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

GIOVANNY ADRIAN OROZCO CAVIEDES

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA. UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA. ECBTI
DIPLOMADO DE PROFUNDIZACIÓN CISCO
INGENIERIA DE SISTEMAS
BARRANQUILLA – ATLANTICO
2020

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

GIOVANNY ADRIAN OROZCO CAVIEDES

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

DIRECTOR:

DIEGO EDINSON RAMIREZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA. UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA. ECBTI
DIPLOMADO DE PROFUNDIZACIÓN CISCO
INGENIERIA DE SISTEMAS
BARRANQUILLA – ATLANTICO
2020

NOTA DE ACEPTACION

_____

_____

_____

_____

_____

Firma del Presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

BARRANQUILLA, ATLANTICO, 30 Noviembre de 2020

AGRADECIMIENTOS

Expreso mi profundo agradecimiento primeramente a Dios por darme la sabiduría para asumir los retos en toda mi carrera, igualmente a mi familia por su amor y paciencia, seguidamente a todos los tutores y directivos de la UNAD, que estuvieron a la altura de sus resposabilidades para conmigo y asumieron siempre una actitud de ayuda y respeto.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

Router: enrutador,(del inglés router) o encaminador,es un dispositivo que permite interconectar computadoras que funcionan en el marco de una red. Su función: se encarga de establecer la ruta que destinará a cada paquete de datos dentro de una red informática.

Switch: Un switch o conmutador es un dispositivo de interconexión utilizado para conectar equipos en red formando lo que se conoce como una red de área local (LAN) y cuyas especificaciones técnicas siguen el estándar conocido como Ethernet

VLAN: Una VLAN, acrónimo de virtual LAN (red de área local virtual), es un método para crear redes lógicas independientes dentro de una misma red física. Varias VLAN pueden coexistir en un único conmutador físico o en una única red física.

NVRAM: El Cisco IOS usa la NVRAM como almacenamiento permanente para el archivo de configuración de inicio (startup-config). Al igual que la ROM, la NVRAM no pierde el contenido cuando se apaga el dispositivo.

TCP/IP: es usado para comunicaciones en redes y, como todo protocolo, describe un conjunto de guías generales de operación para permitir que un equipo pueda comunicarse en una red. TCP/IP provee conectividad de extremo a extremo especificando cómo los datos deberían ser formateados, direccionados, transmitidos, enrutados y recibidos por el destinatario.

Interfaz: Una interfaz de red es el software específico de red que se comunica con el controlador de dispositivo específico de red y la capa IP a fin de proporcionar a la capa IP una interfaz coherente con todos los adaptadores de red que puedan estar presentes.

MAC: En las redes de computadoras, la dirección MAC es un identificador de 48 bits que corresponde de forma única a una tarjeta o dispositivo de red. Se la conoce también como dirección física, y es única para cada dispositivo.

DHCP: El protocolo de configuración dinámica de host es un protocolo de red de tipo cliente/servidor mediante el cual un servidor DHCP asigna dinámicamente una dirección IP y otros parámetros de configuración de red a cada dispositivo en una red para que puedan comunicarse con otras redes IP.

DNS: Un servidor de nombres es un servidor de hardware o software que implementa un servicio de red para proveer respuestas a las consultas en un servicio de directorio.

RESUMEN

Entender la importancia de las telecomunicaciones en el desarrollo de las nuevas tecnologías e implementación de redes LAN/WAN utilizando la plataforma CISCO Networking Academy, tenido en cuenta que este diplomado es una alternativa de grado para el programa de Ingeniería de Sistemas. El presente documento resume lo aprendido durante toda la formación del diplomado en 2 escenarios, donde se explora todo lo refente al direccionamiento IPv4 e IPv6, las configuraciones básicas y avanzadas de router y switch, para la administración de forma segura de los mismos, se trabaja igualmente el enrutamiento entre VLAN, DCHP, Etherchannel y port-security. En el segundo escenario se trabajo lo concerniente al protocolo OSPF, redes estáticas y dinámicas (NAT), listas de control de acceso (ACL). Finalmente con las pruebas respectivas y contruyendo las topologías en los simuladores como packe tracer, se consolidara lo aprendido.

Palabras Claves: Enrutamiento, Direccionamiento, Router, Switch, VLAN, OSPF, ACL

ABSTRACT

Understand the importance of telecommunications in the development of new technologies and implementation of LAN / WAN networks using the CISCO Networking Academy platform, taking into account that this diploma is an alternative degree for the Systems Engineering program. This document summarizes what was learned during the entire training of the diploma in 2 scenarios, where everything related to IPv4 and IPv6 addressing is explored, the basic and advanced router and switch configurations, for the secure administration of the same, it works likewise the routing between VLAN, DCHP, Etherchannel and port-security. In the second

scenario, work was done on the OSPF protocol, static and dynamic networks (NAT), access control lists (ACL). Finally, with the respective tests and building the topologies in the simulators as packe tracer, what has been learned will be consolidated.

Keywords: Routing, Addressing, Router, Switch, VLAN, OSPF, ACL

INTRODUCCION

Dentro de las alternativas de grado que ofrece la Universidad Abierta y a Distancia (UNAD), se encuentra la realización de un diplomado que profundice sobre algun temática especifica de la carrera cursada. En esta caso se oferto el Diplomado de Profundizacfion Cisco (Diseño e implementación de soluciones integradas LAN/WAN).

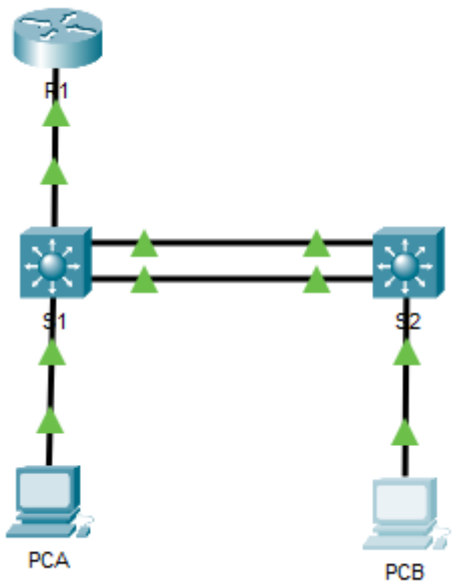
El Diplomado pretende desrrollar en el estudiante la capacidad de configurar dispositivos networking orientados al diseño de redes escalables y de conmutación, utilizando el modelo jerarquico de 3 niveles, esto permite optimizar el rendimiento de la red, igualmente se articulan políticas básicas de seguridad de la información.

En el presente trabajo maneja 2 escenarios, el primer escenario tiene como propósito la configuración de 1 router y 2 switch, estos deben admitir la conectividad IPv4 e IPv6, deben administrase de manera segura y Configurar el enrutamiento entre VLAN, DHCP, Etherchannel y port-security. El segundo escenario igual que el anterior tambien se debe admitir conectividad IPv4 e IPv6, seguridad de los elementos, routing entre vlan, los protocolos OSPF, DCHP, la traducción de direcciones de red dinámica y estatica (NAT), listas de control de acceso y protocolo NTP.

DESARROLLO

ESCENARIO 1

Figura 1. Escenario 1



Fuente: Autor

En este primer escenario mostrado en la **figura 1**, se configurarán los dispositivos de una red pequeña. Debe configurar un router, un switch y equipos que admitan tanto la conectividad IPv4 como IPv6 para los hosts soportados. El router y el switch también deben administrarse de forma segura. Configurará el enrutamiento entre VLAN, DHCP, Etherchannel y port-security.

Tabla 1.1 Tabla de las VLAN.

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

Tabla 1.2 Tabla de asignación de direcciones

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
R1 G0/0/1.2	10.19.8.1 /26	No corresponde
R1 G0/0/1.2	2001:db8:acad:a: :1 /64	No corresponde
R1 G0/0/1.3	10.19.8.65 /27	No corresponde
R1 G0/0/1.3	2001:db8:acad:b: :1 /64	No corresponde
R1 G0/0/1.4	10.19.8.97 /29	No corresponde
R1 G0/0/1.4	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
R1 Loopback0	2001:db8:acad:209: :1 /64	No corresponde
S1 VLAN 4	10.19.8.98 /29	10.19.8.97
VLAN S1 4	2001:db8:acad:c: :98 /64	No corresponde
S1 VLAN 4	fe80: :98	No corresponde
S2 VLAN 4	10.19.8.99 /29	10.19.8.97
S2 VLAN 4	2001:db8:acad:c: :99 /64	No corresponde
S2 VLAN 4	fe80: :99	No corresponde
PC-A NIC	Dirección DHCP para IPv4	DHCP para puerta de enlace predeterminada IPv4
PC-A NIC	2001:db8:acad:a: :50 /64	fe80::1
PC-B NIC	DHCP para dirección IPv4	DHCP para puerta de enlace predeterminada IPv4
PC-B NIC	2001:db8:acad:b: :50 /64	fe80::1

La **Tabla 1.2** nos muestra el direccionamiento a implementar en los diferentes dispositivos de red

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

1.1 Inicializar y volver a cargar los routers y los switches: en esta parte como se visualizara en la **Tabla 1** con los comandos respectivos eliminara las configuraciones de inicio de los router y de los switch, después volver a cargar los dispositivos

1.1.1 Eliminamos el archivo de configuración de inicio del router: a continuación como se estableció se eliminaran los archivos startup-config del Router 1, junto con las VLAN y la carga de los dispositvos

En esta **Tabla 1.4** se encuentran los comandos para eliminar los archivos de configuración del router y las diferentes VLAN y volver a cargar el dispositivo

Tabla 1.4 Proceso de eliminación de de archivos en el Router

Tarea	**Especificación**
Se accesa al modo privilegiado	Router>enable
Eliminacion de los archivos de configuración	Router#erase startup-config
Eliminar las VLANs que estén creadas	Router#delete vlan.dat
Volver a cargar el router	Router#reload

1.1.2 Eliminamos el archivo de configuración de inicio de los switch: a continuación como se estableció en la **Tabla 1.5** se eliminaran los archivos startup-config de los switchs, junto con las VLAN y la carga de los dispositvos, igual que configurar la plantilla SDM para que admita IPv6.

Tabla 1.5 Proceso de eliminación de de archivos en el Switch

Tarea	**Especificación**
Se accesa al modo privilegiado	Switch>enable
Eliminacion de los archivos de configuración	Switch#erase startup-config
Eliminar las VLANs que estén creadas	Switch#delete vlan.dat
Volver a cargar el switch	Switch#reload

En esta tabla se encuentran los comandos para eliminar los archivos de configuración del switch y las diferentes VLAN y volver a cargar el dispositivo

1.2 Configurar R1: se procede a la configuración del Router según las indicaciones en la **Tabla 1**

Tabla 2.Configuracion Incial del Router 1

Tarea	**Especificación**
Desactivar la búsqueda DNS	Router#config terminal Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R1 R1(config)#
Nombre de dominio	R1(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	R1(config)#enable secret ciscoenpass

Contraseña de acceso a la consola	R1(config)#line console 0 R1(config-line)#password ciscoconpass R1(config-line)#login
Establecer la longitud mínima para las contraseñas	R1(config)#security password min-length 10
Crear un usuario administrativo en la base de datos local	R1(config)#username admin password admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	R1(config)#line vty 0 15 R1(config-line)#login local
Configurar VTY solo aceptando SSH	R1(config-line)#transport input ssh
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Configure un MOTD Banner	R1(config)#banner motd %No se permite el acceso a personal no autorizado%
Habilitar el routing IPv6	R1(config)#ipv6 unicast-routing
Configurar interfaz G0/0/1 y subinterfaces	R1#config terminal R1(config)#int g0/0/1 R1(config-if)#no shutdown R1(config)#int g0/0/1.2 R1(config-subif)# R1(config-subif)#encapsulation dot1q 2 R1(config-subif)#description vlan2 R1(config-subif)#ip address 10.19.8.1 255.255.255.192 R1(config-subif)#ipv6 address 2001:DB8:ACAD:A::1/64 R1(config-subif)#ipv6 address FE80::1 link-local R1(config-subif)#no shutdown R1(config-subif)# 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)#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)#int g0/0/1.6 R1(config-subif)# R1(config-subif)#encapsulation dot1q 6 R1(config-subif)#description vlan6 R1(config-subif)#no shutdown R1(config)#interface gigabitEthernet 0/0/1 R1(config-if)#no shutdown
Configure el Loopback0 interface	R1(config)#int loopback 0 R1(config-if)# R1(config-if)#ip route 0.0.0.0 0.0.0.0 loopback0 R1(config)#ipv6 route 0:0:0:0:0:0:0:0/0 loopback 0 R1(config)#ipv6 route 0:0:0:0:0:0:0:0/0 loopback0 R1(config)#int loopback 0 R1(config-if)#ipv6 add fe80::1 link-local
Generar una clave de cifrado RSA	R1(config)#crypto key generate rsa The name for the keys will be: R1.ccna-lab.com Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes. How many bits in the modulus [512]: 1024

En la anterior **Tabla 3** se puede visualizar los comandos que se utilizaron para ejecutar varios procesos de configuración en R1, como la desactivación de la búsqueda DNS, la asignación del nombre del router, el respectivo nombre de dominio, la protección con las contraseña cifradas para el modo EXEC privilegiada y de acceso a la consola, establecer la longitud mínima para estas contraseñas,

además de crear un usuario administrativo en la base de datos local, configurar el inicio de sesión en las líneas VTY para que use la base de datos local y solo aceptando SSH, para después habilitar el routing IPv6 y configurar la interfaz G0/0/1 con sus subinterfaces y para terminar la configuración de el Loopback0 interface y la generación de una clave de cifrado RSA.

1.3 Configure S1 y S2.

En la siguiente **Tabla 4** se muestran los comandos que se implementaron para el proceso de la configuración de Switch 1 y Switch 2, lo primero se desactivaron las búsquedas DNS, se asignaron los nuevos nombres de los switches y dominios, como en la anterior paso con R1 las contraseñas para el modo EXEC privilegiado y acceso a la consola, se crearon usuarios administrativos en la base de datos local, lo mismo que la configuraracion el inicio de sesiónes en las líneas VTY para que usen la base de datos local y para que acepten únicamente las conexiones SSH, se cifraron las contraseñas de texto no cifrado, además de un MOTD Banner, las claves de cifrado RSA, la interfaz de administración (SVI) y por ultimo los gateway predeterminados

Tabla 3. Tabla de configuracion de Switch 1 y Switch 2

Tarea	**Especificación**
	Switch 1
Desactivar la búsqueda DNS.	Switch#config terminal Switch(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S1 S1(config)#
Nombre de dominio	S1(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	S1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	S1(config)#line console 0 S1(config-line)#password ciscoconpass S1(config-line)#login
Crear un usuario administrativo en la base de datos local	S1(config-line)#username admin password admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	S1(config)#line vty 0 15 S1(config-line)#login local
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S1(config-line)#transport input ssh

Cifrar las contraseñas de texto no cifrado	S1(config-line)#service password-encryption
Configurar un MOTD Banner	S1(config)#banner motd %No se permite acceso a personal no autorizado%
Generar una clave de cifrado RSA	S1(config)#crypto key generate rsa The name for the keys will be: S1.ccna-lab.com Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes. How many bits in the modulus [512]: 1024 % Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
Configurar la interfaz de administración (SVI)	S1#config terminal S1(config)#int vlan 4 S1(config-if)#ip add 10.19.8.98 255.255.255.248 S1(config-if)#ipv6 add 2001:DB8:ACAD:C::98/64 S1(config-if)#ipv6 add FE80::98 link-local
Configuración del gateway predeterminado	S1(config)#ip default-gateway 10.19.8.97
	Switch 2
Desactivar la búsqueda DNS.	S2(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S2
Nombre de dominio	S2(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	S2(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	S2(config)#line console 0 S2(config-line)#password ciscoconpass S2(config-line)#login
Crear un usuario administrativo en la base de datos local	S2(config-line)#username admin password admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	S2(config)#line vty 0 15 S2(config-line)#login local
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S2(config-line)#transport input ssh
Cifrar las contraseñas de texto no cifrado	S2(config-line)#service password-encryption

Configurar un MOTD Banner	S2(config)#banner motd %No se permite acceso a personal no autorizado%
Generar una clave de cifrado RSA	S2(config)#crypto key generate rsa The name for the keys will be: S2.ccna-lab.com Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes. How many bits in the modulus [512]: 1024
Configurar la interfaz de administración (SVI)	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	S2(config-if)#ip default-gateway 10.19.8.97

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

2.1 Configurar S1: se realiza la configuracion del Switch según las indicaciones de los comandos en la **Tabla 5,** donde se crean las VLAN, junto con los troncos 802.1Q que utilizan la VLAN 6 nativa, además se crean un grupo de puertos EtherChannel de Capa 2 que usan las interfaces F0/1 y F0/2, después se configura el puerto de acceso de host para VLAN 2, lo mismo que la seguridad del puerto en los puertos de acceso y por ultimo la poteccion de todas las interfaces no utilizadas

Tabla 4. Configuracion de S1 VLAN, Trunking, EtherChannel

Tarea	**Especificación**
Crear VLAN	S1(config)#vlan 2 S1(config-vlan)#name bikes S1(config-vlan)#vlan 3 S1(config-vlan)#name trikes S1(config-vlan)#vlan 4 S1(config-vlan)#name management

	S1(config-vlan)#vlan 5 S1(config-vlan)#name parking S1(config-vlan)#vlan 6 S1(config-vlan)#name native
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	S1(config)#int r f0/1,f0/2,f0/5 S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 6 S1(config-if-range)#switchport mode trunk
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	S1(config)#int r f0/1,f0/2 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(config)#int f0/6 S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 2 S1(config-if)#no shutdown
Configurar la seguridad del puerto en los puertos de acceso	S1(config-if)#switchport port-security maximum 3
Proteja todas las interfaces no utilizadas	S1(config)#int r f0/3-4,f0/7-24, g0/1-2 S1(config-if-range)#switchport access vlan 5 S1(config-if-range)#description APAGADAS S1(config-if-range)#shutdown

2.2 Configurar S2: se realiza la configuracion del Switch según las indicaciones de los comandos en la **Tabla 6**, donde se crean las VLAN, junto con los troncos 802.1Q que utilizan la VLAN 6 nativa, además se crean un grupo de puertos EtherChannel de Capa 2 que usan las interfaces F0/1 y F0/2, después se configura el puerto de acceso de host para VLAN 2, lo mismo que la seguridad del puerto en los puertos de acceso y por ultimo la poteccion de todas las interfaces no utilizadas

Tabla 5. Configuracion de S2 VLAN, Trunking, EtherChannel

Tarea	**Especificación**
Crear VLAN	S2#config terminal S2(config)#vlan 2 S2(config-vlan)# S2(config-vlan)#name bikes S2(config-vlan)#vlan 3 S2(config-vlan)#name trikes S2(config-vlan)#vlan 4 S2(config-vlan)# S2(config-vlan)#name management S2(config-vlan)#vlan 5

	S2(config-vlan)#name parking S2(config-vlan)#vlan 6 S2(config-vlan)#name native
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	S2(config)#int r f0/1,f0/2,f0/5 S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 6 S2(config-if-range)#switchport mode trunk
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	S2(config)#int r f0/1,f0/2 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(config)#int f0/18 S2(config-if)#switchport mode access S2(config-if)#switchport access vlan 3 S2(config-if)#no shutdown
Configure port-security en los access ports	S2(config-if)#switchport port-security maximum 3
Asegure todas las interfaces no utilizadas.	S2#config terminal S2(config)#int r f0/3-17,f0/19-24, g0/1-2 S2(config-if-range)#switchport access vlan 5 S2(config-if-range)#description APAGADAS S2(config-if-range)#shutdown

Parte 3: Configurar soporte de host

3.1 Configuracion de R1: Determinar rutas predeterminadas para IPv4 e IPv6, crear grupoas DHCP para VLAN 2 y VLAN 3.

Los procesos solicitados se evidencian con los comandos que se trabajaron en la **Tabla 7**, donde se configura la ruta predeterminada, lo mismo que la configuracion IPv4 DHCP para VLAN 2 y VLAN 3

Tabla 6. Configuracion de R1, rutas IPv4, IPv6, DCHP para VLAN2 y 3

Tarea	**Especificación**
Configure Default Routing	R1(config)#ip route 0.0.0.0 0.0.0.0 loopback 0 *Mar 1 1:53:6.199: %SSH-5-ENABLED: SSH 1.99 has been enabled

	%Default route without gateway, if not a point-to-point interface, may impact performance R1(config)#ipv6 route 0:0:0:0:0:0:0:0/0 loopback 0
Configurar IPv4 DHCP para VLAN 2	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(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 10.19.8.1 10.19.8.85

3.2 Configurar los servidores

Se configuran los equipos host PC-A como aparece en la **Tabla 8** y PC-B visualizados en la **Tabla 9** para que utilicen DHCP para IPv4 y se asigna estáticamente las direcciones IPv6 GUA y Link Local. Después de configurar cada servidor, se registra las configuraciones de red del host con el comando ipconfig /all.

Tabla 7. Configuracion de PC-A

PC-A Network Configuration	
Descripción	PC-A
Dirección física	0030.A396.9CC3
Dirección IP	10.19.8.53
Máscara de subred	255.255.255.192
Gateway predeterminado	10.19.8.1
Gateway predeterminado IPv6	2001:DB8:ACAD:A::1

Tabla 8. Configuracion de PC-B

PC-B Network Configuration	
Descripción	PC-B
Dirección física	00D0.BCE8.90ED
Dirección IP	10.19.8.85
Máscara de subred	255.255.255.224
Gateway predeterminado	10.19.8.65
Gateway predeterminado IPv6	2001:DB8:ACAD:B::1

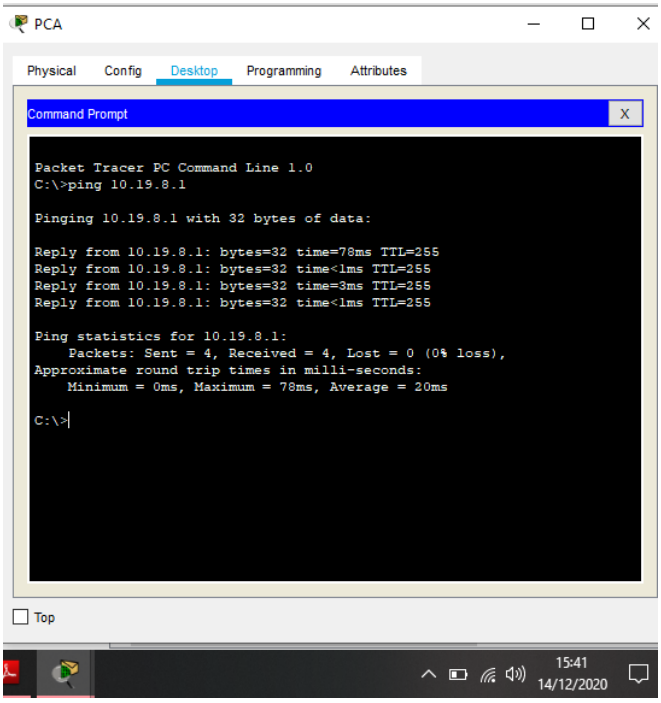
Parte 4: Probar y verificar la conectividad de extremo a extremo: se usa el comando ping para probar la conectividad IPv4 e IPv6 entre todos los dispositivos de red. En la la **Tabla 10** se realiza una descripción detallada de donde se debe generar el ping, porque interfaz y hacia donde se genera con su respectiva dirección, mostrando al final los respectivos resultados

Tabla 9. Resultados de las pruebas de conectividad de los dispositivos

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

A continuacion podrá visualizar en las figuras las pruebas de ping ejecutadas desde el PC-A y PC-B a los distintos equipos de la red, sus resultados se evidencian allí:

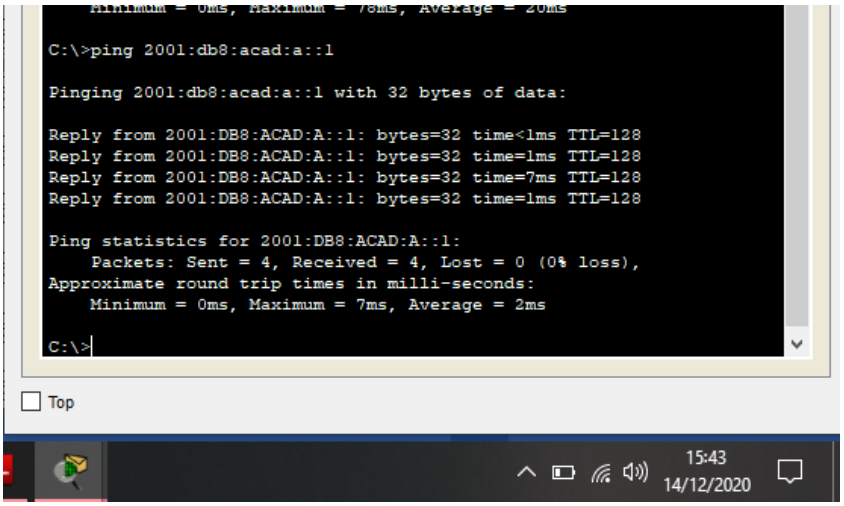
Figura 2. Ping PCA a R1 int G/0/0/1.2 IPv4



Fuente: Autor

En la **figura 2** se realiza un ping desde PCA con dirección IP 10.19.8.53 a R1 por la sub interfaz R1, G0/0/1.2 de dirección IPv4 10.19.8.1, esta fue de resultado exitoso

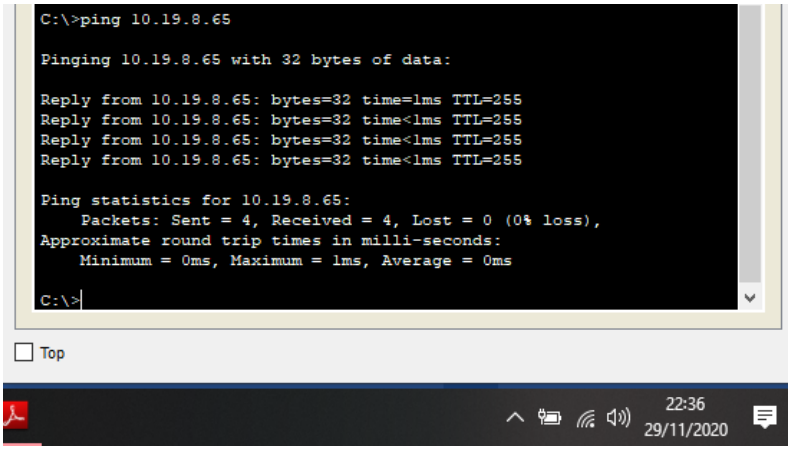
Figura 3. Ping PCA a R1 int G/0/0/1.2 IPv6



Fuente: Autor

En la **figura 3** se realiza un ping desde PCA con dirección IP 10.19.8.53 a R1 por la sub interfaz R1, G0/0/1.2 de dirección IPv6 2001:db8:acad:a::1, esta fue de resultado exitoso

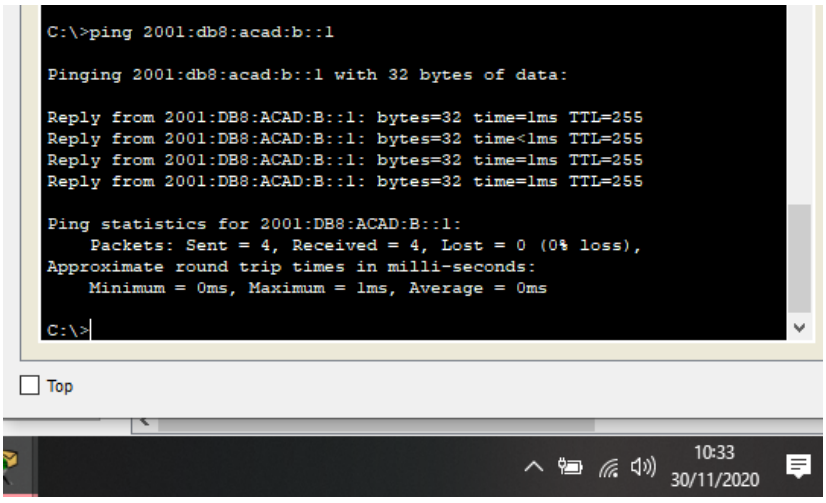
Figura 4. Ping PCA a R1 int G/0/0/1.3 IPv4



Fuente: Autor

En la **figura 4** se realiza un ping desde PCA con dirección IP 10.19.8.53 a R1 por la sub interfaz R1, G0/0/1.3 de dirección IPv4 10.19.8.65, esta fue de resultado exitoso

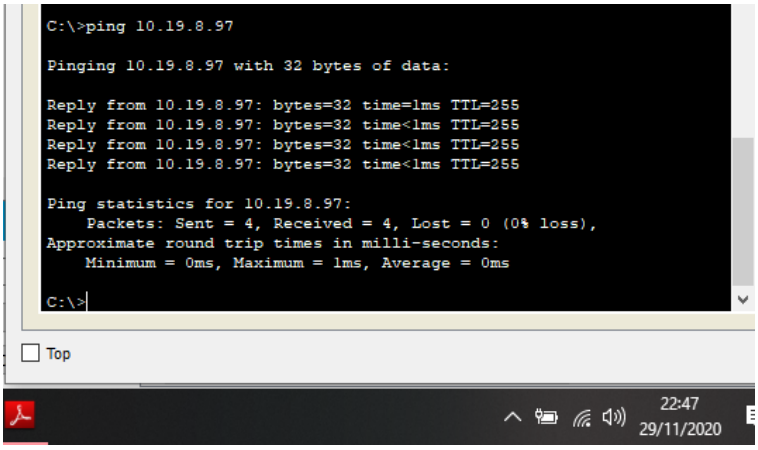
Figura 5. Ping PCA a R1 int G/0/0/1.3 IPv6



Fuente: Autor

En la **figura 5** se realiza un ping desde PCA con dirección IP 10.19.8.53 a R1 por la sub interfaz R1, G0/0/1.3 de dirección IPv6 2001:db8:acad:b::1, esta fue de resultado exitoso

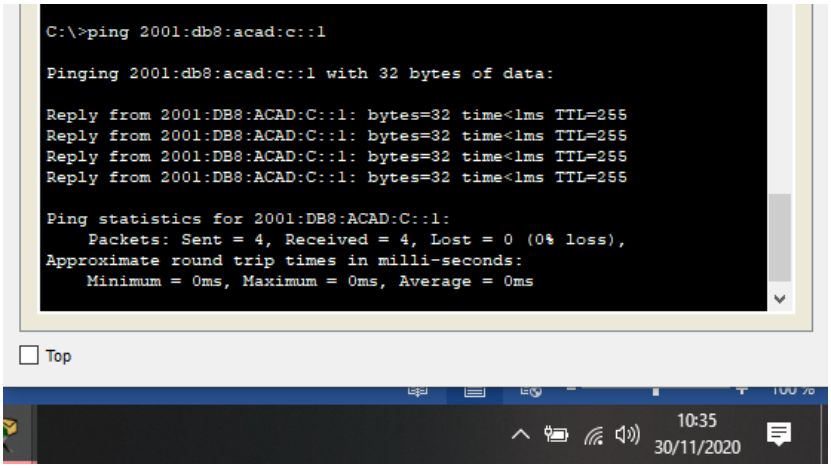
Figura 6. Ping PCA a R1 int G/0/0/1.4 IPv4



Fuente: Autor

En la **figura 6** se realiza un ping desde PCA con dirección IP 10.19.8.53 a R1 por la sub interfaz R1, G0/0/1.4 de dirección IPv4 10.19.8.97, esta fue de resultado exitoso

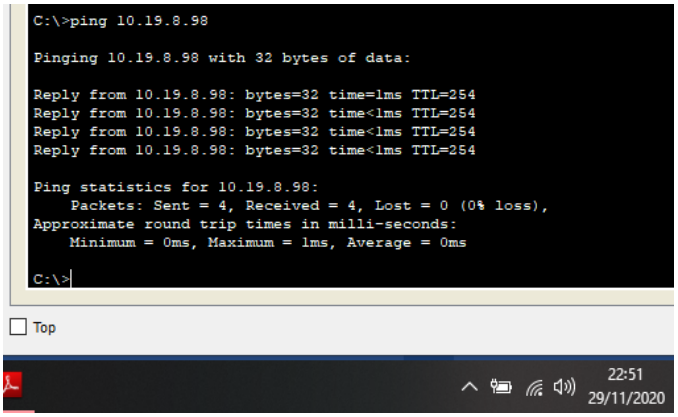
Figura 7. Ping PCA a R1 int G/0/0/1.4 IPv6



Fuente: Autor

En la **figura 7** se realiza un ping desde PCA con dirección IP 10.19.8.53 a R1 por la sub interfaz R1, G0/0/1.4 de dirección IPv6 2001:db8:acad:c::1, esta fue de resultado exitoso

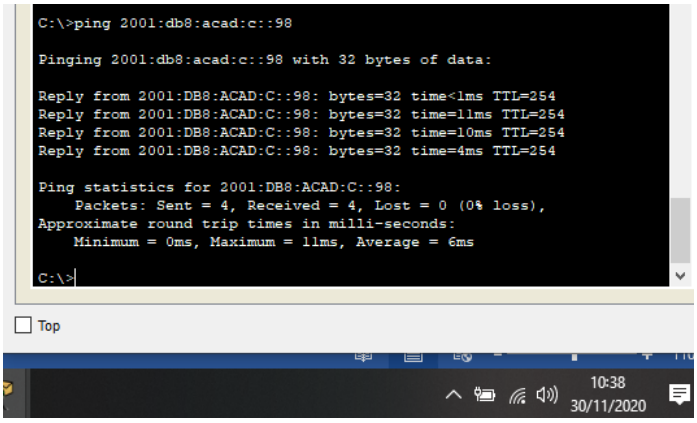
Figura 8 - Ping PCA a S1 Vlan 4 IPv4



Fuente: Autor

En la **figura 8** se realiza un ping desde PCA con dirección IP 10.19.8.53 a S1 VLAN 4, de dirección IPv4 10.19.8.98, esta fue de resultado exitoso

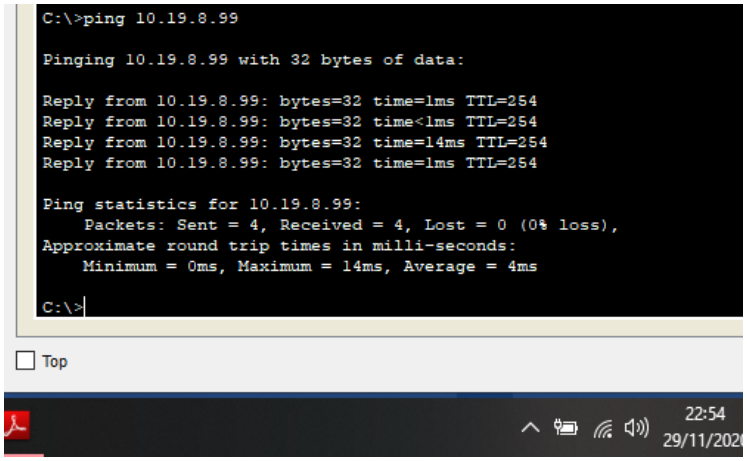
Figura 9. Ping PCA a S1 Vlan 4 IPv6



Fuente: Autor

En la **figura 9** se realiza un ping desde PCA con dirección IP 10.19.8.53 a S1 VLAN 4, de dirección IPv6 2001:db8:acad:c::98, esta fue de resultado exitoso.

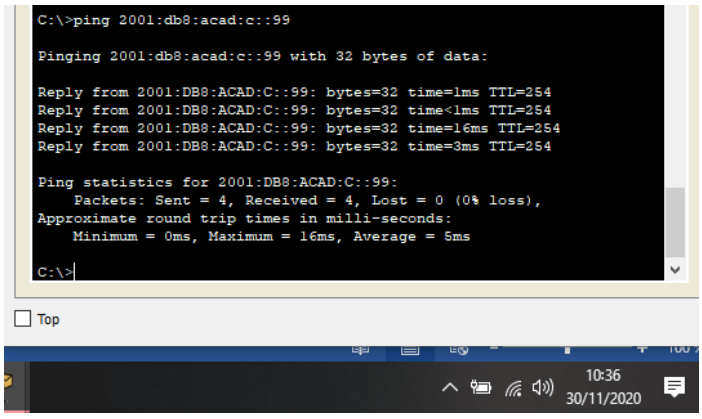
Figura 10. Ping PCA a S2 Vlan 4 IPv4



Fuente: Autor

En la **figura 10** se realiza un ping desde PCA con dirección IP 10.19.8.53 a S2 VLAN 4, de dirección IPv4 10.19.8.99, esta fue de resultado exitoso.

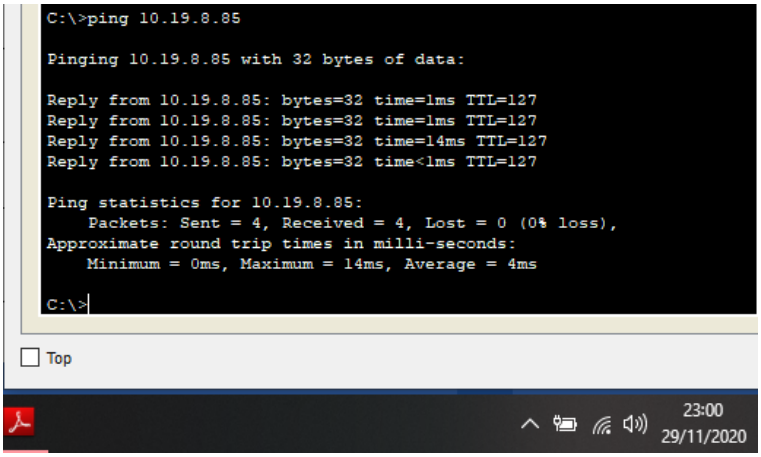
Figura 11. Ping PCA a S2 Vlan 4 IPv6



Fuente: Autor

En la figura 11 se realiza un ping desde PCA con dirección IP 10.19.8.53 a S2 VLAN 4, de dirección IPv6 2001:db8:acad:c::99, esta fue de resultado exitoso

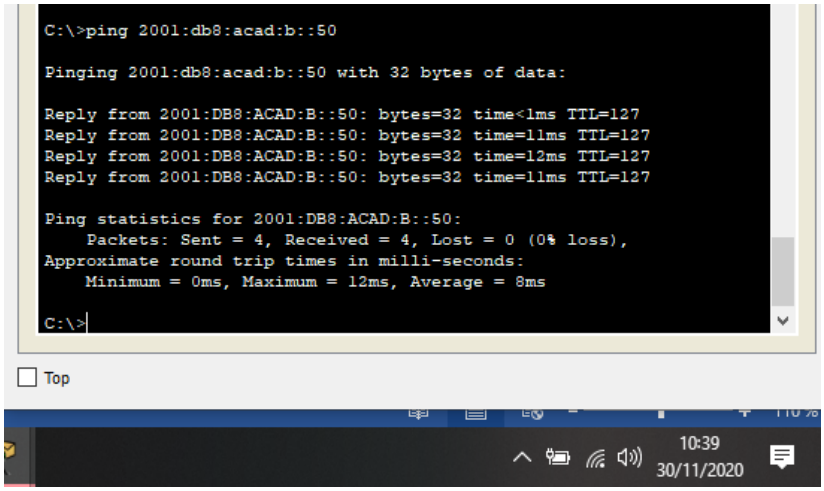
Figura 12 - Ping PCA a PCB IPv4



Fuente: Autor

En la **figura 12** se realiza un ping desde PCA con dirección IP 10.19.8.53 a PC-B, de dirección IPv4 10.19.8.96, esta fue de resultado exitoso

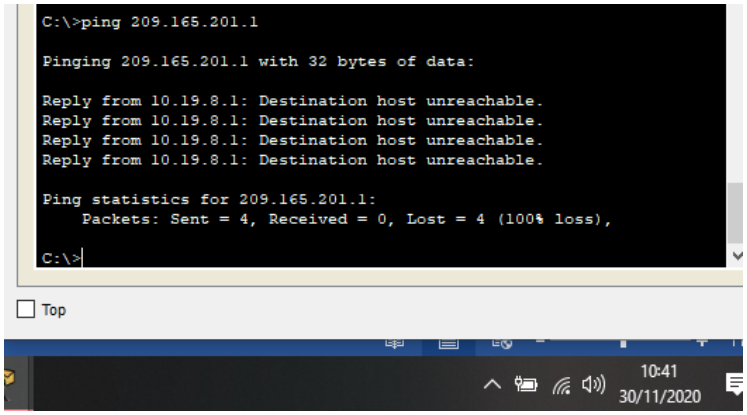
Figura 13 - Ping PCA a PCB IPv6



Fuente: Autor

En la **figura 13** se realiza un ping desde PCA con dirección IP 10.19.8.53 a PC-B, de dirección IPv6 2001:db8:acad:b::50, esta fue de resultado exitoso

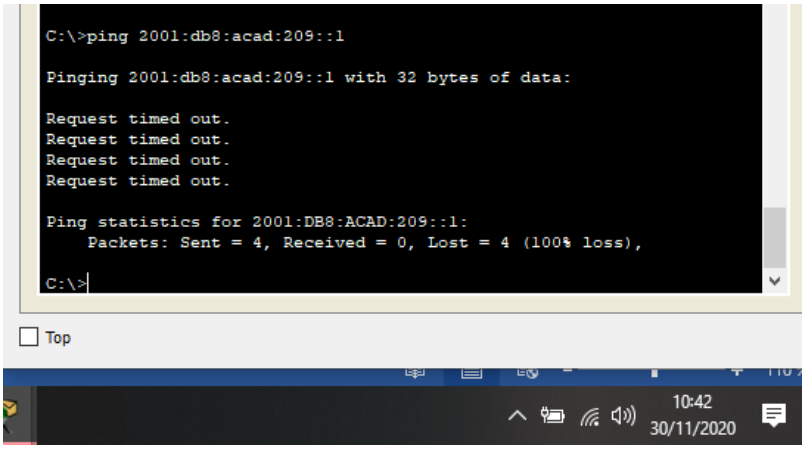
Figura 14. Ping PCA a R1 Bucle 0 IPv4



Fuente: Autor

En la **figura 14** se realiza un ping desde PCA con dirección IP 10.19.8.53 a R1 Bucle0, de dirección IPv4 209.165.201.1, esta fue de resultado fallido

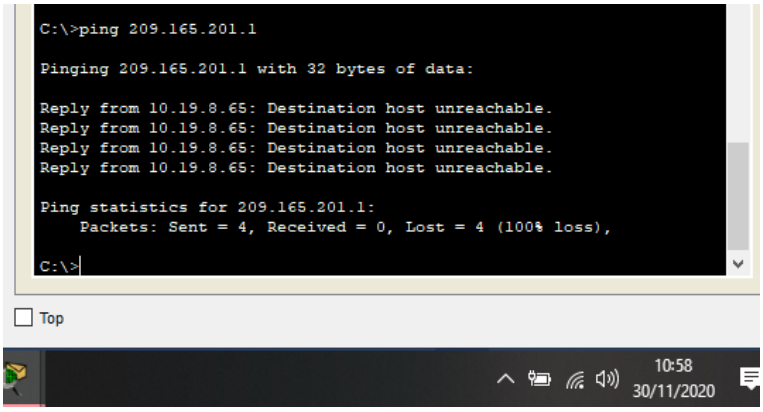
Figura 15. Ping PCA a R1 Bucle 0 IPv6



Fuente: Autor

En la **figura 15** se realiza un ping desde PCA con dirección IP 10.19.8.53 a R1 Bucle0, de dirección IPv6 2001:db8:acad:209::1, esta fue de resultado fallido

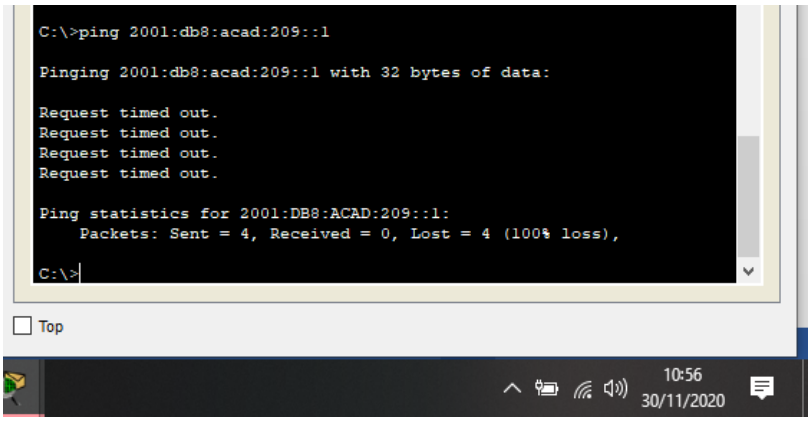
Figura 16. Ping PCB a R1 Bucle 0 IPv4



Fuente: Autor

En la **figura 16** se realiza un ping desde PCB con dirección IP 10.19.8.85 a R1 Bucle0, de dirección IPv4 209.165.201.1, esta fue de resultado fallido

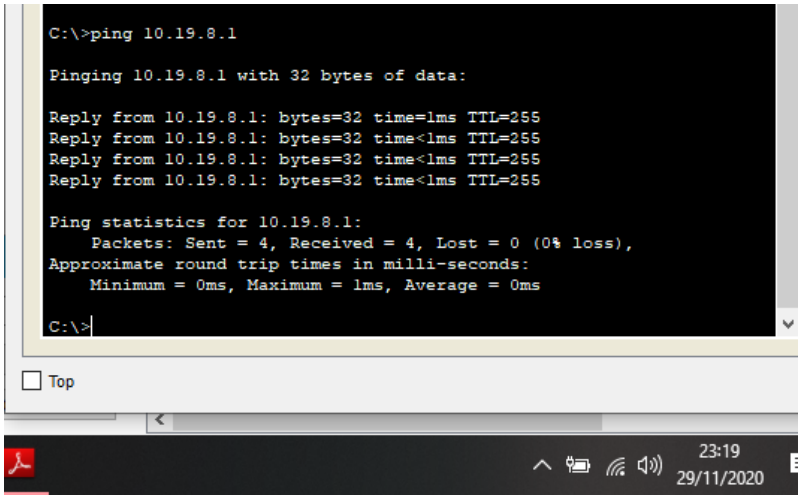
Figura 17. Ping PCB a R1 Bucle 0 IPv6



Fuente: Autor

En la **figura 17** se realiza un ping desde PCB con dirección IP 10.19.8.85 a R1 Bucle0, de dirección IPv6 2001:db8:acad:209::1, esta fue de resultado fallido

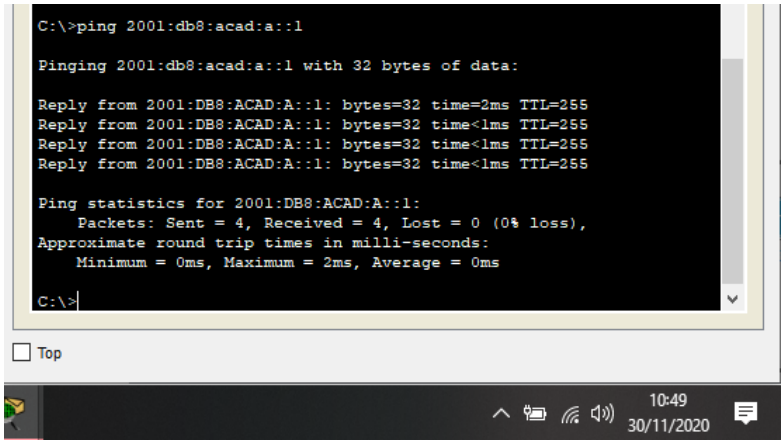
Figura 18. Ping PCB a R1 int G/0/0/1.2 IPv4



Fuente: Autor

En la **figura 18** se realiza un ping desde PCB con dirección IP 10.19.8.85 a R1 por la sub interfaz R1, G0/0/1.2 de dirección IPv4 10.19.8.1, esta fue de resultado exitoso

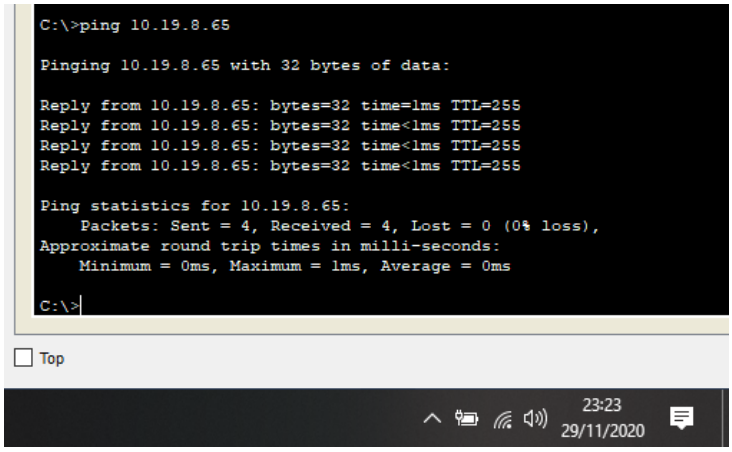
Figura 19. Ping PCB a R1 int G/0/0/1.2 IPv6



Fuente: Autor

En la **figura 19** se realiza un ping desde PCB con dirección IP 10.19.8.85 a R1 por la sub interfaz R1, G0/0/1.2 de dirección IPv6 2001:db8:acad:a::1, esta fue de resultado exitoso

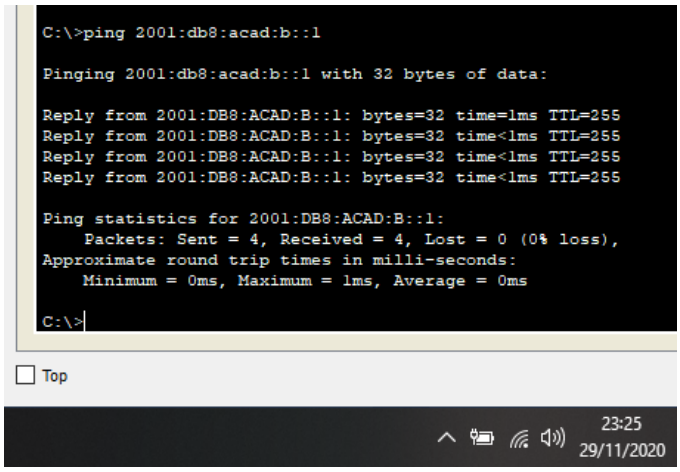
Figura 20 - Ping PCB a R1 int G/0/0/1.3 IPv4



Fuente: Autor

En la **figura 20** se realiza un ping desde PCB con dirección IP 10.19.8.85 a R1 por la sub interfaz R1, G0/0/1.3 de dirección IPv4 10.19.8.65, esta fue de resultado exitoso

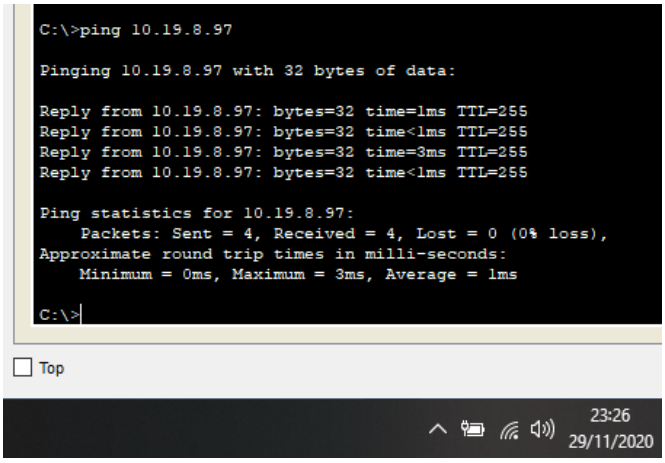
Figura 21. Ping PCB a R1 int G/0/0/1.3 IPv6



Fuente: Autor

En la **figura 21** se realiza un ping desde PCB con dirección IP 10.19.8.85 a R1 por la sub interfaz R1, G0/0/1.3 de dirección IPv6 2001:db8:acad:b::1, esta fue de resultado exitoso

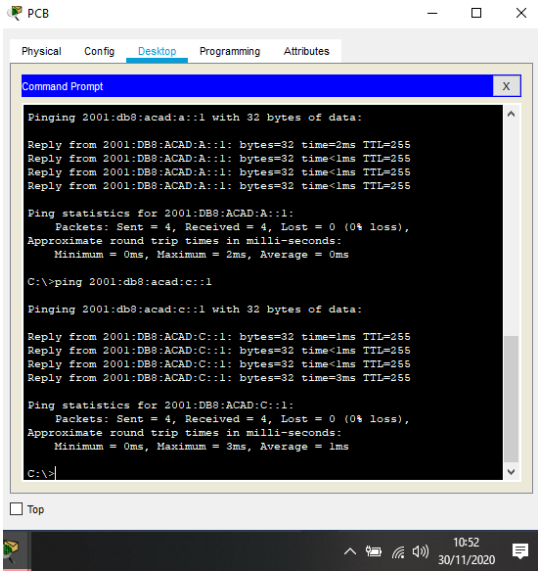
Figura 22. Ping PCB a R1 int G/0/0/1.4 IPv4



Fuente: Autor

En la **figura 22** se realiza un ping desde PCB con dirección IP 10.19.8.85 a R1 por la sub interfaz R1, G0/0/1.4 de dirección IPv4 10.19.8.97, esta fue de resultado exitoso

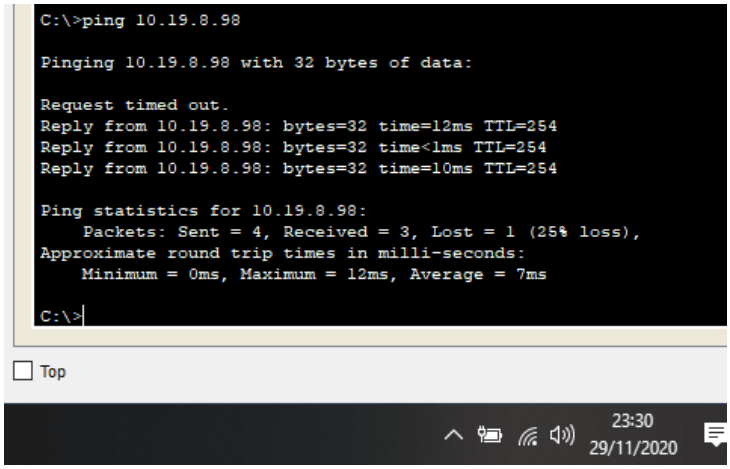
Figura 23. Ping PCB a R1 int G/0/0/1.4 IPv6



Fuente: Autor

En la **figura 23** se realiza un ping desde PCB con dirección IP 10.19.8.85 a R1 por la sub interfaz R1, G0/0/1.4 de dirección IPv6 2001:db8:acad:c::1, esta fue de resultado exitoso

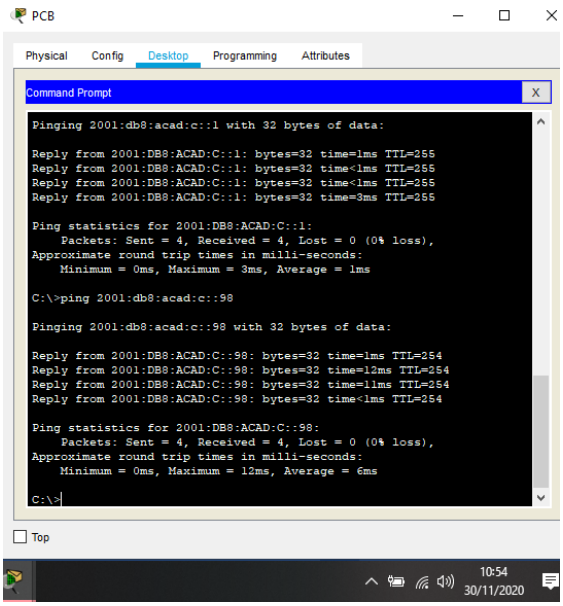
Figura 24 - Ping PCB a S1 Vlan 4 IPv4



Fuente: Autor

En la **figura 24** se realiza un ping desde PCB con dirección IP 10.19.8.85 a S1 VLAN 4, de dirección IPv4 10.19.8.98, esta fue de resultado exitoso

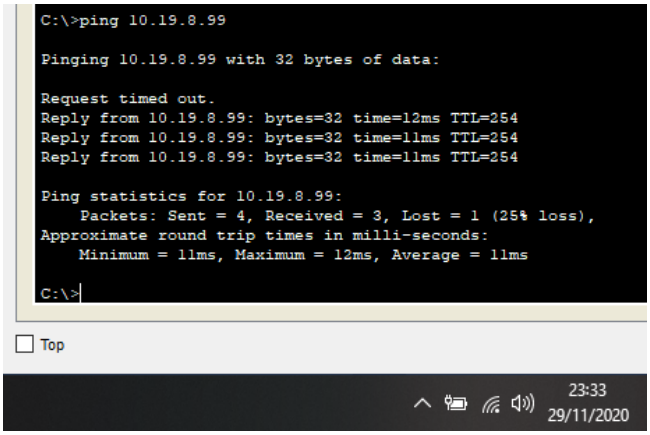
Figura 25. Ping PCB a S1 Vlan 4 IPv6



Fuente: Autor

En la **figura 25** se realiza un ping desde PCB con dirección IP 10.19.8.85 a S1 VLAN 4, de dirección IPv6 2001:db8:acad:c::98, esta fue de resultado exitoso

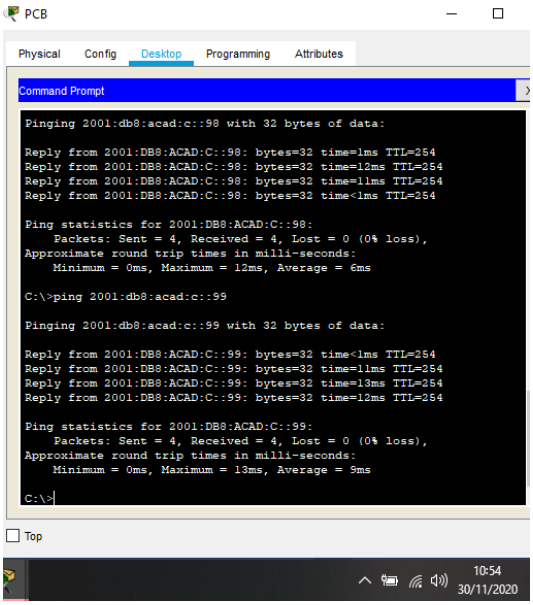
Figura 26. Ping PCB a S2 Vlan 4 IPv4



Fuente: Autor

En la **figura 26** se realiza un ping desde PCB con dirección IP 10.19.8.85 a S2 VLAN 4, de dirección IPv4 10.19.8.99, esta fue de resultado exitoso

Figura 27. Ping PCB a S2 Vlan 4 IPv6

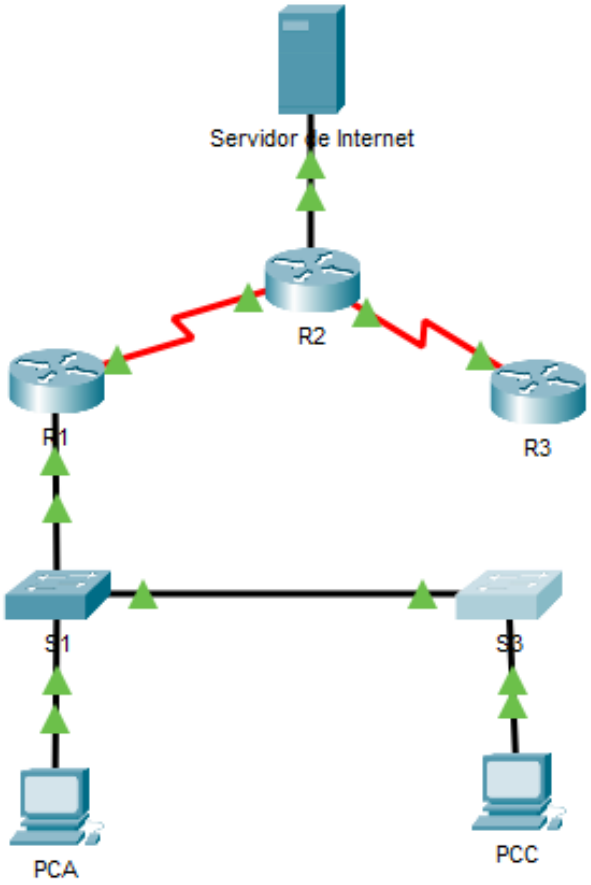


Fuente: Autor

En la **figura 27** se realiza un ping desde PCB con dirección IP 10.19.8.85 a S2 VLAN 4, de dirección IPv6 2001:db8:acad:c::99, esta fue de resultado exitoso

ESCENARIO 2

Figura 28. Escenario 2



Fuente: Autor

Se debe configurar una red pequeña como se visualiza en la **Figura 28** 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.

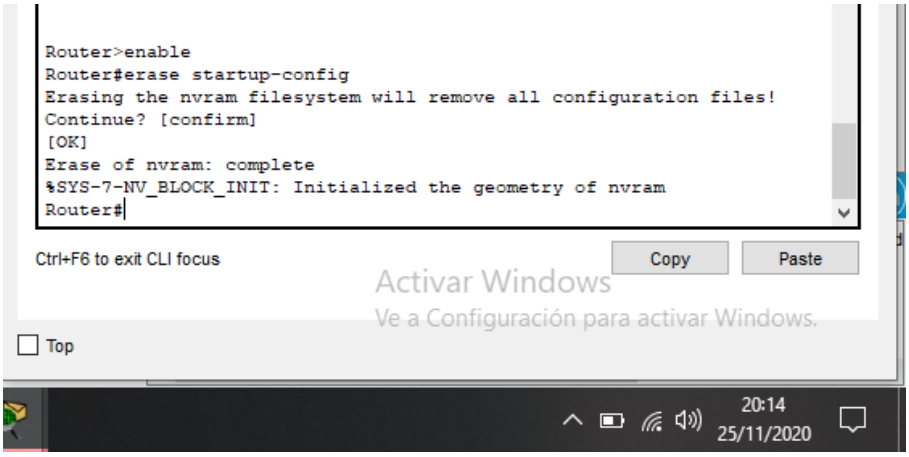
Parte 1: inicialización de los dispositivos

1.1 Inicializar y volver a cargar los routers y los switches: en esta parte como se visualizara en la **Tabla 11** con los comandos respectivos se eliminaran las configuraciones de inicio de los router y de los switch, con las bases de datos VLAN después volver a cargar los dispositivos

Tabla 10. Inicio y carga de router y switches

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#erase startup-config Switch#delete vlan.dat
Volver a cargar ambos switches	Switch#reload
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Switch>enable Switch#show flash:

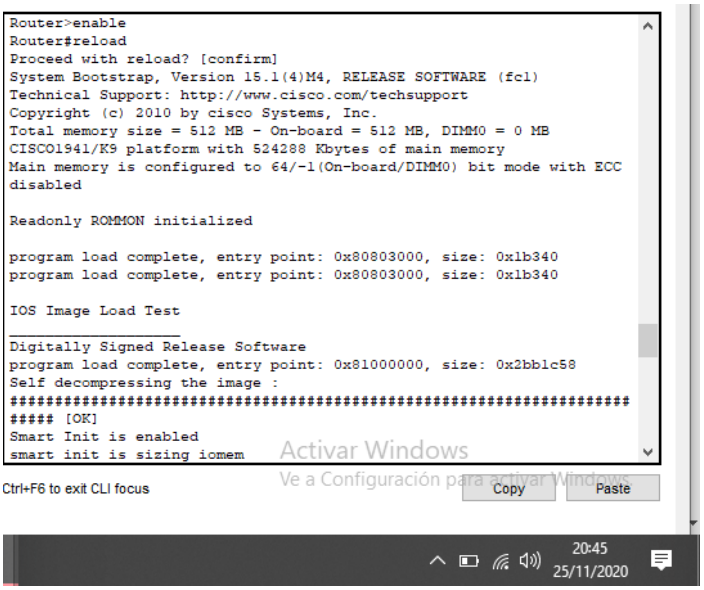
Figura 29. Eliminacion de archivos de configuracion de los Router



Fuente: Autor

En la **figura 29** se evidencia la eliminación de los archivos de configuracion de uno de los 3 Router, este proceso se repite en los otros 2, siguiendo los pasos indicados en la Tabla 9.

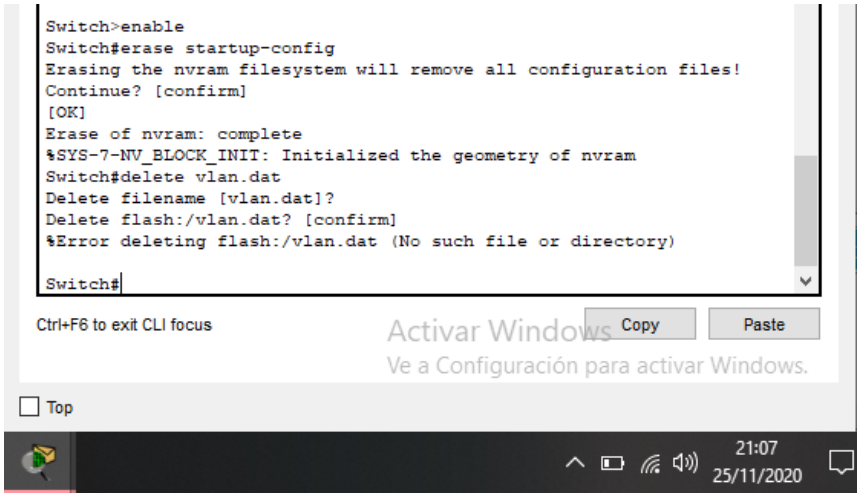
Figura 30. Recarga de los Routers



Fuente: Autor

En la **figura 30** se evidencia los proceos de la recarga de los router que hacen parte de la red

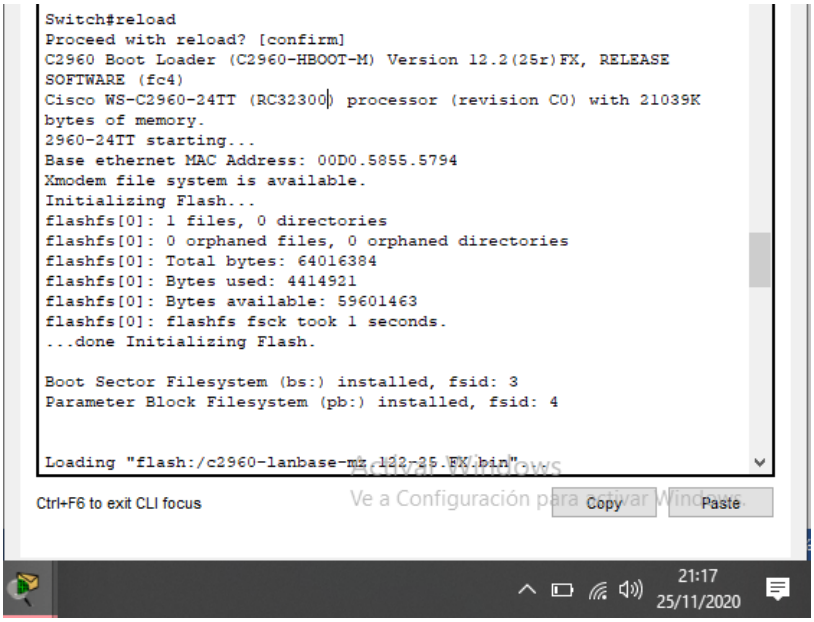
Figura 31. Eliminacion de archivos startup-config de switches y base de datos Vlan



Fuente: Autor

En la **figura 31** se evidencia la eliminación de los archivos de configuracion de uno de los 2 Switches, este proceso se repite en el otro, siguiendo los pasos indicados en la Tabla 9.

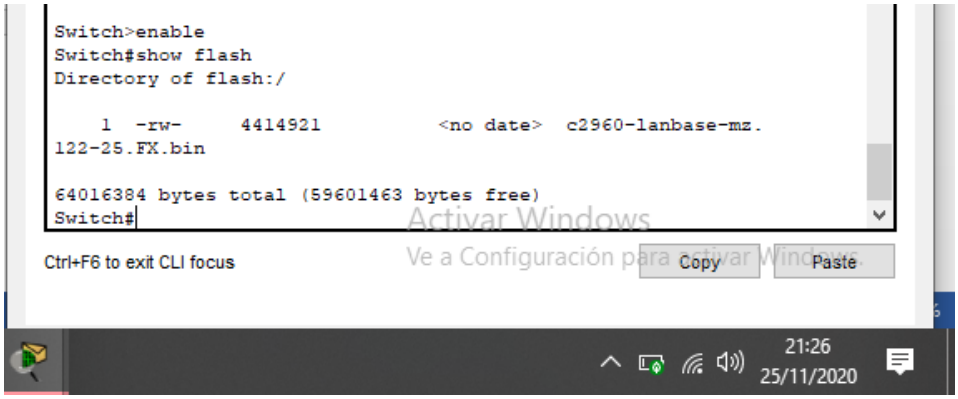
Figura 32. Recarga de Switches



Fuente: Autor

En la **figura 32** se evidencia los procesos de la recarga de los Switches que hacen parte de la red

Figura 33 - verificacion de la BD de Vlan que no esten en la flash de los switches



Fuente: Autor

Se puede visualizar en la figura en la **figura 33** que la base de datos de VLAN no esté en la memoria flash en ambos switches.

Nota: los anteriores procedimientos se aplican para todos los Routers y Switch

Parte 2: Configurar los parámetros básicos de los dispositivos

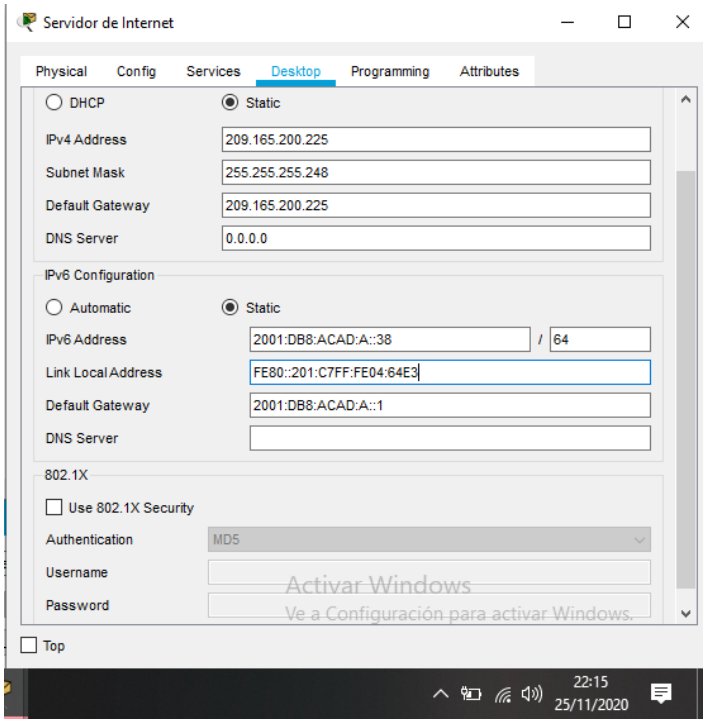
2.1 Configurar la computadora de internet

Los pasos que se describen en la **Tabla 12** se asignan los parámetros respectivos para el sevidor de iternet, su direccionamiento IPv4 e IPv4 con sus Gateway predeterminados.

Tabla 11. Configuracion de la PC 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	209.165.200.225
Dirección IPv6/subred	2001:DB8:ACAD:A::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:2::1

Figura 34. Configuracion del servidor de internet



Fuente: Autor

En la **figura 34** de hace evidencia la configuracion del sevidor web con la asignación respectivas de sus direcciones IP

2.3 Configuracion del Router 1 (R1)

En la **Tabla 13** los comandos que se observan desactivan la búsqueda DNS, asignan el nombre del router (R1), además de que asigna las respectivas contraseñas de exec privilegiado cifrada, de acceso a la consola y de acceso Telnet, seguidamente se cifran las contraseñas de texto no cifrado se le asigna el direccionamiento a la Interfaz S0/0/0 y sus rutas predeterminadas

Tabla 12. Configuracion de R1

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R1
Contraseña de exec privilegiado cifrada	R1(config)#enable secret class
Contraseña de acceso a la consola	R1(config)#line console 0 R1(config-line)#password cisco R1(config-line)#login
Contraseña de acceso Telnet	R1(config-line)#line vty 0 15 R1(config-line)#password cisco R1(config-line)#login
Cifrar las contraseñas de texto no cifrado	R1(config-line)#service passwordencryption
Mensaje MOTD	R1(config)#banner motd %Se prohíbe el acceso no autorizado.%
Interfaz S0/0/0	R1(config)#int s0/0/0 R1(config-if)#ip address 172.16.1.1 255.255.255.252 R1(config-if)#ipv6 address 2001:db8:acad:1::1/64 R1(config-if)#clock rate 128000 R1(config-if)#no shutdown R1(config-if)#exit
Rutas predeterminadas	R1(config)#ipv6 route ::/0 s0/0/0 R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0

2.4 Configuracion del Router 2 (R2)

En la **Tabla 14** a continuación se hace una descripción del proceso con sus respectivos comandos, donde se hace el cambio de nombre, se establecieron y cifraron las contraseñas, se activo un mensaje de advertencia y se habilito el servidor HTTP, además de la asignación de direcciones de las interfaces allí mostradas

Tabla 13. Configuracion de R2

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R2
Contraseña de exec privilegiado cifrada	R2(config)#enable secret class
Contraseña de acceso a la consola	R2(config)#line console 0 R2(config-line)#password cisco R2(config-line)#login
Contraseña de acceso Telnet	R2(config-line)#line vty 0 15 R2(config-line)#password cisco R2(config-line)#login
Cifrar las contraseñas de texto no cifrado	R1(config-line)#service passwordencryption
Habilitar el servidor HTTP	R2(config)#ip http server
Mensaje MOTD	R1(config)#banner motd %Se prohíbe el acceso no autorizado.%
Interfaz S0/0/0	R2(config)#int s0/0/0 R2(config-if)#description connection to R1 R2(config-if)#ip address 172.16.1.2 255.255.255.252 R2(config-if)#ipv6 address 2001:db8:acad:1::2/64 R2(config-if)#no shutdown
Interfaz S0/0/1	R2(config-if)#int s0/0/1 R2(config-if)#description connection to R3 R2(config-if)#ip address 172.16.2.2 255.255.255.252 R2(config-if)#ipv6 address 2001:db8:acad:2::2/64 R2(config-if)#clock rate 128000 R2(config-if)#no shutdown

Interfaz G0/0 (simulación de Internet)	R2(config-if)#int g0/0 R2(config-if)#description connection to Internet R2(config-if)#ip address 209.165.200.233 255.255.255.248 R2(config-if)#ipv6 address 2001:db8:acad:a::2/64 R2(config-if)#no shutdown
Interfaz loopback 0 (servidor web simulado)	R2(config-if)#int loopback 0 R2(config-if)#ip address 10.10.10.10 255.255.255.255 R2(config-if)#description simulated web server
Ruta predeterminada	R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0 R2(config)#ipv6 route ::/0 g0/0

2.5 Configuracion del Router 3 (R3)

En la **Tabla 15** a continuación se hace una descripción del proceso con sus respectivos comandos, donde se hace el cambio de nombre, se establecieron y cifraron las contraseñas, se activo un mensaje de advertencia, además de la asignación de direcciones de las interfaces allí mostradas

Tabla 14. Configuracion de R3

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R3
Contraseña de exec privilegiado cifrada	R3(config)#enable secret class
Contraseña de acceso a la consola	R3(config)#line console 0 R3(config-line)#password cisco R3(config-line)#login
Contraseña de acceso Telnet	R3(config-line)#line vty 0 15 R3(config-line)#password cisco R3(config-line)#login
Cifrar las contraseñas de texto no cifrado	R3(config-line)#service passwordencryption
Mensaje MOTD	R3(config)#banner motd %Se prohíbe el acceso no autorizado.%

Interfaz S0/0/1	R3(config)#int s0/0/1 R3(config-if)#description connection to R2 R3(config-if)#ip address 172.16.2.1 255.255.255.252 R3(config-if)#ipv6 address 2001:db8:acad:2::1/64 R3(config-if)#no shutdown
Interfaz loopback 4	R3(config-if)#int loopback 4 R3(config-if)#ip address 192.168.4.1 255.255.255.0
Interfaz loopback 5	R3(config-if)#int loopback 5 R3(config-if)#ip address 192.168.5.1 255.255.255.0
Interfaz loopback 6	R3(config-if)#int loopback 6 R3(config-if)#ip address 192.168.6.1 255.255.255.0
Interfaz loopback 7	R3(config-if)#int loopback 7 R3(config-if)#ipv6 address 2001:db8:acad:3::1/64
Rutas Predeterminadas	R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1 R3(config)#ipv6 route ::/0 s0/0/1

2.6 Configurar S1

En la **Tabla 16** a continuación se hace una descripción del proceso con sus respectivos comandos, donde se hace el cambio de nombre, se descativo la búsqueda DNS, se establecieron y cifraron las contraseñas, se activo un mensaje de advertencia.

Tabla 15. Configuracion de S1

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Switch(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S1
Contraseña de exec privilegiado cifrada	S1(config)#enable secret class
Contraseña de acceso a la consola	S1(config)#line console 0 S1(config-line)#password cisco S1(config-line)#login

Contraseña de acceso Telnet	S1(config-line)#line vty 0 15 S1(config-line)#password cisco S1(config-line)#login
Cifrar las contraseñas de texto no cifrado	S1(config-line)#service passwordencryption
Mensaje MOTD	S1(config)#banner motd &Se prohibe el acceso no autorizado.&

2.7 Configurar S3

En la **Tabla 17** a continuación se hace una descripción del proceso con sus respectivos comandos, donde se hace el cambio de nombre, se descativo la búsqueda DNS, se establecieron y cifraron las contraseñas, se activo un mensaje de advertencia.

Tabla 16. Configuracion de S3

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Switch(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S3
Contraseña de exec privilegiado cifrada	S3(config)#enable secret class
Contraseña de acceso a la consola	S3(config)#line console 0 S3(config-line)#password cisco S3(config-line)#login
Contraseña de acceso Telnet	S3(config-line)#line vty 0 15 S3(config-line)#password cisco S3(config-line)#login
Cifrar las contraseñas de texto no cifrado	S3(config-line)#service passwordencryption
Mensaje MOTD	S3(config)#banner motd &Se prohibe el acceso no autorizado.&

2.8 Probar la Conectividad de la red.

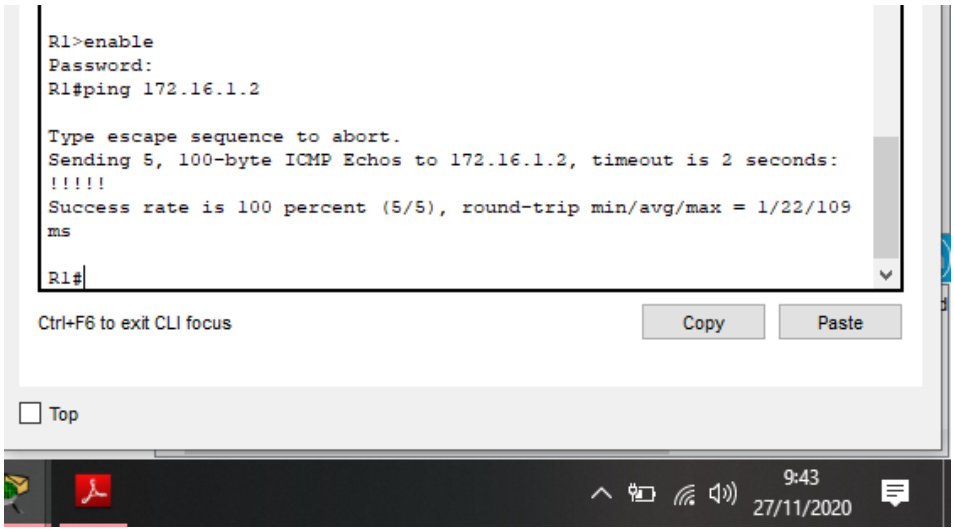
En esta etapa de la segunda parte de la configuración de los dispositivos, se hace la verificación de la conectividad de la red.

Se utiliza el comando ping para probar la conectividad entre los dispositivos de red como se muestra en la **Tabla 18**. Se usa la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red.

Tabla 17. Pruebas de Conectividad

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	Exitoso
R2	R3, S0/0/1	172.16.2.1	Exitoso
PC de Internet	Gateway predeterminado	209.165.200.225	Exitoso

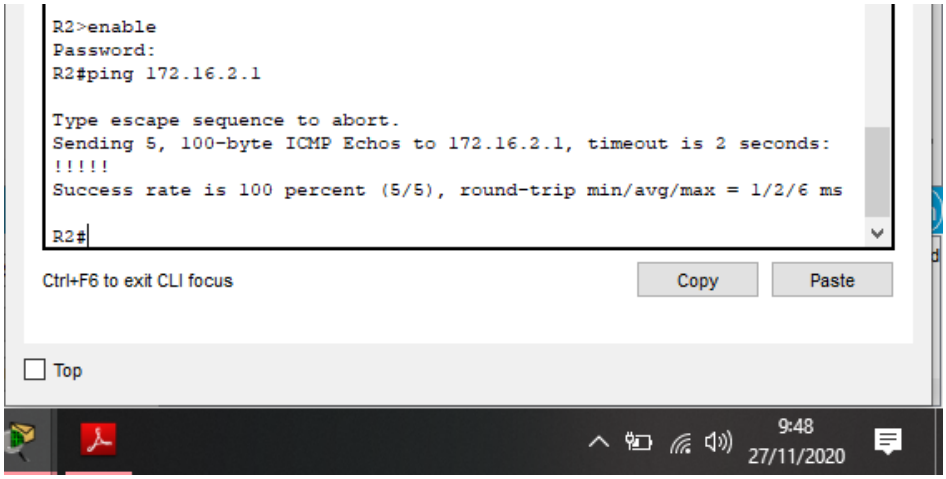
Figura 35. Prueba de conexion de R1



Fuente: Autor

En la **figura 35** se puede detallar los comandos utilizados para asi probar la conectividad de R1 a R2, como se indica debe utilizarse la interfaz S0/0/0, igualmente se muestra los resultados exitosos

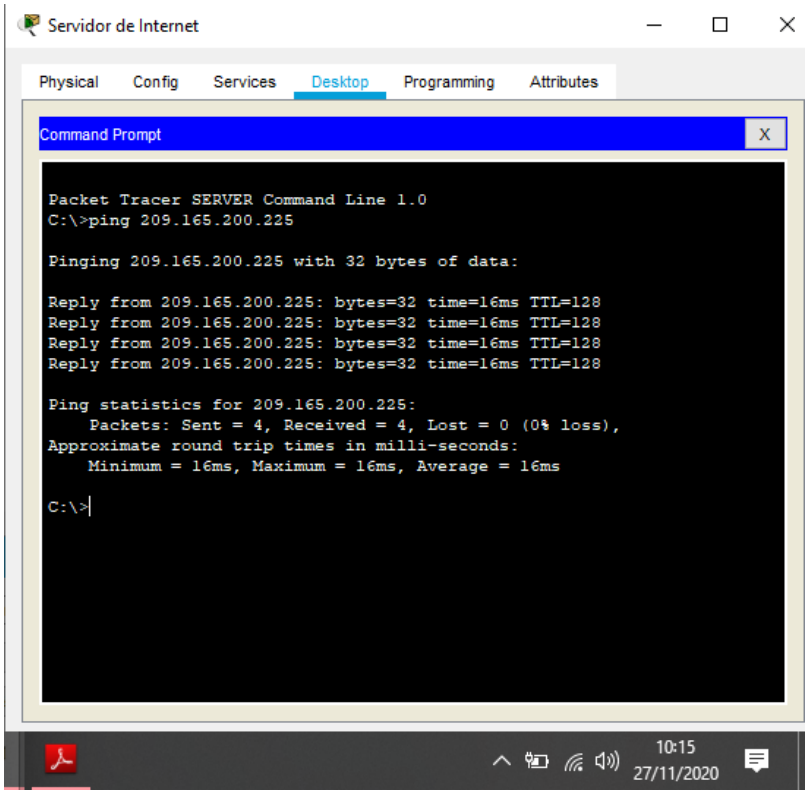
Figura 36. Prueba de conexion de R2



Fuente: Autor

En la **figura 36** se puede detallar los comandos utilizados para así probar la conectividad de R2 a R3, como se indica debe utilizarse la interfaz S0/0/1, igualmente se muestra los resultados exitosos

Figura 37. Prueba de conexion del PC de internet



Fuente: Autor

En la **figura 37** se puede detallar los comandos utilizados para así probar la conectividad del Servidor de Internet al Gateway Predeterminado, igualmente se muestra los resultados exitosos

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

En esta parte del documento procederemos al proceso de configuración de los distintos switches, la creación de las VLAN en ellos y el ruoting entre las mismas

3.1 Configurar S1

Como bien se especifica en los comandos de la **Tabla 19** se procedio a crear la base de datos de VLAN, lo mismo que la asignación de la dirección IP de administración, el gateway predeterminado, después se forzó el enlace troncal en las interfaces F0/3 y F0/5, como tambien configurar el resto de los puertos como

puertos de acceso y para terminar la asignación de F0/6 a la VLAN 21 y el apagado de todos los puertos sin usar

Tabla 18. Configuracion de seguridad, VLAN y routing de S1

Elemento o tarea de configuración	**Especificación**
Crear la base de datos de VLAN	S1#configure terminal S1(config)#vlan 21 S1(config-vlan)#name Contabilidad S1(config-vlan)#vlan 23 S1(config-vlan)#name Ingenieria S1(config-vlan)#vlan 99 S1(config-vlan)#name Administracion
Asignar la dirección IP de administración.	S1#configure terminal S1(config)#int vlan 99 S1(config-if)#ip address 192.168.99.2 255.255.255.0 S1(config-if)#no shutdown
Asignar el gateway predeterminado	S1(config)#ip 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	S1(config-if)#int f0/3 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1
Forzar el enlace troncal en la interfaz F0/5	S1(config-if)#int f0/5 S1(config-if)#switchport mode trunk 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, f0/7-24, g0/1-2 S1(config-if-range)#switchport mode access
Asignar F0/6 a la VLAN 21	S1#configure terminal S1(config-if-range)#int f0/6 S1(config-if)#switchport access vlan 21
Apagar todos los puertos sin usar	S1(config-if-range)#int range f0/1-2, f0/4, f0/7-24, g0/1-2 S1(config-if-range)#shutdown

3.2 Configurar S3

Como bien se especifica en los comandos de la **Tabla 20** se procedio a crear la base de datos de VLAN, lo mismo que la asignación de la dirección IP de administración, el gateway predeterminado, después se forzó el enlace troncal en

la interfaz F0/3, como tambien configurar el resto de los puertos como puertos de acceso, asignar F0/18 a la VLAN 23 y el apagado de todos los puertos sin usar

Tabla 19. Configuracion de seguridad, VLAN y routing de S3

Elemento o tarea de configuración	**Especificación**
Crear la base de datos de VLAN	S3#configure terminal S3(config)#vlan 21 S3(config-vlan)#name Contabilidad S3(config-vlan)#vlan 23 S3(config-vlan)#name Ingenieria S3(config-vlan)#vlan 99 S3(config-vlan)#name Administracion
Asignar la dirección IP de administración	S3#configure terminal S3(config)#int vlan 99 S3(config-if)#ip address 192.168.99.3 255.255.255.0 S3(config-if)#no shutdown
Asignar el gateway predeterminado.	S3#configure terminal S3(config)#ip default-gateway192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	S3#configure terminal S3(config)#int f0/3 S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	S3(config-if)#int range f0/1-2, f0/4-17, f0/19-24, g0/1-2 S3(config-if-range)#switchport mode access
Asignar F0/18 a la VLAN 23	S3#configure terminal S3(config-if-range)#int f0/18 S3(config-if)#switchport access vlan 23
Apagar todos los puertos sin usar	S3(config-if)#int range f0/1-2, f0/4-17, f0/19-24, g0/1-2 S3(config-if-range)#shutdown

3.3. Configuracion de R1

Se realizara las respectivas asignaciones de direcciones ip a las diferentes vlan, esto gracias a los direferentes comandos evidenciados en la **Tabla 21,**

Tabla 20. Asignacion de la direcciones IP a las VLAN

Elemento o tarea de configuración	**Especificación**
Configurar la subinterfaz 802.1Q .21 en G0/1	R1#configure terminal R1(config)#int g0/1.21 R1(config-subif)#description VLAN 21 R1(config-subif)#encapsulation dot1q21 R1(config-subif)#ip address 192.168.21.1 255.255.255.0
Configurar la subinterfaz 802.1Q .23 en G0/1	R1(config-subif)#int g0/1.23 R1(config-subif)#description VLAN 23 R1(config-subif)#encapsulation dot1q23 R1(config-subif)#ip address 192.168.23.1 255.255.255.0
Configurar la subinterfaz 802.1Q .99 en G0/1	R1(config-subif)#description VLAN 99 R1(config-subif)#encapsulation dot1q99 R1(config-subif)#ip address 192.168.99.1 255.255.255.0
Activar la interfaz G0/1	R1(config-subif)#int g0/1 R1(config-if)#no shutdow

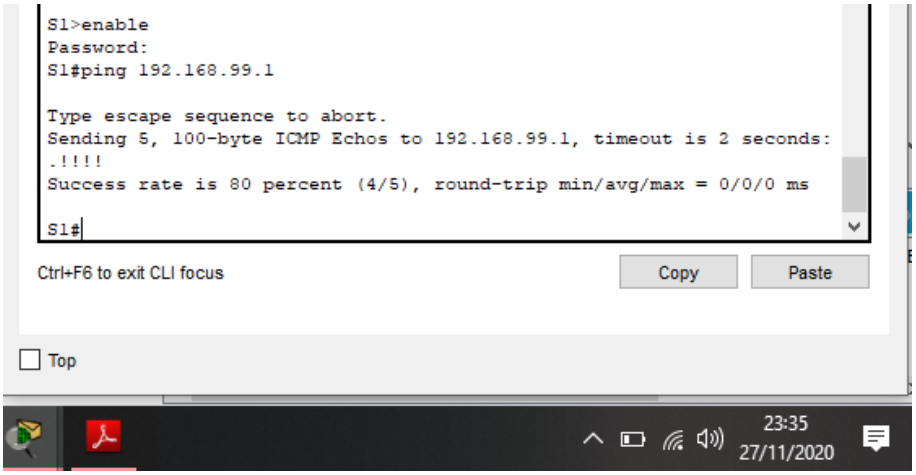
3.4 Verificar la conectividad de la red

En la **Tabla 22** se evidencia la utilización del comando ping para probar la conectividad entre los switches y el R1.

Tabla 21. Verificacion de la conectividad de la red

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

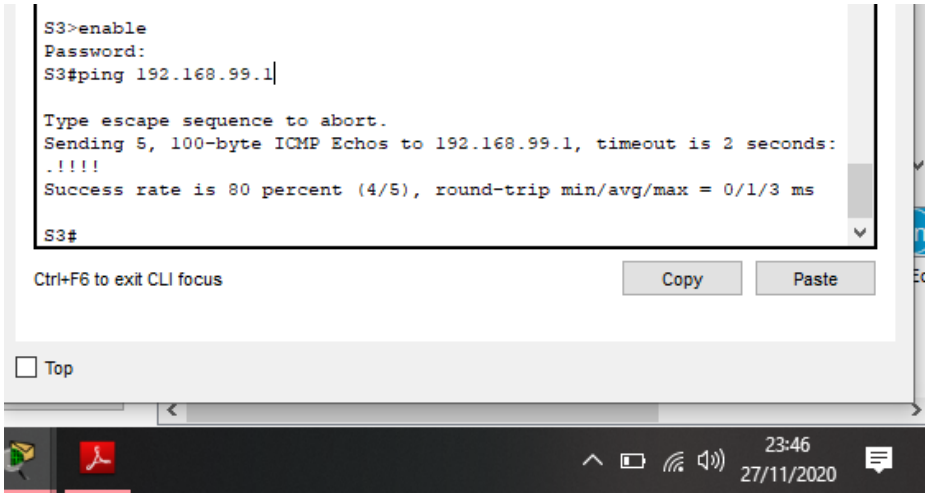
Figura 38. Ping de S1 a R1 por Vlan 99



Fuente: Autor

En la **figura 38** se puede evidenciar la prueba de conectividad, realizando un Ping de S1 a R1 por Vlan 99, siendo este exitoso.

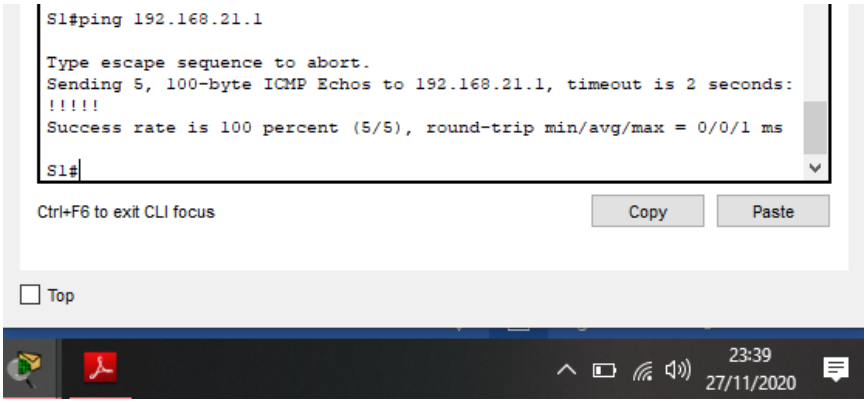
Figura 39. Ping de S3 a R1 por Vlan 99



Fuente: Autor

En la **figura 39** se puede evidenciar la prueba de conectividad, realizando un Ping de S3 a R1 por Vlan 99, siendo este exitoso.

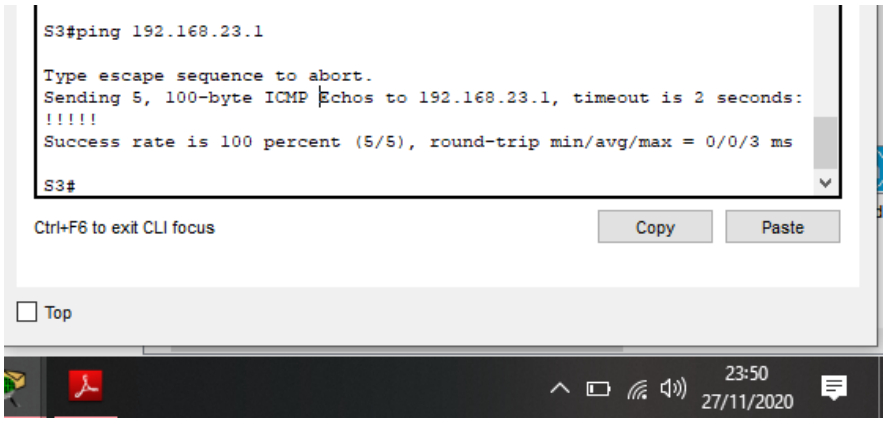
Figura 40. Ping de S1 a R1 por Vlan 21



Fuente: Autor

En la **figura 40** se puede evidenciar la prueba de conectividad, realizando un Ping de S1 a R1 por Vlan 21, siendo este exitoso

Figura 41. Ping de S3 a R1 por Vlan 23



Fuente: Autor

En la **figura 41** se puede evidenciar la prueba de conectividad, realizando un Ping de S3 a R1 por Vlan 23, siendo este exitoso

Parte 4: Configurar el protocolo de routing dinámico OSPF

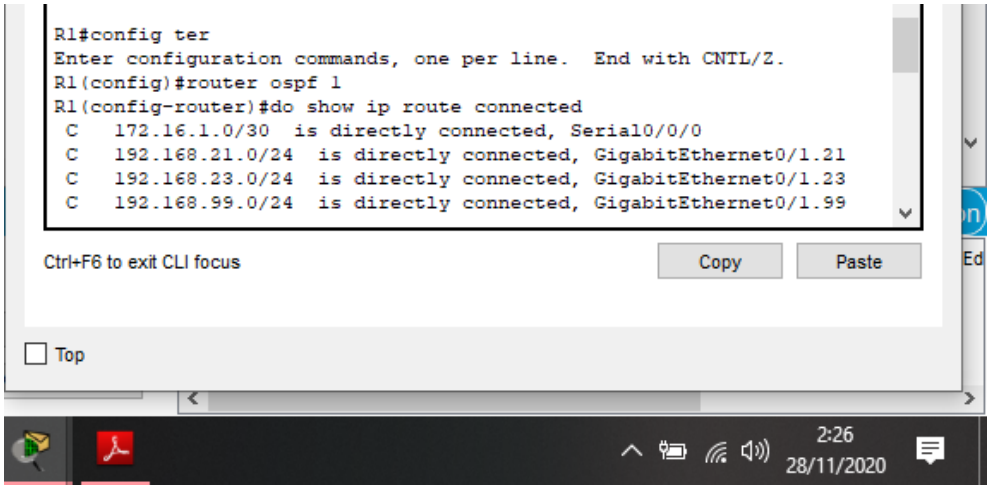
4.1 Configurar OSPF en el R1

En la **Tabla 23** se observar los comandos que se utilizaron para configurar el protocolo OSPF, donde se configura OSPF área 0, se realiza el anuncio de las redes conectadas directamente, se establecen todas las interfaces LAN como pasivas y para culminar se desactiva la sumarización automática

Tabla 22. Tabla de configuracion OSPF en R1

Elemento o tarea de configuración	**Especificación**
Configurar OSPF área 0	R1#config terminal Enter configuration commands, one per line. End with CNTL/Z. R1(config)#router ospf 1 R1(config-router)#network 172.16.1.0 0.0.0.255 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
Anunciar las redes conectadas directamente	R1(config-router)#do show ip route connected C 172.16.1.0/30 is directly connected, Serial0/0/0 C 192.168.21.0/24 is directly connected, GigabitEthernet0/1.21 C 192.168.23.0/24 is directly connected, GigabitEthernet0/1.23 C 192.168.99.0/24 is directly connected, GigabitEthernet0/1.99
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	R1(config-router)#no auto-summary

Figura 42. Anuncio de las redes conectadas directamente



Fuente: Autor

En la **figura 42** se evidencia cuales son las redes que estan conectadas directamente una vez aplicado el procolo OSPF en R1

4.2 Configurar OSPF en el R2

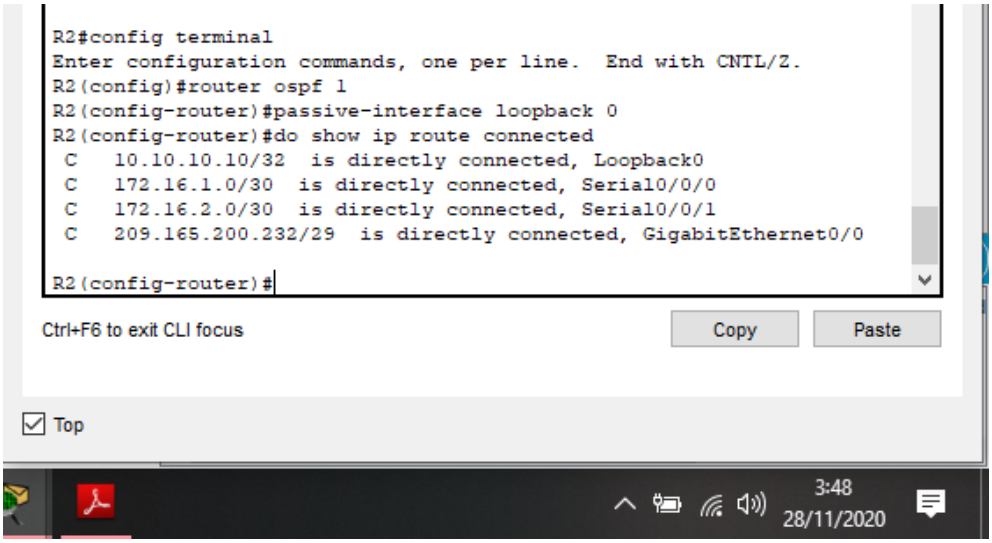
En la **Tabla 24** se observar los comandos que se utilizaron para configurar el protocolo OSPF, donde se configura OSPF área 0, se realiza el anuncio de las redes conectadas directamente, se establecen todas las interfaces LAN (loopback) como pasivas y para culminar se desactiva la sumarización automática

Tabla 23. Tabla de configuracion OSPF en R2

Elemento o tarea de configuración	**Especificación**
Configurar OSPF área 0	R2(config)#router ospf 1 R2(config-router)#network 10.10.10.10 0.0.0.255 area 0 R2(config-router)#network 172.16.1.0 0.0.0.255 area 0 R2(config-router)#network 172.16.1.0 0.0.0.255 area 0 17:47:56: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.99.1 on Serial0/0/0router ospf 1 R2(config-router)#network 172.16.2.0 0.0.0.255 area 0

Anunciar las redes conectadas directamente	R2(config-router)#do show ip route connected C 10.10.10.10/32 is directly connected, Loopback0 C 172.16.1.0/30 is directly connected, Serial0/0/0 C 172.16.2.0/30 is directly connected, Serial0/0/1
Establecer la interfaz LAN (loopback) como pasiva	R2(config)#router ospf 1 R2(config-router)#passive-interface loopback 0
Desactive la sumarización automática.	R1(config-router)#no auto-summary

Figura 43. Anunciar las redes conectadas directamente en R2



Fuente: Autor

En la **figura 43** se evidencia cuales son las redes que estan conectadas directamente una vez aplicado el procolo OSPF en R2

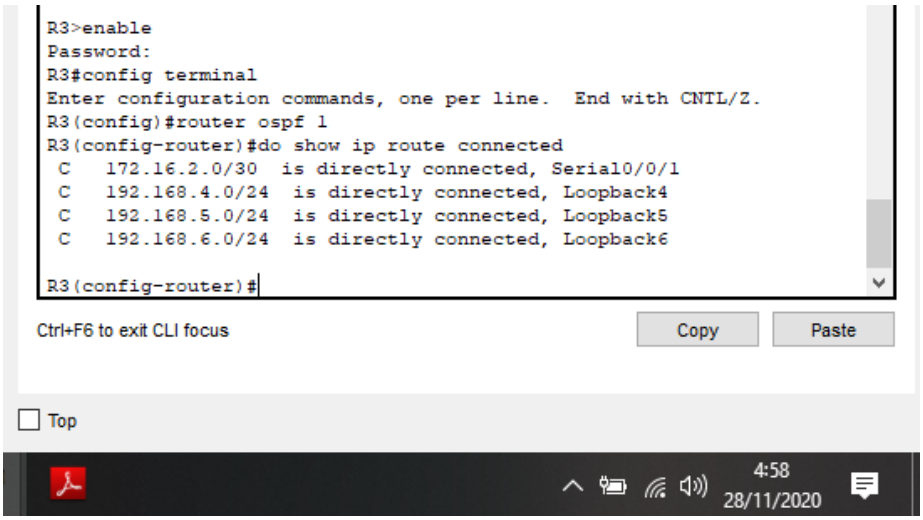
4.3 Configurar OSPF en el R3

En la **Tabla 25** se observar los comandos que se utilizaron para configurar el protocolo OSPF, donde se configura OSPF área 0, se realiza el anuncio de las redes conectadas directamente, se establecen todas las interfaces LAN (loopback) como pasivas y para culminar se desactiva la sumarización automática

Tabla 24. Tabla de configuracion OSPF en R3

Elemento o tarea de configuración	**Especificación**
Configurar OSPF área 0	R3(config)#router ospf 1 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
Anunciar redes IPv4 conectadas directamente	R3(config-router)#do show ip route connected C 172.16.2.0/30 is directly connected, Serial0/0/1 C 192.168.4.0/24 is directly connected, Loopback4 C 192.168.5.0/24 is directly connected, Loopback5 C 192.168.6.0/24 is directly connected, Loopback6
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	R3(config-router)#passive-interface loopback 4 R3(config-router)#passive-interface loopback 5 R3(config-router)#passive-interface loopback 6
Desactive la sumarización automática.	R1(config-router)#no auto-summary

Figura 44. Anunciar las redes conectadas directamente en R3



Fuente: Autor

En la **figura 44** se evidencia cuales son las redes que estan conectadas directamente una vez aplicado el procolo OSPF en R3

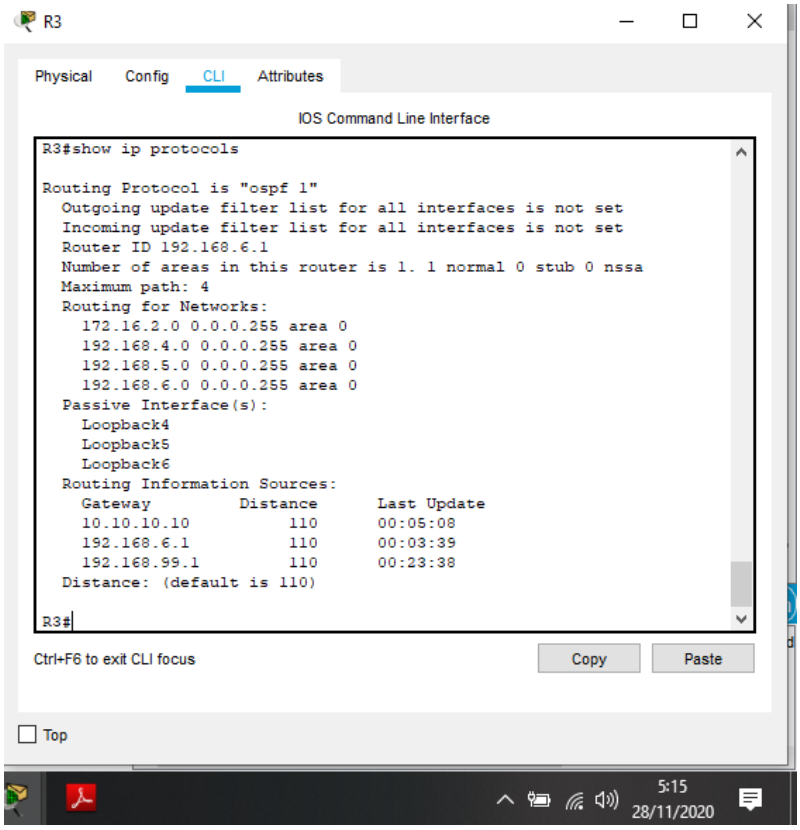
4.5 Verificar la información de OSPF

En la **Tabla 26** se muesra los comandos que se usaron para mostrar la ID del proceso OSPF, la del Router, las redes routing, lo mismo que las interfaces pasivas configuradas, después se la manera como se visualizan las rutas y la configuración de ejecucioln del protocolo

Tabla 25. Verificar la informacion de OSPF

Pregunta	**Respuesta**
¿Con qué comando se muestran la ID del proceso OSPF, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router?	Show ip protocols
¿Qué comando muestra solo las rutas OSPF?	show ip route ospf 1
¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	R3#show run | section router ospf 1

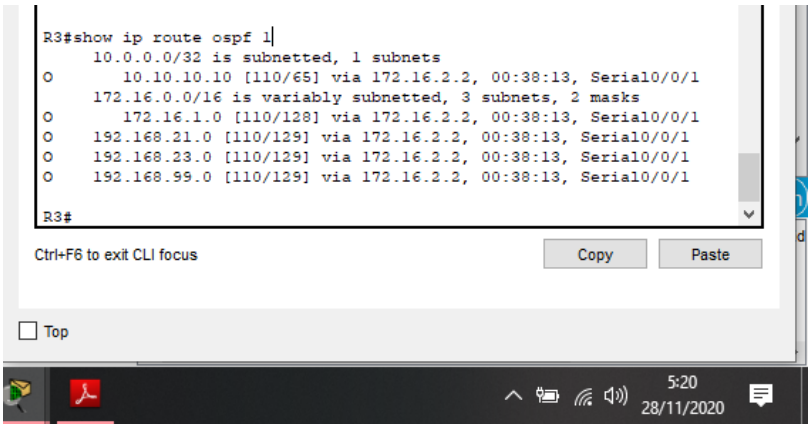
Figura 45. ID del proceso OSPF, la ID del router, las redes de routing y las interfaces pasivas configuradas en R3



Fuente: Autor

Como se muestra en la **figura 45** se aplico el comando descrito en la tabla 24 para mostrar la ID del proceso OSPF, la ID del router, las redes de routing y las interfaces pasivas configuradas en R3

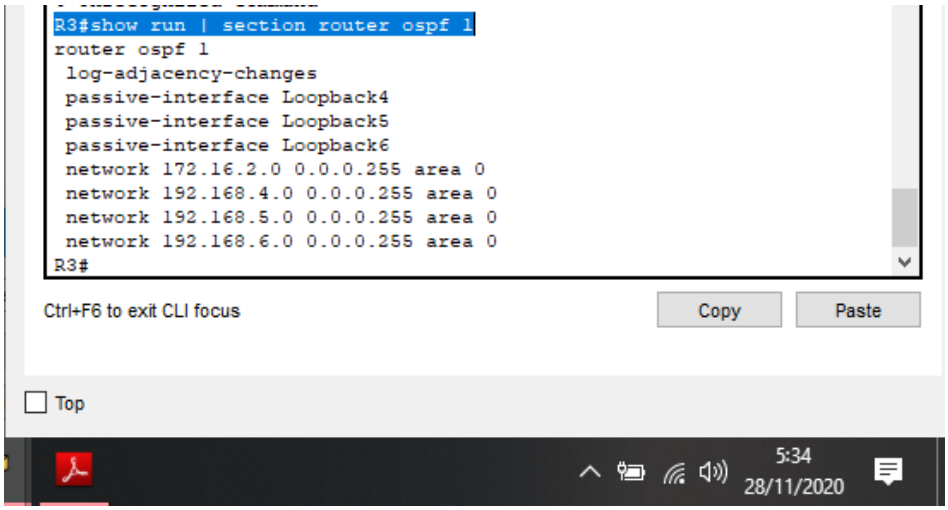
Figura 46. Muestra de las rutas OSPF en R3



Fuente: Autor

Como se muestra en la **figura 46** se aplico el comando descrito en la **tabla 24**, para mostrar las rutas OSPF en R3

Figura 47. Muestra la sección de OSPF de la configuración en ejecución de R3



Fuente: Autor

Como se muestra en la **figura 47** se aplico el comando descrito en la **tabla 24**, para mostrar la sección de OSPF de la configuración en ejecución de R3

Parte 5: Implementar DHCP y NAT para IPv4

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

Las tareas de configuración para R1 mostradas en la **Tabla 27** con sus comandos que incluyen reservar las primeras 20 direcciones IP en la VLAN 21 y 23 y por ultimo crear un pool de DHCP para la VLAN 21 y 23

Tabla 26. Configuracion de R1 como servidor DCHP para vlan21 y 23

Elemento o tarea de configuración	**Especificación**
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20

Crear un pool de DHCP para la VLAN 21.	R1(config)#ip dhcp pool ACCT R1(dhcp-config)#network 192.168.21.0 255.255.255.0 R1(dhcp-config)#default-router 192.168.21.1 R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccnasa.com
Crear un pool de DHCP para la VLAN 23	R1(dhcp-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

5.2 Configurar la NAT estática y dinámica en el R2

En la **Tabla 28** con los comandos mostrados para R2 se crea una base de datos local con una cuenta de usuario, se habilita el servicio del servidor HTTP, para utilizar la base de datos local para la autenticación, después se crea una NAT estática al servidor web y se le asigna la interfaz interna y externa para la NAT estática, mas adelante se configura la NAT dinámica dentro de una ACL privada, trabajando desopues la definición del pool de direcciones IP públicas utilizables y la traducción de NAT dinámica

Tabla 27. Configuracion NAT estatica y dinamica en R2

Elemento o tarea de configuración	**Especificación**
Crear una base de datos local con una cuenta de usuario	R2(config)#username webuser privilege 15 secret cisco12345
Habilitar el servicio del servidor HTTP	R2(config)#ip http server
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	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

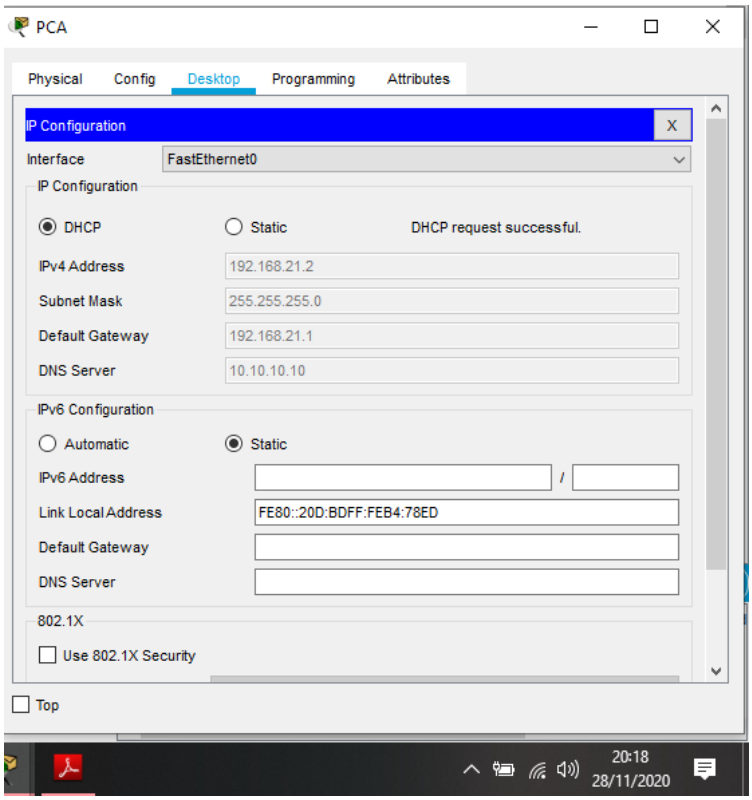
Asignar la interfaz interna y externa para la NAT estática	R2(config)#int g0/0 R2(config-if)#ip nat outside R2(config-if)#int s0/0/0 R2(config-if)#ip nat inside R2(config-if)#int s0/0/1 R2(config-if)#ip nat inside
Configurar la NAT dinámica dentro de una ACL privada	R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255
Defina el pool de direcciones IP públicas utilizables.	R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248
Definir la traducción de NAT dinámica	R2(config)#ip nat inside source list 1 pool INTERNET

Tabla 28. Verificacion del protocolo DHCP y la NAT estatica

En esta **Tabla 29** se puede mostra los resultados una vez configurados el protocolo DCHP y la NAT estatica

Prueba	**Resultados**
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	Exitoso el equipo tomo la dirección 192.168.21.2, observar figura 48
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	Exitoso el equipo tomo la dirección 192.168.23.21, observar figura 49
Verificar que la PC-A pueda hacer ping a la PC-C	Exitoso
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	No fue posible Iniciar sesión

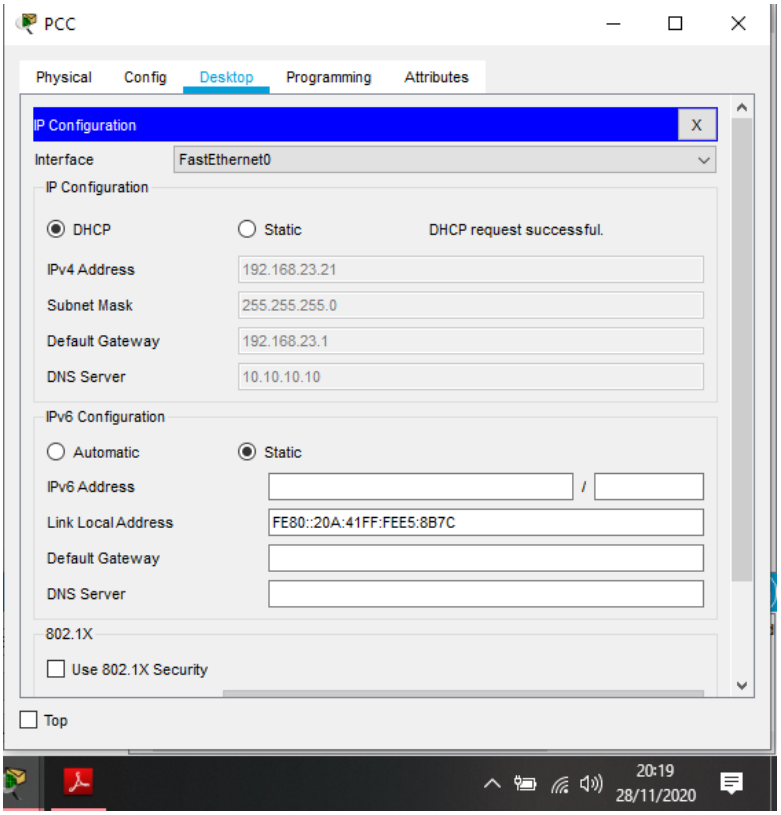
Figura 48. Verificacion que PCA haya adquirido la IP del DHCP



Fuente: Autor

Teniendo en cuenta lo que se observa en la **figura 48** despues de la aplicación del protocolo DCHP, PCA haya adquirido la IP del DHCP

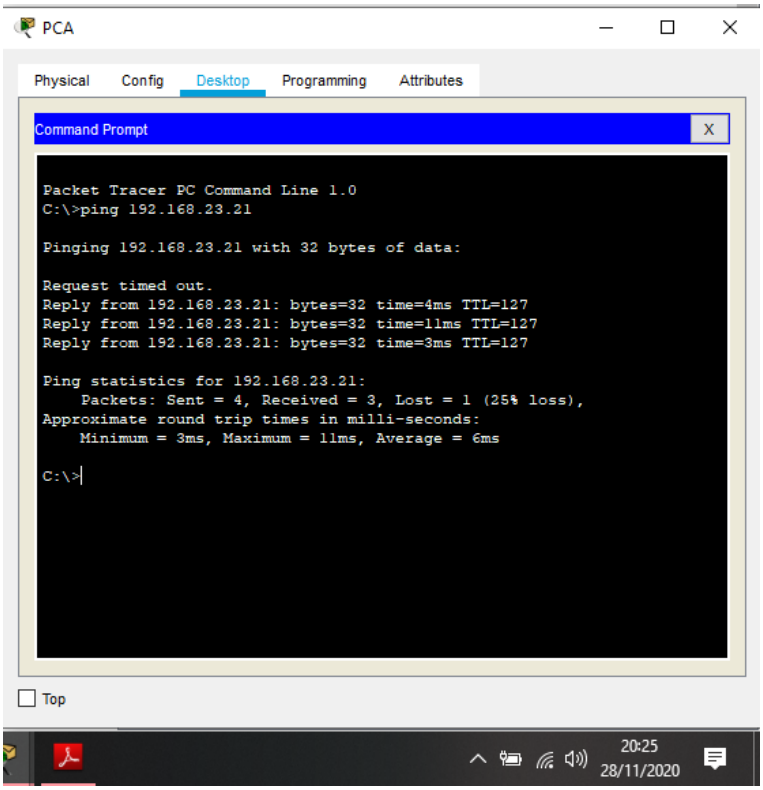
Figura 49. Verificacion que PCC haya adquirido la IP del DHCP



Fuente: Autor

Teniendo en cuenta lo que se observa en la **figura 49** despues de la aplicación del protocolo DCHP, PCC haya adquirido la IP del DHCP

Figura 50. Ping de PCA a PCC



Fuente: Autor

En la **figura 50** se puede visualizar que se ejecuto un ping desde PCA a PCC y este fue exitoso.

Parte 6: Configurar NTP

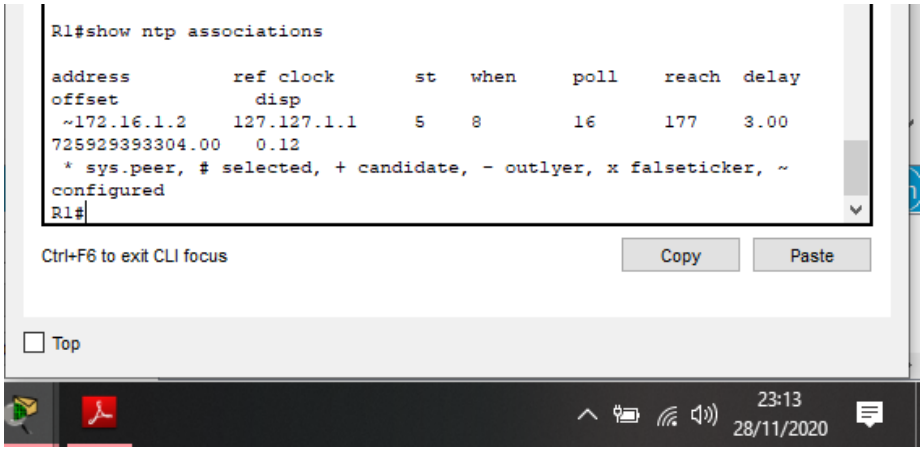
En la siguiente **Tabla 30** se evidencian los comandos que se usaron para el ajuste de la fecha y hora en R2.configurar R2 como un maestro del protoclo NTP, R1 como un cliente NTP y después configurar R1 para actualizaciones de calendario periódicas con hora NTP y all final se verifico la configuración de NTP en R1.

Tabla 29 - tabla de configuracion de NTP

Elemento o tarea de configuración	**Especificación**
Ajuste la fecha y hora en R2.	R2#clock set 09:00:00 05 mar 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 associations

Figura 51. Verificacion de la configuracion NTP en R1



Fuente: Autor

Una vez que se hizo la configuracion del protocolo NTP en R1 en la presente **figura 51** se verifica, aplicando el comando *show ntp associations.*

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

7.1 Restringir el acceso a las líneas VTY en el R2

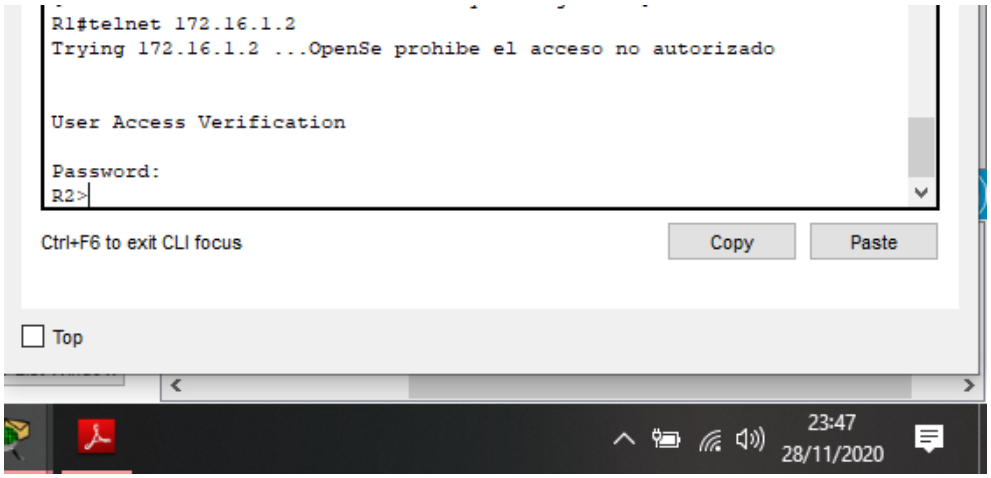
A continuación en la **Tabla 31** con los comando allí descritos se Configura una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2, además se aplica la ACL con nombre a las líneas VTY y se permite el acceso por Telnet a estas líneas y por ultimo se verifica que la ACL funcione como se espera

Tabla 30 - restringir el acceso a las lineas VTY en el R2

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

Permitir acceso por Telnet a las líneas de VTY	R2(config-line)#transport input telnet
Verificar que la ACL funcione como se espera	R1#telnet 172.16.1.2 Trying 172.16.1.2 ...OpenSe prohibe el acceso no autorizado User Access Verification Password: R2>

Figura 52. Verificacion de la ACL en R1



Fuente: Autor

En la **figura 52** se hace la verificación que las listas de control de acceso ACL fuenron aplicadas en R1

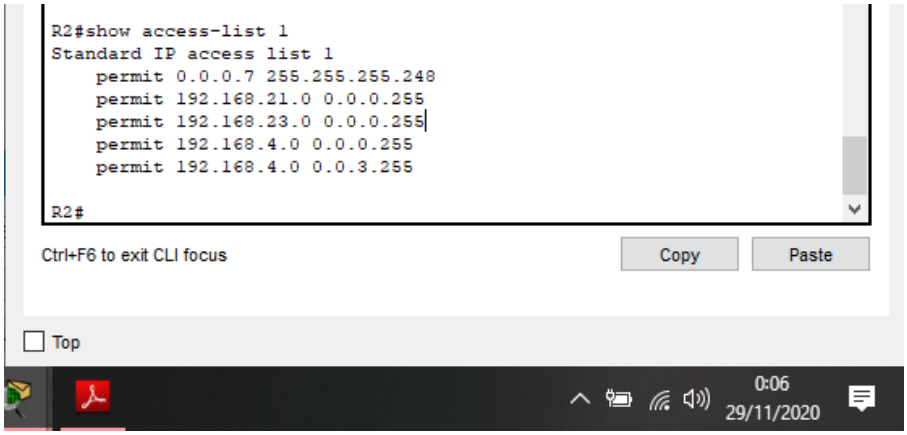
7.2 Introducir el comando de CLI adecuado que se necesita para mostrar lo indicado en la tabla

En la **Tabla 32** con los comandos allí determinados se muestra las coincidencias recibidas por una lista de acceso desde la última vez que se restableció, igualmente se restablecen los contadores de una lista de acceso, tambien se muestra qué ACL se aplica a una interfaz y la dirección en que se aplica, tambien con qué comando se muestran las traducciones NAT y lo que se usa para eliminar las traducciones de NAT dinámicas

Tabla 31 - Tabla de comandos para visulizar aspectos de R2

Descripción del comando	**Entrada del estudiante (comando)**
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	R2#show access-list 1 Standard IP access list 1 permit 0.0.0.7 255.255.255.248 permit 192.168.21.0 0.0.0.255 permit 192.168.23.0 0.0.0.255 permit 192.168.4.0 0.0.0.255 permit 192.168.4.0 0.0.3.255
Restablecer los contadores de una lista de acceso	R2#clear access-list counters
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	R2#show ip interface
¿Con qué comando se muestran las traducciones NAT?	R2#show ip nat translations
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	R2#clear ip nat translation

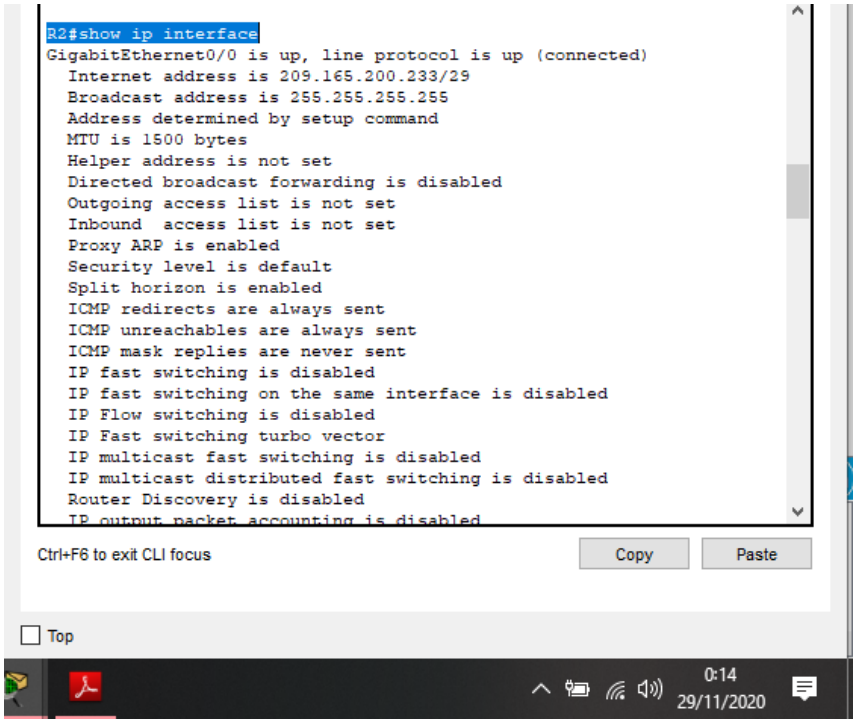
Figura 53. Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció



Fuente: Autor

En la **figura 53** se muestra las coincidencias recibidas por una lista de acceso desde la última vez que se restableció en R2.

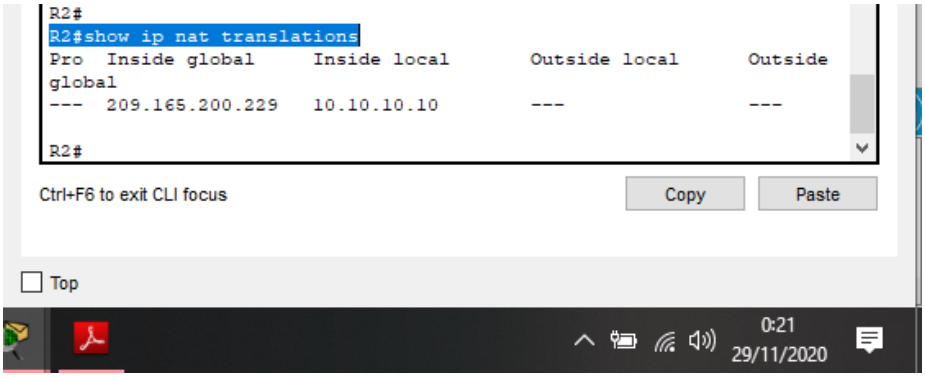
Figura 54. Comando que se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica



Fuente: Autor

Utilizando el comando show ip interface podemos visualizar en la **figura 54** las listas de control de acceso que se aplicaron a una interfaz y la dirección en que se aplico

Figura 55. Muestran las traducciones NAT



Fuente: Autor

En la **figura 55** se pueden visualizar las traducciones NAT en R2

CONCLUSIONES

Teniendo en cuenta lo desarrollado en los 2 escenarios, se pudo profundizar en las diferentes temáticas que se plantearon a lo largo del Diplomado, como todo lo refente con el direccionamiento IPv6 e IPv4, enrutamiento, la aplicación de los diferentes protocolos como OSPF, TCP/IP y DHCP, en los diferentes router y switch de los casos presentados en la prueba de habilidades.

En lo que respecta a la aplicación del protocolo OSPF pudimos darnos cuenta la idoniedad de este para calcular y establecer la ruta más idónea entre dos host que deseen comunicarse.

En los 2 escenarios se tuvo la oportunidad de trabajar igualmente con el protocolo DHCP, permitiendo que los dispositivos configurados con este, pudieran configurarse automanticamente sobre todo en la asignación del direccionamiento IP

De igual manera se observa que la implementación de direcciones de redes dinámicas y estáticas (NAT) permite comunicar redes distintas transportando información mediante paquetes a través del Router, ademas que por medio de comandos como “Ping” se puede verificar el estado de conectividad entre dispositivos y en el que se verifica si existe problemas de red o no y así solucionar la conectividad.

BIBLIOGRAFIA

CISCO. (2019). Routing Estático. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#2

CISCO. (2019). Conceptos de Routing. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#1

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

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

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

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

ANEXOS

ESCENARIO 1

https://drive.google.com/file/d/121wBfgdgpY1HvFXISw_CyAPpDldfuwYS/view?usp=sharing

ESCENARIO 2

https://drive.google.com/file/d/1kS3bqAnFo3p5mrbPPFa4FsNz5AXbDIet/view?usp=sharing

ARTICULO CIENTIFICO

https://drive.google.com/file/d/1KEdolrdPgYx3IBNc0nqOmmEx-ra64XkU/view?usp=sharing

SUSTENTACION

https://youtu.be/uAR1t2i94tI

SOLUCION DE CASO DE ESTUDIO BAJO LA TECNOLGIA CISCO

Giovany Adrian Orozco Caviedes
Universidad Abierta y a distancia – UNAD, gaorozcoc@unadvirtual.edu.co

RESUMEN

El presente artículo presenta el estudio de un caso bajo tecnología CISCO, donde se muestra un escenario de una red pequeña. Se configuraron los router, switches y resto de dispositivos con los parámetros básicos como, nombres, direccionamiento en las interfaces, contraseñas de seguridad en exec privilegiado, consola y telnet, después de estos procesos antes mencionados y ampliados en el artículo, se procede a configurar la seguridad del switch, las VLAN y el routing entre VLAN, se hace la verificación de la conectividad de la red; mas adelante se hace la configuración del protocolo de routing dinámico OSPF en los Router 1 y 2, seguidamente se hace la implementación del protocolo de configuración de host dinámicos DHCP, junto con la implementación de direcciones de red dinámicas y estáticas NAT, a continuación se trabaja el protocolo de tiempo real NTP cliente/servidor, finalizando el artículo se trabajaran las listas de ACL y se muestran los comandos para visualizar algunos aspectos en el Router 2.

Palabras Claves: *cliente/servidor, direccionamiento, interfaces, protocolos.*

ABSTRACT

This article presents a case study under CISCO technology, where a small network scenario is shown. The routers, switches and other devices were configured with the basic parameters such as names, addressing in the interfaces, security passwords in privileged exec, console and telnet, after these processes mentioned above and expanded in the article, we proceed to configure switch security, VLANs and inter-VLAN routing, network connectivity verification is done; Later, the configuration of the dynamic OSPF routing protocol is made in Routers 1 and 2, then the implementation of the dynamic DHCP host configuration protocol is done, along with the implementation of dynamic and static NAT network addresses, then we work the real-time protocol NTP client / server, at the end of the article, the ACL lists will be worked and the commands to display some aspects on Router 2 will be shown.

Keywords: *client/server, addressing, interfaces, protocols.*

I. INTRODUCCION

El objetivo del presente artículo que hace parte de los trabajos del diplomado de profundización de CISCO (Diseño e implementación de soluciones integradas LAN/WAN) es mostrar los resultados de una de las pruebas de habilidades prácticas, esta prueba consta de 2 escenarios con sus respectivas topologías, en la primera se hace énfasis en todo lo correspondiente al enrutamiento entre VLAN, DHCP, Etherchannel y port-security, el segundo escenario hace énfasis en el uso de los protocolos OSPF, NTP, DHCP, también de las listas del control de acceso ACL y la traducción de direcciones de red dinámicas y estáticas (NAT).

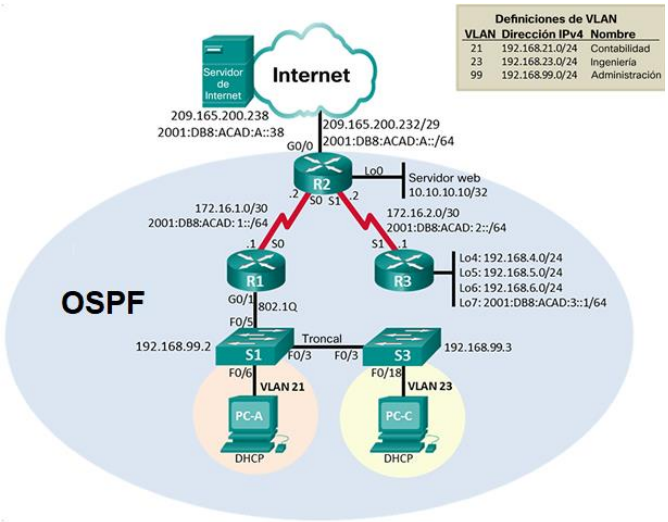
En este documento se mostraran las configuraciones, pruebas y resultados que hacen parte del escenario 2, donde inicialmente se configuran los dispositivos como los router, switches sin antes eliminar los archivos de configuración de inicio y volver a cargarlos todos, en la prueba se trabajara el enrutamiento VLAN que es el proceso reenviar el tráfico de red de una VLAN a otra VLAN. También el protocolo de routing dinámico OSPF, este se usa para encaminamiento jerárquico de pasarela interior o Interior Gateway Protocol (IGP), que usa el algoritmo SmoothWall Dijkstra enlace-estado (Link State Advertisement, LSA) para calcular la ruta idónea entre dos nodos cualesquiera de un sistema autónomo. El protocolo de configuración de host dinámica DCHP, permite a un host obtener una dirección IP de forma dinámica cuando se conecta a la red, elige una dirección de un rango de direcciones configurado llamado “pool” y la asigna al host por un período establecido. El protocolo NTP se usa para sincronizar los relojes de los sistemas de computación de las redes de datos conmutadas por paquetes de latencia variable. Una ACL es una serie de comandos del IOS que

controlan si un router reenvía o descarta paquetes según la información que se encuentra en el encabezado del paquete. Para finalizar mientras que la NAT estática proporciona una asignación permanente entre una dirección local interna y una dirección global interna, la NAT dinámica permite la asignación automática de direcciones locales internas a direcciones globales internas.

II. METODOLOGIA

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 1. Escenario



1. Configurar los parámetros básicos de los dispositivos

1.1Configurar la computadora de internet

Dentro de las tareas de configuración del servidor de internet se establecen las siguientes estipuladas en la **Tabla I**:

Tabla I. Configuración de la PC 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	209.165.200.225
Dirección IPv6/subred	2001:DB8:ACAD:A::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:2::1

1.2 Configuracion de Router 1, 2 y 3 (R1) - (R2) - (R3)

Dentro de los procesos de configuración de estos dispositivos se establecen las siguientes tareas con sus comandos respectivos a su lado tomando como referencia lo establecido en la **tabla II**:

Tabla II. Configuración de R1

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R1
Contraseña de exec privilegiado cifrada	R1(config)#enable secret class
Contraseña de acceso a la consola	R1(config)#line console 0 R1(config-line)#password cisco R1(config-line)#login
Contraseña de acceso Telnet	R1(config-line)#line vty 0 15 R1(config-line)#password cisco R1(config-line)#login
Cifrar las contraseñas de texto no cifrado	R1(config-line)#service passwordencryption
Mensaje MOTD	R1(config)#banner motd %Se prohíbe el acceso no autorizado.%
Interfaz S0/0/0	R1(config)#int s0/0/0 R1(config-if)#ip address 172.16.1.1 255.255.255.252 R1(config-if)#ipv6 address 2001:db8:acad:1::1/64 R1(config-if)#clock rate 128000 R1(config-if)#no shutdown R1(config-if)#exit
Rutas predeterminadas	R1(config)#ipv6 route ::/0 s0/0/0 R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0

Los Router 2 y 3 se hace el proceso de configuración siguiendo los mismos procesos mencionados en la **Tabla II**, pero se tiene en cuenta que el paso donde está la asignación de las interfaces se toma la S0/0/0, S0/0/1, G0/0 para R2 y S0/0/1, loopback 4 – 7 para R3, le son asignadas las direcciones establecidas en la topología que se visualiza en la **Figura 1**

1.2 Configuración de los Switches 1 y 3 (S1) - (S3)
Dentro de las tareas de configuración de estos dispositivos se establecen las siguientes tareas con sus comandos respectivos a su lado, evidenciados en la **Tabla III**:

Tabla III. Configuración de S1

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

El Switch 3 se configura teniendo en cuenta los procesos estipulados en la **Tabla III**, generando cambio solamente en el nombre del Host

2. Configurar la seguridad del switch, las VLAN y el routing entre VLAN
2.1 Configuracion de los switches 1 y 3
Se establecen las siguientes tareas con sus comandos respectivos al frente según lo indicado en las **tablas IV** y **V**

Tabla IV. Configuración de seguridad, VLAN y routing de S1

Elemento o tarea de configuración	**Especificación**
Crear la base de datos de VLAN	S1#configure terminal S1(config)#vlan 21 S1(config-vlan)#name Contabilidad S1(config-vlan)#vlan 23 S1(config-vlan)#name Ingenieria S1(config-vlan)#vlan 99 S1(config-vlan)#name Administracion
Asignar la dirección IP de administración.	S1#configure terminal S1(config)#int vlan 99 S1(config-if)#ip address 192.168.99.2 255.255.255.0 S1(config-if)#no shutdown
Asignar el gateway predeterminado	S1(config)#ip 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	S1(config-if)#int f0/3 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1
Forzar el enlace troncal en la interfaz F0/5	S1(config-if)#int f0/5 S1(config-if)#switchport mode trunk 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, f0/7-24, g0/1-2 S1(config-if-range)#switchport mode access
Asignar F0/6 a la VLAN 21	S1#configure terminal S1(config-if-range)#int f0/6 S1(config-if)#switchport access vlan 21
Apagar todos los puertos sin usar	S1(config-if-range)#int range f0/1-2, f0/4, f0/7-24, g0/1-2 S1(config-if-range)#shutdown

Tabla V. Configuración de seguridad, VLAN y routing de S3

Elemento o tarea de configuración	**Especificación**
Crear la base de datos de VLAN	Aquí se asignan las mismas base de datos de la **tabla IV**
Asignar la dirección IP de administración	S3#configure terminal S3(config)#int vlan 99 S3(config-if)#ip address 192.168.99.3 255.255.255.0 S3(config-if)#no shutdown
Asignar el gateway predeterminado.	S3#configure terminal S3(config)#ip default-gateway192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	S3#configure terminal S3(config)#int f0/3 S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	S3(config-if)#int range f0/1-2, f0/4-17, f0/19-24, g0/1-2 S3(config-if-range)#switchport mode access

Asignar F0/18 a la VLAN 23	S1#configure terminal S1(config-if-range)#int f0/18 S1(config-if)#switchport access vlan 23
Apagar todos los puertos sin usar	S3(config-if)#int range f0/1-2, f0/4-17, f0/19-24, g0/1-2 S3(config-if-range)#shutdown

2.2 Configuración de R1

Se asignaran las respectivas direcciones IP a las diferentes VLAN, teniendo en cuenta las siguientes tareas y comandos según lo establecido en la **tabla VI**:

Tabla VI. Asignación de la direcciones IP a las Vlan

Elemento o tarea de configuración	**Especificación**
Configurar la subinterfaz 802.1Q .21 en G0/1	R1#configure terminal R1(config)#int g0/1.21 R1(config-subif)#description VLAN 21 R1(config-subif)#encapsulation dot1q21 R1(config-subif)#ip address 192.168.21.1 255.255.255.0
Configurar la subinterfaz 802.1Q .23 en G0/1	R1(config-subif)#int g0/1.23 R1(config-subif)#description VLAN 23 R1(config-subif)#encapsulation dot1q23 R1(config-subif)#ip address 192.168.23.1 255.255.255.0
Configurar la subinterfaz 802.1Q .99 en G0/1	R1(config-subif)#description VLAN 99 R1(config-subif)#encapsulation dot1q99 R1(config-subif)#ip address 192.168.99.1 255.255.255.0
Activar la interfaz G0/1	R1(config-subif)#int g0/1 R1(config-if)#no shutdow

3. Configurar el protocolo de routing dinámico OSPF

3.1 Configurar OSPF en el R1, R2 y R3

Las tareas de configuración para R1 incluyen los siguientes procesos, con sus comandos respectivos como se indica en la **tabla VII**

Tabla VII. Tabla de configuración OSPF en R1

Elemento o tarea de configuración	**Especificación**
Configurar OSPF área 0	R1#config terminal Enter configuration commands, one per line. End with CNTL/Z. R1(config)#router ospf 1 R1(config-router)#network 172.16.1.0 0.0.0.255 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
Anunciar las redes conectadas directamente	R1(config-router)#do show ip route connected C 172.16.1.0/30 is directly connected, Serial0/0/0 C 192.168.21.0/24 is directly connected, GigabitEthernet0/1.21 C 192.168.23.0/24 is directly connected, GigabitEthernet0/1.23 C 192.168.99.0/24 is directly connected, GigabitEthernet0/1.99
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

En los Router 2 y 3 las tareas y comandos trabajados son iguales a los mostrados en la **tabla VII**, pero el gran cambio se estipula en las direcciones IP que se ingresan en el paso de configuración OSPF área 0 y además Establecer la interfaz LAN (loopback) como pasiva para cada Router indicado a continuación

R2(config)#router ospf 1
R2(config-router)#passive-interface loopback 0

R3(config-router)#passive-interface loopback 4
R3(config-router)#passive-interface loopback 5
R3(config-router)#passive-interface loopback 6

4. Implementar DHCP y NAT para IPv4

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

Las tareas de configuración para R1 incluyen las siguientes indicadas en la **tabla VIII**

Tabla VIII. Configuración de R1 como servidor DCHP para vlan21 y 23

Elemento o tarea de configuración	**Especificación**

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

4.2 Configurar la NAT estática y dinámica en el R2

La configuración del R2 incluye las siguientes tareas, teniendo en cuenta los procesos indicados en la **tabla IX**

Tabla IX. Configuración 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)#username webuser privilege 15 secret cisco12345
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)#int g0/0 R2(config-if)#ip nat outside R2(config-if)#int s0/0/0 R2(config-if)#ip nat inside R2(config-if)#int s0/0/1 R2(config-if)#ip nat inside
Configurar la NAT dinámica dentro de una ACL privada	R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255
Defina el pool de direcciones IP públicas utilizables.	R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248
Definir la traducción de NAT dinámica	R2(config)#ip nat inside source list 1 pool INTERNET

5. Configurar NTP

Protocolo usado para sincronizar los relojes de los sistemas de computación de las redes de datos conmutadas por paquetes de latencia variable, este proceso se indica en la **tabla X**

Tabla X - tabla de configuración de NTP

Elemento o tarea de configuración	**Especificación**
Ajuste la fecha y hora en R2.	R2#clock set 09:00:00 05 mar 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 associations

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

6.1 Restringir el acceso a las líneas VTY en el R2

Estos procesos se realizan teniendo en cuenta los procesos indicados en la **tabla XI**

Tabla XI - restringir el acceso a las lineas VTY en el R2

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

Permitir acceso por Telnet a las líneas de VTY	R2(config-line)#transport input telnet
Verificar que la ACL funcione como se espera	R1#telnet 172.16.1.2 Trying 172.16.1.2 ...OpenSe prohibe el acceso no autorizado User Access Verification Password: R2>

III. RESULTADOS

Teniendo en cuenta los objetivos planteados en la introducción y confirmados en la metodología se muestran los resultados de la implementación de 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.

Pruebas de la Conectividad de la red.

En esta etapa cuando se configuraron los dispositivos según lo indicado en la **Tabla I, II y III**, se hace la verificación de la conectividad de la red.

Se utiliza el comando ping para probar la conectividad entre los dispositivos de red. Las siguientes figuras **(2, 3 y 4)** verifican metódicamente la conectividad con cada dispositivo de red y al mismo tiempo mostrar los resultados

Figura 2. Prueba de conexión de R1

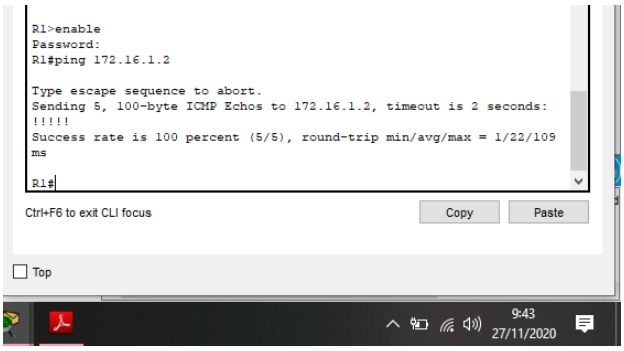


Figura 3. Prueba de conexión de R2

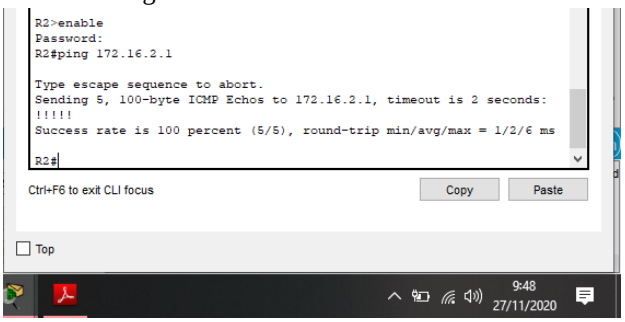
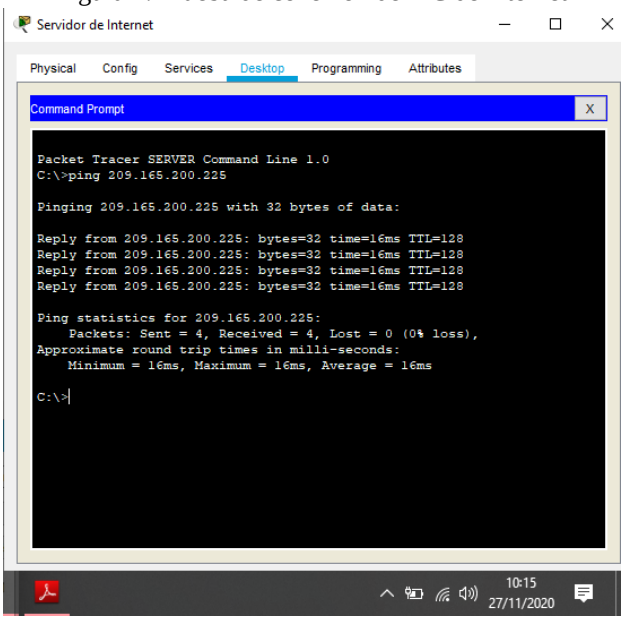


Figura 4. Prueba de conexión del PC de internet



Una vez realizadas las pruebas de configuración inicial de los dispositivos según los pasos indicados anteriormente, a continuación ***verificaremos la seguridad de los switch, las VLAN y Routing entre VLAN***, después de realizar los procesos establecidos en las **Tablas IV, V y VI**.

En este paso se utilizó el comando ping para probar la conectividad entre los switches y el R1 según muestran las **figuras (5, 6, 7 y 8)**

Figura 5. Ping de S1 a R1 por Vlan 99

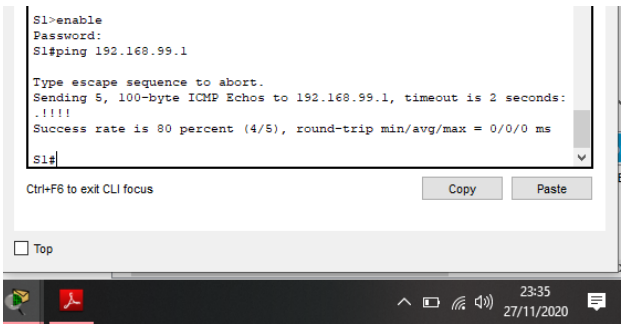


Figura 6. Ping de S3 a R1 por Vlan 99

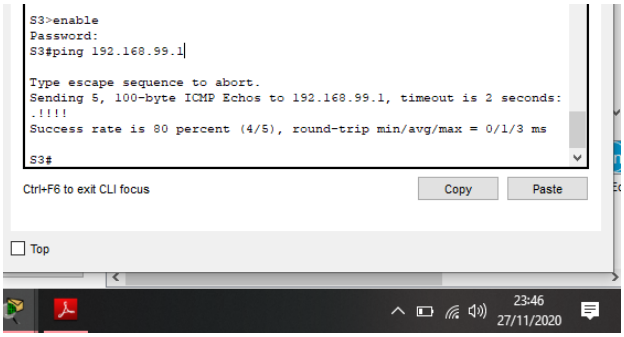


Figura 7. Ping de S1 a R1 por Vlan 21

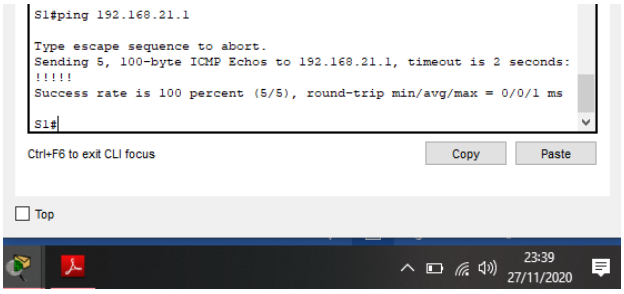
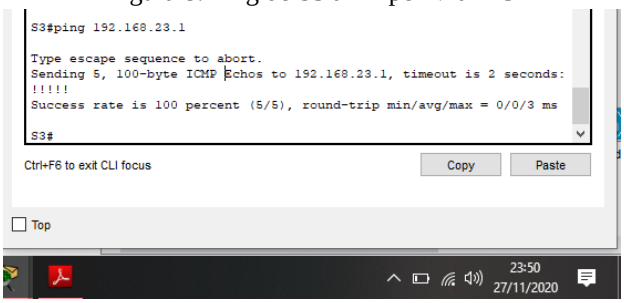


Figura 8. Ping de S3 a R1 por Vlan 23



El siguiente objetivo fue ***configurar el protocolo de routing dinámico OSPF*** que se evidencio en la **tabla VII** con R1 y después siguiendo los pasos con R2 y R3
Se evidencio:

1. La ID del proceso OSPF, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router **(Figura 9)**
2. Las rutas OSPF **(Figura 10)**
3. La sección de OSPF de la configuración en ejecución **(Figura 11)**

Figura 9. ID del proceso OSPF, la ID del router, las redes de routing y las interfaces pasivas configuradas en R3

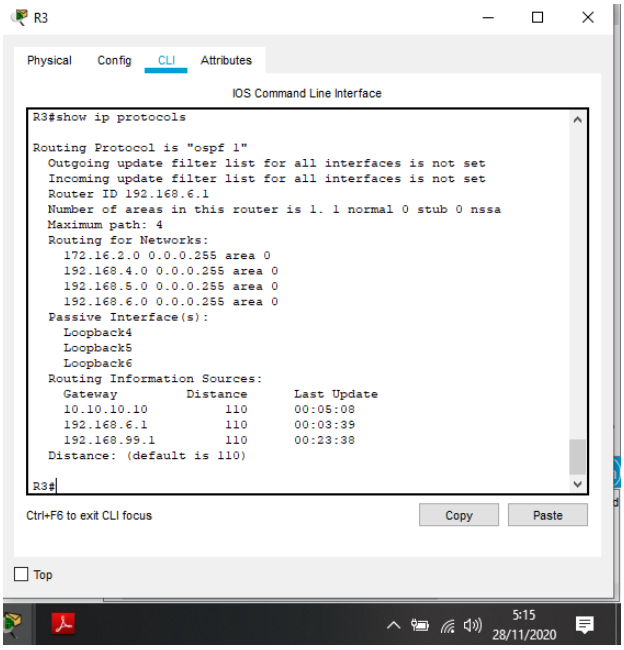


Figura 10. Muestra de las rutas OSPF en R3

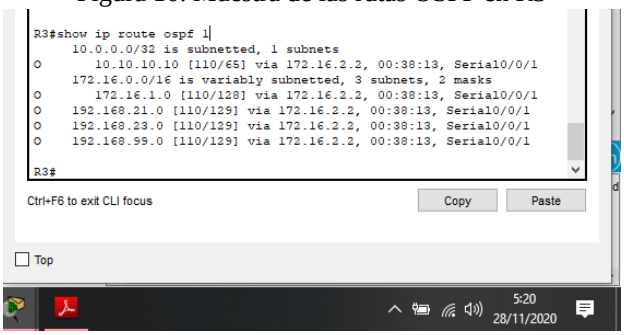
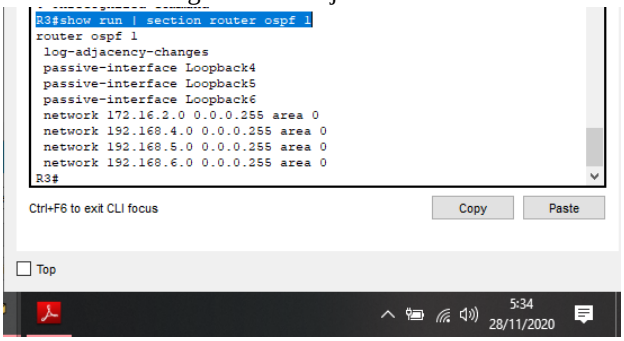


Figura 11. Muestra la sección de OSPF de la configuración en ejecución de R3



A continuación se trabajó la implementación del ***protocolo DCHP en R1***, para colocarlo como servidor de dicho

protocolo para las VLAN 21 y 23 y las configuraciones de ***las NAT estáticas y dinámicas*** para R2 según los pasos dados en las **Tablas VIII y IX** respectivamente.
Los resultados de estos pasos se visualizan a continuación en las **Figuras (12, 13 y 14)**

Figura 12.Verificacion que PCA haya adquirido la IP del DHCP

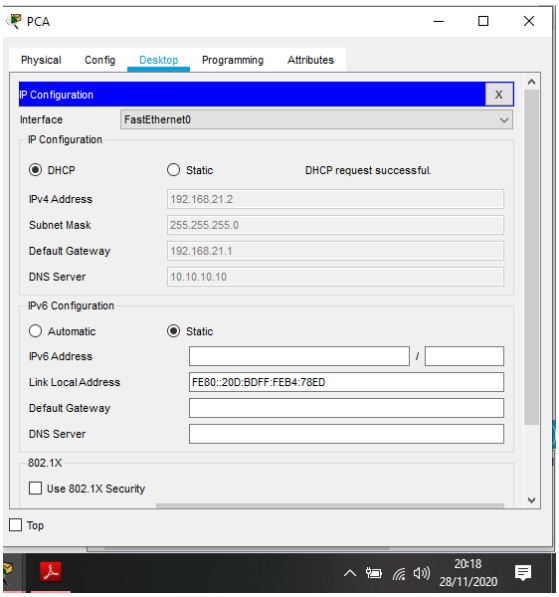


Figura 13. Verificación que PCC haya adquirido la IP del DHCP

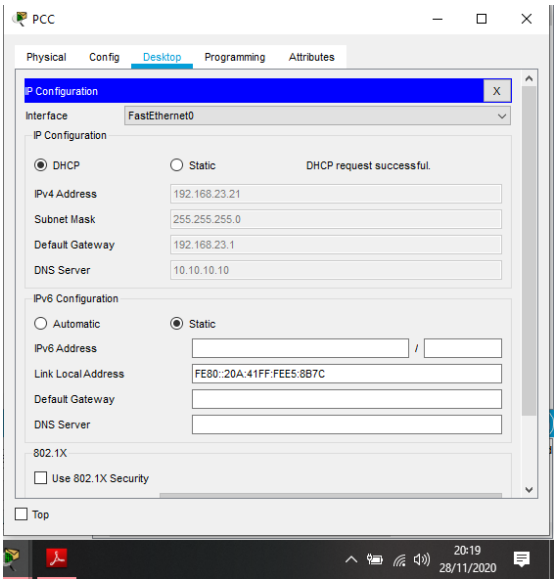
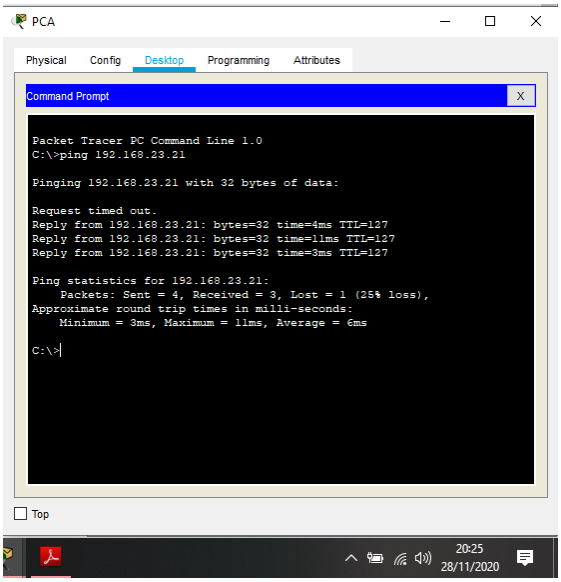
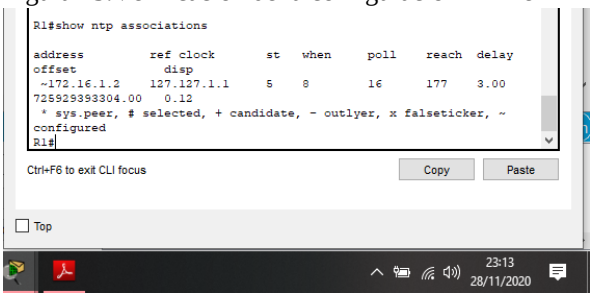


Figura 14. Ping de PCA a PCC



Verificamos ahora la configuración del ***protocolo NTP*** que se estableció en la **Tabla X** y se evidencia en la siguiente **Figura 15**.

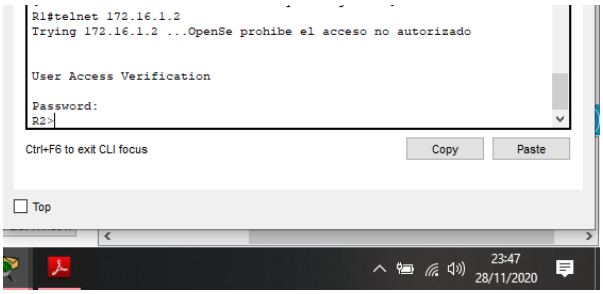
Figura 15.Verificacion de la configuración NTP en R1



Y como último objetivo propuesto en este artículo científico se configuraron las listas de control de acceso (ACL), restringiendo el acceso a las líneas VTY en R2 según se trabajó en la **tabla XI.**

La siguiente **figura 16**, muestra la evidencia

Figura 16.Verificacion de la ACL en R1



IV. CONCLUSIONES

Se puede concluir que observando los resultados de las diferentes pruebas de conectividad se cumplieron los objetivos requeridos con respecto a la configuración plateada del escenario. Se pudo implementar la seguridad de switch y routing entre VLAN, fueron aplicados los protocolos OSPF, DHCP, NTP, además de eso se trabajaron en la topología las listas de control de acceso (ACL) y la traducción de direcciones de redes dinámicas y estáticas (NAT).

V.REFERENCIAS

1. CISCO. (2019). Direccionamiento IP. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#7
2. CISCO. (2019). Routing Estático. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#2
3. UNAD (2017). Configuración de Switches y Routers [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgL9QChD1m9EuGqC
4. CISCO. (2019). Routing Dinámico. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#3
5. UNAD (2017). Principios de Enrutamiento [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgOyjWeh6timi_Tm
6. CISCO. (2019). VLAN. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#6
7. 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
8. CISCO. (2019). DHCP. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#8
9. CISCO. (2019). NAT para IPv4. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#9