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

EDGAR ENRIQUE DUQUE ACOSTA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD)
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA (ECBTI)
INGENIERÍA ELECTRÓNICA
BARRANQUILLA
2020

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

EDGAR ENRIQUE DUQUE ACOSTA

DIPLOMADO DE OPCIÓN DE GRADO PRESENTADO PARA OPTAR EL TÍTULO DE INGENIERO ELECTRONICO

TUTOR
ING. DIEGO EDINSON RAMIREZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA (ECBTI)
INGENIERIA ELECTRONICA
BARRANQUILLA
2020

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Barranquilla Atlántico, Diciembre 2020

DEDICATORIA

Quiero dar gracias a Dios por permitirme culminar esta etapa de mi vida. A mi esposa Mary Luz Ramírez por brindarme su incondicional apoyo y compresión y a mis hijos Edgar Junior Duque Ramírez y Sebastián Fernando Duque Ramírez, quien han sido mi mayor motivación para nunca rendirme en este proceso y poder llegar a ser un ejemplo para ellos.

A mis Padres Fernando Duque y Leonor Acosta de Duque por haberme forjado como la persona que soy en la actualidad.

A todos los tutores de la UNAD que hicieron parte durante mi proceso académico, les doy muchas gracias por haberme compartido sus conocimientos y sabiduría.

CONTENIDO

LISTA DE TABLA

TABLA DE FIGURAS

GLOSARIO

VLAN: (Redes de área local virtual) son redes lógicas independientes dentro de una misma red física.

DHCP: Es un protocolo de configuración dinámica el cual un servidor DHCP asigna dinámicamente una dirección IP, mascara de red y Gateway predeterminado a un host.

OSPF: Es un protocolo de enrutamiento sin clase que utiliza el concepto de áreas para realizar la escalabilidad, desarrollado como reemplazo del protocolo de routing vector distancia RIP.

EtherChannel: Es una tecnología que permite que dos o más puertos físicos se combinen en un puerto lógico que proporciona alta disponibilidad y mayor ancho de banda.

Loopback: Es una interfaz lógica interna del router. Y no se asigna a ningún puerto físico y siempre está activa

RESUMEN

En este trabajo de prueba de habilidades de CISCO se presentará el desarrollo de dos escenarios de entornos de red corporativos donde se analizan y se aplican las soluciones en base a los conceptos adquiridos durante las actividades de laboratorio en el diplomado de profundización CCNA, teniendo en cuenta las topologías de los escenarios se configuran los dispositivos de red, Router y Switch dando solución a los requerimientos de cada uno de los puntos. También se aplicarán los protocolos de comunicación y enrutamiento necesarios para su buen funcionamiento y se simularán los escenarios en Packet Tracer para verificar su conectividad y la seguridad de la red.

Palabras Clave: CISCO, CCNA, Enrutamiento, Conectividad

ABSTRACT

In this CISCO skills test work, the development of two scenarios of corporate network environments will be presented where solutions are analyzed and applied based on the concepts acquired during the laboratory activities in the CCNA deepening diploma, taking into account the topologies of the scenarios are configured the network devices, Router and Switch giving solution to the requirements of each of the points. The communication and routing protocols necessary for its proper operation will also be applied and the scenarios will be simulated in Packet Tracer to verify its connectivity and the security of the network.

Keywords: CISCO, CCNA, Routing, Connectivity

INTRODUCCION

Para esta actividad Pruebas de habilidades del diplomado de profundización Cisco, se realizará dos escenarios, los cuales se deben desarrollar y simular en packet tracer, estos dos escenarios tienen como objetivo la adquisición de habilidades para el acceso y configuración de switch y router.

En el escenario 1 se aplicará los conceptos visto durante los cursos CCNA1 introducción a las redes y configurar una red para que admita conectividad IPv4 e IPv6, seguridad de switch y router, aplicación de EtherChannel en la conexión entre switch para aumentar el ancho de banda y mejorar su disponibilidad.

Escenario 2 se aplicará los conceptos vistos en CCNA 2 Routing and Switching, se configurar el protocolo de routing dinámico OSPF para mejora la escalabilidad de la red, se configura protocolo de configuración de hosts dinámicos (DHCP) para para ahorrar tiempo de gestión de red, 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 para resistir los efectos de latencia variable.

OBJETIVO GENERAL

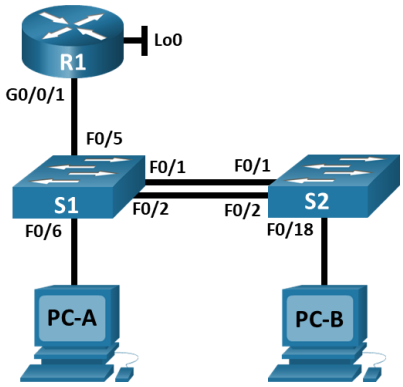
Analizar y configurar los dispositivos de red de los escenarios 1 y 2 aplicando los conocimientos adquiridos durante el diplomado de profundización CCNA. Dando solución a los requerimientos de enrutamiento y conectividad de la red.

OBJETIVOS ESPECIFICOS

- Realizar el análisis y la configuración necesaria para desarrollar los escenarios de la prueba de facilidades.
- Simular los escenarios propuestos en programa Packet Tracer
- Configurar e interconectar los diferentes dispositivos que hacen parte de la topología de red de los escenarios y que admitan enrutamiento de IPV4 e IPv6
- Comprobar el funcionamiento de la red de los escenarios propuestos
- Realizar enlaces troncales Vlan aplicando LACP para controlar los enlaces en forma de EtherChannel para incrementar el ancho de banda y el mejoramiento de la disponibilidad.

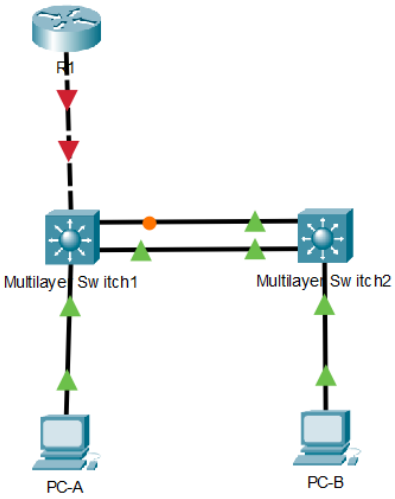
Escenario 1

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.

Figura 2. Topología creada Escenario 1



Fuente: Autor

En la siguiente topología se escogió los switch 3560 de 24 puertos ya que en el escenario se solicita que se admitan conectividad IPv4 como IPv6 capa 3

Tabla 1. Vlan escenario 1

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

Tabla 2. Direccionamiento IPv4 IPv6 del escenario 1

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

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
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

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

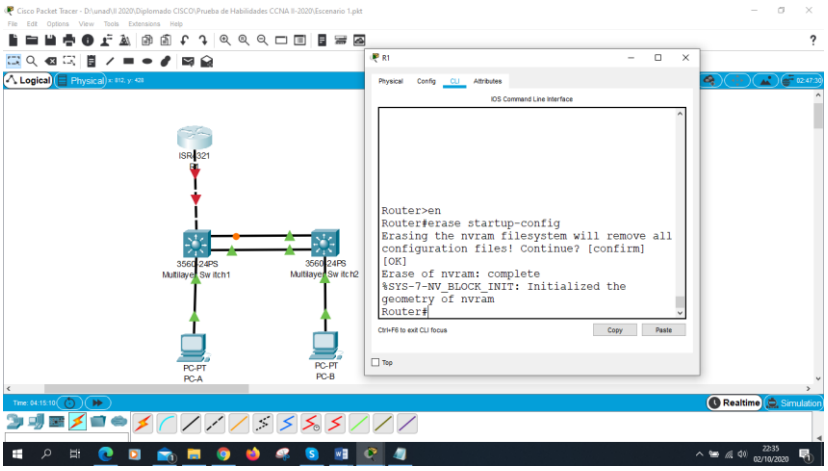
Paso 1 Inicializar y volver a cargar el router y el switch

Antes de configurar el Router y Switch se debe inicializar y recargar los equipos y configurar la tabla SDM en los Switch para que admita IPv4 e IPv6 como se muestra en la tabla 3.

Tabla 3. Comandos inicializar y recargar Router y Switch escenario 1

Tarea	Comando de IOS
Eliminar el archivo del Router	Router > enable Router # erase startup-config
Volver a cargar el routers	Router # reload
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Switch > enable Switch # delete vlan.dat Switch # erase startup-config
Volver a cargar ambos switches	Switch # reload
Configure la plantilla SDM en los switch para que admita IPv6	Switch > enable Switch # config t Switch(config)# sdm prefer dual-ipv4-and-ipv6 routing

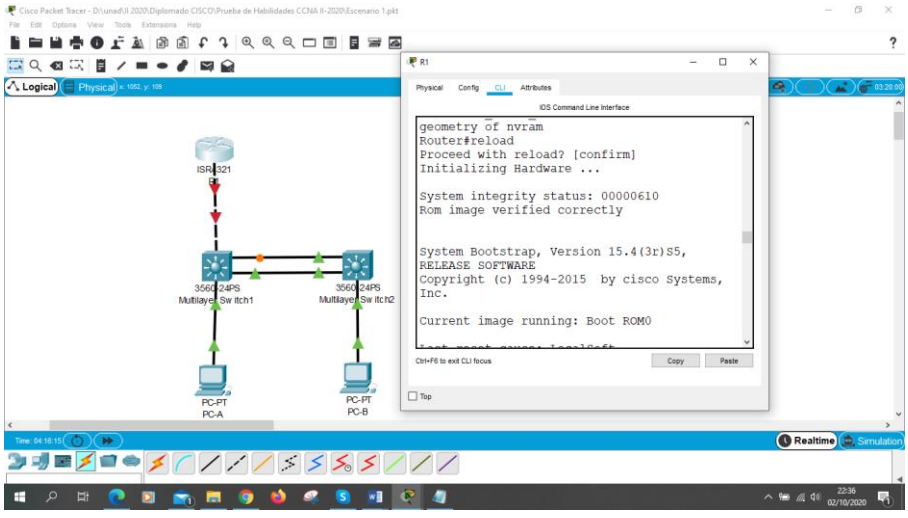
Figura 3. Eliminar Archivo de Configuración del Router 1



Fuente: Autor

Se elimina el archivo de configuración de inicio de la NVRAM del Router 1, Se accede al modo privilegiado con el comando enable, estando en el modo privilegiado se le da el comando erase startup-config, le pregunta que si está seguro confirmar y se le da clic enter.

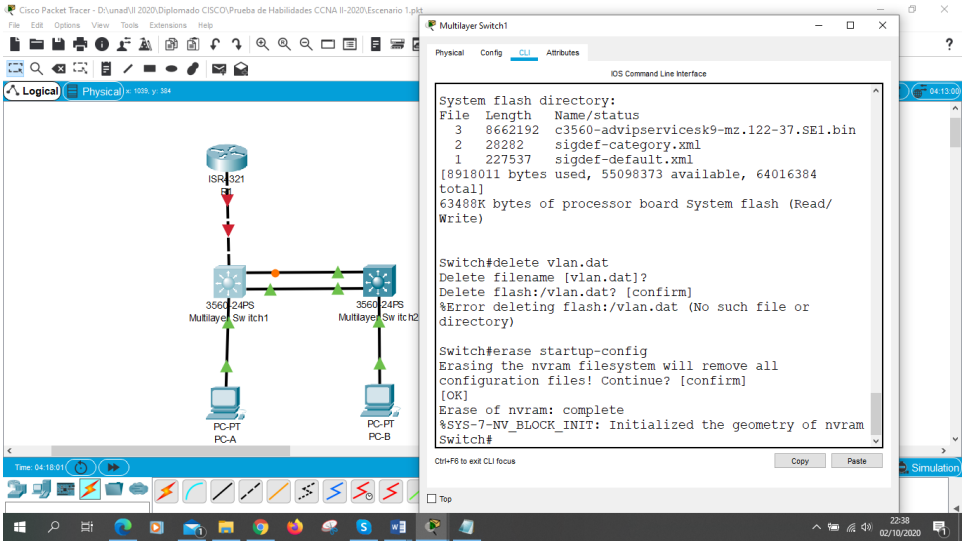
Figura 4. Cargar R1



Fuente: Autor

Se carga el Router 1 con el comando reload y luego se le da enter y se omite dialogo de configuración inicial.

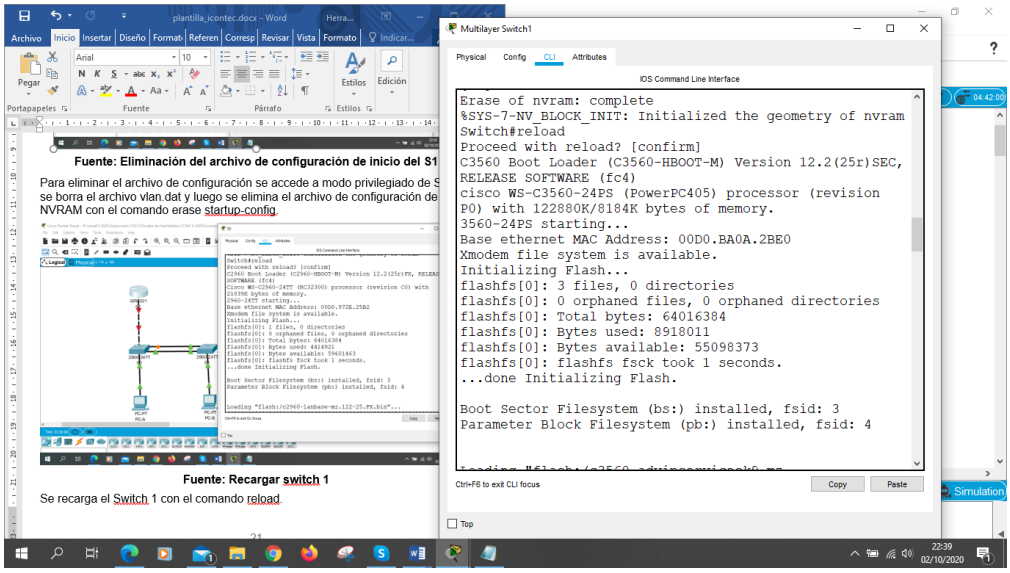
Figura 5. Eliminar Archivo de Configuración de Inicio del S1



Fuente: Autor

Para eliminar el archivo de configuración se accede a modo privilegiado de S1 y se borra el archivo vlan.dat y luego se elimina el archivo de configuración de a NVRAM con el comando erase startup-config.

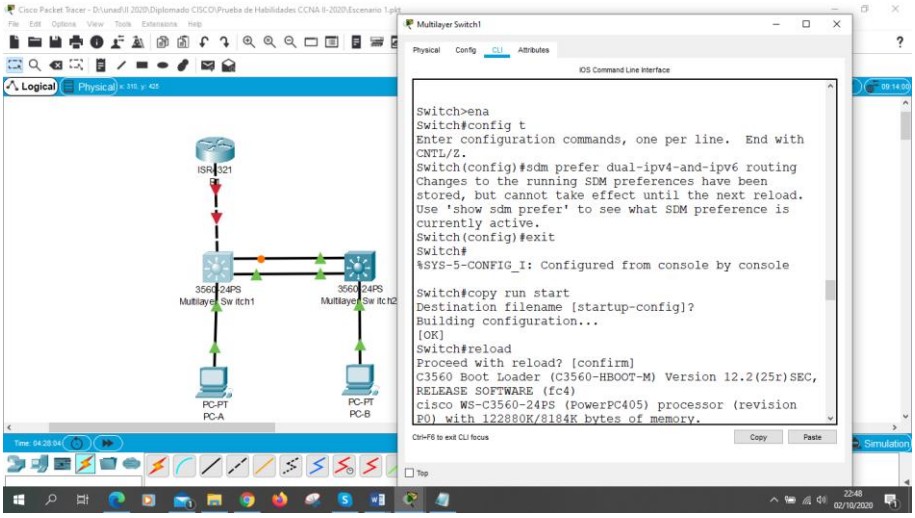
Figura 6. Recargar Switch 1



Fuente: Autor

Se recarga el Switch 1 con el comando reload**.**

Figura 7. Configuración Planilla SDM de Switch 1



Fuente: Autor

En modo privilegiado se accede a configuración terminal, se le da comando sdm prefer dual-ipv4-and-ipv6 routing. Se copia los cambios con el comando copy run start y luego se recarga con el comando reload.

Paso 1 Configurar R1

Para la configuración del Router 1 se realizará las siguientes configuraciones como se muestra en la tabla 4. donde procedemos a desactivar la búsqueda DNS, generamos el nombre al router, se crea un dominio, se establecen las contraseñas cifrada para el modo privilegiado, se configura contraseña de acceso a consola, se establece una longitud mínima para la contraseña, se crear un usuario administrativo en la base de datos local, se configurar el inicio de sesión en las líneas VTY para que use la base de datos local, se configurar líneas VTY solo aceptando conexiones SSH, se Cifran las contraseñas de texto no cifrado, se Configura un MOTD Banner, se habilita el routing IPv6, se configurar la interfaz G0/0/1 y subinterfaces, se configura la interfaz Loopback0 y se genera la clave de cifrado RSA.

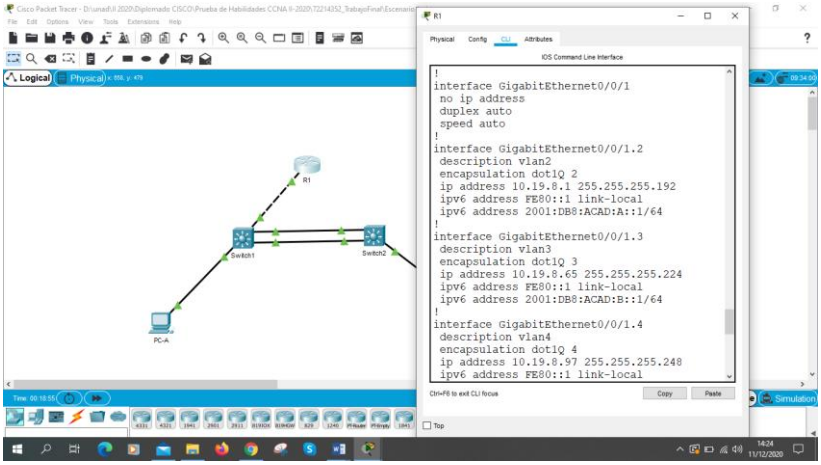
Tabla 4. Comandos configuración Básica de Router 1

Tarea	Especificación
Desactivar la búsqueda DNS	Router>enable Router#configure terminal Router(config)#no ip domain-lookup Router(config)#
Nombre del router	Router>enable Router# configure terminal Router(config)#hostname R1 R1(config)#
Nombre de dominio	R1>enable R1#configure terminal R1(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	R1> enable R1# configure terminal R1(config)# enable secret ciscoenpass R1(config)#
Contraseña de acceso a la consola	R1> enable R1# configure terminal R1(config)# line console 0 R1(config-line)# password ciscoconpass R1(config-line)# login R1(config-line)# exit R1(config)#
Establecer la longitud mínima para las contraseñas	R1#configure terminal R1(config)#security passwords min-length 10
Crear un usuario administrativo en la base de datos local	R1#configure terminal R1(config)#username admin password admin1pass R1(config)#
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	R1#configure terminal R1(config)#line vty 0 4 R1(config-line)#login local R1(config-line)#exit R1(config)#
Configurar VTY solo aceptando SSH	R1(config)#line vty 0 4 R1(config-line)#exec-timeout 10 R1(config-line)#transport input ssh R1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption R1(config)#exit

Tarea	Especificación
Configure un MOTD Banner	R1# configure terminal R1(config)# banner motd "This is a secure system. Authorized Access Only!" R1(config)# exit
Habilitar el routing IPv6	R1# configure terminal R1(config)# ipv6 unicast-routing R1(config)# exit
Configurar interfaz G0/0/1 y subinterfaces	R1#config terminal R1(config)#interface gigabitEthernet 0/0/1.2 R1(config-subif)#encapsulation dot1Q 2 R1(config-subif)#ip address 10.19.8.1 255.255.255.192 R1(config-subif)#ipv6 address 2001:db8:acad:a: :1 /64 R1(config-subif)#ipv6 address fe80::1 link-local R1(confiig-subif)#description vlan 2 R1(config-subif)#no shutdown R1(config-subif)#exit R1(config)#interface gigabitEthernet 0/0/1.3 R1(config-subif)#encapsulation dot1Q 3 R1(config-subif)#ip address 10.19.8.65 255.255.255.224 R1(config-subif)#ipv6 address 2001:db8:acad:b: :1 /64 R1(config-subif)#ipv6 address fe80::1 link-local R1(config-subif)#description vlan3 R1(config-subif)#no shutdown R1(config-subif)#exit R1(config)#interface gigabitEthernet 0/0/1.4 R1(config-subif)#encapsulation dot1Q 4 R1(config-subif)#ip address 10.19.8.97 255.255.255.248 R1(config-subif)#ipv6 address 2001:db8:acad:c: :1 /64 R1(config-subif)#ipv6 address fe80::1 link-local R1(config-subif)#description vlan4 R1(config-subif)#no shutdown R1(config-subif)#exit R1(config)#interface gigabitEthernet 0/0/1 R1(config-if)#no shutdown

Tarea	Especificación
Configure el Loopback0 interface	R1#configure terminal R1(config)#interface 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
Generar una clave de cifrado RSA	R1(config)#crypto key generate rsa Chose the size of the key modulus in the range of 360 to 2048 for your general purpose key. Choosing a key modulus greater than 512 may take a few minutes. How many bits in the modulus [512]:1024

Figura 8. Configuración del Router 1



Fuente: Autor

Se verifica las configuraciones en el router 1 con el comando show run.

Paso 2 Configure S1 y S2.

Para la configuración de los switchs se realizará las siguientes configuraciones como se muestra en la tabla 5. donde procedemos a desactivar la búsqueda DNS, generamos el nombre al Switch, se crea un dominio, se establecen las contraseñas cifrada para el modo privilegiado, se configura contraseña de acceso a consola, se crear un usuario administrativo en la base de datos local, se configurar el inicio de sesión en las líneas VTY para que use la base de datos local, se configurar líneas

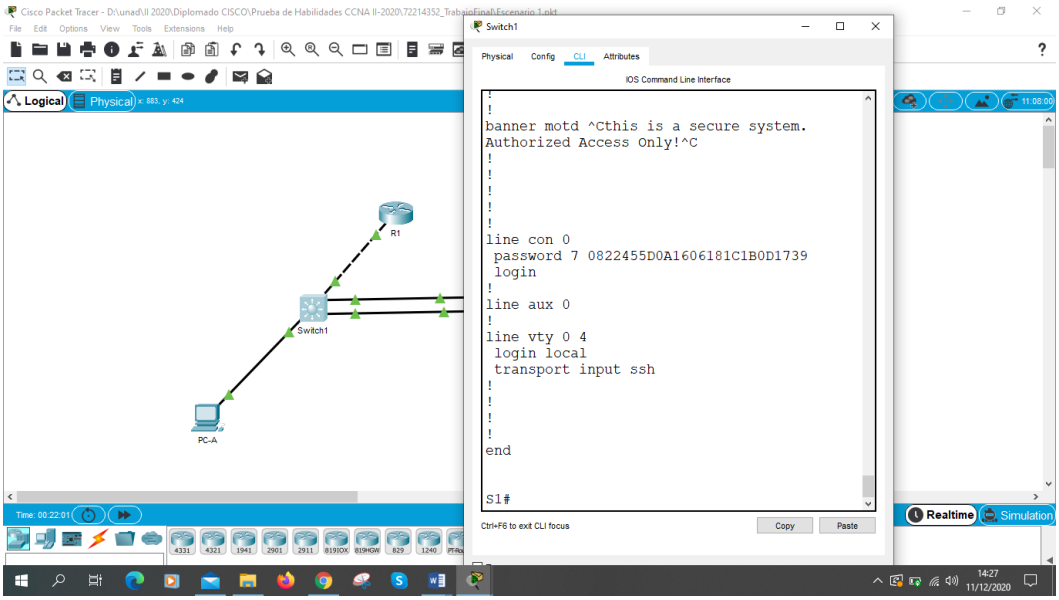
VTY solo aceptando conexiones SSH, se Cifran las contraseñas de texto no cifrado, se Configura un MOTD Banner, se genera la clave de cifrado RSA, se configura la interfaz de administración (SVI) y configuración de Gateway predeterminado.

Tabla 5. Configuración de S1 y S2

Tarea	Especificación
Desactivar la búsqueda DNS.	Switch>enable Switch#configure terminal Switch(config)#no ip domain-lookup Switch(config)#
Nombre del switch	switch>enable switch# configure terminal switch(config)#hostname S1 S1(config)#
Nombre de dominio	S1>enable S1#configure terminal S1(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	S1> enable S1# configure terminal S1(config)# enable secret ciscoenpass S1(config)#
Contraseña de acceso a la consola	S1> enable S1# configure terminal S1(config)# line console 0 S1(config-line)# password ciscoconpass S1(config-line)# login S1(config-line)# exit S1(config)#
Crear un usuario administrativo en la base de datos local	S1#configure terminal S1(config)#username admin password admin1pass S1(config)#
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	S1#configure terminal S1(config)#line vty 0 4 S1(config-line)#login local S1(config-line)#exit S1(config)#

Tarea	Especificación
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S1(config)#line vty 0 4 S1(config-line)#exec-timeout 10 S1(config-line)#transport input ssh S1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption S1(config)#exit
Configurar un MOTD Banner	S1# configure terminal S1(config)# banner motd "This is a secure system. Authorized Access Only!" S1(config)# exit
Generar una clave de cifrado RSA	S1(config)#crypto key generate rsa Chose the size of the key modulus in the range of 360 to 2048 for your general purpose key. Choosing a key modulus greater than 512 may take a few minutes. How many bits in the modulus [512]:1024
Configurar la interfaz de administración (SVI)	S1#configure terminal S1(config)#interface vlan 4 S1(config-vlan)#ip address 10.19.8.98 255.255.255.248 S1(config-vlan)#ipv6 address 2001:db8:acad:c: :98 /64 S1(config-vlan)#ipv6 address fe80::98 link-local S1(config)#ipv6 route ::/0 2001:db8:acad:c::1 S2#configure terminal S2(config)#interface vlan 4 S2(config-vlan)#ip address 10.19.8.99 255.255.255.248 S2(config-vlan)#ipv6 address 2001:db8:acad:c: :99/64 S2(config-vlan)#ipv6 address fe80::99 link-local S2(config)#ipv6 route ::/0 2001:db8:acad:c::1
Configuración del gateway predeterminado	S1#configure terminal S1(config)#ip default-gateway 10.19.8.97

Figura 9. Configuración de Switch 1



Fuente: Autor

Se verifica las configuraciones realizadas en el Switch 1 con el comando show run

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

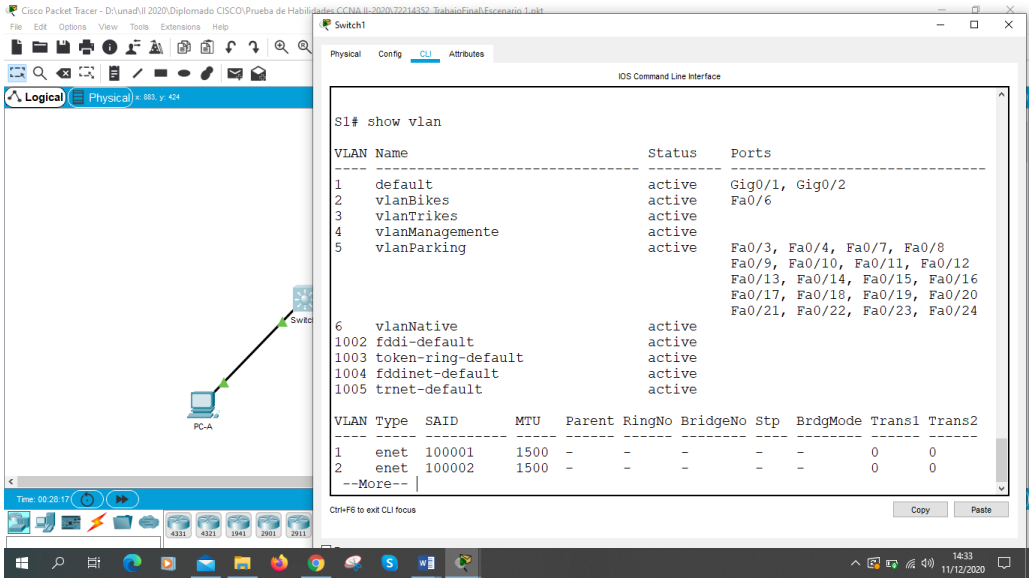
Paso 1 Configurar S1

Para la configuración de la infraestructura de red (VLAN, Trunking, EtherChannel) del Switch 1 se realizan las configuraciones como se muestra en la tabla 6. se precede a crear las Vlan, se crean troncos 802.1Q que utilicen la VLAN 6 nativa, se Crea un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2, se Configura el puerto de acceso de host para VLAN 2, se configura la seguridad del puerto en los puertos de acceso y se protegen las interfaces no utilizadas.

Tabla 6. Configuración de la infraestructura de red en S1(Vlan, Trunking, Etherchannel)

Tarea	Especificación
Crear VLAN	S1(config)#vlan 2 S1(config-vlan)#name vlanBikes S1(config-vlan)#exit S1(config)#vlan 3 S1(config-vlan)#name vlanTrikes S1(config-vlan)#exit S1(config)#vlan 4 S1(config-vlan)#name vlanManagement S1(config-vlan)#exit S1(config)#vlan 5 S1(config-vlan)#name vlanParking S1(config-vlan)#exit S1(config)#vlan 6 S1(config-vlan)#name vlanNative S1(config-vlan)#exit
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	S1#configure terminal S1(config)#interface range f0/1,f0/2,f0/5 S1(config-if-range)# switchport trunk encapsulation dot1q S1(config-if-range)# switchport mode trunk S1(config-if-range)#switchport trunk allowed vlan 6
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	S1#configure terminal S1(config)#int range f0/1-2 S1(config-if-range)#channel-protocol lacp S1(config-if-range)#channel-group 1 mode active
Configurar el puerto de acceso de host para VLAN 2	S1#configuere terminal S1(config)#int f0/6 S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 2
Configurar la seguridad del puerto en los puertos de acceso	S1#configure terminal S1(config)#int f0/6 S1(config-if)#switchport port-security S1(config-if)#switchport port-security Maximum 3 S1(config-if)#switchport port-security violation shutdown
Proteja todas las interfaces no utilizadas	S2#configure terminal S2(config)#int range f0/3-4,f0/7-24 S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 5

Figura 10. Configuración de infraestructura de red en Switch 1



Fuente: Autor

Se verifica que este configurado correctamente los pasos de la tabla 6 en Switch1

Paso 2 Configure el S2.

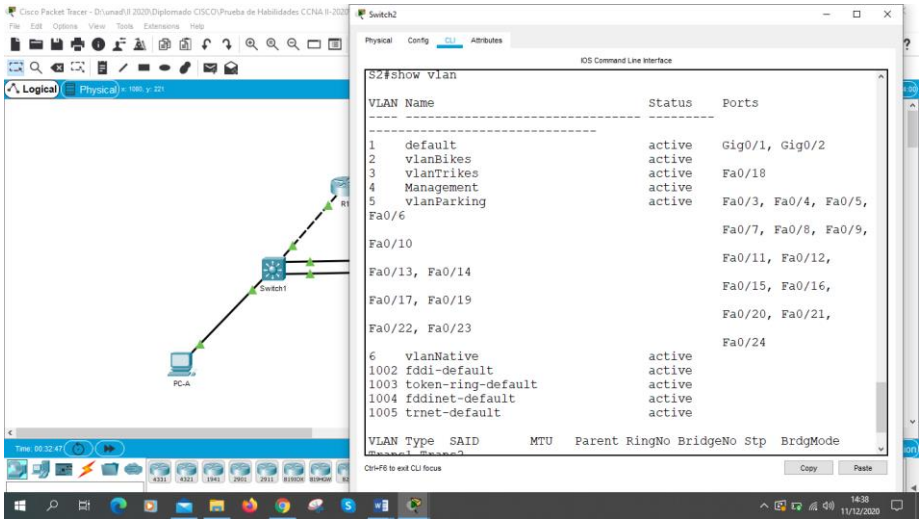
Para la configuración de la infraestructura de red (VLAN, Trunking, EtherChannel) del Switch 2 se realizan las configuraciones como se muestra en la tabla 7. se precede a crear las Vlan, se crean troncos 802.1Q que utilicen la VLAN 6 nativa, se Crea un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2, se Configura el puerto de acceso de host para VLAN 3, se configura la seguridad del puerto en los puertos de acceso y se protegen las interfaces no utilizadas.

Tabla 7. Configuración de la infraestructura de red en S2 (Vlan, Trunking, Etherchannel)

Tarea	Especificación
Crear VLAN	S2(config)#vlan 2 S2(config-vlan)#name vlanBikes S2(config-vlan)#exit S2(config)#vlan 3 S2(config-vlan)#name vlanTrikes S2(config-vlan)#exit S2(config)#vlan 4 S2(config-vlan)#name vlanManagement S2(config-vlan)#exit S2(config)#vlan 5 S2(config-vlan)#name vlanParking S2(config-vlan)#exit S2(config)#vlan 6 S2(config-vlan)#name vlanNative S2(config-vlan)#exit
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	S2#configure terminal S2(config)#int range f0/1,f0/2 S2(config-if-range)# switchport trunk encapsulation dot1q S2(config-if-range)# switchport mode trunk S2(config-if-range)#switchport trunk allowed vlan 6
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	S2#configure terminal S2(config)#int range f0/1-2 S2(config-if-range)#channel-protocol lacp S2(config-if-range)#channel-group 1 mode passive
Configurar el puerto de acceso del host para la VLAN 3	S2#configure terminal S2(config)#int f0/18 S2(config-if)#switchport mode access S2(config-if)#switchport access vlan 3
Configure port-security en los access ports	S2#configure terminal S2(config)#int f0/18 S2(config-if)#switchport port-security Maximum 3 S2 (config-if)#switchport port-security violation shutdown

Tarea	Especificación
Asegure todas las interfaces no utilizadas.	S2#configure terminal S2(config)#int range f0/3-17,f0/19-24 S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 5

Figura 11. Configuración de infraestructura de red en Switch 2



Fuente: Autor

Se verifica que este configurado correctamente los pasos de la tabla 6 en Switch1

Parte 3 Configurar soporte de host

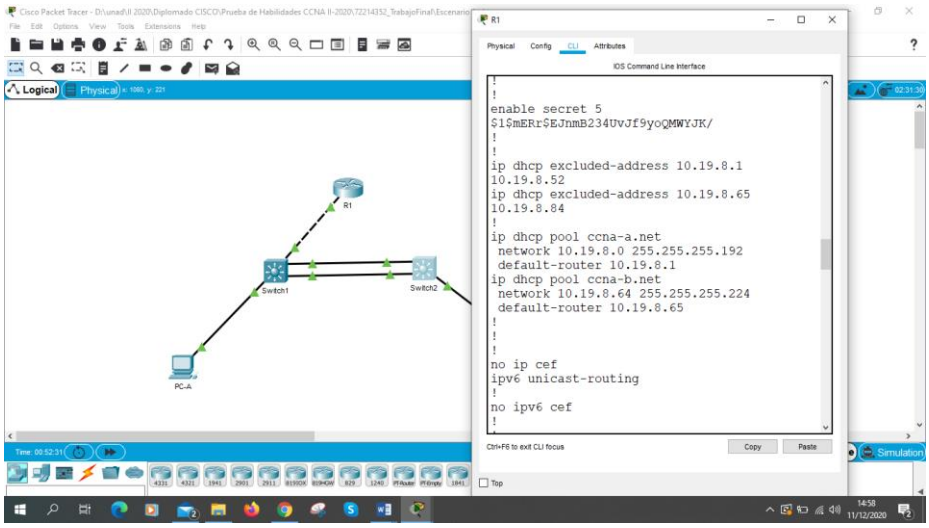
Paso 1 Configure R1

Para la configuración de soporte de host en Router 1 realizan los comandos como se muestra en la tabla 8 se configura el default routing para crear ruta predeterminada para IPv4 e IPv6 que dirijan el tráfico a la interfaz Loopback0, se crea un grupo DHCP para la Vlan 2 con el nombre de dominio ccna-a.net y compuesta por las ultimas 10 direcciones de red, se crea un grupo DHCP para la Vlan 3 con el nombre de dominio ccna-b.net y compuesta por las ultimas 10 direcciones de red.

Tabla 8. Configurar soporte de host en Router 1

Tarea	Especificación
Configure Default Routing	R1#configure terminal R1(config)#ip route ::/0 loopback 0
Configurar IPv4 DHCP para VLAN 2	R1#configure terminal R1(config)#ip dhcp pool ccna-a.net R1(dhcp-config)#network 10.19.8.0 255.255.255.192 R1(dhcp-config)#default-router 10.19.8.1 R1(dhcp-config)#exit R1(config)#ip dhcp excluded-address 10.19.8.1 10.19.8.52
Configurar DHCP IPv4 para VLAN 3	R1#configure terminal R1(config)#ip dhcp pool ccna-b.net R1(dhcp-config)#network 10.19.8.64 255.255.255.224 R1(dhcp-config)#default-router 10.19.8.65 R1(dhcp-config)#exit R1(config)#ip dhcp excluded-address 10.19.8.65 10.19.8.84

Figura 12. Configurar Soporte de host en R1



Fuente: Autor

Se verifica la configuración de los grupos DHCP y default Routing en router 1

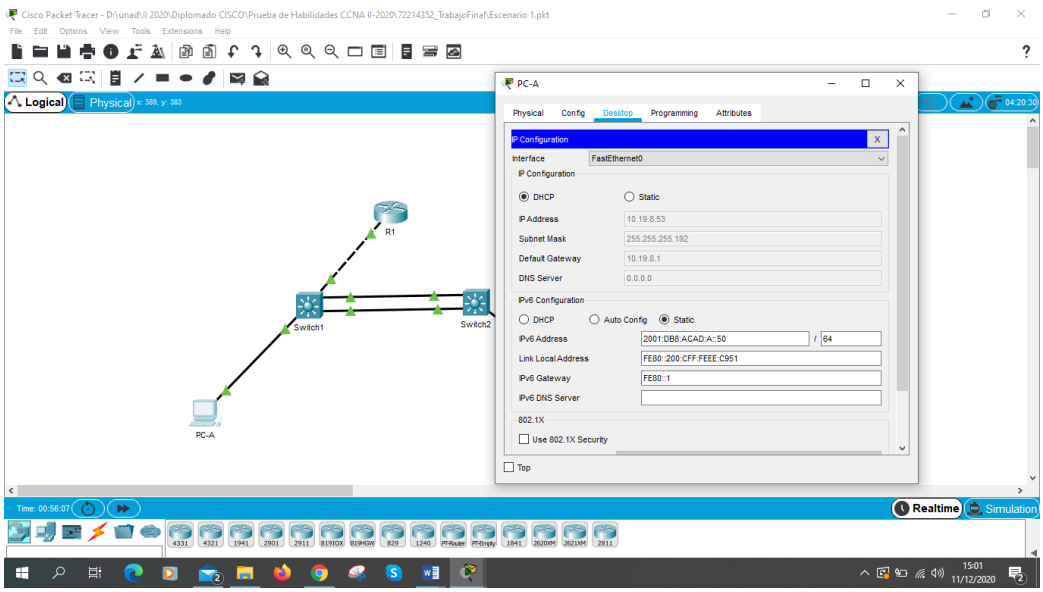
Paso 2 Configurar los servidores

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

Tabla 9. Configuración de red PC-A

PC-A Network Configuration	
Descripción	**PC-A**
Dirección física	0000.0CEE.C951
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 13. Configuración de red en PC-A



Fuente: Autor

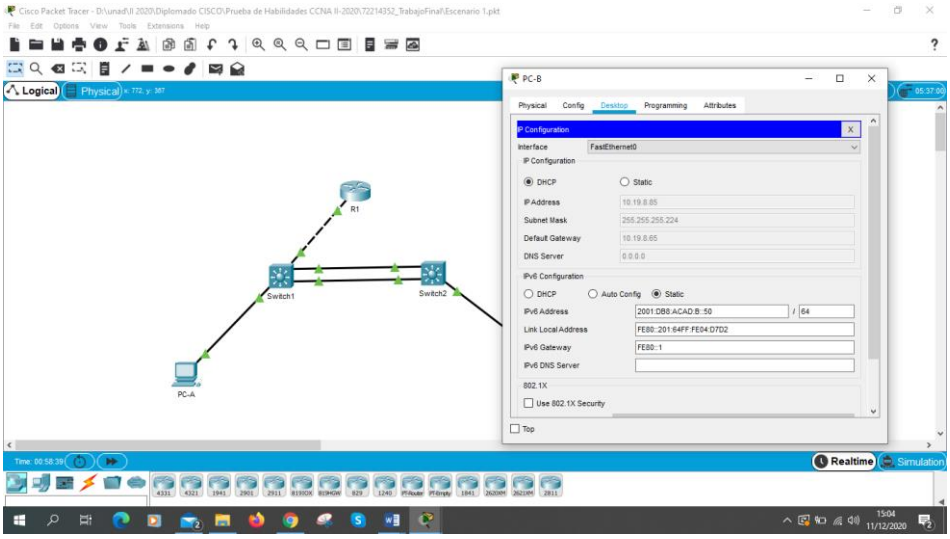
Se configura la IPv4 e IPv 6 en la PC-A

Tabla 10. Configuración de red PC-B

Configuración de red de PC-B	
Descripción	PC-B

Configuración de red de PC-B	
Dirección física	0001.6404.D7D2
Dirección IP	10.19.8.85
Máscara de subred	255.255.255.224
Gateway predeterminado	10.19.8.65
Gateway predeterminado IPv6	FE80::1

Figura 14. Configuración de red en PC-B



Fuente: Autor

Se configura la IPv4 e IPv 6 en la PC-B

Parte 4 Probar y verificar la conectividad de extremo a extremo

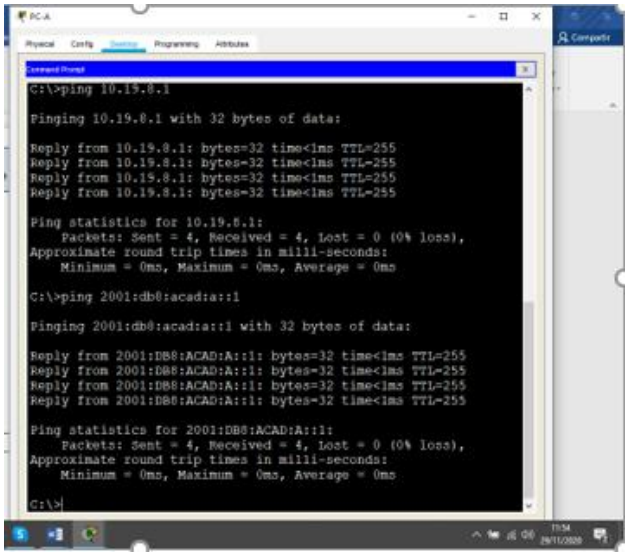
Use el comando ping para probar la conectividad IPv4 e IPv6 entre todos los dispositivos de red.

Tabla 11. Prueba de conectividad de red

Desde	A	de Internet	Dirección IP	Resultados de ping
PC-A	R1, G0/0/1.2	Dirección	10.19.8.1	correcto
		IPv6	2001:db8:acad:a: :1	correcto
	R1, G0/0/1.3	Dirección	10.19.8.65	correcto
		IPv6	2001:db8:acad:b: :1	correcto

Desde	A	de Internet	Dirección IP	Resultados de ping
	R1, G0/0/1.4	Dirección	10.19.8.97	correcto
		IPv6	2001:db8:acad:c: :1	correcto
	S1, VLAN 4	Dirección	10.19.8.98	correcto
		IPv6	2001:db8:acad:c: :98	Correcto
	S2, VLAN 4	Dirección	10.19.8.99.	correcto
		IPv6	2001:db8:acad:c: :99	Correcto
	PC-B	Dirección	10.19.8.85	Correcto
		IPv6	2001:db8:acad:b: :50	Correcto
	R1 Bucle 0	Dirección	209.165.201.1	Correcto
		IPv6	2001:db8:acad:209: :1	Correcto
PC-B	R1 Bucle 0	Dirección	209.165.201.1	Correcto
		IPv6	2001:db8:acad:209: :1	Correcto
	R1, G0/0/1.2	Dirección	10.19.8.1	Correcto
		IPv6	2001:db8:acad:a: :1	Correcto
	R1, G0/0/1.3	Dirección	10.19.8.65	Correcto
		IPv6	2001:db8:acad:b: :1	Correcto
	R1, G0/0/1.4	Dirección	10.19.8.97	Correcto
		IPv6	2001:db8:acad:c: :1	Correcto
	S1, VLAN 4	Dirección	10.19.8.98	Correcto
		IPv6	2001:db8:acad:c: :98	Correcto
	S2, VLAN 4	Dirección	10.19.8.99.	Correcto
		IPv6	2001:db8:acad:c: :99	**Correcto**

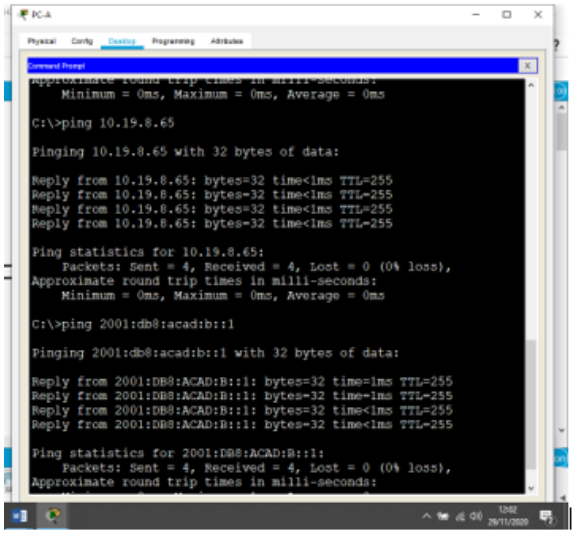
Figura 15. Prueba de conectividad IPv4 e IPv6 desde PC-A a R1, G0/0/1.2



Fuente: Autor

Se realiza ping desde la PC-A a la IPv4 10.19.8.1 y la IPv6 2001:db8:acad:a::1 de R1, G0/0/1.2 comprobando su conexión.

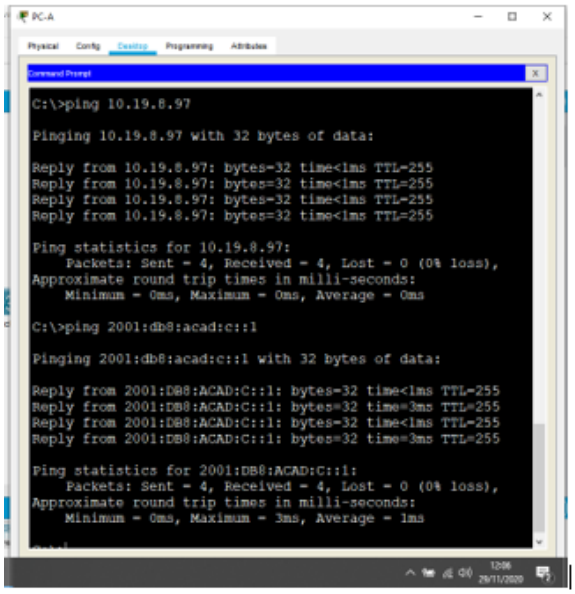
Figura 16. Prueba de conectividad IPv4 e IPv6 entre PC-A y R1 G0/0/1.3



Fuente: Autor

Se realiza ping desde la PC-A a la IPv4 10.19.8.65 y a la IPv6 2001:DB8:ACAD:B::1 de R1 G0/0/1.3 comprobando su conexión.

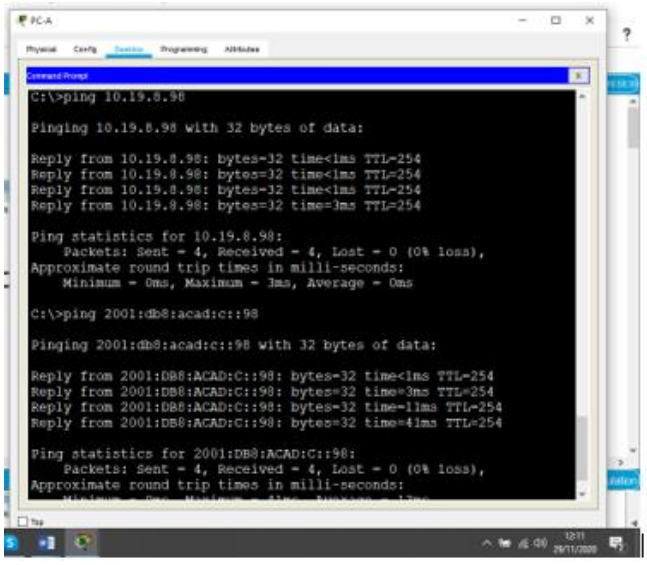
Figura 17. Prueba de conectividad IPv4 e IPv6 entre la PC-A y R1, G0/0/1.4



Fuente: Autor

Se realiza ping desde la PC-A a la IPv4 10.19.8.97 y a la IPv6 2001:DB8:ACAD:C::1 de R1 G0/0/1.4 comprobando su conexión.

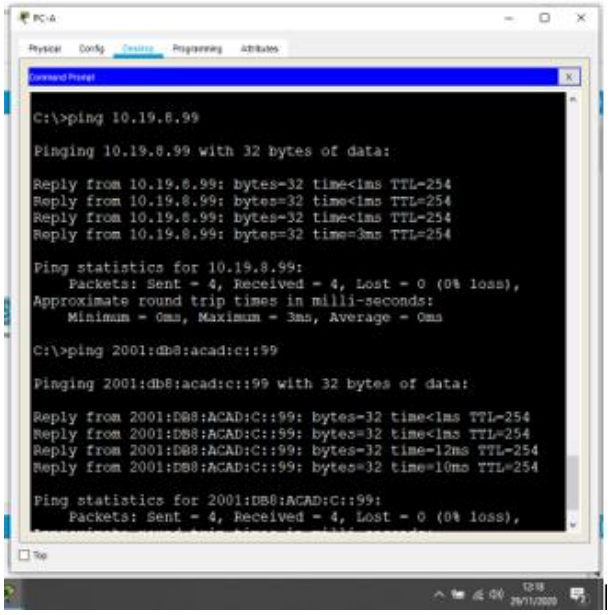
Figura 18. Prueba de conectividad IPv4 e IPv6 entre la PC-A y S1, Vlan 4



Fuente: Autor

Se realiza ping desde la PC-A a la IPv4 10.19.8.98 y a la IPv6 2001:DB8:ACAD:C::98 de S1, Vlan 4 comprobando su conexión.

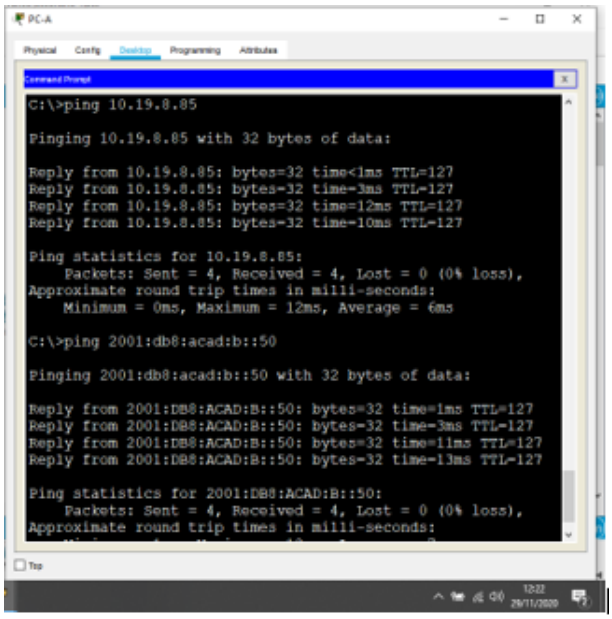
Figura 19. Prueba de conectividad IPv4 e IPv6 entre la PC-A y S2, Vlan 4



Fuente: Autor

Se realiza ping desde la PC-A a la IPv4 10.19.8.99 y a la IPv6 2001:DB8:ACAD:C::99 de S2, Vlan 4. comprobando su conexión.

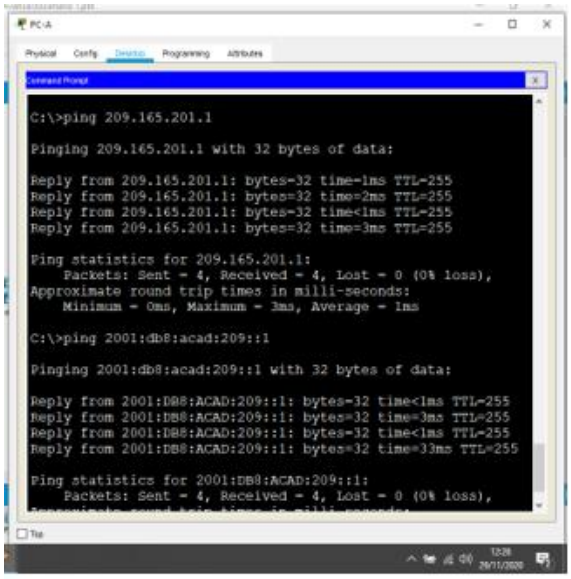
Figura 20. Prueba de conectividad IPv4 e IPv6 entre la PC-A y PC-B



Fuente: Autor

Se realiza ping desde la PC-A a la IPv4 10.19.8.85 y a la IPv6 2001:DB8:ACAD:B::50 de PC-B comprobando su conexión.

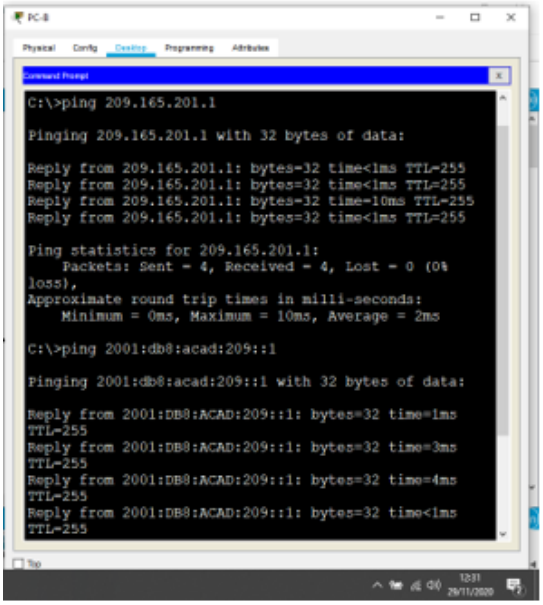
Figura 21. Prueba de conectividad IPv4 e IPv6 entre la PC-A y Bucle 0



Fuente: Autor

Se realiza ping desde la PC-A a la IPv4 209.165.201.1 y a la IPv6 2001:DB8:ACAD:209::1 de Bucle 0 comprobando su conexión.

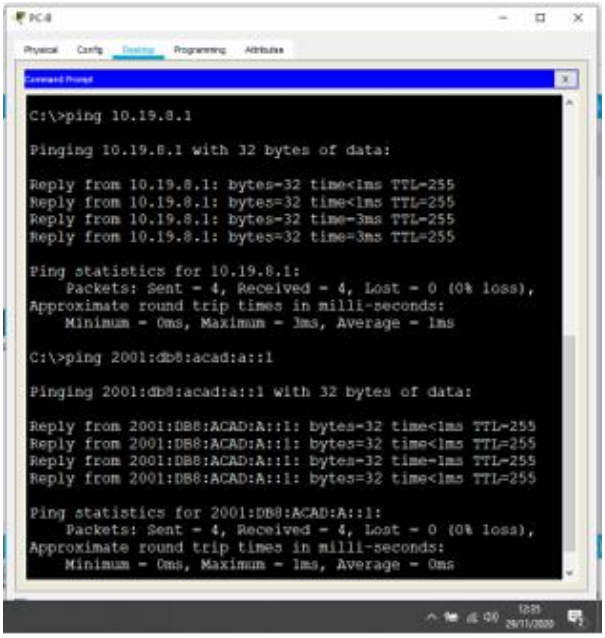
Figura 22. Prueba de conectividad IPv4 e IPv6 entre la PC-B y Bucle 0



Fuente: Autor

Se realiza ping desde la PC-B a la IPv4 209.165.201.1 y a la IPv6 2001:DB8:ACAD:209::1 de Bucle 0 comprobando su conexión.

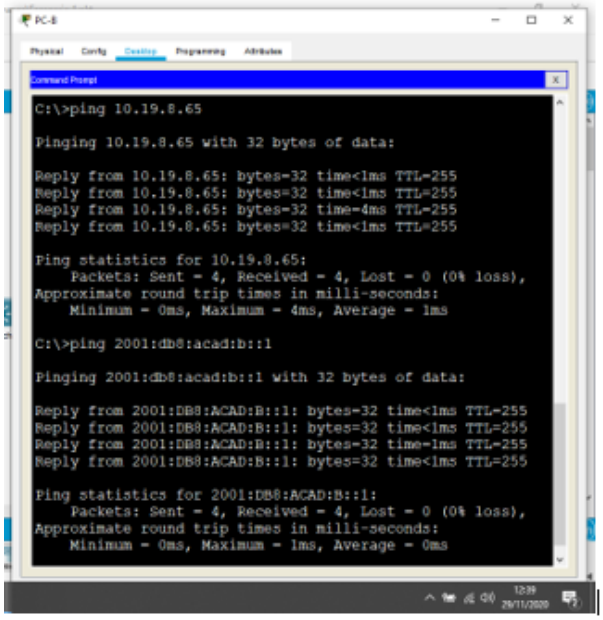
Figura 23. Prueba de conectividad IPv4 e IPv6 entre la PC-B y R1, G0/0/1.2



Fuente: Autor

Se realiza ping desde la PC-B a la IPv4 10.19.8.1 y la IPv6 2001:db8:acad:a::1 de R1, G0/0/1.3 comprobando su conexión.

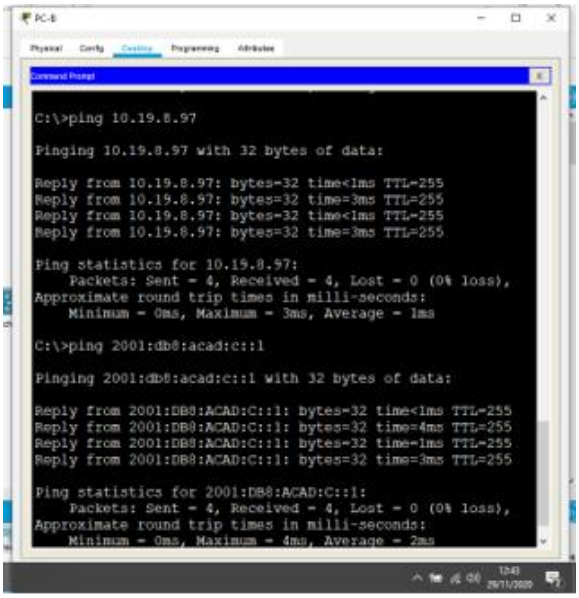
Figura 24. Prueba de conectividad IPv4 e IPv6 entre PC-B y R1 G0/0/1.3



Fuente: Autor

Se realiza ping desde la PC-B a la IPv4 10.19.8.65 y a la IPv6 2001:DB8:ACAD:B::1 de R1 G0/0/1.3 comprobando su conexión.

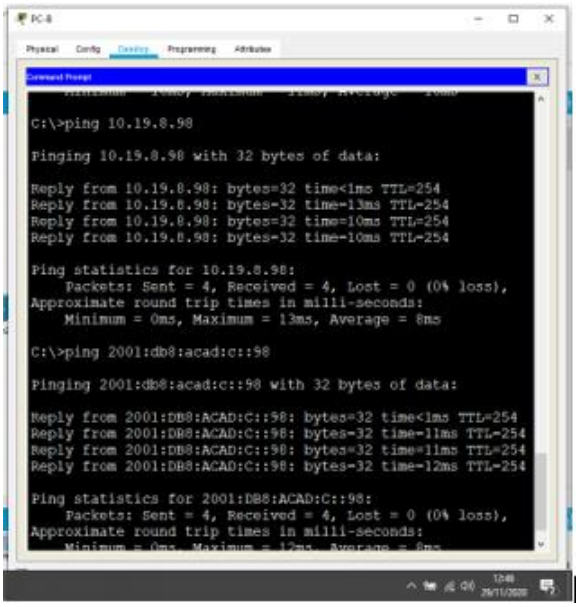
Figura 25. Prueba de conectividad IPv4 e IPv6 entre la PC-B y R1, G0/0/1.4



Fuente: Autor

Se realiza ping desde la PC-B a la IPv4 10.19.8.97 y a la IPv6 2001:DB8:ACAD:C::1 de R1 G0/0/1.4 comprobando su conexión.

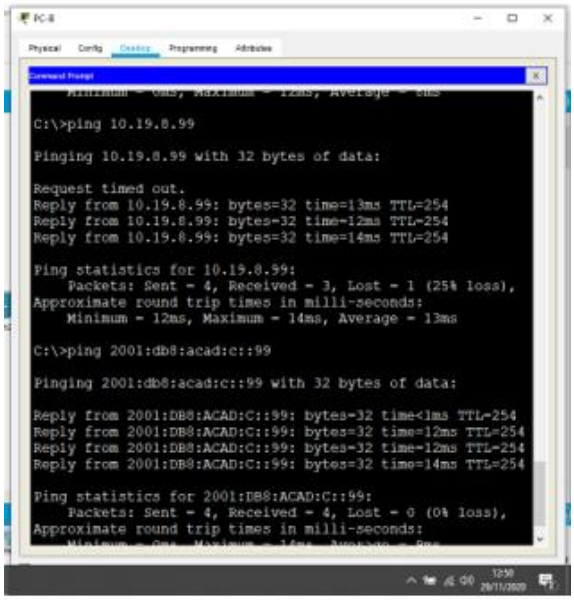
Figura 26. Prueba de conectividad IPv4 e IPv6 entre la PC-B y S1, Vlan 4



Fuente: Autor

Se realiza ping desde la PC-B a la IPv4 10.19.8.98 y a la IPv6 2001:DB8:ACAD:C::98 de S1 Vlan 4 comprobando su conexión.

Figura 27. Prueba de conectividad IPv4 e IPv6 entre la PC-B y S2, Vlan 4



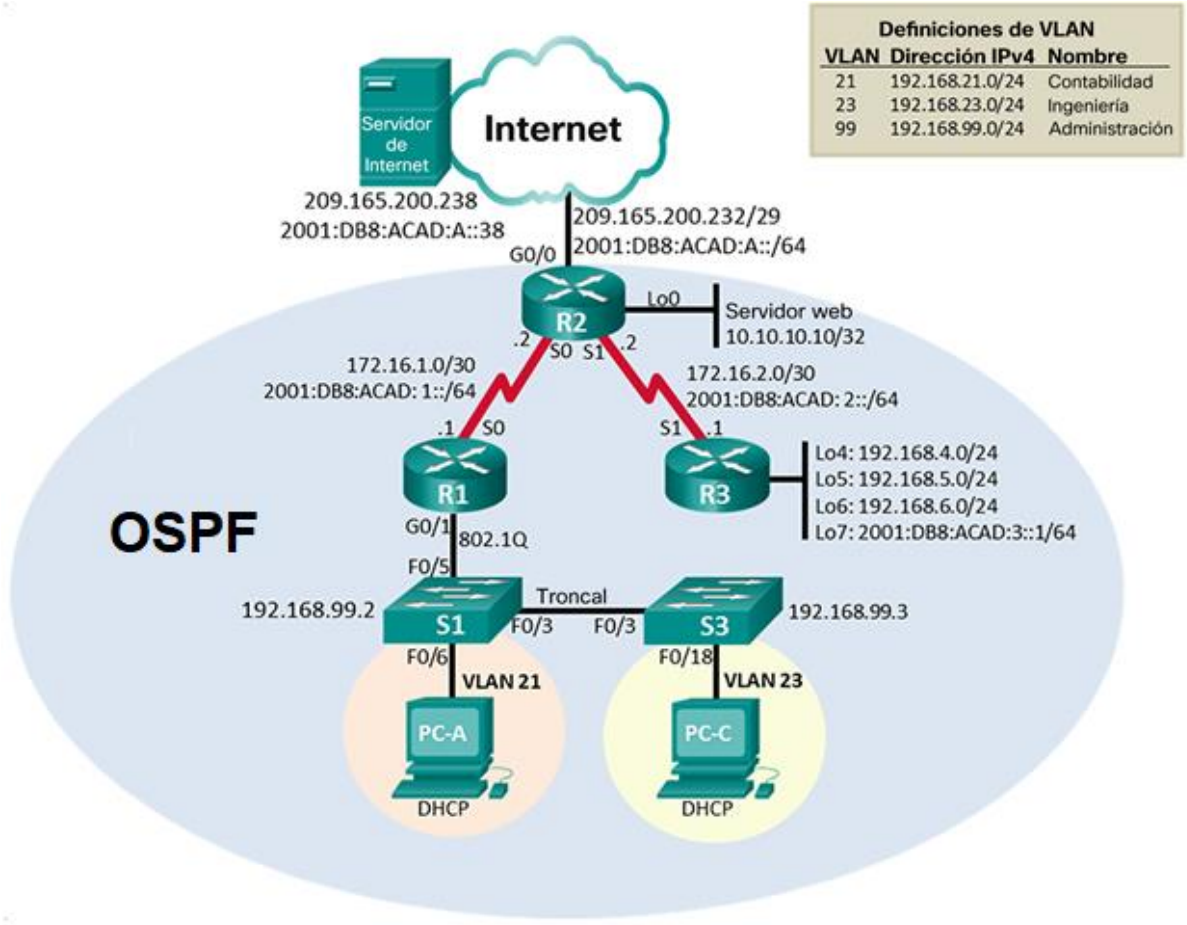
Fuente: Autor

Se realiza ping desde la PC-B a la IPv4 10.19.8.99 y a la IPv6 2001:DB8:ACAD:C::99 de S2 Vlan 4 comprobando su conexión.

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.

Figura 28. Topología Escenario 2



En base a la topología del escenario 2 se diseña tabla de direccionamiento

Tabla 12. Direccionamiento de red Escenario 2

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
R1 S0/0/0	172.16.1.1/30	No corresponde
	2001:db8:acad:1: :1 /64	No corresponde
R1 G0/0/1.21	192.168.21.1/24	No corresponde
R1 G0/0/1.23	192.168.23.1/24	No corresponde
R1 G0/0/1.99	192.168.99.1/24	No corresponde
R2 S0/0/0	172.16.1.2/30	No corresponde
	2001:DB8:ACAD:1::2/64	No corresponde
R2 S0/0/1	172.16.2.2/30	No corresponde
	2001:DB8:ACAD:2::2/64	No corresponde
R2 G0/0	209.165.200.233/29	No corresponde
	2001:DB8:ACAD:A::1/64	No corresponde
R2 Lo0	10.10.10.10/32	No corresponde
R3 S0/0/1	172.16.2.1/30	10.19.8.97
	2001:DB8:ACAD:2::1/64	No corresponde
R3 Lo4	192.168.4.1/24	No corresponde
R3 Lo5	192.168.5.1/24	No corresponde
R3 Lo 6	192.168.6.1/24	No corresponde
S1 Vlan 99	192.168.99.2	192.168.99.1
S3 Vlan 99	192.168.99.3	192.168.99.1
Servidor de Internet	209.165.200.238	209.165.200.233
	2001:DB8:ACAD:2::38	2001:DB8:ACAD:2::1
PC-A	DHCP	192.168.21.1
PC-C	DHCP	192.168.23.1

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.

Antes de configurar los routers y switchs se debe inicializar y recargar los equipos y configurar la tabla SDM en los switch para que admita IPv4 e IPv6 como se muestra en la tabla 13.

Tabla 13. Comandos inicializar y recargar Router y Switch escenario 2

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	Router > enable Router # erase startup-config
Volver a cargar todos los routers	Router # reload
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Switch > enable Switch # delete vlan.dat Switch # erase startup-config
Volver a cargar ambos switches	Switch # reload
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Switch > enable Switch # show vlan brief
Configure la plantilla SDM en los switch para que admita IPv6	Switch > enable Switch # config t Switch(config)# sdm prefer dual-ipv4-and-ipv6 routing

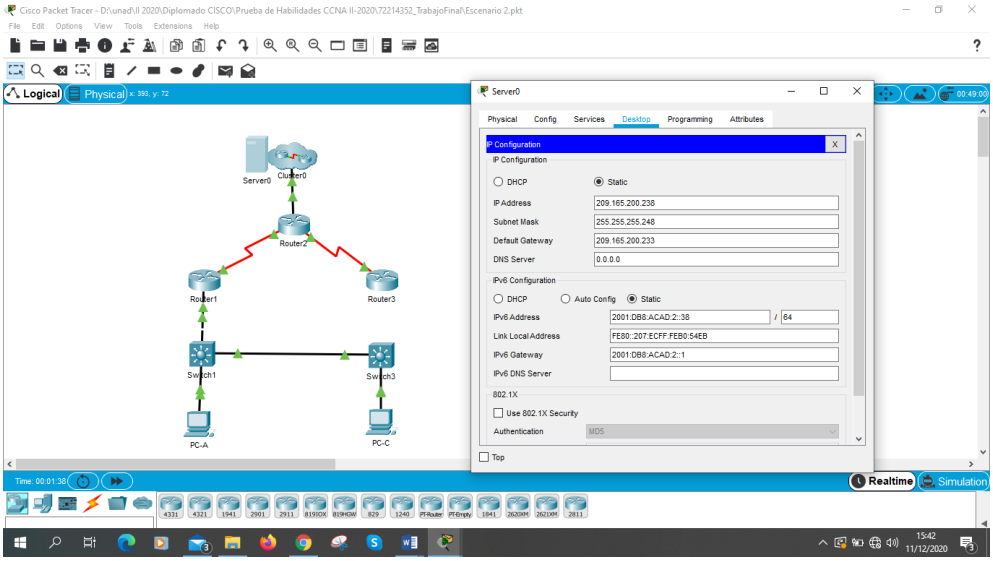
Parte 2: Configurar los parámetros básicos de los dispositivos

Paso 1: Configurar la computadora de Internet

Tabla 14. Configuración direcciones IP de la computadora de Internet

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.233
Dirección IPv6/subred	2001:DB8:ACAD:2::38
Gateway predeterminado IPv6	2001:DB8:ACAD:2::1

Tabla 15. Configuración de red computador de internet



Fuente: Autor

Paso 2: Configurar R1

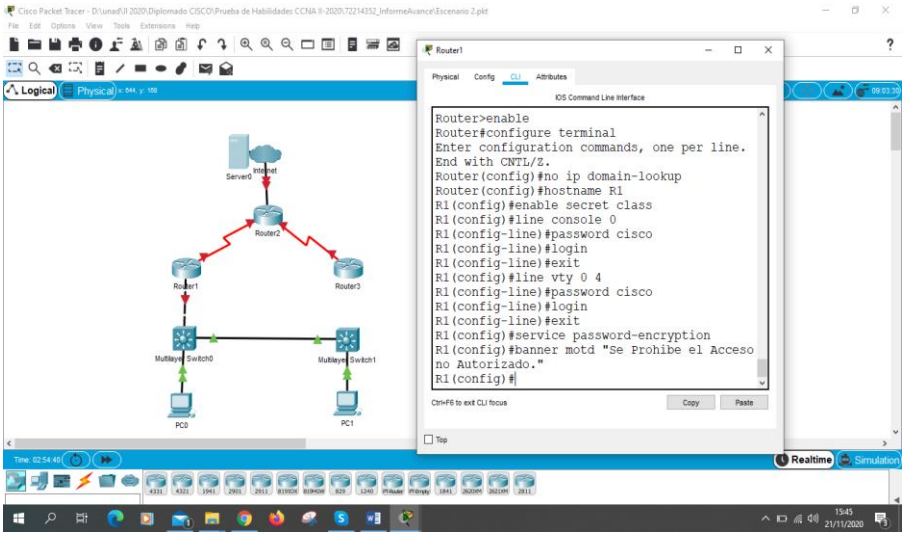
Para la configuración del Router 1 se realizará las siguientes configuraciones como se muestra en la tabla 16. donde procedemos a desactivar la búsqueda DNS, generamos el nombre al router, se crea un dominio, se establecen las contraseñas cifrada para el modo privilegiado, se configura contraseña de acceso a consola, Contraseña de acceso Telnet, Cifrar las contraseñas de texto no cifrado, Mensaje MOTD, Interfaz S0/0/0, Rutas predeterminadas

Tabla 16. Configuración Router 1 escenario 2

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router>enable Router#configure terminal Router(config)#no ip domain-lookup Router(config)#
Nombre del router	Router>enable Router# configure terminal Router(config)#hostname R1 R1(config)#
Contraseña de exec privilegiado cifrada	R1> enable R1# configure terminal R1(config)# enable secret class R1(config)#
Contraseña de acceso a la consola	R1> enable R1# configure terminal R1(config)# line console 0 R1(config-line)# password cisco R1(config-line)# login R1(config-line)# exit R1(config)#
Contraseña de acceso Telnet	R1#configure terminal R1(config)#line vty 0 4 R1(config-line)#lpassword cisco R1(config-line)# login R1(config-line)#exit R1(config)#
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption R1(config)#exit
Mensaje MOTD	R1# configure terminal R1(config)# banner motd " Se prohíbe el acceso no autorizado." R1(config)# exit
Interfaz S0/0/0	R1#config terminal R1(config)#interface s 0/0/0 R1(config-subif)#ip address 172.16.1.1 255.255.255.252 R1(config-subif)#ipv6 address 2001:db8:acad:1: :1 /64 R1(config-subif)#description Conexion R2 R1(config-subif)#no shutdown R1(config-subif)#exit

Rutas predeterminadas	R1#configure terminal R1(config)#ip route 0.0.0.0 0.0.0.0 172.16.1.2 R1#configure terminal R1(config)#ipv6 route ::/0 2001:DB8:ACAD:1::2

Figura 29. Configuración Router 1 escenario 2



Fuente: Autor

Se realiza todas las configuraciones básicas, interfaz y las ruta predeterminadas en el Router 1

Paso 3: Configurar R2

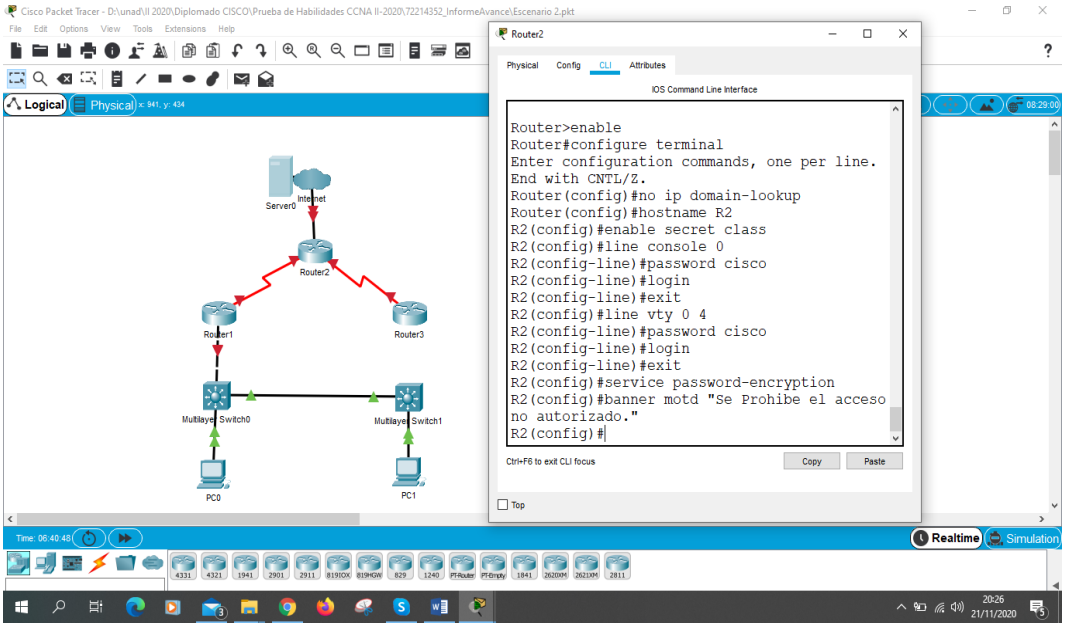
Para la configuración del Router 2 se realizará las siguientes configuraciones como se muestra en la tabla 17. donde procedemos a desactivar la búsqueda DNS, generamos el nombre al router, se crea un dominio, se establecen las contraseñas cifrada para el modo privilegiado, se configura contraseña de acceso a consola, Contraseña de acceso Telnet, Cifrar las contraseñas de texto no cifrado, Mensaje MOTD, Interfaz S0/0/0, Interfaz S0/0/1, Interfaz G0/0 (simulación de Internet), Interfaz loopback 0 (servidor web simulado), Ruta predeterminada

Tabla 17. Configuración Router 2 escenario 2

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router>enable Router#configure terminal Router(config)#no ip domain-lookup Router(config)#
Nombre del router	Router>enable Router# configure terminal Router(config)#hostname R2 R2(config)#
Contraseña de exec privilegiado cifrada	R2> enable R2# configure terminal R2(config)# enable secret class R2(config)#
Contraseña de acceso a la consola	R2> enable R2# configure terminal R2(config)# line console 0 R2(config-line)# password cisco R2(config-line)# login R2(config-line)# exit R2(config)#
Contraseña de acceso Telnet	R2#configure terminal R2(config)#line vty 0 4 R2(config-line)#lpassword cisco R2(config-line)# login R2(config-line)#exit R2(config)#
Cifrar las contraseñas de texto no cifrado	R2(config)#service password-encryption R2(config)#exit
Habilitar el servidor HTTP	R2# configure terminal R2(config)# ip http server R2(config)# ip http secure-server R(config)# ip http authentication local
Mensaje MOTD	R2# configure terminal R2(config)# banner motd " Se prohíbe el acceso no autorizado." R2(config)# exit

Interfaz S0/0/0	R2#config terminal R2(config)#interface S0/0/0 R2(config-subif)#ip address 172.16.1.2 255.255.255.252 R2(config-subif)#ipv6 address 2001:db8:acad:1: :2 /64 R2(config-subif)#description Conexion R1 R2(config-subif)#clock rate128000 R2(config-subif)#no shutdown R2(config-subif)#exit
Interfaz S0/0/1	R2#config terminal R2(config)#interface S0/0/1 R2(config-subif)#ip address 172.16.2.2 255.255.255.252 R2(config-subif)#ipv6 address 2001:db8:acad:2: :2 /64 R2(config-subif)#description Conexion R3 R2(config-subif)#clock rate128000 R2(config-subif)#no shutdown R2(config-subif)#exit
Interfaz G0/0 (simulación de Internet)	R2#config terminal R2(config)#interface gigabitEthernet 0/0 R2(config-subif)#ip address 209.165.200.233 255.255.255.248 R2(config-subif)#ipv6 address 2001:db8:acad:A: :1 /64 R2(config-subif)#description Conexion Servidor R2(config-subif)#no shutdown R2(config-subif)#exit
Interfaz loopback 0 (servidor web simulado)	R2#configure terminal R2(config)#interface loopback 0 R2(config-if)#ip address 10.10.10.10 255.255.255.255 R2(config-if)#description conexion servidor web
Ruta predeterminada	R2#configure terminal R2(config)#ip route 0.0.0.0 0.0.0.0 172.16.1.1 R2(config)#ip route 0.0.0.0 0.0.0.0 172.16.2.1 R2#configure terminal R2(config)#ipv6 route ::/0 2001:DB8:ACAD:1::1 R2(config)#ipv6 route ::/0 2001:DB8:ACAD:2::1

Figura 30. Configuración Básica Router 2



Fuente: Autor

Se realiza todas las configuraciones básicas, interfaz y las ruta predeterminadas en el Router 2

Paso 4: Configurar R3

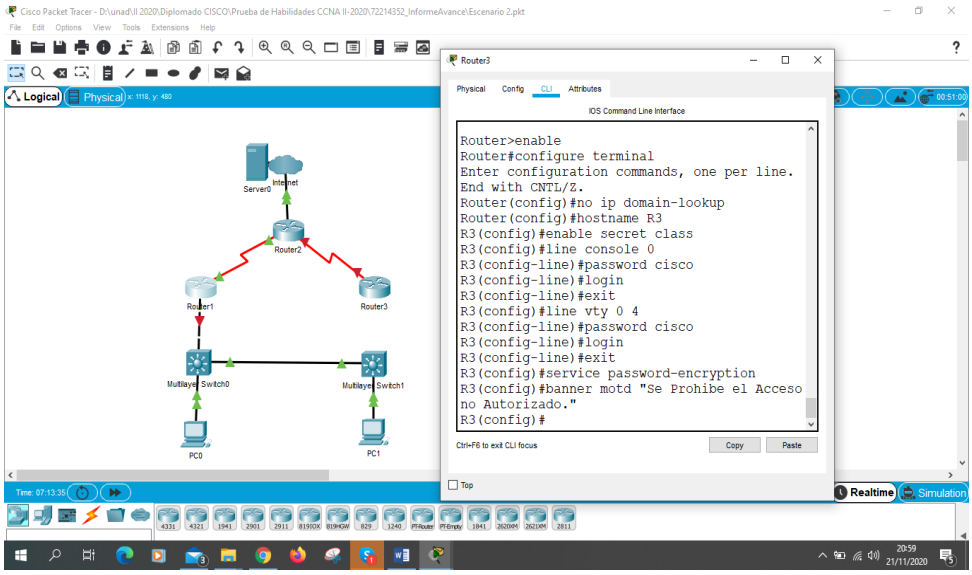
Para la configuración del Router se realizará las siguientes configuraciones como se muestra en la tabla 18. donde procedemos a desactivar la búsqueda DNS, generamos el nombre al router, se crea un dominio, se establecen las contraseñas cifrada para el modo privilegiado, se configura contraseña de acceso a consola, Contraseña de acceso Telnet, Cifrar las contraseñas de texto no cifrado, Mensaje MOTD, Interfaz S0/0/1, Interfaz loopback 4, Interfaz loopback 5, Interfaz loopback 6, Interfaz loopback 7 y Ruta predeterminada

Tabla 18. Configuración Router 3 escenario 2

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router>enable Router#configure terminal Router(config)#no ip domain-lookup Router(config)#
Nombre del router	Router>enable Router# configure terminal Router(config)#hostname R3 R3(config)#
Contraseña de exec privilegiado cifrada	R3> enable R3# configure terminal R3(config)# enable secret class R3(config)#
Contraseña de acceso a la consola	R3> enable R3# configure terminal R3(config)# line console 0 R3(config-line)# password cisco R3(config-line)# login R3(config-line)# exit R3(config)#
Contraseña de acceso Telnet	R3#configure terminal R3(config)#line vty 0 4 R3(config-line)#lpassword cisco R3(config-line)# login R3(config-line)#exit R3(config)#
Cifrar las contraseñas de texto no cifrado	R3(config)#service password-encryption R3(config)#exit
Mensaje MOTD	R3# configure terminal R3(config)# banner motd " Se prohíbe el acceso no autorizado." R3(config)# exit
Interfaz S0/0/1	R3#config terminal R3(config)#interface S0/0/1 R3(config-subif)#ip address 172.16.2.1 255.255.255.252 R3(config-subif)#ipv6 address 2001:db8:acad:2: :1 /64 R3(config-subif)#description Conexion R2 R3(config-subif)#no shutdown R3(config-subif)#exit

Interfaz loopback 4	R3#configure terminal R3(config)#interface loopback 4 R3(config-if)#ip address 192.168.4.1 255.255.255.0 R3(config-if)#description Loopback 4
Interfaz loopback 5	R3#configure terminal R3(config)#interface loopback 5 R3(config-if)#ip address 192.168.5.1 255.255.255.0 R3(config-if)#description Loopback 5
Interfaz loopback 6	R3#configure terminal R3(config)#interface loopback 6 R3(config-if)#ip address 192.168.6.1 255.255.255.0 R3(config-if)#description Loopback 6
Interfaz loopback 7	R3#configure terminal R3(config)#interface loopback 7 R3(config-if)#ipv6 address 2001:db8:acad:3::1/64 R3(config-if)#description Loopback 7
Rutas predeterminadas	R3#configure terminal R3(config)#ip route 0.0.0.0 0.0.0.0 172.16.2.2 R2#configure terminal R2(config)#ipv6 route ::/0 2001:DB8:ACAD:2::2

Figura 31. Configuración Básica Router 3



Fuente: Autor

Se realiza todas las configuraciones básicas, interfaz y las ruta predeterminadas en el Router 3

Paso 5: Configurar S1

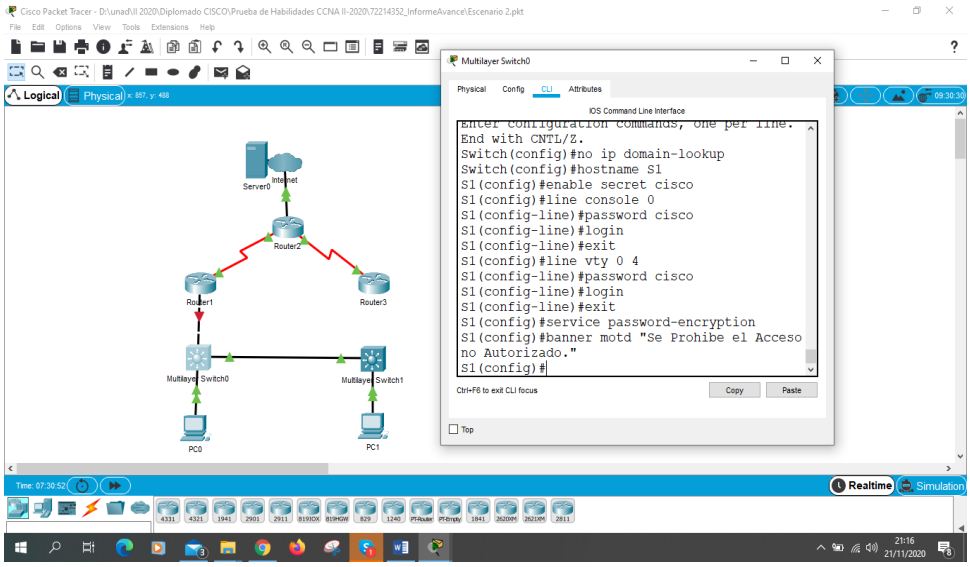
Para la configuración de los switch 1 se realizará las siguientes configuraciones como se muestra en la tabla 19. donde procedemos a desactivar la búsqueda DNS, generamos el nombre al Switch, se establecen las contraseñas cifrada para el modo privilegiado, se configura contraseña de acceso a consola, se configurar líneas VTY solo aceptando conexiones telnet, se Cifran las contraseñas de texto no cifrado, se Configura un MOTD Banner.

Tabla 19. Configuración Switch 1 escenario 2

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch>enable Switch#configure terminal Switch(config)#no ip domain-lookup Switch(config)#
Nombre del switch	switch>enable switch# configure terminal switch(config)#hostname S1 S1(config)#
Contraseña de exec privilegiado cifrada	S1> enable S1# configure terminal S1(config)# enable secret class S1(config)#
Contraseña de acceso a la consola	S1> enable S1# configure terminal S1(config)# line console 0 S1(config-line)# password cisco S1(config-line)# login S1(config-line)# exit S1(config)#
Contraseña de acceso Telnet	S1#configure terminal S1(config)#line vty 0 4 S1(config-line)#lpassword cisco S1(config-line)# login S1(config-line)#exit S1(config)#
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption S1(config)#exit

Mensaje MOTD	S1# configure terminal S1(config)# banner motd " Se prohíbe el acceso no autorizado." S1(config)# exit

Figura 32. Configuración Básica Switch 1



Fuente: Autor

Se realiza las configuraciones básicas en el Switch 1

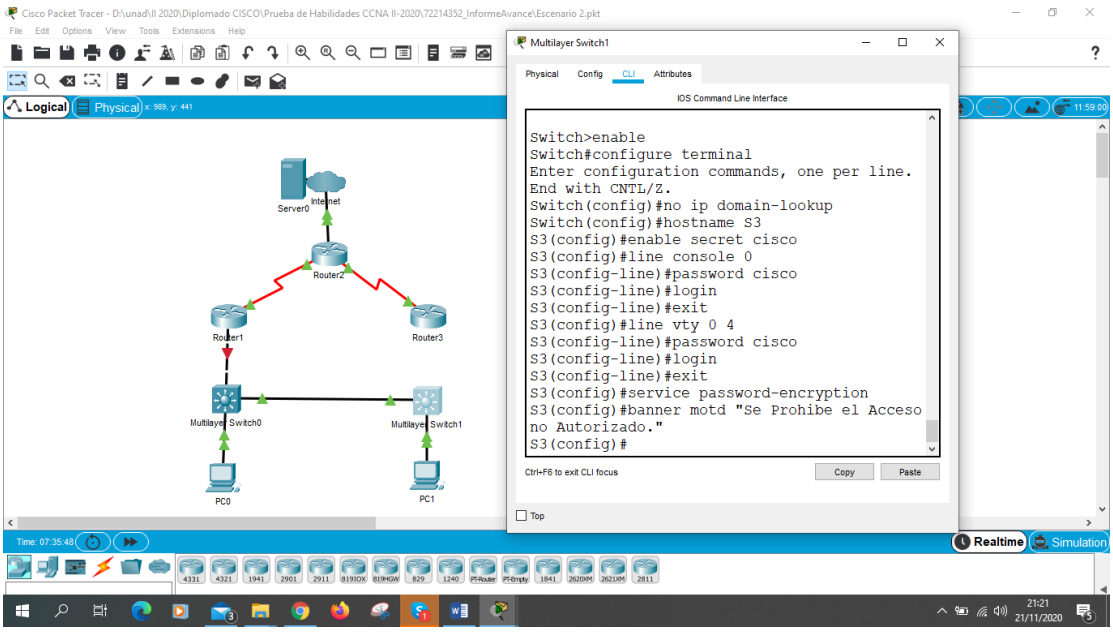
Paso 6: Configurar el S3

Para la configuración de los switch 3 se realizará las siguientes configuraciones como se muestra en la tabla 20. donde procedemos a desactivar la búsqueda DNS, generamos el nombre al Switch, se establecen las contraseñas cifrada para el modo privilegiado, se configura contraseña de acceso a consola, se configurar líneas VTY solo aceptando conexiones telnet, se Cifran las contraseñas de texto no cifrado, se Configura un MOTD Banner.

Tabla 20. Configuración Switch 3 escenario 2

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

Figura 33. Configuración Básica Switch 3



Fuente: Autor

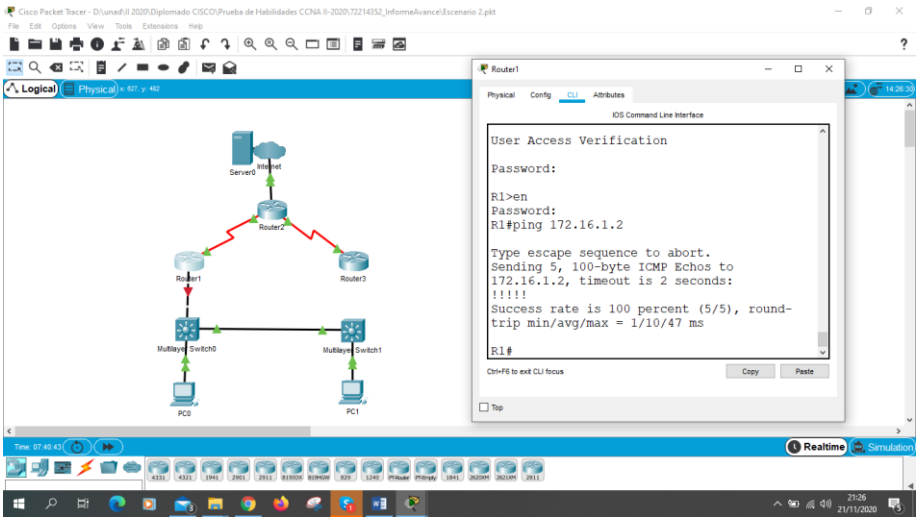
Se realiza las configuraciones básicas en el Switch 3

Paso 7: Verificar la conectividad de la red

Tabla 21. Prueba de conectividad puerto seriales escenario2

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	Correcto
R2	R3, S0/0/1	172.16.2.1	Correcto
PC de Internet	Gateway predeterminado	209.165.200.233	Correcto

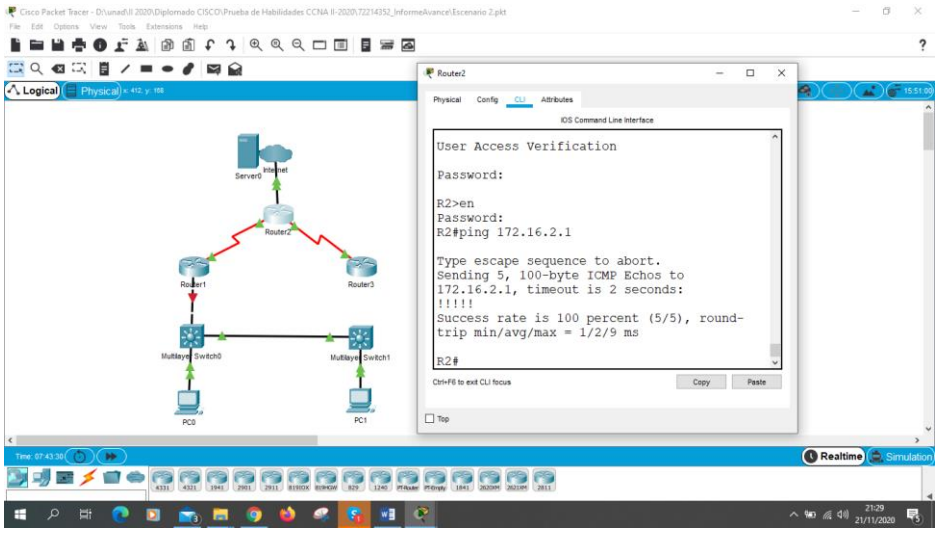
Figura 34. Prueba de conectividad R1 a R2 S0/0/0



Fuente: Autor

Se realiza prueba de conectividad Router 1 ping 172.16.1.2 al Router 2 interfaz S0/0/0 el resultado del ping es que se tiene conexión.

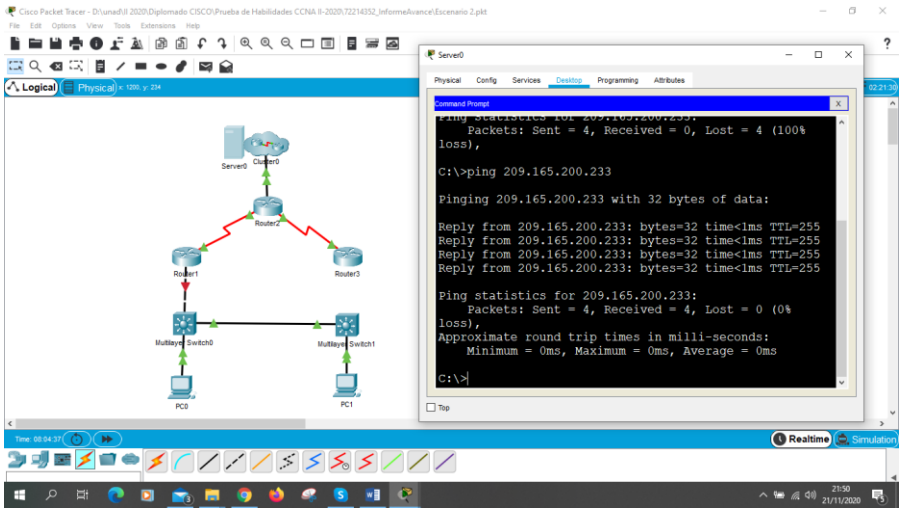
Figura 35. Prueba de Conectividad R2 a R3 S0/0/1



Fuente: Autor

Se realiza prueba de conectividad desde Router 2 ping 172.16.2.1 al Router 3 interfaz S0/0/1 el resultado del ping es que se tiene conexión.

Figura 36. Prueba de conectividad de PC-internet a R2 G0/0



Fuente: Autor

Se realiza prueba de conectividad desde el servidor de internet ping 209.165.200.233 al Router 2 G0/0

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

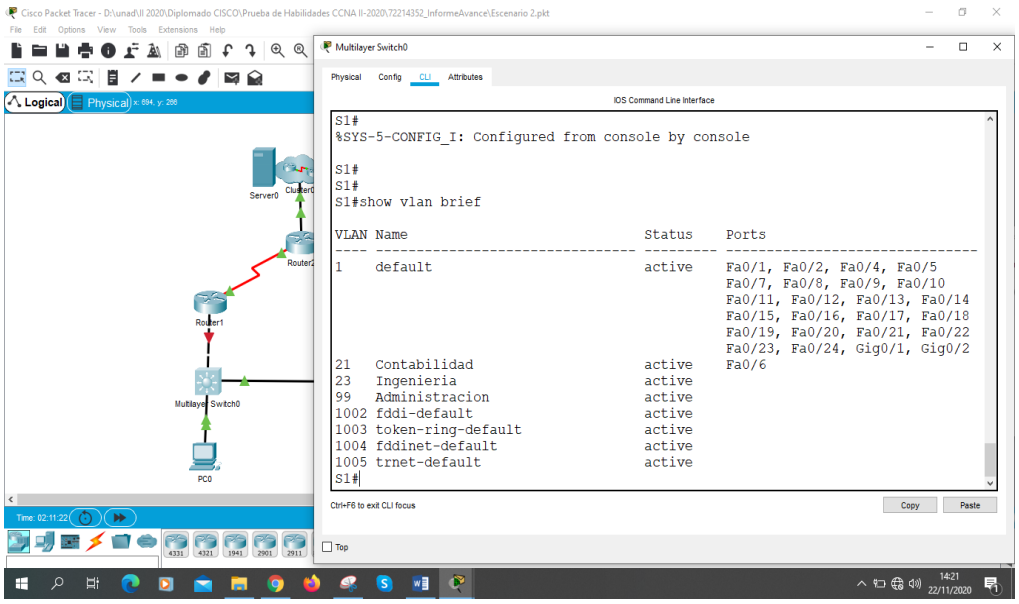
Paso 1: Configurar S1

Para la configuración de la seguridad del switch 1, se crean las VLAN y el routing entre VLAN de los switch 1 se realizará las siguientes configuraciones como se muestra en la tabla 22. donde procedemos a Asignar la dirección IP de administración, se asignar el gateway predeterminado, se Forzar el enlace troncal en la interfaz F0/3 y F0/5, Configurar el resto de los puertos como puertos de acceso, se asigna F0/6 a la VLAN 21 y se apagan los puertos sin usar.

Tabla 22. Configuración de Vlan Switch 1 escenario 2

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	S1(config)#vlan 21 S1(config-vlan)#name Contabilidad S1(config-vlan)#exit S1(config)#vlan 23 S1(config-vlan)#name Ingenieria S1(config-vlan)#exit S1(config)#vlan 99 S1(config-vlan)#name Administracion S1(config-vlan)#exit
Asignar la dirección IP de administración.	S1#configure terminal S1(config)#interface vlan 99 S1(config-vlan)#ip address 192.168.99.2 255.255.255.0
Asignar el gateway predeterminado	S1#configure terminal S1(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	S1#configure terminal S1(config)#interface f0/3 S1(config-if)# switchport mode trunk S1(config-if)#switchport trunk allowed vlan all S1(config-if)#switchport trunk native vlan 1
Forzar el enlace troncal en la interfaz F0/5	S1#configure terminal S1(config)#int f0/5 S1(config-if-range)# switchport trunk encapsulation dot1q S1(config-if-range)# switchport mode trunk S1(config-if-range)#switchport trunk allowed vlan all S1(config-if)#switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	S1#configure terminal S1(config)#int range f0/1-2,f0/4,f0/6-24 S1(config-if-range)#switchport mode access S1(config-if-range)#no shutdown
Asignar F0/6 a la VLAN 21	S1#configure terminal S1(config)#int f0/6 S1(config-if) #switchport access vlan 21
Apagar todos los puertos sin usar	S1#configure terminal S1(config)#int range f0/1-2,f0/4,f0/7-24 S1(config-if-range)#shutdown

Figura 37. Configuración de Vlan en S1



Fuente: Autor

Se crean Vlan en el switch 1 y se configura Vlan de administración, enlaces troncales, se asigna vlan 21 a la interfaz f0/6 y se aseguran los puertos sin usar

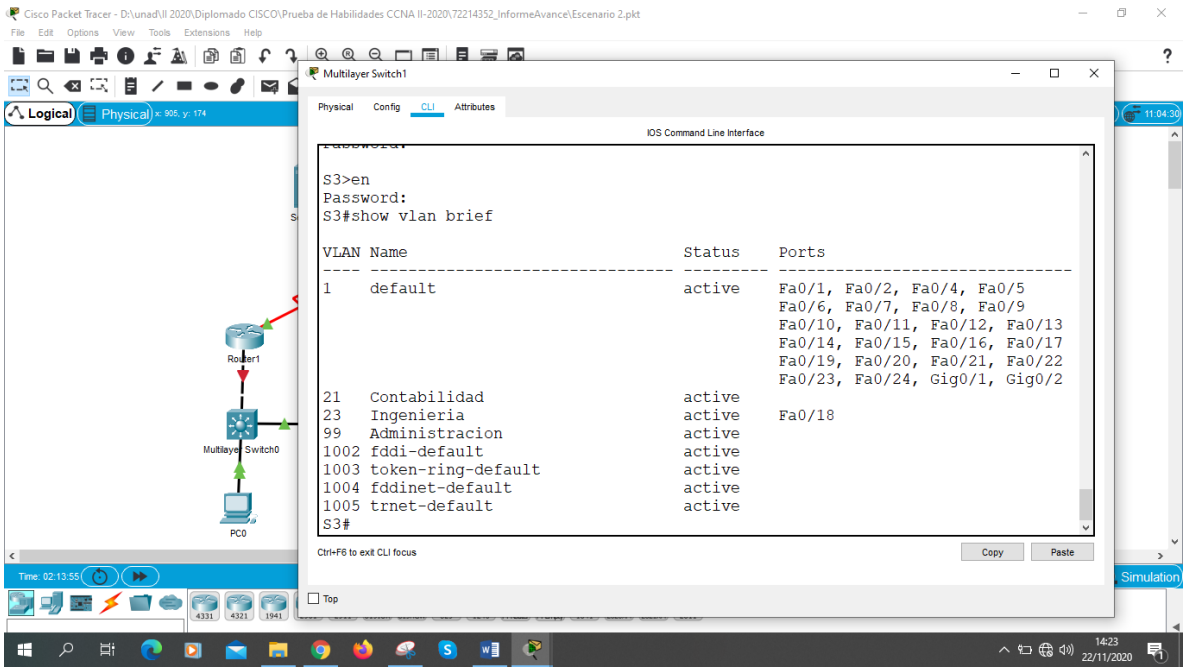
Paso 2: Configurar el S3

Para la configuración de la seguridad del switch 3, se crean las VLAN y el routing entre VLAN de los switch 3 se realizará las siguientes configuraciones como se muestra en la tabla 23. donde procedemos a Asignar la dirección IP de administración, se asignar el gateway predeterminado, se Forzar el enlace troncal en la interfaz F0/3, Configurar el resto de los puertos como puertos de acceso, se asigna F0/18 a la VLAN 23 y se apagan los puertos sin usar.

Tabla 23. Configuración de Vlan Switch 3 escenario 2

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	S3(config)#vlan 21 S3(confi-vlan)#name Contabilidad S3(config-vlan)#exit S3(config)#vlan 23 S3(config-vlan)#name Ingenieria S3(config-vlan)#exit S3(config)#vlan 99 S3(config-vlan)#name Administracion S3(config-vlan)#exit
Asignar la dirección IP de administración	S3#configure terminal S3(config)#interface vlan 99 S3(config-vlan)#ip address 192.168.99.3 255.255.255.0
Asignar el gateway predeterminado.	S3#configure terminal S3(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	S3#configure terminal S3(config)#int f0/3 S3(config-if-range)# switchport mode trunk S3(config-if-range)#switchport trunk allowed vlan all S3(config-if)#switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	S3#configure terminal S3(config)#int range f0/1-2,f0/4-24 S3(config-if-range)#switchport mode access
Asignar F0/18 a la VLAN 23	S3#configure terminal S3(config)#int f0/18 S3(config-if) #switchport access vlan 23
Apagar todos los puertos sin usar	S3#configure terminal S3(config)#int range f0/1-2,f0/4-17,f0/19-24,g0/1-2 S3(config-if-range)#shutdown

Figura 38. Configuración de Vlan en S3



Fuente: Autor

Se crean Vlan en el switch 3 y se configura Vlan de administración, enlaces troncales, se asigna Vlan 23 a la interfaz f0/18 y se aseguran los puertos sin usar

Paso 3: Configurar R1

Se crean las sub interfaz G0/1.21, G0/1.23, G0/1.99 con encapsulación 802.1q y se activa la interfaz G0/1 como se muestra en la tabla 24.

Tabla 24. Configuración de subinterfaces en Router 1

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	R1#config terminal R1(config)#interface gigabitEthernet 0/1.21 R1(config-subif)#encapsulation dot1Q 21 R1(config-subif)#ip address 192.168.21.1 255.255.255.0 R1(confiig-subif)#description vlan 21 R1(config-subif)#no shutdown R1(config-subif)#exit

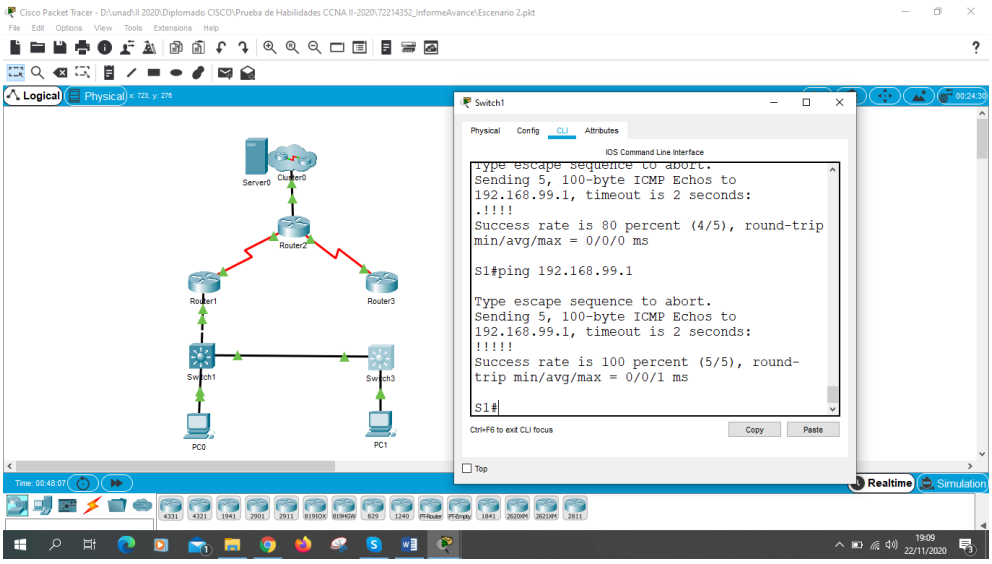
Configurar la subinterfaz 802.1Q .23 en G0/1	R1#config terminal R1(config)#interface gigabitEthernet 0/1.23 R1(config-subif)#encapsulation dot1Q 23 R1(config-subif)#ip address 192.168.23.1 255.255.255.0 R1(confiig-subif)#description vlan 23 R1(config-subif)#no shutdown R1(config-subif)#exit
Configurar la subinterfaz 802.1Q .99 en G0/1	R1#config terminal R1(config)#interface gigabitEthernet 0/1.99 R1(config-subif)#encapsulation dot1Q 99 R1(config-subif)#ip address 192.168.99.1 255.255.255.0 R1(confiig-subif)#description vlan 99 R1(config-subif)#no shutdown R1(config-subif)#exit
Activar la interfaz G0/1	R1#config terminal R1(config)#interface gigabitEthernet 0/1 R1(config-if)#no shutdown

Paso 4: Verificar la conectividad de la red

Tabla 25. Prueba de conectividad de Vlan escenario 2

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

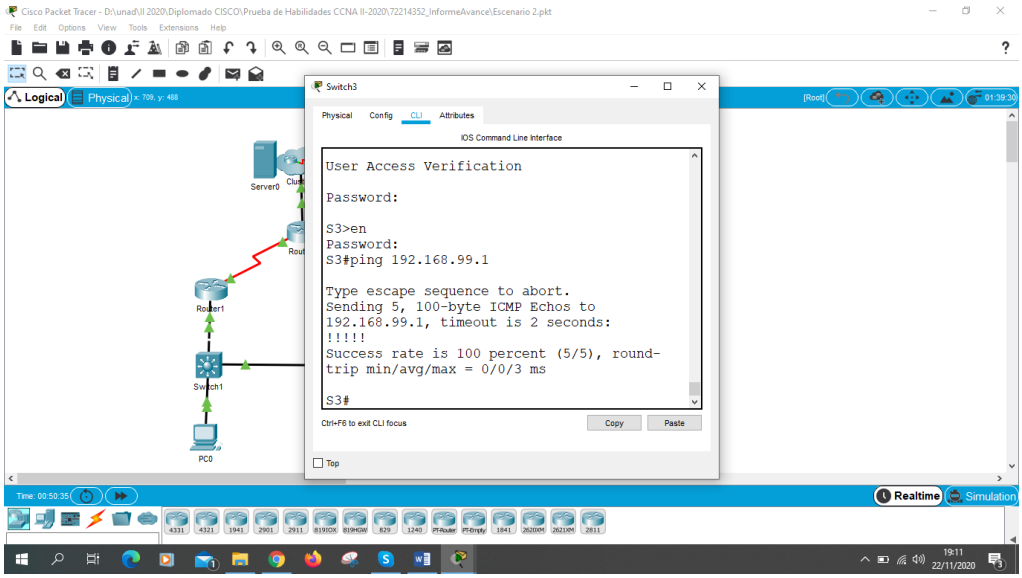
Figura 39. Prueba de Conexión entre S1 y R1 Vlan 99



Fuente: Autor

Configuradas las Vlan y trocales se realiza prueba de conectividad de S1 con el comando ping 192.168.99.1 al R1 interfaz Vlan 99

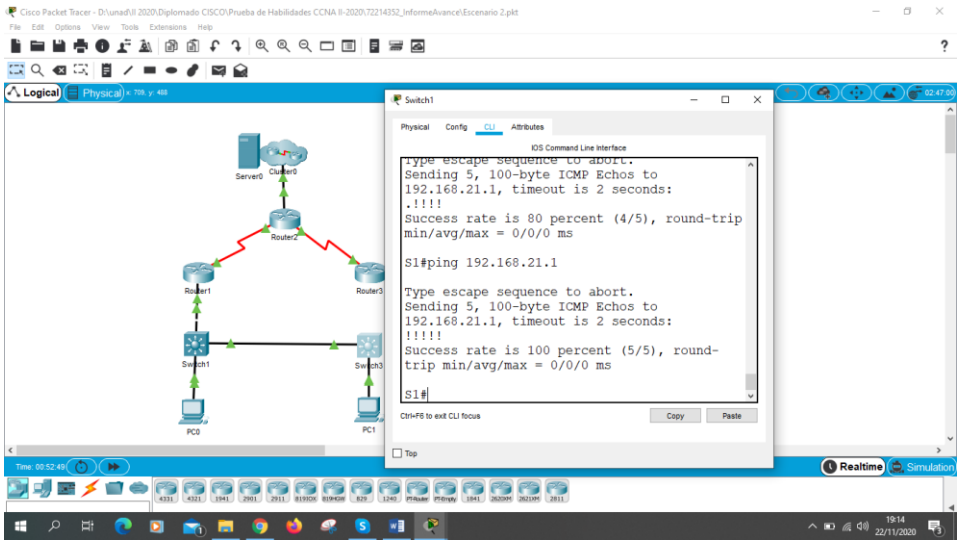
Figura 40. Prueba de conectividad entre S3 y R1 Vlan 99



Fuente: Autor

Configuradas las vlan y trocales se realiza prueba de conectividad de S3 con el comando ping 192.168.99.1 al R1 interfaz vlan 99

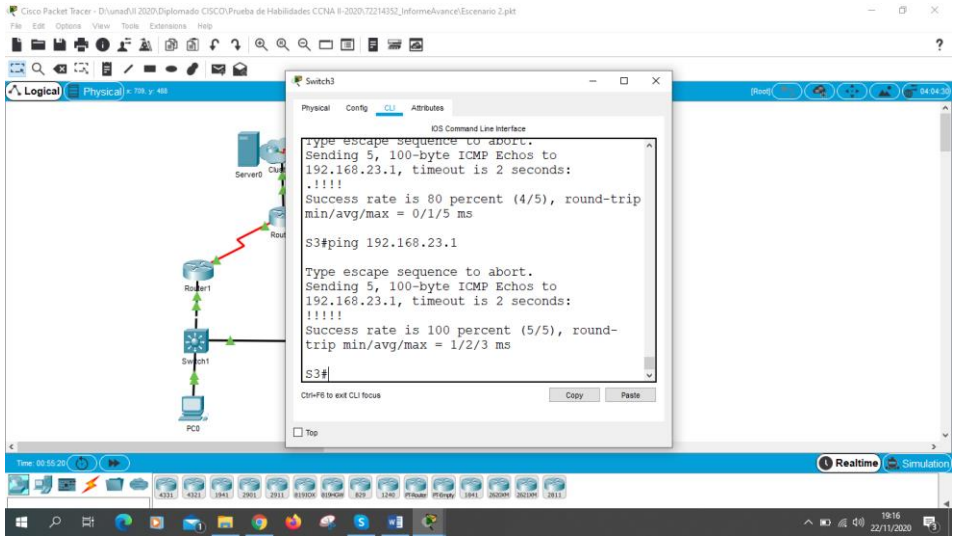
Figura 41. Prueba de Conectividad entre S1 y R1 Vlan 21



Fuente: Autor

Configuradas las Vlan y trocales se realiza prueba de conectividad de S1 con el comando ping 192.168.21.1 al R1 interfaz Vlan 21

Figura 42. Prueba de conectividad entre S3 y R1 Vlan 23



Fuente: Autor

Configuradas las vlan y trocales se realiza prueba de conectividad de S3 con el comando ping 192.168.23.1 al R1 interfaz vlan 23

Parte 4: Configurar el protocolo de routing dinámico OSPF

Paso 1: Configurar OSPF en el R1

En el Router 1 se configura el OSPF con área 0 como se muestra en la tabla 26. Se anuncian las redes conectadas directamente y se establece las subinterfaces como pasivas

Tabla 26. Configuración OSPF en Roter 1

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R1#Configure terminal R1(config)#router ospf 1 R1(config-router)#router-id 1.1.1.1
Anunciar las redes conectadas directamente	R1(config-router)#network 172.16.1.0 0.0.0.3 area 0 R1(config-router)#network 192.168.21.0 0.0.0.255 area 0 R1(config-router)#network 192.168.23.0 0.0.0.255 area 0 R1(config-router)#network 192.168.99.0 0.0.0.255 area 0
Establecer todas las interfaces LAN como pasivas	R1(config-router)#passive-interface g0/1.21 R1(config-router)#passive-interface g0/1.23 R1(config-router)#passive-interface g0/1.99
Desactive la sumarización automática	**No aplica**

Paso 2: Configurar OSPF en el R2

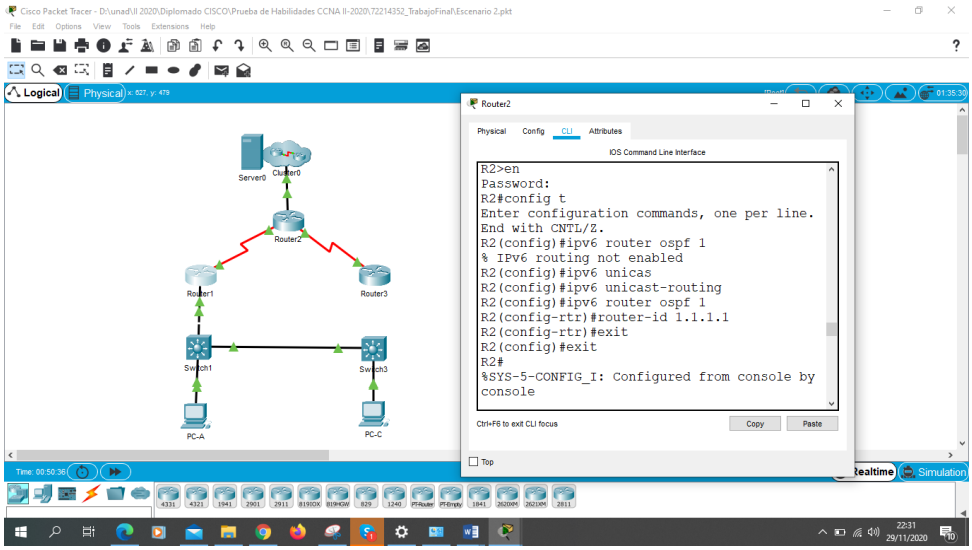
En el Router 2 se configura el OSPF con área 0 como se muestra en la tabla 27. Se anuncian las redes conectadas directamente y se establece la interfaz LAN looopback0 como pasivas

Tabla 27. Configuración OSPF en Router 2

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R2#Configure terminal R2(config)#router ospf 1 R2(config-router)#router-id 2.2.2.2
Anunciar las redes conectadas directamente	R2(config-router)#network 10.10.10.10 0.0.0.0 area 0 R2(config-router)#network 172.16.1.0 0.0.0.3 area 0 R2(config-router)#network 172.16.2.0 0.0.0.3 area 0
Establecer la interfaz LAN (loopback) como pasiva	R2(config-router)#passive-interface lo0
Desactive la sumarización automática.	No aplica

Paso 3: Configurar OSPFv3 en el R2

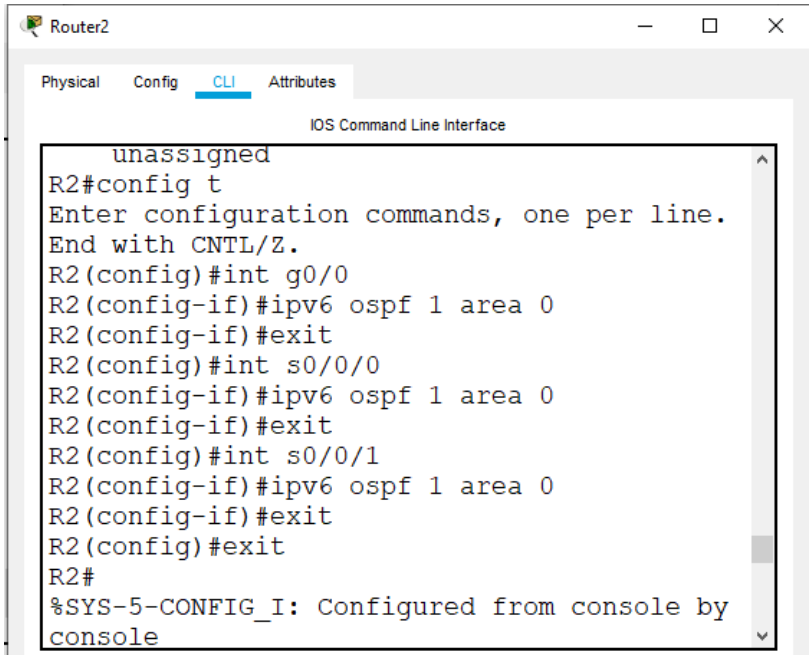
Figura 43. Configuración OSPF V3 Router 2



Fuente: Autor

Se configura el OSPF v3 en el router 2

Figura 44. Configuración OSPF v3 interface



Fuente: Autor

Se configura las interfaces para OSPFv3 en el router 2

Paso 4: Configurar OSPF en el R3

En el Router 3 se configura el OSPF con área 0 como se muestra en la tabla 27. Se anuncian las redes conectadas directamente y se establece la interfaz LAN looopback0 como pasivas

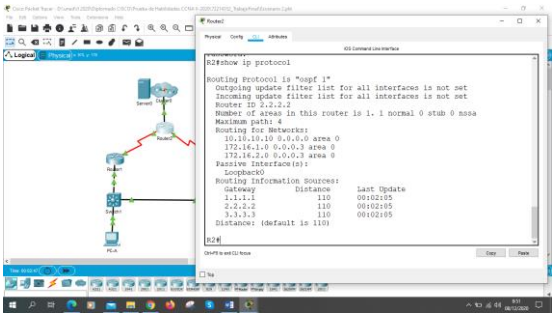
Tabla 28. Configurar OSPF en Router 3

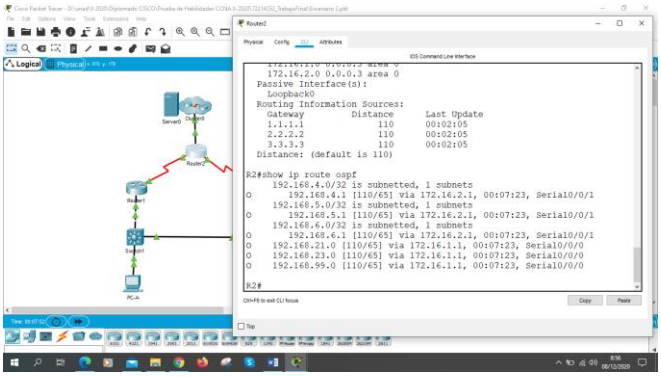
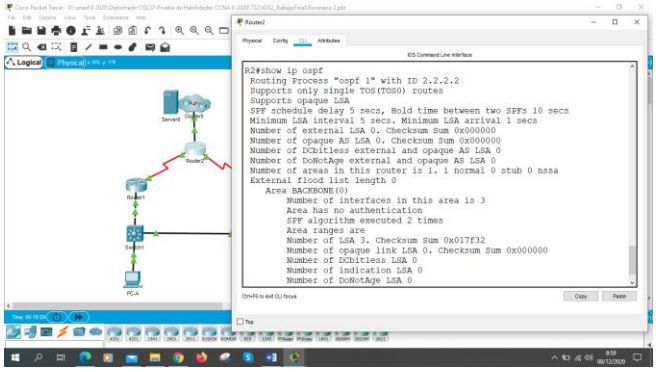
Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R3#Configure terminal R3(config)#router ospf 1 R3(config-router)#router-id 3.3.3.3

Anunciar redes IPv4 conectadas directamente	R3(config-router)#network 172.16.2.0 0.0.0.3 area 0 R3(config-router)#network 192.168.4.0 0.0.0.255 area 0 R3(config-router)#network 192.168.5.0 0.0.0.255 area 0 R3(config-router)#network 192.168.6.0 0.0.0.255 area 0
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	R3(config-router)#passive-interface lo4 R3(config-router)#passive-interface lo5 R3(config-router)#passive-interface lo6
Desactive la sumarización automática.	No aplica

Paso 5: Verificar la información de OSPF

Tabla 29. Verificación de funcionamiento OSPF en Router 2

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 protocol Figura 45. Verificación de procesos OSPF en Router 2.  Fuente: Autor Con el comando Show ip protocol nos muestra la id del proceso OSPF, la id del router y redes routing, como las interface pasivas

¿Qué comando muestra solo las rutas OSPF?	Show ip route ospf Figura 46. Verificación de rutas OSPF  Fuente: Autor Con el comando show ip route ospf, nos muestra solo las rutas OSPF que tiene configuradas el Router 2
¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	Show ip ospf Figura 47. Verificación de la sección OSPF en ejecución.  Fuente: Autor Con el comando show ip OSPF nos muestra la sección de OSPF de configuración en ejecución.

Parte 5: Implementar DHCP y NAT para IPv4

Paso 1: Configurar el R1 como servidor de DHCP para las VLAN 21 y 23

Se configura en R1 como servidor DHCP para Las Vlans 21 y 23 reservando las primeras 20 direcciones de cada red, como se muestra en la tabla 30

Tabla 30. Configuración R1 como servidor de DHCP para las VLAN 21 y 23

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	R1#configure terminal R1(config)# ip dhcp excluded-address 192.168.21.1 192.168.21.20
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	R1#configure terminal R1(config)# ip dhcp excluded-address 192.168.23.1 192.168.23.20
Crear un pool de DHCP para la VLAN 21.	R1#configure terminal R1(config)#ip dhcp pool ACCT R1(dhcp-config)#network 192.168.21.0 255.255.255.0 R1(dhcp-config)#default-router 192.168.21.1 R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com
Crear un pool de DHCP para la VLAN 23	R1#configure terminal R1(config)#ip dhcp pool ENGNR R1(dhcp-config)#network 192.168.23.0 255.255.255.0 R1(dhcp-config)#default-router 192.168.23.1 R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com

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

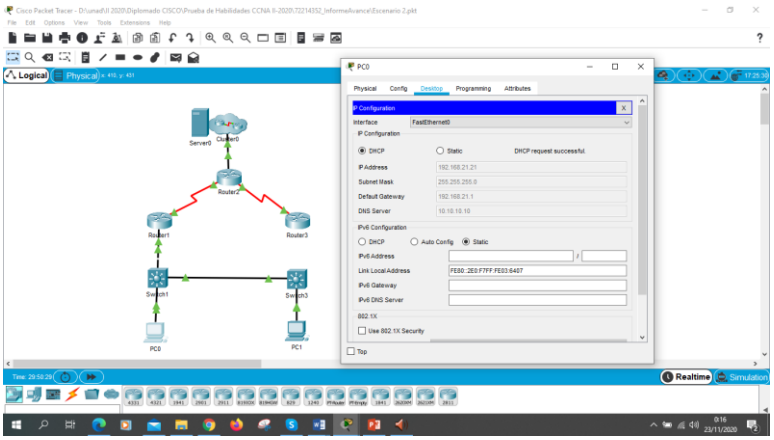
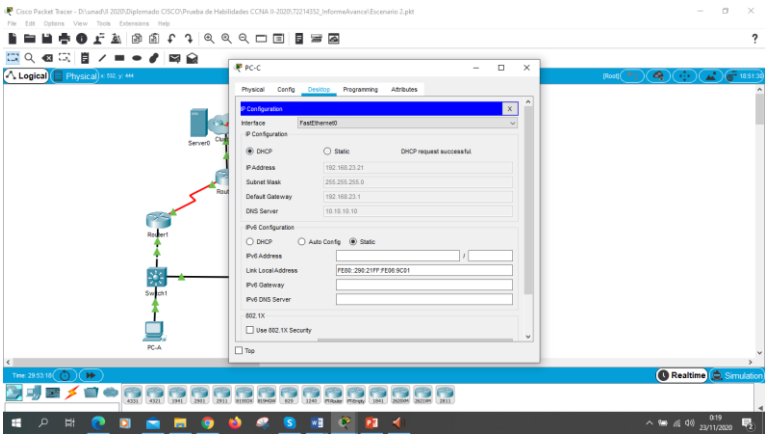
Se configura en el Router 2 la NAT estática y dinámica como se muestra en la tabla 31. Primero se crea una base de datos local con una cuenta de usuario, se configura un servidor HTTP utilizando la base de datos local para la autenticación, se crea una NAT estática al servidor web, se asigna la interfaz interna y externa para la NAT estática, se configura la NAT dinámica dentro de una ACL privada, se define el pool de direcciones IP públicas utilizables, se define la traducción de NAT dinámica

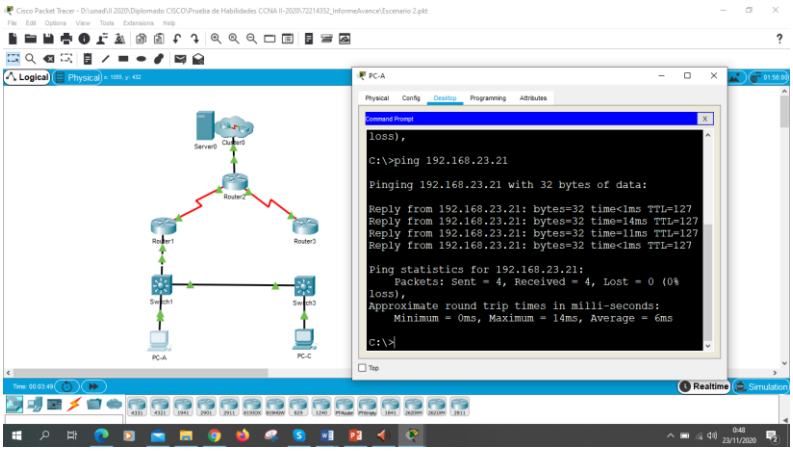
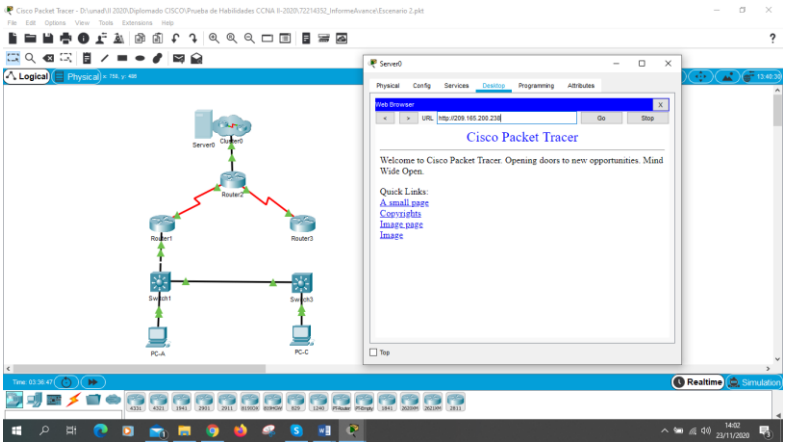
Tabla 31. Configuración de NAT estática y dinámica en R2

Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	R2#config t R2(config)#user webuser privilege 15 secret cisco12345
Habilitar el servicio del servidor HTTP	R2#config t R2(config)#ip http server
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	R2#config t R2(config)#ip http authentication local
Crear una NAT estática al servidor web.	R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229
Asignar la interfaz interna y externa para la NAT estática	R2#config t R2(config)#interface g0/0 R2(config-if)#ip nat outside R2(config-if)#exit R2(config)# R2(config)#interface Lo0 R2(config-if)#ip nat inside R2(config-if)#exit
Configurar la NAT dinámica dentro de una ACL privada	R2#config t 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 192.168.4.1 0.0.0.255 R2(config)#access-list 1 permit 192.168.5.1 0.0.0.255 R2(config)#access-list 1 permit 192.168.6.1 0.0.0.255
Defina el pool de direcciones IP públicas utilizables.	R2#config t R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248
Definir la traducción de NAT dinámica	R2#config t R2(config)#ip nat inside source list 1 pool INTERNET

Paso 3: Verificar el protocolo DHCP y la NAT estática

Tabla 32. Verificación de protocolo DHCP y NAT estática

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	Figura 48. Conexión DHCP PC-A  Fuente: Autor En el PC-A se aceza a desktop luego se da clic IP configuración y se selecciona DHCP para que el servidor DHCP del Router 1 le asigne un IPv4.
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	Figura 49. Conexión DHCP PC-C  Fuente: Autor En el PC-C se aceza a desktop luego se da clic IP configuración y se selecciona DHCP para que el servidor DHCP del Router 1 le asigne un IPv4.

Verificar que la PC-A pueda hacer ping a la PC-C Nota: Quizá sea necesario deshabilitar el firewall de la PC.	Figura 50. Prueba de conectividad entre PC-A y PC-C  Fuente: Autor Una vez asignadas la ipv4 a los PC se precede a realizar una prueba de conectividad entre PC-A y la PC-C con el comando ping 192.168.23.21
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 51. Acceso a al servidor web  Fuente: Autor Se utiliza el navegador web del servidor de internet para acezar al servidor web

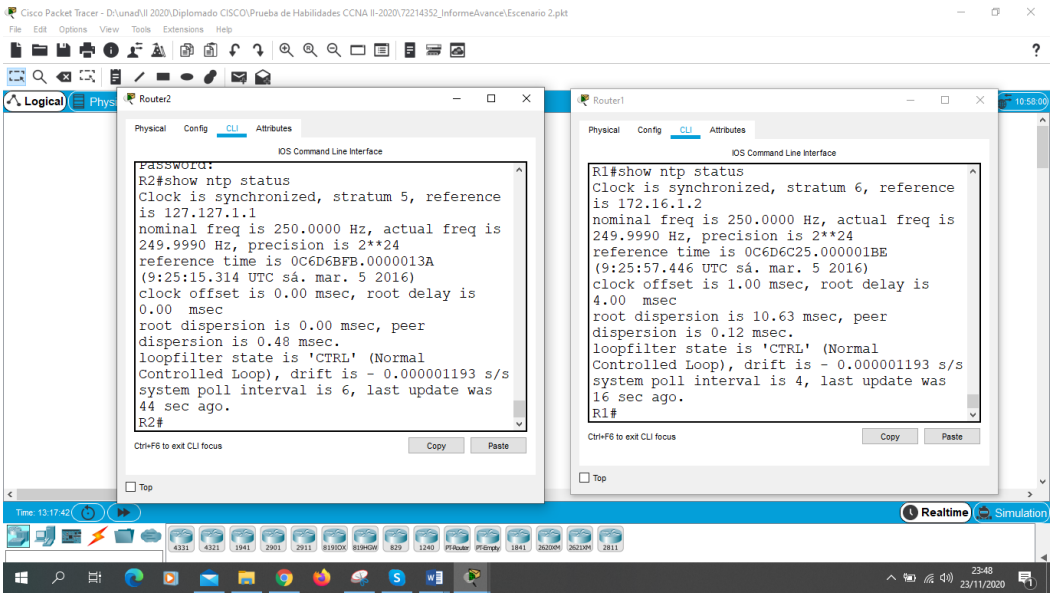
Parte 6: Configurar NTP

Se configura Servidor NTP en router 2 como master y el router 1 se configura para que se sincronice con R2 como se muestra en la tabla 33.

Tabla 33. Configuracion de servidor NTP en Router 2

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

Figura 52. Verificación estado NTP en R1 y R2



Fuente: Autor

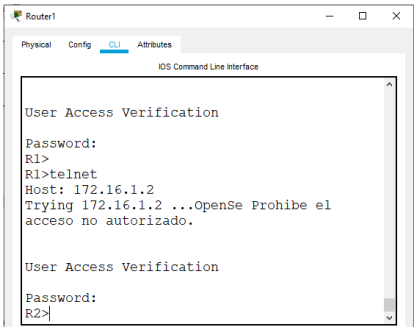
Luego de configuran el servidor NTP en el Router 2 y configura que el Router 1 se sincronice con el Router 2 se procede a dar el comando show ntp status y nos muestra la hora y fecha y que esta sincronizado

Parte 7: Configurar y verificar las listas de control de acceso (ACL)

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

Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2, se aplica la ACL con nombre a las líneas VTY, se permite acceso por Telnet a las líneas de VTY y Verificar que la ACL funcione. Como se muestra en la tabla 34.

Tabla 34. Configura y Verificar listas de control de acceso (ACL)

Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	R2(config)#ip access-list standard ADMIN-MGT R2(config-std-nacl)#permit host 172.16.1.2 R2(config-std-nacl)#exit
Aplicar la ACL con nombre a las líneas VTY	R2(config)#line vty 0 4 R2(config-line)#access-class ADMIN-MGT in R2(config-line)#exit
Permitir acceso por Telnet a las líneas de VTY	R2(config)#line vty 0 4 R2(config)#transport input telnet
Verificar que la ACL funcione como se espera	Figura 53. Conexión telnet desde R1 a R2  Fuente: Autor Se verifica que el ACL quede bien configurado accediendo desde el Router 1 con telnet al Router 2 y solicitando la contraseña.

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

En la tabla 35 se muestra los comandos IOS para Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció, Restablecer los contadores de una lista de acceso, mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica, comando se muestran las traducciones NAT y se utiliza para eliminar las traducciones de NAT dinámicas

Tabla 35. Comandos IOS

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	R1#Show Access-list
Restablecer los contadores de una lista de acceso	R1(config)#clear Access-list counters 1
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	R1#show ip interfaces
¿Con qué comando se muestran las traducciones NAT?	R1#show ip nat translations
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	R1(config)#clear ip nat translations

CONCLUSIONES

En este trabajo de prueba de habilidades del Diplomado de profundización cisco, administramos e implementamos dos escenarios de red mediante el aplicativo de simulación Packet Tracer, se practicarón los conceptos vistos en los laboratorios como la configuración de enrutamiento entre VLAN, DHCP, Etherchannel y la importancia de configurar claves de acceso y su encriptación para evitar que personas no autorizadas puedan acceder a los equipos de red. Este tipo de escenarios son muy importantes para la vida profesional ya que esta herramienta de simulación Packet Tracer.

Escenario 1 se identifica los protocolos de administración de red disponibles en el IOS, para resolver los problemas de las redes de datos LAN/WAN, evaluando el desempeño de routers y switches, mediante el uso de comandos especializados en gestión de redes, con la configuración de Vlan se mejora en seguridad y tiene ventajas para los administradores de red. Se programó el Etherchannel el cual mejora el ancho de banda entre los dos Switch y en caso de fallar una del interfaz nos perdería la conexión ya que la conexión quedaría por la otra interfaz.

Escenario 2 se diseña enrutamiento dinámico OSPF, bajo un esquema de direccionamiento IP, para poder dar solución y conectividad a la red, al igual se mejora en la seguridad y acceso a la WAN mediante las listas de control de acceso ACL permitiendo solo el acceso por telnet desde el Router 1 y traducción de direcciones IP sobre NAT y se configuro la sincronización del R1 con servidor NTP

REFERENCIAS

CISCO. (2019). Protocolos y comunicaciones de red. Fundamentos de Networking. Recuperado de: https://staticcourseassets.s3.amazonaws.com/ITN6/es/index.html#3

CISCO. (2019). Acceso a la red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#4

CISCO. (2019). Capa de red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#6

CISCO. (2019). División de redesIP en subredes. Fundamentos de Networking. Recuperado de: https://staticcourseassets.s3.amazonaws.com/ITN6/es/index.html#8

CISCO. (2019). Configuración de un sistema operativo de red. Fundamentos de Networking. Recuperado de: https://staticcourseassets.s3.amazonaws.com/ITN6/es/index.html#11

CISCO. (2019). Routing Dinámico. Principios de Enrutamiento y Conmutación. Recuperado de: https://staticcourseassets.s3.amazonaws.com/RSE6/es/index.html#3

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

ANEXO

Anexo A link de descarga del escenario 1
https://drive.google.com/file/d/1nrGCtloJWjjt8Ru92IlEedQcThelQug2/view?usp=sharing

Anexo B link de descarga del escenario 2
https://drive.google.com/file/d/1UoINo-bvlxcxLXBYkiV9ZTy2Dc_elNBX/view?usp=sharing

Anexo C link de descarga artículo científico

SOLUCIÓN DE ESCENARIO 2 PRESENTE EN ENTORNOS CORPORATIVOS BAJO EL USO DE TECNOLOGÍA CISCO

Edgar Enrique Duque Acosta
Universidad Nacional Abierta y a Distancia UNAD, eeduquea@unadvirtual.edu.co

Resumen

El presente documento tiene como finalidad desarrollar el escenario 2 prueba de habilidades del diplomado de profundización Cisco, el cual se plantea configuración y la interconexión de los dispositivos de red, de acuerdo al direccionamiento IP mostrado en la topología. se dará solución al problema planteado aplicando los conocimientos adquiridos duran la elaboración de los laboratorios CCNA1 y CCNA2.

Se aplicarán los conceptos de redes como las configuraciones básicas de los routers y conmutadores y la importancia de la seguridad de acceso a dichos equipos. Para ello, existe la herramienta Packet Tracer donde se pueden simular los protocolos de enrutamiento dinámico OSPF, el direccionamiento del enrutador DHCP. Y la creación de Vlan

Palabras clave: DHCP, Enrutamiento, OSPF, Vlan.

Abstract:

The purpose of this document is to develop scenario 2 skills test of the Cisco in-depth diploma, which considers the configuration and interconnection of network devices, according to the IP addressing shown in the topology. a solution will be given to the problem raised, applying the knowledge acquired during the elaboration of the CCNA1 and CCNA2 laboratories.

The concepts of networks will be applied such as the basic configurations for the routers and switches and the importance of access security to said equipment. For this, there is the packet tracer tool where the dynamic routing protocols OSPF, the DHCP Router addressing can be simulated. And the creation of Vlan.

Keywords*— *DHCP, Routing, OSPF, Vlan.

INTRODUCCIÓN

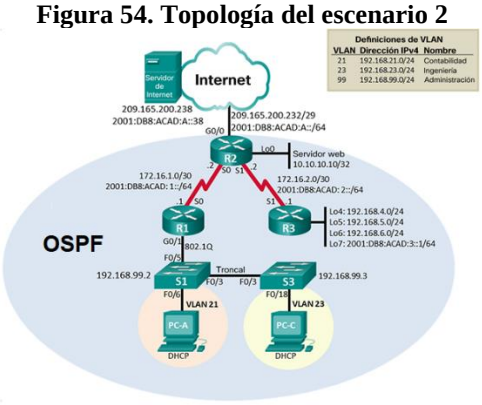
La prueba de habilidades del diplomado cisco, busca prepara a los profesionales en la implementación de tecnologías adecuadas para el diseño y configuración de redes basados en Router, switch y servidores con el fin de mejorar el rendimiento, seguridad de las redes y el enrutamiento de estas.

Para el escenario 2 se investigara el mejoramiento en el direccionamiento dinámico al usar el algoritmo Dijkstra con el protocolo OSPF al calcular la ruta más corta entre nodos y dar solución a los requerimientos solicitados por el usuario donde se aplicará los conceptos visto durante los cursos CCNA1 introducción a las redes y CCNA 2 Routing and Switching, se configurará una red para que admita conectividad IPv4 e IPv6, seguridad en los switches, la configuración VLAN están permiten mejorar el rendimiento y reducir los costos y el tamaño de dominio de difusión, el protocolo de configuración de hosts dinámicos (DHCP).

I. METODOLOGIA

Escenario 2

Figura 54. Topología del escenario 2



Se configura en Packet Tracer la topología de red del escenario 2

Para la configuracion de la red tenemos que realizar una tabla de direcionamiento.

Tabla 36. Direccionamiento de red.

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
R1 S0/0/0	172.16.1.1/30	No corresponde
	2001:db8:acad :1: :1 /64	No corresponde
R1 G0/0/1.21	192.168.21.1/ 24	No corresponde
R1 G0/0/1.23	192.168.23.1/ 24	No corresponde
R1 G0/0/1.99	192.168.99.1/ 24	No corresponde
R2 S0/0/0	172.16.1.2/30	No corresponde
	2001:DB8:AC AD:1::2/64	No corresponde
R2 S0/0/1	172.16.2.2/30	No corresponde
	2001:DB8:AC AD:2::2/64	No corresponde
R2 G0/0	209.165.200.2 33/29	No corresponde
	2001:DB8:AC AD:A::1/64	No corresponde
R2 Lo0	10.10.10.10/3 2	No corresponde
R3 S0/0/1	172.16.2.1/30	10.19.8.97
	2001:DB8:AC AD:2::1/64	No corresponde
R3 Lo4	192.168.4.1/2 4	No corresponde
R3 Lo5	192.168.5.1/2 4	No corresponde
R3 Lo 6	192.168.6.1/2 4	No corresponde
S1 Vlan 99	192.168.99.2	192.168.99.1
S3 Vlan 99	192.168.99.3	192.168.99.1
Servidor de Internet	209.165.200.2 38	209.165.200.2 33
	2001:DB8:AC AD:2::38	2001:DB8:AC AD:2::1
PC-A	DHCP	192.168.21.1
PC-C	DHCP	192.168.23.1

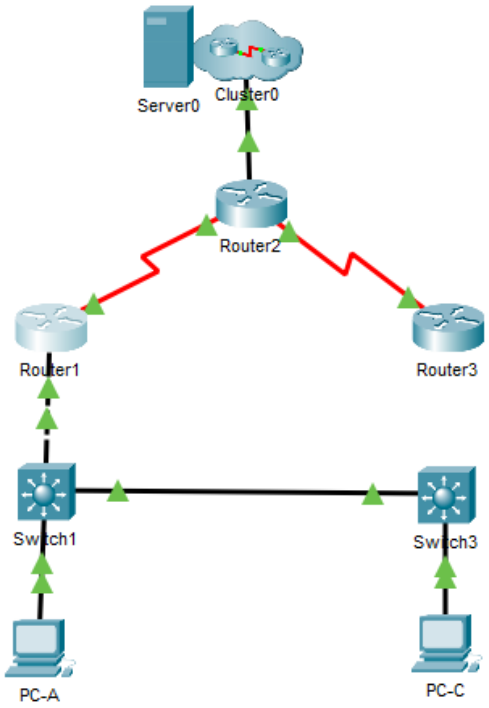
Se crea tabla de direccionamiento para el escenario 2

Tenido la tabla de direccionamiento procedemos a diseñar y configurar la red en Packet Tracer, para este escenario 2 escogemos los siguientes elementos de red.
3 Router 2901
2 Switch multicapa 3560 de 24 puertos
1 Servidor de Internet
2 PC
Procedemos a interconectar la red como se muestra

en la topología.

.

Figura 55. Diseño de red en Packet Tracert



Fuente: Autor

Se configura en Packet Tracer la topología de red del escenario 2

Antes de configurar los routers y switchs, se debe inicializar y recargar los equipos y configurar la tabla SDM en los switch para que admita IPv4 e IPv6 como se muestra en la tabla 2.

Tabla 37. Inicializar Routers y Switch

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	Router > enable Router # erase startup-config
Volver a cargar todos los routers	Router # reload
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Switch > enable Switch # delete vlan.dat Switch # erase startup-config
Volver a cargar ambos switches	Switch # reload
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Switch > enable Switch # show vlan brief
Configure la plantilla SDM en los switch para que admita IPv6	Switch > enable Switch # config t Switch(config)# sdm prefer dual-ipv4-and-ipv6 routing

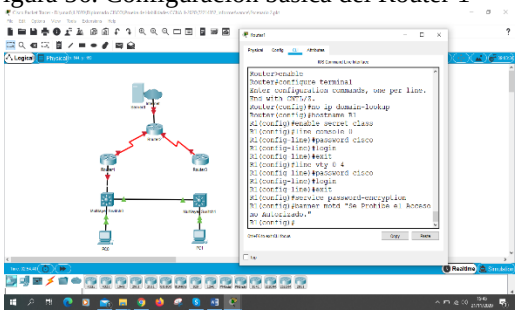
Se configure la computadora internet de acuerdo a la tabla de direccionamiento.

Tabla 38. Configuración de IP en Computador Internet

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.233
Dirección IPv6/subred	2001:DB8:ACAD:2::38
Gateway predeterminado IPv6	2001:DB8:ACAD:2::1

Configuración básica de los Router y Switch

Figura 56. Configuración básica del Router 1



Fuente: Autor

Para la configuración del Router 1 se realizará las siguientes configuraciones como se muestra en la tabla 4. donde procedemos a desactivar la búsqueda DNS, generamos el nombre al router, se crea un dominio, se establecen las contraseñas cifrada para el modo privilegiado, se configura contraseña de acceso a consola, se configura contraseña de acceso Telnet, se Cifran las contraseñas de texto no cifrado, se crea un mensaje MOTD, se configura la Interfaz S0/0/0, Rutas predeterminadas como se muestra tabla de direccionamiento.

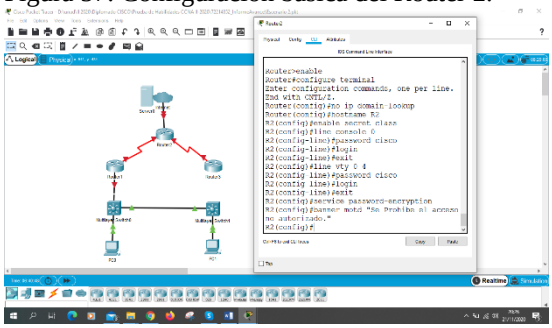
Tabla 39. Configuración Router 1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router>enable Router#configure terminal Router(config)#no ip domain-lookup Router(config)#
Nombre del router	Router>enable Router# configure terminal Router(config)#hostname R1 R1(config)#
Contraseña de exec privilegiado cifrada	R1> enable R1# configure terminal R1(config)# enable secret class R1(config)#
Contraseña de acceso a la consola	R1> enable R1# configure terminal R1(config)# line console 0 R1(config-line)# password cisco R1(config-line)# login R1(config-line)# exit R1(config)#
Contraseña de acceso Telnet	R1#configure terminal R1(config)#line vty 0 4 R1(config-line)#password cisco R1(config-line)# login R1(config-line)#exit R1(config)#
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption R1(config)#exit
Mensaje MOTD	R1# configure terminal R1(config)# banner motd " Se prohíbe el acceso no autorizado." R1(config)# exit
Interfaz S0/0/0	R1#config terminal R1(config)#interface s 0/0/0 R1(config-subif)#ip address 172.16.1.1 255.255.255.252 R1(config-subif)#ipv6 address 2001:db8:acad:1: :1 /64 R1(config-subif)#description Conexion R2 R1(config-subif)#no shutdown R1(config-subif)#exit
Rutas predeterminadas	R1#configure terminal R1(config)#ip route 0.0.0.0 0.0.0.0 172.16.1.2 R1#configure terminal R1(config)#ipv6 route ::/0 2001:DB8:ACAD:1::2

Se realiza la Configuración básica del

Router 2

Figura 57. Configuración básica del Router 2.



Fuente: Autor

Para la configuración del Router 2 se realizará las siguientes configuraciones como se muestra en la tabla 5. donde procedemos a desactivar la búsqueda DNS, generamos el nombre al router, se crea un dominio, se establecen las contraseñas cifrada para el modo privilegiado, se configura contraseña de acceso a consola, se crea contraseña de acceso Telnet, se cifran las contraseñas de texto no cifrado, se crea un mensaje MOTD, se configura la Interfaz S0/0/0, Interfaz S0/0/1, Interfaz G0/0, Interfaz loopback0, Ruta predeterminada como está la tabla de direccionamiento

Tabla 40. Configuración Router 2

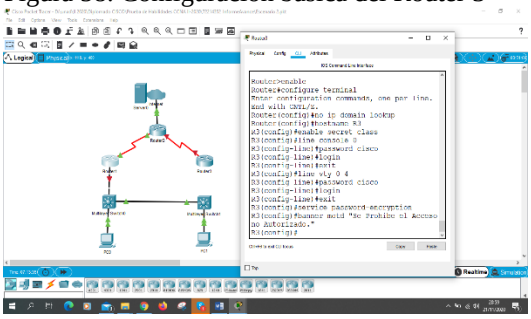
Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router>enable Router#configure terminal Router(config)#no ip domain-lookup Router(config)#
Nombre del router	Router>enable Router# configure terminal Router(config)#hostname R2 R2(config)#
Contraseña de exec privilegiado cifrada	R2> enable R2# configure terminal R2(config)# enable secret class R2(config)#
Contraseña de acceso a la consola	R2> enable R2# configure terminal R2(config)# line console 0 R2(config-line)# password cisco R2(config-line)# login R2(config-line)# exit R2(config)#
Contraseña de acceso Telnet	R2#configure terminal R2(config)#line vty 0 4 R2(config-line)#password cisco R2(config-line)# login R2(config-line)#exit R2(config)#
Cifrar las contraseñas de texto no cifrado	R2(config)#service password-encryption R2(config)#exit
Habilitar el servidor HTTP	R2# configure terminal R2(config)# ip http server R2(config)# ip http secure-server R(config)# ip http authentication local
Mensaje MOTD	R2# configure terminal R2(config)# banner motd " Se prohíbe el acceso no autorizado." R2(config)# exit
Interfaz S0/0/0	R2#config terminal R2(config)#interface S0/0/0 R2(config-subif)#ip address 172.16.1.2 255.255.255.252 R2(config-subif)#ipv6 address 2001:db8:acad:1: :2 /64 R2(config-subif)#description Conexion R1 R2(config-subif)#clock rate128000 R2(config-subif)#no shutdown R2(config-subif)#exit

Interfaz S0/0/1	R2#config terminal R2(config)#interface S0/0/1 R2(config-subif)#ip address 172.16.2.2 255.255.255.252 R2(config-subif)#ipv6 address 2001:db8:acad:2: :2 /64 R2(config-subif)#description Conexion R3 R2(config-subif)#clock rate128000 R2(config-subif)#no shutdown R2(config-subif)#exit
Interfaz G0/0 (simulación de Internet)	R2#config terminal R2(config)#interface gigabitEthernet 0/0 R2(config-subif)#ip address 209.165.200.233 255.255.255.248 R2(config-subif)#ipv6 address 2001:db8:acad:A: :1 /64 R2(config-subif)#description Conexion Servidor R2(config-subif)#no shutdown R2(config-subif)#exit
Interfaz loopback 0 (servidor web simulado)	R2#configure terminal R2(config)#interface loopback 0 R2(config-if)#ip address 10.10.10.10 255.255.255.255 R2(config-if)#description conexion servidor web
Ruta predeterminada	R2#configure terminal R2(config)#ip route 0.0.0.0 0.0.0.0 172.16.1.1 R2(config)#ip route 0.0.0.0 0.0.0.0 172.16.2.1 R2#configure terminal R2(config)#ipv6 route ::/0 2001:DB8:ACAD:1::1 R2(config)#ipv6 route ::/0 2001:DB8:ACAD:2::1

Se realiza la configuracion basica del

Router 3

Figura 58. Configuración básica del Router 3



Fuente: Autor

Para la configuración del Router 3 se realiza las siguientes configuraciones como se muestra en la tabla 6. donde procedemos a desactivar la búsqueda DNS, generamos el nombre al router, se crea un dominio, se establecen las contraseñas cifrada para el modo privilegiado, se configura contraseña de acceso a consola, se configura contraseña de acceso Telnet, se cifran las contraseñas de texto no cifrado, se crea un mensaje MOTD, se configuran la Interfaz S0/0/1, Interfaz loopback 4, Interfaz loopback 5, Interfaz loopback 6, Interfaz loopback 7 y Ruta predeterminada como esta en la tabla de direccionamiento.

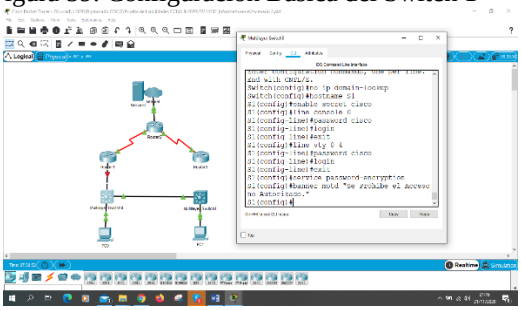
Tabla 41. Configuración Router 3

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

Contraseña de acceso a la consola	R3> enable R3# configure terminal R3(config)# line console 0 R3(config-line)# password cisco R3(config-line)# login R3(config-line)# exit R3(config)#
Contraseña de acceso Telnet	R3#configure terminal R3(config)#line vty 0 4 R3(config-line)#aa 1sspassword cisco R3(config-line)# login R3(config-line)#exit R3(config)#
Cifrar las contraseñas de texto no cifrado	R3(config)#service password-encryption R3(config)#exit
Mensaje MOTD	R3# configure terminal R3(config)# banner motd " Se prohíbe el acceso no autorizado." R3(config)# exit
Interfaz S0/0/1	R3#config terminal R3(config)#interface S0/0/1 R3(config-subif)#ip address 172.16.2.1 255.255.255.252 R3(config-subif)#ipv6 address 2001:db8:acad:2: :1 /64 R3(config-subif)#description Conexion R2 R3(config-subif)#no shutdown R3(config-subif)#exit
Interfaz loopback 4	R3#configure terminal R3(config)#interface loopback 4 R3(config-if)#ip address 192.168.4.1 255.255.255.0 R3(config-if)#description Loopback 4
Interfaz loopback 5	R3#configure terminal R3(config)#interface loopback 5 R3(config-if)#ip address 192.168.5.1 255.255.255.0 R3(config-if)#description Loopback 5
Interfaz loopback 6	R3#configure terminal R3(config)#interface loopback 6 R3(config-if)#ip address 192.168.6.1 255.255.255.0 R3(config-if)#description Loopback 6
Interfaz loopback 7	R3#configure terminal R3(config)#interface loopback 7 R3(config-if)#ipv6 address 2001:db8:acad:3::1/64 R3(config-if)#description Loopback 7
Rutas predeterminadas	R3#configure terminal R3(config)#ip route 0.0.0.0 0.0.0.0 172.16.2.2 R2#configure terminal R2(config)#ipv6 route ::/0 2001:DB8:ACAD:2::2

Configurado los tres Router se procedio a configurar los 2 switch.

Figura 59. Configuración Básica del Switch 1



Fuente: Autor

Para la configuración de los Switch 1 se realizará las siguientes configuraciones como se muestra en la tabla 7. donde procedemos a desactivar la búsqueda DNS, generamos el nombre al Switch, se establecen las contraseñas cifrada para el modo privilegiado, se configura contraseña de acceso a consola, se configura líneas VTY solo aceptando conexiones telnet, se Cifran las contraseñas de

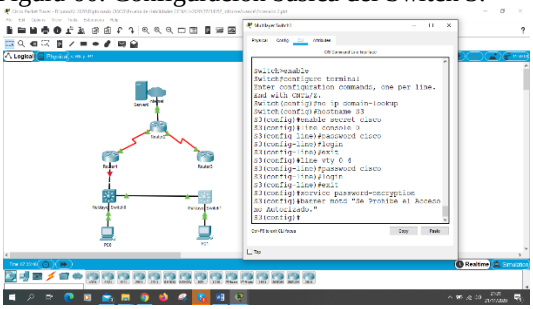
texto no cifrado, se Configura un mensaje MOTD Banner.

Tabla 42. Configuración Básica de Switch 1

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

Configuracion basica del switch 3

Figura 60. Configuración básica del Switch 3.



Fuente: Autor

Para la configuración de los switch 3 se realizará las siguientes configuraciones como se muestra en la tabla 8. donde procedemos a desactivar la búsqueda DNS, generamos el nombre al Switch, se establecen las contraseñas cifrada para el modo privilegiado, se configura contraseña de acceso a consola, se configura líneas VTY solo aceptando conexiones telnet, se Cifran las contraseñas de texto no cifrado, se Configura un mensaje MOTD Banner.

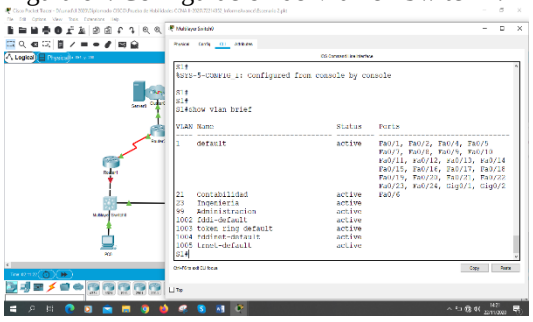
Tabla 43. Configuración de Switch 3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch>enable Switch#configure terminal Switch(config)#no ip domain-lookup Switch(config)#
Nombre del switch	switch>enable switch# configure terminal switch(config)#hostname S3 S3(config)#
Contraseña de exec privilegiado cifrada	S3> enable S3# configure terminal S3(config)# enable secret cisco S3(config)#

Contraseña de acceso a la consola	S3> enable S3# configure terminal S3(config)# line console 0 S3(config-line)# password cisco S3(config-line)# login S3(config-line)# exit S3(config)#
Contraseña de acceso Telnet	S3#configure terminal S3(config)#line vty 0 4 S3(config-line)#lpassword cisco S3(config-line)# login S3(config-line)#exit S3(config)#
Cifrar las contraseñas de texto no cifrado	S3(config)#service password-encryption S3(config)#exit
Mensaje MOTD	S3# configure terminal S3(config)# banner motd " Se prohíbe el acceso no autorizado." S3(config)# exit

Se configuran las vlan las troncales y el Puerto de acceso en el S1.

Figura 61. Configuración de Vlan en Switch 1.



Fuente: Autor

Para la configuración de la seguridad del switch 1, se crean las VLAN 21,23 y 99 y el routing entre VLAN de los switch 1 se realizará las siguientes configuraciones como se muestra en la tabla 8. donde procedemos a Asignar la dirección IP de administración, se asignar el gateway predeterminado, se Forza el enlace troncal en la interfaz F0/3 y F0/5, Configurar el resto de los puertos como puertos de acceso, se asigna F0/6 a la VLAN 21 y se apagan los puertos sin usar.

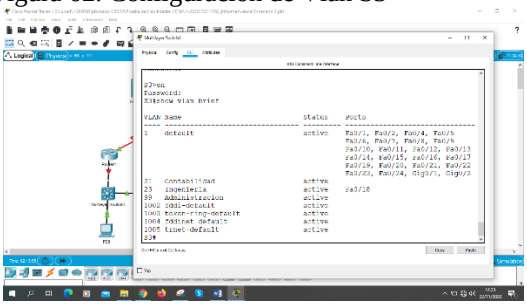
Tabla 44. Configuración de vlan Switch 1

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	S1(config)#vlan 21 S1(config-vlan)#name Contabilidad S1(config-vlan)#exit S1(config)#vlan 23 S1(config-vlan)#name Ingenieria S1(config-vlan)#exit S1(config)#vlan 99 S1(config-vlan)#name Administracion S1(config-vlan)#exit
Asignar la dirección IP de administración.	S1#configure terminal S1(config)#interface vlan 99 S1(config-vlan)#ip address 192.168.99.2 255.255.255.0
Asignar el gateway predeterminado	S1#configure terminal S1(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	S1#configure terminal S1(config)#interface f0/3 S1(config-if)# switchport mode trunk S1(config-if)#switchport trunk allowed vlan all S1(config-if)#switchport trunk native vlan 1
Forzar el enlace troncal en la interfaz F0/5	S1#configure terminal S1(config)#int f0/5 S1(config-if-range)# switchport trunk encapsulation dot1q S1(config-if-range)# switchport mode trunk S1(config-if-range)#switchport trunk allowed vlan all S1(config-if)#switchport trunk native vlan 1

Configurar el resto de los puertos como puertos de acceso	S1#configure terminal S1(config)#int range f0/1-2,f0/4,f0/6-24 S1(config-if-range)#switchport mode access S1(config-if-range)#no shutdown
Asignar F0/6 a la VLAN 21	S1#configure terminal S1(config)#int f0/6 S1(config-if) #switchport access vlan 21
Apagar todos los puertos sin usar	S1#configure terminal S1(config)#int range f0/1-2,f0/4,f0/7-24 S1(config-if-range)#shutdown

Se configuran las vlan las troncales y el Puerto de acceso en el S3.

Figura 62. Configuración de Vlan S3



Fuente: Autor

Para la configuración de la seguridad del switch 3, se crean las VLAN 21, 23 y 99 el routing entre VLAN de los switch 3 se realizará las siguientes configuraciones como se muestra en la tabla 9. donde procedemos a Asignar la dirección IP de administración, se asigna el gateway predeterminado, se Forza el enlace troncal en la interfaz F0/3, Configurar el resto de los puertos como puertos de acceso, se asigna F0/18 a la VLAN 23 y se apagan los puertos sin usar.

Tabla 45. Configuración Vlan en Switch 3

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	S3(config)#vlan 21 S3(confi-vlan)#name Contabilidad S3(config-vlan)#exit S3(config)#vlan 23 S3(config-vlan)#name Ingenieria S3(config-vlan)#exit S3(config)#vlan 99 S3(config-vlan)#name Administracion S3(config-vlan)#exit
Asignar la dirección IP de administración	S3#configure terminal S3(config)#interface vlan 99 S3(config-vlan)#ip address 192.168.99.3 255.255.255.0
Asignar el gateway predeterminado.	S3#configure terminal S3(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	S3#configure terminal S3(config)#int f0/3 S3(config-if-range)# switchport mode trunk S3(config-if-range)#switchport trunk allowed vlan all S3(config-if)#switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	S3#configure terminal S3(config)#int range f0/1-2,f0/4-24 S3(config-if-range)#switchport mode access
Asignar F0/18 a la VLAN 23	S3#configure terminal S3(config)#int f0/18 S3(config-if) #switchport access vlan 23
Apagar todos los puertos sin usar	S3#configure terminal S3(config)#int range f0/1-2,f0/4-17,f0/19-24,g0/1-2 S3(config-if-range)#shutdown

Ahora se precede a configurar las subinterface en R1

Se crean las sub interfaz G0/1.21, G0/1.23, G0/1.99 con encapsulación 802.1q y se activa la interfaz G0/1 como se muestra en la tabla 10.

Tabla 46. Configuracion de subinterfaces en Router 1

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	R1#config terminal R1(config)#interface gigabitEthernet 0/1.21 R1(config-subif)#encapsulation dot1Q 21 R1(config-subif)#ip address 192.168.21.1 255.255.255.0 R1(confiig-subif)#description vlan 21 R1(config-subif)#no shutdown R1(config-subif)#exit
Configurar la subinterfaz 802.1Q .23 en G0/1	R1#config terminal R1(config)#interface gigabitEthernet 0/1.23 R1(config-subif)#encapsulation dot1Q 23 R1(config-subif)#ip address 192.168.23.1 255.255.255.0 R1(confiig-subif)#description vlan 23 R1(config-subif)#no shutdown R1(config-subif)#exit
Configurar la subinterfaz 802.1Q .99 en G0/1	R1#config terminal R1(config)#interface gigabitEthernet 0/1.99 R1(config-subif)#encapsulation dot1Q 99 R1(config-subif)#ip address 192.168.99.1 255.255.255.0 R1(confiig-subif)#description vlan 99 R1(config-subif)#no shutdown R1(config-subif)#exit
Activar la interfaz G0/1	R1#config terminal R1(config)#interface gigabitEthernet 0/1 R1(config-if)#no shutdown

Programamos el Routing dinámico OSPF en los Router 1

En el Router 1 se configura el OSPF con área 0 como se muestra en la tabla 11. Se anuncian las redes conectadas directamente con su wilcard y se establece las subinterfaces como pasivas

Tabla 47. Se configura OSPF en Router 1

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R1#Configure terminal R1(config)#router ospf 1 R1(config-router)#router-id 1.1.1.1
Anunciar las redes conectadas directamente	R1(config-router)#network 172.16.1.0 0.0.0.3 area 0 R1(config-router)#network 192.168.21.0 0.0.0.255 area 0 R1(config-router)#network 192.168.23.0 0.0.0.255 area 0 R1(config-router)#network 192.168.99.0 0.0.0.255 area 0

Establecer todas las interfaces LAN como pasivas	R1(config-router)#passive-interface g0/1.21 R1(config-router)#passive-interface g0/1.23 R1(config-router)#passive-interface g0/1.99
Desactive la sumarización automática	**No aplica**

Programamos el Routing dinámico OSPF en los Router 2

En el Router 2 se configura el OSPF con área 0 como se muestra en la tabla 12. Se anuncian las redes conectadas directamente con su wilcard y se establece la interfaz LAN looopback0 como pasivas

Tabla 48. Configuracion OSPF en Router 2

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R2#Configure terminal R2(config)#router ospf 1 R2(config-router)#router-id 2.2.2.2
Anunciar las redes conectadas directamente	R2(config-router)#network 10.10.10.10 0.0.0.0 area 0 R2(config-router)#network 172.16.1.0 0.0.0.3 area 0 R2(config-router)#network 172.16.2.0 0.0.0.3 area 0
Establecer la interfaz LAN (loopback) como pasiva	R2(config-router)#passive-interface lo0
Desactive la sumarización automática.	No aplica

Programamos el Routing dinámico OSPF en los Router 3

En el Router 3 se configura el OSPF con área 0 como se muestra en la tabla 27. Se anuncian las redes conectadas directamente y se establece la interfaz LAN looopback0 como pasivas

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R3#Configure terminal R3(config)#router ospf 1 R3(config-router)#router-id 3.3.3.3
Anunciar redes IPv4 conectadas directamente	R3(config-router)#network 172.16.2.0 0.0.0.3 area 0 R3(config-router)#network 192.168.4.0 0.0.0.255 area 0 R3(config-router)#network 192.168.5.0 0.0.0.255 area 0 R3(config-router)#network 192.168.6.0 0.0.0.255 area 0
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	R3(config-router)#passive-interface lo4 R3(config-router)#passive-interface lo5 R3(config-router)#passive-interface lo6
Desactive la sumarización automática.	No aplica

Ahora se configura el R1 como servidor DHCP para las vlan 21 y 23. Reservando las 20 primeras IP

Se configura en R1 como servidor DHCP para Las Vlans 21 y 23 reservando las primeras 20

direcciones de cada red, como se muestra en la tabla 13.

Tabla 49.Configuración DHCP en Router para Vlan 21 y 23

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21	R1#configure terminal R1(config)# ip dhcp excluded-address 192.168.21.1 192.168.21.20
Reservar las primeras 20 direcciones IP en la VLAN 23	R1#configure terminal R1(config)# ip dhcp excluded-address 192.168.23.1 192.168.23.20
Crear un pool de DHCP para la VLAN 21.	R1#configure terminal R1(config)#ip dhcp pool ACCT R1(dhcp-config)#network 192.168.21.0 255.255.255.0 R1(dhcp-config)#default-router 192.168.21.1 R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com
Crear un pool de DHCP para la VLAN 23	R1#configure terminal R1(config)#ip dhcp pool ENGNR R1(dhcp-config)#network 192.168.23.0 255.255.255.0 R1(dhcp-config)#default-router 192.168.23.1 R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com

Se configura el NAT estático y dinámico en el R2

Se configura en el Router 2 la NAT estática y dinámica como se muestra en la tabla 14. Primero se crea una base de datos local con una cuenta de usuario, se configura un servidor HTTP utilizando la base de datos local para la autenticación, se crea una NAT estática al servidor web, se asigna la interfaz interna y externa para la NAT estática, se configura la NAT dinámica dentro de una ACL privada, se define el pool de direcciones IP públicas utilizables y se define la traducción de NAT dinámica.

Tabla 50. Configuración NAT Estático y Dinámico en Router 2

Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	R2#config t R2(config)#user webuser privilege 15 secret cisco12345
Habilitar el servicio del servidor HTTP	R2#config t R2(config)#ip http server
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	R2#config t R2(config)#ip http authentication local
Crear una NAT estática al servidor web.	R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229
Asignar la interfaz interna y externa para la NAT estática	R2#config t R2(config)#interface g0/0 R2(config-if)#ip nat outside R2(config-if)#exit R2(config)# R2(config)#interface Lo0 R2(config-if)#ip nat inside R2(config-if)#exit
Defina el pool de direcciones IP públicas utilizables.	R2#config t R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248
Definir la traducción de NAT dinámica	R2#config t R2(config)#ip nat inside source list 1 pool INTERNET

Configurar la NAT dinámica dentro de una ACL privada	R2#config t 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 192.168.4.1 0.0.0.255 R2(config)#access-list 1 permit 192.168.5.1 0.0.0.255 R2(config)#access-list 1 permit 192.168.6.1 0.0.0.255

Se configura el servidor NTP en el R2 y que el R1 se sincronice con R2

Se configura Servidor NTP en router 2 como master 5 y el router 1 se configura para que se sincronice con R2 como se muestra en la tabla 15.

Tabla 51. Configuración servidor NTP

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

Se configura lista de control de acceso a las (ACL)

Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2, se aplica la ACL con nombre a las líneas VTY, se permite acceso por Telnet a las líneas de VTY. Como se muestra en la tabla 34.

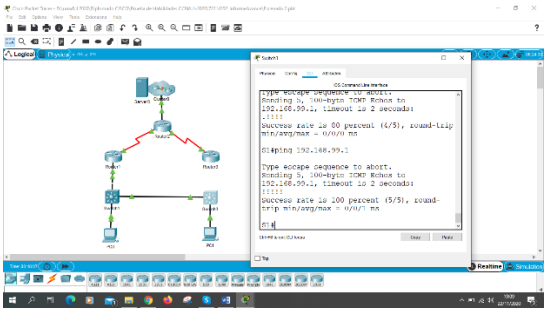
Tabla 52. Configuración lista de acceso ACL

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

III. RESULTADOS

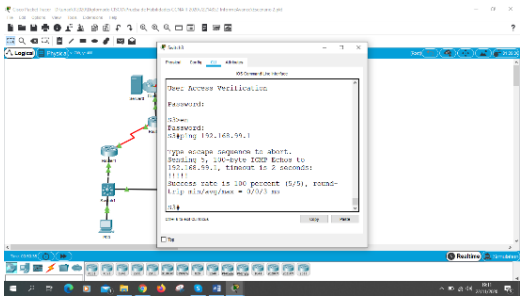
Luego de haber Configurado todos los equipos de la red del escenario 2 con la seguridad y la interconexión solicitadas se precedió a revisar y a realizar pruebas de conectividad. Con el comando ping

Figura 63. Prueba de Conexión entre S1 y R1 Vlan 99



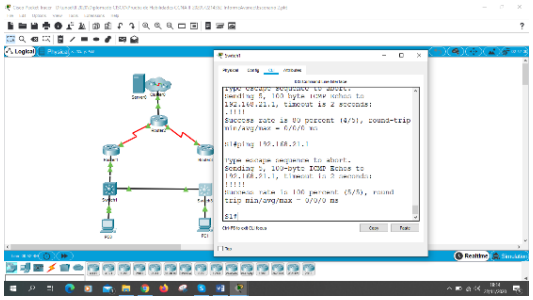
Fuente: Autor

Figura 64. Prueba de conectividad entre S3 y R1 Vlan 99



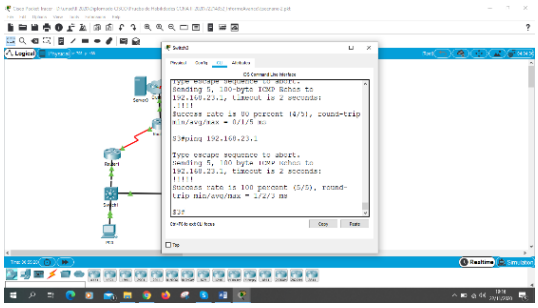
Fuente:Autor

Figura 65. Prueba de Conectividad entre S1 y R1 Vlan 21



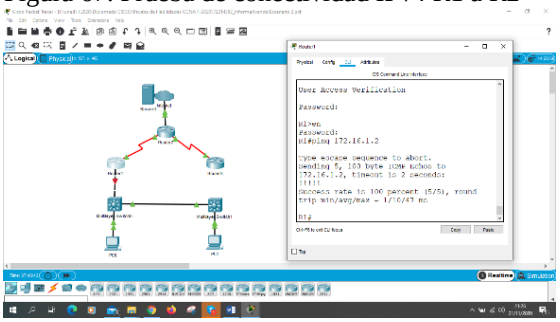
Fuente: Autor

Figura 66, Prueba de conectividad entre S3 y R1 Vlan 23



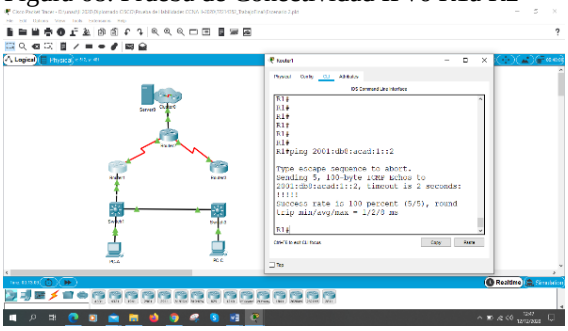
Fuente: Autor

Figura 67. Prueba de conectividad IPv4 R1 a R2



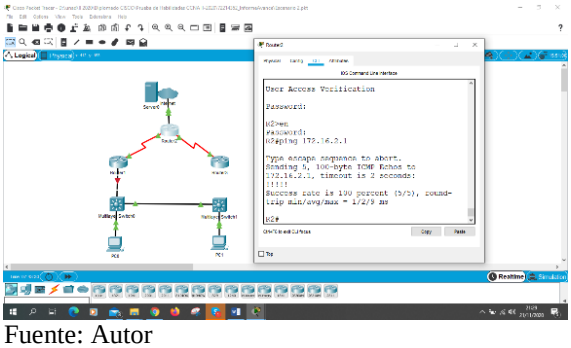
Fuente: Autor

Figura 68. Prueba de Conectividad IPv6 R1a R2



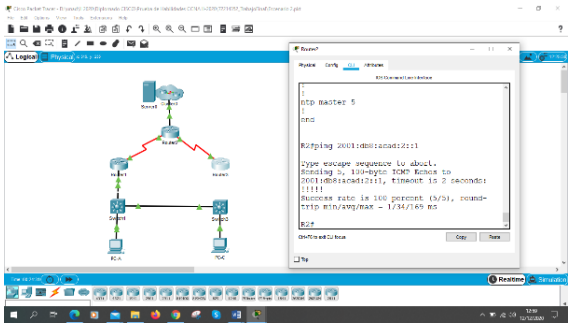
Fuente: Autor

Figura 69. Prueba de Conectividad IPv4 entre R2 a R3



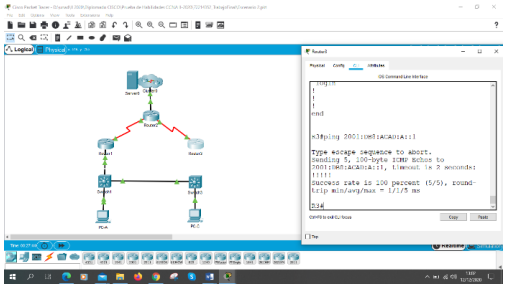
Fuente: Autor

Figura 70. Prueba de conectividad IPv6 entre R2 a R3



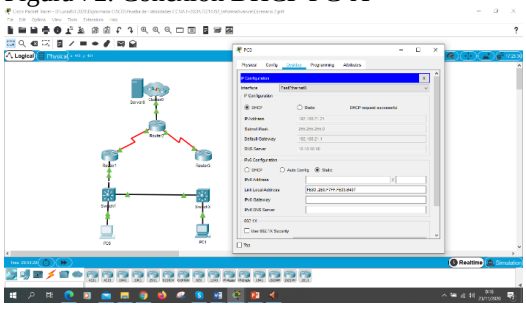
Fuente: Autor

Figura 71. Prueba de conectividad IPv6 entre R3 y R2 G0/0



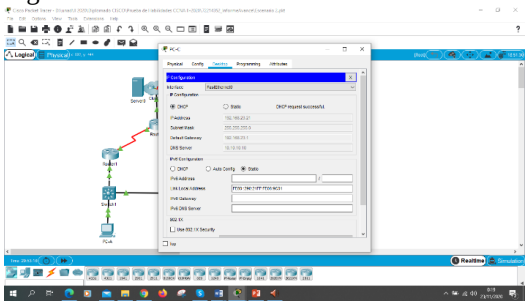
Fuente:Autor

Figura 72. Conexión DHCP PC-A



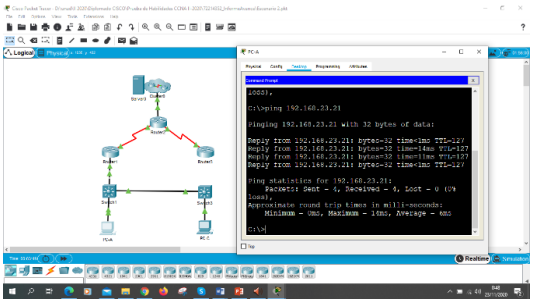
Fuente: Autor

Figura 73.Conexión DHCP PC-C



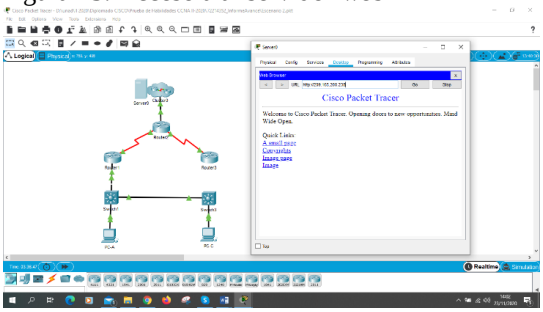
Fuente: Autor

Figura 74. Prueba de conectividad entre PC-A y PC-C



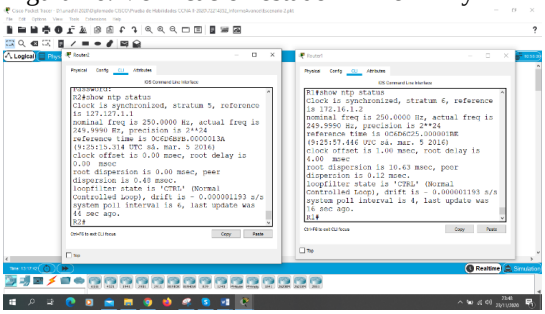
Fuente: Autor

Figura 75. Acceso a al servidor web



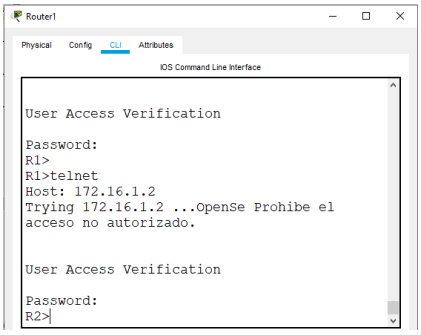
Fuente: Autor

Figura 76. Verificación estado NTP en R1 y R2



Fuente: Autor

Figura 77. Conexión Telnet desde R1 a R2



Fuente: Autor

IV. CONCLUSIONES

Al realizar este artículo científico se pudo poner en practica todos los conocimientos adquiridos durante el Diplomado de Profundización CCNA 1 y CCNA 2, Tales Como, la administración y seguridad de una red.

- En las configuraciones básicas del Router y Switch es importante que al crear las contraseñas de console 0 y líneas vty estas sean encriptadas para que no sean visibles en la configuración general del sistema.
- La configuración de las vlan en una red mejora la seguridad al realizar segmentación de red, reduce costos la propagación de tráfico, lo cual mejora el rendimiento y disponibilidad de todos los servicios que repercuten en seguridad y routing para el buen funcionamiento
- Se configura servidor DHCP para la simplificación de la red, al suministrar direcciones IP automáticamente a cada host conectado a la red.
- Se pudo comprobar el funcionamiento del protocolo OSPF de enrutamiento dinámico sin clase el cual fue desarrollado para remplazar al protocolo de enlace RIP. El OSPF V2 es para IPv4 y el OSPF V3 es para IPv6. Las características del OSPF vista son la Convergencia Rápida, Escalable, Eficaz y Seguro
- Se configura lista de control de acceso ACL para controlar el tráfico desde y hacia la red.

Esto escenarios son muy importantes para nuestra vida profesional, ya que nos enseña a analizar y configurar una red para que sea más segura y robusta.

V. REFERENCIA

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

[2] CISCO. (2019). Protocolos y comunicaciones de red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#3

[3]CISCO. (2019). Direccionamiento IP. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#7

[4] CISCO. (2019). Capa de red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#6

[5] CISCO. (2019). Acceso a la red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#4

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

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

[8] CISCO. (2019). Routing Dinámico. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#3

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

[10] CISCO. (2019). DHCP. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#8

[11] CISCO. (2019). Listas de Control de Acceso. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#7

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