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

MARCEL GIOVANNY HERRERA REYES

UNIVERSIDAD NACIONAL ABIERTA A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI
INGENIERIA DE SISTEMAS
PEREIRA
2020

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

MARCEL GIOVANNY HERRERA REYES

Diplomado de opción de grado presentado para optar el título
de INGENIERO DE SISTEMAS

Presentado al DIRECTOR: Ing. JUAN CARLOS VESGA FERREIRA

UNIVERSIDAD NACIONAL ABIERTA A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI
INGENIERIA DE SISTEMAS
PEREIRA
2020

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____

_____

_____
Firma del presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

Pereira, 15 de diciembre de 2020

AGRADECIMIENTOS

Principalmente a Dios y a mi familia, quienes siempre han creído en mí y demostraron su apoyo incondicional en cada momento. A Los profesores y directores que contribuyeron positivamente a mi formación profesional.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

ACL: Access Control List. Lista de Control de Acceso. Un ACL es una lista que especifica los permisos de los usuarios sobre un archivo, carpeta u otro objeto. Un ACL define cuales usuarios y cuales grupos pueden accesar y que tipo de operaciones pueden realizar una vez dentro.

GATEWAY: Es la primera dirección después de la configuración de dirección de red usada como referente para identificar el punto de acceso a otra red.

IPv4: Protocolo de internet versión 4

IPv6: Protocolo de internet versión 6

LAN: Local Area Network. Red de área local. Red de computadoras personales ubicadas dentro de un área geográfica limitada que se compone de servidores, estaciones de trabajo, sistemas operativos de redes y un enlace encargado de distribuir las comunicaciones.

NAT: (Network Address Translation): La traducción de direcciones de red o también llamado enmascaramiento de IP o NAT, es un mecanismo utilizado por routers IP para intercambiar paquetes entre dos redes que asignan mutuamente direcciones incompatibles.

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

RESUMEN

Las actividades prácticas y de desarrollo de escenarios que simulan problemas que pueden presentarse en un entorno de realidad, resultan una herramienta muy valiosa para demostrar el conocimiento que se ha intentado sea aprehendido por parte de los estudiantes de cualquier curso en general, y los estudiantes del diplomado Cisco CCNA no son la excepción. Concebir, diseñar, configurar y probar las conexiones de una red que puede suplir una necesidad específica, suponen el logro del principal objetivo propuesto de aprendizaje, documentando cada proceso de solución, poniendo a prueba el nivel de comprensión necesario relacionado con diversos aspectos de networking.

Tratar de concebir un diseño de red, sus configuraciones, el enrutamiento adecuado y poder probar que las comunicaciones son exitosas son parte del éxito que demuestra el afianzamiento de los conceptos, la interpretación del contenido de datos, análisis de técnicas, solución de errores de enrutamiento mediante diagnósticos y puesta a prueba para garantizar brindar una solución óptima a una situación planteada.

Palabras clave: CISCO, CCNA, Networking, Enrutamiento.

ABSTRACT

The practical activities and the development of scenarios that simulate problems that can be presented in a reality environment, are a very valuable tool to demonstrate the knowledge that has been tried to be apprehended by the students of any course in general, and the students of the Cisco CCNA are no exception. Conceiving, designing, configuring and testing the connections of a network that can supply a specific need, suppose the achievement of the main proposed learning objective, documenting each solution process, testing the necessary level of understanding related to various networking subjects.

Trying to conceive a network design, its configurations, the adequate routing and being able to prove that the communications are successful are part of the success that demonstrates the consolidation of the concepts, the interpretation of the data content, analysis of techniques, solution of routing errors through diagnostics and testing to ensure an optimal solution to a given situation.

Key words: CISCO, CCNA, Networking, routing.

INTRODUCCION

En un mundo globalizado, donde las comunicaciones y su velocidad son un factor determinante para garantizar el éxito o el fracaso de las organizaciones y sus objetivos, se hace necesario que se formen profesionales que estén a la altura del reto que la infraestructura en comunicación demanda en la actualidad.

Para las ingenierías, el área de las comunicaciones es un área esencial, razón por la cual los profesionales deben de entrenarse adecuadamente en el conocimiento, diseño e implementación de soluciones de telecomunicación, para esto, se pueden valer de herramientas del conocimiento que están en capacidad de realizar simulaciones de escenarios reales, con los cuales se genera el reto de realizar su óptima configuración y asegurar su funcionamiento ideal.

En el presente trabajo, se abordará el reto de dar solución a dos escenarios planteados referentes a redes, a los cuales se les debe realizar el análisis y configuración necesarias, garantizando la seguridad e idoneidad de la transmisión de datos a través de cada uno de los dispositivos que hagan parte de ellas, simulando así una respuesta a un posible escenario real que se pueda presentar en una organización cualquiera que enfrente el mismo reto.

DESARROLLO

Escenario 1

En el primer escenario se configuran los dispositivos de una red pequeña. Se realiza la configuración de un router, un switch y equipos que admiten tanto la conectividad IPv4 como IPv6 para los hosts soportados. Al router y el switch se les realiza la configuración para ser administrados de forma segura. CSe realiza la configuración del enrutamiento entre VLAN, DHCP, Etherchannel y port-security.

Topología

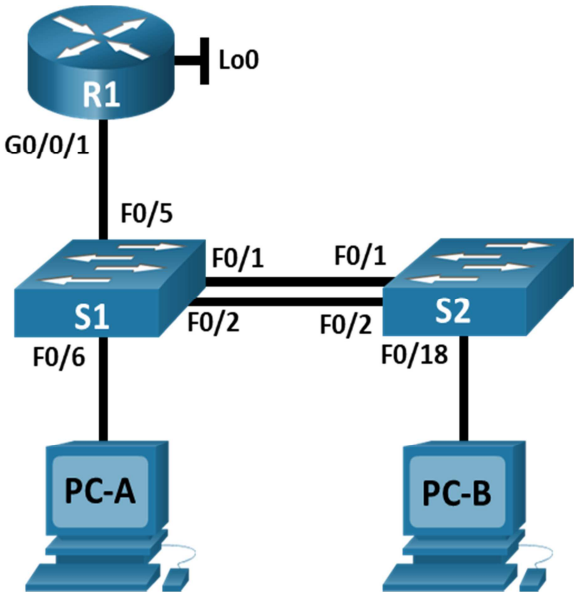


Figura 1. Topología Escenario 1

En la *Figura 1*, se aprecia la topología del escenario, configurada con un router 4331 y dos switch 3560, en el desarrollo del ejercicio se reemplazaron los switch por switch 3650 24 PS Multilayer que soportan ipv4-ipv6 sin necesidad de configuraciones adicionales. Adicionalmente se adicionan las PC de escritorio. Se realizan las conexiones automáticas del R1 al S1, de S2 a S1, de S2 a S1, así como el S1 al PC-A y el S2 al PC-B. Ahora se procede a la configuración de cada dispositivo.

Parte 1

Tabla1. Tabla de VLAN

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

Tabla 2. 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
R1 G0/0/1.3	2001:db8:acad:b: :1 /64	No corresponde
R1 G0/0/1.4	10.19.8.97 /29	No corresponde
	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
VLAN S1 4	2001:db8:acad:c: :98 /64	No corresponde
S1 VLAN 4	fe80: :98	No corresponde
S2 VLAN 4	10.19.8.99 /29	10.19.8.97
	2001:db8:acad:c: :99 /64	No corresponde

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
	fe80: :99	No corresponde
PC-A NIC	Dirección DHCP para IPv4	DHCP para puerta de enlace predeterminada IPv4
PC-A NIC	2001:db8:acad:a: :50 /64	fe80::1
PC-B NIC	DHCP para dirección IPv4	DHCP para puerta de enlace predeterminada IPv4
	2001:db8:acad:b: :50 /64	fe80::1

Tabla 3. Parte 1. Paso 1

Se inicia con la configuración inicial de router y switch, borrando cualquier configuración previa.

Parte 1. Paso 1: Inicializar y volver a cargar el router y el switch	
Descripción del paso	**Comandos utilizados**
Se realiza el borrado de las configuraciones de inicio del router y el switch y se realiza el reinicio de los dispositivos.	Router>en Router#erase startup-config Router#reload Switch>enable Switch#erase startup-config Switch#delete vlan.dat Switch#reload
Una vez se ha recargado el switch, se realiza la configuración de la plantilla SDM de manera que se garantice que se admita la conexión IPv6 cuando sea necesario, finalmente para este paso, se reinicia el switch.	Switch>enable Switch#show sdm prefer Switch#config terminal Switch(config)#sdm prefer dual-ipv4-and-ipv6 default Switch(config)#end Switch#reload Nota: Para el ejercicio práctico se utilizaron Switches 3650 24 PS Multilayer que soportan ipv4-ipv6
Se verifica el reinicio de los dispositivos	Ok

Tabla 4. Parte 1 Paso 2

Paso 2: Configurar R1	
Descripción del paso	**Comandos utilizados**
Para configurar R1, se empieza desactivando la búsqueda DNS	R1(config)#no ip domain-lookup
Se asigna el nombre “R1” al router	Router#conf ter Router(config)#hostname R1
Se establece el nombre del dominio ccna-lab.com	R1(config)#ip domain-name ccna-lab.com
Se establece “ciscoenpass” como contraseña para el modo EXEC privilegiado	R1(config)#enable secret ciscoenpass
Se establece “coscoconpass” como contraseña para el acceso a la consola	R1(config)#line console 0 R1(config-line)#password ciscoconpass R1(config-line)#login
Se determina una longitud mínima de 10 dígitos para las contraseñas	R1(config)#security passwords min-length 10
Se realiza la creación de un usuario administratico en la base de datos y se asigna la contraseña de ingreso.	R1(config)#username admin secret admin1pass
Se realiza la configuración de inicio de sesión en las líneas VTY para que use la base de datos local	R1(config)#line vty 0 15 R1(config-line)#login local
Se realiza la configuración VTY solo aceptando SSH	R1(config-line)#transport input ssh
Se configura la instrucción del crifrado de las contraseñas	R1(config)# service password-encryption
Se realiza la configuración de un mensaje de MOTD (Message of the day) en el cual se indica prevenir el acceso no autorizado.	R1(config)#banner motd #Acceso no autorizado#
Se habilita el routing IPv6	R1(config)# ipv6 unicast-routing
Se realiza la configuración de la interfaz G0/0/1 y las subinterfaces g0/0/1.2, g0/0/1.2, g0/0/1.4 y g0/0/1.6 de acuerdo a la tabla de direccionamiento.	R1(config)#interface g0/0/1.2 R1(config-subif)#encapsulation dot1q 2 R1(config-subif)#description Bikes R1(config-subif)#ip address 10.19.8.1

	255.255.255.192 R1(config-subif)#ipv6 address 2001:db8:acad:a::1/64 R1(config-subif)#ipv6 address fe80::1 link-local R1(config-subif)#interface g0/0/1.3 R1(config-subif)#encapsulation dot1q 3 R1(config-subif)#description Trikes R1(config-subif)#ip address 10.19.8.65 255.255.255.224 R1(config-subif)#ipv6 address 2001:db8:acad:b::1/64 R1(config-subif)#ipv6 address fe80::1 link-local R1(config-subif)#interface g0/0/1.4 R1(config-subif)#encapsulation dot1q 4 R1(config-subif)#description Management R1(config-subif)#ip address 10.19.8.97 255.255.255.248 R1(config-subif)#ipv6 address 2001:db8:acad:c::1/64 R1(config-subif)#ipv6 address fe80::1 link-local R1(config-subif)#interface g0/0/1.6 R1(config-subif)#encapsulation dot1q 6 native R1(config-subif)#description Native R1(config-subif)#interface g0/0/1 R1(config-if)#no shutdown
Se configura la interface Loopback0, la cual simula la conexión a internet de la red.	R1(config-if)#int loopback 0 R1(config-if)#ip address 209.165.201.1 255.255.255.224 R1(config-if)#ipv6 address 2001:db8:acad:209::1/64 R1(config-if)#ipv6 address fe80::1 link-local R1(config-if)#description Internet
Se establece una clave de cifrado RSA	R1(config)#crypto key generate rsa modulus 1024

	No soportado en Packet tracer

Tabla 5. Parte 1. Paso 3

Parte 1. Paso 3: Configure S1 y S2.	
Descripción del paso	**Comandos utilizados**
Para configurar S1 y S2 se realiza en cada uno todos los pasos descritos en esta tabla, iniciando con la desactivación de la búsqueda DNS.	S1(config)#no ip domain-lookup
Se nombra cada switch “S1” y “S2” respectivamente	Switch(config)#hostname S1 S1(config)#
Se establece el dominio ccna-lab.com	S1(config)#ip domain-name ccna-lab.com
Se establece la contraseña “ciscoenpass” como contraseña cifrada para el modo EXEC privilegiado	S1(config)#enable secret ciscoenpass
Se establece la contraseña “ciscoconpass” para el acceso a la consola	S1(config)#line console 0 S1(config-line)#password ciscoconpass S1(config-line)#login
Se realiza la creación de un usuario administrativo para la base de datos local	S1(config)#username admin secret admin1pass
Se realiza la configuración del inicio de sesión en las líneas VTY para que use la base de datos local	S1(config)#line vty 0 15 S1(config-line)#login local
Se realiza la configuración de las líneas VTY para que acepten únicamente las conexiones SSH	S1(config-line)#transport input ssh
Se procede a establecer el cifrado de las contraseñas de texto no cifrado	S1(config)# service password-encryption
Se configura un MOTD para indicar de prevenir el acceso no autorizado	S1(config)#banner motd #Acceso no autorizado#
Se define la 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] S1(config)# *mar 1 0:50:50.376: %SSH-5-ENABLED: SSH 1.99 has been enabled S1# %SYS-5-CONFIG_I: Configured from console by console
Se realiza la configuración de la interfaz de administración (SVI)	S1(config)#int vlan 4 S1(config-if)#ip address 10.19.8.98 255.255.255.248 S1(config-if)#ipv6 address 2001:db8:acad:c::98/64 S1(config-if)#ipv6 address fe80::98 link-local S1(config-if)#description Management Interface S1(config-if)#no shutdown S1(config-if)#
Se establece y se configura la puerta de enlace predeterminada	S1(config)#ip default-gateway 10.19.8.97

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

Tabla 6. Parte 2. Paso 1

Parte 2. Paso 1: Configurar S1	
Descripción del paso	**Comandos utilizados**
Se realiza la creación de todas las VLANs solicitadas y necesarias para el correcto funcionamiento de la red.	S1(config)#vlan 2 S1(config-vlan)#name Bikes S1(config-vlan)#vlan 3 S1(config-vlan)#name Trikes S1(config-vlan)#vlan 4 S1(config-vlan)# %LINK-5-CHANGED: Interface Vlan4, changed state to up S1(config-vlan)#name Management S1(config-vlan)#vlan 5 S1(config-vlan)#name Parking S1(config-vlan)#vlan 6 S1(config-vlan)#name Native S1(config-vlan)#
Se crean los enlaces troncales 802.1Q que utilizan la VLAN 6 nativa	S1(config)#int g1/0/5 S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)# %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/5, changed state to down %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/5, changed state to up %LINEPROTO-5-UPDOWN: Line

	protocol on Interface Vlan4, changed state to up S1(config-if)#switchport trunk native vlan 6 S1(config-if)#int range g1/0/1-2 S1(config-if-range)#shutdown
Se realiza la creación de un grupo de puertos EtherChannel de Capa 2 que usan interfaces F0/1 y F0/2	S1(config-if-range)#channel-group 1 mode active S1(config-if-range)# Creating a port-channel interface Port-channel 1 %EC-5-CANNOT_BUNDLE2: Gig1/0/1 is not compatible with Po1 and will be suspended (native vlan of Gig1/0/1 is 6, Po1 id 1) %EC-5-CANNOT_BUNDLE2: Gig1/0/2 is not compatible with Po1 and will be suspended (native vlan of Gig1/0/2 is 6, Po1 id 1) S1(config-if-range)#int port-channel 1 S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 6
Se procede a la configuración del puerto de acceso de servidor para VLAN 2	S1(config-if)#int g1/0/6 S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 2
Se establece el protocolo de seguridad de puerto para los puertos de acceso	S1(config-if)#switchport port-security S1(config-if)#switchport port-security maximum 3
Se realiza el apagado de todas las interfaces que no son utilizadas, lo cual también se interpreta como un proceso de seguridad pues garantiza que no	S1(config-if)#int range g1/0/3-4 S1(config-if-range)#switchport mode access

sean usadas con fines diferentes.	S1(config-if-range)#switchport access vlan 5 S1(config-if-range)#description Not In Use S1(config-if-range)#shutdown S1(config-if-range)#int range g1/0/7-24 S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 5 S1(config-if-range)#description Not In Use S1(config-if-range)#shutdown S1(config-if-range)#int range g1/1/1-4 S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 5 S1(config-if-range)#description Not In Use S1(config-if-range)#shutdown

Tabla 7. Parte 2. Paso 2.

Parte 2. Paso 2: Configure el S2.	
Descripción del paso	**Comandos utilizados**
Se realiza la creación de todas las VLANs solicitadas, de manera que se garantice la conectividad necesaria.	S2#conf t Enter configuration commands, one per line. End with CNTL/Z. S2(config)#vlan 2 S2(config-vlan)#name Bikes

	S2(config-vlan)#vlan 3 S2(config-vlan)#name Trikes S2(config-vlan)#valan 4 ^ % Invalid input detected at '^' marker. S2(config-vlan)#name Management S2(config-vlan)#vlan 5 S2(config-vlan)#name Parking S2(config-vlan)#vlan 6 S2(config-vlan)#name Native S2(config-vlan)#exit S2(config)#
Se crean los enlaces troncales 802.1Q que utilizan la VLAN 6 nativa	S2(config)#int range g1/0/1-2 S2(config-if-range)#shutdown %LINK-5-CHANGED: Interface GigabitEthernet1/0/1, changed state to administratively down %LINK-5-CHANGED: Interface GigabitEthernet1/0/2, changed state to administratively down S2(config-if-range)#switchport trunk encapsulation dot1q S2(config-if-range)#switchport mode trunk S2(config-if-range)#switchport trunk native vlan 6 S2(config-if-range)#channel-group 1 mode active S2(config-if-range)# Creating a port-channel interface Port-channel 1

	%EC-5-CANNOT_BUNDLE2: Gig1/0/1 is not compatible with Po1 and will be suspended (native vlan of Gig1/0/1 is 6, Po1 id 1) %EC-5-CANNOT_BUNDLE2: Gig1/0/2 is not compatible with Po1 and will be suspended (native vlan of Gig1/0/2 is 6, Po1 id 1) S2(config-if-range)#int port-channel 1 S2(config-if)#switchport trunk encapsulation dot1q S2(config-if)#switchport mode trunk S2(config-if)#switchport trunk native vlan 6
Se realiza la creación de un grupo de puertos EtherChannel de Capa 2 que usan interfaces F0/1 y F0/2	2(config-if-range)#channel-group 1 mode active S2(config-if-range)# Creating a port-channel interface Port-channel 1 %EC-5-CANNOT_BUNDLE2: Gig1/0/1 is not compatible with Po1 and will be suspended (native vlan of Gig1/0/1 is 6, Po1 id 1) %EC-5-CANNOT_BUNDLE2: Gig1/0/2 is not compatible with Po1 and will be suspended (native vlan of Gig1/0/2 is 6, Po1 id 1) S2(config-if-range)#int port-channel 1 S2(config-if)#switchport trunk encapsulation dot1q S2(config-if)#switchport mode trunk S2(config-if)#switchport trunk native vlan 6
Se procede a la configuración del	S2(config-if)#int g1/0/18

puerto de acceso de servidor para VLAN 3	S2(config-if)#switchport mode access S2(config-if)#switchport access vlan 3
Se establece el protocolo de seguridad de puerto para los puertos de acceso	S2(config-if)#switchport port-security S2(config-if)#switchport port-security maximum 3
Se desactivan todos los puertos de enlace no utilizados.	S2(config-if)#int range g1/0/3-17 S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 5 S2(config-if-range)#description Not In Use S2(config-if-range)#shutdown S2(config-if)#int range g1/0/19-24 S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 5 S2(config-if-range)#description Not In Use S2(config-if-range)#shutdown S2(config-if-range)#int range g1/1/1-4 S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 5 S2(config-if-range)#description Not In Use S2(config-if-range)#shutdown

3. Configurar soporte de host

Tabla 8. Parte 3. Paso 1.

Parte 3. Paso 1: Configure R1	
Descripción del paso	**Comandos utilizados**
Para continuar con la configuración de R1, se establece el routing por defecto	R1(config)#ip route 0.0.0.0 0.0.0.0 loopback 0 R1(config)#ipv6 route ::/0 loopback 0
Se realiza la configuración IPv4 DHCP para VLAN 2	R1(config)#ip dhcp excluded-address 10.19.8.1 10.19.8.52 R1(config)#ip dhcp pool VLAN2-Bikes R1(dhcp-config)#network 10.18.8.0 255.255.255.192 R1(dhcp-config)#default-router 10.19.8.1 R1(dhcp-config)#domain-name ccna-a.net
De igual manera se realiza la configuración DHCP IPv4 para VLAN 3	R1(config)#ip dhcp excluded-address 10.19.8.1 10.19.8.52 R1(config)#ip dhcp pool VLAN2-Bikes R1(dhcp-config)#network 10.18.8.0 255.255.255.192 R1(dhcp-config)#default-router 10.19.8.1 R1(dhcp-config)#domain-name ccna-a.net R1(dhcp-config)#exit R1(config)#ip dhcp excluded-address 10.19.8.65 10.19.8.84 R1(config)#ip dhcp pool VLAN3-Trikes R1(dhcp-config)#network 10.19.8.64 255.255.255.224 R1(dhcp-config)#default-router 10.19.8.65 R1(dhcp-config)#domain-name ccna-b.net R1(dhcp-config)#exit

Tabla 9. Parte 3. Paso 7.

Parte 3. Paso 2: Configurar los servidores	
PC-A Network Configuration	
Descripción	ccna-a.net
Dirección física	000C.851A.9A47
Dirección IP	10.19.8.53
Máscara de subred	255.255.255.192
Gateway predeterminado	10.19.8.1
Gateway predeterminado IPv6	FE80::1

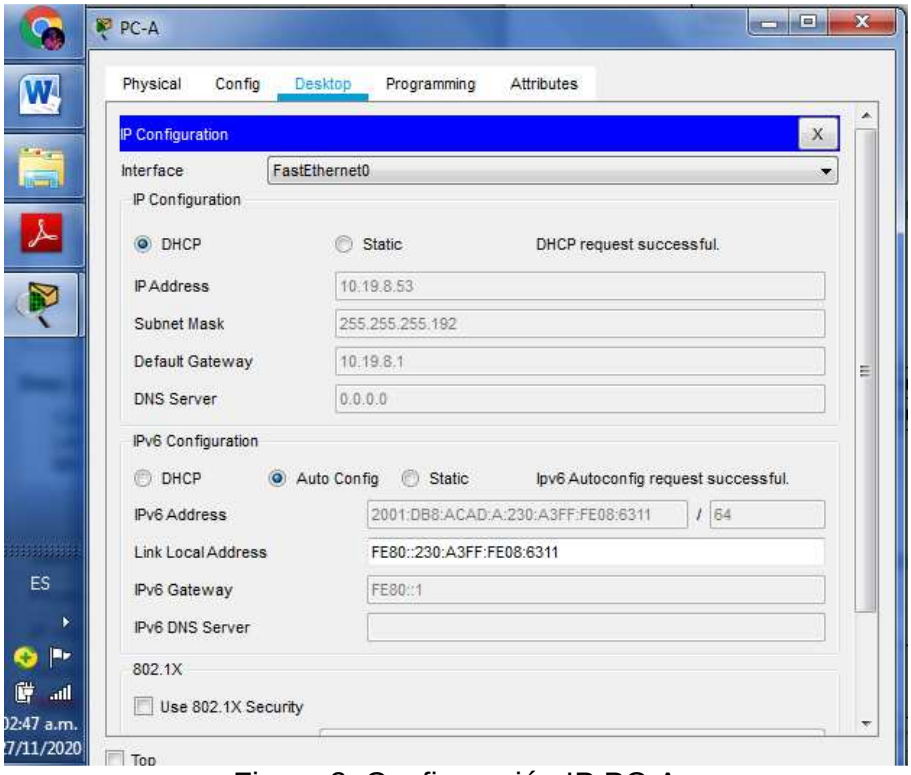
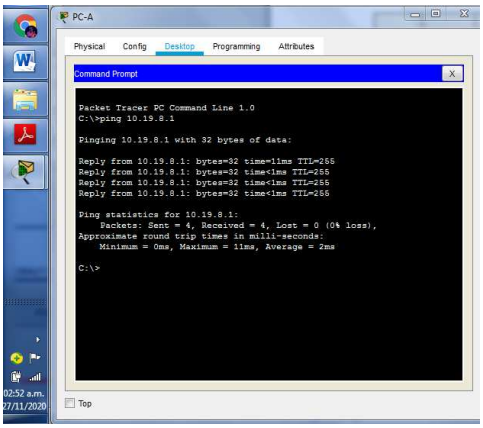
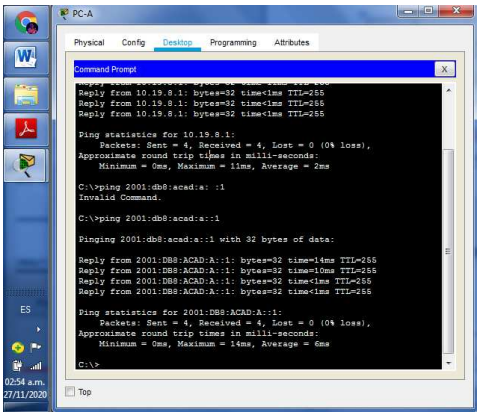


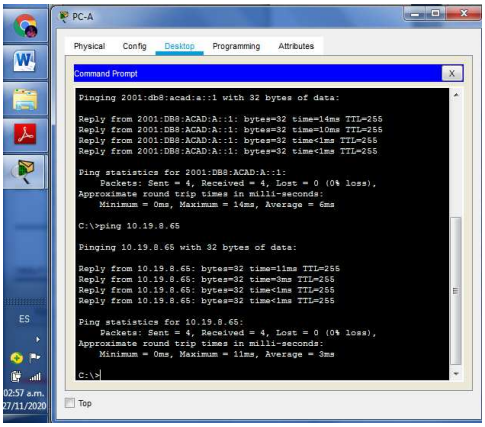
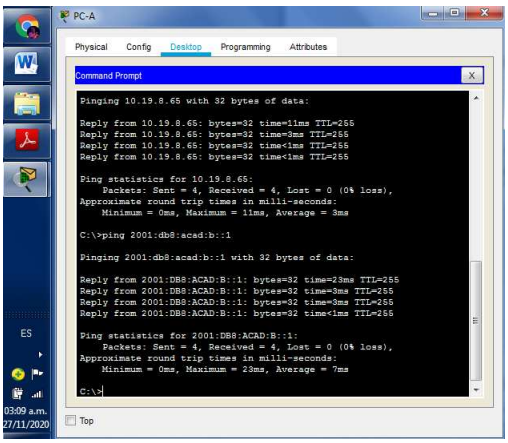
Figura 2. Configuración IP PC-A

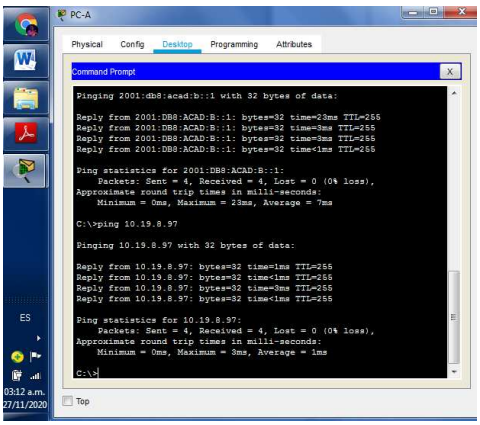
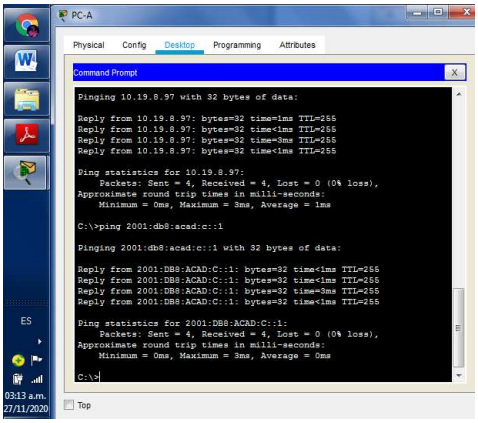
En la *Figura 2* se puede apreciar la correcta configuración del PC-A, se puede apreciar la definición automática de la dirección IP haciendo uso de DHCP para IPV4, así como la autoconfiguración para IPV6.

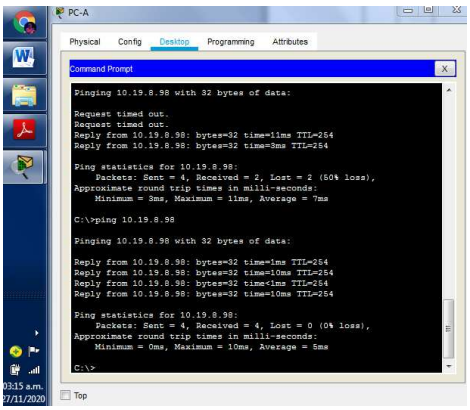
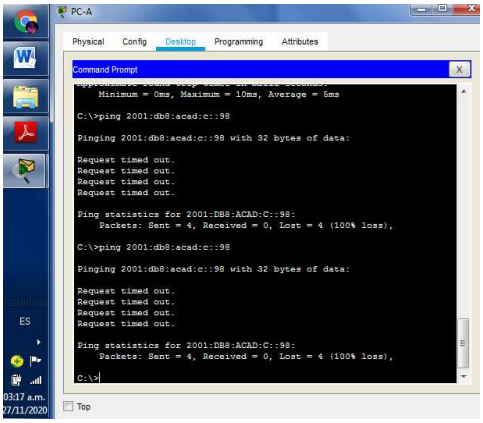
Parte 4. Probar y verificar la conectividad de extremo a extremo

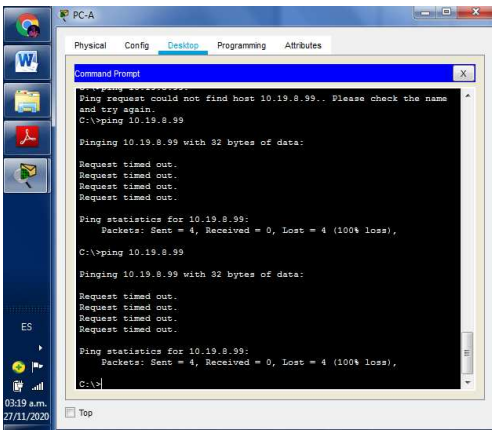
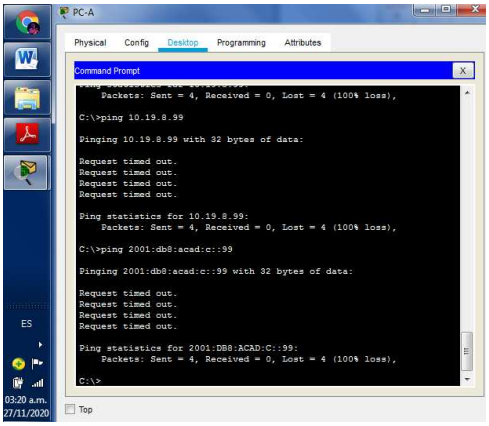
Tabla 10. Parte 4. Se realizan las pruebas de conexión utilizando el comando ping,

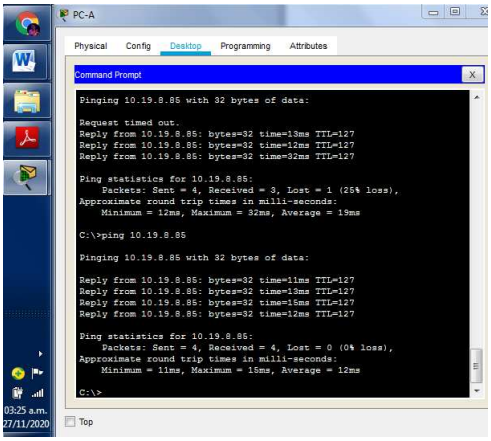
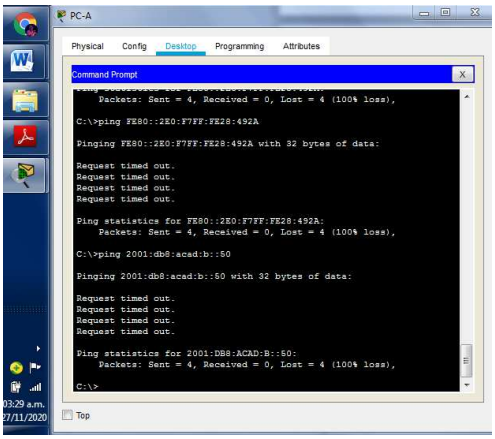
Desde	A	Internet	Dirección IP	Resultados de ping
PC-A	R1, G0/0/1.2	Dirección	10.19.8.1	*Exitoso.*  Figura 3. Ping PC-A a R1 G0/0/1.2 IPV4
		IPv6	2001:db8:acad:a::1	*Exitoso*  Figura 4. Ping PC-A a R1 G0/0/1.2 IPV6

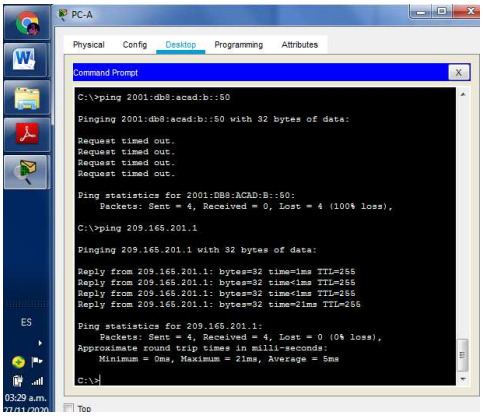
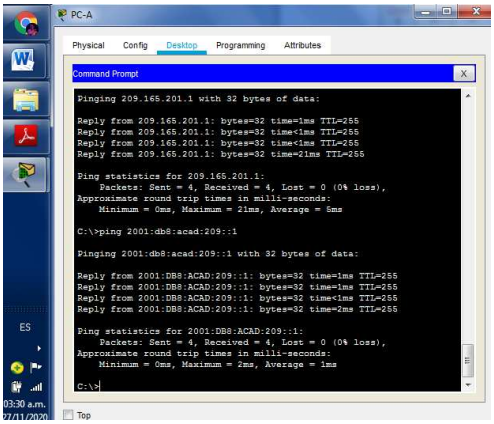
Desde	A	Internet	Dirección IP	Resultados de ping
	R1, G0/0/1.3	Dirección	10.19.8.65	*Exitoso*  Figura 5. Ping PC-A a R1 G0/0/1.3 IPV4
		IPv6	2001:db8:acad:b::1	*Exitoso*  Figura 6. Ping PC-A a R1 G0/0/1.3 IPV6

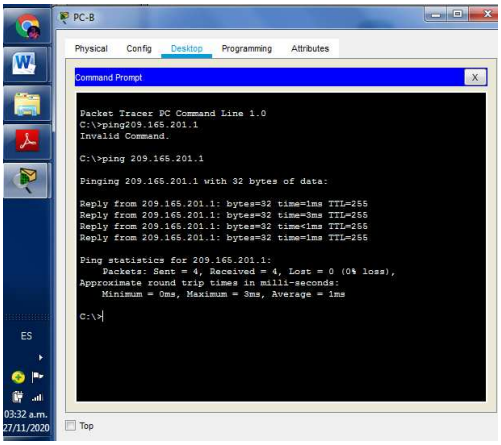
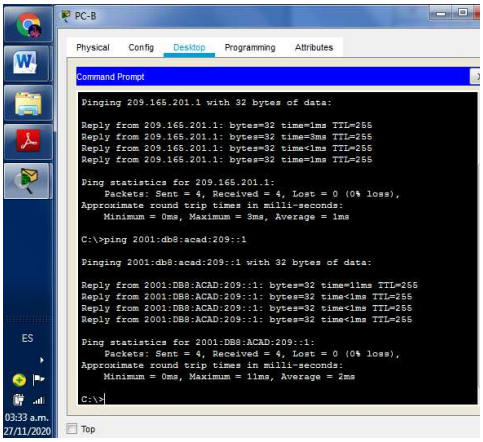
Desde	A	Internet	Dirección IP	Resultados de ping
	R1, G0/0/1.4	Dirección	10.19.8.97	*Exitoso*  Figura 7. Ping PC-A a R1 G0/0/1.4 IPV4
		IPv6	2001:db8:acad:c::1	*Exitoso*  Figura 8. Ping PC-A a R1 G0/0/1.4 IPV6

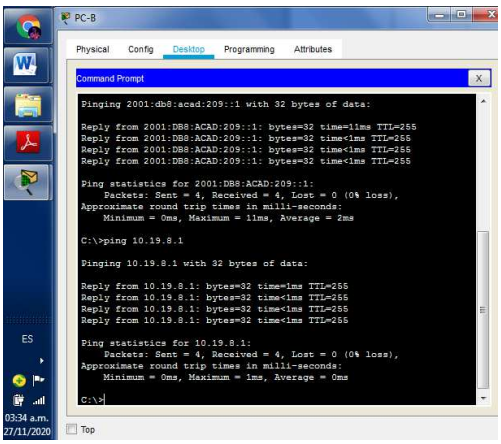
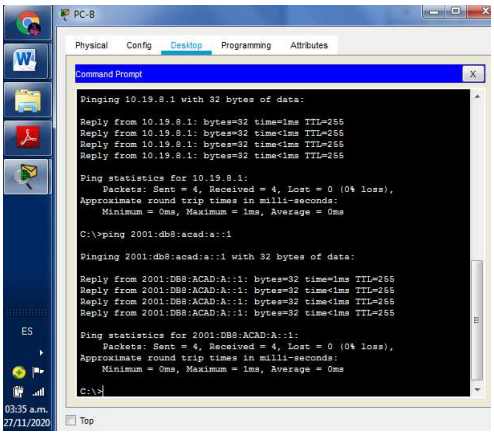
Desde	A	Internet	Dirección IP	Resultados de ping
	S1, VLAN 4	Dirección	10.19.8.98	*Exitoso*  Figura 9. Ping PC-A a S1 G0/0/1.4 IPV4
		IPv6	2001:db8:acad:c::98	*Fallido*  Figura 10. Ping PC-A a S1 G0/0/1.4 IPV6

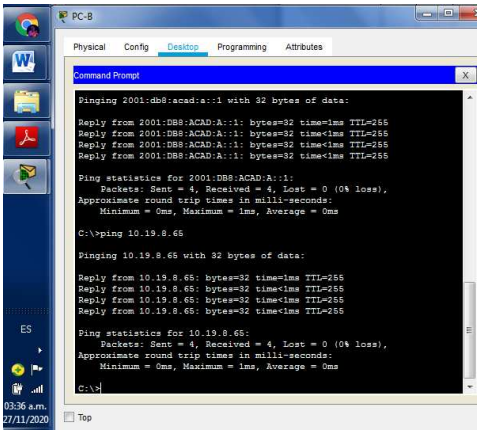
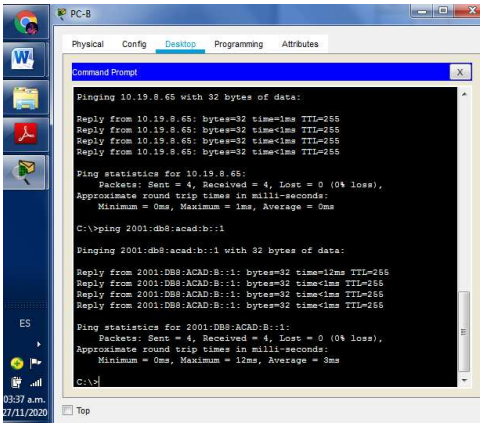
Desde	A	Internet	Dirección IP	Resultados de ping
	S2, VLAN 4	Dirección	10.19.8.99	*Fallido*  Figura 11. Ping PC-A a S2 G0/0/1.4 IPV4
		IPv6	2001:db8:acad:c::99	*Fallido*  Figura 12. Ping PC-A a S2 G0/0/1.4 IPV6

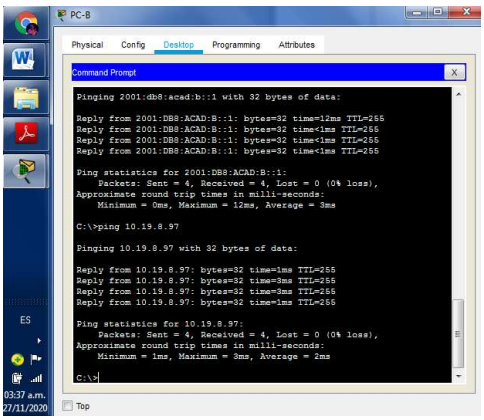
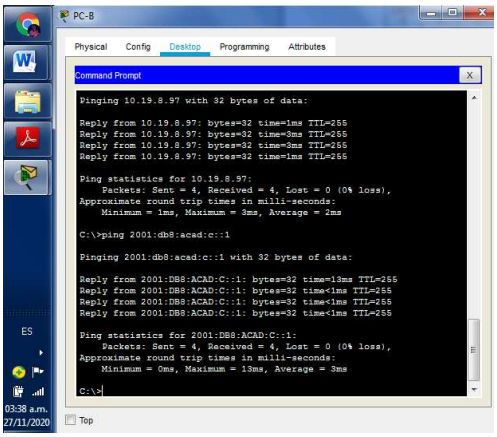
Desde	A	Internet	Dirección IP	Resultados de ping
	PC-B	Dirección	IP address will vary.	*Exitoso*  Figura 13. Ping PC-A a PC-B IVP4
		IPv6	2001:db8:acad:b::50	*Fallido.*  *Figura 14. Ping PC-A a PC-B IVP6*

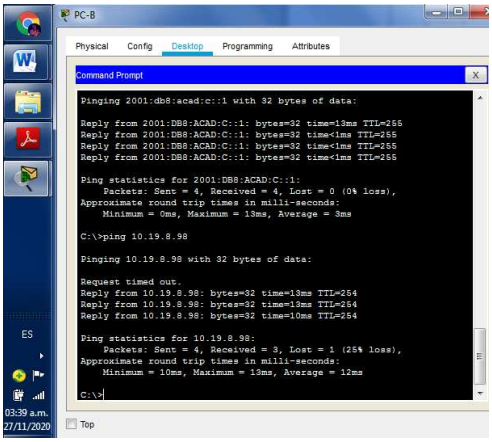
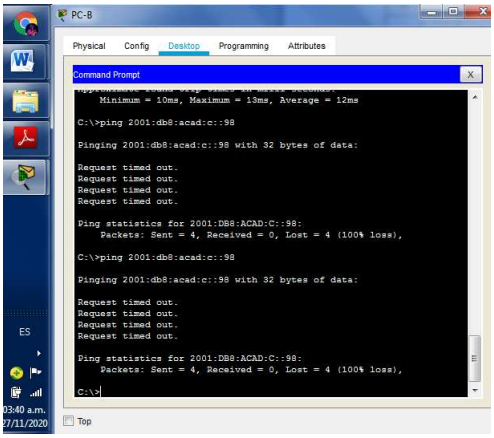
Desde	A	Internet	Dirección IP	Resultados de ping
	R1 Bucle 0	Dirección	209.165.201.1	*Exitoso.*  *Figura 15. Ping PC-A a R1 Bucle 0 IPV4*
		IPv6	2001:db8:acad:209::1	*Exitoso.*  *Figura 16. Ping PC-A a R1 Bucle 0 IPV6*

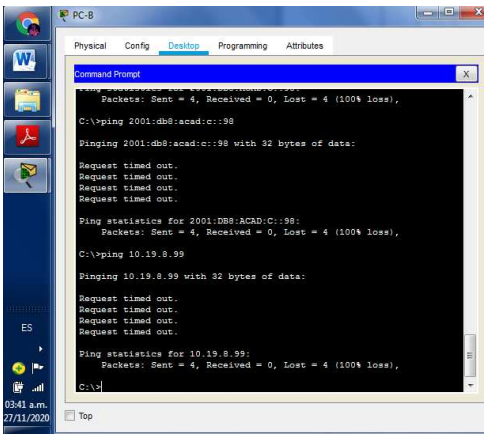
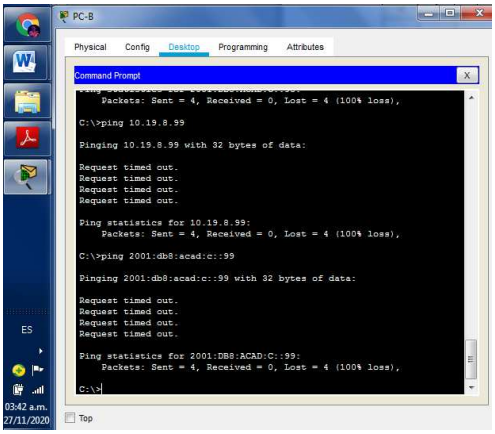
Desde	A	Internet	Dirección IP	Resultados de ping
PC-B	R1 Bucle 0	Dirección	209.165.201.1	*Exitoso.*  *Figura 17. Ping PC-B a R1 Bucle 0 IPV4*
		IPv6	2001:db8:acad:209::1	*Exitoso.*  *Figura 18. Ping PC-B a R1 Bucle 0 IPV6*

Desde	A	Internet	Dirección IP	Resultados de ping
	R1, G0/0/1.2	Dirección	10.19.8.1	*Exitoso.*  *Figura 19. Ping PC-B a R1 G0/0/1.2 IPV4*
		IPv6	2001:db8:acad:a::1	*Exitoso.*  *Figura 20. Ping PC-B a R1 G0/0/1.2 IPV6*

Desde	A	Internet	Dirección IP	Resultados de ping
	R1, G0/0/1.3	Dirección	10.19.8.65	*Exitoso.*  *Figura 21. Ping PC-B a R1 G0/0/1.3 IPV4*
		IPv6	2001:db8:acad:b::1	*Exitoso.*  *Figura 22. Ping PC-B a R1 G0/0/1.3 IPV6*

Desde	A	Internet	Dirección IP	Resultados de ping
	R1, G0/0/1.4	Dirección	10.19.8.97	*Exitoso.*  *Figura 23. Ping PC-B a R1 G0/0/1.4 IPV4*
		IPv6	2001:db8:acad:c::1	*Exitoso.*  *Figura 24. Ping PC-B a R1 G0/0/1.4 IPV6*

Desde	A	Internet	Dirección IP	Resultados de ping
	S1, VLAN 4	Dirección	10.19.8.98	*Exitoso.*  *Figura 25. Ping PC-B a S1 VLAN 4 IPV4*
		IPv6	2001:db8:acad:c::98	*Fallido.*  *Figura 26. Ping PC-B a S1 VLAN 4 IPV6*

Desde	A	Internet	Dirección IP	Resultados de ping
	S2, VLAN 4	Dirección	10.19.8.99	*Fallido.*  *Figura 27. Ping PC-B a S2 VLAN 4 IPV4*
		IPv6	2001:db8:acad:c::99	*Fallido.*  *Figura 28. Ping PC-B a S2 VLAN 4 IPV6*

Realizando el análisis a los resultados arrojados de pruebas de conectividad y detallados en la *Tabla 10*, se puede evidenciar el correcto funcionamiento de la red, ya que las pruebas de envío de paquetes son exitosas en las comunicaciones de los equipos. De acuerdo a la instrucción recibida, en los pings fallidos se procede a desactivar temporalmente el firewall de la computadora y luego se evidencian las conexiones que establecen la conectividad.

Escenario 2

Se realiza la configuración de una red pequeña que admite conectividad IPv4 e IPv6, se establece la seguridad de switches,se configura el 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), se configuran listas de control de acceso (ACL) y el protocolo de tiempo de red (NTP) servidor/cliente. En la parte de evaluación, se realizan las pruebas y registros de red usando comandos comunes de CLI.

Topología

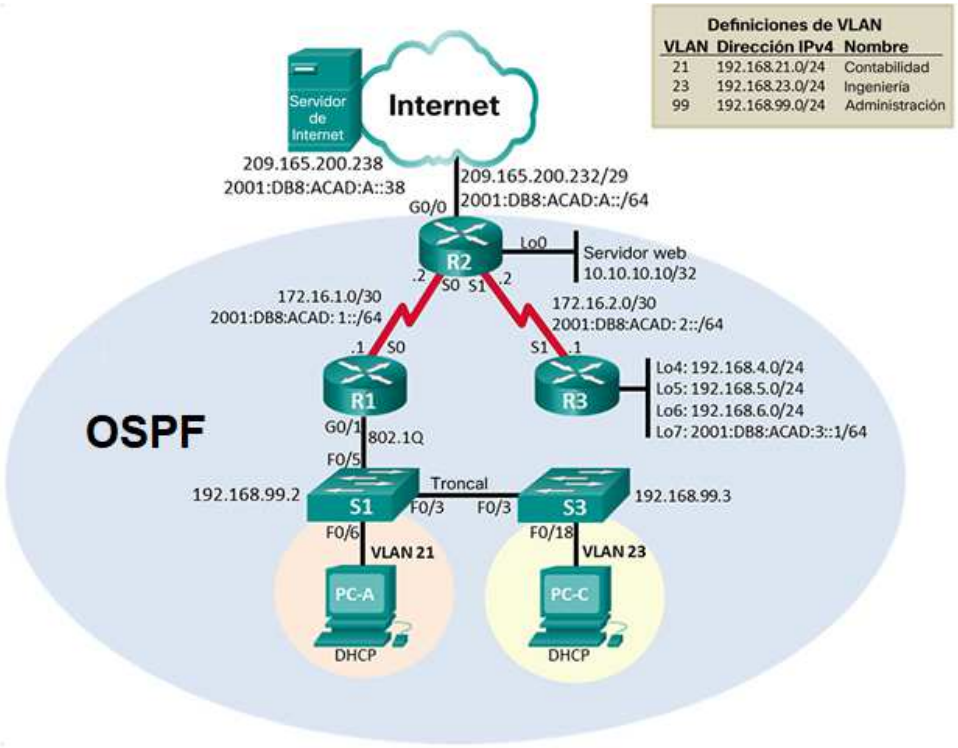


Figura 29.Topología Escenario 2.

Se procede a Inicializar dispositivos, eliminando cualquier tipo de configuración previa.

Tabla 11. Paso1.

Paso 1. Inicializar y volver a cargar los routers y los switches	
Descripción del paso	**Comandos utilizados**
Se realiza la eliminación del archivo startup-config de todos los routers	Router#erase startup-config
Se vuelven a iniciar todos los routers	Router#reload
Se realiza la eliminación del archivo startup-config de todos los switches y se elimina la base de datos de VLAN anterior	Switch#erase startup-config Switch#delete flash:vlan.dat
Se vuelven a iniciar todos los switches	Switch#reload
Se realiza la verificación de que no existe una base de datos de VLAN en la memoria.	Switch#show flash

Es necesario borrar las configuraciones previas que tengan los equipos para evitar conflictos con las configuraciones de los demás dispositivos.

Parte 1. Configurar los parámetros básicos de los dispositivos

Tabla 12. Parte 1. Paso 1

Parte 1. Paso 1. Configurar la computadora de Internet	
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.225
Dirección IPv6/subred	2001:DB8:ACAD:A::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:2::1

Tabla 13. Parte 1. Paso 2.

Parte 1. Paso 2. Configurar R1	
Descripción del paso	**Comandos utilizados**
Se realiza la desactivación de la búsqueda de DNS en el router	Router(config)#no ip domain-lookup
Se asigna el nombre del router “R1”	Router(config)#hostname R1
Se establece “class” como contraseña para acceso al modo EXEC privilegiado cifrada	R1(config)#enable secret class
Se establece la contraseña “cisco” para el acceso a la consola	R1(config)#line console 0 R1(config-line)#password cisco R1(config-line)#login
Se establece la contraseña “cisco” para el acceso a Telnet para conectarse remotamente desde otro dispositivo	R1(config)#line vty 0 4 R1(config-line)#password cisco R1(config-line)#login
Se realiza la configuración del cifrado de contraseñas	R1(config)#service password-encryption
Se establece un MOTD que prevenga el acceso no autorizado	R1(config)#banner motd #Se prohibe el acceso no autorizado#
Se realiza la configuración de la interfaz S0/0/0 Se configura el acceso mediante IPV6 Se establece la hora en el router Se activa la interfaz	R1(config)#interface serial 0/0/0 R1(config-if)#ip address 172.16.1.1 255.255.255.252 R1(config)#ipv6 unicast-routing R1(config)#interface serial 0/0/0 R1(config-if)#ipv6 address 2001:DB8:ACAD:1::1/64 R1(config-if)#clock rate 128000 R1(config-if)#no shutdown
Se establecen las rutas de acceso predeterminados	R1(config)#ip route 0.0.0.0 0.0.0.0 172.16.1.2 R1(config)#ipv6 route ::/0 2001:DB8:ACAD:1::2

Tabla 14. Parte 1. Paso 3

Parte 1. Paso 3. Configurar R2	
Para iniciar a configurar R2 se desactiva la búsqueda DNS	Router(config)#no ip domain-lookup
Se establece el nombre del router como “R2”	Router(config)#hostname R2
Se define la contraseña de acceso al modo EXEC privilegiado como “class”	R2(config)#enable secret class
Se establece la contraseña de acceso a la consola como “cisco”	R2(config)#line console 0 R2(config-line)#password cisco R2(config-line)#login
Se define la contraseña de acceso Telnet como “cisco”	R2(config)#line vty 0 4 R2(config-line)#password cisco R2(config-line)#login
Se configura la instrucción de cifrado de contraseñas	R2(config)#service password-encryption
Se realiza la habilitación del servidor HTTP	Router(config)# ip http server Router(config)# ip http secure-server Router(config)# ip http authentication local
Se configura un MOTD advirtiendo de evitar el ingreso no autorizado	R2(config)#banner motd #Se prohibe el acceso no autorizado#
Se realiza la configuración de la Interfaz S0/0/0. Se habilita la conectividad IPV6. Se enciende la interfaz	R2(config)#interface serial 0/0/0 R2(config-if)#ip address 172.16.1.2 255.255.255.252 R2(config)#ipv6 unicast-routing R2(config)#interface serial 0/0/0 R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64 R2(config-if)#clock rate 128000 R2(config-if)#no shutdown

Se realiza la configuración de la Interfaz S0/0/1. Se habilita la conectividad IPV6. Se establece la hora en el router Se enciende la interfaz	R2(config)#interface serial 0/0/1 R2(config-if)#ip address 172.16.2.2 255.255.255.252 R2(config)#ipv6 unicast-routing R2(config)#interface serial 0/0/1 R2(config-if)#ipv6 address 2001:DB8:ACAD:2::2/64 R2(config-if)#clock rate 128000 R2(config-if)#no shutdown
Se realiza la configuración de la Interfaz G0/0 la cual es utilizada para simular la conexión de internet.	R2(config)#interface G0/0 R2(config-if)#ip address 209.165.200.233 255.255.255.248 R2(config)#ipv6 unicast-routing R2(config)#interface G0/0 R2(config-if)#ipv6 address 2001:DB8:ACAD:A::32/64 R2(config-if)#no shutdown
Se configura la interfaz loopback 0, la cual simula la conexión del servidor web.	R2(config)#interface loopback 0 R2(config-if)#ip address 10.10.10.10 255.255.255.255
Se realiza la configuración del enlace predeterminado	R2(config)#ip route 0.0.0.0 0.0.0.0 209.165.200.238 R2(config)#ipv6 route ::/0 2001:DB8:ACAD:A::38

Tabla 15. Parte 1. Paso 4

Parte 1. Paso 4. Configurar R3	
Descripción del paso	**Comandos utilizados**
En R3, se desactiva la búsqueda DNS	Router(config)#no ip domain-lookup
Se establece el nombre del ruoter como “R3”	Router(config)#hostname R3
Se establece la contraseña para dar acceso al modo EXEC privilegiado	R3(config)#enable secret class
Se establece la contraseña de acceso a la consola como “cisco”	R3(config)#line console 0 R3(config-line)#password cisco R3(config-line)#login
Se establece la contraseña de acceso Telnet como “cisco”	R3(config)#line vty 0 4 R3(config-line)#password cisco R3(config-line)#login
Se configura la instrucción de cifrar las contraseñas	R3(config)#service password-encryption
Se establece un MOTD con la cual se informa de prevenir accesos no autorizados	R3(config)#banner motd #Se prohibe el acceso no autorizado#
Se realiza la configuración de la Interfaz S0/0/1 Se habilita la conectividad IPV6 Se enciende la interfaz	R3(config)#interface serial 0/0/1 R3(config-if)#ip address 172.16.2.1 255.255.255.252 R3(config)#ipv6 unicast-routing R3(config)#interface serial 0/0/1 R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64 R3(config-if)#no shutdown
Se configura la Interfaz loopback 4, se asigna dirección IP y la máscara de subred.	R3(config)#interface loopback 4 R3(config-if)#ip address 192.168.4.1 255.255.255.0

Se configura la Interfaz loopback 5, se asigna dirección IP y la máscara de subred.	R3(config)#interface loopback 5 R3(config-if)#ip address 192.168.5.1 255.255.255.0
Se configura la Interfaz loopback 6, se asigna dirección IP y la máscara de subred.	R3(config)#interface loopback 6 R3(config-if)#ip address 192.168.6.1 255.255.255.0
Se configura la Interfaz loopback 7, se asigna dirección IP y la máscara de subred.	R3(config)#interface loopback 7 R3(config-if)#ip address 2001:DB8:ACAD:3::1/64

Tabla 16. Parte 1. Paso 5

Parte 1. Paso 5. Configurar S1	
Descripción del paso	**Comandos utilizados**
Se inicia la configuración de S1 desactivando la búsqueda DNS	Switch(config)#no ip domain-lookup
Se establece el nombre del switch como “S1”	Switch(config)#hostname S1
Se configura la contraseña del modo EXEC privilegiado “class”	S1(config)#enable secret class
Se establece la contraseña “cisco” para el acceso a la consola	S1(config)#line console 0 S1(config-line)#password cisco S1(config-line)#login
Se establece la contraseña de acceso Telnet “cisco” para acceso remoto	S1(config)#line vty 0 4 S1(config-line)#password cisco S1(config-line)#login
Se realiza la instrucción de cifrado de contraseñas	S1(config)#service password-encryption
Se establece el MOTD para evitar accesos no autorizados	S1(config)#banner motd #Se prohibe el acceso no autorizado#

Tabla 17. Parte 1. Paso 6

Parte 1. Paso 6. Configurar S3	
Descripción del paso	**Comandos utilizados**
Se desactivar la búsqueda DNS en S3	Switch(config)#no ip domain-lookup
Se define el nombre del switch como “S3”	Switch(config)#hostname S3
Se configura la contraseña del modo EXEC privilegiado “class”	S3(config)#enable secret class
Se establece la contraseña “cisco” para el acceso a la consola	S3(config)#line console 0 S3(config-line)#password cisco S3(config-line)#login
Se establece la contraseña de acceso Telnet “cisco” para acceso remoto	S3(config-line)#line vty 0 4 S3(config-line)#password cisco S3(config-line)#login
Se realiza la instrucción de cifrado de contraseñas	S3(config)#service password-encryption
Se establece el MOTD para evitar accesos no autorizados	S3(config)#banner motd #Se prohibe el acceso no autorizado#

Tabla 18. Parte 1. Paso 7.

Parte 1. Paso 7. Verificar conectividad de red			
Desde	**A**	**Dirección IP**	**Resultados de ping**
R1	R2 S0/0/0	172.16.1.2 2001:DB8:ACAD:1::2	*Exitoso*
R2	R3 S0/0/1	172.16.2.1 2001:DB8:ACAD:2::1	*Exitoso*
PC de Internet	Gateway predeterminado	209.165.200.233 2001:DB8:ACAD:A::32	*Exitoso*

Se realizan las pruebas de conectividad de red con resultados exitosos en todos los casos, a continuación se evidencian mediante las figuras, las pruebas de conectividad, realizadas utilizando el comando ping.

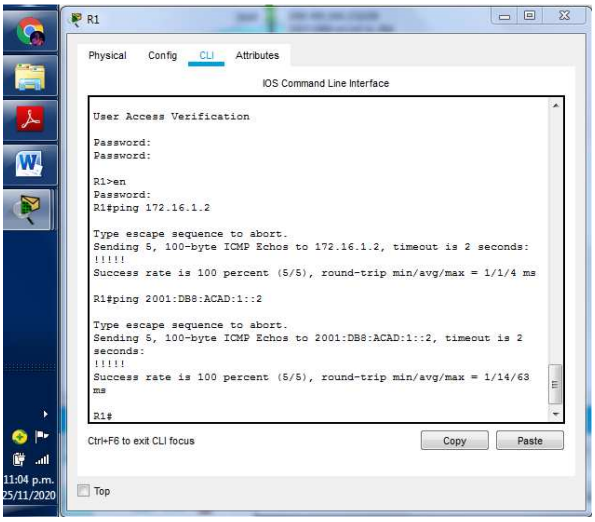


Figura. 30 Pings desde R1

En la *Figura 30,* se aprecian Pings exitosos de R1 a R2, tanto en IPV4 como IPV6.

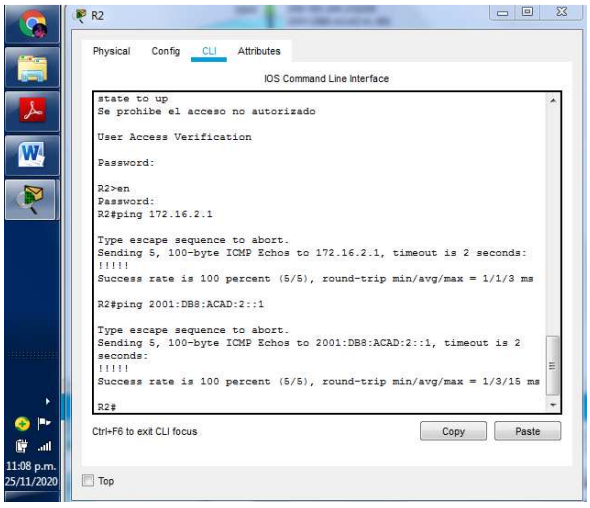


Figura 31. Pings desde R2.

En la *Figura 30,* se aprecian Pings exitosos de R2 a R3, tanto en IPV4 como IPV6.

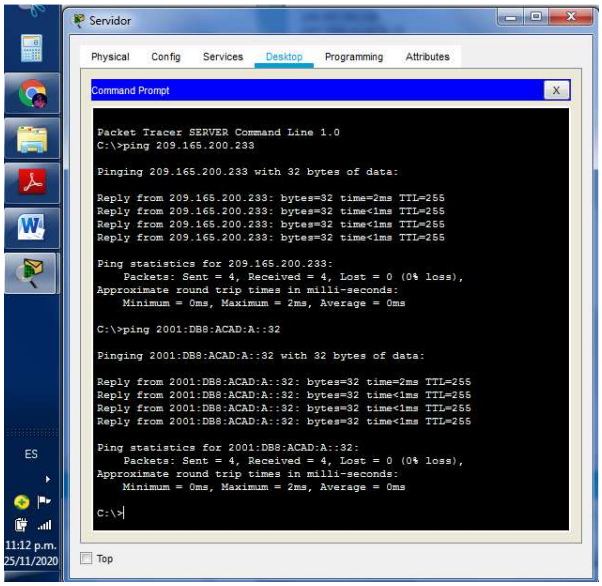


Figura 32. Pings desde Servidor

En la Figura 32, se aprecian los pings exitosos del PC de internet a la puerta de enlace predeterminada.

Parte 2. Configurar la seguridad del switch, las VLAN y el routing entre VLAN

Tabla 19. Parte 2. Paso 1.

Parte 2. Paso 1. Configurar S1	
Al configurar el S1, se empieza por crear todas las VLANs solicitadas para garantizar el correcto funcionamiento de la red.	S1(config)#vlan 21 S1(config-vlan)#name Contabilidad S1(config-vlan)#vlan 23 S1(config-vlan)#name Ingenieria S1(config-vlan)#vlan 99 S1(config-vlan)#name Administracion
Se realiza la configuración de la VLAN 99, asignando la dirección IP y definiéndola como VLAN de administración.	S1(config)#interface vlan 99 S1(config-if)#ip address 192.168.99.2 255.255.255.0

Se asigna el enlace predeterminado	S1(config)#ip default-gateway 192.168.99.1
Se realiza la configuración de la interface F0/3, estableciendo el enlace troncal	S1(config)#interface F0/3 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1
Se realiza la configuración de la interface F0/5, estableciendo el enlace troncal	S1(config)#interface F0/5 S1(config-if)#switch mode trunk S1(config-if)#switchport trunk native vlan 1
Se realiza la configuración del rango de puertos restantes como puertos de acceso	S1(config)#interface range F0/1-2, F0/4, F0/6-24 S1(config-if-range)#switchport mode access
Se realiza la asignación del enlace F0/6 a la VLAN 21	S1(config)#interface F0/6 S1(config-if)#switchport access vlan 21
Se realiza el apagado de todos los demás puertos sin usar en el dispositivo	S1(config)#interface range F0/1-2, F0/4, F0/7-24 S1(config-if-range)#shutdown

Tabla 20. Parte 2. Paso 2.

Parte 2. Paso 2. Configurar S3	
Descripción del paso	**Comandos utilizados**
Se realiza la creación de todas las VLAN solicitadas	S3(config)#vlan 21 S3(config-vlan)#name Contabilidad S3(config-vlan)#vlan 23 S3(config-vlan)#name Ingenieria S3(config-vlan)#vlan 99 S3(config-vlan)#name Administracion
Se realiza la configuración de la VLAN 99, asignando la dirección IP y definiéndola como VLAN de administración	S3(config)#interface vlan 99 S3(config-if)#ip address 192.168.99.3 255.255.255.0
Se asigna el enlace predeterminado	S3(config)#ip default-gateway 192.168.99.1

Se realiza la configuración de la interface F0/3, estableciendo el enlace troncal	S3(config)#interface F0/3 S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1
Se realiza la configuración del rango de puertos restantes como puertos de acceso	S3(config)#interface range F0/1-2, F0/4-24 S3(config-if-range)#switchport mode access
Se realiza la asignación del enlace F0/18 a la VLAN 21	S3(config)#interface F0/18 S3(config-if)#switchport access vlan 23
Se realiza el apagado de todos los demás puertos sin usar en el dispositivo	S3(config)#interface range F0/1-2, F0/4-17, F0/19-24 S3(config-if-range)#shutdown

Tabla 21. Parte 2. Paso 3.

Parte 2. Paso 3. Configurar R1	
Descripción del paso	**Comandos utilizados**
Se configura la subinterfaz 802.1Q .21 en G0/1	R1(config)#interface G0/1.21 R1(config-subif)#description accounting LAN R1(config-subif)#encapsulation dot1q 21 R1(config-subif)#ip address 192.168.21.1 255.255.255.0
Se configura la subinterfaz 802.1Q .23 en G0/1	R1(config)#interface G0/1.23 R1(config-subif)#description accounting LAN R1(config-subif)#encapsulation dot1q 23 R1(config-subif)#ip address 192.168.23.1 255.255.255.0
Se configura la subinterfaz 802.1Q .99 en G0/1	R1(config)#interface G0/1.99 R1(config-subif)#description accounting LAN R1(config-subif)#encapsulation dot1q 99 R1(config-subif)#ip address 192.168.99.1 255.255.255.0
Se realiza la activación de la interfaz G0/1	R1(config)#interface G0/1 R1(config-if)#no shutdown

Tabla 22. Parte 2. Paso 4.

Parte 2. Paso 4. Verificar conectividad de red			
Desde	**A**	**Dirección IP**	**Resultados de ping**
S1	R1, dirección VLAN 99	192.168.99.1	*Exitoso*
S3	R1, dirección VLAN 99	192.168.99.1	*Exitoso*
S1	R1, dirección VLAN 21	192.168.21.1	*Exitoso*
S3	R1, dirección VLAN 23	192.168.23.1	*Exitoso*

En la *Tabla 22* se detallan las pruebas de conectividad a realizar desde los dispositivos a cada una de las VLANs configuradas, utilizando en cada caso el comando Ping.

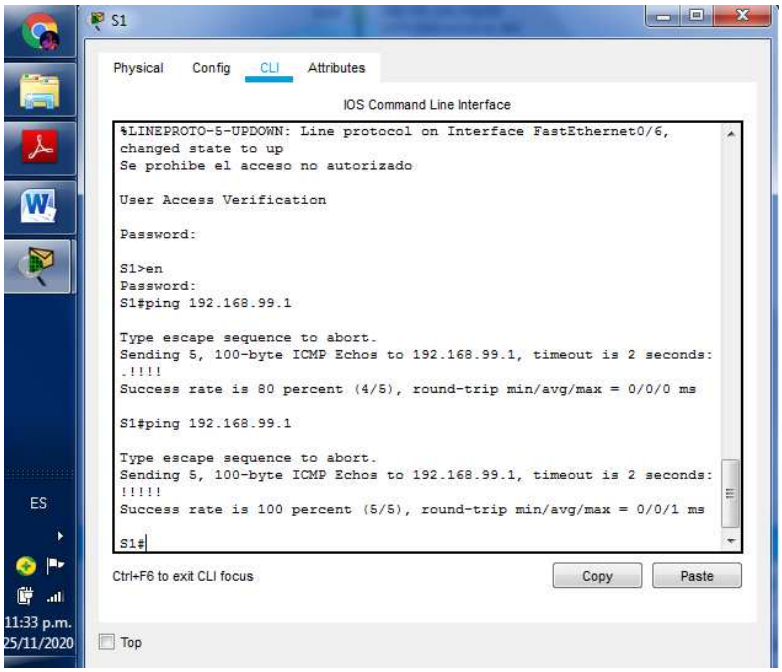


Figura 33. Ping de S1 a R1 VLAN 99

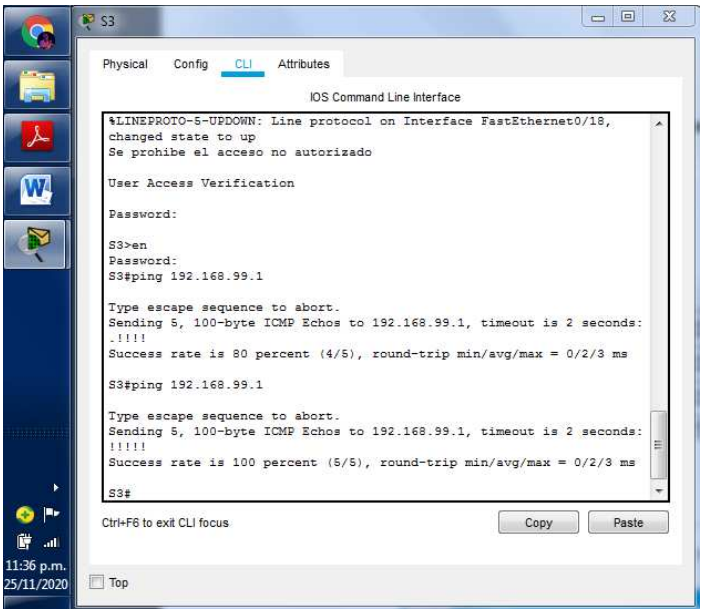


Figura 34. Ping de S3 a R1 VLAN 99

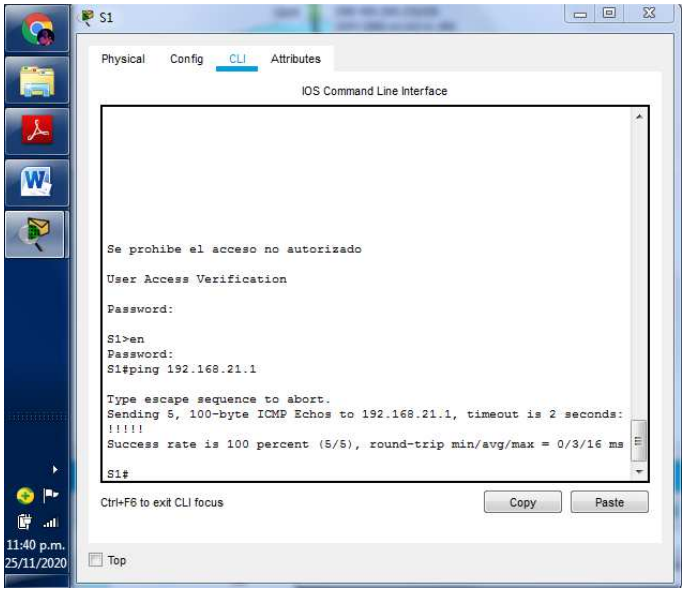


Figura 35. Ping de S1 a R1 VLAN 21

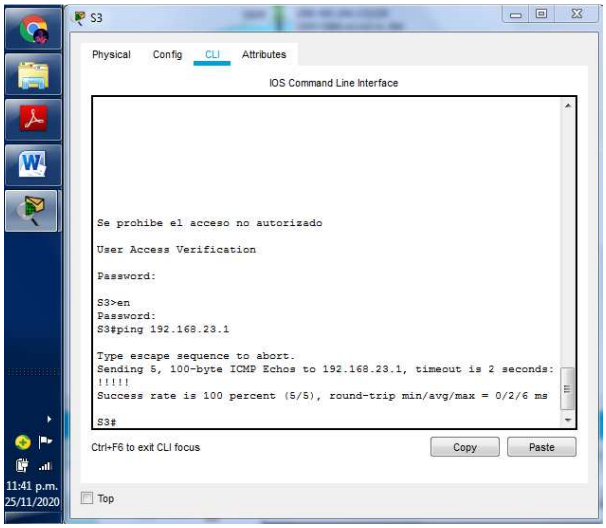


Figura 36. Ping de S3 a R1 VLAN 23

Desde la *Figura 33* a la *Figura 36*, se evidencian las pruebas exitosas de conexión detalladas en la *Tabla 22.*

Parte 3 Configurar el protocolo de routing dinámico OSPF

Tabla 23. Parte 3. Paso1.

Parte 3. Paso 1. Configurar OSPF en el R1	
Descripción del paso	**Comandos utilizados**
Se realiza la configuración OSPF área 0en el R1	R1(config)#router ospf 1
Se realiza la definición de las redes conectadas directamente	R1(config-router)#network 172.16.1.0 0.0.0.255 area 0 R1(config-router)#network 192.168.99.0 0.0.0.255 area 0
Se procede a establecer as interfaces LAN como pasivas	R1(config-router)#passive-interface default
Se realiza la desactivación de la sumarización automática, con la cual se disminuye la cantidad de entradas en las actualizaciones de enrutamiento y reduce la cantidad de entradas en las tablas de enrutamiento locales	R1(cofig-router)#no auto-summary No aplica ya que OSPF no realiza sumarización

Tabla 24. Parte 3. Paso 2.

Parte 3. Paso 2. Paso 2: Configurar OSPF en el R2	
Descripción del paso	**Comandos utilizados**
Se realiza la configuración OSPF área 0 en el R2	R2(config)#router ospf 1
Se realiza la definición de las redes conectadas directamente	R2(config-router)#network 172.16.1.0 0.0.0.255 area 0 R2(config-router)#network 172.16.2.0 0.0.0.255 area 0
Se establece la interfaz LAN (loopback) como pasiva	R2(config-router)#passive-interface loopback 0
Se realiza la desactivación de la sumarización automática.	R2(config-router)#no auto-summary

Tabla 25. Parte 3 Paso 3.

Parte 3. Paso 3. Configurar OSPFv3 en el R3	
Descripción del paso	**Comandos utilizados**
Se realiza la configuración OSPFv3 área 0 en el R3	R3(config)#router ospf 3
Se realiza la definición de las redes IPv4 conectadas directamente	R3(config-router)#network 172.16.2.0 0.0.0.255 area 0
Se establece 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
Se realiza la desactivación de la sumarización automática.	R3(config-router)#no auto-summary

Tabla 26. Parte 3. Paso 4.

Parte 3. Paso 4. Verificar información de OSPF	
Pregunta	**Respuesta**
¿Con qué comando se muestran la ID del proceso OSPF, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router?	Router#show ip protocols
¿Qué comando muestra solo las rutas OSPF?	Router#show ip ospf database
¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	Router#show running-config

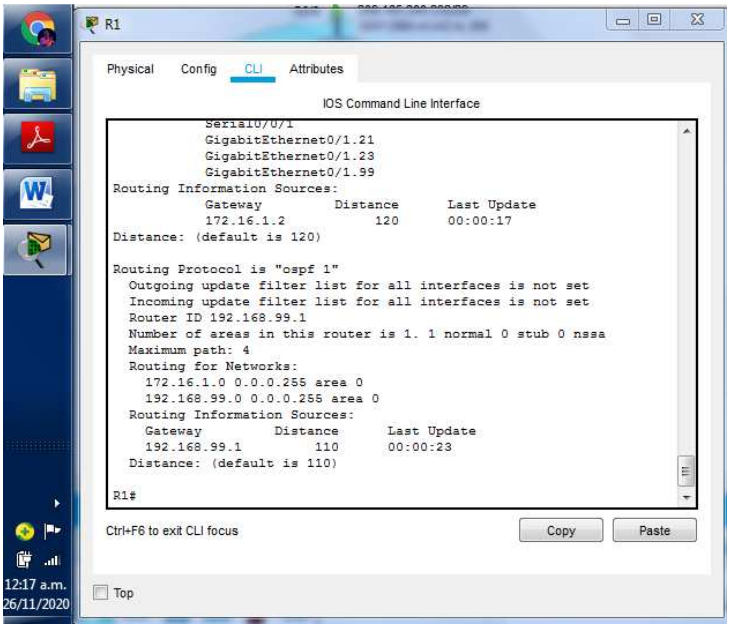


Figura 37. Comando show ip protocols en R1

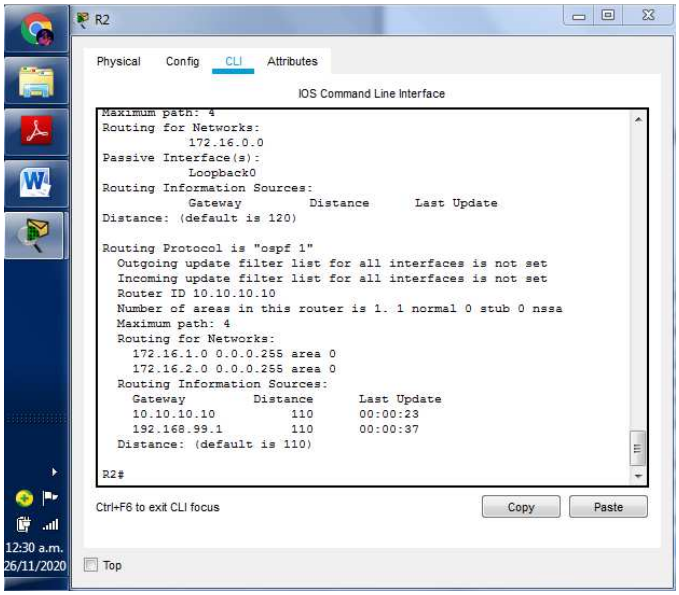


Figura 38. Comando show ip protocols en R2

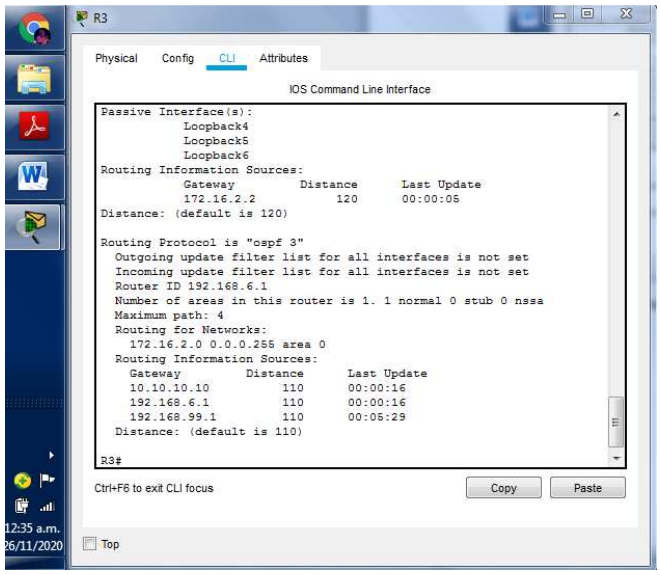


Figura 39. Comando show ip protocols en R3

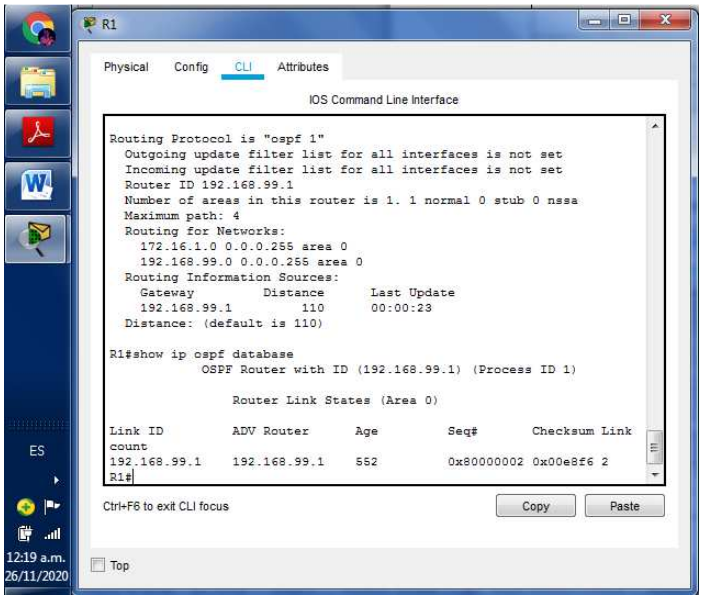


Figura 40. Comando show ip ospf database en R1

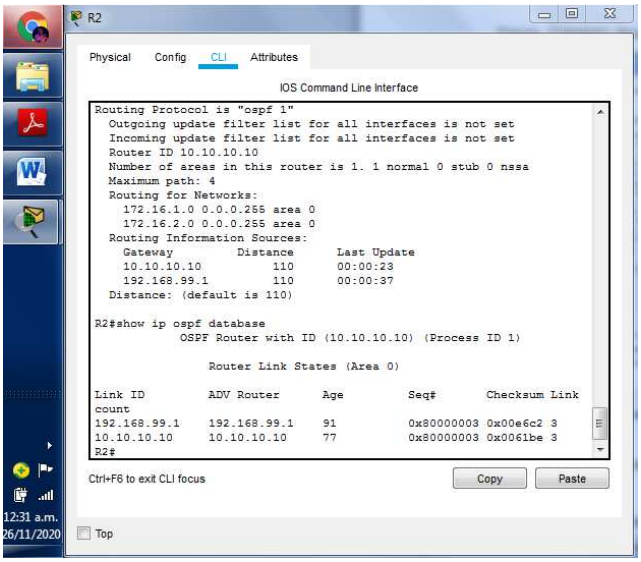


Figura 41. Comando show ip ospf database en R2

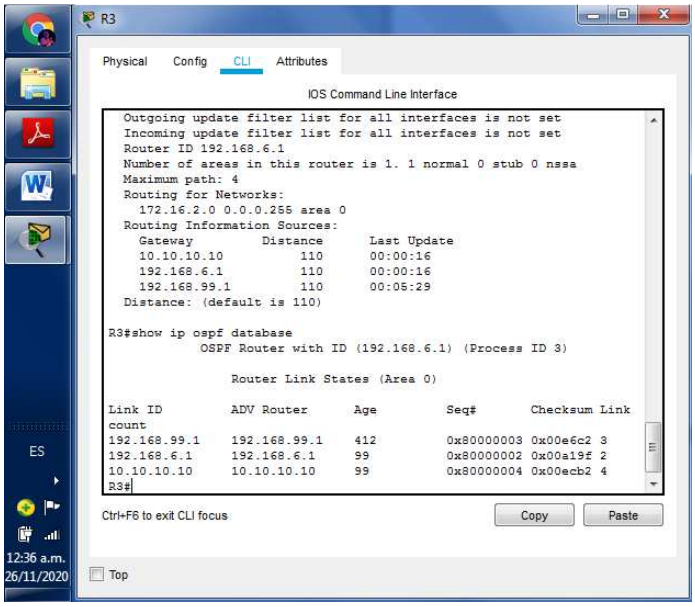


Figura 42. Comando show ip ospf database en R3

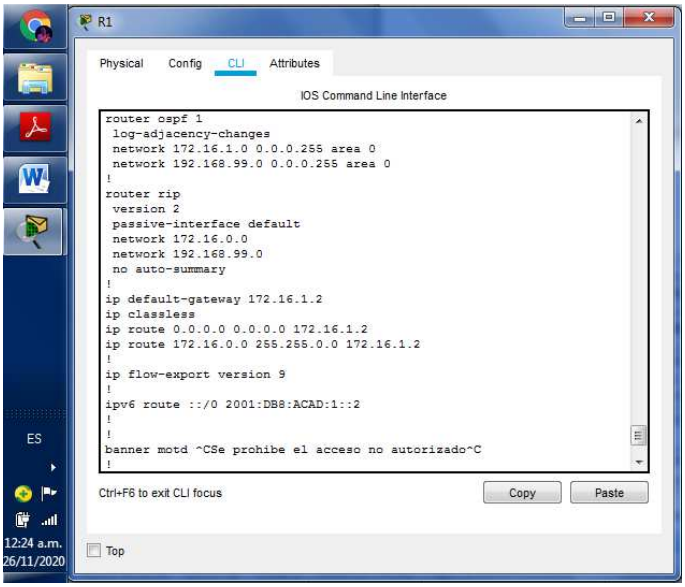


Figura 43. Comando show running-config en R1

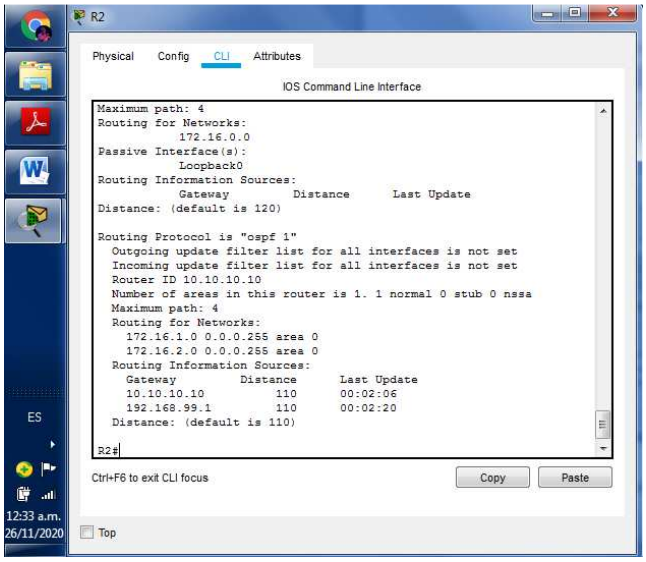


Figura 44. Comando show ip protocols en R2

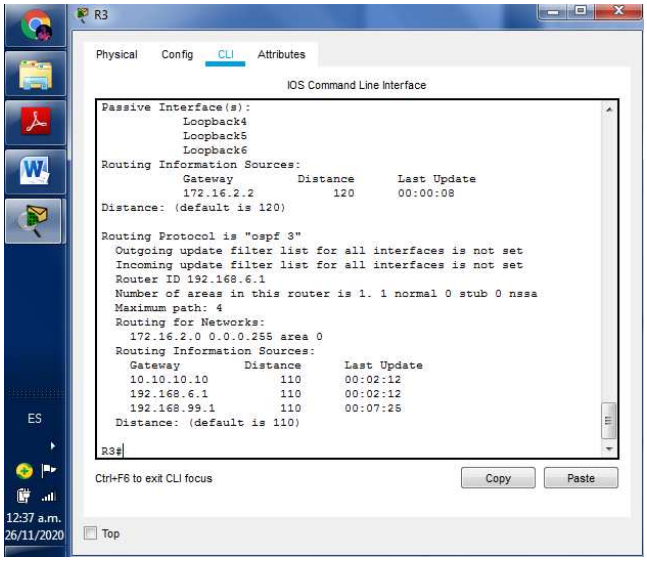


Figura 45. Comando show ip protocols en R3

Desde la *Figura 37* a la *Figura 45*, se evidencia la correcta configuración del protocolo OSPF el cual busca que el router defina el camino más corto para la conexión entre dos dispositivos conectados.

Parte 4 Implementar DHCP y NAT para IPv4

Tabla 27. Parte 4. Paso 1

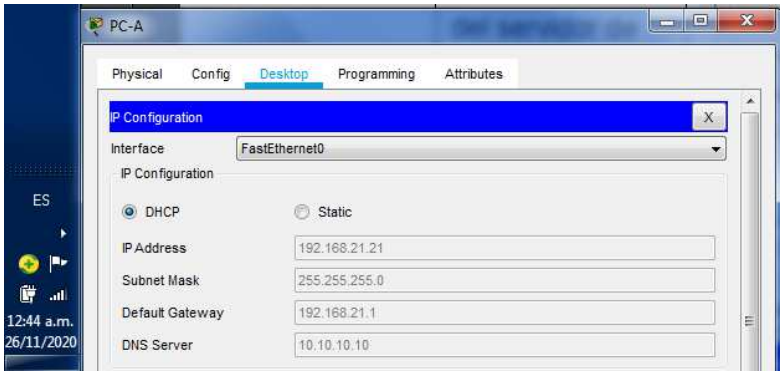
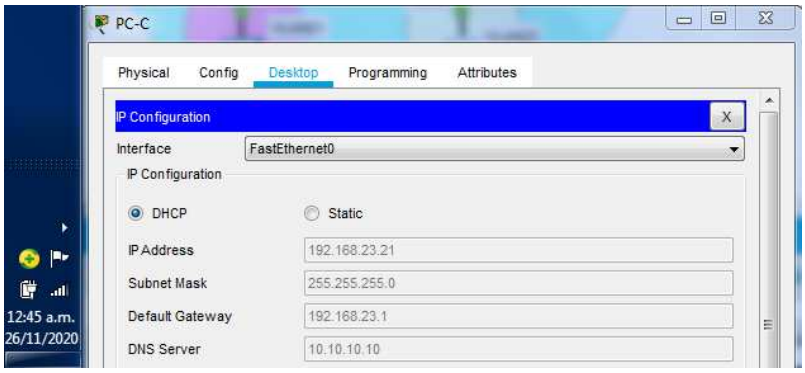
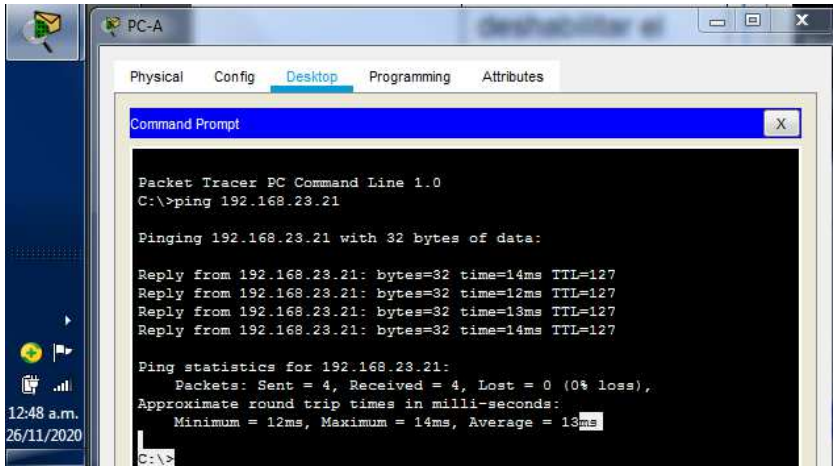
Parte 4. Paso 1. Implementar DHCP y NAT para IPv4	
Descripción del paso	**Comandos utilizados**
Se reservan las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20
Se reservan las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20
Se crear un pool de DHCP para la VLAN 21.	R1(dhcp-config)#ip dhcp pool ACCT R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com R1(dhcp-config)#default-router 192.168.21.1
Se crea un pool de DHCP para la VLAN 23	R1(config)#ip dhcp pool ENGNR R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com R1(dhcp-config)#default-router 192.168.23.1

Tabla 28. Parte 4. Paso 2.

Parte 4. Paso 2. Configurar la NAT estática y dinámica en el R2	
Se crea una base de datos local, con una cuenta de usuario para acceso en el servidor web	R2(config)#user webuser privilege 15 secret cisco12345
Se habilita el servicio del servidor HTTP	R2(config)#ip http server
Se realiza la configuración del servidor HTTP para utilizar la base de datos local para la autenticación	R2(config)#ip http autentication local
Se crea una NAT estática al servidor web.	R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229

Se realiza la configuración de la interfaz interna y externa para la NAT estática	R2(config)#interface G0/1 R2(config-if)#ip nat outside R2(config-if)#interface G0/0 R2(config-if)#ip nat inside
Se realiza la configuración de 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
Se define el grupo de direcciones IP públicas utilizables.	R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248
Se define la traducción de NAT dinámica	R2(config)#ip nat inside source list 1 pool INTERNET

Tabla 29. Parte 4. Paso 3

Parte 4. Paso 3. Verificar el protocolo DHCP y la NAT estática	
Prueba	**Resultados**
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	 Figura 46. DHCP en PC-A
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	 Figura 47. DHCP en PC-C
Verificar que la PC-A pueda hacer ping a la PC-C	 Figura 48. Ping desde PC-A a PC-C

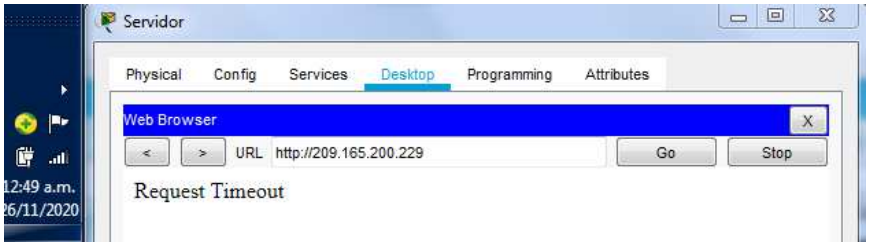
Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.229) Iniciar sesión con el nombre de usuario **webuser** y la contraseña **cisco12345**	 Figura 49. Intento de acceso al servidor web. No fue posible ya que en Packet tracer no está soportada la función ip http server.

Tabla 30. Parte 5.

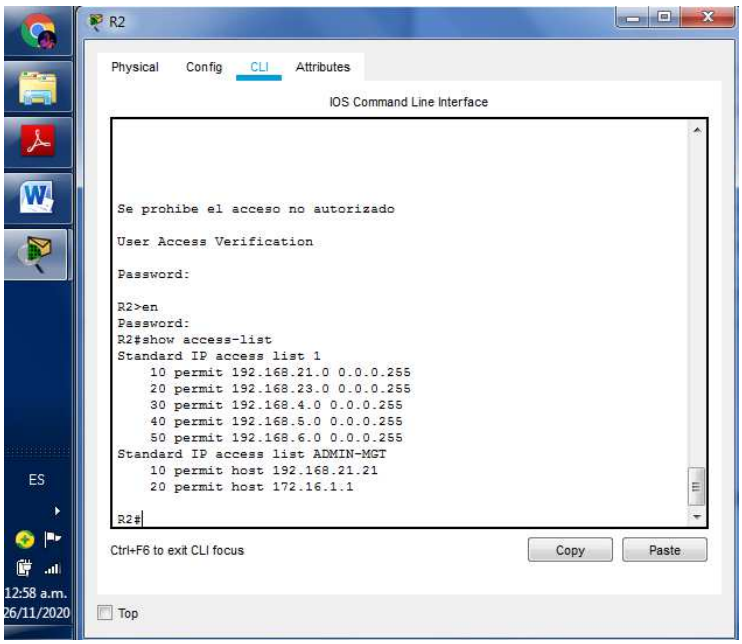
Parte 5. Configurar NTP	
Elemento o tarea de configuración	**Especificación**
Se realiza la configuración de la fecha y hora en R2.	R2#clock set 09:00:00 5 mar 2016
Se realiza la configuración de R2 como un maestro NTP.	R2(config)#ntp master 5
Se realiza la configuración de R1 como un cliente NTP.	R1(config)#ntp server 172.16.1.2
Se realiza la configuración de R1 de manera que se realicen actualizaciones de calendario y periódicas con hora NTP.	R1(config)#ntp update-calendar
Se realiza que no exista la configuración de NTP en R1.	R1#show ntp associations

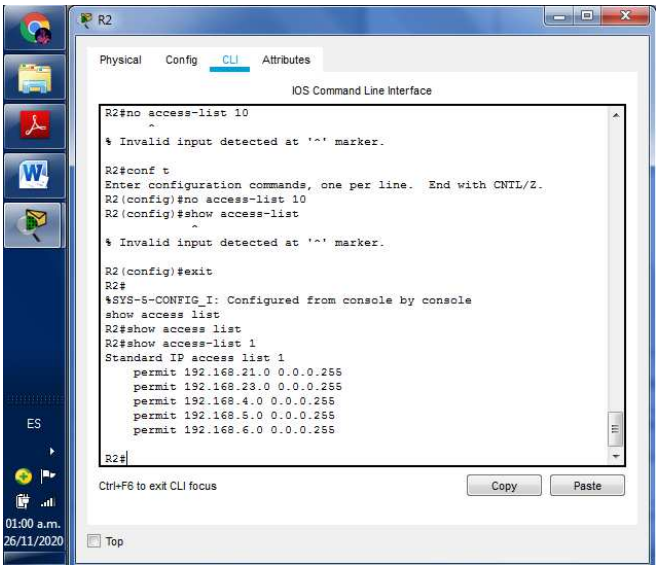
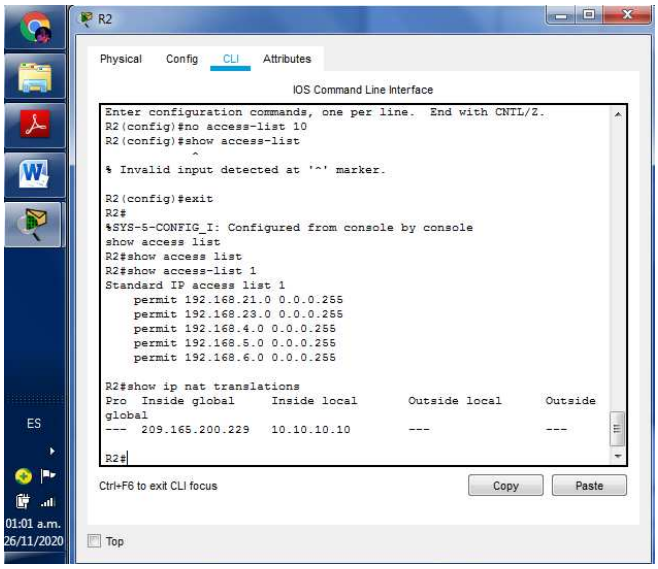
Parte 6. Configurar y verificar las listas de control de acceso (ACL)

Tabla 31. Parte 6. Paso 1.

Parte 6. Paso 1. Restringir el acceso a las líneas VTY en el R2	
Descripción del paso	**Comandos utilizados**
Se realiza la configuración de una lista de acceso 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
Se aplica la ACL con nombre a las líneas VTY	R2(config)#line vty 0 4
Se garantiza que se permita el acceso acceso por Telnet a las líneas de VTY	R2(config-line)#access-class ADMIN-MGT in
Se realiza la verificación para que la ACL funcione como se pretende.	R1#telnet 172.16.1.2

Tabla 32. Parte 6. Paso 2.

Parte 6. Paso 2. Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente	
Descripción del paso	**Comandos utilizados**
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	R2#show access-list  Figura 50. Comando show Access-list en R2
Se reestablecen los contadores de una lista de acceso	R2(config)#no access-list 10

Se evidencia que ACL se aplica a una interfaz, especificando la dirección en que se aplica.	R2#show access-list 1  Figura 51. Comando no Access-list y show access-list 10 en R2
Se evidencian las traducciones NAT	R2#show ip nat translations  Figura 52. Comando show ip nat translations en R2
Se intenta eliminar las traducciones de NAT dinámicas.	R2# clear ip nat translation *config terminal no ip nat pool old pool nameip nat pool new pool. Esta opción no fue eficaz en el packet tracer.

CONCLUSIONES

En el escenario 1, se pudo hacer uso del conocimiento adquirido durante el periodo lectivo, planteando un uso práctico del mismo y evidenciando una comprensión adecuada de los temas tratados en el diplomado, se pudieron realizar diversos análisis sobre protocolos y métricas de enrutamiento.

En el escenario 1, se pusieron en práctica las técnicas y estrategias utilizadas para dar solución a lo planteado, realizando un diseño, configuración de red y pruebas posteriores que garantizaron el correcto funcionamiento de acuerdo a cada necesidad y protocolo de seguridad aplicado.

En el Escenario 2 se hizo uso de los comandos necesarios para realizar las configuraciones de los dispositivos dentro de la red sugerida, se realizaron pruebas exitosas de funcionamiento, control y corrección de posibles errores.

En ambos escenarios se diseñaron políticas de enrutamiento estático y dinámico, para dar soluciones de conectividad a dispositivos como switches y routers que fueron configurados de manera que cumplieran su propósito en ambientes LAN y WAN.

BIBLIOGRAFIA

Julián Pérez Porto y María Merino. Publicado: 2015. Actualizado: 2017. [online]

Definicion.de: Definición de VLAN (https://definicion.de/vlan/)

SOLUTECSA. Glosario de Internet e informática. [online] Recuperado de:

https://www.internetglosario.com/1135/ACL.html

CISCO. Soporte y descargas. [online] Recuperado de: https://www.cisco.com/c/es_mx/support/index.html

TO, 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-consolaauxiliar-y-telnet/

CISCO. Networking Academy. Recuperado de: https://www.netacad.com/es

Byspel, B. (2017, 14 junio). Configurar servidor DHCP en Packet Tracer. [online] Recuperado de:

https://byspel.com/configurar-servidor-dhcpen-cisco-packet-tracer

Enrutamiento Dinámico CISCO. (2014). Enrutamiento Dinámico. Principios de

Enrutamiento y Conmutación. [online] Recuperado de https://staticcourseassets.

s3.amazonaws.com/RSE50ES/module7/index.html#7.0.1.1

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

ANEXOS

Anexo 1
Enlace de descarga y consulta de archivo en Packet Tracer del Escenario 1, alojado en Google Drive: (Por favor copiar y pegar en el navegador)
https://drive.google.com/file/d/1WxEQ65dgmd4ybzr2p4LXQXDBtwwk70t4/view?usp=sharing

Anexo 2
Enlace de descarga y consulta de archivo en Packet Tracer del Escenario 2, alojado en Google Drive: (Por favor copiar y pegar en el navegador)
https://drive.google.com/file/d/1ld7nOZLy52nF01x3Cz-fvEVQDLWzcIbe/view?usp=sharing

Anexo 3
Enlace de descarga y consulta de archivo con el artículo científico "IEEE Marcel_Giovanny_Herrera_Reyes", alojado en Google Drive: (Por favor copiar y pegar en el navegador)
https://drive.google.com/file/d/1cfcbbvRvMlRs0F8SoSMWYCTSvn0ERzXT/view?usp=sharing