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

DIANA PATRICIA ZUÑIGA CHARA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA *DE SISTEMAS*
VIJES VALLE
2020

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

DIANA PATRICIA ZUÑIGA CHARA

INFORME PARA OPTAR EL TITULO
DE INGENIERA DE SISTEMAS

INGENIERA PAULITA FLOR SALAZAR
TUTORA ASIGNADA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA *DE SISTEMAS*
VIJES VALLE
2020

NOTA DE ACEPTACIÓN

_____
_____
_____
_____
_____
_____
_____

_____
Firma del Presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

VIJES - VALLE, 30 de noviembre de 2020

AGRADECIMIENTOS

Deseo agradecer a mis tíos por su apoyo constante desde que ingrese a la universidad, a mis padres y a mi hija por su paciencia y comprensión.

Les agradezco a la universidad nacional abierta y a distancia UNAD todos los compañeros y a los tutores que me acompañaron en esta etapa de aprendizaje especialmente a mi tutora Paulita flor por guiarme en este curso

Quiero agradecer a todas las personas que de una otra manera me apoyaron para cumplir esta meta en mi vida

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

DHCP: minimiza los errores al configurar las direcciones IP de forma manual.se utiliza para asignar las direcciones IP de forma automática.

DNS (Nombres de dominio): Traduce los nombres de host a direcciones IP para ser entendidos por la computadora.

Gateway: es la puerta de enlace que permite la conexión entre la red inicial y la red de destino.

IP: (Internet Protocolo) es una dirección única y permite identificar cada elemento en una red, facilita las comunicaciones en la mayoría de las redes.

IPv4: son direcciones de 32 bits que se utiliza para identificar in dispositivo que está en una red.

IPv6: son direcciones de 128 bits, que se utiliza para identificar una red, es una actualización de las direcciones Ipv4.

Loopback: Interface que dirige el tráfico hacia ellos mismos.

OSPF: (Open Shortest Path First) es un protocolo de red y construye un enlace dinamicoen los routers de la zona.

Packet tracert: Programa de Cisco basado en la simulación en la infraestructura y configuración de dispositivos para crear una red.

Router: Dispositivo que conecta los dispositivos entre sí, establece la ruta que tendrá cada paquete dentro de la red.

RESUMEN

Este informe se realiza para culminar el diplomado de profundización de cisco, las prácticas se desarrollaron en packet tracert que nos permitió crear los escenarios, los cuales nos pueden ayudar en nuestra vida aplicando estos conocimientos.

En este ejercicio se solucionara dos escenarios seleccionados, se documentará cada paso de la configuración de los dispositivos en cada escenario de la red solucionados en la red, al final se verificara la conectividad por medio de comandos, se manejan la conectividad de los equipos configurándolos con dirección ip e ipv6, con protocolos de enrutamiento dinámico, configuración de acceso mediante ssh o telnet, configuración de DHCP y NAT, se configura NTP, se verifica la conectividad para dar solución a los ejercicios.

Palabras claves Cisco, Packet tracert, redes, ipv4, ipv6, vlan y DHCP.

ABSTRACT

This report is done to complete the Cisco in-depth diploma, the practices were developed in packet tracert that allowed us to create the scenarios, which can help us in our lives by applying this knowledge.

In this exercise, two selected scenarios will be solved, each step of the configuration of the devices in each scenario of the network solved in the network will be documented, at the end the connectivity will be verified by means of commands, the connectivity of the equipment is managed by configuring them with IP and IPv6 address, with dynamic routing protocols, access configuration through ssh or telnet, DHCP and NAT configuration, NTP is configured, connectivity is verified to solve the exercises.

Keywords: Cisco, Packet tracert, networks, ipv4, ipv6, vlan and DHCP NAT.

INTRODUCCIÓN

En la actualidad que todos los negocios necesitan estar conectado en la red por ese motivo es importante aprender las habilidades necesarias para conocer como configurar el sistema de redes, logrando de esa manera una conectividad óptima en las empresas,

En este documento muestra los conocimientos que los administradores de red deben tener para cumplir los lineamientos de las topologías de red, mediante instalación, configuración, se desarrollan en el simulador de packet tracert, se mejoran las habilidades al mostrar la configuración de estos dos escenarios, mostrando los comandos más utilizados e importantes en el momento de configurar.

En el primer escenario se desarrolla en packet tracert los conocimientos básicos en las configuración del router, switch y computadores, se configuran las interfaces, se le asignan direcciones Ipv4 e ipv6, se ejecutan las dirección en los computadores se realizan por medio de DHCP y se verifican que las conexiones entre los equipos sea de forma satisfactoria

DESARROLLO

1 - Realizar el escenario

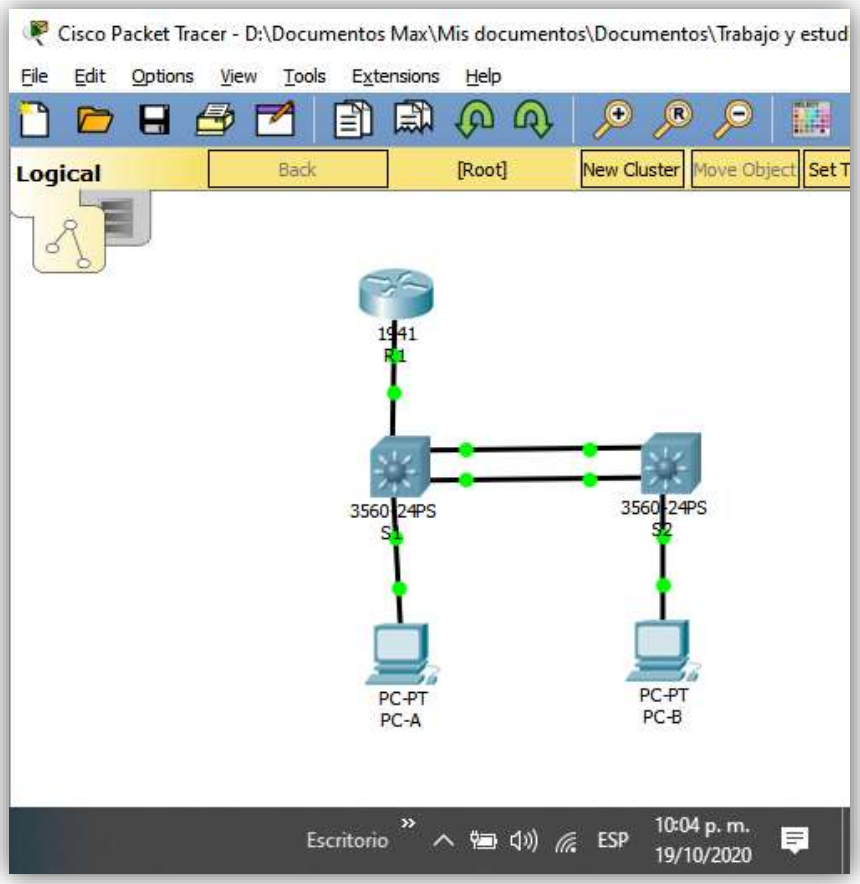


Figura 1 - Primer escenario

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
R1 G0/0/1.2	10.19.8.1 /26	.192
R1 G0/0/1.2	2001:db8:acad:a: :1 /64	No corresponde
R1 G0/0/1.3	10.19.8.65 /27	.224
R1 G0/0/1.3	2001:db8:acad:b: :1 /64	No corresponde
R1 G0/0/1.4	10.19.8.97 /29	.248
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	.224
R1 Loopback0	2001:db8:acad:209: :1 /64	No corresponde
S1 VLAN 4	10.19.8.98 /29	10.19.8.97
VLAN S1 4	2001:db8:acad:c: :98 /64	No corresponde
S1 VLAN 4	fe80: :98	No corresponde
S2 VLAN 4	10.19.8.99 /29	10.19.8.97
S2 VLAN 4	2001:db8:acad:c: :99 /64	No corresponde
S2 VLAN 4	fe80: :99	No corresponde
PC-A NIC	Dirección DHCP para IPv4	DHCP para puerta de enlace predeterminada IPv4
PC-A NIC	2001:db8:acad:a::50 /64	fe80::1
PC-B NIC	DHCP para dirección IPv4	DHCP para puerta de enlace predeterminada IPv4
PC-B NIC	2001:db8:acad:b::50 /64	fe80::1

Tabla 1 - tabla de direccionamiento escenario 1

1.1 : descripción escenario 1.

Este escenario representa una empresa pequeña que compro dos computadores y necesitan ser configurados dos computadores, un switch y un router siendo administrados de manera segura. Se debe configurar el DHCP. Enrutamiento y DHCP.

1.1.2 : Configuración básica y de direccionamiento de los dispositivos.

Al configurar un router lo primero que se realiza antes de configurarlo es recargar en este caso los switch y el router y se eliminan la Vlan y configuraciones antiguas del router y del switch para volverlo a cargar para empezar a configurarlo.

Router

Tarea	Comando
Acceder al modo privilegiado	Router> enable
Configurar el terminal	Router # configure terminal
Borrar configuración de inicio	R1 #erase startup-config
Recargar el router y eliminar Escribir que no para el dialogo de configuración inicial	R1 #reload Would you like to enter the initial configuration dialog? [yes/no] : no

Tabla 2 Borrar configuración Router

Switch1 y Switch 2; se realiza lo mismo en ambos Switch y se utiliza la plantilla ***sdm prefer dual-ipv4-and-ipv6 default*** para que reconozca las direcciones IPv6 y los comandos de dicha dirección

Tarea	Comando
Acceder al modo privilegiado	Switch> enable
Configurar el terminal	Switch # configure terminal
Recargar el switch y eliminar Con enter se confirma	Switch# reload Proceed with reload? [confirm]
Borrar configuración de inicio	Switch# erase startup-config

Configura la plantilla sdm para aceptar IPv6	*Switch(config)#sdm prefer dual-ipv4-and-ipv6 default*
Recargar el switch y eliminar Con enter se confirma	Switch# reload Proceed with reload? [confirm]

Tabla 3 - Borrar configuración switch

1.1.3 : Configurar R1

En este paso se realizan las configuraciones básicas del router, es importante realizar estas configuraciones para que el router funcione correctamente. Esto se hace para poder conectar cualquier dispositivo, en la red asegurarla. La forma más común de realizar esta configuración es por la línea de comandos Cli en el router en packet tracert. Todos los comandos realizados de esta manera son ejecutadas seguidamente al ser ejecutadas

Tarea	Comando
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	Router (config)#hostname R1
Nombre de dominio ccna-lab.com	R1(config)#ip domain name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	R1(config)#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 10 caracteres	R1(config)# security passwords min-length 10
Crear un usuario administrativo en la base de datos local Nombre de usuario: admin Password: admin1pass	R1(config)#username admin password 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
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Configure un MOTD Banner	R1(config)#banner motd "#Acceso restringido a usuarios no autorizado"
Habilitar el routing IPv6	R1(config)#ipv6 unicast-routing
Configurar interfaz G0/0/1 y subinterfaces Establezca la descripción Establece la dirección IPv4. Establezca la dirección local de enlace IPv6 como fe80: :1 Establece la dirección IPv6. Activar la interfaz.	R1(config)#int g0/0/1 R1(config-if)#no ip address R1(config)#interface g0/0/1.2 R1(config-subif)#description link PCA R1(config-subif)#ip address 10.19.8.1 255.255.255.192 R1(config-subif)#ipv6 address 2001:db8:acad:a::1/64 R1(config-subif)#ipv6 address fe80::1 link-local R1(config-subif)#encapsulation dot1Q 2 R1(config-subif)#no sh R1(config)#interface g0/0/1.3 R1(config-subif)#description link PCB R1(config-subif)#ip address 10.19.8.65 255.255.255.224 R1(config-subif)#ipv6 address 2001:db8:acad:b::1/64 R1(config-subif)#ipv6 address fe80::1 link-local R1(config-subif)#encapsulation dot1Q 3 R1(config-subif)#no sh R1(config-subif)#exit R1(config)#interface g0/0/1.4 R1(config-subif)#description link Vlan R1(config-subif)#ip address 10.19.8.97 255.255.255.248 R1(config-subif)#ipv6 address 2001:db8:acad:c::1/64 R1(config-subif)#ipv6 address fe80::1 link-local R1(config-subif)#encapsulation dot1Q 4 R1(config-subif)#no sh R1(config-subif)#exit R1(config)#exit

Establezca la descripción Establece la dirección IPv4. Establece la dirección IPv6. Configure el Loopback0 interface Establezca la dirección local de enlace IPv6 como fe80::1	R1(config)#interface loopback 0 R1(config-if)#ip address 209.165.201.1 255.255.255.224 R1(config-if)#ipv6 address 2001:db8:acad:209::1/64 R1(config-if)#ipv6 address fe80::1 link-local R1(config-if)#no shutdown
Generar una clave de cifrado RSA	R1(config)#crypto key generate rsa % Do you really want to replace them? [yes/no]: yes The name for the keys will be: R1.ccna-lab.com Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes. How many bits in the modulus [512]: 1024 % Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

Tabla 4 Configuración básica R1

1.1.4 : Configure S1 y S2

Se realizan las configuraciones básicas del Switch 1 y Switch 2, en este caso elegi los switch 3560 que permitia las dirección IPv6 e Ipv4 al mismo tiempo. Las configuraciones básicas como cambiar el nombre, agregar las direcciones en las Vlan 4

S1

Tarea	Comandos
Desactivar la búsqueda DNS.	Switch(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S1
Nombre de dominio ccna-lab.com	S1(config)#ip domain name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	S1(config)#line console 0 S1(config-line)#password ciscoconpass

Ciscoenpass	S1(config-line)#login S1(config-line)#exit
Contraseña de acceso a la consola	Ciscoconpass S1(config)# enable secret ciscoenpass
Crear un usuario administrativo en la base de datos local Nombre de usuario: admin Password: admin1pass	S1(config)#username admin password admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	S1(config)#line vty 0 4 S1(config-line)#login local
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S1(config-line)#transport input ssh
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption
Configurar un MOTD Banner	S1(config)#banner motd "#Acceso restringido a usuarios no autorizado"
Generar una clave de cifrado RSA Módulo de 1024 bits	S1(config)#crypto key generate rsa How many bits in the modulus [512]: 1024 % Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
Configurar la interfaz de administración (SVI) Establecer la dirección IPv4 de capa 3 Establezca la dirección local de enlace IPv6 como FE80: :98 para S1 y FE80: :99 para S2	S1#ip routing 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)#no sh
Configuración del gateway predeterminado Configure la puerta de enlace predeterminada como 10.19.8.97 para IPv4	S1(config)# ip default-gateway 10.19.8.97

Tabla 5- Configuración básica S1

S2 Realizamos la misma configuración de Switch 1 en Switch 2

Tarea	Comando
Desactivar la búsqueda DNS.	Switch(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S2
Nombre de dominio ccna-lab.com	S2(config)#ip domain name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado Ciscoenpass	S2(config)#line console 0 S2(config-line)#password ciscoconpass S2(config-line)#login S2(config-line)#exit
Contraseña de acceso a la consola Ciscoconpass	S2(config)# enable secret ciscoenpass
Crear un usuario administrativo en la base de datos local Nombre de usuario: admin Password: admin1pass	S2(config)#username admin password admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	S2(config)#line vty 0 4 S2(config-line)#login local
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S2(config)#line vty 0 4 S2(config-line)#transport input ssh
Cifrar las contraseñas de texto no cifrado	S2(config)#service password-encryption
Configurar un MOTD Banner	S2(config)#banner motd "#Acceso restringido a usuarios no autorizado"
Generar una clave de cifrado RSA Módulo de 1024 bits	S2(config)#crypto key generate rsa How many bits in the modulus [512]: 1024 % Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
Configurar la interfaz de administración (SVI) Establecer la dirección IPv4 de capa 3 Establezca la dirección local de enlace IPv6 como FE80: :98 para S1 y FE80: :99 para S2	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)#no shutdown

Configuracilacpse utilizapara unir ón del gateway predeterminado Configure la puerta de enlace predeterminada como 10.19.8.97 para IPv4	S2(config-if)# ip default-gateway 10.19.8.97

Tabla 6 - Configuración básica S2

1.2 - Configuración de la red (VLAN, Trunking, EtherChannel)

En esta parte se utiliza un router para direccionar las redes entre Vlans, para realizar una comunicación entre vlans que están en un switch, se realiza por trunk que direcciona todo el tráfico hacia el router, es importante nombrarlas para poder identificar las diferentes vlans. A razón de este escenario se va a realizar con el estándar IEEE802.1Q de encapsulamiento de tramas.

El protocolo LACP se utiliza para agrupar varios enlaces y funciona con dispositivos de proveedores distintos

1.2.1: Configurar S1

Tareas	Comando
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)# %LINK-5-CHANGED: Interface Vlan3, changed state to up S1(config-vlan)#name Trikes S1(config-vlan)#exit S1(config)#Vlan 4 S1(config-vlan)# %LINK-5-CHANGED: Interface Vlan4, changed state to up S1(config-vlan)#name Management S1(config-vlan)#exit S1(config)#Vlan 5 S1(config-vlan)# %LINK-5-CHANGED: Interface Vlan5, changed state to up S1(config-vlan)#name Parking S1(config-vlan)#exit S1(config)#Vlan 6 S1(config-vlan)#name Native S1(config-vlan)#exit S1(config)#
Crear troncos 802.1Q que utilicen la VLAN 6 nativa Interfaces F0/1, F0/2 y F0/5	S1(config)#interface range f0/1, f0/2, f0/5 S1(config-if-range)#switchport mode trunk S1(config-if-range)#switchport trunk native vlan 6

	S1(config-if-range)#switchport trunk allowed vlan 2,3,4,5,6 S1(config-if-range)# switchport trunk encapsulation dot1q S1(config-if)#exit
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2 Usar el protocolo LACP	S1(config)#interface range fa0/1, fa0/2 S1(config-if-range)#channel-protocol lacp S1(config-if-range)#channel-group 2 mode active S1(config-if-range)#exit
Configurar el puerto de acceso de host para VLAN 2 Interface F0/6	S1(config)#interface f0/6 S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 2 S1(config-if)#no shut
Configurar la seguridad del puerto en los puertos de acceso Permitir 3 direcciones MAC	S1(config-if)#switchport mode access S1(config-if)#switchport port-security maximum 3 S1(config-if)#switchport port-security violation shutdown S1(config-if)#switchport port-security mac-address 0001.422C.C5B3 S1(config-if)#switchport port-security mac-address 0001.C97B.6173 S1(config-if)#switchport port-security mac-address 0002.1671.8082
Proteja todas las interfaces no utilizadas Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar	S1(config-if)#interface range f0/3-4, f0/7-24, g0/1-2 S1 (config-if-range)#switchport acces vlan 5 S1(config-if-range)#switchport mode Access S1(config-if-range)#description SW1-v5 S1(config-if-range)#sh

Tabla 7 -VLAN, Trunking, EtherChann S1

1.1.2: Configure el S2

Switch 2

Tarea	Comando
Crear VLAN VLAN 2, name Bikes VLAN 3, name Trikes VLAN 4, name Management	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

VLAN 5, nombre Parking VLAN 6, nombre Native	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, fa0/2 S2(config-if-range)#switchport mode trunk S2(config-if-range)#switchport trunk native vlan 6 S2(config-if-range)#switchport trunk allowed vlan 2,3,4,5,6 S2(config-if-range)# switchport trunk encapsulation dot1q S2(config-if-range)#exit
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2 Usar el protocolo LACP para la negociación	S2(config)#interface range fastEthernet 0/1-2 S2(config-if-range)#channel-protocol lacp S2(config-if-range)#channel-group 2 mode passive S2(config-if-range)#exit
Configurar el puerto de acceso del host para la VLAN 3 Interfaz F0/18	S2(config)#interface f0/18 S2(config-if)#switchport mode access S2(config-if)#switchport access vlan 3 S2(config-if-range)#no sh
Configure port-security en los access ports permite 3 MAC addresses	S2(config)#interface f0/18 S2(config-if)#switchport mode access S2(config-if)#switchport port-security maximum 3 S2(config-if)#switchport port-security violation shutdown S2(config-if)#switchport port-security mac-address 0001.422C.C5B3 S2(config-if)#switchport port-security mac-address 0001.C97B.6173 S2(config-if)#switchport port-security mac-address 0002.1671.8082
Asegure todas las interfaces no utilizadas. Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar	S2(config)# interface range f0/3-17, f0/19-24, g0/1-2 S2(config-if-range)#switchport acces vlan 5 S2(config-if-range)#switchport mode access S2(config-if-range)#switchport nonegotiate

	S2(config-if-range)#description SW2-v5 S2(config-if-range)#sh S2#wr

Tabla 8- VLAN, Trunking, EtherChannel S2

1.3 - Configurar soporte de host

1.3.1: Configure R1

En este paso se configura la interface loopback, la cual al configurar la ip, se logra una mejor conectividad porque es una interfaz virtual, en este caso se va a configurar tanto ipv4 e ipv6, configurar el DHCP para que la PCA y la PCB tengan direccionipv4 dinámicas, que se actualicen solas

Tarea	comandos
Configure Default Routing Crear rutas predeterminadas para IPv4 e IPv6 que dirijan el tráfico a la interfaz Loopback 0	R1(config)#ip route 0.0.0.0 0.0.0.0 10.19.8.98 R1(config)#ip route 0.0.0.0 0.0.0.0 10.19.8.99
Configurar IPv4 DHCP para VLAN 2 configurar Asigne el nombre de dominio ccna-a.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada	R1(config)#ip dhcp pool vlan2 R1(dhcp-config)#network 10.19.1.0 255.255.255.0 R1(dhcp-config)#default-router 10.19.1.1 R1(dhcp-config)#exit R1(config)#ip domain-name ccna-a.net R1(dhcp-config)#dns-server 10.0.0.10 R1(dhcp-config)#exit
Configurar DHCP IPv4 para VLAN 3 Cree un grupo DHCP para VLAN 3, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio ccna-b.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada	R1(config)#ip dhcp pool vlan3 R1(dhcp-config)#network 10.19.1.0 255.255.255.0 R1(dhcp-config)#default-router 10.19.1.1 R1(dhcp-config)#exit R1(config)#ip domain-name ccna-a.net R1(dhcp-config)#dns-server 10.0.0.10 R1(dhcp-config)#exit R1# ip dhcp excluded-address 10.19.1.1 10.19.1.99

Tabla 9 - Configurar Host R1

1.4 - Configurar los equipos

Configure los equipos host PC-A y PC-B para que utilicen DHCP para IPv4 y asigne estáticamente las direcciones IPv6 GUA y Link Local. Después de

configurar cada servidor, registre las configuraciones de red del host con el comando **ipconfig /all**

En este paso se configuran el equipo red PC-A y PC-B por medio de DHCP, al estar conectadios se verifica la informaicon cin el comando ipconfig all y se anexanl los datos

PC-A	
Descripción	*en blanco*
Dirección física	*00D0.97E2.9876*
Dirección IP	*10.19.8.52*
Dirección Ipv6	*FE80::2E0:A3FF:FE04:AA0/64*
Máscara de subred	*255.2 55.255.192*
Gateway predeterminado	*10.19.8.1*
Gateway predeterminado IPv6	*FE80::11*

Tabla 10 - Información PC-A

PC-B	
Descripción	
Dirección física	*0040.0B1B.8DE0*
Dirección IP	*10.19.8.84*
Dirección Ipv6	*2001:DB8:ACAD:B::50*
Máscara de subred	*255.255.255.224*
Gateway predeterminado	*10.19.8.65*
Gateway predeterminado IPv6	*FE80::1*

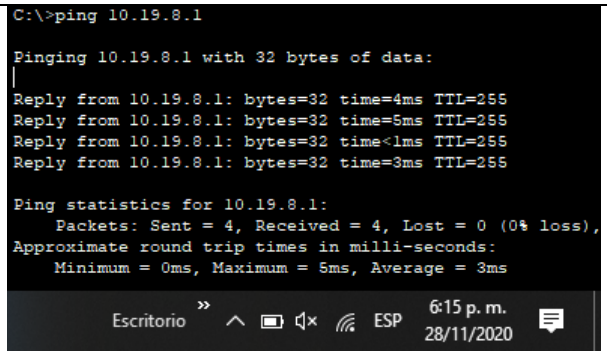
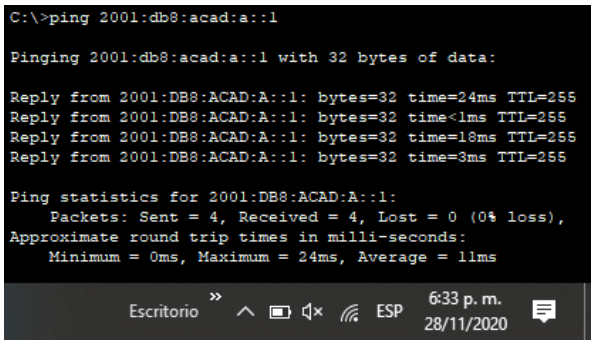
Tabla 11 - Información PC-A

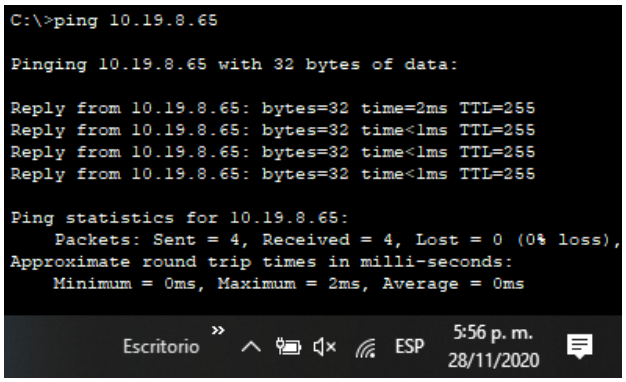
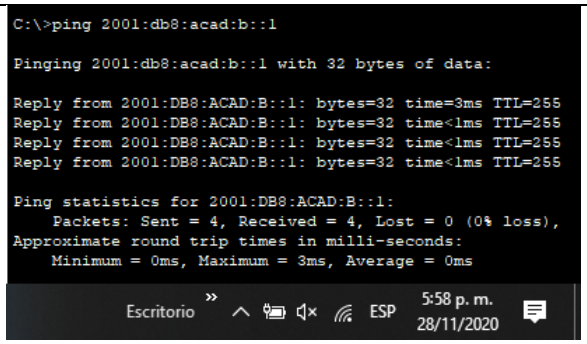
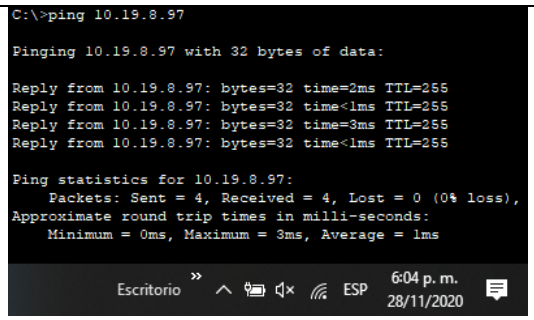
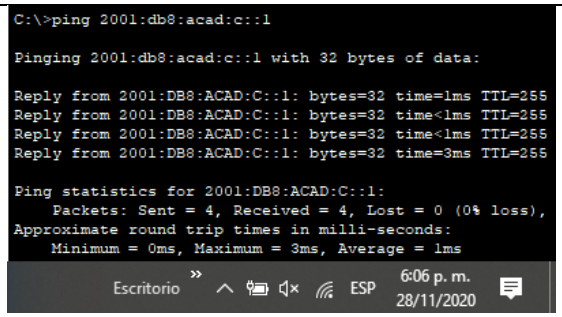
1.5 - Probar y verificar la conectividad de extremo a extremo

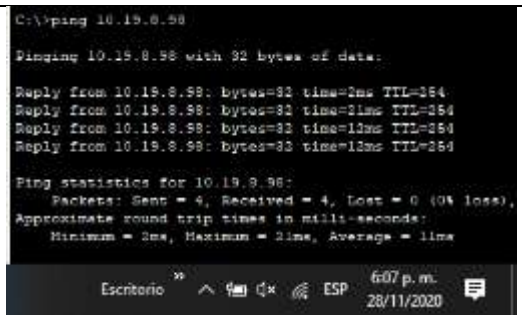
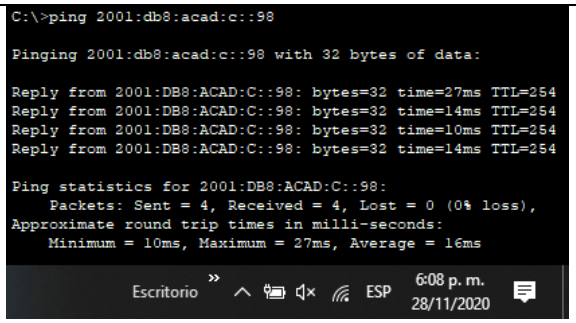
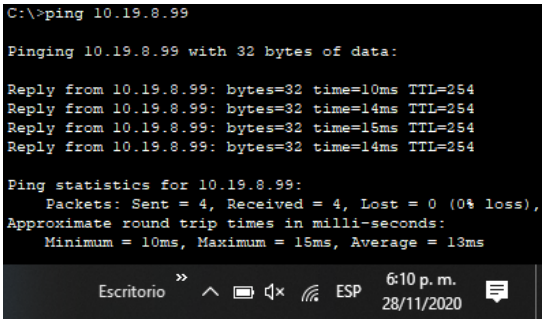
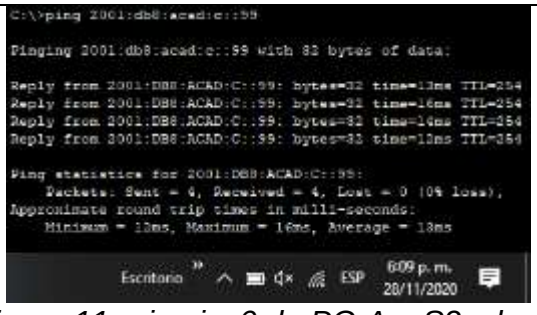
Use el comando ping para probar la conectividad IPv4 e IPv6 entre todos los dispositivos de red.

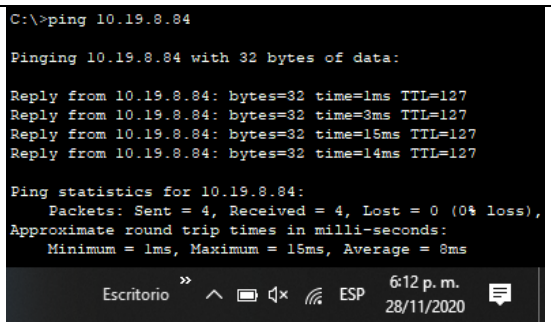
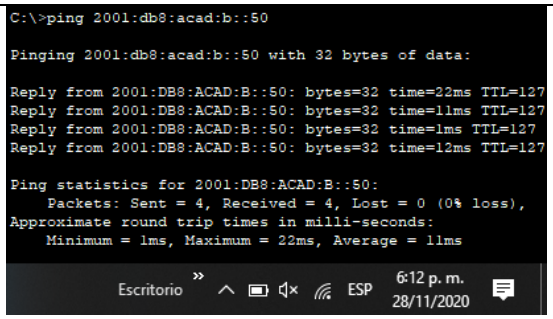
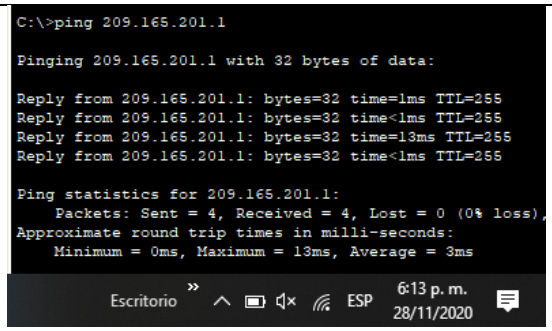
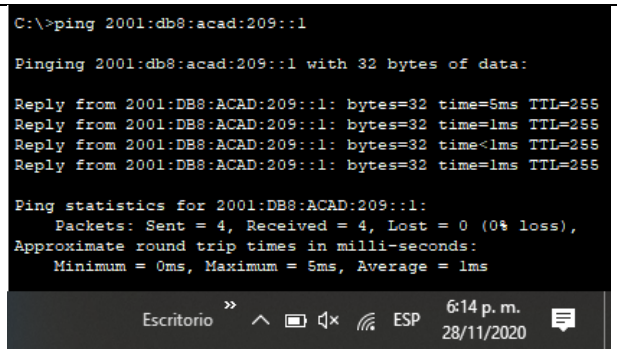
Nota: Si fallan los pings en las computadoras host, desactive temporalmente el firewall de la computadora y vuelva a realizar la prueba.

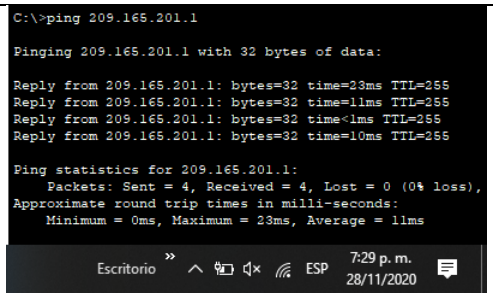
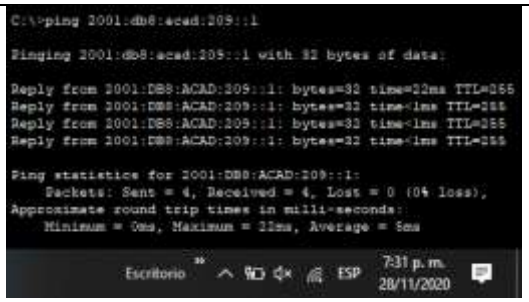
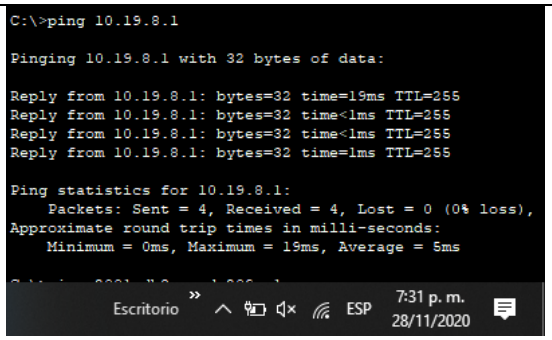
Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

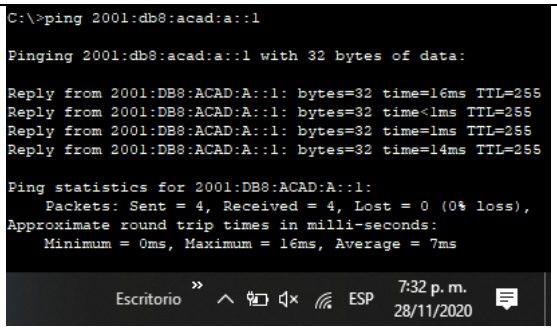
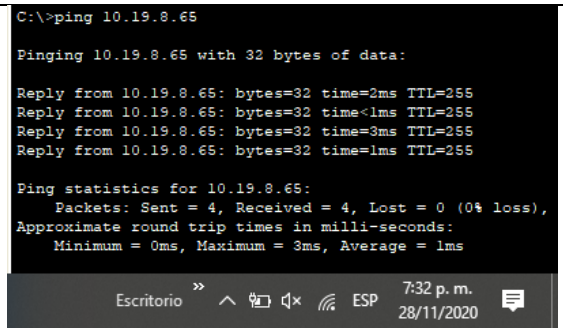
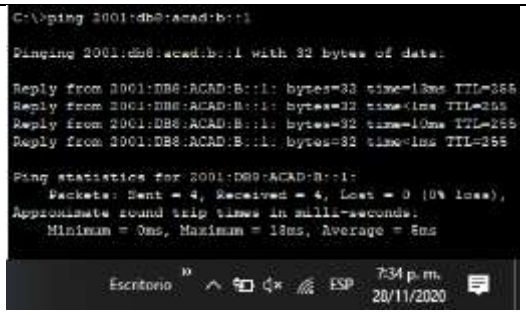
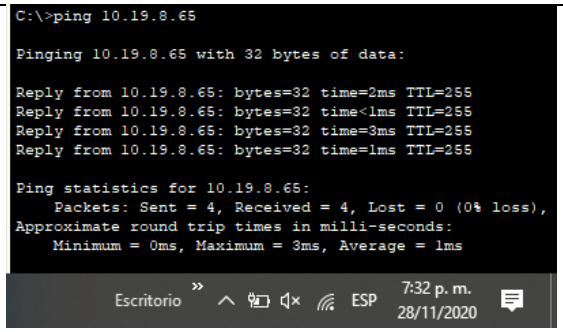
Desde PC-A	**de Internet**	**Dirección IP**	**Resultados de ping**
R1, G0/0/1.2	Dirección	10.19.8.1	 *Figura 2 - ping de PC-A a R1, G0/0/1.2*
R1, G0/0/1.2	IPv6	2001:db8:acad:a::1	*en blanco*  *Figura 3- ping ipv6 de PC-A a R1, G0/0/1.2*

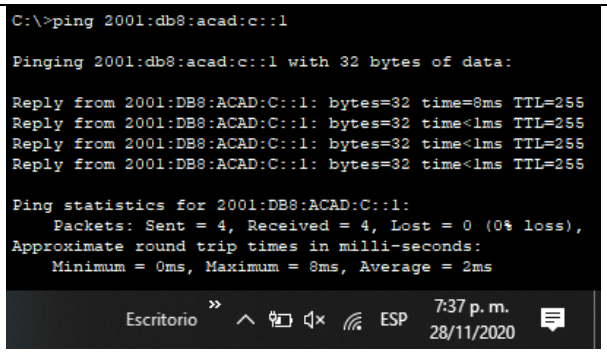
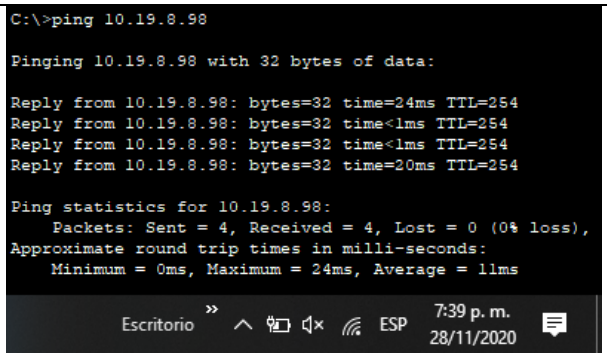
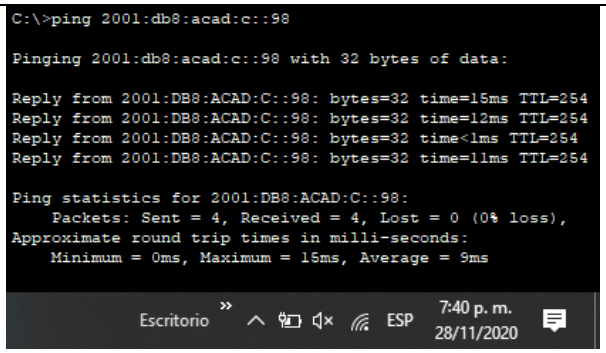
R1, G0/0/1 .3	Dirección	10.19.8.65	*en blanco*  *Figura 4- ping de PC-A a R1, G0/0/1.3*
R1, G0/0/1 .3	IPv6	2001:db8:acad: b: :1	 *Figura 5- ping ipv6 de PC-A a g0/01.3*
R1, G0/0/1 .4	Dirección	10.19.8.97	 *Figura 6– ping de PC-A a g0/01.4*
R1, G0/0/1 .4	IPv6	2001:db8:acad: c: :1	 *Figura 7– ping ipv6 de PC-A a g0/01.4*

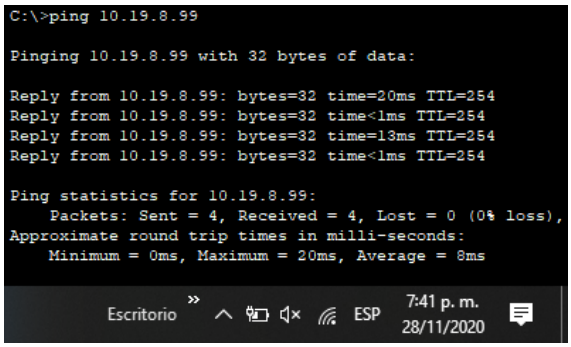
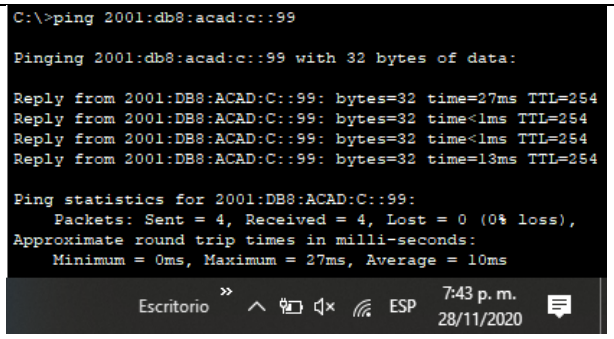
S1, VLAN 4	Dirección	10.19.8.98	 *Figura 8- ping de PC-A a S1, vlan 4*
S1, VLAN 4	IPv6	2001:db8:acad: c: :98	 *Figura 9- ping ipv6 de PC-A a S1, vlan 4*
S2, VLAN 4	Dirección	10.19.8.99.	 *Figura 10- ping de PC-A a S2, vlan 4*
S2, VLAN 4	IPv6	2001:db8:acad: c: :99	 *Figura 11- ping ipv6 de PC-A a S2, vlan 4*

PC-B	Dirección	IP address will vary. 10.19.8.84	 *Figura 12- ping de PC-A a PC-B*
PC-B	IPv6	2001:db8:acad:b: :50	 *Figura 13- ping ipv6 de PC-A a PC-B*
R1 Bucle 0	Dirección	209.165.201.1	 *Figura 14- ping de PC-A R1 loopback 0*
R1 Bucle 0	IPv6	2001:db8:acad:209: :1	 *Figura 15 - ping ipv6 de PC-A R1 loopback 0*

Desde PC B a		Dirección IP	Resultados de ping
R1 loopback 0	Dirección	209.165.201.1	 *Figura 16- ping de PC-B a loopback 0*
	IPv6	2001:db8:acad:209::1	 *Figura 17- ping ipv6 de PC-B a loopback 0*
R1, G0/0/1.2	Dirección	10.19.8.1	 *Figura 18- ping de PC-B a R1, G0/0/1.2*

R1, G0/0/1.2	IPv6	2001:db8:acad:a: :1	 *Figura 19- ping ipv6 de PC-B a R1, G0/0/1.2*
R1, G0/0/1.3	Dirección	10.19.8.65	 *Figura 20- ping de PC-B a R1, G0/0/1.3*
R1, G0/0/1.3	IPv6	2001:db8:acad:b: :1	 *Figura 21- ping ipv6 de PC-B a R1, G0/0/1.3*
R1, G0/0/1.4	Dirección	10.19.8.97	 *Figura 22- ping de PC-B a R1, G0/0/1.4*

R1, G0/0/1.4	IPv6	2001:db8:acad:c: :1	 *Figura 23- ping ipv6 de PC-B a R1, G0/0/1.4*
S1, VLAN 4	Dirección	10.19.8.98	 *Figura 24- ping de PC-B a S1, vlan 4*
S1, VLAN 4	IPv6	2001:db8:acad:c: :98	 *Figura 25- ping ipv6 de PC-B a S1, vlan 4*

S2, VLAN 4	Dirección	10.19.8.99.	 *Figura 26- ping de PC-B a S2, vlan 4*
S2, VLAN 4	IPv6	2001:db8:acad:c: :99	 *Figura 27- ping ipv6 de PC-B a S2, vlan 4*

2 – Descripción escenario 2

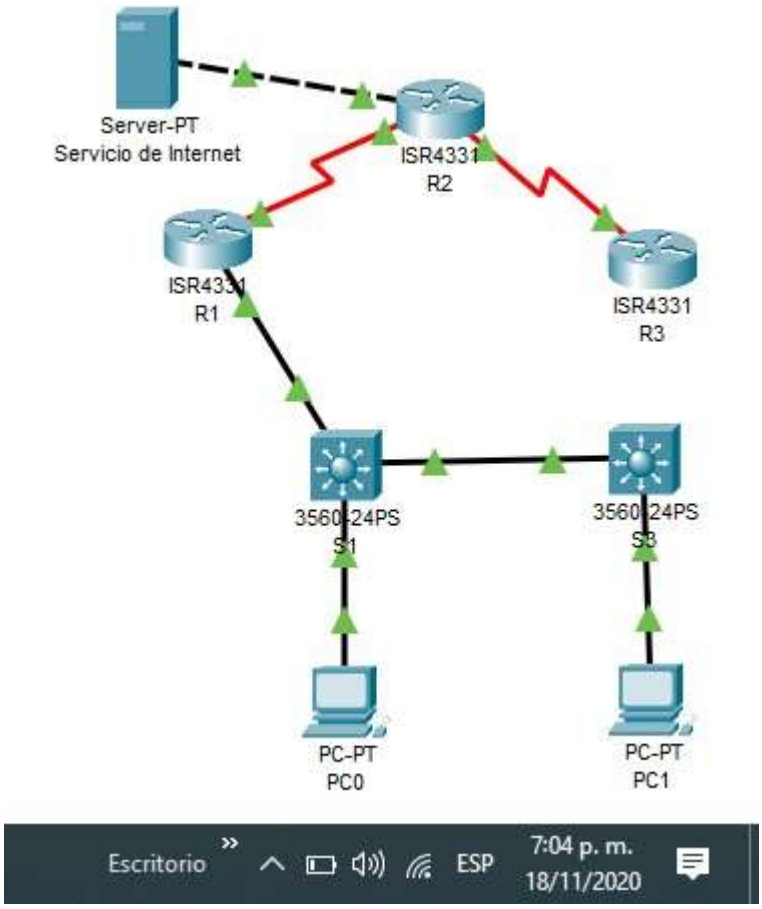


Figura 28 - Segundo escenario

2.1 - Inicializar dispositivos

2.1.1: Inicializar y volver a cargar los routers y los switches

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

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

Para empezar a configurar el router y el switch se borran las configuraciones en ambos y se reinician.

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

Tabla 12 - reiniciar router y switch

2.2 - Configurar los parámetros básicos de los dispositivos

2.2.1 : Configurar la computadora de Internet

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

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

Tabla 13 - configuración servidor de internet

Nota: Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente en partes posteriores de esta práctica de laboratorio.

2.2.2 : Configurar R1

En este paso se realizan las configuraciones más básicas a R1, se le configure el nombre, y las contraseñas, se configura también la interfaz serial configurada elegida en este caso.

Las tareas de configuración para R1 incluyen las siguientes:

Tarea	Comando
Desactivar la búsqueda DNS	R1(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R1
Contraseña de exec privilegiado cifrada	Class R1(config)#enable secret class
Contraseña de acceso a la consola	Cisco R1(config)#password cisco
Contraseña de acceso Telnet Cisco	R1(config)#line vty 0 4 R1(config-line)#password cisco R1(config-line)#login
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Mensaje MOTD	R1(config)#banner motd $Se prohibe el acceso no autorizado$
Interfaz S0/0/0	R1(config)#interface s0/0/0 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 shut R1#copy running-config startup-config Destination filename [startup-config]? Building configuration... [OK]

Rutas predeterminadas	R1(config)#ip route 0.0.0.0 0.0.0.0 serial s0/0/0 R1(config)# ipv6 route ::/0 s0/0/0 R1(config)#ipv6 Unicast-routing

Tabla 14 - Configuración básica R1

Nota: Todavía no configure G0/1.

2.2.3 : Configurar R2

En la configuración del router dos a demas de la configuracion básica se habilita el servidor HTTP que se utiliza para acceder a las aplicación web, se agregan las direcciones ip a las diferentes interfaces y se ingresa la ruta predeterminada.

La configuración del R2 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	R2(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R2
Contraseña de exec privilegiado cifrada	Class R2(config)#enable secret class
Contraseña de acceso a la consola	Cisco R2(config)#password cisco
Contraseña de acceso Telnet	R2(config)#line vty 0 4 R2(config-line)#password cisco R2(config-line)#login R2(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R2(config)#service password-encryption
Habilitar el servidor HTTP	R2(config)# ip http server
Mensaje MOTD	R2(config)#banner motd $Se prohibe el acceso no autorizado$

Interfaz S0/0/0	R2(config)#int s0/0/0 R2(config-if)#ip address 172.16.1.2 255.255.255.252 R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64 R2(config-if)#clock rate 128000 R2(config-if)#no shut
Interfaz S0/0/1	R2(config)#interface s0/3/1 R2(config-if)#ip address 172.16.2.2 255.255.255.252 R2(config-if)#clock rate 128000 R2(config-if)#ipv6 address 2001:DB8:ACAD:2::2/64 R2(config-if)#clock rate 128000 R2(config-if)#no shut
Interfaz G0/0/0 (simulación de Internet)	R2(config)#interface G0/0/0 R2(config-if)#ip address 209.165.200.232 255.255.255.255 R2(config-if)#clock rate 12800 R2(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64 R2(config-if)#no shut
Interfaz loopback 0 (servidor web simulado)	R2(config)#interface loopback 0 R2(config)#description Servidor WEB R2(config-if)#ip address 10.10.10.10 255.255.255.255 R2(config-if)#no shutdown
Ruta predeterminada	R2(config)#ip route 0.0.0.0 0.0.0.0R2(config)#ipv6 route ::/0 gigabitEthernet 0/0 R2#copy running-config startup-config Destination filename [startup-config]? Building configuration... [OK]

Tabla 15 - Configuración básica R2

2.2.4 : Configurar R3

Se configure el router tres con la configuración básica se configure la interfaz serial y las interfaces loopback

La configuración del R3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	R3(config)#no ip domain-lookup
Nombre del router: R3	Router(config)#hostname R3
Contraseña de exec privilegiado cifrada	Class R3(config)#enable secret class
Contraseña de acceso a la consola	R3(config)#password cisco
Contraseña de acceso Telnet Cisco	R3(config)#line vty 0 4 R3(config-line)#password cisco R3(config-line)#login
Cifrar las contraseñas de texto no cifrado	R3(config)#service password-encryption
Mensaje MOTD	R3(config)#banner motd $Se prohibe el acceso no autorizado$
Interfaz S0/0/1	R3(config)#interface s0/0/1 R3(config-if)#ip address 172.16.2.1 255.255.255.252 R3(config-if)#clock rate 128000 R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64 R3(config-if)#no shutdown
Interfaz loopback 4	R3(config)#interface loopback 4 R3(config-if)#ip address 192.168.4.1 255.255.255.0 R3(config-if)#no shutdown
Interfaz loopback 5	R3(config)#interface loopback 5 R3(config-if)#ip address 192.168.5.1 255.255.255.0 R3(config-if)#no shutdown
Interfaz loopback 6	R3(config)#interface loopback 6 R3(config-if)#ip address 192.168.6.1 255.255.255.0 R3(config-if)#no shutdown

Interfaz loopback 7	R3(config)#interface loopback 7 R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64 R3(config-if)#no shutdown
Rutas predeterminadas	R3(config-if)#ip route 0.0.0.0 0.0.0.0 s0/0/1 R3(config)#ipv6 route ::/0 s0/0/1

Tabla 16 - Configuración básica R3

2.2.5 : Configurar S1

Se configure el switch uno con el cambio de nombre para poder identificar el dispositivo, las contraseñas por seguridad del dispositivo, se cifran las contraseñas para aumentar la seguridad.

La configuración del S1 incluye las siguientes tareas:

Tarea	Comando
Desactivar la búsqueda DNS	Switch(config)#no ip domain-lookup
Nombre del switch S1	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 Cisco	S1(config-line)#line vty 0 4 S1(config)#password cisco S1(config-line)#login
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption
Mensaje MOTD	S1(config)#banner motd $Se prohibe el acceso no autorizado$ S1#copy running-config startup-config Destination filename [startup-config]? Building configuration... [OK]

Tabla 17 - Configuración básica S1

2.2.6 : Configurar el S3

Configuraciones básicas del switch tres como cambiar el nombre, agregar las contraseñas y configurar el mensaje de seguridad para evitar que personas no autorizadas ingresen a los dispositivos.

La configuración del S3 incluye las siguientes tareas:

Tarea	Comando
Desactivar la búsqueda DNS	Switch(config)#no ip domain-lookup
Nombre del switch: S3	Switch(config)#hostname S3
Contraseña de exec privilegiado cifrada: Class	S3(config)#enable secret class
Contraseña de acceso a la consola Cisco	S3(config)#line console 0 S3(config-line)#password cisco S3(config-line)#login
Contraseña de acceso Telnet Cisco	S3(config-line)#line vty 0 4 S3(config-line)#password cisco S3(config-line)#login
Cifrar las contraseñas de texto no cifrado	S3(config)#service password-encryption
Mensaje MOTD	S3(config)#banner motd $Se prohibe el acceso no autorizado$ S3#copy running-config startup-config Destination filename [startup-config] Building configuration... [OK]

Tabla 18 - configuración básica del S3

2.2.7 : Verificar la conectividad de la red

En este paso se realizan las verificacion de la conexion entre dispositivos, se debe desabilitar el firewall que puede evitar que se conecten correctamente

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

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	
R2	R3, S0/0/1	172.16.2.1	

PC de Internet	Gateway predeterminado	209.165.200.232	

Tabla 19 - Prueba de conectividad router y servidor

Ping de R1 a R2, S0/0/0

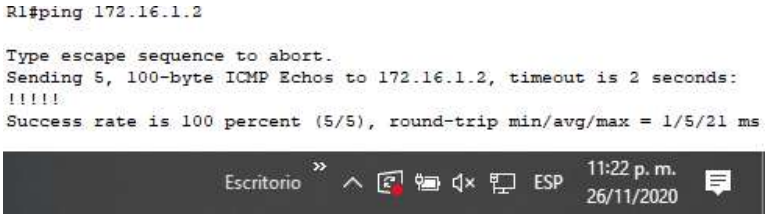


Figura 29 - ping de R1 a S0/0/0

Ping de R2 a R3, S0/0/1

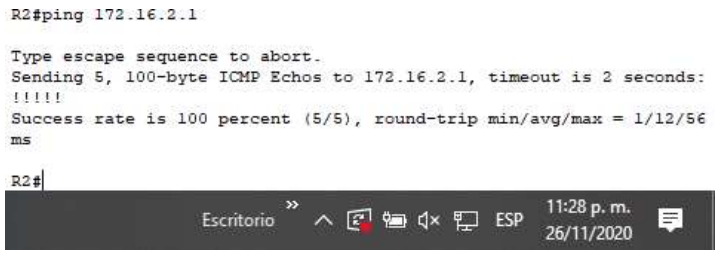


Figura 30- Ping de R2 a R3, S0/0/1

Ping del servidor de internet a Gateway predeterminado

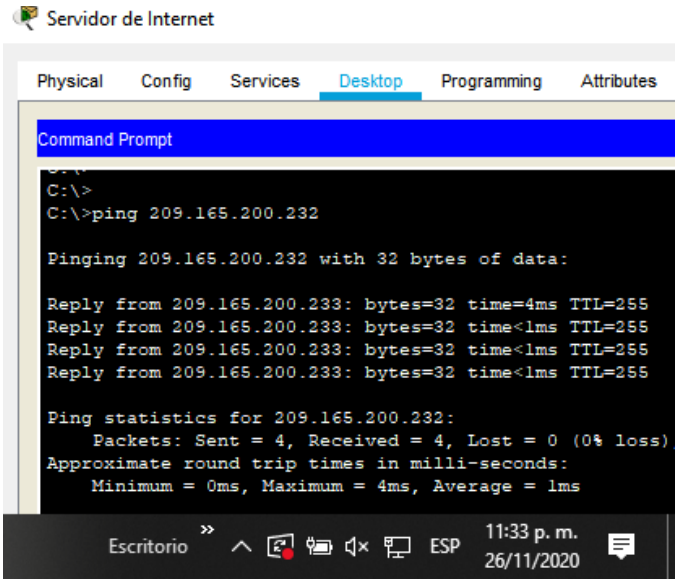


Figura 31 - Ping del servidor de internet a Gateway predeterminado

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

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

2.3.1 : Configurar S1

En este paso se configura el S1

La configuración del S1 incluye las siguientes tareas:

Tarea	Comando
Crear la base de datos de VLAN Utilizar la tabla de equivalencias de VLAN para topología para crear y nombrar cada una de las VLAN que se indican	S1(config)#vlan 21 S1(config-vlan)#name contabilidad S1(config-vlan)#exit S1(config)#vlan 23 S1(config-vlan)#name ingenieria S1(config-vlan)#exit S1(config)#vlan 99 S1(config-vlan)#name Administracion S1(config-vlan)#exit
Asignar la dirección IP de administración. Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S1 en el diagrama de topología	S1(config)#int vlan 99 S1(config-if)# ip address 192.168.99.2 255.255.255.0 S1(config-if)#no shut
Asignar el gateway predeterminado	Asigne la primera dirección IPv4 de la subred como el gateway predeterminado. S1(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3 Utilizar la red VLAN 1 como VLAN native	S1(config)# int F0/3 S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1 S1(config-if)#no shut
Forzar el enlace troncal en la interfaz F0/5 Utilizar la red VLAN 1 como VLAN native	S1(config)# int F0/5 S1(config- if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1 S1(config-if)#no sh

Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range S1(config)# interface range f0/1-2, f0/4, f0/6-24, S1(config-if-range)#switchport mode acces
Asignar F0/6 a la VLAN 21	S1(config)# interface F0/6 S1(config-if)#switchport mode Access S1(config-if)#switchport access vlan 21 S1(config-if)#no shut
Apagar todos los puertos sin usar	S1(config)# interface range f0/1-2, f0/4, f0/6-24 S1(config-if-range)#shut

Tabla 20 - configuración de Vlan en S1

2.3.2 : Configurar el S3

Configurar las vlan en el Switch tres, las vlan se utiliza para dividir la red en partes indeendientes, se utili para mejorar la seguridad, ya que si entran en una vlan no tiene acceso a la otra vlan

La configuración del S3 incluye las siguientes tareas:

Tarea	Comando
Crear la base de datos de VLAN Utilizar la tabla de equivalencias de VLAN para topología para crear cada una de las VLAN que se indican Dé nombre a cada VLAN.	S3(config)#vlan 21 S3(config-vlan)#name contabilidad S3(config-vlan)#exit S3(config-vlan)#vlan 23 S3(config-vlan)#name ingenieria S3(config-vlan)#exit S3(config)#vlan 99 S3(config-vlan)#name Administracion S3(config-vlan)#exit
Asignar la dirección IP de administración Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S3 en el diagrama de topología	S3(config)#interface vlan 99 S3(config-if)#ip address 192.168.99.3 255.255.255.0 S3(config-if)#no shut

Asignar el gateway predeterminado.	Asignar la primera dirección IP en la subred como gateway predeterminado. S3(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	S3(config)#interface fastEthernet 0/3 S3(config-if)#switchport trunk encapsulation dot1q S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1 S3(config-if)#no shut
Configurar el resto de los puertos como puertos de acceso Utilizar el comando interface range	S3(config)# interface range f0/1-2, f0/4-24, g0/1-2 S3(config-if-range)#switchport mode acces
Asignar F0/18 a la VLAN 21	S3(config)#interface f0/18 S3(config-if)#switchport access vlan 21 S3(config-if)#no shut
Apagar todos los puertos sin usar	Utilizar el comando interface range S3(config)# interface range f0/1-2, f0/4, f0/7-f0/17, f0/19-24, g0/1-2 S3(config-if-range)# shut

Tabla 21 - configuración de Vlan en S3

2.3.3 : Configurar R1

Se configura el protocolo 802.1Q en el R1. Este protocolo se configure para crear un Puente entre las vlan configuradas previamente

Las tareas de configuración para R1 incluyen las siguientes:

Elemento	Comando
Configurar la subinterfaz 802.1Q .21 en G0/1 Descripción: LAN de Contabilidad Asignar la VLAN 21 Asignar la primera dirección disponible a esta interfaz	R1(config)#interface g0/1.21 R1(config-subif)#description LAN_Contabilidad R1(config-subif)#encapsulation dot1q 21 R1(config-subif)#ip address 192.168.21.1 255.255.255.0 R1(config-subif)#exit

Configurar la subinterfaz 802.1Q .23 en G0/1 Descripción: LAN de Ingeniería Asignar la VLAN 23 Asignar la primera dirección disponible a esta interfaz	R1(config)#interface g0/1.23 R1(config-subif)#description LAN_Ingenieria R1(config-subif)#encapsulation dot1q 23 R1(config-subif)#ip address 192.168.23.1 255.255.255.0 R1(config-subif)#exit
Configurar la subinterfaz 802.1Q .99 en G0/1 Descripción: LAN de Administración Asignar la VLAN 99 Asignar la primera dirección disponible a esta interfaz interface GigabitEthernet0/0/1.99	R1(config)#interface g0/1.99 R1(config-subif)#description LAN_Administracion R1(config-subif)#encapsulation dot1q 99 R1(config-subif)#ip address 192.168.99.1 255.255.255.0 R1(config-subif)#exit
Activar la interfaz G0/1	R1(config)#interface g0/1 R1(config-if)#no shutdown R1(config-if)#exit

Tabla 22 - Configurar protocolo 802.1Q

2.3.4 : Verificar la conectividad de la red

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

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

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	172.16.1.0	
S3	R1, dirección VLAN 99	192.168.99.0	
S1	R1, dirección VLAN 21	192.168.21.0	
S3	R1, dirección VLAN 23	192.168.23.0	

Tabla 23 - Conectividad de red

Ping de S1 a R1 vlan 99

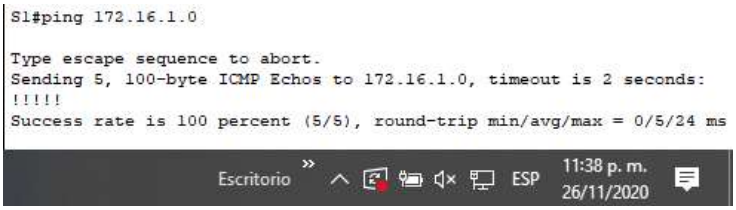


Figura 32- Ping de S1 a R1 vlan 99

Ping de S3 a R1 vlan 99

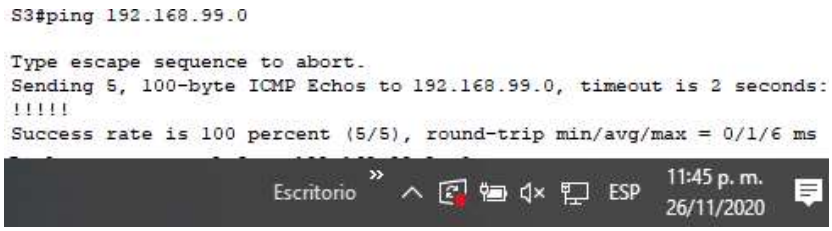


Figura 33 - Ping de S3 a R1 vlan 99

Ping de S1 a R1 vlan 21

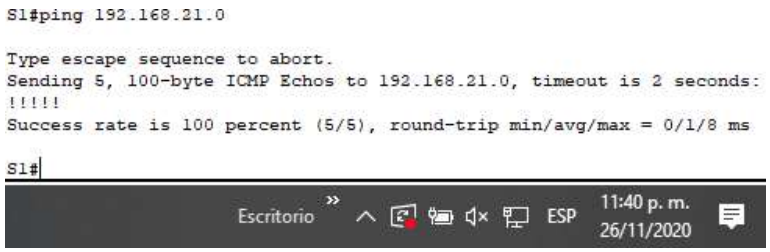


Figura 34 - Ping de S1 a R1 vlan 21

Ping de S1 a R1 vlan 23

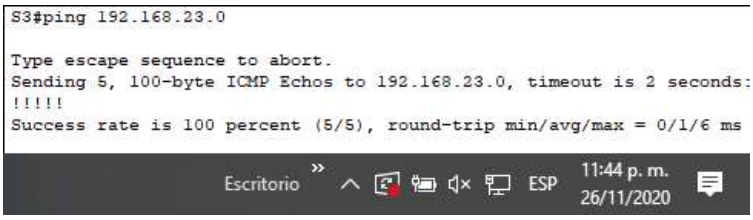


Figura 35 - Ping de S1 a R1 vlan 23

2.4 - Configurar el protocolo de routing dinámico OSPF

2.4.1 : Configurar OSPF en el R1

Este protocolo se usa para permitir el enrutamiento se obtiene un resumen de las rutas a las subredes con clase de forma automática

Las tareas de configuración para R1 incluyen las siguientes:

Elemento	Comando
Configurar OSPF área 0	R1(config)#router ospf 0 R1(config-router)#router-id 1.1.1.1
Anunciar las redes conectadas directamente Asigne todas 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 Serial0/0/0 R1(config-router)#passive-interface GigabitEthernet0/1.21 R1(config-router)#passive-interface GigabitEthernet0/1.23 R1(config-router)#passive-interface GigabitEthernet0/1.99
Desactive la sumarización automática	R1(config-router)#router rip R1(config-router)#no auto-summary R1(config-router)#exit

Tabla 24 - Configurar OSPF en R1

2.4.2 : Configurar OSPF en el R2

La configuración del R2 incluye las siguientes tareas:

Elemento	Comando
Configurar OSPF área 0	R2(config)#router ospf 0 R2(config-router)#router-id 2.2.2.2
Anunciar las redes conectadas directamente Nota: Omitir la red G0/0.	R2(config-router)#network 172.16.1.0 0.0.0.3 area 0 R2(config-router)#network 172.16.2.0 0.0.0.3 area 0 R2(config-router)#network 10.10.10.10 0.0.0.0 area 0
Establecer la interfaz LAN (loopback) como pasiva	R2(config-router)#passive-interface loopback 0
Desactive la sumarización automática.	R2(config-router)#router rip R2(config-router)#no auto-summary R2(config-router)#exit

Tabla 25 - Configurar OSPF en R2

2.4.3 : Configurar OSPFv3 en el R3

La configuración del R3 incluye las siguientes tareas:

Elemento	Comando
Configurar OSPF área 0	R3(config)#router ipv6 ospf 0 R3(config-router)#router-id 3.3.3.3
Anunciar redes IPv4 conectadas directamente	R3(config-router)#network 172.16.2.0 0.0.0.3 area 0 R3(config-router)#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	R2(config-router)#passive-interface loopback4 R2(config-router)#passive-interface loopback5 R2(config-router)#passive-interface loopback6
Desactive la sumarización automática.	R3(config-router)#no auto-summary

Tabla 26 - Configurar OSPv3 en R3

2.4.4 : Verificar la información de OSPF

En este paso muestran los comandos necesarios para verificar que la información de OSPF este configurada correctamente

Elemento	Comando
¿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?	R1#show ip protocols
¿Qué comando muestra solo las rutas OSPF?	R1#show ip route ospf
¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	R1#show ip route

Tabla 27 - Comandos de OSPF

2.5 - Implementar DHCP y NAT para IPv4

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

En el R1 se implementa la configuración DHCP el cual asigna de forma dinámica las direcciones ip en las vlan 21 y la vlan 23, tambien se configura un nombre de dominio y servidos DNS el cual le da el nombre a la URL

Las tareas de configuración para R1 incluyen las siguientes:

Elemento	Comando
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20
Crear un pool de DHCP para la VLAN 21. Nombre: ACCT Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado	R1(config)#ip dhcp pool ACCT R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com R1(dhcp-config)#default-router 192.168.21.1 R1(dhcp-config)#network 192.168.21.0 255.255.255.0 R1(dhcp-config)#exit
Crear un pool de DHCP para la VLAN 23 Nombre: ENGNR Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado	Crear un pool de DHCP para la VLAN 23 R1(config)#ip dhcp pool ENGNR R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com R1(dhcp-config)#default-router 192.168.23.1 R1(dhcp-config)#network 192.168.23.0 255.255.255.0 R1(dhcp-config)#exit

Tabla 28 -DHCP para las vlan 21 y 23

2.5.2 : Configurar la NAT estática y dinámica en el R2

En R2 se configura NAT en el cual se conectan varias redes internas mediante redes públicas, se le agrega seguridad al no usar las redes internas

La configuración del R2 incluye las siguientes tareas:

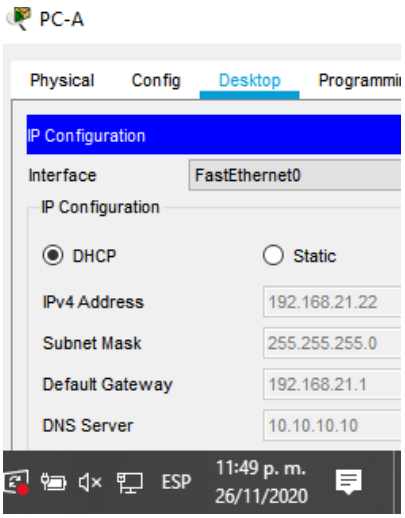
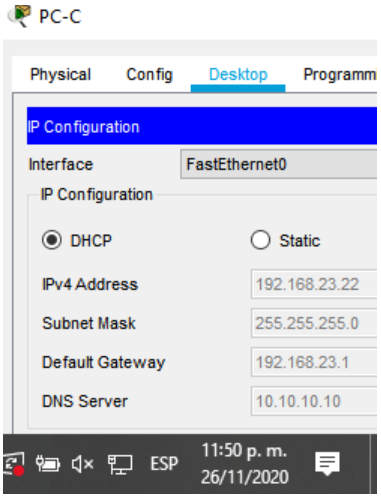
Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario Nombre de usuario: webuser Contraseña: cisco12345 Nivel de privilegio: 15	R2(config)#user webuser privilege 15 secret cisco12345

Habilitar el servicio del servidor HTTP	R2(config)#ip http server
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	R2(config)#ip http authentication local
Dirección global interna: 209.165.200.229	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 g0/0 R2(config-if)#ip nat inside R2(config-if)#exit
Configurar la NAT dinámica dentro de una ACL privada Lista de acceso: 1 Permitir la traducción de las redes de Contabilidad y de Ingeniería en el R1 Permitir la traducción de un resumen de las redes LAN (loopback) en el R3	R2(config)#access-list 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 192.168.4.1 0.0.0.255 R2(config)#access-list 1 permit 192.168.5.1 0.0.0.255 R2(config)#access-list 1 permit 192.168.6.1 0.0.0.255
Defina el pool de direcciones IP públicas utilizables. Nombre del conjunto: INTERNET El conjunto de direcciones incluye: 209.165.200.225 – 209.165.200.228	R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248
Definir la traducción de NAT dinámica	R2(config)#ip nat inside source list 1 pool INTERNET

Tabla 29 - NAT estática y dinámica en R2

2.5.3 : Verificar el protocolo DHCP y la NAT estática

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

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	 *Figura 36 - PC-A DHCP*
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	 *Figura 37- PC-C DHCP*

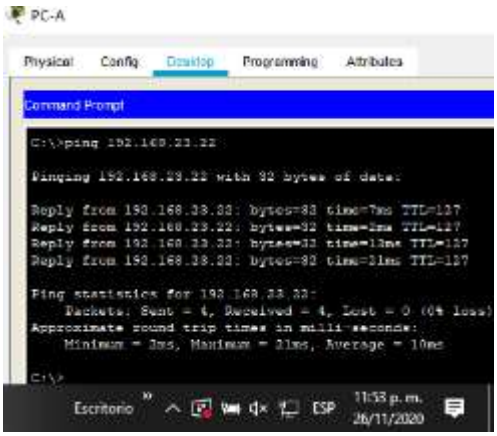
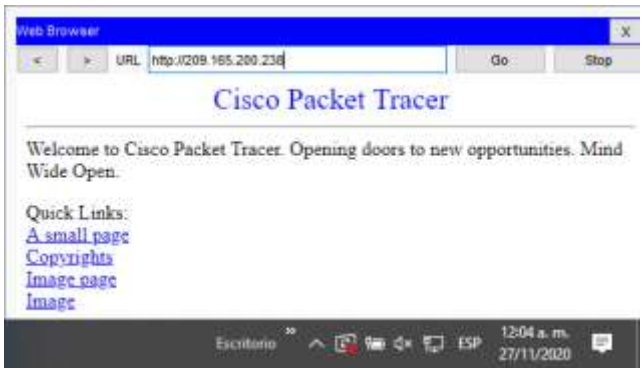
Verificar que la PC-A pueda hacer ping a la PC-C **Nota:** Quizá sea necesario deshabilitar el firewall de la PC.	 *Figura 38 - ping de PC-A a PC-C*
Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.229) Iniciar sesión con el nombre de usuario webuser y la contraseña cisco12345	 *Figura 39 - Acceso al navegador*

Tabla 30 - Verificar DHCP y NAT

2.6 - Configurar NTP

Se habilita el protocolo NTP para sincronizar la hora con el servidor de internet se configura en el R2 para que se pueda sincronizarse

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2. 5 de marzo de 2016, 9 a. m.	R2#clock set 9:00:00 5 March 2016 R2#show clock detail

Configure R2 como un maestro NTP. Nivel de estrato: **5**	R2(config)#ntp master 5
Configurar R1 como un cliente NTP. Servidor: R2	R1(config)#ntp server 172.16.1.2
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	R1(config)#ntp update-calendar
Verifique la configuración de NTP en R1.	R1(config)#do show ntp status R1#do show clock

Tabla 31 - Configurar NTP

2.7 - Configurar y verificar las listas de control de acceso (ACL)

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

Para aumentar la seguridad de la red se restringe el uso de las línea VTY en el R2, se realiza por medio de una ACL, permitiendo restringir las conexiones ingreso y de salida del dispositivo

Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2 Nombre de la ACL: ADMIN-MGT	R2(config)#ip access-list standard ADMIN-MGT R2(config-std-nacl)#permit host 172.16.1.1
Aplicar la ACL con nombre a las líneas VTY	R2(config)#line vty 0 4
Permitir acceso por Telnet a las líneas de VTY	R2(config-line)#access-class ADMIN-MGT in R2(config-line)#exit
Verificar que la ACL funcione como se espera	R1# show access-lists

Tabla 32 - Lista de control de acceso ACL

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

A continuación se relacionan los comandos para mostrar las configuraciones de ACL relacionadas anteriormente y se verifica que esté instalado correctamente

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	Router(config)#show access-list
Restablecer los contadores de una lista de acceso	Router(config)#clear access-list counters
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	Router(config)#interface Fa0/1 Router(config-if)#ip access-group 1 out

¿Con qué comando se muestran las traducciones NAT? **Nota:** Las traducciones para la PC-A y la PC-C se agregaron a la tabla cuando la computadora de Internet intentó hacer ping a esos equipos en el paso 2. Si hace ping a la computadora de Internet desde la PC-A o la PC-C, no se agregarán las traducciones a la tabla debido al modo de simulación de Internet en la red.	Router(config)#show ip nat translations
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	Router(config)#clear ip nat translation

Tabla 33 - Comandos para ACL

CONCLUSIONES

La configuración de las direcciones ipv4 de manual no es recomendable en las empresas porque pueden producir errores y por eso se recomienda automatizar el proceso por medio de DHCP que permite asignación automática de direcciones IP, esto evita errores de asignación

En cada ejercicio se explican las configuraciones realizadas, se accedió a los Switch y a los router para escribir los comandos desde la consola y de forma remota, por medio de ping se muestra el resultado de la configuración establecida.

Las configuraciones se manejaron la herramienta packet tracert que es un entorno de simulación de redes de telecomunicaciones. Se desarrollaron los conceptos desde la configuración básica de los dispositivos, se configuro la conexiones entre vlan, el protocolo OSPF y NTP, se configuraron los equipos por medio de DHCP en el router.

BIBLIOGRAFÍA

CISCO, Configuración de LACP (802.3ad) entre un Catalyst 6500/6000 y un Catalyst 4500/4000. {En línea} {2005} Disponible en: https://www.cisco.com/c/es_mx/support/docs/lan-switching/etherchannel/19642-126.html

CISCO, configuración troncal 802.1Q. En un switch {en línea} {2019} Disponible en: https://www.cisco.com/c/es_mx/support/docs/switches/catalyst-4000-seriesswitches/24064- 171.html

CISCO,Configuración dinámica de las opciones del servidor DHCP {En línea} {2005} Disponible en: https://www.cisco.com/c/es_mx/support/docs/ip/dynamic-address-allocation-resolution/22920-dhcp-ser.html

CISCO, Networking Academy, MODULO DE ESTUDIO CCNA1 (Network Fundamentals). {En línea} {2010} Disponible en: http://www.mediafire.com/?9cq9h4jo23c1359

CISCO, Networking Academy, MODULO DE ESTUDIO CCNA2 (Routing Protocols and Concepts). . {En línea} {2010} Disponible en: http://www.mediafire.com/?5y052miul2vezhj

CISCO. CCNA. Enrutamiento entre VLANs. Principios de Enrutamiento y Conmutación. {En línea} {2010} Disponible en: https://static-courseassets.s3.amazonaws.com/RSE50ES/module5/index.html#5.0.1.1

FLATFEEFSBO (2016) Configure LACP EtherChannel en el Cisco IOS Switch {En línea} {2010} Disponible en: https://flatfeefsbo.com/es/cisco/11-configure-lacp-etherchannel-in-cisco-ios-switch.html

REYES Reynaud, M Calculo de Subredes de México. [Video] {En línea} {2010} Disponible en: http://www.youtube.com/watch?v=Z7DM639rAmQ&list=PLaXGHu_K17nuWSyLNRtX7UvR2LcpTB K7P&index=5

UNAD Principios de Enrutamiento [OVA]. {En línea} {2012} Disponible en https://1drv.ms/u/s!AmlJYei-NT1IhgOyjWeh6timi_Tm

UNAD Videos iniciales de cisco [OVA]. {En línea} {2016} Disponible en https://1drv.ms/u/s!AmlJYei-NT1IhgL9QChD1m9EuGqC

ANEXOS

Anexo A: link a escenarios https://drive.google.com/drive/folders/15amOiIWzYdr-F16GqrLyDEkwZQ59xJqk?usp=sharing

Anexo B al final articulo cientifico

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

Diana patricia Zúñiga Chará
Ingeniera de sistemas Dpzunigac@unadvirtual.edu.co
Universidad Abierta y a distancia - UNAD

RESUMEN
En la solución de los escenarios que se compone de equipos, routers y switch y los cables necesarios para el envió de la información, se recrean los modelos de red en packet tracer
Los ejercicios están desarrollados para automatizar un empresa realizando las configuraciones necesarias por medio de direcciones ipv4 e ipv6, vlans, protocolo OSPF y NTP, se configuro DHCP y NAT para el correcto funcionamiento de la red

Palabras claves: Ip, DHCP, NAT, Packet tracert,OSFP y NTP

Absact
In the solution of the scenarios that consists of equipment, routers and switch and the necessary cables to send the information, the network models are recreated in packet tracer The exercises are developed to automate a company by making the necessary configurations through ipv4 and ipv6 addresses, vlans, OSPF and NTP protocol, DHCP and NAT were configured for the correct operation of the network

Keywords: Ip, DHCP, NAT, Packet tracert, OSFP and NTP

1. INTRODUCCIÓN

En la actualidad que todos los negocios necesitan estar conectado en la red por ese motivo es importante aprender las habilidades necesarias para conocer como configurar el sistema de redes, logrando de esa manera una conectividad óptima en las empresas,

En este documento muestra los conocimientos que los administradores de red deben tener para cumplir los lineamientos de las topologías de red, mediante instalación, configuración, se desarrollan en el simulador de packet tracert, se mejoran las habilidades al mostrar la configuración de estos dos escenarios, mostrando los comandos más utilizados e importantes en el momento de configurar.

Este escenario se desarrollan los conocimientos básicos en las configuración del router, switch y computadores, se configuran las interfaces, se le asignan direcciones Ipv4 e ipv6, se ejecutan las dirección en los computadores se realizan por medio de DHCP y se verifican que las conexiones entre los equipos sea de forma satisfactoria

2. DESCRIPCIÓN DEL PROBLEMA

Se necesitan configurar en la red de esta empresa pequeña, las direcciones ipv4 e ipv6, los equipos deben soportar ambas direcciones, se realiza un enrutamiento para VLAN, se configurara DHCP para los equipos entre vlans, falta de seguridad en los puertos

3. MATERIALES Y MÉTODOS,

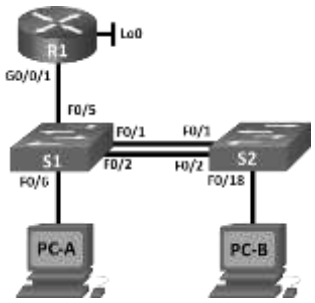
La metodología que se utiliza en escenarios en la investigación aplicada, porque busca

generar conocimiento a través del desarrollo propuesto. Este trabajo pretende transferir conocimiento mostrando los pasos de cómo fue solucionado los escenarios. Se realizan los ejercicios en el programa de packet tracert
Se utiliza un router ISR 331
Se utilizan dos switch 3560-24 PS o cualquier otro router que soporte tanto direcciones ipv4 e ipv6
Se utilizan dos equipos

4. RESULTADOS,

En el escenario 1, se realiza la topología según muestra en la imagen, La configuración del primer escenario consta de un router y dos switch y dos equipos

Figura 1. Escenario 1



Para realizar la configuración de las vlan

Tabla 1

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

Para asignar las direcciones ip se realiza la tabla de direccionamiento

Tabla 2- tabla de direcciones

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

Con esta información se puede realizar los escenarios con la consola se le asigna un nombre de los equipos, las contraseñas de seguridad.
Primero se le borran las configuraciones al switch y al router se reinician. Al switch se habilitan las direcciones IPV6 Se les asigna el nombre, las claves de seguridad y se cifra la

contraseña para aumentar seguridad se le da permisos de ipv6 al router, se le configuran las interfaces.
Se realizan las mismas configuraciones en el switch

Tabla3 - Configurar S1

Tareas	Comando
Crear VLAN	Vlan 2 name Bikes Vlan 3 name Trikes Vlan 4 name Management Vlan 5 name Parking Vlan 6 name Native exit
Crear troncos 802.1Q que utilicen la VLAN 6 nativa Interfaces F0/1, F0/2 y F0/5	interface range f0/1-2, f0/5 switchport mode trunk switchport trunk native vlan 6 switchport trunk allowed vlan 2,3,4,5,6 switchport trunk encapsulation dot1q exit
Crear puertos EtherChannel en F0/1 y F0/2 Usar el protocolo LACP	interface f0/6 switchport mode access switchport access vlan 2 no shut config t
Configurar el puerto de acceso de host para VLAN 2 Interface F0/6	S1(config)#interface f0/6 S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 2 S1(config-if)#no shut
Configurar seguridad del puerto en los puertos de acceso Permitir 3 direcciones MAC	switchport port-security maximum 3 switchport port-security violation shutdown switchport port-security mac-address 0001.422C.C5B3 switchport port-security mac-address 0001.C97B.6173 switchport port-security mac-address 0002.1671.8082
Proteja todas las interfaces no utilizadas Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar	interface range f0/3-4, f0/7-9, f0/11-24 switchport mode Access switchport acces vlan 5 description SW1-v5 shutdown exit

Vlan crea redes creadas virtualmente e independientes en el resto de la red y para poder comunicarse entre ellas necesita un puerto troncal para enviar y recibir información de otra vlan. Se realiza la misma configuración en el S2

Tabla 4 Configurar S2

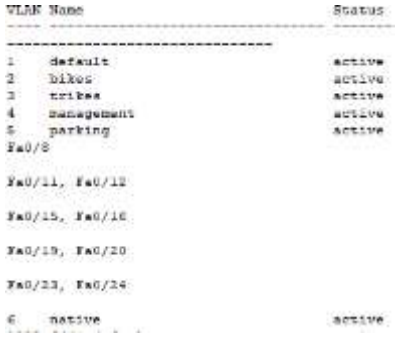
Tarea	Comando
nombre Native	Vlan 2 name Bikes Vlan 3 name Trikes Vlan 4 name Management Vlan 5 name Parking Vlan 6 name Native exit
Crear troncos 802.1Q que utilicen la VLAN 6 nativa Interfaces F0/1 y F0/2	interface range fa0/1-2 switchport mode access switchport mode trunk switchport trunk native vlan 6 switchport trunk allowed vlan 2,3,4,5,6

	switchport trunk encapsulation dot1q exit exit
Crear puertos EtherChannel para interfaces F0/1 y F0/2 protocolo LACP	interface range fastEthernet0/1-2 channel-protocol lacp channel-group 2 mode passive exit
Configurar el puerto de acceso del host para la VLAN 3 Interfaz F0/18	interface f0/18 switchport mode access switchport access vlan 3 S2(config-if-range)#no sh
Configure port-security en los access ports permite 3 MAC addresses	switchport mode access switchport access vlan 3 switchport port-security maximum 3 switchport port-security violation shutdown switchport port-security mac-address 0001.422C.C5B3 switchport port-security mac-address 0001.C97B.6173 switchport port-security mac-address 0002.1671.8082
Asegure todas las interfaces no utilizadas a la VLAN 5, en modo de acceso y apagar	interface range f0/3-9,f0/11-17,f0/19-24 switchport mode access switchport acces vlan 5 description SW2-v5 shutdown

.

Con el comando show vlan brief se ven las vlan activas

Figura 2 - Vlan



En el router se crea el DHCP de direccionamiento ipv4 para las vlan para los switch de ultimo se configura los equipo con DHCP para que tengan la dirección ip y los equipos e conecten de forma automática y queden listos para trabajar y por último se muestra la el resultado de la conexión-

En este paso se configura la interface loopback 0 para una mejor conectividad se configura tanto ipv4 e ipv6, y el DHCP para que la PCA y la PCB tengan dirección ipv4 dinámicas.

Tabla 5- DHCP

Tarea	**comandos**
Crear rutas que dirijan el tráfico a la interfaz Loopback 0	ip route 0.0.0.0 0.0.0.0 10.19.8.98 ip route 0.0.0.0 0.0.0.0 10.19.8.99
Configurar IPv4 DHCP para VLAN 2	ip dhcp pool vlan2 network 10.19.8.0 255.255.255.192 default-router 10.19.8.1 dns-server 10.10.10.10 domain-name ccna-lab.net
Configurar DHCP IPv4 para VLAN 3 Cree un grupo DHCP para VLAN 3,	ip dhcp pool vlan3 network 10.19.8.0 255.255.255.224 default-router 10.19.8.65 dns-server 10.10.10.10 domain-name ccna-lab.net

En este paso se configuran el equipo red PC-A y PC-B por medio de DHCP, al estar conectadios se verifica la información con el comando ipconfig all y se anexanl los datos

Tabla 6. PC-A

PC-A	
Dirección física	*00D0.97E2.9876*
Dirección IP	*10.19.8.52*
Dirección Ipv6	*FE80::2E0:A3FF:FE04:AA0/64*

Máscara de subred	*255.2 55.255.192*
Gateway predeterminado	*10.19.8.1*
Gateway predeterminado IPv6	*FE80::11*

Tabla 7 PC- B

PC-B	
Dirección física	*0040.0B1B.8DE0*
Dirección IP	*10.19.8.84*
Dirección Ipv6	*2001:DB8:ACAD:B::50*
Máscara de subred	*255.255.255.224*
Gateway predeterminado	*10.19.8.65*
Gateway predeterminado IPv6	*FE80::1*

Se verifica la conectividad de ipv4 e ipv6 con el comando ping y se relacionan a acontinuación los resultados

Figura 3 - PC-A a R1, G0/0/1.2

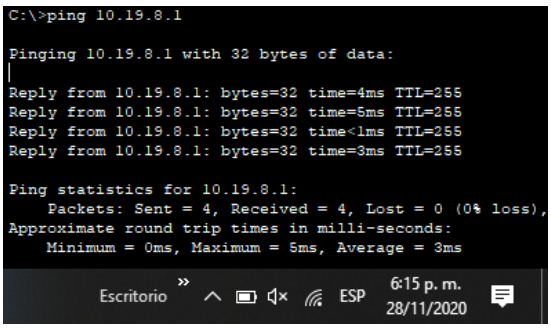


Figura 4 - PC-A R1, G0/0/1.3 IPv6 2001:db8:acad:b: :1

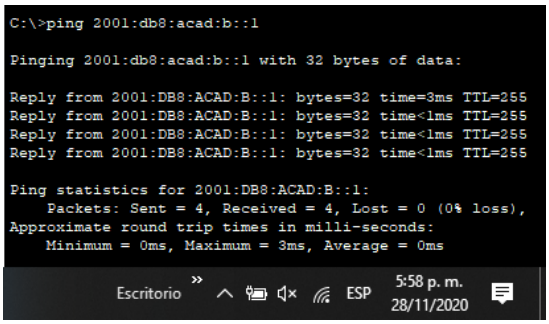


Figura 5 - PC-A S1, VLAN 4 Dirección 10.19.8.98

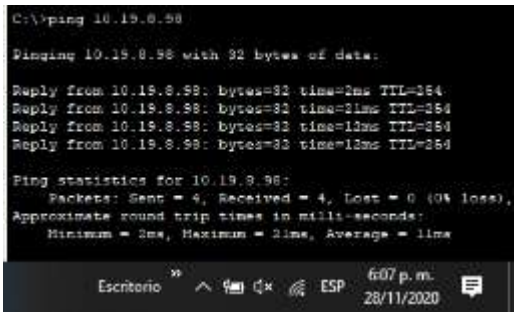


Figura 6 - PC-B R1 Bucle 0 Dirección 209.165.201.1

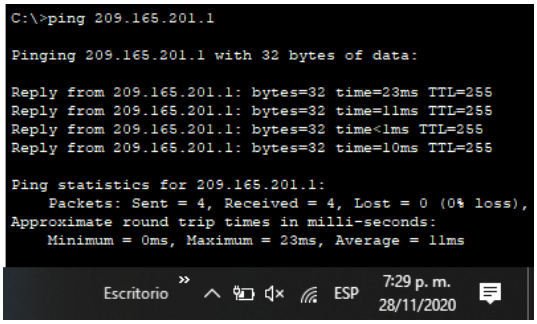


Figura 7 - PC-B R1, G0/0/1.2 IPv6 2001:db8:acad:a: :1

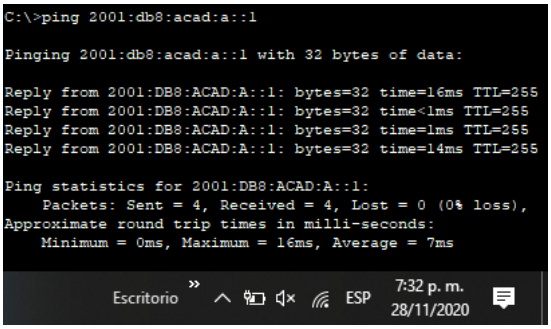


Figura 8 - PC-B R1, G0/0/1.3 Dirección 10.19.8.65

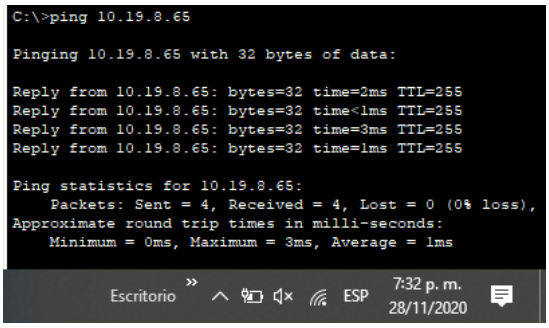
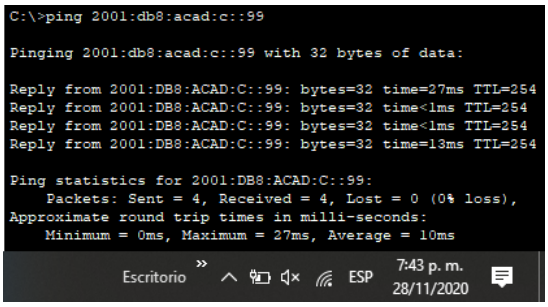


Figura 9 - PC-B S2, VLAN 4 IPv6 2001:db8:acad:c: :99



5. CONCLUSIONES

El trabajo realizado durante el diplomado ayudo a resolver este escenario y como la configuración de redes puede ayudar a una empresa a mejorar sus condiciones

La vlan aumenta la seguridad ya que crea direcciones ip virtuales para que no puedan acceder a ella, es posible separa los componentes de LAN y no se envían información entre si

El enlace troncal transmite información entre vlans, permite crear varias VLAN en toda la red

El servicio DHCP provee direcciones ip de forma automática, dentro de una misma red, es muy ventajoso en lugares con varios equipos

6. REFERENCIAS

[1] CISCO, Networking Academy, MODULO DE ESTUDIO CCNA1 (Network Fundamentals). {En línea} {2010} Disponible en: http://www.mediafire.com/?9cq9h4jo23c1359

[2] CISCO, configuración troncal 802.1Q. En un switch {en línea} {2019} Disponible en: https://www.cisco.com/c/es_mx/support/docs/switches/catalyst-4000-seriesswitches/24064-171.html

[3] CISCO, Configuración dinámica de las opciones del servidor DHCP {En línea} {2005} Disponible en: https://www.cisco.com/c/es_mx/support/docs/ip/dynamic-address-allocation-resolution/22920-dhcp-ser.html