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

HAROL HEYDER CORTEZ MARTINEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
INGENIERÍA DE SISTEMAS
INZÁ CAUCA
OCTUBRE DE 2020

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

HAROL HEYDER CORTEZ MARTINEZ

DIPLOMADO DE PROFUNDIZACIÓN EN CISCO CNA

TUTOR:
DIEGO EDINSON RAMIREZ CLAROS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
INGENIERÍA DE SISTEMAS
INZÁ CAUCA
OCTUBRE DE 2020

NOTA DE ACEPTACION

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

AGRADECIMIENTOS

Agradezco primeramente a Dios por haberme guiado y permitirme culminar mis estudios como Ingeniero de Sistemas, es Él quien en este proceso me ha dado la sabiduría suficiente para aprender y enriquecer mis conocimientos, también para sobreponerme a cada uno de los retos que se han presentado a lo largo de este proceso de formación.

A mis padres, esposa e hijo, por siempre estar a mi lado y pendientes para brindándome su apoyo incondicional y sus acertados consejos, es gracias a ese grato acompañamiento que en este momento me veo muy cerca de lograr mi gran sueño.

A mis profesores quienes han tenido el don de la paciencia y acertadas estrategias de transmisión de conocimiento, fueron pieza fundamental en mi formación profesional, gracias infinitas por permitirme hoy estar a punto de terminar mi carrera universitaria.

CONTENIDO

TABLA DE FIGURAS

TABLA DE TABLAS

GLOSARIO

Sevidor Web: Es un programa que utiliza protocolo de transferencia de hipertexto, HTTP para servir los archivos que forman páginas Web a los usuarios en respuesta a sus solicitudes, que son reenviadas por clientes HTTP se sus computadoras.

Servidor DNS: Esta es una tecnología basada, en una base de datos que sirve para resolver nombre en las redes, es decir, para conocer la dirección IP de la máquina, donde está alojado el dominio al que queremos acceder.

Servidor FTP: Es un protocolo de red, utilizado para la transferencia de archivos entre sistemas conectados a una res TCP (Transmission Control Protocol), basado en la arquitectura cliente-servidor

VLAN: acrónico derivado de virtual LAN (red de área local virtual), método que se utiliza para crear una red lógica que sea independiente dentro de la red física, de esta forma se puede afirmar que una VLAN describe una red de área local.

Direccion IP: Es un conjunto de números que identifica, de manera lógica y jerárquica, a una interfaz en la red

Direccion IPv4: Las direcciones IPv4 pueden representarse en cualquier notación que exprese un valor entero de 32 bits

Direccion IPv6: La Dirección de Internet Protocol versión 6 (o dirección IPv6) es una etiqueta numérica usada para identificar una interfaz de red

OSPF: es un protocolo de enrutamiento de fuente abierta (open source), es por eso que puede ser utilizado por equipos de diferentes marcas a cisco, este protocolo se puede configurar para ipv4 con su versión ospfv2 y para ipv6 con su versión ospfv3.

NAT: siglas en ingles Network Address Translator y en español traductor de direcciones de red, como su nombre lo indica es la encargada de traducir las direcciones para que se pueda establecer las conexiones.

RESUMEN

En el siguiente trabajo tiene como principal objetivo poner en práctica sus conocimientos profundizando en el área de redes y comunicaciones, en este se plantean dos escenarios, los cuales se deben armar con su topología respectiva y ademas hacer la configuración de cada uno de los dispositivo, teniendo en cuenta los parámetros dados para su correcto funcionamiento. De esta manera se pone en práctica las capacidades y de manera especial se prepara como profesional, para afrontar las demandas del mercado en especialización de las tecnologías informáticas de las telecomunicaciones. El desarrollo de estas actividades se evidenciara, mediante el uso del software de CISCO herramienta Packet Tracer la cual permitirá evidenciar lo realizado de forma práctica, mediante una simulación.

Palabras clave: Telecomunicaciones, Packet Tracer, simulación, laboratorios.

ABSTRACT

The main objective of the following work is to put into practice their knowledge, deepening in the area of networks and communications, in this two scenarios are proposed, which must be assembled with their respective topology and also make the configuration of each of the devices, taking into account the parameters given for its correct operation. In this way, the skills are put into practice and in a special way they prepare as a professional, to face the demands of the market in specialization of information technology in telecommunications. The development of these activities will be evidenced, through the use of the CISCO software, the Packet Tracer tool, which will allow to demonstrate what has been done in a practical way, through a simulation.

Keywords: Telecommunications, Packet Tracer, simulation, laboratories.

INTRODUCCIÓN

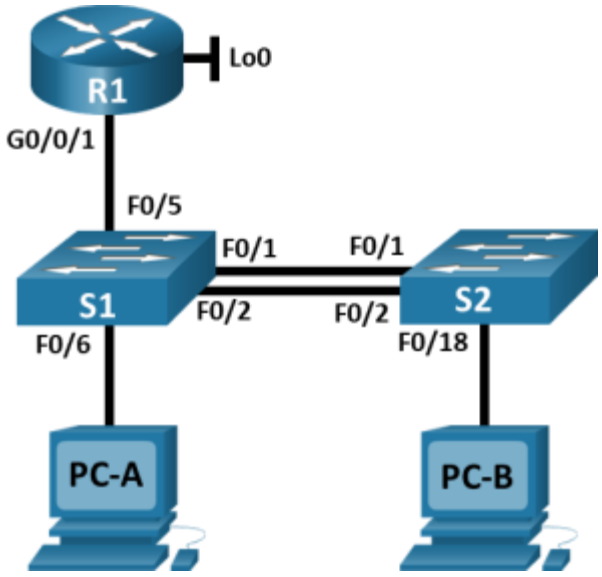
El presente trabajo tiene como fin el desarrollo de prueba de habilidades correspondiente al diplomado en Cisco CCNA, con este se busca identificar y también fortalecer los saberes adquiridos durante la formación académica en el programa de ingeniería de sistemas.

Por medio de esta actividad en la que se implementan dos escenarios, cada uno con sus propios requerimientos, se busca reconocer e identificar las principales funciones y características de los modelos de red y sus componentes usando la herramienta de simulación Cisco Packet Tracer en cualquiera de sus versiones, en este software se desarrollan de manera práctica los ejercicios y de esta manera hacer un aprendizaje acertado y significativo, el cual también permitirá analizar cómo funcionan las redes.

Por último se puede evidenciar que con el desarrollo de esta actividad, fue posible identificar diferentes maneras de configurar los dispositivos que hacen parte de la red, entre ellos routers, switches, servidores, entre otros. Con los cuales podemos acercarnos a la realidad y aterrizarnos de manera correcta a lo que serán nuestras tareas como profesionales una vez culminemos nuestra etapa de aprendizaje.

Escenario 1

Figura No. 1 Topología escenario 1



Fuente: autor

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

Tabla 1 Tabla 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
	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

Parte 1: inicializar y recargar y configurar aspectos básicos de los dispositivos

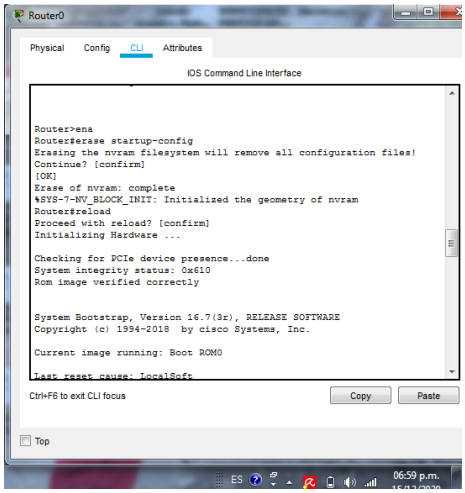
Paso 1: Inicializar y volver a cargar el router y el switch

En el siguiente paso de configuraciones se realiza la actividad que consiste en borrar la configuración que viene por defecto en los equipos con el fin de realizar una configuración de cero, este proceso se hace en los swich y el router, que hacen parte de la red.

Tabla 3 Borrado configuraciones Router

Borrado de configuraciones y volver a cargar el Router	
Tarea	Especificación
Eliminar el archivo startup-config de todos los routers	Router>enable Router#erase startup-config Con los anteriores comandos hacemos el borrado de las configuraciones de inicio del router.
Volver a cargar los routers	Router#reload Con el uso del comando anterior se hace para recargar o reiniciar las configuraciones del router

Figura No. 2 .Borrado configuraciones y reinicio del Router



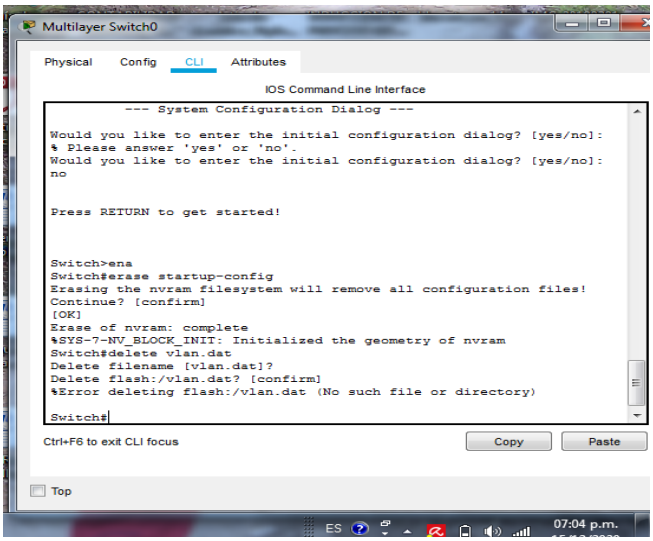
Fuente: autor

Con el uso del comando erase startup-config se realiza el borrado de la base de datos en la memoria flash y reinicio del router con resultado satisfactorio.

Tabla 4 Borrado configuraciones switch y cargue de plantilla SDM

Borrado de configuraciones y volver a cargar los switch	
Tarea	Especificación
Eliminar el archivo startup-config de todos los switch y eliminar la base de datos de VLAN	Switch>enable Switch#erase startup-config Switch#delete vlan.dat Con los anteriores comandos hacemos el borrado de las configuraciones de inicio de los switch y borrado la base de datos de VLAN
Volver a cargar los switch	Router#reload Con el uso del comando anterior se hace para recargar o reiniciar las configuraciones del switch
Configurar la plantilla SDM para que admita IPv6	Switch>enable witch#configure terminal Switch(config)# sdm prefer dual-ipv4-and-ipv6 default Con el uso de estos comandos hacemos la configuración de la plantilla SDM, la cual es utilizada para activar el funcionamiento del direccionamiento IPV4 en conjunto de IPV6. Switch(config)#end Switch# reload Teniendo en cuenta que el comando para habilitar la plantilla SDM solo producirá efecto en la próxima reiniciada del Switch, utilizamos los anteriores comando para hacer su respectivo reinicio.

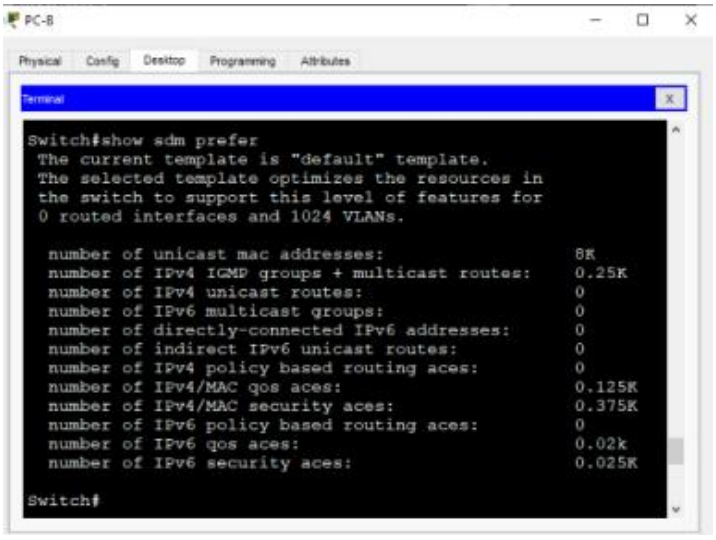
Figura No. 3 borrado de base de datos de VLAN en la memoria flash de S1



Fuente: autor

Con el uso de los comando erase statup-config y delete vlan.dat, se elimina las configuraciones y la base de datos de VLAN del switch. Este mismo proceso se realiza con los demás switch que hacen parte de la red

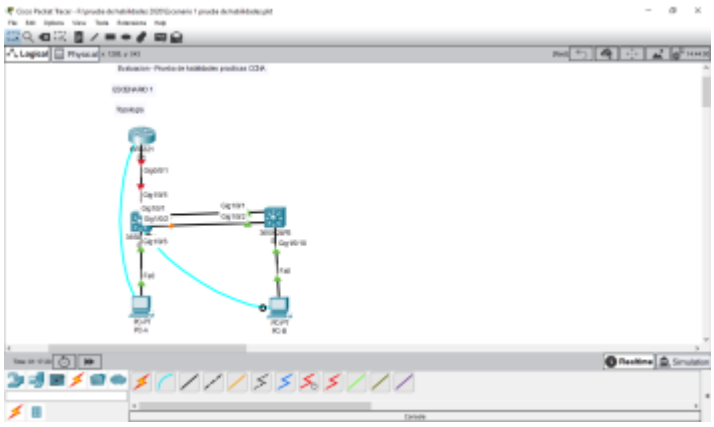
Figura No. 4 Configuración de la plantilla SDM



Fuente: Autor

Se hace la configuración de la plantilla SDM para que admita direcciones IPv6 y se verifican los cambios realizados mediante el comando show sdm pefer. Este mismo proceso se realiza con los demás switch que hacen parte de la red

Figura No. 5 Topología creada en Packet Tracer



Fuente: Autor

La anterior imagen se muestra la topología creada en el software Packet Tracer, utilizado para realizar la simulación necesaria.

Paso 2: Configurar R1

Se hace la configuración de router R1, teniendo en cuenta las especificaciones dadas en la siguiente tabla.

Luego de hacer el reinicio del dispositivo, se inicia por desactivar la búsqueda DNS con el comando necesario, se le asigna el nombre al router (R1), se hace la asignación del dominio ccna-lab.com, se cifra la contraseña para modo EXCEC privilegiado y también se establece la contraseña para ingresa a la consola, se establece la longitud mínima de caracteres, se crea un usuario administrativo en la base de datos local, luego se configura el inicio de sesión en las líneas VTY para que use la base de datos local esta vty, se configura para que solo acepte SSH, se cifran las contraseñas de texto no cifrado, se hace la configuración de un MOTD Banner con su respectivo mensaje de alerta y por último se habilita el routing ipv6.

Tabla 5 Configuración de router R1

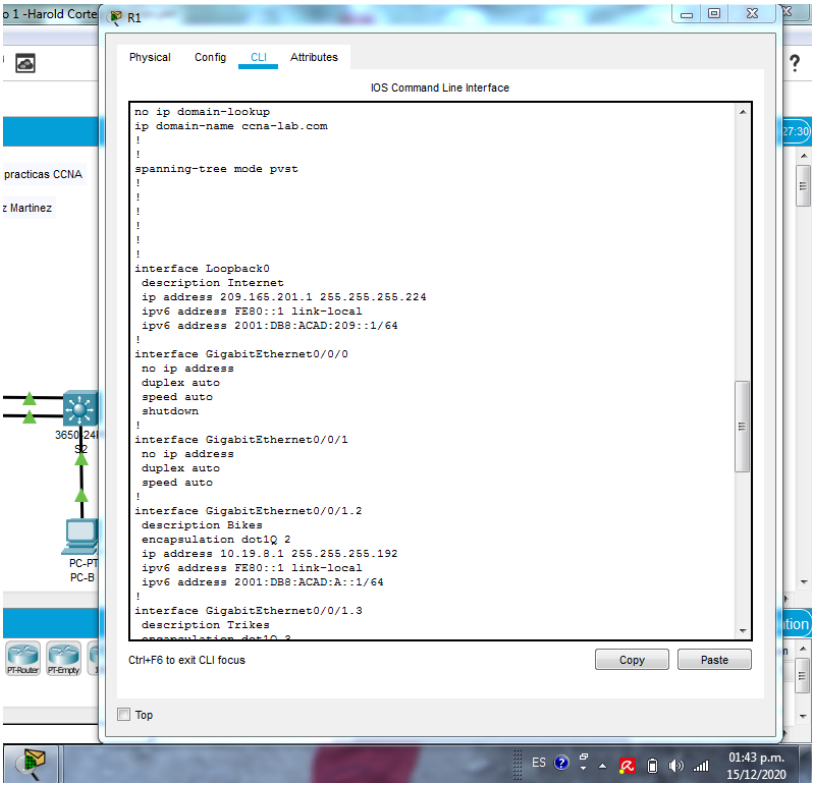
Tarea	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain lookup
Nombre del router	R1 Router(config)#hostname R1 R1(config)#
Nombre de dominio	ccna-lab.com R1(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	Ciscoenpass R1(config)#enable secret ciscoenpass

Contraseña de acceso a la consola	Ciscoconpass R1(config)#line console 0 R1(config-line)#pas R1(config-line)#password ciscoconpass R1(config-line)#login R1(config-line)# R1(config-line)#exit
Establecer la longitud mínima para las contraseñas	10 caracteres 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 secret adminlpass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	R1(config)#line vty 0 15
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 %Unauthorized Access is prohibited!%
Habilitar el routing IPv6	R1(config)#ipv6 unicast-routing
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 g0/0/1.2 R1(config-subif)#encapsulation dot1Q 2 R1(config-subif)#description Bikes R1(config-subif)#ip address 10.19.8.1 255.255.255.192 R1(config-subif)#ipv6 address 2001:db8:acad:a::1/64 R1(config-subif)#ipv6 address fe80::1 link-local R1(config-subif)# R1(config-subif)#int g0/0/1.3

	R1(config-subif)#encapsulation dot1Q 3 R1(config-subif)#description Trikes R1(config-subif)#ip address 10.19.8.65 255.255.255.224 R1(config-subif)#ipv6 address 2001:db8:acad:b::1/64 R1(config-subif)#ipv6 address fe80::1 link-local R1(config-subif)#int g0/0/1.4 R1(config-subif)#encapsulation dot1Q 4 R1(config-subif)#description Management R1(config-subif)#ip address 10.19.8.97 255.255.255.248 R1(config-subif)#ipv6 address 2001:db8:acad:c::1/64 R1(config-subif)#ipv6 address fe80::1 link-local R1(config-subif)# R1(config-if)#int g0/0/1.6 R1(config-subif)# R1(config-subif)#encapsulation dot1Q 6 native R1(config-subif)#description Native R1(config-subif)#int g0/0/1 R1(config-if)#no shutdown R1(config-if)#
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)#int loopback 0 R1(config-if)#ip ad R1(config-if)#ip address 209.165.201.1 255.255.255.224 R1(config-if)#ipv6 address 2001:db8:acad:209::1/64 R1(config-if)#ipv6 address fe80::1 link-local R1(config-if)#description Internet R1(config)#crypto key generate RSA modulus 1024

Generar una clave de cifrado RSA	Módulo de 1024 bits R1(config)#crypto key generate rsa generalkeys modulus 1024

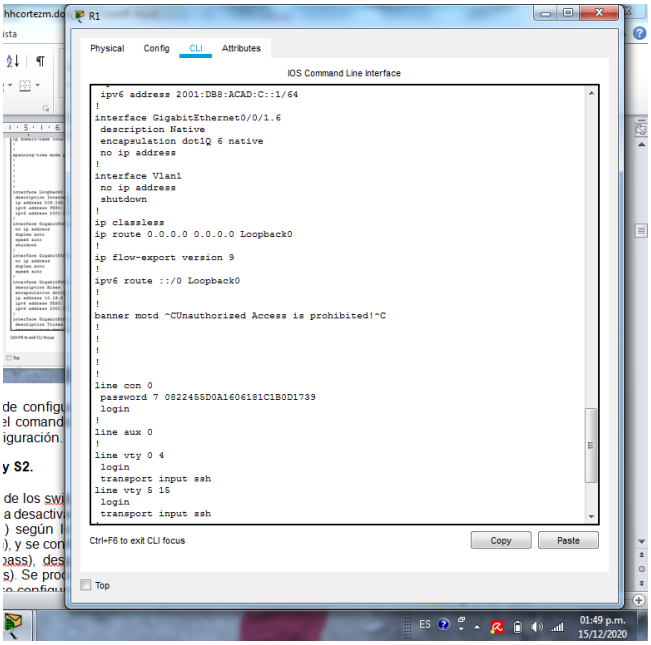
Figura No. 6 Verificación de configuraciones comando show running-config en router R1



Fuente: autor

Se hace verificación de configuración realizada de la interfaces y dominio del Router R1 mediante el comando show running-config obteniendo un resultado satisfactorio de la configuración.

Figura No. 7 Verificación de configuraciones comando show running-config en router R1



Fuente: autor

Se hace la verificación de las configuraciones de contraseñas, cifrado y MOTD Banner del Router R1, con el uso del comando show running-config obteniendo un resultado satisfactorio de la configuración.

Paso 3.Configure S1 y S2.

Para la configuración de los switches, después de haberlo inicializado y cargado nuevamente, se hace la desactivación de la búsqueda DNS, para luego asignar el nombre al switch (S1) según lo solicitado, ademas se asigna un nombre del dominio (ccna-lab.com), y se configura una contraseña cifrada para el modo EXEC privilegiado (Ciscoenpass), despues se asigna la contraseña de acceso a la consola (Ciscoconpass). Se procede a crear un usuario administrativo en la base de datos local, luego se configura el inicio de sesión en las líneas VTY para que use la base de datos local, estas lines vty se configuran para que solo acepte SSH, se cifran las contraseñas de texto, se configura un mensaje MOTD Banner y se genera la clave de cifrado RSA, se configura la interfaz de administración SVI y se realiza la configuración del Gateway predeterminado.

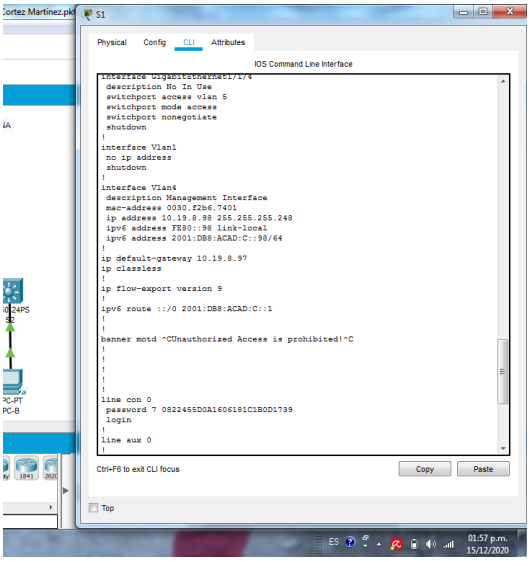
Tabla 6 Configuración de Switch S1 y S2

Tarea	Especificación
Desactivar la búsqueda DNS.	**S1** Switch>enable Switch#config t Switch(config)#no ip domain lookup S2 Switch>enable Switch#configure terminal Switch(config)#no ip domain lookup
Nombre del switch	**S1 o S2, según proceda** Switch(config)#hostname S1 Switch(config)#hostname S2
Nombre de dominio	**ccna-lab.com** S1(config)#ip domain-name ccna-lab.com S2(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	**Ciscoenpass** S1(config)#line console 0 S1(config)#enable secret ciscoenpass S1(config-line)#login S1(config-line)#exit S1(config)# S2(config)#line console 0 S2(config)#enable secret ciscoenpass S2(config-line)#login S2(config-line)#exit S2(config)#
Contraseña de acceso a la consola	**Ciscoconpass** S1(config-line)#password ciscoconpass S2(config-line)#password ciscoconpass
Crear un usuario administrativo en la base de datos local	Nombre de usuario: **admin** Password: **admin1pass** S1(config)#username admin secret admin1pass S2(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 S2(config)#line vty 0 15 S2(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 S2(config-line)#transport input ssh S2(config-line)#exit
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption S2(config)#service password-encryption
Configurar un MOTD Banner	S1(config)#banner motd &Unauthorized Access is prohibited!& S1(config)# S2(config)#banner motd (Unauthorized access is prohibited!(S2(config)#
Generar una clave de cifrado RSA	**Módulo de 1024 bits** S1(config)#crypto key generate rsa generalkeys 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 FE80: :99 para S2** Establecer la dirección IPv6 de capa 3 S1(config)#int vlan 4 S1(config-if)#ip address 10.19.8.98 255.255.255.248 S1(config-if)#ipv6 address 2001:db8:acad:c::98/64 S1(config-if)#ipv6 address fe80::98 link-local S1(config-if)#description Management Interface S1(config-if)#no shutdown S1(config-if)#

	S2(config)#int vlan 4 *mar. 1 1:42:36.414: %SSH-5-ENABLED: SSH 1.99 has been enabled S2(config-if)#ip address 10.19.8.99 255.255.255.248 S2(config-if)#ipv6 address 2001:db8:acad:c::99/64 S2(config-if)#ipv6 address fe80::99 link-local S2(config-if)#description Management interface S2(config-if)#no shutdown S2(config-if)#exit
Configuración del gateway predeterminado	Configure la puerta de enlace predeterminada como 10.19.8.97 para IPv4 S1(config)#ip default-gateway 10.19.8.97 S2(config)#ip default-gateway 10.19.8.97 S2(config)#

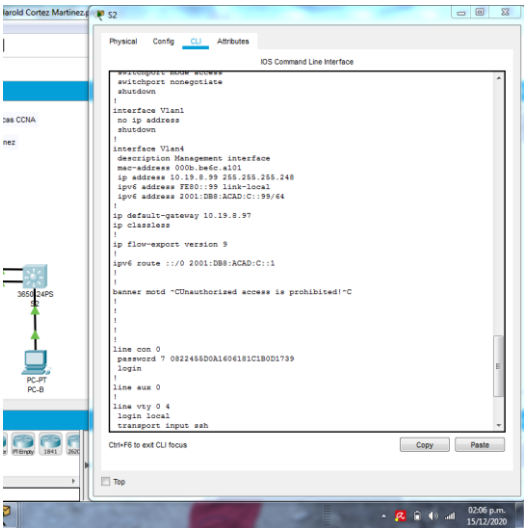
Figura No. 8 Verificación de configuraciones en switch S1



Fuente: autor

Se hace la verificación de las configuración realizadas en el switch S1, de interfaces puerta enlace, contraseñas, cifrado y MOTD Banner, con uso del comando show running-config obteniendo resultado satisfactorio

Figura No. 9 Verificación de configuraciones en switch S2



Fuente: autor

Se hace la verificación de las configuración realizadas en el switch S2, de interfaces puerta enlace, contraseñas, cifrado y MOTD Banner, con uso del comando show running-config obteniendo resultado satisfactorio

PARTE 2: CONFIGURACIÓN DE LA INFRAESTRUCTURA DE RED (VLAN, TRUNKING, ETHERCHANNEL)

Paso 4: Configurar S1

En este paso se crean todas las vlan que se van a usar ya que por defecto el, se configuran los puertos troncales, dentro de la interface del switch se debe confirmar el tipo de encapsulamiento, se crea un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2, se configura el puerto de acceso en donde se conecta el PCA, se configura la seguridad del puerto y para proteger las interfaces se dejan deshabilitadas las que no serán usadas.

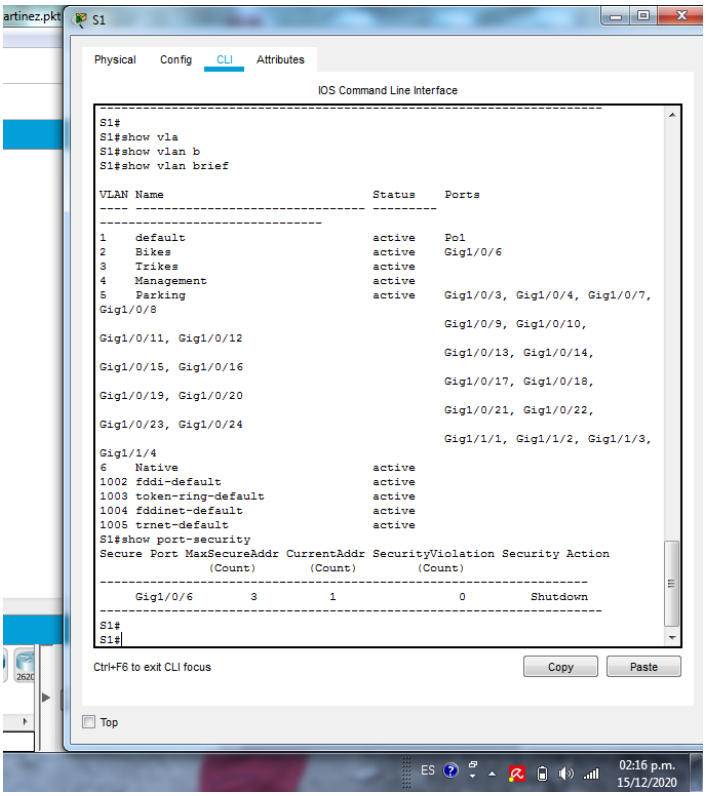
Tabla 7 Tabla de configuración de S1

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)#int vlan 4 S1(config-if)#ip address 10.19.8.98

	255.255.255.248 S1(config-if)#ipv6 address 2001:db8:acad:c::98/64 S1(config-if)#ipv6 address fe80::98 link-local S1(config-if)#description Management Interface S1(config-if)#no shutdown S1(config-if)#ip default-gateway 10.19.8.97 S1(config)# S1(config)#vlan 2 S1(config-vlan)#name Bikes S1(config-vlan)#vlan 3 S1(config-vlan)#name Trikes S1(config-vlan)#vlan 4 S1(config-vlan)#name Management S1(config-vlan)#vlan 5 S1(config-vlan)#name Parking S1(config-vlan)#vlan 6 S1(config-vlan)#name Native S1(config-vlan)#
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	Interfaces F0/1, F0/2 y F0/5 S1(config)#int g1/0/5 S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 6 S1(config-if)#interface range g1/0/1-2 S1(config-if-range)#shutdown S1(config-if-range)#switchport trunk encapsulation dot1q S1(config-if-range)#switchport mode trunk S1(config-if-range)#switchport trunk native vlan 6
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-if-range)#channel group 1 mode active S1(config-if-range)#int port-channel 1 S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 6
Configurar el puerto de acceso de host para VLAN 2	Interface F0/6

	S1(config-if)#int g1/0/6 S1(config-if)#switchport mode acces S1(config-if)#switchport access vlan 2
Configurar la seguridad del puerto en los puertos de acceso	Permitir 3 direcciones MAC S1(config-if)#switchport port-security 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-if)#int range g1/0/3-4 S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 5 S1(config-if-range)#description Not In Use S1(config-if-range)#shutdown S1(config)#int range g1/0/7-24 S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 5 S1(config-if-range)#description Not In Use S1(config-if-range)#shutdown S1(config-if-range)#int range g1/1/1-4 S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 5 S1(config-if-range)#description No In Use S1(config-if-range)#shutdown

Figura No. 10 Verificación de configuración de switch S1



Fuente: autor

Se hace verificación de la configuración de las VLAN en el Swicht 1, también se verifica la configuración de la seguridad del puerto, en los puertos de acceso para permitir 3 direcciones MAC, observando su creación de forma correcta, cumpliendo los parámetros solicitados. Los comandos utilizados para esta fueron show vlan brief y show port-security respectivamente

Paso 5: Configure el S2.

En este paso se crean todas las vlan que se van a usar ya que por defecto el, se configuran los puertos troncales, dentro de la interface del switch se debe confirmar el tipo de encapsulamiento, se crea un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2, se configura el puerto de acceso en donde se conecta el PCA, se configura la seguridad del puerto y para proteger las interfaces se dejan deshabilitadas las que no serán usadas.

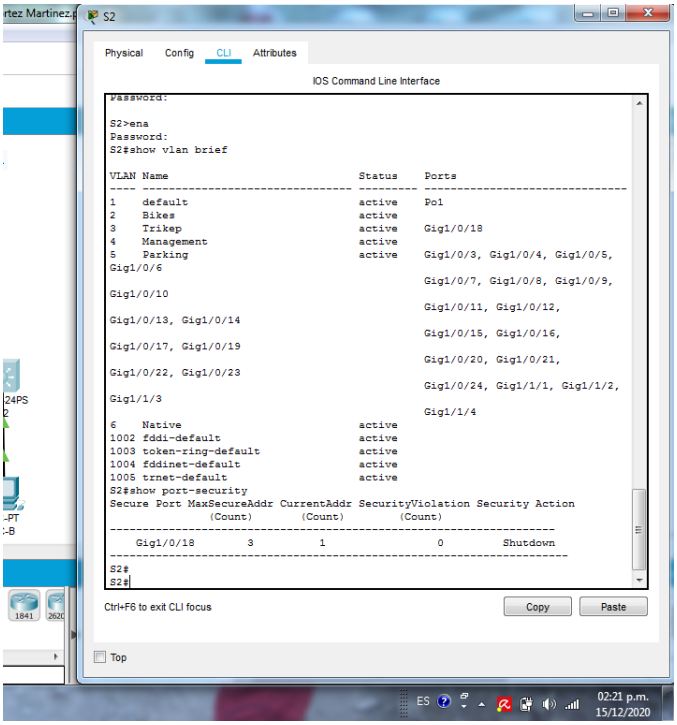
Tabla 8 Tabla de configuración de switch S2

Tarea	Especificación
Crear VLAN	VLAN 2, name Bikes VLAN 3, name Trikes VLAN 4, name Management VLAN 5, nombre Parking VLAN 6, nombre Native S2(config)#vlan 2 S2(config-vlan)#name Bikes S2(config-vlan)#vlan 3 S2(config-vlan)#name Trikep S2(config-vlan)#vlan 4 S2(config-vlan)#name Management S2(config-vlan)#vlan 5 S2(config-vlan)#name Parking S2(config-vlan)#vlan 6 S2(config-vlan)#name Native S2(config-vlan)#exit S2(config)#
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	Interfaces F0/1 y F0/2 S2(config)#int range g1/0/1-2 S2(config-if-range)#shutdown S2(config-if-range)#switchport trunk encapsulation dot1q S2(config-if-range)#switchport mode trunk S2(config-if-range)#switchport trunk native vlan 6 S2(config-vlan)#exit S2(config)#int range g1/0/1-2 S2(config-if-range)#shutdown S2(config-if-range)#switchport trunk encapsulation dot1q

	S2(config-if-range)#switchport mode trunk S2(config-if-range)#switchport trunk native vlan 6
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-if-range)#channel group 1 mode active S2(config-if-range)#int port-channel 1
Configurar el puerto de acceso del host para la VLAN 3	Interfaz F0/18 S2(config-if)#int g1/0/18 S2(config-if)#switchport mode access S2(config-if)#switchport access vlan 3 S2(config-if)#
Configure port-security en los access ports	permite 3 MAC addresses S2(config-if)#switchport port-security S2(config-if)#switchport port-security maximum 3
Asegure todas las interfaces no utilizadas.	Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar S2(config-if)#int range g1/0/3-17 S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 5 S2(config-if-range)#description Not In Use S2(config-if-range)#shutdown S2(config-if-range)#int range g1/0/19-24 S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 5 S2(config-if-range)#description Not in Use S2(config-if-range)#Shutdown S2(config-if-range)#int range g1/1/1-4 S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 5 S2(config-if-range)#description Not In Use S2(config-if-range)#shutdown S2(config-if-range)#int range g1/0/1-2 S2(config-if-range)#no shutdown

	S1(config)#int range g1/0/1-2 S1(config-if-range)#no shutdown

Figura No. 11 Verificación de configuración de switch S2



Fuente: autor

Se hace verificación de la configuración de las VLAN en el Swicht 2, también se verifica la configuración de la seguridad del puerto, en los puertos de acceso para permitir 3 direcciones MAC, observando su creación de forma correcta, cumpliendo los parámetros solicitados. Los comandos utilizados para esta fueron show vlan brief y show port-security respectivamente

Parte 2: Configurar soporte de host

Paso 1: Configure R1

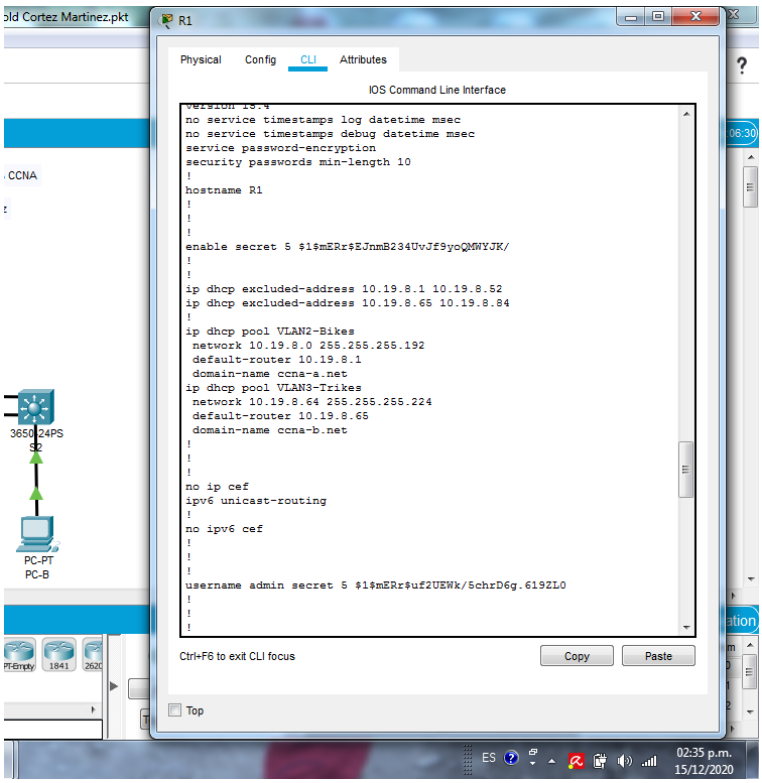
En el router R1 primero se configura el Default routing o rutas predeterminadas para direccionamiento IPv4 e IPv6, luego se configura IPv4 DHCP para VLAN 2 y también para VLAN 3

Tabla 9 Tabla de configuraciones 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 loopback 0 R1(config)#ipv6 route ::/0 loopback 0
Configurar IPv4 DHCP para VLAN 2	Cree un grupo DHCP para VLAN 2, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio ccna-a.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada 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
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(dhcp-config)#exit

Figura No. 12 Verificación de configuración IPv4 DHCP para VLAN 2 y VLAN 3



Fuente: autor

Se verifica la Configuración Default Routing, IPv4 DHCP para VLAN 2 y la configuración de DHCP IPv4 para VLAN 3 en la configuración general de R1 obteniendo resultado satisfactorio.

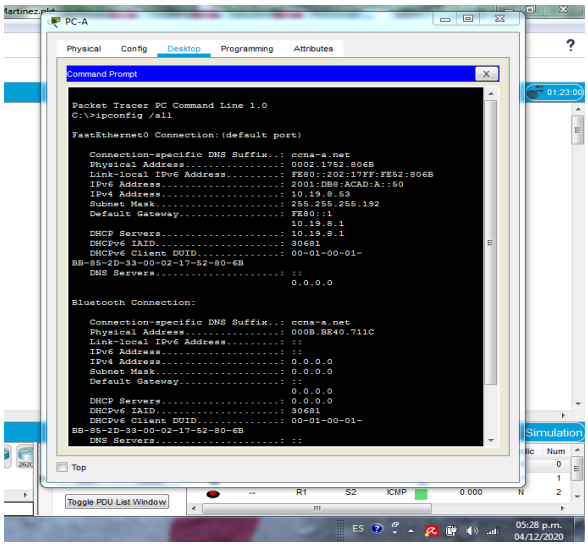
Paso 2: Configurar los servidores

Se configuran los equipos PC-A y PC-B para que utilicen DHCP para IPv4 y se asigna estáticamente las direcciones IPv6 GUA y Link Local. Luego se procede a registrar las configuraciones de red del host con el comando **ipconfig /all**.

Tabla 10 Configuración PC-A

PC-A Network Configuration	
Descripción	DHCP resquest successful
Dirección física	en 10.19.8.1
Dirección IP	10.19.8.53
Máscara de subred	255.255.255.192
Gateway predeterminado	10.19.8.1
Gateway predeterminado IPv6	FE80::1

Figura No. 13 Comando ipconfig /all en PC-A



Fuente: Autor

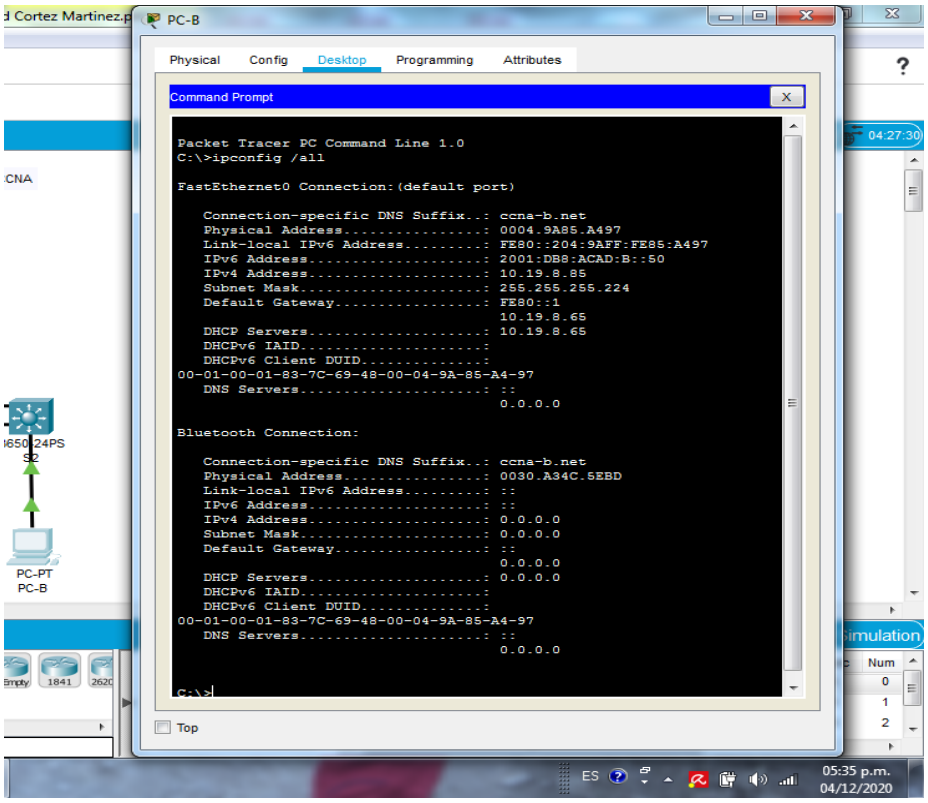
Se realiza la respectiva configuración del direccionamiento de red de PC-A usando las direcciones propuestas de acuerdo a Datos tomados por DHCP mostrados, teniendo un resultado exitoso en su configuración.

Tabla 11 Tabla 12 Configuración PC-B

PC-B Network Configuration	
Descripción	Connection-specific DNS Suffix
Dirección física	10.19.8.1
Dirección IP	10.19.8.85
Máscara de subred	255.255.255.224

Gateway predeterminado	10.19.8.65
Gateway predeterminado IPv6	FE80::1

Figura No. 14 Comando ipconfig /all en PC-B



Fuente: Autor

Se realiza la respectiva configuración del direccionamiento de red de PC-A usando las direcciones propuestas de acuerdo a Datos tomados por DHCP mostrados, teniendo un resultado exitoso en su configuración.

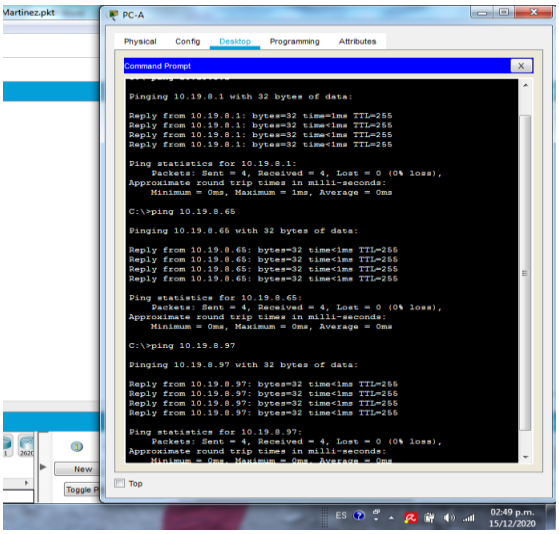
Parte 3: Probar y verificar la conectividad de extremo a extremo

Con el uso del comando ping se procede a verificar conectividad IPv4 e IPv6 entre los diferentes dispositivos de la red.

Tabla 13 Tabla de verificación de conectividad

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

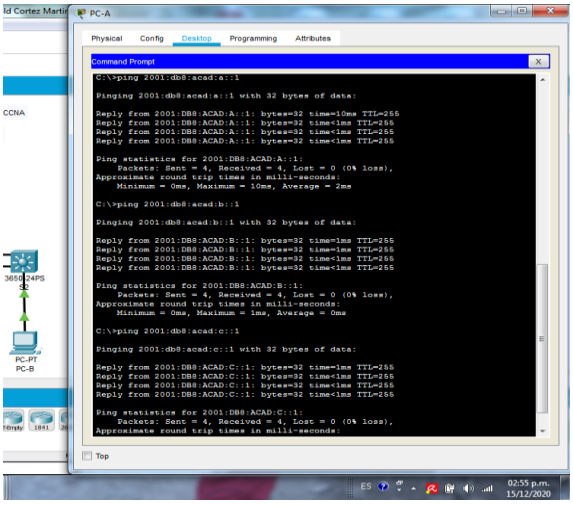
Figura No. 15 Prueba de conectividad



Fuente: autor

Se hace la respectiva verificación de conectividad desde PC-A a diferente puntos de la red, entre ellos: R1, G0/0/1.2, R1, G0/0/1.3 y R1, G0/0/1.4, en IPv4 obteniendo resultado satisfactorio.

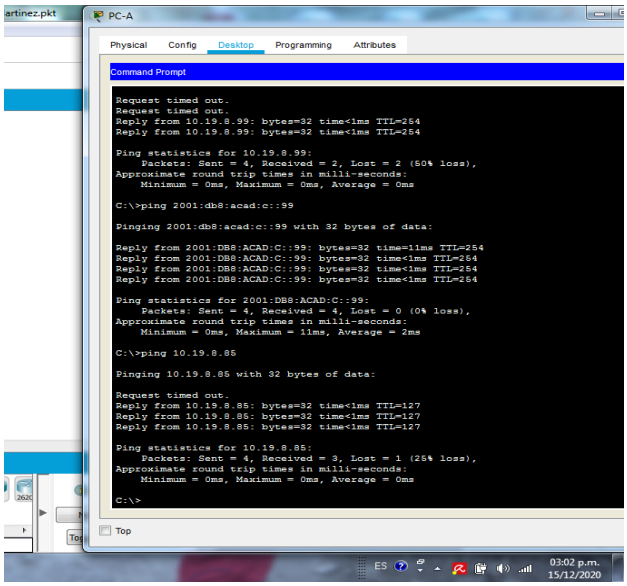
Figura No. 16 Prueba de conectivvidad



Fuente: autor

Se hace la respectiva verificación de conectividad desde PC-A a diferente puntos de la red, entre ellos: R1, G0/0/1.2, R1, G0/0/1.3 y R1, G0/0/1.4, en IPv6 obteniendo resultado satisfactorio.

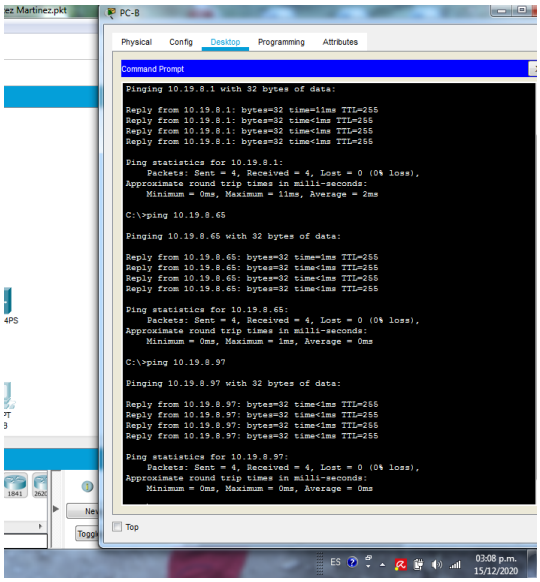
Figura No. 17 Verificación de conectividad



Fuente: autor

Se hace la respectiva verificación de conectividad desde PC-A a diferentes puntos de la red, entre ellos: S2, VLAN 4 en IPv4 e IPv6, y a PC-B en IPv4 obteniendo resultado satisfactorio.

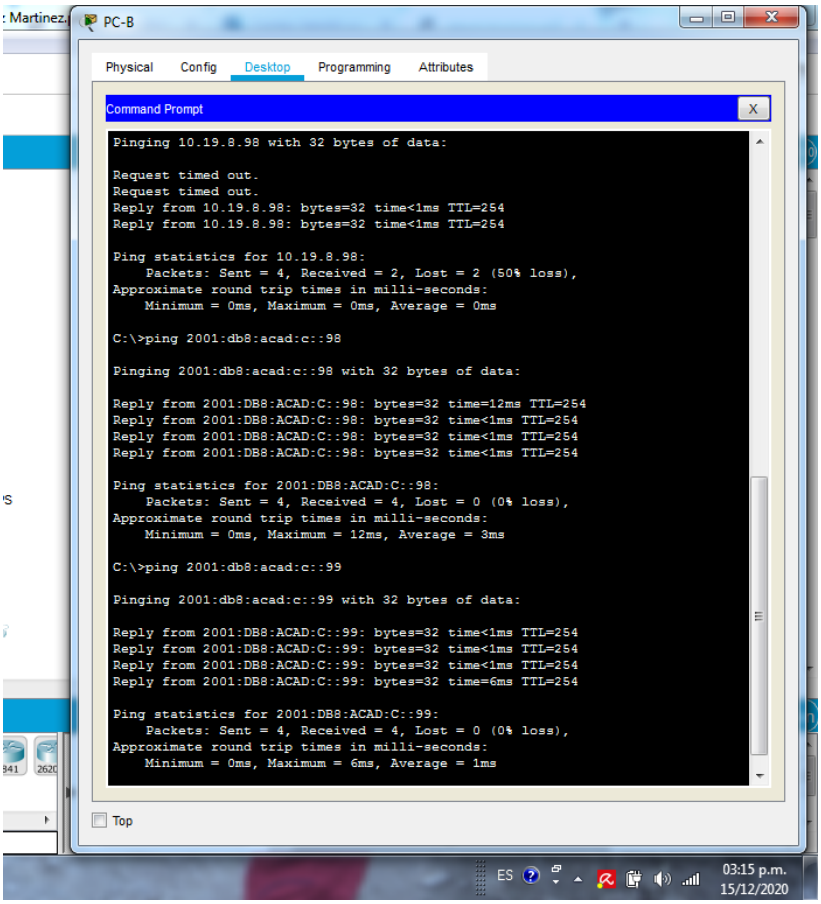
Figura No. 18 Verificación de conectividad



Fuente: autor

Se hace la respectiva verificación de conectividad desde PC-B a diferente puntos de la red, entre ellos: R1, G0/0/1.2, R1, G0/0/1.3 y R1, G0/0/1.4, en IPv4 obteniendo resultado satisfactorio.

Figura No. 19 Prueba de conectividad



Fuente: autor

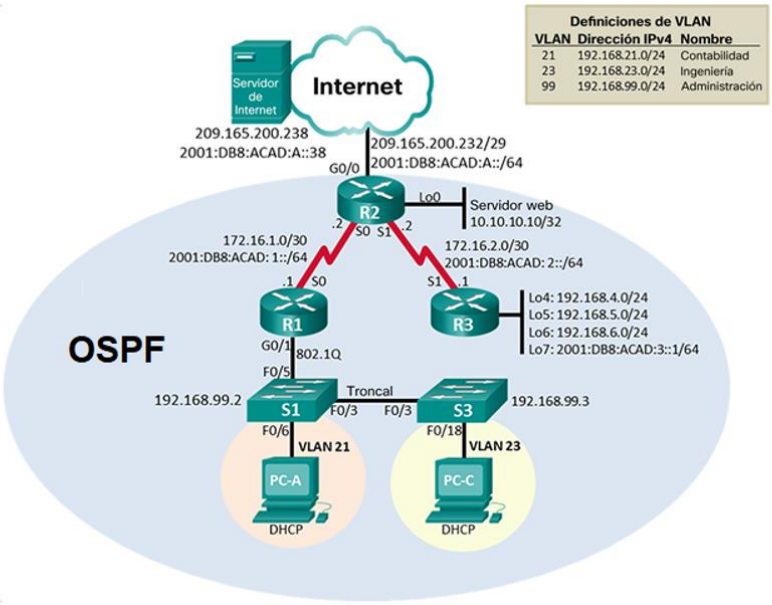
Se hace la respectiva verificación de conectividad desde PC-B a diferentes puntos de la red, entre ellos: S1, VLAN 4 en IPv4 e IPv6, también hacia S2, VLAN 4 en IPv6 obteniendo resultado satisfactorio.

ESCENARIO 2

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

Desarrollo

Figura No. 20 Topología escenario 2



Fuente: autor

Parte 1: inicializar dispositivos

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

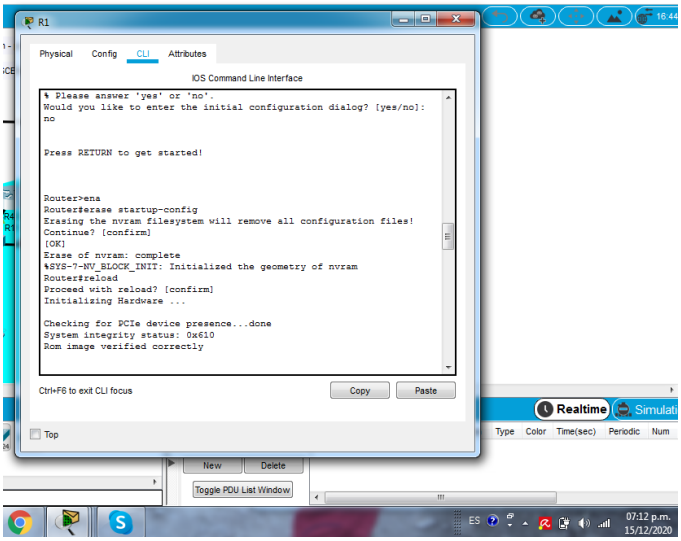
Elimine las configuraciones de inicio y vuelva a cargar los dispositivos.

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

Tabla 14 Eliminar las configuraciones de router y switch y volver cargar

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	Router>enable Router#erase startup-config Router# Con el uso del comando anterior se procede a borrar las configuraciones de inicio del Router
Volver a cargar todos los routers	Router#reload Con el uso del comando anterior procede a cargar las configuraciones del Router
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Switch>enable Switch#delete vlan.dat Switch#erase startup-config Switch# Con el anterior comando se elimina la base de datos de Vlan anteriores
Volver a cargar ambos switches	Switch#reload Con el anterior comando Se carga la configuración Switch
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Switch#show flash Con el comando anterior se verifica que la base de datos de VLAN no esté en la memoria flash de los Switch

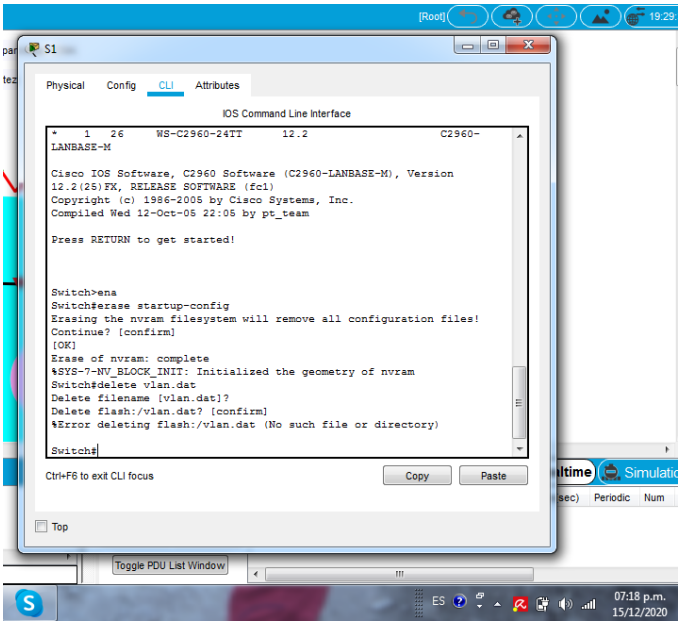
Figura No. 21 Borrado de configuraciones y reinicio del router



Fuente: autor

Con el uso del comando erase startup-config se realiza el borrado de la base de datos en la memoria flash y reinicio del router con resultado satisfactorio. Este mismo proceso se realiza con los demás router que hacen parte de la red

Figura No. 22 borrado de base de datos de VLAN en la memoria flash de switch



Fuente: autor

Con el uso de los comando erase statup-config y delete vlan.dat, se elimina las configuraciones y la base de datos de VLAN del switch. Este mismo proceso se realiza con los demás switch que hacen parte de la red

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):

Tabla 15 Configuraciones del servidor de Internet

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

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

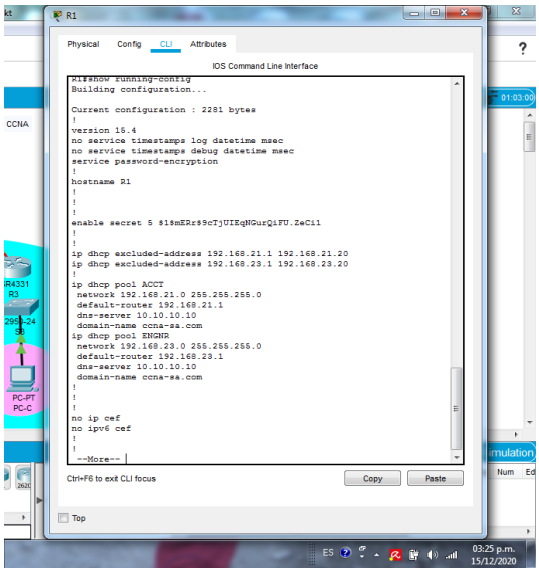
Tabla 16 configuración en el router R1

Elemento o tarea de configuración	Comandos utilizados
Desactivar la búsqueda DNS	Router>ena Router#config t Router(config)#no ip domain-lookup Para hacer uso de comando no ip domain-lookup se debe ingresa a modo privilegiado, luego se ingresa a modo de configuración y se ejecuta. Con el uso del comando desactiva la traducción de nombres a dirección del dispositivo.

Nombre del router	Router(config)#hostname R1 R1(config)# Para establecer esta configuración, se ingresa al modo de configuración se coloca el comando respectivo con el nombre que se le va a asignar al dispositivo y se ejecuta, esto permitirá identificar y diferenciar los diferentes dispositivos de la red.
Contraseña de exec privilegiado cifrada	R1(config)#enable secret class Para el uso de este comando se ingresa al modo de configuración y se lo ejecuta. Esto con el fin de permitir asignar la contraseña para el modo EXEC privilegiado y proporcionar mayor seguridad a la contraseña de enable.
Contraseña de acceso a la consola	R1(config)#line console 0 R1(config-line)#password cisco R1(config-line)#login R1(config-line)# Con este comando se utiliza para asignar contraseña de acceso a la consola, y restringir el acceso de cualquier persona no autorizada.
Contraseña de acceso Telnet	R1(config-line)#line vty 0 15 R1(config-line)#password cisco R1(config-line)#login Con este comando se asigna la contraseña de acceso Telnet, con este se habilita el acceso por las líneas vty, estas permiten acceder a un dispositivo a través de telnet o ssh.
Cifrar las contraseñas de texto no cifrado	R1(config-line)#service password-encryption R1(config)# Con este comando se aplica un cifrado básico a las contraseñas que se encuentren sin cifrar.

Mensaje MOTD	R1(config)#banner motd %Acceso no autorizado% R1(config)# Esta configuración se realiza para emitir notificaciones o mensajes de advertencias para el que se conecte al dispositivo, la configuración del Banner MOTD permite prohibir el acceso no autorizado.
Interfaz S0/0/0	R1(config)#interface serial 0/0/0 R1(config-if)#description conexion con R2 R1(config-if)#ip address 172.16.1.1 255.255.255.252 R1(config-if)#no shut %LINK-5-CHANGED: Interface Serial0/1/0, changed state to down R1(config-if)#ipv6 address 2001:DB8:ACAD:1::/64 R1(config-if)#clock rate 128000 R1(config-if)#no shut R1(config-if)# Con los comandos anteriores se configura la interface serial 0/0/0 asignándole una descripción, ademas se configura el direccionamiento IPv4 e IPv6, también el clock rate por ser una conexión serial DCE.
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 R1(config)# En esta se configura las rutas predeterminadas de ipv4 e ipv6

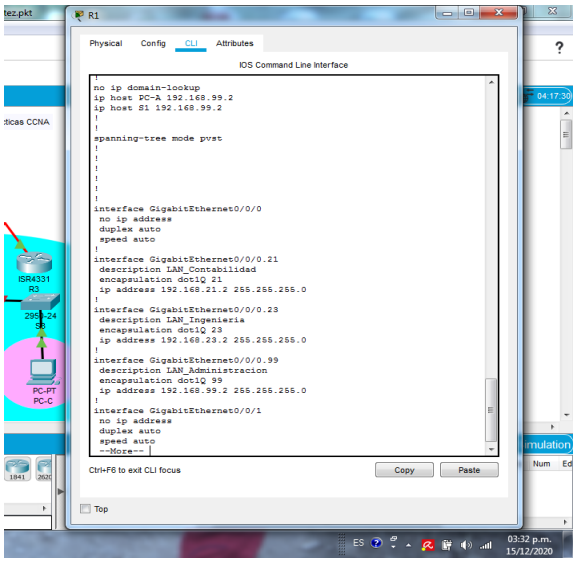
Figura No. 23 configuraciones en router R1



Fuente: autor

Se hace la verificación de la configuración realizada de cambio de nombre, direccionamiento IPv4 e IPv6, así como también la creación de interfaces, los diferentes tipos de contraseñas, obteniendo resultado satisfactorio

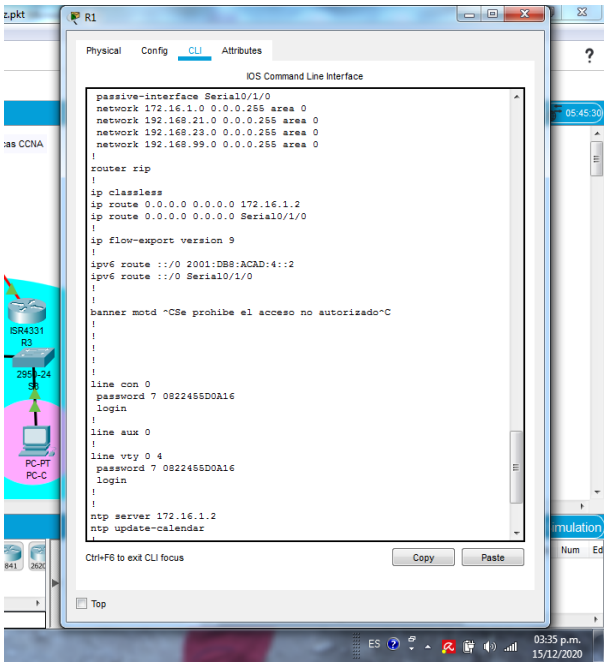
Figura No. 24 configuraciones en router R1



Fuente: autor

Se hace la verificación de la configuración realizada de cambio de nombre, direccionamiento IPv4 e IPv6, así como también la creación de interfaces, los diferentes tipos de contraseñas, obteniendo resultado satisfactorio

Figura No. 25 configuraciones en router R1



Fuente: autor

Se hace la verificación de la configuración realizada de cambio de nombre, direccionamiento IPv4 e IPv6, así como también la creación de interfaces, los diferentes tipos de contraseñas, obteniendo resultado satisfactorio

Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Tabla 17 configuración en el router R2

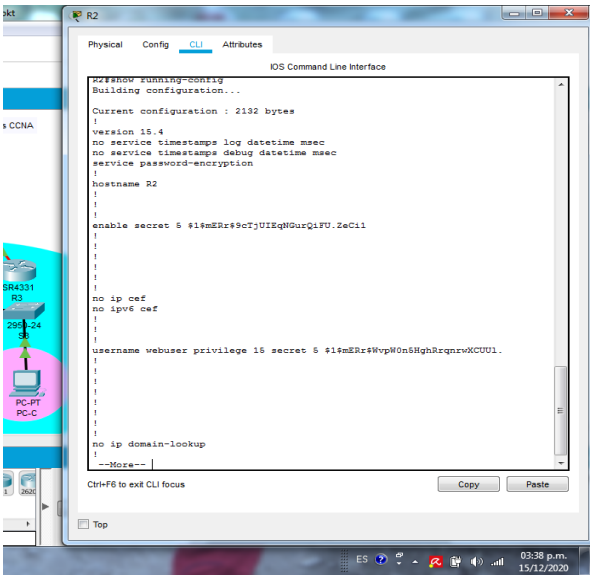
Elemento o tarea de configuración	Comandos utilizados
Desactivar la búsqueda DNS	Router>ena Router#config t Router(config)#no ip domain-lookup Para hacer uso de comando no ip domain-lookup se debe ingresa a modo privilegiado, luego se ingresa a modo de configuración y se ejecuta. Con el uso del comando desactiva la traducción de nombres a dirección del dispositivo.

Nombre del router	Router(config)#hostname R2 R2(config)# Para establecer esta configuración, se ingresa al modo de configuración se coloca el comando respectivo con el nombre que se le va a asignar al dispositivo y se ejecuta, esto permitirá identificar y diferenciar los diferentes dispositivos de la red.
Contraseña de exec privilegiado cifrada	R2(config)#enable secret class R2(config)# Para el uso de este comando se ingresa al modo de configuración y se lo ejecuta. Esto con el fin de permitir asignar la contraseña para el modo EXEC privilegiado y proporcionar mayor seguridad a la contraseña de enable.
Contraseña de acceso a la consola	R2(config)#line console 0 R2(config-line)#password cisco R2(config-line)#login R2(config-line)# Con este comando se utiliza para asignar contraseña de acceso a la consola, y restringir el acceso de cualquier persona no autorizada.
Contraseña de acceso Telnet	R2(config)#line vty 0 15 R2(config-line)#password cisco R2(config-line)#login R2(config-line)# Con este comando se asigna la contraseña de acceso Telnet, con este se habilita el acceso por las líneas vty, estas permiten acceder a un dispositivo a través de telnet o ssh.
Cifrar las contraseñas de texto no cifrado	R2(config)#service password-encryption Con este comando se aplica un cifrado básico a las contraseñas que se encuentren sin cifrar.

Habilitar el servidor HTTP	R2(config)#ip http server Se hace ingreso al modo de configuración y se ejecuta el comando para habilita el servidor de HTTP.
Mensaje MOTD	R2(config)#banner motd %Acceso no autorizado.% Esta configuración se realiza para emitir notificaciones o mensajes de advertencias para el que se conecte al dispositivo, la configuración del Banner MOTD permite prohibir el acceso no autorizado.
Interfaz S0/0/0	R2(config)#interface serial 0/0/0 R2(config-if)#description conexion con R1 R2(config-if)#ip address 172.16.1.2 255.255.255.252 R2(config-if)#no shut R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64 R2(config-if)#no shut R2(config-if)# Con los comandos anteriores se configura la interface serial 0/0/0 asignándole una descripción, ademas se configura el direccionamiento IPv4 e IPv6, ademas se habilita la interfaz con el uso del comando no shutdown
Interfaz S0/0/1	R2(config)#interface serial 0/0/1 R2(config-if)#description conexion con R3 R2(config-if)#ip address 172.16.1.2 255.255.255.252 R2(config-if)#no shut R2(config-if)#ipv6 address 2001:DB8:ACAD:2::2/64 R2(config-if)#clock rate 128000 R2(config-if)#no shut Con los comandos anteriores se configura la interface serial 0/1/1 asignándole una descripción, ademas se configura el direccionamiento IPv4 e IPv6, , también el clock rate por ser una conexión serial DCE y se habilita la interfaz con el uso del comando no shutdown

Interfaz G0/0 (simulación de Internet)	R2(config)#interface g0/0 R2(config-if)#description conexion a internet R2(config-if)#ip address 209.165.200.233 255.255.255.248 R2(config-if)#no shut R2(config-if)#Ipv6 address 2001:DB8:ACAD:A::11/64 R2(config-if)#no shut Con los comandos anteriores se configura la interface serial 0/0/0 asignándole una descripción, ademas se configura el direccionamiento IPv4 e IPv6, ademas se habilita la interfaz con el uso del comando no shutdown
Interfaz loopback 0 (servidor web simulado)	R2(config)#interface loopback 0 R2(config-if)#ip address 10.10.10.10 255.255.255.255 R2(config-if)#description simulacion de servidor web R2(config-if)#no shut Con los comandos anteriores se configura la loopback 0, asignándole una descripción, ademas se configura el direccionamiento IPv4, esta interfaz se utiliza como simulación y no tiene asociado un puerto físico
Ruta predeterminada	R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0 R2(config)#ipv6 route ::/0 g0/0 R2(config)# Se configuran las rutas predeterminadas de ipv4 e ipv6 con el fin de que se direccionen todos lo paquetes que no estén en la tabla de enrutamiento de la interfaz g0/0

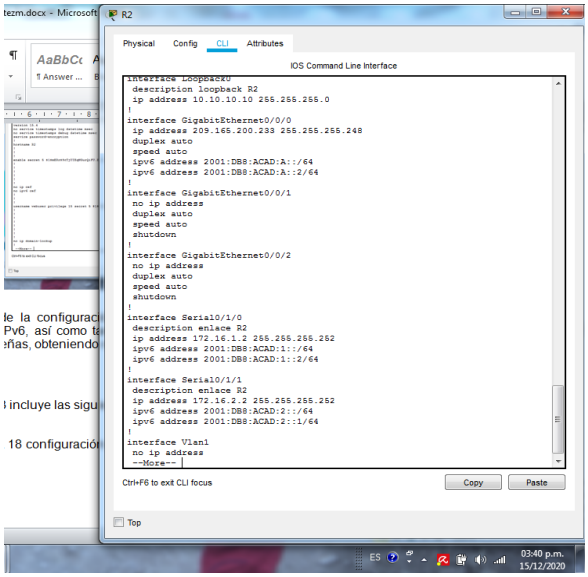
Figura No. 26 configuraciones en router R2



Fuente: autor

Se hace la verificación de la configuración realizada de cambio de nombre, direccionamiento IPv4 e IPv6, así como también la creación de interfaces, los diferentes tipos de contraseñas, obteniendo resultado satisfactorio

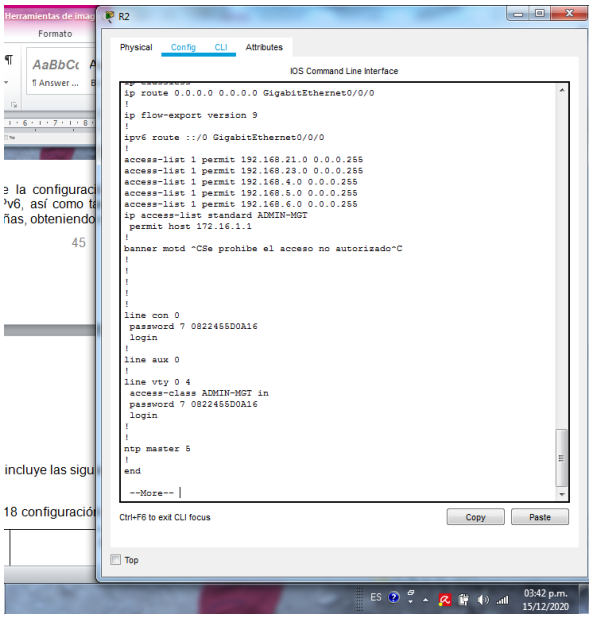
Figura No. 27 configuraciones en router R2



Fuente: autor

Se hace la verificación de la configuración realizada de cambio de nombre, direccionamiento IPv4 e IPv6, así como también la creación de interfaces, los diferentes tipos de contraseñas, obteniendo resultado satisfactorio

Figura No. 28 configuraciones en router R2



Fuente: autor

Se hace la verificación de la configuración realizada de cambio de nombre, direccionamiento IPv4 e IPv6, así como también la creación de interfaces, los diferentes tipos de contraseñas, obteniendo resultado satisfactorio

Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Tabla 18 configuración en el router R3

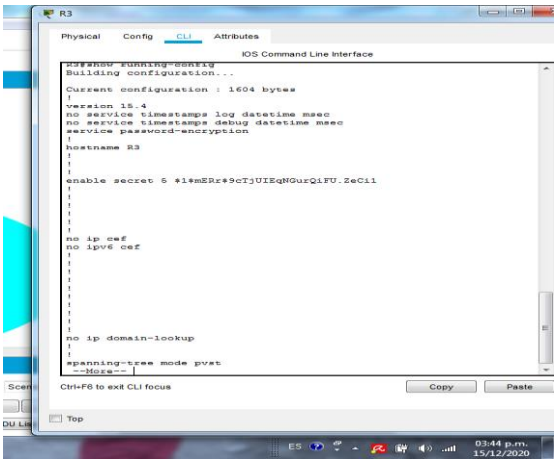
Elemento o tarea de configuración	**Comandos utilizados**
Desactivar la búsqueda DNS	Router>ena Router#conf t Router(config)#no ip domain-lookup Router(config)# Para hacer uso de comando no ip domain-lookup se debe ingresa a modo privilegiado, luego se ingresa a modo de configuración y se ejecuta. Con el uso del comando desactiva la traducción de nombres a dirección del dispositivo.

Nombre del router	Router(config)#hostname R3 R3(config)# Para establecer esta configuración, se ingresa al modo de configuración se coloca el comando respectivo con el nombre que se le va a asignar al dispositivo y se ejecuta, esto permitirá identificar y diferenciar los diferentes dispositivos de la red.
Contraseña de exec privilegiado cifrada	R3(config)#enable secret class R3(config)# Para el uso de este comando se ingresa al modo de configuración y se lo ejecuta. Esto con el fin de permitir asignar la contraseña para el modo EXEC privilegiado y proporcionar mayor seguridad a la contraseña de enable.
Contraseña de acceso a la consola	R3(config)#line console 0 R3(config-line)#password cisco R3(config-line)#login R3(config-line)# Con este comando se utiliza para asignar contraseña de acceso a la consola, y restringir el acceso de cualquier persona no autorizada.
Contraseña de acceso Telnet	R3(config)#line vty 0 15 R3(config-line)#password cisco R3(config-line)#login R3(config-line)# Con este comando se asigna la contraseña de acceso Telnet, con este se habilita el acceso por las líneas vty, estas permiten acceder a un dispositivo a través de telnet o ssh.
Cifrar las contraseñas de texto no cifrado	R3(config)#service password-encryption R3(config)# Con este comando se aplica un cifrado básico a las contraseñas que se encuentren sin cifrar.

Mensaje MOTD	R3(config)#banner motd %Acceso no autorizado.% Esta configuración se realiza para emitir notificaciones o mensajes de advertencias para el que se conecte al dispositivo, la configuración del Banner MOTD permite prohibir el acceso no autorizado.
Interfaz S0/0/1	R3(config)#interface serial 0/0/1 R3(config-if)#description conexion con 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 shut Con los comandos anteriores se configura la interface serial 0/1/1 asignándole una descripción, ademas se configura el direccionamiento IPv4 e IPv6, se habilita la interfaz con el uso del comando **no shutdown**
Interfaz loopback 4	R3(config)#interface loopback 4 R3(config-if)#ip address 192.168.4.1 255.255.255.0 Con los comandos anteriores se configura la loopback 4, asignándole una descripción, ademas se configura el direccionamiento IPv4, esta interfaz se utiliza como simulación y no tiene asociado un puerto físico
Interfaz loopback 5	R3(config)#interface loopback 5 R3(config-if)#ip address 192.168.5.1 255.255.255.0 R3(config-if)# Con los comandos anteriores se configura la loopback 5, asignándole una descripción, ademas se configura el direccionamiento IPv4, esta interfaz se utiliza como simulación y no tiene asociado un puerto físico

Interfaz loopback 6	R3(config)#interface loopback 6 R3(config-if)#ip address 192.168.6.1 255.255.255.0 R3(config-if)# Con los comandos anteriores se configura la loopback 6, asignándole una descripción, ademas se configura el direccionamiento IPv4, esta interfaz se utiliza como simulación y no tiene asociado un puerto físico
Interfaz loopback 7	R3(config)#interface loopback 7 R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64 R3(config-if)# Con los comandos anteriores se configura la loopback 7, asignándole una descripción, ademas se configura el direccionamiento IPv4, esta interfaz se utiliza como simulación y no tiene asociado un puerto físico
Rutas predeterminadas	R3(config)#ip route 0.0.0.0 0.0.0.0 serial 0/0/1 R3(config)#ipv6 route ::/0 serial 0/0/1 R3(config)# Se configuran las rutas predeterminadas de ipv4 e ipv6 con el fin de que se direccionen todos los paquetes que no estén en la tabla de enrutamiento de la interfaz g0/0

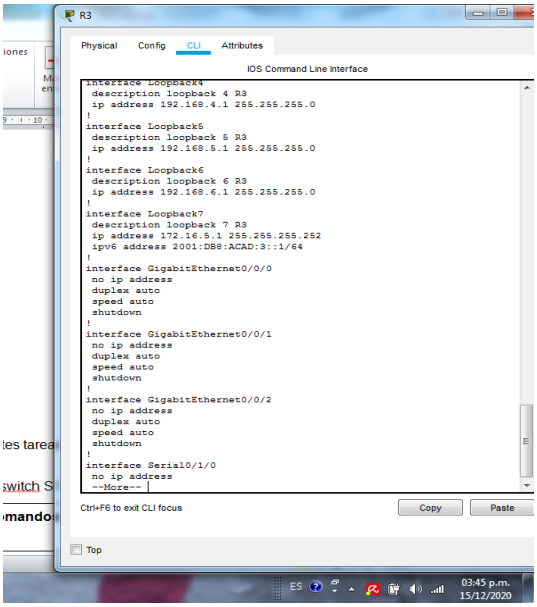
Figura No. 29 configuraciones en router R3



Fuente: autor

Se hace la verificación de la configuración realizada de cambio de nombre, direccionamiento IPv4 e IPv6, así como también la creación de interfaces, los diferentes tipos de contraseñas, obteniendo resultado satisfactorio

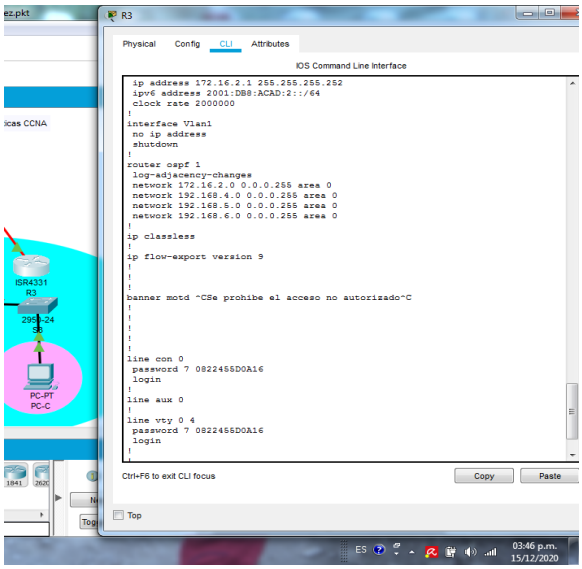
Figura No. 30 configuraciones en router R3



Fuente: autor

Se hace la verificación de la configuración realizada de cambio de nombre, direccionamiento IPv4 e IPv6, así como también la creación de interfaces, los diferentes tipos de contraseñas, obteniendo resultado satisfactorio

Figura No. 31 configuraciones en router R3



Fuente: autor

Se hace la verificación de la configuración realizada de cambio de nombre, direccionamiento IPv4 e IPv6, así como también la creación de interfaces, los diferentes tipos de contraseñas, obteniendo resultado satisfactorio

Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

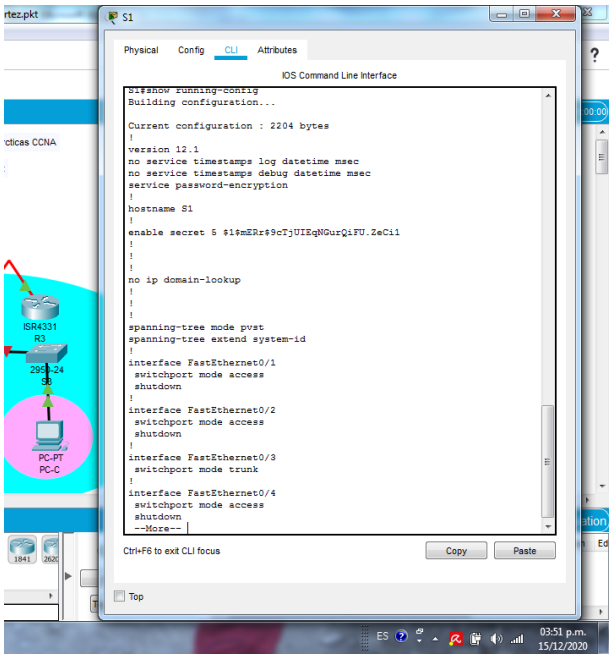
Tabla 19 Configurar switch S1

Elemento o tarea de configuración	**Comandos utilizados**
Desactivar la búsqueda DNS	Switch>ena Switch#conf t Switch(config)#no ip domain-lookup Para hacer uso de comando no ip domain-lookup se debe ingresa a modo privilegiado, luego se ingresa a modo de configuración y se ejecuta. Con el uso del comando desactiva la traducción de nombres a dirección del dispositivo.

Nombre del switch	Switch(config)#hostname S1 S1(config)# Para establecer esta configuración, se ingresa al modo de configuración se coloca el comando respectivo con el nombre que se le va a asignar al dispositivo y se ejecuta, esto permitirá identificar y diferenciar los diferentes dispositivos de la red.
Contraseña de exec privilegiado cifrada	S1(config)#enable secret class S1(config)# Para el uso de este comando se ingresa al modo de configuración y se lo ejecuta. Esto con el fin de permitir asignar la contraseña para el modo EXEC privilegiado y proporcionar mayor seguridad a la contraseña de enable.
Contraseña de acceso a la consola	S1(config)#line console 0 S1(config-line)#password cisco S1(config-line)#login S1(config-line)# Con este comando se utiliza para asignar contraseña de acceso a la consola, y restringir el acceso de cualquier persona no autorizada.
Contraseña de acceso Telnet	S1(config)#line vty 0 15 S1(config-line)#password cisco S1(config-line)#login S1(config-line)# Con este comando se asigna la contraseña de acceso Telnet, con este se habilita el acceso por las líneas vty, estas permiten acceder a un dispositivo a través de telnet o ssh.

Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption S1(config)# Con este comando se aplica un cifrado básico a las contraseñas que se encuentren sin cifrar.
Mensaje MOTD	S1(config)#banner motd %Prohibido el acceso no autorizado% S1(config)# Esta configuración se realiza para emitir notificaciones o mensajes de advertencias para el que se conecte al dispositivo, la configuración del Banner MOTD permite prohibir el acceso no autorizado.

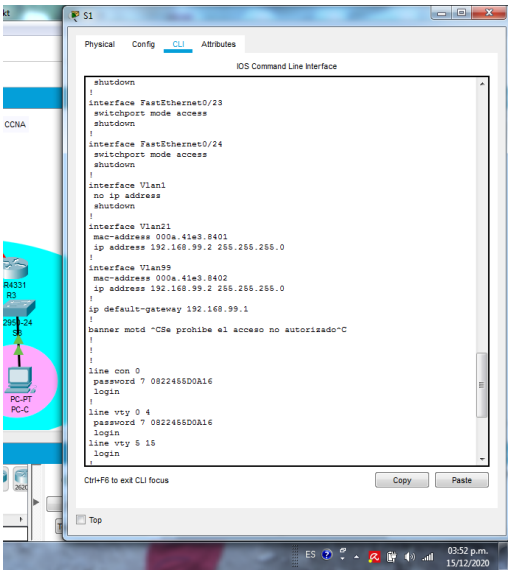
Figura No. 32 Configuración en switch S1



Fuente: autor

Se hace la verificación de las configuraciones realizadas, como la desactivación la búsqueda DNS, cambio de nombre, las diferentes tipos de contraseñas que pueden asignarse en S1, creación de Mensaje MOTD banner y guardado de la configuración del Switch obteniendo resultado satisfactorio

Figura No. 33 Configuración en switch S1



Fuente: autor

Se hace la verificación de las configuraciones realizadas, como la desactivación la búsqueda DNS, cambio de nombre, las diferentes tipos de contraseñas que pueden asignarse en S1, creación de Mensaje MOTD banner y guardado de la configuración del Switch obteniendo resultado satisfactorio

Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

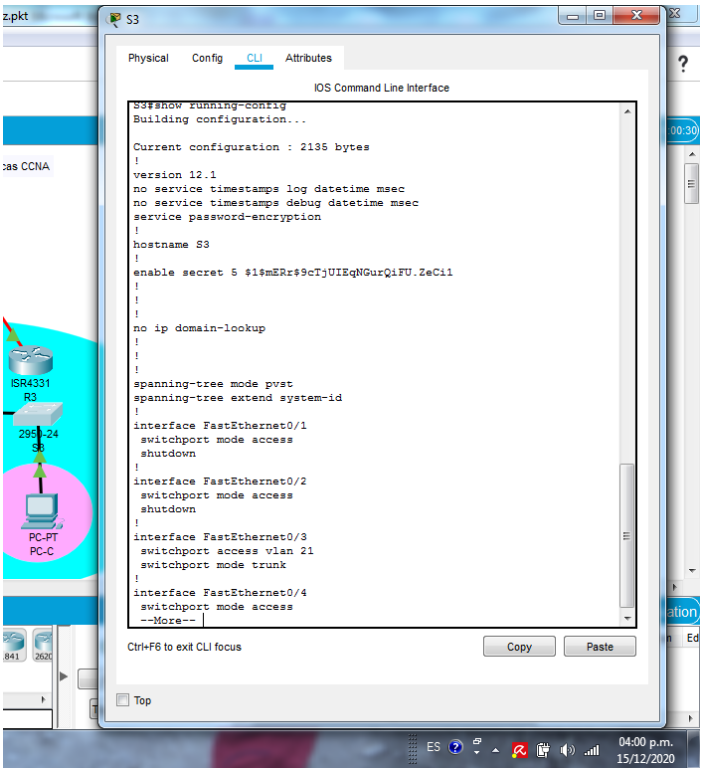
Tabla 20 Configuración de switch s3

Elemento o tarea de configuración	Comandos utilizados
Desactivar la búsqueda DNS	Switch>ena Switch#conf t Switch(config)#no ip domain-lookup Para hacer uso de comando no ip domain-lookup se debe ingresa a modo privilegiado, luego se ingresa a modo de configuración y se ejecuta. Con el uso del comando desactiva la traducción de nombres a dirección del dispositivo.

Nombre del switch	Switch(config)#hostname S3 S3(config)# Para establecer esta configuración, se ingresa al modo de configuración se coloca el comando respectivo con el nombre que se le va a asignar al dispositivo y se ejecuta, esto permitirá identificar y diferenciar los diferentes dispositivos de la red.
Contraseña de exec privilegiado cifrada	S3(config)#enable secret class S3(config)# Para el uso de este comando se ingresa al modo de configuración y se lo ejecuta. Esto con el fin de permitir asignar la contraseña para el modo EXEC privilegiado y proporcionar mayor seguridad a la contraseña de enable.
Contraseña de acceso a la consola	S3(config)#line console 0 S3(config-line)#password cisco S3(config-line)#login S3(config-line)# Con este comando se utiliza para asignar contraseña de acceso a la consola, y restringir el acceso de cualquier persona no autorizada.
Contraseña de acceso Telnet	S3(config)#line vty 0 15 S3(config-line)#password cisco S3(config-line)#login Con este comando se asigna la contraseña de acceso Telnet, con este se habilita el acceso por las líneas vty, estas permiten acceder a un dispositivo a través de telnet o ssh.
Cifrar las contraseñas de texto no cifrado	S3(config)#service password-encryption S3(config)# Con este comando se aplica un cifrado básico a las contraseñas que se encuentren sin cifrar.

Mensaje MOTD	S3(config)#banner motd %Prohibido el acceso no autorizado.% S3(config)# Esta configuración se realiza para emitir notificaciones o mensajes de advertencias para el que se conecte al dispositivo, la configuración del banner MOTD permite prohibir el acceso no autorizado.

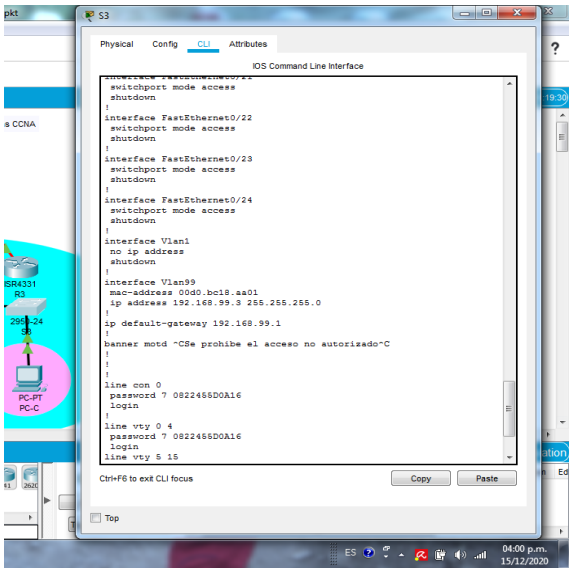
Figura No. 34 Configuración en switch S3



Fuente: autor

Se hace la verificación de las configuraciones realizadas, como la desactivación la búsqueda DNS, cambio de nombre, las diferentes tipos de contraseñas que pueden asignarse en S1, creación de Mensaje MOTD banner y guardado de la configuración del Switch obteniendo resultado satisfactorio

Figura No. 35 Configuración en switch S3



Fuente: autor

Se hace la verificación de las configuraciones realizadas, como la desactivación la búsqueda DNS, cambio de nombre, las diferentes tipos de contraseñas que pueden asignarse en S1, creación de Mensaje MOTD banner y guardado de la configuración del Switch obteniendo resultado satisfactorio

Paso 7: Verificar la conectividad de la red

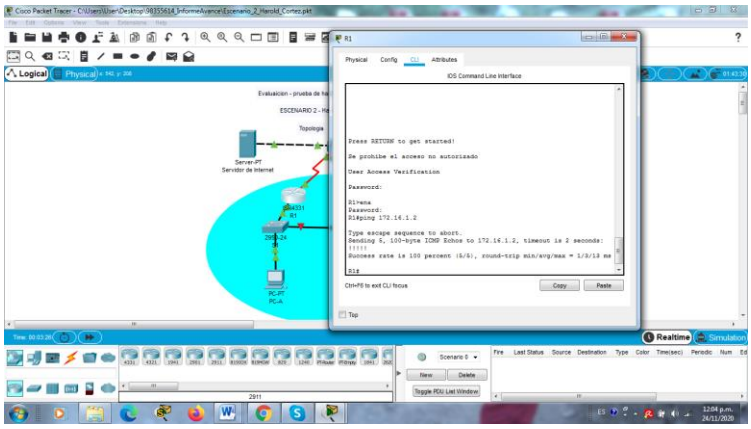
Utilice el comando **ping** para probar la conectividad entre los dispositivos de red.

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 21 Verificación de conectividad

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	Prueba de conectividad exitosa, ver Figura No. 32
R2	R3, S0/0/1	172.16.2.1	Prueba de conectividad exitosa, ver Figura No. 33
PC de Internet	Gateway predeterminado	::	Prueba de conectividad exitosa, ver Figura No. 34

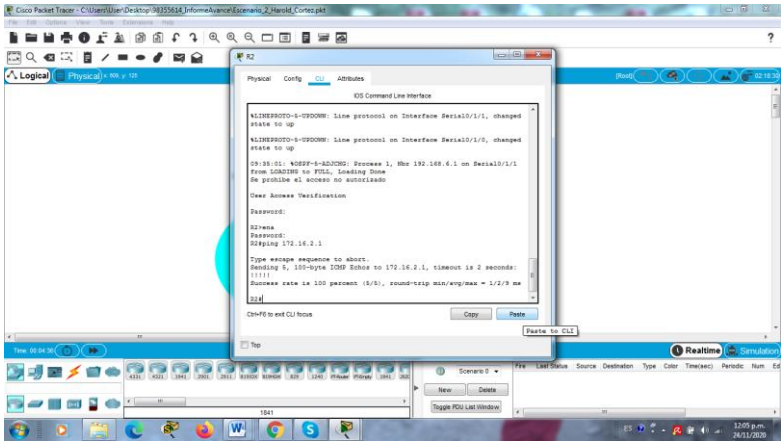
Figura No. 36 Prueba de conectividad



Fuente: autor

Se realiza ping desde R1 hacia R2, S0/0/0 obteniendo resultado satisfactorio.

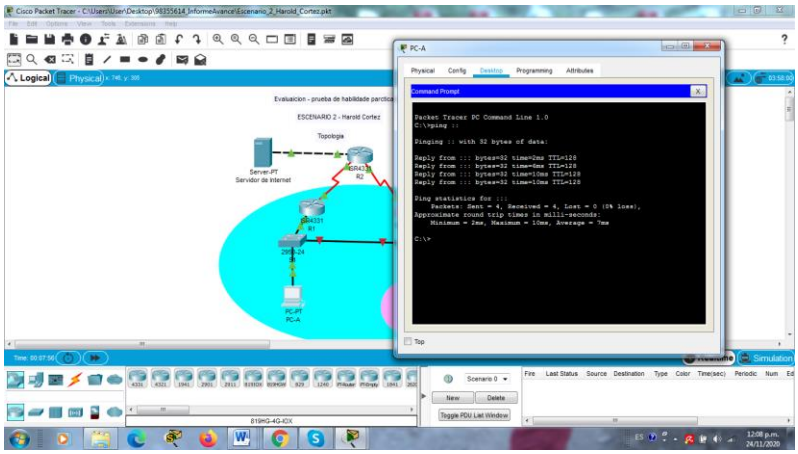
Figura No. 37 Prueba de conectividad



Fuente: autor

Se realiza ping desde R2 hacia R3, S0/0/1 obteniendo resultado satisfactorio.

Figura No. 38 Prueba de conectividad



Fuente: autor

Se realiza ping desde la PC de Internet hacia Gateway predeterminado, obteniendo resultado satisfactorio

Parte 3: configurar la seguridad del switch, las vlan y el routing entre vlan

Paso 1: Configurar S1

La configuración del S1 incluye las siguientes tareas:

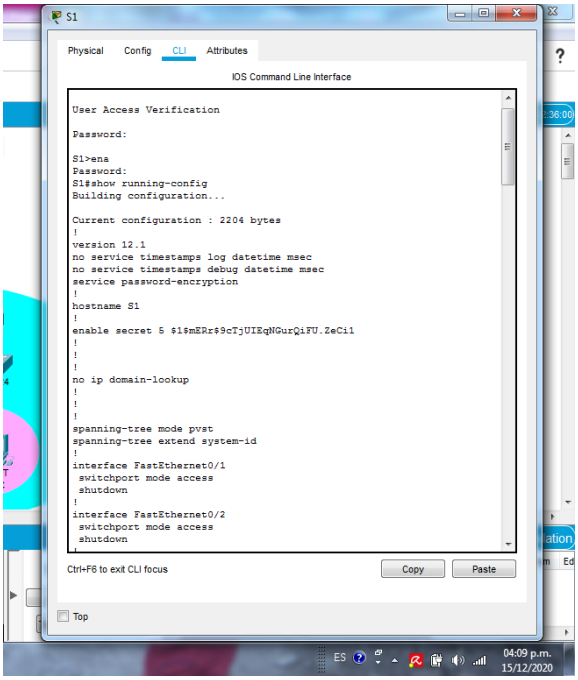
Tabla 22 Configuración de switch S1

Elemento o tarea de configuración	Comandos Utilizados
Crear la base de datos de VLAN	S1(config)#vlan 99 S1(config-vlan)#name Administracion S1(config-vlan)#vlan 21 S1(config-vlan)#name Contabilidad S1(config-vlan)#vlan 23 S1(config-vlan)#name Ingenieria S1(config-vlan)# Se ingresa el comando y se crea la base de datos de Vlan que serán usadas, estas se deben crear una a la vez para poder asignarles un nombre a cada Vlan.

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)# Se hace uso del comando y se le asigna una dirección Ip a la vlan 99, la cual es la vlan administración, se termina la acción activando la interface con el comando no shutdown.
Asignar el gateway predeterminado	S1(config)#ip default-gateway 192.168.99.1 S1(config)# Con el uso de comando se le asigna el gateway predeterminado al dispositivo, lo cual permitirá ser administrado de manera remota.
Forzar el enlace troncal en la interfaz F0/3	S1(config)#interface f0/3 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1 S1(config-if)# Con este comando se hace la configuración que permite al puerto int f0/3 funcionar como troncal.
Forzar el enlace troncal en la interfaz F0/5	S1(config)#interface f0/5 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1 S1(config-if)# Con este comando se hace la configuración que permite al puerto int f0/5 funcionar como troncal.
Configurar el resto de los puertos como puertos de acceso	S1(config-if-range)#int range fa0/1-2, fa0/4, fa0/6-24, g0/1-2 S1(config-if-range)#switchport mode access Con el uso de este comando y el ingreso del rango de las interfaces es posible configurar los puertos de acceso, pero también es necesario definir una vlan.

Asignar F0/6 a la VLAN 21	S1(config)#interface f0/6 S1(config-if)#switchport access vlan 21 S1(config-if)# Con este comando se le asigna a la f0/6 a la vlan 21, también se configura el puerto en modo acceso.
Apagar todos los puertos sin usar	S1(config)#interface range fa 0/1-2, fa 0/4, fa 0/7-24, g0/1-2 S1(config-if-range)#shutdown Con el uso de este comando se apagan los puertos sin usar, es necesario ingresar el rango de los puertos para completar la configuración.

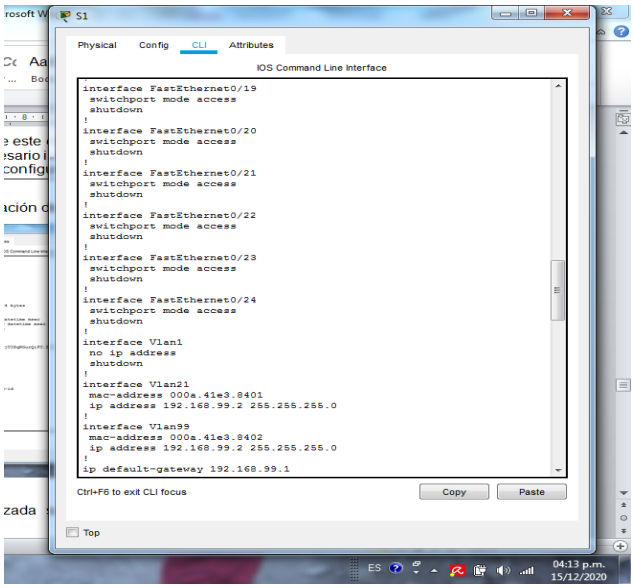
Figura No. 39 Configuración de seguridad y VLAN en switch S1



Fuente: autor

Se verifica la configuración realizada sobre la seguridad del switch S1, obteniendo resultado exitoso

Figura No. 40 Configuración de seguridad y VLAN en switch S1



Fuente: autor

Se verifica la configuración realizada sobre las VLAN y el routing entre VLAN en S1 obteniendo resultado exitoso

Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

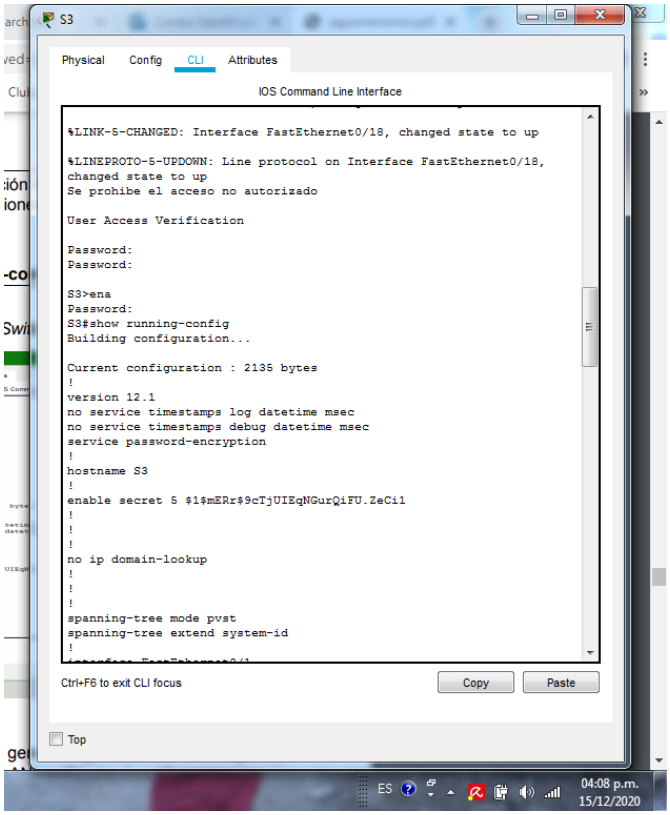
Tabla 23 Configuración del switch S3

Elemento o tarea de configuración	Comandos utilizados
Crear la base de datos de 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)# Se ingresa el comando y se crea la base de datos de Vlan que serán usadas, estas se deben crear una a la vez para poder asignarles un nombre a cada Vlan.

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)# Se hace uso del comando y se le asigna una dirección IP a la vlan 99, la cual es la vlan administración, se termina la acción activando la interface con el comando no shutdown.
Asignar el gateway predeterminado.	S3(config)#ip default-gateway 192.168.99.1 S3(config)# Con el uso de comando se le asigna el gateway predeterminado al dispositivo, lo cual permitirá ser administrado de manera remota.
Forzar el enlace troncal en la interfaz F0/3	S3(config)#interface f0/3 S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1 S3(config-if)# Con este comando se hace la configuración que permite al puerto int f0/3 funcionar como troncal.
Configurar el resto de los puertos como puertos de acceso	S3(config-if)#int range fa0/1-2, fa0/4-24, g0/1-2 S3(config-if-range)#switchport mode access Con el uso de este comando y el ingreso del rango de las interfaces es posible configurar los puertos de acceso, pero también es necesario definir una vlan.
Asignar F0/18 a la VLAN 23	S3(config)#interface f0/18 S3(config-if)#switchport access vlan 23 S3(config-if)# Con este comando se le asigna a la f0/18 a la vlan 21, también se configura el puerto en modo acceso

Apagar todos los puertos sin usar	S3(config)#interface range fa 0/1-2, fa0/4-17, fa0/19-24, g0/1-2 S3(config-if-range)#shutdown Con el uso de este comando se apagan los puertos sin usar, es necesario ingresar el rango de los puertos para completar la configuración.

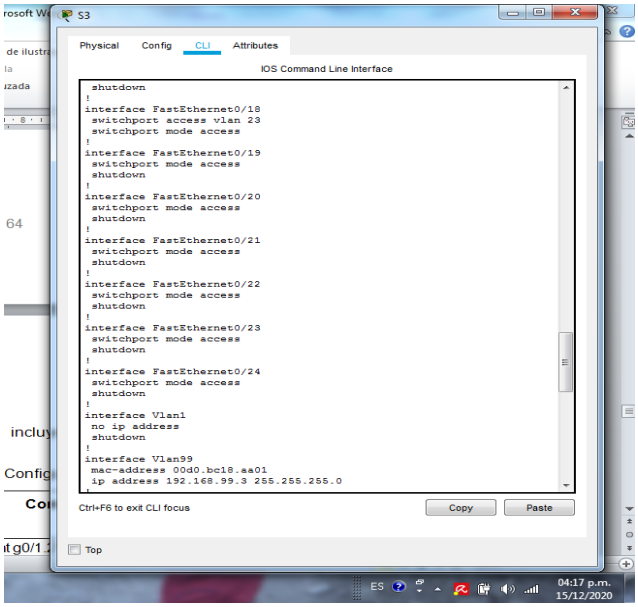
Figura No. 41 Configuración de seguridad y VLAN en switch S3



Fuente: autor

Se verifica la configuración realizada sobre la seguridad del switch S1, obteniendo resultado exitoso

Figura No. 42 Configuración de seguridad y VLAN en switch S3



Fuente: autor

Se verifica la configuración realizada sobre las VLAN y el routing entre VLAN en S1 obteniendo resultado exitoso

Paso 3: Configurar R1

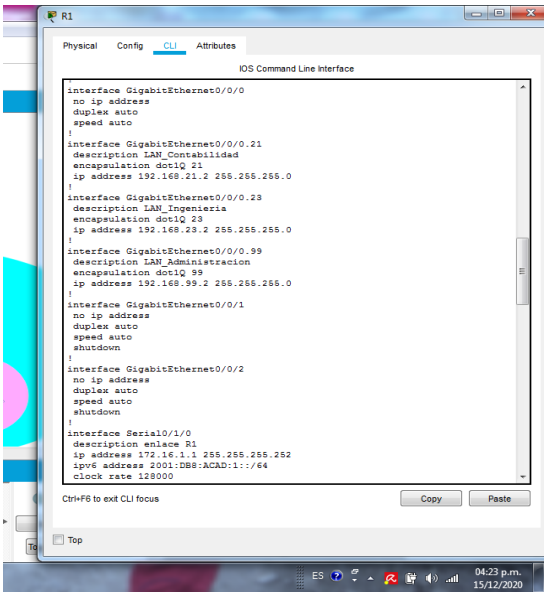
Las tareas de configuración para R1 incluyen las siguientes:

Tabla 24 Tareas de Configuración para R1

Elemento o tarea de configuración	Comandos Utilizados
Configurar la subinterfaz 802.1Q .21 en G0/1	R1(config)#int g0/1.21 R1(config-subif)#description vlan 21 R1(config-subif)#encapsulation dot1Q 21 R1(config-subif)#ip address 192.168.21.1 255.255.255.0 Con este comando se hace la configuración de la Int g0/1 con la creación de la subinterfaz 802.1Q.21, estas son interfaces virtuales creadas sobre el puerto físico, lo cual le permite al router tener control sobre el tráfico de las subinterfaz, que en esta, está asociada a la vlan 21.

Configurar la subinterfaz 802.1Q .23 en G0/1	R1(config-subif)#int g0/1.23 R1(config-subif)#description vlan 23 R1(config-subif)#encapsulation dot1Q 23 Con este comando se hace la configuración de la Int g0/1 con la creación de la subinterfaz 802.1Q.23, estas son interfaces virtuales creadas sobre el puerto físico, lo cual le permite al router tener control sobre el tráfico de las subinterfaz, que en esta, está asociada a la vlan 23.
Configurar la subinterfaz 802.1Q .99 en G0/1	R1(config-subif)#int g0/1.99 R1(config-subif)#description vlan 99 R1(config-subif)#encapsulation dot1Q 99 R1(config-subif)#ip address 192.168.99.1 255.255.255.0 Con este comando se hace la configuración de la Int g0/1 con la creación de la subinterfaz 802.1Q.99, estas son interfaces virtuales creadas sobre el puerto físico, lo cual le permite al router tener control sobre el tráfico de las subinterfaz, que en esta, está asociada a la vlan 99.
Activar la interfaz G0/1	R1(config)#interface g0/1 R1(config-if)#no shut Con el uso de esta comando se habilita el puerto físico G0/1, este paso es necesario para activar también las subinterfaces que están asociadas al puerto.

Figura No. 43 Configuración subinterfaz 802.1Q en Router R1



Fuente: autor

Se hace la verificación de la configuración realizada, sobre creación de interfaces o subinterfaz 802.1Q .21 en G0/1, subinterfaz 802.1Q .23 en G0/1, Configurar la subinterfaz 802.1Q .99 en G0/1, Activar la interfaz G0/1, así como la descripción que pueden asignarse en R1 obteniendo resultado satisfactorio.

Paso 4: Verificar la conectividad de la red

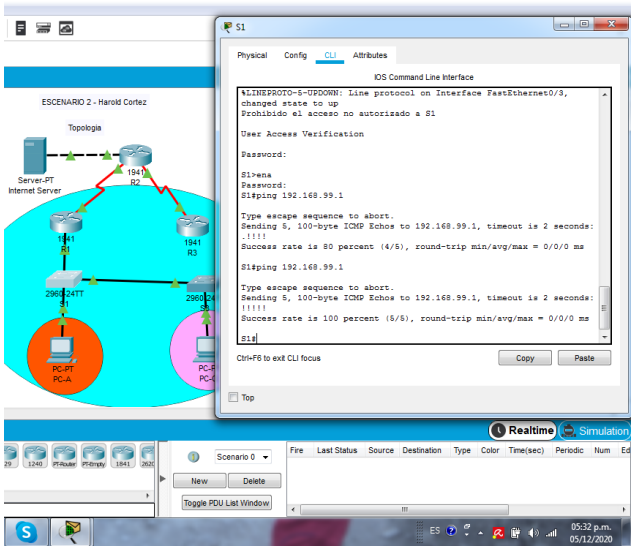
Utilice el comando **ping** para probar la conectividad entre los switches y el R1.

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 25 Tabla de verificación de conectividad

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	Prueba de conectividad exitosa, ver Figura No. 12
S3	R1, dirección VLAN 99	192.168.99.1	Prueba de conectividad exitosa, ver Figura No. 13
S1	R1, dirección VLAN 21	192.168.21.1	Prueba de conectividad exitosa, ver Figura No. 14
S3	R1, dirección VLAN 23	192.168.23.1	Prueba de conectividad exitosa, ver Figura No. 15

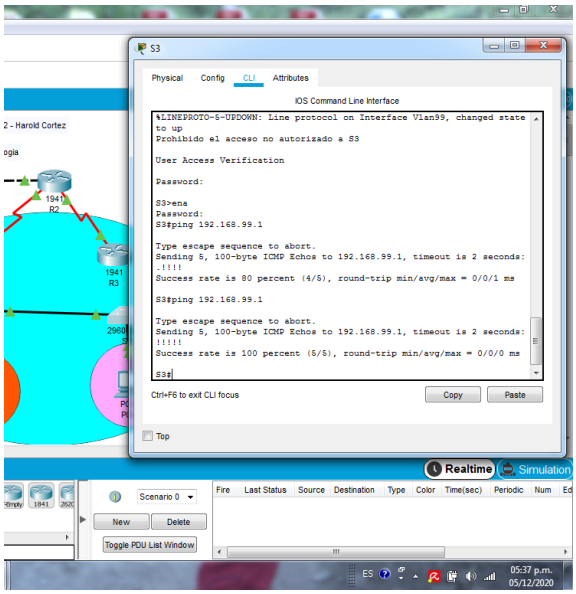
Figura No. 44 Verificación de conectividad



Fuente: autor

Se realiza Ping desde Switch S1, hacia cada dirección asignada a las VLAN 99 R1, obteniendo resultado satisfactorio.

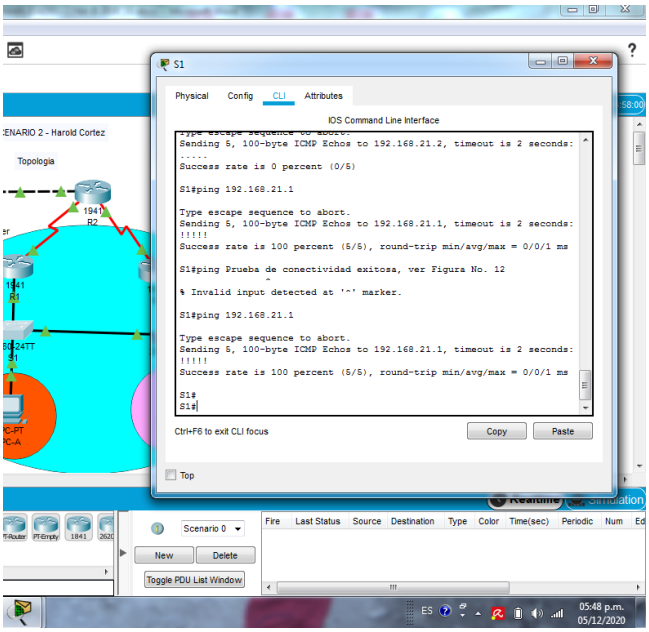
Figura No. 45 Verificación de conectividad



Fuente: autor

Se realiza Ping desde Switch S3, hacia cada dirección asignada a las VLAN 99 R1, obteniendo resultado satisfactorio.

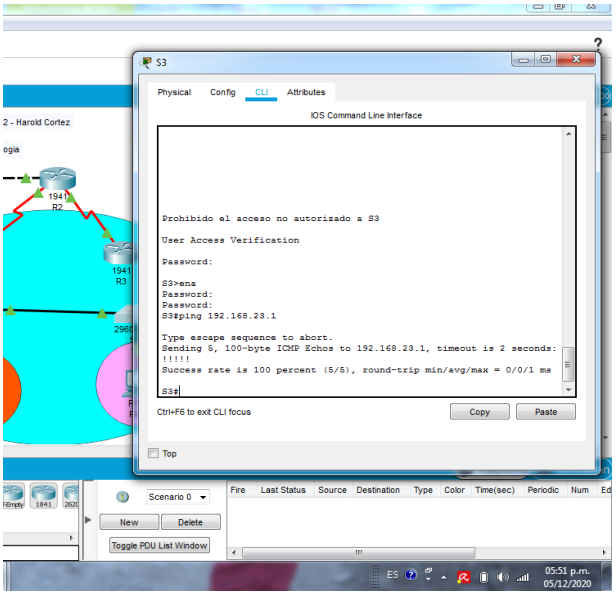
Figura No. 46 Verificación de conectividad



Fuente: autor

Se realiza Ping desde Switch S1 hacia cada dirección asignada a las VLAN 21 R1, obteniendo resultado satisfactorio.

Figura No. 47 Verificación de conectividad



Fuente: autor

Se realiza Ping desde Switch S3 hacia cada dirección asignada a las VLAN 23 R1, obteniendo resultado satisfactorio.

Parte 4: configurar el protocolo de routing dinámico ospf

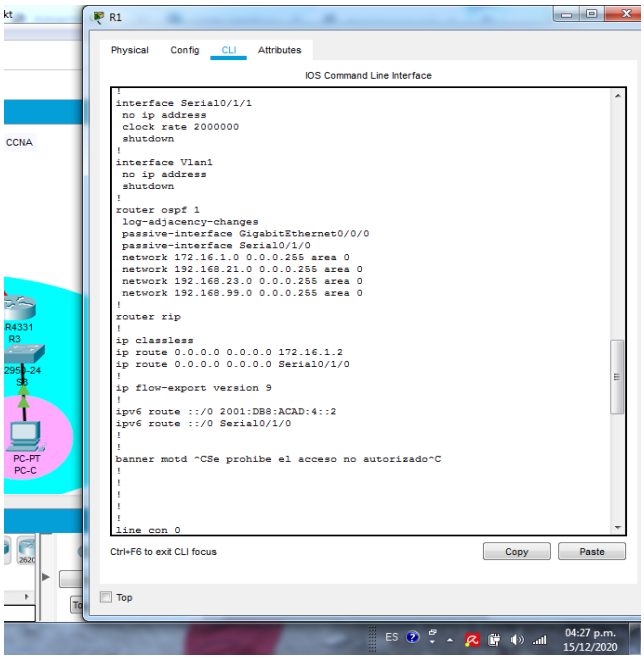
Paso 1: Configurar OSPF en el R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 26 Configuración de OSPF en R1

Elemento o tarea de configuración	Comandos Utilizados
Configurar OSPF área 0	R1(config)#router ospf 1 Con el uso de este comando se habilita el protocolo de enrutamiento OSPF en el router.
Anunciar las redes conectadas directamente	R1(config)#router ospf 1 R1(config-router)#network 172.16.1.0 0.0.0.3 area 0 R1(config-router)#network 192.168.21.0 0.0.0.255 area 0 R1(config-router)#network 192.168.23.0 0.0.0.255 area 0 R1(config-router)#network 192.168.99.0 0.0.0.255 area 0 R1(config-router)# Con anterior configuración una vez habilitado el enrutamiento sopf, se establecen las redes por las que se envían los mensajes de actualización de rutas
Establecer todas las interfaces LAN como pasivas	R1(config)#router ospf 1 R1(config-router)#passive-interface g0/1.21 R1(config-router)#passive-interface g0/1.23 R1(config-router)#passive-interface g0/1.99 R1(config-router)# Con el anterior comando se establece la interfaz LAN como pasiva y ademas se evita que se envíen actualizaciones a través de esta interfaz.
Desactive la sumarización automática	OSPF no sumariza

Figura No. 48 Configuración OSPF en Router R1



Fuente: autor

Se hace la verificación en el router R1 mediante el comando show running-config sobre la configuración OSPF área 0, anunciar las redes conectadas directamente, Estableciendo todas las interfaces LAN como pasivas, realizar la desactivación de la sumarización automática obteniendo resultado satisfactorio.

Paso 2: Configurar OSPF en el R2

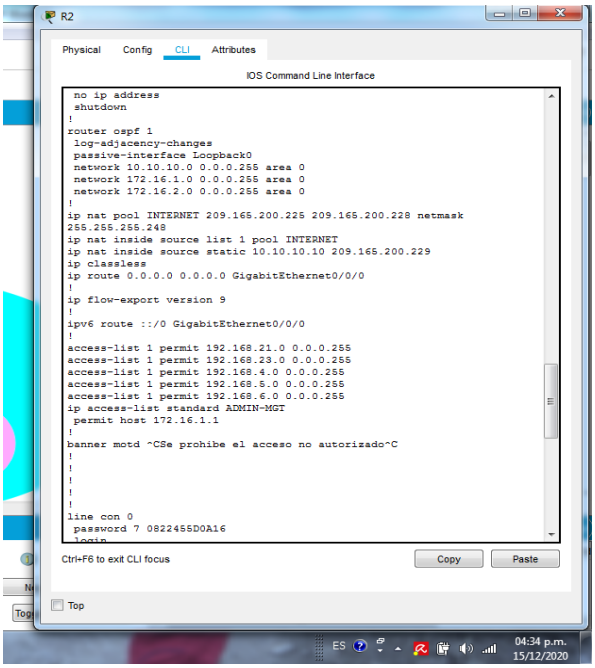
La configuración del R2 incluye las siguientes tareas:

Tabla 27 Configuración de OSPF en R2

Elemento o tarea de configuración	**Comandos Utilizados**
Configurar OSPF área 0	R2(config)#router ospf 1 Con el uso de este comando se habilita el protocolo de enrutamiento OSPF en el router.

Anunciar las redes conectadas directamente	R2(config)#router ospf 1 R2(config-router)#network 10.10.10.0 0.0.0.255 area 0 R2(config-router)#network 172.16.1.0 0.0.0.3 area 0 R2(config-router)#network 172.16.2.0 0.0.0.3 area 0 R2(config-router)# Con anterior configuración una vez habilitado el enrutamiento sopf, se establecen las redes por las que se envían los mensajes de actualización de rutas
Establecer la interfaz LAN (loopback) como pasiva	R2(config-router)#passive-interface loopback0 R2(config-router)# Con el anterior comando se establece la interfaz LAN como pasiva y ademas se evita que se envíen actualizaciones a través de esta interfaz.
Desactive la sumarización automática.	OSPF no sumariza

Figura No. 49 Configuración OSPF en Router R2



Fuente: autor

Se hace la verificación en el router R2 mediante el comando show running-config sobre la configuración OSPF área 0, anunciar las redes conectadas directamente,

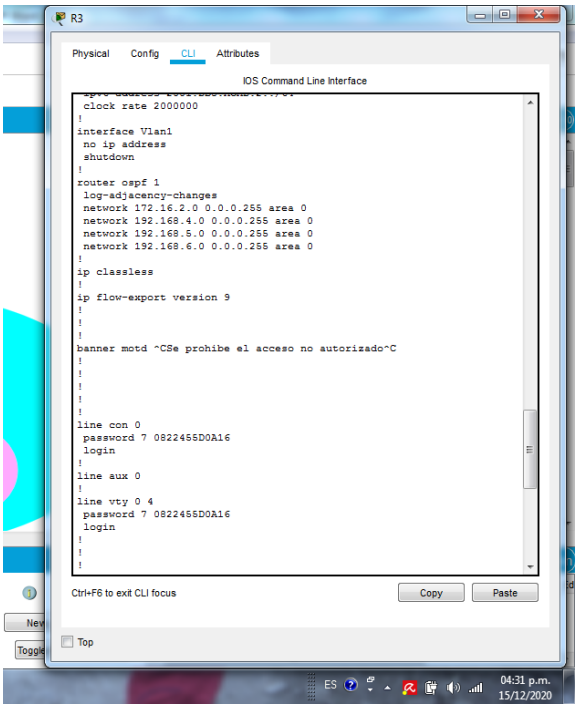
Estableciendo todas las interfaces LAN como pasivas, realizar la desactivación de la sumarización automática obteniendo resultado satisfactorio.

Paso 3: Configurar OSPFv3 en el R3

La configuración del R3 incluye las siguientes tareas:

Elemento o tarea de configuración	Comandos Utilizados
Configurar OSPF área 0	R3(config)#router ospf 1 R3(config-router)# Con el uso de este comando se habilita el protocolo de enrutamiento OSPF en el router.
Anunciar redes IPv4 conectadas directamente	R3(config-router)# network 172.16.2.0 0.0.0.3 area 0 R3(config-router)#network 192.168.4.0 0.0.0.255 area 0 R3(config-router)#network 192.168.5.0 0.0.0.255 area 0 R3(config-router)#network 192.168.6.0 0.0.0.255 area 0 Para el uso del anterior comando ingresamos a la interface y mencionamos el area
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 Con el anterior comando se establece las interfaz LAN como pasiva y ademas se evita que se envíen actualizaciones a través de esta interfaz.
Desactive la sumarización automática.	OSPF no sumariza

Figura No. 50 Configuración OSPF en Router R3



Fuente: autor

Se hace la verificación en el router R3 mediante el comando show running-config sobre la configuración OSPF área 0, anunciar las redes conectadas directamente, Estableciendo todas las interfaces LAN como pasivas, realizar la desactivación de la sumarización automática obteniendo resultado satisfactorio.

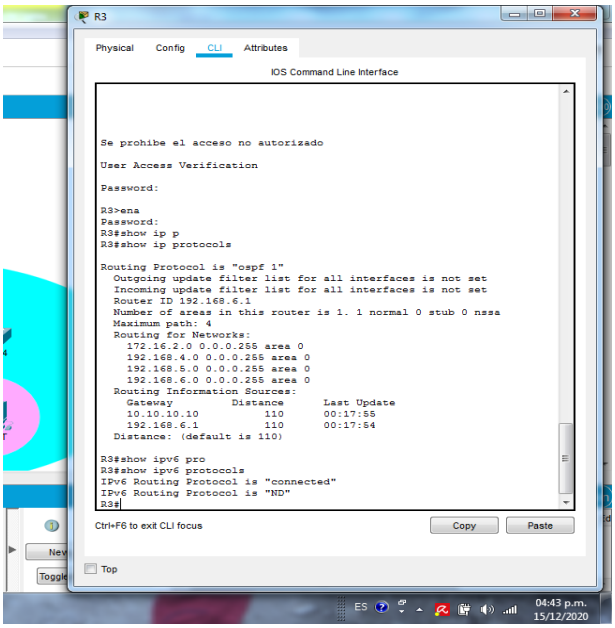
Paso 4: Verificar la información de OSPF

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

Tabla 28 Verificación de 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?	show ip protocols show ipv6 protocols
¿Qué comando muestra solo las rutas OSPF?	R3#show ip route ospf
¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	R3#show running-config | section router ospf

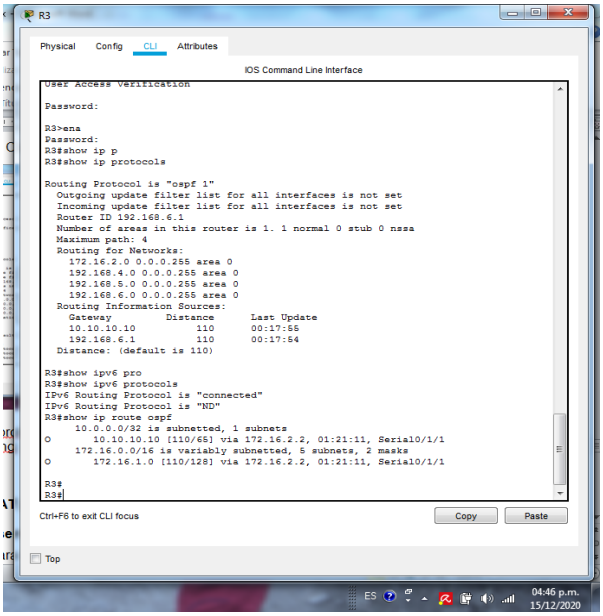
Figura No. 51 Comando show Ip protocols



Fuente: autor

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

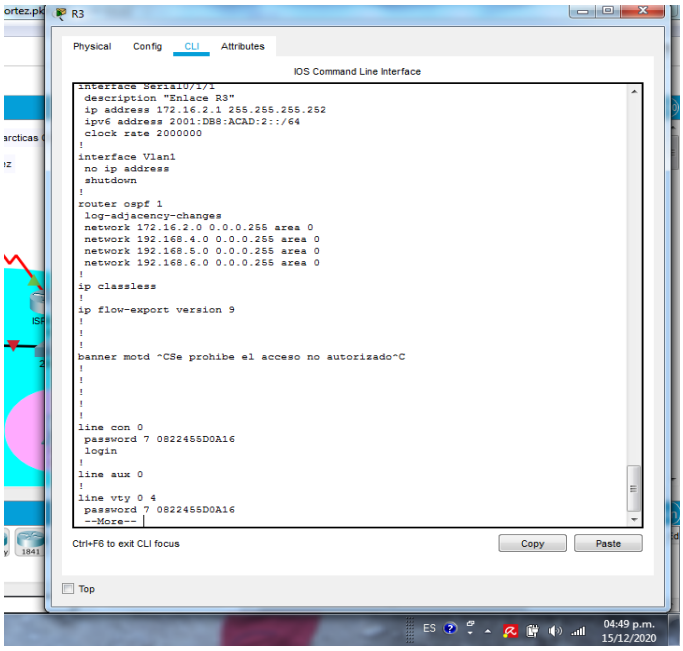
Figura No. 52 Comando show ip route ospf



Fuente: autor

Con el uso del comando show ip route ospf se muestra solo las rutas OSPF

Figura No. 53 Comando show run



Fuente: autor

Con el comando show run | section route ospf se muestra la sección de OSPF de la configuración en ejecución, pero packet tracer no soporta el comando se debe utilizar el comando show run

Parte 5: Implementar DHCP y NAT para IPv4

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

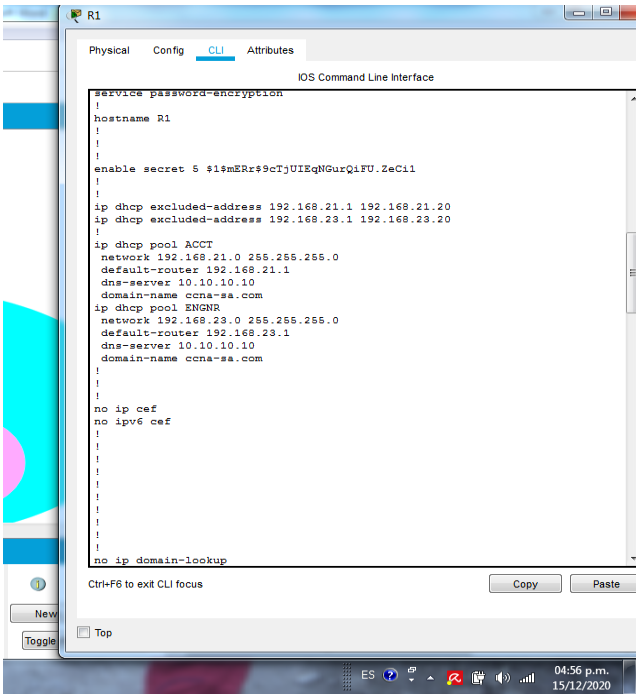
Las tareas de configuración para R1 incluyen las siguientes:

Tabla 29 Configuración de R1 como servidor DHCP

Elemento o tarea de configuración	Comandos utilizados
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 R1(config)# Con el uso de este comando, se reservan las primeras direcciones ip en la vlan 21 para configuraciones estáticas, las cuales no serán asignadas a ningún dispositivo.

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)# Con el uso de este comando, se reservan las primeras direcciones ip en la vlan 21 para configuraciones estáticas, las cuales no serán asignadas a ningún dispositivo.
Crear un pool de DHCP para la VLAN 21.	R1(config)#ip dhcp pool ACCT R1(dhcp-config)#network 192.168.21.0 255.255.255.0 R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com R1(dhcp-config)#default-router 192.168.21.1 Con la anterior configuración, se crea un pool de DHCP para la Vlan 21, asignando un nombre especifico, designando la red a utilizar, el Gateway predeterminado, el dominio y la dirección DNS
Crear un pool de DHCP para la VLAN 23	R1(config)#ip dhcp pool ENGNR R1(dhcp-config)#network 192.168.23.0 255.255.255.0 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)# Con la anterior configuración, se crea un pool de DHCP para la Vlan 21, asignando un nombre especifico, designando la red a utilizar, el Gateway predeterminado, el dominio y la dirección DNS

Figura No. 54 Configuración DHCP y Pool en Router R1



Fuente: autor

Se realiza la verificación de la configuración general ingresada sobre reservar las primeras 20 direcciones IP en las VLAN 21 Y 23, así como crear un pool de DHCP para la VLAN 21 y otro para la VLAN 23 mediante el comando show running-config en el R1

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

La configuración del R2 incluye las siguientes tareas:

Tabla 30 Configuración de router R2 con NAT estática y dinámica

Elemento o tarea de configuración	Comandos Utilizados
Crear una base de datos local con una cuenta de usuario	R2(config)#username webuser privilege 15 secret cisco12345 R2(config)# Con este comando se crea una base de datos local con una cuenta de usuario, con su respectiva contraseña, que deberá ser usada para ingreso al servidor web.

Habilitar el servicio del servidor HTTP	R2(config)#ip http server Packet Tracer no soporta este comando
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	R2(config)#ip http authentication local Packet Tracer no soporta este comando
Crear una NAT estática al servidor web.	R2(config)#ip nat inside source static 10.10.10.10 209.165.200.237 Con este comando se crea una NAT estática al servidor web, para que el router pueda traducir, la dirección privada del servidor interno y la dirección publica
Asignar la interfaz interna y externa para la NAT estática	R2(config)#int g0/0 R2(config-if)#ip nat outside R2(config-if)#int s0/0/0 R2(config-if)#ip nat outside R2(config-if)#int s0/0/1 R2(config-if)#ip nat outside Con la anterior configuración, se asigna la interfaz interna y extrema para NAT estática y también se define cual será la interfaz de entrada y salida de las traslaciones
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 Con la anterior configuración, se configura la NAT dinámica dentro de una ACL privada y se crean las listas de control de acceso para cada red.
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 Con el anterior comando se define el pool de direcciones IP públicas utilizables.

Definir la traducción de NAT dinámica	R2(config)#ip nat inside source list 1 pool INTERNET Con el anterior comando se define la traducción de NAT dinámica la cual asigna las direcciones públicas según el orden de llegada.

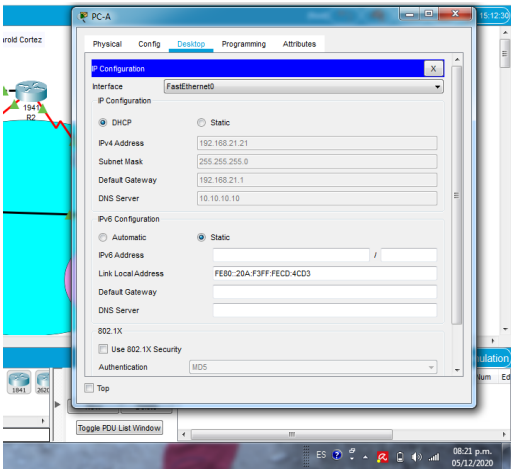
Paso 3: Verificar el protocolo DHCP y la NAT estática

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

Tabla 31 Verificación de protocolo DHCP y la NAT

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	Recibió por DHCP la dirección 192.168.21.21/24, ver figura 16
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	Recibió por DHCP la dirección192.168.23.21/24, ver figura 17
Verificar que la PC-A pueda hacer ping a la PC-C **Nota:** Quizá sea necesario deshabilitar el firewall de la PC.	Ping exitoso, ver figura 18
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**	Prueba no exitosa el simulador no recibe el comando IP http server en el router.

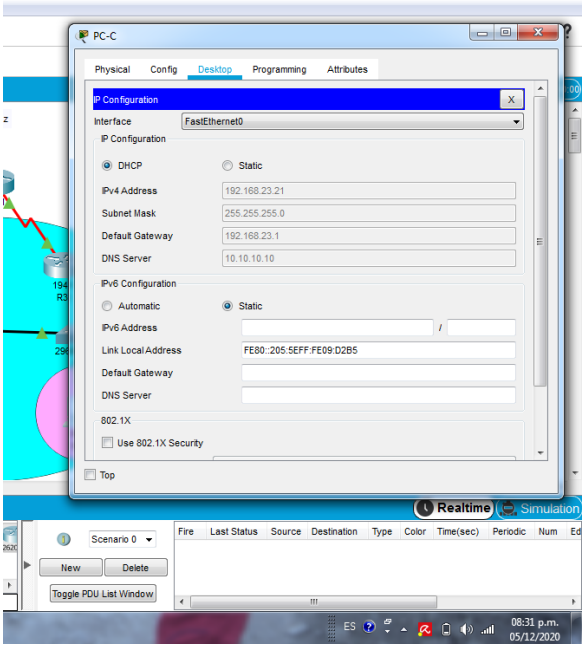
Figura No. 55 Verificación de asignación IP por DHCP



Fuente: autor

Se verifica que la PC-A haya adquirido información de IP del servidor de DHCP, obteniendo resultado satisfactorio.

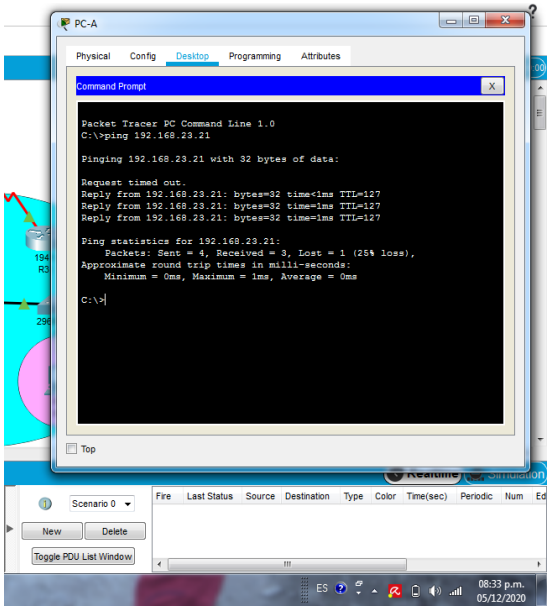
Figura No. 56 Verificación de asignación IP por DHCP



Fuente: autor

Se verifica que la PC-C haya adquirido información de IP del servidor de DHCP, obteniendo resultado satisfactorio.

Figura No. 57 Prueba de conectividad



Fuente: autor

Se hace verificación de que la PC-A pueda hacer ping a la PC-C, obteniendo resultado satisfactorio

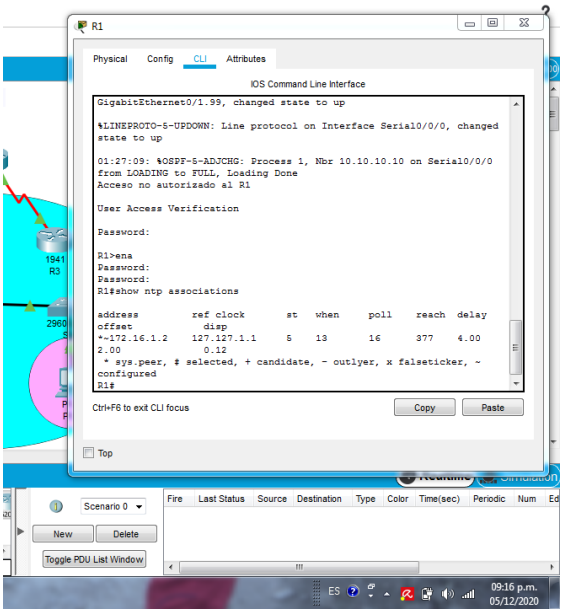
Parte 6: Configurar NTP

Tabla 32 Configuración de NTP

Elemento o tarea de configuración	Comandos utilizados
Ajuste la fecha y hora en R2.	R2#clock set 9:00:00 5 may 2016 R2# Con el anterior comando se configura la fecha y la hora en el router R2.
Configure R2 como un maestro NTP.	R2(config)#ntp master 5 R2(config)# Con el anterior comando se configura R2 como un maestro NTP.

Configurar R1 como un cliente NTP.	R1(config)#ntp server 172.16.1.2 En este comando se configura R1 como un cliente NTP.
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	R1(config)#ntp update-calendar Con este comando se configura el R1 para actualizaciones de calendario periódicas con hora NTP.
Verifique la configuración de NTP en R1.	R1(config)#show ntp associations Ver Figura 19

Figura No. 58 Verificación de configuración de NTP



Fuente: autor

Se realiza la respectiva verificación de la configuración ingresada sobre la creación y ajuste de la fecha y hora en R2 y R2 como un maestro NTP y R1 como un cliente NTP y configurar las actualizaciones de calendario periódicas con hora NTP en R1, obteniendo respuesta satisfactoria

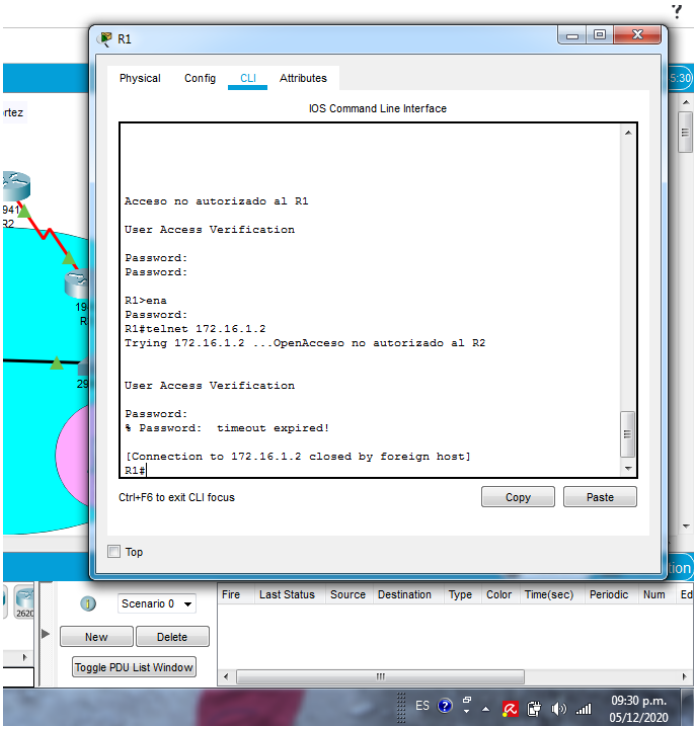
Parte 7: Configurar y verificar las listas de control de acceso (ACL)

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

Tabla 33 Restricción de acceso a líneas VTY

Elemento o tarea de configuración	Comandos Utilizados
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	R2(config)#ip access-list standard ADMIN-MGT R2(config-std-nacl)#permit host 172.16.1.2 R2(config-std-nacl)#exit Con la anterior se configura la lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2. Ademas las ACL compara la dirección de origen de los paquetes IP con las direcciones configuradas en la ACL lo cual permite controlar el tráfico.
Aplicar la ACL con nombre a las líneas VTY	R2(config)#line vty 0 15 R2(config-line)#access-class ADMIN-MGT in Con la configuracion anterior se aplica la ACL con nombre a las líneas VTY para un correcto funcionamiento
Permitir acceso por Telnet a las líneas de VTY	R2(config-line)#transport input telnet Con el anterior comando especifica en las líneas vty que permita el acceso por Telnet.
Verificar que la ACL funcione como se espera	R1#telnet 172.16.1.2 Ver figura No. 20 y Figura No. 21

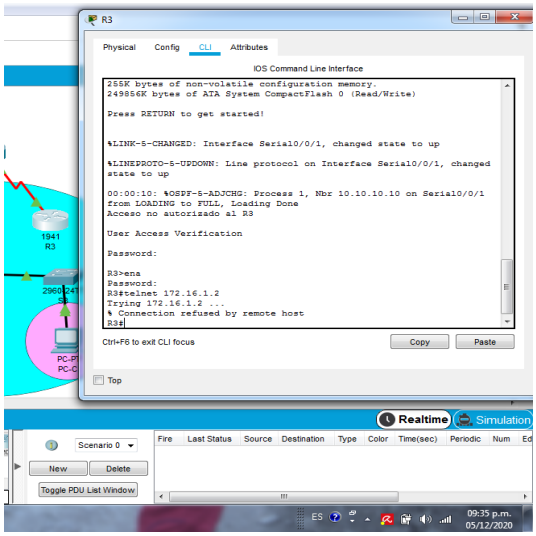
Figura No. 59 Verificación de funcionamiento de la ACL



Fuente: autor

Se verifica funcionamiento de la ACL, obteniendo correcto funcionamiento

Figura No. 60 Verificación de funcionamiento de la ACL



Fuente: autor

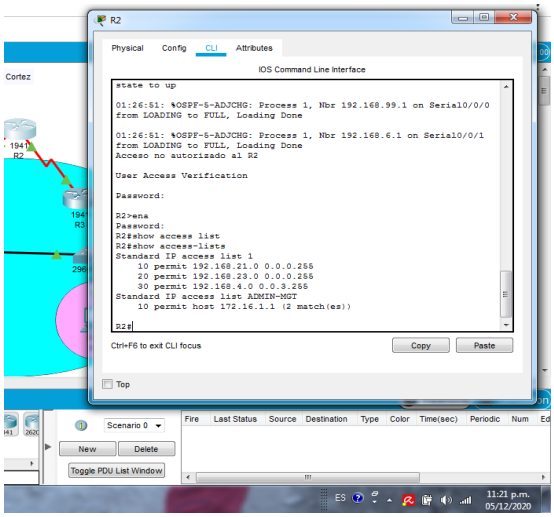
Se verifica funcionamiento de la ACL, obteniendo correcto funcionamiento

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

Tabla 34 Comandos que muestran determinadas configuraciones en Router

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 Ver figura No. 22
Restablecer los contadores de una lista de acceso	R2#clear Access-list counters
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	R2#show ip interface Ver figura No. 23
¿Con qué comando se muestran las traducciones NAT?	R2#show ip nat translations Ver figura No. 24
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	R2#clear ip nat translation

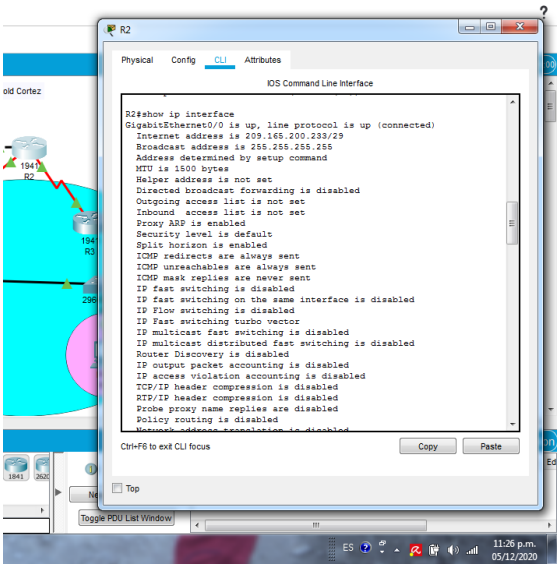
Figura No. 61 Verificación de comando show access-lists



Fuente: autor

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

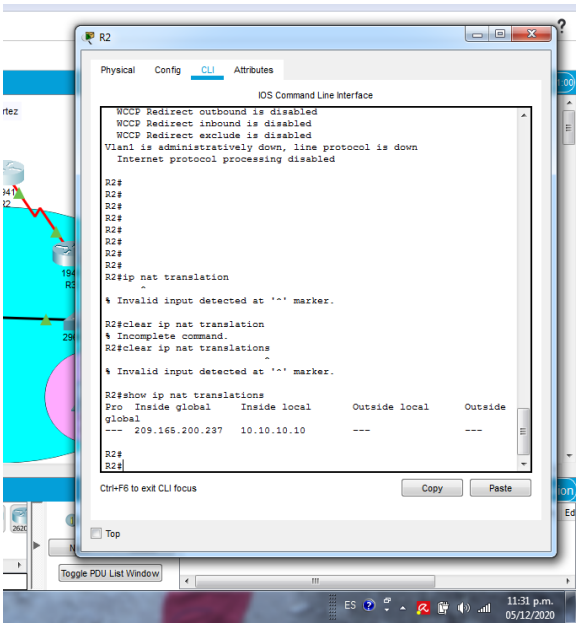
Figura No. 62 Verificación de comando show ip interface



Fuente: autor

En esta imagen se muestra qué ACL se aplica a una interfaz y la dirección en que se aplica

Figura No. 63 Verificación de comando show ip nat translations



Fuente: autor

En la anterior figura se muestra el comando utilizado para eliminar las traducciones de NAT dinámicas

CONCLUSIONES

Luego de realizar las actividades propuestas se hace un aprendizaje acertado y significativo, acerca de lo que son redes LAN, logrando hacer cada una de las configuraciones de los diferentes dispositivos, especialmente en swtiches y router, que eran necesarios para la conformación de la topología propuesta.

Con el desarrollo practico de los anteriores escenarios, se puede evidenciar los conocimientos adquiridos necesarios e implementados en el área de redes LAN y WAN, ademas se logra aprender sobre el direccionamiento mediante interfaces específicas en un router, con el cual que estemos trabajando, permitiendo conectividad IPv4 e IPv6, seguridad de switches, routing entre VLAN, el protocolo de routing dinámico OSPF, el protocolo de configuración de hosts dinámicos (DHCP), la traducción de direcciones de red dinámicas y estáticas (NAT), listas de control de acceso (ACL) y el protocolo de tiempo de red (NTP) servidor/cliente. Durante la evaluación, probará y registrará la red mediante los comandos comunes de CLI.

Se concluye sebre la importancia que tiene la inserción de comandos, con los cuales se logran hacer una configuración de interfaces y subinterfaces asignando direcciones, con sus respectivos protocolos de seguridad. Ademas se evidencia la importancia de la realización de pruebas de seguimiento a los comandos ejecutados, con los cuales podemos verificar la correcta configuración de los dispositivos, mediante las pruebas de conectividad entre equipos, por medio de comandos ping a las direcciones IP en cualquiera de sus versiones y comprobar él envió y recibido de paquetes de manera exitosa.

Por último se destaca la acertada proposición de trabajo con los dos escenarios propuestos para su desarrollo, ya que con la resolución de los mismos y siguiendo el paso a paso del manual de instrucciones, se logra el objetivo planteado que va desde el armado de la topología, la eliminación de sus configuraciones de inicio de los dispositivos, borrado de bases de datos de VLAN en los switch, hasta lograr el total de las configuraciones y realizar las respectivas pruebas de funcionamiento.

BIBLIOGRAFÍA

Configuración de conexión troncal ISL y 802.1q entre un switch CatOS y un router externo (ruteo InterVLAN)
https://www.cisco.com/c/es_mx/support/docs/switches/catalyst-4000-series-switches/24064-171.html

Cisco CCNA – Configuración DHCP
http://blog.capacityacademy.com/2014/01/09/cisco-ccna-como-configurar-dhcp-en-cisco-router/

Como configurar OSPF en router
http://blog.capacityacademy.com/2014/06/23/cisco-ccna-como-configurar-ospf-en-cisco-router/

UNAD (2014). Configuración de Switches y Routers [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgL9QChD1m9EuGqC

CISCO. (2014). Enrutamiento Dinámico. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-courseassets.s3.amazonaws.com/RSE50ES/module7/index.html#7.0.1.1

ANEXOS

Enlace a archivos de Packet Tracer escenarios 1 y 2

https://drive.google.com/drive/folders/1cX4idLiukI0kNLHKDWSrTjj6jo1si5X0?usp=sharing

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

Harol Heyder Cortéz Martínez
Universidad Nacional Abierta y a Distancia UNAD, hhcortezm@unadvirtual.edu.co

Resumen - En el siguiente documento se evidenciara la práctica de conocimientos específicos, y profundizando en el área de redes y comunicaciones de tal forma que se ponga en práctica las capacidades y demandas del mercado en especialización de las tecnologías informáticas y telecomunicaciones, en donde se verá reflejado acompañado de un practica de laboratorio la cual se evidenciará en el software de CISCO packet tracer, la cual nos permitirá evidenciar la practica teórica en una simulación que permite un acercamiento al mundo real.

Abstract: The following document intends to put into practice specific knowledge, deepening in the area of networks and communications in such a way that the capacities and demands of the market in specialization of information technology and telecommunications are put into practice, where it will be reflected accompanied by a laboratory practice which will be evidenced in the CISCO packet tracer software, which will allow us to demonstrate the theoretical practice in a simulation that allows an approach to the real world.

Palabras claves: Índice de Términos - Telecomunicaciones, Packet Tracer, simulación, laboratorios

I. INTRODUCCION

El siguiente trabajo se basará en la simulación de CISCO y Networking, pero ¿en qué consiste CISCO?

CISCO se le conoce como una de las empresa global y principalmente en el medio de mantenimiento y consultoría de equipos de telecomunicaciones, donde uno de los fuertes es la fabricación y venta de equipo de telecomunicaciones.

Networking: consiste en una ampliación o contacto profesional donde consiste ser usada por empresas donde se presenta un proceso de búsqueda de nuevas alianzas estratégicas o profesionales.
En el siguiente trabajo se deberá tener presente los siguientes términos los cuales serán esenciales para su elaboración:
Topología: consiste en la propiedad de los cuerpos geométricos que permanecen inalteradas por transformaciones continuas donde se pretende conocer los espacio y funciones topológicas continua.

Enrutamiento: esta función consiste en buscar los posibles paquetes en una red donde su topología consiste en una gran conectividad.

Se debe conocer que la utilización de datos es algo que se utiliza a diario, como se presentan de manera locales y ya sean de manera más amplia LAN O WAN , estas redes se pueden encontrar en desde la comodidad desdés un router donde esté presente una conexión de uno o más dispositivos como lo son computadoras
En el laboratorio los switches consisten en atender las diferentes problemas u necesidades de comunicación de datos de una red de computadoras

A través de este trabajo se pretende evidenciar los conocimientos mediante la aplicación de enrutamiento, estándares de seguridad y ingreso en los diferentes dispositivos de la red, sin dejar de menos importancia las configuraciones OSPF, RIP, NAT, verificación de ACL.

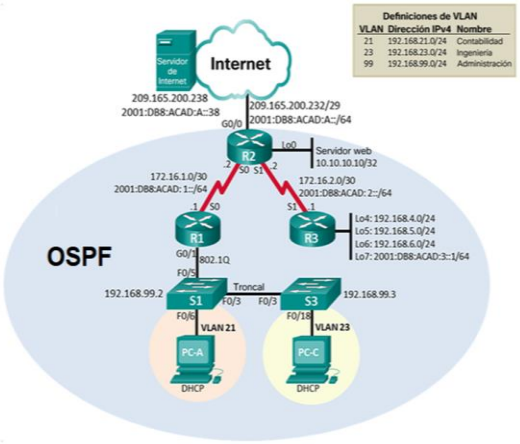
II. PROCEDIMIENTO

A. Desarrollo del escenario

El objetivo que pretende la resolución de este examen de habilidades CCNA consiste en configurar una red pequeña para que admita conectividad IPv4 e IPv6, seguridad de switches, routing entre VLAN, el protocolo de routing dinámico OSPF, el protocolo de configuración de hosts dinámicos (DHCP), la traducción de direcciones de red dinámicas y estáticas (NAT), listas de control de acceso (ACL) y el protocolo de tiempo de red (NTP) servidor/cliente. Durante la evaluación, probará y registrará la red mediante los comandos comunes de CLI.

Inicialmente se plantea la topología lógica que ofrece el desafío en cuestión:

Fig. 1. Topología lógica del escenario 2.



Fuente: autor

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

Para iniciar una correcta práctica en la resolución del problema inicialmente es necesario eliminar configuraciones preestablecidas y reiniciar los dispositivos intermedios (routers y switches) presentes en la topología. Es por esto que acudimos al los comandos:

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

Erase startup-config	Eliminar el archivo de configuración inicial startup-config de todos los routers y switches
Reload	Se reinician al estado de fábrica los switches y routers
Delete flash:vlan.dat	Con esto nos aseguramos de eliminar bases de datos VLAN alojadas previamente en los routers y switches

Estos comandos deben ejecutarse en todos los dispositivos intermedios de la topología para asegurar la correcta integridad.

Parte 2: Configurar los parámetros básicos de los dispositivos

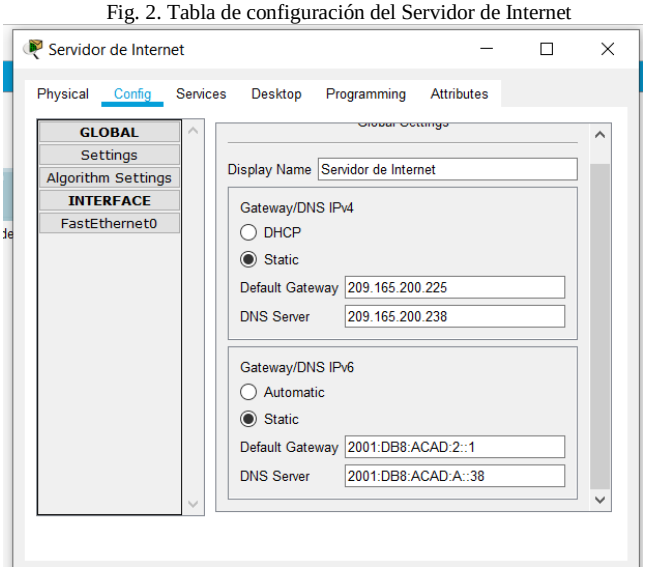
Paso 1: Configurar la computadora de Internet

Ahora lo que se procede es configurar correctamente el servidor de internet al que estaremos realizando consultas, siguiendo como base la tabla siguiente:

TABLA 2: ESPECIFICACIONES EN LOS ELEMENTOS DE CONFIGURACIÓN

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.0
Gateway predeterminado	209.165.200.225
Dirección IPv6/subred	2001:DB8:ACAD:A::38
Gateway predeterminado IPv6	2001:DB8:ACAD:2::1

Fig. 2. Tabla de configuración del Servidor de Internet



Fuente: autor

Paso 2: Configurar R1

Después de configurar el servidor de internet, se procede a realizar las confguraciones iniciales del router R1, es por ello que se ejecutan los siguientes comandos:

Tabla 3: configuración en el router R1

Enable	entrar en modo EXEC privilegiado
Config t	Entrar a la configuración de la terminal
No ip domain-lookup	Permite desactivar la búsqueda DNS automática
Hostname R1	cambia el nombre del host a R1
Enable secret class	asigna una clave de acceso para acceder al modo EXEC privilegiado
line console 0	acceder a la configuración de la consola de acceso normal
password cisco	asigna una clave de acceso
login	habilita el acceso por contraseña
line vty 0 4	acceder a la configuración de las líneas vty telnet
password cisco	asigna una clave de acceso
login	habilita el acceso por contraseña
service password-encryption	Cifra todas las contraseñas que estén en texto plano
banner motd “Se prohíbe el acceso no autorizado”	Establece un banner de acceso para alertar a los intrusos y dejar mensajes descriptivos sobre la conexión

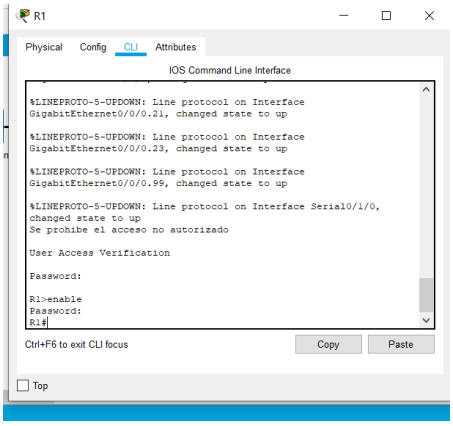
Hasta aquí van las configuraciones iniciales de la mayoría de los dispositivos intermedios de la topología, ahora siguen con las configuraciones de la interfaz:

Tabla 4: Configuraciones de la interfaz

interface serial 0/1/0	habilita la configuración de la interfaz del serial del puerto especificado
description “Enlace R1”	añade una descripción a la interfaz cuando se accede a ella
ip address 172.16.1.1 255.255.255.252	Establece por defecto la ipv4
no shutdown	habilita la interfaz
ipv6 address 2001:DB8:ACAD:1::/64	establece por defecto la ipv6
clock rate 128000	establece el reloj de sincronización en 128000
no shutdown	habilita la interfaz
ip route 0.0.0.0 0.0.0.0 s0/1/0	configura una ruta ipv4 predeterminada
ipv6 route ::/0 s0/1/0	configura una ruta ipv6 predeterminada

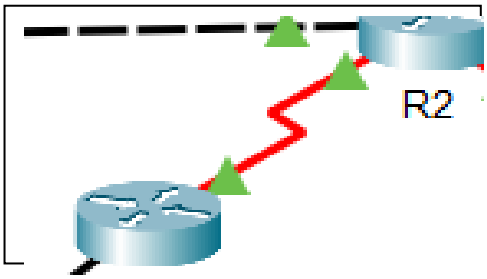
Al realizar estas configuraciones, el resultado del router R1 se despliega de la siguiente manera:

Fig 3. CLI del Router R1. Se aprecia el acceso a la consola y al EXEC privilegiado con contraseña



Fuente: autor

Fig. 4. Conexión entre R1 y R2. Se aprecia la conexión exitosa después de habilitar la interfaz serial



Fuente: autor

Paso 3: Configurar R2

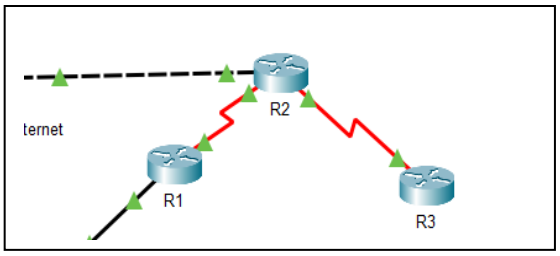
Para la configuración del segundo router se repiten la secuencia de comandos del router r1 hasta el banner (modificando descripciones, banners y nombres de host para adecuarlos a R2), para seguir con las configuraciones de las interfaces:

Tabla 5: Configuraciones de R2

ip http server	Se habilita el servidor http
interface serial 0/1/0	habilita la configuración de la interfaz serial
description “enlace R2”	Añade una descripción
ip address 172.16.1.2 255.255.255.252	establece una ruta ipv4
no shutdown	habilita la interfaz
ipv6 address 2001:DB8:ACAD:1::2/64	establece una ruta ipv6
clock rate 128000	ajusta el reloj de sincronización en 128000
no shutdown	habilita la interfaz
interface serial 0/1/1	habilita la configuración de la interfaz serial
description “enlace R2”	Añade una descripción
ip address 172.16.2.2 255.255.255.252	establece una ruta ipv4
no shutdown	habilita la interfaz
ipv6 address 2001	DB8:ACAD:2::1/64: establece una ruta ipv6
clock rate 128000	ajusta el reloj de sincronización en 128000
no shutdown	habilita la interfaz
interface gigabitEthernet 0/0/0	habilita la configuración de la interfaz gigabitEthernet
ip address 209.165.200.233 255.255.255.248	establece la dirección ipv4
no shutdown	habilita la interfaz
Ipv6 address 2001:DB8:ACAD:A::2/64	establece la dirección ipv6
No shutdown	habilita la interfaz
Interface lookback 0	habilita la configuración de la interfaz loopback (para dirigir el tráfico hacia el mismo)
description “loopback R2”	establece una descripción
ip address 10.10.10.10 255.255.255.0	establece una ruta ipv4
no shutdown	habilita la interfaz

Después de estas configuraciones el router queda igual que R2 en protección, y en al topología se muestra de la siguiente manera:

Fig. 5. Conexiónes desde y hacia R2. Al habilitar los 3 puertos la conexión se establece entre el servidor y ambos routers



Fuente: autor

Paso 4: Configurar R3

Para la configuración del tercer router se repiten la secuencia de comandos del router r1 hasta el banner (modificando descripciones, banners y nombres de host para adecuarlos a R3), para seguir con las configuraciones de las interfaces:
(Nota. Para efectos de evitar redundancia se eliminará la definición innecesaria de comandos ya explicados)

Tabla 6: Configuración de R3

interface serial 0/1/1:	description “enlace R3” ip address 172.16.2.1 255.255.255.252 ipv6 address 2001:DB8:ACAD:2::/64 no shutdown
interface loopback 4	description “loopback 4 R3” ip address 192.168.4.1 255.255.255.0
interface loopback 5	description “loopback 5 R3” ip address 192.168.5.1 255.255.255.0
interface loopback 6	description “loopback 6 R3” ip address 192.168.6.1 255.255.255.0
interface loopback 7	description “loopback 7 R3” ipv6 address 2001:DB8:ACAD:3::1/64

Paso 5: Configurar S1

Para la configuración del primer switch se repiten la secuencia de comandos del router r1 hasta el banner (modificando descripciones, banners y nombres de host para adecuarlos a S1).

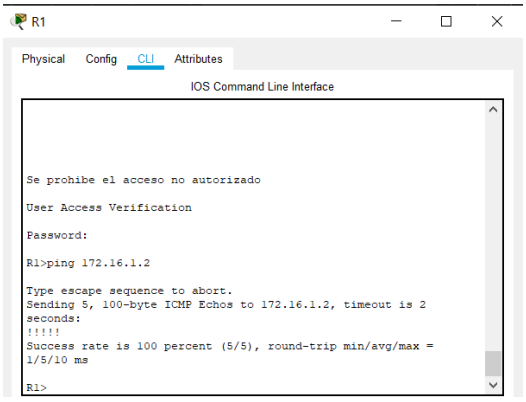
Paso 6: Configurar el S3

Para la configuración del segundo switch se repiten la secuencia de comandos del router r1 hasta el banner (modificando descripciones, banners y nombres de host para adecuarlos a S3).

Paso 7: Verificar la conectividad de la red

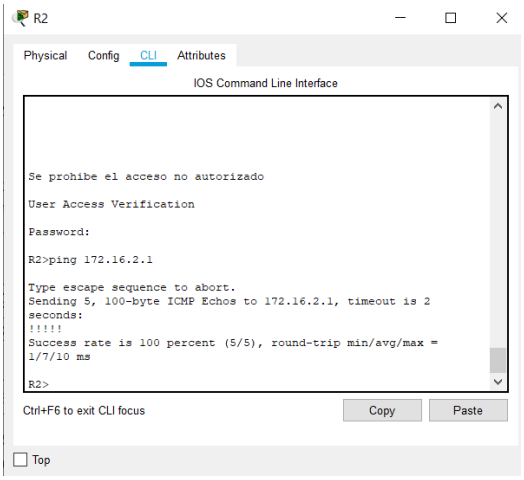
Para asegurar que los dispositivos intermedios y las configuraciones fueron correctamente realizadas se realizará una prueba de ping. Adjunto se encuentran descripciones y resultados del ping:

Fig. 6 Prueba de ping realizada satisfactoriamente



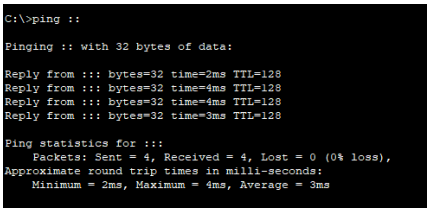
Fuente: autor

Fig. 7 .Prueba de ping realizada satisfactoriamente



Fuente: autor

Fig. 8. Prueba de ping realizada satisfactoriamente



Fuente: autor

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

Para realizar esta parte del trabajo, de forma generalizada se siguieron estos pasos para configurar S1 y S3 (haciendo uso de los datos brindados en la topología lógica):

Tabla 7: Configuración de switch

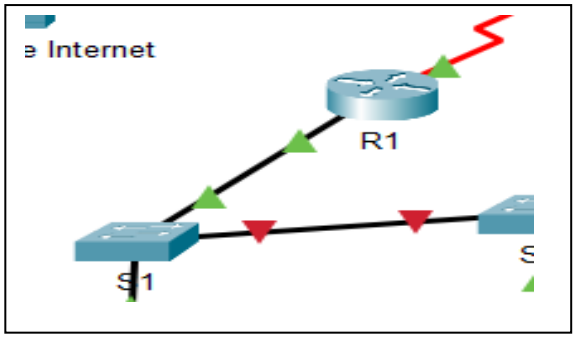
vlan 21	habilita la configuración de la vlan 21
name Contabilidad	asigna un nombre a la vlan
vlan 23	habilita la configuración de la vlan 23
name Ingenieria	asigna un nombre a la vlan
vlan 99	habilita la configuración de la vlan 99
name Administración	asigna un nombre a la vlan
interface vlan 99	habilita la configuración de la vlan
ip address 192.168.99.2 255.255.255.0	Asigna una dirección IP a la vlan
ip default-gateway 192.168.99.1	establece el default Gateway con esa ruta ipv4
interface f0/3	Habilita la configuración de la interfaz
switchport mode trunk	habilita el modo trunk para la conexión
switchport trunk native vlan 1	fuerza el enlace troncal en el puerto f0/3
interface range f0/1,f0/2,f0/4,f0/7-24	habilita la configuraciond e los puertos en esos rangos
interface f0/18	Habilita la configuración de la interfaz
switchport access vlan 23	le brinda acceso a la interface de fastethernet para conectarse a la vlan

Al realizar esta operación el enlace troncal entre los switches queda habilitado

Paso 3: Configurar R1

En R1 se configura las subinterfaces de la itnerfaz de ethernet dispuesta para conectarse al switch, se crean las subinterfaces para la vlan 21, 23 y 99 y se les asigna la primera ruta ip disponible del subdominio, para al final activar la interfaz y habilitar la conexión

Fig. 9.Conexión entre S1 y R1 satisfactoriamente creada



Fuente: autor

Paso 4: Verificar la conectividad de la red

Se realiza una prueba de verificación de la conectividad con las vlan y las subinterfaces recientemente creadas

Tabla 8: Verificación de conectividad

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

Parte 4: Configurar el protocolo de routing dinámico OSPF

En está parte se habilitara el routing dinámico OSPF (Open Shortest Path First) para el encaminamiento jerárquico de peticiones

La configuración tanto en el router 1, router 2, configuración OSPFv3 en router 3 se realizan de la siguiente manera:

Tabla 9: Tabla de configuracion el protocolo de routing dinámico OSPF en router 1 y 2

router ospf 1	habilita el routing dinámico
network 172.16.1.0 0.0.0.255 area 0 network 172.16.1.8 0.0.0.255 area 0 network 192.168.21.0 0.0.0.255 area 0 network 192.168.23.0 0.0.0.255 area 0 network 192.168.99.0 0.0.0.255 area 0	Se asignarán todas las redes conectadas directamente
passive-interface s0/1/0 passive-interface g0/0/0	Todas las interfaces LAN se habilitan como pasivas

La diferencia entre R1 y R2 es que en el router 1 se siguen estas indicaciones, mientras que en el router 2 se habilitan como pasivas la interfaz de lookback con el comando passive-interface loopback0

Tabla 10 OSPFv3 en R3

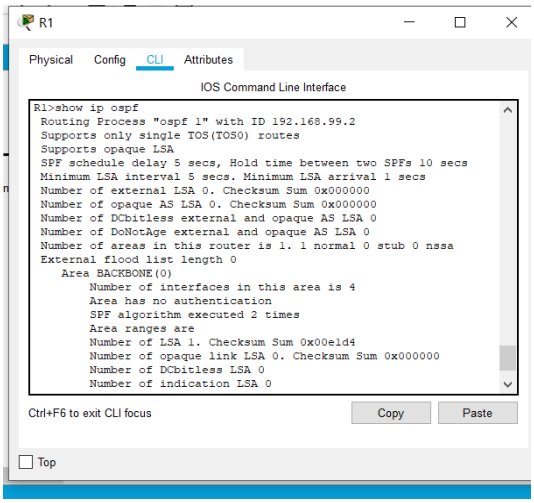
network 172.16.2.0 0.0.0.255 area 0 network 192.168.4.0 0.0.0.255 area 0 network 192.168.5.0 0.0.0.255 area 0 network 192.168.6.0 0.0.0.255 area 0	Se asignas las ipv4 directamente
passive-interface loopback0	Se colocan las interfaces LAN como pasivas

Paso 4: Verificar la información de OSPF

Para comprobar la correcta configuración del routing dinámico se solicita consultar la ID del proceso OSPF, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router (show ip protocols), solo las rutas OSPF (show ip ospf)

y la sección de OSPF de la configuración en ejecución (show ip ospf interface)

Fig. 10.Resultado de show ip ospf en la CLI del router 1



Fuente: autor

Parte 5: Implementar DHCP y NAT para IPv4

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

En esta parte de la configuración al router 1 se le reservan las primeras 20 direcciones ip en la vilan 21 y 23, y luego se crea un pool (agrupación de direcciones asignables) de DHCP para la vlan 21 y 23 con los siguientes comandos:

Tabla 11: Configuración de R1 como servidor DHCP para las VLAN 21 y 23

ip dhcp excluded-address 192.168.21.1 192.168.21.20	Reserva las 20 direcciones para la vlan 21
ip dhcp excluded-address 192.168.23.1 192.168.23.20	reserva las direcciones para la vlan23
ip dhcp pool ACCT network 192.168.21.0 255.255.255.0: establece network dns-server 10.10.10.10: establece dns domain-name ccna-sa.com: establece dominio default-router 192.168.21.1: establece router default	crea la pool de DHCP con el nombre ACCT
ip dhcp pool ENGNR network 192.168.23.0 255.255.255.0 dns-server 10.10.10.10 domain-name ccna-sa.com default-router 192.168.23.1	crea la pool de DHCP con el nombre ENGNR

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

En este paso se configura la NAT (Network Address Translation o traductor de direcciones de red) en R2. Se crea una base de datos local con cuenta de usuario:

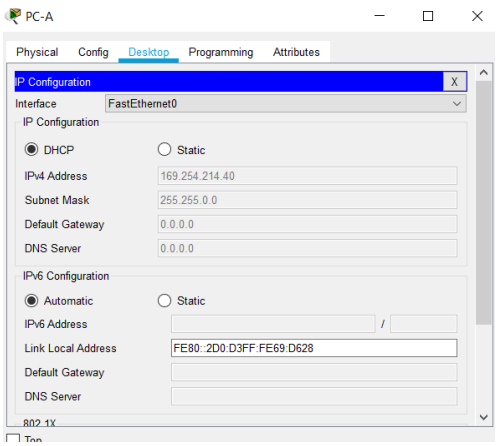
Tabla 12: Configuración de NAT estática y dinámica en el R2

user webuser privilege 15 secret cisco12345	Se crea una base de datos local con una cuenta de usuario
ip http server	Se habilita el servicio http
ip http authentication local	Se configura el servidor http para usar la base de datos local como autenticación
ip nat inside source static 10.10.10.10 209.165.200.237	Se asignan las interfaces internas y externas de la NAT
access-list 1 permit 192.168.21.0 0.0.0.255 access-list 1 permit 192.168.23.0 0.0.0.255 access-list 1 permit 192.168.4.1 0.0.0.255 access-list 1 permit 192.168.5.1 0.0.0.255 access-list 1 permit 192.168.6.1 0.0.0.255	Configura la NAT dinámica dentro de una ACL (Access Control List)
ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248 ip nat inside source list 1 pool INTERNET	Se define el pool de direcciones públicas utilizables

Paso 3: Verificar el protocolo DHCP y la NAT estática

Para verificar la correcta configuración del DHCP y la NAT en la topología se verifica que PC-A haya adquirido la información IP del servidor DHCP y se pide que se acceda al servidor web con el nombre de usuario webuser y la contraseña cisco12345

Fig. 11.Configuración IP del PC-A



Fuente: autor

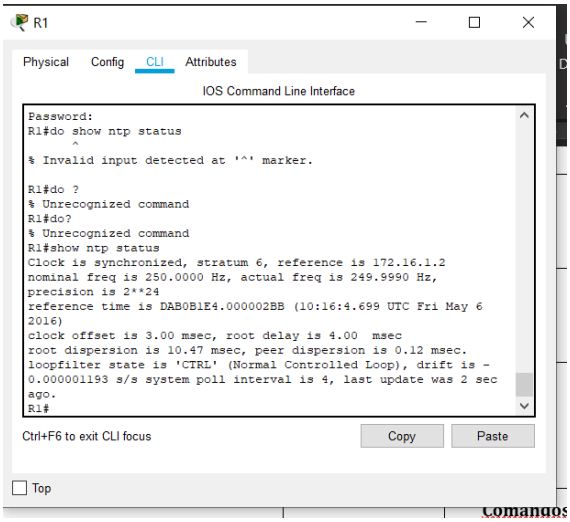
Parte 6: Configurar NTP

En esta parte se configura el NTP de routers (Network Time Protocol). Se asignan tareas como ajustar fecha y hora del router r2, configurar R2 como un maestro NTP (servidor que controlará la sincronización del tiempo), configurar R1 como un cliente NTP, brindarle actualizaciones automáticas a R1 del NTP y verificar la conexión de NTP en R1

Tabla 13: Configuración de NTP

clock set 9:00:00 5 may 2016	Ajusta la fecha y hora en R2.
ntp master 5	Configura R2 como un maestro NTP
ntp server 172.16.1.2	Configura R1 como un cliente NTP
ntp update-calendar	Configura R1 para actualizaciones de calendario periódicas con hora NTP

Fig. 12.Verificación de la sincronización NTP en R1



Fuente: autor

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

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

Para este paso se configuran y verifican las listas de control de acceso ACL. Se establecen configuraciones para una lista de acceso con nombre para que solamente R1 establezca conexión con R2:

Tabla 14: Restringir el acceso a las líneas VTY en R2

ip access-list standard ADMIN-MGT permit host 172.16.1.2	Configura una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2 (Se aplica la ACL en todas las interfaces vty)
line vty 0 4 access-class ADMIN-MGT in	Aplicar la ACL con nombre a las líneas VTY (Además se permitió el acceso por Telnet a las líneas de vty y se verificó que la ACL funcione como se espera)

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

En este ultimo paso se solicitan cosas cómo:

Tabla 15: Comandos que muestran determinadas configuraciones en Router

show access-list	Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció
clear Access-list counters	Restablecer los contadores de una lista de acceso
show ip interface	mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica
show ip nat translations	mostrar las traducciones NAT
clear ip nat translation	eliminar las traducciones de NAT dinámicas

III. CONCLUSIÓN

Con el desarrollo de la anterior practica y laboratorio, se puede evidenciar los conocimientos necesarios e implementados en el área de IPv6 donde este pretende realizarlos bloquear necesarios para que si ingreso no sea fácil para cualquier usuario solo el asignado.

Se logra aprender y permitir el direccionamiento mediante interfaces específicas en el router que estemos trabajando conectividad IPv4 e IPv6, seguridad de switches, routing entre VLAN, el protocolo de routing dinámico OSPF, el protocolo de configuración de hosts dinámicos (DHCP), la traducción de direcciones de red dinámicas y estáticas (NAT), listas de control de acceso (ACL) y el protocolo de tiempo de red (NTP) servidor/cliente. Durante la evaluación, probará y registrará la red mediante los comandos comunes de CLI.

REFERENCES

III. REFERENCIAS

[1.] Cisco, «Información sobre los modos de loopback en routers de Cisco,» 21 November 2007. [En línea]. Available: https://www.cisco.com/c/es_mx/support/docs/asynchronous-transfer-mode-atm/permanent-virtual-circuits-pvc-switched-virtual-circuits-svc/6337-atmloopback.html. [Último acceso: November 20]

[2.] Cisco Systems, «CCNP 1: Advanced IP Addressing Management,» Cisco Press, 27 August 2004. [En línea]. Available:

https://www.ciscopress.com/articles/article.asp?p=330807&seqNum=8. [Último acceso: November 2020].

[3.] P. Murphy, «The OSPF Not-So-Stubby Area (NSSA) Option,» January 2003. [En línea]. Available: https://tools.ietf.org/html/rfc3101.html. [Último acceso: November 2020].

[4.] Cisco, «The OSPF Not-So-Stubby Area (NSSA) Option,» 12 October 2005. [En línea]. Available: https://www.cisco.com/c/en/us/support/docs/ip/dynamic-address-allocation-resolution/22920-dhcp-ser.html. [Último acceso: November 2020].

[5.] Cisco, «Preguntas frecuentes sobre la traducción de direcciones de red (NAT),» 18 November 2020. [En línea]. Available: https://www.cisco.com/c/es_mx/support/docs/ip/network-address-translation-nat/26704-nat-faq-00.html. [Último acceso: November 2020].

[6.] R. Shirey, « Internet Security Glossary, Version 2,» August 2007. [En línea]. Available: https://tools.ietf.org/html/rfc4949. [Último acceso: November 2020].

[7.] Linux Foundation, «Securing Network Time,» 27 September 2017. [En línea]. Available: https://web.archive.org/web/20171028123642/https://www.coreinfrastructure.org/news/blogs/2017/09/securing-network-time. [Último acceso: 2020 November].

[8.] G. B. C. J. L. V. S. Y. P. S. V. Mauricio Olaya Tellez, «Principios de enrutamiento y conmutación,» 14 December 2017. [En línea]. Available: https://repository.unad.edu.co/handle/10596/14997. [Último acceso: November 2020].

[9.] Cisco, «Guía de diseño de OSPF,» 10 August 2005. [En línea]. Available: https://www.cisco.com/c/es_mx/support/docs/ip/open-shortest-path-first-ospf/7039-1.html. [Último acceso: November 2020].

[10.] J. A. B. Bravo, «CONECTIVIDADY CONFIGURACIÓN DINÁMICA DE DIRECCIONES NAT, ACLY DHCP.,» 2018. [En línea]. Available: https://repository.unad.edu.co/bitstream/handle/10596/18989/1088972655.pdf?sequence=1&isAllowed=y. [Último acceso: November 2020].

Biografía

Cortez Martinez Harol Heyder: nació en El Tablón de Gómez Nariño, en el año 1984, estudió tecnología en Promoción de la Salud en la Universidad de Nariño de la Ciudad de Pasto (N), en la actualidad estudiante de Ingeniería de Sistemas en la Universidad Nacional Abierta y a Distancia UNAD.