SOLUCIÓN DE DOS ESTUDIOS DE CASO BAJO EL USO DE TECNOLOGÍA CISCO 2

MAYERLY RONDON SALAZAR

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIAS E INGENIERIAS
INGENIERÍA DE SISTEMAS
BOGOTA D.C
2020

SOLUCIÓN DE DOS ESTUDIOS DE CASO BAJO EL USO DE TECNOLOGÍA CISCO 2

MAYERLY RONDON SALAZAR

PRUEBA DE HABILIDADES PRÁCTICAS CCNA

JOSE IGNACIO CARDONA
ING. TELECOMUNICACIONES

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIAS E INGENIERIAS
INGENIERÍA DE SISTEMAS
BOGOTÁ
2020

CONTENIDO

Pág.

LISTA DE TABLAS

Pág

INTRODUCCIÓN

El desarrollo del presente trabajo plantea la solución propuesta a los ejercicios prácticos asignados como examen de habilidades en el curso CCNA CISCO, durante el desarrollo del informe se da solución asignando los comandos necesarios para la solución del paso a paso según la guía.

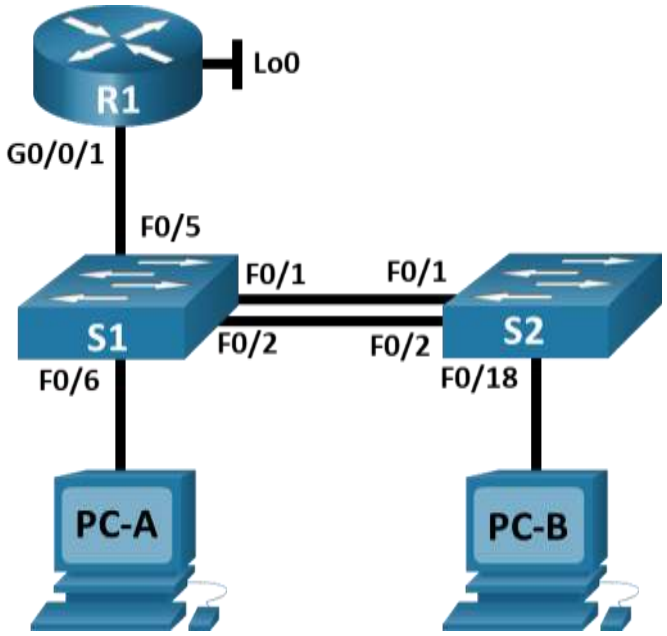
La implementación del ejercicio se realizará sobre el aplicativo packet tracer en la versión 7.3, el cual permite la integración de equipos tecnológicos a una red como computadores, switches, routers, y completar la conexión de redes a través de diferentes tipos de cableado de acuerdo al requerimiento.

Con la práctica de este tipo de ejercicios se pretende poner a prueba los conocimientos obtenidos durante el curso, teniendo como base las actividades realizadas durante el semestre.

1. DESARROLLO DE LOS ESCENARIOS

1.1 ESCENARIO 1

Figura 1. Topología 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.

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

Tabla de VLAN

VLAN	Nombre de la VLAN

2	Bikes
3	Trikes
4	Management
5	Parking
6	Native

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

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

PROCEDIMIENTO:

Parte 1: Inicializar y Recargar y Configurar aspectos básicos de los dispositivos

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

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

Ejecutar los comando:

enable

erase startup-config

reload

Paso 1: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Ejecutar los siguientes comandos para iniciar la configuración

enable
configure terminal

Tarea	Especificación	Comando
Desactivar la búsqueda DNS		*no ip domain lookup*
Nombre del router	R1	*hostname R1*
Nombre de dominio	ccna-lab.com	*ip domain-name ccna-lab.com*
Contraseña cifrada para el modo EXEC privilegiado	ciscoenpass	*enable secret ciscoenpass*
Contraseña de acceso a la consola	ciscoconpass	*line console 0* *password ciscoconpass* *login* *exit*
Establecer la longitud mínima para las contraseñas	10 caracteres	*security passwords min-length 10*

Crear un usuario administrativo en la base de datos local	Nombre de usuario: **admin** Password: **admin1pass**	*username admin secret admin1pass*
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local		*line vty 0 15* *login local*
Configurar VTY solo aceptando SSH		*transport input ssh* *exit*
Cifrar las contraseñas de texto no cifrado		*service password-encryption*
Configure un MOTD Banner		*banner motd #Unauthorized Access#*
Habilitar el routing IPv6		*ipv6 unicast-routing*
Configurar interfaz G0/0/1 y subinterfaces	Establezca la descripción Establece la dirección IPv4. Establezca la dirección local de enlace IPv6 como **fe80: :1** Establece la dirección IPv6. Activar la interfaz.	*interface g 0/0/1.2* *encapsulation dot1Q 2* *description Bikes* *ip address 10.19.8.1 255.255.255.192* *ipv6 address 2001:db8:acad:a::1/64* *ipv6 address fe80::1 link-local* *interface g 0/0/1.3* *encapsulation dot1Q 3* *description Trikes* *ip address 10.19.8.65 255.255.255.224* *ipv6 address 2001:db8:acad:b::1/64* *ipv6 address fe80::1 link-local* *interface g 0/0/1.4* *encapsulation dot1Q 4* *description Management* *ip address 10.19.8.97 255.255.255.248* *ipv6 address 2001:db8:acad:c::1/64* *ipv6 address fe80::1 link-local*

		interface g 0/0/1.6 *encapsulation dot1Q 6 native* *description Native* *interface g 0/0/1* *no shutdown*
Configure el Loopback0 interface	Establezca la descripción Establece la dirección IPv4. Establece la dirección IPv6. Establezca la dirección local de enlace IPv6 como **fe80::1**	*interface Loopback 0* *description Loopback* *ip address 209.165.201.1 255.255.255.224* *ipv6 address 2001:db8:acad:209::1/64* *ipv6 address fe80::1 link-local* *exit*
Generar una clave de cifrado RSA	Módulo de 1024 bits	*crypto key generate rsa 1024*

Paso 2: Configurar S1.

Las tareas de configuración incluyen lo siguiente:

Ejecutar los siguientes comandos para iniciar la configuración

enable
configure terminal

Tarea	Especificación	Comandos
Desactivar la búsqueda DNS.		*no ip domain lookup*
Nombre del switch	**S1**	*hostname S1*
Nombre de dominio	**ccna-lab.com**	*ip domain-name ccna-lab.com*
Contraseña cifrada para el modo EXEC privilegiado	**ciscoenpass**	*enable secret ciscoenpass*
Contraseña de acceso a la consola	**ciscoconpass**	*line console 0* *password ciscoconpass* *login* *exit*
Crear un usuario administrativo en la base de datos local	Nombre de usuario: **admin**	*username admin secret admin1pass*

	Password: **admin1pass**	
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local		*line vty 0 15* *login local*
Configurar las líneas VTY para que acepten únicamente las conexiones SSH		*transport input ssh* *exit*
Cifrar las contraseñas de texto no cifrado		*service password-encryption*
Configurar un MOTD Banner		*banner motd #Unauthorized Access#*
Generar una clave de cifrado RSA	**Módulo de 1024 bits**	*crypto key generate rsa 1024*
Configurar la interfaz de administración (SVI)	Establecer la dirección IPv4 de capa 3 Establezca la dirección local de enlace IPv6 como **FE80: :98 para S1** Establecer la dirección IPv6 de capa 3	*ip address 10.19.8.98 255.255.255.248* *ipv6 address 2001:db8:acad:c::98/64* *ipv6 address fe80::98 link-local* *description Management Interface* *no shutdown*
Configuración del gateway predeterminado	Configure la puerta de enlace predeterminada como 10.19.8.97 para IPv4	*ip default-gateway 10.19.8.97*

Paso 3: Configurar S2

Ejecutar los siguientes comandos para iniciar la configuración

enable
configure terminal

Tarea	Especificación	Comandos
Desactivar la búsqueda DNS.		*no ip domain lookup*
Nombre del switch	**S2**	*hostname S2*
Nombre de dominio	**ccna-lab.com**	*ip domain-name ccna-lab.com*

Contraseña cifrada para el modo EXEC privilegiado	**ciscoenpass**	*enable secret ciscoenpass*
Contraseña de acceso a la consola	**ciscoconpass**	*line console 0* *password ciscoconpass* *login* *exit*
Crear un usuario administrativo en la base de datos local	Nombre de usuario: **admin** Password: **admin1pass**	*username admin secret admin1pass*
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local		*line vty 0 15* *login local*
Configurar las líneas VTY para que acepten únicamente las conexiones SSH		*transport input ssh* *exit*
Cifrar las contraseñas de texto no cifrado		*service password-encryption*
Configurar un MOTD Banner		*banner motd #Unauthorized Access#*
Generar una clave de cifrado RSA	**Módulo de 1024 bits**	*crypto key generate rsa 1024*
Configurar la interfaz de administración (SVI)	Establecer la dirección IPv4 de capa 3 Establezca la dirección local de enlace IPv6 como **FE80: :98 para S1 y FE80: :99 para S2** Establecer la dirección IPv6 de capa 3	*interface vlan 4* *ip address 10.19.8.99 255.255.255.248* *ipv6 address 2001:db8:acad:c::99/64* *ipv6 address fe80::99 link-local* *description Management Interface* *no shutdown* *exit*
Configuración del gateway predeterminado	Configure la puerta de enlace predeterminada como 10.19.8.97 para IPv4	*ip default-gateway 10.19.8.97*

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

Paso 4: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tarea	Especificación	Comandos
Crear VLAN	VLAN 2, nombre Bikes VLAN 3, nombre Trikes VLAN 4, name Management VLAN 5, nombre Parking VLAN 6, nombre Native	*vlan 2* *name Bikes* *vlan 3* *name Trikes* *vlan 4* *name Management* *vlan 5* *name Parking* *vlan 6* *name Native*
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	Interfaces F0/1, F0/2 y F0/5	*interface range g 1/0/1-2* *shutdown*
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	Usar el protocolo LACP para la negociación	*interface range g 1/0/1-2* *shutdown*
Configurar el puerto de acceso de host para VLAN 2	Interface F0/6	*interface range g 1/0/1-2* *shutdown* *switchport trunk encapsulation dot1q* *switchport mode trunk* *switchport trunk native vlan 6* *channel-group 1 mode active* *interface port-channel 1*

		switchport trunk encapsulation dot1q *switchport mode trunk* *switchport trunk native vlan 6* *exit* *interface g 1/0/5* *switchport trunk encapsulation dot1q* *switchport mode trunk* *switchport trunk native vlan 6* *exit* *interface g 1/0/6* *switchport mode access* *switchport access vlan 2* *switchport port-security*
Configurar la seguridad del puerto en los puertos de acceso	Permitir 3 direcciones MAC	*switchport port-security maximum 3*
Proteja todas las interfaces no utilizadas	Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar	*interface range g 1/0/3-4* *switchport mode access* *switchport access vlan 5* *description Disabled Interfaces* *shutdown* *interface range g 1/0/7-24* *switchport mode access* *switchport access vlan 5* *description Disabled Interfaces* *shutdown* *interface range g 1/1/1-4*

		switchport mode access *switchport access vlan 5* *description Disabled Interfaces* *shutdown* *interface range g 1/0/1-2* *no shutdown*

Paso 6: Configure el S2.

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

Tarea	Especificación	
Crear VLAN	VLAN 2, name Bikes VLAN 3, name Trikes VLAN 4, name Management VLAN 5, nombre Parking VLAN 6, nombre Native	*vlan 2* *name Bikes* *vlan 3* *name Trikes* *vlan 4* *name Management* *vlan 5* *name Parking* *vlan 6* *name Native*
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	Interfaces F0/1 y F0/2	*interface range g 1/0/1-2* *shutdown*
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	Usar el protocolo LACP para la negociación	*switchport trunk encapsulation dot1q* *switchport mode trunk* *switchport trunk native vlan 6* *//switchport trunk allowed vlan 2 3 4 5 6* *channel-group 1 mode active* *interface port-channel 1*

		switchport trunk encapsulation dot1q *switchport mode trunk* *switchport trunk native vlan 6* *exit*
Configurar el puerto de acceso del host para la VLAN 3	Interfaz F0/18	*interface g 1/0/18* *switchport mode access* *switchport access vlan 3* *switchport port-security*
Configure port-security en los access ports	permite 3 MAC addresses	*switchport port-security maximum 3* *interface range g 1/0/3-17* *switchport mode access* *switchport access vlan 5* *description Disabled Interfaces* *shutdown* *interface range g 1/0/19-24* *switchport mode access* *switchport access vlan 5* *description Disabled Interfaces* *shutdown*
Asegure todas las interfaces no utilizadas.	Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar	*interface range g 1/1/1-4* *switchport mode access* *switchport access vlan 5* *description Disabled Interfaces* *shutdown* *interface range g 1/0/1-2* *no shutdown*

Parte 3 Configurar soporte de host

Paso 7: Configure R1

Las tareas de configuración para R1 incluyen las siguientes:

Tarea	Especificación	Comandos
Configure Default Routing	Crear rutas predeterminadas para IPv4 e IPv6 que dirijan el tráfico a la interfaz Loopback 0	*ip route 0.0.0.0 0.0.0.0 loopback 0* *ipv6 route ::/0 loopback 0*
Configurar IPv4 DHCP para VLAN 2	Cree un grupo DHCP para VLAN 2, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio ccna-a.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada	*ip dhcp excluded-address 10.19.8.1 10.19.8.52* *ip dhcp pool Bikes-VLAN2* *network 10.19.8.0 255.255.255.192* *default-router 10.19.8.1* *domain-name ccna-a.net* *exit*
Configurar DHCP IPv4 para VLAN 3	Cree un grupo DHCP para VLAN 3, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio ccna-b.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada	*ip dhcp excluded-address 10.19.8.65 10.19.8.84* *ip dhcp pool Trikes-VLAN3* *network 10.19.8.64 255.255.255.224* *default-router 10.19.8.65* *domain-name ccna-b.net* *exit*

Paso 8: Configurar los servidores

Configure los equipos host PC-A y PC-B para que utilice 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**.

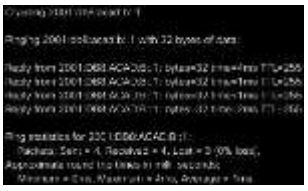
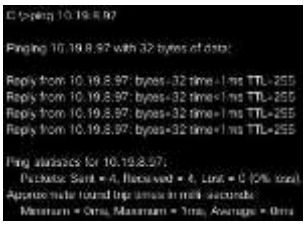
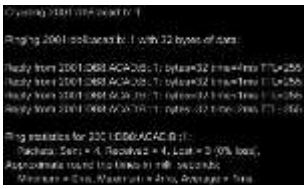
Configuración de red de PC-A	
Descripción	
Dirección física	*0060.708D.7782*
Dirección IP	*2001:DB8:ACAD:A::50*
Máscara de subred	*255.255.255.192*
Gateway predeterminado	*10.19.8.1*
Gateway predeterminado IPv6	*FE80::1*

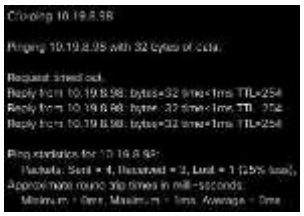
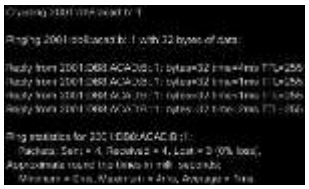
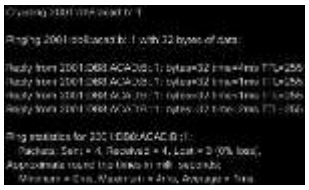
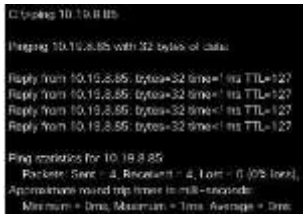
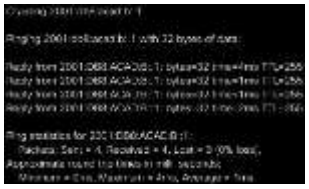
Configuración de red de PC-B	
Descripción	
Dirección física	*0001.643A.B3AA*
Dirección IP	*2001:DB8:ACAD:B::50*
Máscara de subred	*255.255.255.224*
Gateway predeterminado	*10.19.8.65*
Gateway predeterminado IPv6	*FE80::1*

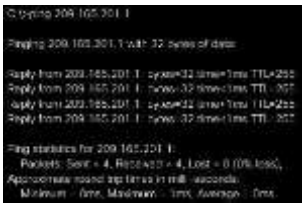
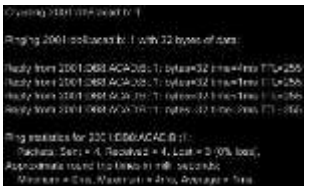
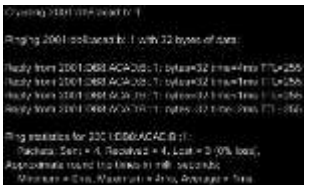
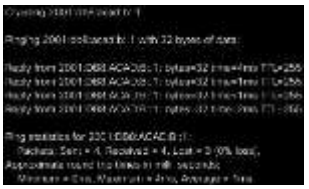
Parte 4: Probar y verificar la conectividad de extremo a extremo

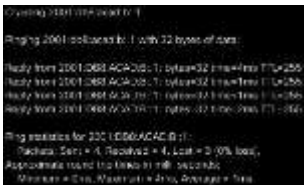
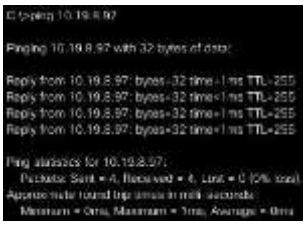
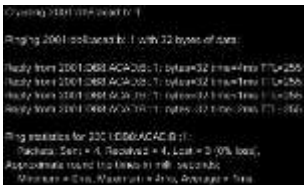
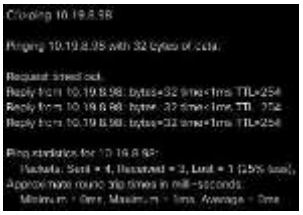
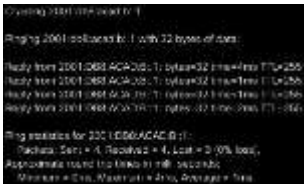
Use el comando ping para probar la conectividad IPv4 e IPv6 entre todos los dispositivos de red.

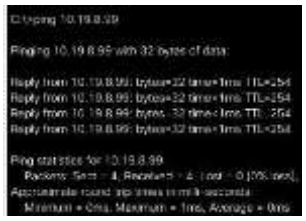
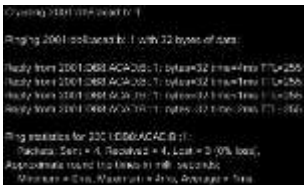
Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Desde	A	de Internet	Dirección IP	Resultados de ping
PC-A	R1, G0/0/1.2	Dirección	10.19.8.1	**Figura 2. ping PCA -R1 G0/0/1.2** 
		IPv6	2001:db8:acad:a: :1	**Figura 3. ping PCA -R1 G0/0/1.2 Ipv6** 
	R1, G0/0/1.3	Dirección	10.19.8.65	**Figura 4. ping PCA -R1 G0/0/1.3** 
		IPv6	2001:db8:acad:b::1	**Figura 5. ping PCA -R1 G0/0/1.3 Ipv6** 
	R1, G0/0/1.4	Dirección	10.19.8.97	**Figura 6. ping PCA -R1 G0/0/1.4** 
		IPv6	2001:db8:acad:c::1	**Figura 7. ping PCA -R1 G0/0/1.4 Ipv6** 

	S1, VLAN 4	Dirección	10.19.8.98	**Figura 8. ping PCA -S1 VLAN 4** 
		IPv6	2001:db8:acad:c::98	**Figura 9. ping PCA -S1 VLAN 4 IPV6** 
	S2, VLAN 4	Dirección	10.19.8.99.	**Figura 10. ping PCA -S2 VLAN 4** 
		IPv6	2001:db8:acad:c::99	**Figura 11. ping PCA -S2 VLAN 4 IPV6** 
	PC-B	Dirección	10.19.8.85	**Figura 12. ping PCA - PCB** 
		IPv6	2001:db8:acad:b: :50	**Figura 13. ping PCA - PCB IPV6** 

	R1 Bucle 0	Dirección	209.165.201.1	**Figura 12. ping PCA - R1** 
		IPv6	2001:db8:acad:209: :1	**Figura 13. ping PCA-R1 IPV6** 
PC-B	R1 Bucle 0	Dirección	209.165.201.1	**Figura 14. ping PCB-R1** 
		IPv6	2001:db8:acad:209: :1	**Figura 15. ping PCB-R1 IPV6** 
	R1, G0/0/1.2	Dirección	10.19.8.1	**Figura 16. ping PCB-R1 G0/0/1.2** 
		IPv6	2001:db8:acad:a: :1	**Figura 17. ping PCB-R1 G0/0/1.2 IPV6** 

R1, G0/0/1.3	Dirección	10.19.8.65	**Figura 18. ping PCB-R1 G0/0/1.3** 
	IPv6	2001:db8:acad:b: :1	**Figura 19. ping PCB-R1 G0/0/1.3 IPV6** 
R1, G0/0/1.4	Dirección	10.19.8.97	**Figura 20. ping PCB-R1 G0/0/1.4** 
	IPv6	2001:db8:acad:c: :1	**Figura 21. ping PCB-R1 G0/0/1.4 IPV6** 
S1, VLAN 4	Dirección	10.19.8.98	**Figura 22. ping PCB-S1 VLAN 4** 
	IPv6	2001:db8:acad:c: :98	**Figura 23. ping PCB-S1 VLAN 4 IPV6** 

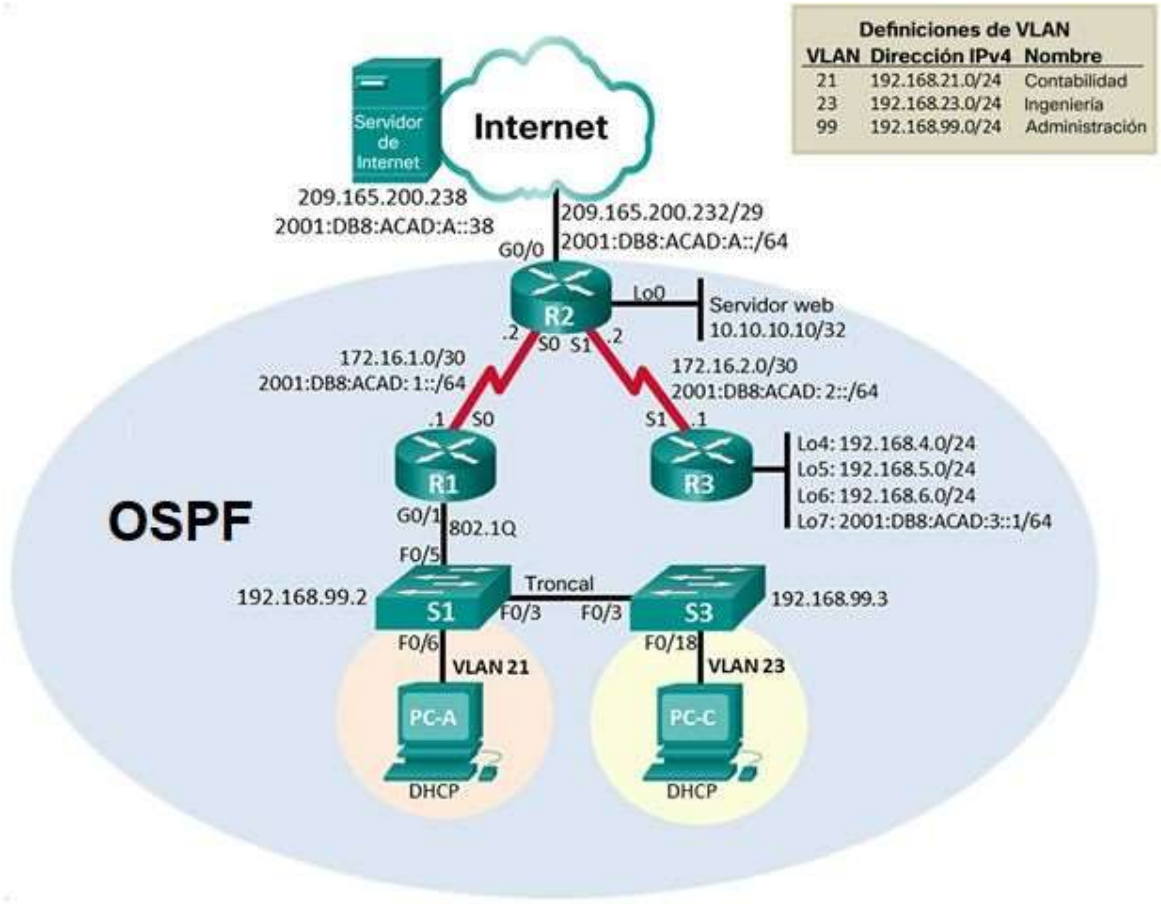
	S2, VLAN 4	Dirección	10.19.8.99.	**Figura 24. ping PCB-S2 VLAN 4** 
		IPv6	2001:db8:acad:c: :99	**Figura 25. ping PCB-S2 VLAN 4 IPV6** 

1.2 ESCENARIO 2

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

Topología

Figura 26. Topología escenario 2



Parte 1: Inicializar dispositivos

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

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

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

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	*Erase startup-config* *delete vlan.dat*
Volver a cargar ambos switches	*reload*
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	*Show flash*

Parte 2: Configurar los parámetros básicos de los dispositivos

Paso 2: 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	
Máscara de subred para IPv4	
Gateway predeterminado	209.165.200.225
Dirección IPv6/subred	
Gateway predeterminado IPv6	2001:DB8:ACAD:2::1

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación	Comandos
Desactivar la búsqueda DNS		*no ip domain-lookup*
Nombre del router	R1	*hostname R1*
Contraseña de exec privilegiado cifrada	class	*enable secret class*
Contraseña de acceso a la consola	cisco	*line console 0* *password cisco* *login*
Contraseña de acceso Telnet	cisco	*line vty 0 15* *password cisco* *login* *exit*
Cifrar las contraseñas de texto no cifrado		*service password-encryption*
Mensaje MOTD	Se prohíbe el acceso no autorizado.	*banner motd $Se prohíbe el acceso no autorizado$*
Interfaz S0/0/0	Establezca la descripción Establecer la dirección IPv4 Consultar el diagrama de topología para conocer la información de direcciones Establecer la dirección IPv6 Consultar el diagrama de topología para conocer la información de direcciones Establecer la frecuencia de reloj en 128000 Activar la interfaz	*interface s 0/0/0* *description ToR2* *ip address 172.16.1.1 255.255.255.252* *ipv6 address 2001:DB8:ACAD:1::1/64* *clock rate 128000* *no shutdown* *exit*
Rutas predeterminadas	Configurar una ruta IPv4 predeterminada de S0/0/0 Configurar una ruta IPv6 predeterminada de S0/0/0	*ip route 0.0.0.0 0.0.0.0 s0/0/0* *ipv6 route ::/0 s0/0/0*

Nota: Todavía no configure G0/1.

Paso 4: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación	Comando
Desactivar la búsqueda DNS		*no ip domain-lookup*
Nombre del router	R2	*hostname R2*
Contraseña de exec privilegiado cifrada	class	*enable secret class*
Contraseña de acceso a la consola	cisco	*line console 0* *password cisco* *login*
Contraseña de acceso Telnet	cisco	*line vty 0 15* *password cisco* *login* *exit*
Cifrar las contraseñas de texto no cifrado		*service password-encryption*
Habilitar el servidor HTTP		*ip http server*
Mensaje MOTD	Se prohíbe el acceso no autorizado.	*banner motd $Se prohíbe el acceso no autorizado$*
Interfaz S0/0/0	Establezca la descripción Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz	*interface s 0/0/0* *description ToR1* *ip address 172.16.1.2 255.255.255.252* *ipv6 address 2001:DB8:ACAD:1::2/64* *no shutdown*
Interfaz S0/0/1	Establecer la descripción Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Establezca la dirección IPv6.	*interface s 0/0/1* *description ToR3* *ip address 172.16.2.2 255.255.255.252*

	Consulte el diagrama de topología para conocer la información de direcciones. Establecer la frecuencia de reloj en 128000. Activar la interfaz	*ipv6 address 2001:DB8:ACAD:2::2/64* *clock rate 128000* *no shutdown*
Interfaz G0/0 (simulación de Internet)	Establecer la descripción. Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Establezca la dirección IPv6. Utilizar la primera dirección disponible en la subred. Activar la interfaz	*interface g 0/0* *description ToInternet* *ip address 209.165.200.233 255.255.255.248* *ipv6 address 2001:DB8:ACAD:A::1/64* *no shutdown*
Interfaz loopback 0 (servidor web simulado)	Establecer la descripción. Establezca la dirección IPv4.	*interface loopback 0* *ip address 10.10.10.10 255.255.255.255* *description SimulatedLoopback* *exit*
Ruta predeterminada	Configure una ruta IPv4 predeterminada de G0/0. Configure una ruta IPv6 predeterminada de G0/0.	*ip route 0.0.0.0 0.0.0.0 g0/0* *ipv6 route ::/0 g0/0*

Paso 5: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Elemento o tarea de configuración	**Especificación**	**Comando**
Desactivar la búsqueda DNS		*no ip domain-lookup*
Nombre del router	R3	*hostname R3*
Contraseña de exec privilegiado cifrada	class	*enable secret class*
Contraseña de acceso a la consola	cisco	*line console 0* *password cisco* *login*

Contraseña de acceso Telnet	cisco	*line vty 0 15* *password cisco* *login* *exit*
Cifrar las contraseñas de texto no cifrado		*service password-encryption*
Mensaje MOTD	Se prohíbe el acceso no autorizado.	*banner 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	*interface s 0/0/1* *description ToR2* *ip address 172.16.2.1 255.255.255.252* *ipv6 address 2001:DB8:ACAD:2::1/64* *no shutdown*
Interfaz loopback 4	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.	*interface loopback 4* *ip address 192.168.4.1 255.255.255.0*
Interfaz loopback 5	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.	*interface loopback 5* *ip address 192.168.5.1 255.255.255.0*
Interfaz loopback 6	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.	*interface loopback 6* *ip address 192.168.6.1 255.255.255.0*
Interfaz loopback 7	Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.	*interface loopback 7* *ipv6 address 2001:DB8:ACAD:3::1/64*
Rutas predeterminadas		*ip route 0.0.0.0 0.0.0.0 s0/0/1* *ipv6 route ::/0 s0/0/1*

Paso 6: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación	Comando
Desactivar la búsqueda DNS		*no ip domain-lookup*
Nombre del switch	S1	*hostname S1*
Contraseña de exec privilegiado cifrada	class	*enable secret class*
Contraseña de acceso a la consola	cisco	*line console 0* *password cisco* *login*
Contraseña de acceso Telnet	cisco	*line vty 0 15* *password cisco* *login*
Cifrar las contraseñas de texto no cifrado		*service password-encryption*
Mensaje MOTD	Se prohíbe el acceso no autorizado.	*banner motd $Se prohíbe el acceso no autorizado$*

Paso 7: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

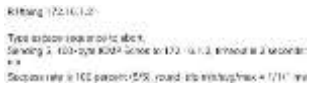
Elemento o tarea de configuración	Especificación	Comando
Desactivar la búsqueda DNS		*no ip domain-lookup*
Nombre del switch	S3	*hostname S3*
Contraseña de exec privilegiado cifrada	class	*enable secret class*
Contraseña de acceso a la consola	cisco	*line console 0* *password cisco*

		login
Contraseña de acceso Telnet	cisco	*line vty 0 15* *password cisco* *login*
Cifrar las contraseñas de texto no cifrado		*service password-encryption*
Mensaje MOTD	Se prohíbe el acceso no autorizado.	*banner motd $Se prohíbe el acceso no autorizado$*

Paso 8: 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 27. ping R1-R2** 
R2	R3, S0/0/1	172.16.2.1	**Figura 28. ping R2-R3** 
PC de Internet	Gateway predeterminado	209.165.200.233	**Figura 29. ping PC -gateway** 

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 9: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación	Comando
Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para topología para crear y nombrar cada una de las VLAN que se indican	*vlan 21* *name Contabilidad* *vlan 23* *name Ingenieria* *vlan 99* *name Administracion* *exit*
Asignar la dirección IP de administración.	Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S1 en el diagrama de topología	*interface vlan 99* *ip address 192.168.99.2 255.255.255.0* *no shutdown* *exit*
Asignar el gateway predeterminado	Asigne la primera dirección IPv4 de la subred como el gateway predeterminado.	*ip default-gateway 192.168.99.1*
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa	*interface fa 0/3* *switchport mode trunk* *switchport trunk native vlan 1*
Forzar el enlace troncal en la interfaz F0/5	Utilizar la red VLAN 1 como VLAN nativa	*interface fa 0/5* *switchport mode trunk* *switchport trunk native vlan 1*
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range	*interface range fa0/1-2, fa0/4, fa0/6-24, g0/1-2* *switchport mode access*
Asignar F0/6 a la VLAN 21		*interface fa 0/6* *switchport access vlan 21*

Apagar todos los puertos sin usar		*interface range fa0/1-2, fa0/4, fa0/7-24, g0/1-2* *shutdown*

Paso 10: Configurar S3

La configuración del S3 incluye las siguientes tareas:

Elemento o tarea de configuración	**Especificación**	**Comando**
Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para topología para crear cada una de las VLAN que se indican Dé nombre a cada VLAN.	*vlan 21* *name Contabilidad* *vlan 23* *name Ingenieria* *vlan 99* *name Administracion* *exit*
Asignar la dirección IP de administración	Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S3 en el diagrama de topología	*interface vlan 99* *ip address 192.168.99.3 255.255.255.0* *no shutdown* *exit*
Asignar el gateway predeterminado.	Asignar la primera dirección IP en la subred como gateway predeterminado.	*ip default-gateway 192.168.99.1*
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa	*interface fa 0/3* *switchport mode trunk* *switchport trunk native vlan 1*
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range	*interface range fa0/1-2, fa0/4-24, g0/1-2* *switchport mode access*
Asignar F0/18 a la VLAN 21		*interface fa 0/18* *switchport access vlan 21*
Apagar todos los puertos sin usar		*interface range fa0/1-2, fa0/4-17, fa0/19-24, g0/1-2* *shutdown*

Paso 11: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación	Comando
Configurar la subinterfaz 802.1Q .21 en G0/1	Descripción: LAN de Contabilidad Asignar la VLAN 21 Asignar la primera dirección disponible a esta interfaz	*interface g 0/1.21* *description Lan de Contabilidad* *encapsulation dot1q 21* *ip address 192.168.21.1 255.255.255.0*
Configurar la subinterfaz 802.1Q .23 en G0/1	Descripción: LAN de Ingeniería Asignar la VLAN 23 Asignar la primera dirección disponible a esta interfaz	*interface g 0/1.23* *description Lan de Ingenieria* *encapsulation dot1q 23* *ip address 192.168.23.1 255.255.255.0*
Configurar la subinterfaz 802.1Q .99 en G0/1	Descripción: LAN de Administración Asignar la VLAN 99 Asignar la primera dirección disponible a esta interfaz	*interface g 0/1.99* *description Lan de Administracion* *encapsulation dot1q 99* *ip address 192.168.99.1 255.255.255.0*
Activar la interfaz G0/1		*interface g 0/1* *no shutdown*

Paso 12: 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 30. ping S1 - R1** 

S3	R1, dirección VLAN 99	192.168.99.1	**Figura 31. ping S3 - R1** 
S1	R1, dirección VLAN 21	192.168.21.1	**Figura 32. ping S1 - R1** 
S3	R1, dirección VLAN 23	192.168.23.1	**Figura 33. ping S3 - R1** 

Parte 4: Configurar el protocolo de routing dinámico OSPF

Paso 13: Configurar OSPF en el R1

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación	Comando
Configurar OSPF área 0		*router ospf 1* *router-id 1.1.1.1*
Anunciar las redes conectadas directamente	Asigne todas las redes conectadas directamente.	*do show ip route connected* *network 172.16.1.0 255.255.255.252 area 0* *network 192.168.21.0 255.255.255.0 area 0* *network 192.168.23.0 255.255.255.0 area 0* *network 192.168.99.0 255.255.255.0 area 0*
Establecer todas las interfaces LAN como pasivas		*passive-interface g 0/1.21* *passive-interface g 0/1.23* *passive-interface g 0/1.99*
Desactive la sumarización automática	Command exclusive for	*no auto-summary*

	RIP protocol	

Paso 14: Configurar OSPF en el R2

La configuración del R2 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación	Comando
Configurar OSPF área 0		*router ospf 1* *router-id 2.2.2.2*
Anunciar las redes conectadas directamente	**Nota:** Omitir la red G0/0.	*do show ip route connected* *network 10.10.10.10 255.255.255.252 area 0* *network 172.16.1.0 255.255.255.252 area 0* *network 172.16.2.0 255.255.255.252 area 0* *network 209.165.200.232 255.255.255.248 area 0*
Establecer la interfaz LAN (loopback) como pasiva		*passive-interface loopback 0*
Desactive la sumarización automática.	Command exclusive for RIP protocol	*no auto-summary*

Paso 15: Configurar OSPFv3 en el R3

La configuración del R3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación	Comando
Configurar OSPF área 0		*router ospf 1* *router-id 3.3.3.3*

Anunciar redes IPv4 conectadas directamente		*do show ip route connected* *network 172.16.2.0 255.255.255.252 area 0* *network 192.168.4.0 255.255.255.0 area 0* *network 192.168.5.0 255.255.255.0 area 0* *network 192.168.6.0 255.255.255.0 area 0*
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas		*passive-interface loopback 4* *passive-interface loopback 5* *passive-interface loopback 6*
Desactive la sumarización automática.	Command exclusive for RIP protocol	*no auto-summary*

Paso 16: Verificar la información de OSPF

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

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

Implementar DHCP y NAT para IPv4

Paso 17: 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	Comando
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas		*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		*ip dhcp excluded-address 192.168.23.1 192.168.23.20*
Crear un pool de DHCP para la VLAN 21.	Nombre: ACCT Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado	*ip dhcp pool ACCT* *network 192.168.21.0 255.255.255.0* *dns-server 10.10.10.10* *domain-name ccna-sa.com* *default-router 192.168.21.1*
Crear un pool de DHCP para la VLAN 23	Nombre: ENGNR Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado	*ip dhcp pool ENGNR* *network 192.168.23.0 255.255.255.0* *dns-server 10.10.10.10* *domain-name ccna-sa.com* *default-router 192.168.23.1*

Paso 18: Configurar la NAT estática y dinámica en el R2

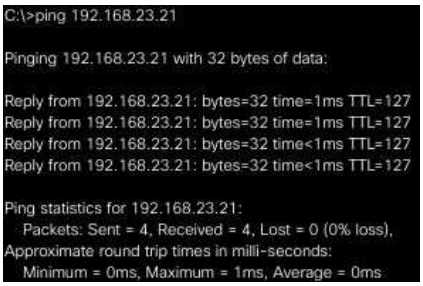
La configuración del R2 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación	Comando
Crear una base de datos local con una cuenta de usuario	Nombre de usuario: **webuser** Contraseña: **cisco12345** Nivel de privilegio: **15**	*username webuser privilege 15 secret cisco12345*
Habilitar el servicio del servidor HTTP		*ip http server*

Configurar el servidor HTTP para utilizar la base de datos local para la autenticación		*ip http authentication local*
Crear una NAT estática al servidor web.	Dirección global interna: **209.165.200.229**	*ip nat inside source static 10.10.10.10 209.165.200.229*
Asignar la interfaz interna y externa para la NAT estática		*interface loopback 0* *ip nat inside* *interface g 0/0* *ip nat outside* *exit*
Configurar la NAT dinámica dentro de una ACL privada	Lista de acceso: 1 Permitir la traducción de las redes de Contabilidad y de Ingeniería en el R1 Permitir la traducción de un resumen de las redes LAN (loopback) en el R3	*access-list 1 permit 192.168.21.0 0.0.0.255* *access-list 1 permit 192.168.23.0 0.0.0.255* *access-list 1 permit 192.168.4.0 0.0.3.255*
Defina el pool de direcciones IP públicas utilizables.	Nombre del conjunto: **INTERNET** El conjunto de direcciones incluye: **209.165.200.225** – **209.165.200.228**	*ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248*
Definir la traducción de NAT dinámica		*ip nat inside source list 1 pool INTERNET* *end*

Paso 19: 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 31. IP- PC-A** 
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	**Figura 31. IP- 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 32. ping PC-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	PT No soporta esta operación, el error es: Server Reset Connection, doing ping to this IP does work.

contraseña **cisco12345**	

Paso 20: Configurar NTP

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

Paso 21: Configurar y verificar las listas de control de acceso (ACL)

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	Nombre de la ACL: **ADMIN-MGT**	ip access-list standard ADMIN-MGT permit host 172.16.1.1 exit
Aplicar la ACL con nombre a las líneas VTY		line vty 0 15 access-class
Permitir acceso por Telnet a las líneas de VTY		ADMIN-MGT in transport input telnet end
Verificar que la ACL funcione como se espera		show access-list clear ip access-list counters

		show ip interface

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
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 agregaran las traducciones a la tabla debido al modo de simulación de Internet en la red. show ip nat translations It doesn't work because S 0/0/0 and S 0/0/1 interfaces aren't configured as inside interfaces on R2.
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	clear ip nat translations *

CONCLUSIONES

El desarrollo de los ejercicios prácticos obtuvieron resultados positivos para el aprendizaje, sin embargo se encontraron funcionalidades no soportadas para el aplicativo packet tracer, que si están disponibles para un ambiente real.

El análisis final realizado sobre los ejercicios permite validar el conocimiento obtenido a través del curso, apropiando y creando estrategias aplicables durante un ejercicio real que se pueda presentar en el ejercicio de la profesión.

BIBLIOGRAFÍA

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

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

CISCO. (2019). VLAN. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#6

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

UNAD (2017). Configuración de Switches y Routers [OVA]. Recuperado de https://1drv.ms/u/s!AmlJYei-NT1IhgL9QChD1m9EuGqC

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

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