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

JUAN GABRIEL BUSTOS ALDANA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
INGENIERÍA DE SISTEMAS
GIRARDOT
2020

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

JUAN GABRIEL BUSTOS ALDANA

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

DIEGO EDINSON RAMIREZ CLAROS
Tutor de Curso

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
INGENIERÍA DE SISTEMAS
GIRARDOT
2020

NOTA DE ACEPTACIÓN:

_____

_____

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

Girardot, 03 de diciembre de 2020

DEDICATORIA

Esta tesis está dedicada a la honra y gloria de Dios, a mi esposa y mis hijos que has sido mi apoyo incondicional, a mis padres y mis hermanos que me han acompañado en este proceso tan maravillosos que no termina, sino que inicia teniendo siempre la premisa de ayudar con mis conocimientos y fortalecerlos cada día más, aportando al mundo que me rodea y afrontando los retos con responsabilidad y entrega de la mano de Dios para culminar con éxito todo lo que emprenda.

AGRADECIMIENTO

Gratitud enorme hacia el todo poderoso, Dios quien en todo lugar y circunstancia guía mis pasos y orienta mi vida.

A cada uno de los integrantes de la Universidad Nacional Abierta y a Distancia, quienes dan lo mejor de sí para brindarnos las herramientas que forman los profesionales que se necesitan para esta nueva era.

CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

RESUMEN

El presente trabajo ha sido elaborado con el fin de poner en práctica los conceptos de cada una de las unidades del diplomado, el manejo y la utilización de software que simulan la realidad a la que nos vamos a enfrentar como Ingenieros, se presentan dos (2) escenarios que evidencian la ejecución, manejo y administración de redes mediante la aplicación de cada uno de los pasos que se desarrollan en cada ejercicio; en el escenario 1es necesario configurar los dispositivos de una red pequeña.

Es de obligatorio cumplimiento configurar un router, un switch y cada uno de los dispositivos que admitan la conectividad IPv4 como IPv6 para los hosts soportados, los cuales deben ser administrados de tal forma que tengan un buen nivel de seguridad realizando el enrutamiento VLAN, DHCP, Etherchannel y port-security.

En el siguiente escenario No dos (2) se verificarán los comandos aprendidos y se aplicarán en los protocolos exigidos para el cumplimiento de los procedimientos tal como OSPF, DHCP.

Palabras Clave: CISCO, CCNA, Conmutación, Enrutamiento, Redes.

ABSTRACT

This work has been prepared in order to put into practice the concepts of each of the units of the diploma, the management and use of software that simulates the reality that we are going to face as Engineers, two (2) scenarios that show the execution, management and administration of networks through the application of each of the steps that are developed in each exercise in scenario 1 it is necessary to configure
devices on a small network.
It is mandatory to configure a router, a switch and each of the devices that support IPv4 and IPv6 connectivity for the supported hosts, which must be managed in such a way that they have a good level of security by performing VLAN, DHCP, Etherchannel and routing. port-security.
In the following scenario, the commands learned will be verified and they will be applied in the protocols required to comply with the procedures such as OSPF, DHCP.

Keywords: CISCO, CCNA, Routing, Swicthing, Networking.

GLOSARIO

Interfaz: puertos especializados en un dispositivo de red que se conecta a redes individuales. Puesto que los routers se utilizan para interconectar redes, los puertos de un router se conocen como interfaces de red.

Red de área local (LAN): que proporciona un red no muy grande y con un alcance reducido o limitado pero que brinda los parámetros de conectiviad suficiente en infraestructuras pequeñas.

ICPM (Internet Control Message Protocol, Protocolo de mensajes de control de Internet): este nos ayuda a administrar aquella información que tiene que ver con los con errores de todos aquellos equipos de una red.

ISP (Internet Services Provider/Proveedor de Servicios de Internet): Una compañía que proporciona a sus clientes acceso a Internet.

DSL: el servicio de DSL empresarial está disponible en diversos formatos. Una opción muy utilizada es la línea de suscriptor digital simétrica (SDSL), que es similar a la versión de DSL para el consumidor, pero proporciona las mismas velocidades de subida y descarga.

Filtrado de firewall: es aquel que brinda la protección para el bloqueo en caso de acceso no autorizado en la red. Puede ejecutarse en un host especifico para este tipo de accesos en la terminal o un servicio de filtrado básico como en un router.

Sistemas de prevención de intrusión (IPS): Este sistema puede dar aviso en cuanto a amenazas se refiera.

Redes privadas virtuales (VPN): es aquel que brinda protección en caso de emplear conexiones remotas.

INTRODUCCIÓN

El presente trabajo describe los dos escenarios prácticos establecidos para la prueba de habilidades, mostrando el nivel de competencias adquiridas en el tiempo de desarrollo del Diplomado, poniendo en práctica lo visto en cada una de las unidades brindando la solución de problemas que se presentan a diario en la vida cotidiana del Networking.

Los escenarios fueron realizados en el software de simulación “Cisco Packet Tracer versión 7.3.1, donde se probó la conectividad de la red con los comandos comunes de CLI que muestran lo insertado en la programación de cada router y switch.

En el primer escenario se pretenden configurar un (01) router y dos 02 switch, que van desde la asignación del nombre del host, conectividad IPv4 como IPv6 administración de forma segura y configuración del enrutamiento entre VLAN, DHCP, Etherchannel y port-security.

En el segundo escenario se configurará la red teniendo en cuenta que debe admitir conectividad tanto de IPv4 como IPv6, debe haber acceso seguro a los switch, debe generarse routing entre las VLAN, se trabajara con el protocolo OSPF, (DHCP), (NAT), (ACL) y (NTP) servidor/cliente.

OBJETIVOS

General

Realizar solución de conectividad de los dispositivos de una red pequeña mediante las diferentes configuraciones LAN, en los escenarios propuestos de la prueba de habilidades.

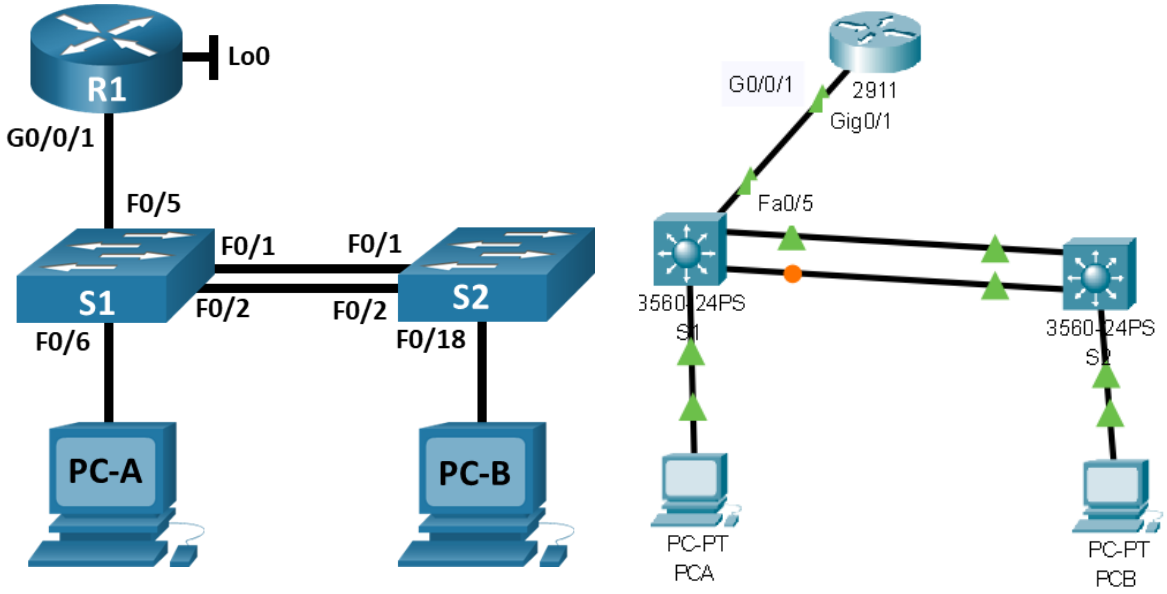
Específicos

- ✓ Configurar router, switch y equipos que admitan tanto la conectividad IPv4 como IPv6.
- ✓ Configurar el enrutamiento entre VLAN, DHCP, Etherchannel y port-security.
- ✓ Emplear y realizar la configuración del protocolo OSPF y (DHCP).
- ✓ Realizar configuración de (NAT), (ACL) y el protocolo (NTP).

ESCENARIO 1

Configurar un (01) router y dos 02 switch, que van desde la asignación del nombre del host, conectividad IPv4 como IPv6 administración de forma segura y configuración del enrutamiento entre VLAN, DHCP, Etherchannel y port-security.

Figura 1 Topología de la red



Topología de red para el escenario 1

Tabla 1 Tabla nombres de Vlan

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

Tabla 2 Tabla de asignación de direcciones

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

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

Parte1: Inicializar, Recargar y Configurar aspectos básicos de los dispositivos

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

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

- ✓ Después de recargar el switch, configure la plantilla SDM para que admita IPv6 según sea necesario y vuelva a cargar el switch.

Para iniciar el ejercicio se debe ingresar a la configuración del router R1 y mediante la ejecución del comando **erase startup-config** se borra la configuración inicial del router, permitiendo la ejecución con las preferencias de usuario, de esta manera se garantizará que todo lo que se haya programado en R1 se borre y se listo para aplicar el comando **reload** donde se carga la configuración predeterminada del router.

La misma tarea se realizará en cada uno de los dispositivos a emplear, en este caso en S1 y S2.

Tabla 3 Inicializar y recargar router y switch

Descripción	Comando
Ingreso a R1 y Switch 1 y 2	enable
Estando en modo privilegiado	erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue?	Dar enter
Reiniciar el dispositivo	reload
¿Continuar con la recarga?	Dar enter
Entrar al dialogo de configuración inicial	Escribir No

Fuente: Autor

Paso 2: Configurar R1

En R1 se realizan los siguientes pasos para lograr el objetivo de configurar el dispositivo:

Lo primero es ingresar al modo de configuración en CLI escribir "configure terminal" y acceder a "Router (config) #" seguidamente se Introduce "no ip domain-lookup" realizando la desactivar la busqueda DNS se hace necesario acambiar el nombre inicial parea asignaer el nombre de R1 lo cual se logra mediante el commando hostname y se da nombre al dominio mediante el commando ip domain-name ccna-lab.com.

El siguiente paso es asignar la contraseña para ingreso a modo privilegiado mediante el commando enable secret ciscoenpass y se emplea el commando password ciscoconpass para asignar contraseña de acceso a la consola.

Se hace necesario establecer la longitud mínima para las contraseñas en donde se realiza mediante el commando security passwords min-length 10 para garantizar que la contraseña tenga como mínimo 10 caracteres
Se crea usuario administrativo en la BD local y se asigna contraseña mediante el commando username admin password admin1pass.

Se realiza la configuración en las líneas VTY para que use la database mediante el comando line vty 0 4, en VTY también se realiza el siguiente paso que es aceptar sólo SSH mediante el comando transport input ssh.

Se emplea el commando service password-encryption, el cual nos sirve y es adecuado para cifrar las contraseña de texto no cifrado, siguiendo la configuración se emplea el comando banner motd para reflejar el mensaje deseado cuando se intenta acceder al usuario, y se habilita el routing para aceptar IPv6.

Una vez realizados los pasos anteriores se procede a Configurar la interfaz G0/0/1 y subinterfaces al igual que el Loopback0 interface estableciendo las direcciones ip asignadas, también se realiza la clave de cifrado RSA mediante el commando crypto key generate rsa general-keys modulus 1024.

Tabla 4 Configuración de R1

Tarea	Especificación
Desactivar la búsqueda DNS	Router> Router>enable Router#configure terminal Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R1
Nombre de dominio	ccna-lab.com R1(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	R1(config)#ena secret ciscoenpass
Contraseña de acceso a la consola	R1(config)#line console 0 R1(config-line)#password ciscoconpass R1(config-line)#login R1(config-line)#exit
Establecer la longitud mínima para las contraseñas	R1(config)#security passwords min-length 10
Crear un usuario administrativo en la base de datos local	Nombre de usuario: **admin** Password: **admin1pass** R1(config)#username admin password admin1pass R1(config)# line console 0 R1(config)# login local R1(config)# exit
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	R1(config)#line vty 0 4 R1(config-line)#login local R1(config-line)#exit
Configurar VTY solo aceptando SSH	R1(config-line)#transport input ssh
Cifrar las contraseñas de texto no cifrado	R1(config-line)#service password-encryption
Configure un MOTD Banner	R1(config)#banner motd # R1 Juan Escenario 1#
Habilitar el routing IPv6	R1(config)#ipv6 unicast-routing

Tarea	Especificación
Configurar interfaz G0/0/1 y subinterfaces	Establezca la descripción Establece la dirección IPv4. Establezca la dirección local de enlace IPv6 como **fe80::1** Establece la dirección IPv6. Activar la interfaz. R1(config)#int g0/1 R1(config-if)#no shutdown
Configure el Loopback0 interface	Establezca la descripción Establece la dirección IPv4. Establece la dirección IPv6. Establezca la dirección local de enlace IPv6 como fe80::1 R1(config-if)#description lookback 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)#no shutdown R1(config)#crypto key generate rsa general-keys modulus 1024
Generar una clave de cifrado RSA	Módulo de 1024 bits R1(config)#crypto key generate rsa general-keys modulus 1024

Configure S1 y S2.

Las tareas de configuración incluyen lo siguiente:

En la presente configuración se desactivan búsquedas de DNS con no ip domain-lookup y se da nombre al switch S1 y también se nombra el dominio “ccna-lab.com“ aplicando el comando ip domain name ccna-lab.com, seguido a acceder mediante la configuración de contraseña cifrada para el modo EXEC privilegiado empleando el comando “enable secret ciscoenpass” para luego acceder mediante contraseña de acceso a la consola en este caso “password ciscoconpass” y “login” para que pida la contraseña anteriormente escrita.

Una vez realizada la ejecución de los comandos anteriores se procede a crear un admin user en la database local empleando el comando “username admin password admin1pass” configurando líneas VTY para que use la database local empleando el comando “line vty 0 4””privilege level 5”, se establecen las líneas VTY para que acepten únicamente las conexiones SSH mediante el commando “transport input ssh” y se cifran las contraseñas de texto no cifrado “service password-encryption”

Se procede a configurar un MOTD Banner “banner motd # Switch1 Escenario 1#” y se genera una clave de cifrado RSA mediante el comando crypto key generate rsa general-keys modulus 1024, se procede a realizar la configuración de la interfaz de administración (SVI) estableciendo la dirección IPv4 de capa 3 y la dirección local de enlace IPv6 como FE80: :98 para S1 y Permitiendo IPV6 en el router mediante “sdm prefer dual-ipv4-and-ipv6 ?” “sdm prefer dual-ipv4-and-ipv6 luego se configura mediante “int vlan4” la description vlan 4 la ip address 10.19.8.98 255.255.255.248, ipv6 address 2001:db8:acad:c::98/64 y ipv6 address fe80::98 link-local, se procede a prender y establecer la puerta de enlace predeterminada mediante “ip default-gateway 10.19.8.97”.

Tabla 5 Configuración de S1 y S2

Tarea	Especificación
Desactivar la búsqueda DNS.	Switch(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S1
Nombre de dominio	ccna-lab.com S1(config)#ip domain name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	S1(config)#enable secret ciscoenpass

Tarea	Especificación
Contraseña de acceso a la consola	S1(config)#line console 0 S1(config-line)#password ciscoconpass S1(config-line)#login
Crear un usuario administrativo en la base de datos local	Nombre de usuario: admin Password: admin1pass S1(config-line)#username admin password admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	S1(config)#line vty 0 4 S1(config-line)#privilege level 5
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S1(config-line)#transport input ssh
Cifrar las contraseñas de texto no cifrado	S1(config-line)#service password-encryption
Configurar un MOTD Banner	S1(config)#banner motd # Switch1 Escenario 1#
Generar una clave de cifrado RSA	Módulo de 1024 bits S1(config)#crypto key generate rsa general-keys modulus 1024
Configurar la interfaz de administración (SVI)	Establecer la dirección IPv4 de capa 3 Establezca la dirección local de enlace IPv6 como FE80: :98 para S1 y Permitir IPV6 en el router S1(config)#int vlan4 S1(config-if)#description 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)#no shutdown S1(config-if)#ip default-gateway 10.19.8.97 S1(config)#exit

Tarea	Especificación
Configurar la interfaz de administración (SVI)	**Configuración de S2** S2(config)#int vlan4 S2(config-if)#description 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)#no shutdown S2(config-if)#ip default-gateway 10.19.8.97
Configuración del gateway predeterminado	Configure la puerta de enlace predeterminada como 10.19.8.97 para IPv4 S1(config-if)#ip default-gateway 10.19.8.97 S1(config)#exit

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

Configurar S1: La configuración del S1 incluye las siguientes tareas:

En S1 se inicia creando las VLAN asignando nombre a cada una de ellas VLAN 2 nombre Bikes, VLAN 3 nombre Trikes, VLAN 4 name Management, VLAN 5 nombre Parking, VLAN 6 nombre Native, seguido a este paso se deben crear troncos 802.1Q que utilicen la VLAN 6 nativa en las interfaces F0/1, F0/2 y F0/5 mediante el comando “interface range fa0/1, fa0/2, fa0/5”” switchport mode Access” y se crea un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2 “channel-group 2 mode active” “Creating a port-channel interface Port-channel 2”

Se realiza la configuración del Puerto de acceso host para VLAN2 verificando desde int fa 0/6 ingresando al modo switchport para ingresar a VLAN 2 y se realiza la configuración de la seguridad con el fin de permitir 3 direcciones MAC mediante el comando switchport port-security maximum 3, agora se procede a la asignación a VLAN 5, estableciendo en modo de acceso, mediante int range fa 0/3-4, fa 0/7-24, G 0/1-2.

Tabla 6 Configuración de S1

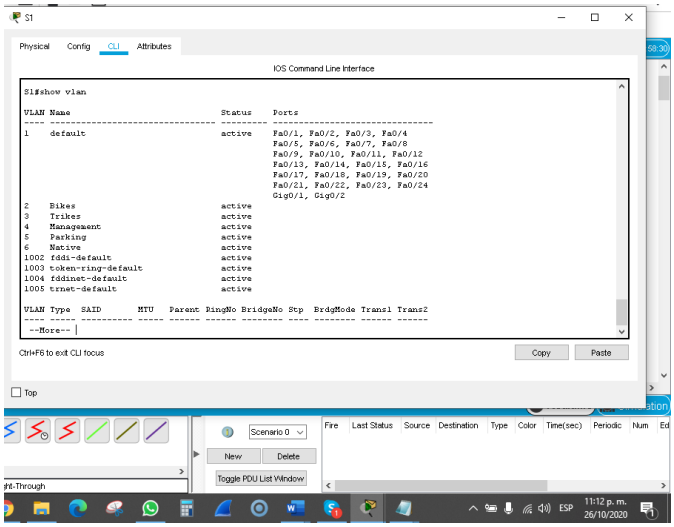
Tarea	Especificación
Crear VLAN	**VLAN 2, nombre Bikes** S1>enable S1#configure terminal S1(config)#vlan 2 S1(config-vlan)#name Bikes S1(config-vlan)#exit **VLAN 3, nombre Trikes** S1(config)#Vlan 3 S1(config-vlan)#name Trikes S1(config-vlan)#exit S1(config)# **VLAN 4, name Management** S1(config)#Vlan 4 S1(config-vlan)# S1(config-vlan)#name Management S1(config-vlan)#exit **VLAN 5, nombre Parking** S1(config)#Vlan 5 S1(config-vlan)#name Parking **VLAN 6, nombre Native** S1(config)#Vlan 6 S1(config-vlan)#name Native

Tarea	Especificación
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	Interfaces F0/1, F0/2 y F0/5 S1(config)#interface range fa0/1, fa0/2, fa0/5 S1(config-if-range)#no shutdown S1(config-if-range)#switchport mode access S1(config-if-range)#switchport mode trunk S1(config-if-range)#switchport trunk native vlan 6 S1(config-if-range)#switchport trunk encapsulation dot1q
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	Usar el protocolo LACP para la negociación S1#enable S1#configure terminal S1(config)#interface range fa0/1,fa0/2 S1(config-if-range)#channel-group 2 mode active
Configurar el puerto de acceso de host para VLAN 2	Interface F0/6 S1(config)#int fa 0/6 S1(config-if)#no shutdown S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 4 S1(config-if)#switchport access vlan 2

Tarea	Especificación
configurar la seguridad del puerto en los puertos de acceso	Permitir 3 direcciones MAC S1(config)#int fa 0/6 S1(config-if)#no shutdown S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 4 S1(config-if)#switchport access vlan 2 S1(config-if)#no shutdown S1(config-if)#exit S1(config)#int fa0/6 S1(config-if)#switchport port-security S1(config-if)#switchport port-security maximum 3 S1(config-if)#show port-security
Proteja todas las interfaces no utilizadas	Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar S1#enable S1#configure terminal S1(config)#int range fa 0/3-4, fa 0/7-24, G 0/1-2 S1(config-if-range)#no shutdown S1(config-if-range)#switchport access vlan 5 S1(config-if-range)#description puertos sin usa

En la tabla No 6 se crean las VLAN y troncos 802.1Q que utilicen la VLAN 6 nativa junto con un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2 y el puerto de acceso de host para VLAN 2 protejiendo todas las interfaces no utilizadas

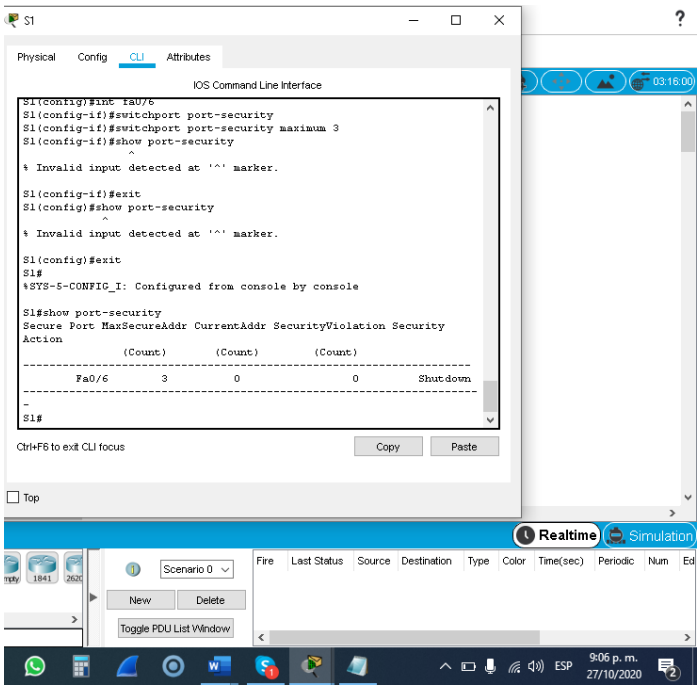
Figura 2 Comprobación de las VLAN



Fuente: Autor

Se realiza la verificación de la creación de las vlan

Figura 3 Configurar la seguridad del puerto en los puertos de acceso



Fuente: Autor

Se realiza la configuración para paermitir 3 direcciones MAC mediante el comando switchport port-security maximum 3.

Configure el S2

Entre las tareas de configuración de S2 se incluyen las siguientes:
En la presente configuración se realiza la asignación de nombre a las VLAN pues son quienes cumplirán las tareas para aumentar la eficiencia de los switch haciendo la división en dominios de broadcast, asignación de usuarios en grupos determinados aumentando la calidad del servicio solicitado.

Luego de asignar el nombre ingresando a cada una de ellas “name”. Seprocede a crear los troncos 802.1Q que utilicen la VLAN 6 nativa, permitiendo que el haya concordancia en los enlaces troncales en Fast y Gigabit Ethernet.

En el siguiente paso solicitado se creará un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2 permitiendo que la parte lógica que se compuestos de enlaces físicos rindan de mejor manera para lo cual se ingresa a la interface range fa0/1, fa0/2 de S2 y se aplica en comando channel-group 2 mode passive.

En el siguiente paso se configurará el puerto de acceso del host para la VLAN 3 ingresando a la interfaz “int fa0/18” luego se prende con el comando no shutdown Ingresando al switch “switchport mode Access - switchport access vlan 3 y salimos de la configuración mediante el comando exit.

Ahora se configura port-security en los access ports para especificar cuantas direcciones MAC se va a permitir acceder al puerto ingresando a int fa 0/18 aplicando el comando switchport port-security y el comando switchport port-security maximum 3 y verificando la configuración con el comandoshow port-security.

Para finalizar la configuración se aseguran todas las interfaces no utilizadas en R2 ingresando a int range fa 0/3-17, fa 0/19-24, G 0/1-2 no shutdown, switchport mode Access, switchport access vlan 5,description puertos sin usa y shutdown.

Tabla 7 Configuración S2

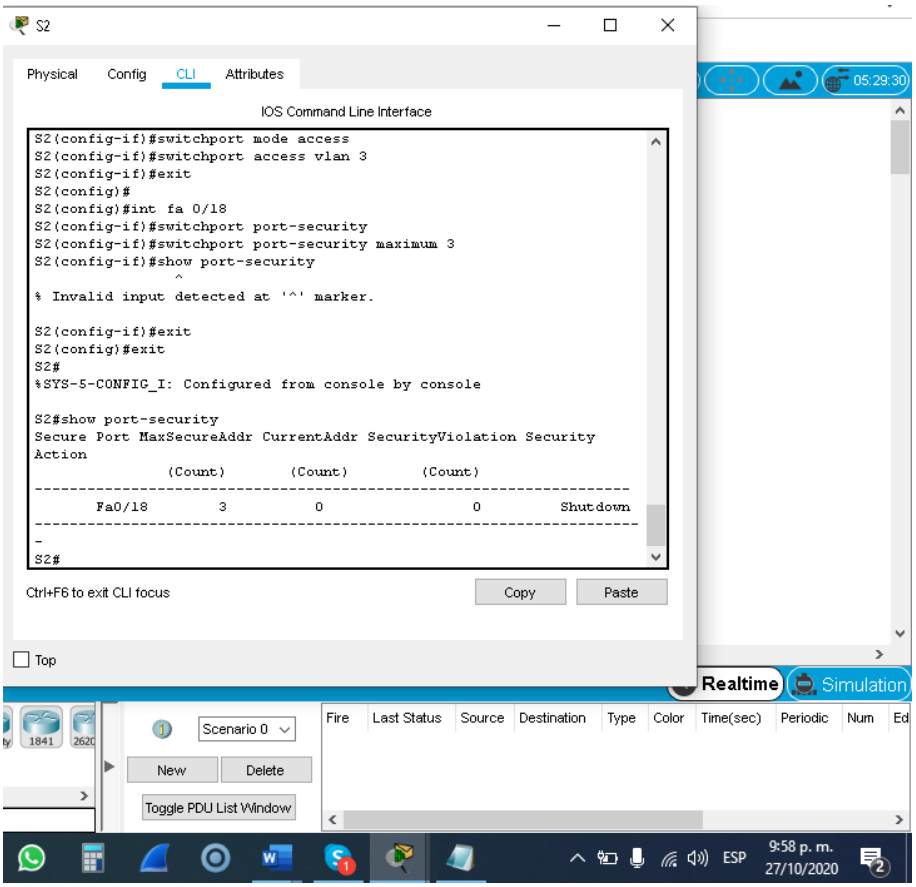
Tarea	Especificación
Crear VLAN	VLAN 2, name Bikes VLAN 3, name Trikes VLAN 4, name Management VLAN 5, nombre Parking

Tarea	Especificación
Crear VLAN	VLAN 6, nombre Native S2(config)#Vlan 2 S2(config-vlan)#name Bikes S2(config-vlan)#exit S2(config)#Vlan 3 S2(config-vlan)#name Trikes S2(config-vlan)#exit S2(config)#Vlan 4 S2(config-vlan)# S2(config-vlan)#name Management S2(config-vlan)#exit S2(config)#Vlan 5 S2(config-vlan)#name Parking S2(config-vlan)#exit S2(config)#Vlan 6 S2(config-vlan)#name Native S2(config-vlan)#exit
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	Interfaces F0/1 y F0/2 S2(config)#interface range fa0/1, fa0/2, fa0/5 S2(config-if-range)#no shutdown S2(config-if-range)#switchport mode access S2(config-if-range)#switchport mode trunk
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	S2(config-if-range)#switchport trunk native vlan 6 S2(config-if-range)#switchport trunk encapsulation dot1q
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	Usar el protocolo LACP para la negociación S2(config)#interface range fa0/1, fa0/2 S2(config-if-range)#channel-group 2 mode passive

Tarea	Especificación
Configurar el puerto de acceso del host para la VLAN 3	Interfaz F0/18 S2(config)#int fa0/18 S2(config-if)#no shutdown S2(config-if)#switchport mode access S2(config-if)#switchport access vlan 3 S2(config-if)#exit.
Configure port-security en los access ports	permite 3 MAC addresses S2(config)#int fa 0/18 S2(config-if)#switchport port-security S2(config-if)#switchport port-security maximum 3 S2(config-if)#show port-security
Asegure todas las interfaces no utilizadas.	Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar S2#enable S2#configure terminal S2(config)#int range fa 0/3-17, fa 0/19-24, G 0/1-2 S2(config-if-range)#no shutdown S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 5 S2(config-if-range)#description puertos sin usa S2(config-if-range)#shutdown

En la tabla 6 se realiza la creación de las VLAN y troncos y grupos de puertos EtherChannel de Capa 2.

Figura 4 Comprobación 3 MAC addresses



Fuente: Autor

Se realiza la verificación de la configuración de las 3 MAC addresses.

Parte 1: Configurar soporte de host

Paso 1: Configure R1

Las tareas de configuración para R1 incluyen las siguientes:

Se procede a crear los direccionamientos para IPv4 e IPv6 que dirijan el tráfico a la interfaz Loopback 0 y configurar Default Routing comando ip route 0.0.0.0 0.0.0.0 Loopback0.

Se realiza la configuración de IPv4 DHCP para VLAN 2 aplicando ip dhcp pool para la y asignando network 10.19.8.0 255.255.255.192 por intermedio de default-router 10.19.8.1, de igual manera se configura DHCP IPv4 para VLAN 3 donde es necesario crear un grupo DHCP para VLAN 3, compuesto por las últimas 10 direcciones de la subred solamente.

Se asigna el nombre de dominio ccna-b.net especificando la gateway como ubicación de interfaz del router para la subred involucrada mediante los

comandos, ip dhcp pool vlan3,network 10.19.8.64 255.255.255.224 y default-router 10.19.8.65 expluyendo las direcciones ip dhcp excluded-address 10.19.8.1 10.19.8.58 - ip dhcp excluded-address 10.19.8.65 10.19.8.84.

Tabla 8 Configuración de R1

Tarea	Especificación
Configure Default Routing	Crear rutas predeterminadas para IPv4 e IPv6 que dirijan el tráfico a la interfaz Loopback 0 R1(config)#ip route 0.0.0.0 0.0.0.0 Loopback0 %Default route without gateway, if not a point-to-point interface, may impact performance R1(config)#ipv6 route ::/0 Loopback0 R1(config)#copy running-config startup-config
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 Gateway como dirección de interfaz del router para la subred involucrada. R1(config)#ip dhcp pool vlan2 R1(dhcp-config)#network 10.19.8.0 255.255.255.192 R1(dhcp-config)#default-router 10.19.8.1 R1(dhcp-config)#exit

Tarea	Especificación
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 gateway como dirección de interfaz del router para la subred involucrada R1(config)#ip dhcp pool vlan3 R1(dhcp-config)#network 10.19.8.64 255.255.255.224 R1(dhcp-config)#default-router 10.19.8.65 R1(config)#ip dhcp excluded-address 10.19.8.1 10.19.8.58 R1(config)#ip dhcp excluded-address 10.19.8.65 10.19.8.84

En la tabla No 7 se realiza la configuración de soporte de host en R1

Configurar los servidores

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

Tabla 9 DHCP para dirección IPv4 en PC-A y PC-B

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

En la tabla No 8 se realiza la configuración de DHCP para puerta de enlace predeterminada y dirección IPv4.

Tabla 10 PC-A Network Configuration

PC-A Network Configuration	
Descripción:	Configuración red en PC-A
Dirección física	00D0.5815.6937
Dirección IP	10.19.8.59
Máscara de subred	255.255.255.192
Gateway predeterminado	10.19.8.1
Gateway predeterminado IPv6	FE80::1

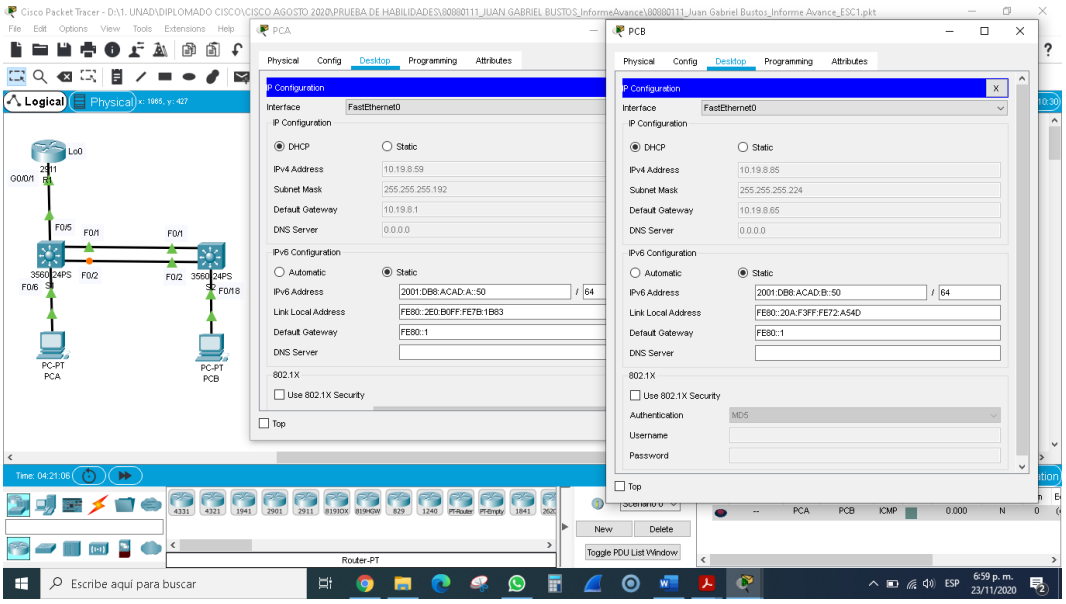
En la tabla No 9 se realiza la configuración de red en PC-A dando la dirección física, dirección IP mascara de subred y Gateway.

Tabla 11 Configuración de red de PC-B

Configuración de red de PC-B	
Descripción	Se toma la configuración por DHCP
Dirección física	000A.F372.A54D
Dirección IP	10.19.8.85
Máscara de subred	255.255.255.224
Gateway predeterminado	10.19.8.65
Gateway predeterminado IPv6	FE80::1

En la tabla No 10 se realiza la Configuración de red de PC-B Se toma DHCP.

Figura 5 Configuración PC-A y PC-B



Fuente: Autor

Se visualiza la configuración de PC-A y PC-B para que utilicen DHCP para IPv4 de tal forma que asigne estáticamente las direcciones IPv6.

Parte 2: 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:

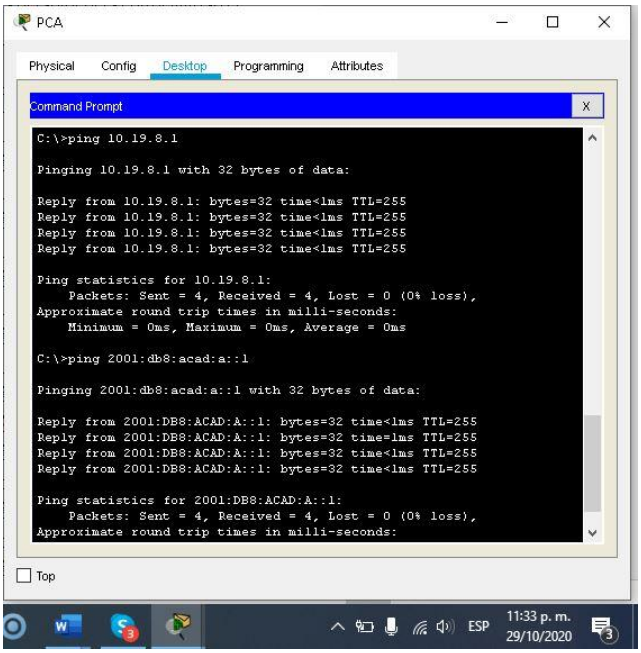
Tabla 12 Verificación de la conectividad con los dispositivos que se encuentran en la red

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

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

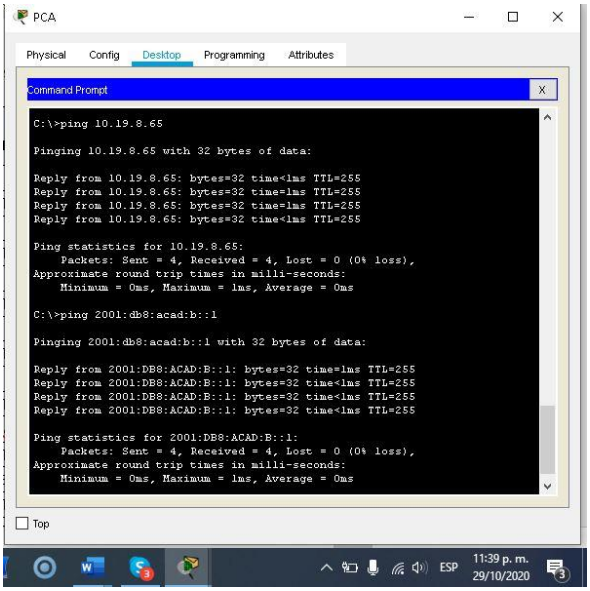
En la tabla 12 se realiza la verificación de la conectividad con los dispositivos que se encuentran en la red.

Figura 6 Conectividad desde PC-A A R1, G0/0/1.2



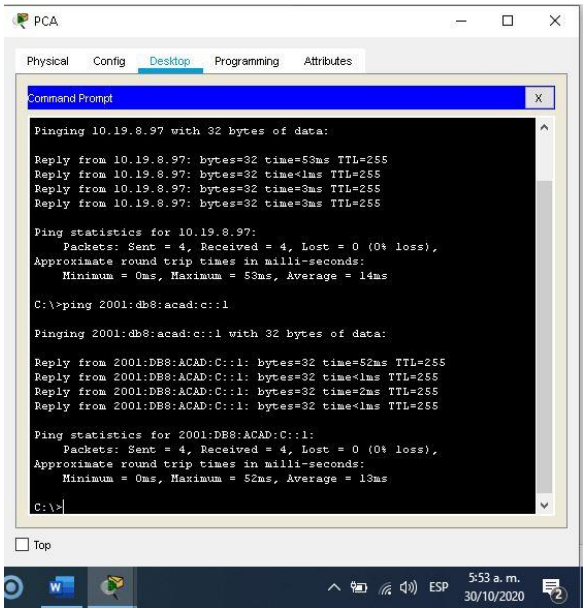
Fuente: Autor
Se realiza ping desde PC-A A R1, G0/0/1. A la dirección IP 10.19.8.65 e IPv6 2001:db8:acad:a::1de R1.

Figura 7 Conectividad desde PC-A A R1, G0/0/1.3



Fuente: Autor
Se realiza ping desde PC-A A R1, G0/0/1.3 A la dirección IP 10.19.8.65 e IPv6 2001:db8:acad:b::1 de R1.

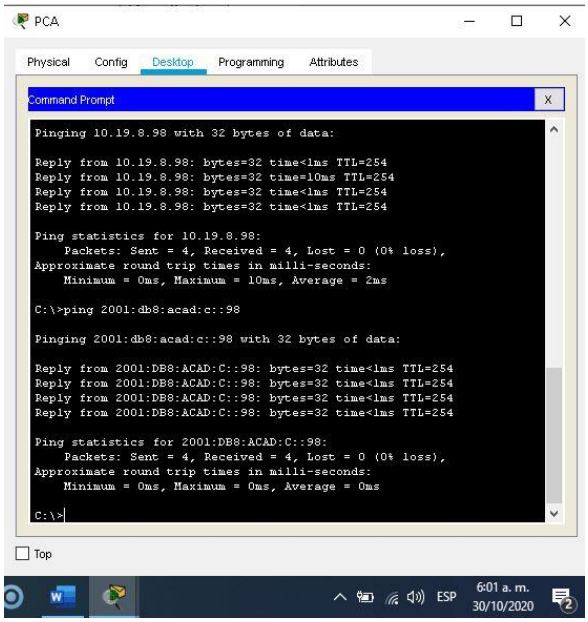
Figura 8 Conectividad desde PC-A A R1, G0/0/1.4



Fuente: Autor

Se realiza ping desde PC-A A R1, G0/0/1.4 A la dirección IP 10.19.8.97 e IPv6 2001:db8:acad:c::1 de R1.

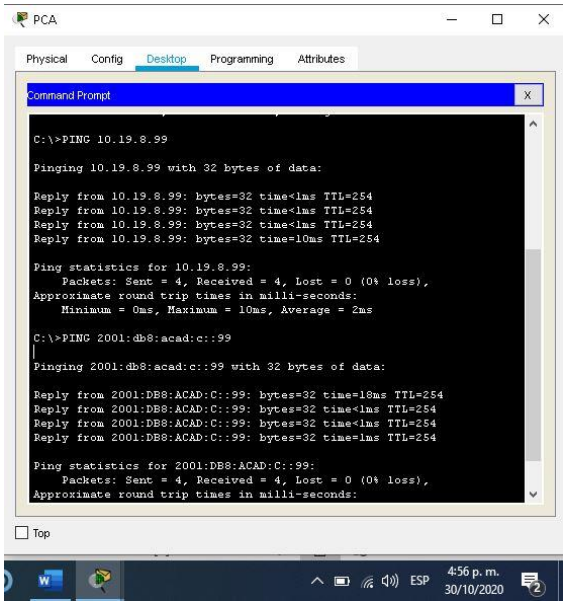
Figura 9 S1, Conectividad desde PC-A A S1 VLAN 4



Fuente: Autor

Se realiza ping desde PC-A   S1 VLAN 4 A la dirección IP 10.19.8.98 e IPv6 2001:db8:acad:c::98 de R1.

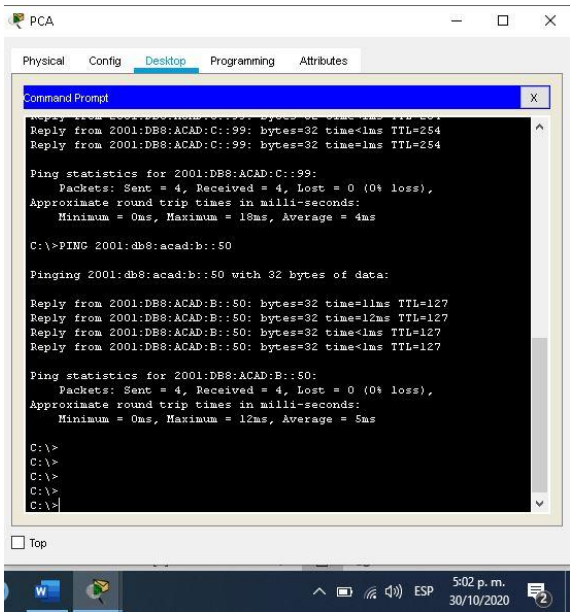
Figura 10 S2, Conectividad desde PC-A A S2 VLAN 4



Fuente: Autor

Se realiza ping desde PC-A S2 VLAN 4 A la dirección IP 10.19.8.99 e IPv6 2001:db8:acad:c::99 de R1.

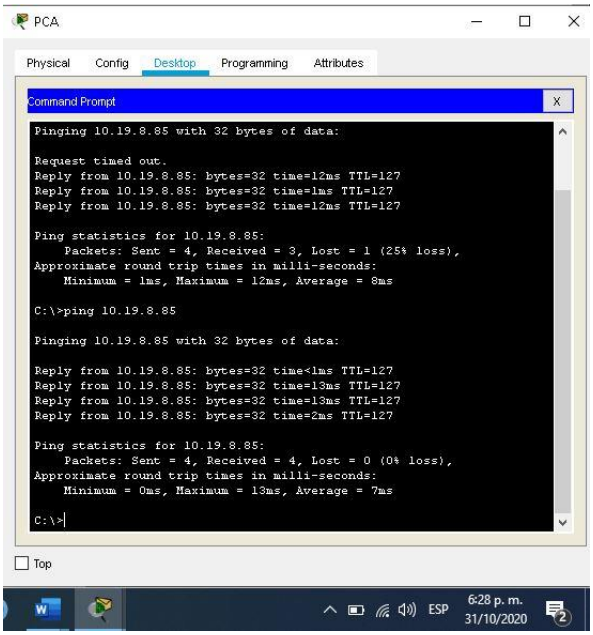
Figura 11 Conectividad desde PC-A a PC-B



Fuente: Autor

Se realiza ping desde PC-A A IPv6 2001:db8:acad:b::50.

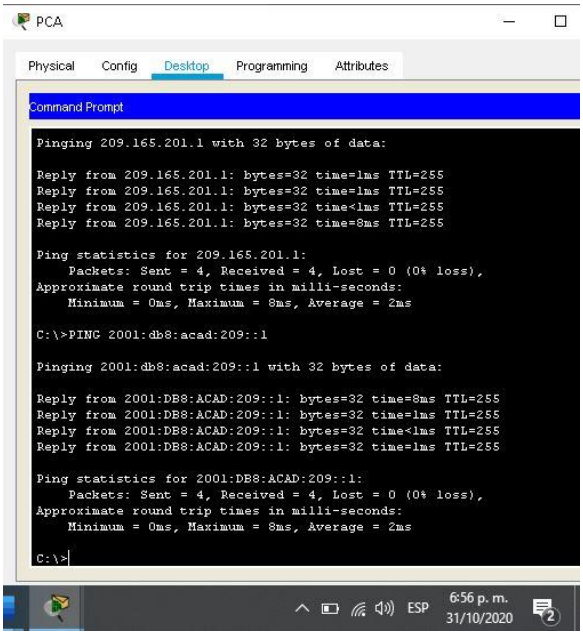
Figura 12 Conectividad desde PC-A a PC-B



Fuente: Autor

Se realiza ping desde PC-A IP address will vary.

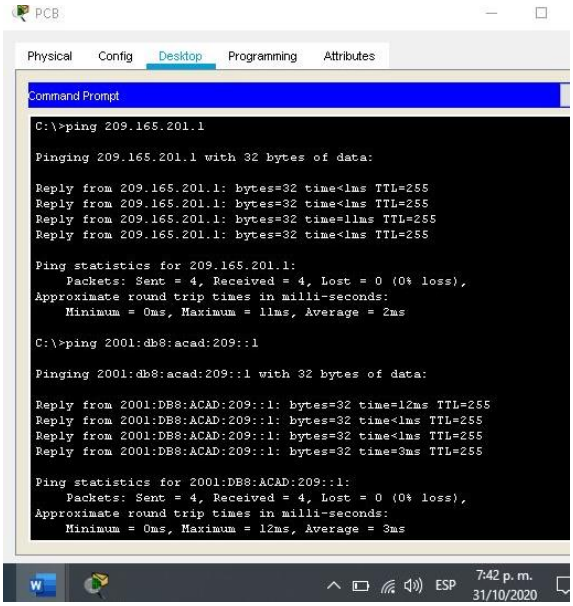
Figura 13 conexión desde PCA a R1 Bucle 0



Fuente: Autor

Se realiza ping desde PC-A R1 Bucle 0 a la dirección IP 209.165.201.1 e IPv6 2001:db8:acad:209::1.

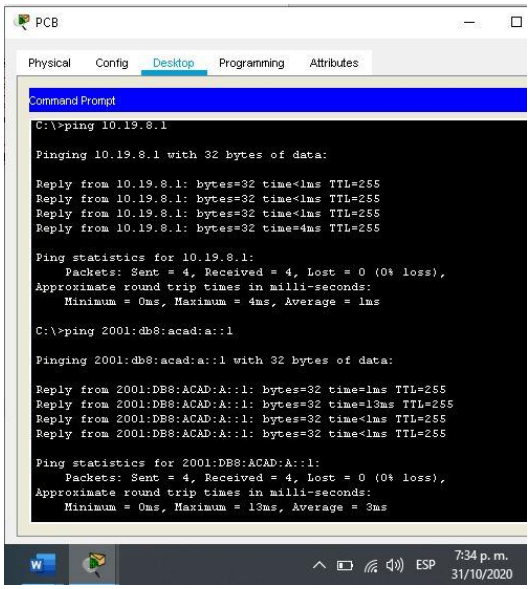
Figura 14 Conectividad desde R1 Bucle 0



Fuente: Autor

Se realiza ping desde PC-B R1 Bucle 0 a la dirección IP 209.165.201.1 e IPv6 2001:db8:acad:209::1.

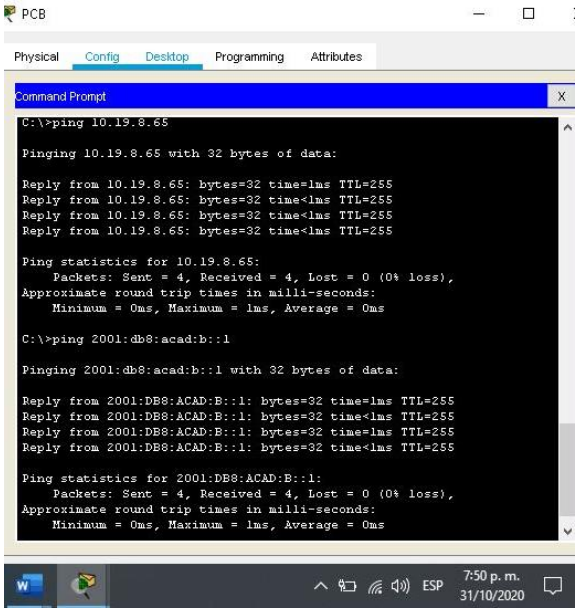
Figura 15 Conectividad R1, G0/0/1.2



Fuente: Autor

Se realiza ping desde PC-B R1, G0/0/1. A la dirección IP 2 10.19.8.1 y dirección IPv6 2001:db8:acad:a::1.

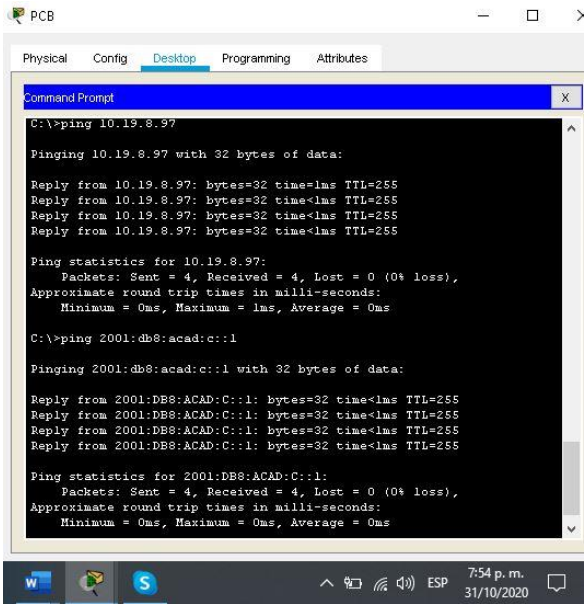
Figura 16 Conectividad R1, G0/0/1.3



Fuente:Autor

Se realiza ping desde PC-B R1, G0/0/1.3. A la dirección IP 10.19.8.65 y dirección IPv6 2001:db8:acad:b::1.

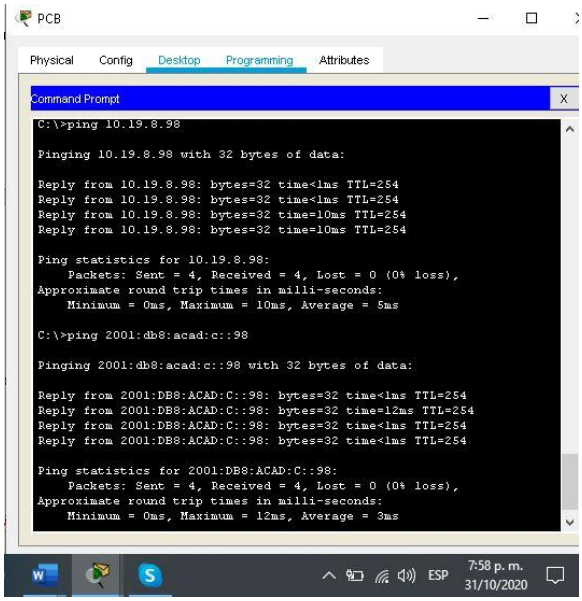
Figura 17 Conectividad R1, G0/0/1.4



Fuente: Autor

Se realiza ping desde PC-B R1, G0/0/1.4 A la dirección IP 10.19.8.97 y dirección IPv6 2001:db8:acad:b::1.

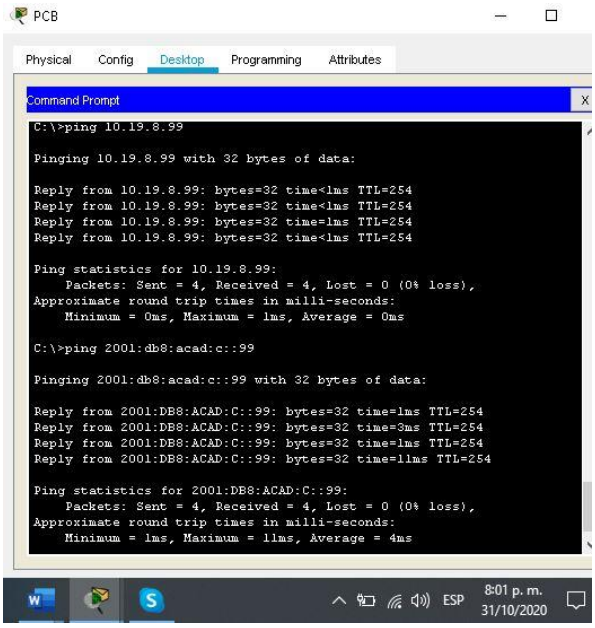
Figura 18 Conectividad S1, VLAN 4



Fuente: Autor

Se realiza ping desde PC-B S1, VLAN 4 A la dirección IP 10.19.8.98 y dirección IPv6 2001:db8:acad:c::98.

Figura 19 Conectividad S2, VLAN 4

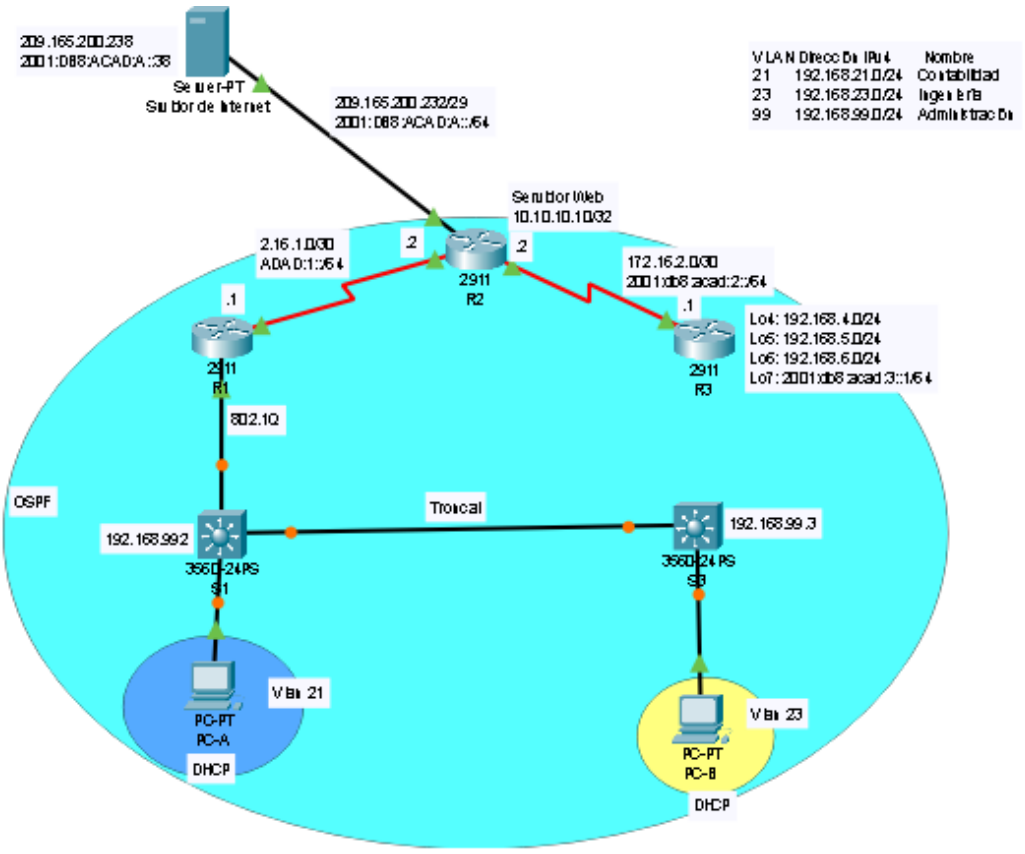


Fuente: Autor

Se realiza ping desde PC-B S2, VLAN 4A la dirección IP 10.19.8.99 y dirección IPv6 2001:db8:acad:c::99.

ESCENARIO 2

Figura 20 Topología de red Escenario 2



Fuente: Autor

Ejercicio escenario 2 realizado por estudiante Juan Bustos en Cisco Packet Tracer

Parte 1: Inicializar dispositivos

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

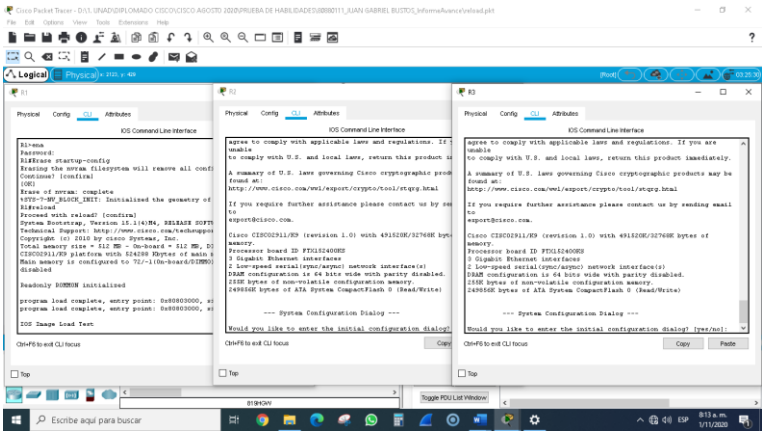
El primer paso a realizer es eliminar la configuración inicial de los routers y los switches, para ello es necesario la aplicación de los diferentes commandos aprendidos uno de ellos es erase startup-config el cual sirve para borrar o restablecer el switch y los router al valor predeterminado de fábrica, seguidamente se ejecuta el commando reload para volver a cargar todos los routers y switches.

Tabla 13 Inicializar dispositivos

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	Switch#Erase startup-config
Volver a cargar todos los routers	Switch#reload
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Switch#Erase startup-config Switch#Delete vlan.dat
Volver a cargar ambos switches	Switch#reload
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Switch#show vlan brief

En la tabla No 13 se realiza la configuración de Inicializar dispositivos mediante los comandos erase startup-config y reload.

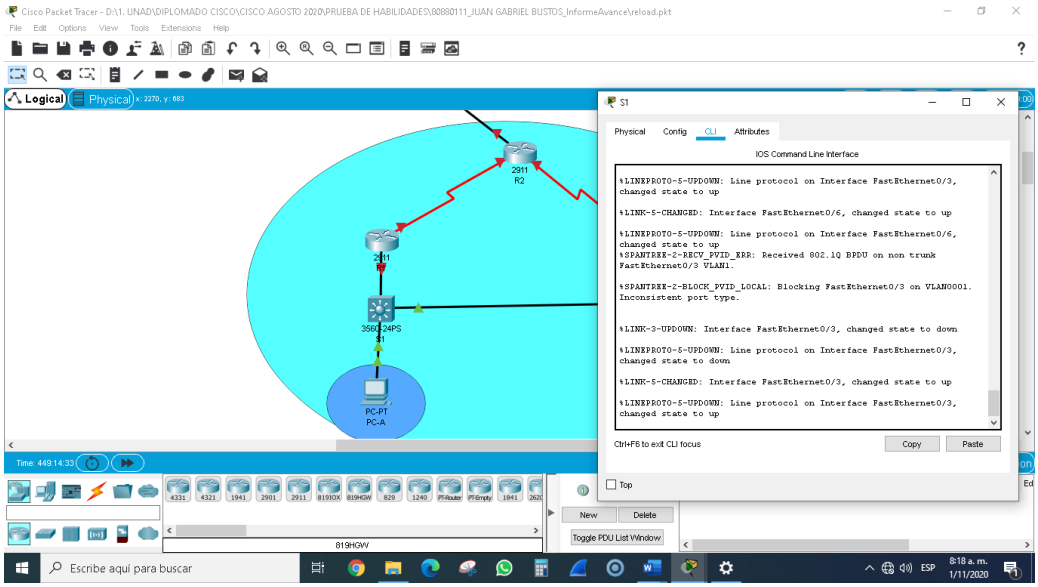
Figura 21 Eliminación de archivos y volver a cargar los routers



Fuente: Autor

Se ejecuta el comando erase startup-config y el comando reload para la eliminación de archivos y volver a cargar los routers.

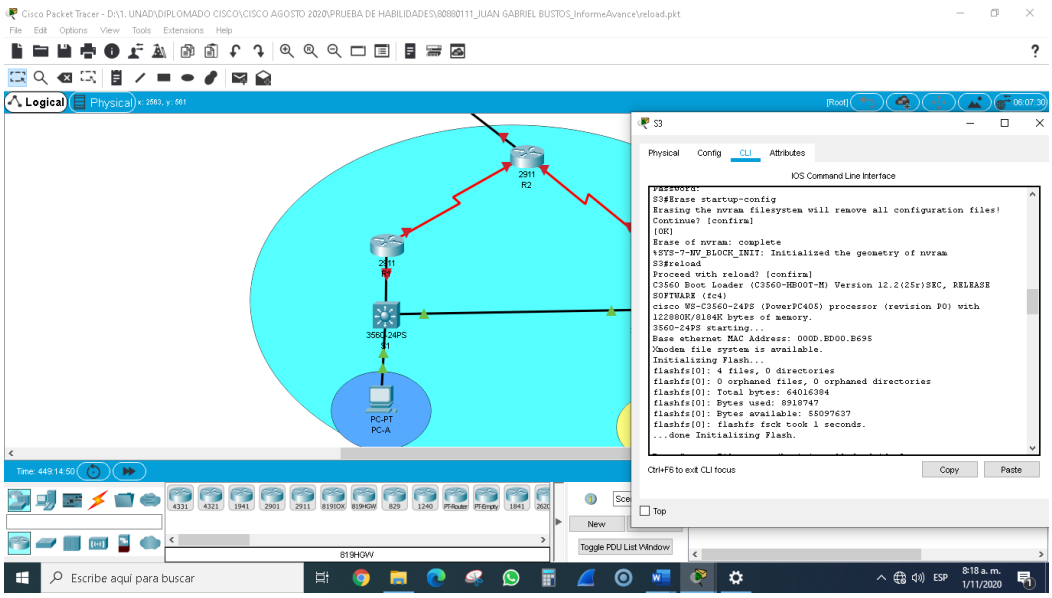
Figura 22 Eliminación de archivos y volver a cargar el Switch S1



Fuente: Autor

Se ejecuta el comando erase startup-config y el comando reload para la eliminación de archivos y volver a cargar el Switch S1.

Figura 23 Eliminación de archivos y volver a cargar el Switch S3



Fuente: Autor

Se ejecuta el comando erase startup-config y el comando reload para la eliminación de archivos y volver a cargar el Switch S1.

Parte 2: Configurar los parámetros básicos de los dispositivos

Paso 1: Configurar la computadora de Internet

Tabla 14 Configurar la computadora de Internet

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.225
Dirección IPv6/subred	2001:db8:acad:a::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:2::1

Se ingresan las direcciones para poder acceder a internet.

Paso 2 Configurar R1

R1 se configura para evitar las búsquedas de DNS no deseadas, se asigna el nombre de R1 con el commando hostname, protección por consola en modo privilegiado acceso Telnet con line vty 0 4 asignando la contraseña cisco para luego salir del modo configuración mediante el commando exit.

Ahora se cifran las contraseñas de texto no cifrado y se envia un mesaje MOTD con el comando banner motd # Se prohibe el acceso no autorizado#.

Para la Interfaz S0/0/0 se establece la descripción que es “description Conexion con R2”, la dirección IPv4 “ip address 172.16.1.1 255.255.255.252”, se establece la frecuencia de reloj en 128000 “clock rate 128000” y se activa la interfaz con el comando “no shutdown”, se configura una ruta IPv4 predeterminada de S0/0/0 con el comando “ip route 0.0.0.0 0.0.0.0 s0/0/0” e IPv6 de S0/0/0 con el comando “ ipv6 route ::/0 s0/0/0”.

Tabla 15 Configuración de R1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R1
Contraseña de exec privilegiado cifrada	R1(config)#enable secret class

Contraseña de acceso a la consola	R1(config)#line console 0
Contraseña de acceso Telnet	R1(config)#line vty 0 4 R1(config-line)#password cisco R1(config-line)#login R1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Mensaje MOTD	R1(config)#banner motd # Se prohibe el acceso no autorizado#
Interfaz S0/0/0	Establezca la descripción Establecer la dirección IPv4 Consultar el diagrama de topología para conocer la información de direcciones Establecer la dirección IPv6 Consultar el diagrama de topología para conocer la información de direcciones Establecer la frecuencia de reloj en 128000 Activar la interfaz R1(config)#int s0/0/0 R1(config-if)#description Conexion con 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
Rutas predeterminadas	Configurar una ruta IPv4 predeterminada de S0/0/0 Configurar una ruta IPv6 predeterminada de S0/0/0 R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0 R1(config)#ipv6 route ::/0 s0/0/0

En la tabla No 15 se realiza la configuración basica de R1, incluyendo interfaces y rutas predeterminadas.

Paso 3 Configurar R2

La configuración en R2 incluye las siguientes tareas:

Para la configuración en R2 se desactiva DNS que sirve para evitar las búsquedas de DNS no deseadas, se asigna el nombre de R2 con el commando hostname, y se ejecuta la protección por consola.

Ahora se aplica el comando para cifrar las contraseñas de texto no cifrado y se envia un mesaje MOTD con el comando banner motd # Se prohibe el acceso no autorizado#.

Ahora se aplica el comando service password-encryption para cifrar las contraseñas de texto no cifrado y se envia un mesaje MOTD # Se prohibe el acceso no autorizado#.

En la int S0/0/0 se establece la descripción que es “description Conexion con R2”, la dirección IPv4 “ip address 172.16.1.2 255.255.255.252”, se establece la dirección IPv6 2001:db8:acad:1::2/64 por ultimo se prende el router mediante el comando no shutdown.

En la interfaz S0/0/1 se establece la descripción con “description Connection to R3”, se asigna la dirección IPv4 “ip address 172.16.2.2 255.255.255.252” se usa la primera dirección disponible en la subred con “ipv6 address 2001:db8:acad:2::2/64”, se asigna la frecuencia de reloj en 128000 con “clock rate 128000” y por ultimo se activa la interfaz con el comando “no shutdown”.

En la interfaz G0/0 (simulación de Internet) se da la “description Connection to Internet” se asigna la dirección IPv4 con “ip address 209.165.200.233 255.255.255.248” se establece la dirección IPv6 “ipv6 address 2001:db8:acad:a::1/64” y se active la interfaz con “no shutdown”.

En la interfaz loopback 0 (servidor web simulado) se identifica el servidor “description Simulated Web Server” y se assigna la dirección IPv4 con “ip address 10.10.10.10 255.255.255.255” se realiza la configuración de una ruta IPv4 predeterminada de G0/0 con “ip route 0.0.0.0 0.0.0.0 g0/0” Tambien se configura una ruta IPv6 de G0/0 con -2 ipv6 route ::/0 g0/0”.

Tabla 16 Configuración de R2

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router>enable Router#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Router(config)#no ip domain-lookup
Nombre del router	R2 - Router(config)#hostname R2
Contraseña de exec privilegiado cifrada	Class R2(config)#enable secret class
Contraseña de acceso a la consola	Cisco R2(config)#line console 0 R2(config-line)#password cisco R2(config-line)#login R2(config-line)#exit
Contraseña de acceso Telnet	Cisco R2(config)#line vty 0 4 R2(config-line)#password cisco R2(config-line)#login R2(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R2(config)#service password-encryption
Habilitar el servidor HTTP	El paso de Habilitar el servidor HTTP no se realiza ya que packet tracer no admite el commando para realizer este punto.
Mensaje MOTD	R2(config)#banner motd %Se prohibe el acceso no autorizado.%.

Interfaz S0/0/0	Establezca la descripción Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz R2(config)#int s0/0/0 R2(config-if)#description Conexion a R1 R2(config-if)#ip address 172.16.1.2 255.255.255.252 R2(config-if)#ipv6 address 2001:db8:acad:1::2/64 R2(config-if)#no shutdown
Interfaz S0/0/1	Establecer la descripción Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Establecer la frecuencia de reloj en 128000. Activar la interfaz 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 This command applies only to DCE interfaces R2(config-if)#no shutdown

Interfaz G0/0 (simulación de Internet)	Establecer la descripción. Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Establezca la dirección IPv6. Utilizar la primera dirección disponible en la subred. Activar la interfaz 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
Interfaz loopback 0 (servidor web simulado)	Establecer la descripción. Establezca la dirección IPv4. 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
Ruta predeterminada	Configure una ruta IPv4 predeterminada de G0/0. Configure una ruta IPv6 predeterminada de G0/0. R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0 %Default route without gateway, if not a point-to-point interface, may impact performance R2(config)#ipv6 route ::/0 g0/0

En la tabla No 16 se realiza la configuración de R2 desde su configuración básica, interfaces, loopback y ruta predeterminada.

Nota: El paso de Habilitar el servidor HTTP no se realiza ya que packet tracer no admite el commando para realizer este punto.

Paso 4 Configurar R3

Para la configuración de R3 se desactiva la busqueda DNS mediante el commando no ip domain-lookup que sirve para evitar las búsquedas de DNS no deseadas, se asigna el nombre de R3 con el comando hostname, protección por consola con la contraseña cifrada con el comando enable secret class y line console 0 con el acceso Telnet con line vty 0 4 asignando la contraseña cisco para luego salir del modo configuración mediante el commando exit.

Ahora se aplica el comando service password-encryption que se emplea para configurar contraseñas en conexiones de consola en modo usuario y Telnet y se envia un mesaje MOTD de prohibicion de acceso no autorizado.

Para la Int S0/0/1 se establece la descripción que es “description Conexion con R2”, la dirección IPv4 “ip address 172.16.2.1 255.255.255.252”, se establece la dirección IPv6 2001:db8:acad:2::1/64 por ultimo se prende el router mediante el comando no shutdown.

Se crea la interfaz loopback 4 al ciual sde le asigna la ip address 192.168.4.1 255.255.255.0, interfaz loopback 5 ip address 192.168.5.1, loopback 6 ip address 192.168.6.1 255.255.255.0, loopback 7 ipv6 address 2001:DB8:ACAD:3::1/64,para terminar la configuración de R3 se crean rutas predeterminadas.

Tabla 17 Configuración de R3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router>enable Router#configure terminal Router(config)#no ip domain-lookup
Nombre del router (R3)	Router(config)#hostname R3
Contraseña de exec privilegiado cifrada	Class R3(config)#enable secret class
Contraseña de acceso a la consola (cisco)	R3(config)#line console 0 R3(config-line)#password cisco R3(config-line)#login
Contraseña de acceso Telnet (cisco)	R3(config-line)#line vty 0 4 R3(config-line)#password cisco R3(config-line)#login
Cifrar las contraseñas de texto no cifrado	R3(config)#service password-encryption

Mensaje MOTD	Se prohíbe el acceso no autorizado. R3(config)# banner motd # Se prohíbe el acceso no autorizado.#
Interfaz S0/0/1	Establecer la descripción Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz R3(config)#int s0/0/1 R3(config-if)#description Connection to R2 R3(config-if)#ip address 172.16.2.1 255.255.255.252 R3(config-if)#ipv6 address 2001:db8:acad:2::1/64 R3(config-if)#no shutdown
Interfaz loopback 4	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. R3(config)#int loopback 4 R3(config-if)#ip address 192.168.4.1 255.255.255.0 R3(config-if)#exit
Interfaz loopback 5	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. R3(config)#int loopback 5 R3(config-if)# R3(config-if)#ip address 192.168.5.1 255.255.255.0 R3(config-if)#exit
Interfaz loopback 6	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. R3(config)#int loopback 6 R3(config-if)#ip address 192.168.6.1 255.255.255.0 R3(config-if)#exit

Interfaz loopback 7	Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. R3(config)#int loopback 7 R3(config-if)# R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64 R3(config-if)#exit
Rutas predeterminadas	R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1 %Default route without gateway, if not a point-to-point interface, may impact performance R3(config)#ipv6 route ::/0 s0/0/1 R3(config)#

En la tabla No 17 se configura R3 desde su configuración básica, interfaces, loopback y ruta predeterminada.

Paso 5 Configurar S1

Para la configuración en S1 se desactivan las busquedas DNS mediante el commando no ip domain-lookup que sirve para evitar las búsquedas de DNS no deseadas, se asigna el nombre de a S1 con el comando hostname, protección por consola con la contraseña cifrada, se accede a la consola line console 0 que permite ingresar al Telnet con line vty 0 4 asignando la contraseña cisco y cifrar las contraseñas de texto no cifrado empleando“service password-encryption” y luego salir del modo configuración mediante el commando exit.

Se envia un mesaje MOTD de la prohibicion de accesos no autorizados.

Tabla 18 Configuración de S1

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Switch>enable Switch#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#no ip domain-lookup
Nombre del switch	S1 Switch(config)#hostname S1

Contraseña de exec privilegiado cifrada	Class S1(config)#enable secret class
Contraseña de acceso a la consola (Cisco)	S1(config)#line console 0 S1(config-line)#password cisco S1(config-line)#login S1(config-line)#exit
Contraseña de acceso Telnet (Cisco)	S1(config)#line vty 0 4 S1(config-line)#password cisco S1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado. banner motd #Se Se prohíbe el acceso no autorizado.#

En la tabla No 18 se realoiza la configuración de R2 desde su configuración básica, interfaces, loopback y ruta predeterminada.

Paso 6 Configurar S3

Para la configuración de S3 se desactivan busquedas DNS para evitar las búsquedas de DNS no deseadas, se asigna el nombre de S3 con el comando hostname, es necesaria la protección por consola empleando el comando para asignar parametros de usuario privilegiado cifrada en este caso enable secret class se accede a la consola mediante line console 0 y de acceso Telnet con line vty 0 4 asignando la contraseña cisco y cifrar las contraseñas de texto no cifrado con el comando service password-encryption,ahora se envia un mesaje MOTD con el comando banner motd .

Tabla 19 Configuración de S3

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

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

En la tabla No 19 se realiza la configuración inicial de S3, uso de contraseñas y mensaje MOTD.

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:

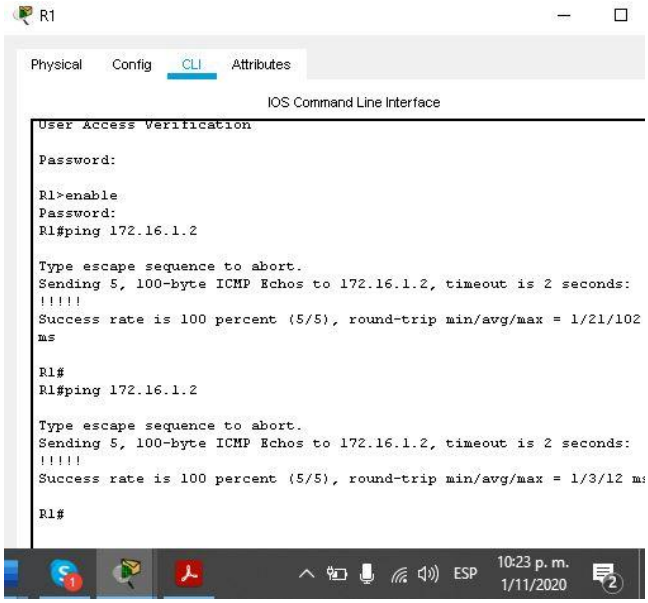
Tabla 20 verificación de la red conectividad con cada dispositivo

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

Se realiza la verificación de la red conectividad con cada dispositivo en R1, R2 Y PC de internet.

Nota: Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

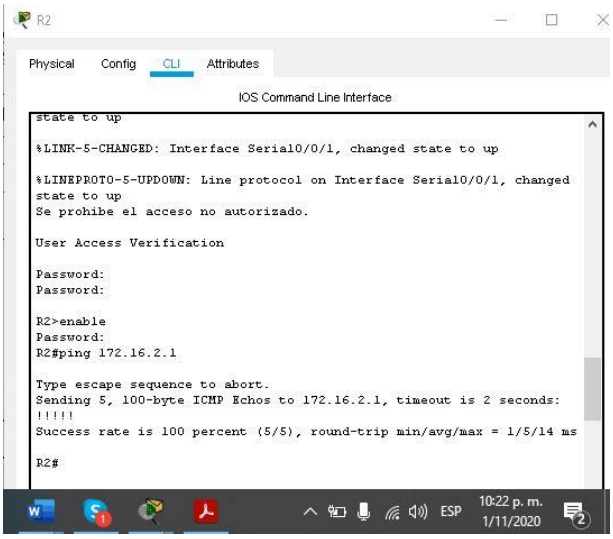
Figura 24 Ping desde R1 a R2, S0/0/0



Fuente: Autor

Se realiza Ping desde R1 a R2, S0/0/0 a la dirección IP 172.16.1.2 dando exitoso resultado.

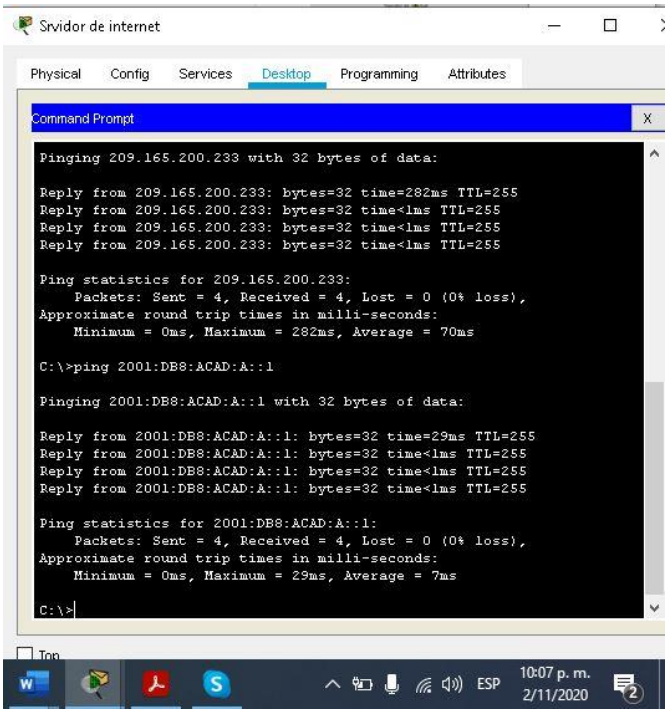
Figura 25 Ping desde R2 a R3, S0/0/1



Fuente: Autor

Se realiza Ping desde R2 a R3, S0/0/1a la dirección IP 172.16.2.1 dando exitoso resultado.

Figura 26 ping desde servidor a puerta de enlace predeterminada



Fuente: Autor

Se realiza ping desde PC de Internet a la Puerta de enlace predetermianda a la direccion IP 209.165.200.233.

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

Paso 1 Configurar S1

Nuevamente se ingresa a S1 para crear la database de las VLAN según la asignación dada y se ingresa en modo privilegiado en configure terminal se asignan los nombres: vlan 21 (name contabilidad), vlan 23 (name ingenieria), vlan 99 (name Administracion), en la vlan 99 se le asigna la dirección ip address 192.168.99.2 255.255.255.0 por último se enciende con no shutdown.

En la primera dirección IPv4 de la subred se establece como Puerta de enlace predetermianda mediante el comando “ip default-gateway 192.168.99.1”

Ahora se procee a forzará el enlace troncal en int F0/3 empleando la VLAN 1 como nativa, para ello ingresamos a la interface f0/3 se aplica el comando switchport mode trunk que se emplea para cambiar el modo de enlace del puerto de acceso a trunk para permitir su operación como puerto tronca, en este caso a para la vlan 1, la misma operación se repite para la int F0/5.

Se configuran los puertos restantes como puertos de acceso “int range f0/1-2, f0/4, f0/6-24, g0/1-2” – “switch mode Access” asi mismo se asigna la F0/6 a la VLAN 21 mediante los commandos int f0/6 - switchport mode access - witchport access vlan 21.

Para terminar la configuración de S1 se debenapagar todos los puertos sin usar y shutdown para terminar el proceso.

Tabla 21 Configuración de las VLAN en S1

Elemento o tarea de configuración	**Especificación**
Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para topología para crear y nombrar cada una de las VLAN que se indican: S1>enable Password: S1#enable S1#configure terminal Enter configuration commands, one per line. End with CNTL/Z.
Crear la base de datos de VLAN	S1(config)#vlan 21 S1(config-vlan)#name contabilidad S1(config-vlan)#exit S1(config)#vlan 23 S1(config-vlan)#name ingenieria S1(config-vlan)#exit S1(config)#vlan 99 S1(config-vlan)#name Administracion S1(config-vlan)#exit
Asignar la dirección IP de administración.	Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S1 en el diagrama de topología S1(config)#int vlan 99 S1(config-if)#ip address 192.168.99.2 255.255.255.0 S1(config-if)#no shutdown S1(config-if)#Description Vlan Administracion
Asignar el gateway predeterminado	Asigne la primera dirección IPv4 de la subred como el gateway predeterminado. S1(config)#ip default-gateway 192.168.99.1

Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa S1#conf t S1(config)#int f0/3 S1(config-if)#switchport mode trunk Command rejected: An interface whose trunk encapsulation is "Auto" can not be configured to "trunk" mode. S1(config-if)#switchport trunk native vlan 1 S1(config-if)#exit S1(config)#
Forzar el enlace troncal en la interfaz F0/5	Utilizar la red VLAN 1 como VLAN nativa S1(config)#int f0/5 S1(config-if)#switchport mode trunk Command rejected: An interface whose trunk encapsulation is "Auto" can not be configured to "trunk" mode. S1(config-if)#switchport trunk native vlan 1 S1(config-if)#exit
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range S1(config)#int range f0/1-2, f0/4, f0/6-24, g0/1-2 S1(config-if-range)#switch mode Access S1(config-if-range)#exit
Asignar F0/6 a la VLAN 21	S1(config)#interface f0/6 S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 21 S1(config-if)#exit
Apagar todos los puertos sin usar	S1(config-if)#int range fa0/1-2, fa0/4, fa0/7-24, g0/1-2 S1(config)#shutdown S1(config-if-range)#exit S1(config)#exit

En la tabla No 21 se realiza la configuración de S1 empezando con la creación de la base de datos de las VLAN, asignación de IP y Forzar el enlace troncal en las interfaces.

Paso 2: Configurar el S3

Nuevamente se ingresa a S3 para crear la database de las VLAN de acuerdo a la asignación dada y se ingresa en modo privilegiado en configure terminal se asignan los nombres: vlan 21, vlan 23 y vlan 99, en la vlan 99 se le asigna la dirección ip address 192.168.99.3 255.255.255.0 por último se enciende con no shutdown.

Se asigna la primera dirección IP en la subred como puerta de enlace predeterminada quedando la ip de la siguiente manera: 192.168.99.1.

Ahora se procede a forzar el enlace troncal en la int F0/3 empleando la red VLAN 1 como nativa, para ello ingresamos a la f0/cambiando el modo de enlace del puerto de acceso a trunk para permitir su operación como puerto troncal.

Se deben configuran el restante de los puertos como puertos de acceso “int range f0/1-2, f0/4, f0/6-24, g0/1-2” – “switch mode Access” asi mismo se asigna la F0/18 a la VLAN 21 mediante los commandos interface f0/18 - switchport mode access - witchport access vlan 21.

Para terminar la configuración de S3 se deben apagar los puertos que no se encuentran en uso aplicando int range f0/1-2, f0/4-17, f0/19-24, g0/1-2 y shutdown y exit para terminar el proceso.

Tabla 22 Creación de las VLAN en S3

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para topología para crear cada una de las VLAN que se indican Dé nombre a cada VLAN. 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

Asignar la dirección IP de administración	Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S3 en el diagrama de topología S3(config)#int vlan 99 S3(config-if)# %LINK-5-CHANGED: Interface Vlan99, changed state to up S3(config-if)#ip address 192.168.99.3 255.255.255.0 S3(config-if)#no shutdown S3(config-if)#exit
Asignar el gateway predeterminado.	Asignar la primera dirección IP en la subred como gateway predeterminado. S3(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3 (Utilizar la red VLAN 1 como VLAN nativa)	S3(config)#int f0/3 S3(config-if)#switchport mode trunk Command rejected: An interface whose trunk encapsulation is "Auto" can not be configured to "trunk" mode. S3(config-if)#switchport trunk native vlan 1 S3(config-if)#
Configurar el resto de los puertos como puertos de acceso (Utilizar el comando interface range)	int range f0/1-2, f0/4-24, g0/1-2 S3(config-if-range)#switchport mode access
Asignar F0/18 a la VLAN 21	S3(config)#interface f0/18 S3(config-if)#switchport mode access S3(config-if)#switchport access vlan 21 S3(config-if)#exit
Apagar todos los puertos sin usar	S3(config)#interface range f0/1-2, f0/4-17, f0/19-24, g0/1-2 S3(config-if-range)#shutdown S3(config-if-range)#exit

En la tabla No 22 Se realiza la configuración de S3 empezando con la creación de la base de datos de las VLAN, asignación de IP y Forzar el enlace troncal en las interfaces.

Paso 3: Configurar R1

En R1 ingresamos a la subinterfaz 802.1Q .21 en G0/1, descripción LAN "Contabilidad" y se le asigna a la VLAN 21 como primera disponible int g0/1.21, "description Contabilidad LAN", "encapsulation dot1q 21" y se le asigna la ip address 192.168.21.1 255.255.255.0.

Se realiza la configuración de la subinterfaz 802.1Q .23 en G0/1 haciendo la respectiva descripción asignandola a la VLAN 23 la primera dirección disponible a esta interfaz mediante el comando "int g0/1.23 con dirección ip 192.168.23.1 255.255.255.0, se repite el procedimienro para la subinterfaz 802.1Q .99 se hace la encapsulación dot1q 99 y la asignación de la dirección ip address 192.168.99.2 255.255.255.0.

La activación de la interfaz G0/1en R1se realiza ingresando a la interfaz g0/1 y aplicando el comando "no shutdown".

Tabla 23 Configuración de las subinterfaces

Elemento o tarea de configuración	**Especificación**
Configurar la subinterfaz 802.1Q .21 en G0/1	Descripción: LAN de Contabilidad Asignar la VLAN 21 Asignar la primera dirección disponible a esta interfaz R1(config)#int g0/1.21 R1(config-subif)#description Contabilidad LAN R1(config-subif)#encapsulation dot1q 21 R1(config-subif)#ip address 192.168.21.1 255.255.255.0 R1(config-subif)#exit
Configurar la subinterfaz 802.1Q .23 en G0/1	Descripción: LAN de Ingeniería Asignar la VLAN 23 Asignar la primera dirección disponible a esta interfaz R1(config)#int g0/1.23 R1(config-subif)#description Ingeniera LAN R1(config-subif)#encapsulation dot1q 23 R1(config-subif)#ip address 192.168.23.1 255.255.255.0 R1(config-subif)#exit

Configurar la subinterfaz 802.1Q .99 en G0/1	Descripción: LAN de Administración Asignar la VLAN 99 Asignar la primera dirección disponible a esta interfaz R1(config)#int g0/1.99 R1(config-subif)#description Administracin LAN R1(config-subif)#encapsulation dot1q 99 R1(config-subif)#ip address 192.168.99.2 % Incomplete command. R1(config-subif)#ip address 192.168.99.2 255.255.255.0 R1(config-subif)#exit
Activar la interfaz G0/1	R1(config)#int g0/1 R1(config-if)#no shutdown R1(config-subif)#exit R1(config)#exit

En la tabla No 23 se realiza la configuración de las subinterfaces en R1.

Paso 4: Verificar la conectividad de la red

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

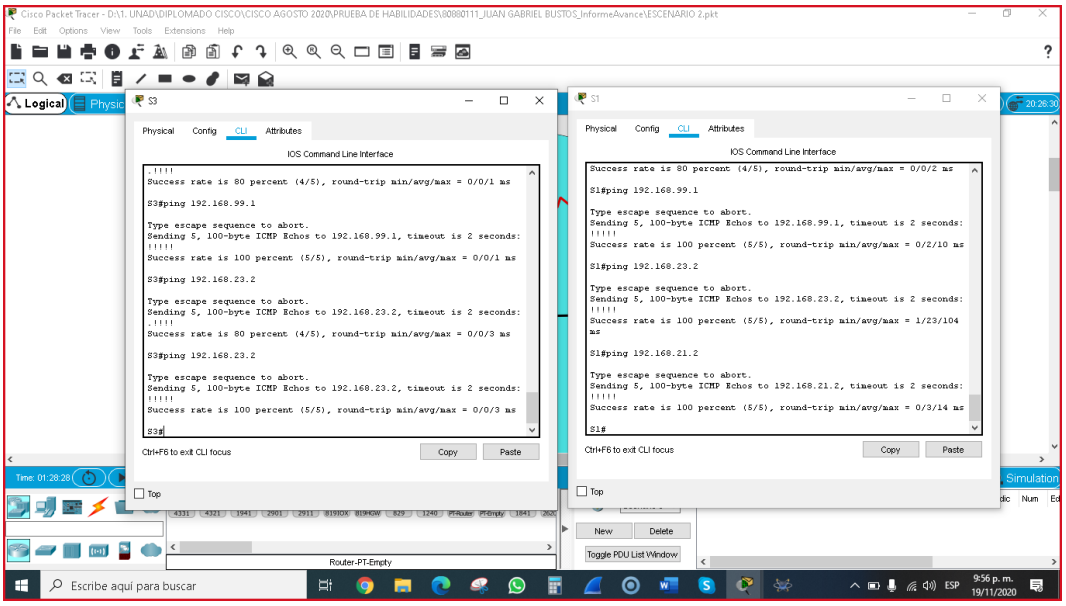
Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 24 Verificación de la conectividad de la red

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	Ping ok
S3	R1, dirección VLAN 99	192.168.99.1	Ping ok
S1	R1, dirección VLAN 21	192.168.21.2	Ping ok
S3	R1, dirección VLAN 23	192.168.23.2	Ping ok

En la tabla No 24 se realiza la verificación de la conectividad de la red.

Figura 27 Verificación la conectividad de la red



Fuente: Autor

Se realiza la comprobación de la conectividad desde S1 y S3 de acuerdo a lo solicitado en la tabla de verificación de la conectividad de la red.

Parte 4: Configurar el protocolo de routing dinámico OSPF

Configurar OSPF en el R1

Se configura el protocolo OSPF para se active en el router todas aquellas direcciones de red asi como informaciones de areas de host que pueden intervenir en dicha red ingresando al router en modo configuración con el comando “router ospf 1” se asignan todas las redes conectadas directamente en R1partiendo desde la identificación mediante los commandos “router-id 1.1.1.1.

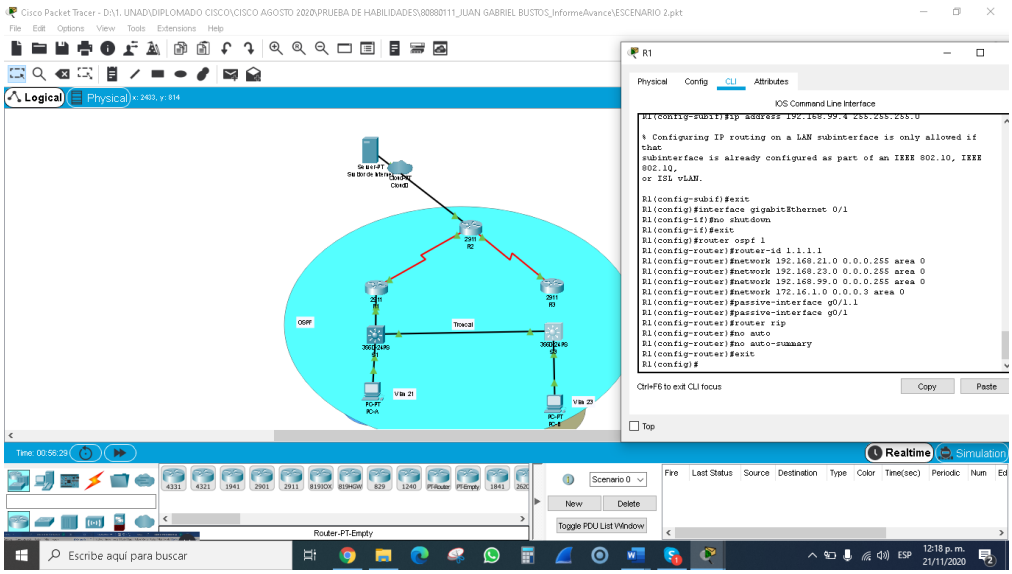
En el siguiente paso se debe establecer todas las interfaces LAN como pasivas en g0/1.1 mediante el comado “passive-interface g0/1.1 - passive-interface g0/1.

Tabla 25 Configuración OSPF en el R1

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R1(config)#router ospf 1
Anunciar las redes conectadas directamente	Asigne todas las redes conectadas directamente. R1(config-router)#router-id 1.1.1.1 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 R1(config-router)#network 172.16.1.0 0.0.0.3 area 0
Establecer todas las interfaces LAN como pasivas	R1(config-router)#passive-interface g0/1.1 R1(config-router)#passive-interface g0/1
Desactive la sumarización automática	R1(config-router)#router rip R1(config-router)#no auto R1(config-router)#no auto-summary

En la tabla No 25 se realiza la Configuración OSPF en el R1.

Figura 28 Configuración de R1



Fuente: Autor

Se realiza la configuración de R1 con los parámetros de OSPF área 0.

Paso 2: Configurar OSPF en el R2

En este paso se configura OSPF asignando el ID 2.2.2.2 y se anuncian las redes que se encuentran conectadas de forma directa empleando el comando log-adjacency-changes.

En el siguiente paso se debe establece la int LAN (loopback) como pasiva en la interface g0/1 para que evite transmisiones de mensajes de routing por medio de la interfaz del router, permitiendo anunciar dicha red a otros routers, se realiza mediante el comando passive-interface g0/1.

Se hace la desactivación de la sumarización automática ingresando al router ospf 1 - router rip - no auto-summary.

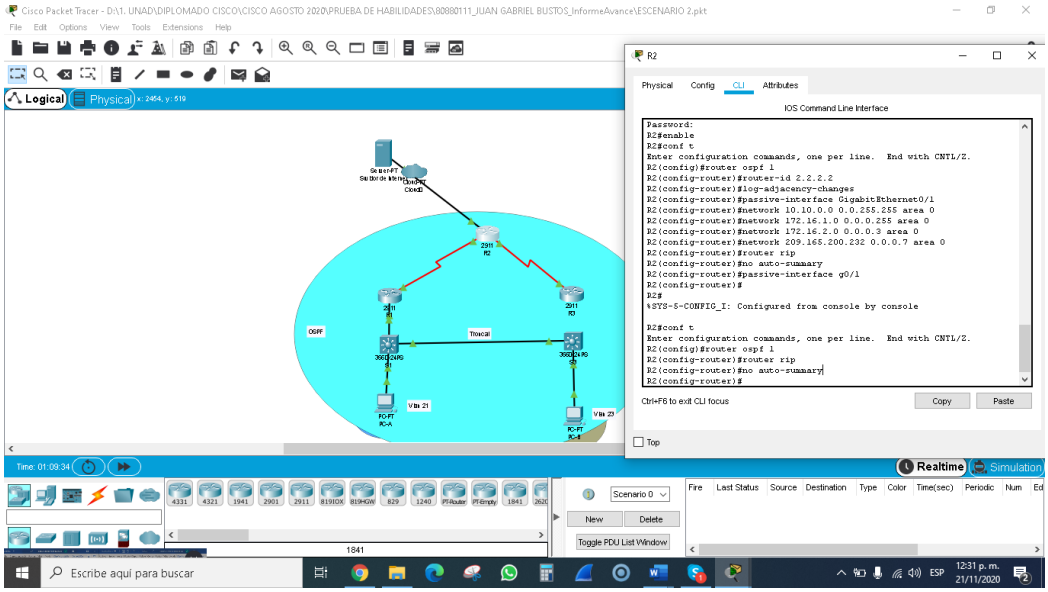
Tabla 26 Configuración OSPF en el R2

Elemento o tarea de configuración	**Especificación**
Configurar OSPF área 0	R2(config)#router ospf 1 R2(config-router)#router-id 2.2.2.2
Anunciar las redes conectadas directamente	**Nota:** Omitir la red G0/0. R2(config-router)#log-adjacency-changes R2(config-router)#passive-interface GigabitEthernet0/1 R2(config-router)#network 10.10.0.0 0.0.255.255 area 0 R2(config-router)#network 172.16.1.0 0.0.0.255 area 0 R2(config-router)#network 172.16.2.0 0.0.0.3 area 0 R2(config-router)#network 209.165.200.232 0.0.0.7 area 0 R2(config-router)#router rip R2(config-router)#no auto-summary
Establecer la interfaz LAN (loopback) como pasiva	R2(config-router)#passive-interface g0/1

Desactive la sumarización automática.	R2(config)#router ospf 1 R2(config-router)#router rip R2(config-router)#no auto-summary R2(config-router)#

En la tabla No 26 se realiza la Configuración OSPF en el R2.

Figura 29 Configuración R2



Fuente: Autor

Se hacela configuracion de R2 junto con la desactivación de la sumarización automática ingresando al router ospf 1 - router rip - no auto-summary.

Paso 3: Configurar OSPFv3 en el R2

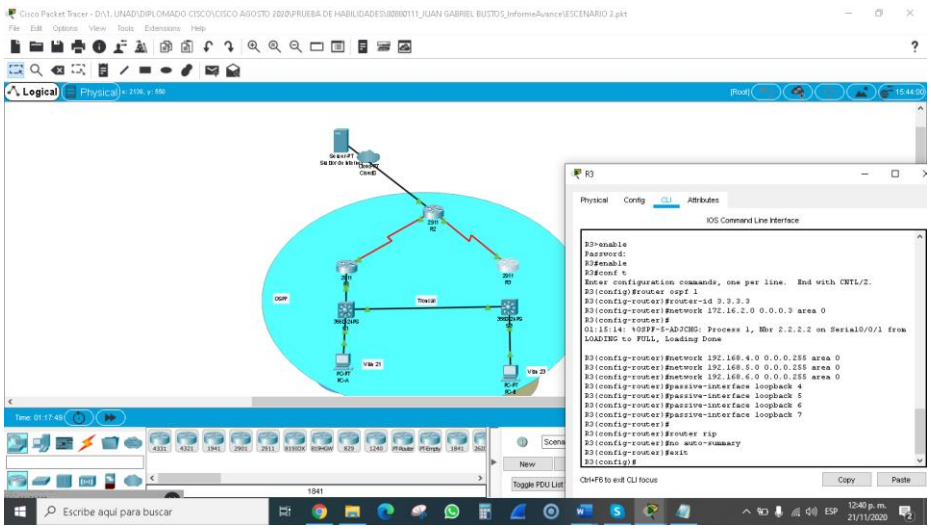
Se realiza la configuración de OSPF asignando le el ID router-id 3.3.3.3 y Anunciar redes IPv4 conectadas directamente empleando el comando network 172.16.2.0 0.0.0.3 area,ahora se procede a establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas, por ultimo de3 la configuración se desactiva la sumarización automática con router rip - no auto-summary

Tabla 27 Configurar OSPFv3 en el R2

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R3(config)#router ospf 1 R3(config-router)#router-id 3.3.3.3
Anunciar redes IPv4 conectadas directamente	R3(config-router)#network 172.16.2.0 0.0.0.3 area 0 R3(config-router)# 06:11:05: %OSPF-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Serial0/0/1 from LOADING to FULL, Loading Done R3(config-router)#network 192.168.4.0 0.0.0.255 area 0 R3(config-router)#network 192.168.5.0 0.0.0.255 area 0 R3(config-router)#network 192.168.6.0 0.0.0.255 area 0
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	R3(config-router)#passive-interface loopback 4 R3(config-router)#passive-interface loopback 5 R3(config-router)#passive-interface loopback 6 R3(config-router)#passive-interface loopback 7
Desactive la sumarización automática.	R3(config-router)#router rip R3(config-router)#no auto-summary R3(config-router)#

En la tabla No 27 se realiza la configuración de OSPFv3 en el R2 Anunciando las redes IPv4 conectadas directamente.

Figura 30 Configuración de R3



Fuente: Autor

Se muestra toda la configuración de R3 para verificar la correcta aplicación.

Paso 4: Verificar la información de OSPF

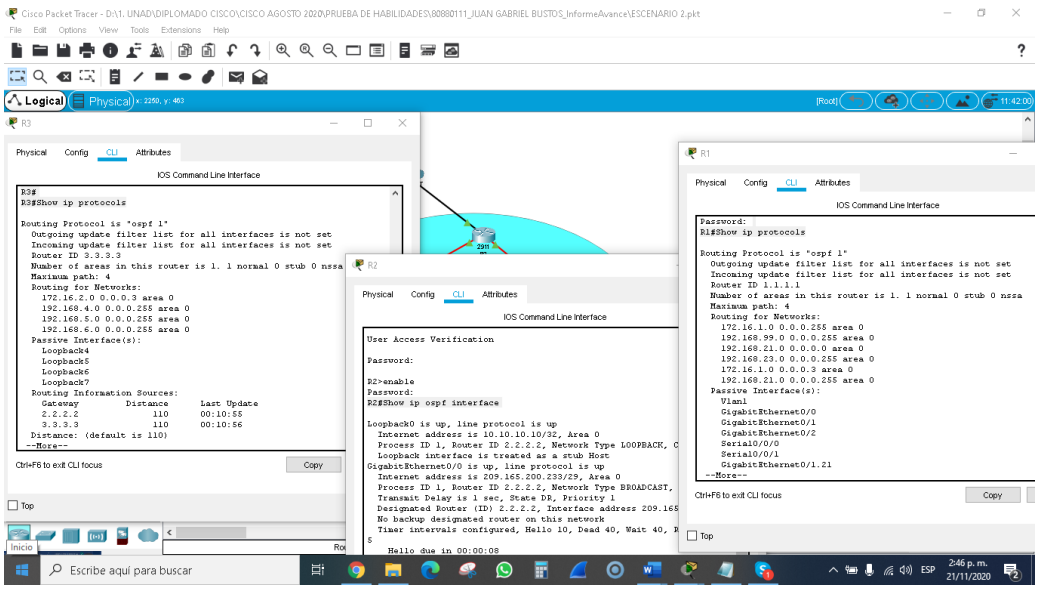
Verifique que OSPF esté funcionando como se espera. Introduzca el comando de CLI adecuado para obtener la siguiente información:

Tabla 28 Verificación de la información de OSPF

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

En la tabla No 28 Se verifica la información de OSPF.

Figura 31 Obtención de información OSPF



Fuente: Autor

Se realiza la investigación para la obtencion de informacion de la ID del proceso OSPF, la ID del router asi mismo se muestra solo las rutas OSPF mediante el

commando Show ip ospf interface y la sección de OSPF de la configuración en ejecución mediante el commando Show ip protocols.

Parte 5 Implementar DHCP y NAT para IPv4

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

Para continuar con R1 se ingresa en modo configuración y hace la reserve de las 20 direcciones IP que están de primeras en la VLAN 21 con ip dhcp excluded-address 192.168.21.1 - 192.168.21.20 asi mismo en la VLAN 23 para configuraciones estáticas en este caso address 192.168.23.1 192.168.23.20.

Ahora se creará un pool de DHCP para la VLAN 21, con la configuracion descrita en la table y se le asigna un nombre al dominio ip domain-name ccna-sa.com.

El siguiente paso es crear un pool de DHCP para la VLAN 23 al cual se nombra como ENGNR con el comando ip dhcp pool ENGNR, el servidor DNS es asignado mediante el comando dns-server el gateway predeterminado mediante default-router 192.168.23.1 network 192.168.23.0 255.255.255.0 y el nombre de dominio mediante ip domain-name ccna-sa.com.

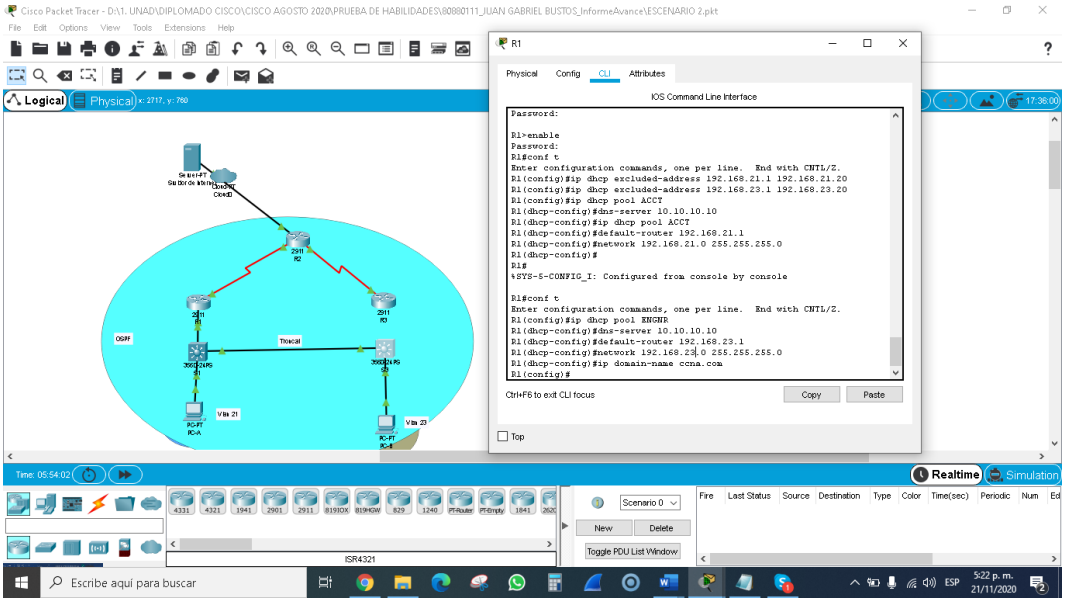
Tabla 29 Configuración el R1 como servidor de DHCP para las VLAN 21 y 23

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

Crear un pool de DHCP para la VLAN 23	Nombre: ENGNR Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado R1(config)#ip dhcp pool ENGNR R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#default-router 192.168.23.1 R1(dhcp-config)#network 192.168.23.0 255.255.255.0 R1(dhcp-config)#ip domain-name ccna-sa.com

En la tabla No 29 Se realiza la Configuración de R1 como servidor de DHCP para las VLAN 21 y 23.

Figura 32 Configuración de R1



Fuente: Autor

Configuracion el R1 como servidor de DHCP

Paso 2 Configurar la NAT estática y dinámica en el R2

En R2 se creará una database local con la cuenta **webuser** cisco12345 Nivel de privilegio: 15 al cual se aplica el comando user webuser privilege 15 secret cisco12345, la guia nos indica que se debe habilitar el servicio del servidor HTTP

lo cual no es posible ya que para equipos de simulación como Cisco Packet Tracer No Aplica.

Se procede a realizer la configuracion del servidor HTTP para que emplee la database local para la autenticación y se asigna una NAT estática al servidor web 209.165.200.229, luego se asigna la interfaz interna y externa para la NAT.

Ahora se configura la NAT dinámica dentro de una ACL estándar que permite aquellas direcciones que se deben traducer con una Lista de acceso: 1 es decir que se van a traducir de las redes de contabilidad e Ingeniería en el R1y las redes LAN (loopback) en el R3

El pool del direccionamiento IP públicas utilizadas con nombre INTERNET incluidas en las direcciones 209.165.200.225 – 209.165.200.228.

Tabla 30 Configurar la NAT estática y dinámica en el R2

Elemento o tarea de configuración	**Especificación**
Crear una base de datos local con una cuenta de usuario	Nombre de usuario: **webuser** Contraseña: **cisco12345** Nivel de privilegio: **15** R2(config)#user webuser privilege 15 secret cisco12345
Habilitar el servicio del servidor HTTP	Para equipos de simulación No Aplica
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	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 192.168.99.0 0.0.0.255
Crear una NAT estática al servidor web.	Dirección global interna: **209.165.200.229**
Asignar la interfaz interna y externa para la NAT estática	R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229

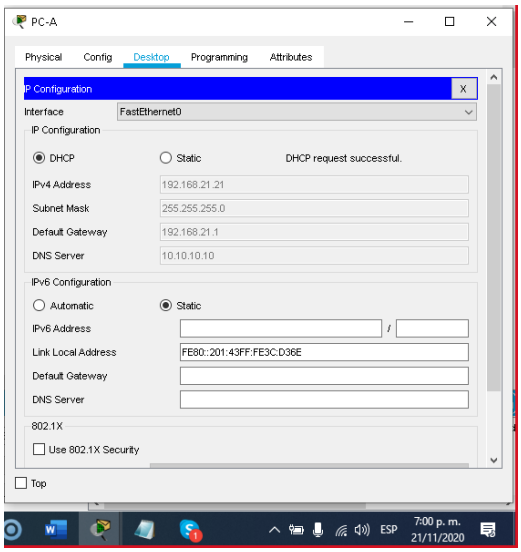
Configurar la NAT dinámica dentro de una ACL privada	Lista de acceso: 1 Permitir la traducción de las redes de Contabilidad y de Ingeniería en el R1 Permitir la traducción de un resumen de las redes LAN (loopback) en el R3. R2(config)#access-list 100 permit tcp any host 209.165.200.229 eq www R2(config)#access-list 100 permit icmp any
Defina el pool de direcciones IP públicas utilizables.	Nombre del conjunto: INTERNET El conjunto de direcciones incluye: 209.165.200.225 – 209.165.200.228 R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248
Definir la traducción de NAT dinámica	Show ip nat statistics

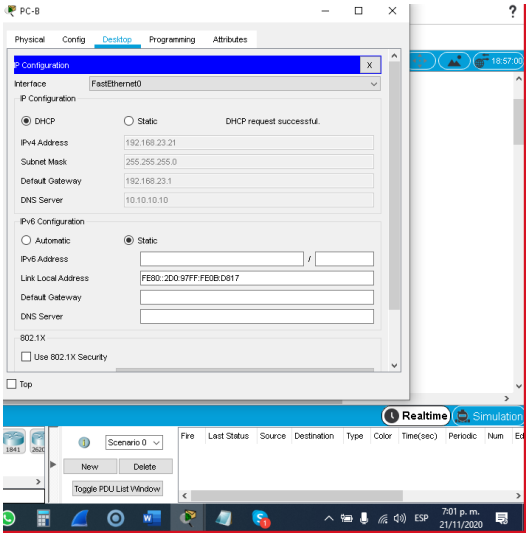
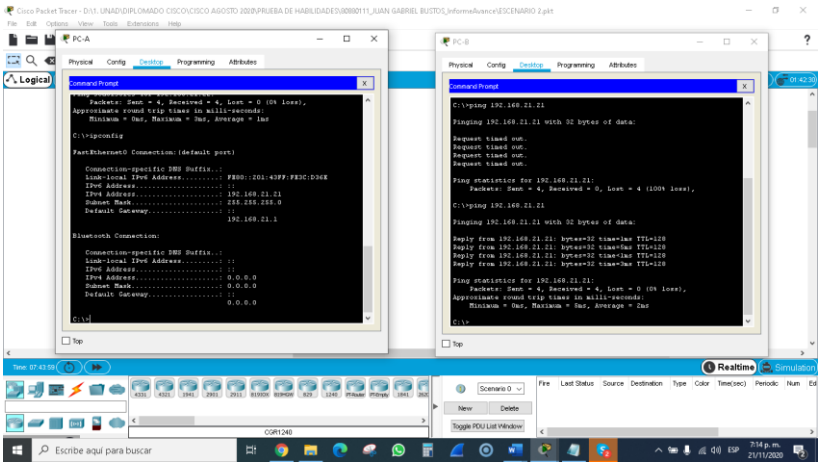
En la tabla No 30 se realiza la Configuración de la NAT estática y dinámica en el R2.

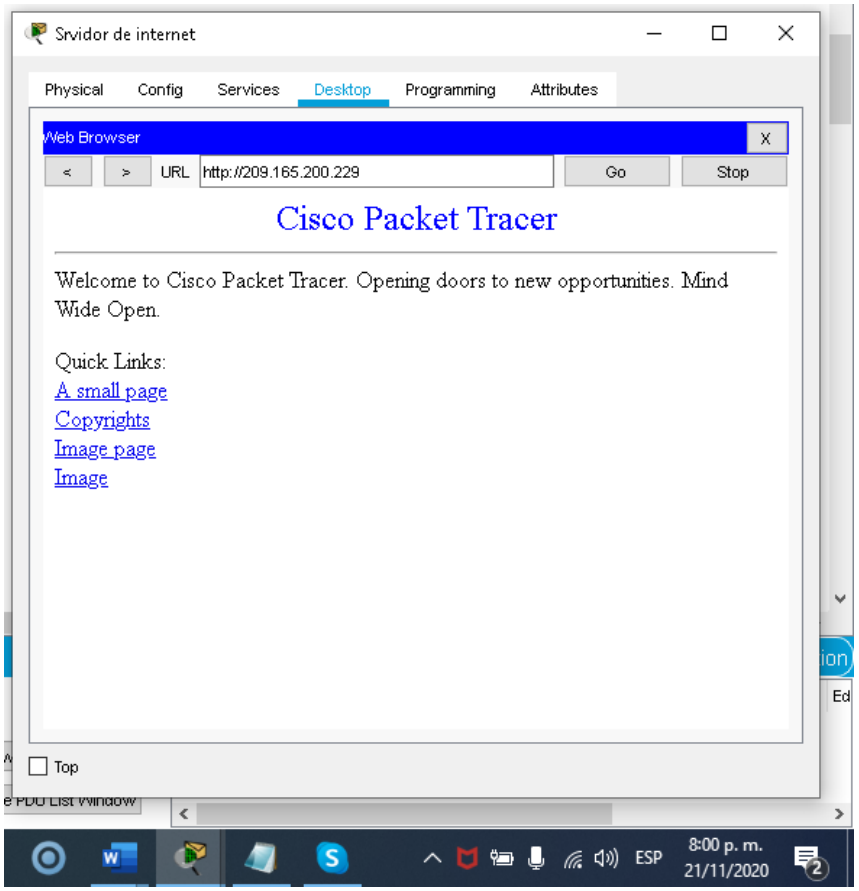
Paso 1: Verificar el protocolo DHCP y la NAT estática

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 31 Verificación del protocolo DHCP y la NAT estática

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	Figura 33 Verificacion del protocolo DHCP y la NAT estática en el PC-A y PC-B  Fuente: Autor Se verifican las configuraciones de DHCP y NAT estática funcionando de forma correcta en PC-A.

Verificar que la PC-B haya adquirido información de IP del servidor de DHCP	 Fuente: Autor Se verifican la configuracion funcionando de forma correcta en PC-B.
Verificar que la PC-A pueda hacer ping a la PC-B **Nota:** Quizá sea necesario deshabilitar el firewall de la PC.	 Fuente: Autor Se verifica que la PC-A pueda hacer ping a la PC-B

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**	 Fuente: Autor Se accede al servidor web (209.165.200.229

En la tabla No 31 se realiza la verificación del protocolo DHCP y la NAT estática.

Parte 6: Configurar NTP

En la configuración de NTP se realiza el ajuste la fecha y hora en R2 clock set 09:00:00 may 05 2016 R2 queda como un maestro NTP ntp master 5 ntp server 172.16.1.1 se configura para actualizaciones de calendario periódicas con hora NTP con el comando ntp update-calendar.

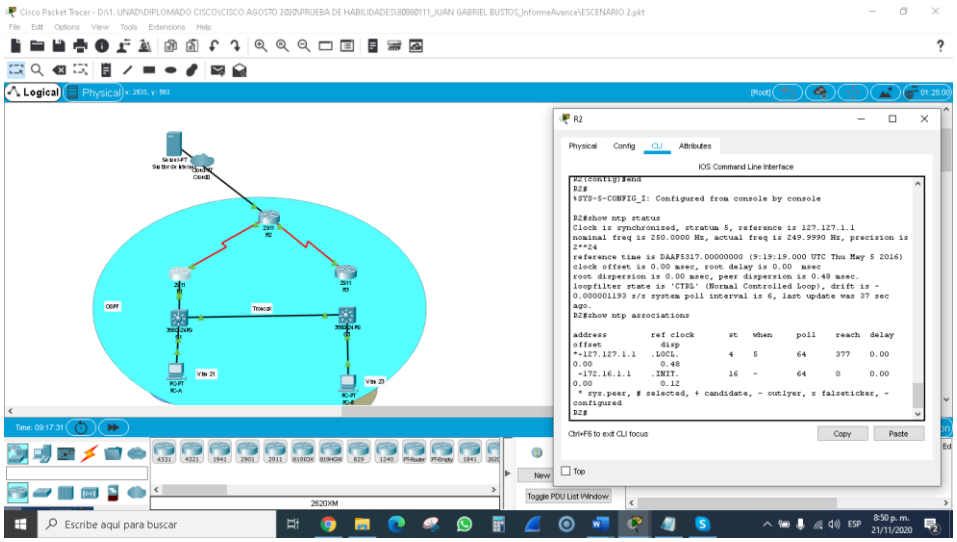
Tabla 32 Configuración NTP

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	**5 de marzo de 2016, 9 a. m.** R2#clock set 09:00:00 may 05 2016
Configure R2 como un maestro NTP.	Nivel de estrato: **5** **R2(config)#ntp master 5**

Configurar R1 como un cliente NTP.	Servidor: **R2** R2(config)#ntp server 172.16.1.1
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	R2(config)#ntp update-calendar R2(config)#end
Verifique la configuración de NTP en R1.	R2#show ntp status R2#show ntp associations

En la tabla No 32 se realiza la Configuraciòn de NTP, se realiza el ajuste la fecha y hora en R.

Figura 34Configuración de R2



Fuente: Autor

Se realiza la verificación de la configuración de R2 verificando con el comando show ntp associations.

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

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

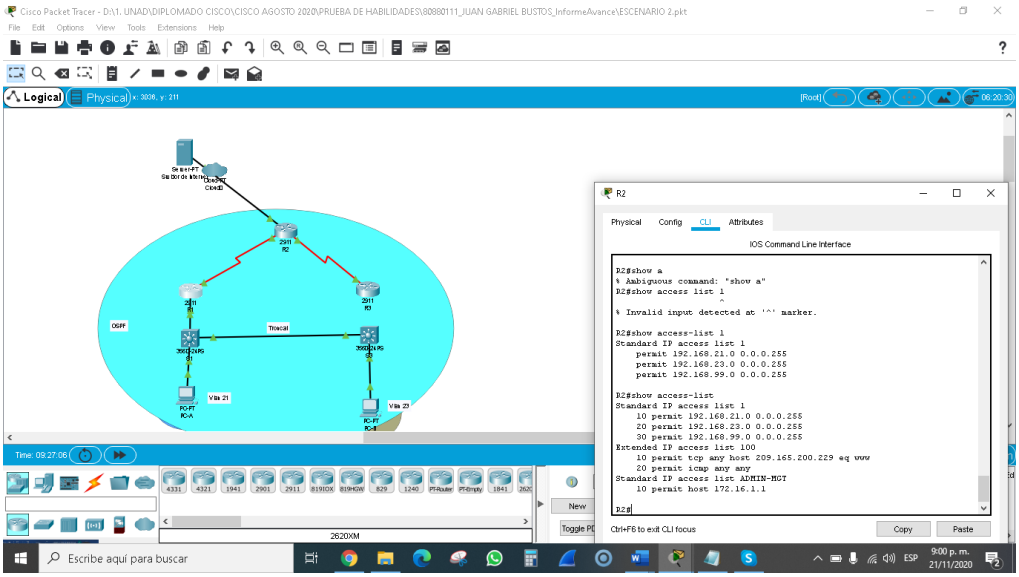
En R2 se ingresa mediante al comando permit host 172.16.1.1para configurar una lista de acceso con el propósito que R1 establezca una conexión Telnet con R2 aplicando la ACL con nombre a las líneas VTY.

Tabla 33 Configuración restricción del acceso a las líneas VTY en el R2

Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	Nombre de la ACL: **ADMIN-MGT** R2(config-std-nacl)#permit host 172.16.1.1 R2(config-std-nacl)#exit
Aplicar la ACL con nombre a las líneas VTY	R2(config)#line VTY 0 15 R2(config-line)#access-class ADMIN-MGT in R2(config-line)#exit
Permitir acceso por Telnet a las líneas de VTY	R2(config)#line VTY 0 4 shR2(config-line)#access-class ADMIN-MGT in R2(config-line)#end

En la tabla No 33 se realiza la configuración de la restricción del acceso a las líneas VTY en el R2.

Figura 35 Verificación del ACL



Fuente: Autor

se verifica en R2 el funcionamiento de la configuracion de manera correcta.

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

Tabla 34 Mostrar las coincidencias recibidas por una lista de acceso.

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-lists
Restablecer los contadores de una lista de acceso	R1(config)#ip access-list standard 2 R1(config-std-nacl)#18 permit 172.22.1.1 R1(config-std-nacl)#exit
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	R2#show ip nat translations
¿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. show ip nat translations
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	R2#clear ip nat translation *

En la tabla No 34 Se Introduce el comando de CLI adecuado que se necesita para mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció.

CONCLUSIONES

Se estableció la solución de diversas tareas de cada uno de los escenarios propuestos en el software de simulación Cisco Packet Tracer tales como: enrutamiento entre VLAN, DHCP, etherchannel y port-security, equipos como router y el switch que admitan tanto la conectividad IPv4 como 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).

Dentro del desarrollo del escenario se configuraron listas de control de acceso (ACL) protocolo de tiempo de red (NTP) servidor/cliente y se comprobó el registro de los procesos de verificación de conectividad mediante el uso de comandos ping, traceroute, show ip route, show running-config, show ip interface brief, show flash, show ipv6 interface brief, show versión, show ip route, show vlan, show port-security, show port-security address.

Los escenarios solucionados nos brindan la experiencia como futuros Ingenieros de sistemas que ayudan a solucionar problemáticas propias de la disciplina en el campo profesional, permiten generar habilidades y destrezas que servirán para adelantar futuros proyectos relacionados con el Networking.

El software de simulación Cisco Packet Tracer fue ideal para el desarrollo de cada escenario solicitado, llevándonos a experiencias que se viven a diario en entornos profesionales de Networking, la creación y configuración de dos (2) redes simples en diferentes dispositivos como routers y switches ayudan a fortalecer nuestro conocimiento para dar soluciones pertinentes con configuraciones simples y complejas en los equipos que interconectan al mundo.

BIBLIOGRAFÍA

CISCO. (2014). Enrutamiento entre VLANs. Principios de Enrutamiento y Conmutación. Recuperado de https://static-courseassets.s3.amazonaws.com/RSE50ES/module5/index.html#5.0.1.1

Cisco Networking Academy. (2018). CP - CCNA2. Routing y switching de CCNA: Principios básicos de routing y switching. Capítulo 1 al 6. Recuperado de https://1314297.netacad.com/courses/627676

CISCO. (2014). Introducción a redes conmutadas. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-courseassets.s3.amazonaws.com/RSE50ES/module1/index.html#1.0.1.1

CISCO. (2014). Configuración y conceptos básicos de Switching. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-courseassets.s3.amazonaws.com/RSE50ES/module2/index.html#2.0.1.1

CISCO. (2014). DHCP. Principios de Enrutamiento y Conmutación. Recuperado de: https://staticcourseassets.s3.amazonaws.com/RSE50ES/module10/index.html#10.0.1.1

Felipe, J. (2012). Juan Felipe.https://youtu.be/OSACL0bLJrY (Compositor). (2013). configuracion de red con dos routers packet tracer.-Networking, C. (23 de 05 de2018).

Macfarlane, J. (2014). Network Routing Basics : Understanding IP Routing in Cisco Systems. Recuperado de: http://bibliotecavirtual.unad.edu.co:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=e000xww&AN=158227&lang=es&site=ehost-live

Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). EIGRP Implementation. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. Recuperado de https://1drv.ms/b/s!AmIJYei-NT1IlnMfy2rhPZHwEoWx

Victor E. Martinez G, V. E. (2018, 16 agosto). Configuración de rutas estáticas (static route) Router Cisco. Recuperado 5 junio, 2019, de http://theosnews.com/2013/02/configuracion-de-rutas-estaticas-static-route-routercisco/

ANEXOS

ANEXO 1

Enlace de descarga de archivos de simulación

https://drive.google.com/drive/folders/1iKpDVAv1Ei-HjCt_yU5HJdPRsROnvRmm?usp=sharing

ANEXO 2

Enlace Artículo Científico IEEE

https://drive.google.com/file/d/13uIqsLFFvlAAWnpOWvQRDw5SGYPDk9o8/view?usp=sharing