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

DUBER ANDRÉS ESPAÑOL RODRÍGUEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI
INGENIERÍA DE SISTEMAS
MONTERÍA
2020

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

DUBER ANDRÉS ESPAÑOL RODRÍGUEZ

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

DIRECTOR:
DIEGO EDINSON RAMÍREZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI
INGENIERÍA DE SISTEMAS
MONTERÍA
2020

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____

_____

_____
Firma del Presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

Montería, 26 de noviembre de 2020

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

BANNER MOTD: Mensaje de aviso del día que va en medio de dos delimitadores.

DHCP (Dynamic Host Configuration Protocol): Protocolo de configuración dinámica de host, permite asignar direcciones de forma automática a cada dispositivo.

ENLACE TRONCAL: Enlace que se configura en uno o varios puertos de un switch, que permite el trafico der varias VLANs configuradas. Pertenece al estándar IEEE 802.1Q

LOOPBACK: Interfaz de red virtual que prueba el funcionamiento de transmisión de datos y conectividad.

TOPOLOGÍA DE RED: Mapa físico o lógico de los componentes de una red.

VLAN (Virtual LAN): Red de área local de carácter virtual, como método para la creación de redes lógicas dentro de una red fisca.

RESUMEN

La prueba de habilidades prácticas, hace parte del diplomado de profundización Cisco CCNP, el cual evalúa unos criterios de aprendizaje a través de unos módulos educativos, orientado al diagnóstico y solución de problemas, que se puedan presentar en una red. La metodología de trabajo práctico, está compuesto por dos escenarios diseñados y construidos, en la herramienta que ofrece Cisco System, Packet Tracer, para las configuraciones básicas de seguridad, arquitectura de conexión, enrutamiento y de comunicación, para las redes conmutadas. Las redes agrupan distintos dispositivos como router, switches, PC y servidores, conectados por medio de cable de cobre directo, cable de cobre cruzado y cable serial DCE, según la topología y que dentro de la configuración básica admita conectividad IPv4 e IPv6, entre VLAN, DHCP, OSPF Etherchannel y port-security.

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

ABSTRACT

The practical skills test is part of the Cisco CCNP in-depth diploma, which assesses learning criteria through educational modules, aimed at diagnosing and solving problems, which can be presented on a network. The practical work methodology is composed of two scenarios designed and built, in the tool offered by Cisco System, Packet Tracer, for basic security configurations, connection architecture, routing and communication, for switched networks. The networks group different devices such as router, switches, PCs and servers, connected by means of direct copper cable, crossed copper cable and DCE serial cable, according to the topology and that within the basic configuration supports IPv4 and IPv6 connectivity, between VLANs, DHCP, OSPF Etherchannel and port-security.

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

INTRODUCCIÓN

La metodología del documento presenta dos escenarios, donde se desarrolla las pruebas de habilidades prácticas CCNA, aplicando conocimientos y habilidades adquiridas académicamente en el transcurso del diplomado de profundización de CISCO, entre los temas se encuentran, configuración básica de dispositivos, manejo de direccionamiento IPv4 e IPv6, protocolos de conmutación mejorados, como es el caso de VLAN, protocolo de enlace troncal, protocolos de routing dinámicos OSPF, protocolo de tiempo de red, configuración de servidores DHCP, Network Address Translation (NAT), listas de control de acceso, encapsulamiento por 802.1q, entre otros.

Es importante establecer niveles de seguridad básica de protección en los dispositivos de la red, ya sea un router o un switch, aún más, cuando alguien intenta ingresar sin permiso o ante un posible ataque; entre las medidas se encuentran, el servicio de encriptación de contraseñas, contraseñas cifradas para el modo EXEC privilegiado, contraseña de consola, deshabilitar puertos no utilizados, y demás que sean necesarias, con el fin de proteger la integridad de la información.

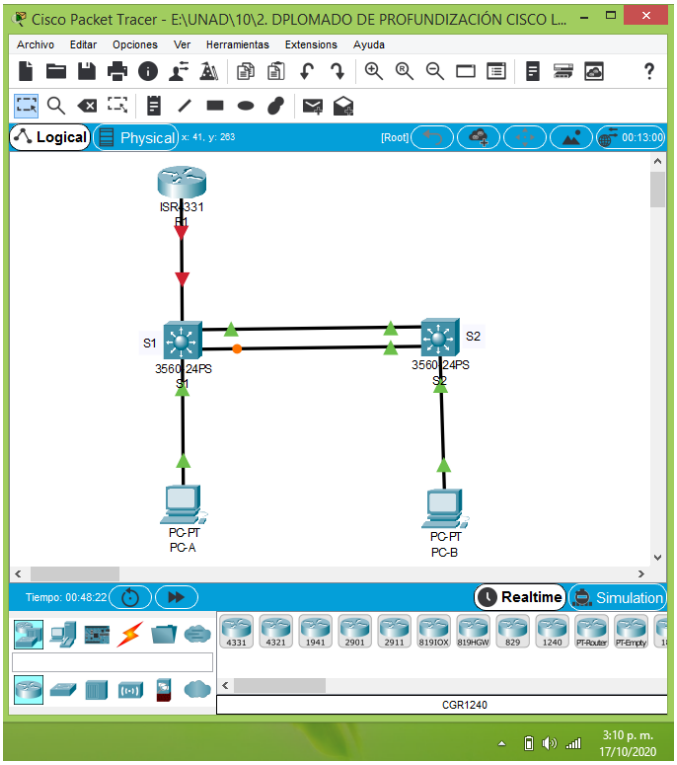
Dentro de las configuraciones básicas de los dispositivos y en caminados en las buenas prácticas de la gerencia de redes, es importante la creación de usuarios administrativos locales y remotos, en donde las conexiones del protocolo SSH son totalmente cifradas y la información viaja a través de un canal seguro, generando una clave criptográfica RSA con un módulo de 1024 bits, por otro lado está el protocolo Telnet que no ofrece ningún nivel de seguridad y permite ver a terceros toda la información que se escribe a lo largo de la sesión.

DESARROLLO

1. Escenario 1

Topología

Figura 1. Topología escenario 1



Fuente: Autor

En la topología del escenario 1 se utilizó un router Cisco ISR 4331, 2 (dos) switches de red de Cisco 3560 y 2 (dos) PC, las conexiones se llevaron a cabo por medio de cable de cobre directo y así poder configurar una red pequeña, donde se pueda administrar de forma segura y se admita la conectividad IPv4 e IPv6.

Tabla de VLAN

Tabla 1. Tabla de Vlan escenario 1

VLAN	Nombre de la VLAN
2	Bikes

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

Tabla de asignación de direcciones

Tabla 2. Tabla de asignación de direcciones escenario 1

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

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

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

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

Inicialmente para la configuración de la red, es importante que los dispositivos que se vayan a utilizar en la topología del escenario 1, no cuenten con información de configuración inicial, ya que se podrían presentar inconvenientes durante el proceso, por tal razón es importante, inicializar y volver a cargar el router y los switches, con los comandos que se pueden observar a continuación.

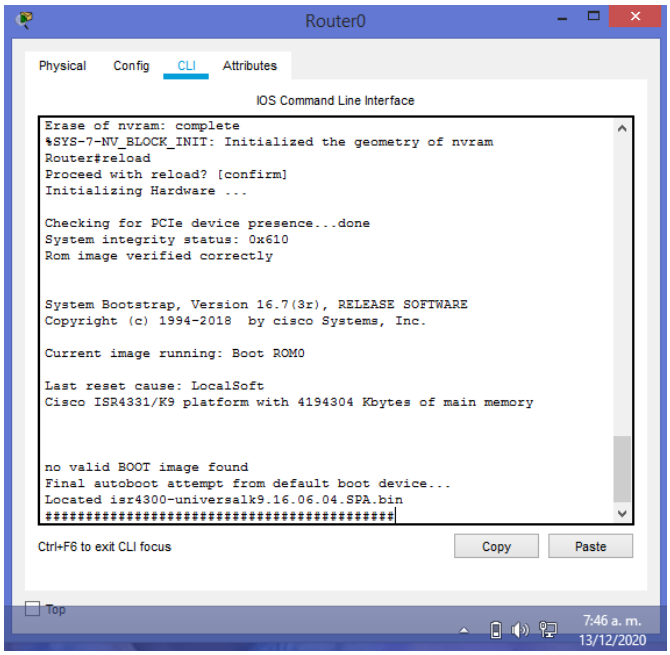
Tabla 3. Inicialización y recarga del router y el switch escenario 1

Tarea	Comando de IOS
Ingresar modo privilegiado del router	Router>enable
Eliminar configuración inicial	Router#erase startup-config
Reiniciar manualmente el router	Router#reload
Ingresar modo privilegiado del switch	Switch>enable
Verificar datos de VLAN en la memoria	Switch#show flash
Eliminar configuración anterior. Confirmar la acción a realizar.	Switch#erase startup-config Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
Reiniciar manualmente el switch	Switch#reload

Se ingresa al modo EXEC privilegiado del router *R1* y se escribe el comando *erase startup-config*, el cual elimina las configuraciones iniciales de la memoria NVRAM, aparecerá un mensaje de aviso, que informara si se desea borrar todos los archivos de configuración del sistema, la respuesta es sí, entonces se confirma con la tecla ENTER, luego se aplica el comando *reload*, el cual reinicia manualmente el router, pedirá

confirmar la acción a realizar, lo cual se lleva a cabo presionando la tecla ENTER, el proceso tardara unos cuantos segundos, al finalizar, va a aparecer un diálogo de configuración del sistema, escribimos las letras *no.*

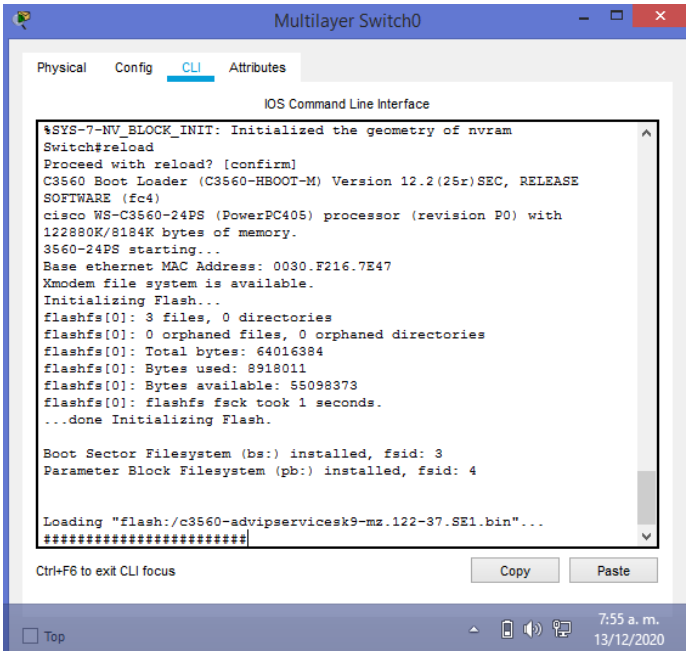
Figura 2. Comando reload en router R1 escenario 1



Fuente: Autor

Una vez terminado lo anterior con el router, se identifican los switches de nombre *S1* y *S2*, posteriormente se ingresa al modo privilegiado del dispositivo, por medio del comando *show flash* se verifica que no se encuentren almacenados datos de VLAN en la memoria, sin embargo, se escribe el comando *erase startup-config*, que para confirmar el proceso a ejecutar se presiona ENTER, ahora se aplica un reiniciado manual.

Figura 3. Comando reload en switch S1 escenario 1



Fuente: Autor

Con lo anterior se da por terminado las acciones de borrado de las configuraciones del router y los dos switches, siendo cargados nuevamente.

El siguiente paso es configurar la plantilla SDM y optimizar la compatibilidad para que pueda admitir IPv4 e IPv6 los dos switches de cisco 3560 ya que no soporta capacidades IPv6. Se ingresa al modo privilegiado, de configuración global y se ingresa el comando *sdm prefer dual-ipv4-and-ipv6 default*, la palabra clave default mantiene un equilibrio de las funciones de capa 2 y capa 3; al finalizar aparece un mensaje que nos informa que la configuración del sistema ha sido modificada, y pregunta si desea guardar los cambios realizados, la respuesta es sí (yes), seguido presionar la tecla ENTER.

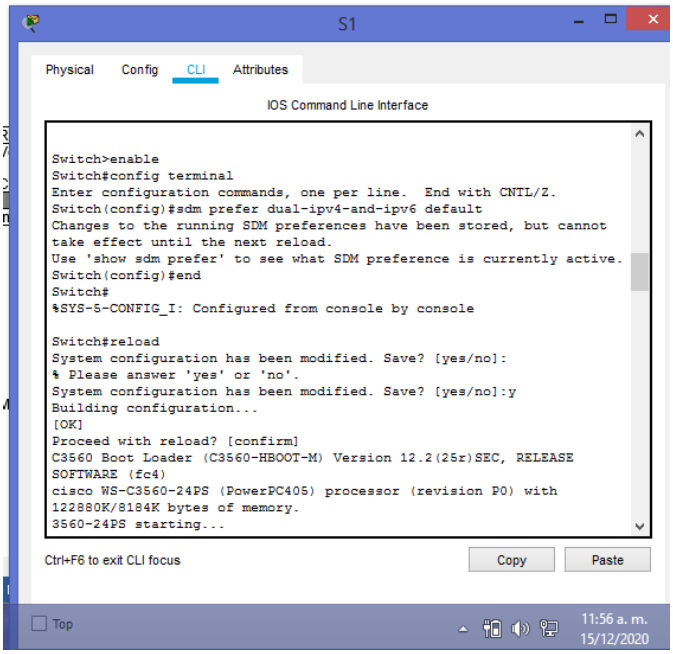
Tabla 4. Comandos para configuración de la plantilla SDM en switch S1 y S2

Tarea	Comando de IOS
Ingresar modo privilegiado del switch	Switch>enable
Ingresar al modo de configuración global	Switch#config terminal
Plantilla que admite un equilibrio de funciones de Ipv4 e IPv6	Switch(config)#sdm prefer dual-ipv4-and-ipv6 default
Regresar al modo privilegiado	Switch(config)#end

Volver a cargar el sistema. Confirmar la acción a realizar.	Switch#reload System configuration has been modified. Save? [yes/no]:

Una vez adelantadas las tareas descritas en la *tabla 4*, se puede evidenciar las configuraciones realizadas en el switch S1 en la siguiente figura.

Figura 4. Configuración de la plantilla SDM en switch S1



Fuente: Autor

Para conocer lo que se ha hecho hasta el momento, se ingresa nuevamente al Switch S1 y S2 en modo privilegiado y se ingresa el comando *show sdm prefer*.

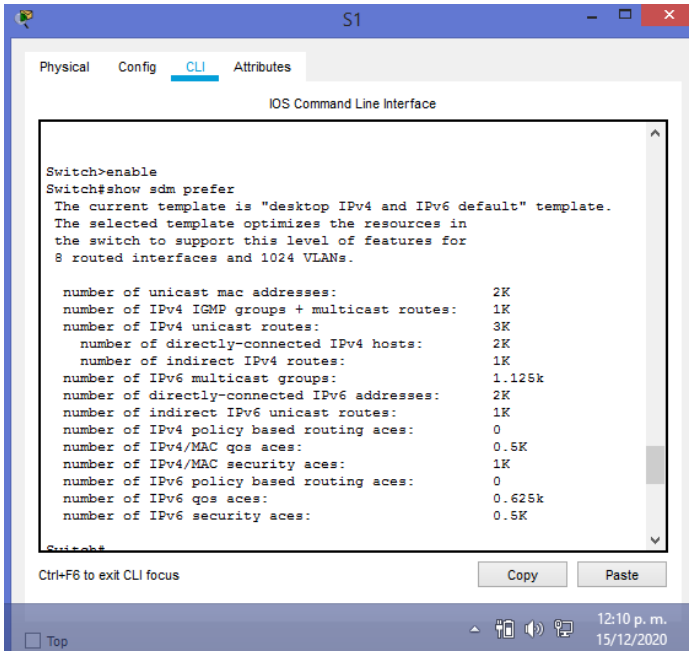
Tabla 5. Comando show sdm prefer, switch S1

Tarea	Comando de IOS
Ingresar modo privilegiado del switch	Switch>enable
Mostrar información de la plantilla en uso	Switch #show sdm prefer The current template is "desktop IPv4 and IPv6 default" template. The selected template optimizes the resources in the switch to support this level of features for 8 routed interfaces and 1024 VLANs. number of unicast mac addresses: 2K

	number of IPv4 IGMP groups + multicast routes: 1K number of IPv4 unicast routes: 3K number of directly-connected IPv4 hosts: 2K number of indirect IPv4 routes: 1K number of IPv6 multicast groups: 1.125k number of directly-connected IPv6 addresses: 2K number of indirect IPv6 unicast routes: 1K number of IPv4 policy based routing aces: 0 number of IPv4/MAC qos aces: 0.5K number of IPv4/MAC security aces: 1K number of IPv6 policy based routing aces: 0 number of IPv6 qos aces: 0.625k number of IPv6 security aces: 0.5K

Lo anterior aplica, con el fin de verificar la actualización actual realizada y ver la plantilla activa, como se observa en la *figura 5*.

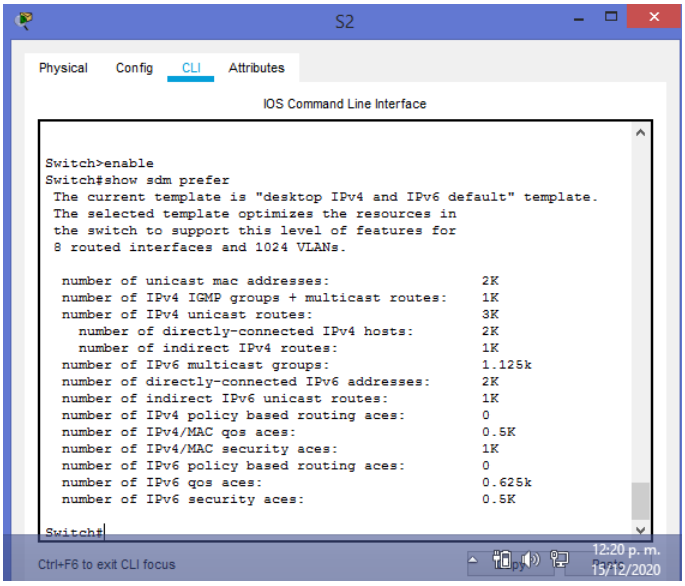
Figura 5. Utilización del comando show sdm prefer en S1



Fuente: Autor

En la *figura 6* se puede ver la plantilla SDM luego de ejecutar el comando *show sdm prefer* en el switch S2 en donde está habilitado el direccionamiento IPv6

Figura 6. Utilización del comando show sdm prefer en S2



Fuente: Autor

1.1.2 Paso 2: Configurar R1

Se ingresa al modo EXEC privilegiado del router, se inhabilita la búsqueda DNS por medio del comando *no ip domain-lookup* y así evitar que intente traducir comandos mal ingresados. Con el fin de diferenciar cada dispositivo en la topología, es importante asignar un nombre a cada uno de ellos, para ello se utiliza el comando *hostname*, seguido de *R1* nombre para el actual dispositivo, ahora es necesario asignar el nombre de dominio ccna-lab.com con el uso del comando *ip domain-name*.

Teniendo en cuenta la importancia de la seguridad del dispositivo, es necesario crear una contraseña de acceso al modo privilegiado con el comando *enable secret* y otra de acceso por consola con *password* habilitando con *login* el inicio de sesión. Por otro lado, se crea en la base de datos local, un usuario y una contraseña, que serán utilizadas al momento de conectarse al router a través de SSH, pero que no permita conexiones Telnet, para ello se utiliza el comando *transport input ssh*, al finalizar es necesario encriptar todas las contraseñas que se han creado y las futuras, por medio del comando *service password-encryption*. Cuando una persona intenta acceder al router es importante crear un banner por medio del comando *banner motd*, un mensaje que informe, que '*El acceso no autorizado está estrictamente prohibido y perseguido con todo el peso de la ley Colombiana*'.

Es hora de configurar la interfaz del router *G0/0/1* y sus subinterfaces *G0/0/1.2*, *G0/0/1.3*, *G0/0/1.4* y *G0/0/1.6* donde se les asignará una descripción, una dirección IPv4 e IPv6 y un enlace local IPv6 para el buen funcionamiento del protocolo, al finalizar se ingresa el comando *no shutdown*, el cual habilita las interfaces. De igual manera, se realiza la configuración de la interface lógica de R1 interface *loopback0*, asegurando que la se encuentre siempre disponible, al terminar se ejecuta el comando *exit*, por otro lado, escribiendo el comando *crypto key generate rsa* se genera una clave criptográfica RSA con un módulo de 1024 bits.

Las tareas de configuración para R1 son las siguientes:

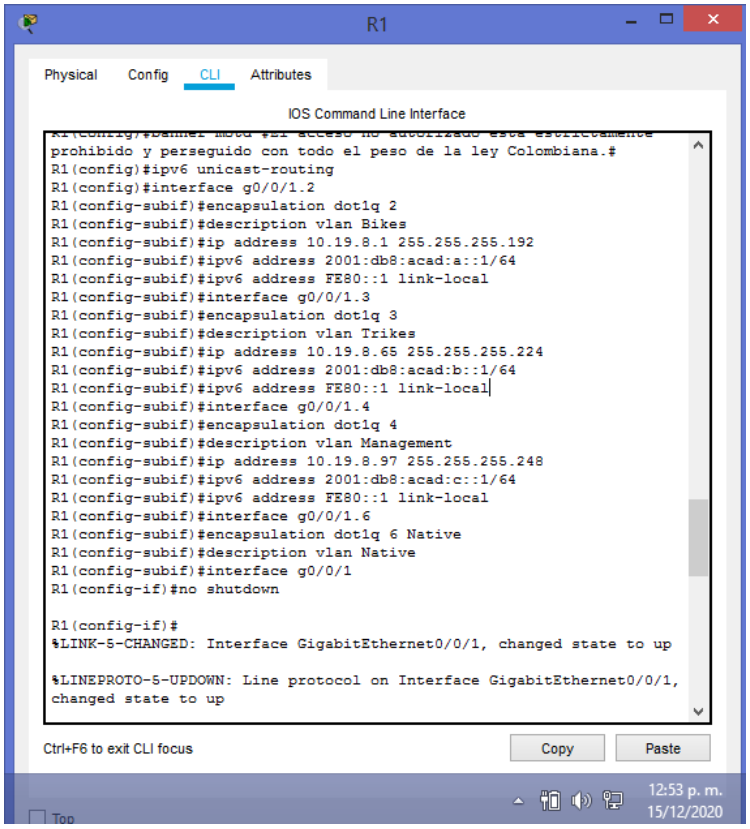
Tabla 6. Configuración router R1 escenario 1

Tarea	Comando de IOS
Inhabilitar la búsqueda DNS	Router(config)# no ip domain-lookup
Modificar nombre del router	Router(config)#hostname R1
Nombre de dominio	R1(config)# ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	R1(config)# enable secret ciscoenpass
Contraseña de acceso a la consola	R1(config)#line console 0 R1(config-line)# password ciscoconpass R1(config-line)#login R1(config-line)#exit
Establecer la longitud mínima para las contraseñas	R1(config)# security passwords min-length 10
Crear un usuario administrativo en la base de datos local	R1(config)# username admin privilege 1 secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	R1(config)# line vty 0 4 R1(config-line)# login local
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 #El acceso no autorizado esta estrictamente prohibido y perseguido con todo el peso de la ley Colombiana.#
Habilitar el routing IPv6	R1(config)# ipv6 unicast-routing

Tarea	Comando de IOS
Configurar interfaz G0/0/1 y subinterfaces	R1(config)#interface g0/0/1.2 R1(config-subif)#encapsulation dot1q 2 R1(config-subif)#description vlan 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)# interface g0/0/1.3 R1(config-subif)#encapsulation dot1q 3 R1(config-subif)#description vlan 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)# interface g0/0/1.4 R1(config-subif)#encapsulation dot1q 4 R1(config-subif)#description vlan 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)# interface g0/0/1.6 R1(config-subif)#encapsulation dot1q 6 Native R1(config-subif)#description vlan Native R1(config-subif)#interface g0/0/1 R1(config-if)#no shutdown
Configure el Loopback0 interface	R1(config-if)# interface loopback0 R1(config-if)#ip address 209.165.201.1 255.255.255.224 R1(config-if)#ipv6 address 2001:db8:acad:209::1/64 R1(config-if)#ipv6 address FE80::1 link-local R1(config-if)#description Internet R1(config-if)#exit
Generar una clave de cifrado RSA	R1(config)# crypto key generate rsa How many bits in the modulus [512]: 1024

En la *figura 7* se puede ver la configuración de los parámetros básicos del router R1, descritos en la *tabla 6.*

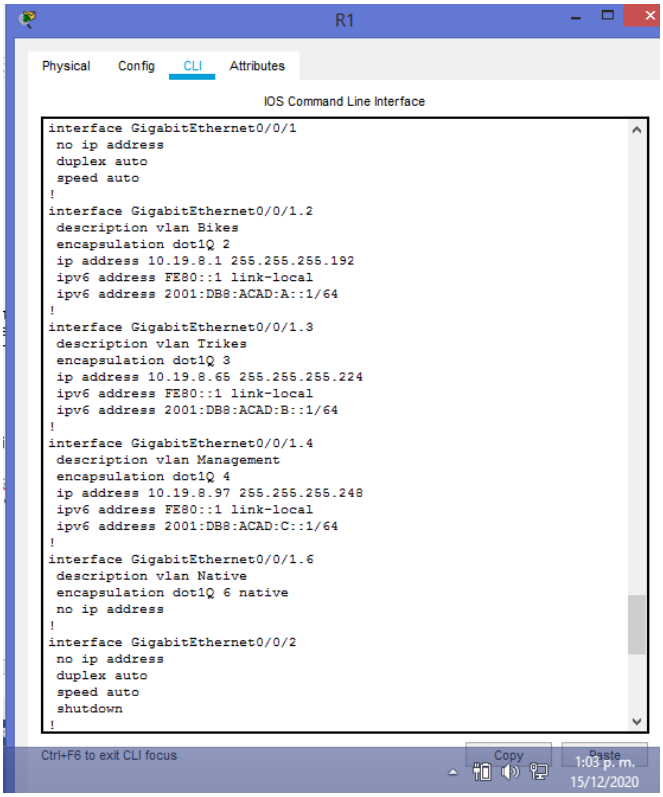
Figura 7. Configuración parámetros básicos del Router R1



Fuente: Autor

Con el fin de verificar los comandos IOS ejecutados en el router R1 dentro las tareas de la *tabla 6*, se ejecuta el comando show running-config y así comparar la información de la memoria en ejecución, tal como se puede ver en la *figura 8*.

Figura 8. Comando show running-config en router R1



Fuente: Autor

1.1.3 Paso 3: Configurar S1 Y S2

Las tareas de configuración para S1 incluyen las siguientes:

Tabla 7. Configuración del switch S1 escenario 1

Tarea	Comando de IOS
Desactivar la búsqueda DNS.	Switch(config)#no ip domain lookup
Nombre del switch	Switch(config)#hostname S1
Nombre de dominio	S1(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	S1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	S1(config)#line console 0 S1(config-line)#password ciscoconpass S1(config-line)#login S1(config-line)#exit

Tarea	Comando de IOS
Crear un usuario administrativo en la base de datos local	S1(config)#username admin secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	S1(config)#line vty 0 15 S1(config-line)#login local
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S1(config-line)#transport input ssh S1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption
Configurar un MOTD Banner	S1 (config)# banner motd #El acceso no autorizado está estrictamente prohibido y perseguido con todo el peso de la ley Colombiana.#
Generar una clave de cifrado RSA	S1(config)#crypto key generate rsa How many bits in the modulus [512]: 1024
Configurar la interfaz de administración (SVI)	S1(config)#interface 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 vlan Management S1(config-if)#no shutdown S1(config-if)#exit
Configuración del gateway predeterminado	S1(config)#ip default-gateway 10.19.8.97

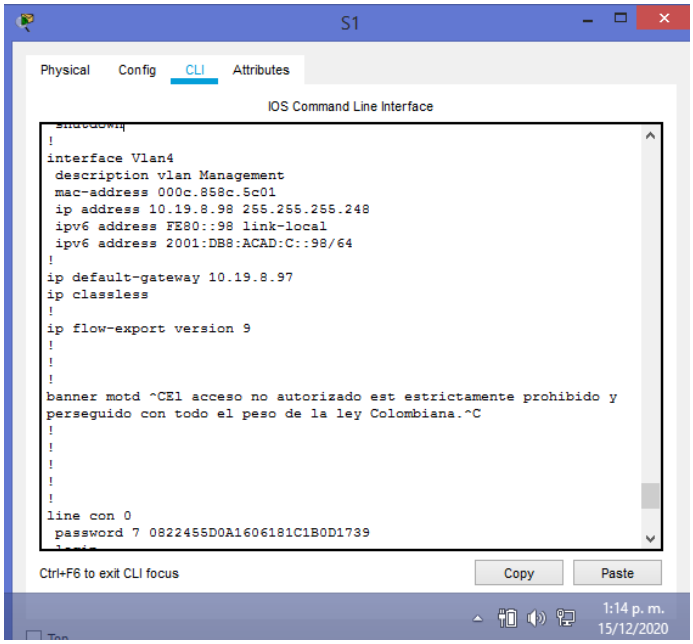
Se ingresa al switch en modo EXEC privilegiado, se inhabilita la búsqueda DNS por medio del comando *no ip domain-lookup*, se asigna un nombre por medio del comando *hostname*, seguido de *S1* nombre para el actual dispositivo, ahora es necesario asignar el nombre de dominio *ccna-lab.com* con el uso del comando *ip domain-name*.

Continuando con la seguridad de los dispositivos de la topología, se realiza la asignación de contraseñas modo privilegiado con el comando *enable secret* y otra de acceso por consola con *password* habilitando con *login* el inicio de sesión. Al igual que en paso anterior, se crea en la base de datos local, un usuario y una contraseña, que serán utilizadas al momento de conectarse al switch a través de SSH, pero que no permita conexiones Telnet, para ello se utiliza el comando *transport input ssh*, además se realiza una encriptación de las contraseñas actuales.

Cuando una persona intente acceder al switch, leva a aparecer un mensaje que informa, que '*El acceso no autorizado está estrictamente prohibido y perseguido con todo el peso de la ley Colombiana*'. Ahora se configura la interfaz de administración por medio del comando *interface*, una dirección IPv4 e IPv6 y una dirección de enlace local IPv6, luego se aplica el comando *no shutdown*, el cual habilita las interfaces.

Un terminal para que se comunique a través de la red, además de la dirección IP correcta, necesita la dirección gateway predeterminada, la cual es configurada con el uso del comando *ip default-gateway* seguido de la dirección IP *10.19.8.97*. Con el fin de verificar la configuración realizada en el switch S1 se ejecuta el comando show running-config visible en la *figura 9*.

Figura 9. Comando show running-config en switch S1



Fuente: Autor

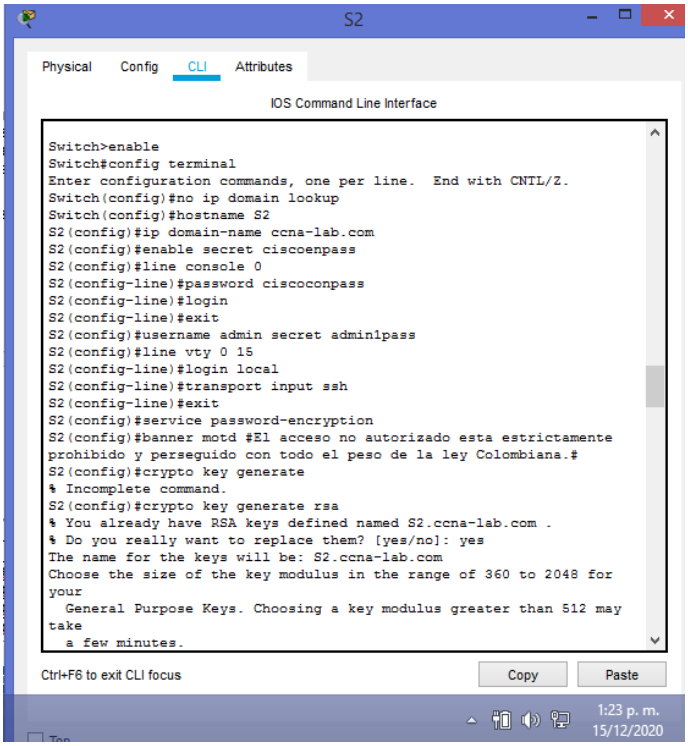
Las tareas de configuración para el switch S2 incluyen las siguientes:

Tabla 8. Configuración del switch S2 escenario 1

Tarea	Comando de IOS
Desactivar la búsqueda DNS.	Switch(config)#no ip domain lookup
Nombre del switch	Switch(config)#hostname S2

Tarea	Comando de IOS
Nombre de dominio	S2(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	S2(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	S2(config)#line console 0 S2(config-line)#password ciscoconpass S2(config-line)#login S2(config-line)#exit
Crear un usuario administrativo en la base de datos local	S2(config)#username admin secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	S2(config)#line vty 0 15 S2(config-line)#login local
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S2(config-line)#transport input ssh S2(config-line)#exit
Cifrar las contraseñas de texto no cifrado	S2(config)#service password-encryption
Configurar un MOTD Banner	S2 (config)# banner motd #El acceso no autorizado esta estrictamente prohibido y perseguido con todo el peso de la ley Colombiana.#
Generar una clave de cifrado RSA	S2(config)#crypto key generate rsa How many bits in the modulus [512]: 1024
Configurar la interfaz de administración (SVI)	S2(config)#interface vlan 4 S2(config-if)#ip address 10.19.8.99 255.255.255.248 S2(config-if)#ipv6 address 2001:db8:acad:c::99/64 S2(config-if)#ipv6 address FE80::99 link-local S2(config-if)#description vlan Management S2(config-if)#no shutdown S2(config-if)#exit
Configuración del gateway predeterminado	S2(config)#ip default-gateway 10.19.8.97

Figura 10. Configuración del switch S2 escenario 1



Fuente: Autor

Para la configuración del switch de nombre S2, se llevan a cabo los mismos pasos descritos en el *paso 3*, con la diferencia que en la interfaz de administración (SVI) correspondiente a la VLAN 4 Management, la dirección IPv4 e IPv6 y la dirección local de enlace cambia, como se puede observar en la *tabla 8* y la *figura 10*.

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

1.2.1 Paso 4: Configurar S1

Las tareas de configuración para switch S1 incluyen las siguientes:

Tabla 9. Configuración infraestructura de red switch S1

Tarea	Comando de IOS
Crear VLAN VLAN 2, nombre Bikes VLAN 3, nombre Trikes VLAN 4, name Management VLAN 5, nombre Parking VLAN 6, nombre Native	S1(config)#vlan 2 S1(config-vlan)#name Bikes S1(config-vlan)#exit S1(config)#vlan 3 S1(config-vlan)#name Trikes S1(config-vlan)#exit S1(config)#vlan 4 S1(config-vlan)#name Management S1(config-vlan)#exit S1(config)#vlan 5 S1(config-vlan)#name Parking S1(config-vlan)#exit S1(config)#vlan 6 S1(config-vlan)#name Native S1(config-vlan)#exit
Crear troncos 802.1Q que utilicen la VLAN 6 nativa Interfaces F0/1, F0/2 y F0/5	S1(config)#interface range fa0/1-2 S1(config-if-range)#switchport trunk encapsulation dot1q S1(config-if-range)#switchport mode trunk S1(config-if-range)#switchport trunk native vlan 6 S1(config-if-range)#exit S1(config)#interface fa0/5 S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 6 S1(config-if-range)#shutdown
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	S1(config)#interface range fa0/1-2 S1(config-if-range)#channel-group 1 mode active S1(config-if-range)#interface 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)#interface fa0/6 S1(config-if)#switchport mode acces S1(config-if)#switchport acces vlan 2
Configurar la seguridad del puerto en los puertos de acceso Permitir 3 direcciones MAC	S1(config-if)#switchport port-security maximum 3

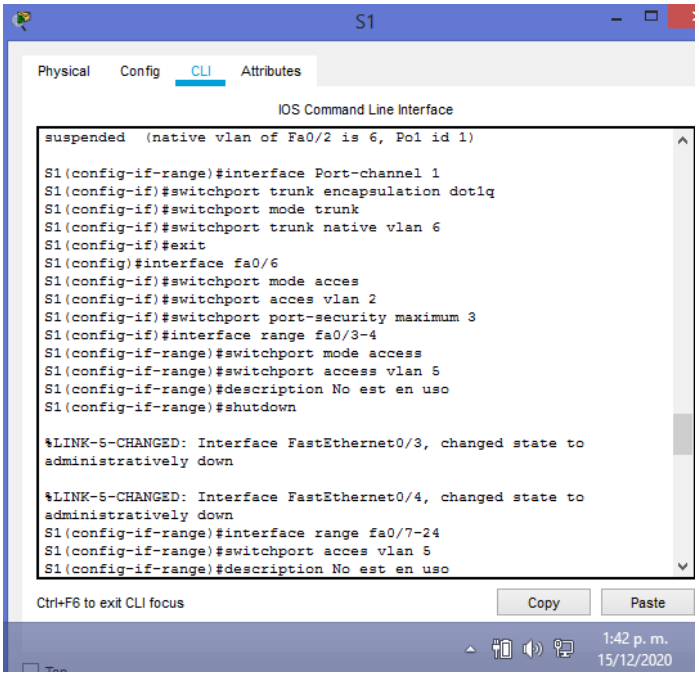
Tarea	Comando de IOS
Proteja todas las interfaces no utilizadas	S1(config-if)#interface range fa0/3-4 S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 5 S1(config-if-range)#description No está en uso S1(config-if-range)#shutdown S1(config-if-range)#interface range fa0/7-24 S1(config-if-range)#switchport acces vlan 5 S1(config-if-range)#description No está en uso S1(config-if-range)#shutdown

Es de recordar, que en el paso anterior se llevó a cabo un proceso de configuración de seguridad donde se crearon unas contraseñas seguras para lo switches, en dado caso que una persona intente acceder al sistema, inicialmente va a aparecer el banner creado con el mensaje '*El acceso no autorizado está estrictamente prohibido y perseguido con todo el peso de la ley Colombiana'*. Para dar inicio con la configuración de la infraestructura de red del switch S1, es necesario ingresar la contraseña de acceso *ciscoconpass*, se le indica que se desea ingresar al modo EXEC privilegiado escribiendo el comando *enable*, aquí solicita la contraseña *ciscoenpass*.
Como ya se cuenta con acceso al sistema, se ingresa el comando *config terminal*, en este punto del proceso, se da inicio a la creación de las VLANs mediante el comando *vlan* (número de la vlan) y *name* seguido del nombre que se la va a asignar.

Luego se identifica la interface a configurar y por medio el protocolo 802.1Q se agrega una etiqueta a cada trama con el ID de la VLAN que en este caso hace referencia al comando *switchport trunk native vlan 6*, que a su vez es canalizado por los puertos Trunk, que funciona como enlace entre el switch *S1* y *S2*, que sin necesidad de crear de crear subredes, se aumenta la seguridad interna de los dispositivos, para las interfaces *F0/1, F0/2 y F0/5.*

Para configurar el EtherChanenel en el switch *S1* capa 2, se usa el comando channel-group 1 mode active, habilitando el enlace troncal del puerto e ingresando la encapsulación troncal 802.1Q, que hace referencia al comando *dot1q,* después para cambiar el Vlan nativo, se ingresa el comando *switchport trunk native vlan 6*. Ahora se configura el puerto de acceso de host para Vlan 2, llamando a la interface *Fa0/6,* diciéndole que va a tener acceso con el comando *switchport acces vlan 2*. Por otro lado, para configurar un número máximo de 3 direcciones, se utiliza el comando *switchport port-security maximum 3*. Finalmente se seleccionan las interface que no se van a utilizar, se establece el modo de acceso, se les asigna la Vlan 5, se les agrega una descripción y se apagan, lo anterior se puede ver reflejado en la *figura 11*.

Figura 11. Configuración de la infraestructura de red switch S1



Fuente: Autor

1.2.2 Paso 5: Configurar S2

Las tareas de configuración para switch *S2* incluyen las siguientes:

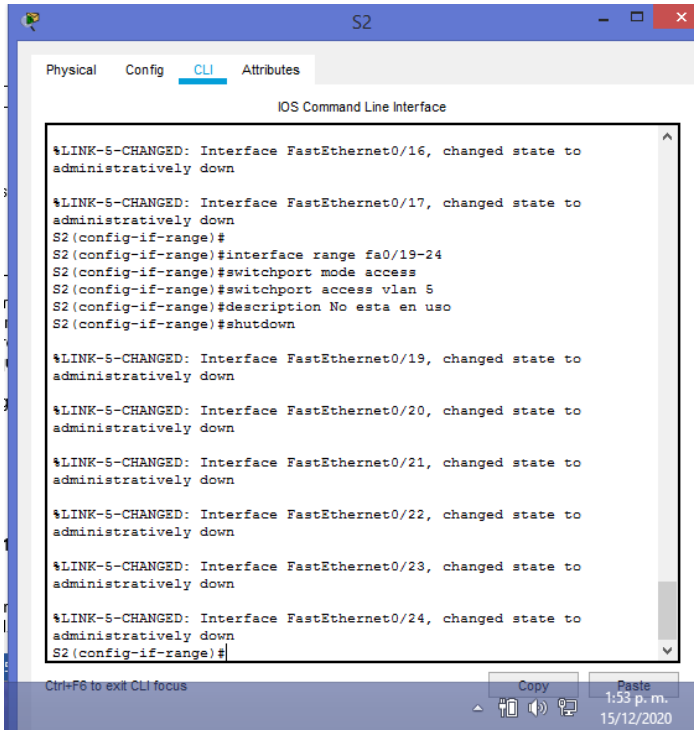
Tabla 10. Configuración infraestructura de red switch S2

Tarea	Comando de IOS
Crear VLAN	S2#config terminal S2(config)#vlan 2 S2(config-vlan)#name Bikes S2(config-vlan)#exit S2(config)#vlan 3 S2(config-vlan)#name Trikes S2(config-vlan)#exit S2(config)#vlan 4 S2(config-vlan)#name Management S2(config-vlan)#exit S2(config)#vlan 5 S2(config-vlan)#name Parking S2(config-vlan)#exit S2(config)#vlan 6 S2(config-vlan)#name Native S2(config-vlan)#exit
Crear troncos 802.1Q que utilicen la VLAN 6 nativa Interfaces F0/1 y F0/2	S2(config)#interface range fa0/1-2 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	S2(config-if-range)#channel-group 1 mode active S2(config-if-range)#interface Port-channel 1 S2(config-if)#switchport trunk encapsulation dot1q S2(config-if)#switchport mode trunk S2(config-if)#switchport trunk native vlan 6
Configurar el puerto de acceso de host VLAN 3 Interfaz F0/18	S2(config-if)# interface fa0/18 S2(config-if)#switchport mode access S2(config-if)#switchport access vlan 3
Configurar la seguridad del puerto en los puertos de acceso Permitir 3 direcciones MAC	S2(config-if)#switchport port-security maximum 3

Tarea	Comando de IOS
Asegure todas las interfaces no utilizadas.	S2(config-if)#interface range fa0/3-17 S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 5 S2(config-if-range)#description No esta en uso S2(config-if-range)#shutdown S2(config-if-range)#interface range fa0/19-24 S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 5 S2(config-if-range)#description No esta en uso S2(config-if-range)#shutdown

Para la configuración del switch S2, se lleva a cabo el mismo procedimiento del S1, se ingresa por modo EXEC privilegiado, se crean las VLAN, se utiliza el protocolo 802.1Q, pero a diferencia del switch S1, solo se crea un grupo de puertos EtherChannel de Capa 2 que use interfaces *fa0/1* y *fa0/2*, de igual manera para este caso se configura el puerto de acceso del host para la VLAN 3 con la interface *fa0/18*, así mismo se configura la seguridad de los puertos y se aseguran las interfaces no utilizadas, como se puede evidenciar en la *figura 12.*

Figura 12. Configuración de la infraestructura de red switch S2



Fuente: Autor

1.3 Parte 3: Configurar soporte de host

1.3.1 Paso 1: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 11. Configurar soporte de host R1

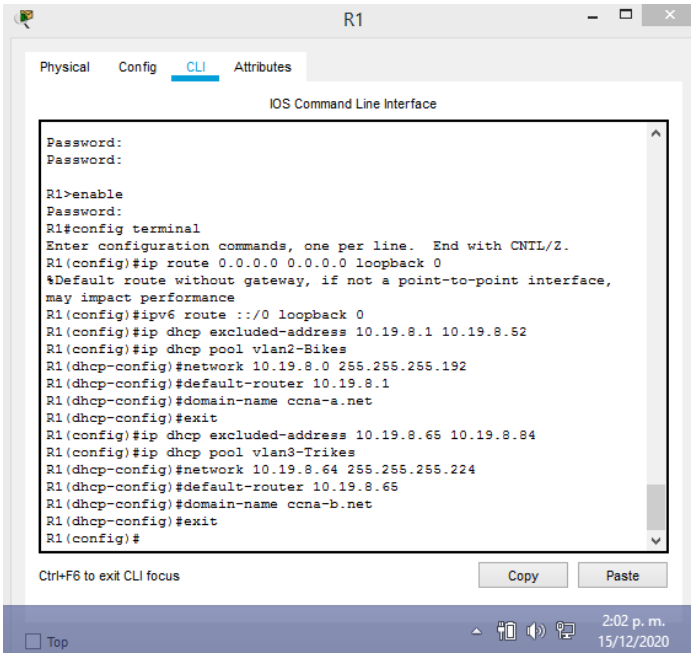
Tarea	Comando de IOS
Configure Default Routing	R1(config)#ip route 0.0.0.0 0.0.0.0 loopback 0 R1(config)#ipv6 route ::/0 loopback 0
Configurar IPv4 DHCP para VLAN 2	R1(config)#ip dhcp excluded-address 10.19.8.1 10.19.8.52 R1(config)#ip dhcp pool vlan2-Bikes R1(dhcp-config)#network 10.19.8.0 255.255.255.192 R1(dhcp-config)#default-router 10.19.8.1 R1(dhcp-config)#domain-name ccna-a.net R1(dhcp-config)#exit
Configurar DHCP IPv4 para VLAN 3	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

Continuando con la configuración de soporte de host, se establece una ruta estática de red, como forma de configurar la puerta de enlace como última alternativa en un enrutador, esto se realiza por medio del comando *ip route 0.0.0.0 0.0.0.0* creando rutas para direccionamiento IPv4 e IPv6 hacia la interface *loopback 0.*

Con el protocolo DHCP, mediante el comando *ip dhcp excluded-address* se especifica las direcciones excluidas que no se deben asignar, dando el rango de una IP de inicio y una IP final para el grupo VLAN 2. Luego se pone el nombre del rango del servicio por medio del comando *ip dhcp pool*, en la siguiente línea se define la red que se encargara de dar servicio DHCP, su respectiva puerta de enlace y por último el nombre del dominio

ccna-a.net, el anterior procedimiento se repite para el grupo VLAN 3 con diferentes direcciones y nombre de dominio que sería ccna-b.net.

Figura 13. Configuración de soporte de host en Router



Fuente: Autor

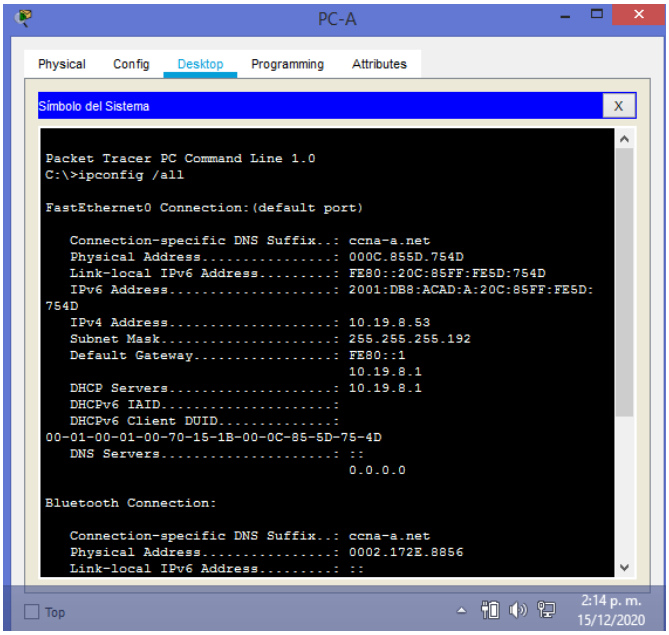
1.3.2 Paso 2: Configurar los servidores

Tabla 12. Configuración de red del equipo PC-A

Configuración de red de PC-A	
Descripción	Datos por DHCP
Dirección física	000C.855D.754D
Dirección IP	10.19.8.53
Máscara de subred	255.255.255.192
Gateway predeterminado	10.19.8.1
Gateway predeterminado IPv6	FE80::1

Luego de configurar el equipo host PC-A, a continuación se pueden ver las especificaciones realizadas por medio del *comando ipconfig /all* en la *figura 14*

Figura 14. Comando ipconfig /all en PC-A



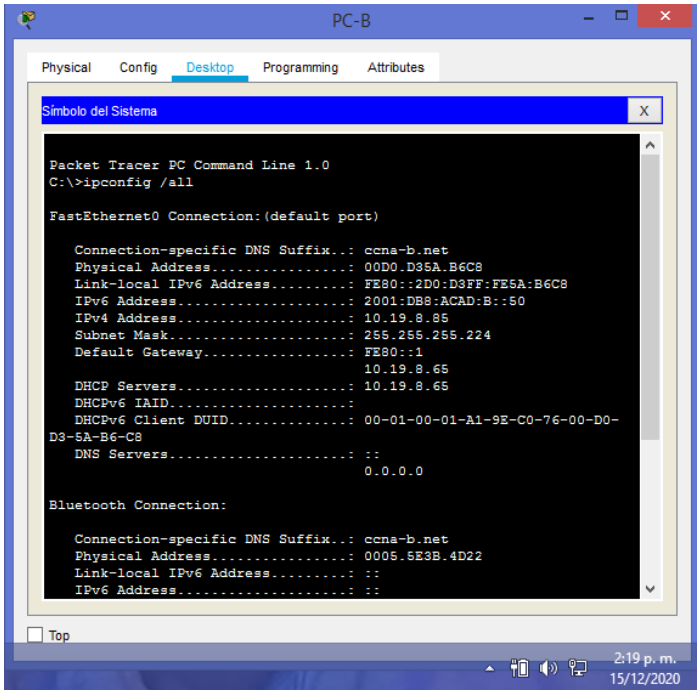
Fuente: Autor

Tabla 13. Configuración de red del equipo PC-B

Configuración de red de PC-B	
Descripción	Datos por DHCP
Dirección física	00D0.D35A.B6C8
Dirección IP	10.19.8.85
Máscara de subred	255.255.255.224
Gateway predeterminado	10.19.8.65
Gateway predeterminado IPv6	FE80::1

Luego de configurar el equipo host PC-B, a continuación se pueden ver las especificaciones realizadas por medio del *comando ipconfig /all* en la *figura 15*

Figura 15. Comando ipconfig /all en PC-B



Fuente: Autor

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

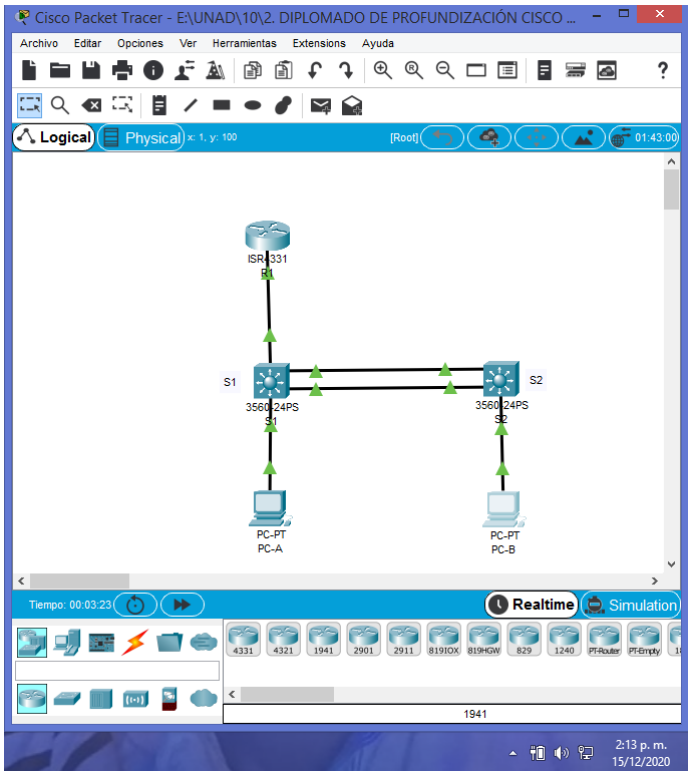
Por medio de la siguiente tabla se puede verificar metódicamente la conectividad con cada dispositivo de red.

Tabla 14. Pruebas para conectividad IPv4 e IPv6 en la red

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

Desde	A	de Internet	Dirección IP	Resultados de ping
PC-A	PC-B	Dirección	10.19.8.85	4/4
		IPv6	2001:db8:acad:b::50	4/4
	R1 Bucle 0	Dirección	209.165.201.1	4/4
		IPv6	2001:db8:acad:209::1	4/4
PC-B	R1 Bucle 0	Dirección	209.165.201.1	4/4
		IPv6	2001:db8:acad:209::1	4/4
	R1, G0/0/1.2	Dirección	10.19.8.1	4/4
		IPv6	2001:db8:acad:a::1	4/4
	R1, G0/0/1.3	Dirección	10.19.8.65	4/4
		IPv6	2001:db8:acad:b::1	4/4
	R1, G0/0/1.4	Dirección	10.19.8.97	4/4
		IPv6	2001:db8:acad:c: :1	4/4
	S1, VLAN 4	Dirección	10.19.8.98	4/4
		IPv6	2001:db8:acad:c::98	4/4
	S2, VLAN 4	Dirección	10.19.8.99	4/4
		IPv6	2001:db8:acad:c::99	4/4

Figura 16. Topología escenario 1 funcionando correctamente



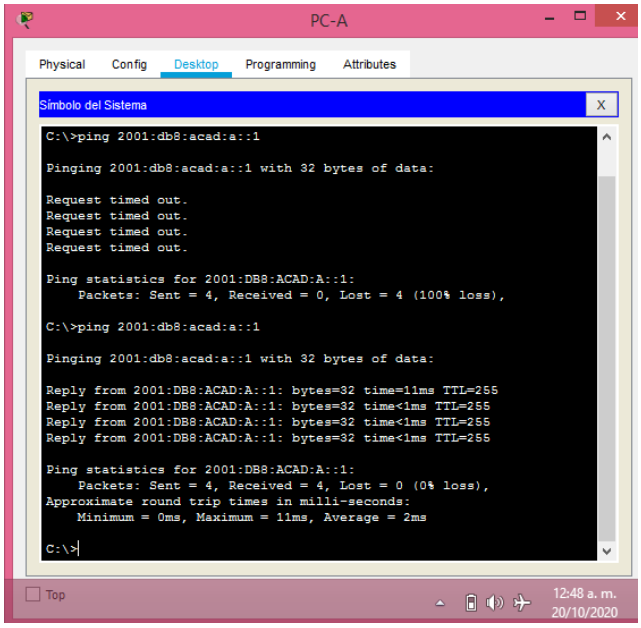
Fuente: Autor

Finalmente en la *figura 16* se puede observar el correcto funcionamiento de la red pequeña, en equipos que admiten conectividad Ipv4 e IPv6 en los host soportados, para tener una mejor certeza de la afirmación anterior, se usara el comando *Ping* en base a la *tabla 14* con el fin de probar la conectividad entre todos los dispositivos de la red.

Pruebas para conectividad IPv4 e IPv6 en la red

En la *figura 17* se puede verificar la conectividad desde PC-A a la dirección IPv6 2001:db8:acad:a: :1 del router R1, subinterfaz G0/0/1.2

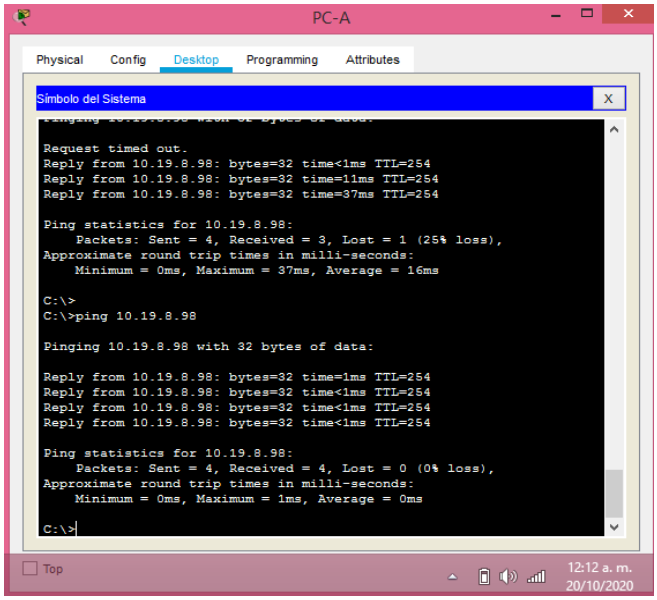
Figura 17. Ping PC-A a R1, G0/0/1.2 IPv6



Fuente: Autor

En la *figura 18* se puede verificar la conectividad desde PC-A a la dirección IPv4 10.19.8.98 del switch S1, VLAN 4.

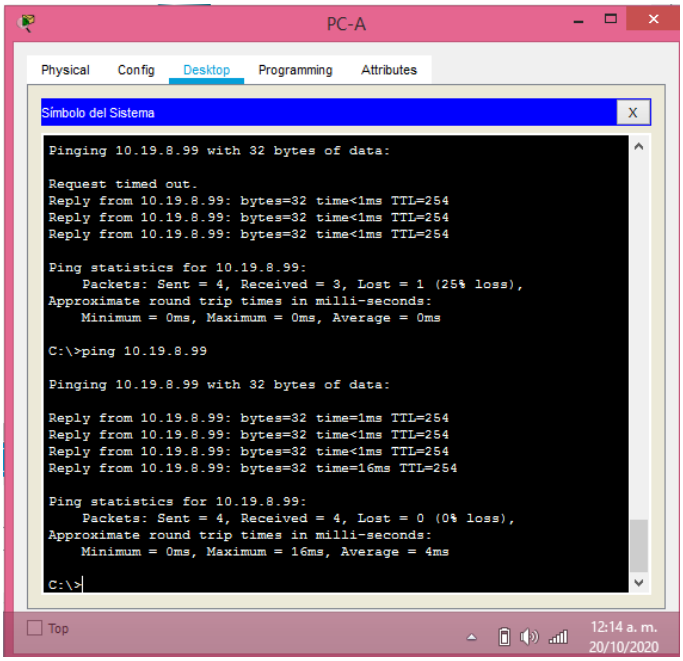
Figura 18. Ping PC-A a S1, VLAN 4 IPv4



Fuente: Autor

En la *figura 19* se puede verificar la conectividad desde PC-A a la dirección IPv4 10.19.8.98 del switch S1, VLAN 4.

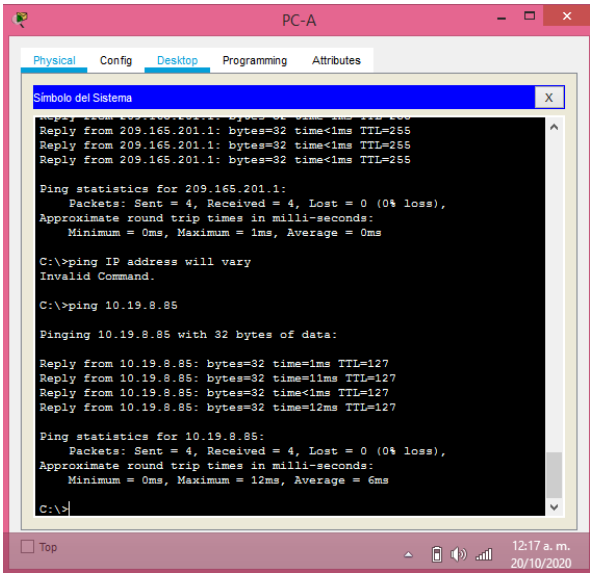
Figura 19. Ping PC-A a S2, VLAN 4 IPv4



Fuente: Autor

En la *figura 20* se puede verificar la conectividad desde PC-A a la dirección IPv4 10.19.8.85 del PC-B.

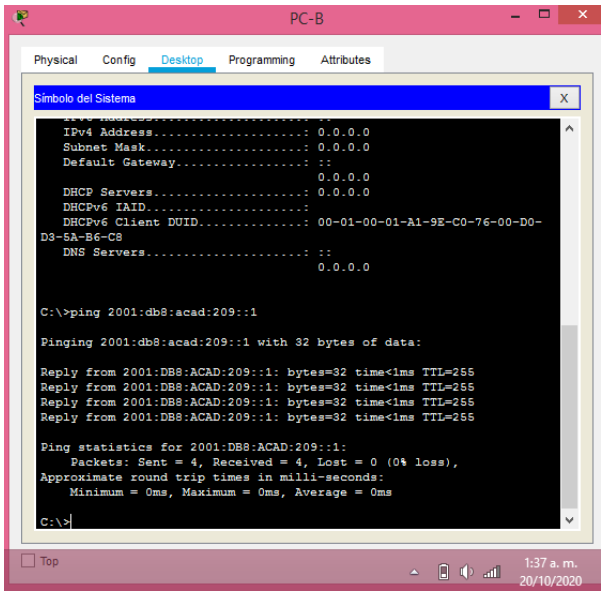
Figura 20. Ping PC-A a PC-B IPv4



Fuente: Autor

En la *figura 21* se puede verificar la conectividad desde PC-B a la dirección IPv6 2001:db8:acad:209: :1 del router R1 bucle 0

Figura 21. Ping PC-B a R1 Bucle 0 IPv6

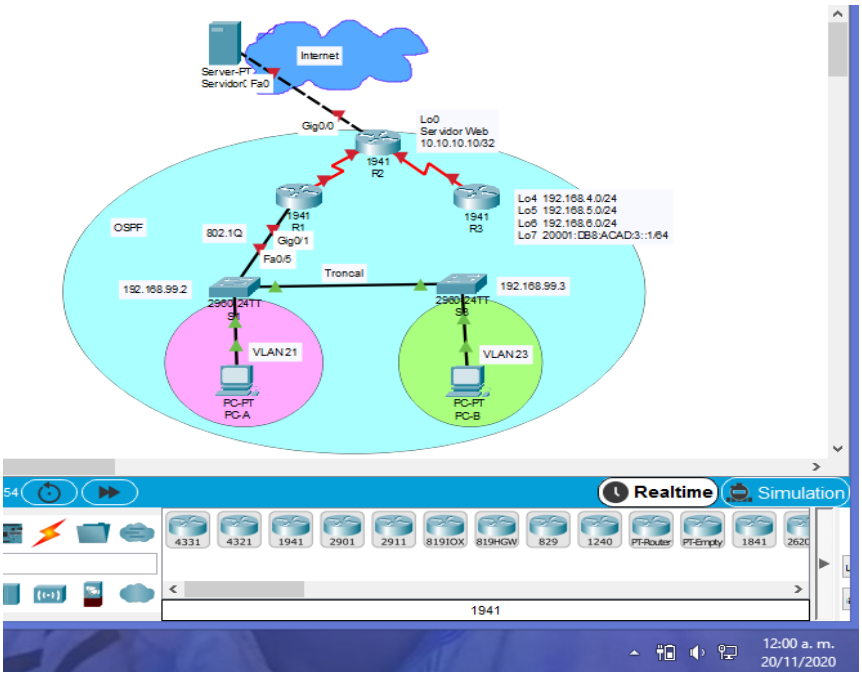


Fuente: Autor

2. Escenario 2

Topología

Figura 22. Topología escenario 2



Fuente: Autor

En la topología del escenario 2 se utilizó un servidor, 3 (tres) router de servicios integrados Cisco 1941, 2 (dos) switches Cisco 2960-24TT y 2 (dos) PC, como medio de conexión se utilizó, cable serial DCE, cable de cobre directo y cable de cobre cruzado, con el fin de configurar una pequeña red segura, que además admita conectividad IPv4 e IPv6.

Es importante resaltar que antes de dar inicio a la conexión del cableado es importante apagar los router manualmente e incorporar en una ranura, una tarjeta de interfaz WAN HWIC-2T, la cual proporciona 2 (dos) puertos seriales necesarios en la topología de la red a configurar.

Figura 23. Incorporar tarjeta de interfaz WAN HWIC-2T en router R1 escenario2

Fuente: Autor

2.1 Parte 1: Inicializar dispositivos

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

Antes de dar inicio a la configuración del escenario 2, es importante que cada uno de los dispositivos que hacen parte de la topología, no almacenen información de alguna configuración anterior, teniendo en cuenta, que podría generar dificultades en el proceso, de lo anterior a través de unos comandos de IOS, se inicializa y se vuelve a cargar cada uno de los routers y los switches.

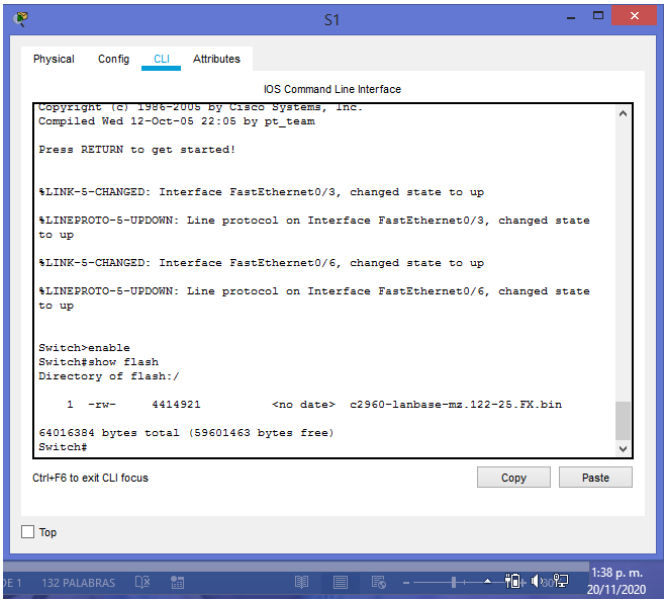
Como primera tarea, se ingresa al modo privilegiado del router *R1* y se escribe el comando *enable,* seguido de *erase startup-config*, el cual elimina el archivo startup-config del router, al aparecer un mensaje de aviso, se confirma la eliminación del archivo del sistema. Ahora para cargar manualmente el router, se aplica el comando *reload*, dicho proceso tardara unos segundos; los mismos comandos se utilizaran para el router de nombre R2 y R3 respectivamente.

Tabla 15. Inicialización y recarga de los routers y los switches escenario 2

Tarea	Comando de IOS
Eliminar configuración inicial	Router>enable Router#erase startup-config Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
Reiniciar manualmente el router	Router#reload
Ingresar modo privilegiado del switch Eliminar configuración anterior.	Switch>enable Switch#erase startup-config Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
Eliminar la base de datos de VLAN anterior	Switch#delete vlan.dat
Reiniciar manualmente el switch	Switch#reload
Verificar datos de VLAN en la memoria	Switch>enable Switch#show flash

Como segunda tarea, se identifica el switch de nombre *S1*, posteriormente se ingresa al modo privilegiado, después de ingresar el comando IOS *erase startup-config* se eliminan los archivos de configuración inicial y con el comando *delete vlan.dat* se elimina la base de datos de VLAN anterior, al confirmar la acción aparece un mensaje que indica que no existe tal archivo. Se procede a cargar el switch, por lo que es necesario ingresar nuevamente al modo privilegiado con el comando *enable* y ahora sí, se verifica que en la memoria flash no exista base de datos de VLAN, lo anterior se puede comprobar escribiendo el comando *show flash.*

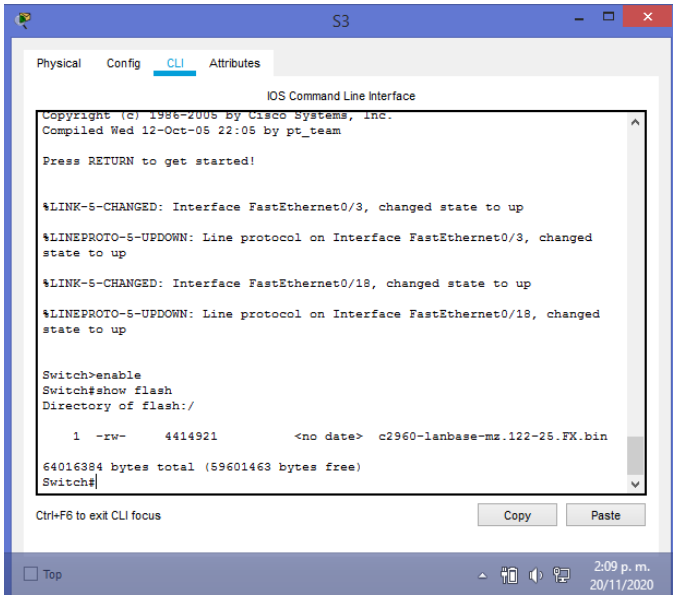
Figura 24. Show flash switch S1 escenario 2



Fuente: Autor

Los comandos utilizados en esta segunda tarea, se utilizan de igual forma para la configuración del switch de nombre *S3.*

Figura 25. Show flash switch S3 escenario 2



Fuente: Autor

2.2 Parte 2: Configurar los parámetros básicos de los dispositivos

2.2.1 Paso 1: Configurar la computadora de Internet

Teniendo en cuenta las siguientes especificaciones, se configura el servidor de internet.

Tabla 16. Configuración 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

2.2.2 Paso 2: Configurar R1

Al igual que en anteriores configuraciones, primero se ingresa al modo privilegiado del router, se desactiva la búsqueda DNS por medio del comando *no ip domain-lookup*, se asigna un nombre al router, para ello se utiliza el comando *hostname*, seguido de *R1*. La seguridad del dispositivo es importante, por tal razón se crea una contraseña de acceso al modo privilegiado definida como *class*, otra de acceso por consola como cisco y finalmente la contraseña cisco para Telnet, por medio del comando *service password-encryption* se aplica un cifrado a las contraseñas sin cifrar.

Es hora de establecer una descripción a la interfaz *S0/0/0* que indique el acceso al router R2 por medio de la dirección IP 172.16.1.1 y de establecer la frecuencia de reloj en 12800 por medio del comando *clock rate*, una vez hecho esto se activa la interfaz con el comando *no shutdown.* Finalmente se configuran las rutas IPv4 e IPv6 predeterminadas 0.0.0.0 0.0.0.0 ::/0 respectivamente.

Tabla 17. Configuración router R1 escenario 2

Tarea	Comando de IOS
Desactivar la búsqueda DNS	Router>enable Router#config terminal Router(config)# no ip domain-lookup
Modificar nombre del router	Router(config)#hostname R1
Contraseña de exec privilegiado cifrada	R1(config)# enable secret class
Contraseña de acceso a la consola	R1(config)#line console 0 R1(config-line)# password cisco R1(config-line)#login R1(config-line)#exit
Contraseña de acceso Telnet	R1(config)#line vty 0 15 R1(config-line)# password cisco R1(config-line)#login
Cifrar las contraseñas de texto no cifrado	R1(config-line)# service password-encryption
Mensaje MOTD	R1 (config)# banner motd # Se prohíbe el acceso no autorizado#
Interfaz S0/0/0	R1(config)#interface s0/0/0 R1(config-if)#description connection to R2 R1(config-if)#ip address 172.16.1.1 255.255.255.252 R1(config-if)#ipv6 address 2001:DB8:ACAD:1::1/64 R1(config-if)#clock rate 128000 R1(config-if)#no shutdown R1(config-if)#exit
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

2.2.3 Paso 3: Configurar R2

A diferencia de las tareas de configuración del router R1, en el router R2 se habilita el servidor HTTP, se establece una descripción a la interfaz *S0/0/0* que indique el acceso al router R1 por medio de la dirección IP 172.16.1.2 y una descripción a la interfaz *S0/0/1* que indique el acceso al router R3 por medio de la dirección IP 172.16.2.2. Por otro lado la interfaz *G0/0* con la descripción de conexión a internet, al finalizar se ingresa el comando *no shutdown*, el cual habilita las interfaces. De igual manera, se realiza la configuración de la interface lógica de R2 interface *loopback0*, con la descripción servidor web simulado.

Tabla 18. Configuración router R2 escenario 2

Tarea	Comando de IOS
Desactivar la búsqueda DNS	Router>enable Router#config terminal Router(config)# no ip domain-lookup
Modificar nombre del router	Router(config)#hostname R2
Contraseña de exec privilegiado cifrada	R2(config)# enable secret class
Contraseña de acceso a la consola	R2(config)#line console 0 R2(config-line)# password cisco R2(config-line)#login R2(config-line)#exit
Contraseña de acceso Telnet	R2(config)#line vty 0 15 R2(config-line)# password cisco R2(config-line)#login
Cifrar las contraseñas de texto no cifrado	R2(config-line)# service password-encryption
Habilitar el servidor HTTP	R2 (config)# ip http server
Mensaje MOTD	R2 (config)# banner motd # Se prohibe el acceso no autorizado#
Interfaz S0/0/0	R2(config)#interface s0/0/0 R2(config-if)#description connection to R1 R2(config-if)#ip address 172.16.1.2 255.255.255.252 R2(config-if)#ipv6 address 2001:DB8:ACAD:1::1/64 R2(config-if)#no shutdown R2(config-if)#exit
Interfaz S0/0/1	R2(config)#interface s0/0/1 R2(config-if)#description connection to R3 R2(config-if)#ip address 172.16.2.2 255.255.255.252 R2(config-if)#ipv6 address 2001:DB8:ACAD:2::2/64 R2(config-if)#clock rate 128000 R2(config-if)#no shutdown
Interfaz G0/0 (simulación de Internet)	R2(config-if)#interface g0/0 R2(config-if)#description conexion to Internet R2(config-if)#ip address 209.165.200.233 255.255.255.248 R2(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64 R2(config-if)#no shutdown

Tarea	Comando de IOS
Interfaz loopback 0 (servidor web simulado)	R2(config-if)#interface loopback 0 R2(config-if)#description Servidor Web Simulado R2(config-if)#ip address 10.10.10.10 255.255.255.255 R2(config-if)#exit
Rutas predeterminadas	R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0 R2(config)#ipv6 route ::/0 g0/0

2.2.4 Paso 4: Configurar R3

Dentro de las tareas de configuración del router R3, se establece una descripción a la interfaz *S0/0/1* que indique el acceso al router R2 por medio de la dirección IP 172.16.2.1 y las direcciones IP de interfaces lógicas loopback 4, 5, 6 y 7

Tabla 19. Configuración router R3 escenario 2

Tarea	Comando de IOS
Desactivar la búsqueda DNS	Router>enable Router#config terminal Router(config)# no ip domain-lookup
Modificar nombre del router	Router(config)#hostname R3
Contraseña de exec privilegiado cifrada	R3(config)# enable secret class
Contraseña de acceso a la consola	R3(config)#line console 0 R3(config-line)# password cisco R3(config-line)#login R3(config-line)#exit
Contraseña de acceso Telnet	R3(config)#line vty 0 15 R3(config-line)# password cisco R3(config-line)#login
Cifrar las contraseñas de texto no cifrado	R3(config-line)# service password-encryption
Mensaje MOTD	R3 (config)# banner motd # Se prohibe el acceso no autorizado#
Interfaz S0/0/1	R3(config)#interface s0/0/1 R3(config-if)#description conexion to R2 R3(config-if)#ip address 172.16.2.1 255.255.255.252 R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64 R3(config-if)#no shutdown
Interfaz loopback 4	R3(config-if)#interface loopback 4 R3(config-if)#ip address 192.168.4.1 255.255.255.0

Tarea	Comando de IOS
Interfaz loopback 5	R3(config-if)#interface loopback 5 R3(config-if)#ip address 192.168.5.1 255.255.255.0
Interfaz loopback 6	R3(config-if)#interface loopback 6 R3(config-if)#ip address 192.168.6.1 255.255.255.0
Interfaz loopback 7	R3(config-if)#interface loopback 7 R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64 R3(config-if)#exit
Rutas predeterminadas	R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1 R3(config)#ipv6 route ::/0 s0/0/1

2.2.5 Paso 5: Configurar S1

Cuando se inicia una nueva configuración, es necesario ingresar al modo privilegiado del switch y por seguridad asignar contraseñas para exec privilegiado, otra de acceso a la consola, una de acceso Telnet y al finalizar realizar el proceso de cifrado de las contraseñas creadas. Cuando se intente acceder al dispositivo, va a aparecer un mensaje al usuario que dice: “Se prohíbe el acceso no autorizado”, esto se logra configurado el banner con el comando *banner motd.*

Tabla 20. Configuración del switch S1 escenario 2

Tarea	Comando de IOS
Desactivar la búsqueda DNS.	Switch >enable Switch #config terminal Switch(config)#no ip domain lookup
Nombre del switch	Switch(config)#hostname S1
Contraseña de exec privilegiado cifrada	S1(config)#enable secret class
Contraseña de acceso a la consola	S1(config)#line console 0 S1(config-line)#password cisco S1(config-line)#login
Contraseña de acceso Telnet	S1(config-line)#line vty 0 15 S1(config-line)#password cisco S1(config-line)#login
Cifrar las contraseñas de texto no cifrado	S1(config- line)#service password-encryption
Configurar un MOTD Banner	S1 (config)# banner motd # Se prohibe el acceso no autorizado #

2.2.6 Paso 6: Configurar S3

En la configuración del switch S3, se realizan los mismos pasos que en la configuración del switch S1 e incluye las siguientes tareas:

Tabla 21. Configuración del switch S3 escenario 2

Tarea	Comando de IOS
Desactivar la búsqueda DNS.	Switch >enable Switch #config terminal Switch(config)#no ip domain lookup
Nombre del switch	Switch(config)#hostname S3
Contraseña de exec privilegiado cifrada	S3(config)#enable secret class
Contraseña de acceso a la consola	S3(config)#line console 0 S3(config-line)#password cisco S3(config-line)#login
Contraseña de acceso Telnet	S3(config-line)#line vty 0 15 S3(config-line)#password cisco S3(config-line)#login
Cifrar las contraseñas de texto no cifrado	S3(config- line)#service password-encryption
Configurar un MOTD Banner	S3 (config)# banner motd # Se prohibe el acceso no autorizado #

2.2.7 Paso 7: Verificar la conectividad de la red

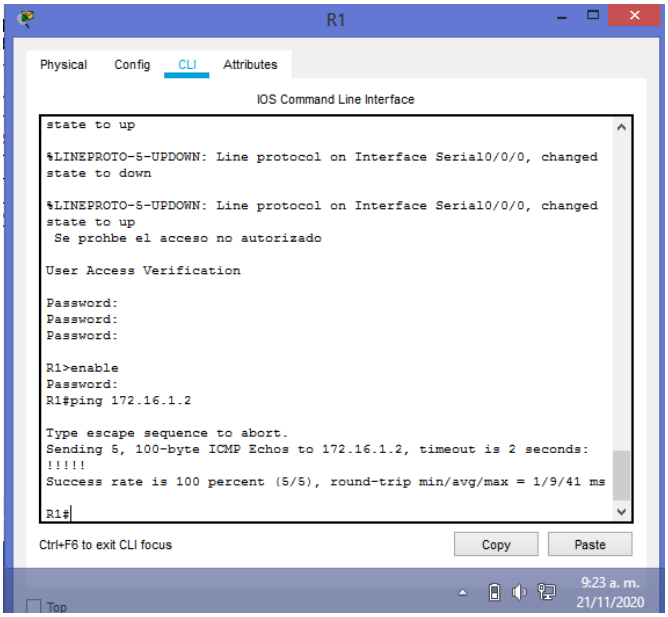
Tabla 22. Pruebas para conectividad en la red escenario 2

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	5/5
R2	R3, S0/0/1	172.16.2.1	5/5
PC de Internet	Gateway predeterminado	209.165.200.233	4/4

Para comprobar la conectividad entre los dispositivos de la red, se ingresa al modo EXEC privilegiado y se hace uso del comando *ping* seguido de la dirección IP de destino, utilizando la información de la *tabla 22*.

En la *figura 26* se puede verificar la conectividad desde R1 a la dirección IPv4 172.16.1.2 del router R2

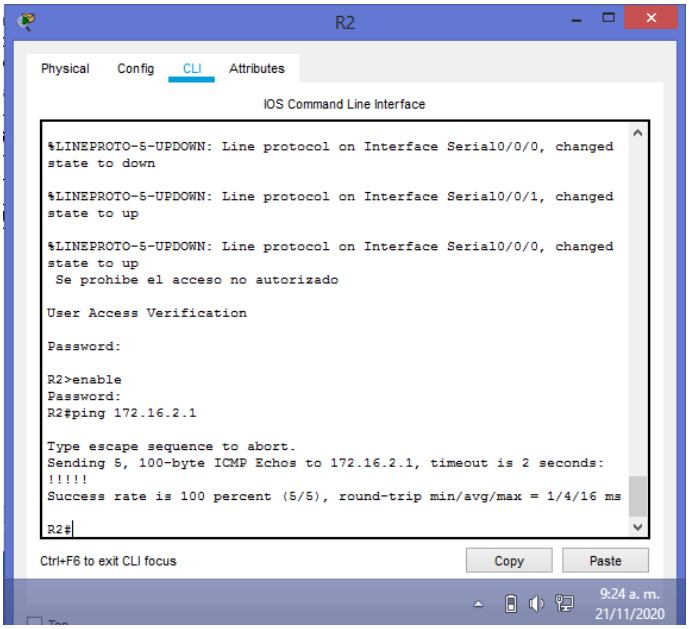
Figura 26. Ping desde R1 a R2 S0/0/0 escenario 1



Fuente: Autor

En la *figura 27* se puede verificar la conectividad desde R2 a la dirección IPv4 172.16.2.1 del router R3

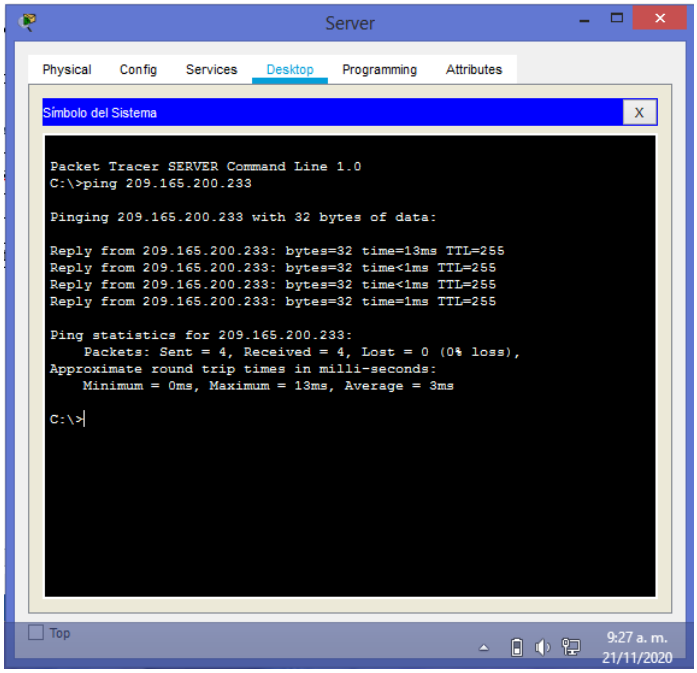
Figura 27. Ping desde R2 a R3 S0/0/1 escenario 1



Fuente: Autor

En la *figura 28* se puede verificar la conectividad desde PC de internet a la dirección IPv4 Gateway predeterminado 209.165.200.233.

Figura 28. Ping desde PC de Internet a Gateway predeterminado escenario 1



Fuente: Autor

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

2.3.1 Paso 1: Configurar S1

Uno vez se haya ingresado al modo de configuración, el indicador cambia a *S1#* lo que indica que ya se puede seguir con las tareas de configuración del switch, como primer paso se definen los nombres de las VLAN a utilizar, VLAN 21,23 y 99, que corresponden a contabilidad, ingeniería y administración respectivamente, a esta última VLAN se le asigna la dirección IPv4 192.168.99.2 con una puerta de enlace predeterminada 255.255.255.0.

Con el fin de evitar posibles accesos no autorizados a demás de contraseñas del sistema, es importante inhabilitar los puertos que no se vayan a utilizar en la red por medio del

comando IOS *shutdown,* que lo antecede *interface range* seguido de las conexiones *Fa0/1-2, Fa0/4, Fa0/7-24, g0/1-2*.

Tabla 23. Configuración de seguridad del switch S1 escenario 2

Tarea	Comando de IOS
Crear la base de datos de VLAN	Password: cisco S1>enable Password: class S1#config terminal S1(config)#vlan 21 S1(config-vlan)#name Contabilidad S1(config-vlan)#vlan 23 S1(config-vlan)#name Ingenieria S1(config-vlan)#vlan 99 S1(config-vlan)#name Administracion S1(config-vlan)#exit
Asignar la dirección IP de administración.	S1(config)#interface vlan 99 S1(config-if)#ip address 192.168.99.2 255.255.255.0 S1(config-if)#no shutdown S1(config-if)#exit
Asignar el gateway predeterminado	S1(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	S1(config)#interface Fa0/3 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1
Forzar el enlace troncal en la interfaz F0/5	S1(config-if)#interface Fa0/5 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	S1(config-if)#interface range Fa0/1-2, Fa0/4, Fa0/6-24, g0/1-2 S1(config-if-range)#switchport mode access
Asignar F0/6 a la VLAN 21	S1(config-if-range)#interface Fa0/6 S1(config-if)#switchport access vlan 21
Apagar todos los puertos sin usar	S1(config-if)#interface range Fa0/1-2, Fa0/4, Fa0/7-24, g0/1-2 S1(config-if-range)#shutdown

2.3.2 Paso 2: Configurar S3

Al igual que las tareas del paso 1 del switch S1, en el switch S3 se definen los nombres de las VLAN 21, 23 y 99, por otro lado la dirección Ipv4 de la interface VLAN 99 cambia a 192.168.99.3, se configura el puerto 18 a la VLAN de Ingeniería y se llevan a cabo las siguientes tareas de configuración:

Tabla 24. Configuración de seguridad del switch S3 escenario 2

Tarea	Comando de IOS
Crear la base de datos de VLAN	Password: cisco S3>enable Password: class S3#config terminal S3(config)#vlan 21 S3(config-vlan)#name Contabilidad S3(config-vlan)#vlan 23 S3(config-vlan)#name Ingenieria S3(config-vlan)#vlan 99 S3(config-vlan)#name Administracion S3(config-vlan)#exit
Asignar la dirección IP de administración.	S3(config)#interface vlan 99 S3(config-if)#ip address 192.168.99.3 255.255.255.0 S3(config-if)#no shutdown S3(config-if)#exit
Asignar el gateway predeterminado	S3(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	S3(config)#interface Fa0/3 S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	S3(config-if)#interface range Fa0/1-2, Fa0/4-24, g0/1-2 S3(config-if-range)#switchport mode Access
Asignar F0/18 a la VLAN 23	S3(config-if-range)#interface Fa0/18 S3(config-if)#switchport access vlan 23
Apagar todos los puertos sin usar	S3(config-if)#interface range Fa0/1-2, Fa0/4-17, Fa0/19-24, g0/1-2 S3(config-if-range)#shutdown

2.3.3 Paso 3: Configurar R1

En este paso se realiza la configuración de enrutamiento entre VLAN con el protocolo 802.1Q en el router R1, para ello se deben personalizar las subinterfaces *802.1Q .21, 802.1Q .23 y 802.1Q .99*, primero se habilita el modo privilegiado, se ingresa al modo de configuración, se asignan las VLAN y las primeras direcciones disponibles, finalmente se activa la interfaz g0/1 por medio del comando *no shutdown*.

Tabla 25. Configuración de seguridad del router R1 escenario 2

Tarea	Comando de IOS
Configurar la subinterfaz 802.1Q .21 en G0/1	Password: cisco R1>enable Password: class R1#config terminal R1(config)#interface 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
Configurar la subinterfaz 802.1Q .23 en G0/1	R1(config-subif)#interface g0/1.23 R1(config-subif)#description vlan 23 R1(config-subif)#encapsulation dot1q 23 R1(config-subif)#ip address 192.168.23.1 255.255.255.0
Configurar la subinterfaz 802.1Q .99 en G0/1	R1(config-subif)#interface 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
Activar la interfaz G0/1	R1(config-subif)#interface g0/1 R1(config-if)#no shutdown

2.3.4 Paso 4: Verificar la conectividad de la red.

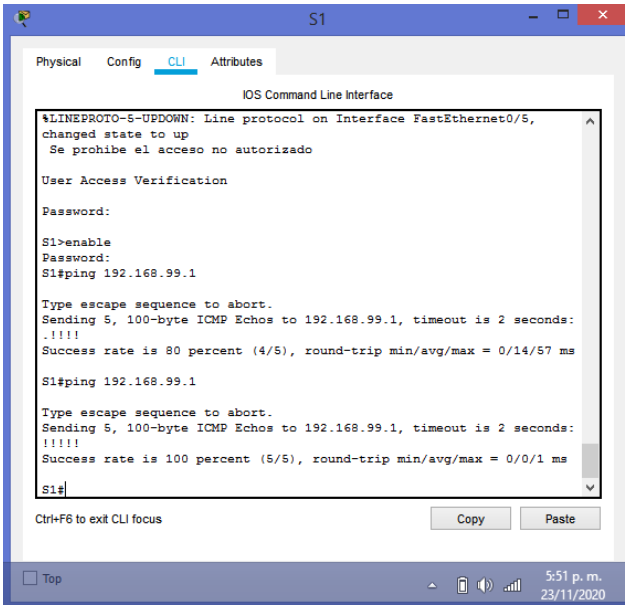
Con el uso del comando *ping* seguido de la dirección IP de las VLAN de destino, se llevan a cabo las pruebas de conectividad entre los switches y el router R1, utilizando la información de la siguiente tabla.

Tabla 26. Pruebas para conectividad entre los switches y R1 escenario 2

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	5/5
S3	R1, dirección VLAN 99	192.168.99.1	5/5
S1	R1, dirección VLAN 21	192.168.21.1	5/5
S3	R1, dirección VLAN 23	192.168.23.1	5/5

En la *figura 29* se puede verificar la conectividad desde S1 a la dirección IPv4 192.168.99.1 del router R1 VLAN 99

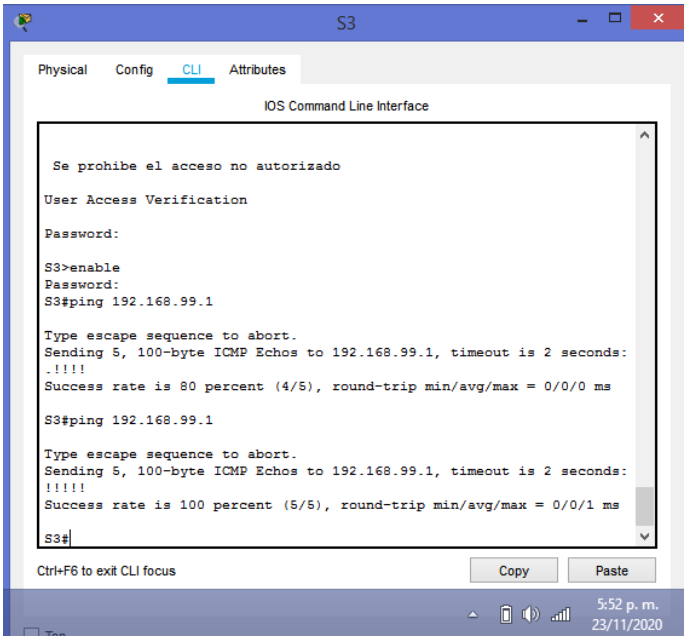
Figura 29. Ping desde S1 a R1 vlan 99 escenario 2



Fuente: Autor

En la *figura 30* se puede verificar la conectividad desde S3 a la dirección IPv4 192.168.99.1 del router R1 VLAN 99

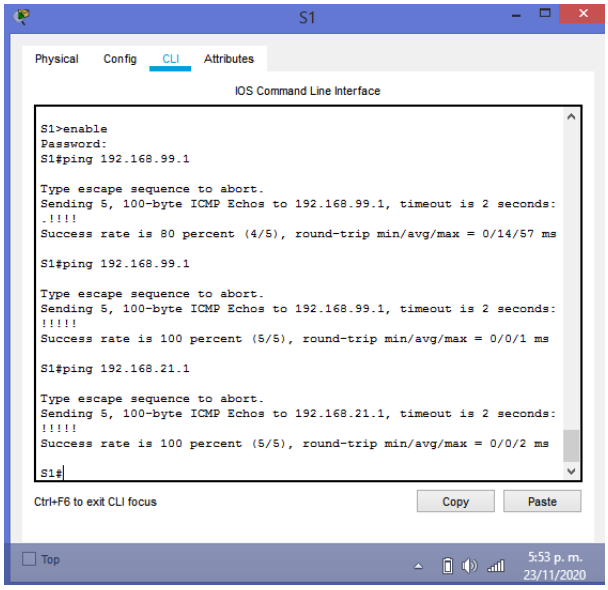
Figura 30. Ping desde S3 a R1 vlan 99 escenario 2



Fuente: Autor

En la *figura 31* se puede verificar la conectividad desde S1 a la dirección IPv4 192.168.21.1 del router R1 VLAN 21

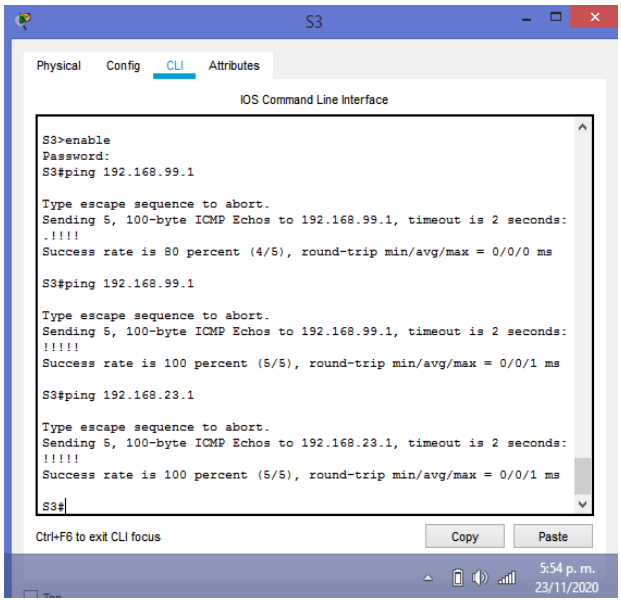
Figura 31. Ping desde S1 a R1 vlan 21 escenario 2



Fuente: Autor

En la *figura 31* se puede verificar la conectividad desde S3 a la dirección IPv4 192.168.23.1 del router R1 VLAN 23

Figura 32. Ping desde S3 a R1 vlan 23 escenario 2



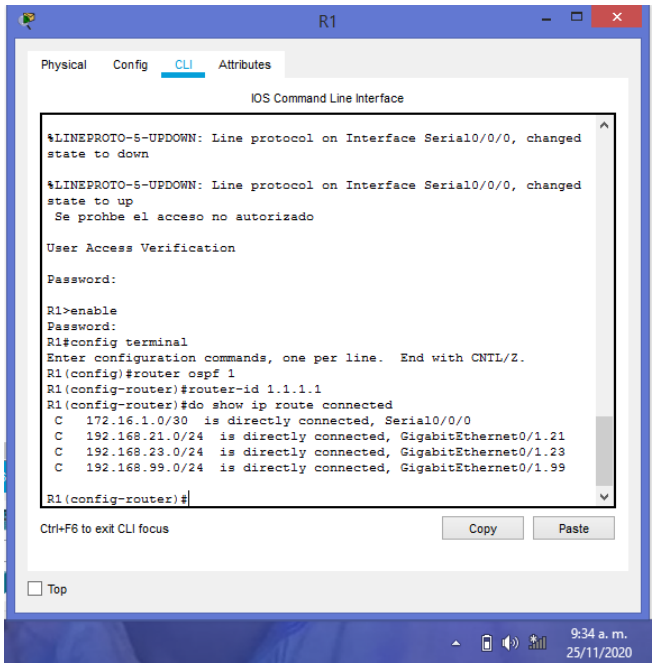
Fuente: Autor

2.4 Parte 4: Configurar el protocolo de routing dinámico OSPF

2.4.1 Paso 1: Configurar OSPF en el R1

El protocolo OSPF que del inglés hace referencia a protocolo Open Shortest Path First permite encontrar la mejor ruta de comunicación entre los dispositivos, es decir la trayectoria más corta. Luego de ingresar al modo privilegiado y a la configuración global, se procede a habilitar OSPF por medio del comando *router ospf* seguido de *id del proceso*, el cual pertenece a un valor numérico comprendido entre 1 y 65.535 correspondiente a un valor de 16 bits. Luego es necesario el comando *router-id* es cual es un indicador escrito en formato IPv4, como en el caso del router R1 el valor seria 1.1.1.1

Figura 33. Comando show ip route connected en R1 escenario 2



Fuente: Autor

El comando *show ip route connected* permite observar la información del enrutamiento que se va a utilizar para el reenvío de información, en base a lo anterior, en cada red debe identificar la dirección, la máscara wildcard y el indicador del área al cual pertenece, para la presente red, es *área 0* (cero). Como siguiente paso es ejecutar el comando *passive-interface* que deshabilita el envío de mensajes de saludo donde no se necesita

intercambiar información, finalmente se utiliza el comando *no auto-summary* que desactiva la sumarización automática de las redes, pero OSPF no lo ejecuta.

Tabla 27. Configuración del protocolo OSPF en el R1 escenario 2

Tarea	Comando de IOS
Configurar OSPF área 0	Password: cisco R1>enable Password: class R1#config terminal R1(config)#router ospf 1 R1(config-router)#router-id 1.1.1.1 R1(config-router)#show ip route connected
Anunciar las redes conectadas directamente	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
Establecer todas las interfaces LAN como pasivas	R1(config-router)#passive-interface g0/1.21 R1(config-router)#passive-interface g0/1.23 R1(config-router)#passive-interface g0/1.99
Desactive la sumarización automática	R1(config-router)#no auto-summary

2.4.2 Paso 2: Configurar OSPF en el R2

Al igual que las tareas de configuración del router R1, en el router R2 se establece una interface lógica *loopback 0* como pasiva, asegurando la estabilidad del protocolo OSPF.

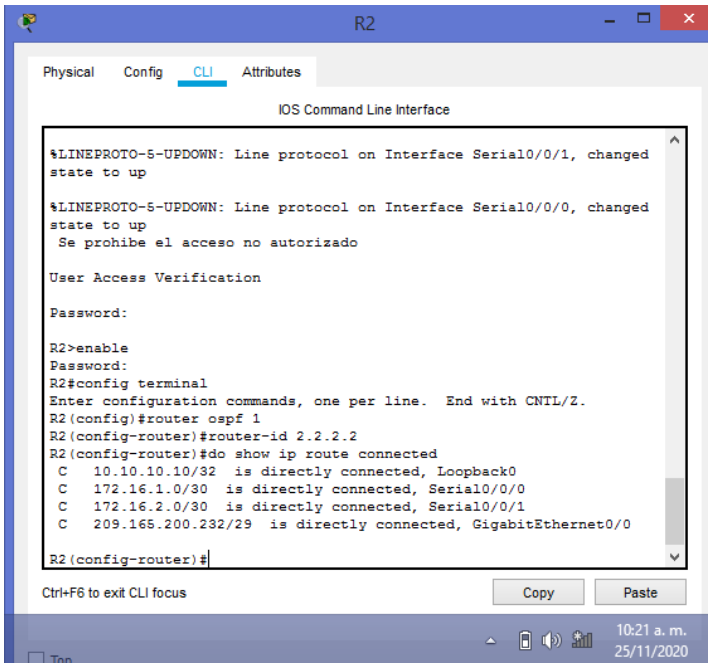
Tabla 28. Configuración del protocolo OSPF en el R2 escenario 2

Tarea	Comando de IOS
Configurar OSPF área 0	Password: cisco R2>enable Password: class R2#config terminal R2(config)#router ospf 1 R2(config-router)#router-id 2.2.2.2 R2(config-router)#show ip route connected
Anunciar las redes conectadas directamente	R2(config-router)#network 10.10.10.10 0.0.0.255 area 0 R2(config-router)#network 172.16.1.0 0.0.0.3 area 0 R2(config-router)#network 172.16.2.0 0.0.0.3 area 0
Establecer la interfaz LAN (loopback) como pasiva	R2(config-router)#passive-interface loopback 0

Tarea	Comando de IOS
Desactive la sumarización automática.	R2(config-router)#no auto-summary

Ejecucion del comando *show ip route connected* en el router R2

Figura 34. Comando show ip route connected en R2 escenario 2



Fuente: Autor

2.4.3 Paso 3: Configurar OSPF en el R3

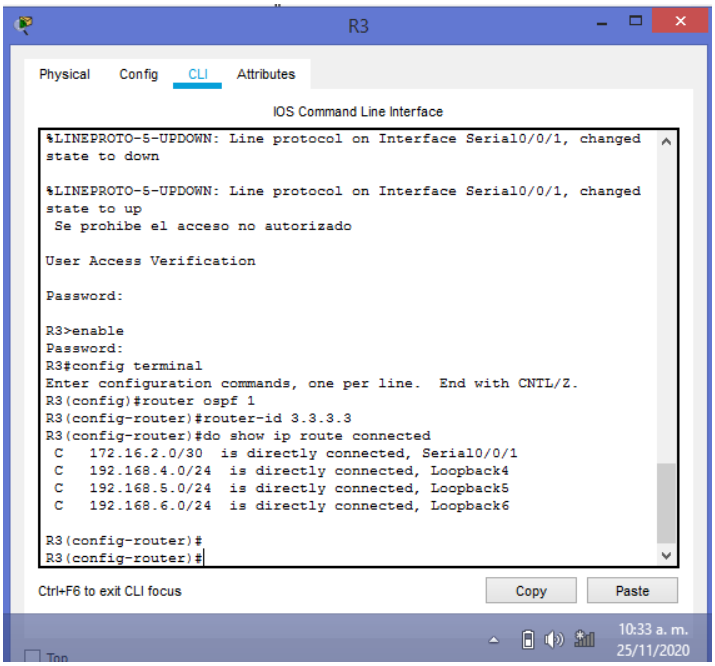
En el router R2 se establecen 3 (tres) interfaces lógicas *loopback 4, loopback 5* y *loopback 6* como pasiva y se continua trabajando con el indicador de área 0 (cero)

Tabla 29. Configuración del protocolo OSPF en el R3 escenario 2

Tarea	Comando de IOS
Configurar OSPF área 0	Password: cisco R3>enable Password: class R3#config terminal R3(config)#router ospf 1 R3(config-router)#router-id 3.3.3.3 R3(config-router)#show ip route connected
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
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	R3(config-router)#passive-interface loopback 4 R3(config-router)#passive-interface loopback 5 R3(config-router)#passive-interface loopback 6
Desactive la sumarización automática.	R3(config-router)#no auto-summary

Ejecucion del comando *show ip route connected* en el router R3

Figura 35. Comando show ip route connected en R3 escenario 2



Fuente: Autor

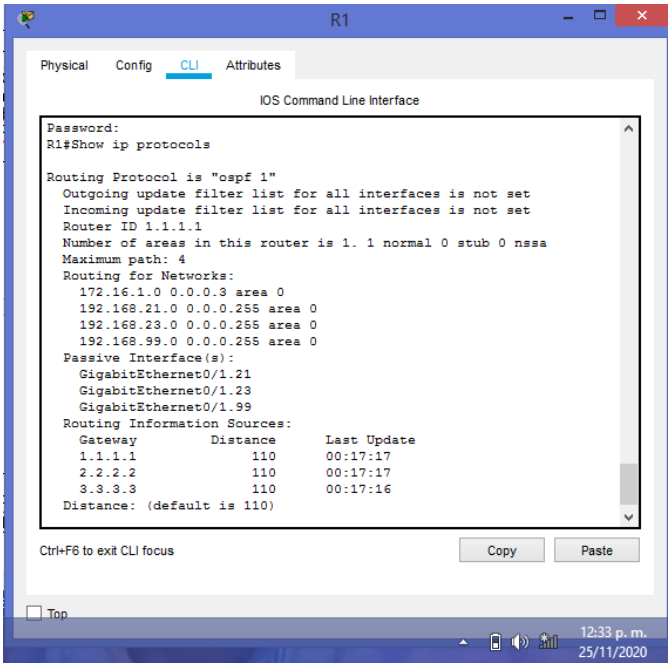
2.4.4 Paso 4: Verificar la información de OSPF

Con el fin de verificar que el protocolo OSPF funcione correctamente se ingresan lo siguientes comando IOS y así obtener información específica como se relaciona en la siguiente tabla.

Tarea	Comando de IOS
¿Con qué comando se muestran la ID del proceso OSPF, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router?	Show ip protocols
¿Qué comando muestra solo las rutas OSPF?	Show ip route ospf
¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	Show running | section router ospf

En *figura 36* se ejecuta el comando *show ip protocols* en el router R1,

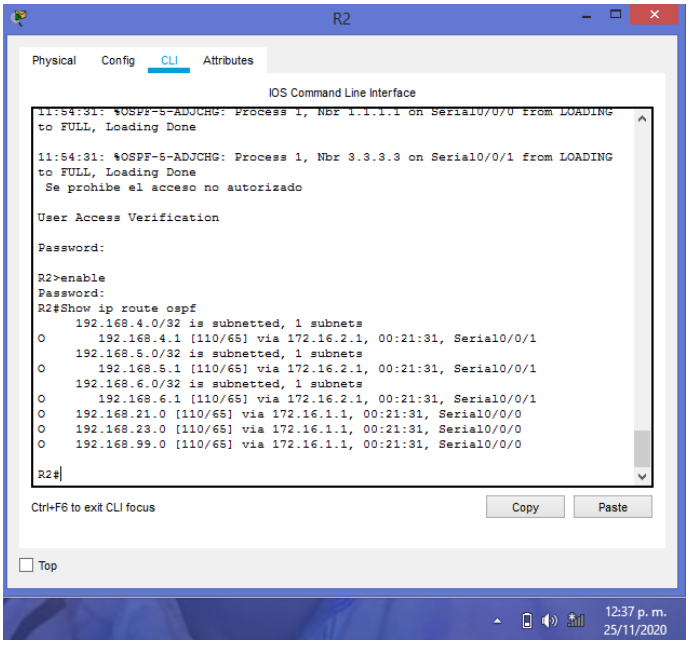
Figura 36. Comando show ip protocols en R1 escenario 2



Fuente: Autor

En *figura 37* se ejecuta el comando *Show ip route ospf* en el router R2

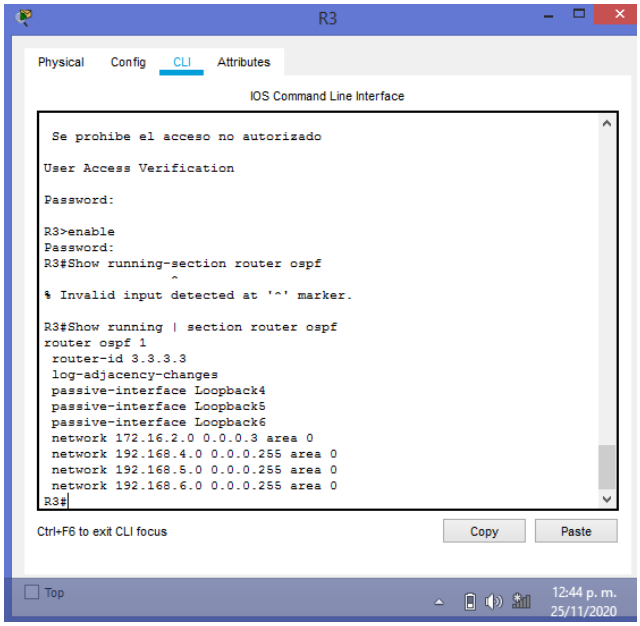
Figura 37. Comando show ip route ospf en R2 escenario 2



Fuente: Autor

En *figura 38* se ejecuta el comando *show running | section router ospf* en el router R3.

Figura 38. Comando show running | section router ospf en R3 escenario 2



Fuente: Autor

2.5 Parte 5: Implementar DHCP y NAT para IPv4

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

El router de Cisco R1 se configura para que funcione como servidor DHCP y como primer tarea, se reservan las primeras 20 (veinte) direcciones IPv4 por medio del comando *ip dhcp excluded-address* seguido del conjunto de direcciones a excluir en la VLAN 21 Contabilidad, el mismo procedimiento se repite para la reservación de las primeras 20 direcciones IP en la VLAN 23 de Ingeniería.

Con el uso del comando *ip dhcp pool* seguido del nombre elegido, que para la presente topología es ACCT, hace que el router ingrese al modo de configuración DHCP, allí se asigna la dirección IPv4 para el servidor DNS, el nombre del dominio, el rango de direcciones disponibles en el router y se define la dirección Gateway predeterminada utilizando el comando *default-router* para la VLAN 21, lo mismo se configura en la VLAN 23 creando un pool de DHCP de nombre ENGNR.

Tabla 30. Configuración del router R1 como servidor de DHCP para las VLAN 21 y 23

Tarea	Comando de IOS
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	Password: cisco R1>enable Password: class R1#config terminal R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20
Crear un pool de DHCP para la VLAN 21.	R1(config)#ip dhcp pool ACCT R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com R1(dhcp-config)#network 192.168.21.0 255.255.255.0 R1(dhcp-config)#default-router 192.168.21.1
Crear un pool de DHCP para la VLAN 23	R1(dhcp-config)#ip dhcp pool ENGNR R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com R1(dhcp-config)#network 192.168.23.0 255.255.255.0 R1(dhcp-config)#default-router 192.168.23.1

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

Luego de ingresar las contraseñas de seguridad, se ingresa al modo de configuración del router R2, una vez aquí, se crea en la base de datos local el nombre de usuario *webuser*, con un nivel de privilegio *15* y contraseña *cisco12345.* El comando *ip http server* e *ip http authentication* no están soportados en Cisco, posteriormente se crea una NAT estática o Network Address Translation, que es el traductor de direcciones de la red, en este dispositivo se asigna como dirección local interna 10.10.10.10 y como dirección global 209.165.200.229; es importante resaltar que los dispositivos conectados por NAT no son perceptibles desde el exterior de la red, una vez realizado lo anterior se configuran las interfaces para la NAT estática.

Por medio del comando *access-list 1 permit* se configura la lista de control de acceso para el filtro y flujo de tráfico, que permita la traducción de las redes asignadas en el router R1 y las redes *loopback* en el router R3. Se define el pool de direcciones IP públicas utilizables de nombre INTERNET y se define la traducción NAT dinámica por medio del comando *ip nat inside source list 1 pool.*

Tabla 31. Configurar la NAT estática y dinámica en el R2

Tarea	Comando de IOS
Crear una base de datos local con una cuenta de usuario	Password: cisco R2>enable Password: class R2#config terminal R2(config)#username webuser privilege 15 secret cisco12345
Habilitar el servicio del servidor HTTP	R2(config)#ip http server
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	R2(config)#ip http authentication
Crear una NAT estática al servidor web.	R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229
Asignar la interfaz interna y externa para la NAT estática	R2(config)#interface g0/0 R2(config-if)#ip nat outside R2(config-if)#interface s0/0/0 R2(config-if)#ip nat inside R2(config-if)#interface s0/0/1 R2(config-if)#ip nat inside R2(config-if)#exit

Tarea	Comando de IOS
Configurar la NAT dinámica dentro de una ACL privada	R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255
Defina el pool de direcciones IP públicas utilizables.	R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248
Definir la traducción de NAT dinámica	R2(config)#ip nat inside source list 1 pool INTERNET

2.5.3 Paso 3: Verificar el protocolo DHCP y la NAT estática

Por medio de las siguientes tareas, se podrá verificar las configuraciones de DHCP y NAT estática configuradas:

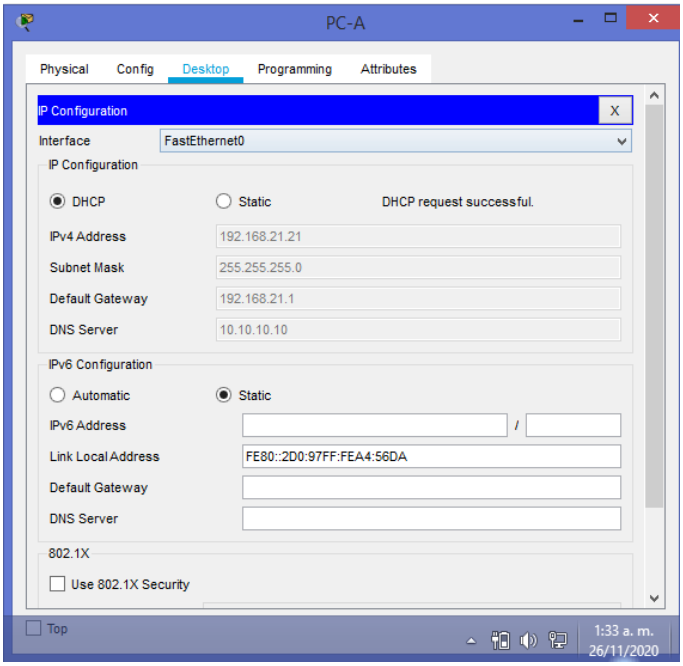
Tabla 32. Verificación del protocolo DHCP y la NAT estática escenario 2

Prueba	Resultado
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	Solicitud exitosa IPv4 Addrress: 192.168.21.21 Subnet Mask: 255.255.255.0 Default gateway: 192.168.21.1 DNS Server: 10.10.10.10
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	Solicitud exitosa IPv4 Addrress: 192.168.23.2 Subnet Mask: 255.255.255.0 Default gateway: 192.168.23.1 DNS Server: 10.10.10.10
Verificar que la PC-A pueda hacer ping a la PC-C	Ping exitoso 4/4 Ping statistics for 192.168.23.2: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 3ms, Average = 1ms

Prueba	Resultado
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	Server Reset Connection

En la *figura 39* se puede verificar que la PC-A ha adquirido información de IP del servidor de DHCP

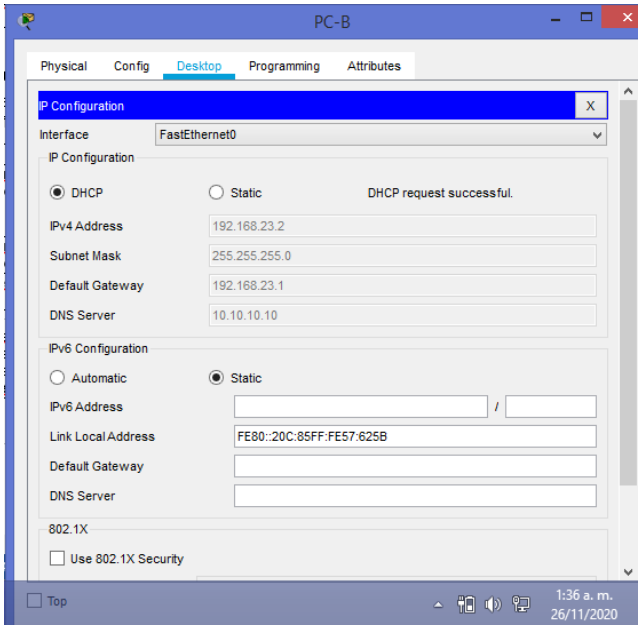
Figura 39. PC-A con información de IP del servidor de DHCP escenario 2



Fuente: Autor

En la *figura 40* se puede verificar que la PC-B ha adquirido información de IP del servidor de DHCP

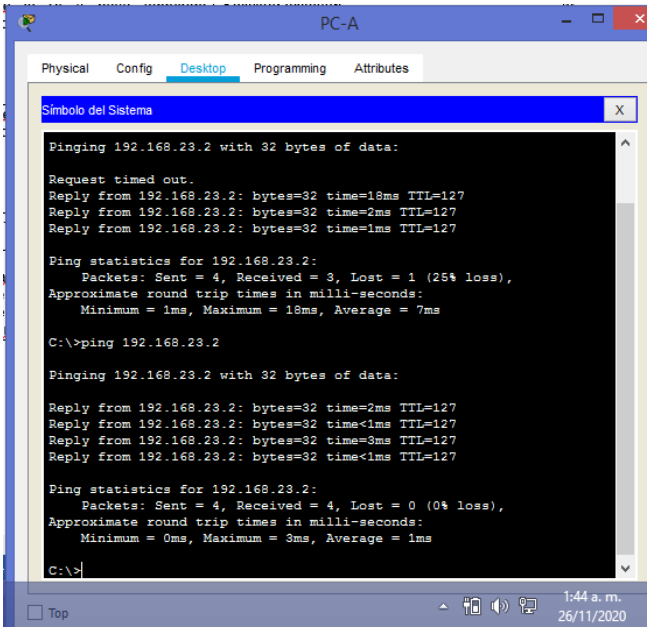
Figura 40. PC-C con información de IP del servidor de DHCP escenario 2



Fuente: Autor

En la *figura 41* se puede verificar que la PC-A puede hacer ping con la PC-C

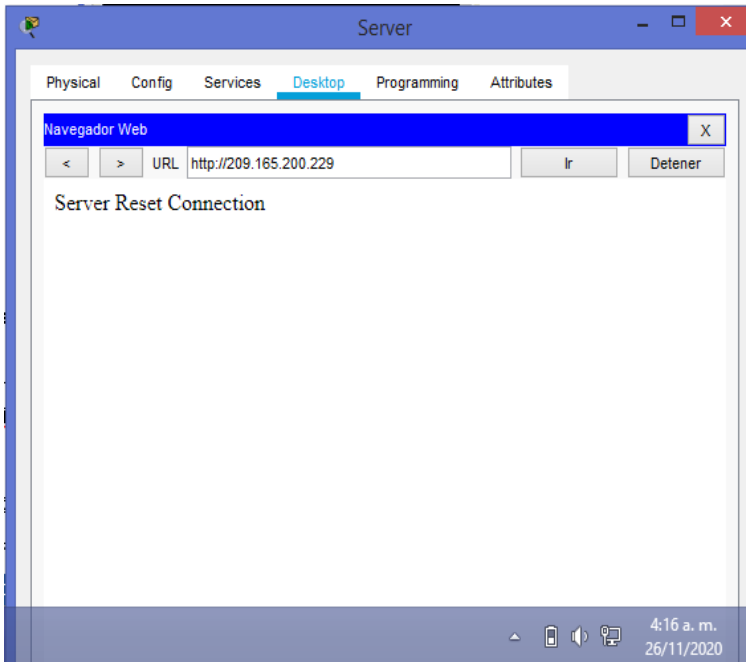
Figura 41. Ping PC-A a la PC-C escenario 2



Fuente: Autor

Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.229)

Figura 42. Navegador web en la computadora de Internet escenario 2



Fuente: Autor

2.6 Parte 6: Configurar NTP

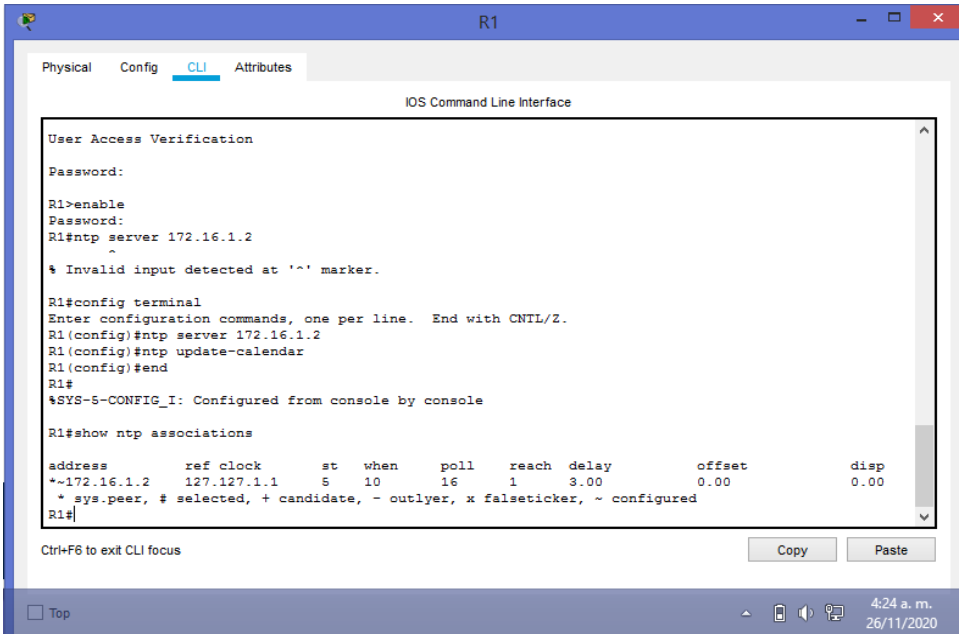
Se accede a la consola del router R2 y se procede a configurar el protocolo NTP, inicialmente se realiza el ajuste de la fecha y hora, para ello se ejecuta el comando *clock set* seguido del formato de hora militar que incluye segundos, se especifica el mes. En la siguiente línea de comando se ingresa a la configuración del terminal y se configura el router R2 como un servidor NTP autorizado de nivel de estrato 5 por medio del comando ntp master, por otro lado se ingresa a la configuración del terminal del router R1 y se configura como un cliente NTP del servidor R2 con la línea de comando *ntp server* seguido de la dirección IPv4 de R2 172.16.1.2. Una vez se está en R1 se aplica el comando *ntp update-calendar* con el fin de que se realice actualizaciones periódicas de calendario con hora NTP.

Tabla 33. Configuración NTP en router R2

Tarea	Comando de IOS
Ajuste la fecha y hora en R2.	Password: cisco R2>enable Password: class R2#clock set 09:00:00 5 March 2016
Configure R2 como un maestro NTP.	R2#config terminal R2(config)#ntp master 5
Configurar R1 como un cliente NTP.	Password: cisco R1>enable Password: class R1#config terminal R1(config)#ntp server 172.16.1.2
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	R1(config)#ntp update-calendar R1(config)#end
Verifique la configuración de NTP en R1.	R1#show ntp associations

Por medio del comando *show ntp associations* se verifica el estado de NTP en el router R1, en el primer dato de salida del comando se puede ver que la dirección IPv4 172.16.1.2 está acompañada en la margen izquierda de los caracteres *~, es decir esta sincronizado con el par del sistema y está configurado estáticamente.

Figura 43. Comando show ntp associations en router R1 escenario 2



Fuente: Autor

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

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

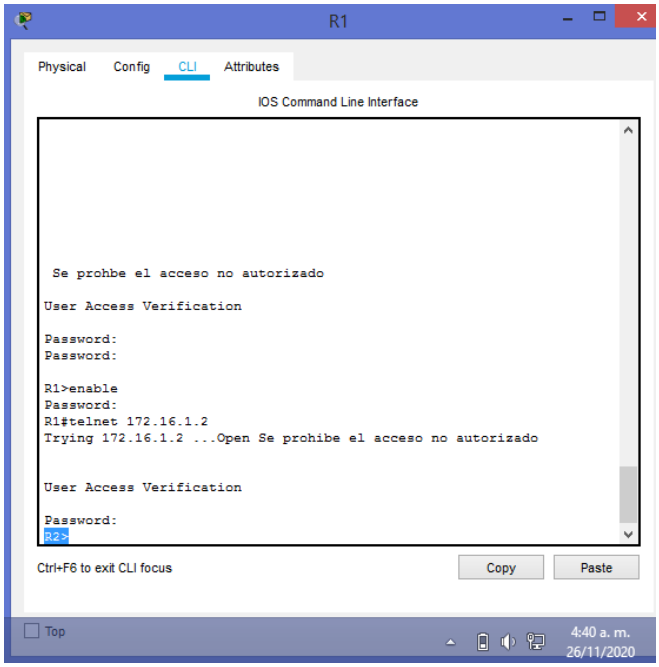
A través del comando *ip access-list standard* se configura la lista de acceso con el nombre de la ACL *ADMIN-MGT* con el objetivo de permitir que solo el router R1 pueda establecer una conexión Telnet con el router R2, estableciendo la estrada y acceso a líneas VTY, con el fin de asegurar la conexión de manera correcta, se deben aplicar los siguientes comandos de las tareas de la *tabla 33*.

Tabla 34. Restricción de acceso a las líneas VTY en el R2

Tarea	Comando de IOS
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	Password: cisco R2>enable Password: class R2#config terminal R2(config)#ip access-list standard ADMIN-MGT R2(config-std-nacl)#permit host 172.16.1.1 R2(config-std-nacl)#exit
Aplicar la ACL con nombre a las líneas VTY	R2(config)#line vty 0 15 R2(config-line)#access-class ADMIN-MGT in
Permitir acceso por Telnet a las líneas de VTY	R2(config-line)#transport input telnet
Verificar que la ACL funcione como se espera	R1>enable Password: R1#telnet 172.16.1.2 Trying 172.16.1.2 ...Open Se prohibe el acceso no autorizado User Access Verification Password: R2>

Finalmente se realiza una verificación de la conexión remota entre los routers R1 y R2, ingresando a la consola de R1 se escribe la línea de comando *telnet 172.16.1.2*, luego solicita la contraseña de seguridad de acceso al dispositivo y se podrá acceder remotamente al router R2 desde R1.

Figura 44. Conexión remota desde el router R1 al router R2



Fuente: Autor

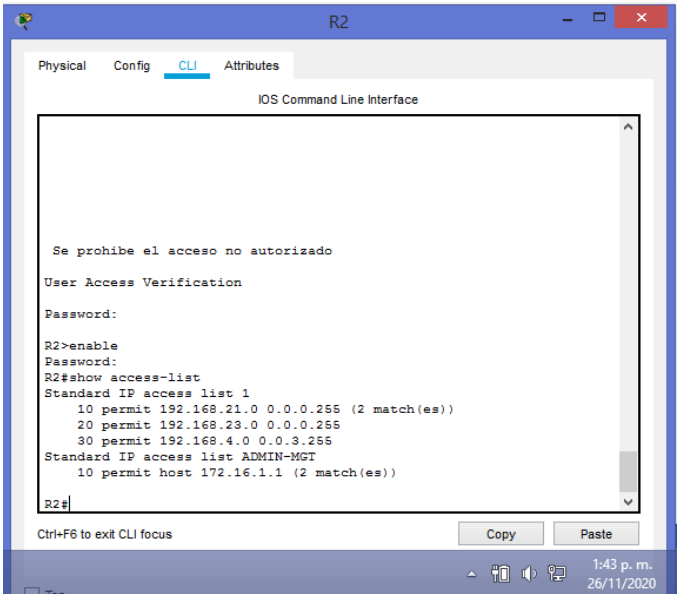
2.7.2 Paso 2: Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente en R2

Tabla 35. Comandos de verificación de información CLI

Tarea	Comando de IOS
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	show access-list
Restablecer los contadores de una lista de acceso	show access-list counters
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	show ip interface
¿Con qué comando se muestran las traducciones NAT?	show ip nat translations
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	clear ip nat translation *

Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció por medio de la ejecución del comando show access-list en el router R2

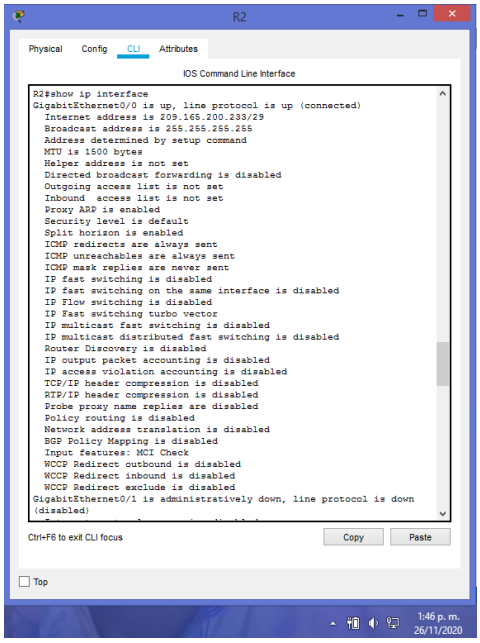
Figura 45. Comando show access-list en R2 escenario 2



Fuente: Autor

El comando *show ip interface* se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica.

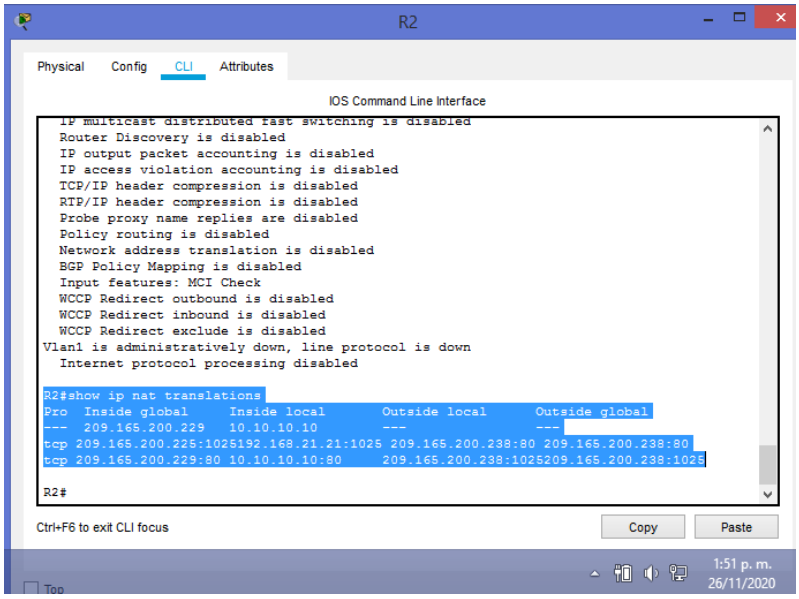
Figura 46. Comando show ip interface en R2 captura 1 escenario 2



Fuente: Autor

En la *figura 49* el comando *show ip nat translations*, muestra las traducciones NAT

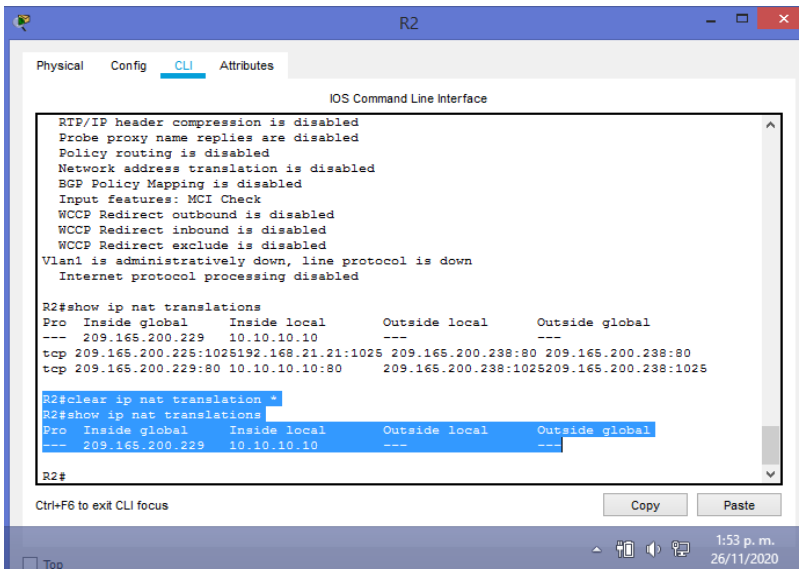
Figura 47. Comando show ip nat translations en R2 escenario 2



Fuente: Autor

En la *figura 50* el comando *clear ip nat translation* * se utiliza para eliminar las traducciones de NAT dinámicas

*Figura 48. Comando clear ip nat translation **



Fuente: Autor

CONCLUSIONES

Los protocolos de seguridad SSH y DNS implementados en los dispositivos que integran la topología de la red de los escenarios 1 y 2, sumado a los niveles de acceso configurados por medio de línea de comando Cisco CLI, ayudan a mantener la información de un sistema seguro y confidencial, además es importante inhabilitar los puertos de acceso de un dispositivo que no se vayan a utilizar y evitar así, posibles accesos no autorizados.

En el escenario 1 por medio de las conexiones remotas, un usuario autorizado puede acceder de manera segura a un dispositivo por medio del protocolo Telnet o el protocolo de red cifrado SSH a través del enrutamiento de la red a la cual pertenece, asegurando el acceso a través de una contraseña para el modo EXEC privilegiado y otra de acceso a la consola de Cisco.

Por medio del modo NAT que es el traductor de direcciones de red, permitió realizar intercambios de paquetes entre dos redes, disminuyendo el agotamiento de direcciones IP válidas, al usar las direcciones válidas para tener acceso a internet.

Por medio de las conexiones remotas, le permite a un usuario autorizado puede acceder de manera segura a un dispositivo por medio del protocolo Telnet o el protocolo de red cifrado SSH a través del enrutamiento de la red a la cual pertenece como es el caso del escenario número 1, asegurando el acceso a través de una contraseña para el modo EXEC privilegiado y otra de acceso a la consola de Cisco.

El escenario número 2 al ser una red configurada con protocolo de ruteo OSPF ayuda a recolectar información para las tablas de ruteo y adyacentes, que converge rápidamente y a su vez facilita la configuración como el mantenimiento para las rutas de conectividad en la red. Por otro lado es importante configurar la hora NTP, la cual incrementa en gran parte la seguridad de la red, evitando que existan discrepancias de tiempo entre los dispositivos administrados en la misma.

Con la ayuda del protocolo de configuración dinámica de host o más conocido como DHCP en el escenario 2, permite asignar automáticamente una dirección IP a un dispositivo que requiere conectarse en la red basada en un modelo cliente-servidor, en lugar de tener que realizar la asignación de las direcciones IP de manera manual.

BIBLIOGRAFÍA

Amazonaws. (sf de sf de 2020). *Protocolo de configuración dinámica de host v4*. Recuperado el 20 de Noviembre de 2020, de Amazonaws: https://static-course-assets.s3.amazonaws.com/RSE50ES/module10/10.1.2.1/10.1.2.1.html#:~:text=Para%20excluir%20direcciones%20espec%C3%ADficas%2C%20utilice,direcci%C3%B3n%20m%C3%A1s%20alta%20del%20rango.

Bitacora Byte. (18 de Julio de 2017). *Configurar DHCP en router CISCO*. Recuperado el 19 de Octubre de 2020, de Bitacora Byte: https://bitacorabyte.wordpress.com/2017/07/18/configurar-dhcp-en-router-cisco/

Cisco. (10 de Agosto de 2005). *Configuración de una puerta de enlace de último recurso mediante comandos IP*. Recuperado el 18 de Octubre de 2020, de Cisco: https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/16448-default.html

Cisco. (10 de Agosto de 2005). *Guía de diseño de OSPF*. Recuperado el 20 de Noviembre de 2020, de Cisco: https://www.cisco.com/c/es_mx/support/docs/ip/open-shortest-path-first-ospf/7039-1.html

Cisco. (21 de Noviembre de 2007). *Información sobre los modos de loopback en routers de Cisco*. Recuperado el 18 de Octubre de 2020, de Cisco: https://www.cisco.com/c/es_mx/support/docs/asynchronous-transfer-mode-atm/permanent-virtual-circuits-pvc-switched-virtual-circuits-svc/6337-atmloopback.html

Cisco. (17 de Agosto de 2013). *Guía de resolución de problemas y depuración de problemas del protocolo de tiempo de red (NTP)*. Recuperado el 21 de Noviembre de 2020, de Cisco: https://www.cisco.com/c/en/us/support/docs/ip/network-time-protocol-ntp/116161-trouble-ntp-00.html

Cisco. (19 de Marzo de 2014). *Verificación del estado de NTP con el comando show ntp association*. Recuperado el 21 de Noviembre de 2020, de Cisco: https://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/ios-software-releases-110/15171-ntpassoc.html

Cisco. (sf de sf de 2020). *Guía de configuración del software del switch Catalyst 3750-X y 3560-X, versión 12.2 (55) SE*. Recuperado el 18 de Octubre de 2020, de Cisco:

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x_3560x/software/release/12-2_55_se/configuration/guide/3750xscg/swsdm.html

Cisco. (30 de Agosto de 2005). *Configuración de EtherChannel y enlace troncal 802.1Q entre switches de configuración fija Catalyst L2 y un enrutador (enrutamiento InterVLAN)*. Recuperado el 22 de Noviembre de 2020, de Cisco: https://www.cisco.com/c/en/us/support/docs/switches/catalyst-2950-series-switches/24042-158.html

ANEXOS

Anexo 1. Link de descarga escenario 1

https://drive.google.com/file/d/1Ft7U8LttEX7XtgEXAio_pLVY8QSzDah3/view?usp=sharing

Anexo 2. Link de descarga escenario 2

https://drive.google.com/file/d/1W08QFlZEHpWDWt-1nwb-WnQtC3NDyYPg/view?usp=sharing

Anexo 3. Link de descarga Artículo científico

https://drive.google.com/file/d/1prR1fIgm8bHp0NbuM2bYA2ahyC0sFE4D/view?usp=sharing

Solución de un escenario bajo el uso de tecnología CISCO que se pueda administrar de forma segura y admita conectividad IPv4 e IPv6.

Duber Andrés Español Rodríguez
Universidad nacional Abierta y a Distancia UNAD, daespanolr@unadvirtual.edu.co

Resumen

En la presente configuración de la topología diseñada y construida en la herramienta de Cisco, Packet Tracer que hace referencia a una red pequeña, se utilizó un router Cisco ISR 4331, 2 switches de red 3560 y 2 equipos PC, para sus conexiones fue necesario utilizar cable de cobre directo. Dentro de las configuraciones básicas, se realiza un borrado de las configuraciones previas que se hubieras presentado en los dispositivos y teniendo en cuenta que es necesario que los dispositivos puedan admitir conectividad IPv4 e IPv6 se configura la plantilla SMD en los dos switches manteniendo un equilibrio de funciones de capa 2 y 3. Pensando en la seguridad de la red, se crea una contraseña cifrada para el acceso al modo EXEC privilegiado, una para el acceso a la consola y se crea un usuario administrativo local, de igual forma se configura las líneas VTY para conexiones seguras SSH. Por otro lado se configura el enrutamiento entre las VLANs, el protocolo DHCP, Etherchannel para los enlaces troncales y port-security que brinda seguridad a los switch.

Palabras clave: Banner Motd, Enlace troncal, Enrutamiento, Red, VLAN.

Abstract:

In the present configuration of the topology designed and built in the Cisco tool, Packet Tracer that refers to a small network, a Cisco ISR 4331 router, 2 3560 network switches and 2 PCs were used, for their connections it was necessary to use direct copper wire. Within the basic configurations, an erasure of the previous configurations that would have been presented in the devices is carried out and taking into account that it is necessary that the devices can support IPv4 and IPv6 connectivity, the SMD template is configured in the two switches maintaining a balance of Layer 2 and 3 functions. Thinking about network security, an encrypted password is created for access to privileged EXEC mode, one for access to the console and a local administrative user is created, in the same way the lines are configured VTY for secure SSH connections. On the other hand, the routing between the VLANs, the DHCP protocol, Etherchannel for the trunk links and port-security that provides security to the switches are configured.

Keywords— Banner Motd, Trunk, Routing, Network, VLAN.

I. INTRODUCCIÓN

El diseño y configuración de la red, presenta una topología de configuración básica, necesaria para la ejecución del proceso de conectividad IPv4 e IPv6 [1], donde se utiliza la plantilla SDM en los dos switches, que permite que el conmutador admite trafico tanto IPv4 como IPv6, la cual da como resultado una menor capacidad de hardware y se ejecuta un conjunto de funciones de LAN [2]. Po medio del protocolo SSH de red cifrada, hace de una red no segura en una red segura, ofreciendo sus servicios para el inicio de sesión de manera remota por parte de los usuarios [3].

En la topología construida en Packet Tracer[4], fue necesario utilizar 2 equipos PC, un router 4331 y 2 switches de red de referencia 3560, los cuales son importantes cuando los host de una VLAN necesitan tener comunicación con el host de otra VLAN [5], entonces es necesario crear link troncales del Etherchannel de punto a punto entre dos dispositivos de una misma red, es de resaltar que Cisco admite protocolo IEEE 802.1Q para la coordinación de los enlaces troncales [6], dentro de la configuración de la infraestructura se crean unas contraseñas de seguridad para los switches y se incorpora un banner [7], que informe al usuario, que el acceso no está autorizado será perseguido con todo el peso de la ley.

Al configurar el protocolo dinámico de host, ayuda a que la topología funcione de manera eficiente y sencilla, el cual hace referencia al protocolo de red cliente/servidor, lo que permite que se comuniquen los dispositivos con otras redes IP. En la actualidad DHCP está presente tanto en redes inalámbricas como mixtas, que se pueden conectar de manera simultánea [8].

II. METODOLOGÍA

El desarrollo del diseño y configuración de la red, se plantea en 4 partes y busca dar solución en la transmisión de paquetes para el proceso de conectividad entre IPv4 e IPv6. Inicialmente se realiza la descripción de los dispositivos que integran la topología de la red y los medios de conexión a utilizar, cable de cobre directo *figura 1*.

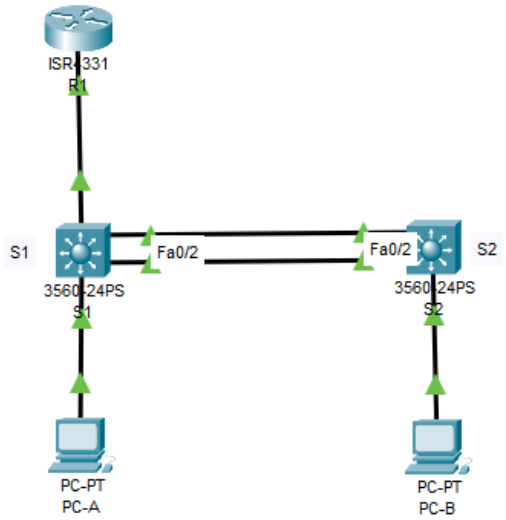


Figura 1. Topología de la red

Posteriormente se realiza un proceso de inicialización y recarga del router y los switches.

Tabla 1. Inicialización y recarga del router y el switch

Tarea	Comando de IOS
Ingresar modo privilegiado del router	Router>enable
Eliminar configuración inicial	Router#erase startup-config
Reiniciar manualmente el router	Router#reload
Ingresar modo privilegiado del switch	Switch>enable
Verificar datos de VLAN en la memoria	Switch#show flash
Eliminar configuración anterior. Confirmar la acción a realizar.	Switch#erase startup-config Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
Reiniciar manualmente el switch	Switch#reload

Ingresando al modo privilegiado, luego por medio del comando de IOS *erase startup-config* se elimina algún tipo de configuración anterior con la que cuente el dispositivo o datos de VLAN en la memoria. Se realiza un reinicio manual de los dispositivos (router y switches) por medio del comando reload, *figura 2*.

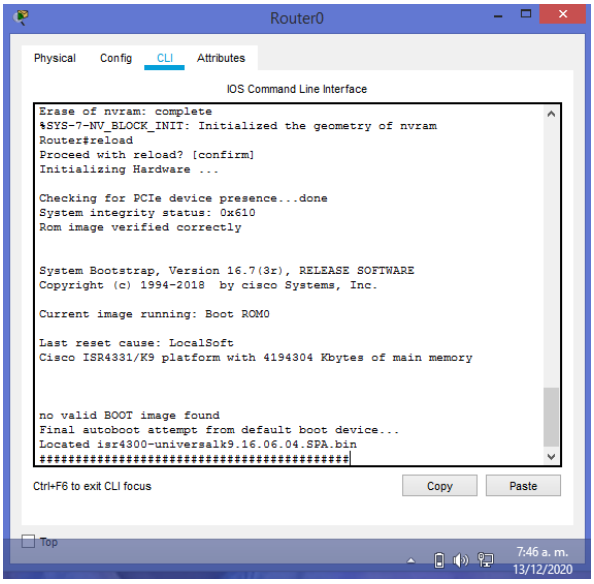


Figura 2. Ejecución comando reload en router

Luego es necesario implementar la plantilla SMD [9] y así poder optimizar la compatibilidad entre IPv4 e IPv6. Se ingresa al modo privilegiado de la configuración global de los dos switches y con el fin de mantener un equilibrio de funciones de las capas 2 y 3, se ejecuta el comando *sdm prefer dual-ipv4-and-ipv6 default.*

Tabla 2. Configuración de la plantilla SDM

Tarea	Comando de IOS
Ingresar modo privilegiado del switch	Switch>enable
Ingresar al modo de configuración global	Switch#config terminal
Plantilla que admite un equilibrio de funciones de Ipv4 e IPv6	Switch(config)#sdm prefer dual-ipv4-and-ipv6 default
Regresar al modo privilegiado	Switch(config)#end
Volver a cargar el sistema. Confirmar la acción a realizar.	Switch#reload System configuration has been modified. Save? [yes/no]:

Para que sea mostrada a información de la plantilla en uso, se ingresa el comando *show sdm prefer* y aparecerá la información de la plantilla activa *figura 3.*

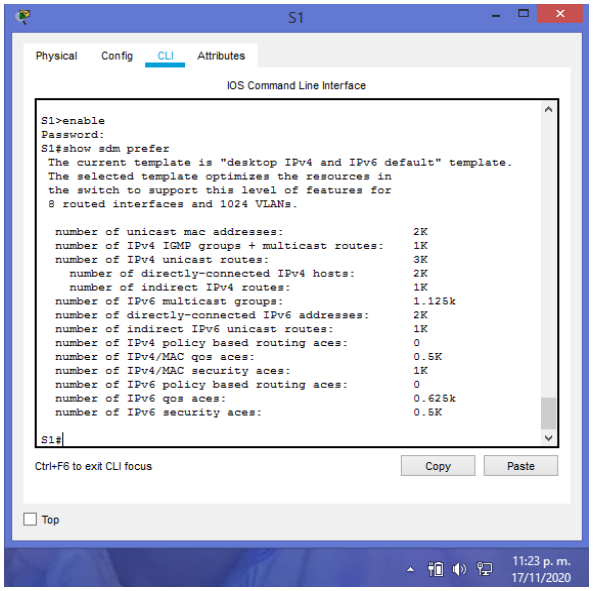


Figura 3. Utilización del comando show sdm prefer en S1

Es importante identificar los nombres de las VLANs *tabla 3* teniendo en cuenta que serán implementadas en la configuración del router R1 en sus subinterfaces, en donde además se inhabilita la búsqueda DNS [10] por medio del comando *no ip domain-lookup*, y se establecen unas contraseñas de seguridad para el acceso al dispositivo, una al modo privilegiado y otra de acceso por consola al momento de conectarse a través de SSH habilitando el inicio de sesión, para ello se utiliza el comando *transport input ssh* y que no admita conexiones Telnet por su inseguridad. Es fundamental encriptar todas las contraseñas que se han creado y las futuras, a través del comando *service password-encryption.*

Tabla 3. Nombres de VLAN

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

De igual manera se protegen los switches S1 y S2, con el cifrado de contraseñas de texto y una clave de cifrado RSA [11] con un módulo de 1024 bits, escribiendo el comando *crypto key generate rsa.*

Como segunda parte, en el switch S1 y S2 se configura la infraestructura de la red, no sin antes ingresar las contraseñas solicitadas para el acceso *ciscoconpass* y al sistema en modo privilegiado *ciscoenpass*. Al ingresar a la configuración del termina, se da inicio a la configuración de las VLANs *tabla 3* mediante el comando *vlan* (número de la vlan) y *name* seguido del nombre que se la va a asignar *tabla 4.*

Tabla 4. Configuración de las VLANs S1

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

Luego se crean los troncos por medio del protocolo 802.1q agregando una etiqueta a cada trama utilizando la id de la VLAN en referencia al comando *switchport trunk native vlan 6* luego se configura el Etherchannel [12].de Capa 2.

En la tercera parte se configura los soportes de host, en el router R1 se asigna una ruta estática por medio del comando *ip route 0.0.0.0 0.0.0.0* para el direccionamiento IPv4 e IPv6 hacia la interface de loopback 0 [13], así mismo se hace uso del protocolo DHCP [14] *tabla 5* para el grupo de VLAN 2 y VLAN 3.

Tabla 5. Configurar soporte de host R1

Tarea	Comando de IOS
Configurar IPv4 DHCP para VLAN 2	R1(config)#ip dhcp excluded-address 10.19.8.1 10.19.8.52 R1(config)#ip dhcp pool vlan2-Bikes R1(dhcp-config)#network 10.19.8.0 255.255.255.192 R1(dhcp-config)#default-router 10.19.8.1 R1(dhcp-config)#domain-name ccna-a.net R1(dhcp-config)#exit
Configurar DHCP IPv4 para VLAN 3	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

Luego de configurar los equipos host PC-A *tabla 6* y PC-B *tabla 7*

Tabla 6. Configuración de red del equipo PC-A

PC-A	
Dirección física	000C.855D.754D
Dirección IP	10.19.8.53
Máscara de subred	255.255.255.192
Gateway predeterminado	10.19.8.1

Gateway predeterminado IPv6	FE80::1

Tabla 7. Configuración de red del equipo PC-B

PC-B	
Dirección física	00D0.D35A.B6C8
Dirección IP	10.19.8.85
Máscara de subred	255.255.255.224
Gateway predeterminado	10.19.8.65
Gateway predeterminado IPv6	FE80::1

Como última parte, se realiza el proceso de verificación de la conectividad IPv4 e IPv6 entre los dispositivos, usando el comando ping [15].

III. RESULTADOS

Al finalizar con la configuración de las 3 partes de la red LAN, que fue implementado en Cisco Packet Tracer, se puede evidenciar la correcta conectividad IPv4 e IPv6 entre todos los dispositivos de la red por medio del comando ping.

La configuración básica de seguridad, una armónica arquitectura de conexión y el protocolo de enlace troncal, evita que personas sin autorización ingresen al sistema y efectúen un posible ataque o en el peor de los casos secuestre información valiosa de la compañía u organización, por tal razón se hizo uso de la encriptación de contraseñas y la configuración de las contraseñas de acceso a la consola y al modo privilegiado.

En la *figura 4* se puede ver el resultado del ping desde PC-A al router R1 con su G0/0//1.2 de dirección IPv4 10.19.8.1

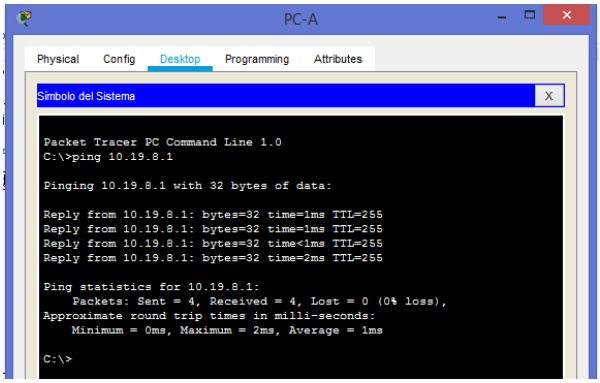


Figura 4. Ping PC-A a R1, G0/0/1.2 IPv4

En la *figura 5* se puede ver el resultado del ping desde PC-A al router R1 con su G0/0//1.2 de dirección IPv6 2001:db8:acad:a::1

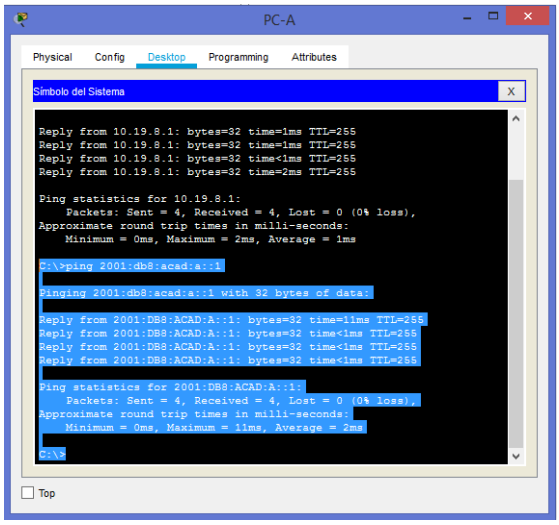


Figura 5. Ping PC-A a R1, G0/0/1.2 IPv6

Finalmente en la *figura 6* se puede observar el correcto funcionamiento de la red pequeña, en equipos que admiten conectividad Ipv4 e IPv6 en los host soportados, para tener una mejor certeza de la afirmación anterior.

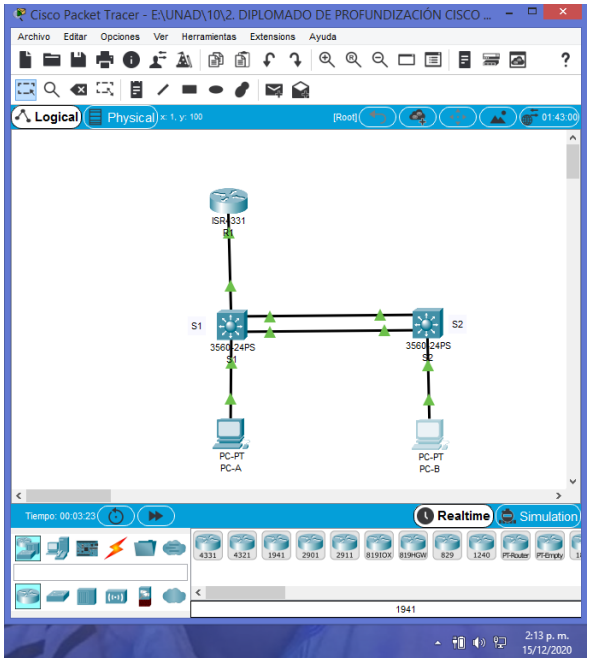


Figura 6. Topología escenario 1 funcionando correctamente

IV. CONCLUSIÓN

Utilizando el protocolo de seguridad de la red, que integra cada uno de los dispositivos de la topología, el enrutamiento entre VLAN, las configuraciones para efectuar conexiones remotas a usuarios autorizados, por medio del protocolo de cifrado SSH y los enlaces troncales, ayudan a mantener una red segura y confidencial, además es importante que como mínimo se creen contraseñas para acceder a los dispositivos

por medio de consola de cisco y modo EXEC privilegiado.

V. Referencias

[1] Cisco. (sf de sf de 2020). Aspectos básicos sobre la conectividad de red: qué tiene que saber. Recuperado el 23 de Noviembre de 2020, de Cisco: https://www.cisco.com/c/es_es/solutions/small-business/resource-center/networking/networking-basics.html.2 (55) SE. Recuperado el 23 de Noviembre de 2020, de Cisco: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x_3560x/software/release/12-2_55_se/configuration/guide/3750xscg/swsdm.html

[2] Cisco. (sf de sf de 2020). Guía de configuración del software del switch Catalyst 3750-X y 3560-X, versión 12.2 (55) SE. Recuperado el 23 de Noviembre de 2020, de Cisco: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x_3560x/software/release/12-2_55_se/configuration/guide/3750xscg/swsdm.html

[3] Cisco. (12 de Octubre de 2016). Configurar el acceso de Telnet o SSH al dispositivo. Recuperado el 23 de Noviembre de 2020, de Cisco: https://www.cisco.com/c/es_mx/support/docs/ip/telnet/200718-Configure-Telnet-SSH-Access-to-Device-wi.html

[4] Netacad. (sf de sf de 2020). Cisco Packet Tracer. Recuperado el 23 de Noviembre de 2020, de Cisco: https://www.netacad.com/es/courses/packet-tracer

[5] Cisco. (20 de Abril de 2016). Configurar routing interVLAN en switches de capa 3. Recuperado el 23 de Noviembre de 2020, de Cisco: https://www.cisco.com/c/es_mx/support/docs/lan-switching/inter-vlan-routing/41860-howto-L3-intervlanrouting.html

[6] Cisco. (sf de sf de sf). Enlaces Troncales de las VLAN. Recuperado el 23 de Noviembre de 2020, de Modulo 3 Cisco : https://sites.google.com/site/paginamodulo3vlan/3-2-enlaces-troncales

[7] Cisco. (sf de sf de 2020). Banner motd. Recuperado el 23 de Noviembre de 2020, de Cisco: https://www.cisco.com/c/m/en_us/techdoc/dc/reference/cli/n5k/commands/banner-motd.html

[8] Carlos, G. (21 de Julio de 2020). Protocolo DHCP: qué es, cómo activarlo y desactivarlo y por qué. Recuperado el 23 de Noviembre de 2020, de adslzone: https://www.adslzone.net/como-se-hace/wifi/activar-dhcp/

[9] Antonio, D. (26 de Abril de 2019). Qué son las SDM Templates. Recuperado el 23 de Noviembre de 2020, de Openwebinars: https://openwebinars.net/blog/cisco-sdm-templates/#:~:text=Las%20SDM%20Templates%20son%20plantillas,un%20gran%20rendimiento%20de%20%C3%A9l.

[10] Cisco. (sf de sf de sf). Configuración de DNS en los routers de Cisco. Recuperado el 23 de Noviembre de 2020, de Cisco: https://www.cisco.com/c/es_mx/support/docs/ip/domain-name-system-dns/24182-reversedns.pdf

[11] Cisco. (16 de Enero de 2018). Generación de claves criptográficas rsa. Recuperado el 23 de Noviembre de 2020, de Cisco: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/a1/sec-a1-xe-3se-3850-cr-book/sec-a1-xe-3se-3850-cr-book_chapter_0110.html

[12] Cisco. (30 de Agosto de 2005). Configuración de EtherChannel y enlace troncal 802.1Q entre switches de configuración fija Catalyst L2 y un enrutador (enrutamiento InterVLAN). Recuperado el 23 de Noviembre de 2020, de Cisco: https://www.cisco.com/c/en/us/support/docs/switches/catalyst-2950-series-switches/24042-158.html

[13] Cisco. (Noviembre de 21 de 2007). Understanding Loopback Modes on Cisco Routers. Recuperado el 23 de Noviembre de 2020, de Cisco: https://www.cisco.com/c/en/us/support/docs/asynchronous-transfer-mode-atm/permanent-virtual-circuits-pvc-switched-virtual-circuits-svc/6337-atmloopback.html

[14] Bitacora Byte. (18 de Julio de 2017). Configurar DHCP en router CISCO. Recuperado el 19 de Octubre de 2020, de Bitacora Byte: https://bitacorabyte.wordpress.com/2017/07/18/configurar-dhcp-en-router-cisco/

[15] Cisco. (28 de Julio de 2006). Uso de los Comandos Ping Extendido y Traceroute Extendido. Recuperado el 23 de Noviembre de 2020, de Cisco: https://www.cisco.com/c/es_mx/support/docs/ip/routing-information-protocol-rip/13730-ext-ping-trace.html.

Biografía

Duber Andrés Español Rodríguez nació en Bogotá Colombia, el 3 de agosto de 1990, vivió durante 11 años en la capital del país junto a sus padres José Español, Dora Rodríguez y su hermano menor William. En el año de 2002 llegan al municipio de la

Belleza Santander, donde viven alrededor de 3 años, posteriormente por razones de fuerza mayor tuvieron que desplazarse hacia la ciudad de Sogamoso Boyacá para el año 2005, en donde se encuentra su familia actualmente. A su familia llega una nueva integrante Dayana, el 26 de enero del año 2007. Siendo mayor de edad, durante los años 2008-2010 presto su servicio militar en el Ejército Nacional de Colombia, para el año 2014 ingresa a la Policía Nacional. Labora desde el año 2018 como servidor público en la ciudad de Montería Córdoba en la oficina de prensa, actualmente es estudiante de la Universidad Nacional Abierta y a Distancia (UNAD) perteneciente a la Escuela de Ciencias Básicas, Tecnología e Ingeniera (ECBTI) el programa de Ingeniería de sistemas.

Cuenta con experiencia en diseño y programación de páginas web, en el editor de fotografías Adobe Photoshop, en el software de edición de videos Adobe Premiere y le gusta plasmar composiciones fotográficas de la naturaleza.