SOLUCION DE DOS ESCENARIOS PRESENTES EN ENTORNOS CORPORATIVOS BAJO EL USO DE TECNOLOGIA CISCO

LINA MAYRENA LOPEZ PANCHO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
INGENIERIA DE SISTEMAS
LA PLATA HUILA
2020

SOLUCION DE DOS ESCENARIOS PRESENTES EN ENTORNOS CORPORATIVOS BAJO EL USO DE TECNOLOGIA CISCO

LINA MAYRENA LOPEZ PANCHO

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

DIRECTOR
DIEGO EDINSON RAMIREZ CLAROS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
INGENIERIA DE SISTEMAS
LA PLATA HUILA
2020

NOTA DE ACEPTACIÓN

_____
_____
_____
_____
_____
_____
_____

_____
Firma del Presidente de Jurado

_____
Firma del Jurado

_____
Firma del Jurado

La Plata 15, Diciembre 2020

Tabla de contenido

1. INDICE DE FIGURAS

2. INDICE DE TABLAS

3. INTRODUCCIÓN

Como sabemos en la actualidad las tecnología de la información y las telecomunicaciones se aplican en la mayoría de ámbitos de la vida cotidiana, y todos lo niveles sociales, como administrativos, científicos, educativos, empresariales y familiares lo cual conlleva a tener una excelente calidad de recursos e información, las tecnología mas destacadas en estos momentos la constituyen las redes de transmisión de datos por el cual permiten compartir recursos físicos como información y servicios como es el caso de internet y para ello se requiere de diseño y modelacion de redes, de topologías y la configuración de dispositivos y demás.

Hoy en día las tecnologias y las redes de comunicación son el eje principal de toda organización, puesto que estas permiten un excelente desarrollo y productiva como herramientas de trabajo para el cuerpo de quienes la conforman, pero para ello esta requiera garantizar una excelente implementación completa y eficaz que permita el buen funcionamiento cumpliendo con lo solicitado de quienes la administran.

Para llevar a cabo la solución de los escenarios expuestos haremos uso de Packet Tracert que es una herramienta tipo software que nos permitirá poner en practica el conocimiento teorico que tenemos frente a las redes, diseñando y modelando topologias de estas , donde se configurara cada uno de los dispositivos que la conforman, como router,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, Configurar el protocolo de routing dinámico OSPF
Se verificara la información de OSPF, se Implementara y se verificara el protocolo DHCP y NAT para IPV4, se configurara y verificar las listas de control de acceso (ACL), se Introducira el comando de CLI adecuado y por ultimo se verificara la conexión completa de los dispositivos.

4. OBJETIVO ESPECIFICO

- Modelar y diseñar las topologias de redes de los escenarios expuestos utilizando Packet Tracer.

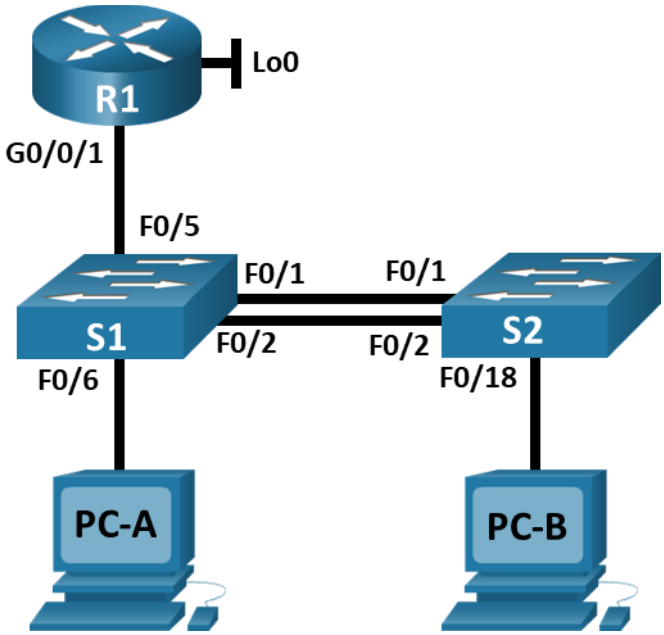
Objetivos Generales

- Inicializar, recargar y configurar aspectos básicos de los dispositivos
- Configurar la estructura de red (VLAN, Truking, EtherChannel)
- Configurar soporte de Host
- Configurar el protocolo de routing dinámico OSPF
- Verificar la información de OSPF
- Implementar y verificar protocolo DHCP y NAT para IPV4
- Configurar y verificar las listas de control de acceso (ACL)
- Introducir el comando de CLI adecuado

5. DESARROLLO

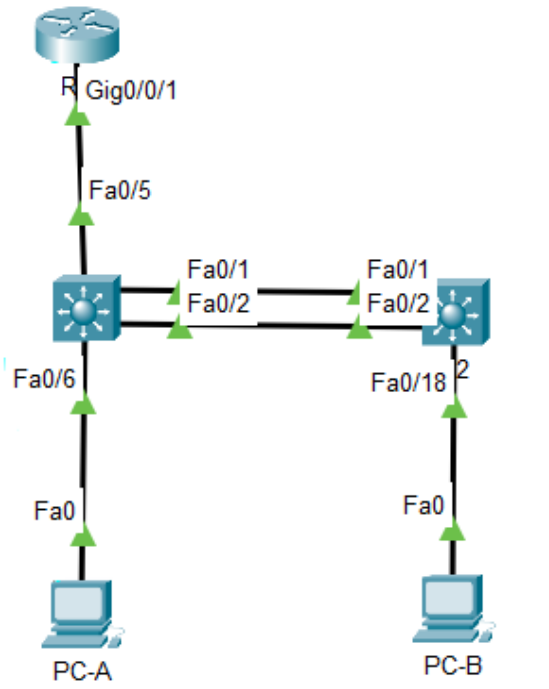
6. ESCENARIO 1

Figura 1: Escenario 1



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

Figura 2: Simulación de Escenario



Fuente: Autor

Tabla 1 - VLAN

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

Tabla 2 - asignación de direcciones

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
R1 G0/0/1.2	10.19.8.1 /26	No corresponde
	2001:db8:acad:a: :1 /64	No corresponde
R1 G0/0/1.3	10.19.8.65 /27	No corresponde
	2001:db8:acad:b: :1 /64	No corresponde
R1 G0/0/1.4	10.19.8.97 /29	No corresponde
	2001:db8:acad:c: :1 /64	No corresponde
R1 G0/0/1.6	No corresponde	No corresponde
R1 Loopback0	209.165.201.1 /27	No corresponde
	2001:db8:acad:209: :1 /64	No corresponde
S1 VLAN 4	10.19.8.98 /29	10.19.8.97
	2001:db8:acad:c: :98 /64	No corresponde
	fe80: :98	No corresponde
S2 VLAN 4	10.19.8.99 /29	10.19.8.97
	2001:db8:acad:c: :99 /64	No corresponde
	fe80: :99	No corresponde
PC-A NIC	Dirección DHCP para IPv4	DHCP para puerta de enlace predeterminada IPv4
	2001:db8:acad:a: :50 /64	fe80::1
PC-B NIC	DHCP para dirección IPv4	DHCP para puerta de enlace predeterminada IPv4
	2001:db8:acad:b: :50 /64	fe80::1

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

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

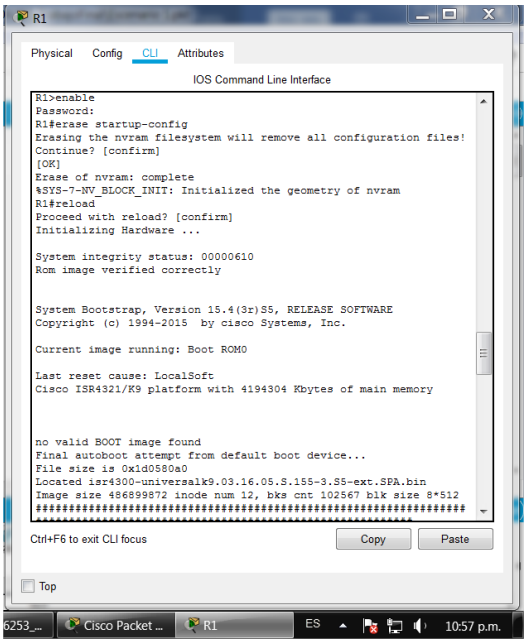
Paso 1: Inicializar y volver a cargar el router y switch

- Borre las configuraciones de inicio y las VLAN del router y del switch y vuelva a cargar los dispositivos.
- Después de recargar el switch, configure la plantilla SDM para que admita IPv6 según sea necesario y vuelva a cargar el switch.
- Antes de continuar, solicite al instructor que verifique la inicialización de los dispositivos.

Tabla 3- Configuración Inicial

Comandos	Especificación
Router>enable Router#erase startup-config Router#reload	Ingreso a modo privilegiado Eliminar configuración de inicio Recargar el equipo
Switch>enable Switch#erase startup-config Switch#delete vlan.dt Swicth#reload	Ingreso a modo privilegiado Eliminar configuración de inicio Eliminar el archivo vlan Recargar el equipo
Switch>enable Switch#config t Switch(config)#sdm prefer dual-ipv4-and-ipv6 default Switch(config)#exit Switch#reload	Ingreso a modo privilegiado Ingreso a modo de configuracion Configuración para que nuestro swicth admita el ipv4 e ipv6 Salir Recargar el equipo para que funcione la configuracion sdm

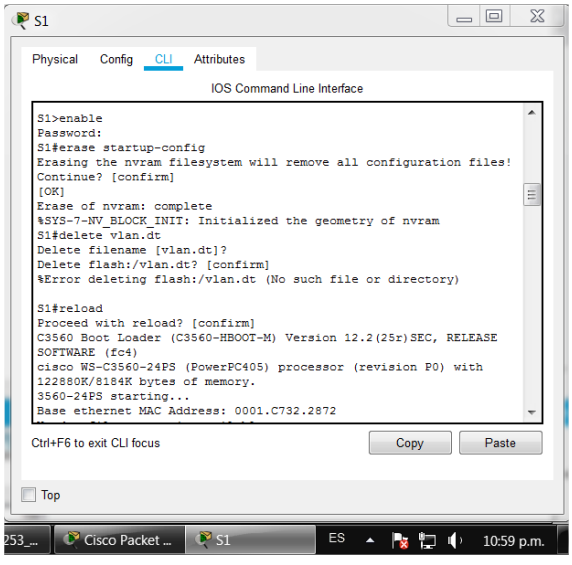
Figura 3: Inicializar y volver a cargar el router



Fuente: Autor

Desde la terminal del PCA- Se borra las configuraciones de inicio y las VLAN del router y se recarga de nuevo.

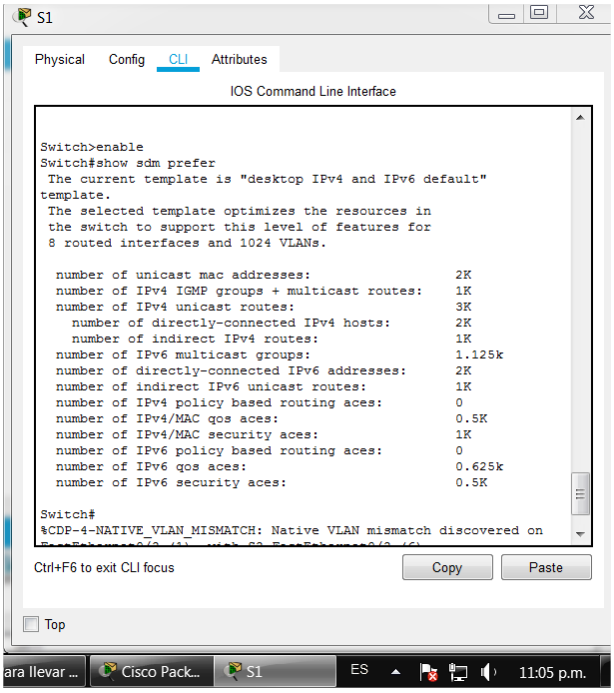
Figura 4: Inicializar y volver a cargar el Switch



Fuente: Autor

Desde la terminal del PCB Se borra las configuraciones de inicio y las VLAN del router y se recarga de nuevo.

Figura 5: show sdm prefer



Fuente: Autor

Se realiza la configuración de la plantilla SDM para que este la admita el IPV6.

Paso 2: Configurar R1

Continuando en la terminal del PC-A proseguimos a la configuración del R1

Tabla 4 - Configurar R1

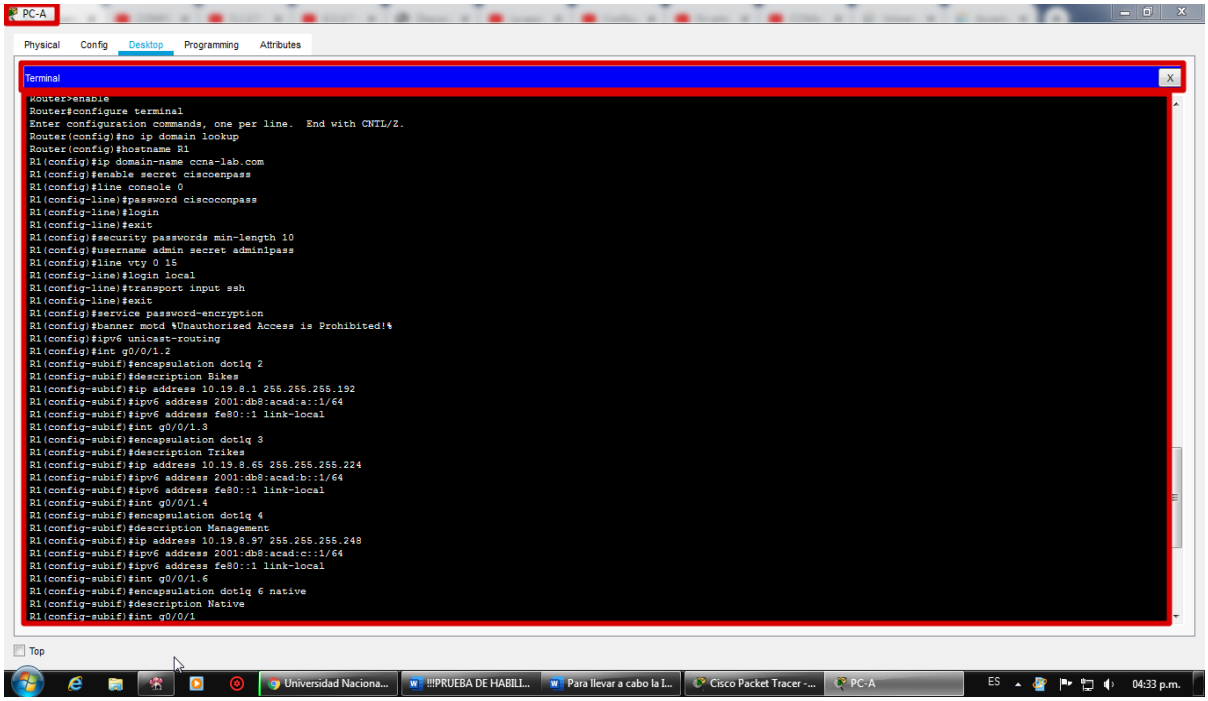
Comandos Utilizados Configuración R1	Especificación
Router>enable Router#configure terminal Router(config)# no ip domain lookup	Ingreso a modo privilegiado Ingreso a modo de configuracion Desactivar la búsqueda DNS
Router(config)# hostname R1	Asignar nombre del router
R1(config)#ip domain-name ccna-lab.com	Asignar el nombre de dominio

Comandos Utilizados Configuración R1	Especificación
R1(config)#enable secret ciscoenpass	Asignar la contraseña cifrada para el modo EXEC privilegiado
R1(config)#line console 0 R1(config-line)#password ciscoconpass R1(config-line)#login R1(config-line)#exit	Ingreso al modo de configuración de la consola Agsinar acceso de consola Contraseña de acceso a la consola Activa autenticación inicio sesion salir
R1(config)#security passwords min-length 10	Instaura los caracteres minimos que debe tener una contraseña
R1(config)#username admin secret admin1pass	crea el usuario administrativo en la base de datos local
R1(config)#line vty 0 15 R1(config-line)#login local	Ingreso a configuracion de telnet Activa autenticación de inicio de sesión en las líneas VTY para que use la base de datos local
R1(config-line)#transport input ssh	Configura acceso remoto
R1(config)#service password-encryption	Cifrado de contraseñas
R1(config)#banner motd %Unauthorized Access is Prohibited!%	Configura mensaje de inicio de sesión, mensaje del día
R1(config)#ipv6 unicast-routing	Habilita la interfaz IPv6 en el router

Comandos Utilizados Configuración R1	Especificación
R1(config)#int g0/0/1.2 R1(config-subif)#encapsulation dot1q 2 R1(config-subif)#description Bikes R1(config-subif)#ip address 10.19.8.1 255.255.255.192 R1(config-subif)#ipv6 address 2001:db8:acad:a::1/64 R1(config-subif)#ipv6 address fe80:1link-local R1(config-)#int g0/0/1.3 R1(config-subif)#encapsulation dot1q 3 R1(config-subif)#description Trikes R1(config-subif)#ip address 10.19.8. 65 255.255.255.224 R1(config-subif)#ipv6 address 2001:db8:acad:b::1/64 R1(config-subif)#ipv6 address fe80:1link-local R1(config)#int g0/0/1.4 R1(config-subif)#encapsulation dot1q 4 R1(config-subif)#description Management R1(config-subif)#ip address 10.19.8.97 255.255.255.248 R1(config-subif)#ipv6 address 2001:db8:acad:c::1/64 R1(config-subif)#ipv6 address fe80:1link-local R1(config)#int g0/0/1.6 R1(config-subif)#encapsulation dot1q 6 native R1(config-subif)#description Native R1(config-subif)#int g0/0/1 R1(sonfig-if)#no shutdown	configura la interfaz G0/0/1 y subinterfaces, tambien permite establecer la dirección IPV4, también la IPV6 como enlace fe:80::1 y activando las mismas, teniendo en cuenta los valores asignados en la tabla de direcciones y vlan.

Comandos Utilizados Configuración R1	Especificación
R1(config-if)#int loopback 0 R1(config-if)#ip address 209.165.201.1 255.255.255.224 R1(config-if)#ipv6 address 2001:db8:acad:209::1/64 R1(config-if)#ipv6 address fe80::1 link-local R1(config-if)#description Internet R1(config-if)#exit	Permite la configuración de la interfaz loopback0, teniendo en cuenta los valores asignados en la tabla de direcciones.
R1(config)#crypto key generate rsa How many bits in the modulus [512]: 1024	Genera una clave de cifrado RSA 1024

Figura 6: Configuracion R1



Fuente: Autor

Se lleva a cabo la configuración del R1, según lo solicitado en la tabla de tareas.

Paso 3: Configurar S1 y S2

Continuando en la terminal del PC-B y proseguimos a la configuración del S1.

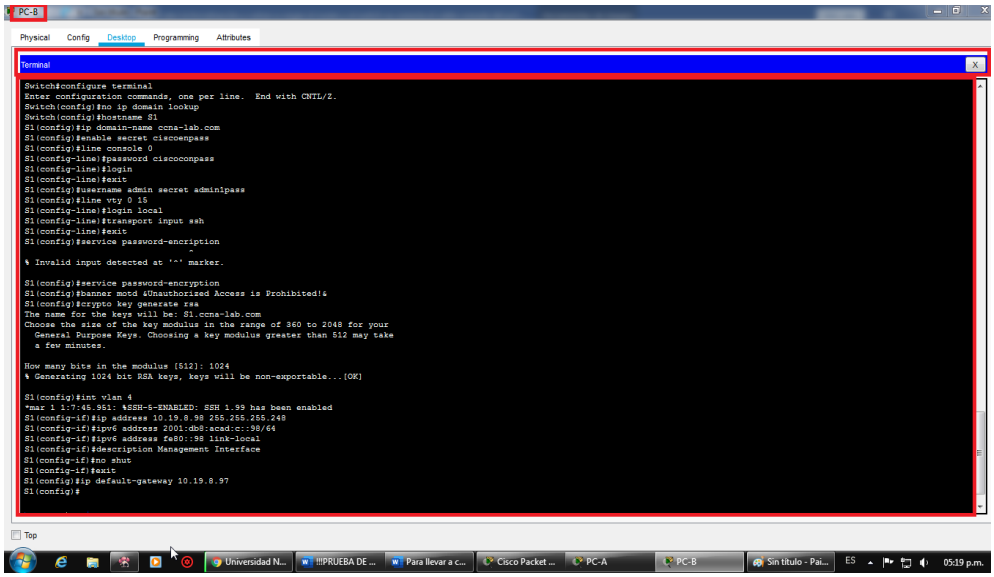
Tabla 5 - Configure S1 y S2

Comando Utilizados Configuración S1	Comandos Utilizados Configuración S2	Especificación
Switch>enable Switch#configure terminal Switch(config)no ip domain	Switch>enable Switch#configure terminal Switch(config)no ip domain	Ingreso a modo privilegiado Ingreso a modo de configuracion Desactivar la búsqueda DNS
Switch(config)#hostname S1	Switch(config)#hostname S2	Asignar nombre del switch
S1(config)#ip domain-name ccna-lab.com	S2(config)#ip domain-name ccna-lab.com	Asignar nombre de dominio
S1(config)#enable secret ciscoenpass	S2(config)#enable secret ciscoenpass	Asignar contraseña cifrada para el modo EXEC privilegiado
S1(config)#line console 0 S1(config-line)#password ciscoconpass S1(config-line)#login S1(config-line)#exit	S2(config)#line console 0 S2(config-line)#password ciscoconpass S2(config-line)#login S2(config-line)#exit	Ingreso al modo de configuración de la consola Agsinar acceso de consola Contraseña de acceso a la consola Activa autenticación inicio sesion salir
S1(config)#username admin secret admin1pass	S2(config)#username admin secret admin1pass	crea un usuario administrativo en la base de datos local

Comando Utilizados Configuración S1	Comandos Utilizados Configuración S2	Especificación
S1(config)#line vty 0 15 S1(config-line)#login local	S2(config)#line vty 0 15 S2(config-line)#login local	Ingreso a configuracion de telnet Activa autenticación de inicio de sesión en las líneas VTY para que use la base de datos local
S1(config-line)#transport input ssh S1(config-line)#exit	S2(config-line)#transport input ssh S2(config-line)#exit	Configura acceso remoto salir
S1(config)#service password-encryption	S2(config)#service password-encryption	Cifrado de contraseñas
S1(config)#banner &Unauthorized Access is Prohibited!&	S2(config)#banner (Unauthorized Access is Prohibited!(	Configura mensaje de inicio de sesión, mensaje del día
S1(config)#crypto key generate rsa How many bits in the modulus [512]: 1024	S2(config)#crypto key generate rsa How many bits in the modulus [512]: 1024	Genera una clave de cifrado RSA 1024

Comando Utilizados Configuración S1	Comandos Utilizados Configuración S2	Especificación
S1(config)#int vlan 4 S1(config-if)#ip address 10.19.8.98 255.255.255.248 S1(config-if)#ipv6 address 2001:db8:acad:c::98/64 S1(config-if)#ipv6 address fe80::98 link-local S1(config-if)#description Management Interface S1(config-if)#no shutdown S1(config-if)#exit	S2(config)#int vlan 4 S2(config-if)#ip address 10.19.8.99 255.255.255.248 S2(config-if)#ipv6 address 2001:db8:acad:c::99/64 S2(config-if)#ipv6 address fe80::99 link-local S2(config-if)#description Management Interface S2(config-if)#no shutdown S2(config-if)#exit	configura la interfaz de administración (SVI), estableciendo dirección IPV4 de capa3, igual la dirección local de enlace IPV6 y su dirección de capa 3, teniendo en cuenta los valores dados en la tabla de direcciones y vlan.
S1(config)#ip default-gateway 19.19.8.97	S2(config)#ip default-gateway 19.19.8.97	Configura la ip Gateway predeterminado dejando la puerta de enlace ipv6 automaticamente, teniendo en cuenta los valores asignados en la tabla de direcciones

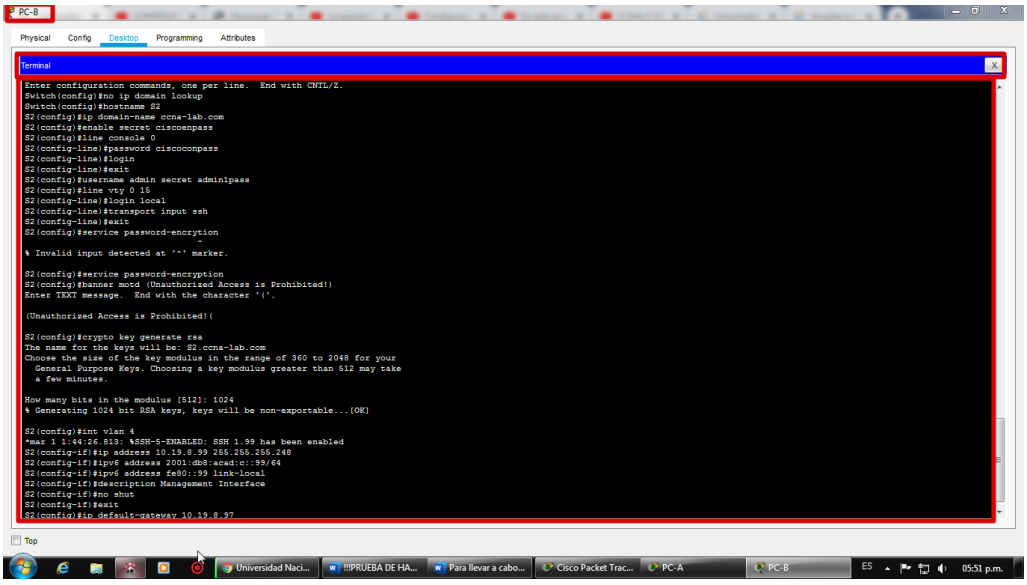
Figura 7: Configuració de S1



Fuente: Autor

Continuando en la terminal del PC-B y proseguimos a la configuración del S1 según lo solicitado en la tabla de tareas.

Figura 8: Configuración del S2



Fuente: Autor

Continuando en la terminal del PC-B y proseguimos a la configuración del S2 según lo solicitado en la tabla de tareas.

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

Paso 1: Configurar S1

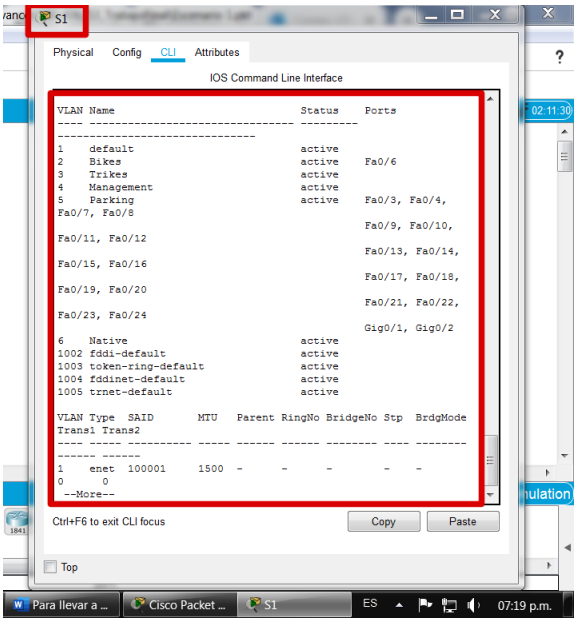
Continuando en la terminal del PC-B y proseguimos a la configuración de la infraestructura de red (VLAN, Trucking, EtherChannel) del S1 según lo solicitado en la tabla de tareas con los siguientes comandos:

Tabla 6 - Configurar S1 infraestructura de red (VLAN, Truking, Etherchannel

Comandos Utilizados Configuración S1	Especificación
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 S1(config-vlan)#exit	permite crear las VLAN en el S1
S1(config)#int f0/5 S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 6 S1(config-if)#int range f0/1-2 S1(config-if-range)#shutdown S1(config-if-range)#switchport trunk encapsulation dot1q S1(config-if-range)#switchport mode trunk S1(config-if-range)#switchport trunk native vlan 6	permite crear los troncos 802.1Q en las interfaces F0/1, F0/2, F0/5 que utilicen la Vlan 6 native, de igual manera se apagan las interfaces F0/1-2 para poder crear el EtherChannel

Comandos Utilizados Configuración S1	Especificación
S1(config-if-range)#channel-group 1 mode active S1(config-if-range)#int port-channel 1 S1(config-if)#switchport trunk encapsulation dotlq S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 6	permite crear un grupo de puertos EtherChannel de capa 2 donde se usa las interfaces F0/1 y F0/2, utilizando protocolos LACP para la negación
S1(config-if)#int F0/6 S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 2	configura el puerto de interfaz F0/6 de acceso de host para VLAN2
S1(config-if)#switchport port-security S1(config-if)#switchport port-security maximum 3	Configura la seguridad del puerto en los puertos de acceso, con solo 3 intentos al ultimo fallido se apagará
S1(config-if)#int range F0/3-4 S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 5 S1(config-if-range)#description Not in Use S1(config-if-range)#shutdown S1(config-if-range)#int range F0/7-24 S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 5 S1(config-if-range)#description Not in Use S1(config-if-range)#shutdown S1(config-if-range)#int range G0/1-2 S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 5 S1(config-if-range)#description Not in Use S1(config-if-range)#shutdown	permite proteger las interfaces que no se encuentran en uso, asignando a VLAN 5 , se establece en modo accesso y agregando una descripción de identificación y se apagara.

Figura 9: Show VLAN S1



Fuente: Autor

En la figura 9 se muestra las VLAN creadas y configuradas en el S1.

Paso 2: Configurar S2

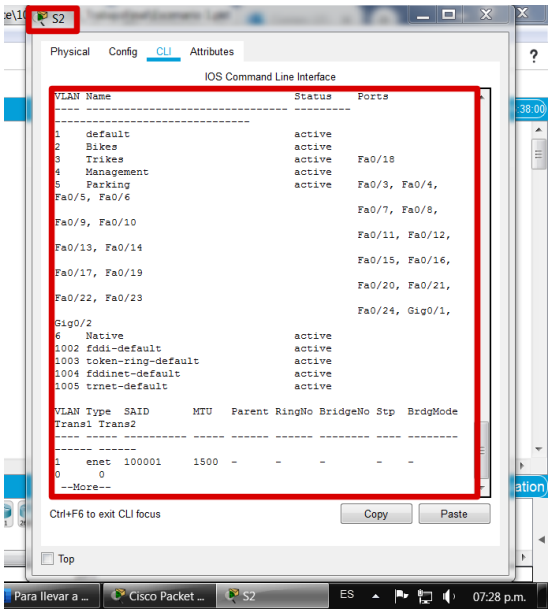
Continuando en la terminal del PC-B y proseguimos a la configuración de la infraestructura de red (VLAN, Trucking, EtherChannel) del S2.

Tabla 7 - Configurar S2 infraestructura de red (VLAN, Truking, Etherchannel

Comandos utilizados Configuración S2	Especificación
S2(config)#vlan 2 S2(config-vlan)#name Bikes S2(config-vlan)#vlan 3 S2(config-vlan)#name Trikes S2(config-vlan)#vlan 4 S2(config-vlan)#name Management S2(config-vlan)#vlan 5 S2(config-vlan)#name Parking S2(config-vlan)#vlan 6 S2(config-vlan)#name Native S2(config-vlan)#exit	permite crear las VLAN en el S2

Comandos utilizados Configuración S2	Especificación
S2(config-if)#int range f0/1-2 S2(config-if-range)#shutdown S2(config-if-range)#switchport trunk encapsulation dot1q S2(config-if-range)#switchport mode trunk S2(config-if-range)#switchport trunk native vlan 6	crea los troncos 802.1Q en las interfaces F0/1, F0/2, que utilicen la Vlan 6 native, de igual manera se apagan las interfaces F0/1-2 para poder crear el EtherChannel
S2(config-if-range)#channel-group 1 mode active S2(config-if-range)#int port-channel 1 S2(config-if)#switchport trunk encapsulation dotlq S2(config-if)#switchport mode trunk S2(config-if)#switchport trunk native vlan 6	crea un grupo de puertos EtherChannel de capa 2 donde se usa las interfaces F0/1 y F0/2, utilizando protocolos LACP para la negación
S2(config-if)#int F0/18 S2(config-if)#switchport mode access S2(config-if)#switchport access vlan 3	configura el puerto de acceso de host para VLAN3
S2(config-if)#switchport port-security S2(config-if)#switchport port-security maximum 3	configura la seguridad del puerto en los puertos de acceso, con solo 3 intentos al ultimo fallido se apagará
S2(config-if)#int range F0/3-17 S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 5 S2(config-if-range)#description Not in Use S2(config-if-range)#shutdown S2(config-if-range)#int range F0/19-24 S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 5 S2(config-if-range)#description Not in Use S2(config-if-range)#shutdown S2(config-if-range)#int range G0/1-2 S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 5 S2(config-if-range)#description Not in Use S2(config-if-range)#shutdown	permite proteger las interfaces que no se encuentran en uso, asignandolas a VLAN 5 , se establece en modo acceso y agregando una descripción de no uso d y se apagara.

Figura 10: Show VLAN S2



Fuente: Autor

En la figura 10 se muestra las VLAN creadas y configuradas en el S1.

Por ultimo se activan las interfaces F0/1 y F0/2, tanto del S1 y el S2 con los siguientes comandos:

S1(config-if-range)#int range F0/1-2
S1(config-if-range)# No shutdown

S2(config-if-range)#int range F0/1-2
S2(config-if-range)# No shutdown

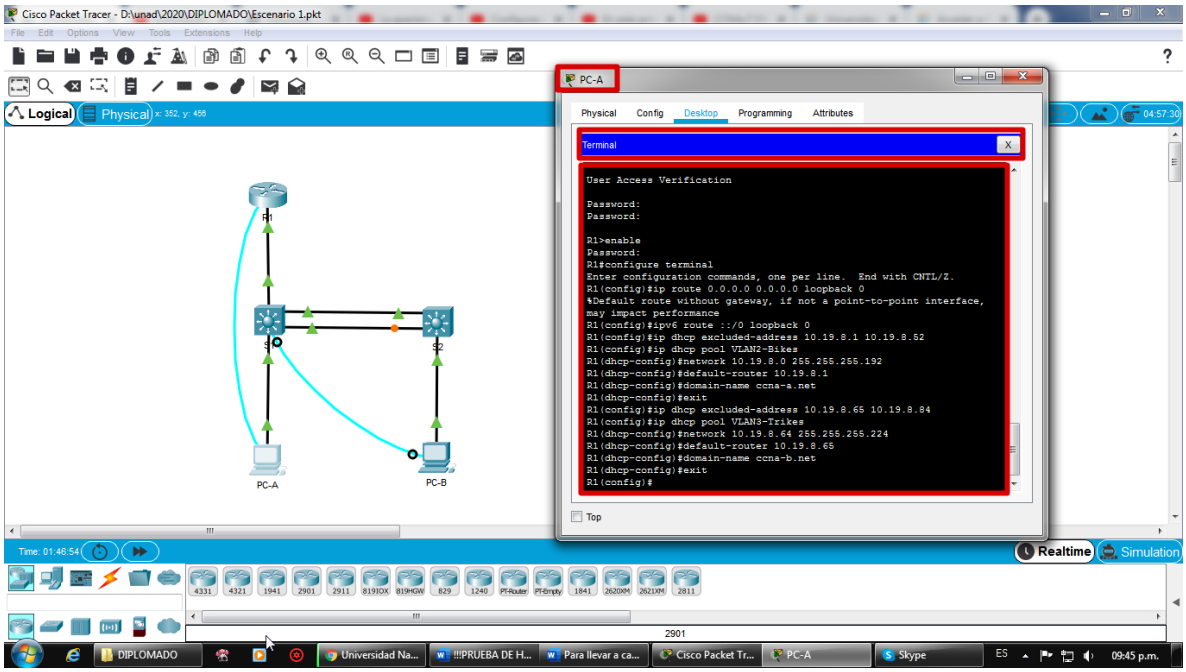
Parte 3: Configurar Soporte de host

Paso 1: Configure R1

Tabla 8 – Configure R1 soporte de host

Comandos Utilizados Configuración Soporte Host	Especificación
R1>enable R1#configure terminal R1(config)# ip route 0.0.0.0 0.0.0.0 loopback 0 R1(config)#ipv6 route ::/0 loopback 0	Ingreso a modo privilegiado Ingreso a modo de configuracion configura y crea las rutas predeterminadas para la Ipv4 e Ipv6 dirijan el trafico a la interfaz Loopback.
R1(config)#ip dhcp excluded-address 10.19.8.1 10.19.8.52 R1(config)#ip dhcp pool VLAN2-Bikes R1(dhcp-config)#network 10.19.8.0 255.255.255.192 R1(dhcp-config)#default-router 10.19.8.1 R1(dhcp-config)#domain-name ccn-a.net	Permite crear un grupo DHCP para VLAN 2, compuesto por las últimas 10 direcciones de la subred solamente. Asigna nombre de dominio ccna-a.net y especifica la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada
R1(config)#ip dhcp excluded-address 10.19.8.65 10.19.8.84 R1(config)#ip dhcp pool VLAN3-Trikes R1(dhcp-config)#network 10.19.8.64 255.255.255.224 R1(dhcp-config)#default-router 10.19.8.65 R1(dhcp-config)#domain-name ccn-b.net	Permite crear un grupo DHCP para VLAN 3, compuesto por las últimas 10 direcciones de la subred solamente. Asigna el nombre de dominio ccna-b.net y especifican la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada

Figura 11: Configure R1 soporte de host



Fuente: Autor

Continuando en la terminal del PC-A proseguimos a la configuración del Soporte de Host del R1.

Paso 2: Configurar Los Servidores

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

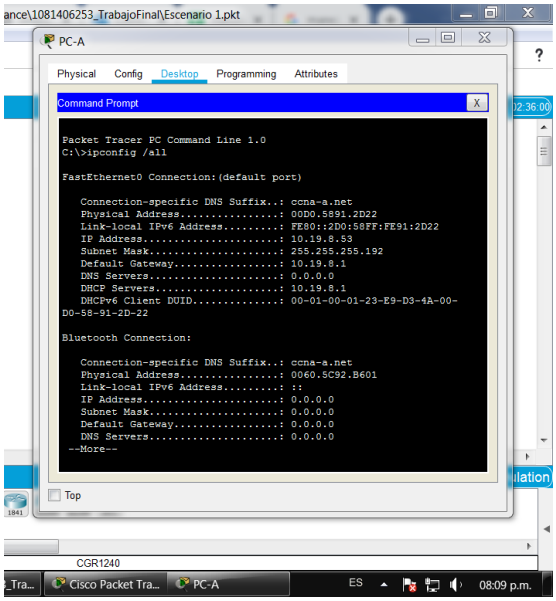
Tabla 9 - PC-A Network Configuration

PC-A Network Configuration	
Descripción	Ccna-a.net
Dirección física	00D0.5891.2D22
Dirección IP	10.19.8.53
Máscara de subred	255.255.255.192
Gateway predeterminado	10.19.8.1
Gateway predeterminado IPv6	FE80::1

Tabla 10 - Configuración de red PC-A

Configuración de red de PC-A	
Descripción	FastEthernet0
Dirección física	2001:db8:acad:a: :50 /64
Dirección IP	10.19.8.53
Máscara de subred	255.255.255.192
Gateway predeterminado	10.19.8.1
Gateway predeterminado IPv6	FE80::1

Figura 12: registro de las configuraciones de red del host PC-A con el comando ipconfig /all.



Fuente: Autor

En la figura 12, se puede observar como se encuentra registrada las configuraciones de la red del host del PC-A.

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

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

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

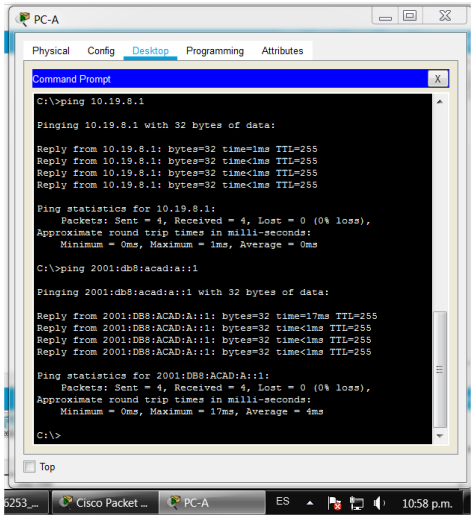
Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 11 - Verificación de conectividad con los dispositvos de red

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

Desde	A	de Internet	Dirección IP	Resultados de ping
		IPv6	2001:db8:acad:209: :1	*OK*
	R1, G0/0/1.2	Dirección	10.19.8.1	*OK*
		IPv6	2001:db8:acad:a: :1	*OK*
	R1, G0/0/1.3	Dirección	10.19.8.65	*OK*
		IPv6	2001:db8:acad:b: :1	*OK*
	R1, G0/0/1.4	Dirección	10.19.8.97	*OK*
		IPv6	2001:db8:acad:c: :1	*OK*
	S1, VLAN 4	Dirección	10.19.8.98	*OK*
		IPv6	2001:db8:acad:c: :98	*OK*
	S2, VLAN 4	Dirección	10.19.8.99.	*OK*
		IPv6	2001:db8:acad:c: :99	*OK*

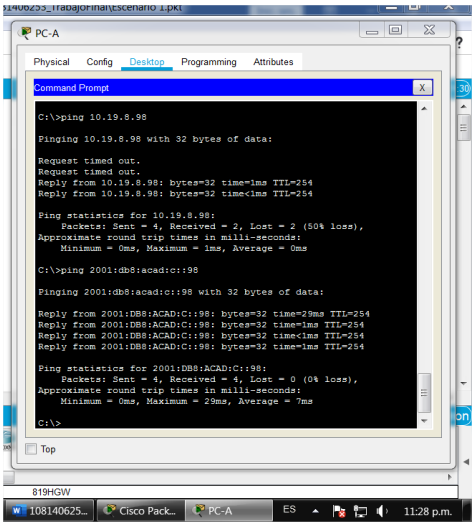
Figura 13: ping PCA- R1, G0/0/1.2



Fuente: Autor

Se realiza Ping desde la PCA- R1, G0/0/1.2 a las direcciones 10.19.8.1, ipv6 2001:db8:acad:a: :1

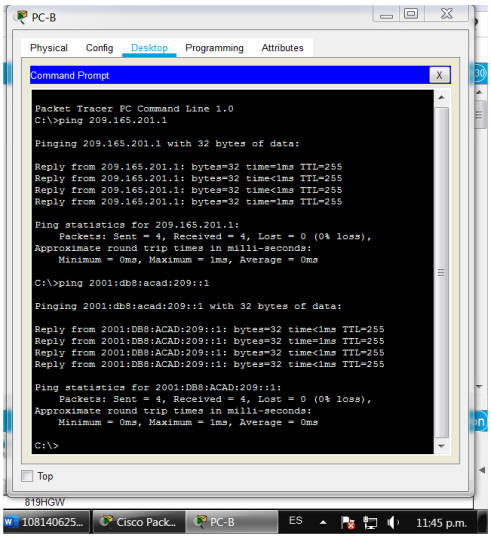
Figura 14: Ping PCA- S1, VLAN 4



Fuente: Autor

Se realiza ping desde el PC-A a S1, VLAN 4 con las direcciones 10.19.8.98, ipv6 2001:db8:acad:c: :98

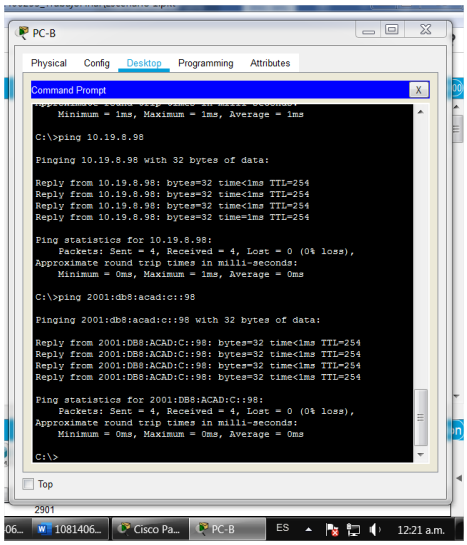
Figura 15: Ping PCB- R1 Bucle 0



Fuente: Autor

Se realiza ping desde el PC-B a R1 Bucle 0 con las direcciones 209.165.201.1, ipv62001:db8:acad:209: :1

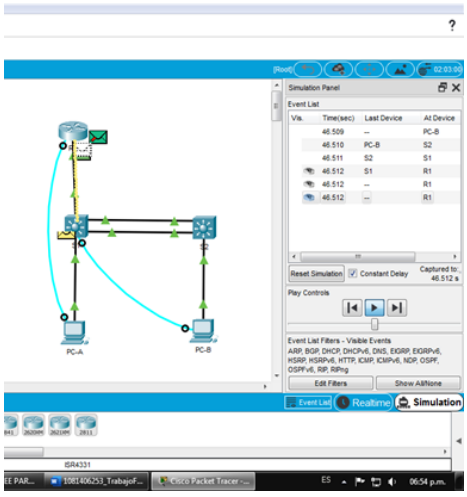
Figura 16: Ping PCB- S1, VLAN 4



Fuente: Autor

Se realiza ping desde el PC-B a S1, VLAN 4, con las direcciones 10.19.8.98, ipv6 2001:db8:acad:c: :98

Figura 17 : Simulación de envío de mensajes escenario 1



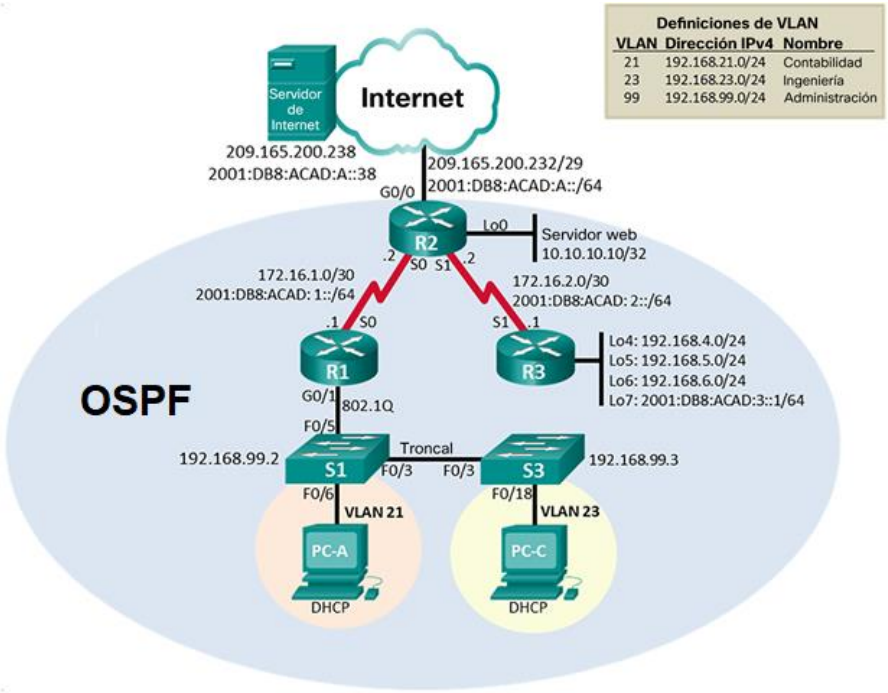
Fuente: Autor

En la figura 15, se puede observar la simulación de envío de mensajes que es exitosa en el escenario 1.

7. ESCENARIO 2

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

Figura 18: Escenario 2



Parte 1: Inizializar dispositivos

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

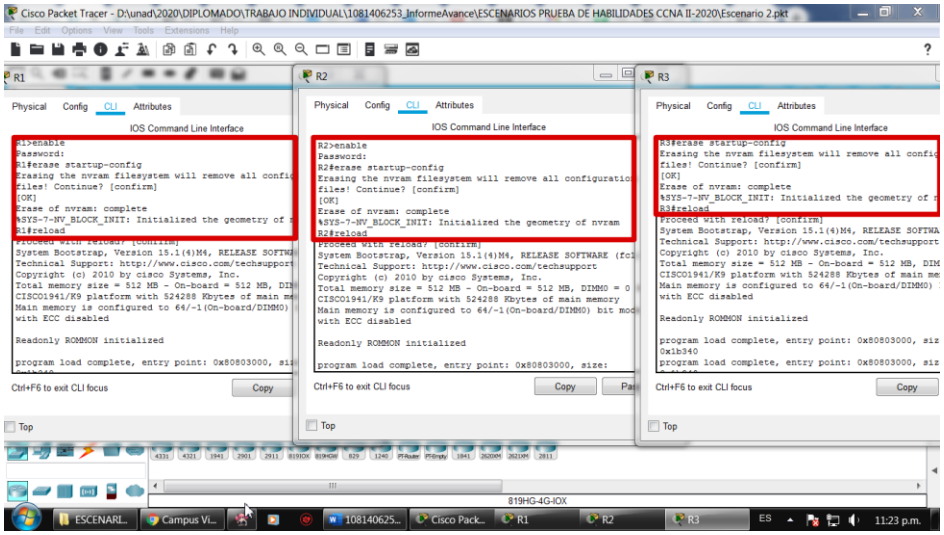
Elimine las configuraciones de inicio y vuelva a cargar los dispositivos.

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

Tabla 12 – Pasos Configuración inicial Escenario 2

Comando de IOS	Especificación
Router>enable Router#erase startup-config	Ingreso modo privilegiado Eliminar configuración de inicio
Router#reload	Recarga los routers
Switch>enable Switch#erase startup-config Switch#delete vlan.dat	Ingreso a modo privilegiado Eliminar configuración de inicio Eliminar el archivo vlan
Switch#reload	Recarga ambos switches
Switch#show vlan brief	Verifica que la base de datos de VLAN no esté en la memoria flash en ambos switches

Figura 19: Eliminación configuración inicial y cargue de los Routers

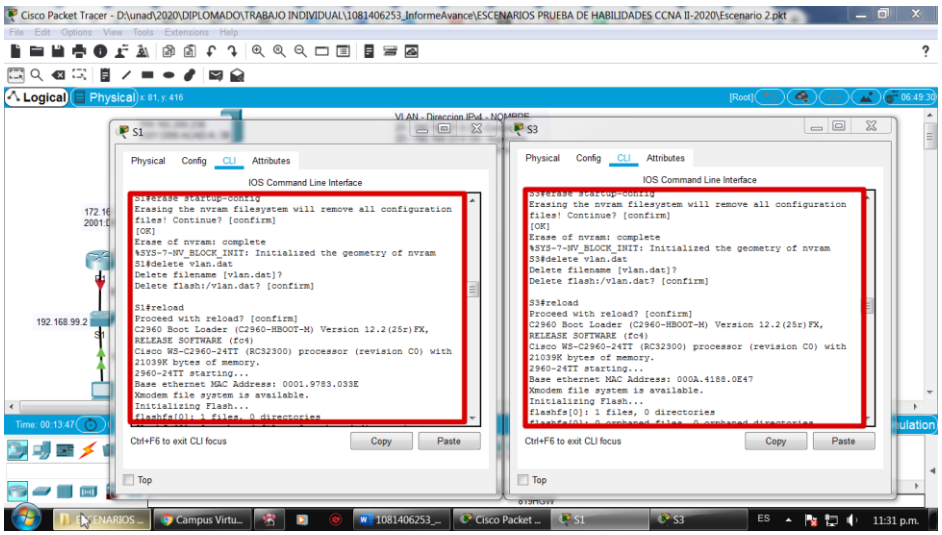


Fuente: Autor

Se accede al Router 1,2 y 3 a través de la consola en modo privilegiado para borrar cualquier configuración de inicio con el comando erase startup-config

posteriormente a ello se recarga de nuevo con wl comando reload se reinicia quedando esté listo para su configuración inicial.

Figura 20: Eliminación configuración inicial y cargue de los Switches



Fuente: Autor

Se accede al Switch 1 y 3 a través de la consola en modo privilegiado para borrar cualquier configuración de inicio con el comando erase startup-config posteriormente a ello se recarga de nuevo con el comando reload se reinicia quedando esté listo para su configuración inicial, y se verifica con el comando Switch#show vlan brief para que las vlan no se encuentren en la memoria flash de ambos swicths.

Parte 2. Configurar los para metros basico de los dispositivos

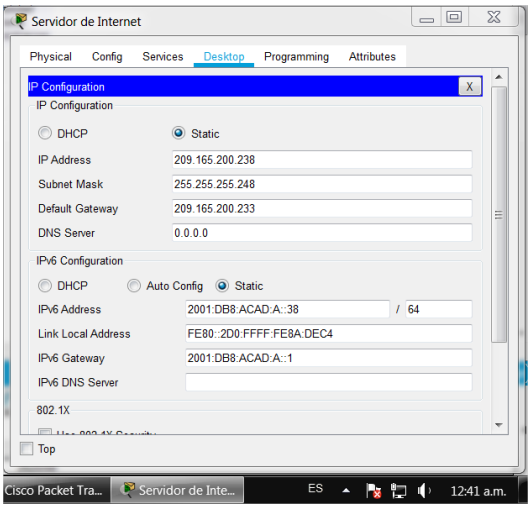
Paso 1. Configurar la computadora de Internet

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

Tabla 13 - Direccionamiento PC Internet

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.233
Dirección IPv6/subred	2001:db8:acad:a::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:A::1

Figura 21: Configuración IP Servidor de Interne



Fuente: Autor

Se lleva a cabo la configuracion de la IP del servidor de Internet.

Paso 2. Configurar R1

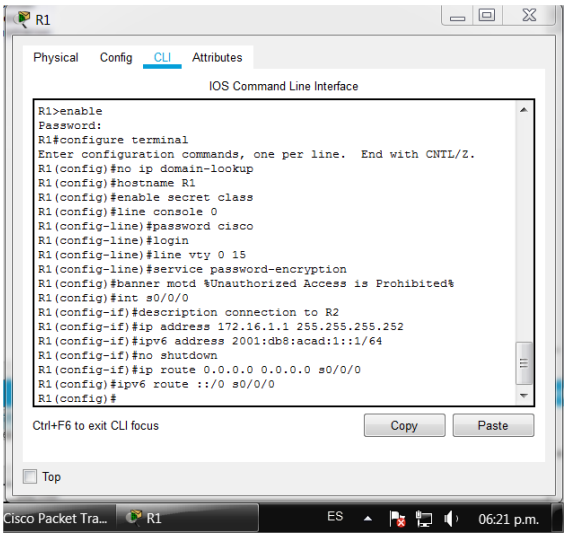
Las tareas de configuración para R1 incluyen las siguientes:

Tabla 14 – Configurar R1

Comandos Utilizados	Especificación
Router>enable Router#configure terminal Router(config)#no ip domain-lookup	Ingreso a modo privilegiado Ingreso a modo de configuracion Desactiva la búsqueda DNS

Router(config)#hostname R1	Asignar nombre del router
R1(config)#enable secret class	Asignar la contraseña cifrada para el modo EXEC privilegiado
R1(config)#line console 0 R1(config-line)#password cisco	Ingreso al modo de configuración de la consola Agsinar acceso de consola Contraseña de acceso a la consola
R1(config-line)#login R1(config-line)#line vty 0 15	Ingreso a configuracion de telnet Activa autenticación de inicio de sesión en las líneas VTY para que use la base de datos local
R1(config-line)#service password-encryption	Cifrado de contraseñas
R1(config)#banner motd %Unauthorized Access is Prohibited!%	Configura mensaje de inicio de sesión, mensaje del día
R1(config)#int s0/0/0 R1(config-if)#description connection to R2 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	permite configurar la interfaz s0/0/0, donde establecemos la descripción, la dirección IPV4, la dirección IPV6, frecuencia de reloj y activarla.
R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0 R1(config)#ipv6 route ::/0 s0/0/0	permite configurar la ruta IPV4 e IPV6 predeterminada de la interfaz s0/0/0

Figura 22: Configuracion R1



Fuente: Autor

Se evidencia el desarrollo de la configuración en el R1, donde asignamos las direcciones ip correspondientes a cada interface según la topología, así mismo creamos una ruta predeterminada para ipv4 e ipv6.

Paso 3. Configurar R2

La configuración del R2:

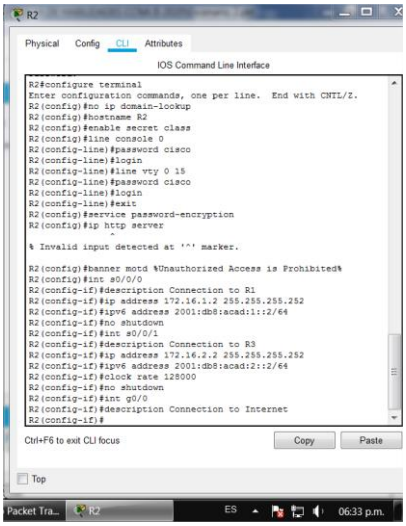
Tabla 15 - Configurar R2

Comandos Utilizados	Elemento o tarea de configuración
Router>enable Router#configure terminal Router(config)#no ip domain-lookup	Ingreso a modo privilegiado Ingreso a modo de configuracion Desactivar la búsqueda DNS
Router(config)#hostname R2	Asignar nombre del router
R2(config)#enable secret class	Asignar el nombre de dominio
R2(config)#line console 0 R2(config-line)#password cisco R2(config-line)#login	Ingreso al modo de configuración de la consola Agsinar acceso de consola Contraseña de acceso a la consola Activa autenticación inicio sesion salir

R2(config-line)#line vty 0 15 R2(config-line)#password cisco R2(config-line)#login R2(config-line)#exit	Ingreso a configuracion de telnet Activa autenticación de inicio de sesión en las líneas VTY para que use la base de datos local Inicio sesion y salir
R2(config)#service password-encryption	Cifrado de contraseña
R2(config)#ip http server	permite habilitar el servidor HTTP, pero este no es soportado por Packet Tracer
R2(config)#banner motd %Unauthorized Access is Prohibited!%	Configura mensaje de inicio de sesión, mensaje del día
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	permite configurar la interfaz s0/0/0, donde establecemos la descripción, la dirección IPV4, la dirección IPV6, frecuencia de reloj y activarla del R2
R2(config)#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	permite configurar la interfaz s0/0/1, donde establecemos, la dirección IPV4, la dirección IPV6, la frecuencia de reloj y activarla del R2

R2(config)#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::1/64 R2(config-if)#no shutdown	permiten configurar la interfaz g0/0, estableciendo la dirección IPV4 y utilizando la primera direccion de la subred disponible, y permite establecer la dirección IPV6 y activar la interfaz.
R2(config)#int loopback 0 R2(config-if)#ip address 10.10.10.10 255.255.255.255 R2(config-if)#description Simulated Web Server R2(config-if)#exit	permite configurar la interfaz loopback0, estableciendo la dirección IPV4.
R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0 R2(config)#ipv6 route ::/0 g0/0	permite configurar rutas del IPV4 , IPV6 predeterminadas de la interfaz g0/0.

Figura 23: Configuración R2



Fuente: Autor

Se evidencia el desarrollo de la configuración en el R2, donde asignamos las direcciones ip correspondientes a cada interface según la topología, así mismo

creamos una ruta predeterminada para ipv4 e ipv6, según lo solicitado en la tabla de tareas.

Paso 4. Configurar R3

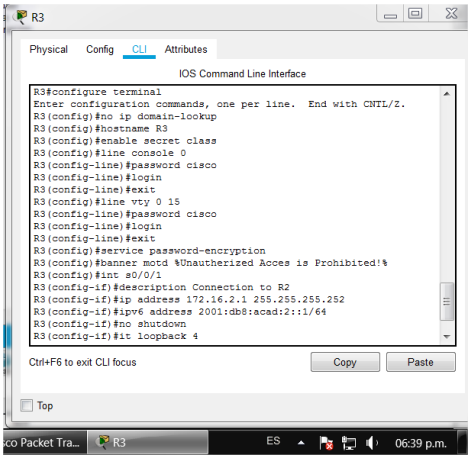
La configuración del R3:

Tabla 16 - Configurar R3

Comandos Utilizados	Especificación
Router>enable Router#configure terminal Router(config)#no ip domain-lookup	Ingreso a modo privilegiado Ingreso a modo de configuracion Desactivar la búsqueda DNS
Router(config)#hostname R3	Asignar nombre del router
R3(config)#enable secret class	Asignar el nombre de dominio
R3(config)#line console 0 R3(config-line)#password cisco R3(config-line)#login R3(config-line)#exit	Ingreso al modo de configuración de la consola Agsinar acceso de consola Contraseña de acceso a la consola Activa autenticación inicio sesion salir
R3(config-line)#line vty 0 15 R3(config-line)#password cisco R3(config-line)#login R3(config-line)#exit	Ingreso a configuracion de telnet Activa autenticación de inicio de sesión en las líneas VTY para que use la base de datos local Inicio de sesion y salir
R3(config)#service password-encryption	Cifrado de contraseñas
R3(config)#banner motd %Unauthorized Access is Prohibited!%	Configura mensaje de inicio de sesión, mensaje del día
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	permite configurar la interfaz S0/0/1 del R3, estableciendo la dirección IPV4, la dirección IPV6 y activando la interfaz.

R3(config-if)#int loopback 4 R3(config-if)#ip address 192.168.4.1 255.255.255.0	permiten configurar la interfaz loopback 4, estableciendo dirección IPv4, y se utiliza la primera direccion de subred disponible
R3(config-if)#int loopback 5 R3(config-if)#ip address 192.168.5.1 255.255.255.0	permite configurar la interfaz loopback 5, estableciendo dirección IPv4 y se utiliza la primera direccion de subred disponible
R3(config-if)#int loopback 6 R3(config-if)#ip address 192.168.6.1 255.255.255.0	permite configurar la interfaz loopback 6, estableciendo dirección IPv4 y se utiliza la primera direccion de subred disponible
R3(config-if)#int loopback 7 R3(config-if)#ipv6 address 2001:db8:acad:3::1/64 R3(config-if)#exit	permite configurar la interfaz loopback 7, estableciendo dirección IPv6.
R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1 R3(config)#ipv6 route ::/0 s0/0/1	permite configurar las rutas Ipv4 y la Ipv6 predeterminada de la interfaz s0/0/1.

Figura 24: Configuracion R3



Fuente: Autor

Se evidencia el desarrollo de la configuración en el R3, donde asignamos las direcciones ip correspondientes a cada interface según la topología, así mismo creamos una ruta predeterminada para ipv4 e ipv6, según lo solicitado en la tabla de tareas.

Paso 5. Configurar S1

La configuración del S1:

Tabla 17 - Configurar S1

Comandos Utilizados	Especificación
Switch>enable Switch#configure terminal Switch(config)#no ip domain-lookup	Ingreso a modo privilegiado Ingreso a modo de configuracion Desactivar la búsqueda DNS
Switch(config)#hostname S1	Asignar nombre del switch
S1(config)#enable secret class	Asignar Contraseña de exec privilegiado cifrada
S1(config)#line console 0 S1(config-line)#password cisco S1(config-line)#login S1(config-line)#exit	Ingreso al modo de configuración de la consola Agsinar acceso de consola Contraseña de acceso a la consola Activa autenticación inicio sesion salir
S1(config-line)#line vty 0 15 S1(config-line)#password cisco S1(config-line)#login	Ingreso a configuracion de telnet Activa autenticación de inicio de sesión en las líneas VTY para que use la base de datos local Activa autenticación de inicio
S1(config-line)#service password-encryption	Cifrado de contraseñas
S1(config)#banner motd %Unauthorized Access is Prohibited!% Este comando nos permite configurar el mensaje de aviso del día	Configura mensaje de inicio de sesión, mensaje del día

Paso 6. Configurar el S3.

La configuración del S3:

Tabla 18 - Configurar S3

Comandos Utilizados	Especificación
Switch>enable Switch#configure terminal Switch(config)#no ip domain-lookup.	Ingreso a modo privilegiado Ingreso a modo de configuracion Desactivar la búsqueda DNS
Switch(config)#hostname S3	Asignar nombre del switch
S3(config)#enable secret class Este comando nos permite asignar contraseña de exec privilegiado cifrada	 Asignar contraseña de exec privilegiado cifrada
S3(config)#line console 0 S3(config-line)#password cisco S3(config-line)#login	Ingreso al modo de configuración de la consola Agsinar acceso de consola Contraseña de acceso a la consola Activa autenticación inicio sesion salir
S3(config-line)#line vty 0 15 S3(config-line)#password cisco S3(config-line)#login	Ingreso a configuracion de telnet Activa autenticación de inicio de sesión en las líneas VTY para que use la base de datos local Activa autenticación de inicio
S3(config-line)#service password-encryption	Cifrado de contraseñas
S3(config)#banner motd %Unauthorized Access is Prohibited!%	Configura mensaje de inicio de sesión, mensaje del día

Paso 7. Verificar la conectividad de la red

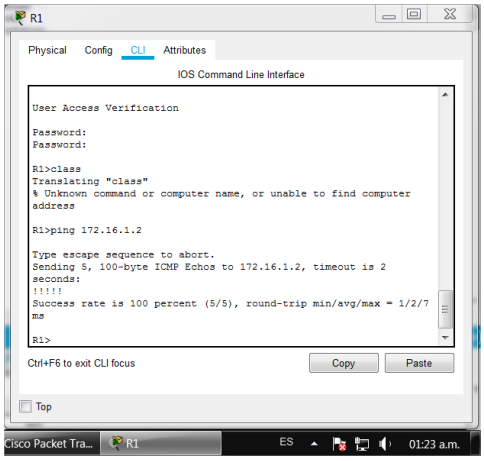
Utilice el comando **ping** para probar la conectividad entre los dispositivos de red.

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

Tabla 19 - Verificar la conectividad de la red

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

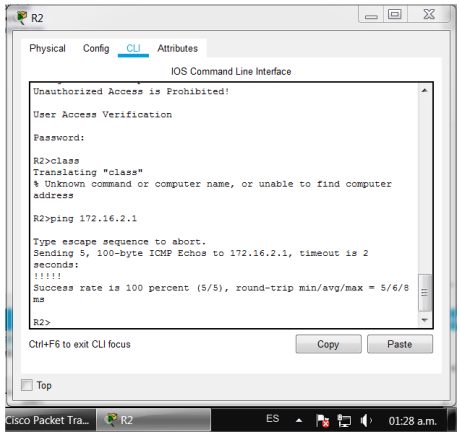
Figura 25: Ping realizado entre R1 – R2 S0/0/0



Fuente: Autor

Se realiza ping probando la conectividad entre el R1 y el R2 y es exitosa.

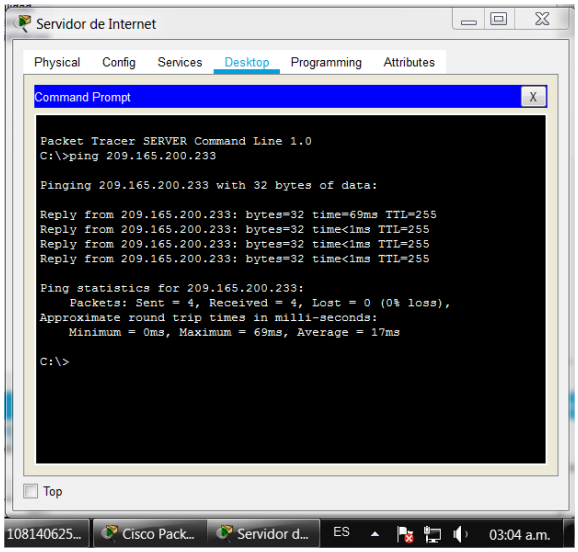
Figura 26 : Ping realizado entre R2 – R3 S0/0/0 172.16.2.1



Fuente: Autor

Se realiza ping probando la conectividad entre el R2 y el R3 y es exitosa.

Figura 27: Ping realizado entre PC de Internet – Gateway predeterminado 209.165.200.233



Fuente: Autor

Se realiza ping probando la conectividad entre el PC de internet y el Gateway predeterminado 209.165.200.233y es exitosa.

Parte 3 . Configurar la seguridad swiitch, las VLAN y el routing entre VLAN

Paso 1. Configurar S1

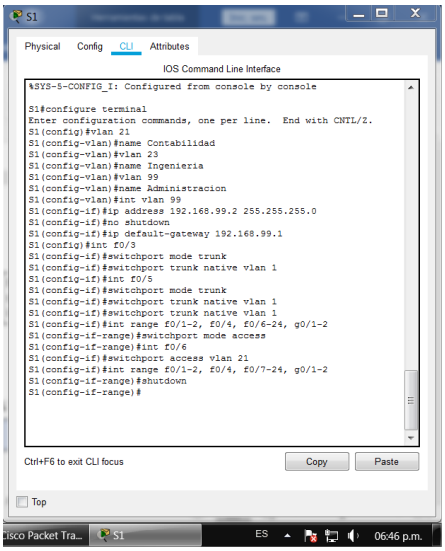
La configuración del S1 las VLAN y el routing entre VLAN:

Tabla 20 - Configurar S1 seguridad, VLAN, y el routing entre VLAN

Comandos Utilizados	Especificación
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	Permite Crea la base de datos de VLAN

S1(config)#int vlan 99 S1(config-if)#ip address 192.168.99.2 255.255.255.0 S1(config-if)#no shutdown	Permite asignar la dirección ip de administrador al igual que la Ipv4 a la VLAN, y activarlas
S1(config)#ip default-gateway 192.168.99.1	Permite asignar el Gateway predeterminado.
S1(config)#int f0/3 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1	Permite forzar el enlace troncal en la interfaz f0/3, utilizando la red VLAN 1 como VLAN native.
S1(config-if)#int f0/5 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1 S1(config-if)#switchport trunk native vlan 1	Permite forzar el enlace troncal en la interfaz f0/5, utilizando la red VLAN 1 como VLAN native.
S1(config-if)#int range f0/1-2, f0/4, f0/6-24, g0/1-2 S1(config-if-range)#switchport mode access	permiten configurar los puertos sobrantes como puertos de acceso.
S1(config-if-range)#int f0/6 S1(config-if)#switchport access vlan 21	Permiten asignar la interfaz f0/6 a la VLAN 21
S1(config-if)#int range f0/1-2, f0/4, f0/7-24, g0/1-2 S1(config-if-range)#shutdown	Permite apagar todos los puertos sin uso para evitar violaciones de intrusos.

Figura 28 : Configuracion S1 seguridad, VLAN, y el routing entre VLAN



Fuente: Autor

Se evidencia el desarrollo de la configuración mas importante en el S1, donde se configurar la seguridad del switch, las VLAN y el routing entre VLAN.

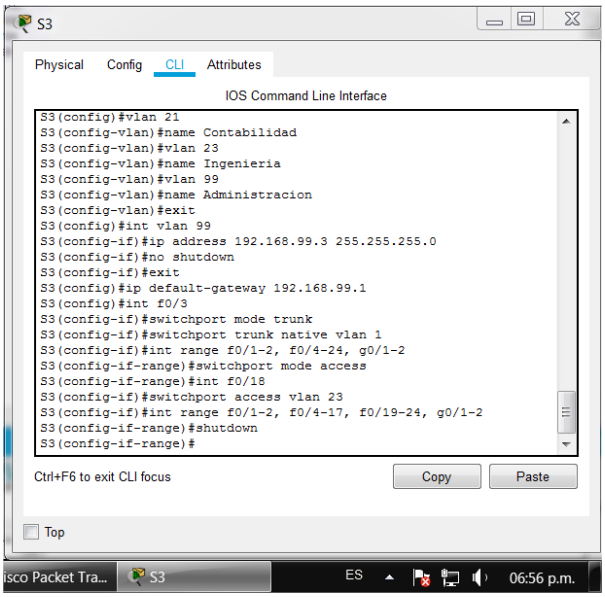
Paso 2: Configurar S3

La configuración del S3:

Tabla 21 - Configurar S3 seguridad, VLAN, y el routing entre VLAN

Comandos Utilizados	Especificación
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 S3(config-vlan)#exit	Permiten crear la base de datos de VLAN
S3(config)#int vlan 99 S3(config-if)#ip address 192.168.99.3 255.255.255.0 S3(config-if)#no shutdown S3(config-if)#exit	Permiten asignar la dirección ip de administrador al igual que la Ipv4 a la VLAN 99
S3(config)#ip default-gateway 192.168.99.1	Permite asignar el Gateway predeterminado..
S3(config)#int f0/3 S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1	permiteN forzar el enlace troncal en la interfaz f0/3, utilizando la red VLAN 1 como VLAN native.
S3(config-if)#int range f0/1-2, f0/4-24, g0/1-2 S3(config-if-range)#switchport mode access	Permiten configurar los puertos sobrantes como puertos de acceso.
S3(config-if-range)#int f0/18 S3(config-if)#switchport access vlan 23	permiten asignar la interfaz f0/18 a la VLAN 21.
S3(config-if)#int range f0/1-2, f0/4-17, f0/19-24, g0/1-2 S3(config-if-range)#shutdown	permiten apagar todos los puertos sin uso para evitar violaciones de intrusos

Figura 29: Configuracion S3



Fuente: Autor

Se evidencia el desarrollo de la configuración mas importante en el S3, donde se configurar la seguridad del switch, las VLAN y el routing entre VLAN.

Paso 3. Configurar R1

Configuración R1:

Tabla 22 - Paso 3 Configurar R1 entre VLAN

Comandos Utilizados	Especificación
R1(config)#int g0/1.21 R1(config-subif)#description LAN Contabilidad R1(config-subif)#encapsulation dot1q 21 R1(config-subif)#ip address 192.168.21.1 255.255.255.0	permiten configurar la subinterfaz 802.1Q.21 en g0/1, asignándola a la VLAN 21

R1(config-subif)#int g0/1.23 R1(config-subif)#description LAN Ingenieria R1(config-subif)#encapsulation dot1q 23 R1(config-subif)#ip address 192.168.23.1 255.255.255.0 R1(config-subif)#exit	permiten configurar la subinterfaz 802.1Q.23 en g0/1, asignándola a la VLAN 23
R1(config-subif)#int g0/1.99 R1(config-subif)#description LAN Administracion R1(config-subif)#encapsulation dot1q 99 R1(config-subif)#ip address 192.168.99.1 255.255.255.0 R1(config-subif)#exit	Permiten configurar la subinterfaz 802.1Q.99 en g0/1, asignándola a la VLAN 99
R1(config-subif)#int g0/1 R1(config-if)#no shutdown	Permiten activar la interfaz g0/1

Paso 4. Verificar la conectividad de la red

Utilice el comando **ping** para probar la conectividad entre los switches y el R1.

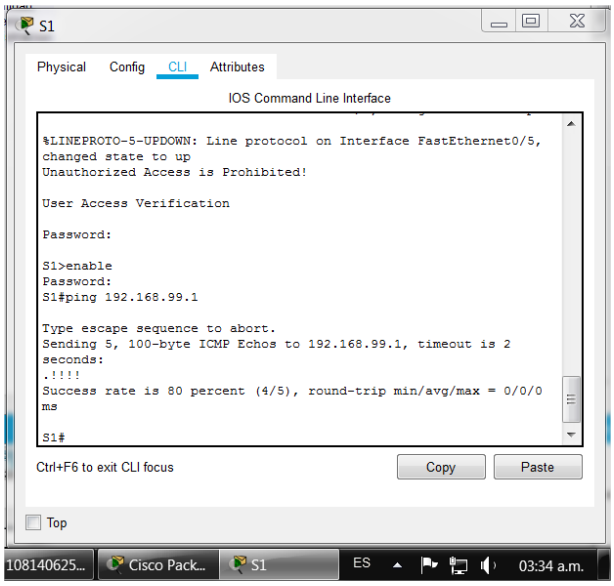
Utilice la sieguiente tabla para verificar metodicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla.

Tabla 23 - Paso 4 Verificar conectividad de red

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

Verificacion de concetividad de los Switches y el R1

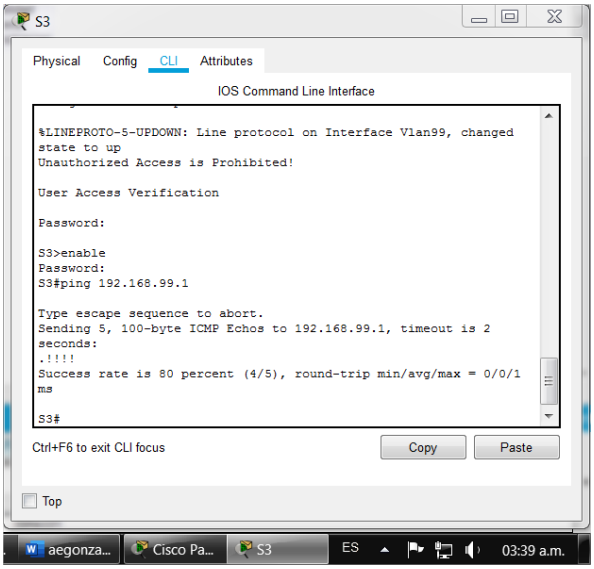
Figura 30: Ping realizado entre S1 – R1, 192.168.99.1 VLAN 99



Fuente: Autor

Se realiza ping entre el S1 y R1 192.168.99.1 VLAN 99 arrojando una conectividad exitosa

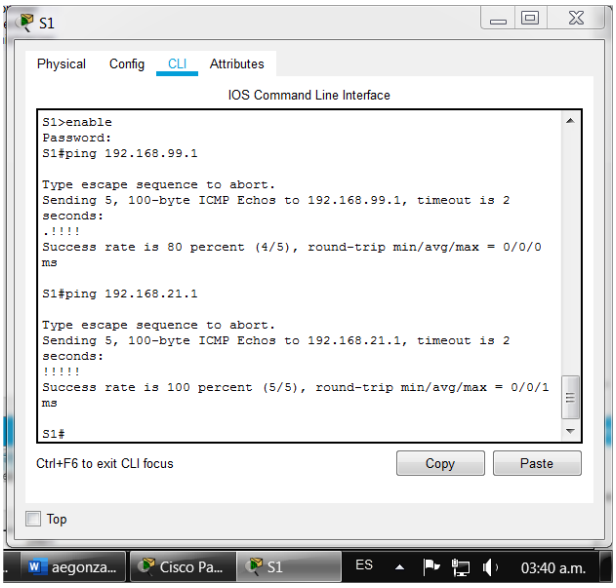
Figura 31: Ping realizado entre S3 – R1, 192.168.99.1 VLAN 99



Fuente: Autor

Se realiza ping entre el S3 y R1 192.168.99.1 VLAN 99 arrojando una conectividad exitosa

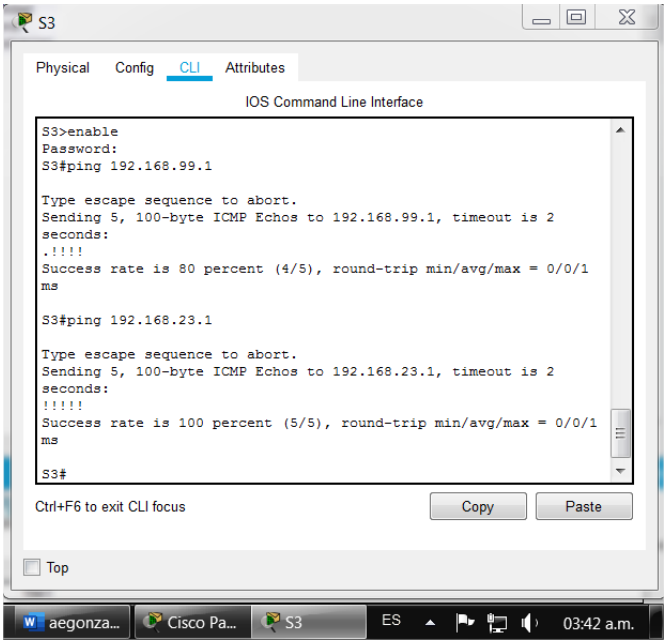
Figura 32: Ping realizado entre S1 – R1, 192.168.21.1 VLAN 21



Fuente: Autor

Se realiza ping entre el S1 y R1 192.168.21.1 VLAN 21 arrojando una conectividad exitosa

Figura 33: Ping realizado entre S3 – R1, 192.168.23.1 VLAN 23



Fuente: Autor

Se realiza ping entre el S1 y R1 192.168.23.1 VLAN 23 arrojando una conectividad exitosa

Parte 4. Configurar el protocolo de routing dinámico OSPF

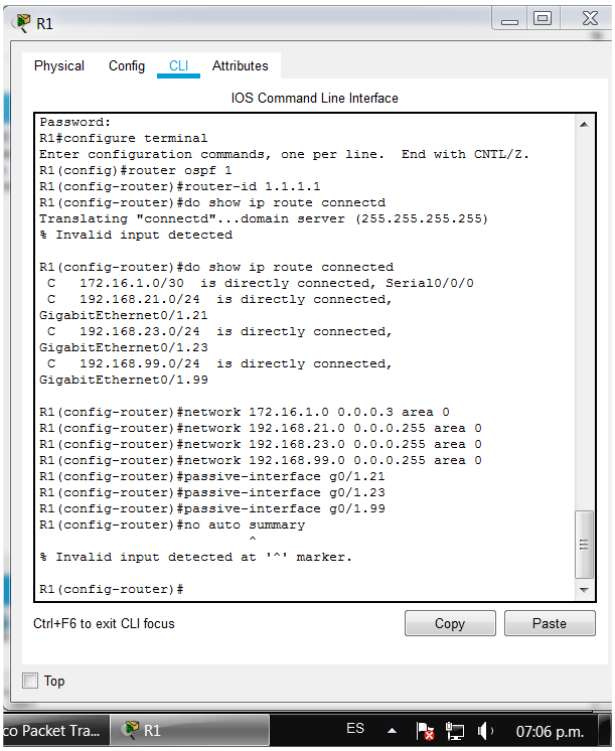
Paso 1. Configurar OSPF en el R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 24 - Configurar OSPF en el R1

Comandos Utilizados	Especificación
R1(config)#router ospf 1 R1(config-router)#router-id 1.1.1.1	Configura el OSPF área 0 del R1
R1(config-router)#do show ip route connected R1(config-router)#network 172.16.1.0 0.0.0.3 area 0 R1(config-router)#network 192.168.21.0 0.0.0.255 area 0 R1(config-router)#network 192.168.23.0 0.0.0.255 area 0 R1(config-router)#network 192.168.99.0 0.0.0.255 area 0	permiten anunciar y asignar todas las redes conectadas directamente.
R1(config-router)#passive-interface g0/1.21 R1(config-router)#passive-interface g0/1.23 R1(config-router)#passive-interface g0/1.99	Permite establecer todas las interfaces LAN como pasivas
R1(config-router)#no auto summary	Permite desactivar la sumarización automática, (OSPF no realiza sumarización así que no aplica)

Figura 34: Configuración de OSPF en el R1



Fuente: Autor

Se evidencia el desarrollo de la configuración mas importante en R1, donde se Configura el protocolo de routing dinámico OSPFv2 y OSPFv3

Paso 2. Configurar OSPF en el R2

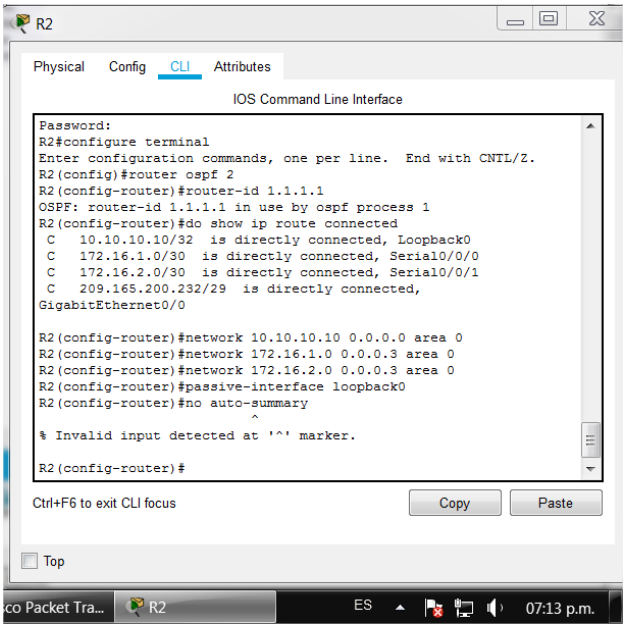
La configuración del R2 incluye las siguientes tareas:

Tabla 25 - Configurar OSPF en el R2

Comandos Utilizados	Especificación
R2(config)#router ospf 2 R2(config-router)#router-id 1.1.1.1	Configurar el OSPF área 0 del R2

R2(config-router)#do show ip route connected R2(config-router)#network 10.10.10.10 0.0.0.0 area 0 R2(config-router)#network 172.16.1.0 0.0.0.3 area 0 R2(config-router)#network 172.16.2.0 0.0.0.3 area 0	Permiten anunciar las redes conectadas directamente al R2
R2(config-router)#passive-interface loopback0	Establecen la interfaz LAN (loopback) como pasiva
R2(config-router)#no auto-summary	desactiva la sumarización automática, aunque la configuración OSPF no realiza esta sumarización así que no aplica.

Figura 35: Configuración del OSPF en el R2



Fuente: Autor

Se evidencia el desarrollo de la configuración mas importante en R2, donde se Configura el protocolo de routing dinámico OSPFv2 y OSPFv3

Paso 3. Configurar OSPFv3 en el R3

La configuración del R3 incluye las siguientes tareas

Tabla 26 - Paso 3 Configurar OSPFv3 en el R3

Comandos Utilizados	Especificación
R3(config)#router ospf 3 R3(config-router)#router-id 1.1.1.1	Configura el OSPF área 0
R3(config)#do show ip route connected C 172.16.2.0/30 is directly connected, Serial0/0/1 R3(config-router)#network 172.16.2.0 0.0.0.3 area 0	anuncian las redes Ipv4 conectadas directamente
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	Establece todas las interfaces de LAN IPv4 (Loopback) como pasivas
R3(config-router)#no auto-summary	desactiva la sumarización automática, aunque la configuración OSPF no realiza esta sumarización así que no aplica.

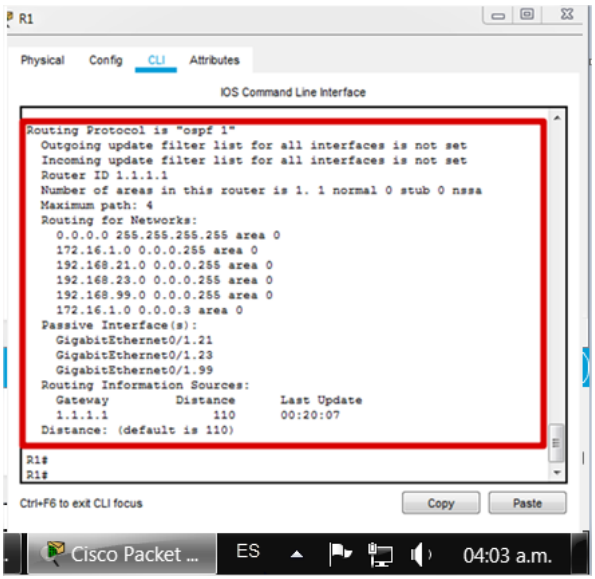
Paso 4. Verificar la información de OSPF

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

Tabla 27 - Paso 4 Verificar la información de OSPF

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

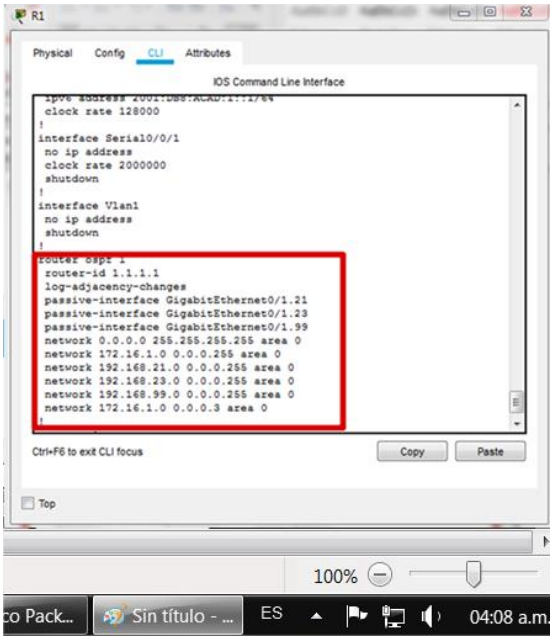
Figura 36: Detalle del proceso OSPF



Fuente: Autor.

Con el comando **show ip portocols** se muestran la ID del proceso OSPF, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router.

Figura 37: sección de OSPF De La Configuración en ejecución



El comando **show run** muestra la sección de OSPF de la configuración en ejecución.

Parte 5. Implementar DHCP y NAT para IPV4

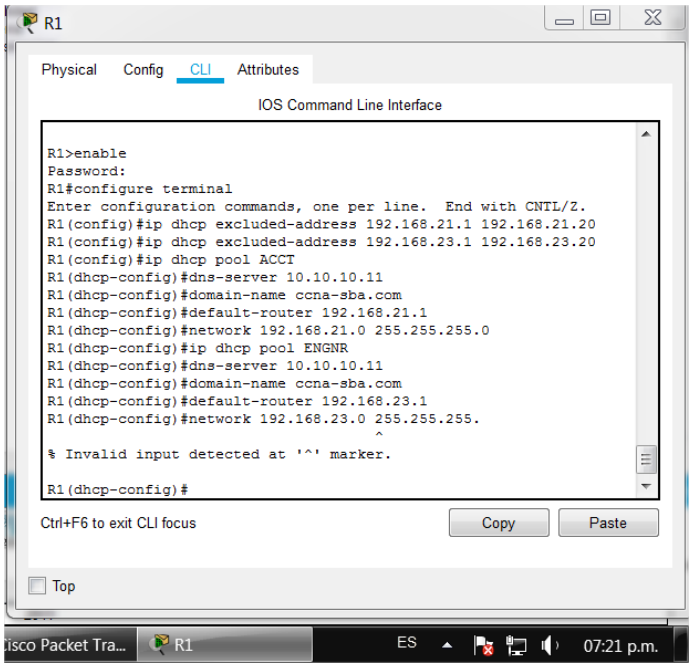
Paso 1. Configurar el R1 como servidor de DHCP para las VLAN 21 y 23

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 28 - Configurar el R1 como servidor de DHCP para las VLAN 21 y 23

Comandos Utilizados	Especificación
R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20	Reserva las primeras 20 direcciones IP en la VLAN 21 para las configuraciones estáticas
R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20	Reserva las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas
R1(config)#ip dhcp pool ACCT R1(dhcp-config)#dns-server 10.10.10.11 R1(dhcp-config)#domain-name ccna-sba.com R1(dhcp-config)#default-router 192.168.21.1 R1(dhcp-config)#network 192.168.21.0 255.255.255.0	crean un pool de DHCP para la VLAN 21, asignando nombre, servidor DNS, nombre de dominio y estableciendo el Gateway predeterminado
R1(dhcp-config)#ip dhcp pool ENGNR R1(dhcp-config)#dns-server 10.10.10.11 R1(dhcp-config)#domain-name ccna-sba.com R1(dhcp-config)#default-router 192.168.23.1 R1(dhcp-config)#network 192.168.23.0 255.255.255.	Crean un pool de DHCP para la VLAN 23 asignando nombre, servidor DNS, nombre de dominio y estableciendo el Gateway predeterminado

Figura 38: Configuración de R1 como servidor DHCP



Fuente: Autor

Se evidencia el desarrollo de la configuración mas importante en R1, donde se Configura el R1 como servidor de DHCP para las VLAN 21 y 23

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

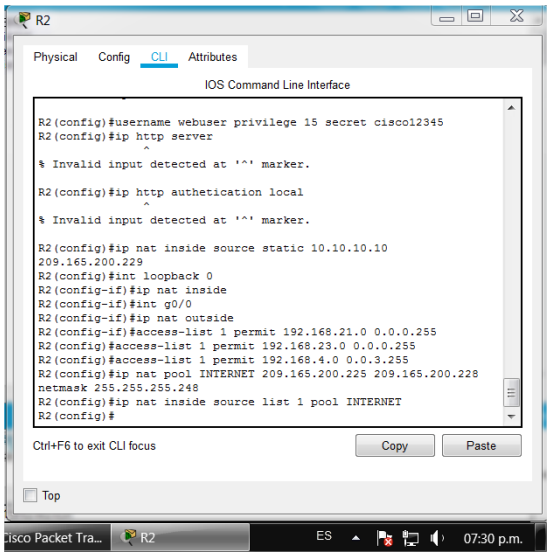
La configuración del R2:

Tabla 29 - Paso 2 Configurar la NAT estatica y dinamica del R2

Comandos Utilizados	Elemento o tarea de configuración
R2(config)#username webuser privilege 15 secret cisco12345	Crea una base de datos local con una cuenta de usuario
R2(config)#ip http server	permite habilitar el servicio del servidor HTTP pero este comando no es aplicable en Packet Tracer

R2(config)#ip http authetication local(commando no applicable en packet tracer)	permite configurar el servidor HTTP y permite utilizar la base de datos local para autenticación, aunque este comando no es aplicable en Packet Tracer
R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229	crea una NAT estática al servidor web, con una dirección global 209.165.200.229
R2(config)#int loopback 0 R2(config-if)#ip nat inside R2(config-if)#int g0/0 R2(config-if)#ip nat outside	asignan una interfaz interna y externa para la NAT estatica.
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	permite configurar la NAT dinámica dentro de una ACL privada, permitiendo la traducción de las redes de Contabilidad, Ingenieria y redes LAN llopback en el R3.
R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248	define la pool de direcciones IP publicas utilizadas
R2(config)#ip nat inside source list 1 pool INTERNET	define la traducción de NAT dinamica

Figura 39: Configuración R2 con NAT estática y dinámica



Fuente: Autor

Se evidencia el desarrollo de la configuración mas importante en R1, donde se configurar la NAT estática y dinámica en el R2

Paso 3. Verificar el protocolo DHCP y la NAT estática

Utilice las siguientes tareas para verificar que las configuraciones de DHCP y NAT estática funcionen de forma correcta. Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

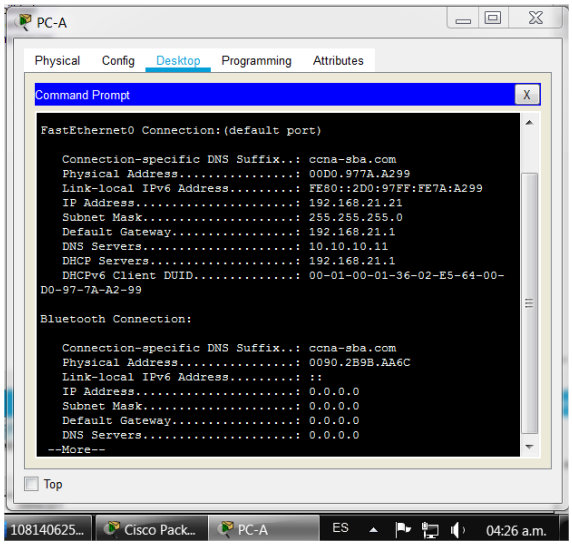
Tabla 30 - Verificar el protocolo DCHP y la NAT estatica

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	Exitoso, toma ip 192.168.21.21
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	Exitoso, toma ip 192.168.23.22

Verificar que la PC-A pueda hacer ping a la PC-C **Nota:** Quizá sea necesario deshabilitar el firewall de la PC.	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**	Packet Tracer no soporta esta operación Se puede realizar ping a esta dirección y es satisfactorio

A continuación se muestran las imágenes de los equipos donde se pueden visualizar las IPs tomadas por cada uno y el resultado del ping realizado entre ambos PCs.

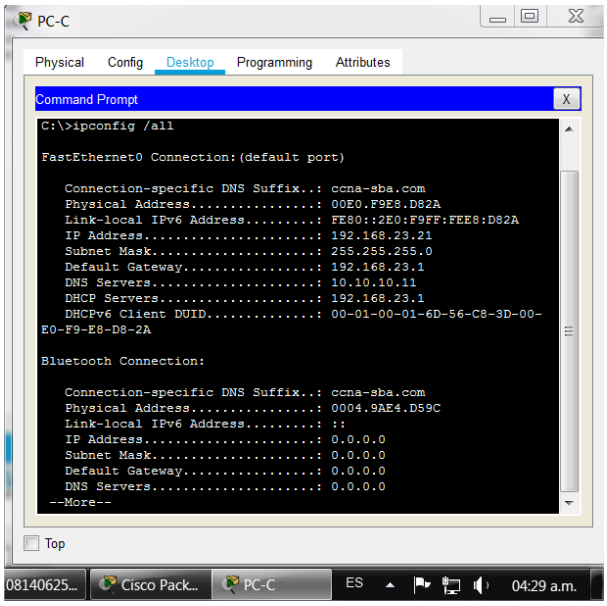
Figura 40: DHCP PC-A



Fuente: Autor

Se verifica que la PC-A haya adquirido información de IP del servidor de DHCP

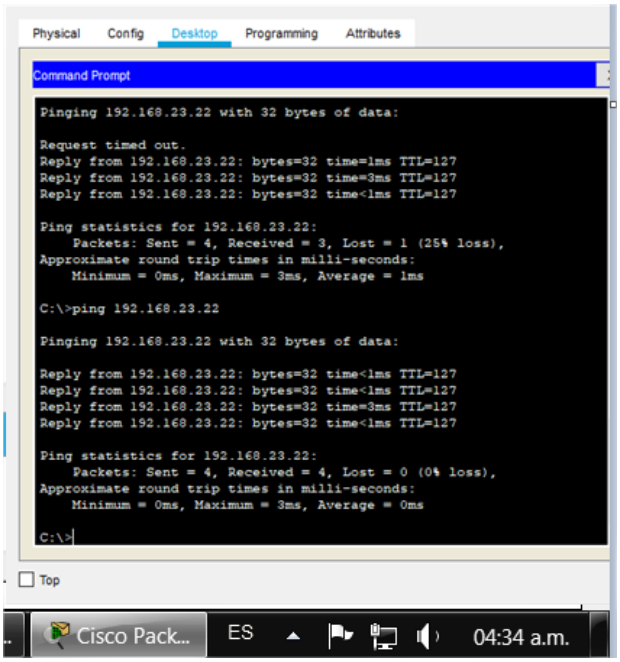
Figura 41: DHCP PC-C



Fuente: Autor

Verificar que la PC-C haya adquirido información de IP del servidor de DHCP

Figura 42: PING PC-A A PC-C



Fuente: Autor

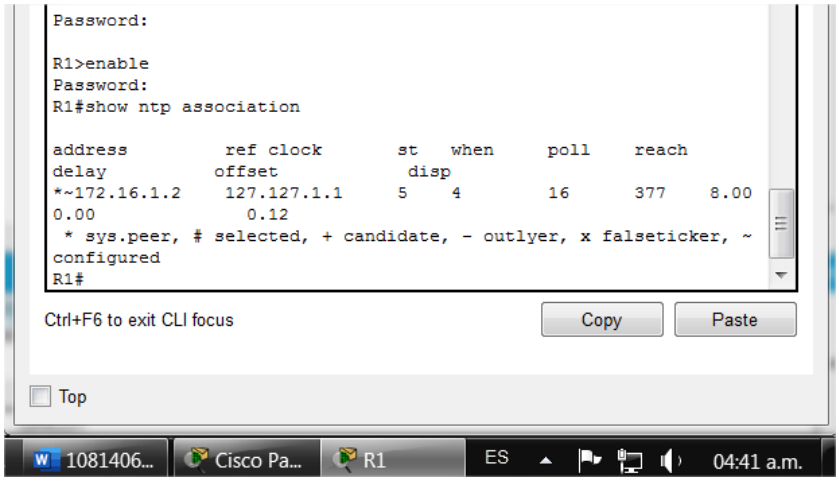
Se verificar que la PC-A pueda hacer ping a la PC-C

Parte 6. Configuración NTP

Tabla 31 - Configurar NTP

Comandos Utilizados	Función
R2#clock set 9:00:00 5 march 2016	Establece la fecha y hora en R2.
R2(config)#ntp master 5	configura el R2 como maestro NTP nivel 5.
R1(config)#ntp server 172.16.1.2	permite configurar el R1 como cliente NTP.
R1(config)#ntp update-calendar	configura el R1 para actualizaciones de hora NTP y calendario periódicamente
R1#show ntp association	verifica la configuración NTP en el R1.

Figura 43: Verificacion de configuración NTP en R1



Fuente: Autor

Se verifica la configuración NTP en el R1.

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

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

Tabla 32 -Restringir el acces a las lineas VTY en el R2

Comandos Utilizados	Elemento o tarea de configuración
R2(config)#ip access-list standard ADMIN-MGT R2(config-std-nacl)#permit host 172.16.1.1	configura una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2
R2(config)#line vty 0 4 R2(config-line)#access-class ADMIN-MGT in	Aplica la ACL con nombre a las líneas VTY
R2(config-line)#transport input telnet	Permite el acceso por Telnet a las líneas de VTY
Verificación de la ACL satisfactorio	R1#telnet 172.16.1.2

Figura 44: telnet 172.16.1.2

Fuente: Autor

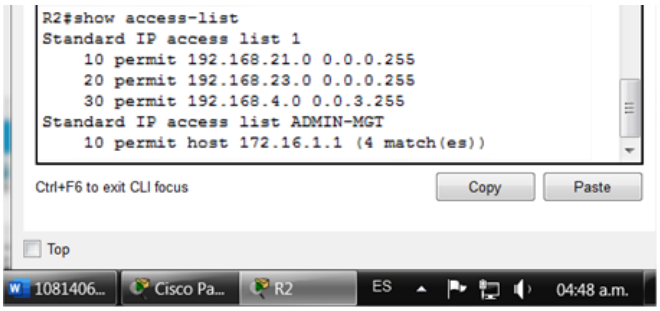
Verificación de la ACL satisfactorio

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

Tabla 33: Comando de CLI adecuado

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
Restablecer los contadores de una lista de acceso	R2#clear ip access-list counters (Packet tracer no soporta este comando9
¿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?	**Nota:** Las traducciones para la PC-A y la PC-C se agregaron a la tabla cuando la computadora de Internet intentó hacer ping a esos equipos en el paso 2. Si hace ping a la computadora de Internet desde la PC-A o la PC-C, no se agregarán las traducciones a la tabla debido al modo de simulación de Internet en la red. PC-A ping 209.165.200.232 R2#show ip nat translations
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	R2#clear ip nat translation * R2#show ip nat translation

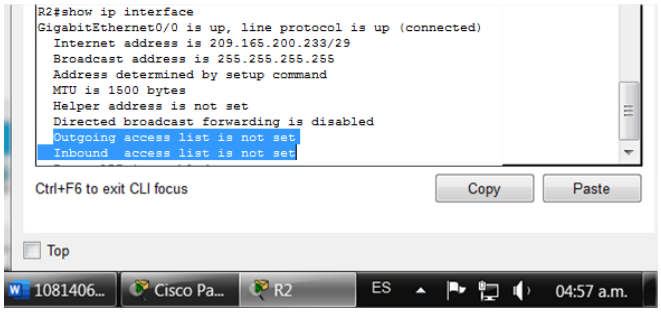
Figura 45: R2#show Access-list



Fuente: Autor

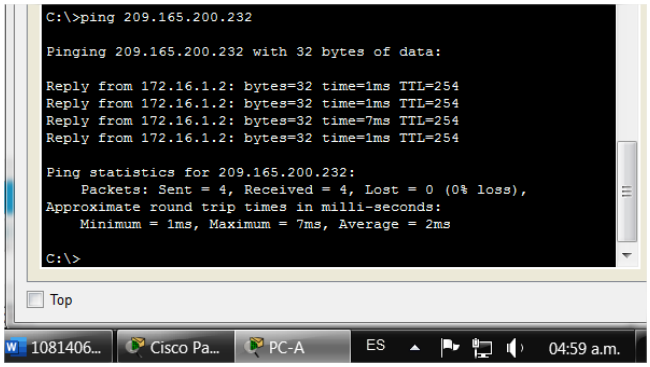
Se muestra las coincidencias recibidas por una lista de acceso desde la última vez que se restableció

Figura 46: R2#show ip interface



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

Figura 47: PC-A ping 209.165.200.232



Fuente: Autor

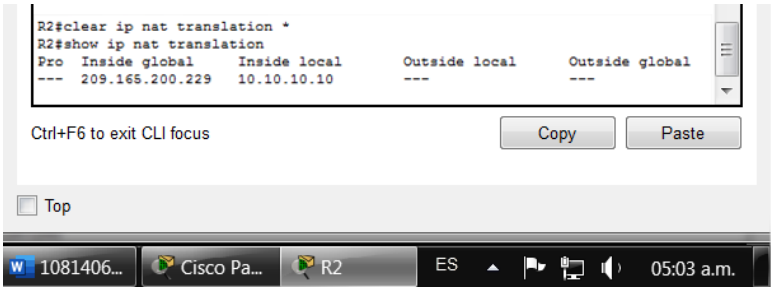
Ping realizado a la ip 209.165.200.232

Figura 48: R2#show ip nat translations

Fuente: Autor

Comando que muestran las traducciones NAT

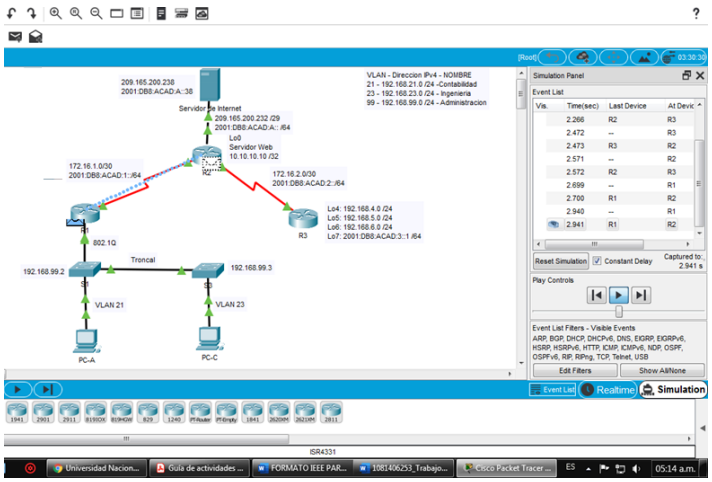
Figura 49: R2#clear ip nat translation * / R2#show ip nat translation



Fuente: Autor

Comando que se utiliza para eliminar las traducciones de NAT dinámica

Figura 46: Simulacion envío de mensajes escenario 2



Fuente: Autor

Se realiza simulación de envío de mensajes en el escenario 2 y es exitosa

8. Conclusiones

Este desarrollo del 1 y del 2 escenario se llevó a cabo cumpliendo con cada uno de los puntos solicitados, teniendo en cuenta los adecuados comandos para configuración de cada dispositivo, configuración de estructuras de red y soporte, de igual manera se realizó la debida verificación de la conectividad de extremo a extremo de la red diseñada, cabe resaltar que fue utilizada la herramienta Packet Tracer para llevar a cabo la solución de este.

Se llevo a cabo la inicialización, recarga y configuración de los dispositivos antes de iniciar las debidas configuraciones pertinentes, utilizando los debidos comandos que nos permito realizar este proceso.

Se Configuro la estructura de red (VLAN, Truking, EtherChannel) en el S1 y S2 en el S1 y S2, por medio de la terminal del PC-B, pues este nos permitio crear las VLAN , crear troncos Crear troncos 802.1Q utilizando VLAN, tambien crear un grupo de puerto Etherchannel, puertos de acceso de interfaces, y asegurar los accesos de de interfaces no utilizadas, pues llevo a cabo de acuerdo a lo solicitado, utilizando los debidos comandos.

Se implemento y se verifivo protocolo DHCP para IPv4 que nos permitio asignar automaticamente las direcciones basadas en el modelo cliente-servidor, de igual manera el protocolo NAT que nos permitio el intercambio de paquetes entre dos redes que tienen asignadas mutuamente direcciones IP incompatibles, siguiendo debidamente las instrucciones de configuración y utilizando los debidos comandos para ello.

Se configuro y se verifico las listas de control de acceso ACL, con nombre para permitir que solo R1 establezca una conexión Telnet con R2, de igual manera permitiendo el acceso por telnet a las lineas VTY y verificando su funcionamiento.

Como herramienta basica para el desarrollo de los escenarios expuestos como informe final, se utilizo el software Packet Tracer, pues esta nos permitio diseñar, modelar y configurar los dispositivos debidamente, cumpliendo con los solicitado, se adquirio bastante conocimiento ya que es una herramienta muy util y facil de manejar, siempre cuando se tenga encuenta el debido usuo para realizar los procesos.

9. Bibliografias

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

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

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

- 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

- CISCO. (2019). Redes Conmutadas. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#4

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

- CISCO Networking Academy, 2014. CCNA Routing and Switching. Introduction to Networks. Principios Básicos de Enrutamiento y Switching. CCNA1 V5

10. Indice de Anexos

Anexo 1 – Link Escenarios Pruebas de habilidades CCNA II-2020

https://drive.google.com/file/d/11huVpfG0FFy46PwR8HVN-tL0tsmTUfsR/view?usp=sharing

Anexo 2 – Articulo IEEE_Lina_Lopez

PRUEBA DE HABILIDADES PRACTICAS CNNA ESCENARIO 1

Lina Mayrena López Pancho

Universidad Nacional Abierta y a Distancia, llopezpa@unadvirtual.edu.co

Resumen

Se lleva a cabo el artículo de reflexión, donde se presentan los resultados obtenidos del desarrollo de la prueba de habilidades practicas CNN escenario 1, utilizando técnicas, metodologías y herramientas como el software de simulación Packet Tracer que permite estructurar las topologías de red de cualquier tipo, configurando los dispositivos y aplicando comandos correctamente para una administración segura y permitiendo la configuración de enrutamiento entre VLAN, DHCP, Etherchannel y port-security y así probar y verificar la conectividad de extremo a extremo de los dispositivos de red utilizados.

Es de suma importancia esta investigación porque permitirá que los ingenieros potencien sus conocimientos teóricos sobre redes y desarrollen competencias a través del uso del software de simulación Packet Tracer sobre un escenario real de donde es necesario contar con información confiable para toma de decisiones y así obtener resultados esperados, dando solución a cualquier problemática presentada en el ámbito de redes.

Palabras clave: VLAN, DHCP, Etherchannel, Port-security, enrutamiento, conectividad

Abstract:

The case report is carried out, where the results obtained from the development of the CNN practical skills test, scenario 1, are presented, using techniques, methodologies and tools such as the Packet Tracer simulation software that allows to structure network topologies of any type , configuring the devices and applying commands correctly for a secure administration and allowing the configuration of routing between VLAN, DHCP, Etherchannel and port-security and thus test and verify the end-to-end connectivity of the network devices used.

This research is of utmost importance because it will allow engineers to enhance their theoretical knowledge about networks and develop skills through the use of Packet tracer simulation software on a real scenario where it is necessary to have reliable information for decision making and thus obtain results. expected, giving solution to any problem presented in the field of networks.

Keywords— VLAN, ***DHCP, Etherchannel, Port-security, routing, connectivity***

I. Introducción

Cada uno de los tres últimos siglos ha estado dominado por una nueva tecnología. El siglo XVIII fue la época de los grandes sistemas mecánicos que dieron paso a la Revolución Industrial. El siglo XIX fue la era de la máquina de vapor. Durante el siglo XX, la tecnología clave fue la recopilación, procesamiento y distribución de información. Entre otros desarrollos vimos la instalación de las redes telefónicas a nivel mundial, la invención de la radio y la televisión, el nacimiento y crecimiento sin precedentes de la industria de la computación, el lanzamiento de satélites de comunicaciones y, desde luego, Internet, y el siglo XIX ha ido a pasos agigantados en los avances tecnológicos hasta llegar a la nanotecnología.

Dentro de este marco podemos observar que las TIC (Tecnología de la Información y las Comunicaciones), han generado un impacto de gran escala en lo social, económico y cultura, y es de ver que cada vez la humanidad depende más de las tecnologías de comunicación.

De acuerdo a ello nos damos cuenta que los avances entorno a las redes informáticas han sido muy significativos, a tal punto que hoy en día cualquier organización ya sea en la parte laboral, académica o familiar poseen una red en su entorno para así garantizar las correctas y efectivas comunicaciones y de seguridad.

Teniendo en cuenta la prueba de habilidades practicas CNN escenario 1 que reporto en este articulo he decidido dar a conocer el desarrollo de dicho escenario utilizando la herramienta de software Packet Trace ya que esta nos permite

afianzar nuestros conocimientos teóricos y nos permite modelar y probar diseños de redes basados en topologías seleccionando los dispositivos necesarios para una administración segura y permitiendo la configuración de enrutamiento entre VLAN, DHCP, Etherchannel y port-security y así probar y verificar la conectividad de extremo a extremo.

II. DESARROLLO

Escenario 1

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

Topologia

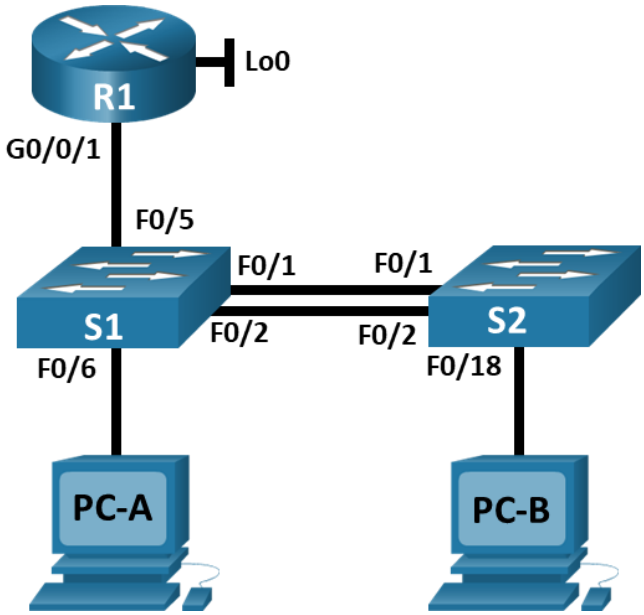


Figura 1: Topología de red a diseñar

TABLA 1
VLAN

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

TABLA 2
ASIGNACION DE DIRECCIONES

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
R1 G0/0/1.2	10.19.8.1 /26	No corresponde
	2001:db8:acad:a: :1 /64	No corresponde
R1 G0/0/1.3	10.19.8.65 /27	No corresponde
	2001:db8:acad:b: :1 /64	No corresponde
R1 G0/0/1.4	10.19.8.97 /29	No corresponde
	2001:db8:acad:c: :1 /64	No corresponde
R1 G0/0/1.6	No corresponde	No corresponde
R1 Loopback0	209.165.201.1 /27	No corresponde
	2001:db8:acad:209: :1 /64	No corresponde
S1 VLAN 4	10.19.8.98 /29	10.19.8.97
	2001:db8:acad:c: :98 /64	No corresponde
	fe80: :98	No corresponde
S2 VLAN 4	10.19.8.99 /29	10.19.8.97
	2001:db8:acad:c: :99 /64	No corresponde
	fe80: :99	No corresponde
PC-A NIC	Dirección DHCP para IPv4	DHCP para puerta de enlace predeterminada IPv4

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
	2001:db8:acad:a: :50 /64	fe80::1
PC-B NIC	DHCP para dirección IPv4	DHCP para puerta de enlace predeterminada IPv4
	2001:db8:acad:b: :50 /64	fe80::1

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

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

Se llevara a cabo la eliminación de las configuraciones de inici y las VLAN del router y de cada switch y luego se recargaran de nuevo los dispositivos para inicializar la configuracion.

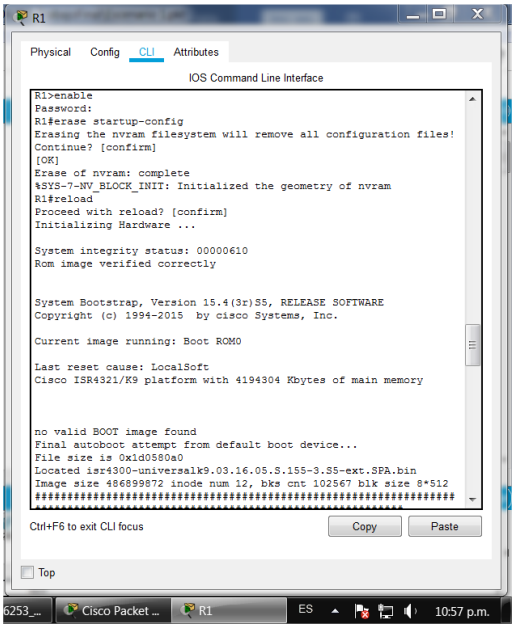


Figura 2: Inicializar y volver a cargar el router

Se ingresa a modo privilegiado y se borra las configuraciones de inicio y las VLAN del router y se recarga de nuevo.

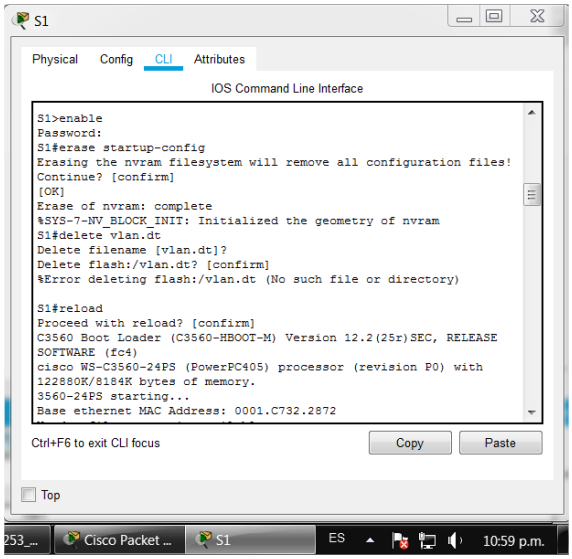


Figura 3: Inicializar y volver a cargar el Switch

Se ingresa en modo priviliegiado y se borra las configuraciones de inicio y las VLAN del switch y se recarga de nuevo para iniciar configuración.

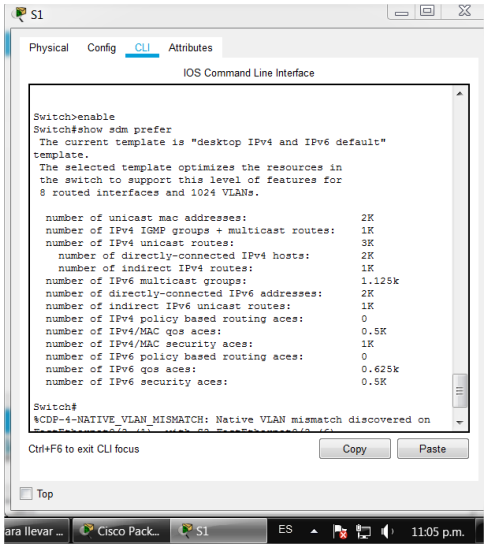


Figura 4: show sdm prefer

Se realiza la configuración y posteriro a ello la verificación de la plantilla SDM para que este admita el IPV6.

Paso 2: Configurar R1

En este paso se configura el R1, utilizando debidamente los comandos donde se desactiva el DNS, se le asigna nombre al router, tambien al dominio, se le asigna una contraseña para ingresar al modo privilegiado y a la consola del R1, se le crea usuario administrativo, se le configura el acceso remoto, el cifrado de contraseñas, sele habilita el ipv6 y las interfacez.

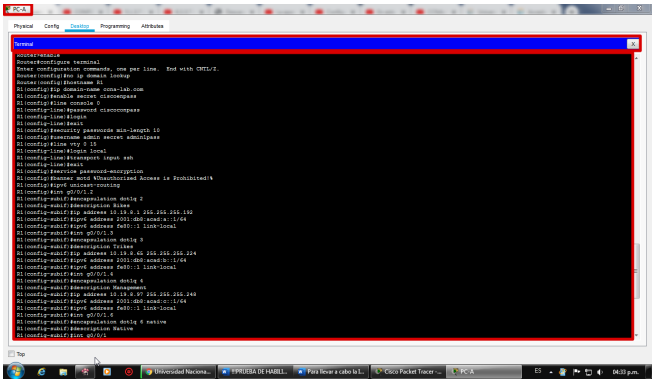


Figura 5: Configuración del R1

Paso 3: Configuración del S1 y el S2

En este paso se configura los switches tanto el S1 como el S2, donde se les desactiva las busquedad del DNS, se le asigna los nombres, el dominio y tambien se le asigna la contraseñas para el ingreso al modo privilegiado y de consola de los mismos, se le crea usuarios administrativos en la base de datos local entre otras configuraciones de gran importancia**.**

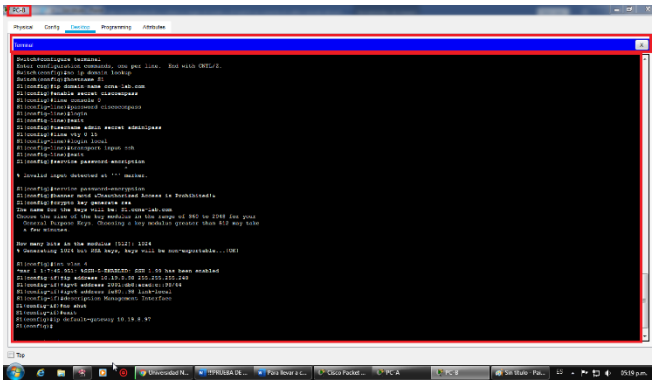


Figura 6: Configuración del S1

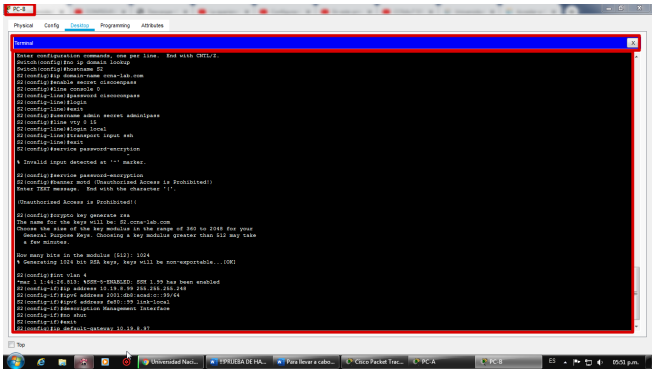


Figura 7: Configuracion del S2

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

En esta parte se crean las VLAN en los S1 y S2, tabien se crean los troncos 802.1Q en las interfaces en las interfacez, tambien se crea el grupo de puertso EtherChannel, se configura la seguridad de los puertos sin utilizar asignandolas a las VLAN.

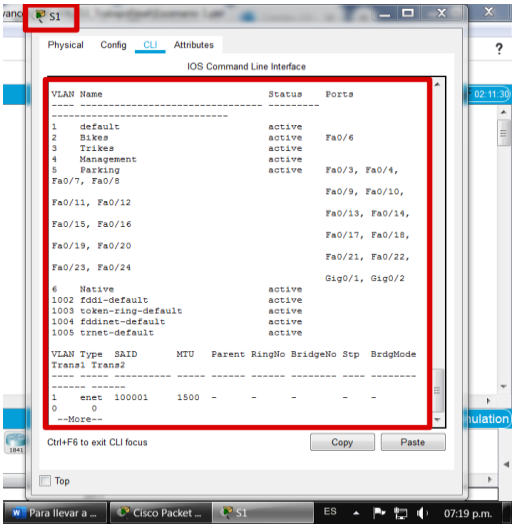


Figura 8: Show VLAN S1

Se muestra las VLAN creadas y configuradas en el S1.

Paso 2: Configurar S2

Continuando en la terminal del PC-B y proseguimos a la configuración de la infraestructura de red (VLAN, Trucking, EtherChannel) del S2 según lo solicitado en la tabla de tareas con los siguientes comandos:

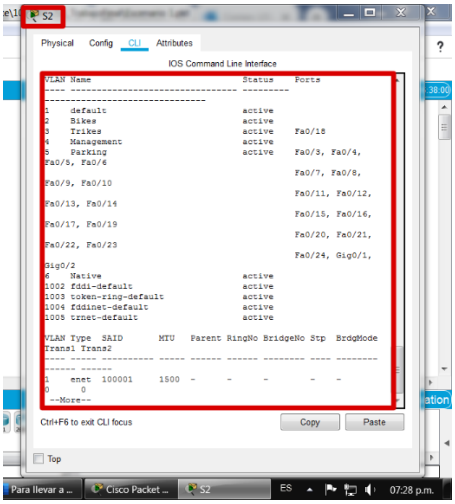


Figura 9*:* Show VLAN S2

Parte 3. Configurar soporte Host

Paso 1. Configure R1

Continuando en la terminal del PC-A proseguimos a la configuración del Soporte de Host del R1 según lo solicitado en la tabla de tareas con los siguientes comandos:

Se llevará la configuración de soporte Host en el R1, utilizando los debidos comandos que nos permitan cumplir con lo solicitado en la tabla de tareas.

Configure Default Routing, Crear rutas predeterminadas para IPv4 e IPv6 que dirijan el tráfico a la interfaz Loopback 0

Configurar IPv4 DHCP para VLAN 2

Cree un grupo DHCP para VLAN 2, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio ccna-a.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada

Configurar DHCP IPv4 para VLAN 3

Cree un grupo DHCP para VLAN 3, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio ccna-b.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada

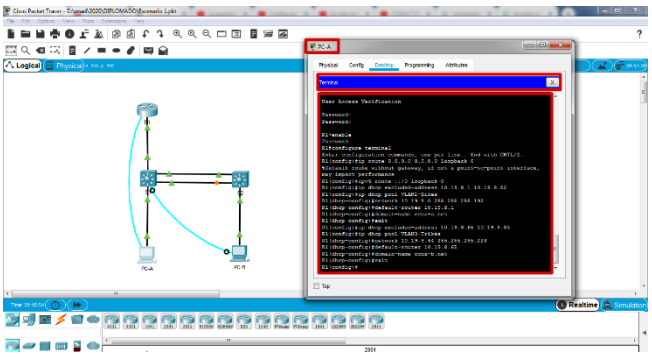


Figura 10: Configuración soporte Host del R1

Se configura el R1, Crear rutas predeterminadas para IPv4 e IPv6 que dirijan el tráfico a la interfaz Loopback 0, de igual manera Configurar IPv4 DHCP para VLAN 2 y se configura DHCP IPv4 para VLAN 3 utilizando los debidos comandos que permitan dicho proceso.

Paso 2. Configurar los servidores

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

TABLA 3

REGISTRO DE LAS CONFIGURACIONES DE RED DEL HOST

PC-A Network Configuration	
Descripción	*Ccna-a.net*
Dirección física	*00D0.5891.2D22*
Dirección IP	*10.19.8.53*
Máscara de subred	*255.255.255.192*
Gateway predeterminado	*10.19.8.1*
Gateway predeterminado IPv6	*FE80::1*

TABLA 4

CONFIGURACION DE RED DEPC-A

Configuración de red de PC-A	
Descripción	*FastEthernet0*
Dirección física	*2001:db8:acad:a: :50 /64*
Dirección IP	*10.19.8.53*
Máscara de subred	*255.255.255.192*
Gateway predeterminado	*10.19.8.1*
Gateway predeterminado IPv6	*FE80::1*

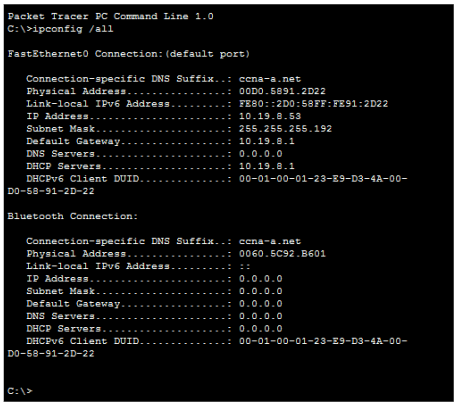


Figura 11: registro de las configuraciones de red del host

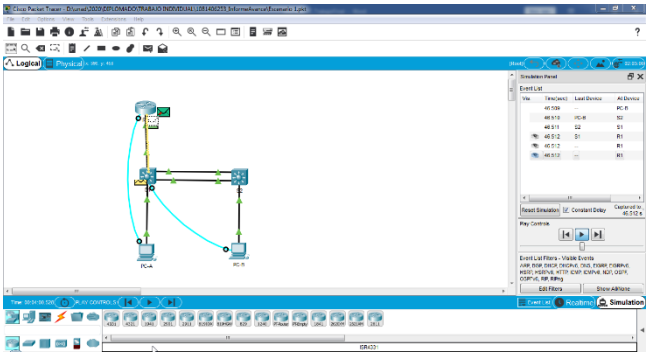


Figura 11: Simulación de mensajes escenario 1

Se muestra la simulación de envío de mensajes instantaneos

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

Se lleva a cabo la verficación de la conectividad de los dispositvos de red, realizando ping a las direcciones ip e ipv6.

TABLA 5

VERIFICACION DE CONECTIVIDAD CON CADA DISPOSITIVO DE RED

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

2

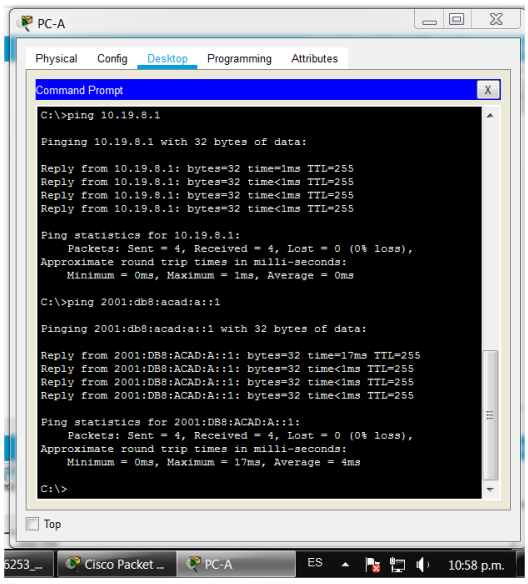


Figura 12: ping PCA- R1, G0/0/1.2

Se realiza Ping desde la PCA- R1, G0/0/1.2 a las direcciones 10.19.8.1, ipv6 2001:db8:acad:a: :1

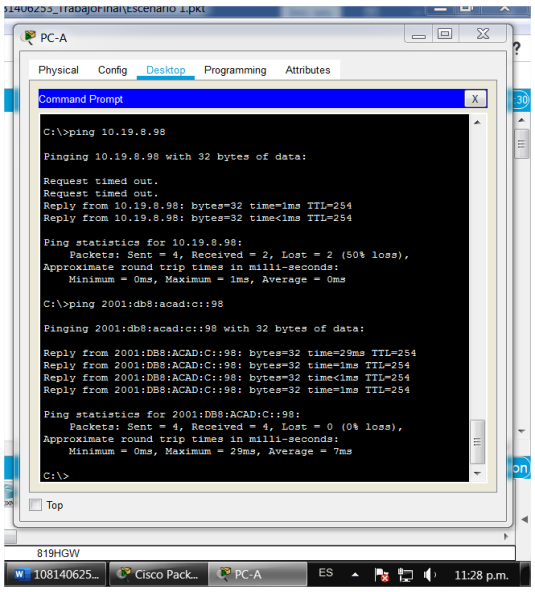


Figura 13: Ping PCA- S1, VLAN 4

Se realiza ping desde el PC-A a S1, VLAN 4 con las direcciones 10.19.8.98, ipv6 2001:db8:acad:c: :98

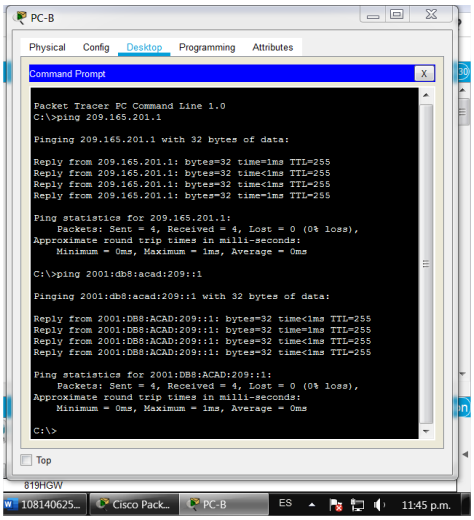


Figura 14: Ping PCB- R1 Bucle 0

Se realiza ping desde el PC-B a R1 Bucle 0 con las direcciones 209.165.201.1, ipv62001:db8:acad:209:

III. CONCLUSIONES

Este artículo se llevó a cabo con el fin de dar a conocer el desarrollo del escenario 1, cumpliendo con cada uno de los puntos solicitados, teniendo en cuenta la importancia ya que este potenciara más los conocimientos teóricos de los ingenieros o cualquier persona interesada en el tema.

En el artículo se logra evidenciar los resultados de la conectividad de los dispositivos, cumpliendo con cada paso solicitado.

Packet Trcer es una herramienta muy importante ya que esta nos permitió llevar a cabo el desarrollo del escenario 1, donde se diseñó, modelo, y se logró configurar cada uno de los dispositivos de la red de la topología.

Para el desarrollo de dicho escenario se utilizaron los debidos comandos que nos permitió llevar a cabo la configuración de la red en general.

Se llevo a cabo la configuración de enrutamiento entre VLAN, DHCP, Etherchannel y port-security se y verifio la conectividad de extremo a extremo de los dispositivos de red utilizados**.**

Se Configuro la estructura de red (VLAN, Truking, EtherChannel) en el S1 y S2 en el S1 y S2, por medio de la terminal del PC-B, pues este nos permitió crear las VLAN , crear troncos Crear troncos 802.1Q utilizando VLAN, también crear un grupo de puerto Etherchannel, puertos de acceso de interfaces, y asegurar los accesos de interfaces no utilizadas, pues llevo a cabo de acuerdo a lo solicitado, utilizando los debidos comandos

IV. REFERENCIAS

[1] **CROVELLA, M. y KRISHNAMURTHY, B.** *Internet Measurement*, Nueva York, John Wiley & Sons, 2006

[2] **DAY, J. D. y ZIMMERMANN, H.** "The OSI Reference Model", *Proc. Of the IEEE*, vol. 71, págs. 1334-1340, diciembre de 1983

[3] **DEERING, S.E.** "SIP: Simple Internet Protocol", *IEEE Network Magazine*, vol. 7, págs. 16-28, mayo/junio de 1993

[4] **DENNING, D.E. y SACCO, G.M.** "Timestamps in Key Distribution Protocols", *Commun. of the ACM*, vol. 24, págs. 533-536, agosto de 1981

[5] **DONAHOO, M. y CALVERT, K.** *TCP/IP Sockets in C*, 2a. ed., San Francisco, Morgan Kaufmann, 2009.

[6] **DONAHOO, M. y CALVERT, K.** *TCP/IP Sockets in Java*, 2a. ed., San Francisco, Morgan Kaufmann,2008.

[7] **FALL, K.** "A Delay-Tolerant Network Architecture for Challenged Internets", *Proc. SIGCOMM 2003 Conf.*, ACM, págs. 27-34, agosto de 2003.

[8] **FALOUTSOS, M., FALOUTSOS, P. y FALOUTSOS, C.** "On Power-Law Relationships of the InternetTopology", *Proc. SIGCOMM '99 Conf.*, ACM, págs. 251-262, 1999

[9] **FENNER, B., HANDLEY, M., HOLBROOK, H. y KOUVELAS, I.** "Protocol Independent Multicast-Sparse Mode (PIM-SM)", RFC 4601, agosto de 2006

[10] **FOX, A., GRIBBLE, S., BREWER, E. y AMIR, E.** "Adapting to Network and Client Variability via On-Demand Dynamic Distillation", *SIGOPS Oper. Syst. Rev.*, vol. 30, págs. 160-170, diciembre de 1996.

[11] **FRANCIS, P.** "A Near-Term Architecture for Deploying Pip", *IEEE Network Magazine*, vol. 7, págs.30-37, mayo/junio de 1993.

[12] **FRASER, A. G.** "Towards a Universal Data Transport System", *IEEE J. on Selected Areas in Commun.*, vol. 5, págs. 803-816, noviembre de 1983

[13] **FULLER, V. y LI, T.** "Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan", RFC 4632, agosto de 2006.

[14] **GAST, M.** *802.11 Wireless Networks: The Definitive Guide*, 2a. ed., Sebastopol, CA: O'Reilly, 2005.

[15] **HUITEMA, C.** *Routing in the Internet*, 2a. ed., Englewood Cliffs, NJ: Prentice Hall, 1999

IV. BIOGRAFÍA

Lina Mayrena López Pancho nació en La Plata Huila, Colombia, el 25 de octubre de 1990. Se graduó de la Institución Educativa San Sebastián, realizo un Técnico en Sistemas en el SENA del mismo Municipio y actualmente está culminando la carrera Profesional de Ingeniería de Sistemas en la Universidad Nacional Abierta y a Distancia CEAD La Plata Huila, realizando como opción de grado Diplomado de Profundización Cisco CNNA.

Actualmente labora en Medimas Eps, en el área de salud, como Gestora Municipal RS, en el Municipio de La Plata.