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

IVAN DARIO MURCIA ANGEL

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA PROGRAMA DE INGENIERIA DE SISTEMAS

ATACO TOLIMA

2020

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

IVAN DARIO MURCIA ANGEL

Trabajo como opción de grado para optar al título de Ingeniero de Sistemas

DIRECTOR
DIEGO EDINSON RAMIREZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA PROGRAMA DE INGENIERIA DE SISTEMAS
ATACO TOLIMA
2020

Nota de Aceptación

Presidente del Jurado

Jurado

Jurado

Ataco Tolima, Diciembre 2020

AGRADECIMIENTOS

Agradezco a la universidad por su gran laboral por labrar a este estudiante durante el proceso formativo, a mis padres por el empuje y acompañamiento que estuvo presente en toda la carrera, a mi esposa y mi hijo porque son la razón de ser hoy un profesional.

TABLA DE CONTENIDO

Contenido

RESUMEN 10

ABSTRACT 11

INTRODUCCIÓN 12

OBJETIVOS 13

OBJETIVO GENERAL 13

OBJETIVOS ESPECÍFICOS 13

TOPOLOGIA ESCENERARIO No 1 14

Paso 4: Configure el S2 26

Paso 5: Parte 2: configurar soporte de host 29

Configure R1 29

ESCENARIO 2 34

Parte 1: Inicializar dispositivos 35

Paso 1: Inicializar y volver a cargar los routers y los switches 35

Parte 2 Configurar los parámetros básicos de los dispositivos 36

Paso 1: Configurar la computadora de Internet 36

Paso 2: Configurar R1 36

Paso 3: Configurar R2 38

Paso 4: Configurar R3 42

Paso 5: Configurar S1 43

Paso 6: Configurar el S3 44

Paso 7: Revisar la conectividad de la red 45

Parte 3: Configurar la seguridad del switch, las VLAN y el routing entre VLAN 47

Paso 2: Configurar el S3 49

Paso 3: Configurar R1 50

Paso 4: Verificar la conectividad de la red 51

Parte 2: Configurar el protocolo de routing dinámico OSPF 52

Paso 1: Configurar OSPF en el R1 52

Paso 2: Configurar OSPF en el R2 53

Paso 3: Configurar OSPFv3 en el R2 54

Paso 4: Verificar la información de OSPF 55

Parte 3: Implementar DHCP y NAT para IPv4 56

Paso 1: Configurar el R1 como servidor de DHCP para las VLAN 21 y 23 56
Paso 2: Configurar la NAT estática y dinámica en el R2 57
Paso 3: Verificar el protocolo DHCP y la NAT estática 59
Parte 4: Configurar NTP 60
Parte 5: Configurar y verificar las listas de control de acceso (ACL) 60
Paso 1: Restringir el acceso a las líneas VTY en el R2 60
Paso 2: Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente 61
CONCLUSIONES 62
BIBLIOGRAFÍA 63
RESUMEN 64

TABLAS

Contenido

Tabla de VLAN 14
Tabla de asignación de direcciones 15
Tabla 1 – Configuración R1 19
Tabla 2 – Configuración S1 21
Tabla 3 – Configuración S2 23
Tabla 4 – interfaz de administración 23
Tabla 5 – Configuración S1 26
Tabla 6 – Configuración VLAN 28
Tabla 7 – IPv4 DHCP para VLAN 2 30
ESCENARIO 2 34
Tabla 1 Iniciar dispositivos 35
Tabla 2 Configuración PC-A 36
Tabla 3 Configuración R1 37
Tabla 4 Configuración R2 41
Tabla 5 Configuración R3 43
Tabla 6 Configuración S1 44
Tabla 7 Configuración S3 45
Tabla 8 Verificación de conectividad 45
Tabla 9 seguridad del S3 48
Tabla 10 seguridad del S3 50
Tabla 11 seguridad del R1 50
Tabla 12 Verificación de conectividad 51
Tabla 13 Configuración RIP EN R1 53
Tabla 14 Configuración RIP EN R2 54
Tabla 15 Configuración RIP EN R3 55
Tabla 16 Verificación OSPF 55
Tabla 17 DHCP y NAT IPv4 en R1 57
Tabla 18 DHCP y NAT IPv4 en R2 58
Tabla 19 verificación DHCP y la NAT 59
Tabla 20 configuración NTP 60
Tabla 21 configuración ACL 60
Tabla 22 Visualización comando CLI 61

IMÁGENES

Contenido

TOPOLOGIA ESCENERARIO No 1 14
Imagen 1. Trabajo Unad 14
Imagen 2. Configuración R1 16
Imagen 3. Configuración direccionamiento de ipv6 16
Imagen 4. Configuración direccionamiento de ipv6 17
Imagen 5. Configuración direccionamiento de ipv6 19
Imagen 6. Configuración S1 20
Imagen 7. Configurar la interfaz de administración 20
Imagen 8. Configuración S2 22
Imagen 9. Configuración modo privilegiado y contraseña cifrado RSA 22
Imagen 10. Configuración VLAN 24
Imagen 11. Crear troncos 802.1Q 24
Imagen 12. Nombramiento VLAN 26
Imagen 13. Verificación VLAN activas 28
Imagen 14. protocolo LACP para la negociación 29
ESCENARIO 2 34
Figura 1. Trabajo unad 34
Figura 2 -Autor 35
Figura 3 – Reinicio R1 36
Figura 4 – Configuración R1 38
Figura 5 – Configuración R2 38
Figura 6 – Activación serial1 40
Figura 7 – activación interfaz gibabit 40
Figura 8 – activación interfaz gibabit 41
Figura 9 – Configuración R3 42
Figura 10 – Configuración lo 42
Figura 11 – Configuración S1 43
Figura 12 – Configuración S3 44
Figura 13 Ping R1 a R2 Fuente: Packet Tracer 46

Figura 14 Ping R2 a R3Fuente: Packet Tracer 46
Figura 15 Configuración VLAN S1 47
Figura 16 Asignación IP y gateway 47
Figura 17 - Ping S1 a VLAN 99 y VLAN 21 51
Figura 18 - Ping S3 - VLAN 99 y VLAN 23 52
Figura 19 – Verificación de protocolos 56
Figura 20 – Comando show run 56

RESUMEN

La presente actividad contiene dos escenarios que se debe aplicar los conocimientos adquiridos en CISCO de armar la topología y programas los diferentes dispositivos para que se conecten entre si y se permite satisfacer la necesidad de una población a futura que se pueda presentar.

Palabras Claves: Red Lan, Dispositivos, Red Wan, Router, Computadores

ABSTRACT

This activity contains two scenarios that should apply the knowledge acquired in CISCO to build the topology and programs the different devices so that they connect with each other and allow to satisfy the need of a future population that may arise.

Keywords: Lan Network, Devices, Wan Network, Router, Computers

INTRODUCCIÓN

En un entorno simulado se debe desarrollar dos ejercicios utilizando diferentes dispositivos como son Switches, computadoras y Routers en una red para realizar la programación requerida para su correcto funcionamiento donde se pondrá a prueba los conocimientos adquiridos en el diplomado, afianzando cada vez más nuestras habilidades en el mundo laboral,

OBJETIVOS

OBJETIVO GENERAL

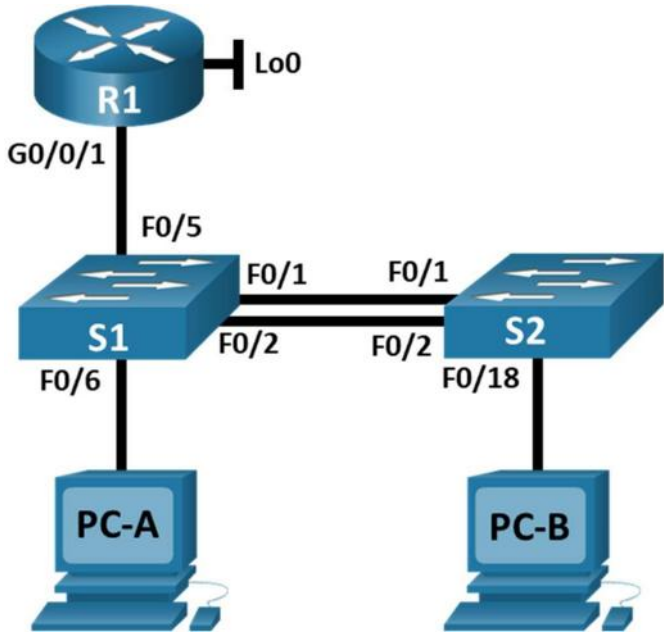
- Resolver los escenarios propuestos por la prueba de habilidades CISCO

OBJETIVOS ESPECÍFICOS

- Crear la topología propuesta y relacionar los dispositivos requeridos.
- Configurar cada uno de los dispositivos acorde a la guía.
- Implementar las listas de control de acceso ACL y establecer protocolos.
- Documentar paso a paso la configuración y resultados.

TOPOLOGIA ESCENERARIO No 1

Imagen 1. Trabajo Unad



Fuente - Autor

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.

Tabla de VLAN

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

Tabla de asignación de direcciones

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
R1 G0/0/1.2	10.19.8.1 /26	No corresponde
	2001:db8:acad:a: :1 /64	No corresponde
R1 G0/0/1.3	10.19.8.65 /27	No corresponde
	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.

Instrucciones

Inicializar y Recargar y Configurar aspectos basicos de los

dispositivos Inicializar y volver a cargar el router y el switch

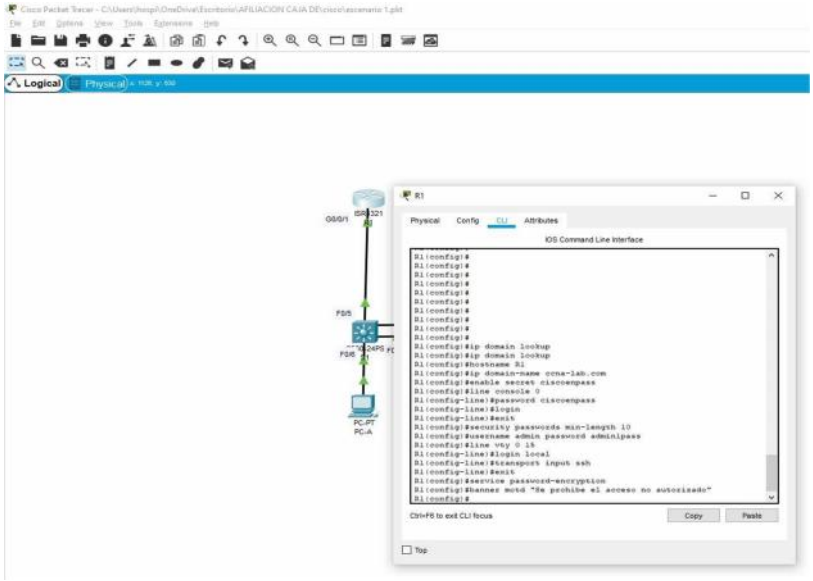
- Borre las configuraciones de inicio y las VLAN del router y del switch y vuelva a cargar los dispositivos.
- Después de recargar el switch, configure la plantilla SDM para que admita IPv6 según sea

necesario y vuelva a cargar el switch.

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

Tabla Paso 1: Configurar R1

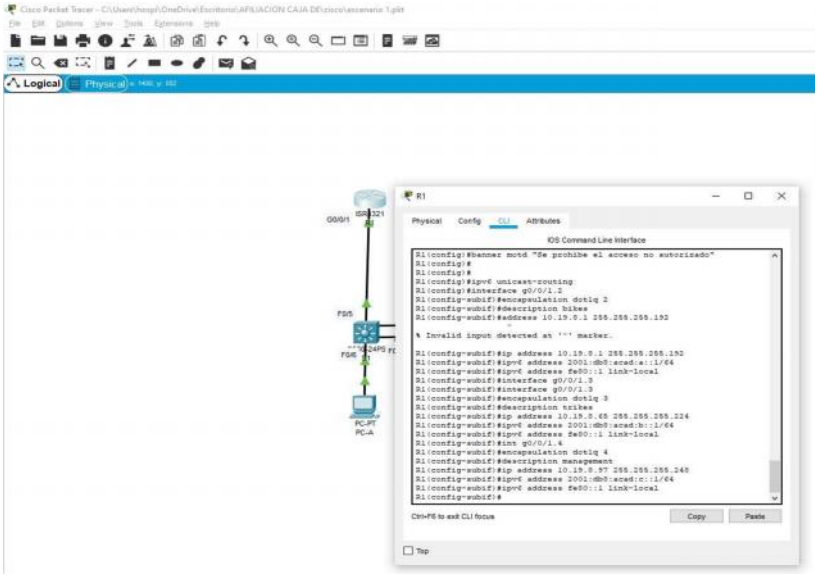
Imagen 2. Configuración R1



Fuente - Autor

Continuando con la configuración del Router realizamos el direccionamiento de ipv6

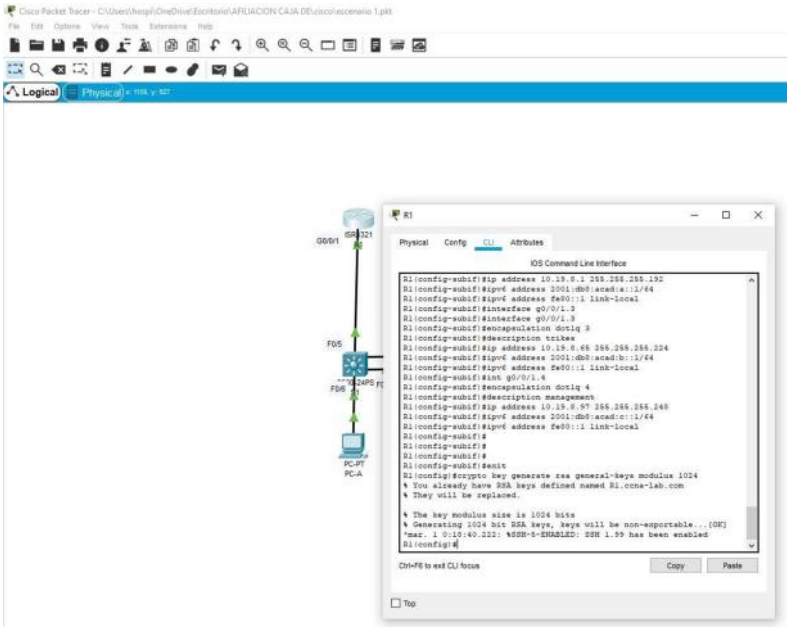
Imagen 3. Configuración direccionamiento de ipv6



Fuente – Autor

Para culminar en esta primera etapa configuramos del Router con una clave de cifrado RSA de 1024 bits, como se muestra a continuación:

Imagen 4. Configuración direccionamiento de ipv6



Fuente - Autor

Realizamos la eliminación del archivo de configuración de inicio, ingresamos el dominio, Procedemos a configurar el router, asignando un nombre, el dominio, las contraseñas de ingrese modo privilegiado, configuramos MOTD Banner, creamos un usuario en base de datos local, habilitamos epv6 y las interfaces. Continuando con la configuración

Tarea	Especificación
Desactivar la búsqueda DNS	Router>enable Router#erase startup-config Router# reload
Nombre del router	Router>enable Router#config t Router(config)#ip domain lookup Router(config)#hostname R1
Nombre de dominio	R1(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	R1(config)#enable secret ciscoenpass R1(config)#line console 0
Contraseña de acceso a la consola	R1(config-line)#password ciscoenpass 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	R1(config)#username admin password admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	R1(config)#line vty 0 15 R1(config-line)#login local
Configurar VTY solo aceptando SSH	R1(config-line)#transport input ssh R1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Configure un MOTD Banner	R1(config)#banner motd “Se prohíbe el acceso no autorizado”
Habilitar el routing IPv6	R1(config)#ipv6 unicast-routing
Configurar interfaz G0/0/1 y subinterfaces	R1(config)#interface g0/0/1.2 R1(config-subif)#encapsulation dot1q 2 R1(config-subif)#description bikes R1(config-subif)#ip address 10.19.8.1 255.255.255.192 R1(config-subif)#ipv6 address 2001:db8:acad:a::1/64 R1(config-if)#ipv6 address fe80::1 link-local R1(config)#interface g0/0/1.3 R1(config-subif)#encapsulation dot1q 3 R1(config-subif)#description trikes R1(config-subif)#ip address 10.19.8.65 255.255.255.224 R1(config-subif)#ipv6 address 2001:db8:acad:b::1/64 R1(config-if)#ipv6 address fe80::1 link-local

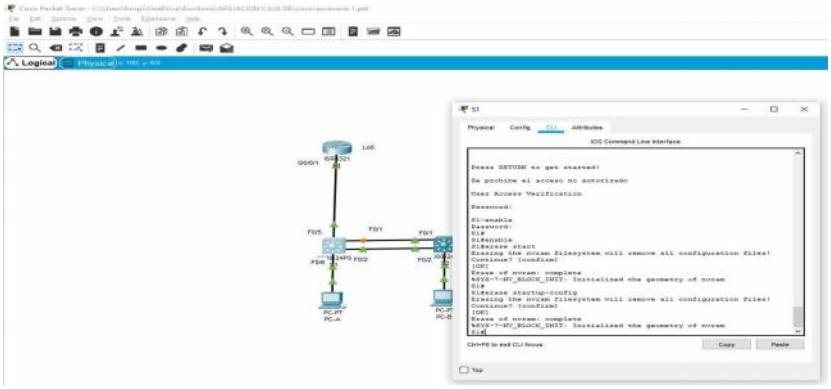
Configurar interfaz G0/0/1 y subinterfaces	R1(config)#int g0/0/1.4 R1(config-subif)#encapsulation dot1q4 R1(config-subif)#description management R1(config-subif)#ip address 10.19.8.97 255.255.255.248 R1(config-subif)#ipv6 address 2001:db8:acad:c::1/64 R1(config-if)#ipv6 address fe80::1 link-local R1(config)#int g0/0/1.6 R1(config-subif)#encapsulation dot1q 6 R1(config-subif)#description native R1(config)#int g0/0/1 R1(config-subif)#no shut
	R1(config)#int loopback 0 R1(config-subif)#description loopback R1(config-subif)#ip address 209.165.201.1 255.255.255.224 R1(config-subif)#ipv6 address 2001:db8:acad:209::1/64 R1(config-if)#ipv6 address fe80::1 link-local R1(config-subif)#description native R1(config)#exit
Generar una clave de cifrado RSA Módulo de 1024 bits	R1(config)# crypto key generate rsa general- keys modulus 1024

Tabla 1 – Configuración R1

Paso 2. Configure S1 y S2.

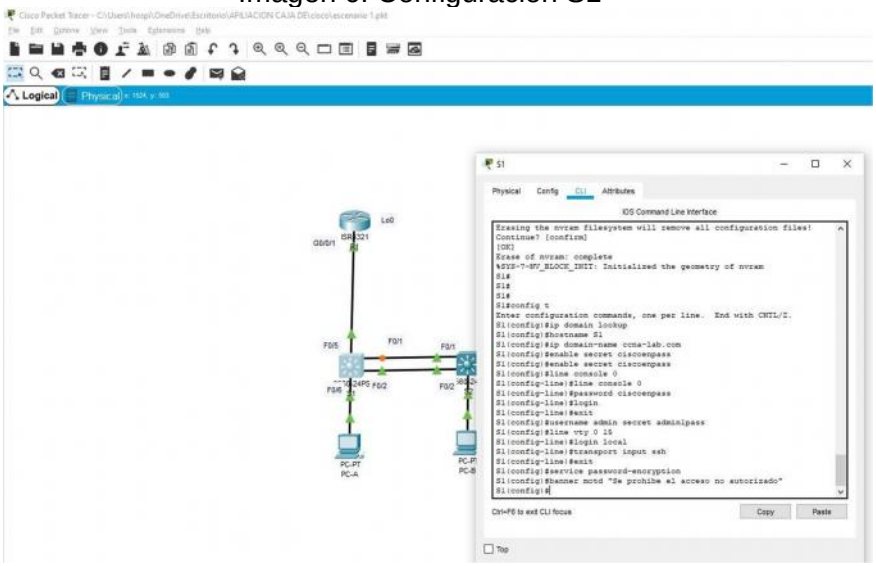
Configuración S1

Imagen 5. Configuración direccionamiento de ipv6



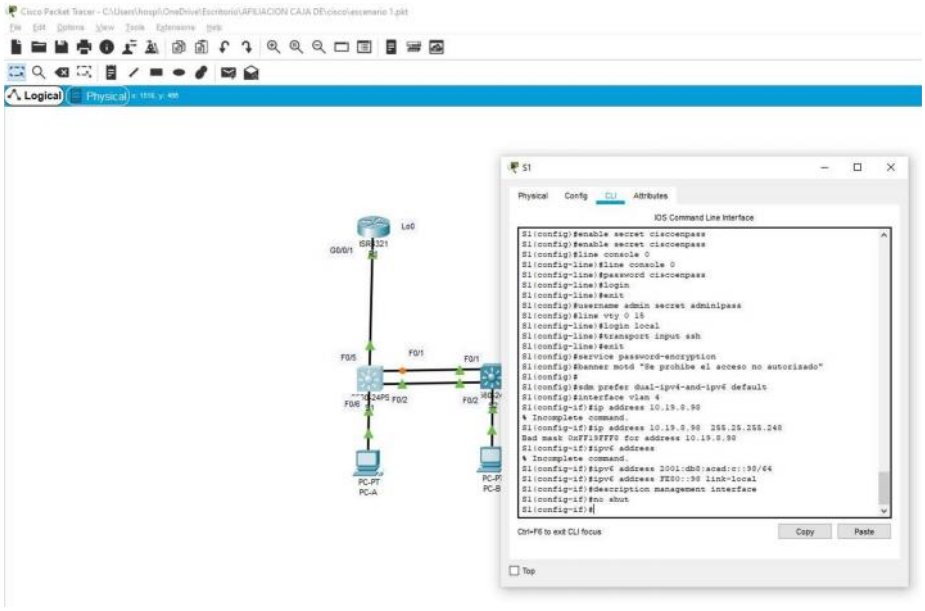
Fuente - Autor

Imagen 6. Configuración S1



Fuente - Autor

Imagen 7. Configurar la interfaz de administración



Fuente - Autor

Las tareas de configuración incluyen lo siguiente:

Realizamos la configuración del S1 desactivando las búsquedas de las DNS y bautizamos el S1

Tarea	Especificación
Desactivar la búsqueda DNS.	Switch>enable Switch#erase start Switch#erase startup-config Switch#reload
Nombre del switch	Switch>enable Switch#config t Switch#ip domain lookup Switch(config)#hostname S1

Damos nombramiento al dominio, encriptados la contraseña, generamos contraseña para ingresar a la consola, configuramos VTY para la utilización de la base de datos, configuramos el banner para cuando ingrese un usuario sin permisos sala la ventana emergente diciendo “no está autorizado” y configuramos la interfaz.

Para realizar la siguiente configuración utilizamos dos switch 3560 viene por defecto para visualizar la activación de direcciones ipv4 – ipv 6 para habilitarlo es necesario utilizar el comando

sdm prefer dual-ipv4-and-ipv6 defaultU

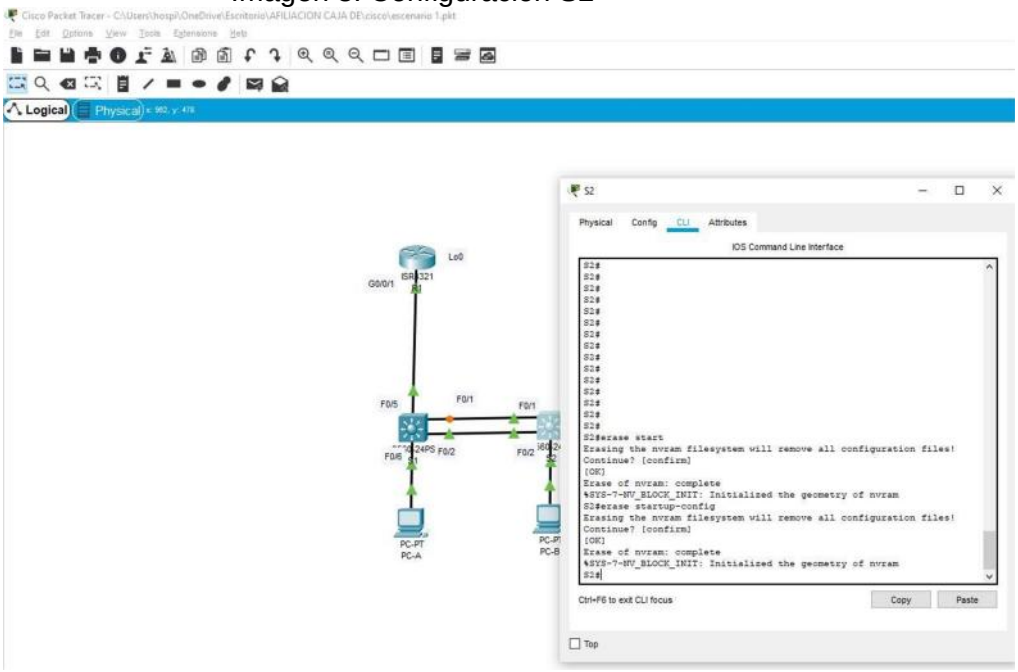
Tarea	Especificación
Nombre de dominio	S1(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	S1 (config)#enable secret ciscoenpass S1 (config)#line console 0
Contraseña de acceso a la consola	S1(config-line)#password ciscoenpass S1(config-line)#login S1(config-line)#exit
Crear un usuario administrativo en la base de datos local	S1(config)#username admin secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	S1(config)#line vty 0 15 S1(config-line)#login local
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S1(config-line)#transport input ssh S1(config-line)#exit

Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption
Configurar un MOTD Banner	S1(config)#banner motd “Se prohibe el acceso no autorizado”
Generar una clave de cifrado RSA	S1(config)# crypto key generate rsa general-keys modulus 1024
Configurar la interfaz de administración (SVI) Se utiliza switch 3560 que se puede utilizar para IPV6 utilizando un comando para la activación	S1(config)#sdm prefer dual-ipv4-and-ipv6 default S1(config)#interface vlan 4 S1(config-if)#ip address 10.19.8.98 255.25.255.248 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 shut S1(config)#exit
Configuración del gateway predeterminado	S1(config)#ip default-gateway 10.19.8.97 S1(config)#exit

Tabla 2 – Configuración S1

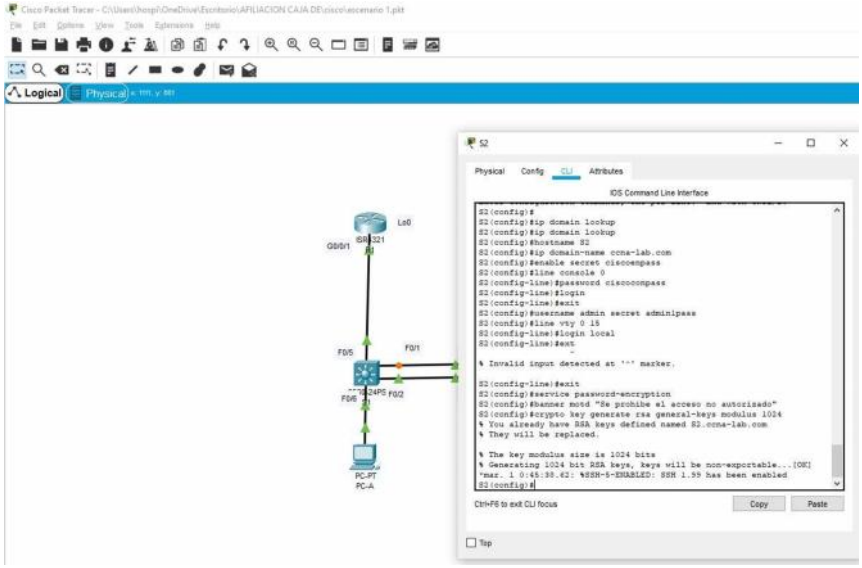
Configuración S2

Imagen 8. Configuración S2



Fuente Autor

Imagen 9. Configuración modo privilegiado y contraseña cifrado RSA



Fuente - autor

Las tareas de configuración incluyen lo siguiente:

Damos nombramiento al dominio, encriptados la contraseña, generamos contraseña para ingresar a la consola, configuramos VTY para la utilización de la base de datos, configuramos el banner para cuando ingrese un usuario sin permisos sala la ventana emergente diciendo “no está autorizado” y configuramos la interfaz.

Para realizar la siguiente configuración utilizamos dos switch 3560 viene por defecto para visualizar la activación de direcciones ipv4 – ipv 6 para habilitarlo es necesario utilizar el comando

sdm prefer dual-ipv4-and-ipv6 default

Tarea	Especificación
Desactivar la búsqueda DNS.	Switch>enable Switch#erase start Switch#erase startup-config Switch#reload
Nombre del switch	Switch>enable Switch#config t Switch#ip domain lookup Switch(config)#hostname S2
Nombre de dominio	S2(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	S2 (config)#enable secret ciscoenpass

Contraseña de acceso a la consola	S2 (config)#line console 0 S2 (config-line)#password ciscoconpass S2 (config-line)#login S2 (config-line)#exit
Crear un usuario administrativo en la base de datos local	S2(config)#username admin secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	S2(config-line)# line vty 0 15 S2(config-line)#login local
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	S2(config)#service password-encryption
Configurar un MOTD Banner	S2(config)#banner motd “Se prohibe el acceso no autorizado”
Generar una clave de cifrado RSA	S2(config)# crypto key generate rsa general-keys modulus 1024

Tabla 3 – Configuración S2

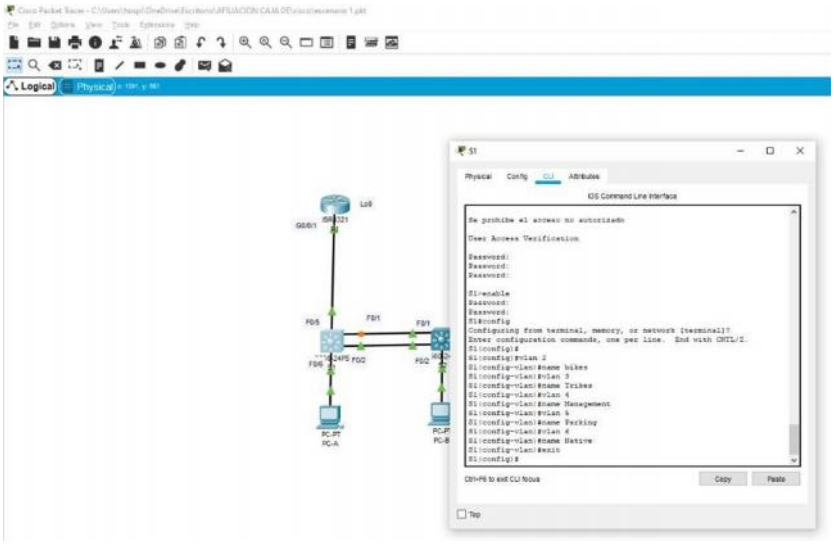
Se utiliza el comando sdm para el S2 pueda utilizar IPV6 y configuramos el gateway

Configurar la interfaz de administración (SVI) Se utiliza switch 3560 que se puede utilizar para IPV6 utilizando un comando para la activación	S2(config)#interface vlan 4 S2(config-if)#ip address 10.19.8.99 255.25.255.248 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 shut S2(config)#exit S2(config)#sdm prefer dual-ipv4-and-ipv6 default
Configuración del gateway predeterminado	S2(config)#ip default-gateway 10.19.8.97 S2(config)#exit

Tabla 4 – interfaz de administración

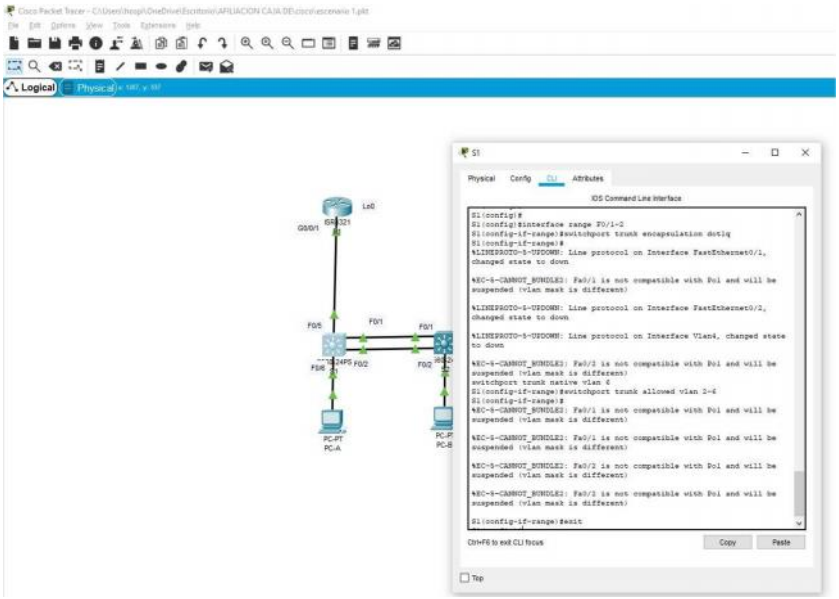
La configuración del S1 incluye las siguientes tareas:

Imagen 10. Configuración VLAN



Fuente - Autor

Imagen 11. Crear troncos 802.1Q



Fuente - autor

Realizamos el nombramiento de cada una de las vlan en el S1 y
Creamos las troncales que se utilicen la vlan 6 nativa y configuramos las troncales configurando las interfaces permitiendo la trasmisión de datos

Tarea	Especificación
Crear VLAN VLAN 2, nombre Bikes VLAN 3, nombre Trikes VLAN 4, name Management VLAN 5, nombre Parking VLAN 6, nombre Native	S1(config)#vlan 2 S1(config-vlan)#name bikes S1(config-vlan)#exit S1(config)#vlan 3 S1(config-vlan)#name Trikes S1(config)#vlan 4 S1(config-vlan)#name Management S1(config-vlan)#exit S1(config)#vlan 5 S1(config-vlan)#name Parking S1(config)#vlan 6 S1(config-vlan)#name Native S1(config-vlan)#exit

Crear troncos
802.1Q que utilicen
la VLAN 6 nativa
Interfaces F0/1, F0/2 y F0/5
	S1#config t
	S1(config)#interface range F0/1-2
	S1(config-if)#switchport trunk encapsulation dot1q
	S1(config-if)#switchport trunk native vlan 6
	S1(config-if)#switchport trunk allowed vlan 2-6
	S1(config-if)#exit
	
	S1(config)#interface range F0/5
	S1(config)# switchport trunk encapsulation dot1q (#option)
	S1(config-if)#switchport trunk native vlan 6
	S1(config-if)#switchport trunk allowed vlan 2-6
	S1(config-if)#exit

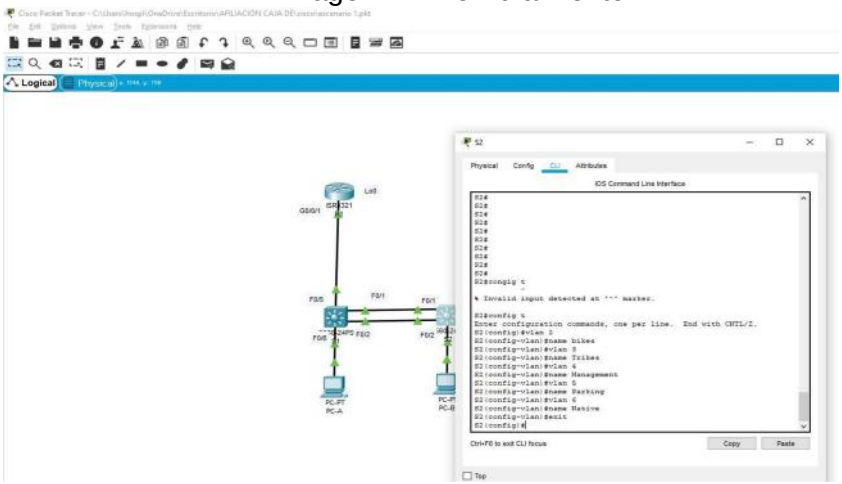
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2 Usar el protocolo LACP para la negociación	S1(config)#interface range FastEthernet 0/1-2 S1(config-if-range)#channel-group 1 mode active S1(config-if)#exit

Configurar el puerto de acceso de host para VLAN 2 Interface F0/6	S1(config)#int f0/6 S1(config-if)#switchport mode access
Configurar la seguridad del puerto en los puertos de acceso Permitir 3 direcciones MAC	S1(config-if)#switchport Access vlan 2 S1(config-if)#switchport port-security maximum 3
Proteja todas las interfaces no utilizadas Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar	S1(config)#interface range f0/3-4 S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 5 S1(config-if-range)#description unused interfaces S1(config-if-range)#shutdown S1(config)#interface range f0/7-24 S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 5 S1(config-if-range)#description unused interfaces S1(config-if-range)#shutdown S1(config)#interface range g0/1-2 S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 5 S1(config-if-range)#description unused interfaces S1(config-if-range)#shutdown

Tabla 5 – Configuración S1 y troncales

Paso 4: Configure el S2.

Imagen 12. Nombramiento VLAN



Fuente – Autor

Realizamos el nombramiento de cada una de las vlan en el S2 y creamos las troncales que se utilicen la vlan 6 nativa y configuramos las troncales configurando las interfaces permitiendo la trasmisión de datos utilizando los comandos anteriores

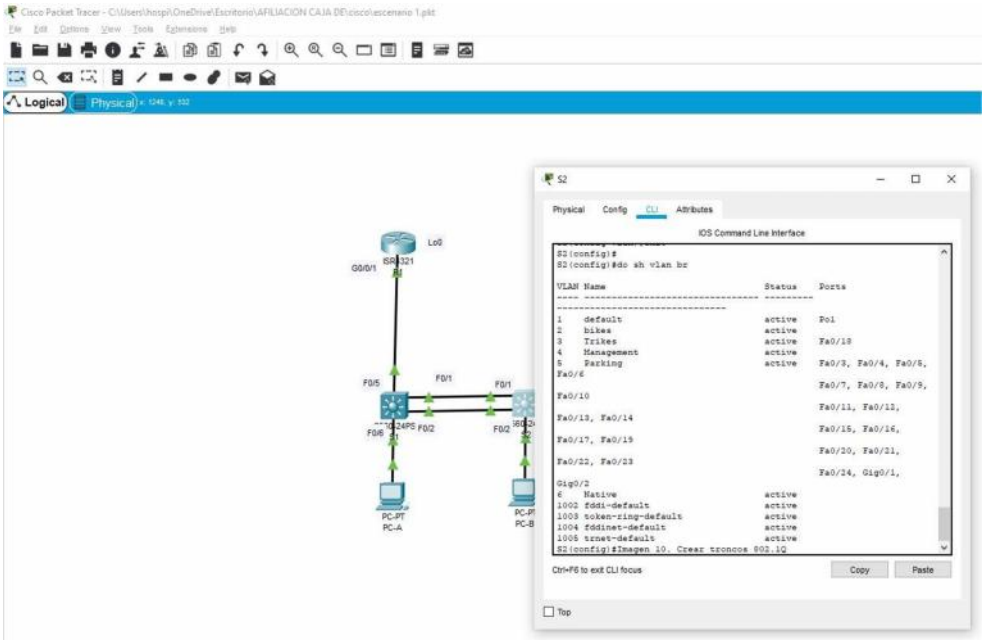
Tarea	Especificación
Crear VLAN	S2(config)#vlan 2 S2(config-vlan)#name bikes S2(config)#vlan 3 S2(config-vlan)#name Trikes S2(config)#vlan 4 S2(config-vlan)#name Management S2(config)#vlan 5 S2(config-vlan)#name Parking S2(config)#vlan 6 S2(config-vlan)#name Native S2(config-vlan)#exit

Crear troncos 802.1Q que utilicen la VLAN 6 nativa Interfaces F0/1y F0/2	S2#config t
	S2(config)#interface range F0/1-2
	S2(config-if)#switchport trunk encapsulation dot1q (#option)
	S2(config-if)#switchport mode trunk
	S2(config-if)#switchport trunk native vlan 6
	S2(config-if)#switchport trunk allowed vlan 2-6

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 f0/1-2 S2(config-if-range)#channel-group 1 mode active S2(config-if-range)#exit
Configurar el puerto de acceso del host para la VLAN 3 Interfaz F0/18	S2(config)#int f0/18 S2(config-if)#switchport mode access
Configurar la seguridad del puerto en los puertos de acceso Permitir 3 direcciones MAC	S2(config-if)#switchport Access vlan 3 S2(config-if)#switchport port-security maximum 3
Proteja todas las interfaces no utilizadas Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar	S2(config)#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 unused interfaces S2(config-if-range)#shutdown S2(config)#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 unused interfaces S2(config-if-range)#shutdown S2(config)#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 unused interfaces S2(config-if-range)#shutdown

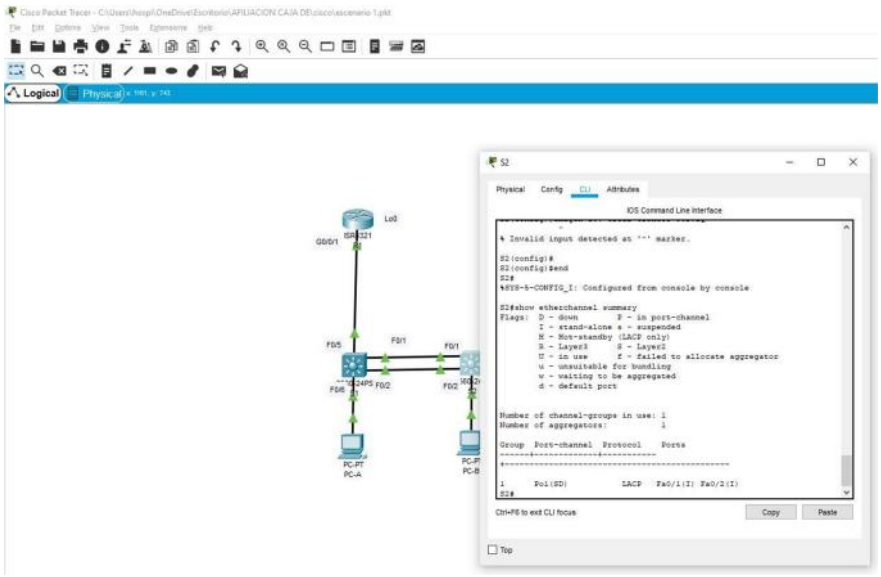
Tabla 6 – Configuración VLAN y troncales

Imagen 13. Verificación VLAN activas



Fuente – Autor

Imagen 14. Protocolo LACP para la negociación



Fuente – Autor

Paso 5: Parte 2: configurar soporte de host

Configure R1

Realizamos la Configuración del default routing, crear rutas predeterminadas para IPv4 e IPv6 que dirijan el tráfico a la interfaz loopback 0

Tarea	**Especificación**
Cofigura 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 loopback 0 R1(config)#ipv6 route ::0 loopback 0

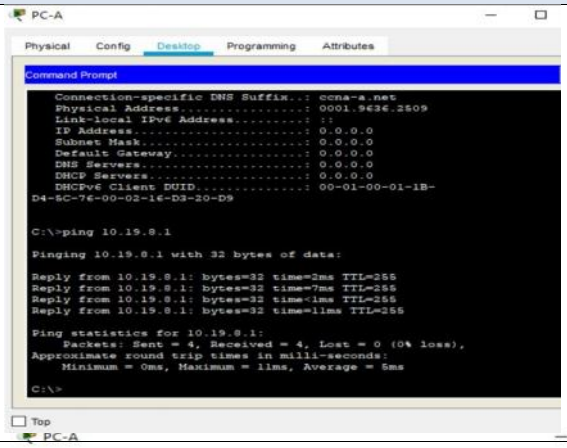
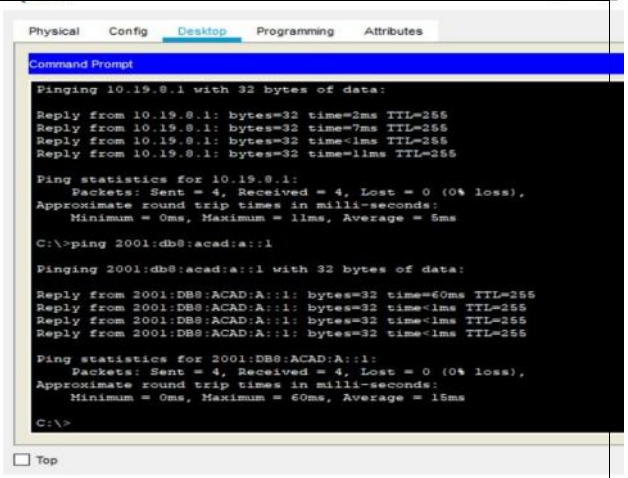
Las tareas de configuración para R1 incluyen las siguientes:

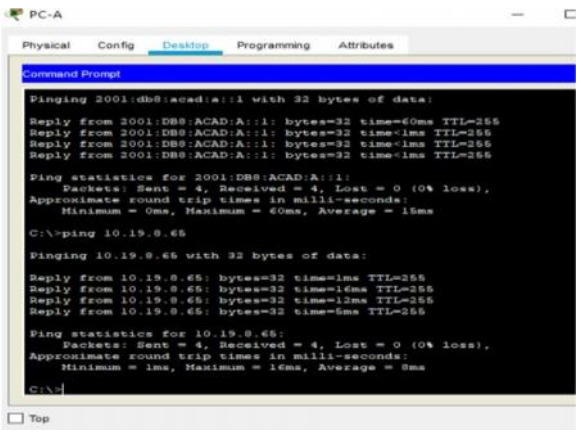
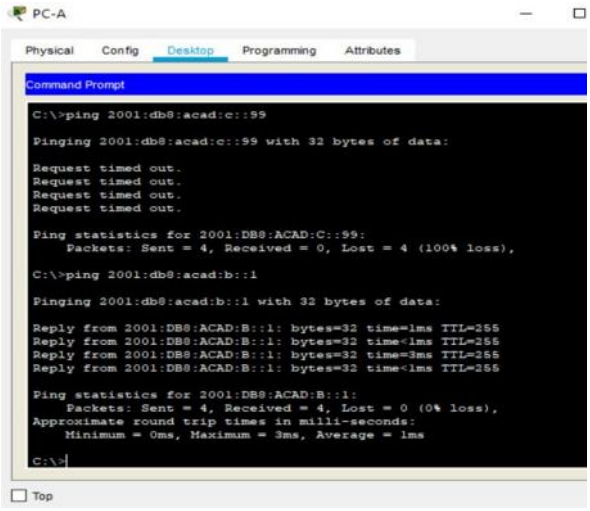
Configuráramos IPv4 DHCP para VLAN 2 y para VLAN 3, Creamos un grupo DHCP para VLAN 2 compuesto y por las últimas 10 direcciones de la subred solamente

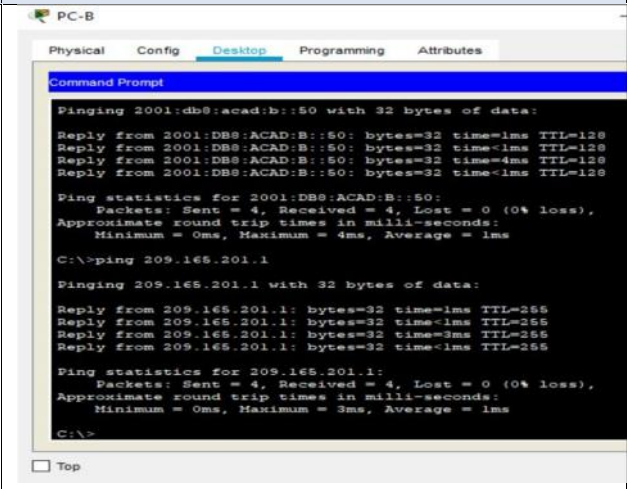
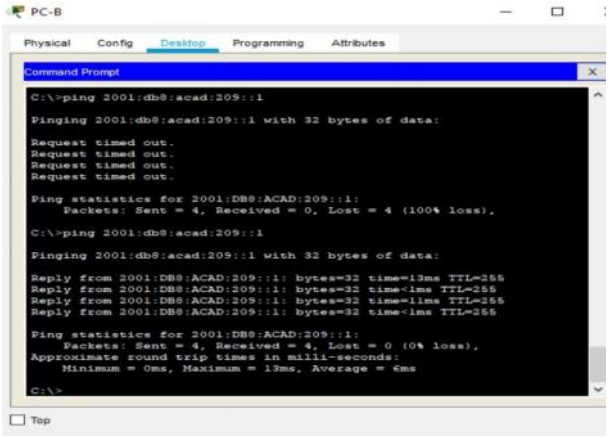
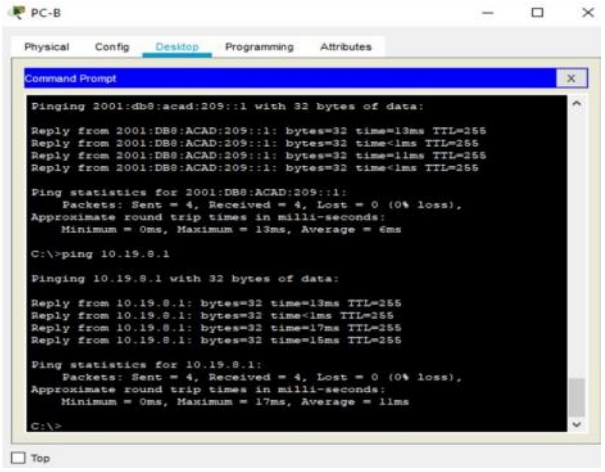
Configurar IPv4 DHCP para VLAN 2 Cree un grupo DHCP para VLAN 2, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio ccna- a.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada	R1(config)#ip 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 ccna-a.net R1(config)#exit

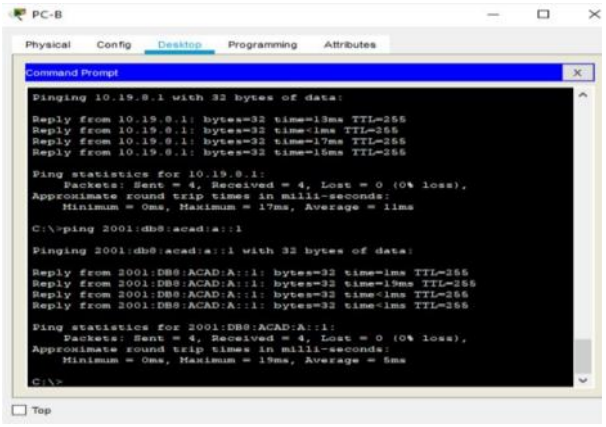
Configurar DHCP IPv4 para VLAN 3 Cree un grupo DHCP para VLAN 3, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio ccna- b.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada	R1(config)#ip dhcp excluded-address 10.19.8.65 10.19.8.84 R1(config)#ip dhcp pool vlan3-trikes R1(dhcp-config)#network 10.19.8.64 255.255.255.224 R1(dhcp-config)#default-router 10.19.8.65 R1(dhcp-config)#domain-name ccna-b.net R1(config)#exit

Tabla 7 – IPv4 DHCP para VLAN 2

Desde	A	de Interne t	Dirección IP	Resultados de ping
PC-A	R1, G0/0/1. 2	Dirección	10.19.8.1	
		IPv6	2001:db8:acad: a: :1	

Desde	A	de Internet	Dirección IP	Resultados de ping
	R1, G0/0/1.3	Dirección	10.19.8.65	
		IPv6	2001:db8:acad:b::1	

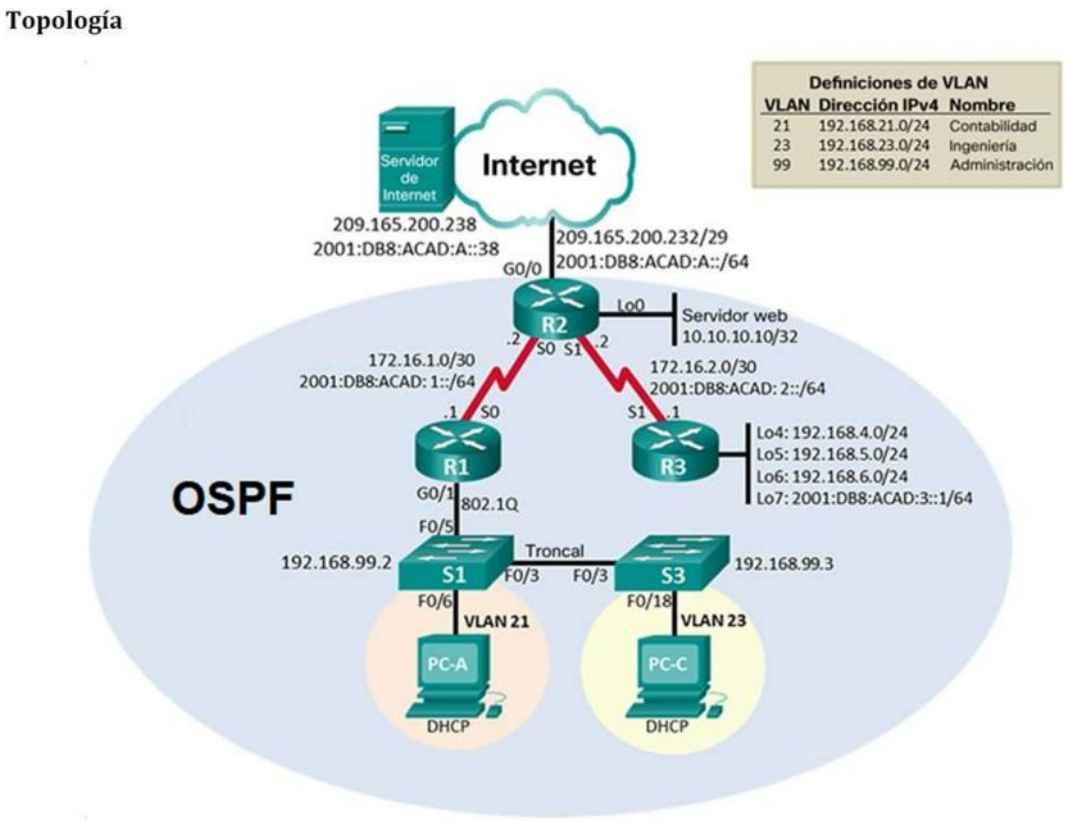
PC-A	*R1 Bucle 0*	IPv6	2001:db8:acad:209::1	*en blanco*
PC-B	R1 Bucle 0	Dirección	209.165.201.1	
		IPv6	2001:db8:acad:209: :1	
	R1, G0/0/1.2	Dirección	10.19.8.1	

		IPv6	2001:db8:acad:a::1	

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 RIPv2, el protocolo de configuración de hosts dinámicos (DHCP), la traducción de direcciones de red dinámicas y estáticas (NAT), listas de control de acceso (ACL) y el protocolo de tiempo de red (NTP) servidor/cliente. Durante la evaluación, probará y registrará la red mediante los comandos comunes de CLI.

Figura 1. TOPOLOGIA ESCENERARIO No 2



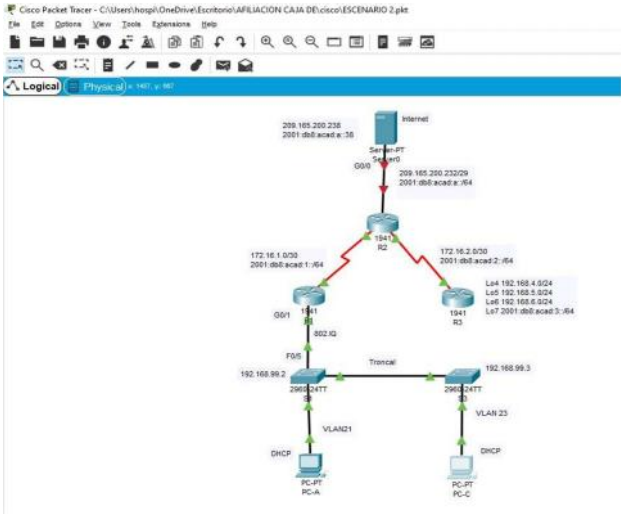
Fuente – trabajo UNAD

Parte 1: Inicializar dispositivos

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

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

Figura 2 –Topología realizada en cisco packet



Fuente -Autor

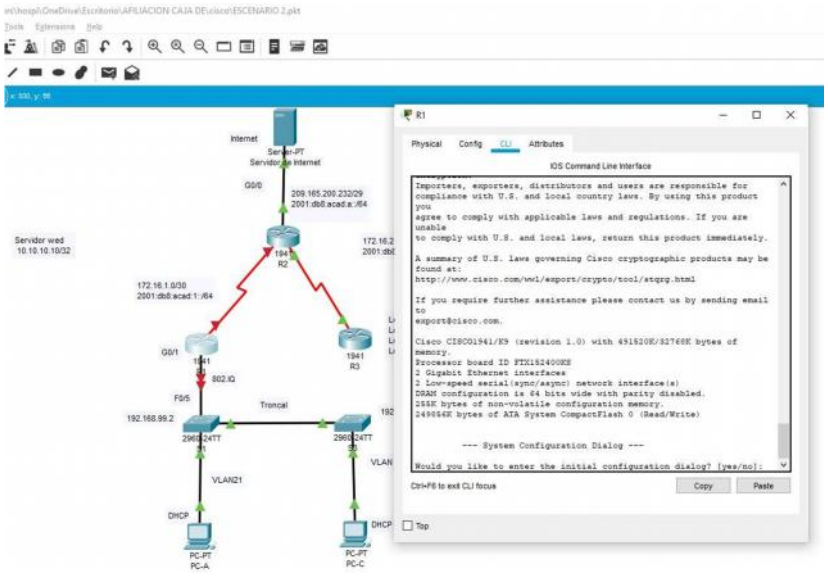
Realizamos la eliminación del archivo de configuración de inicio, ingresamos el dominio, Procedemos a configurar el router, asignando un nombre, el dominio, las contraseñas de ingrese modo privilegiado, configuramos MOTD Banner, creamos un usuario en base de datos local, habilitamos epv6 y las interfaces. Continuando con la configuración

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

Tabla 1 Iniciar dispositivos

Borramos las configuraciones de routers y se reinician

Figura 3 – Reinicio R1



Fuente - autor

Parte 2 Configurar los parámetros básicos 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):

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.230
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.225
Dirección IPv6/subred	2001:DB8:ACAD:2::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:2::1

Tabla 2 Configuración PC-A

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Realizamos la eliminación del archivo de configuración de inicio, ingresamos el dominio, Procedemos a configurar el router, asignando un nombre al R1 y al dominio, protegemos el ingreso a la consola con contraseña y e igual forma a telnet, configuramos MOTD Banner, creamos un usuario en base de datos local, habilitamos IPv6 y las interfaces

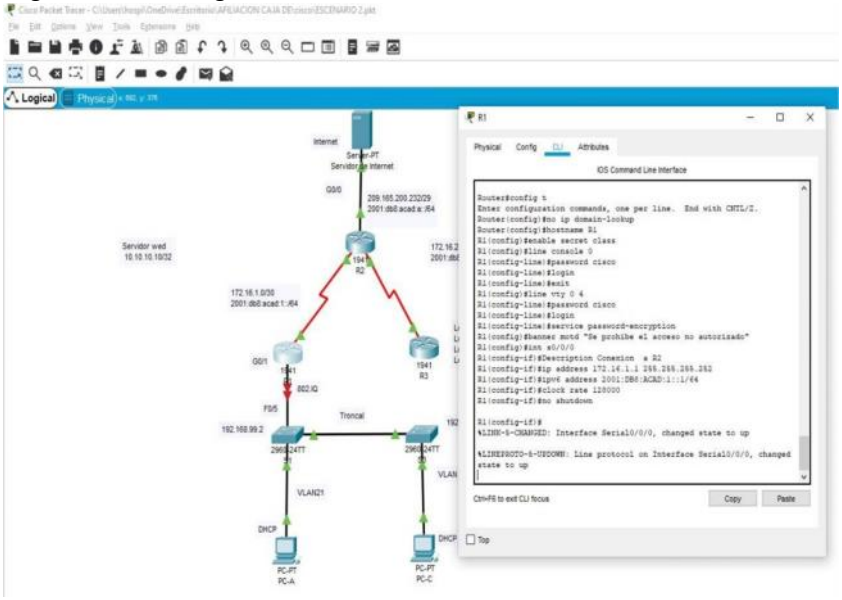
Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R1
Contraseña de exec privilegiado cifrada	R1(config)#enable secret class
Contraseña de acceso a la consola	R1(config)#line console 0 R1(config-line)#password cisco R1(config-line)#login R1(config-line)#exit
Contraseña de acceso Telnet	R1(config)#line vty 0 4 R1(config-line)#password cisco R1(config-line)#login
Cifrar las contraseñas de texto no cifrado	R1(config-line)#service password-encryption
Mensaje MOTD	R1(config)#banner motd “Se prohibe el acceso no autorizado”
Interfaz S0/0/0	R1(config)#int s0/0/0 R1(config-if)#Description Conexion a 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)#no shutdown R1(config-if)#clock rate 128000
Rutas predeterminadas	R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0 R1(config)#ipv6 route ::/0 s0/0/0

Tabla 3 Configuración R1

Se configura el router 1

Desactivar lookup DNS y configuración del router con su dirección IP, passorwd y su interfaz seria

Figura 4 – Configuración R1

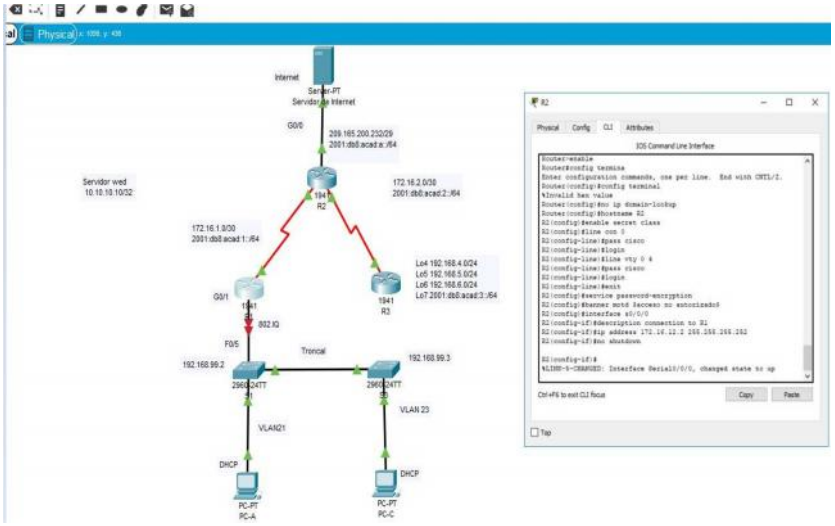


Fuente - Autor

Paso 3: Configurar R2

Configuración del router 2, configuramos el password, nombre del router R2, activación interfaz serial 0/0/0

Figura 5 – Configuración R2



Fuente - autor

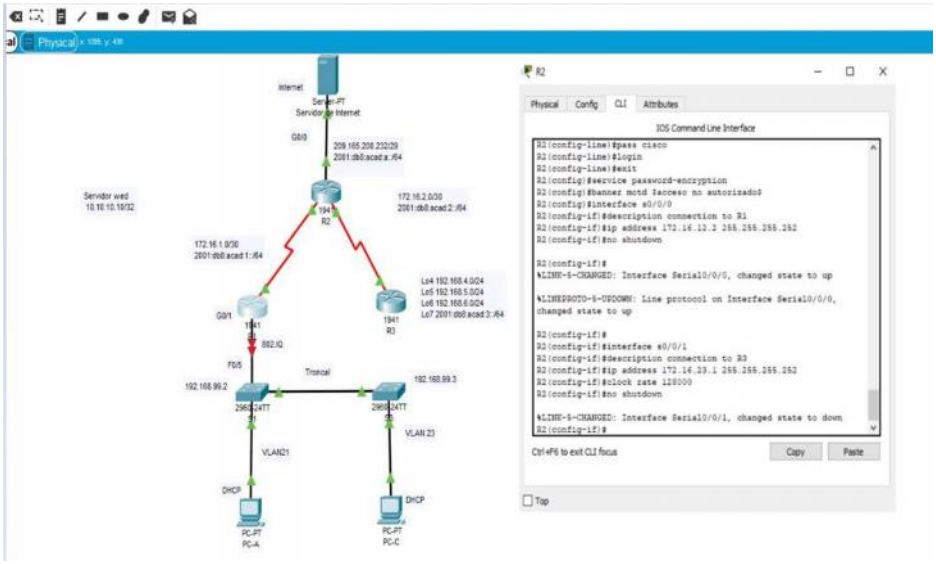
La configuración del R2 incluye las siguientes tareas:

Realizamos la eliminación del archivo de configuración de inicio, ingresamos el dominio, Procedemos a configurar el router, asignando un nombre y al dominio, asignamos contraseñas de ingrese modo privilegiado a la consola y telnet, configuramos MOTD Banner, creamos un usuario en base de datos local, habilitamos IPV6 y las interfaces

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R2
Contraseña de exec privilegiado cifrada	R2(config)#enable secret class
Contraseña de acceso a la consola	R2(config)#line console 0 R2(config-line)#password cisco R2(config-line)#login
Contraseña de acceso Telnet	R2(config)#line vty 0 4 R2(config-line)#password cisco R2(config-line)#login
Cifrar las contraseñas de texto no cifrado	R2(config)#service password-encryption
Mensaje MOTD	R2(config)#banner motd “Se prohibe el acceso no autorizado.”
Interfaz S0/0/0	R2(config)#int s0/0/0 R2(config-if)# Description Conexion a R1 R2(config-if)#ip address 172.16.12.2 255.255.255.252 R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64 R2(config-if)#no shutdown

Realizamos Activación del puerto serial 1, interfaz gibabit, configura del servidor WEB

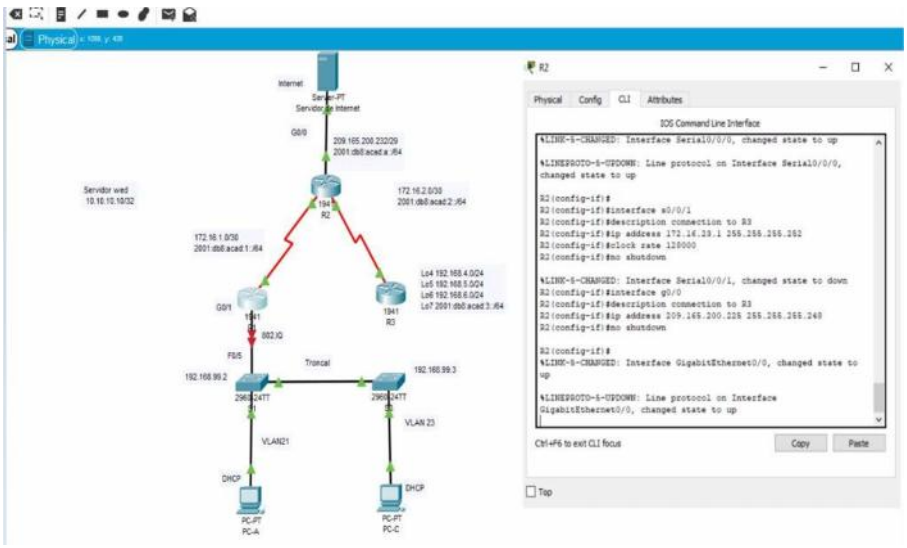
Figura 6 – Activación serial1



Fuente - Autor

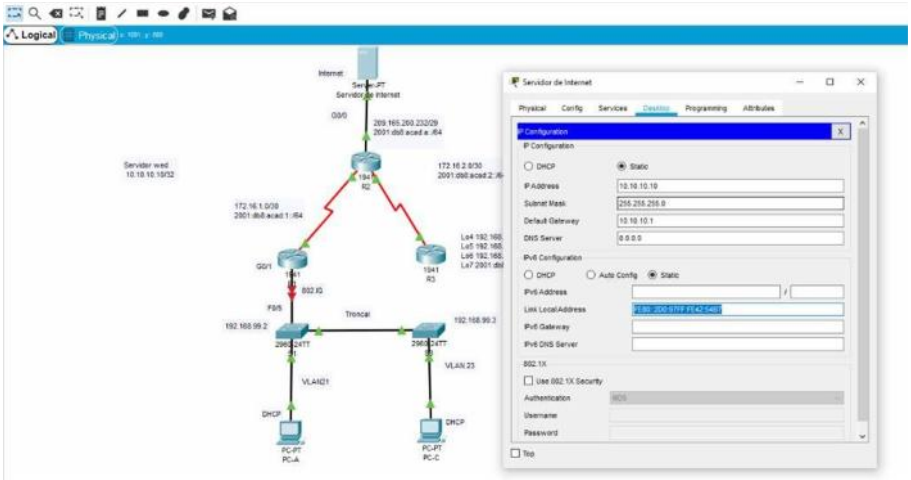
Realizamos la Activación del interfaz gigabit

Figura 7 – activación interfaz gigabit



Fuente - autor

Figura 8 – activación interfaz gibabit



Fuente - Autor

Realizamos la configuración de las interfaces permitiendo las conectividades entre ellas en IPV4 y IPV6

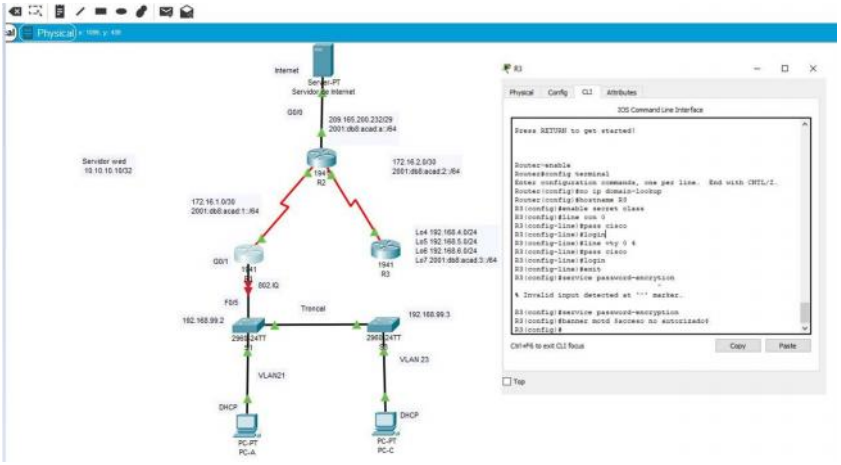
Interfaz S0/0/1	R2(config)#int s0/0/1 R2(config-if)#description Conexion a R3 R2(config-if)#ip address 172.16.23.1 255.255.255.252 R2(config-if)#ipv6 address 2001:DB8:ACAD:2::2/64 R2(config-if)#clock rate 128000 R2(config-if)#no shutdown
Interfaz G0/0 (simulación de Internet)	R2(config)#int g0/0 R2(config-if)#description connection R3 R2(config-if)#ip address 209.165.200.225 255.255.255.248 R2(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64 R2(config-if)#no shutdown
Interfaz G0/1 (simulación de Internet)	R2(config)#int g0/1 R2(config-if)# ip address 10.10.10.10 255.255.255.255 R2(config-if)#no shutdown
Ruta predeterminada	R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0 %Default route without gateway, if not a point-topoint interface, may impact performance R2(config)#ipv6 route ::/0 g0/0

Tabla 4 Configuración R2

Paso 4: Configurar R3

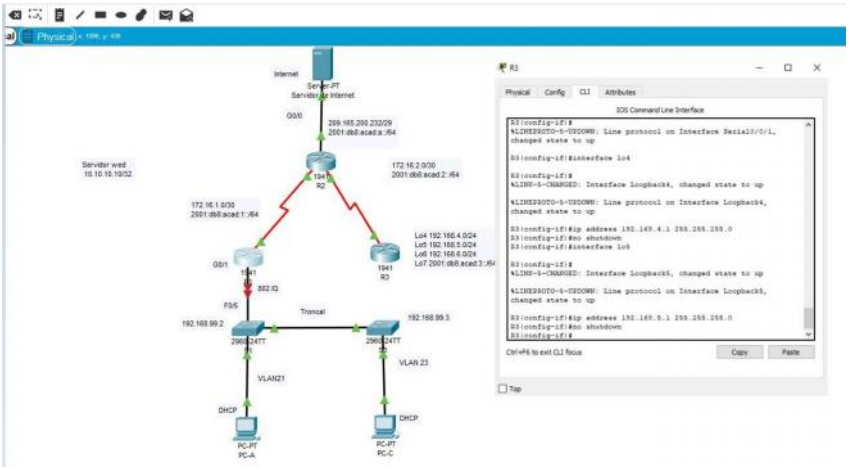
Realizamos la configuración del router 3, utilizando los parámetros del router anterior y configuramos el lookbackp

Figura 9 – Configuración R3



Fuente- autor

Figura 10 – Configuración lo



Fuente- autor

La configuración del R3 incluye las siguientes tareas:

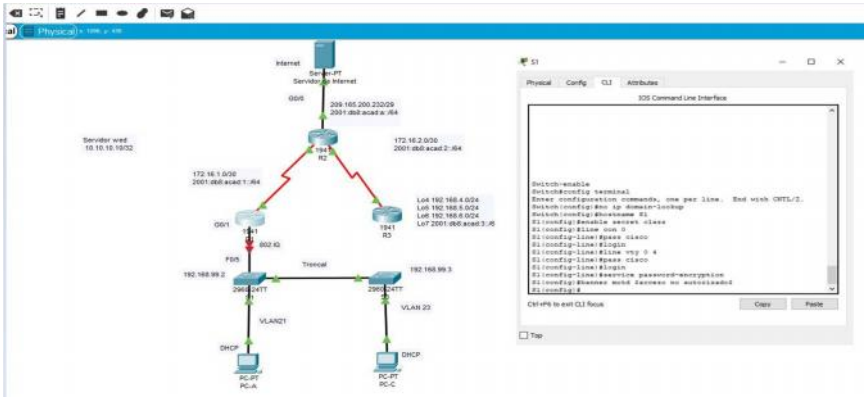
Realizamos la eliminación del archivo de configuración de inicio, ingresamos el dominio, Procedemos a configurar el router, asignando un nombre y al dominio, asignamos contraseñas de ingrese modo privilegiado a la consola y telnet, configuramos MOTD Banner, creamos un usuario en base de datos local, habilitamos IPV6 y las interfaces

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R3
Contraseña de exec privilegiado cifrada	R3(config)#enable secret class
Contraseña de acceso a la consola	R3(config)#line console 0 R3(config-line)#password cisco R3(config-line)#login
Contraseña de acceso Telnet	R3(config)#line vty 0 4 R3(config-line)#password cisco R3(config-line)#login
Cifrar las contraseñas de texto no cifrado	R3(config-line)#service password-encryption
Mensaje MOTD	R3(config)#banner motd “se prohibe el acceso no autorizado”
Interfaz S0/0/1	R3(config)#int s0/0/1 R3(config-if)#description connection R2 R3(config-if)#ip address 172.16.2.1 255.255.255.252 R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64 R3(config-if)#no shutdown
Interfaz loopback 4	R3(config)#int loopback 4 R3(config-if)#ip address 192.168.4.1 255.255.255.0
Interfaz loopback 5	R3(config)#int loopback 5 R3(config-if)#ip address 192.168.5.1 255.255.255.0
Interfaz loopback 6	R3(config-if)#int loopback 6 R3(config-if)#ip address 192.168.6.1 255.255.255.0
Interfaz loopback 7	R3(config)#int loopback 7 R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64
Rutas Predeterminada s	R3(config)#int s0/0/1 R3(config-if)#ip route 0.0.0.0 0.0.0.0 s0/0/1 %Default route without gateway, if not a pointtopoint interface, may impact performance R3(config)#ipv6 route ::/0 s0/0/1

Tabla 5 Configuración R3

Paso 5: Configurar S1

Figura 10 – Realizamos la configuración del S1



Fuente- autor

La configuración del S1 incluye las siguientes tareas:

Damos nombramiento al dominio, encriptados la contraseña, generamos contraseña para ingresar a la consola, configuramos VTY para la utilización de la base de datos, configuramos el banner para cuando ingrese un usuario sin permisos sala la ventana emergente diciendo “no está autorizado” y configuramos la interfaz.

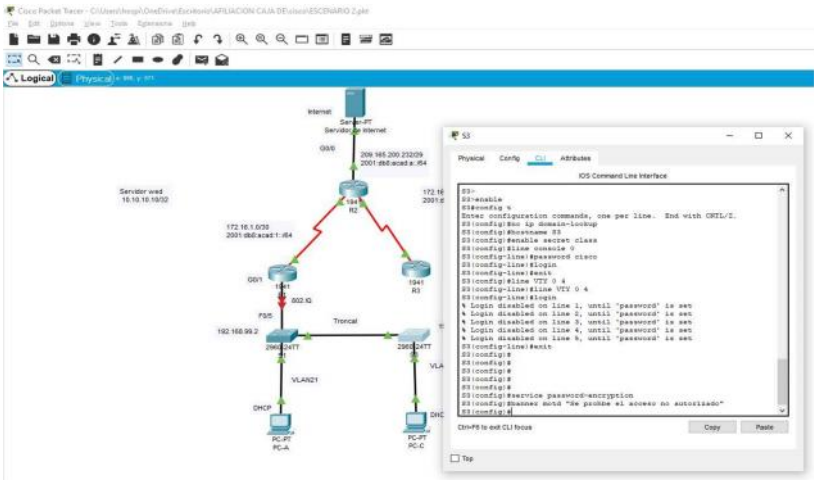
Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch>enable Switch# config t Switch(config)# no ip domain-lookup
Nombre del switch	Switch(config)# hostname S1
Contraseña de exec privilegiado cifrada	S1(config)# enable secret class
Contraseña de acceso a la consola	S1(config)#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

Contraseña de acceso Telnet	S1(config)# line VTY 0 4 S1(config-if)# password cisco S1(config-if)# login S1(config-if)# exit
Cifrar las contraseñas de texto no cifrado	S1(config)# service password-encryption
Mensaje MOTD	S1(config)# banner motd “Se prohíbe el acceso no autorizado” S1(config)# exit S1# copy running-config startup-config

Tabla 6 Configuración S1

Paso 6: Configurar el S3

Figura 11 – Realizamos la configuración de los comandos correspondientes



Fuente- autor

La configuración del S3 incluye las siguientes tareas:

Damos nombramiento al dominio, encriptados la contraseña, generamos contraseña para ingresar a la consola, configuramos VTY para la utilización de la base de datos, configuramos el banner para cuando ingrese un usuario sin permisos sala la ventana

emergente diciendo “no está autorizado” y configuramos la interfaz.

Desactivar la búsqueda DNS	Switch>enable Switch# config t Switch(config)# no ip domain-lookup
Nombre del switch	Switch(config)# hostname S3
Contraseña de exec privilegiado cifrada	S3(config)# enable secret class
Contraseña de acceso a la consola	S3(config)# line console 0 S3(config-if)# password cisco S3(config-if)# login S3(config-if)# exit
Contraseña de acceso Telnet	S3(config)# line VTY 0 4 S3(config-if)# password cisco S3(config-if)# login S3(config-if)# exit
Cifrar las contraseñas de texto no cifrado	S3(config)# service password-encryption
Mensaje MOTD	S3(config)# banner motd “Se prohíbe el acceso no autorizado”

Tabla 7 Configuración S3

Paso 7: Revisar la conectividad de la red

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

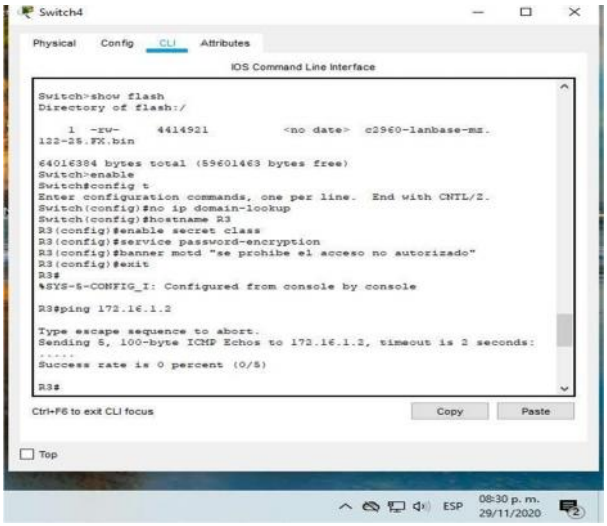
Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	Success rate is 100 percent (5/5), round-trip min/avg/max = 1/7/16 ms
R2	R3, S0/0/1	172.16.2.2	Success rate is 100 percent (5/5), round-trip min/avg/max = 1/7/12 ms
PC de Internet	Gateway predeterminado	209.165.200.233	Success

Tabla 8 Verificación de conectividad

Pantallazo de prueba de ping desde Router 1 y Router 2. Ping hacia la ip 172.16.1.2

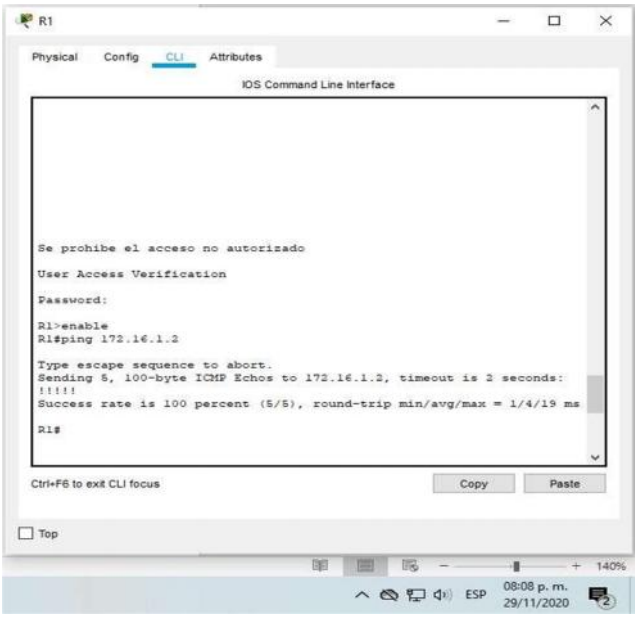
Figura 13 Ping R1 a R2



Fuente -autor

Pantallazo de prueba de ping desde Router 2 y Router 3. Ping hacia la ip 172.16.1.2

Figura 14 Ping R2 a R3Fuente: Packet Tracer

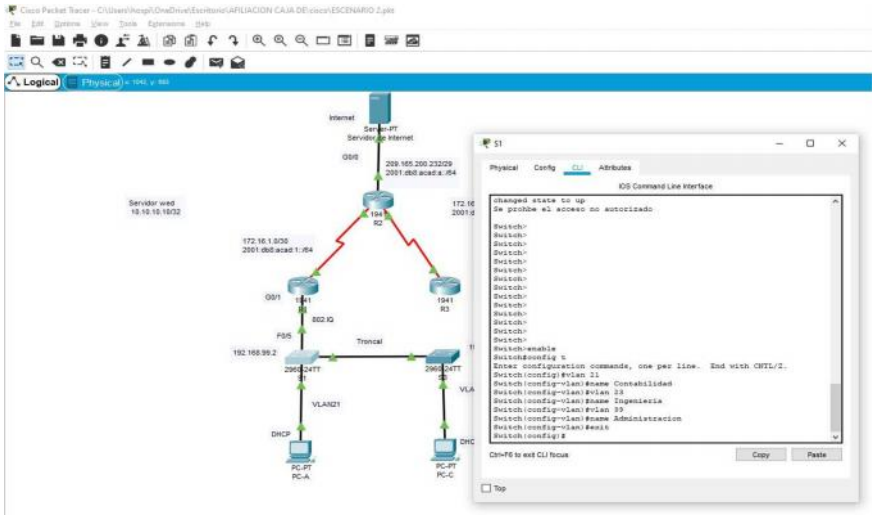


Fuente -autor

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

Configurar S1

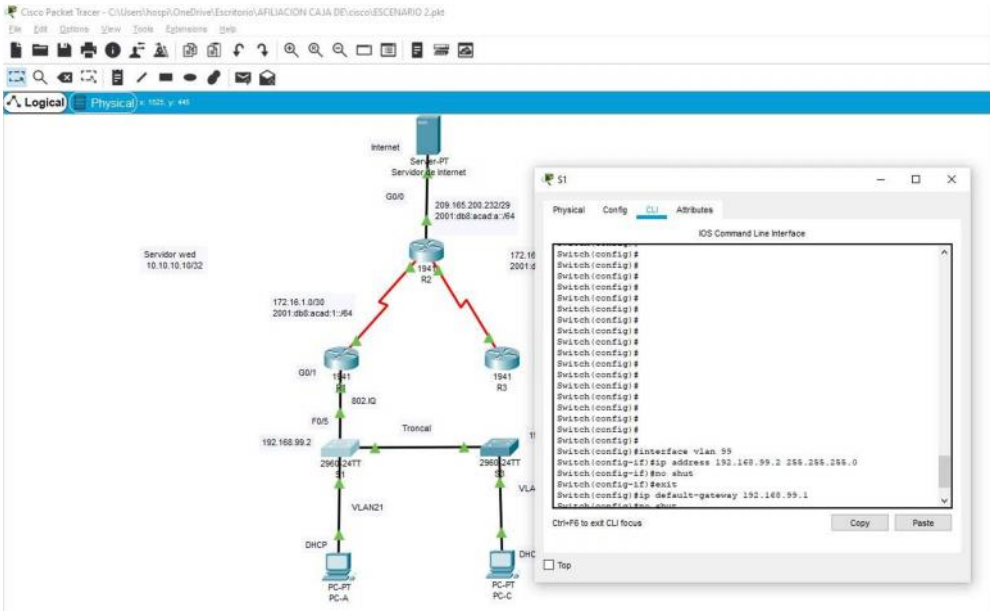
Figura 15 Configuración VLAN S1



Fuente - autor

Realizamos la asignación la dirección IP de administración y el Gateway

Figura 16 Asignación IP y gateway



Fuente Autor

Se realiza la creación de base de datos de VLAN 21, VLAN 23 y VLAN 99, se le asignan sus nombres a cada área Contabilidad, Ingeniería y Administración, asigna el direccionamiento respectivo y la configuración del gateway predeterminado.

ELEMENTO O TAREA DE CONFIGURACIÓN	ESPECIFICACIÓN
Crear la base de datos de VLAN	S1> enable S1# conf t S1(config)# vlan 21 S1(config-vlan)# name Contabilidad S1(config)# vlan 23 S1(config-vlan)# name Ingenieria S1(config)# vlan 99 S1(config-vlan)# name Administracion S1(config-vlan)# exit
Asignar la dirección IP de administración.	S1(config)# interface vlan 99 S1(config-if)# ip address 192.168.99.2 255.255.255.0 S1(config-if)#no shut S1(config-if)# exit
Asignar el gateway predeterminado	S1(config)# ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	S1(config)# interface f 0/3 S1(config-if)# switchport mode trunk S1(config-if)# switchport trunk native VLAN 1 S1(config-if)# end
Forzar el enlace troncal en la interfaz F0/5	S1(config)# interface F 0/5 S1(config-if)# switchport mode trunk S1(config-if)# switchport trunk native VLAN 1 S1(config-if)# int range f0/1-2, f0/4, f0/6-24 S1(config-if-range)# switchport mode access S1(config-if)# end
Asignar F0/6 a la VLAN 21	S1(config)# interface F 0/6 S1(config-if)# switchport access VLAN 21 S1(config-if)# int range f0/1-2, f0/4, f0/7-24 S1(config-if-range)# switchport mode access S1(config-if)# exit

Tabla 9 seguridad del S3

Paso 2: Configurar el S3

Realizamos el nombramiento de cada base VLAN, Asignar la dirección IP de administración, configuramos el Gateway.

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	S3> enable S3# conf t S3(config)# vlan 21 S3(config-vlan)# name Contabilidad S3(config)# vlan 23 S3(config-vlan)# name Ingenieria S3(config)# vlan 99 S3(config-vlan)# name Administracion S3(config-vlan)# exit
Asignar la dirección IP de administración	S3(config)# interface vlan 99 S3(config-if)# ip address 192.168.99.3 255.255.255.0 S3(config-if)# no shut S3(config-if)# exit
Asignar el gateway predeterminado.	S3(config)# ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	S3(config)# interface f 0/3 S3(config-if)# switchport mode trunk S3(config-if)# switchport trunk native VLAN 1 S3(config)# interface f 0/5 S3(config-if)# switchport mode trunk S3(config-if)# switchport trunk native VLAN 1 S3(config-if)# int range f0/1-2, f0/4, f0/7-24, g0/1-2 S3(config-if-range)# switchport mode Access S3(config-if)# exit S3(config)# interface f 0/6 S3(config-if)# switchport mode trunk S3(config-if)#

	switchport trunk native VLAN 1
Asignar F0/18 a la VLAN 23	S3(config-if)# int range f0/1-2, f0/4, f0/7-24, g0/1-2 S3(config-if)# no shutdown S3(config-if)# exit

Tabla 10 seguridad del S3

Paso 3: Configurar R1

Configurarnos la sub interfaz y encapsulación de las IP y realizamos la activación de la interfaz g0/1

Elemento o tarea de configuración	**Especificación**
Configurar la subinterfaz 802.1Q .21 en G0/1	R1> enable R1# conf t R1(config)# interface G 0/1.21 R1(config-subif)# encapsulation dot1Q 21 R1(config-subif)# ip address 192.168.21.1 255.255.255.0
Configurar la subinterfaz 802.1Q .23 en G0/1	R1(config)# interface G 0/1.23 R1(config-subif)# description vlan23 R1(config-subif)# encapsulation dot1Q 23 R1(config-subif)# ip address 192.168.23.1 255.255.255.0
Configurar la subinterfaz 802.1Q .99 en G0/1	R1(config)# interface G 0/1.99 R1(config-subif)# description vlan99 R1(config-subif)# encapsulation dot1Q 99 R1(config-subif)# ip address 192.168.99.1 255.255.255.0
Activar la interfaz G0/1	R1(config)# interface G 0/1 R1(config-if)# no sh R1(config-if)#end

Tabla 11 seguridad del R1

Paso 4: Verificar la conectividad de la red

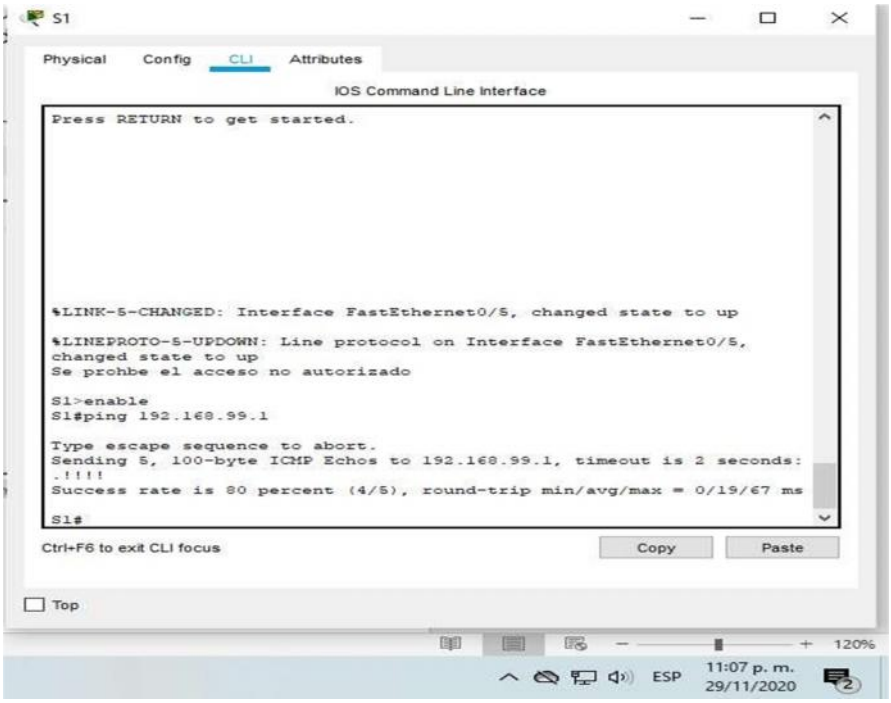
Utilice el comando **ping** para probar la conectividad entre los switches y el R1.

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:

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

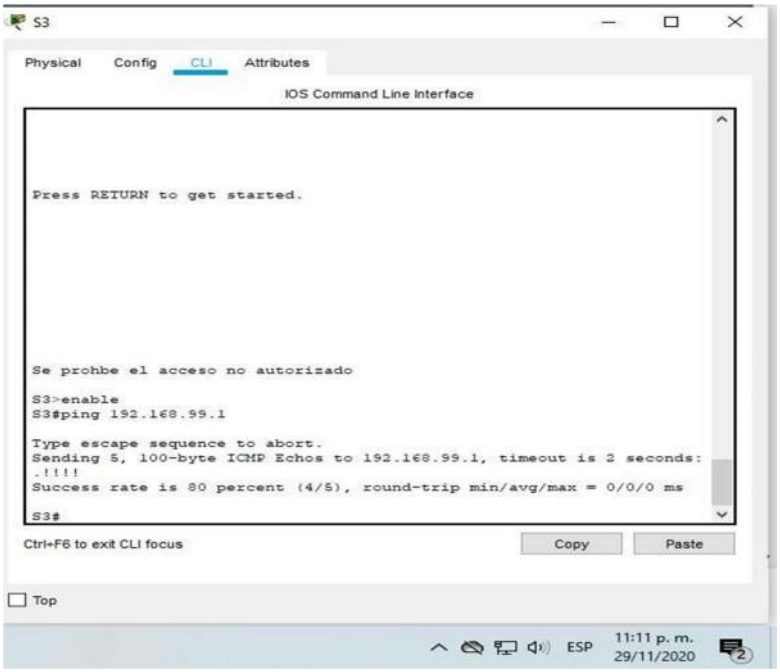
Tabla 12 Verificación de conectividad

Figura 17 - Ping S1 a VLAN 99 y VLAN 21



Fuente – autor

Figura 18 - Ping S3 a VLAN 99 y VLAN 21



Fuente - autor

Parte 2: Configurar el protocolo de routing dinámico OSPF

Paso 1: Configurar OSPF en el R1

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	
Anunciar las redes conectadas directamente	Asigne todas las redes conectadas directamente.
Establecer todas las interfaces LAN como pasivas	
Desactive la sumarización automática	

Realizamos la configuración del RIP versión 2, Anunciar las redes conectadas, Establecer todas las interfaces LAN y Desactive la sumarización automática

Elemento o tarea de configuración	Especificación
Configurar RIP Versión 2	R1> enable R1# config t R1(config)# router rip R1(config-router)# version 2
	R1(config-router)# do show ip route connected
Anunciar las redes conectadas directamente	R1(config-router)# network 172.16.1.0 R1(config-router)# network 192.168.21.0 R1(config-router)# network 192.168.23.0 R1(config-router)# network 192.168.99.0
Establecer todas las interfaces LAN como pasivas	R1(config-router)# passive-interface G 0/1.21 R1(config-router)# passive-interface G 0/1.23 R1(config-router)# passive-interface G 0/1.99
Desactive la sumarización automática	R1(config-router)# no auto-summary R1(config-router)# end

Tabla 13 Configuración RIP EN R1

Paso 2: Configurar OSPF en el R2

La configuración del R2 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	
Anunciar las redes conectadas directamente	**Nota:** Omitir la red G0/0.
Establecer la interfaz LAN (loopback) como pasiva	
Desactive la sumarización automática.	

Realizamos la configuración del RIP versión 2, Anunciar las redes conectadas, Establecer todas las interfaces LAN y Desactive la sumarización automática

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	R2> enable R2# config t R2(config)# router rip R2(config-router)# version 2
	R2(config-router)# do show ip route connected
Anunciar las redes conectadas directamente	R2(config-router)# network 10.10.10.10 R2(config-router)# network 172.16.1.0 R2(config-router)# network 172.16.2.0
Anunciar las redes conectadas directamente	R2(config-router)# passive-interface loopback 0
Desactive la sumarización automática.	R2(config-router)# no auto-summary R2(config-router)# end

Tabla 14 Configuración RIP EN R2

Paso 3: Configurar OSPFv3 en el R2

La configuración del R3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	
Anunciar redes IPv4 conectadas directamente	
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	
Desactive la sumarización automática.	

Configurar RIP versión 2 en R3, Anunciar redes IPv4 conectadas directamente Establecer todas las interfaces de LAN

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	R3>enable R3(config)#ip Access-list standard ADMIN-MGT R3(config-sld-nacl)#permit host 172.16.1.1
Anunciar redes IPv4 conectadas directamente	R3(config)#line vty 0 4 R3(config-line)#access-class ADMIN-MGT in
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	R3(config-line)#transport input telnet
Desactive la sumarización automática.	R3(config-router)# no auto-summary R3(config-router)# end

Tabla 15 Configuración RIP EN R3

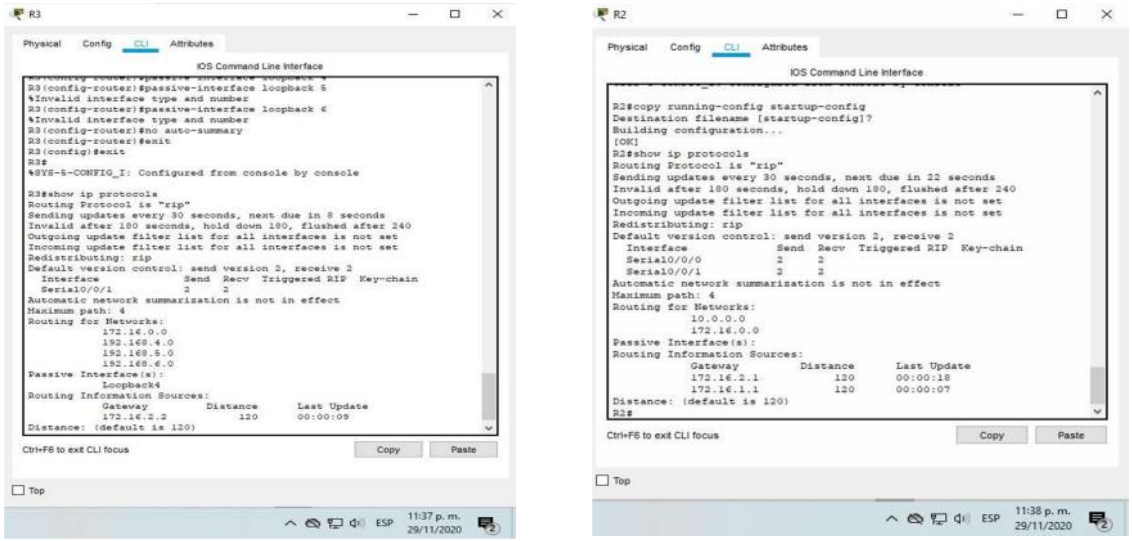
Paso 4: Verificar la información de OSPF

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

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?	R3#show ip protocols
¿Qué comando muestra solo las rutas OSPF?	R3#show ip route rip
¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	R3#show run I section router rip R3#show run

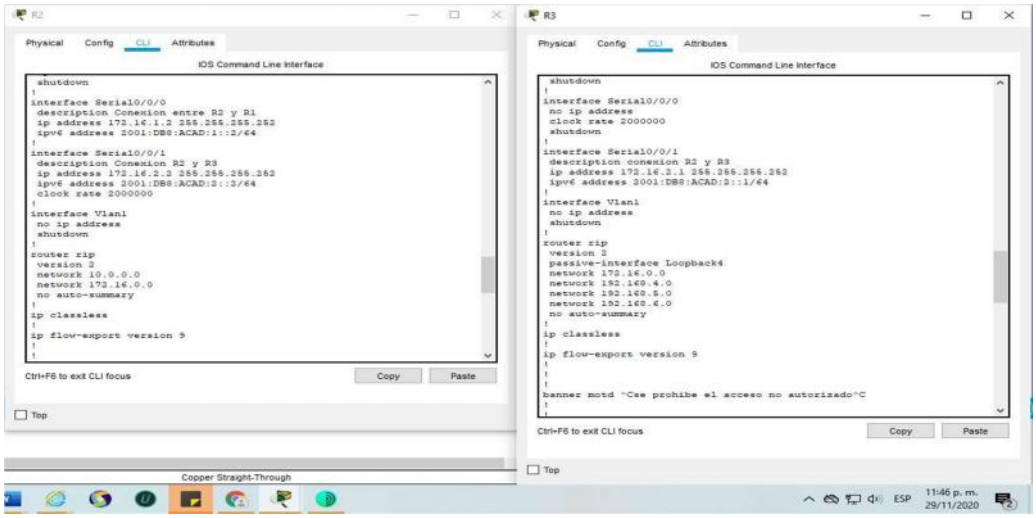
Tabla 16 Verificación OSPF

Figura 19 – Verificación de protocolos



Fuente – autor

Figura 20 – Comando show run



Fuente - autor

Parte 3: 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:

Reservar las primeras 20 direcciones para configuraciones estáticas IP en la VLAN 21 Y VLAN 23, Crear un pool de DHCP para la VLAN 21 y VLAN 23

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

Tabla 17 DHCP y NAT IPv4 en R1

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

La configuración del R2 incluye las siguientes tareas:

Creamos una base de datos locales con una cuenta de usuario, Habilitar el servicio del servidor HTTP y los configuramos, Crear una NAT estática al servidor web, Asignar la interfaz interna y externa para la NAT estática, Configurar la NAT dinámica dentro de una ACL privada y Defina el pool de direcciones IP públicas utilizables.

Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	R2> enable R2# config t R2(config)# username webuser password cisco12345 R2(config)# line console 0 R2(config)# login local
Habilitar el servicio del servidor HTTP	R2(config)# ip http server R2(config)# ip http secure-server
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	R2(config)# ip http authentication local R2(config)# username webuser privilege 15 secret cisco12345 R2(config)# line vty 0 15 R2(config-line)# privilege level 15 R2(config-line)# login local R2(config-line)# transport input ssh
Crear una NAT estática al servidor web.	R2(config)# ip nat insidesource static 10.10.10.10 209.165.200.237
Asignar la interfaz interna y externa para la NAT estática	R2(config)# int G 0/0 R2(config-if)# ip nat outside R2(config)# int S 0/0/0 R2(config-if)# ip nat inside R2(config)#exit R2(config)# int S 0/0/1 R2(config-if)# ip nat inside R2(config)#exit
Configurar la NAT dinámica dentro de una ACL privada	R2(config)# access-list 1 permit 192.168.21.0 0.0.0.255 R2(config)# access-list 1 permit 192.168.23.0 0.0.0.255 R2(config)# access-list 1 permit 192.168.4.0 0.0.3.255

Defina el pool de direcciones IP públicas utilizables.	R2(config)# ip nat pool INTERNET 209.165.200.233 209.165.200.236 netmask 255.255.255.248
Definir la traducción de NAT dinámica	R2(config)# ip nat inside source list 1 pool INTERNET

Tabla 18 DHCP y NAT IPv4 en 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.

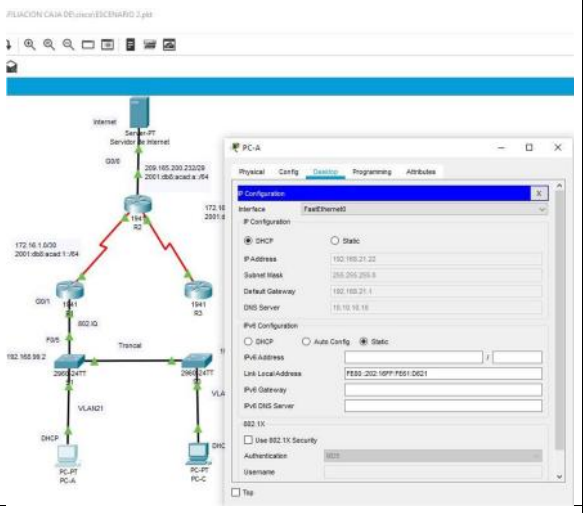
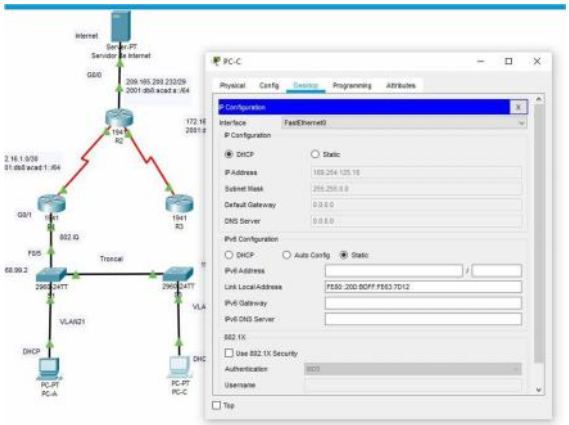
Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	

Tabla 19 verificación DHCP y la NAT

Parte 4: Configurar NTP

Configure R2 como un maestro NTP y Configurar R1 como un cliente NTP.

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	R2> enable R2# clock set 10:00:00 jun 9 2020
Configure R2 como un maestro NTP.	R2(config)# ntp master 5 R2(config)# end
Configurar R1 como un cliente NTP.	R1> enable R1# config t R1(config)# ntp server 172.16.1.2 R1(config)# ntp update-calendar R1#ntp up

Tabla 20 configuración NTP

Parte 5: Configurar y verificar las listas de control de acceso (ACL)

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

Realizamos la configurcionr una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2 y Aplicar la ACL con nombre a las líneas VTY

Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	R2> enable R2# conf t R2(config)# ip access-list standard ADMIN-MGT R2(config-std-nacl)# permit host 172.16.1.1
Aplicar la ACL con nombre a las líneas VTY	R2(config)# line VTY 0 4 R2(config-line)#transport input telnet R2(config)# access-class standard ADMIN- MGT in R2(config-line)# exit
Permitir acceso por Telnet a las líneas de VTY	R2(config)# line telnet 172.16.1.2 Password

Tabla 21 configuración ACL

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

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 R2#show ip access-list
Restablecer los contadores de una lista de acceso	R2#clear ip access-list counters
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	R2#show ip interfaces
¿Con qué comando se muestran las traducciones NAT?	R2#show ip nat translations
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	R2#clear ip nat translation *

Tabla 22 Visualización comando CLI

CONCLUSIONES

El comando show ip route además de mostrar la información de las redes, enrutamiento e interfaces, es importante para identificar problemas de enrutamiento. Las interfaces físicas que enrutan los datos enviados a través del protocolo ICMP entre los tres Switches están configuradas en modo troncal.

Mediante el uso del comando show interfaces trunk, se evidencia el encapsulamiento, observándose en un modo compatible. Es significativo utilizar correctamente las topologías para realizar las conexiones Switch de capa 3 los cuales comple con la función de enrutamiento entre VLANs, logrando comunicar el tráfico ICMP en la red propuestas.

Cuando se realizó ping entre los Switches y los PCs no fue exitoso debido a que tienen habilitadas las VLANs en cada uno de los Switches con el protocolo VTP y también se dispusieron todas las interfaces están conectadas en modo de acceso con la VLAN correspondiente. Se pudo evidenciar la ventaja del protocolo BGP porque permite intercambiar la información de encaminamiento entre sistemas autónomos.

BIBLIOGRAFÍA

CISCO. (2017). Listas de control de acceso. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module9/index.html#9.0.1.1

CISCO. (2017). Configurar las Listas de Acceso IP. Recuperado de https://www.cisco.com/c/es_mx/support/docs/security/ios-firewall/23602-confaccesslists.html

CISCO. (2006). Uso de los comandos Ping Extendido y Traceroute Extendido. Recuperado de https://www.cisco.com/c/es_mx/support/docs/ip/routing-information-protocol-rip/13730-ext-ping-trace.html

CISCO. (2006). Configurar ACL de IP de uso general. Recuperado de https://www.cisco.com/c/es_mx/support/docs/ip/access-lists/26448-ACLsamples.html.

OBSERVATORIO TECNOLOGICO. (2012). Utilización de ACL en routers.

Recuperado de

http://recursostic.educacion.es/observatorio/web/es/component/content/article/1065-listas-de-control-de-acceso-acl?start=3

ANEXOS

Escenario 1

https://onedrive.live.com/?cid=8BDFEF49486A8908&id=8BDFEF49486A8908%21261&parId=8BDFEF49486A8908%21259&o=OneUp

Escenario 2

https://onedrive.live.com/?cid=8BDFEF49486A8908&id=8BDFEF49486A8908%21260&parId=8BDFEF49486A8908%21259&o=OneUp

Video

https://onedrive.live.com/?cid=8BDFEF49486A8908&id=8BDFEF49486A8908%21262&parId=8BDFEF49486A8908%21259&o=OneUp

Diseño de una red

Ivan dario Murcia Angel

universidad nacional, abierta y a distancia (unad), ivan83_d@hotmail.com

RESUMEN

La presente actividad contiene dos escenarios que se debe aplicar los conocimientos adquiridos en CISCO de armar la topología y realizar la configuración de cada uno de los dispositivos de una red, garantizar la seguridad de ingreso utilizando contraseña, se debe realizar el nombramiento de vlan.

Palabras Claves: Red Lan, Dispositivos, Red Wan, Router, Computadores

Abstrac:

This activity contains two scenarios that must apply the knowledge acquired in CISCO to build the topology and configure each of the devices in a network, guarantee the security of entry using a password, and the vlan must be appointed.

Keywords: Lan Network, Devices, Wan Network, Router, Computers

Introducción

En este artículo se menciona el desarrollo de un escenario, teniendo en cuenta que se debe realizar las respectivas configuraciones de switchs y router el cual se implementa protocolo de autenticación para ingresar con contraseña. el host se realiza configuración del protocolo dhcp y NAT, el cual permite intensificar las direcciones ip de origen dentro de direcciones definida

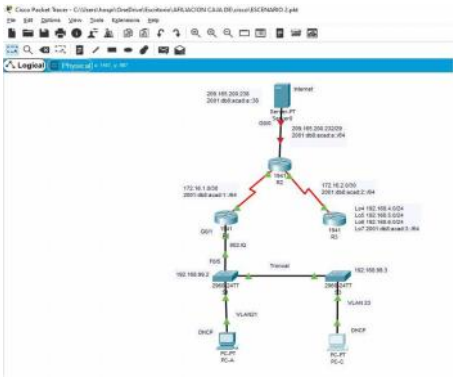
Metodología:

Diseño de redes: Se realiza la configuración de una topología red utilizando 3 router, dos swiches, dos PC y un servidor, en el proceso de ingreso a los dispositivos se debe digitar la contraseña, se nombran vlan en cada interfaz y se ingresan cada puerto. Utilizando el encapsulamiento avala la seguridad de la red.

Implementación:

Utilizando un simulador que permite emular la vida real, utilizamos para crear una topología utilizando los diferentes dispositivos que aquí encontramos.

En el escenario se desarrolla utilizando los siguientes dispositivos, 1 servidor con acceso a configuración de cada dispositivo utilizando de protección una contraseña, se realiza la configuración del servidor para acceder a internet, en cada router se nombran las vlan y se asignan los puertos e interfaz activas las que se requiere. Posteriormente se implementa el protocolo DHCP el cual permite generar automática una dirección IP a los Pc y el protocolo NAT que admite tomar cualquier dirección IP definiendo un rango para



mostrar como dirección IP de origen.

Figura 2 –Topología realizada en cisco packet
Fuente -Autor

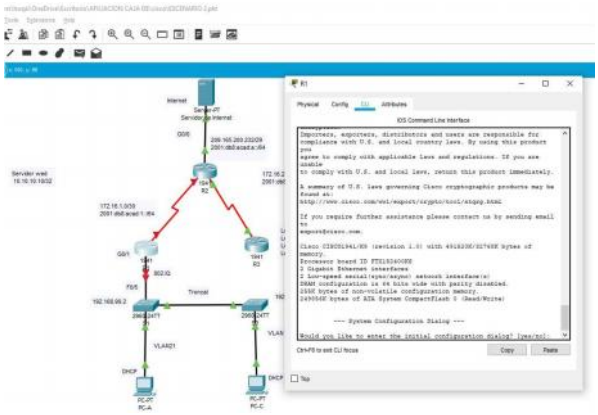
Elimine las configuraciones de inicio y vuelva a cargar los dispositivos.

Realizamos la eliminación del archivo de configuración de inicio, ingresamos el dominio, Procedemos a configurar el router, asignando un nombre, el dominio, las contraseñas de ingrese modo privilegiado, configuramos MOTD Banner, creamos un usuario en base de datos local, habilitamos epv6 y las interfaces. Continuando con la configuración

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

Borramos las configuraciones de routers y se reinician

Figura 3 – Reinicio R1



Fuente - autor

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

Elemento o tarea de configuración	**Especificación**
Dirección IPv4	209.165.200.230
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.225
Dirección IPv6/subred	2001:DB8:ACAD:2::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:2::1

Tabla 2 Configuración PC-A

Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Realizamos la eliminación del archivo de configuración de inicio, ingresamos el dominio, Procedemos a configurar el router, asignando un nombre al R1 y al dominio, protegemos el ingreso a la consola con contraseña y e igual forma a telnet, configuramos MOTD Banner, creamos un usuario en base de datos local, habilitamos IPv6 y las interfaces

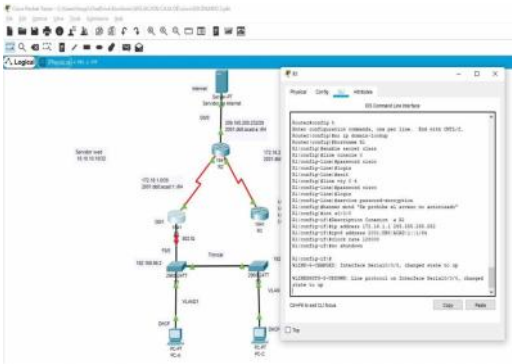
Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R1
Contraseña de exec privilegiado cifrada	R1(config)#enable secret class
Contraseña de acceso a la consola	R1(config)#line console 0 R1(config-line)#password cisco R1(config-line)#login R1(config-line)#exit
Contraseña de acceso Telnet	R1(config)#line vty 0 4 R1(config-line)#password cisco R1(config-line)#login
Cifrar las contraseñas de texto no cifrado	R1(config-line)#service password-encryption
Mensaje MOTD	R1(config)#banner motd “Se prohibe el acceso no autorizado”
Interfaz S0/0/0	R1(config)#int s0/0/0 R1(config-if)#Description Conexion a 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)#no shutdown R1(config-if)#clock rate 128000
Rutas predeterminadas	R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0 R1(config)#ipv6 route ::/0 s0/0/0

Tabla 3 Configuración R1

Se configura el router 1

Desactivar lookup DNS y configuración del router con su dirección IP, password y su interfaz seria

Figura 4 – Configuración R1

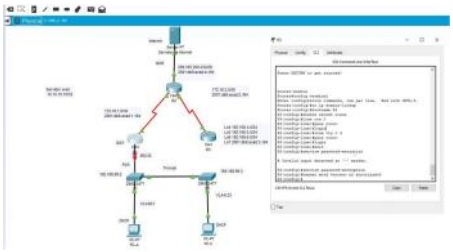


Fuente - Autor

Configurar R3

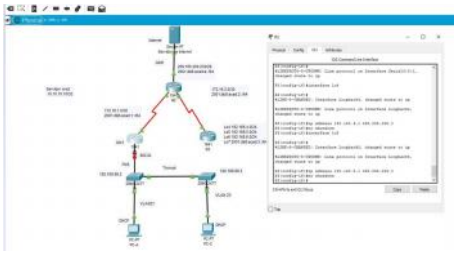
Realizamos la configuración del router 3, utilizando los parámetros del router anterior y configuramos el lookbackp

Figura 9 – Configuración R3



Fuente- autor

Figura 10 – Configuración lo



Fuente- autor

La configuración del S1 incluye las siguientes tareas:

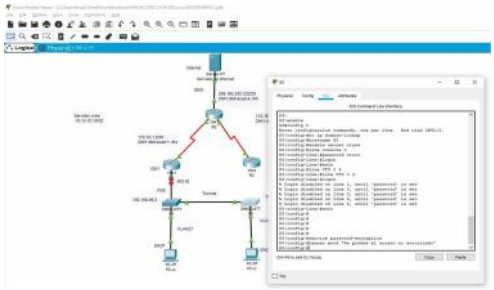
Damos nombramiento al dominio, encriptados la contraseña, generamos contraseña para ingresar a la consola, configuramos VTY para la utilización de la base de datos, configuramos el banner para cuando ingrese un usuario sin permisos sala la ventana emergente diciendo “no está autorizado” y configuramos la interfaz.

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch>enable Switch# config t Switch(config)# no ip domain-lookup
Nombre del switch	Switch(config)# hostname S1
Contraseña de exec privilegiado cifrada	S1(config)# enable secret class
Contraseña de acceso a la consola	S1(config)# line console 0 S1(config-if)# password cisco S1(config-if)# login S1(config-if)# exit
Contraseña de acceso Telnet	S1(config)# line VTY 0 4 S1(config-if)# password cisco S1(config-if)# login S1(config-if)# exit
Cifrar las contraseñas de texto no cifrado	S1(config)# service password-encryption
Mensaje MOTD	S1(config)# banner motd “Se prohíbe el acceso no autorizado” S1(config)# exit S1# copy running-config startup-config

Tabla 6 Configuración S1

Configurar el S3

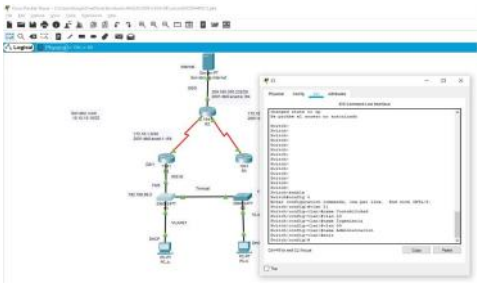
Figura 11 – Realizamos la configuración de los comandos correspondientes



Fuente- autor

Configurar la seguridad del switch, las VLAN y el routing entre VLAN Configurar S1

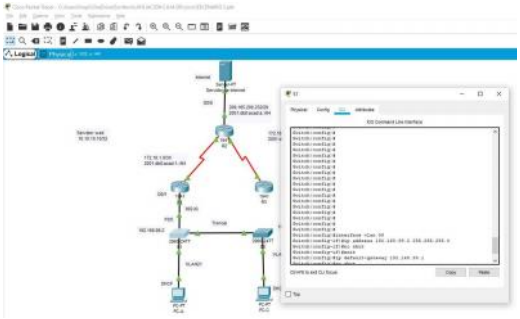
Figura 15 Configuración VLAN S1



Fuente - autor

Realizamos la asignación la dirección IP de administración y el Gateway

Figura 16 Asignación IP y Gateway



Fuente Autor

Se realiza la creación de base de datos de VLAN 21, VLAN 23 y VLAN 99, se le asignan sus nombres a cada área Contabilidad, Ingeniería y Administración, asigna el direccionamiento respectivo y la configuración del gateway predeterminado

ELEMENTO O TAREA DE CONFIGURACIÓN	ESPECIFICACIÓN
Crear la base de datos de VLAN	S1> enable S1# conf t S1(config)# vlan 21 S1(config-vlan)# name Contabilidad S1(config)# vlan 23 S1(config-vlan)# name Ingenieria S1(config)# vlan 99 S1(config-vlan)# name Administracion S1(config-vlan)# exit
Asignar la dirección IP de administración.	S1(config)# interface vlan 99 S1(config-if)# ip address 192.168.99.2 255.255.255.0 S1(config-if)#no shut S1(config-if)# exit
Asignar el gateway predeterminado	S1(config)# ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	S1(config)# interface f 0/3 S1(config-if)# switchport mode trunk S1(config-if)# switchport trunk native VLAN 1 S1(config-if)# end
Forzar el enlace troncal en la interfaz F0/5	S1(config)# interface F 0/5 S1(config-if)# switchport mode trunk S1(config-if)# switchport trunk native VLAN 1 S1(config-if)# int range f0/1-2, f0/4, f0/6-24 S1(config-if-range)# switchport mode access S1(config-if)# end
Asignar F0/6 a la VLAN 21	S1(config)# interface F 0/6 S1(config-if)# switchport access VLAN 21 S1(config-if)# int range f0/1-2, f0/4, f0/7-24 S1(config-if-range)# switchport mode access S1(config-if)# exit

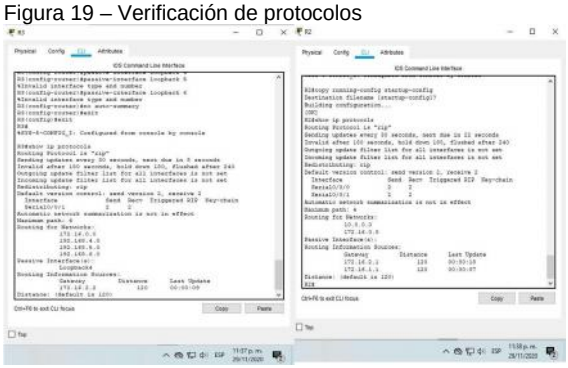
Tabla 9 seguridad del S3

Configurarnos la sub interfaz y encapsulación de las IP y realizamos la activación de la interfaz g0/1

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	R1> enable R1# conf t R1(config)# interface G 0/1.21 R1(config-subif)# encapsulation dot1Q 21 R1(config-subif)# ip address 192.168.21.1 255.255.255.0
Configurar la subinterfaz 802.1Q .23 en G0/1	R1(config)# interface G 0/1.23 R1(config-subif)# description vlan23 R1(config-subif)# encapsulation dot1Q 23 R1(config-subif)# ip address 192.168.23.1 255.255.255.0
Configurar la subinterfaz 802.1Q .99 en G0/1	R1(config)# interface G 0/1.99 R1(config-subif)# description vlan99 R1(config-subif)# encapsulation dot1Q 99 R1(config-subif)# ip address 192.168.99.1 255.255.255.0
Activar la interfaz G0/1	R1(config)# interface G 0/1 R1(config-if)# no sh R1(config-if)#end

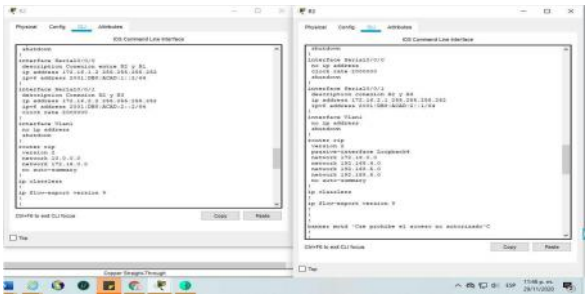
Tabla 11 seguridad del R1

Figura 19 – Verificación de protocolos



Fuente – autor

Figura 20 – Comando show run



Fuente - autor

Conclusiones:

Para realizar las configuraciones pertinentes debemos tener conocimientos necesarios para enrutar cada dispositivo, protegiéndolos con contraseñas para que el personal no autorizado no ingrese y solucionando los errores que se presenten en cada configuración. Es importante los protocolo de DHCP y NAT que permite de una forma mas ágil configurar el canal de comunicación de cada PC.

Pruebas de funcionalidad

PC A

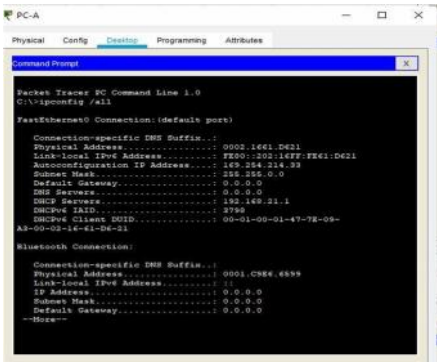


Figura 1

Servido de internet

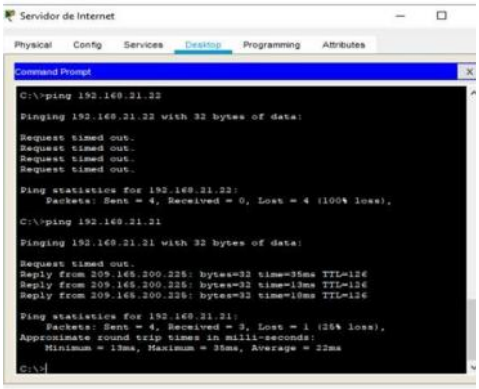


Figura 2

BIOGRAFIA

Mi nombre es Ivan Dario Murcia ángel, nací el 11 de febrero de 1983 en el municipio de Falan Tolima ubicado en el norte del Tolima, realicé mis estudios hasta cuarto grado de escolaridad en la escuela a la normal de Fabio Lozano Torrijo.

Llegamos al municipio de Planadas Tolima en el año 1992 por motivos de ascenso laboral de mi padre, continúe mis estudios en la escuela Maria Inmaculada, terminando con éxito la básica primaria; continúe en el colegio departamental de enseñanza media culminado con honores mi bachiller.

Estudié en el SENA en el año 2004 terminando como auxiliar de enfermería y en el año 2014 obtuve el título de Tecnólogo en ADSI.

Actualmente laboro en el Hospital Nuestra Señora De Lourdes del municipio de Ataco Tolima, vivo con mi esposa, mi hijo, hijastra y mi suegra.

Mis sueños siempre fue convertirme en un profesional y gracias a ello me entere de la UNAD, universidad que tiene horarios flexibles de estudio, me embarque en esta nueva aventura donde logre culminar mis materias en el presente año