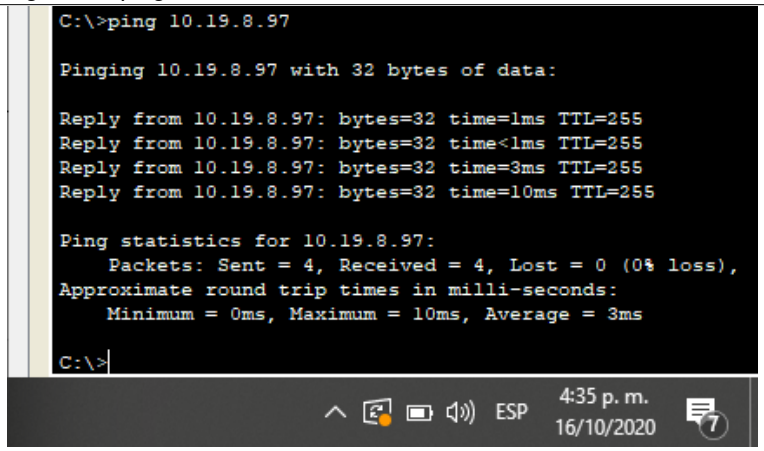
Figura 22: ping de PC-B a 2001:db8:acad:b::1</td></tr>
<tr><td>Dirección</td><td>10.19.8.97</td><td> 

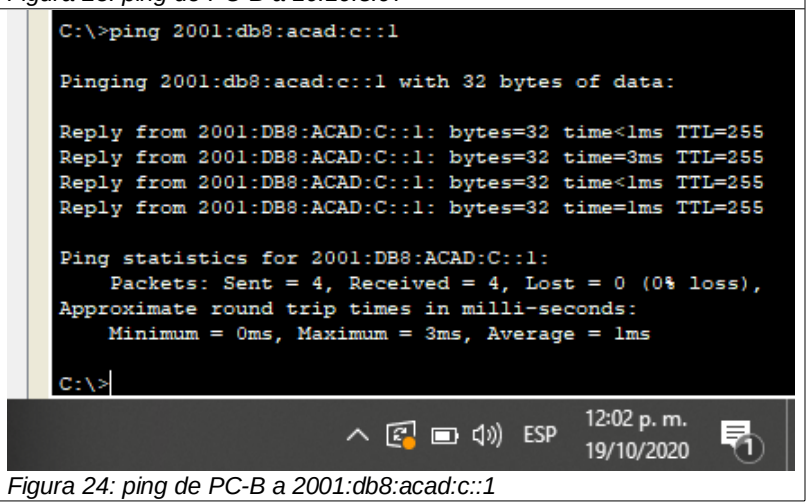
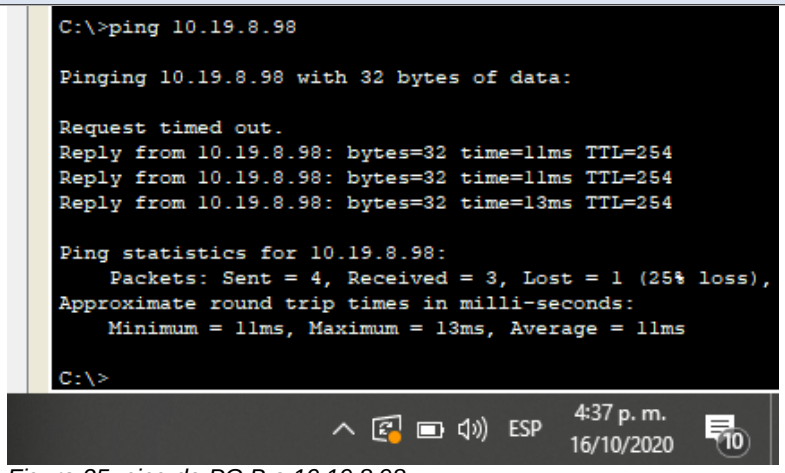
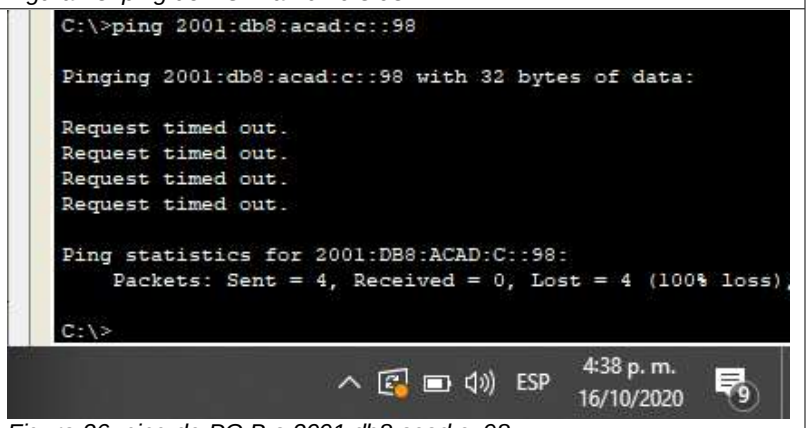
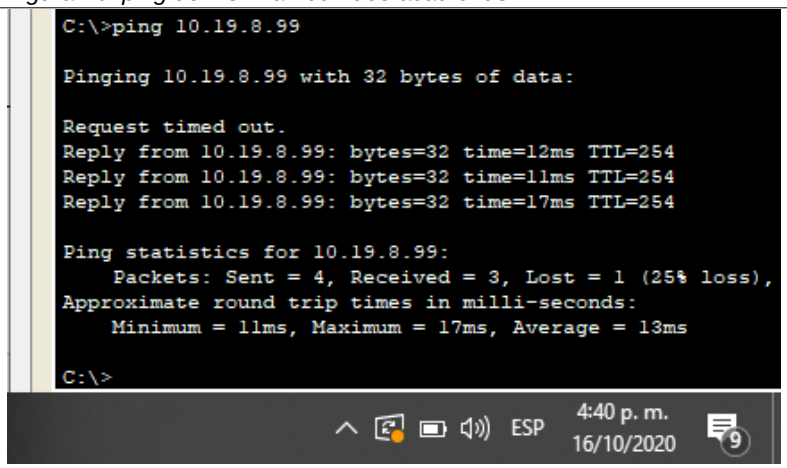
Figura 23: ping de PC-B a 10.19.8.97</td></tr>
<tr><td>IPv6</td><td>2001:db8:acad:c::1</td><td> 

Figura 24: ping de PC-B a 2001:db8:acad:c::1</td></tr>
</table>

Desde	A	de Internet	Dirección IP	Resultados de ping
PC-B	S1, VLAN 4	Dirección	10.19.8.98	 *Figura 25: ping de PC-B a 10.19.8.98*
PC-B	S1, VLAN 4	IPv6	2001:db8:acad:c::98	 *Figura 26: ping de PC-B a 2001:db8:acad:c::98*
PC-B	S2, VLAN 4	Dirección	10.19.8.99	 *Figura 27: ping de PC-B a 10.19.8.99*

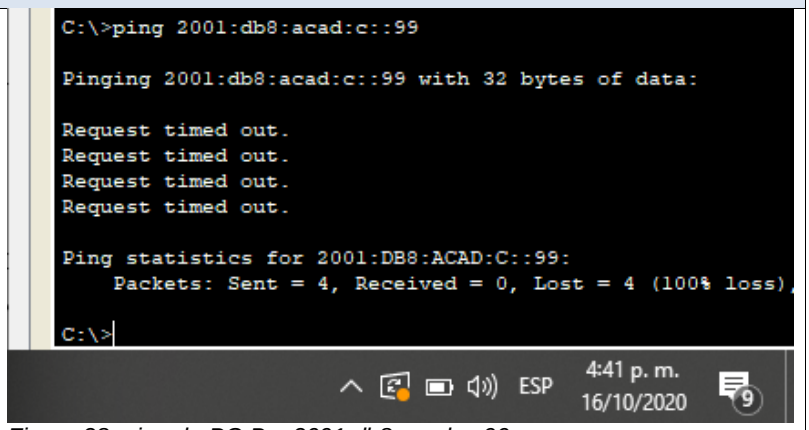
Desde	A	de Internet	Dirección IP	Resultados de ping
PC-B		IPv6	2001:db8:acad:c::99	

Figura 28: ping de PC-B a 2001:db8:acad:c::99

Tabla 12: Configuración general

Escenario 2

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

Topología

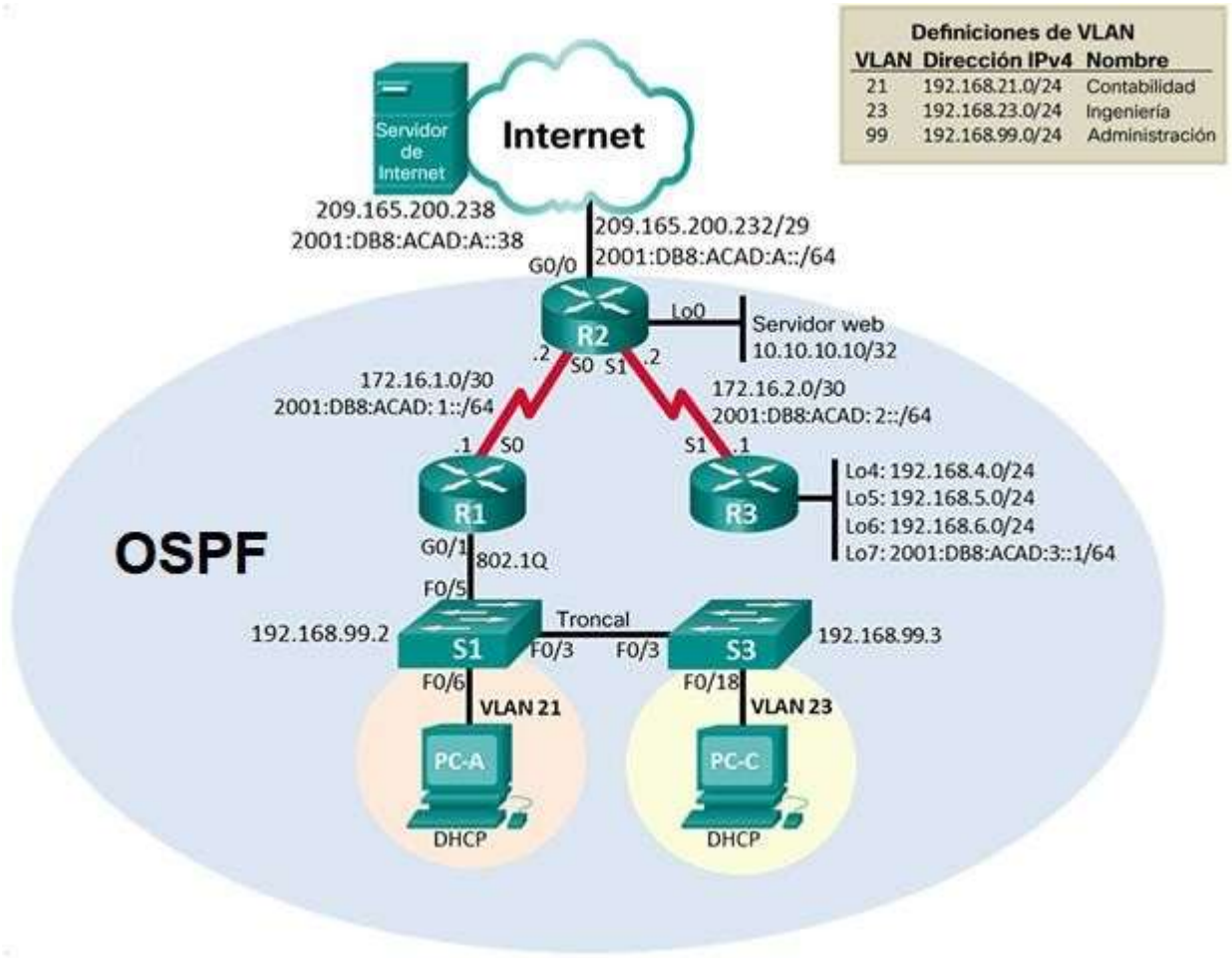


Figura 29: Topología original escenario 2

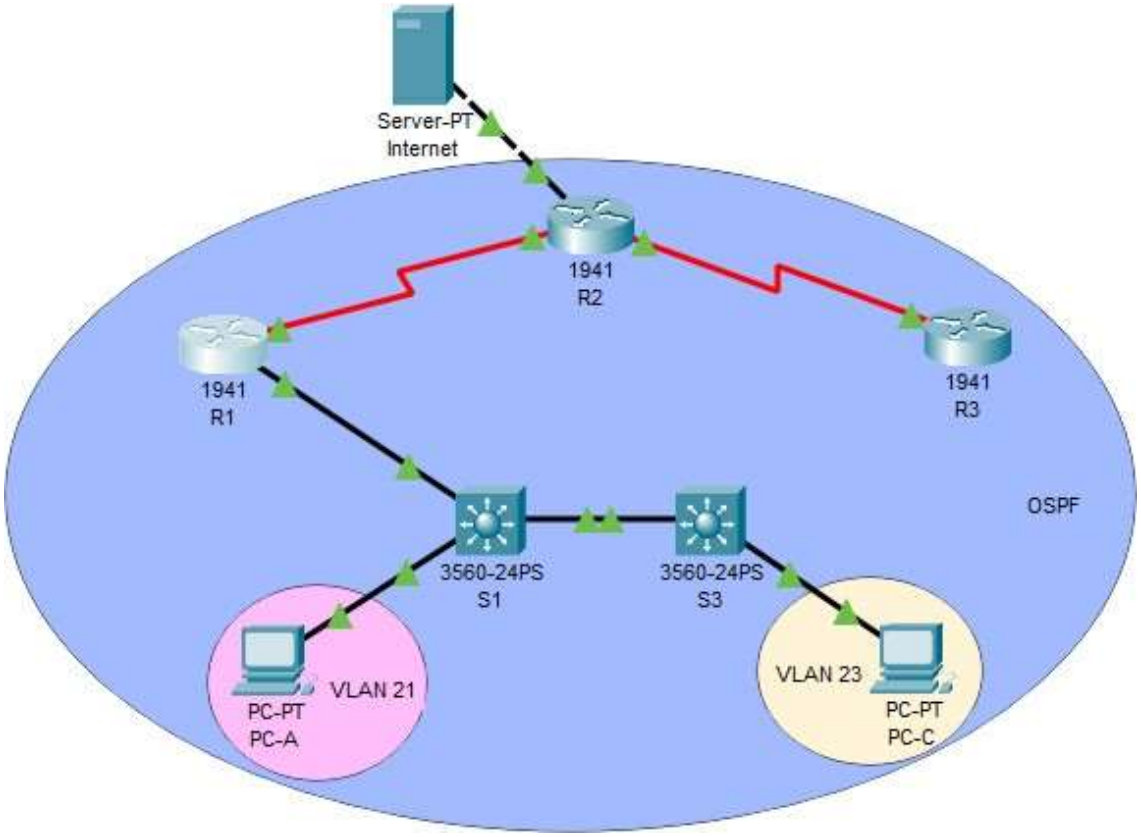


Figura 30: Topología Packet Tracer Escenario 2

Parte 1: Inicializar dispositivos

Paso 1: Inicializar y volver a cargar los routers y los switches

Elimine las configuraciones de inicio y vuelva a cargar los dispositivos. Antes de continuar, solicite al instructor que verifique la inicialización de los dispositivos.

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	Router#erase startup-config /Se realiza esta operación en los tres Router/
Volver a cargar todos los routers	Router#reload /Se realiza esta operación en los tres Router/
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Switch#erase startup-config Switch#del vlan.dat /Se realiza esta operación en los tres Switch/

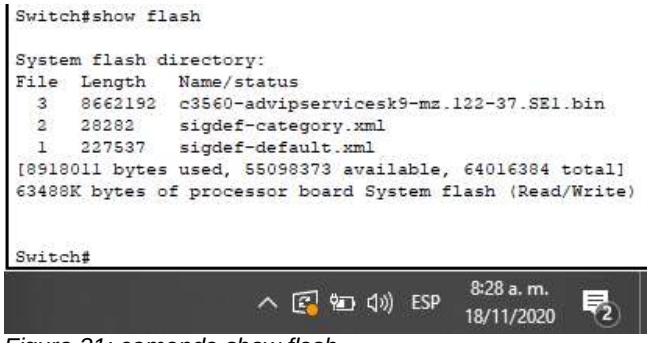
Volver a cargar ambos switches	Switch#reload /Se realiza esta operación en los tres Switch/
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Switch#show flash /Vemos la información guardada en la memoria flash/  *Figura 31: comando show flash*

Tabla 13: Inicializar Router y Switch

Parte 2: Configurar los parámetros básicos de los dispositivos

Paso 1: Configurar la computadora de Internet

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

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::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:2::1

Tabla 14: Conf. computadora de internet

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

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router>enable Router#config t Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R1
Contraseña de exec privilegiado cifrada	R1(config)#enable secret class
Contraseña de acceso a la consola	R1(config)#line console 0 R1(config-line)#password cisco R1(config-line)#login
Contraseña de acceso Telnet	R1(config)#line vty 0 4 R1(config-line)#password cisco R1(config-line)#login
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Mensaje MOTD	R1(config)#banner motd "Se prohibe el acceso no autorizado”
Interfaz S0/0/0	R1(config)#interface serial 0/0/0 R1(config-if)#description CONECTAR2 R1(config-if)#ip address 172.16.1.1 255.255.255.252 R1(config-if)#ipv6 address 2001:db8:acad:1::1/64 R1(config-if)#clock rate 128000 R1(config-if)#no shutdown 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	R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0 R1(config)#ipv6 route ::/0 s0/0/0 R1(config)#copy run start Configurar una ruta IPv4 predeterminada de S0/0/0 Configurar una ruta IPv6 predeterminada de S0/0/0

Tabla 15: Configurar R1 básico

Nota: Todavía no configure G0/1.

Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router>enable Router#config t Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R2
Contraseña de exec privilegiado cifrada	R2(config)#enable secret class
Contraseña de acceso a la consola	R2(config)#line console 0 R2(config-line)#password cisco R2(config-line)#login
Contraseña de acceso Telnet	R2(config)#line vty 0 4 R2(config-line)#password cisco R2(config-line)#login
Cifrar las contraseñas de texto no cifrado	R2(config)#service password-encryption
Habilitar el servidor HTTP	R2(config)#ip http server /Este commando no funciona en PT por lo tanto no se usará/
Mensaje MOTD	R2(config)#banner motd "Se prohibe el acceso no autorizado”

Interfaz S0/0/0	R2(config)#interface serial 0/0/0 R2(config-if)#description CONECTAR1 R2(config-if)#ip address 172.16.1.2 255.255.255.252 R2(config-if)#ipv6 address 2001:db8:acad:1::2/64 R2(config-if)#no shutdown 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	R2(config)#interface serial 0/0/1 R2(config-if)#description CONECTAR3 R2(config-if)#ip address 172.16.2.2 255.255.255.252 R2(config-if)#ipv6 address 2001:db8:acad:2::2/64 R2(config-if)#clock rate 128000 R2(config-if)#no shutdown 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)	R2(config)#interface g0/0 R2(config-if)#description INTERNET R2(config-if)#ip address 209.165.200.233 255.255.255.248 R2(config-if)#ipv6 address 2001:db8:acad:A::1/64 R2(config-if)#no shutdown 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)	R2(config)#interface loopback 0 R2(config-if)#description SERVIDORWEB R2(config-if)#ip address 10.10.10.10 255.255.255.255 Establecer la descripción. Establezca la dirección IPv4.
Ruta predeterminada	R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0 R2(config)#ipv6 route ::/0 g0/0 R2(config)#copy run start Configure una ruta IPv4 predeterminada de G0/0. Configure una ruta IPv6 predeterminada de G0/0.

Tabla 16: Configurar R2 básico

Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router>enable Router#config t Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R3
Contraseña de exec privilegiado cifrada	R3(config)#enable secret class

Contraseña de acceso a la consola	R3(config)#line console 0 R3(config-line)#password cisco R3(config-line)#login
Contraseña de acceso Telnet	R3(config)#line vty 0 4 R3(config-line)#password cisco R3(config-line)#login
Cifrar las contraseñas de texto no cifrado	R3(config)#service password-encryption
Mensaje MOTD	R3(config)#banner motd "Se prohibe el acceso no autorizado”
Interfaz S0/0/1	R3(config)#interface serial 0/0/1 R3(config-if)#description CONECTAR2 R3(config-if)#ip address 172.16.2.1 255.255.255.252 R3(config-if)#ipv6 address 2001:db8:acad:2::1/64 R3(config-if)#no shutdown 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	R3(config)#interface loopback 4 R3(config-if)#ip address 192.168.4.1 255.255.255.0 R3(config-if)#no shutdown Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.
Interfaz loopback 5	R3(config)#interface loopback 5 R3(config-if)#ip address 192.168.5.1 255.255.255.0 R3(config-if)#no shutdown Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.

Interfaz loopback 6	R3(config)#interface loopback 6 R3(config-if)#ip address 192.168.6.1 255.255.255.0 R3(config-if)#no shutdown Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.
Interfaz loopback 7	R3(config)#interface loopback 7 R3(config-if)#ipv6 address 2001:db8:acad:3::1/64 R3(config-if)#no shutdown R1(config-if)#end R1#copy run start Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.
Rutas predeterminadas	

Tabla 17: Configurar R3 básico

Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch>enable Switch#config t Switch(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S1
Contraseña de exec privilegiado cifrada	S1(config)#enable secret class
Contraseña de acceso a la consola	S1(config)#line console 0 S1(config-line)#password cisco S1(config-line)#login
Contraseña de acceso Telnet	S1(config)#line vty 0 4 S1(config-line)#password cisco S1(config-line)#login
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption
Mensaje MOTD	S1(config)#banner motd "Se prohibe el acceso no autorizado”

Tabla 18: Configurar S1 básico

Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch>enable Switch#config t Switch(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S3
Contraseña de exec privilegiado cifrada	S3(config)#enable secret class
Contraseña de acceso a la consola	S3(config)#line console 0 S3(config-line)#password cisco S3(config-line)#login
Contraseña de acceso Telnet	S3(config)#line vty 0 4 S3(config-line)#password cisco S3(config-line)#login
Cifrar las contraseñas de texto no cifrado	S3(config)#service password-encryption
Mensaje MOTD	S3(config)#banner motd "Se prohibe el acceso no autorizado”

Tabla 19: Configurar S3 básico

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:

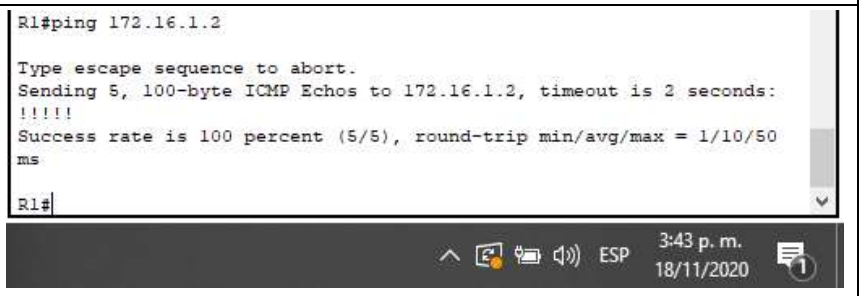
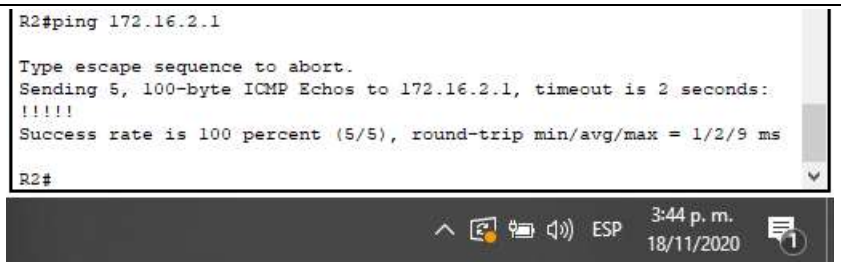
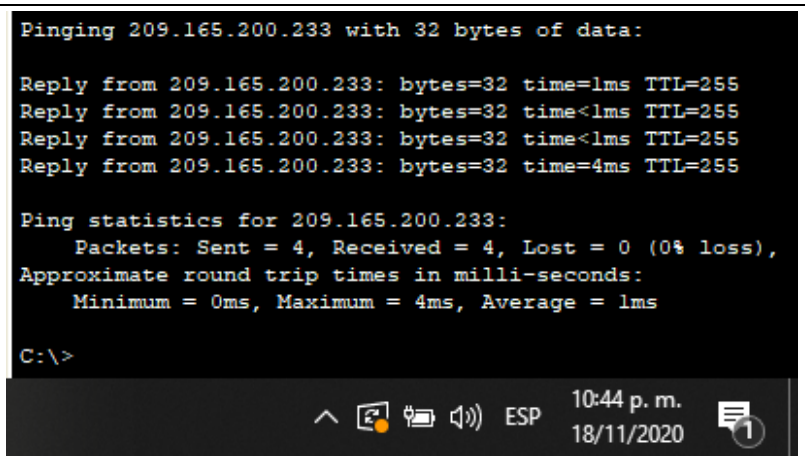
Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	 *Figura 32: Ping de R1 a 172.16.1.2*
R2	R3, S0/0/1	172.16.2.1	 *Figura 33: Ping de R2 a 172.16.2.1*
PC de Internet	Gateway predeterminado	200.165.200.233	 *Figura 34: Ping de PC de internet a 200.165.200.233*

Tabla 20: Verificar conectividad

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

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

Paso 1: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	S1(config)#vlan 21 S1(config-if)#name CONTABILIDAD S1(config-if)#exit S1(config)#vlan 23 S1(config-if)#name INGENIERIA S1(config-if)#exit S1(config)#vlan 99 S1(config-if)#name ADMINISTRACION S1(config-if)#exit 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.	S1(config)#interface vlan 99 S1(config-if)#ip address 192.168.99.2 255.255.255.0 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	S1(config-if)#ip default-gateway 192.168.99.1 Asigne la primera dirección IPv4 de la subred como el gateway predeterminado.
Forzar el enlace troncal en la interfaz F0/3	S1(config)#interface fastEthernet 0/3 S1(config-if)#switchport trunk encapsulation dot1Q S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1 S1(config-if)#no shutdown Utilizar la red VLAN 1 como VLAN nativa

Forzar el enlace troncal en la interfaz F0/5	S1(config)#interface fastEthernet 0/5 S1(config-if)#switchport trunk encapsulation dot1Q S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1 S1(config-if)#no shutdown Utilizar la red VLAN 1 como VLAN nativa
Configurar el resto de los puertos como puertos de acceso	S1(config)#interface range f0/1-2, f0/4, f0/6-24 S1(config-if-range)#switchport mode access S1(config-if-range)#exit Utilizar el comando interface range
Asignar F0/6 a la VLAN 21	S1(config)#interface fastEthernet 0/6 S1(config-if)#switchport access vlan 21 S1(config-if)#no shutdown
Apagar todos los puertos sin usar	S1(config)#interface range f0/1-2, f0/4, f0/7-24 S1(config-if-range)#shutdown S1(config-if-range)#end S1#copy run start

Tabla 21: Seguridad y vlan S1

Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	S3(config)#vlan 21 S3(config-if)#name CONTABILIDAD S3(config-if)#exit S3(config)#vlan 23 S3(config-if)#name INGENIERIA S3(config-if)#exit S3(config)#vlan 99 S3(config-if)#name ADMINISTRACION S3(config-if)#exit 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	S3(config)#interface vlan 99 S3(config-if)#ip address 192.168.99.3 255.255.255.0 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.	S3(config-if)#ip default-gateway 192.168.99.1 Asignar la primera dirección IP en la subred como gateway predeterminado.
Forzar el enlace troncal en la interfaz F0/3	S3(config)#interface fastEthernet 0/3 S3(config-if)#switchport trunk encapsulation dot1Q S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1 S3(config-if)#no shutdown Utilizar la red VLAN 1 como VLAN nativa
Configurar el resto de los puertos como puertos de acceso	S3(config)#interface range f0/1-2, f0/4-24 S3(config-if-range)#switchport mode access S3(config-if-range)#exit Utilizar el comando interface range
Asignar F0/18 a la VLAN 23	S3(config)#interface fastEthernet 0/18 S3(config-if)#switchport access vlan 23 S3(config-if)#no shutdown
Apagar todos los puertos sin usar	S3(config)#interface range f0/1-2, f0/4-17, f0/19-24 S3(config-if-range)#shutdown S3(config-if-range)#end S3#copy run start

Tabla 22: Seguridad y vlan S3

Paso 3: Configurar R1

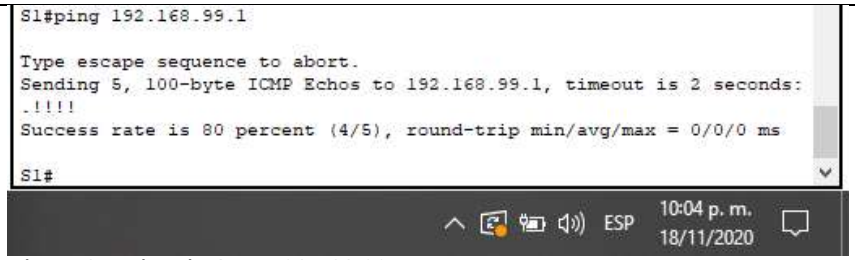
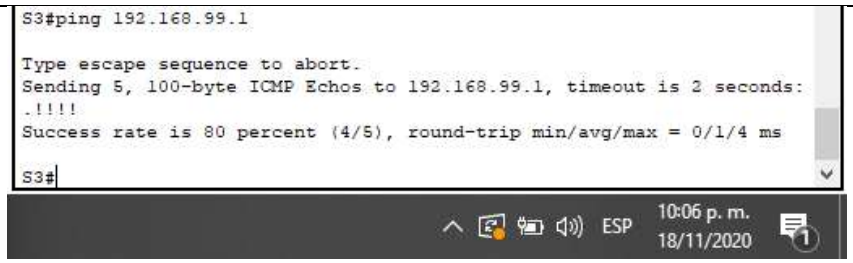
Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	R1(config)#interface gigabitEthernet 0/1.21 R1(config-subif)#encapsulation dot1Q 21 R1(config-subif)#description LAN de Contabilidad R1(config-subif)#ip address 192.168.21.1 255.255.255.0 R1(config-subif)#exit 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	R1(config)#interface gigabitEthernet 0/1.23 R1(config-subif)#encapsulation dot1Q 23 R1(config-subif)#description LAN de Ingenieria R1(config-subif)#ip address 192.168.23.1 255.255.255.0 R1(config-subif)#exit 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	R1(config)#interface gigabitEthernet 0/1.99 R1(config-subif)#encapsulation dot1Q 99 R1(config-subif)#description LAN de Administración R1(config-subif)#ip address 192.168.99.1 255.255.255.0 R1(config-subif)#exit Descripción: LAN de Administración Asignar la VLAN 99 Asignar la primera dirección disponible a esta interfaz
Activar la interfaz G0/1	R1(config)#interface gigabitEthernet 0/1 R1(config-if)#no shutdown R1(config-if)#end R1#copy run start

Tabla 23: Seguridad y vlan R1

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:

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	 *Figura 35: Ping de S1 a 192.168.99.1*
S3	R1, dirección VLAN 99	192.168.99.1	 *Figura 36: Ping de S3 a 192.168.99.1*

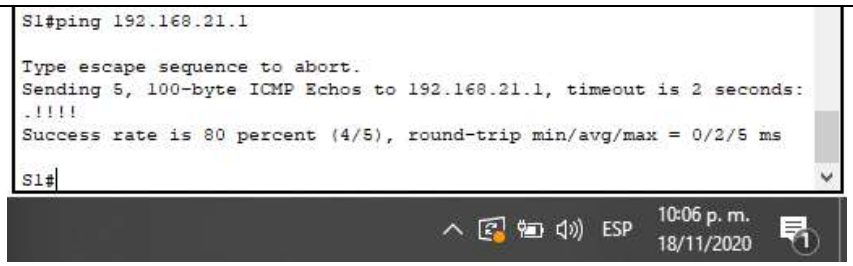
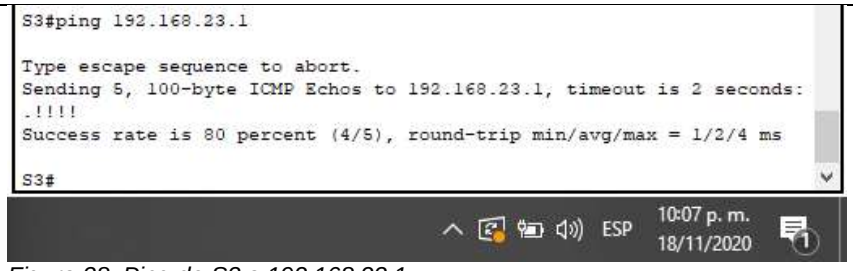
S1	R1, dirección VLAN 21	192.168.21.1	 *Figura 37: Ping de S1 a 192.168.21.1*
S3	R1, dirección VLAN 23	192.168.23.1	 *Figura 38: Ping de S3 a 192.168.23.1*

Tabla 24: Verificar conectividad

Parte 4: Configurar el protocolo de routing dinámico OSPF

Paso 1: Configurar OSPF en el R1

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R1(config)#router ospf 1 R1(config-router)#router-id 1.1.1.1
Anunciar las redes conectadas directamente	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 Asigne todas las redes conectadas directamente.
Establecer todas las interfaces LAN como pasivas	R1(config-router)#passive-interface gigabitEthernet 0/1

Desactive la sumarización automática	R1(config-router)#no auto-summary /Dado que OSPF no sumariza automáticamente, no necesita el comando “no auto-summary”/

Tabla 25: OSPF en R1

Paso 2: Configurar OSPF en el R2

La configuración del R2 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R2(config)#router ospf 1 R2(config-router)#router-id 2.2.2.2
Anunciar las redes conectadas directamente	R2(config-router)#network 172.16.1.0 0.0.0.3 area 0 R2(config-router)#network 172.16.2.0 0.0.0.3 area 0 R2(config-router)#network 10.10.10.10 0.0.0.0 area 0 **Nota:** Omitir la red G0/0.
Establecer la interfaz LAN (loopback) como pasiva	R2(config-router)#passive-interface loopback 0
Desactive la sumarización automática.	R2(config-router)#no auto-summary /Dado que OSPF no sumariza automáticamente, no necesita el comando “no auto-summary”/

Tabla 26: OSPF en R2

Paso 3: Configurar OSPFv3 en el R3

La configuración del R3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Configurar OSPFv3 área 0	R3(config)#ipv6 unicast-routing R3(config)#ipv6 router ospf 1 R3(config-rtr)#router-id 33.33.33.33 R3(config-rtr)#passive-interface default R3(config-rtr)#no passive-interface s0/0/1 R3(config-rtr)#exit R3(config)#interface s0/0/1 R3(config-if)#ipv6 ospf 1 area 0 R3(config)#interface loopback 7 R3(config-if)#ipv6 ospf 1 area 0 R3(config-if)#exit
Configurar OSPF área 0	R3(config)#router ospf 1 R3(config-router)#router-id 3.3.3.3

Anunciar redes IPv4 conectadas directamente	R3(config-router)#network 172.16.2.0 0.0.0.3 area 0 R3(config-router)#network 192.168.4.0 0.0.0.255 area 0 R3(config-router)#network 192.168.5.0 0.0.0.255 area 0 R3(config-router)#network 192.168.6.0 0.0.0.255 area 0
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	R3(config-router)#passive-interface loopback 4 R3(config-router)#passive-interface loopback 5 R3(config-router)#passive-interface loopback 6
Desactive la sumarización automática.	R3(config-router)#no auto-summary /Dado que OSPF no sumariza automáticamente, no necesita el comando “no auto-summary”/

Tabla 27: OSPFv3 en R3

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:

Pregunta	Respuesta
¿Con qué comando se muestran la ID del proceso OSPF, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router?	show ip protocols show ip ospf interface /Las capturas de pantalla de la ejecución de estos comandos show se encuentran debajo de la tabla 28/
¿Qué comando muestra solo las rutas OSPF?	show ip route ospf /Se relaciona la captura de pantalla debajo de la table 28/
¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	show run | section ospf /Se relaciona la captura de pantalla debajo de la tabla 28/

Tabla 28: Verificar información OSPF

```
R1#show ip protocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 1.1.1.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.21.0 0.0.0.255 area 0
    192.168.23.0 0.0.0.255 area 0
    192.168.99.0 0.0.0.255 area 0
    172.16.1.0 0.0.0.3 area 0
  Passive Interface(s):
    GigabitEthernet0/1
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1              110      00:09:52
    2.2.2.2              110      00:09:53
    3.3.3.3              110      00:09:53
  Distance: (default is 110)

R1#
```

Figura 39: Comando show ip protocols

```
R1#show ip ospf interface

GigabitEthernet0/1.21 is up, line protocol is up
  Internet address is 192.168.21.1/24, Area 0
  Process ID 1, Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 1.1.1.1, Interface address 192.168.21.1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit
5
    Hello due in 00:00:02
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
GigabitEthernet0/1.23 is up, line protocol is up
  Internet address is 192.168.23.1/24, Area 0
  Process ID 1, Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 1.1.1.1, Interface address 192.168.23.1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit
```

Figura 40: Parte del comando show ip ospf interface

```
R1#show ip route ospf
     10.0.0.0/32 is subnetted, 1 subnets
O       10.10.10.10 [110/65] via 172.16.1.2, 09:23:29, Serial0/0/0
     172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
O       172.16.2.0 [110/128] via 172.16.1.2, 09:23:29, Serial0/0/0
     192.168.4.0/32 is subnetted, 1 subnets
O       192.168.4.1 [110/129] via 172.16.1.2, 09:23:19, Serial0/0/0
     192.168.5.0/32 is subnetted, 1 subnets
O       192.168.5.1 [110/129] via 172.16.1.2, 09:23:19, Serial0/0/0
     192.168.6.0/32 is subnetted, 1 subnets
O       192.168.6.1 [110/129] via 172.16.1.2, 09:23:19, Serial0/0/0

R1#
```


Figura 41: Comando show ip route ospf

```
R1#show run | section ospf
router ospf 1
 router-id 1.1.1.1
 log-adjacency-changes
 passive-interface GigabitEthernet0/1
 network 192.168.21.0 0.0.0.255 area 0
 network 192.168.23.0 0.0.0.255 area 0
 network 192.168.99.0 0.0.0.255 area 0
 network 172.16.1.0 0.0.0.3 area 0
R1#
```

Figura 42: Comando show run | section ospf

Paso 5: Implementar DHCP y NAT para IPv4

a. Configurar el R1 como servidor de DHCP para las VLAN 21 y 23

Las tareas de configuración para R1 incluyen las siguientes:

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(config)#ip dhcp pool ACCT R1(dhcp-config)#network 192.168.21.0 255.255.255.0 R1(dhcp-config)#default-router 192.168.21.1 R1(dhcp-config)#dns-server 10.10.10.10 R1(config)#domain-name ccna-sa.com 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	R1(config)#ip dhcp pool ENGNR R1(dhcp-config)#network 192.168.23.0 255.255.255.0 R1(dhcp-config)#default-router 192.168.23.1 R1(dhcp-config)#dns-server 10.10.10.10 R1(config)#domain-name ccna-sa.com Nombre: ENGNR Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado

Tabla 29: R1 como DHCP

b. Configurar la NAT estática y dinámica en el R2

La configuración del R2 incluye las siguientes tareas:

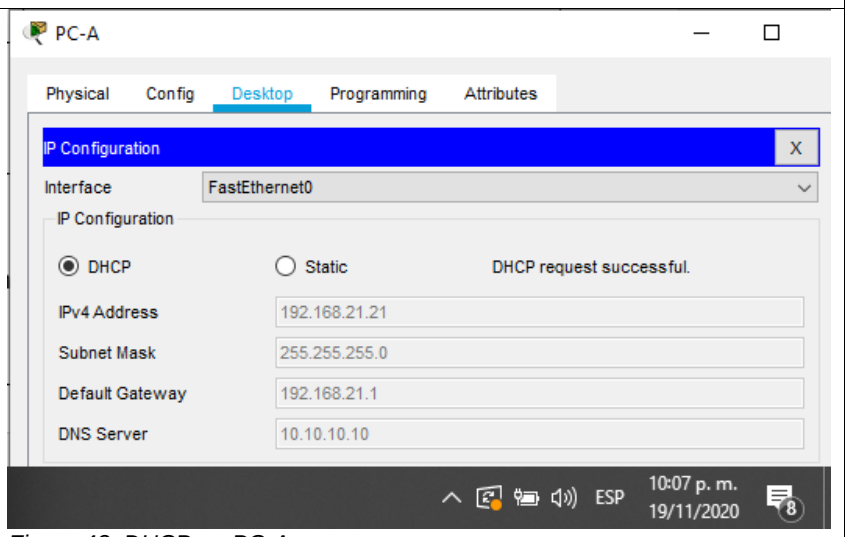
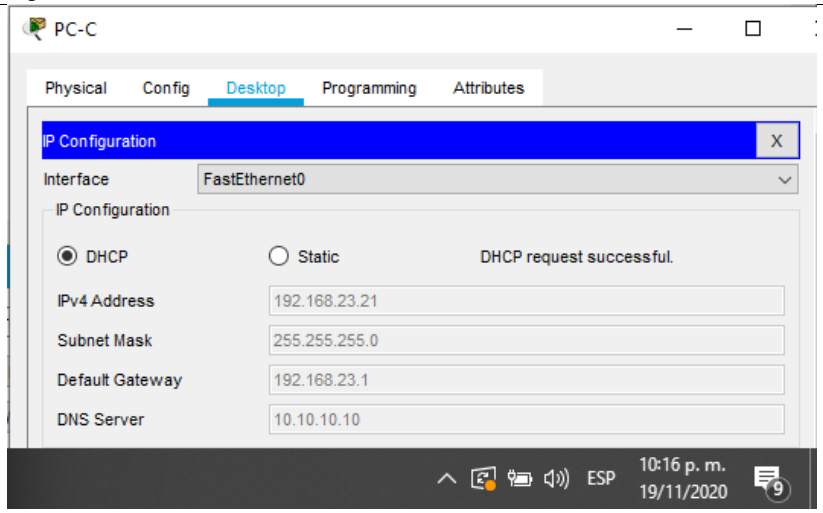
Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	R2(config)#username webuser privilege 15 password cisco12345 Nombre de usuario: **webuser** Contraseña: **cisco12345** Nivel de privilegio: **15**
Habilitar el servicio del servidor HTTP	R2(config)#ip http server /Este comando no funciona en Packet Tracer/
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	R2(config)#ip http secure-server R2(config)#ip http authentication login local /Estos comandos no funcionan en Packet Tracer pero en un servidor real deberían funcionar/

Crear una NAT estática al servidor web.	R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229 Dirección global interna: **209.165.200.229**
Asignar la interfaz interna y externa para la NAT estática	R2(config)#interface g0/0 R2(config-if)#ip nat outside R2(config-if)#interface loopback 0 R2(config-if)#ip nat inside R2(config-if)#exit
Configurar la NAT dinámica dentro de una ACL privada	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 R2(config)#access-list 1 permit 192.168.5.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.6.0 0.0.0.255 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.	R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248 Nombre del conjunto: **INTERNET** El conjunto de direcciones incluye: **209.165.200.225** – **209.165.200.228**
Definir la traducción de NAT dinámica	R2(config)#ip nat inside source list 1 pool INTERNET R2(config)#exit R2#copy run start

Tabla 30: Configuración de NAT en R2

c. 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.

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	 *Figura 43: DHCP en PC-A*
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	 *Figura 44: DHCP en PC-C*

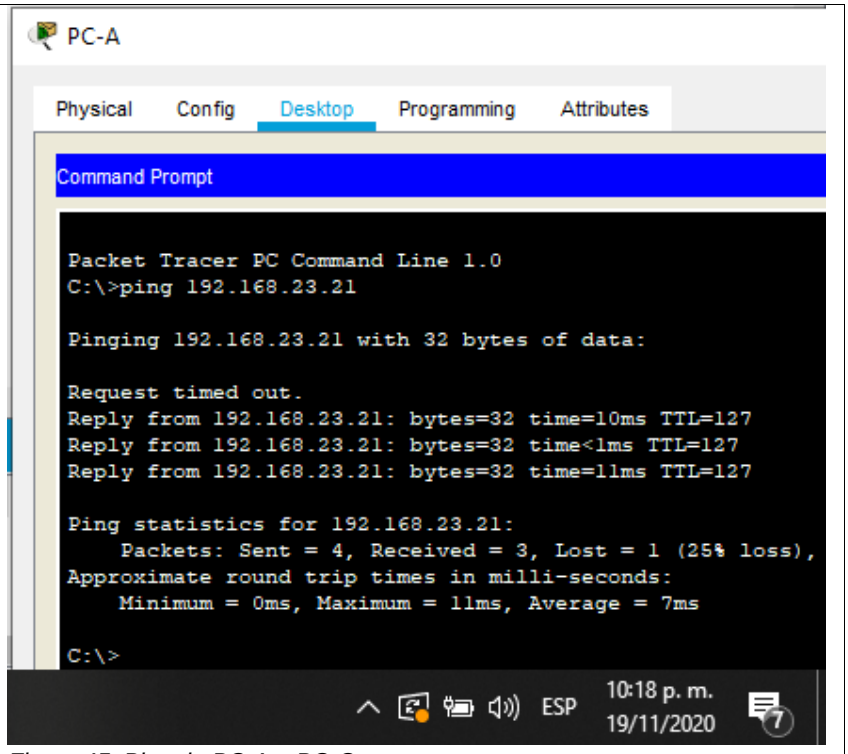
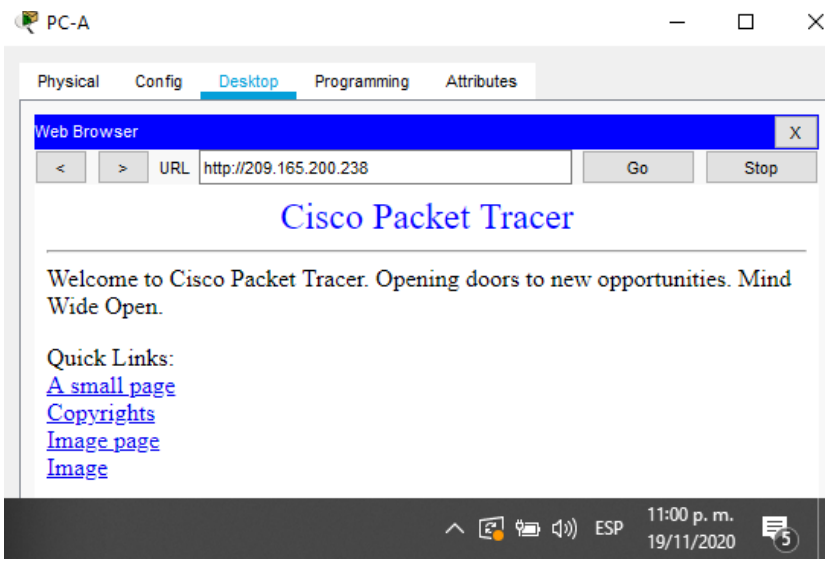
Verificar que la PC-A pueda hacer ping a la PC-C **Nota:** Quizá sea necesario deshabilitar el firewall de la PC.	 *Figura 45: Ping de PC-A a PC-C*
Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.229) Iniciar sesión con el nombre de usuario **webuser** y la contraseña **cisco12345**	 *Figura 46: 209.165.200.238 desde el navegador de PC-A* Se ingresó al servidor de internet 209.165.200.238 desde el PC-A e ingresó correctamente. Al servidor web 209.165.200.229 no fue posible teniendo en cuenta que los comandos para habilitar el servidor web HTTP no sirven sobre Packet Tracer.

Tabla 31: Verificar DHCP y NAT

Parte 5: Configurar NTP

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

Tabla 32: Configurar NTP

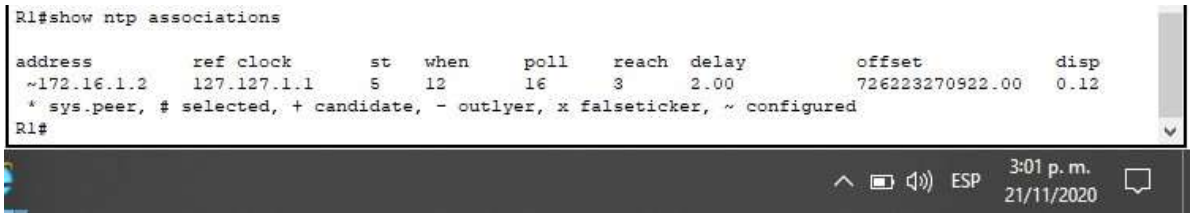


Figura 47: Comando show ntp associations

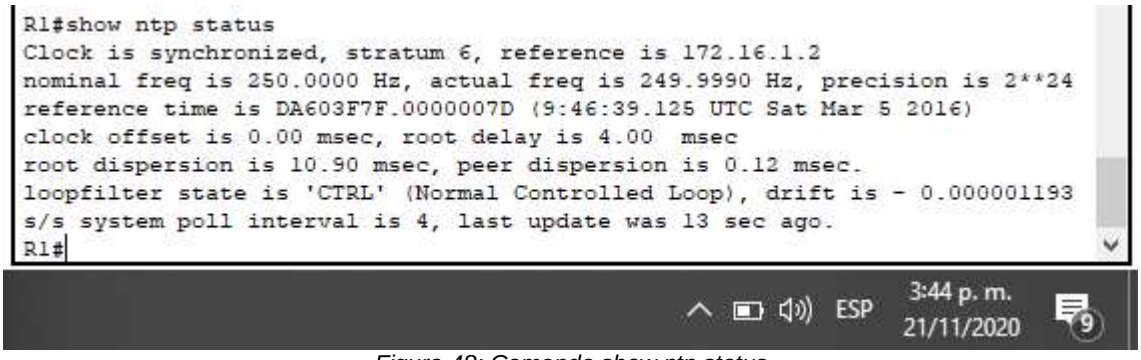


Figura 48: Comando show ntp status

Parte 6: Configurar y verificar las listas de control de acceso (ACL)

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

Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	R2(config)#ip access-list standard ADMIN-MGT R2(config-std-nacl)#permit host 172.16.1.1 Nombre de la ACL: **ADMIN-MGT**
Aplicar la ACL con nombre a las líneas VTY	R2(config)#line vty 0 4 R2(config-line)#access-class ADMIN-MGT in
Permitir acceso por Telnet a las líneas de VTY	R2(config-line)#transport input telnet
Verificar que la ACL funcione como se espera	R1#telnet 172.16.1.2

Tabla 33: Restringir acceso VTY en R2

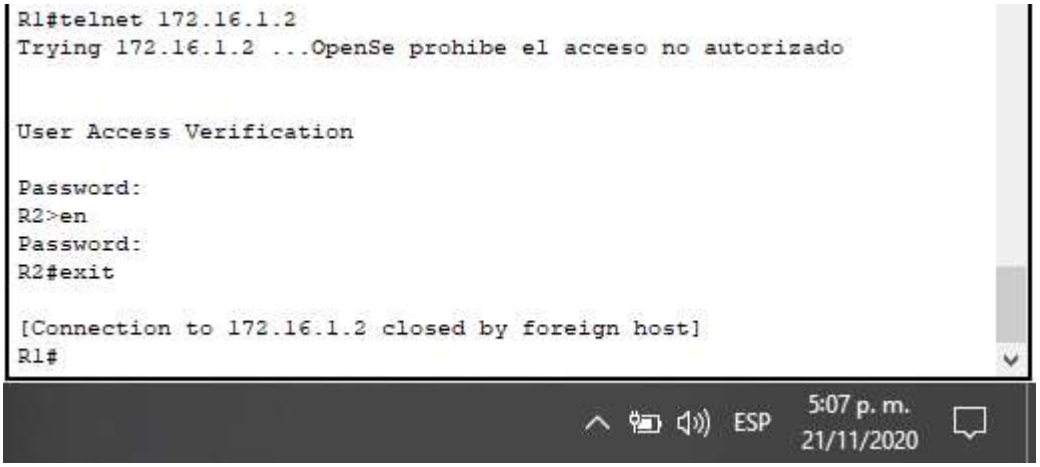
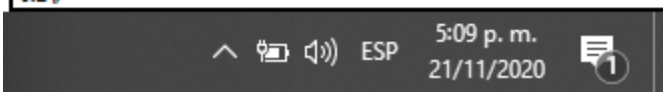
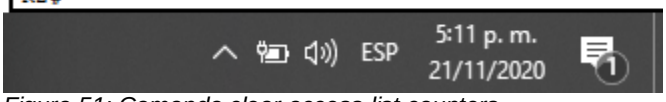


Figura 49: telnet desde R1 a R2 172.16.1.2, password: cisco

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

Descripción del comando	Entrada del estudiante (comando)

Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	show access-list
	`R2#show access-list`
	`Standard IP access list 1`
	`    10 permit 192.168.21.0 0.0.0.255`
	`    20 permit 192.168.23.0 0.0.0.255`
	`    30 permit 192.168.4.0 0.0.0.255`
	`    40 permit 192.168.5.0 0.0.0.255`
	`    50 permit 192.168.6.0 0.0.0.255`
	`Standard IP access list ADMIN-MGT`
	`    10 permit host 172.16.1.1 (6 match(es))`
	`R2#`
	 
	Figura 50: Comando show access-list

Restablecer los contadores de una lista de acceso	clear access-list counters
	`R2#clear ip ?`
	`  bgp    Clear BGP connections`
	`  dhcp   Delete items from the DHCP database`
	`  nat    Clear NAT`
	`  ospf   OSPF clear commands`
	`  route  Delete route table entries`
	`R2#clear acc`
	`R2#clear access-list ?`
	`  counters  Clear access list counters`
	`R2#clear access-list co`
	`R2#clear access-list counters`
	`R2#`
	 
	Figura 51: Comando clear 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 /Se relaciona la captura de pantalla debajo de la tabla 34/
¿Con qué comando se muestran las traducciones NAT?	show ip nat translations /Se relaciona la captura de pantalla debajo de la tabla 34/ **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 *
	`R2#clear ip nat translation ?`
	`  *  Deletes all dynamic translations`
	`R2#clear ip nat translation *`
	`R2#`
	ESP 10:44 a. m. 22/11/2020

*Figura 52: Comando clear ip nat translation **

Tabla 34: Comandos CLI

```
R2#show ip interface
GigabitEthernet0/0 is up, line protocol is up (connected)
  Internet address is 209.165.200.233/29
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is disabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP Fast switching turbo vector
  IP multicast fast switching is disabled
  IP multicast distributed fast switching is disabled
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
```

ESP 10:43 a. m. 22/11/2020

Figura 53: Parte del comando show ip interface

```
R2#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside
global
---  209.165.200.229   10.10.10.10        ---                ---

R2#
```

ESP 5:12 p. m. 21/11/2020

Figura 54: Comando show ip nat translations

CONCLUSIONES

Antes de realizar el curso en CISCO uno estaba acostumbrado a conectar un PC a internet y que automáticamente funcionara. Al realizar los ejercicios 1 y 2 del documento de grado se evidencia lo complejo que se torna el funcionamiento de las redes que usamos a diario en nuestro hogar o empresa.

En el escenario uno se configuraron varias interfaces, se les asignó IPs, tanto ipv4 como ipv6; se crearon VLAN, se conectaron dos hosts que tomaron direcciones ipv4 por DHCP y se les asignó ipv6 estática. En el escenario dos se realizó básicamente la misma configuración del primer escenario al inicio como la configuración de las interfaces y asignación de IPs, pero además, tratándose de tres router interconectados, se implementó un protocolo llamado OSPF que permite compartir las rutas entre sí, por otra parte se implementó el servicio NAT para realizar la traducción de direcciones de red para intercambiar paquetes entre redes con IPs incompatibles y por último se usó el protocolo NTP que permite sincronizar el reloj entre los diferentes dispositivos que conforman la topología para llevar un mejor control del tiempo.

Fue todo un ejercicio complejo y que dejó mucho aprendizaje para implementarlo en la vida real. Al final todo salió bien y las pruebas de ping respondieron satisfactoriamente indicándonos una configuración correcta en los dispositivos que hacen parte de las dos topologías.

BIBLIOGRAFÍA

AKADEMIKA E, 2016. OSPF (Ipv4/Ipv6) Konfiguracija. [online] www.youtube.com. Recuperado de: https://www.youtube.com/watch?v=yh4I-9OGKkY

CISCO.COM. n.d. Configuración de DNS en los routers de Cisco [online] Recuperado de: https://www.cisco.com/c/es_mx/support/docs/ip/domain-name-system-dns/24182-reversedns.pdf

CORTES ROBLES, D., 2015. Configurar DHCP Por VLAN En Equipos CISCO, Packet Tracer. [online] Seguridadyfirewall.cl. Recuperado de: https://www.seguridadyfirewall.cl/2015/08/configurar-dhcp-por-vlan-en-equipos.html

DEL BARRIO, D., 2012. Configurar Un Servidor De DHCP En Cisco - El Taller Del Bit. [online] El Taller del BIT. Recuperado de: https://eltallerdelbit.com/servidor-dhcp-packet-tracer/

ELMUNDOENBITS.COM. 2013. *Cisco, Establecer Longitud De Una Contraseña*. [online] Recuperado de: https://www.elmundoenbits.com/2013/03/cisco-passwd-length.html#.X4POJmgzbIU

ERNESTO, 2020. Aprende Redes.Com » Configuración De Contraseñas De Consola, Auxiliar Y Telnet. [online] Aprenderedes.com. Recuperado de: https://aprenderedes.com/2020/04/configuracion-de-contrasenas-de-consola-auxiliar-y-telnet/

FERNÁNDEZ, R., 2016. ⋆ Enrutamiento Dinámico OSPF Con Packet Tracer. [online] Raulprietofernandez.net. Recuperado de: https://www.raulprietofernandez.net/blog/packet-tracer/enrutamiento-dinamico-ospf-con-packet-tracer

GUERRERO, J., 2017. Enrutamiento Ipv6 Ospfv3. [online] Es.slideshare.net. Recuperado de: https://es.slideshare.net/IsaiGuerrero1/enrutamiento-ipv6-ospfv3

HOTTLE, J., 2006. *Sub-Interface Routing Error*. [online] Community.cisco.com. Recuperado de: https://community.cisco.com/t5/switching/sub-interface-routing-error/td-p/684199

INTERPOLADOS. 2017. *CONFIGURACIÓN DEL ACCESO A LA ADMINISTRACIÓN BÁSICA DE UN SWITCH CON IPV4*. [online] Recuperado de: https://interpolados.wordpress.com/2017/05/01/configuracion-del-acceso-a-la-administracion-basica-de-un-switch-con-ipv4/

MARIONTECHACADEMY, 2013. CS071 21.02 OSPF - Configuracion OSPF En Packet Tracer. [online] www.youtube.com. Recuperado de: https://www.youtube.com/watch?v=lw-IekHi9eY

MOISA, J., 2018. *Asignación De IP A VLAN Administrativa*. [online] Community.cisco.com. Recuperado de: https://community.cisco.com/t5/discusiones-routing-y-switching/asignaci%C3%B3n-de-ip-a-vlan-administrativa/td-p/3357709

MOISA, J., 2018. Configurar La Hora Y Fecha Correcta. [online] Community.cisco.com. Recuperado de: https://community.cisco.com/t5/discusiones-general/configurar-la-hora-y-fecha-correcta/td-p/3735472

MOODLECF.SAPALOMERA.CAT. n.d. *3.2.1.2 Configuración De Interfaces*. [online] Recuperado de: http://moodlecf.sapalomera.cat/RS/3/course/module3/3.2.1.2/3.2.1.2.html

NETACAD.COM, n.d. 2.2.4.8 Protocolo De Hora De Red (NTP). [online] Static-course-assets.s3.amazonaws.com. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE50ES/module2/2.2.4.8/2.2.4.8.html

NET CLOUD ENGINEERING. 2019. *Configuración De Una VLAN En Cisco Switch | Netcloud Engineering*. [online] Recuperado de: https://netcloudengineering.com/configuracion-vlan-cisco-switch/

PEREZ, J., 2018. Cómo Habilitar El Soporte De Ipv6 En Un Switch Cisco Catalisys 3560. [online] red10education.com. Recuperado de: https://red10education.com/blog/como-habilitar-el-soporte-de-ipv6-en-un-switch-cisco-catalisys-3560/

ROSALES, D., 2014. *Autenticación, Utilizando La Base De Datos Local*. [online] Seguridad y Redes. Recuperado de: https://delfirosales.blogspot.com/2014/04/autenticacion-utilizando-la-base-de.html

SCRIBD. 2017. ITN Skills Assess - Student Trng - Ans Key | Dirección IP | Yo Pv6. [online] Recuperado de: https://es.scribd.com/document/361602419/ITN-Skills-Assess-Student-Trng-Ans-Key

SITES.GOOGLE.COM. n.d. *3.2 Enlaces Troncales De Las VLAN - MODULO 3 CISCO CCNA Exploration 3*. [online] Recuperado de: https://sites.google.com/site/paginamodulo3vlan/3-2-enlaces-troncales

SITES.GOOGLE.COM. n.d. 5. Configuración Del Acceso Via HTTP - Redes Locales Y Globales. [online] Recuperado de: https://sites.google.com/site/redeslocalesyglobales/4-configuracion-de-red/2-configuracion-de-routers/3-configuracion-del-router/2-configuracion-de-los-accesos-al-router/ddddd-1

SONIA, M., n.d. *7.2.5.4 Configuración De Direcciones Ipv6 En Dispositivos De Red - CCNA CISCO Sitio Wiki De Maria Sonia*. [online] Sites.google.com. Recuperado de: https://sites.google.com/site/redesintroduccion/7-2-5-4-configuracion-de-direcciones-ipv6-en-dispositivos-de-red

SUÁREZ, M., 2019. *Seguridad En El Switch: Puertos Y Acceso - CCNA Desde Cero*. [online] CCNA Desde Cero. Recuperado de: https://ccnadesdecero.com/curso/seguridad-switch-puertos-acceso/

W0LF_F4NG, 2020. *Configuración Básica Ipv6 Router Cisco*. [online] WF-Networking. Recuperado de: https://www.w0lff4ng.org/configuracion-basica-ipv6-router-cisco/

WALTON, A., 2017. Configuración De NAT Dinámica. [online] ccnadesdecero.es. Recuperado de: https://ccnadesdecero.es/configuracion-nat-dinamica/

WILLEMVWYK, 2007. *Err-Disabled On Fastethernet Port*. [online] Community.cisco.com. Recuperado de: https://community.cisco.com/t5/switching/err-disabled-on-fastethernet-port/td-p/716827

ANEXOS

ANEXO 1

Enlace de descarga de archivo de simulación del escenario 1 realizado en Packet Tracer alojado en Google drive: https://drive.google.com/file/d/1rN-MNCA14cV7mGNV15NcxCP57pRVkGkP/view

ANEXO 2

Enlace de descarga de archivo de simulación del escenario 2 realizado en Packet Tracer alojado en Google drive: https://drive.google.com/file/d/1jZ0mwgjWZGUc2eXNoIGfkojnXMXBbvn3/view

ANEXO 3

Enlace de descarga del artículo científico “IEEE.Jeisson_Hernandez.pdf” alojado en Google drive: https://drive.google.com/file/d/1BsDCgZbCJQGvsjTSNHEmnc2hJStPam3l/view